WatchGuard Certified Training

Fireware Basics

Courseware: WatchGuard System Manager 10
Student Guide

Part Number: 2270-000
# Table of Contents

## Course Introduction

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training Options</td>
<td>1</td>
</tr>
<tr>
<td>Necessary Equipment and Software</td>
<td>1</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>2</td>
</tr>
<tr>
<td>Certification</td>
<td>2</td>
</tr>
<tr>
<td>Training Scenario</td>
<td>2</td>
</tr>
</tbody>
</table>

## Getting Started

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What You Will Learn</td>
<td>3</td>
</tr>
<tr>
<td>Start with the WatchGuard System Manager</td>
<td>3</td>
</tr>
<tr>
<td>WSM Components</td>
<td>4</td>
</tr>
<tr>
<td>Register the Firebox with LiveSecurity</td>
<td>4</td>
</tr>
<tr>
<td>Exercise 1: Create a Configuration File with the Quick Setup Wizard</td>
<td>5</td>
</tr>
<tr>
<td>Exercise 2: Open WSM and Connect to Fireboxes and Servers</td>
<td>5</td>
</tr>
<tr>
<td>Connect to a Firebox</td>
<td>5</td>
</tr>
<tr>
<td>Connect to a Management Server</td>
<td>7</td>
</tr>
<tr>
<td>Exercise 3: Open Policy Manager</td>
<td>8</td>
</tr>
<tr>
<td>Related Courseware and Information</td>
<td>9</td>
</tr>
<tr>
<td>Test Your Knowledge</td>
<td>10</td>
</tr>
</tbody>
</table>

## Administration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What You Will Learn</td>
<td>11</td>
</tr>
<tr>
<td>Manage Configuration Files and Firebox Properties</td>
<td>11</td>
</tr>
<tr>
<td>Exercise 1: Open and Save Configuration Files</td>
<td>12</td>
</tr>
<tr>
<td>Exercise 2: Configure a Firebox for Remote Administration</td>
<td>13</td>
</tr>
<tr>
<td>Exercise 3: Change the Firebox Passphrases</td>
<td>13</td>
</tr>
<tr>
<td>Exercise 4: Create and Restore a Firebox Backup Image</td>
<td>14</td>
</tr>
<tr>
<td>Exercise 5: Add Firebox Identification Information</td>
<td>15</td>
</tr>
<tr>
<td>Related Courseware and Information</td>
<td>16</td>
</tr>
<tr>
<td>Test Your Knowledge</td>
<td>17</td>
</tr>
</tbody>
</table>

## Network Settings

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What You Will Learn</td>
<td>19</td>
</tr>
<tr>
<td>Properties and Features of Firebox Interfaces</td>
<td>19</td>
</tr>
<tr>
<td>Requirements for Firebox Interfaces</td>
<td>20</td>
</tr>
<tr>
<td>About DHCP Server and DHCP Relay</td>
<td>20</td>
</tr>
<tr>
<td>About WINS/DNS</td>
<td>20</td>
</tr>
<tr>
<td>About Drop-In and Routed modes</td>
<td>21</td>
</tr>
<tr>
<td>About dynamic DNS</td>
<td>21</td>
</tr>
<tr>
<td>About secondary networks</td>
<td>21</td>
</tr>
<tr>
<td>Exercise 1: Use a Dynamic IP Address for an External Interface</td>
<td>22</td>
</tr>
<tr>
<td>Configure the External Interface for DHCP</td>
<td>22</td>
</tr>
<tr>
<td>Configure the External Interface for PPPoE</td>
<td>23</td>
</tr>
<tr>
<td>Configure the External Interface for use with Dynamic DNS</td>
<td>24</td>
</tr>
<tr>
<td>Exercise 2: Configure an External Interface with a Static IP Address</td>
<td>25</td>
</tr>
<tr>
<td>Exercise 3: Configure a Trusted Interface as a DHCP Server</td>
<td>26</td>
</tr>
<tr>
<td>Exercise 4: Configure an Optional Interface</td>
<td>27</td>
</tr>
<tr>
<td>Exercise 5: Configure WINS/DNS Server Information</td>
<td>28</td>
</tr>
<tr>
<td>Exercise 6: Configure a Secondary Network</td>
<td>29</td>
</tr>
</tbody>
</table>
Test Your Knowledge ............................................................................................................... 107
FTP Proxy .................................................................................................................................. 109
What You Will Learn .................................................................................................................. 109
What is a Proxy Policy? .............................................................................................................. 109
Proxy Actions ............................................................................................................................. 109
Proxies and the Quick Setup Wizard ......................................................................................... 110
Control File Transfers In and Out of Your Network ............................................................... 110
FTP Proxy Rulesets .................................................................................................................. 111
Exercise 1: Configure an FTP-Client Proxy Action ................................................................. 112
Deny the FTP STOR command .................................................................................................. 113
Control FTP downloads by file extension ................................................................................ 114
Enable alarms for denied connections from FTP clients ......................................................... 115
Exercise 2: Configure an FTP-Server Proxy Action .............................................................. 116
Deny the Delete command ........................................................................................................ 116
Restrict FTP File uploads to text only .................................................................................... 118
Frequently Asked Questions .................................................................................................... 118
Related Courseware and Information ...................................................................................... 118
Test Your Knowledge ............................................................................................................... 120
Email Proxies ............................................................................................................................. 123
What You Will Learn ................................................................................................................ 123
Control the Flow of Email In and Out of Your Network .......................................................... 123
SMTP Rulesets .......................................................................................................................... 123
POP3 Rulesets ........................................................................................................................... 124
Exercise 3: Use the SMTP Proxy to Protect your Mail Server ................................................. 124
Add an incoming SMTP proxy policy ....................................................................................... 124
Edit an existing SMTP proxy policy ....................................................................................... 124
Decrease maximum message size ............................................................................................ 125
Allow and deny content types and filenames .......................................................................... 125
Control mail domain use for incoming traffic ........................................................................ 126
Exercise 4: Control Outgoing SMTP Connections .................................................................. 127
Add an outgoing SMTP proxy policy ....................................................................................... 127
Control email message size ...................................................................................................... 128
Control mail domain use for outbound SMTP ...................................................................... 128
Restrict email by attachment filename ................................................................................. 129
Exercise 5: Using a POP3 Client Policy ................................................................................... 131
Add a POP3 client policy ........................................................................................................ 131
Configure the POP3 policy to lock attachments .................................................................... 131
Related Courseware and Information ...................................................................................... 132
Test Your Knowledge ............................................................................................................... 133
Blocking Spam ........................................................................................................................ 137
What You Will Learn ................................................................................................................. 137
Stop Unwanted Email at the Network Edge .......................................................................... 137
spamBlocker tags ..................................................................................................................... 138
spamBlocker categories ........................................................................................................... 138
spamBlocker exceptions .......................................................................................................... 138
Global spamBlocker settings ................................................................................................... 139
Exercise 1: Activate and Configure a Quarantine Server ....................................................... 140
Prepare the Quarantine Server ............................................................................................... 140
Configure the Firebox to use the Quarantine Server .............................................................. 141
Exercise 2: Activate spamBlocker .......................................................................................... 142
Exercise 3: Configure the spamBlocker Service ................................................................. 143
    Determine what happens to spam email ........................................................................ 143
    Add spamBlocker exceptions ....................................................................................... 144
    Turn on alarms when a virus is detected ..................................................................... 145
Exercise 4: Monitor spamBlocker activity ........................................................................... 146

Related Courseware and Information ........................................................................... 147
Test Your Knowledge ...................................................................................................... 148

DNS Proxy ........................................................................................................................ 149
What You Will Learn ........................................................................................................ 149
Protect a DNS Server On Your Trusted Network ........................................................... 149
    DNS-Incoming rulesets ................................................................................................ 150
    Using the DNS-Outgoing proxy action ....................................................................... 151
Exercise 1: Configure a DNS-Incoming Proxy Action ....................................................... 151
    Add a DNS incoming proxy policy .............................................................................. 152
    Log denials for reporting .......................................................................................... 152
    Allow a DNS query type ............................................................................................ 153
Exercise 2: Use the DNS-Outgoing Proxy Action ............................................................... 155
    Add a DNS outgoing proxy policy ............................................................................ 155
    Block a DNS request by query name ......................................................................... 155
Related Courseware and Information ........................................................................... 156
Test Your Knowledge ...................................................................................................... 157

Web Traffic .................................................................................................................... 159
What You Will Learn ........................................................................................................ 159
Control Web Traffic Through Your Firewall ................................................................... 159
    Controlling outgoing HTTP requests ........................................................................ 160
    Protecting your web server ....................................................................................... 160
    HTTP rulesets .......................................................................................................... 161
    Restrict Web Access with WebBlocker ..................................................................... 162
Exercise 1: Configure HTTP Connections from Trusted Users ........................................ 164
    Add an HTTP client proxy policy .............................................................................. 164
    Enable a log message for each HTTP client connection ......................................... 164
    Block HTTP client connections by URL path ......................................................... 165
    Allow Microsoft Office documents and Zip files through the HTTP proxy .............. 166
    Customize the Deny message .................................................................................. 167
Exercise 2: Use HTTP Proxy Exceptions to allow Software Updates ................................ 168
Exercise 3: Configure an HTTP-Server Proxy Action ......................................................... 169
    Add the HTTP-Server proxy policy ......................................................................... 169
    Create a new proxy policy ruleset ............................................................................. 169
Exercise 4: Selectively Block Web Sites with WebBlocker .............................................. 171
    Add a WebBlocker action ......................................................................................... 171
    Select Categories to Block ....................................................................................... 171
    Create an exception ................................................................................................. 172
Frequently Asked Questions .......................................................................................... 174
Related Courseware and Information ........................................................................... 174
Test Your Knowledge ...................................................................................................... 174

Threat Protection ............................................................................................................. 177
What You Will Learn ........................................................................................................ 177
Default Threat Protection Measures Block Intruders ..................................................... 177
    Using Default Packet Handling Options .................................................................. 178
    Automatically Block the Source of Suspicious Traffic ............................................. 179
What You Will Learn ........................................................................................................ 197

Exercise 1: Configure Default Packet Handling Options ................................................. 180
Exercise 2: Block Potential Sources of Attacks ................................................................. 181
  Block a site permanently .................................................................................................... 181
  Create exceptions to the Blocked Sites list ........................................................................ 181
Exercise 3: Block sites automatically .................................................................................. 183

Related Courseware and Information ................................................................................ 184

Test Your Knowledge ..................................................................................................... 185

Signature Services ........................................................................................................ 187

What You Will Learn ........................................................................................................ 187

Identify and Stop Viruses at the Edge of Your Network ..................................................... 187
  AntiVirus Scans User Traffic for Viruses and Trojans ........................................................ 188
  Intrusion Prevention Service Blocks Direct Attacks .......................................................... 189
Exercise 1: Automate Gateway AntiVirus/IPS Status and Updates ......................................... 190
Exercise 2: Setup Gateway AntiVirus ................................................................................... 190
Activate Gateway AntiVirus ................................................................................................. 190
Configure Gateway AntiVirus ............................................................................................... 191
Exercise 3: Configure a SMTP proxy policy for Gateway AntiVirus ......................................... 192
Exercise 4: Configure the Intrusion Prevention Service ....................................................... 193
  Intrusion Prevention .......................................................................................................... 193

Related Courseware and Information ................................................................................ 193

Test Your Knowledge ..................................................................................................... 195

Mobile VPN .................................................................................................................. 197

What You Will Learn ........................................................................................................ 197

Connect Remote Users Securely to the Corporate Network ................................................ 197
  Types of Mobile VPN .......................................................................................................... 198
  Enabling the Firebox for Mobile VPN ................................................................................ 198
Exercise 1: Set Up Mobile User VPN with PPTP ................................................................. 199
Activate PPTP on the Firebox .............................................................................................. 199
Restrict PPTP users by policy ............................................................................................... 200
Exercise 2: Configuring the Firebox for SSL VPN ............................................................... 200
Activate the Firebox for SSL VPN ....................................................................................... 201
Restrict SSL VPN users by policy ....................................................................................... 201
Exercise 3: Prepare Mobile VPN End-User Profiles ........................................................... 202
  Setting Advanced Preferences ........................................................................................... 203
Exercise 4: Using the Mobile VPN with IPsec Client ........................................................... 204
  Installing the Mobile VPN with IPsec Client .................................................................... 204
  Connecting and Disconnecting the Mobile VPN with IPsec VPN ..................................... 205

Related Courseware and Information ................................................................................ 205

Test Your Knowledge ..................................................................................................... 206

Manual BOVPN .............................................................................................................. 209

What You Will Learn ........................................................................................................ 209

About Manual BOVPNs ..................................................................................................... 209
  When to use Policy Manager to create BOVPNs ................................................................. 210
  Steps to make a BOVPN tunnel with Policy Manager ....................................................... 210
Exercise 1: Configure a VPN Gateway ................................................................................ 210
Exercise 2: Define a VPN Tunnel ......................................................................................... 214
Exercise 3: Make a Tunnel Policy ....................................................................................... 216
  Allow only TCP port 80 through the BOVPN .................................................................... 216
Centralized Management ................................................................. 241
What You Will Learn ................................................................. 241
Manage Edge Devices with WSM .................................................. 241
  Edge configuration templates .................................................. 242
  Firmware updates ................................................................. 242
  Aliases for template destinations ........................................... 242
Exercise 1: Use Aliases with Managed Edge Devices ................. 242
  Define an alias on the Edge ................................................. 244
Exercise 2: Set Up Centralized Management .............................. 245
Exercise 3: Use an Edge Configuration Template ......................... 249
  Add a policy to a configuration template ............................... 249
Exercise 4: Schedule Firmware Updates ..................................... 254
  Install firmware .................................................................. 254
  Schedule an update ........................................................... 254
  See firmware updates ........................................................ 256
Exercise 5: Define a VPN Tunnel .................................................. 256
Exercise 6: Start Firebox X Edge Tools ....................................... 257
Related Courseware and Information ......................................... 258
Test Your Knowledge ............................................................... 258
  Answers ........................................................................... 260
Glossary .................................................................................... 261
Course Introduction

Learning Firewall Basics with Firebox Peak and Core

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak / Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware®/Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Course Introduction</td>
</tr>
</tbody>
</table>

Training Options

If you use WatchGuard® System Manager with Fireware® for your Firebox® X Core or Peak e-Series appliance, there are several training options available to you:

Classroom training with a WatchGuard Certified Training Partner (WCTP)
WatchGuard maintains a worldwide network of certified training partners available to host training on your Firebox. A list of training partners can be found on our web site at:
http://www.watchguard.com/training/partners_locate.asp

Quick review presentation
You can download and review the Firewall Basics presentation. This PowerPoint file gives an overview of the WatchGuard System Manager and Fireware Policy Manager. Students learn how to install a Firebox using the Quick Setup Wizard, create basic security policies, and get more information about additional security services.

Firewall Basics with Fireware Training Modules
Each training module available for WatchGuard System Manager and Fireware focuses on a specific feature or function of configuration and security management. These downloadable documents in PDF format include exercises to give you practice in configuring key product components.

Necessary Equipment and Software

For the majority of Firewall Basics training modules, you only need a default WatchGuard® Firebox® configuration file that you view and modify locally. You do not need to connect to a Firebox to complete the exercises. The few modules that require additional hardware include instructions on what is needed and how to set it up.

To complete the majority of the Firewall Basics with Fireware training modules, you must have the hardware and software listed here:

Management station computer
Your management station is a personal computer running Microsoft® Windows XP or Microsoft Vista. For more information about management station system requirements for WSM and Fireware® v10, see the WSM User Guide.

WSM and Fireware version 10 software
If you have a valid LiveSecurity® Service login, you can download the software from the WatchGuard web site. The software is also available from your instructor during classes delivered by WatchGuard Certified Training Partners.
Firewall configuration file
During the exercise portions of the training, you open, modify, and save Firebox configuration files. You can use the Policy Manager to create a new configuration file. You can also open the configuration file of your production Firebox and save it to your local hard drive. We recommend that you do not save any configuration files you make during the training exercises to a Firebox that is in production on your network.

Firebox X Core or Peak e-Series device (optional)
For some exercises, particularly the exercises which introduce logging, monitoring, and reports, it is useful to connect to a live Firebox on a production network. You do not need to change the configuration properties. While you can learn the material without the Firebox, it is much easier to grasp the concepts when you see records and information from a live network.

Prerequisites
This course is intended for moderately experienced network administrators. A basic understanding of TCP/IP networking is required. No previous experience with network security, WatchGuard® System Manager, or a Firebox® hardware appliance is required.

Certification
The WatchGuard® Certified System Professional (WCSP) exam is available for all WatchGuard partners. The exam is based on the contents of this course. Studying the information in this courseware can help you prepare to take the exam. If you are a WCSP, you can log in to your LiveSecurity® Service account and browse to the exam at:

https://www.watchguard.com/training/CertCentral.asp

Training Scenario
Throughout the Firewall Basics with Fireware training modules, we use a fictional company called Successful Company. While the modules build on a story of configuring a firewall and network for Successful Company, you can complete many of the exercises using examples from your own network or a set of addresses and situations provided by your WatchGuard® Certified Training instructor. Any resemblance between the situations described for Successful Company and a real company are purely coincidental.
Getting Started

Setting Up Your Management Station and Firebox

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak /Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Getting Started</td>
</tr>
</tbody>
</table>

What You Will Learn

WatchGuard® System Manager is the primary management software to monitor and manage WatchGuard Firebox® devices. In this training module, you learn how to:

- Use the Quick Setup Wizard to make a basic Firebox® configuration file
- Start WatchGuard System Manager
- Connect to devices and servers
- Start Policy Manager and open a Firebox configuration file

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

In this module, you will connect to one or more Firebox devices and a Management Server. If you take this course with a WatchGuard Certified Training Partner, your instructor will provide the IP address and passphrases for devices used in the exercises. For self-instruction, you can safely connect to a Firebox or Management Server on a production network. You will not change the configuration files of any device.

Start with the WatchGuard System Manager

Any operations you conduct with the Firebox® start from WatchGuard® System Manager (WSM). WSM is the primary management software for all the Firebox devices and WatchGuard servers in your network. From WatchGuard System Manager, you use monitoring and configuration tools such as Policy Manager, HostWatch™, LogViewer, and Firebox System Manager.

You can use WSM to connect to any WatchGuard firewall appliance including the legacy hardware such as the Firebox SOHO6 as well as all current Core and Peak hardware.
WSM Components

The basic components of WatchGuard System Manager are the WatchGuard System Manager window, and the five WSM server components. WatchGuard System Manager also provides access to other WatchGuard tools, including Policy Manager and Firebox System Manager. The diagram to the left shows the components of WatchGuard System Manager and how you can access and navigate among them.

You install the WSM management software on a personal computer running Microsoft® Windows 2000 or later. We call this computer your management station. When you install WSM on your management station, you have the option to install any or all of these server components:

- **Management Server** – Use to manage all firewall devices and create virtual private network (VPN) tunnels using a simple drag-and-drop function.
- **Log Server** – Collects log messages from each WatchGuard Firebox.
- **Report Server** – Periodically consolidates data collected by your Log Servers from your Firebox devices, and then generates reports.
- **WebBlocker Server** – Operates with the Firebox HTTP proxy to deny user access to specified categories of web sites.
- **Quarantine Server** – Collects and isolates SMTP mail confirmed as spam by spamBlocker or confirmed to have a virus by Gateway Antivirus or by spamBlocker’s Virus Outbreak Detection feature.

While you can install these servers on your management station, you can also put them on dedicated personal computers on your network. Each type of server has unique requirements to connect to other servers, the Firebox, or the management station. For more information, see the training modules which install and configure each type of server.

Register the Firebox with LiveSecurity

The LiveSecurity® Service provides Firebox users with alerts, threat responses, and expert advice to help you keep your Firebox security up-to-date. When you subscribe to LiveSecurity, you also get access to the latest software upgrades for your Firebox, and access to technical support and training resources.

