Fireware XTM

Web UI
11.4 User Guide

WatchGuard XTM Devices

About this User Guide

The *Fireware XTM Web UI User Guide* is updated with each major product release. For minor product releases, only the *Fireware XTM Web UI Help* system is updated. The Help system also includes specific, task-based implementation examples that are not available in the *User Guide*.

Fireware XTM Web UI Help

Guide revised: 1/26/2011

Copyright, Trademark, and Patent Information

Note *This product is for indoor use only.*

About WatchGuard

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

Table of Contents

1 Introduction to Network Security

About Networks and Network Security

A *network* is a group of computers and other devices that are connected to each other. It can be two computers in the same room, dozens of computers in an organization, or many computers around the world connected through the Internet. Computers on the same network can work together and share data.

Although networks like the Internet give you access to a large quantity of information and business opportunities, they can also open your network to attackers. Many people think that their computers hold no important information, or that a hacker is not interested in their computers. This is not correct. A hacker can use your computer as a platform to attack other computers or networks. Information from your organization, including personal information about users, employees, or customers, is also valuable to hackers.

Your XTM device and LiveSecurity subscription can help you prevent these attacks. A good network security policy, or a set of access rules for users and resources, can also help you find and prevent attacks to your computer or network. We recommend that you configure your XTM device to match your security policy, and think about threats from both inside and outside your organization.

About Internet Connections

ISPs (Internet service providers) are companies that give access to the Internet through network connections. The rate at which a network connection can send data is known as *bandwidth*: for example, 3 megabits per second (Mbps).

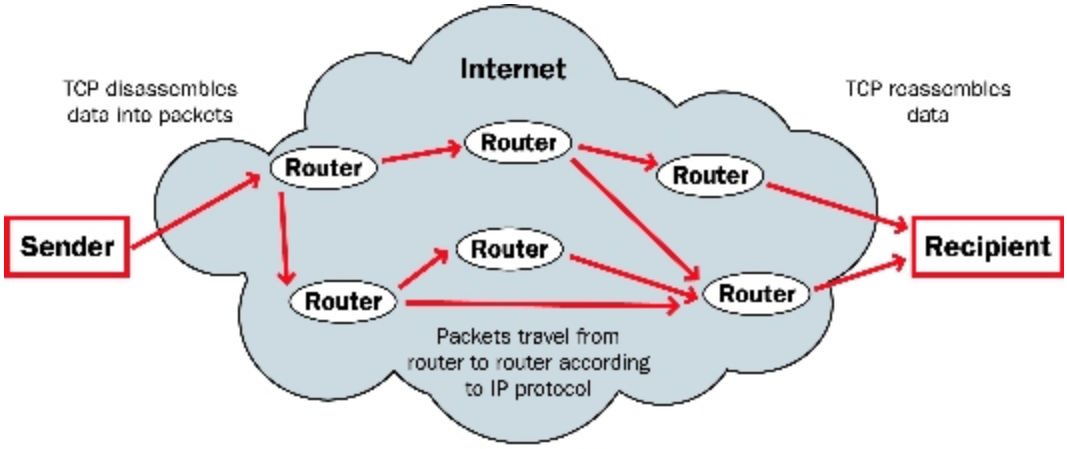
A high-speed Internet connection, such as a cable modem or a DSL (Digital Subscriber Line), is known as a *broadband connection*. Broadband connections are much faster than dial-up connections. The bandwidth of a dial-up connection is less than .1 Mbps, while a cable modem can be 5 Mbps or more.

Typical speeds for cable modems are usually lower than the maximum speeds, because each computer in a neighborhood is a member of a LAN. Each computer in that LAN uses some of the bandwidth. Because of this *shared-medium* system, cable modem connections can become slow when more users are on the network.

DSL connections supply constant bandwidth, but they are usually slower than cable modem connections. Also, the bandwidth is only constant between your home or office and the DSL central office. The DSL central office cannot guarantee a good connection to a web site or network.

How Information Travels on the Internet

The data that you send through the Internet is cut into units, or packets. Each packet includes the Internet address of the destination. The packets that make up a connection can use different routes through the Internet. When they all get to their destination, they are assembled back into the original order. To make sure that the packets get to the destination, address information is added to the packets.



About Protocols

A *protocol* is a group of rules that allow computers to connect across a network. Protocols are the *grammar* of the language that computers use when they speak to each other across a network. The standard protocol when you connect to the Internet is the IP (Internet Protocol). This protocol is the usual language of computers on the Internet.

A protocol also tells how data is sent through a network. The most frequently used protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP/IP is the basic protocol used by computers that connect to the Internet.

You must know some of the TCP/IP settings when you set up your XTM device. For more information on TCP/IP, see *Find Your TCP/IP Properties* on page 33.

About IP Addresses

To send ordinary mail to a person, you must know his or her street address. For one computer on the Internet to send data to a different computer, it must know the address of that computer. A computer address is known as an *Internet Protocol (IP) address*. All devices on the Internet have unique IP addresses, which enable other devices on the Internet to find and interact with them.

An IP address consists of four octets (8-bit binary number sequences) expressed in decimal format and separated by periods. Each number between the periods must be within the range of 0 and 255. Some examples of IP addresses are:

- 206.253.208.100
- 4.2.2.2
- 10.0.4.1

Private Addresses and Gateways

Many companies create private networks that have their own address space. The addresses 10.x.x.x and 192.168.x.x are reserved for private IP addresses. Computers on the Internet cannot use these addresses. If your computer is on a private network, you connect to the Internet through a *gateway* device that has a public IP address.

Usually, the *default gateway* is the router that is between your network and the Internet. After you install the XTM device on your network, it becomes the default gateway for all computers connected to its trusted or optional interfaces.

About Subnet Masks

Because of security and performance considerations, networks are often divided into smaller portions called subnets. All devices in a subnet have similar IP addresses. For example, all devices that have IP addresses whose first three octets are 50.50.50 would belong to the same subnet.

A network IP address's subnet mask, or netmask, is a series of bits that *mask* sections of the IP address that identify which parts of the IP address are for the network and which parts are for the host. A subnet mask can be written in the same way as an IP address, or in slash or CIDR notation.

About Slash Notation

Your XTM device uses *slash notation* for many purposes, including policy configuration. Slash notation, also known as CIDR (Classless Inter-Domain Routing) notation, is a compact way to show or write a subnet mask. When you use slash notation, you write the IP address, a forward slash (/), and the subnet mask number.

To find the subnet mask number:

1. Convert the decimal representation of the subnet mask to a binary representation.
2. Count each "1" in the subnet mask. The total is the subnet mask number.

For example, to write the IP address 192.168.42.23 with a subnet mask of 255.255.255.0 in slash notation:

1. Convert the subnet mask to binary.
   In this example, the binary representation of 255.255.255.0 is: 11111111.11111111.11111111.00000000.
2. Count each *1* in the subnet mask.
   In this example, there are twenty-four (24).
3. Write the original IP address, a forward slash (/), and then the number from Step 2.
   The result is 192.168.42.23/24.

This table shows common network masks and their equivalents in slash notation.

Network mask	Slash equivalent
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

About Entering IP Addresses

When you type IP addresses in the Quick Setup Wizard or dialog boxes, type the digits and decimals in the correct sequence. Do not use the TAB key, arrow keys, spacebar, or mouse to put your cursor after the decimals.

For example, if you type the IP address 172.16.1.10, do not type a space after you type *16*. Do not try to put your cursor after the subsequent decimal to type *1*. Type a decimal directly after *16*, and then type *1.10*. Press the slash (/) key to move to the netmask.

Static and Dynamic IP Addresses

ISPs (Internet service providers) assign an IP address to each device on their network. The IP address can be *static* or *dynamic*.

Static IP Addresses

A static IP address is an IP address that always stays the same. If you have a web server, FTP server, or other Internet resource that must have an address that cannot change, you can get a static IP address from your ISP. A static IP address is usually more expensive than a dynamic IP address, and some ISPs do not supply static IP addresses. You must configure a static IP address manually.

Dynamic IP Addresses

A dynamic IP address is an IP address that an ISP lets you use temporarily. If a dynamic address is not in use, it can be automatically assigned to a different device. Dynamic IP addresses are assigned using either DHCP or PPPoE.

About DHCP

Dynamic Host Configuration Protocol (DHCP) is an Internet protocol that computers on a network use to get IP addresses and other information such as the default gateway. When you connect to the Internet, a computer configured as a DHCP server at the ISP automatically assigns you an IP address. It could be the same IP address you had before, or it could be a new one. When you close an Internet connection that uses a dynamic IP address, the ISP can assign that IP address to a different customer.

You can configure your XTM device as a DHCP server for networks behind the device. You assign a range of addresses for the DHCP server to use.

About PPPoE

Some ISPs assign IP addresses through Point-to-Point Protocol over Ethernet (PPPoE). PPPoE adds some of the features of Ethernet and PPP to a standard dial-up connection. This network protocol allows the ISP to use the billing, authentication, and security systems of their dial-up infrastructure with DSL modem and cable modem products.

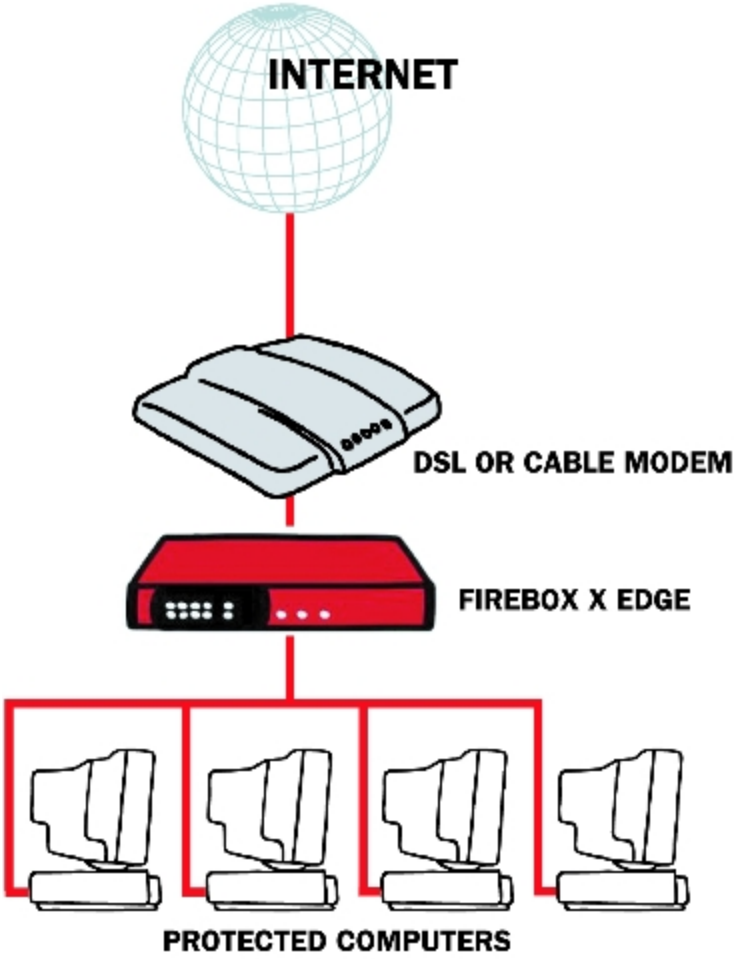
About DNS (Domain Name System)

You can frequently find the address of a person you do not know in the telephone directory. On the Internet, the equivalent to a telephone directory is the *DNS*(Domain Name System). DNS is a network of servers that translate numeric IP addresses into readable Internet addresses, and vice versa. DNS takes the *friendly* domain name you type when you want to see a particular web site, such as www.example.com, and finds the equivalent IP address, such as 50.50.50.1. Network devices need the actual IP address to find the web site, but domain names are much easier for users to type and remember than IP addresses.

A *DNS server* is a server that performs this translation. Many organizations have a private DNS server in their network that responds to DNS requests. You can also use a DNS server on your external network, such as a DNS server provided by your ISP (Internet Service Provider.)

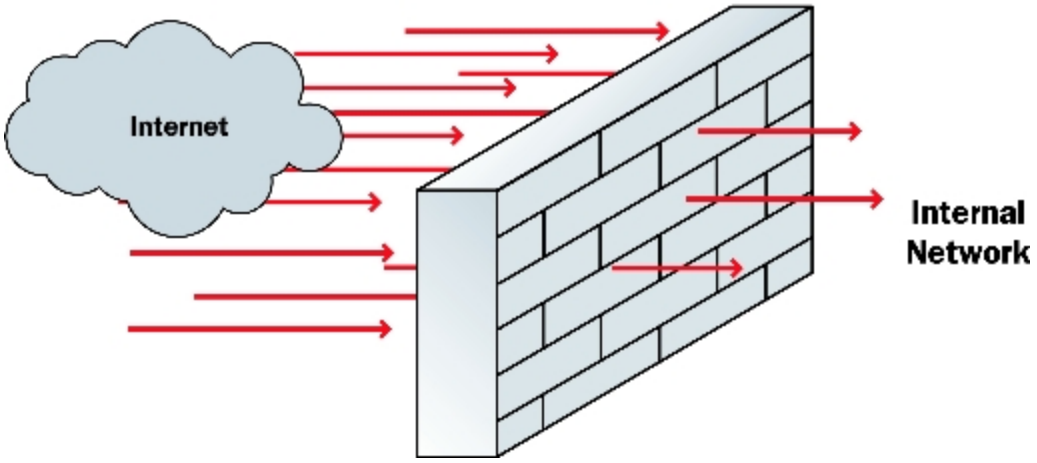
About Firewalls

A network security device, such as a firewall, separates your internal networks from external network connections to decrease the risk of an external attack. The figure below shows how a firewall protects the computers on a trusted network from the Internet.



Firewalls use access policies to identify and filter different types of information. They can also control which policies or ports the protected computers can use on the Internet (outbound access). For example, many firewalls have sample security policies that allow only specified traffic types. Users can select the policy that is best for them. Other firewalls, such as XTM devices, allow the user to customize these policies.

For more information, see *About Services and Policies* on page 7 and *About Ports* on page 8



Firewalls can be in the form of hardware or software. A firewall protects private networks from unauthorized users on the Internet. Traffic that enters or leaves the protected networks is examined by the firewall. The firewall denies network traffic that does not match the security criteria or policies.

In some closed, or *default-deny* firewalls, all network connections are denied unless there is a specific rule to allow the connection. To deploy this type of firewall, you must have detailed information about the network applications required to meet needs of your organization . Other firewalls allow all network connections that have not been explicitly denied. This type of open firewall is easier to deploy, but it is not as secure.

About Services and Policies

You use a *service* to send different types of data (such as email, files, or commands) from one computer to another across a network or to a different network. These services use protocols. Frequently used Internet services are:

- World Wide Web access uses Hypertext Transfer Protocol (HTTP)
- Email uses Simple Mail Transfer Protocol (SMTP) or Post Office Protocol (POP3)
- File transfer uses File Transfer Protocol (FTP)
- Resolve a domain name to an Internet address uses Domain Name Service (DNS)
- Remote terminal access uses Telnet or SSH (Secure Shell)

When you allow or deny a service, you must add a *policy* to your XTM device configuration. Each policy you add can also add a security risk. To send and receive data, you must *open a door* in your computer, which puts your network at risk. We recommend that you add only the policies that are necessary for your business.

As an example of how you can use a policy, suppose the network administrator of a company wants to activate a Windows terminal services connection to the company's public web server on the optional interface of the XTM device. He or she routinely administers the web server with a Remote Desktop

connection. At the same time, he or she wants to make sure that no other network users can use the Remote Desktop Protocol terminal services through the XTM device. The network administrator would add a policy that allows RDP connections only from the IP address of his or her own desktop computer to the IP address of the public web server.

When you configure your XTM device with the Quick Setup Wizard, the wizard adds only limited outgoing connectivity. If you have more software applications and network traffic for your XTM device to examine, you must:

- Configure the policies on your XTM device to pass through necessary traffic
- Set the approved hosts and properties for each policy
- Balance the requirement to protect your network against the requirements of your users to get access to external resources

About Ports

Although computers have hardware ports you use as connection points, ports are also numbers used to map traffic to a particular process on a computer. These ports, also called *TCP and UDP ports*, are where programs transmit data. If an IP address is like a street address, a port number is like an apartment unit number or building number within that street address. When a computer sends traffic over the Internet to a server or another computer, it uses an IP address to identify the server or remote computer, and a port number to identify the process on the server or computer that receives the data.

For example, suppose you want to see a particular web page. Your web browser attempts to create a connection on port 80 (the port used for HTTP traffic) for each element of the web page. When your browser receives the data it requests from the HTTP server, such as an image, it closes the connection.

Many ports are used for only one type of traffic, such as port 25 for SMTP (Simple Mail Transfer Protocol). Some protocols, such as SMTP, have ports with assigned numbers. Other programs are assigned port numbers dynamically for each connection. The IANA (Internet Assigned Numbers Authority) keeps a list of well-known ports. You can see this list at:
http://www.iana.org/assignments/port-numbers

Most policies you add to your XTM device configuration have a port number between 0 and 1024, but possible port numbers can be from 0 to 65535.

Ports are either open or closed. If a port is open, your computer accepts information and uses the protocol identified with that port to create connections to other computers. However, an open port is a security risk. To protect against risks created by open ports, you can block ports used by hackers to attack your network. For more information, see *About Blocked Ports* on page 453.

The XTM Device and Your Network

Your XTM device is a powerful network security device that controls all traffic between the external network and the trusted network. If computers with *mixed trust* connect to your network, you can also configure an optional network interface that is separate from the trusted network. You can then configure the firewall on your device to stop all suspicious traffic from the external network to your trusted and

optional networks. If you route all traffic for the *mixed trust* computers through your optional network, you can increase the security for those connections to add more flexibility to your security solution. For example, customers frequently use the optional network for their remote users or for public servers such as a web server or an email server.

Some customers who purchase an XTM device do not know a lot about computer networks or network security. Fireware XTM Web UI (web-based user interface), provides many self-help tools for these customers. Advanced customers can use the advanced integration and multiple WAN support features of the Fireware XTM OS with a Pro upgrade to connect an XTM device to a larger wide area network. The XTM device connects to a cable modem, DSL modem, or ISDN router.

You can use the Web UI to safely manage your network security settings from different locations at any time. This gives you more time and resources to use on other components of your business.

2 Introduction to Fireware XTM

About Fireware XTM

Fireware XTM gives you an easy and efficient way to view, manage, and monitor each XTM device in your network. The Fireware XTM solution includes four software applications:

- WatchGuard System Manager (WSM)
- Fireware XTM Web UI
- Fireware XTM Command Line Interface (CLI)
- WatchGuard Server Center

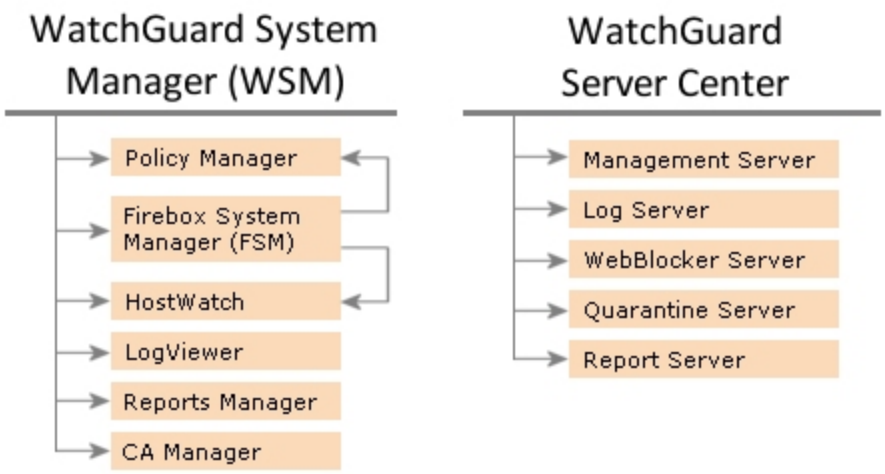
You can use one or more of the Fireware XTM applications to configure your network for your organization. For example, if you have only one XTM 2 Series device, you can perform most configuration tasks with Fireware XTM Web UI or Fireware XTM Command Line Interface. However, for more advanced logging and reporting features, you must use WatchGuard Server Center. If you manage more than one XTM device, or if you have purchased Fireware XTM with a Pro upgrade, we recommend that you use WatchGuard System Manager (WSM). If you choose to manage and monitor your configuration with Fireware XTM Web UI, there are some features that you cannot configure.

For more information about these limitations, see *Limitations of Fireware XTM Web UI*.

For more information on how to connect to your XTM device with WatchGuard System Manager or Fireware XTM Command Line Interface, see the *Help* or *User Guide* for those products. You can view and download the most current documentation for these products on the Fireware XTM Product Documentation page:
http://www.watchguard.com/help/documentation/xtm.asp

Fireware XTM Components

To start WatchGuard System Manager or WatchGuard Server Center from your Windows desktop, select the shortcut from the Start Menu. You can also start WatchGuard Server Center from an icon in the System Tray. From these applications, you can launch other tools that help you manage your network. For example, from WatchGuard System Manager (WSM), you can launch Policy Manager or HostWatch.



WatchGuard System Manager

WatchGuard System Manager (WSM) is the primary application for network management with your XTM device. You can use WSM to manage many different XTM devices, even those that use different software versions. WSM includes a comprehensive suite of tools to help you monitor and control network traffic.

Policy Manager

You can use Policy Manager to configure your firewall. Policy Manager includes a full set of pre-configured packet filters, proxy policies, and application layer gateways (ALGs). You can also make a custom packet filter, proxy policy, or ALG in which you set the ports, protocols, and other options. Other features of Policy Manager help you to stop network intrusion attempts, such as SYN Flood attacks, spoofing attacks, and port or address space probes.

Firebox System Manager (FSM)

Firebox System Manager gives you one interface to monitor all components of your XTM device. From FSM, you can see the real-time status of your XTM device and its configuration.

HostWatch

HostWatch is a real-time connection monitor that shows network traffic between different XTM device interfaces. HostWatch also shows information about users, connections, ports, and services.

LogViewer

LogViewer is the WatchGuard System Manager tool you use to see log file data. It can show the log data page by page, or search and display by key words or specified log fields.

Report Manager

You can use Report Manager to generate reports of the data collected from your Log Servers for all your XTM devices. From Report Manager, you can see the available WatchGuard Reports for you XTM devices.

CA Manager

The Certificate Authority (CA) Manager shows a complete list of security certificates installed on your management computer with Fireware XTM. You can use this application to import, configure, and generate certificates for use with VPN tunnels and other authentication purposes.

WatchGuard Server Center

WatchGuard Server Center is the application where you configure and monitor all your WatchGuard servers.

Management Server

The Management Server operates on a Windows computer. With this server, you can manage all firewall devices and create virtual private network (VPN) tunnels using a simple drag-and-drop function. The basic functions of the Management Server are:

- Certificate authority to distribute certificates for Internet Protocol Security (IPSec) tunnels
- VPN tunnel configuration management
- Management for multiple XTM devices

Log Server

The Log Server collects log messages from each XTM device. These log messages are encrypted when they are sent to the Log Server. The log message format is XML (plain text). The information collected from firewall devices includes these log messages: traffic, event, alarm, debug (diagnostic), and statistic.

WebBlocker Server

The WebBlocker Server operates with the XTM device HTTP proxy to deny user access to specified categories of web sites. When you configure your XTM device, you specify the categories of web sites to allow or block.

For more information on WebBlocker and the WebBlocker Server, see *About WebBlocker*.

Quarantine Server

The Quarantine Server collects and isolates email messages that spamBlocker suspects to be email spam, or emails that are suspected to have a virus.

For more information, see *About the Quarantine Server*.

Report Server

The Report Server periodically consolidates data collected by your Log Servers from your XTM devices, and then periodically generates reports. Once the data is on the Report Server, you can use Report Manager to generate and see reports.

Fireware XTM Web UI and Command Line Interface

Fireware XTM Web UI and Command Line Interface are alternative management solutions that can perform most of the same tasks as WatchGuard System Manager and Policy Manager. Some advanced configuration options and features, such as FireCluster settings, are not available in Fireware XTM Web UI or Command Line Interface.

For more information, see *About Fireware XTM Web UI*.

Fireware XTM with a Pro Upgrade

The Pro upgrade to Fireware XTM provides several advanced features for experienced customers, such as server load balancing and additional SSL VPN tunnels. The features available with a Pro upgrade depend on the type and model of your XTM device:

Feature	XTM 5 Series	XTM 5 Series, 8 Series, and 1050 (Pro)	XTM 2 Series	XTM 2 Series (Pro)
FireCluster		X		
VLANs	75 max.	75 max. (Core/5 Series) 200 max. (Peak/XTM 8 Series and 1050)	20 max.	50 max.
Dynamic Routing (OSPF and BGP)		X		X
Policy-Based Routing		X		X
Server Load Balancing		X		
Maximum SSL VPN Tunnels		X		X
Multi-WAN Failover	X	X		X
Multi-WAN Load Balancing		X		X

To purchase Fireware XTM with a Pro upgrade, contact your local reseller.

3 Service and Support

About WatchGuard Support

WatchGuard® knows just how important support is when you must secure your network with limited resources. Our customers require greater knowledge and assistance in a world where security is critical. LiveSecurity® Service gives you the backup you need, with a subscription that supports you as soon as you register your XTM device.

LiveSecurity Service

Your XTM device includes a subscription to our ground-breaking LiveSecurity Service, which you activate online when you register your product. As soon as you activate, your LiveSecurity Service subscription gives you access to a support and maintenance program unmatched in the industry.

LiveSecurity Service comes with the following benefits:

Hardware Warranty with Advance Hardware Replacement

An active LiveSecurity subscription extends the one-year hardware warranty that is included with each XTM device. Your subscription also provides advance hardware replacement to minimize downtime in case of a hardware failure. If you have a hardware failure, WatchGuard will ship a replacement unit to you before you have to send back the original hardware.

Software Updates

Your LiveSecurity Service subscription gives you access to updates to current software and functional enhancements for your WatchGuard products.

Technical Support

When you need assistance, our expert teams are ready to help:

- Representatives available 12 hours a day, 5 days a week in your local time zone*
- Four-hour targeted maximum initial response time
- Access to online user forums moderated by senior support engineers

Support Resources and Alerts

Your LiveSecurity Service subscription gives you access to a variety of professionally produced instructional videos, interactive online training courses, and online tools specifically designed to answer questions you may have about network security in general or the technical aspects of installation, configuration, and maintenance of your WatchGuard products.

Our Rapid Response Team, a dedicated group of network security experts, monitors the Internet to identify emerging threats. They then deliver LiveSecurity Broadcasts to tell you specifically what you can do to address each new menace. You can customize your alert preferences to fine-tune the kind of advice and alerts the LiveSecurity Service sends you.

LiveSecurity Service Gold

LiveSecurity Service Gold is available for companies that require 24-hour availability. This premium support service gives expanded hours of coverage and faster response times for around-the-clock remote support assistance. LiveSecurity Service Gold is required on each unit in your organization for full coverage.

Service Features	LiveSecurity Service	LiveSecurity Service Gold
Technical Support hours	6AM–6PM, Monday–Friday*	24/7
Number of support incidents (online or by phone)	5 per year	Unlimited
Targeted initial response time	4 hours	1 hour
Interactive support forum	Yes	Yes
Software updates	Yes	Yes
Online self-help and training tools	Yes	Yes
LiveSecurity broadcasts	Yes	Yes
Installation Assistance	Optional	Optional
Three-incident support package	Optional	N/A
One-hour, single incident priority response upgrade	Optional	N/A
Single incident after-hours upgrade	Optional	N/A

* *In the Asia Pacific region, standard support hours are 9AM–9PM, Monday–Friday (GMT +8).*

Service Expiration

To secure your organization, we recommend that you keep your LiveSecurity subscription active. When your subscription expires, you lose up-to-the-minute security warnings and regular software updates. This loss can put your network at risk. Damage to your network is much more expensive than a LiveSecurity Service subscription renewal. If you renew within 30 days, there is no reinstatement fee.

4 Getting Started

Before You Begin

Before you begin the installation process, make sure you complete the tasks described in the subsequent sections.

> ***Note*** *In these installation instructions, we assume your XTM device has one trusted, one external, and one optional interface configured. To configure additional interfaces on your device, use the configuration tools and procedures described in the Network Setup and Configuration topics.*

Verify Basic Components

Make sure that you have these items:

- A computer with a 10/100BaseT Ethernet network interface card and a web browser installed
- A WatchGuard XTM device
- A serial cable (blue)
- One crossover Ethernet cable (red)
- One straight Ethernet cable (green)
- Power cable or AC power adapter

Get an XTM Device Feature Key

To enable all of the features on your XTM device, you must register the device on the WatchGuard LiveSecurity web site and get your feature key. The XTM device has only one user license (seat license) until you apply your feature key.

If you register your XTM device before you use the Quick Setup Wizard, you can paste a copy of your feature key in the wizard. The wizard then applies it to your device. If you do not paste your feature key into the wizard, you can still finish the wizard. Until you add your feature key, only one connection is allowed to the Internet.

You also get a new feature key for any optional products or services when you purchase them. After you register your XTM device or any new feature, you can synchronize your XTM device feature key with the feature keys kept in your registration profile on the WatchGuard LiveSecurity site. You can use Fireware XTM Web UI at any time to get your feature key.

To learn how to register your XTM device and get a feature key, see *Get a Feature Key from LiveSecurity* on page 51.

Gather Network Addresses

We recommend that you record your network information before and after you configure your XTM device. Use the first table below for your network IP addresses before you put the device into operation. For information about how to identify your network IP addresses, see *Identify Your Network Settings* on page 32.

WatchGuard uses slash notation to show the subnet mask. For more information, see *About Slash Notation* on page 3. For more information on IP addresses, see *About IP Addresses* on page 3.

Table 1: Network IP addresses without the XTM device	
Wide Area Network	_____._____._____._____ / ____
Default Gateway	_____._____._____._____
Local Area Network	_____._____._____._____ / ____
Secondary Network (if applicable)	_____._____._____._____ / ____
Public Server(s) (if applicable)	_____._____._____._____
	_____._____._____._____
	_____._____._____._____

Use the second table for your network IP addresses after you put the XTM device into operation.

External interface

Connects to the external network (typically the Internet) that is not trusted.

Trusted interface

Connects to the private LAN (local area network) or internal network that you want to protect.

Optional interface(s)

Usually connects to a mixed trust area of your network, such as servers in a DMZ (demilitarized zone). You can use optional interfaces to create zones in the network with different levels of access.

Table 2: Network IP addresses with the XTM device	
Default Gateway	_____._____._____._____
External Interface	_____._____._____._____/ ____
Trusted Interface	_____._____._____._____ / ____
Optional Interface	_____._____._____._____ / ____
Secondary Network (if applicable)	_____._____._____._____ / ____

Select a Firewall Configuration Mode

You must decide how you want to connect the XTM device to your network before you run the Quick Setup Wizard. The way you connect the device controls the interface configuration. When you connect the device, you select the configuration mode—routed or drop-in—that is best suited to your current network.

Many networks operate best with mixed routing configuration, but we recommend the drop-in mode if:

- You have already assigned a large number of static IP addresses and do not want to change your network configuration.
- You cannot configure the computers on your trusted and optional networks that have public IP addresses with private IP addresses.

This table and the descriptions below the table show three conditions that can help you to select a firewall configuration mode.

Mixed Routing Mode	Drop-in Mode
All of the XTM device interfaces are on different networks.	All of the XTM device interfaces are on the same network and have the same IP address.
Trusted and optional interfaces must be on different networks. Each interface has an IP address on its network.	The computers on the trusted or optional interfaces can have a public IP address.
Use static NAT (network address translation) to map public addresses to private addresses behind the trusted or optional interfaces.	NAT is not necessary because the computers that have public access have public IP addresses.

For more information about drop-in mode, see *Drop-In Mode* on page 90.

For more information about mixed routing mode, see *Mixed Routing Mode* on page 83.

The XTM device also supports a third configuration mode called bridge mode. This mode is less commonly used. For more information about bridge mode, see *Bridge Mode* on page 96.

> ***Note*** *You can use the Web Setup Wizard or the WSM Quick Setup Wizard to create your initial configuration. When you run the Web Setup Wizard, the firewall configuration is automatically set to mixed routing mode. When you run the WSM Quick Setup Wizard, you can configure the device in mixed routing mode or drop-in mode.*

You can now start the Quick Setup Wizard. For more information, see *About the Quick Setup Wizard* on page 22.

About the Quick Setup Wizard

You can use the Quick Setup Wizard to create a basic configuration for your XTM device. The device uses this basic configuration file when it starts for the first time. This enables it to operate as a basic firewall. You can use this same procedure at any time to reset the device to a new basic configuration. This is helpful for system recovery.

When you configure your XTM device with the Quick Setup Wizard, you set only the basic policies (TCP and UDP outgoing, FTP packet filter, ping, and WatchGuard) and interface IP addresses. If you have more software applications and network traffic for the device to examine, you must:

- Configure the policies on the XTM device to let the necessary traffic through
- Set the approved hosts and properties for each policy
- Balance the requirement to protect your network against the requirements of your users to connect to external resources

For instructions to run the wizard from a web browser, see *Run the Web Setup Wizard* on page 23.

Run the Web Setup Wizard

You can use the Web Setup Wizard to set up a basic configuration on any WatchGuard XTM device. The Web Setup Wizard automatically configures the XTM device for mixed routing mode.

To use the Web Setup Wizard, you must make a direct network connection to the XTM device and use a web browser to start the wizard. When you configure your XTM device, it uses DHCP to send a new IP address to your computer.

Before you start the Web Setup Wizard, make sure you:

- Register your XTM device with LiveSecurity Service
- Store a copy of your XTM device feature key in a text file on your computer

Start the Web Setup Wizard

1. Use the red crossover Ethernet cable that ships with your XTM device to connect the management computer to interface number 1 of your XTM device. This is the trusted interface.
2. Connect the power cord to the XTM device power input and to a power source.
3. Start the XTM device in factory default mode. This is also known as safe mode.

   For more information, see *Reset an XTM Device to a Previous or New Configuration* on page 47.
4. Make sure your computer is configured to accept a DHCP-assigned IP address.

   If your computer uses Windows XP:

   - In the Windows **Start** menu, select **All Programs > Control Panel > Network Connections > Local Area Connections**.
   - Click **Properties**.
   - Select **Internet Protocol (TCP/IP)** and click **Properties**.
   - Make sure **Obtain an IP Address Automatically** is selected.

   For more detailed instructions, see *Identify Your Network Settings* on page 32.
5. If your browser uses an HTTP proxy server, you must temporarily disable the HTTP proxy setting in your browser.

   For more information, see *Disable the HTTP Proxy in the Browser* on page 36.
6. Open a web browser and type the factory default IP address of the trusted interface (interface 1), `https://10.0.1.1:8080`.
   If you use Internet Explorer, make sure you type `https://` at the start of the IP address. This opens a secure HTTP connection between your management computer and the XTM device.
   The Web Setup Wizard starts automatically.
7. Log in with the default administrator account credentials:
   Username: `admin`
   Passphrase: `readwrite`

8. Complete the subsequent screens of the wizard.

   The Web Setup Wizard includes this set of dialog boxes. Some dialog boxes appear only if you select certain configuration methods:

   Login

   Log in with the default administrator account credentials. For **Username**, select admin. For **Passphrase**, use the passphrase: readwrite.

   Welcome

   The first screen tells you about the wizard.

   Select a configuration type

   Select whether to create a new configuration or restore a configuration from a saved backup image.

   License agreement

   You must accept the license agreement to continue with the wizard.

   Retrieve Feature Key, Apply Feature Key, Feature key options

   If your XTM device does not already have a feature key the wizard provides options for you to download or import a feature key. The wizard can only download a feature key if it has a connection to the Internet. If you have downloaded a local copy of the feature key to your computer, you can paste that into the setup wizard.

   If the XTM device does not have an Internet connection while you run the wizard, and you did not register the device and download the feature key to your computer before you started the wizard, you can choose to not apply a feature key.

   Note *If you do not apply a feature key in the Web Setup Wizard you must register the device and apply the feature key in the Fireware XTM Web UI. Functionality of the device is limited until you apply a feature key.*

   Configure the External Interface of your Firebox

   Select the method your ISP uses to assign your IP address. The choices are DHCP, PPPoE or Static.

   Configure the External Interface for DHCP

   Type your DHCP identification as supplied by your ISP.

   Configure the External Interface for PPPoE

   Type your PPPoE information as supplied by your ISP.

   Configure the External Interface with a static IP address

   Type your static IP address information as supplied by your ISP.

   Configure the DNS and WINS Servers

   Type the Domain DNS and WINS server addresses you want the XTM device to use.

Configure the Trusted Interface of the Firebox

Type the IP address of the trusted interface. Optionally, you can enable the DHCP server for the trusted interface.

Create passphrases for your device

Type a passphrase for the status (read only) and admin (read/write) management accounts on the XTM device.

Enable remote management

Enable remote management if you want to manage this device from the external interface.

Add contact information for your device

You can type a device name, location, and contact information to save management information for this device. By default, the device name is set to the model number of your XTM device. We recommend that you choose a unique name that you can use to easily identify this device, especially if you use remote management.

Set the Time Zone

Select the time zone where the XTM device is located.

The Quick Setup Wizard is complete

After you complete the wizard, the XTM device restarts.

If you leave the Web Setup Wizard idle for 15 minutes or more, you must go back to Step 3 and start again.

> ***Note*** *If you change the IP address of the trusted interface, you must change your network settings to make sure your IP address matches the subnet of the trusted network before you connect to the XTM device. If you use DHCP, restart your computer. If you use static addressing, see Use a Static IP Address on page 35.*

After the Wizard Finishes

After you complete all screens in the wizard, the XTM device is configured with a basic configuration that includes four policies (TCP outgoing, FTP packet filter, ping, and WatchGuard) and the interface IP addresses you specified. You can use Fireware XTM Web UI to expand or change the configuration for your XTM device.

- For information about how to complete the installation of your XTM device after the Web Setup Wizard is finished, see *Complete Your Installation* on page 30.
- For information about how to connect to Fireware XTM Web UI, see *Connect to Fireware XTM Web UI* on page 26.

If You Have Problems with the Wizard

If the Web Setup Wizard is unable to install the Fireware XTM OS on the XTM device, the wizard times out. If you have problems with the wizard, check these things:

- The Fireware XTM OS file you downloaded from the LiveSecurity web site could be corrupted. For an XTM 5 Series, 8 Series, or 1050 device, if the software image is corrupted, this message can appear on the LCD interface: *File Truncate Error*.

  If this message appears, download the software again and try the wizard once more.
- If you use Internet Explorer 6, clear the file cache in your web browser and try again.

  To clear the cache, in Internet Explorer select **Tools > Internet Options > Delete Files**.

Connect to Fireware XTM Web UI

To connect to Fireware XTM Web UI, you use a web browser to go to the IP address of the XTM device trusted or optional interface over the correct port number. Connections to the Web UI are always encrypted with HTTPS; the same high-strength encryption used by banking and shopping web sites. You must use https when you type the URL into your browser's address bar instead of http.

By default, the port used for the Web UI is 8080. The URL to connect to the Web UI in your browser is:

```
https://<firebox-ip-address>:8080
```

Where <firebox-ip-address> is the IP address assigned to the trusted or optional interface. When you make this connection, the browser loads the login prompt. The default URL for a WatchGuard XTM device is:

```
https://10.0.1.1:8080
```

You can change the IP address of the trusted network to a different IP address. For more information, see *Common Interface Settings* on page 98.

For example, to use the default URL to connect to an XTM 2 Series device:

1. Open your web browser and go to `https://10.0.1.1:8080`.
   A security certificate notification appears in the browser.
2. When you see the certificate warning, click **Continue to this website** (IE 7) or **Add Exception** (Firefox 3).
   This warning appears because the certificate the XTM device uses is signed by the WatchGuard certificate authority, which is not in the list of trusted authorities on your browser.

   > ***Note*** *This warning appears each time you connect to the XTM device unless you permanently accept the certificate, or generate and import a certificate for the device to use. For more information, see About Certificates on page 491.*
3. From the **Username** drop-down list, select the user name.

4. In the **Passphrase** text box, type the passphrase.
   - If you selected the Username **admin**, type the configuration (read-write) passphrase.
   - If you selected the Username **status**, type the status (read-only) passphrase.

Note *By default, the XTM device configuration only allows connections to Fireware XTM Web UI from the trusted and optional networks. To change the configuration to allow connections to the Web UI from the external network, see Connect to Fireware XTM Web UI from an External Network on page 27.*

Connect to Fireware XTM Web UI from an External Network

The Fireware XTM device configuration has a policy called **WatchGuard Web UI**. This policy controls which XTM device interfaces can connect to Fireware XTM Web UI. By default, this policy only allows connections from **Any-Trusted** and **Any-Optional** networks. If you want to allow access to the Web UI from the external network, you must edit the **WatchGuard Web UI** policy and add **Any-External** to the **From** list.

In Fireware XTM Web UI:

1. Select **Firewall > Firewall Policies**.
2. Double-click the **WatchGuard Web UI** policy to edit it.
3. Select the **Policy** tab.
4. In the **From** section, click **Add**.
5. Select **Any-External**.
6. Click **OK**.
7. Click **Save**.

About Fireware XTM Web UI

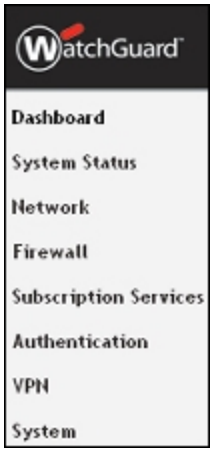
The Fireware XTM Web UI lets you monitor and manage any XTM device without any extra software installed on your computer. The only software you need is a browser with support for Adobe Flash.

Because there is no software to install, you can use the Web UI from any computer that has TCP/IP connectivity and a browser. This means you can administer your XTM device from a computer running Windows, Linux, Mac OS, or any other platform, as long as it has a supported browser with Adobe Flash 9 and network connectivity.

The Web UI is a real-time management tool. This means that when you use the Web UI to make changes to a device, the changes you make generally take effect immediately. The Web UI does not let you build a list of changes to a locally-stored configuration file, to send many changes to the device all at once at a later time. This is different from the Fireware XTM Policy Manager, which is an off-line configuration tool. Changes you make to a locally-stored configuration file using Policy Manager do not take effect until you save the configuration to the device.

> ***Note*** *You must complete the Quick Setup Wizard before you can see Fireware XTM Web UI. For more information, see Run the Web Setup Wizard on page 23. You must also use an account with full administrative access privileges to see and change the configuration pages.*

At the left side of Fireware XTM Web UI is the main menu navigation bar you use to select a set of configuration pages.



The top item in the navigation bar is the **Dashboard**, which returns you to the Fireware XTM Dashboard page that you see when you first connect to Fireware XTM Web UI.

All of the other items on the navigation bar contain secondary menu items that you use to configure the properties of that feature.

- To see these secondary menu items, click the menu item name. For example, if you click **Authentication**, these secondary menu items appear: **Servers, Settings**, **Users and Groups**, **Web Server Certificate**, and **Single Sign-On**.
- To hide the secondary menu items, click the top level menu item again.

To show menu items that you expand or click, the documentation uses the right arrow (>) symbol. Menu names are in **bold** text. For example, the command to open the **Authentication Settings** page appears in the text as **Authentication > Settings**.

Limitations of Fireware XTM Web UI

You can use Fireware XTM Web UI, WatchGuard System Manager, and Fireware XTM Command Line Interface (CLI) to configure and monitor your Fireware XTM device. When you want to change a device configuration file, you can use any of these programs. There are, however, several device configuration changes you cannot make with Fireware XTM Web UI.

Some of the tasks you can complete in Policy Manager, but not with the Web UI include:

- Export a certificate or see details about a certificate (You can only import certificates)
- Enable diagnostic logging or change diagnostic log levels
- Change the logging of default packet handling options
- Enable or disable notification of branch office VPN events
- Add or remove static ARP entries in the device ARP table
- Manually get the Mobile VPN with SSL configuration file
- Get the encrypted (.wgx) Mobile VPN with IPSec end-user client configuration (You can only get the equivalent, but unencrypted, .ini file)
- Edit the name of a policy
- Add a custom address to a policy
- Use a host name (DNS lookup) to add an IP address to a policy
- Use role-based administration (also known as role-based access control, or RBAC)
- View or change the configuration of a device that is a member of a FireCluster

The group of applications that comes with WatchGuard System Manager includes many other tools for monitoring and reporting. Some of the functions provided by HostWatch, LogViewer, Report Manager, and WSM are also not available in the Web UI.

To use some Fireware XTM features related to WatchGuard servers, you must install WatchGuard Server Center. You do not have to use WatchGuard System Manager to install WatchGuard Server Center. You can use WatchGuard Server Center to configure these WatchGuard servers:

- Management Server
- Log Server
- Report Server
- Quarantine Server
- WebBlocker Server

To learn how to configure features not supported by the Web UI or how to use WatchGuard Server Center, see the *Fireware XTM WatchGuard System Manager v11 Help* at http://www.watchguard.com/help/docs/wsm/11/en-US/index.html.

To learn more about the CLI, see the *WatchGuard Command Line Interface Reference* at http://www.watchguard.com/help/documentation.

Complete Your Installation

After you are finished with the Web Setup Wizard , you must complete the installation of your XTM device on your network.

1. Put the XTM device in its permanent physical location.
2. Make sure the gateway of management computer and the rest of the trusted network is the IP address of the trusted interface of your XTM device.
3. To connect to your XTM device with Fireware XTM Web UI, open a web browser and type: `https://10.0.1.1:8080`. This is the default IP address of the trusted interface.

   For more information, see *Connect to Fireware XTM Web UI* on page 26.
4. If you use a routed configuration, make sure you change the default gateway on all the computers that connect to your XTM device to match the IP address of the XTM device trusted interface.
5. Customize your configuration as necessary for the security purposes of your business.

   For more information, see the subsequent *Customize your security policy* section.

Customize Your Security Policy

Your security policy controls who can get into and out of your network, and where they can go in your network. The configuration file of your XTM device manages the security policies.

When you completed the Quick Setup Wizard, the configuration file that you made was only a basic configuration. You can modify this configuration to align your security policy with the business and security requirements of your company. You can add packet filter and proxy policies to set what you let in and out of your network. Each policy can have an effect on your network. The policies that increase your network security can decrease access to your network. And the policies that increase access to your network can put the security of your network at risk. For more information on policies, see *About Policies* on page 287.

For a new installation, we recommend that you use only packet filter policies until all your systems operate correctly. As necessary, you can add proxy policies.

About LiveSecurity Service

Your XTM device includes a subscription to LiveSecurity Service. Your subscription:

- Makes sure that you get the newest network protection with the newest software upgrades
- Gives solutions to your problems with full technical support resources
- Prevents service interruptions with messages and configuration help for the newest security problems
- Helps you to find out more about network security through training resources
- Extends your network security with software and other features
- Extends your hardware warranty with advanced replacement

For more information about LiveSecurity Service, see *About WatchGuard Support* on page 17.

Additional Installation Topics

Connect to an XTM Device with Firefox v3

Web browsers use certificates to ensure that the device on the other side of an HTTPS connection is the device you expect. Users see a warning when a certificate is self-signed, or when there is a mismatch between the requested IP address or host name and the IP address or host name in the certificate. By default, your XTM device uses a self-signed certificate that you can use to set up your network quickly. However, when users connect to the XTM device with a web browser, a *Secure Connection Failed* warning message appears.

To avoid this warning message, we recommend that you add a valid certificate signed by a CA (Certificate Authority) to your configuration. This CA certificate can also be used to improve the security of VPN authentication. For more information on the use of certificates with XTM devices, see *About Certificates* on page 491.

If you continue to use the default self-signed certificate, you can add an exception for the XTM device on each client computer. Current versions of most Web browsers provide a link in the warning message that the user can click to allow the connection. If your organization uses Mozilla Firefox v3, your users must add a permanent certificate exception before they can connect to the XTM device.

Actions that require an exception include:

- *About User Authentication*
- *Install and Connect the Mobile VPN with SSL Client*
- *Run the Web Setup Wizard*
- *Connect to Fireware XTM Web UI*

Common URLs that require an exception include:

```
https://IP address or host name of an XTM device interface:8080
    https://IP address or host name of an XTM device interface:4100
    https://IP address or host name of an XTM device:4100/sslvpn.html
```

Add a Certificate Exception to Mozilla Firefox v3

If you add an exception in Firefox v3 for the XTM device certificate, the warning message does not appear on subsequent connections. You must add a separate exception for each IP address, host name, and port used to connect to the XTM device. For example, an exception that uses a host name does not operate properly if you connect with an IP address. Similarly, an exception that specifies port 4100 does not apply to a connection where no port is specified.

> ***Note*** *A certificate exception does not make your computer less secure. All network traffic between your computer and the XTM device remains securely encrypted with SSL.*

There are two methods to add an exception. You must be able to send traffic to the XTM device to add an exception.

- Click the link in the **Secure Connection Failed** warning message.
- Use the Firefox v3 Certificate Manager to add exceptions.

In the *Secure Connection Failed* warning message:

1. Click **Or you can add an exception**.
2. Click **Add Exception**.
   The Add Security Exception dialog box appears.
3. Click **Get Certificate**.
4. Select the **Permanently store this exception** check box.
5. Click **Confirm Security Exception**.

To add multiple exceptions:

1. In Firefox, select **Tools > Options**.
   The Options dialog box appears.
2. Select **Advanced**.
3. Click the **Encryption** tab, then click **View Certificates**.
   The Certificate Manager dialog box opens.
4. Click the **Servers** tab, then click **Add Exception**.
5. In the **Location** text box, type the URL to connect to the XTM device. The most common URLs are listed above.
6. When the certificate information appears in the **Certificate Status** area, click **Confirm Security Exception**.
7. Click **OK**.
8. To add more exceptions, repeat Steps 4–6.

Identify Your Network Settings

To configure your XTM device, you must know some information about your network. You can use this section to learn how to identify your network settings.

For an overview of network basics, see *About Networks and Network Security* on page 1.

Network Addressing Requirements

Before you can begin installation, you must know how your computer gets an IP address. Your Internet Service Provider (ISP) or corporate network administrator can give you this information. Use the same method to connect the XTM device to the Internet that you use for your computer. For example, if you connect your computer directly to the Internet with a broadband connection, you can put the XTM device between your computer and the Internet and use the network configuration from your computer to configure the XTM device external interface.

You can use a static IP address, DHCP, or PPPoE to configure the XTM device external interface. For more information about network addressing, see *Configure an External Interface* on page 84.

Your computer must have a web browser. You use the web browser to configure and manage the XTM device. Your computer must have an IP address on the same network as the XTM device.

In the factory default configuration, the XTM device assigns your computer an IP address with DHCP (Dynamic Host Configuration Protocol). You can set your computer to use DHCP and then you can connect to the device to manage it. You can also give your computer a static IP address that is on the same network as the trusted IP address of the XTM device. For more information, see *Set Your Computer to Connect to Your XTM Device* on page 35.

Find Your TCP/IP Properties

To learn about the properties of your network, look at the TCP/IP properties of your computer or any other computer on the network. You must have this information to install your XTM device:

- IP address
- Subnet mask
- Default gateway
- Whether your computer has a static or dynamic IP address
- IP addresses of primary and secondary DNS servers

> ***Note*** *If your ISP assigns your computer an IP address that starts with 10, 192.168, or 172.16 to 172.31, then your ISP uses NAT (Network Address Translation) and your IP address is private. We recommend that you get a public IP address for your XTM device external IP address. If you use a private IP address, you can have problems with some features, such as virtual private networking.*

To find the TCP/IP properties for your computer operating system, use the instructions in the subsequent sections .

Find Your TCP/IP Properties on Microsoft Windows Vista

1. Select **Start > Programs > Accessories > Command Prompt**.
   The Command Prompt dialog box appears.
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Write down the values that you see for the primary network adapter.

Find Your TCP/IP Properties on Microsoft Windows 2000, Windows 2003, and Windows XP

1. Select **Start > All Programs > Accessories > Command Prompt**.
   The Command Prompt dialog box appears.
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Write down the values that you see for the primary network adapter.

Find Your TCP/IP Properties on Microsoft Windows NT

1. Select **Start > Programs > Command Prompt**.
   The Command Prompt dialog box appears.
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Write down the values that you see for the primary network adapter.

Find Your TCP/IP Properties on Macintosh OS 9

1. Select the **Apple menu > Control Panels > TCP/IP**.
   The TCP/IP dialog box appears.
2. Write down the values that you see for the primary network adapter.

Find Your TCP/IP Properties on Macintosh OS X 10.5

1. Select the **Apple** menu > **System Preferences**, or select the icon from the Dock.
   The System Preferences dialog box appears.
2. Click the **Network** icon.
   The Network preference pane appears.
3. Select the network adapter you use to connect to the Internet.
4. Write down the values that you see for the network adapter.

Find Your TCP/IP Properties on Other Operating Systems (Unix, Linux)

1. Read your operating system guide to find the TCP/IP settings.
2. Write down the values that you see for the primary network adapter.

Find PPPoE Settings

Many ISPs use Point to Point Protocol over Ethernet (PPPoE) because it is easy to use with a dial-up infrastructure. If your ISP uses PPPoE to assign IP addresses, you must get this information:

- Login name
- Domain (optional)
- Password

Set Your Computer to Connect to Your XTM Device

Before you can use the Web Setup Wizard, you must configure your computer to connect to your XTM device. You can set your network interface card to use a static IP address, or use DHCP to get an IP address automatically.

Use DHCP

If your computer does not use the Windows XP operating system, read the operating system help for instructions on how to set your computer to use DHCP.

To configure a computer with Windows XP to use DHCP:

1. Select **Start > Control Panel**.
   The Control Panel window appears.
2. Double-click **Network Connections**.
3. Double-click **Local Area Connection**.
   The Local Area Connection Status window appears.
4. Click **Properties**.
   The Local Area Connection Properties window appears.
5. Double-click **Internet Protocol (TCP/IP)**.
   The Internet Protocol (TCP/IP) Properties dialog box appears.
6. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
7. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.
8. Click **OK** to close the **Local Area Network Connection Properties** dialog box.
9. Close the **Local Area Connection Status**, **Network Connections**, and **Control Panel** windows.
   Your computer is ready to connect to the XTM device.
10. When the XTM device is ready, open a web browser.
11. In the browser address bar, type the IP address of your XTM device and press **Enter**.
12. If a security certificate warning appears, accept the certificate.
    The Quick Setup Wizard starts.

    Note *The default IP address for a WatchGuard XTM device is* `https://10.0.1.1/`.

13. *Run the Web Setup Wizard*.

Use a Static IP Address

If your computer does not use the Windows XP operating system, read the operating system help for instructions on how to set your computer to use a static IP address. You must select an IP address on the same subnet as the trusted network.

To configure a computer with Windows XP to use a static IP address:

1. Select **Start > Control Panel**.
   The Control Panel window appears.
2. Double-click **Network Connections**.
3. Double-click **Local Area Connection**.
   The Local Area Connection Status window appears.
4. Click **Properties**.
   The Local Area Connection Properties window appears.

5. Double-click **Internet Protocol (TCP/IP)**.
   The Internet Protocol (TCP/IP) Properties dialog box appears.
6. Select **Use the following IP address**.
7. In the **IP address** field, type an IP address on the same network as the XTM device trusted interface. For example, you can set the IP address on your computer to `10.0.1.2`.
   The default IP address for the XTM device trusted interface is 10.0.1.1.
8. In the **Subnet Mask** field, type `255.255.255.0`.
9. In the **Default Gateway** field, type the IP address of the XTM device trusted interface, `10.0.1.1`.
10. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.
11. Click **OK** to close the **Local Area Network Connection Properties** dialog box.
12. Close the **Local Area Connection Status**, **Network Connections**, and **Control Panel** windows.
    Your computer is ready to connect to the XTM device.
13. When the XTM device is ready, open a web browser.
14. In the browser address bar, type the IP address of your XTM device and press **Enter**.

    Note *The default IP address for a WatchGuard XTM device is `https://10.0.1.1/`.*

15. If a security certificate warning appears, accept the certificate.
    The Quick Setup Wizard starts.
16. *Run the Web Setup Wizard*.

Disable the HTTP Proxy in the Browser

Many web browsers are configured to use an HTTP proxy server to increase the download speed of web pages. To manage or configure the XTM device with the Web UI, your browser must connect directly to the device. If you use an HTTP proxy server, you must temporarily disable the HTTP proxy setting in your browser. You can enable the HTTP proxy server setting in your browser again after you set up the XTM device.

Use these instructions to disable the HTTP proxy in Firefox, Safari, or Internet Explorer. For other browsers, use the browser Help system to find the necessary information. Many browsers automatically disable the HTTP proxy feature.

Disable the HTTP proxy in Internet Explorer 6.x, 7.x, or 8.x

1. Open Internet Explorer.
2. Select **Tools > Internet Options**.
   The Internet Options dialog box appears.
3. Select the **Connections** tab.
4. Click **LAN Settings**.
   The Local Area Network (LAN) Settings dialog box appears.
5. Clear the **Use a proxy server for your LAN** check box.
6. Click **OK** to close the **Local Area Network (LAN) Settings** dialog box.
7. Click **OK** to close the **Internet Options** dialog box.

Disable the HTTP proxy in Firefox 2.x or 3.x

1. Open Firefox.
2. Select **Tools > Options**.
   The Options dialog box appears.

3. Click **Advanced**.
4. Select the **Network** tab.
5. Click **Settings**.
6. Click **Connection Settings**.
   The Connection Settings dialog box appears.
7. For Firefox 2.x, make sure the **Direct Connection to the Internet** option is selected.
   For Firefox 3.x, make sure the **No proxy** option is selected.
8. Click **OK** to close the **Connection Settings** dialog box.
9. Click **OK** to close the **Options** dialog box.

Disable the HTTP proxy in Safari 2.0

1. Open Safari.
2. Select **Preferences**.
   The Safari preferences dialog ox appears.
3. Click **Advanced**.
4. Click **Change Settings**.
   The System Preference dialog box appears.
5. Clear the **Web Proxy (HTTP)** check box.
6. Click **Apply Now**.

5 Configuration and Management Basics

About Basic Configuration and Management Tasks

After your XTM device is installed on your network and is set up with a basic configuration file, you can start to add custom configuration settings. The topics in this section help you complete these basic management and maintenance tasks.

Make a Backup of the XTM Device Image

An XTM device backup image is an encrypted and saved copy of the flash disk image from the XTM device flash disk. It includes the XTM device OS, configuration file, licenses, and certificates. You can save a backup image to your computer or to a directory on your network.

We recommend that you regularly make backup files of the XTM device image. We also recommend that you create a backup image of the XTM device before you make significant changes to your configuration file, or before you upgrade your XTM device or its OS. You can use Fireware XTM Web UI to make a backup of your device image.

1. Select **System > Backup Image**.
2. Type and confirm an encryption key. This key is used to encrypt the backup file. If you lose or forget this encryption key, you cannot restore the backup file.
3. Click **Backup**.
4. Select a location to save the backup image file and type a filename.
   The backup image is saved to the location you specify.

Restore an XTM Device Backup Image

You can use Fireware XTM Web UI to restore a previously created backup image to your XTM device. If your device is centrally managed, you must open Policy Manager for your device from your Management Server to restore a backup image to your device.

For more information about Centralized Management and how to update a Fully Managed device, see *Fireware XTM WatchGuard System Manager Help*.

1. Select **System > Restore Image**.
2. Click **Restore Image**.
3. Click **Browse**.
4. Select the saved backup image file. Click **Open**.
5. Click **Restore**.
6. Type the encryption key you used when you created the backup image.
   The XTM device restores the backup image. It restarts and uses the backup image.

   Wait for two minutes before you connect to the XTM device again.

If you cannot successfully restore your XTM device image, you can reset the XTM device. Depending on the XTM device model you have, you can reset a XTM device to its factory-default settings or rerun the Quick Setup Wizard to create a new configuration.

For more information, see *Reset an XTM Device to a Previous or New Configuration* on page 47.

Use a USB Drive for System Backup and Restore

A WatchGuard XTM device backup image is a copy of the flash disk image from the XTM device that is encrypted and saved. The backup image file includes the XTM device OS, configuration file, feature key, and certificates.

For XTM 2 Series, 5 Series, 8 Series, or XTM 1050 devices, you can attach a USB drive or storage device to the USB port on the XTM device for system backup and restore procedures. When you save a system backup image to a connected USB drive, you can restore your XTM device to a known state more quickly.

About the USB Drive

The USB drive must be formatted with the FAT or FAT32 file system. If the USB drive has more than one partition, Fireware XTM only uses the first partition. Each system backup image can be as large as 30 MB. We recommend you use a USB drive large enough to store several backup images.

Save a Backup Image to a Connected USB Drive

For this procedure, a USB drive must be connected to your XTM device.

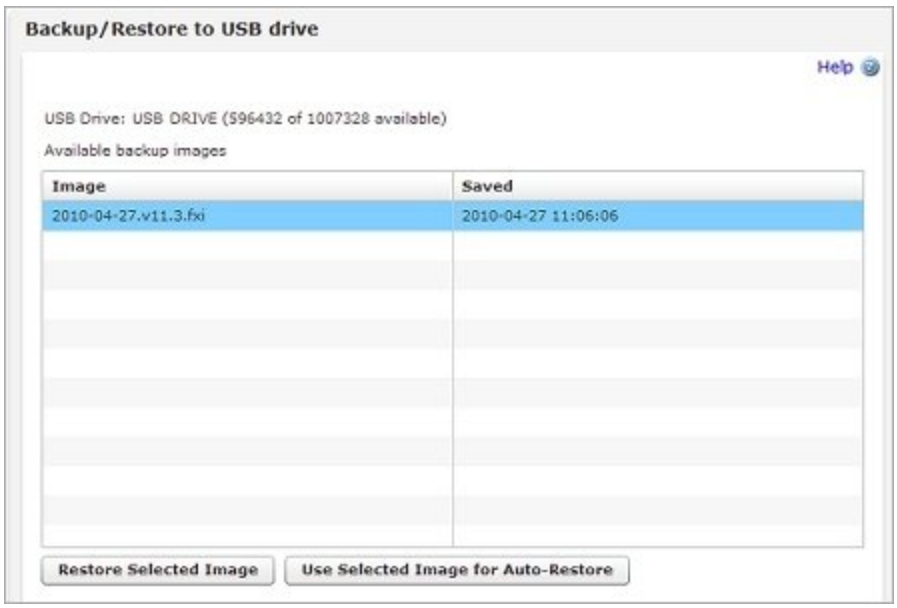
1. Select **System > USB Drive**.
   The Backup/Restore to USB drive page appears.

2. In the **New backup image** section, type a **Filename** for the backup image.
3. Type and confirm an **Encryption key**. This key is used to encrypt the backup file. If you lose or forget this encryption key, you cannot restore the backup file.
4. Click **Save to USB Drive**.
   *The saved image appears on the list of **Available device backup images** after the save is complete.*

Restore a Backup Image from a Connected USB Drive

For this procedure, a USB drive must be connected to your XTM device.

1. Select **System > USB Drive**.
   The Backup/Restore to USB Drive page appears.



2. From the **Available backup images** list, select a backup image file to restore.
3. Click **Restore Selected Image**.
4. Type the **Encryption key** you used when you created the backup image.
5. Click **Restore**.
   The XTM device restores the backup image. It restarts and uses the backup image.

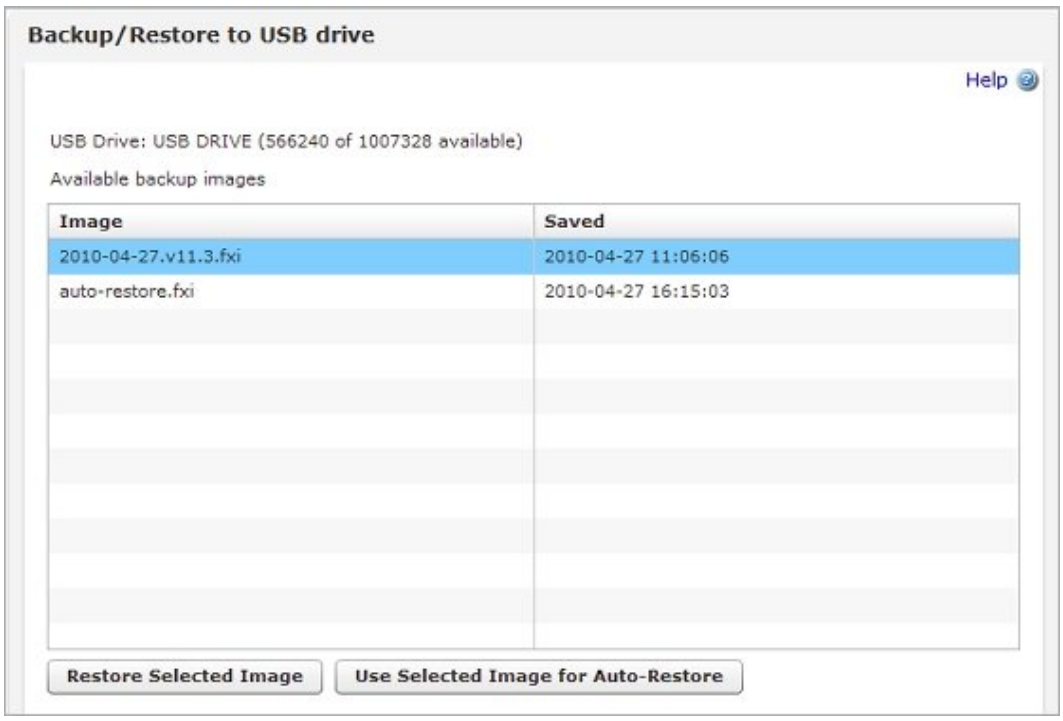
Automatically Restore a Backup Image from a USB Drive

If a USB drive (storage device) is connected to a WatchGuard XTM device in recovery mode, the device can automatically restore the previously backed up image from the USB drive. To use the auto-restore feature, you must first select a backup image on the USB drive as the one you want to use for the restore process. You must use Fireware XTM Web UI, Firebox System Manager, or Fireware XTM command line interface to select this backup image.

You can use the same backup image for more than one device in the same WatchGuard XTM model family. For example, you can use a backup image saved from an XTM 530 as the backup image for any other XTM 5 Series device.

Select the Backup Image to Auto-restore

1. Select **System > USB Drive**.
   The Backup/Restore to USB Drive page appears. The saved backup image files appear in a list at the top of the page.



2. From the **Available backup images** list, select a backup image file.
3. Click **Use Selected Image for Auto-Restore**.
4. Type the **Encryption key** used to create the backup image. Click **OK**.
   The XTM device saves a copy of the selected backup image on the USB drive.

If you had a previous auto-restore image saved, the auto-restore.fxi file is replaced with a copy of the backup image you selected.

> ***Warning*** *If your XTM device has used a version of the Fireware XTM OS before v11.3, you must update the recovery mode software image on the device to v11.3 for the auto-restore feature to operate. See the Fireware XTM 11.3 Release Notes for upgrade instructions.*

Restore the Backup Image for an XTM 5 Series, 8 Series, or XTM 1050 Device

1. Connect the USB drive with the auto-restore image to a USB port on the XTM device.
2. Power off the XTM device.
3. Press the up arrow on the device front panel while you power on the device.
4. Keep the button depressed until `Recovery Mode starting` appears on the LCD display.
   The device restores the backup image from the USB drive, and automatically uses the restored image after it reboots.

If the USB drive does not contain a valid auto-restore image for this XTM device model family, the device does not reboot and is instead started in recovery mode. If you restart the device again, it uses your current configuration. When the device is in recovery mode, you can use the WSM Quick Setup Wizard to create a new basic configuration.

For information about the WSM Quick Setup Wizard, see Run the WSM Quick Setup Wizard.

Restore the Backup Image for an XTM 2 Series Device

1. Attach the USB drive with the auto-restore image to a USB port on the XTM 2 Series device.
2. Disconnect the power supply.
3. Press and hold the **Reset** button on the back of the device.
4. Connect the power supply while you continue to hold down the **Reset** button.
5. After 10 seconds, release the **Reset** button.
   The device restores the backup image from the USB drive, and automatically uses the restored image after it reboots.

If the USB drive does not contain a valid 2 Series auto-restore image, the auto-restore fails and the device does not reboot. If the auto-restore process is not successful, you must disconnect and reconnect the power supply to start the 2 Series device with factory-default settings.

For information about factory default settings, see *About Factory-Default Settings*.

USB Drive Directory Structure

The USB drive contains directories for backup images, configuration files, feature key, certificates and diagnostics information for your XTM device.

When you save a backup image to a USB drive, the file is saved in a directory on the USB drive with the same name as the serial number of your XTM device. This means that you can store backup images for more than one XTM device on the same USB drive. When you restore a backup image, the software automatically retrieves the list of backup images stored in the directory associated with that device.

For each device, the directory structure on the USB device is as follows, where `sn` is replaced by the serial number of the XTM device:

```
\sn\flash-images\
\sn\configs\
\sn\feature-keys\
\sn\certs\
```

The backup images for a device is saved in the `\sn\flash-images` directory. The backup image file saved in the flash-images directory contains the Fireware XTM OS, the device configuration, feature keys, and certificates. The `\configs`, `\feature-keys` and `\certs` subdirectories are not used for any USB drive backup and restore operations. You can use these to store additional feature keys, configuration files, and certificates for each device.

There is also one directory at the root level of the directory structure which is used to store the designated auto-restore backup image.

```
\auto-restore\
```

When you designate a backup image to use for automatic restore, a copy of the selected backup image file is encrypted and stored in the `\auto-restore` directory with the file name `auto-restore.fxi`. You can have only one auto-restore image saved on each USB drive. You can use the same auto-restore backup image for more than one device, if both devices are the same WatchGuard XTM model family. For example, you can use an auto-restore image saved from an XTM 530 as the auto-restore image for any other XTM 5 Series device.

You must use the **System > USB Drive** command to create an auto-restore image. If you manually copy and rename a backup image and store it in this directory, the automatic restore process does not operate correctly.

There is also another directory at the root level of the directory structure which is used to store the support snapshot that can be used by WatchGuard technical support to help diagnose issues with your XTM device.

```
\wgdiag\
```

For more information about the support snapshot, see Use a USB Drive to Save a Support Snapshot.

Save a Backup Image to a USB Drive Connected to Your Computer

You can use Fireware XTM Web UI to save a backup image to a USB drive or storage device connected to your computer. If you save the configuration files for multiple devices to the same USB drive, you can attach the USB drive to any of those XTM devices for recovery.

If you use the **System > USB Drive** command to do this, the files are automatically saved in the proper directory on the USB drive. If you use the **System > Backup Image** command, or if you use Windows or another operating system to manually copy configuration files to the USB device, you must manually create the correct serial number and flash-image directories for each device (if they do not already exist).

Before You Begin

Before you begin, it important that you understand the *USB Drive Directory Structure* used by the USB backup and restore feature. If you do not save the backup image in the correct location, the device cannot find it when you attach the USB drive to the device.

Save the Backup Image

To save a backup image to a USB drive connected to your computer, follow the steps in *Make a Backup of the XTM Device Image*. When you select the location to save the file, select the drive letter of the USB drive attached to your computer. If you want the backup image you save to be recognized by the XTM device when you attach the USB drive, make sure to save the backup in the `\flash-images` folder, in the directory that is named with the serial number of your XTM device.

For example, if your XTM device serial number is `70A10003C0A3D`, save the backup image file to this location on the USB drive:

```
\70A10003C0A3D\flash-images\
```

Designate a Backup Image for Auto-restore

To designate a backup image for use with the auto-restore feature, you must connect the USB drive to the device and designate the backup image to use for auto-restore, as described in *Use a USB Drive for System Backup and Restore*. If you manually save a backup image to the auto-restore directory, the automatic restore process does not operate correctly.

Reset an XTM Device to a Previous or New Configuration

If your XTM device has a severe configuration problem, you can reset the device to its factory-default settings. For example, if you do not know the configuration passphrase or if a power interruption causes damage to the Fireware XTM OS, you can use the Quick Setup Wizard to build your configuration again or restore a saved configuration.

For a description of the factory-default settings, see *About Factory-Default Settings* on page 48.

> ***Note*** *You can also use safe mode to automatically restore a system backup image from a USB storage device. For more information, see Automatically Restore a Backup Image from a USB Drive.*

Start an XTM Device in Safe Mode

To restore the factory-default settings for a WatchGuard XTM 5 Series, 8 Series, or 10 Series device, you must start the XTM device in safe mode.

1. Power off the XTM device.
2. Press the down arrow on the device front panel while you power on the XTM device.
3. Keep the down arrow button depressed until the message `Safe Mode Starting` appears on the LCD display:

   When the device is started in safe mode, the display shows the model number followed by the word "safe".

When you start a device in safe mode:

- The device temporarily uses the factory-default network and security settings.
- The current feature key is not removed. If you run the Quick Setup Wizard to create a new configuration, the wizard uses the feature key you previously imported.
- Your current configuration is deleted only when you save a new configuration. If you restart the XTM device before you save a new configuration, the device uses your current configuration again.

Reset an XTM 2 Series Device to Factory-Default Settings

When you reset an XTM 2 Series device, the original configuration settings are replaced by the factory-default settings. To reset the device to factory-default settings:

1. Disconnect the power supply.
2. Press and hold the **Reset** button on the back of the device.
3. While you continue to hold down the **Reset** button, connect the power supply.
4. Continue to hold down the **Reset** button until the yellow **Attn** indicator stays lit. This shows that the device successfully restored the factory-default settings.
   For a 2 Series device, this process can take 75 seconds or more.
5. Release the **Reset** button.

> ***Note*** *You must start the device again before you can connect to it. If you do not restart, when you try to connect to the device, a web page appears with this message: Your device is running from a backup copy of firmware. You can also see this message if the* ***Reset*** *button is stuck in the depressed position. If you continue to see this message, check the* ***Reset*** *button and restart the device.*

6. Disconnect the power supply.
7. Connect the power supply again.
   The Power Indicator lights and your device is reset.

Run the Quick Setup Wizard

After you restore the factory-default settings, you can use the Quick Setup Wizard to create a basic configuration or restore a saved backup image.

For more information, see *About the Quick Setup Wizard* on page 22.

About Factory-Default Settings

The term *factory-default settings* refers to the configuration on the XTM device when you first receive it before you make any changes. You can also reset the XTM device to factory-default settings as described in *Reset an XTM Device to a Previous or New Configuration* on page 47.

The default network and configuration properties for the XTM device are:

Trusted network

The default IP address for the trusted network is 10.0.1.1. The subnet mask for the trusted network is 255.255.255.0.

The default IP address and port for the Fireware XTM Web UI is `https://10.0.1.1:8080`.

The XTM device is configured to give IP addresses to computers on the trusted network through DHCP. By default, these IP addresses can be from 10.0.1.2 to 10.0.1.254.

External network

The XTM device is configured to get an IP address with DHCP.

Optional network

The optional network is disabled.

Administrator (read/write) account credentials

Username: `admin`

Passphrase: `readwrite`

Status (read-only) account credentials

Username: `status`

Passphrase: `readonly`

Firewall settings

All incoming traffic is denied. The outgoing policy allows all outgoing traffic. Ping requests received from the external network are denied.

System Security

The XTM device has the built-in administrator accounts *admin* (read-write access) and *status* (read-only access). When you first configure the device with the Quick Setup Wizard, you set the status and configuration passphrases. After you complete the Quick Setup Wizard, you can log in to Fireware XTM Web UI with the either the admin or status administrator accounts. For full administrator access, log in with the *admin* user name and type the configuration passphrase. For read-only access, log in with the *status* user name and type the read-only passphrase.

By default, the XTM device is set up for local management from the trusted network only. Additional configuration changes must be made to allow administration from the external network.

Upgrade Options

To enable upgrade options such as WebBlocker, spamBlocker, and Gateway AV/IPS, you must paste or import the feature key that enables these features into the configuration page or use the **Get Feature Key** command to activate upgrade options. If you start the XTM device in safe mode, you do not need to import the feature key again.

About Feature Keys

A feature key is a license that enables you to use a set of features on your XTM device. You increase the functionality of your device when you purchase an option or upgrade and get a new feature key.

When You Purchase a New Feature

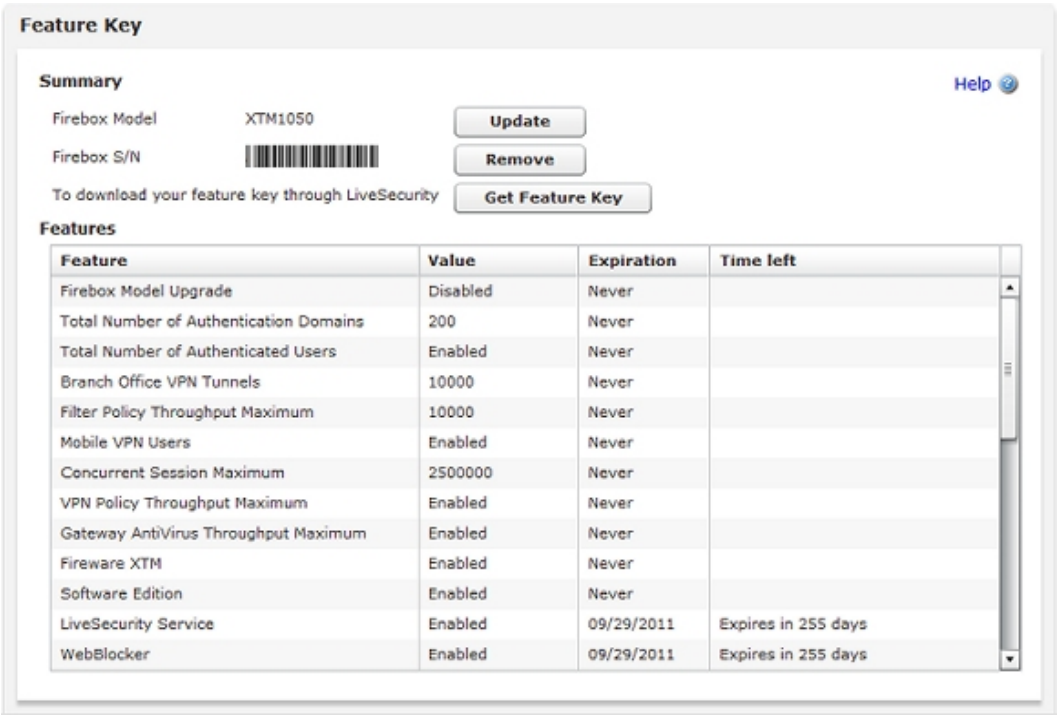
When you purchase a new feature for your XTM device, you must:

- *Get a Feature Key from LiveSecurity*
- *Add a Feature Key to Your XTM Device*

See Features Available with the Current Feature Key

Your XTM device always has one currently active feature key. To see the features available with this feature key:

1. *Connect to Fireware XTM Web UI.*
2. Select **System > Feature Key**.
   The Feature Key page appears.



The **Features** section includes:

- A list of available features
- Whether the feature is enabled or disabled
- Value assigned to the feature such as the number of VLAN interfaces allowed
- Expiration date of the feature
- Current status on expiration, such as how many days remain before the feature expires

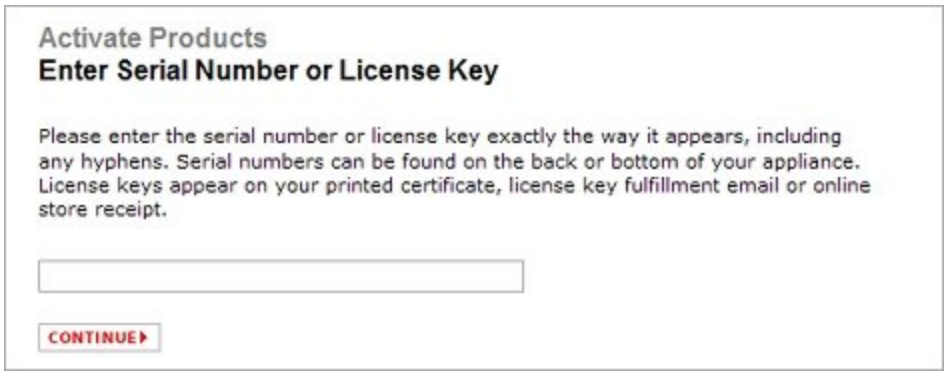
Get a Feature Key from LiveSecurity

Before you activate a new feature, or renew a subscription service, you must have a license key certificate from WatchGuard that is not already registered on the LiveSecurity web site. When you activate the license key, you can get the feature key that enables the activated feature on the XTM device. You can also retrieve an existing feature key at a later time.

Activate the License Key for a Feature

To activate a license key and get the feature key for the activated feature:

1. Open a web browser and go to https://www.watchguard.com/activate.
   If you have not already logged in to LiveSecurity, the LiveSecurity Log In page appears.
2. Type your LiveSecurity user name and password.
   The Activate Products page appears.
3. Type the serial number or license key for the product as it appears on your printed certificate. Make sure to include any hyphens.
   Use the serial number to register a new XTM device, and the license key to register add-on features.



4. Click **Continue**.
   The Choose Product to Upgrade page appears.
5. In the drop-down list, select the device to upgrade or renew.
   If you added a device name when you registered your XTM device, that name appears in the list.
6. Click **Activate**.
   The Retrieve Feature Key page appears.
7. Copy the full feature key to a text file and save it on your computer.
8. Click **Finish**.

Get a Current Feature Key

You can log in to the LiveSecurity web site to get a current feature key, or you can use Fireware XTM Web UIto retrieve the current feature key and add it directly to your XTM device.

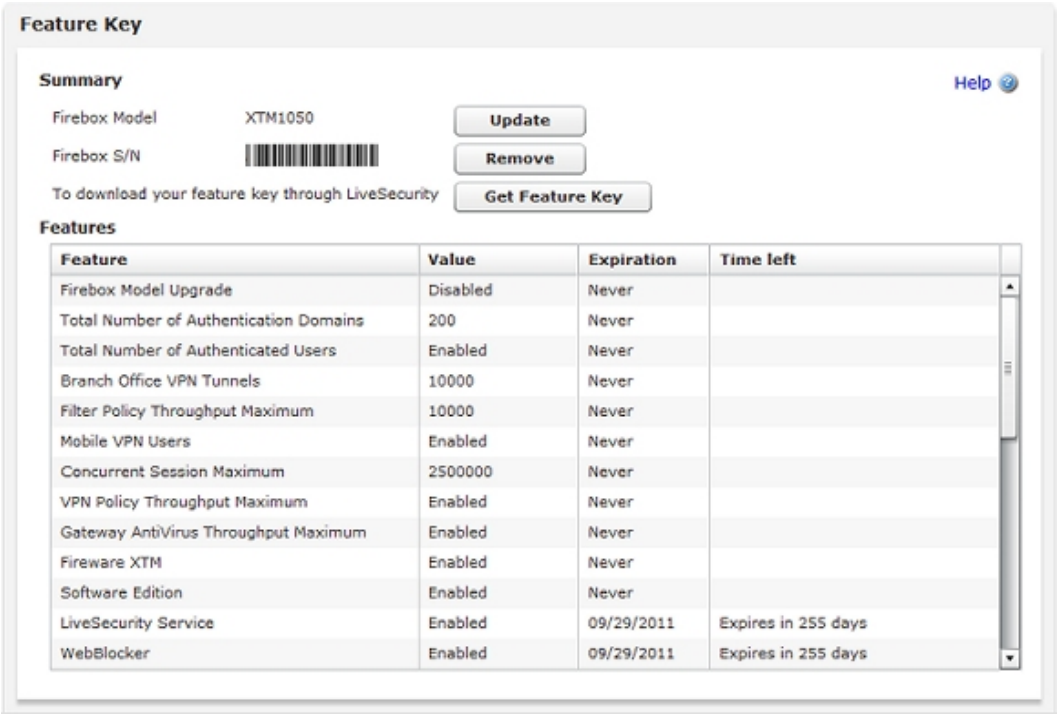
When you go to the LiveSecurity web site to retrieve your feature key, you can choose to download one or more feature keys in a compressed file. If you select multiple devices, the compressed file contains one feature key file for each device.

To retrieve a current feature key from the LiveSecurity web site:

1. Open a web browser and go to https://www.watchguard.com/archive/manageproducts.asp.
   If you have not already logged in to LiveSecurity, the LiveSecurity Log In page appears.
2. Type your LiveSecurity user name and password.
   The Manage Products page appears.
3. Select **Feature Keys**.
   The Retrieve Feature Key page appears, with a drop-down list to select a product.
4. In the drop-down list, select your XTM device.
5. Click **Get Key**.
   A list of all your registered devices appears. A check mark appears next to the device you selected.
6. Select **Show feature keys on screen**.
7. Click **Get Key**.
   The Retrieve Feature Key page appears.
8. Copy the feature key to a text file and save it on your computer.

To use Fireware XTM Web UI to retrieve the current feature key:

1. *Connect to Fireware XTM Web UI*.
   The Fireware XTM Web UI Dashboard appears.
2. Select **System > Feature Key**.
   The Feature Key Summary page appears.



3. Click **Get Feature Key**.
   Your feature key is downloaded from LiveSecurity and automatically updated on your XTM device.

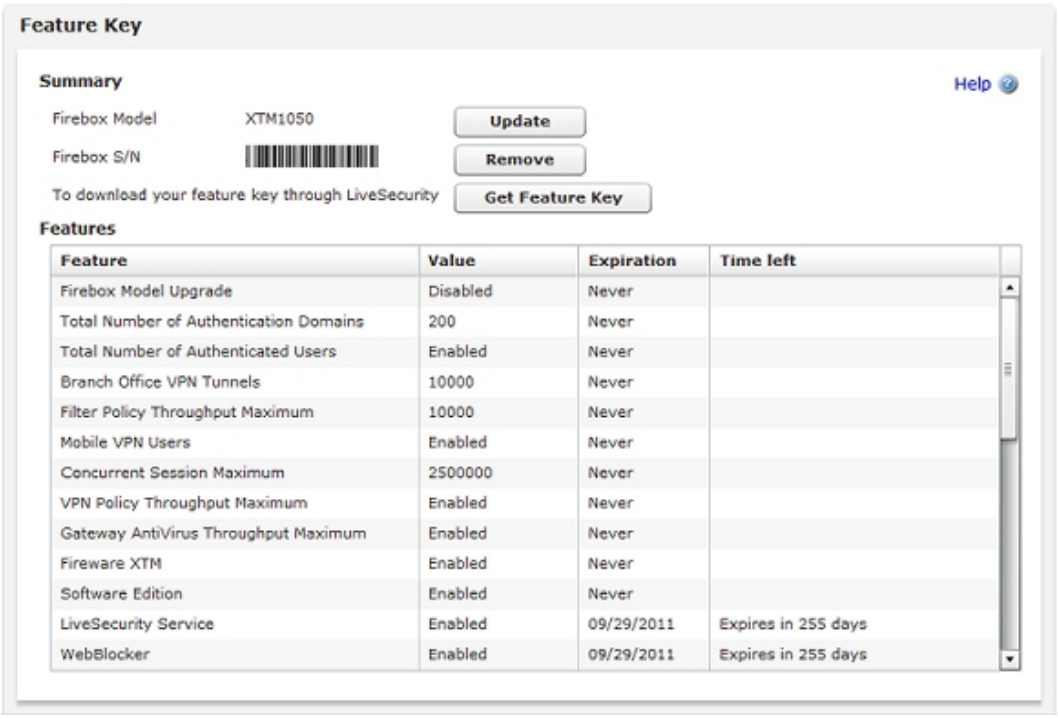
Add a Feature Key to Your XTM Device

If you purchase a new option or upgrade your XTM device, you can use Fireware XTM Web UI to add a new feature key to enable the new features. Before you install the new feature key, you must completely remove the old feature key.

1. Select **System > Feature Keys**.
   The Firebox Feature Key page appears.

   The features that are available with this feature key appear on this page. This page also includes:

   - Whether each feature is enabled or disabled
   - A value assigned to the feature, such as the number of VLAN interfaces allowed
   - The expiration date of the feature
   - The amount of time that remains before the feature expires



2. To remove the current feature key, click **Remove**.
   All feature key information is cleared from the page.
3. Click **Import**.Click **Update**.
   The Add Firebox Feature Key page appears.

4. Copy the text of the feature key file and paste it in the text box.
5. Click **Save**.
   The Feature Key page reappears with the new feature key information.

Remove a Feature Key

1. Select **System > Feature Keys**.
   The Firebox Feature Key page appears.
2. Click **Remove**.
   All feature key information is cleared from the page.
3. Click **Save**.

Restart Your XTM Device

You can use Fireware XTM Web UI to restart your XTM device from a computer on the trusted network. If you enable external access, you can also restart the XTM device from a computer on the Internet. You can set the time of day at which your XTM device reboots automatically.

Restart the XTM Device Locally

To restart the XTM device locally, you can use Fireware XTM Web UI or you can power cycle the device.

Reboot from Fireware XTM Web UI

To reboot the XTM device from Fireware XTM Web UI, you must log in with read-write access.

1. Select **Dashboard > System**.
2. In the **Device Information** section, click **Reboot**.

Power Cycle

On the XTM 2 Series:

1. Disconnect the 2 Series device power supply.
2. Wait for a minimum of 10 seconds.
3. Connect the power supply again.

On the XTM 5 Series, 8 Series and XTM 1050:

1. Use the power switch to power off the device.
2. Wait for a minimum of 10 seconds.
3. Power on the device.

Restart the XTM Device Remotely

Before you can connect to your XTM device to manage or restart it from a remote computer external to the XTM device, you must first configure the XTM device to allow management from the external network.

For more information, see *Manage an XTM device from a Remote Location* on page 72.

To restart the XTM device remotely from Fireware XTM Web UI:

1. Select **Dashboard > System**.
2. In the **Device Information** section, click **Reboot**.

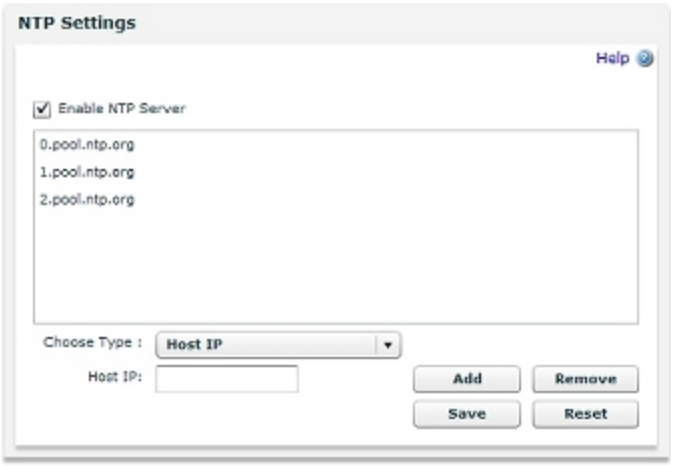
Enable NTP and Add NTP Servers

Network Time Protocol (NTP) synchronizes computer clock times across a network. Your XTM device can use NTP to get the correct time automatically from NTP servers on the Internet. Because the XTM device uses the time from its system clock for each log message it generates, the time must be set correctly. You can change the NTP server that the XTM device uses. You can also add more NTP servers or delete existing ones, or you can set the time manually.

To use NTP, your XTM device configuration must allow DNS. DNS is allowed in the default configuration by the Outgoing policy. You must also configure DNS servers for the external interface before you configure NTP.

For more information about these addresses, see Add WINS and DNS server addresses.

1. Select **System > NTP**.
   The NTP Setting dialog box appears.



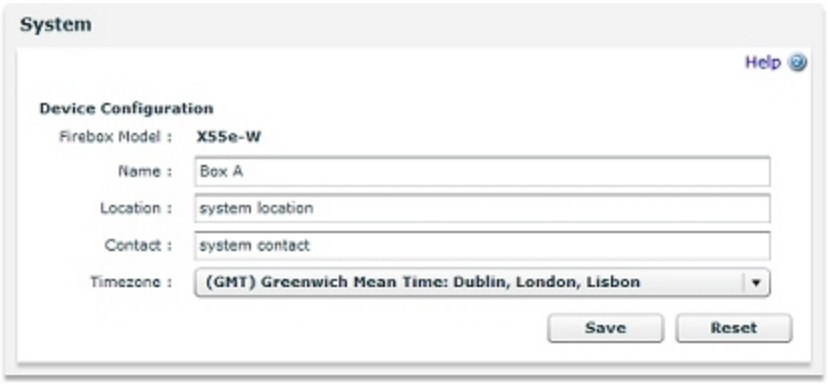
2. Select the **Enable NTP Server** check box.
3. To add an NTP server, select **Host IP** or **Host name (lookup)** in the **Choose Type** drop-down list, then type the IP address or host name of the NTP server you want to use in the adjacent text box.
   You can configure up to three NTP servers.
4. To delete a server, select the server entry and click **Remove**.
5. Click **Save**.

Set the Time Zone and Basic Device Properties

When you run the Web Setup Wizard, you set the time zone and other basic device properties.

To change the basic device properties:

1. Connect to Fireware XTM Web UI.
2. Select **System > System**.
   The Device Configuration settings appear.



3. Configure these options:

   Firebox model

   The XTM device model number, as determined by Quick Setup Wizard.If you add a new feature key to the XTM device with a model upgrade, the XTM device model in the device configuration is automatically updated.

   Name

   The friendly name of the XTM device. You can give the XTM device a friendly name that appears in your log files and reports. Otherwise, the log files and reports use the IP address of the XTM device external interface. Many customers use a Fully Qualified Domain Name as the friendly name if they register such a name with the DNS system. You must give the XTM device a friendly name if you use the Management Server to configure VPN tunnels and certificates.

   Location, Contact

   Type any information that could be helpful to identify and maintain the XTM device. These fields are filled in by the Quick Setup Wizard if you entered this information there.

   Time zone

   Select the time zone for the physical location of the XTM device. The time zone setting controls the date and time that appear in the log file and on tools such as LogViewer, WatchGuard Reports, and WebBlocker.

4. Click **Save**.

About SNMP

SNMP (Simple Network Management Protocol) is used to monitor devices on your network. SNMP uses management information bases (MIBs) to define what information and events are monitored. You must set up a separate software application, often called an event viewer or MIB browser, to collect and manage SNMP data.

There are two types of MIBs: standard and enterprise. Standard MIBs are definitions of network and hardware events used by many different devices. Enterprise MIBs are used to give information about events that are specific to a single manufacturer. Your XTM device supports eight standard MIBs: IP-MIB, IF-MIB, TCP-MIB, UDP-MIB, SNMPv2-MIB, SNMPv2-SMI, RFC1213-MIB, and RFC1155 SMI-MIB. It also supports two enterprise MIBs: WATCHGUARD-PRODUCTS-MIB and WATCHGUARD-SYSTEM-CONFIG-MIB.

SNMP Polls and Traps

You can configure your XTM device to accept SNMP polls from an SNMP server. The XTM device reports information to the SNMP server such as the traffic count from each interface, device uptime, the number of TCP packets received and sent, and when each network interface on the XTM device was last modified.

A SNMP trap is an event notification your XTM device sends to an SNMP management station. The trap identifies when a specific condition occurs, such as a value that is more than its predefined threshold. Your XTM device can send a trap for any policy in Policy Manager.

A SNMP inform request is similar to a trap, but the receiver sends a response. If your XTM device does not get a response, it sends the inform request again until the SNMP manager sends a response. A trap is sent only once, and the receiver does not send any acknowledgement when it gets the trap.

About Management Information Bases (MIBs)

Fireware XTM supports two types of Management Information Bases (MIBs).

Standard MIBs

Standard MIBs are definitions of network and hardware events used by many different devices. Your XTM device supports these eight standard MIBs:

- IP-MIB
- IF-MIB
- TCP-MIB
- UDP-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- RFC1213-MIB
- RFC1155 SMI-MIB

These MIBs include information about standard network information, such as IP addresses and network interface settings.

Enterprise MIBs

Enterprise MIBs are used to give information about events that are specific to a single manufacturer. Your XTM device supports these enterprise MIBs:

- WATCHGUARD-PRODUCTS-MIB
- WATCHGUARD-SYSTEM-CONFIG-MIB
- UCD-SNMP-MIB

These MIBs include more specific information about device hardware.

When you install the Fireware XTM OS on your management computer, MIBs are installed in this location:

Windows XP

```
C:\Documents and Settings\All Users\Shared WatchGuard\SNMP
```

Windows 7, Windows Server 2008, and Windows Vista

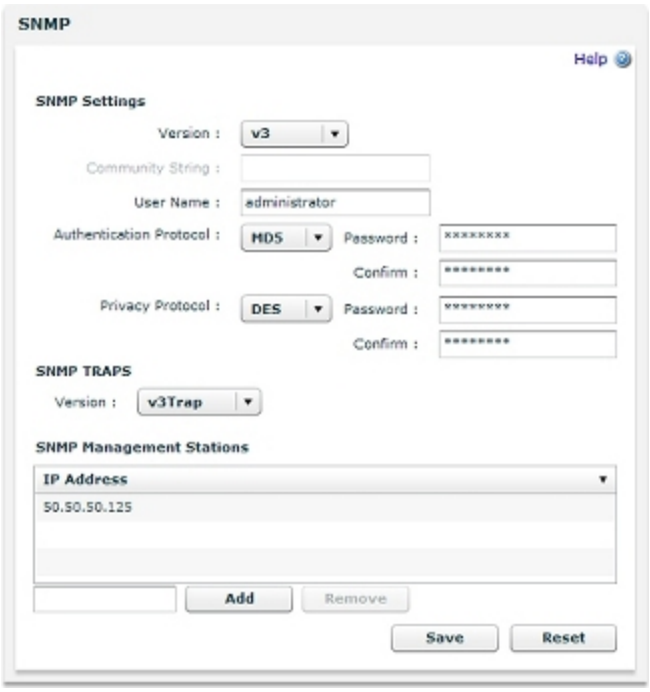
```
C:\Users\Public\Shared WatchGuard\SNMP
```

If you want to install all MIBs, you must run the Fireware XTM OS installer for all XTM models you use. You can find the Fireware XTM OS installation on the Software Downloads section of the WatchGuard web site, http://www.watchguard.com.

Enable SNMP Polling

You can configure your XTM device to accept SNMP polls from an SNMP server. Your XTM device reports information to the SNMP server such as the traffic count from each interface, device uptime, the number of TCP packets received and sent, and when each network interface was last modified.

1. Select **System > SNMP**.
   The SNMP page appears.



2. To enable SNMP, from the **Version** drop-down list, select **v1**, **v2c**, or **v3**.
3. If you selected **v1** or **v2c** for the SNMP version, type the **Community String** the SNMP server uses when it contacts the XTM device. The community string is like a user ID or password that allows access to the statistics of a device.

   If you selected **v3** for the SNMP version, type the **User name** the SNMP server uses when it contacts the XTM device.
4. If your SNMP server uses authentication, from the **Authentication Protocol** drop-down list, select **MD5** or **SHA**. In the adjacent **Password** and **Confirm** text boxes, type the authentication password.
5. If your SNMP server uses encryption, from the **Privacy Protocol** drop-down list, select **DES**. In the adjacent **Password** and **Confirm** text boxes, type the encryption password.
6. Click **Save**.

To enable your XTM device to receive SNMP polls, you must also add an SNMP packet filter policy.

1. Select **Firewall > Firewall Policies**.
2. Click .
3. Expand the **Packet Filters** list and select **SNMP**. Click **Add policy**.
   The Policy Configuration page appears.
4. In the **From** section, click **Add**.
   The Add Member dialog box appears.

5. From the **Member Type** drop-down list, select **Host IP**.
6. In the **Member Type** text box, type the IP address of your SNMP server. Click **OK**.
7. From the **From** list, select **Any-Trusted**. Click **Remove**.
8. In the **To** section, click **Add**.
   The Add Member dialog box appears.
9. From the **Select Members** list, select **Firebox**. Click **OK**.
10. From the **To** list, select **Any-External**. Click **Remove**.
11. Click **Save**.

Enable SNMP Management Stations and Traps

An SNMP trap is an event notification your XTM device sends to an SNMP management station. The trap identifies when a specific condition occurs, such as a value that is more than its predefined threshold. Your XTM device can send a trap for any policy.

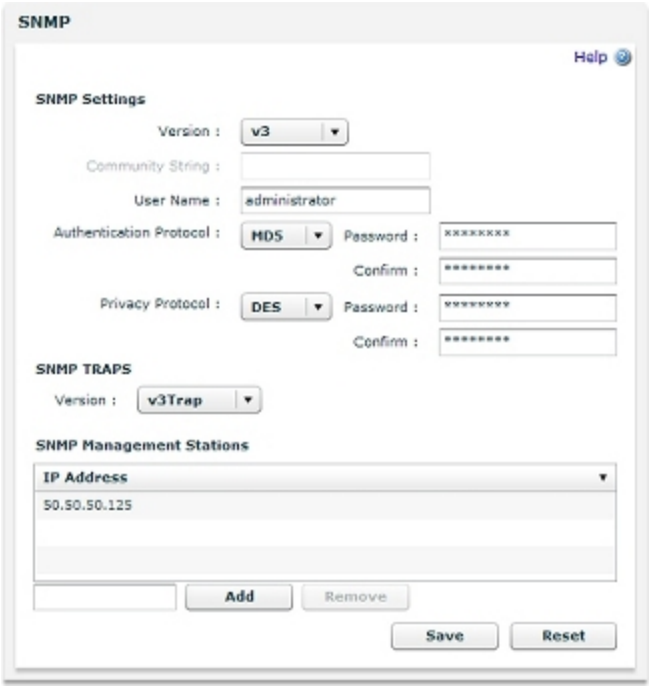
An SNMP inform request is similar to a trap, but the receiver sends a response. If your XTM device does not get a response, it sends the inform request again until the SNMP manager sends a response. A trap is sent only once, and the receiver does not send any acknowledgement when it gets the trap.

An inform request is more reliable than a trap because your XTM device knows whether the inform request was received. However, inform requests consume more resources. They are held in memory until the sender gets a response. If an inform request must be sent more than once, the retries increase traffic. We recommend you consider whether the receipt every SNMP notification is worth the use of memory in the router and increase in network traffic.

To enable SNMP inform requests, you must use SNMPv2 or SNMPv3. SNMPv1 supports only traps, not inform requests.

Configure SNMP Management Stations

1. Select **System > SNMP**.
   The SNMP page appears.



2. From the **SNMP Traps** drop-down list, select a version of trap or inform.
   SNMPv1 supports only traps, not inform requests.
3. In the **SNMP Management Stations** text box, type the IP address of your SNMP server. Click **Add**.
4. To remove a server from the list, select the entry and click **Remove**.
5. Click **Save**.

Add an SNMP Policy

To enable your XTM device to receive SNMP polls, you must also add an SNMP policy.

1. Select **Firewall > Firewall Policies**.
2. Click .
3. Expand the **Packet Filters** category and select **SNMP**. Click **Add Policy**.
   The Policy Configuration page appears.
4. In the **Name** text box, type a name for the policy.
5. Select the **Enable** check box.
6. In the **From** section, click **Add**.
   The Add Member dialog box appears.
7. From the **Member Type** drop-down list, select **Host IP**.
8. In the **Member Type** text box, type the IP address of your SNMP server. Click **OK**.
9. From the **From** list, select **Any-Trusted**. Click **Remove**.
10. In the **To** section, click **Add**.
    The Add Member dialog box appears.

11. From the **Select Members** list, select **Firebox**. Click **OK**.
12. From the **To** list, select **Any-External**. Click **Remove**.
13. Click **Save**.

Send an SNMP Trap for a Policy

Your XTM device can send an SNMP trap when traffic is filtered by a policy. You must have at least one SNMP management station configured to enable SNMP traps.

1. Select **Firewall > Firewall Policies**.
2. Double-click a policy.
   Or, select a policy and click **Edit**.
   The Policy Configuration page appears.
3. Click the **Properties** tab.
4. In the **Logging** section, select the **Send SNMP Trap** check box.
5. Click **Save**.

About WatchGuard Passphrases, Encryption Keys, and Shared Keys

As part of your network security solution, you use passphrases, encryption keys, and shared keys. This topic includes information about most of the passphrases, encryption keys, and shared keys you use for WatchGuard products. It does not include information about third-party passwords or passphrases. Information about restrictions for passphrases, encryption keys, and shared keys is also included in the related procedures.

Create a Secure Passphrase, Encryption Key, or Shared Key

To create a secure passphrase, encryption key, or shared key, we recommend that you:

- Use a combination of uppercase and lowercase ASCII characters, numbers, and special characters (for example, Im4e@tiN9).
- Do not use a word from standard dictionaries, even if you use it in a different sequence or in a different language.
- Do not use a name. It is easy for an attacker to find a business name, familiar name, or the name of a famous person.

As an additional security measure, we recommend that you change your passphrases, encryption keys, and shared keys at regular intervals.

XTM Device Passphrases

An XTM device uses two passphrases:

Status passphrase

The read-only password or passphrase that allows access to the XTM device. When you log in with this passphrase, you can review your configuration, but you cannot save changes to the XTM device. The status passphrase is associated with the user name *status*.

Configuration passphrase

The read-write password or passphrase that allows an administrator full access to the XTM device. You must use this passphrase to save configuration changes to the XTM device. This is also the passphrase you must use to change your XTM device passphrases. The configuration passphrase is associated with the user name *admin*.

Each of these XTM device passphrases must be at least 8 characters.

User Passphrases

You can create user names and passphrases to use with Firebox authentication and role-based administration.

User Passphrases for Firebox authentication

After you set this user passphrase, the characters are masked and it does not appear in simple text again. If the passphrase is lost, you must set a new passphrase. The allowed range for this passphrase is 8–32 characters.

User Passphrases for role-based administration

After you set this user passphrase, it does not appear again in the **User and Group Properties** dialog box. If the passphrase is lost, you must set a new passphrase. This passphrase must be at least 8 characters.

Server Passphrases

Administrator passphrase

The Administrator passphrase is used to control access to the WatchGuard Server Center. You also use this passphrase when you connect to your Management Server from WatchGuard System Manager (WSM). This passphrase must be at least 8 characters. The Administrator passphrase is associated with the user name *admin*.

Authentication server shared secret

The shared secret is the key the XTM device and the authentication server use to secure the authentication information that passes between them. The shared secret is case-sensitive and must be the same on the XTM device and the authentication server. RADIUS, SecurID, and VASCO authentication servers all use a shared key.

Encryption Keys and Shared Keys

Log Server encryption key

The encryption key is used to create a secure connection between the XTM device and the Log Servers, and to avoid man-in-the-middle attacks. The allowed range for the encryption key is 8–32 characters. You can use all characters except spaces and slashes (/ or \).

Backup/Restore encryption key

This is the encryption key you create to encrypt a backup file of your XTM device configuration. When you restore a backup file, you must use the encryption key you selected when you created the configuration backup file. If you lose or forget this encryption key, you cannot restore the backup file. The encryption key must be at least 8 characters, and cannot be more than 15 characters.

VPN shared key

The shared key is a passphrase used by two devices to encrypt and decrypt the data that goes through the tunnel. The two devices use the same passphrase. If the devices do not have the same passphrase, they cannot encrypt and decrypt the data correctly.

Change XTM Device Passphrases

An XTM device uses two passphrases:

Status passphrase

The read-only password or passphrase that allows access to the XTM device.

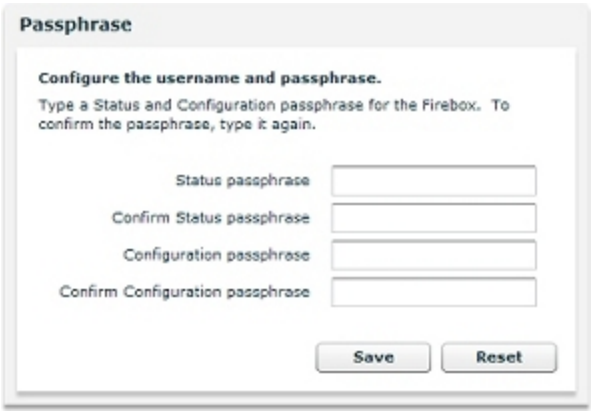
Configuration passphrase

The read-write password or passphrase that allows an administrator full access to the XTM device.

For more information about passphrases, see *About WatchGuard Passphrases, Encryption Keys, and Shared Keys* on page 63.

To change the passphrases:

1. Select **System > Passphrase**.
   The Passphrase page appears.



2. Type and confirm the new status (read-only) and configuration (read/write) passphrases. The status passphrase must be different from the configuration passphrase.
3. Click **Save**.

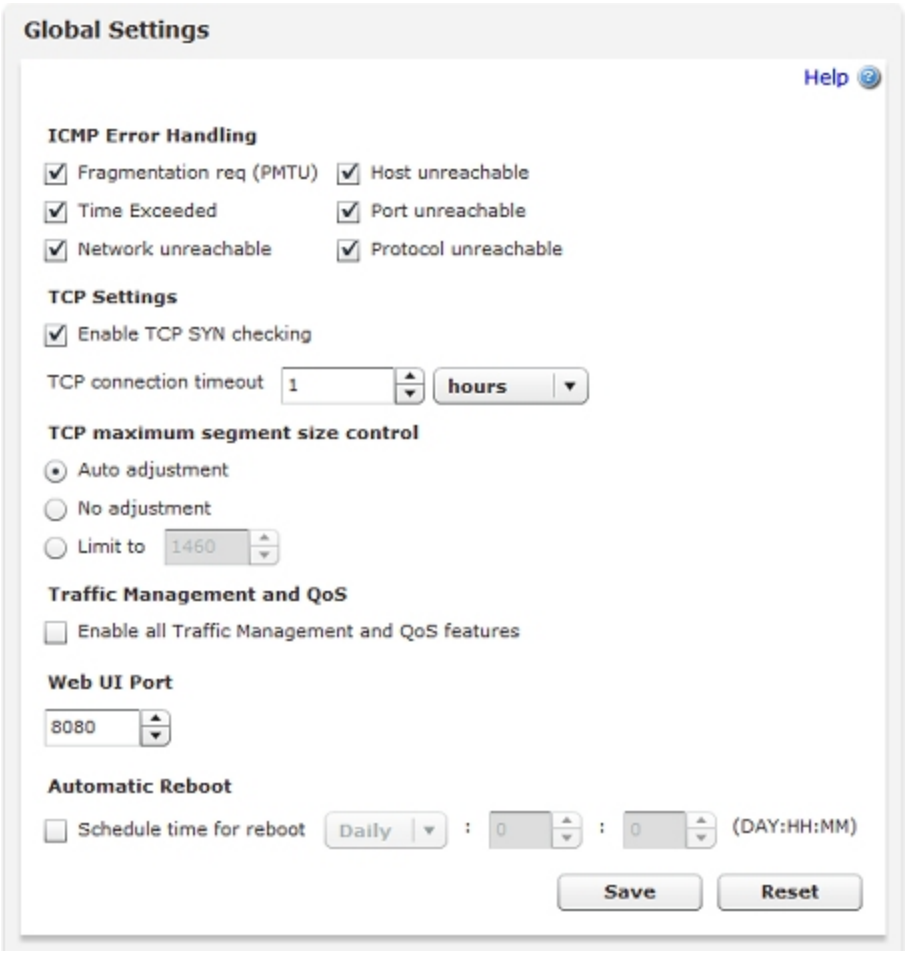
Define XTM Device Global Settings

From Fireware XTM Web UI, you can select settings that control the actions of many XTM device features. You can specify the basic parameters for:

- ICMP error handling
- TCP SYN checking
- TCP maximum size adjustment
- Traffic management and QoS
- Web UI port

To configure the global settings:

1. Select **System > Global Settings**.
   The Global Settings dialog box appears.



2. Configure the different categories of global settings as described in the subsequent sections.
3. Click **Save**.

Define ICMP Error Handling Global Settings

Internet Control Message Protocol (ICMP) settings control errors in connections. It is used for two types of operations:

- To tell client hosts about error conditions
- To probe a network to find general characteristics about the network

The XTM device sends an ICMP error message each time an event occurs that matches one of the parameters you selected. These messages are good tools to use when you troubleshoot problems, but can also decrease security because they expose information about your network. If you deny these ICMP messages, you can increase security if you prevent network probes, but this can also cause timeout delays for incomplete connections, which can cause application problems.

Settings for global ICMP error handling are:

Fragmentation Req (PMTU)

Select this check box to allow ICMP Fragmentation Req messages. The XTM device uses these messages to find the MTU path.

Time Exceeded

Select this check box to allow ICMP Time Exceeded messages. A router usually sends these messages when a route loop occurs.

Network Unreachable

Select this check box to allow ICMP Network Unreachable messages. A router usually sends these messages when a network link is broken.

Host Unreachable

Select this check box to allow ICMP Host Unreachable messages. Your network usually sends these messages when it cannot use a host or service.

Port Unreachable

Select this check box to allow ICMP Port Unreachable messages. A host or firewall usually sends these messages when a network service is not available or is not allowed.

Protocol Unreachable

Select this check box to allow ICMP Protocol Unreachable messages.

To override these global ICMP settings for a specific policy, from Fireware XTM Web UI:

1. Select **Firewall > Firewall Policies**.
2. Double-click the policy to edit it.
   The Policy Configuration page appears.
3. Select the **Advanced** tab.
4. Select the **Use policy-based ICMP error handling** check box.
5. Select only the check boxes for the settings you want to enable.
6. Click **Save**.

Configure TCP Settings

Enable TCP SYN checking

To enable TCP SYN checking to make sure that the TCP three-way handshake is completed before the XTM device allows a data connection, select this option.

TCP connection timeout

Specify the connection timeout value in seconds, minutes, hours, or days. The default setting is 1 hour.

TCP maximum segment size control

The TCP segment can be set to a specified size for a connection that must have more TCP/IP layer 3 overhead (for example, PPPoE, ESP, or AH). If this size is not correctly configured, users cannot get access to some web sites.

The global TCP maximum segment size adjustment settings are:

- **Auto Adjustment**— This option enables the XTM device to examine all maximum segment size (MSS) negotiations and changes the MSS value to the applicable one.
- **No Adjustment**— The XTM device does not change the MSS value.
- **Limit to**— Type or select a size adjustment limit.

Enable or Disable Traffic Management and QoS

For performance testing or network debugging purposes, you can disable the Traffic Management and QoS features.

To enable these features:

Select the **Enable all traffic management and QoS features** check box.

To disable these features:

Clear the **Enable all traffic management and QoS features** check box.

Change the Web UI Port

By default, Fireware XTM Web UI uses port 8080.

To change the default port:

1. In the **Web UI Port** text box, type or select a different port number.
2. Use the new port to connect to Fireware XTM Web UI and test the connection with the new port.

Automatic Reboot

You can schedule your XTM device to automatically reboot at the day and time you specify.

To schedule an automatic reboot for your device:

1. Select the **Schedule time for reboot** check box.
2. In the adjacent drop-down list, select **Daily** to reboot at the same time every day, or select a day of the week for a weekly reboot.
3. In the adjacent text boxes, type or select the hour and minute of the day (in 24-hour time format) that you want the reboot to start.

About WatchGuard Servers

When you install the WatchGuard System Manager software, you can choose to install one or more of the WatchGuard servers. You can also run the installation program and select to install only one or more of the servers, without WatchGuard System Manager. When you install a server, the WatchGuard Server Center program is automatically installed. WatchGuard Server Center is a single application you can use to set up and configure all your WatchGuard System Manager servers. You can also use WatchGuard Server Center to backup and restore your Management Server.

When you use Fireware XTM Web UI to manage your XTM devices, you can choose to also use WatchGuard servers and WatchGuard Server Center. For more information about WatchGuard System Manager, WatchGuard servers, and WatchGuard Server Center, see the *Fireware XTM WatchGuard System Manager v11.x Help* and the *Fireware XTM WatchGuard System Manager v11.x User Guide*.

The five WatchGuard servers are:

- Management Server
- Log Server
- Report Server
- Quarantine Server
- WebBlocker Server

For more information about WatchGuard System Manager and WatchGuard servers, see the *Fireware XTM WatchGuard System Manager v11.x Help* or *v11.x User Guide*.

Each server has a specific function:

Management Server

The Management Server operates on a Windows computer. With this server, you can manage all firewall devices and create virtual private network (VPN) tunnels with a simple drag-and-drop function. The basic functions of the Management Server are:

- Certificate authority to distribute certificates for Internet Protocol Security (IPSec) tunnels
- VPN tunnel configuration management
- Management for multiple XTM devices

For more information about the Management Server, see About the WatchGuard Management Server the *Fireware XTM WatchGuard System Manager v11.x Help* or *v11.x User Guide*.

Log Server

The Log Server collects log messages from each XTM device and stores them in a PostgreSQL database. The log messages are encrypted when they are sent to the Log Server. The log message format is XML (plain text). The types of log message that the Log Server collects include traffic log messages, event log messages, alarms, and diagnostic messages.

For more information about Log Servers, see the *Fireware XTM WatchGuard System Manager v11.x Help* or *v11.x User Guide*.

Report Server

The Report Server periodically consolidates data collected by your Log Servers from your XTM devices, and stores them in a PostgreSQL database. The Report Server then generates the reports you specify. When the data is on the Report Server, you can review it with Report Manager or Reporting Web UI.

For more information about how to use Reporting Web UI, see the *Reporting Web UI Help*.

For more information about the Report Server, see the *Fireware XTM WatchGuard System Manager v11.x Help* or *v11.x User Guide*.

Quarantine Server

The Quarantine Server collects and isolates email messages that spamBlocker identifies as possible spam.

For more information on the Quarantine Server, see *About the Quarantine Server* on page 759.

WebBlocker Server

The WebBlocker Server operates with the HTTP proxy to deny user access to specified categories of web sites. When you configure an XTM device, you set the web site categories you want to allow or block.

For more information about WebBlocker and the WebBlocker Server, see *About WebBlocker* on page 669.

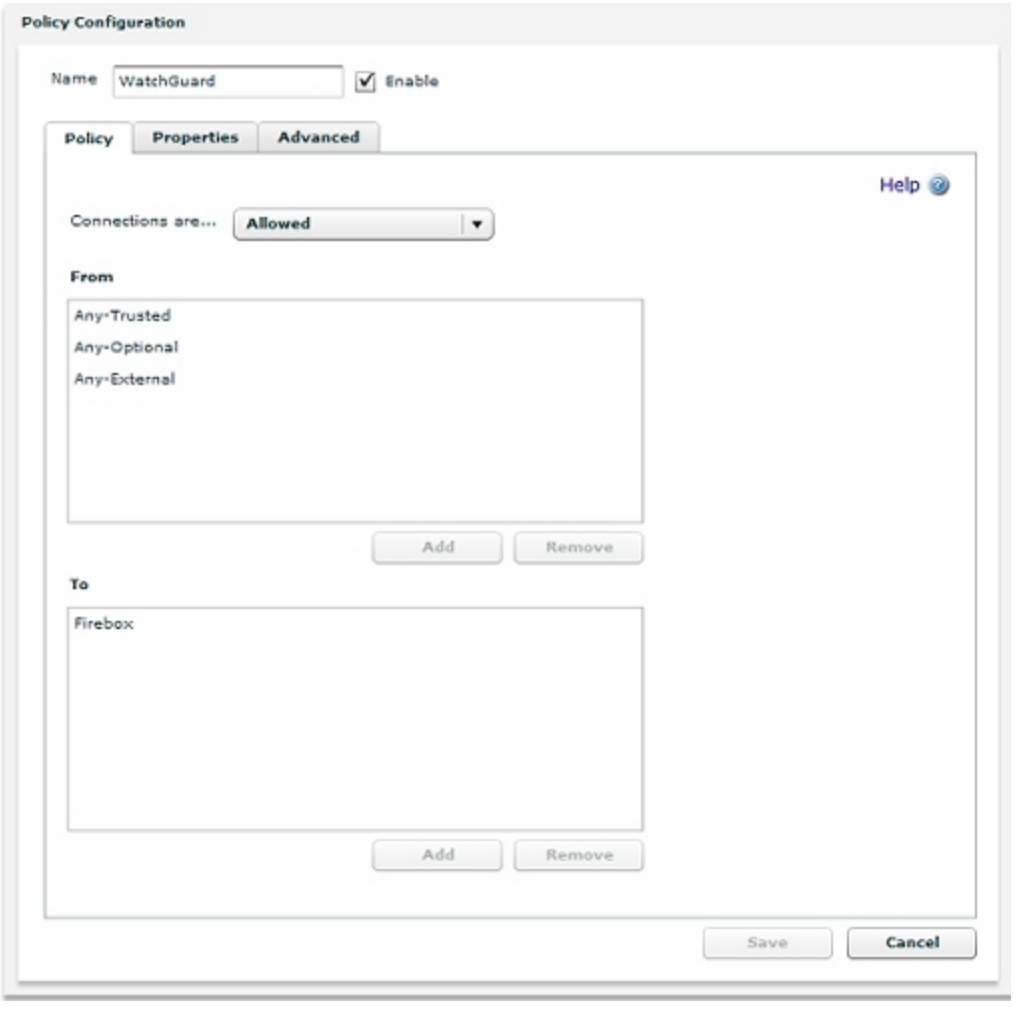
Manage an XTM device from a Remote Location

When you configure an XTM device with the Quick Setup Wizard, the WatchGuard policy is created automatically. This policy allows you to connect to and administer the XTM device from any computer on the trusted or optional networks. If you want to manage the XTM device from a remote location (any location external to the XTM device), then you must modify the WatchGuard policy to allow administrative connections from the IP address of your remote location.

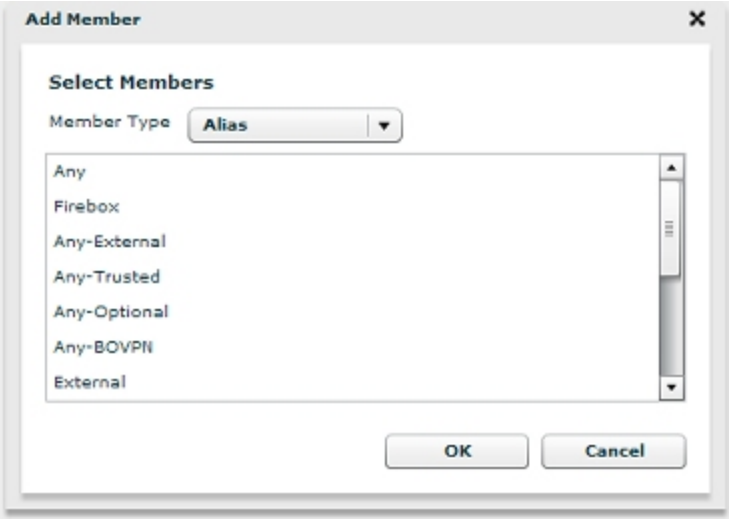
The WatchGuard policy controls access to the XTM device on these four TCP ports: 4103, 4105, 4117, 4118. When you allow connections in the WatchGuard policy, you allow connections to each of these four ports.

Before you modify the WatchGuard policy, we recommend that you consider connecting to the XTM device with a VPN. This greatly increases the security of the connection. If this is not possible, we recommend that you allow access from the external network to only certain authorized users and to the smallest number of computers possible. For example, your configuration is more secure if you allow connections from a single computer instead of from the alias *Any-External*.

1. Select **Firewall > Firewall Policies**.
2. Double click the **WatchGuard** policy.
   Or, select the WatchGuard policy and click .
   The Policy Configuration page appears.



3. In the **From** section, click **Add**.
   The Add Member dialog box appears.



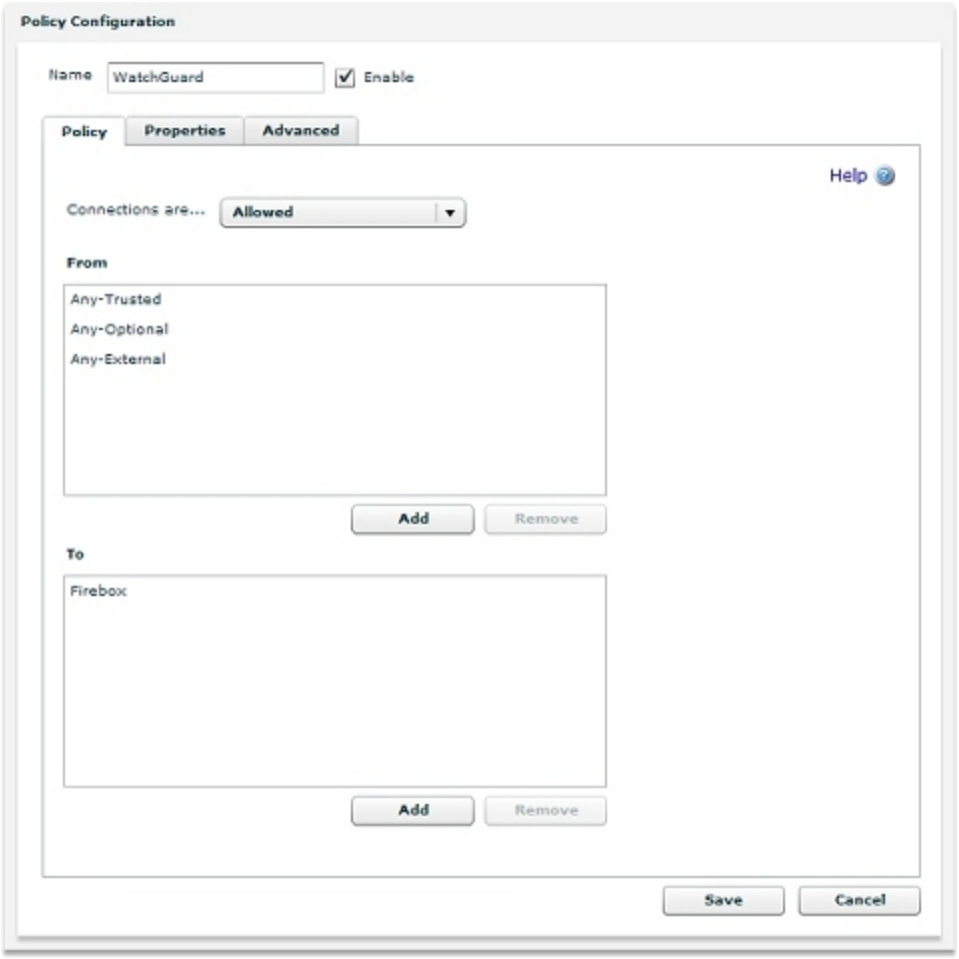
4. To add the IP address of the external computer that connects to the XTM device, from the **Member Type** drop-down list, select **Host IP**, and click **OK**. Type the IP address.
5. To give access to an authorized user, from the **Member Type** drop-down list, select **Alias**.
   For information about how to create an alias, see *Create an Alias* on page 295.

Configure an XTM Device as a Managed Device

If your XTM device has a dynamic IP address, or if the Management Server cannot connect to it for another reason, you can configure the XTM device as a managed device before you add it to the Management Server.

Edit the WatchGuard Policy

1. Select **Firewall > Firewall Policies**.
   The Firewall policies page appears.
2. Double-click the **WatchGuard** policy to open it.
   The Policy Configuration page for the WatchGuard policy appears.



3. In the **Connections are** drop-down list, make sure **Allowed** is selected.
4. In the **From** section, click **Add**.
   The Add Member dialog box appears.
5. In the **Member Type** drop-down list, select **Host IP**.
6. In the **Member type** text box, type the IP address of the external interface of the gateway Firebox. If you do not have a gateway Firebox that protects the Management Server from the Internet, type the static IP address of your Management Server.

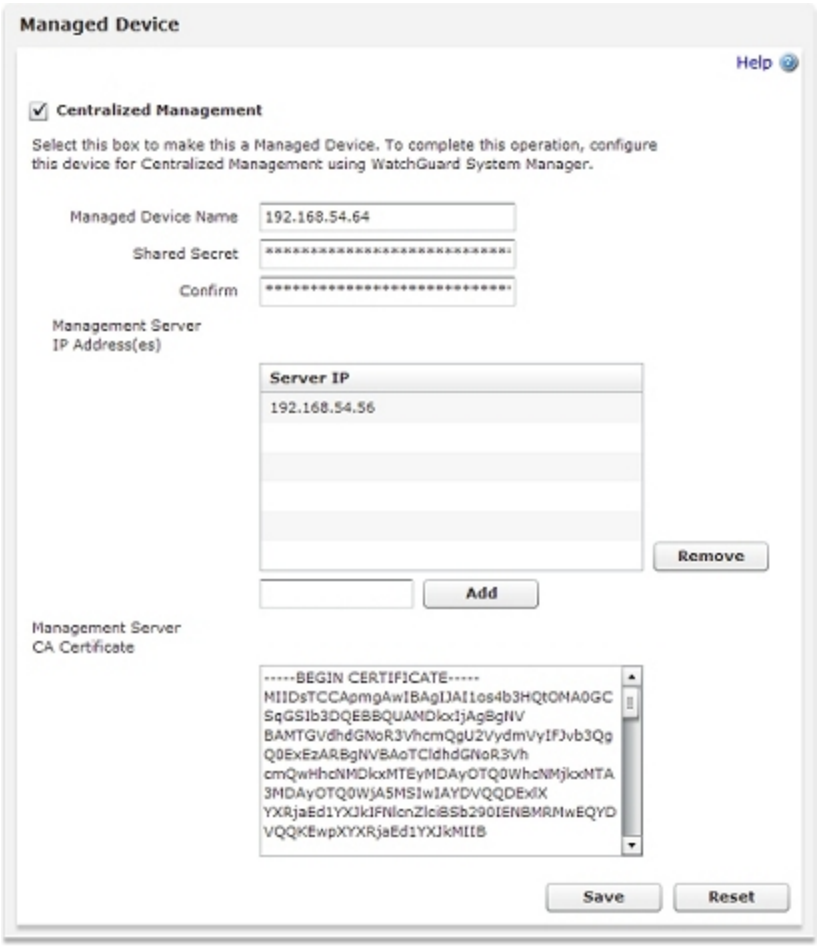
7. Click **OK** to close the **Add Member** dialog box.
8. Make sure the **To** section includes an entry of either **Firebox** or **Any**.
9. Click **Save**.

You can now add the device to your Management Server configuration. When you add this XTM device to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the XTM device as a managed device.

Set Up the Managed Device

(Optional) If your XTM device has a dynamic IP address, or if the Management Server cannot find the IP address of the XTM device for any reason, you can use this procedure to prepare your XTM device to be managed by the Management Server.

1. Select **System > Managed Device**.
   The Managed Device page appears.



2. To set up an XTM device as a managed device, select the **Centralized Management** check box.
3. In the **Managed Device Name** text box, type the name you want to give the XTM device when you add it to the Management Server configuration.

This name is case-sensitive and must match the name you use when you add the device to the Management Server configuration.

4. In the **Management Server IP Address(es)** list, select the IP address of the Management Server if it has a public IP address.

   Or, select the public IP address of the gateway Firebox for the Management Server.

5. To add an address, click **Add**.

   The XTM device that protects the Management Server automatically monitors all ports used by the Management Server and forwards any connection on these ports to the configured Management Server. When you use the Management Server Setup Wizard, the wizard adds a *WG-Mgmt-Server* policy to your configuration to handle these connections. If you did not use the Management Server Setup Wizard on the Management Server, or, if you skipped the **Gateway Firebox** step in the wizard, you must manually add the *WG-Mgmt-Server* policy to the configuration of your gateway Firebox.

6. In the **Shared Secret** and the **Confirm** fields, type the shared secret.

   The shared secret you type here must match the shared secret you type when you add the XTM device to the Management Server configuration.

7. Copy the text of your Management Server CA certificate file, and paste it in the **Management Server Certificate** text box.
8. Click **Save**.

When you save the configuration to the XTM device, the XTM device is enabled as a managed device. The managed XTM device tries to connect to the IP address of the Management Server on TCP port 4110. Management connections are allowed from the Management Server to this managed XTM device.

You can now add the device to your Management Server configuration. For more information, see the *WatchGuard System Manager Help* or *User Guide*.

You can also use WSM to configure the management mode for your device. For more information, see the *WatchGuard System Manager Help* or *User Guide*.

Upgrade to a New Version of Fireware XTM

Periodically, WatchGuard makes new versions Fireware XTM appliance software available to XTM device users with active LiveSecurity subscriptions. To upgrade from one version of Fireware XTM to a new version of Fireware XTM, use the procedures in the subsequent sections.

Install the Upgrade on Your Management Computer

1. Download the updated Fireware XTM software from the Software Downloads section of the WatchGuard web site at http://www.watchguard.com.
2. Launch the file that you downloaded from the LiveSecurity web site and use the on-screen procedure to install the Fireware XTM upgrade file in the WatchGuard installation directory on your management computer.
   By default, the file is installed in a folder in:
   `C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\11.x`

Upgrade the XTM Device

1. Select **System > Backup Image** to save a backup image of your XTM device.
   For more information, see *Make a Backup of the XTM Device Image* on page 39.
2. Select **System > Upgrade OS**.
3. Type the filename or click **Browse** to select the upgrade file from the directory it is installed in.
   The filename ends with .sysa_dl.
4. Click **Upgrade**.

The upgrade procedure can take up to 15 minutes and automatically reboots the XTM device.

If your XTM device has been in operation for some time before you upgrade, you might have to restart the device before you start the upgrade to clear the temporary memory.

Download the Configuration File

From the Fireware XTM Web UI, you can download your XTM device configuration to a compressed file. This can be useful if you want to open the same configuration file in Fireware XTM Policy Manager but are unable to connect to the device from Policy Manager. This can also be useful if you want to send your configuration file to a WatchGuard technical support representative.

1. Select **System > Configuration File**.
   The Configuration file download page appears.
2. Click **Download the configuration file**.
   The Select location for download dialog box appears.
3. Select a location to save the configuration file.

The configuration file is saved in a compressed (.tgz) file format. Before you can use this file with Fireware XTM Policy Manager, you must extract the zipped file to a folder on your computer.

For more information about Policy Manager see the WatchGuard System Manager Help.

About Upgrade Options

You can add upgrades to your XTM device to enable additional subscription services, features, and capacity.

For a list of available upgrade options, see www.watchguard.com/products/options.asp.

Subscription Services Upgrades

WebBlocker

The WebBlocker upgrade enables you to control access to web content.

For more information, see *About WebBlocker* on page 669.

spamBlocker

The spamBlocker upgrade allows you to filter spam and bulk email.

For more information, see *About spamBlocker* on page 683.

Gateway AV/IPS

The Gateway AV/IPS upgrade enables you to block viruses and prevent intrusion attempts by hackers.

For more information, see *About Gateway AntiVirus* on page 707.

Appliance and Software Upgrades

Pro

The Pro upgrade to Fireware XTM provides several advanced features for experienced customers, such as server load balancing and additional SSL VPN tunnels. The features available with a Pro upgrade depend on the type and model of your XTM device.

For more information, see *Fireware XTM with a Pro Upgrade* on page 15.

Model upgrades

For some XTM device models, you can purchase a license key to upgrade the device to a higher model in the same product family. A model upgrade gives your XTM device the same functions as a higher model.

To compare the features and capabilities of different XTM device models, go to http://www.watchguard.com/products/compare.asp.

How to Apply an Upgrade

When you purchase an upgrade, you register the upgrade on the WatchGuard LiveSecurity web site. Then you download a feature key that enables the upgrade on your XTM device.

For information about feature keys, see *About Feature Keys* on page 50.

Renew Security Subscriptions

Your WatchGuard subscription services (Gateway AntiVirus, Intrusion Prevention Service, Application Control, WebBlocker, and spamBlocker) must get regular updates to operate effectively.

To see the expiration date of your subscription services, from Fireware XTM Web UI, select **System > Feature Key**. The **Expiration** column shows when the subscription expires. You can also see the number of days until each service expires on the system Dashboard. Select **Dashboard > System** to see the system Dashboard.

When you renew the security subscription, you must update the feature key on the XTM device. To update the feature key, from Fireware XTM Web UI, select **System > Feature Key**.

For more information about feature keys, see *About Feature Keys* on page 50.

Subscription Services Status and Manual Signatures Updates

The Gateway AntiVirus, Intrusion Prevention Service, and Application Control security services use a frequently-updated set of signatures to identify the latest viruses, threats, and applications. You can configure these services to update signatures automatically. For information about signature update settings see:

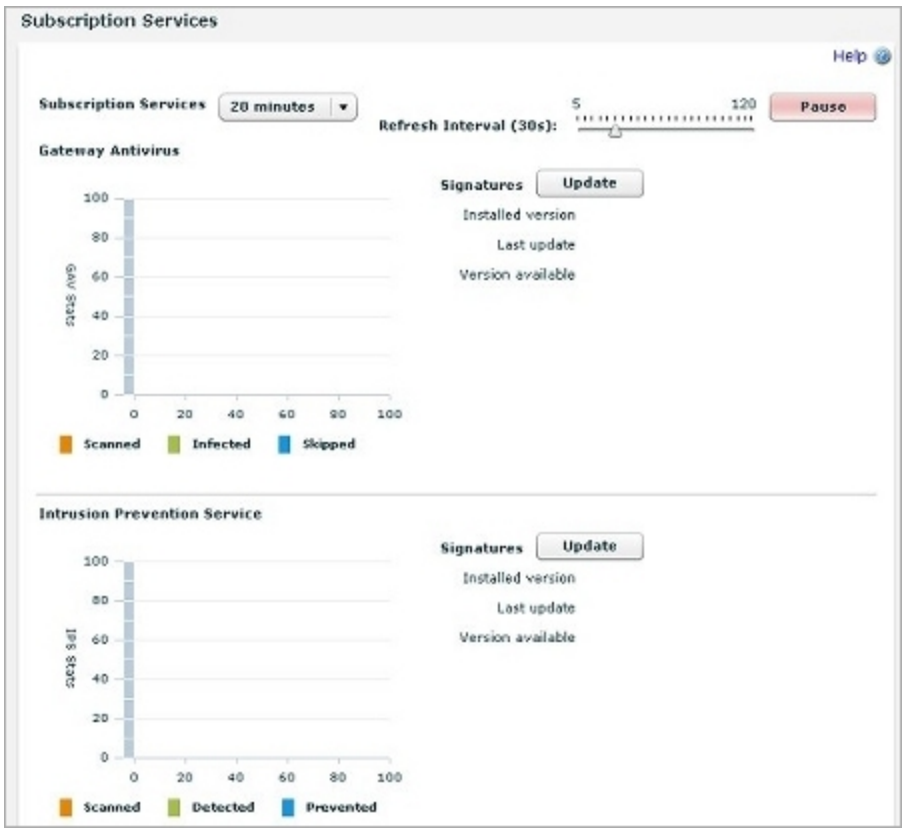
- *Configure the Gateway AV Update Server*
- *Configure the IPS Update Server*
- *Configure the Application Control Update Server*

You can also update signatures manually. If the signatures on the XTM device are not current, you are not protected from the latest viruses and intrusions.

The **Subscription Services** status page shows statistics about the subscription services activity, and shows the status of signature updates. For each signature-based service, you can see the current signature version installed and whether a newer version of signatures is available.

To see the status of Subscription Services:

1. Connect to Fireware XTM Web UI for your device.
2. Select **Dashboard > Subscription Services**.
   The Subscription Services status page appears.



1. To manually update signatures for a service, click **Update** for each service you want to update.
   The XTM device downloads the most recent available signature update.

For more information about the statistics on this page, see *About the Dashboard and System Status Pages* on page 471.

6 Network Setup and Configuration

About Network Interface Setup

A primary component of your XTM device setup is the configuration of network interface IP addresses. When you run the Quick Setup Wizard, the external and trusted interfaces are set up so traffic can flow from protected devices to an outside network. You can use the procedures in this section to change the configuration after you run the Quick Setup Wizard, or to add other components of your network to the configuration. For example, you can set up an optional interface for public servers such as a web server.

Your XTM device physically separates the networks on your Local Area Network (LAN) from those on a Wide Area Network (WAN) like the Internet. Your device uses *routing* to send packets from networks it protects to networks outside your organization. To do this, your device must know what networks are connected on each interface.

We recommend that you record basic information about your network and VPN configuration in the event that you need to contact technical support. This information can help your technician resolve your problem quickly.

Network Modes

Your XTM device supports several network modes:

Mixed routing mode

In mixed routing mode, you can configure your XTM device to send network traffic between a wide variety of physical and virtual network interfaces. This is the default network mode, and this mode offers the greatest amount of flexibility for different network configurations. However, you must configure each interface separately, and you may have to change network settings for each computer or client protected by your XTM device. The XTM device uses Network Address Translation (NAT) to send information between network interfaces.

For more information, see *About Network Address Translation* on page 143.

The requirements for a mixed routing mode are:

- All interfaces of the XTM device must be configured on different subnets. The minimum configuration includes the external and trusted interfaces. You also can configure one or more optional interfaces.
- All computers connected to the trusted and optional interfaces must have an IP address from that network.

Drop-in mode

In a drop-in configuration, your XTM device is configured with the same IP address on all interfaces. You can put your XTM device between the router and the LAN and not have to change the configuration of any local computers. This configuration is known as *drop-in* because your XTM device is *dropped in* to an existing network. Some network features, such as bridges and VLANs (Virtual Local Area Networks), are not available in this mode.

For drop-in configuration, you must:

- Assign a static external IP address to the XTM device.
- Use one logical network for all interfaces.
- Not configure multi-WAN in Round-robin or Failover mode.

For more information, see *Drop-In Mode* on page 90.

Bridge mode

Bridge mode is a feature that allows you to place your XTM device between an existing network and its gateway to filter or manage network traffic. When you enable this feature, your XTM device processes and forwards all incoming network traffic to the gateway IP address you specify. When the traffic arrives at the gateway, it appears to have been sent from the original device. In this configuration, your XTM device cannot perform several functions that require a public and unique IP address. For example, you cannot configure an XTM device in bridge mode to act as an endpoint for a VPN (Virtual Private Network).

For more information, see *Bridge Mode* on page 96.

Interface Types

You use three interface types to configure your network in mixed routing or drop-in mode:

External Interfaces

An external interface is used to connect your XTM device to a network outside your organization. Often, an external interface is the method by which you connect your XTM device to the Internet. You can configure a maximum of four (4) physical external interfaces.

When you configure an external interface, you must choose the method your Internet service provider (ISP) uses to give you an IP address for your XTM device. If you do not know the method, get this information from your ISP or network administrator.

Trusted Interfaces

Trusted interfaces connect to the private LAN (local area network) or internal network of your organization. A trusted interface usually provides connections for employees and secure internal resources.

Optional Interfaces

Optional interfaces are *mixed-trust* or *DMZ* environments that are separate from your trusted network. Examples of computers often found on an optional interface are public web servers, FTP servers, and mail servers.

For more information on interface types, see *Common Interface Settings* on page 98.

If you have an XTM 2 Series device, you can use Fireware XTM Web UI to configure failover with an external modem over the serial port.

For more information, see *Serial Modem Failover* on page 135.

When you configure the interfaces on your XTM device, you must use slash notation to denote the subnet mask. For example, you would enter the network range 192.168.0.0 subnet mask 255.255.255.0 as 192.168.0.0/24. A trusted interface with the IP address of 10.0.1.1/16 has a subnet mask of 255.255.0.0.

For more information on slash notation, see *About Slash Notation* on page 3.

Mixed Routing Mode

In mixed routing mode, you can configure your XTM device to send network traffic between many different types of physical and virtual network interfaces. Mixed routing mode is the default network mode. While most network and security features are available in this mode, you must carefully check the configuration of each device connected to your XTM device to make sure that your network operates correctly.

A basic network configuration in mixed routing mode uses at least two interfaces. For example, you can connect an external interface to a cable modem or other Internet connection, and a trusted interface to an internal router that connects internal members of your organization. From that basic configuration, you can add an optional network that protects servers but allows greater access from external networks, configure VLANs, and other advanced features, or set additional options for security like MAC address restrictions. You can also define how network traffic is sent between interfaces.

To get started on interface configuration in mixed routing mode, see *Common Interface Settings* on page 98.

It is easy to forget IP addresses and connection points on your network in mixed routing mode, especially if you use VLANs (Virtual Local Area Networks), secondary networks, and other advanced features. We recommend that you record basic information about your network and VPN configuration in the event that you need to contact technical support. This information can help your technician resolve your problem quickly.

Configure an External Interface

An external interface is used to connect your XTM device to a network outside your organization. Often, an external interface is the method by which you connect your device to the Internet. You can configure a maximum of four (4) physical external interfaces.

When you configure an external interface, you must choose the method your Internet service provider (ISP) uses to give you an IP address for your device. If you do not know the method, get this information from your ISP or network administrator.

For information about methods used to set and distribute IP addresses, see *Static and Dynamic IP Addresses* on page 4.

Use a Static IP Address

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.
2. Select an external interface. Click **Configure**.
3. From the **Configuration Mode** drop-down list, select **Static IP**.
4. In the **IP address** text box, type the IP address of the interface.
5. In the **Gateway** text box, type the IP address of the default gateway.

6. Click **Save**.

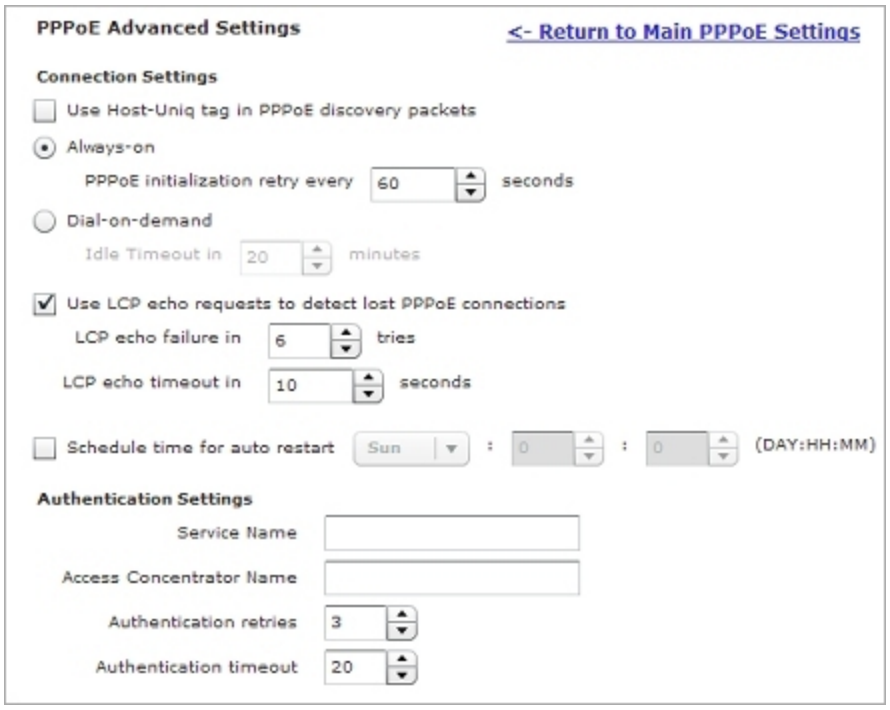
Use PPPoE Authentication

If your ISP uses PPPoE, you must configure PPPoE authentication before your device can send traffic through the external interface.

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.
2. Select an external interface. Click **Configure**.
3. From the **Configuration Mode** drop-down list, select **PPPoE**.

4. Select an option:
   - **Obtain an IP address automatically**
   - **Use this IP address** (supplied by your Internet Service Provider)
5. If you selected **Use this IP Address**, in the adjacent text box, type the IP address.
6. Type the **User Name** and **Password**. Type the password again.
   ISPs use the email address format for user names, such as user@example.com.

7. To configure additional PPPoE options, click **Advanced PPPoE Settings**.
   Your ISP can tell you if you must change the timeout or LCP values.



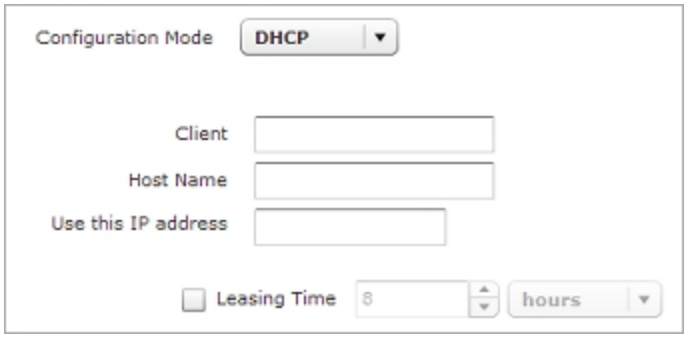
8. If your ISP requires the Host-Uniq tag for PPPoE discovery packets, select the **Use Host-Uniq tag in PPPoE discovery packets** check box.
9. Select when the device connects to the PPPoE server:
   - **Always-on** — The XTM device keeps a constant PPPoE connection. It is not necessary for network traffic to go through the external interface.
     If you select this option, type or select a value in the **PPPoE initialization retry every** text box to set the number of seconds that PPPoE tries to initialize before it times out.

- **Dial-on-Demand** — The XTM device connects to the PPPoE server only when it gets a request to send traffic to an IP address on the external interface. If your ISP regularly resets the connection, select this option.
  If you select this option, in the **Idle timeout in** text box, set the length of time a client can stay connected when no traffic is sent. If you do not select this option, you must manually restart the XTM device each time the connection resets.

10. In the **LCP echo failure in** text box, type or select the number of failed LCP echo requests allowed before the PPPoE connection is considered inactive and closed.
11. In the **LCP echo timeout in** text box, type or select the length of time, in seconds, that the response to each echo timeout must be received.
12. To configure the XTM device to automatically restart the PPPoE connection on a daily or weekly basis, select the **Schedule time for auto restart** check box.
13. In the **Schedule time for auto restart** drop-down list, select **Daily** to restart the connection at the same time each day, or select a day of the week to restart weekly. Select the hour and minute of the day (in 24 hour time format) to automatically restart the PPPoE connection.
14. In the **Service Name** text box, type a PPPoE service name.
    This is either an ISP name or a class of service that is configured on the PPPoE server. Usually, this option is not used. Select it only if there is more than one access concentrator, or you know that you must use a specified service name.
15. In the **Access Concentrator Name** text box, type the name of a PPPoE access concentrator, also known as a PPPoE server. Usually, this option is not used. Select it only if you know there is more than one access concentrator.
16. In the **Authentication retries** text box, type or select the number of times that the XTM device can try to make a connection.
    The default value is three (3) connection attempts.
17. In the **Authentication timeout** text box, type a value for the amount of time between retries.
    The default value is 20 seconds between each connection attempt.
18. Click **Return to Main PPPoE Settings**.
19. Save your configuration.

Use DHCP

1. From the **Configuration Mode** drop-down list, select **DHCP**.
2. If your ISP or external DHCP server requires a client identifier, such as a MAC address, in the **Client** text box, type this information.
3. To specify a host name for identification, type it in the **Host Name** text box.



4. To manually assign an IP address to the external interface, type it in the **Use this IP address** text box.

To configure this interface to obtain an IP address automatically, clear the **Use this IP address** text box.

5. To change the lease time, select the **Leasing Time** check box and select the value you want from the adjacent text box and drop-down list.

   IP addresses assigned by a DHCP server have an eight hour lease by default; each address is valid for eight hours.

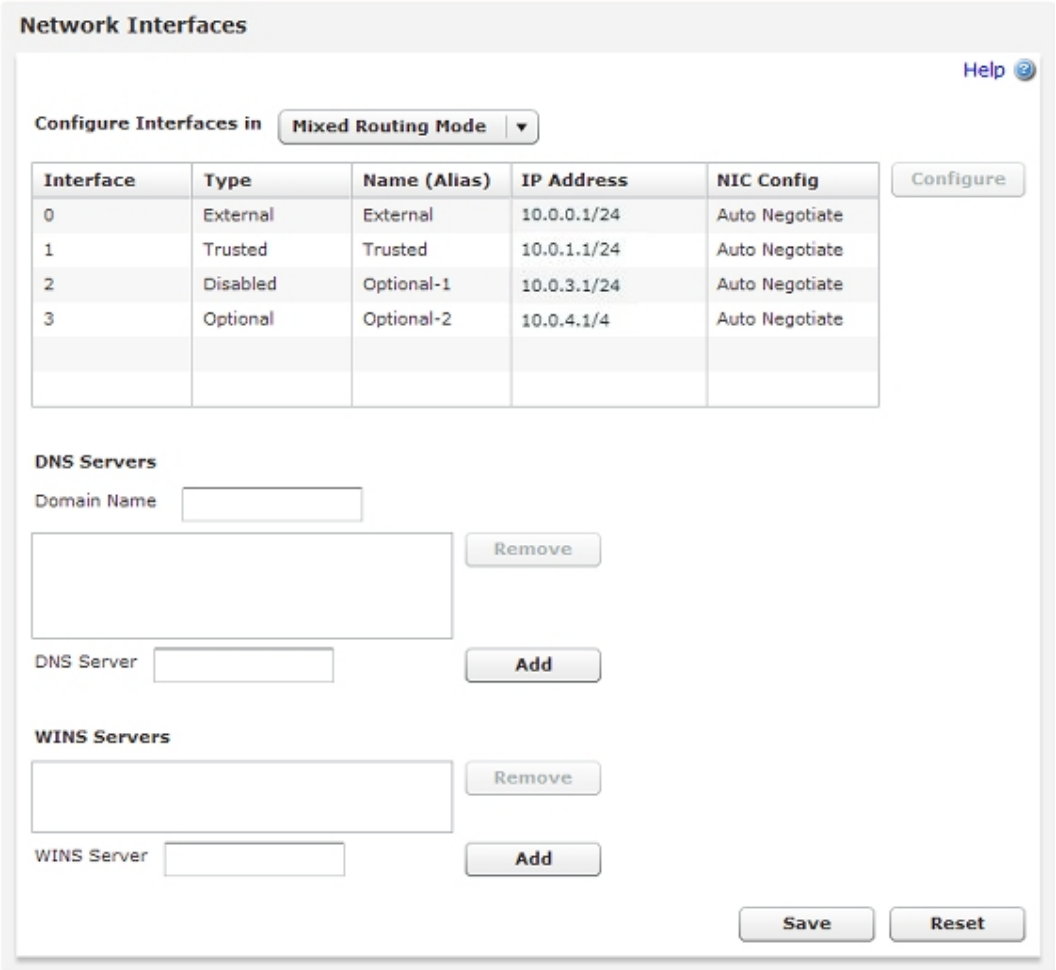
Configure DHCP in Mixed Routing Mode

DHCP (Dynamic Host Configuration Protocol) is a method to assign IP addresses automatically to network clients. You can configure your XTM device as a DHCP server for the networks that it protects. If you have a DHCP server, we recommend that you continue to use that server for DHCP.

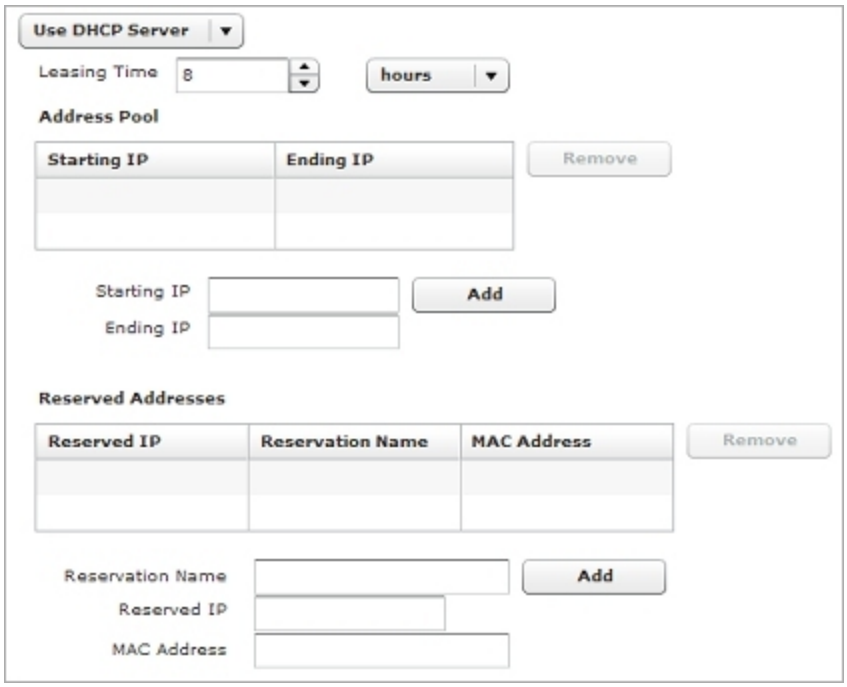
If your XTM device is configured in drop-in mode, see *Configure DHCP in Drop-In Mode* on page 93.

Configure DHCP

1. Select **Network > Interfaces**.
2. Select a trusted or an optional interface. Click **Configure**.



3. In the **Configuration Mode** drop-down list, select **Use DHCP Server**.



4. To add a group of IP addresses to assign to users on this interface, type a **Starting IP** address and an **Ending IP** address from the same subnet, then click **Add**.
   The address pool must belong either to the interface's primary or secondary IP subnet.
   You can configure a maximum of six address ranges. Address groups are used from first to last. Addresses in each group are assigned by number, from lowest to highest.
5. To change the default lease time, select a different option in the **Leasing Time** drop-down list.
   This is the time interval that a DHCP client can use an IP address that it receives from the DHCP server. When the lease time is about to expire, the client sends data to the DHCP server to get a new lease.
6. By default, when it is configured as a DHCP server your XTM device gives out the DNS and WINS server information configured on the **Network Configuration > WINS/DNS** tab. To specify different information for your device to assign when it gives out IP addresses, click the **DNS/WINS** tab.

   - Type a **Domain Name** to change the default DNS domain.
   - To create a new DNS or WINS server entry, click **Add** adjacent to the server type you want, type an IP address, and click **OK**.
   - To change the IP address of the selected server, click **Edit**.
   - To remove the selected server from the adjacent list, click **Delete**.

Configure DHCP Reservations

To reserve a specific IP address for a client:

1. Type a name for the reservation, the IP address you want to reserve, and the MAC address of the client's network card.
2. Click **Add**.

About the Dynamic DNS Service

You can register the external IP address of your XTM device with the dynamic Domain Name System (DNS) service DynDNS.org. A dynamic DNS service makes sure that the IP address attached to your domain name changes when your ISP gives your device a new IP address. This feature is available in either mixed routing or drop-in network configuration mode.

If you use this feature, your XTM device gets the IP address of members.dyndns.org when it starts up. It makes sure the IP address is correct every time it restarts and at an interval of every twenty days. If you make any changes to your DynDNS configuration on your XTM device, or if you change the IP address of the default gateway, it updates DynDNS.com immediately.

For more information on the Dynamic DNS service or to create a DynDNS account, go to http://www.dyndns.com.

> ***Note*** *WatchGuard is not affiliated with DynDNS.com.*

Configure Dynamic DNS

1. Select **Network > Dynamic DNS**.
   The Dynamic DNS client page appears.
2. Select a network interface, then click **Configure**.
   The Dynamic DNS configuration page appears.

3. Select the **Enable Dynamic DNS** check box.
4. Type the **Username** and **Password**.
5. In the **Confirm** text box, type the password again.
6. In the **Domain** text box, type the domain of your organization.
7. In the **Service Type** drop-down list, select the system to use for Dynamic DNS:

   - **dyndns** — Sends updates for a Dynamic DNS host name. Use the **dyndns** option when you have no control over your IP address (for example, it is not static, and it changes on a regular basis).
   - **custom** — Sends updates for a custom DNS host name. This option is frequently used by businesses that pay to register their domain with dyndns.com.

   For an explanation of each option, see http://www.dyndns.com/services/.

8. In the **Options** text box, type one or more of these options:

   - `mx=mailexchanger&` — Specifies a Mail eXchanger (MX) for use with the hostname.
   - `backmx=YES|NO&` — Requests that the MX in the previous parameter is set up as a backup MX (includes the host as an MX with a lower preference value).
   - `wildcard=ON|OFF|NOCHG&` — Enables or disables wildcards for this host (ON to enable).
   - `offline=YES|NO` — Sets the hostname to offline mode. One or more options can be chained together with the ampersand character. For example: `&mx=backup.kunstlerandsons.com&backmx=YES&wildcard=ON`

   For more information, see http://www.dyndns.com/developers/specs/syntax.html.

9. Click **Save**.

Drop-In Mode

In a drop-in configuration, your XTM device is configured with the same IP address on all interfaces. The drop-in configuration mode distributes the network's logical address range across all available network interfaces. You can put your XTM device between the router and the LAN and not have to change the configuration of any local computers. This configuration is known as drop-in mode because your XTM device is *dropped in* to a previously configured network.

In drop-in mode:

- You must assign the same primary IP address to all interfaces on your XTM device (external, trusted, and optional).
- You can assign secondary networks on any interface.
- You can keep the same IP addresses and default gateways for hosts on your trusted and optional networks, and add a secondary network address to the primary external interface so your XTM device can correctly send traffic to the hosts on these networks.
- The public servers behind your XTM device can continue to use public IP addresses. Network address translation (NAT) is not used to route traffic from outside your network to your public servers.

The properties of a drop-in configuration are:

- You must assign and use a static IP address on the external interface.
- You use one logical network for all interfaces.
- You cannot configure more than one external interface when your XTM device is configured in drop-in mode. Multi-WAN functionality is automatically disabled.

It is sometimes necessary to Clear the ARP cache of each computer protected by the XTM device, but this is not common.

> ***Note*** *If you move an IP address from a computer located behind one interface to a computer located behind a different interface, it can take several minutes before network traffic is sent to the new location. Your XTM device must update its internal routing table before this traffic can pass. Traffic types that are affected include logging, SNMP, and XTM device management connections.*

You can configure your network interfaces with drop-in mode when you run the Quick Setup Wizard. If you have already created a network configuration, you can use Policy Manager to switch to drop-in mode.
For more information, see *Run the Web Setup Wizard* on page 23.

Use Drop-In Mode for Network Interface Configuration

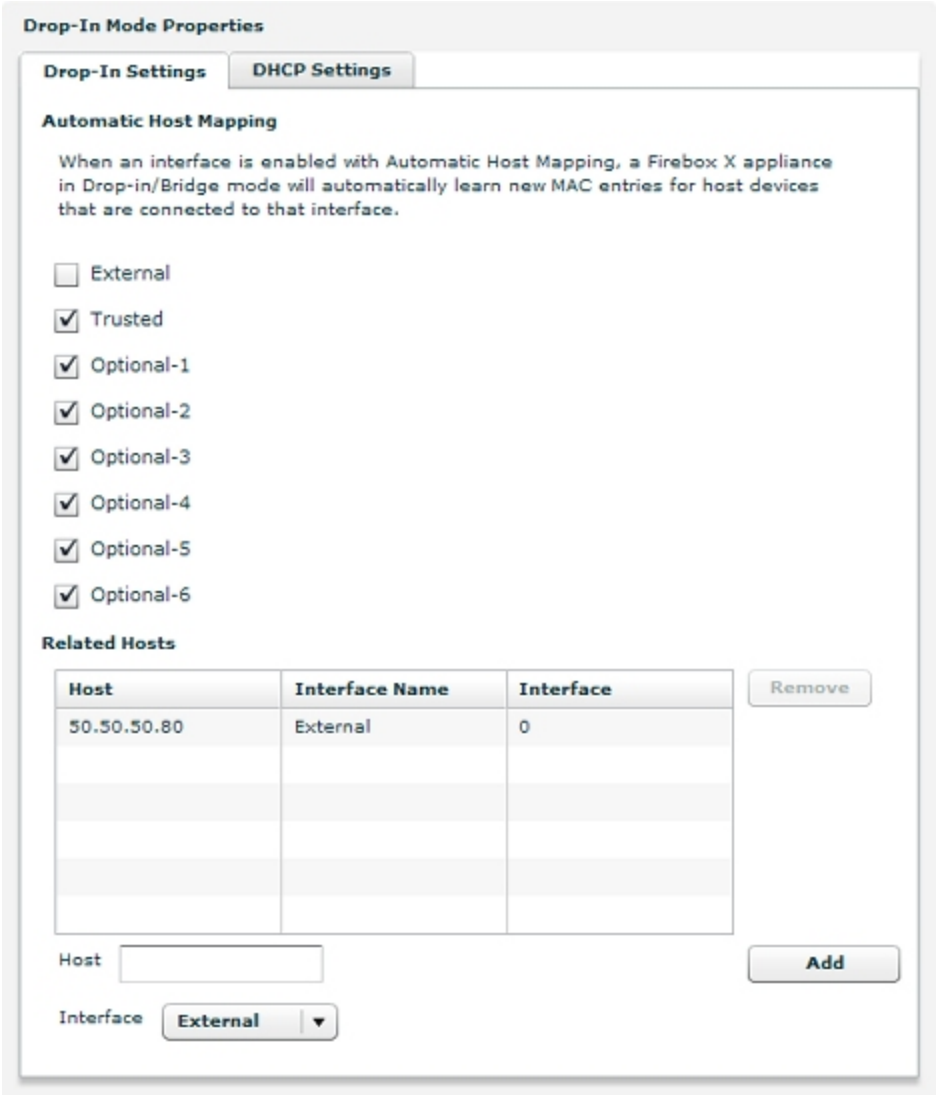
1. Select **Network > Interfaces**.
   The Network Interfaces dialog box appears.
2. From the **Configure Interfaces in** drop-down list, select **Drop-In Mode**.
3. In the **IP Address** text box, type the IP address you want to use as the primary address for all interfaces on your XTM device.
4. In the **Gateway** text box, type the IP address of the gateway. This IP address is automatically added to the Related Hosts list.

5. Click **Save**.

Configure Related Hosts

In a drop-in or bridge configuration, the XTM device is configured with the same IP address on each interface. Your XTM device automatically discovers new devices that are connected to these interfaces and adds each new MAC address to its internal routing table. If you want to configure device connections manually, or if the Automatic Host Mapping feature does not operate correctly, you can add a related hosts entry. A related hosts entry creates a static route between the host IP address and one network interface. We recommend that you disable Automatic Host Mapping on interfaces for which you create a related hosts entry.

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.
2. Configure network interfaces in drop-in or bridge mode. Click **Properties**.
   The Drop-In Mode Properties page appears.
3. Clear the check box for any interface for which you want to add a related hosts entry.
4. In the **Host** text box, type the IP address of the device for which you want to build a static route from the XTM device. Select the **Interface** from the adjacent drop-down list, then click **Add**. Repeat this step to add additional devices.



5. Click **Save**.

Configure DHCP in Drop-In Mode

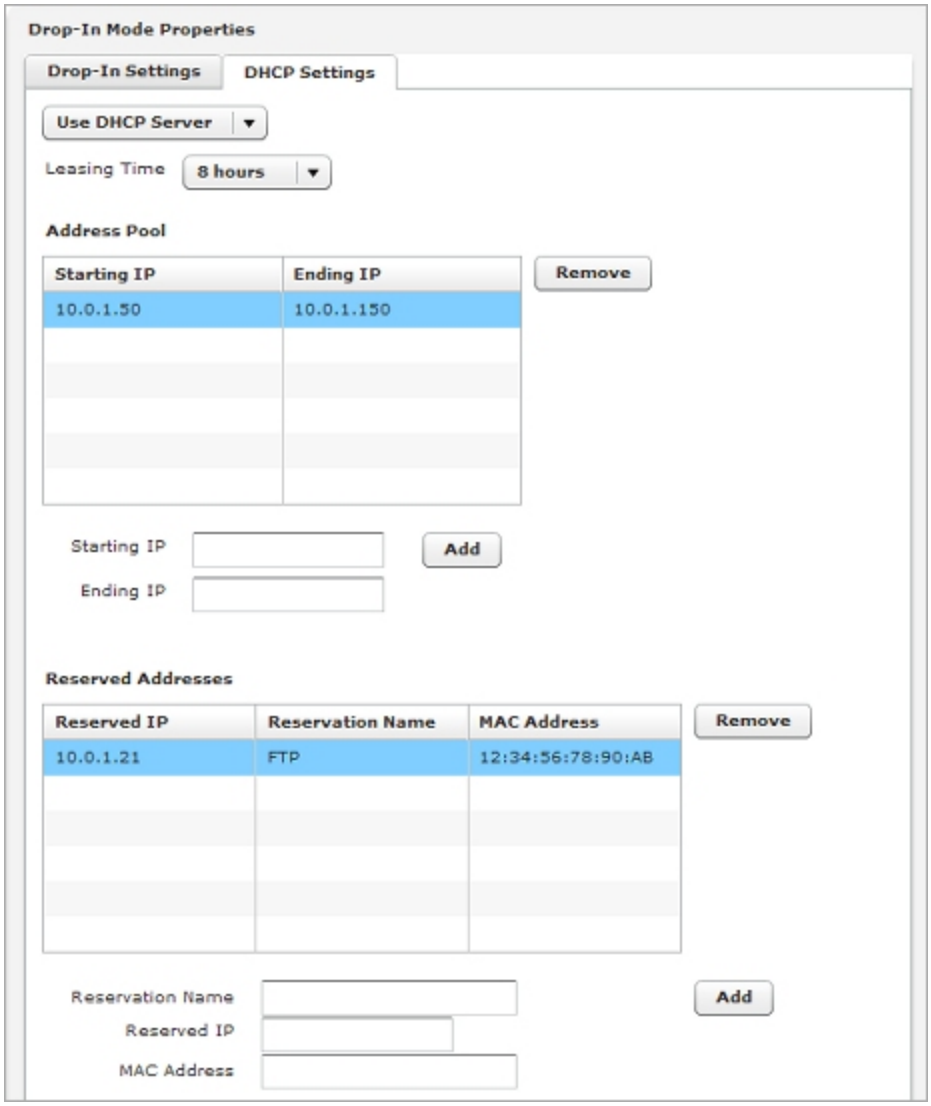
When you use drop-in mode for network configuration, you can optionally configure the XTM device as a DHCP server for the networks it protects, or make the XTM device a DHCP relay agent. If you have a configured DHCP server, we recommend that you continue to use that server for DHCP.

Use DHCP

When you use drop-in mode for network configuration, you can optionally configure the XTM device as a DHCP server for networks it protects, or make the XTM device a DHCP relay agent. If you have a configured DHCP server, we recommend that you continue to use that server for DHCP.

By default, your XTM device gives out the configure DNS/WINS server information when it is configured as a DHCP server. You can configure DNS/WINS information on this page to override the global configuration. For more information, see the instructions in *Add WINS and DNS Server Addresses* on page 102.

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.
2. If your XTM device is not already configured in drop-in mode, from the **Configure Interfaces in** drop-down list select **Drop-In Mode**.
3. Click **Properties**.
4. Select the **DHCP Settings** tab.
5. From the drop-down list, select **Use DHCP Server**.
   The DHCP configuration settings appear.



6. To change the DHCP lease time, select a different option in the **Leasing Time** drop-down list.
7. To add an address pool from which your XTM device can give out IP addresses: in the **Starting IP** and **Ending IP** text boxes, type a range of IP addresses that are on the same subnet as the drop-in IP address. Click **Add**.
   Repeat this step to add more address pools.
   You can configure a maximum of six address pools.
8. To reserve a specific IP address from an address pool for a device or client, in the **Reserved Addresses** section:
   - Type a **Reservation Name** to identify the reservation.
   - Type the **Reserved IP** address you want to reserve.
   - Type the **MAC address** for the device.
   - Click **Add**.
     Repeat this step to add more DHCP reservations.
9. If necessary, *Add WINS and DNS Server Addresses*.
10. At the top of the page, click **Return**.
11. Click **Save**.

Use DHCP Relay

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.
2. Select any trusted or optional interface and click **Configure**.
   Or, double-click a trusted or optional interface.
   The Interface Configuration page appears.
3. Adjacent to the **IP Address** text box, select **Use DHCP Relay**.

4. Type the IP address of the DHCP server in the related field. Make sure to *Add a Static Route* to the DHCP server, if necessary.
5. Click **Save**. Click **Save** again.

Specify DHCP Settings for a Single Interface

You can specify different DHCP settings for each trusted or optional interface in your configuration. To modify these settings:

1. Scroll to the bottom of the **Network Configuration** dialog box.
2. Select an interface.
3. Click **Configure**.
4. To use the same DHCP settings that you configured for drop-in mode, select **Use System DHCP Setting**.

   To disable DHCP for clients on that network interface, select **Disable DHCP**.

   To configure different DHCP options for clients on a secondary network, select **Use DHCP Server for Secondary Network**.
5. To add IP address pools, set the default lease time, and manage DNS/WINS servers, complete Steps 3–6 of the *Use DHCP* section.
6. Click **OK**.

Bridge Mode

Bridge mode is a feature that allows you to install your XTM device between an existing network and its gateway to filter or manage network traffic. When you enable this feature, your XTM device processes and forwards all network traffic to other gateway devices. When the traffic arrives at a gateway from the XTM device, it appears to have been sent from the original device.

To use bridge mode, you must specify an IP address that is used to manage your XTM device. The device also uses this IP address to get Gateway AV/IPS updates and to route to internal DNS, NTP, or WebBlocker servers as necessary. Because of this, make sure you assign an IP address that is routable on the Internet.

In bridge mode, L2 and L3 headers are not changed. If you want traffic on the same physical interface of a XTM device to pass through the device, you cannot use bridge mode. In this case, you must use drop-in or mixed routing mode, and set the default gateway of those computers to be the XTM device itself.

When you use bridge mode, your XTM device cannot complete some functions that require the device to operate as a gateway. These functions include:

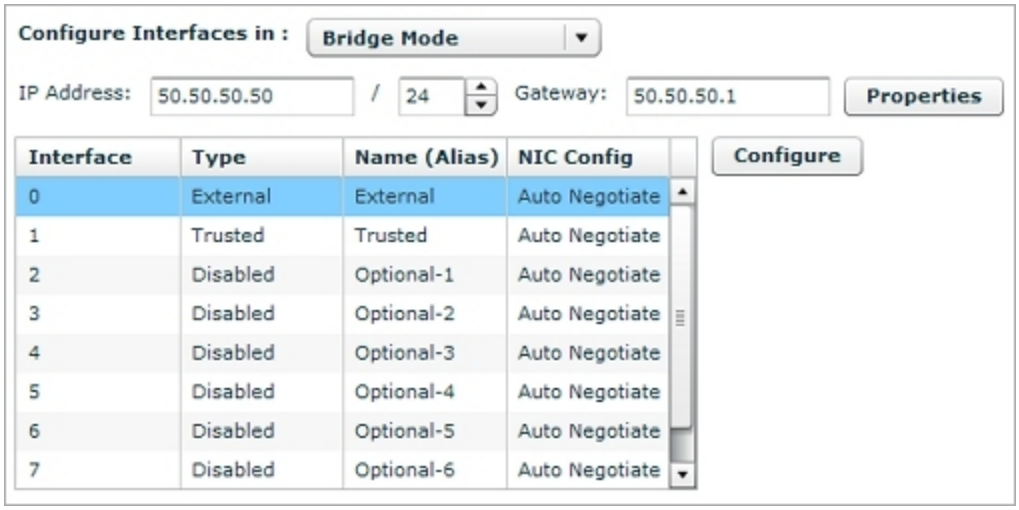
- Multi-WAN
- VLANs (Virtual Local Area Networks)
- Network bridges
- Static routes
- FireCluster
- Secondary networks
- DHCP server or DHCP relay
- Serial modem failover (XTM 2 Series only)
- 1-to-1, dynamic, or static NAT
- Dynamic routing (OSPF, BGP, or RIP)
- Any type of VPN for which the XTM device is an endpoint or gateway
- Some proxy functions, including HTTP Web Cache Server

If you have previously configured these features or services, they are disabled when you switch to bridge mode. To use these features or services again, you must use a different network mode. If you return to drop-in or mixed routing mode, you might have to configure some features again.

> ***Note*** *When you enable bridge mode, any interfaces with a previously configured network bridge or VLAN are disabled. To use those interfaces, you must first change to either drop-in or mixed routing mode, and configure the interface as External, Optional, or Trusted, then return to bridge mode. Wireless features on XTM wireless devices operate correctly in bridge mode.*

To enable bridge mode:

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.
2. From the **Configure Interfaces In** drop-down list, select **Bridge Mode**.



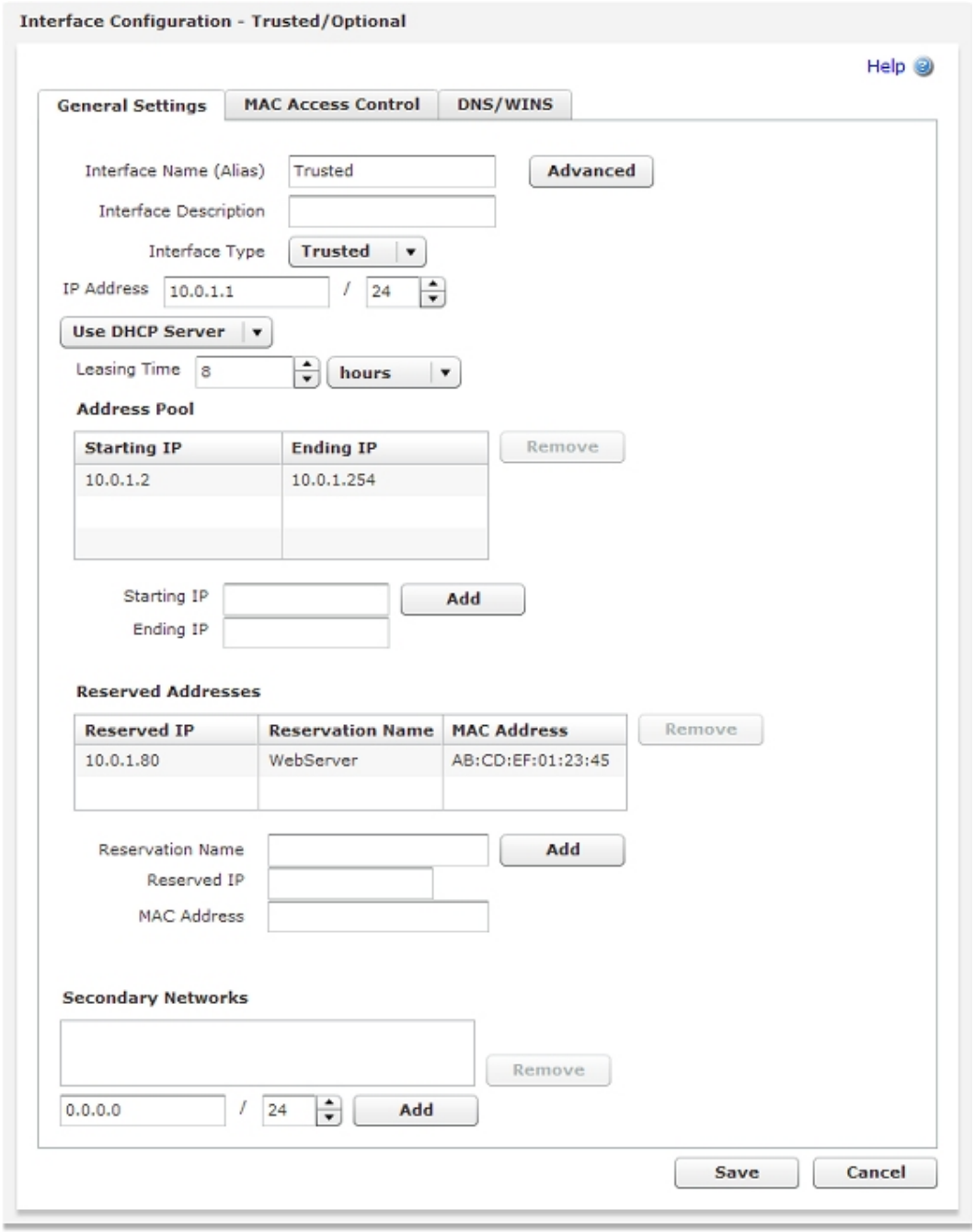
3. If you are prompted to disable interfaces, click **Yes** to disable the interfaces, or **No** to return to your previous configuration.
4. Type the **IP Address** of your XTM device in slash notation.
   For more information on slash notation, see *About Slash Notation* on page 3.
5. Type the **Gateway** IP address that receives all network traffic from the device.
6. Click **Save**.

Common Interface Settings

With mixed routing mode, you can configure your XTM device to send network traffic between a wide variety of physical and virtual network interfaces. This is the default network mode, and it offers the greatest amount of flexibility for different network configurations. However, you must configure each interface separately, and you may have to change network settings for each computer or client protected by your XTM device.

To configure your XTM device with mixed routing mode:

1. Select **Network > Interfaces**.
   The Network Interfaces dialog box appears.
2. Select the interface you want to configure, then click **Configure**. The options available depend on the type of interface you selected.
   The Interface Configuration dialog box appears.



3. In the **Interface Name (Alias)** text box, you can retain the default name or change it to one that more closely reflects your own network and its own trust relationships.
   Make sure the name is unique among interface names as well as all MVPN group names and tunnel names. You can use this alias with other features, such as proxy policies, to manage network traffic for this interface.
4. (Optional) Enter a description of the interface in the **Interface Description** text box.
5. In the **Interface Type** drop-down list, you can change the interface type from its default value. You can select **External**, **Trusted**, **Optional**, **Bridge**, **Disabled**, or **VLAN**. Some interface types have additional settings.

- For more information about how to assign an IP address to an external interface, see *Configure an External Interface* on page 84. To set the IP address of a trusted or optional interface, type the IP address in slash notation.
- To assign IP addresses automatically to clients on a trusted or optional interface, see *Configure DHCP in Mixed Routing Mode* on page 87 or *Configure DHCP Relay* on page 100.
- To use more than one IP address on a single physical network interface, see *Configure a Secondary Network* on page 102.
- For more information about VLAN configurations, see *About Virtual Local Area Networks (VLANs)* on page 111.
- To remove an interface from your configuration, see *Disable an Interface* on page 100.

6. Configure your interface as described in one of the above topics.
7. Click **Save**.

Disable an Interface

In the **Network Configuration** dialog box, the interface now appears as type **Disabled**.

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.
2. Select the interface you want to disable. Click **Configure**.
   The Interface Configuration page appears.
3. From the **Interface Type** drop-down list, select **Disabled**. Click **Save**.

In the Network Interfaces page, the interface now appears as type **Disabled**.

Configure DHCP Relay

One way to get IP addresses for the computers on the trusted or optional networks is to use a DHCP server on a different network. You can use DHCP relay to get IP addresses for the computers on the trusted or optional network. With this feature, the XTM device sends DHCP requests to a server on a different network.

If the DHCP server you want to use is not on a network protected by your XTM device, you must set up a VPN tunnel between your XTM device and the DHCP server for this feature to operate correctly.

> ***Note*** *You cannot use DHCP relay on any interface on which FireCluster is enabled.*

To configure DHCP relay:

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.
2. Select a trusted or an optional interface and click **Configure**.
3. In the drop-down list below the interface IP address, select **Use DHCP Relay**.
4. Type the IP address of the DHCP server in the related field. Make sure to *Add a Static Route* to the DHCP server, if necessary.
5. Click **Save**.

Restrict Network Traffic by MAC Address

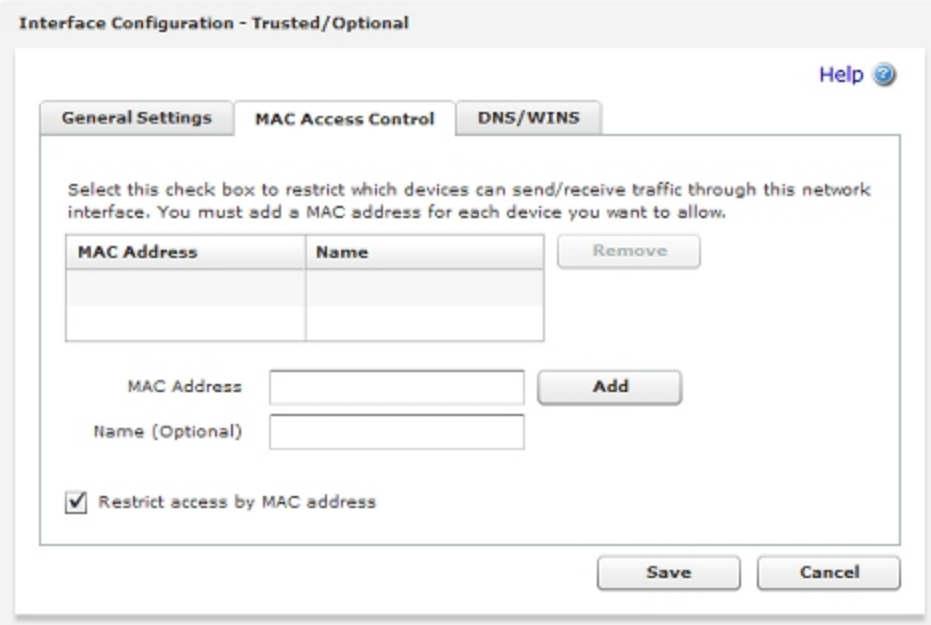
You can use a list of MAC addresses to manage which devices are allowed to send traffic on the network interface you specify. When you enable this feature, your XTM device checks the MAC address of each computer or device that connects to the specified interface. If the MAC address of that device is not on the MAC Access Control list for that interface, the device cannot send traffic.

This feature is especially helpful to prevent any unauthorized access to your network from a location within your office. However, you must update the MAC Address Control list for each interface when a new, authorized computer is added to the network.

> ***Note*** *If you choose to restrict access by MAC address, you must include the MAC address for the computer you use to administer your XTM device.*

To enable MAC Access Control for a network interface:

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.
2. Select the interface on which you want to enable MAC Access Control, then click **Configure**.
   The Interface Configuration page appears.
3. Select the **MAC Access Control** tab.



4. Select the **Restrict access by MAC address** check box.
5. Type the **MAC address** of the computer or device to give it access to the specified interface.
6. (Optional) Type a **Name** for the computer or device to identify it in the list.
7. Click **Add**.
   Repeat steps 5 - 7 to add more computers or devices to the MAC Access Control list.

Add WINS and DNS Server Addresses

Your XTM device shares Windows Internet Name Server (WINS) and Domain Name System (DNS) server IP addresses for some features. These features include DHCP and Mobile VPN. The WINS and DNS servers must be accessible from the XTM device trusted interface.

This information is used for two purposes:

- The XTM device uses the DNS server to resolve names to IP addresses for IPSec VPNs and for the spamBlocker, Gateway AV, and IPS features to operate correctly.
- The WINS and DNS entries are used by DHCP clients on the trusted or optional networks, and by Mobile VPN users to resolve DNS queries.

Make sure that you use only an internal WINS and DNS server for DHCP and Mobile VPN. This helps to make sure that you do not create policies that have configuration properties that prevent users from connecting to the DNS server.

1. Select **Network > Interfaces**.
2. Scroll to the **DNS Servers** and **WINS Servers** section.

3. In the **DNS Server** or **WINS Server** text box, type the primary and secondary addresses for each WINS and DNS servers.
4. Click **Add**.
5. Repeat Steps 3–4 to specify up to three DNS servers.
6. (Optional) In the **Domain Name** text box, type a domain name for a DHCP client to use with unqualified names such as *watchguard_mail*.

Configure a Secondary Network

A secondary network is a network that shares one of the same physical networks as one of the XTM device interfaces. When you add a secondary network, you make (or add) an IP alias to the interface. This IP alias is the default gateway for all the computers on the secondary network. The secondary network tells the XTM device that there is one more network on the XTM device interface.

For example, if you configure an XTM device in drop-in mode, you give each XTM device interface the same IP address. However, you probably use a different set of IP addresses on your trusted network. You can add this private network as a secondary network to the trusted interface of your XTM device. When you add a secondary network, you create a route from an IP address on the secondary network to the IP address of the XTM device interface.

If your XTM device is configured with a static IP address on an external interface, you can also add an IP address on the same subnet as your primary external interface as a secondary network. You can then configure static NAT for more than one of the same type of server. For example, configure an external secondary network with a second public IP address if you have two public SMTP servers and you want to configure a static NAT rule for each.

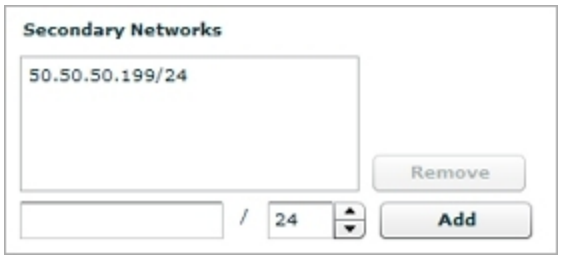
You can add up to 2048 secondary networks per XTM device interface. You can use secondary networks with either a drop-in or a routed network configuration. You can also add a secondary network to an external interface of an XTM device if that external interface is configured to get its IP address through PPPoE or DHCP.

To define a secondary IP address, you must have:

- An unused IP address on the secondary network to assign to the XTM device interface
- An unused IP address on the same network as the XTM device external interface

To define a secondary IP address:

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.
2. Select the interface for the secondary network and click **Configure**, or double-click an interface.
   The Interface Configuration page appears.
3. In the Secondary Networks section, type an unassigned host IP address in slash notation from the secondary network. Click **Add**. Repeat this step to add additional secondary networks.
4. Click **Save**.
5. Click **Save** again.



Note *Make sure to add secondary network addresses correctly. The XTM device does not tell you if the address is correct. We recommend that you do not create a subnet as a secondary network on one interface that is a component of a larger network on a different interface. If you do this, spoofing can occur and the network cannot operate correctly.*

About Advanced Interface Settings

You can use several advanced settings for XTM device interfaces:

Network Interface Card (NIC) Settings

Configures the speed and duplex parameters for XTM device interfaces to automatic or manual configuration. We recommend you keep the link speed configured for automatic negotiation. If you use the manual configuration option, you must make sure the device the XTM device connects to is also manually set to the same speed and duplex parameters as the XTM device. Use the manual configuration option only when you must override the automatic XTM device interface parameters to operate with other devices on your network.

Set Outgoing Interface Bandwidth

When you use Traffic Management settings to guarantee bandwidth to policies, this setting makes sure that you do not guarantee more bandwidth than actually exists for an interface. This setting also helps you make sure the sum of guaranteed bandwidth settings does not fill the link such that non-guaranteed traffic cannot pass.

Enable QoS Marking for an Interface

Creates different classifications of service for different kinds of network traffic. You can set the default marking behavior as traffic goes out of an interface. These settings can be overridden by settings defined for a policy.

Set DF Bit for IPSec

Determines the setting of the Don't Fragment (DF) bit for IPSec.

PMTU Setting for IPSec

(External interfaces only) Controls the length of time that the XTM device lowers the MTU for an IPSec VPN tunnel when it gets an ICMP Request to Fragment packet from a router with a lower MTU setting on the Internet.

Use Static MAC Address Binding

Uses computer hardware (MAC) addresses to control access to an XTM device interface.

Network Interface Card (NIC) Settings

1. Select **Network > Interfaces**.
2. Select the interface you want to configure. Click **Configure**.
3. Click **Advanced General Settings**.

4. In the **Link Speed** drop-down list, select **Auto Negotiate** if you want the XTM device to select the best network speed. You can also select one of the half-duplex or full-duplex speeds that you know is compatible with your other network equipment.

   Auto Negotiate is the default setting. We strongly recommend that you do not change this setting unless instructed to do so by Technical Support. If you set the link speed manually and other devices on your network do not support the speed you select, this can cause a conflict that does not allow your XTM device interface to reconnect after failover.

5. In the **Maximum Transmission Unit (MTU)** text box, select the maximum packet size, in bytes, that can be sent through the interface. We recommend that you use the default, 1500 bytes, unless your network equipment requires a different packet size.
   You can set the MTU from a minimum of 68 to a maximum of 9000.
6. To change the MAC address of the external interface, select the **Override MAC Address** check box and type the new MAC address.

   For more information about MAC addresses, see the subsequent section.

7. Click **Save**.
8. Click **Save** again.

About MAC Addresses

Some ISPs use a MAC address to identify the computers on their network. Each MAC address gets one static IP address. If your ISP uses this method to identify your computer, then you must change the MAC address of the XTM device external interface. Use the MAC address of the cable modem, DSL modem, or router that connected directly to the ISP in your original configuration.

The MAC address must have these properties:

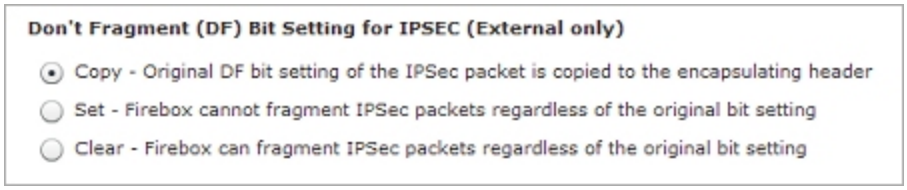
- The MAC address must use 12 hexadecimal characters. Hexadecimal characters have a value between 0 and 9 or between “a” and “f.”
- The MAC address must operate with:
  - One or more addresses on the external network.
  - The MAC address of the trusted network for the device.
  - The MAC address of the optional network for the device.
- The MAC address must not be set to 000000000000 or ffffffffffff.

If the **Override MAC Address** check box is not selected when the XTM device is restarted, the device uses the default MAC address for the external network.