Your Firebox must be registered with LiveSecurity before you can configure the device. To register the Firebox, you must have:

- A LiveSecurity account
- The Firebox serial number

To create a new LiveSecurity account, browse to:

https://www.watchguard.com/account/registration_gate.asp
To register your Firebox with an existing LiveSecurity account, log in to LiveSecurity and in the LiveSecurity Service Subscribers section, click Activate a Product.

**Exercise 1: Create a Configuration File with the Quick Setup Wizard**

The quickest and easiest method to create a functional configuration file for your network is to use the Quick Setup Wizard. However, you must be connected to a Firebox® to use this method. Before you start the Quick Setup Wizard, you must have:

- **Firebox feature key** — You receive the Firebox feature key when you register your Firebox with the LiveSecurity® Service. A feature key is created that is unique to the serial number of the device. Save a copy of the feature key to complete the Quick Setup Wizard.

- **WSM and Fireware installed on the management station** — WSM is the software installed on the management station and WatchGuard servers. Fireware® is the software installed with a configuration file on the Firebox itself. Download the latest versions from the LiveSecurity software downloads site. WSM and Fireware are separate software downloads. You must download and install both packages on your management station. The management station must be on the same subnet as the Firebox.

- **Network information** — You must know the IP address of your gateway router, and IP addresses to give to the external and trusted interfaces of the Firebox.

When you configure the Firebox with the Quick Setup Wizard, the wizard adds four basic policies: TCP/UDP outgoing, FTP packet filter, ping, and WatchGuard. It also sets interface IP addresses. In this exercise, we use the Quick Setup Wizard to create and install a basic configuration file on our Firebox.

1. From the Windows desktop, select **Start > All Programs > WatchGuard System Manager 10 > Quick Setup Wizard**.
   The Quick Setup Wizard launches and attempts to detect a Firebox on the same network as your computer.

2. Select the Firebox you are using for this training session from the list provided.
3. Follow the step-by-step instructions in the wizard to create a basic configuration file.
   When you are done with the wizard, you have a Firebox which allows all traffic from the trusted and optional networks to the external network but blocks everything from the external to the protected networks.

**Exercise 2: Open WSM and Connect to Fireboxes and Servers**

When you open WatchGuard® System Manager, no Firebox® appears automatically. You must connect to a Firebox or to a Management Server. You can connect to many devices and Management Servers at the same time.

**Connect to a Firebox**

1. From the Windows desktop, click **Start > All Programs > WatchGuard System Manager 10 > WatchGuard System Manager**.
2. Click the **Connect to Device** icon on the main toolbar.
   You can also select File > Connect To Device.
3. Type the trusted IP address of the Firebox you want to connect to. Use your Firebox IP address, or get the IP address from your instructor.

4. Type the Firebox status (read-only) **Passphrase**. Use the status passphrase to connect to a Firebox and display status. If you change a configuration property or make a tunnel from the device to another Firebox using Management Server, you are prompted to type the configuration passphrase.

5. If necessary, change the value in the **Timeout** field. This value sets the time (in seconds) that the management station listens for data from the Firebox, before it sends a message that shows that it cannot get data from the device. If you have a slow network or Internet connection to the device, you can increase the timeout value. If you decrease the value, you decrease the time you must wait for a time out message if you try to connect to a Firebox that is not available.

6. Click **Login**. WSM connects to the Firebox and then shows its status on the Device Status tab.

7. On the **Device Status** tab, click the plus sign (+) to expand the Firebox entry. Information about the Firebox appears.
Connect to a Management Server

A WatchGuard Management Server allows you to manage many Firebox devices at the same time from a single management station. With a Management Server you can quickly build virtual private network (VPN) tunnels between devices, and you centrally manage a large number of Firebox X Edge devices.

When you add the Management Server to the WSM display, it shows the status of all the Firebox devices under management on that Management Server. The VPN tunnels between the managed devices appear on the page for each device.

In this optional exercise, you add a Management Server to the WSM display. This exercise is only possible if your instructor has pre-configured a Management Server and clients for the classroom or if you have a Management Server configured for use on your network.

1. From WatchGuard System Manager, click the Connect to Server icon.
   You can also select File > Connect To Server. The Connect to Management Server dialog box appears.

2. Type the IP address of the Management Server.
   You can connect to a Management Server on your network or to a Management Server on the training network. Your instructor will provide you with the IP address, user name, and passphrase.

3. Type the user name and passphrase for the Management Server.

   admin is the default account for connecting to a Management Server. Your instructor may give you a different account to use.
4. Click Login. The Device Management tab appears with the Management Server and the devices it manages shown below.

Exercise 3: Open Policy Manager

Policy Manager is the tool you use to build the security rules your Firebox® uses to protect your network. For example, you use Policy Manager to configure your policies, set up virtual private networks, change Firebox passphrases, and configure logging and notification.

A policy is a set of rules that defines how the Firebox manages packets that come to its interfaces. The policy identifies the source and destination of the packets. It also can specify the protocol and ports that match the traffic. It includes instructions to the Firebox on how to identify the packet and what to do with the packet: allow, deny, drop, or block. Policy Manager displays each policy as a separate rule set. You can view these policies either as icons or in a list with a display of detailed information about each policy.

1. From WatchGuard® System Manager, select your Firebox on the Device Status tab. If there is no Firebox visible in WSM, select File > Connect To Device, and then connect to your Firebox.

2. With the Firebox selected, click the Policy Manager icon on the WSM toolbar. You can also select Tools > Policy Manager. WSM checks the model and the appliance software version of the device. If you have multiple versions of WSM software installed, WSM automatically opens the correct Policy Manager version.
3. Select **View > Details**.

![Firewall Policy Manager screenshot](image)

Related Courseware and Information

You can use these resources for more information on how to work with configuration files.

**WatchGuard® System Manager User Guide**

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/)
## Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. **True or False:** You must have a WatchGuard® Management server to use the Firebox® X Edge centralized management feature.

2. **Circle the best tool for each task:**

<table>
<thead>
<tr>
<th>Task</th>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>A) Monitor the status of one Firebox</td>
<td>WatchGuard System Manager Policy Manager</td>
</tr>
<tr>
<td>B) Change the Firebox network interfaces</td>
<td>WatchGuard System Manager Policy Manager</td>
</tr>
<tr>
<td>C) Configure a policy for web traffic</td>
<td>WatchGuard System Manager Policy Manager</td>
</tr>
</tbody>
</table>

3. **True or False:** It may be necessary to decrease the **Timeout** setting on the **Connect to Firebox** dialog box if you have a slow network or Internet connection to the device.

4. Which of the following are required before you can use the Quick Setup Wizard to make a basic Firebox configuration file:

- A) A LiveSecurity Service account
- B) The Firebox model number
- C) The IP address of your gateway router
- D) A Firebox feature key
- E) A live connection to the Internet
- F) A personal computer running Macintosh OS 10 or later
- G) A web browser
- H) An IP address to give to the external and trusted interfaces of the Firebox

5. **Fill in the blank:** A ____________ is a set of rules that defines how the Firebox manages packets that come to its interfaces.

6. **Which of the following is a WatchGuard System Manager component (select all that apply):**

- A) LogViewer
- B) Router
- C) Policy Manager
- D) Appliance Monitor
- E) Windows NT Server
- F) Report Server
- G) Management Station

---

**ANSWERS**

1. True - While you can remotely manage a Firebox X Edge by connecting to its administrative interface, you can not centrally manage the device.

2. A) WatchGuard System Manager B) Policy Manager C) Policy Manager

3. False - You should increase the Timeout setting if you have a slow network or Internet connection to the device.

4. A, C, D, and H

5. policy

6. A, C, G, and H
Administration

Working with Firebox Configuration Files

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox X Core / Firebox X Core e-Series / Firebox X Peak / Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Administration</td>
</tr>
</tbody>
</table>

What You Will Learn

After you install the WatchGuard® Firebox in your network and you use the Quick Setup Wizard to give it a basic configuration file, you can add custom configuration settings to meet the needs of your organization. You save configuration files in a variety of locations. In this training module, you learn how to:

- Open and save configuration files
- Configure the Firebox for remote administration
- Reset Firebox passphrases
- Back up and restore the Firebox configuration
- Add Firebox identification information

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

In this module, you will connect to one or more Firebox devices. If you take this course with a WatchGuard Certified Training Partner, your instructor will provide the IP address and passphrases for devices used in the exercises. For self-instruction, you can safely connect to a Firebox on a production network. You will not change the configuration files of any device.

Manage Configuration Files and Firebox Properties

A configuration file includes all configuration data, options, IP addresses, and other information that you add with Policy Manager. On the Firebox®, the configuration file works with the appliance software to control the flow of traffic through the device. A Firebox configuration file has an XML file extension.

Fireware Policy Manager is a WatchGuard® software tool that lets you make, change, and save configuration files. When you use Policy Manager, you see a version of your configuration file that is easy to examine and change. Changes you make in Policy Manager have no effect on Firebox operation until you save them to the Firebox.
Exercise 1: Open and Save Configuration Files

The Quick Setup Wizard makes a basic configuration file for your Firebox®. We recommend that you use this configuration file as the base for all your configuration files. You can also use Policy Manager to make a new configuration file with only the default configuration properties. To do this, select File > New from Policy Manager.

Most of the time, when you want to work on your Firebox configuration you connect to the Firebox from WatchGuard® System Manager and launch Policy Manager from the WSM toolbar. When you do this, WSM connects to the Firebox and loads the configuration file currently running on the Firebox into Policy Manager. You can save a copy locally and open the local copy in Policy Manager any time you want to work offline.

In this exercise, you open the configuration file currently running on your Firebox and save it to your local hard drive:

1. From the Windows desktop, open WatchGuard System Manager and connect it to your Firebox. If you are not familiar with this procedure, see the “Getting Started” training module or ask your instructor.

2. Select your Firebox. Click the Policy Manager icon. Policy Manager starts and displays the configuration file currently running on your Firebox.

3. From Policy Manager, select File > Save > As File. The Save dialog box opens.

4. In the File Name text box, type Basics-Start. Click Save. By default, configuration files are saved to the My Documents\My WatchGuard\configs folder. Notice that the configuration file type is XML.
Exercise 2: Configure a Firebox for Remote Administration

When you configure a WatchGuard® Firebox® with the Quick Setup Wizard, a policy is created automatically that allows you to connect to and administer the Firebox from any computer on the trusted or optional networks. If you want to manage the Firebox from a remote location (any location external to the Firebox), then you must change your configuration to allow administrative connections from your remote location.

The packet filter policy that controls administrative connections to the Firebox itself is called WG-Firebox-Mgmt. The Quick Setup Wizard adds the policy with the name “WatchGuard”. This policy controls access to the Firebox on these four TCP ports: 4103, 4105, 4117, 4118. When you allow connections in the WatchGuard policy, you are allowing connections to each of these four ports.

Before you change a policy to allow connections to the Firebox from a computer external to your network, it is a good idea to consider:

- Is it possible to connect to the Firebox using VPN? This greatly increases the security of the connection. If it is not possible to connect to the Firebox using VPN, you may want to consider using authentication as an additional layer of security.
- It is more secure to limit access from the external network to the smallest number of computers possible. For example, it is more secure to allow connections from a single computer than it is to allow connections from the alias “Any-External”.

To configure the WatchGuard policy to allow administrative access from an external computer:

1. From Policy Manager, double-click the WatchGuard policy. While the name of this policy is WatchGuard, the packet filter type is WG-Firebox-Mgmt. This policy is specifically designed to be used for administration of the Firebox. You can also right-click the WatchGuard policy and select Edit. The Edit Policy Properties dialog box appears.

2. From the From list, click Add.

3. To enter the IP address of the external computer you will be connecting to the Firebox from, click Add Other. Make sure Host IP is the selected type, and type the IP address of the remote administration computer. If you use authentication and want to enter a user name instead of an IP address, click Add User instead of Add Other. Select the type of user and the method of authentication you will be use. From the User/Group drop-down list, select User and type your use name.

4. Click OK. Close all policy property dialog boxes.

Exercise 3: Change the Firebox Passphrases

In this exercise, you change the passphrases for your Firebox®. A Firebox uses two passphrases:

- Status passphrase—The read-only password that allows you to see information about the Firebox but does not allow you to make any changes to the configuration.
- Configuration passphrase—The read-write password that allows an administrator to save a new configuration to the Firebox.

We recommend that you change the Firebox passphrases at regular intervals as part of your company’s security policy. The passphrases used in this exercise are examples. When you develop a passphrase, it is important to use a strong password. A strong password is one that contains at least eight characters, and includes a combination of letters, numbers, and symbols.

You must have the current configuration passphrase of a Firebox to do this exercise. Do not complete this exercise if you do not have permission to change the configuration passphrase of a Firebox in a production network.
1. From Policy Manager, select File > Open > Firebox. The Open Firebox dialog box appears.

2. Type the IP address of your Firebox. Type the status passphrase of your Firebox. Policy Manager contacts the Firebox and gets the configuration file. A dialog box opens asking you to save the file to a local disk drive.

3. Click Save.


5. Type the current configuration passphrase of your Firebox.

6. In the Status Passphrase field, type 33333333. Type it again. In the Configuration Passphrase field, type 44444444. Type it again.

7. Click OK. The new passphrases are saved to the Firebox.

Exercise 4: Create and Restore a Firebox Backup Image

A Firebox® backup image is a saved copy of the working image from the Firebox flash disk. The backup image includes the Firebox appliance software, configuration file, licenses, and certificates. You can save an encrypted backup image to your management station or to a directory on your network.

We recommend that you regularly back up your Firebox image. We also recommend that you create a backup image of the Firebox before you make significant changes to your Firebox configuration or upgrade your Firebox or its appliance software.

Create a Firebox backup image

1. From Policy Manager, select File > Backup. The Backup dialog box appears.

2. In the Backup dialog box, type the configuration passphrase for your Firebox. If you have been following the exercises in this training module, the configuration passphrase is 44444444. The second part of the Backup dialog box appears.

3. Type and confirm an encryption key. For this exercise, type MyStrongKey. This key is used to encrypt the backup file. If you lose or forget this encryption key, you cannot restore the backup file. The encryption key is case-sensitive.

4. Select the directory in which to save the backup file. Click OK. The default location for a backup file with a “.fxi” extension is C:\Documents and Settings\All Users\Shared WatchGuard\backups\<Firebox IP address>-<date>.<wsm_version>.fxi.
**Restore a Firebox backup image**

1. From Policy Manager, select **File > Restore**.
   The Restore dialog box appears.

2. Type the configuration passphrase for your Firebox.
   If you have been following the exercises in this training module, the configuration passphrase is 44444444.

3. Type the encryption key you used when you created the backup image. For this exercise, the value is **MyStrongKey**.
   The Firebox restores the backup image and restarts. It uses the backup image on restart.

**Exercise 5: Add Firebox Identification Information**

You can save information about the Firebox in the configuration file, which helps you to identify it in reports, log files, and multibox management tools. The Firebox model is particularly important because some software features only function on certain models.

You can give the Firebox a name to use in your log files and reports. If you do not give your Firebox a name, the log files and reports use the IP address of the Firebox external interface. You can use a Fully Qualified Domain Name if you register it with your authoritative DNS server. You must give the Firebox a name if you use the Management Server to configure VPN tunnels and certificates for the Firebox.

The Firebox time zone controls the date and time that appear in the log file and on tools that include LogViewer, WatchGuard Reports, and WebBlocker. Set the Firebox time zone to match the time zone for the physical location of the Firebox. This time zone setting allows for the time to appear correctly in the log messages. A default configuration file sets the Firebox system time to Greenwich Mean Time (GMT).

In this exercise, you set the device information for your student Firebox. If you are working alone, you can use the example of our fictional organization—the Successful Company. In later training modules, you see this information in reports and WatchGuard® System Manager.

1. From Policy Manager, click **Setup > System**.
   The Device Configuration dialog box appears.

2. In the **Name** field, type **SuccessfulMain**.
   Your instructor may give you another name for your student Firebox.

3. In the **Location** field, type **Seattle**.
   This field is to identify the physical location of the Firebox.

4. In the **Contact** field, type your name.
   This field is for the name of the person in your organization responsible for the management of the device.
5. Use the **Timezone** drop-down list to select your local time zone. This should be the time zone of the Firebox itself. This enables you to synchronize reports from devices in multiple time zones.

![Device Configuration](image)

6. Click **OK**.

**Related Courseware and Information**

You can use these resources for more information on how to work with configuration files.

**WatchGuard® System Manager User Guide**
Browse to [https://www.watchguard.com/help/documentation/](https://www.watchguard.com/help/documentation/) and download the User Guide. See the chapter “Basic Configuration Setup.”

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/)
Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. Circle the correct answer: To save a changed policy to the Firebox®, enter the \[ status | configuration \] passphrase.
2. Circle the correct answer: Corporate headquarters is in Detroit. The branch office Firebox is located in Tokyo. You should set the branch office Firebox time zone to:
   
   A. (GM-06:00) Central Time (US & Canada)   B. (GMT+09:00) Osaka, Sapporo, Tokyo
3. True or False: You can save the Firebox configuration file to a floppy disk drive.
4. How frequently should you make a backup image of your Firebox?
   - A) Daily
   - B) Weekly
   - C) Monthly
   - D) Each time you make a substantial change to the configuration
   - E) Never

5. Which of the following is information used by WatchGuard® System Manager applications to identify a Firebox (select all that apply)?
   - A) Firebox Name
   - B) System administrator name
   - C) Encryption key
   - D) Model number
   - E) External IP address

Administration
3. True - You can save the Firebox configuration file to any local disk drive including a floppy disk or a network share.

2. (GMT+09:00) Osaka, Sapporo, Tokyo - Set the Firebox time zone to its physical location.

1. A, D

5. A, D

4. D
Network Settings

Configuring Firebox Interfaces

The WatchGuard® Firebox® has three types of interface: external, trusted, and optional. To use your Firebox in a network, you must set the IP addresses of the interfaces. You can also enable routing features on some interfaces. In this training module, you are shown how to:

- Configure external network interfaces using a static IP address, DHCP and PPPoE
- Configure a trusted and optional network interface
- Use the Firebox as a DHCP server
- Add WINS/DNS server locations to the Firebox configuration
- Add Dynamic DNS settings to the Firebox configuration
- Set up a secondary network or address

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

Properties and Features of Firebox Interfaces

A firewall physically separates the networks on your local area network (LAN) from those on a wide area network (WAN) like the Internet. One of the basic functions of a firewall is to move packets from one side of the firewall to the other. The common name for this is routing. To route packets correctly, the firewall must know what networks are accessible through each of its interfaces.

The Firebox® provides additional functionality for some interfaces. External interfaces can be configured to work with Dynamic DNS. Trusted and optional interfaces can be set up with the Firebox as a DHCP (Dynamic Host Configuration Protocol) server.

The Firebox® has three types of network interface:

**External Interfaces**

A Firebox external interface connects to a wide area network (WAN) such as the Internet and can have either a static or dynamic IP address. The Firebox gets a dynamic IP address for the external interface from either a DHCP (Dynamic Host Configuration Protocol) or PPPoE (Point-to-Point Protocol over Ethernet) server. With DHCP, the Firebox uses a DHCP server that is controlled by your Internet Service Provider (ISP) to get an IP address, gateway, and netmask. With PPPoE, the Firebox makes a PPPoE protocol connection to the PPPoE server of your ISP. Fireware® supports unnumbered and static PPPoE.
**Trusted Interfaces**
A Firebox trusted interface connects to the private local area network (LAN) or internal network that you want to secure. Because a trusted interface is a LAN interface, the IP address for a trusted interface is static. Usually, these IP addresses conform to [RFC 1918 — Address Allocation for Private Internets](https://tools.ietf.org/rfc/rfc1918.txt).

**Optional Interfaces**
Optional interfaces are “mixed trust” or “DMZ” environments separate from your trusted network. Examples of computers often found on an optional interface are public web, FTP, and mail servers. Optional interfaces use static IP addresses.

Most users configure at least one external and one trusted interface on their Firebox. You can configure any interface as trusted, optional, or external. You can have a maximum of four external interfaces.

When configuring the interfaces on a Firebox, you must use slash notation to denote the subnet mask. For example, 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.

**Requirements for Firebox Interfaces**
You install the Firebox with different networks and network addresses on its interfaces. The public servers behind the Firebox use either private or public IP addresses. The Firebox can use network address translation (NAT) to route traffic from the external network to the public servers.

All devices behind the trusted and optional interfaces must have an IP address from a network assigned to that interface. To make this easy to remember, many administrators set the interface address to the first or last IP address in the range. In the graphic below, the trusted interface could be 10.0.1.1/24 and the optional interface could be 10.0.2.254/24.

**About DHCP Server and DHCP Relay**
On optional and trusted interfaces you can configure the Firebox as a DHCP server for networks behind the firewall. You can also configure the Firebox for DHCP relay. When you use DHCP relay, computers behind the Firebox can use a DHCP server on a different network to get IP addresses. The Firebox sends the DHCP request to a DHCP server at a different location than the DHCP client. When the Firebox gets a reply, it sends it to the computers on the Firebox trusted or optional network. This option lets computers in more than one office use the same network address range.

**About WINS/DNS**
A number of the features of the Firebox have shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server IP addresses. Therefore, access to these servers must be available from the trusted interface of the Firebox. For example, this information is used by remote user virtual private networks. Make
sure that you use only an internal WINS and DNS server to make sure you do not create policies that have configuration properties that prevent users and services from connecting to the DNS server.

About Drop-In and Routed modes
The Firebox can be configured in Routed or Drop-In mode, depending on the requirements of the network the Firebox is being placed into.

<table>
<thead>
<tr>
<th>Routed Configuration</th>
<th>Drop-in Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>All interfaces of the Firebox are on different networks.</td>
<td>All interfaces of the Firebox are on the same network and have the same IP address.</td>
</tr>
<tr>
<td>Trusted and optional interfaces must be on different networks. Each interface has an IP address on its network.</td>
<td>The computers on the trusted or optional interfaces can have a public IP address.</td>
</tr>
<tr>
<td>Use static NAT (network address translation) or 1-to-1 NAT to map public addresses to private addresses behind the trusted or optional interfaces.</td>
<td>The computers can have public IP addresses. No NAT is necessary.</td>
</tr>
</tbody>
</table>

The most common configuration method is a routed configuration and it is the method used in most of the examples in this document.

About dynamic DNS
A dynamic domain name service (dynamic DNS) makes sure that the IP address attached to your domain name changes when your ISP gives your Firebox a new IP address. The Firebox supports the use of one dynamic DNS provider — DynDNS. For more information, browse to the DynDNS web site:

http://www.dyndns.com

About secondary networks
A secondary network is a network that shares one of the same physical networks as one of the Firebox 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 Firebox that there is one more network on the Firebox interface.

If your Firebox is configured with a static IP address, you can 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 web servers and you want to configure a static NAT rule for each.

Exercise 1: Use a Dynamic IP Address for an External Interface

The Firebox® can get a dynamic IP address for an external interface with DHCP or Point-to-Point Protocol over Ethernet (PPPoE). At the Successful Company, the network administrators start with a DHCP-assigned address for their Firebox external interface. However, as their company grows, they change to a static IP address and add a backup PPPoE connection.

Configure the External Interface for DHCP

In this exercise, we configure an external interface of the Successful Company’s Firebox from to get its IP address from a DHCP server.

1. From Policy Manager, open the configuration file you are editing for these exercises.
3. Click the External (Interface 0) entry. Click Configure. The Interface Settings dialog box opens.
4. In the Interface Name text box, type InternetConnection. In the Interface Description text box, type Connect to the Cloud.
5. Make sure that the Interface Type is set to External.
6. Select Use DHCP Client.
7. Select **Obtain an IP automatically**.
   For most DHCP connections, this is a sufficient configuration.

![Image of Network Configuration dialog box with DHCP selected]

8. Click **OK**.
   DHCP appears in the IP address field in the Network Configuration dialog box.

![Image of Network Configuration dialog box with PPPoE interface settings]

**Configure the External Interface for PPPoE**

Another way to get a dynamically assigned address for a Firebox external interface is to use a PPPoE server. When you do this, your ISP gives you the user name and password. In this exercise, we configure a Successful Company IP interface to use PPPoE.

1. From the Network Configuration dialog box, click the **Optional-2** (Interface 3) entry. Click **Configure**.
   The Interface Settings dialog box opens.

2. In the **Interface Name** text box, type **BackupInternet**. In the **Interface Description** text box, type **Use when primary account fails**.

3. Use the **Interface Type** drop-down list to set the interface to **External**.

4. Select **Use PPPoE**.

5. Select **Obtain an IP address automatically**.

6. Type the PPPoE user name. For this exercise, use **username**.
7. Type the PPPoE passphrase, then type it again to confirm. For this exercise use passphrase for the passphrase.

8. Click OK. PPPoE appears in the IP address field in the Network Configuration dialog box.

Configure the External Interface for use with Dynamic DNS
When you use a dynamically assigned IP address for an external interface, it is important to maintain the connection between your current IP address and your domain name. In this exercise, we configure the Successful Company Firebox to use the DynDNS service.

1. From the Network Configuration dialog box, click the Dynamic DNS tab.
2. Select the 0 (InternetConnection) enter and click Configure. The Per Interface Dynamic DNS dialog box appears.
3. Select the Enable Dynamic DNS check box.
4. Type the user name, password, and domain name for the Dynamic DNS account. For this exercise, use successfulco for User Name, password for Password and mywatchguard.com for Domain.
5. In the Service Type drop-down list, verify the default selection of dyndns (Dynamic DNS).
6. In the Options field, you can type dynamic DNS options. For this exercise, leave this field blank. For more information on options, see http://www.dyndns.com/developers/specs/syntax.html
7. Use the arrows to set a time interval, in days, to force an update of the IP address. For this exercise, leave this number at 28 days.

8. Click OK. The Network Configuration Dynamic DNS tab shows the Dynamic DNS status as Enabled.

**Exercise 2: Configure an External Interface with a Static IP Address**

To configure an external interface with a static IP address, you must know:

- Static IP address
- Subnet mask in slash notation
- Default gateway

In this exercise, you reconfigure the primary external IP address of the Successful Company network.

1. From the Network Configuration dialog box, click the **Interfaces** tab.
2. Click the **InternetConnect** (Interface 0) entry. Click **Configure**. The Interface Settings dialog box opens.
3. Select **Use Static IP**.
4. In the **IP Address** text box, type `50.50.50.10/24`. This is the fictional IP address. With a real world static IP address, the Internet Service Provider (ISP) provides the IP address, subnet and default gateway.

If you are in a classroom, get the address information from your instructor.
5. In the **Default Gateway** text box, type 50.50.50.1.

![Interface Settings - Interface #0 dialog box](image)

6. Click **OK**.
   The external IP address appears in the Network Configuration dialog box.

![Network Configuration dialog box](image)

**Exercise 3: Configure a Trusted Interface as a DHCP Server**

In this exercise, we configure a Successful Company Firebox® trusted interface as a dynamic host configuration protocol (DHCP) server.

1. From the Network Configuration dialog box, click the **Trusted** (Interface 1) entry. Click **Configure**. The Interface Settings dialog box opens.
2. In the **Interface Name** text box, type **OurLAN**.
3. Make sure that the **Interface Type** is set to **Trusted**.
4. Type an IP address for the interface. For this exercise, we use the default 10.0.1.1/24.
5. Select **Use DHCP Server**.
6. In the **Address Pool** area, click **Add**.
7. For the **Starting address**, type 10.0.1.100. For the **Ending address**, type 10.0.1.200. Click **OK**.
8. Use the Leasing Time drop-down list to set the duration to **24 hours**.

![Interface Settings Dialog Box](image)

9. Click **OK**.

**Exercise 4: Configure an Optional Interface**

Optional interfaces represent “DMZ” or “mixed trust networks. They are commonly used for servers which are used by both the public and members of your organization, such as web and FTP servers. In this exercise, we configure an optional network that Successful Company will use for their public servers.

1. From the Network Configuration dialog box, click the **Optional-1** (Interface 2) entry. Click **Configure**.
   
   The Interface Settings dialog box opens.

2. In the **Interface Name** text box, type **PublicServers**.

3. In the **Interface Description** text box, type **Servers used by customers and vendors.**
4. Make sure that the Interface Type is set to Optional. For this exercise, we use the default network IP address of 10.0.2.1/24. This network will not use DHCP so you do not need to change any other setting.

5. Click OK. The new settings appear for Interface 2.

Exercise 5: Configure WINS/DNS Server Information

Several Fireware features work correctly only if you use a WINS/DNS server on your trusted network. These features include Gateway AntiVirus/IPS, spamBlocker, and mobile virtual private networks. In this exercise, we configure the Successful Company Firebox® to use WINS/DNS servers on its OurLAN and WebServer networks.

1. From the Network Configuration dialog box, click the WINS/DNS tab.
2. In the Domain Name text box, type mywatchguard.com.
3. For DNS Servers enter the IP addresses of your internal DNS servers. For this exercise, type 10.0.1.53 and 10.0.2.53.
   You are not required to enter more than one DNS server. Having more than one helps make sure users can still get DNS name resolution when the primary server is not available.
Exercise 6: Configure a Secondary Network

4. For WINS Servers enter the IP addresses for your internal WINS servers. For this exercise, type 10.0.1.53 and 10.0.2.53.

5. Click OK.

Exercise 6: Configure a Secondary Network

A secondary network is a network that shares one of the same physical networks as one of the Firebox® interfaces. In this exercise, we add a secondary network to the Successful Company OurLAN trusted network.

1. From the Network Configuration dialog box, select the **OurLAN (interface 1)** entry and click **Configure**. The Interface Settings dialog box appears.
2. Select the **Secondary** tab.
3. Click **Add**.
4. Type 172.16.0.1/24 and click **OK**.

5. Click **OK** to close the Interface Settings dialog box. Click **OK** again to close the Network Configuration dialog box.
6. Save the configuration file.
Frequently Asked Questions

**Question: Can I use any IP address for my trusted and optional networks?**
Answer: You can, but we suggest you only use only IP addresses specified in RFC 1918 — Address Allocation for Private Internets. These include any of these network ranges.

- 10.0.0.0 - 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 -192.168.255.255 (192.168.0.0/16)

If you use any other IP address you can have a conflict. For example, let’s say your trusted network is configured with the IP address 206.253.208.100/24. Any user on the trusted network that tried to go to the WatchGuard web site would fail because 206.253.208.100 is the IP address of the WatchGuard web site. The Firebox would route 206.253.208.100 traffic to the trusted interface instead of the external interface to get to the WatchGuard web site server.

**Question: What is slash notation?**
Slash notation is another way to write a network mask. Below is a conversion table:

<table>
<thead>
<tr>
<th>Network mask</th>
<th>Slash</th>
</tr>
</thead>
<tbody>
<tr>
<td>255.0.0.0</td>
<td>/8</td>
</tr>
<tr>
<td>255.255.0.0</td>
<td>/16</td>
</tr>
<tr>
<td>255.255.255.0</td>
<td>/24</td>
</tr>
<tr>
<td>255.255.255.125</td>
<td>/25</td>
</tr>
<tr>
<td>255.255.255.192</td>
<td>/26</td>
</tr>
<tr>
<td>255.255.255.224</td>
<td>/27</td>
</tr>
<tr>
<td>255.255.255.240</td>
<td>/28</td>
</tr>
</tbody>
</table>

Related Courseware and Information
You can use these resources for more information on how to work with configuration files.

**WatchGuard® System Manager User Guide**
Browse to [https://www.watchguard.com/help/documentation/](https://www.watchguard.com/help/documentation/) and download the User Guide. See the chapter “Basic Network Setup.”

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/).

Test Your Knowledge
Use these questions to practice what you have learned and exercise new skills.

1. When you use a static IP address for the external interface, you must get this information from your ISP (select all that apply):
   - [ ] A) An IP address
   - [ ] B) A default gateway address
   - [ ] C) A subnet mask
   - [ ] D) A password or passphrase
   - [ ] E) A user name
2. The Firebox interface types are (select all that apply):
   - A) Optional
   - B) External
   - C) Alias
   - D) Trusted
   - E) All the above

3. True or False: If you use DHCP on the external interface of the Firebox, you can configure a secondary network for the external interface.

4. True or False: You can configure the Firebox as a DHCP server.

5. The WINS/DNS settings in the Network Configuration dialog box are used by (select all that apply):
   - A) Mobile VPN connections to the Firebox
   - B) Your ISP to route to the Firebox
   - C) Computers on your trusted and optional networks
   - D) Your WatchGuard Management Station
   - E) DHCP

6. True or False: You can only add Secondary Networks or addresses to Routed configurations, not Drop-In configurations

7. Which two interfaces do most users, at a minimum, configure as part of a Firebox configuration:
   - A) External and optional
   - B) Trusted and optional
   - C) External and trusted

8. Which of these items is NOT a method for assigning an IP address to the external interface of a Firebox:
   - A) Static IP assignment
   - B) DHCP
   - C) PPPoE
   - D) PPPoA

9. True or False: Only the trusted interface of a Firebox is able to assign IP addresses as a DHCP Server.
ANSWERS

1. A, B, C
2. A, B, D
3. False - If you configure your external interface using DHCP or PPPoE, you cannot add external secondary networks or use external aliases in Policy Manager.
4. True
5. A, C, E
6. False
7. C
8. D
9. False
Logging

Setting Up Logging and Notification

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak /Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Logging</td>
</tr>
</tbody>
</table>

What You Will Learn

The WatchGuard® Firebox® sends log messages to a Log Server which in turn provides data for the Report Server and triggers notifications and alerts. In this training module, you are shown how to:

- Set up a Log Server
- Configure the Firebox to send messages to a Log Server
- Configure logging and notification preferences
- Enable advanced diagnostics

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

In this module, you will connect to one or more Firebox devices. If you take this course with a WatchGuard Certified Training Partner, your instructor will provide the IP address and passphrases for devices used in the exercises.

Maintain a Record of Firebox Activity

At its most basic level, logging is the process of recording the activity that occurs at a Firebox®. Notification is the process of telling an administrator when a particular activity that represents a potential security threat has occurred.

For example, when the Firebox denies a packet, this event is recorded in the log file. When the Firebox determines that a set of events indicates a port space probe or some other threat that you have flagged for notification, your network security administrator is alerted. Notification can be an email message or a pop-up window, or can be sent by way of an SNMP trap. The network security administrator can examine the log files and make decisions about how to make the network more secure. He could decide to block the ports on which the probe was used, block the IP address that sent the packets, or inform the ISP through which the packets were sent.
Logging and notification architecture
To understand the architecture of logging and notification, you must know the components of the WatchGuard® logging system.

WSM and Policy Manager
You use WSM and Policy Manager on the management station to set rules for the types of events for which the Firebox sends log messages and notification requests to the Log Server. WSM and Policy Manager supply the tools to see the log messages the Firebox creates, and create reports of Firebox events. You can also use Policy Manager to add backup Log Servers.

Firebox
The WatchGuard Firebox creates log messages for each event that occurs on the Firebox and sends the messages to the configured Log Server according to the rules set in its security policy. If an event has a notification action associated with it, the Firebox sends a notification trigger to the Log Server so that a message is sent when that event occurs.

Log Server
The WatchGuard Log Server is the computer to which your Firebox sends all log messages which are stored in a SQL database. It can be the same computer as your management station or you can use a second computer. The Firebox must be able to route data to the Log Server.

Seeing log messages
You can use two different tools to see the log messages generated by the Firebox.

LogViewer
To see log file data from WSM, use the LogViewer tool. It can show the log data page by page, or you can search and display by key words or specified log fields.

Traffic Monitor
For a quick look at the log messages generated by the Firebox, use Traffic Monitor. With Traffic Monitor, you can apply color to different types of messages, and ping or traceroute to the IP addresses of computers included in the log messages.

Log Server
The Log Server collects log messages from a WatchGuard Firebox. The Log Server also sends notification messages when it gets a notification request from the Firebox. You can install Log Server software on the computer you are using as a management station or on a different computer using the WSM installation program and selecting to install only the Log Server component.
In addition to installing the software, you must configure the Log Server with a Log Server encryption key. This is the key that the Firebox uses to encrypt log messages sent to the Log Server. The same key must be used on the Firebox and on the Log Server. The encryption key must be no less than eight and no more than 32 characters. The first time you connect to a Log Server, the default log encryption key is the status passphrase you set when you used the Quick Setup Wizard on your management station. One Log Server can receive and store logs from many Fireboxes.

If you install the Log Server on a computer with a desktop firewall other than Windows Firewall, you must open TCP ports 4107 and TCP port 4115 on that firewall for the WatchGuard Log Server to connect through the firewall. There is no need for Windows Firewall users to change their configuration.

Log Servers operate in fail over mode, not redundancy mode. In other words, a Firebox can only write to one Log Server at a time. The backup server is used when the primary server becomes unavailable.

Log messages
WatchGuard System Manager includes strong and flexible log message tools. An important feature of a good network security policy is to log messages from your security systems, examine those records frequently, and keep them in an archive. You can use log files to monitor your network security and activity, identify any security risks, and address them.

WatchGuard Firebox appliances send log messages to the Log Server. They can also send log messages to a syslog server or keep a limited number of log records locally on the Firebox. You can choose to send logs to either or both of these locations.

The Firebox sends five types of log messages: Traffic, Alarm, Event, Debug and Status. Log messages created in Fireware include the name of the log type in each log message.

Traffic Log Messages
The Firebox sends traffic log messages as it applies packet filter and proxy rules to traffic that goes through the Firebox.

Alarm Log Messages
Alarm log messages are sent when an event occurs that causes the Firebox to send a notification request.

Event Log Messages
The Firebox sends an event log message because of user activity. Actions that cause the Firebox to send an event log message include:
- Firebox start up and shut down
- Firebox and VPN authentication
- Process start up and shut down
- Problems with the Firebox hardware components

Debug Log Messages
Debug log messages include information used to help troubleshoot problems. You can select the level of debug log messages to see in your Traffic Monitor or write to your log file.

Status Log Messages
Statistic log messages include information about the performance of the Firebox. By default, the Firebox sends log messages about external interface performance and VPN bandwidth statistics to your log file. You can use these logs to change your Firebox settings as necessary to improve performance.

Log files
The Firebox sends log messages to a primary or backup Log Server. Log messages are stored in a SQL database file. The default location for the log file is: Documents and Settings\WatchGuard\logs.
Exercise 1: Set Up the Log Server

In this exercise, we set up our training computer as a Log Server. In most organizations, the Log Server is a dedicated computer on the trusted or optional network running Microsoft® Windows.

You can also configure a Log Server on the external network if you have many Firebox devices and want to store log files in a central location. The logging channel is encrypted, so you do not need to use a VPN tunnel between the Firebox and the Log Server. Use network address translation to route from the external interface to the Log Server behind a firewall. Then configure a WG-Logging policy to open the following ports:

- TCP 4115 - Used by devices with Fireware appliance software
- TCP 4107 - Used by devices with WFS appliance software and by all SOHO, SOHO6, and older Edge devices

Setup the Log Server

The first step is to use the Log Server Setup Wizard to activate the Log Server.

1. From the Windows desktop, right-click the Log Server icon in the WatchGuard toolbar.

2. Select Start Service.
   The Log Server Setup Wizard appears.

3. Click Next. In the Encryption Key text box, type mylogserverkey. Type it again to confirm.
   The Encryption Key is used to encrypt log messages between the appliance and the Log Server. It must match what you use in the Policy Manager.

4. Click Next. In the Master Passphrase text box, type mymasterpassphrase. Type it again to confirm.
   The Master Passphrase is used to encrypt all WatchGuard passphrases stored on the hard drive of the Management Station.

5. Click Next. In the Server Management Passphrase text box, type myservermanagementphrase. Type it again to confirm.
   The Server Management Passphrase is the used by the administrator account when you to connect to server configuration utilities.

6. Click Next.
   The wizard installs a Postgres database to store the log records. When the install is complete, the wizard prompts for an organization name.