To decrease problems with MAC addresses, the XTM device makes sure that the MAC address you assign to the external interface is unique on your network. If the XTM device finds a device that uses the same MAC address, the XTM device changes back to the standard MAC address for the external interface and starts again.

Set DF Bit for IPSec

When you configure the external interface, select one of the three options to determine the setting for the **Don't Fragment (DF) bit for IPSec** section.



Copy

Select **Copy** to apply the DF bit setting of the original frame to the IPSec encrypted packet. If a frame does not have the DF bits set, Fireware XTM does not set the DF bits and fragments the packet if needed. If a frame is set to not be fragmented, Fireware XTM encapsulates the entire frame and sets the DF bits of the encrypted packet to match the original frame.

Set

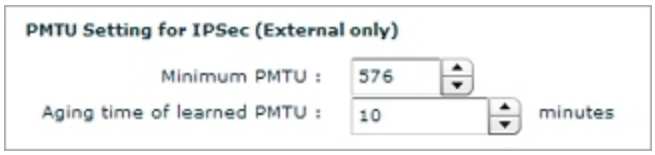
Select **Set** if you do not want your XTM device to fragment the frame regardless of the original bit setting. If a user must make IPSec connections to a XTM device from behind a different XTM device, you must clear this check box to enable the IPSec pass-through feature. For example, if mobile employees are at a customer location that has a XTM device, they can make IPSec connections to their network with IPSec. For your local XTM device to correctly allow the outgoing IPSec connection, you must also add an IPSec policy.

Clear

Select **Clear** to break the frame into pieces that can fit in an IPSec packet with the ESP or AH header, regardless of the original bit setting.

PMTU Setting for IPSec

This advanced interface setting applies to external interfaces only.



The Path Maximum Transmission Unit (PMTU) setting controls the length of time that the XTM device lowers the MTU for an IPSec VPN tunnel when it gets an ICMP Request to Fragment packet from a router with a lower MTU setting on the Internet.

We recommend that you keep the default setting. This can protect you from a router on the Internet with a very low MTU setting.

Use Static MAC Address Binding

You can control access to an interface on your XTM device by computer hardware (MAC) address. This feature can protect your network from ARP poisoning attacks, in which hackers try to change the MAC address of their computers to match a real device on your network. To use MAC address binding, you must associate an IP address on the specified interface with a MAC address. If this feature is enabled, computers with a specified MAC address can only send and receive information with the associated IP address.

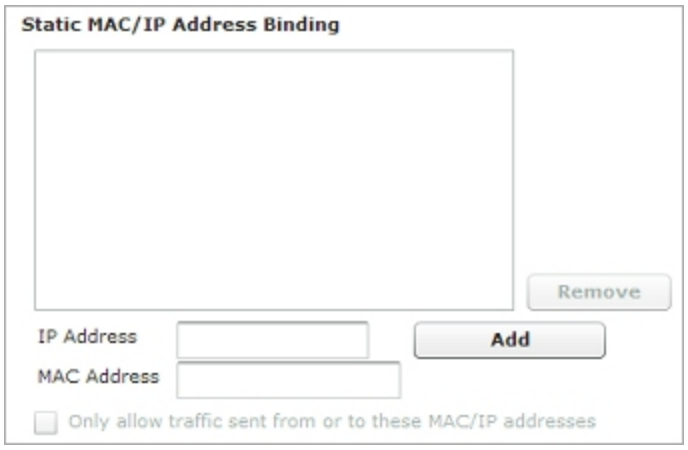
You can also use this feature to restrict all network traffic to devices that match the MAC and IP addresses on this list. This is similar to the MAC access control feature.

For more information, see *Restrict Network Traffic by MAC Address* on page 101.

> ***Note*** *If you choose to restrict network access by MAC address binding, make sure that you include the MAC address for the computer you use to administer your XTM device.*

To configure the static MAC address binding settings:

1. Select **Network > Interfaces**. Select an interface, then click **Configure**.
2. Click **Advanced**.



3. Type an IP address and MAC address pair. Click **Add**. Repeat this step to add additional pairs.
4. If you want this interface to pass only traffic that matches an entry in the **Static MAC/IP Address Binding** list, select the **Only allow traffic sent from or to these MAC/IP addresses** check box.

   If you do not want to block traffic that does not match an entry in the list, clear this check box.

Find the MAC Address of a Computer

A MAC address is also known as a hardware address or an Ethernet address. It is a unique identifier specific to the network card in the computer. A MAC address is usually shown in this form: XX-XX-XX-XX-XX-XX, where each X is a digit or letter from A to F. To find the MAC address of a computer on your network:

1. From the command line of the computer whose MAC address you want to find, type `ipconfig /all` (Windows) or `ifconfig` (OS X or Linux).
2. Look for the entry for the computer's "physical address." This value is the MAC or hardware address for the computer.

About LAN Bridges

A network bridge makes a connection between multiple physical network interfaces on your XTM device. A bridge can be used in the same ways as a normal physical network interface. For example, you can configure DHCP to give IP addresses to clients on a bridge, or use it as an alias in firewall policies.

To use a bridge, you must:

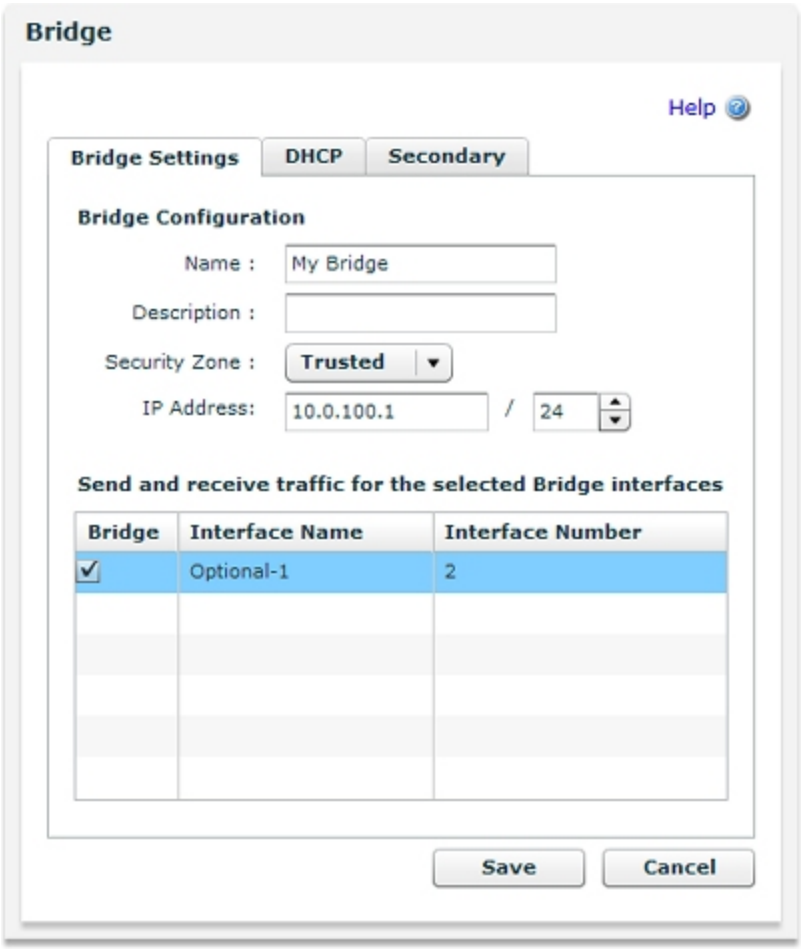
1. *Create a Network Bridge Configuration*.
2. *Assign a Network Interface to a Bridge*.

If you want to bridge all traffic between two interfaces, we recommend that you use bridge mode for your network configuration.

Create a Network Bridge Configuration

To use a bridge, you must create a bridge configuration and assign one or more network interfaces to the bridge.

1. Select **Network > Bridge**.
   The Bridge page appears.
2. Click **New**.



3. On the **Bridge Settings** tab, type a **Name** and **Description** (optional) for the bridge configuration.
4. Select a **Security Zone** from the drop-down list and type an **IP Address** in slash notation for the bridge.
   The bridge is added to the alias of the security zone you specify.
5. To add network interfaces, select the check box adjacent to each network interface you want to add to the bridge configuration.
6. To configure DHCP settings, select the **DHCP** tab. Select **DHCP Server** or **DHCP Relay** from the **DHCP Mode** drop-down list.
   For more information on DHCP configuration, see *Configure DHCP in Mixed Routing Mode* on page 87 or *Configure DHCP Relay* on page 100.
7. If you want to add secondary networks to the bridge configuration, select the **Secondary** tab.
   Type an IP address in slash notation and click **Add**.
   For more information on secondary networks, see *Configure a Secondary Network* on page 102.
8. Click **Save**.

Assign a Network Interface to a Bridge

To use a bridge, you must create a bridge configuration and assign it to one or more network interfaces. You can create the bridge configuration in the **Network Configuration** dialog box, or when you configure a network interface.

1. Select **Network > Bridge**.
   The Bridge page appears.
2. Select a bridge configuration in the **Bridge Settings** list, then click **Configure**.
3. Select the check box next to each network interface that you want to add to the bridge.
4. Click **Save**.

About Routing

A *route* is the sequence of devices through which network traffic is sent. Each device in this sequence, usually called a *router*, stores information about the networks it is connected to inside a *route table*. This information is used to forward the network traffic to the next router in the route.

Your XTM device automatically updates its route table when you change network interface settings, when a physical network connection fails, or when it is restarted. To update the route table at other times, you must use *dynamic routing* or add a *static route*. Static routes can improve performance, but if there is a change in the network structure or if a connection fails, network traffic cannot get to its destination. Dynamic routing ensures that your network traffic can reach its destination, but it is more difficult to set up.

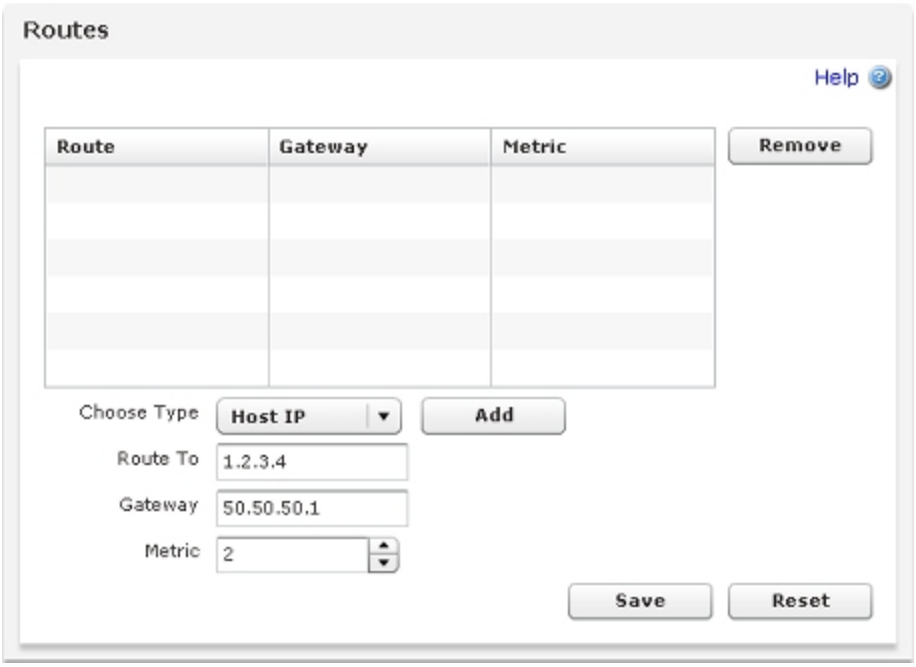
Add a Static Route

A *route* is the sequence of devices through which network traffic must go to get from its source to its destination. A *router* is the device in a route that finds the subsequent network point through which to send the network traffic to its destination. Each router is connected to a minimum of two networks. A packet can go through a number of network points with routers before it gets to its destination.

You can create *static routes* to send traffic to specific hosts or networks. The router can then send the traffic from the specified route to the correct destination. If you have a full network behind a router on your local network, add a network route. If you do not add a route to a remote network, all traffic to that network is sent to the XTM device default gateway.

Before you begin, you must understand the difference between a network route and a host route. A network route is a route to a full network behind a router located on your local network. Use a host route if there is only one host behind the router, or if you want traffic to go to only one host.

1. Select **Network > Routes**.
   The Routes page appears.



2. From the **Type** drop-down list, select **Host IP** or **Network IP**.
   - Select **Network IP** if you have a full network behind a router on your local network.
   - Select **Host IP** if only one host is behind the router, or if you want traffic to go to only one host.
3. In the **Route To** text box, type the destination IP address.
4. In the **Gateway** text box, type the local interface IP address of the router.
   The gateway IP address must be an IP address managed by your XTM device.
5. In the **Metric** text box, type or select a metric for the route. Routes with lower metrics have higher priority.
6. Click **Add**.
7. To add another static route, repeat Steps 2–4.
   To remove a static route, select the IP address in the list and click **Remove**.
8. Click **Save**.

About Virtual Local Area Networks (VLANs)

An 802.1Q VLAN (virtual local area network) is a collection of computers on a LAN or LANs that are grouped together in a single broadcast domain independent of their physical location. This enables you to group devices according to traffic patterns, instead of physical proximity. Members of a VLAN can share resources as if they were connected to the same LAN. You can also use VLANs to split a switch into multiple segments. For example, suppose your company has full-time employees and contract workers on the same LAN. You want to restrict the contract employees to a subset of the resources used by the full-time employees. You also want to use a more restrictive security policy for the contract workers. In this case, you split the interface into two VLANs.

VLANs enable you to divide your network into groups with a logical, hierarchical structure or grouping instead of a physical one. This helps free IT staff from the restrictions of their existing network design and cable infrastructure. VLANs make it easier to design, implement, and manage your network. Because VLANs are software-based, you can quickly and easily adapt your network to additions, relocations, and reorganizations.

VLANs use bridges and switches, so broadcasts are more efficient because they go only to people in the VLAN, not everyone on the wire. Consequently, traffic across your routers is reduced, which means a reduction in router latency. You can configure your XTM device to act as a DHCP server for devices on the VLAN, or use DHCP relay with a separate DHCP server.

You assign a VLAN to the Trusted, Optional, or External security zone. VLAN security zones correspond to aliases for interface security zones. For example, VLANs of type Trusted are handled by policies that use the alias Any-Trusted as a source or destination. VLANs of type External appear in the list of external interfaces when you configure policy-based routing.

VLAN Requirements and Restrictions

- The WatchGuard VLAN implementation does not support the spanning tree link management protocol.
- If your XTM device is configured to use drop-in network mode, you cannot use VLANs.
- A physical interface can be an untagged VLAN member of only one VLAN. For example, if External-1 is an untagged member of a VLAN named VLAN-1, it cannot be an untagged member of a different VLAN at the same time. Also, external interfaces can be a member of only one VLAN.
- Your multi-WAN configuration settings are applied to VLAN traffic. However, it can be easier to manage bandwidth when you use only physical interfaces in a multi-WAN configuration.
- Your device model and license controls the number of VLANs you can create.
  To see the number of VLANs you can add to your configuration, select **System Status > License**. Find the row labeled **Total number of VLAN interfaces**.
- We recommend that you do not create more than 10 VLANs that operate on external interfaces. Too many VLANs on external interfaces affect performance.
- All network segments you want to add to a VLAN must have IP addresses on the VLAN network.

> ***Note*** *If you define VLANs, you can ignore messages with the text "802.1d unknown version". These occur because the WatchGuard VLAN implementation does not support spanning tree link management protocol.*

About Tagging

To enable VLANs, you must deploy VLAN-capable switches in each site. The switch interfaces insert tags at layer 2 of the data frame that identify a network packet as part of a specified VLAN. These tags, which add an extra four bytes to the Ethernet header, identify the frame as belonging to a specific VLAN. Tagging is specified by the IEEE 802.1Q standard.

The VLAN definition includes disposition of tagged and untagged data frames. You must specify whether the VLAN receives tagged, untagged, or no data from each interface that is enabled. Your XTM device can insert tags for packets that are sent to a VLAN-capable switch. Your device can also remove tags from packets that are sent to a network segment that belongs to a VLAN that has no switch.

About VLAN ID Numbers

By default, each interface on most new, unconfigured switches belongs to VLAN number 1. Because this VLAN exists on every interface of most switches by default, the possibility exists that this VLAN can accidentally span the entire network, or at least very large portions of it.

We recommend you use a VLAN ID number that is not 1 for any VLAN that passes traffic to the XTM device.

Define a New VLAN

Before you create a new VLAN, make sure you understand the concepts about, and restrictions for VLANs, as described in *About Virtual Local Area Networks (VLANs)* on page 111.

Before you can create a VLAN configuration, you must also change at least one interface to be of type VLAN.

1. Select **Network > Interfaces**.
2. Select the interface that is connected to your VLAN switch. Click **Configure**.
3. From the **Interface Type** drop-down list, select **VLAN**.

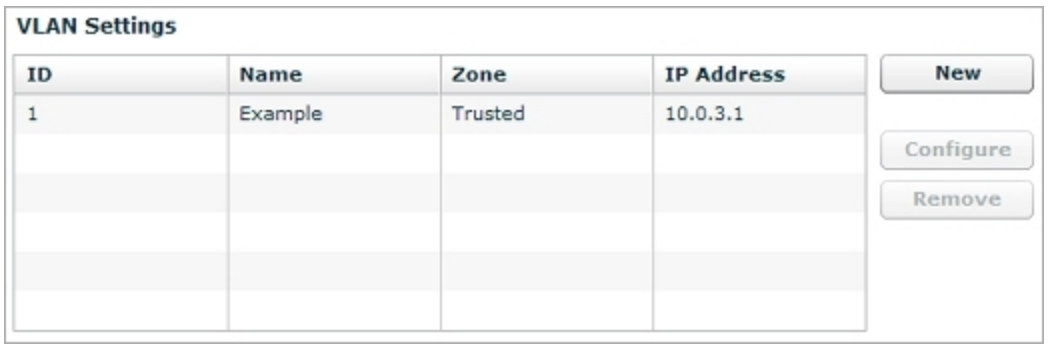
When you define a new VLAN, you add an entry in the **VLAN Settings** table. You can change the view of this table:

- Click a column header to sort the table based on the values in that column.
- The table can be sorted in descending or ascending order.
- The values in the Interface column show the physical interfaces that are members of this VLAN.
- The interface number in bold is the interface that sends untagged data to that VLAN.

To create a new VLAN:

1. Select **Network > VLAN**.
   The VLAN page appears.
2. A table of existing user-defined VLANs and their settings appears:

   You can also configure network interfaces from the **Interfaces** table.



3. Click **New**.
   The VLAN Settings page appears.

4. In the **Name** field, type a name for the VLAN. The name cannot contain spaces.
5. (Optional) In the **Description** field, type a description of the VLAN.
6. In the **VLAN ID** field, or type or select a value for the VLAN.
7. In the **Security Zone** field, select **Trusted**, **Optional**, or **External**.
   Security zones correspond to aliases for interface security zones. For example, VLANs of type *Trusted* are handled by policies that use the alias *Any-Trusted* as a source or destination.
8. In the **IP Address** field, type the address of the VLAN gateway.
   Note that any computer in this new VLAN must use this IP address as its default gateway.

Use DHCP on a VLAN

You can configure the XTM device as a DHCP server for the computers on your VLAN network.

1. On the **Network** tab, select **DHCP Server** from the **DHCP Mode** drop-down list to configure the XTM device as the DHCP server for your VLAN network. If necessary, type your domain name to supply it to the DHCP clients.
2. To add an IP address pool, type the first and last IP addresses in the pool. Click **Add**.
   You can configure a maximum of six address pools.
3. To reserve a specific IP address for a client, type the **IP address**, **reservation name**, and **MAC address** for the device. Click **Add**.

4. To change the default **lease time**, select a different time interval from the drop-down list at the top of the page.
   This is the time interval that a DHCP client can use an IP address that it receives from the DHCP server. When the lease time is about to expire, the client sends a request to the DHCP server to get a new lease.
5. To add DNS or WINS servers to your DHCP configuration, type the server address in the field adjacent to the list. Click **Add**.
6. To delete a server from the list, select the entry and click **Remove**.

Use DHCP Relay on a VLAN

1. On the **Network** tab, select **DHCP Relay** from the **DHCP Mode** drop-down list.
2. Type the IP address of the DHCP server. Make sure to add a route to the DHCP server, if necessary.

Before you can save this VLAN, you must *Assign Interfaces to a VLAN*.

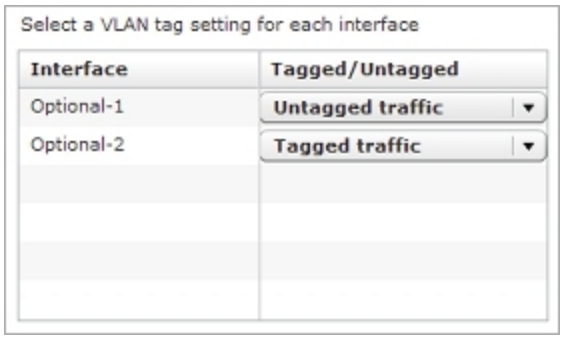
Assign Interfaces to a VLAN

When you create a new VLAN, you specify the type of data it receives from XTM device interfaces. However, you can also make an interface a member of a VLAN that is currently defined, or remove an interface from a VLAN.

> ***Note*** *You must change an interface type to VLAN before you can use it in a VLAN configuration.*

To assign a network interface to a VLAN:

1. Select **Network > VLAN**.
   The VLAN page appears.
2. Click **New**, or select a VLAN interface and click **Configure**.
3. In the **Select a VLAN tag setting for each interface** list, click the **Tagged/Untagged** column adjacent to an interface and select an option in the drop-down list:
   - **Tagged traffic** — The interface sends and receives tagged traffic.
   - **Untagged traffic** — The interface sends and receives untagged traffic.
   - **No traffic** — Remove the interface from this VLAN configuration.



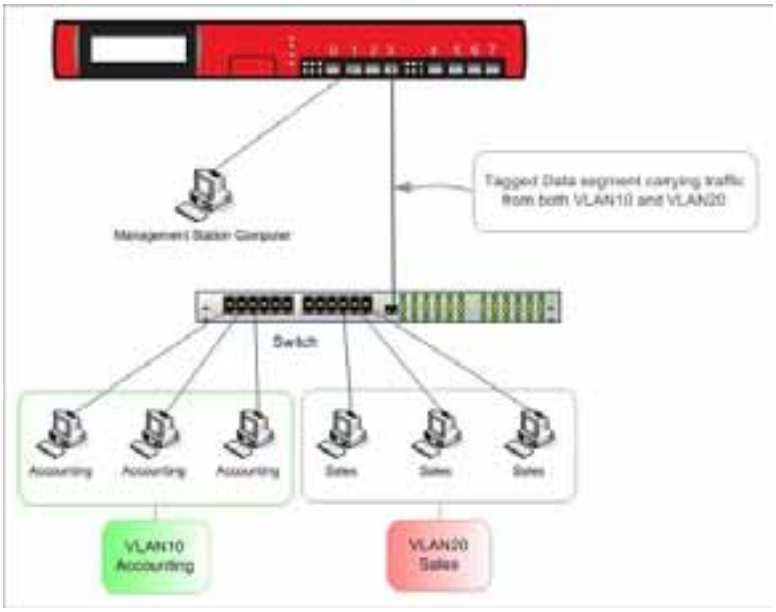
4. Click **Save**.

Network Setup Examples

Configure Two VLANs on the Same Interface

A network interface on a XTM device is a member of more than one VLAN when the switch that connects to that interface carries traffic from more than one VLAN. This example shows how to connect one switch that is configured for two different VLANs to a single interface on the XTM device.

The subsequent diagram shows the configuration for this example.



In this example, computers on both VLANs connect to the same 802.1Q switch, and the switch connects to interface 3 on the XTM device.

The subsequent instructions show you how to configure these VLANs:

Configure Interface 3 as a VLAN Interface

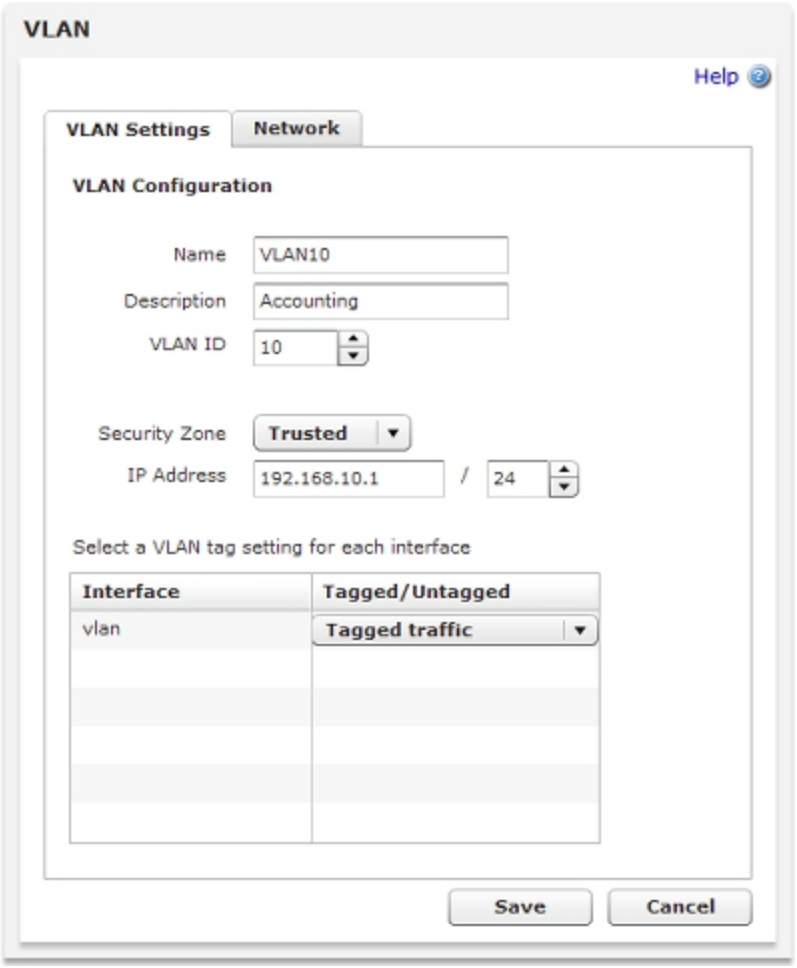
1. Select **Network > Interfaces**.
2. In the **Interface Name (Alias)** text box type **vlan**.
3. Select Interface number 3. Click **Configure**.

4. From the **Interface Type** drop-down list, select **VLAN**.
5. Click **Save**.

Define the two VLANs and Assign Them to the VLAN Interface

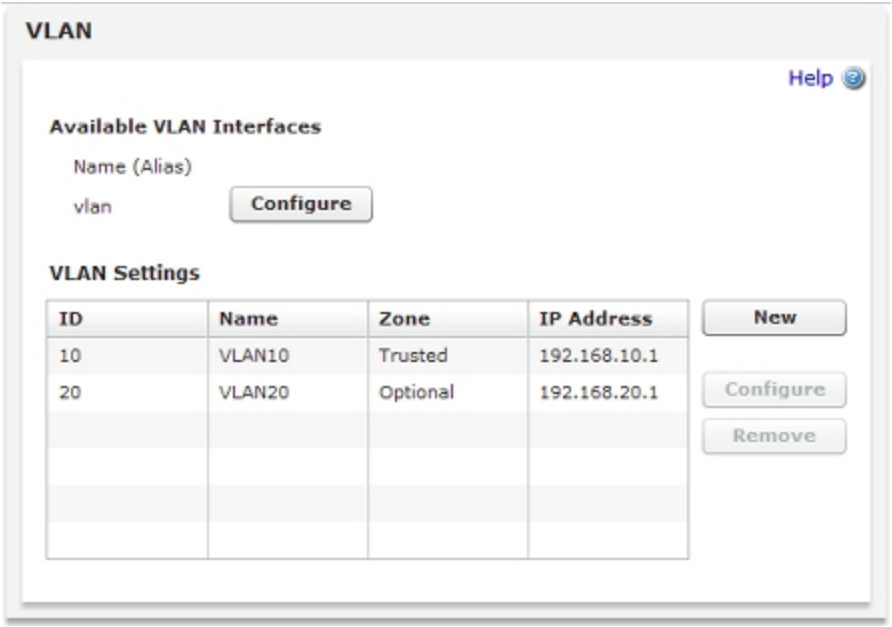
1. Select **Network > VLAN**.
2. Click **New**.

3. In the **Name (Alias)** text box, type a name for the VLAN. For this example, type `VLAN10`.
4. In the **Description** text box, type a description. For this example, type `Accounting`.
5. In the **VLAN ID** text box, type the VLAN number configured for the VLAN on the switch. For this example, type `10`.
6. From the **Security Zone** drop-down list, select the security zone. For this example, select **Trusted**.
7. In the **IP Address** text box, type the IP address to use for the XTM device on this VLAN. For this example, type `192.168.10.1/24`.
8. In the **Select a VLAN tag setting for each interface** list, click the **Tagged/Untagged** column adjacent to an interface and select **Tagged traffic** in the drop-down list.



9. Click **Save**.
10. Click **New** to add the second VLAN.
11. In the **Name (Alias)** text box, type `VLAN20`.
12. In the **Description** text box, type `Sales`.
13. In the **VLAN ID** text box, type `20`.
14. From the **Security Zone** drop-down list, select **Optional**.
15. In the **IP Address** field, type the IP address to use for the XTM device on this VLAN. For this example, type `192.168.20.1/24`.

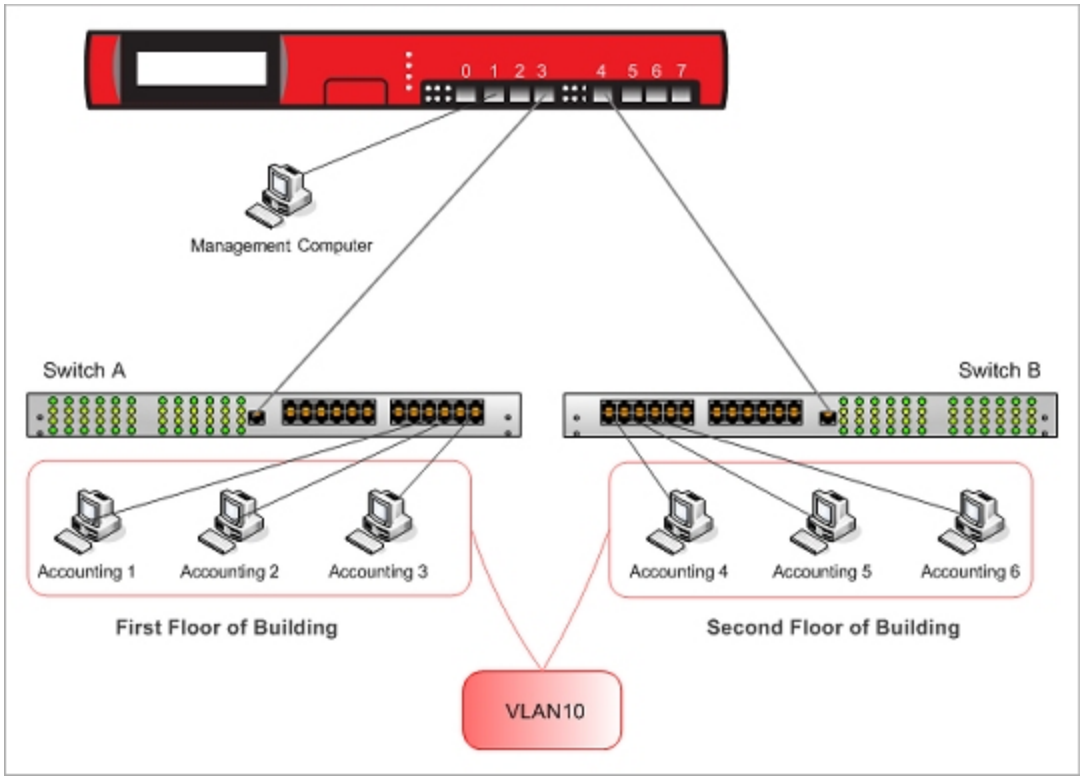
16. In the **Select a VLAN tag setting for each interface** list, click the **Tagged/Untagged** column adjacent to an interface and select **Tagged** in the drop-down list.
17. Click **Save**.
18. Both VLANS now appear in the list, and are configured to use the defined VLAN interface.



Configure One VLAN Bridged Across Two Interfaces

You can configure a VLAN to bridge across two interfaces of the XTM device. You might want to bridge one VLAN across two interfaces if your organization is spread across multiple locations. For example, suppose your network is on the first and second floors in the same building. Some of the computers on the first floor are in the same functional group as some of the computers on the second floor. You want to group these computers into one broadcast domain so that they can easily share resources, such as a dedicated file server for their LAN, host-based shared files, printers, and other network accessories.

This example shows how to connect two 802.1Q switches so that both switches can send traffic from the same VLAN to two interfaces on the same XTM device.

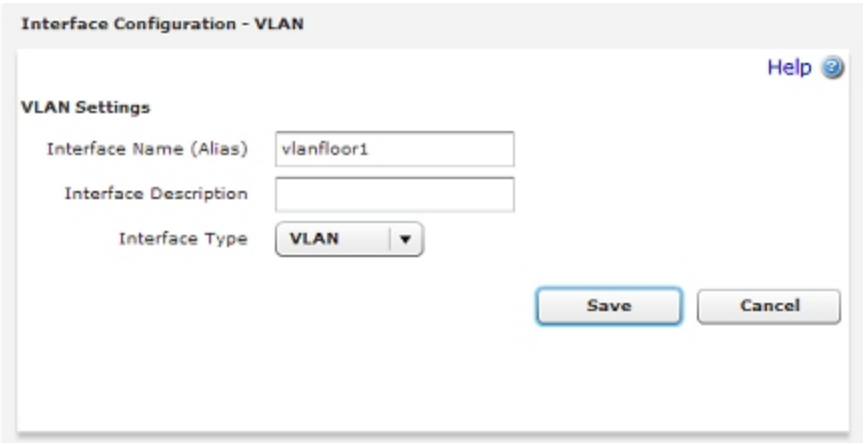


In this example, two 802.1Q switches are connected to XTM device interfaces 3 and 4, and carry traffic from the same VLAN.

> ***Note*** *Any computer in this new VLAN must use this IP address as its default gateway.*

Configure Interfaces 3 and 4 as VLAN Interfaces

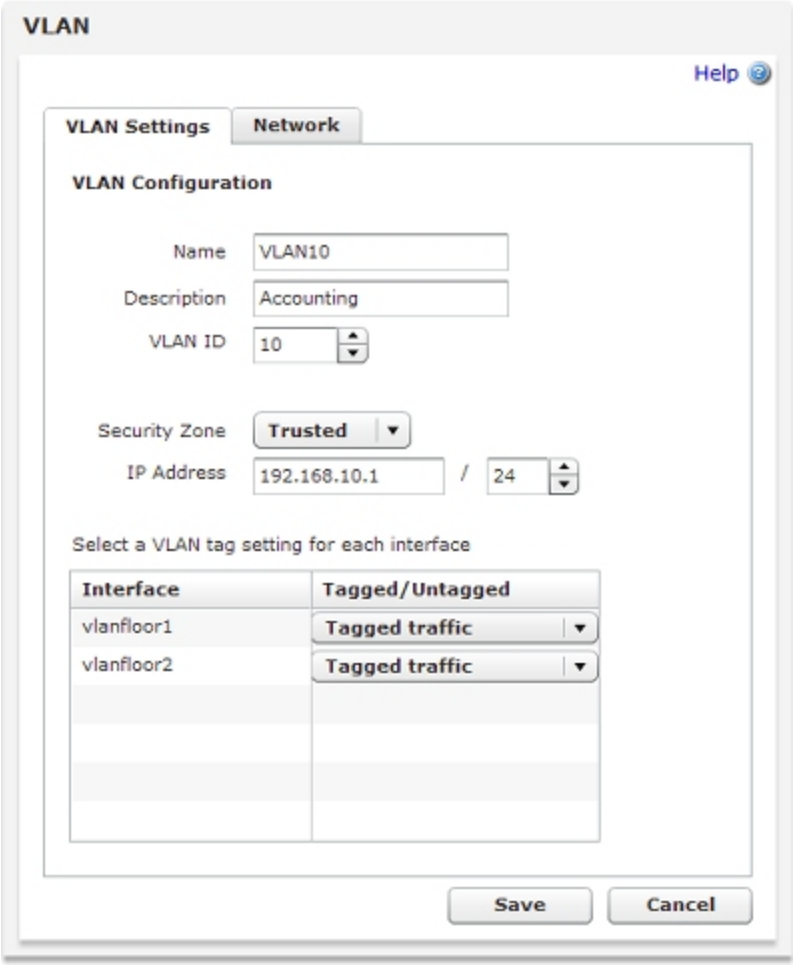
1. Select **Network > Interfaces**.
2. In the **Interface Name (Alias)** text box, type a name. For this example, type**vlanfloor1**.
3. Select Interface number 3. Click **Configure**.



4. From the **Interface Type** drop-down list, select **VLAN**.
5. Click **Save**.
6. Repeat the same steps to configure Interface 4 as a VLAN interface.

Configure the VLAN

1. Select **Network > VLAN**.
2. Click **New**.
3. In the **Name (Alias)** text box, type a name for the VLAN. For this example, type `VLAN10`.
4. In the **Description** text box, type a description. For this example, type `Accounting`.
5. In the **VLAN ID** text box, type the VLAN number configured for the VLAN on the switch. For this example, type `10`.
6. From the **Security Zone** drop-down list, select the security zone. For this example, select **Trusted**.
7. In the **IP Address** text box, type the IP address to use for the XTM device on this VLAN. For this example, type `192.168.10.1/24`.
8. In the **Select a VLAN tag setting for each interface** list, click the **Tagged/Untagged** column adjacent to each interface and select **Tagged traffic** from the drop-down list.



9. Click **Save**.

Configure the Switches

Configure each of the switches that connect to interfaces 3 and 4 of the XTM device. Refer to the instructions from your switch manufacturer for details about how to configure your switches.

Configure the Switch Interfaces Connected to the XTM Device

The physical segment between the switch interface and the XTM device interface is a tagged data segment. Traffic that flows over this segment must use 802.1Q VLAN tagging.

> ***Note*** *Some switch manufacturers refer to an interface configured in this way as a trunk port or a trunk interface.*

On each switch, for the switch interface that connects to the XTM device:

- Disable Spanning Tree Protocol.
- Configure the interface to be a member of VLAN10.
- Configure the interface to send traffic with the VLAN10 tag.
- If necessary for your switch, set the switch mode to trunk.
- If necessary for your switch, set the encapsulation mode to 802.1Q.

Configure the Other Switch Interfaces

The physical segments between each of the other switch interfaces and the computers (or other networked devices) that connect to them are untagged data segments. Traffic that flows over these segments does not have VLAN tags.

On each switch, for the switch interfaces that connect computers to the switch:

- Configure these switch interfaces to be members of VLAN10.
- Configure these switch interfaces to send untagged traffic for VLAN10.

Physically Connect All Devices

1. Use an Ethernet cable to connect XTM device interface 3 to the Switch A interface that you configured to tag for VLAN10 (the VLAN trunk interface of Switch A).
2. Use an Ethernet cable to connect the XTM device interface 4 to the Switch B interface that you configured to tag for VLAN10 (the VLAN trunk interface of Switch B).
3. Connect a computer to the interface on Switch A that you configured to send untagged traffic for VLAN10.
4. Configure the network settings on the connected computer. The settings depend on whether you configured the XTM device to act as a DHCP server for the computers on VLAN10 in Step 9 of **Define the VLAN on the XTM Device**.
    - If you configured the XTM device to act as a DHCP server for the computers on VLAN10, configure the computer to use DHCP to get an IP address automatically. See Step 9 in the procedure **Define the VLAN**, above.

- If you did not configure the XTM device to act as a DHCP server for the computers on VLAN10, configure the computer with an IP address in the VLAN subnet 192.168.10.x. Use subnet mask 255.255.255.0 and set the default gateway on the computer to the XTM device VLAN IP address 192.168.10.1

5. Repeat the previous two steps to connect a computer to Switch B.

Test the Connection

After you complete these steps, the computers connected to Switch A and Switch B can communicate as if they were connected to the same physical local area network. To test this connection you can:

- Ping from a computer connected to Switch A to a computer connected to Switch B.
- Ping from a computer connected to Switch B to a computer connected to Switch A.

Use Your XTM Device with the 3G Extend Wireless Bridge

The WatchGuard 3G Extend wireless bridge adds 3G cellular connectivity to your WatchGuard XTM 2 Series device. When you connect the external interface of your XTM device to the 3G Extend wireless bridge, computers on your network can connect wirelessly to the Internet via the 3G cellular network.

The 3G Extend has two models based on technology from Top Global and Cradlepoint.

To connect your XTM device to the 3G cellular network you need:

- An XTM 2 Series device
- A 3G Extend wireless bridge
- A 3G wireless broadband data card

Use the 3G Extend/Top Global MB5000K Device

Follow these steps to use the 3G Extend wireless bridge with your XTM 2 Series device.

1. Configure the external interface on your XTM device to get its address with PPPoE. Make sure to set the PPPoE user name / password to public/public. To learn more about how to configure your external interface for PPPoE, see *Configure an External Interface* on page 84.
2. Activate your broadband data card. See the instructions included with your broadband data card for more information.
3. Prepare your 3G Extend wireless bridge:
   - Insert the broadband data card into the slot on the 3G Extend wireless bridge
   - Plug in the power to the 3G Extend wireless bridge
   - Verify the LED lights are active
4. Use an Ethernet cable to connect the 3G Extend wireless bridge to the external interface of your XTM device.

It is not necessary to change any settings on the 3G Extend device before you connect it to your XTM device. There are some times when it is necessary to connect to the web management interface of the 3G Extend device. To connect to the 3G Extend web interface, connect your computer directly to the MB5000K with an Ethernet cable and make sure your computer is configured to get its IP address with DHCP. Open your web browser and type `http://172.16.0.1`. Connect with a user name/password of public/public.

- To operate correctly with your XTM device, the 3G Extend wireless bridge must be configured to run in "Auto Connect" mode. All 3G Extend/MB5000K devices are pre-configured to run in this mode by default. To verify if your 3G Extend device is configured in Auto Connect mode, connect directly to the device and select **Interfaces > Internet access**. Select the **WAN#0** interface. In the **Networking** section, make sure the **Connect** mode drop-down list is set to **Auto**.
- If your 3G wireless card runs on the GPRS cellular network, it may be necessary to add a network login and password to our 3G Extend device configuration. To add a network login and password, connect to the 3G Extend wireless bridge and select **Services > Manageable Bridge**.
- To reset the MB5000K to its factory default settings, connect to the 3G Extend wireless bridge and select **System > Factory defaults**. Click **Yes**.

For security, we recommend that you change the default PPPoE user name/password from public/public after your network is up and running. You must change the user name and password on both your XTM device and your 3G Extend Wireless Bridge.

- To change the PPPoE user name and password on your XTM device, see *Configure an External Interface* on page 84.
- To change the PPPoE user name and password on the 3G Extend device, connect to the device and go to **Services > Manageable Bridge**.

The 3G Extend device supports more than 50 modem cards and ISP plan options. For detailed information about the Top Global product, including the MB5000 User Guide, go to http://www.topglobaluse.com/support_mb5000.htm.

Use the 3G Extend/Cradlepoint CBA250 Device

Follow these steps to use the 3G Extend Cradlepoint cellular broadband adapter with your WatchGuard XTM 2 Series device.

1. Follow the instructions in the Cradlepoint CBA250 Quick Start Guide to set up the Cradlepoint device and update the device firmware. If you have a newer modem that is not supported by the firmware version that ships on the device, you must use different steps to upgrade your firmware to the latest version:
   - Download the latest firmware for the CBA250 to your computer from the Cradlepoint support site at http://www.cradlepoint.com/support/cba250.
   - Use these instructions to update your firmware: Updating the Firmware on your Cradlepoint Router.
2. Configure the external interface on your XTM device to get its address with DHCP. To learn how to configure your external interface for PPPoE, see *Configure an External Interface* on page 84.
3. Use an Ethernet cable to connect the Cradlepoint device to the external interface of the XTM device.
4. Start (or restart) the XTM device.
   When the XTM device starts, it gets a DHCP address from the Cradlepoint device. After an IP address is assigned, the XTM device can connect to the Internet via the cellular broadband network.

The Cradlepoint supports a large number of USB or ExpressCard broadband wireless devices. For a list of supported devices, see http://www.cradlepoint.com/support./cba250.

7 Multi-WAN

About Using Multiple External Interfaces

You can use your XTM device to create redundant support for the external interface. This is a helpful option if you must have a constant Internet connection.

With the multi-WAN feature, you can configure up to four external interfaces, each on a different subnet. This allows you to connect your XTM device to more than one Internet Service Provider (ISP). When you configure a second interface, the multi-WAN feature is automatically enabled.

Multi-WAN Requirements and Conditions

You must have a second Internet connection and more than one external interface to use most multi-WAN configuration options.

Conditions and requirements for multi-WAN use include:

- If you have a policy configured with an individual external interface alias in its configuration, you must change the configuration to use the alias *Any-External*, or another alias you configure for external interfaces. If you do not do this, some traffic could be denied by your firewall policies.
- Multi-WAN settings do not apply to incoming traffic. When you configure a policy for inbound traffic, you can ignore all multi-WAN settings.
- To override the multi-WAN configuration in any individual policy, enable policy-based routing for that policy. For more information on policy-based routing, see *Configure Policy-Based Routing* on page 309.
- Map your company's Fully Qualified Domain Name to the external interface IP address of the lowest order. If you add a multi-WAN XTM device to your Management Server configuration, you must use the lowest-ordered external interface to identify it when you add the device.
- To use multi-WAN, you must use mixed routing mode for your network configuration. This feature does not operate in drop-in or bridge mode network configurations.
- To use the Interface Overflow method, you must have Fireware XTM with a Pro upgrade. You must also have a Fireware XTM Pro license if you use the Round-robin method and configure different weights for the XTM device external interfaces.

You can use one of four multi-WAN configuration options to manage your network traffic.

For configuration details and setup procedures, see the section for each option.

Multi-WAN and DNS

Make sure that your DNS server can be reached through every WAN. Otherwise, you must modify your DNS policies such that:

- The **From** list includes **Firebox**.
- The **Use policy-based routing** check box is selected.
  If only one WAN can reach the DNS server, select that interface in the adjacent drop-down list.
  If more than one WAN can reach the DNS server, select any one of them, select **Failover**, select **Configure**, and select all the interfaces that can reach the DNS server. The order does not matter.

> ***Note*** *You must have Fireware XTM with a Pro upgrade to use policy-based routing.*

About Multi-WAN Options

When you configure multiple external interfaces, you have several options to control which interface an outgoing packet uses. Some of these features require that you have Fireware XTM with a Pro upgrade.

Round-Robin Order

When you configure multi-WAN with the Round-robin method, the XTM device looks at its internal routing table to check for specific static or dynamic routing information for each connection. If no specified route is found, the XTM device distributes the traffic load among its external interfaces. The XTM device uses the average of sent (TX) and received (RX) traffic to balance the traffic load across all external interfaces you specify in your round-robin configuration.

If you have Fireware XTM with a Pro upgrade, you can assign a weight to each interface used in your round-robin configuration. By default and for all Fireware XTM users, each interface has a weight of 1. The weight refers to the proportion of load that the XTM device sends through an interface. If you have Fireware XTM Pro and you assign a weight of 2 to an interface, you double the portion of traffic that will go through that interface compared to an interface with a weight of 1.

As an example, if you have three external interfaces with 6M, 1.5M, and .075M bandwidth and want to balance traffic across all three interfaces, you would use 8, 2, and 1 as the weights for the three interfaces. Fireware will try to distribute connections so that 8/11, 2/11, and 1/11 of the total traffic flows through each of the three interfaces.

For more information, see *Configure Round-Robin* on page 129.

Failover

When you use the failover method to route traffic through the XTM device external interfaces, you select one external interface to be the primary external interface. Other external interfaces are backup interfaces, and you set the order for the XTM device to use the backup interfaces. The XTM device monitors the primary external interface. If it goes down, the XTM device sends all traffic to the next external

interface in its configuration. While the XTM device sends all traffic to the backup interface, it continues to monitor the primary external interface. When the primary interface is active again, the XTM device immediately starts to send all new connections through the primary external interface again.

You control the action for the XTM device to take for existing connections; these connections can failback immediately, or continue to use the backup interface until the connection is complete. Multi-WAN failover and FireCluster are configured separately. Multi-WAN failover caused by a failed connection to a link monitor host does not trigger FireCluster failover. FireCluster failover occurs only when the physical interface is down or does not respond. FireCluster failover takes precedence over multi-WAN failover.

For more information, see *Configure Failover* on page 130.

Interface Overflow

When you use the Interface Overflow multi-WAN configuration method, you select the order you want the XTM device to send traffic through external interfaces and configure each interface with a bandwidth threshold value. The XTM device starts to send traffic through the first external interface in its Interface Overflow configuration list. When the traffic through that interface reaches the bandwidth threshold you have set for that interface, the XTM device starts to send traffic to the next external interface you have configured in your Interface Overflow configuration list.

This multi-WAN configuration method allows the amount of traffic sent over each WAN interface to be restricted to a specified bandwidth limit. To determine bandwidth, the XTM device examines the amount of sent (TX) and received (RX) packets and uses the higher number. When you configure the interface bandwidth threshold for each interface, you must consider the needs of your network for this interface and set the threshold value based on these needs. For example, if your ISP is asymmetrical and you set your bandwidth threshold based on a large TX rate, interface overflow will not be triggered by a high RX rate.

If all WAN interfaces have reached their bandwidth limit, the XTM device uses the ECMP (Equal Cost MultiPath Protocol) routing algorithm to find the best path.

> ***Note*** *You must have Fireware XTM with a Pro upgrade to use this multi-WAN routing method.*

For more information, see *Configure Interface Overflow* on page 132.

Routing Table

When you select the Routing Table option for your multi-WAN configuration, the XTM device uses the routes in its internal route table or routes it gets from dynamic routing processes to send packets through the correct external interface. To see whether a specific route exists for a packet's destination, the XTM device examines its route table from the top to the bottom of the list of routes. You can see the list of routes in the route table on the **Status** tab of Firebox System Manager. The Routing Table option is the default multi-WAN option.

If the XTM device does not find a specified route, it selects the route to use based on source and destination IP hash values of the packet, using the ECMP (Equal Cost Multipath Protocol) algorithm specified in: http://www.ietf.org/rfc/rfc2992.txt

With ECMP, the XTM device uses an algorithm to decide which next-hop (path) to use to send each packet. This algorithm does not consider current traffic load.

For more information, see *When to Use Multi-WAN Methods and Routing* on page 134.

Serial Modem (XTM 2 Series only)

If your organization has a dial-up account with an ISP, you can connect an external modem to the USB port on your XTM 2 Series and use that connection for failover when all other external interfaces are inactive.

For more information, see *Serial Modem Failover* on page 135.

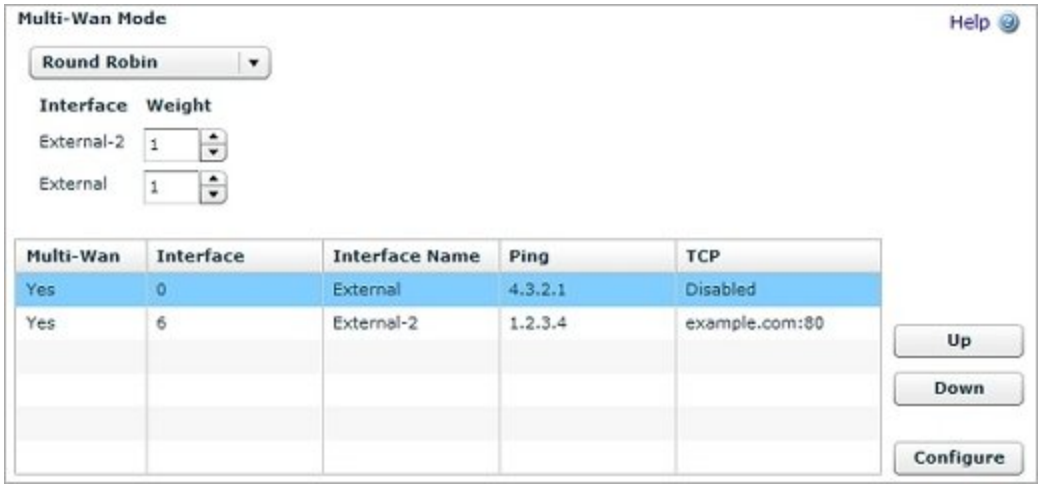
Configure Round-Robin

Before You Begin

- To use the multi-WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in *Configure an External Interface* on page 84.
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in *About Using Multiple External Interfaces* on page 125 and *About Multi-WAN Options* on page 126.

Configure the Interfaces

1. Select **Network > Multi-WAN**.
2. From the **Multi-WAN Mode** drop-down list, select **Round Robin**.



3. If you have Fireware XTM with a Pro upgrade, you can modify the weight associated with each interface. Choose an interface, then type or select a new value in the adjacent **Weight** field. The default value is 1 for each interface.

   For information on interface weight, see *Find How to Assign Weights to Interfaces* on page 129.

4. To assign an interface to the multi-WAN configuration, select an interface and click **Configure**.
5. Select the **Participate in Multi-WAN** check box and click **OK**.
6. To complete your configuration, you must add link monitor information as described in *About WAN Interface Status* on page 140.
7. Click **Save**.

Find How to Assign Weights to Interfaces

If you use Fireware XTM with a Pro upgrade, you can assign a weight to each interface used in your round-robin multi-WAN configuration. By default, each interface has a weight of 1. The weight refers to the proportion of load that the XTM device sends through an interface.

You can use only whole numbers for the interface weights; no fractions or decimals are allowed. For optimal load balancing, you might have to do a calculation to know the whole-number weight to assign for each interface. Use a common multiplier so that the relative proportion of the bandwidth given by each external connection is resolved to whole numbers.

For example, suppose you have three Internet connections. One ISP gives you 6 Mbps, another ISP gives you 1.5 Mbps, and a third gives you 768 Kbps. Convert the proportion to whole numbers:

- First convert the 768 Kbps to approximately .75 Mbps so that you use the same unit of measurement for all three lines. Your three lines are rated at 6, 1.5, and .75 Mbps.
- Multiply each value by 100 to remove the decimals. Proportionally, these are equivalent: [6 : 1.5 : .75] is the same ratio as [600 : 150 : 75]
- Find the greatest common divisor of the three numbers. In this case, 75 is the largest number that evenly divides all three numbers 600, 150, and 75.
- Divide each of the numbers by the greatest common divisor.

The results are 8, 2, and 1. You could use these numbers as weights in a round-robin multi-WAN configuration.

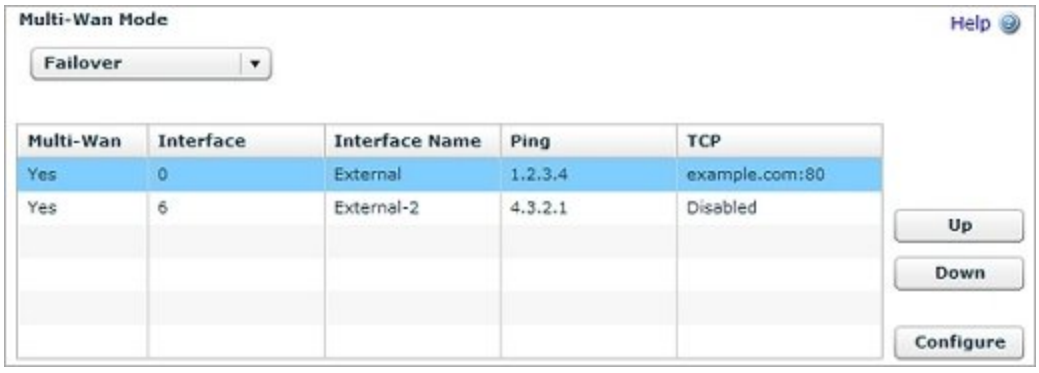
Configure Failover

Before You Begin

- To use the multi-WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in *Configure an External Interface* on page 84.
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in *About Using Multiple External Interfaces* on page 125 and *About Multi-WAN Options* on page 126.

Configure the Interfaces

1. Select **Network > Multi-WAN**.
2. In the **Multi-WAN Mode** drop-down list, select **Failover**.



3. Select an interface in the list and click **Up** or **Down** to set the order for failover. The first interface in the list is the primary interface.
4. To complete your configuration, you must add link monitor information as described in *About WAN Interface Status* on page 140.

For information on advanced multi-WAN configuration options, see *About Advanced Multi-WAN Settings* on page 139.

5. Click **Save**.

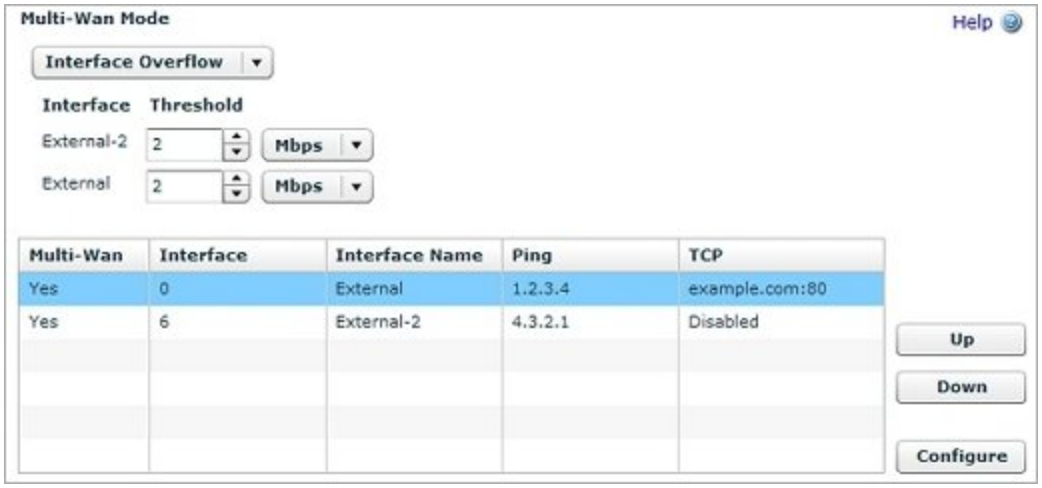
Configure Interface Overflow

Before You Begin

- To use the multiple WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in *Configure an External Interface* on page 84.
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in *About Using Multiple External Interfaces* on page 125 and *About Multi-WAN Options* on page 126.

Configure the Interfaces

1. Select **Network > Multi-WAN**.
2. From the **Multi-WAN Mode** drop-down list, select **Interface Overflow**.



3. In the **Threshold** field for each interface, type or select the amount of network traffic in megabits per second (Mbps) that the interface must carry before traffic is sent on other interfaces.
4. To set the order of interface operation, select an interface in the table and click **Up** and **Down** to change the order. The interfaces are used from first to last in the list.
5. To complete your configuration, you must add information as described in *About WAN Interface Status* on page 140.

For information on advanced multi-WAN configuration options, see About advanced multi-WAN settings.

Configure Routing Table

Before You Begin

- To use the multi-WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in *Configure an External Interface* on page 84.
- You must decide whether the Routing Table method is the correct multi-WAN method for your needs. For more information, see *When to Use Multi-WAN Methods and Routing* on page 134

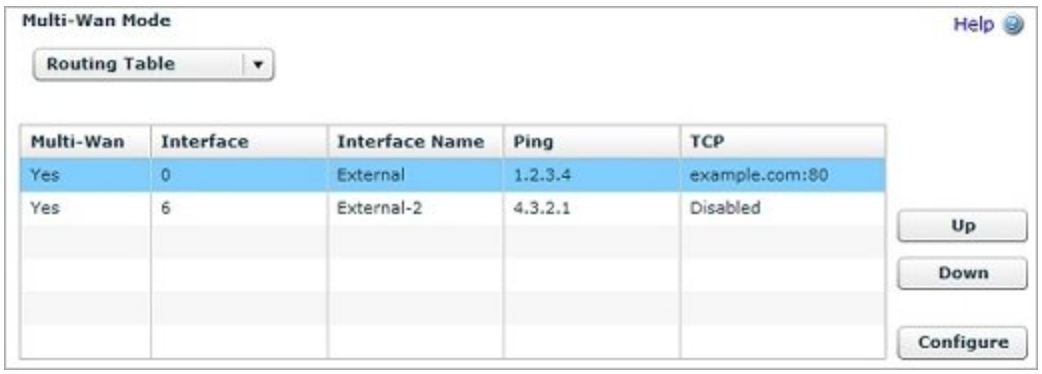
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in *About Using Multiple External Interfaces* on page 125 and *About Multi-WAN Options* on page 126.

Routing Table mode and load balancing

It is important to note that the Routing Table option does not do load balancing on connections to the Internet. The XTM device reads its internal route table from top to bottom. Static and dynamic routes that specify a destination appear at the top of the route table and take precedence over default routes. (A default route is a route with destination 0.0.0.0/0.) If there is no specific dynamic or static entry in the route table for a destination, the traffic to that destination is routed among the external interfaces of the XTM device through the use of ECMP algorithms. This may or may not result in even distribution of packets among multiple external interfaces.

Configure the Interfaces

1. Select **Network > Multi-WAN**.
2. In the **Multi-WAN Mode** drop-down list, select **Routing Table**.



3. To add interfaces to the multi-WAN configuration, select an interface and click **Configure**.
4. Select the **Participate in Multi-WAN** check box. Click **OK**.
5. To complete your configuration, you must add link monitor information as described in *About WAN Interface Status* on page 140.

For information on advanced multi-WAN configuration options, see Advanced Multi-WAN Settings.

About the XTM Device Route Table

When you select the Routing Table configuration option, it is a good idea to know how to look at the routing table that is on your XTM device.

From Fireware XTM Web UI:

Select **System Status > Routes**.
This shows the internal route table on your XTM device.

Routes in the internal route table on the XTM device include:

- The routes the XTM device learns from dynamic routing processes running on the device (RIP, OSPF, and BGP) if you enable dynamic routing.

- The permanent network routes or host routes you add.
- The routes the XTM device automatically makes when it reads the network configuration information.

If your XTM device detects that an external interface is down, it removes any static or dynamic routes that use that interface. This is true if the hosts specified in the Link Monitor become unresponsive and if the physical Ethernet link is down.

For more information on interface status and route table updates, see *About WAN Interface Status* on page 140.

When to Use Multi-WAN Methods and Routing

If you use dynamic routing, you can use either the Routing Table or Round-Robin multi-WAN configuration method. Routes that use a gateway on an internal (optional or trusted) network are not affected by the multi-WAN method you select.

When to Use the Routing Table Method

The Routing Table method is a good choice if:

- You enable dynamic routing (RIP, OSPF, or BGP) and the routers on the external network advertise routes to the XTM device so that the device can learn the best routes to external locations.
- You must get access to an external site or external network through a specific route on an external network. Examples include:
  - You have a private circuit that uses a frame relay router on the external network.
  - You want all traffic to an external location to always go through a specific XTM device external interface.

The Routing Table method is the fastest way to load balance more than one route to the Internet. After you enable this option, the ECMP algorithm manages all connection decisions. No additional configuration is necessary on the XTM device.

When to Use the Round-Robin Method

Load balancing traffic to the Internet using ECMP is based on connections, not bandwidth. Routes configured statically or learned from dynamic routing are used before the ECMP algorithm. If you have Fireware XTM with a Pro upgrade, the weighted round-robin option gives you options to send more traffic through one external interface than another. At the same time, the round-robin algorithm distributes traffic to each external interface based on bandwidth, not connections. This gives you more control over how many bytes of data are sent through each ISP.

Serial Modem Failover

(This topic applies only to XTM 2 Series devices.)

You can configure your XTM 2 Series device to send traffic through a serial modem when it cannot send traffic with any external interface. You must have a dial-up account with an ISP (Internet Service Provider) and an external modem connected on the USB port (2 Series) to use this option.

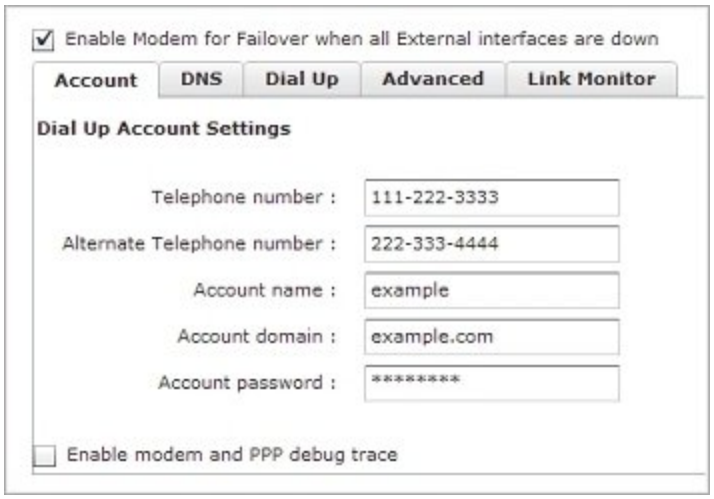
The XTM 2 Series has been tested with these modems:

- Zoom FaxModem 56K model 2949
- MultiTech 56K Data/Fax Modem International
- OMRON ME5614D2 Fax/Data Modem
- Hayes 56K V.90 serial fax modem

For a serial modem, use a USB to serial adapter to connect the modem to the XTM 2 Series device.

Enable Serial Modem Failover

1. Select **Network > Modem**.
   The Modem page appears.
2. Select the **Enable Modem for Failover when all External interfaces are down** check box.



3. Complete the **Account**, **DNS**, **Dial-Up**, and **Link Monitor** settings, as described in the subsequent sections.
4. Click **Save**.

Account Settings

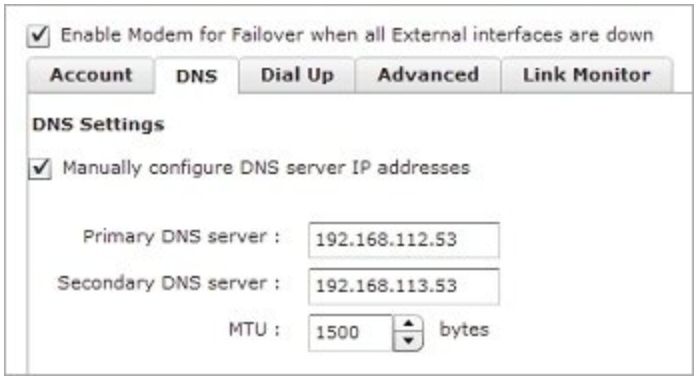
1. Select the **Account** tab.
2. In the **Telephone number** text box, type the telephone number of your ISP.
3. If you have another number for your ISP, the **Alternate Telephone number** text box, type that number.
4. In the **Account name** text box, type your dial-up account name.

5. If you log in to your account with a domain name, in the **Account domain** text box, type the domain name.
   An example of a domain name is msn.com.
6. In the **Account password** text box, type the password you use to connect to your dial-up account.
7. If you have problems with your connection, select the **Enable modem and PPP debug trace** check box. When this option is selected, the XTM device sends detailed logs for the serial modem failover feature to the event log file.

DNS Settings

If your dial-up ISP does not give DNS server information, or if you must use a different DNS server, you can manually add the IP addresses for a DNS server to use after failover occurs.

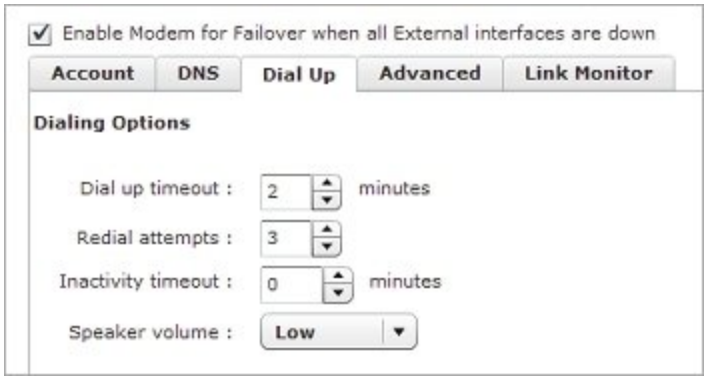
1. Select the **DNS** tab.
   The DNS Settings page appears.



2. Select the **Manually configure DNS server IP addresses** check box.
3. In the **Primary DNS Server** text box, type the IP address of the primary DNS server.
4. If you have a secondary DNS server, in the **Secondary DNS server** text box, type the IP address for the secondary server.
5. In the **MTU** text box, for compatibility purposes, you can set the Maximum Transmission Unit (MTU) to a different value. Most users can keep the default setting.

Dial-up Settings

1. Select the **Dial Up** tab.
   The Dialing Options page appears.



2. In the **Dial up timeout** text box, type or select the number of seconds before a timeout occurs if your modem does not connect. The default value is two (2) minutes.
3. In the **Redial attempts** text box, type or select the number of times the XTM device tries to redial if your modem does not connect. The default is to wait for three (3) connection attempts.
4. In the **Inactivity Timeout** text box, type or select the number of minutes to wait if no traffic goes through the modem before a timeout occurs. The default value is no timeout.
5. From the **Speaker volume** drop-down list, select your modem speaker volume.

Advanced Settings

Some ISPs require that you specify one or more ppp options in order to connect. In China, for example, some ISPs require that you use the ppp option *receive-all*. The receive-all option causes ppp to accept all control characters from the peer.

1. Select the **Advanced** tab.

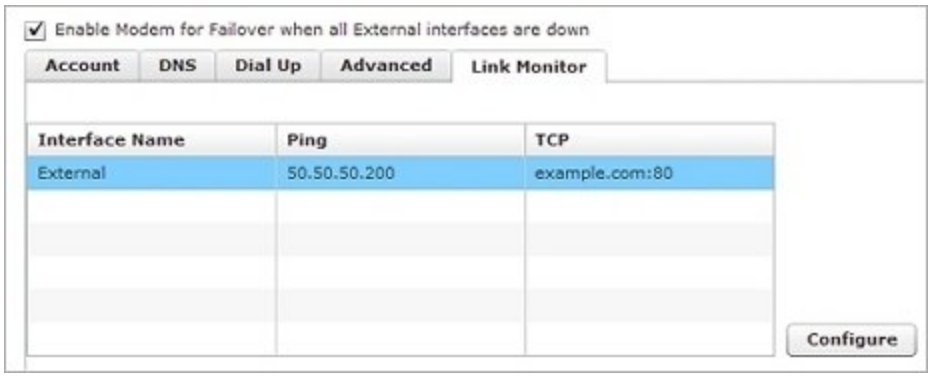
2. In the **PPP options** text box, type the required ppp options. To specify more than one ppp option, separate each option with a comma.

Link Monitor Settings

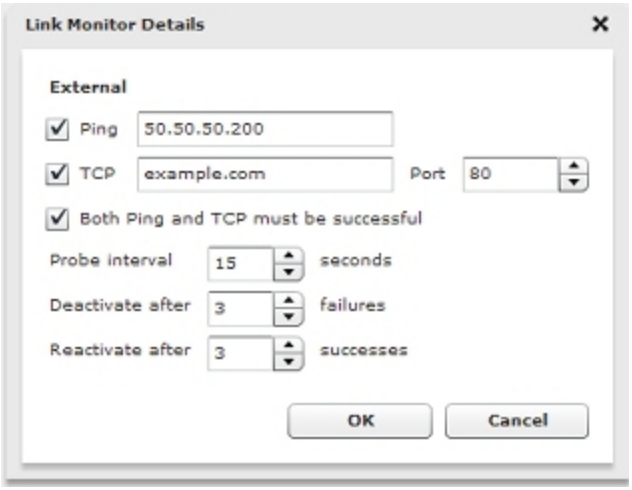
You can set options to test one or more external interfaces for an active connection. When an external interface becomes active again, the XTM device no longer sends traffic over the serial modem and uses the external interface or interfaces instead. You can configure the Link Monitor to ping a site or device on the external interface, create a TCP connection with a site and port number you specify, or both. You can also set the time interval between each connection test, and configure the number of times a test must fail or succeed before an interface is activated or deactivated.

To configure the link monitor settings for an interface:

1. Select the **Link Monitor** tab.
   The ping and TCP connection options you set for each external interface appear.



2. To configure an interface, select it from the list and click **Configure**.
   The Link Monitor Details dialog box appears.



3. To ping a location or device on the external network, select the **Ping** check box and type an IP address or host name in the adjacent text box.
4. To create a TCP connection to a location or device on the external network, select the **TCP** check box and type an IP address or host name in the adjacent text box. You can also type or select a **Port** number.
   The default port number is 80 (HTTP).

5. To require successful ping and TCP connections before an interface is marked as active, select the **Both Ping and TCP must be successful** check box.
6. To change the time interval between connection attempts, in the **Probe interval** text box, type or select a different number.
   The default setting is 15 seconds.
7. To change the number of failures that mark an interface as inactive, in the **Deactivate after** text box, type or select a different number .
   The default value is three (3) connection attempts.
8. To change the number of successful connections that mark an interface as active, in the **Reactivate after** text box, type or select a different number.
   The default value is three (3) connection attempts.
9. Click **OK**.

About Advanced Multi-WAN Settings

You can configure sticky connections, failback, and notification of multi-WAN events. Not all configuration options are available for all multi-WAN configuration options. If a setting does not apply to the multi-WAN configuration option you selected, those fields are not active.

To configure multi-WAN settings:

1. Select **Network > Multi-WAN**.
2. Select the **Advanced Settings** tab.
3. Configure **Sticky Connection Duration** and **Failback for Active Connections** as described in the subsequent sections.
4. Click **Save**.

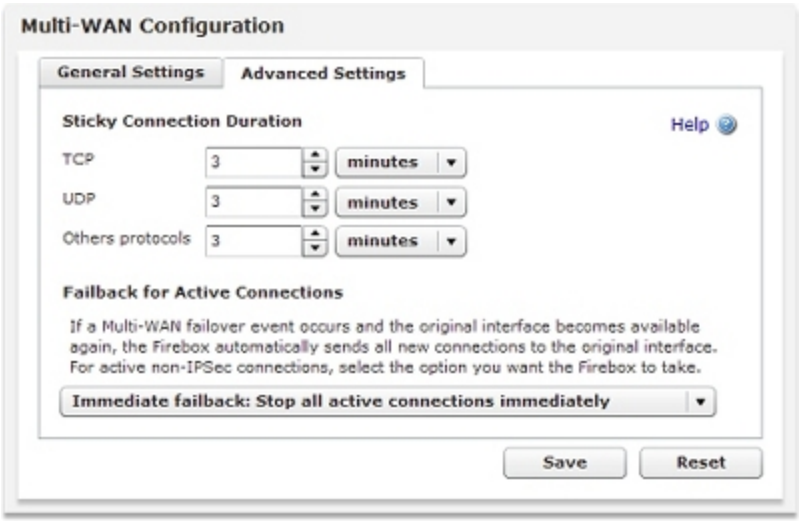
Set a Global Sticky Connection Duration

A sticky connection is a connection that continues to use the same WAN interface for a defined period of time. You can set sticky connection parameters if you use the Round-robin or Interface Overflow options for multi-WAN. Stickiness makes sure that, if a packet goes out through an external interface, any future packets between the source and destination IP address pair use the same external interface for a specified period of time. By default, sticky connections use the same interface for 3 minutes.

If a policy definition contains a sticky connection setting, the policy setting is used instead of the global setting.

To change the global sticky connection duration for a protocol or set of protocols:

1. In the text box for the protocol, type or select a number.
2. In the adjacent drop-down list, select a time duration.



If you set a sticky connection duration in a policy, you can override the global sticky connection duration. For more information, see *Set the Sticky Connection Duration for a Policy* on page 313.

Set the Failback Action

You can set the action you want your XTM device to take when a failover event has occurred and the primary external interface becomes active again. When this occurs, all new connections immediately fail back to the primary external interface. You select the method you want to use for connections in process at the time of failback.

In the **Failback for Active Connections** drop-down list:

- **Immediate failback** — Select this option if you want the XTM device to immediately stop all existing connections.
- **Gradual failback** — Select this option if you want the XTM device to continue to use the failover interface for existing connections until each connection is complete.

This failback setting also applies to any policy-based routing configuration you set to use failover external interfaces.

About WAN Interface Status

You can choose the method and frequency you want the XTM device to use to check the status of each WAN interface. If you do not configure a specified method for the XTM device to use, it pings the interface default gateway to check interface status.

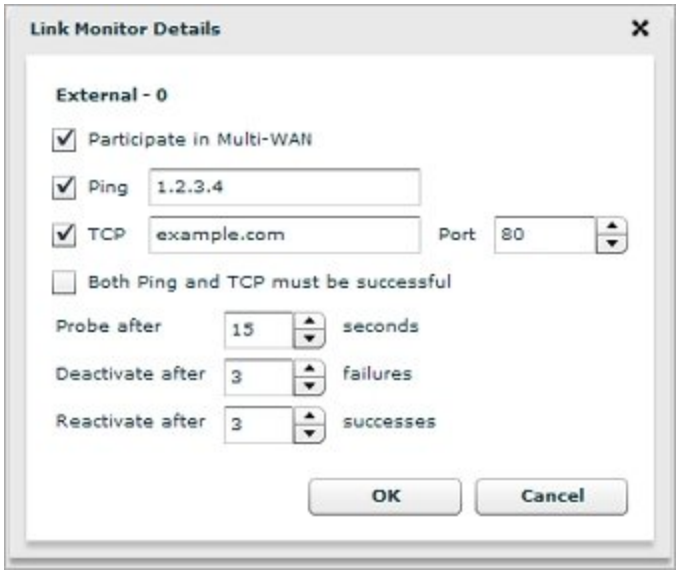
Time Needed for the XTM Device to Update its Route Table

If a link monitor host does not respond, it can take from 40–60 seconds for the XTM device to update its route table. When the same Link Monitor host starts to respond again, it can take from 1–60 seconds for your XTM device to update its route table.

The update process is much faster when your XTM device detects a physical disconnect of the Ethernet port. When this happens, the XTM device updates its route table immediately. When your XTM device detects the Ethernet connection is back up, it updates its route table within 20 seconds.

Define a Link Monitor Host

1. Select **Network > Multi-WAN**.
2. Select the interface and click **Configure**.
   The Link Monitor Details dialog box appears.



3. Select the check boxes for each link monitor method you want the XTM device to use to check status of each external interface:

   - **Ping** — Add an IP address or domain name for the XTM device to ping to check for interface status.
   - **TCP** — Add the IP address or domain name of a computer that the XTM device can negotiate a TCP handshake with to check the status of the WAN interface.
   - **Both ping and TCP must be successful** — The interface is considered inactive unless both a ping and TCP connection complete successfully.

   If an external interface is a member of a FireCluster configuration, a multi-WAN failover caused by a failed connection to a link monitor host does not trigger FireCluster failover. FireCluster failover occurs only when the physical interface is down or does not respond. If you add a domain name for the XTM device to ping and any one of the external interfaces has a static IP address, you must configure a DNS server, as described in Add WINS and DNS Server Addresses.

4. To configure the frequency you want the XTM device to use to check the status of the interface, type or select a **Probe after** setting.
   The default setting is 15 seconds.
5. To change the number of consecutive probe failures that must occur before failover, type or select a **Deactivate after** setting.
   The default setting is three (3). After the selected number of failures, the XTM device starts to send traffic through the next specified interface in the multi-WAN failover list.

6. To change the number of consecutive successful probes through an interface before an interface that was inactive becomes active again, type or select a **Reactivate after** setting.
7. Repeat these steps for each external interface.
8. Click **Save**.

8 Network Address Translation (NAT)

About Network Address Translation

Network Address Translation (NAT) is a term used to describe any of several forms of IP address and port translation. At its most basic level, NAT changes the IP address of a packet from one value to a different value.

The primary purposes of NAT are to increase the number of computers that can operate off a single publicly routable IP address, and to hide the private IP addresses of hosts on your LAN. When you use NAT, the source IP address is changed on all the packets you send.

You can apply NAT as a general firewall setting, or as a setting in a policy. Firewall NAT settings do not apply to BOVPN policies.

If you have Fireware XTM with a Pro upgrade, you can configure server load balancing as part of an SNAT rule. The server load balancing feature is designed to help you increase the scalability and performance of a high-traffic network with multiple public servers protected by your XTM device. With server load balancing, you can have the XTM device control the number of sessions initiated to multiple servers for each firewall policy you configure. The XTM device controls the load based on the number of sessions in use on each server. The XTM device does not measure or compare the bandwidth that is used by each server.

For more information on server load balancing, see *Configure Server Load Balancing* on page 163.

Types of NAT

The XTM device supports three different types of NAT. Your configuration can use more than one type of NAT at the same time. You apply some types of NAT to all firewall traffic, and other types as a setting in a policy.

Dynamic NAT

Dynamic NAT is also known as IP masquerading. The XTM device can apply its public IP address to the outgoing packets for all connections or for specified services. This hides the real IP address of the computer that is the source of the packet from the external network. Dynamic NAT is generally used to hide the IP addresses of internal hosts when they get access to public services.

For more information, see *About Dynamic NAT* on page 144.

Static NAT

Also known as port forwarding, you configure static NAT in an SNAT action and then use that action when you configure policies. Static NAT is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes this IP address to an IP address and port behind the firewall.

For more information, see *Configure Static NAT* on page 160.

1-to-1 NAT

1-to-1 NAT creates a mapping between IP addresses on one network and IP addresses on a different network. This type of NAT is often used to give external computers access to your public, internal servers.

For more information, see *About 1-to-1 NAT* on page 149.

About Dynamic NAT

Dynamic NAT is the most frequently used type of NAT. It changes the source IP address of an outgoing connection to the public IP address of the XTM device. Outside the XTM device, you see only the external interface IP address of the XTM device on outgoing packets.

Many computers can connect to the Internet from one public IP address. Dynamic NAT gives more security for internal hosts that use the Internet, because it hides the IP addresses of hosts on your network. With dynamic NAT, all connections must start from behind the XTM device. Malicious hosts cannot start connections to the computers behind the XTM device when the XTM device is configured for dynamic NAT.

In most networks, the recommended security policy is to apply NAT to all outgoing packets. With Fireware, dynamic NAT is enabled by default in the **Network > NAT** dialog box. It is also enabled by default in each policy you create. You can override the firewall setting for dynamic NAT in your individual policies, as described in *Apply NAT Rules* on page 312.

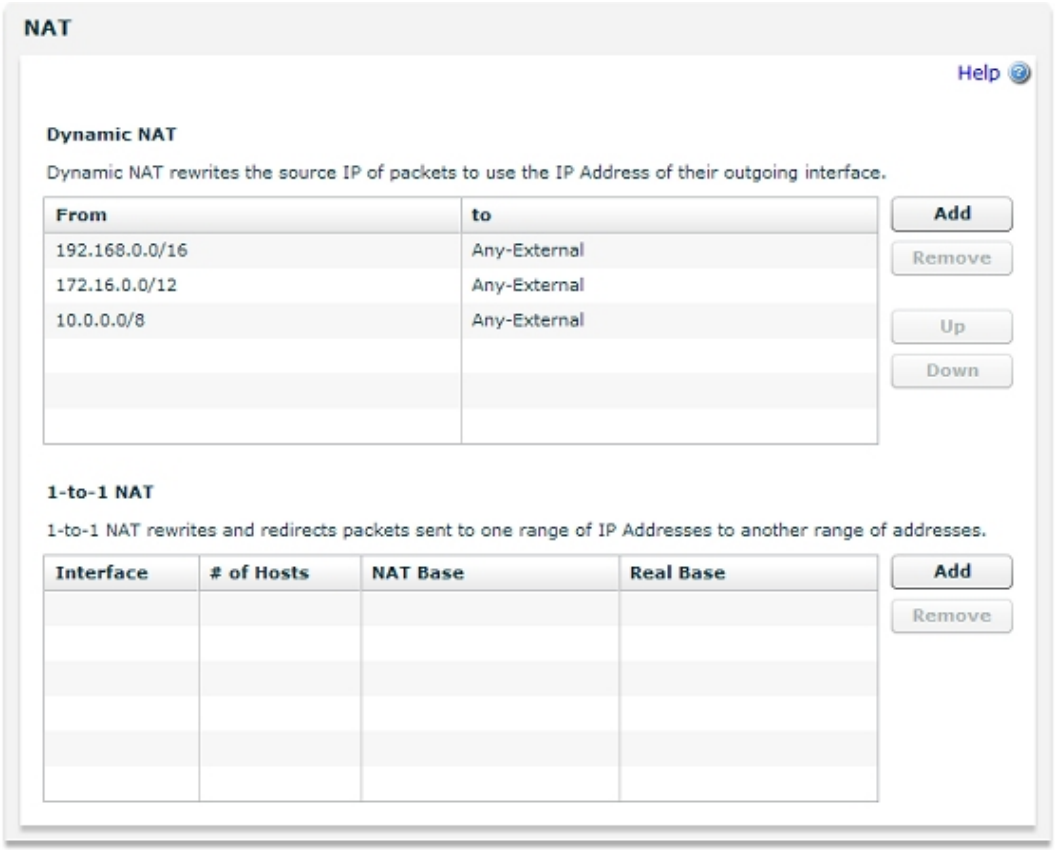
Add Firewall Dynamic NAT Entries

The default configuration of dynamic NAT enables dynamic NAT from all private IP addresses to the external network. The default entries are:

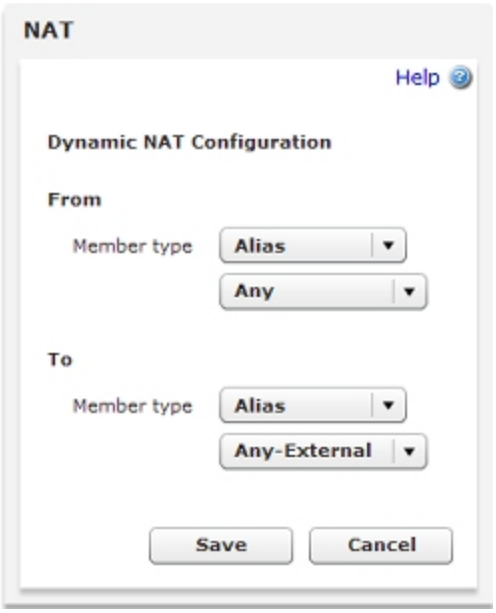
- 192.168.0.0/16 – Any-External
- 172.16.0.0/12 – Any-External
- 10.0.0.0/8 – Any-External

These three network addresses are the private networks reserved by the Internet Engineering Task Force (IETF) and usually are used for the IP addresses on LANs. To enable dynamic NAT for private IP addresses other than these, you must add an entry for them. The XTM device applies the dynamic NAT rules in the sequence that they appear in the Dynamic NAT Entries list. We recommend that you put the rules in a sequence that matches the volume of traffic the rules apply to.

1. Select **Network > NAT**.
   The NAT settings page appears.



2. In the **Dynamic NAT** section, click **Add**.
   The Dynamic NAT configuration page appears.



3. In the **From** section, click the **Member Type** drop-down list to select the type of address to use to specify the source of the outgoing packets: **Host IP**, **Network IP**, **Host Range**, or **Alias**.
4. In the **From** section, below the **Member Type** drop-down list, type the host IP address, network IP address, or host IP address range, or select an alias in the drop-down list.
   You must type a network address in slash notation.

   For more information on built-in XTM device aliases, see *About Aliases* on page 294.
5. In the **To** section, click the **Member Type** drop-down list to select the type of address to use to specify the destination of the outgoing packets.
6. In the **To** section, below the **Member Type** drop-down list, type the host IP address, network IP address, or host IP address range, or select an alias in the drop-down list.
7. Click **Save**.
   The new entry appears in the Dynamic NAT Entries list.

Delete a Dynamic NAT Entry

You cannot change an existing dynamic NAT entry. If you want to change an existing entry, you must delete the entry and add a new one.

To delete a dynamic NAT entry:

1. Select the entry to delete.
2. Click **Remove**.
   A warning message appears.
3. Click **Yes**.

Reorder Dynamic NAT Entries

To change the sequence of the dynamic NAT entries:

1. Select the entry to change.
2. Click **Up** or **Down** to move it in the list.

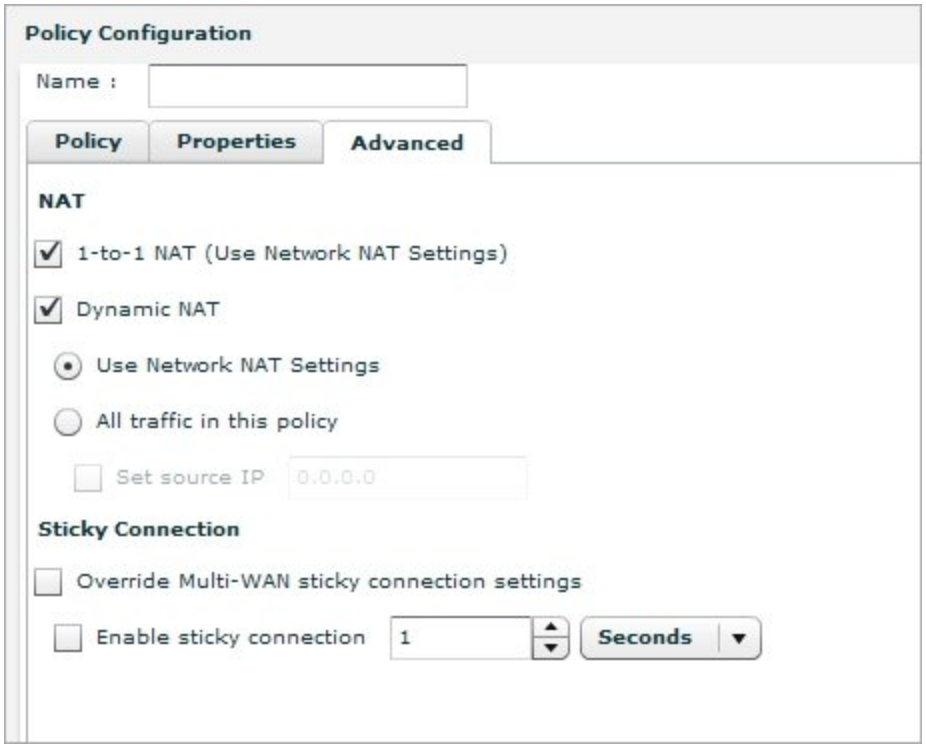
Configure Policy-Based Dynamic NAT

In policy-based dynamic NAT, the XTM device maps private IP addresses to public IP addresses. Dynamic NAT is enabled in the default configuration of each policy. You do not have to enable it unless you previously disabled it.

For policy-based dynamic NAT to work correctly, use the **Policy** tab of the **Edit Policy Properties** dialog box to make sure the policy is configured to allow traffic out through only one XTM device interface.

1-to-1 NAT rules have higher precedence than dynamic NAT rules.

1. Select **Firewall > Firewall Policies**.
   The Firewall Policies list appears.
2. Select a policy and click .
   The Policy Configuration page appears.
3. Click the **Advanced** tab.



4. Select the **Dynamic NAT** check box.
5. Select **Use Network NAT Settings** if you want to use the dynamic NAT rules set for the XTM device. Select **All traffic in this policy** if you want to apply NAT to all traffic in this policy. You can set a dynamic NAT source IP address for any policy that uses dynamic NAT. Select the **Set source IP** check box.

   When you select a source IP address, any traffic that uses this policy shows a specified address from your public or external IP address range as the source. This is most often used to force outgoing SMTP traffic to show the MX record address for your domain when the IP address on the XTM device external interface is not the same as your MX record IP address. This source address must be on the same subnet as the interface you specified for outgoing traffic.

   We recommend that you do not use the **Set source IP** option if you have more than one external interface configured on your XTM device.

   If you do not select the **Set source IP** check box, the XTM device changes the source IP address for each packet to the IP address of the interface from which the packet is sent.
6. Click **Save**.

Disable Policy-Based Dynamic NAT

Dynamic NAT is enabled in the default configuration of each policy. To disable dynamic NAT for a policy:

1. Select **Firewall > Firewall Policies**.
   The Firewall Policies list appears.
2. Select a policy and click **Edit**.
   The Policy Configuration page appears.
3. Click the **Advanced** tab.
4. To disable NAT for the traffic controlled by this policy, clear the **Dynamic NAT** check box.
5. Click **Save**.

About 1-to-1 NAT

When you enable 1-to-1 NAT, your XTM device changes the routes for all incoming and outgoing packets sent from one range of addresses to a different range of addresses. A 1-to-1 NAT rule always has precedence over dynamic NAT.

1-to-1 NAT is frequently used when you have a group of internal servers with private IP addresses that must be made public. You can use 1-to-1 NAT to map public IP addresses to the internal servers. You do not have to change the IP address of your internal servers. When you have a group of similar servers (for example, a group of email servers), 1-to-1 NAT is easier to configure than static NAT for the same group of servers.

To understand how to configure 1-to-1 NAT, we give this example:

Company ABC has a group of five privately addressed email servers behind the trusted interface of their XTM device. These addresses are:

10.1.1.1

10.1.1.2

10.1.1.3

10.1.1.4

10.1.1.5

Company ABC selects five public IP addresses from the same network address as the external interface of their XTM device, and creates DNS records for the email servers to resolve to.

These addresses are:

50.1.1.1

50.1.1.2

50.1.1.3

50.1.1.4

50.1.1.5

Company ABC configures a 1-to-1 NAT rule for their email servers. The 1-to-1 NAT rule builds a static, bi-directional relationship between the corresponding pairs of IP addresses. The relationship looks like this:

10.1.1.1 <--> 50.1.1.1

10.1.1.2 <--> 50.1.1.2

10.1.1.3 <--> 50.1.1.3

10.1.1.4 <--> 50.1.1.4

10.1.1.5 <--> 50.1.1.5

When the 1-to-1 NAT rule is applied, your XTM device creates the bi-directional routing and NAT relationship between the pool of private IP addresses and the pool of public addresses. 1-to-1 NAT also operates on traffic sent from networks that your XTM device protects.

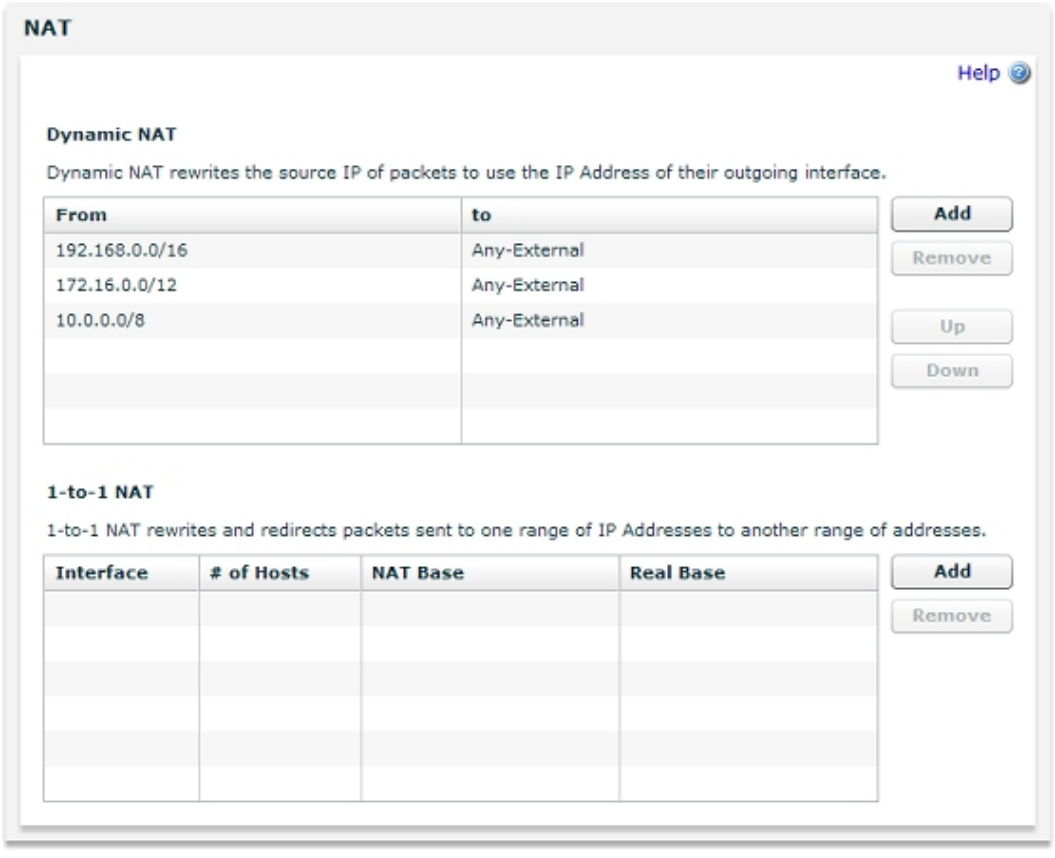
About 1-to-1 NAT and VPNs

When you create a VPN tunnel, the networks at each end of the VPN tunnel must have different network address ranges. You can use 1-to-1 NAT when you must create a VPN tunnel between two networks that use the same private network address. If the network range on the remote network is the same as on the local network, you can configure both gateways to use 1-to-1 NAT.

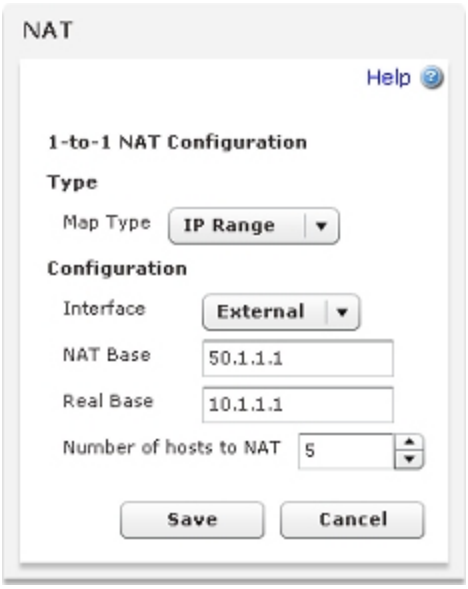
1-to-1 NAT for a VPN tunnel is configured when you configure the VPN tunnel and not in the **Network > NAT** page.

Configure Firewall 1-to-1 NAT

1. Select **Network > NAT**.
   The NAT settings page appears.



2. In the **1-to-1 NAT** section, click **Add**.
   The 1-to-1 NAT configuration page appears.



3. In the **Map Type** drop-down list, select **Single IP** (to map one host), **IP range** (to map a range of hosts), or **IP subnet** (to map a subnet).
   If you select **IP range** or **IP subnet**, do not include more than 256 IP addresses in that range or subnet. To apply NAT to more than 256 IP addresses, you must create more than one rule.
4. Complete all the fields in the **Configuration** section.

   For more information about how to use these fields, see the subsequent *Define a 1-to-1 NAT rule* section.
5. Click **Save**.
6. Add the NAT IP addresses to the appropriate policies.
   - For a policy that manages outgoing traffic, add the **Real Base** IP addresses to the **From** section of the policy configuration.
   - For a policy that manages incoming traffic, add the **NAT Base** IP addresses to the **To** section of the policy configuration.

In the previous example, where we used 1-to-1 NAT to give access to a group of email servers described in *About 1-to-1 NAT* on page 149, we must configure the SMTP policy to allow SMTP traffic. To complete this configuration, you must change the policy settings to allow traffic from the external network to the IP address range 10.1.1.1–10.1.1.5.

1. Add a new policy, or modify an existing policy.
2. Adjacent to the **From** list, click **Add**.
3. Select the alias **Any-External** and click **OK**.
4. Adjacent to the **To** list, click **Add**.
5. To add one IP address at a time, select **Host IP** from the drop-down list and type the IP address in the adjacent text box. Click **OK**.
6. Repeat Steps 3–4 for each IP address in the NAT address range.
   To add several IP addresses at once, select **Host Range** in the drop-down list. Type the first and last IP addresses from the NAT Base range and click **OK**.

Note *To connect to a computer located on a different interface that uses 1-to-1 NAT, you must use that computer's public (NAT base) IP address. If this is a problem, you can disable 1-to-1 NAT and use static NAT.*

Define a 1-to-1 NAT Rule

In each 1-to-1 NAT rule, you can configure a host, a range of hosts, or a subnet. You must also configure:

Interface

The name of the Ethernet interface on which 1-to-1 NAT is applied. Your XTM device applies 1-to-1 NAT for packets sent in to, and out of, the interface. In our example above, the rule is applied to the external interface.

NAT base

When you configure a 1-to-1 NAT rule, you configure the rule with a *from* and a *to* range of IP addresses. The NAT base is the first available IP address in the *to* range of addresses. The NAT base IP address is the address that the real base IP address changes to when the 1-to-1 NAT is applied. You cannot use the IP address of an existing Ethernet interface as your NAT base. In our example above, the NAT base is 50.50.50.1.

Real base

When you configure a 1-to-1 NAT rule, you configure the rule with a *from* and a *to* range of IP addresses. The Real base is the first available IP address in the *from* range of addresses. It is the IP address assigned to the physical Ethernet interface of the computer to which you will apply the 1-to-1 NAT policy. When packets from a computer with a real base address go through the specified interface, the 1-to-1 action is applied. In the example above, the Real base is 10.0.1.50.

Number of hosts to NAT (for ranges only)

The number of IP addresses in a range to which the 1-to-1 NAT rule applies. The first real base IP address is translated to the first NAT Base IP address when 1-to-1 NAT is applied. The second real base IP address in the range is translated to the second NAT base IP address when 1-to-1 NAT is applied. This is repeated until the *Number of hosts to NAT* is reached. In the example above, the number of hosts to apply NAT to is 5.

You can also use 1-to-1 NAT when you must create a VPN tunnel between two networks that use the same private network address. When you create a VPN tunnel, the networks at each end of the VPN tunnel must have different network address ranges. If the network range on the remote network is the same as on the local network, you can configure both gateways to use 1-to-1 NAT. Then, you can create the VPN tunnel and not change the IP addresses of one side of the tunnel. You configure 1-to-1 NAT for a VPN tunnel when you configure the VPN tunnel and not in the **Network > NAT** dialog box.

For an example of how to use 1-to-1 NAT, see *1-to-1 NAT Example*.

Configure Policy-Based 1-to-1 NAT

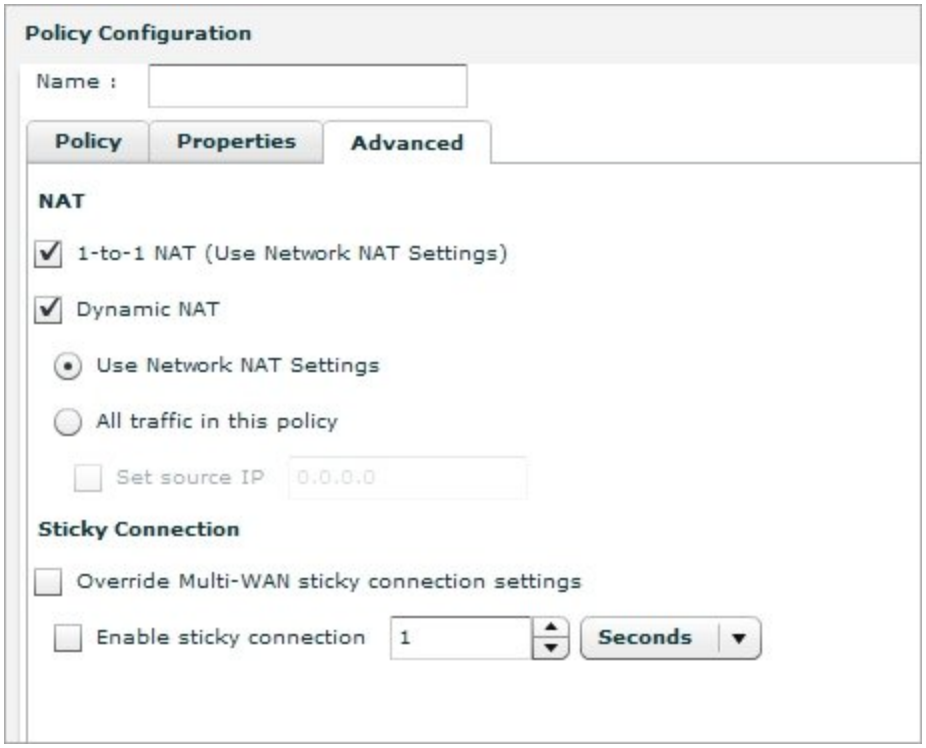
In policy-based 1-to-1 NAT, your XTM device uses the private and public IP ranges that you set when you configured global 1-to-1 NAT, but the rules are applied to an individual policy. 1-to-1 NAT is enabled in the default configuration of each policy. If traffic matches both 1-to-1 NAT and dynamic NAT policies, 1-to-1 NAT takes precedence.

Enable Policy-Based 1-to-1 NAT

Because policy-based 1-to-1 NAT is enabled by default, you do not need to do anything else to enable it. If you have previously disabled policy-based 1-to-1 NAT, select the check box inStep 4 of the subsequent procedure to enable it again.

Disable Policy-Based 1-to-1 NAT

1. Select **Firewall > Firewall Policies**.
   The Firewall Policies list appears.
2. Select a policy and click **Edit**.
   The Policy Configuration page appears.
3. Click the **Advanced** tab.



4. Clear the **1-to-1 NAT** check box to disable NAT for the traffic controlled by this policy.
5. Click **Save**.

Configure NAT Loopback with Static NAT

Fireware XTM includes support for NAT loopback. NAT loopback allows a user on the trusted or optional networks to get access to a public server that is on the same physical XTM device interface by its public IP address or domain name. For NAT loopback connections, the XTM device changes the source IP address of the connect to be the IP address of the internal XTM device interface (the primary IP address for the interface where the client and server both connect to the XTM device).

To understand how to configure NAT loopback when you use static NAT, we give this example:

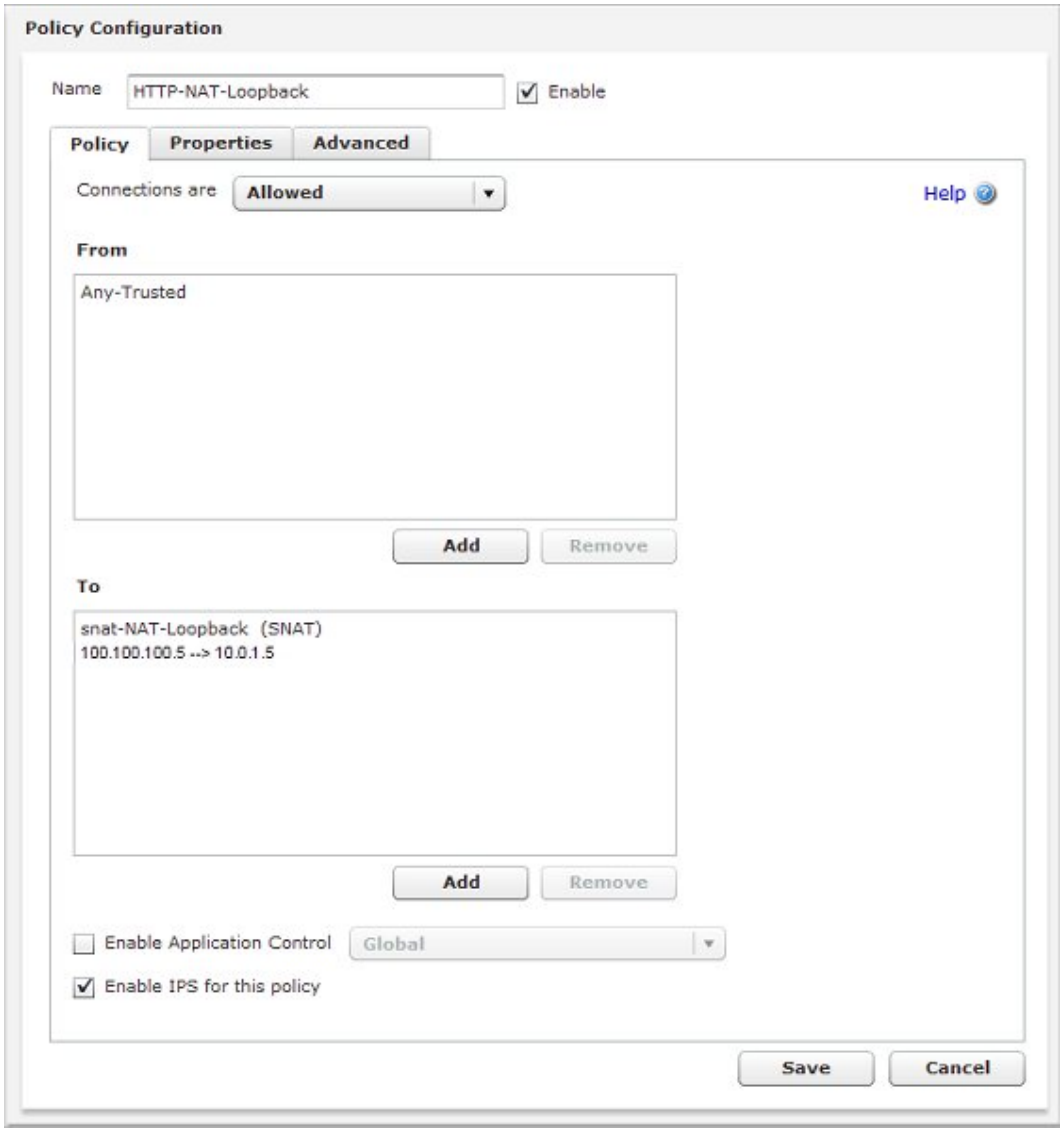
Company ABC has an HTTP server on the XTM device trusted interface. The company uses static NAT to map the public IP address to the internal server. The company wants to allow users on the trusted network to use the public IP address or domain name to get access to this public server.

For this example, we assume:

- The trusted interface is configured with an IP address on the 10.0.1.0/24 network
- The trusted interface is also configured with a secondary IP address on the 192.168.2.0/24 network
- The HTTP server is physically connected to the 10.0.1.0/24 network. The Real Base address of the HTTP server is on the trusted network.

Add a Policy for NAT Loopback to the Server

In this example, to allow users on your trusted and optional networks to use the public IP address or domain name to access a public server that is on the trusted network, you must create an SNAT action and add it to an HTTP policy. The policy addresses could look like this:



The **To** section of the policy contains an SNAT action that defines a static NAT route from the public IP address of the HTTP server to the real IP address of that server.

For more information about static NAT, see *Configure Static NAT* on page 160.

If you use 1-to-1 NAT to route traffic to servers inside your network, see *NAT Loopback and 1-to-1 NAT* on page 156.

NAT Loopback and 1-to-1 NAT

NAT loopback allows a user on the trusted or optional networks to connect to a public server with its public IP address or domain name if the server is on the same physical XTM device interface. If you use 1-to-1 NAT to route traffic to servers on the internal network, use these instructions to configure NAT loopback from internal users to those servers. If you do not use 1-to-1 NAT, see *Configure NAT Loopback with Static NAT* on page 154.

To understand how to configure NAT loopback when you use 1-to-1 NAT, we give this example:

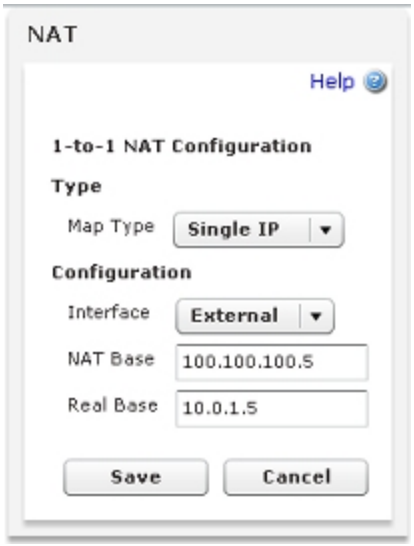
Company ABC has an HTTP server on the XTM device trusted interface. The company uses a 1-to-1 NAT rule to map the public IP address to the internal server. The company wants to allow users on the trusted interface to use the public IP address or domain name to access this public server.

For this example, we assume:

- A server with public IP address 100.100.100.5 is mapped with a 1-to-1 NAT rule to a host on the internal network.

  In the 1-to-1 NAT section of the NAT configuration page, select these options:

  Interface — **External**, NAT Base — **100.100.100.5**, Real Base — **10.0.1.5**



- The trusted interface is configured with a primary network, 10.0.1.0/24
- The HTTP server is physically connected to the network on the trusted interface. The **Real Base** address of that host is on the trusted interface.
- The trusted interface is also configured with a secondary network, 192.168.2.0/24.

For this example, to enable NAT loopback for all users connected to the trusted interface, you must:

1. Make sure that there is a 1-to-1 NAT entry for each interface that traffic uses when internal computers get access to the public IP address 100.100.100.5 with a NAT loopback connection.

   You must add one more 1-to1 NAT mapping to apply to traffic that starts from the trusted interface. The new 1-to-1 mapping is the same as the previous one, except that the **Interface** is set to **Trusted** instead of **External**.

After you add the second 1-to-1 NAT entry, the **1-to-1 NAT** section on the **NAT** page shows two 1-to-1 NAT mappings: one for External and one for Trusted.

In the 1-to-1 NAT section of the NAT configuration page, add these two entries:

Interface — **External**, NAT Base — **100.100.100.5**, Real Base — **10.0.1.5**
Interface — **Trusted**, NAT Base — **100.100.100.5**, Real Base — **10.0.1.5**

2. Add a Dynamic NAT entry for every network on the interface that the server is connected to.

   The **From** field for the Dynamic NAT entry is the network IP address of the network from which computers get access to the 1-to-1 NAT IP address with NAT loopback.

   The **To** field for the Dynamic NAT entry is the NAT base address in the 1-to-1 NAT mapping.

   For this example, the trusted interface has two networks defined, and we want to allow users on both networks to get access to the HTTP server with the public IP address or host name of the server. We must add two Dynamic NAT entries.

   In the Dynamic NAT section of the NAT configuration page, add:

   10.0.1.0/24 - 100.100.100.5
   192.168.2.0/24 - 100.100.100.5

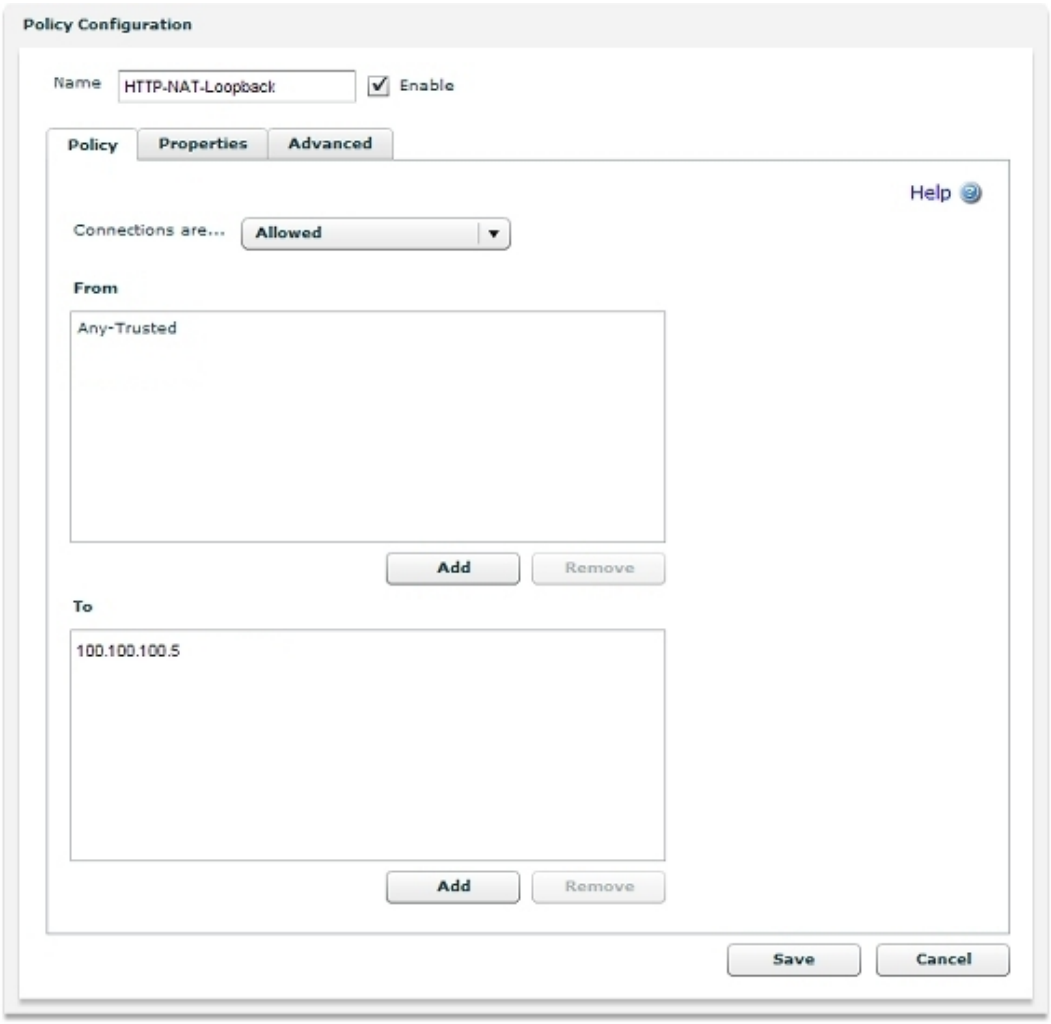
3. Add a policy to allow users on your trusted network to use the public IP address or domain name to get access to the public server on the trusted network. For this example:

   From

   Any-Trusted

   To

   100.100.100.5



The public IP address that users want to connect to is 100.100.100.5. This IP address is configured as a secondary IP address on the external interface.

In the **To** section of the policy, add 100.100.100.5 .

For more information about configuring static NAT, see *Configure Static NAT* on page 160.

For more information about how to configure 1-to-1 NAT, see *Configure Firewall 1-to-1 NAT* on page 150.

About SNAT

An SNAT action is a user-defined action that includes static NAT or server load balancing members which can be referenced by a policy. An SNAT action is a NAT mapping which replaces the original destination IP address (and optionally, port) with a new destination. For a server load balancing SNAT action, the original destination is mapped to multiple server IP addresses, which the XTM device can load balance between.

You can create SNAT actions and apply them to one or more policies in your configuration. To reference an SNAT object in a policy, you add it to the *To* (destination) list in the policy. If you add a server load balancing SNAT action to a policy, it must be the only destination in the policy.

For more information about static NAT and server load balancing, see *Configure Static NAT* and *Configure Server Load Balancing*.

Configure Static NAT

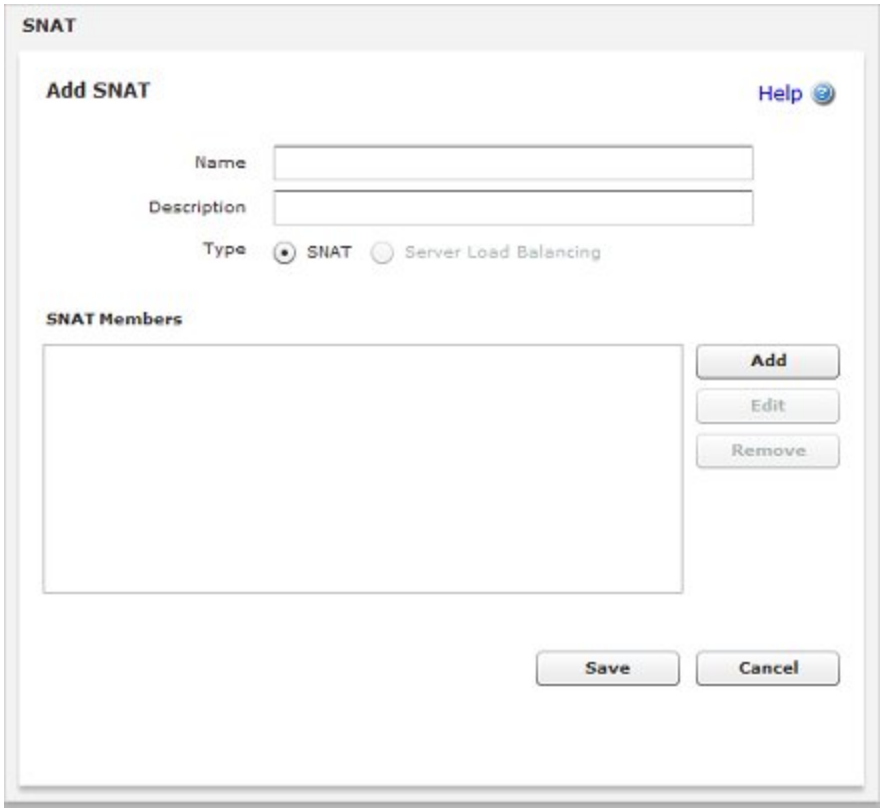
Static NAT, also known as port forwarding, is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes the destination IP address to an IP address and port behind the firewall. If a software application uses more than one port and the ports are selected dynamically, you must either use 1-to-1 NAT, or check whether a proxy on your XTM device manages this kind of traffic. Static NAT also operates on traffic sent from networks that your XTM device protects.

When you use static NAT, you use an external IP address from your XTM device instead of the IP address from a public server. You could do this because you choose to, or because your public server does not have a public IP address. For example, you can put your SMTP email server behind your XTM device with a private IP address and configure static NAT in your SMTP policy. Your XTM device receives connections on port 25 and makes sure that any SMTP traffic is sent to the real SMTP server behind the XTM device.

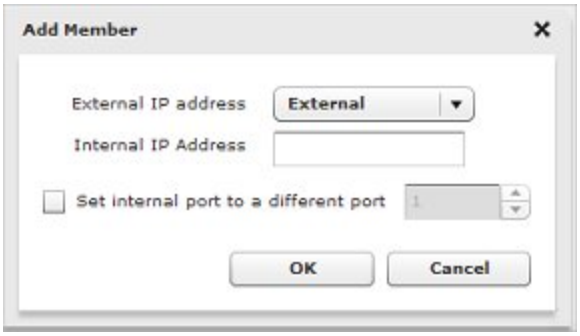
Add a Static NAT Action

Before you can configure a policy to use static NAT, you must define the static NAT action. After you add a static NAT action, you can use it in one or more policies.

1. Select **Firewall > SNAT**.
   The SNAT page appears.
2. Click **Add**.
   The Add SNAT page appears.



3. In the **Name** text box, type a name for this SNAT action. Optionally, type a **Description**.
4. Select the **Static NAT** radio button to specify a static NAT action.
   This is the default selection.
5. Click **Add**.
   The Add Member dialog box appears.



6. In the **External IP address** drop-down list, select the external IP address or alias you want to use in this action.

   For example, you can use static NAT for packets received on only one external IP address. Or, you can use static NAT for packets received on any external IP address if you select the Any-External alias.

7. Type the **Internal IP Address**. This is the destination on the trusted or optional network.
8. If necessary, select the **Set internal port to a different port** check box. This enables port address translation (PAT).

   This feature enables you to change the packet destination not only to a specified internal host but also to a different port. If you select this check box, type the port number or click the up or down arrow to select the port you want to use.

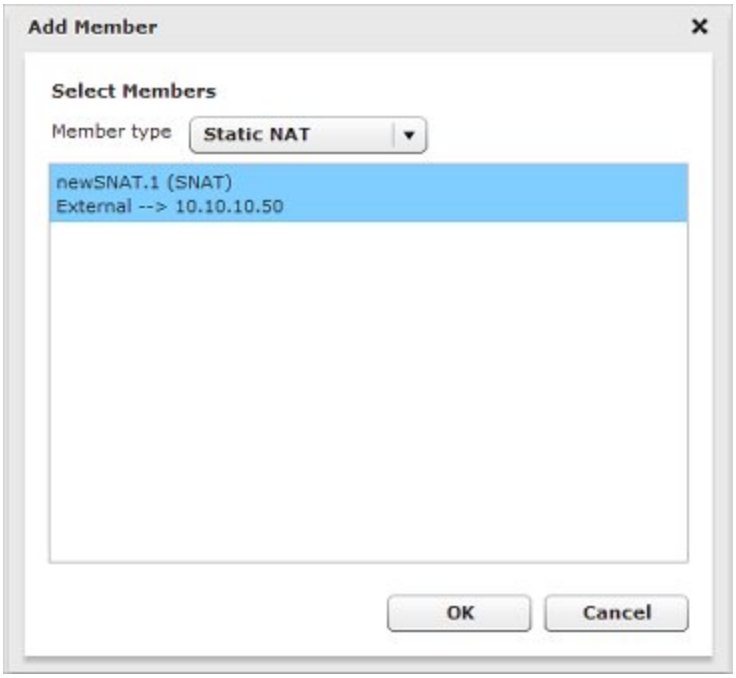
   Note *If you use static NAT in a policy that allows traffic that does not have ports (traffic other than TCP or UDP), the internal port setting is not used for that traffic.*

9. Click **OK**.
   The static NAT route appears in the SNAT Members list.
10. Click **Save**.
    The new SNAT action appears in the SNAT page.

Add a Static NAT Action to a Policy

After you create a static NAT action, you can add it to one or more policies.

1. Select **Firewall > Firewall Policies**.
2. Double click a policy to edit it.
3. In the **Connections are** drop-down list, select **Allowed**.
   To use static NAT, the policy must let incoming traffic through.
4. Below the **To** list, click **Add**.
   The Add Member dialog box appears.



5. From the **Member Type** drop-down list, select **Static NAT**.
   A list of the configured Static NAT Actions appears.
6. Select the Static NAT action to add to this policy, Click **OK**.
   The static NAT route appears in the To section of the policy configuration.
7. Click **Save**.

Edit or Remove a Static NAT Action

To edit an SNAT action:

1. Select **Firewall > SNAT**.
   The SNAT page appears.
2. Click an SNAT action to select it.
3. Click **Edit** to edit the SNAT action.
4. Make any changes you want to the SNAT action.
   When you edit an SNAT action, any changes you make apply to all policies that use that SNAT action.
5. Click **Save**.

To remove an SNAT action:

1. Select **Firewall > SNAT**.
   The SNAT page appears.
2. Click an SNAT action to select it.
3. Click **Remove** to remove the SNAT action.
   You cannot remove an SNAT action that is used by a policy.
4. Click **Yes** to confirm that you want to remove the action.

Configure Server Load Balancing

> ***Note*** *To use the server load balancing feature your XTM device must have an XTM 5 Series, 8 Series, or XTM 1050 device and Fireware XTM with a Pro upgrade.*

The server load balancing feature in Fireware XTM is designed to help you increase the scalability and performance of a high-traffic network with multiple public servers. With server load balancing, you can enable the XTM device to control the number of sessions initiated to as many as 10 servers for each firewall policy you configure. The XTM device controls the load based on the number of sessions in use on each server. The XTM device does not measure or compare the bandwidth that is used by each server.

You configure server load balancing as an SNAT action. The XTM device can balance connections among your servers with two different algorithms. When you configure server load balancing, you must choose the algorithm you want the XTM device to apply.

Round-robin

If you select this option, the XTM device distributes incoming sessions among the servers you specify in the policy in round-robin order. The first connection is sent to the first server specified in your policy. The next connection is sent to the next server in your policy, and so on.

Least Connection

If you select this option, the XTM device sends each new session to the server in the list that currently has the lowest number of open connections to the device. The XTM device cannot tell how many connections the server has open on other interfaces.

You can add any number of servers to a server load balancing action. You can also add a weight to each server to make sure that your most powerful servers are given the heaviest load.. By default, each server has a weight of 1. The weight refers to the proportion of load that the XTM device sends to a server. If you assign a weight of 2 to a server, you double the number of sessions that the XTM device sends to that server, compared to a server with a weight of 1.

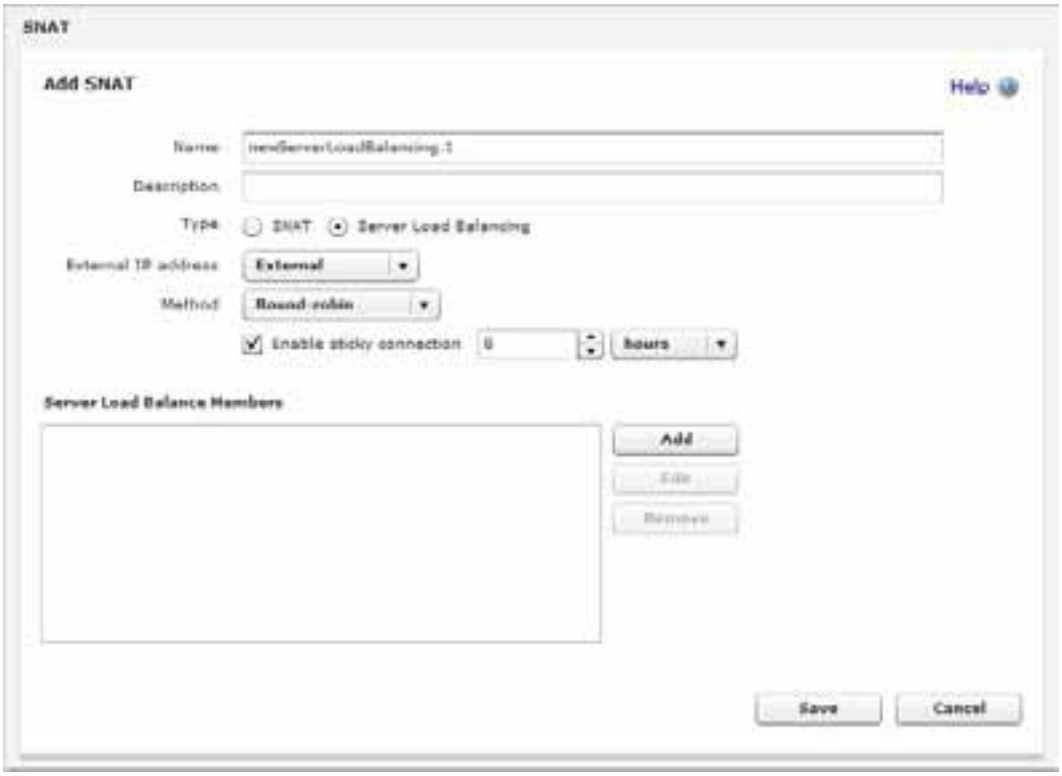
When you configure server load balancing, it is important to know:

- You can configure server load balancing for any policy to which you can apply static NAT.
- If you apply server load balancing to a policy, you cannot set policy-based routing or other NAT rules in the same policy.
- The XTM device does not modify the *sender*, or source IP address, of traffic sent to these devices. While the traffic is sent directly from the XTM device, each device that is part of your server load balancing configuration sees the original source IP address of the network traffic.
- If you use server load balancing in an active/passive FireCluster configuration, real-time synchronization does not occur between the cluster members when a failover event occurs. When the passive backup master becomes the active cluster master, it sends connections to all servers in the server load balancing list to see which servers are available. It then applies the server load balancing algorithm to all available servers.
- If you use server load balancing for connections to a group of RDP servers, you must configure the firewall on each RDP server to allow ICMP requests from the XTM device.

Add a Server Load Balancing SNAT Action

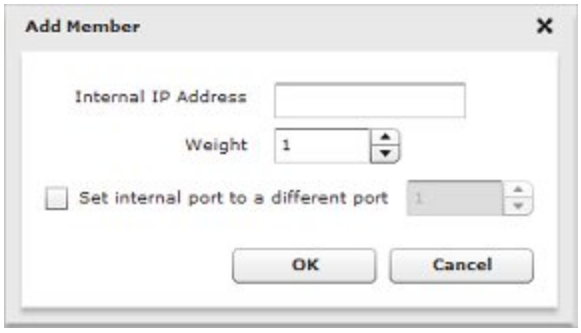
Before you can configure a policy to use server load balancing, you must define the server load balancing in an SNAT action. After you define a Server Load Balancing SNAT action, you can use it in one or more policies.

1. Select **Firewall > SNAT**.
   The SNAT page appears.
2. Click **Add**.
   The Add SNAT page appears.



3. In the **Name** text box, type a name for this action. Optionally, type a **Description**.
4. Select the **Server Load Balancing** radio button to configure a Server Load Balancing SNAT action.
5. From the **External IP address** drop-down list, select the external IP address or alias you want to use in this server load balancing action.

   For example, you can have the XTM device apply server load balancing for this action to packets received on only one external IP address. Or, you can have the XTM device apply server load balancing for packets received on any external IP address if you select the Any-External alias.
6. From the **Method** drop-down list, select the algorithm you want the XTM device to use for server load balancing: **Round-robin** or **Least Connection**.
7. Click **Add** to add the IP address of an internal server to this action.
   The Add Member dialog box appears.

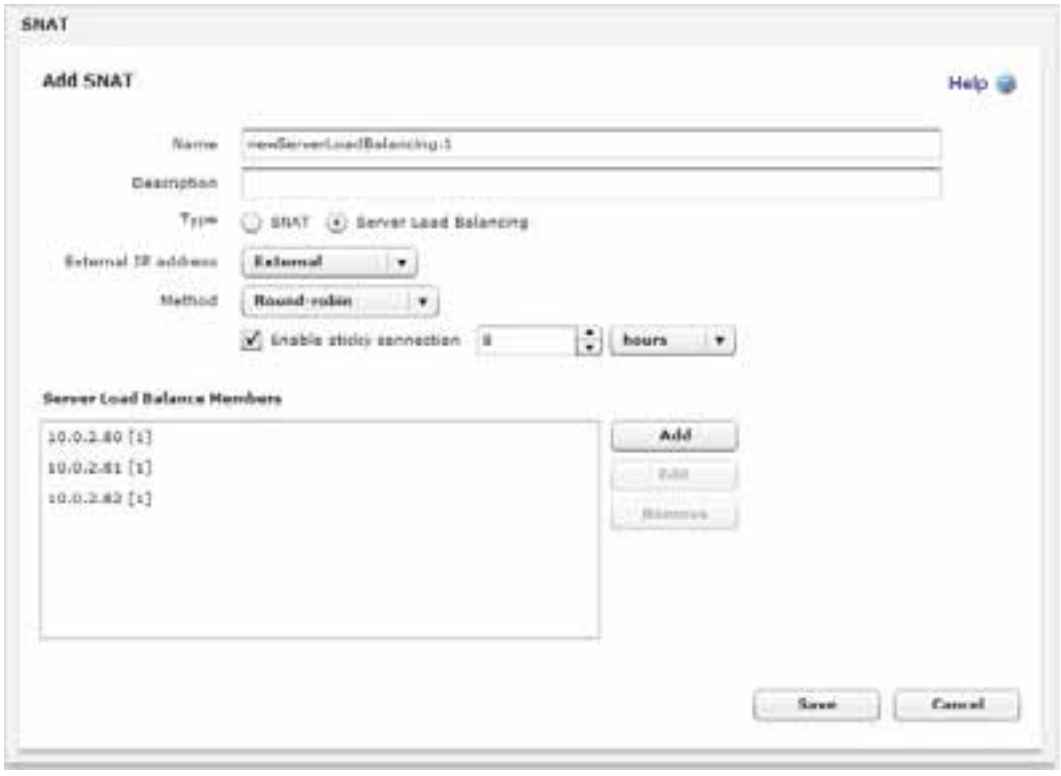


8. In the **Internal IP Address** text box, type the IP address of the server to add.
9. In the **Weight** text box. select the weight for this server for load balancing.
10. If necessary, select the **Set internal port to a different port** check box. This enables port address translation (PAT).

    This feature enables you to change the packet destination not only to a specified internal host but also to a different port. If you select this check box, type the port number or click the up or down arrow to select the port you want to use.

> ***Note*** *If you use static NAT in a policy that allows traffic that does not have ports (traffic other than TCP or UDP), the internal port setting is not used for that traffic.*

11. Click **OK**.
    The server is added to the Server Load Balance Members for this action.

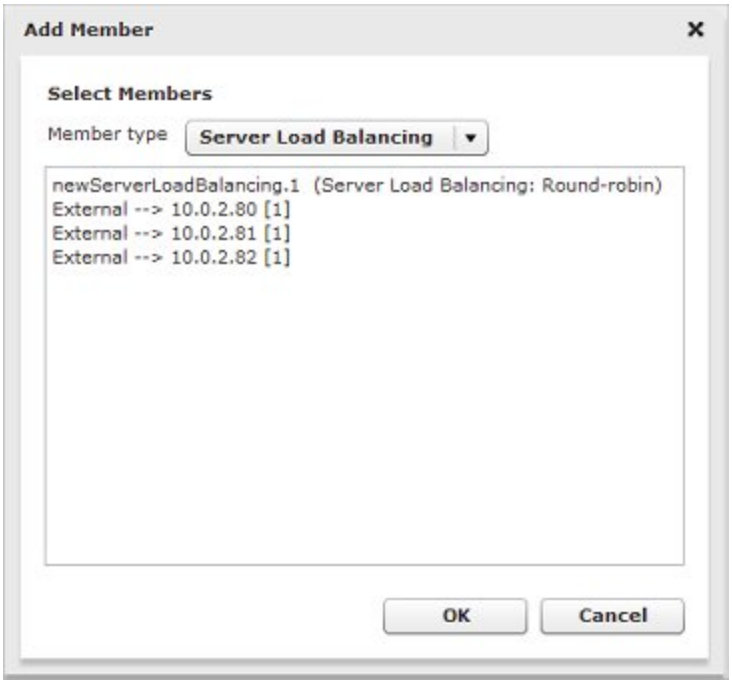


12. Click **Add** to add another server to this action.
13. To set sticky connections for your internal servers, select the **Enable sticky connection** check box and set the time period in the **Enable sticky connection** text box and drop-down list.

    A sticky connection is a connection that continues to use the same server for a defined period of time. Stickiness makes sure that all packets between a source and destination address pair are sent to the same server for the time period you specify.
14. Click **Save**.

Add a Server Load Balancing SNAT Action to a Policy

1. Select **Firewall > Firewall Policies**. Select the policy you want to modify and click **Edit**.
   Or, add a new policy.
2. In the **To** section, click **Add**.
   The Add Member dialog box appears.
3. From the **Member Type** drop-down list, select **Server Load Balancing**.
   The list of server load balancing actions appears.



4. Select the server load balancing action to use. Click **OK**.
   The server load balancing action is added to the To section of the policy.
5. Click **Save**.

Edit or Remove a Server Load Balancing SNAT Action

To edit an SNAT action:

1. Select **Firewall > SNAT**.
   The SNAT page appears.
2. Click an SNAT action to select it.

3. Click **Edit** to edit the SNAT action.
4. Make any changes you want to the SNAT action.
   When you edit an SNAT action, any changes you make apply to all policies that use that SNAT action.
5. Click **Save**.

To remove an SNAT action:

1. Select **Firewall > SNAT**.
   The SNAT page appears.
2. Click an SNAT action to select it.
3. Click **Remove** to remove the SNAT action.
   You cannot remove an SNAT action that is used by a policy.
4. Click **Yes** to confirm that you want to remove the action.

NAT Examples

1-to-1 NAT Example

When you enable 1-to-1 NAT, the XTM device changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses.

Consider a situation in which you have a group of internal servers with private IP addresses that must each show a different public IP address to the outside world. You can use 1-to-1 NAT to map public IP addresses to the internal servers, and you do not have to change the IP addresses of your internal servers. To understand how to configure 1-to-1 NAT, consider this example:

A company has a group of three privately addressed servers behind an optional interface of their XTM device. The addresses of these servers are:

10.0.2.11

10.0.2.12

10.0.2.13

The administrator selects three public IP addresses from the same network address as the external interface of their XTM device, and creates DNS records for the servers to resolve to. These addresses are:

50.50.50.11

50.50.50.12

50.50.50.13

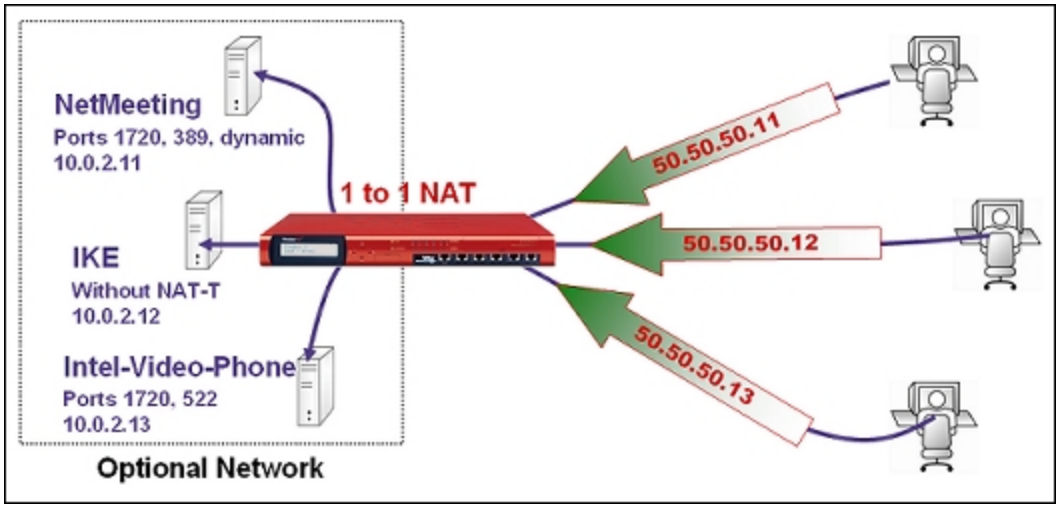
Now the administrator configures a 1-to-1 NAT rule for the servers. The 1-to-1 NAT rule builds a static, bidirectional relationship between the corresponding pairs of IP addresses. The relationship looks like this:

10.0.2.11 <--> 50.50.50.11

10.0.2.12 <--> 50.50.50.12

10.0.2.13 <--> 50.50.50.13

When the 1-to-1 NAT rule is applied, the XTM device creates the bidirectional routing and NAT relationship between the pool of private IP addresses and the pool of public addresses.



For the instructions to define a 1-to-1 NAT rule, see *Configure Firewall 1-to-1 NAT*.

9 Wireless Setup

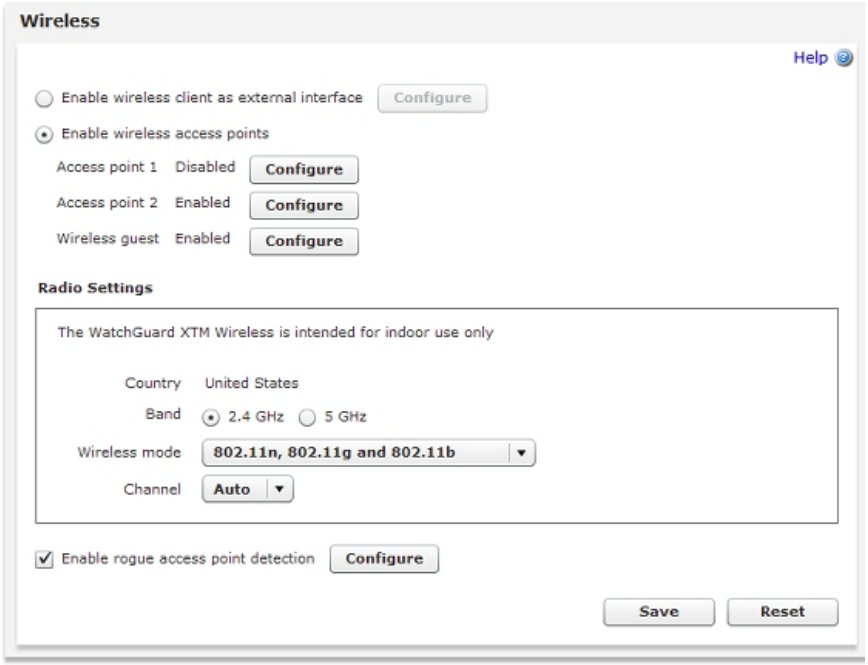
About Wireless Configuration

When you enable the wireless feature of the XTM wireless device, you can configure the external interface to use wireless, or you can configure the XTM device as a wireless access point for users on the trusted, optional, or guest networks.

Before you set up wireless network access, see *Before You Begin* on page 171.

To enable the wireless feature on your XTM device:

1. Select **Network > Wireless**.
   The Wireless page appears.



2. In the **Wireless** page, select a wireless configuration option:

   Enable wireless client as external interface

   This setting allows you to configure the external interface of the XTM wireless device to connect to a wireless network. This is useful in areas with limited or no existing network infrastructure.

   For information about how to configure the external interface as wireless, see *Configure Your External Interface as a Wireless Interface* on page 192.

   Enable wireless access points

   This setting allows you to configure the XTM wireless device as an access point for users on the trusted, optional or guest networks.

   For more information, see *About Wireless Access Point Configuration* on page 170.

3. In the **Radio Settings** section, select your wireless radio settings.

   For more information, see *About Wireless Radio Settings* on page 196.

4. Select the **Enable rogue access point detection** check box to enable the device to scan for untrusted wireless access points.

   For more information, see *Enable Rogue Access Point Detection* on page 199.

5. Click **Save**.

About Wireless Access Point Configuration

Any XTM wireless device can be configured as a wireless access point with three different security zones. You can enable other wireless devices to connect to the XTM wireless device as part of the trusted network or part of the optional network. You can also enable a wireless guest services network for XTM device users. Computers that connect to the guest network connect through the XTM wireless device, but do not have access to computers on the trusted or optional networks.

Before you enable the XTM wireless device as a wireless access point, you must look carefully at the wireless users who connect to the device and determine the level of access you want for each type of user. There are three types of wireless access you can allow:

Allow Wireless Connections to a Trusted Interface

When you allow wireless connections through a trusted interface, wireless devices have full access to all computers on the trusted and optional networks, and full Internet access based on the rules you configure for outgoing access on your XTM device. If you enable wireless access through a trusted interface, we strongly recommend that you enable and use the MAC restriction feature to allow access through the XTM device only for devices you add to the Allowed MAC Address list.

For more information about restricting access by MAC addresses, see *Use Static MAC Address Binding* on page 107.

Allow Wireless Connections to an Optional Interface

When you allow wireless connections through an optional interface, those wireless devices have full access to all computers on the optional network, and full Internet access based on the rules you configure for outgoing access on your XTM wireless device.

Allow Wireless Guest Connections Through the External Interface

Computers that connect to the wireless guest network connect through the XTM wireless device to the Internet based on the rules you configure for outgoing access on your XTM device. Thesewirelessly connected computers do not have access to computers on the trusted or optional network.

For more information about how to configure a wireless guest network, see *Enable a Wireless Guest Network* on page 184.

Before you set up wireless network access, see *Before You Begin* on page 171.

To allow wireless connections to your trusted or optional network, see *Enable Wireless Connections to the Trusted or Optional Network* on page 182.

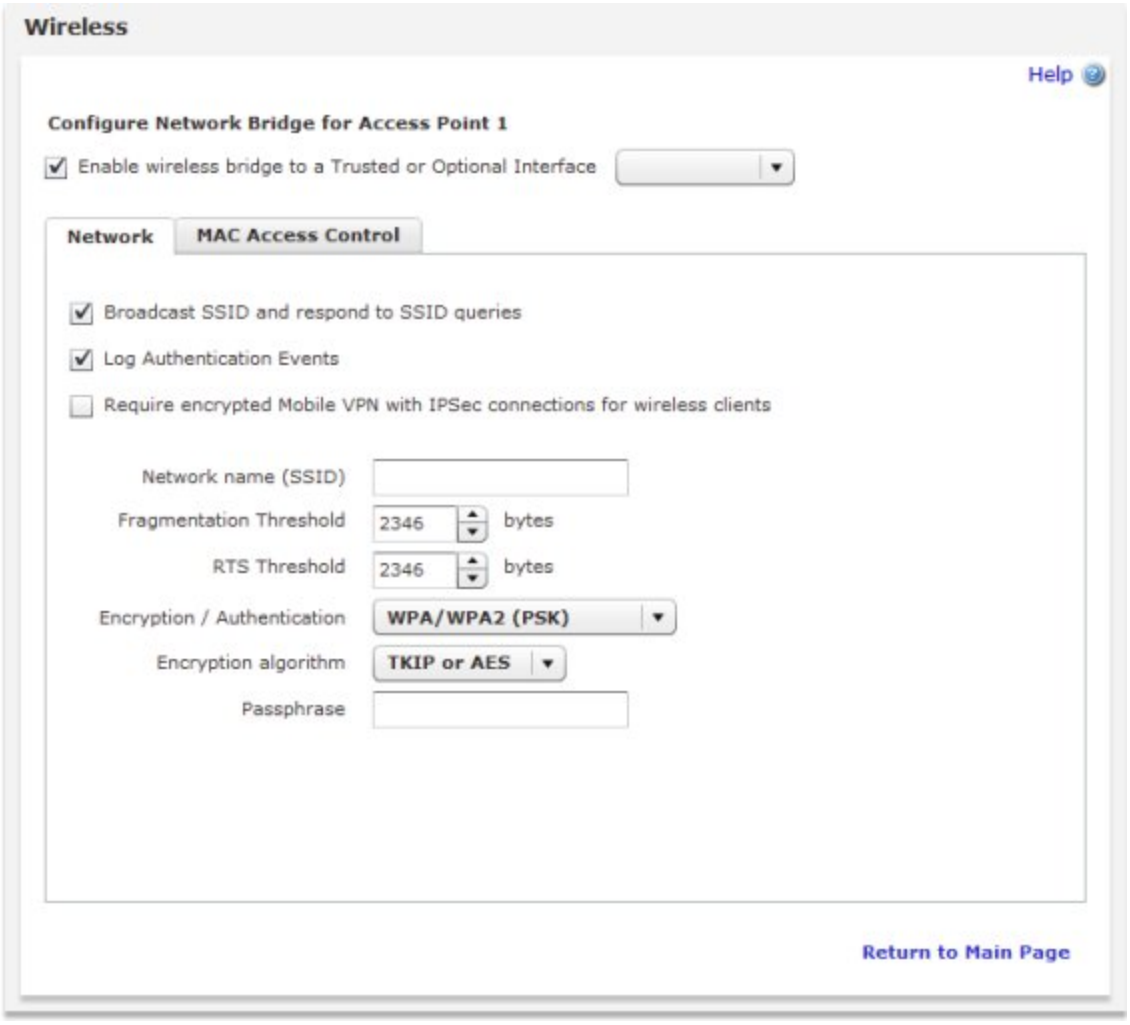
Before You Begin

WatchGuard XTM wireless devices adhere to 802.11n, 802.11b and 802.11g guidelines set by the Institute of Electrical and Electronics Engineers (IEEE). When you install an XTM wireless device:

- Make sure that the wireless device is installed in a location more than 20 centimeters from all persons. This is an FCC requirement for low power transmitters.
- It is a good idea to install the wireless device away from other antennas or transmitters to decrease interference
- The default wireless authentication algorithm configured for each wireless security zone is not the most secure authentication algorithm. If you the wireless devices that connect to your XTM wireless device can operate correctly with WPA2, we recommend that you increase the authentication level to WPA2.
- A wireless client that connects to the XTM wireless device from the trusted or optional network can be a part of any branch office VPN tunnels in which the local network component of the Phase 2 settings includes optional or trusted network IP addresses. To control access to the VPN tunnel, you can force XTM device users to authenticate.

About Wireless Configuration Settings

When you enable wireless access to the trusted, optional, or wireless guest network, some configuration settings are defined the same way for each of the three security zones. These can be set to different values for each zone.



For information about the **Broadcast SSID and respond to SSID queries** setting, see *Enable/Disable SSID Broadcasts* on page 173.

For information about setting the **Network Name (SSID)**, see *Change the SSID* on page 173.

For information about the **Log Authentication Events** setting, see *Log Authentication Events* on page 173.

For information about the **Fragmentation Threshold**, see *Change the Fragmentation Threshold* on page 173.

For information about the **RTS Threshold**, see *Change the RTS Threshold* on page 175.

For information about the **Encryption (Authentication)** setting, see *Set the Wireless Authentication Method* on page 176.

For information about the **Encryption algorithm** setting, see *Set the Encryption Level* on page 180.

Enable/Disable SSID Broadcasts

Computers with wireless network cards send requests to see whether there are wireless access points to which they can connect.

To configure an XTM device wireless interface to send and answer these requests, select the **Broadcast SSID and respond to SSID queries** check box. For security, enable this option only while you configure computers on your network to connect to the XTM wireless device. Disable this option after all your clients are configured. If you use the wireless guest services feature, it can be necessary to allow SSID broadcasts in standard operation.

Change the SSID

The SSID (Service Set Identifier) is the unique name of your wireless network. To use the wireless network from a client computer, the wireless network card in the computer must have the same SSID as the WatchGuard wireless network to which the computer connects.

The Fireware XTM OS automatically assigns an SSID to each wireless network. This SSID uses a format that contains the interface name and the 5th-9th digits from the XTM wireless device serial number. To change the SSID, type a new name in the SSID field to uniquely identify your wireless network.

Log Authentication Events

An authentication event occurs when a wireless computer tries to connect to the wireless interface of a WatchGuard XTM wireless device. To include these events in the log file, select the **Log Authentication Events** check box.

Change the Fragmentation Threshold

Fireware XTM allows you to set the maximum frame size the XTM wireless device can send and not fragment the frame. This is called the fragmentation threshold. This setting is rarely changed. The default setting is the maximum frame size of 2346, which means that it will never fragment any frames that it sends to wireless clients. This is best for most environments.

When to Change the Default FragmentationThreshold

A collision happens when two devices that use the same medium transmit packets at exactly the same time. The two packets can corrupt each other, and the result is a group of unreadable pieces of data. If a packet results in a collision, the packet is discarded and it must be transmitted again. This adds to the overhead on the network and can reduce the throughput or speed of the network.

Larger frames are more likely to collide with each other than smaller frames. To make the wireless packets smaller, you lower the fragmentation threshold on the XTM wireless device. If you lower the maximum frame size, it can reduce the number of repeat transmissions caused by collisions, and lower the overhead caused by repeat transmissions.

Smaller frames introduce more overhead on the network. This is especially true on a wireless network, because every fragmented frame sent from one wireless device to another requires the receiving device to acknowledge the frame. When packet error rates are high (more than five or ten percent collisions or errors), you can help improve the performance of the wireless network if you lower the fragmentation threshold. The time that is saved when you reduce repeat transmissions can be enough to offset the extra overhead added with smaller packets. This can result in higher throughput.

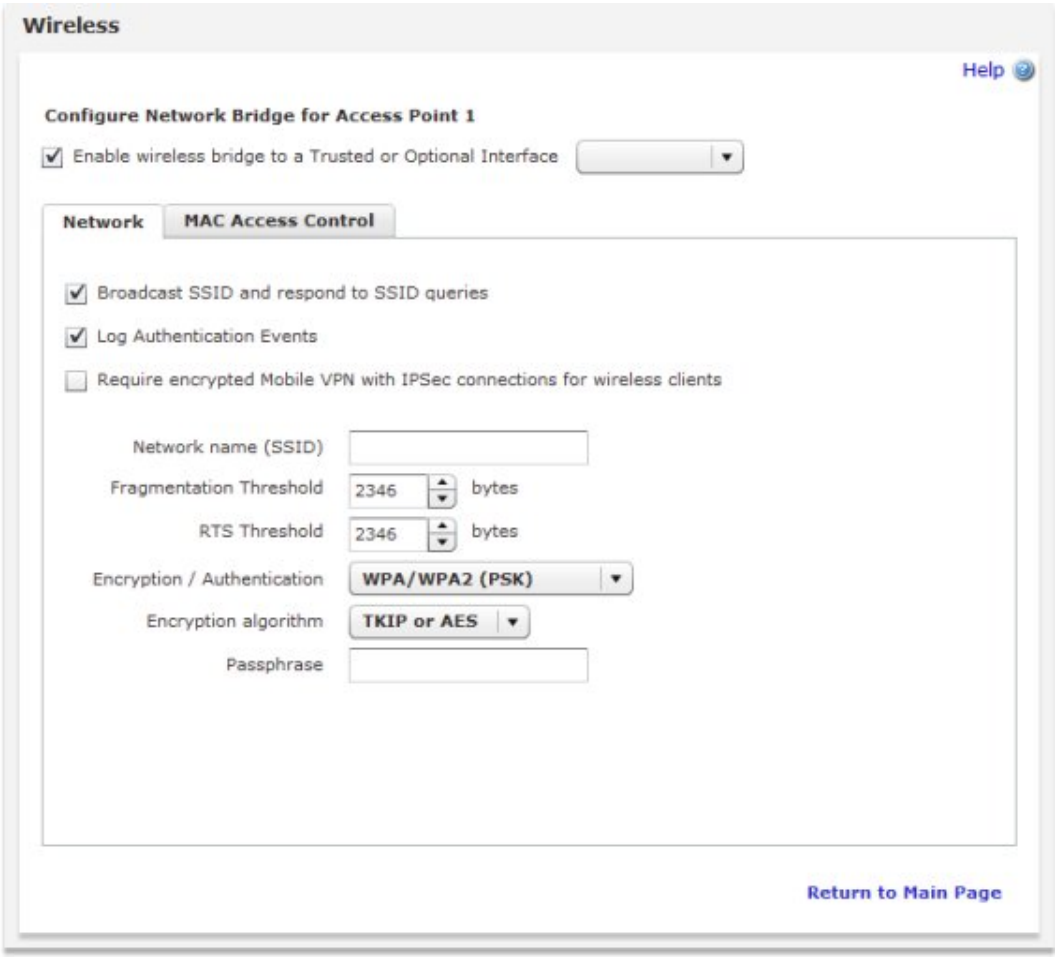
If the rate of packet error is low and you lower the fragmentation threshold, wireless network performance decreases. This occurs because when you lower the threshold, protocol overhead is added and protocol efficiency is reduced.

If you want to experiment, start with the default maximum 2346, and lower the threshold a small amount at a time. To get the most benefit, you must monitor the network for packet errors at different times of the day. Compare the effect that a lower threshold has on network performance when errors are very high with the effect on performance when errors are moderately high.

In general, we recommend that you leave this setting at its default of 2346.

Change the Fragmentation Threshold

1. Select **Network > Wireless**.
2. Select the wireless network to configure. Adjacent to **Access point 1** or **Access point 2** or **Wireless Guest**, click **Configure**.
   The wireless configuration settings for that wireless network appear.



3. To change the fragmentation threshold, in the **Fragmentation Threshold** text box, type or select a value between 256 and 2346.
4. Click **Return to Main Page**.
5. Click **Save**.

Change the RTS Threshold

RTS/CTS (Request To Send / Clear To Send) helps prevent problems when wireless clients can receive signals from more than one wireless access point on the same channel. The problem is sometimes known as *hidden node*.

We do not recommend that you change the default RTS threshold. When the **RTS Threshold** is set to the default of 2346, RTS/CTS is disabled.

If you must change the RTS threshold, adjust it incrementally. Lower it a small amount at a time. After each change, allow enough time to decide whether the change in network performance is positive before you change it again. If you lower this value too much, you can introduce more latency into the network, as *Requests to Send* are increased so much that the shared medium is reserved more often than necessary.

About Wireless Security Settings

WatchGuard XTM wireless devices use three security protocol standards to protect your wireless network: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2. Each protocol standard can encrypt the transmissions on the wireless LAN between the computers and the access points. They also can prevent unauthorized access to the wireless access point.

To protect privacy, you can use these features together with other LAN security mechanisms such as password protection, VPN tunnels, and user authentication.

Set the Wireless Authentication Method

From the **Encryption (Authentication)** drop-down list in the wireless access point configuration, select the level of authentication method for your wireless connections. The eight available authentication methods, from least secure to most secure, are listed below. Select the most secure authentication method that is supported by your wireless network clients.

Open System and Shared Key

The Open System and Shared Key authentication methods use WEP encryption. WEP is not as secure as WPA2 and WPA (Wi-Fi Protected Access). We recommend you do not use these less secure methods unless your wireless clients do not support WPA or WPA2.

- **Open System** — Open System authentication allows any user to authenticate to the access point. This method can be used with no encryption or with WEP encryption.
- **Shared Key** — In Shared Key authentication, only those wireless clients that have the shared key can connect. Shared Key authentication can be used only with WEP encryption.

WPA and WPA2 with Pre-Shared Keys

WPA (PSK) and WPA2 (PSK) Wi-Fi Protected Access methods use pre-shared keys for authentication. WPA (PSK) and WPA2 (PSK) are more secure than WEP shared key authentication. When you choose one of these methods, you configure a pre-shared key that all wireless devices must use to authenticate to the wireless access point.

The XTM wireless device supports three wireless authentication settings that use pre-shared keys:

- **WPA ONLY (PSK)** — The XTM wireless device accepts connections from wireless devices configured to use WPA with pre-shared keys.
- **WPA/WPA2 (PSK)** — The XTM wireless device accepts connections from wireless devices configured to use WPA or WPA2 with pre-shared keys.
- **WPA2 ONLY (PSK)** — The XTM wireless device accepts connections from wireless devices configured to use WPA2 with pre-shared keys authentication. WPA2 implements the full 802.11i standard; it does not work with some older wireless network cards.

WPA and WPA2 with Enterprise Authentication

The WPA Enterprise and WPA2 Enterprise authentication methods use the IEEE 802.1X standard for network authentication. These authentication methods use the EAP (Extensible Authentication Protocol) framework to enable user authentication to an external RADIUS authentication server or to the XTM device (Firebox-DB). The WPA Enterprise and WPA2 Enterprise authentication methods are more secure than WPA/WPA2 (PSK) because users authenticate with their own credentials instead of a shared key.

The XTM wireless device supports three WPA and WPA2 Enterprise wireless authentication methods:

- **WPA Enterprise** — The XTM wireless device accepts connections from wireless devices configured to use WPA Enterprise authentication.
- **WPA/WPA2 Enterprise** — The XTM wireless device accepts connections from wireless devices configured to use WPA Enterprise or WPA2 Enterprise authentication.
- **WPA2 Enterprise** — The XTM wireless device accepts connections from wireless devices configured to use WPA2 Enterprise authentication. WPA2 implements the full 802.11i standard; it does not work with some older wireless network cards.

For more information about these authentication methods, see *WPA and WPA2 Enterprise Authentication*.

To use the Enterprise authentication methods, you must configure an external RADIUS authentication server or configure the XTM device as an authentication server.

For more information about how to configure the settings for these authentication methods, see

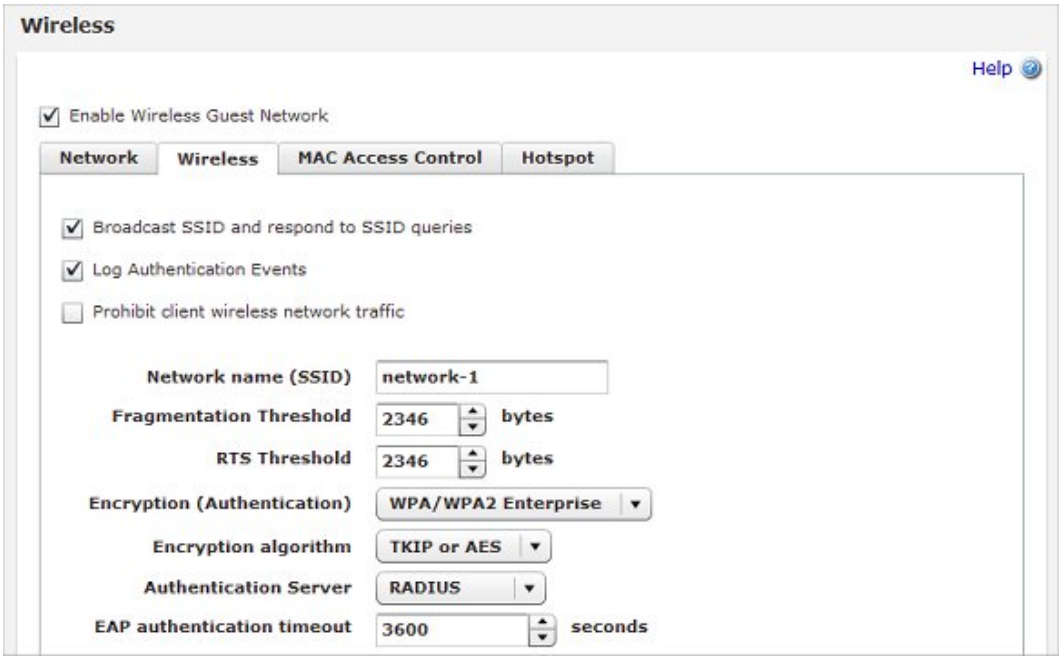
- *Use a RADIUS Server for Wireless Authentication*
- *Use the XTM Device as an Authentication Server for Wireless Authentication*

Use a RADIUS Server for Wireless Authentication

If you select the **WPA Enterprise**, **WPA2 Enterprise**, or **WPA/WPA2 Enterprise** authentication methods in your wireless configuration, you can use a RADIUS server for wireless authentication.

To configure your wireless access point to use RADIUS authentication:

1. Select **Network > Wireless**.
2. Click **Configure** adjacent to the **Access point 1**, **Access point 2**, or **Wireless Guest** configuration.
3. Select the **Wireless** tab.



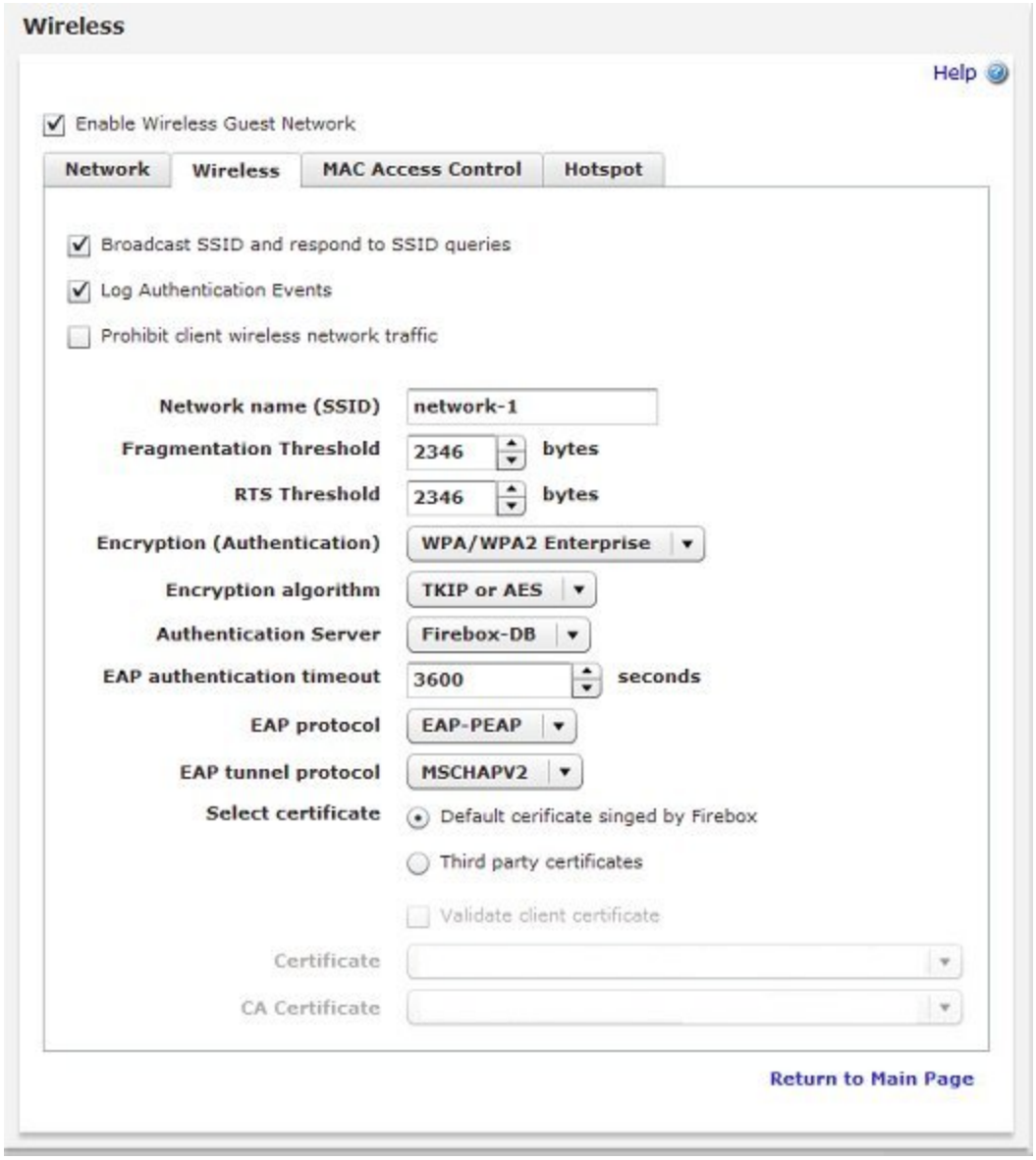
4. From the **Encryption (Authentication)** drop-down list, select **WPA Enterprise**, **WPA2 Enterprise**, or **WPA/WPA2 Enterprise**.
   The Encryption, Authentication server, and EAP authentication timeout settings appear.
5. From the **Encryption algorithm** drop-down list, select the encryption method. For more information, see *Set the Encryption Level*.
6. From the **Authentication server** drop-down list, select **RADIUS**.
   The authentication and protocol configuration settings are disabled. You must configure these settings on your RADIUS server.
7. In the **EAP authentication timeout** text box, you can change the timeout value for authentication. The default is 3600 seconds.
8. Click **Return to Main Page**.
9. Click **Save**.

If you have not previously configured a RADIUS server, you are prompted to do this when you click **Save**. For more information, see *Configure RADIUS Server Authentication*.

Use the XTM Device as an Authentication Server for Wireless Authentication

If you select the **WPA Enterprise**, **WPA2 Enterprise**, or **WPA/WPA2 Enterprise** authentication methods in your wireless configuration, you can use the XTM device as the authentication server for wireless authentication.

1. Select **Network > Wireless**.
2. Click **Configure** adjacent to the **Access point 1**, **Access point 2**, or **Wireless Guest** configuration.
3. Select the **Wireless** tab.



4. From the **Encryption (Authentication)** drop-down list, select **WPA Enterprise**, **WPA2 Enterprise** or **WPA/WPA2 Enterprise**.
5. From the **Encryption algorithm** drop-down list, select the encryption method to use. For more information, see *Set the Encryption Level*.
6. From the **Authentication server** drop-down list, select **Firebox-DB**.
7. In the **EAP authentication timeout** text box, you can change the timeout value for authentication. The default is 3600 seconds.
8. From the **EAP protocol** drop-down list, select the EAP protocol wireless clients must use to connect to the access point.

   - **EAP-PEAP** — EAP Protected Extensible Authentication Protocol
   - **EAP-TTLS** — EAP Tunneled Transport Layer Security
   - **EAP-TLS** — EAP Transport Layer Security

9. From the **EAP tunnel protocol** drop-down list, select the EAP tunnel protocol to use. The available tunnel protocols depend on the selected EAP protocol.
10. Select the certificate type to use for authentication.
    - **Default certificate signed by Firebox** — This is the default.
    - **Third party certificates** — Select from a list of installed third party certificates.
11. If you selected **Third party certificates**, select a certificate from the **Certificate** drop-down list.
12. If you want to use a certificate authority (CA) to validate the client certificate, select the **Validate client certificate** check box and select a CA certificate from the **CA Certificate** drop-down list.

    For more information about certificates, see *About Certificates*.
13. Click **Return to Main Page**.
14. Click **Save**.

To use this authentication method, you must configure your XTM device as an authentication server. For more information, see *Configure Your XTM Device as an Authentication Server*.

Set the Encryption Level

From the **Encryption algorithm** drop-down list in the wireless access point configuration, select the level of encryption for your wireless connections. The available selections change when you use different authentication mechanisms. The Fireware XTM OS automatically creates a random encryption key for you when a key is required. You can use this key or change it to a different key. Each wireless client must use this same key when they connect to the XTM wireless device.

Encryption for Open System and Shared Key Authentication

Encryption options for Open System and Shared Key authentication are WEP 64-bit hexadecimal, WEP 40-bit ASCII, WEP 128-bit hexadecimal, and WEP 128-bit ASCII. If you select Open System authentication, you can also select **No encryption**.

1. If you use WEP encryption, in the **Key** text boxes, type hexadecimal or ASCII characters. Not all wireless adapter drivers support ASCII characters. You can have a maximum of four keys.
    - A WEP 64-bit hexadecimal key must have 10 hexadecimal (0-f) characters.
    - A WEP 40-bit ASCII key must have 5 characters.
    - A WEP 128-bit hexadecimal key must have 26 hexadecimal (0-f) characters.
    - A WEP 128-bit ASCII key must have 13 characters.
2. If you typed more than one key, from the **Key Index** drop-down list, select the key to use as the default key.

    The XTM wireless device can use only one wireless encryption key at a time. If you select a key other than the first key in the list, you also must set your wireless client to use the same key.

Encryption for WPA and WPA2 Authentication

The encryption options for Wi-Fi Protected Access (WPA and WPA2) authentication methods are:

- **TKIP** — Use only TKIP (Temporal Key Integrity Protocol) for encryption. This option is not available for wireless modes that support 802.11n.

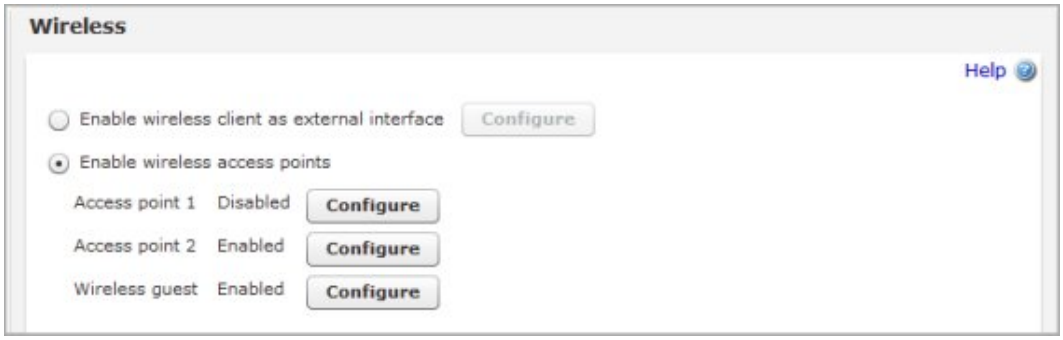
- **AES** — Use only AES (Advanced Encryption Standard) for encryption.
- **TKIP or AES** — Use either TKIP or AES.

We recommend that you select **TKIP or AES**. This allows the XTM wireless device to accept connections from wireless clients configured to use TKIP or AES encryption. For 802.11n wireless clients, we recommend you configure the wireless client to use AES encryption.

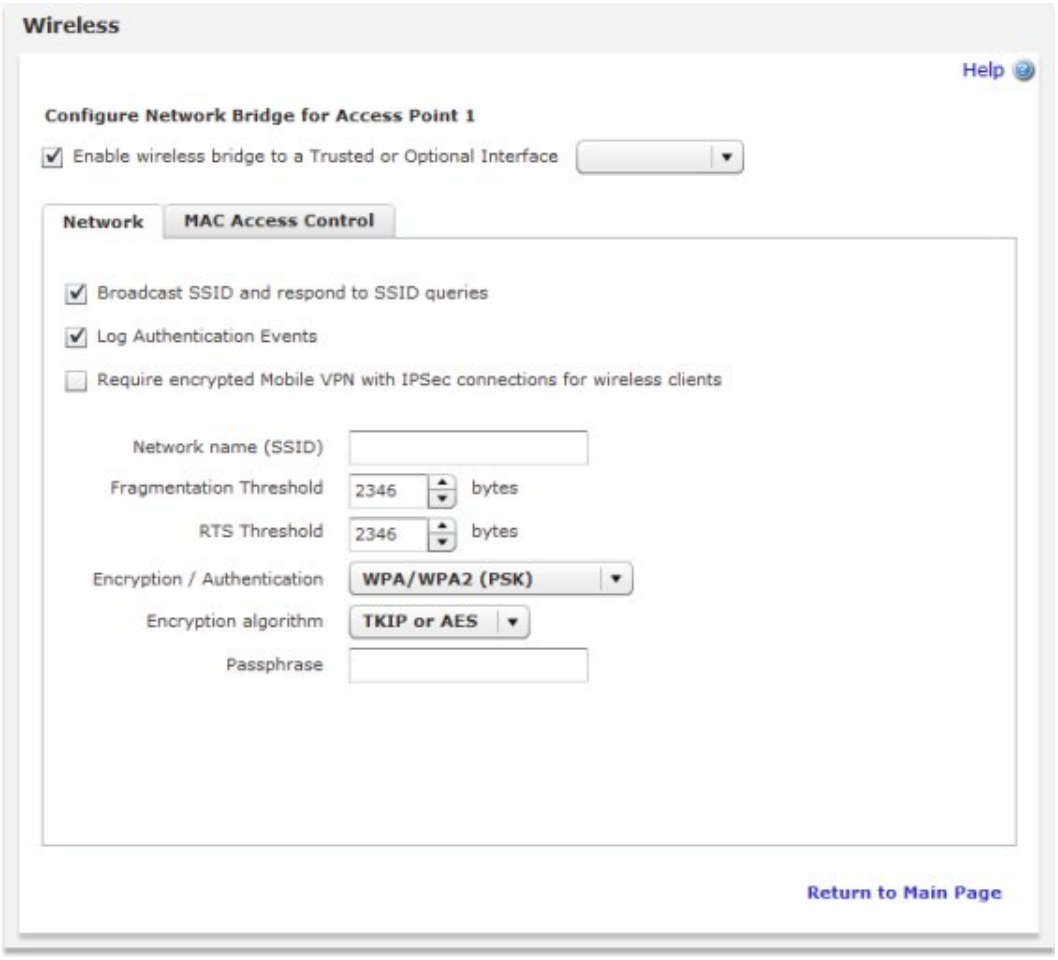
Enable Wireless Connections to the Trusted or Optional Network

To allow wireless connections to your trusted or optional network:

1. Select **Network > Wireless**.
   The Wireless configuration page appears.



2. Select **Enable wireless access points**.
3. Adjacent to **Access point 1** or **Access point 2**, click **Configure**.
   The Wireless Access Point configuration dialog box appears.



4. Select the **Enable wireless bridge to a Trusted or Optional interface** check box.
5. In the drop-down list adjacent to **Enable wireless bridge to a Trusted or Optional interface**, select a trusted or optional interface.

   Trusted

   Any wireless clients on the trusted network have full access to computers on the trusted and optional networks, and access to the Internet as defined in the outgoing firewall rules on your XTM device.
   If the wireless client sets the IP address on its wireless network card with DHCP, the DHCP server on the optional network of the XTM device must be active and configured.

   Optional

   Any wireless clients on the optional network have full access to computers on the optional network, and access to the Internet as defined in the outgoing firewall rules on your XTM device.
   If the wireless client sets the IP address on its wireless network card with DHCP, the DHCP server on the optional network of the XTM device must be active and configured.

6. To configure the wireless interface to send and answer SSID requests, select the **Broadcast SSID and respond to SSID queries** check box.

   For information about this setting, see *Enable/Disable SSID Broadcasts* on page 173.

7. Select the **Log Authentication Events** check box if you want the XTM device to send a log message to the log file each time a wireless computer tries to connect to the interface.

   For more information about logging, see *Log Authentication Events* on page 173.

8. To require wireless users to use the Mobile VPN with IPSec client, select the **Require encrypted Mobile VPN with IPSec connections for wireless clients** check box.

   When you select this check box, the only packets the XTM device allows over the wireless network are DHCP, ICMP, IKE (UDP port 500), ARP and IPSec (IP protocol 50). If you require wireless users to use the Mobile VPN with IPSec client, it can increase the security for wireless clients if you do not select WPA or WPA2 as the wireless authentication method.

9. In the **Network name (SSID**) text box, type a unique name for your wireless optional network or use the default name.

   For information about changing the SSID, see *Change the SSID* on page 173.

10. To change the fragmentation threshold, in the **Fragmentation Threshold** text box, type a value: 256–2346. We do not recommend you change this setting.

    For more information about this setting, see *Change the Fragmentation Threshold* on page 173.

11. In the **Encryption (Authentication)** drop-down list, select the encryption and authentication to enable for wireless connections to the optional interface. We recommend that you use WPA2 if the wireless devices in your network can support WPA2.

    For more information about this setting, see *Set the Wireless Authentication Method*.

12. In the **Encryption algorithm** drop-down list, select the type of encryption to use for the wireless connection and add the keys or passwords required for the type of encryption you select. If you

select an encryption option with pre-shared keys, a random pre-shared key is generated for you. You can use this key or type your own.

For more information, see *Set the Encryption Level* on page 180.

13. Save the configuration.

> ***Note*** *If you enable wireless connections to the trusted interface, we recommend that you restrict access by MAC address. This prevents users from connecting to the XTM wireless device from unauthorized computers that could contain viruses or spyware. Click the* ***MAC Access Control*** *tab to enable MAC access control. You use this tab the same way as when you restrict network traffic on an interface as described in Restrict Network Traffic by MAC Address on page 101.*

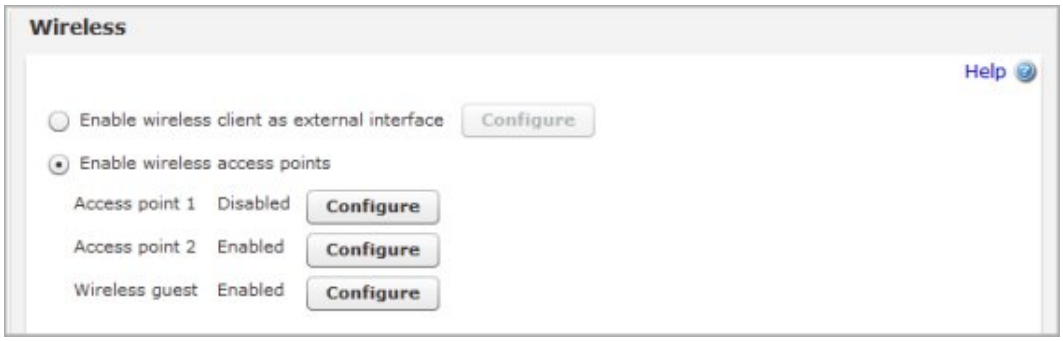
To configure a wireless guest network with no access to the computers on your trusted or optional networks, see *Enable a Wireless Guest Network* on page 184.

Enable a Wireless Guest Network

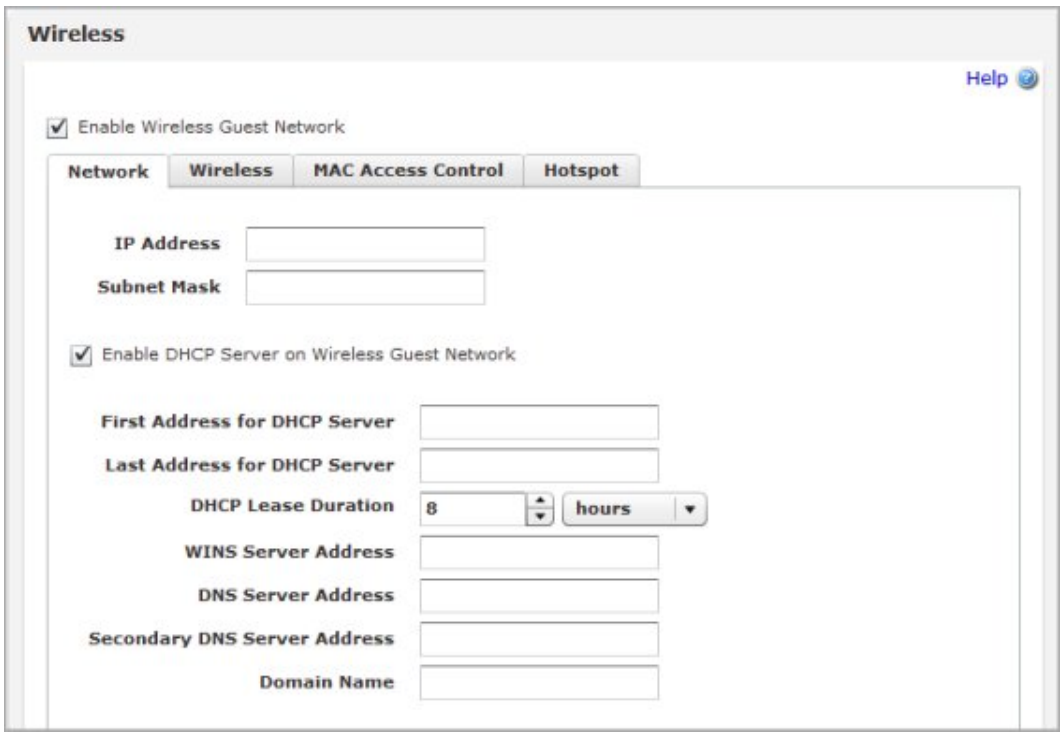
You can enable a wireless guest network to give a guest user wireless access to the Internet without access to computers on your trusted and optional networks.

To set up a wireless guest network:

1. Select **Network > Wireless**.
   The Wireless Configuration page appears.



2. Select **Enable wireless access points**.
3. Adjacent to **Wireless guest**, click **Configure**.
   The Wireless Guest Configuration dialog box appears.



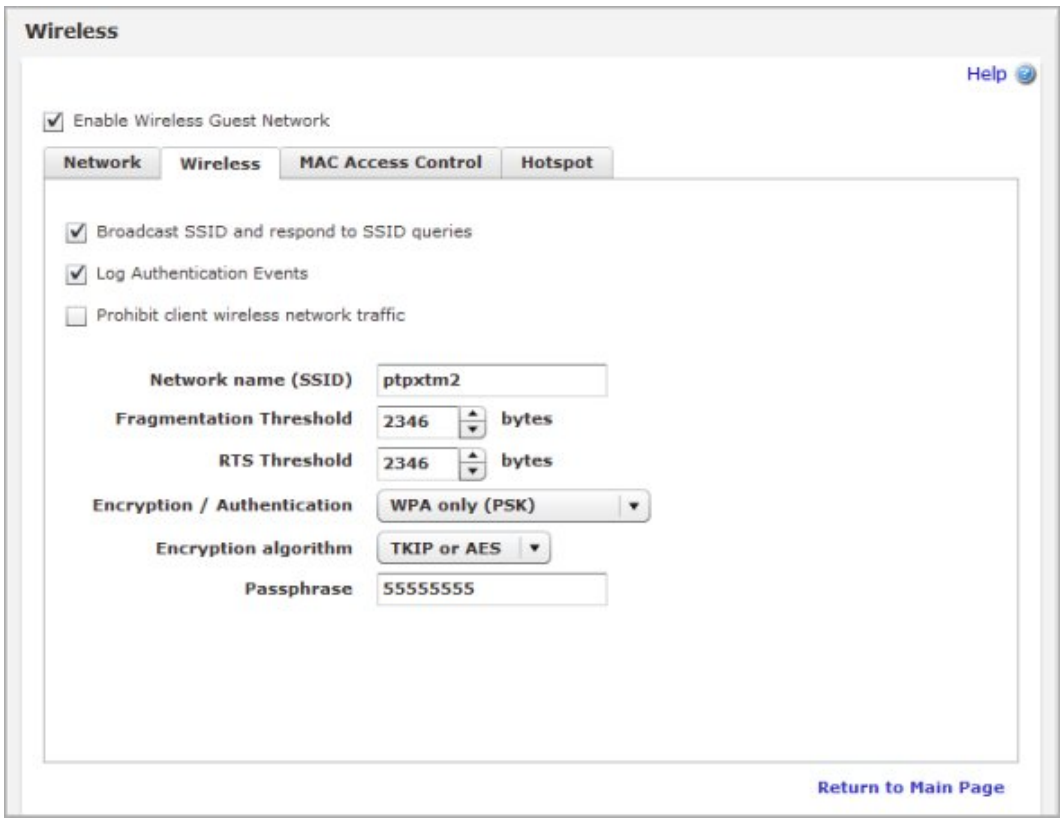
4. Select the **Enable Wireless Guest Network** check box.

   Wireless connections are allowed through the XTM device to the Internet based on the rules you have configured for outgoing access on your device. These computers have no access to computers on the trusted or optional network.

5. In the **IP Address** text box, type the private IP Address to use for the wireless guest network. The IP address you type must not already in use on one of your network interfaces.
6. In the **Subnet Mask** text box, type the subnet mask. The correct value is usually 255.255.255.0.
7. To configure the XTM device as a DHCP server when a wireless device tries to make a connection, select the **Enable DHCP Server on Wireless Guest Network** check box.

   For more information about how to configure the settings for the DHCP Server, see *Configure DHCP in Mixed Routing Mode* on page 87.

8. Click the **Wireless** tab to see the security settings for the wireless guest network.
   The Wireless settings appear.



9. Select the **Broadcast SSID and respond to SSID queries** check box to make your wireless guest network name visible to guest users.

   For information about this setting, see *Enable/Disable SSID Broadcasts* on page 173.

10. To send a log message to the log file each time a wireless computer tries to connect to the guest wireless network, select the **Log Authentication Events** check box.

    For more information about logging, see *Log Authentication Events* on page 173.

11. To allow wireless guest users to send traffic to each other, clear the **Prohibit client to client wireless network traffic** check box.
12. In the **Network name (SSID)**) text box, type a unique name for your wireless guest network or use the default name.

    For information about changing the SSID, see *Change the SSID* on page 173.

13. To change the fragmentation threshold, in the **Fragmentation Threshold** text box, type a value: 256–2346. We do not recommend you change this setting.

    For more information about this setting, see *Change the Fragmentation Threshold* on page 173.

14. In the **Authentication** drop-down list, select the type of authentication to enable for connections to the wireless guest network. The setting you choose depends on the type of guest access you want to provide, and whether you want to require your guests to enter a passphrase to use the network.

    For more information about this setting, see *Set the Wireless Authentication Method* on page 176.

15. In the **Encryption / Authentication** drop-down list, select the type of encryption to use for the wireless connection and add the keys or passwords required for the type of encryption you select. If you select an authentication option that uses pre-shared keys, a random pre-shared key is generated for you. You can use this key or type your own.

    For more information, see *Set the Encryption Level* on page 180.

16. Click **Return to Main Page**.
17. Click **Save**.

Optionally, you can configure your wireless guest network as a wireless hotspot. Click the **Hotspot** tab to enable a wireless hotspot. For more information, see *Enable a Wireless Hotspot*.

You can also restrict access to the Guest network by MAC address. Click the **MAC Access Control** tab to enable MAC access control. You use this tab the same way as when you restrict network traffic on an interface as described in *Restrict Network Traffic by MAC Address* on page 101.

Enable a Wireless Hotspot

You can configure your WatchGuard XTM wireless guest network as a wireless hotspot to give wireless Internet connectivity to your visitors or customers. When you enable the hotspot feature, you have more control over connections to your wireless guest network.

When you configure your device as a wireless hotspot you can customize:

- A splash screen that users see when they connect
- Terms and conditions that users must accept before they can browse to a web site
- Maximum length of time a user can be continuously connected

When you enable the wireless hotspot feature, the **Allow Hotspot-Users** policy is automatically created. This policy allows connections from the wireless guest interface to your external interfaces. This gives wireless hotspot users wireless access to the Internet without access to computers on your trusted and optional networks.

Before you set up a wireless hotspot, you must configure the settings for your wireless guest network as described in *Enable a Wireless Guest Network*.

To set up the wireless hotspot:

1. Select **Network > Wireless**.
2. Adjacent to **Wireless guest**, click **Configure**.
3. On the **Wireless** page, select the **Hotspot** tab.
4. Select the **Enable hotspot** check box.

Configure User Timeout Settings

You can configure timeout settings to limit the amount of time that users can continuously use your hotspot. When the timeout period expires, the user is disconnected. When a user is disconnected, the user loses all Internet connectivity but is still connected to the wireless network. The hotspot splash screen reappears, and the user must accept the Terms and Conditions again before they can continue to use the wireless hotspot.

1. In the **Session timeout** text box, specify the maximum amount of time a user can remain continuously connected to your hotspot. You can specify the unit of time with the adjacent drop-down list. If the Session timeout is set to 0 (the default value), wireless guest users are not disconnected after a specified time interval.
2. In the **Idle timeout** text box, specify the amount of time that a user must be idle for the connection to time out. You can specify the unit of time with the adjacent drop-down list. If the Idle timeout is set to 0, users are not disconnected if they do not send or receive traffic.

Customize the Hotspot Splash Screen

When users connect to your hotspot, they see a *splash screen*, or a web site they must visit before they can browse to other web sites. You can configure the text that appears on this page, and the appearance of the page. You can also redirect the user to a specified web page after they accept the terms and conditions.