7. Type Successful Company, Inc. Click Next.
   You can also type the name of your own organization or a company name provided by your instructor. The wizard configures the server.

8. Click Finish.
**Exercise 2: Configure the Firebox to send log messages to the server**

Now, we tell each Firebox® in our network to send log messages to the Log Server. In a real network setup, after the configuration is saved to the Firebox, the log encryption key on the Firebox matches the log encryption key on the Log Server, and the Log Server and Firebox can communicate. The Firebox waits until it sends its first log message then it establishes a connection with the Log Server.

In this exercise, we configure the Firebox to send messages to the Log Server.

1. From Policy Manager, open the configuration file you are editing for these exercises. For self-study, you can download exercises files from the WatchGuard training site. Open Logging-Start.xml.
2. Select **Setup > Logging**.
3. Select the **Send log messages to the log servers at these IP addresses** check box. Click **Configure**. The Configure Log Servers dialog box appears.
4. Click **Add**. The Add Event Processor dialog box appears.
5. In the **Log Server Address** box, type your workstation IP address. In the **Encryption Key** text box, type mylogserverkey. Type it again to confirm.
   For the exercise files, we put the Log Server on the Successful Company trusted network at 10.0.1.17.
6. Click **OK** to close the **Add Event Processor** dialog box. Click **OK** again to close the **Configure Log Servers** dialog box.
7. Click **OK** to close the **Logging Setup** dialog box.
   Remember, the Firebox does not establish a connection with the Firebox until you save the configuration file and it tries to send the first log message.
8. If you have access to a Firebox for this lesson, save the configuration file to the Firebox.
Exercise 3: Control Log Database and Notification Properties

In this exercise, we configure the Log Server to comply with the Successful Company document archive policy. At Successful Company, the network administrator must retain all records for six months and backup critical network data such as log messages to a secure drive at least once a week.

Configure log database settings

We use Log Server expiration settings to control how long we maintain log messages as well as when and where we back them up to a location off the Log Server.

1. From your Windows toolbar, right-click the Log Server icon and select Configure. The Log Server Configuration utility appears.
2. In the Database Settings section, select the Send a warning if the database reaches the warning threshold check box. In the Send warning message to text box, type me@mywatchguard.com.
3. Select the Expiration Settings tab.
4. In the Log Deletion Settings section, select the Enable log message deletion check box.
5. In the Retain log messages for setting, type 183. 183 days equals six months.
6. In the Database Backup Settings section, select the Enable backup of log messages check box.
7. In the Backup log data every setting, type 7. This sets the frequency of backups to once a week.
Send log notifications to a network administrator

We also need to configure the Log Server to use the Successful Company email server to send messages to the network administrators’ group.

1. In the Notification Setup section, select the **Turn on appliance notification** check box.
2. In the **Send email from** text box, type netadmin@mywatchguard.com.

3. Select the **Server Settings** tab. In the **Database Settings** section, select the **Send an email notification if the database reaches the warning threshold** check box. In the **Send warning message to** text box, type administrator@watchguard.com.

You can configure the Log Server to use your email server to send messages.

4. In the SMTP Server Settings section in the **Outgoing email server** text box, type mail.mywatchguard.com.

5. Select the **Use login information for the e-mail server** check box. In the **User Name** text box, type netadmingroup. In the **Password** text box, type mailpassword.

6. Click **OK** to apply your changes and close the **Log Server Configuration** utility.

When you type the domain name of a mail host in the notification setup fields, the Log Server tries to do a DNS lookup on the mail host. In this exercise, the DNS lookup fails because mywatchguard is a fictitious domain.
Change the encryption key

When a network administrator at Successful Company moves to London to take a job with another company, the remaining staff recognize that they need to change all the firewall passwords. In this exercise, we change their encryption key. While we are there, we add the Log Server administrator email address. This is the address to which all messages from the Log Server are sent.

1. Right-click the Log Server icon on the WatchGuard toolbar and select Configure.
   Before you can make any changes to the server, you must provide the Server Management Passphrase.
2. Type myservermanagementphrase. Click OK.
   The Log Server Configuration dialog box appears.
3. Select File > Set Master Encryption Key.
   The Master Encryption Key dialog box appears.
4. Type these three passphrases:
   - Old key
   - New key
   - Confirm new key
   - mylogserverkey
   - myencryptionkey
   - myencryptionkey

5. Click OK. Click OK again to close the Log Server Configuration utility.
   This changes the encryption key on the Log Server. Now, we must change the encryption key on every Firebox which sends its log messages to this server.
6. From Policy Manager, select Setup > Logging. Click Configure.
7. Select the Log Server IP address in the list, and click Edit. Type myencryptionkey. Type it again to confirm. Click OK. Click OK again.
8. If you have access to a Firebox for this lesson, save the configuration file to the Firebox.
Exercise 4: Enable Advanced Diagnostics and Performance Statistics

You can select the level of diagnostic logging to write to your log file or to Traffic Monitor. If you set the diagnostic level to the highest level, your log file will be much larger than usual. We recommend that you do not set the diagnostic level to the highest levels unless you are troubleshooting a problem. You can also enable Performance Statistics. The Firebox® sends log messages about external interface performance and VPN bandwidth statistics to your log file.

In this exercise, a Successful Company network administrator is troubleshooting a problem with the HTTP proxy on the Firebox. A WatchGuard® technical support representative asked the administrator to set diagnostic logging for the HTTP proxy to its highest level and send the resulting log file.

1. From Policy Manager, select Setup > Logging.
2. Click Advanced Diagnostics.
3. Expand the Proxy category on the left side of the screen, and select HTTP. Move the Settings slider up to the highest level to get the most information possible in the log messages generated regarding the HTTP proxy. Browse to My Documents\My WatchGuard\Shared WatchGuard\logs to find the database log file. This is the file you send to the technical support representative that is helping you troubleshoot your problem.

4. Click OK to close the Advanced Diagnostics dialog box. Click OK again to close Logging Setup.
5. Save the configuration file as Logging-Done. You can compare your results with the Logging-Finish file included with the training.
Related Courseware and Information

You can use these resources for more information on how to install a Log Server and set log database preferences.

**WatchGuard® System Manager User Guide**

**WatchGuard LiveSecurity® Online Resources**

**Reference Guide**
Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. What is the default location for a WatchGuard log file?
2. True or False: By default, the Log Server deletes log messages that are older than 365 days.
3. Which logging component is responsible for sending notification email messages when an event occurs on the Firebox that triggers notification?
   - A) Firebox
   - B) Log Server
   - C) Policy Manager

4. Which of these log configuration settings are available in the Policy Manager (select all that apply):
   - A) Scheduling reports
   - B) Setting the maximum size for a log database file
   - C) Setting the log encryption key
   - D) Selecting a backup Log Server for log messages
   - E) Setting the mail host and email address for email notifications
   - F) Configuring email notification for denied SMTP packets

5. Which of these log configuration settings are available in the Log Server Configuration utility (select all that apply):
   - A) Scheduling reports
   - B) Setting the maximum size for a log database file
   - C) Setting the log encryption key
   - D) Selecting a backup server for log message database files
   - E) Setting the mail host and email address for email notifications
   - F) Configuring email notification for denied SMTP packets

6. True or False: Log files created by a Firebox using Fireware appliance software are stored in a proprietary format, readable only by the WatchGuard LogViewer and Report Manager tools.

7. CHALLENGE: You are troubleshooting a problem with one of your branch office VPN tunnels. WatchGuard technical support asks you to enable the highest level of diagnostic logging for your IPSec VPN tunnels to try to get more information about the problem. Where do you go to get the information?
ANSWERS

1. Documents and Settings\WatchGuard\logs

2. False - By default, the Log Server does not delete old messages. You can use the Expiration Settings tab to configure it to do so on an interval that you set.

3. B. Log Server - The Log Server sends out the notification email in response to the log message it receives from the Firebox.

4. C, D, F

5. B, C, E

6. False - Log messages are stored in a SQL database file.

7. Open Policy Manager > Setup > Logging. Click the Advanced Diagnostics button. Expand VPN and select IKE. Move the slider up to select the highest level of diagnostic logging.

Copyright © 2008 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, the WatchGuard logo, Firebox, and Core are registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries.
Monitors

Monitoring Activity Through the Firebox

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak /Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Monitors</td>
</tr>
</tbody>
</table>

What You Will Learn

WatchGuard® System Manager includes several tools to monitor the health of your Firebox® and network. In this training module, you are shown how to:

- Interpret the information in WatchGuard System Manager display
- Modify the Security Traffic display to match your network configuration
- Change Traffic Monitor settings and trace the source of a connection
- Use Performance Console to create a graph that shows traffic to the external interface
- Use HostWatch to view network activity and block a site
- Add and remove sites from the Blocked Sites list
- Add feature keys to the Firebox

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

In this module, you will connect to one or more Firebox devices. If you take this course with a WatchGuard Certified Training Partner, your instructor will provide the IP address and passphrases for devices used in the exercises. For self-instruction, you can safely connect to a Firebox on a production network. You will not change the configuration files of any device.
As with any security product, regular monitoring of your firewall improves both performance and security. When you use WatchGuard® System Manager (WSM) to connect to a Firebox®, you are immediately presented with key information regarding the health of your firewall and the WatchGuard servers on your network. WSM is particularly useful for networks with more than one Firebox since you can see many devices at the same time. You can also monitor connections between Firebox devices.

With Firebox System Manager, you can quickly scan the configuration and status of a single Firebox, spot unusual activity, and take immediate action. Firebox System Manager includes eight monitors, each presented on a separate tab:

- **Front Panel** — Displays the status of each Firebox interface along with information about active tunnels and security services.
- **Traffic Monitor** — Displays a color-coded, scrolling list of the traffic passing through the Firebox.
- **Bandwidth Meter** — Provides a real-time graphical display of network activities across a Firebox.
- **Service Watch** — Shows a graph of the policies configured on a Firebox. The Y axis (vertical) shows the number of connections or bandwidth used per policy. The X axis (horizontal) shows the time. To get more information about a policy at a point in time, click a location on the chart.
- **Status Report** — Shows the technical details of the Firebox.
- **Authentication List** — Identifies the IP addresses and user names of all the users that are authenticated to the Firebox. To remove an authenticated user from the list, right-click a user name and close the authenticated session.
- **Blocked Sites** — Lists all the sites currently blocked by the Firebox. From this tab, you can remove a site from the temporary blocked sites list.
- **Security Services** — Shows the status of Gateway AntiVirus, Intrusion Prevention Service, and spamBlocker. From here, you can also perform a manual update of the signature databases used by Gateway AV and IPS. This tab is active only if you have purchased these services.

From the Firebox System Manager toolbar, you can also launch other Firebox monitoring tools, including:

- **Performance Console** — Used to prepare graphs based on Firebox performance counters to better understand how your Firebox is functioning.
- **HostWatch** — Shows the network connections between the trusted and external networks.
Exercise 1: Review Network Status in WSM

The Successful Company network administrator has now saved a basic configuration to his Firebox® and has installed and configured a Management Server, Log Server, and Report Server. We can now look at this network security infrastructure using the WatchGuard® System Manager.

1. From the Windows desktop, click Start > All Programs > WatchGuard System Manager 10 > WatchGuard System Manager.

2. Click the Connect to Device icon on the main toolbar.
   You can also select File > Connect To Device.

3. Type the trusted IP address of the Firebox you want to connect to.
   Use your Firebox IP address, or get the IP address from your instructor.

4. Type the Firebox status (read-only) Passphrase.
   Use the status passphrase to connect to a Firebox and display the status. The Firebox appears in the WSM display.

Interpreting the Device Status display
Information about a device you connect to appears in the WatchGuard System Manager Device Status tab. The information that appears includes the status, IP address, and MAC address for each Ethernet interface, and the installed certificates. It also includes the status of all virtual private network (VPN) tunnels that are configured in WSM.
Expanded information for each Firebox includes the IP address and subnet mask of each Firebox interface. It also includes:

- IP address and netmask of the default gateway (for external interfaces only).
- Media Access Control (MAC) address of the interface.
- Number of packets sent and received on each interface since the last Firebox restart.

Each device can be in one of four possible states, as indicated by the appearance of the device in the window:

- Normal icon — Usual operation. The device is successfully sending data to WatchGuard System Manager.
- Yellow question mark — The device has a dynamic IP address and has not yet contacted the Management Server.
- Red exclamation point and gray icon — WatchGuard System Manager cannot make a network connection to the device at this time.
- No exclamation point and gray icon — The device is being contacted for the first time or has not been contacted yet.

The Device Status tab also includes information on Branch Office VPN Tunnels and Mobile VPN tunnels.
Exercise 2: Use Firebox System Manager

The first tab of Firebox® System Manager has a group of indicator lights in the shape of a triangle or star to show the direction and volume of the traffic between the Firebox interfaces. The points of the star and triangle show the traffic that flows through the interfaces. Each point shows incoming and outgoing connections with different arrows. When traffic flows between the two interfaces, the arrows show the direction of the traffic.

In the star figure, the location where the points come together can show one of two conditions:

- Red (deny) — The Firebox denied a connection on that interface.
- Green (allow) — Traffic flows between this interface and a different interface (but not the center) on the star. When traffic flows from this interface to the center, the point between these interfaces shows as green arrows.

In the triangle, the network traffic shows in the points of the triangle. The points show only the idle and deny conditions.

If you use the star figure, you can customize which interface is in its center. The default star figure shows the external interface in the center. When you put a different interface in the center, you can see all traffic between that interface and the other interfaces. All allowed and denied traffic is relative to the interface in the center of the diagram. You see no information about traffic between interfaces on the perimeter of the star.

In this exercise, you start Firebox System Manager and change the status display.
Connect to a Firebox and change the display

1. From WatchGuard® System Manager, connect to your Firebox. Click the Connect to Device icon. Type your Firebox trusted IP address. Type the status passphrase. Click OK.

2. On the **Device Status** tab click the name or icon of the Firebox.

3. On the toolbar, click the **Firebox System Manager** icon. Firebox System Manager opens. It contacts your Firebox and gets data about network traffic, interface settings, and other status information.

4. As shown in the upper-left corner of the FSM window, the default mode shows in interfaces in a star shape.

5. In star display, click the red ball next to **eth2**. The eth2 interface moves to the center of the display. The other interfaces move in a clockwise direction.

6. Click the red ball next to **eth0** to move it back to the center of the display.
Use Traffic Monitor
Traffic Monitor is an application that displays a continuous list of log messages. With a default refresh interval set to five seconds, this almost real-time log monitoring tool may be the first place you look to troubleshoot any problems you have with your Firebox. A unique feature of Traffic Monitor is the ability to ping or trace the source of a connection you see in the Traffic Monitor window.

In this exercise, you use Traffic Monitor to trace the source of a connection through a Firebox accessible through the training lab.

1. From Firebox System Manager, select the Traffic Monitor tab.

![Traffic Monitor Screen Shot](image)

2. Select an entry in Traffic Monitor and right-click it.
3. From the Source IP address menu, select trace route. This executes the tracert command against the IP address identified as the source of the packet.
   Trace route is a utility that traces a packet from your computer to an Internet host. This shows how many hops the packet needs to reach the host and how long each hop takes.
4. In the pop-up window that appears with the results of the trace route, click OK.

Change Traffic Monitor settings
You can configure Traffic Monitor to use different colors to show different types of information. In this exercise, we change the source IP address for denied traffic to bright pink so that we can see it better.

1. From the Firebox System Manager menu, select File > Settings. The Settings dialog box appears.
2. On the Traffic Denied tab (which is selected by default), click source ip in the list of fields.
3. Click the color control adjacent to Text Control. The Text Color field to the right of the tabs show the current color set for the field.
4. Select a bright pink and click OK. The information included in this field opens in the new color in Traffic Monitor. A sample of how Traffic Monitor looks opens at the bottom of the dialog box.
5. Click OK again to close the Settings dialog box.
   For log messages of denied traffic, the source IP is now a bright pink.
Check Bandwidth Usage and Service Volume

When you connect to a training lab Firebox, you may not see lines form in these tabs. This is because your training Firebox is passing only a small amount of traffic.

Firebox System Manager also has a way for you to quickly check your firewall bandwidth usage and the volume of traffic for your primary proxies.

1. From Firebox System Manager, select the Bandwidth Meter tab.
   - The list of Firebox interfaces appears on the left. Each interface is a different color to identify them. The central panel shows the relative volume of traffic through each Firebox interface.

2. From Firebox System Manager, select the Service Watch tab.
   - On the left is a list of policies configured for your Firebox. Each interface is a different color to identify them. The central panel shows the relative volume of traffic examined by each proxy policy.
Exercise 3: Create a Performance Console Graph

Performance Console is a Firebox utility that you use to monitor different performance counters on the Firebox. With Performance Console, you define counters that identify the information that you want to see. You can see the information displayed as a graph, or export it to a third-party application.

Settings available for counter configuration include:

**Chart Window**
- `<New Window>` will open the new chart in a new window. If there is a chart already open, you can select it to show both charts in the same window.

**Poll Interval**
- Set how frequently data is gathered from the Firebox.

**Type**
- Use this drop-down list to select the type of graph to create: Rate, Difference, or Raw Value. Suppose you want to graph value_1 and time_1, value_2 at time_2, and so on.
  - **Rate** — If you create a graph by rate, you use the value difference divided by the time difference: (value_2-value_1)/(time_2-time_1), (value_3-value_2)/(time_3-time_2), and so on.
  - **Difference** — If you specify difference, you use the increase from the previous value to the new value: value_2-value_1, value_3-value_2, and so on.
  - **Raw Value** — If you specify raw value, you use the value only: value_1, value_2, and so on. The raw values are generally counters of content such as bytes or packets. The raw values can only increase, not decrease.

**Policy**
- To view the data for the traffic that is passing through an individual policy, select that policy from the drop-down list.

**Save Chart Data to File**
- Select this check box to save the data collected by Performance Console to an XML data file or a comma-separated data file. For example, you can open an XML data file in Microsoft Excel to see the counter value recorded for each polling interval. You can use other tools to merge data from more than one chart.

In this exercise, you use Firebox System Manager and your local Firebox to run a Performance Console graph that shows the utilization of the Firebox CPU.

1. From Firebox System Manager, click the **Performance Console** icon.
   - The Performance Console dialog box appears.
2. Click the **Add Chart** icon.
3. Expand **System Configuration** and select **CPU Utilization**.

4. Click **OK**.
   A performance graph opens to show the data collected for this counter.

5. Click **Close**.
Exercise 4: Use HostWatch to View Network Activity

HostWatch is an application that graphically shows the network connections between the trusted and external networks. HostWatch also gives information about users, connections, and network address translation (NAT).

In this exercise, you use HostWatch to view the activity on the training network.

1. From Firebox System Manager, click the HostWatch icon.
   The top part of the HostWatch window has two sides. You set the interface on the left side. The right side represents all other interfaces. HostWatch shows the connections to and from the interface configured on the left side.

2. To select an interface, right-click the current interface name or select View > Interface.

3. As you view the connections through the Firebox, double-click an item on either side. The Connections For dialog box shows information on the connections that involve that item. Click the X on the upper-right corner of the dialog box to close it.

4. In the HostWatch window, right-click any connection and select to add the source IP address to the Blocked Sites list.
   The Choose Expiration dialog box appears.

5. Set the time period to block the IP address and type the configuration passphrase when prompted. Click OK.
   The IP address is added to the temporary blocked sites list for the period of time you set here.

6. Close HostWatch.
Exercise 5: Use the Blocked Sites List

The Blocked Sites list shows all the sites currently blocked as a result of the rules defined in Policy Manager. From this tab, you can add sites to the list, or remove blocked sites. In this exercise, you remove the blocked site you added in the HostWatch exercise. You then add a site to the list.

1. From Firebox System Manager, select the **Blocked Sites** tab.

2. Find the IP address you just blocked in the list of blocked sites. Click **Delete** in the lower-right corner.

3. Type the configuration passphrase to remove the IP address from the Blocked Sites list.

4. To add a site, click the **Add** button at the bottom of the **Blocked Sites** display. Add the site 10.1.1.1 and block it for 24 hours.
   The site appears on the Blocked Sites list.
Exercise 6: Examine and Update Firebox Feature Keys

When you purchase an option for your Firebox®, you add a new feature key to your configuration file. You can use either Firebox System Manager or Policy Manager to see the feature keys currently installed on your Firebox. Use Policy Manager to update a Firebox with a new feature key.

View Feature Keys added to the Firebox

1. From Firebox System Manager, select View > Feature Keys. The Firebox License Keys dialog box appears.

2. Select one of the feature keys in the list and click Detail. The Feature Key Detail dialog box shows a list of the features in the feature key.
3. Click **OK** to close the **Feature Key Detail** dialog box. From the **Firebox License Keys** dialog box, click **Show Active Features**.
   The Active Features dialog box shows the name of each feature, the capacity the feature enables (such as number of users or a speed in Mbps), whether the feature is enabled or disabled, and (if applicable) the feature’s expiration date.

![Active Features](image)

Add a feature key to the Firebox
1. From Policy Manager, open the configuration file you are editing for these exercises.
2. Select **Setup > Feature Keys**.
   The Firebox Feature Keys dialog box appears.
3. Click **Import**.
   The Import Firebox Feature Key dialog box appears.
4. Paste an updated feature key which into the open space.
   You can purchase this key from WatchGuard. If you attend a WatchGuard Certified Training course, you will receive this key from your instructor.
5. Click **OK** to close the **Import Firebox Feature Key** dialog box. Click **OK**.
6. Save the configuration file to the Firebox.
   You can not use an optional feature until you both add the feature key to the configuration file and save it to your Firebox.

Related Courseware and Information

You can use these resources for more information on how to monitor the traffic through the Firebox®.

**WatchGuard® System Manager User Guide**
Browse to [https://www.watchguard.com/help/documentation/](https://www.watchguard.com/help/documentation/) and download the User Guide. See the chapter “Monitoring Firebox Status” and “Monitoring and Managing Your Network.”

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/)
Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. True or False: Performance Console is a Firebox utility that is used to prepare graphs that show various Firebox functions based on performance counters.

2. Which of the following monitoring tools can be viewed directly in a Firebox System Manager tab (select all that apply)?
   - [ ] A) LogViewer
   - [ ] B) Bandwidth Meter
   - [ ] C) HostWatch
   - [ ] D) Policy Manager
   - [ ] E) Traffic Monitor

3. True or False: You can add a site to the Blocked Sites list from HostWatch.

4. True or False: Service Watch is a monitor that provides a real-time display of the bandwidth consumed by policies across the Firebox.
   
   Match the correct monitoring tool to complete these tasks:
   1) Service Watch  
      a. Ping the source of a denied packet
   2) HostWatch  
      b. Not a Fireware monitoring tool
   3) Log Server  
      c. View a list of users connected through the Firebox
   4) Security Services  
      d. Add an IP address for the Firebox to block all traffic
   5) Traffic Monitor  
      e. Learn the status of your IPS signature database
   6) Blocked Sites List  
      f. See the volume of traffic generated by each proxy policy
1. True
2. B and D
3. True
4. False
5. 1: f, 2: c, 3: b, 4: a, 5: d

ANSWERS
Reports

Generating Reports of Network Activity

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak / Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Reporting</td>
</tr>
</tbody>
</table>

What You Will Learn

WatchGuard System Manager includes powerful tools to gather log data and generate reports. In this module, you are shown how to:

- Set up and configure a Report Server
- Generate and save reports at regular intervals
- Change report settings
- Save, print and share reports

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

Build Reports from Firebox Log Messages

When you install the WatchGuard® System Manager, you have the option to install the Report Server on either the management station or another, dedicated computer with Microsoft® Windows installed. The Report Server periodically pulls select data from one or more Log Servers. You can then use the Report Manager to review the collected data and generate reports.
Predefined Reports

WatchGuard Reports are summaries of the log data that you have selected to collect from the Firebox® log files. Report Manager consolidates the log data into a variety of predefined reports so you can quickly and easily locate and review Firebox actions and events. Predefined reports include:

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Traffic</td>
<td>Web activity trend</td>
<td>Trends, active clients, most popular domains, WebBlocker information, and web sites blocked by proxy rules.</td>
</tr>
<tr>
<td></td>
<td>Web trend summary</td>
<td>Hourly trend data</td>
</tr>
<tr>
<td></td>
<td>Most active clients</td>
<td>Top 50 clients by # of web connections</td>
</tr>
<tr>
<td></td>
<td>Most popular domains</td>
<td>Top 50 web sites visited by clients</td>
</tr>
<tr>
<td></td>
<td>WebBlocker service</td>
<td>Statistics and web sites blocked by WebBlocker</td>
</tr>
<tr>
<td></td>
<td>URL details by time</td>
<td>All URLs in chronological order</td>
</tr>
<tr>
<td></td>
<td>URL details by client</td>
<td>All URLs in order by client</td>
</tr>
<tr>
<td></td>
<td>URL details by domain</td>
<td>All URLs in order by domain</td>
</tr>
<tr>
<td></td>
<td>Web activity audit</td>
<td>Includes allowed web sites for HTTP connections, if you enable the audit flag for HTTP in Policy Manager.</td>
</tr>
<tr>
<td>Intrusion Prevention</td>
<td>Intrusion Prevention Summary</td>
<td>All intrusion prevention actions</td>
</tr>
<tr>
<td></td>
<td>Detail by protocol</td>
<td>Prevention summary details by protocol</td>
</tr>
<tr>
<td></td>
<td>Detail by severity</td>
<td>Prevention summary details by severity</td>
</tr>
<tr>
<td></td>
<td>Detail by source IP</td>
<td>Prevention summary details by source IP</td>
</tr>
<tr>
<td></td>
<td>Detail by signature</td>
<td>Prevention summary details by signature</td>
</tr>
<tr>
<td>AntiVirus Summary</td>
<td>AntiVirus summary</td>
<td>AntiVirus action summary</td>
</tr>
<tr>
<td></td>
<td>Detail by protocol</td>
<td>AntiVirus action details by protocol</td>
</tr>
<tr>
<td></td>
<td>Detail by host (HTTP)</td>
<td>AntiVirus action details by host</td>
</tr>
<tr>
<td></td>
<td>Detail by virus</td>
<td>AntiVirus action details by virus</td>
</tr>
<tr>
<td></td>
<td>Detail by email sender</td>
<td>AntiVirus action details by email sender</td>
</tr>
<tr>
<td></td>
<td>spamBlocker summary</td>
<td>Statistics by spam type, action, and top spam senders and recipients</td>
</tr>
<tr>
<td></td>
<td>spamBlocker by sender</td>
<td>Statistics by sender</td>
</tr>
<tr>
<td>Proxy Summaries</td>
<td>Host summary</td>
<td>Proxy action summary</td>
</tr>
<tr>
<td>SMTP Proxy Summary</td>
<td>SMTP server summary</td>
<td>SMTP server activity summary (for internal and external email accounts)</td>
</tr>
<tr>
<td></td>
<td>SMTP email summary</td>
<td>SMTP email activity summary (for internal and external servers)</td>
</tr>
<tr>
<td></td>
<td>SMTP proxy detail</td>
<td>SMTP proxy action records by time</td>
</tr>
<tr>
<td>POP3 Proxy</td>
<td>Email account summary</td>
<td>Internal and external email accounts</td>
</tr>
<tr>
<td></td>
<td>Email server summary</td>
<td>Internal and external servers</td>
</tr>
<tr>
<td></td>
<td>POP3 detail</td>
<td>All records by time</td>
</tr>
<tr>
<td>Packet-Filtered Summary</td>
<td>Host summary</td>
<td>Summary of all packet-filter data</td>
</tr>
</tbody>
</table>
### Customizing Reports

With the advanced features of Report Manager, you can:

- Set report options such as background color, maximum number of records per file, and the directory in which to store reports.
- Select report parameters, such as date ranges for reports and groups of Firebox devices you want to create reports for.
- Change the report type from HTML to PDF or back.
- Email, print, or save a report.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firebox Statistics</td>
<td>Firebox statistics</td>
<td>Firebox bandwidth statistics for all interfaces</td>
</tr>
<tr>
<td></td>
<td>External interface bandwidth</td>
<td>Firebox bandwidth statistics summary (for external interfaces)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The data sampling interval is based on the report time range. The minimum</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interval is 1 minute. The published report samples data every 10 minutes.</td>
</tr>
<tr>
<td></td>
<td>VPN tunnel bandwidth</td>
<td>VPN tunnel traffic summary</td>
</tr>
<tr>
<td>Exceptions</td>
<td>Denied packet summary</td>
<td>Log summary for all denied packets</td>
</tr>
<tr>
<td></td>
<td>Denied incoming packets detail</td>
<td>Detailed log for each incoming action</td>
</tr>
<tr>
<td></td>
<td>Denied outgoing packet detail</td>
<td>Detailed log for each outgoing action</td>
</tr>
<tr>
<td></td>
<td>Alarms</td>
<td>All alarm records</td>
</tr>
<tr>
<td>Management Server</td>
<td>Server audit summary</td>
<td>Server audit details summary</td>
</tr>
<tr>
<td>Audit</td>
<td>Server audit detail</td>
<td>All server audit details</td>
</tr>
<tr>
<td></td>
<td>Server Authentication Report</td>
<td>All server authentication failures</td>
</tr>
<tr>
<td>Reports</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Exercise 1: Configure a Report Server

Successful Company network administrators decide that for performance reasons, they are going to install the Report Server on a dedicated computer. In this exercise, we activate and configure their Report Server.

Activate the Report Server

After you install the WatchGuard® Report Server on a personal computer with Microsoft® Windows, you must use the wizard to activate the server.

1. From the Windows desktop, right-click the Report Server icon in the WatchGuard toolbar.

2. Select Setup Wizard.

3. Click Next.

4. In the Master Passphrase field, type myreportserver. Type it again. Click Next.

5. In the Server Management Passphrase, type myservermanagementphrase. Type it again. Click Next.

6. Type Successful Company, Inc. Click Next.

7. Click Finish.

Add a Log Server

A Report Server can consolidate data from one or more Log Servers. You must add the IP address of each Log Server to the Report Server configuration file.

1. From the Windows desktop, right-click the Report Server icon in the WatchGuard toolbar. Select Configure.

2. Type myservermanagementphrase. Click OK.


4. To the right of the Log Server(s) section, click Add.

5. In the IP address field, type the IP address of your Log Server.

6. In the Password field, type mylogserverkey.

If attending a class, your instructor installed the Report Server on your workstation.
7. Click OK. The IP address of the Log Server appears in the list of Log Servers. A single Report Server can consolidate data from more than one Log Server.

Select reports and timing
By default, the Report Server automatically generates all predefined reports every Monday just after midnight. At Successful Company, the network administrator would prefer to generate these reports on Friday night. He also has not purchased the WatchGuard® Gateway Antivirus/IPS option and turns off those reports.

1. From the Report Generation tab, use the Begin generating weekly reports on drop-down list to select Friday.
2. In the Begin generating reports at text box, type 11:59 PM.
3. In the Select Report Type section, clear the IPS Reports and AV Reports check boxes.

4. Click OK to close the Report Server Configuration utility and save your changes.
Exercise 2: Use the Report Manager

While the Report Server collects and consolidates raw log data from one or more Log Servers, the Report Manager enables you to review and share these reports. In this exercise, the Successful Company network administrator uses the WatchGuard Report Manager to review several recent reports.

Connect to a Report Server

The first step is to connect the WatchGuard® Report Manager to a Report Server. This is particularly important for large organizations with multiple Report Servers.

1. From WatchGuard System Manager, select **Tools > Logs > Report Manager**. The Connect to Report Server dialog box appears.

2. In the **Name/IP Address** text box, type the IP address of your Report Server. In most training environments, this is the same IP address as your management station.

3. In the **Passphrase** text box, type **myreportserver**. Click **Login**. The Accept Certificate dialog box appears.


Your instructor may ask you to connect to a training lab Report Server which already has reports built for the training lab firewall.
Create a report group
Now we create a group for the Successful Company home offices, which each use a Firebox Edge device.

1. From the Report Manager, select **Edit > Define a Group**.
   The Create a Group dialog box appears.
2. In the **Group Name** text box, type Edge Devices.
   This is the name that appears in the list of available reports.
3. Select the check boxes for the Edge devices.
   Your instructor will help you select devices on the training lab Report Server.
4. Click **OK**.
   The Group name appears in the Devices drop-down list. You now see a list of reports available for those devices.
5. Click the first report in the list.
   Report Manager runs the report, and it appears on the right.

Change default report settings
The Successful Company network administrator would like to increase the maximum number of records for his HTML report. He also can't read the dark charts.

1. From the Report Manager, select **View > Options**.
   The Options dialog box appears.
2. Clear the **Use dark background for charts and dialogs** check box.
   This will change the charts from white on black to black on white.
3. In the **Maximum records per HTML file**, type 400.
   This increases the total number of records per report to 400.

4. Click **OK**.
5. Double-click the first report in the list.
   Report Manager runs the report again and the display reflects the new settings.

Exercise 3: Share reports
In this exercise, the Successful Company network administrator mails a weekly report to his manager. He also makes a hard copy for the SarbOx auditors. Finally, he decides to pull the data from a report into a spreadsheet so he saves the report as a CSV file.

1. From the Report Manager, select the second report in the report list.
2. Select **File > Send To**. Report Manager opens the email composition dialog box for your default email application. The URL of the report is in the body of the message.

3. Use the compose email dialog box to add the email address and subject of the message. You can also add text to the body of the message. Send the message. Your instructor will tell you which printer driver to use in the training lab.

4. Select **File > Print**. Select a local printer. Click **Print**.

5. Select **File > Save**. The Save dialog box appears.

6. In the **File Name** text box, type **Edge Report**. Use the **File Type** drop-down list to select **CSV file (*.csv)**. Click **Save**. Report Manager saves the data in the report as a CSV file.

7. Click **OK**.

**Related Courseware and Information**

You can use these resources for more information on how to work with configuration files.

**WatchGuard® System Manager User Guide**

Browse to [https://www.watchguard.com/help/documentation/](https://www.watchguard.com/help/documentation/) and download the User Guide. See the chapter “WatchGuard Reports.”
Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. True or False: You can run a report about more than one Firebox at the same time.

2. Which one of these is a device used in the WatchGuard reporting architecture (select all that apply):
   - [ ] A) Report Server
   - [ ] B) Quarantine Server
   - [ ] C) Log Server
   - [ ] D) Firebox
   - [ ] E) Active Directory Server

3. Circle the WatchGuard utility you use to configure each of the following:
   - Select Log Server used by a Firebox
     - Policy Manager
     - Report Server
     - Log Server
     - Report Manager
   - Set number of HTML records per report
     - Policy Manager
     - Report Server
     - Log Server
     - Report Manager
   - Select Log Server polled by Report Server
     - Policy Manager
     - Report Server
     - Log Server
     - Report Manager
   - Set the frequency reports are generated
     - Policy Manager
     - Report Server
     - Log Server
     - Report Manager
   - Email a report
     - Policy Manager
     - Report Server
     - Log Server
     - Report Manager
   - Set the date range for a report
     - Policy Manager
     - Report Server
     - Log Server
     - Report Manager
   - Select the reports compiled
     - Policy Manager
     - Report Server
     - Log Server
     - Report Manager
Set the date range for a report - Report Manager, Select the reports completed - Report Server, Select the Log Server used by a Firebox - Policy Manager, Set the number of HTML records per report - Report Manager, Select the Log Server polled by Report Server - Report Server, Set the frequency reports are generated - Report Server, Email a report - Report Manager, Select the date range for a report - Report Manager, Select the reports compiled - Report Server, Set the frequency reports are generated - Report Server, Email a report - Report Manager.
**NAT**

**Using Network Address Translation**

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak / Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Category</td>
<td>NAT</td>
</tr>
</tbody>
</table>

**What You Will Learn**

As with many routing devices, the WatchGuard® Firebox® can use network address translation (NAT) to conceal the IP address space of your network. In this training module, you are shown how to:

- Learn the forms of NAT available with the Firebox
- Add more IP addresses to which the Firebox will apply Dynamic NAT
- Use Static NAT to protect public servers

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

**NAT Hides Your Network Architecture**

Networks use network address translation (NAT) to hide IP addresses of servers and computers from users on the external network. Using NAT, addresses of IP packets are changed to a new value as they pass through the Firebox®.

NAT is an important tool for today’s network administrators. When a user’s computer sends a message to the outside world through a Firebox that uses NAT, the Firebox changes the IP address to an assigned value before it sends the message to the Internet. When a user on the outside sends a reply, the Firebox restores the actual address and delivers it back to the internal user.
Dynamic NAT
With Dynamic NAT, the Firebox changes outgoing source IP addresses to the IP address of the Firebox’s external interface. The Firebox tracks the private source IP address and destination address, as well as other IP header information such as source and destination ports, and protocol.

With Dynamic NAT, all connections must start from behind the Firebox. Malicious hosts cannot start connections to the computers behind the Firebox when the Firebox is configured for Dynamic NAT. When Dynamic NAT is applied to a packet, the source port is usually changed along with the source IP and related to the corresponding original IP header information. When a response arrives with the same protocol to the public IP and new source port, the firewall examines the stateful table and finds the original, private IP address. It reverses the NAT process to send the packet to the correct host.

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 NAT Setup 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.

1-to-1 NAT
When you enable 1-to-1 NAT, the Firebox 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 be made public. You can use 1-to-1 NAT to map public IP addresses to the internal servers, and you do not need to change the IP address of your internal servers. To understand how to configure 1-to-1 NAT, we give this example:

Successful Company has a group of three privately addressed servers behind the optional interface of their Firebox X. These addresses are:

- 10.0.2.11
- 10.0.2.12
- 10.0.2.13

The Successful Company administrator selects three public IP addresses from the same network address as the external interface of their Firebox, and creates DNS records for the email servers to resolve to. These addresses are:

- 50.50.50.11
- 50.50.50.12
- 50.50.50.13

Now the Successful administrator configures a 1-to-1 NAT rule for his email 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 Firebox creates the bidirectional routing and NAT relationship between the pool of private IP addresses and the pool of public addresses.

To connect to a computer located on a different Firebox interface that uses 1-to-1 NAT, you must use the private (NAT base) IP address for that computer. If this is a problem, you can disable 1-to-1 NAT and use Static NAT.

Defining 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. A 1-to-1 NAT rule always has precedence over Dynamic NAT. You must also configure:

**Interface**
The name of the Firebox Ethernet interface on which 1-to-1 NAT is applied. The Firebox will apply 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**
The NAT base IP address is the address that the real base IP address changes to when 1-to-1 NAT is applied. In our example above, the NAT base is 50.50.50.11.

**Real base**
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 interface specified, the 1-to-1 action is applied. In our example above, the real base is 10.0.2.11.

**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 our example above, the number of hosts to apply NAT to is three.
### Policy-based NAT

With policy-based Dynamic NAT, the Firebox uses the primary IP address of the outgoing interface or another specified IP address for the outgoing packets for a policy. Each policy has Dynamic NAT enabled by default. You can disable Dynamic NAT for all traffic in a policy. Double-click any policy and select the Advanced tab to see the NAT settings.

With this type of NAT, the Firebox 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. To change the Dynamic NAT configuration in a policy, open a policy for edit and select the Advanced tab. Select the Dynamic NAT check box. Select Use Network NAT Settings if you want to use the Dynamic NAT rules set for the Firebox. Select All traffic in this policy if you want to apply NAT to all traffic in this policy.

If you select All traffic in this policy, you can also select the Set source IP check box to set 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. Select this option to force outgoing SMTP traffic to show the MX record address for your domain when the IP address on the external interface for the Firebox is not the same as your MX record IP address.

### Policy-based 1-to-1 NAT

With this type of NAT, the Firebox 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, the 1-to-1 NAT takes precedence.