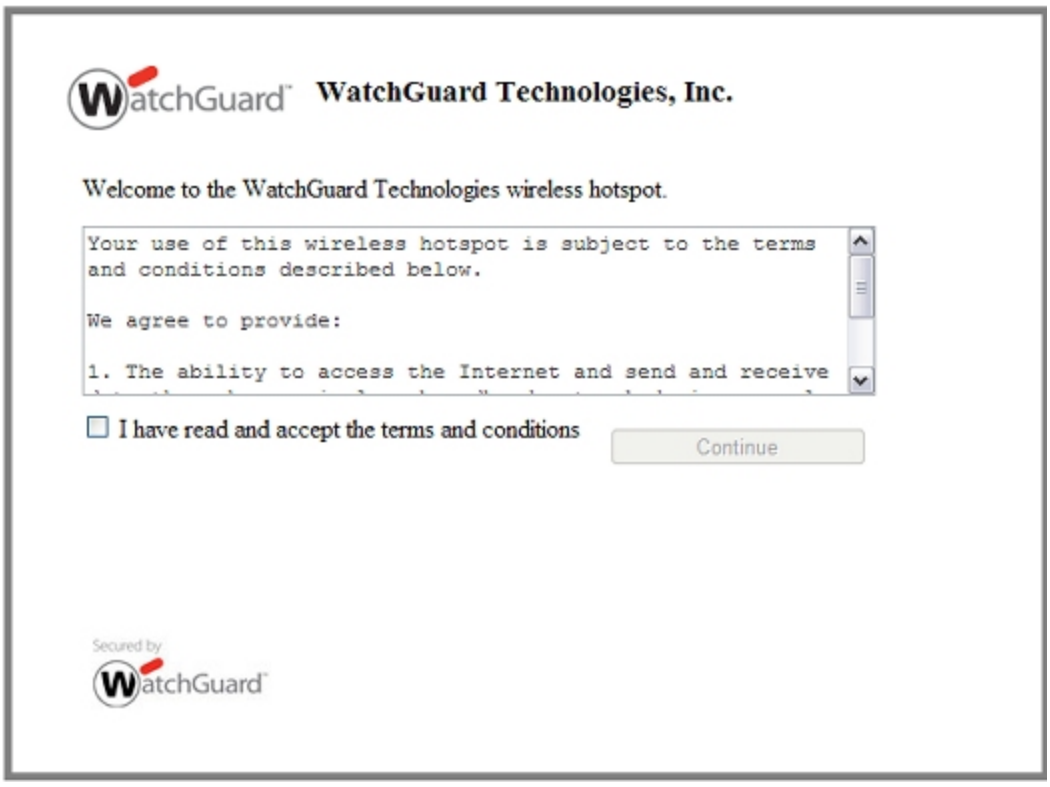
At a minimum, you must specify the **Page title** and the **Terms and Conditions** to enable this feature.

1. In the **Page title** text box, type the title text you want to appear on the hotspot splash screen.

2. To include a welcome message:
   - Select the **Welcome Message** check box.
   - In the **Welcome Message** text box, type the message your users see when they connect to the hotspot.
3. (Optional) To use a custom logo in the splash screen:
   - Select the **Use a custom logo** check box.
   - Click **Upload** to upload your custom logo file.
     The file must be in .jpg, .gif or .png format. We recommend that the image be no larger than 90 x 50 (width x height) pixels, or 50 kB.
4. In the **Terms and Conditions** text box, type or paste the text you want your users to agree to before they can use the hotspot. The maximum length is 20,000 characters.
5. To automatically redirect users to a web site after they accept the Terms and Conditions, in the **Redirect URL** text box, type the URL of the web site.
6. You can customize the fonts and colors for your Welcome page:
   - **Font** — Select the font from the **Font** drop-down list. If you do not specify a font, the Welcome page uses the browser default font for each user.
   - **Size** — Select the text size from the **Size** drop-down list. The default text size is Medium.
   - **Text Color** — This is the color for the text on the hotspot splash screen. The default color is #000000 (black). The configured color appears in a square adjacent to the Text Color text box. Click the colored square to select a different color from a color palette. Or, type the HTML color code in the **Text Color** text box.

- **Background Color** — This is the color to use for the background of the hotspot splash screen. The default color is #FFFFFF (white). The configured color appears in a square adjacent to the Background Color text box. Click the colored square to select a different color from a color palette. Or, type the HTML color code in the **Background Color** text box.

7. Click **Preview Splash Screen**.
   A preview of the splash screen appears in a new browser window.

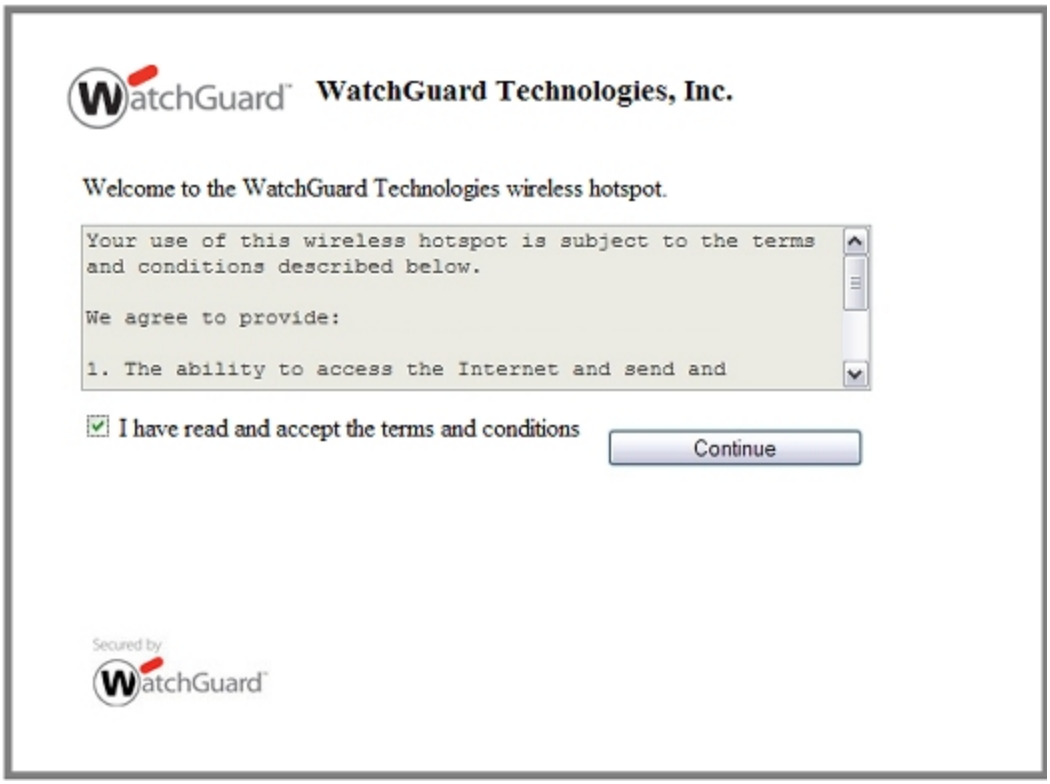


8. Close the preview browser window.
9. When you are finished with your hotspot settings, click **Return to Main Page**.
10. Click **Save** to save the settings.

Connect to a Wireless Hotspot

After you configure your wireless hotspot, you can connect to it to see the hotspot splash screen.

1. Use a wireless client to connect to your wireless guest network. Use the SSID and other settings that you configured for the wireless guest network.
2. Open a web browser. Browse to any web site.
   The wireless hotspot splash screen appears in the browser.



3. Select the **I have read and accept the terms and conditions** check box.
4. Click **Continue**.
   The browser displays the original URL you requested. Or, if the hotspot is configured to automatically redirect the browser to a URL, the browser goes to the web site.

The content and appearance of the hotspot splash screen can be configured with the hotspot settings for your wireless guest network.

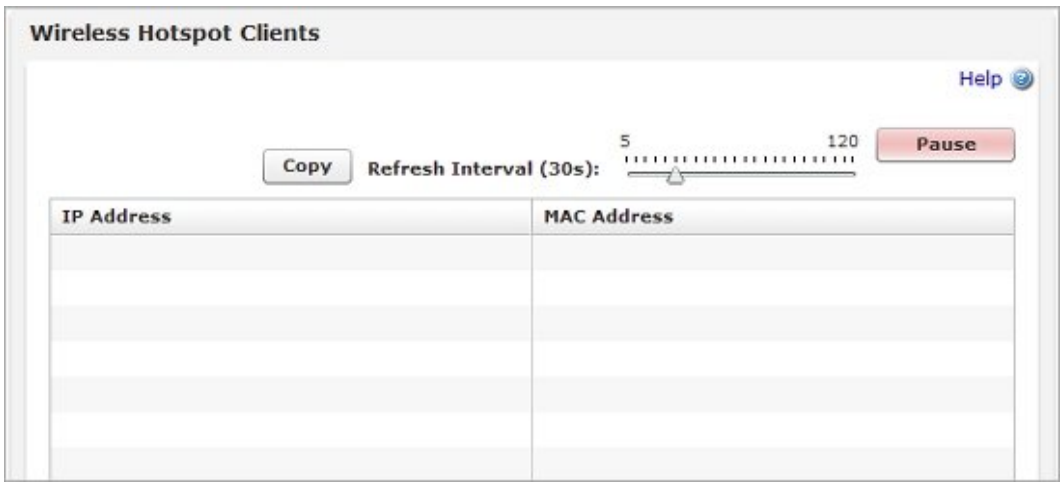
The URL of the wireless hotspot splash screen is:
`https://<IP address of the wireless guest network>:4100/hotspot`.

See Wireless Hotspot Connections

When you enable the wireless hotspot feature, you can see information about the number of wireless clients that are connected. You can also disconnect wireless clients.

To see the list of connected wireless hotspot clients:

1. Connect to Fireware XTM Web UI on your wireless device.
2. Select **System Status > Wireless Hotspot**.
   The IP address and MAC address for each connected wireless client appears.



To disconnect a wireless hotspot client, from the **Wireless Hotspot Clients**page:

1. Select one or more connected wireless hotspot clients.
2. Click **Disconnect**.

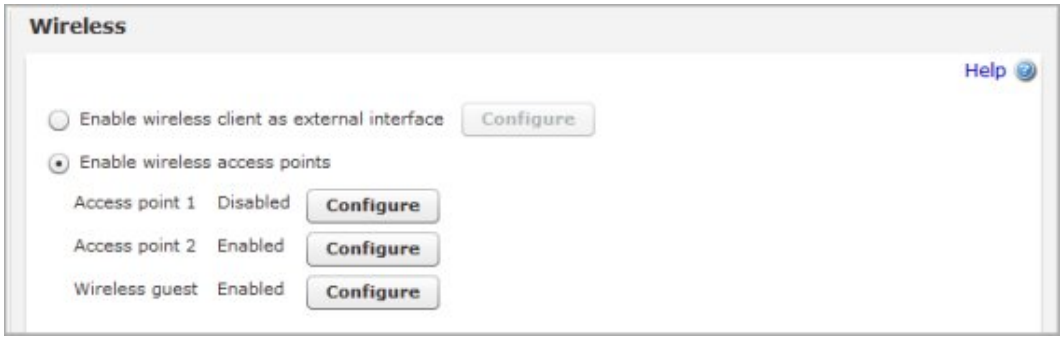
Configure Your External Interface as a Wireless Interface

In areas with limited or no existing network infrastructure, you can use your XTM wireless device to provide secure network access. You must physically connect your network devices to the XTM device. Then you configure your external interface to connect to a wireless access point that connects to a larger network.

> ***Note*** *When the external interface is configured with a wireless connection, the XTM wireless device can no longer be used as a wireless access point. To provide wireless access for users, connect a wireless access point device to the XTM wireless device.*

Configure the Primary External Interface as a Wireless Interface

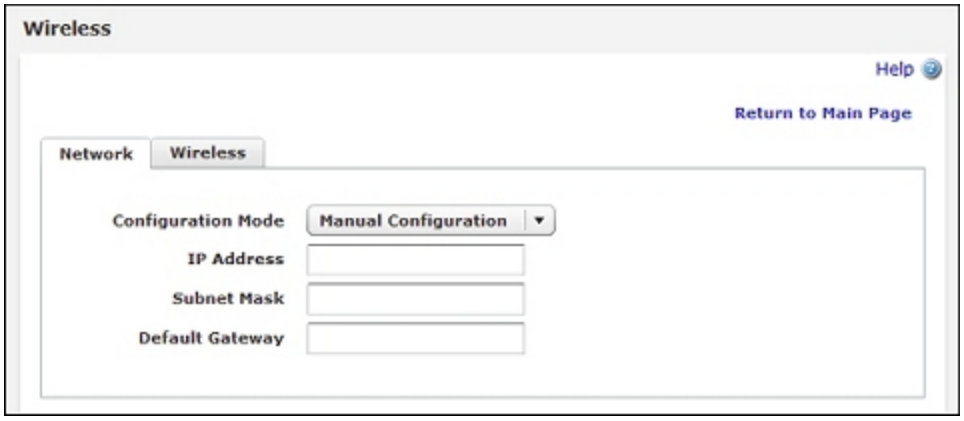
1. Select **Network > Wireless**.
   The Wireless Configuration page appears.



2. Select **Enable wireless client as external interface**.
3. Click **Configure**.
   The external interface settings appear.
4. In the **Configuration Mode** drop-down list, select an option:

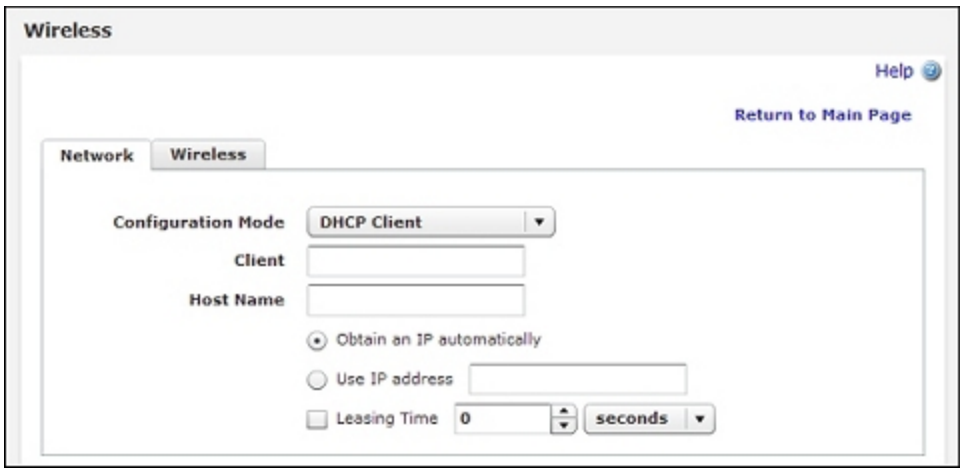
   Manual Configuration

   To use a static IP address, select this option. Type the **IP Address**, **Subnet Mask**, and **Default Gateway**.



   DHCP Client

   To configure the external interface as a DHCP client, select this option. Type the DHCP configuration settings.



For more information about how to configure the external interface to use a static IP address or DHCP, see *Configure an External Interface* on page 84.

5. Click the **Wireless** tab.
   The wireless client configuration settings appear.

6. In the **Network name (SSID)** text box, type a unique name for your wireless external network.
7. In the **Authentication** drop-down list, select the type of authentication to enable for wireless connections. We recommend that you use WPA2 if the wireless devices in your network can support WPA2.

   For more information about wireless authentication methods, see *About Wireless Security Settings* on page 176.

8. In the **Encryption** drop-down list, select the type of encryption to use for the wireless connection and add the keys or passwords required for the type of encryption you select. If you select an encryption option with pre-shared keys, a random pre-shared key is generated for you. You can use this key or type your own.

9. Click **Save**.

Configure a BOVPN tunnel for additional security

To create a wireless bridge and provide additional security, add a BOVPN tunnel between your XTM device and the external gateway. You must set the mode to **Aggressive Mode** in the Phase 1 settings of your BOVPN configuration on both devices.

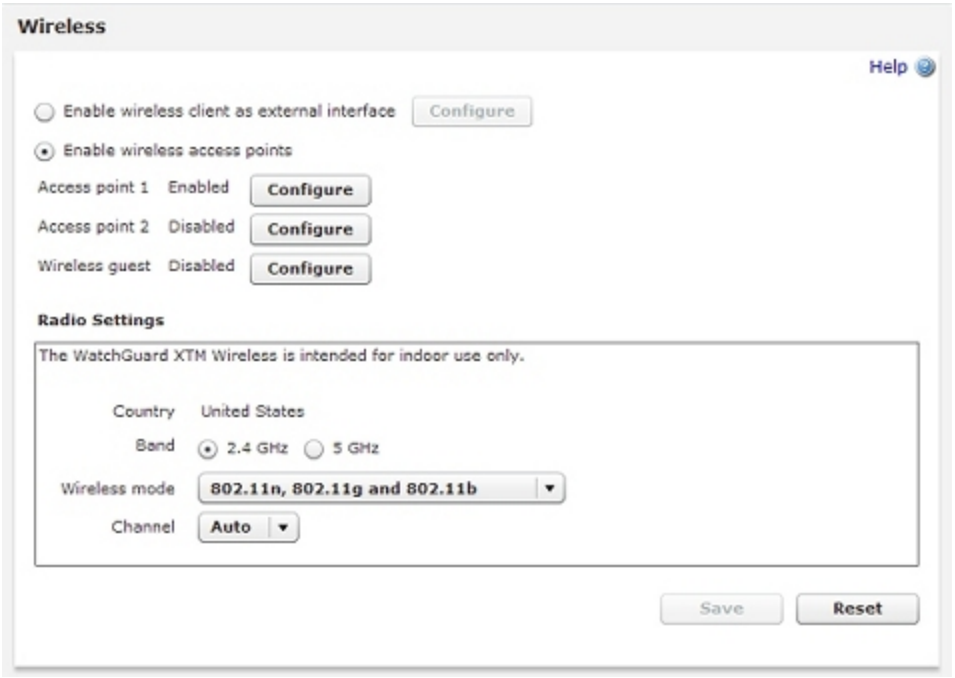
For information about how to set up a BOVPN tunnel, see *About Manual Branch Office VPN Tunnels* on page 528.

About Wireless Radio Settings

WatchGuard XTM wireless devices use radio frequency signals to send and receive traffic from computers with wireless Ethernet cards.

To view or change the radio settings:

1. *Connect to Fireware XTM Web UI*.
2. Select **Network > Wireless**.
   The Wireless page appears.



The **Radio Settings** appear at the bottom of this page.

Country is Set Automatically

Due to regulatory requirements in different parts of the world, you cannot use all wireless radio settings in every country. Each time you power on the XTM wireless device, the device contacts a WatchGuard server to determine the country and the allowed wireless radio settings for that country. To do this, the device must have an Internet connection. Once the country is determined, you can configure all supported wireless radio settings that can be used in that country.

In the Wireless Configuration dialog box, the **Country** setting shows which country the device detects it is in. You cannot change the **Country** setting. The available options for the other radio settings are based on the regulatory requirements of the country the device detects it is located in.

> ***Note*** *If the XTM wireless device cannot connect to the WatchGuard server, the country is unknown. In this case, you can only select from the limited set of wireless radio settings that are allowed in all countries. The XTM wireless device periodically continues to retry to connect to the WatchGuard server to determine the country and allowed wireless radio settings.*

If the XTM wireless device does not have a region set yet, or if the region is not up to date, you can force the device to update the wireless radio region.

To update the Wireless Radio Region:

1. Select **System Status > Wireless Statistics**.
2. Click **Update Country Info**.
   The 2 Series device contacts a WatchGuard server to determine the current operating region.

Select the Band and Wireless Mode

The WatchGuard XTM wireless device supports two different wireless bands, 2.4 GHz and 5 GHz. The the band you select and the country determine the wireless modes available. Select the **Band** that supports the wireless mode you want to use. Then select the mode from the **Wireless mode** drop-down list.

The 2.4 GHz band supports these wireless modes:

802.11n, 802.11g and 802.11b

This is the default mode in the 2.4 GHz band, and is the recommended setting. This mode allows the XTM wireless device to connect with devices that use 802.11n, 802.11g, or 802.11b.

802.11g and 802.11b

This mode allows the XTM wireless device to connect to devices that use 802.11g or 802.11b.

802.11b ONLY

This mode allows the XTM wireless device to connect only to devices that use 802.11b.

The 5 GHz band supports these wireless modes:

802.11a and 802.11n

This is the default mode in 5 GHz band. This mode allows the XTM wireless device to connect to devices that use 802.11a or 802.11n.

802.11a ONLY

This mode allows the XTM wireless device to connect only to devices that use 802.11a.

> ***Note*** *If you choose a wireless mode that supports multiple 802.11 standards, the overall performance can drop considerably. This is partly because of the need for backward compatibility when devices that use slower modes are connected. The slower devices tend to dominate the throughput because it can take much longer to send or receive the same amount of data to devices that use a slower mode.*

The 5 GHz band provides greater performance than the 2.4 GHz band, but may not be compatible with all wireless devices. Select the band and mode based on the wireless cards in the devices that will connect to the XTM wireless device.

Select the Channel

The available channels depend on the country and the wireless mode you select. By default, the **Channel** is set to **Auto**. When the channel is set to Auto, the XTM wireless device automatically selects a quiet channel from the available list in the band you have selected. Or you can select a specific channel from the **Channel** drop-down list.

Configure the Wireless Card on Your Computer

These instructions are for the Windows XP with Service Pack 2 operating system. For installation instructions for other operating systems, see your operating system documentation or help files.

1. Select **Start > Settings > Control Panel > Network Connections**.
   The Network Connections dialog box appears.
2. Right-click **Wireless Network Connection** and select **Properties**.
   The Wireless Network Connection dialog box appears.
3. Select the **Wireless Networks** tab.
4. Below **Preferred Networks**, click **Add**.
   The Wireless Network Properties dialog box appears.
5. Type the SSID in the **Network Name (SSID)** text box.
6. Select the network authentication and data encryption methods in the drop-down lists. If necessary, clear **The key is provided for me automatically** check box and type the network key two times.
7. Click **OK** to close the **Wireless Network Properties** dialog box.
8. Click **View Wireless Networks**.
   All available wireless connections appear in the Available Networks text box.
9. Select the SSID of the wireless network and click **Connect**.

   If the network uses encryption, type the network key twice in the Wireless Network Connection dialog box and click **Connect** again.
10. Configure the wireless computer to use DHCP.

Rogue Access Point Detection

You can configure your XTM wireless device to detect (unknown) wireless access points that operate in the same area. A rogue access point is any wireless access point within range of your network that is not recognized as an authorized access point. When you enable rogue access point detection on your XTM wireless device, the wireless radio in the device scans wireless channels to identify unknown wireless access points. You can configure the scan to run continuously, or to run at a scheduled interval and time of day.

When a rogue access point scan begins, the XTM wireless device scans the airwaves within range for other radio broadcasts.The device scans for wireless access points in 802.11a, 802.11b, 802.11g, and 802.11n wireless modes on all available wireless channels for the country where the device is located. The scan is not limited to the wireless mode and channel settings configured in the radio settings of your device.

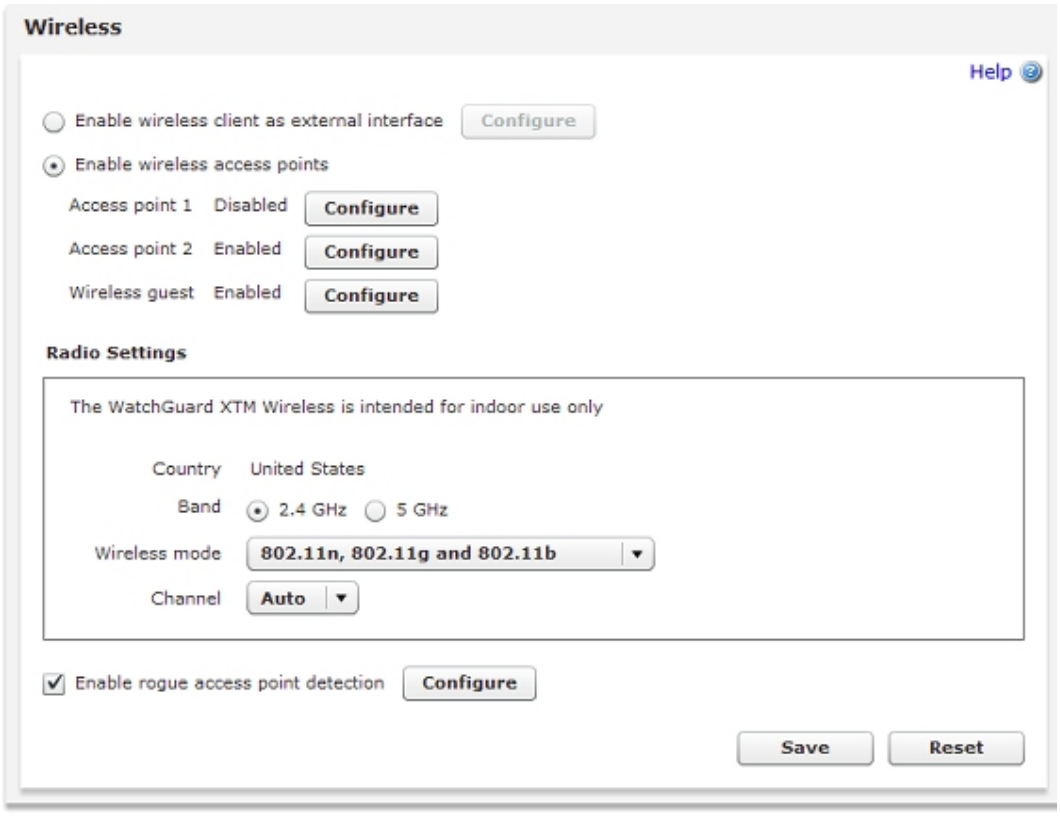
When the XTM wireless device detects the signal of another wireless access point, it compares the characteristics of the access point to a list of trusted access points that you configure. If the discovered access point does not match any trusted access point, the XTM device reports the device as a potential rogue access point. You can configure the device to send an alarm when a rogue access point is detected. If you enable logging, you can run a report of all scans and scan results.

Enable Rogue Access Point Detection

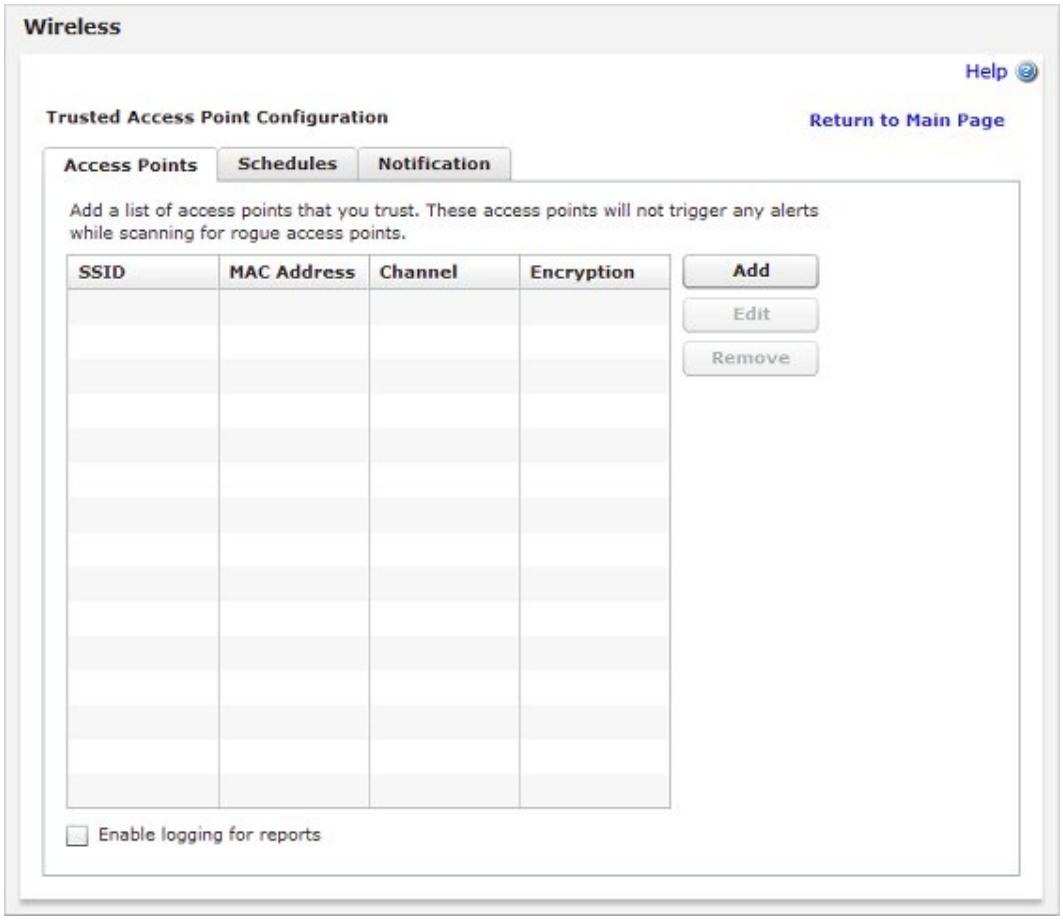
To configure rogue access point detection on your XTM wireless device, you need to know the configuration of the other wireless access points on your network; this enables you to identify them as trusted in your configuration. You can then set up a schedule for rogue access point detection scans.

Configure Rogue Access Point Detection

1. Select **Network > Wireless**.
   The Wireless page appears.



2. Select the **Enable rogue access point detection** check box.
3. Adjacent to the **Enable rogue access point detection** check box, click **Configure**.
   The Trusted Access Point Configuration page appears.



On the **Access Points** tab you can add information about all other trusted wireless access points on your network so the rogue access point scan does not identify them as potential rogue access points.

Add a Trusted Access Point

1. To add a trusted access point to the list, click **Add**.
   The Trusted access point dialog box appears.

In the **Trusted access point** dialog box, provide as much information as you can to identify your trusted access point. The more information you provide, the more likely it is that a rogue access point detection scan can correctly identify a trusted access point.

2. In the **Network name (SSID)** text box, type the SSID of the trusted access point.
3. In the **MAC address (Optional)** text box, type the wireless MAC address of the trusted access point. If your trusted access point is an XTM wireless device, see *Find the Wireless MAC Address of a Trusted Access Point*.
4. From the **Channel** drop-down list, select the channel used by the trusted access point. If the trusted access point is a WatchGuard device and the **Channel** in the radio settings of that trusted wireless device is set to **Auto**, select **Any**.
5. From the **Encryption** drop-down list, select the encryption method used by the trusted access point. *The WPA or WPA2 authentication and encryption settings that apply to the encryption method you select are enabled.*

6. If you select **WPA** or **WPA/WPA2** as the encryption method, configure the WPA settings to match the configuration of your trusted access point.
   Or, if you do not know these settings, select the **Match any authentication and encryption algorithms** check box.
7. If you selected **WPA2** or **WPA/WPA2** as the encryption method, configure the WPA settings to match the configuration of your trusted access point.
   Or, if you do not know these settings, select the **Match any authentication and encryption algorithms** check box.
8. Click **OK**.
   The trusted access point is added to the list of trusted access points.

For information about how to add an XTM 2 Series device as a trusted access point, see *Add an XTM Wireless Device as a Trusted Access Point*.

Edit or Remove a Trusted Access Point

To edit a trusted access point:

1. Select the access point in the list.
2. Click **Edit**.
3. Edit the information used to identify the trusted access point as described in the previous section.

To remove a trusted access point, select the access point in the list and click **Remove**.

Configure Logging and Notification

You must enable logging to see information about rogue access point scans in a report. When you enable logging, the log records the start and stop time, and the results of each scan. To enable logging, select the **Enable logging for reports** check box.

You can also configure the device to notify you when a rogue access point is detected. To configure notification:

1. Click the **Notification** tab.
2. Select a notification method: SNMP trap, email message, or pop-up window.

For more information about notification settings, see *Set Logging and Notification Preferences* on page 466.

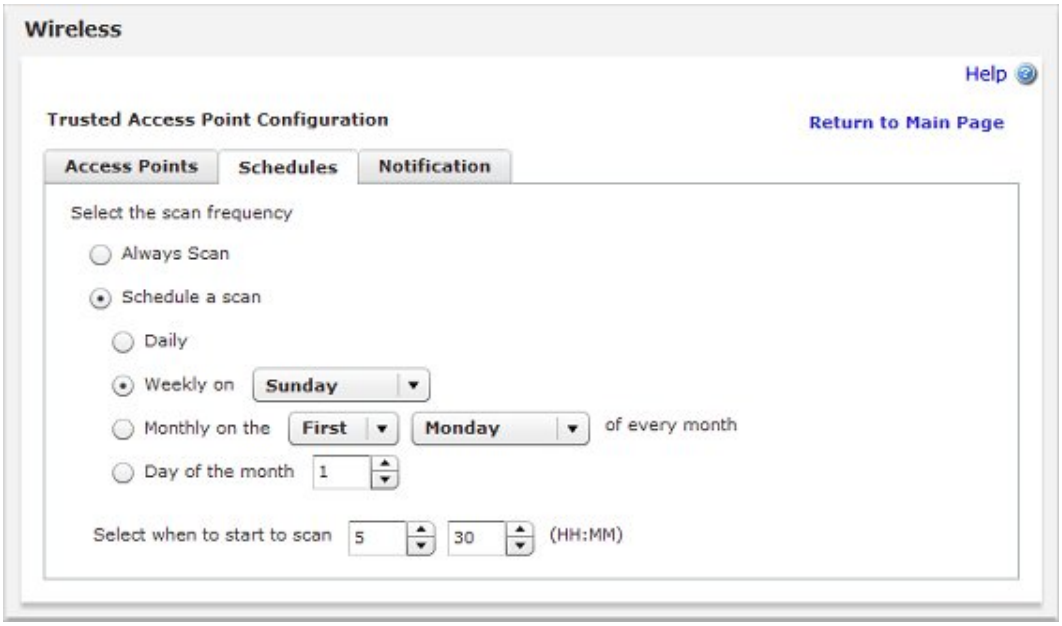
Set the Scan Frequency

If you enable rogue access point detection on an XTM wireless device that is also configured as a wireless access point, the device alternates between the two functions. When a rogue access point scan is not in progress, the device operates as wireless access point. When a rogue access point scan begins, the XTM device access point functionality is temporarily disabled, and wireless clients cannot connect to the XTM wireless device until the scan completes. You cannot set the scan frequency to **Always scan** if your device is also configured as a wireless access point.

If your XTM wireless device is configured to operate as a wireless client, the rogue access point scan does not interrupt the wireless connection, but it does decrease the throughput of the wireless connection while the scan is in progress.

To set the scan frequency:

1. In the **Trusted Access Point Configuration** dialog box, select the **Schedules** tab.



2. Select the scan frequency.
   - Select **Always scan** to automatically scan for rogue access points every 15 minutes.
   - Select **Schedule a scan** to scan on a periodic schedule.
3. If you selected **Schedule a scan**, select how often the scan should run (daily, weekly, or monthly) and select the time of day to start the scan.
4. Click **Return to Main Page**.
5. Click **Save**.

If you have added information about some trusted access points but still need to collect information about other trusted access points, you might not be ready to enable the rogue access point scan. To disable rogue access point detection scans, in the Wireless Configuration page, clear the **Enable rogue access point detection** check box. When you disable rogue access point detection, your trusted access point information is saved, but the device does not scan for rogue access points.

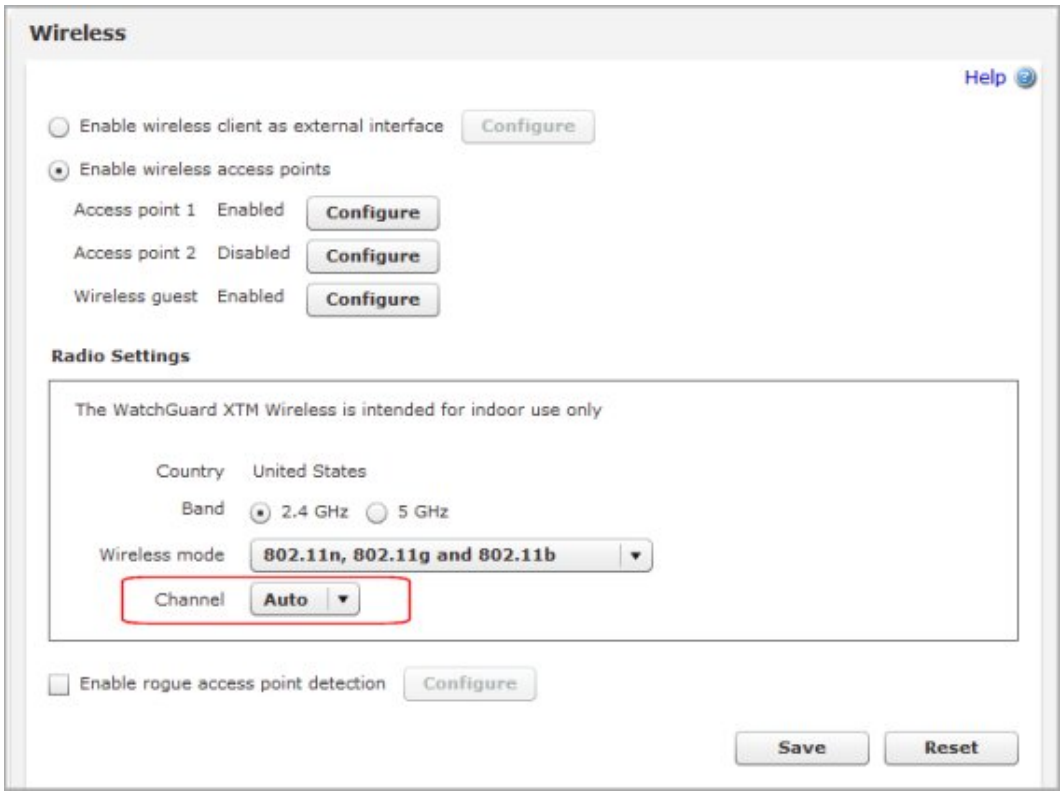
Add an XTM Wireless Device as a Trusted Access Point

If you have multiple wireless access points, you must add their information to the rogue access point detection configuration's trusted access points list. The wireless settings you can select to identify a trusted wireless access point are similar to the settings you use to configure an XTM wireless device as a wireless access point. Use these steps to find the settings for your XTM wireless device so you can add it to the trusted access point list.

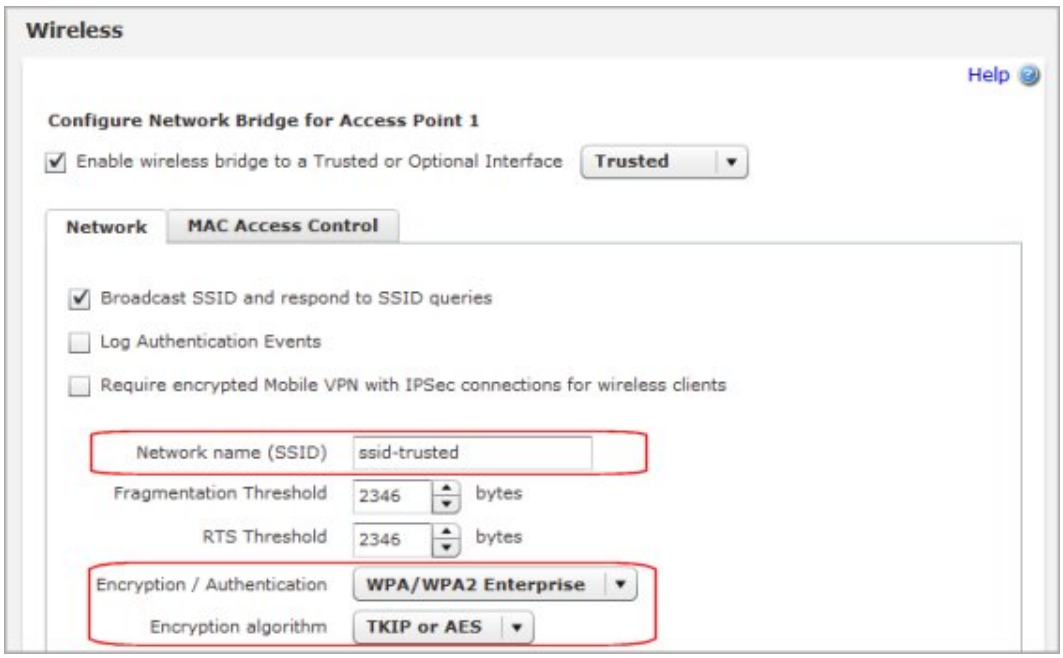
Find the Settings for Your XTM Trusted Access Points

To find the required settings to identify a trusted access point:

1. Select **Network > Wireless**.
   The Wireless Configuration dialog box appears.



2. In the **Radio Settings** section, make a note of the **Channel**.
3. Click **Configure** adjacent to the enabled wireless access point name.
   The Wireless settings for this access point appear.



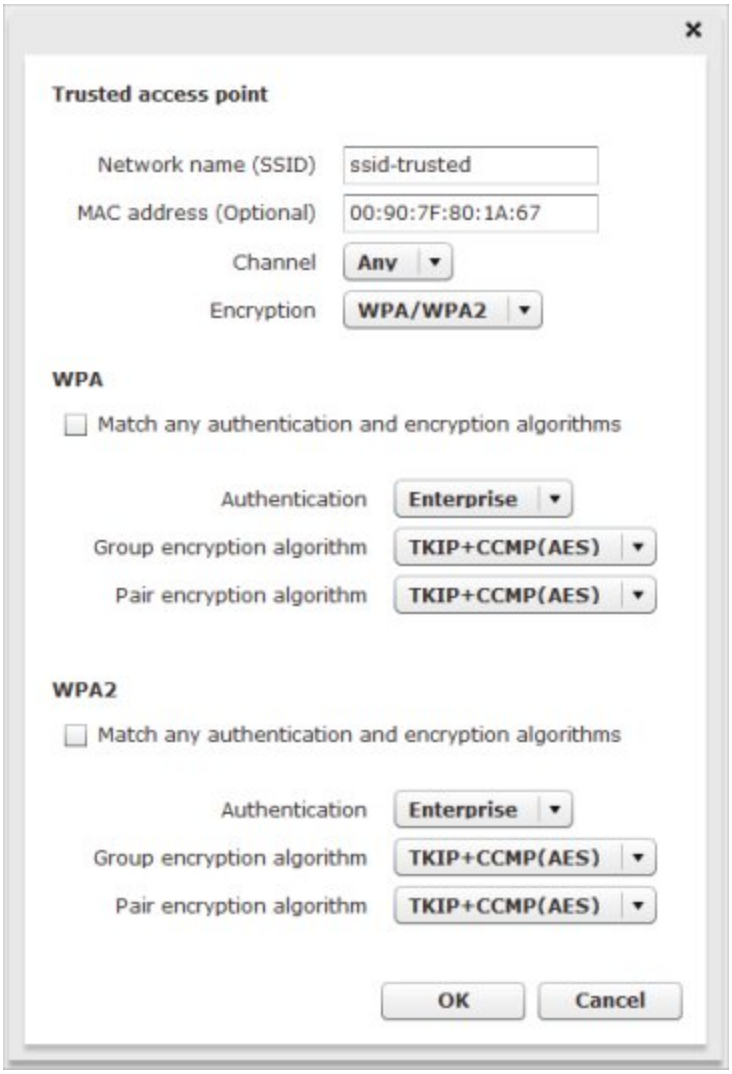
4. Make a note of these settings:
   - Network name (SSID)
   - Encryption / Authentication
   - Encryption algorithm
5. Find the wireless MAC address. For an XTM 2 Series wireless device, the wireless MAC address is six higher than the MAC address of the Eth0 interface.
   For more information, see *Find the Wireless MAC Address of a Trusted Access Point*.

An XTM wireless device can have up to three enabled wireless access points with different settings. If the XTM wireless device has multiple enabled access points, repeat these steps to get the information about each enabled access point. Repeat these steps for any other trusted access points on your network.

Add the Trusted Access Points to the Trusted Access Point List

On the wireless device that performs the rogue access point scan:

1. Select **Network > Wireless**.
2. Adjacent to **Enable rogue access point detection**, click **Configure**.
   The list of trusted access points appears.
3. Click **Add**.
   The Trusted access point page appears.



4. Type or select the information to match the configuration of your trusted access point.
   For more information about these settings, see *Enable Rogue Access Point Detection*.

> ***Note*** *The **Encryption / Authentication** setting in the wireless network configuration corresponds to two settings (**Encryption** and **Authentication**) in the Trusted Access Point configuration.*

5. Click **OK** to add the trusted access point.

Repeat these steps to add other trusted wireless access points.

Find the Wireless MAC Address of a Trusted Access Point

When you enable rogue access point detection, you can specify the wireless MAC address of your other trusted wireless access points so they can be identified as trusted.

For an XTM 2 Series wireless device, the wireless MAC address is six higher than the MAC address of the Eth0 interface. So, for example, if the Eth0 Interface on the 2 Series wireless device has a MAC address of `00:90:7F:80:1A:61`, the wireless MAC address for that device is `00:90:7F:80:1A:67`.

To see the Eth0 interface MAC address, select **System Status > Interfaces**.

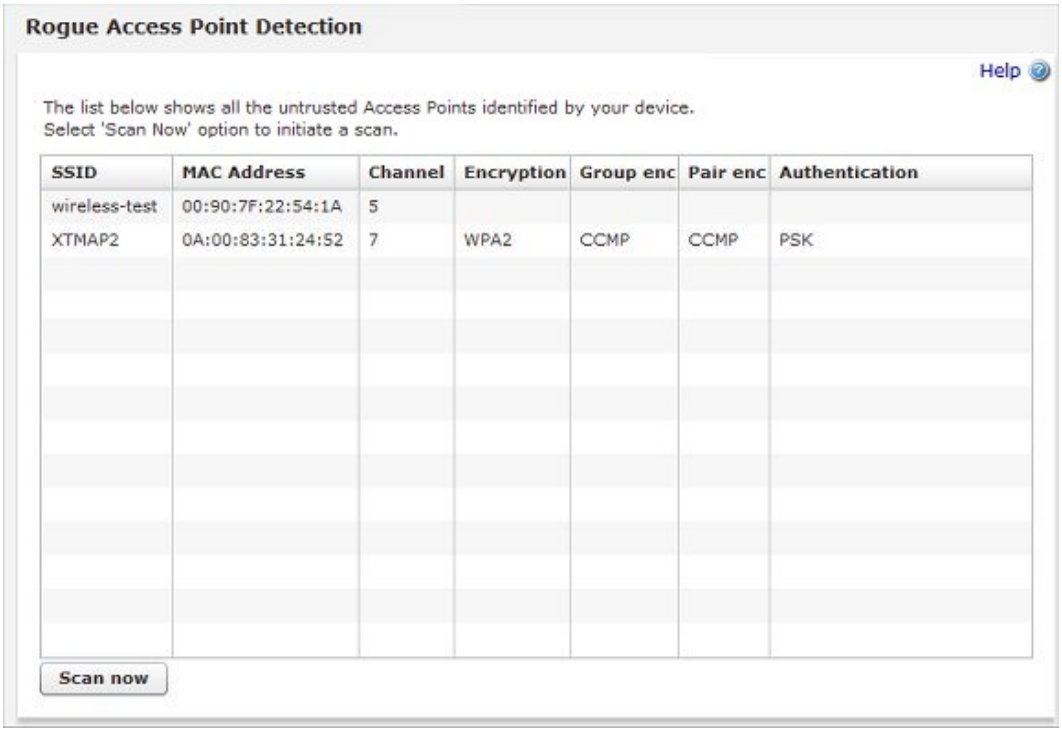
You can also see the wireless MAC address of a WatchGuard wireless device in the Status Report in Firebox System Manager. For more information, see the WatchGuard System Manager User Guide or online help system.

Rogue Access Point Scan Results

You can see the results of a wireless rogue access detection point scan in the **Rogue Access Point Detection** (Wireless Intrusion Detection System) page. This page displays a list of untrusted wireless access points found by the most recent rogue access point detection scan. This list does not include access points that match the trusted access points defined in your wireless rogue access point detection configuration.

To see and update the list:

1. Select **System Status > Rogue AP Detection**.
   The Rogue Access Point Detection system status page appears.



2. To start an immediate scan for rogue access points, click **Scan now**.
   The wireless access point starts a rogue access point detection scan and updates the list of untrusted access points.

If a trusted access point appears on this list, it is because you have not yet added it as a trusted access point. For information about how to add an access point to the trusted access point list, see *Enable Rogue Access Point Detection*.

10 Dynamic Routing

About Dynamic Routing

A routing protocol is the language a router speaks with other routers to share information about the status of network routing tables. With static routing, routing tables are set and do not change. If a router on the remote path fails, a packet cannot get to its destination. Dynamic routing makes automatic updates to route tables as the configuration of a network changes.

> ***Note*** *Support for some dynamic routing protocols is available only on Fireware XTM with a Pro upgrade.*

Fireware XTM supports the RIP v1 and RIP v2 protocols. Fireware XTM with a Pro upgrade supports the RIP v1, RIP v2, OSPF, and BGP v4 protocols.

About Routing Daemon Configuration Files

To use any of the dynamic routing protocols with Fireware XTM, you must type a dynamic routing configuration file for the routing daemon you choose. This configuration file includes information such as a password and log file name. To see sample configuration files for each of the routing protocols, see these topics:

- *Sample RIP Routing Configuration File*
- *Sample OSPF Routing Configuration File*
- *Sample BGP Routing Configuration File*

Notes about configuration files:

- The "!" and "#" characters are placed before comments, which are lines of text in configuration files that explain the function of subsequent commands. If the first character of a line is a comment character, then the rest of the line is interpreted as a comment.
- You can use the word "no" at the beginning of the line to disable a command. For example: "no network 10.0.0.0/24 area 0.0.0.0" disables the backbone area on the specified network.

About Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is used to manage router information in a self-contained network, such as a corporate LAN or a private WAN. With RIP, a gateway host sends its routing table to the closest router each 30 seconds. This router, then sends the contents of its routing tables to neighboring routers.

RIP is best for small networks. This is because the transmission of the full routing table each 30 seconds can put a large traffic load on the network, and because RIP tables are limited to 15 hops. OSPF is a better alternative for larger networks.

There are two versions of RIP. RIP v1 uses a UDP broadcast over port 520 to send updates to routing tables. RIP v2 uses multicast to send routing table updates.

Routing Information Protocol (RIP) Commands

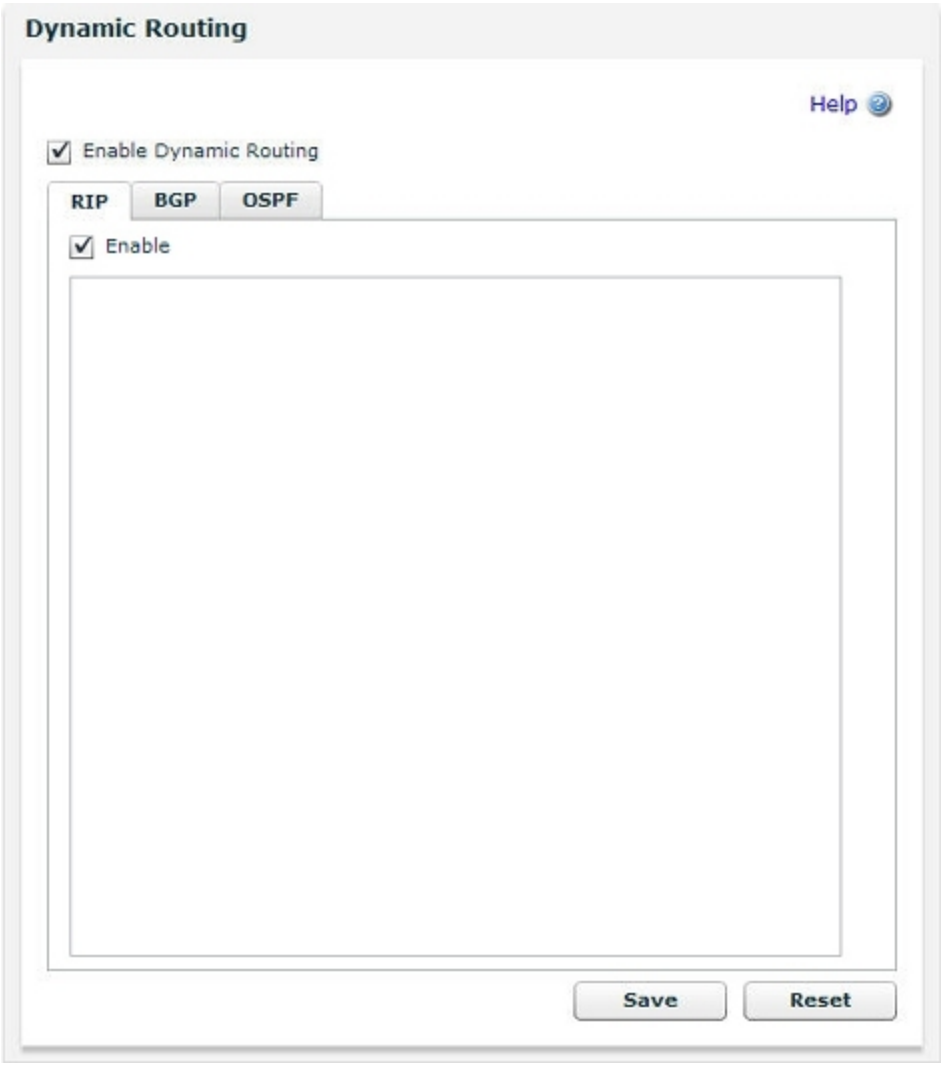
The subsequent table is a catalog of supported routing commands for RIP v1 and RIP v2 that you can use to create or modify a routing configuration file. If you use RIP v2, you must include the subnet mask with any command that uses a network IP address or RIP v2 will not operate. The sections must appear in the configuration file in the same order they appear in this table.

Section	Command	Description
Set simple password or MD5 authentication on an interface		
	interface eth [N]	Begin section to set
		Authentication type for interface
	ip rip authentication string [PASSWORD]	Set RIP authentication password
	key chain [KEY-CHAIN]	Set MD5 key chain name
	key [INTEGER]	Set MD5 key number
	key-string [AUTH-KEY]	Set MD5 authentication key
	ip rip authentication mode md5	Use MD5 authentication
	ip rip authentication mode key-chain [KEY-CHAIN]	Set MD5 authentication key-chain
Configure RIP routing daemon		
	router rip	Enable RIP daemon
	version [1/2]	Set RIP version to 1 or 2 (default version 2)
	ip rip send version [1/2]	Set RIP to send version 1 or 2
	ip rip receive version [1/2]	Set RIP to receive version 1 or 2
	no ip split-horizon	Disable split-horizon; enabled by default

Section	Command	Description
Configure interfaces and networks		
	no network eth[N]	
	passive-interface eth[N]	
	passive-interface default	
	network [A.B.C.D/M]	
	neighbor [A.B.C.D/M]	
Distribute routes to RIP peers and inject OSPF or BGP routes to RIP routing table		
	default-information originate	Share route of last resort (default route) with RIP peers
	redistribute kernel	Redistribute firewall static routes to RIP peers
	redistribute connected	Redistribute routes from all interfaces to RIP peers
	redistribute connected route-map [MAPNAME]	Redistribute routes from all interfaces to RIP peers, with a route map filter (mapname)
	redistribute ospf	Redistribute routes from OSPF to RIP
	redistribute ospf route-map [MAPNAME]	Redistribute routes from OSPF to RIP, with a route map filter (mapname)
	redistribute bgp	Redistribute routes from BGP to RIP
	redistribute bgp route-map [MAPNAME]	Redistribute routes from BGP to RIP, with a route map filter (mapname)
Configure route redistribution filters with route maps and access lists		
	access-list [PERMIT|DENY] [LISTNAME] [A,B,C,D/M | ANY]	Create an access list to allow or deny redistribution of only one IP address or for all IP addresses
	route-map [MAPNAME] permit [N]	Create a route map with a name and allow with a priority of N
	match ip address [LISTNAME]	

Configure the XTM Device to Use RIP v1

1. Select **Network > Dynamic Routing**.
   The Dynamic Routing Setup page appears.
2. Select the **Enable Dynamic Routing** check box.
3. Click the **RIP** tab.



4. Select the **Enable** check box.
5. Copy and paste the text of your routing daemon configuration file in the window.
6. Click **Save**.

For more information, see *About Routing Daemon Configuration Files* on page 209.

Allow RIP v1 Traffic Through the XTM Device

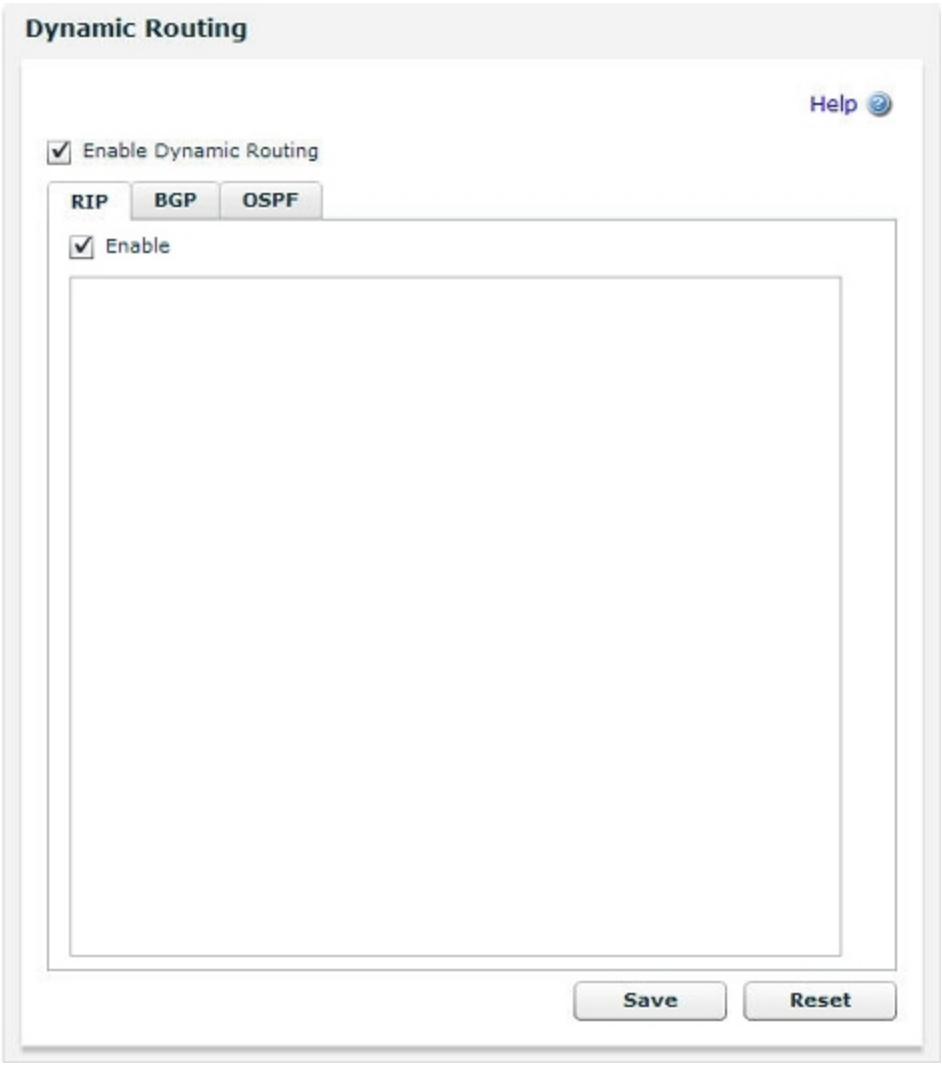
You must add and configure a policy to allow RIP broadcasts from the router to the network broadcast IP address. You must also add the IP address of the XTM device interface to the **To** section.

1. Select **Firewall > Firewall Policies**. Click  .
   The Select a Policy Type page appears.
2. From the list of packet filters, select **RIP**. Click **Add Policy**.
3. On the **Policy Configuration** page, configure the policy to allow traffic from the IP or network address of the router that uses RIP to the XTM device interface to which it connects. You must also add the network broadcast IP address.
4. Click **Save**.
5. Set up the router you selected in Step 3.
6. After you configure the router, select **System Status > Routes** and verify the XTM device and the router are sending updates to each other.

   You can then add authentication and restrict the RIP policy to listen only on the correct interfaces.

Configure the XTM Device to Use RIP v2

1. Select **Network > Dynamic Routing**.
   The Dynamic Routing Setup page appears.
2. Select the **Enable Dynamic Routing** check box.
3. Select the **RIP** tab.



4. Select the **Enable** check box.
5. Copy and paste your routing daemon configuration file in the window.
6. Click **Save**.

For more information, see *About Routing Daemon Configuration Files* on page 209.

Allow RIP v2 Traffic Through the XTM Device

You must add and configure a policy to allow RIP v2 multicasts from the routers that have RIP v2 enabled to the reserved multicast IP address for RIP v2.

1. Select **Firewall > Firewall Policies**. Click ..
   The Select a Policy Type page appears.
2. From the list of packet filters, select **RIP**. Click **Add Policy**.
3. On the **Policy Configuration** page, configure the policy to allow traffic from the IP or network address of the router that uses RIP to the multicast address 224.0.0.9.
4. Click **Save**.
5. Set up the router you selected in Step 3.
6. After you configure the router, select **System Status > Routes** and verify the XTM device and the router are sending updates to each other.

   You can then add authentication and restrict the RIP policy to listen only on the correct interfaces.

Sample RIP Routing Configuration File

To use any of the dynamic routing protocols with Fireware XTM, you must copy and paste a configuration file for the dynamic routing daemon. This topic includes a sample configuration file for the RIP routing daemon. If you want to use this configuration file as a base for your own configuration file, copy the text into an application such as Notepad or Wordpad and save it with a new name. You can then edit the parameters to meet the requirements of your organization.

Optional commands are commented with the "!" character. To enable a command, delete the "!" and modify variables as necessary.

```
!! SECTION 1: Configure MD5 authentication keychains.
! Set MD5 authentication key chain name (KEYCHAIN), key number (1),
! and authentication key string (AUTHKEY).
! key chain KEYCHAIN
! key 1 ! key-string AUTHKEY
!! SECTION 2: Configure interface properties.
! Set authentication for interface (eth1).
! interface eth1
!
! Set RIP simple authentication password (SHAREDKEY).
! ip rip authentication string SHAREDKEY
!
! Set RIP MD5 authentication and MD5 keychain (KEYCHAIN).
! ip rip authentication mode md5
! ip rip authentication key-chain KEYCHAIN
!
!! SECTION 3: Configure global RIP daemon properties.
! Enable RIP daemon. Must be enabled for all RIP configurations. router rip
!
! Set RIP version to 1; default is version 2.
! version 1
!
! Set RIP to send or received to version 1; default is version 2.
! ip rip send version 1
! ip rip receive version 1
!
! Disable split-horizon to prevent routing loop. Default is enabled.
! no ip split-horizon
!! SECTION 4: Configure interfaces and networks.
! Disable RIP send and receive on interface (eth0).
! no network eth0
!
! Set RIP to receive-only on interface (eth2).
! passive-interface eth2
!
! Set RIP to receive-only on all interfaces.
! passive-interface default
!
! Enable RIP broadcast (version 1) or multicast (version 2) on
! network (192.168.253.0/24). !network 192.168.253.0/24
!
```

```
! Set unicast routing table updates to neighbor (192.168.253.254).
! neighbor 192.168.253.254
!! SECTION 5: Redistribute RIP routes to peers and inject OSPF or BGP
!! routes to RIP routing table.
! Share route of last resort (default route) from kernel routing table
! with RIP peers.
! default-information originate
!
! Redistribute firewall static routes to RIP peers.
! redistribute kernel
!
! Set route maps (MAPNAME) to restrict route redistribution in Section 6.
! Redistribute routes from all interfaces to RIP peers or with a route map
! filter (MAPNAME).
! redistribute connected
! redistribute connected route-map MAPNAME
!
! Redistribute routes from OSPF to RIP or with a route map filter (MAPNAME).
! redistribute ospf !redistribute ospf route-map MAPNAME
!
! Redistribute routes from BGP to RIP or with a route map filter (MAPNAME).
! redistribute bgp !redistribute bgp route-map MAPNAME
!! SECTION 6: Configure route redistribution filters with route maps and
!! access lists.
! Create an access list to only allow redistribution of 172.16.30.0/24.
! access-list LISTNAME permit 172.16.30.0/24
! access-list LISTNAME deny any
!
! Create a route map with name MAPNAME and allow with a priority of 10.
! route-map MAPNAME permit 10
! match ip address LISTNAME
```

About Open Shortest Path First (OSPF) Protocol

> ***Note*** *Support for this protocol is available only on Fireware XTM with a Pro upgrade.*

OSPF (Open Shortest Path First) is an interior router protocol used in larger networks. With OSPF, a router that sees a change to its routing table or that detects a change in the network immediately sends a multicast update to all other routers in the network. OSPF is different from RIP because:

- OSPF sends only the part of the routing table that has changed in its transmission. RIP sends the full routing table each time.
- OSPF sends a multicast only when its information has changed. RIP sends the routing table every 30 seconds.

Also, note the following about OSPF:

- If you have more than one OSPF area, one area must be area 0.0.0.0 (the backbone area).
- All areas must be adjacent to the backbone area. If they are not, you must configure a virtual link to the backbone area.

OSPF Commands

To create or modify a routing configuration file, you must use the correct routing commands. The subsequent table is a catalog of supported routing commands for OSPF. The sections must appear in the configuration file in the same order they appear in this table. You can also use the sample text found in the *Sample OSPF Routing Configuration File* on page 223.

Section	Command	Description
Configure Interface		
	ip ospf authentication-key [PASSWORD]	Set OSPF authentication password
	interface eth[N]	Begin section to set properties for interface
	ip ospf message-digest-key [KEY-ID] md5 [KEY]	Set MD5 authentication key ID and key
	ip ospf cost [1-65535]	Set link cost for the interface (see OSP Interface Cost table below)
	ip ospf hello-interval [1-65535]	Set interval to send hello packets; default is 10 seconds
	ip ospf dead-interval [1-65535]	Set interval after last hello from a neighbor before declaring it down; default is 40 seconds
	ip ospf retransmit-interval [1-65535]	Set interval between link-state advertisements (LSA) retransmissions; default is 5 seconds
	ip ospf transmit-delay [1-3600]	Set time required to send LSA update; default is 1 second
	ip ospf priority [0-255]	Set route priority; high value increases eligibility to become the designated router (DR)
Configure OSPF Routing Daemon		
	router ospf	Enable OSPF daemon
	ospf router-id [A.B.C.D]	set router ID for OSPF manually; router determines its own ID if not set
	ospf rfc 1583compatibility	Enable RFC 1583 compatibility (can lead to route loops)

Section	Command	Description
	ospf abr-type [cisco|ibm|shortcut|standard]	More information about this command can be found in draft-ietf-abr-o5.txt
	passive-interface eth[N]	Disable OSPF announcement on interface eth[N]
	auto-cost reference bandwidth[0-429495]	Set global cost (see OSPF cost table below); do not use with "ip ospf [COST]" command
	timers spf [0-4294967295][0-4294967295]	Set OSPF schedule delay and hold time
Enable OSPF on a Network		
*The "area" variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z].		
	network [A.B.C.D/M] area [Z]	Announce OSPF on network A.B.C.D/M for area 0.0.0.Z
Configure Properties for Backbone area or Other Areas		
The "area" variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z].		
	area [Z] range [A.B.C.D/M]	Create area 0.0.0.Z and set a classful network for the area (range and interface network and mask setting should match)
	area [Z] virtual-link [W.X.Y.Z]	Set virtual link neighbor for area 0.0.0.Z
	area [Z] stub	Set area 0.0.0.Z as a stub
	area [Z] stub no-summary	
	area [Z] authentication	Enable simple password authentication for area 0.0.0.Z
	area [Z] authentication message-digest	Enable MD5 authentication for area 0.0.0.Z
Redistribute OSPF Routes		
	default-information originate	Share route of last resort (default route) with OSPF

Section	Command	Description
	default-information originate metric [0-16777214]	Share route of last resort (default route) with OSPF, and add a metric used to generate the default route
	default-information originate always	Always share the route of last resort (default route)
	default-information originate always metric [0-16777214]	Always share the route of last resort (default route), and add a metric used to generate the default route
	redistribute connected	Redistribute routes from all interfaces to OSPF
	redistribute connected metrics	Redistribute routes from all interfaces to OSPF, and a metric used for the action
Configure Route Redistribution with Access Lists and Route Maps		
	access-list [LISTNAME] permit [A.B.C.D/M]	Create an access list to allow distribution of A.B.C.D/M
	access-lists [LISTNAME] deny any	Restrict distribution of any route map not specified above
	route-map [MAPNAME] permit [N]	Create a route map with name [MAPNAME] and allow with a priority of [N]
	match ip address [LISTNAME]	

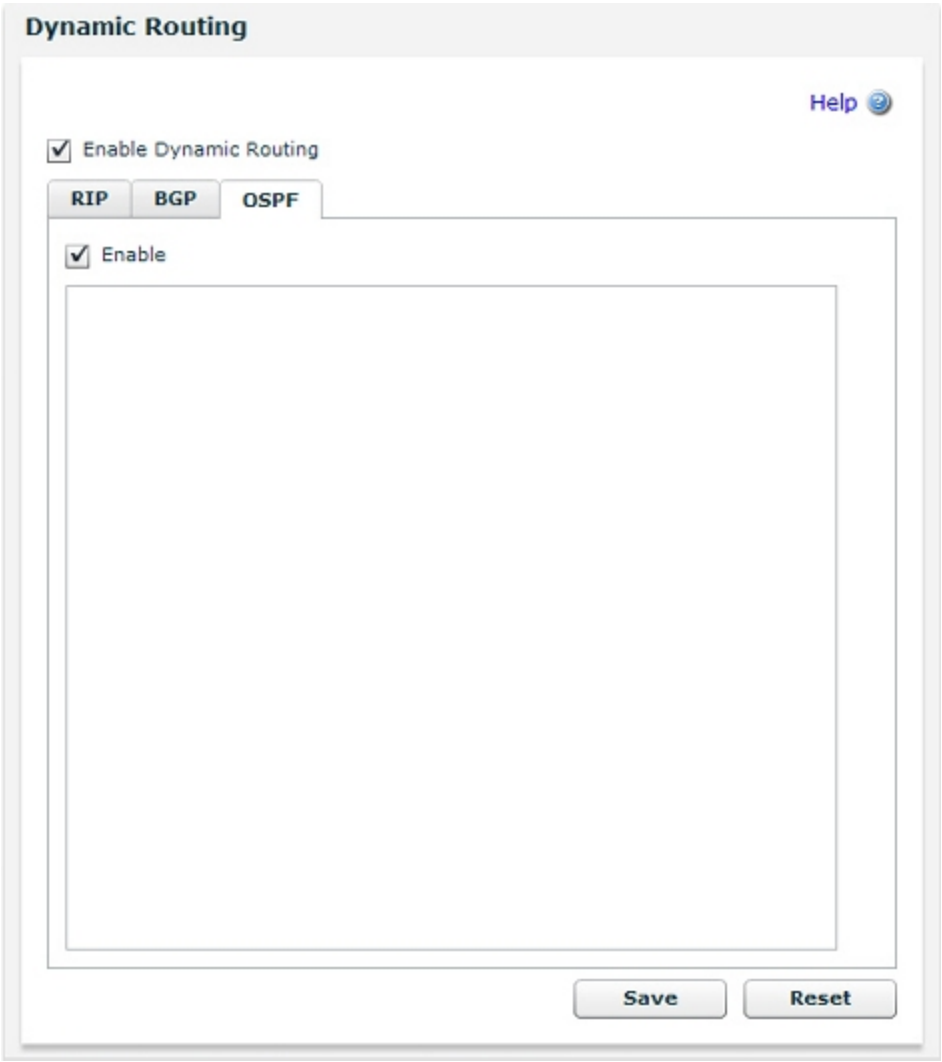
OSPF Interface Cost Table

The OSPF protocol finds the most efficient route between two points. To do this, it looks at factors such as interface link speed, the number of hops between points, and other metrics. By default, OSPF uses the actual link speed of a device to calculate the total cost of a route. You can set the interface cost manually to help maximize efficiency if, for example, your gigabyte-based firewall is connected to a 100M router. Use the numbers in this table to manually set the interface cost to a value different than the actual interface cost.

Interface Type	Bandwidth in bits/second	Bandwidth in bytes/second	OSPF Interface Cost
Ethernet	1G	128M	1
Ethernet	100M	12.5M	10
Ethernet	10M	1.25M	100
Modem	2M	256K	500
Modem	1M	128K	1000
Modem	500K	62.5K	2000
Modem	250K	31.25K	4000
Modem	125K	15625	8000
Modem	62500	7812	16000
Serial	115200	14400	10850
Serial	57600	7200	21700
Serial	38400	4800	32550
Serial	19200	2400	61120
Serial	9600	1200	65535

Configure the XTM Device to Use OSPF

1. Select **Network > Dynamic Routing**.
   The Dynamic Routing Setup page appears.
2. Select the **Enable Dynamic Routing** check box.
3. Click the **OSPF** tab.



4. Select the **Enable** check box.
5. Copy and paste your routing daemon configuration file in the window.

   For more information, see *About Routing Daemon Configuration Files* on page 209.

   To get started, you need only two commands in your OSPF configuration file. These two commands, in this order, start the OSPF process:

   `router ospf`
   `network` <network IP address of the interface you want the process to listen on and distribute through the protocol> `area` <area ID in x.x.x.x format, such as 0.0.0.0>
6. Click **Save**.

Allow OSPF Traffic Through the XTM Device

You must add and configure a policy to allow OSPF multicasts from the routers that have OSPF enabled, to the reserved multicast addresses for OSPF.

1. Select **Firewall > Firewall Policies**. Click **Add**.
   The Select a Policy Type page appears.
2. From the list of packet filters, select **OSPF**. Click **Add**.
3. On the **Policy Configuration** page, configure the policy to allow traffic from the IP or network address of the router using OSPF to the IP addresses 224.0.0.5 and 224.0.0.6.

   For information on how to set the source and destination addresses for a policy, see *Set Access Rules for a Policy* on page 307.
4. Click **Save**.
5. Set up the router you selected in Step 3.
6. After you configure the router, select **System Status > Routes** and verify the XTM device and the router are sending updates to each other.

   You can then add authentication and restrict the OSPF policy to listen only on the correct interfaces.

Sample OSPF Routing Configuration File

To use any of the dynamic routing protocols with Fireware XTM, you must copy and paste a configuration file for the dynamic routing daemon. This topic includes a sample configuration file for the OSPF routing daemon. To use this configuration file as a base for your own configuration file, copy the text into a new text file and save it with a new name. You can then edit the parameters to meet the requirements of your organization.

Optional commands are commented with the "!" character. To enable a command, delete the "!" and modify variables as necessary.

```
!! SECTION 1: Configure interface properties.
! Set properties for interface eth1.
! interface eth1
!
! Set simple authentication password (SHAREDKEY).
! ip ospf authentication-key SHAREDKEY
!
! Set MD5 authentication key ID (10) and MD5 authentication key (AUTHKEY).
! ip ospf message-digest-key 10 md5 AUTHKEY
!
! Set link cost to 1000 (1-65535) on interface eth1.
! for OSPF link cost table. !ip ospf cost 1000
!
! Set hello interval to 5 seconds (1-65535); default is 10 seconds.
! ip ospf hello-interval 5
!
! Set dead-interval to 15 seconds (1-65535); default is 40 seconds.
! ip ospf dead-interval 15
!
! Set interval between link-state advertisements (LSA) retransmissions
! to 10 seconds (1-65535); default is 5 seconds.
! ip ospf retransmit-interval 10
!
! Set LSA update interval to 3 seconds (1-3600); default is 1 second.
! ip ospf transmit-delay 3
!
```

```
! Set high priority (0-255) to increase eligibility to become the
! designated router (DR).
! ip ospf priority 255
!! SECTION 2: Start OSFP and set daemon properties.
! Enable OSPF daemon. Must be enabled for all OSPF configurations.
! router ospf
!
! Set the router ID manually to 100.100.100.20. If not set, the firewall will
! set its own ID based on an interface IP address.
! ospf router-id 100.100.100.20
!
! Enable RFC 1583 compatibility (increases probability of routing loops).
! ospf rfc1583compatibility
!
! Set area border router (ABR) type to cisco, ibm, shortcut, or standard.
! More information about ABR types is in draft-ietf-ospf-abr-alt-05.txt.
! ospf abr-type cisco
!
! Disable OSPF announcement on interface eth0.
! passive interface eth0
!
! Set global cost to 1000 (0-429495).
! auto-cost reference bandwidth 1000
!
! Set SPF schedule delay to 25 (0-4294967295) seconds and hold time to
! 20 (0-4294967295) seconds; default is 5 and 10 seconds. !timers spf 25 20
!! SECTION 3: Set network and area properties. Set areas with W.X.Y.Z
!! or Z notation.
! Announce OSPF on network 192.168.253.0/24 network for area 0.0.0.0.
! network 192.168.253.0/24 area 0.0.0.0
!
! Create area 0.0.0.1 and set a classful network range (172.16.254.0/24)
! for the area (range and interface network settings must match).
! area 0.0.0.1 range 172.16.254.0/24
!
! Set virtual link neighbor (172.16.254.1) for area 0.0.0.1.
! area 0.0.0.1 virtual-link 172.16.254.1
!
! Set area 0.0.0.1 as a stub on all routers in area 0.0.0.1.
! area 0.0.0.1 stub
!
! area 0.0.0.2 stub no-summary
!
! Enable simple password authentication for area 0.0.0.0.
! area 0.0.0.0 authentication
!
! Enable MD5 authentication for area 0.0.0.1.
! area 0.0.0.1 authentication message-digest
!! SECTION 4: Redistribute OSPF routes
! Share route of last resort (default route) from kernel routing table
! with OSPF peers.
! default-information originate
!
! Redistribute static routes to OSPF.
```

```
! redistribute kernel
!
! Redistribute routes from all interfaces to OSPF.
! redistribute connected
! redistribute connected route-map
! ! Redistribute routes from RIP and BGP to OSPF.
! redistribute rip !redistribute bgp
!! SECTION 5: Configure route redistribution filters with access lists
!! and route maps.
! Create an access list to only allow redistribution of 10.0.2.0/24.
! access-list LISTNAME permit 10.0.2.0/24
! access-list LISTNAME deny any
!
! Create a route map with name MAPNAME and allow with a
priority of 10 (1-199).
! route-map MAPNAME permit 10
! match ip address LISTNAME
```

About Border Gateway Protocol (BGP)

Note *Support for this protocol is available only in Fireware XTM with a Pro upgrade.*

Border Gateway Protocol (BGP) is a scalable dynamic routing protocol used on the Internet by groups of routers to share routing information. BGP uses route parameters or *attributes* to define routing policies and create a stable routing environment. This protocol allows you to advertise more than one path to and from the Internet to your network and resources, which gives you redundant paths and can increase your uptime.

Hosts that use BGP use TCP to send updated routing table information when one host finds a change. The host sends only the part of the routing table that has the change. BGP uses classless interdomain routing (CIDR) to reduce the size of the Internet routing tables. The size of the BGP routing table in Fireware XTM is set at 32K.

The size of the typical WatchGuard customer wide area network (WAN) is best suited for OSPF dynamic routing. A WAN can also use external border gateway protocol (EBGP) when more than one gateway to the Internet is available. EBGP allows you to take full advantage of the redundancy possible with a multi-homed network.

To participate in BGP with an ISP you must have an autonomous system number (ASN). You must get an ASN from one of the regional registries in the table below. After you are assigned your own ASN, you must contact each ISP to get their ASNs and other necessary information.

Region	Registry Name	Web Site
North America	RIN	www.arin.net
Europe	RIPE NCC	www.ripe.net
Asia Pacific	APNIC	www.apnic.net
Latin America	LACNIC	www.lacnic.net
Africa	AfriNIC	www.afrinic.net

BGP Commands

To create or modify a routing configuration file, you must use the correct routing commands. The subsequent table is a catalog of supported BGP routing commands. The sections must appear in the configuration file in the same order they appear in this table.

Do not use BGP configuration parameters that you do not get from your ISP.

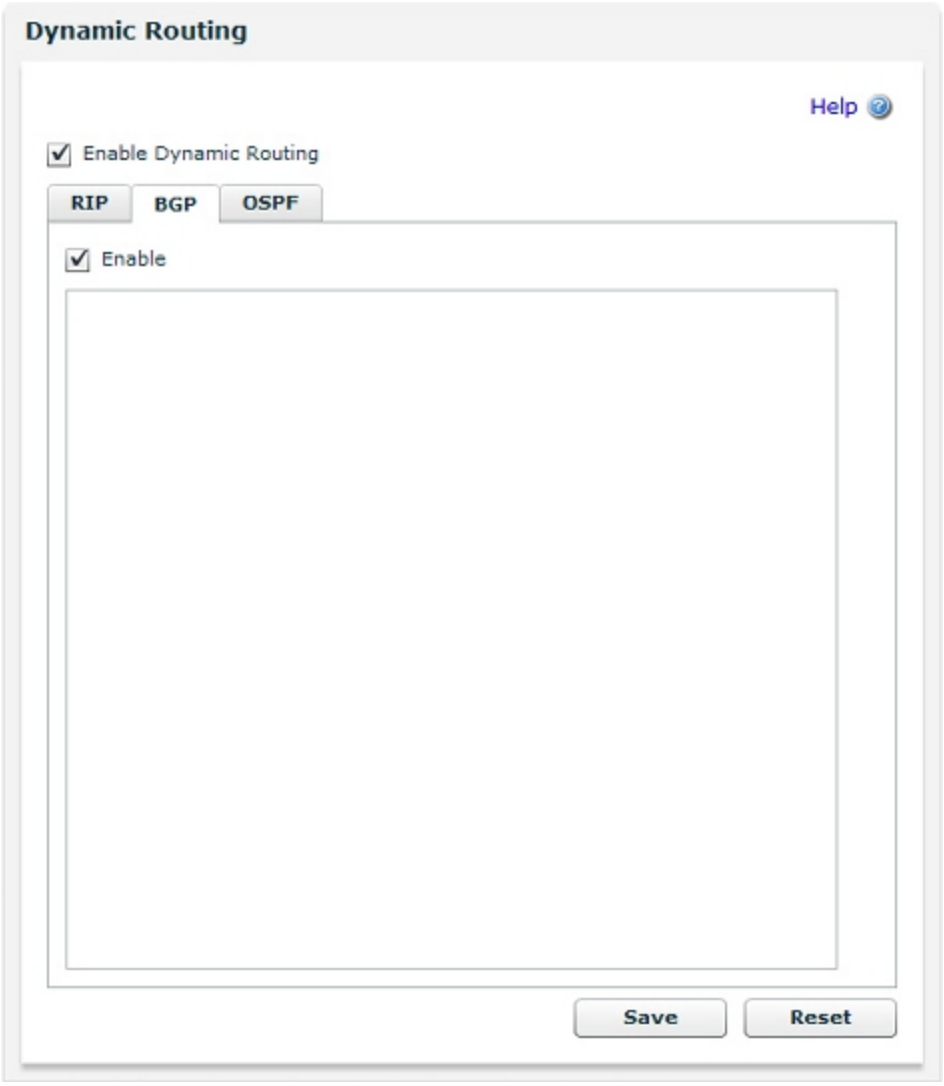
Section	Command	Description
Configure BGP Routing Daemon		
	router bgp [ASN]	Enable BGP daemon and set autonomous system number (ASN); this is supplied by your ISP
	network [A.B.C.D/M]	Announce BGP on network A.B.C.D/M
	no network [A.B.C.D/M]	Disable BGP announcements on network A.B.C.D/M
Set Neighbor Properties		
	neighbor [A.B.C.D] remote-as [ASN]	Set neighbor as a member of remote ASN
	neighbor [A.B.C.D] ebgp-multihop	Set neighbor on another network using EBGP multi-hop
	neighbor [A.B.C.D] version 4+	Set BGP version (4, 4+,4-) for communication with neighbor; default is 4
	neighbor [A.B.C.D] update-source [WORD]	Set the BGP session to use a specific interface for TCP connections
	neighbor [A.B.C.D] default-originate	Announce default route to BGP neighbor [A,B,C,D]
	neighbor [A.B.C.D] port 189	Set custom TCP port to communicate with BGP neighbor [A,B,C,D]
	neighbor [A.B.C.D] send-community	Set peer send-community
	neighbor [A.B.C.D] weight 1000	Set a default weight for neighbor's [A.B.C.D] routes
	neighbor [A.B.C.D] maximum-prefix [NUMBER]	Set maximum number of prefixes allowed from this neighbor
Community Lists		
	ip community-list [<1-99>|<100-199>] permit AA:NN	Specify community to accept autonomous system number and network number separated by a colon

Section	Command	Description
Peer Filtering		
	neighbor [A.B.C.D] distribute-list [LISTNAME] [IN|OUT]	Set distribute list and direction for peer
	neighbor [A.B.C.D] prefix-list [LISTNAME] [IN|OUT]	To apply a prefix list to be matched to incoming advertisements or outgoing advertisements to that neighbor
	neighbor [A.B.C.D] filter-list [LISTNAME] [IN|OUT]	To match an autonomous system path access list to incoming routes or outgoing routes
	neighbor [A.B.C.D] route-map [MAPNAME] [IN|OUT]	To apply a route map to incoming or outgoing routes
Redistribute Routes to BGP		
	redistribute kernel	Redistribute static routes to BGP
	redistribute rip	Redistribute RIP routes to BGP
	redistribute ospf	Redistribute OSPF routes to BGP
Route Reflection		
	bgp cluster-id A.B.C.D	To configure the cluster ID if the BGP cluster has more than one route reflector
	neighbor [W.X.Y.Z] route-reflector-client	To configure the router as a BGP route reflector and configure the specified neighbor as its client
Access Lists and IP Prefix Lists		
	ip prefix-lists PRELIST permit A.B.C.D/E	Set prefix list
	access-list NAME [deny|allow] A.B.C.D/E	Set access list
	route-map [MAPNAME] permit [N]	In conjunction with the "match" and "set" commands, this defines the conditions and actions for redistributing routes
	match ip address prefix-list [LISTNAME]	Matches the specified access-list
	set community [A:B]	Set the BGP community attribute
	match community [N]	Matches the specified community_list
	set local-preference [N]	Set the preference value for the autonomous system path

Configure the XTM Device to Use BGP

To participate in BGP with an ISP you must have an autonomous system number (ASN). For more information, see *About Border Gateway Protocol (BGP)* on page 226.

1. Select **Network > Dynamic Routing**.
   The Dynamic Routing Setup page appears.
2. Select the **Enable Dynamic Routing** check box.
3. Click the **BGP** tab.



4. Select the **Enable** check box.
5. Copy and paste your routing daemon configuration file in the window.

   For more information, see *About Routing Daemon Configuration Files* on page 209.

   To get started, you need only three commands in your BGP configuration file. These three commands, start the BGP process, set up a peer relationship with the ISP, and create a route for a network to the Internet. You must use the commands in this order.

`router BGP:` BGP autonomous system number supplied by your ISP
`network:` network IP address that you want to advertise a route to from the Internet
`neighbor:` <IP address of neighboring BGP router> `remote-as` <BGP autonomous number>

6. Click **Save**.

Allow BGP Traffic Through the XTM Device

You must add and configure a policy to allow BGP traffic to the XTM device from the approved networks. These networks must be the same networks you defined in your BGP configuration file.

1. Select **Firewall > Firewall Policies**. Click **Add**.
   The Select a Policy Type page appears.
2. From the list of packet filters, select **BGP**. Click **Add**.
3. On the **Policy Configuration** page, configure the policy to allow traffic from the IP or network address of the router that uses BGP to the XTM device interface it connects to. You must also add the network broadcast IP address.
4. Click **Save**.
5. Set up the router you selected in Step 3.
6. After you configure the router, select **System Status > Routes** and verify the XTM device and the router are sending updates to each other.

   You can then add authentication and restrict the BGP policy to listen only on the correct interfaces.

Sample BGP Routing Configuration File

To use any of the dynamic routing protocols with Fireware XTM, you must import or type a configuration file for the dynamic routing daemon. This topic includes a sample configuration file for the BGP routing daemon. If you want to use this configuration file as a base for your own configuration file, copy the text into an application such as Notepad or Wordpad and save it with a new name. You can then edit the parameters to meet your own business requirements.

Optional commands are commented with the "!" character. To enable a command, delete the "!" and modify variables as necessary.

```
!! SECTION 1: Start BGP daemon and announce network blocks to BGP neighbors
! Enable BGP and set local ASN to 100 router bgp 100
! Announce local network 64.74.30.0/24 to all neighbors defined in section 2
! network 64.74.30.0/24
!! SECTION 2: Neighbor properties
! Set neighbor (64.74.30.1) as member of remote ASN (200)
! neighbor 64.74.30.1 remote-as 200
! Set neighbor (208.146.43.1) on another network using EBGP multi-hop
! neighbor 208.146.43.1 remote-as 300
! neighbor 208.146.43.1 ebgp-multihop
! Set BGP version (4, 4+, 4-) for communication with a neighbor; default is 4
! neighbor 64.74.30.1 version 4+
! Announce default route to BGP neighbor (64.74.30.1)
! neighbor 64.74.30.1 default-originate
! Set custom TCP port 189 to communicate with BGP neighbor (64.74.30.1). Default
    port is TCP 179
! neighbor 64.74.30.1 port 189
```

```
! Set peer send-community
! neighbor 64.74.30.1 send-community
! Set a default weight for neighbor's (64.74.30.1) routes
! neighbor 64.74.30.1 weight 1000
! Set maximum number of prefixes allowed from this neighbor
! neighbor 64.74.30.1 maximum-prefix NUMBER

!! SECTION 3: Set community lists
    ! ip community-list 70 permit 7000:80

!! SECTION 4: Announcement filtering
! Set distribute list and direction for peer
! neighbor 64.74.30.1 distribute-list LISTNAME [in|out]
    ! To apply a prefix list to be matched to incoming or outgoing advertisements
    to that neighbor
! neighbor 64.74.30.1 prefix-list LISTNAME [in|out
! To match an autonomous system path access list to incoming or outgoing routes
! neighbor 64.74.30.1 filter-list LISTNAME [in|out]
! To apply a route map to incoming or outgoing routes
! neighbor 64.74.30.1 route-map MAPNAME [in|out]

!! SECTION 5: Redistribute routes to BGP
! Redistribute static routes to BGP
! Redistribute kernel
! Redistribute rip routes to BGP
! Redistribute rip
! Redistribute ospf routes to BGP

! Redistribute ospf

!! SECTION 6: Route reflection
! Set cluster ID and firewall as a client of route reflector server 51.210.0.254
! bgp cluster-id A.B.C.D
! neighbor 51.210.0.254 route-reflector-client

!! SECTION 7: Access lists and IP prefix lists
! Set prefix list
! ip prefix-list PRELIST permit 10.0.0.0/8
! Set access list!access-list NAME deny 64.74.30.128/25
! access-list NAME permit 64.74.30.0/25
! Create a route map with name MAPNAME and allow with a priority of 10
! route-map MAPNAME permit 10
! match ip address prefix-list LISTNAME
! set community 7000:80
```

11 Authentication

About User Authentication

User authentication is a process that finds whether a user is who he or she is declared to be and verifies the privileges assigned to that user. On the XTM device, a user account has two parts: a user name and a passphrase. Each user account is associated with an IP address. This combination of user name, passphrase, and IP address helps the device administrator to monitor connections through the device. With authentication, users can log in to the network from any computer, but access only the network ports and protocols for which they are authorized. The XTM device can then map the connections that start from a particular IP address and also transmit the session name while the user is authenticated.

You can create firewall polices to give users and groups access to specified network resources. This is useful in network environments where different users share a single computer or IP address.

You can configure your XTM device as a local authentication server, or use your existing Active Directory or LDAP authentication server, or an existing RADIUS authentication server. When you use Firebox authentication over port 4100, account privileges can be based on user name. When you use third-party authentication, account privileges for users that authenticate to the third-party authentication servers are based on group membership.

The WatchGuard user authentication feature allows a user name to be associated with a specific IP address to help you authenticate and track user connections through the device. With the device, the fundamental question that is asked and answered with each connection is, *"Should I allow traffic from source X to go to destination Y?"* For the WatchGuard authentication feature to work correctly, the IP address of the user's computer must not change while the user is authenticated to the device.

In most environments, the relationship between an IP address and the user computer is stable enough to use for authentication. Environments in which the association between the user and an IP address is not consistent, such as kiosks or networks where applications are run from a terminal server, are usually not good candidates for the successful use of the user authentication feature.

WatchGuard supports Authentication, Accounting, and Access control (AAA) in the firewall products, based on a stable association between IP address and person.

The WatchGuard user authentication feature also supports authentication to an Active Directory domain with Single Sign-On (SSO), as well as other common authentication servers. In addition, it supports inactivity settings and session time limits. These controls restrict the amount of time an IP address is allowed to pass traffic through the XTM device before users must supply their passwords again (reauthenticate).

If you control SSO access with a white list and manage inactivity timeouts, session timeouts, and who is allowed to authenticate, you can improve your control of authentication, accounting, and access control.

To prevent a user from authenticating, you must disable the account for that user on the authentication server.

User Authentication Steps

After you configure your XTM device as a local authentication server, the HTTPS server on the XTM device accepts authentication requests. To authenticate, a user must connect to the authentication portal web page on the XTM device.

1. Go to either:

   `https://[device interface IP address]:4100/`

   or

   `https://[device hostname]:4100`

   An authentication web page appears.
2. Type a user name and password.
3. Select the authentication server from the drop-down list, if more than one type of authentication is configured.
   The XTM device sends the name and password to the authentication server using PAP (Password Authentication Protocol).

When authenticated, the user is allowed to use the approved network resources.

> ***Note*** *Because Fireware XTM uses a self-signed certificate by default for HTTPS, you see a security warning from your web browser when you authenticate. You can safely ignore this security warning. If you want to remove this warning, you can use a third-party certificate or create a custom certificate that matches the IP address or domain name used for authentication.*

Manually Close an Authenticated Session

Users do not have to wait for the session timeout to close their authenticated sessions. They can manually close their sessions before the timeout occurs. The Authentication web page must be open for a user to close a session. If it is closed, the user must authenticate again to log out.

To close an authenticated session:

1. Go to the Authentication portal web page:

   `https://[device interface IP address]:4100/`

   or

   `https://[device host name]:4100`

2. Click **Logout**.

> ***Note*** *If the Authentication portal web page is configured to automatically redirect to another web page, the portal is redirected just a few seconds after you open it. Make sure you logout before the page redirects.*

Manage Authenticated Users

You can use Fireware XTM Web UI to see a list of all the users authenticated to your XTM device and close sessions for those users.

See Authenticated Users

To see the users authenticated to your XTM device:

1. *Connect to Fireware XTM Web UI*.
2. Select **System Status > Authentication List**.
   A list of all users authenticated to the Firebox appears.

Close a User Session

From Fireware XTM Web UI:

1. Select **System Status > Authentication List**.
   A list of all users authenticated to the Firebox appears.
2. Select one or more user names from the list.
3. Right-click the user name(s) and select **Log Off User**.

Use Authentication to Restrict Incoming Traffic

One function of the authentication tool is to restrict outgoing traffic. You can also use it to restrict incoming network traffic. When you have an account on the XTM device and the device has a public external IP address, you can authenticate to the device from a computer external to the device.

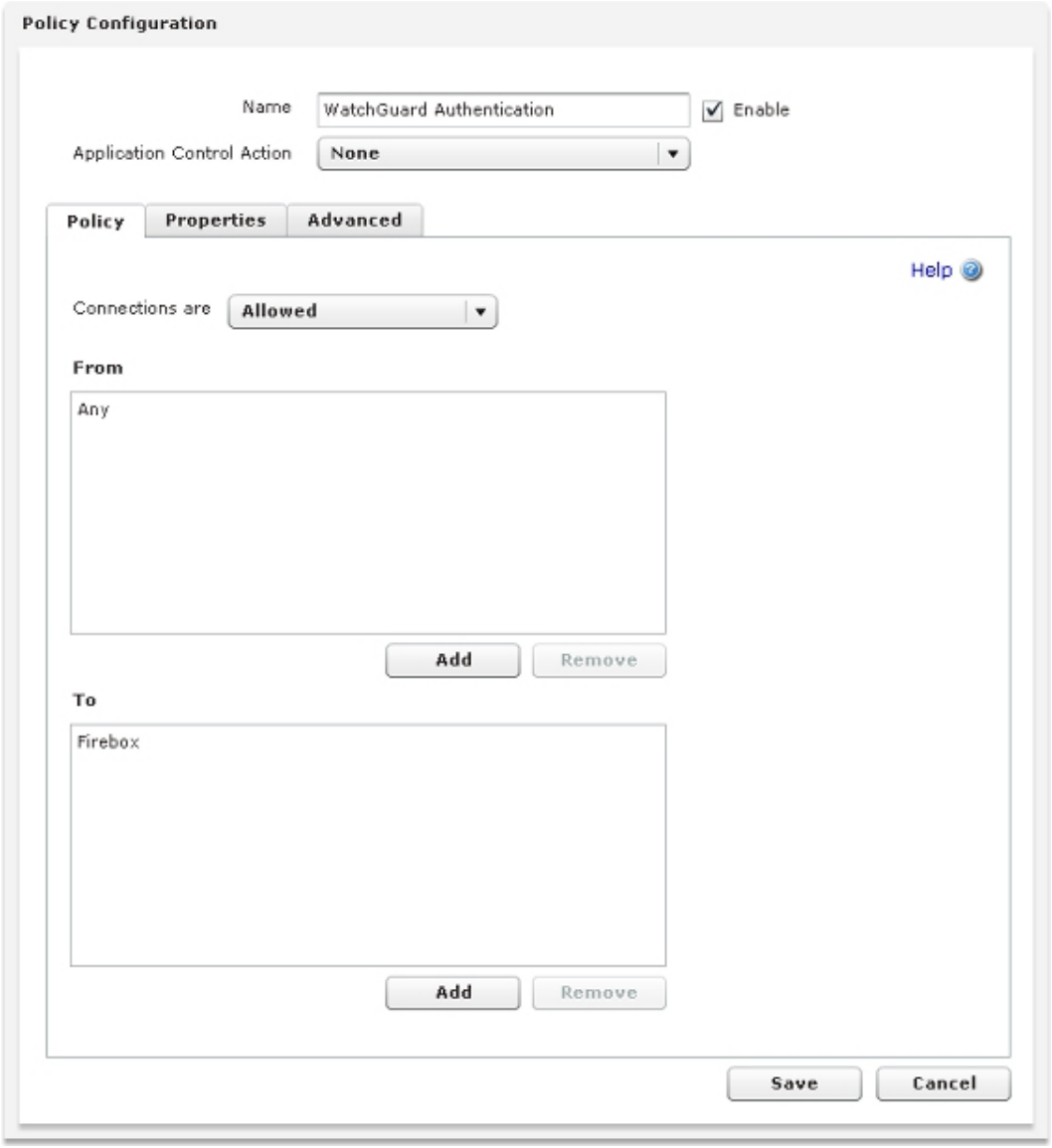
For example, you can type this address in your web browser: `https://<IP address of XTM device external interface>:4100/`.

After you authenticate, you can use the policies that are configured for you on the device.

To enable a remote user to authenticate from the external network:

1. Select **Firewall > Firewall Policies**.
   The Firewall Polices Page appears.
2. Select the **WatchGuard Authentication** policy and click  .
   Or, double-click the policy. This policy appears after you add a user or group to a policy configuration.
   The Policy Configuration page appears.
3. From the **Connections are** drop-down list, make sure **Allowed** is selected.
4. In the **From** section, click **Add**.
   The Add Member dialog box appears.
5. From the **Select Members** list, select **Any**.
6. Click **OK**.
   Any appears in the From list.
7. In the **To** section, click **Add**.
8. From the **Select Members** list, select **Firebox**.

9. Click **OK**.
   Firebox appears in the To list.



10. Click **Save**.

Use Authentication Through a Gateway Firebox

The gateway Firebox is the XTM device that you place in your network to protect your Management Server from the Internet.

To send an authentication request through a gateway Firebox to a different device, you must have a policy that allows the authentication traffic on the gateway device. If authentication traffic is denied on the gateway device, add the WG-Auth policy. This policy controls traffic on TCP port 4100. You must configure the policy to allow traffic to the IP address of the destination device.

About the WatchGuard Authentication (WG-Auth) Policy

The WatchGuard Authentication (WG-Auth) policy is automatically added to your XTM device configuration when you add the first policy that has a user or group name in the **From** list on the **Policy** tab of the policy definition. The WG-Auth policy controls access to port 4100 on your XTM device. Your users send authentication requests to the device through this port. For example, to authenticate to an XTM device with an IP address of 10.10.10.10, your users type `https://10.10.10.10:4100` in the web browser address bar.

If you want to send an authentication request through a gateway device to a different device, you might have to add the WG-Auth policy manually. If authentication traffic is denied on the gateway device, you must use Policy Manager to add the WG-Auth policy. Modify this policy to allow traffic to the IP address of the destination device.

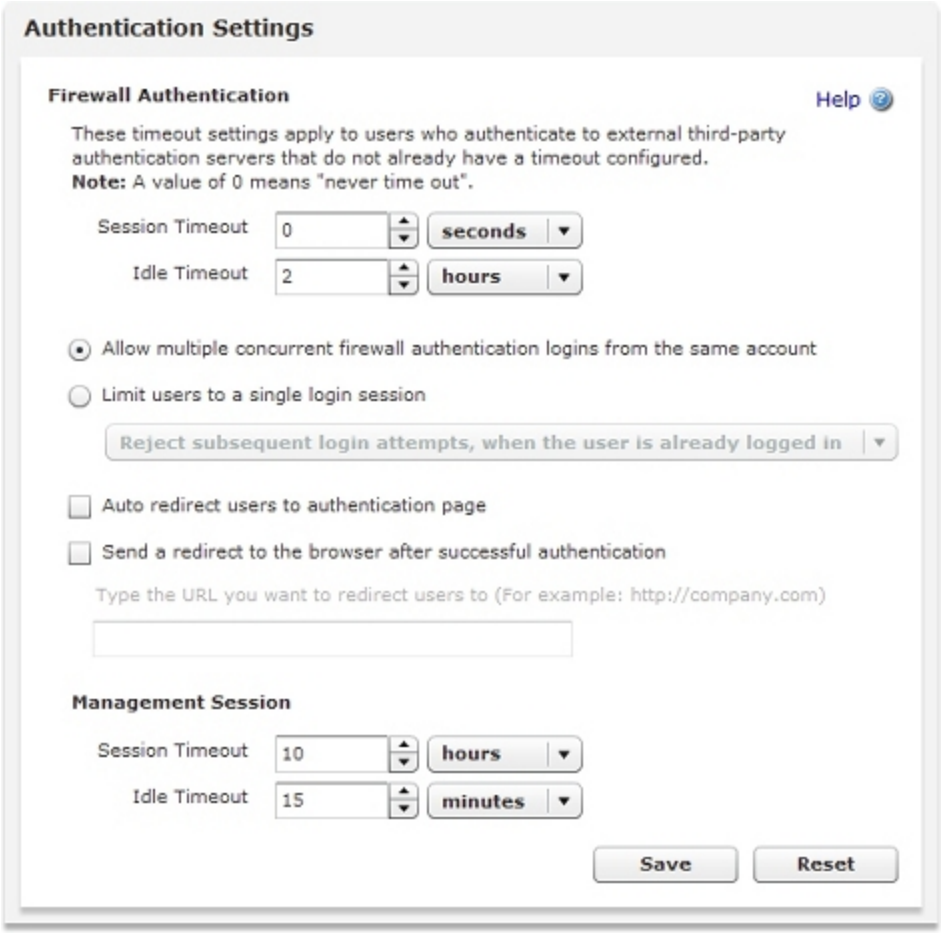
For more information on when to modify the WatchGuard Authentication policy, see *Use Authentication to Restrict Incoming Traffic* on page 236.

Set Global Firewall Authentication Values

When you configure your global authentication settings, you can configure the global values for firewall authentication, such as timeout values, user login session limits, and authentication page redirect settings. You can also enable Single Sign-On (SSO), and configure settings for Terminal Services. For more information, see the topics *Enable Single Sign-On (SSO)* and *Configure Terminal Services Settings*.

To configure Firewall Authentication settings:

1. *Connect to Fireware XTM Web UI*.
2. Select **Authentication > Settings**.
   The Authentication Settings page appears.



3. Configure authentication settings as described in the subsequent sections.
4. Click **Save**.

Set Global Authentication Timeouts

You can set the time period that users remain authenticated after they close their last authenticated connection. This timeout is set either in the **Authentication Settings** dialog box, or on the **Setup Firebox User** page.

For more information about user authentication settings and the **Setup Firebox User** page, see *Define a New User for Firebox Authentication* on page 256.

For users authenticated by third-party servers, the timeouts set on those servers also override the global authentication timeouts.

Authentication timeout values do not apply to Mobile VPN with PPTP users.

Session Timeout

The maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, the session does not expire and the user can stay connected for any length of time.

Idle Timeout

The maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network). If you set this field to zero (0) seconds, minutes, hours, or days, the session does not timeout when idle and the user can stay idle for any length of time.

Allow Multiple Concurrent Logins

You can allow more than one user to authenticate with the same user credentials at the same time, to one authentication server. This is useful for guest accounts or in laboratory environments. When the second user logs in with the same credentials, the first user authenticated with the credentials is automatically logged out. If you do not allow this feature, a user cannot authenticate to the authentication server more than once at the same time.

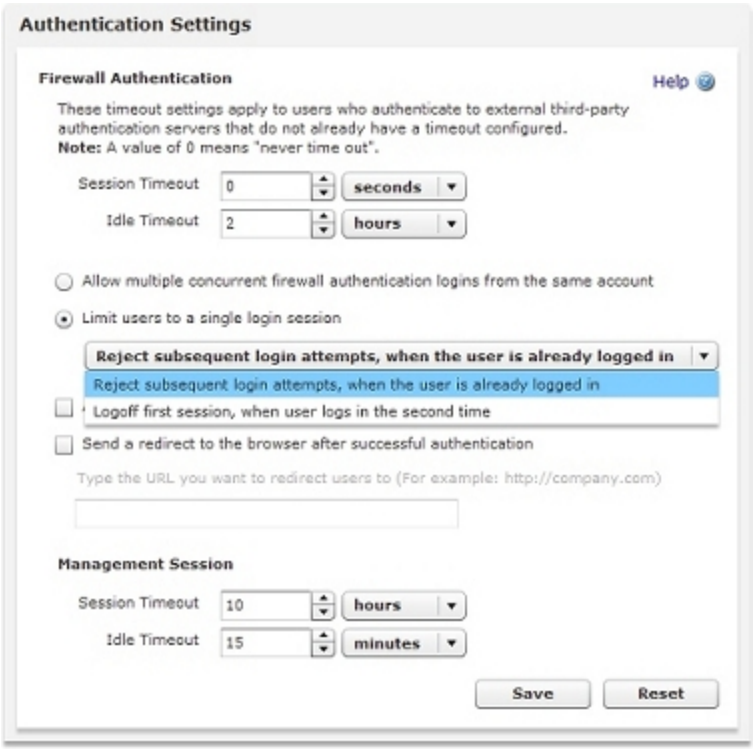
1. Go to the **Authentication Settings** page.
2. Select the **Allow multiple concurrent firewall authentication logins from the same account** option.

For Mobile VPN with IPSec and Mobile VPN with SSL users, concurrent logins from the same account are always supported regardless of whether this option is selected. These users must log in from different IP addresses for concurrent logins, which means that they cannot use the same account to log in if they are behind an XTM device that uses NAT. Mobile VPN with PPTP users do not have this restriction.

Limit Login Sessions

From the **Authentication Settings** page, you can limit your users to a single authenticated session. If you select this option, your users cannot login to one authentication server from different IP addresses with the same credentials. When a user is authenticated, and tries to authenticate again, you can select whether the first user session is terminated when the subsequent session is authenticated, or if the subsequent session is rejected.

1. Select **Limit users to a single login session**.
2. From the drop-down list, select an option:
   - **Reject subsequent login attempts, when the user is already logged in**
   - **Logoff first session, when user logs in the second time**.



Automatically Redirect Users to the Authentication Portal

If you require your users to authenticate before they can get access to the Internet, you can choose to automatically send users who are not already authenticated to the authentication portal, or have them manually navigate to the portal. This applies only to HTTP and HTTPS connections.

Auto redirect users to authentication page for authentication

When you select this check box, all users who have not yet authenticated are automatically redirected to the authentication portal when they try to get access to the Internet. If you do not select this checkbox, unauthenticated users must manually navigate to the authentication portal to log in.

For more information about user authentication, see *User Authentication Steps* on page 234.

If you have users who must manually authenticate to the authentication portal, and you use SSO, you can add an SSO exception for those users to reduce the amount of time it takes for them to authenticate. For more information about SSO exceptions, see *Enable Single Sign-On (SSO)*.

Use a Custom Default Start Page

When you select the **Auto redirect users to authentication page for authentication** check box to require your users to authenticate before they can get access to the Internet, the Authentication portal appears when a user opens a web browser. If you want the browser to go to a different page after your users successfully log in, you can define a redirect.

From the **Authentication Settings** page:

1. Select the **Send a redirect to the browser after successful authentication** check box.
2. In the text box, type the URL of the web site to which users are redirected.

Set Management Session Timeouts

Use these fields to set the time period that a user logged in with read/write privileges remains authenticated before the XTM device terminates the session.

Session Timeout

The maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, the session does not expire and the user can stay connected for any length of time.

Idle Timeout

The maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network). If you set this field to zero (0) seconds, minutes, hours, or days, the session does not expire when the user is idle, and the user can stay idle for any length of time.

About Single Sign-On (SSO)

When users log on to computers on your network, they must give a user name and password. If you use Active Directory authentication on your XTM device to restrict outgoing network traffic to specified users or groups, they must also log on again when they manually authenticate to the device to access network resources such as the Internet. You can use Single Sign-On (SSO) to enable users on the trusted or optional networks to automatically authenticate to the XTM device when they log on to their computers.

WatchGuard SSO is a two-part solution that includes the SSO agent and SSO client services. For SSO to work, you must install the SSO agent software on a computer in your domain. The SSO client software is optional and is installed on each user's client computer. If you configure multiple Active Directory domains, your users must install the SSO client. For more information, see *Configure Active Directory Authentication* on page 272 and *Install the WatchGuard Single Sign-On (SSO) Client* on page 245.

The SSO agent software makes a call to the client computer over port 4116 to verify who is currently logged in. If there is no response, the SSO agent reverts to the previous protocol from versions prior to WSM 10.2.4, and makes a *NetWkstaUserEnum* call to the client computer. It then uses the information it gets to authenticate a user for Single Sign-On.

If the SSO client is not installed, the SSO agent can get more than one answer from the computer it queries. This can occur if more than one user logs on to the same computer or because of service or batch logons that occur on the computer. The SSO agent uses only the first answer it gets from the computer and reports that user to the XTM device as the user that is logged on. The device can then check the user information against all the defined policies for that user and/or user group at one time. The SSO agent caches this data for about 10 minutes by default so that a query does not have to be generated for every connection.

When the SSO client software is installed, it receives the call from the SSO agent and returns accurate information about the user who is currently logged in to the workstation. The SSO agent does not contact the Active Directory server for user credentials from the SSO client, because it receives the correct information about who is currently logged in to the computer and to which Active Directory groups the user belongs. If you configure multiple Active Directory domains, your users must install the SSO client.

If you work in an environment where more than one person uses a computer, we recommend that you install the SSO client software. If you do not use the SSO client, there are access control limitations you must be aware of. For example, for services installed on a client computer (such as a centrally administered antivirus client) that have been deployed so that they log on with domain account credentials, the XTM device gives all users access rights as defined by the first user that is logged on (and the groups of which that user is a member), and not the credentials of the individual users that log on interactively. Also, all log messages generated from the user's activity show the user name of the service account, and not the individual user.

> ***Note*** *If you do not install the SSO client, we recommend you do not use SSO for environments where users log on to computers with service or batch logons. When more than one user is associated with an IP address, network permissions may not operate correctly. This can be a security risk.*

If you enable Single Sign-On, you can also use Firewall authentication to log in to Firewall authentication page and authenticate with different user credentials. For more information, see *Firewall Authentication* on page 255.

Before You Begin

- You must have an Active Directory server configured on a trusted or optional network.
- Your XTM device must be configured to use Active Directory authentication.
- Each user must have an account set up on the Active Directory server.
- Each user must log on to a domain account for Single Sign-On (SSO) to operate correctly. If users log on to an account that exists only on their local computers, their credentials are not checked and the XTM device does not recognize that they are logged in.
- If you use third-party firewall software on your network computers, make sure that TCP port 445 (Samba/ Windows Networking) is open on each client.
- Make sure that printing and file sharing is enabled on every computer from which users authenticate with SSO.
- Make sure that NetBIOS and SMB ports are not blocked on every computer from which users authenticate with SSO. NetBIOS uses TCP/UDP ports 137, 138, and 139. SMB uses TCP port 445.
- Make sure that port 4116 is open on the client computers.
- Make sure that all computers from which users authenticate with SSO are members of the domain with unbroken trust relationships.

Set Up SSO

To use SSO, you must install the SSO agent software. We recommend that you also install the SSO client on your users' computers. Though you can use SSO with only the SSO agent, you increase your security and access control when you also use the SSO client.

To set up SSO, follow these steps:

1. *Install the WatchGuard Single Sign-On (SSO) Agent*.
2. *Install the WatchGuard Single Sign-On (SSO) Client* (optional, but recommended).
3. *Enable Single Sign-On (SSO)*.

Install the WatchGuard Single Sign-On (SSO) Agent

To use Single Sign-On (SSO), you must install the WatchGuard SSO agent. The SSO agent is a service that receives requests for Firebox authentication and checks user status with the Active Directory server. The service runs with the name *WatchGuard Authentication Gateway* on the computer on which you install the SSO agent software. This computer must have the Microsoft .NET Framework 2.0 or later installed.

Download the SSO Agent Software

1. Open a web browser and go to http://www.watchguard.com/.
2. Log in with your LiveSecurity Service user name and password.
3. Click the **Software Downloads** link.
4. Select your device type and model number.
5. Download the WatchGuard Authentication Gateway software and save the file to a convenient location.

Before You Install

The SSO agent service must run as a user account, not an administrator account. We recommend that you create a new user account for this purpose. For the SSO agent service to operate correctly, make sure you configure the user account with a password that never expires.

Install the SSO Agent Service

1. Double-click **WG-Authentication-Gateway.exe** to start the Authentication Gateway Setup Wizard. On some operating systems, you might need to type a local administrator password to run the installer.
2. To install the software, use the instructions on each page and complete the wizard.

   For the domain user name, you must type the user name in the form: `domain\username`. Do not include the .com or .net part of the domain name.

   For example, if your domain is *mywatchguard.com* and you use the domain account *ssoagent*, type `mywatchguard\ssoagent`.
   You can also use the UPN form of the user name: `username@mywatchguard.com`. If you use the UPN form of the user name then you must include the .com or .net part of the domain name.
3. Click **Finish** to close the wizard.

When the wizard completes, the WatchGuard Authentication Gateway service starts automatically. Each time the computer starts, the service starts automatically.

After you have completed the SSO Agent installation, you must configure the domain settings for the SSO Agent. For more information, see Configure the SSO Agent.

Install the WatchGuard Single Sign-On (SSO) Client

As a part of the WatchGuard Single Sign-On (SSO) solution, you can install the WatchGuard SSO client. The SSO client installs as a Windows service that runs under the Local System account on a workstation to verify the credentials of the user currently logged in to that computer. When a user tries to authenticate, the SSO agent sends a request to the SSO client for the user's credentials. The SSO client then returns the credentials of the user who is logged in to the workstation.

The SSO client listens on port 4116.

If you configure multiple Active Directory domains, your users must install the SSO client. For more information, see *Configure Active Directory Authentication* on page 272.

Because the SSO client installer is an MSI file, you can choose to automatically install it on your users' computers when they log on to your domain. You can use Active Directory Group Policy to automatically install software when users log on to your domain. For more information about software installation deployment for Active Directory group policy objects, see the documentation for your operating system.

Download the SSO Client Software

1. Use your web browser to go to http://www.watchguard.com/.
2. Log in with your LiveSecurity Service user name and password.
3. Click the **Software Downloads** link.
4. Select your device type and model number.
5. Download the WatchGuard Authentication Client software and save the file to a convenient location.

Install the SSO Client Service

1. Double-click **WG-Authentication-Client.msi** to start the Authentication Client Setup Wizard.
   On some operating systems, you might need to type a local administrator password to run the installer.
2. To install the software, use the instructions on each page and complete the wizard.

   To see which drives are available to install the client, and how much space is available on each of these drives, click **Disk Cost**.
3. Click **Close** to exit the wizard.

   After the wizard completes, the WatchGuard Authentication Client service starts automatically. Each time the computer starts, the service starts automatically.

Enable Single Sign-On (SSO)

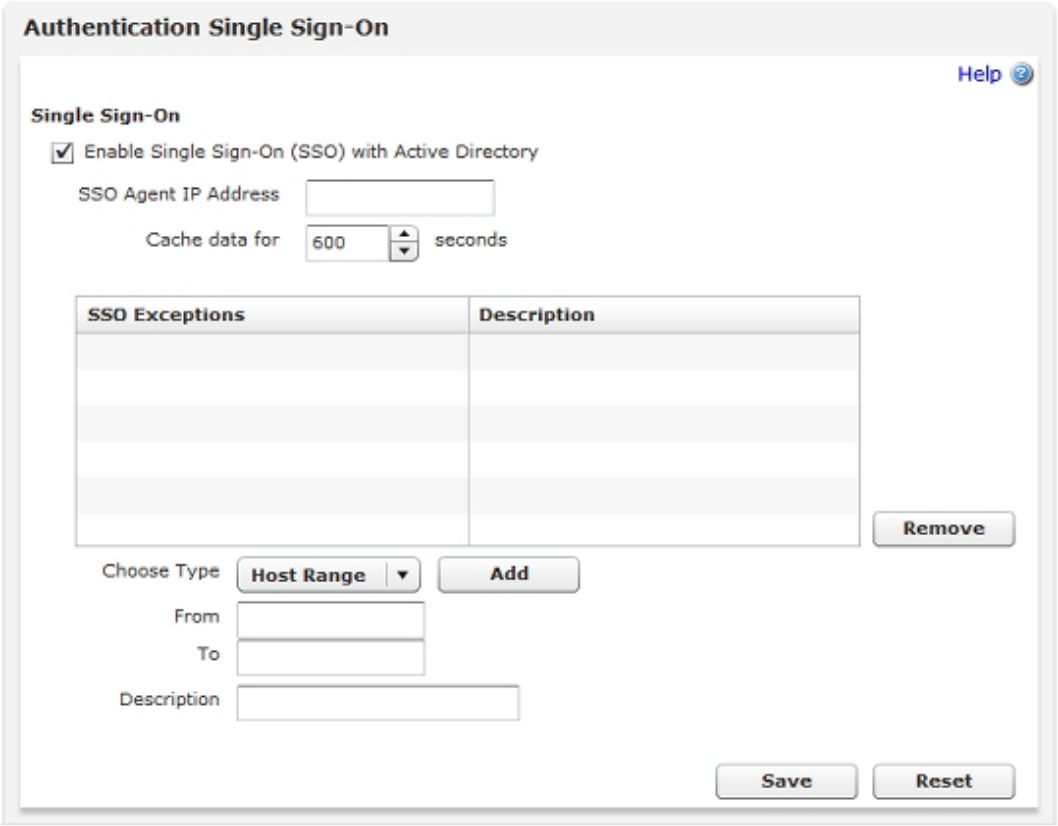
Before you can configure SSO, you must:

- Configure your Active Directory server
- *Install the WatchGuard Single Sign-On (SSO) Agent*
- *Install the WatchGuard Single Sign-On (SSO) Client* (Optional)

Enable and Configure SSO

To enable and configure SSO from Fireware XTM Web UI:

1. Select **Authentication > Single Sign-On**.
   The Authentication Single Sign-On page appears.
2. Select the **Enable Single Sign-On (SSO) with Active Directory** check box.



3. In the **SSO Agent IP address** text box, type the IP address of your SSO Agent.
4. In the **Cache data for** text box, type or select the amount of time the SSO Agent caches data.
5. In the **SSO Exceptions** list, add or remove the IP addresses or ranges to exclude from SSO queries.

   For more information about SSO exceptions, see the *Define SSO Exceptions* on page 247 section.
6. Click **Save** to save your changes.

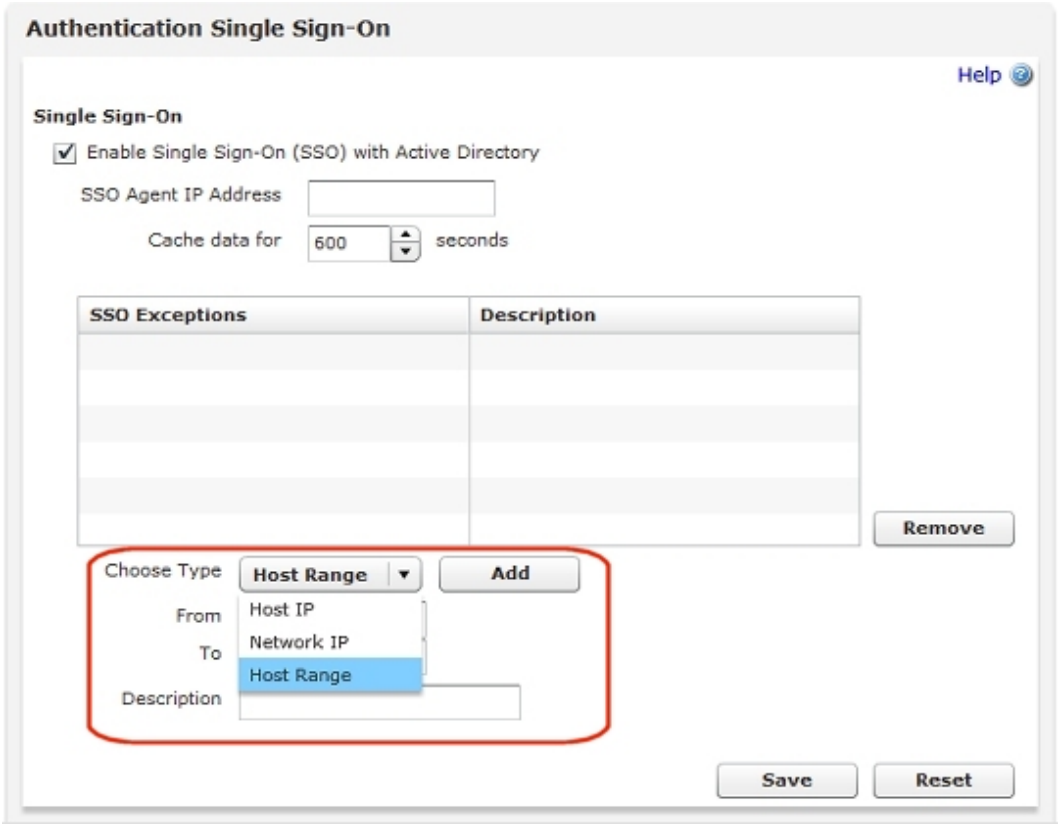
Define SSO Exceptions

If your network includes devices with IP addresses that do not require authentication, such as network servers, print servers, or computers that are not part of the domain, or if you have users on your internal network who must manually authenticate to the authentication login portal, we recommend that you add their IP addresses to the SSO Exceptions list. Each time a connection attempt occurs from an IP address that is not in the SSO Exceptions list, the XTM device contacts the SSO agent to try to associate the IP address with a user name. This takes about 10 seconds. You can use the SSO Exceptions list to prevent this delay for each connection, to reduce unnecessary network traffic, and enable users to authenticate and connect to your network without delay.

When you add an entry to the SSO Exceptions list, you can choose to add a host IP address, network IP address, subnet, or a host range.

To add an entry to the SSO Exceptions list:

1. From the **Choose Type** drop-down list, select the type of entry to add to the SSO Exceptions list:
   - **Host IP**
   - **Network IP**
   - **Host Range**



The text boxes that appear change based on the type you select.

2. Type the IP address for the type you selected.
   If you selected the type **Host Range**, type the start and end IP addresses for the range.
3. (Optional) In the **Description** text box, type a description to include with this exception in the **SSO Exceptions** list.
4. Click **Add**.
   The IP address or range appears in the SSO Exceptions list.
5. Click **Save**.

To remove an entry from the SSO Exceptions list:

1. From the **SSO Exceptions** list, select an entry.
2. Click **Remove**.
   The selected entry is removed from the SSO Exceptions list.
3. Click **Save**.

Install and Configure the Terminal Services Agent

When you have more than one user who connects to your Terminal Server or Citrix server and then connects to your network or the Internet, it can be difficult to control the individual traffic flows from these users based on their user names or group memberships. This is because when one user authenticates to the XTM device, the XTM device maps that user to the IP address of the Terminal Server or Citrix server. Then, when another user sends traffic from the Terminal Server or Citrix server IP address, it appears to the XTM device that this traffic also came from the first user that authenticated. There is no way for the XTM device to distinguish which of the several users who are concurrently logged on to your Terminal Server or Citrix generated any particular traffic.

To make sure that your users are correctly identified, you must:

1. Install the WatchGuard Terminal Services Agent on your Terminal Server (2003 or 2008) or Citrix server.
2. Configure your XTM device to redirect users to the authentication page for authentication.
3. Enable Terminal Services settings in your XTM device configuration file.

After you complete these configuration settings, when each Terminal Server or Citrix server user authenticates to your XTM device, the XTM device sends the Terminal Services Agent a user session ID for each user who logs in. The Terminal Services Agent monitors traffic generated by individual users and reports the user session ID to the XTM device for each traffic flow generated by a Terminal Server or Citrix server client. Your XTM device can then correctly identify each user and apply the correct security policies to the traffic for each user, based on user or group names.

When you use the Terminal Services Agent, your XTM device can enforce policies based on user or group names only for traffic that is authenticated. If traffic comes to the XTM device without session ID information, the XTM device manages the traffic in the same way it manages any other traffic for which it does not have the username mapped to an IP address. If there is a policy in your configuration file that can process traffic from that IP address, the XTM device uses that policy to process the traffic. If there is no policy that matches the source IP address of the traffic, the XTM device uses the *unhandled packet* rules to process the traffic.

For more information about how to configure settings for unhandled packets, see *About Unhandled Packets* on page 448.

If you use the Terminal Services Agent, your XTM device cannot automatically redirect users to the authentication portal.

To enable your XTM device to correctly process system related traffic from the Terminal Server or Citrix server, the Terminal Services Agent uses a special user account named *Backend-Service*, which is part of the Terminal Services Agent. The Terminal Services Agent identifies the traffic generated by system processes (instead of user traffic) with the Backend-Service user account. You can add this user to the **Authorized Users and Groups** list in your XTM device configuration and then use it in a policy to allow traffic to and from your server. For example, you can add a custom packet filter policy that is similar to the default Outgoing policy. Configure the policy to use the TCP-UDP protocol and allow traffic from the *Backend-Service* user account to *Any-External*.

For more information about how to add the Backend-Service user account to your XTM device configuration, see *Use Authorized Users and Groups in Policies* on page 285. Make sure to select **Any** from the **Auth Server** drop-down list.

For more information about how to add a policy, see *Add Policies to Your Configuration* on page 291.

Make sure the updates on your Terminal Server or Citrix server are scheduled to run as the system, local service, or network service user account. The Terminal Services Agent recognizes these user account as the Backend-Service account and allows the traffic. If you schedule updates to run as a different user account, that user must manually authenticate to the application portal for the server to receive the updates. If that user is not authenticated to the authentication portal, the traffic is not allowed and the server does not receive the update.

Before you install the Terminal Services Agent on your Terminal Server or Citrix server, make sure that terminal services or remote desktop services is enabled on your server, and open ports 4131–4134.

You cannot use the Terminal Services Agent with Single Sign-On (SSO). For more information about SSO, see *About Single Sign-On (SSO)*.

The Terminal Services Agent cannot control ICMP, NetBIOS, or DNS traffic. It also does not control traffic to port 4100 for Firebox Authentication. To control this traffic, you must add specific policies to your XTM device configuration file to allow ICMP, NetBIOS, or DNS traffic, and to allow Firebox Authentication.

Install the Terminal Services Agent

You can install the Terminal Services Agent on a Terminal Server or Citrix server with either a 32-bit or a 64-bit operating system. There are two versions of the Terminal Services Agent installer available: one for a 32-bit operating system and one for a 64-bit operating system. Make sure you select the correct installer for your operating system:

- 32-bit installer — **TO_AGENT_32.exe**
- 64-bit installer — **TO_AGENT_64.exe**

To install the Terminal Services Agent on your server:

1. Log in to the WatchGuard web site and go to the Software Downloads page.
2. Get the latest version of the TO Agent Installer (**TO_AGENT_32.exe** or **TO_AGENT_64.exe**) and copy it to the server where you have installed Terminal Services or a Citrix server.
3. Double-click the installer file to start the installer.
   The TO Agent wizard appears.
4. To start the wizard, click **Next**.
5. Complete the wizard to install the TO Agent on your server.
6. Reboot your Terminal Server or Citrix server.

Configure the Terminal Services Agent

After you install the Terminal Services Agent or TO (Traffic Owner) Agent on your Terminal Server or Citrix server, you can use the TO Settings tool to configure the settings for the TO Agent.

Because it is not necessary for the TO Agent to monitor traffic that is not controlled by the XTM device, you can specify a single destination IP address or a range of destination IP addresses for traffic that you do not want the TO Agent to monitor.

1. Select **Start > All programs > WatchGuard > TO Agent > Set Tool**.
   The TO Setting Tool dialog box appears, with the XTM Device Setting tab selected.

2. In the **Device IP Address** text box, type the IP address of the XTM device interface for the Terminal Server.
   If the terminal server is on the *Trusted* interface, type the trusted interface IP address.
   If the Terminal Server is on the *External* interface, type the external interface IP address.
3. Click **OK**.
4. To create log messages for the TO Agent, select the **Enable logging of TO Agent processes** check box.
5. To add destinations for traffic that you do not want the TO Agent to monitor, select the **Destination Exception List** tab.
6. Click **Add**.
   The Add Destination Exception dialog box appears.
7. From the **Choose Type** drop-down list, select an option:
   - **Host IP Address**
   - **Network IP Address**
   - **IP Address Range**
8. If you select **Host IP Address**, type the **IP Address** for the exception.
   If you select **Network IP Address**, type the **IP Address** and **Mask** for the exception.
   If you select **IP Address Range**, type the **Range from** and **Range to** for the exception.
9. Click **Add**.
   The information you specified appears in the Destination Exception List.
10. To add more addresses to the **Destination Exception List**, repeat Steps 4–7.
11. To view the available log files for the TO Agent, click **View Logs**.
    An Explorer window opens with the available log files you can review.
12. Click **Close**.

For detailed steps to complete the Terminal Services configuration for your XTM device, see *Configure Terminal Services Settings* on page 251.

Configure Terminal Services Settings

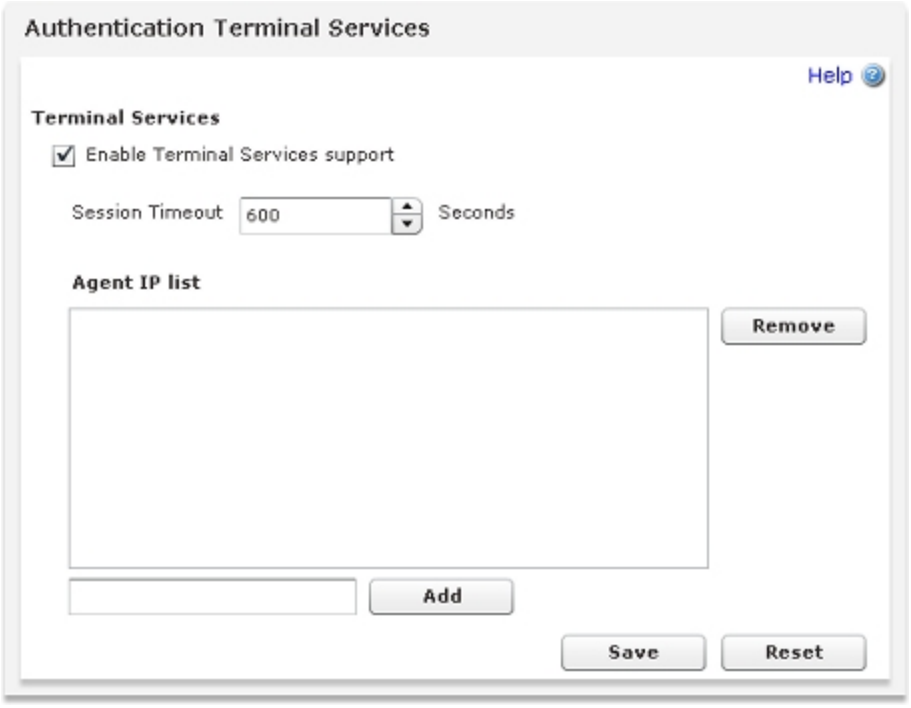
To enable your users to authenticate to your XTM device over a Terminal Server or Citrix server, you must configure the authentication settings for terminal services. When you configure these settings, you set the maximum length of time a session can be active and specify the IP address of your Terminal Server or Citrix server.

When you configure the Terminal Services Settings, if your users authenticate to your XTM device, the XTM device reports the actual IP address of each user who logs in. This enables your XTM device to correctly identify each user who logs in to your network, so the correct security policies can be applied to each user's traffic.

You can use any of your configured authentication server methods (for example, Firebox authentication, Active Directory, or RADIUS) with terminal services.

To configure Authentication Settings for terminal services:

1. Select **Authentication > Terminal Services**.
   The Authentication Terminal Services page appears.
2. Select the **Enable Terminal Services Support** check box.
   The terminal services settings are enabled.



3. In the **Session Timeout** text box, type or select the maximum length of time in seconds that the user can send traffic to the external network.
   If you select zero (0) seconds, the session does not expire and the user can stay connected for any length of time.
4. To add a Terminal Server or Citrix server to the **Agent IP list** list, in the text box, type the IP address of the server and click **Add**.
   The IP address appears in the Terminal Services Agent IPs List list.
5. To remove a server IP address from the **Agent IP list** list, select an IP address in the list and click **Remove**.
6. Click **Save**.

Authentication Server Types

The Fireware XTM OS supports six authentication methods:

- *Configure Your XTM Device as an Authentication Server*
- *Configure RADIUS Server Authentication*
- *Configure VASCO Server Authentication*
- *Configure SecurID Authentication*
- *Configure LDAP Authentication*
- *Configure Active Directory Authentication*

You can configure one or more authentication server types for an XTM device. If you use more than one type of authentication server, users must select the authentication server type from a drop-down list when they authenticate.

About Third-Party Authentication Servers

If you use a third-party authentication server, you do not have to keep a separate user database on the XTM device. You can configure a third-party server, install the authentication server with access to your XTM device, and put the server behind the device for security. You then configure the device to forward user authentication requests to that server. If you create a user group on the XTM device that authenticates to a third-party server, make sure you create a group on the server that has the same name as the user group on the device.

For detailed information about how to configure an XTM device for use with third-party authentication servers, see:

- *Configure RADIUS Server Authentication*
- *Configure VASCO Server Authentication*
- *Configure SecurID Authentication*
- *Configure LDAP Authentication*
- *Configure Active Directory Authentication*

Use a Backup Authentication Server

You can configure a primary and a backup authentication server with any of the third-party authentication server types. If the XTM device cannot connect to the primary authentication server after three attempts, the primary server is marked as inactive and an alarm message is generated. The device then connects to the backup authentication server.

If the XTM device cannot connect to the backup authentication server, it waits ten minutes, and then tries to connect to the primary authentication server again. The inactive server is marked as active after the specified time interval is reached.

For detailed procedures to configure primary and backup authentication servers, see the configuration topic for your third-party authentication server.

Configure Your XTM Device as an Authentication Server

If you do not use a third-party authentication server, you can use your XTM device as an authentication server, also known as Firebox authentication. When you configure Firebox authentication, you create users accounts for each user in your company, and then divide these users into groups for authentication. When you assign users to groups, make sure to associate them by their tasks and the information they use. For example, you can have an accounting group, a marketing group, and a research and development group. You can also have a new employee group with more controlled access to the Internet.

When you create a group, you set the authentication procedure for the users, the system type, and the information they can access. A user can be a network or one computer. If your company changes, you can add or remove users from your groups.

The Firebox authentication server is enabled by default. You do not have to enable it before you add users and groups.

Types of Firebox Authentication

You can configure your XTM device to authenticate users with four different types of authentication:

- Firewall Authentication
- Mobile VPN with PPTP Connections
- Mobile VPN with IPSec Connections
- Mobile VPN with SSL Connections

When authentication is successful, the XTM device links these items:

- User name
- Firebox User group (or groups) of which the user is a member
- IP address of the computer used to authenticate
- Virtual IP address of the computer used to connect with Mobile VPN

Firewall Authentication

To enable your users to authenticate, you create user accounts and groups. When a user authenticates with the XTM device, the user credentials and computer IP address are used to find whether a policy applies to the traffic that the computer sends and receives.

To create a Firebox user account:

1. *Define a New User for Firebox Authentication*.
2. *Define a New Group for Firebox Authentication* and put the new user in that group.
3. Create a policy that allows traffic only to or from a list of Firebox user names or groups.
   This policy is applied only if a packet comes from or goes to the IP address of the authenticated user.

To authenticate with an HTTPS connection to the XTM device over port 4100:

1. Open a web browser and go to `https://<IP address of a XTM device interface>:4100/`
   The login page appears.
2. Type the **Username** and **Password**.
3. From the **Domain** drop-down list, select the domain to use for authentication.
   This option only appears if you can choose from more than one domain.
4. Click **Login**.

If the credentials are valid, the user is authenticated.

Firewall authentication takes precedence over Single Sign-On, and replaces the user credentials and IP address from your Single Sign-On session with the user credentials and IP address you select for Firewall authentication. For more information about how to configure Single Sign-On, see *About Single Sign-On (SSO)* on page 242.

Mobile VPN with PPTP Connections

When you activate Mobile VPN with PPTP on your XTM device, users included in the Mobile VPN with PPTP group can use the PPTP feature included in their computer operating system to make a PPTP connection to the device.

Because the XTM device allows the PPTP connection from any Firebox user that gives the correct credentials, it is important that you make a policy for PPTP sessions that includes only users you want to allow to send traffic over the PPTP session. You can also add a group or individual user to a policy that restricts access to resources behind the XTM device. The XTM device creates a pre-configured group called *PPTP-Users* for this purpose.

To configure a Mobile VPN with PPTP connection:

1. From Fireware XTM Web UI, select **VPN > Mobile VPN with PPTP**.
2. Select the **Activate Mobile VPN with PPTP** check box.
3. Make sure the **Use Radius authentication for PPTP users** check box is not selected.

   If this check box is selected, the RADIUS authentication server authenticates the PPTP session.
   If you clear this check box, the XTM device authenticates the PPTP session.

The XTM device checks to see whether the user name and password the user types in the VPN connection dialog box match the user credentials in the Firebox User database that is a member of the PPTP-Users group.
If the credentials supplied by the user match an account in the Firebox User database, the user is authenticated for a PPTP session.

4. Create a policy that allows traffic only from or to a list of Firebox user names or groups.
The XTM device does not look at this policy unless traffic comes from or goes to the IP address of the authenticated user.

Mobile VPN with IPSec Connections

When you configure your XTM device to host Mobile VPN with IPSec sessions, you create policies on your device and then use the Mobile VPN with IPSec client to enable your users to access your network. After the XTM device is configured, each client computer must be configured with the Mobile VPN with IPSec client software.

When the user's computer is correctly configured, the user makes the Mobile VPN connection. If the credentials used for authentication match an entry in the Firebox User database, and if the user is in the Mobile VPN group you create, the Mobile VPN session is authenticated.

To set up authentication for Mobile VPN with IPSec:

1. *Configure a Mobile VPN with IPSec Connection*.
2. *Install the Mobile VPN with IPSec Client Software*.

Mobile VPN with SSL Connections

You can configure the XTM device to host Mobile VPN with SSL sessions. When the XTM device is configured with a Mobile VPN with SSL connection, users included in the Mobile VPN with SSL group can install and use the Mobile VPN with SSL client software to make an SSL connection.

Because the XTM device allows the SSL connection from any of your users who give the correct credentials, it is important that you make a policy for SSL VPN sessions that includes only users you want to allow to send traffic over SSL VPN. You can also add these users to a Firebox User Group and make a policy that allows traffic only from this group. The XTM device creates a pre-configured group called *SSLVPN-Users* for this purpose.

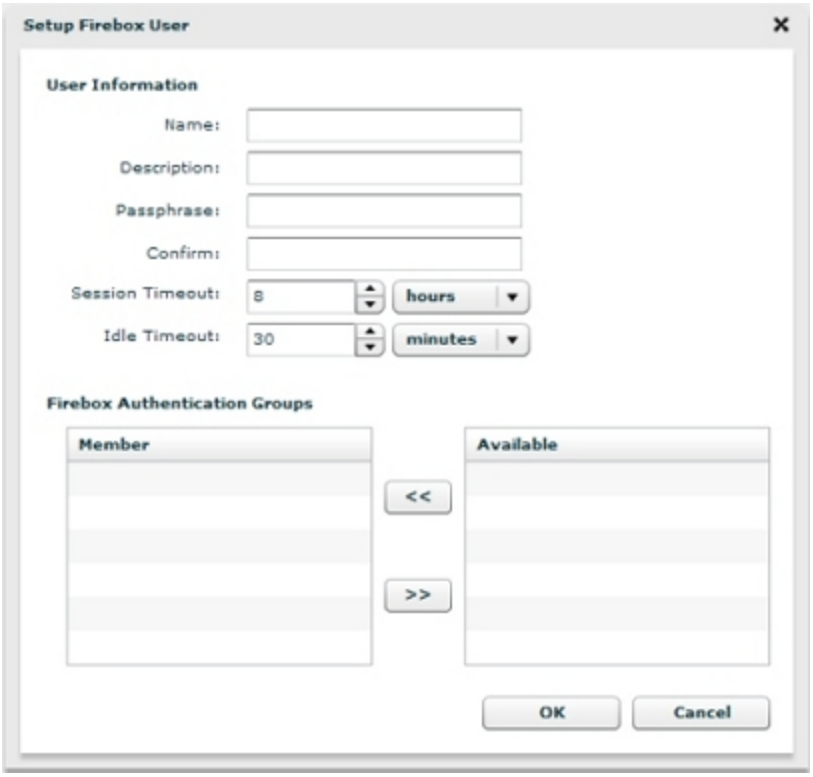
To configure a Mobile VPN with SSL connection:

1. From Fireware XTM Web UI, select **VPN > Mobile VPN with SSL**.
The Mobile VPN with SSLVPN page appears.
2. *Configure the XTM Device for Mobile VPN with SSL*.

Define a New User for Firebox Authentication

You can use Fireware XTM Web UI to specify which users can authenticate to your XTM device.

1. Select **Authentication > Servers**.
The Authentication Servers page appears.
2. On the **Firebox** tab, in the **Users** section, click **Add**.
The Setup Firebox User dialog box appears.



3. Type the **Name** and (optional) a **Description** of the new user.
4. Type and confirm the **Passphrase** you want the person to use to authenticate.

> ***Note*** *When you set this passphrase, the characters are masked and it does not appear in simple text again. If you lose the passphrase, you must set a new passphrase.*

5. In the **Session Timeout** text box, type or select the maximum length of time the user can send traffic to the external network.

   The minimum value for this setting is one (1) seconds, minutes, hours, or days. The maximum value is 365 days.

6. In the **Idle Timeout** text box, type or select the length of time the user can stay authenticated when idle (not passing any traffic to the external network).

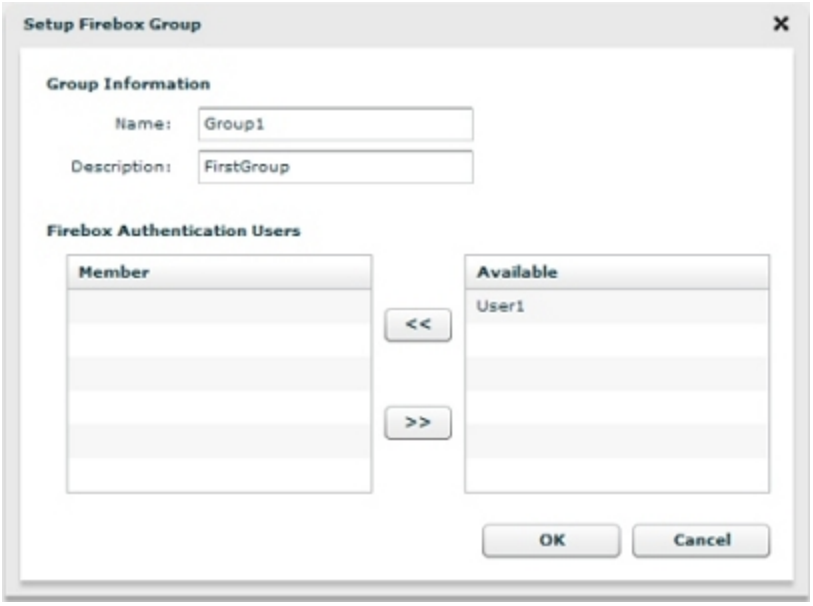
   The minimum value for this setting is one (1) seconds, minutes, hours, or days. The maximum value is 365 days.

7. To add a user to a Firebox Authentication Group, select the user name in the **Available** list.
8. Click to move the name to the **Member** list.
   Or, you can double-click the user name in the **Available** list.
   The user is added to the user list. You can then add more users.
9. To close the **Setup Firebox User** dialog box, click **OK**.
   The Firebox Users tab appears with a list of the new users.

Define a New Group for Firebox Authentication

You can use Fireware XTM Web UI to specify which user groups can authenticate to your XTM device.

1. Select **Authentication > Servers**.
   The Authentication Servers page appears.
2. Select the **Firebox** tab.
3. In the **Groups** section, click **Add**.
   The Setup Firebox Group dialog box appears.



4. Type a name for the group.
5. (Optional) Type a description for the group.
6. To add a user to the group, select the user name in the **Available** list. Click to move the name to the **Member** list.
   You can also double-click the user name in the Available list.
7. After you add all necessary users to the group, click **OK**.

You can now configure policies and authentication with these users and groups, as described in *Use Authorized Users and Groups in Policies* on page 285.

Configure RADIUS Server Authentication

RADIUS (Remote Authentication Dial-In User Service) authenticates the local and remote users on a company network. RADIUS is a client/server system that keeps the authentication information for users, remote access servers, VPN gateways, and other resources in one central database.

For more information on RADIUS authentication, see *How RADIUS Server Authentication Works* on page 261.

Authentication Key

The authentication messages to and from the RADIUS server use an authentication key, not a password. This authentication key, or shared secret, must be the same on the RADIUS client and server. Without this key, there is no communication between the client and server.

RADIUS Authentication Methods

For web and Mobile VPN with IPSec or SSL authentication, RADIUS supports only PAP (Password Authentication Protocol) authentication.

For authentication with PPTP, RADIUS supports only MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).

For authentication with WPA Enterprise and WPA2 Enterprise authentication methods, RADIUS supports the EAP (Extensible Authentication Protocol) framework.

Before You Begin

Before you configure your XTM device to use your RADIUS authentication server, you must have this information:

- Primary RADIUS server — IP address and RADIUS port
- Secondary RADIUS server (optional) — IP address and RADIUS port
- Shared secret — Case-sensitive password that is the same on the XTM device and the RADIUS server
- Authentication methods — Set your RADIUS server to allow the authentication method your XTM device uses: PAP, MS CHAP v2, WPA Enterprise, WPA2 Enterprise, or WPA/WPA2 Enterprise

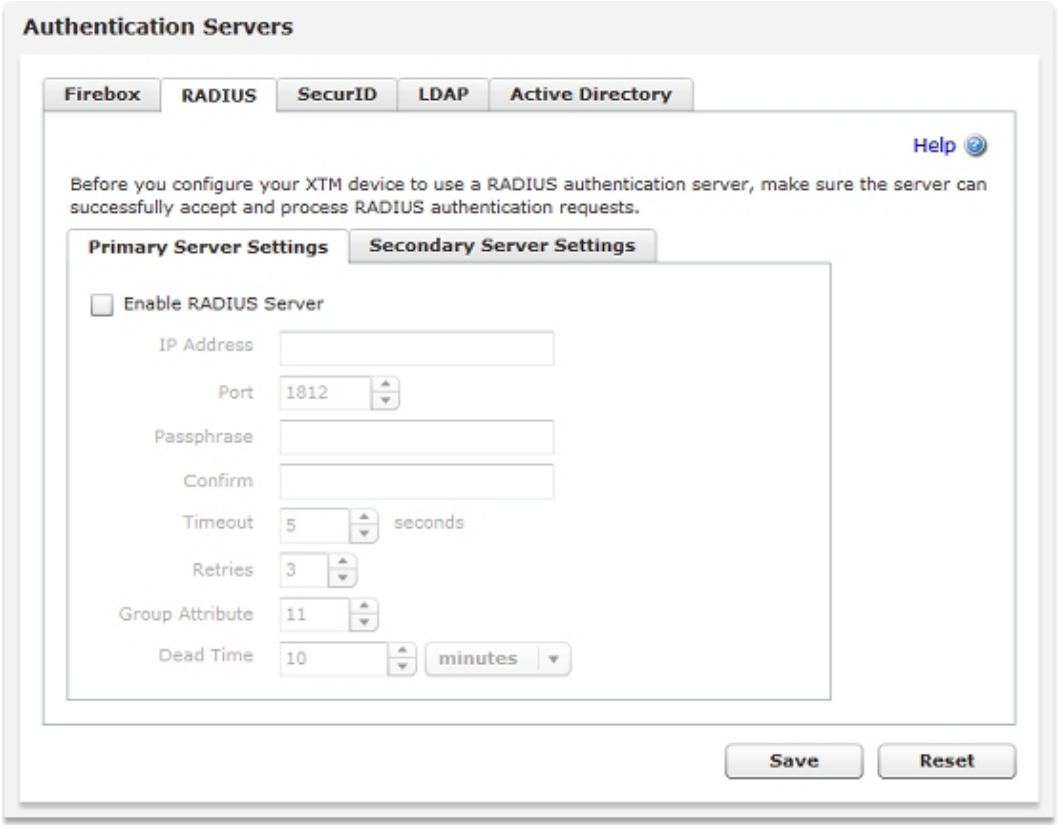
Use RADIUS Server Authentication with Your XTM Device

To use RADIUS server authentication with your XTM device, you must:

- Add the IP address of the XTM device to the RADIUS server as described in the documentation from your RADIUS vendor.
- Enable and specify the RADIUS server in your XTM device configuration.
- Add RADIUS user names or group names to your policies.

To enable and specify the RADIUS server(s) in your configuration, from Fireware XTM Web UI:

1. Select **Authentication > Servers**.
   The Authentication Servers page appears.
2. Select the **RADIUS** tab.



3. Select the **Enable RADIUS Server** check box.
4. In the **IP Address** text box, type the IP address of the RADIUS server.
5. In the **Port** text box, make sure that the port number RADIUS uses for authentication appears. The default port number is 1812. Older RADIUS servers might use port 1645.
6. In the **Passphrase** text box, type the shared secret between the XTM device and the RADIUS server. The shared secret is case-sensitive, and it must be the same on the XTM device and the RADIUS server.
7. In the **ConfirmPassphrase** text box, type the shared secret again.
8. Type or select the **Timeout** value.

   The timeout value is the amount of time the XTM device waits for a response from the authentication server before it tries to connect again.

9. In the **Retries** text box, type or select the number of times the XTM device tries to connect to the authentication server (the timeout is specified above) before it reports a failed connection for one authentication attempt.
10. In the **Group Attribute** text box, type or select an attribute value. The default group attribute is FilterID, which is RADIUS attribute **11**.

    The group attribute value is used to set the attribute that carries the User Group information. You must configure the RADIUS server to include the Filter ID string with the user authentication message it sends to the XTM device. For example, *engineerGroup* or *financeGroup*. This information is then used for access control. The XTM device matches the FilterID string to the group name configured in the XTM device policies.

11. In the **Dead Time** text box, type or select the amount of time after which an inactive server is marked as active again. Select **minutes** or **hours** from the drop-down list to change the duration.

    After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts will not try this server until it is marked as active again.

12. To add a backup RADIUS server, select the **Secondary Server Settings** tab, and select the **Enable Secondary RADIUS Server** check box.
13. Repeat Steps 4–11 to configure the backup server. Make sure the shared secret is the same on the primary and backup RADIUS server.

    For more information, see *Use a Backup Authentication Server* on page 253.

14. Click **Save**.

How RADIUS Server Authentication Works

RADIUS is a protocol that was originally designed to authenticate remote users to a dial-in access server. RADIUS is now used in a wide range of authentication scenarios. RADIUS is a client-server protocol, with the XTM device as the client and the RADIUS server as the server. (The RADIUS client is sometimes called the Network Access Server or NAS.) When a user tries to authenticate, the XTM device sends a message to the RADIUS server. If the RADIUS server is properly configured to have the XTM device as a client, RADIUS sends an *accept* or *reject* message back to the XTM device (the Network Access Server).

When the XTM device uses RADIUS for an authentication attempt:

1. The user tries to authenticate, either through a browser-based HTTPS connection to the XTM device over port 4100, or through a connection using Mobile VPN with PPTP or IPSec. The XTM device reads the user name and password.
2. The XTM device creates a message called an Access-Request message and sends it to the RADIUS server. The XTM device uses the RADIUS shared secret in the message. The password is always encrypted in the Access-Request message.
3. The RADIUS server makes sure that the Access-Request message is from a known client (the XTM device). If the RADIUS server is not configured to accept the XTM device as a client, the server discards the Access-Request message and does not send a message back.
4. If the XTM device is a client known to the RADIUS server and the shared secret is correct, the server looks at the authentication method requested in the Access-Request message.
5. If the Access-Request message uses an allowed authentication method, the RADIUS server gets the user credentials from the message and looks for a match in a user database. If the user name and password match an entry in the database, the RADIUS server can get additional information about the user from the user database (such as remote access approval, group membership, logon hours, and so on).
6. The RADIUS server checks to see whether it has an access policy or a profile in its configuration that matches all the information it has about the user. If such a policy exists, the server sends a response.
7. If any of the previous conditions fail, or if the RADIUS server has no matching policy, it sends an Access-Reject message that shows authentication failure. The RADIUS transaction ends and the user is denied access.
8. If the Access-Request message meets all the previous conditions, RADIUS sends an Access-Accept message to the XTM device.
9. The RADIUS server uses the shared secret for any response it sends. If the shared secret does not match, the XTM device rejects the RADIUS response.

To see diagnostic log messages for authentication, *Set the Diagnostic Log Level* and change the log level for the **Authentication** category.

10. The XTM device reads the value of any FilterID attribute in the message. It connects the user name with the FilterID attribute to put the user in a RADIUS group.
11. The RADIUS server can put a large amount of additional information in the Access-Accept message. The XTM device ignores most of this information, such as the protocols the user is allowed to use (such as PPP or SLIP), the ports the user can access, idle timeouts, and other attributes.
12. The XTM device only requires the FilterID attribute (RADIUS attribute number 11). The FilterID is a string of text that you configure the RADIUS server to include in the Access-Accept message. This attribute is necessary for the XTM device to assign the user to a RADIUS group, however, it can support some other Radius attributes such as Session-Timeout (RADIUS attribute number 27) and Idle-Timeout (RADIUS attribute number 28).

For more information on RADIUS groups, see the subsequent section.

About RADIUS Groups

When you configure RADIUS authentication, you can set the Group Attribute number. Fireware XTM reads the Group Attribute number from Fireware XTM Web UI to tell which RADIUS attribute carries RADIUS group information. Fireware XTM recognizes only RADIUS attribute number 11, FilterID, as the Group Attribute. When you configure the RADIUS server, do not change the Group Attribute number from its default value of 11.

When the XTM device gets the Access-Accept message from RADIUS, it reads the value of the FilterID attribute and uses this value to associate the user with a RADIUS group. (You must manually configure the FilterID in your RADIUS configuration.) Thus, the value of the FilterID attribute is the name of the RADIUS group where the XTM device puts the user.

The RADIUS groups you use in Fireware XTM Web UI are not the same as the Windows groups defined in your domain controller, or any other groups that exist in your domain user database. A RADIUS group is only a logical group of users the XTM device uses. Make sure you carefully select the FilterID text string. You can make the value of the FilterID match the name of a local group or domain group in your organization, but this is not necessary. We recommend you use a descriptive name that helps you remember how you defined your user groups.

Practical Use of RADIUS Groups

If your organization has many users to authenticate, you can make your XTM device policies easier to manage if you configure RADIUS to send the same FilterID value for many users. The XTM device puts those users into one logical group so you can easily administer user access. When you make a policy in Fireware XTM Web UI that allows only authenticated users to access a network resource, you use the RADIUS Group name instead of adding a list of many individual users.

For example, when Mary authenticates, the FilterID string RADIUS sends is *Sales*, so the XTM device puts Mary in the *Sales* RADIUS group for as long as she is authenticated. If users John and Alice subsequently authenticate, and RADIUS puts the same FilterID value *Sales* in the Access-Accept messages for John and Alice, then Mary, John, and Alice are all in the *Sales* group. You can make a policy in Fireware XTM Web UI that allows the group *Sales* to access a resource.

You can configure RADIUS to return a different FilterID, such as *IT Support*, for the members of your internal support organization. You can then make a different policy to allow *IT Support* users to access resources.

For example, you might allow the *Sales* group to access the Internet using a Filtered-HTTP policy. Then you can filter their web access with WebBlocker. A different policy in Policy Manager can allow the *IT Support* users to access the Internet with the Unfiltered-HTTP policy, so that they access the web without WebBlocker filtering. You use the RADIUS group name (or user names) in the **From** field of a policy to show which group (or which users) can use the policy.

Timeout and Retry Values

An authentication failure occurs when no response is received from the primary RADIUS server. After three authentication attempts fail, Fireware XTM uses the secondary RADIUS server. This process is called *failover*.

> ***Note*** *This number of authentication attempts is not the same as the Retry number. You cannot change the number of authentication attempts before failover occurs.*

The XTM device sends an Access-Request message to the first RADIUS server in the list. If there is no response, the XTM device waits the number of seconds set in the **Timeout** box, and then it sends another Access-Request. This continues for the number of times indicated in the **Retry** box (or until there is a valid response). If there is no valid response from the RADIUS server, or if the RADIUS shared secret does not match, Fireware XTM counts this as one failed authentication attempt.

After three authentication attempts fail, Fireware XTM uses the secondary RADIUS server for the next authentication attempt. If the secondary server also fails to respond after three authentication attempts, Fireware XTM waits ten minutes for an administrator to correct the problem. After ten minutes, Fireware XTM tries to use the primary RADIUS server again.

WPA and WPA2 Enterprise Authentication

To add another layer of security when your users connect to your wireless network, you can enable enterprise authentication methods on your XTM wireless device. When you configure an enterprise authentication method, the client must have the correct authentication method configured to successfully connect to the XTM device. The XTM wireless device then sends authentication requests to the configured authentication server (RADIUS server or Firebox-DB). If the authentication method information is not correct, the user cannot connect to the device, and is not allowed access to your network.

In Fireware XTM v11.4 and later, the available enterprise authentication methods are WPA Enterprise and WPA2 Enterprise. These authentication methods are based on the IEEE 802.1X standard, which uses the EAP (Extensible Authentication Protocol) framework to enable user authentication to an external RADIUS server or to your XTM device (Firebox-DB). The WPA Enterprise and WPA2 Enterprise authentication methods are more secure than WPA/WPA2 (PSK) because users must first have the correct authentication method configured, and then authenticate with their own enterprise credentials instead of one shared key that is known by everyone who uses the wireless access point.

You can use the WPA Enterprise and WPA2 Enterprise authentication methods with XTM wireless devices. For more information about how to configure your XTM wireless device to use enterprise authentication, see *Set the Wireless Authentication Method* on page 176.

Configure VASCO Server Authentication

VASCO server authentication uses the VACMAN Middleware or IDENTIKEY Server software to authenticate remote users on a company network through a RADIUS or web server environment. VASCO also supports multiple authentication server environments. The VASCO one-time password token system enables you to eliminate the weakest link in your security infrastructure—the use of static passwords.

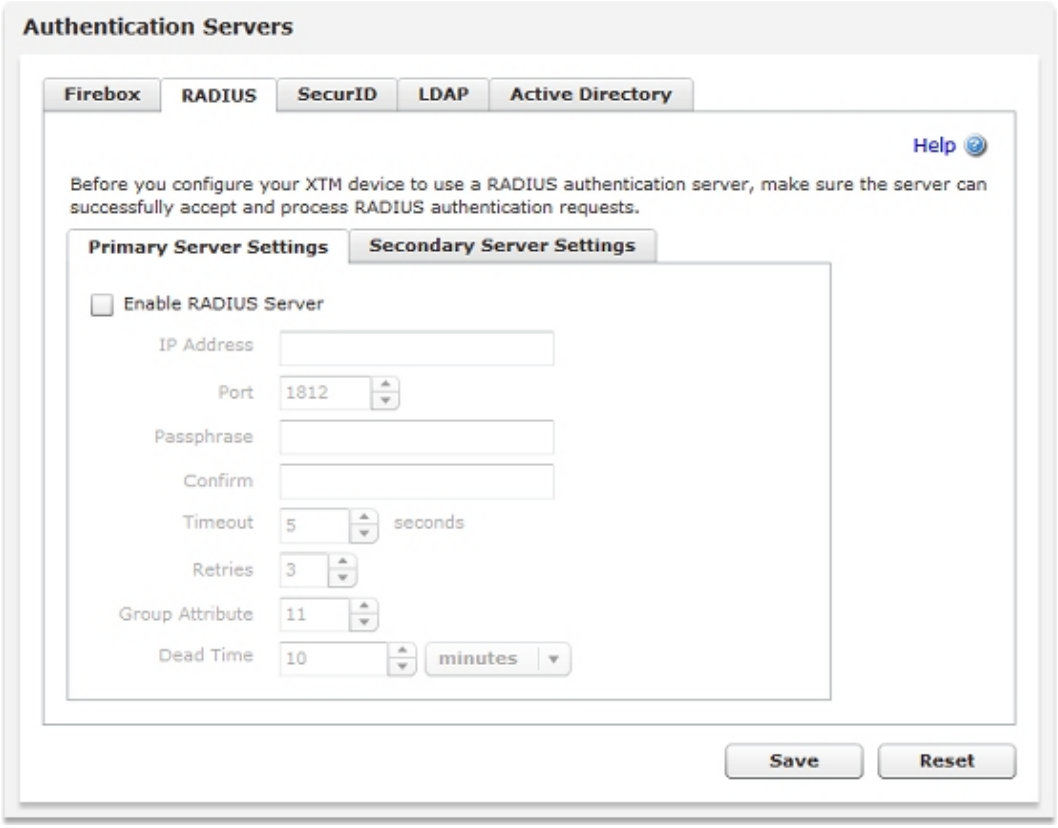
To use VASCO server authentication with your XTM device, you must:

- Add the IP address of the XTM device to the VACMAN Middleware or IDENTIKEY server, as described in the documentation from your VASCO vendor.
- Enable and specify the VACMAN Middleware or IDENTIKEY server in your XTM device configuration.
- Add user names or group names to the policies in Policy Manager.

To configure VASCO server authentication, use the RADIUS server settings. The **Authentication Servers** dialog box does not have a separate tab for VACMAN Middleware or IDENTIKEY servers.

From Fireware XTM Web UI:

1. Select **Authentication > Servers**.
   The Authentication Servers page appears.
2. Select the **RADIUS** tab.



3. To enable the VACMAN Middleware or IDENTIKEY server, select the **Enable RADIUS Server** check box.
4. In the **IP Address** text box, type the IP address of the VACMAN Middleware or IDENTIKEY server.
5. In the **Port** text box, make sure that the port number VASCO uses for authentication appears. The default port number is 1812.
6. In the **Passphrase** text box, type the shared secret between the XTM device and the VACMAN Middleware or IDENTIKEY server.
   The shared secret is case-sensitive, and it must be the same on the XTM device and the server.
7. In the **Confirm** text box, type the shared secret again.
8. In the **Timeout** text box, type or select the amount of time the XTM device waits for a response from the authentication server before it tries to connect again.
9. In the **Retries** text box, type or select the number of times the XTM device tries to connect to the authentication server before it reports a failed connection for one authentication attempt.
10. Type or select the **Group Attribute** value. The default group attribute is FilterID, which is VASCO attribute **11**.

    The group attribute value is used to set which attribute carries the user group information. You must configure the VASCO server to include the Filter ID string with the user authentication message it sends to the XTM device. For example, *engineerGroup* or *financeGroup*. This information is then used for access control. The XTM device matches the FilterID string to the group name configured in the XTM device policies.

11. In the **Dead Time** text box, type or select the amount of time after which an inactive server is marked as active again. Select **minutes** or **hours** from the drop-down list to change the duration.

After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts do not try to connect to this server until it is marked as active again.

12. To add a backup VACMAN Middleware or IDENTIKEY server, select the **Secondary Server Settings** tab, and select the **Enable Secondary RADIUS Server** check box.
13. Repeat Steps 4–11 to configure the backup server. Make sure the shared secret is the same on the primary and secondary VACMAN Middleware or IDENTIKEY server.

    For more information, see *Use a Backup Authentication Server* on page 253.

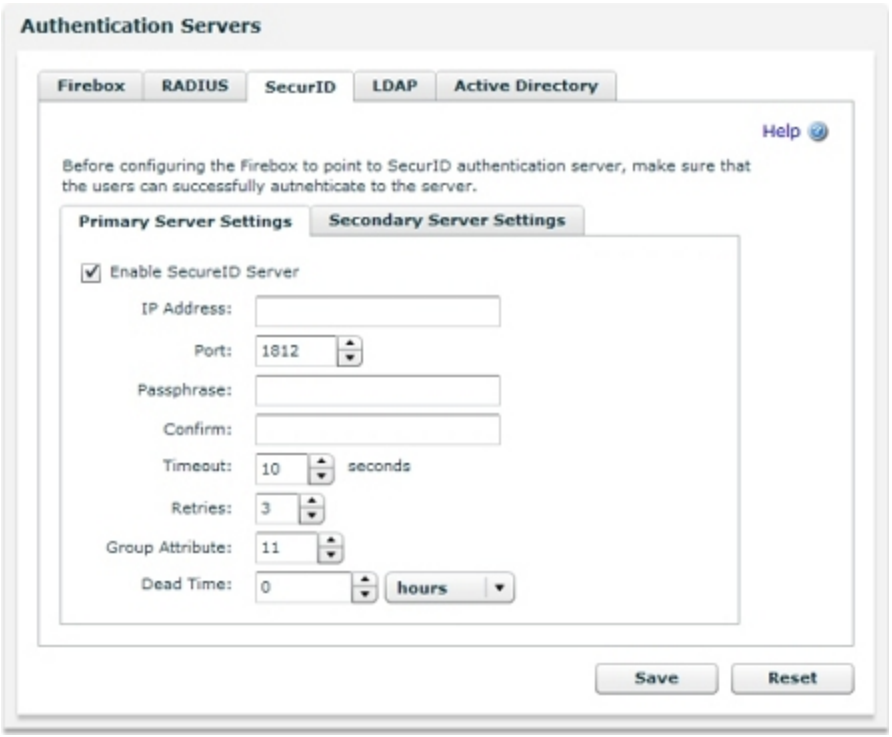
14. Click **Save**.

Configure SecurID Authentication

To use SecurID authentication, you must configure the RADIUS, VASCO, and ACE/Server servers correctly. The users must also have an approved SecurID token and a PIN (personal identification number). Refer to the RSA SecurID documentation for more information.

From Fireware XTM Web UI:

1. Select **Authentication > Servers**.
   The Authentication Servers page appears.
2. Select the **SecurID** tab.



3. Select the **Enable SecurID Server** check box.
4. In the **IP Address** text box, type the IP address of the SecurID server.
5. Click the **Port** field up or down arrow to set the port number to use for SecurID authentication. The default number is 1812.
6. In the **Passphrase** text box, type the shared secret between the XTM device and the SecurID server. The shared secret is case-sensitive and must be the same on the XTM device and the SecurID server.
7. In the **Confirm** text box, type the shared secret again.
8. In the **Timeout** text box, type or select the amount of time that the XTM device waits for a response from the authentication server before it tries to connect again.
9. In the **Retries**text box, type or select the number of times the XTM device tries to connect to the authentication server before it reports a failed connection for one authentication attempt.
10. In the **Group Attribute** text box, type or select the group attribute value. We recommend that you do not change this value.

The group attribute value is used to set the attribute that carries the user group information. When the SecurID server sends a message to the XTM device that a user is authenticated, it also sends a user group string. For example, *engineerGroup* or *financeGroup*. This information is then used for access control.

11. In the **Dead Time** text box, type or select the amount of time after which an inactive server is marked as active again. Select **minutes** or **hours** from the adjacent drop-down list to change the duration.

    After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts do not use this server until it is marked as active again, after the dead time value is reached.

12. To add a backup SecurID server, select the **Secondary Server Settings** tab, and select the **Enable Secondary SecurID Server** check box.
13. Repeat Steps 4–11 to configure the backup server. Make sure the shared secret is the same on the primary and backup SecurID servers.

    For more information, see *Use a Backup Authentication Server* on page 253.

14. Click **Save**.

Configure LDAP Authentication

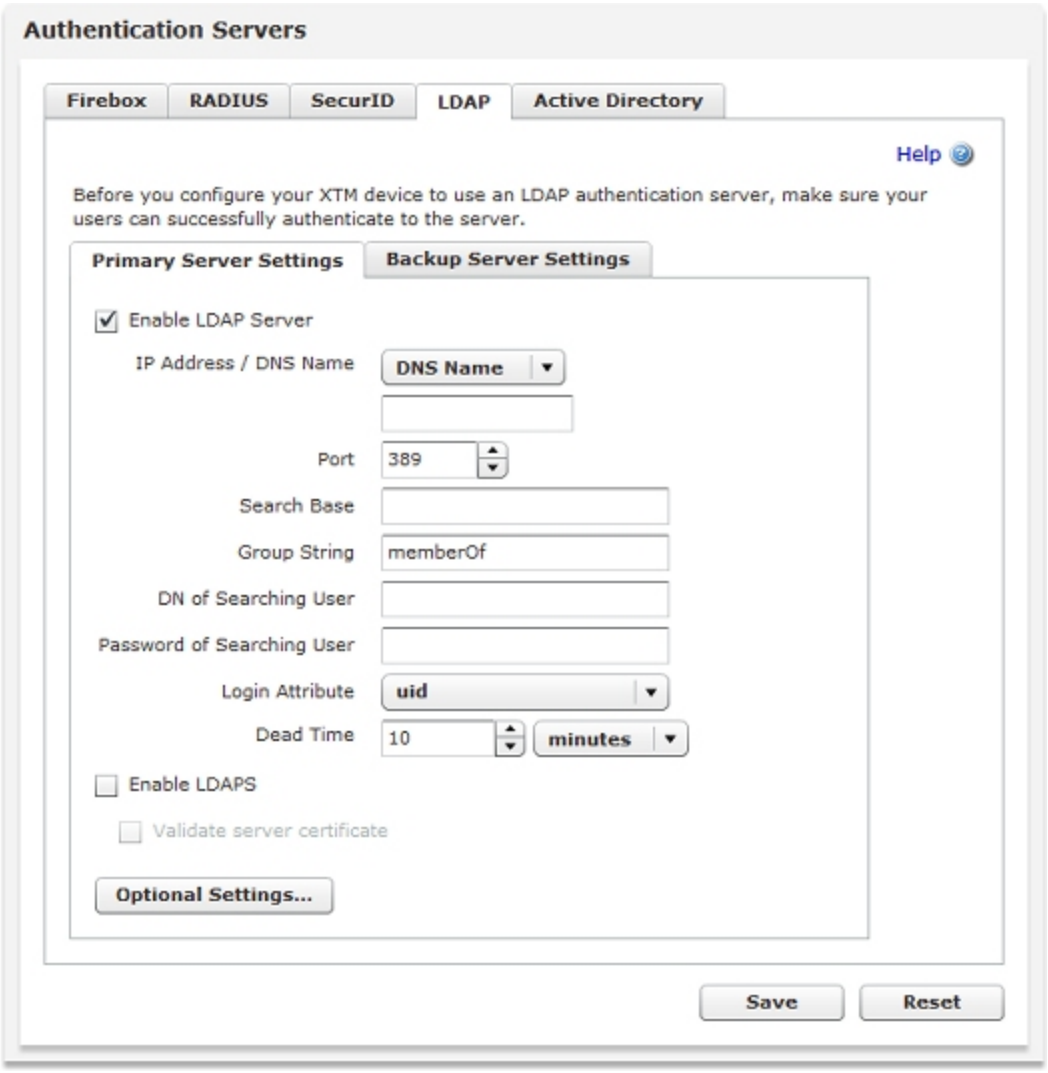
You can use an LDAP (Lightweight Directory Access Protocol) authentication server to authenticate your users with the XTM device. LDAP is an open-standard protocol for using online directory services, and it operates with Internet transport protocols, such as TCP. Before you configure your XTM device for LDAP authentication, make sure you check the documentation from your LDAP vendor to see if your installation supports the *memberOf* (or equivalent) attribute. When you configure your primary and backup LDAP server settings, you can select whether to specify the IP address or the DNS name of your LDAP server.

If your users authenticate with the LDAP authentication method, their distinguished names (DN) and passwords are not encrypted. To use LDAP authentication and encrypt user credentials, you can select the LDAPS (LDAP over SSL) option. When you use LDAPS, the traffic between the LDAP client on your XTM device and your LDAP server is secured by an SSL tunnel. When you enable this option, you can also choose whether to enable the LDAPS client to validate the LDAP server certificate, which prevents man-in-the-middle attacks. If you choose to use LDAPS and you specify the DNS name of your server, make sure the search base you specify includes the DNS name of your server. The standard LDAPS port is 636. For Active Directory Global Catalog queries, the SSL port is 3269.

When you configure the LDAP authentication method, you set a search base to specify where in the authentication server directories the XTM device can search for an authentication match. For example, if your user accounts are in an OU (organizational unit) you refer to as *accounts* and your domain name is *example.com*, your search base is `ou=accounts,dc=example,dc=com`.

From Fireware XTM Web UI:

1. Select **Authentication > Servers**.
   The Authentication Servers page appears.
2. Select the **LDAP** tab.
3. Select the **Enable LDAPServer** check box
   The LDAP server settings are enabled.



3. From the **IP Address/DNS Name** drop-down list, select whether to use the IP address or DNS name to contact your primary LDAP server.
4. In the **IP Address/DNS Name** text box, type the IP address or DNS name of the primary LDAP server for the XTM device to contact with authentication requests.
   The LDAP server can be located on any XTM device interface. You can also configure your device to use an LDAP server on a remote network through a VPN tunnel.
5. In the **Port** text box, select the TCP port number for the XTM device to use to connect to the LDAP server. The default port number is 389.
   If you enable LDAPS, you must select port 636.
6. In the **Search Base** text box, type the search base settings in the standard format: ou=organizational unit,dc=first part of distinguished server name,dc=any part of the distinguished server name that appears after the dot.
   For example: `ou=accounts,dc=example,dc=com`
7. In the **Group String** text box, type the group string attribute.

   This attribute string holds user group information on the LDAP server. On many LDAP servers, the default group string is *uniqueMember*; on other servers, it is *member*.

8. In the **DN of Searching User** text box, type the distinguished name (DN) for a search operation.

   You can add any user DN with the privilege to search LDAP/Active Directory, such as *Administrator*. Some administrators create a new user that only has searching privileges for use in this field.

9. In the **Password of Searching User** text box, type the password associated with the distinguished name for a search operation.
10. In the **Login Attribute** text box, select a LDAP login attribute to use for authentication from the drop-down list.

    The login attribute is the name used for the bind to the LDAP database. The default login attribute is *uid*. If you use *uid*, the **DN of Searching User** and the **Password of Searching User** text boxes can be empty.

11. In the **Dead Time** text box, type or select the amount of time after which an inactive server is marked as active again. Select **minutes** or **hours** from the adjacent drop-down list to set the duration.

    After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts do not try this server until it is marked as active again.

12. To enable secure SSL connections to your LDAP server, select the **Enable LDAPS** check box.
13. To verify the certificate of the LDAP server is valid, select the **Validate server certificate** check box.
14. To specify optional attributes for the primary LDAP server, click **Optional Settings**.
    For more information about how to configure optional settings, see the subsequent section.
15. To add a backup LDAP server, select the **Secondary Server Settings** tab, and select the **Enable Secondary LDAP Server** check box.
16. Repeat Steps 3–14 to configure the backup server. Make sure the shared secret is the same on the primary and backup LDAP servers.
    For more information, see *Use a Backup Authentication Server* on page 253.
17. Click **Save**.

About LDAP Optional Settings

Fireware XTM can get additional information from the directory server (LDAP or Active Directory) when it reads the list of attributes in the server's search response. This lets you use the directory server to assign extra parameters to the authenticated user sessions, such as timeouts and Mobile VPN with IPSec address assignments. Because the data comes from LDAP attributes associated with individual user objects, you are not limited to the global settings in Fireware XTM Web UI. You can set these parameters for each individual user.

For more information, see *Use Active Directory or LDAP Optional Settings* on page 280.

Configure Active Directory Authentication

Active Directory is the Microsoft® Windows-based application of an LDAP directory structure. Active Directory lets you expand the concept of domain hierarchy used in DNS to an organizational level. It keeps information and settings for an organization in a central, easy-to-access database.You can use an Active Directory authentication server to enable your users to authenticate to the XTM device with their current network credentials. You must configure both your XTM device and the Active Directory server for Active Directory authentication to work correctly.

When you configure Active Directory authentication, you can specify one or more Active Directory domains that your users can select when they authenticate. For each domain, you can add up to two Active Directory servers: one primary server and one backup server. If the first server you add fails, the second server is used to complete authentication requests. When you add an Active Directory server, you can select whether to specify the IP address or the DNS name of each server.

If you configure more than one Active Directory domain and you use Single Sign-On (SSO), to enable your users to select from the available Active Directory domains and authenticate, your users must install the SSO client. For more information, see *About Single Sign-On (SSO)* on page 242 and *Install the WatchGuard Single Sign-On (SSO) Client* on page 245.

If your users authenticate with the Active Directory authentication method, their distinguished names (DN) and passwords are not encrypted. To use Active Directory authentication and encrypt user credentials, you can select the LDAPS (LDAP over SSL) option. When you use LDAPS, the traffic between the LDAPS client on your XTM device and your Active Directory server is secured by an SSL tunnel. When you enable this option, you can also choose whether to enable the LDAPS client to validate the Active Directory server certificate. If you choose to use LDAPS and you specify the DNS name of your server, make sure the search base you specify includes the DNS name of your server.

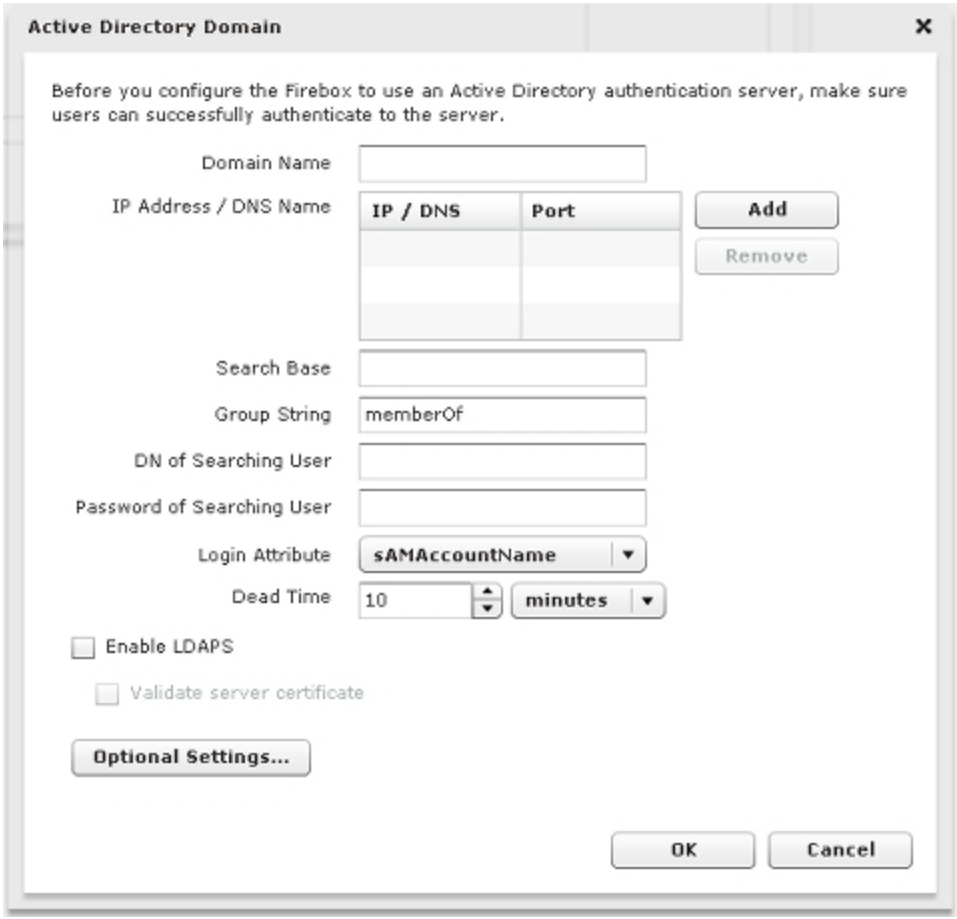
The Active Directory server can be located on any XTM device interface. You can also configure your XTM device to use an Active Directory server available through a VPN tunnel. For more information, see Authentication to an Active Directory Server Through a BOVPN Tunnel.

Before you begin, make sure your users can successfully authenticate to your Active Directory server. You can then use Fireware XTM Web UI to configure your XTM device. You can add, edit, or delete the Active Directory domains and servers defined in your configuration.

Add an Active Directory Authentication Domain and Server

1. Select **Authentication > Servers**.
   The Authentication Servers page appears.
2. Select the **Active Directory** tab.
   The Active Directory settings appear.

3. Click **Add**.
   The Active Directory Domain page appears.

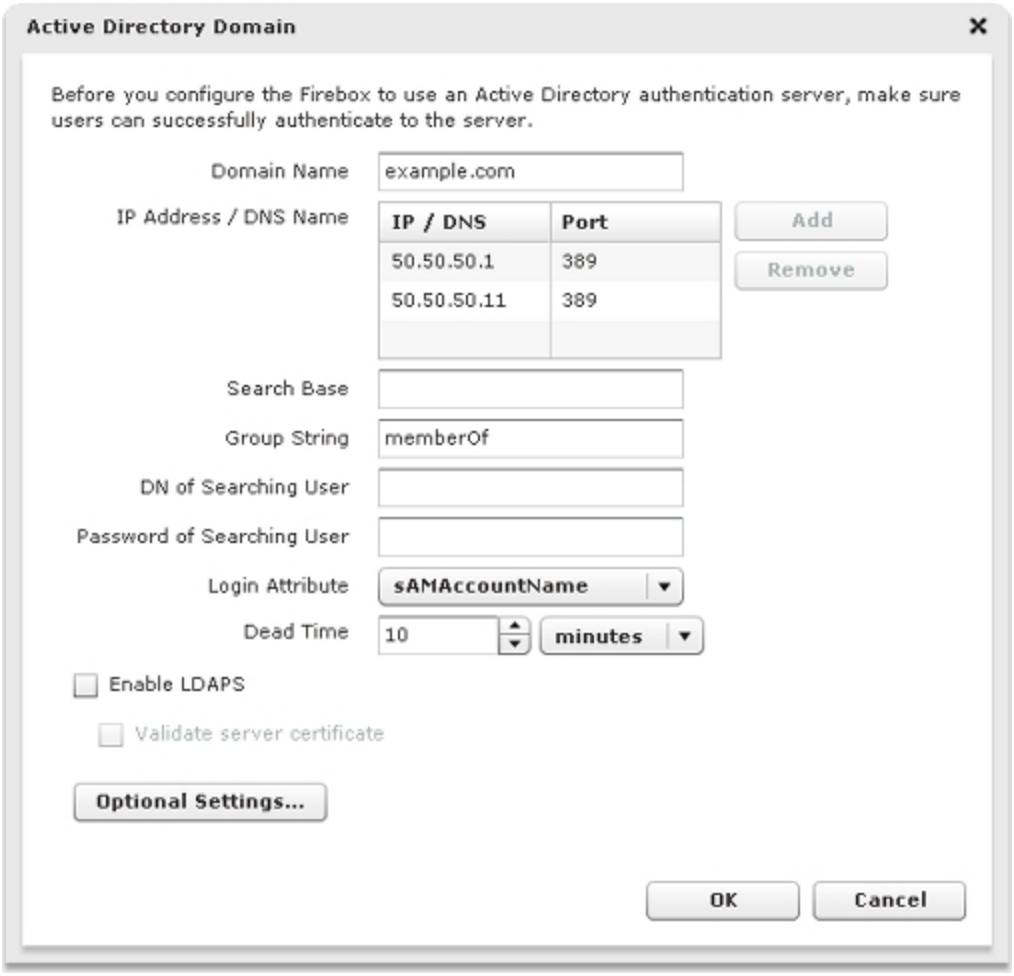


4. In the **Domain Name** text box, type the domain name to use for this Active Directory server.
5. Click **Add**.
   The Add IP/DNS Name page appears.

6. From the **Choose Type** drop-down list, select **IP Address** or **DNS Name**.
7. In the **Host IP** or **Host Name** text box, type the IP address or DNS name of this Active Directory server.
8. In the **Port** text box, type or select the TCP port number for the device to use to connect to the Active Directory server.
   The default port number is 389. If you enable LDAPS, you must select port 636.

   If your Active Directory server is a global catalog server, it can be useful to change the default port.
   For more information, see *Change the Default Port for the Active Directory Server* on page 279.
9. Click **OK**.
   The IP address or DNS name you added appears in the Add Active Directory Domain page.
10. To add another Active Directory server to this domain, repeat Steps 3–9. You can add up to two servers.
    Make sure the shared secret is the same on all the Active Directory servers you specify.

    For more information, see *Use a Backup Authentication Server* on page 253.



11. In the **Search Base** text box, type the location in the directory to begin the search.

    The standard format for the search base setting is: *ou=<name of organizational unit>,dc=<first part of the distinguished server name>,dc=<any part of the distinguished server name that appears after the dot>*.

    To limit the directories on the authentication server where the XTM device can search for an authentication match, you can set a search base. We recommend that you set the search base to the root of the domain. This enables you to find all users and all groups to which those users belong.

    For more information, see *Find Your Active Directory Search Base* on page 278.

12. In the **Group String** text box, type the attribute string that is used to hold user group information on the Active Directory server. If you have not changed your Active Directory schema, the group string is always `memberOf`.
13. In the **DN of Searching User** text box, type the distinguished name (DN) for a search operation.

    If you keep the login attribute of `sAMAccountName`, you do not have to type anything in this text box.

    If you change the login attribute, you must add a value in the **DN of Searching User** text box. You can use any user DN with the privilege to search LDAP/Active Directory, such as *Administrator*. However, a weaker user DN with only the privilege to search is usually sufficient.

14. In the **Password of Searching User** text box, type the password associated with the distinguished name for a search operation.
15. In the **Login Attribute** drop-down list, select an Active Directory login attribute to use for authentication.

    The login attribute is the name used for the bind to the Active Directory database. The default login attribute is *sAMAccountName*. If you use *sAMAccountName*, you do not have to specify a value for the **DN of Searching User** and **Password of Searching User** settings.
16. In the **Dead Time** text box, type or select a time after which an inactive server is marked as active again.
17. From the **Dead Time** drop-down list, select **minutes** or **hours** to set the duration.

    After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts do not try this server until it is marked as active again.
18. To enable secure SSL connections to your Active Directory server, select the **Enable LDAPS** check box.
19. To verify the certificate of the Active Directory server is valid, select the **Validate server certificate** check box.
20. To specify optional attributes for the primary LDAP server, click **Optional Settings**.

    For more information about how to configure optional settings, see the subsequent section.
21. To add another Active Directory domain, repeat Steps 3–20. Make sure the shared secret is the same on all the Active Directory domains you specify.
22. Click **Save**.

About Active Directory Optional Settings

Fireware XTM can get additional information from the directory server (LDAP or Active Directory) when it reads the list of attributes in the server's search response. This lets you use the directory server to assign extra parameters to the authenticated user sessions, such as timeouts and Mobile VPN with IPSec address assignments. Because the data comes from LDAP attributes associated with individual user objects, you are not limited to the global settings in Fireware XTM Web UI. You can set these parameters for each individual user.

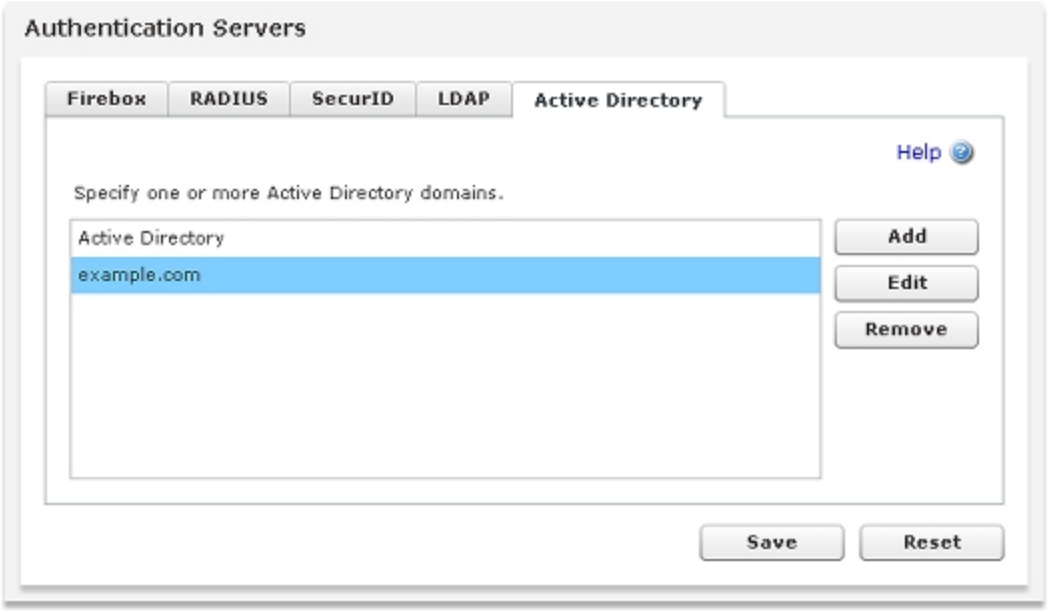
For more information, see *Use Active Directory or LDAP Optional Settings* on page 280.

Edit an Existing Active Directory Domain

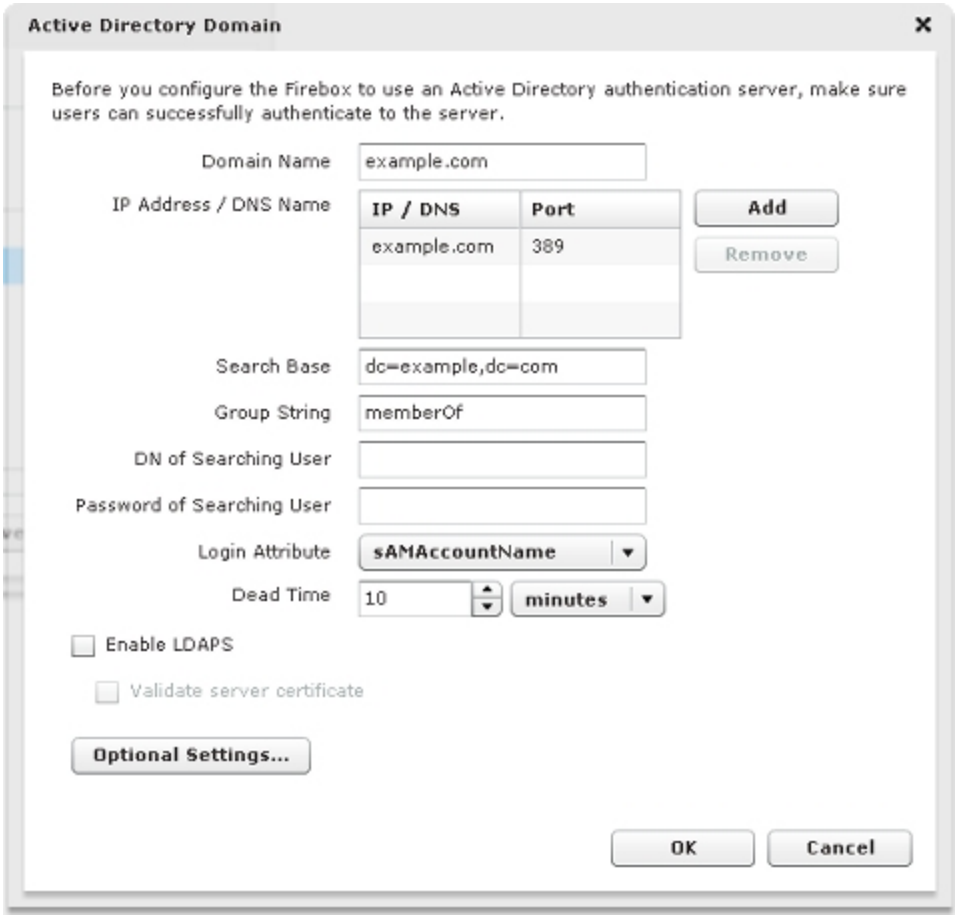
When you edit an Active Directory domain, you cannot change the details of the Active Directory servers configured in the domain. Instead, you must add a new server. If there are two servers in the list, you must remove one of the servers before you can add a new one.