### Static NAT

Static NAT is also known as port forwarding. Static NAT allows inbound connections on specific ports to one or more public servers from a single external IP address. The Firebox changes the destination IP address of the packets and forwards them based on the original destination port number. You can also translate the original destination port to an alternative port on which the server is listening.

You typically use Static NAT for public services such as web sites and email. For example, you can use Static NAT to designate a specific internal server to receive all email. Then, whenever someone sends email to the Firebox's external IP address, the Firebox can forward the connection to the private IP address of the designated email (SMTP) server.

Static NAT is available only for policies that use a specified TCP or UDP port. If you have a policy that uses a protocol other than TCP or UDP, the NAT button in the Properties dialog box of that policy is disabled. To make a Static NAT policy, the internal host must be on a network configured to use Dynamic NAT.
Exercise 1: 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 Firebox® applies the Dynamic NAT rules in the sequence that they appear in the Dynamic NAT Entries list.

In this exercise, we configure the Successful Company Firebox to dynamically NAT all traffic from their trusted network to any external network.

1. From Policy Manager, open the configuration file you are editing for these exercises.
2. Select Network > NAT. The NAT Setup dialog box appears.
3. Select the Dynamic NAT rule for 10.0.0.0/8 - Any-External, click Remove. Click Yes to confirm.
5. In the From text box, type 10.0.1.0/24. The From field defines the source of the IP packets. In this exercise, the 10.0.1.0/24 network is the Successful Company trusted network on interface #0. We have reduced the range of addresses from the larger 10.0.0.0/8 to only those addresses actually in the Successful Company network.
6. From the To drop-down list, select Any-External. This sets the Firebox to dynamically NAT all traffic to any external network.
7. Click OK. The new entry appears in the Dynamic NAT Entries list.
8. Click OK to close the NAT Setup dialog box.
Exercise 2: Configure Static NAT to Protect Public Servers

In this exercise, you configure the Successful Company Firebox® to use Static NAT for their SMTP server.

1. From Policy Manager, select **Edit > Add Policy**.
2. From the **Proxies** list of policies, select **SMTP-proxy** and click **Add**.
   The New Policy Properties dialog box appears.
3. Under the **From** list, select **Any-Trusted**. Click **Remove**.
4. Under the **From** list, click **Add**. Select **Any-External** and click **Add**, then click **OK**.
5. Under the **To** list, click **Add**. Then click **Add NAT**.
   The Add Static NAT dialog box appears.
6. Make sure the **External IP Address** field includes the external interface IP address of your Firebox. In the **Internal IP Address** field, type **10.0.2.25**.
   This is the private IP address of the SMTP server located on the trusted network.
7. Click **OK** to close the **Edit Static NAT** dialog box. Click **OK** to close the **Add Address** menu. Click **OK** to close the **New Policy Properties** dialog box. Click **Close** on the **Add Policies** dialog box.
   The SMTP-proxy policy appears in the policy list. Notice the setting in the **To** column.
8. Save the configuration file as **NAT-Done**.
   You can compare your results with the NAT-Finish file included with the training.

Frequently Asked Questions

**Are there any other reasons to use NAT?**
Yes. When you create a branch office VPN tunnel between two networks that use the same private IP address range, an IP address conflict occurs. To prevent this, both networks must apply 1-to-1 NAT to the VPN. This makes the IP addresses on your computers appear to be different from their true IP addresses when traffic goes through the VPN. 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.
Related Courseware and Information

You can use these resources for more information on how to work with configuration files.

**WatchGuard® System Manager User Guide**

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/).

---

**Test Your Knowledge**

Use these questions to practice what you have learned and exercise new skills.

1. Fill in the blank: ________________ NAT conserves IP addresses and hides the internal topology of your network.
2. Fill in the blank: ________________ NAT is often used for policies that require more than one port or port numbers that change dynamically, such as for many messaging and video conferencing applications.
3. Complete the missing entries:
The default Dynamic NAT entries in Policy Manager are:

   __________/___  Any-External
   172.160.0.0/12  __________
   __________/___  Any-External

4. Static NAT for a policy is also known as (select all that apply):
   - [ ] A) IP masquerading
   - [ ] B) Port forwarding
   - [ ] C) Tunnel swapping
   - [ ] D) Quality of Service
   - [ ] E) All the above

5. True or False: Dynamic NAT rewrites the source IP of packets to use the IP addresses of the outgoing interface.
ANSWERS

1. Dynamic
2. 1-to-1
3. 192.168.0.0/16 Any-External
   172.16.0.0/12 Any-External
   10.0.0.0/8 Any-External
4. B
5. True
Authentication

Verifying a User’s Identity

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak /Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Authentication</td>
</tr>
</tbody>
</table>

**What You Will Learn**

*User authentication* is a process that allows a device to verify the identity of someone who connects to a network resource. In this training module, you are shown how to:

- Understand authentication and how it works with the Firebox®
- List the types of third-party authentication servers you can use with Fireware
- Use Firebox authentication users and groups
- Add a Firebox authentication group to a policy definition
- Modify authentication timeout values
- Use the Firebox to create a custom web server certificate

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

In this module, you will configure the Firebox to use third party authentication servers. If you take this course with a WatchGuard Certified Training Partner, your instructor may provide you with configuration details for servers in the training network. For self-instruction, we encourage you to get the information needed to configure the Firebox to use your internal authentication method.

**Monitor and Control Network Traffic by User**

Because all traffic in to and out of your network passes through the Firebox®, you can use its authentication features to monitor and control connections on a user by user basis. Several technologies are currently integrated with WatchGuard® System Manager to authenticate users. In addition, the Firebox has its own authentication server.

Authentication is very important when you use dynamic IP addressing (DHCP) for computers on trusted or optional networks. It is also important if you must identify your users before you let them connect to resources on the external network. Because the Firebox associates a user name to an IP address, we do not
recommend that you use authentication features in a network with multi-user computers such as Unix servers, terminal servers or Citrix servers. The Firebox authenticates one user per computer.

With WatchGuard® System Manager, you can configure authentication on a per policy basis. For example, you can force some users to authenticate before they connect to an FTP server although they can browse the Internet without authentication.

**How Firebox User Authentication Works**

A special HTTPS server operates on the Firebox to accept authentication requests. To authenticate, a user must connect to the authentication web page on the Firebox. The address is:

```
https://trusted or optional IP address of a Firebox interface:4100/
```

The user must type a user name and password. The page sends the name and password to the authentication server using a challenge and response protocol (known as PAP). When the user is authenticated, the user is then allowed to use the approved network resources. The user can close the browser window. The user is authenticated for two hours after the last connection to a network resource for which authentication is necessary.

To stop an authentication session before the two-hour timeout, click **Logout** on the authentication web page. If the window is closed, you must open it again to disconnect. To prevent an account from authenticating, you must disable the account on the authentication server.

**Using Authentication from the External Network**

The primary function of the authentication tool is for outgoing traffic. You can also create policies that require external users to authenticate before getting access to network services incoming through the Firebox. You must configure the WG-Auth policy to allow users external to the Firebox to authenticate to the Firebox. External users type this URL in their browser to connect to the Firebox for authentication:

```
https://public IP address of a Firebox interface:4100/
```

**Using Authentication through a Gateway Firebox to Another Firebox**

To send an authentication request through a gateway Firebox to a different Firebox, you must add a policy to allow the authentication traffic on the gateway Firebox. On the gateway Firebox, use Policy Manager to add the WG-Auth policy. This policy controls traffic on TCP port 4100. Configure the policy to allow traffic to the IP address of the destination Firebox.

**Authentication methods available with Fireware**

Fireware® supports multiple authentication methods:

- Firebox
- RADIUS
- SecurID
- VASCO
- Generic LDAP (Lightweight Directory Access Protocol)
- Active Directory

When you use a third-party authentication server, you configure it with the instructions from its manufacturer. You install the server with access to the Firebox and put it behind the Firebox for security.

You can configure a primary and backup authentication server with any type of third-party authentication. If the Firebox cannot connect to the primary authentication server after three attempts, the primary server is marked as dead and an alarm message is generated. The Firebox then connects to the backup authentication server. If the Firebox cannot connect to the backup authentication server, it waits ten minutes, and then tries to connect to the primary authentication server again.
Monitor and Control Network Traffic by User

Using the Firebox authentication server
You can use the Firebox as an authentication server. This feature is often used by customers who do not have a third-party authentication server and do not need to manage user accounts centrally for multiple applications.

You must perform these steps to prepare your Firebox as an authentication server:

- Divide your company into groups according to tasks people do and information they need
- Create users for the groups
- Assign groups and users to policies

About third-party authentication servers
The procedure to configure the Firebox to use a third-party authentication server is similar for all the types Fireware supports. Before you configure your authentication server:

- You must have the configuration information for your server such as server port, IP address, and shared secret. If you use Active Directory or LDAP you must also know the group membership attribute and Distinguished Name (DN) of the Organizational Unit (OU) that contains the user accounts.
- If it is available, you can configure the Firebox with a backup authentication server to contact if it cannot connect to the primary authentication server.
- The Firebox must be able to connect to the authentication server.
- You must add the WatchGuard Authentication policy.

RADIUS authentication servers
Remote Authentication Dial-In User Service (RADIUS) 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.

The authentication messages to and from the RADIUS server always use an authentication key. This authentication key, or shared secret, must be the same on the RADIUS client and server. Without this key, hackers cannot get to the authentication messages. Note that RADIUS sends a key, and not a password, during authentication. For web and MUVPN authentication, RADIUS supports only PAP (not CHAP) authentication. For authentication with PPTP, RADIUS supports only MSCHAPv2.

To use RADIUS server authentication with the Firebox, you must:

- Add the IP address of the Firebox to the RADIUS server, as described in the RADIUS vendor documentation.
- Enable and specify the RADIUS server in your Firebox configuration.
- Add RADIUS user names or group names into the policies in Policy Manager.

To configure VASCO server authentication, use the RADIUS configuration user interface.

SecurID authentication servers
To use SecurID authentication, you must configure both the RADIUS 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 instructions for more information.

LDAP authentication servers
You can use an LDAP (Lightweight Directory Access Protocol) authentication server to authenticate your users to the Firebox. 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 Firebox for LDAP authentication, make sure you check your LDAP vendor documentation to see if your installation requires case-sensitive attributes.

When you configure the Firebox to use LDAP authentication, you must set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match. The standard
format for the search base setting is: ou=organizational unit,dc=first part of distinguished server name,dc=any part of the distinguished server name appearing after the dot. For example, if your user accounts are in an OU (organizational unit) you refer to as “accounts” and your domain name is mywatchguard.com, your search base is: ‘ou=accounts,dc=mywatchguard,dc=com’.

**Active Directory authentication servers**

Configuring the Firebox to use Active Directory authentication is similar to the process for LDAP authentication. You must set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match. The standard format for the search base setting is: ou=organizational unit,dc=first part of distinguished server name,dc=any part of the distinguished server name appearing after the dot.

For those who use an Active Directory authentication server, the Firebox supports Single Sign-On (SSO). SSO is a method of network access control that allows a user to enter credentials once to gain access to many resources. The WatchGuard SSO agent caches the user name and password and then passes it to each network resource as needed. You can install the WatchGuard SSO agent behind the Firebox on the trusted network. Users log in to the Windows domain controller which then passes the credentials to the SSO agent. The Firebox in turn queries the SSO Agent when users try to connect to resources outside their own network.

**About authentication timeout values**

Users are authenticated for some time after they close their last authenticated connection. This timeout is set either as a global setting in the Authentication Settings dialog box, or in the Setup Firebox User dialog box. The Firebox User setting overrides the global setting. The global setting is used only if no Firebox User value is defined.

For users authenticated by third-party servers, the timeouts set on those servers also override the global authentication timeouts.

**Exercise 1: Add a Firebox User Group and Add Users**

In this exercise, we learn that Successful Company does not yet have an authentication server. The network administrator decides to use the Firebox® for authentication. We will configure a group for the Marketing department and add four of the department employees.

**Create a Firebox user group**

1. From Policy Manager, open the configuration file you are editing for these exercises.
2. Select **Setup > Authentication > Authentication Servers**. The Authentication Servers dialog box appears. The top tab is the Firebox authentication server tab.
3. Click **Add** below the **User Groups** list on the **Firebox** tab. The Setup Firebox Group dialog box appears.
4. In the **Name** field, type Marketing.
5. Click **OK**.
   The new group appears in the User Groups list.

Add Firebox users

An **authorized user** is someone with access permission to your network. Each user must have a unique user name. When you use the Firebox authentication server, this information is saved in a database that is stored on the Firebox.

1. From the **Authentication Servers** dialog box, below the **Users** list, click **Add**.
   The Setup Firebox User dialog box appears.
2. Type this information into the dialog box:
   
<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>allison</td>
</tr>
<tr>
<td>Description</td>
<td>Allison Grayson</td>
</tr>
<tr>
<td>Passphrase</td>
<td>allyscomputer</td>
</tr>
<tr>
<td>Confirm</td>
<td>allyscomputer</td>
</tr>
</tbody>
</table>

   When the passphrase is set, you cannot see the passphrase in plain text again. If the passphrase is lost, you must set a new passphrase. A passphrase contains a minimum of eight characters.
3. To add Allison to the Marketing group, select **Marketing** in the **Available** list. Click the button with two arrows that points to the left side.

4. Click **OK**. Allison appears in the User list.

5. Repeat steps 2 - 4 to add these users to the Marketing group.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Passphrase</th>
</tr>
</thead>
<tbody>
<tr>
<td>joe</td>
<td>Joe Uknalis</td>
<td>joescomputer</td>
</tr>
<tr>
<td>tim</td>
<td>Tim Warner</td>
<td>timscomputer</td>
</tr>
<tr>
<td>wyatt</td>
<td>Wyatt Hare</td>
<td>wyattscomputer</td>
</tr>
</tbody>
</table>

6. After you add all users to the Marketing group, click **OK**. The Authentication Servers dialog box should look like this.

7. Click **OK** to close the **Authentication Servers** dialog box.
Exercise 2: Edit Policies to Use Firebox Authentication

After you configure the Firebox® with authentication user names and groups, you can add user names to your policies. In this exercise, you give the Marketing group permission to connect to an FTP server on the optional network that Successful Company uses to share files with outside vendors. You also block all FTP connections from other users on the network.

1. From Fireware Policy Manager, double-click the FTP policy. The Edit Policy Properties dialog box appears. The default configuration of the FTP proxy policy allows connections from any computer on the trusted or optional networks to any FTP server on the external network.

2. In the From list, click Any-Trusted. Click Remove. Click Any-Optional. Click Remove. With the Any-Trusted and Any-Optional entries, any user on your optional or trusted network is able to start an FTP connection to the entries on the To list. When you remove these entries, you block FTP connections from your optional and trusted networks.

3. In the To list, click Any-External. Click Remove. With the Any-External entry, users on your network can connect to any FTP server on the external network.

4. Below the From box, click Add. The Add Address dialog box appears.

5. Click Add User. The Add Authorized Users or Groups dialog box appears.

6. In the Type box, make sure Firewall is selected.

7. In the box to the right of the Type box, use the drop list to select Select. The Add button on this dialog box opens the Authorized Users and Groups dialog box from which you can add additional users and groups to the Firebox database.

8. Select the Marketing (Firebox-DB) group and click Add. Click OK to add the entry to the FTP policy. The Marketing group appears in the From list.

9. Under the To list, click Add. The Add Address dialog box appears.

10. Click Add Other. The Add Member dialog box appears.

11. Verify that the Choose Type drop-down list is set to Host IP. In the Value field, type 10.0.2.21. This is the IP address of the FTP server on the optional network. In a real-world environment, you must activate NAT for external users to be able to connect to this FTP server because it has a private IP address. For more information, see the “NAT” training module.
12. Click OK to close the Add Member dialog box. Click OK again to close the Add Address dialog box. You configured the FTP policy to allow connections from anyone in the Marketing group to an FTP server on the optional network. The Edit Policy Properties dialog box should look like this.

![Edit Policy Properties](image)

13. Click OK to close the Edit Policy Properties dialog box.

**Exercise 3: Set Global Authentication Values**

In this exercise, you set authentication values that the Firebox® uses by default. If you set session and idle timeouts in the Setup Firebox User dialog box or on any third-party server you use for authentication, these values override the global settings.

**Set global timeout values**

1. From Policy Manager, select Setup > Authentication > Authentication Settings. The Authentication Settings dialog box appears.
2. In the Session Timeout field, type 4. Use the drop list to select Hours. This is 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.
3. In the Idle Timeout field, type 10. Use the drop list to select Minutes. This is 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, no idle timeout is used and the user can stay idle for any length of time.
Set other global values

The Successful Company network administrator is concerned with users logging in to multiple computers simultaneously. In this exercise, we block concurrent authentication and set the browsers to automatically redirect to the home page of the internal web server.

1. From the Authentication Settings dialog box, disable the **Allow multiple concurrent firewall authentication logins from the same account** check box.
   
   If you use the Firebox as an authentication server, 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. This feature is enabled by default.

2. Enable the **Send a redirect to the browser after successful authentication** check box. In the text box, type `http://10.0.1.80/home.html`.
   This is the home page of the Successful Company internal web server located on the trusted network.

3. Click **OK** to close the Authentication Settings dialog box.

Exercise 4: Enable Single Sign On For the Firebox

Successful Company is growing and adding employees. They need to shift to a system that allows them to track users and groups in one location rather than both the Firebox® and their Windows Active Directory server. In this exercise, we configure the Firebox to use Active Directory and enter the server address for the Single Sign-On (SSO) agent.

1. From the Policy Manager, select **Setup > Authentication > Authentication Servers**. Click the **Active Directory** tab.

2. Click the **Enable Active Directory server** check box.

   This action enables the fields to configure the Firebox to use Active Directory. For more information about how to configure the Firebox for Active Directory authentication, see the WatchGuard System Manager User Guide.
3. In the **IP Address** field, type 10.0.1.89.

4. Click **OK** to close the Authentication Servers dialog box. The Firebox is now configured to use Active Directory.

5. Select **Setup > Authentication > Authentication Settings**. The Authentication Settings dialog box appears.

6. Click the **Enable Single Sign-On (SSO) with Active Directory** check box. This action enables the fields to configure Single Sign-On.

7. In the **SSO Agent IP Address**, type 10.0.1.90. This is the IP address of the Successful Company computer on which the WatchGuard Single Sign-On agent has been installed.

8. Click **OK** to close the Authentication Settings dialog box.
Use a Web Server Certificate

The WatchGuard® authentication applet is a form of web page. If your user community uses a very strict browser security policy, it will verify that the page certificate is from a trusted source. Each time the authentication applet loads, the user is presented with a security alert to let them know that the certificate is not from a trusted source.

You can avoid this problem by configuring the Firebox with a certificate to use for all secure HTTP connections. Each user must then import the certificate to their trusted root store. The Firebox can either use the default certificate signed by the Firebox, use a third party certificate, or generate a custom certificate.

In this exercise, we configure the Firebox to generate and use a custom certificate signed by the device itself:

2. Click the Custom certificate signed by Firebox option.
3. In the Common Name text box, type successfulco. You should enter a value that reflects your Firebox such as the domain name part of the URL.
4. In the Organization Name text box, type Successful Company, Inc. In the Organization Unit text box, type Corporate Headquarters. You should enter a value that helps the user verify that the certificate originates with your organization.
5. Click OK. The Web Server Certificate closes.
6. Save the configuration file to the Firebox. The certificate is not created until you save the configuration file to the Firebox.
7. Save the configuration file as Authentication-Done.
Related Courseware and Information

You can use these resources for more information on how to work with authentication services.

**WatchGuard® System Manager User Guide**

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/)

**WatchGuard LiveSecurity® Alerts & Advice**
Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. Which of the statements below are a reason to use user authentication (select all that apply):
   - A) Monitor users who connect through your network
   - B) Restrict who can connect to resources on the Internet
   - C) Block incoming connections from specific Web sites
   - D) Identify connections in monitoring tools by IP address
   - E) Reduce the total number of public IP addresses you need
   - F) Prevent unauthorized users from accessing network resources
   - G) All of the above

2. True or False: Fireware appliance software supports Windows NT authentication.

3. True or False: You can configure a policy to allow a single user.

4. Which of the authentication types below is compatible with Fireware appliance software:
   - A) Kerberos
   - B) SecurID
   - C) Linux Authentication
   - D) AppleTalk Authorization
   - E) Windows NT
   - F) Lightweight Directory Access Protocol
   - G) Active Directory
   - H) Firebox Users and Groups
   - I) RADIUS
   - J) Single Sign-On agents

5. Which of the following is the URL for the Firebox Authentication web page:
   - A) https://auth.watchguard.com:4100/
   - B) http://ip address of Firebox interface:411/
   - C) https://gateway IP address of Firebox:4000/
   - D) http://ip address of the Firebox interface:4100/
ANSWERS
1. A, B, C, H, I, J
2. False
3. True
5. D
Firewall Basics
Student Guide

Policies

Converting Network Policy to Firebox Configuration

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak / Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Category</td>
<td>Policies</td>
</tr>
</tbody>
</table>

What You Will Learn

A Firebox® controls traffic to and from your trusted, optional, and external networks. You define what should be allowed and what should be denied through a set of rules known as policies. In this training module, you are shown how to:

- Understand the difference between a packet filter policy and a proxy policy
- Add a policy to Policy Manager and configure its access rules
- Create a custom packet filter
- Set up logging and notification rules for a policy
- Use advanced policy properties
- Understand how the Firebox determines precedence

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

Policies are Rules for Your Network Traffic

When you add a policy to the Policy Manager, you add rules to tell the Firebox® what types of traffic to allow or deny through the firewall. You can set the rule to allow or deny traffic based upon factors such as source and destination of the packet, the TCP/IP port or protocol used in the packet, or the time of day. You can use the same rule to give the Firebox more instructions on how to handle the packet. For example, you can define logging and notification parameters for the rule or use network address translation (NAT).

There are two types of policies:

Packet Filter Policy
A packet filter examines each packet’s IP header to control the network traffic into and out of your network. It is the most basic feature of a firewall. If the packet header information is valid, then the firewall allows the packet. If the packet header information is not valid, the firewall drops the packet.

Proxy Policy
A proxy monitors and scans whole connections. It examines the commands used in the connection to make sure they are in the correct syntax and order. It also uses deep packet inspection to make sure that connections are secure. A proxy operates at the application layer, as well as the network and transport layers of a TCP/IP packet, while a packet filter operates only at the network and transport protocol layers.

Proxies can prevent potential threats from reaching your network without blocking the entire
connection. The Firebox includes default rulesets for each proxy policy available in the Firebox configuration. These default rulesets can be used without changing them, or, you can customize the rulesets to meet your business needs.

**Adding policies**

Policy Manager uses icons or a list view to show the policies that you configure for your Firebox. For each policy you:

- Enable the policy
- Set the allowed traffic source and destination for the policy
- Configure properties such as logging, notification, and any advanced properties (described below)

The Firebox includes a default list of predefined packet filter and proxy policies for your use. You can add one of these policies and then set your own policy properties. Based upon the access rules you configure, connections can be allowed, denied, or denied with a reset and sent back to the client. You can either keep the default ruleset or modify it based on your Successful Company’s requirements.

To allow access through the Firebox for an Internet protocol that is not included in the list of predefined policies, you must create a custom policy template. A custom policy includes ports and/or protocols that specify one type of network traffic. This covers any Internet protocol and TCP or UDP protocols that use ports.

**Configuring logging and notification for a policy**

With WatchGuard® System Manager, you can create custom logging and notification rules for each policy. These rules tell the Firebox the events for which it needs to create log messages that trigger a notification message. Notification can occur through email, a pop-up window on the WatchGuard management station, or with a Simple Network Management Protocol (SNMP) trap. An SNMP trap is a notification event issued by a managed device to the network SNMP manager when a significant event occurs.

**Advanced policy properties**

You can use several advanced property settings for your policies:

**Proxy Actions**

Each time you add a proxy policy to Policy Manager, you can use separate sets of rules for clients and servers—to protect both your trusted users and your public servers. You can use these rulesets unchanged or you can modify them to meet the needs of your organization.

**Schedules**

You can set an operating schedule for any policy in Policy Manager. You can create schedule templates to use the same schedule in more than one policy, or you can create a custom schedule for any policy.

**Traffic Management**

If you use Fireware® Pro, you can assign a Traffic Management action to any policy. A Traffic Management action can guarantee that a particular policy always has certain amount of bandwidth through the Firebox or it can limit the amount of traffic a policy can request.

**Quality of Service (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. QoS marking for a policy marks traffic that uses the policy, and is available for Fireware Pro users.

**Network Address Translation (NAT)**

You can enable or selectively disable 1-to-1 and dynamic NAT in any policy. You can also configure incoming NAT properties to allow Internet connections to privately addressed servers protected by the Firebox. For more information, see the “NAT” training module.
ICMP Error Handling
You can customize the method the Firebox uses to handle ICMP errors for each policy.

Custom Idle Timeout
You can customize the idle timeout for each policy.

Sticky Connections
A sticky connection is a connection that continues to use the same interface for a defined period of time when your Firebox is configured with multiple WAN interfaces. Stickiness makes sure that, if a packet goes out through one external interface, any future packets between the source and destination address pair use the same external interface for a specified period of time.

Policy-based Routing
If your Firebox is configured with multi-WAN, you can configure a policy with a specific external interface to use for all outbound traffic that matches that policy.

TCP-UDP policies
There are three policies that control all TCP-UDP traffic. It is very important to understand the differences between them:

Outgoing packet filter
The Outgoing packet filter allows all outbound TCP and UDP connections through the Firebox. This is done so that users behind a new Firebox are not cut off from the Internet when the Firebox is placed in their network and before their administrator adds policies for each type of allowed access through the Firebox. The Outgoing policy is added automatically when you create a new configuration file with the Policy Manager. It is not added by the Quick Setup Wizard.

TCP-UDP packet filter
If you decide to remove the Outgoing policy, you must add a policy for any type of traffic you want to allow through the Firebox. If you remove the Outgoing policy and then decide you want to allow all TCP and UDP connections through the Firebox again, you must add the TCP-UDP packet filter to provide the same function. This is because the Outgoing policy does not appear in the list of standard policies available from Policy Manager.

TCP-UDP proxy
The TCP-UDP proxy is used to enable TCP and UDP protocols for outgoing traffic. It also applies proxy rules to traffic on non-standard ports for these protocols: HTTP, HTTPS, SIP, TCP, UDP, and FTP. One very useful feature of this proxy is that it enables you to block IM and P2P applications on non-standard ports.

Policy precedence
Precedence is the sequence in which the Firebox examines network traffic and applies a policy rule. The Firebox routes the traffic using the rules for the first policy that the traffic matches. Fireware Policy Manager automatically sorts policies from the most specific to the most general. You can also set the precedence manually.

When traffic is passed through the firewall, each policy is compared for a match beginning with the policy whose order is listed first until there is a match. If no user-defined policy matches, traffic is denied as an unhandled packet.

Automatic order
Unless you manually set precedence, Policy Manager gives the highest precedence to the most specific policies and the lowest to the least specific. Policy Manager examines specificity of the following criteria in this order. If it cannot determine the precedence from the first criterion, it moves to the second, and so on.

To set the precedence, Policy Manager applies these criteria in order:

1. The policy itself. For example, an Any policy is less specific than policies that allow only specific traffic.
2. Protocols set for the policy type. For example, a policy that specifies many ports for a given protocol is less specific than a policy with fewer ports.

3. Traffic rules of the To field. Most specific to least specific are: rules specifying IP address ranges, users, groups, interfaces.

4. Traffic rules of the From field. Most specific to least specific are: rules specifying IP address ranges, users, groups, interfaces.

5. Firewall action applied to the policies. Most specific to least specific is: Denied or Denied (send reset), Allowed (proxied policy), Allowed (packet filter policy)

6. Schedules applied to the policies. Most to least specific is: Always off, Sometimes on, Always on, no schedule applied to policy (always on).

7. Alphanumeric sequence based on policy type.

8. Alphanumeric sequence based on policy name.

**Comparing To and From fields**

Given a set of traffic specifications, the least specific entry is compared to the least specific entry of the policy. The more specific entry between the two is considered the more specific policy. For example, compare these two policies:

- HTTP-1 From: Trusted, user1
- HTTP-2 From: 10.0.0.1, Any-Trusted

Trusted is the least specific entry in HTTP-1 and Any-Trusted is the least specific entry in HTTP-2. Because Trusted is within Any-Trusted, HTTP-1 is considered more specific even though the other policy contains an IP address. If the two policies are still considered equal, the firewall action is compared. To make the 10.0.0.1 rule most specific, create a third HTTP policy.

**Comparing names**

- If the two policies are considered equal, the protocol name is compared alphabetically
- If the policy names are identical, the policy names are compared alphabetically

**Exercise 1: Add a Packet Filter Policy and Configure Its Access**

Successful Company’s network administrator was told to stop employees from using Internet Relay Chat (IRC) at the office. The management team decided that IRC is too distracting for employees and a potential security risk.

The administrator also wants to activate a Windows terminal services connection to the Successful Company public web server on the optional interface of the Firebox. He routinely administers the web server with a Remote Desktop connection. At the same time, he wants to make sure that no other network users can use the Remote Desktop Protocol terminal services through the Firebox.

In this exercise, you open a basic Firebox configuration file in Policy Manager. You add two predefined policies to the configuration and configure the access rule for each policy.

**Add a pre-defined policy**

First, we must add policies to the Firebox to control IRC and RDP traffic.

1. From Policy Manager, open the configuration file you are editing for these exercises.

2. Select **Edit > Add Policies**.
   - The Add Policies dialog box appears. From here, you can select to add a predefined packet filter policy, a proxy policy, or a custom policy you have created. You can also create a new policy.
3. Expand the **Packet Filter** list. Select **IRC**.

4. Click **Add**. Click **OK**.
This adds a base IRC policy to your configuration. If you do not change this policy, it allows all IRC traffic from any trusted computer to any external computer.

5. Scroll down further through the list of predefined packet filter policies and select **RDP**. Click **Add**. Click **OK**.
This adds a base RDP policy to your configuration. If you do not change this policy, it allows all RDP traffic from any trusted computer to any external computer.

6. Click **Close** to close the **Add Policies** dialog box.
The IRC and RDP policies appear in the list displayed by the Policy Manager.

---

**Use a policy to restrict traffic**

By default, a new policy allows traffic from any trusted interface to any external interface. Now, we modify the policy to block all IRC traffic originating from computers on the Successful Company’s trusted and optional networks.

1. To configure the access rules for the IRC policy, double-click the **IRC** icon.
   The Edit Policy Properties dialog box appears.
2. On the **Policy** tab, use the **IRC connections are** drop-down list to select **Denied**.
   At this point, the rule denies traffic from any computer that connects through the trusted Firebox interface to any external computer.
3. To further restrict IRC traffic, you must also deny IRC from any computer on any optional Firebox interface. To add this, click **Add** below the **From** list.
   The Add Address dialog box appears.
4. Select **Any-Optional** from the list and click **Add**. Click **OK**. The rule now denies IRC traffic from all computers behind the Firebox to any external computer. Traffic that comes from the external interface is always denied by default unless you create a rule to allow it.

![Edit Policy Properties dialog box](image)

5. Click **OK** to close the **Edit Policy Properties** dialog box.

Notice that the policy is now marked with a red X in the list view or a red top banner in the large icon view. This indicates a deny policy.

![Policy icon](image)

**Use a policy to allow traffic**

We also want to allow RDP traffic to the Successful Company web server on the optional network. However, we want only our network administrator to be able to connect so we will restrict this policy to only the static IP address of his home office computer.

1. From Policy Manager, double-click the **RDP** policy. Select **Any-Trusted** from the **From** list box and click **Remove**.

We started with a policy that allows all RDP traffic from any computer on trusted networks to any computer on an external network.
2. Under the From list, click Add. Click the Add Other button. For this exercise, type 50.51.200.22 as the IP address of the network administrator’s computer. Click OK.

3. Under the To list, click Any-External. Click Remove.

4. Under the From list, click Add. Click Add Other. Type 10.0.2.80. This is the IP address of the Successful Company public web server on the PublicServers (Interface #3) optional network.

5. Click OK.

   The rule now allows RDP connections from the IP address of the network administrator’s desktop computer to the IP address of the public web server.

6. If the Outgoing policy is not present in this configuration, there is no default rule to allow general outgoing TCP connections. All other RDP traffic will be denied. Click OK to close the Edit Policy Properties dialog box.

Exercise 2: Create a Custom Packet Filter Template

Successful Company’s network administrator frequently troubleshoots their public servers from the network server room. These public servers are all connected to the optional interface of the Firebox®. The network administrator would like to be able to use VNC to view the files on his trusted desktop computer. To do this, he must create a custom VNC policy and allow access from any computer on the optional network to his desktop computer on the trusted network (10.0.1.201). To create a custom policy, we must know that VNC uses TCP protocol, and server port 5900. To learn more about the service ports used by different network services, refer to the WSM Reference Guide, “Services and Ports” chapter.

In this exercise, you learn how to create a custom packet filter to solve a problem in the Successful Company network.

Make a new policy template

1. From Policy Manager, select Edit > Add Policy.

2. Click New to create a new policy template.

   The New Policy Template appears.

3. In the Name field, type VNC. In the Description field, type ORL’s Virtual Network Computing.

4. Make sure that the policy type selected is Packet Filter.

5. Click Add to define a protocol and ports for the new policy template.

   The Add Protocol dialog box appears.
6. Make sure that the **Type** field is set to Single Port. Make sure that the **Protocol** is set to TCP. In the **Server Port** field, type 5900.

![Add Protocol](image)

7. Click **OK** to close the **Add Protocol** dialog box. The TCP 5900 protocol appears in the list of Protocols controlled by this policy.

![New Policy Template](image)

8. Click **OK** to close the **New Policy Template** dialog box.

**Add and configure the custom policy**

Now that you have a custom policy template that controls VNC traffic, you can add it to the Firebox configuration.

1. In the **Add Policies** dialog box, expand **Custom Policy**. Click **VNC**. Click **Add**. The New Policy Properties dialog box appears with the VNC packet filter.

2. In the **From** list, select **Any- Trusted**. Click **Remove**. Under the **From** list, click **Add**. Double-click **Any- Optional**. Click **OK**. This procedure enables the Firebox to allow VNC traffic from any computer on an optional network.

3. In the **To** list box, select **Any- External**. Click **Remove**. Under the **To** list, click **Add**. Click **Add Other**. Type 10.0.1.201. This address restricts VNC traffic to only the desktop computer of the network administrator.
4. Click **OK** to close the Add Member dialog box. Click **OK** again to close the Add Address dialog box.

![New Policy Properties dialog box](image)

5. Click **OK** to close the New Policy Properties dialog box. Click **Close** to close the Add Policies dialog box.

   The VNC policy appears in the list of configured policies.

![Policy list](image)

**Exercise 3: Configure Logging and Notification for a Policy**

In this exercise, you make sure the Firebox creates a log record for any IRC connection denied by the IRC policy we created earlier in the lesson.

1. From Policy Manager, double-click the **IRC** policy.
2. Select the **Properties** tab. Click **Logging**.
   The Logging and Notification dialog box appears.

![Logging and Notification dialog box](image)

3. Select the **Send log message** check box and the **Send Notification** check box.
   With these options selected, the Firebox sends a log message to the WatchGuard Log Server each time an IRC packet is denied. Also, when an IRC packet is denied, the Firebox sends a message to the Log Server that tells it to send an email notification to the email address specified in the Log Server Status/Configuration dialog box. For more information, see the “Logging” training module.

![Logging and Notification settings](image)

4. Click OK to close the **Logging and Notification** dialog box. Click OK to close the **Edit Policy Properties** dialog box.

5. Save the configuration file to your local hard drive as **Policies-Configured.xml**.

**Exercise 4: Change Policy Precedence**

When you define a new policy and configure the policy parameters, it is automatically sorted and placed in the proper order within Policy Manager. To illustrate the policy auto-ordering process, add the NetMeeting packet filter and watch for the position in which it is placed.

1. Verify that the Policy Manager is set to the Details view.
   From Policy Manager, select **View > Details**. In this view, policies appear in the order the Firebox will use to process traffic.
2. From Policy Manager, add a NetMeeting policy. Do not change the default properties.
   Reminder: Click Add Policy, Expand Packet Filters. Double-Click NetMeeting. Click OK. Click Close. The Firebox automatically places the NetMeeting policy in the correct position according to its ordering criteria.

Override the default order of policy precedence
You can override the order in which the Firebox automatically puts policies. To change the order of policies:

- Switch to manual-order mode.
- Select the policy whose order you want to change and drag it to its new location.

In this exercise, we reduce the NetMeeting policy so it has lowest precedence:

1. Select View > Auto-order Mode.
   The Auto-order Mode feature is a toggle. When the check appears, Policy Manager sets the precedence. When the check is cleared, Policy Manager uses manual-order mode.
2. Click Yes to confirm that you want to switch from auto-order mode to manual-order mode.
   The policy order numbers are now gray to indicate that you can move them.
3. Drag and drop the NetMeeting policy to the bottom of the list.

Exercise 5: Use Advanced Policy Properties

After a few weeks of blocking all outgoing IRC traffic, the Successful Company managers notice that many of their engineering team are leaving at 5:00pm. A little research into the problem returns the surprising result that the engineers are perfectly willing to work late as long as they can chat on IRC with their friends who are online playing World of Warcraft. Productivity will increase if we schedule the IRC policy let them chat in the evenings.

1. From Policy Manager, double-click the IRC policy.
   The Edit Policy Properties dialog box appears.
2. Click the **Advanced** tab.

3. Next to the **Schedule** drop-down list, click ![Clone Schedule](image). The Clone Schedule dialog box appears.

4. In the **Name** text box, type **Evenings**. In the **Description** text box, type **Turn off the policy in the evenings**.
   You can use this schedule for other policies so you should describe it with the hours blocked or allowed rather than the policy for which you are building it.

5. In the schedule grid, toggle the hours from 5:00pm to 10:00pm, Monday through Friday.

6. Click **OK** to save the schedule and apply it to the IRC policy. Click **OK** again to close the **Edit Policy Properties** dialog box.

7. Save the configuration file as **Policies-Done**.
   You can compare your results with the Policies-Finish file included with the training.
Related Courseware and Information

You can use these resources for more information on how to use policies and proxies:

**WatchGuard System Manager User Guide**
Browse to [https://www.watchguard.com/help/documentation/](https://www.watchguard.com/help/documentation/) and download the WSM User Guide. See the chapter “Policies.”

**Reference Guide**
Browse to [https://www.watchguard.com/help/documentation/](https://www.watchguard.com/help/documentation/) and download the Reference Guide. See the chapter “Services and Ports.”

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/)

Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. Select the box if you can use Policy Manager to configure a policy to do the task listed (select all that apply):

<table>
<thead>
<tr>
<th>Task</th>
<th>Packet Filter</th>
<th>Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examine the header information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strip an attachment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examine the application layer content</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check for RFC compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block based on server command type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check the source against a list of blocked sites</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify that the destination is a valid location on the trusted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send a log message if the packet is malformed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generate a report on network traffic</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. True or False: The default configuration automatically includes a policy that enables the TCP/UDP outgoing proxy.