From the Authentication Servers page:

1. In the **Active Directory domains** list, select the server to change.



2. Click **Edit**.
   The Edit Active Directory Domain page appears.



3. To add an IP address or DNS name to the server for this domain, click **Add** and follow the instructions in Steps 5–9 of the previous section.
4. To remove an IP address or DNS name from the server for this domain, select the entry in the **IP Address / DNS Name** list and click **Remove**.
5. Update the settings for your Active Directory server.

Delete an Active Directory Domain

From the **Authentication Servers** page:

1. In the **Active Directory domains** list, select the domain to delete.
2. Click **Remove**.
   The server is removed from the list.

Find Your Active Directory Search Base

When you configure your XTM device to authenticate users with your Active Directory server, you add a *search base*. The search base is the place the search starts in the Active Directory hierarchical structure for user account entries. This can help to make the authentication procedure faster.

Before you begin, you must have an operational Active Directory server that contains account information for all users for whom you want to configure authentication on the XTM device.

From your Active Directory server:

1. Select **Start > Administrative Tools > Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** tree, find and select your domain name.
3. Expand the tree to find the path through your Active Directory hierarchy.

   Domain name components have the format *dc=domain name component*, are appended to the end of the search base string, and are also comma-delimited.

   For each level in your domain name, you must include a separate domain name component in your Active Directory search base. For example, if your domain name is *prefix.example.com*, the domain name component in your search base is `DC=prefix,DC=example,DC=com`.

To make sure that the Active Directory search can find any user object in your domain, specify the root of the domain. For example, if your domain name is kunstlerandsons.com, and you want the Active Directory search to find any user object in the entire domain, the search base string to add is:

```
dc=kunstlerandsons,dc=com.
```

If you want to limit the search to begin in some container beneath the root of the domain, specify the fully-qualified name of the container in comma-delimited form, starting with the name of the base container and progressing toward the root of the domain. For example, assume your domain in the tree looks like this after you expand it:

Also assume that you want the Active Directory search to begin in the **Sales** container that appears in the example. This enables the search to find any user object inside the **Sales** container, and inside any containers within the **Sales** container.

The search base string to add in the XTM device configuration is:

```
ou=sales,ou=accounts,dc=kunstlerandsons,dc=com
```

The search string is not case-sensitive. When you type your search string, you can use either uppercase or lowercase letters.

This search does not find user objects inside the **Development** or **Admins** containers, or inside the **Builtin**, **Computers**, **Domain Controllers**, **ForeignSecurityPrincipals**, or **Users** containers.

DN of Searching User and Password of Searching User Fields

You must complete these fields only if you select an option for the **Login Attribute** that is different from the default value, *sAMAccountName*. Most organizations that use Active Directory do not change this. When you leave this field at the default *sAMAccountName* value, users supply their usual Active Directory login names for their user names when they authenticate. This is the name you see in the **User logon name** text box on the **Account** tab when you edit the user account in **Active Directory Users and Computers**.

If you use a different value for the **Login Attribute**, a user who tries to authenticate gives a different form of the user name. In this case, you must add *Searching User credentials* to your XTM device configuration.

Change the Default Port for the Active Directory Server

If your WatchGuard device is configured to authenticate users with an Active Directory (AD) authentication server, it connects to the Active Directory server on the standard LDAP port by default, which is TCP port 389. If the Active Directory servers that you add to your WatchGuard device configuration are set up to be Active Directory global catalog servers, you can tell the WatchGuard device to use the global catalog port—TCP port 3268—to connect to the Active Directory server.

A *global catalog server* is a domain controller that stores information about all objects in the forest. This enables the applications to search Active Directory, but not have to refer to specific domain controllers that store the requested data. If you have only one domain, Microsoft recommends that you configure all domain controllers as global catalog servers.

If the primary or secondary Active Directory server you use in your WatchGuard device configuration is also configured as a global catalog server, you can change the port the WatchGuard device uses to connect to the Active Directory server to increase the speed of authentication requests. However, we do not recommend that you create additional Active Directory global catalog servers just to speed up authentication requests. The replication that occurs among multiple global catalog servers can use significant bandwidth on your network.

Configure the XTM Device to Use the Global Catalog Port

1. From Fireware XTM Web UI, select **Authentication > Servers**.
   The Authentication Servers page appears.
2. Select the **Active Directory** tab.
3. In the **Port** text box, clear the contents and type **3268**.
4. Click **Save**.

Find Out if Your Active Directory Server is Configured as a Global Catalog Server

1. Select **Start > Administrative Tools > Active Directory Sites and Services**.
2. Expand the **Sites** tree and find the name of your Active Directory server.
3. Right-click **NTDS Settings** for your Active Directory server and select **Properties**.

   If the **Global Catalog** check box is selected, the Active Directory server is configured to be a global catalog.

Use Active Directory or LDAP Optional Settings

When Fireware XTM contacts the directory server (Active Directory or LDAP) to search for information, it can get additional information from the list of attributes in the search response returned by the server. This lets you use the directory server to assign extra parameters to the authenticated user session, such as timeouts and Mobile VPN address assignments. Because the data comes from LDAP attributes associated with individual user objects, you can set these parameters for each individual user and you are not limited to the global settings in Fireware XTM Web UI.

Before You Begin

To use these optional settings you must:

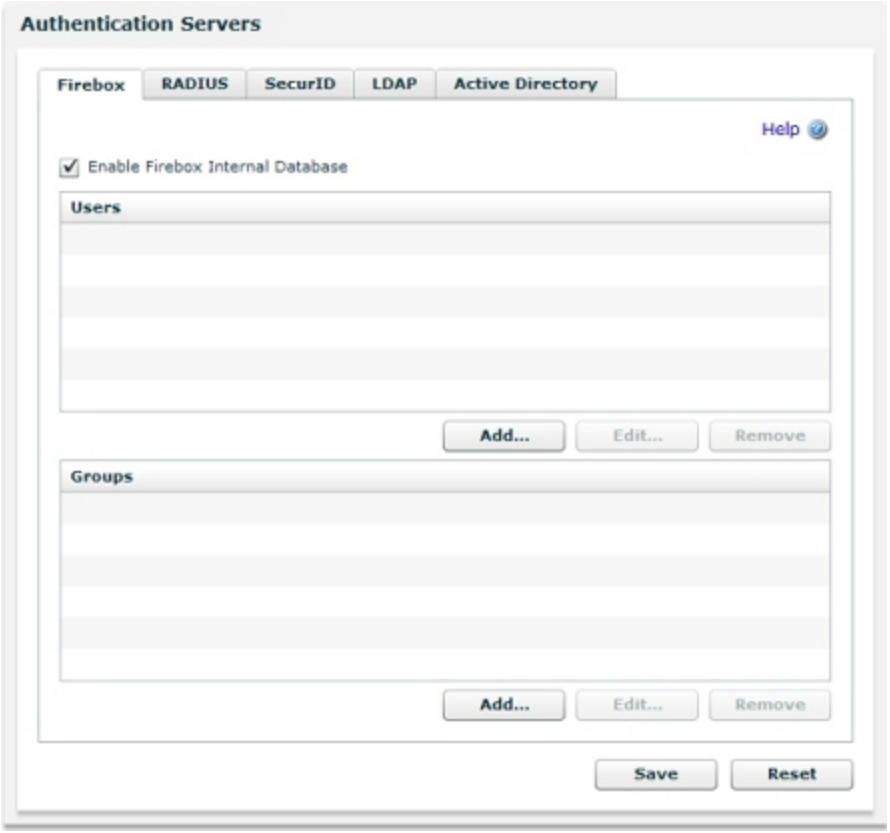
- Extend the directory schema to add new attributes for these items.
- Make the new attributes available to the object class that user accounts belong to.
- Give values to the attributes for the user objects that should use them.

Make sure you carefully plan and test your directory schema before you extend it to your directories. Additions to the Active Directory schema, for example, are generally permanent and cannot be undone. Use the Microsoft® web site to get resources to plan, test, and implement changes to an Active Directory schema. Consult the documentation from your LDAP vendor before you extend the schema for other directories.

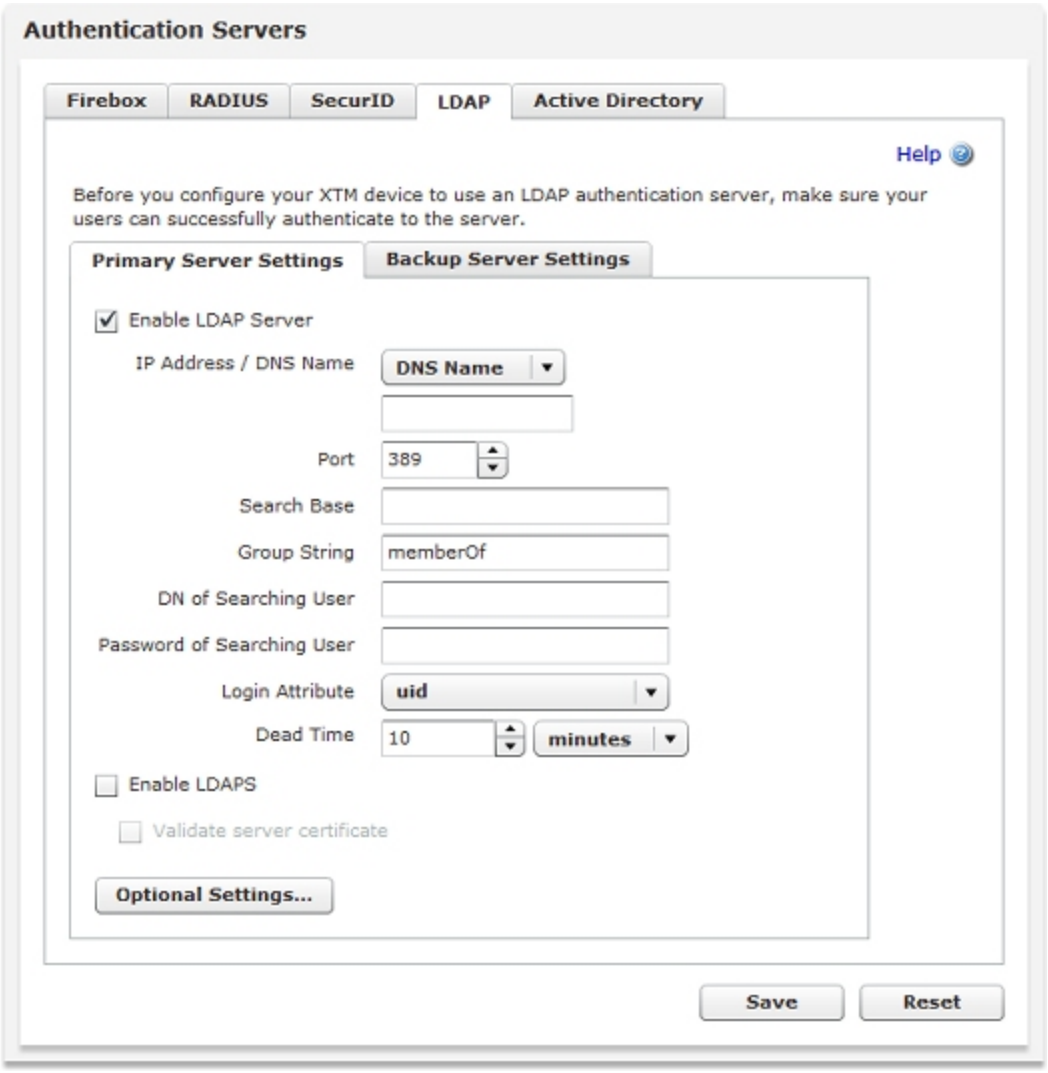
Specify Active Directory or LDAP Optional Settings

You can use Fireware XTM Web UI to specify the additional attributes Fireware XTM looks for in the search response from the directory server.

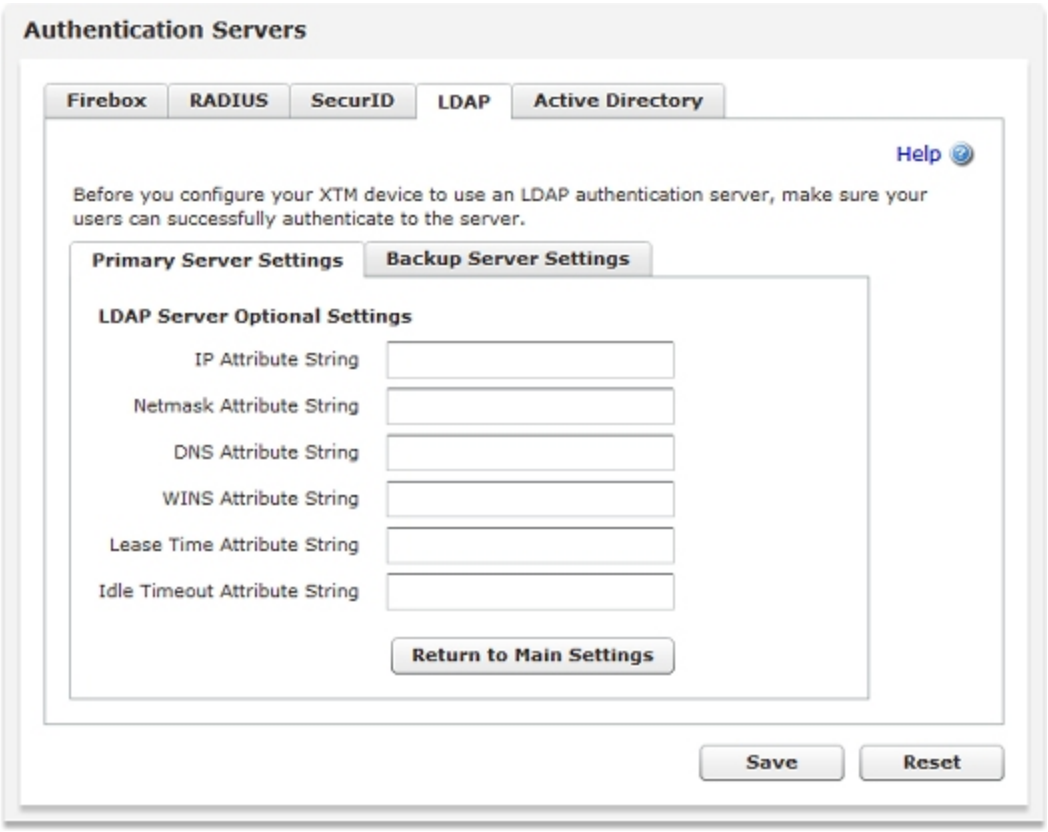
1. Select **Authentication > Servers**.
   The Authentication Servers page appears.



2. Click the **LDAP** tab or the **Active Directory** tab and make sure the server is enabled.



3. Click **Optional Settings**.
   The Server Optional Settings page appears.



4. Type the attributes you want to include in the directory search in the string fields.

   IP Attribute String

   This field applies only to Mobile VPN clients.

   Type the name of the attribute for Fireware XTM to use to assign a virtual IP address to the Mobile VPN client. This must be a single-valued attribute and an IP address in decimal format. The IP address must be within the pool of virtual IP addresses you specify when you create the Mobile VPN Group.

   If the XTM device does not see the IP attribute in the search response or if you do not specify an attribute in Fireware XTM Web UI, it assigns the Mobile VPN client a virtual IP address from the virtual IP address pool you create when you make the Mobile VPN Group.

   Netmask Attribute String

   This field applies only to Mobile VPN clients.

   Type the name of the attribute for Fireware XTM to use to assign a subnet mask to the Mobile VPN client's virtual IP address. This must be a single-valued attribute and a subnet mask in decimal format.

   The Mobile VPN software automatically assigns a netmask if the XTM device does not see the netmask attribute in the search response or if you do not specify one in Fireware XTM Web UI.

   DNS Attribute String

   This field applies only to Mobile VPN clients.

Type the name of the attribute Fireware XTM uses to assign the Mobile VPN client one or more DNS addresses for the duration of the Mobile VPN session. This can be a multi-valued attribute and must be a normal dotted-decimal IP address. If the XTM device does not see the DNS attribute in the search response, or if you do not specify an attribute in Fireware XTM Web UI, it uses the WINS addresses you enter when you *Configure WINS and DNS Servers*.

WINS Attribute String

This field applies only to Mobile VPN clients.

Type the name of the attribute Fireware XTM should use to assign the Mobile VPN client one or more WINS addresses for the duration of the Mobile VPN session. This can be a multi-valued attribute and must be a normal dotted-decimal IP address. If the XTM device does not see the WINS attribute in the search response or if you do not specify an attribute in Fireware XTM Web UI, it uses the WINS addresses you enter when you *Configure WINS and DNS Servers*.

Lease Time Attribute String

This applies to Mobile VPN clients and to clients that use Firewall Authentication.

Type the name of the attribute for Fireware XTM to use to control the maximum duration a user can stay authenticated (session timeout). After this amount of time, the user is removed from the list of authenticated users. This must be a single-valued attribute. Fireware XTM interprets the attribute's value as a decimal number of seconds. It interprets a zero value as *never time out*.

Idle Timeout Attribute String

This applies to Mobile VPN clients and to clients that use Firewall Authentication.

Type the name of the attribute Fireware XTM uses to control the amount of time a user can stay authenticated when no traffic is passed to the XTM device from the user (idle timeout). If no traffic passes to the device for this amount of time, the user is removed from the list of authenticated users. This must be a single-valued attribute. Fireware XTM interprets the attribute's value as a decimal number of seconds. It interprets a zero value as *never time out*.

5. Click **Save**.
   The attribute settings are saved.

Use a Local User Account for Authentication

Any user can authenticate as a Firewall user, PPTP user, or Mobile VPN user, and open a PPTP or Mobile VPN tunnel if PPTP or Mobile VPN is enabled on the XTM device. However, after authentication or a tunnel has been successfully established, users can send traffic through the VPN tunnel only if the traffic is allowed by a policy on the XTM device. For example, a Mobile VPN-only user can send traffic through a Mobile VPN tunnel. Even though the Mobile VPN-only user can authenticate and open a PPTP tunnel, he or she cannot send traffic through that PPTP tunnel.

If you use Active Directory authentication and the group membership for a user does not match your Mobile VPN policy, you can see an error message that says *Decrypted traffic does not match any policy*. If you see this error message, make sure that the user is in a group with the same name as your Mobile VPN group.

Use Authorized Users and Groups in Policies

You can use specified user and group names when you create policies in Fireware XTM Web UI. For example, you can define all policies to only allow connections for authenticated users. Or, you can limit connections on a policy to particular users.

The term *authorized users and groups* refers to users and groups that are allowed to access network resources.

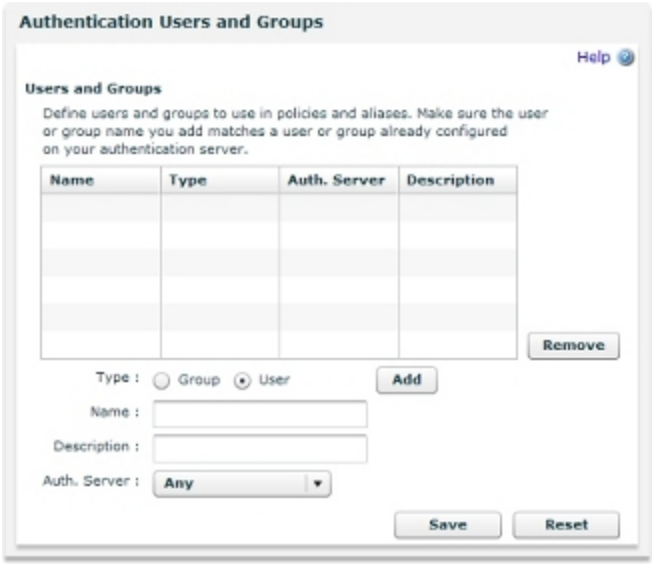
Define Users and Groups for Firebox Authentication

If you use your XTM device as an authentication server and want to define users and groups that authenticate to the XTM device, see *Define a New User for Firebox Authentication* on page 256 and *Define a New Group for Firebox Authentication* on page 258.

Define Users and Groups for Third-Party Authentication

You can use Fireware XTM Web UI to define the users and groups to use for third-party authentication. When you create a group, if you use more than one Active Directory domain for authentication, you must specify the domain that you want users in the group to use to authenticate.

1. Create a group on your third-party authentication server that contains all the user accounts on your system.
2. Select **Authentication > Users and Groups**.
   The Authentication Users and Groups page appears.



3. Type a user or group name you created on the authentication server.
4. (Optional) Type a description for the user or group.
5. Select **Group** or **User**.
6. From the **Auth Server** drop-down list, select your authentication server type.

Available options include **Any**, **Firebox-DB**, **RADIUS** , **SecurID**, **LDAP**, or **Active Directory**. For authentication through a RADIUS or VACMAN Middleware server, select **RADIUS**. For Active Directory authentication, select the specific domain to use for this user or group.

7. Click **Add**.
8. Click **Save**.

Add Users and Groups to Policy Definitions

Any user or group that you want to use in your policy definitions must be added as an authorized user. All users and groups you create for Firebox authentication, and all Mobile VPN users, are automatically added to the list of authorized users and groups on the **Authorized Users and Groups** dialog box. You can add any users or groups from third-party authentication servers to the authorized user and group list with the previous procedure. You are then ready to add users and groups to your policy configuration.

1. From Fireware XTM Web UI, select **Firewall > Firewall Policies**.
   The Firewall Policies page appears.
2. Select a policy from the list and click **Edit**.
   Or, double-click a policy.
   The Policy Configuration page appears.
3. On the **Policy** tab, below the **From** box, click **Add**.
   The Add Address dialog box appears.
4. Click **Add User**.
   The Add Authorized Users or Groups dialog box appears.
5. From the left **Type** drop-down list, select whether the user or group is authorized as a Firewall, PPTP, or SSL VPN user.

   For more information on these authentication types, see *Types of Firebox Authentication* on page 254.
6. From the right **Type** drop-down list, select either **User** or **Group**.
7. If your user or group appears in the **Groups** list, select the user or group and click **Select**.
   The Add Address dialog box reappears with the user or group in the Selected Members or Addresses box.

   Click **OK** to close the **Edit Policy Properties** dialog box.
8. If your user or group does not appear in the **Groups** list, see *Define a New User for Firebox Authentication* on page 256, *Define a New Group for Firebox Authentication* on page 258, or the previous *Define users and groups for third-party authentication* procedure, and add the user or group.

After you add a user or group to a policy configuration, Fireware XTM Web UI automatically adds a WatchGuard Authentication policy to your XTM device configuration. Use this policy to control access to the authentication portal web page.

For instructions to edit this policy, see *Use Authentication to Restrict Incoming Traffic* on page 236.

12 Policies

About Policies

The *security policy* of your organization is a set of definitions to protect your computer network and the information that goes through it. The XTM device denies all packets that are not specifically allowed. When you add a *policy* to your XTM device configuration file, you add a set of rules that tell the XTM device to allow or deny traffic based upon factors such as source and destination of the packet or the TCP/IP port or protocol used for the packet.

As an example of how a policy could be used, suppose the network administrator of a company wants to log in remotely to a web server protected by the XTM device. The network administrator manages the web server with a Remote Desktop connection. At the same time, the network administrator wants to make sure that no other network users can use Remote Desktop. To create this setup, the network administrator adds a policy that allows RDP connections only from the IP address of the network administrator's desktop computer to the IP address of the web server.

A policy can also give the XTM device more instructions on how to handle the packet. For example, you can define logging and notification settings that apply to the traffic, or use NAT (Network Address Translation) to change the source IP address and port of network traffic.

Packet Filter and Proxy Policies

Your XTM device uses two categories of policies to filter network traffic: *packet filters* and *proxies*. A packet filter examines each packet's IP and TCP/UDP header. If the packet header information is legitimate, then the XTM device allows the packet. Otherwise, the XTM device drops the packet.

A proxy examines both the header information and the content of each packet to make sure that connections are secure. This is also called *deep packet inspection*. If the packet header information is legitimate and the content of the packet is not considered a threat, then the XTM device allows the packet. Otherwise, the XTM device drops the packet.

Add Policies to Your XTM device

The XTM device includes many pre-configured packet filters and proxies that you can add to your configuration. For example, if you want a packet filter for all Telnet traffic, you add a pre-defined Telnet policy that you can modify for your network configuration. You can also make a custom policy for which you set the ports, protocols, and other parameters.

When you configure the XTM device with the Quick Setup Wizard, the wizard adds several packet filters: Outgoing (TCP-UDP), FTP, ping, and up to two WatchGuard management policies. If you have more software applications and network traffic for the XTM device to examine, you must:

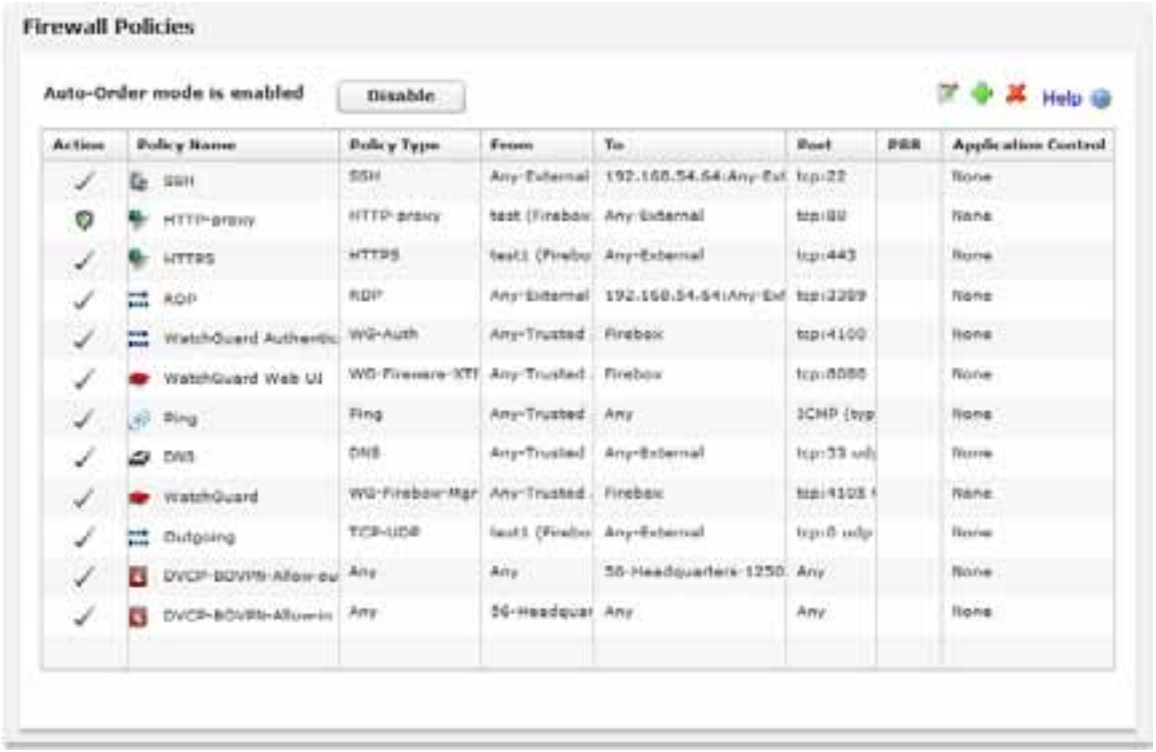
- Configure the policies on your XTM device to let the necessary traffic through
- Set the approved hosts and properties for each policy
- Balance the requirement to protect your network against the requirements of your users to get access to external resources

We recommend that you set limits on outgoing access when you configure your XTM device.

> ***Note*** *In all documentation, we refer to both packet filters and proxies as policies. Information on policies refers to both packet filters and proxies unless otherwise specified.*

About the Policies Pages

The policies included in your current XTM device configuration appear on the **Firewall Policies** and **Mobile VPN Policies** pages. From these pages you can see configuration information, such as source and destination addresses, assigned ports, policy-based routing, and application control settings, as well as whether notification, scheduling, and QoS/Traffic Management are configured. You can also add, edit, and delete policies on these pages.



By default, Fireware XTM Web UI sorts policies from the most specific to the most general. The order determines how traffic flows through the policies.

To set the policy order manually, adjacent to **Auto-Order mode is enabled**, click **Disable**.

For more information on policy order, see *About Policy Precedence*.

For more information about how to add policies, see *Add Policies to Your Configuration* on page 291.

This information appears for each policy:

Action

The action taken by the policy for traffic that matches the policy definition. The symbols in this column also indicate whether the policy is a packet filter policy or a proxy policy, and the settings that are configured for the policy:

- — Packet filter policy; traffic is allowed
- — Packet filter policy; traffic is denied
- — Disabled packet filter policy

-  — Proxy policy; traffic is allowed
-  — Proxy policy; traffic is denied
-  — Disabled proxy policy
-  — Application Control is configured
-  —Traffic Management/ QoS is configured
-  — Scheduling is configured
-  — Logging is enabled
-  — Notification is enabled

Policy Name

Name of the policy, as defined in the **Name** text box on the **Policy Configuration** page.

Policy Type

The protocol that the policy manages. Packet filters include the protocol name only. Proxies include the protocol name and *-proxy*. ALGs include the protocol name and *-ALG*.

From

The source addresses for this policy.

To

The destination addresses for this policy.

Port

Protocols and ports used by the policy.

PBR

The interface numbers that are used for failover in the policy-based routing settings for the policy.

Application Control

The Application Control action enabled for the policy.

For more information, see *Enable Application Control in a Policy*.

Add Policies to Your Configuration

To add a firewall or Mobile VPN policy:

1. Select **Firewall > Firewall Policies** or **Firewall > Mobile VPN Policies**.
   The Policies page you selected appears.
2. Click  .
3. Expand the list of packet filters or policies to find a protocol or port.
4. For a packet filter, select a policy type.
   For a proxy, select a policy type and from the **Proxy action** drop-down list, select the **Client** or **Server** option.
   For a Mobile VPN policy, first select a Mobile VPN group, then select the policy type.
5. Click **Add policy**

The XTM device includes a default definition for each policy included in the XTM device configuration file. The default definition consists of settings that are appropriate for most installations. However, you can modify them for your particular business purposes, or if you want to include special policy properties such as Traffic Management actions and operating schedules.

After you add a policy to your configuration, you define rules to:

- Set allowed traffic sources and destinations
- Make filter rules
- Enable or disable the policy
- Configure properties such as Traffic Management, NAT, and logging

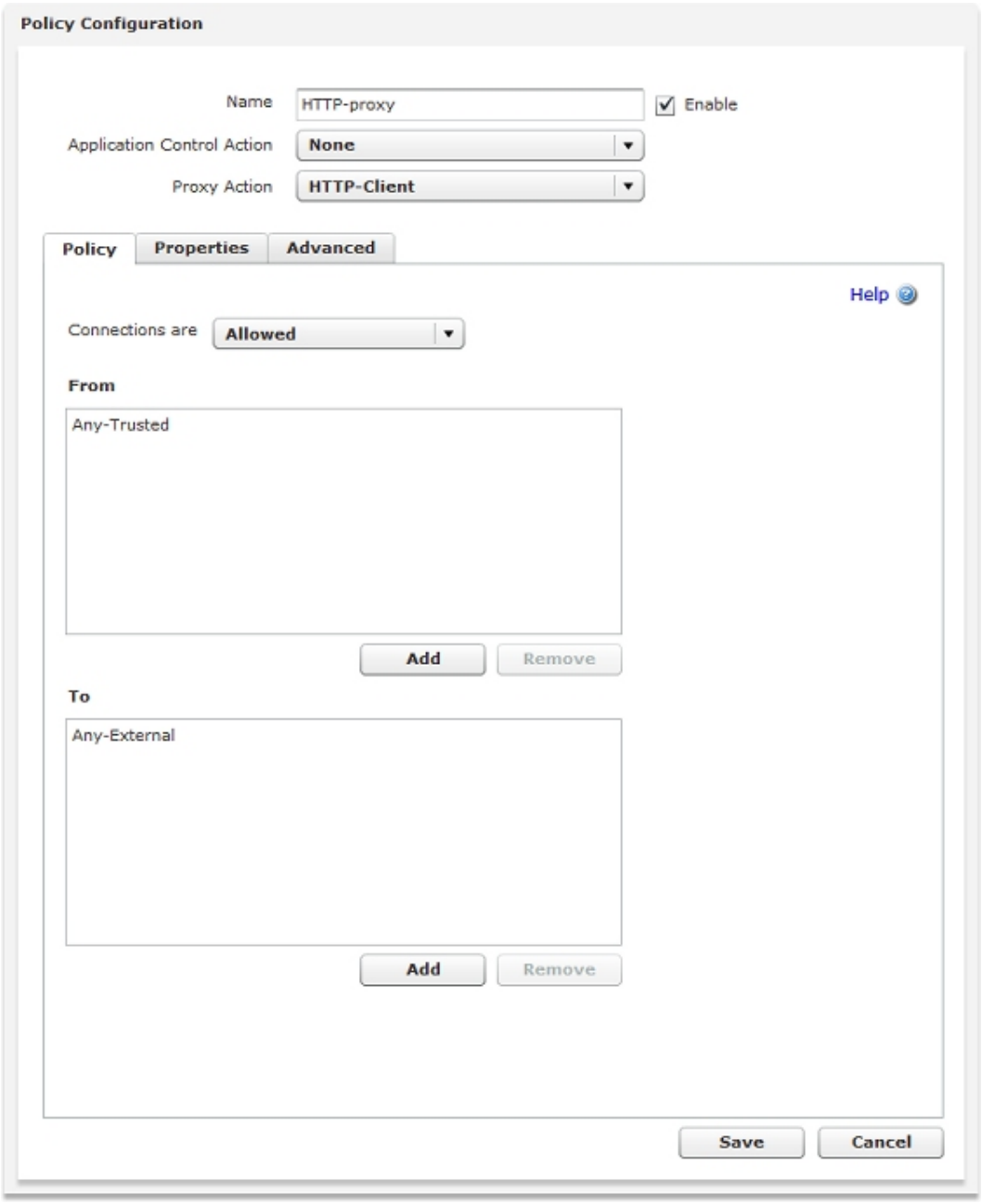
For more information on policy configuration, see *About Policy Properties* on page 306.

Add a Policy from the List of Templates

Your XTM device includes a default definition for each policy included in the XTM device configuration. The default definition settings are appropriate for most installations, however, you can modify them to include special policy properties, such as QoS actions and operating schedules.

On the **Add Policy** page:

1. Expand the **Packet Filters**, **Proxies**, or **Custom** folder.
   A list of templates for packet filter or proxy policies appears.
2. Select a policy and click **Add Policy**.
   The Policy Configuration page appears, with the Policy tab selected.



3. To change the name of the policy, in the **Name** text box, type a new name.
4. Configure the access rules and other settings for the policy.
5. Click **Save**.

For more information on policy properties, see *About Policy Properties* on page 306.

For more information about how to configure proxy actions, see *About Proxy Actions*.

For more information about how to configure application control actions, see *Configure Application Control Actions*.

When you configure the access rules for your policy, you can choose to use an alias. For more information about aliases, see *About Aliases* on page 294 and *Create an Alias* on page 295.

Disable or Delete a Policy

As your network security requirements change, you can disable or delete the policies in your configuration.

To disable a policy:

1. Select **Firewall > Firewall Policies** or **Firewall > Mobile VPN Policies**.
   The Policy Configuration page appears.
2. Select the policy and click  .
3. Clear the **Enable** check box.
4. Click **Save**.

Delete a Policy

To delete a policy:

1. Select **Firewall > Firewall Policies** or **Firewall > Mobile VPN Policies**.
2. Select the policy and click  .
   A confirmation message appears.
3. Click **Yes**.
   Your configuration changes are saved automatically.

About Aliases

An alias is a shortcut that identifies a group of hosts, networks, or interfaces. When you use an alias, it is easy to create a security policy because the XTM device allows you to use aliases when you create policies.

Default aliases in Fireware XTM Web UI include:

- **Any** — Any source or destination aliases that correspond to XTM device interfaces, such as *Trusted* or *External*.
- **Firebox** — An alias for all XTM device interfaces.
- **Any-Trusted** — An alias for all XTM device interfaces configured as *Trusted* interfaces, and any network you can get access to through these interfaces.
- **Any-External** — An alias for all XTM device interfaces configured as *External*, and any network you can get access to through these interfaces.
- **Any-Optional** — Aliases for all XTM device interfaces configured as *Optional*, and any network you can get access to through these interfaces.
- **Any-BOVPN** — An alias for any BOVPN (IPSec) tunnel.
  When you use the BOVPN Policy wizard to create a policy to allow traffic through a BOVPN tunnel, the wizard automatically creates *.in* and *.out* aliases for the incoming and outgoing tunnels.

Alias names are different from user or group names used in user authentication. With user authentication, you can monitor a connection with a name and not as an IP address. The person authenticates with a user name and a password to get access to Internet protocols.

For more information about user authentication, see *About User Authentication* on page 233.

Alias Members

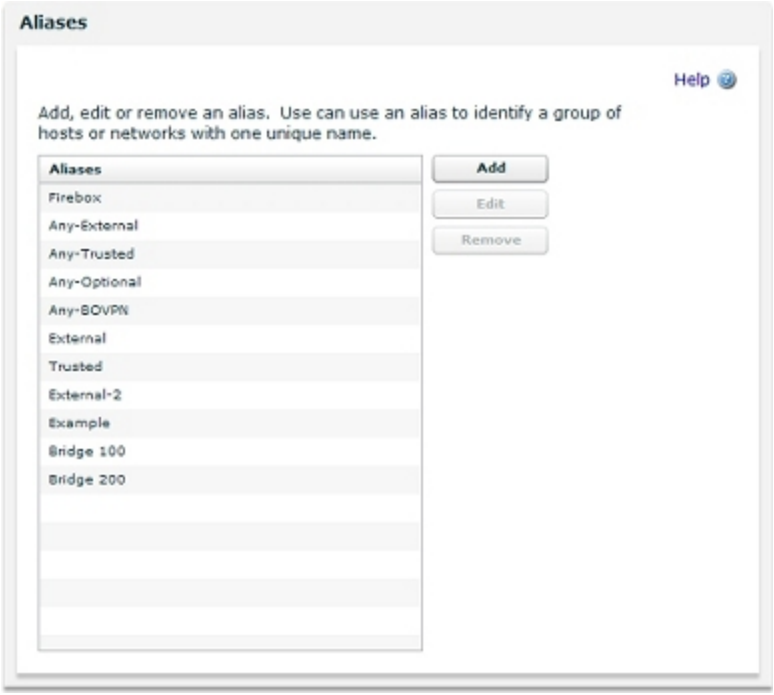
You can add these objects to an alias:

- Host IP
- Network IP
- A range of host IP addresses
- DNS name for a host
- Tunnel address — defined by a user or group, address, and name of the tunnel
- Custom address — defined by a user or group, address, and XTM device interface
- Another alias
- An authorized user or group

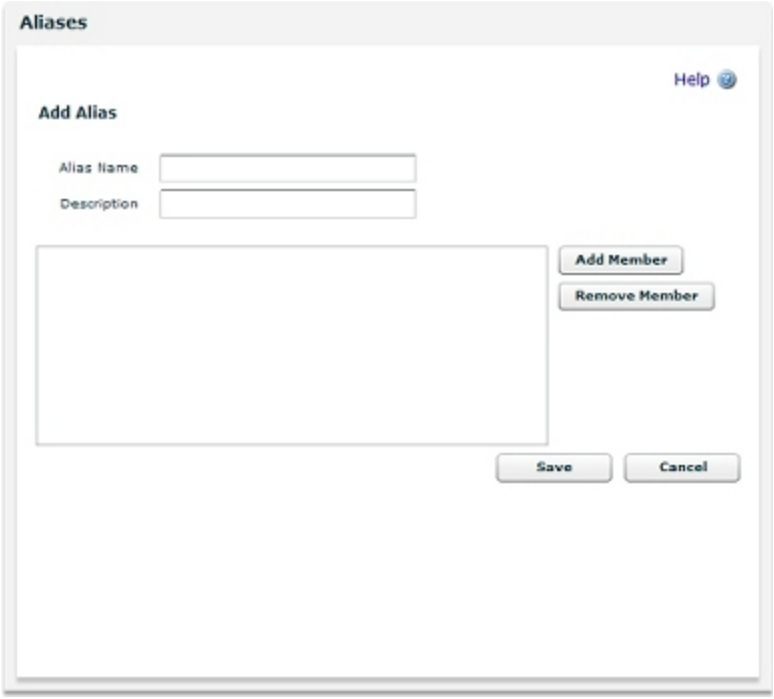
Create an Alias

To create an alias to use with your security policies:

1. Select **Firewall > Aliases**.
   The Aliases page appears.



2. Click **Add**.
   The Add Alias page appears.



3. In the **Alias Name** text box, type a unique name to identify the alias.
   This name appears in lists when you configure a security policy.
4. In the **Description** text box, type a description of the alias.
5. Click **Save**.

Add an Address, Address Range, DNS Name, User, Group, or Another Alias to the Alias

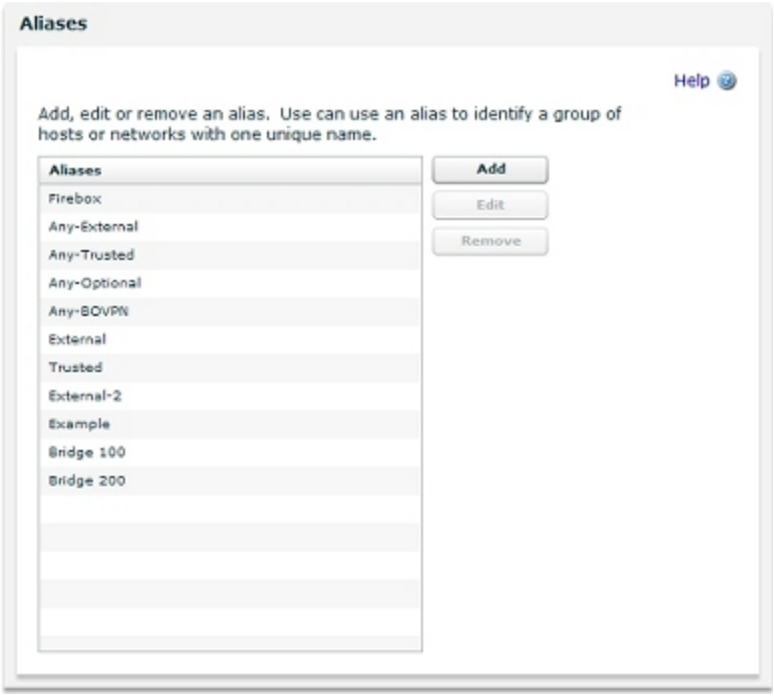
1. In the **Add Alias** dialog box, click **Add Member**.
   The Add Member dialog box appears.
2. From the **Member type** drop-down list, select the type of member you want to add.
3. Type the address or name in the adjacent text box, or select the user or group.
4. Click **OK**.
   The new member appears in the Alias Members section of the Add Alias page.
5. To add more members, repeat Steps 1–4.
6. Click **Save**.

Edit an Alias

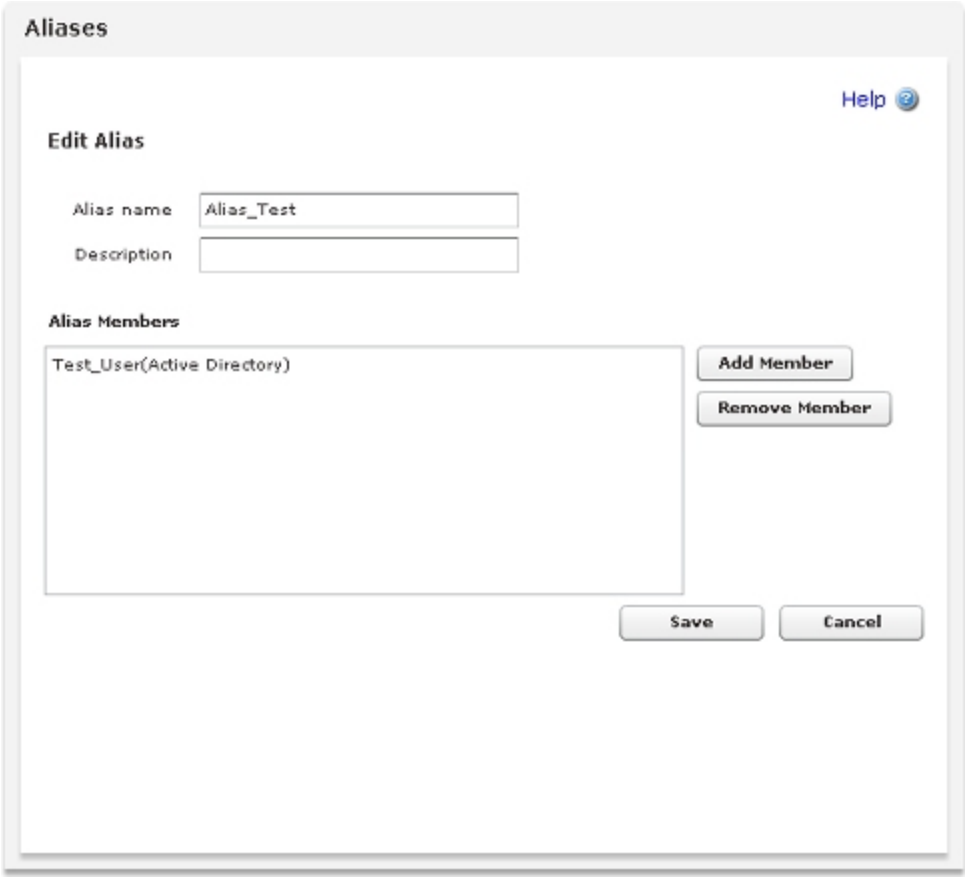
You can edit user-defined aliases from the **Aliases** page.

To edit an alias from the **Aliases** page:

1. Select **Firewall > Aliases**.
   The Aliases page appears.



2. From the **Aliases** list, select the user-defined alias to change.
3. Click **Edit**.
   The Edit Alias page appears.



4. To add a member to the **Alias Members** list, click **Add Member**.
   For more information, see the previous sections.

   To remove a member from the **Alias Members** list, select the entry and click **Remove Member**

5. Click **Save**.

About Policy Precedence

Precedence is the sequence in which the XTM device examines network traffic and applies a policy rule. The XTM device automatically sorts policies from the most detailed to the most general. It compares the information in the packet to the list of rules in the first policy. The first rule in the list to match the conditions of the packet is applied to the packet. If the detail level in two policies is equal, a proxy policy always takes precedence over a packet filter policy.

Automatic Policy Order

The XTM device automatically gives the highest precedence to the most specific policies and the lowest to the least specific. The XTM device examines specificity of the subsequent criteria in the following order. If it cannot determine the precedence from the first criterion, it moves to the second, and so on.

1. Policy specificity
2. Protocols set for the policy type
3. Traffic rules of the **To** list
4. Traffic rules of the **From** list
5. Firewall action (Allowed, Denied, or Denied (send reset)) applied to the policies
6. Schedules applied to the policies
7. Alphanumeric sequence based on policy type
8. Alphanumeric sequence based on policy name

The subsequent sections include more details about what the XTM device does within these eight steps.

Policy Specificity and Protocols

The XTM device uses these criteria in sequence to compare two policies until it finds that the policies are equal, or that one is more detailed than the other.

1. An Any policy always has the lowest precedence.
2. Check for the number of TCP 0 (any) or UDP 0 (any) protocols. The policy with the smaller number has higher precedence.
3. Check for the number of unique ports for TCP and UDP protocols. The policy with the smaller number has higher precedence.
4. Add up the number of unique TCP and UDP ports. The policy with the smaller number has higher precedence.
5. Score the protocols based on their IP protocol value. The policy with the smaller score has higher precedence.

If the XTM device cannot set the precedence when it compares the policy specificity and protocols, it examines traffic rules.

Traffic Rules

The XTM device uses these criteria in sequence to compare the most general traffic rule of one policy with the most general traffic rule of a second policy. It assigns higher precedence to the policy with the most detailed traffic rule.

1. Host address
2. IP address range (smaller than the subnet being compared to)
3. Subnet
4. IP address range (larger than the subnet being compared to)
5. Authentication user name
6. Authentication group
7. Interface, XTM device
8. Any-External, Any-Trusted, Any-Optional
9. Any

For example, compare these two policies:

(HTTP-1) From: Trusted, user1

(HTTP-2) From: 10.0.0.1, Any-Trusted

Trusted is the most general entry for HTTP-1. *Any-Trusted* is the most general entry for HTTP-2. Because *Trusted* is included in the *Any-Trusted* alias, HTTP-1 is the more detailed traffic rule. This is correct despite the fact that HTTP-2 includes an IP address, because the XTM device compares the most general traffic rule of one policy to the most general traffic rule of the second policy to set precedence.

If the XTM device cannot set the precedence when it compares the traffic rules, it examines the firewall actions.

Firewall Actions

The XTM device compares the firewall actions of two policies to set precedence. Precedence of firewall actions from highest to lowest is:

1. Denied or Denied (send reset)
2. Allowed proxy policy
3. Allowed packet-filter policy

If the XTM device cannot set the precedence when it compares the firewall actions, it examines the schedules.

Schedules

The XTM device compares the schedules of two policies to set precedence. Precedence of schedules from highest to lowest is:

1. Always off
2. Sometimes on
3. Always on

If the XTM device cannot set the precedence when it compares the schedules, it examines the policy types and names.

Policy Types and Names

If the two policies do not match any other precedence criteria, the XTM device sorts the policies in alphanumeric sequence. First, it uses the policy type. Then, it uses the policy name. Because no two policies can be the same type and have the same name, this is the last criteria for precedence.

Set Precedence Manually

You can disable Auto-Order mode to switch to manual-order mode and change the policy precedence for your XTM device or template.

1. Select **Firewall > Firewall Policies**.
   The Firewall Policies page appears.
2. Adjacent to **Auto-Order mode is enabled**, click **Disable**.
   A confirmation message appears.
3. Click **Yes** to confirm that you want to switch to manual-order mode.
4. To change the order of a policy, select it and drag it to the new location.
   Or, select a policy and click **Move Up** or **Move Down** to move it higher or lower in the list.
5. Click **Save**.

Create Schedules for XTM Device Actions

A schedule is a set of times for which a feature is active or disabled. You must use a schedule if you want a policy or WebBlocker action to automatically become active or inactive at the times you specify. You can apply a schedule you create to more than one policy or WebBlocker action if you want those policies or actions to be active at the same times.

For example, an organization wants to restrict certain types of network traffic during normal business hours. The network administrator could create a schedule that is active on weekdays, and set each policy in the configuration to use the same schedule.

To create a schedule:

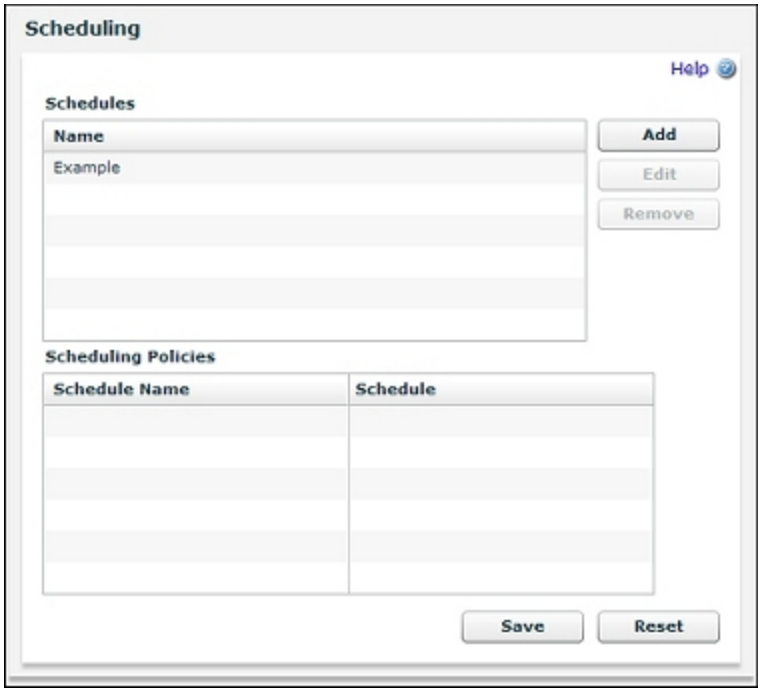
1. Select **Firewall > Scheduling**.
   The Scheduling page appears.
2. To create a new schedule, click **Add**.
   To modify a schedule, select the schedule and click **Edit**.
   The Schedule Settings page appears.
3. For a new schedule, in the **Name** text box, type a descriptive name for the schedule.
   You cannot modify the name of a saved schedule.
4. Select the times for the schedule to operate for each day of the week.
5. Click **Save**.

Set an Operating Schedule

You can set an operating schedule for a policy so that it runs at the times you specify. Schedules can be shared by more than one policy.

To modify a policy schedule:

1. Select **Firewall > Scheduling**.
   The Scheduling page appears.



2. In the **Scheduling Policies** list, select the **Schedule Name** of a policy.
3. In the **Schedule** column, select a schedule in the drop-down list.
4. Click **Save**.

About Custom Policies

If you need to allow for a protocol that is not included by default as a XTM device configuration option, you must define a custom traffic policy. You can add a custom policy that uses:

- TCP ports
- UDP ports
- An IP protocol that is not TCP or UDP, such as GRE, AH, ESP, ICMP, IGMP, and OSPF. You identify an IP protocol that is not TCP or UDP with the IP protocol number.

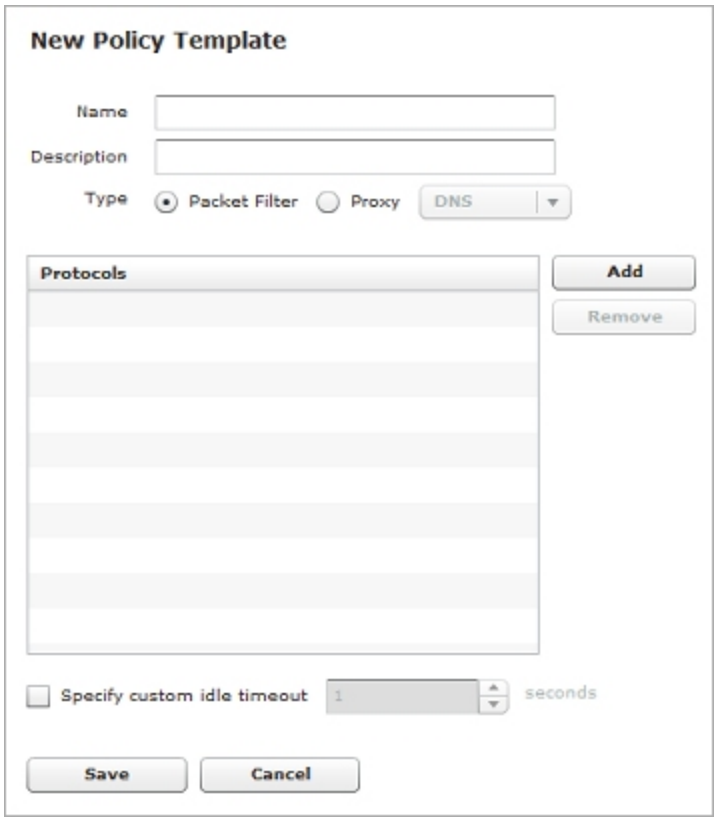
To create a custom policy, you must first create or edit a custom policy template that specifies the ports and protocols used by policies of that type. Then, you create one or more policies from that template to set access rules, logging, QoS, and other settings.

Create or Edit a Custom Policy Template

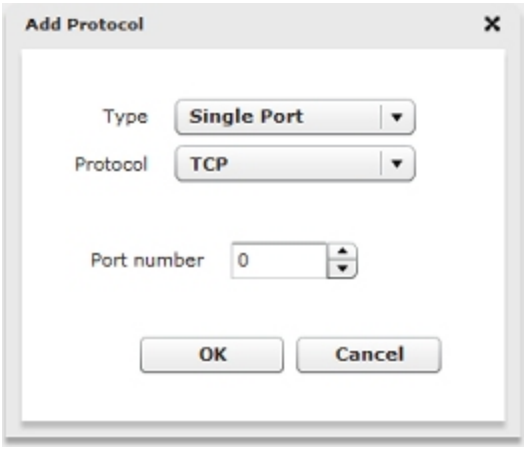
To add specialized policies to your configuration files, you can create custom policy templates. These templates can be packet filter or proxy policies and use any available protocol. When you add a custom policy template to your configuration file, make sure to specify a unique name for the policy. A unique name helps you to find the policy when you want to change or remove it. This name must not be the same as any other policy name in the policies list for your device.

From Fireware XTM Web UI:

1. Select **Firewall > Firewall Policies**.
2. Click .
3. Click **Custom**.
   Or, select an existing custom policy template and click .



4. In the **Name** text box, type the name of the custom policy.
   The name appears in the policies list in the **Policy Name** column.
5. In the **Description** text box, type a description of the policy.
   This appears in the Details section when you click the policy name in the list of User Filters.
6. Select the type of policy: **Packet Filter** or **Proxy**.
7. If you select **Proxy**, choose the proxy protocol from the adjacent drop-down list.
8. To add protocols for this policy, click **Add**.
   The Add Protocol dialog box appears.



9. From the **Type** drop-down list, select **Single Port** or **Port Range**.
10. From the **Protocol** drop-down list, select the protocol for this new policy.
    If you select **Single Port**, you can select **TCP**, **UDP**, **GRE**, **AH**, **ESP**, **ICMP**, **IGMP**, **OSP**, **IP**, or **Any**.
    If you select **Port Range**, you can select **TCP** or **UDP**. The options below the drop-down list change for each protocol.

> ***Note*** *Fireware XTM does not pass IGMP multicast traffic through the XTM device, or between XTM device interfaces. It passes IGMP multicast traffic only between an interface and the XTM device.*

11. If you selected **Single Port**, in the **Port Number** text box, type or select the port for this new policy.
    If you selected **Port Range**, in the **First port number** and **Last port number** text boxes, type or select the starting server port and the ending server port.
12. Click **Save**.
    The policy template is added to the Custom policies folder.

You can now use the policy template you created to add one or more custom policies to your configuration. Use the same procedure as you would for a predefined policy.

About Policy Properties

Each policy type has a default definition, which consists of settings that are appropriate for most organizations. However, you can modify policy settings for your particular business purposes, or add other settings such as traffic management and operating schedules.

Mobile VPN policies are created and operate in the same way as firewall policies. However, you must specify a Mobile VPN group to which the policy applies.

At the top of the policy configuration page, you can change the policy name. If the policy is a proxy policy, you can also change the proxy action. For more information, see *About Proxy Actions* on page 317.

To set properties for an existing policy, on the **Firewall Policies** page, double-click the policy to open the **Policy Configuration** page. When you add a new policy to your configuration, the **Policy Configuration** page automatically appears.

Policy Tab

Use the **Policy** tab to set basic information about a policy, such as whether it allows or denies traffic, and which devices it manages. You can use the Policy tab settings to create access rules for a policy, or configure policy-based routing, static NAT, or server load balancing.

For more information on the options for this tab, see the following topics:

- *Set Access Rules for a Policy* on page 307
- *Configure Policy-Based Routing* on page 309
- *Configure Static NAT* on page 160
- *Configure Server Load Balancing* on page 163

Properties Tab

The **Properties** tab shows the port and protocol to which the policy applies, as well as a description of the policy that you set. You can use the settings on this tab to set logging, notification, automatic blocking, and timeout preferences.

For more information on the options for this tab, see the following topics:

- *Set Logging and Notification Preferences* on page 466
- *Block Sites Temporarily with Policy Settings* on page 452
- *Set a Custom Idle Timeout* on page 312

Advanced Tab

The **Advanced** tab includes settings for NAT and Traffic Management (QoS), as well as multi-WAN and ICMP options.

For more information on the options for this tab, see the following topics:

- *Set an Operating Schedule* on page 302
- *Add a Traffic Management Action to a Policy* on page 438
- *Set ICMP Error Handling* on page 312
- *Apply NAT Rules* on page 312
- *Enable QoS Marking or Prioritization Settings for a Policy* on page 435
- *Set the Sticky Connection Duration for a Policy* on page 313

Proxy Settings

Each proxy policy has connection-specific settings that you can customize. To learn more about the options for each proxy, see the *About* topic for that protocol.

About the DNS-Proxy on page 331
About the FTP-Proxy on page 343
About the H.323-ALG on page 349
About the HTTP-Proxy on page 357
About the HTTPS-Proxy on page 377
About the POP3-Proxy on page 384
About the SIP-ALG on page 395
About the SMTP-Proxy on page 404
About the TCP-UDP-Proxy on page 422

Set Access Rules for a Policy

To configure access rules for a policy, select the **Policy** tab of the **Policy Configuration** dialog box.

The **Connections are** drop-down list defines whether traffic that matches the rules in the policy is allowed or denied. To configure how traffic is handled, select one of these settings:

Allowed

The XTM device allows traffic that uses this policy if it matches the rules you set in the policy. You can configure the policy to create a log message when network traffic matches the policy.

Denied

The XTM device denies all traffic that matches the rules in this policy and does not send a notification to the device that sent the traffic. You can configure the policy to create a log message when a computer tries to use this policy. The policy can also automatically add a computer or network to the Blocked Sites list if it tries to start a connection with this policy.

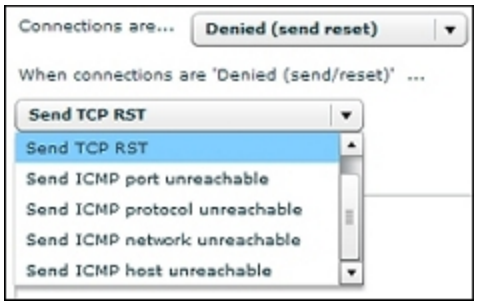
For more information, see *Block Sites Temporarily with Policy Settings* on page 452.

Denied (send reset)

The XTM device denies all traffic that matches the rules in this policy. You can configure it to create a log message when a computer tries to use this policy. The policy can also automatically add a computer or network to the Blocked Sites list if it tries to start a connection with this policy

For more information, see *Block Sites Temporarily with Policy Settings* on page 452.

With this option, the XTM device sends a packet to tell the device which sent the network traffic that the session is refused and the connection is closed. You can set a policy to return other errors instead, which tell the device that the port, protocol, network, or host is unreachable. We recommend that you use these options with caution to ensure that your network operates correctly with other networks.



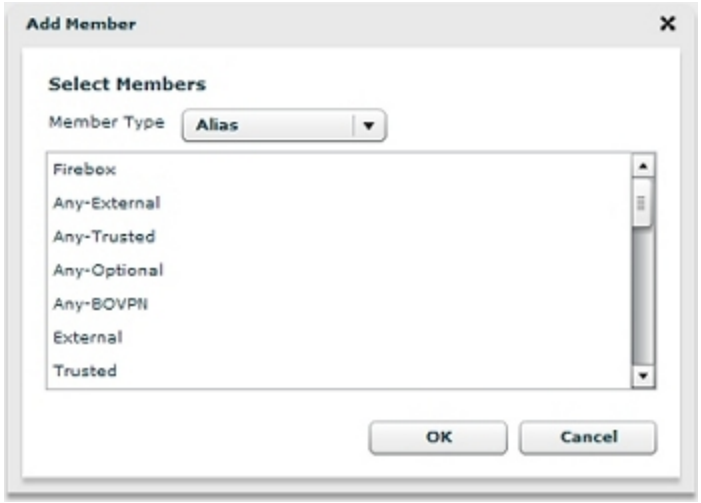
The **Policy** tab also includes:

- A **From** list (or *source*) that specifies who can send (or cannot send) network traffic with this policy.
- A **To** list (or *destination*) that specifies who the XTM device can route traffic to if the traffic matches (or does not match) the policy specifications.

For example, you could configure a ping packet filter to allow ping traffic from all computers on the external network to one web server on your optional network. However, when you open the destination network to connections over the port or ports that the policy controls, you can make the network vulnerable. Make sure you configure your policies carefully to avoid vulnerabilities.

To add members to your access specifications:

1. Adjacent to the **From** or the **To** member list, click **Add** .
   The Add Member dialog box appears.



   The list contains the members you can add to the **From** or **To** lists. A member can be an alias, user, group, IP address, or range of IP addresses.
2. In the **Member Type** drop-down list, specify the type of member you want to add to the box.
3. Select a member you want to add and click **Add**, or double-click an entry in this list.

4. To add other members to the **From** or **To** list, repeat the previous steps.
5. Click **OK**.

The source and destination can be a host IP address, host range, host name, network address, user name, alias, VPN tunnel, or any combination of those objects.

For more information on the aliases that appear in the **From** and **To** list, see *About Aliases* on page 294.

For more information about how to create a new alias or edit a user-defined alias, see *Create an Alias* on page 295.

Configure Policy-Based Routing

To send network traffic, a router usually examines the destination address in the packet and looks at the routing table to find the next-hop destination. In some cases, you want to send traffic to a different path than the default route specified in the routing table. You can configure a policy with a specific external interface to use for all outbound traffic that matches that policy. This technique is known as policy-based routing. Policy-based routing takes precedence over other multi-WAN settings.

Policy-based routing can be used when you have more than one external interface and have configured your XTM device for multi-WAN. With policy-based routing, you can make sure that all traffic for a policy always goes out through the same external interface, even if your multi-WAN configuration is set to send traffic in a round-robin configuration. For example, if you want email to be routed through a particular interface, you can use policy-based routing in the SMTP-proxy or POP3-proxy definition.

> ***Note*** *To use policy-based routing, you must have Fireware XTM with a Pro upgrade. You must also configure at least two external interfaces.*

Policy-Based Routing, Failover, and Failback

When you use policy-based routing with multi-WAN failover, you can specify whether traffic that matches the policy uses another external interface when failover occurs. The default setting is to drop traffic until the interface is available again.

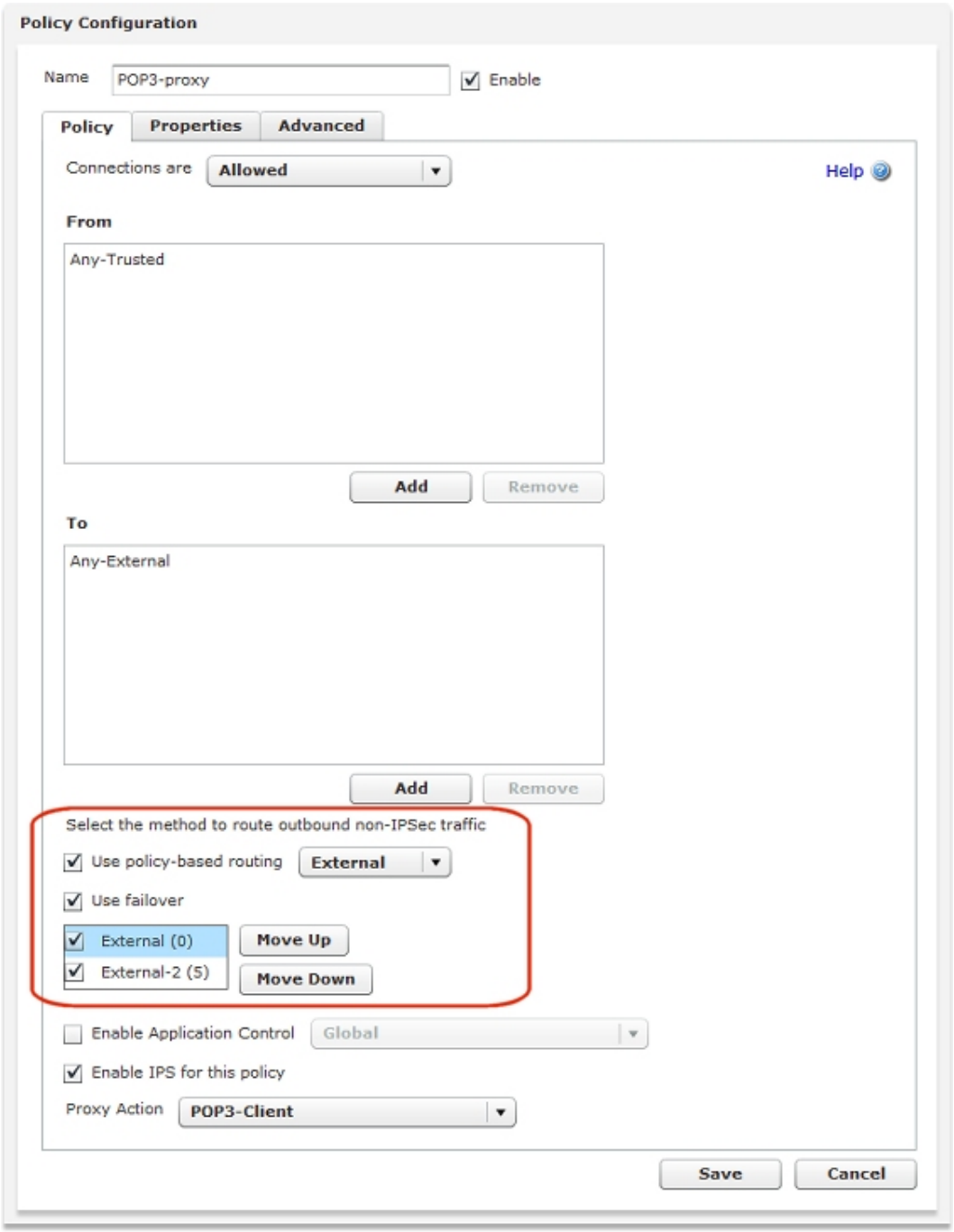
Failback settings (defined on the **Multi-WAN** tab of the **Network Configuration** dialog box) also apply to policy-based routing. If a failover event occurs, and the original interface later becomes available, the XTM device can send active connections to the failover interface, or it can fail back to the original interface. New connections are sent to the original interface.

Restrictions on Policy-Based Routing

- Policy-based routing is available only if multi-WAN is enabled. If you enable multi-WAN, the **Edit Policy Properties** dialog box automatically includes fields to configure policy-based routing.
- By default, policy-based routing is not enabled.
- Policy-based routing does not apply to IPSec traffic, or to traffic destined for the trusted or optional network (incoming traffic).

Add Policy-Based Routing to a Policy

1. Select **Firewall > Firewall Policies**.
2. Select a policy and click .
   Or, double-click a policy.
   The Policy Configuration page appears.
3. Select the **Use policy-based routing** check box.



4. To specify the interface to send outbound traffic that matches the policy, select the interface name from the adjacent drop-down list. Make sure that the interface you select is a member of the alias or network that you set in the **To** list for your policy.
5. (Optional) Configure policy-based routing with multi-WAN failover as described below. If you do not select **Failover** and the interface you set for this policy is becomes inactive, traffic is dropped until the interface becomes available again.
6. Click **Save**.

Configure Policy-Based Routing with Failover

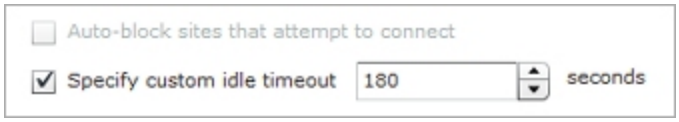
You can set the interface you specified for this policy as the primary interface, and define other external interfaces as backup interfaces for all non-IPSec traffic. If the primary interface you set for a policy is not active, traffic is sent to the backup interface or interfaces you specify.

1. On the **Policy Configuration** page, select **Use Failover**.
2. In the adjacent list, select the check box for each interface you want to use in the failover configuration.
3. To set the order for failover, click **Move Up** and **Move Down**.
   The first interface in the list is the primary interface.
4. Click **Save**.

Set a Custom Idle Timeout

Idle timeout is the maximum length of time that a connection can stay active when no traffic is sent. By default, the XTM device closes network connections after 8 hours for a packet filter policy and 10 minutes for a proxy policy. When you enable the custom idle timeout setting for a policy, the XTM device closes the connection after the length of time that you specify. The default custom idle timeout setting is 180 seconds (3 minutes).

1. On the **Policy Configuration** page, select the **Properties** tab.
2. Select the **Specify Custom Idle Timeout** check box.



3. In the adjacent text box, type or select the number of seconds before a timeout occurs.

Set ICMP Error Handling

You can set the ICMP error handling settings associated with a policy. These settings override the global ICMP error handling settings.

To change the ICMP error handling settings for the current policy:

1. Select the **Advanced** tab.
2. Select the **Use policy based ICMP error handling** check box.
3. Select one or more check boxes to override the global ICMP settings for that parameter.

For more information on global ICMP settings, see *Define XTM Device Global Settings* on page 67.

Apply NAT Rules

You can apply Network Address Translation (NAT) rules to a policy. You can select 1-to-1 NAT or Dynamic NAT.

1. On the **Policy Configuration** page, select the **Advanced** tab.
2. Select one of the options described in the subsequent sections.

1-to-1 NAT

With this type of NAT, the XTM device uses private and public IP ranges that you set, as described in *About 1-to-1 NAT* on page 149.

Dynamic NAT

With this type of NAT, the XTM device maps private IP addresses to public IP addresses. All policies have dynamic NAT enabled by default.

Select **Use Network NAT Settings** if you want to use the dynamic NAT rules set for the XTM device.

Select **All traffic in this policy** if you want to apply NAT to all traffic in this policy.

In the **Set Source IP** field, you can select a dynamic NAT source IP address for any policy that uses dynamic NAT. This makes sure that any traffic that uses this policy shows a specified address from your public or external IP address range as the source. This is helpful if you want to force outgoing SMTP traffic to show your domain's MX record address when the IP address on the XTM device external interface is not the same as your MX record IP address.

1-to-1 NAT rules have higher precedence than dynamic NAT rules.

Set the Sticky Connection Duration for a Policy

The sticky connection setting for a policy overrides the global sticky connection setting. You must enable multi-WAN to use this feature.

1. On the **Policy Properties** page, select the **Advanced** tab.
2. To use the global multi-WAN sticky connection setting, clear the **Override Multi-WAN sticky connection setting** check box.
3. To set a custom sticky connection value for this policy, select the **Enable sticky connection** check box.
4. In the **Enable sticky connection** text box, type the amount of time in minutes to maintain the connection.

13 Proxy Settings

About Proxy Policies and ALGs

All WatchGuard policies are important tools for network security, whether they are packet filter policies, proxy policies, or application layer gateways (ALGs). A packet filter examines each packet's IP and TCP/UDP header, a proxy monitors and scans whole connections, and an ALG provides transparent connection management in addition to proxy functionality. Proxy policies and ALGs examine the commands used in the connection to make sure they are in the correct syntax and order, and use deep packet inspection to make sure that connections are secure.

A proxy policy or ALG opens each packet in sequence, removes the network layer header, and examines the packet's payload. A proxy then rewrites the network information and sends the packet to its destination, while an ALG restores the original network information and forwards the packet. As a result, a proxy or ALG can find forbidden or malicious content hidden or embedded in the data payload. For example, an SMTP proxy examines all incoming SMTP packets (email) to find forbidden content, such as executable programs or files written in scripting languages. Attackers frequently use these methods to send computer viruses. A proxy or ALG can enforce a policy that forbids these content types, while a packet filter cannot detect the unauthorized content in the packet's data payload.

If you have purchased and enabled additional subscription services (Gateway AntiVirus, Intrusion Prevention Service, spamBlocker, WebBlocker), WatchGuard proxies can apply these services to network traffic.

Proxy Configuration

Like packet filters, proxy policies include common options to manage network traffic, including traffic management and scheduling features. However, proxy policies also include settings that are related to the specified network protocol. These settings are configured with *rulesets*, or groups of options that match a specified action. For example, you can configure rulesets to deny traffic from individual users or devices, or allow VoIP (Voice over IP) traffic that matches the codecs you want. When you have set all of the configuration options in a proxy, you can save that set of options as a user-defined proxy action and use it with other proxies.

Fireware XTM supports proxy policies for many common protocols, including DNS, FTP, H.323, HTTP, HTTPS, POP3, SIP, SMTP, and TCP-UDP. For more information on a proxy policy, see the section for that policy.

About the DNS-Proxy on page 331
About the FTP-Proxy on page 343
About the H.323-ALG on page 349
About the HTTP-Proxy on page 357
About the HTTPS-Proxy on page 377
About the POP3-Proxy on page 384
About the SIP-ALG on page 395
About the SMTP-Proxy on page 404
About the TCP-UDP-Proxy on page 422

Add a Proxy Policy to Your Configuration

When you add a proxy policy or ALG (application layer gateway) to your Fireware XTM configuration, you specify types of content that the XTM device must find as it examines network traffic. If the content matches (or does not match) the criteria you set in the proxy or ALG definition, the traffic is either allowed or denied.

You can use the default settings of the proxy policy or ALG, or you can change these settings to match network traffic in your organization. You can also create additional proxy policies or ALGs to manage different parts of your network.

It is important to remember that a proxy policy or ALG requires more processor power than a packet filter. If you add a large number of proxy policies or ALGs to your configuration, network traffic speeds might decrease. However, a proxy or ALG uses methods that packet filters cannot use to catch dangerous packets. Each proxy policy includes several settings that you can adjust to create a balance between your security and performance requirements.

You can use Fireware XTM Web UI to add a proxy policy.

1. Select **Firewall > Firewall Policies**.
2. Click  .
3. From the **Select a Policy Type** list, select a packet filter, proxy policy, or ALG (application layer gateway). Click **Add Policy**.
   The Policy Configuration page appears.

For more information on the basic properties of all policies, see *About Policy Properties* on page 306.

Proxy policies and ALGs have default proxy action rulesets that provide a good balance of security and accessibility for most installations. If a default proxy action ruleset does not match the network traffic you want to examine, you can add a new proxy action, or clone an existing proxy action to modify the rules. You cannot modify a default predefined proxy action. For more information, see *About Rules and Rulesets* on page 323 and the *About* topic for the type of policy you added.

About the DNS-Proxy on page 331
About the FTP-Proxy on page 343
About the H.323-ALG on page 349
About the HTTP-Proxy on page 357
About the HTTPS-Proxy on page 377
About the POP3-Proxy on page 384
About the SIP-ALG on page 395
About the SMTP-Proxy on page 404
About the TCP-UDP-Proxy on page 422

About Proxy Actions

A proxy action is a specific group of settings, sources, or destinations for a type of proxy. Because your configuration can include several proxy policies of the same type, each proxy policy uses a different proxy action. Each proxy policy has predefined, or default, proxy actions for clients and servers. For example, you can use one proxy action for packets sent to a POP3 server protected by the XTM device, and a different proxy action to apply to email messages retrieved by POP3 clients. You can clone, edit, and delete proxy actions in your XTM device configuration.

Fireware XTM proxy actions are divided into two categories: *predefined* proxy actions , and *user-defined* proxy actions. The predefined proxy actions are configured to balance the accessibility requirements of a typical company, with the need to protect your computer assets from attacks. You cannot change the settings of predefined proxy actions. Instead, you must clone (copy) the existing predefined proxy action definition and save it as a new, user-defined proxy action. You cannot configure subscription services, such as Gateway AntiVirus, for predefined proxy actions. For example, if you want to change a setting in the POP3-Client proxy action, you must save it with a different name, such as POP3-Client.1.

You can create many different proxy actions for either clients or servers, or for a specified type of proxy policy. However, you can assign only one proxy action to each proxy policy. For example, a POP3 policy is linked to a *POP3-Client* proxy action. If you want to create a POP3 proxy action for a POP3 server, or an additional proxy action for POP3 clients, you must add new POP3 proxy policies to Policy Manager that use those new proxy actions.

Set the Proxy Action in a Proxy Policy

To set the proxy action for a proxy policy when you add a new policy:

1. Select **Firewall > Firewall Policies**.
   The Firewall Policies page appears.
2. Click  .
   The Select a policy type page appears.
3. Expand the **Proxies** list and select a proxy policy.
4. From the **Proxy Action** drop-down list, select the action to use with this policy.
5. Click **Add policy**.

To change a proxy action for an existing proxy policy:

1. Select **Firewall > Firewall Policies**.
   The Firewall Policies page appears.

2. Select the proxy policy you want to change.
   The Policy Configuration page appears.
3. From the **Proxy Action** drop-down list, select the proxy action to use with this policy.
4. Click **Save**.

Clone, Edit, or Delete Proxy Actions

To manage the proxy actions for your XTM device, you can clone, edit, and delete proxy actions. You can clone, edit, or delete any user-defined proxy action. You cannot make changes to predefined proxy actions, or delete them. You also cannot delete user-defined proxy actions that are used by a policy.

If you want to change the settings in a predefined proxy action, you can clone it and create a new, user-defined proxy action with the same settings. You can then edit the proxy action to modify the settings as necessary. If you choose to edit a predefined proxy action, you cannot save your changes. Instead, you are prompted to clone the changes you have made to a new, user-defined proxy action.

When you edit a proxy action, you can change the rules and rulesets, and the associated actions. Each the proxy action includes proxy action rules, which are organized into categories. Some categories are further subdivided into subcategories of rules.

The available categories of settings for each proxy action appear in an accordion list, with section headers that are always visible. When you select the section header for a category, the category section expands and the settings and rules for each category appear on the category panel. If the category includes more than one subcategory of settings, a *link bar* navigation menu appears at the top of the category panel.

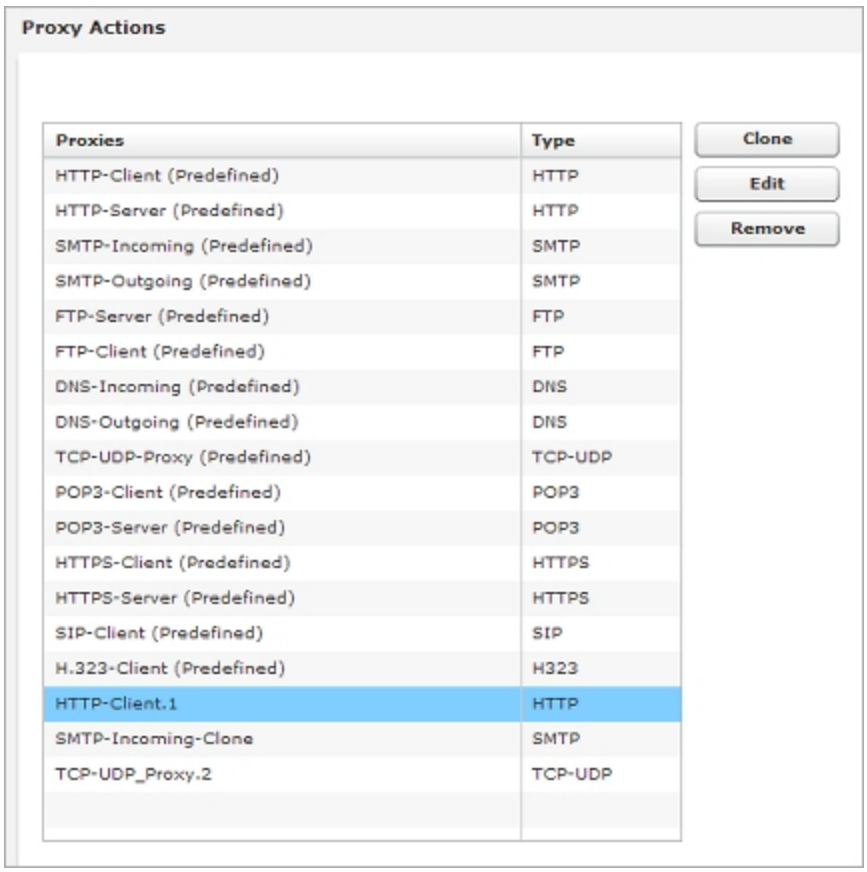
For more information on the available proxy action settings for each proxy, see the *About* topic for that proxy.

About the DNS-Proxy on page 331
About the FTP-Proxy on page 343
About the H.323-ALG on page 349
About the HTTP-Proxy on page 357
About the HTTPS-Proxy on page 377
About the POP3-Proxy on page 384
About the SIP-ALG on page 395
About the SMTP-Proxy on page 404
About the TCP-UDP-Proxy on page 422

Clone or Edit a Proxy Action

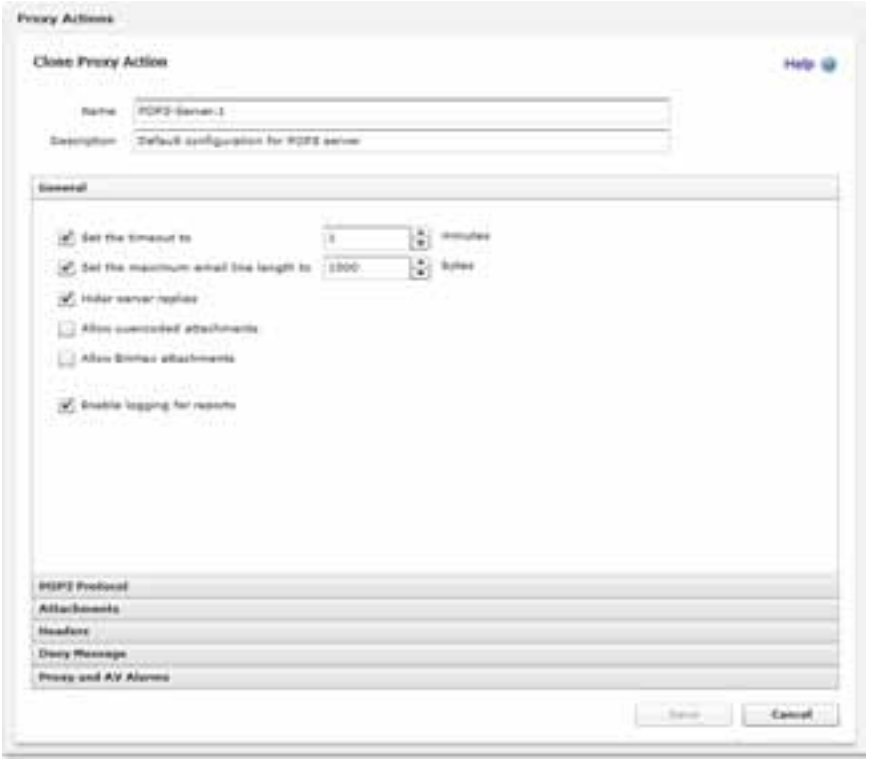
You can clone both predefined and user-defined proxy actions. But, you can only edit a user-defined proxy action.

1. Select **Firewall > Proxy Actions**.
   The Proxy Actions page appears.

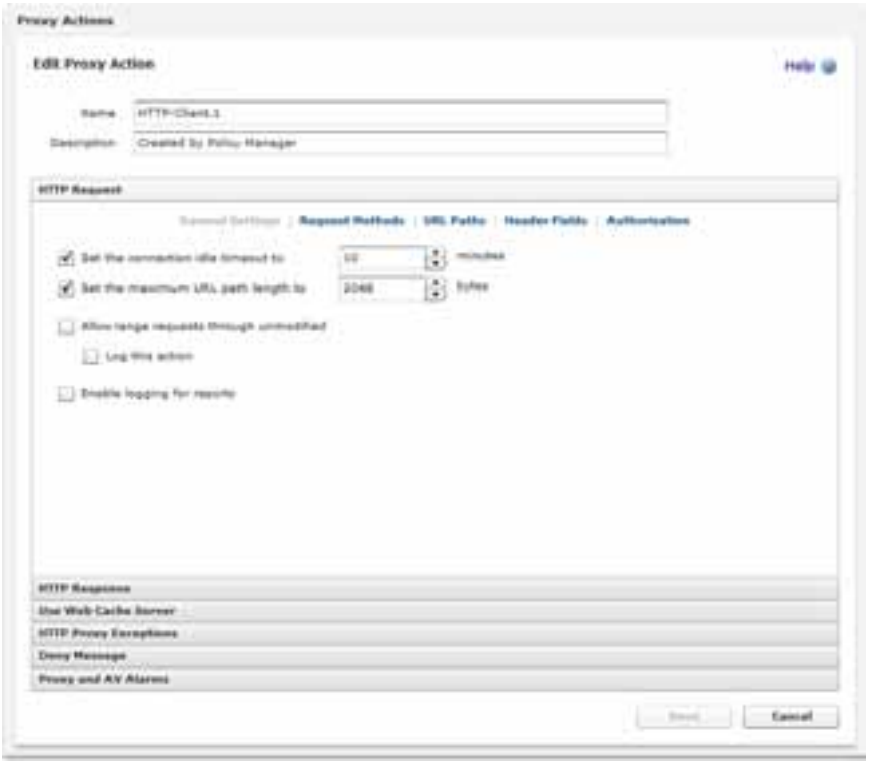


2. Select the proxy action to clone or edit.
3. Click **Clone** or **Edit**.

   If you selected to clone a proxy action, the Clone Proxy Action page appears, with the available categories displayed in an accordion list.



If you selected to edit a proxy action, the Edit Proxy Action page appears, with the available categories displayed in an accordion list.



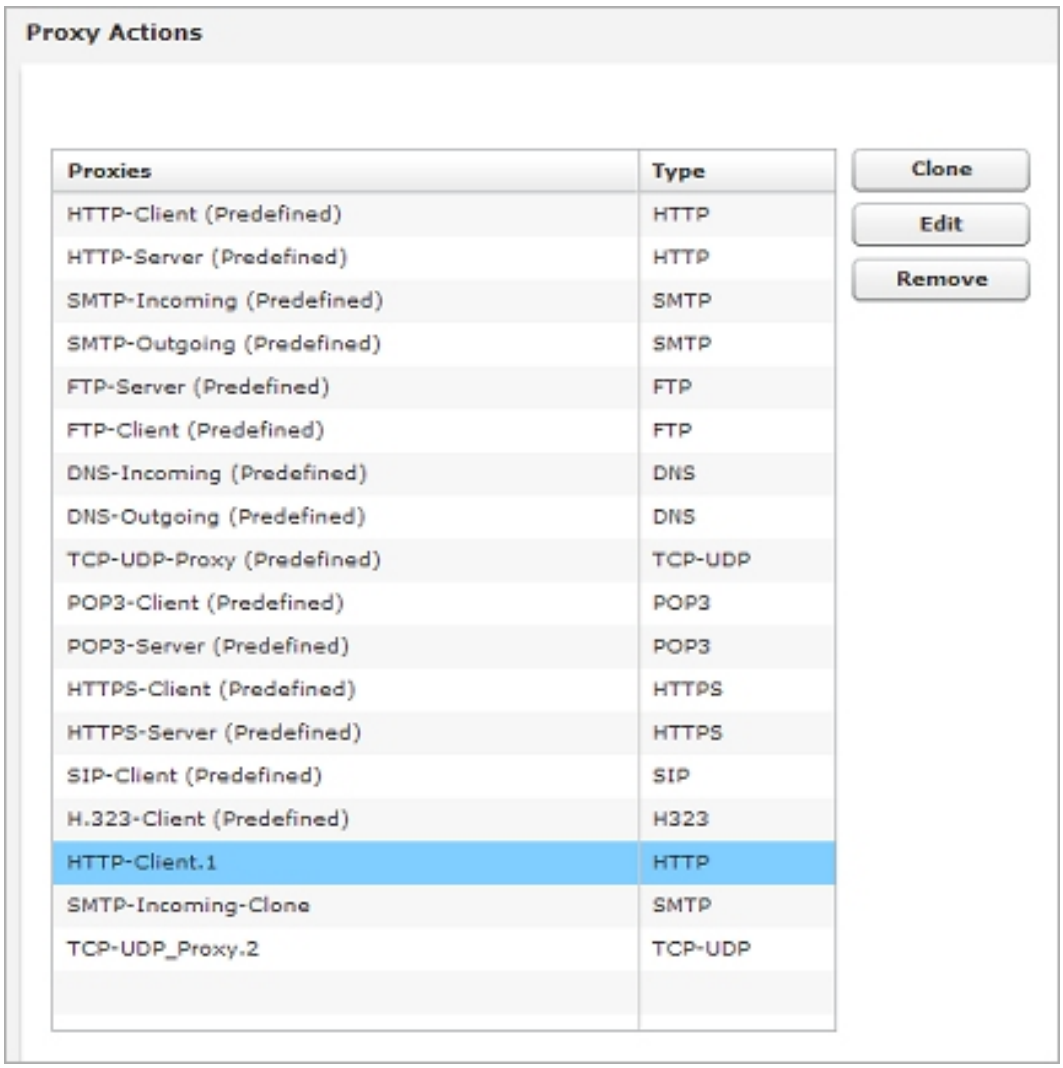
4. Select a category section header to expand the panel for that category.
   The panel for the selected category appears. If the category you selected includes subcategories, the link bar also appears.

5. If necessary, from the link bar, select a subcategory to edit.
6. Edit the rules and settings for the proxy action for all the necessary categories.
7. Click **Save**.

Delete a Proxy Action

You cannot delete predefined proxy actions. You can only delete user-defined proxy actions that are not used by a policy.

1. Select **Firewall > Proxy Actions**.
   The Proxy Actions page appears.



2. Select the proxy action to delete.
3. Click **Remove**.
   A confirmation dialog box appears.
4. To delete the proxy action, click **Yes**.
   The proxy action is removed from your device configuration.

Proxy and AV Alarms

An alarm is an event that triggers a *notification*, which is a mechanism to tell a network administrator about a condition in the network. In a proxy definition, an alarm might occur when traffic matches, or does not match, a rule in the proxy. An alarm might also occur when the **Actions to take** selections are set to an action other than **Allow**.

For example, the default definition of the FTP-proxy has a rule that denies the download of files whose file types match any of these patterns: .cab, .com, .dll, .exe, and .zip. You can specify that an alarm is generated whenever the XTM device takes the **Deny** action because of this rule.

For each proxy action, you can define what the XTM device does when an alarm occurs.

AV alarm settings are only available if Gateway AntiVirus applies to the proxy. Gateway AntiVirus is available for the SMTP, POP3, HTTP, FTP, or TCP-UDP proxies. For all other proxies, you can only configure the proxy alarm settings.

From the **Edit Proxy Action** page:

1. Expand the **Proxy and AV Alarms** category.
2. Configure the XTM device to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email message to a network administrator or a pop-up window on the administrator's management computer.

   For more information on the Proxy and AV alarms settings, see *Set Logging and Notification Preferences* on page 466.
3. To change settings for one or more other categories in this proxy, go to the topic on the next category you want to modify.
4. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

About Rules and Rulesets

When you configure a proxy policy or ALG (application layer gateway), you must select a proxy action to use. You can use either a predefined proxy action or create a new proxy action. Each proxy action contains rules. Rules are sets of criteria to which a proxy compares traffic.

A rule consists of a type of content, pattern, or expression, and the action of the XTM device when a component of the packet's content matches that content, pattern, or expression. Rules also include settings for when the XTM device sends alarms or creates a log entry. A ruleset is a group of rules based on one feature of a proxy such as the content types or filenames of email attachments. The process to create and modify rules is consistent for each type of proxy action.

Your XTM device configuration includes default sets of rules in each proxy actions used by each proxy policy. Separate sets of rules are provided for clients and servers, to protect both your trusted users and your public servers. You can use the default configuration for these rules, or you can customize them for your particular business purposes. You cannot modify or delete predefined proxy actions. If you want to make changes to a predefined proxy action, you can clone it a new proxy action and then make the necessary changes in the new proxy action.

About Working with Rules and Rulesets

When you edit a proxy action, you can see the list of rulesets that apply to that proxy action. You can expand each ruleset to see and edit the rules for that proxy action.

WatchGuard provides a set of predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can *Add, Change, or Delete Rules*.

Configure Rulesets

To configure rulesets for a proxy action:

1. Select **Firewall > Proxy Actions**.
   The Proxy Actions page appears.
2. Double-click a proxy action to edit it.
   The Edit Proxy Action page appears,with an expandable list of rulesets.
3. *Add, Change, or Delete Rules*.

Add, Change, or Delete Rules

When you configure rules, you can use wildcard pattern matches, exact matches, and Perl-compatible regular expressions to identify content. When you add rules, you select the action for each rule, and you can edit, clone (use an existing rule definition to create a new rule), delete, or reset rules.

For more information, see *About Rules and Rulesets* on page 323 and *About Regular Expressions* on page 328.

When you configure a rule, you select the actions the proxy takes for each packet. Different actions appear for different proxies or for different features of a particular proxy. This list includes all possible actions:

Allow

Allows the connection.

Deny

Denies a specific request but keeps the connection if possible. Sends a response to the client.

Drop

Denies the specific request and drops the connection. Does not send a response to the sender. The XTM device sends only a TCP reset packet to the client. The client's browser might display "The connection was reset" or "The page cannot be displayed" but the browser does not tell the user why.

Block

Denies the request, drops the connection, and blocks the site. For more information on blocked sites, see *About Blocked Sites* on page 450.
All traffic from this site's IP address is denied for the amount of time specified in the **Firewall > Blocked Sites** page on the **Auto-Blocked** tab. Use this action only if you want to stop all traffic from the offender for this time.

Strip

Removes an attachment from a packet and discards it. The other parts of the packet are sent through the XTM device to its destination.

Lock

Locks an attachment, and wraps it so that it cannot be opened by the user. Only the administrator can unlock the file.

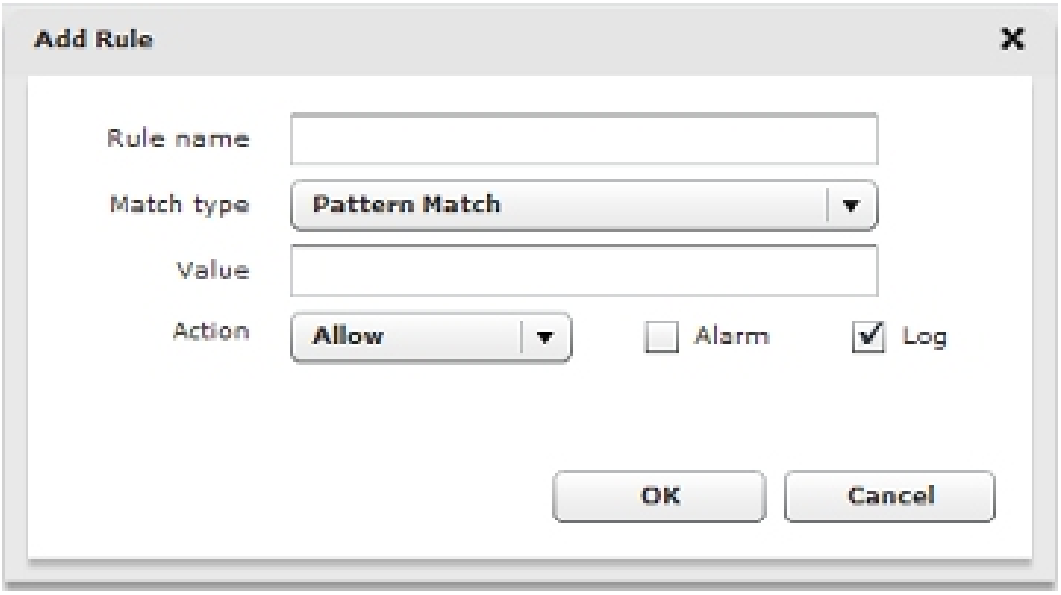
AV Scan

Scans the attachment for viruses. If you select this option, Gateway AntiVirus is enabled for the policy.

Add Rules

For information on how to work with regular expressions, see *About Regular Expressions* on page 328.

1. On the **Edit Proxy Action** page, in the list of rules for a ruleset, click **Add**.
   The Add Rule dialog box appears.



2. In the **Rule Name** text box, type the name of the rule.
   This text box is blank when you add a rule, and cannot be changed when you edit a rule.
3. In the **Match Type** drop-down list, select an option:

- **Exact Match** — Select when the contents of the packet must match the rule text exactly.
- **Pattern Match** — Select when the contents of the packet must match a pattern of text, can include wildcard characters.
- **Regular Expression** — Select when the contents of the packet must match a pattern of text with a regular expression.

4. In the **Value** text box, type the text of the rule.
   If you selected **Pattern Match** as the rule setting, use an asterisk (*), a period (.), or a question mark (?) as wildcard characters.
5. In the **Rule Actions** section, in the **Action** drop-down list, select the action the proxy takes for this rule.
6. To create an alarm for this event, select the **Alarm** check box. An alarm tells users when a proxy rule applies to network traffic.
7. To create a message for this event in the traffic log, select the **Log** check box.

Cut and Paste Rule Definitions

You can copy and paste content in text boxes from one proxy definition to another. For example, suppose you write a custom deny message for the POP3 proxy. You can select the deny message, copy it, and paste it into the **Deny Message** text box for the SMTP proxy.

When you copy between proxy definitions, you must make sure the text box you copy from is compatible with the proxy you paste it into. You can copy rulesets only between proxies or categories within these four groups. Other combinations are not compatible.

Content Types	Filenames	Addresses	Authentication
HTTP Content Types	FTP Download	SMTP Mail From	SMTP Authentication
SMTP Content Types	FTP Upload	SMTP Mail To	POP3 Authentication
POP3 Content Types	HTTP URL Paths		
	SMTP Filename		
	POP3 Filenames		

Change the Order of Rules

The order that rules are listed in a proxy action category is the same as the order in which traffic is compared to the rules. The proxy compares traffic to the first rule in the list and continues in sequence from top to bottom. When traffic matches a rule, the XTM device performs the related action. It performs no other actions, even if the traffic matches a rule later in the list.

To change the sequence of rules in a proxy action:

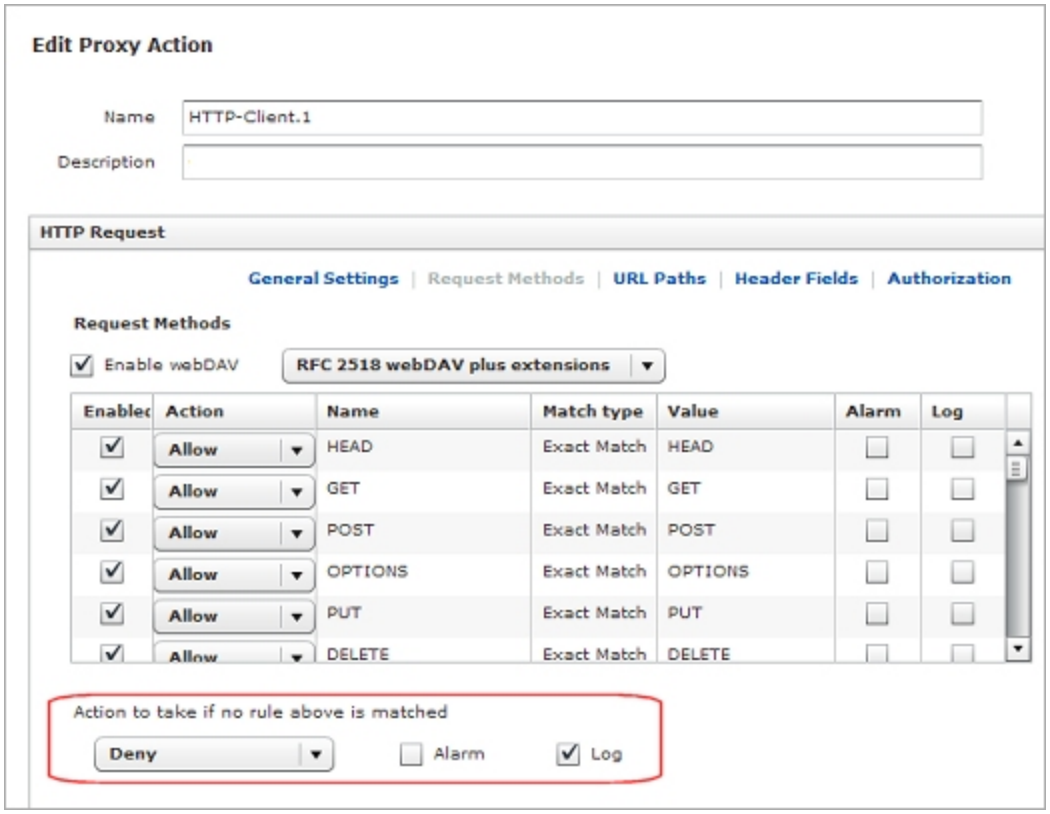
1. Select the rule whose order you want to change.
2. Click **Up** or **Down** to move the rule up or down in the list.

Change the Default Rule

If traffic does not match any of the rules you have defined for a proxy category, the XTM device uses the *default rule*. The action for the default rule appears in a drop-down list below the rule list.

To modify the default rule:

1. Select the default rule from the **Action to take if no rule above is matched** drop-down list.



2. Select the adjacent **Alarm** check box to send an alarm for the default rule.
3. Select the **Log** check box to save a log message for the default rule.
4. Click **Save**.

About Regular Expressions

A regular expression is a group of letters, numbers, and special characters used to match data. You can use Perl-compatible regular expressions (PCRE) in your XTM device configuration to match certain types of traffic in proxy actions. For example, you can use one regular expression to block connections to some web sites and allow connections to other web sites. You can also deny SMTP connections when the recipient is not a valid email address for your company. For example, if you want to block parts of a web site that violate your company's Internet use policy, you can use a regular expression in the URL Paths category of the HTTP proxy configuration.

General Guidelines

- Regular expressions in Fireware are case-sensitive — When you create a regular expression, you must be careful to match the case of the letters in your regular expression to the letters of the text you want to match. You can change the regular expression to not be case-sensitive when you put the (?i) modifier at the start of a group.
- Regular expressions in Fireware are different from MS-DOS and Unix wildcard characters — When you change files using MS-DOS or the Windows Command Prompt, you can use ? or * to match one or more characters in a file name. These simple wildcard characters do not operate the same way in Fireware.

For more information on how wildcard characters operate in Fireware, see the subsequent sections.

How to Build a Regular Expression

The most simple regular expression is made from the text you want to match. Letters, numbers, and other printable characters all match the same letter, number, or character that you type. A regular expression made from letters and numbers can match only a character sequence that includes all of those letters and numbers in order.

Example: fat matches fat, fatuous, and infatuated, as well as many other sequences.

> ***Note*** *Fireware accepts any character sequence that includes the regular expression. A regular expression frequently matches more than one sequence. If you use a regular expression as the source for a Deny rule, you can block some network traffic by accident. We recommend that you fully test your regular expressions before you save the configuration to your XTM device.*

To match different sequences of characters at the same time, you must use a special character. The most common special character is the period (.), which is similar to a wildcard. When you put a period in a regular expression, it matches any character, space, or tab. The period does not match line breaks (\r\n or \n).

Example: f..t matches foot, feet, f&#t, f -t, and f\t3t.

To match a special character, such as the period, you must add a backslash (\) before the character. If you do not add a backslash to the special character, the rule may not operate correctly. It is not necessary to add a second backslash if the character usually has a backslash, such as \t (tab stop).

You must add a backslash to each of these special characters to match the real character: ? . * | + $ \ ^ ( ) [

Example: \$9\.99 matches $9.99

Hexadecimal Characters

To match hexadecimal characters, use \x or %0x%. Hexadecimal characters are not affected by the case-insensitive modifier.

Example: \x66 or %0x66% matches f, but cannot match F.

Repetition

To match a variable amount of characters, you must use a repetition modifier. You can apply the modifier to a single character, or a group of characters. There are four types of repetition modifiers:

- Numbers inside curly braces (such as {2,4}) match as few as the first number, or as many as the second number.
  Example: 3{2,4} matches 33, 333, or 3333. It does not match 3 or 33333.
- The question mark (?) matches zero or one occurrence of the preceding character, class, or group.
  Example: me?et matches met and meet.
- The plus sign (+) matches one or more occurrences of the preceding character, class, or group.
  Example: me+t matches met, meet, and meeeeeeeeet.

- The asterisk (*) matches zero or more occurrences of the preceding character, class, or group. Example: me*t matches mt, met, meet, and meeeeeeeeet.

To apply modifiers to many characters at once, you must make a group. To group a sequence of characters, put parentheses around the sequence.

Example: ba(na)* matches ba, bana, banana, and bananananananana.

Character Classes

To match one character from a group, use square brackets instead of parentheses to create a character class. You can apply repetition modifiers to the character class. The order of the characters inside the class does not matter.

The only special characters inside a character class are the closing bracket (]), the backslash (\), the caret (^), and the hyphen (-).

Example: gr[ae]y matches gray and grey.

To use a caret in the character class, do not make it the first character.

To use a hyphen in the character class, make it the first character.

A negated character class matches everything but the specified characters. Type a caret (^) at the beginning of any character class to make it a negated character class.

Example: [Qq][^u] matches Qatar, but not question or Iraq.

Ranges

Character classes are often used with character ranges to select any letter or number. A range is two letters or numbers, separated by a hyphen (-), that mark the start and finish of a character group. Any character in the range can match. If you add a repetition modifier to a character class, the preceding class is repeated.

Example: [1-3][0-9]{2} matches 100 and 399, as well as any number in between.

Some ranges that are used frequently have a shorthand notation. You can use shorthand character classes inside or outside other character classes. A negated shorthand character class matches the opposite of what the shorthand character class matches. The table below includes several common shorthand character classes and their negated values.

Class	Equivalent to	Negated	Equivalent to
\w	Any letter or number [A-Za-z0-9]	\W	Not a letter or number
\s	Any whitespace character [\t\r\n]	\S	Not whitespace
\d	Any number [0-9]	\D	Not a number

Anchors

To match the beginning or end of a line, you must use an anchor. The caret (^) matches the beginning of a line, and the dollar sign ($) matches the end of a line.

Example: ^am.*$ matches ampere if ampere is the only word on the line. It does not match dame.

You can use \b to match a word boundary, or \B to match any position that is not a word boundary.

There are three kinds of word boundaries:

- Before the first character in the character sequence, if the first character is a word character (\w)•
- After the last character in the character sequence, if the last character is a word character (\w)•
- Between a word character (\w) and a non-word character (\W)

Alternation

You can use alternation to match a single regular expression out of several possible regular expressions. The alternation operator in a regular expression is the pipe character (|). It is similar to the boolean operator *OR*.

Example: m(oo|a|e)n matches the first occurrence of moon, man, or men.

Common Regular Expressions

Match the PDF content type (MIME type)

^%PDF-

Match any valid IP address

(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9] [0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]? [0-9][0-9]?)

Match most email addresses

[A-Za-z0-9._-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}

About the DNS-Proxy

The Domain Name System (DNS) is a network system of servers that translates numeric IP addresses into readable, hierarchical Internet addresses, and vice versa. DNS enables your computer network to understand, for example, that you want to reach the server at 200.253.208.100 when you type a domain name into your browser, such as www.example.com. With Fireware XTM, you have two methods to control DNS traffic: the DNS packet filter and the DNS-proxy policy. The DNS-proxy is useful only if DNS requests are routed through your XTM device.

When you create a new configuration file, the file automatically includes an Outgoing packet filter policy that allows all TCP and UDP connections from your trusted and optional networks to external. This allows your users to connect to an external DNS server with the standard TCP 53 and UDP 53 ports. Because Outgoing is a packet filter, it is unable to protect against common UDP outgoing trojans, DNS exploits, and

other problems that occur when you open all outgoing UDP traffic from your trusted networks. The DNS-proxy has features to protect your network from these threats. If you use external DNS servers for your network, the DNS-Outgoing ruleset offers additional ways to control the services available to your network community.

To add the DNS-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 316.

If you must change the proxy definition, you can use the **New/Edit Proxy Policies** page to modify the definition. This dialog box has three tabs: **Policy**, **Properties**, and **Advanced**.

Action Settings

At the top of the **Policy Configuration** page, you can set these actions:

- **Application Control Action** — If Application Control is enabled on your device, specify the application control action to use for this policy. For more information, see *Enable Application Control in a Policy*.
- **Proxy action** — Select the proxy action to use for this policy. For information about proxy actions, see *About Proxy Actions* on page 317.

Policy Tab

- **Connections are**— Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). See *Set Access Rules for a Policy* on page 307.
- **Use policy-based routing** — See *Configure Policy-Based Routing* on page 309.
- You can also configure static NAT or configure server load balancing. See *Configure Static NAT* on page 160 and *Configure Server Load Balancing* on page 163.

Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, configure the settings in the **Logging** section.
  For more information, see *Set Logging and Notification Preferences* on page 466.
- If you set the **Connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use DNS.
  For more information, see *Block Sites Temporarily with Policy Settings* on page 452.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

Advanced Tab

You can also configure these options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

Configure the Proxy Action

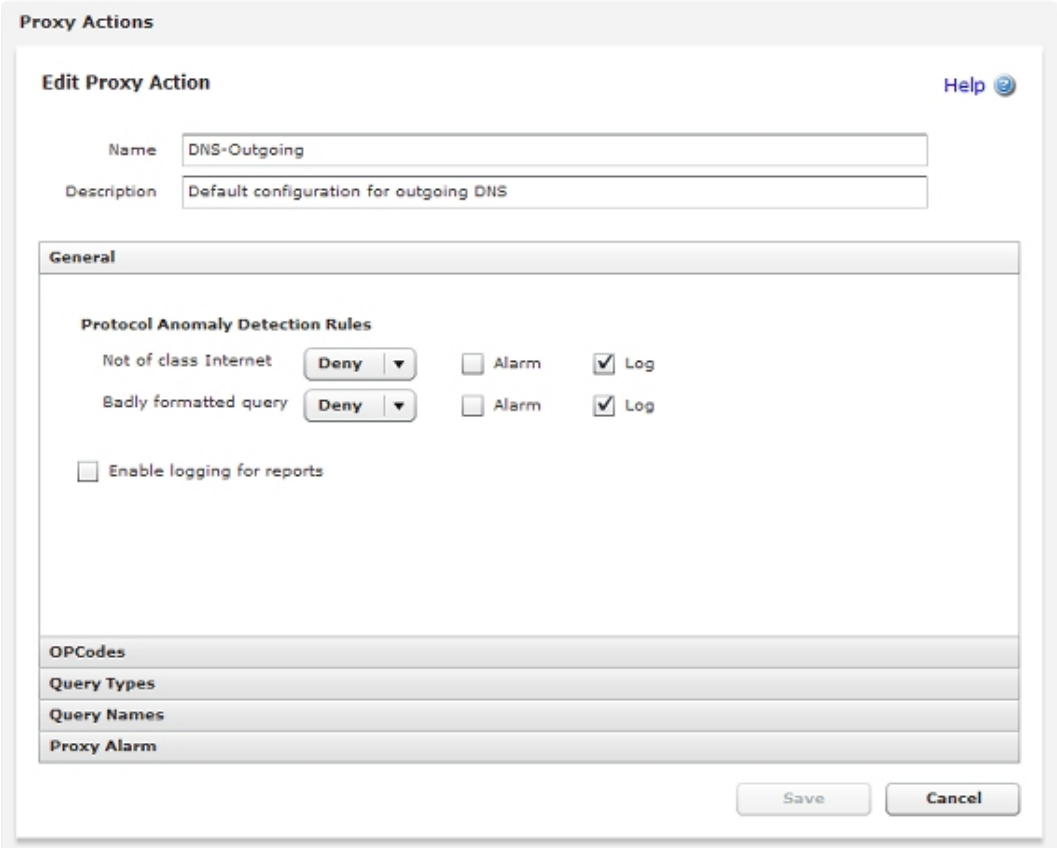
You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 317.

For the DNS-proxy, you can configure these categories of settings for a proxy action:

- *DNS-Proxy: General Settings*
- *DNS-Proxy: OPcodes*
- *DNS-Proxy: Query Types*
- *DNS-Proxy: Query Names*
- *DNS-Proxy: Proxy Alarm*

DNS-Proxy: General Settings

In the **General** section of the **Edit Proxy Action** page for a DNS-proxy action, you can change the settings of the two protocol anomaly detection rules. We recommend that you do not change the default rule settings. You can also select whether to create a traffic log message for each transaction.



Not of class Internet

Select the action when the proxy examines DNS traffic that is not of the Internet (IN) class. The default action is to deny this traffic. We recommend that you do not change this default action.

Badly formatted query

Select the action when the proxy examines DNS traffic that does not use the correct format.

Alarm

An alarm is a mechanism to tell users when a proxy rule applies to network traffic.

To configure an alarm for this event, select the **Alarm** check box.

To set the options for the alarm, from the **Categories** tree, select **Proxy Alarm**. Alarm notifications are sent in an SNMP trap, email, or a pop-up window.

For more information about proxy alarms, see *Proxy and AV Alarms*.

For more information about notification messages, see *Set Logging and Notification Preferences*.

Log

Select this check box to send a message to the traffic log for this event.

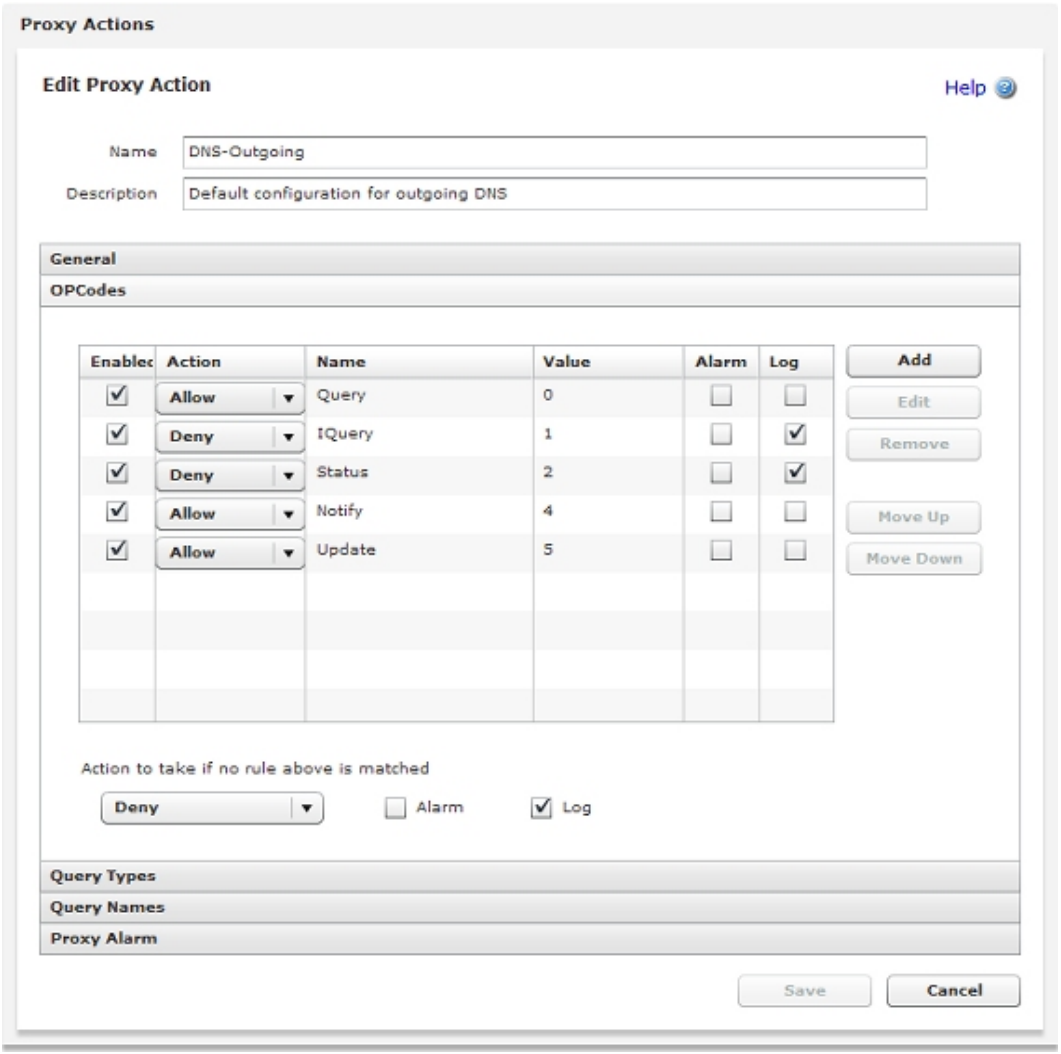
Enable logging for reports

Select this check box to create a traffic log message for each transaction. This option creates a large log file, but this information is very important if your firewall is attacked. If you do not select this check box, detailed information about DNS-proxy connections does not appear in your reports.

DNS-Proxy: OPcodes

DNS OPcodes (operation codes) are commands given to the DNS server that tell it to do some action, such as a query (Query), an inverse query (IQuery), or a server status request (STATUS). They operate on items such as registers, values in memory, values stored on the stack, I/O ports, and the bus. You can add, delete, or modify rules in the default ruleset. You can allow, deny, drop, or block specified DNS OPcodes.

1. In the **Edit Proxy Action** page for a DNS-proxy action, select the **OPCodes** category.



2. To enable a rule in the list, select the adjacent **Enabled** check box.
   To disable a rule, clear the **Enabled** check box.

> ***Note*** *If you use Active Directory and your Active Directory configuration requires dynamic updates, you must allow DNS OPcodes in your DNS-Incoming proxy action rules. This is a security risk, but can be necessary for Active Directory to operate correctly.*

Add a New OPcodes Rule

1. Click **Add**.
   The New OPCodes Rule dialog box appears.
2. Type a name for the rule.
   Rule names can have no more than 200 characters.
3. Click the arrows to set the **OPCode** value. DNS OPcodes have an integer value.

   For more information on the integer values of DNS OPcodes, see RFC 1035.

Delete or Modify Rules

1. Add, delete, or modify rules, as described in *Add, Change, or Delete Rules* on page 324.
2. To change settings for one or more other categories in this proxy, go to the topic on the next category you want to modify.
3. Click **Save**.

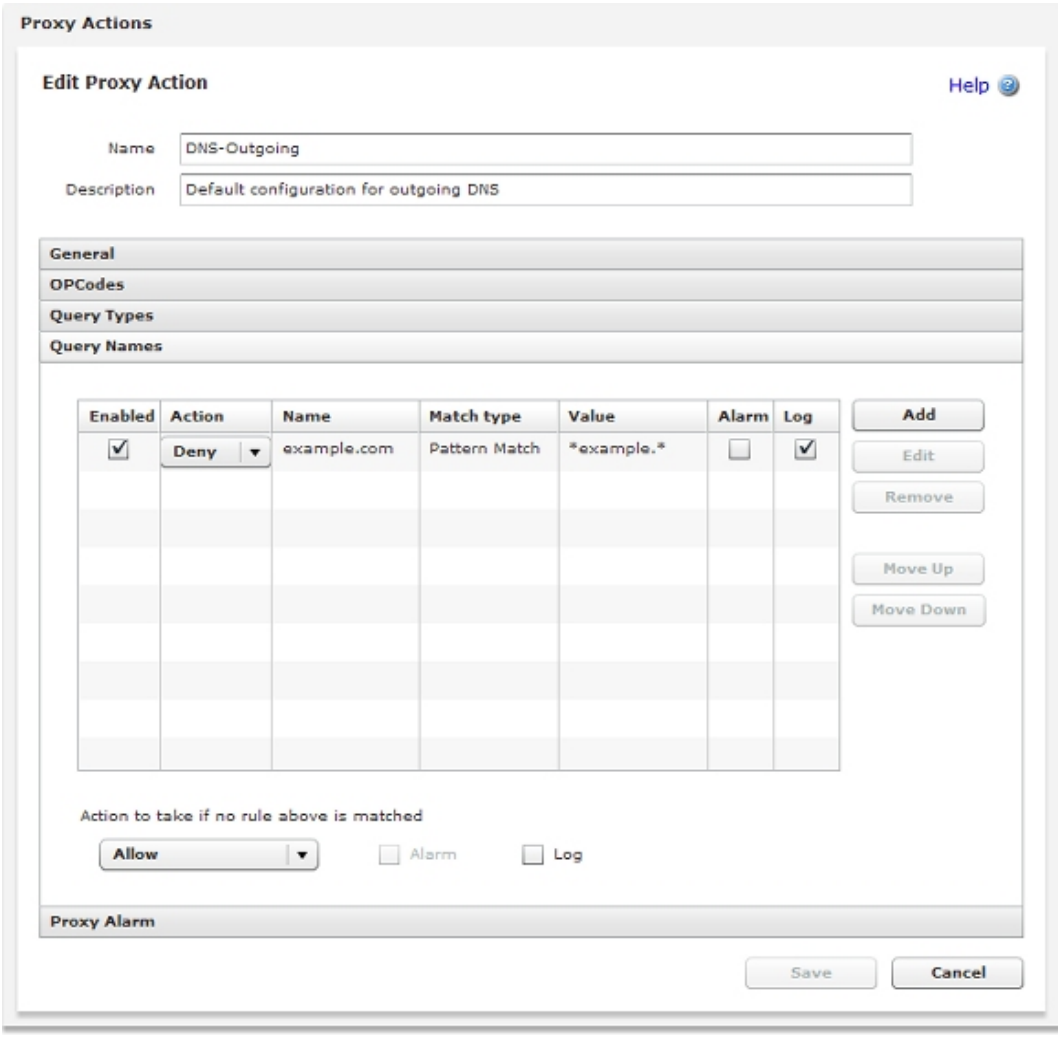
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

DNS-Proxy: Query Names

A DNS query name refers to a specified DNS domain name, shown as a fully qualified domain name (FQDN). You can add, delete, or modify rules.

1. On the **Edit Proxy Action** page, select the **Query Names** category.



2. Configure the rule action.
   For more information, see *Add, Change, or Delete Rules*.
3. To change settings for other categories in this proxy, go to the topic for the next category you want to modify and follow the instructions.
4. Click **Save**.

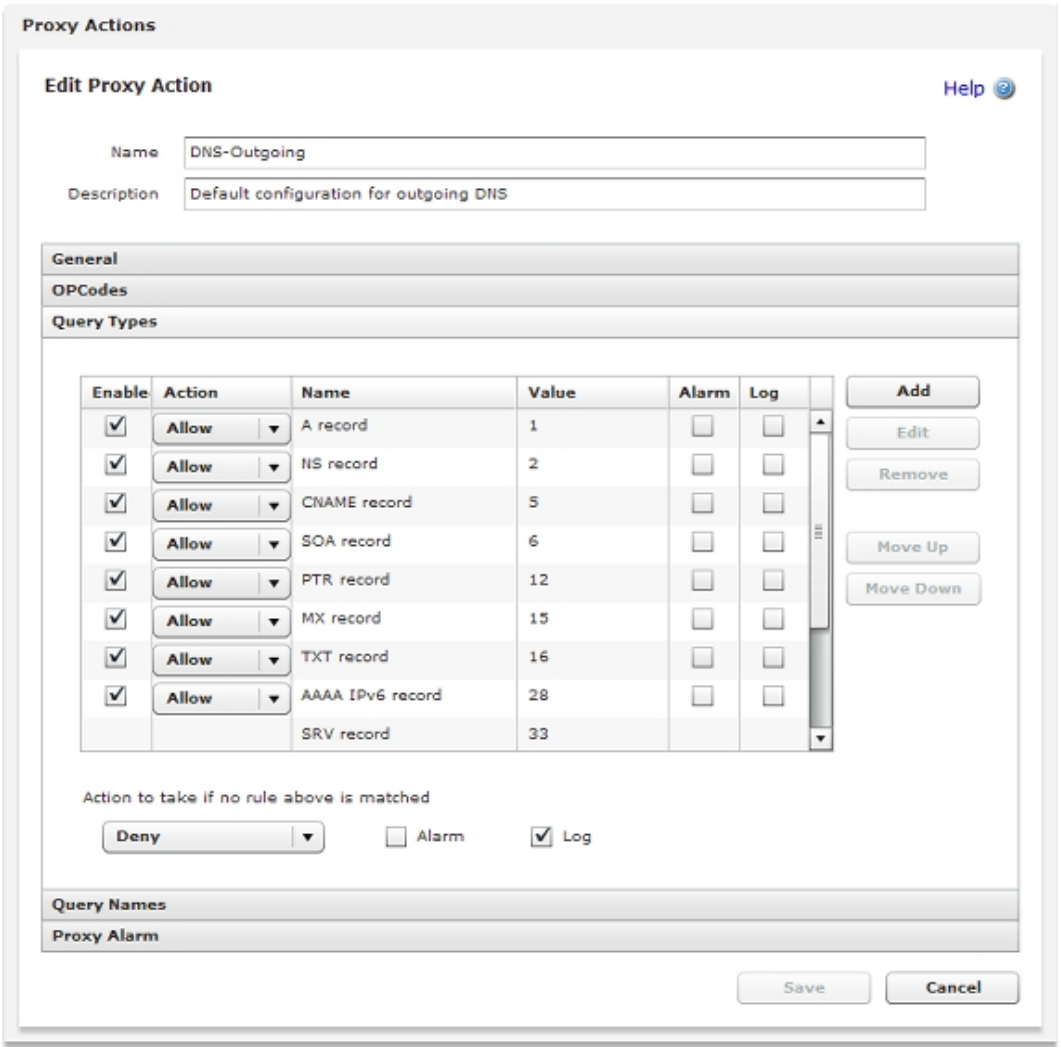
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

DNS-Proxy: Query Types

A DNS query type can configure a resource record by type (such as a CNAME or TXT record) or as a custom type of query operation (such as an AXFR Full zone transfer). You can add, delete, or modify rules. You can allow, deny, drop, or block specified DNS query types.

1. On the **Edit Proxy Action** page, select the **Query Types** category.



2. To enable a rule, select the **Enabled** check box adjacent to the action and name of the rule.

Add a New Query Types Rule

1. To add a new query types rule, click **Add**.
   The New Query Types Rule dialog box appears.
2. Type a name for the rule.
   Rules can have no more than 200 characters.
3. DNS query types have a resource record (RR) value. Use the arrows to set the value.
   For more information on the values of DNS query types, see RFC 1035.

4. Configure the rule action.
   For more information, see *Add, Change, or Delete Rules*.
5. To change settings for other categories in this proxy, go to the topic for the next category you want to modify and follow the instructions.
6. Click **Save**.

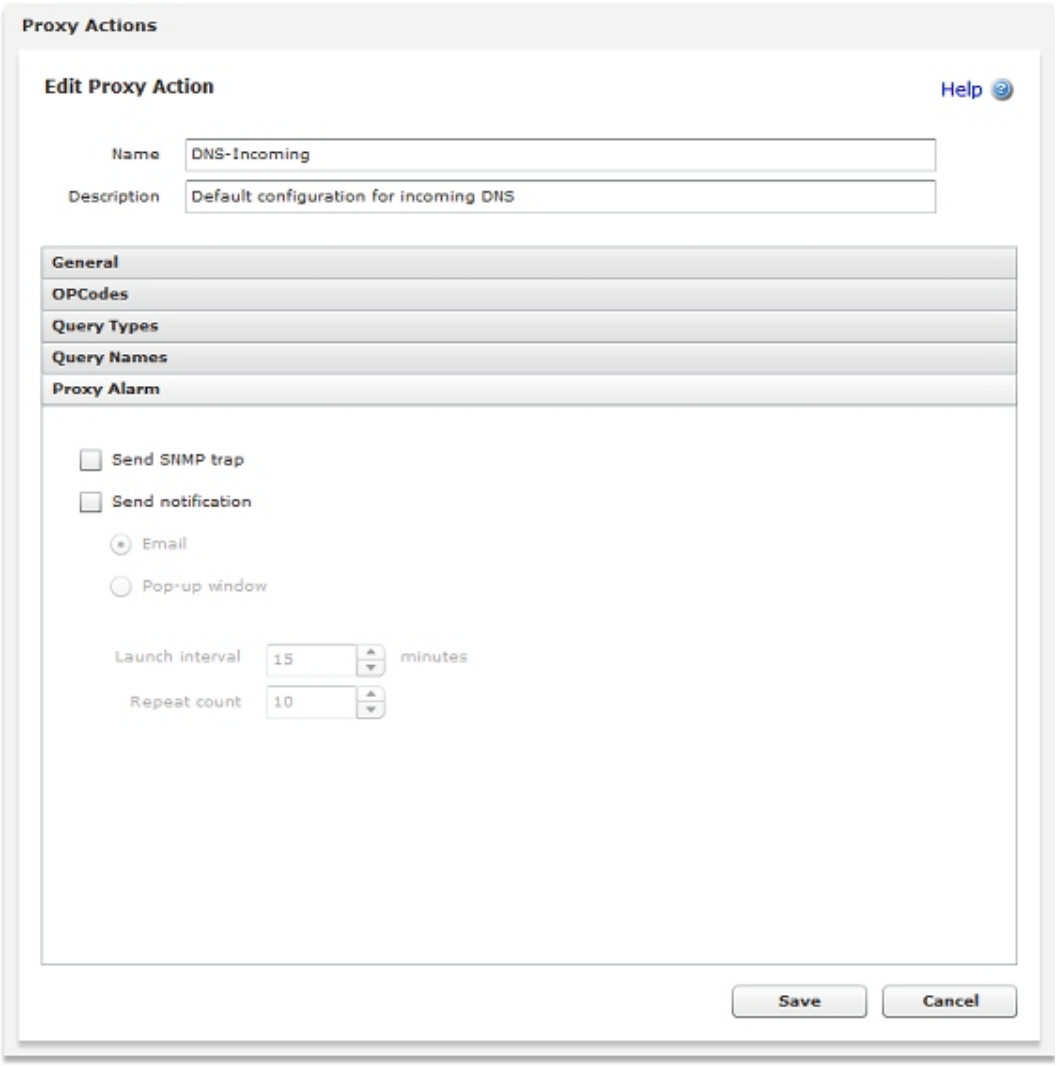
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

DNS-Proxy: Proxy Alarm

You can configure how the DNS-proxy sends messages for alarm events that occur through the DNS-proxy. You can define the proxy to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email message to a network administrator or a pop-up window on the management computer.

1. On the **Edit Proxy Action** page, select the **Proxy Alarm** category.
   The Proxy Alarm settings appear.



2. Configure the notification settings for the DNS-proxy action.
   For more information, see *Set Logging and Notification Preferences* on page 466.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

About MX (Mail eXchange) Records

An MX (Mail eXchange) record is a type of DNS record that gives one or more host names of the email servers that are responsible for and authorized to receive email for a given domain. If the MX record has more than one host name, each name has a number that tells which is the most preferred host and which hosts to try next if the most preferred host is not available.

MX Lookup

When an email server sends email, it first does a DNS query for the MX record of the recipient's domain. When it gets the response, the sending email server knows the host names of authorized mail exchangers for the recipient's domain. To get the IP addresses associated with the MX host names, a mail server does a second DNS lookup for the A record of the host name. The response gives the IP address associated with the host name. This lets the sending server know what IP address to connect to for message delivery.

Reverse MX Lookup

Many anti-spam solutions, including those used by most major ISP networks and web mail providers such as AOL, MSN, and Yahoo!, use a reverse MX lookup procedure. Different variations of the reverse lookup are used, but the goals are the same: the receiving server wants to verify that the email it receives does not come from a spoofed or forged sending address, and that the sending server is an authorized mail exchanger for that domain.

To verify that the sending server is an authorized email server, the receiving email server tries to find an MX record that correlates to the sender's domain. If it cannot find one, it assumes that the email is spam and rejects it.

The domain name that the receiving server looks up can be:

- Domain name in the email message's **From:** header
- Domain name in the email message's **Reply-To:** header
- Domain name the sending server uses as the FROM parameter of the MAIL command. (An SMTP command is different from an email header. The sending server sends the MAIL FROM: command to tell the receiving sender who the message is from.)
- Domain name returned from a DNS query of the connection's source IP address. The receiving server sometimes does a lookup for a PTR record associated with the IP address. A PTR DNS record is a record that maps an IP address to a domain name (instead of a normal *A* record, which maps a domain name to an IP address).

Before the receiving server continues the transaction, it makes a DNS query to see whether a valid MX record for the sender's domain exists. If the domain has no valid DNS MX record, then the sender is not valid and the receiving server rejects it as a spam source.

MX Records and Multi-WAN

Because outgoing connections from behind your XTM device can show different source IP addresses when your XTM device uses multi-WAN, you must make sure that your DNS records include MX records for each external IP address that can show as the source when you send email. If the list of host names in your domain's MX record does not include one for each external XTM device interface, it is possible that some remote email servers could drop your email messages.

For example, Company XYZ has an XTM device configured with multiple external interfaces. The XTM device uses the Failover multi-WAN method. Company XYZ's MX record includes only one host name. This host name has a DNS *A* record that resolves to the IP address of the XTM device primary external interface.

When Company XYZ sends an email to test@yahoo.com, the email goes out through the primary external interface. The email request is received by one of Yahoo's many email servers. That email server does a reverse MX lookup to verify the identify of Company XYZ. The reverse MX lookup is successful, and the email is sent.

If a WAN failover event occurs at the XTM device, all outgoing connections from Company XYZ start to go out the secondary, backup external interface. In this case, when the Yahoo email server does a reverse MX lookup, it does not find an IP address in Company XYZ's MX and *A* records that matches, and it rejects the email. To solve this problem, make sure that:

- The MX record has multiple host names, at least one for each external XTM device interface.
- At least one host name in the MX record has a DNS *A* record that maps to the IP address assigned to each XTM device interface.

Add Another Host Name to an MX Record

MX records are stored as part of your domain's DNS records. For more information on how to set up your MX records, contact your DNS host provider (if someone else hosts your domain's DNS service) or consult the documentation from the vendor of your DNS server software.

About the FTP-Proxy

FTP (File Transfer Protocol) is used to send files from one computer to a different computer over a TCP/IP network. The FTP client is usually a computer. The FTP server can be a resource that keeps files on the same network or on a different network. The FTP client can be in one of two modes for data transfer: active or passive. In active mode, the server starts a connection to the client on source port 20. In passive mode, the client uses a previously negotiated port to connect to the server. The FTP-proxy monitors and scans these FTP connections between your users and the FTP servers they connect to.

With an FTP-proxy policy, you can:

- Set the maximum user name length, password length, file name length, and command line length allowed through the proxy to help protect your network from buffer overflow attacks.
- Control the type of files that the FTP-proxy allows for downloads and uploads.

The TCP/UDP proxy is available for protocols on non-standard ports. When FTP uses a port other than port 20, the TCP/UDP proxy relays the traffic to the FTP-proxy. For information on the TCP/UDP proxy, see *About the TCP-UDP-Proxy* on page 422.

For detailed instructions on how to add the FTP-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 316.

If you must change the proxy definition, you can use the **Policy Configuration page** to modify the definition. This page has three tabs: **Policy**, **Properties**, and **Advanced**.

Action Settings

At the top of the **Policy Configuration** page, you can set these actions:

- **Application Control Action** — If Application Control is enabled on your device, specify the application control action to use for this policy. For more information, see *Enable Application Control in a Policy*.
- **Proxy action** — Select the proxy action to use for this policy. For information about proxy actions, see *About Proxy Actions* on page 317.

You can also configure Gateway AntiVirus service settings for the FTP-proxy. For more information, see *Configure the Gateway AntiVirus Service*.

Policy Tab

To set access rules and other options, select the **Policy** tab.

- **Connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**. Define who appears in the **From** and **To** lists.
  For more information, see *Set Access Rules for a Policy*.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing*.
- You can also configure static NAT or configure server load balancing.
  For more information, see *Configure Static NAT* on page 160 or *Configure Server Load Balancing* on page 163.

Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, configure the settings in the **Logging** section. For more information, see *Set Logging and Notification Preferences* on page 466.
- If you set the **Connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use FTP.
  For more information, see *Block Sites Temporarily with Policy Settings* on page 452.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

Advanced Tab

You can also configure these options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

Configure the Proxy Action

You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 317.

For the FTP-proxy, you can configure these categories of settings for a proxy action:

- *FTP-Proxy: General Settings*
- *FTP-Proxy: Commands*
- *FTP-Proxy: Content*
- *FTP-Proxy: Proxy and AV Alarms*

FTP-Proxy: General Settings

In the **General** section of the **Edit Proxy Action** page for an FTP-proxy action, you can set basic FTP parameters including maximum user name length.

1. On the **Edit Proxy Action** page, select the **General** category.
   The General settings appear.

2. To set limits for FTP parameters, select the applicable check boxes. These settings help to protect your network from buffer overflow attacks.

   Set the maximum user name length to

   Sets a maximum length for user names on FTP sites.

   Set the maximum password length to

   Sets a maximum length for passwords used to log in to FTP sites.

   Set the maximum file name length to

   Sets the maximum file name length for files to upload or download.

Set the maximum command line length to

Sets the maximum length for command lines used on FTP sites.

Set the maximum number of failed logins per connection to

Allows you to limit the number of failed connection requests to your FTP site. This can protect your site against brute force attacks.

3. In the text box for each setting, type or select the limit for the selected parameter.
4. For each setting, select or clear the **Auto-block** check box.
   If someone tries to connect to an FTP site and exceeds a limit whose **Auto-block** check box is selected, the computer that sent the commands is added to the temporary Blocked Sites List.
5. To create a log message for each transaction, select the **Enable logging for reports** check box.
   You must select this option to get detailed information on FTP traffic.
6. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
7. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

FTP-Proxy: Commands

FTP has a number of commands to manage files. You can configure rules to put limits on some FTP commands. To put limits on commands that can be used on an FTP server protected by the XTM device, you can configure the FTP-Server proxy action.

The default configuration of the FTP-Server proxy action blocks these commands:

ABOR*	HELP*	PASS*	REST*	STAT*	USER*
APPE*	LIST*	PASV*	RETR*	STOR*	XCUP*
CDUP*	MKD*	PORT*	RMD*	STOU*	XCWD*
CWD*	NLST*	PWD*	RNFR*	SYST*	XMKD*
DELE*	NOOP*	QUIT*	RNTO*	TYPE*	XRMD*

Use the FTP-Client proxy action to put limits on commands that users protected by the XTM device can use when they connect to external FTP servers. The default configuration of the FTP-Client is to allow all FTP commands.

You can add, delete, or modify rules. You usually should not block these commands, because they are necessary for the FTP protocol to work correctly.

Protocol Command	Client Command	Description
USER	n/a	Sent with login name
PASS	n/a	Sent with password
PASV	pasv	Select passive mode for data transfer
SYST	syst	Print the server's operating system and version. FTP clients use this information to correctly interpret and show a display of server responses.

To add, delete, or modify rules:

1. In the **Edit Proxy Action** page, select the **Commands** category.
2. *Add, Change, or Delete Rules*.
3. If you want to change settings for one or more other categories in this proxy, go to the topic for the next category you want to modify.
4. If you are finished with your changes to this proxy definition, click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

FTP-Proxy: Content

You can control the type of files that the FTP-proxy allows for downloads and uploads. For example, because many hackers use executable files to deploy viruses or worms on a computer, you could deny requests for *.exe files. Or, if you do not want to let users upload Windows Media files to an FTP server, you could add *.wma to the proxy definition and specify that these files are denied. Use the asterisk (*) as a wildcard character.

Use the FTP-Server proxy action to control rules for an FTP server protected by the XTM device. Use the FTP-Client proxy action to set rules for users connecting to external FTP servers.

1. On the **Edit Proxy Action** page, select the **Upload** or **Download** category.
2. *Add, Change, or Delete Rules*.
3. If you want uploaded files to be scanned for viruses by Gateway AntiVirus, from the **Action** drop-down list, select **AV Scan** for one or more rules.
4. To change settings for one or more other categories in this proxy, see the topics on the categories you want to modify.
5. When you are finished with your changes to this proxy action definition, click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

FTP-Proxy: Proxy and AV Alarms

You can configure how the FTP-proxy sends messages for alarm and antivirus events that occur through the FTP-proxy. You can define the proxy to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email message to a network administrator or a pop-up window on the management computer.

1. On the **Edit Proxy Action** page, select the **Proxy Alarm** category.
   The Proxy Alarm settings appear.

2. Configure the notification settings for the FTP-proxy action.
   For more information, see *Set Logging and Notification Preferences* on page 466.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

About the H.323-ALG

If you use Voice-over-IP (VoIP) in your organization, you can add an H.323 or SIP (Session Initiation Protocol) ALG (Application Layer Gateway) to open the ports necessary to enable VoIP through your XTM device. An ALG is created in the same way as a proxy policy and offers similar configuration options. These ALGs have been created to work in a NAT environment to maintain security for privately addressed conferencing equipment protected by your XTM device.

H.323 is commonly used on videoconferencing equipment. SIP is commonly used with IP phones. You can use both H.323 and SIP ALGs at the same time, if necessary. To determine which ALG to add, consult the documentation for your VoIP devices or applications.

VoIP Components

It is important to understand that you usually implement VoIP by using either:

Peer-to-peer connections

In a peer-to-peer connection, each of the two devices knows the IP address of the other device and connects to the other directly, without the use of a proxy server to route their calls. If both peers are behind the XTM device, the XTM device can route the call traffic correctly.

Hosted connections

Connections hosted by a call management system (PBX)

With H.323, the key component of call management is known as a *gatekeeper*. A gatekeeper manages VoIP calls for a group of users, and can be located on a network protected by your XTM device or at an external location. For example, some VoIP providers host a gatekeeper on their network that you must connect to before you can place a VoIP call. Other solutions require you to set up and maintain a gatekeeper on your network.

Coordinating the many components of a VoIP installation can be difficult. We recommend you make sure that VoIP connections work successfully before you add a H.323 or SIP ALG. This can help you to troubleshoot any problems.

ALG Functions

When you enable an H.323-ALG, your XTM device:

- Automatically responds to VoIP applications and opens the appropriate ports
- Makes sure that VoIP connections use standard H.323 protocols
- Generates log messages for auditing purposes

Many VoIP devices and servers use NAT (Network Address Translation) to open and close ports automatically. The H.323 and SIP ALGs also perform this function. You must disable NAT on your VoIP devices if you configure an H.323 or SIP ALG.

To change the ALG definition, you can use the **Policy Configuration** page. This page has three tabs: **Policy**, **Properties**, and **Advanced**.

For more information on how to add a proxy to your configuration, see *Add a Proxy Policy to Your Configuration* on page 316.

Action Settings

At the top of the **Policy Configuration** page, you can set these actions:

- **Application Control Action** — If Application Control is enabled on your device, specify the application control action to use for this policy. For more information, see *Enable Application Control in a Policy*.
- **Proxy action** — Select the proxy action to use for this policy. For information about proxy actions, see *About Proxy Actions* on page 317.

Policy Tab

- **Connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**and define who appears in the **From** and **To** list (on the **Policy** tab of the ALG definition).
  For more information, see *Set Access Rules for a Policy* on page 307.
- **Use policy-based routing** — If you want to use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 309.
- You can also configure static NAT or configure server load balancing.
  For more information, see *Configure Static NAT* on page 160 and *Configure Server Load Balancing* on page 163.

Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, configure the settings in the **Logging** section. For more information, see *Set Logging and Notification Preferences* on page 466.
- If you set the **Connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use H.323. For more information, see *Block Sites Temporarily with Policy Settings* on page 452.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

Advanced Tab

You can also configure these options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

Configure the Proxy Action

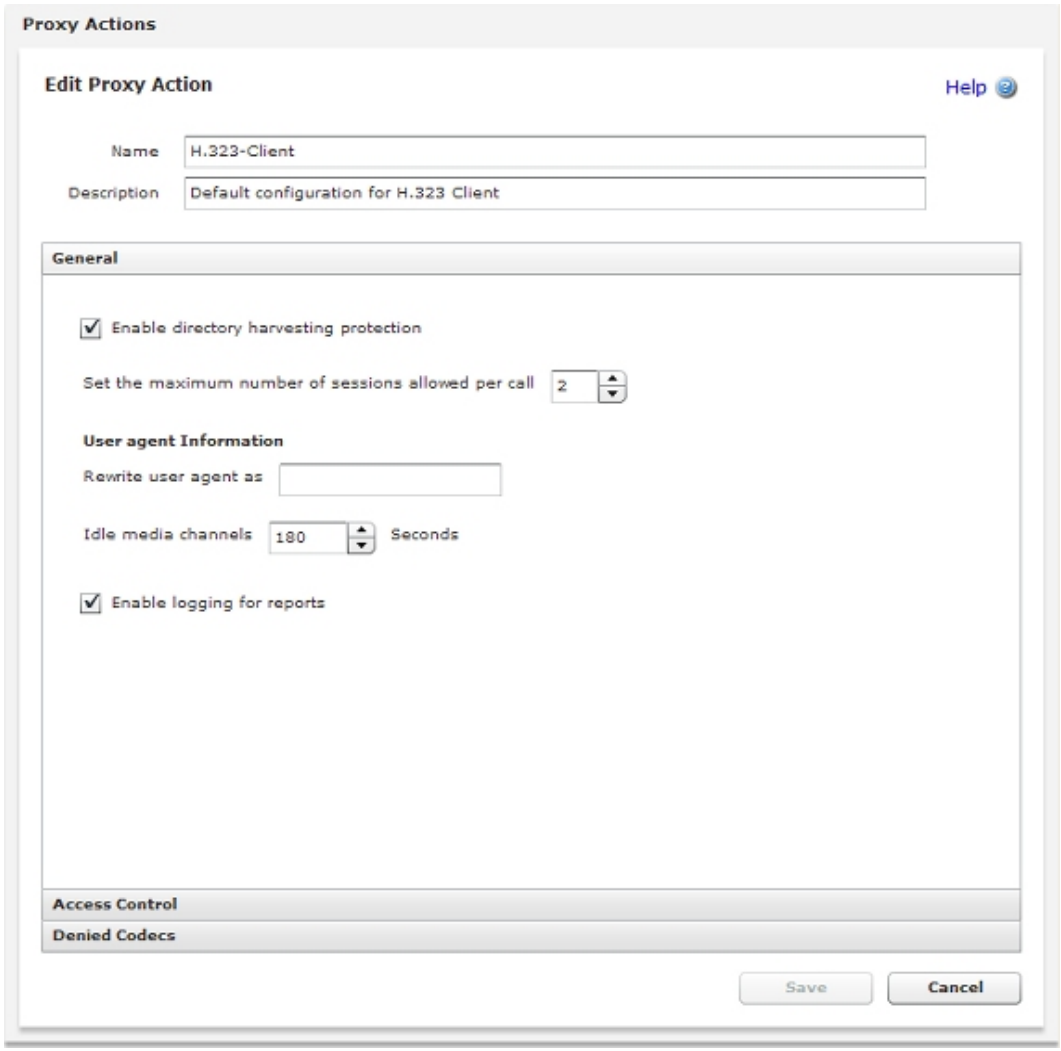
You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 317.

For the H.323-ALG, you can configure these categories of settings for a proxy action:

- *H.323-ALG: General Settings*
- *H.323-ALG: Access Control*
- *H.323 ALG: Denied Codecs*

H.323-ALG: General Settings

On the **Edit Proxy Action** page for an H.323-ALG proxy action, in the **General** section, you can set security and performance options for the H.323-ALG (Application Layer Gateway).



Enable directory harvesting protection

Select this check box to prevent attackers from stealing user information from VoIP gatekeepers protected by your XTM device. This option is enabled by default.

Set the maximum number of sessions allowed per call

Use this feature to restrict the maximum number of audio or video sessions that can be created with a single VoIP call. For example, If you set the number of maximum sessions to one and participate in a VoIP call with both audio and video, the second connection is dropped. The default value is two sessions, and the maximum value is four sessions. The XTM device creates a log entry when it denies a media session above this number.

User agent information

To have outgoing H.323 traffic identify as a client you specify, in the **Rewrite user agent as** text box, type a new user agent string. To remove the false user agent, clear the text box.

Idle media channels

When no data is sent for a specified amount of time on a VoIP audio, video, or data channel, your XTM device closes that network connection. The default value is 180 seconds (three minutes) and the maximum value is 3600 seconds (sixty minutes).

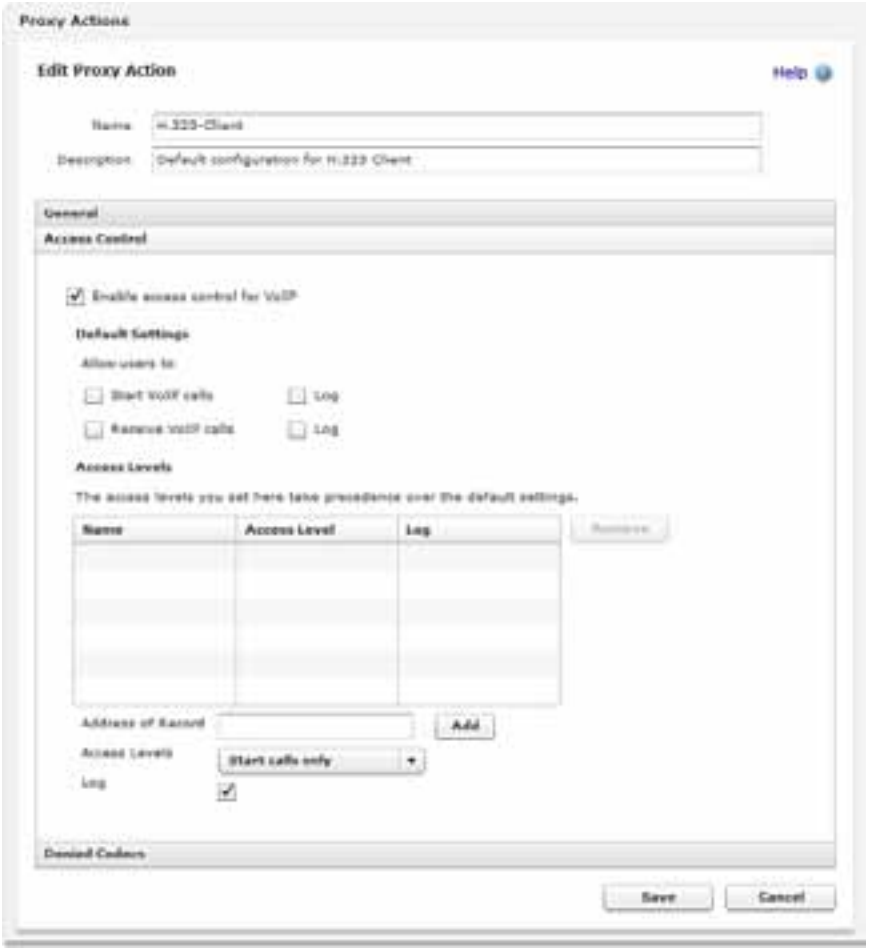
To specify a different time interval, in the **Idle media channels** text box, type the amount in seconds.

Enable logging for reports

To send a log message for each connection request managed by the H.323-ALG, select this check box. This option is necessary to create accurate reports on H.323 traffic.

H.323-ALG: Access Control

On the **Edit Proxy Action** page for an H.323-ALG proxy action, in the **General** section, you can create a list of users who are allowed to send VoIP network traffic.



Enable access control for VoIP

Select this check box to enable the access control feature. When enabled, the H.323-ALG allows or restricts calls based on the options you set.

Default Settings

To enable all VoIP users to start calls by default, select the **Start VoIP calls** check box.

To enable all VoIP users to receive calls by default, select the **Receive VoIP calls** check box.

To create a log message for each H.323 VoIP connection started or received, select the adjacent **Log** check box.

Access Levels

To create an exception to the default settings you specified, type the **Address of Record** (the address that shows up in the TO and FROM headers of the packet) for the exception. This is usually an H.323 address in the format *user@domain*, such as `myuser@example.com`.

From the **Access Levels** drop-down list, select an access level and click **Add**.

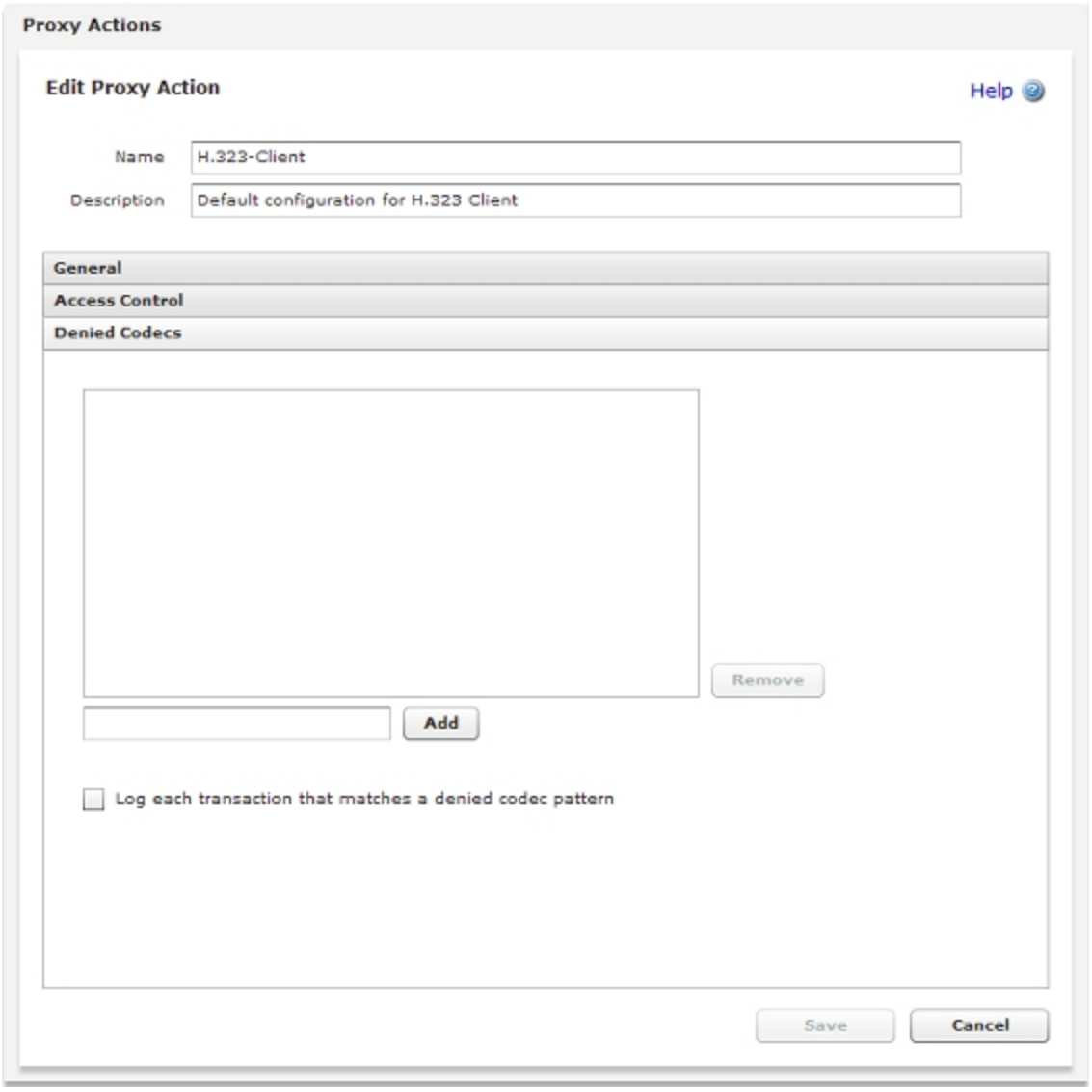
You can allow users to **Start calls only**, **Receive calls only**, **Start and receive calls**, or give them **No VoIP access**. These settings apply only to H.323 VoIP traffic.

To delete an exception, select it in the list and click **Remove**.

Connections made by users who have an access level exception are logged by default. If you do not want to log connections made by a user with an access level exception, clear the **Log** check box adjacent to the exception name in the list.

H.323 ALG: Denied Codecs

On the **Edit Proxy Action** page for an H.323 ALG proxy action, in the **Denied Codecs** section, you can set the VoIP voice, video, and data transmission codecs that you want to deny on your network.



Denied Codecs list

Use this feature to deny one or more VoIP codecs. When an H.323 VoIP connection is opened that uses a codec specified in this list, your XTM device closes the connection automatically. This list is empty by default. We recommend that you add a codec to this list if it consumes too much bandwidth, presents a security risk, or if it is necessary to have your VoIP solution operate correctly. For example, you may choose to deny the G.711 or G.726 codecs because they use more than 32 Kb/sec of bandwidth, or you may choose to deny the Speex codec because it is used by an unauthorized VOIP codec.

To add a codec to the list, type the codec name or unique text pattern in the text box and click **Add**. Do not use wildcard characters or regular expression syntax. The codec patterns are case sensitive.

To delete a codec from the list, select it and click **Remove**.

Log each transaction that matches a denied codec pattern

To send a log message when your XTM device denies H.323 traffic that matches a codec in this list, select this option.

About the HTTP-Proxy

Hyper Text Transfer Protocol (HTTP) is a request/response protocol between clients and servers. The HTTP client is usually a web browser. The HTTP server is a remote resource that stores HTML files, images, and other content. When the HTTP client starts a request, it establishes a TCP (Transmission Control Protocol) connection on Port 80. An HTTP server listens for requests on Port 80. When it receives the request from the client, the server replies with the requested file, an error message, or some other information.

The HTTP-proxy is a high-performance content filter. It examines Web traffic to identify suspicious content that can be a virus or other type of intrusion. It can also protect your HTTP server from attacks.

With an HTTP-proxy filter, you can:

- Adjust timeout and length limits of HTTP requests and responses to prevent poor network performance, as well as several attacks.
- Customize the deny message that users see when they try to connect to a web site blocked by the HTTP-proxy.
- Filter web content MIME types.
- Block specified path patterns and URLs.
- Deny cookies from specified web sites.

You can also use the HTTP-proxy with the WebBlocker security subscription. For more information, see *About WebBlocker* on page 669.

To enable your users to downloads Windows updates through the HTTP-proxy, you must change your HTTP-proxy settings. For more information, see *Enable Windows Updates Through the HTTP-Proxy*.

The TCP/UDP proxy is available for protocols on non-standard ports. When HTTP uses a port other than Port 80, the TCP/UDP proxy sends the traffic to the HTTP-proxy. For more information on the TCP/UDP proxy, see *About the TCP-UDP-Proxy* on page 422.

To add the HTTP-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 316.

If you must change the proxy definition, you can use the **New/Edit Proxy Policies** page to modify the definition. This page has three tabs: **Policy**, **Properties**, and **Advanced**.

You can also configure subscription service settings for the HTTP-proxy. For more information, see:

- *Get Started with WebBlocker*
- *Configure the Gateway AntiVirus Service*
- *Configure Gateway AntiVirus Actions*
- *Configure Reputation Enabled Defense*
- *Configure Application Control for Policies*

Action Settings

At the top of the **Policy Configuration** page, you can set these actions:

- **Application Control Action** — If Application Control is enabled on your device, specify the application control action to use for this policy. For more information, see *Enable Application Control in a Policy*.
- **Proxy action** — Select the proxy action to use for this policy. For information about proxy actions, see *About Proxy Actions* on page 317.

Policy Tab

- **Connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and select the users, computers, or networks that appear in the **From** and **To** list (on the **Policy** tab of the proxy definition). For more information, see *Set Access Rules for a Policy* on page 307.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 309.
- You can also configure static NAT or configure server load balancing.
  For more information, see *Configure Static NAT* on page 160 and *Configure Server Load Balancing* on page 163.

Properties Tab

- To define the logging settings for the policy, configure the settings in the **Logging** section. For more information, see *Set Logging and Notification Preferences* on page 466.
- If you set the **Connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block devices that try to connect on port 80.
  For more information, see *Block Sites Temporarily with Policy Settings* on page 452.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

Advanced Tab

You can also configure these options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

Configure the Proxy Action

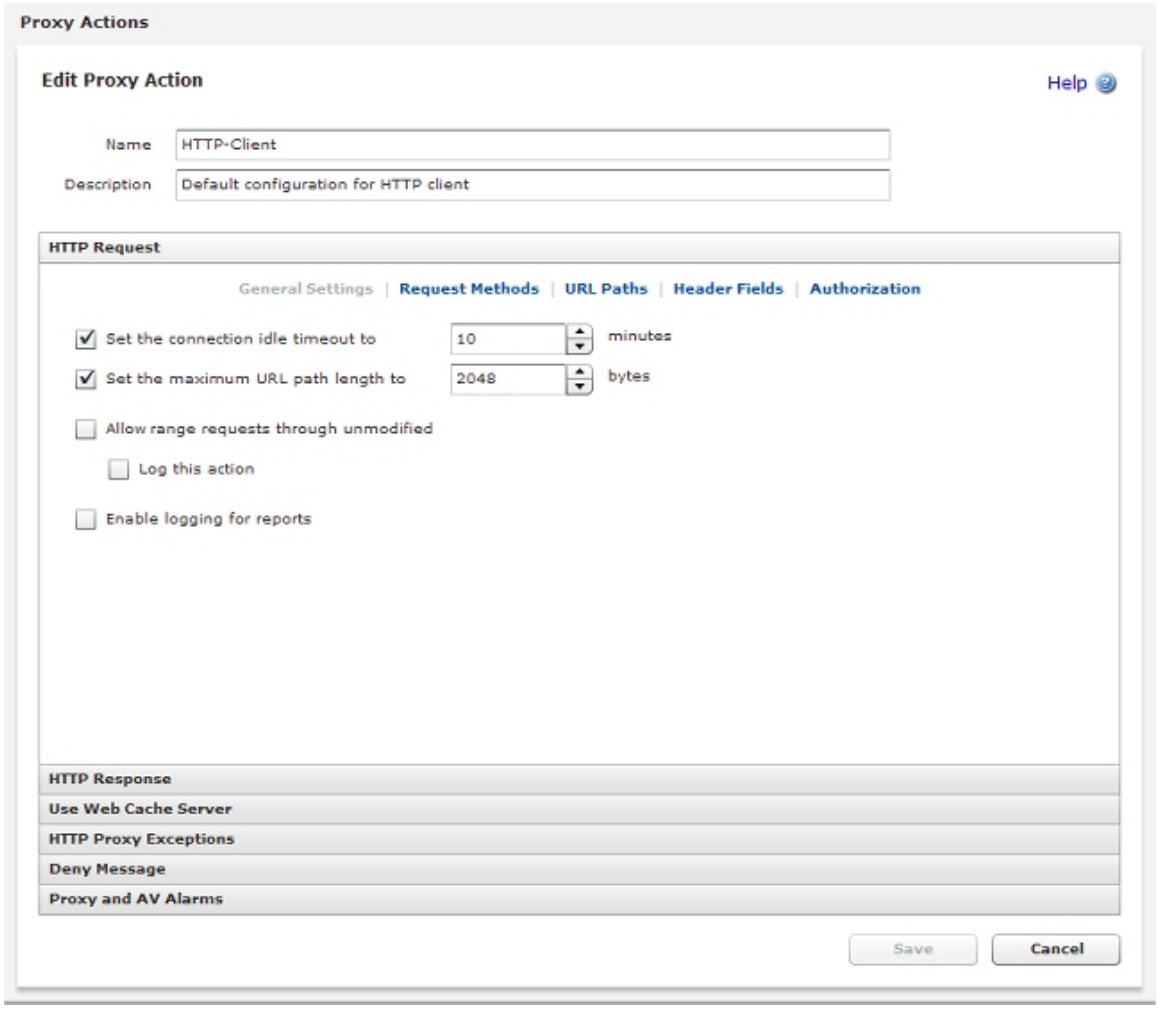
You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 317.

For the HTTP-proxy, you can configure these categories of settings for a proxy action:

- *HTTP Request: General Settings* on page 359
- *HTTP Request: Request Methods* on page 361
- *HTTP Request: URL Paths* on page 363
- *HTTP Request: Header Fields* on page 363
- *HTTP Request: Authorization* on page 364
- *HTTP Response: General Settings* on page 365
- *HTTP Response: Header Fields* on page 366
- *HTTP Response: Content Types* on page 367
- *HTTP Response: Cookies* on page 369
- *HTTP Response: Body Content Types* on page 369
- *Use a Caching Proxy Server* on page 375
- *HTTP-Proxy: Exceptions* on page 370
- *HTTP-Proxy: Deny Message* on page 372
- *HTTP-Proxy: Proxy and AV Alarms* on page 373

HTTP Request: General Settings

On the **Edit Proxy Action** page for an HTTP-proxy action, in the **General Settings** section, you can set basic HTTP parameters such as idle time out and URL length.



Idle Timeout

This option controls performance.

To close the TCP socket for the HTTP when no packets have passed through the TCP socket in the amount of time you specify, select the **Set the connection idle timeout to** check box. In the adjacent text box, type or select the number of minutes before the proxy times out.

Because every open TCP session uses a small amount of memory on the XTM device, and browsers and servers do not always close HTTP sessions cleanly, we recommend that you keep this check box selected. This makes sure that stale TCP connections are closed and helps the XTM device save memory. You can lower the timeout to five minutes and not reduce performance standards.

URL Path Length

To set the maximum number of characters allowed in a URL, select the **Set the maximum URL path link to** check box.

In this area of the proxy, *URL* includes anything in the web address after the top-level-domain. This includes the slash character but not the host name (*www.myexample.com* or *myexample.com*). For example, the URL www.myexample.com/products counts nine characters toward this limit because /products has nine characters.

The default value of 2048 is usually enough for any URL requested by a computer behind your XTM device. A URL that is very long can indicate an attempt to compromise a web server. The minimum length is 15 bytes. We recommend that you keep this setting enabled with the default settings. This helps protect against infected web clients on the networks that the HTTP-proxy protects.

Range Requests

To allow range requests through the XTM device, select this check box. Range requests allow a client to request subsets of the bytes in a web resource instead of the full content. For example, if you want only some sections of a large Adobe file but not the whole file, the download occurs more quickly and prevents the download of unnecessary pages if you can request only what you need.

Range requests introduce security risks. Malicious content can hide anywhere in a file and a range request makes it possible for any content to be split across range boundaries. The proxy can fail to see a pattern it is looking for when the file spans two GET operations. If you have a subscription for Gateway AntiVirus (Gateway AV) or the signature-based Intrusion Prevention Service (IPS), and you enable either of those subscription services, Fireware denies range requests regardless of whether this check box is selected.

We recommend that you do not select this check box if the rules you make in the Body Content Types section of the proxy are designed to identify byte signatures deep in a file, instead of just in the file header.

To add a traffic log message when the proxy takes the action indicated in the check box for range requests, select the **Log this action** check box.

Enable logging for reports

To create a traffic log message for each transaction, select this check box. This option creates a large log file, but this information is very important if your firewall is attacked. If you do not select this check box, you do not see detailed information about HTTP-proxy connections in reports.

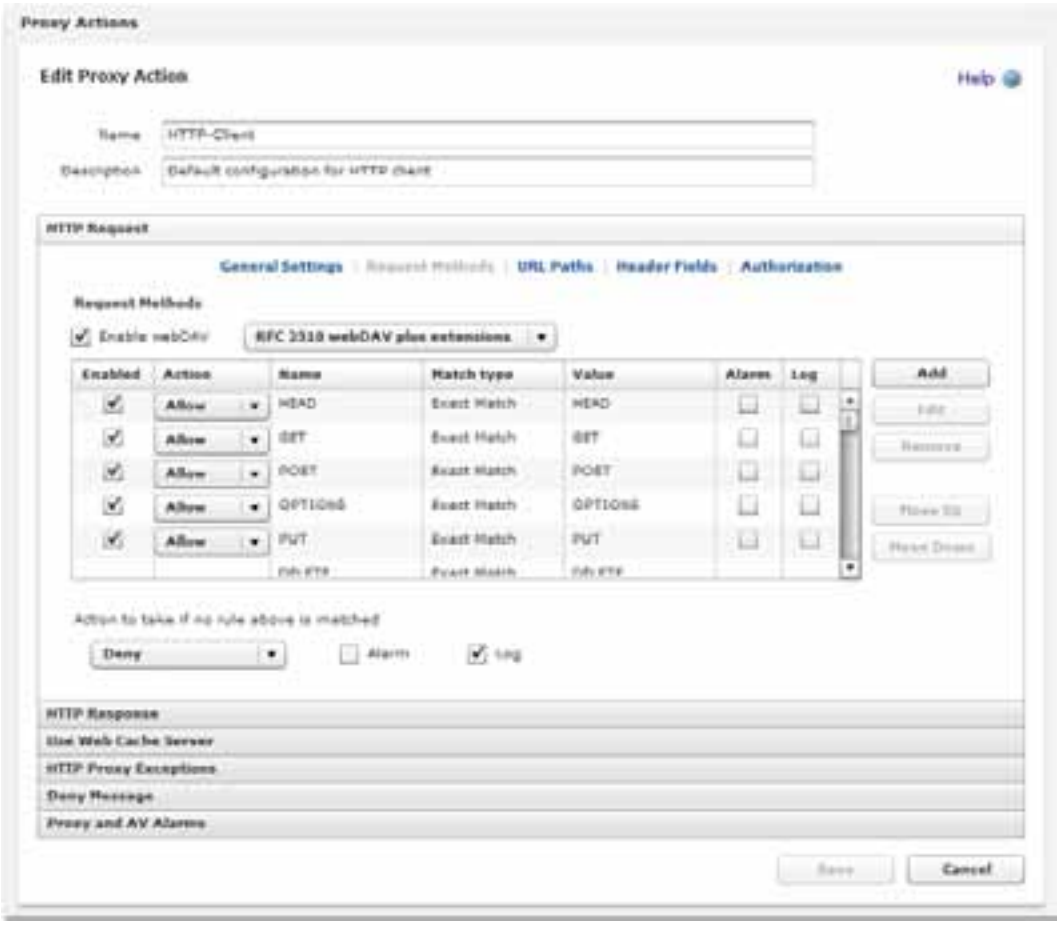
HTTP Request: Request Methods

Most browser HTTP requests are in one of two categories: GET or POST operations. Browsers usually use GET operations to download objects such as a graphic, HTML data, or Flash data. More than one GET is usually sent by a client computer for each page, because web pages usually contain many different elements. The elements are put together to make a page that appears as one page to the end user.

Browsers usually use POST operations to send data to a web site. Many web pages get information from the end user such as location, email address, and name. If you disable the POST command, the XTM device denies all POST operations to web servers on the external network. This feature can prevent your users from sending information to a web site on the external network.

Web-based Distributed Authoring and Versioning (webDAV) is a set of HTTP extensions that allows users to edit and manage files on remote web servers. WebDAV is compatible with Outlook Web Access (OWA). If webDAV extensions are not enabled, the HTTP proxy supports these request methods: HEAD, GET, POST, OPTIONS, PUT, and DELETE. For HTTP-Server, the proxy supports these request methods by default: HEAD, GET, and POST. The proxy also includes these options (disabled by default): OPTIONS, PUT, and DELETE.

1. On the **Edit Proxy Action** page, select the **HTTP Request** category.
   The HTTP Request panel expands.
2. In the link bar, select **Request Methods** .
   The Request Methods settings appear.



3. To enable your users to use these extensions, select the **Enable webDAV** check box.
   Many extensions to the base webDAV protocol are also available. If you enable webDAV, from the adjacent check box, select whether you want to enable only the extensions described in RFC 2518 or if you want to include an additional set of extensions to maximize interoperability.
4. *Add, Change, or Delete Rules*.
5. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
6. Click Save.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTP Request: URL Paths

A URL (Uniform Resource Locator) identifies a resource on a remote server and gives the network location on that server. The URL path is the string of information that comes after the top level domain name. You can use the HTTP-proxy to block web sites that contain specified text in the URL path. You can add, delete, or modify URL path patterns. Here are examples of how to block content with HTTP request URL paths:

- To block all pages that have the host name www.test.com, type the pattern: `www.test.com*`
- To block all paths containing the word *sex*, on all web sites: `*sex*`
- To block URL paths ending in **.test*, on all web sites: `*.test`

> ***Note*** *If you filter URLs with the HTTP request URL path ruleset, you must configure a complex pattern that uses full regular expression syntax from the advanced view of a ruleset. It is easier and gives better results to filter based on header or body content type than it is to filter by URL path.*

To block web sites with specific text in the URL path:

1. On the **Edit Proxy Action** page, select the **HTTP Request** category.
   The HTTP Request panel expands.
2. In the link bar, select **URL paths**.
   The URL Paths settings appear.
3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTP Request: Header Fields

This ruleset supplies content filtering for the full HTTP header. By default, the HTTP proxy uses exact matching rules to strip *Via* and *From* headers, and allows all other headers. This ruleset matches the full header, not only the name.

To match all values of a header, type the pattern: “[header name]:*”. To match only some values of a header, replace the asterisk (*) wildcard with a pattern. If your pattern does not start with an asterisk (*) wildcard, include one space between the colon and the pattern when you type in the **Pattern** text box. For example, type: `[header name]: [pattern]`, not `[header name]:[pattern]`.

The default rules do not strip the *Referer* header, but do include a disabled rule to strip this header. To enable the rule to strip the header, select **Change View**. Some web browsers and software applications must use the Referer header to operate correctly.

1. On the **Edit Proxy Action** page, select the **HTTP Request** category.
   The HTTP Request category expands.

2. In the link bar, select **Header Fields**.
   The Header Fields settings appear.
3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTP Request: Authorization

This rule sets the criteria for content filtering of HTTP Request Header authorization fields. When a web server starts a *WWW-Authenticate* challenge, it sends information about which authentication methods it can use. The proxy puts limits on the type of authentication sent in a request. It uses only the authentication methods that the web server accepts. With a default configuration, the XTM device allows Basic, Digest, NTLM, and Passport1.4 authentication, and strips all other authentication. You can add, delete, or modify rules in the default ruleset.

1. On the **Edit Proxy Action** page, select the **HTTP Request** category.
   The HTTP Request category expands.
2. In the link bar, select **Authorization**.
   The Authorization settings appear.
3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

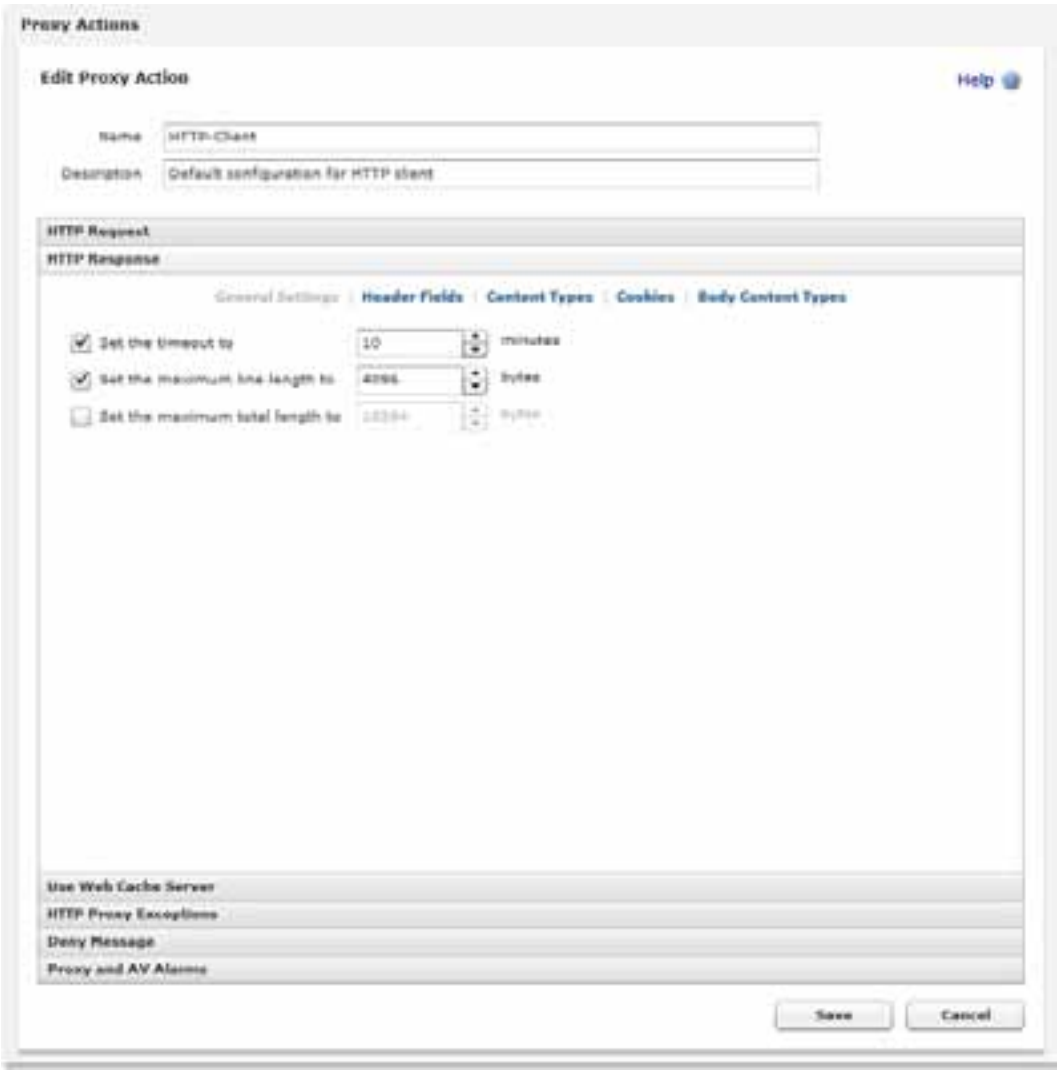
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTP Response: General Settings

On the **General Settings** page, you can configure basic HTTP parameters such as idle time out, and limits for line and total length.

1. On the **Edit Proxy Action** page, select the **HTTP Response** category.
   The HTTP Response category expands.
2. In the link bar, select **General Settings**.
   The General Settings page appears.



3. To set limits for HTTP parameters, select the applicable check boxes. Type or select a value for the limits.

   Set the timeout to

   Controls how long the XTM device HTTP proxy waits for the web server to send the web page. When a user clicks a hyperlink or types a URL in a web browser, it sends an HTTP request to a remote server to get the content. In most browsers, a message similar to *Contacting site...*, appears in the status bar. If the remote server does not respond, the HTTP client continues to send the request until it receives an answer or until the request times out. During this time, the HTTP proxy continues to monitor the connection and uses valuable network resources.

   Set the maximum line length to

   Controls the maximum allowed length of a line of characters in HTTP response headers. Use this property to protect your computers from buffer overflow exploits. Because URLs for many commerce sites continue to increase in length over time, you may need to adjust this value in the future.

   Set the maximum total length to

   Controls the maximum length of HTTP response headers. If the total header length is more than this limit, the HTTP response is denied.

4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTP Response: Header Fields

This ruleset controls which HTTP response header fields the XTM device allows. You can add, delete, or modify rules. Many of the HTTP response headers that are allowed in the default configuration are described in RFC 2616. For more information, see http://www.ietf.org/rfc/rfc2616.txt.

1. On the **Edit Proxy Action** page, select the **HTTP Response** category.
   The HTTP Response category expands.
2. In the link bar, select **Header Fields**.
   The Header Fields settings appear.
3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTP Response: Content Types

When a web server sends HTTP traffic, it usually adds a MIME type, or content type, to the packet header that shows what kind of content is in the packet. The HTTP header on the data stream contains this MIME type. It is added before the data is sent.

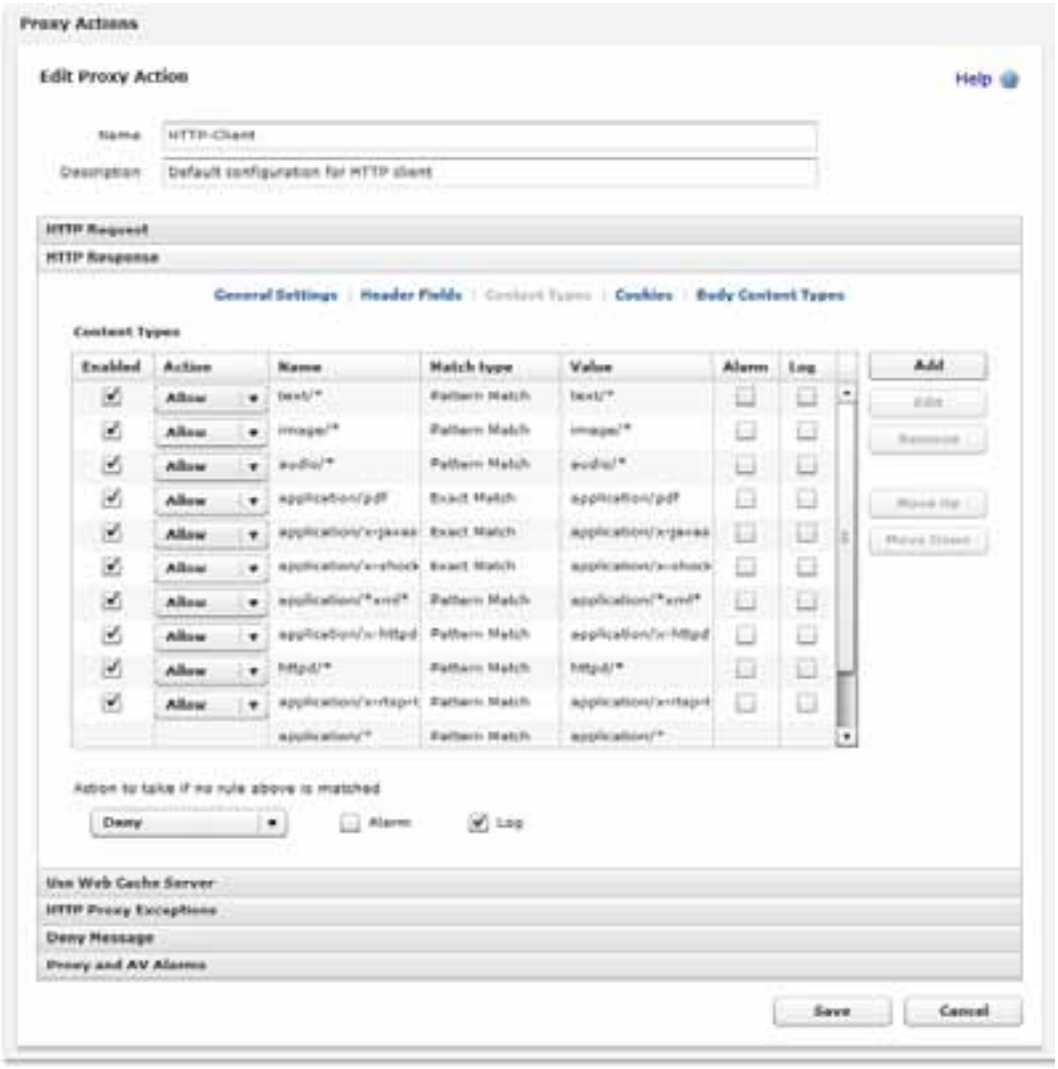
Certain kinds of content that users request from web sites can be a security threat to your network. Other kinds of content can decrease the productivity of your users. By default, the XTM device allows some safe content types, and denies MIME content that has no specified content type. The HTTP proxy includes a list of commonly used content types that you can add to the ruleset. You can also add, delete, or modify the definitions.

The format of a MIME type is **type/subtype**. For example, if you wanted to allow JPEG images, you would add `image/jpg` to the proxy definition. You can also use the asterisk (*) as a wildcard. To allow any image format, you add `image/*`.

For a list of current, registered MIME types, see http://www.iana.org/assignments/media-types.

Add, Delete, or Modify Content Types

1. On the **Edit Proxy Action** page, select the **HTTP Request** category.
   The HTTP Response panel expands.
2. In the link bar, select **Content Types**.
   The Content Types settings appear.



3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

Allow Web Sites with a Missing Content Type

By default, the XTM device denies MIME content that has no specified content type. In most cases, we recommend that you keep this default setting. Sites that do not supply legitimate MIME types in their HTTP responses do not follow RFC recommendations and could pose a security risk. However, some organizations need their employees to get access to web sites that do not have a specified content type.

You must make sure that you change the proxy action used by the correct policy or policies. You can apply the change to any policy that uses an HTTP client proxy action. This could be an HTTP-proxy policy, the Outgoing policy (which also applies an HTTP client proxy action), or the TCP-UDP policy.

To allow web sites with a missing content type:

1. In the **Content Types** list, select the **Enabled** check box adjacent to the **Allow (none)** rule.
2. Click **Save**.

HTTP Response: Cookies

HTTP cookies are small files of alphanumeric text that web servers put on web clients. Cookies monitor the page a web client is on, to enable the web server to send more pages in the correct sequence. Web servers also use cookies to collect information about an end user. Many web sites use cookies for authentication and other legitimate functions, and cannot operate correctly without cookies.

The HTTP proxy gives you control of the cookies in HTTP responses. You can configure rules to strip cookies, based on your network requirements. The default rule for the HTTP-Server and HTTP-Client proxy action allows all cookies. You can add, delete, or modify rules.

The proxy looks for packets based on the domain associated with the cookie. The domain can be specified in the cookie. If the cookie does not contain a domain, the proxy uses the host name in the first request. For example, to block all cookies for nosy-adware-site.com, use the pattern: `*.nosy-adware-site.com`. If you want to deny cookies from all subdomains on a web site, use the wildcard symbol (*) before and after the domain. For example, `*example.com*` blocks all subdomains of example.com, such as images.example.com and mail.example.com.

Change Settings for Cookies

1. On the **Edit Proxy Action** page, select the **HTTP Request** category.
   The HTTP Response panel expands.
2. In the link bar, select **Cookies**.
   The Cookies settings appear.
3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTP Response: Body Content Types

This ruleset gives you control of the content in an HTTP response. The XTM device is configured to deny Java bytecodes, Zip archives, Windows EXE/DLL files, and Windows CAB files. The default proxy action for outgoing HTTP requests (HTTP-Client) allows all other response body content types. You can add, delete, or modify rules. We recommend that you examine the file types that are used in your organization and allow only those file types that are necessary for your network.

1. On the **Edit Proxy Action** page, select the **HTTP Response** category.
   The HTTP Response panel expands.
2. In the link bar, select **Body Content Types**.
   The Body Content Types settings appear.
3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTP-Proxy: Exceptions

For certain web sites, you can use HTTP-proxy exceptions to bypass HTTP-proxy rules, but not bypass the proxy framework. Traffic that matches HTTP-proxy exceptions still goes through the standard proxy handling used by the HTTP-proxy. However, when a match occurs, some proxy settings are not included.

Excluded Proxy Settings

These settings are not included:

- HTTP request — range requests, URL path length, all request methods, all URL paths, request headers, authorization pattern matching
- HTTP response — response headers, content types, cookies, body content types

Request headers and response headers are parsed by the HTTP-proxy even when the traffic matches the HTTP-proxy exception. If a parsing error does not occur, all headers are allowed. Also, antivirus scanning, IPS scanning, and WebBlocker are not applied to traffic that matches an HTTP-proxy exception.

Included Proxy Settings

These settings are included:

- HTTP request — Idle timeout
- HTTP response — Idle timeout, maximum line length limit, maximum total length limit

All transfer-encoding parsing is still applied to allow the proxy to determine the encoding type. The HTTP-proxy denies all invalid or malformed transfer encoding.

Define Exceptions

You can add host names or patterns as HTTP-proxy exceptions. For example, if you block all web sites that end in *.test* but want to allow your users to go to the site www.example.test, you can add *www.example.test* as an HTTP-proxy exception.

When you define exceptions, you specify the IP address or domain name of sites to allow. The domain (or host) name is the part of a URL that ends with .com, .net, .org, .biz, .gov, or .edu. Domain names can also end in a country code, such as .de (Germany) or .jp (Japan).

To add a domain name, type the URL pattern without the leading "http://". For example, to allow your users to go to the Example web site http://www.example.com, type `www.example.com`. If you want to allow all subdomains that contain *example.com*, you can use the asterisk (*) as a wildcard character. For example, to allow users to go to *www.example.com*, and *support.example.com* type `*.example.com`.

1. On the **Edit Proxy Action** page, select the **HTTP Proxy Exceptions** category.
   The HTTP Proxy Exceptions settings appear.
2. In the text box, type the host name or host name pattern. Click **Add**.
3. Repeat this process to add more exceptions.
4. To add a traffic log message each time the HTTP-proxy takes an action on a proxy exception, select the **Log each transaction that matches an HTTP proxy exception** check box.
5. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
6. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTP-Proxy: Deny Message

When content is denied, the XTM device sends a default deny message that replaces the denied content. You can change the text of that deny message. You can customize the deny message with standard HTML. You can also use Unicode (UTF-8) characters in the deny message. The first line of the deny message is a component of the HTTP header. You must include an empty line between the first line and the body of the message.

You get a deny message in your web browser from the XTM device when you make a request that the HTTP-proxy does not allow. You also get a deny message when your request is allowed, but the HTTP-proxy denies the response from the remote web server. For example, if a user tries to download an *.exe* file and you have blocked that file type, the user sees a deny message in the web browser. If the user tries to download a web page that has an unknown content type and the proxy policy is configured to block unknown MIME types, the user sees an error message in the web browser.

The default deny message appears in the **Deny Message** text box. To change this to a custom message, use these variables:

%(transaction)%

Select *Request* or *Response* to show which side of the transaction caused the packet to be denied.

%(reason)%

Includes the reason the XTM device denied the content.

%(method)%

Includes the request method from the denied request.

%(url-host)%

Includes the server host name from the denied URL. If no host name was included, the IP address of the server is included.

%(url-path)%

Includes the path component of the denied URL.

To configure the Deny Message:

1. On the **Edit Proxy Action** page, select the **Deny Message** category.
   The Deny Message panel expands.
2. In the **Deny Message** text box, type the deny message.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

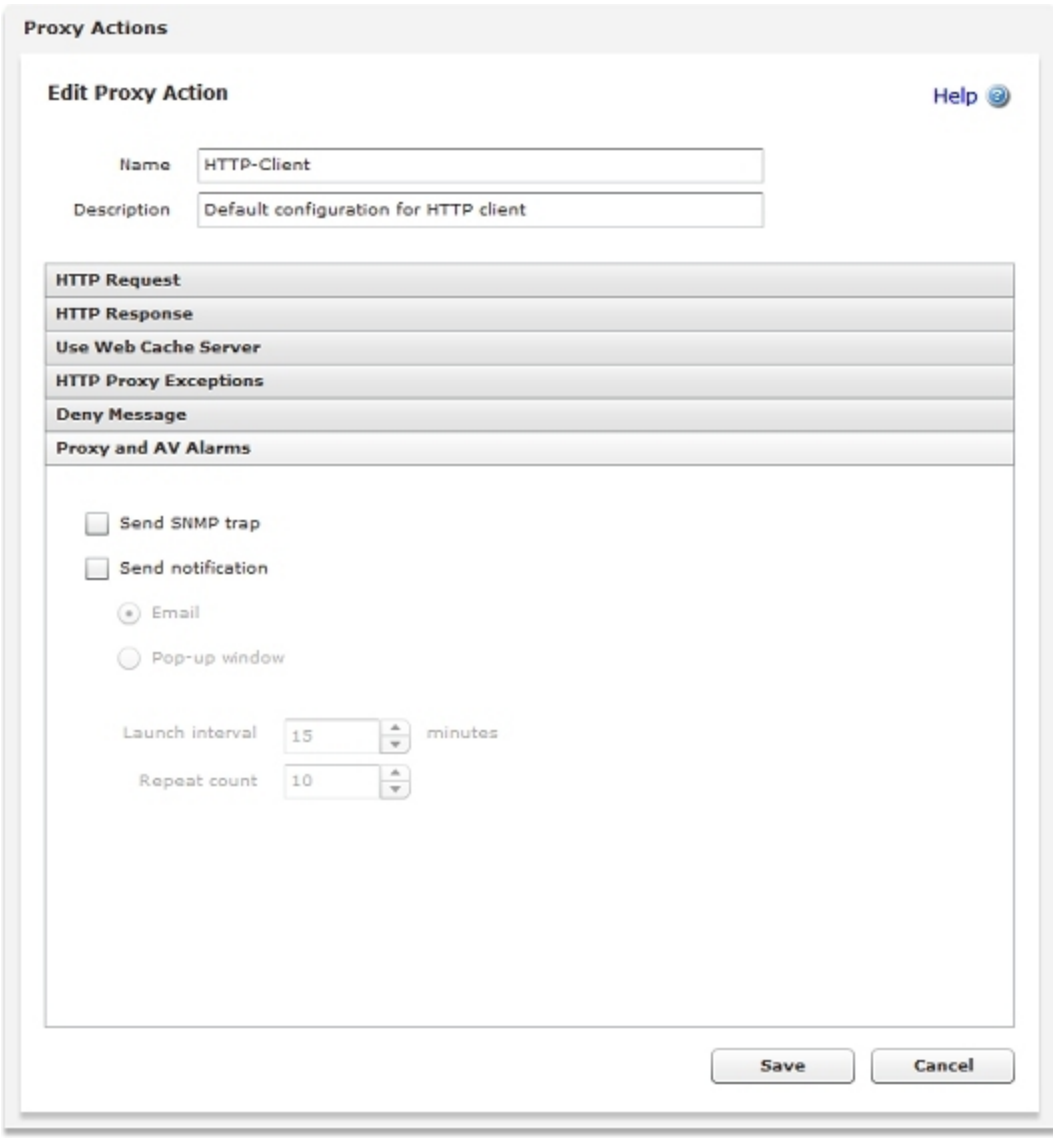
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTP-Proxy: Proxy and AV Alarms

You can configure how the HTTP-proxy sends messages for alarm and antivirus events that occur through the HTTP-proxy. You can define the proxy to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email message to a network administrator or a pop-up window on the management computer.

1. On the **Edit Proxy Action** page, select the **Proxy Alarm** category.
   The Proxy Alarm settings appear.



2. Configure the notification settings for the HTTP-proxy action.
   For more information, see *Set Logging and Notification Preferences* on page 466.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

Enable Windows Updates Through the HTTP-Proxy

Windows Update servers identify the content they deliver to a computer as a generic binary stream (such as octet stream), which is blocked by the default HTTP proxy rules. To allow Windows updates through the HTTP-proxy, you must edit your HTTP-Client proxy ruleset to add HTTP-proxy exceptions for the Windows Update servers.

1. Make sure that your XTM device allows outgoing connections on port 443 and port 80. These are the ports that computers use to contact the Windows Update servers.
2. On the **Edit Proxy Action** page, select the **HTTP Proxy Exceptions** category.
3. In the text box, type or paste each of these domains, and click **Add** after each one:
   ```
   windowsupdate.microsoft.com
   download.windowsupdate.com
   update.microsoft.com
   download.microsoft.com
   ntservicepack.microsoft.com
   wustat.windows.com
   v4.windowsupdate.microsoft.com
   v5.windowsupdate.microsoft.com
   ```
4. Click **Save**.

If You Still Cannot Download Windows Updates

If you have more than one HTTP-proxy policy, make sure that you add the HTTP exceptions to the correct policy and proxy action.

Microsoft does not limit updates to only these domains. Examine your logs for denied traffic to a Microsoft-owned domain. Look for any traffic denied by the HTTP-proxy. The log line should include the domain. Add any new Microsoft domain to the HTTP-proxy exceptions list, and then run Windows Update again.

Use a Caching Proxy Server

Because your users can look at the same web sites frequently, a caching proxy server increases the traffic speed and decreases the traffic volume on the external Internet connections. Although the HTTP-proxy on the XTM device does not cache content, you can use a caching proxy server with the HTTP proxy. All XTM device proxy and WebBlocker rules continue to have the same effect.

The XTM device connection with a proxy server is the same as with a client. The XTM device changes the GET function to: GET / HTTP/1.1 to GET www.mydomain.com / HTTP/1.1 and sends it to a caching proxy server. The proxy server moves this function to the web server in the GET function.

Use an External Caching Proxy Server

To set up your HTTP-proxy to work with an external caching proxy server:

1. Configure a proxy server, such as Microsoft Proxy Server 2.0.
2. Select **Firewall > Proxy Actions**.
3. Select the **HTTP-Client** proxy action used by your HTTP-proxy policy. Click **Edit**.
4. On the **Edit Proxy Action** page, select the **Use Web Cache Server** category.
   The Use Web Cache Server page appears.
5. Select the **Use external caching proxy server for HTTP traffic** check box.
6. Type the **IP address** and **Port** for the external caching proxy server.
7. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
8. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

Use an Internal Caching Proxy Server

You can also use an internal caching proxy server with your XTM device.

To use an internal caching proxy server:

1. Configure the HTTP-proxy action with the same settings as for an external proxy server.
2. In the same HTTP-proxy policy, allow all traffic from the users on your network whose web requests you want to route through the caching proxy server.
3. Add an HTTP packet filter policy to your configuration.
4. Configure the HTTP packet filter policy to allow traffic from the IP address of your caching proxy server to the Internet.
5. If necessary, manually move this policy up in your policy list so that it has a higher precedence than your HTTP-proxy policy.

About the HTTPS-Proxy

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a request/response protocol between clients and servers used for secure communications and transactions. You can use the HTTPS-proxy to secure a web server protected by your XTM device, or to examine HTTPS traffic requested by clients on your network. By default, when an HTTPS client starts a request, it establishes a TCP (Transmission Control Protocol) connection on port 443. Most HTTPS servers listen for requests on port 443.

HTTPS is more secure than HTTP because HTTPS uses a digital certificate to encrypt and decrypt user page requests as well as the pages that are returned by the web server. Because HTTPS traffic is encrypted, the XTM device must decrypt it before it can be examined. After it examines the content, the XTM device encrypts the traffic with a certificate and sends it to the intended destination.

You can export the default certificate created by the XTM device for this feature, or import a certificate for the XTM device to use instead. If you use the HTTPS-proxy to examine web traffic requested by users on your network, we recommend that you export the default certificate and distribute it to each user so that they do not receive browser warnings about untrusted certificates. If you use the HTTPS-proxy to secure a web server that accepts requests from an external network, we recommend that you import the existing web server certificate for the same reason.

When an HTTPS client or server uses a port other than port 443 in your organization, you can use the TCP/UDP proxy to relay the traffic to the HTTPS-proxy. For information on the TCP/UDP proxy, see *About the TCP-UDP-Proxy* on page 422.

To add the HTTPS-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 316.

If you must change the proxy definition, you can use the **Policy Configuration page** to modify the definition. This page has three tabs: **Policy**, **Properties**, and **Advanced**.

Action Settings

At the top of the **Policy Configuration** page, you can set these actions:

- **Application Control Action** — If Application Control is enabled on your device, specify the application control action to use for this policy. For more information, see *Enable Application Control in a Policy*.
- **Proxy action** — Select the proxy action to use for this policy. For information about proxy actions, see *About Proxy Actions* on page 317.

You can also configure WebBlocker service actions for the HTTPS proxy. For more information, see *Get Started with WebBlocker*

Policy Tab

- **Connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**. Define who appears in the **From** and **To** lists.
  For more information, see *Set Access Rules for a Policy* on page 307.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 309.

- You can also configure static NAT or configure server load balancing.
  For more information, see *Configure Static NAT* on page 160 and *Configure Server Load Balancing* on page 163.

Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, configure the settings in the **Logging** section. For more information, see *Set Logging and Notification Preferences* on page 466.
- If you set the **Connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use HTTPS. For more information, see *Block Sites Temporarily with Policy Settings* on page 452.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

Advanced Tab

You can use several other options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

Configure the Proxy Action

You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 317.

For the HTTPS-proxy, you can configure these categories of settings for a proxy action:

- *HTTPS-Proxy: General Settings*
- *HTTPS-Proxy: Content Inspection*
- *HTTPS-Proxy: Certificate Names*
- *HTTPS-Proxy: Proxy Alarm*

HTTPS-Proxy: General Settings

On the **Edit Proxy Action** page, in the **General** section, you can configure basic HTTPS parameters such as ,connection timeout, and logging.

Connection Timeout

Configure these settings to specify how long the HTTPS proxy waits for the web client to make a request from the external web server after it starts a TCP/IP connection, or after an earlier request for the same connection. If the time period exceeds this setting, the HTTPS proxy closes the connection.

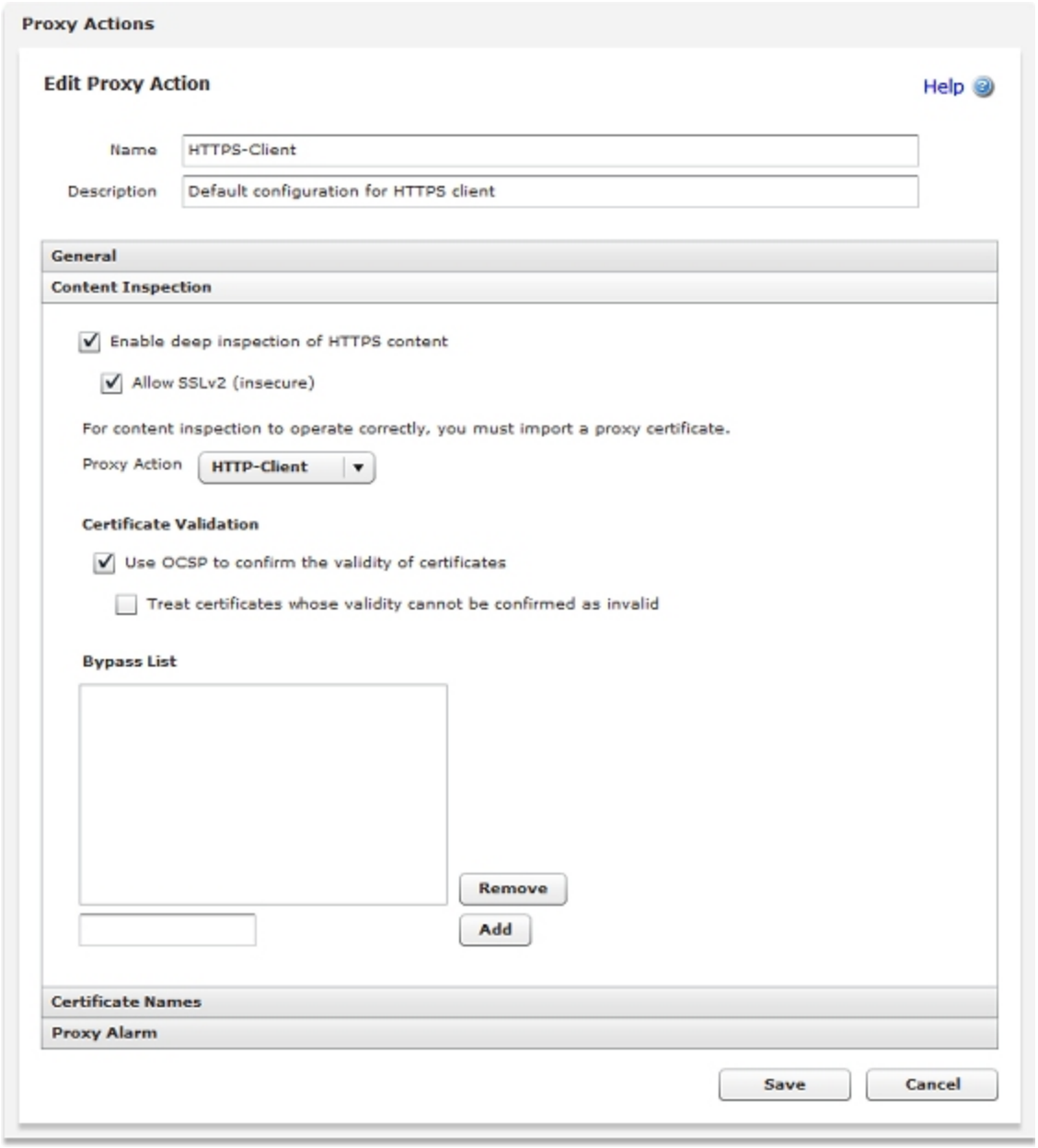
To enable this feature, select the **Connection timeout** check box. In the adjacent text box, type or select the number of minutes before the proxy times out.

Enable logging for reports

To create a traffic log message for each transaction, select this check box. This option increases the size of your log file, but this information is very important if your firewall is attacked. If you do not select this check box, you do not see detailed information about HTTPS proxy connections in reports.

HTTPS-Proxy: Content Inspection

You can enable and configure deep inspection of HTTPS content on the HTTPS-Proxy Action Configuration **Content Inspection** section.



Enable deep inspection of HTTPS content

When this check box is selected, the XTM device decrypts HTTPS traffic, examines the content, and encrypts the traffic again with a new certificate. The content is examined by the HTTP-proxy policy that you choose on this page.

Note *If you have other traffic that uses the HTTPS port, such as SSL VPN traffic, we recommend that you evaluate this option carefully. The HTTPS-proxy attempts to examine all traffic on TCP port 443 in the same way. To ensure that other traffic sources operate correctly, we recommend that you add those sources to the* ***Bypass List****. See the subsequent section for more information.*

By default, the certificate used to encrypt the traffic is generated automatically by the XTM device. You can also upload your own certificate to use for this purpose. If the original web site or your web server has a self-signed or invalid certificate, or if the certificate was signed by a CA the XTM device does not recognize, clients are presented with a browser certificate warning. Certificates that cannot be properly re-signed appear to be issued by *Fireware HTTPS-proxy: Unrecognized Certificate* or simply *Invalid Certificate*.

We recommend that you import the certificate you use, as well as any other certificates necessary for the client to trust that certificate, on each client device. When a client does not automatically trust the certificate used for the content inspection feature, the user sees a warning in their browser, and services like Windows Update do not operate correctly.

Some third-party programs store private copies of necessary certificates and do not use the operating system certificate store, or transmit other types of data over TCP port 443. These programs include:

- Communications software, such as AOL Instant Messenger and Google Voice
- Remote desktop and presentation software, including LiveMeeting and WebEx
- Financial and business software, such as ADP, iVantage, FedEx, and UPS

If these programs do not have a method to import trusted CA certificates, they do not operate correctly when content inspection is enabled. Contact your software vendor for more information about certificate use or technical support, or add the IP addresses of computers that use this software to the Bypass list.

For more information, see *About Certificates* on page 491 or *Use Certificates for the HTTPS-Proxy* on page 505.

Enable SSLv2 (insecure)

SSLv3, SSLv2, and TLSv1 are protocols used for HTTPS connections. SSLv2 is not as secure as SSLv3 and TLSv1. By default, the HTTPS-proxy only allows connections that negotiate the SSLv3 and TLSv1 protocols. If your users connect to client or server applications that only support SSLv2, you can allow the HTTPS-proxy to use the SSLv2 protocol for connections to these web sites.

To enable this option, select the **SSLv2 (insecure)** check box. This option is disabled by default.

Proxy Action

Select an HTTP-proxy policy for the XTM device to use when it inspects decrypted HTTPS content.

When you enable content inspection, the HTTP-proxy action WebBlocker settings override the HTTPS-proxy WebBlocker settings. If you add IP addresses to the bypass list for content inspection, traffic from those sites is filtered with the WebBlocker settings from the HTTPS-proxy.

For more information on WebBlocker configuration, see *About WebBlocker* on page 669.

Use OCSP to confirm the validity of certificates

Select this check box to have the XTM device automatically check for certificate revocations with OCSP (Online Certificate Status Protocol). When this feature is enabled, the XTM device uses information in the certificate to contact an OCSP server that keeps a record of the certicate status. If the OCSP server responds that the certificate has been revoked, the XTM device disables the certificate.

If you select this option, there can be a delay of several seconds as the XTM device requests a response from the OCSP server. The XTM device keeps between 300 and 3000 OCSP responses in a cache to improve performance for frequently visited web sites. The number of responses stored in the cache is determined by your XTM device model.

Treat certificates whose validity cannot be confirmed as invalid

When this option is selected and an OCSP responder does not send a response to a revocation status request, the XTM device considers the original certificate as invalid or revoked. This option can cause certificates to be considered invalid if there is a routing error or a problem with your network connection.

Bypass list

The XTM device does not inspect content sent to or from IP addresses on this list. To add a web site or hostname, type its IP address in the text box and click the **Add** button.

When you enable content inspection, the HTTP proxy action WebBlocker settings override the HTTPS proxy WebBlocker settings. If you add IP addresses to the bypass list for content inspection, traffic from those sites is filtered with the WebBlocker settings from the HTTPS-proxy.

For more information on WebBlocker configuration, see *About WebBlocker* on page 669.

HTTPS-Proxy: Certificate Names

Certificate names are used to filter content for an entire site. The XTM device allows or denies access to a site if the domain of an HTTPS certificate matches an entry in this list.

For example, if you want to deny traffic from any site in the *example.com* domain, add a Certificate Names rule with the pattern *.example.com and set the **If matched** action to **Deny**.

1. On the **Edit Proxy Action** page, select the **Certificate Names** category.
   The Certificate Names panel expands.
2. *Add, Change, or Delete Rules*.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click Save.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

HTTPS-Proxy: Proxy Alarm

You can configure how the HTTPS-proxy sends messages for alarm events that occur through the HTTPS-proxy. You can define the proxy to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email message to a network administrator or a pop-up window on the management computer.

1. On the **Edit Proxy Action** page, select the **Proxy Alarm** category.
   The Proxy Alarm settings appear.

2. Configure the notification settings for the HTTPS-proxy action.
   For more information, see *Set Logging and Notification Preferences* on page 466.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

About the POP3-Proxy

POP3 (Post Office Protocol v.3) is a protocol that moves email messages from an email server to an email client on a TCP connection over port 110. Most Internet-based email accounts use POP3. With POP3, an email client contacts the email server and checks for any new email messages. If it finds a new message, it downloads the email message to the local email client. After the message is received by the email client, the connection is closed.

With a POP3-proxy filter you can:

- Adjust timeout and line length limits to make sure the POP3-proxy does not use too many network resources, and to prevent some types of attacks.
- Customize the deny message that users see when an email sent to them is blocked.
- Filter content embedded in email with MIME types.
- Block specified path patterns and URLs.

To add the POP3-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 316.

If you must change the proxy definition, you can use the **Policy Configuration page** to modify the definition. This page has three tabs: **Policy**, **Properties**, and **Advanced**.

You can also configure subscription service settings for the POP3 proxy. For more information, see *Get Started with WebBlocker* and *Configure the Gateway AntiVirus Service*.

Action Settings

At the top of the **Policy Configuration** page, you can set these actions:

- **Application Control Action** — If Application Control is enabled on your device, specify the application control action to use for this policy. For more information, see *Enable Application Control in a Policy*.
- **Proxy action** — Select the proxy action to use for this policy. For information about proxy actions, see *About Proxy Actions* on page 317.

Policy Tab

- **Connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**. Define who appears in the **From** and **To** lists.
  For more information, see *Set Access Rules for a Policy* on page 307.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 309.
- You can also configure static NAT or configure server load balancing.
  For more information, see *Configure Static NAT* on page 160 and *Configure Server Load Balancing* on page 163.

Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, configure the settings in the **Logging** section. For more information, see *Set Logging and Notification Preferences* on page 466.
- If you set the **Connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use POP3.
  For more information, see *Block Sites Temporarily with Policy Settings* on page 452.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

Advanced Tab

You can use several other options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

Configure the Proxy Action

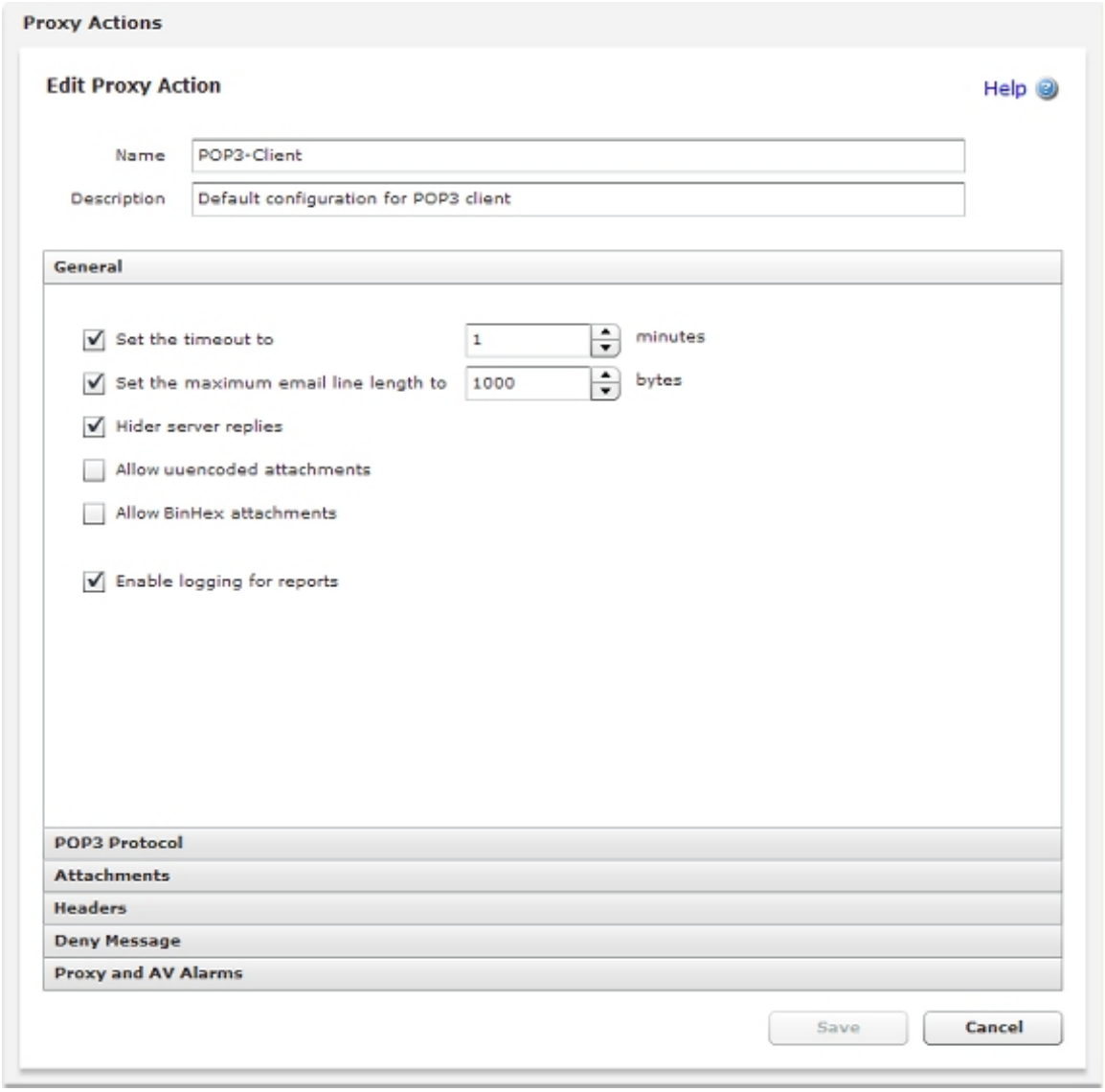
You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 317.

For the POP3-proxy, you can configure these categories of settings for a proxy action:

- *POP3-Proxy: General Settings*
- *POP3-Proxy: Authentication*
- *POP3-Proxy: Content Types*
- *POP3-Proxy: File Names*
- *POP3-Proxy: Headers*
- *POP3-Proxy: Deny Message*
- *POP3-Proxy: Proxy and AV Alarms*

POP3-Proxy: General Settings

In the **General** section of the **Edit Proxy Action** page for a POP3-proxy action, you can adjust time out and line length limits as well as other general parameters for the POP3-proxy.



Set the timeout to

To limit the number of minutes that the email client tries to open a connection to the email server before the connection is closed, select this check box. In the adjacent text box, type or select the number of minutes for the timeout value. This makes sure the proxy does not use too many network resources when the POP3 server is slow or cannot be reached.

Set the maximum email line length to

To prevent some types of buffer overflow attacks, select this check box. In the adjacent text box, type or select the limit of the line length. Very long line lengths can cause buffer overflows on some email systems. Most email clients and systems send relatively short lines, but some web-based email systems send very long lines. However, it is unlikely that you will need to change this setting unless it prevents access to legitimate mail.

Hide server replies

To replace the POP3 greeting strings in email messages, select this check box. These strings can be used by hackers to identify the POP3 server vendor and version.

Allow uuencoded attachments

To enable the POP3-proxy to allow uuencoded attachments in email messages, select this check box. Uuencode is an older program used to send binary files in ASCII text format over the Internet. UUencoded attachments can be security risks because they appear as ASCII text files, but can actually contain executable files.

Allow BinHex attachments

To enable the POP3-proxy to allow BinHex attachments in email messages, select this check box. BinHex, which is short for binary-to-hexadecimal, is a utility that converts a file from binary format to ASCII text format.

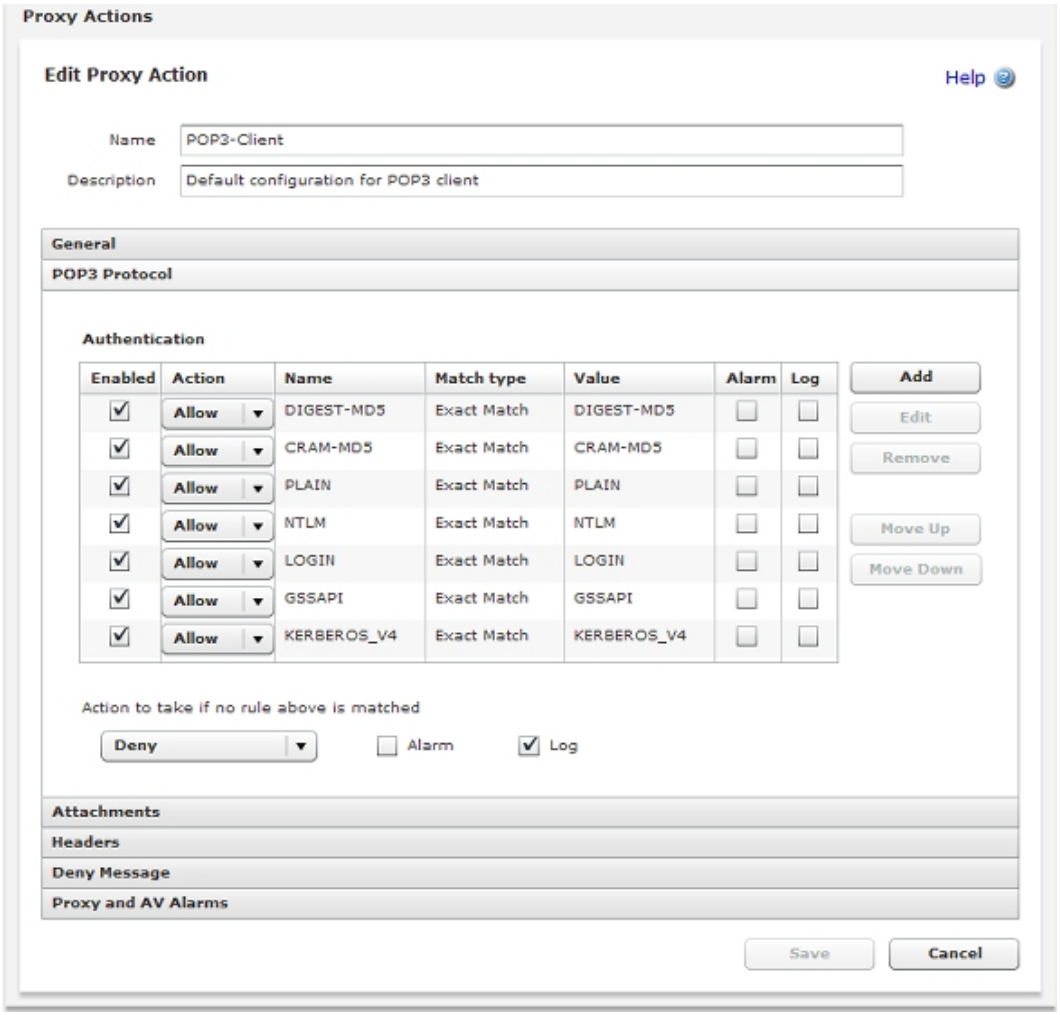
Enable logging for reports

To enable the POP3-proxy to send a log message for each POP3 connection request, select this check box. To use WatchGuard Reports to create reports of POP3 traffic, you must select this check box.

POP3-Proxy: Authentication

A POP3 client must authenticate to a POP3 server before they exchange information. You can set the types of authentication for the proxy to allow and the action to take for types that do not match the criteria. You can add, delete, or modify rules.

1. On the **Edit Proxy Action** page, select the **POP3 Protocol** category.
   The POP3 authentication rules appear.



2. *Add, Change, or Delete Rules*.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

POP3-Proxy: Content Types

The headers for email messages include a Content Type header to show the MIME type of the email and of any attachments. The content type or MIME type tells the computer the types of media the message contains. Certain kinds of content embedded in email can be a security threat to your network. Other kinds of content can decrease the productivity of your users.

You can enable the POP3-proxy to automatically detect the content type of an email message and any attachments. If you do not enable this option, the POP3-proxy uses the value stated in the email header, which clients sometimes set incorrectly. Because hackers often try to disguise executable files as other content types, we recommend that you enable content type auto detection to make your installation more secure.

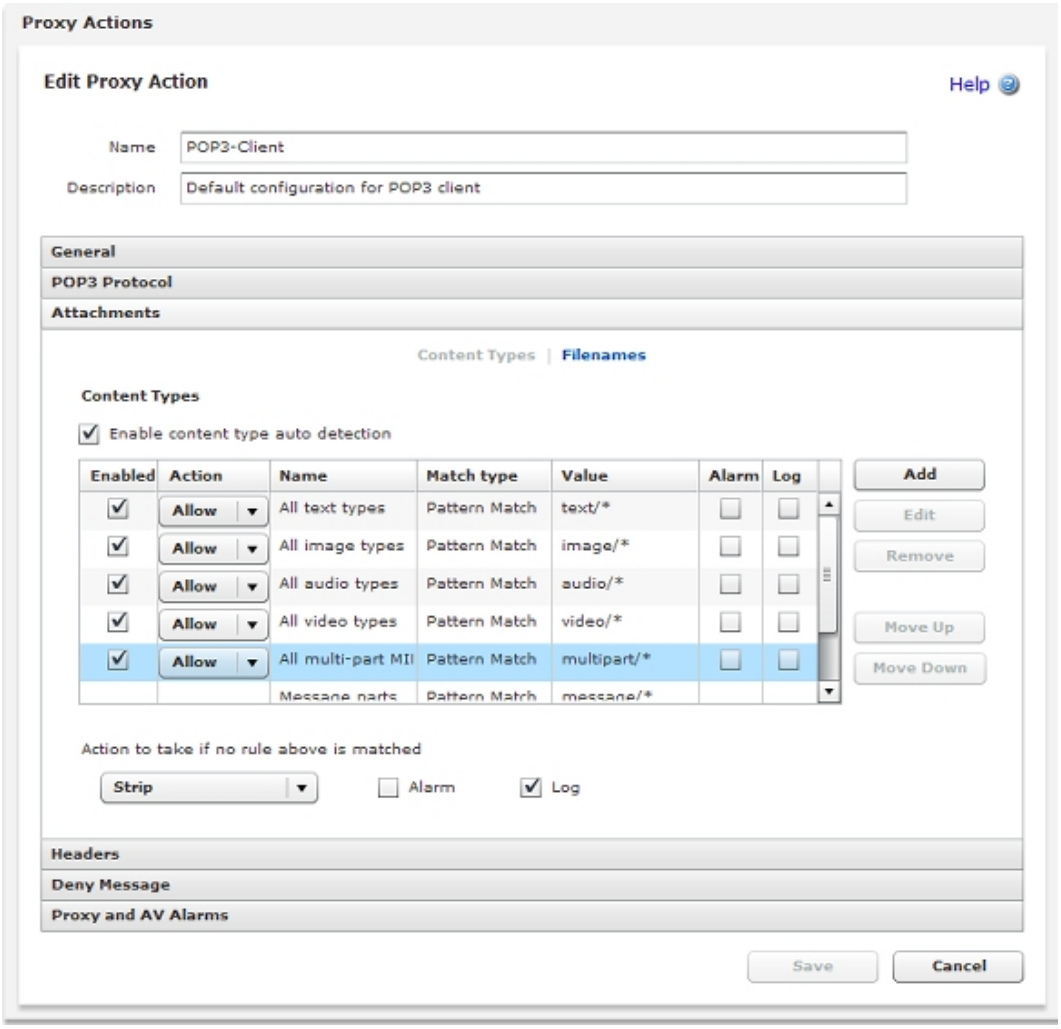
For example, a .pdf file attached to an email might have a content type stated as application/octet-stream. If you enable content type auto detection, the POP3-proxy recognizes the .pdf file and uses the actual content type, application/pdf. If the proxy does not recognize the content type after it examines the content, it uses the value stated in the email header, as it would if content type auto detection were not enabled.

You can add, delete, or modify rules. You can also set values for content filtering and the action to take for content types that do not match the criteria. For the POP3-Server proxy action, you set values for incoming content filtering. For the POP3-Client action, you set values for outgoing content filtering.

When you specify the MIME type, make sure to use the format type/subtype. For example, if you want to allow JPEG images, you add `image/jpg`. You can also use the asterisk (*) as a wildcard. To allow any image format, add `image/*` to the list.

To specify the content types for automatic detection:

1. On the **Edit Proxy Action** page, select the **Attachments** category.
   The Attachments category expands.
2. In the link bar, select **Content Types**.
   The Content Types page appears.



3. To enable the POP3 proxy to examine content and determine the content type, select the **Enable content type auto detection** check box.
   If you do not select this option, the POP3 proxy uses the value stated in the email header.
4. *Add, Change, or Delete Rules*.
5. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
6. Click **Save**.

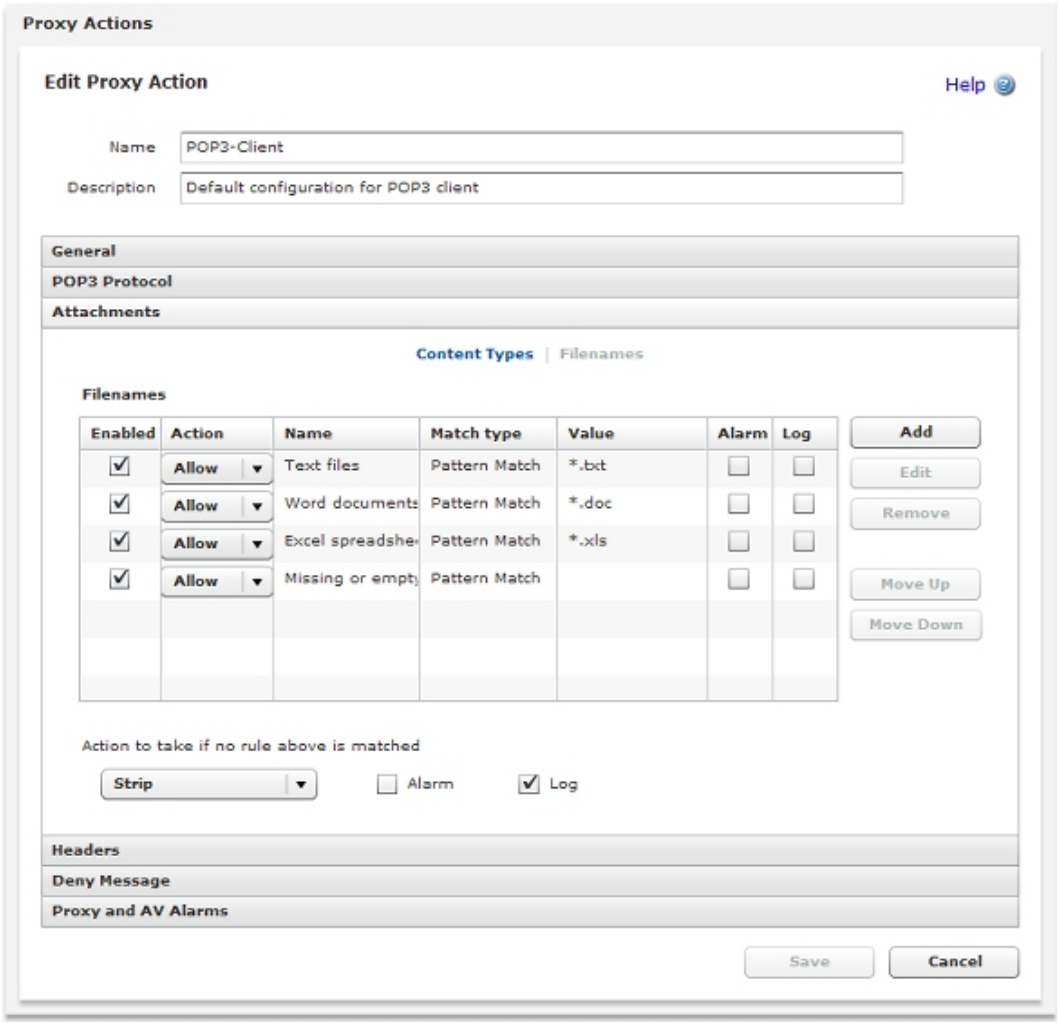
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

POP3-Proxy: File Names

You can use this ruleset in a POP3-Server proxy action to put limits on file names for incoming email attachments. Or, you can use the ruleset for the POP3-Client proxy action to put limits on file names for outgoing email attachments. You can add, delete, or modify rules.

1. On the **Edit Proxy Action** page, select the **Attachments** category.
   The Attachments category expands.
2. In the link bar, select **Filenames**.
   The Filenames page appears.



3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

POP3-Proxy: Headers

The POP3-proxy examines email headers to find patterns common to forged email messages, as well as those from legitimate senders. You can add, delete, or modify rules.

1. On the **Edit Proxy Action** page, select the **Headers** category.
   The Headers category expands.
2. *Add, Change, or Delete Rules*.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

POP3-Proxy: Deny Message

When content is denied, the XTM device sends a default *deny message* that replaces the denied content. This message appears in a recipients email message when the proxy blocks an email. You can change the text of that deny message. The first line of the deny message is a section of the HTTP header. You must include an empty line between the first line and the body of the message.

The default deny message appears in the **Deny Message** text box. To change this to a custom message, use these variables:

%(reason)%

Includes the reason the XTM device denied the content.

%(filename)%

Includes the file name of the denied content.

%(virus)%

Includes the name or status of a virus for Gateway AntiVirus users.

%(action)%

Includes the name of the action taken. For example: lock or strip.

%(recovery)%

Includes whether you can recover the attachment.

To configure the deny message:

1. On the **Edit Proxy Action** page, select the **Deny Message** category.
   The Deny Message category expands.

2. In the **Deny Message** text box, type a custom plain text message in standard HTML.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

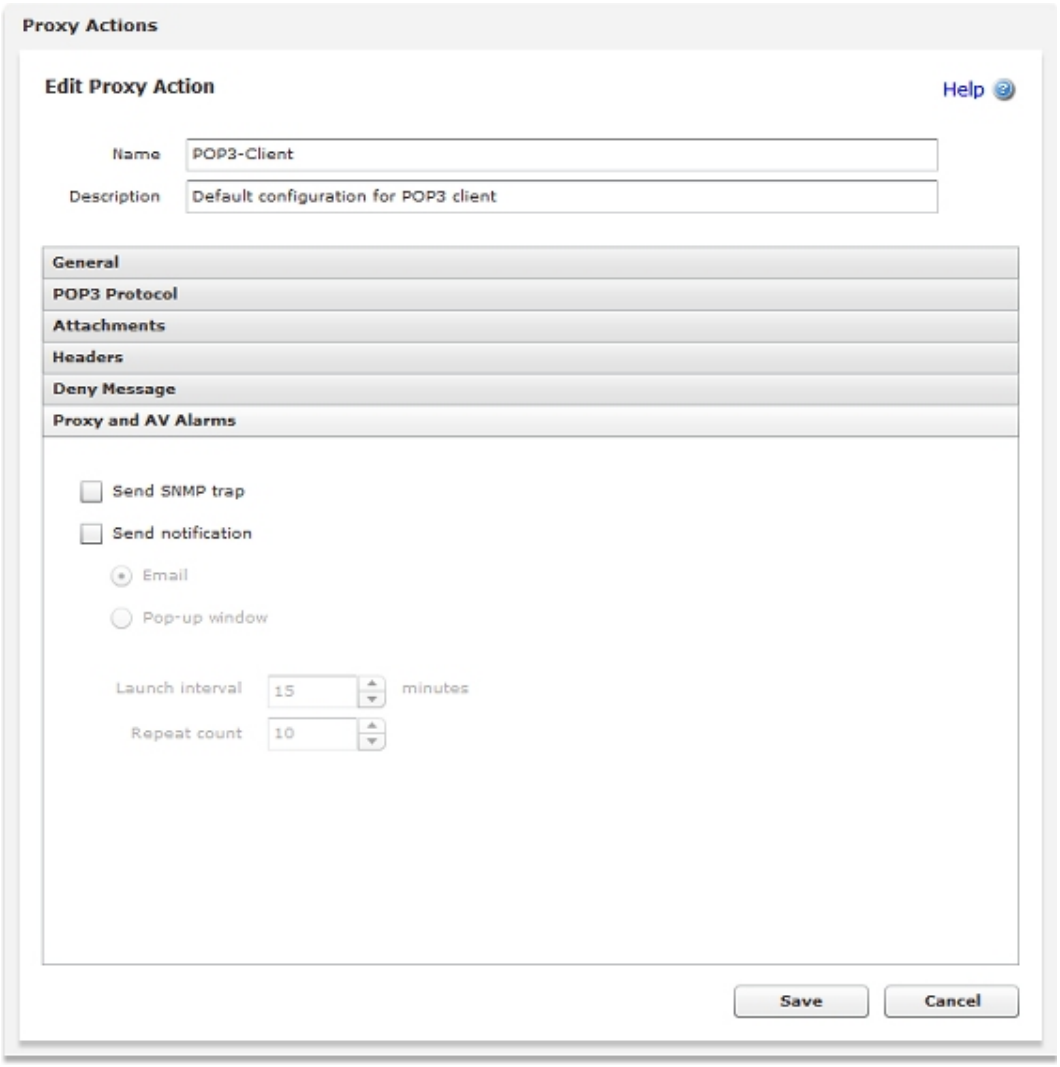
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

POP3-Proxy: Proxy and AV Alarms

You can configure how the POP3-proxy sends messages for alarm and antivirus events that occur through the POP3-proxy. You can define the proxy to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email message to a network administrator or a pop-up window on the management computer.

1. On the **Edit Proxy Action** page, select the **Proxy Alarm** category.
   The Proxy Alarm settings appear.



2. Configure the notification settings for the POP3-proxy action.
   For more information, see *Set Logging and Notification Preferences* on page 466.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

About the SIP-ALG

If you use Voice-over-IP (VoIP) in your organization, you can add a SIP (Session Initiation Protocol) or H.323 ALG (Application Layer Gateway) to open the ports necessary to enable VoIP through your XTM device. An ALG is created in the same way as a proxy policy and offers similar configuration options. These ALGs have been created to work in a NAT environment to maintain security for privately-addressed conferencing equipment behind the XTM device.

H.323 is commonly used on videoconferencing equipment. SIP is commonly used with IP phones. You can use both H.323 and SIP-ALGs at the same time, if necessary. To determine which ALG you need to add, consult the documentation for your VoIP devices or applications.

VoIP Components

It is important to understand that you usually implement VoIP with either:

Peer-to-peer connections

In a peer-to-peer connection, each of the two devices knows the IP address of the other device and connects to the other directly without the use of a proxy server to route their calls. If both peers are behind the XTM device, the XTM device can route the call traffic correctly.

Hosted connections

Connections hosted by a call management system (PBX)

In the SIP standard, two key components of call management are the *SIP Registrar* and the *SIP Proxy*. Together, these components manage connections hosted by the call management system. The WatchGuard SIP-ALG opens and closes the ports necessary for SIP to operate. The WatchGuard SIP-ALG supports SIP trunks. It can support both the SIP Registrar and the SIP Proxy when used with a call management system that is external to the XTM device.

It can be difficult to coordinate the many components of a VoIP installation. We recommend you make sure that VoIP connections work successfully before you add an H.323 or SIP-ALG. This can help you to troubleshoot any problems.

Instant Messaging Support

There are no configuration steps necessary to use instant messaging (IM) with the SIP-ALG. We support these types of IM:

- Page-based IM — Supported as part of the default SIP protocol.
- Session-based IM — Available through our support of MSRP (Messaging Session Relay Protocol) over TCP.

ALG Functions

When you enable a SIP-ALG, your XTM device:

- Automatically responds to VoIP applications and opens the appropriate ports
- Makes sure that VoIP connections use standard SIP protocols
- Generates log messages for auditing purposes
- Supports SIP presence through the use of the SIP *Publish* method. This allows softphone users to see peer status.

Many VoIP devices and servers use NAT (Network Address Translation) to open and close ports automatically. The H.323 and SIP-ALGs also perform this function. You must disable NAT on your VoIP devices if you configure an H.323 or SIP-ALG.

For instructions to add the SIP-ALG to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 316.

If you must change the proxy definition, you can use the **Policy Configuration page** to modify the definition. This page has three tabs: **Policy**, **Properties**, and **Advanced**.

Action Settings

At the top of the **Policy Configuration** page, you can set these actions:

- **Application Control Action** — If Application Control is enabled on your device, specify the application control action to use for this policy. For more information, see *Enable Application Control in a Policy*.
- **Proxy action** — Select the proxy action to use for this policy. For information about proxy actions, see *About Proxy Actions* on page 317.

Policy Tab

- **Connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**. Define who appears in the **From** and **To** lists.
  For more information, see *Set Access Rules for a Policy* on page 307.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 309.
- You can also configure static NAT or configure server load balancing.
  For more information, see *Configure Static NAT* on page 160 and *Configure Server Load Balancing* on page 163.

Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, configure the settings in the **Logging** section. For more information, see *Set Logging and Notification Preferences* on page 466.
- If you set the **Connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use SIP.
  For more information, see *Block Sites Temporarily with Policy Settings* on page 452.

- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

Advanced Tab

You can use several other options in your SIP-ALG definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

Configure the Proxy Action

You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 317.

For the SIP-ALG, you can configure these categories of settings for a proxy action:

- *SIP-ALG: General Settings*
- *SIP-ALG: Access Control*
- *SIP-ALG: Denied Codecs*

SIP-ALG: General Settings

In the **General** section of the **Edit Proxy Action** page for a SIP-ALG action, you can set security and performance options for the SIP-ALG (Application Layer Gateway).

Enable header normalization

To deny malformed or extremely long SIP headers, select this check box . While these headers often indicate an attack on your XTM device, you can disable this option if necessary for your VoIP solution to operate correctly.

Enable topology hiding

This feature rewrites SIP traffic headers to remove private network information, such as IP addresses. We recommend that you select this option unless you have an existing VoIP gateway device that performs topology hiding.

Enable directory harvesting protection

To prevent attackers from stealing user information from VoIP gatekeepers protected by your XTM device, select this check box. This option is enabled by default.

Maximum sessions

Use this feature to restrict the maximum number of audio or video sessions that can be created with a single VoIP call.

For example, if you set the number of maximum sessions to one and participate in a VoIP call with both audio and video, the second connection is dropped. The default value is two sessions and the maximum value is four sessions. The XTM device sends a log message when it denies a media session above this number.

User agent information

To identify outgoing H.323 traffic as a client you specify, type a new user agent string in the **Rewrite user agent as** text box.

To remove the false user agent, clear the text box.

Timeouts

When no data is sent for a specified amount of time on a VoIP audio, video, or data channel, your XTM device closes that network connection. The default value is 180 seconds (three minutes) and the maximum value is 600 seconds (ten minutes).

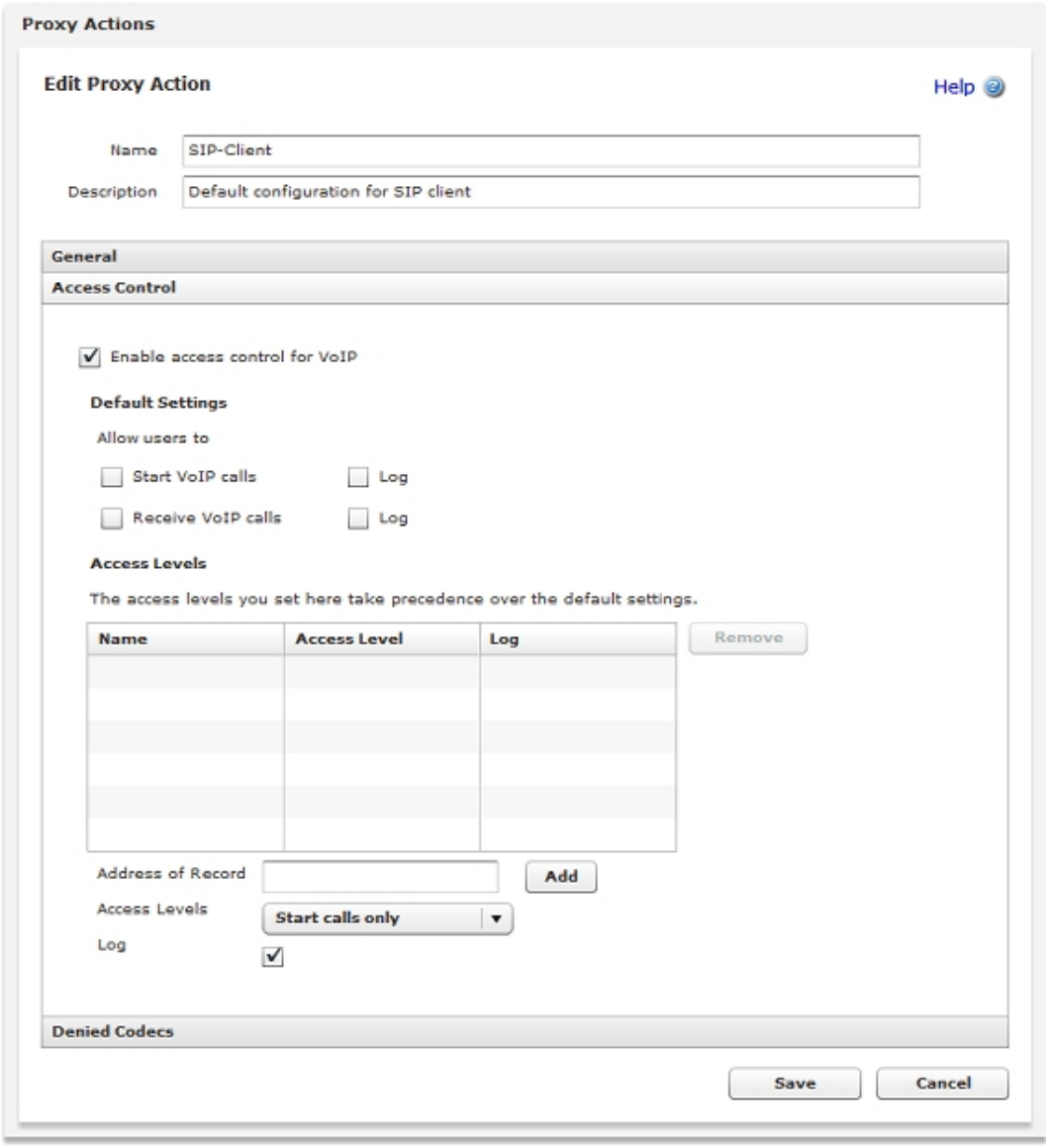
To specify a different time interval, type or select the time in seconds in the **Idle media channels** text box.

Enable logging for reports

To send a log message for each connection request managed by the SIP-ALG, select this check box. To create accurate reports on SIP traffic, you must select this check box.

SIP-ALG: Access Control

On the **Edit Proxy Action** page for a SIP-ALG action, in the **Access Control** section, you can create a list of users who are allowed to send VoIP network traffic.



Enable access control for VoIP

To enable the access control feature, select this check box. When enabled, the SIP-ALG allows or restricts calls based on the options you set.

Default Settings

To allow all VoIP users to start calls by default, select the **Start VoIP calls** check box.

To allow all VoIP users to receive calls by default, select the **Receive VoIP calls** check box.

To create a log message for each SIP VoIP connection that is started or received, select the adjacent **Log** check box.

Access Levels

To create an exception to the default settings you specified, type the **Address of Record** (the address that shows up in the TO and FROM headers of the packet) for the exception. This is usually a SIP address in the format *user@domain*, such as `myuser@example.com`.

From the **Access Level** drop-down list, select an access level and click **Add**.

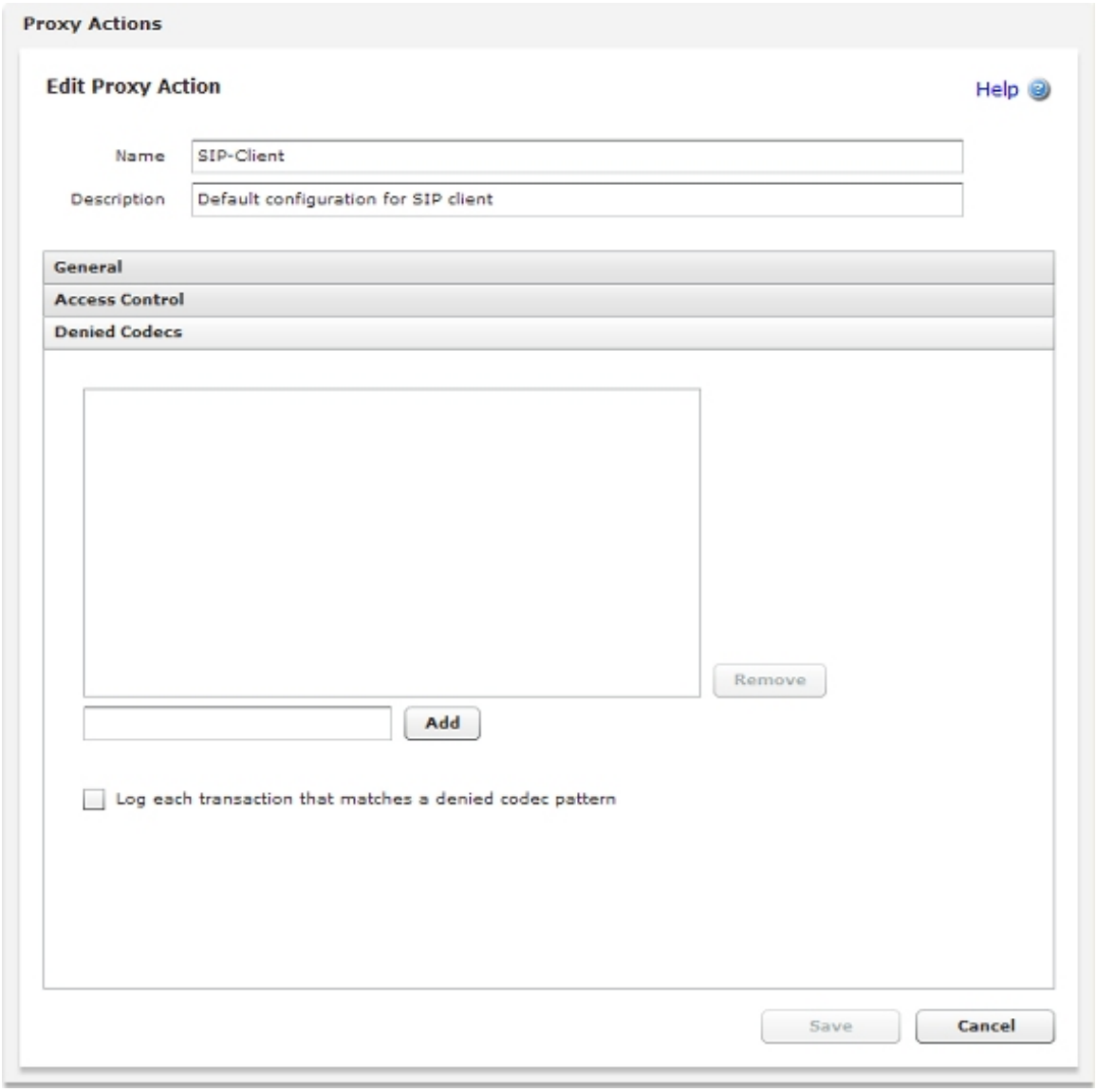
You can select whether to allow users to **Start calls only**, **Receive calls only**, **Start and receive calls**, or give them **No VoIP access**. These settings apply only to SIP VoIP traffic.

To delete an exception, select it in the list and click **Remove**.

Connections made by users who have an access level exception are logged by default. If you do not want to log connections made by a user with an access level exception, clear the **Log** check box adjacent to the exception.

SIP-ALG: Denied Codecs

On the **Denied Codecs** page, you can set the VoIP voice, video, and data transmission codecs that you want to deny on your network.



Denied Codecs list

Use this feature to deny one or more VoIP codecs. When a SIP VoIP connection is opened that uses a codec specified in this list, your XTM device closes the connection automatically.

This list is empty by default. We recommend that you add a codec to this list if it consumes too much bandwidth, presents a security risk, or if it is necessary to have your VoIP solution operate correctly.

For example, you may choose to deny the G.711 or G.726 codecs because they use more than 32 Kb/sec of bandwidth, or you may choose to deny the Speex codec because it is used by an unauthorized VOIP application.

To add a codec to the list, type the codec name or unique text pattern in the text box and click **Add**. Do not use wildcard characters or regular expression syntax. The codec patterns are case sensitive.

To delete a codec from the list, select it and click **Remove**.

Log each transaction that matches a denied codec pattern

Select this option to create a log message when your XTM device denies SIP traffic that matches a codec in this list.

About the SMTP-Proxy

SMTP (Simple Mail Transport Protocol) is a protocol used to send email messages between email servers and also between email clients and email servers. It usually uses a TCP connection on Port 25. You can use the SMTP-proxy to control email messages and email content. The proxy scans SMTP messages for a number of filtered parameters, and compares them against the rules in the proxy configuration.

With an SMTP-proxy filter you can:

- Adjust timeout, maximum email size, and line length limit to make sure the SMTP-proxy does not use too many network resources and can prevent some types of attacks.
- Customize the deny message that users see when an email they try to receive is blocked.
- Filter content embedded in email with MIME types and name patterns.
- Limit the email addresses that email can be addressed to and automatically block email from specific senders.

To add the SMTP-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 316.

You can also configure subscription service settings for the SMTP proxy. For more information, see:

- *Configure spamBlocker*
- *Configure the Gateway AntiVirus Service*

If you must change the proxy definition, you can use the **Policy Configuration page** to modify the definition. This page has three tabs: **Policy**, **Properties**, and **Advanced**.

Action Settings

At the top of the **Policy Configuration** page, you can set these actions:

- **Application Control Action** — If Application Control is enabled on your device, specify the application control action to use for this policy. For more information, see *Enable Application Control in a Policy*.
- **Proxy action** — Select the proxy action to use for this policy. For information about proxy actions, see *About Proxy Actions* on page 317.

Policy Tab

- **Connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**. Define who appears in the **From** and **To** lists.
  For more information, see *Set Access Rules for a Policy* on page 307.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 309.
- You can also configure static NAT or configure server load balancing.
  For more information, see *Configure Static NAT* on page 160 and *Configure Server Load Balancing* on page 163.

Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, configure the settings in the **Logging** section. For more information, see *Set Logging and Notification Preferences* on page 466.
- If you set the **Connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use SMTP.
  For more information, see *Block Sites Temporarily with Policy Settings* on page 452.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

Advanced Tab

You can use several other options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

Configure the Proxy Action

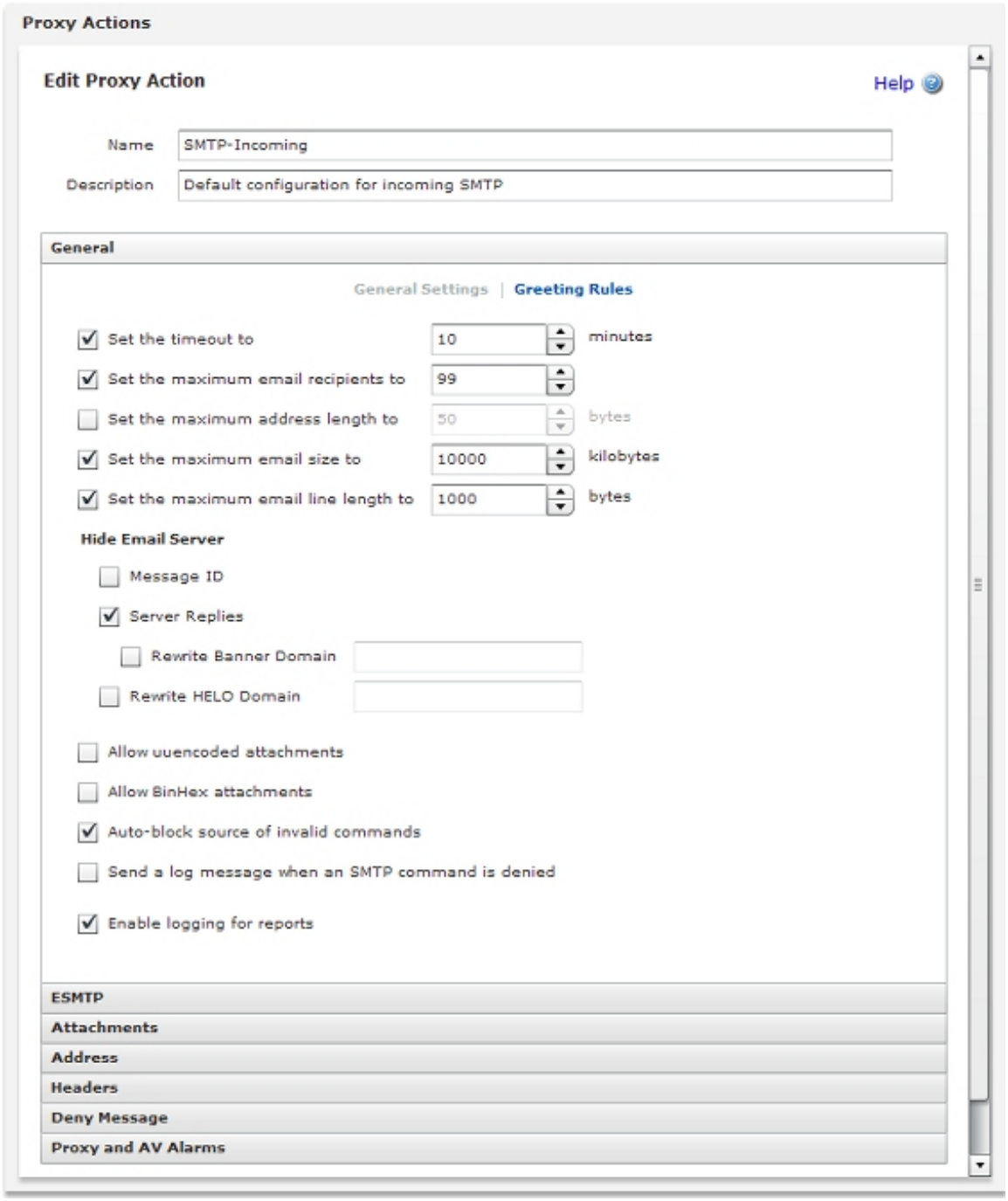
You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 317.

For the SMTP-proxy, you can configure these categories of settings for a proxy action:

- *SMTP-Proxy: General Settings*
- *SMTP Proxy: Greeting Rules*
- *SMTP-Proxy: ESMTP Settings*
- *SMTP-Proxy: Authentication*
- *SMTP-Proxy: Content Types*
- *SMTP-Proxy: File Names*
- *SMTP-Proxy: Mail From/Rcpt To*
- *SMTP-Proxy: Headers*
- *SMTP-Proxy: Deny Message*
- *SMTP-Proxy: Proxy and AV Alarms*

SMTP-Proxy: General Settings

In the **General** section of the **Edit Proxy Action** page for an SMTP proxy action, you can set basic SMTP-proxy parameters such as idle timeout, message limits, and email message information.



Idle timeout

You can set the length of time an incoming SMTP connection can be idle before the connection times out. The default value is 10 minutes.

Set the maximum email recipients

To set the maximum number of email recipients to which a message can be sent, select this check box. In the adjacent text box that appears, type or select the number of recipients.

The XTM device counts and allows the specified number of addresses through, and then drops the other addresses. For example, if you set the value to 50 and there is a message for 52 addresses, the first 50 addresses get the email message. The last two addresses do not get a copy of the message. The XTM device counts a distribution list as one SMTP email address (for example, support@example.com). You can use this feature to decrease spam email because spam usually includes a large recipient list. When you enable this option, make sure you do not also deny legitimate email.

Set the maximum address length to

To set the maximum length of email addresses, select this check box. In the adjacent text box that appears, type or select the maximum length for an email address in bytes.

Set the maximum email size to

To set the maximum length of an incoming SMTP message, select this check box. In the adjacent text box that appears, type or select the maximum size for each email in kilobytes.

Most email is sent as 7-bit ASCII text. The exceptions are Binary MIME and 8-bit MIME. 8-bit MIME content (for example, MIME attachments) is encoded with standard algorithms (Base64 or quote-printable encoding) to enable them to be sent through 7-bit email systems. Encoding can increase the length of files by as much as one third. To allow messages as large as 10 KB, you must set this option to a minimum of 1334 bytes to make sure all email gets through.

Set the maximum email line length to

To set the maximum line length for lines in an SMTP message, select this check box. In the adjacent text box that appears, type or select the length in bytes for each line in an email.

Very long line lengths can cause buffer overflows on some email systems. Most email clients and systems send short line lengths, but some web-based email systems send very long lines.

Hide Email Server

You can replace MIME boundary and SMTP greeting strings in email messages.These are used by hackers to identify the SMTP server vendor and version.

Select the **Message ID** and **Server Replies** check boxes.

If you have an email server and use the SMTP-Incoming proxy action, you can set the SMTP-proxy to replace the domain that appears in your SMTP server banner with a domain name you select. To do this, you must select the **Server Replies** and **Rewrite Banner Domain** check boxes. In the **Rewrite Banner Domain** text box, type the domain name to use in your banner.

If you use the SMTP-Outgoing proxy action, you can set the SMTP-proxy to replace the domain shown in the HELO or EHLO greetings. A HELO or EHLO greeting is the first part of an SMTP transaction, when your email server announces itself to a receiving email server. To do this, select the **Rewrite HELO Domain** check box. In the **Rewrite HELO Domain** text box, type the domain name to use in your HELO or EHLO greeting.

Allow uuencoded attachments

To enable the SMTP-proxy to allow uuencoded attachments to email messages, select this check box. Uuencode is an older program used to send binary files in ASCII text format over the Internet. UUencode attachments can be security risks because they appear as ASCII text files but can actually contain executable files.

Allow BinHex attachments

To enable the SMTP-proxy to allow BinHex attachments to email messages, select this check box. BinHex, which is short for binary-to-hexadecimal, is a utility that converts a file from binary to ASCII format.

Auto-block sources of invalid commands

To add senders of invalid SMTP commands to the Blocked Sites list, select this check box. Invalid SMTP commands often indicate an attack on your SMTP server.

Send a log message when an SMTP command is denied

To send a log message for connection requests that are denied by the SMTP-proxy, select this check box.

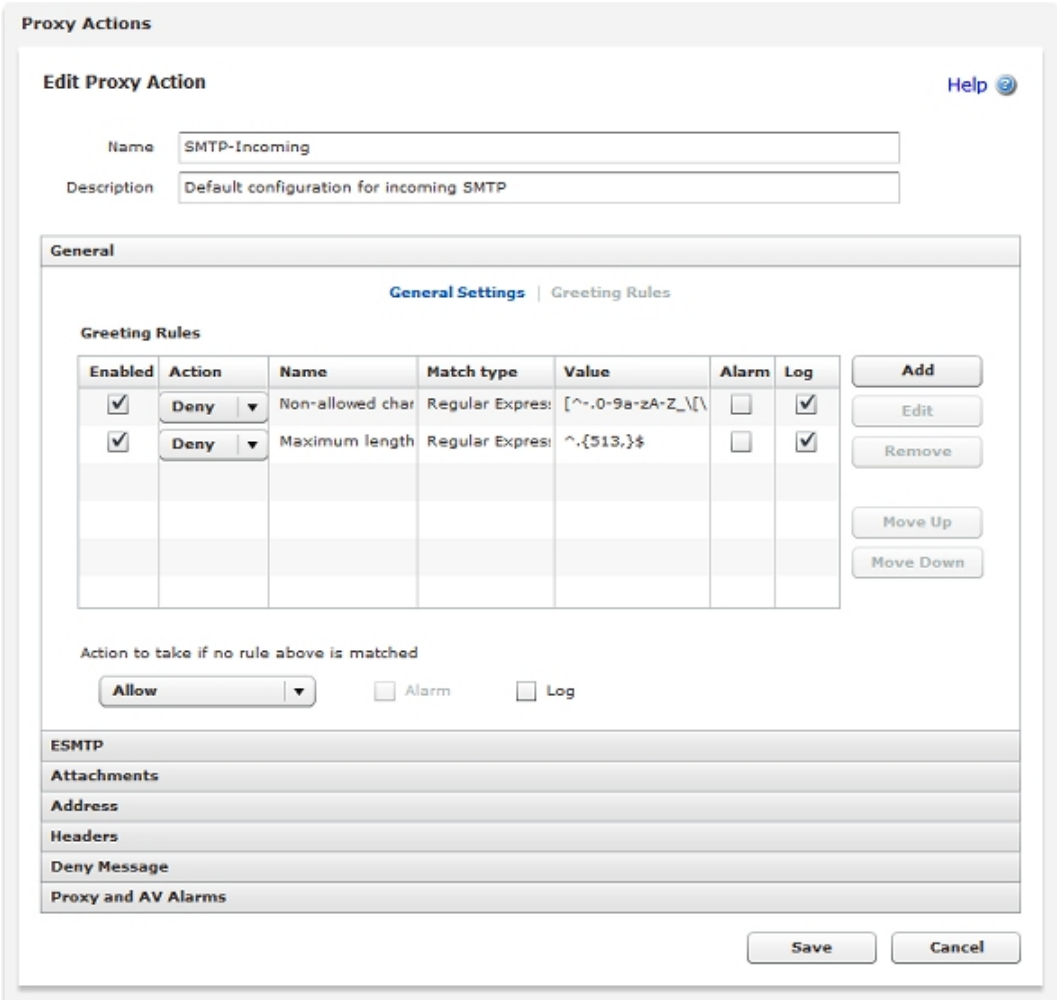
Enable logging for reports

To send a log message for each connection request through the SMTP-proxy, select this check box. To create accurate reports on SMTP traffic, you must select this check box.

SMTP Proxy: Greeting Rules

The proxy examines the initial HELO/EHLO responses when the SMTP session is initialized. The default rules for the SMTP-Incoming proxy action make sure that packets with greetings that are too long, or include characters that are not correct or expected, are denied. You can add, delete, or modify rules.

1. On the **Edit Proxy Action** page, select the **General** category.
   The General category expands.
2. In the link bar, select **Greeting Rules**.
   The Greeting Rules page appears.



3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

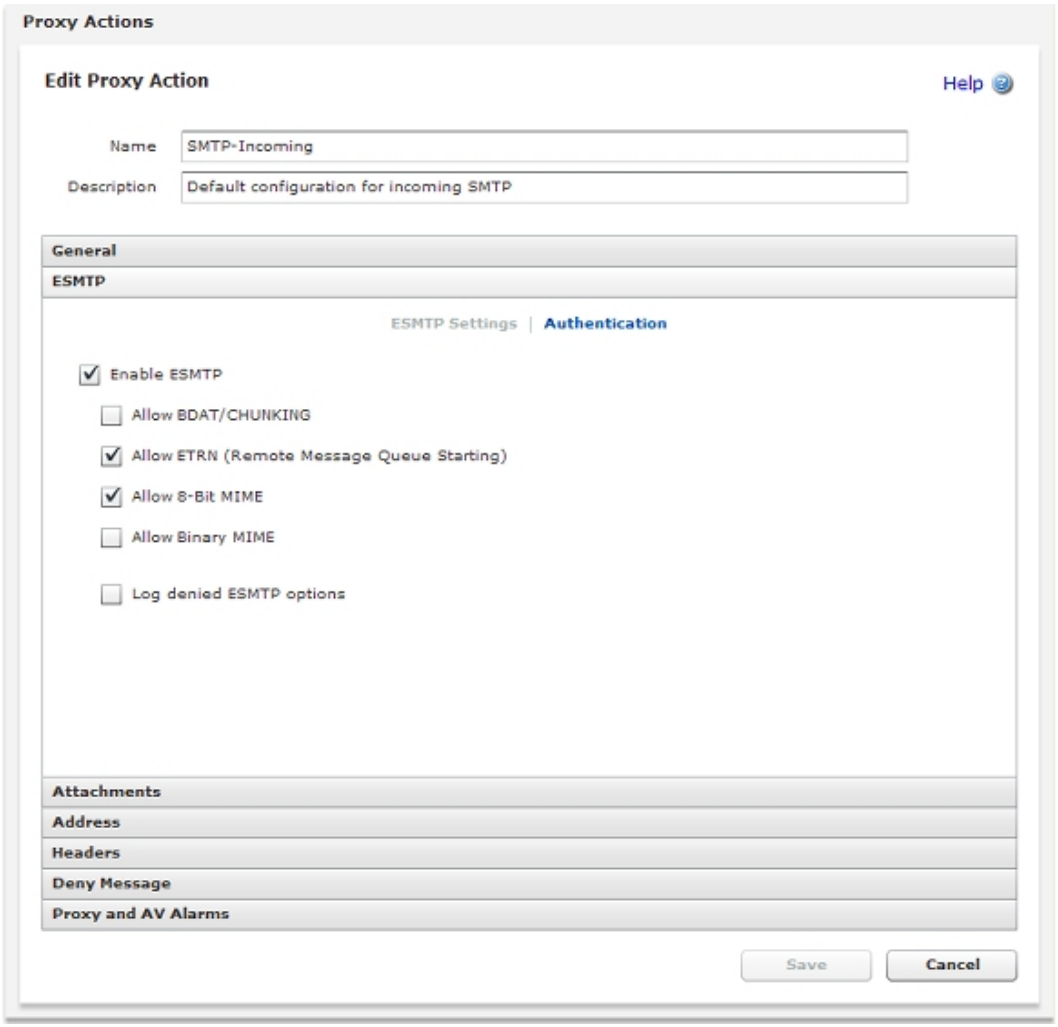
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

SMTP-Proxy: ESMTP Settings

On the **ESMTP Settings** page, you can set the filtering for ESMTP content. Although SMTP is widely accepted and widely used, some parts of the Internet community want more functionality in SMTP. ESMTP gives a method for functional extensions to SMTP, and to identify servers and clients that support extended features.

1. On the **Edit Proxy Action** page, select the **ESMTP** category.
   The ESMTP category expands.
2. In the link bar, select **ESMTP Settings**.
   The ESMTP Settings page appears.



3. Configure these options:

   Enable ESMTP

   Select this check box to enable all fields. If you clear this check box, all other check boxes on this page are disabled. When the options are disabled, the settings for each options are saved. If this option is enabled again, all the settings are restored.

   Allow BDAT/CHUNKING

Select this check box to allow BDAT/CHUNKING. This enables large messages to be sent more easily through SMTP connections.

Allow ETRN (Remote Message Queue Starting)

This is an extension to SMTP that allows an SMTP client and server to interact to start the exchange of message queues for a given host.

Allow 8-Bit MIME

Select this check box to allow transmission of 8-bit data messages. When this option is disabled, messages encoded with 8-big MIME are denied by the SMTP-proxy. Enable this option only if your email server has the ability to send 8-bit data transmissions.

Allow Binary MIME

Select to allow the Binary MIME extension, if the sender and receiver accept it. Binary MIME prevents the overhead of base64 and quoted-printable encoding of binary objects sent that use the MIME message format with SMTP. We do not recommend you select this option as it can be a security risk.

Log denied ESMTP options

Select this check box to create a log message for unknown ESMTP options that are stripped by the SMTP-proxy. Clear this check box to disable this option.

4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

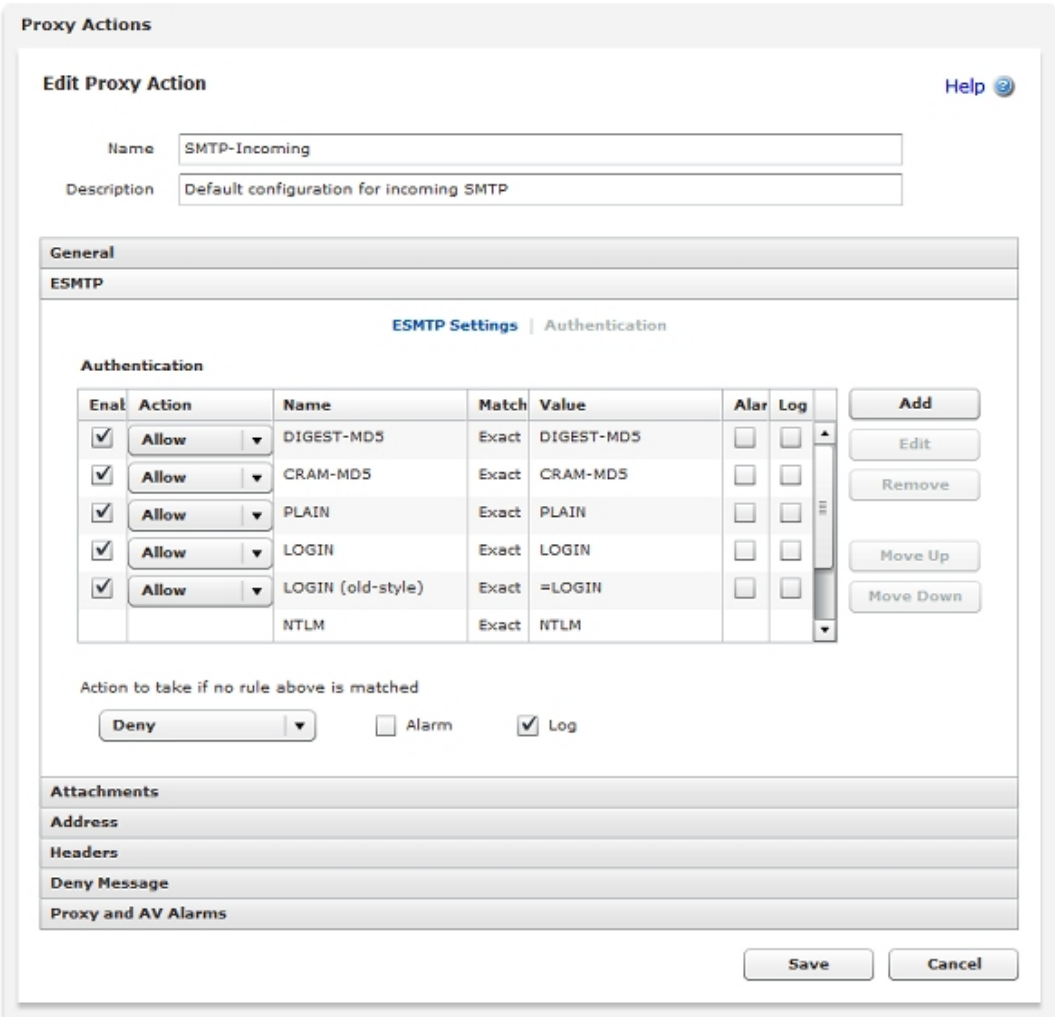
For more information on predefined proxy actions, see *About Proxy Actions*.

SMTP-Proxy: Authentication

This ruleset allows these ESMTP authentication types: DIGEST- MD5, CRAM-MD5, PLAIN, LOGIN, LOGIN (old style), NTLM, and GSSAPI. The default rule denies all other authentication types. The RFC that tells about the SMTP authentication extension is RFC 2554.

If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules:

1. On the **Edit Proxy Action** page, select the **ESMTP** category.
   The ESMTP category expands.
2. In the link bar, select **Authentication**.
   The Authentication page appears.



3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

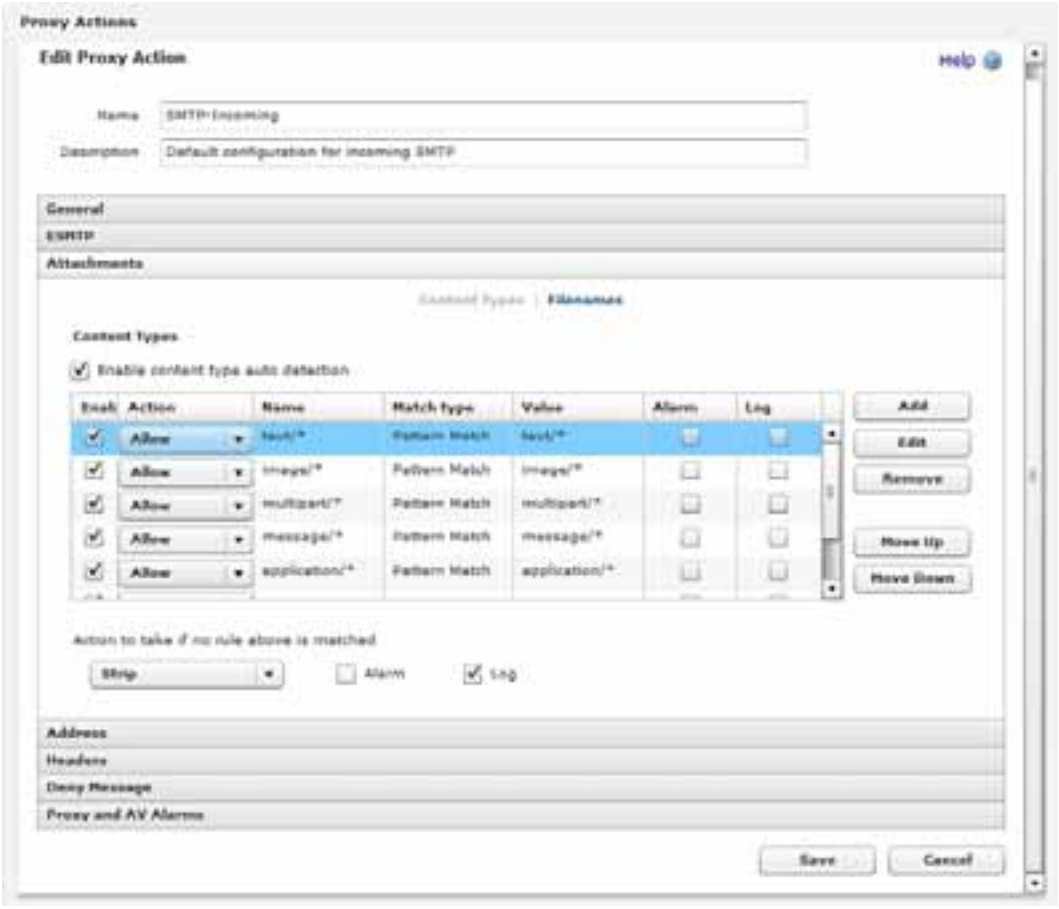
For more information on predefined proxy actions, see *About Proxy Actions*.

SMTP-Proxy: Content Types

Certain kinds of content embedded in email can be a security threat to your network. Other kinds of content can decrease the productivity of your users. You can use the ruleset for the SMTP-Incoming proxy action to set values for incoming SMTP content filtering. You can use the ruleset for the SMTP-Outgoing proxy action to set values for outgoing SMTP content filtering. The SMTP-proxy allows these content types: text/*, image/*, multipart/*, and message/*. You can add, delete, or modify rules.

You can also configure the SMTP-proxy to automatically examine the content of email messages to determine the content type. If you do not enable this option, the SMTP-proxy uses the value stated in the email header, which clients sometimes set incorrectly. For example, an attached .pdf file might have a content type stated as application/octet-stream. If you enable content type auto detection, the SMTP-proxy recognizes the .pdf file and uses the actual content type, application/pdf. If the proxy does not recognize the content type after it examines the content, it uses the value stated in the email header, as it would if content type auto detection were not enabled. Because hackers often try to disguise executable files as other content types, we recommend that you enable content type auto detection to make your installation more secure.

1. On the **Edit Proxy Action** page, select the **Attachments** category.
   The Attachments category expands.
2. In the link bar, select **Content Types**.
   The Content Types page appears.



3. To enable the SMTP-proxy to examine content to determine content type, select the **Enable content type auto detection** check box.
4. *Add, Change, or Delete Rules*.
5. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
6. Click **Save**.

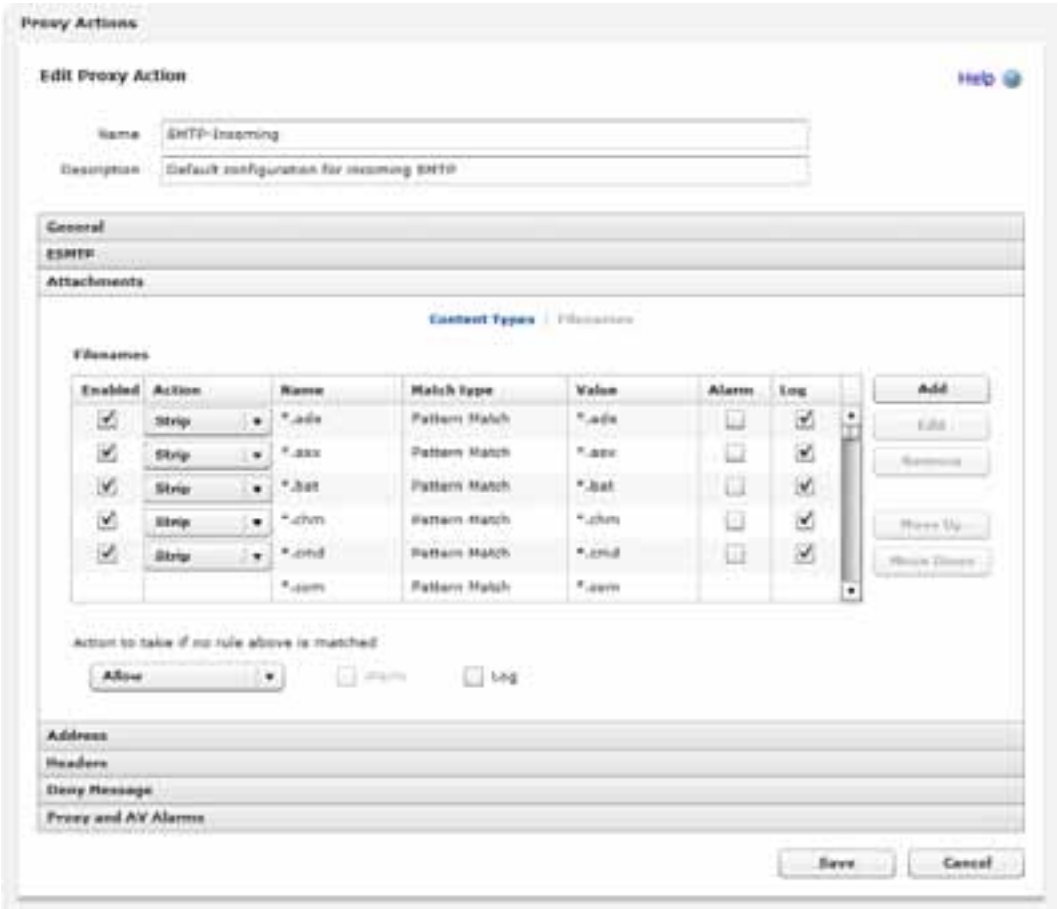
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

SMTP-Proxy: File Names

You can use the ruleset for the SMTP-Incoming proxy action to put limits on file names for incoming email attachments. You use the ruleset for the SMTP-Outgoing proxy action to put limits on file names for outgoing email attachments. You can add, delete, or modify rules.

1. On the **Edit Proxy Action** page, select the **Attachments** category.
   The Attachments category expands.
2. In the link bar, select **Filenames**.
   The Filenames page appears.



3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

SMTP-Proxy: Mail From/Rcpt To

You can use the **Address: Mail From** ruleset to put limits on email and to allow email into your network only from specified senders. The default configuration is to allow email from all senders. You can add, delete, or modify rules.

The **Address: Rcpt To** ruleset can limit the email that goes out of your network to only specified recipients. The default configuration allows email to all recipients out of your network. On an SMTP-Incoming proxy action, you can use the **Rcpt To** ruleset to make sure your email server can not be used for email relaying. For more information, see *Protect Your SMTP Server from Email Relaying* on page 421.

You can also use the **Replace** option in a rule to configure the XTM device to change the *From* and *To* components of your email address to a different value. This feature is also known as *SMTP masquerading*.

Other options available in the **Mail From** and **Rcpt To** rulesets:

Block source-routed addresses

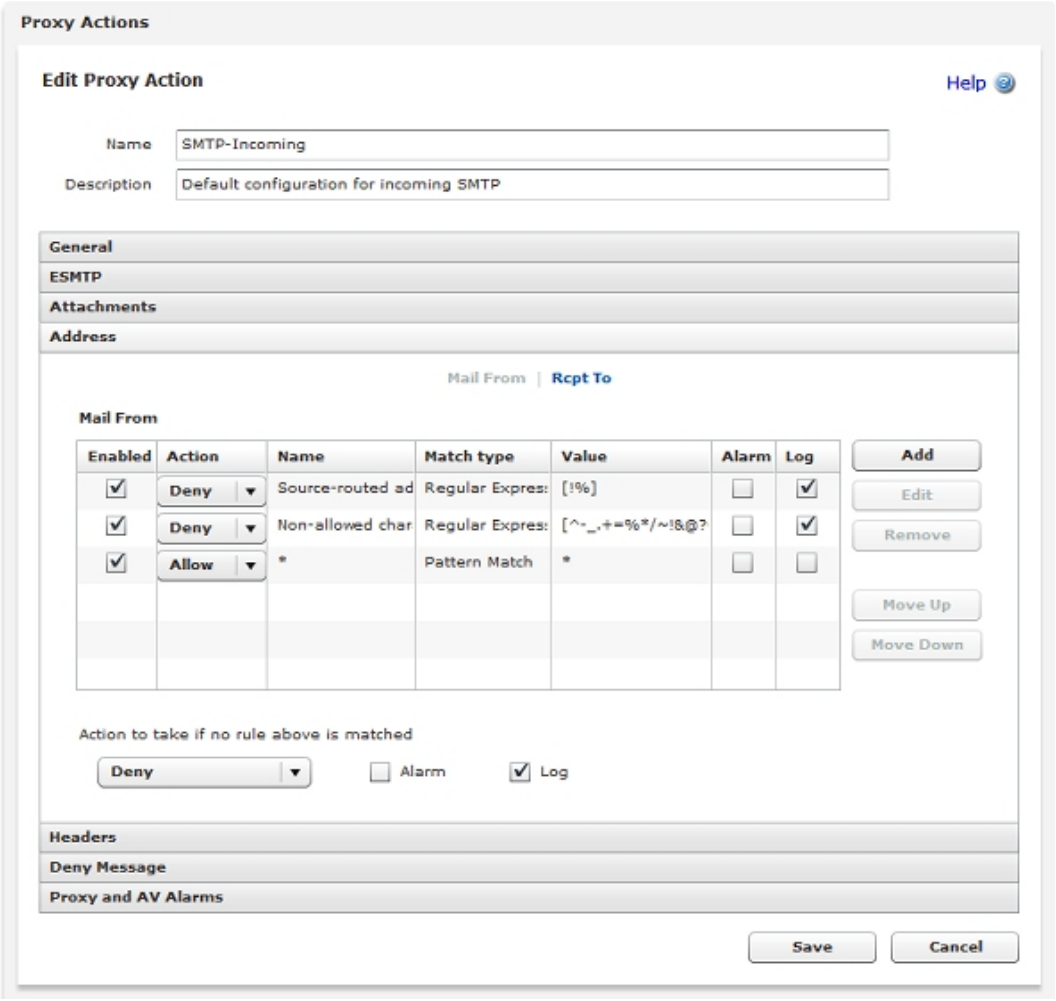
Select this check box to block a message when the sender address or recipient address contains source routes. A source route identifies the path a message must take when it goes from host to host. The route can identify which mail routers or *backbone* sites to use. For example, @backbone.com:freddyb@something.com means that the host named Backbone.com must be used as a relay host to deliver mail to freddyb@something.com. By default, this option is enabled for incoming SMTP packets and disabled for outgoing SMTP packets.

Block 8-bit characters

Select this check box to block a message that has 8-bit characters in the sender user name or recipient user name. This allows an accent on an alphabet character. By default, this option is enabled for incoming SMTP packets and disabled for outgoing SMTP packets.

To configure the SMTP proxy to put limits on the email traffic through your network:

1. On the **Edit Proxy Action** page, select the **Address** category.
   The Address category expands.
2. In the link bar, select **Mail From** or **Rcpt To**.
   The Mail From or Rcpt To settings page appears.



3. *Add, Change, or Delete Rules*.
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

SMTP-Proxy: Headers

Header rulesets allow you to set values for incoming or outgoing SMTP header filtering. You can add, delete, or modify rules.

1. On the **Edit Proxy Action** page, select the **Headers** category.
   The ESMTP category settings appear.
2. *Add, Change, or Delete Rules*.

3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

SMTP-Proxy: Deny Message

When content is denied, the XTM device sends a default *deny message* that replaces the denied content. This message appears in a recipients email message when the proxy blocks an email. You can change the text of that deny message. The first line of the deny message is a section of the HTTP header. You must include an empty line between the first line and the body of the message.

The default deny message appears in the **Deny Message** text box. To change this to a custom message, use these variables:

%(reason)%

Includes the reason the XTM device denied the content.

%(type)%

Includes the type of content that was denied.

%(filename)%

Includes the file name of the denied content.

%(virus)%

Includes the name or status of a virus for Gateway AntiVirus users.

%(action)%

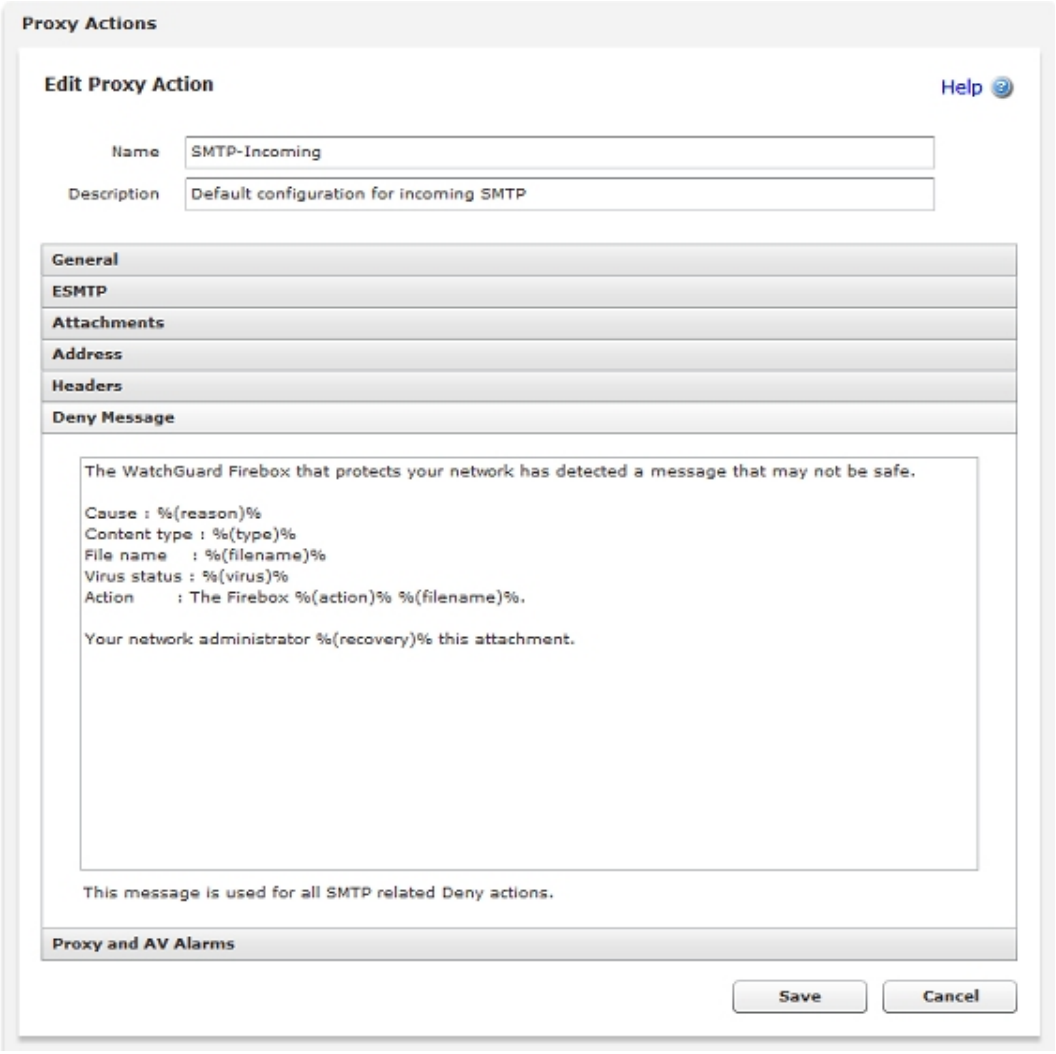
Includes the name of the action taken. For example: lock or strip.

%(recovery)%

Includes whether you can recover the attachment.

To configure the deny message:

1. On the **Edit Proxy Action** page, select the **Deny Message** category.
   The Deny Message category settings appear.



2. In the **Deny Message** text box, type a custom plain text message in standard HTML.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

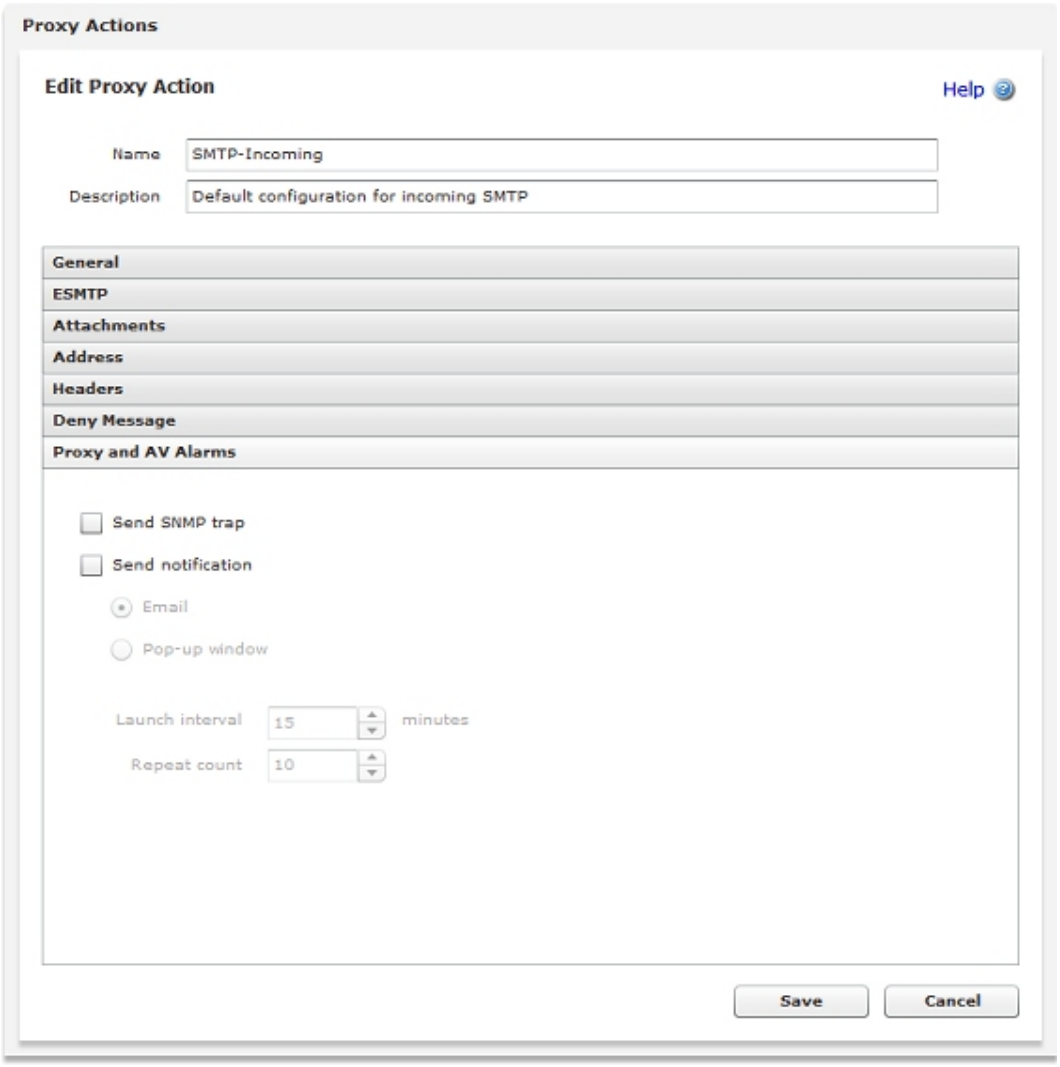
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

SMTP-Proxy: Proxy and AV Alarms

You can configure how the SMTP-proxy sends messages for alarm and antivirus events that occur through the SMTP-proxy. You can define the proxy to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email message to a network administrator or a pop-up window on the management computer.

1. On the **Edit Proxy Action** page, select the **Proxy Alarm** category.
   The Proxy Alarm settings appear.



2. Configure the notification settings for the SMTP-proxy action.
   For more information, see *Set Logging and Notification Preferences* on page 466.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **Save**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

Configure the SMTP-Proxy to Quarantine Email

The WatchGuard Quarantine Server provides a safe, full-featured quarantine mechanism for any email messages suspected or known to be spam or to contain viruses. This repository receives email messages from the SMTP-proxy and filtered by spamBlocker.

To configure the SMTP-proxy to quarantine email:

1. Add the SMTP proxy to your configuration and enable spamBlocker in the proxy definition.
   Or, enable spamBlocker and select to enable it for the SMTP-proxy.
2. When you set the actions spamBlocker applies for different categories of email (as described in *Configure spamBlocker* on page 687), make sure you select the **Quarantine** action for at least one of the categories. When you select this action, you are prompted to configure the Quarantine Server if you have not already done so.

You can also select the **Quarantine** action for email messages identified by Virus Outbreak Detection as containing viruses. For more information, see *Configure Virus Outbreak Detection Actions for a Policy* on page 691.

Protect Your SMTP Server from Email Relaying

Email relaying, also called *mail spamming* or open mail relay, is an intrusion in which a person uses your email server, address, and other resources, to send large amounts of spam email. This can cause system crashes, equipment damage, and financial loss.

If you are not familiar with the issues involved with mail relaying, or are unsure whether your email server is vulnerable to mail relaying, we recommend you research your own email server and learn its potential vulnerabilities. The XTM device can give basic mail relay protection if you are unsure of how to configure your email server. However, you find out how to use your email server to prevent email relaying.

To protect your server, you change the configure of the SMTP-proxy policy that filters traffic from the external network to your internal SMTP server to include your domain information. When you type your domain, you can use the wildcard * character. Then, any email address that ends with *@your-domain-name* is allowed. If your email server accepts email for more than one domain, you can add more domains. For example, if you add both **@example.com* and **@*.example.com* to the list, your email server will accept all email destined to the top-level*example.com* domain and all email destined to sub-domains of *example.com*. For example, *rnd.example.com*.

Before you start this procedure, you must know the names of all domains that your SMTP email server receives email for.

1. Select **Firewall > Proxy Actions**.
2. Select the SMTP-proxy action for the SMTP-proxy policy that filters traffic from the external network to an internal SMTP server. Click **Edit**.
3. On the **Edit Proxy Action** page, select the **Address** category.
4. In the link bar, click **Mail From** or **Rcpt To**.
5. In the **Actions to Take** section, from the **Action to take if no rule above is matched** drop-down list, select **Deny**.
   Any email destined to an address other than the domains in the list is denied.

Another way to protect your server is to type a value in the **Rewrite As** text box in this dialog box. The XTM device then changes the From and To components of your email address to a different value. This feature is also known as *SMTP masquerading*.

About the TCP-UDP-Proxy

The TCP-UDP-proxy is included for these protocols on non-standard ports: HTTP, HTTPS, SIP, and FTP. For these protocols, the TCP-UDP proxy relays the traffic to the correct proxies for the protocols or enables you to allow or deny traffic. For other protocols, you can select to allow or deny traffic. You can also use this proxy policy to allow or deny IM (instant messaging) and P2P (peer-to-peer) network traffic. The TCP-UDP proxy is intended only for outgoing connections.

To add the TCP-UDP-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 316.

If you must change the proxy definition, you can use the **Policy Configuration page** to modify the definition. This page has three tabs: **Policy**, **Properties**, and **Advanced**.

Action Settings

At the top of the **Policy Configuration** page, you can set these actions:

- **Application Control Action** — If Application Control is enabled on your device, specify the application control action to use for this policy. For more information, see *Enable Application Control in a Policy*.
- **Proxy action** — Select the proxy action to use for this policy. For information about proxy actions, see *About Proxy Actions* on page 317.

Policy Tab

- **TCP-UDP-proxy connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**, and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). Fore more information, see *Set Access Rules for a Policy* on page 307.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 309.
- You can also configure static NAT or configure server load balancing.
  For more information, see *Configure Static NAT* on page 160 and *Configure Server Load Balancing* on page 163.

Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, configure the settings in the **Logging** section. For more information, see *Set Logging and Notification Preferences* on page 466.
- If you set the **Connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use TCP-UDP.
  For more information, see *Block Sites Temporarily with Policy Settings* on page 452.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

Advanced Tab

You can use several other options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

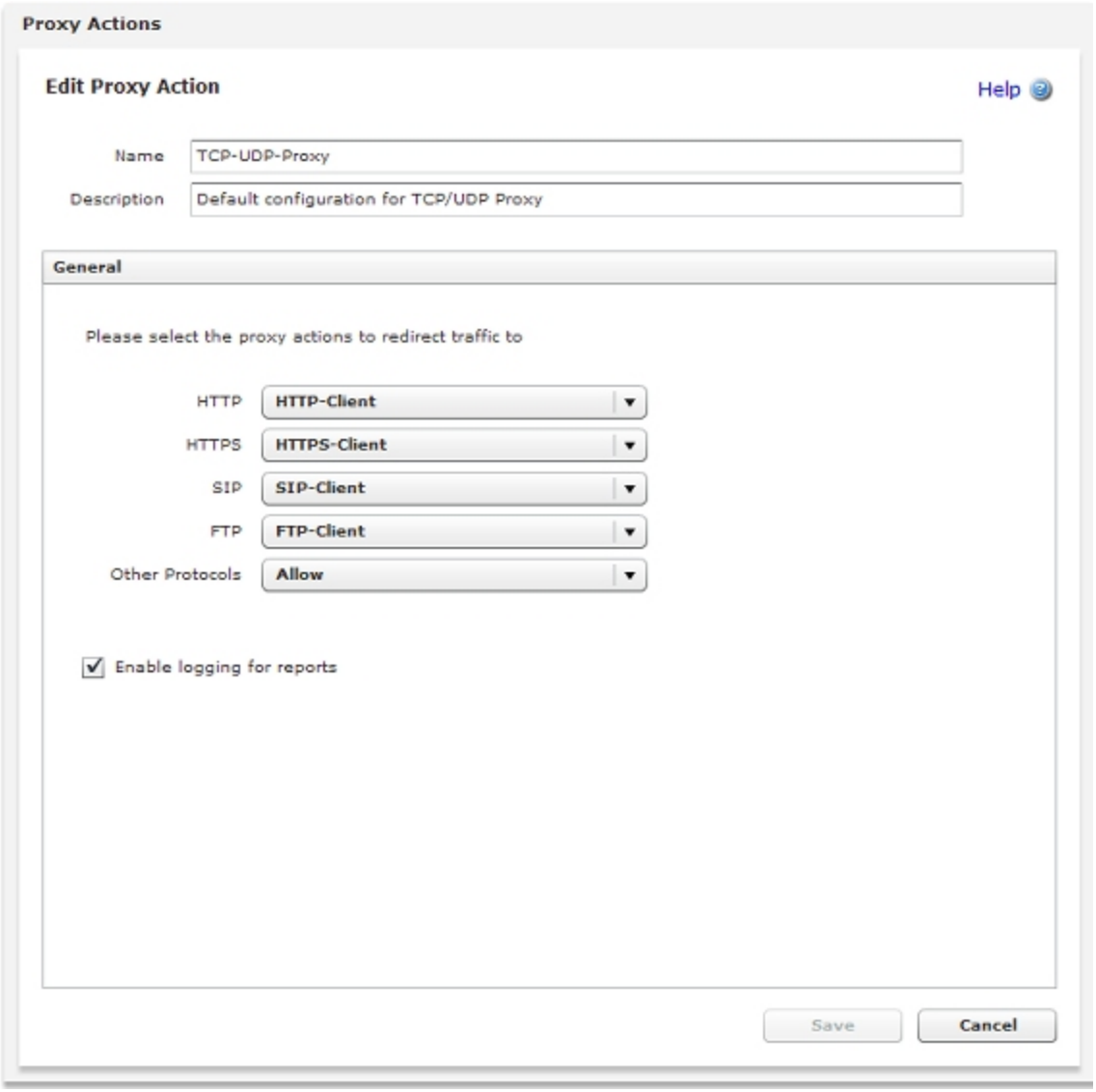
Configure the Proxy Action

You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 317.

For the TCP-UDP-proxy, you can configure the general settings for a proxy action. For more information, see *TCP-UDP-Proxy: General Settings*.

TCP-UDP-Proxy: General Settings

On the **Edit Proxy Action** page for a TCP-UDP proxy action, in the **General** section, you set basic parameters for the TCP-UDP-proxy.



Proxy actions to redirect traffic

The TCP-UDP-proxy can pass HTTP, HTTPS, SIP, and FTP traffic to proxy policies that you have already created when this traffic is sent over non-standard ports.

For each of these protocols, from the adjacent drop-down list, select the proxy policy to use to manage this traffic.

If you do not want your XTM device to use a proxy policy to filter a protocol, select **Allow** or **Deny** from the adjacent drop-down list.

> ***Note*** *To ensure that your XTM device operates correctly, you cannot select the **Allow** option for the FTP protocol.*

Enable logging for reports

To send a log message for each connection request through the TCP-UDP-proxy, select this check box. To create accurate reports on TCP-UDP traffic, you must select this check box.

14 Traffic Management and QoS

About Traffic Management and QoS

In a large network with many computers, the volume of data that moves through the firewall can be very large. A network administrator can use Traffic Management and Quality of Service (QoS) actions to prevent data loss for important business applications, and to make sure mission-critical applications take priority over other traffic.

Traffic Management and QoS provide a number of benefits. You can:

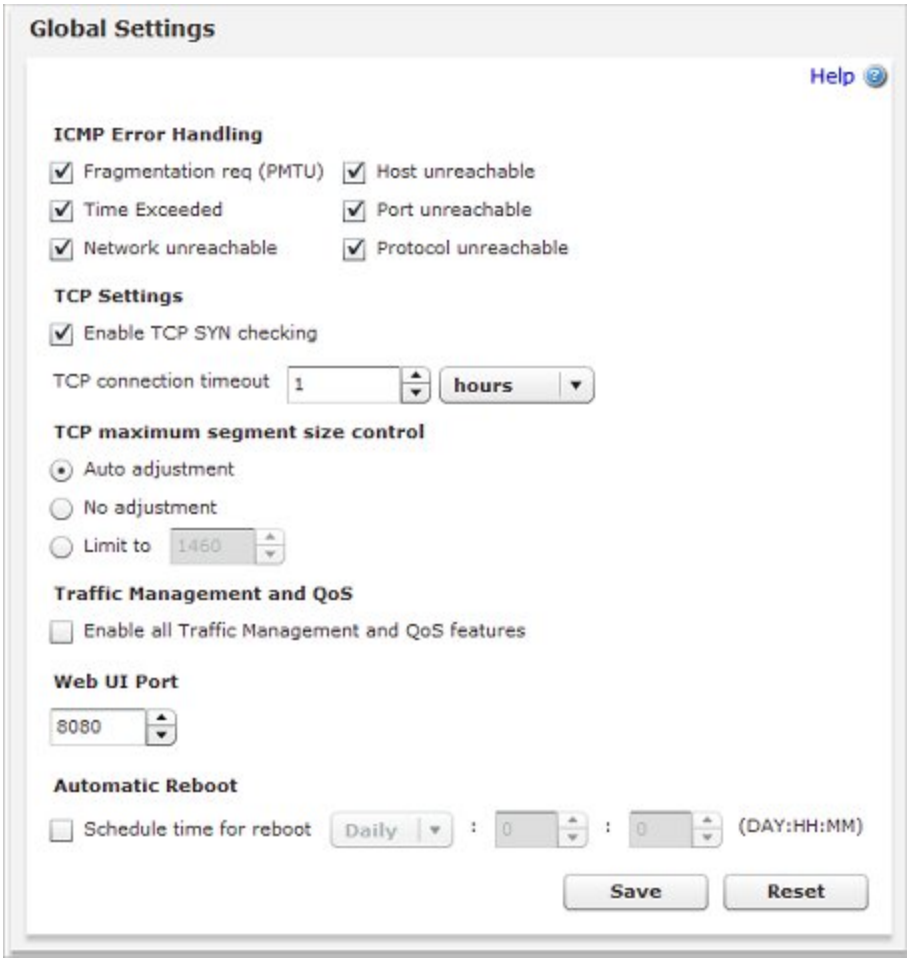
- Guarantee or limit bandwidth
- Control the rate at which the XTM device sends packets to the network
- Prioritize when to send packets to the network

To apply traffic management to policies, you define a Traffic Management action, which is a collection of settings that you can apply to one or more policy definitions. This way you do not need to configure the traffic management settings separately in each policy. You can define additional Traffic Management actions if you want to apply different settings to different policies.

Enable Traffic Management and QoS

For performance reasons, all traffic management and QoS features are disabled by default. You must enable these features in Global Settings before you can use them.

1. Select **System > Global Settings**.
   The Global Settings page appears.



2. Select the **Enable all traffic management and QoS features** check box.
3. Click **Save**.

Guarantee Bandwidth

Bandwidth reservations can prevent connection timeouts. A traffic management queue with reserved bandwidth and low priority can give bandwidth to real-time applications with higher priority when necessary without disconnecting. Other traffic management queues can take advantage of unused reserved bandwidth when it becomes available.

For example, suppose your company has an FTP server on the external network and you want to guarantee that FTP always has at least 200 kilobytes per second (KBps) through the external interface. You might also consider setting a minimum bandwidth from the trusted interface to make sure that the connection has end-to-end guaranteed bandwidth. To do this, you would create a Traffic Management action that defines a minimum of 200 KBps for FTP traffic on the external interface. You would then create an FTP policy and apply the Traffic Management action. This will allow *ftp put* at 200 KBps. If you want to allow *ftp get* at 200 KBps, you must configure the FTP traffic on the trusted interface to also have a minimum of 200 KBps.

As another example, suppose your company uses multimedia materials (streaming media) to train external customers. This streaming media uses RTSP over port 554. You have frequent FTP uploads from the trusted to external interface, and you do not want these uploads to compete with your customers ability to receive the streaming media. To guarantee sufficient bandwidth, you could apply a Traffic Management action to the external interface for the streaming media port.

The guaranteed bandwidth setting works with the **Outgoing Interface Bandwidth** setting configured for each interface to make sure you do not guarantee more bandwidth than actually exists. This setting also helps you make sure the sum of your guaranteed bandwidth settings does not fill the link such that non-guaranteed traffic cannot pass. For example, suppose the link is 1 Mbps and you try to use a Traffic Management action that guarantees 973 Kbps (0.95 Mbps) to the FTP policy on that link. With these settings, the FTP traffic could use so much of the available bandwidth that other types of traffic cannot use the interface.

Restrict Bandwidth

To preserve the bandwidth that is available for other applications, you can restrict the amount of bandwidth for certain traffic types or applications. This can also discourage the use of certain applications when users find that the speed of the application's performance is significantly degraded.

The **Maximum Bandwidth** setting in a Traffic Management action enables you to set a limit on the amount of traffic allowed by the Traffic Management action.

For example, suppose that you want to allow FTP downloads but you want to limit the speed at which users can download files. You can add a Traffic Management action that has the Maximum bandwidth set to a low amount on the trusted interface, such as 100 kbps. This can help discourage FTP downloads when the users on the trusted interface find the FTP experience is unsatisfactory.

QoS Marking

QoS marking creates different classes of service for different kinds of outbound network traffic. When you *mark* traffic, you change up to six bits on packet header fields defined for this purpose. Other devices can make use of this marking and provide appropriate handling of a packet as it travels from one point to another in a network.

You can enable QoS marking for an individual interface or an individual policy. When you define QoS marking for an interface, each packet that leaves the interface is marked. When you define QoS marking for a policy, all traffic that uses that policy is also marked.

Traffic priority

You can assign different levels of priority either to policies or for traffic on a particular interface. Traffic prioritization at the firewall allows you to manage multiple class of service (CoS) queues and reserve the highest priority for real-time or streaming data. A policy with high priority can take bandwidth away from existing low priority connections when the link is congested so traffic must compete for bandwidth.

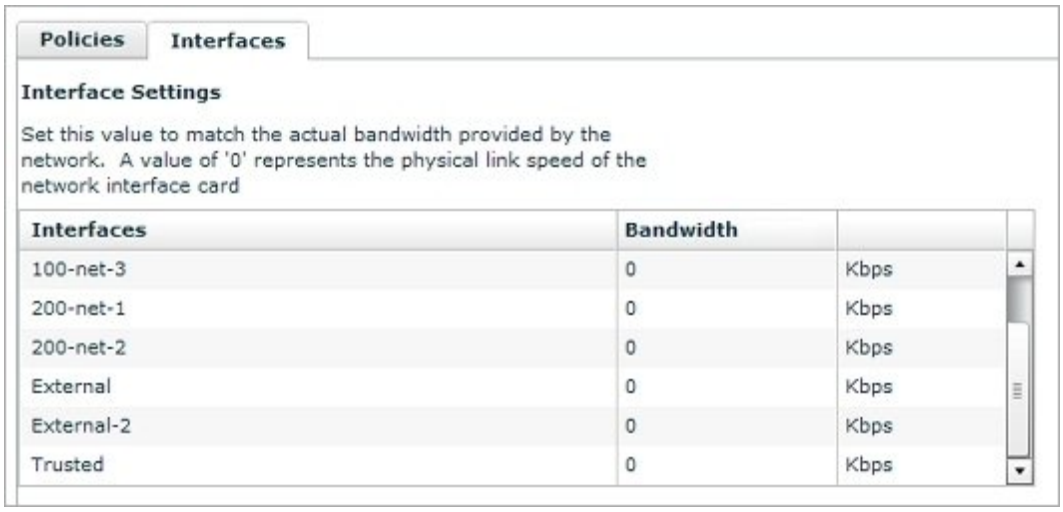
Set Outgoing Interface Bandwidth

Some traffic management features require that you set a bandwidth limit for each network interface. For example, you must configure the **Outgoing Interface Bandwidth** setting to use QoS marking and prioritization.

After you set this limit, your XTM device completes basic prioritization tasks on network traffic to prevent problems with too much traffic on the specified interface. Also, a warning appears in Fireware XTM Web UI if you allocate too much bandwidth as you create or adjust traffic management actions.

If you do not change the **Outgoing Interface Bandwidth** setting for any interface from the default value of 0, it is set to the auto-negotiated link speed for that interface.

1. Select **Firewall > Traffic Management**.
   The Traffic Management page appears.
2. Select the **Interfaces** tab.

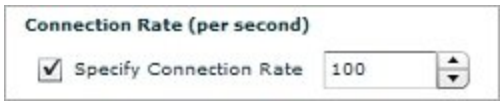


3. In the **Bandwidth** column adjacent to the interface name, type the amount of bandwidth provided by the network.
   Use your Internet connection upload speed in kilobits or megabits per second (Kbps or Mbps).
   Set your LAN interface bandwidth based on the minimum link speed supported by your LAN infrastructure.
4. To change the speed unit, select an interface in the list, then click the adjacent speed unit and select a different option in the drop-down list.
5. Click **Save**.

Set Connection Rate Limits

To improve network security, you can create a limit on a policy so that it only filters a specified number of connections per second. If additional connections are attempted, the traffic is denied and a log message is created.

1. Select **Firewall > Firewall Policies** or **Firewall > Mobile VPN Policies**.
   The Policies page appears.
2. Double-click a policy, or select the policy to configure and click .
3. Select the **Advanced** tab.
4. Select the **Specify Connection Rate** check box.
5. In the adjacent text box, type or select the number of connections that this policy can process in one second.



6. Click **Save**.

About QoS Marking

Today's networks often consist of many kinds of network traffic that compete for bandwidth. All traffic, whether of prime importance or negligible importance, has an equal chance of reaching its destination in a timely manner. Quality of Service (QoS) marking gives critical traffic preferential treatment to make sure it is delivered quickly and reliably.

QoS functionality must be able to differentiate the various types of data streams that flow across your network. It must then *mark* data packets. QoS marking creates different classifications of service for different kinds of network traffic. When you mark traffic, you change up to six bits on packet header fields defined for this purpose. The XTM device and other QoS-capable devices can use this marking to provide appropriate handling of a packet as it travels from one point to another in a network.

Fireware XTM supports two types of QoS marking: IP Precedence marking (also known as Class of Service) and Differentiated Service Code Point (DSCP) marking. For more information on these marking types and the values you can set, see *Marking Types and Values* on page 433.

Before you begin

- Make sure your LAN equipment supports QoS marking and handling. You may also need to make sure your ISP supports QoS.
- The use of QoS procedures on a network requires extensive planning. You can first identify the theoretical bandwidth available and then determine which network applications are high priority, particularly sensitive to latency and jitter, or both.

QoS marking for interfaces and policies

You can enable QoS marking for an individual interface or an individual policy. When you define QoS marking for an interface, each packet that leaves the interface is marked. When you define QoS marking for a policy, all traffic that uses that policy is also marked. The QoS marking for a policy overrides any QoS marking set on an interface.

For example, suppose your XTM device receives QoS-marked traffic from a trusted network and sends it to an external network. The trusted network already has QoS marking applied, but you want the traffic to your executive team to be given higher priority than other network traffic from the trusted interface. First, set the QoS marking for the trusted interface to one value. Then, add a policy with QoS marking set for the traffic to your executive team with a higher value.

QoS marking and IPSec traffic

If you want to apply QoS to IPsec traffic, you must create a specific firewall policy for the corresponding IPsec policy and apply QoS marking to that policy.

You can also choose whether to preserve existing marking when a marked packed is encapsulated in an IPSec header.

To preserve marking:

1. Select **VPN > Global Settings**.
   The Global VPN Settings page appears.
2. Select the **Enable TOS for IPSec** check box.
3. Click **Save**.
   All existing marking is preserved when the packet is encapsulated in an IPSec header.

To remove marking:

1. Select **VPN > Global Settings**.
   The Global VPN Settings page appears.
2. Clear the **Enable TOS for IPSec** check box.
3. Click **Save**.
   The TOS bits are reset and marking is not preserved.

Marking Types and Values

Fireware XTM supports two types of QoS Marking: IP Precedence marking (also known as Class of Service) and Differentiated Service Code Point (DSCP) marking. IP Precedence marking affects only the first three bits in the IP type of service (TOS) octet. DSCP marking expands marking to the first six bits in the IP TOS octet. Both methods allow you to either preserve the bits in the header, which may have been marked previously by an external device, or change them to a new value.

DSCP values can be expressed in numeric form or by special keyword names that correspond to per-hop behavior (PHB). Per-hop behavior is the priority applied to a packet when it travels from one point to another in a network. Fireware DSCP marking supports three types of per-hop behavior:

Best-Effort

Best-Effort is the default type of service and is recommended for traffic that is not critical or real-time. All traffic falls into this class if you do not use QoS Marking.

Assured Forwarding (AF)

Assured Forwarding is recommended for traffic that needs better reliability than the best-effort service. Within the Assured Forwarding (AF) type of per-hop behavior, traffic can be assigned to three classes: Low, Medium, and High.

Expedited Forwarding (EF)

This type has the highest priority. It is generally reserved for mission-critical and real-time traffic.

Class-Selector (CSx) code points are defined to be backward compatible with IP Precedence values. CS1–CS7 are identical to IP Precedence values 1–7.

The subsequent table shows the DSCP values you can select, the corresponding IP Precedence value (which is the same as the CS value), and the description in PHB keywords.

DSCP Value	Equivalent IP Precedence value (CS values)	Description: Per-hop Behavior keyword
0		Best-Effort (same as no marking)
8	1	Scavenger*
10		AF Class 1 - Low
12		AF Class 1 - Medium
14		AF Class 1 - High
16	2	
18		AF Class 2 - Low
20		AF Class 2 - Medium
22		AF Class 2- High
24	3	

DSCP Value	Equivalent IP Precedence value (CS values)	Description: Per-hop Behavior keyword
26		AF Class 3 - Low
28		AF Class 3 - Medium
30		AF Class 3 - High
32	4	
34		AF Class 4 - Low
36		AF Class 4 - Medium
38		AF Class 4 - High
40	5	
46		EF
48	6	Internet Control
56	7	Network Control

* The Scavenger class is used for the lowest priority traffic (for example, media sharing or gaming applications). This traffic has a lower priority than Best-Effort.

For more information on DSCP values, see this RFC: http://www.rfc-editor.org/rfc/rfc2474.txt.

Enable QoS Marking for an Interface

You can set the default marking behavior as traffic goes out of an interface. These settings can be overridden by settings defined for a policy.

1. Select **Firewall > Traffic Management**.
   The Traffic Management page appears.
2. Clear the **Disable all Traffic Management** check box. Click **Save**.
   You might want to disable these features at a later time if you do performance testing or network debugging.
3. Select **Network > Interfaces**.
   The Network Interfaces page appears.
4. Select the interface for which you want to enable QoS Marking. Click **Configure**.
   The Interface Configuration page appears.
5. Click **Advanced**.

6. In the **Marking Type** drop-down list, select either **DSCP** or **IP Precedence**.
7. In the **Marking Method** drop-down list, select the marking method:
   - **Preserve** — Do not change the current value of the bit. The XTM device prioritizes the traffic based on this value.
   - **Assign** — Assign the bit a new value.
8. If you selected **Assign** in the previous step, select a marking value.
   If you selected the **IP precedence** marking type you can select values from 0 (normal priority) through 7 (highest priority).
   If you selected the **DSCP** marking type, the values are 0–56.
   For more information on these values, see *Marking Types and Values* on page 433.
9. Select the **Prioritize traffic based on QoS Marking** check box.
10. Click **Save**.

Enable QoS Marking or Prioritization Settings for a Policy

In addition to marking the traffic that leaves a XTM device interface, you can also mark traffic on a per-policy basis. The marking action you select is applied to all traffic that uses the policy. Multiple policies that use the same marking actions have no effect on each other. XTM device interfaces can also have their own QoS Marking settings. To use QoS Marking or prioritization settings for a policy, you must override any per-interface QoS Marking settings.

1. Select **Firewall > Firewall Policies** or **Firewall > Mobile VPN Policies**.
   The Policies page appears.
2. Select the policy you want to change. Click .
3. Select the **Advanced** tab.
4. To enable the other QoS and prioritization options, select the **Override per-interface settings** check box.
5. Complete the settings as described in the subsequent sections.
6. Click **Save**.

QoS Marking Settings

For more information on QoS marking values, see *Marking Types and Values* on page 433.

1. From the **Marking Type** drop-down list, select either **DSCP** or **IP Precedence**.
2. From the **Marking Method** drop-down list, select the marking method:

- **Preserve** — Do not change the current value of the bit. The XTM device prioritizes the traffic based on this value.
- **Assign** — Assign the bit a new value.

3. If you selected **Assign** in the previous step, select a marking value.
   If you selected the **IP precedence** marking type you can select values from 0 (normal priority) through 7 (highest priority).
   If you selected the **DSCP** marking type, the values are 0–56.
4. From the **Prioritize Traffic Based On** drop-down list, select **QoS Marking**.

Prioritization Settings

Many different algorithms can be used to prioritize network traffic. Fireware XTM uses a high performance, class-based queuing method based on the Hierarchical Token Bucket algorithm. Prioritization in Fireware XTM is applied per policy and is equivalent to CoS (class of service) levels 0–7, where 0 is normal priority (default) and 7 is the highest priority. Level 5 is commonly used for streaming data such as VoIP or video conferencing. Reserve levels 6 and 7 for policies that allow system administration connections to make sure they are always available and avoid interference from other high priority network traffic. Use the Priority Levels table as a guideline when you assign priorities.

1. From the **Prioritize Traffic Based On** drop-down list, select **Custom Value**.
2. From the **Value** drop-down list, select a priority level.

Priority Levels

We recommend that you assign a priority higher than 5 only to WatchGuard administrative policies, such as the WatchGuard policy, the WG-Logging policy, or the WG-Mgmt-Server policy. Give high priority business traffic a priority of 5 or lower.

Priority	Description
0	Routine (HTTP, FTP)
1	Priority
2	Immediate (DNS)
3	Flash (Telnet, SSH, RDP)
4	Flash Override
5	Critical (VoIP)
6	Internetwork Control (Remote router configuration)
7	Network Control (Firewall, router, switch management)

Traffic Control and Policy Definitions

Define a Traffic Management Action

Traffic Management actions can enforce bandwidth restrictions and guarantee a minimum amount of bandwidth for one or more policies. Each Traffic Management action can include settings for multiple interfaces. For example, on a Traffic Management action used with an HTTP policy for a small organization, you can set the minimum guaranteed bandwidth of a trusted interface to 250 kbps and the maximum bandwidth to 1000 kbps. This limits the speeds at which users can download files, but ensures that a small amount of bandwidth is always available for HTTP traffic. You can then set the minimum guaranteed bandwidth of an external interface to 150 kbps and the maximum bandwidth to 300 kbps to manage upload speeds at the same time.

Determine Available Bandwidth

Before you begin, you must determine the available bandwidth of the interface used for the policy or policies you want to guarantee bandwidth. For external interfaces, you can contact your ISP (Internet Service Provider) to verify the service level agreement for bandwidth. You can then use a speed test with online tools to verify this value. These tools can produce different values depending on a number of variables. For other interfaces, you can assume the link speed on the XTM device interface is the theoretical maximum bandwidth for that network. You must also consider both the sending and receiving needs of an interface and set the threshold value based on these needs. If your Internet connection is asymmetric, use the uplink bandwidth set by your ISP as the threshold value.

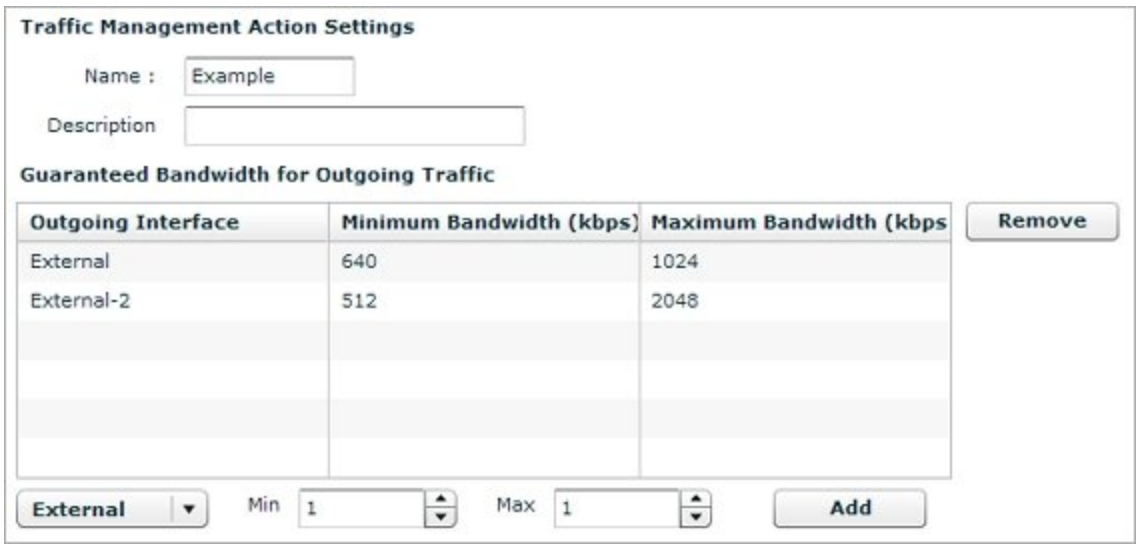
Determine the Sum of Your Bandwidth

You must also determine the sum of the bandwidth you want to guarantee for all policies on a given interface. For example, on a 1500 kbps external interface, you might want to reserve 600 kbps for all the guaranteed bandwidth and use the remaining 900 kbps for all other traffic.

All policies that use a given Traffic Management action share its connection rate and bandwidth settings. When they are created, policies automatically belong to the default Traffic Management action, which enforces no restrictions or reservations. If you create a Traffic Management action to set a maximum bandwidth of 10 Mbps and apply it to an FTP and an HTTP policy, all connections handled by those policies must share 10Mbps. If you later apply the same Traffic Management action to an SMTP policy, all three must share 10 Mbps. This also applies to connection rate limits and guaranteed minimum bandwidth. Unused guaranteed bandwidth reserved by one Traffic Management action can be used by others.

Create or Modify a Traffic Management Action

1. Select **Firewall > Traffic Management**.
   The Traffic Management page appears.
2. Click **Add** to create a new Traffic Management action.
   Or, select an action and click **Configure**.



3. Type a **Name** and a **Description** (optional) for the action. You use the action name to refer to the action when you assign it to a policy.
4. In the drop-down list, select an interface. Type the minimum and maximum bandwidth for that interface in the adjacent text boxes.
5. Click **Add**.
6. Repeat Steps 4–5 to add traffic limits for additional interfaces.
7. To remove an interface from the Traffic Management action, select it and click **Remove**.
8. Click **Save**.

You can now apply this Traffic Management action to one or more policies.

Add a Traffic Management Action to a Policy

After you *Define a Traffic Management Action*, you can add it to policy definitions. You can also add any existing traffic management actions to policy definitions.

1. Select **Firewall > Traffic Management**.
   The Traffic Management page appears.
2. In the **Traffic Management Policies** list, select a policy.

3. In the adjacent column, click the drop-down list and select a traffic management action.
4. To set an action for other policies, repeat Steps 2–3.

5. Click **Save**.

> ***Note*** *If you have a multi-WAN configuration, bandwidth limits are applied separately to each interface.*

Add a Traffic Management Action to Multiple Policies

When the same traffic management action is added to multiple policies, the maximum and minimum bandwidth apply to each interface in your configuration. If two policies share an action that has a maximum bandwidth of 100 kbps on a single interface, then all traffic on that interface that matches those policies is limited to 100 kbps total.

If you have limited bandwidth on an interface used for several applications, each with unique ports, you might need all the high priority connections to share one traffic management action. If you have lots of bandwidth to spare, you could create separate traffic management actions for each application.

15 Default Threat Protection

About Default Threat Protection

WatchGuard Fireware XTM OS and the policies you create give you strict control over access to your network. A strict access policy helps keep hackers out of your network. But, there are other types of attacks that a strict policy cannot defeat. Careful configuration of default threat protection options for the XTM device can stop threats such as SYN flood attacks, spoofing attacks, and port or address space probes.

With default threat protection, a firewall examines the source and destination of each packet it receives. It looks at the IP address and port number and monitors the packets to look for patterns that show your network is at risk. If a risk exists, you can configure the XTM device to automatically block a possible attack. This proactive method of intrusion detection and prevention keeps attackers out of your network.

To configure default threat protection, see:

- *About Default Packet Handling Options*
- *About Blocked Sites*
- *About Blocked Ports*

You can also purchase an upgrade for your XTM device to use signature-based intrusion prevention. For more information, see *About Gateway AntiVirus* on page 707.

About Default Packet Handling Options

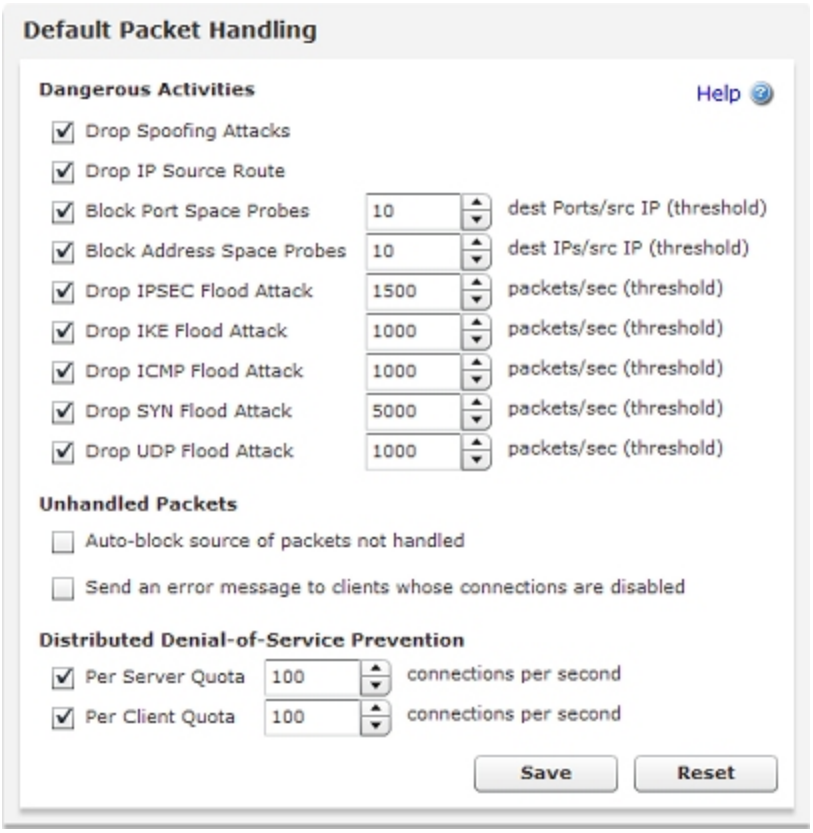
When your XTM device receives a packet, it examines the source and destination for the packet. It looks at the IP address and the port number. The device also monitors the packets to look for patterns that can show your network is at risk. This process is called *default packet handling*.

Default packet handling can:

- Reject a packet that could be a security risk, including packets that could be part of a spoofing attack or SYN flood attack
- Automatically block all traffic to and from an IP address
- Add an event to the log file
- Send an SNMP trap to the SNMP management server
- Send a notification of possible security risks

Most default packet handling options are enabled in the default XTM device configuration. You can use Fireware XTM Web UI to change the thresholds at which the XTM device takes action. You can also change the options selected for default packet handling.

1. Select **Firewall > Default Packet Handling**.
   The Default Packet Handling page appears.



2. Select the check boxes for the traffic patterns you want to take action against, as explained in these topics:

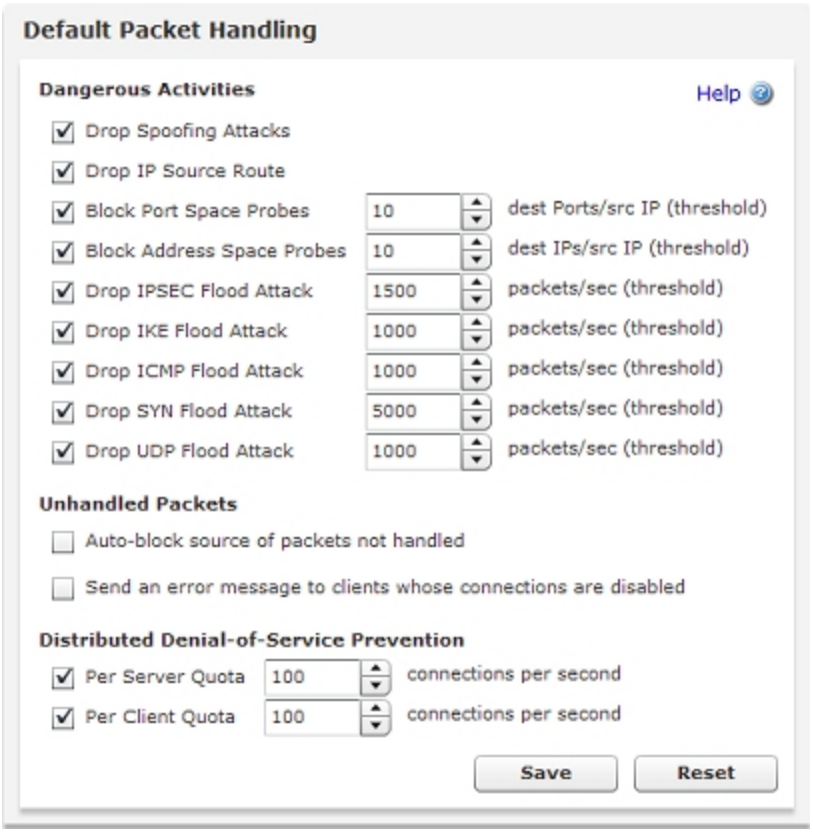
About Spoofing Attacks

One method that attackers use to enter your network is to make an *electronic false identity*. This is an *IP spoofing* method that attackers use to send a TCP/IP packet with a different IP address than the computer that first sent it.

When anti-spoofing is enabled, the XTM device verifies the source IP address of a packet is from a network on the specified interface.

The default configuration of the XTM device is to drop spoofing attacks. From Fireware XTM Web UI, you can change the settings for this feature:

1. Select **Firewall > Default Packet Handling**.
   The Default Packet Handling page appears.



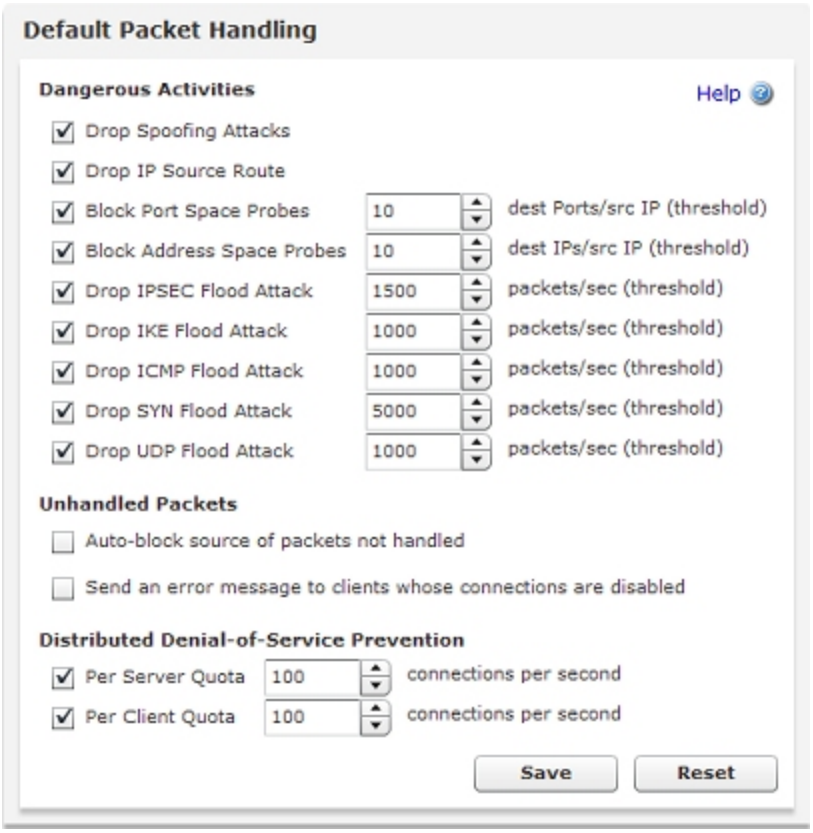
2. Select or clear the **Drop Spoofing Attacks** check box.
3. Click **Save**.

About IP Source Route Attacks

To find the route that packets take through your network, attackers use IP source route attacks. The attacker sends an IP packet and uses the response from your network to get information about the operating system of the target computer or network device.

The default configuration of the XTM device is to drop IP source route attacks. From Fireware XTM Web UI, you can change the settings for this feature.

1. Select **Firewall > Default Packet Handling**.
   The Default Packet Handling page appears.



2. Select or clear the **Drop IP Source Route** check box.
3. Click **Save**.

About Port Space and Address Space Probes

Attackers frequently look for open ports as starting points to launch network attacks. A *port space probe* is TCP or UDP traffic that is sent to a range of ports. These ports can be in sequence or random, from 0 to 65535. An *address space probe* is TCP or UDP traffic that is sent to a range of network addresses. Port space probes examine a computer to find the services that it uses. Address space probes examine a network to see which network devices are on that network.

For more information about ports, see *About Ports* on page 8.

How the XTM Device Identifies Network Probes

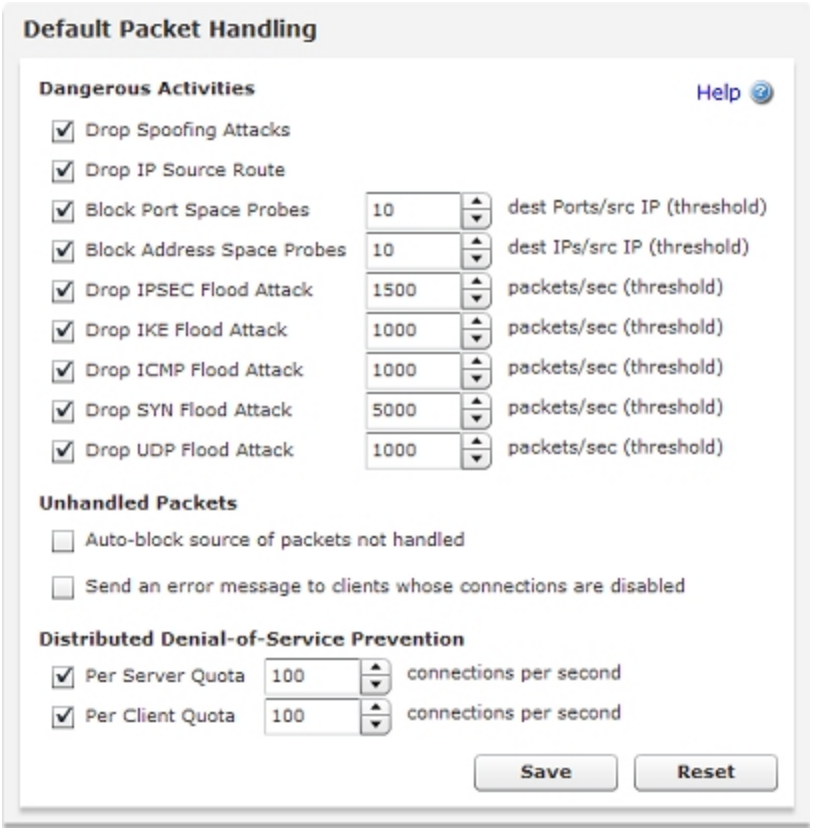
An address space probe is identified when a computer sends a specified number of packets to different IP addresses assigned to an XTM device interface. To identify a port space probe, your XTM device counts the number of packets sent from one IP address to any XTM device interface IP address. The addresses can include the primary IP addresses and any secondary IP addresses configured on the interface. If the number of packets sent to different IP addresses or destination ports in one second is larger than the number you select, the source IP address is added to the Blocked Sites list.

When the **Block Port Space Probes** and **Block Address Space Probes** check boxes are selected, all incoming traffic on all interfaces is examined by the XTM device. You cannot disable these features for specified IP addresses, specified XTM device interfaces, or different time periods.

To Protect Against Port Space and Address Space Probes

The default configuration of the XTM device blocks network probes. You can use Fireware XTM Web UI to change the settings for this feature, and change the maximum allowed number of address or port probes per second for each source IP address (the default value is 50).

1. Select **Firewall > Default Packet Handling**.
   The Default Packet Handling page appears.



2. Select or clear the **Block Port Space Probes** and the **Block Address Space Probes** check boxes.
3. Click the arrows to select the maximum number of address or port probes to allow per second from the same IP address. The default for each is 10 per second. This means that a source is blocked if it initiates connections to 10 different ports or hosts within one second.
4. Click **Save**.

To block attackers more quickly, you can set the threshold for the maximum allowed number of address or port probes per second to a lower value. If the number is set too low, the XTM device could also deny legitimate network traffic . You are less likely to block legitimate network traffic if you use a higher number, but the XTM device must send TCP reset packets for each connection it drops. This uses bandwidth and resources on the XTM device and provides the attacker with information about your firewall.

About Flood Attacks

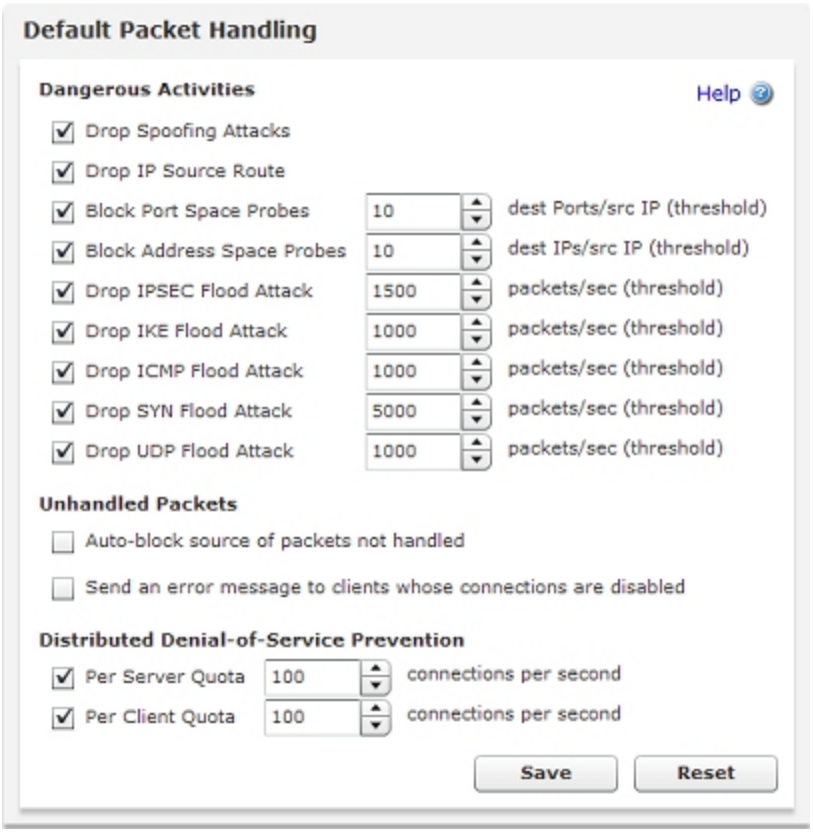
In a flood attack, attackers send a very high volume of traffic to a system so it cannot examine and allow permitted network traffic. For example, an ICMP flood attack occurs when a system receives too many ICMP ping commands and must use all of its resources to send reply commands. The XTM device can protect against these types of flood attacks:

- IPSec
- IKE
- ICMP
- SYN
- UDP

Flood attacks are also known as Denial of Service (DoS) attacks. The default configuration of the XTM device is to block flood attacks.

You can use Fireware XTM Web UI to change the settings for this feature, or to change the maximum allowed number of packets per second.

1. Select **Firewall > Default Packet Handling**.
   The Default Packet Handling page appears.



2. Select or clear the **Flood Attack** check boxes.
3. Click the arrows to select the maximum allowed number of packets per second for each source IP address.
   For example, if the setting is 1000, the XTM device blocks a source if it receives more than 1000 packets per second from that source.
4. Click **Save**.

About the SYN Flood Attack Setting

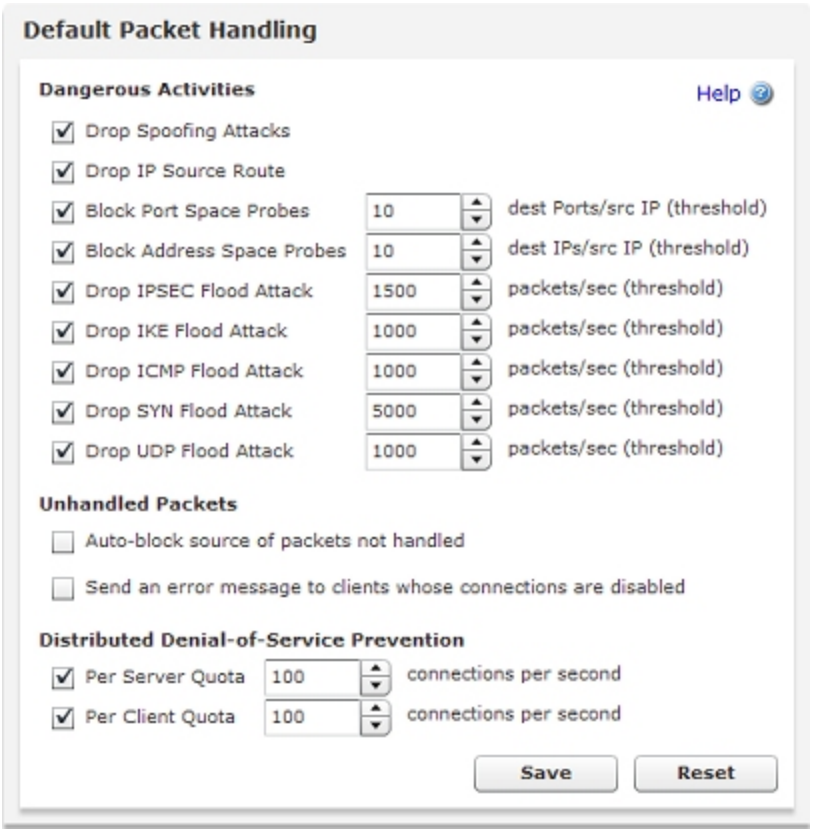
For SYN flood attacks, you can set the threshold at which the XTM device reports a possible SYN flood attack, but no packets are dropped if only the number of packets you selected are received. At twice the selected threshold, all SYN packets are dropped. At any level between the selected threshold and twice that level, if the src_IP, dst_IP, and total_length values of a packet are the same as the previous packet received, then it is always dropped. Otherwise, 25% of the new packets received are dropped.

For example, you set the SYN flood attack threshold to 18 packets/sec. When the XTM device receives 18 packets/sec, it reports a possible SYN flood attack to you, but does not drop any packets. If the device receives 20 packets per second, it drops 25% of the received packets (5 packets). If the device receives 36 or more packets, the last 18 or more are dropped.

About Unhandled Packets

An *unhandled* packet is a packet that does not match any policy rule. By default, the XTM device always denies unhandled packets. From Fireware XTM Web UI, you can change the device settings to further protect your network.

1. Select **Firewall > Default Packet Handling**.
   The Default Packet Handling page appears.



2. Select or clear the check boxes for these options:

   Auto-block source of packets not handled

   Select to automatically block the source of unhandled packets. The XTM device adds the IP address that sent the packet to the temporary Blocked Sites list.

   Send an error message to clients whose connections are disabled

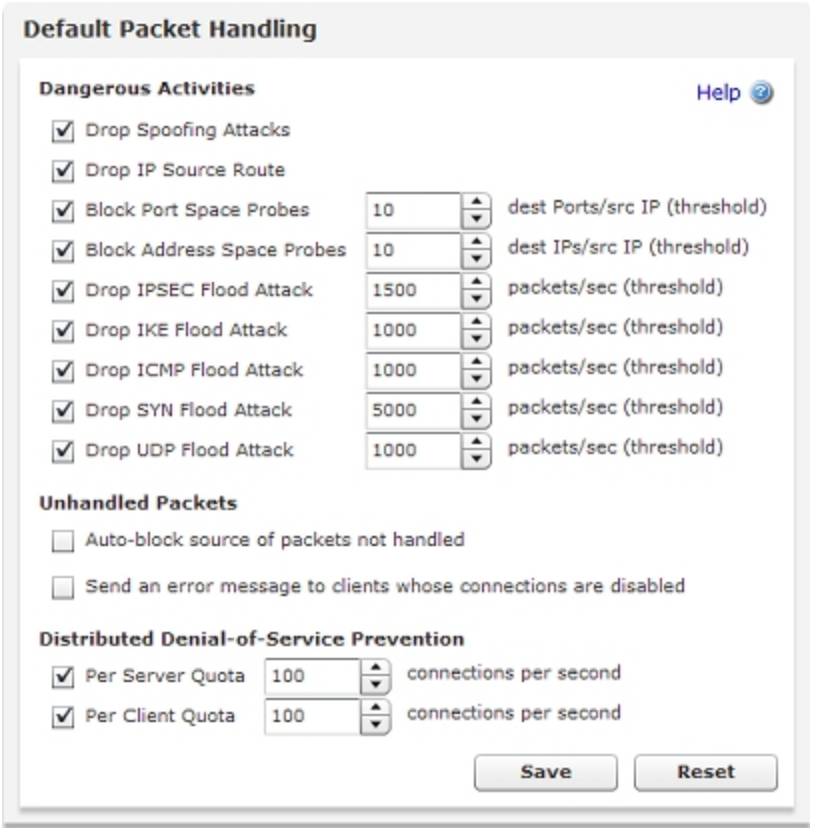
   Select to send a TCP reset or ICMP error back to the client when the XTM device receives an unhandled packet.

About Distributed Denial-of-Service Attacks

Distributed Denial of Service (DDoS) attacks are very similar to flood attacks. In a DDoS attack, many different clients and servers send connections to one computer system to try to flood the system. When a DDoS attack occurs, legitimate users cannot use the targeted system.

The default configuration of the XTM device is to block DDoS attacks. From Fireware XTM Web UI, you can change the settings for this feature, and change the maximum allowed number of connections per second.

1. Select **Firewall > Default Packet Handling**.
   The Default Packet Handling page appears.



2. Select or clear the **Per Server Quota** and **Per Client Quota** check boxes.
3. Click the arrows to set the **Per Server Quota** and the **Per Client Quota**.

Per Server Quota

The Per Server Quota applies a limit to the number of connections per second from any external source to the XTM device external interface. This includes connections to internal servers allowed by a static NAT policy. For example, when the Per Server Quota is set to the default value of 100, the XTM device drops the 101st connection request received in a one second time frame from an external IP address. The IP address is not added to the blocked sites list.

Per Client Quota

The Per Client Quota applies a limit to the number of outbound connections per second from any source protected by the XTM device to any one destination. For example, when the Per Client Quota is set to the default value of 100, the XTM device drops the 101st connection request received in a one second time frame from an IP address on the trusted or optional network to any one destination IP address.

About Blocked Sites

A blocked site is an IP address that cannot make a connection through the XTM device. You tell the XTM device to block specific sites you know, or think, are a security risk. After you find the source of suspicious traffic, you can block all connections from that IP address. You can also configure the XTM device to send a log message each time the source tries to connect to your network. From the log file, you can see the services that the sources use to launch attacks.

The XTM device denies all traffic from a blocked IP address. You can define two different types of blocked IP addresses: permanent and auto-blocked.

Permanently Blocked Sites

Network traffic from permanently blocked sites is always denied. These IP addresses are stored in the Blocked Sites list and must be added manually. For example, you can add an IP address that constantly tries to scan your network to the Blocked Sites list to prevent port scans from that site.

To block a site, see *Block a Site Permanently* on page 451.

Auto-Blocked Sites/Temporary Blocked Sites List

Packets from auto-blocked sites are denied for the amount of time you specify. The XTM device uses the packet handling rules specified for each policy to determine whether to block a site. For example, if you create a policy that denies all traffic on port 23 (Telnet), any IP address that tries to send Telnet traffic through that port is automatically blocked for the amount of time you specify.

To automatically block sites that send denied traffic, see *Block Sites Temporarily with Policy Settings* on page 452.

You can also automatically block sites that are the source of packets that do not match any policy rule. For more information, see *About Unhandled Packets* on page 448.

Blocked Site Exceptions

If the XTM device blocks traffic from a site you believe to be safe, you can add the site to the Blocked Site Exceptions list, so that traffic from that site is not automatically blocked.

To add a blocked site exception, see *Create Blocked Site Exceptions*.

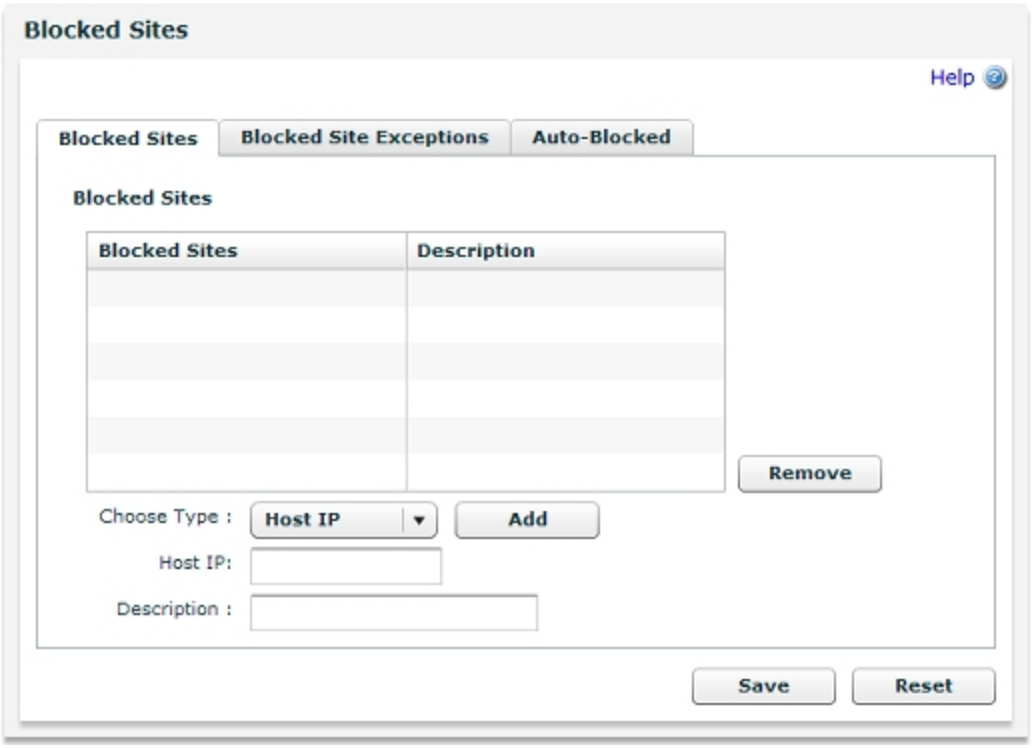
See and Edit the Sites on the Blocked Sites List

To see a list of all sites currently on the blocked sites list, select **System Status > Blocked Sites**.
For more information, see *Blocked Sites* on page 476.

Block a Site Permanently

You can use Fireware XTM Web UI to permanently add sites to the Blocked Sites list.

1. Select **Firewall > Blocked Sites**.

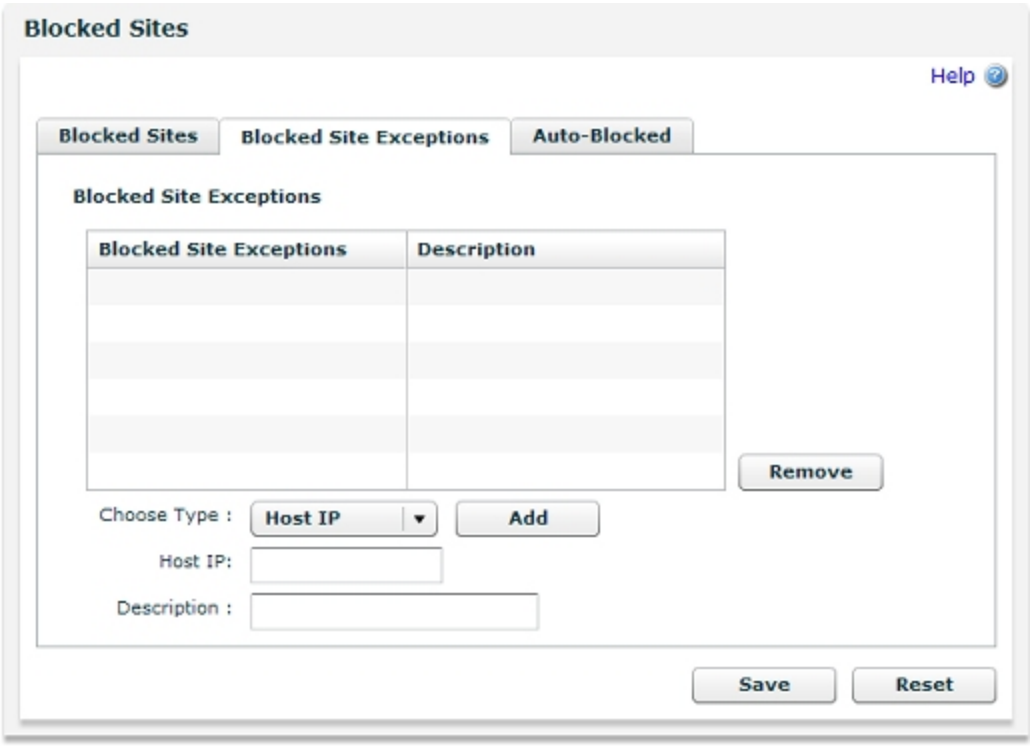


2. From the **Choose Type** drop-down list, select whether you want to enter a host IP address, a network address, or a range of IP addresses.
3. Type the value in the subsequent text box and click **Add**. If you must block an address range that includes one or more IP addresses assigned to the XTM device, you must first add these IP addresses to the Blocked Sites Exceptions list.
   To add exceptions, see *Create Blocked Site Exceptions* on page 451.
4. Click **Save**.

Create Blocked Site Exceptions

When you add a site to the Blocked Site Exceptions list in Fireware XTM Web UI, the traffic from that site is not blocked by the auto-blocking feature.

1. Select **Firewall > Blocked Sites**.
2. Click the **Blocked Site Exceptions** tab.



3. From the **Choose Type** drop-down list, select whether you want to enter a host IP address, a network address, or a range of IP addresses.
4. Type the value in the subsequent text box and click **Add**.
5. Click **Save**.

Block Sites Temporarily with Policy Settings

You can use Fireware XTM Web UI to temporarily block sites that try to use a denied service. IP addresses from the denied packets are added to the Temporary Blocked sites list for 20 minutes (by default).

1. Select **Firewall > Firewall Policies**. Double-click a policy to edit it.
   The Policy Configuration dialog box appears.
2. On the **Policy** tab, make sure you set the **Connections Are** drop-down list to **Denied** or **Denied (send reset)**.
3. On the **Properties** tab, select the **Auto-block sites that attempt to connect** check box. By default, IP addresses from the denied packets are added to the Temporary Blocked Sites list for 20 minutes.

Change the Duration that Sites are Auto-Blocked

To see a list of IP addresses that are auto-blocked by the XTM device, select **System Status > Blocked Sites**. You can use the Temporary Blocked Sites list together and your log messages to help you decide which IP addresses to block permanently.

You can use Fireware XTM Web UI to enable the auto-block feature.

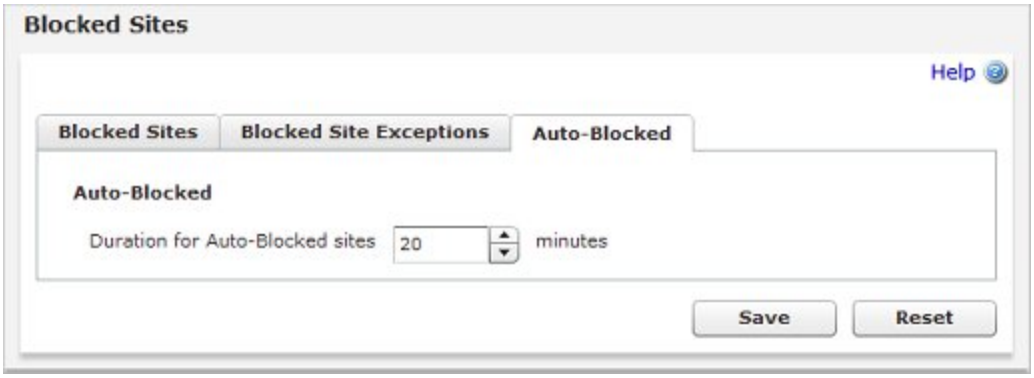
Select **Firewall > Default Packet Handling**.

For more information, see *About Unhandled Packets* on page 448.

You can also use policy settings to auto-block sites that try to use a denied service. For more information, see *Block Sites Temporarily with Policy Settings* on page 452.

You can use Fireware XTM Web UI to set the duration that sites are blocked automatically.

1. Select **Firewall > Blocked Sites**.
2. Select the **Auto-Blocked** tab.



3. To change the amount of time a site is auto-blocked, in the **Duration for Auto-Blocked sites** text box, type or select the number of minutes to block a site. The default is 20 minutes.
4. Click **Save**.

About Blocked Ports

You can block the ports that you know can be used to attack your network. This stops specified external network services. Blocking ports can protect your most sensitive services.

When you block a port, you override all of the rules in your policy definitions. To block a port, see *Block a Port* on page 455.

Default Blocked Ports

In the default configuration, the XTM device blocks some destination ports. You usually do not need to change this default configuration. TCP and UDP packets are blocked for these ports:

X Window System (ports 6000-6005)

The X Window System (or X-Windows) client connection is not encrypted and is dangerous to use on the Internet.

X Font Server (port 7100)

Many versions of X Windows operate X Font Servers. The X Font Servers operate as the super-user on some hosts.

NFS (port 2049)

NFS (Network File System) is a frequently used TCP/IP service where many users use the same files on a network. New versions have important authentication and security problems. To supply NFS on the Internet can be very dangerous.

> ***Note*** *The portmapper frequently uses port 2049 for NFS. If you use NFS, make sure that NFS uses port 2049 on all your systems.*

rlogin, rsh, rcp (ports 513, 514)

These services give remote access to other computers. They are a security risk and many attackers probe for these services.

RPC portmapper (port 111)

The RPC Services use port 111 to find which ports a given RPC server uses. The RPC services are easy to attack through the Internet.

port 8000

Many vendors use this port, and many security problems are related to it.

port 1

The TCPmux service uses Port 1, but not frequently. You can block it to make it more difficult for tools that examine ports.

port 0

This port is always blocked by the XTM device. You cannot allow traffic on port 0 through the device.

> ***Note*** *If you must allow traffic through any of the default blocked ports to use the associated software applications, we recommend that you allow the traffic only through a VPN tunnel or use SSH (Secure Shell) with those ports.*

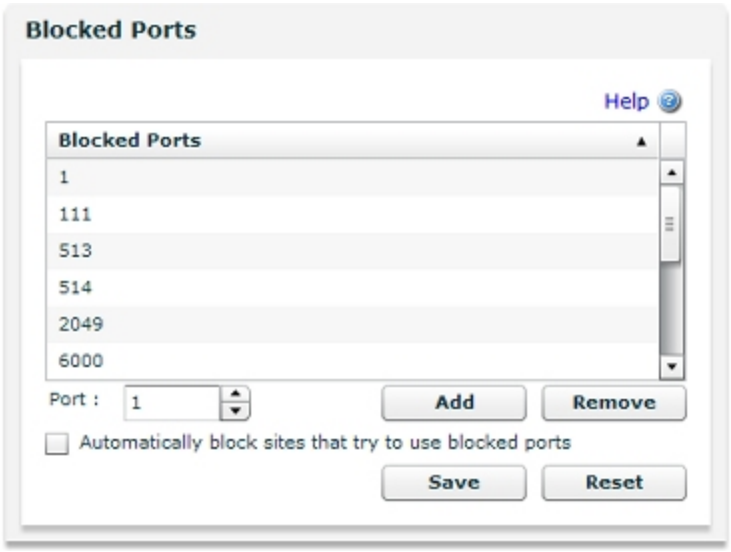
Block a Port

You can use Fireware XTM Web UI to add a port number to the Blocked Ports list.

> ***Note*** *Be very careful if you block port numbers higher than 1023. Clients frequently use these source port numbers.*

To add a port number to the Blocked Ports list:

1. Select **Firewall > Blocked Ports**.
2. In the **Port** text box, type or select the port number to block.
3. Click **Add**.
   The new port number appears in the Blocked Ports list.



Block IP Addresses That Try to Use Blocked Ports

You can configure the XTM device to automatically block an external computer that tries to use a blocked port. In the **Blocked Ports** page, select the **Automatically block sites that try to use blocked ports** check box.

16 Logging and Notification

About Logging and Log Files

An important feature of network security is to gather messages from your security systems, to examine those records frequently, and to keep them in an archive for future reference. The WatchGuard log message system creates log files with information about security related events that you can review to monitor your network security and activity, identify security risks, and address them.

A *log file* is a list of events, along with information about those events. An *event* is one activity that occurs on the XTM device. An example of an event is when the device denies a packet. Your XTM device can also capture information about allowed events to give you a more complete picture of the activity on your network.

The log message system has several components, which are described below.

Log Servers

There are two methods to save log files with Fireware XTM Web UI:

WatchGuard Log Server

This is a component of WatchGuard System Manager (WSM). If you have a Firebox III, Firebox X Core or Firebox X Peak, Firebox X Edge with Fireware XTM, or WatchGuard XTM 2 Series, 5 Series, 8 Series, or 1050, you can configure a primary Log Server to collect log messages.

Syslog

This is a log interface developed for UNIX but also used on many other computer systems. If you use a syslog host, you can set your XTM device to send log messages to your syslog server. To find a syslog server compatible with your operating system, search the Internet for "syslog daemon".

If your XTM device is configured to send log files to a WatchGuard Log Server and the connection fails, the log files are not collected. You can configure your device to also send log messages to a syslog host that is on the local trusted network to prevent the loss of log files.

For more information about sending log messages to a WatchGuard Log Server, see *Send Log Messages to a WatchGuard Log Server* on page 460.

For more information about sending log messages to a syslog host, see *Send Log Information to a Syslog Host* on page 461.

System Status Syslog

The Fireware XTM Web UI **Syslog** page shows real-time log message information that includes data on the most recent activity on the XTM device.

For more information, see *Use Syslog to See Log Message Data* on page 467.

Logging and Notification in Applications and Servers

The Log Server can receive log messages from your XTM device or a WatchGuard server. After you have configured your XTM device and Log Server, the device sends log messages to the Log Server. You can enable logging in the various WatchGuard System Manager applications and policies that you have defined for your XTM device to control the level of logs that you see. If you choose to send log messages from another WatchGuard server to the Log Server, you must first enable logging on that server.

About Log Messages

Your XTM device sends log messages to the Log Server. It can also send log messages to a syslog server or keep logs locally on the XTM device. You can choose to send logs to one or both of these locations.

Types of Log Messages

Your XTM device sends several types of log messages for events that occur on the device. Each message includes the message type in the text of the message. The log messages types are:

- Traffic
- Alarm
- Event
- Debug
- Statistic

Traffic Log Messages

The XTM device sends traffic log messages as it applies packet filter and proxy rules to traffic that goes through the device.

Alarm Log Messages

Alarm log messages are sent when an event occurs that triggers the XTM device to run a command. When the alarm condition is matched, the device sends an Alarm log message to the Log Server or syslog server, and then it does the specified action.

There are eight categories of Alarm log messages:

- System
- IPS
- AV
- Policy
- Proxy
- Counter
- Denial of Service
- Traffic

The XTM device does not send more than 10 alarms in 15 minutes for the same conditions.

Event Log Messages

The XTM device sends event log messages because of user activity. Actions that can cause the XTM device to send an event log message include:

- Device start up and shut down
- Device and VPN authentication
- Process start up and shut down
- Problems with the device hardware components
- Any task done by the device administrator

Debug Log Messages

Debug log messages include diagnostic information that you can use to help troubleshoot problems. There are 27 different product components that can send debug log messages.

Statistic Log Messages

Statistic log messages include information about the performance of the XTM device. By default, the device sends log messages about external interface performance and VPN bandwidth statistics to your log file. You can use these logs to change your XTM device settings as necessary to improve performance.

Send Log Messages to a WatchGuard Log Server

The WatchGuard Log Server is a component of WatchGuard System Manager. If you have WatchGuard System Manager, you can configure a primary Log Server and backup Log Servers to collect the log messages from your XTM devices. You designate one Log Server as the primary (Priority 1) and other Log Servers as backup servers.

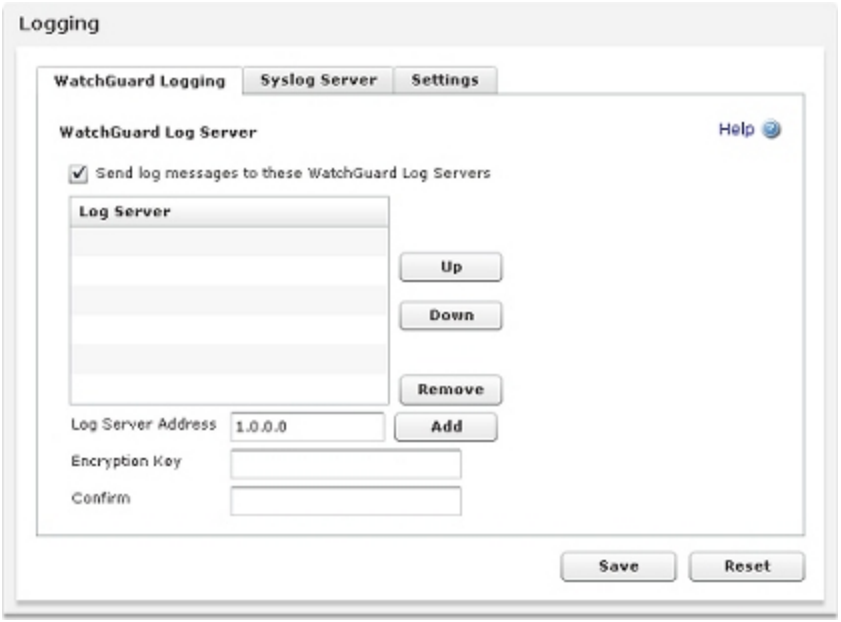
If the XTM device cannot connect to the primary Log Server, it tries to connect to the next Log Server in the priority list. If the XTM device examines each Log Server in the list and cannot connect, it tries to connect to the first Log Server in the list again. When the primary Log Server is not available, and the XTM device is connected to a backup Log Server, the XTM device tries to reconnect to the primary Log Server every 6 minutes. This does not impact the XTM device connection to the backup Log Server until the primary Log Server is available.

For more information about WatchGuard Log Servers and instructions to configure the Log Server to accept log messages, see the *Fireware XTM WatchGuard System Manager Help* or *User Guide*.

Add, Edit, or Change the Priority of Log Servers

To send log messages from your XTM device to a WatchGuard Log Server:

1. Select **System > Logging**.
   The Logging page appears.



2. To send log messages to one or more WatchGuard Log Servers, select the **Send log messages to these WatchGuard Log Servers** check box.
3. In the **Log Server Address** text box, type the IP address of the primary Log Server.
4. In the **Encryption Key** text box, type the Log Server encryption key.
5. In the **Confirm** text box, type the encryption key again.
6. Click **Add**.
   The information for the Log Server appears in the Log Server list.
7. Repeat Steps 3–6 to add more Log Servers to the **Server** list.
8. To change the priority of a Log Server in the list, select an IP address in the list and click **Up** or **Down**. The priority number changes as the IP address moves up or down in the list.
9. Click **Save**.

Send Log Information to a Syslog Host

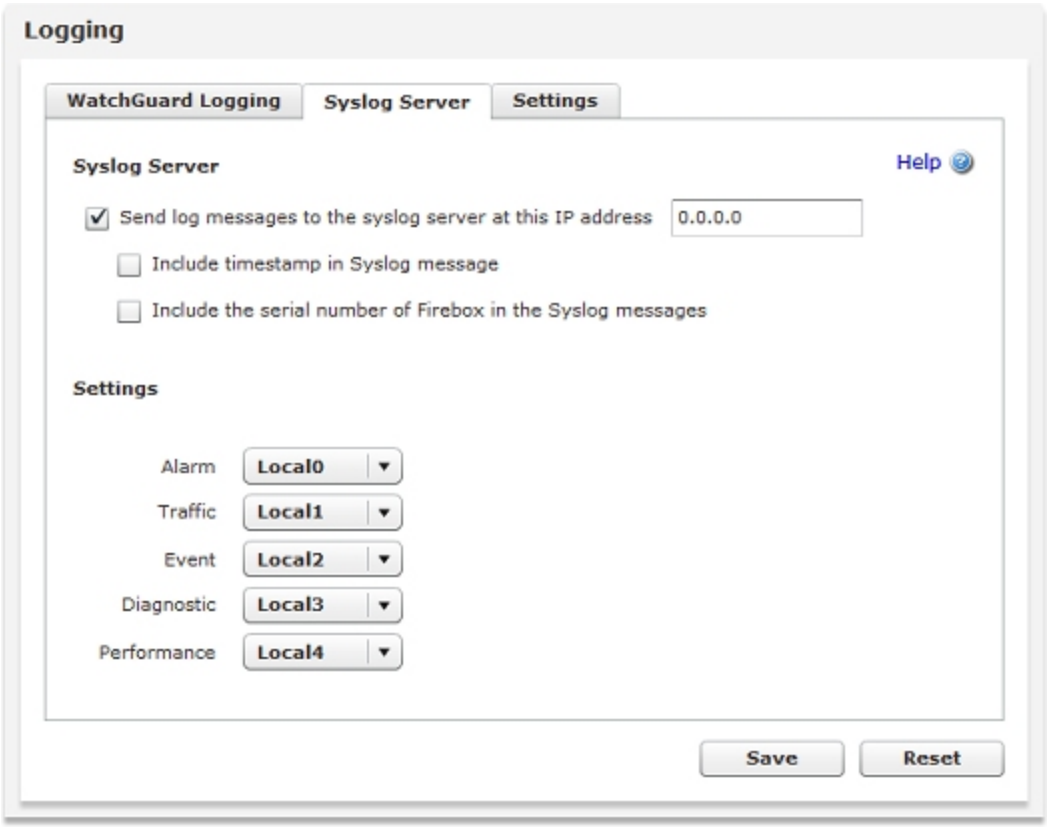
Syslog is a log interface developed for UNIX but also used by a number of other computer systems. You can configure the XTM device to send log information to a syslog server. An XTM device can send log messages to a WatchGuard Log Server or a syslog server, or to both at the same time. Syslog log messages are not encrypted. We recommend that you do not select a syslog host on the external interface.

When you configure the settings for the syslog server, you specify the syslog facility to use for your log messages. The syslog facility refers to one of the fields in the syslog packet and to the file where syslog sends a log message. For high priority syslog messages, such as alarms, you can select**Local0**. To assign priorities for other types of log messages (lower numbers have greater priority), you can select **Local1**–**Local7**. For more information on logging facilities, see your syslog documentation .

For information about the different types of messages, see *Types of Log Messages* on page 459.

To configure the XTM device to send log messages to a syslog host, you must have a syslog host configured, operational, and ready to receive log messages.

1. Select **System > Logging**.
   The Logging page appears.
2. Select the **Syslog Server** tab.
3. Select the **Send log messages to the syslog server at this IP address** check box.



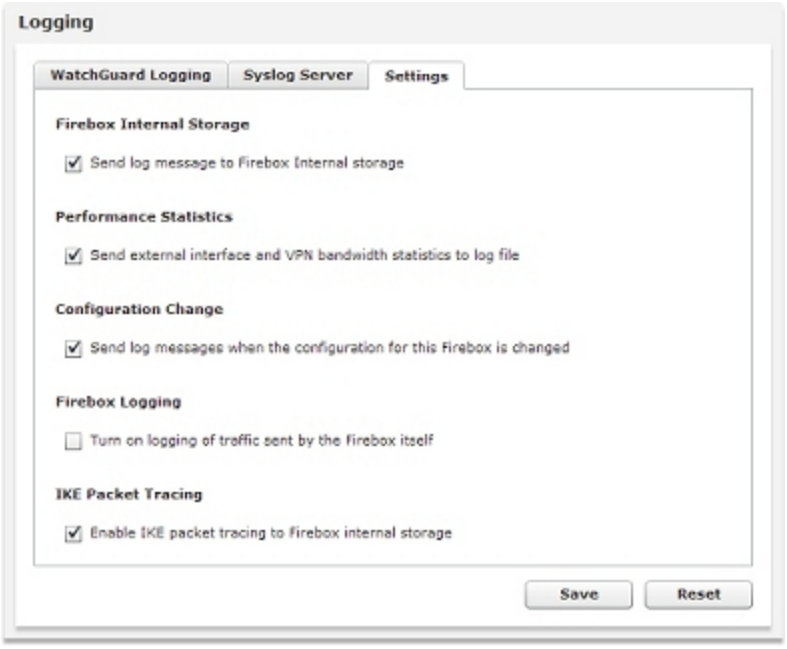
4. In the **Send log messages to the syslog server at this IP address** text box, type the IP address of the syslog host.
5. In the **Settings** section, for each type of log message, select a syslog facility from the drop-down list. If you select **NONE**, details for that message type are not sent to the syslog host.
6. Click **Save**.

> ***Note*** *Because syslog traffic is not encrypted, syslog messages that are sent through the Internet decrease the security of the trusted network. It is more secure if you put your syslog host on your trusted network.*

Configure Logging Settings

You can choose to save log messages on your XTM device and select the performance statistics to include in your log files.

1. Select **System > Logging**.
   The Logging page appears.
2. Select the **Settings** tab.



3. To store log messages on your XTM device, select the **Send log message to Firebox Internal storage** check box.
4. To include performance statistics in your log files, select the **Enter external interface and VPN bandwidth statistics in log file** check box.
5. To send a log message when the XTM device configuration file is changed, select the **Send log messages when the configuration for this Firebox is changed** check box.
6. To send log messages about traffic sent by the XTM device, select the **Turn on logging of traffic sent by the Firebox itself** check box.
7. To enable the XTM device to collect a packet trace for IKE packets, select the **Enable IKE packet tracing to Firebox internal storage** check box
8. Click **Save**.

Set the Diagnostic Log Level

From Fireware XTM Web UI you can select the level of diagnostic logging to write to your log file. We do not recommend that you select the highest logging level unless a technical support representative tells you to do so while you troubleshoot a problem. When you use the highest diagnostic log level, the log file can fill up very quickly, and performance of the XTM device is often reduced.

1. Select **System > Diagnostic Log**.
   The Diagnostic Log Level page appears.

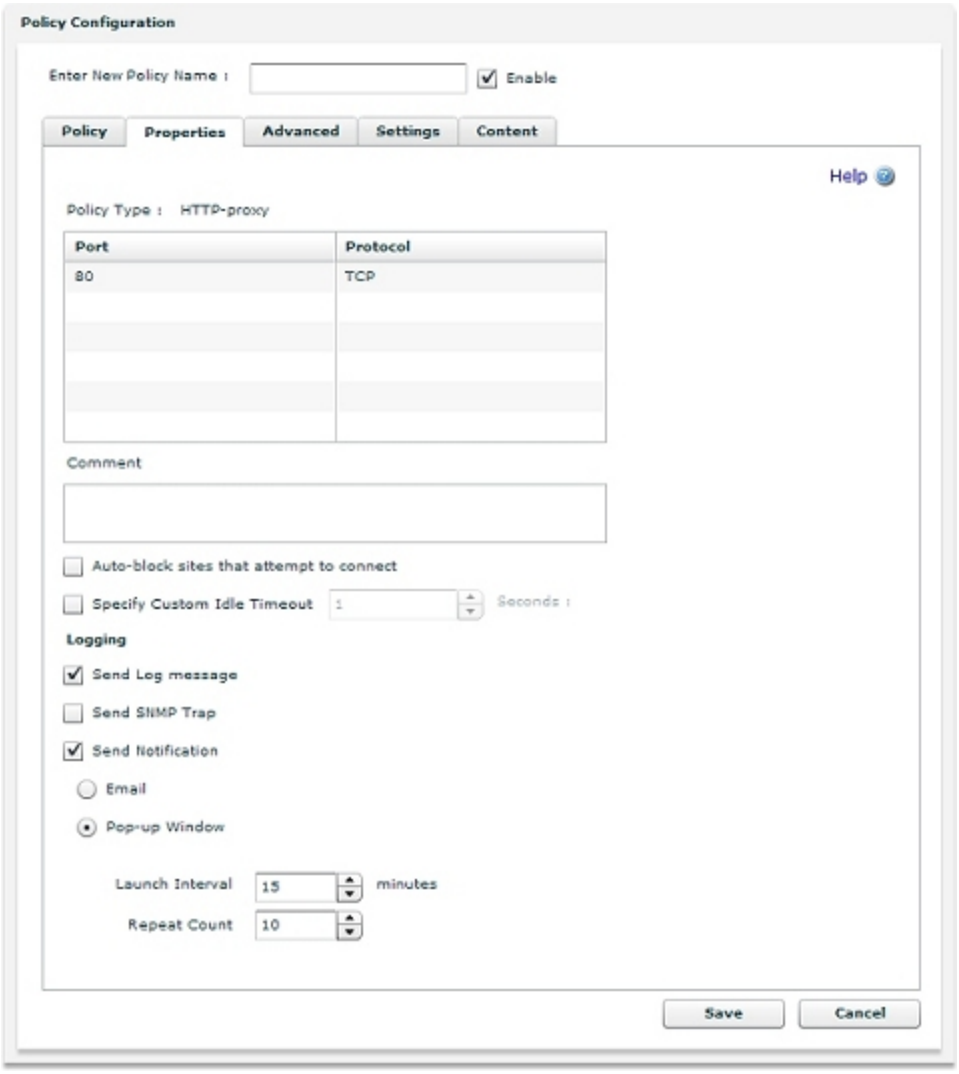
2. Use the scroll bar to find a category.
3. From the drop-down list for the category, select the level of detail to include in the log message for the category:
   - Off
   - Error
   - Warning
   - Information
   - Debug

   When **Off** (the lowest level) is selected, diagnostic messages for that category are disabled.
4. Click **Save**.

Configure Logging and Notification for a Policy

You can configure the logging and notification settings for each policy in your configuration. To see information about a policy in your log files, you must enable logging for that policy.

1. Select **Firewall > Firewall Policies**.
   The Firewall Policies page appears.
2. Add a policy, or double-click a policy.
   The Policy Configuration page appears.
3. Select the **Properties** tab.



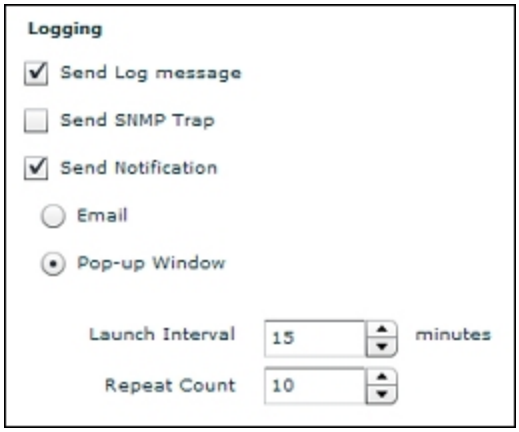
4. In the **Logging** section, set the parameters to match your security policy.

   For information about the settings in the **Logging** section, see *Set Logging and Notification Preferences* on page 466.

5. Click **Save**.

Set Logging and Notification Preferences

The settings for logging and notification are similar throughout the XTM device configuration. For each place you define logging and notification preferences, most or all of the options described below are available.



Send Log message

When you select this check box, the XTM device sends a log message when an event occurs.

You can select to send log messages to a WatchGuard Log Server, Syslog server, or XTM device internal storage. For detailed steps to select a destination for your log messages, see *Configure Logging Settings* on page 463.

Send SNMP trap

When you select this check box, the XTM device sends an event notification to the SNMP management system. Simple Network Management Protocol (SNMP) is a set of tools used to monitor and manage networks. A SNMP trap is an event notification the XTM device sends to the SNMP management system when a specified condition occurs.

> ***Note*** *If you select the **Send SNMP Trap** check box and you have not yet configured SNMP, a dialog box appears and asks you if you want to do this. Click **Yes** to go to the **SNMP Settings** dialog box. You cannot send SNMP traps if you do not configure SNMP.*

For more information about SNMP, see *About SNMP* on page 58.

To enable SNMP traps or inform requests, see *Enable SNMP Management Stations and Traps* on page 61.

Send Notification

When you select this check box, the XTM device sends a notification when the event you specified occurs. For example, when a policy allows a packet.

You can select how the XTM device sends the notification:

- **Email** — The Log Server sends an email message when the event occurs.
- **Pop-up Window** — The Log Server opens a dialog box when the event occurs.
  Set the:
  Launch Interval — The minimum time (in minutes) between different notifications. This parameter prevents more than one notification in a short time for the same event.
  Repeat Count — This setting tracks how frequently an event occurs. When the number of events reaches the selected value, a special repeat notification starts. This notification creates a repeat log entry about that specified notification. Notification starts again after the number of events you specify in this field occurs.

For example, set the **Launch interval** to 5 minutes and the **Repeat count** to 4. A port space probe starts at 10:00 AM. and continues each minute. This starts the logging and notification mechanisms. These actions occur at these times:

- 10:00 — Initial port space probe (first event)
- 10:01 — First notification starts (one event)
- 10:06 — Second notification starts (reports five events)
- 10:11 — Third notification starts (reports five events)
- 10:16 — Fourth notification starts (reports five events)

The launch interval controls the time intervals between each event (1, 2, 3, 4, and 5). This was set to 5 minutes. Multiply the repeat count by the launch interval. This is the time interval an event must continue to in order to start the repeat notification.

Use Syslog to See Log Message Data

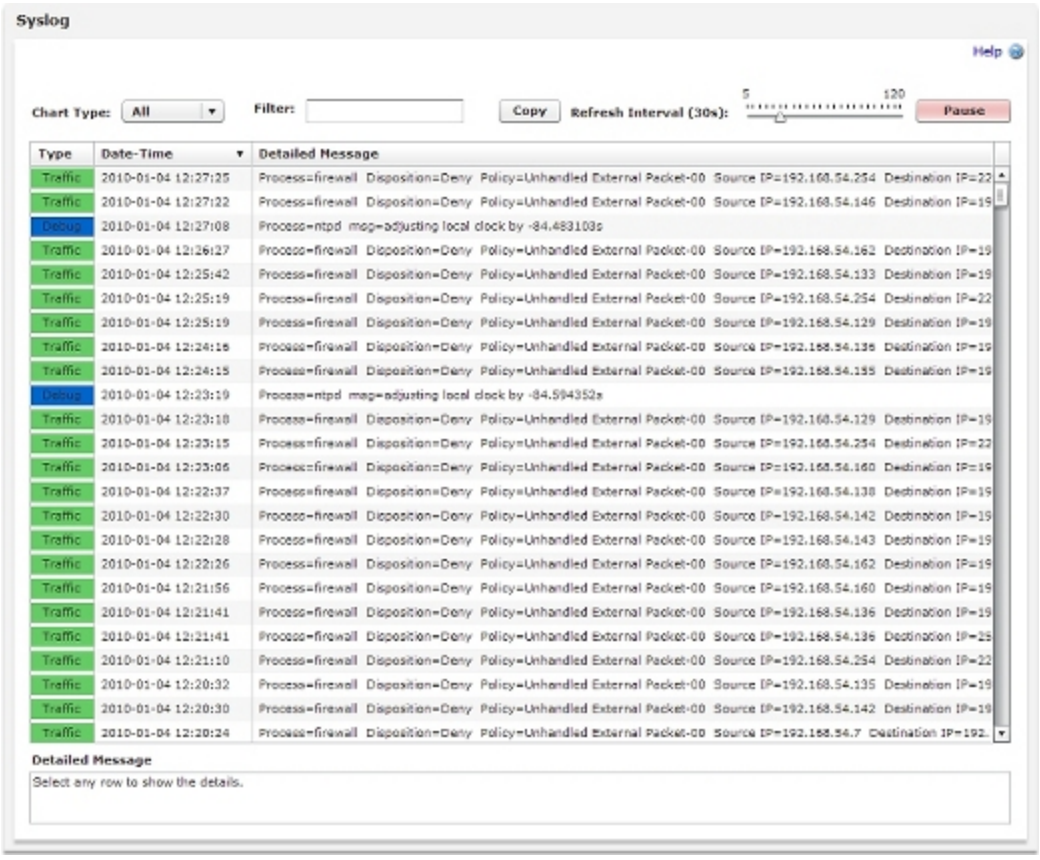
You can see real-time log message data on the **Syslog** page. You can choose to see only one type of log message, or to filter all the log messages for specific details. You can also control the frequency at which the log message data is refreshed.

When you use the **Filter** text box to specify which log messages you see, the filter search results include all entries that are a partial match for the selected filter.

View, Sort, and Filter Log Message Data

You can choose to see only specific types of log messages and apply filters to refine the data you see in Syslog log messages.

1. Select **System Status > Syslog**.
   The Syslog page appears with a complete list of real-time log messages for all message types.



2. To view only one type of log message, in the **Chart Type** drop-down list, select a message type:
   - **Traffic**
   - **Alarm**
   - **Event**
   - **Debug**
   - **Statistic**
3. To see all the log message types again, in the **Chart Type** drop-down list, select **All**.
4. To sort the log messages by a data type, click the column header for that data type. Different data columns appear based on the log message type selected in the **Chart Type** drop-down list.
5. To see only log messages with a specific message detail, in the **Filter** text box, type the detail.
   The Syslog display updates automatically to show only the log messages that include the detail you specified. If no messages match the filter details you type, the Syslog display is blank.

   For example, if you only want to see log messages from the user *Admin*, type `userID=Admin`. The results include log messages with the user *Admin*, *Admins*, *Administrator*, and any other user name that includes the characters *Admin*.
6. To remove a filter, clear all details from the **Filter** text box.
   The Syslog display updates automatically.
7. To copy log message data from the list, select one or more items in the list and click **Copy**.

Refresh Log Message Data

- To change the frequency at which the log message data is refreshed in the display, set the **Refresh Interval**.
- To temporarily disable the display refresh option, click **Pause**.
- To enable the display to refresh again, click **Restart**.

17 Monitor Your Device

About the Dashboard and System Status Pages

To monitor the status and activity on your XTM device, you can use the **Dashboard** and **System Status** pages.

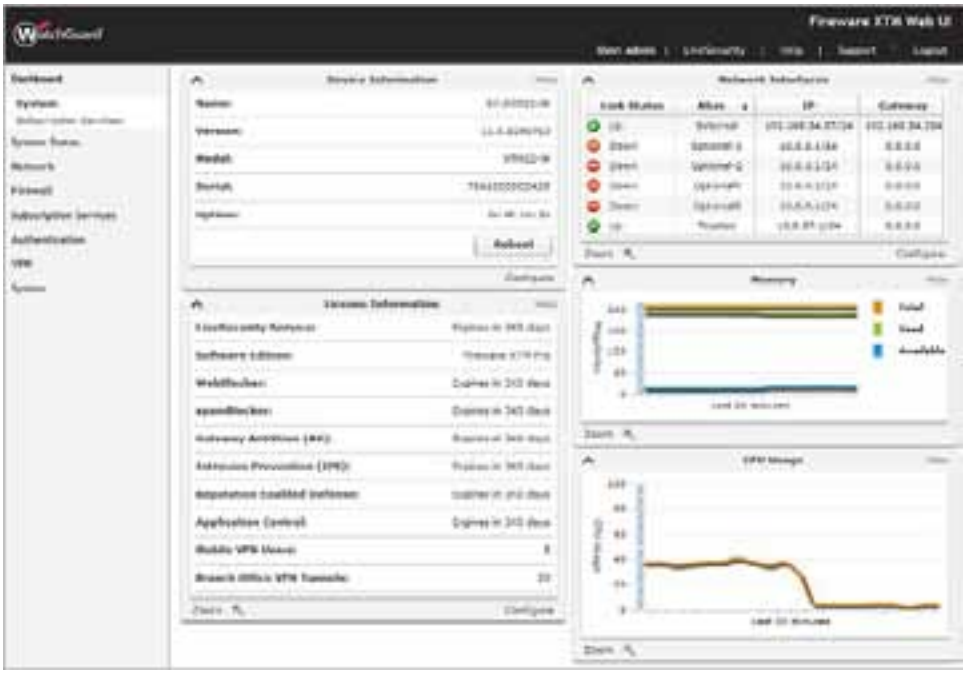
The Dashboard

The Dashboard includes two pages: the **System** page and the **Subscription Services** page.

The **System** page includes a quick view of the status of your device. If you have read-write configuration access, you can reboot your device from this page. The **System** page of the Dashboard automatically appears when you connect to Fireware XTM Web UI.

To open the **System** page from another page in the Web UI:

Select **Dashboard > System**.



The **System** page of the Dashboard shows:

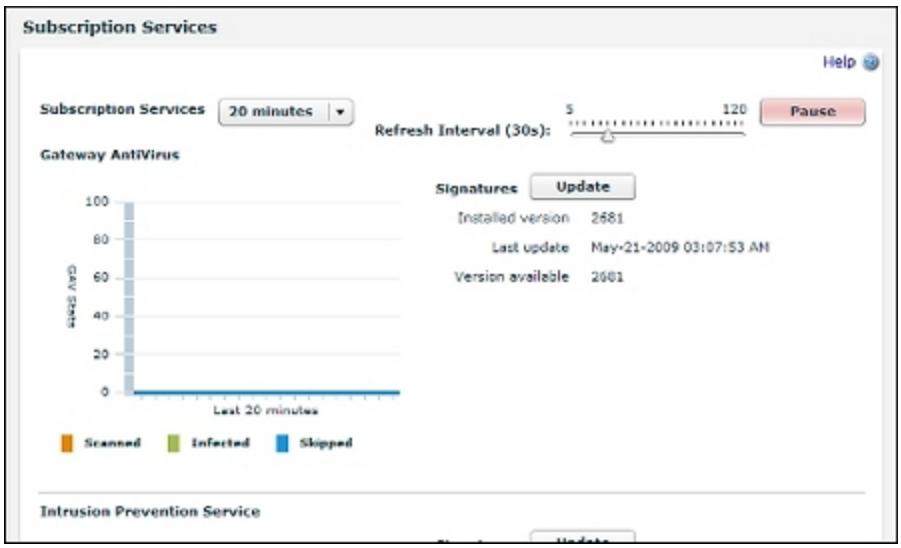
- Device information:
  - Device name
  - Fireware XTM OS software version
  - Model number of the device
  - Serial number of the device
  - Uptime since last restart
- Network interface information:
  - Link status
  - Alias — the name of the interface
  - IP — the IP address assigned to the interface
  - Gateway — the Gateway for the interface
- Memory and CPU usage statistics
- License information

To see statistics for a longer period of time, or to see more detail about statistics on the Dashboard:

At the bottom of a Dashboard item, click **Zoom**.
The System Status page appears, with more information and options.

You can also see information about your subscription services.

Select **Dashboard > Subscription Services**.
The Subscription Services page appears.



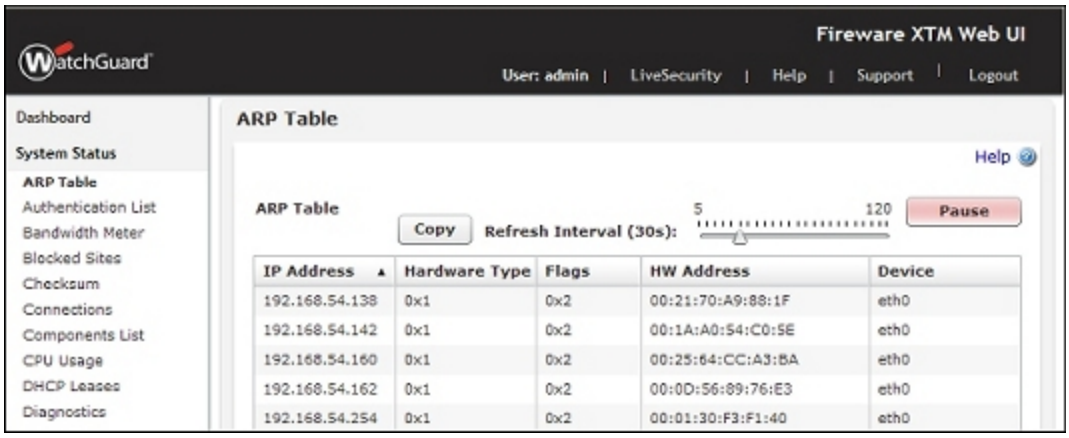
The **Subscription Services** page shows:

- Scanned, infected, and skipped traffic that is monitored by Gateway AntiVirus
- Scanned, detected, and prevented traffic that is monitored by Intrusion Prevention Service
- Signature version and update information for Gateway AntiVirus and Intrusion Prevention Service
- Good, bad and inconclusive reputation score statistics for URLs checked by Reputation Enabled Defense
- HTTP requests and traffic that is denied by WebBlocker
- Clean, confirmed, bulk, and suspect mail that is identified by spamBlocker

For more information about manual signature updates, see *Subscription Services Status and Manual Signatures Updates* on page 79.

System Status Pages

The **System Status** pages include a list of monitoring categories. On these pages, you can monitor all the components of your XTM device.



The **System Status** pages are set to refresh automatically every 30 seconds.

To change these settings:

1. To change the refresh interval, click and drag the triangle on the **Refresh Interval** slider bar.
2. To temporarily stop the refreshes, click **Pause**.
3. To force an immediate refresh, click **Pause** and then click **Restart**.

The numbers on the x-axis of the charts indicate the number of minutes ago. The statistical charts on the Dashboard show data for the past 20 minutes.

Some **System Status** pages have a **Copy** function.

To copy information from a list:

1. Select one or more list items.
2. Click **Copy**.
3. Paste the data in another application.

ARP Table

To see the ARP table for the XTM device:

Select **System Status > ARP Table**.

The **ARP Table** page includes devices that have responded to an ARP (Address Resolution Protocol) request from the XTM device:

IP Address

The IP address of the computer that responds to the ARP request.

Hardware Type

The type of Ethernet connection that the IP address uses to connect.

Flags

If the hardware address of the IP resolves, it is marked as **valid**. If it does not, it is marked as **invalid**.

> ***Note*** *A valid hardware address can briefly appear as **invalid** while the XTM device waits for a response for the ARP request.*

HW Address

The MAC address of the network interface card that is associated with the IP address.

Device

The interface on the XTM device where the hardware address for that IP address was found. The Linux kernel name for the interface is shown in parentheses.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Authentication List

To view the list of authenticated users for the XTM device:

Select **System Status > Authentication List**.

The **Authentication List** page includes information about every user who is currently authenticated to the XTM device.

User

The name of the authenticated user.

Type

The type of user who authenticated: Firewall or Mobile User.

Auth Domain

The authentication server that authenticated the user.

Start Time

The amount of time since the user authenticated.

Last Activity

The amount of time since the last user activity.

IP Address

The internal IP address being used by the user - for mobile users, this IP address is the IP address assigned to them by the XTM device.

From Address

The IP address on the computer the user authenticates from. For mobile users, this IP address is the IP address on the computer they used to connect to the XTM device. For Firewall users, the IP Address and From Address are the same.

To sort the Authentication List:

Click a column header.

To end a user session:

Select the user name and select **Log Off Users**.

For more information about authentication, see *About User Authentication* on page 233.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Bandwidth Meter

This Bandwidth Meter page shows the real time throughput statistics for all the XTM device interfaces over time. The Y axis (vertical) shows the throughput. The X axis (horizontal) shows the time.

To monitor the bandwidth usage for XTM device interfaces:

1. Select **System Status > Bandwidth Meter**.
2. To see the value for each data point, move your mouse over the lines in the graph.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Blocked Sites

To see a list of IP addresses currently blocked by the XTM device:

Select **System Status > Blocked Sites**.

The **Blocked Sites** page includes a list of IP addresses currently on the **Blocked Sites** list, the reason they were added to the list, and the expiration time (when the site is removed from the **Blocked Sites** list).

For each blocked site, the table includes this information:

IP

The IP address of the blocked site.

Source

The source of the blocked site. Sites added on the **System Status > Blocked Sites** page are shown as **admin**, while sites added from the **Firewall > Blocked Sites** page are shown as **configuration**.

Reason

The reason the site was blocked.

Timeout

The total amount of time the site is blocked.

Expiration

The amount of time that remains until the timeout period expires.

Blocked sites with a **Reason** of **Static Blocked IP**, and a **Timeout** and **Expiration** of **Never Expire** are permanently blocked. You cannot delete or edit a permanently blocked site from this page.

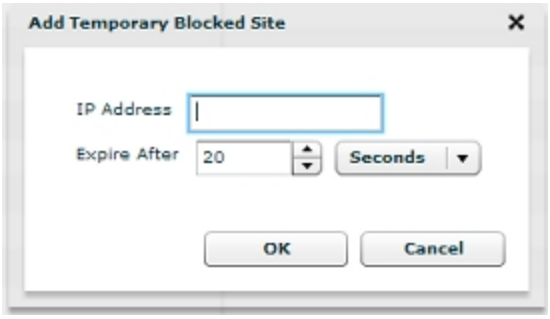
To add or remove a permanently blocked site, select **Firewall > Blocked Sites**. For more information, see *Block a Site Permanently* on page 451.

Add or Edit Temporary Blocked Sites

On the **Blocked Sites** page, you can also add and remove temporarily blocked sites in the blocked sites list, and change the expiration of those sites.

To add a temporary blocked site to the blocked sites list:

1. Click **Add**.
   The Add Temporary Blocked Site dialog box appears.



2. Type the **IP Address** of the site you want to block.
3. In the **Expire After** text box and drop-down list, select how long you this site is to stay on the blocked sites list.
4. Click **OK**.

To change the expiration for a temporarily blocked site:

1. In the **Connections List**, select the site.
2. Click **Change Expiration**.
   The Edit Temporary Blocked Site dialog box appears.
3. In the **Expire After** text box and drop-down list, select how long this site is to stay on the blocked sites list.
4. Click **OK**.

To remove a temporarily blocked site from the blocked sites list:

1. Select the site in the **Connections List**.
2. Click **Delete**.
   The blocked site is removed from the list.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Checksum

To see the checksum of the OS (operating system) files currently installed on the XTM device:

Select **System Status > Checksum**.

The XTM device calculates the checksum for the installed OS. It may take a few minutes for the XTM device to complete the checksum calculation. The checksum appears, with the date and time that the checksum calculation was completed.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Connections

To monitor the connections to the XTM device:

Select **System Status > Connections**.

The **Connections** page includes the number of connections that go through the XTM device. The current number of connections for each protocol appears in the **Connections** column.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Components List

To view a list of the software components installed on the XTM device:

Select **System Status > Components List**.

The **Components** page includes a list of the software installed on the XTM device.

The software list includes these attributes:

- Name
- Version
- Build
- Date

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

CPU Usage

To monitor CPU usage on the XTM device:

1. Select **System Status > CPU Usage**.
   The **CPU Usage** page contains graphs that show CPU usage and average load over a period of time.
2. To see the value for each data point, move your mouse over the lines in the graph.
3. To select a time period, click the **CPU Usage** drop-down list.
   - The x-axis indicates the number of minutes ago.
   - The y-axis scale is the percentage of CPU capacity used.

A smaller version of this graph appears on the **Dashboard** page.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

DHCP Leases

To see a list of the DHCP leases for the XTM device:

Select **System Status > DHCP Leases**.

The **DHCP Leases** page includes the DHCP server and the leases used by the XTM device, with the DHCP reservations.

Interface

The XTM device interface that the client is connected to.

IP Address

The IP address for the lease.

Host

The host name. If there is not an available host name, this item is empty.

MAC Address

The MAC address associated with the lease.

Start Time

The time that the client requested the lease.

End Time

The time that the lease expires.

Hardware Type

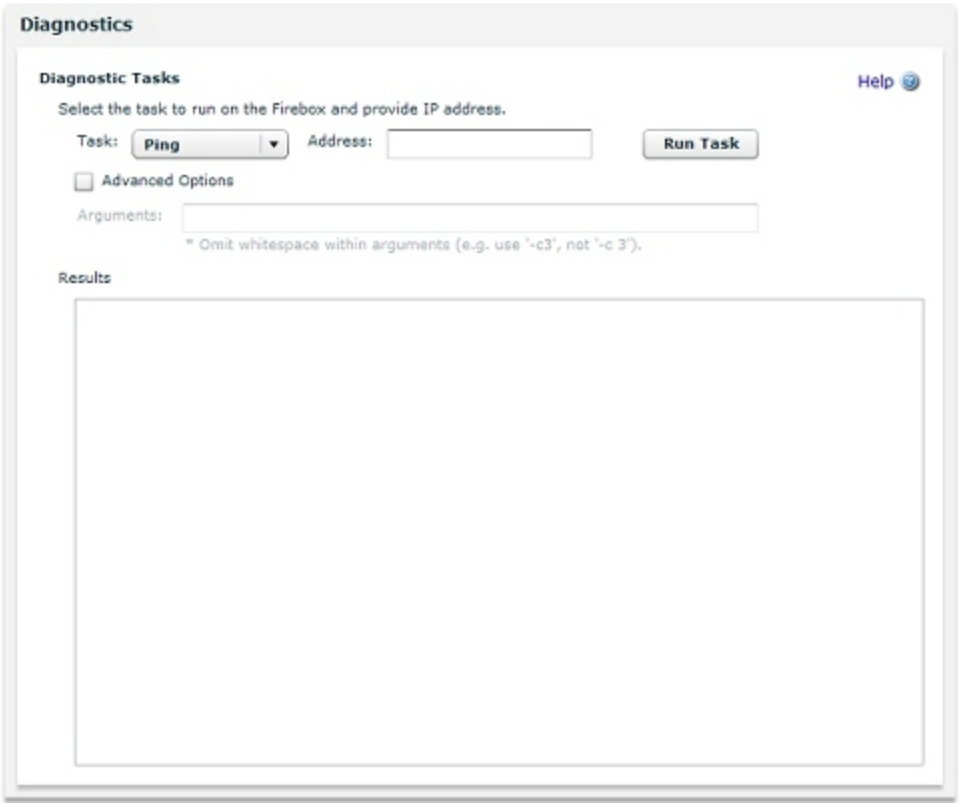
The type of hardware.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Diagnostics

To find diagnostic information for your XTM device, you can ping an IP address or host, trace the route to an IP address or host, lookup DNS information for host, or see information about the packets transmitted across your network (TCP dump).

1. Connect to Fireware XTM Web UI for your device.
2. Select **System Status > Diagnostics**.
   The Diagnostics page appears.



Run a Basic Diagnostics Command

1. From the **Task** drop-down list, select a command:
   - **Ping**
   - **traceroute**
   - **DNS lookup**
   - **tcpdump**

   If you select Ping, traceroute, or DNS lookup, the Address text box appears.

   If you select TCP Dump, the Interface text box appears.
2. If you select **Ping**, **traceroute**, or **DNS lookup**, in the **Address** text box, type an IP address or host name.

   If you select **tcpdump**, from the **Interface** drop-down list, select an interface.
3. Click **Run Task**.

   The output of the command appears in the Results window and the Stop Task button appears.
4. To stop the diagnostic task, click **Stop Task**.

Use Command Arguments

1. From the **Task** drop-down list, select a command:
   - **Ping**
   - **traceroute**
   - **DNS lookup**
   - **tcpdump**
2. Select the **Advanced Options** check box.

   The Arguments text box is enabled and the Address or Interface text box is disabled.

3. In the **Arguments** text box , type the command arguments.
   To see the available arguments for a command, leave the **Arguments** text box blank.
4. Click **Run Task**.
   The output of the command appears in the Results window and the Stop Task button appears.
5. To stop the diagnostic task, click **Stop Task**.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Dynamic DNS

To view the dynamic DNS routes table:

Select **System Status > Dynamic DNS**.

The **Dynamic DNS** page contains the DNS routes table with this information:

Name

The interface name.

User

The Dynamic DNS account user name.

Domain

The domain for which Dynamic DNS is being provided.

System

The Dynamic DNS service type.

Address

The IP address associated with the domain.

IP

The current IP address of the interface.

Last

The last time the DNS was updated.

Next Date

The next time the DNS is scheduled to be updated.

State

The state of Dynamic DNS.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Feature Key

A feature key is a license that enables you to use a set of features on your XTM device. You increase the functionality of your device when you purchase an option or upgrade and get a new feature key.

When You Purchase a New Feature

When you purchase a new feature for your XTM device, you must:

- *Get a Feature Key from LiveSecurity*
- *Add a Feature Key to Your XTM Device*

See Features Available with the Current Feature Key

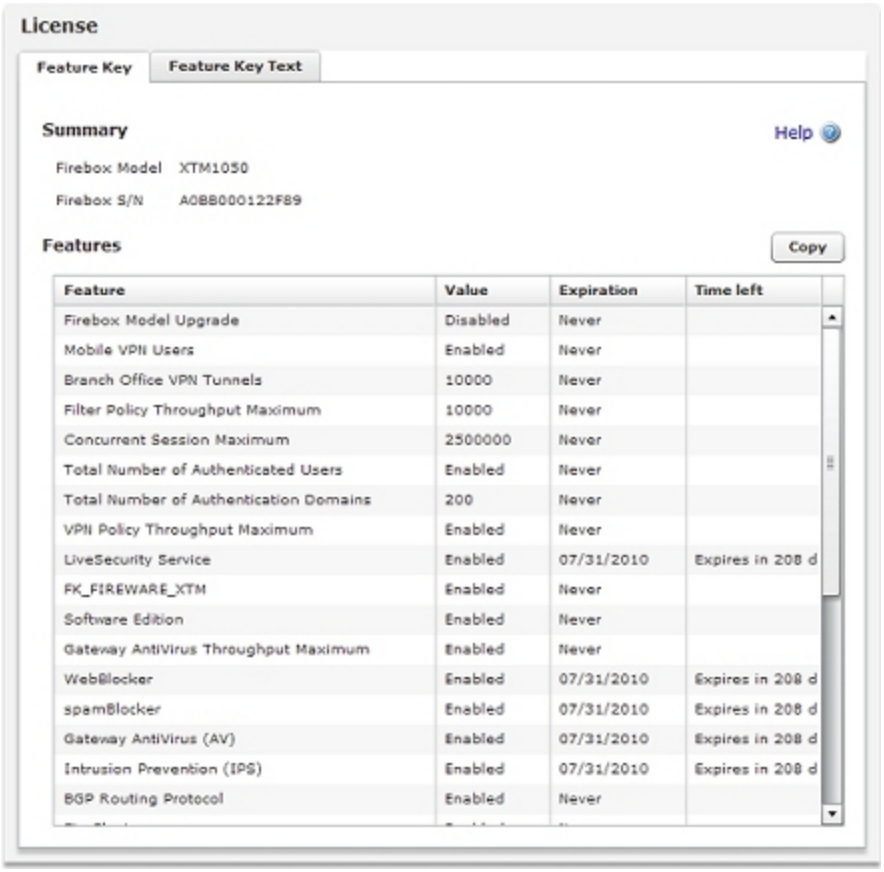
Your XTM device always has one currently active feature key. You can use Fireware XTM Web UI to see the features available with this feature key. You can also review the details of your current feature key.

The available details include:

- Serial number of the XTM device to which this feature key applies
- XTM device ID and name
- Device model and version number
- Available features

To see information about the licensed features for your XTM device:

1. Select **System Status > Feature Key**.
   The Feature Key page appears, with basic information about the features enabled by the feature key for this device.



2. To see information for each feature, use the scroll bar on the **Feature Key** tab.
   This information appears:

   - Feature — The name of the licensed feature.
   - Value — The feature the license enables. For example, a capacity or number of users.
   - Expiration — When the license expires.
   - Time left — The number of days until the license expires.

3. To see the details of the feature key, select the **Feature Key Text** tab.
   The licensed features for your device appear.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Interfaces

To see information about the XTM device network interfaces:

Select **System Status > Interfaces**.
The Interfaces page appears.

The **Interfaces** page includes this information for each interface:

Link Status

If the interface is active, **Up** appears. If it is not active, **Down** appears.

Alias

The interface name.

Enabled

Includes whether each interface is enabled or disabled.

Gateway

The gateway defined for each interface.

IP

The IP address configured for each interface.

MAC Address

The MAC Address for each interface,

Name

The interface number.

Netmask

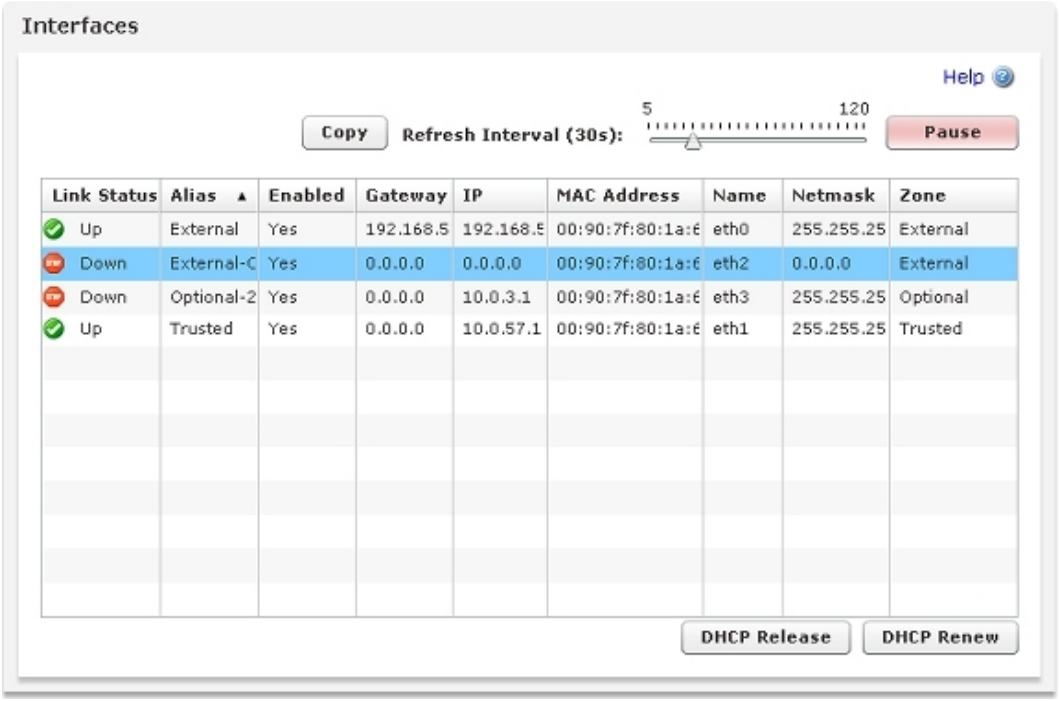
Network mask for each interface.

Zone

The trust zone for each interface.

For an External interface with DHCP enabled, you can also release or renew the DHCP lease on an IP address.

1. Select **System Status > Interfaces**.
   The Interfaces page appears.
2. Select the External interface with DHCP enabled.
   The DHCP Release and DHCP Renew buttons are enabled at the bottom of the page.



3. To release the DHCP lease for the selected interface, click **DHCP Release**.

   To refresh the DHCP lease for the selected interface, click **DHCP Renew**.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

LiveSecurity

Fireware XTM Web UI includes a page with the most recent alert notifications sent from the WatchGuard LiveSecurity Service. LiveSecurity alerts give you information that applies to the appliance, such as notification about available software updates. Alert notifications are sent no more than one time each day.

To see alerts from WatchGuard:

1. Select **System Status > LiveSecurity**.
2. Click **Refresh** to check for new alerts.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Memory

To monitor memory usage on the XTM device:

1. Select **System Status > Memory**.
   A graph appears that shows the usage of Linux kernel memory over a period of time.
2. To see the value for each data point, move your mouse over the lines in the graph.
3. To select the time period for the graph, click the **Memory** drop-down list.

- The x-axis indicates the number of minutes ago.
- The y-axis scale is the amount of memory used, in megabytes.

You can also see a smaller version of this graph on the **Dashboard** page.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Processes

To see a list of processes that run on the XTM device:

1. Connect to Fireware XTM Web UI for your device.
2. Select **System Status > Processes**.
   The Processes page appears.

The **Processes** page includes information about all processes that run on the XTM device.

PID

The Process ID is a unique number that shows when the process started,

Name

The name of the process.

State

The state of the process:

R — Running

S — Sleeping

D,**Z** — Inactive

RSS

The total number of kilobytes of physical memory the process uses.

Share

The total number of kilobytes of shared memory the process uses.

Time

The time that the process has used after the last time the device was started.

CPU

The percentage of CPU time the process has used after the last device reboot.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Routes

To see the routes table for the XTM device:

Select **System Status > Routes**.

The routes table includes this information about each route:

Destination

The network that the route was created for.

Interface

The interface associated with the route.

Gateway

The gateway that the network uses.

Flag

The flags set for each route.

Metric

The metric set for this route in the routing table.

Mask

The network mask for the route.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Syslog

You can use syslog to see the log data in the XTM device log file.

Select **System Status > Syslog**.
The Syslog page appears with the most recent entries in the XTM device log file.

For more information about how to use this page, see *Use Syslog to See Log Message Data* on page 467.

For more information about the **System Status** pages, see *About the Dashboard and System Status Pages* on page 471.

Traffic Management

To see traffic management statistics:

Select **System Status > Traffic Management**.
The statistics associated with each traffic management action you have configured appear.

The **Traffic Management** page includes these statistics:

Action

The name of the traffic management action.

Interface

The XTM device interface to which the traffic action applies.

Bytes

The total number of bytes.

Bytes/second

The current bits per second (rate estimator).

Packets

The total number of packets.

Packets/second

The current packets per second (rate estimator).

For information about Traffic Management, see *About Traffic Management and QoS* on page 427.

For more information about the System Status pages, see *About the Dashboard and System Status Pages* on page 471.

VPN Statistics

To see statistics about VPN tunnels:

1. Select **System Status > VPN Statistics**.
   The traffic statistics for Branch Office VPN and Mobile VPN with IPSec tunnels appear.

   For each VPN tunnel, this page includes:

   Name

   The tunnel name.

   Local

   The IP address at the local end of the tunnel.

   Remote

   The IP address at the remote end of the tunnel.

   Gateway

   The gateway endpoints used by this tunnel.

   Packets In

   The number of packets received through the tunnel.

   Bytes In

   The number of bytes received through the tunnel.

   Packets Out

   The number of packets sent out through the tunnel.

   Bytes Out

   The number of bytes sent out through the tunnel.

Rekeys

The number of rekeys for the tunnel.

2. To force a BOVPN tunnel to rekey, selected a BOVPN tunnel and click **Rekey selected BOVPN tunnel**.

   For more information, see *Rekey BOVPN Tunnels* on page 570.

3. To see additional information for use when you troubleshoot, click **Debug**.

   We recommend you use this feature when you troubleshoot a VPN problem with a technical support representative.

For more information about the System Status pages, see *About the Dashboard and System Status Pages* on page 471.

Wireless Statistics

To see statistics about your wireless network:

Select **System Status > Wireless Statistics**.
A summary of wireless configuration settings and some statistics about wireless traffic appears.

This summary includes:

- Wireless configuration information
- Interface statistics
- Keys
- Bit rates
- Frequencies

You can also update the wireless country information for this device from this page. The available options for the wireless radio settings are based on the regulatory requirements of the country in which the device detects that it is located.

To update the wireless country information:

Click **Update Country Info**.
The 2 Series device contacts a WatchGuard server to determine the current operating region.

For more information about radio settings on the WatchGuard XTM wireless device, see *About Wireless Radio Settings*.

For more information about the System Status pages, see *About the Dashboard and System Status Pages* on page 471.

Wireless Hotspot Connections

When you enable the wireless hotspot feature for your WatchGuard XTM wireless device, you can see information about the number of wireless clients that are connected. You can also disconnect wireless clients.

For more information about how to enable the wireless hotspot feature, see *Enable a Wireless Hotspot*.

To see the wireless hotspot connections:

1. Connect to Fireware XTM Web UI for your wireless device.
2. Select **System Status > Wireless Hotspot**.
   The IP address and MAC address for each connected wireless client appears.

For more information about how to manage wireless hotspot connections, see *See Wireless Hotspot Connections*.

18 Certificates

About Certificates

Certificates match the identity of a person or organization with a method for others to verify that identity and secure communications. They use an encryption method called a key pair, or two mathematically related numbers called the *private key* and the *public key*. A certificate includes both a statement of identity and a public key, and is signed by a private key.

The private key used to sign a certificate can be from the same key pair used to generate the certificate, or from a different key pair. If the private key is from the same key pair used to create the certificate, the result is called a *self-signed certificate*. If the private key is from a different key pair, the result is a regular *certificate*. Certificates with private keys that can be used to sign other certificates are called *CA (Certificate Authority) Certificates*. A certificate authority is an organization or application that signs and revokes certificates.

If your organization has a PKI (public key infrastructure) set up, you can sign certificates as a CA yourself. Most applications and devices automatically accept certificates from prominent, trusted CAs. Certificates that are not signed by prominent CAs, such as self-signed certificate are not automatically accepted by many servers or programs, and do not operate correctly with some Fireware XTM features.

Use Multiple Certificates to Establish Trust

Several certificates can be used together to create a *chain of trust*. For example, the CA certificate at the start of the chain is from a prominent CA, and is used to sign another CA certificate for a smaller CA. That smaller CA can then sign another CA certificate used by your organization. Finally, your organization can use this CA certificate to sign another certificate for use with the HTTPS proxy content inspection feature. However, to use that final certificate at the end of the chain of trust, you must first import all of the certificates in the chain of trust in this order:

1. CA certificate from the prominent CA (as type "Other")
2. CA certificate from the smaller CA (as type "Other")
3. CA certificate from the organization (as type "Other")
4. Certificate used to re-encrypt HTTPS proxy content after inspection (as type "HTTPS Proxy Authority")

It could also be necessary to import all of these certificates on each client device so that the last certificate is also trusted by users.

For more information, see Manage XTM Device Certificates.

How the XTM device Uses Certificates

Your XTM device can use certificates for several purposes:

- Management session data is secured with a certificate.
- BOVPN or Mobile VPN with IPSec tunnels can use certificates for authentication.
- When content inspection is enabled, the HTTPS-proxy uses a certificate to re-encrypt incoming HTTPS traffic after it is decrypted for inspection.
- You can use a certificate with the HTTPS-proxy to protect a web server on your network.
- When a user authenticates with the XTM device for any purpose, such as a WebBlocker override, the connection is secured with a certificate.
- When RADIUS or Firebox authentication is configured to use WPA Enterprise or WPA2 Enterprise authentication methods.

By default, your XTM device creates self-signed certificates to secure management session data and authentication attempts for Fireware XTM Web UI and for HTTPS proxy content inspection. To make sure the certificate used for HTTPS content inspection is unique, its name includes the serial number of your device and the time at which the certificate was created. Because these certificates are not signed by a trusted CA, users on your network see warnings in their web browsers.

You have three options to remove this warning:

1. You can import certificates that are signed by a CA your organization trusts, such as a PKI you have already set up for your organization, for use with these features. We recommend that you use this option if possible.
2. You can create a custom, self-signed certificate that matches the name and location of your organization.
3. You can use the default, self-signed certificate.

For the second and third options, you can ask network clients to accept these self-signed certificates manually when they connect to the XTM device. Or, you can export the certificates and distribute them with network management tools. You must have WatchGuard System Manager installed to export certificates.

Certificate Lifetimes and CRLs

Each certificate has a set lifetime when it is created. When the certificate reaches the end of that set lifetime, the certificate expires and can no longer be used automatically. You can also remove certificates manually with Firebox System Manager (FSM).

Sometimes, certificates are *revoked*, or disabled before their lifetime expiration, by the CA. Your XTM device keeps a current list of these revoked certificates, called the Certificate Revocation List (CRL), to verify that certificates used for VPN authentication are valid. If you have WatchGuard System Manager installed, this list can be updated manually with Firebox System Manager (FSM), or automatically with information from a certificate. Each certificate includes a unique number used to identify the certificate. If the unique number on a Web Server, BOVPN, or Mobile VPN with IPSec certificate matches an identifier from its associated CRL, the XTM device disables the certificate.

When content inspection is enabled on an HTTPS proxy, the XTM device can check the OCSP (Online Certificate Status Protocol) responder associated with the certificates used to sign the HTTPS content. The OCSP responder sends the revocation status of the certificate. The XTM device accepts the OCSP response if the response is signed by a certificate the XTM device trusts. If the OCSP response is not signed by a certificate the XTM device trusts, or if the OCSP responder does not send a response, then you can configure the XTM device to accept or reject the original certificate.

For more information about OCSP options, see .

Certificate Authorities and Signing Requests

To create a self-signed certificate, you put part of a cryptographic key pair in a certificate signing request (CSR) and send the request to a CA. It is important that you use a new key pair for each CSR you create. The CA issues a certificate after they receive the CSR and verify your identity. If you have FSM or Management Server software installed, you can use these programs to create a CSR for your XTM device. You can also use other tools, such as OpenSSL or the Microsoft CA Server that comes with most Windows Server operating systems.

If you want to create a certificate for use with the HTTPS proxy content inspection feature, it must be a CA certificate that can re-sign other certificates. If you create a CSR with Firebox System Manager and have it signed by a prominent CA, it can be used as a CA certificate.

If you do not have a PKI set up in your organization, we recommend that you choose a prominent CA to sign the CSRs you use, except for the HTTPS proxy CA certificate. If a prominent CA signs your certificates, your certificates are automatically trusted by most users. WatchGuard has tested certificates signed by VeriSign, Microsoft CA Server, Entrust, and RSA KEON. You can also import additional certificates so that your XTM device trusts other CAs.

For a complete list of automatically trusted CAs, see *Certificate Authorities Trusted by the XTM Device* on page 495.

Create a CSR with OpenSSL

Certificate Authorities Trusted by the XTM Device

By default, your XTM device trusts most of the same certificate authorities (CAs) as modern web browsers. We recommend that you import certificates signed by a CA on this list for the HTTPS proxy or Fireware XTM Web UI, so that users do not see certificate warnings in their web browser when they use those features. However, you can also import certificates from other CAs so that your certificates are trusted.

If you have installed WatchGuard System Manager, a copy of each certificate is stored on your hard drive at:

```
C:\Documents and Settings\WatchGuard\wgauth\certs\README
```

Certificate Authority List

```
C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority - G2,
    OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust
    Network
    C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification
    Services Division, CN=Thawte Personal Premium CA/emailAddress=personal-
    premium@thawte.com
    C=ES, L=C/ Muntaner 244 Barcelona, CN=Autoridad de Certificacion
    Firmaprofesional CIF A62634068/emailAddress=ca@firmaprofesional.com
    C=HU, ST=Hungary, L=Budapest, O=NetLock Halozatbiztonsagi Kft.,
    OU=Tanusitvanykiadok, CN=NetLock Kozjegyzoi (Class A) Tanusitvanykiado
    C=ZA, ST=Western Cape, L=Durbanville, O=Thawte, OU=Thawte Certification,
    CN=Thawte Timestamping CA
    C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc.
    - For authorized use only, CN=VeriSign Class 4 Public Primary Certification
    Authority - G3
    C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Qualified CA Root
    C=DK, O=TDC Internet, OU=TDC Internet Root CA
    C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification Authority -
    G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust
    Network
    C=US, O=Wells Fargo, OU=Wells Fargo Certification Authority, CN=Wells Fargo
    Root Certificate Authority
    OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign
    CN=Test-Only Certificate
    C=US, O=Entrust, Inc., OU=www.entrust.net/CPS is incorporated by reference,
    OU=(c) 2006 Entrust, Inc., CN=Entrust Root Certification Authority
    C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Class 1 CA Root
    C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO
    Certification Authority
    O=RSA Security Inc, OU=RSA Security 2048 V3
    C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification
    Services Division, CN=Thawte Personal Basic CA/emailAddress=personal-
    basic@thawte.com
    C=FI, O=Sonera, CN=Sonera Class1 CA
    O=VeriSign Trust Network, OU=VeriSign, Inc., OU=VeriSign International Server
    CA - Class 3, OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97
    VeriSign
    C=ZA, O=Thawte Consulting (Pty) Ltd., CN=Thawte SGC CA
    C=US, O=Equifax Secure Inc., CN=Equifax Secure eBusiness CA-1
```

C=JP, O=SECOM Trust.net, OU=Security Communication RootCA1
C=US, O=America Online Inc., CN=America Online Root Certification Authority 1
C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok, CN=NetLock Uzleti (Class B) Tanusitvanykiado
C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN - DATACorp SGC
C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification Authority
C=CH, O=SwissSign AG, CN=SwissSign Gold CA - G2
C=US, O=RSA Data Security, Inc., OU=Secure Server Certification Authority
C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G3
C=US, OU=www.xrampsecurity.com, O=XRamp Security Services Inc, CN=XRamp Global Certification Authority
C=PL, O=Unizeto Sp. z o.o., CN=Certum CA
C=US, O=Entrust.net, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Secure Server Certification Authority
L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert Class 3 Policy Validation Authority, CN=http://www.valicert.com//emailAddress=info@valicert.com
C=CH, O=SwissSign AG, CN=SwissSign Platinum CA - G2
OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign
O=Digital Signature Trust Co., CN=DST Root CA X3
C=US, O=AOL Time Warner Inc., OU=America Online Inc., CN=AOL Time Warner Root Certification Authority 1
C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=Secure Certificate Services
O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)00, CN=VeriSign Time Stamping Authority CA
O=Entrust.net, OU=www.entrust.net/GCCA_CPS incorp. by ref. (limits liab.), OU=(c) 2000 Entrust.net Limited, CN=Entrust.net Client Certification Authority
C=US, O=SecureTrust Corporation, CN=Secure Global CA
C=US, O=Equifax, OU=Equifax Secure Certificate Authority
O=beTRUSTed, OU=beTRUSTed Root CAs, CN=beTRUSTed Root CA - RSA Implementation
C=WW, O=beTRUSTed, CN=beTRUSTed Root CAs, CN=beTRUSTed Root CA
C=US, O=GeoTrust Inc., CN=GeoTrust Primary Certification Authority
C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority
C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA/emailAddress=premium-server@thawte.com
C=US, O=SecureTrust Corporation, CN=SecureTrust CA
OU=Extended Validation CA, O=GlobalSign, CN=GlobalSign Extended Validation CA
C=US, O=GeoTrust Inc., CN=GeoTrust Global CA 2
C=NL, O=Staat der Nederlanden, CN=Staat der Nederlanden Root CA
C=IL, ST=Israel, L=Eilat, O=StartCom Ltd., OU=CA Authority Dep., CN=Free SSL Certification Authority/emailAddress=admin@startcom.org
C=US, O=VISA, OU=Visa International Service Association, CN=Visa eCommerce Root
O=beTRUSTed, OU=beTRUSTed Root CAs, CN=beTRUSTed Root CA - Entrust

Implementation
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5
C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l., O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA Chained CAs Certification Authority, CN=IPS CA Chained CAs Certification Authority/emailAddress=ips@mail.ips.es
DC=com, DC=microsoft, DC=corp, DC=redmond, CN=Microsoft Secure Server Authority
C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware
C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 3
C=TW, O=Government Root Certification Authority
C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=Trusted Certificate Services
C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA 2
C=US, O=Entrust.net, OU=www.entrust.net/Client_CA_Info/CPS incorp. by ref. limits liab., OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Client Certification Authority
C=FR, O=Certplus, CN=Class 2 Primary CA
C=US, O=Starfield Technologies, Inc., OU=Starfield Class 2 Certification Authority
C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Freemail CA/emailAddress=personal-freemail@thawte.com
O=Entrust.net, OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Certification Authority (2048)
C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l., O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA CLASEA1 Certification Authority, CN=IPS CA CLASEA1 Certification Authority/emailAddress=ips@mail.ips.es
C=US, O=AOL Time Warner Inc., OU=America Online Inc., CN=AOL Time Warner Root Certification Authority 2
C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust Network
C=US, O=VISA, OU=Visa International Service Association, CN=GP Root 2
C=US, O=GeoTrust Inc., CN=GeoTrust Global CA
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)06, CN=VeriSign Class 3 Extended Validation SSL CA
C=EU, O=AC Camerfirma SA CIF A82743287, OU=http://www.chambersign.org, CN=Global Chambersign Root
C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in Data Networks GmbH, OU=TC TrustCenter Class 2 CA/emailAddress=certificate@trustcenter.de
C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE CyberTrust Global Root
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)05, CN=VeriSign Class 3 Secure Server CA
C=US, O=GTE Corporation, CN=GTE CyberTrust Root

C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 1 Public Primary Certification Authority - G3
C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Network Applications
C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok, CN=NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado/emailAddress=info@netlock.hu
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 2 Public Primary Certification Authority - G3
C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co., OU=DSTCA X2, CN=DST RootCA X2/emailAddress=ca@digsigtrust.com
C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l., O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA CLASE3 Certification Authority, CN=IPS CA CLASE3 Certification Authority/emailAddress=ips@mail.ips.es
O=RSA Security Inc, OU=RSA Security 1024 V3
C=US, O=Equifax Secure, OU=Equifax Secure eBusiness CA-2
C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA
C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co., OU=DSTCA X1, CN=DST RootCA X1/emailAddress=ca@digsigtrust.com
C=US, O=Network Solutions L.L.C., CN=Network Solutions Certificate Authority
C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA/emailAddress=server-certs@thawte.com
C=US, O=VeriSign, Inc., OU=Class 4 Public Primary Certification Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust Network
C=NL, O=DigiNotar, CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
C=US, O=America Online Inc., CN=America Online Root Certification Authority 2
C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l., O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA Timestamping Certification Authority, CN=IPS CA Timestamping Certification Authority/emailAddress=ips@mail.ips.es
C=US, O=DigiCert Inc., CN=DigiCert Security Services CA
C=US, O=Digital Signature Trust, OU=DST ACES, CN=DST ACES CA X6
C=DK, O=TDC, CN=TDC OCES CA
C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority
C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l., O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA CLASEA3 Certification Authority, CN=IPS CA CLASEA3 Certification Authority/emailAddress=ips@mail.ips.es
C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Client Authentication and Email
C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA Certificate Services
L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert Class 1 Policy Validation Authority, CN=http://www.valicert.com//emailAddress=info@valicert.com
C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l., O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA CLASE1 Certification Authority, CN=IPS CA CLASE1 Certification

Authority/emailAddress=ips@mail.ips.es
C=BM, O=QuoVadis Limited, OU=Root Certification Authority, CN=QuoVadis Root Certification Authority
C=US, O=Network Solutions L.L.C., CN=Network Solutions Certificate Authority
C=CH, O=SwissSign AG, CN=SwissSign Silver CA - G2
C=US, O=Digital Signature Trust Co., OU=DSTCA E2
C=US, O=Digital Signature Trust Co., OU=DSTCA E1
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA
C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certificates.godaddy.com/repository, CN=Go Daddy Secure Certification Authority/serialNumber=07969287
C=EU, O=AC Camerfirma SA CIF A82743287, OU=http://www.chambersign.org, CN=Chambers of Commerce Root
C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 2
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance EV Root CA
C=US, ST=DC, L=Washington, O=ABA.ECOM, INC., CN=ABA.ECOM Root CA/emailAddress=admin@digsigtrust.com
C=ES, ST=BARCELONA, L=BARCELONA, O=IPS Seguridad CA, OU=Certificaciones, CN=IPS SERVIDORES/emailAddress=ips@mail.ips.es
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Assured ID Root CA
C=ch, O=Swisscom, OU=Digital Certificate Services, CN=Swisscom Root CA 1
CN=T\xC3\x9CRKTRUST Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1, C=TR, L=ANKARA, O=(c) 2005 T\xC3\x9CRKTRUST Bilgi \xC4\xB0leti\xC5\x9Fim ve Bili\xC5\x9Fim G\xC3\xBCvenli\xC4\x9Fi Hizmetleri A.\xC5\x9E.
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5
C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in Data Networks GmbH, OU=TC TrustCenter Class 3 CA/emailAddress=certificate@trustcenter.de
C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok, CN=NetLock Expressz (Class C) Tanusitvanykiado
C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Object
C=US, O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority
C=US, O=Akamai Technologies Inc, CN=Akamai Subordinate CA 3
C=US, O=Network Solutions L.L.C., CN=Network Solutions Certificate Authority
C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Public CA Root
CN=T\xC3\x9CRKTRUST Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1, C=TR, L=Ankara, O=T\xC3\x9CRKTRUST Bilgi \xC4\xB0leti\xC5\x9Fim ve Bili\xC5\x9Fim G\xC3\xBCvenli\xC4\x9Fi Hizmetleri A.\xC5\x9E. (c) Kas\xC4\xB1m 2005
C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)06, CN=VeriSign Class 3 Extended Validation SSL SGC CA
O=Entrust.net, OU=www.entrust.net/SSL_CPS incorp. by ref. (limits liab.), OU=(c) 2000 Entrust.net Limited, CN=Entrust.net Secure Server Certification Authority
CN=Microsoft Internet Authority
L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert Class 2 Policy Validation Authority,

```
CN=http://www.valicert.com//emailAddress=info@valicert.com
C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network,
OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware
C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External
CA Root
C=FI, O=Sonera, CN=Sonera Class2 CA
O=beTRUSTed, OU=beTRUSTed Root CAs, CN=beTRUSTed Root CA-Baltimore
Implementation
C=IL, O=StartCom Ltd., OU=Secure Digital Certificate Signing, CN=StartCom
Certification Authority
```

Manage XTM Device Certificates

You can use Fireware XTM Web UI to see and manage your XTM device certificates. This includes:

- See a list of the current XTM device certificates and their properties
- Import a certificate
- Select a web server certificate for Firebox authentication
- Select a certificate to use with a Branch Office VPN or Mobile User VPN

> ***Note*** *You must use Firebox System Manager (FSM) to create certificate signing requests (CSRs), import certificate revocation lists (CRLs), remove certificates, or delete certificates. For more information, see the WatchGuard System Manager help system.*

See Current Certificates

To see the current list of certificates:

1. Select **System > Certificates**.
   The Certificates list appears, with all the certificates and certificate signing requests (CSRs).

   The **Certificates** list includes:

   - The status and type of the certificate.
   - The algorithm used by the certificate.
   - The subject name or identifier of the certificate.

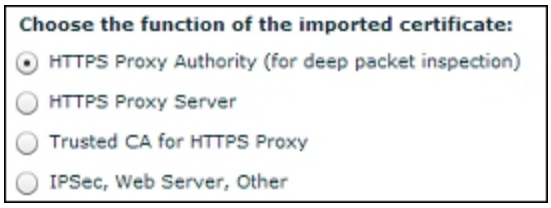
   By default, trusted CA certificates are not included in this list.
2. To show all of the certificates from trusted CAs, select the **Show Trusted CAs for HTTPS Proxy** check box.
3. To hide the trusted CA certificates, clear the **Show Trusted CAs for HTTPS Proxy** check box.

Import a Certificate from a File

You can import a certificate from the Windows clipboard, or from a file on your local computer. Certificates must be in PEM (base64) format. Before you import a certificate to use with the HTTPS proxy content inspection feature, you must import each previous certificate in the chain of trust of the type *Other*. This configures the XTM device to trust the certificate. You must import these certificates from first to last, or from most prominent to least prominent, so the XTM device can connect the certificates in the chain of trust properly.

For more information, see *About Certificates* on page 491 and *Use Certificates for the HTTPS-Proxy* on page 505.

1. Select **System > Certificates**.
   The Certificates page appears.
2. Click **Import**.
3. Select the option that matches the function of the certificate:
   - **HTTPS Proxy Authority (for deep packet inspection)** — Select this option if the certificate is for an HTTPS proxy policy that manages web traffic requested by users on trusted or optional networks from a web server on an external network. A certificate you import for this purpose must be a CA certificate. Before you import the CA certificate used to re-encrypt traffic with an HTTPS proxy, make sure the CA certificate used to sign this certificate was imported with the *Other* category.
   - **HTTPS Proxy Server** — Select this option if the certificate is for an HTTPS proxy policy that manages web traffic requested by users on an external network from a web server protected by the XTM device. before you import the CA certificate used to re-encrypt traffic from an HTTPS web server, make sure the CA certificate used to sign this certificate was imported with the *Other* category .
   - **Trusted CA for HTTPS Proxy** — Select this option for a certificate used to trust HTTPS traffic that is not re-encrypted by the HTTPS proxy. For example, a root certificate or intermediate CA certificate used to sign the certificate of an external web server.
   - **IPSec, Web Server, Other** — Select this option if the certificate is for authentication or other purposes, or if you want to import a certificate to create a chain of trust to a certificate that is used to re-encrypt network traffic with an HTTPS proxy.

4. Copy and paste the contents of the certificate in the large text box. If the certificate includes a private key, type the password to decrypt the key.
5. Click **Import Certificate**.
   The certificate is added to the XTM device.

Use a Web Server Certificate for Authentication

To use a third-party certificate for this purpose, you must first import that certificate. See the previous procedure for more information. If you use a custom certificate signed by the XTM device, we recommend that you export the certificate and then import it on each client device that connects to the XTM device.

1. Select **Authentication > Web Server Certificate**.
   The Authentication Web Server Certificate page appears.
2. To use a previously imported third-party certificate, select **Third party certificate** and select the certificate in the drop-down list.
   Click **Save** and do not complete the other steps in this procedure.
3. To create a new certificate for XTM device authentication, select **Custom certificate signed by Firebox**.
4. Type a domain name or IP address of an interface on your XTM device in the text box at the bottom of the dialog box. Click **Add**. When you have added all the domain names you want, click **OK**.

5. Type the **Common name** for your organization. This is usually your domain name.
   Or, you can also type an **Organization name** and an **Organization unit name** (both optional) to identify what part of your organization created the certificate.
6. Click **Save**.

Create a CSR with OpenSSL

To create a certificate, you first need to create a Certificate Signing Request (CSR). You can send the CSR to a certification authority, or use it to create a self-signed certificate.

Use OpenSSL to Generate a CSR

OpenSSL is installed with most GNU/Linux distributions. To download the source code or a Windows binary file, go to http://www.openssl.org/ and follow the installation instructions for your operating system. You can use OpenSSL to convert certificates and certificate signing requests from one format to another. For more information, see the OpenSSL man page or online documentation.

1. Open a command line interface terminal.
2. To generate a private key file called privkey.pem in your current working directory, type `openssl genrsa -out privkey.pem 1024`
3. Type `openssl req -new -key privkey.pem -out request.csr`
   This command generates a CSR in the PEM format in your current working directory.
4. When you are prompted for the x509 Common Name attribute information, type your fully-qualified domain name (FQDN). Use other information as appropriate.
5. Follow the instructions from your certificate authority to send the CSR.

To create a temporary, self-signed certificate until the CA returns your signed certificate:

1. Open a command line interface terminal.
2. Type:
   `openssl x509 -req -days 30 -in request.csr -key privkey.pem -out sscert.cert`

This command creates a certificate inside your current directory that expires in 30 days with the private key and CSR you created in the previous procedure.

> ***Note*** *You cannot use a self-signed certificate for VPN remote gateway authentication. We recommend that you use certificates signed by a trusted Certificate Authority.*

Sign a Certificate with Microsoft CA

Although you can create a self-signed certificate with Firebox System Manager or other tools, you can also create a certificate with the Microsoft Certificate Authority (CA).

Each certificate signing request (CSR) must be signed by a certificate authority (CA) before it can be used for authentication. When you create a certificate with this procedure, you act as the CA and digitally sign your own CSR. For compatibility reasons, however, we recommend that you instead send your CSR to a widely known CA. The root certificates for these organizations are installed by default with most major Internet browsers and XTM devices, so you do not have to distribute the root certificates yourself.

You can use most Windows Server operating systems to complete a CSR and create a certificate. The subsequent instructions are for Windows Server 2003.

Send the Certificate Request

1. Open your web browser. In the location or address bar, type the IP address of the server where the Certification Authority is installed, followed by `certsrv`.
   For example: `http://10.0.2.80/certsrv`
2. Click the **Request a Certificate** link.
3. Click the **Advanced certificate request** link.
4. Click **Submit a certificate**.
5. Paste the contents of your CSR file into the **Saved Request** text box.
6. Click **OK**.
7. Close your web browser.

Issue the Certificate

1. Connect to the server where the Certification Authority is installed, if necessary.
2. Select **Start > Control Panel > Administrative Tools > Certification Authority**.
3. In the **Certification Authority (Local)** tree, select **Your Domain Name > Pending Requests**.
4. Select the **CSR** in the right navigation pane.
5. In the **Action** menu, select **All Tasks > Issue**.
6. Close the Certification Authority window.

Download the Certificate

1. Open your web browser. In the location or address bar, type the IP address of the server where the certification authority is installed, followed by certsrv.
   Example: `http://10.0.2.80/certsrv`
2. Click the **View the status of a pending certificate request** link.
3. Click the certificate request with the time and date you submitted.
4. To choose the PKCS10 or PKCS7 format, select **Base 64 encoded**.
5. Click **Download certificate** to save the certificate on your hard drive.

Certification Authority is distributed with Windows Server 2003 as a component. If the Certification Authority is not installed in the Administrative Tools folder of the Control Panel, follow the instructions from the manufacturer to install it.

Use Certificates for the HTTPS-Proxy

Many web sites use both the HTTP and HTTPS protocols to send information to users. While HTTP traffic can be examined easily, HTTPS traffic is encrypted. To examine HTTPS traffic requested by a user on your network, you must configure your XTM device to decrypt the information and then encrypt it with a certificate signed by a CA that each network user trusts.

By default, the XTM device re-encrypts the content it has inspected with an automatically generated self-signed certificate. Users without a copy of this certificate see a certificate warning when they connect to a secure web site with HTTPS. If the remote web site uses an expired certificate, or if that certificate is signed by a CA (Certificate Authority) the XTM device does not recognize, the XTM device re-signs the content as *Fireware HTTPS Proxy: Unrecognized Certificate* or simply *Invalid Certificate*.

This section includes information about how to export a certificate from the XTM device and import it on a Microsoft Windows or Mac OS X system to operate with the HTTPS-proxy. To import the certificate on other devices, operating systems, or applications, see the documentation from their manufacturers.

Protect a Private HTTPS Server

To protect an HTTPS server on your network, you must first import the CA certificate used to sign the HTTPS server certificate, and then import the HTTPS server certificate with its associated private key. If the CA certificate used to sign the HTTPS server certificate is not automatically trusted itself, you must import each trusted certificate in sequence for this feature to operate correctly. After you have imported all of the certificates, configure the HTTPS-proxy.

First, edit an HTTPS proxy action to enable deep content inspection of HTTPS content.

From Fireware XTM Web UI:

1. Select **Firewall > Proxy Actions**.
   The Proxy Actions page appears.
2. Select an HTTPS proxy action: **HTTPS-Client** or **HTTPS-Server**. Click **Edit**.
   The Edit Proxy Action page appears for the proxy action you selected.
3. Expand the **Content Inspection** section.
4. Select the **Enable deep inspection of HTTPS content** check box.
5. From the **Proxy Action** drop-down list, select the HTTP proxy action to use to inspect HTTPS content. For example, **HTTP-Client**.
6. Clear the **Use OCSP to confirm the validity of certificates** check box.
7. In the **Bypass List** text box, type the IP address of a web site for which you do not want to inspect traffic. Click **Add**.
8. (Optional) Repeat Step 7 to add more IP addresses to the **Bypass List**.
9. Click **Save**.
   If you edited a predefined proxy action, you must clone your changes to a new proxy action before you can save them and apply them to a proxy policy. The Clone Proxy Action dialog box appears.
10. In the **Name** text box, type a new name for the proxy action.
    For example, type `HTTPS-Client DCI`.
11. Click **OK**.
    The new proxy action appears in the Proxies list.

Next, add an HTTPS-proxy that uses the proxy action you added.

From Fireware XTM Web UI:

1. Select **Firewall > Firewall Policies**.
   The Firewall Policies page appears.
2. Click .
   The Select a Policy Type page appears.
3. Expand the **Proxies** category and select **HTTPS-proxy**.
4. Click **Add policy**.
   The Policy Configuration page appears for the HTTPS-proxy.
5. From the **Proxy Action** drop-down list, select the proxy action you added.
   For example, select **HTTPS-Client DCI**.
6. Click **Save**.

For more information, see*Manage XTM Device Certificates* on page 500.

Examine Content from External HTTPS Servers

If your organization already has a PKI (Public Key Infrastructure) set up with a trusted CA, then you can import a certificate on the XTM device that is signed by your organization CA. If the CA certificate is not automatically trusted itself, you must import each previous certificate in the chain of trust for this feature to operate correctly. For more information, see *Manage XTM Device Certificates* on page 500.

> ***Note*** *If you have other traffic that uses the HTTPS port, such as SSL VPN traffic, we recommend that you evaluate the content inspection feature carefully. The HTTPS-proxy attempts to examine all traffic on TCP port 443 in the same way. To ensure that other traffic sources operate correctly, we recommend that you add those IP addresses to the Bypass List. For more information, see HTTPS-Proxy: Content Inspection on page 380.*

Before you enable this feature, we recommend that you provide the certificate(s) used to sign HTTPS traffic to all of the clients on your network. You can attach the certificates to an email with instructions, or use network management software to install the certificates automatically. Also, we recommend that you test the HTTPS-proxy with a small number of users to ensure that it operates correctly before you apply the HTTPS-proxy to traffic on a large network.

If your organization does not have a PKI, you must copy the default or a custom self-signed certificate from the XTM device to each client device.

First, edit an HTTPS proxy action to enable deep content inspection of HTTPS content.

From Fireware XTM Web UI:

1. Select **Firewall > Proxy Actions**.
   The Proxy Actions page appears.
2. Select an HTTPS proxy action: **HTTPS-Client** or **HTTPS-Server**. Click **Edit**.
   The Edit Proxy Action page appears for the proxy action you selected.
3. Expand the **Content Inspection** section.
4. Select the **Enable deep inspection of HTTPS content** check box.
5. From the **Proxy Action** drop-down list, select the HTTP proxy action to use to inspect HTTPS content.
   For example, **HTTP-Client**.
6. Specify the options for OCSP certificate validation.

7. Click **Save**.
   If you edited a predefined proxy action, you must clone your changes to a new proxy action before you can save them and apply them to a proxy policy. The Clone Proxy Action dialog box appears.
8. In the **Name** text box, type a new name for the proxy action.
9. Click **OK**.
   The new proxy action appears in the Proxies list.

Next, add an HTTPS-proxy that uses the proxy action you added.

From Fireware XTM Web UI:

1. Select **Firewall > Firewall Policies**.
   The Firewall Policies page appears.
2. Click  .
   The Select a Policy Type page appears.
3. Expand the **Proxies** category and select **HTTPS-proxy**.
4. Click **Add policy**.
   The Policy Configuration page appears for the HTTPS-proxy.
5. From the **Proxy Action** drop-down list, select the proxy action you added.
   For example, select **HTTPS-Client DCI**.
6. Click **Save**.

When you enable content inspection, the HTTP proxy action WebBlocker settings override the HTTPS proxy WebBlocker settings. If you add IP addresses to the Bypass list, traffic from those sites is filtered with the WebBlocker settings from the HTTPS proxy.

For more information on WebBlocker configuration, see *About WebBlocker* on page 669.

Import the Certificates on Client Devices

To use certificates you have installed on the XTM device with client devices, you must export the certificates with Firebox System Manager, then import the certificates on each client. You cannot export a certificate from your XTM device with the Web UI.

For more information about how to import a certificate, see *Import a Certificate on a Client Device* on page 512.

For more information about how to export a certificate with Firebox System Manager, see Use Certificates for the HTTPS-Proxy in the *Fireware XTM WatchGuard System Manager Help*.

Troubleshoot Problems with HTTPS Content Inspection

The XTM device often creates log messages when there is a problem with a certificate used for HTTPS content inspection. We recommend that you check these log messages for more information.

If connections to remote web servers are often interrupted, check to make sure you have imported all of the certificates necessary to trust the CA certificate used to re-encrypt the HTTPS content, as well as the certificates necessary to trust the certificate from the original web server. You must import all of these certificates on the XTM device and each client device for connections to be successful.

Use Certificates for Mobile VPN With IPSec Tunnel Authentication

When a Mobile VPN tunnel is created, the identity of each endpoint must be verified with a key. This key can be a passphrase or pre-shared key (PSK) known by both endpoints, or a certificate from the Management Server. Your XTM device must be a managed device to use a certificate for Mobile VPN authentication. You must use WatchGuard System Manger to configure your XTM device as a managed device.

For more information, see WatchGuard System Manager Help.

To use certificates for a new Mobile VPN with IPSec tunnel:

1. Select **VPN > Mobile VPN with IPSec**.
2. Click **Add**.
3. Select the **IPSec Tunnel** tab.
4. In the **IPSec Tunnel** section, select **Use a certificate**.
5. In the **CA IP Address** text box, type the IP address of your Management Server.
6. In the **Timeout** text box, type or select the time in seconds the Mobile VPN with IPSec client waits for a response from the certificate authority before it stops connection attempts. We recommend you keep the default value.
7. Complete the Mobile VPN group configuration.

   For more information, see *Configure the XTM Device for Mobile VPN with IPSec* on page 596.

To change an existing Mobile VPN tunnel to use certificates for authentication:

1. Select **VPN > Mobile VPN with IPSec**.
2. Select the Mobile VPN group you want to change. Click **Edit**.
3. Select the **IPSec Tunnel** tab.
4. In the **IPSec Tunnel** section, select **Use a certificate**.
5. In the **CA IP Address** text box, type the IP address of your Management Server.
6. In the **Timeout** text box, type or select the time in seconds the Mobile VPN with IPSec client waits for a response from the certificate authority before it stops connection attempts. We recommend you keep the default value.
7. Click **Save**.

When you use certificates, you must give each Mobile VPN user three files:

- The end-user profile (.wgx)
- The client certificate (.p12)
- The CA root certificate (.pem)

Copy all of the files to the same directory. When an Mobile VPN user imports the .wgx file, the root and client certificates in the cacert.pem and the .p12 files are automatically loaded.

For more information on Mobile VPN with IPSec, see *About Mobile VPN with IPSec* on page 593.

Certificates for Branch Office VPN (BOVPN) Tunnel Authentication

When a BOVPN tunnel is created, the IPSec protocol checks the identity of each endpoint with either a pre-shared key (PSK) or a certificate imported and stored on the XTM device.

To use a certificate for BOVPN tunnel authentication:

1. Select **VPN > Branch Office VPN**.
2. In the **Gateways** section, click **Add** to create a new gateway.
   Or, select an existing gateway and click **Edit**.
3. Select **Use IPSec Firebox Certificate**.
4. Select the certificate you want to use.
5. Set other parameters as necessary.
6. Click **Save**.

If you use a certificate for BOVPN authentication:

- You must first import the certificate.
  For more information, see *Manage XTM Device Certificates* on page 500.
- Firebox System Manager must recognize the certificate as an IPSec-type certificate.
- Make sure certificates for the devices at each gateway endpoint use the same algorithm. Both endpoints must use either DSS or RSA. The algorithm for certificates appears in the table on the **Gateway** page.
- If you do not have a third-party or self-signed certificate, you must use the certificate authority on a WatchGuard Management Server.

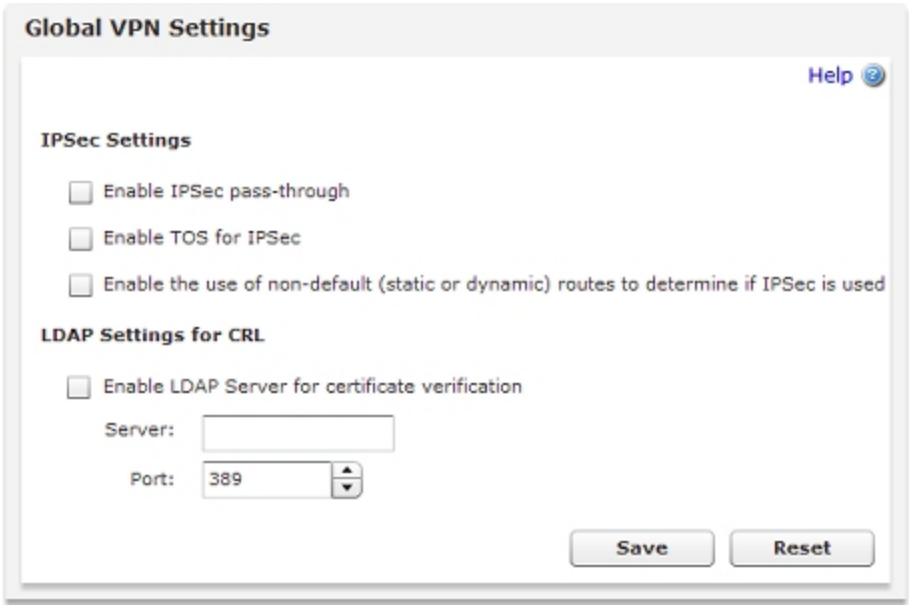
Verify the Certificate with FSM

1. Select **System > Certificates**.
   The Certificates page appears.
2. In the **Type** column, verify *IPSec* or *IPSec/Web* appears.

Verify VPN Certificates with an LDAP Server

You can use an LDAP server to automatically verify certificates used for VPN authentication if you have access to the server. You must have LDAP account information provided by a third-party CA service to use this feature.

1. Select **VPN > Global Settings**.
   The Global VPN Settings page appears.



2. Select the **Enable LDAP server for certificate verification** check box.
3. In the **Server** text box, type the name or address of the LDAP server.
4. (Optional) Type the **Port** number.
5. Click **Save**.
   Your XTM device checks the CRL stored on the LDAP server when tunnel authentication is requested.

Configure the Web Server Certificate for Firebox Authentication

When users connect to your XTM device with a web browser, they often see a security warning. This warning occurs because the default certificate is not trusted, or because the certificate does not match the IP address or domain name used for authentication. If you have Fireware XTM with a Pro upgrade, you can use a third-party or self-signed certificate that matches the IP or domain name for user authentication. You must import that certificate on each client browser or device to prevent the security warnings.

To configure the web server certificate for Firebox authentication:

1. Select **Authentication > Web Server Certificate**.

2. To use the default certificate, select **Default certificate signed by Firebox** and proceed to the last step in this procedure.
3. To use a certificate you have previously imported, select **Third-party certificate**.
4. Select a certificate from the adjacent drop-down list and continue with the last step in this procedure.
   This certificate must be recognized as a Web certificate.
5. If you want to create a custom certificate signed by your XTM device, select **Custom certificate signed by Firebox**.
6. Type the **common name** for your organization. This is usually your domain name.
7. (Optional) You can also type an **Organization Name** and an **Organization Unit Name** to identify the part of your organization that created the certificate.
8. To create additional subject names, or interface IP addresses for IP addresses on which the certificate is intended for use, type a **Domain name**.
9. Click the **Add** button adjacent to the text box to add each entry
10. Repeat Steps 8–9 to add more domain names.
11. Click **Save**.

Import a Certificate on a Client Device

When you configure your XTM device to use a custom or third-party certificate for authentication or HTTPS content inspection, you must import that certificate on each client in your network to prevent security warnings. This also allows services like Windows Update to operate correctly.

> ***Note*** *If you normally use Fireware XTM Web UI, you must install Firebox System Manager before you can export certificates.*

Import a PEM Format Certificate with Windows XP

This process allows Internet Explorer, Windows Update, and other programs or services that use the Windows certificate store on Microsoft Windows XP to get access to the certificate.

1. In the Windows **Start** menu, select **Run**.
2. Type `mmc` and click **OK**.
   A Windows Management Console appears.
3. Select **File > Add/Remove Snap-In**.
4. Click **Add**.
5. Select **Certificates**, then click **Add**.
6. Select **Computer account** and click **Next**.
7. Click **Finish**, **Close**, and **OK** to add the certificates module.
8. In the **Console Root** window, expand the **Certificates** tree.
9. Expand the **Trusted Root Certification Authorities** object.
10. Under the **Trusted Root Certification Authorities** object, right-click **Certificates** and select **All Tasks > Import**.
11. Click **Next**.
12. Click **Browse** to find and select the HTTPS Proxy Authority CA certificate you previously exported. Click **OK**.
13. Click **Next**, then click **Finish** to complete the wizard.

Import a PEM format certificate with Windows Vista

This process allows Internet Explorer, Windows Update, and other programs or services that use the Windows certificate store on Microsoft Windows Vista to get access to the certificate.

1. On the Windows **Start** menu, type `certmgr.msc` in the **Search** text box and press **Enter**.
   If you are prompted to authenticate as an administrator, type your password or confirm your access.
2. Select the **Trusted Root Certification Authorities** object.
3. From the **Action** menu, select **All Tasks > Import**.
4. Click **Next**. Click **Browse** to find and select the HTTPS Proxy Authority CA certificate you previously exported. Click **OK**.
5. Click **Next**, then click **Finish** to complete the wizard.

Import a PEM Format Certificate with Mozilla Firefox 3.x

Mozilla Firefox uses a private certificate store instead of the operating system certificate store. If clients on your network use the Firefox browser, you must import the certificate into the Firefox certificate store even if you have already imported the certificate on the host operating system.

When you have more than one XTM device that uses a self-signed certificate for HTTPS content inspection, clients on your network must import a copy of each XTM device certificate. However, the default self-signed XTM device certificates use the same name, and Mozilla Firefox only recognizes the first certificate you import when more than one certificate has the same name. We recommend that you replace the default self-signed certificates with a certificate signed by a different CA, and then distribute those CA certificates to each client.

1. In Firefox, select **Tools > Options**.
   The Options dialog box appears.
2. Click the **Advanced** icon.
3. Select the **Encryption** tab, then click **View Certificates**.
   The Certificate Manager dialog box appears.
4. Select the **Authorities** tab, then click **Import**.
5. Browse to select the certificate file, then click **Open**.
6. In the **Downloading Certificate** dialog box, select the **Trust this CA to identify web sites** check box. Click **OK**.
7. Click **OK** twice to close the **Certificate Manager** and **Options** dialog boxes.
8. Restart Firefox.

Import a PEM Format Certificate with Mac OS X 10.5

This process allows Safari and other programs or services that use the Mac OS X certificate store to get access to the certificate.

1. Open the **Keychain Access** application.
2. Select the **Certificates** category.
3. Click the **plus icon** (+) button on the lower toolbar, then find and select the certificate.
4. Select the **System** keychain, then click **Open**. You can also select the System keychain, then drag and drop the certificate file into the list.
5. Right-click the certificate and select **Get Info**.
   A certificate information window appears.
6. Expand the **Trust** category.
7. In the **When using this certificate** drop-down list, select **Always Trust**.
8. Close the certificate information window.
9. Type your administrator password to confirm your changes.

19 Virtual Private Networks (VPNs)

Introduction to VPNs

To move data safely between two private networks across an unprotected network, such as the Internet, you can create a virtual private network (VPN). You can also use a VPN for a secure connection between a host and a network. The networks and hosts at the endpoints of a VPN can be corporate headquarters, branch offices, or remote users. VPNs use encryption to secure data, and authentication to identify the sender and the recipient of the data. If the authentication information is correct, the data is decrypted. Only the sender and the recipient of the message can read the data sent through the VPN.

A VPN *tunnel* is the virtual path between the two private networks of the VPN. We refer to this path as a tunnel because a tunneling protocol such as IPSec, SSL, or PPTP is used to securely send the data packets. A gateway or computer that uses a VPN uses this tunnel to send the data packets across the public Internet to private IP addresses behind a VPN gateway.

Branch Office VPN

A Branch Office VPN (BOVPN) is an encrypted connection between two dedicated hardware devices. It is used most frequently to make sure the network communications between networks at two offices is secure. WatchGuard provides two methods to set up a BOVPN:

Manual BOVPN

You can use Policy Manager or Fireware XTM Web UI to manually configure a BOVPN between any two devices that support IPSec VPN protocols.

For more information, see *About Manual Branch Office VPN Tunnels* on page 528.

Managed BOVPN

You can use WatchGuard System Manager to set up a managed BOVPN between any two managed Firebox or XTM devices.

For more information, see the *Fireware XTM WatchGuard System Manager User Guide* or *Help* system.

All WatchGuard BOVPNs use the IPSec protocol suite to secure the BOVPN tunnel.

For more information about IPSec VPNs, see *About IPSec VPNs* on page 516.

Mobile VPN

A Mobile VPN is an encrypted connection between a dedicated hardware device and a laptop or desktop computer. A Mobile VPN allows your employees who telecommute and travel to securely connect to your corporate network. WatchGuard supports three types of Mobile VPNs:

- Mobile VPN with IPSec
- Mobile VPN with PPTP
- Mobile VPN with SSL

For a comparison of these Mobile VPN solutions, see *Select a Mobile VPN*.

About IPSec VPNs

WatchGuard Branch Office VPN and Mobile VPN with IPSec both use the IPSec protocol suite to establish VPNs between devices or mobile users. Before you configure an IPSec VPN, especially if you configure a manual BOVPN tunnel, it is helpful to understand how IPSec VPNs work.

For more information, see:

- *About IPSec Algorithms and Protocols*
- *About IPSec VPN Negotiations*
- *Configure Phase 1 and Phase 2 Settings*

About IPSec Algorithms and Protocols

IPSec is a collection of cryptography-based services and security protocols that protect communication between devices that send traffic through an untrusted network. Because IPSec is built on a collection of widely known protocols and algorithms, you can create an IPSec VPN between your XTM device and many other devices that support these standard protocols. The protocols and algorithms used by IPSec are discussed in the subsequent sections.

Encryption Algorithms

Encryption algorithms protect the data so it cannot be read by a third-party while in transit. Fireware XTM supports three encryption algorithms:

- DES (Data Encryption Standard) — Uses an encryption key that is 56 bits long. This is the weakest of the three algorithms.
- 3DES (Triple-DES) — An encryption algorithm based on DES that uses DES to encrypt the data three times.
- AES (Advanced Encryption Standard) — The strongest encryption algorithm available. Fireware XTM can use AES encryption keys of these lengths: 128, 192, or 256 bits.

Authentication Algorithms

Authentication algorithms verify the data integrity and authenticity of a message. Fireware XTM supports two authentication algorithms:

- HMAC-SHA1 (Hash Message Authentication Code — Secure Hash Algorithm 1) — SHA-1 produces a 160-bit (20 byte) message digest. Although slower than MD5, this larger digest size makes it stronger against brute force attacks.
- HMAC-MD5 (Hash Message Authentication Code — Message Digest Algorithm 5) — MD5 produces a 128 bit (16 byte) message digest, which makes it faster than SHA-1.

IKE Protocol

Defined in RFC2409, IKE (Internet Key Exchange) is a protocol used to set up security associations for IPSec. These security associations establish shared session secrets from which keys are derived for encryption of tunneled data. IKE is also used to authenticate the two IPSec peers.

Diffie-Hellman Key Exchange Algorithm

The Diffie-Hellman (DH) key exchange algorithm is a method used to make a shared encryption key available to two entities without an exchange of the key. The encryption key for the two devices is used as a symmetric key for encrypting data. Only the two parties involved in the DH key exchange can deduce the shared key, and the key is never sent over the wire.

A Diffie-Hellman *key group* is a group of integers used for the Diffie-Hellman key exchange. Fireware XTM can use DH groups 1, 2, and 5. The higher group numbers provide stronger security.

For more information, see *About Diffie-Hellman Groups* on page 539.

AH

Defined in RFC 2402, AH (Authentication Header) is a protocol that you can use in manual BOVPN Phase 2 VPN negotiations. To provide security, AH adds authentication information to the IP datagram. Most VPN tunnels do not use AH because it does not provide encryption.

ESP

Defined in RFC 2406, ESP (Encapsulating Security Payload) provides authentication and encryption of data. ESP takes the original payload of a data packet and replaces it with encrypted data. It adds integrity checks to make sure that the data is not altered in transit, and that the data came from the proper source. We recommend that you use ESP in BOVPN Phase 2 negotiations because ESP is more secure than AH. Mobile VPN with IPSec always uses ESP.

About IPSec VPN Negotiations

The devices at either end of an IPSec VPN tunnel are IPSec peers. When two IPSec peers want to make a VPN between them, they exchange a series of messages about encryption and authentication, and attempt to agree on many different parameters. This process is known as VPN negotiations. One device in the negotiation sequence is the initiator and the other device is the responder.

VPN negotiations happen in two distinct phases: *Phase 1* and *Phase 2*.

Phase 1

The main purpose of Phase 1 is to set up a secure encrypted channel through which the two peers can negotiate Phase 2. When Phase 1 finishes successfully, the peers quickly move on to Phase 2 negotiations. If Phase 1 fails, the devices cannot begin Phase 2.

Phase 2

The purpose of Phase 2 negotiations is for the two peers to agree on a set of parameters that define what traffic can go through the VPN, and how to encrypt and authenticate the traffic. This agreement is called a Security Association.

The Phase 1 and Phase 2 configurations must match for the devices on either end of the tunnel.

Phase 1 Negotiations

In Phase 1 negotiations, the two peers exchange credentials. The devices identify each other and negotiate to find a common set of Phase 1 settings to use. When Phase 1 negotiations are completed, the two peers have a Phase 1 Security Association (SA). This SA is valid for only a certain amount of time. After the Phase 1 SA expires, if the two peers must complete Phase 2 negotiations again, they must also negotiate Phase 1 again.

Phase 1 negotiations include these steps:

1. The devices exchange credentials.

   The credentials can be a certificate or a pre-shared key. Both gateway endpoints must use the same credential method. If one peer uses a pre-shared key, the other peer must also use a pre-shared key, and the keys must match. If one peer uses a certificate, the other peer must also use a certificate.

2. The devices identify each other.

   Each device provides a Phase 1 identifier, which can be an IP address, domain name, domain information, or an X500 name. The VPN configuration on each peer contains the Phase 1 identifier of the local and the remote device, and the configurations must match.

3. The peers decide whether to use Main Mode or Aggressive Mode.

   Phase 1 negotiations can use one of two different modes: Main Mode or Aggressive Mode. The device that starts the IKE negotiations (the initiator) sends either a Main Mode proposal or an Aggressive Mode proposal. The responder can reject the proposal if it is not configured to use that mode. Aggressive Mode communications take place with fewer packet exchanges. Aggressive Mode is less secure but faster than Main Mode.

4. The peers agree on Phase 1 parameters.
   - Whether to use NAT traversal
   - Whether to send IKE keep-alive messages (supported between Firebox or XTM devices only)
   - Whether to use Dead Peer Detection (RFC 3706)
5. The peers agree on Phase 1 Transform settings.

   Transform settings include a set of authentication and encryption parameters, and the maximum amount of time for the Phase 1 SA. The settings in the Phase 1 transform must exactly match a Phase 1 transform on the IKE peer, or IKE negotiations fail.

   The items you can set in the transform are:

   - Authentication — The type of authentication (SHA1 or MD5).
   - Encryption — The type of encryption algorithm (DES, 3DES or AES).
   - SA Life — The amount of time until the Phase 1 Security Association expires.
   - Key Group — The Diffie-Hellman key group.

Phase 2 Negotiations

After the two IPSec peers complete Phase 1 negotiations, Phase 2 negotiations begin. Phase 2 negotiations is to establish the Phase 2 SA (sometimes called the IPSec SA). The IPSec SA is a set of traffic specifications that tell the device what traffic to send over the VPN, and how to encrypt and authenticate that traffic. In Phase 2 negotiations, the two peers agree on a set of communication parameters. When you configure the BOVPN tunnel in Policy Manager or in Fireware XTM Web UI, you specify the Phase 2 parameters.

Because the peers use the Phase 1 SA to secure the Phase 2 negotiations, and you define the Phase 1 SA settings in the BOVPN Gateway settings, you must specify the gateway to use for each tunnel.

Phase 2 negotiations include these steps:

1. The peers use the Phase 1 SA to secure Phase 2 negotiations.

   Phase 2 negotiations can only begin after Phase 1 SA has been established.

2. The peers exchange Phase 2 identifiers (IDs).

   Phase 2 IDs are always sent as a pair in a Phase 2 proposal: one indicates which IP addresses behind the local device can send traffic over the VPN, and the other indicates which IP addresses behind the remote device can send traffic over the VPN. This is also known as a *tunnel route*. You can specify the Phase 2 IDs for the local and remote peer as a host IP address, a network IP address, or an IP address range.

3. The peers agree on whether to use Perfect Forward Secrecy (PFS).

   PFS specifies how Phase 2 keys are derived. When PFS is selected, both IKE peers must use PFS, or Phase 2 rekeys fail. PFS guarantees that if an encryption key used to protect the data transmission is compromised, an attacker can access only the data protected by that key, not subsequent keys. If the peers agree to use PFS, they must also agree on the Diffie-Hellman key group to use for PFS.

4. The peers agree on a Phase 2 proposal.

   The Phase 2 proposal includes the IP addresses that can send traffic over the tunnel, and a group of encryption and authentication parameters. Fireware XTM sends these parameters in a Phase 2 proposal. The proposal includes the algorithm to use to authenticate data, the algorithm to use to encrypt data, and how often to make new Phase 2 encryption keys.

The items you can set in a Phase 2 proposal include:

Type

For a manual BOVPN, you can select the type of protocol to use: Authentication Header (AH) or Encapsulating Security Payload (ESP). ESP provides authentication and encryption of the data. AH provides authentication without encryption. We recommend you select ESP. Managed BOVPN and Mobile VPN with IPSec always use ESP.

Authentication

Authentication makes sure that the information received is exactly the same as the information sent. You can use SHA or MD5 as the algorithm the peers use to authenticate IKE messages from each other. SHA1 is more secure.

Encryption

Encryption keeps the data confidential. You can select DES, 3DES, or AES. AES is the most secure.

Force Key Expiration

To make sure Phase 2 encryption keys change periodically, always enable key expiration. The longer a Phase 2 encryption key is in use, the more data an attacker can collect to use to mount an attack on the key.

Configure Phase 1 and Phase 2 Settings

You configure Phase 1 and Phase 2 settings for each IPSec VPN you configure.

Branch Office VPN

For a manual Branch Office VPN (BOVPN), you configure Phase 1 settings when you define a Branch Office gateway, and you configure Phase 2 settings when you define a Branch Office tunnel.

For more information about BOVPN Phase 1 and Phase 2 settings, see:

- *Configure Gateways* on page 532
- *Define a Tunnel* on page 542

Mobile VPN with IPSec

For Mobile VPN with IPSec, you configure the Phase 1 and Phase 2 settings when you add or edit a Mobile VPN with IPSec configuration.

For more information, see:

- *Configure the XTM Device for Mobile VPN with IPSec*
- *Modify an Existing Mobile VPN with IPSec Group Profile*

Use a Certificate for IPSec VPN Tunnel Authentication

When an IPSec tunnel is created, the IPSec protocol checks the identity of each endpoint with either a pre-shared key (PSK) or a certificate imported and stored on the XTM device. You configure the tunnel authentication method in the VPN Phase 1 settings.

For more information about how to use a certificate for tunnel authentication, see:

- *Certificates for Branch Office VPN (BOVPN) Tunnel Authentication*
- *Use Certificates for Mobile VPN With IPSec Tunnel Authentication*

About Mobile VPNs

A *Mobile VPN* enables your employees who telecommute and travel to securely connect to your corporate network. Fireware XTM supports three forms of remote user virtual private networks: Mobile VPN with IPSec, Mobile VPN with PPTP, and Mobile VPN with SSL.

When you use Mobile VPN, you first configure your XTM device and then configure the remote client computers. You use Policy Manager or Fireware XTM Web UI to configure the settings for each user or group of users. For Mobile VPN with IPSec and Mobile VPN with SSL, you use Policy Manager or the Web UI to create an end user profile configuration file that includes all the settings necessary to connect to the XTM device. You can also configure your policies to allow or deny traffic from Mobile VPN clients. Mobile VPN users authenticate either to the XTM device user database or to an external authentication server.

Select a Mobile VPN

Fireware XTM supports three types of Mobile VPN. Each type uses different ports, protocols, and encryption algorithms.

Mobile VPN with PPTP

- PPTP (Point-to-Point Tunneling Protocol) — Secures the tunnel between two endpoints
- TCP port 1723 — Establishes the tunnel
- IP protocol 47 — Encrypts the data
- Encryption algorithms — 40 bit or 128 bit

Mobile VPN with IPSec

- IPSec (Internet Protocol Security) — Secure the tunnel between two endpoints
- UDP port 500 (IKE) — Establishes the tunnel
- UDP port 4500 (NAT Traversal) — Used if the XTM device is configured for NAT
- IP protocol 50 (ESP) or IP Protocol 51 (AH) — Encrypts the data
- Encryption algorithms — DES, 3DES, or AES (128, 192, or 256 bit)

Mobile VPN with SSL

- SSL (Secure Sockets Layer) — Secures the tunnel between two endpoints
- TCP port 443 or UDP port 443 — Establishes the tunnel and encrypts the data
- Encryption algorithms — Blowfish, DES, 3DES, or AES (128, 192, or 256 bit)

> ***Note*** *For Mobile VPN with SSL, you can choose a different port and protocol. For more information, see Choose the Port and Protocol for Mobile VPN with SSL on page 658*

The type of Mobile VPN you select largely depends on your existing infrastructure and your network policy preferences. The XTM device can manage all three types of mobile VPN simultaneously. A client computer can be configured to use one or more methods. Some of the things to consider when you select what type of Mobile VPN to use are described in the subsequent sections.

VPN Tunnel Capacity and Licensing

When you select a type of tunnel, make sure to consider the number of tunnels your device supports and whether you can purchase an upgrade to increase the number of tunnels.

Mobile VPN	Maximum VPN tunnels
Mobile VPN with PPTP	50 tunnels
Mobile VPN with IPSec	▪ Base and maximum tunnels vary by XTM device model. ▪ License purchase is required to enable the maximum number of tunnels.
Mobile VPN with SSL	▪ Base and maximum tunnels vary by XTM device model. ▪ Pro upgrade for the Fireware XTM OS is required for maximum SSL VPN tunnels. ▪ To support more than one SSL VPN tunnel you must have a Pro upgrade.

For the base and maximum number of tunnels supported for Mobile VPN with IPSec and Mobile VPN with SSL, see the detailed specifications for your XTM device model.

Authentication Server Compatibility

When you select a Mobile VPN solution, make sure to choose a solution that supports the type of authentication server you use.

Mobile VPN	XTM device	RADIUS	Vasco/ RADIUS	Vasco Challenge Response	RSA SecurID	LDAP	Active Directory
Mobile VPN with PPTP	Yes	Yes	No	No	No	No	No
Mobile VPN with IPSec	Yes	Yes	Yes	N/A	Yes	Yes	Yes
Mobile VPN with SSL	Yes	Yes	Yes	N/A	Yes	Yes	Yes

Client Configuration Steps and Operating System Compatibility

The configuration steps you must complete are different for each Mobile VPN solution. Each VPN solution is also compatible with different operating systems.

Mobile VPN with PPTP

You do not install WatchGuard VPN client software. You must manually configure the network settings on each client computer to set up a PPTP connection.

Compatible with: Windows XP, and Windows Vista.

Mobile VPN with IPSec

You must install the WatchGuard Mobile VPN with IPSec client and manually import the end user profile. The Mobile VPN with IPSec client requires more steps to set up than the Mobile VPN with SSL client.

Compatible with: Windows XP SP2 (32 bit and 64 bit), Windows Vista (32 bit and 64 bit), and Windows 7 (32 bit and 64 bit).

Mobile VPN with SSL

You must install the WatchGuard Mobile VPN with SSL client and configuration file.

Compatible with: Windows XP SP2 (32 bit and 64 bit), Windows Vista (32 bit and 64 bit), Windows 7 (32 bit and 64 bit), Mac OS X 10.6 Snow Leopard, and Mac OS X 10.5 Leopard

Internet Access Options for Mobile VPN Users

For all three types of Mobile VPN, you have two options for Internet access for your Mobile VPN users:

Force all client traffic through tunnel (default-route VPN)

The most secure option is to require that all remote user Internet traffic is routed through the VPN tunnel to the XTM device. Then, the traffic is sent back out to the Internet. With this configuration (known as default-route VPN), the XTM device is able to examine all traffic and provide increased security, although it uses more processing power and bandwidth.

When you use default-route VPN with Mobile VPN for IPSec or Mobile VPN for PPTP, a dynamic NAT policy must include the outgoing traffic from the remote network. This enables remote users to browse the Internet when they send all traffic to the XTM device.

Allow direct access to the Internet (split tunnel VPN)

Another configuration option is to enable split tunneling. With this option, your users can browse the Internet, but Internet traffic is not sent through the VPN tunnel. Split tunneling improves network performance, but decreases security because the policies you create are not applied to the Internet traffic. If you use split tunneling, we recommend that each client computer have a software firewall.

For more information specific to each type of Mobile VPN, see:

- *Options for Internet Access Through a Mobile VPN with IPSec Tunnel*
- *Options for Internet Access Through a Mobile VPN with PPTP Tunnel*

- *Options for Internet Access Through a Mobile VPN with SSL Tunnel*

Mobile VPN Setup Overview

When you set up Mobile VPN, you must first configure the XTM device and then configure the client computers. Regardless of which type of Mobile VPN you choose, you must complete the same five configuration steps. The details for each step are different for each type of VPN.

1. Activate Mobile VPN in Policy Manager.
2. Define VPN settings for the new tunnel.
3. Select and configure the method of authentication for Mobile VPN users.
4. Define policies and resources.
5. Configure the client computers.
    - For Mobile VPN with IPSec and Mobile VPN with SSL, install the client software and configuration file.
    - For Mobile VPN with PPTP, manually configure the PPTP connection in the client computer network settings.

For more information and detailed steps to set up each type of Mobile VPN, see:

- *About Mobile VPN with IPSec*
- *About Mobile VPN with PPTP*
- *About Mobile VPN with SSL*

20 Branch Office VPNs

What You Need to Create a Manual BOVPN

Before you configure a branch office VPN network on your XTM device, read these requirements:

- You must have two XTM devices, or one XTM device and a second device that uses IPSec standards. You must enable the VPN option on the other device if it is not already active.
- You must have an Internet connection.
- The ISP for each VPN device must allow IPSec traffic on their networks.
  Some ISPs do not let you create VPN tunnels on their networks unless you upgrade your Internet service to a level that supports VPN tunnels. Speak with a representative from each ISP to make sure these ports and protocols are allowed:
    - UDP Port 500 (Internet Key Exchange or IKE)
    - UDP Port 4500 (NAT traversal)
    - IP Protocol 50 (Encapsulating Security Payload or ESP)
- If the other side of the VPN tunnel is a XTM device and each device is under management, you can use the Managed VPN option. Managed VPN is easier to configure than Manual VPN. To use this option, you must get information from the administrator of the XTM device on the other side of the VPN tunnel.
- You must know whether the IP address assigned to the external interface of your XTM device is static or dynamic.
  For more information about IP addresses, see *About IP Addresses* on page 3.
- Your XTM device model tells you the maximum number of VPN tunnels that you can create. If your XTM device model can be upgraded, you can purchase a model upgrade that increases the maximum number of supported VPN tunnels.
- If you connect two Microsoft Windows NT networks, they must be in the same Microsoft Windows domain, or they must be trusted domains. This is a Microsoft Networking issue, and not a limitation of the XTM device.
- If you want to use the DNS and WINS servers from the network on the other side of the VPN tunnel, you must know the IP addresses of these servers.
  The XTM device can give WINS and DNS IP addresses to the computers on its trusted network if those computers get their IP addresses from the XTM device with DHCP.

- If you want to give the computers the IP addresses of WINS and DNS servers on the other side of the VPN, you can type those addresses into the DHCP settings in the trusted network setup.
  For information on how to configure the XTM device to distribute IP addresses with DHCP, see *Configure DHCP in Mixed Routing Mode* on page 87.
- You must know the network address of the private (trusted) networks behind your XTM device and of the network behind the other VPN device, and their subnet masks.

> ***Note*** *The private IP addresses of the computers behind your XTM device cannot be the same as the IP addresses of the computers on the other side of the VPN tunnel. If your trusted network uses the same IP addresses as the office to which it will create a VPN tunnel, then your network or the other network must change their IP address arrangement to prevent IP address conflicts.*

About Manual Branch Office VPN Tunnels

A *VPN (Virtual Private Network)* creates secure connections between computers or networks in different locations. Each connection is known as a *tunnel*. When a VPN tunnel is created, the two tunnel endpoints authenticate with each other. Data in the tunnel is encrypted. Only the sender and the recipient of the traffic can read it.

Branch Office Virtual Private Networks (BOVPN) enable organizations to deliver secure, encrypted connectivity between geographically separated offices. The networks and hosts on a BOVPN tunnel can be corporate headquarters, branch offices, remote users, or telecommuters. These communications often contain the types of critical data exchanged inside a corporate firewall. In this scenario, a BOVPN provides confidential connections between these offices. This streamlines communication, reduces the cost of dedicated lines, and maintains security at each endpoint.

Manual BOVPN tunnels are those created with the Fireware XTM Web UI, which provides many additional tunnel options. Another type of tunnel is a *managed BOVPN tunnel*,which is a BOVPN tunnel that you can create in WatchGuard System Manager with a drag-and-drop procedure, a wizard, and the use of templates. For information about this type of tunnel, see the WatchGuard System Manager User Guide or online help system.

What You Need to Create a VPN

In addition to the VPN requirements, you must have this information to create a manual VPN tunnel:

- You must know whether the IP address assigned to the other VPN device is static or dynamic. If the other VPN device has a dynamic IP address, your XTM device must find the other device by domain name and the other device must use Dynamic DNS.
- You must know the shared key (passphrase) for the tunnel. The same shared key must be used by each device.
- You must know the encryption method used for the tunnel (DES, 3DES, AES-128 bit, AES-192 bit, or AES-256 bit). The two VPN devices must use the same encryption method.
- You must know the authentication method for each end of the tunnel (MD5 or SHA-1). The two VPN devices must use the same authentication method.

For more information, see *What You Need to Create a Manual BOVPN* on page 527.

We recommend that you write down your XTM device configuration and the related information for the other device. See the *Sample VPN Address Information Table* on page 531 to record this information.

How to Create a Manual BOVPN Tunnel

The basic procedure to create a manual tunnel includes these steps:

1. *Configure Gateways* — Configure the connection points on both the local and remote sides of the tunnel.
2. *Make Tunnels Between Gateway Endpoints* — Configure routes for the tunnel, specify how the devices control security, and make a policy for the tunnel.

Other options you can use for BOVPN tunnels are described in the subsequent sections.

One-Way Tunnels

Set up outgoing dynamic NAT through a BOVPN tunnel if you want to keep the VPN tunnel open in one direction only. This can be helpful when you make a tunnel to a remote site where all VPN traffic comes from one public IP address.

VPN Failover

VPN tunnels automatically fail over to the backup WAN interface during a WAN failover. You can configure BOVPN tunnels to fail over to a backup peer endpoint if the primary endpoint becomes unavailable. To do this, you must define at least one backup endpoint, as described in *Configure VPN Failover* on page 568.

Global VPN Settings

Global VPN settings on your XTM device apply to all manual BOVPN tunnels, managed tunnels, and Mobile VPN tunnels. You can use these settings to:

- Enable IPSec pass-through
- Clear or maintain the settings of packets with Type of Service (TOS) bits set
- Enable the use of non-default routes to determine if IPSec is used
- Use an LDAP server to verify certificates
- Configure the XTM device to send a notification when a BOVPN tunnel is down (BOVPN tunnels only)

To change these settings, from the Fireware XTM Web UI, select **VPN > Global Settings**. For more information on these settings, see *About Global VPN Settings* on page 549.

BOVPN Tunnel Status

To see the current status of BOVPN tunnels. In the Fireware XTM Web UI, select **System Status > VPN Statistics**. For more information, see *VPN Statistics* on page 488.

Rekey BOVPN Tunnels

You can use the Fireware Web UI to immediately generate new keys for BOVPN tunnels instead of waiting for them to expire. For more information, see *Rekey BOVPN Tunnels* on page 570.

Sample VPN Address Information Table

Item	Description	Assigned by
External IP Address	The IP address that identifies the IPSec-compatible device on the Internet. ISP Example: Site A: 207.168.55.2 Site B: 68.130.44.15	ISP
Local Network Address	An address used to identify a local network. These are the IP addresses of the computers on each side that are allowed to send traffic through the VPN tunnel. We recommend that you use an address from one of the reserved ranges: 10.0.0.0/8—255.0.0.0 172.16.0.0/12—255.240.0.0 192.168.0.0/16—255.255.0.0 The numbers after the slashes indicate the subnet masks. /24 means that the subnet mask for the trusted network is 255.255.255.0. For more information about slash notation, see *About Slash Notation* on page 3. Example: Site A: 192.168.111.0/24 Site B: 192.168.222.0/24	You
Shared Key	The shared key is a passphrase used by two IPSec-compatible devices to encrypt and decrypt the data that goes through the VPN tunnel. The two devices use the same passphrase. If the devices do not have the same passphrase, they cannot encrypt and decrypt the data correctly. Use a passphrase that contains numbers, symbols, lowercase letters, and uppercase letters for better security. For example, “Gu4c4mo!3” is better than “guacamole”. Example: Site A: OurSharedSecret Site B: OurSharedSecret	You
Encryption Method	DES uses 56-bit encryption. 3DES uses 168-bit encryption. AES encryption is available at the 128-bit, 192-bit, and 256-bit levels. AES-256 bit is the most secure encryption. The two devices must use the same encryption method. Example: Site A: 3DES Site B: 3DES	You
Authentication	The two devices must use the same authentication method. Example: Site A: MD5 (or SHA-1) Site B: MD5 (or SHA-1)	You

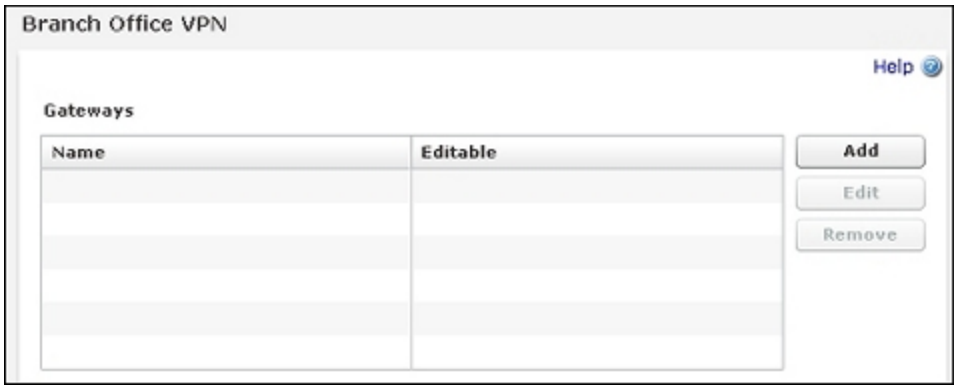
Configure Gateways

A gateway is a connection point for one or more tunnels. To create a tunnel, you must set up gateways on both the local and remote endpoint devices. To configure these gateways, you must specify:

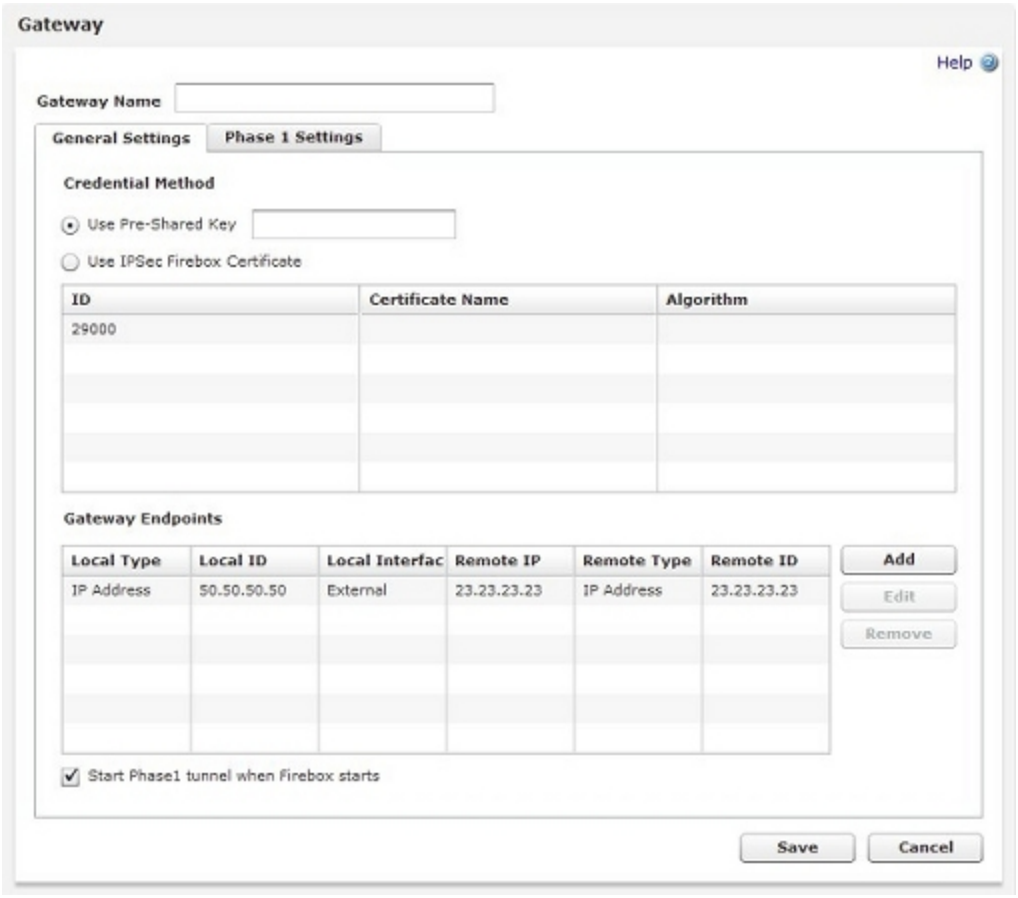
- Credential method — Either pre-shared keys or an IPSec XTM device certificate.
  For information about using certificates for BOVPN authentication, see *Certificates for Branch Office VPN (BOVPN) Tunnel Authentication* on page 509.
- Location of local and remote gateway endpoints, either by IP address or domain information.
- Settings for Phase 1 of the Internet Key Exchange (IKE) negotiation. This phase defines the security association, or the protocols and settings that the gateway endpoints will use to communicate, to protect data that is passed in the negotiation.

You can use Fireware XTM Web UI to configure the gateways for each endpoint device.

1. Select **VPN > Branch Office VPN**.
   The Branch Office VPN configuration page appears, with the Gateways list at the top.



2. To add a gateway, click **Add** adjacent to the Gateways list.
   The Gateway settings page appears.



3. In the **Gateway Name** text box, type a name to identify the gateway for this XTM device.
4. From the **Gateway** page, select either **Use Pre-Shared Key** or **Use IPSec Firebox Certificate** to identify the authentication procedure this tunnel uses.

   If you selected Use Pre-Shared Key

   Type or paste the shared key. You must use the same shared key on the remote device. This shared key must use only standard ASCII characters.

   If you selected Use IPSec Firebox Certificate

   The table below the radio button shows current certificates on the XTM device. Select the certificate to use for the gateway.

   For more information, see *Certificates for Branch Office VPN (BOVPN) Tunnel Authentication* on page 509.

You can now *Define Gateway Endpoints*.

Define Gateway Endpoints

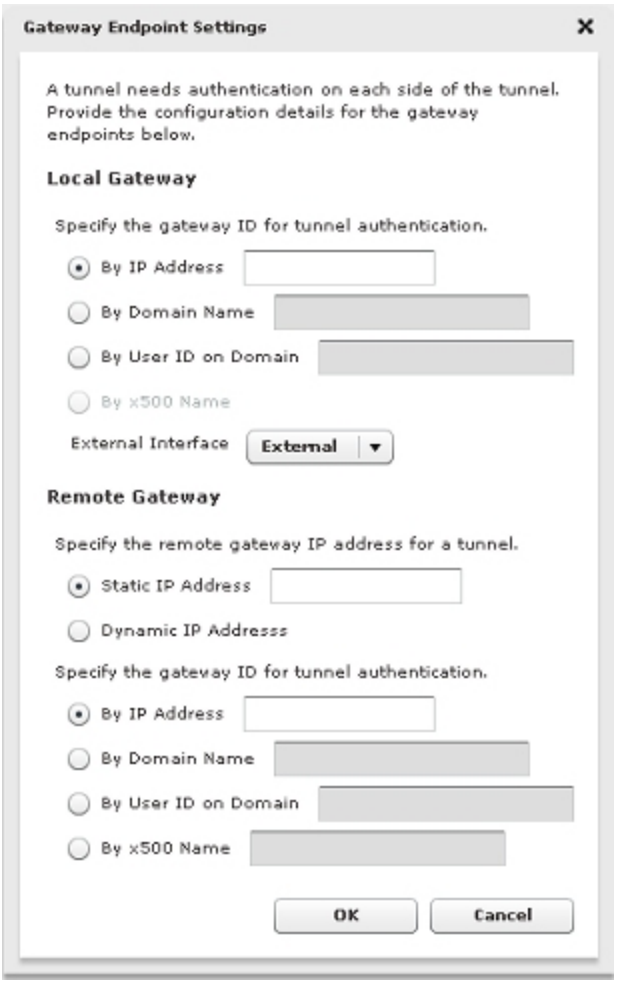
Gateway Endpoints are the local and remote gateways that a BOVPN connects. This information tells your XTM device how to identify and communicate with the remote endpoint device when it negotiates the BOVPN. It also tells the XTM device how to identify itself to the remote endpoint when it negotiates the BOVPN.

Any external interface can be a gateway endpoint. If you have more than one external interface, you can configure multiple gateway endpoints to *Configure VPN Failover*.

Local Gateway

In the Local Gateway section, you configure the gateway ID and the interface the BOVPN connects to on your XTM device. For the gateway ID, if you have a static IP address you can select **By IP Address**. Use **By Domain Information** if you have a domain that resolves to the IP address the BOVPN connects to on your XTM device.

1. In the **Gateway Endpoints** section of the **Gateway** page, click **Add**.
   The New Gateway Endpoints Settings dialog box appears.



2. Specify the gateway ID.
   - **By IP address** — Select **By IP Address**. Type the IP address of the XTM device interface IP address .
   - **By Domain Name** — Type your domain name.
   - **By User ID on Domain** — Type the user name and domain with the format `UserName@DomainName`.
   - **By x500 Name** — Type the x500 name.
3. From the **External Interface** drop-down list, select the interface on the XTM device with the IP address or domain you choose for the gateway ID.

Remote Gateway

In the Remote Gateway section, you configure the gateway IP address and gateway ID for the remote endpoint device that the BOVPN connects to. The gateway IP address can be either a **Static IP address** or a **Dynamic IP address**. The gateway ID can be **By Domain Name**, **By User ID on Domain**, or **By x500 Name**. The administrator of the remote gateway device can tell you which to use.

1. Select the remote gateway IP address.
   - **Static IP address** — Select this option if the remote device has a static IP address. For IP Address, type the IP address or select it from the drop-down list.
   - **Dynamic IP address** — Select this option if the remote device has a dynamic IP address.
2. Select the gateway ID.
   - **By IP address** — Select the **By IP Address** radio button. Type the IP address.
   - **By Domain Name** — Type the domain name.
   - **By User ID on Domain** — Type the user ID and domain.
   - **By x500 Name** — Type the x500 name.

   Note *If the remote VPN endpoint uses DHCP or PPPoE to get its external IP address, set the ID type of the remote gateway to **Domain Name**. Set the peer name to the fully qualified domain name of the remote VPN endpoint. The XTM device uses the IP address and domain name to find the VPN endpoint. Make sure the DNS server used by the XTM device can identify the name.*
3. Click **OK** to close the **New Gateway Endpoints Settings** dialog box.
   The Gateway page appears. The gateway pair you defined appears in the list of gateway endpoints.
4. Go to *Configure Mode and Transforms (Phase 1 Settings)* to configure Phase 1 settings for this gateway.

Configure Mode and Transforms (Phase 1 Settings)

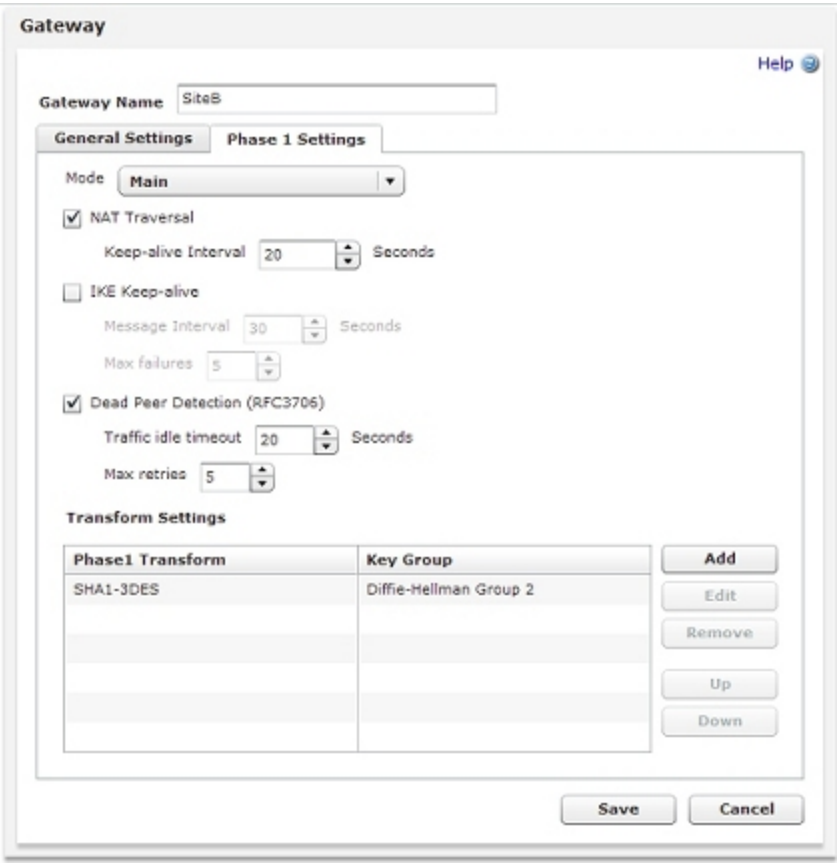
Phase 1 of establishing an IPSec connection is where the two peers make a secure, authenticated channel they can use to communicate. This is known as the ISAKMP Security Association (SA).

A Phase 1 exchange can use either *Main Mode* or *Aggressive Mode*. The mode determines the type and number of message exchanges that take place during this phase.

A transform is a set of security protocols and algorithms used to protect VPN data. During IKE negotiation, the peers make an agreement to use a certain transform.

You can define a tunnel such that it offers a peer more than one transform for negotiation. For more information, see *Add a Phase 1 Transform* on page 538.

1. In the **Gateway** page, select the **Phase 1 Settings** tab.



2. From the **Mode** drop-down list, select **Main**, **Aggressive**, or **Main fallback to Aggressive**.

   Main Mode

   This mode is more secure, and uses three separate message exchanges for a total of six messages. The first two messages negotiate policy, the next two exchange Diffie-Hellman data, and the last two authenticate the Diffie-Hellman exchange. Main Mode supports Diffie-Hellman groups 1, 2, and 5. This mode also allows you to use multiple transforms, as described in *Add a Phase 1 Transform* on page 538.

Aggressive Mode

This mode is faster because it uses only three messages, which exchange *About Diffie-Hellman Groups* data and identify the two VPN endpoints. The identification of the VPN endpoints makes Aggressive Mode less secure.

Main fallback to aggressive

The XTM device attempts Phase 1 exchange with Main Mode. If the negotiation fails, it uses Aggressive Mode.

3. If you want to build a BOVPN tunnel between the XTM device and another device that is behind a NAT device, select the **NAT Traversal** check box. NAT Traversal, or UDP Encapsulation, enables traffic to get to the correct destinations.
4. To have the XTM device send messages to its IKE peer to keep the VPN tunnel open, select the **IKE Keep-alive** check box.
5. In the **Message Interval** text box, type or select the number of seconds that pass before the next IKE Keep-alive message is sent.

> ***Note*** *IKE Keep-alive is used only by XTM devices. Do not enable it if the remote endpoint is a third-party IPSec device.*

6. To set the maximum number of times the XTM device tries to send an IKE keep-alive message before it tries to negotiate Phase 1 again, type the number you want in the **Max failures** box.
7. Use the **Dead Peer Detection** check box to enable or disable traffic-based dead peer detection. When you enable dead peer detection, the XTM device connects to a peer only if no traffic is received from the peer for a specified length of time and a packet is waiting to be sent to the peer. This method is more scalable than IKE keep-alive messages.

   If you want to change the XTM device defaults, in the **Traffic idle timeout**text box, type or select the amount of time (in seconds) that passes before the XTM device tries to connect to the peer. In the **Max retries** text box, type or select the number of times the XTM device tries to connect before the peer is declared dead.

   Dead Peer Detection is an industry standard that is used by most IPSec devices. We recommend that you select Dead Peer Detection if both endpoint devices support it.

> ***Note*** *If you configure VPN failover, you must enable DPD. For more information about VPN failover, see Configure VPN Failover on page 568*

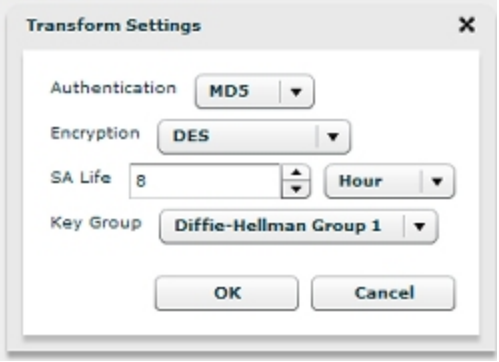
8. The XTM device contains one default transform set, which appears in the **Transform Settings** list. This transform specifies SHA-1 authentication, 3DES encryption, and Diffie-Hellman Group 2.
   You can:
   - Use this default transform set.
   - Remove this transform set and replace it with a new one.
   - Add an additional transform, as explained in *Add a Phase 1 Transform* on page 538.

Add a Phase 1 Transform

You can define a tunnel to offer a peer more than one transform set for negotiation. For example, one transform set might include SHA1-DES-DF1 ([authentication method]-[encryption method]-[key group]) and a second transform might include MD5-3DES-DF2, with the SHA1-DES-DF1 transform as the higher priority transform set. When the tunnel is created, the XTM device can use either SHA1-DES-DF1 or MD5-3DES-DF2 to match the transform set of the other VPN endpoint.

You can include a maximum of nine transform sets. You must specify Main Mode in the Phase 1 settings to use multiple transforms.

1. On the **Gateway** page, select the **Phase 1 Settings** tab.
2. In the **Transform Settings** section, click **Add**.
   The Transform Settings dialog box appears.



2. From the **Authentication** drop-down list, select **SHA1** or **MD5** as the type of authentication.
3. From the **Encryption** drop-down list, select **AES (128-bit**), **AES (192-bit)**, **AES (256-bit)**, **DES**, or **3DES** as the type of encryption.
4. To change the SA (security association) life, type a number in the **SA Life** text box, and select **Hour** or **Minute** from the adjacent drop-down list.
5. From the **Key Group** drop-down list, select a Diffie-Hellman group. Fireware XTM supports groups 1, 2, and 5.
   Diffie-Hellman groups determine the strength of the master key used in the key exchange process. A higher the group number provides greater security, but more time is required to make the keys. For more information, see *About Diffie-Hellman Groups* on page 539.
6. Click **OK**.
   The Transform appears in the New Gateway page in the Transform Settings list. You can add up to nine transform sets.
7. Repeat Steps 2–6 to add more transforms. The transform set at the top of the list is used first.
8. To change the priority of a transform set, select the transform set and click **Up** or **Down**.
9. Click **OK**.

About Diffie-Hellman Groups

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key.

Fireware XTM supports Diffie-Hellman groups 1, 2, and 5:

- DH Group 1: 768-bit group
- DH Group 2: 1024-bit group
- DH Group 5: 1536-bit group

Both peers in a VPN exchange must use the same DH group, which is negotiated during Phase 1 of the IPSec negotiation process. When you define a manual BOVPN tunnel, you specify the Diffie-Hellman group as part of Phase 1 of creating an IPSec connection. This is where the two peers make a secure, authenticated channel they can use to communicate.

DH groups and Perfect Forward Secrecy (PFS)

In addition to Phase 1, you can also specify the Diffie-Hellman group in Phase 2 of an IPSec connection. Phase 2 configuration includes settings for a security association (SA), or how data packets are secured when they are passed between two endpoints. You specify the Diffie-Hellman group in Phase 2 only when you select Perfect Forward Secrecy (PFS).

PFS makes keys more secure because new keys are not made from previous keys. If a key is compromised, new session keys are still secure. When you specify PFS during Phase 2, a Diffie-Hellman exchange occurs each time a new SA is negotiated.

The DH group you choose for Phase 2 does not need to match the group you choose for Phase 1.

How to Choose a Diffie-Hellman Group

The default DH group for both Phase 1 and Phase 2 is Diffie-Hellman Group 1. This group provides basic security and good performance. If the speed for tunnel initialization and rekey is not a concern, use Group 2 or Group 5. Actual initialization and rekey speed depends on a number of factors. You might want to try DH Group 2 or 5 and decide whether the slower performance time is a problem for your network. If the performance is unacceptable, change to a lower DH group.

Performance Analysis

The following table shows the output of a software application that generates 2000 Diffie-Hellman values. These figures are for a 1.7GHz Intel Pentium 4 CPU.

DH Group	No. of key pairs	Time required	Time per key pair
Group 1	2000	43 sec	21 ms
Group 2	2000	84 sec	42 ms
Group 5	2000	246 sec	123 ms

Edit and Delete Gateways

To change the definition of a gateway

1. Select **VPN > BOVPN**.
2. Select a gateway and click **Edit**.
   The Gateway settings page appears.
3. Make your changes and click **Save**.

To delete a gateway, select the gateway and click **Remove**.

Disable Automatic Tunnel Startup

BOVPN tunnels are automatically created each time the XTM device starts. You can use Fireware XTM Web UI to change this default behavior. A common reason to change it would be if the remote endpoint uses a third-party device that must initiate the tunnel instead of the local endpoint.

To disable automatic startup for tunnels that use a gateway:

1. Select **VPN > Branch Office VPN**.
   The Branch Office VPN configuration page appears
2. Select a gateway and click **Edit**.
   The Gateway page appears.
3. Clear the **Start Phase1 tunnel when Firebox starts** check box at the bottom of the page.

If Your XTM Device is Behind a Device That Does NAT

The XTM device can use NAT Traversal. This means that you can make VPN tunnels if your ISP does NAT (Network Address Translation) or if the external interface of your XTM device is connected to a device that does NAT. We recommend that the XTM device external interface have a public IP address. If that is not possible, follow the subsequent instructions.

Devices that do NAT frequently have some basic firewall features. To make a VPN tunnel to your XTM device when the XTM device is installed behind a device that does NAT, the NAT device must let the traffic through. These ports and protocols must be open on the NAT device:

- UDP port 500 (IKE)
- UDP port 4500 (NAT Traversal)
- IP protocol 50 (ESP)

See the documentation for your NAT device for information on how to open these ports and protocols on the NAT device.

If the external interface of your XTM device has a private IP address, you cannot use an IP address as the local ID type in the Phase 1 settings.

- If the NAT device to which the XTM device is connected has a dynamic public IP address:
  - First, set the device to Bridge Mode. For more information, see *Bridge Mode* on page 96. In Bridge Mode, the XTM device gets the public IP address on its external interface. Refer to the documentation for your NAT device for more information.

- Set up Dynamic DNS on the XTM device. For information, see *About the Dynamic DNS Service* on page 89. In the Phase 1 settings of the Manual VPN, set the local ID type to **Domain Name**. Enter the DynDNS domain name as the Local ID. The remote device must identify your XTM device by domain name and it must use the DynDNS domain name associated with your XTM device in its Phase 1 configuration.

- If the NAT device to which the XTM device is connected has a static public IP address — In the Phase 1 settings of the Manual VPN, set the local ID type drop-down list to **Domain Name**. Enter the public IP address assigned to the external interface of the NAT device as the local ID. The remote device must identify your XTM device by domain name, and it must use the same public IP address as the domain name in its Phase 1 configuration.

Make Tunnels Between Gateway Endpoints

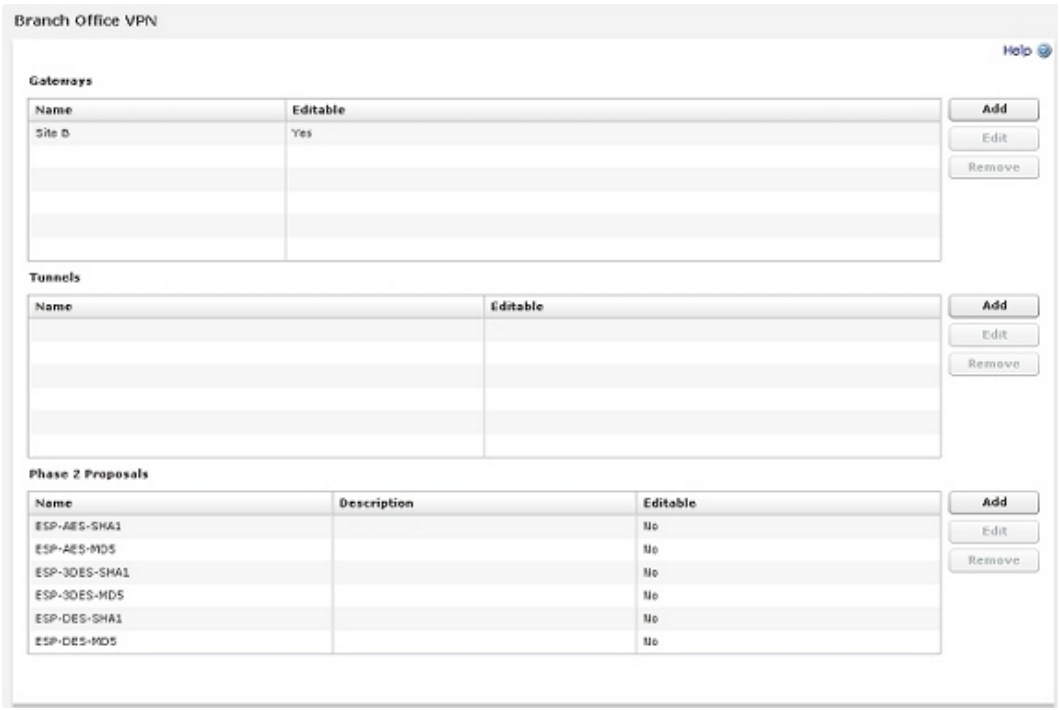
After you define gateway endpoints, you can make tunnels between them. To make a tunnel, you must:

- *Define a Tunnel*
- *Configure Phase 2 Settings* for the Internet Key Exchange (IKE) negotiation. This phase sets up security associations for the encryption of data packets.

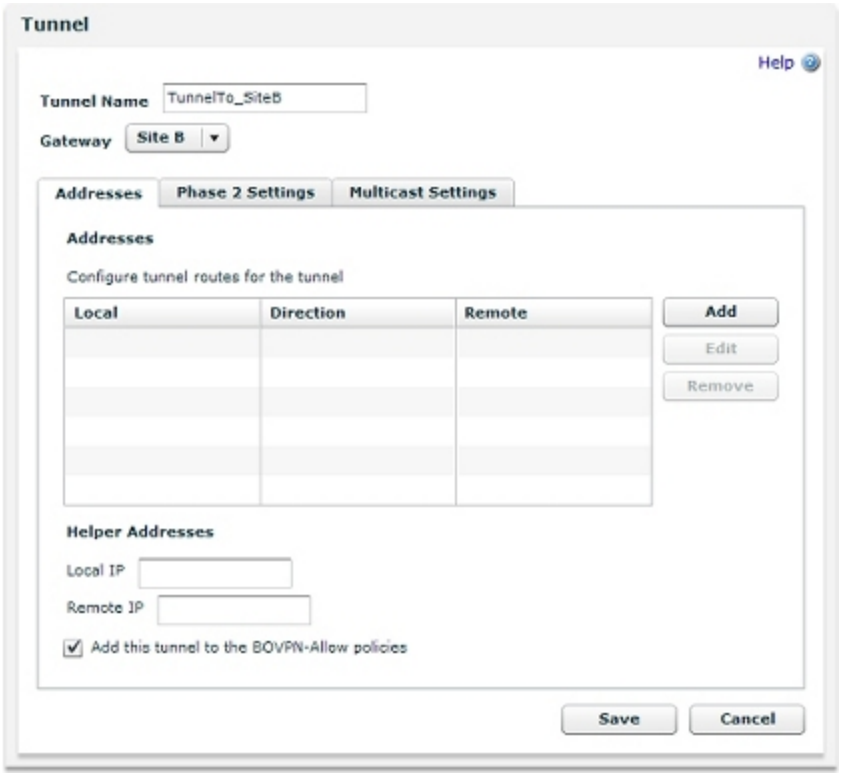
Define a Tunnel

From Fireware XTM Web UI, you can add, edit, and delete Branch Office VPN tunnels.

1. Select **VPN > Branch Office VPN**.
   The Branch Office VPN page appears.



2. In the **Tunnels** section, click **Add**.
   The New Tunnel dialog box appears.



3. In the **Tunnel Name** text box, type a name for the tunnel.
   Make sure the name is unique among tunnel names, Mobile VPN group names, and interface names.
4. From the **Gateway** drop-down list, select the gateway for this tunnel to use.
5. To add the tunnel to the BOVPN-Allow.in and BOVPN-Allow.out policies, select the **Add this tunnel to the BOVPN-Allow policies** check box. These policies allow all traffic that matches the routes for this tunnel.
   To restrict traffic through the tunnel, clear this check box and create custom policies for types of traffic that you want to allow through the tunnel.

You can now *Add Routes for a Tunnel*, *Configure Phase 2 Settings*, or *Enable Multicast Routing Through a Branch Office VPN Tunnel*.

Edit and Delete a Tunnel

You can use Fireware XTM Web UI to change or remove a tunnel.

To edit a tunnel:

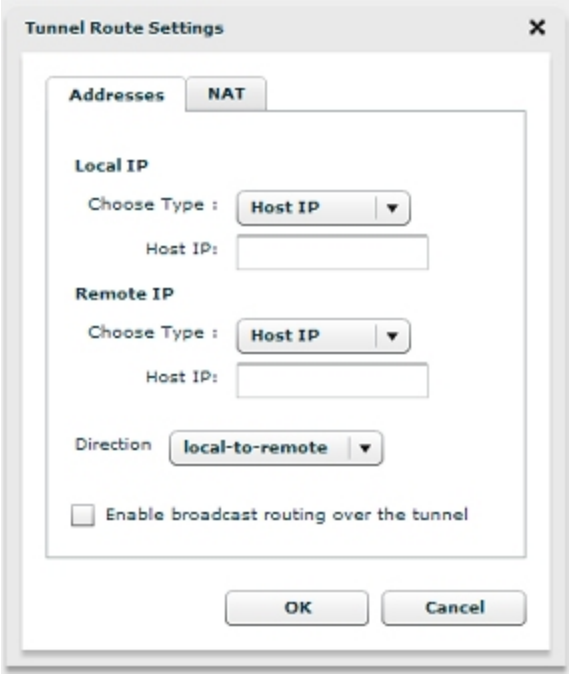
1. Select select **VPN > BOVPN**.
2. Select the tunnel and click **Edit**.
   The Tunnel page appears.
3. Make the changes and click **Save**.

To delete a tunnel:

1. From the **BOVPN** page, select the tunnel..
2. Click **Remove**.

Add Routes for a Tunnel

1. On the **Addresses** tab of the **Tunnel** dialog box, click **Add**.
   The Tunnel Route Settings dialog box appears.



2. In the **Local IP** section, select the type of local address from the **Choose Type** drop-down list. Then type the value in the adjacent text box. You can enter a host IP address, network address, a range of host IP addresses, or a DNS name.
3. In the **Remote IP** section, select the type of remote address from the **Choose Type** drop-down list. Then type the value in the adjacent text box. You can enter a host IP address, network address, a range of host IP addresses, or a DNS name.
4. In the **Direction** drop-down list, select the direction for the tunnel. The tunnel direction determines which endpoint of the VPN tunnel can start a VPN connection through the tunnel.

5. You can use the NAT tab to enable 1-to-1 NAT and dynamic NAT for the tunnel if the address types and tunnel direction you selected are compatible. For more information, see Set up outgoing dynamic NAT through a BOVPN tunnel and *Use 1-to-1 NAT Through a Branch Office VPN Tunnel* on page 552.
6. Click **OK**.

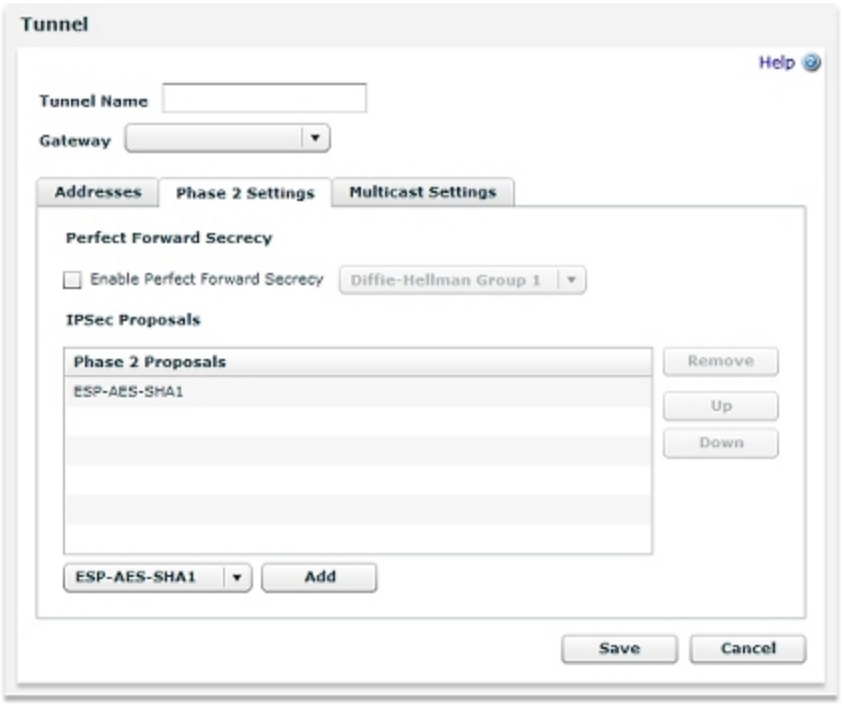
Configure Phase 2 Settings

Phase 2 settings include settings for a security association (SA), which defines how data packets are secured when they are passed between two endpoints. The SA keeps all information necessary for the XTM device to know what it should do with the traffic between the endpoints. Parameters in the SA can include:

- Encryption and authentication algorithms used.
- Lifetime of the SA (in seconds or number of bytes, or both).
- The IP address of the device for which the SA is established (the device that handles IPSec encryption and decryption on the other side of the VPN, not the computer behind it that sends or receives traffic).
- Source and destination IP addresses of traffic to which the SA applies.
- Direction of traffic to which the SA applies (there is one SA for each direction of traffic, incoming and outgoing).

To configure Phase 2 settings:

1. From the **Tunnel** page, select the **Phase2 Settings** tab.



2. Select the **PFS** check box if you want to enable Perfect Forward Secrecy (PFS). If you enable PFS, select the Diffie-Hellman group.

Perfect Forward Secrecy gives more protection to keys that are created in a session. Keys made with PFS are not made from a previous key. If a previous key is compromised after a session, your new session keys are secure. For more information, see *About Diffie-Hellman Groups* on page 539.

3. The XTM device contains one default proposal, which appears in the **IPSec Proposals** list. This proposal specifies the ESP data protection method, AES encryption, and SHA-1 authentication. You can either:
   - Click **Add** to add the default proposal.
   - Select a different proposal from the drop-down list and click **Add**.
   - Add an additional proposal, as explained in *Add a Phase 2 Proposal* on page 546.

If you plan to use the IPSec pass-through feature, you must use a proposal with ESP (Encapsulating Security Payload) as the proposal method. IPSec pass-through supports ESP but not AH. For more information on IPSec pass-through, see *About Global VPN Settings* on page 549.

Add a Phase 2 Proposal

You can define a tunnel to offer a peer more than one proposal for Phase 2 of the IKE. For example, you might specify ESP-3DES-SHA1 in one proposal, and ESP-DES-MD5 for second proposal. When traffic passes through the tunnel, the security association can use either ESP-3DES-SHA1 or ESP-DES-MD5 to match the transform settings on the peer.

You can include a maximum of nine proposals.

Add an Existing Proposal

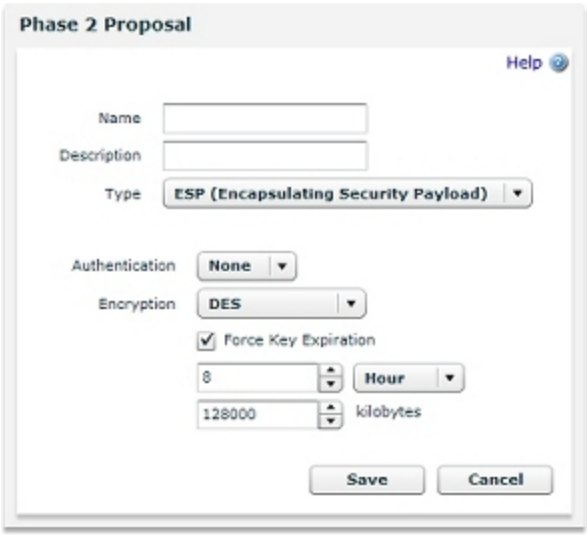
There are six pre-configured proposals that you can choose. The names follow the format <Type>-<Authentication>-<Encryption>. For all six, Force Key Expiration is enabled for 8 hours or 128000 kilobytes.

To use one of the six pre-configured proposals:

1. From the **Tunnels** page in the **IPSec Proposals** section, select the proposal you want to add.
2. Click **Add**.

Create a New Proposal

1. From Fireware XTM Web UI, select **VPN > Branch Office VPN**. In the **Phase 2 Proposals** section, click **Add**.
   The Phase 2 Proposal page appears.



2. In the **Name** text box, type a name for the new proposal.

   In the **Description** text box, type a description to identify this proposal (optional).
3. From the **Type** drop-down list, select **ESP** or **AH** as the proposal method. We recommend that you use ESP (Encapsulating Security Payload). The differences between ESP and AH (Authentication Header) are:

   - ESP is authentication with encryption.
   - AH is authentication only. ESP authentication does not include the protection of the IP header, while AH does.
   - IPSec pass-through supports ESP but not AH. If you plan to use the IPSec pass-though feature, you must specify ESP as the proposal method. For more information on IPSec pass-through, see *About Global VPN Settings* on page 549.
4. From the **Authentication** drop-down list, select **SHA1**, **MD5**, or **None** for the authentication method.
5. If you selected **ESP** from the **Type** drop-down list, from the **Encryption** drop-down list, select the encryption method.
   The options are DES, 3DES, and AES 128, 192, or 256 bit, which appear in the list from the most simple and least secure to most complex and most secure.
6. To make the gateway endpoints generate and exchange new keys after a quantity of time or amount of traffic passes, select the **Force Key Expiration** check box. In the fields below, enter a quantity of time and a number of bytes after which the key expires.
   If Force Key Expiration is disabled, or if it is enabled and both the time and kilobytes are set to zero, the XTM device tries to use the key expiration time set for the peer. If this is also disabled or zero, the XTM device uses a default key expiration time of 8 hours.
   The maximum time before a forced key expiration is one year.
7. Click **Save**.

Edit a Proposal

You can edit only user-defined proposals.

1. Select **VPN > BOVPN**
2. In the **Phase 2 Proposals** section, select a proposal and click **Edit**.
3. Make changes to the fields as described in the **Create a new proposal** section of this topic.

Change Order of Tunnels

The order of VPN tunnels is particularly important when more than one tunnel uses the same routes or when the routes overlap. A tunnel higher in the list of tunnels on the **Branch Office IPSec Tunnels** dialog box takes precedence over a tunnel below it when traffic matches tunnel routes of multiple tunnels.

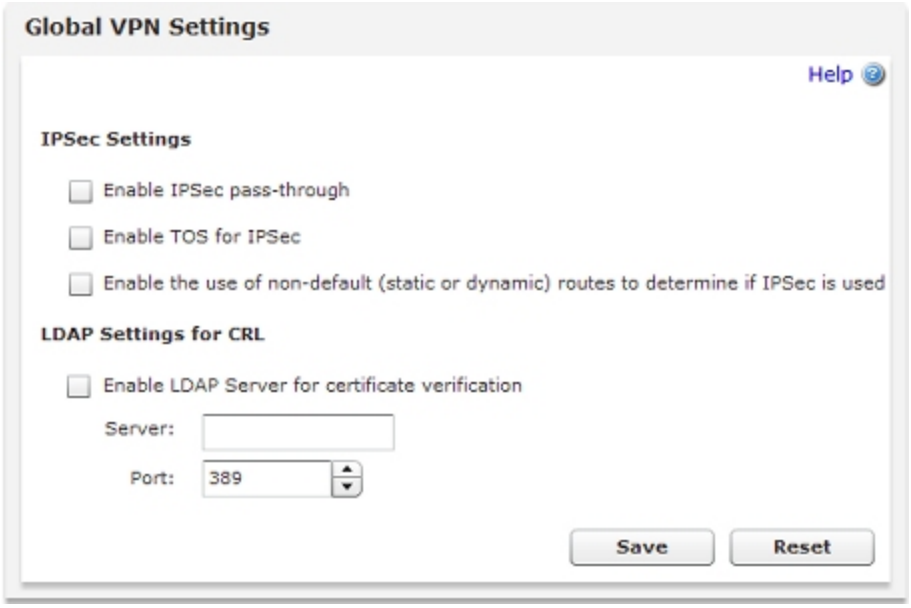
From Fireware XTM Web UI, you can change the order in which the XTM device attempts connections. You can only change the order of tunnels for manual VPN tunnels.

1. Select **VPN > Branch Office VPN**.
   The Branch Office VPN page appears.
2. Select a tunnel and click **Move Up** or **Move Down** to move it up or down in the list.

About Global VPN Settings

From Fireware XTM Web UI, you can select settings that apply to manual BOVPN tunnels, managed BOVPN tunnels, and Mobile VPN with IPSec tunnels.

1. Select **VPN > Global Settings**.
   The Global VPN Settings page appears.



2. Configure the settings for your VPN tunnels, as explained in the subsequent sections.

Enable IPSec Pass-Through

For a user to make IPSec connections to an XTM device located behind a different XTM device, you must make sure the **Enable IPSec Pass-through** check box is selected. For example, if mobile employees are at a customer location that has a XTM device, they can use IPSec to make IPSec connections to their network. For the local XTM device to correctly allow the outgoing IPSec connection, you must also add an IPSec policy to the configuration.

When you enable IPSec pass-through, a policy called *WatchGuard IPSec* is automatically added to the configuration. The policy allows traffic from any trusted or optional network to any destination. When you disable IPSec pass-through, the *WatchGuard IPSec* policy is automatically deleted.

Enable TOS for IPSec

Type of Service (TOS) is a set of four-bit flags in the IP header that can tell routing devices to give an IP datagram more or less priority than other datagrams. Fireware XTM gives you the option to allow IPSec tunnels to clear or maintain the settings on packets that have TOS flags. Some ISPs drop all packets that have TOS flags.

If you do not select the **Enable TOS for IPSec** check box, all IPSec packets do not have the TOS flags. If the TOS flags were set before, they are removed when Fireware XTM encapsulates the packet in an IPSec header.

When the **Enable TOS for IPSec** check box is selected and the original packet has TOS flags, Fireware XTM keeps the TOS flags set when it encapsulates the packet in an IPSec header. If the original packet does not have the TOS flags set, Fireware XTM does not set the TOS flag when it encapsulates the packet in an IPSec header.

Make sure to carefully consider whether to select this check box if you want to apply QoS marking to IPSec traffic. QoS marking can change the setting of the TOS flag. For more information on QoS marking, see *About QoS Marking* on page 431.

Enable the Use of Non-Default (Static or Dynamic) Routes to Determine if IPSec is Used

When this option is not enabled, all packets that match the tunnel route specified in the IPSec gateway are sent through the IPSec VPN. If this option is enabled, the XTM device uses the routing table to determine whether to send the packet through the IPSec VPN tunnel.

If a default route is used to route a packet

The packet is encrypted and sent through the VPN tunnel, to the interface specified in the VPN gateway configuration.

If a non-default route is used to route a packet

The packet is routed to the interface specified in the non-default route in the routing table. When a non-default route is used, the decision about whether to send the packet through the IPSec VPN tunnel depends on the interface specified in the routing table. If the interface in the non-default route matches the interface in the BOVPN gateway, the packet goes through the BOVPN tunnel configured for that interface. For example, if the BOVPN gateway interface is set to Eth0, and the matched non-default route uses Eth1 as the interface, the packet is not sent through the BOVPN tunnel. However, if the matched non-default route uses Eth0 as the interface, the packet is sent through the BOVPN tunnel.

This feature works with any non-default route (static or dynamic).You can use this feature in conjunction with dynamic routing to enable dynamic network failover from a private network route to an encrypted IPSec VPN tunnel.

For example, consider an organization that sends traffic between two networks, Site A and Site B. They use a dynamic routing protocol to send traffic between the two sites over a private network connection, with no VPN required. The private network is connected to the Eth1 interface of each device. They have also configured a BOVPN tunnel between the two sites to send BOVPN traffic over the local Internet connection, over the Eth0 interface of each device. They want to send traffic over the BOVPN tunnel only if the private network connection is not available.

If they select the **Enable the use of non-default (static or dynamic) routes to determine if IPSec is used** check box in the Global VPN Settings, the XTM device sends traffic over the private network if a dynamic route to that network is present over the Eth1 interface. Otherwise, it sends traffic over the encrypted IPSec BOVPN tunnel on the Eth0 interface.

Enable LDAP Server for Certificate Verification

When you create a VPN gateway, you specify a credential method for the two VPN endpoints to use when the tunnel is created. If you choose to use an IPSec XTM device certificate, you can identify an LDAP server that validates the certificate. Type the IP address for the LDAP server. You can also specify a port if you want to use a port other than 389.

This setting does not apply to Mobile VPN with IPSec tunnels.

Use 1-to-1 NAT Through a Branch Office VPN Tunnel

When you create a Branch Office VPN (BOVPN) tunnel between two networks that use the same private IP address range, an IP address conflict occurs. To create a tunnel without this conflict, both networks must apply 1-to-1 NAT to the VPN. 1-to-1 NAT makes the IP addresses on your computers appear to be different from their true IP addresses when traffic goes through the VPN.

1-to-1 NAT maps one or more IP addresses in one range to a second IP address range of the same size. Each IP address in the first range maps to an IP address in the second range. In this document, we call the first range the real IP addresses and we call the second range the masqueraded IP addresses. For more information on 1-to-1 NAT, see *About 1-to-1 NAT* on page 149.

1-to-1 NAT and VPNs

When you use 1-to-1 NAT through a BOVPN tunnel:

- When a computer in your network sends traffic to a computer at the remote network, the XTM device changes the source IP address of the traffic to an IP address in the masqueraded IP address range. The remote network sees the masqueraded IP addresses as the source of the traffic.
- When a computer at the remote network sends traffic to a computer at your network through the VPN, the remote office sends the traffic to the masqueraded IP address range. The XTM device changes the destination IP address to the correct address in the real IP address range and then sends the traffic to the correct destination.

1-to-1 NAT through a VPN affects only the traffic that goes through that VPN. The rules you see in Fireware XTM Web UI at **Network > NAT** do not affect traffic that goes through a VPN.

Other Reasons to Use 1-to-1 NAT Through a VPN

In addition to the previous situation, you would also use 1-to-1 NAT through a VPN if the network to which you want to make a VPN already has a VPN to a network that uses the same private IP addresses you use in your network. An IPSec device cannot route traffic to two different remote networks when the two networks use the same private IP addresses. You use 1-to-1 NAT through the VPN so that the computers in your network appear to have different (masqueraded) IP addresses. However, unlike the situation described at the beginning of this topic, you need to use NAT only on your side of the VPN instead of both sides.

A similar situation exists when two remote offices use the same private IP addresses and both remote offices want to make a VPN to your XTM device. In this case, one of the remote offices must use NAT through its VPN to your XTM device to resolve the IP address conflict.

Alternative to Using NAT

If your office uses a common private IP address range such as 192.168.0.x or 192.168.1.x, it is very likely that you will have a problem with IP address conflicts in the future. These IP address ranges are often used by broadband routers or other electronic devices in homes and small offices. You should consider changing to a less common private IP address range, such as 10.x.x.x or 172.16.x.x.

How to Set Up the VPN

1. Select a range of IP addresses that your computers show as the source IP addresses when traffic comes from your network and goes to the remote network through the BOVPN. Consult with the network administrator for the other network to select a range of IP addresses that are not in use. Do not use any of the IP addresses from:

   - The trusted, optional, or external network connected to your XTM device
   - A secondary network connected to a trusted, optional, or external interface of your XTM device
   - A routed network configured in your XTM device policy (**Network > Routes**)
   - Networks to which you already have a BOVPN tunnel
   - Mobile VPN virtual IP address pools
   - Networks that the remote IPSec device can reach through its interfaces, network routes, or VPN routes

2. *Configure Gateways* for the local and remote XTM devices.
3. *Make Tunnels Between Gateway Endpoints*. In the **Tunnel Route Settings** dialog box for each XTM device, select the **1:1 NAT** check box and type its masqueraded IP address range in the adjacent text box.

   The number of IP addresses in this text box must be exactly the same as the number of IP addresses in the **Local** text box at the top of the dialog box. For example, if you use slash notation to indicate a subnet, the value after the slash must be the same in both text boxes. For more information, see *About Slash Notation* on page 3.

You do not need to define anything in the **Network > NAT** settings in Fireware XTM Web UI. These settings do not affect VPN traffic.

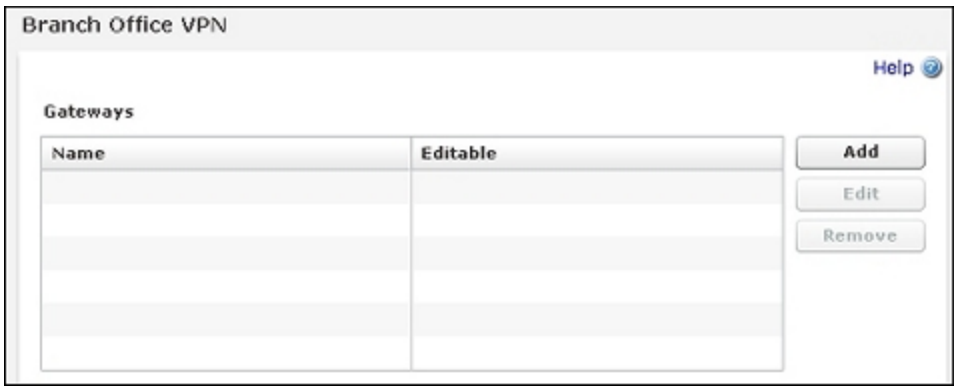
Example

Suppose two companies, Site A and Site B, want to make a Branch Office VPN between their trusted networks. Both companies use a WatchGuard XTM device with Fireware XTM. Both companies use the same IP addresses for their trusted networks, 192.168.1.0/24. Each company's XTM device uses 1-to-1 NAT through the VPN. Site A sends traffic to Site B's masqueraded range and the traffic goes outside Site A's local subnet. Also, Site B sends traffic to the masqueraded range that Site A uses. This solution solves the IP address conflict at both networks. The two companies agree that:

- Site A makes its trusted network appear to come from the 192.168.100.0/24 range when traffic goes through the VPN. This is Site B's masqueraded IP address range for this VPN.
- Site B makes its trusted network appear to come from the 192.168.200.0/24 range when traffic goes through the VPN. This is Site B's masqueraded IP address range for this VPN.

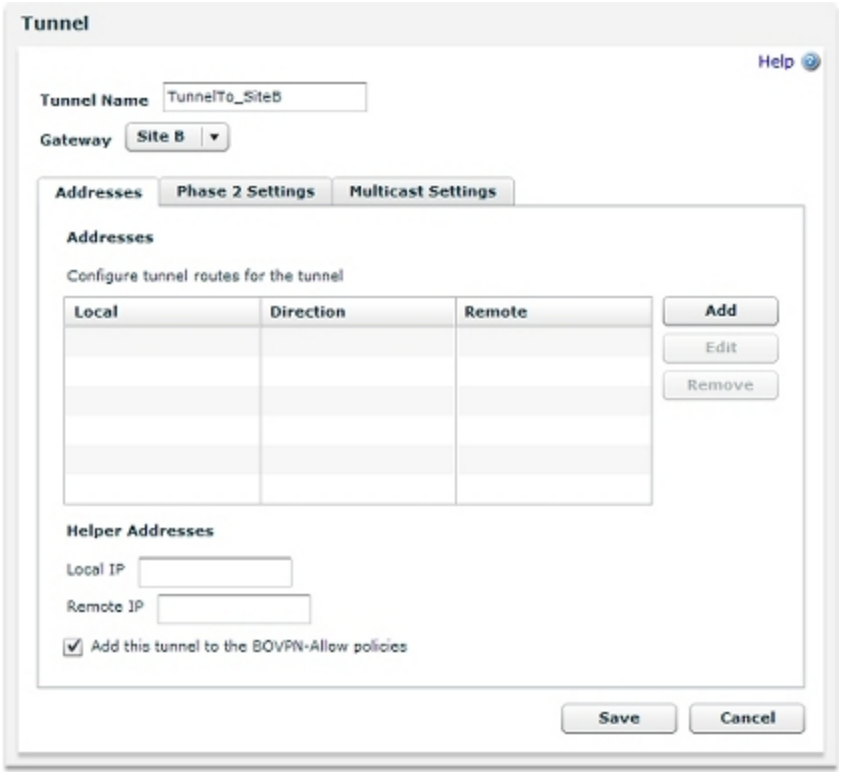
Define a Branch Office Gateway on Each XTM Device

The first step is to make a gateway that identifies the remote IPSec device. When you make the gateway, it appears in the list of gateways in Fireware XTM Web UI. To see the list of gateways from Fireware XTM Web UI, select **VPN > Branch Office VPN**.

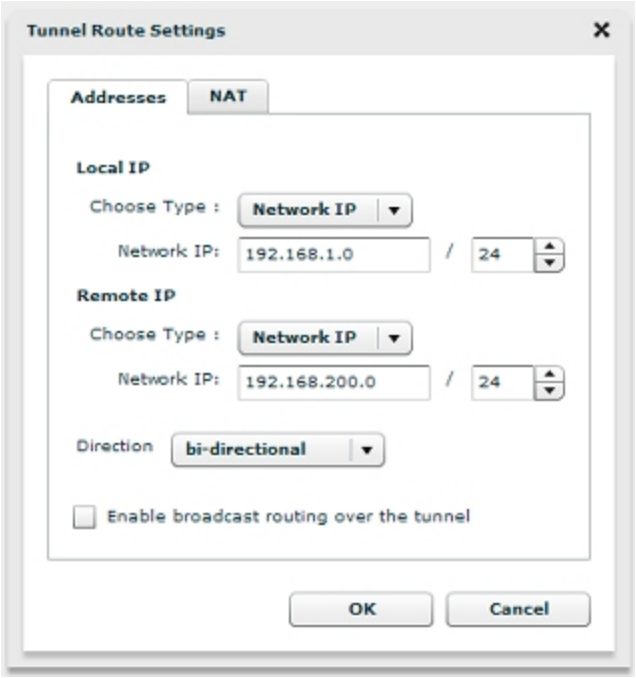


Configure the Local Tunnel

1. Select **VPN > Branch Office VPN**.
   The Branch Office VPN page appears.
2. In the **Tunnel** section of the **BOVPN** page, click **Add**.
   The Tunnel settings page appears.

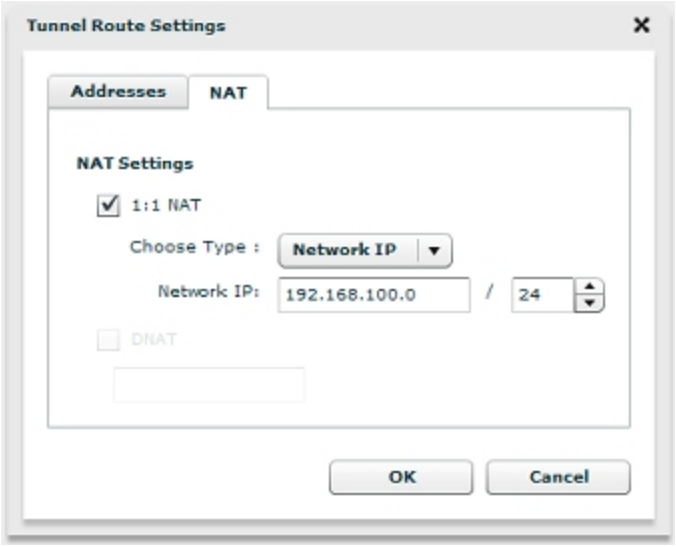


3. Type a descriptive name for the tunnel. The example uses "TunnelTo_SiteB".
4. From the **Gateway** drop-down list, select the gateway that points to the IPSec device of the remote office. The example uses the gateway called "SiteB".
5. Select the **Phase 2 Settings** tab. Make sure the Phase 2 settings match what the remote office uses for Phase 2.
6. Select the **Addresses** tab. Click **Add** to add the local-remote pair.
   The Tunnel Route Settings dialog box appears.



7. In the **Local IP** section, select **Network IP** from the **Choose Type** drop-down list. In the **Network IP** text box, type the real IP address range of the local computers that use this VPN. This example uses 192.168.1.0/24.
8. In the **Remote** section, select **Network IP** from the **Choose Type** drop-down list. In the **Network IP** text box type the private IP address range that the local computers send traffic to.

   In this example, the remote office Site B uses 1-to-1 NAT through its VPN. This makes Site B's computers appear to come from Site B's masqueraded range, 192.168.200.0/24. The local computers at Site A send traffic to Site B's masqueraded IP address range. If the remote network does not use NAT through its VPN, type the real IP address range in the **Remote** text box.
9. Select the **NAT** tab. Select the **1:1 NAT** check box and type the masqueraded IP address range for this office. This is the range of IP addresses that the computers protected by this XTM device show as the source IP address when traffic comes from this XTM device and goes to the other side of the VPN. (The **1:1 NAT** check box is enabled after you type a valid host IP address, a valid network IP address, or a valid host IP address range in the **Local** text box on the **Addresses** tab.) Site A uses 192.168.100.0/24 for its masqueraded IP address range.

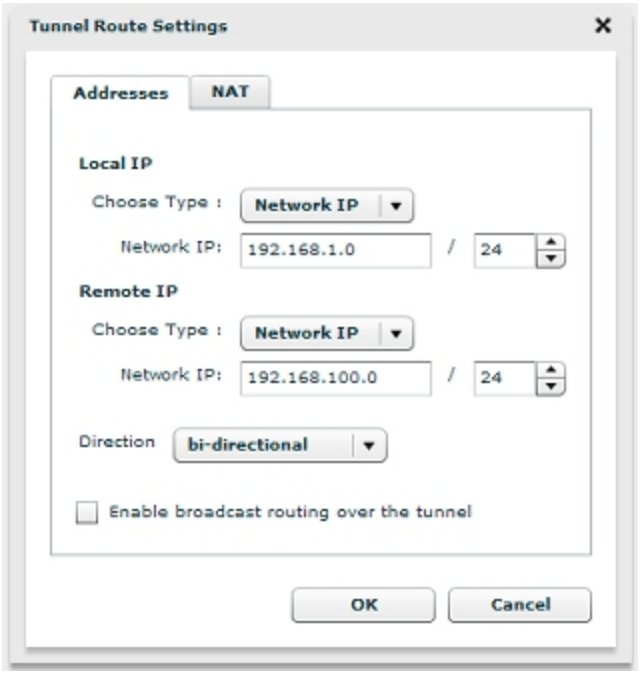


10. Click **OK**. The device adds the new tunnel to the BOVPN-Allow.out and BOVPN-Allow.in policies.
11. Save the configuration file.

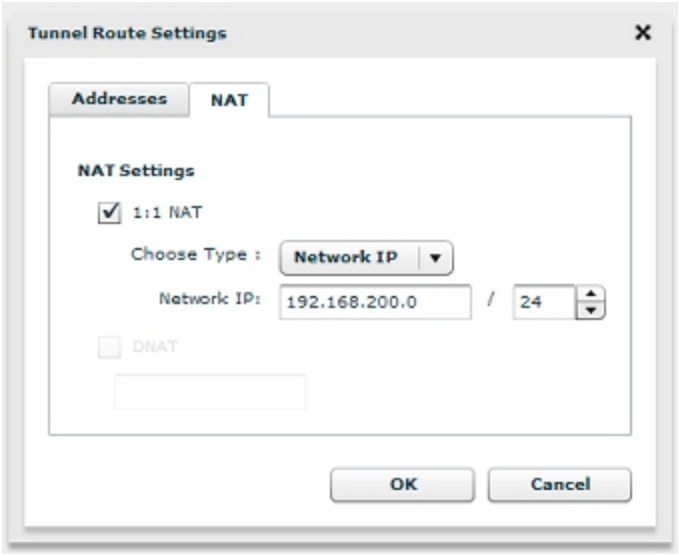
If you need 1-to-1 NAT on your side of the VPN only, you can stop here. The device at the other end of the VPN must configure its VPN to accept traffic from your masqueraded range.

Configure the Remote Tunnel

1. Follow Steps 1–6 in the previous procedure to add the tunnel on the remote XTM device. Make sure the Phase 2 settings match.
2. In the **Local IP** section, select **Network IP** from the **Choose Type** drop-down list. In the **Network IP** text box, type the real IP address range of the local computers that use this VPN. This example uses 192.168.1.0/24.
3. In the **Local IP** section, select **Network IP** from the **Choose Type** drop-down list. In the Network IP text box, type the private IP address range that the computers at the remote office send traffic to. In our example, Site A does 1-to-1 NAT through its VPN. This makes the computers at Site A appear to come from its masqueraded range, 192.168.100.0/24. The local computers at Site B send traffic to the masqueraded IP address range of Site A.



4. Select **the NAT** tab. Select the **1:1 NAT** check box and type the masqueraded IP address range of this site. This is the range of IP addresses that computers behind this XTM device show as the source IP address when traffic comes from this XTM device and goes to the other side of the VPN. Site B uses 192.168.200.0/24 for its masqueraded IP address range.



5. Click **OK**. The device adds the new tunnel to the BOVPN-Allow.out and BOVPN-Allow.in policies.

Define a Route for All Internet-Bound Traffic

When you enable remote users to access the Internet through a VPN tunnel, the most secure setup is to require that all remote user Internet traffic is routed through the VPN tunnel to the XTM device. From the XTM device, the traffic is then sent back out to the Internet. With this configuration (known as a hub route or default-route VPN), the XTM device is able to examine all traffic and provide increased security, although more processing power and bandwidth on the XTM device is used. When you use default-route VPN, a dynamic NAT policy must include the outgoing traffic from the remote network. This allows remote users to browse the Internet when they send all traffic to the XTM device.

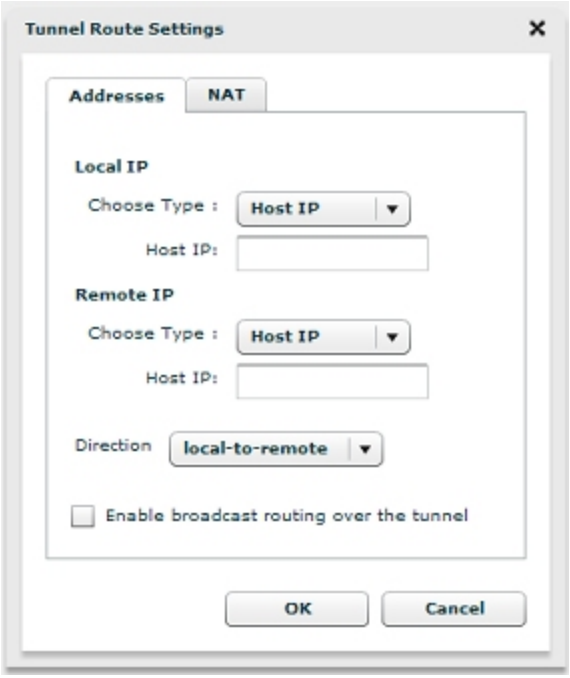
When you define a default route through a BOVPN tunnel, you must do three things:

- Configure a BOVPN on the remote XTM device (whose traffic you want to send through the tunnel) to send all traffic from its own network address to 0.0.0.0/0.
- Configure a BOVPN on the central XTM device to allow traffic to pass through it to the remote XTM device.
- Add a route on the central XTM device from 0.0.0.0/0 to the network address of the remote XTM device.

Before you begin the procedures in this topic, you must have already created a manual branch office VPN between the central and remote XTM devices. For information on how to do this, see *About Manual Branch Office VPN Tunnels* on page 528.

Configure the BOVPN Tunnel on the Remote XTM Device

1. Log into the Web UI for the remote XTM device.
2. Select **VPN > Branch Office VPN**. Find the name of the tunnel to the central XTM device and click **Edit**.
   The Tunnel page appears.
3. Click **Add**.
   The Tunnel Route Settings dialog box appears.



4. Under **Local IP**, in the **Host IP** text box, type the trusted network address of the remote XTM device.
5. Under **Remote IP**, select **Network IP** from the **Choose Type** drop-down list. In the **Host IP** text box, type 0.0.0.0/0 and click **OK**.
6. Select any other tunnel to the central XTM device and click **Remove**.
7. Click **Save** to save the configuration change.

Configure the BOVPN Tunnel on the Central XTM Device

1. Log into the Web UI for the central XTM device.
2. Select **VPN > Branch Office VPN**. Find the name of the tunnel to the remote XTM device and click **Edit**.
   The Tunnel page appears.
3. Click **Add**.
   The Tunnel Route Settings dialog box appears.
4. Under **Local IP**, select **Network IP** from the **Choose Type** drop-down list. In the **Host IP** text box, type 0.0.0.0/0.
5. Under **Remote IP**, type the trusted network address of the remote XTM device and click **OK**.
6. Select any other tunnel to the remote XTM device and click **Remove**.
7. Click **Save** to save the configuration change.

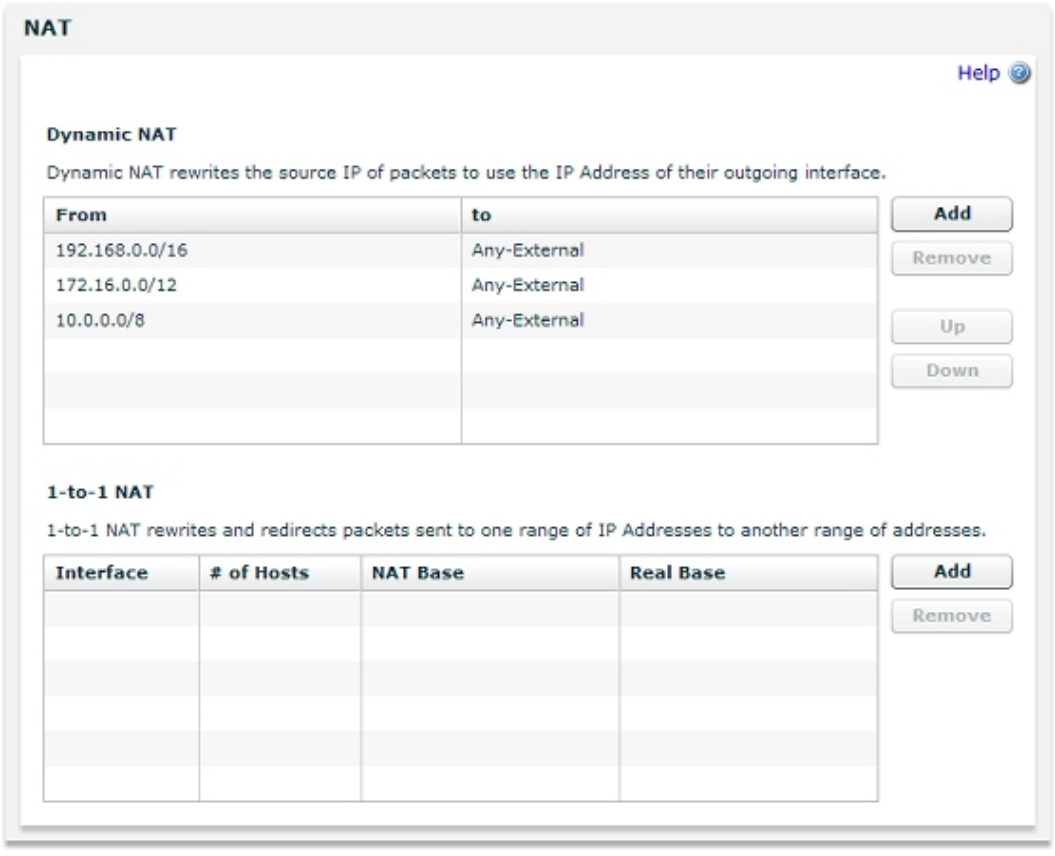
Add a Dynamic NAT Entry on the Central XTM Device

To allow a computer with a private IP address to access the Internet through the XTM device, you must configure the central XTM device to use dynamic NAT. With dynamic NAT, the XTM device replaces the private IP address included in a packet sent from a computer protected by the XTM device with the public IP address of the XTM device itself. By default, dynamic NAT is enabled and active for the three RFC-approved private network addresses:

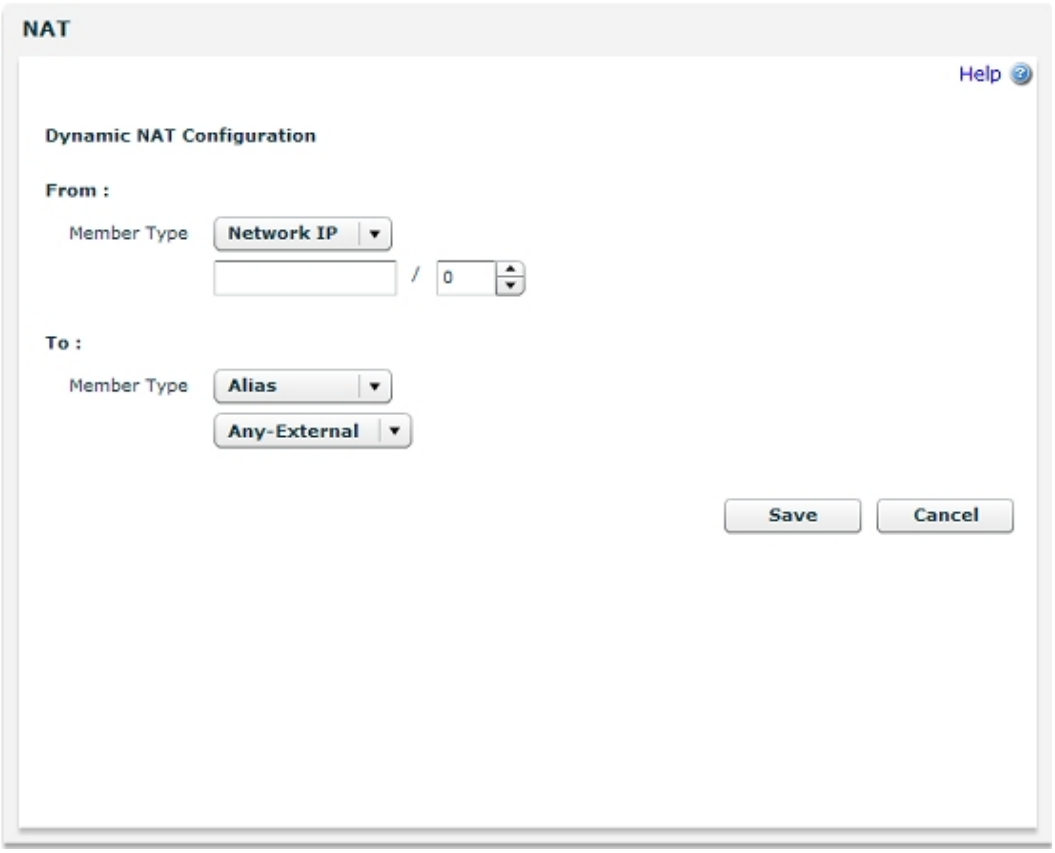
192.168.0.0/16 - Any-External
172.16.0.0/12 - Any-External
10.0.0.0/8 - Any-External

When you set up a default route through a branch office VPN tunnel to another XTM device, you must add a dynamic NAT entry for the subnet behind the remote XTM device if its IP addresses are not within one of the three private network ranges.

1. Select **Network > NAT**.
   The NAT page appears.



2. In the **Dynamic NAT** section of the **NAT** page, click **Add**.
   The Dynamic NAT configuration page appears.



3. In the **From** section, select **Network IP** from the **Member Type** drop-down list.
4. Type the network IP address of the network behind the remote XTM device.
5. In the **To** section, select **Any-External** from the second drop-down list.
6. Click **Save**.

Enable Multicast Routing Through a Branch Office VPN Tunnel

You can enable multicast routing through a Branch Office VPN (BOVPN) tunnel to support one-way multicast streams between networks protected by XTM devices. For example, you can use multicast routing through a BOVPN tunnel to stream media from a video on demand (VOD) server to users on the network at the other end of a branch office VPN tunnel.

> ***Note*** *Multicast routing through a BOVPN tunnel is supported only between XTM devices.*

When you enable multicast routing through a BOVPN tunnel, the tunnel sends multicast traffic from a single IP address on one side of the tunnel to an IP Multicast Group address. You configure the multicast settings in the tunnel to send multicast traffic to this IP Multicast Group address through the tunnel.

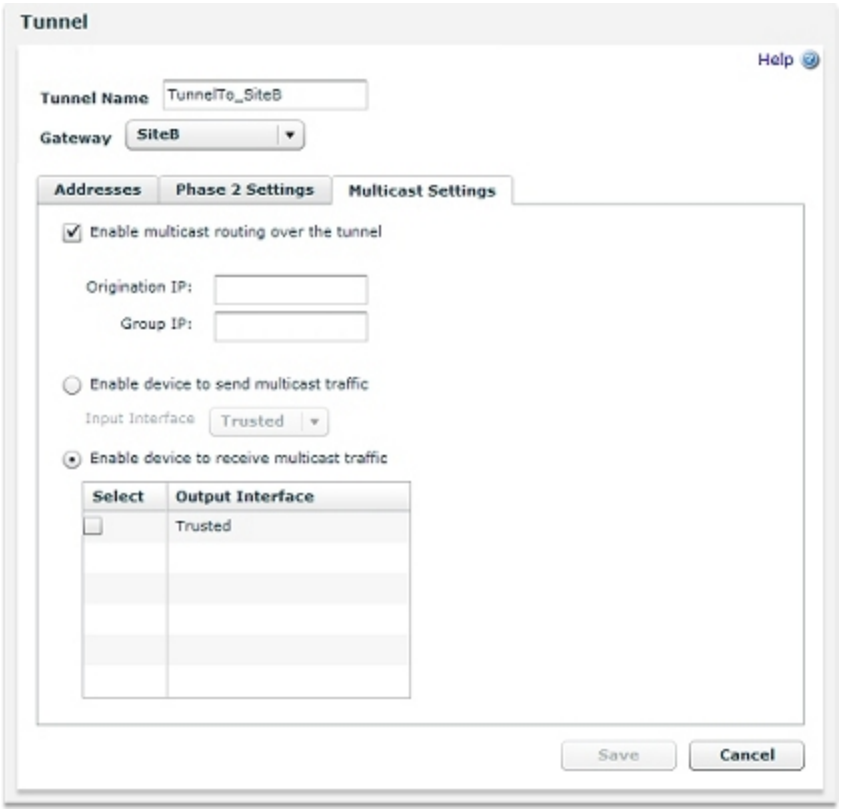
You must configure the multicast settings on each XTM device differently. You must configure the tunnel on one XTM device to send multicast traffic through the tunnel, and configure the tunnel settings on the other XTM device to receive multicast traffic. You can configure only one origination IP address per tunnel.

When you enable multicast routing through a BOVPN tunnel, the XTM device creates a GRE tunnel inside the IPSec VPN tunnel between the networks. The XTM device sends the multicast traffic through the GRE tunnel. The GRE tunnel requires an unused IP address on each side of the tunnel. You must configure helper IP addresses for each end of the BOVPN tunnel.

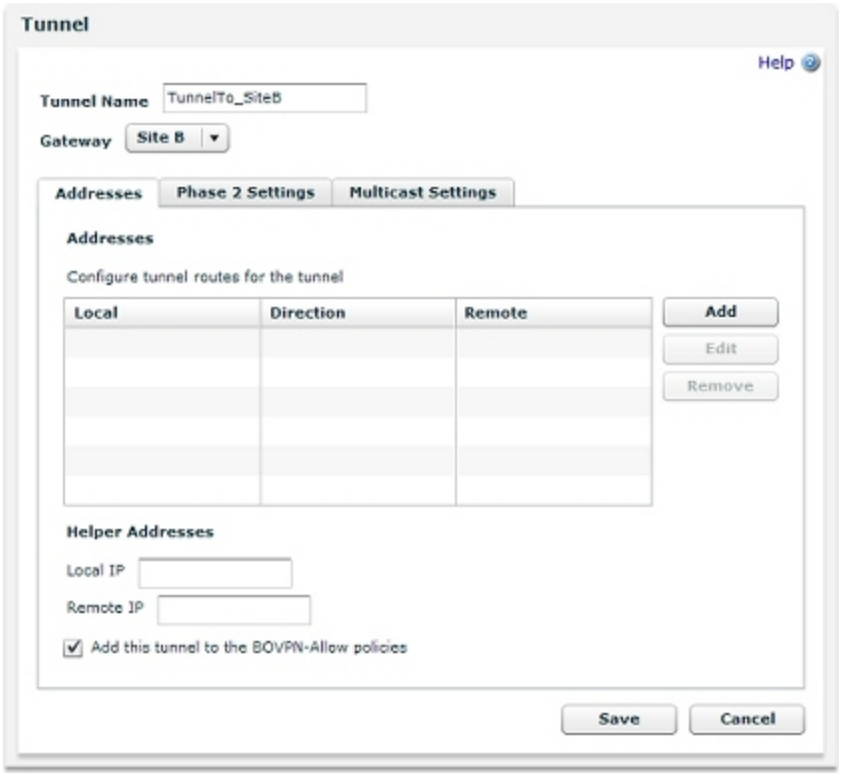
Enable an XTM Device to Send Multicast Traffic Through a Tunnel

On the XTM device from which the multicast traffic is sent, edit the tunnel configuration to enable the device to send multicast traffic through the BOVPN tunnel.

1. Select **VPN > Branch Office VPN**.
2. Select a tunnel and click **Edit**.
3. From the **Tunnel** page, click the **Multicast Settings** tab.



4. Select the **Enable multicast routing over the tunnel** check box.
5. In the **Origination IP** text box, type the IP address of the originator of the traffic.
6. In the **Group IP** text box, type the multicast IP address to receive the traffic.
7. Select **Enable device to send multicast traffic**.
8. From the **Input Interface** drop-down list, select the interface from which the multicast traffic originates.
9. Click the **Addresses** tab.
   The Broadcast/Multicast Tunnel Endpoints settings appear at the bottom of the Addresses tab.



10. In the **Helper Addresses** section, type IP addresses for each end of the multicast tunnel. The XTM device uses these addresses as the endpoints of the broadcast/multicast GRE tunnel inside the IPSec BOVPN tunnel. You can set Local IP and Remote IP to any unused IP address. We recommend that you use IP addresses that are not used on any network known to the XTM device.
    - In the **Local IP** text box, type an IP address to use for the local end of the tunnel.
    - In the **Remote IP** text box, type an IP address to use for the remote end of the tunnel.

Enable the Other XTM Device to Receive Multicast Traffic Through a Tunnel

On the XTM device on the network on which you want to receive the multicast traffic, configure the multicast settings to enable the device to receive multicast traffic through the tunnel.

1. Select **VPN > Branch Office VPN**.
2. Select a tunnel and click **Edit**.
3. From the **Tunnel** page, click the **Multicast Settings** tab.
4. Select the **Enable multicast routing over the tunnel** check box.
5. In the **Origination IP** text box, type the IP address of the originator of the traffic.
6. In the **Group IP** text box, type the multicast address to receive the traffic.
7. Select **Enable device to receive multicast traffic**.
8. Select the check box for each interfaces that you want to receive the multicast traffic.
9. Select the **Addresses** tab.
   The Broadcast/Multicast Tunnel Endpoints settings appear at the bottom of the Addresses tab.
10. In the **Helper Addresses** section, type the opposite IP addresses you typed in the configuration for the other end of the tunnel.
    - In the **Local IP** text box, type the IP address that you typed in the Remote IP field for the XTM device at the other end of the tunnel.
    - In the **Remote IP** text box, type the IP address that you typed in the Local IP field for the XTM device at the other end of the tunnel.

Enable Broadcast Routing Through a Branch Office VPN Tunnel

You can configure your XTM device to support limited broadcast routing through a Branch Office VPN (BOVPN) tunnel. When you enable broadcast routing, the tunnel supports broadcasts to the limited broadcast IP address, 255.255.255.255. Local subnet broadcast traffic is not routed through the tunnel. Broadcast routing supports broadcast only from one network to another through a BOVPN tunnel.

> ***Note*** *Broadcast routing through a BOVPN tunnel is supported only between XTM devices.*

Broadcast routing through a BOVPN tunnel does not support these broadcast types:

- DHCP/ Bootstrap Protocol (bootp) broadcast
- NetBIOS broadcast
- Server Message Block (SMB) broadcast

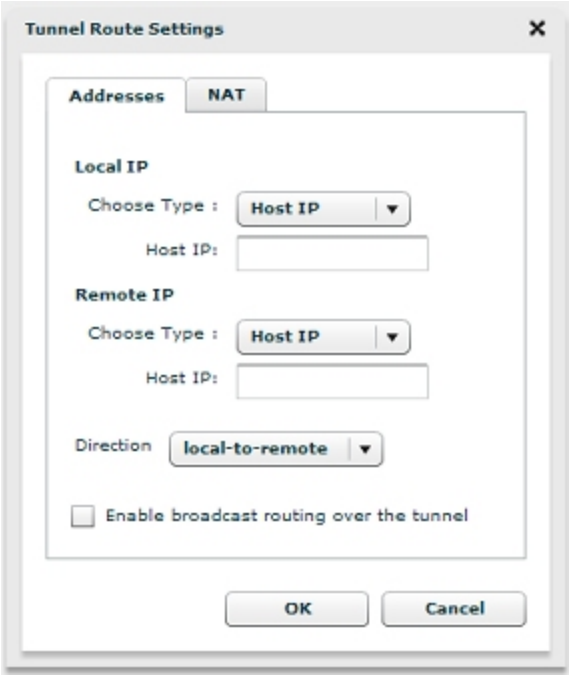
For an example that shows which broadcasts can be routed through a BOVPN tunnel, see Broadcast Routing Through a BOVPN Tunnel.

Some software applications require the ability to broadcast to other network devices in order to operate. If devices that need to communicate this way are on networks connected by a BOVPN tunnel, you can enable broadcast routing through the tunnel so the application can find the devices on the network at the other end of the tunnel.

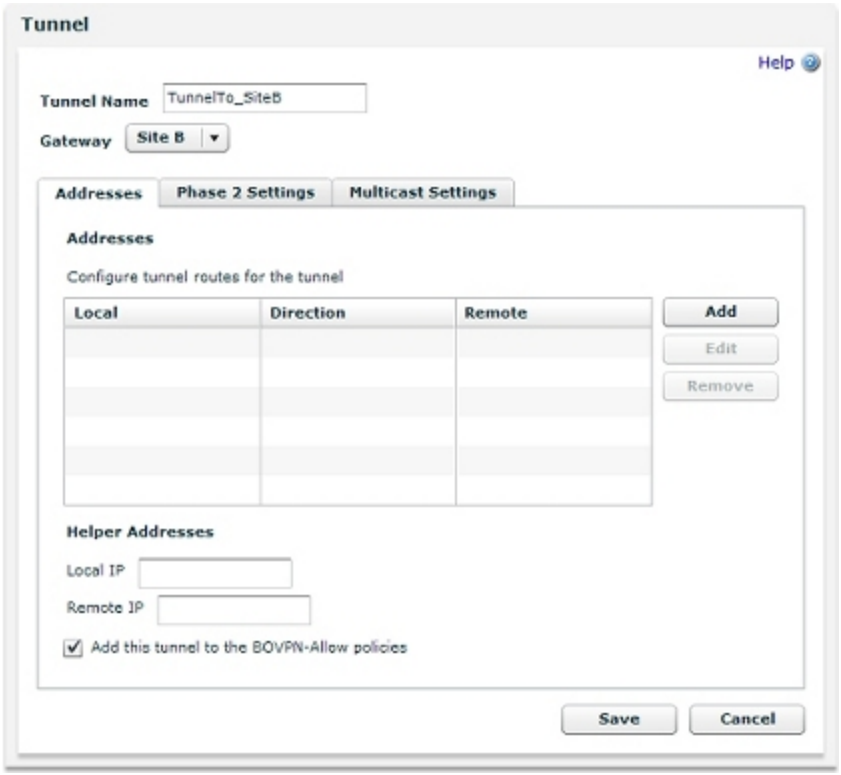
When you enable broadcast routing through a BOVPN tunnel, the XTM device creates a GRE tunnel inside the IPSec VPN tunnel between the networks. The XTM device sends the broadcast traffic through the GRE tunnel. The GRE tunnel requires an unused IP address on each side of the tunnel. So you must configure helper IP addresses for each end of the BOVPN tunnel.

Enable Broadcast Routing for the Local XTM device

1. Select **VPN > Branch Office VPN**.
2. Select a tunnel and click **Edit**.
3. From the **Tunnel** page, select the tunnel route and click **Edit**.
   The Tunnel Route Settings dialog box appears.



4. Select the **Enable broadcast routing over the tunnel** check box. Click **OK**.
   The Tunnel pageappears.The Helper Addresses appear at the bottom of the Addresses tab.



5. In the **Helper Addresses** section, type IP addresses for each end of the broadcast tunnel. The XTM device uses these addresses as the endpoints of the broadcast/multicast GRE tunnel inside the IPSec BOVPN tunnel. You can set the **Local IP** and **Remote IP** to any unused IP address. We recommend you use IP addresses that are not used on any network known to the XTM device.
   - In the **Local IP** text box, type an IP address to use for the local end of the tunnel.
   - In the **Remote IP** text box, type an IP address to use for the remote end of the tunnel.

Configure Broadcast Routing for the XTM Device at the Other End of the Tunnel

1. Repeat Steps 1–4 above to enable broadcast routing for the device at the other end of the tunnel.
2. In the **Helper Addresses** section, type the opposite addresses you typed in the configuration for the other end of the tunnel.
   - In the **Local IP** text box, type the IP address that you typed in the **Remote IP** text box for the device at the other end of the tunnel.
   - In the **Remote IP** text box, type the IP address that you typed in the **Local IP** text box for the device at the other end of the tunnel.

Configure VPN Failover

Failover is an important function of networks that need high availability. When you have multi-WAN failover configured, VPN tunnels automatically fail over to a backup external interface if a failure occurs. You can also configure VPN tunnels to fail over to a backup endpoint if the primary endpoint becomes unavailable.

VPN Failover occurs when one of these two events occur:

- A physical link is down. The XTM device monitors the status of the VPN gateway and the devices identified in the multi-WAN link monitor configuration. If the physical link is down, VPN failover occurs.
- The XTM device detects the VPN peer is not active.

When failover occurs, if the tunnel uses IKE keep-alive IKE continues to send Phase 1 keep-alive packets to the peer. When it gets a response, IKE triggers failback to the primary VPN gateway. If the tunnel uses Dead Peer Detection, failback occurs when a response is received from the primary VPN gateway.

When a failover event occurs, most new and existing connections failover automatically. For example, if you start an FTP "PUT" command and the primary VPN path goes down, the existing FTP connection continues on the backup VPN path. The connection is not lost, but there is some delay. Note that VPN Failover can occur only if:

- Firebox or XTM devices at each tunnel endpoint have Fireware v11.0 or higher installed.
- Multi-WAN failover is configured, as described in *About Using Multiple External Interfaces* on page 125.
- The interfaces of your XTM device are listed as gateway pairs on the remote Firebox or XTM device. If you have already configured multi-WAN failover, your VPN tunnels will automatically fail over to the backup interface.
- DPD is enabled in the Phase 1 settings for the branch office gateway on each end of the tunnel.

VPN Failover does not occur for BOVPN tunnels with dynamic NAT enabled as part of their tunnel configuration. For BOVPN tunnels that do not use NAT, VPN Failover occurs and the BOVPN session continues. With Mobile VPN tunnels, the session does not continue. You must authenticate your Mobile VPN client again to make a new Mobile VPN tunnel.

Define Multiple Gateway Pairs

To configure manual BOVPN tunnels to fail over to a backup endpoint, you must define more than one set of local and remote endpoints (gateway pairs) for each gateway.

For complete failover functionality for a VPN configuration, you must define gateway pairs for each combination of external interfaces on each side of the tunnel. For example, suppose your primary local endpoint is 23.23.1.1/24 with a backup of 23.23.2.1/24. Your primary remote endpoint is 50.50.1.1/24 with a backup of 50.50.2.1/24. For complete VPN Failover, you would need to define these four gateway pairs:

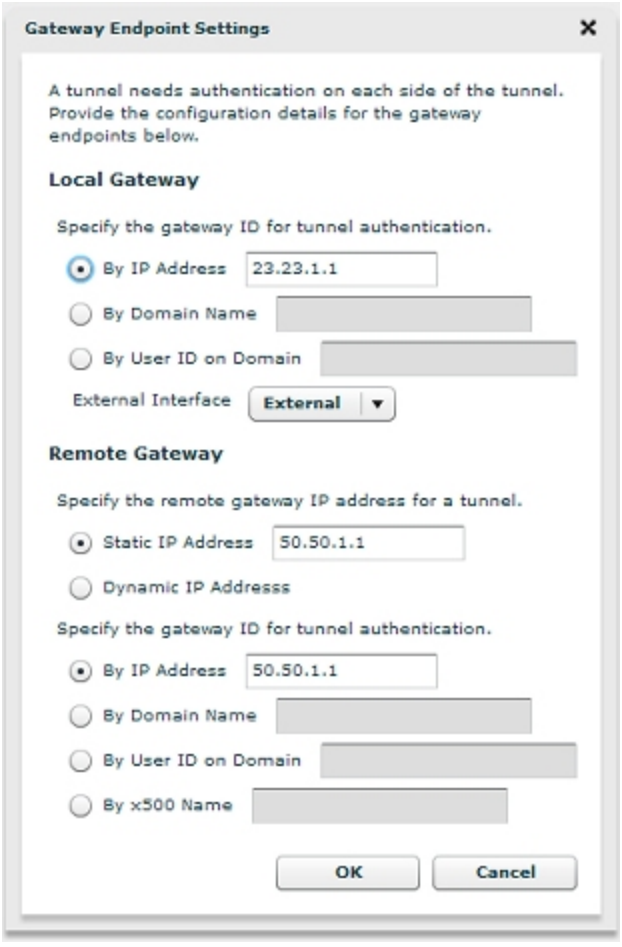
23.23.1.1 - 50.50.1.1

23.23.1.1 - 50.50.2.1

23.23.2.1 - 50.50.1.1

23.23.2.1 - 50.50.2.1

1. Select **VPN > Branch Office VPN**. Click **Add** adjacent to the **Gateways** list to add a new gateway. Give the gateway a name and define the credential method, as described in *Configure Gateways* on page 532.
2. In the **Gateway Endpoints** section of the **Gateway** settings page, click **Add**.
   The Gateway Endpoints Settings dialog box appears.



3. Specify the location of the local and remote gateways. Select the external interface name that matches the local gateway IP address or domain name you add.
   You can add both a gateway IP address and gateway ID for the remote gateway. This can be necessary if the remote gateway is behind a NAT device and requires more information to authenticate to the network behind the NAT device.
4. Click **OK** to close the **New Gateway Endpoints Settings** dialog box.
   The Gateway dialog box appears. The gateway pair you defined appears in the list of gateway endpoints.
5. Repeat this procedure to define additional gateway pairs. You can add up to nine gateway pairs. You can select a pair and click **Up** or **Down** to change the order in which the XTM device attempts connections.
6. Click **Save**.

See VPN Statistics

You can use Fireware XTM Web UI to monitor XTM device VPN traffic and troubleshoot the VPN configuration.

1. Select **System Status > VPN Statistics**.
   The VPN Statistics page appears.
2. To force the selected BOVPN tunnel to rekey, click **Rekey selected BOVPN tunnel**.

   For more information, see *Rekey BOVPN Tunnels* on page 570.
3. To see additional information for use when you troubleshoot, click **Debug**.

For more information, see *VPN Statistics* on page 488.

Rekey BOVPN Tunnels

The gateway endpoints of BOVPN tunnels must generate and exchange new keys after either a set period of time or an amount of traffic passes through the tunnel. If you want to immediately generate new keys before they expire, you can rekey a BOVPN tunnel to force it to expire immediately. This can be helpful when you troubleshoot tunnel issues.

To rekey a BOVPN tunnel:

1. Select **System Status > VPN Statistics**.
   The VPN Statistics page appears.
2. In the **Branch Office VPN Tunnels** list, select a tunnel.
3. Click **Rekey selected BOVPN tunnel**.

Related Questions About Branch Office VPN Set Up

Why do I Need a Static External Address?

To make a VPN connection, each device must know the IP address of the other device. If the address for a device is dynamic, the IP address can change. If the IP address changes, connections between the devices cannot be made unless the two devices know how to find each other.

You can use Dynamic DNS if you cannot get a static external IP address. For more information, see *About the Dynamic DNS Service* on page 89.

How do I Get a Static External IP Address?

You get the external IP address for your computer or network from your ISP or a network administrator. Many ISPs use dynamic IP addresses to make their networks easier to configure and use with many users. Most ISPs can give you a static IP address as an option.

How do I Troubleshoot the Connection?

If you can send a ping to the trusted interface of the remote Firebox and to the computers on the remote network, the VPN tunnel is up. The configuration of the network software or the software applications are possible causes of other problems.

Why is Ping not Working?

If you cannot send a ping to the local interface IP address of the remote XTM device, use these steps:

1. Ping the external address of the remote XTM device.

   For example, at Site A, ping the IP address of Site B. If you do not receive a response, make sure the external network settings of Site B are correct. Site B must be configured to respond to ping requests on that interface. If the settings are correct, make sure that the computers at Site B have a connection to the Internet. If the computers at site B cannot connect, speak to your ISP or network administrator.

2. If you can ping the external address of each XTM device, try to ping a local address in the remote network.

   From a computer at Site A, ping the internal interface IP address of the remote XTM device. If the VPN tunnel is up, the remote XTM device sends the ping back. If you do not receive a response, make sure the local configuration is correct. Make sure that the local DHCP address ranges for the two networks connected by the VPN tunnel do not use any of the same IP addresses. The two networks connected by the tunnel must not use the same IP addresses.

Improve Branch Office VPN Tunnel Availability

There are Branch Office VPN (BOVPN) installations in which all the settings are correct, but BOVPN connections do not always operate correctly. You can use the information below to help you troubleshoot your BOVPN tunnel availability problems. These procedures do not improve general BOVPN tunnel performance.

Most BOVPN tunnels remain available to pass traffic at all times. Problems are often associated with one or more of these three conditions:

- One or both endpoints have unreliable external connections. High latency, high packet fragmentation, and high packet loss can make a connection unreliable. These factors have a greater impact on BOVPN traffic than on other common traffic, like HTTP and SMTP. With BOVPN traffic, the encrypted packets must arrive at the destination endpoint, be decrypted, and then reassembled before the unencrypted traffic can be routed to the destination IP address.
- One endpoint is not an XTM device, or is an older Firebox with older system software. Compatibility tests between new WatchGuard products and older devices are done with the latest software available for older devices. With older software, you could have problems that have been fixed in the latest software release.
  Because they are based on the IPSec standard, XTM devices are compatible with most third-party endpoints. However, some third-party endpoint devices are not IPSec-compliant because of software problems or proprietary settings.
- If there is a low volume of traffic through the tunnel, or if there are long periods of time when no traffic goes through the tunnel, some endpoints terminate the VPN connection. Firebox devices that run Fireware XTM, and Firebox X Edge devices do not do this. Some third-party devices and Firebox devices with older versions of the WFS software use this condition as a way to terminate tunnels that seem to be dead.

You can install the latest operating system and management software on all XTM devices, but all of the other conditions in this list are out of your control. You can, however, take certain actions to improve the availability of the BOVPN.

Select either IKE Keep-alive or Dead Peer Detection, but not both

Both IKE Keep-alive and Dead Peer Detection settings can show when a tunnel is disconnected. When they find the tunnel has disconnected, they start a new Phase 1 negotiation. If you select both IKE Keep-alive and Dead Peer Detection, the Phase 1 renegotiation that one starts can cause the other to identify the tunnel as disconnected and start a second Phase 1 negotiation. Each Phase 1 negotiation stops all tunnel traffic until the tunnel has been negotiated. To improve tunnel stability, select either IKE Keep-alive or Dead Peer Detection. Do not select both.

Note the following about these settings:

*The **IKE Keep-alive** setting is used only by XTM devices. Do not use it if the remote endpoint is a third-party IPSec device.*

When you enable IKE Keep-alive, the XTM device sends a message to the remote gateway device at a regular interval and waits for a response. **Message interval** determines how often a message is sent. **Max Failures** is how many times the remote gateway device can fail to respond before the XTM device tries to renegotiate the Phase 1 connection.

Dead Peer Detection is an industry standard that is used by most IPSec devices. Select Dead Peer detection if both endpoint devices support it.

When you enable Dead Peer Detection, the XTM device monitors tunnel traffic to identify whether a tunnel is active. If no traffic has been received from the remote peer for the amount of time entered for **Traffic idle timeout**, and a packet is waiting to be sent to the peer, the XTM device sends a query. If there is no response after the number of **Max retries**, the XTM device renegotiates the Phase 1 connection. For more information about Dead Peer Detection, see http://www.ietf.org/rfc/rfc3706.txt.

The IKE Keep-alive and Dead Peer Detection settings are part of the Phase 1 settings.

1. From Fireware XTM Web UI, select **VPN > BOVPN**.
2. Select the gateway and click **Edit**.
3. Click the **Phase 1 Settings** tab.

Use the default settings

The default BOVPN settings provide the best combination of security and speed. Use the default settings when possible. If the remote endpoint device does not support one of the WatchGuard default settings, configure the XTM device to use the default setting from the remote endpoint. These are the default settings for WSM 11.x:

> ***Note*** *If a setting is not displayed on the **VPN > BOVPN** configuration pages, you cannot change it.*

General Settings	
Mode	Main (Select Aggressive if one of the devices has a dynamic external IP address.)
NAT Traversal	Yes
NAT Traversal Keep-alive Interval	20 seconds
IKE Keep-alive	Disabled
IKE Keep-alive Message Interval	None
IKE Keep-alive Max Failures	None
Dead Peer Detection (RFC3706)	Enabled
Dead Peer Detection Traffic Idle Timeout	20 seconds
Dead Peer Detection Max Retries	5

PHASE 1 Transform Settings	
Authentication Algorithm	SHA-1
Encryption Algorithm	3DES
SA Life or Negotiation Expiration (hours)	8
SA Life or Negotiation Expiration (kilobytes)	0
Diffie-Hellman Group	2

PHASE 2 Proposal Settings	
Type	ESP
Authentication Algorithm	SHA-1
Encryption Algorithm	AES (256 bit)
Force Key Expiration	Enable
Phase 2 Key Expiration (hours)	8
Phase 2 Key Expiration (kilobytes)	128000
Enable Perfect Forward Secrecy	No
Diffie-Hellman Group	None

Configure the XTM device to send log traffic through the tunnel

If no traffic goes through a tunnel for a period of time, an endpoint can decide that the other endpoint is unavailable and not try to renegotiate the VPN tunnel immediately. One way to make sure traffic goes through the tunnel at all times is to configure the XTM device to send log traffic through the tunnel. You do not need a Log Server to receive and keep records of the traffic. In this case, you intentionally configure the XTM device to send log traffic to a log server that does not exist. This creates a consistent but small amount of traffic sent through the tunnel, which can help to keep the tunnel more stable.

There are two types of log data: WatchGuard logging and syslog logging. If the XTM device is configured to send log data to both a WatchGuard Log Server and a syslog server, you cannot use this method to pass traffic through the tunnel.

You must choose a Log Server IP address to send the log data to. To choose the IP address, use these guidelines.

- The Log Server IP address you use must be an IP address that is included in the remote tunnel route settings. For more information, see *Add Routes for a Tunnel* on page 544.

- The Log Server IP address should not be an IP address that is used by a real device.

The two types of logging generate different amounts of traffic.

WatchGuard Logging

No log data is sent until the XTM device has connected to a Log Server. The only types of traffic sent through the tunnel are attempts to connect to a Log Server that are sent every three minutes. This can be enough traffic to help tunnel stability with the least impact on other BOVPN traffic.

Syslog Logging

Log data is immediately sent to the syslog server IP address. The volume of log data depends on the traffic that the XTM device handles. Syslog logging usually generates enough traffic that packets are always passing through the tunnel. The volume of traffic can occasionally make regular BOVPN traffic slower, but this is not common.

To improve stability and have the least impact on BOVPN traffic, try the WatchGuard Logging option first. If this does not improve the stability of the BOVPN tunnel, try syslog logging. The subsequent procedures assume that both endpoint devices are WatchGuard devices, and that neither endpoint is configured to send log data to either a WatchGuard Log Server or a syslog server. If an endpoint is already configured to send log data that a server collects, do not change those logging settings.

Different options you can try include:

- Configure one endpoint to send WatchGuard log traffic through the tunnel.
- Configure the other endpoint to send WatchGuard log traffic through the tunnel.
- Configure both endpoints to send WatchGuard log traffic through the tunnel.
- Configure one endpoint to send syslog log traffic through the tunnel.
- Configure only the other endpoint to send syslog log traffic through the tunnel.
- Configure both endpoints to send syslog log traffic through the tunnel.

Send WatchGuard log data through the tunnel

1. Select **System > Logging**.
   The Logging page appears.
2. Select the **Enable WatchGuard logging to these servers** check box.
3. In the **Log Server Address** text box, type the IP address you have selected for the Log Server in the **Log Server IP Address** text box.
4. Type an encryption key in the **Encryption Key** text box and confirm the encryption key in the **Confirm** text box.
   The allowed range for the encryption key is 8–32 characters. You can use all characters except spaces and slashes (/ or \).
5. Click **Add**. Click **Save**.

Send syslog data through the tunnel

1. Select **System > Logging**.
   The Logging page appears.
2. Click the **Syslog Server** tab.
3. Select the **Enable Syslog logging to this server** check box.
4. Type the IP address you have chosen for the syslog server in the adjacent text box.
5. Click **Save**.

21 Mobile VPN with PPTP

About Mobile VPN with PPTP

Mobile Virtual Private Networking (Mobile VPN) with Point-to-Point Tunneling Protocol (PPTP) creates a secure connection between a remote computer and the network resources behind the XTM device. Each XTM device supports as many as 50 users at the same time. Mobile VPN with PPTP users can authenticate to the XTM device, or to a RADIUS or VACMAN Middleware authentication server. To use Mobile VPN with PPTP, you must configure the XTM device and the remote client computers.

Mobile VPN with PPTP Requirements

Before you configure an XTM device to use Mobile VPN with PPTP, make sure you have this information:

- The IP addresses for the remote client to use for Mobile VPN with PPTP sessions.

  For Mobile VPN with PPTP tunnels, the XTM device gives each remote user a virtual IP address. These IP addresses cannot be addresses that the network behind the XTM device uses. The safest procedure to give addresses for Mobile VPN users is to install a "placeholder" secondary network. Then, select an IP address from that network range. For example, create a new subnet as a secondary network on your trusted network 10.10.0.0/24. Select the IP addresses in this subnet for your range of PPTP addresses.
- The IP addresses of the DNS and WINS servers that resolve host names to IP addresses.
- The user names and passwords of users that are allowed to connect to the XTM device with Mobile VPN with PPTP.

Encryption Levels

For Mobile VPN with PPTP, you can select to use 128-bit encryption or 40-bit encryption. Software versions of Windows XP in the United States have 128-bit encryption enabled. You can get a strong encryption patch from Microsoft for other versions of Windows. The XTM device always tries to use 128-bit encryption first. It can be configured to use 40-bit encryption if the client cannot use a 128-bit encrypted connection.

For more information on how to allow 40-bit encryption, see *Configure Mobile VPN with PPTP* on page 578.

If you do not live in the United States and you want to have strong encryption allowed on your LiveSecurity Service account, send an email message to supportid@watchguard.com and include all of the following information:

- Your LiveSecurity Service key number
- Date of purchase for your WatchGuard product
- Name of your company
- Company mailing address
- Telephone number and contact name
- Email address

If you live in the United States and do not already use WatchGuard System Manager (WSM) with strong encryption, you must download the strong encryption software from your Software Downloads page in the LiveSecurity Service web site.

1. Open a web browser and go to www.watchguard.com.
2. Log in to your LiveSecurity Service account.
3. Click **Support**.
   Your WatchGuard Support Center appears.
4. In the **Managing Your Products** section, click **Software Downloads**.
5. From the **Choose product family** list, select your XTM device.
   The Software Downloads page appears.
6. Download **WatchGuard System Manager with Strong Encryption**.

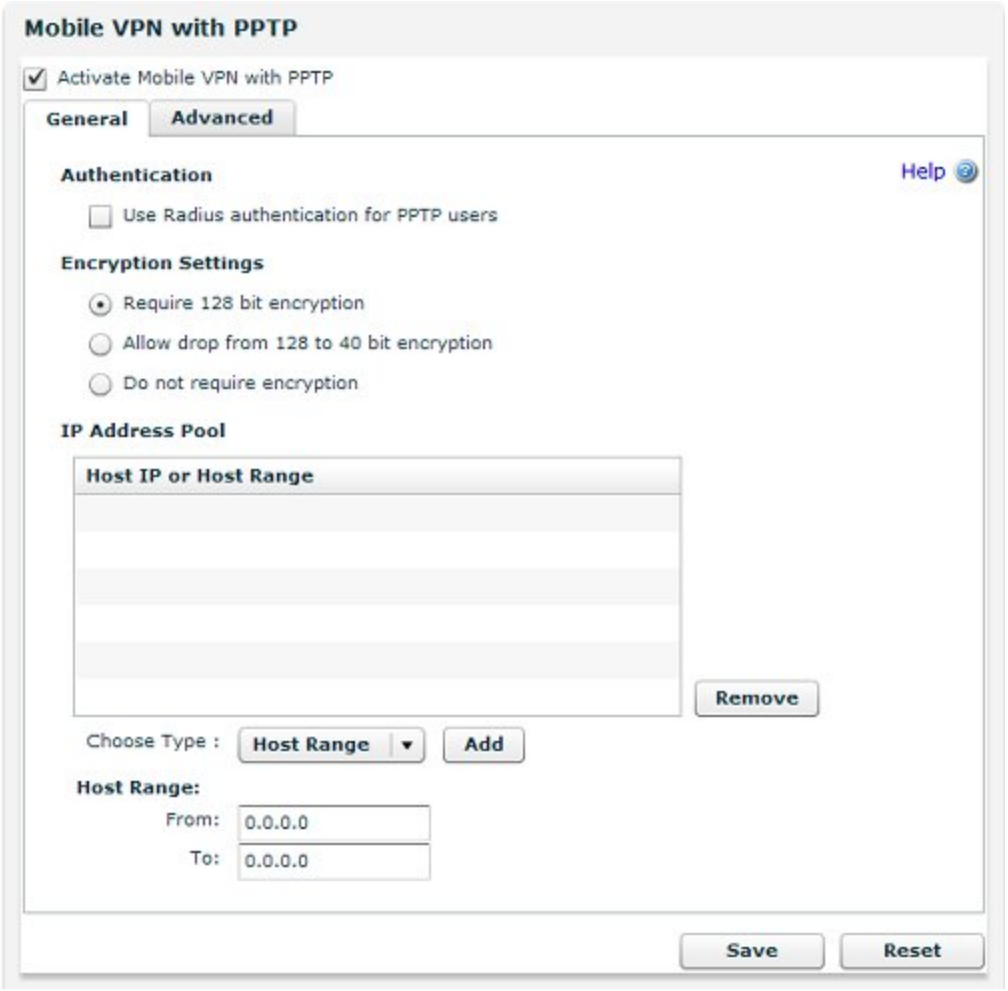
Before you install the WatchGuard System Manager with Strong Encryption software, you must uninstall any other versions of WatchGuard System Manager from your computer.

> ***Note*** *To keep your current XTM device configuration, do not use the Quick Setup Wizard when you install the new software. Open WatchGuard System Manager, connect to the XTM device, and save your configuration file. Configurations with a different encryption version are compatible.*

Configure Mobile VPN with PPTP

To configure your XTM device to accept PPTP connections you must first activate and configure the settings for Mobile VPN with PPTP.

1. Select **VPN > Mobile VPN with PPTP**.



2. Select the **Activate Mobile VPN with PPTP** check box.
   This allows PPTP remote users to be configured and automatically creates a WatchGuard PPTP policy to allow PPTP traffic to the XTM device. We recommend that you do not change the default properties of the WatchGuard PPTP policy.
3. Configure the authentication settings as described in the subsequent sections.
4. Click **Save**.

Authentication

Mobile VPN with PPTP users can authenticate to the XTM device internal database or use extended authentication to a RADIUS or VACMAN Middleware server as an alternative to the XTM device. The instructions to use a VACMAN Middleware server are identical to the instructions to use a RADIUS server.

To use the XTM device internal database, do not select the **Use RADIUS authentication for PPTP users** check box.

To use a RADIUS or VACMAN Middleware server for authentication:

1. Select the **Use RADIUS Authentication for PPTP users** check box.
2. *Configure RADIUS Server Authentication* or *Configure VASCO Server Authentication*.

3. On the RADIUS server, create a PPTP-Users group and add names or groups of PPTP users.

> ***Note*** *To establish the PPTP connection, the user must be a member of a group named PPTP-Users. Once the user is authenticated, the XTM device keeps a list of all groups that a user is a member of. Use any of the groups in a policy to control traffic for the user.*

Encryption Settings

U.S. domestic versions of Windows XP have 128-bit encryption enabled. You can get a strong encryption patch from Microsoft for other versions of Windows.

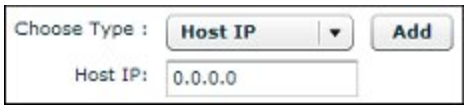
- If you want to require 128-bit encryption for all PPTP tunnels, select **Require 128-bit encryption**. We recommend that you use 128-bit encryption for VPN.
- To allow the tunnels to drop from 128-bit to 40-bit encryption for connections that are less reliable, select **Allow Drop from 128-bit to 40-bit**.
  The XTM device always tries to use 128-bit encryption first. It uses 40-bit encryption if the client cannot use the 128-bit encrypted connection. Usually, only customers outside the United States select this check box.
- To allow traffic that is not encrypted through the VPN, select **Do not require encryption**.

Add to the IP Address Pool

Mobile VPN with PPTP supports as many as 50 users at the same time. The XTM device gives an open IP address to each incoming Mobile VPN user from a group of available IP addresses. This continues until all the addresses are in use. After a user closes a session, the address is put back in the available group. The subsequent user who logs in gets this address.

You must configure two or more IP addresses for PPTP to operate correctly.

1. In the **IP Address Pool** section, in the **Choose Type** drop-down list, select either **Host IP** (for a single IP address) or **Host Range** (for a range of IP addresses).

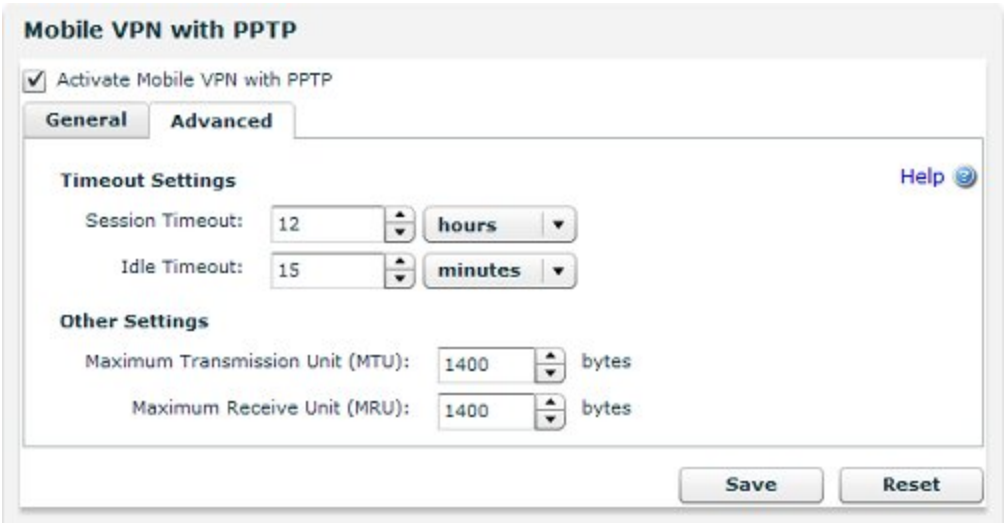


2. In the **Host IP** text box, type an IP address.
   If you selected **Host Range**, the first IP address in the range is **From** and the last IP address in the range is **To**.

3. Click **Add** to add the host IP address or host range to the IP address pool.
   You can configure up to 50 IP addresses.
   If you select **Host IP**, you must add at least two IP addresses.
   If you select **Host Range** and add a range of IP addresses that is larger than 50 addresses, Mobile VPN with PPTP uses the first 50 addresses in the range.
4. Repeat Steps 1–3 to configure all the addresses for use with Mobile VPN with PPTP.

Advanced Tab Settings

1. On the **Mobile VPN with PPTP** page, select the **Advanced** tab.
2. Configure the **Timeout Settings**, and the **Maximum Transmission Unit (MTU)** and **Maximum Receive Unit (MRU)** settings as described in the subsequent sections.
   We recommend that you keep the default settings.



Timeout Settings

You can define two timeout settings for PPTP tunnels if you use RADIUS authentication:

Session Timeout

The maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, no session timeout is used and the user can stay connected for any length of time.

Idle Timeout

The maximum length of time the user can stay authenticated when idle (no traffic passes to the external network interface). If you set this field to zero (0) seconds, minutes, hours, or days, no idle timeout is used and the user can stay idle for any length of time.

If you do not use RADIUS for authentication, the PPTP tunnel uses the timeout settings that you set for each Firebox User. For more information about Firebox user settings, see *Define a New User for Firebox Authentication* on page 256.

Other Settings

The **Maximum Transmission Unit (MTU)** or **Maximum Receive Unit (MRU)** sizes are sent to the client as part of the PPTP parameters to use during the PPTP session. Do not change MTU or MRU values unless you know the change fixes a problem with your configuration. Incorrect MTU or MRU values cause traffic through the PPTP VPN to fail.

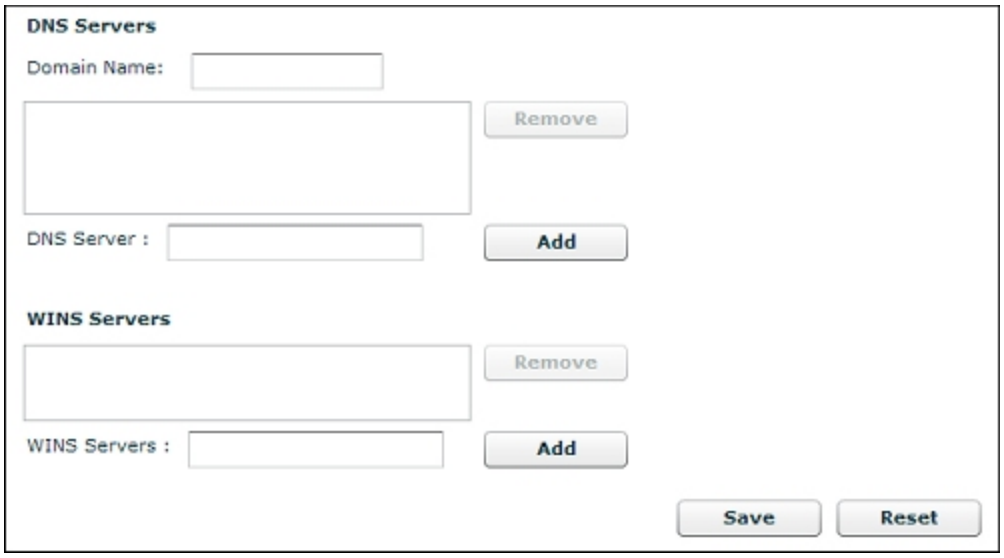
To change the MTU or MRU values:

1. On the **Mobile VPN with PPTP** page, select the **Advanced** tab.
2. In the **Other Settings** section, type or select the **Maximum Transmission Unit (MTU)** or **Maximum Receive Unit (MRU)** values.

Configure WINS and DNS Servers

Mobile VPN with PPTP clients use shared Windows Internet Naming Service (WINS) and Domain Name System (DNS) server addresses. DNS changes host names to IP addresses, while WINS changes NetBIOS names to IP addresses. The trusted interface of the XTM device must have access to these servers.

1. Select **Network > Interfaces**.
   The Network Interfaces page appears. The WINS and DNS settings are at the bottom.



2. In the **DNS Servers** section, type a **Domain Name** for the DNS server.
3. In the **DNS Server** text box, type the IP address for the DNS Server and click **Add**.
   You can add up to three addresses for DNS servers.
4. In the **WINS Servers** text box, type the IP address for a WINS server and click **Add**.
   You can add up to two addresses for WINS servers.
5. Click **Save**.

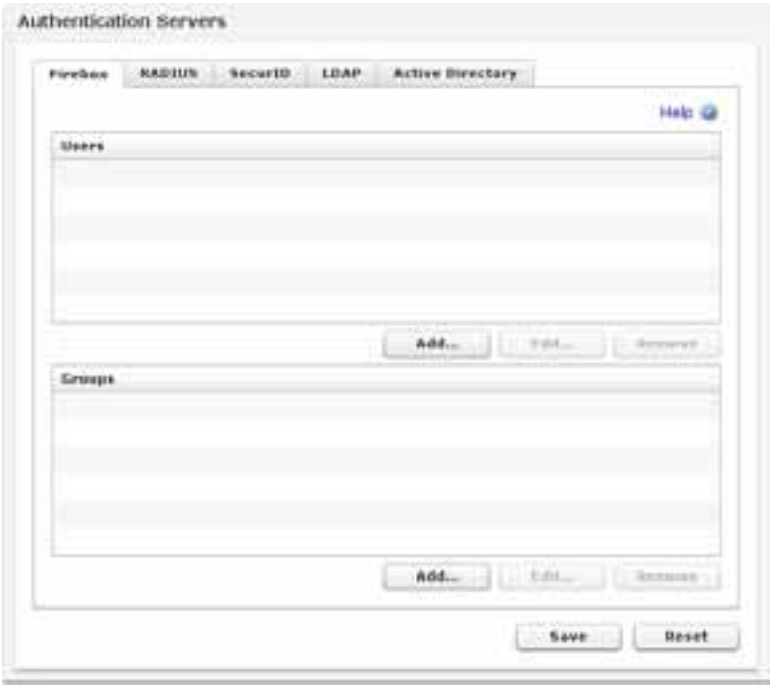
Add New Users to the PPTP-Users Group

To create a PPTP VPN tunnel with the XTM device, mobile users type their user names and passphrases to authenticate. The XTM device uses this information to authenticate the user.

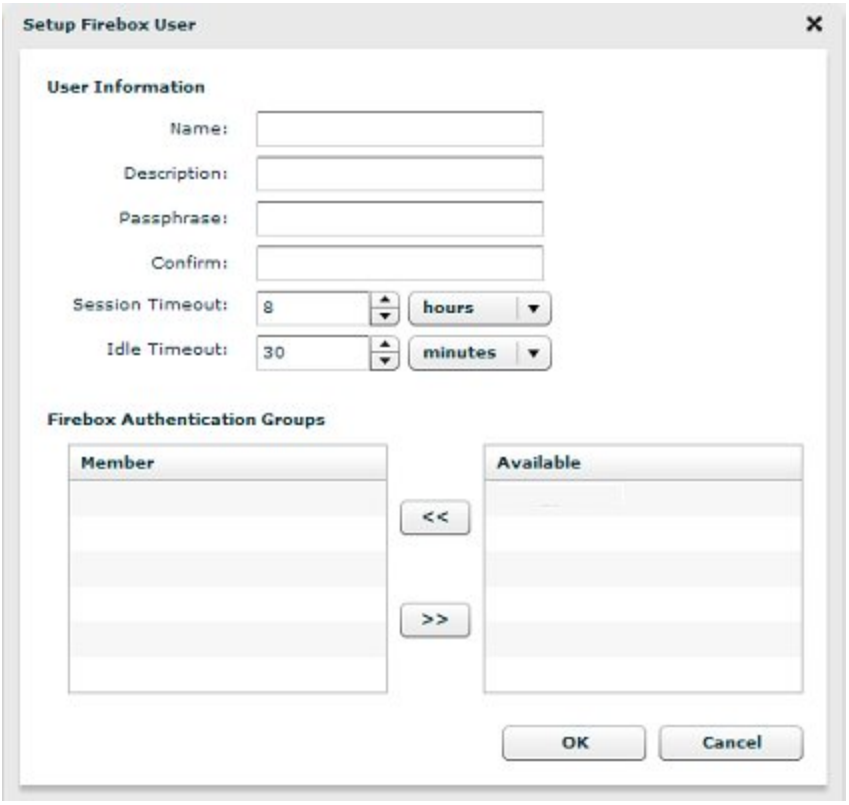
When you enable PPTP in your XTM device configuration, a default user group is created automatically. This user group is called PPTP_Users. You see this group name when you create a new user or add user names to policies.

For more information on XTM device groups, see *Configure Your XTM Device as an Authentication Server* on page 254.

1. Select **Authentication > Servers**.
   The Authentication Servers page appears.
2. Select the **Firebox** tab.



3. In the **Users** section, click **Add**.
   The Setup Firebox User dialog box appears.



4. Type a **Name** and **Passphrase** for the new user. Type the passphrase again to confirm it.
   A description is not required. We recommend that you do not change the default values for Session Timeout and Idle Timeout.
5. In the **Available** list, select **PPTP-Users** and click <<.
   PPTP-Users appears in the Member list.
6. Click **OK**.
7. Click **Save**.

Configure Policies to Allow Mobile VPN with PPTP Traffic

Mobile VPN with PPTP users do not have access privileges through a XTM device by default. To give remote users access to specified network resources, you must add user names, or the PPTP-Users group, as sources and destinations in individual policy definitions.

For more information, see *Use Authorized Users and Groups in Policies* on page 285.

To use WebBlocker to control remote user access, add PPTP users or the PPTP-Users group to a proxy policy that controls WebBlocker.

> ***Note*** *If you assign addresses from a trusted network to PPTP users, the traffic from the PPTP user is not considered to be trusted. All Mobile VPN with PPTP traffic is not trusted by default. Regardless of assigned IP address, policies must be created to allow PPTP users to get access to network resources.*

Configure Policies to Allow Mobile VPN with PPTP Traffic

Mobile VPN with PPTP users do not have access privileges through a XTM device by default. You must configure policies to allow PPTP users to get access to network resources. You can add new policies or edit existing policies.

> ***Note*** *If you assign addresses from a trusted network to PPTP users, the traffic from the PPTP user is not considered to be trusted. All Mobile VPN with PPTP traffic is untrusted by default. Regardless of assigned IP address, policies must be created to allow PPTP users access to network resources.*

Allow PPTP Users to Access a Trusted Network

In this example, you add an Any policy to give all members of the PPTP-Users group full access to resources on all trusted networks.

1. Select **Firewall > Firewall Policies**.
2. Click  .
   The Select a policy type page appears.
3. Expand the **Packet Filters** folder.
   A list of templates for packet filters appears.
4. Select **Any**.
5. In the **Name** text box, type a name for the policy.
   Choose a name to help you identify this policy in your configuration.
6. Click **Add policy**.
   The Policy Configuration page appears, with the Policy tab selected.
7. In the **From** section, select **Any-Trusted** and click **Remove**.
8. In the **From** section, click **Add**.
   The Add Member dialog box appears.
9. From the **Member Type** drop-down list, select **PPTP Group**.
10. Select **PPTP-Users** and click **OK**.
    The name of the authentication method appears in parenthesis .
    If the PPTP-Users group does not appear in the list, you must first define it for your device. For more information, see Use Authorized Users and Groups in Policies on page 285.
11. Click **OK** to close the **Add Member** dialog box.
12. In the **To** section, select **Any-External** and click **Remove.**
13. In the **To** section, click **Add**.
    The Add Member dialog box appears.
14. In the **Select Members** list, select **Any-Trusted** and click **OK**.
    Any-Trusted appears in the To list.
15. Click **Save**.

For more information about policies, see *Add Policies to Your Configuration* on page 291.

Use Other Groups or Users in a PPTP Policy

Users must be a member of the PPTP-Users group to make a PPTP connection. When you configure a policy to give the PPTP users access to network resources, you can use the individual user name or any other group that the user is a member of.

To select add user or group other than PPTP-Users to a policy:

1. Select **Firewall > Firewall Policies**.
2. Double-click a policy.
   The Policy configuration page appears with the Policy tab selected.
3. In the **From** section, click **Add**.
   The Add Member dialog box appears.
4. From the **Member Type** drop-down list, select **Firewall User** or **Firewall Group**.
5. Select the user or group you want to add and click **OK**.
   The user you selected appears in the From list.
6. Click **Save**.

For more information on how to use users and groups in policies, see *Use Authorized Users and Groups in Policies* on page 285.

Options for Internet Access Through a Mobile VPN with PPTP Tunnel

You can enable remote users to access the Internet through a Mobile VPN tunnel. This option affects your security because this Internet traffic is not filtered or encrypted. You have two options for Mobile VPN tunnel routes: default-route VPN and split tunnel VPN.

Default-Route VPN

The most secure option is to require that all remote user Internet traffic is routed through the VPN tunnel to the XTM device. Then, the traffic is sent back out to the Internet. With this configuration (known as default-route VPN), the XTM device is able to examine all traffic and provide increased security, although it uses more processing power and bandwidth. When you use default-route VPN, a dynamic NAT policy must include the outgoing traffic from the remote network. This allows remote users to browse the Internet when they send all traffic to the XTM device.

> ***Note*** *If you use the "route print" or "ipconfig" commands after you start a Mobile VPN tunnel on a computer with Microsoft Windows installed, you see incorrect default gateway information. The correct information is located on the **Details** tab of the **Virtual Private Connection Status** dialog box.*

Split Tunnel VPN

Another configuration option is to enable split tunneling. This configuration enables users to browse the Internet without the need to send Internet traffic through the VPN tunnel. Split tunneling improves network performance, but decreases security because the policies you create are not applied to the Internet traffic. If you use split tunneling, we recommend that each client computer have a software firewall.

Default-Route VPN Setup for Mobile VPN with PPTP

In Windows Vista, XP, and 2000, the default setting for a PPTP connection is default-route. Your XTM device must be configured with dynamic NAT to receive the traffic from a PPTP user. Any policy that manages traffic going out to the Internet from behind the XTM device must be configured to allow the PPTP user traffic.

When you configure your default-route VPN:

- Make sure that the IP addresses you have added to the PPTP address pool are included in your dynamic NAT configuration on the XTM device.
  From Policy Manager, select **Network > NAT**.
- Edit your policy configuration to allow connections from the PPTP-Users group through the external interface.
  For example, if you use WebBlocker to control web access, add the PPTP-Users group to the proxy policy that is configured to with WebBlocker enabled.

Split Tunnel VPN Setup for Mobile VPN with PPTP

On the client computer, edit the PPTP connection properties to not send all traffic through the VPN.

1. For Windows Vista, XP, or 2000, select **Control Panel > Network Connections** and right-click the VPN connection.
2. Select **Properties**.
   The VPN properties dialog box appears.
3. Select the **Networking** tab.
4. Select **Internet Protocol (TCP/IP)** in the list box and click **Properties**.
   The Internet Protocol (TCP/IP) Properties dialog box appears.
5. On the **General** tab, click **Advanced**.
   The Advanced TCP/IP Settings dialog box appears.
6. Windows XP and Windows 2000 — On the **General** tab (XP and Windows 2000), clear the **Use default gateway on remote network** check box.
   Windows Vista — On the **Settings** tab (XP and Windows 2000), clear the **Use default gateway on remote network** check box.

Prepare Client Computers for PPTP

Before you can use your client computers as Mobile VPN with PPTP remote hosts, you must first prepare each computer with Internet access. Then, you can use the instructions in the subsequent sections to:

- Install the necessary version of Microsoft Dial-Up Networking and the necessary service packs
- Prepare the operating system for VPN connections
- Install a VPN adapter (not necessary for all operating systems)

Prepare a Windows NT or 2000 Client Computer: Install MSDUN and Service Packs

To correctly configure Mobile VPN with PPTP on a computer with Windows NT and 2000, make sure these options are installed:

- MSDUN (Microsoft Dial-Up Networking) upgrades
- Other extensions
- Service packs

For Mobile VPN with PPTP, you must have these upgrades installed:

Encryption	Platform	Application
Base	Windows NT	40-bit SP4
Strong	Windows NT	128-bit SP4
Base	Windows 2000	40-bit SP2*
Strong	Windows 2000	128-bit SP2*

*40-bit encryption is the default for Windows 2000. If you upgrade from Windows 98 with strong encryption, Windows 2000 automatically sets strong encryption for the new installation.

To install these upgrades or service packs, go to the Microsoft Download Center web site at:

http://www.microsoft.com/downloads/

The steps to configure and establish a PPTP connection are different for each version of Microsoft Windows.

To set up a PPTP connection on Windows Vista, see *Create and Connect a PPTP Mobile VPN for Windows Vista* on page 589.

To set up a PPTP connection on Windows XP, see *Create and Connect a PPTP Mobile VPN for Windows XP* on page 589.

To set up a PPTP connection on Windows 2000, see *Create and Connect a PPTP Mobile VPN for Windows 2000* on page 590.

Create and Connect a PPTP Mobile VPN for Windows Vista

Create a PPTP Connection

To prepare a Windows Vista client computer, you must configure the PPTP connection in the network settings.

1. From the Windows **Start** menu, select **Settings > Control Panel**.
   The Start menu in Windows Vista is located in the lower-left corner of the screen.
2. Click **Network and Internet**.
   The Network and Sharing Center appears.
3. In the left column, below **Tasks**, click **Connect to a network**.
   The New Connection Wizard starts.
4. Select **Connect to a workplace** and click **Next**.
   The Connect to a workplace dialog box appears.
5. Select **No, create a new connection** and click **Next**.
   The How do you want to connect dialog box appears.
6. Click **Use my Internet connection (VPN)**.
   The Type the Internet address to connect to dialog box appears.
7. Type the hostname or IP address of the XTM device external interface in the **Internet address** field.
8. Type a name for the Mobile VPN (such as "PPTP to XTM") in the **Destination name** text box.
9. Select whether you want other people to be able to use this connection.
10. Select the **Don't connect now; just set it up so I can connect later** check box so that the client computer does not try to connect at this time.
11. Click **Next**.
    The Type your user name and password dialog box appears.
12. Type the **User name** and **Password** for this client.
13. Click **Create**.
    The connection is ready to use dialog box appears.
14. To test the connection, click **Connect now**.

Establish the PPTP Connection

To connect a Windows Vista client computer, replace **[name of the connection]** with the actual name you used when configuring the PPTP connection. The user name and password refers to one of the users you added to the PPTP-Users group. For more information, see *Add New Users to the PPTP-Users Group* on page 583.

Make sure you have an active connection to the Internet before you begin.

1. Select **Start > Settings > Network Connections > [name of the connection]**
   The Windows Vista Start button is located in the lower-left corner of your screen.
2. Type the user name and password for the connection and click **Connect**.
3. The first time you connect, you must select a network location. Select **Public location**.

Create and Connect a PPTP Mobile VPN for Windows XP

To prepare a Windows XP client computer, you must configure the PPTP connection in the network settings.

Create the PPTP Mobile VPN

From the Windows Desktop of the client computer:

1. From the Windows **Start** menu, select **Control Panel > Network Connections**.
2. Select **Create a new connection**.
   Or, click **New Connection Wizard** in Windows Classic view.
   The New Connection wizard appears.
3. Click **Next**.
4. Select **Connect to the network at my workplace** and click **Next**.
5. Select **Virtual Private Network connection** and click **Next**.
6. Type a name for the new connection (such as "Connect with Mobile VPN") and click **Next**.
7. Select if Windows ensures the public network is connected:
   - For a broadband connection, select **Do not dial the initial connection**.
     Or,
   - For a modem connection, select **Automatically dial this initial connection**, and then select a connection name from the drop-down list.
8. Click **Next**.
   The VPN Server Selection screen appears. The wizard includes this screen if you use Windows XP SP2. Not all Windows XP users see this screen.
9. Type the host name or IP address of the XTM device external interface and click **Next**.
   The Smart Cards screen appears.
10. Select whether to use your smart card with this connection profile and click **Next**.
    The Connection Availability screen appears.
11. Select who can use this connection profile and click **Next**.
12. Select **Add a shortcut to this connection to my desktop**.
13. Click **Finish**.

Connect with the PPTP Mobile VPN

1. Start an Internet connection through a dial-up network, or directly through a LAN or WAN.
2. Double-click the shortcut to the new connection on your desktop.
   Or, select **Control Panel > Network Connections** and select your new connection from the Virtual Private Network list.
3. Type the user name and passphrase for the connection.
   For more information about the user name and passphrase, see *Add New Users to the PPTP-Users Group* on page 583.
4. Click **Connect**.

Create and Connect a PPTP Mobile VPN for Windows 2000

To prepare a Windows 2000 remote host, you must configure the PPTP connection in the network settings.

Create the PPTP Mobile VPN

From the Windows Desktop of the client computer:

1. From the Windows **Start** menu, select **Settings > Network Connections > Create a New Connection**.

The New Connection wizard appears.

2. Click **Next**.
3. Select **Connect to the network at my workplace** and click **Next**.
4. Click **Virtual Private Network connection**.
5. Type a name for the new connection (such as "Connect with Mobile VPN") and click **Next**.
6. Select to not dial (for a broadband connection), or to automatically dial (for a modem connection) this connection, and click **Next**.
7. Type the host name or IP address of the XTM device external interface and click **Next**.
8. Select **Add a shortcut to this connection to my desktop** and click **Finish**.

Connect with the PPTP Mobile VPN

1. Start your Internet connection through a dial-up network, or connect directly through a LAN or WAN.
2. Double-click the shortcut to the new connection on your desktop.
   Or, select **Control Panel > Network Connections** and select your new connection from the Virtual Private Network list.
3. Type the user name and passphrase for the connection.
   For more information about the user name and passphrase, see *Add New Users to the PPTP-Users Group* on page 583.
4. Click **Connect**.

Make Outbound PPTP Connections from Behind an XTM Device

If necessary, you can make a PPTP connection to a XTM device from behind a different XTM device. For example, one of your remote users goes to a customer office that has a XTM device. The user can connect to your network with a PPTP connection. For the local XTM device to correctly allow the outgoing PPTP connection, add the PPTP policy and allow traffic from the network the user is on to the *Any-External* alias.

To add a policy, see *Add Policies to Your Configuration* on page 291.

22 Mobile VPN with IPSec

About Mobile VPN with IPSec

Mobile VPN with IPSec is a client software application that is installed on a remote computer. The client makes a secure connection from the remote computer to your protected network through an unsecured network, such as the Internet. The Mobile VPN client uses Internet Protocol Security (IPSec) to secure the connection.

These topics include instructions to help you configure a Mobile VPN tunnel between the Mobile VPN with IPSec client and a XTM device with Fireware XTM installed.

Configure a Mobile VPN with IPSec Connection

You can configure the XTM device to act as an endpoint for Mobile VPN with IPSec tunnels.

1. Connect to Fireware XTM Web UI for your XTM device.
2. Select **VPN > Mobile VPN with IPSec**.

A user must be a member of a Mobile VPN group to be able to make a Mobile VPN with IPSec connection. When you add a Mobile VPN group, an *Any* policy is added to **Firewall > Mobile VPN Policies** tab that allows traffic to pass to and from the authenticated Mobile VPN user.

Click the **Generate** button to create an end-user profile (called a .wgx file) that you can save.

The user must have this .wgx file to configure the Mobile VPN client computer. If you use a certificate for authentication, .p12 and cacert.pem files are also generated. These files can be found in the same location as the .wgx end-user profile.

To restrict Mobile VPN client access, delete the *Any* policy and add policies to **Firewall > Mobile VPN Policies** that allow access to resources.

When the XTM device is configured, the client computer must have the Mobile VPN with IPSec client software installed. For information on how to install the Mobile VPN with IPSec client software, see *Install the Mobile VPN with IPSec Client Software* on page 622.

When the user computer is correctly configured, the user makes the Mobile VPN connection. If the credentials the user authenticates with match an entry in the XTM device user database, and if the user is in the Mobile VPN group you create, the Mobile VPN session is authenticated.

System Requirements

Before you configure your XTM device for Mobile VPN with IPSec, make sure you understand the system requirements for the WatchGuard management computer and the mobile user client computer.

WatchGuard System Manager with strong encryption

Because strict export restrictions are put on high encryption software, WatchGuard System Manager is available with two encryption levels. To generated an encrypted end-user profile for Mobile VPN with IPSec, you must make sure you set up your XTM device with the version of WatchGuard System Manager with strong encryption. The IPSec standard requires a minimum of 56-bit encryption. For more information, see Install WatchGuard System Manager software.

Mobile user client computer

You can install the Mobile VPN with IPSec client software on any computer with Windows 2000 Professional, Windows XP (32-bit and 64-bit), or Windows Vista (32-bit and 64-bit). Before you install the client software, make sure the remote computer does not have any other IPSec VPN client software installed. You must also uninstall any desktop firewall software (other than Microsoft firewall software) from each remote computer. For more information, see *Client Requirements* on page 622.

> ***Note*** *To distribute the end-user profile as an encrypted (.wgx) file, we recommend that you use WatchGuard System Manager. You can use Fireware XTM Web UI to configure Mobile VPN with IPSec and generate the unencrypted (.ini) end-user profile.*
> *For more information about the two types of end-user profile configuration files, see About Mobile VPN Client Configuration Files on page 595.*

Options for Internet Access Through a Mobile VPN with IPSec Tunnel

You can allow remote users to access the Internet through a Mobile VPN tunnel. This option affects your security because Internet traffic is not filtered or encrypted. You have two options for Mobile VPN tunnel routes: default-route VPN and split tunnel VPN.

Default-Route VPN

The most secure option is to require that all remote user Internet traffic is routed through the VPN tunnel to the XTM device. From the XTM device, the traffic is then sent back out to the Internet. With this configuration (known as default-route VPN), the XTM device is able to examine all traffic and provide increased security, although the XTM device uses more processing power and bandwidth. When you use default-route VPN, a dynamic NAT policy must include the outgoing traffic from the remote network. This allows remote users to browse the Internet when they send all traffic to the XTM device.

For more information about dynamic NAT, see *Add Firewall Dynamic NAT Entries* on page 145.

Split Tunnel VPN

Another configuration option is to enable split tunneling. This configuration allows users to browse the Internet normally. Split tunneling decreases security because XTM device policies are not applied to the Internet traffic, but performance is increased. If you use split tunneling, your client computers should have a software firewall.

About Mobile VPN Client Configuration Files

With Mobile VPN with IPSec, the network security administrator controls end user profiles. Policy Manager is used to create the Mobile VPN with IPSec group and create an end user profile, with the file extension .wgx or .ini. The .wgx and .ini files contain the shared key, user identification, IP addresses, and settings that are used to create a secure tunnel between the remote computer and the XTM device.

The .wgx file is encrypted with a passphrase that is eight characters or greater in length. Both the administrator and the remote user must know this passphrase. When you use the Mobile VPN with IPSec client software to import the .wgx file, the passphrase is used to decrypt the file and configure the client. The .wgx file does not configure the Line Management settings.

The .ini configuration file is not encrypted. It should only be used if you have changed the **Line Management** setting to anything other than **Manual**. For more information, see **Line Management** on the **Advanced** tab in *Modify an Existing Mobile VPN with IPSec Group Profile* on page 604.

You can create or re-create the .wgx and .ini file at any time. For more information, see *Mobile VPN with IPSec Configuration Files* on page 616.

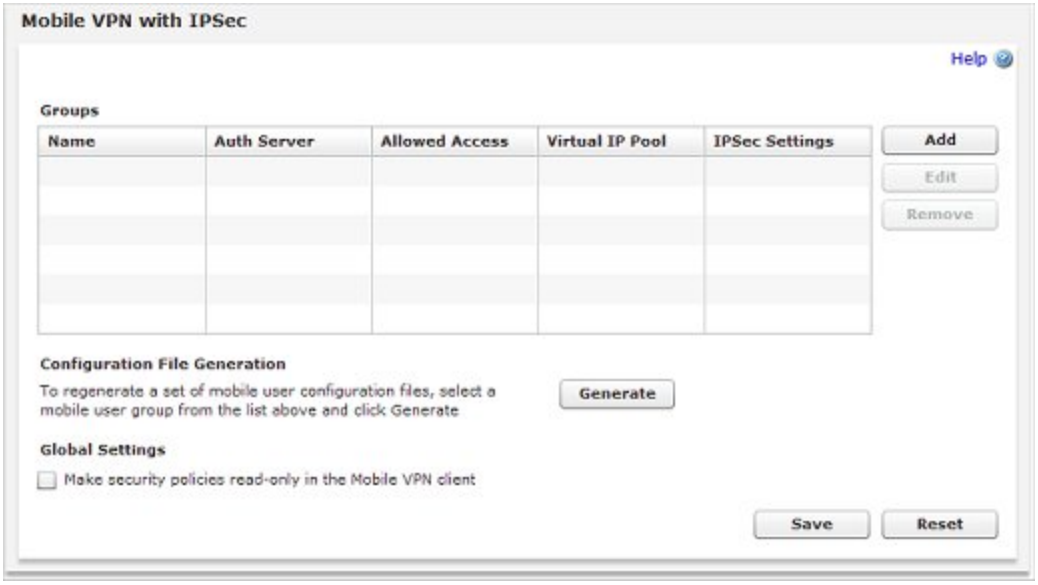
If you want to lock the profiles for mobile users, you can make them read-only. For more information, see *Lock Down an End User Profile* on page 615.

Configure the XTM Device for Mobile VPN with IPSec

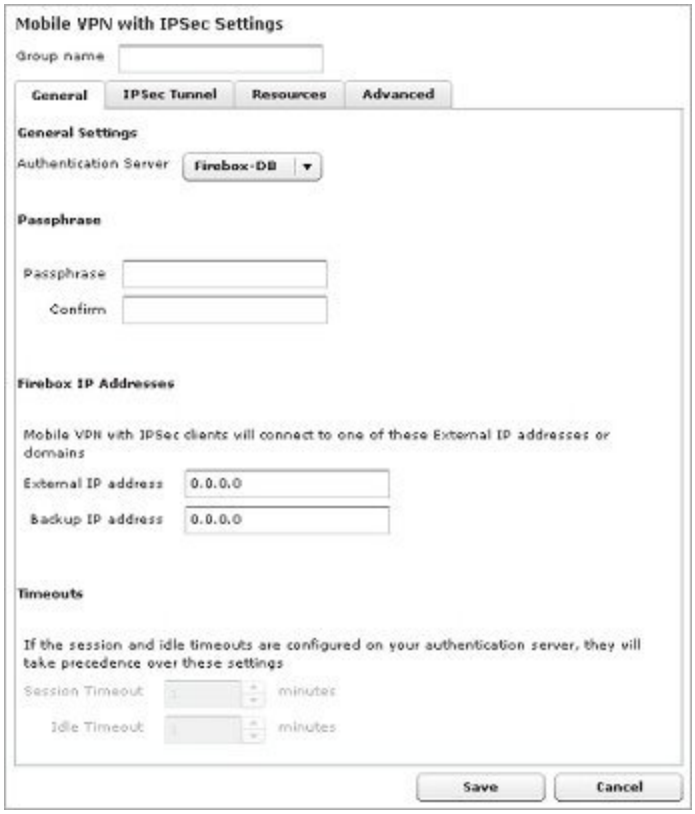
You can enable Mobile VPN with IPSec for a group of users you have already created, or you can create a new user group. The users in the group can authenticate either to the XTM device or to a third-party authentication server included in your XTM device configuration.

Configure a Mobile VPN with IPSec Group

1. Select **VPN > Mobile VPN with IPSec**.
   The Mobile VPN with IPSec page appears.



2. Click **Add**.
   The Mobile User VPN with IPSec Settings page appears.



3. In the **Group name** text box, type a group name.
   You can type the name of an existing group, or the name for a new Mobile VPN group. Make sure the name is unique among VPN group names, as well as all interface and VPN tunnel names.
4. Configure these settings to edit the group profile:

   Authentication Server

   Select the authentication server to use for this Mobile VPN group. You can authenticate users with the internal XTM device database (Firebox-DB) or with a RADIUS, VASCO, SecurID, LDAP, or Active Directory server. Make sure that the method of authentication you choose is enabled.

   Passphrase

   Type a passphrase to encrypt the Mobile VPN profile (.wgx file) that you distribute to users in this group. The shared key can use only standard ASCII characters. If you use a certificate for authentication, this is the PIN for the certificate.

   Confirm

   Type the passphrase again.

   External IP address

   Type the primary external IP address to which Mobile VPN users in this group can connect.

   Backup IP address

Type a backup external IP address to which Mobile VPN users in this group can connect. This backup IP address is optional. If you add a backup IP address, make sure it is an IP address assigned to an XTM device external interface.

Session Timeout

Select the maximum time in minutes that a Mobile VPN session can be active.

Idle Timeout

Select the time in minutes before the XTM device closes an idle Mobile VPN session. The session and idle timeout values are the default timeout values if the authentication server does not have its own timeout values. If you use the XTM device as the authentication server, the timeouts for the Mobile VPN group are always ignored because you set timeouts for each XTM device user account.

The session and idle timeouts cannot be longer than the value in the **SA Life** field.
To set this value, in the **Mobile VPN with IPSec Settings** dialog box, click the **IPSec Tunnel** tab, and click **Advanced** for **Phase 1 Settings**. The default value is 8 hours.

5. Select the **IPSec Tunnel** tab.
The IPSec Tunnel page opens.

6. Configure these settings:

Use the passphrase of the end user profile as the pre-shared key

Select this option to use the passphrase of the end user profile as the pre-shared key for tunnel authentication. You must use the same shared key on the remote device. This shared key can use only standard ASCII characters.

Use a certificate

Select this option to use a certificate for tunnel authentication.
For more information, see *Use Certificates for Mobile VPN With IPSec Tunnel Authentication* on page 508.

CA IP address

If you use a certificate, type the IP address of the Management Server that has been configured as a certificate authority.

Timeout

If you use a certificate, type the time in seconds before the Mobile VPN with IPSec client stops an attempt to connect if there is no response from the certificate authority. We recommend you keep the default value.

Phase 1 Settings

Select the authentication and encryption methods for the VPN tunnel. These settings must be the same for both VPN endpoints. To configure advanced settings, such as NAT Traversal or the key group, click **Advanced**, and see *Define Advanced Phase 1 Settings* on page 611.

The Encryption options are listed from the most simple and least secure, to the most complex and most secure:

DES

3DES

AES (128 bit)

AES (192 bit)

AES (256 bit)

Phase 2 Settings

Select PFS (Perfect Forward Secrecy) to enable PFS and set the Diffie-Hellman group.

To change other proposal settings, click **Advanced** and see *Define Advanced Phase 2 Settings* on page 613.

7. Select the **Resources** tab.
The Resources page appears.

8. Configure these settings:

Allow All Traffic Through Tunnel

To send all Mobile VPN user Internet traffic through the VPN tunnel, select this check box.
If you select this check box, the Mobile VPN user Internet traffic is sent through the VPN. This is more secure, but network performance decreases.
If you do not select this check box, Mobile VPN user Internet traffic is sent directly to the Internet. This is less secure, but users can browse the Internet more quickly.

Allowed Resources list

This list includes the resources that users in the Mobile VPN authentication group can get access to on the network.

To add an IP address or a network IP address to the network resources list, select **Host IP** or **Network IP**, type the address, and click **Add**.

To delete the selected IP address or network IP address from the resources list, select a resource and click **Remove**.

Virtual IP Address Pool

This list includes the internal IP addresses that are used by Mobile VPN users over the tunnel. These addresses cannot be used by any network devices or other Mobile VPN group.

To add an IP address or a network IP address to the virtual IP address pool, select **Host IP** or **Network IP**, type the address, and click **Add**.

To remove it from the virtual IP address pool, select a host or network IP address and click **Remove**.

9. Select the **Advanced** tab.
   The Advanced page appears.

10. Configure the **Line Management** settings:

    Connection mode

    Manual — In this mode, the client does not try to restart the VPN tunnel automatically if the VPN tunnel goes down. This is the default setting.

    To restart the VPN tunnel, you must click the **Connect** button in Connection Monitor, or right-click the Mobile VPN icon on your Windows desktop toolbar and click **Connect**.

    Automatic — In this mode, the client tries to start the connection when your computer sends traffic to a destination that you can reach through the VPN. The client also tries to restart the VPN tunnel automatically if the VPN tunnel becomes unavailable.

    Variable — In this mode, the client tries to restart the VPN tunnel automatically until you click **Disconnect**. After you disconnect, the client does not try to restart the VPN tunnel again until you click **Connect**.

    Inactivity timeout

If the **Connection Mode** is set to **Automatic** or **Variable**, the Mobile VPN with IPSec client software does not try to renegotiate the VPN connection until there has not been traffic from the network resources available through the tunnel for the length of time you enter for Inactivity timeout.

Note *The default Line Management settings are **Manual** and **0 seconds**. If you change either setting, you must use the .ini file to configure the client software.*

11. Click **Save**.
    The Mobile VPN with IPSec page opens and the new IPSec group appears in the Groups list.
12. Click **Save**.

Users that are members of the group you create are not able to connect until they import the correct configuration file in their Mobile VPN with IPSec client software. You must generate the configuration file and then provide it to the end users.

To generate the end user profiles for the group you edited:

1. Select **VPN > Mobile VPN with IPSec**.
   The Mobile VPN with IPSec page appears.
2. Click **Generate**.

Note *Fireware XTM Web UI can only generate the .ini mobile user configuration file. If you want to generate the .wgx file, you must use Policy Manager.*

Configure the External Authentication Server

If you create a Mobile VPN user group that authenticates to a third-party server, make sure you create a group on the server that has the same name as the name you added in the wizard for the Mobile VPN group.

If you use Active Directory as your authentication server, the users must belong to an Active Directory *security group* with the same name as the group name you configure for Mobile VPN with IPSec.

For RADIUS, VASCO, or SecurID, make sure that the RADIUS server sends a *Filter-Id* attribute (RADIUS attribute 11) when a user successfully authenticates, to tell the XTM device what group the user belongs to. The value for the *Filter-Id* attribute must match the name of the Mobile VPN group as it appears in the Fireware XTM RADIUS authentication server settings. All Mobile VPN users that authenticate to the server must belong to this group.

Add Users to a Firebox Mobile VPN Group

To open a Mobile VPN tunnel with the XTM device, remote users type their user name and password to authenticate. WatchGuard System Manager software uses this information to authenticate the user to the XTM device. To authenticate, users must be part of a Mobile VPN with IPSec group.

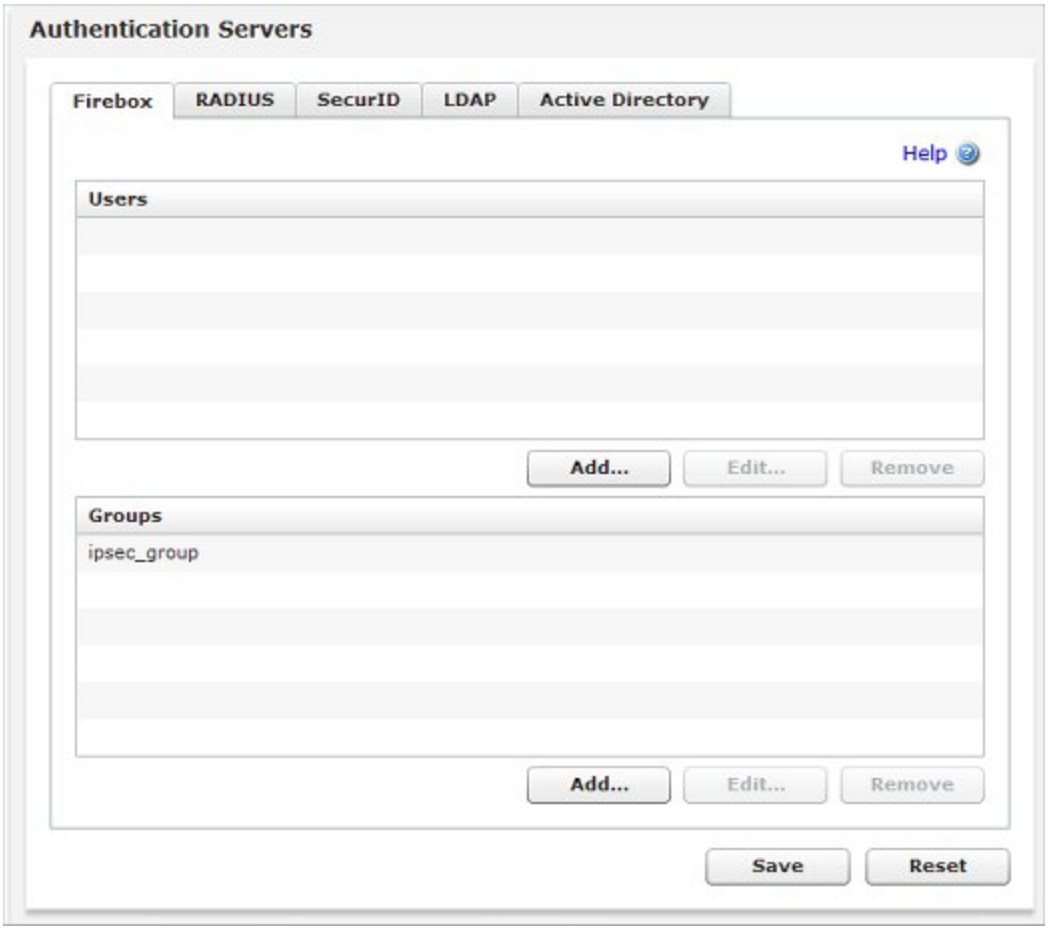
For information about how to create a Mobile VPN with IPSec group, see *Configure the XTM Device for Mobile VPN with IPSec*.

For more information on XTM device groups, see *Types of Firebox Authentication* on page 254.

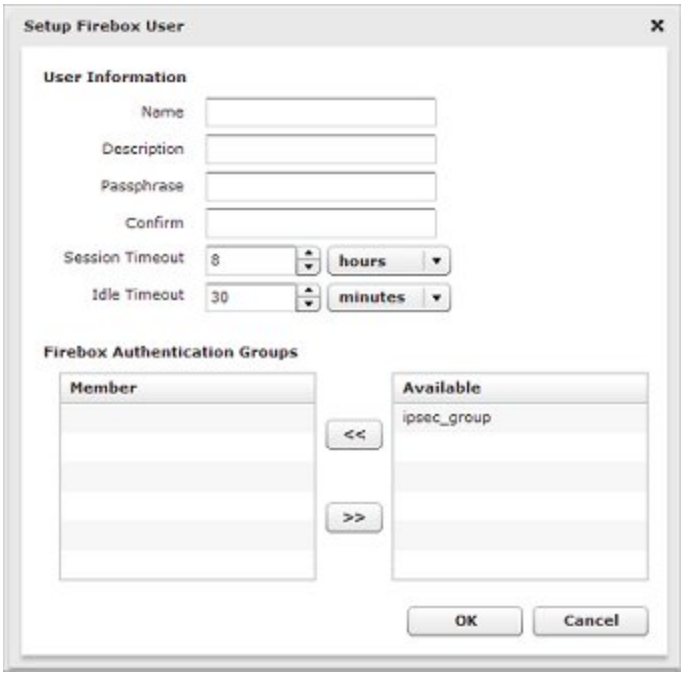
To add users to a group if you use a third-party authentication server, use the instructions provided in your vendor documentation.

To add users to a group if you use Firebox authentication:

1. Select **Authentication > Servers**.
   The Authentication Servers page appears.



2. Select the **Firebox** tab.
3. To add a new user, in the **Users** section, click **Add**.
   The Setup Firebox User dialog box appears.



4. Type a **Name** and **Passphrase** for the new user. The passphrase must be at least 8 characters long. Type the passphrase again to confirm it.
   The description is not required. We recommend that you do not change the values for Session Timeout and Idle Timeout.
5. In the **Firebox Authentication Groups** section, in the **Available** list, select the group name and click <<.
6. Click **OK**.
   The Setup Firebox User dialog box closes. The new user appears on the Authentication Servers page in the Users list.
7. Click **Save**.

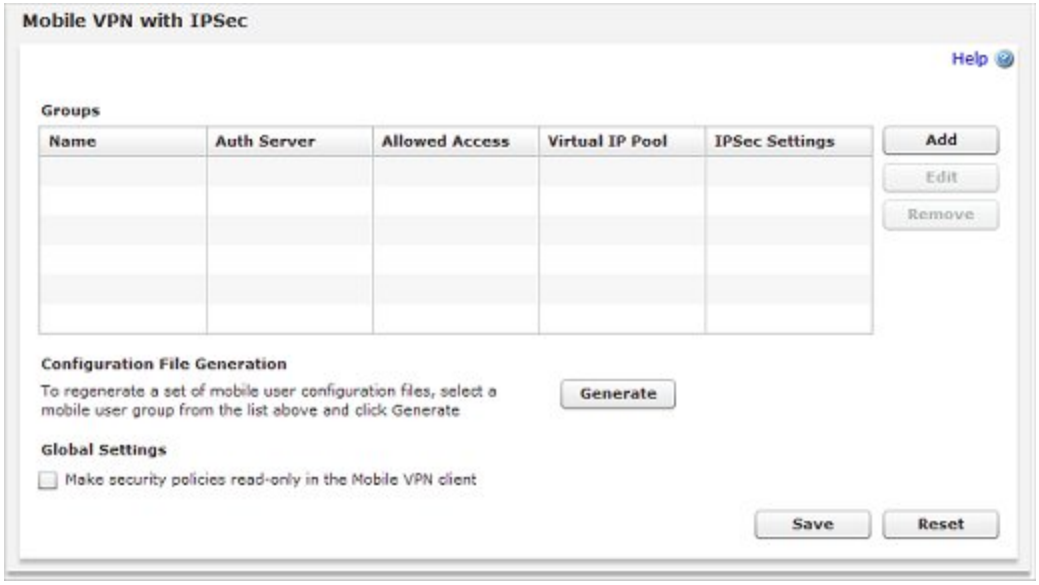
Modify an Existing Mobile VPN with IPSec Group Profile

After you create a Mobile VPN with IPSec group, you can edit the profile to:

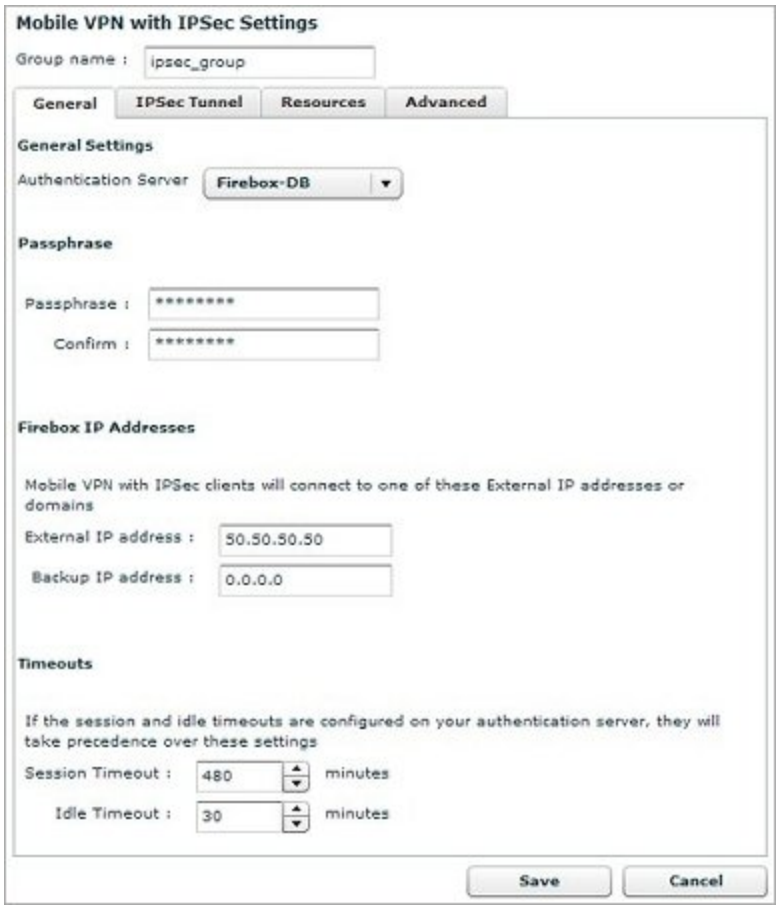
- Change the shared key
- Add access to more hosts or networks
- Restrict access to a single destination port, source port, or protocol
- Change the Phase 1 or Phase 2 settings

Configure a Mobile VPN with IPSec Group

1. Select **VPN > Mobile VPN with IPSec**.
   The Mobile VPN with IPSec page appears.



2. Select the group you want to edit and click **Edit**.
   The Mobile User VPN with IPSec Settings page appears.



3. Configure these options to edit the group profile:

   Authentication Server

Select the authentication server to use for this Mobile VPN group. You can authenticate users to the XTM device (Firebox-DB) or to a RADIUS, VASCO, SecurID, LDAP, or Active Directory server. Make sure that this method of authentication is enabled.

Passphrase

To change the passphrase that encrypts the .wgx file, type a new passphrase. The shared key can use only standard ASCII characters. If you use a certificate for authentication, this is the PIN for the certificate.

Confirm

Type the new passphrase again.

Primary

Type the primary external IP address or domain to which Mobile VPN users in this group can connect.

Backup

Type a backup external IP address or domain to which Mobile VPN users in this group can connect. This backup IP address is optional. If you add a backup IP address, make sure it is an IP address assigned to a XTM device external interface.

Session Timeout

Select the maximum time in minutes that a Mobile VPN session can be active.

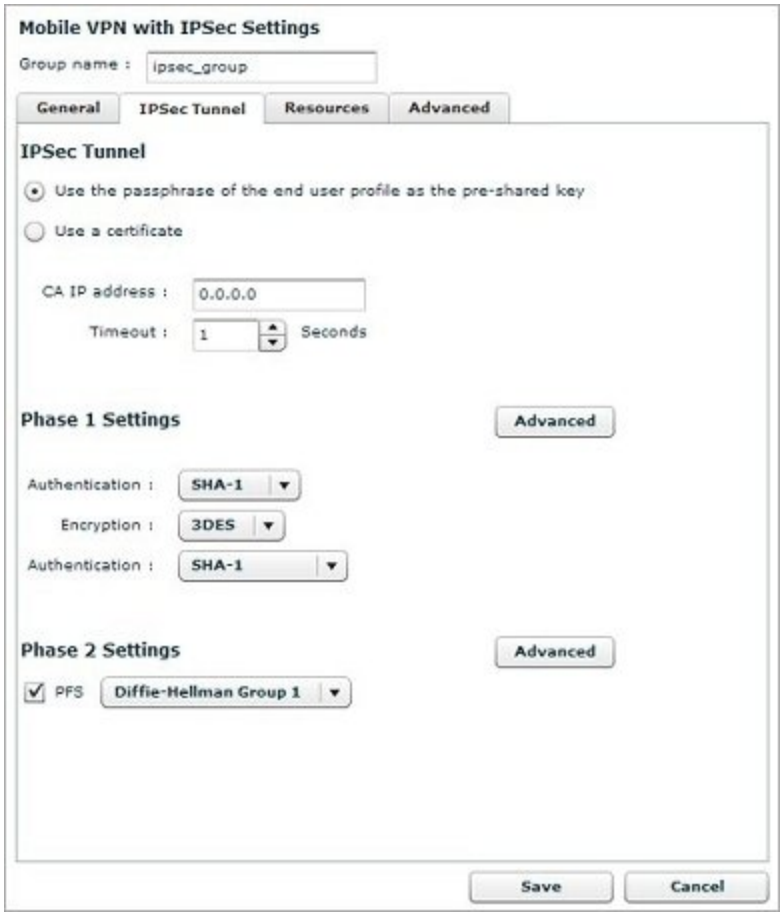
Idle Timeout

Select the time in minutes before the XTM device closes an idle Mobile VPN session. The session and idle timeout values are the default timeouts if the authentication server does not return specific timeout values. If you use the XTM device as the authentication server, the timeouts for the Mobile VPN group are always ignored because you set timeouts in each XTM device user account.

The session and idle timeouts cannot be longer than the value in the **SA Life** text box.

To set this value, in the **Mobile VPN with IPSec Settings** dialog box, select the **IPSec Tunnel** tab. In the **Phase 1 Settings** section, click **Advanced**. The default value is 8 hours.

4. Select the **IPSec Tunnel** tab.



5. Configure these options to edit the IPSec settings:

Use the passphrase of the end-user profile as the pre-shared key

Select this setting to use the passphrase of the end-user profile as the pre-shared key for tunnel authentication. The passphrase is set on the **General** tab in the **Passphrase** section. You must use the same shared key on the remote device, and this shared key can use only standard ASCII characters.

Use a certificate

Select this option to use a certificate for tunnel authentication.
For more information, see *Use Certificates for Mobile VPN With IPSec Tunnel Authentication* on page 508.

CA IP address

If you select to use a certificate, type the IP address of the Management Server that has been configured as a certificate authority.

Timeout

If you select to use a certificate, type the time in seconds before the Mobile VPN with IPSec client no longer attempts to connect to the certificate authority without a response. We recommend that you use the default setting.

Phase 1 Settings

Select the authentication and encryption methods for the Mobile VPN tunnel.

To configure advanced settings, such as NAT Traversal or the key group, click **Advanced**, and *Define Advanced Phase 1 Settings*.

These Encryption options appear in the list from the most simple and least secure, to the most complex and most secure.

DES

3DES

AES (128 bit)

AES (192 bit)

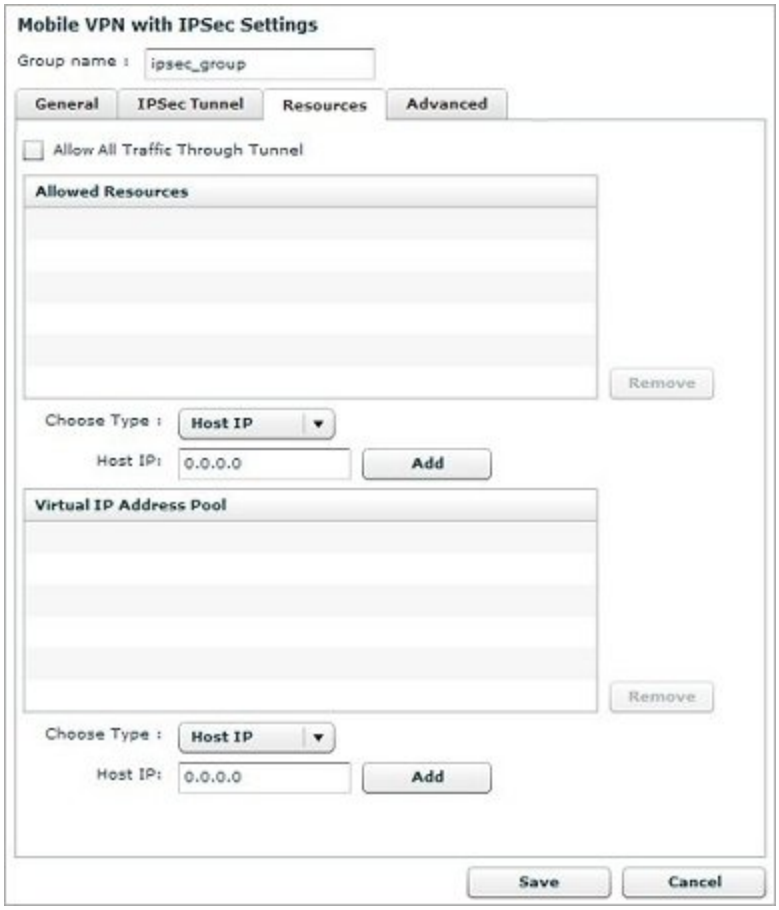
AES (256 bit)

Phase 2 Settings

Select PFS (Perfect Forward Secrecy) to enable PFS and set the Diffie-Hellman group.

To change other proposal settings, click **Advanced**, and Define advanced Phase 2 settings.

6. Select the **Resources** tab.



7. Configure these options:

   Allow All Traffic Through Tunnel

   To send all Mobile VPN user Internet traffic through the VPN tunnel, select this check box.
   If you select this check box, the Mobile VPN user Internet traffic is sent through the VPN. This is more secure, but web site access can be slow.
   If you do not select this check box, Mobile VPN user Internet traffic is sent directly to the Internet. This is less secure, but users can browse the Internet more quickly.

   Allowed Resources list

   This list includes the network resources that are available to users in the Mobile VPN group.

   To add an IP address or a network IP address to the network resources list, select **Host IP** or **Network IP**, type the address, and click **Add**.

   To delete an IP address or network IP address from the resources list, select a resource and click **Remove**.

   Virtual IP Address Pool

   The internal IP addresses that are used by Mobile VPN users over the tunnel appear in this list. These addresses cannot be used by any network devices or other Mobile VPN group.

   To add an IP address or a network IP address to the virtual IP address pool, select **Host IP** or **Network IP**, type the address, and click **Add**.

   To delete a host or network IP address from the virtual IP address pool, select the host or IP address and click **Remove**.

8. Select the **Advanced** tab.

9. Configure the **Line Management** settings:

   Connection mode

   Manual — In this mode, the client does not try to restart the VPN tunnel automatically if the VPN tunnel goes down. This is the default setting.

   To restart the VPN tunnel, you must click **Connect** in Connection Monitor, or right-click the Mobile VPN icon on your Windows desktop toolbar and select **Connect**.

   Automatic — In this mode, the client tries to start the connection when your computer sends traffic to a destination that you can reach through the VPN. The client also tries to restart the VPN tunnel automatically if the VPN tunnel becomes unavailable.

   Variable — In this mode, the client tries to restart the VPN tunnel automatically until you click **Disconnect**. After you disconnect, the client does not try to restart the VPN tunnel again until after the next time you click **Connect**.

   Inactivity timeout

   If you set the **Connection Mode** to **Automatic** or **Variable**, the Mobile VPN with IPSec client software does not try to renegotiate the VPN connection for the duration you specify.

   Note *The default Line Management settings are **Manual** and **0 seconds**. If you change either setting, you must use the .ini file to configure the client software.*

10. Click **Save**.
    The Mobile VPN with IPSec page appears.

11. Click **Save**.

End users that are members of the group you edit are not able to connect until they import the correct configuration file in their Mobile VPN with IPSec client software. You must generate the configuration file and then provide it to the end users.

To generate the end user profiles for the group you edited:

1. Select **VPN > Mobile VPN with IPSec**.
   The Mobile VPN with IPSec page appears.
2. Click **Generate**.

> ***Note*** *Fireware XTM Web UI can only generate the .ini mobile user configuration file. If you want to generate the .wgx file, you must use Policy Manager.*

Define Advanced Phase 1 Settings

You can define the advanced Phase 1 settings for your Mobile VPN user profile.

1. On the **Edit Mobile VPN with IPSec** page, select the **IPSec Tunnel** tab.
2. In the **Phase 1 Settings** section, click **Advanced**.
   The Phase1 Advanced Settings appear.

3. Configure the setting options for the group, as described in the subsequent sections.
   We recommend you use the default settings.

4. Click **Save**.

Phase 1 Options

SA Life

Select a SA (security association) lifetime duration and select **Hour** or **Minute** in the drop-down list. When the SA expires, a new Phase 1 negotiation starts. A shorter SA life is more secure but the SA negotiation can cause existing connections to fail.

Key Group

Select a Diffie-Hellman group. WatchGuard supports groups 1, 2, and 5.
Diffie-Hellman groups determine the strength of the master key used in the key exchange process. Higher group numbers are more secure, but use more time and resources on the client computer, and the XTM device is required to make the keys.

NAT Traversal

Select this check box to build a Mobile VPN tunnel between the XTM device and another device that is behind a NAT device. NAT Traversal, or UDP Encapsulation, allows traffic to route to the correct destinations.

IKE Keep-alive

Select this check box only if this group connects to an older Firebox that does not support Dead Peer Detection. All Firebox devices with Fireware v9.x or lower, Edge v8.x or lower, and all versions of WFS do not support Dead Peer Detection. For these devices, select this check box to enable the Firebox to send messages to its IKE peer to keep the VPN tunnel open. Do not select both IKE Keep-alive and Dead Peer Detection.

Message interval

Select the number of seconds for the IKE keep-alive message interval.

Max failures

Set the maximum number of times the XTM device waits for a response to the IKE keep-alive messages before it terminates the VPN connection and starts a new Phase 1 negotiation.

Dead Peer Detection

Select this check box to enable Dead Peer Detection (DPD). Both endpoints must support DPD. All Firebox or XTM devices with Fireware v10.x or higher and Edge v10.x or higher support DPD. Do not select both IKE Keep-alive and Dead Peer Detection.

DPD is based on RFC 3706 and uses IPSec traffic patterns to determine if a connection is available before a packet is sent. When you select DPD, a message is sent to the peer when no traffic has been received from the peer within the selected time period. If DPD determines a peer is unavailable, additional connection attempts are not made.

Traffic Idle Timeout

Set the number of seconds the XTM device waits before it checks to see if the other device is active.

Max retries

Set the maximum number of times the XTM device tries to connect before it determines the peer is unavailable, terminates the VPN connection, and starts a new Phase 1 negotiation.

Define Advanced Phase 2 Settings

You can define the advanced Phase 2 settings for your Mobile VPN user profile.

1. On the **Edit Mobile VPN with IPSec** page, click the **IPSec Tunnel** tab.
2. In the **Phase 2 Settings**section, click **Advanced**.
   The Phase 2 Advanced Settings appear.

3. Configure the Phase 2 options as described in the subsequent section.
   We recommend that you use the default settings.
4. Click **Save**.

Phase 2 Options

Type

The two proposal method options are **ESP** or **AH**. Only **ESP** is supported at this time.

Authentication

Select the authentication method: **SHA1** or **MD5**.

Encryption

Select an encryption method. The options are listed from the most simple and least secure, to the most complex and most secure.

- DES
- 3DES
- AES (128-bit)
- AES (192-bit)
- AES (256-bit)

Force Key Expiration

To regenerate the gateway endpoints and exchange new keys after the specified amount of time or amount of traffic passes through the gateway, select this check box.

In the **Force Key Expiration** fields, select the amount of time and number of kilobytes that can pass before the key expires.

If you disabled **Force Key Expiration**, or if you enabled it and both the time and number of kilobytes are set to zero, the XTM device uses the key expiration time set for the peer. If this is also disabled or set to zero, the XTM device uses the default key expiration time of 8 hours. The maximum amount of time that can pass before a key can expire is one year.

Configure WINS and DNS Servers

Mobile VPN clients rely on shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. DNS translates host names into IP addresses. WINS resolves NetBIOS names to IP addresses. These servers must be accessible from the XTM device trusted interface.

Make sure you use only an internal DNS server. Do not use external DNS servers.

1. Select **Network > Interfaces**.
   The Network Interfaces page appears.

2. In the **Domain Name** text box, type a domain name for the DNS server.
3. In the **DNS Servers** and **WINS Servers** text boxes, type the addresses for the WINS and DNS servers.
4. Click **Save**.

Lock Down an End User Profile

You can use the global settings to lock down the end user profile so that users can see some settings but not change them, and hide other settings so that users cannot change them. We recommend that you lock down all profiles so that users cannot make changes to their profiles. This setting is for .wgx end user profile files. You cannot make .ini end user profile files read-only.

1. Select **VPN > Mobile VPN with IPSec**.
2. To give mobile users read-only access to their profiles, select the **Make security policies read-only in the Mobile VPN client** check box.

Note *This setting only applies to .wgx files. You must use Policy Manager to generate .wgx files for your users.*

Mobile VPN with IPSec Configuration Files

To configure the Mobile VPN with IPSec client, you import a configuration file. The configuration file is also called the end user profile. There are two types of configuration files.

.wgx

.wgx files are encrypted and can be configured so that the end user cannot change settings in the Mobile VPN with IPsec client software. A .wgx file cannot set the Line Management settings in the client software. If you set Line Management to anything other than **Manual**, you must use a .ini configuration file.

For more information, see Lock down an end user profile.

.ini

The .ini file is used only if you did not set Line Management to **Manual**. The .ini configuration file is not encrypted.

For more information, see Line Management on the Advanced tab in Modify an existing Mobile VPN with IPSec group profile.

When you first configure a Mobile VPN with IPSec group, or if you make a change to the settings for a group, you must generate the configuration file for the group and provide it to end-users.

To use Fireware XTM Web UI to generate an end-user profile file for a group:

1. Select **VPN > Mobile VPN > IPSec**.
2. Select the Mobile VPN group and click **Generate.**
3. Select a location to save the .ini configuration file.

You can now distribute the configuration file to the end-users.

> ***Note*** *Fireware XTM Web UI can only generate the .ini mobile user configuration file. If you want to generate the .wgx file, you must use Policy Manager.*

Configure Policies to Filter Mobile VPN Traffic

In a default configuration, Mobile VPN with IPSec users have full access to XTM device resources with the *Any* policy. The *Any* policy allows traffic on all ports and protocols between the Mobile VPN user and the network resources available through the Mobile VPN tunnel. To restrict VPN user traffic by port and protocol, you can delete the *Any* policy and replace it with policies that restrict access.

Add an Individual Policy

1. Select **Firewall > Mobile VPN Policies**.
2. You must select a group before you add a policy.
3. Add, edit, and delete policies as described in *About Policies* on page 287.

Distribute the Software and Profiles

WatchGuard recommends that you distribute end-user profiles by encrypted email or another secure method. Each client computer must have:

- **Software installation package**

  The **WatchGuard Mobile VPN with IPSec** installation package is located on the WatchGuard LiveSecurity Service web site at https://www.watchguard.com/archive/softwarecenter.asp
  To download software, you must log in to the site with your LiveSecurity Service user name and password.

- **The end-user profile**

  This file contains the group name, shared key, and settings that enable a remote computer to connect securely over the Internet to a protected, private computer network. The end-user profile has the file name **groupname.wgx**. The default location of the .wgx file is:
  `C:\Documents and Settings\All Users\Shared WatchGuard \mobilevpn\<IP address of XTM device>\<Mobile VPN with IPSec group name\wgx`

- **Two certificate files, if you are authenticating with certificates**

  These are the .p12 file, which is an encrypted file containing the certificate, and cacert.pem, which contains the root (CA) certificate. The .p12 and cacert.pem files can be found in the same location as the .wgx end-user profile.

- **User documentation**

  Documentation to help the remote user install the Mobile VPN client and import the Mobile VPN configuration file can be found in the *About Mobile VPN Client Configuration Files* topics.

- **Passphrase**

  To import the end-user profile, the user must type a passphrase. This key decrypts the file and imports the security policy into the Mobile VPN client. The passphrase is set when the Mobile VPN group is created in Policy Manager.

  For information about how to change the shared key, see *Modify an Existing Mobile VPN with IPSec Group Profile* on page 604.

> ***Note*** *The end-user profile passphrase, user name, and user password are sensitive information. For security reasons, we recommend that you do not provide this information by email. Because email is not secure, an unauthorized user can use the information to get access to your internal network. Give the user the information to the use by a method that does not allow an unauthorized person to intercept it.*

Additional Mobile VPN Topics

This section describes special topics for Mobile VPN with IPSec.

Making Outbound IPSec Connections from Behind an XTM Device

A user might have to make IPSec connections to an XTM device from behind another XTM device. For example, if a mobile employee travels to a customer site that has a XTM device, that user can make IPSec connections to their network. For the local XTM device to correctly manage the outgoing IPSec connection, you must set up an IPSec policy that includes the IPSec packet filter.

For more information on how to enable policies, see *About Policies* on page 287.

Because the IPSec policy enables a tunnel to the IPSec server and does not complete any security checks at the firewall, add only the users that you trust to this policy.

Terminate IPSec Connections

To fully stop VPN connections, the XTM device must be restarted. Current connections do not stop when you remove the IPSec policy.

Global VPN Settings

Global VPN settings on your XTM device apply to all manual BOVPN tunnels, managed tunnels, and Mobile VPN tunnels. You can use these settings to:

- Enable IPSec pass-through.
- Clear or maintain the settings of packets with Type of Service (TOS) flags set.
- Use an LDAP server to verify certificates.

To change these settings, from Fireware XTM Web UI, select **VPN > Global Settings**. For more information on these settings, see *About Global VPN Settings* on page 549.

See the Number of Mobile VPN Licenses

From Fireware XTM Web UI, you can see the number of Mobile VPN licenses that are available with the feature key.

1. Select **System > Feature Key**.
   The Feature Key page appears.
2. Scroll down to **Mobile VPN Users** in the **Feature** column, and find the number in the **Value** column. This is the maximum number of Mobile VPN users that can connect at the same time.

Purchase Additional Mobile VPN Licenses

WatchGuard Mobile VPN with IPSec is an optional feature. Each XTM device includes a number of Mobile VPN licenses. You can purchase more licenses for Mobile VPN.

Licenses are available through your local reseller, or on the WatchGuard web site:
http://www.watchguard.com/sales

Add Feature Keys

For more information on how to add feature keys, see *About Feature Keys* on page 50.

Mobile VPN and VPN Failover

You can configure VPN tunnels to fail over to a backup endpoint if the primary endpoint becomes unavailable. For more information on VPN failover, see *Configure VPN Failover* on page 568.

If VPN failover is configured and failover occurs, Mobile VPN sessions do not continue. You must authenticate your Mobile VPN client again to make a new Mobile VPN tunnel.

From Fireware XTM Web UI, you can configure VPN failover for Mobile VPN tunnels.

1. Select **VPN > Mobile VPN with IPSec**.
   The Mobile VPN with IPSec Settings page appears.
2. Select a mobile user group from the list and click **Edit**.
   The Edit Mobile VPN with IPSec dialog box appears.
3. Select the **General** tab.
4. In the **Firebox IP Addresses** section, type a backup WAN interface IP address in the **Backup IP address** text box.
   You can specify only one backup interface for tunnels to fail over to, even if you have additional WAN interfaces.

Configure Mobile VPN with IPSec to a Dynamic IP Address

We recommend that you use either a static IP address for a XTM device that is a VPN endpoint, or use Dynamic DNS. For more information about Dynamic DNS, see *About the Dynamic DNS Service* on page 89.

If neither of these options are possible, and the external IP address of the XTM device changes, you must either give remote IPSec users a new .wgx configuration file or have them edit the client configuration to include the new IP address each time that the IP address changes. Otherwise, IPSec users cannot connect until they get the new configuration file or IP address.

Use these instructions to configure the XTM device and support the IPSec client users if the XTM device has a dynamic IP address and you cannot use Dynamic DNS.

Keep a Record of the Current IP Address

From Fireware XTM Web UI, you can find the current IP address of the XTM device external interface.

1. Select **System Status > Interfaces**.
2. Look for the interface with the alias **External** and look at the IP address in the **IP** column. This is the external IP address of the XTM device.

This is the IP address that is saved to the .wgx configuration files. When remote users say that they cannot connect, check the external IP address of the XTM device to see if the IP address has changed.

Configure the XTM Device and IPSec Client Computers

The XTM device must have an IP address assigned to the external interface before you download the .wgx files. This is the only difference from the normal configuration of the XTM device and IPSec client computers.

Update the Client Configurations when the Address Changes

When the external IP address of the XTM device changes, the remote Mobile VPN with IPSec client computers cannot connect until they have been configured with the new IP address. You can change the IP address in two ways.

- Give remote users a new .wgx configuration file to import.
- Have remote users manually edit the IPSec client configuration. For this option, you must configure the XTM device so remote users can edit the configuration. For more information, see *Lock Down an End User Profile* on page 615.

From Fireware XTM Web UI, you can give users a new .wgx configuration file.

1. Select **VPN > Mobile VPN with IPSec**.
2. Select a Mobile VPN user group and click **Generate** to generate and download the .wgx files.
3. Distribute the .wgx files to the remote users.
4. Tell the remote users to *Import the End-User Profile*.

To have users manually edit the client configuration:

1. Give remote users the new external IP address of the XTM device and tell them to perform the next five steps.
2. On the IPSec client computer, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor.**
3. Select **Configuration > Profile Settings**.
4. Select the profile and click **Configure**.
5. In the left column, select **IPSec General Settings**.
6. In the **Gateway** text box, type the new external IP address of the XTM device.

About the Mobile VPN with IPSec Client

The WatchGuard Mobile VPN with IPSec client is installed on a mobile client computer, whether the user travels or works from home. The user connects with a standard Internet connection and activates the Mobile VPN client to get access to protected network resources.

The Mobile VPN client creates an encrypted tunnel to your trusted and optional networks, which are protected by a XTM device. The Mobile VPN client allows you to supply remote access to your internal networks and not compromise your security.

Client Requirements

Before you install the client, make sure you understand these requirements and recommendations.

You must configure your XTM device to work with Mobile VPN with IPSec. If you have not, see the topics that describe how to configure your XTM device to use Mobile VPN.

- You can install the Mobile VPN with IPSec client software on any computer with Windows 2000, Windows XP (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), or Windows 7 (32 bit and 64 bit). Before you install the client software, make sure the remote computer does not have any other IPSec VPN client software installed. You must also uninstall any desktop firewall software (other than Microsoft firewall software) from each remote computer.
- If the client computer uses Windows XP, you must log on using an account that has administrator rights to install the Mobile VPN client software and to import the .wgx or .ini configuration file. Administrator rights are not required to connect after the client has been installed and configured.
- If the client computer uses Windows Vista, you must log on using an account that has administrator rights to install the Mobile VPN client software. Administrator rights are not required to import a .wgx or .ini file or to connect after the client has been installed.
- We recommend that you check to make sure all available service packs are installed before you install the Mobile VPN client software.
- WINS and DNS settings for the Mobile VPN client are obtained in the client profile you import when you set up your Mobile VPN client.
- We recommend that you do not change the configuration of any Mobile VPN client setting not explicitly described in this documentation.

Install the Mobile VPN with IPSec Client Software

The installation process consists of two parts: install the client software on the remote computer, and import the end-user profile into the client. Before you start the installation, make sure you have the following installation components:

- The Mobile VPN installation file
- An end-user profile, with a file extension of .wgx or .ini
- Passphrase
- A cacert.pem and a .p12 file (if you use certificates to authenticate)
- User name and password

> ***Note*** *Write the passphrase down and keep it in a secure location. You must use it during the final steps of the installation procedure.*

To install the client:

1. Copy the Mobile VPN installation file to the remote computer and extract the contents of the file.
2. Copy the end user profile (the .wgx or .ini file) to the root directory on the remote (client or user) computer. Do not run the installation software from a CD or other external drive.
   If you use certificates to authenticate, copy the cacert.pem and .p12 files to the root directory.
3. Double-click the .exe file you extracted in Step 1. This starts the WatchGuard Mobile VPN Installation wizard. You must restart your computer when the installation wizard completes.

For detailed instructions written for Mobile VPN with IPSec client end-users, see *End-User Instructions for WatchGuard Mobile VPN with IPSec Client Installation* on page 635.

Import the End-User Profile

When the computer restarts, the WatchGuard Mobile VPN Connection Monitor dialog box appears. When the software starts for the first time after you install it, you see this message:

```
There is no profile for the VPN dial-up!
Do you want to use the configuration wizard for creating a profile now?
```

Click **No**.

To turn off the Connection Monitor auto-start functionality, select **View > AutoStart > No Autostart**.

To import a Mobile VPN configuration .wgx or .ini file:

1. From your Windows desktop, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor**.
2. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Profile Import**.
   The Profile Import Wizard starts.
3. On the **Select User Profile** screen, browse to the location of the .wgx or .ini configuration file.
4. Click **Next**.
5. If you use a .wgx file, on the **Decrypt User Profile** screen, type the passphrase. The passphrase is case-sensitive.
6. Click **Next**.
7. On the **Overwrite or add Profile** screen, you can select to overwrite a profile of the same name. This is useful if your network administrator gives you a new .wgx file to import.
8. Click **Next**.
9. On the **Authentication** screen, you can select whether to type the user name and password that you use to authenticate the VPN tunnel.
   If you keep these fields empty, you are prompted to enter your user name and password each time you connect.
   If you type your user name and password, the XTM device stores them and you do not have to enter this information each time you connect. However, this is a security risk. You can also type just your user name and keep the **Password** text box empty.
10. Click **Next**.
11. Click **Finish**.
    The computer is now ready to use Mobile VPN with IPSec.

Select a Certificate and Enter the PIN

If you use certificates for authentication, you must add the correct certificate and then configure the Mobile VPN connection profile to use that certificate.

Add the Certificate

To add the certificate to the Mobile VPN client configuration, you must have a cacert.pem and a .p12 file.

1. Select **Configuration > Certificates**.
2. Click **Add**.
3. On the **User Certificate** tab, select **from PKS#12 file** from the **Certificate** drop-down list.
4. Adjacent to the **PKS#12 Filename** text box, click the button and browse to the location of the .p12 file.
5. Click **OK**.
6. Click **Close**.

Select the Certificate for the Mobile VPN profile

After you add the certificate, you must select the correct certificate set for the connection profile.

1. Select **Configuration > Profiles**.
2. Select the profile name. Click **Edit**.
3. Click **Identities**.
4. From the **Certificate configuration** drop-down box, select the certificate configuration you added.
5. Select **Connection > Enter PIN**.
6. Type the passphrase and click **OK**.

Uninstall the Mobile VPN Client

It can become necessary to uninstall the Mobile VPN client. We recommend that you use the Windows **Add/Remove Programs** tool to uninstall the Mobile VPN client. After the Mobile VPN client software is installed the first time, it is not necessary to uninstall the Mobile VPN client software before you apply an upgrade to the client software.

Before you start, disconnect all tunnels and close the Mobile VPN Connection Monitor. From the Windows desktop:

1. Click **Start > Settings > Control Panel**.
   The Control Panel window appears.
2. Double-click the **Add/Remove** Programs icon.
   The Add/Remove Programs window appears.
3. Select **WatchGuard Mobile VPN** and click **Change/Remove**.
   The InstallShield Wizard window appears.
4. Click **Remove** and click **Next**.
   The Confirm File Deletion dialog box appears.
5. Click **OK** to completely remove all of the components. If you do not select this check box at the end of the uninstall, the next time you install the Mobile VPN software the connection settings from this installation are used for the new installation.

Connect and Disconnect the Mobile VPN Client

The WatchGuard Mobile VPN with IPSec client software makes a secure connection from a remote computer to your protected network over the Internet. To start this connection, you must connect to the Internet and use the Mobile VPN client to connect to the protected network.

Start your connection to the Internet through a Dial-Up Networking connection or LAN connection. Then, use the instructions below or select your profile, connect, and disconnect by right-clicking the Mobile VPN icon on your Windows toolbar.

1. From your Windows desktop, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor**.
2. From the **Profile** drop-down list, select the name of the profile you created for your Mobile VPN connections to the XTM device.

3. Click  to connect.

Disconnect the Mobile VPN Client

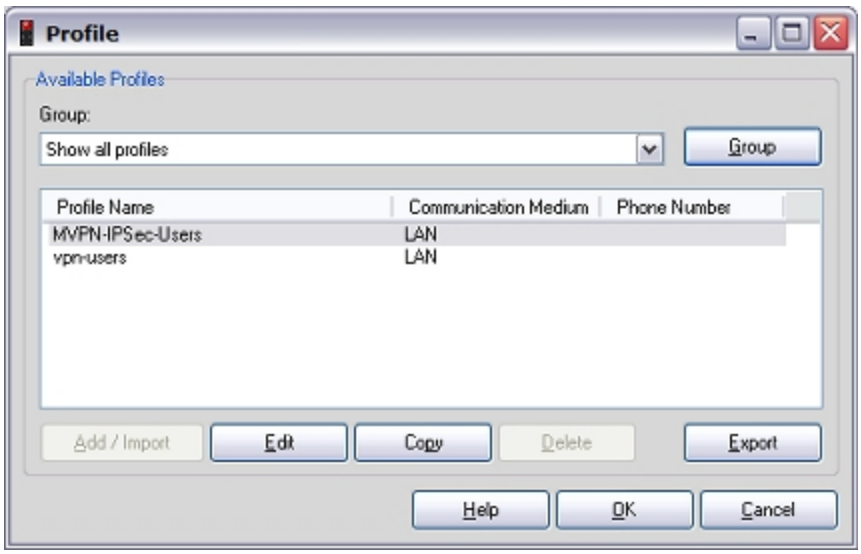
On the Mobile VPN Monitor dialog box, click  to disconnect.

Control Connection Behavior

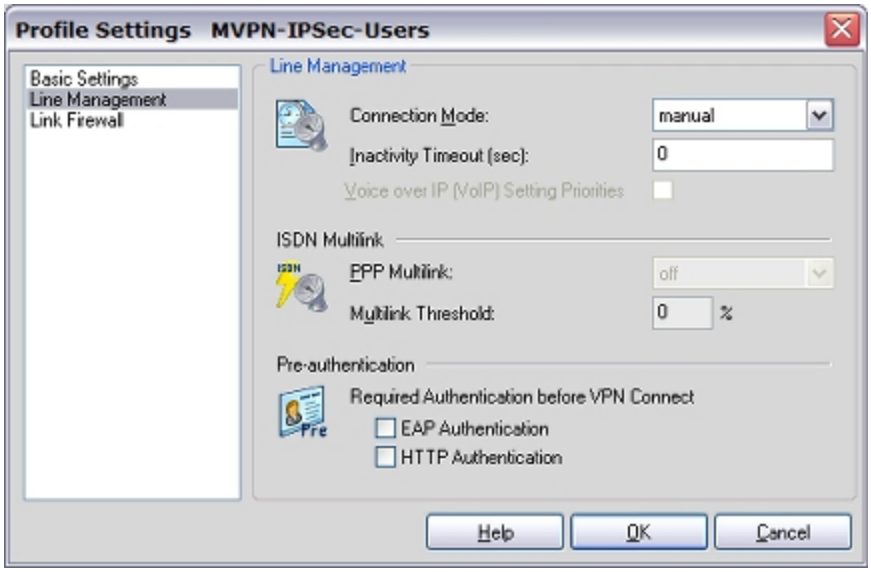
For each profile you import, you can control the action the Mobile VPN client software takes when the VPN tunnel becomes unavailable for any reason. You can configure these settings on the XTM device and use a .ini file to configure the client software. A .wgx file does not change these settings.

From the WatchGuard Mobile VPN Connection Monitor, you can manually set the behavior of the Mobile VPN client when the VPN tunnel becomes unavailable.

1. Select **Configuration > Profiles**.
2. Select the name of the profile and click **Edit**.



3. Select **Line Management**.



4. In the **Connection Mode** drop-down list, select a connection behavior for this profile.

   - **Manual** — When you select **manual** connection mode, the client does not try to restart the VPN tunnel automatically if the VPN tunnel goes down. To restart the VPN tunnel, you must click the **Connect** button in Connection Monitor, or right-click the Mobile VPN icon on your Windows desktop toolbar and click **Connect**.
   - **Automatic** — When you select **automatic** connection mode, the client tries to start the connection when your computer sends traffic to a destination that you can reach through the VPN. The client also tries to restart the VPN tunnel automatically if the VPN tunnel goes down.
   - **Variable** — When you select **variable** connection mode, the client tries to restart the VPN tunnel automatically until you click **Disconnect**. The client does not try to restart the VPN tunnel again until after the next time you click **Connect**.

5. Click **OK**.

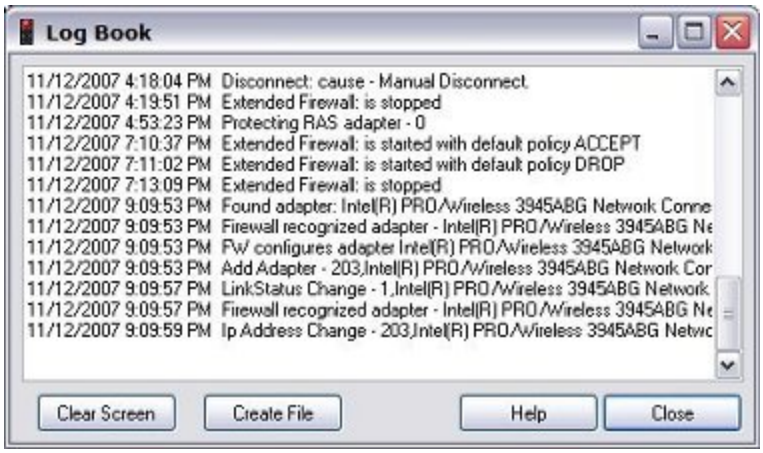
Mobile VPN With IPSec Client Icon

The Mobile VPN with IPSec client icon appears in the Windows desktop system tray to show the status of the desktop firewall, the link firewall, and the VPN network. You can right-click the icon to connect and disconnect your Mobile VPN and see which profile is in use.

See Mobile VPN Log Messages

You can use the Mobile VPN client log file to troubleshoot problems with the VPN client connection.

To see Mobile VPN log messages, select **Log > Logbook** from the Connection Monitor.
The Log Book dialog box appears.



Secure Your Computer with the Mobile VPN Firewall

The WatchGuard Mobile VPN with IPSec client includes two firewall components:

Link firewall

The link firewall is not enabled by default. When the link firewall is enabled, your computer discards any packets received from other computers. You can choose to enable the link firewall only when a Mobile VPN tunnel is active, or enable it all the time.

Desktop firewall

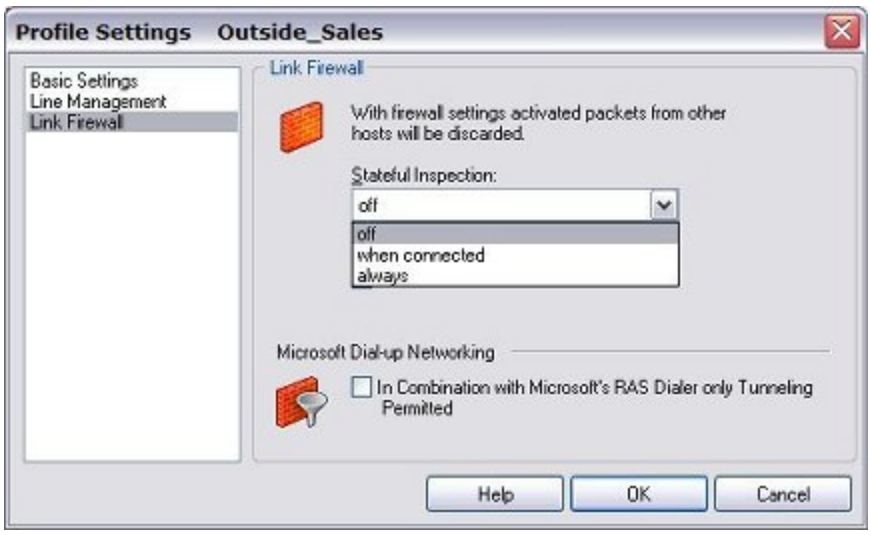
This full-featured firewall can control connections to and from your computer. You can define friendly networks and set access rules separately for friendly and unknown networks.

Enable the Link Firewall

When the link firewall is enabled, the Mobile VPN client software drops any packets sent to your computer from other hosts. It allows only packets sent to your computer in response to packets your computer sends. For example, if you send a request to an HTTP server through the tunnel from your computer, the reply traffic from the HTTP server is allowed. If a host tries to send an HTTP request to your computer through the tunnel, it is denied.

To enable the link firewall:

1. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Profiles**.
2. Select the profile you want to enable the link firewall for and select **Edit**.
3. From the left pane, select **Link Firewall**.



4. From the **Stateful Inspection** drop-down list, select **when connected** or **always**.

   If you select **when connected**, the link firewall operates only when the VPN tunnel is active for this profile.

   If you select **always**, the link firewall is always active, whether the VPN tunnel is active or not.
5. Click **OK**.

About the Desktop Firewall

When you enable a rule in your firewall configurations, you must specify what type of network the rule applies to. In the Mobile VPN client, there are three different types of networks:

VPN networks

Networks defined for the client in the client profile they import.

Unknown networks

Any network not specified in the firewall.

Friendly networks

Any network specified in the firewall as a known network.

For information about how to enable the desktop firewall, see *Enable the Desktop Firewall* on page 629.

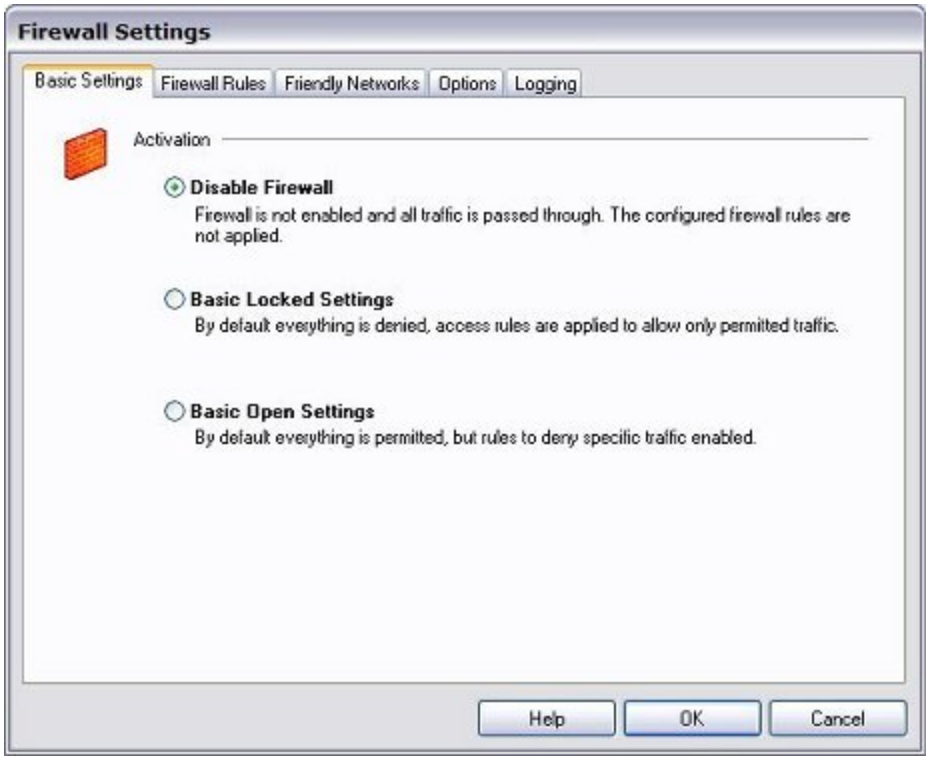
Enable the Desktop Firewall

To enable the full-featured desktop firewall:

1. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Firewall**.
   The firewall is disabled by default.
2. When you enable the firewall, you must choose between two firewall modes:

   - **Basic Locked Settings** — When you enable this mode, the firewall denies all connections to or from your computer unless you have created a rule to allow the connection.

- **Basic Open Settings** — When you enable this mode, the firewall allows all connections unless you have created a rule to deny the connection.



3. Click **OK**.

After you have enabled the desktop firewall, you can configure your firewall settings.

For more information about how to define friendly networks and create firewall rules, see *Define Friendly Networks* on page 630 and *Create Firewall Rules* on page 631.

Define Friendly Networks

You can generate a firewall rule set for specific known networks that you define. For example, if you want to use the Mobile VPN client on a local network where you want your computer available to other computers, you can add the network address of that LAN as a friendly network. This makes the firewall rules for that LAN different from the firewall rules you create for connections to the Internet and to remote VPN networks.

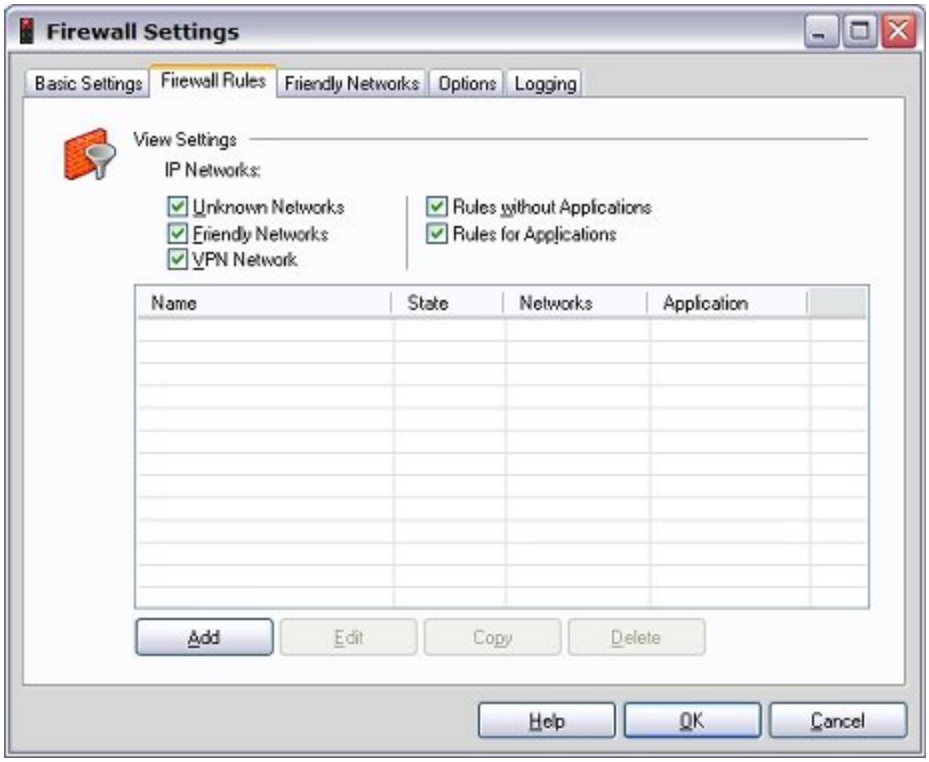
1. From the **Firewall Settings** dialog box, select the **Friendly Networks** tab.
2. Click **Add** to add a new friendly network.

The Automatic Friendly Network detection feature does not operate correctly in this release of the Mobile VPN with IPSec client software.

Create Firewall Rules

You can create exceptions to the firewall mode you set when you enabled the firewall on the **Firewall Rules** tab of the **Firewall Settings** dialog box. For example, if you selected **Basic Locked Settings** when you enabled the firewall, then the rules you create here allow traffic. If you selected **Basic Open Settings**, then the rules you create here deny traffic. Firewall rules can include multiple port numbers from a single protocol.

Select or clear the check boxes below **View Settings** to show or hide categories of firewall rules. Some options are not available in the Mobile VPN for Windows Mobile version of the desktop firewall.



To create a rule, click **Add**. Use the four tabs in the **Firewall Rule Entry** dialog box to define the traffic you want to control:

- *General Tab*
- *Local Tab*
- *Remote Tab*
- *Applications Tab*

General Tab

You can define the basic properties of your firewall rules on the **General** tab of the **Firewall Rule Entry** dialog box.

Rule Name

Type a descriptive name for this rule. For example, you might create a rule called "Web surfing" that includes traffic on TCP ports 80 (HTTP), 8080 (alternate HTTP), and 443 (HTTPS).

State

To make a rule inactive, select **Disabled**. New rules are enabled by default.

Direction

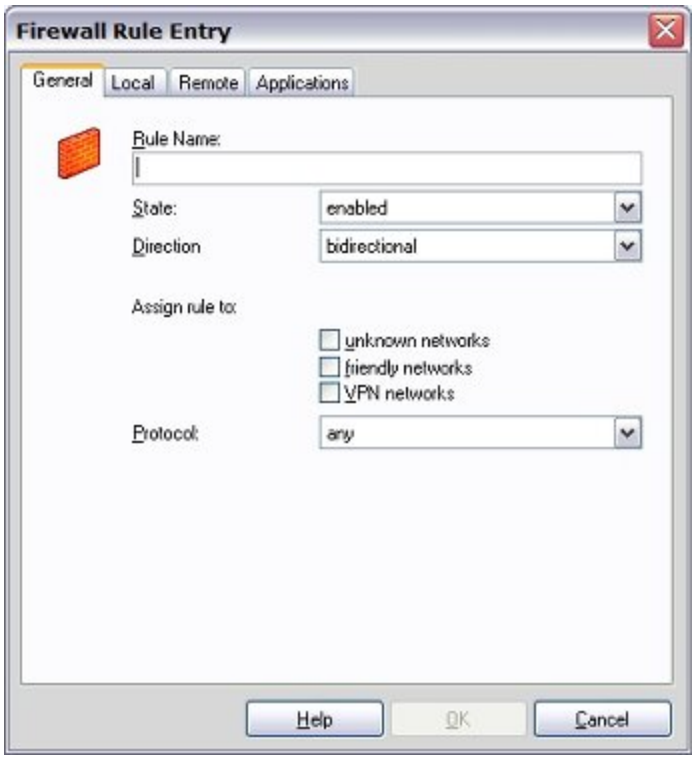
To apply the rule to traffic that comes from your computer, select **outgoing**. To apply the rule to traffic that is sent to your computer, select **incoming**. To apply the rule to all traffic, select **bidirectional**.

Assign rule to

Select the check boxes adjacent to the network types that this rule applies to.

Protocol

Use this drop-down list to select the type of network traffic you want to control.

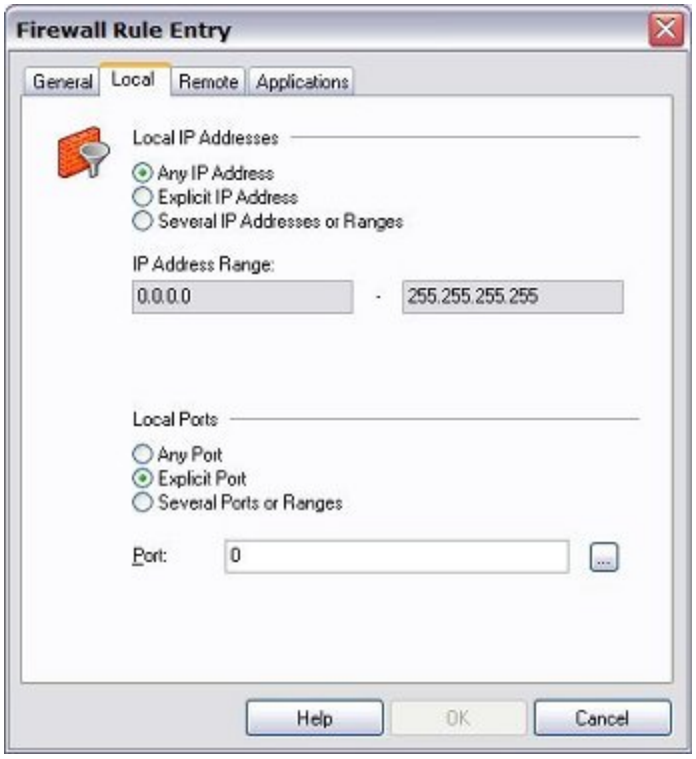


Local Tab

You can define any local IP addresses and ports that are controlled by your firewall rule on the **Local** tab of the **Firewall Rule Entry** dialog box. We recommend that, in any rule, you configure the **Local IP Addresses** setting to enable the **Any IP address** radio button. If you configure an incoming policy, you can add the ports to control with this policy in the Local Ports settings. If you want to control more than one port in the same

policy, select **Several Ports or Ranges**. Click **New** to add each port.

If you select **Explicit IP Address**, you must specify an IP address. The IP address must not be set to 0.0.0.0.

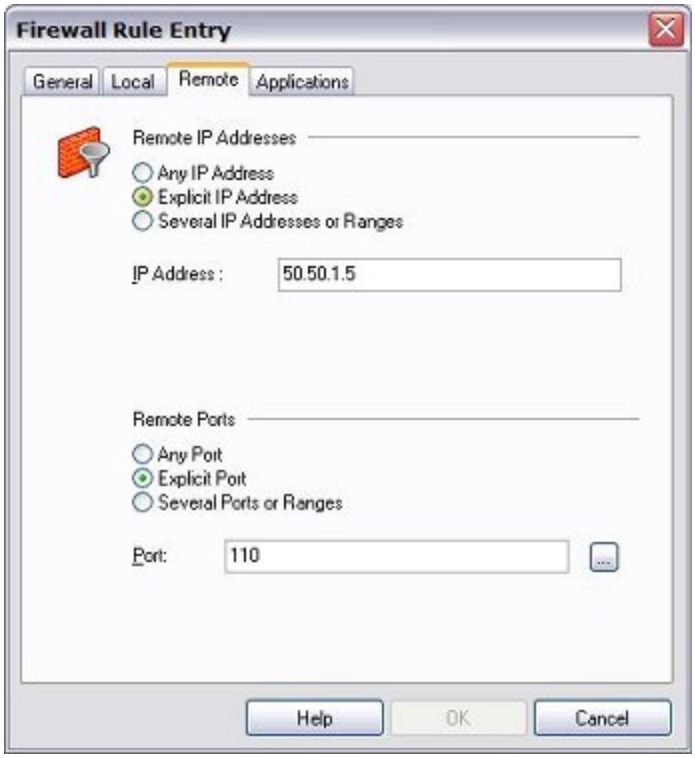


Remote Tab

You can define any remote IP addresses and ports that are controlled by this rule on the **Remote** tab of the **Firewall Rule Entry** dialog box.

For example, if your firewall is set to deny all traffic and you want to create a rule to allow outgoing POP3 connections, add the IP address of your POP3 server as an **Explicit IP Address** in the **Remote IP Addresses** section. Then, in the **Remote Ports** section, specify port 110 as an **Explicit Port** for this rule.

If you select the **Explicit IP Address** radio button, make sure you specify an IP address. The IP address must not be set to 0.0.0.0.



Applications Tab

You can limit your firewall rule so that it applies only when a specified program is used.

1. On the **Applications** tab of the **Firewall Rule Entry** dialog box, select the **Bind Rule To Application below** check box. This tab is not available in the Mobile VPN for Windows Mobile version of the desktop firewall.

2. Click **Select Application** to browse your local computer for a list of available applications.
3. Click **OK**.

End-User Instructions for WatchGuard Mobile VPN with IPSec Client Installation

> ***Note*** *These instructions are written for Mobile VPN with IPSec client end users. They tell end users to contact their network administrator for instructions on how to install a desktop firewall or configure the firewall that is part of the client software, and for the settings to control the connection behavior if they do not use a .ini file. You can print these instructions or use them to create a set of instructions for your end users.*

The WatchGuard Mobile VPN with IPSec client creates an encrypted connection between your computer and the XTM device with a standard Internet connection. The Mobile VPN client enables you to get access to protected network resources from any remote location with an Internet connection.

Before you install the client, make sure you understand these requirements and recommendations:

- You can install the Mobile VPN with IPSec client software on any computer with Windows XP SP2 (32 bit and 64 bit), Windows Vista (32 bit and 64 bit), or Windows 7 (32 bit and 64 bit) operating system.
- Make sure the computer does not have any other IPSec VPN client software installed.
- Uninstall any desktop firewall software other than Microsoft firewall software from your computer.
- If the client computer uses Windows XP, to install the Mobile VPN client software and to import the .wgx configuration file, you must log on with an account that has administrator rights. Administrator rights are not required to connect after the client has been installed and configured.

- If the client computer uses Windows Vista, to install the Mobile VPN client software, you must log on with an account that has administrator rights. Administrator rights are not required to import a .wgx or .ini file or to connect after the client has been installed.
- We recommend that you check to make sure all available service packs are installed before you install the Mobile VPN client software.
- We recommend that you do not change the configuration of any Mobile VPN client setting not explicitly described in this documentation.

Before you start the installation, make sure you have the following installation components:

- Mobile VPN with IPSec software installation file
- End-user profile, with a .wgx or .ini file extension
- Passphrase (if the end-user profile is a .wgx file or the connection uses certificates for authentication)
- User name and password
- cacert.pem and .p12 certificate file (if the connection uses certificates for authentication)

Install the Client Software

1. Copy the Mobile VPN .zip file to the remote computer and extract the contents of the file to the root directory on the remote (client or user) computer. Do not run the installation software from a CD or other external drive.
2. Copy the end user profile (the .wgx or .ini file) to the root directory.
   If you use certificates to authenticate, copy the cacert.pem and .p12 files to the root directory as well.
3. Double-click the .exe file you extracted in Step 1. This starts the WatchGuard Mobile VPN Installation Wizard. You must restart your computer when the installation wizard completes.
4. Click through the wizard and accept all the default settings.
5. Restart your computer when the installation wizard completes.
6. When the computer restarts, the WatchGuard Mobile VPN Connection Monitor dialog box appears. When the software starts for the first time after you install it, you see this message:

   ```
   There is no profile for the VPN dial-up!
   Do you want to use the configuration wizard for creating a profile now?
   ```

7. Click **No**.
8. Select **View > Autostart > No Autostart** so that the program does not run automatically.

After you install the client software, reinstall the original desktop firewall software or configure the firewall that is part of the client software. If you use a third-party desktop firewall, make sure you configure it to allow traffic to establish the VPN tunnel and the traffic that goes through the tunnel. Contact your network administrator for instructions.

Import the End User Profile

The end user profile file configures the Mobile VPN client with the settings required to create a VPN tunnel.

To import a Mobile VPN configuration .wgx or .ini file:

1. From your Windows desktop, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor**.
2. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Profile Import**.
   The Profile Import Wizard starts.

3. On the **Select User Profile** screen, browse to the location of the .wgx or .ini configuration file.
4. Click **Next**.
5. If you use a .wgx file, on the **Decrypt User Profile** screen, type the passphrase. The passphrase is case-sensitive.
6. Click **Next**.
7. On the **Overwrite or add Profile** screen, you can select to overwrite a profile of the same name. This is useful if your network administrator gives you a new .wgx file to import.
8. Click **Next**.
9. On the **Authentication** screen, you can select whether to type the user name and password that you use to authenticate the VPN tunnel.

   If you keep these fields empty, you must enter your user name and password each time you connect.

   If you type your user name and password, the Firebox stores them and you do not have to enter this information each time you connect. However, this is a security risk. You can also type just your user name and keep the **Password** field empty.
10. Click **Next**.
11. Click **Finish**.

Select a Certificate and Enter the Passphrase

Complete this section only if you have a cacert.pem and a .p12 file.

1. Select **Configuration > Certificates**.
2. Click **Add**.
3. On the **User Certificate** tab, select **from PKS#12 file** from the **Certificate** drop-down list.
4. Adjacent to the **PKS#12 Filename** text box, click the button and browse to the location of the .p12 file.
5. Click **OK**. Click **Close**.
6. Select **Configuration > Profiles**.
7. Select the profile name. Click **Edit**.
8. Click **Identities**.
9. From the **Certificate configuration** drop-down box, select the certificate configuration you added.
10. Select **Connection > Enter PIN**.
11. Type the passphrase and click **OK**.

Connect and Disconnect the Mobile VPN Client

Connect to the Internet through a Dial-Up Networking connection or a LAN connection. Then, use the instructions below to select your profile, connect, and disconnect.

To select your profile and connect the Mobile VPN client:

1. From your Windows desktop, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor**.
   The WatchGuard Mobile VPN dialog box appears.
2. From the **Profile** drop-down list, select the name of the profile you imported.

3. Click to connect.
   The Mobile VPN with IPSec client icon appears in the Windows system tray when you are connected.

To disconnect the Mobile VPN client:

1. Restore the Mobile VPN Monitor dialog box.
2. Click to disconnect.

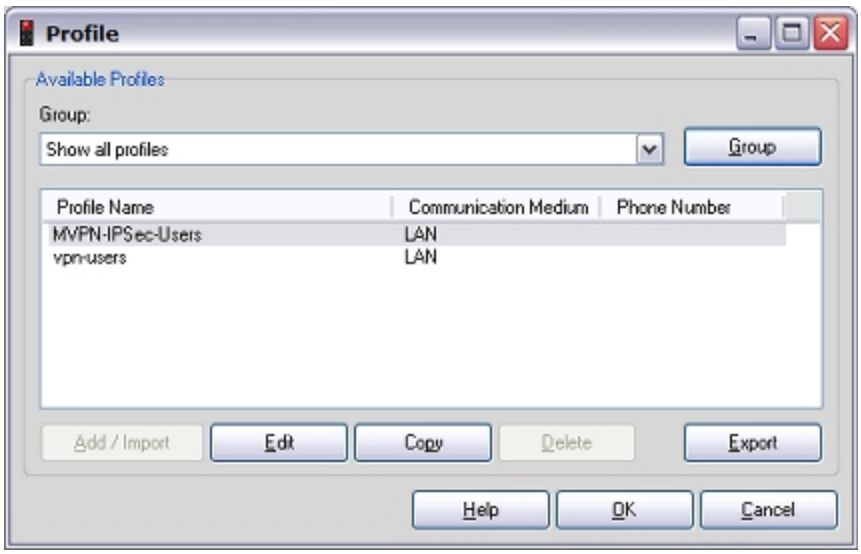
Control the Connection Behavior

The connection behavior controls the action the Mobile VPN client software takes when the VPN tunnel becomes unavailable for any reason. By default, you must manually reconnect. You are not required to change the connection behavior, but you can select to automatically or variably reconnect. Contact your network administrator for the suggested setting.

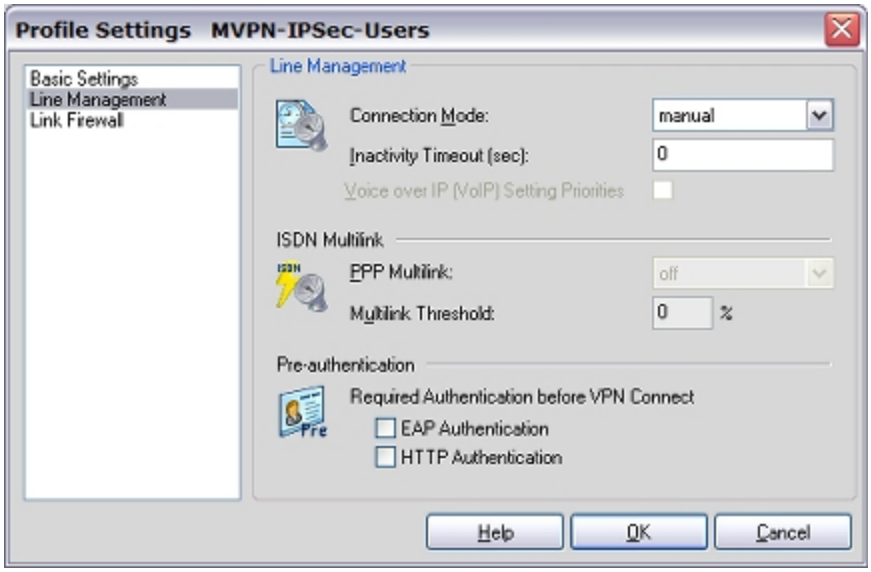
> ***Note*** *If you import a .ini file to configure the client software, do not change any of the Line Management settings. The .ini file configures these settings for you.*

To set the behavior of the Mobile VPN client when the VPN tunnel becomes unavailable:

1. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Profiles**.
2. Select the name of the profile and click **Edit**.



3. From the left pane, select **Line Management**.



4. Use the **Connection Mode** drop-down list to set a connection behavior for this profile.
   - **Manual** — When you select **manual** connection mode, the client does not try to restart the VPN tunnel automatically if the VPN tunnel goes down.
     To restart the VPN tunnel, you must click the **Connect** button in Connection Monitor or right-click the Mobile VPN icon on your Windows desktop toolbar and click **Connect**.
   - **Automatic** — When you select **automatic** connection mode, the client tries to start the connection when your computer sends traffic to a destination that you can reach through the VPN. The client also tries to restart the VPN tunnel automatically if the VPN tunnel goes down.
   - **Variable** — When you select **variable** connection mode, the client tries to restart the VPN tunnel automatically until you click **Disconnect**. After you disconnect, the client does not try to restart the VPN tunnel again until after the next time you click **Connect**.
5. Click **OK**.

Mobile VPN with IPSec Client Icon

The Mobile VPN with IPSec client icon appears in the Windows system tray to show the VPN connection status. You can right-click the icon to reconnect and disconnect your Mobile VPN, and to see the profile in use.

Mobile VPN for Windows Mobile Setup

WatchGuard Mobile VPN for Windows Mobile uses the data connection on a device running the Windows Mobile operating system to establish a secure VPN connection to networks protected by an XTM device that supports Mobile VPN with IPSec. Mobile VPN for Windows Mobile has two components:

- **WatchGuard Mobile VPN WM Configurator** runs on a computer that can establish a connection to the Windows Mobile device using Microsoft ActiveSync. The Configurator configures and uploads the client software to the Windows Mobile device.
- The WatchGuard Mobile VPN client software runs on the Windows Mobile device. The **WatchGuard Mobile VPN Service** must be running in order to establish a VPN connection**. WatchGuard Mobile VPN Monitor** allows you to select an uploaded end-user profile and connect the VPN.

Mobile VPN for Windows Mobile uses the same .wgx end-user profile files that are used to configure Mobile VPN with IPSec. To create the end-user profile, see *Configure the XTM Device for Mobile VPN with IPSec* on page 596.

Mobile VPN WM Configurator and Windows Mobile IPSec Client Requirements

Before you install the client, make sure you understand these requirements and recommendations to work with Mobile VPN with IPsec. If you have not, see the topics that describe how to configure your XTM device to use Mobile VPN.

You must *Configure the XTM Device for Mobile VPN with IPSec*. This process creates the end user profile used to configure the Windows Mobile client software.

The Mobile VPN WM Configurator system requirements are:

Operating System	Microsoft ActiveSync Version
Windows 2000	4.5 or higher
Windows XP (32-bit and 64-bit)	4.5 or higher
Windows Vista	6.1

The Windows Mobile IPSec client device requirements are:

- Windows Mobile 5.0
- Windows Mobile 6.0

Supported devices include:

- Symbol MC70 (Windows Mobile 5 Premium Phone)
- T-Mobile Dash (Windows Mobile 6 Smartphone)
- Samsung Blackjack (Windows Mobile 5 Smartphone)

> ***Note*** *The devices in this list have been tested with WatchGuard Mobile VPN for Windows Mobile. A good way to learn if other users have successfully configured other device is to check the WatchGuard user forum, at http://forum.watchguard.com/.*

To install the Windows Mobile VPN WM Configurator on some operating systems, you must log on to the computer with an account that has administrator rights and import the .wgx configuration file. Administrator rights are not required to upload the client and configuration to the Windows Mobile device.

Install the Mobile VPN WM Configurator Software

The Mobile VPN WM Configurator software must be installed on a computer that can connect to the Windows Mobile device through ActiveSync. Before you start the installation, make sure you have these installation components:

- The WatchGuard Mobile VPN WM Configurator installation file
- An end user profile, with a file extension of .wgx
- Shared Key
- A .p12 certificate file (if the VPN connects to a Firebox X Core or Peak and use certificates to authenticate)
- User name and password (if the VPN connects to a Firebox X Core or Peak and use Extended Authentication)

> ***Note*** *Write the shared key down and keep it in a secure location. You must use it when you import the end-user profile.*

To install the Configurator:

1. Copy the Mobile VPN WM Configurator .zip file to the computer and extract the contents of the file.
2. Copy the end user profile (the .wgx file) to the root directory on the remote computer.
3. Double-click the .exe file you extracted in Step 1. This starts the WatchGuard Mobile VPN WM Installation Wizard.
4. Follow the steps in the wizard. In the **InstallShield Wizard Complete** dialog box keep the **Start PDA Installation** check box selected only if the Windows Mobile device is currently connected through ActiveSync.

Select a Certificate and Enter the PIN

If the VPN uses a certificate to authenticate, you must:

1. Save the .p12 file to the \certs\ directory. The default location is `C:\Program Files\WatchGuard\Mobile VPN WM\certs\`.
2. Select **Start > All Programs > WatchGuard Mobile VPN > WatchGuard Mobile VPN WM** to start the Configurator.
3. Select **Configuration > Certificates**.
4. On the **User Certificate** tab, select **from PKS#12 file** from the **Certificate** drop-down list.

5. Adjacent to the **PKS#12 Filename** text box, type `%installdir%\certs\mycert.p12`. Replace `mycert.p12` with the name of your .p12 file. Click **OK**.
6. Select **Connection > Enter PIN**.
7. Type the PIN and click **OK**.
   The PIN is the shared key entered to encrypt the file in the Add Mobile VPN with IPSec wizard.

Import an End-User Profile

To import a Mobile VPN configuration .wgx file:

1. Select **Start > All Programs > WatchGuard Mobile VPN > WatchGuard Mobile VPN WM** to start the Configurator.
2. Select **Configuration > Profile Import**.
   The Profile Import Wizard starts.
3. On the **Select User Profile** screen, browse to the location of the .wgx configuration file supplied by your network administrator. Click **Next**.
4. On the **Decrypt User Profile** screen, type the shared key or passphrase supplied by your network administrator. The shared key is case-sensitive. Click **Next**.
5. On the **Overwrite or add Profile** screen, you can select to overwrite a profile of the same name. This is useful if your network administrator gives you a new .wgx file and you must reimport it. Click **Next**.
6. On the **Authentication** screen, you can type the user name and password that you use to authenticate the VPN tunnel. If you type your user name and password here, the XTM device stores it and you do not have to type this information each time you connect. However, this is a security risk. You can type just your user name and keep the **Password** field empty. This can minimize the amount of data required for the VPN connection.

   If you keep the fields empty, you must type your user name and password the first time you connect the VPN. The next time you connect, the user name field is automatically filled with the last user name entered.
7. Click **Next**.

> ***Note*** *If the password you use is your password on an Active Directory or LDAP server and you choose to store it, the password becomes invalid when it changes on the authentication server.*

8. Click **Finish**.

Install the Windows Mobile Client Software on the Windows Mobile Device

After you import the end user profile to the Configurator, connect the Configurator to the Windows Mobile device. The computer and the Windows Mobile device must have an ActiveSync connection when you start the Configurator.

> ***Note*** *After the WatchGuard Mobile VPN software is installed on your Windows Mobile device you must reboot it.*

1. Connect your Windows Mobile device to your computer with Microsoft ActiveSync.

2. To start the Configurator, select **Start > All Programs > WatchGuard Mobile VPN > WatchGuard Mobile VPN WM**.
3. If the WatchGuard Mobile VPN WM software has not been installed on the Windows Mobile device, a **Confirmation** dialog box opens. Click **Yes**.

4. An Information dialog box opens. Click **OK**.

5. The WatchGuard Mobile VPN WM software is installed on the Windows Mobile device. Click **OK**.

6. Reboot the Windows Mobile device.

Upload the End-User Profile to the Windows Mobile Device

After the Windows Mobile software is installed, you can upload the end-user profile to the Windows Mobile device.

1. Connect your Windows Mobile device to your computer with Microsoft ActiveSync.
2. Select **Start > All Programs > WatchGuard Mobile VPN > WatchGuard Mobile VPN WM** to start the Configurator.
3. From the **Profile** drop-down list, select the profile you want to upload to the Windows Mobile device.

4. Click **Upload**.
5. When the upload is complete, the Configurator status area shows **Upload completed successfully!**

If the VPN uses a certificate to authenticate, you must upload the certificate to the Windows Mobile device. Before you upload the certificate, the Configurator must be set up to use the certificate.

For more information, see select a certificate and enter the PIN.

To upload a certificate:

1. In the Configurator, select **Configuration > Upload PKS#12 File**.
2. Browse to the PKS#12 file and select it. Click **Open**.

Connect and Disconnect the Mobile VPN for Windows Mobile Client

The WatchGuard Mobile VPN for Windows Mobile client software uses the data connection of a Windows Mobile device to make a secure connection to networks protected by an XTM device. The Windows Mobile device must be able to make a data connection to the Internet.

1. On your Windows Mobile device, select **Start > Programs > WatchGuard Mobile VPN Monitor.** If the WatchGuard Mobile VPN Service is not running, a dialog box opens. Click **Yes** to start the service.

2. The WatchGuard Mobile VPN dialog box opens. Select the end user profile from the drop-down list at the top of the WatchGuard Mobile VPN dialog box.

3. Click **Connect** and type your user name and password. Click **OK**.

> ***Note*** *After the first successful VPN connection, the client saves the user name and only asks for a password. To change the user name, click* ***OK*** *with the password area clear. A dialog box opens in which you can enter a different user name and password.*

4. A yellow line with the word **Connecting** appears between the phone and computer in the WatchGuard Mobile VPN dialog box. The line turns green when the VPN tunnel is ready.

To disconnect the Mobile VPN client:

1. On your Windows Mobile device, select **Start > Programs > WatchGuard Mobile VPN Monitor**.
2. Click **Disconnect**. The green line changes to yellow.

When there is no line between the phone and computer, the VPN is disconnected.

Secure Your Windows Mobile Device with the Mobile VPN Firewall

The WatchGuard Mobile VPN for Windows Mobile client includes two firewall components:

Link firewall

The link firewall is not enabled by default. When the link firewall is enabled, your Windows Mobile device drops any packets received from other computers. You can choose to enable the link firewall only when a Mobile VPN tunnel is active, or enable it all the time.

Desktop firewall

This full-featured firewall can control connections to and from your Windows Mobile device. You can define friendly networks and set access rules separately for friendly and unknown networks.

For more information, see *Enable the Link Firewall* on page 628 and *Enable the Desktop Firewall* on page 629.

Stop the WatchGuard Mobile VPN Service

The WatchGuard Mobile VPN Service must be running on the Windows Mobile device to use the WatchGuard Mobile VPN Monitor to create VPN tunnels. When you close the Monitor, the service does not stop. You must stop the service manually.

1. On your Windows Mobile device, select **Start > Programs > WatchGuard Mobile VPN Service**.
   The WatchGuard Mobile VPN dialog box appears.

2. To stop the service, click **Yes**.

Uninstall the Configurator, Service, and Monitor

To uninstall WatchGuard Mobile VPN for Windows Mobile, you must uninstall software from your Windows computer and your Windows Mobile device.

Uninstall the Configurator from Your Windows Computer

1. On your Windows computer, select **Start > Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **WatchGuard Mobile VPN WM** and click **Change/Remove**.
4. Click **Yes** to uninstall the application.
5. Click **OK** when the uninstall is complete.

Uninstall the WatchGuard Mobile VPN Service and Monitor from Your Windows Mobile Device

1. On your Windows Mobile device, select **Start > Settings**.
2. In Settings, click the **System** tab and double-click **Remove Programs**.
3. Select **WatchGuard Mobile VPN** and click **Remove**.
4. The **Remove Program** dialog box opens. Click **Yes** to remove the software.
   A dialog box appears and asks if you want to reboot the device now.
5. To reboot the device now, click **Yes**.
   To reboot the device later, click **No**.
   The uninstall program does not complete until you reboot the device.

23 Mobile VPN with SSL

About Mobile VPN with SSL

The WatchGuard Mobile VPN with SSL client is a software application that is installed on a remote computer. The client makes a secure connection from the remote computer to your protected network through an unsecured network, such as the Internet. The Mobile VPN client uses SSL (Secure Sockets Layer) to secure the connection.

Configure the XTM Device for Mobile VPN with SSL

From Fireware XTM Web UI, when you enable Mobile VPN with SSL, an "SSLVPN-Users" user group and a "WatchGuard SSLVPN" policy are created to allow SSL VPN connections from the Internet to your external interface.

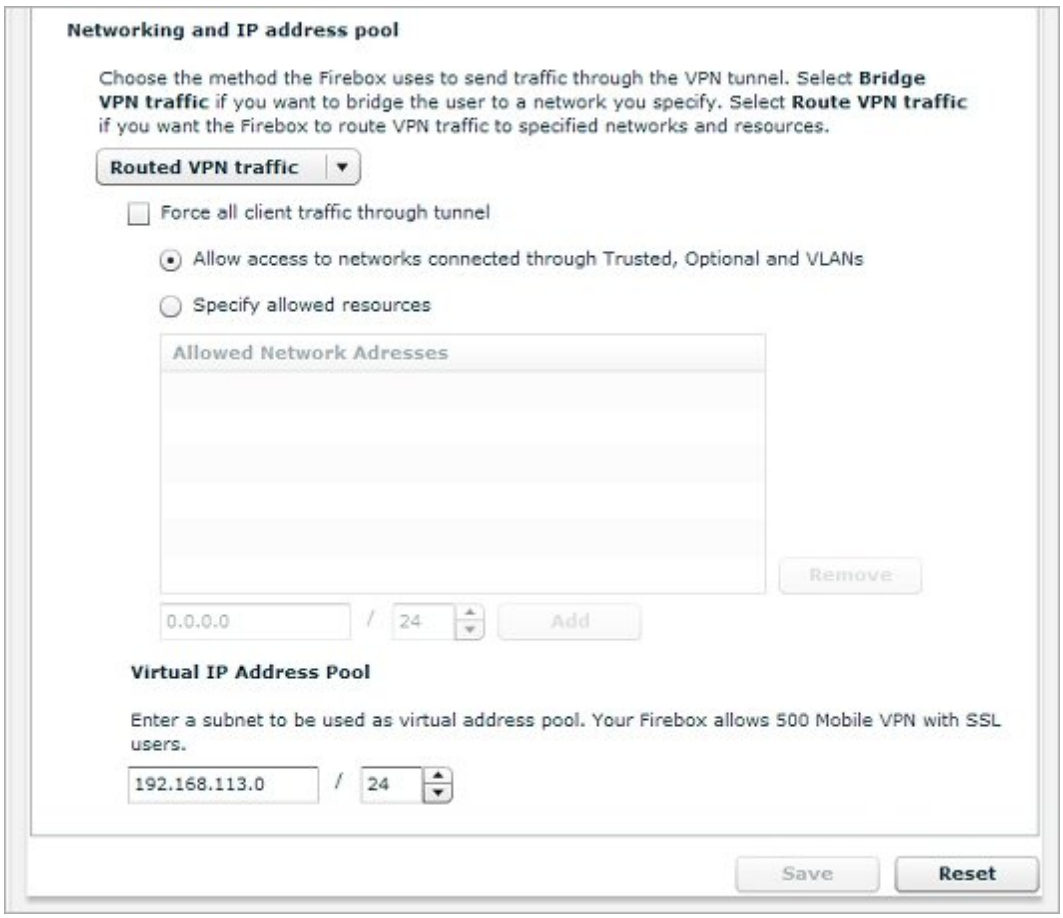
Configure Authentication and Connection Settings

1. Select **VPN > Mobile VPN with SSL**.
   The Mobile VPN with SSL Configuration page opens.

2. Select the **Activate Mobile VPN with SSL** check box.
3. Select an authentication server from the **Authentication Server** drop-down list. You can authenticate users with the internal XTM device database (Firebox-DB) or with a RADIUS, VACMAN Middleware, SecurID, LDAP, or Active Directory server.
   Make sure that the method of authentication is enabled (select **Authentication > Authentication Servers**). For more information, see Configure user authentication for Mobile VPN with SSL.
4. If you select RADIUS or SecurID as your authentication server, you can select the **Force users to authenticate after a connection is lost** check box to require users to authenticate after a Mobile VPN with SSL connection is disconnected. We recommend you select this check box if you use two-factor authentication that uses a one-time password, such as SecurID or Vasco.
   If you do not force users to authenticate after a connection is lost, the automatic connection attempt can fail. The Mobile VPN with SSL client automatically tries to reconnect after a connection is lost with the one-time password the user originally entered, which is no longer correct.
5. From the **Primary** drop-down list, select or type a public IP address or domain name. Mobile VPN with SSL clients connect to this IP address or domain name by default.
6. If your XTM device has more than one WAN connection, select a different public IP address from the **Backup** drop-down list. A Mobile VPN with SSL client connects to the backup IP address when it is unable to establish a connection with the primary IP address.

Configure the Networking and IP Address Pool Settings

In the **Networking and IP address pool** section, you configure the network resources Mobile VPN with SSL clients can use.



1. From the drop-down list in the **Networking and IP Address Pool** section, select the method the XTM device uses to send traffic through the VPN tunnel.

   - Select **Bridge VPN Traffic** to bridge SSL VPN traffic to a network you specify. When you select this option, you cannot filter traffic between the SSL VPN users and the network that the SSL VPN traffic is bridged to.
   - Select **Routed VPN Traffic** to route VPN traffic to specified networks and resources. This is the default for all WatchGuard XTM devices.

2. Select or clear the **Force all client traffic through the tunnel** check box.

   - Select **Force all client traffic through tunnel** to send all private network and Internet traffic through the tunnel. This option sends all external traffic through the XTM device policies you create and offers consistent security for mobile users. However, because it requires more processing power on the XTM device, access to Internet resources can be very slow for the mobile user. To allow clients to access the Internet when this option is selected, see *Options for Internet Access Through a Mobile VPN with SSL Tunnel* on page 659.
   - Clear the **Force all client traffic through tunnel** check box to send only private network information through the tunnel. This option gives your users better network speeds by routing

only necessary traffic through the XTM device, but access to Internet resources is not restricted by the policies on your XTM device. To restrict Mobile VPN with SSL client access to only specified devices on your private network, select the **Specify allowed resources** radio button. Type the IP address of the network resource in slash notation and click **Add**.

3. Configure the IP addresses the XTM device assigns to Mobile VPN with SSL client connections. The virtual IP addresses in this address pool cannot be part of a network protected by the XTM device, any network accessed through a route or BOVPN, assigned by DHCP to a device behind the XTM device, or used for Mobile VPN with IPSec or Mobile VPN with SSL address pools.

   Routed VPN traffic

   For the Virtual IP Address Pool, keep the default setting of 192.168.113.0/24, or enter a different range. Type the IP address of the subnet in slash notation. IP addresses from this subnet are automatically assigned to Mobile VPN with SSL client connections. You cannot assign an IP address to a user.

   The virtual IP addresses in this address pool cannot be part of a network protected by the XTM device, any network accessed through a route or BOVPN, assigned by DHCP to a device behind the XTM device, or used for Mobile VPN with IPSec or Mobile VPN with PPTP address pools.

   Bridge VPN traffic

   From the **Bridge to interface** drop-down list, select the name of the interface to bridge to. In the **Start** and **End** fields, type the first and last IP addresses in the range that is assigned to the Mobile VPN with SSL client connections. The **Start** and **End** IP addresses must be on the same subnet as the bridged interface.

   > ***Note*** *The **Bridge to interface** option does not bridge SSL VPN traffic to any secondary networks on the selected interface.*

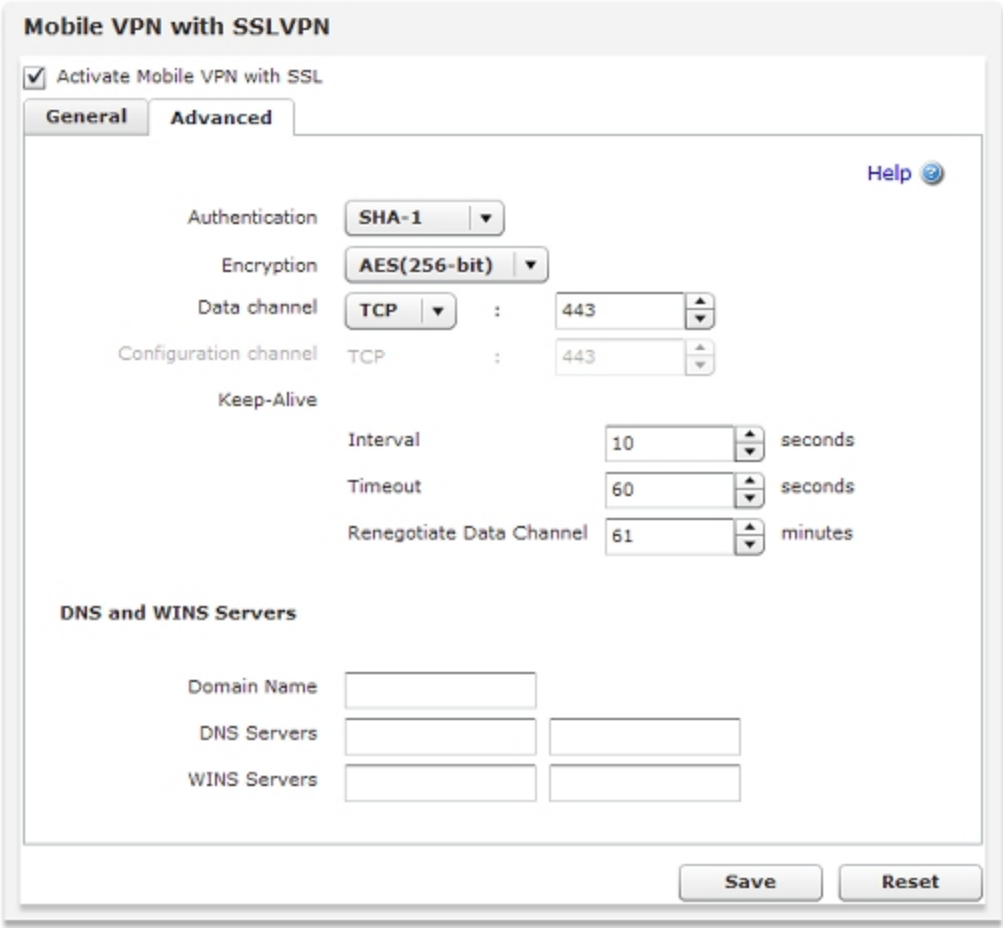
4. Click **Save** to save your changes to the XTM device.

After you save the changes to your XTM device, you must configure user authentication for Mobile VPN with SSL before users can download and install the software. Any changes you make are distributed to clients automatically the next time they connect using Mobile VPN with SSL.

For more information on using slash notation, see *About Slash Notation* on page 3.

Configure Advanced Settings for Mobile VPN with SSL

1. Select **VPN > Mobile VPN with SSL**.
   The Mobile VPN with SSL Configuration page opens.



2. Click the **Advanced** tab.
   The options you can configure on this tab include:

Authentication

Authentication method used to establish the connection. The options are **MD5**, **SHA**, **SHA-1**, **SHA-256**, and **SHA-512**.

Encryption

Algorithm that is used to encrypt the traffic. The options are **Blowfish**, **DES**, **3DES**, **AES (128 bit)**, **AES (192 bit)**, or **AES (256 bit)**. The algorithms are shown in order from weakest to strongest, with the exception of Blowfish, which uses a 128-bit key for strong encryption.

For best performance with a high level of encryption, we recommend that you choose MD5 authentication with Blowfish encryption.

Data channel

The protocol and port Mobile VPN with SSL uses to send data after a VPN connection is established. You can use the **TCP** or **UDP** protocol. Then, select a port. The default protocol and port for Mobile VPN with SSL is TCP port 443. This is also the standard protocol and port for HTTPS traffic. Mobile VPN with SSL can share port 443 with HTTPS.

If you change the data channel to use a port other than 443,users must manually type this port in the Mobile VPN with SSL connection dialog box. For example, if you change the data channel to 444, and the XTM device IP address is 50.50.50.50, the user must type `50.50.50.50:444` instead of `50.50.50.50`.

If the port is set to the default 443, the user must type only the XTM device's IP address. It is not necessary to type :443 after the IP address.

For more information, see *Choose the Port and Protocol for Mobile VPN with SSL* on page 658.

Configuration channel

The protocol and port Mobile VPN with SSL uses to negotiate the data channel and to download configuration files. If you set the data channel protocol to TCP, the configuration channel automatically uses the same port and protocol. If you set the data channel protocol to UDP, you can set the configuration channel protocol to **TCP** or **UDP**, and you can use a different port than the data channel.

Keep-alive

Defines how often the XTM device sends traffic through the tunnel to keep the tunnel active when no other traffic is being sent through the tunnel.

Timeout

Defines how long the XTM device waits for a response. If there is no response before the timeout value, the tunnel is closed and the client must reconnect.

Renegotiate Data Channel

If a Mobile VPN with SSL connection has been active for the amount of time specified in the **Renegotiate Data Channel** text box, the Mobile VPN with SSL client must create a new tunnel. The minimum value is 60 minutes.

DNS and WINS Servers

You can use DNS or WINS to resolve the IP addresses of resources that are protected by the XTM device. If you want the Mobile VPN with SSL clients to use a DNS or WINS server behind the XTM device instead of the servers assigned by the remote network they are connected to, type the domain name and IP addresses of the DNS and WINS servers on your network. For more information on DNS and WINS, see *Name Resolution for Mobile VPN with SSL* on page 660.

Restore Defaults

Click to reset the **Advanced** tab settings to their default values. All DNS and WINS server information on the **Advanced** tab is deleted.

Configure User Authentication for Mobile VPN with SSL

To allow users to authenticate to the XTM device and connect with Mobile VPN with SSL, you must configure user authentication on the XTM device. You can configure your XTM device as an authentication server or use a third-party authentication server. When you enable Mobile VPN with SSL, an SSLVPN-Users group is created automatically.

Users must be a member of the SSLVPN-Users group to make a Mobile VPN with SSL connection. Users cannot connect if they are a member of a group that is part of the SSLVPN-Users group. The user must be a direct member of the SSLVPN-Users group.

For more information, see *Configure Your XTM Device as an Authentication Server* on page 254 and *About Third-Party Authentication Servers* on page 253.

Configure Policies to Control Mobile VPN with SSL Client Access

When you enable Mobile VPN with SSL, an *Allow SSLVPN-Users* policy is added. It is has no restrictions on the traffic that it allows from SSL clients to network resources protected by the XTM device. To restrict Mobile VPN with SSL client access, disable the Allow SSLVPN-Users policy. Then, add new policies to your configuration or add the group with Mobile VPN with SSL access to the **From** section of existing policies.

> ***Note*** *If you assign addresses from a trusted network to Mobile VPN with SSL users, the traffic from the Mobile VPN with SSL user is not considered trusted. All Mobile VPN with SSL traffic is untrusted by default. Regardless of assigned IP address, policies must be created to allow Mobile VPN with SSL users access to network resources.*

Allow Mobile VPN with SSL Users to Access a Trusted Network

In this example, you use Fireware XTM Web UI to add an Any policy which gives all members of the SSLVPN-Users group full access to resources on all trusted networks.

1. Select **Firewall > Firewall Policies**. Click  .
2. Expand the **Packet Filters** folder.
   A list of templates for packet filters appears.
3. Select **Any** and click **Add**.
   The Policy Configuration page appears.
4. Type a name for the policy in the **Name** text box. Choose a name that will help you identify this policy in your configuration.
5. On the **Policy** tab, in the **From** section, select **Any-Trusted** and click **Remove**.
6. In the **From** section, click **Add**.
   The Add Member dialog box appears.
7. From the **Member Type** drop-down list, select **SSLVPN Group**.
8. Select **SSLVPN-Users** and click **OK**.
   After SSLVPN-Users is the name of the authentication method in parenthesis.
9. Click **OK** to close the **Add Member** dialog box.
10. In the **To** section, select **Any-External** and click **Remove**.
11. In the **To** section, click **Add**.
    The Add Member dialog box appears.

12. In the **Select Members** list, select **Any-Trusted** and click **OK**.
13. Click **Save** to save the changes to the XTM device.

For more information on policies, see *Add Policies to Your Configuration* on page 291.

Use Other Groups or Users in a Mobile VPN with SSL Policy

Users must be a member of the SSLVPN-Users group to make a Mobile VPN with SSL connection. You can use policies with other groups to restrict access to resources after the user connects. You can use Fireware XTM Web UI to select a user or group other than SSLVPN-Users.

1. Select **Firewall > Firewall Policies**.
2. Double-click the policy to which you want to add the user or group.
3. On the **Policy** tab, click **Add** in the **From** area.
   The Add Member dialog box appears.
4. From the **Member Type** drop-down list, select **Firewall User** or **Firewall Group**.
5. Select the user or group you want to add and click **OK**.
6. Click **Save**.

For more information on how to use users and groups in policies, see *Use Authorized Users and Groups in Policies* on page 285.

Choose the Port and Protocol for Mobile VPN with SSL

The default protocol and port for Mobile VPN with SSL is TCP port 443. If you try to configure the XTM device to use a port and protocol that is already in use, you see an error message.

Common network configurations that require the use of TCP 443 include:

- The XTM device protects a web server that uses HTTPS.
- The XTM device protects a Microsoft Exchange server with Microsoft Outlook Web Access configured.

If you have an additional external IP address that does not accept incoming TCP port 443 connections, you can configure it as the primary IP address for Mobile VPN with SSL.

> ***Note*** *Mobile VPN with SSL traffic is always encrypted using SSL, even if you use a different port or protocol.*

How to Choose a Different Port and Protocol

If you need to change the default port or protocol for Mobile VPN with SSL, we recommend that you choose a port and protocol that is not commonly blocked. Some additional considerations include:

Select a common port and protocol

Mobile VPN with PPTP and Mobile VPN with IPSec use specific ports and protocols that are blocked by some public Internet connections. By default, Mobile VPN with SSL operates on the port and protocol used for encrypted web site traffic (HTTPS) to avoid being blocked. This is one of the main advantages of SSL VPN over other Mobile VPN options. We recommend that you choose TCP port 53, or UDP port 53 (DNS) to keep this advantage.

These ports are allowed by almost all Internet connections. If the access site uses packet filters, the SSL traffic should pass. If the access site uses proxies, the SSL traffic is likely to be denied because it does not follow standard HTTP or DNS communications protocols.

UDP versus TCP

Normally TCP works as well as UDP, but TCP can be significantly slower if the connection is already slow or unreliable. The additional latency is caused by the error checking that is part of the TCP protocol. Because the majority of traffic that passes through a VPN tunnel uses TCP, the addition of TCP error checking to the VPN connection is redundant. With slow and unreliable connections, the TCP error checking timeouts cause VPN traffic to be sent more and more slowly. If this happens enough times, the poor connection performance is noticed by the user.

UDP is a good choice if the majority of the traffic generated by your MVPN with SSL clients is TCP-based. The HTTP, HTTPS, SMTP, POP3 and Microsoft Exchange protocols all use TCP by default. If the majority of the traffic generated by your Mobile VPN with SSL clients is UDP, we recommend that you select TCP for the MVPN with SSL protocol.

Options for Internet Access Through a Mobile VPN with SSL Tunnel

Force All Client Traffic Through Tunnel

This is the most secure option. It requires that all remote user Internet traffic is routed through the VPN tunnel to the XTM device. From the XTM device, the traffic is then sent back out to the Internet. With this configuration (also known as default-route VPN), the XTM device is able to examine all traffic and provide increased security. However, this requires more processing power and bandwidth from the XTM device. This can affect network performance if you have a large number of VPN users. By default, a policy named *Allow SSLVPN-Users* allows access to all internal resources and the Internet.

Allow Direct Access to the Internet

If you select **Routed VPN traffic** in the Mobile VPN with SSL configuration, and you do not force all client traffic through the tunnel, you must configure the allowed resources for the SSL VPN users. If you select **Specify allowed resources** or **Allow access to networks connected through Trusted, Optional and VLANs**, only traffic to those resources is sent through the VPN tunnel. All other traffic goes directly to the Internet and the network that the remote SSL VPN user is connected to. This option can affect your security because any traffic sent to the Internet or the remote client network is not encrypted or subject to the policies you configured on the XTM device.

Use the HTTP Proxy to Control Internet Access for Mobile VPN with SSL Users

If you configure Mobile VPN with SSL to force all client traffic through the tunnel, you can use HTTP proxy policies to restrict Internet access. The default *Allow SSLVPN-Users* policy has no restrictions on the traffic that it allows from SSL clients to the Internet. To restrict Internet access, you can use an HTTP proxy policy you have already configured, or add a new HTTP proxy policy for SSL clients.

1. Select **Firewall > Firewall Policies**.
2. Double-click the policy to open the **Policy Configuration** page.
3. On the **Policy** tab, click **Add** in the **From** area.
4. From the **Member Type** drop-down list, select **SSLVPN Group**.
5. Select **SSLVPN-Users** and click **OK**.
6. Click **Save**.

The HTTP proxy policy takes precedence over the Any policy. You can leave the Any policy to handle traffic other than HTTP, or you can use these same steps with another policy to manage traffic from the SSL clients.

For more information on how to configure an HTTP proxy policy, see *About the HTTP-Proxy* on page 357.

Name Resolution for Mobile VPN with SSL

The goal of a mobile VPN connection is to allow a user to connect to network resources as if they were connected locally. With a local network connection, NetBIOS traffic on the network allows you to connect to devices using the device name. It is not necessary to know the IP address of each network device. However, Mobile VPN tunnels cannot pass broadcast traffic, and NetBIOS relies on broadcast traffic to operate correctly. An alternative method for name resolution must be used.

Methods of Name Resolution Through a Mobile VPN with SSL Connection

You must choose one of these two methods for name resolution:

WINS/DNS (Windows Internet Name Service/Domain Name System)

A WINS server holds a database of NetBIOS name resolution for the local network. DNS works in a similar way. If your domain uses only Active Directory, you must use DNS for name resolution.

LMHOSTS file

An LMHOSTS file is a manually created file that you install on all computers with Mobile VPN with SSL installed. The file contains a list of resource names and their associated IP addresses.

Select the Best Method for Your Network

Because of the limited administration requirements and current information it provides, WINS/DNS is the preferred solution for name resolution through a Mobile VPN tunnel. The WINS server constantly listens to the local network and updates its information. If a resource changes its IP address or a new resource is added, nothing on the SSL client must be changed. When the client tries to get access to a resource by name, a request is sent to the WINS/DNS servers and the most current information is given.

If you do not already have a WINS server, the LMHOSTS file is a fast way to provide name resolution to Mobile VPN with SSL clients. Unfortunately, it is a static file and you must edit it manually any time there is a change. Also, the resource name/IP address pairs in the LMHOSTS file are applied to all network connections, not only the Mobile VPN with SSL connection.

Configure WINS or DNS for Name Resolution

Each network is unique in the resources available and the skills of the administrators. The best resource to learn how to configure a WINS server is the documentation for your server, such as the Microsoft web site. When you configure your WINS or DNS server, note that:

- The WINS server must be configured to be a client of itself.
- Your XTM device must be the default gateway of the WINS and DNS servers.
- You must make sure that network resources do not have more than one IP address assigned to a single network interface. NetBIOS only recognizes the first IP address assigned to a NIC. For more information, refer to http://support.microsoft.com/kb/q131641/.

Add WINS and DNS Servers to a Mobile VPN with SSL Configuration

1. Select **VPN > Mobile VPN with SSL**.
2. Select the **Advanced** tab.
   The Mobile VPN with SSL Advanced tab page appears.
3. In the **WINS and DNS Servers** area, type the primary and secondary addresses for the WINS and DNS servers. You can also type a domain suffix in the **Domain Name** text box for a client to use with unqualified names.
4. Click **Save**.
5. The next time an SSL client computer authenticates to the XTM device, the new settings are applied to the connection.

Configure an LMHOSTS File to Provide Name Resolution

When you use an LMHOSTS file to get name resolution for your Mobile VPN clients, no changes to the XTM device or the Mobile VPN client software are necessary. Basic instructions to help you create an LMHOSTS file are shown below. For more information on LMHOSTS files, refer to http://support.microsoft.com/kb/q150800/.

Edit an LMHOSTS File

1. Look for an LMHOSTS file on the Mobile VPN client computer. The LMHOSTS file (sometimes named lmhosts.sam) is usually located in:
   `C:\WINDOWS\system32\drivers\etc`
2. If you find an LMHOSTS file in that location, open it with a text editor like Notepad. If you cannot find an LMHOSTS file, create a new file in a text editor.
3. To create an entry in the LMHOSTS file, type the IP address of a network resource, five spaces, and then the name of the resource. The resource name must be 15 characters or less. It should look like this:
   `192.168.42.252      server_name`
4. If you started with an older LMHOSTS file, save the file with its original name. If you created a new file in Notepad, save it with the name `lmhost` in the C:\WINDOWS\system32\drivers\etc directory. You must also choose the type "All Files" in the **Save** dialog box, or Notepad appends ".txt" to the file name.
5. Reboot the SSL client computer for the LMHOSTS file to become active.

Install and Connect the Mobile VPN with SSL Client

The Mobile VPN with SSL software allows users to connect, disconnect, gather more information about the connection, and to exit or quit the client. The Mobile VPN with SSL client adds an icon to the system tray on the Windows operating system, or an icon in the menu bar on Mac OS X. You can use this icon to control the client software.

To use Mobile VPN with SSL, you must:

1. Verify system requirements
2. Download the client software
3. Install the client software
4. Connect to your private network

> **Note** *If a user is unable to connect to the XTM device, or cannot download the installer from the XTM device, you can Manually Distribute and Install the Mobile VPN with SSL Client Software and Configuration File.*

Client Computer Requirements

You can install the Mobile VPN with SSL client software on computers with these operating systems:

- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP
- Mac OS X 10.5 (Leopard)

If the client computer has Windows Vista or Windows XP, you must log on with an account that has administrator rights to install the Mobile VPN with SSL client software. Administrator rights are not required to connect after the SSL client has been installed and configured. In Windows XP Professional, the user must be a member of the *Network Configuration Operators* group to run the SSL client.

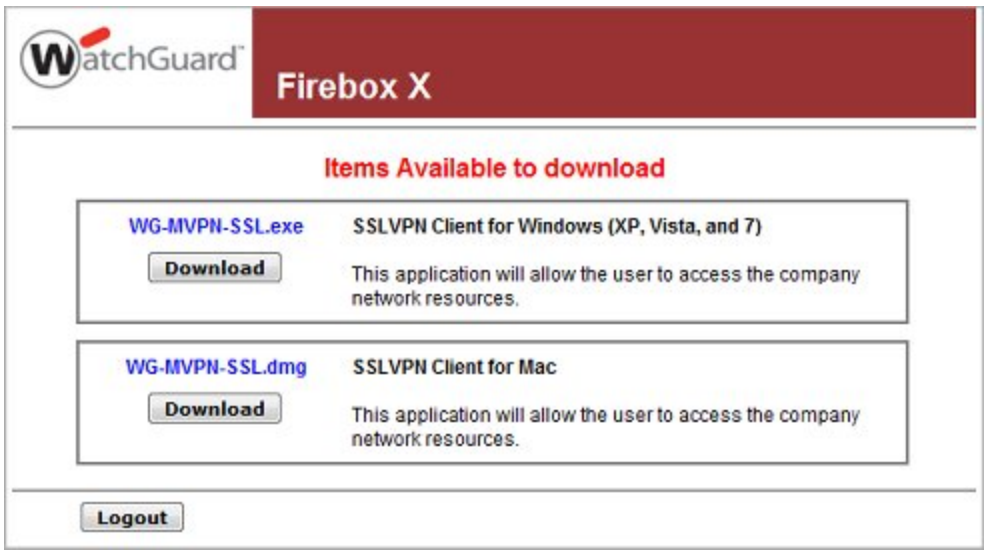
If the client computer has Mac OS X, administrator rights are not required to install or use the SSL client.

Download the Client Software

1. Connect to this address with a web browser:

```
https://<IP address of an XTM device interface>/sslvpn.html
    or
    https://<Host name of the XTM device>/sslvpn.html
```

2. Enter your user name and password to authenticate to the XTM device.
   The SSL VPN client download page appears.



3. Click the **Download** button for the installer you want to use. There are two available versions: Windows (WG-MVPN-SSL.exe) and Mac OS X (WG-MVPN-SSL.dmg).
4. Save the file to your desktop or another folder of your choice.

Install the Client Software

For Microsoft Windows:

1. Double-click **WG-MVPN-SSL.exe**.
   The Mobile VPN with SSL client Setup Wizard starts.
2. Accept the default settings on each screen of the wizard.
3. If you want to add a desktop icon or a Quick Launch icon, select the check box in the wizard that matches the option. A desktop or Quick Launch icon is not required.
4. Finish and exit the wizard.

For Mac OS X:

1. Double-click **WG-MVPN-SSL.dmg**.
   A volume named WatchGuard Mobile VPN is created on your desktop.
2. In the WatchGuard Mobile VPN volume, double-click **WatchGuard Mobile VPN with SSL Installer V15.mpkg**.
   The client installer starts.
3. Accept the default settings on each screen of the installer.
4. Finish and exit the installer.

After you download and install the client software, the Mobile VPN client software automatically connects to the XTM device. Each time you connect to the XTM device, the client software checks for configuration updates.

Connect to Your Private Network

For Microsoft Windows:

1. Use one of these three methods to start the client software:
   - From the **Start Menu**, select **All Programs > WatchGuard > Mobile VPN with SSL client > Mobile VPN with SSL client**.
   - Double-click the Mobile VPN with SSL icon on your desktop.
   - Click the Mobile VPN with SSL icon in the Quick Launch toolbar.
2. Type the information for the XTM device you want to connect to, and the username and password for the user.

   The Server is the IP address of the primary external interface of the XTM device. If you configured Mobile VPN with SSL to use a port other than the default port 443, in the Server field, type the primary external interface followed by a colon and the port number. For example, if Mobile VPN with SSL is configured to use port 444, and the primary external IP address is 50.50.50.1. the Server is 50.50.50.1:444.
3. Click **Connect**.

For Mac OS X:

1. Open a Finder window. Go to **Applications > WatchGuard** and double-click the **WatchGuard Mobile VPN with SSL** application.
   The WatchGuard Mobile VPN with SSL icon appears in the menu bar.
2. Click the icon in the menu bar and select **Connect**.
3. Type the information for the XTM device you want to connect to, and the username and password for the user.

   The Server is the IP address of the primary external interface of the XTM device. If you configured Mobile VPN with SSL to use a port other than the default port 443, in the Server field, type the primary external interface followed by a colon and the port number. For example, if Mobile VPN with SSL is configured to use port 444, and the primary external IP address is 50.50.50.1. the Server is 50.50.50.1:444.
4. Click **Connect**.

The SSL client user must enter their login credentials. Mobile VPN with SSL does not support any Single Sign-On (SSO) services. If the connection between the SSL client and the XTM device is temporarily lost, the SSL client tries to establish the connection again.

Mobile VPN with SSL Client Controls

When the Mobile VPN with SSL client runs, the WatchGuard Mobile VPN with SSL icon appears in the system tray (Windows) or on the right side of the menu bar (Mac OS X). The VPN connection status is shown by the icon's magnifying glass.

- The VPN connection is not established.
- The VPN connection has been established. You can securely connect to resources behind the XTM device.
- The client is in the process of connecting or disconnecting.

To see the client controls list, right-click the Mobile VPN with SSL icon in the system tray (Windows), or click the Mobile VPN with SSL icon in the menu bar (Mac OS X). You can select the following actions:

Connect/Disconnect

Start or stop the SSL VPN connection.

View Logs

Open the connection log file.

Properties

Windows — Select **Launch program on startup** to start the client when Windows starts. Type a number for **Log level** to change the level of detail included in the logs.

Mac OS X — Shows detailed information about the SSL VPN connection. You can also set the log level.

About

The WatchGuard Mobile VPN dialog box opens with information about the client software.

Exit (Windows) or Quit (Mac OS X)

Disconnect from the XTM device and shut down the client.

Manually Distribute and Install the Mobile VPN with SSL Client Software and Configuration File

If there is some reason your users cannot download the client software from the XTM device, you can manually provide them with the client software and configuration file. You can download the Mobile VPN with SSL client software from the Software Downloads section of the WatchGuard LiveSecurity web site. Use the steps below to get the SSL VPN configuration file to distribute.

Get the Configuration File from the XTM device

You must configure the XTM device to use Mobile VPN with SSL before you use this procedure.

To get the Mobile VPN with SSL configuration file, you must install WatchGuard System Manager. Then you can use Firebox System Manager to get the file. For more information, see the Mobile VPN for SSL chapter in the WatchGuard System Manager Help or User Guide.

Install and Configure the SSL Client Using the Installation Software and a Configuration File

You must have two files:

- Mobile VPN with SSL VPN client installation software
  WG-MVPN-SSL.exe (Microsoft Windows) or WG-MVPN-SSL.dmg (Mac OS X)
- Mobile VPN with SSL VPN configuration file
  sslvpn_client.wgssl

For Microsoft Windows:

1. Double-click **WG-MVPN-SSL.exe**.
   The Mobile VPN with SSL client Setup Wizard starts.
2. Accept the default settings on each screen of the wizard.
3. If you want to add a desktop icon or a Quick Launch icon, select the check box for that option.
   A desktop or Quick Launch icon is not required. The client icon is added to the Windows Start menu by default.
4. Finish and exit the wizard.
5. Use one of these three methods to start the client software:
   - From the **Start Menu**, select **All Programs > WatchGuard > Mobile VPN with SSL client > Mobile VPN with SSL client**.
     The client installer starts.
   - Double-click the Mobile VPN with SSL client icon on the desktop.
   - Click the Mobile VPN with SSL client icon in the Quick Launch toolbar.
6. Double-click **sslvpn-client.wgssl** to configure the Mobile VPN with SSL client software.

For Mac OS X:

1. Double-click **WG-MVPN-SSL.dmg**.
   A volume named WatchGuard Mobile VPN is created on the desktop.
2. In the WatchGuard Mobile VPN volume, double-click **WatchGuard Mobile VPN with SSL Installer V15.mpkg**.
   The client installer starts.
3. Accept the default settings in the installer.
4. Finish and exit the installer.
5. Start the client software. Open a Finder window and go to **Applications > WatchGuard**.
6. Double-click the **WatchGuard Mobile VPN with SSL** application.
   The WatchGuard Mobile VPN with SSL logo appears in the menu bar.
7. Double-click **sslvpn-client.wgssl** to configure the Mobile VPN with SSL client software.

Update the Configuration of a Computer that is Unable to Connect to the XTM Device

You must have an updated sslvpn-client.wgssl file. For information on how to get the sslvpn-client.wgssl file, see Get the configuration file from the XTM device.

1. Double-click **sslvpn-client.wgssl**.
   The SSL client starts.
2. Type your user name and password. Click **Connect**.

The SSL VPN connects with the new settings.

Uninstall the Mobile VPN with SSL Client

You can use the uninstall application to remove the Mobile VPN with SSL client from a computer.

Windows Vista and Windows XP

1. From the **Start Menu**, select **All Programs > WatchGuard > Mobile VPN with SSL client > Uninstall Mobile VPN with SSL client**.
   The Mobile VPN with SSL client uninstall program starts.

2. Click **Yes** to remove the Mobile VPN with SSL client and all of its components.
3. When the program is finished, click **OK**.

Mac OS X

1. In a Finder window, go to the **Applications > WatchGuard** folder.
2. Double-click the **Uninstall WG SSL VPN** application to start the uninstall program.
   The Mobile VPN with SSL client uninstall program starts.
3. Click **OK** on the **Warning** dialog box.
4. Click **OK** on the **Done** dialog box.
5. In a Finder window, go to the **Applications** folder.
6. Drag the **WatchGuard** folder to the Trash.

24 WebBlocker

About WebBlocker

If you give users unlimited web site access, your company can suffer lost productivity and reduced bandwidth. Uncontrolled Internet surfing can also increase security risks and legal liability. The WebBlocker security subscription gives you control of the web sites that are available to your users.

WebBlocker uses a database of web site addresses controlled by SurfControl, a leading web filter company. When a user on your network tries to connect to a web site, the XTM device examines the WebBlocker database. If the web site is not in the database or is not blocked, the page opens. If the web site is in the WebBlocker database and is blocked, a notification appears and the web site is not displayed.

WebBlocker works with the HTTP and HTTPS proxies to filter web browsing. If you have not configured an HTTP or HTTPS proxy, a proxy is automatically configured and enabled for you when you enable WebBlocker.

The WebBlocker Server hosts the WebBlocker database that the XTM device uses to filter web content. If you use WebBlocker on any XTM device other than an XTM 2 Series, you must first set up a local WebBlocker Server on your management computer. By default, WebBlocker on an XTM 2 Series device uses a WebBlocker Server hosted and maintained by WatchGuard.

The WebBlocker Server is installed as part of the WatchGuard System Manager installation. To learn about how to set up a WebBlocker Server, see the WatchGuard System Manager help at http://www.watchguard.com/help/docs/fireware/11/en-US/index.html.

To configure WebBlocker on the XTM device, you must have a WebBlocker license key and register it on the LiveSecurity web site. After you register the license key, LiveSecurity gives you a new feature key.

For more information about feature keys, see *About Feature Keys* on page 50.

Configure a Local WebBlocker Server

When you use WebBlocker on your XTM device, it connects to a WebBlocker server to check to see if a web site matches a WebBlocker category.

To use WebBlocker on an XTM 1050, XTM 8 Series or XTM 5 Series device, you must first configure a WebBlocker server on your local network. To use WebBlocker on an XTM 2 Series device, you do not have to configure a local WebBlocker server. By default, WebBlocker on an XTM 2 Series device connects to a WebBlocker Server maintained by WatchGuard.

To install your own WebBlocker Server, you must download and install the WatchGuard System Manager software.

To learn about how to set up a local WebBlocker Server, see the WatchGuard System Manager help at http://www.watchguard.com/help/docs/wsm/11/en-US/index.html.

After you install a WebBlocker Server on a computer in your local network, you must change your WebBlocker profiles to use your local WebBlocker Server.

For instructions to change your WebBlocker profiles, see *Get Started with WebBlocker* on page 670.

Get Started with WebBlocker

To use WebBlocker, you must define WebBlocker actions for at least one WebBlocker profile, which specifies the WebBlocker Server to use and the content categories to block. Then you can apply the WebBlocker profile to a user-defined HTTP or HTTP proxy policy.

When a user tries to visit a web site, your XTM device sends a request to the WebBlocker Server to find out if the user can get access to that web site based on the site category. The result of this request is saved in a cache. You can change the size of this cache to improve performance.

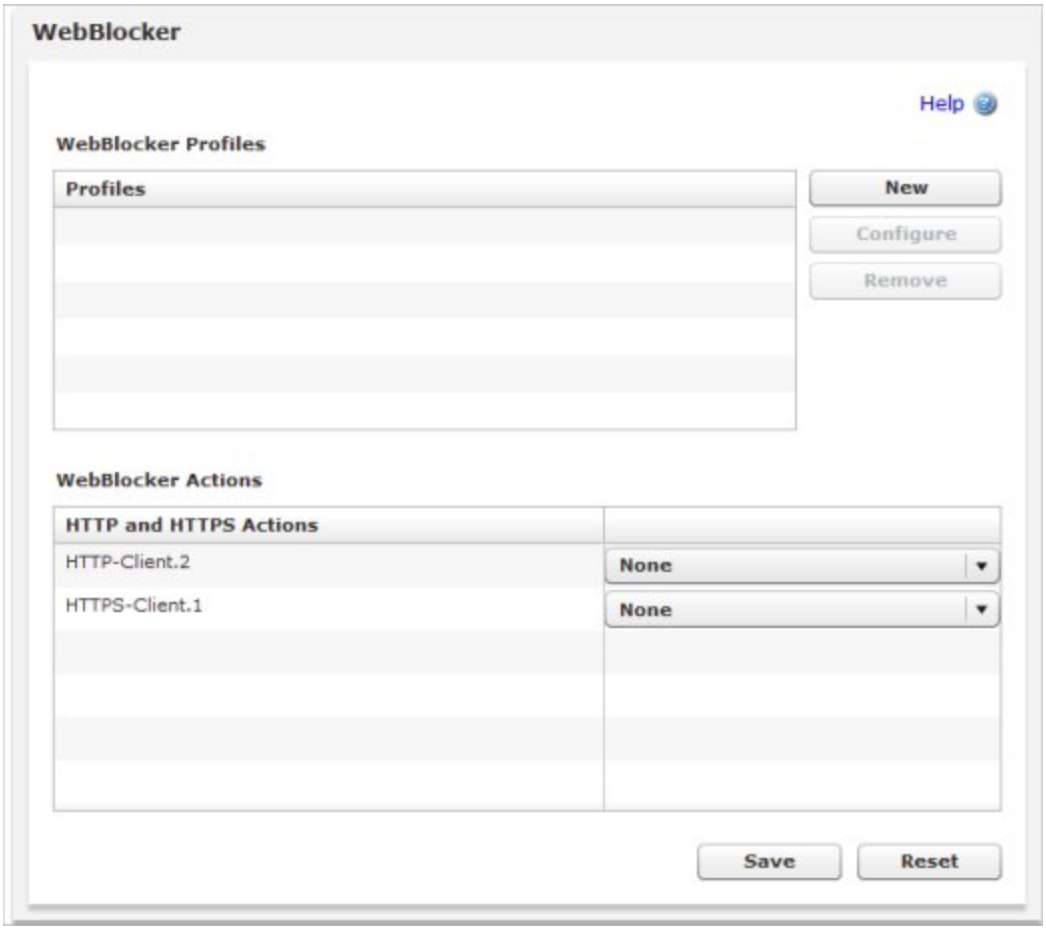
Before You Begin

For all XTM devices except the XTM 2 Series, you must install a local WebBlocker server before you can configure WebBlocker.

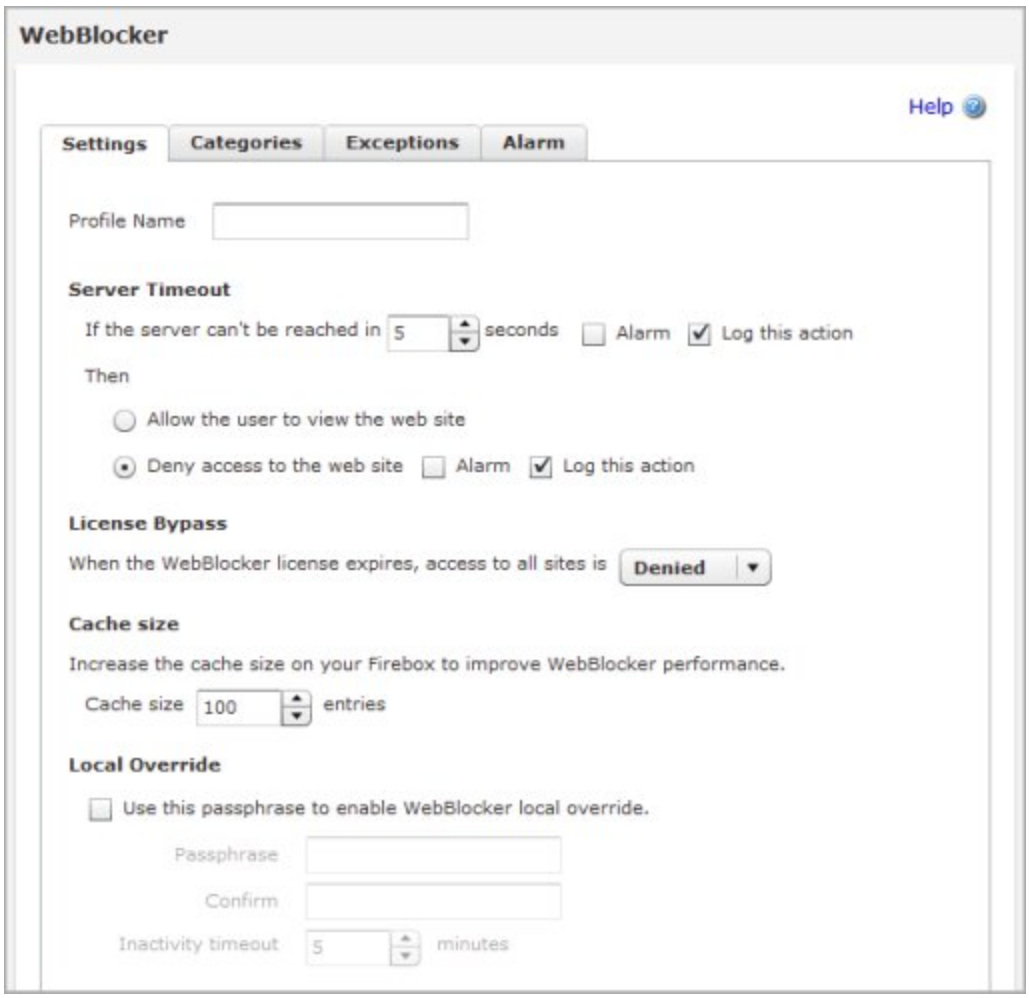
For more information, see *Configure a Local WebBlocker Server* on page 669.

Create WebBlocker Profiles

1. Select **Subscription Services > WebBlocker**.
   The WebBlocker page appears.



2. In the **WebBlocker Profiles** section, click **New**.
   The WebBlocker settings page appears.



3. In the **Profile Name** text box, type a name for the WebBlocker profile.
4. In the **Server Timeout** section, set the server timeout settings:

If your Firebox cannot connect to the WebBlocker server in

Set the number of seconds to try to connect to the server before the XTM device times out.

Alarm

Select to send an alarm when the XTM device cannot connect to the WebBlocker Server and times out. To set parameters for the alarms, click the **Alarm** tab. For information about the settings on the **Alarm** tab, see *Set Logging and Notification Preferences* on page 466.

Log this action

Select to send a message to the log file if the XTM device times out.

Allow the user to view the web site

Select if you want to allow the user to see the web site if the XTM device times out and does not connect to the WebBlocker Server.

Deny access to the web site

Select to deny access if the XTM device times out.

Optionally select the Alarm or Log this action

5. To control whether users on your network can access web sites if WebBlocker is enabled but the WebBlocker security subscription expires, from the **When the WebBlocker license expires, access to all sites is** drop-down list, select one of these options:

   Denied

   Select this option to block access to all web sites when the WebBlocker license expires.

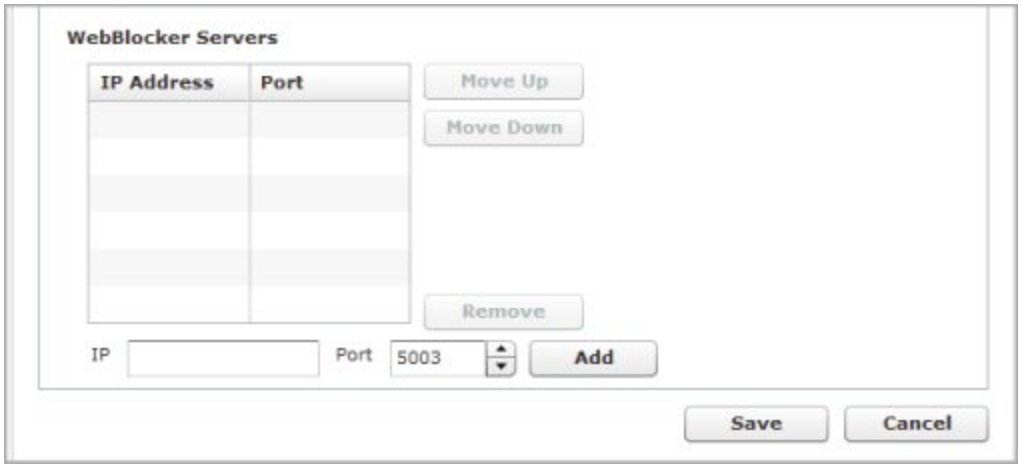
   Allowed

   Select this option to allow access to all web sites when the WebBlocker license expires.

   By default, License Bypass is configured to block access to all web sites if your WebBlocker security subscription is expired. This is the most secure option if you must block your users from specific types of content.

   For information about how to renew your security subscription, see *Renew Security Subscriptions* on page 79.

6. To improve WebBlocker performance, increase the **Cache Size** value.
7. In the **WebBlocker Servers** section, configure a WebBlocker Server.



If your XTM device is a 2 Series model, you can either use a WebBlocker Server hosted by WatchGuard or use a local WebBlocker server. To use the WatchGuard hosted WebBlocker Server, select the **Use WatchGuard hosted WebBlocker Server** check box. This option is only available if your device is an XTM 2 Series.

To add an entry for a local WebBlocker Server:

- In the **IP** text box, type the IP address of your WebBlocker Server.
- In the **Port** text box, type or select the port number. The default port number for the WebBlocker Server is 5003.
- To add the WebBlocker Server to the list, click **Add**.

You can add a second WebBlocker Server to use as a backup server if the XTM device cannot connect to the primary server. Follow the same steps to add a backup WebBlocker Server. The first server in the list is the primary server.

- To move a server higher or lower in the list, click the server IP address and click **Move Up** or **Move Down**.
- To remove a server from the list, select it and click **Remove**.

Enable Local Override

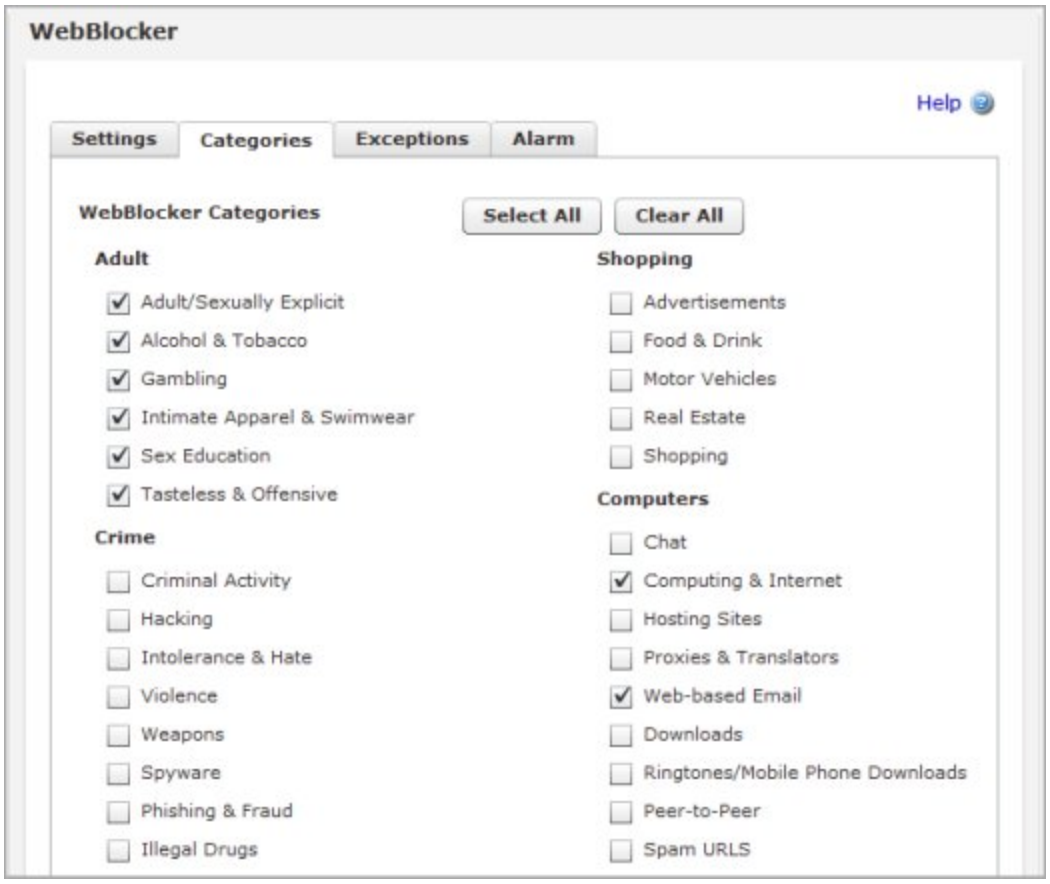
When you enable WebBlocker local override, if a user tries to connect to a site that is denied by WebBlocker the user is prompted to enter the override password. When the user enters the correct password, WebBlocker allows the user to go to the destination web site until the inactivity timeout is reached or until an authenticated user logs out. This feature operates only with HTTP proxy policies. For more information about local override, see *Use WebBlocker Local Override* on page 676.

To allow users to bypass WebBlocker if they have the correct passphrase:

1. In the **Local Override** section, select the **Use this passphrase and inactivity timeout to enable WebBlocker local override** check box.
2. In the **Passphrase** text box, type the passphrase.
3. In the **Confirm** text box, type the same password again.
4. (Optional) Change the **Inactivity Timeout** value.

Select Categories to Block

1. Select the **Categories** tab.
   The list of WebBlocker categories appears.



2. Select the check boxes adjacent to the categories of web sites you want to block in this WebBlocker profile.

   For more information on WebBlocker categories, see *About WebBlocker Categories* on page 677.

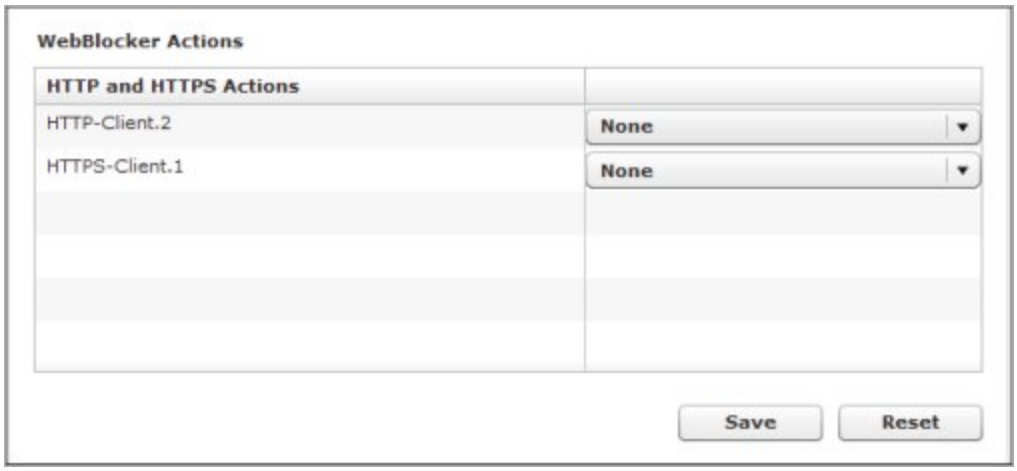
3. To create a log message when a web site is denied based on a category you choose to block, select the **Log this action** check box.
4. Click **Save**.
   The WebBlocker policy is added to the list.

Use the WebBlocker Profile with HTTP and HTTPS Proxies

You can use the WebBlocker profile you created with user-defined HTTP and HTTPS proxy actions. For more information about proxy actions, see *About Proxy Actions*.

On the WebBlocker page:

1. In the **WebBlocker Actions** section, in the **HTTP and HTTPS Actions** list, adjacent to each user-defined proxy action, click the drop-down list and select a WebBlocker profile.



2. Click **Save**.

Add WebBlocker Exceptions

To always allow or deny access to specific web sites, regardless of the WebBlocker category, select the **Exceptions** tab. You can add the URL or URL pattern of sites you want WebBlocker to always allow or deny.

For more information about how to add WebBlocker exceptions, see *Add WebBlocker Exceptions* on page 681.

Use WebBlocker Local Override

WebBlocker local override is a feature that allows a user to type an override password to go to a web site that is blocked by the WebBlocker policy. For example, in a school, a teacher could use the override password to allow a student to access an approved site that is blocked by WebBlocker content categories.

When a user tries to go to a site that is blocked by the WebBlocker policy, if local override is enabled, the user sees a deny message in the browser.

If the XTM device uses a self-signed certificate for authentication, the user can also see a certificate warning. We recommend that you install a trusted certificate on the XTM device for this purpose, or import the self-signed certificate on each client device.

To get access to the requested site, the user must type the override destination and the override password.

1. In the **Override destination** text box, type the URL to allow access to. By default, the override destination is set to the URL that was blocked. You can use wildcards in the override destination to allow access to more than one site, or more pages in one site. Examples of override destinations that use wildcards:

   *.amazon.com

   allows access to all subdomains. of amazon.com

   *amazon.com

   allows access to all domain names that end with amazon.com, such as images-amazon.com

   www.amazon.com/books-used-books-textbooks/*

   allows access to only pages in that path

2. In the **Override Password** text box, type the override password configured in the WebBlocker profile.
3. Click **Submit**.

After the user types the correct override password, the XTM device allows access to the override destination until an authenticated user logs out, or until there is no traffic to a matching site for the amount of time specified in the WebBlocker local override inactivity timeout. You enable local override and set the local override inactivity timeout in the WebBlocker profile..

For more information about how to configure WebBlocker local override, see *Get Started with WebBlocker* on page 670.

About WebBlocker Categories

The WebBlocker database contains nine category groups, with 54 web site categories.

A web site is added to a category when the contents of the web site meet the correct criteria. Web sites that give opinions or educational material about the subject matter of the category are not included. For example, the **Illegal Drugs** category denies sites that tell how to use marijuana. They do not deny sites with information about the historical use of marijuana.

SurfControl periodically adds new web site categories. The new categories do not appear on the WebBlocker configuration page until WatchGuard updates the software to add the new categories.

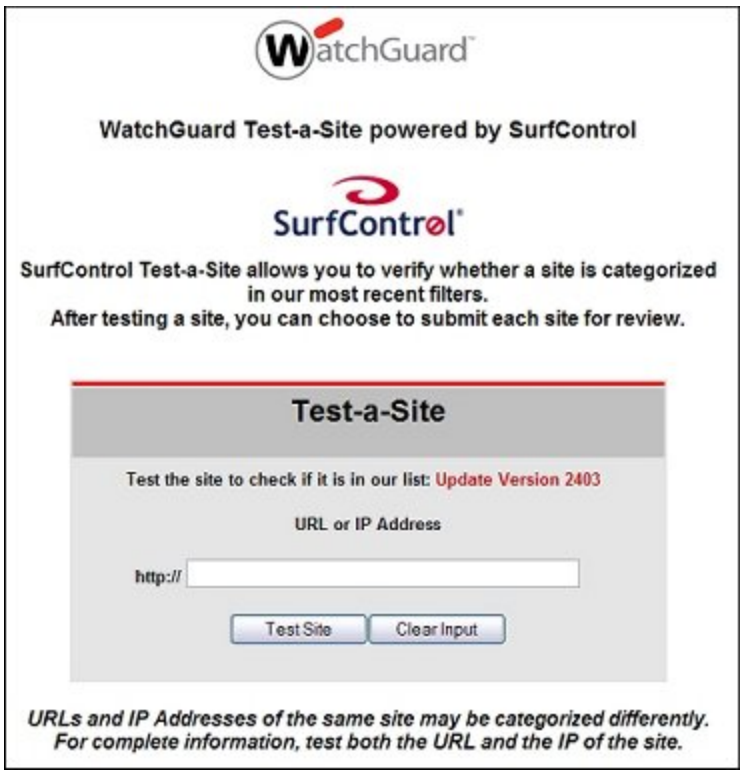
To block sites that meet the criteria for a new SurfControl category that is not yet part of a WebBlocker software update, select the **Other** category.

To block sites that do not meet the criteria for any other category, select the **Uncategorized** category.

See Whether a Site is Categorized

To see whether WebBlocker denies access to a web site as part of a category block, go to the Test-a-Site page on the SurfControl web site.

1. Open a web browser and go to http://mtas2.surfcontrol.com/mtas/WatchGuardTest-a-Site_MTAS.asp.
   The WatchGuard Test-a-Site page appears.



2. Type the URL or IP address of the site to check.
3. Click **Test Site**.
   The WatchGuard Test-a-Site Results page appears.

Add, Remove, or Change a Category

If you get a message that the URL you entered is not in the SurfControl list, you can submit it on the Test Results page.

1. On the **Test Results** page, click **Submit A Site**.
   The Submit A Site page appears.

2. Select whether you want to **Add a site**, **Delete a site**, or **Change the category**.
3. Type the site URL.
4. To request that the category assigned to a site is changed, select the new category from the drop-down list.
5. Click **Submit**.

About WebBlocker Exceptions

WebBlocker could deny a web site that is necessary for your business. You can override WebBlocker when you define a web site usually denied by WebBlocker as an *exception* to allow users to get access to it. For example, suppose employees in your company frequently use web sites that contain medical information. Some of these web sites are forbidden by WebBlocker because they fall into the sex education category. To override WebBlocker, you specify the web site domain name. You can also deny sites that WebBlocker usually allows

WebBlocker exceptions apply only to HTTP traffic. If you deny a site with WebBlocker, the site is not automatically added to the Blocked Sites list.

To add WebBlocker exceptions, see *Add WebBlocker Exceptions* on page 681.

Define the Action for Sites that do not Match Exceptions

In the **Use category list** section below the list of exception rules, you can configure the action to occur if the URL does not match the exceptions you configure. By default the **Use the WebBlocker category list to determine accessibility** radio button is selected, and WebBlocker compares sites against the categories you selected on the **Categories** tab to determine accessibility.

You can also choose not to use the categories at all and instead use exception rules only to restrict web site access. To do this, click the **Deny website access** radio button.

Log this action

Select to send a message to the log file when the XTM device denies a WebBlocker exception.

Components of Exception Rules

You can have the XTM device block or allow a URL with an exact match. Usually, it is more convenient to have the XTM device look for URL patterns. The URL patterns do not include the leading "http://". To match a URL path on all web sites, the pattern must have a trailing “/*”.

Exceptions with Part of a URL

You can create WebBlocker exceptions with the use of any part of a URL. You can set a port number, path name, or string that must be blocked for a special web site. For example, if it is necessary to block only www.sharedspace.com/~dave because it has inappropriate photographs, you type “www.sharedspace.com/~dave/*”. This gives the users the ability to browse to www.sharedspace.com/~julia, which could contain content you want your users to see.

To block URLs that contain the word “sex” in the path, you can type “*/*sex*”. To block URLs that contain “sex” in the path or the host name, type “*sex*”.

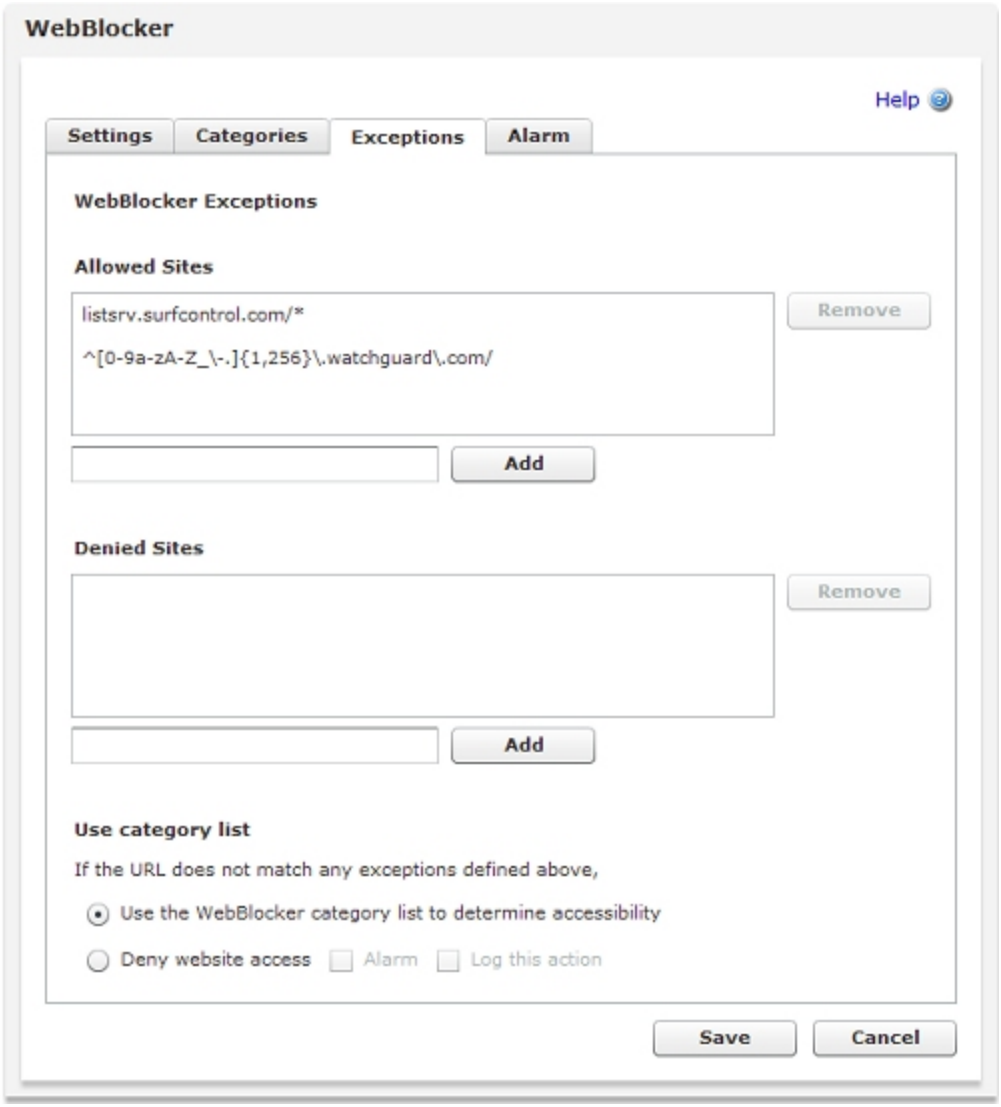
You can block ports in an URL. For example, look at the URL http://www.hackerz.com/warez/index.html:8080. This URL has the browser use the HTTP protocol on TCP port 8080 instead of the default method that uses TCP 80. You can block the port by matching *8080.

Add WebBlocker Exceptions

From Fireware XTM Web UI, you can add an exception that is an exact match of a URL, or you can use the wildcard symbol "*" in the URL to match any character. For example, if you add "www.example.com" to the Allowed Sites list, and a user types "www.example.com/news", the request is denied. If you add "www.example.com/*" to the Allowed Sites list, WebBlocker allows requests to go to all URL paths on the www.example.com web site.

To add exceptions:

1. Select **Subscription Services > WebBlocker**.
   The WebBlocker page appears.
2. In the **WebBlocker Profiles** section, adjacent to the WebBlocker policy, click **Configure**.
   The WebBlocker policy settings appear.
3. Select the **Exceptions** tab.



4. In the text box below the **Allowed Sites** list, type the exact URL or URL pattern of a site you want to always allow access to. Click **Add** to add it to the Allowed Sites exceptions list.
5. In the text box below the **Denied Sites** list, type the exact URL or URL pattern of a site you want to always deny access to. Click **Add** to add it to the Denied Sites list.

   Note *When you type a URL exception,do not include the leading "http://". You can use the wildcard symbol, *, to match any character. For example, the exception www.somesite.com/* will match all URL paths on the www.somesite.com web site. You can use more than one wildcard in a URL exception.*

6. In the **Use category list** section, you can configure the action to take if the URL does not match the exceptions you configure. The default setting is that the **Use the WebBlocker category list to determine accessibility** radio button is selected, and WebBlocker compares sites against the categories you selected on the **Categories** tab to determine accessibility.

   You can also choose to not use the categories at all, and instead use exception rules only to restrict web site access. There are two ways you can do this:

   - To deny access to all sites not listed on the exceptions list, select **Deny website access**.
   - To allow access to all sites not listed on the exceptions list, select **Use the WebBlocker category list to determine accessibility**. Then, make sure that no categories are selected on the **Categories** tab.

7. Click **Save**.

Define WebBlocker Alarms

To configure notification parameters for WebBlocker alarms, select the **Alarm** tab on the WebBlocker configuration page.

You can send an alarm when the XTM device cannot connect to the WebBlocker Server and times out, or when the XTM device times out and access to a site is denied. For information about the **Alarm** tab settings, see *Set Logging and Notification Preferences* on page 466.

About WebBlocker Subscription Services Expiration

If your site uses WebBlocker, you must renew or disable the WebBlocker subscription as soon as it expires to prevent an interruption in web browsing. WebBlocker has a default setting that blocks all traffic when the connections to the server time out. When your WebBlocker expires, it no longer contacts the server. This appears to the XTM device as a server timeout. All HTTP traffic is blocked unless this default was changed before expiration.

To change this setting:

1. On the **WebBlocker** configuration page, select the **Settings** tab.
2. In the **License Bypass** section, change the setting to **Allowed**.

25 spamBlocker

About spamBlocker

Unwanted email, also known as spam, fills the average Inbox at an astonishing rate. A large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources. The WatchGuard spamBlocker option uses industry-leading pattern detection technology from Commtouch to block spam at your Internet gateway and keep it away from your email server.

Commercial mail filters use many methods to find spam. Blacklists keep a list of domains that are used by known spam sources or are open relays for spam. Content filters search for key words in the header and body of the email message. URL detection compares a list of domains used by known spam sources to the advertised link in the body of the email message. However, all of these procedures scan each individual email message. Attackers can easily bypass those fixed algorithms. They can mask the sender address to bypass a blacklist, change key words, embed words in an image, or use multiple languages. They can also create a chain of proxies to disguise the advertised URL.

spamBlocker uses the Recurrent-Pattern Detection (RPD) solution created by Commtouch to detect these hard-to-find spam attacks. RPD is an innovative method that searches the Internet for spam outbreaks in real time. RPD finds the patterns of the outbreak, not only the pattern of individual spam messages. Because it does not use the content or header of a message, it can identify spam in any language, format, or encoding. To see an example of real-time spam outbreak analysis, visit the Commtouch Outbreak Monitor at: http://www.commtouch.com/Site/ResearchLab/map.asp

spamBlocker also provides optional virus outbreak detection functionality. For more information, see *Enable and Set Parameters for Virus Outbreak Detection (VOD)* on page 696.

To see statistics on current spamBlocker activity, select **Dashboard > Subscription Services**.

spamBlocker Requirements

Before you enable spamBlocker, you must have:

- A spamBlocker feature key — To get a feature key, contact your WatchGuard reseller or go to the WatchGuard LiveSecurity web site at: http://www.watchguard.com/store
- POP3 or SMTP email server — spamBlocker works with the WatchGuard POP3 and incoming SMTP proxies to scan your email. If you have not configured the POP3 or SMTP proxy, they are enabled when you configure the spamBlocker service. If you have more than one proxy policy for POP3 or for SMTP, spamBlocker works with all of them.
- DNS configured on your XTM device — In Fireware XTM Web UI, select **Network > Interfaces**. In the **DNS Servers** list, add the IP addresses of the DNS servers your XTM device uses to resolve host names.
- A connection to the Internet

spamBlocker Actions, Tags, and Categories

The XTM device uses spamBlocker actions to apply decisions about the delivery of email messages. When a message is assigned to a category, the related action is applied. Not all actions are supported when you use spamBlocker with the POP3 proxy.

Allow

Let the email message go through the XTM device.

Add subject tag

Let the email message go through the XTM device, but insert text in the subject line of the email message to mark it as spam or possible spam. You can keep the default tags or you can customize them, as described in the spamBlocker tags section below. You can also create rules in your email reader to sort the spam automatically, as described in *Create Rules for Your Email Reader* on page 697.

Quarantine (SMTP only)

Send the email message to the Quarantine Server. Note that the **Quarantine** option is supported only if you use spamBlocker with the SMTP proxy. The POP3 proxy does not support this option.

Deny (SMTP only)

Stop the email message from being delivered to the mail server. The XTM device sends this 571 SMTP message to the sending email server: *Delivery not authorized, message refused*.The **Deny** option is supported only if you use spamBlocker with the SMTP proxy. The POP3 proxy does not support this option.

Drop (SMTP only)

Drop the connection immediately. The XTM device does not give any error messages to the sending server. The **Drop** option is supported only if you use spamBlocker with the SMTP proxy. The POP3 proxy does not support this option.

spamBlocker tags

If you select the spamBlocker action to add a tag to certain email messages, the XTM device adds a text string to the subject line of the message. You can use the default tags provided, or you can create a custom tag. The maximum length of the tag is 30 characters.

This example shows the subject line of an email message that was found to be spam. The tag added is the default tag: ***SPAM***.

```
Subject: ***SPAM*** Free auto insurance quote
```

This example shows a custom tag: [SPAM]

```
Subject: [SPAM] You've been approved!
```

spamBlocker Categories

The Commtouch Recurrent-Pattern Detection (RPD) solution classifies spam attacks in its Anti-Spam Detection Center database by severity. spamBlocker queries this database and assigns a category to each email message.

spamBlocker has three categories:

The **Confirmed Spam** category includes email messages that come from known spammers. If you use spamBlocker with the SMTP proxy, we recommend you use the **Deny** action for this type of email.If you use spamBlocker with the POP3 proxy, we recommend you use the **Add subject tag** action for this type of email.

The **Bulk** category includes email messages that do not come from known spammers, but do match some known spam structure patterns. We recommend you use the **Add subject tag** action for this type of email, or the **Quarantine** action if you use spamBlocker with the SMTP proxy.

The **Suspect** category includes email messages that look like they could be associated with a new spam attack. Frequently, these messages are legitimate email messages. We recommend that you consider a suspect email message as a *false positive* and therefore not spam unless you have verified that is not a false positive for your network. We also recommend that you use the **Allow** action for suspect email, or the **Quarantine** action if you use spamBlocker with the SMTP proxy.

See the spamBlocker Category for a Message

After spamBlocker categorizes a message, it adds the spam category to the full email message header as a spam score.

To find the spam score for a message, open the full email message header.

If you have Microsoft Outlook, open the message, select **View > Options**, and look in the **Internet headers** dialog box.
The spam score appears in this line:

```
X-WatchGuard-Spam_Score:
```

For example:

```
X-WatchGuard-Spam-Score: 3, bulk; 0, no virus
```

The first number on this line is the spam category. This number has one of these values:

0 - clean

1 - clean

2 - suspect

3 - bulk

4 - spam

If you enable Virus Outbreak Detection (VOD) in your spamBlocker configuration, the spam score in the email message header has a second number, the VOD category. This number has one of these values:

0 - no virus

1 - no virus

2 - virus threat possible

3 - virus threat high

Configure spamBlocker

You can enable spamBlocker for the SMTP or POP3 proxy.

Before You Begin

Before you can configure spamBlocker for a proxy policy, you must configure the policy to use a user-defined proxy action. To create a user-defined proxy action, you can clone the default (predefined) proxy action, and then apply that proxy action to the proxy policy.

To find the proxy action your policy uses:

1. Select **Firewall > Firewall Policies**.
2. Select the proxy policy. Click .
   The Policy Configuration page appears. The Proxy Action drop-down list appears at the top of the page.
3. Verify whether the proxy action is a predefined or user-defined proxy action.
   For more information about proxy actions, see *About Proxy Actions*.

If the proxy uses a predefined proxy action that you want to change, you must first clone the proxy action.

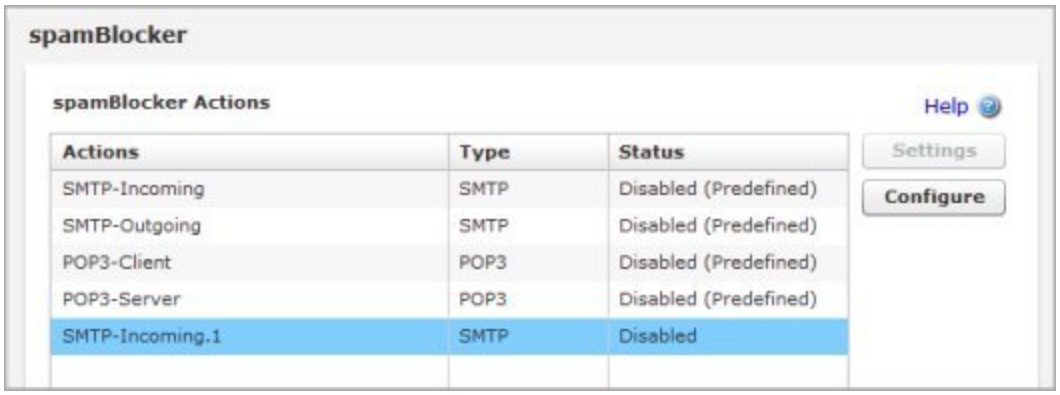
1. Select **Firewall > Proxy Actions**.
2. Select the proxy action that your proxy policy uses.
3. Click **Clone**.
4. Type a new name for the cloned proxy action.
5. Edit the proxy action.
   For more information, see *About Proxy Actions*.

If you cloned the proxy action, edit the policy to select the cloned proxy action.

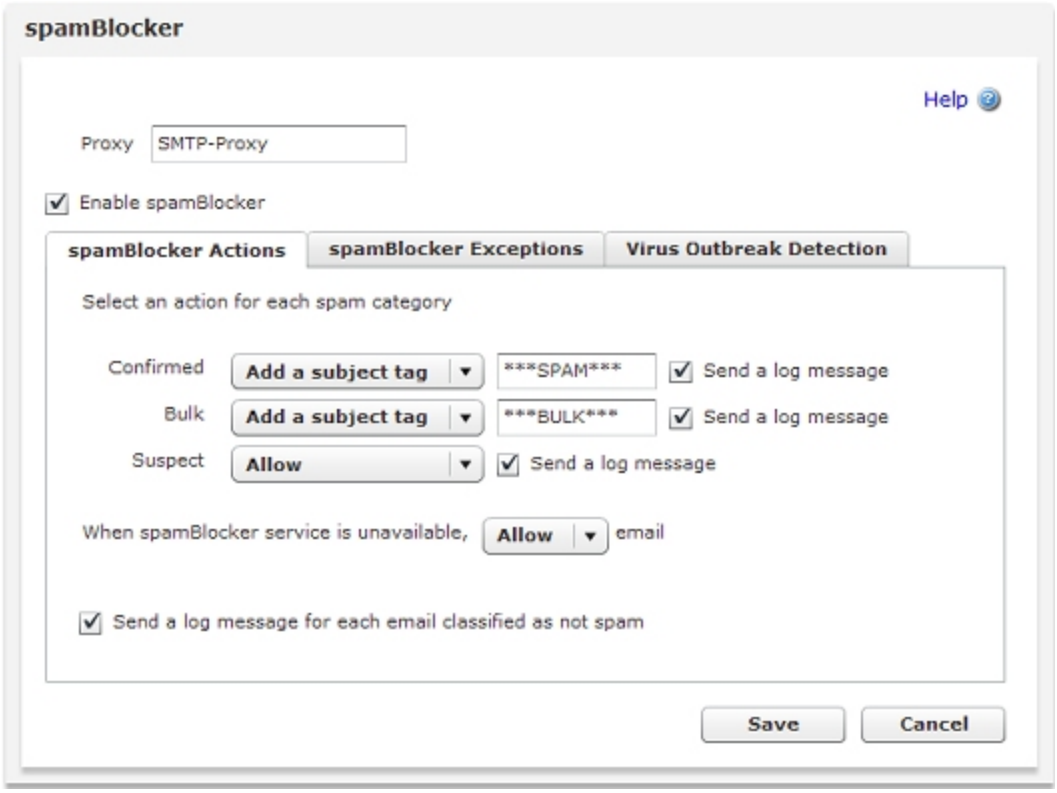
1. Select **Firewall > Firewall Policies**.
2. Select the proxy. Click .
   The Policy Configuration page appears.
3. From the **Proxy-Action** drop-down list, select the name of the new proxy action.
4. Click **Save**.

Configure spamBlocker for an SMTP or POP3 Proxy Action

1. Select **Subscription Services > spamBlocker**.
   The spamBlocker configuration page appears, with a list of the SMTP and POP3 proxy actions on your XTM device and whether spamBlocker is enabled for each one.



2. In the **spamBlocker Action**s list, select a user-defined SMTP or POP3 proxy action. Click **Configure**. You cannot configure spamBlocker for a predefined proxy action.
   The spamBlocker configuration settings appear.



3. Select the **Enable spamBlocker** check box.
4. Set the actions spamBlocker applies for each category of email in the drop-down lists adjacent to **Confirm**, **Bulk**, and **Suspect**. If you select **Add subject tag** for any category, you can change the default tag that appears in the text box to the right of the drop-down list.
   For more information on spamBlocker tags, see *spamBlocker Actions, Tags, and Categories* on page 684.
5. If you want to send a log message each time spamBlocker takes an action, select the **Send a log message** check box for the action. If you do not want to record log messages for an action, clear this check box.
6. The **When the spamBlocker server is unavailable** drop-down list specifies how the XTM device handles incoming email when the spamBlocker server cannot be contacted. We recommend you use the default **Allowed** action.

   - If you set this option to **Denied** for the POP3 or SMTP proxy, it causes a conflict with Microsoft Outlook. When Outlook starts a connection to the email server, spamBlocker tries to contact the spamBlocker server. If the spamBlocker server is not available, spamBlocker stops the email download. When this happens, a cycle starts. Outlook tries to download email and spamBlocker stops the download. This continues until the XTM device can connect to the spamBlocker server, or the request is dropped because the proxy times out, or you cancel the request.
   - If you set this option to **Denied** with the SMTP proxy, the XTM device sends this 450 SMTP message to the sending email server: “Mailbox is temporarily unavailable.”

7. The **Send log message for each email classified as not spam** check box specifies whether a message is added to the log file if an email message is scanned by spamBlocker but is not designated as Confirmed Spam, Bulk, or Suspect. Select this check box if you want to add a message to the log file in this situation.
8. (Optional) Add spamBlocker exception rules, as described in *About spamBlocker Exceptions* on page 689.
9. Configure Virus Outbreak Detection actions, as described in *Configure Virus Outbreak Detection Actions for a Policy* on page 691.
10. Click **Save**.

> ***Note*** *If you have any perimeter firewall between the XTM device that uses spamBlocker and the Internet, it must not block HTTP traffic. The HTTP protocol is used to send requests from the XTM device to the spamBlocker server.*

After you enable spamBlocker for a proxy action or policy, you can define global spamBlocker settings. These settings apply to all spamBlocker configurations. Click **Settings** to see or modify the global spamBlocker configuration settings. For more information, see *Set Global spamBlocker Parameters* on page 692.

About spamBlocker Exceptions

You can create an exception list to the general spamBlocker actions that is based on the sender's or recipient's address. For example, if you want to allow a newsletter that spamBlocker identifies as Bulk email, you can add that sender to the exception list and use the **Allow** action regardless of the spamBlocker category the sender is assigned to. Or, if you want to apply a tag to a sender that spamBlocker designates as safe, you can add that to the exceptions list as well.

Make sure you use the sender's actual address that is listed in the "Mail-From" field in the email message header, which may not match the address in the "From:" field that you see at the top of the email message. To get the actual address for an exception, get the full email message header (from Microsoft Outlook, with the message open, select **View > Options** and look in the **Internet headers** box). The addresses of the sender and recipient are in these lines:

```
X-WatchGuard-Mail-From:
X-WatchGuard-Mail-Recipients:
```

Use care when you add wildcards to an exception. Spammers can spoof header information. The more specific the addresses in your exception list, the more difficult it will be to spoof them.

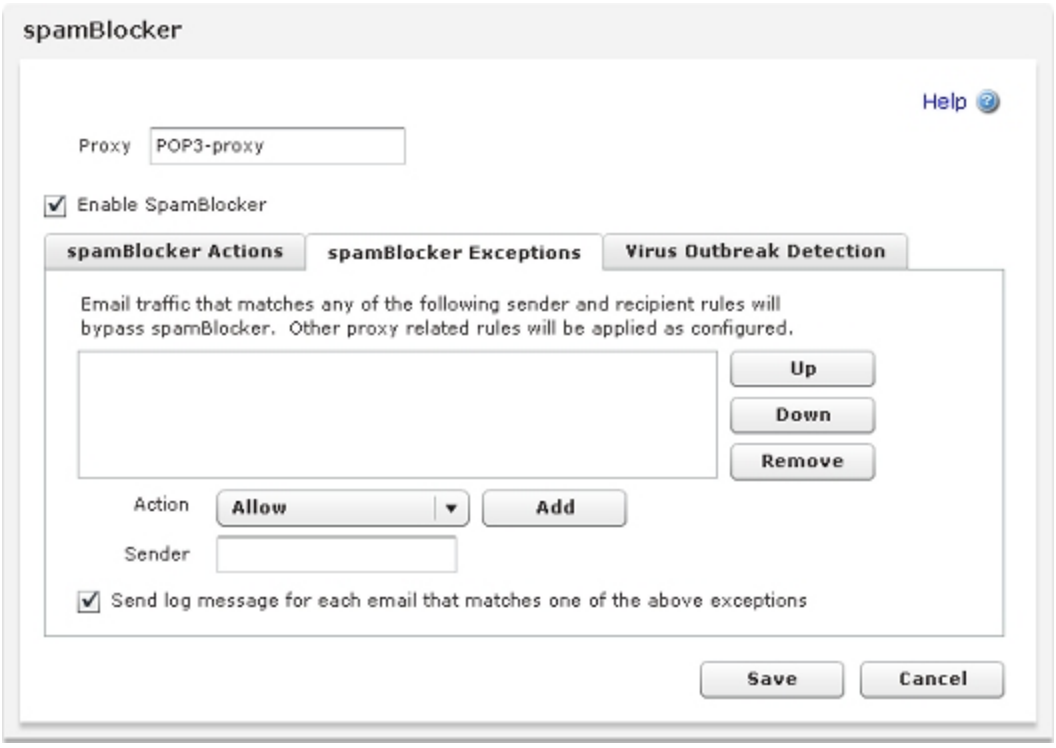
To add an exception rule, see *Add spamBlocker Exception Rules* on page 689.

To change the order of the rules listed in the dialog box, see *Change the Order of Exceptions* on page 691.

Add spamBlocker Exception Rules

After you enable spamBlocker, you can use Fireware XTM Web UI to define exceptions that allow email from specific senders to bypass spamBlocker.

1. Select **Subscription Services > spamBlocker**.
   The spamBlocker Configuration page appears.
2. Select a proxy policy and click **Configure**. Select the **Exceptions** tab.
   The spamBlocker configuration page appears, and shows the spamBlocker Exceptions list.



3. From the **Action** drop-down list, select a rule action: **Allow**, **Add subject tag**, **Quarantine**, **Deny**, or **Drop**. (Remember that the POP3 proxy supports only the **Allow** and **Add subject tag** actions in spamBlocker.)
4. Type a sender, a recipient, or both. You can type the full email address or use wildcards.
   Make sure you use the actual address of the sender. You can find this address in the "Mail-From" field in the email message header. This address may not match the address in the "From:" field that you see at the top of the email message. To get the actual address for an exception, get the full email message header (from Microsoft Outlook, with the message open, select **View > Options** and look in the **Internet headers** box). The addresses of the sender and recipient are in these lines:
   `X-WatchGuard-Mail-From:`
   `X-WatchGuard-Mail-Recipients:`
   Use care when you add wildcards to an exception. Spammers can spoof header information. The more specific the addresses in your exception list, the more difficult it will be to spoof them.
5. Click **Add**.
   The exception is added to the bottom of the exceptions list.
6. To send a log message each time an email matches one of the exceptions, select the **Log exceptions** check box.

The exceptions are processed in the order they appear in the list. To *Change the Order of Exceptions*, click **Up** and **Down**.

Change the Order of Exceptions

The order that the spamBlocker exception rules appear in the dialog box shows the order in which email messages are compared to the rules. The proxy policy compares messages to the first rule in the list and continues in sequence from top to bottom. When a message matches a rule, the XTM device performs the related action. It performs no other actions, even if the message matches a rule or rules later in the list.

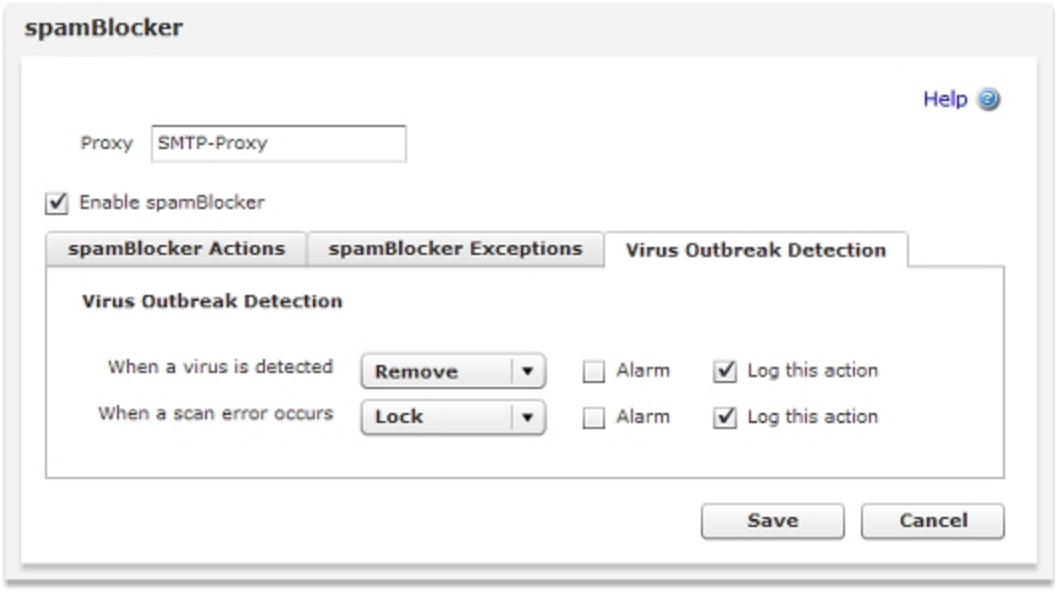
To change the order of rules, select the rule whose order you want to change. Click **Up** or **Down** to move the selected rule up or down in the list.

Configure Virus Outbreak Detection Actions for a Policy

Virus Outbreak Detection (VOD) is a technology that uses traffic analysis technology to identify email virus outbreaks worldwide within minutes and then provides protection against those viruses. Provided by Commtouch, an industry leader in email spam and virus protection, VOD is incorporated into the spamBlocker subscription service. After you enable spamBlocker you can use Fireware XTM Web UI to configure Virus Outbreak Detection.

To configure Virus Outbreak Detection actions:

1. Select **Subscription Services > spamBlocker**.
2. Make sure Virus Outbreak Detection is enabled:
   - On the **spamBlocker** page, click **Settings**.
   - On the **spamBlocker Settings** page, select the **VOD** tab.
   - Select the **Enable Virus Outbreak Detection (VOD)** check box.
     For more information, see *Enable and Set Parameters for Virus Outbreak Detection (VOD)* on page 696.
   - Click **Save**.
3. On the **spamBlocker** page, select a proxy policy and click **Configure**. Select the **Virus Outbreak Detection** tab.



4. From the **When a virus is detected** drop-down list, select the action the XTM device takes if VOD detects a virus in an email message.
5. From the **When a scan error occurs** drop-down list, select the action the XTM device takes when VOD cannot scan an email message or attachment.
   Attachments that cannot be scanned include binhex-encoded messages, certain encrypted files, or files that use a type of compression that we do not support such as password-protected Zip files.
6. Select the **Log this action** check boxes to send a log message when a virus is detected or when a scan error occurs.
7. Select the **Alarm** check boxes to send an alarm when a virus is detected or when a scan error occurs.

The SMTP proxy supports the **Allow**, **Lock**, **Remove**, **Quarantine**, **Drop**, and **Block** actions. The POP3 proxy supports only the **Allow**, **Lock**, and **Remove** actions.

For more information on these actions, see *spamBlocker Actions, Tags, and Categories* on page 684.

Configure spamBlocker to Quarantine Email

The WatchGuard Quarantine Server provides a safe, full-featured quarantine mechanism for any email messages suspected or known to be spam or to contain viruses. This repository receives email messages from the SMTP proxy and filtered by spamBlocker.

To configure spamBlocker to quarantine email:

1. When you configure spamBlocker (as described in *Configure spamBlocker* on page 687), you must make sure you enable spamBlocker for the SMTP proxy.
2. When you set the actions spamBlocker applies for different categories of email (as described in *Configure spamBlocker* on page 687), make sure you select the Quarantine action for at least one of the categories.

You can also select the **Quarantine** action for email messages identified by Virus Outbreak Detection to contain viruses. For more information, see *Configure Virus Outbreak Detection Actions for a Policy* on page 691.

About Using spamBlocker with Multiple Proxies

You can configure more than one SMTP or POP3 proxy policy to use spamBlocker. This lets you create custom rules for different groups in an organization. For example, you can allow all email to your management employees and use a spam tag for the marketing team.

If you want to use more than one proxy policy with spamBlocker, your network must use one of these configurations:

- Each proxy policy must send email to a different internal email server.
- You must set the external source or sources that can send email for each proxy policy.

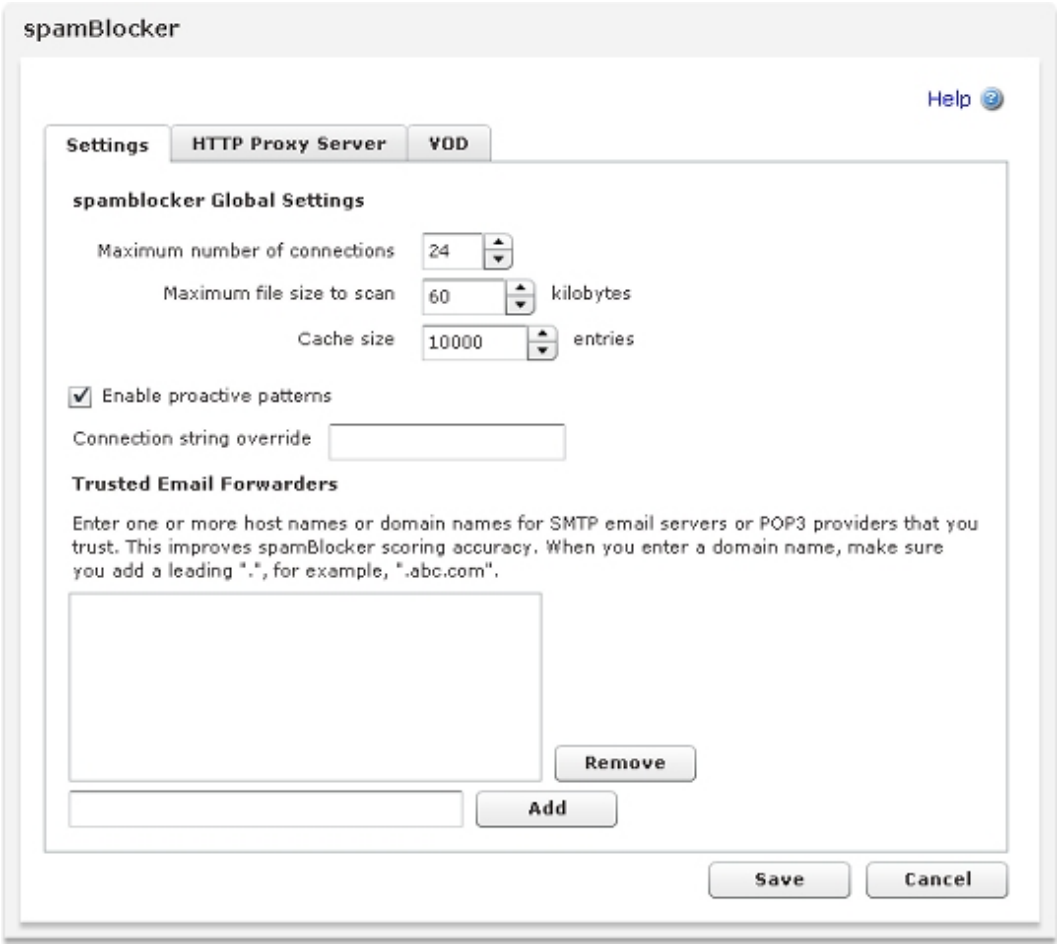
Set Global spamBlocker Parameters

You can use global spamBlocker settings to optimize spamBlocker for your own installation. Because most of these parameters affect the amount of memory that spamBlocker uses on the XTM device, you must balance spamBlocker performance with other XTM device functions.

> ***Note*** *To configure global spamBlocker settings, you must enable spamBlocker for at least one proxy policy.*

From Fireware XTM Web UI, you can configure the global parameters for spamBlocker.

1. Select **Subscription Services > spamBlocker**.
2. Click **Settings**.
   The spamBlocker settings page appears.



3. spamBlocker creates a connection for each message it processes. This connection includes information about the message that is used to generate its spam score. spamBlocker sets a default maximum number of connections that can be simultaneously buffered according to your XTM device model. You can use the **Maximum number of connections** text box to increase or decrease this value. If the amount of traffic handled by your proxy policies is low, you can increase the number of supported connections for spamBlocker without affecting performance. If you have limited available memory on the XTM device, you may want to decrease the value in this field.
4. In the **Maximum file size to scan** text box, type or select the number of bytes of an email message to be passed to spamBlocker to be scanned. Usually, 20–40K is enough for spamBlocker to correctly

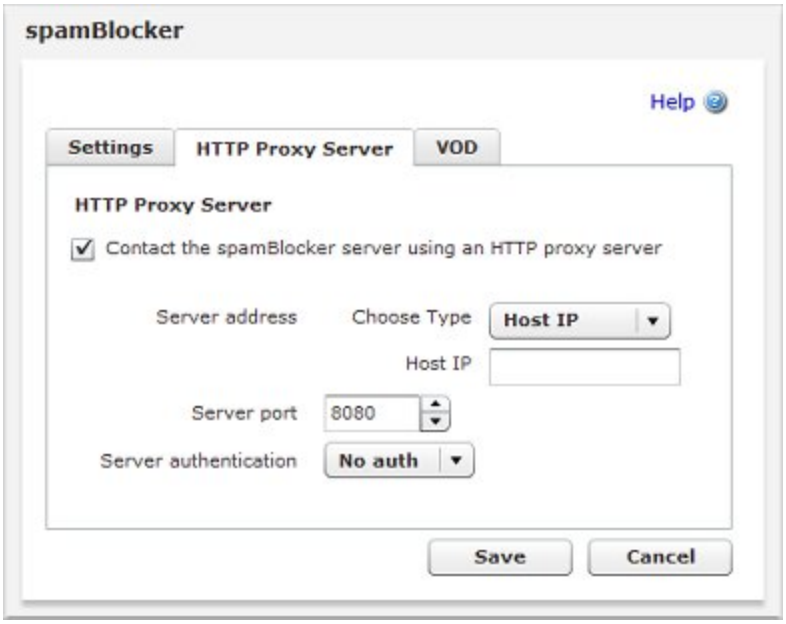
detect spam. However, if image-based spam is a problem for your organization, you can increase the maximum file size to block more image-based spam.
For information about the default and maximum scan limits for each XTM device model, see *About spamBlocker and VOD Scan Limits* on page 696.

5. In the **Cache size** text box, enter the number of entries spamBlocker caches locally for messages that have been categorized as spam and bulk. A local cache can improve performance because network traffic to Commtouch is not required. Usually, you do not have to change this value.
You can set the **Cache size** to 0 to force all email to be sent to Commtouch. This is most often used only for troubleshooting.
6. Clear the **Enabled** check box adjacent to **Proactive Patterns** if you want to disable the Commtouch CT Engine Proactive Patterns feature. This feature is automatically enabled. This feature uses a large amount of memory while the local database is updated. If you have limited memory or processor resources, you may want to disable this feature.
7. The **Connection string override** text box is used only when you must troubleshoot a spamBlocker problem with a technical support representative. Do not change this value unless you are asked to give additional debug information for a technical support problem.
8. You can also define several other optional parameters for spamBlocker:
   - *Enable and Set Parameters for Virus Outbreak Detection (VOD)*
   - *Use an HTTP Proxy Server for spamBlocker*
   - *Add Trusted Email Forwarders to Improve Spam Score Accuracy*
9. Click **Save**.

Use an HTTP Proxy Server for spamBlocker

If spamBlocker must use an HTTP proxy server to connect to the CommTouch server through the Internet, you must configure the HTTP proxy server settings on the **spamBlocker Settings** page.

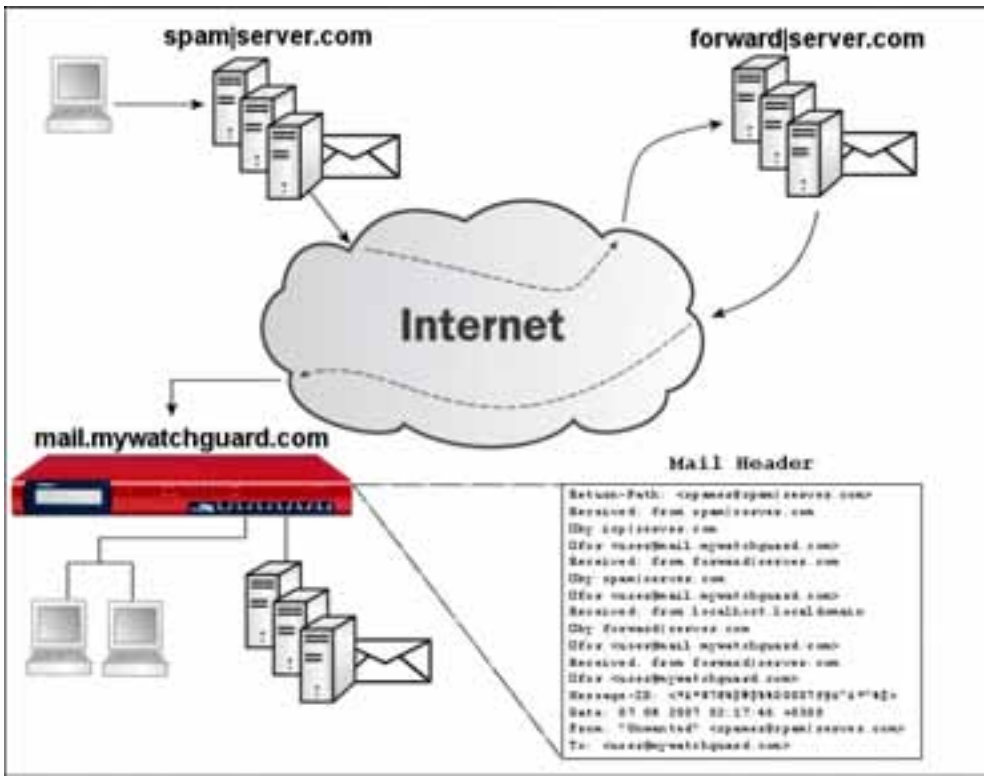
1. On the spamBlocker page, click **Settings**.
2. Click the **HTTP Proxy Server** tab.



3. On the **HTTP Proxy Server** tab, select the **Contact the spamBlocker using an HTTP Proxy server** check box.
4. Use the other fields in this tab to set up parameters for the proxy server, which include the address of the proxy server, the port the XTM device must use to contact the proxy server, and authentication credentials for the XTM device to use for proxy server connections (if required by the proxy server).

Add Trusted Email Forwarders to Improve Spam Score Accuracy

Part of the spam score for an email message is calculated using the IP address of the server that the message was received from. If an email forwarding service is used, the IP address of the forwarding server is used to calculate the spam score. Because the forwarding server is not the initial source email server, the spam score can be inaccurate.



To improve spam scoring accuracy, you can enter one or more host names or domain names of email servers that you trust to forward email to your email server. If you use SMTP, enter one or more host names or domain names for SMTP email servers that you trust to forward messages to your email server. If you use POP3, enter domain names for known or commonly used POP3 providers that you trust to download messages from.

After you add one or more trusted email forwarders, spamBlocker ignores the trusted email forwarder in email message headers. The spam score is calculated using the IP address of the source email server.

1. From the **spamBlocker Settings** page, select the **Settings** tab.
2. Below the **Trusted Email Forwarders** list, type a host or domain name in the text box. Click **Add**.
   If you add a domain name, make sure you add a leading period (.) to the name, as in `.firebox.net`.
3. (Optional) Repeat Step 2 to add more trusted email forwarders.
4. Click **Save**.

Enable and Set Parameters for Virus Outbreak Detection (VOD)

Virus Outbreak Detection (VOD) is a technology that identifies email virus outbreaks worldwide within minutes and then provides protection against those viruses. Provided by Commtouch, an industry leader in email spam and virus protection,VOD catches viruses even faster than signature-based systems.

To enable and configure VOD:

1. On the **spamBlocker Settings** page, select the **VOD** tab.
2. Select the **Enable Virus Outbreak Detection (VOD)** check box.
3. By default, VOD scans inbound email messages up to a default size limit that is optimal for the XTM device model. You can increase or decrease this limit with the arrows adjacent to **VOD maximum file size to scan**.
   For information about the default and maximum scan limits for each XTM device model, see *About spamBlocker and VOD Scan Limits* on page 696.

VOD uses the larger of the maximum file size values set for VOD or spamBlocker. If the global spamBlocker value of the **Maximum file size to scan** field set on the **Settings** tab is greater than the **VOD maximum file size to scan** value, VOD uses the global spamBlocker value. For information about spamBlocker global settings, see *Set Global spamBlocker Parameters* on page 692.

In the proxy definitions for spamBlocker, you can set the actions for spamBlocker to take when a virus is found, as described in *Configure Virus Outbreak Detection Actions for a Policy* on page 691.

About spamBlocker and VOD Scan Limits

spamBlocker scans each file up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. The default and maximum scan limits can be different for each XTM device model.

File Scan Limits by XTM Device Model, in Kilobytes

Model	Minimum	Maximum	Default
XTM 2 Series	1	1000	60
XTM 5 Series	1	2000	100
XTM 8 Series	1	2000	100
XTM 1050	1	2000	100

For information about how to set the maximum file size to scan for spamBlocker and VOD, see *Set Global spamBlocker Parameters* on page 692 and *Enable and Set Parameters for Virus Outbreak Detection (VOD)* on page 696

Create Rules for Your Email Reader

To use the **Tag** action in spamBlocker, it is best to configure your email reader to sort messages. Most email readers, such as Outlook, Thunderbird, and Mac Mail, allow you to set rules that automatically send email messages with tags to a subfolder. Some email readers also let you create a rule to automatically delete the message.

Because you can use a different tag for each spamBlocker category, you can set a different rule for each category. For example, you can set one rule to move any email message with the ***BULK*** tag in the subject line to a Bulk subfolder in your Inbox. You can set another rule that deletes any email message with the ***SPAM*** tag in the subject line.

For instructions on how to configure the Microsoft Outlook email client, see *Send Spam or Bulk Email to Special Folders in Outlook* on page 697. For information about how to use this procedure on other types of email clients, look at the user documentation for those products.

> ***Note*** *If you use spamBlocker with the SMTP proxy, you can have spam email sent to the Quarantine Server. For more information on the Quarantine Server, see About the Quarantine Server on page 759.*

Send Spam or Bulk Email to Special Folders in Outlook

This procedure shows you the steps to create rules for bulk and suspect email in Microsoft Outlook. You can have email with a “spam” or “bulk” tag delivered directly to special folders in Outlook. When you create these folders, you keep possible spam email out of your usual Outlook folders, but you can get access to the email if it becomes necessary.

Before you start, make sure that you configure spamBlocker to add a tag for spam and bulk email. You can use the default tags, or create custom tags. The steps below describe how to create folders with the default tags.

1. From your Outlook Inbox, select **Tools > Rules and Alerts**.
2. Click **New Rule** to start the Rules wizard.
3. Select **Start from a blank rule**.
4. Select **Check messages when they arrive**. Click **Next**.
5. Select the condition check box: **with specific words in the subject**. Then, in the bottom pane, edit the rule description by clicking on **specific**.
6. In the **Search Text** dialog box, type the spam tag as ***SPAM***. If you use a custom tag, type it here instead.
7. Click **Add** and then click **OK**.
8. Click **Next**.
9. The wizard asks what you want to do with the message. Select the **move it to the specified folde**r check box. Then, in the bottom pane, click **specified** to select the destination folder.
10. In the **Choose a Folder** dialog box, click **New**.
11. In the folder name field, type `Spam`. Click **OK**.
12. Click **Next** two times.

13. To complete the rule setup, type a name for your spam rule and click **Finish**.
14. Click **Apply**.

Repeat these steps to create a rule for bulk email, using the bulk email tag. You can send bulk email to the same folder, or create a separate folder for bulk email.

Send a Report about False Positives or False Negatives

A false positive email message is a legitimate message that spamBlocker incorrectly identifies as spam. A false negative email message is a spam message that spamBlocker does not correctly identify as spam. If you find a false positive or false negative email message, you can send a report directly to Commtouch. You can also send a report about a false positive for a solicited bulk email message. This is a message that spamBlocker identifies as bulk email when a user actually requested the email message.

> ***Note*** *Do not send a report about a false positive when the email is assigned to the Suspect category. Because this is not a permanent category, Commtouch does not investigate error reports for suspected spam.*

You must have access to the email message to send a false positive or false negative report to Commtouch. You must also know the category (Confirmed Spam, Bulk) into which spamBlocker put the email message. If you do not know the category, see the "Find the category a message is assigned to" section below.

1. Save the email as a .msg or .eml file.
   You cannot forward the initial email message because Commtouch must see the email header. If you use email software such as Microsoft Outlook or Mozilla Thunderbird, you can drag and drop the email message into a computer desktop folder. If you use email software that does not have drag-and-drop functionality, you must select **File > Save As** to save the email message to a folder.
2. Create a new email message addressed to:
   `reportfp@blockspam.biz` for false positives
   `reportfn@blockspam.biz` for false negatives
   `reportso@blockspam.biz` for false positive solicited bulk email
3. Type the following on the subject line of your email message:
   `FP Report <Your Company Name> <Date of submission>` for false positives
   `FN Report <Your Company Name> <Date of submission>` for false negatives
   `FP Report <Your Company Name> <Date of submission>` for false positive solicited bulk email
4. Attach the .msg or .eml file to the email message and send the message.

If you have many messages to tell Commtouch about, you can put them all into one Zip file. Do not put the Zip file into a Zip archive. The Zip file can be compressed to only one level for Commtouch to analyze it automatically.

Use RefID Record Instead of Message Text

If you want to send a report to Commtouch but cannot send the initial email message because the information in the message is confidential, you can use the RefID record from the email header instead. The RefID record is the reference number for the transaction between the XTM device and the Commtouch Detection Center.

spamBlocker adds an X-WatchGuard-Spam-ID header to each email. The header looks like this:
`X-WatchGuard-Spam-ID: 0001.0A090202.43674BDF.0005-G-gg8BuArWNRyK9/VKO3E51A==`
The long sequence of numbers and letters after `X-WatchGuard-Spam-ID:` part of the header is the RefID record.

Instead of attaching the initial email, put the RefID record in the body of your email message. If you have more than one email message you want to send a report about, put each RefID record on a separate line.

To see email headers if you use Microsoft Outlook:

1. Open the email message in a new window or select it in Outlook.
2. If you open the email in a separate window, select **View > Options**.
   If you highlight the email in Outlook, right-click the email message and select **Options**.
   The headers appear at the bottom of the Message Options window.

To see email headers if you use Microsoft Outlook Express:

1. Open the email message in a new window or highlight it in Outlook Express.
2. If you open the email in a separate window, select **File > Properties**.
   If you highlight the email in Outlook Express, right-click the email and select **Properties**.
3. Click the **Details** tab to view the headers.

To see email headers if you use Mozilla Thunderbird:

1. Open the email messages in a new window.
2. Select **View > Headers > All**.

Find the Category a Message is Assigned To

Message tags are the only way to know which category a message is assigned to. Change the action to **Add subject tag** and use a unique sequence of characters to add to the beginning of the email subject line. For more information on how to use spamBlocker tags, see *spamBlocker Actions, Tags, and Categories* on page 684.

26 Reputation Enabled Defense

About Reputation Enabled Defense

You can use the Reputation Enabled Defense (RED) security subscription to increase the performance and enhance the security of your XTM device.

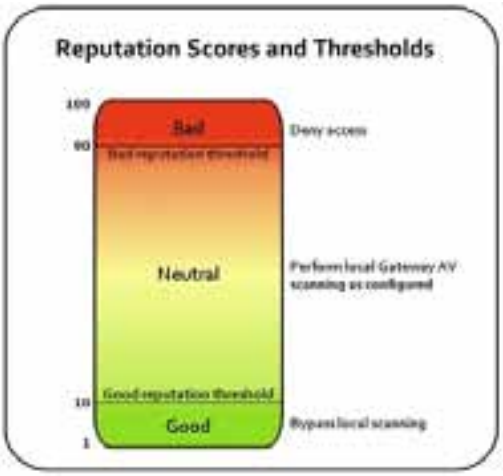
WatchGuard RED uses a cloud-based WatchGuard reputation server that assigns a reputation score between 1 and 100 to every URL. When a user goes to a web site, RED sends the requested web address (or URL) to the WatchGuard reputation server. The WatchGuard server responds with a reputation score for that URL. Based on the reputation score, and on locally configured thresholds, RED determines whether the XTM device should drop the traffic, allow the traffic and scan it locally with Gateway AV, or allow the traffic without a local Gateway AV scan. This increases performance, because Gateway AV does not need to scan URLs with a known good or bad reputation.

Reputation Thresholds

There are two reputation score thresholds you can configure:

- **Bad reputation threshold** — If the score for a URL is higher than the Bad reputation threshold, the HTTP proxy denies access without any further inspection.
- **Good reputation threshold** — If the score for a URL is lower than the Good reputation threshold and Gateway AntiVirus is enabled, the HTTP proxy bypasses the Gateway AV scan.

If the score for a URL is equal to or between the configured reputation thresholds and Gateway AV is enabled, the content is scanned for viruses.



Reputation Scores

The reputation score for a URL is based on feedback collected from devices around the world. It incorporates scan results from two leading anti-malware engines: Kaspersky and AVG. Reputation Enabled Defense uses the collective intelligence of the cloud to keep Internet browsing safe and to optimize performance at the gateway.

A reputation score closer to 100 indicates that the URL is more likely to contain a threat. A score closer to 1 indicates that the URL is less likely to contain a threat. If the RED server does not have a previous score for a web address, it assigns a neutral score of 50. The reputation score changes from the default score of 50 based on a number of factors.

These factors can cause the reputation score of a URL to increase, or move toward a score of 100:

- Negative scan results
- Negative scan results for a referring link

These factors can cause the reputation score of a URL to decrease, or move toward a score of 1:

- Multiple clean scans
- Recent clean scans

Reputation scores can change over time. For increased performance, the XTM device stores the reputation scores for recently accessed web addresses in a local cache.

Reputation Lookups

The XTM device uses UDP port 10108 to send reputation queries to the WatchGuard reputation server. UDP is a best-effort service. If the XTM device does not receive a response to a reputation query soon enough to make a decision based on the reputation score, the HTTP proxy does not wait for the response, but instead processes the HTTP request normally. In this case the content is scanned locally if Gateway AV is enabled.

> ***Note*** *A reputation score of -1 means that your device did not get a response soon enough to make a decision based on the reputation score.*

Reputation lookups are based on the domain and URL path, not just the domain. Parameters after escape or operator characters, such as & and ? are ignored.

For example, for the URL:

```
http://www.example.com/example/default.asp?action=9&parameter=26
```

the reputation lookup is:

```
http://www.example.com/example/default.asp
```

Reputation Enabled Defense does not do a reputation lookup for sites listed in the HTTP Proxy Exceptions area of the HTTP proxy action.

Reputation Enabled Defense Feedback

If Gateway AntiVirus is enabled, you can choose if you want to send the results of local Gateway AV scans to the WatchGuard server. You can also choose to upload Gateway AV scan results to WatchGuard even if Reputation Enabled Defense is not enabled or licensed on your device. All communications between your network and the Reputation Enabled Defense server are encrypted.

We recommend that you enable the upload of local scan results to WatchGuard to improve overall coverage and accuracy of Reputation Enabled Defense.

Configure Reputation Enabled Defense

You can enable Reputation Enabled Defense (RED) to increase the security and performance of the HTTP proxy policies on your XTM device.

Before You Begin

Reputation Enabled Defense is a subscription service. Before you can configure RED, you must *Get a Feature Key from LiveSecurity* on page 51 and *Add a Feature Key to Your XTM Device* on page 53.

> ***Note*** *The XTM device sends reputation queries over UDP port 10108. Make sure this port is open between your XTM device and the Internet.*

Before you can configure Reputation Enabled Defense for the HTTP proxy policy, you must configure the policy to use a user-defined proxy action. To create a user-defined proxy action, you can clone the default (predefined) proxy action, and then apply that to your proxy policy.

To find the proxy action your policy uses:

1. Select **Firewall > Firewall Policies**.
2. Select the proxy policy. Click  .
   The Policy Configuration page appears. The Proxy Action drop-down list appears at the top of the page.
3. Verify whether the proxy action is a predefined or user-defined proxy action.
   For more information about proxy actions, see *About Proxy Actions*.

If the proxy uses a predefined proxy action that you want to change, you must first clone the proxy action.

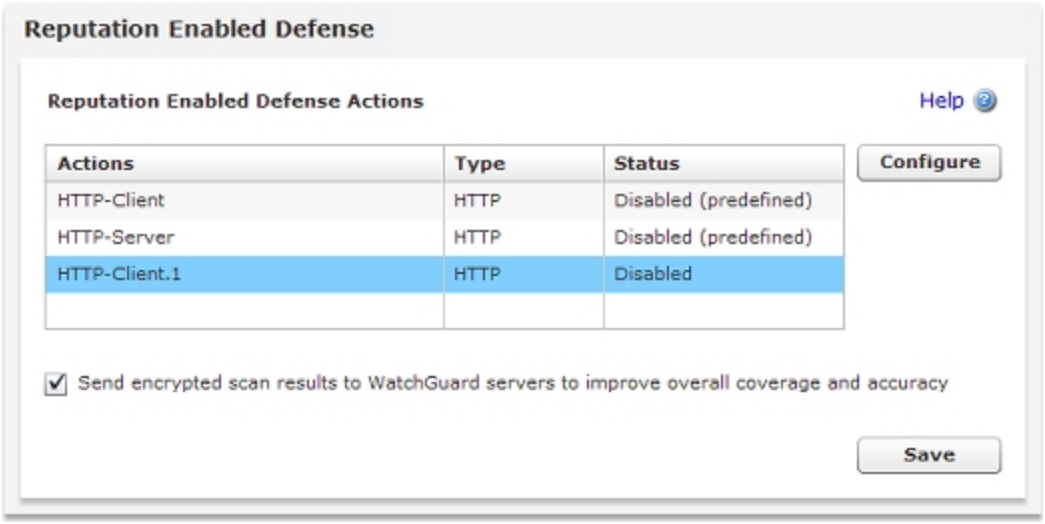
1. Select **Firewall > Proxy Actions**.
2. Select the proxy action that your proxy policy uses.
3. Click **Clone**.
4. Type a new name for the cloned proxy action.
5. Edit the proxy action.
   For more information, see *About Proxy Actions*.

If you cloned the proxy action, edit the policy to select the cloned proxy action.

1. Select **Firewall > Firewall Policies**.
2. Select the proxy. Click  .
   The Policy Configuration page appears.
3. From the **Proxy-Action** drop-down list, select the name of the new proxy action.
4. Click **Save**.

Configure Reputation Enabled Defense for a Proxy Action

1. Select **Subscription Services > Reputation Enabled Defense**.
   The Reputation Enabled Defense configuration page appears with a list of HTTP proxy actions.



2. Select a user-defined HTTP proxy action. Click **Configure**. You cannot configure Reputation Enabled Defense settings for predefined proxy actions.
   The Reputation Enabled Defense configuration settings for that proxy action appear.

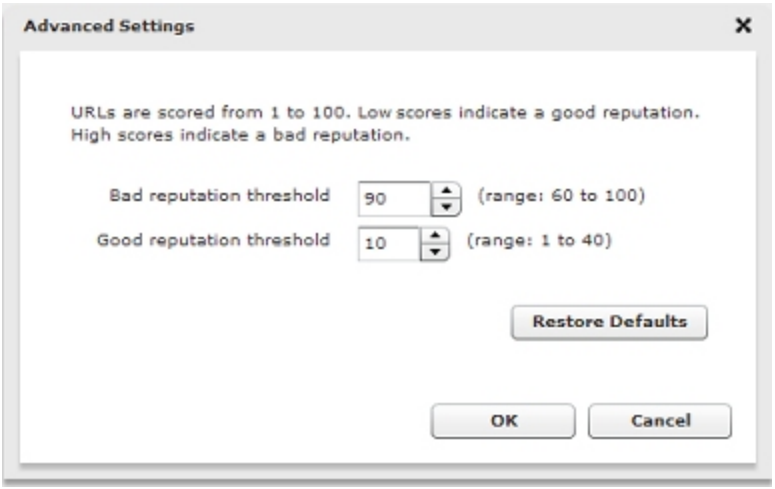
3. Select the **Immediately block URLs that have a bad reputation** check box to block access to sites that score higher than the configured Bad reputation threshold.
4. Select the **Bypass any configured virus scanning for URLs that have a good reputation** check box to have Gateway AntiVirus ignore sites that have a score lower than the configured Good reputation threshold.
5. If you want to trigger an alarm for an action, select the **Alarm** check box for that RED action. If you do not want an alarm, clear the **Alarm** check box for that action.

6. If you want to record log messages for an action, select the **Log** check box for that RED action. If you do not want to record log messages for a RED response, clear the **Log** check box for that action.

Configure the Reputation Thresholds

You can change the reputation thresholds in the Advanced settings.

1. On the Reputation Enabled Defense settings page, click **Advanced**.
   The Advanced Settings dialog box appears.



2. In the **Bad reputation threshold** text box, type or select the threshold score for bad reputation.
   The proxy can block access to sites with a reputation higher than this threshold.
3. In the **Good reputation threshold** text box, type or select the threshold score for good reputation.
   The proxy can bypass a Gateway AntiVirus scan for sites with a reputation score lower than this threshold.
4. Click **Restore Defaults** if you want to reset the reputation thresholds to the default values.
5. Click **OK**.

Send Gateway AV Scan Results to WatchGuard

When you enable Reputation Enabled Defense, the default configuration allows your XTM device to send the results of local Gateway AntiVirus scans to WatchGuard servers. This action helps to improve Reputation Enabled Defense results for all Fireware XTM users. If you have Gateway AntiVirus, but do not have Reputation Enabled Defense, you can still send Gateway AntiVirus scan results to WatchGuard.

To see or change the feedback setting, select **Subscription Services > Reputation Enabled Defense**.

The **Send encrypted scan results to WatchGuard servers to improve overall coverage and accuracy** check box controls whether the XTM device sends results of Gateway AntiVirus scans to the WatchGuard servers. This check box is selected by default when you configure Reputation Enabled Defense.

- Select this check box to send Gateway AntiVirus scan results to WatchGuard.
- Clear this check box if you do not want to send Gateway AntiVirus scan results.

We recommend that you allow the XTM device to send anti-virus scan results to WatchGuard. This can help improve performance, because the scan results help to improve the accuracy of the reputation scores. All feedback sent to the WatchGuard Reputation Enabled Defense service is encrypted.

27 Gateway AntiVirus

About Gateway AntiVirus

Hackers use many methods to attack computers on the Internet. Viruses, including worms and Trojans, are malicious computer programs that self-replicate and put copies of themselves into other executable code or documents on your computer. When a computer is infected, the virus can destroy files or record key strokes.

To help protect your network from viruses, you can purchase the Gateway AntiVirus subscription service. Gateway AntiVirus operates with the SMTP, POP3, HTTP, FTP, and TCP-UDP proxies. When a new attack is identified, the features that make the virus unique are recorded. These recorded features are known as the signature. Gateway AV uses these signatures to find viruses when content is scanned by the proxy.

When you enable Gateway AV for a proxy, Gateway AV scans the content types configured for that proxy. Gateway AV/IPS can scan these compressed file types: .zip, .gzip, .tar, .jar, .rar, .chm, .lha, .pdf, XML/HTML container, OLE container (Microsoft Office documents), MIME (mainly email messages in EML format), .cab, .arj, .ace, .bz2 (Bzip), .swf (flash; limited support).

> ***Note*** *WatchGuard cannot guarantee that Gateway AV can stop all viruses, or prevent damage to your systems or networks from a virus.*

You can see statistics on current Gateway AntiVirus activity on the **Dashboard > Subscription Services** page as described in *Subscription Services Status and Manual Signatures Updates* on page 79.

Install and Upgrade Gateway AV

To install Gateway AntiVirus, you must *Get a Feature Key from LiveSecurity* on page 51 and *Add a Feature Key to Your XTM Device* on page 53.

New viruses appear on the Internet frequently. To make sure that Gateway AV gives you the best protection, you must update the signatures frequently. You can configure the XTM device to update the signatures automatically from WatchGuard, as described in *Configure the Gateway AV Update Server* on page 717. You can also *Subscription Services Status and Manual Signatures Updates*.

About Gateway AntiVirus and Proxy Policies

Gateway AV can work with the WatchGuard SMTP, POP3, HTTP, FTP, and TCP-UDP proxies. When you enable Gateway AV, these proxies examine various types of traffic and perform an action that you specify, such as to drop the connection or to block the packet and add its source address to the Blocked Sites list.

Gateway AV scans different types of traffic according to which proxy policies you use the feature with:

- SMTP or POP3 proxy — Gateway AV looks for viruses and intrusions encoded with frequently used email attachment methods. You can also use Gateway AV and the SMTP proxy to send virus-infected email to the Quarantine Server. For more information, see *About the Quarantine Server* on page 759 and *Configure Gateway AntiVirus to Quarantine Email* on page 715.
- HTTP proxy — Gateway AV looks for viruses in web pages that users try to download.
- TCP-UDP proxy — This proxy scans traffic on dynamic ports. It recognizes traffic for several different types of proxies, including HTTP and FTP. The TCP-UDP proxy then sends traffic to the appropriate proxy to scan for viruses or intrusions.
- FTP proxy — Gateway AV looks for viruses in uploaded or downloaded files.
- DNS proxy — Gateway AV looks for viruses in DNS packets.

Each proxy that uses Gateway AV is configured with options that are special to that proxy. For example, the categories of items you can scan is different for each proxy.

For all proxies, you can limit file scanning up to a specified kilobyte count. The default scan limit and maximum scan limits are different for each XTM device model. The XTM device scans the start of each file up to the specified kilobyte count. This allows large files to pass with partial scanning.

For more information about the default and maximum scan limits for each XTM device model, see *About Gateway AntiVirus Scan Limits* on page 715.

> ***Note*** *To make sure Gateway AV has current signatures, you can enable automatic updates for the Gateway AV server, as described in Configure the Gateway AV Update Server on page 717.*

Configure the Gateway AntiVirus Service

You can configure Gateway AV to work with the WatchGuard SMTP, POP3, HTTP, FTP, and TCP-UDP proxies.

Before You Begin

Before you enable the Gateway AntiVirus Service, you must:

1. Get a Gateway AV feature key. Contact your WatchGuard reseller or go to the WatchGuard LiveSecurity web site at: http://www.watchguard.com/store.
2. *Add a Feature Key to Your XTM Device*.

Before you can configure the Gateway AntiVirus service for a proxy policy, you must configure the policy to use a user-defined proxy action. To create a user-defined proxy action, you can clone the default (predefined) proxy action, and then apply that proxy action to the proxy policy.

To find the proxy action your policy uses:

1. Select **Firewall > Firewall Policies**.
2. Select the proxy policy. Click  .
   The Policy Configuration page appears. The Proxy Action drop-down list appears at the top of the page.
3. Verify whether the proxy action is a predefined or user-defined proxy action.
   For more information about proxy actions, see *About Proxy Actions*.

If the proxy uses a predefined proxy action that you want to change, you must first clone the proxy action.

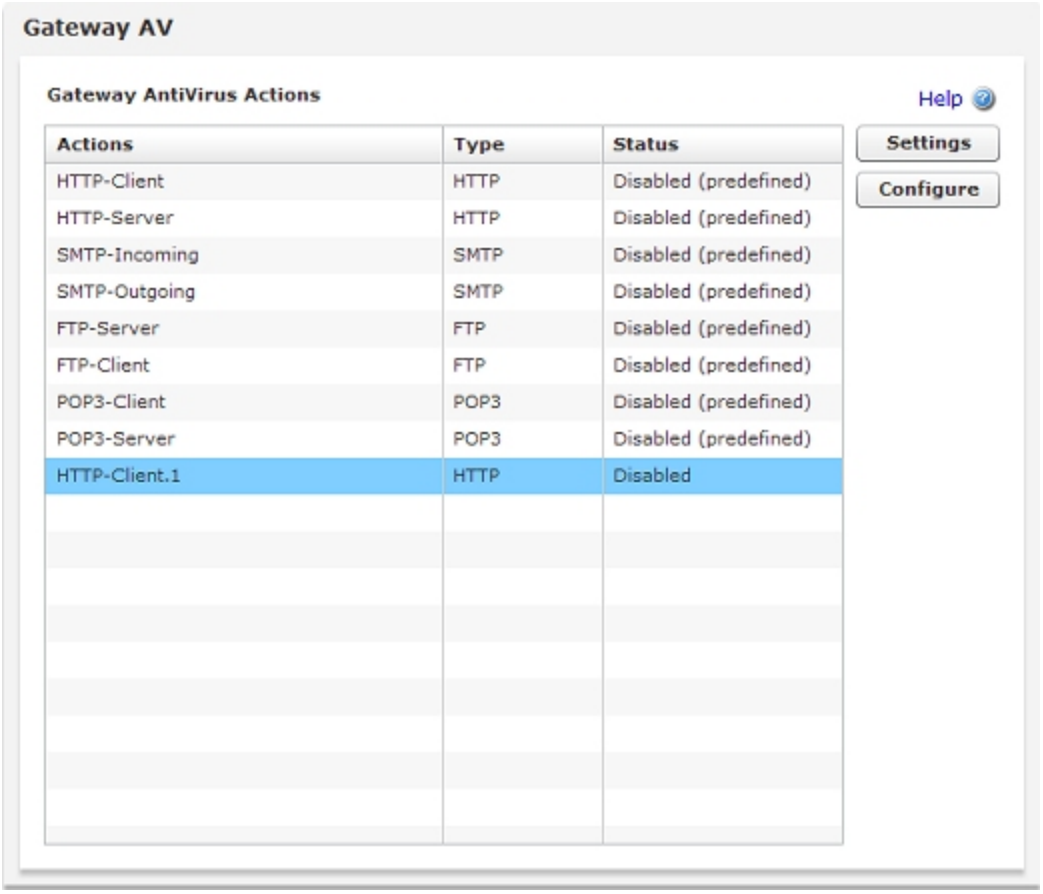
1. Select **Firewall > Proxy Actions**.
2. Select the proxy action that your proxy policy uses.
3. Click **Clone**.
4. Type a new name for the cloned proxy action.
5. Edit the proxy action.
   For more information, see *About Proxy Actions*.

If you cloned the proxy action, edit the policy to select the cloned proxy action.

1. Select **Firewall > Firewall Policies**.
2. Select the proxy. Click  .
   The Policy Configuration page appears.
3. From the **Proxy-Action** drop-down list, select the name of the new proxy action.
4. Click **Save**.

Configure the Gateway AntiVirus Service

1. Select **Subscription Services > Gateway AV**.
   The Gateway AV page appears.



2. To update global settings, click **Settings** and *Update Gateway AntiVirus Settings*.
3. To configure actions for a specific proxy action, select a user-defined proxy action and click **Configure**. You cannot configure Gateway AntiVirus for a predefined proxy action.
   The Gateway AntiVirus settings for that proxy action appear.
4. Configure the Gateway AV settings as described in *Configure Gateway AntiVirus Actions*.

Configure Gateway AntiVirus Actions

When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an email message (SMTP or POP3 proxies), web page (HTTP proxy), or uploaded or downloaded file (FTP proxy). When Gateway AntiVirus is enabled, it scans each file up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance.

The options for antivirus actions are:

Allow

Allows the packet to go to the recipient, even if the content contains a virus.

Deny

(FTP proxy only)

Denies the file and send a deny message.

Lock

(SMTP and POP3 proxies only)

Locks the attachment. This is a good option for files that cannot be scanned by the XTM device. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment.

For information about how to unlock a file locked by Gateway AntiVirus, see the WatchGuard System Manager help at http://www.watchguard.com/help/docs/wsm/11/en-US/Content/en-US/services/gateway_av/av_unlock_file_wsm.html.

Quarantine

(SMTP proxy only)

When you use the SMTP proxy with the spamBlocker security subscription, you can send email messages with viruses, or possible viruses, to the Quarantine Server. For more information on the Quarantine Server, see *About the Quarantine Server* on page 759. For information on how to set up Gateway AntiVirus to work with the Quarantine Server, see *Configure Gateway AntiVirus to Quarantine Email* on page 715.

Remove

(SMTP and POP3 proxies only)

Removes the attachment and allows the message through to the recipient.

Drop

(Not supported in POP3 proxy)

Drops the packet and drops the connection. No information is sent to the source of the message.

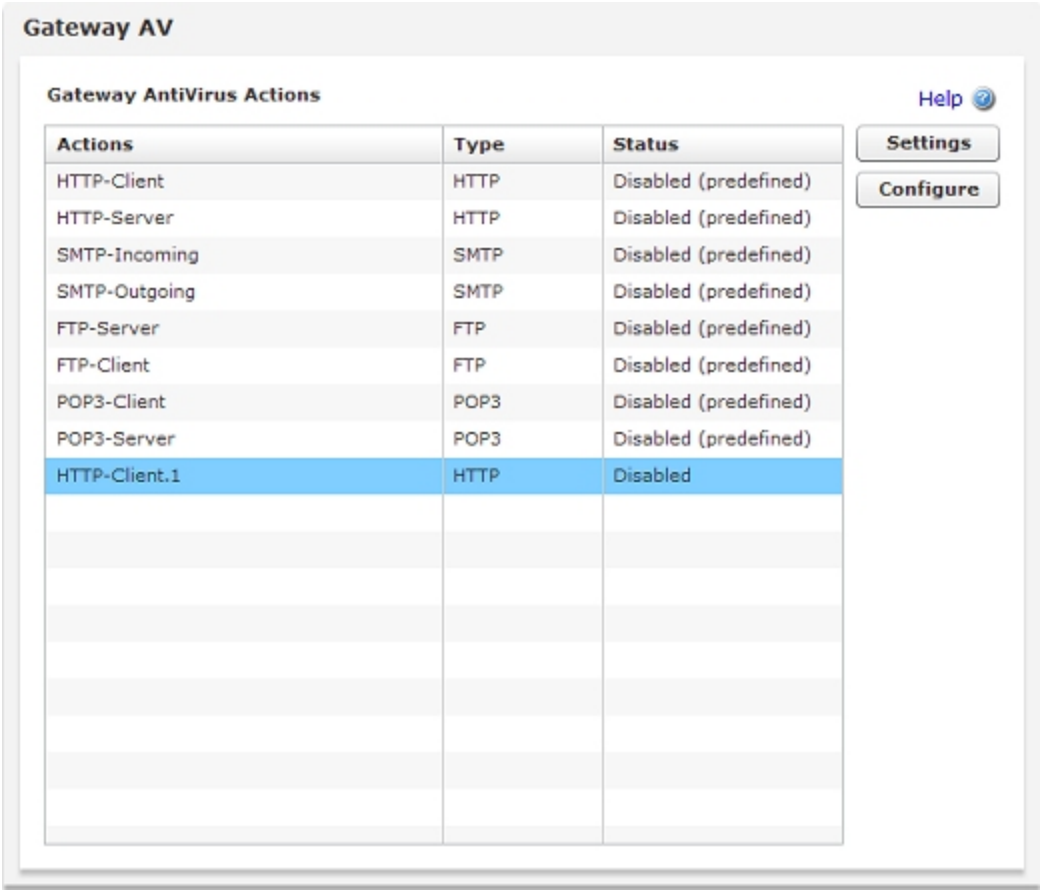
Block

(Not supported in POP3 proxy)

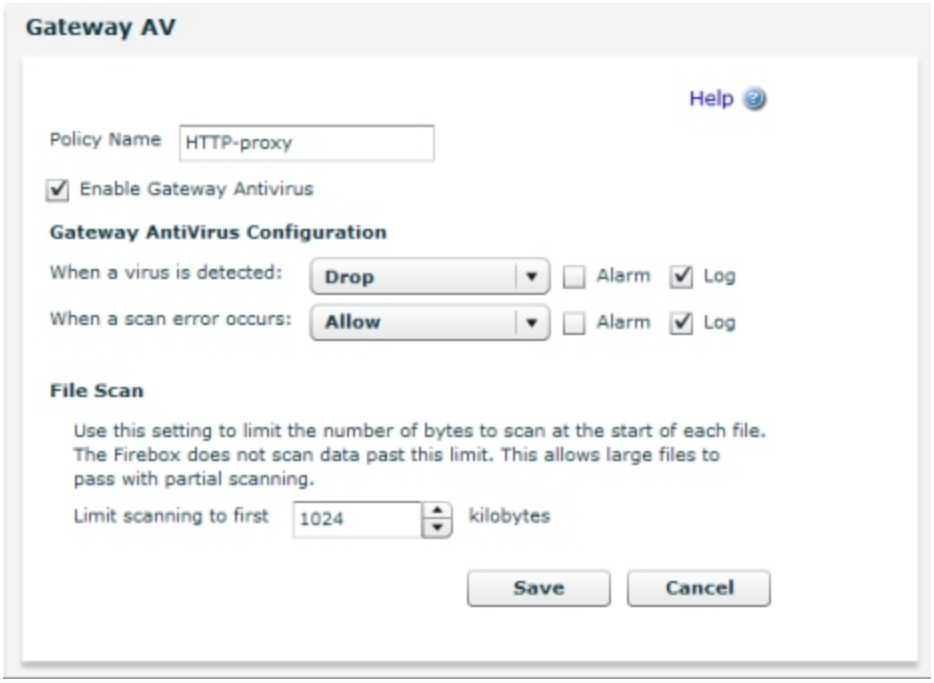
Blocks the packet, and adds the IP address of the sender to the Blocked Sites list.

Configure Gateway AntiVirus Actions for a Proxy Action

1. Select **Subscription Services > Gateway AV**.
   The Gateway AV configuration page appears.



2. Select a user-defined proxy action and click **Configure**. You cannot modify Gateway AntiVirus settings for predefined proxy actions.
   The Gateway AntiVirus configuration settings for that proxy action appear.



3. To enable Gateway AntiVirus for this proxy action, select the **Enable Gateway AntiVirus** check box.
4. From the **When a virus is detected** drop-down list, select the action the XTM device takes if a virus is detected in an email message, file, or web page. See the beginning of this section for a description of the actions.
5. From the **When a scan error occurs** drop-down list, select the action the XTM device takes when it cannot scan an object or an attachment. Attachments that cannot be scanned include binhex-encoded messages, certain encrypted files, or files that use a type of compression that Gateway AV does not support such as password-protected Zip files. See the beginning of this section for a description of the actions.
6. To create log messages for the action, select the **Log** check box for the antivirus response. If you do not want to record log messages for an antivirus response, clear the **Log** check box.
7. To trigger an alarm for the action, select the **Alarm** check box for the antivirus response. If you do not want to set an alarm, clear the **Alarm** check box for that action.
8. In the **Limit scanning to first** text box, type the file scan limit.
   For information about the default and maximum scan limits for each XTM device model, see *About Gateway AntiVirus Scan Limits* on page 715.

Configure Alarm Notifications for Antivirus Actions

You can configure an alarm notification to tell users when a proxy rule applies to network traffic. If you enable alarms for a proxy antivirus action, you must also configure the type of alarm to use in the proxy policy.

To configure the alarm type to use for a proxy policy:

1. Select **Firewall > Firewall Policies**.
2. Double click a policy to edit.
3. Select the **Properties** tab.
4. Configure the notification settings as described in *Set Logging and Notification Preferences* on page 466.

Configure Gateway AntiVirus to Quarantine Email

The WatchGuard Quarantine Server provides a safe, full-featured quarantine mechanism for any email messages suspected or known to be spam or to contain viruses. This repository receives email messages from the SMTP proxy and filtered by spamBlocker.

To configure Gateway AntiVirus to quarantine email:

1. When you configure Gateway AntiVirus (as described in *Configure Gateway AntiVirus Actions* on page 710), you must make sure you enable Gateway AntiVirus for the SMTP proxy. The POP3 proxy does not support the Quarantine Server.
2. When you set the actions spamBlocker applies for different categories of email (as described in *Configure spamBlocker* on page 687), make sure you select the **Quarantine** action for at least one of the categories. When you select this action, you are prompted to configure the Quarantine Server if you have not already done so.

You can also select the **Quarantine** action for email messages identified by Virus Outbreak Detection to contain viruses. For more information, see *Configure Virus Outbreak Detection Actions for a Policy* on page 691.

About Gateway AntiVirus Scan Limits

Gateway AntiVirus scans each file up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. The default and maximum scan limits can be different for each XTM device model.

File Scan Limits by XTM Device Model, in Kilobytes

Model	Minimum	Maximum	Default
XTM 2 Series	250	5120	512
XTM 5 Series	250	30720	1024
XTM 8 Series	250	30720	1024
XTM 1050	250	30720	1024

For information about how to set the scan limit, see *Configure Gateway AntiVirus Actions* on page 710.

Update Gateway AntiVirus Settings

The XTM device has several settings for the Gateway AntiVirus engine regardless of which proxy it is configured to work with. For more information, see *Configure Gateway AV Decompression Settings* on page 716.

It is important to update the signatures for Gateway AntiVirus/Intrusion Prevention Service. The signatures for these services are not automatically updated by default. You can update the signatures in two ways:

- *Configure the Gateway AV Update Server* to enable automatic updates
- Update the signatures manually in Firebox System Manager, as described in *Subscription Services Status and Manual Signatures Updates* on page 79.

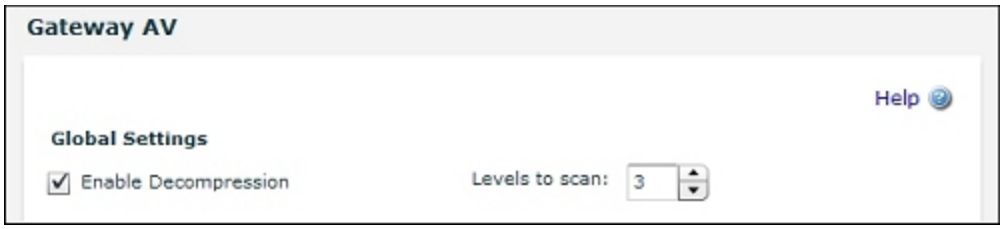
If you Use a Third-Party Antivirus Client

If you use a third-party antivirus service on computers that are protected by your XTM device, you could have problems with updates for the third-party service. When the client for that secondary service tries to update its signature database on port 80, the WatchGuard Gateway AV service, working through the HTTP proxy, recognizes the signatures and strips them before they download to the client. The secondary service cannot update its database. To avoid this problem, you must add *HTTP-Proxy: Exceptions* to the policy that denies the update traffic. You must know the host name of the third-party signature database. Then you can add that host name as an allowed exception.

Configure Gateway AV Decompression Settings

Gateway AV can scan inside compressed files if you enable decompression in the Gateway AV configuration settings.

1. From the Fireware XTM Web UI, select **Subscription Services > Gateway AV**.
   The Gateway AV configuration page appears.
2. Click **Settings**.
   The Gateway AV Global Settings page appears.



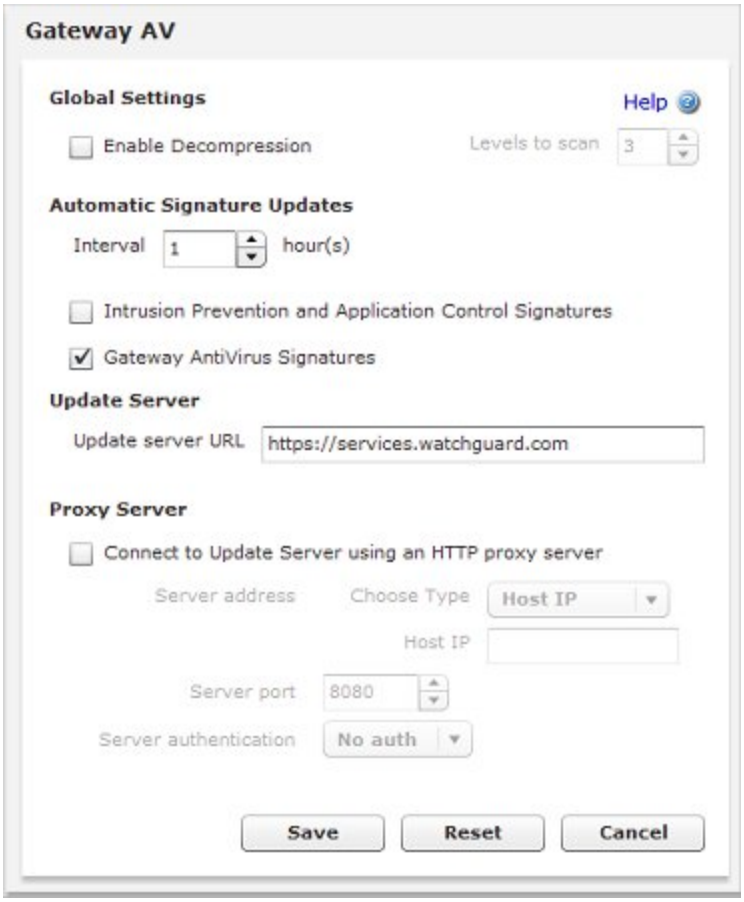
3. To scan inside compressed attachments, select the **Enable Decompression** check box. Select or type the number of compression levels to scan. If you enable decompression, we recommend that you keep the default setting of three levels, unless your organization must use a larger value. If you specify a larger number, your XTM device could send traffic too slowly. Gateway AntiVirus supports up to six levels. If Gateway AntiVirus detects that the archive depth is greater than the value set in this field, it will generate a scan error for the content.
   Compressed attachments that cannot be scanned include encrypted files or files that use a type of compression that we do not support such as password-protected Zip files. To set the action for the XTM device when it finds a message it cannot scan, select an action for **When a scan error occurs** in the **General** category of the policy configuration.

4. Click **Restore Defaults** if you want to reset the user interface to default settings.
5. Click **Save**.

Configure the Gateway AV Update Server

Gateway AntiVirus downloads signature updates from a signature update server. Gateway AV, IPS, and Application Control use the same signature update server. When you configure the signature update server for any of these subscription services, the settings apply to all three services.

1. From the Fireware XTM Web UI, select **Subscription Services > Gateway AV**.
2. Click **Settings**.
   The Gateway AV settings page appears.



3. From the **Interval** drop-down list, enter the number of hours between automatic updates.
4. Automatic updates for Gateway AV are not enabled by default. To enable automatic updates at the selected update interval, click the check boxes.
   - Select the **Intrusion Prevention and Application Control Signatures** check box if you want the XTM device to download a new set of IPS and Application Control signatures at the automatic update interval.
   - Select the **Gateway AntiVirus Signatures** check box If you want the XTM device to download a new set of Gateway AntiVirus signatures at the automatic update interval.

3. Do not change the URL of the update server for Gateway AV or IPS unless you are told to do so by WatchGuard. If you change the URL accidentally or incorrectly, click **Reset** to return to the last saved setting.
4. Click **Save**.

Connect to the Update Server Through an HTTP Proxy Server

If your XTM device must connect through an HTTP proxy to get to the signature update server, you must add information about the HTTP proxy server to your update server configuration.

1. From the **Gateway AV** configuration page, click **Settings**.
2. Select the **Contact the Update Server using an HTTP proxy server** check box.
3. From the **Choose Type** drop-down list, select whether you identify your HTTP proxy server by host name or IP address. Type the host name or IP address in the adjacent text box.
4. Most HTTP proxy servers receive requests on port 8080. If your HTTP proxy uses a different port, enter it in the **Server port** text box.
5. From the **Server authentication** drop-down list, select the type of authentication your HTTP proxy server uses. Select **NoAuth** if your HTTP proxy does not require authentication. If your HTTP proxy server requires **NTLM** or **Basic** authentication, enter your user name, user domain, and password in the text boxes.
6. Click **Save**.

Block Access from the Trusted Network to the Update Server

If you do not want to allow all users on your trusted network to have unfiltered access to the IP address of the signature database, you can use an internal server on your trusted network to receive the updates. You can create a new HTTP proxy policy with *HTTP-Proxy: Exceptions* or an HTTP packet filter policy that allows traffic only from the IP address of your internal server to the signature database.

Update Signatures Manually

For information about how to see the status of Gateway AntiVirus signature updates, and how to manually force an update to the most current signatures, see *Subscription Services Status and Manual Signatures Updates*.

28 Intrusion Prevention Service

About Intrusion Prevention Service

Intrusions are direct attacks on your computer. Usually the attack exploits a vulnerability in an application. These attacks are created to cause damage to your network, get sensitive information, or use your computers to attack other networks.

Intrusion Prevention Service (IPS) provides real-time protection from threats, including spyware, SQL injections, cross-site scripting, and buffer overflows. When a new attack is identified, the features that make the intrusion attack unique are recorded. These recorded features are known as the signature. IPS uses these signatures to identify intrusion attacks.

By default, when you enable and configure IPS, the IPS configuration applies globally to all traffic. You can also choose to disable IPS on a per-policy basis.

IPS Threat Levels

IPS categorizes IPS signatures into five threat levels, based on the severity of the threat. The severity levels, from highest to lowest are:

- Critical
- High
- Medium
- Low
- Information

When you enable IPS, the default setting is to drop and log traffic that matches the Critical, High, Medium, or Low threat levels. Traffic that matches the information threat level is allowed and not logged by default.

Add the IPS Upgrade

To enable IPS on your XTM device, you must:

1. *Get a Feature Key from LiveSecurity* on page 51
2. *Add a Feature Key to Your XTM Device* on page 53
3. *Configure Intrusion Prevention*

Keep IPS Signatures Updated

New intrusion threats appear on the Internet frequently. To make sure that IPS gives you the best protection, you must update the signatures frequently. You can configure the XTM device to update the signatures automatically from WatchGuard, as described in *Configure the IPS Update Server*.

> ***Note*** *The XTM 2 Series models have a smaller number of IPS signatures than the other XTM device models.*

See IPS Status

On the **Dashboard > Subscription Services** page, you can see statistics on current IPS activity and update the IPS signatures. For more information, see *Subscription Services Status and Manual Signatures Updates* on page 79.

Configure Intrusion Prevention

To use Intrusion Prevention Service (IPS), you must have a feature key to enable the service.

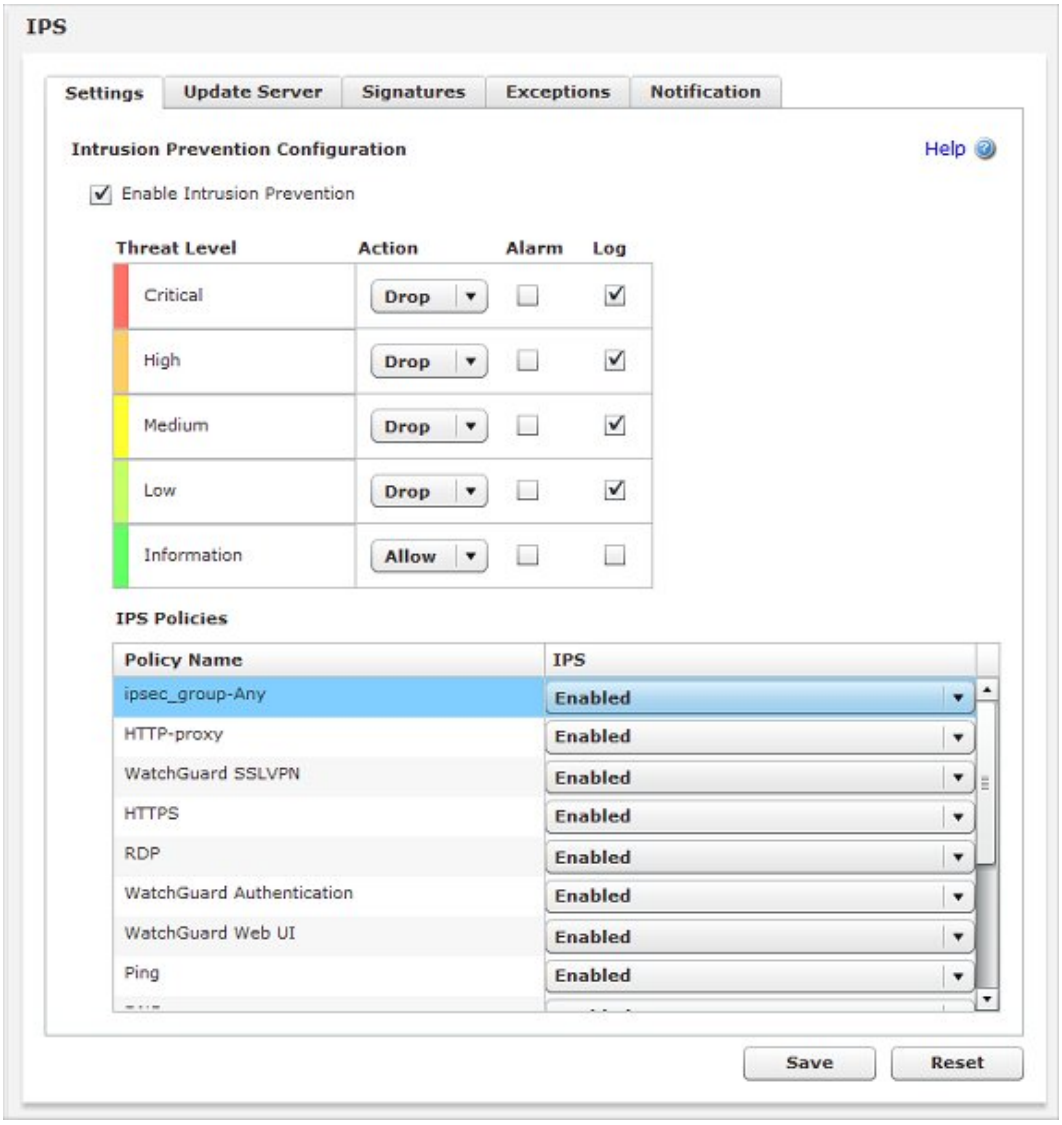
For more information, see:

- *Get a Feature Key from LiveSecurity* on page 51
- *Add a Feature Key to Your XTM Device* on page 53

Enable IPS and Configure IPS Actions

To enable IPS:

1. Select **Subscription Services > IPS**.
   The IPS page appears.



2. Select the **Enable Intrusion Prevention** check box.
3. For each threat level, select the action. Available actions are:

   - **Allow** — Allows the connection.
   - **Drop** — Denies the request and drops the connection. No information is sent to the source of the message.
   - **Block** — Denies the request, drops the connection, and adds the IP address of the sender to the Blocked Sites list.

4. For each threat level, select the **Log** check box if you want to send a log message for an IPS action. Or, clear the **Log** check box if you do not want to log IPS actions for that threat level.
5. For each threat level, select the **Alarm** check box if you want to trigger an alarm for an IPS action. Or, clear the **Alarm** check box if you do not want to trigger an alarm for that threat level.
6. Click **Save**.

Configure other IPS Settings

In the **IPS Policies** section, you can disable or enable IPS for each policy in your configuration. For more information, see *Disable or Enable IPS for a Policy*.

Select the **Update Server** tab to configure signature update settings. For more information, see *Configure the IPS Update Server*.

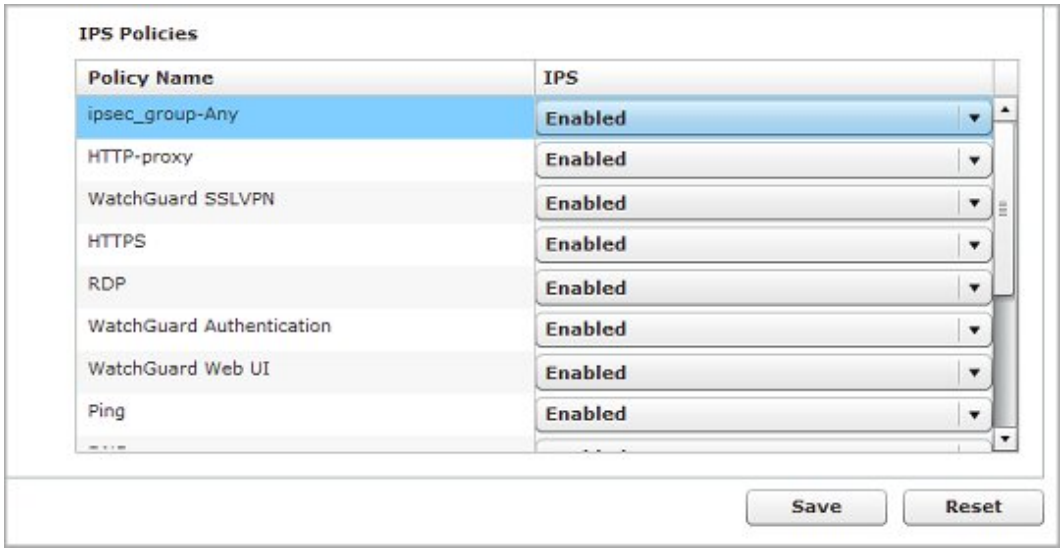
Select the **Signatures** tab to add signatures to the exceptions list. For more information, see *Configure IPS Exceptions*.

Disable or Enable IPS for a Policy

When you enable IPS, it is automatically enabled for all policies. You can choose to disable it for a specific policy in the IPS configuration or when you edit a policy.

To disable or enable IPS for a policy:

1. Select **Subscription Services > IPS**.
   The IPS configuration page appears. The IPS Policies section shows whether IPS is enabled for each policy.



2. To disable IPS for a policy, click the IPS column for that policy.
   A drop-down list appears, with the choices Enabled or Disabled.
3. Select **Disabled** to disable IPS for the selected policy.
   Or, click **Enabled** to enable IPS for the policy.
4. Click **Save**.

You can also choose to enable or disable IPS when you edit a policy:

1. Select **Firewall > Firewall Policies**.
2. Double-click a policy to edit it.
3. Select the **Enable IPS for this policy** check box to to enable IPS.
   Or, clear the check box to disable it.
4. Click **Save**.

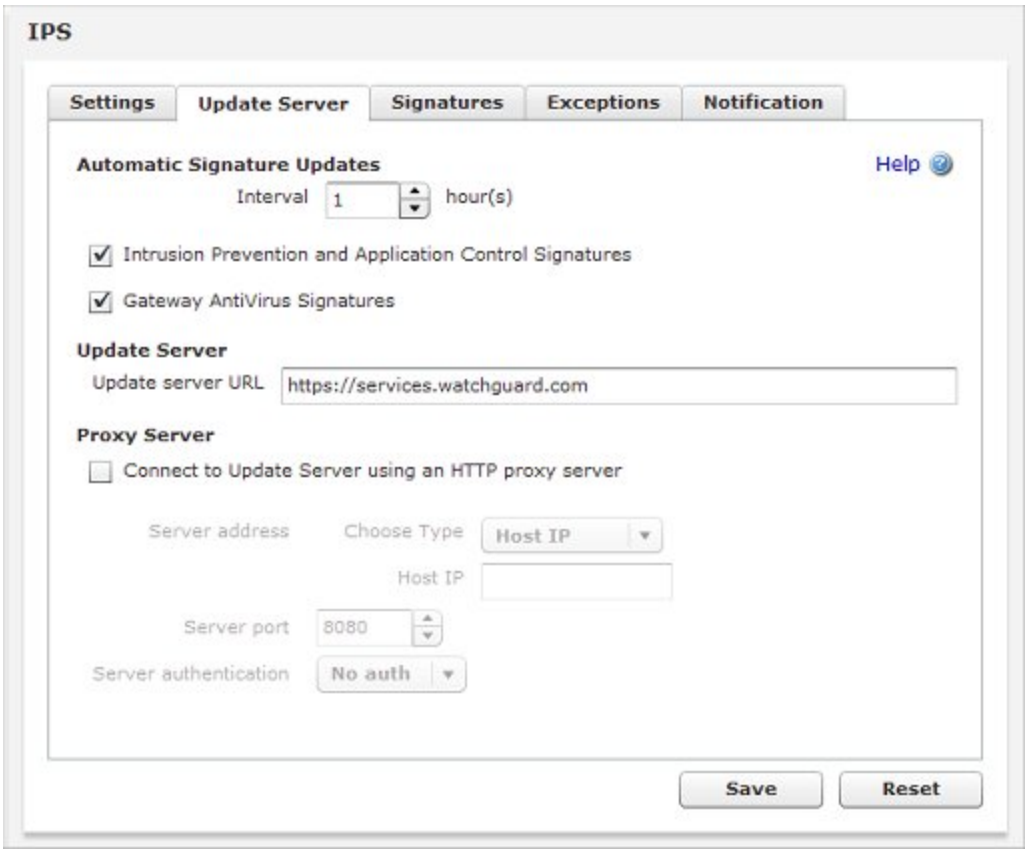
Configure the IPS Update Server

The Intrusion Prevention Service (IPS) downloads signature updates from a signature update server. Gateway AV, IPS, and Application Control use the same update server settings. When you configure the update server for any one of these subscription services, the settings apply to all three services.

IPS and Application Control signature updates are delivered together in one file.

Configure Automatic Signature Updates

1. Select **Subscription Services > IPS**.
2. Click the **Update Server** tab.
   The Update Server settings appear.



3. From the **Interval** drop-down list, enter the number of hours between automatic updates.
4. Select the **Intrusion Prevention and Application Control Signatures** check box to automatically update signatures at the selected update interval.

Do not change the **Update server URL** unless you are told to do so by WatchGuard. If you change the URL accidentally or incorrectly, click **Reset** to return to the last saved setting.

Connect to the Update Server Through an HTTP Proxy Server

If your XTM device must connect through an HTTP proxy to get to the signature update server, you must add information about the HTTP proxy server to your update server configuration.

1. In the **Proxy Server** section, select the **Connect to Update server using an HTTP proxy server** check box.
2. From the **Choose Type** drop-down list, select whether you identify your HTTP proxy server by host name or IP address. Type the host name or IP address in the adjacent text box.
3. Most HTTP proxy servers receive requests on port 8080. If your HTTP proxy uses a different port, type it in the **Server port** text box.
4. From the **Server authentication** drop-down list, select the type of authentication your HTTP proxy server uses.
   - If your HTTP proxy does not require authentication, select **NoAuth**
   - If your HTTP proxy server requires **NTLM** or **Basic** authentication, type your **User name**, **Domain**, and **Password** in the text boxes
5. Click **Save**.

Block Access from the Trusted Network to the Update Server

If you do not want to allow all users on your trusted network to have unfiltered access to the IP address of the signature database, you can use an internal server on your trusted network to receive the updates. You can create a new HTTP proxy policy with *HTTP-Proxy: Exceptions* or an HTTP packet filter policy that allows traffic only from the IP address of your internal server to the signature database.

Update Signatures Manually

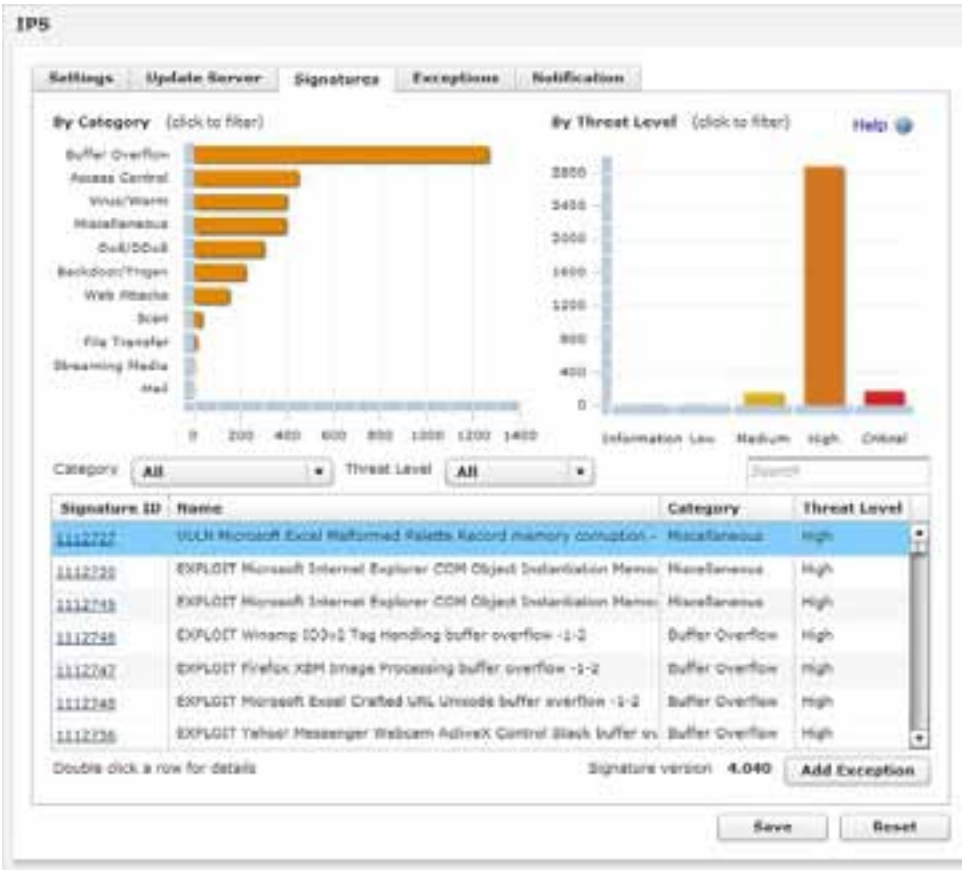
For information about how to see the status of IPS signature updates and how to manually force an update to the most current signatures, see *Subscription Services Status and Manual Signatures Updates*.

Show IPS Signature Information

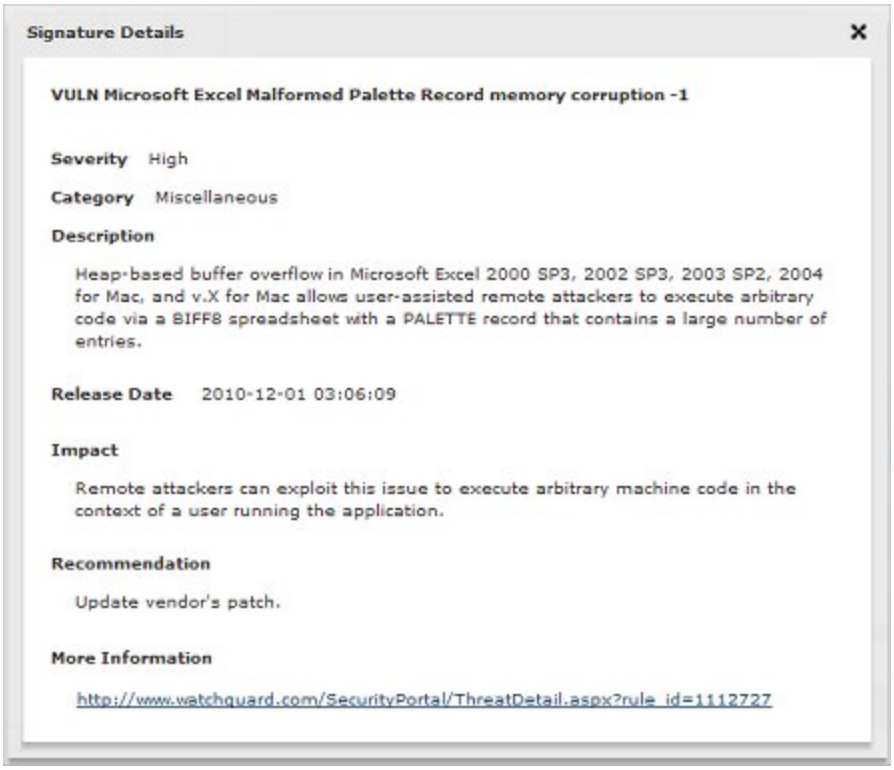
On the Signatures tab of the Intrusion Prevention Service configuration, you can see information about all the IPS signatures. You can filter and sort the signature list, and you can see details about individual signatures. You can also add a signature to the IPS exceptions list from this tab.

See IPS Signatures

1. Select **Subscription Services > IPS**.
   The IPS configuration page appears.
2. Select the **Signatures** tab.
   The list of IPS signatures appears.



3. Double-click a signature name to see more information about the signature.



4. Click the link in the **More Information** section to look up the signature on the WatchGuard IPS Security Portal.
   You can also click the Signature ID on the Signatures tab to look up the signature in the Security Portal.

For more information about the Security Portal, see *Look up IPS Signatures on the Security Portal*.

Search, Sort and Filter the IPS Signatures

The graphs at the top of the Signatures tab show the proportion and number of signatures in each signature category and each threat level. You can filter the signature list by signature category or threat level.

- To filter the signature list by signature category, click the bar for that category in the **By Category** graph. Or, select the category from the **Category** drop-down list.
- To filter the signature list by signature threat level, click the bar in the **By Threat Level** graph. Or, select the threat level severity from the **Threat Level** drop-down list.

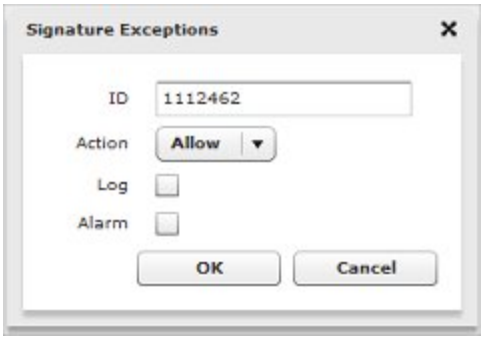
To search for signatures that contain a specific word or ID number, type the text to search for in the **Search** text box.

To sort the IPS signatures by **Signature ID**, **Name**, **Category**, or **Threat Level**, click one of the column headings.

Add an IPS Exception

You can add a signature to the IPS Exceptions list directly from the Signatures tab.

1. Select a signature in the **Signatures** list.
2. Click **Add Exception**.
   The Signature Exceptions dialog box appears. The ID text box shows the ID of the signature you want to add.



3. Select the **Action**, **Log**, and **Alarm** settings for this exception.
4. Click **OK**.
   The signature exception is added to the Exceptions tab.

For more information about IPS exceptions, see *Configure IPS Exceptions*.

Configure IPS Exceptions

When you enable the IPS feature, the XTM device examines traffic to look for patterns of traffic that match the signatures of known intrusions. When an IPS signature match occurs, the XTM device denies the content and the intrusion is blocked. If you want to allow traffic that is blocked by an IPS signature, you can find the identification number for the signature (the signature ID) and add the signature ID to the IPS exception list.

Find the IPS Signature ID

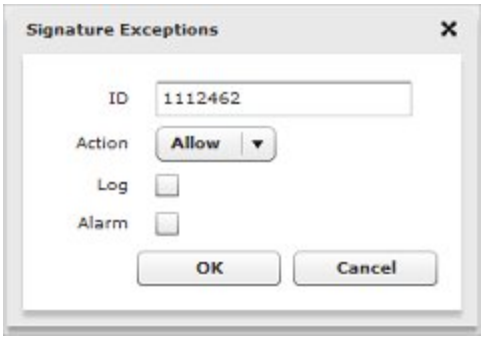
When the XTM device blocks a connection based on a match with an IPS signature, the signature ID appears in the log file if you have enabled logging for IPS. To see which IPS signature blocked the connection, look in the log file for the IPS signature ID number. If a connection that you want to allow is blocked by an IPS signature, use the signature ID to add an IPS exception to allow that connection.

On the **Signatures** tab, you can look up the IPS signature ID to see information about the threat a signature ID represents. For more information about how to look up an IPS signature, see *Show IPS Signature Information*.

Add an IPS Signature Exception

To add an IPS signature exception:

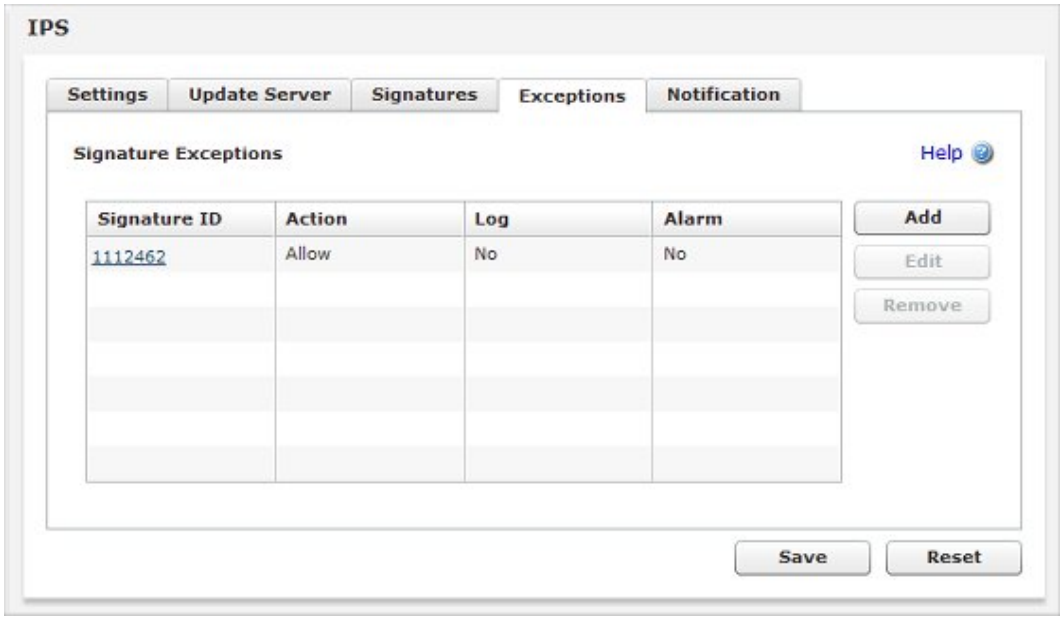
1. Select **Subscription Services > IPS**.
   The IPS configuration page appears.
2. Select the **Exceptions** tab.
   The list of IPS signature exceptions appears.
3. Click **Add**.
   The Signature Exceptions dialog box appears.



4. In the **ID** text box, type the ID of the IPS signature you want to add.
5. From the **Action** drop-down list, select the action you want IPS to take for this signature. The available actions are:

   - **Allow** — Allows the connection.
   - **Drop** — Denies the request and drops the connection. No information is sent to the source of the message.
   - **Block** — Denies the request, drops the connection, and adds the IP address of the sender to the Blocked Sites list.

6. Select the **Log** check box if you want to send a log message for this IPS exception.
7. Select the **Alarm** check box if you want to send an alarm for this IPS exception.
8. Click **OK**.
   The exception is added to the Signature Exceptions list.



9. Click **Save**

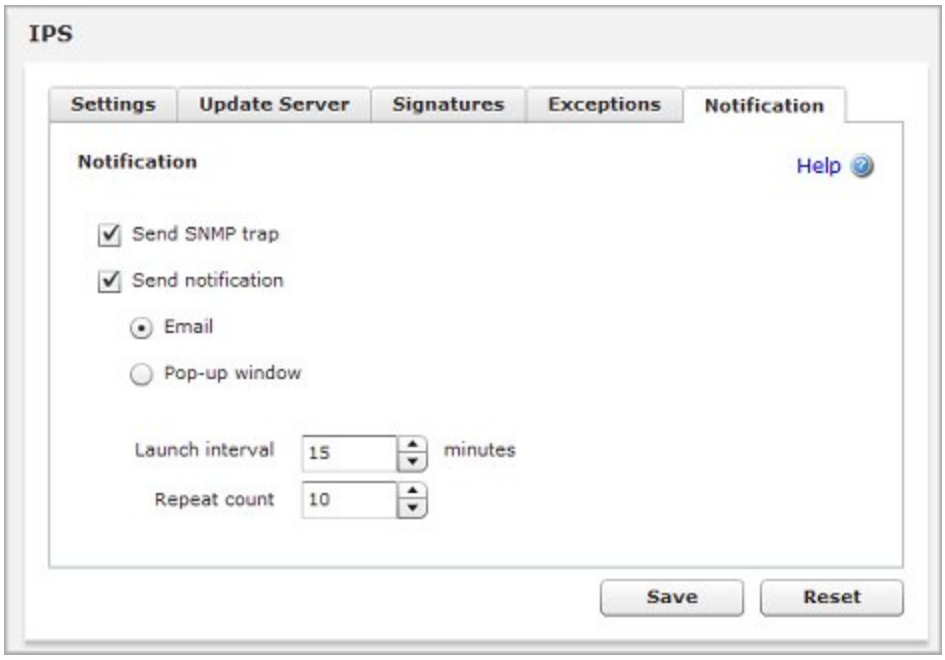
To look up the IPS signature of an exception on the WatchGuard Security Portal, click the Signature ID.

To edit the settings for an exception, select the exception and click **Edit**.

To remove an exception, select the exception and click **Remove**.

Configure IPS Notification

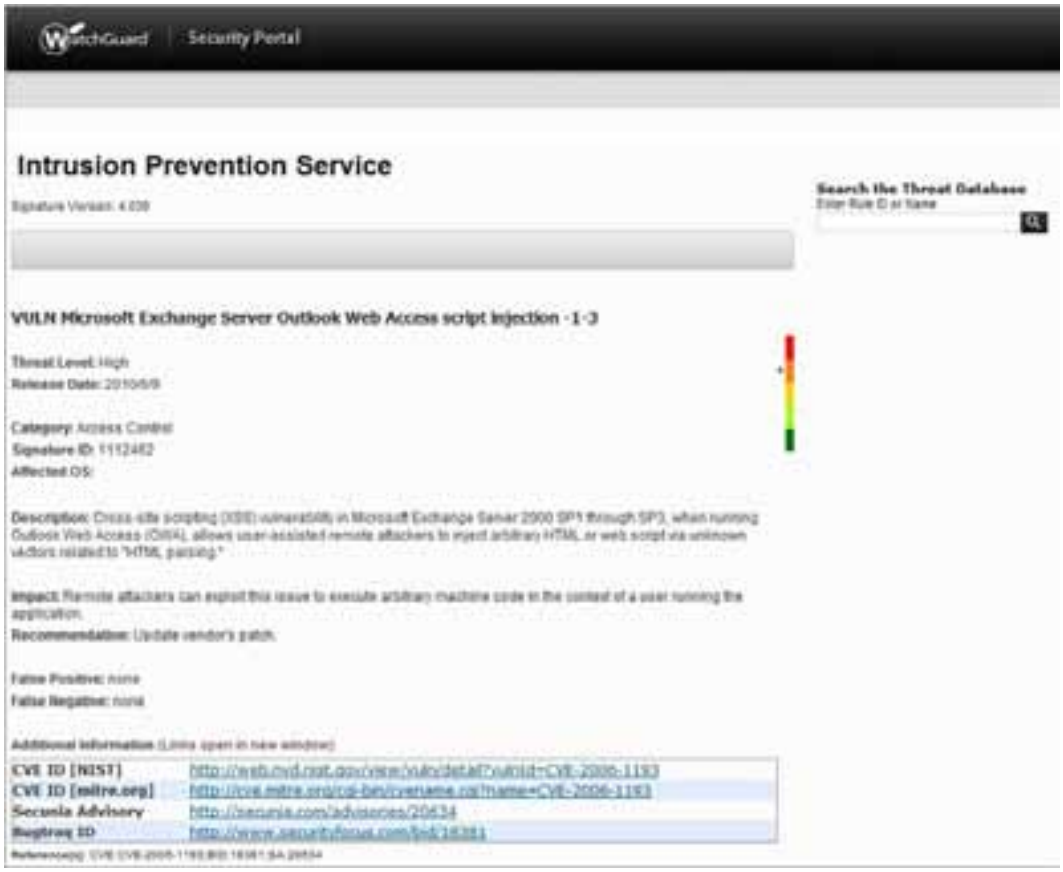
To configure notification parameters for Intrusion Prevention Service, select the **Notification** tab on the IPS configuration page. The notification settings determine how the XTM device notifies you when content is blocked by an IPS signature at a threat level when alarms are enabled.



For information about the **Notification** tab settings, see *Set Logging and Notification Preferences* on page 466.

Look up IPS Signatures on the Security Portal

You can look up information about IPS signatures on the WatchGuard IPS Security Portal at: http://www.watchguard.com/SecurityPortal/ThreatDB.aspx. From the IPS Security Portal, you can search for an IPS signature by ID or name. Signature descriptions on the IPS Security Portal include links to additional information about the signature, based on Bugtraq ID, CVE ID, or other sources about a threat the signature blocks.



To look up an IPS signature from the Web UI, you can click a signature ID in the **Signatures** or **Exceptions** tabs in the IPS configuration page.

If you have enabled logging for Intrusion Prevention Service (IPS) signatures, you can also use Traffic Monitor to find more information about the signature IDs associated with traffic log messages. When you look up signature information for a traffic log message, you see the signature information in the IPS Security Portal.

For more information about Traffic Monitor, see the *WatchGuard System Manager Help* or *User Guide*.

29 Application Control

About Application Control

Application Control is a subscription service that enables you to monitor and control the use of applications on your network. Application Control uses signatures that can identify and block over 1500 applications. In the Application Control action, you select the applications by name, and choose to block or allow traffic for each application. Then you apply the Application Control action to the applicable policy. You do not need to create or maintain your own custom rules to identify applications. The Application Control service provides frequent updates to application signatures to keep the protection current.

You can use Application Control to block the usage of specific applications, and you can report on application use and use attempts. For some applications, you can block specific application behaviors, such as file transfer.

When Application Control blocks content that matches an Application Control action, the user who requested the content sees that the content is not available, but does not get a message that the content was blocked by Application Control.

Add the Application Control Upgrade

To enable Application Control on your XTM device, you must:

1. *Get a Feature Key from LiveSecurity* on page 51
2. *Add a Feature Key to Your XTM Device* on page 53
3. *Configure Application Control Actions*

Keep Application Control Signatures Updated

New applications appear on the Internet frequently. To make sure that Application Control can recognize the latest applications, you must update the signatures frequently. You can configure the XTM device to update the signatures automatically from WatchGuard, as described in *Configure the Application Control Update Server*.

> ***Note*** *The XTM 2 Series models have a smaller number of Application Control signatures than the other XTM device models.*

Application Control — Begin with Monitoring

When you start to use Application Control, we recommend that you first configure your policies to send log messages for all application use so that you get a true understanding of the applications that are used on the network. To monitor application use, you can enable Application Control and logging for all policies that match the application traffic. After you enable Application Control and logging for a policy, all application activity for traffic through that policy is recorded in the log database and available for the Application Control reports, even if the Global Application Control action is empty.

Monitor Application Use

To monitor application use:

1. Create an Application Control action that does not block any applications.
   The Global action is empty by default, so it does not block applications.

   For more information, see *Configure Application Control Actions*.
2. Apply the empty Application Control action to the policies that handle traffic you want to monitor.

   For information about how to enable Application Control, see *Enable Application Control in a Policy*.

   For information about which policies to configure, see *Policy Guidelines for Application Control*.
3. Enable logging in each policy that has Application Control enabled.

   For information about how to enable logging in a policy, see *Configure Logging and Notification for a Policy*.

> ***Note*** *If you do not enable logging for a policy that has Application Control enabled, Application Control saves log information only for blocked applications.*

Application Control Reports

After you have enabled Application Control and logging in your policies, you can use Report Manager to run Application Control reports that summarize information about the applications used on your network.

> ***Note*** *To run Application Control reports, you must set up a Log Server and a Report Server. For more information about WatchGuard servers, see About WatchGuard Servers.*

Report Manager includes these predefined reports for Application Control:

Application Control Reports

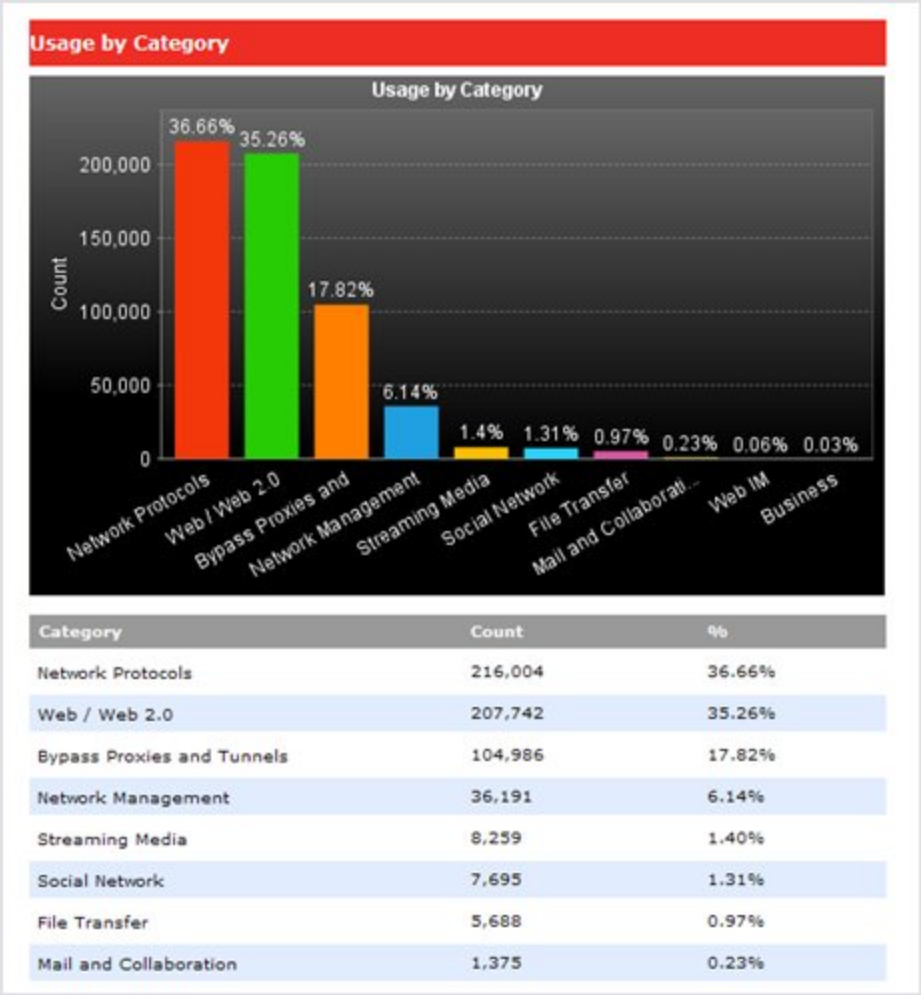
- Application Usage Summary
- Blocked Application Summary

Client Reports — Show which users use the applications

- Top Clients by Application Usage
- Top Clients by Blocked Applications
- Top Clients by Blocked Categories

Client reports show the names of users who use applications if you have configured authentication on the firewall.

Before you configure Application Control to block applications, we recommend that you examine the Application Usage Summary and the Top Clients by Application Usage reports.



Category	Count	%
Network Protocols	216,004	36.66%
Web / Web 2.0	207,742	35.26%
Bypass Proxies and Tunnels	104,986	17.82%
Network Management	36,191	6.14%
Streaming Media	8,259	1.40%
Social Network	7,695	1.31%
File Transfer	5,688	0.97%
Mail and Collaboration	1,375	0.23%

When you look at the Application Usage reports, consider these questions:

- Does the report show any application categories that seem to conflict with corporate policy?
- Are the applications appropriate for business use?
- Which users use the applications? Fireware XTM provides reports that show application use by client. The authentication capabilities in Fireware XTM enable you to see client reports by user name rather than by IP address. You can also identify user traffic in Terminal Services environments.

  For information about how to configure Terminal Services, see *Configure Terminal Services Settings*.

If the reports show an application that you are not familiar with, you can look up information about the application on the WatchGuard Application Control Security Portal at http://www.watchguard.com/SecurityPortal/AppDB.aspx.

For more information about Report Manager, see the *WatchGuard System Manager Help* or *User Guide*.

Policy Guidelines for Application Control

To monitor or block application usage, you must enable Application Control for all policies that handle the application traffic. WatchGuard does not recommend that you apply the Global Application Control action to every policy. Because of the performance implications, you don't want — or need — to enable Application Control for every policy.

We recommend that you enable Application Control for these types of policies:

- Any outbound policy that handles HTTP or HTTPS traffic
- VPN policies that use 0.0.0.0/0 routes (default-route VPNs)
- Any outbound policy if you are not sure how the policy is used
- Policies that use the 'Any' protocol
- Policies that use an 'Any-*' alias, for example Allow 'Any-Trusted' to 'Any-External', on a specific port/protocol

It is not necessary to enable Application Control for a policy if you control the network on both sides of a traffic flow the policy handles. Some examples of these types of policies include:

- POS systems
- Intranet web applications
- Internal databases and traffic in a DMZ

It usually not necessary to enable Application Control for policies that are restricted by port and protocol and that allow only a known service. Some examples of these types of policies include:

- Default WatchGuard policies
- DNS traffic
- RDP
- VoIP - SIP and H.323 application layer gateways

To block evasive applications that dynamically use different ports, you must enable Application Control to block those applications in all of your policies. For more information about evasive applications, see *Manage Evasive Applications*.

For some examples of how to use Application Control with policies, see *Application Control Policy Examples*.

Global Application Control Action

The Global Application Control action is created by default and cannot be removed. You can configure the Global Application Control action to control overall corporate policy. For example you can:

- Block all games
- Block use of peer-to-peer applications

The Global Application Control action does not apply to traffic unless you enable Application Control for policies in your configuration. You can assign the Global Application Control action directly to a policy, or you can use the Global Application Control action as a secondary action if traffic does not match the applications configured in a user-defined Application Control action assigned to a policy.

You can create more specific application actions to implement rules that apply to user groups or to specific interfaces. For example, you might want to apply some specific rules to allow one department to have access to an application.

If you know that an application is specifically restricted to a specific port, you can apply an Application Control action to a packet filter or proxy policy on that port only. If not, you must apply the Application Control action to an outgoing policy that covers all ports to make sure that you capture all possible traffic for the application.

Configure Application Control Actions

To block application traffic, you need to create Application Control actions. You apply these actions to one or more policies to enforce consistent rules for application usage. An Application Control action contains a list of applications and associated actions. For each application, you can specify whether to drop or allow the connection. You also configure what action to take if traffic that does not match the applications is detected.

For each application, you can choose one of these actions:

- **Drop** — Block the selected application.
- **Allow** — Allow the selected application

For some applications, you can control specific application behaviors. For each behavior, you can set the action to **Drop** or **Allow**. The behaviors you can control depend on the application. The application behaviors you can control are:

- **Authority** — Log in
- **Access** — Command to access a server or peer
- **Communicate** — Communicate with server or peer (chat)
- **Connect** — Unknown command (P2P connect to peer)
- **Games** — Games
- **Media** — Audio and video
- **Transfer** — File transfer

For each Application Control action, you configure an action to take if traffic does not match the configured applications. You can set this action to:

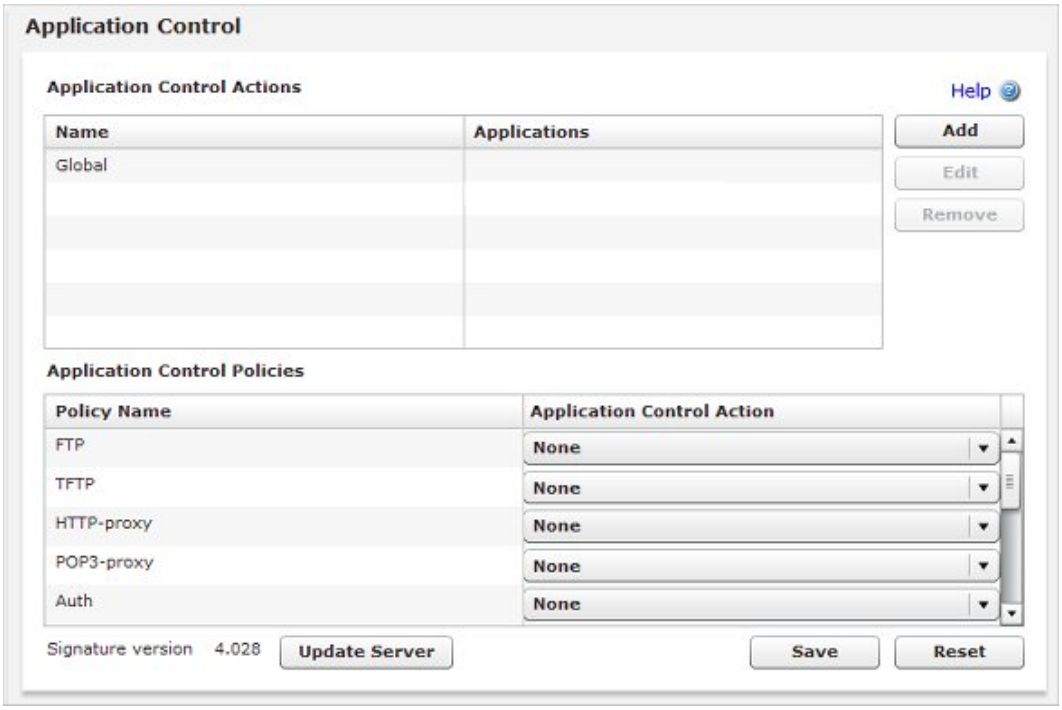
- **Allow** — Allow traffic that does not match the configured applications
- **Drop** — Drop traffic that does not match the configured applications
- **Use Global Action** — Use the Global Application Control action if traffic does not match

When you set the action to take if traffic does not match to **Use Global action**,Application Control uses the **Global** Application Control action for any traffic that does not match. You can also assign the Global Application Control action to a policy. The **Global** Application Control action is created by default and cannot be removed.

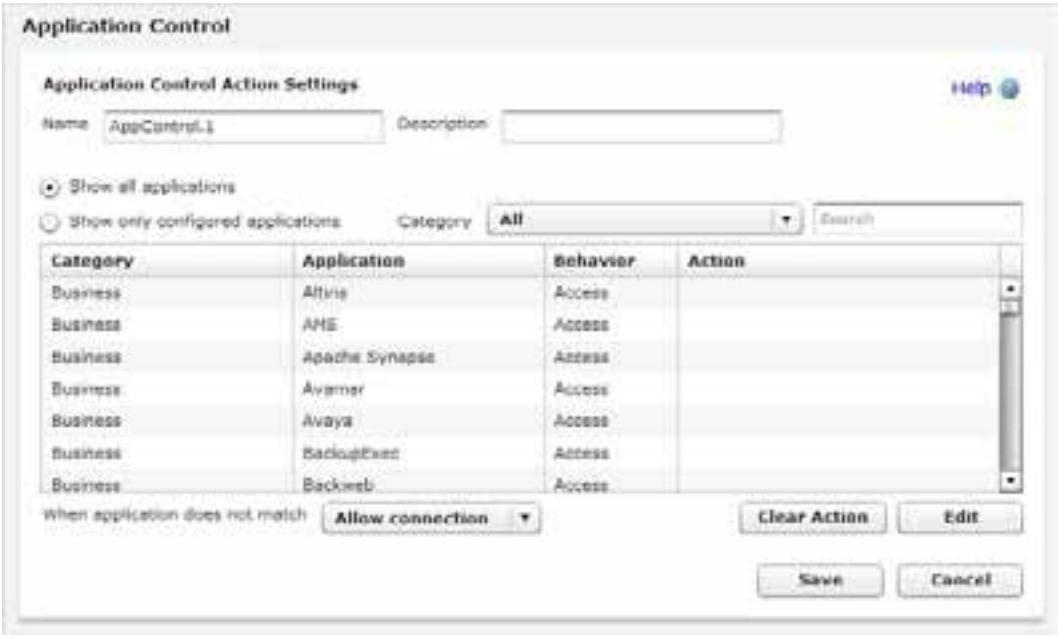
Add or Edit Application Control Actions

To see and edit all of the Application Control actions:

1. Select **Subscription Services > Application Control**.
   The Application Control page appears.



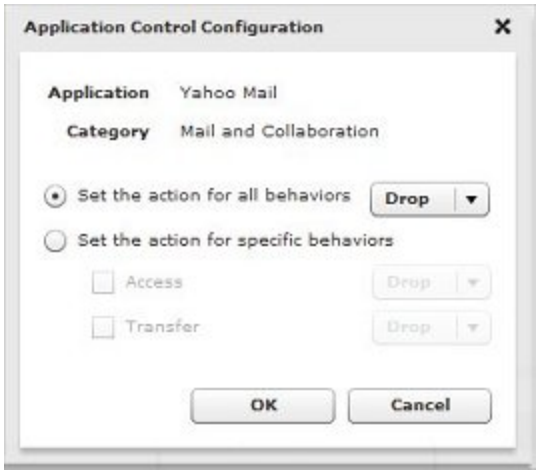
2. To create a new Application Control action, click **Add**.
   Or, to edit an action, click the action name and click **Edit**.
   The Application Control Actions dialog box appears.



3. If this is a new action, in the **Name** text box, type the name for the action. Optionally, type a **Description**.
4. To filter the application list, use these options:

   - **Show all applications** — Show all applications you can configure.
   - **Show only configured applications** — Show the applications that have an action configured
   - **Category** — Filter by application category
   - **Search** — Search for applications that contain a specific word or phrase

5. To configure an application for this Application Control action, click an application in the list. Then click **Edit**.
   The Application Control Configuration dialog box appears.



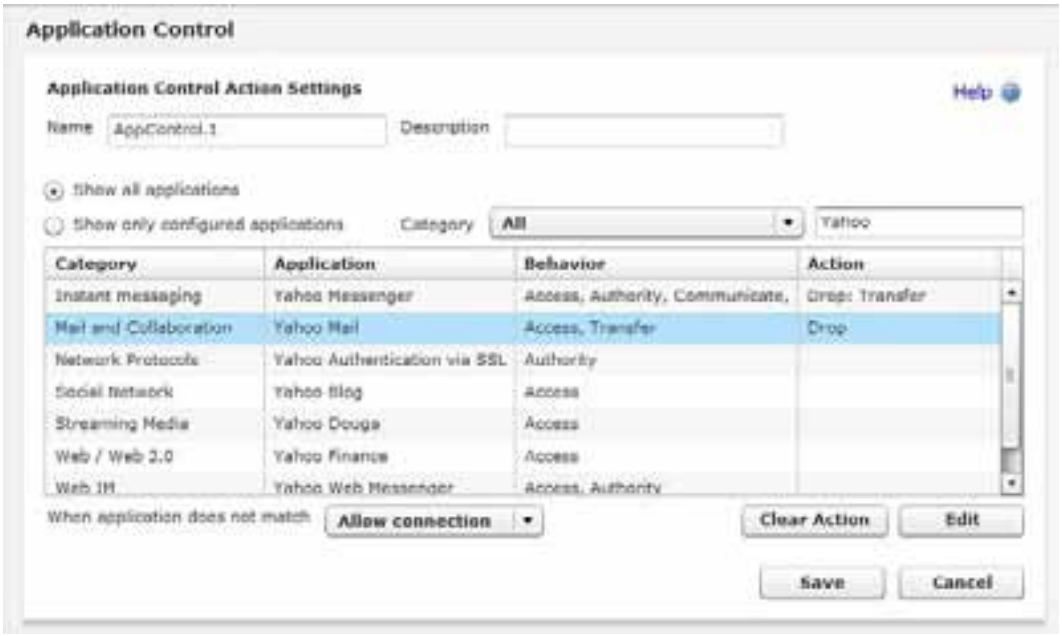
6. From the **Set the action for all behaviors** drop-down box, select the action to take for this application

- Select **Drop** to block the selected application.
- Select **Allow** to allow the selected application.

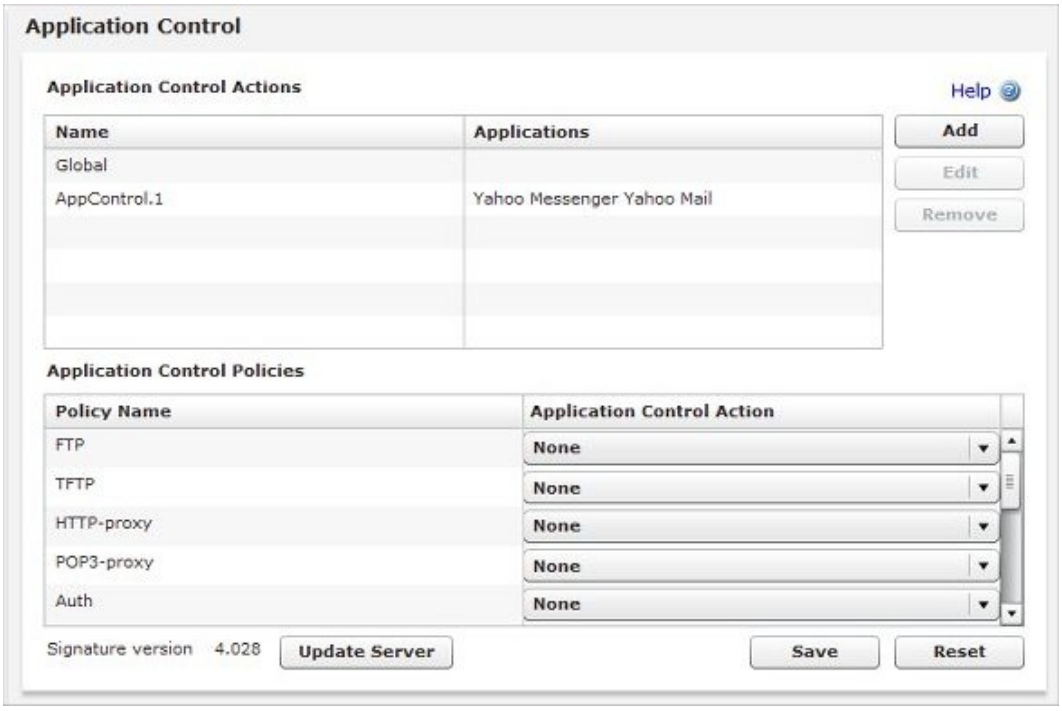
Or, select **Set the action for specific behaviors**. Select the check box for each behavior to control. Select **Drop** or **Allow** for each selected behavior.

> ***Note*** *If you select multiple applications, you can set the action to apply to all selected applications, but you cannot set the action for specific behaviors.*

7. Click **OK**.
   The configured action appears in the Action column.



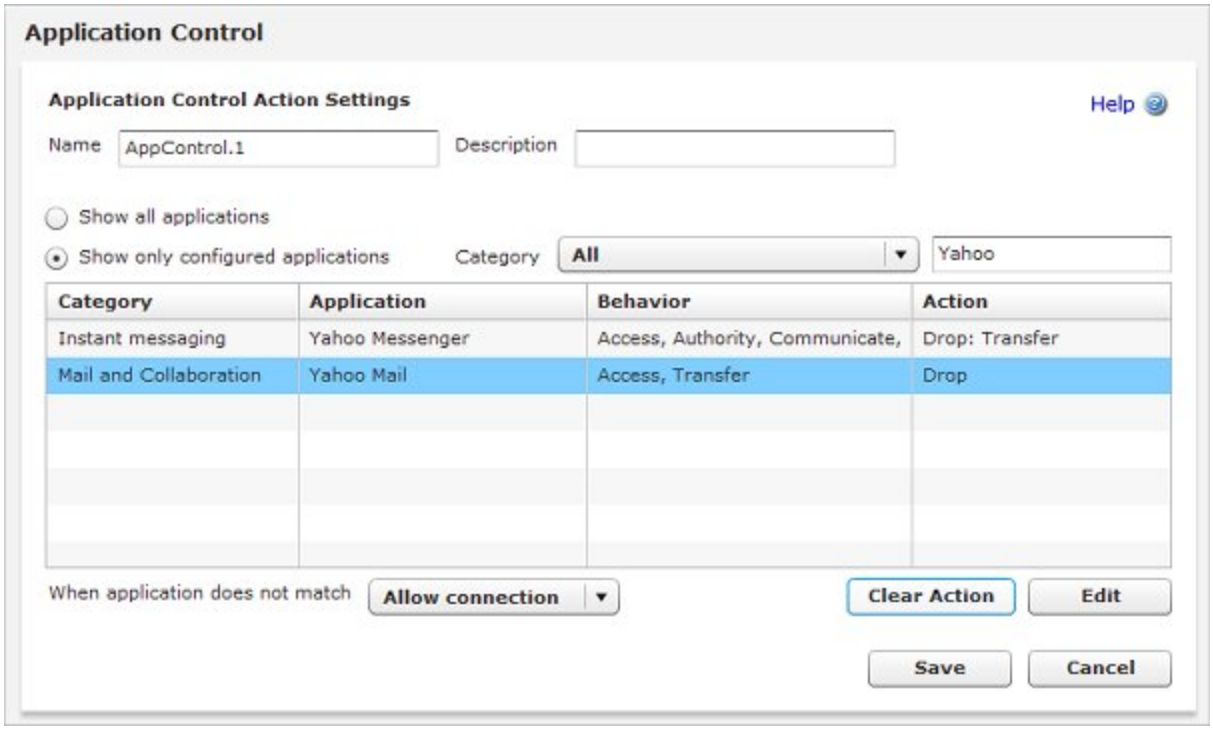
8. Click **Save** to save the Application Control action.
   The Application Control action is added to the list, but is not yet applied to any policy.



Remove Configured Applications From an Application Control Action

To remove a configured application from an Application Control action:

1. Select **Subscription Services > Application Control**.
   The Application Control page appears.
2. Select the Application Control action to edit. Click **Edit**.
   The settings for the selected Application Control Action appear.
3. To show only the configured applications, select **Show only configured applications**
   The list updates to show only the applications configured for this Application Control action.



4. Select one or more configured applications you want to remove from this Application Control action.
5. To clear the action for the selected applications, click **Clear Action**.
   The action for the selected applications is cleared. The application is removed from the configured applications list.
6. Click **Save** to save the Application Control action.

Apply an Application Control Action to a Policy

When you create an Application Control action, it is not automatically applied to your policies. There are two ways you can apply an application control to a policy.

- Select which Application Control action to enable for each policy in the **Application Control Policies** section of the Application Control page .
  For more information, see *Configure Application Control for Policies*.
- Change the Application Control action when you edit a policy
  For more information, see *Enable Application Control in a Policy*.

Remove Application Control Actions

From the Application Control page, you can remove any Application Control action that is not used in a policy. To remove an application, click the Application Control action. Then click **Remove**.

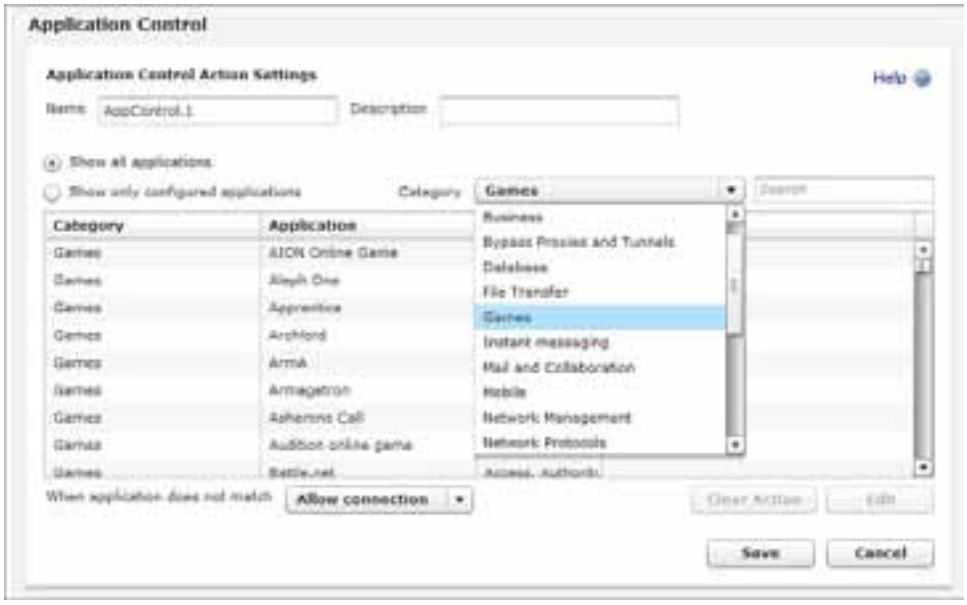
Use Categories

Categories are used to classify applications in Application Control reports. Categories also provide a convenient way to find applications when you edit an Application Control action. There is also a search option if you want to find a specific application.

You can select a group of applications by category to conveniently restrict use of a set of applications that do not have legitimate business value. A good example is the **Games** application category.

To block all applications in the Games category for an Application Control action:

1. From the **Category** drop-down list, select **Games**.
   All Applications in the Games category appear.



2. Select the first application in the list. Press the **Shift** key while you select the last application.
   All applications in the category are selected.
3. Click **Edit** to set the action for the selected applications to **Drop**.
4. Click **OK**.

If you configure Application Control to block all applications in a category, be aware of everything that is included in the category and the expected consequences. For example, SWF (Shockwave Flash) is included in the streaming media category. Flash is used widely in many web sites to deliver content.

We do not recommend that you configure Application Control to block general categories like Web / Web 2.0, Business, or Network Protocols. It is highly likely that there could be an application blocked that may not have the consequences that you intend.

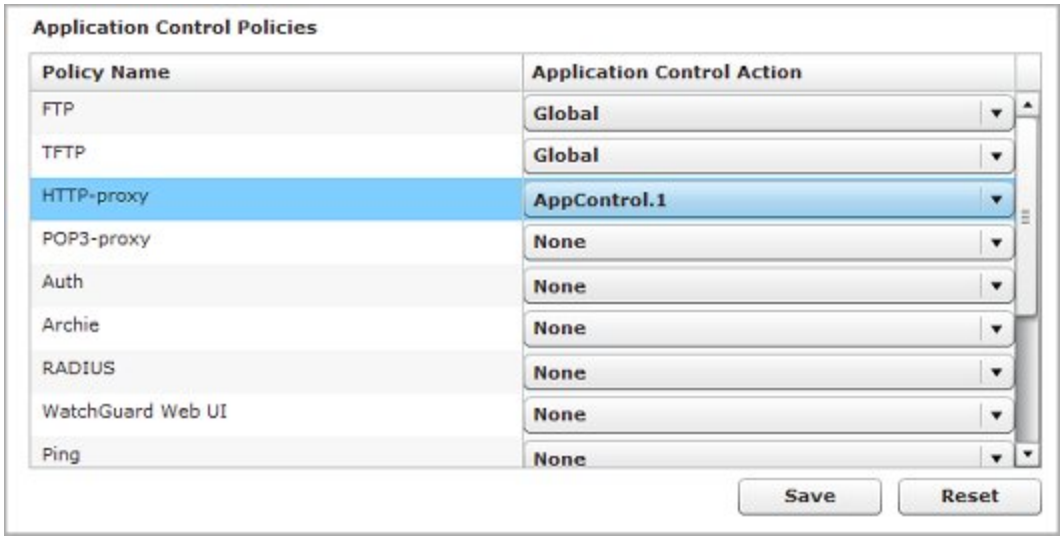
It is a good practice to set up Application Control to send log messages and report on all activity for a period of time before you configure any actions that block applications.

> **Note** *When you configure an Application Control action to block all applications in a category, this selects all applications currently in the category. Application Control signatures are updated frequently. If new applications are added to the category later, these new applications are not automatically blocked by Application Control.*

Configure Application Control for Policies

Application Control is configured globally, but is not used by a policy unless you enable it. After you create an Application Control action in the Application Control configuration, you can change the Application Control action enabled for each policy.

1. Select **Subscription Services > Application Control**.
   The Application Control Actions page appears. The Application Control Policies section shows the Application Control action enabled for each policy.



2. To change the Application Control action for a policy, select the **Application Control Action** column for that policy.
   The available Application Control actions appear in the drop-down list.
3. From the drop-down list, select an Application Control action.
   Or, to disable Application Control for the selected policy, select **None**.
4. Click **Save**.

Enable Application Control in a Policy

To enable Application Control in the policy configuration:

1. Select **Firewall > Firewall Policies**.
2. Add or edit a policy.
3. Select the **Enable Application Control** check box..

4. From the adjacent drop-down list, select the Application Control action to use for this policy.
5. Click **Save**.

Get Information About Applications

When you configure Application Control, or when you look at Application Control reports, you might see application names you are not familiar with. To get information about any application that Application Control can identify, you can look up the application on the WatchGuard Application Control Security Portal at http://www.watchguard.com/SecurityPortal/AppDB.aspx.

On the Application Control Security Portal page, you can:

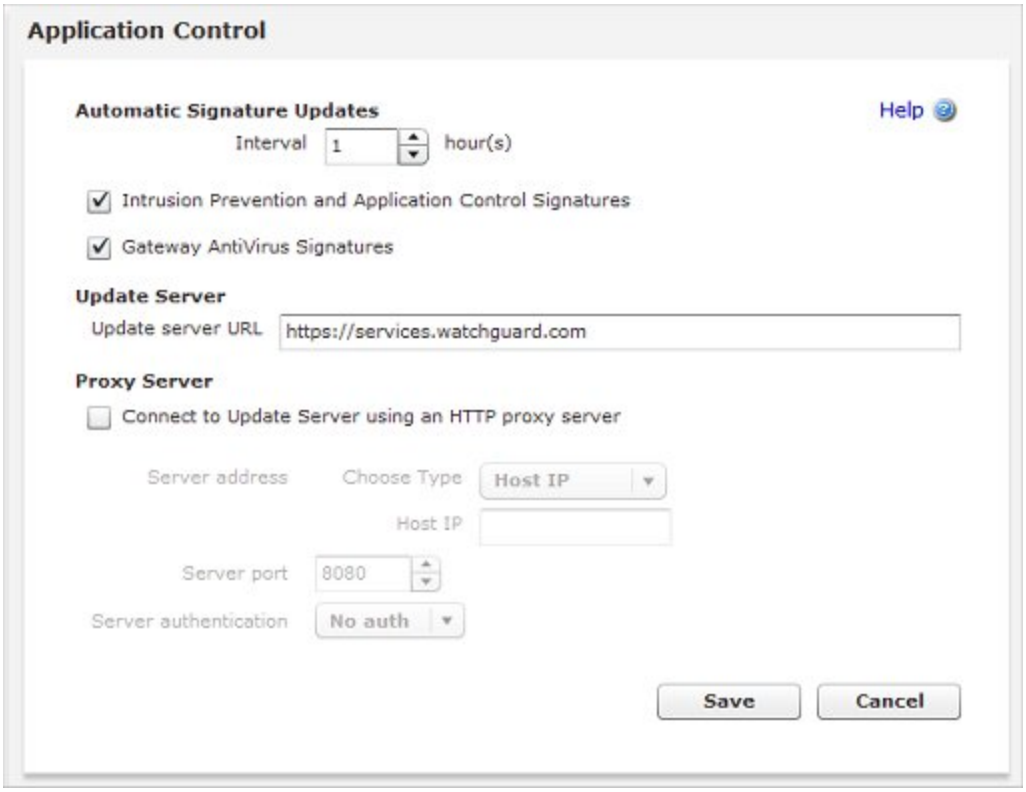
- See a list of all applications that Application Control can identify.
- Search for an application by name.
- See a description of the application and supported application behaviors.

Configure the Application Control Update Server

Application Control downloads signature updates from a signature update server. Gateway AV, IPS, and Application Control use the same update server settings. When you change configuration of the update server for any of these subscription services, the settings apply to all three services.

Configure Signature Updates

1. Select **Subscription Services > Application Control**.
2. Click **Update Server**.
   The Update Server dialog box appears.



3. From the **Interval** drop-down list, enter the number of hours between automatic updates.
4. Select the **Intrusion Prevention and Application Control Signatures** check box to automatically update signatures at the selected update interval.

Do not change the **Update server URL** unless you are told to do so by WatchGuard. If you change the URL accidentally or incorrectly, click **Reset** to return to the last saved setting.

Connect to the Update Server Through an HTTP Proxy Server

If your XTM device must connect through an HTTP proxy to get to the signature update server, you must add information about the HTTP proxy server to your update server configuration.

1. In the **Proxy Server** section, select the **Connect to Update server using an HTTP proxy server** check box.
2. In the **Server address** text box, type the IP address or host name of your HTTP proxy server.
3. Most HTTP proxy servers receive requests on port 8080. If your HTTP proxy uses a different port, type it in the **Server port** field.
4. From the **Server authentication** drop-down list, select the type of authentication your HTTP proxy server uses.
   - If your HTTP proxy does not require authentication, select **NoAuth** .
   - If your HTTP proxy server requires **NTLM** or **Basic** authentication, type your **User name**, **Domain**, and **Password** in the text boxes.
5. Click **Save**.

Block Access from the Trusted Network to the Update Server

If you do not want to allow all users on your trusted network to have unfiltered access to the IP address of the signature database, you can use an internal server on your trusted network to receive the updates. You can create a new HTTP proxy policy with *HTTP-Proxy: Exceptions* or an HTTP packet filter policy that allows traffic only from the IP address of your internal server to the signature database.

Update Signatures Manually

For information about how to see the status of Application Control signature updates, and how to manually force an update to the most current signatures, see *Subscription Services Status and Manual Signatures Updates*.

Application Control and Proxies

There is some duplication of the functions available in the Application Control service and in the WatchGuard proxy policies. In general, the proxies perform different and more detailed inspection and provide more granular control over the type of content. For example with the HTTP proxy, you can

- Adjust timeout and length limits of HTTP requests and responses to prevent poor network performance, as well as several attacks
- Customize the deny message that users see when they try to connect to a web site blocked by the HTTP proxy
- Filter web content MIME types

- Block specified path patterns and URLs
- Deny cookies from specified web sites

Proxies are also used to provide Gateway AntiVirus, WebBlocker, and Reputation Enabled Defense services.

By default, the HTTP proxy action blocks the download of these content types:

- Java bytecode
- ZIP archives
- Windows EXE/DLL files
- Windows CAB archive

The Application Control feature does not override settings in the proxy policy configuration. For example, if you allow YouTube in Application Control, but the proxy policy is already configured with an action to block streaming video, YouTube videos are still blocked.

Application Control and WebBlocker

If both WebBlocker and Application Control are configured in the same policy, and the traffic matches for a web site and application, the Application Control action triggers first. For example, consider facebook.com. All access to facebook.com can be blocked in WebBlocker if the “personals and dating” category is blocked.

One advantage of WebBlocker is that it displays a specific warning message in the user’s browser when a site is blocked. If your company policy is to restrict all access to Facebook, it may be appropriate to block it in WebBlocker. You can either block the “personals and dating” category or add a WebBlocker exception. Application Control provides more granular control over applications and their associated subfunctions. With Application Control, it is possible to allow access to Facebook, but not allow access to Facebook Games.

Manage SSL Applications

Many web-based applications are accessible through SSL (HTTPS), as well as through HTTP. Organizations offer encrypted SSL connections to provide more security to users. SSL encryption can also make applications more difficult for Application Control to detect. When you block applications that are accessible through SSL, you might also need to specifically block the SSL login for that application to make sure that you block all access to that application.

For example, when you select to block the application **Google-Finance**, this blocks Google’s financial applications. But it does not block Google Finance over SSL. To block that, you must also block the application **Google Authentication via SSL**. It is important to understand that, once you block Google Authentication over SSL, you lose control over the granularity of all Google SSL applications to block. For example, access to Google Docs and Gmail over SSL is also blocked.

Similar behavior occurs for some Microsoft and Yahoo applications when they are accessed over SSL. There are corresponding signatures for Authentication over SSL for Microsoft and Yahoo and many other applications in the Application Control application list. To granularly manage these types of applications, you might want to block Authentication over SSL. Then you can use the application signatures to granularly configure the applications that can be used over the http access that is allowed.

Manage Evasive Applications

Some applications use dynamic ports and protocols, encryption, and other techniques to make the application traffic difficult to detect and manage. For these types of applications, there can be some limitations to the application behaviors that Application Control can manage.

One example of this type of evasive application is Skype, a popular peer-to-peer (P2P) network application. The Skype client uses a dynamic combination of ports that include outbound ports 80 and 443. Skype traffic is very difficult to detect and block because it is encrypted, and because the Skype client is able to bypass many network firewalls.

For information about how to block Skype, see *Block User Logins to Skype*.

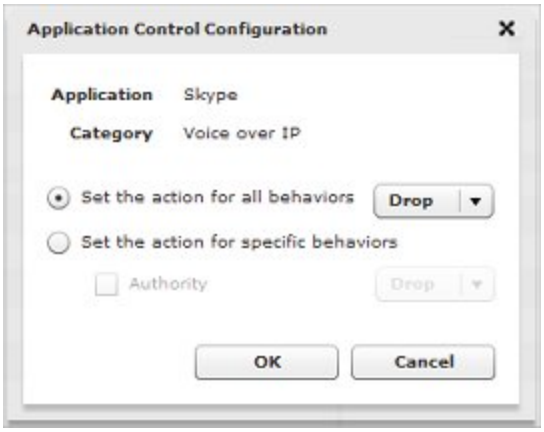
Block User Logins to Skype

You can configure Application Control to block a user login to the Skype network. It is important to understand that Application Control can only block the Skype login process. It cannot block traffic for a Skype client that has already logged in and has an active connection. For example:

- If a remote user logs in to Skype when the computer is not connected to your network, and then the user connects to your network while the Skype client is still active, Application Control cannot block the Skype traffic until the user logs off the Skype network or restarts their computer.
- When you first configure Application Control to block Skype, any users that are already logged in to the Skype network are not blocked until they log off the Skype network, or restart their computers.

To configure an Application Control action to block user logins to Skype:

1. Select **Subscription Services > Application Control**.
   The Application Control page appears.
2. Double-click the Application Control action you want to edit.
3. From the list of applications, select the **Skype** application. To quickly find the Skype application, type "skype" in the search text box.
4. Click **Edit**.



5. Set the action for all behaviors to **Drop**.
6. Click **OK** to save the action for the Skype application.
7. Click **Save** to save the Application Control action.

After you configure the Application Control action to block Skype, you must apply this Application Control action to all policies in your configuration. You can do this when you edit the policy, or in the **Application Control Policies** section of the Application Control configuration page.

If you have a high precedence policy that allows all DNS, you must configure the DNS policy to use the Application Control action that blocks Skype.

Manage Applications that Use Multiple Protocols

Many applications today, especially instant messaging and peer-to-peer applications, use multiple protocols and techniques to transfer files. For example, there are many clients that use the BitTorrent protocol and other protocols to transfer files. To fully block applications that use multiple protocols, you must configure Application Control with a combination of actions. This is best illustrated as an example.

Example: Block FlashGet

When you select the BitTorrent Series application in an Application Control action, Application Control uses a set of rules that identify the BitTorrent protocol for peer-to-peer file sharing.

FlashGet is a client application that is used for file sharing. The FlashGet client application can use the BitTorrent peer-to-peer protocol to download files, or it can use simple HTTP downloads, FTP file transfer, or the proprietary FlashGet protocol.

If you do not block, but only record activity in the log files, BitTorrent downloads that are triggered by the FlashGet client appear in the log files and reports as both FlashGet and BitTorrent application activity, at different times.

To block all possible file transfers by the FlashGet client, you must configure Application Control to block FlashGet, and also to block BitTorrent Series, Web File Transfer, and FTP Applications. It is important to understand that if you block BitTorrent Series, Application Control also blocks BitTorrent use by all other applications. There is no way to block BitTorrent use by FlashGet, but allow it for other applications.

If you block FlashGet, but do not block BitTorrent or Web File Transfer, downloads through BitTorrent or HTTP are not blocked, even if the downloads are started by the FlashGet client.

If you block Web File Transfer or FTP Applications, this functionality is blocked for all applications. There is no way to block HTTP file transfers or FTP file transfers for FlashGet but allow it for other applications.

File Transfer Applications and Protocols

The table below shows some common applications and the variety of protocols that they use for file transfer. The names of applications and protocols in the table correspond to application names in Application Control.

Category	Application	Protocols and Applications Used
P2P	Thunder Series	Thunder Private Protocol Web File Transfer ASFV1, MP4,MMS,FLV,RMVB, SWF,AVI,MP3, WMA, MOV, WMA, ASF BitTorrent Series FTP Applications
P2P	BitTorrent	BitTorrent Series Web File Transfer ASFV1, MP4, MMS, FLV, RMVB, SWF, AVI, MP3, WMA, MOV, WMA, ASF FTP Applications

Category	Application	Protocols and Applications Used
P2P	FlashGet	BitTorrent Series Web File Transfer ASFV1, MP4, MMS,FLV,RMVB, SWF,AVI,MP3, WMA, MOV, WMA, ASF FTP Applications
P2P	QQDownload	BitTorrent Series Web File Transfer ASFV1, MP4, MMS,FLV,RMVB, SWF,AVI,MP3, WMA, MOV, WMA, ASF FTP Applications QQ Private Protocol
MEDIA	QQLive	QQLive ASFV1, MP4, MMS,FLV,RMVB, SWF,AVI,MP3, WMA, MOV, WMA, ASF QQ Private Protocol QQ/TM
MEDIA	PPTV	PPTV (PPLive) ASFV1, MP4, MMS,FLV,RMVB, SWF,AVI,MP3, WMA, MOV, WMA, ASF
MEDIA	PPStream	PPStream ASFV1, MP4, MMS,FLV,RMVB, SWF,AVI,MP3, WMA, MOV, WMA, ASF
MEDIA	UUSee	UUSee ASFV1, MP4, MMS,FLV,RMVB, SWF,AVI,MP3, WMA, MOV, WMA, ASF
IM	QQ	QQ/TM QQ Private Protocol
GAME	QQ/QQFO	QQ Game QQ Private Protocol

To fully block all file transfers through applications that use multiple protocols and applications, you must block the application, and you must block all protocols and applications the application uses. There are some common applications and protocols that you may not want to block because they are used by many applications.

For a description of any of the applications or protocols in this table, you can look up the application on the WatchGuard Application Control Security Portal at http://www.watchguard.com/SecurityPortal/AppDB.aspx.

Monitor Downloads and File Transfers

Application Control includes two general purpose applications called **Web File Transfer** and **FTP Applications** that you can use to record log messages for common download and file transfer activity.

Web File Transfer

Web File Transfer is a general application that detects the download of common file formats that are often downloaded through popular P2P and File Transfer programs, including: bz2 ,doc , exe , gz, pdf, ppt, rar , rpm, tar, xls, zip, torrent, dll, manifest, xdap, deploy, xps, , xaml, application, mkv, and dat. It also covers HTTP upload of files.

FTP Applications

FTP Applications is an application that detects a range of FTP commands —pass, list, eprt, epsv, create directory, delete directory, get (binary and ascii), put (binary and ascii), passive and active file transfer.

These applications are best used to generate log messages of activity. Consider the implications carefully before you decide to block these applications.

Manage Facebook Applications

Some applications, such as Facebook, contain multiple application types that Application Control can identify. You can use Application Control to granularly control which applications your users can use.

Facebook is a social networking site that includes a large number of features and applications. You can use Application Control to block some or all Facebook applications. For example, you can configure an Application Control action that allows Facebook, but blocks the use of Facebook games or IM. Or you can block the use of all Facebook applications.

You can see the list of Facebook applications when you configure an Application Control action for your device, or you can search for *facebook* in the Application Control security portal at http://www.watchguard.com/SecurityPortal/AppDB.aspx.

Application Control can identify and block different types of Facebook activity.

Facebook Web IM

Identifies Facebook chat sessions.

Facebook

Identifies attempts to log in to Facebook or see Facebook web pages.

Facebook Game

Identifies the top 25 most popular Facebook games.

Facebook Applications

Identifies all applications available through the Facebook apps directory.

Facebook Plug-in

Identifies all Facebook social plug-ins that can be embedded in other sites on the Internet. This includes plug-ins such as **Like** and **Comments**. To see the current list of Facebook social plug-ins, see http://developers.facebook.com/plugins.

Facebook Post

Identifies information posts to Facebook. This includes:

- Post a message to the wall
- Share status
- Share a link

Facebook Video

Identifies video uploads to Facebook.

Facebook Picture

Identifies photo uploads to Facebook.

Facebook EditProfile

Identifies Facebook user profile updates.

To block Facebook applications:

1. Create or edit an Application Control action.
2. In the search text box, type `facebook`.
   The list of applications is filtered to show only the Facebook applications.
3. Select one or more Facebook applications to block.
4. Select **Edit**. Set the action for the selected applications to **Block**.
5. Apply the Application Control action to your policies.

Application Control Policy Examples

You can use the **Global** Application Control action with other Application Control actions to allow or block different applications based on the time of day, or based on the user name or user group. To do this, you create Application Control actions that block or allow different sets of applications. Then you apply different Application Control actions to different policies as described in the examples below.

Each of the examples below enables Application Control actions for a single type of policy. If your configuration includes other policy types, such as TCP-UDP, or Outgoing, you can use the same steps to set up a two-tiered Application Control configuration for those policies. The policies you need to apply an Application Control action to depend on which policies exist in your configuration, and which applications you want to block. For example, if you want to block an application that you know uses FTP, you must enable the Application Control action for the FTP policy.

For recommendations on which types of policies to configure for Application Control, see *Policy Guidelines for Application Control*.

Allow an Application For a Group of Users

If the Global Application Control action blocks an application, you can create a separate Application Control action to allow that same application for a department or other user group. For example, if you want to block the use of MSN instant messaging for most users, but you want to allow this application for the people in the Sales department, you can create different Application Control actions and policies to get this result.

If you already have an **HTTP** packet filter policy that applies to all users, you can use these steps to allow different applications for the Sales department.

1. Configure the **Global** Application Control action to block MSN instant messaging, and any other applications you do not want to allow.
2. Apply the **Global** Application Control action to the existing **HTTP** packet filter policy.
3. Create a new Application Control action to allow MSN instant messaging. For example, you could call this action, **AllowIM**. Configure this action to use the **Global** action when the application does not match.
4. Create an HTTP policy for the users in the Sales department. For example, you could call this policy **HTTP-Sales**. For information about how to create a policy for a group of users, see *Use Authorized Users and Groups in Policies*.
5. Apply the **AllowIM** Application Control action to the **HTTP-Sales** policy.
6. Enable logging for the **HTTP** and **HTTP-Sales** policies.
   You must enable logging to see information about Application Control in the log files and reports.

In this example, the two resulting HTTP policies could look like this:

Policy: HTTP-Sales

HTTP connections are: **Allowed**
From: **Sales** To: **Any-External**
Application Control: **AllowIM**

Policy: HTTP

HTTP connections are: **Allowed**
From: **Any-Trusted** To: **Any-External**
Application Control: **Global**

The **AllowIM** Application Control action applied to the **HTTP-Sales** policy acts as an exception to the Global Application Control action. The users in the Sales group can use MSN instant messaging, but cannot use any other applications blocked by the **Global** Application Control action.

If this device configuration included other policies, such as HTTP-Proxy, TCP-UDP, or Outgoing, that could be used for IM traffic, you can repeat the steps above to set up a two-tiered Application Control configuration for other policies.

Block Applications During Business Hours

You can use Application Control with policies to block different applications based on the time of day. For example, you might want to block the use of games during business hours. To block applications during certain hours, you can use Application Control with policies that have an operating schedule.

If you already have an **HTTP-Proxy** policy that does not have an operating schedule, use these steps to add a new policy and Application Control action to block applications during business hours.

1. Configure the **Global** Application Control action to block applications you want to always block.
2. Apply the **Global** Application Control action to the existing **HTTP-Proxy** policy.
3. Create a schedule called **Business-Hours** that defines the business hours. For more information about schedules, see *Create Schedules for XTM Device Actions*.
4. Create a new HTTP-Proxy policy that uses the **Business-Hours** schedule you configured. For example, you could call the new policy **HTTP-Proxy-Business**. For more information about how to set the schedule for a policy, see *Set an Operating Schedule*.
5. Create an Application Control action that blocks the applications you want to block during business hours. For example, you could call this action **Business**.
6. Apply the **Business** Application Control action to the **HTTP-Proxy-Business** policy.
7. Enable logging for the **HTTP-Proxy** and **HTTP-Proxy-Business** policies.
   You must enable logging to see information about Application Control in the log files and reports.

In this example, the two resulting policies could look like this:

Policy: HTTP-Proxy-Business

HTTP connections are: **Allowed**
From: **Sales** To: **Any-External**
Application Control: **Business**

Policy: HTTP-Proxy

HTTP connections are: **Allowed**
From: **Any-Trusted** To: **Any-External**
Application Control: **Global**

The **Business** Application Control action in the **HTTP-Proxy-Business** policy blocks games only during business hours. All other applications in the **Global** Application Control action are blocked at all times of day.

If this device configuration included other policies, such as HTTP, TCP-UDP, or Outgoing, that might be used for games traffic, you can repeat the steps above to set up a two-tiered Application Control configuration for other policies.

For more information about policy precedence, see *About Policy Precedence*.

30 Quarantine Server

About the Quarantine Server

The WatchGuard Quarantine Server provides a safe mechanism to quarantine any email messages suspected or known to be spam or to contain viruses. The Quarantine Server is a repository for email messages that the SMTP proxy decides to quarantine based on analysis by spamBlocker or Gateway AntiVirus. Granular control allows you to configure preferences for mail disposition, storage allocation, and other parameters.

> ***Note*** *The SMTP proxy requires a Quarantine Server if you configure it to quarantine emails that spamBlocker classifies as spam, or if you configure Gateway AntiVirus to quarantine emails from a specified category.*

The Quarantine Server provides tools for both users and administrators. Users get regular email message notifications from the Quarantine Server when they have email stored on the Quarantine Server. Users can then click a link in the email message to go to the Quarantine Server web site. On the Quarantine Server web site, they see the sender and the subject of the suspicious email messages. For spam email, the user can release any email messages they choose to their email inbox, and delete the other messages. Administrators can configure the Quarantine Server to automatically delete future messages from a specific domain or sender, or those that contain specified text in the subject line.

The administrator can see statistics on Quarantine Server activity, such as the number of messages quarantined during a specific range of dates, and the number of suspected spam messages.

The SMTP proxy adds messages to different categories based on analysis by spamBlocker and Gateway AntiVirus. The Quarantine Server displays these classifications for quarantined messages:

- Suspected spam — The message could be spam, but there is not enough information to decide.
- Confirmed spam — The message is spam.
- Bulk — The message was sent as commercial bulk email .
- Virus — The message contains a virus.
- Possible virus — The message might contain a virus, but there is not enough information to decide.

You install the Quarantine Server as part of the WatchGuard System Manager installation.

To learn about how to set up a Quarantine Server, see the Fireware XTM WSM User Guide at http://www.watchguard.com/help/documentation/.

Configure the XTM Device to Quarantine Email

After you install and configure the Quarantine Server, you must update the XTM device configuration to use the Quarantine Server.

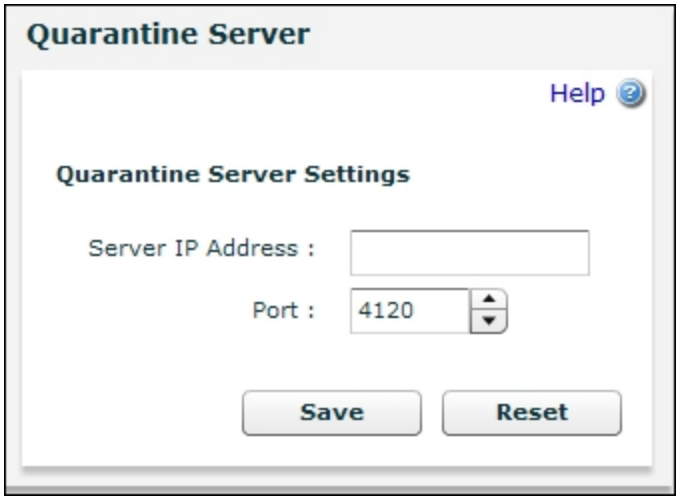
There are two steps:

1. Configure the Quarantine Server IP address as described in *Define the Quarantine Server Location on the XTM Device* on page 761.
2. Set up spamBlocker and Gateway AntiVirus actions for the SMTP proxy to quarantine email.
   For more information, see *Configure spamBlocker to Quarantine Email* on page 692, and *Configure Gateway AntiVirus to Quarantine Email* on page 715.

Define the Quarantine Server Location on the XTM Device

You must define the location of the Quarantine Server in the XTM device configuration. You can use Fireware XTM Web UI to specify the IP address of the of the Quarantine Server where the XTM device sends email messages to be quarantined.

1. Select **Subscription Services > Quarantine Server**.
   The Quarantine Server settings page appears.



2. Type the IP address for the Quarantine Server. We recommend that you do not change the Quarantine Server port unless asked to do so by a WatchGuard technical support representative.
3. Click **Save**.