3. List the order in which these comparisons are made by the Firebox to determine precedence by placing the correct number next to the item (use numbers 1-7):

   A) ______  Schedule
   B) ______  Sources in the To field
   C) ______  Firewall action
   D) ______  Alphabetically based on protocol name
   E) ______  Policy type
   F) ______  Sources in the From field
   G) ______  Alphabetically based upon policy name

4. True or False: Policies are ordered based upon a series of comparisons and scores.

5. True or False: Given a set of sources, the least specific entry is compared to the least specific entry of the policy to which it is compared.
ANSWERS

1. | Filter | Proxy |
---|---|---|
Examine the header information | ☑ | ☑ |
Strip an attachment | ☐ | ☑ |
Examine the application layer content | ☐ | ☑ |
Check for RFC compliance | ☐ | ☑ |
Block based on server command type | ☐ | ☑ |
Check the source against a list of blocked sites | ☑ | ☑ |
Verify that the destination is a real location on the trusted | ☑ | ☑ |
Send a log message if the packet is malformed | ☑ | ☑ |
Generate a report on network traffic | ☐ | ☐ |

2. False
3. A-5 B-2 C-4 D-6 E-1 F-3 G-7
4. True
5. True
FTP Proxy

Configuring the FTP Proxy

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak / Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>FTP Proxy</td>
</tr>
</tbody>
</table>

What You Will Learn

In the “Policies” training module, we learned that WatchGuard® System Manager includes two types of policies: packet filters and proxies. We then learned how to add and configure a packet filter policy as well as create a custom policy. In this training module, we explore proxy configuration with the FTP proxy as an example. In this training module, you are shown how to:

- Prevent users from putting files on an external FTP server
- Prevent any user from deleting files on a local server
- Restrict file downloads by type
- Set up notification for denied connections
- Restrict uploads by file type

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

What is a Proxy Policy?

Policy Manager includes ten proxies. Each is capable of all the same features as an equivalent packet filter. In addition, each can examine the traffic for that protocol in considerably greater depth. A proxy monitors and scans whole connections. It examines the commands used in the connection to make sure they are in the correct syntax and order. It also uses deep packet inspection to make sure that connections are secure.

A proxy operates at the application layer, as well as the network and transport layers of a TCP/IP packet, while a packet filter operates only at the network and transport protocol layers.

Proxies can prevent potential threats from reaching your network without blocking the entire connection. The Firebox® includes default rulesets for each proxy policy available in the Firebox configuration. These default rulesets can be used without changing them, or, you can customize the rulesets to meet your business needs.

Proxy Actions

A proxy action is a set of rules that control how the Firebox applies a proxy to control traffic of a particular type. Policy Manager includes at least one proxy action ruleset for each proxy. Many proxies, such as FTP, include both a client and a server proxy action. You can either use the default rulesets provided or customize the proxy action.

When you modify the settings of a proxy action, such as changing the types of file downloads that are allowed, Policy Manager creates a new proxy action based on the proxy action you modified and keeps the
original proxy action and its default settings unmodified. For example, modified FTP-Client proxy action would create an ‘FTP-Client.1’ proxy that could be applied to other FTP policies in the future. The original proxy action is always available, since it is never actually changed when these new actions are ‘cloned’.

You can also import proxy actions, rulesets, WebBlocker exceptions, and spamBlocker exceptions. This significantly reduces setup time when you have multiple policies or multiple Fireboxes.

Proxies and the Quick Setup Wizard
The Quick Setup Wizard does not include any proxy policies by default. Because no proxies are used by the Firebox by default, there are no default restrictions on the types of files that users can download from the Internet or the types of files they can upload. To add these types of restrictions to the Firebox configuration, proxy policies must be added to the Firebox configuration.

Control File Transfers In and Out of Your Network
WatchGuard® System Manager includes an FTP packet filter and an FTP proxy. The FTP packet filter can handle both active and passive FTP sessions without any special client configuration. In active mode FTP, the FTP server establishes the data connection. In passive mode, the client establishes the connection. In general, and by default, FTP user agents use active mode and web user agents use passive mode.

Like the FTP packet filter, the FTP proxy handles active and passive FTP sessions, but it also protects your FTP server and restricts FTP protocol commands between clients and servers. You can use the FTP proxy to:

- Restrict the commands sent on the control channel by file name or the type of file based on file-name extension
- Protect against buffer overflow attacks caused by the abuse of the FTP protocol
- Prevent unauthorized directory traversal through unusual use of FTP commands with the WatchGuard Intrusion Prevention Service

When you add an FTP proxy policy to your Firebox® configuration, you get access to two proxy actions. You can use the default rulesets included with these proxy actions, or you can use the rulesets as a base for a proxy action to meet the needs of your organization. This module shows you how to customize these two proxy actions.

FTP-Client
This proxy action includes rulesets to control FTP commands sent from computers protected by your Firebox. FTP client applications use specific commands that the Firebox can identify and control. Use the FTP-Client proxy action to control outbound FTP traffic.
FTP-Server

This proxy action controls inbound FTP connections to an FTP server protected by your Firebox. The default configuration includes rules that prevent commands and actions that frequently indicate an attack on your FTP server.

FTP Proxy Rulesets

The FTP proxy action has six default rulesets. These rulesets are shown in the Category list to the left of the FTP Proxy Configuration dialog box.

General

These rules control basic FTP parameters such as maximum user name length.

Commands

You can configure rules to put limits on some FTP commands. Use the FTP-Server proxy action to put limits on commands that can be used on an FTP server protected by the Firebox. Use the FTP-Client proxy action to put limits on commands that users protected by the Firebox can use when they connect to external FTP servers. The default configuration of the FTP-Client is to allow all FTP commands.

You generally should not block these commands, because they are necessary for the FTP protocol to work correctly.

<table>
<thead>
<tr>
<th>Protocol Command</th>
<th>Client Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER</td>
<td>n/a</td>
<td>Sent with login name</td>
</tr>
<tr>
<td>PASS</td>
<td>n/a</td>
<td>Sent with password</td>
</tr>
<tr>
<td>PASV</td>
<td>pasv</td>
<td>Select passive mode for data transfer</td>
</tr>
<tr>
<td>SYST</td>
<td>syst</td>
<td>Print the server’s operating system and version. FTP clients use this information to correctly interpret and show a display of server responses.</td>
</tr>
</tbody>
</table>

Users can block other commands depending upon their needs.

<table>
<thead>
<tr>
<th>Protocol Command</th>
<th>Client Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RETR</td>
<td>get</td>
<td>Retrieve a file from the server</td>
</tr>
<tr>
<td>STOR</td>
<td>put</td>
<td>Put a file on the server</td>
</tr>
<tr>
<td>DELE</td>
<td>delete</td>
<td>Delete a file on the server</td>
</tr>
<tr>
<td>RMD</td>
<td>rmdir</td>
<td>Delete a directory on the server</td>
</tr>
<tr>
<td>MDK</td>
<td>mkdir</td>
<td>Create a directory on the server</td>
</tr>
<tr>
<td>PWD</td>
<td>pwd</td>
<td>Print the Present Working Directory (PWD) path</td>
</tr>
<tr>
<td>LIST</td>
<td>ls</td>
<td>List the names in the current directory path</td>
</tr>
</tbody>
</table>
Download
The Download ruleset controls the file names, extensions, or URL paths that users can use FTP to download. Use the FTP-Server proxy action to control download rules for an FTP server protected by the Firebox. Use the FTP-Client proxy action to set download rules for users connecting to external FTP servers.

Upload
The Upload ruleset controls the file names, extensions, or URL paths that users can use FTP to upload. Use the FTP-Server proxy action to control upload rules for an FTP server protected by the Firebox. Use the FTP-Client proxy action to set upload rules for users connecting to external FTP servers. The default configuration of the FTP-Client is to allow all files to be uploaded.

Antivirus
If you have purchased and enabled the Gateway AntiVirus feature, the fields in the AntiVirus category set the actions necessary if a virus is found in a file that is uploaded or downloaded. For more information, see the “Signature Services” training module.

Intrusion Prevention
You can use the Intrusion Prevention Service (IPS) to monitor the FTP control channel to look for signatures that match those in the IPS database. This option is available when you purchase a license for the optional Intrusion Prevention Service.

Proxy and AV Alarm
An alarm is a mechanism to tell a network administrator when network traffic matches criteria for suspicious traffic or content. When an alarm event occurs, the Firebox does an action that you configure. For example, you can set a threshold value for file length. If the file is larger than the threshold value, the Firebox can send a log message to the Log Server.

Exercise 1: Configure an FTP-Client Proxy Action
Successful Company would like to restrict the FTP usage of its employees. Specifically, the network administrator must:

- Prevent Successful Company users from using FTP to transfer files from the company’s network to an external FTP server.
- Allow the FTP download of zipped files by Successful Company employees, but deny the FTP download of Windows screen savers with a .scr extension. These have been used as virus or trojan vectors.
- Make sure that any time an FTP connection is denied by any of the rules, an email notification is sent to the network administrator.

Add the FTP Proxy
To configure the Firebox® to restrict the FTP traffic of Successful Company in the ways described, we must first add the FTP Proxy.

1. From Policy Manager, open the configuration file you are editing for these exercises.
2. Click the plus (+) sign on the Policy Manager toolbar to open the **Policies** dialog box. You can also select Edit > Add Policy.

![FTP Proxy Configuration](image)

3. Expand the **Proxies** folder. Click FTP-proxy to select it. Click **Add**. The New Policy Properties dialog box appears.

4. In the **Name** text box, type FTP-Proxy-Client. The Name identifies the policy in your policy list.

5. Select the **Properties** tab. Make sure that FTP-Client is the selected proxy action.

![New Policy Properties](image)

6. Click ![FTP Proxy Configuration](image). The FTP Proxy Configuration dialog box appears for the FTP-Client action.

**Deny the FTP STOR command**
The STOR command controls whether a user can move a file from a client computer to an FTP server. In this exercise, we prevent Successful Company employees from copying files to an FTP server on the external network.

1. From the **FTP Proxy Configuration** dialog box, select **Commands**.

2. In the **Pattern** text box, type **STOR**. Click **Add**.

   As shown in the table in “FTP Proxy Rulesets” on page 111, the command to put files on a server is STOR. The client command is PUT.

3. Below **Actions to Take**, use the **If matched** drop-down list to select **Deny**. This rule tells the Firebox to deny any FTP command connection originated on the FTP client that includes the STOR command.
4. Select the check boxes adjacent to **Alarm** and **Log**. This tells the Firebox to send a notification each time an FTP client tries to use the STOR command that is denied by the Firebox. At the same time, the Firebox also sends a log message about the denied event to the Log Server.

**Control FTP downloads by file extension**

The FTP proxy examines packets for the file extensions it is configured to deny. It does not confirm that the file sent has the correct file extension. For example, a hacker could put a file on an FTP server and change the file extension from *.scr to *.txt. The Firebox would allow this file transfer. When you add the asterisk wildcard at the end of the pattern, the Firebox blocks the most common change, which is to add “.txt” to a file name.

Per the Successful Company policy, employees are allowed to download ZIP files but they must not download any SCR (screensaver theme) file as these are known vectors for trojans and viruses.

1. From the **Categories** list, select **Download**. A list appears of the file extensions that the Firebox denies in the default FTP proxy configuration.
2. Select *.zip. Click **Remove**. Click **Yes**. The action defined by this rule tells the Firebox to deny all files that match the strings in the list. By removing the *.zip entry, this rule now allows files with a “.zip” extension.
3. In the **Pattern** text box, type *.scr. Click **Add**. Wildcard pattern matches are not case sensitive.
4. Select *.scr. Make sure that under Actions to Take, the If matched value is set to Deny.

Enable alarms for denied connections from FTP clients
To meet Successful Company objectives, you also need to make sure that an alarm is sent any time an FTP connection is denied because of the rules you created above.

1. Earlier in this exercise, you selected the Alarm and the Log check boxes for the STOR command. Repeat the steps for the extension *.scr.
2. From the Categories list, select Proxy and AV Alarm. Select the Send Notification check box. Make sure that the E-mail option is selected.
In Fireware v9.1 and higher, you can export custom proxy configurations from one configuration to an XML file, and then import the ruleset to another Firebox configuration file. You can see the Import and Export functions when you look at a proxy ruleset in the Advanced view.

3. Click **OK** to close the **FTP Proxy Configuration** dialog box. Because FTP-Client is a template, you cannot change it. You can only make a copy and use it for your policies.

4. Click **OK** to clone the template. The default name for a clone is FTP-Client1. You can also give it a friendly name to help you recognize it. The Edit Policy Properties dialog box appears. The proxy action selected is FTP-Client1.

5. Click **OK** to close the **New Policy Properties** dialog box. Click **Close** to close the **Add Policies** dialog box.

**Exercise 2: Configure an FTP-Server Proxy Action**

In this exercise, you edit the predefined FTP-Server ruleset to restrict the types of FTP connections to the Successful Company FTP server. Specifically, you will:

- Make sure that no user connecting to the Successful FTP server is able to delete a file on the server.
- Restrict the type of files that users can upload to the FTP server to text files only, to help prevent abuse of the Successful Company FTP server as a warez repository.

**Deny the Delete command**

In this section, you prevent a user from deleting a file on the FTP server.

1. From Policy Manager, click +.
2. Click the plus (+) sign on the left side of the folder to expand the Proxies folder. Click FTP-proxy to select it. Click Add.
3. In the Name text box, type FTP-Proxy-Server.
4. Click the Properties tab. Use the Proxy action drop-down list to select FTP-Server. Click 
5. From the Categories list, select Commands.
   The table in “FTP Proxy Rulesets” on page 111 shows that the command to delete files from a server is DELE. The DELE* command appears in the rules list in the FTP-Server template, and the default configuration allows connection.
6. In the **Rules** list, select **DELE***. Click **Change View**.
   In the Advanced View, you can change command order as well as add, remove, enable, and disable individual commands.

   ![FTP Proxy Action Configuration](image)

   The default FTP-Server proxy action template denies any FTP command to the server that is not on the list. In other words, most commands to your FTP server will not operate. This is a strong security policy that allows only the minimum number of commands needed to meet your business requirements.

7. Clear the check box adjacent to **Allow DELE***. Click **Edit**.
   The Edit Command Rules dialog box appears for the Rule Name **DELE***.

8. Below **Rule Actions**, use the **Action** drop-down list to select **Deny**.

   ![Edit Command Rules](image)

9. Click **OK** to close the Edit Commands Rule dialog box. Select the check box adjacent to **Deny DELE*** to enable the rule.
   This rule tells the Firebox to deny any FTP connections that try to delete a file from the FTP server.

   ![Rule Settings](image)
Restrict FTP File uploads to text only

In this section, you allow a user to save a text file to the Successful Company FTP server.

1. From the **Categories** list, select **Upload**.
2. In the **Pattern** text box, type *\.txt*. Click **Add**.
3. In the **Actions to Take** section, use the **If Matched** drop-down list to select **Allow**.
   This tells the Firebox to allow the upload of files with the *\.txt* file extension to the FTP server.

4. Click **OK** to close the **FTP Proxy Configuration** dialog box.
   Because FTP-Server is a template, you cannot change it. You can make a copy and use it for your policies.
5. Click **OK** to clone the template.
   The default name for a clone is FTP-Server.1. You can also give it a friendly name to help you recognize it. The Edit Policy Properties dialog box appears. The Proxy action selected is FTP-Server.1.
6. Click **OK** to close the **New Policy Properties** dialog box. Click **Close** to close the **Add Policies** dialog box.
7. Save the configuration file as **FTPProxy-Done**.
   You can compare your results with the FTPProxy-Finish file included with the training.

**Frequently Asked Questions**

**Can I get a report of FTP traffic on my Firebox?**
Yes. On the tab for the **General** category, select the **Turn on logging for Reports** check box. The Firebox creates a log message for each FTP transaction. You can use WatchGuard Reports to get detailed reports on FTP traffic.

**Related Courseware and Information**

You can use these resources for more information on how to work with the FTP proxy.

**WatchGuard® System Manager User Guide**
Browse to [https://www.watchguard.com/help/documentation/](https://www.watchguard.com/help/documentation/) and download the **WSM User Guide**. See the chapters “Proxies” and “Signature-Based Security Services.”

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/)
Request for Comments (RFC) 959
Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. True or False: You must use the FTP proxy if you want to use the File Transfer Protocol through the Firebox. The FTP packet filter does not handle active mode.

2. Fill in the blanks: A _____________ examines the commands used in a connection to make sure they are in the correct syntax and order. A ______________ examines only the packet IP header information.

3. Select the best pattern match to block FTP upload of Microsoft Excel spreadsheets:
   ○ A) *.xls
   ○ B) *XLS
   ○ D) secure_file.*Is
   ○ E) All of the above

Use the information in this screen capture to answer the next two questions.

4. True or False: If an FTP server is protected with an FTP proxy server ruleset with this configuration, an FTP client will be able to log in to this FTP server.
5. Which of these FTP client commands can be successfully used, based on the commands shown in the image above?
   - A) site
   - B) dir
   - C) help
   - D) syst
   - E) pasv
   - F) bin
   - G) get
   - H) None of the above
   - I) All of the above

6. Fill in the blank: To control access to an FTP server on your optional network, start with the ____________ proxy action.

ANSWERS

1. False — Both the FTP packet filter and the FTP proxy can handle active mode FTP.

2. True — The necessary FTP protocol commands USER and PASS are allowed and will allow authentication.

3. A)

4. proxy, packet filter

5. FTP-Server

6. B, D, G
Email Proxies

Working with the SMTP and POP3 Proxies

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak /Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Email Proxies</td>
</tr>
</tbody>
</table>

What You Will Learn

The Firebox® uses two proxies to control email traffic: SMTP and POP3. In this training module, you are shown how to:

- Restrict the types of connections to an SMTP server
- Modify the allowable message size
- Allow and deny different content types and filenames
- Restrict email by attachment filename
- Restrict incoming SMTP traffic by domain
- Restrict outgoing POP3 traffic and lock attachments

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

Control the Flow of Email In and Out of Your Network

WatchGuard® System Manager includes two proxies that control the flow of email through the Firebox®: SMTP (Simple Mail Transfer Protocol) and POP3 (Post Office Protocol). There are significant differences between the two protocols, which make most organizations rely on either one or the other rather than having both in the same network. In addition to how the Firebox handles the two protocols, the proxies differ as well in that you can deny or quarantine SMTP messages. With POP3, you can only strip or lock attachments but not stop the delivery of a message. This makes it slightly less secure than the SMTP proxy.

SMTP Rulesets

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.

The SMTP proxy checks the message for harmful content and RFC compliance. It examines the SMTP headers, message recipients, senders, and content as well as any attachments. The proxy can restrict traffic from specific user names or domains. It can also strip unwanted or dangerous SMTP headers, filter attachments by filename and MIME content type, or deny based upon address pattern. The ability to strip header information is particularly valuable to many network administrators. The SMTP proxy is transparent to your end users and mail server. No configuration is necessary in the email clients.

When you add an SMTP proxy policy to your Firebox configuration, you get access to two proxy actions.
**SMTP-Incoming**

This proxy action includes rulesets to protect your SMTP email server.

**SMTP-Outgoing**

This proxy action includes rulesets to control outgoing SMTP connections from users on your trusted and optional networks.

You can use the SMTP proxy policy without changing the ruleset or you can use the default as a base for a ruleset to match the needs of your organization. In this module, we will show you how to modify both the incoming and outgoing rulesets.

**POP3 Rulesets**

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 on 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.

When you add a POP3 proxy policy to your Firebox configuration, you get access to two proxy actions.

**POP3-Server**

This proxy action includes rulesets to protect your POP3 email server.

**POP3-Client**

This proxy action includes rulesets to control outgoing POP3 connections from users on your trusted and optional networks to public POP3 servers.

You can use the POP3 proxy policy without changing the ruleset or you can use the default as a base for a ruleset to match the needs of your organization. In this module, we will show you how to modify the client rulesets.

---

**Exercise 3: Use the SMTP Proxy to Protect your Mail Server**

Successful Company is growing. With all the new employees, incoming email is increasingly a potential vector for malware. In this exercise, we configure an incoming SMTP proxy policy to protect their SMTP server.

**Add an incoming SMTP proxy policy**

In “Configure Static NAT to Protect Public Servers” in the NAT training module, we added an incoming SMTP proxy policy so that we could use network address translation (NAT) to protect the Successful Company SMTP server. If you did not complete that exercise, however, you may need to add an SMTP incoming proxy policy.

1. From Policy Manager, open the configuration file you are editing for these exercises.

2. Click .
   
   You can also select Edit > Add Policy. The Add Policies dialog box appears.

3. Expand the Proxies folder. Click SMTP-proxy and click Add.
   
   The New Policy Properties dialog box appears.

4. Under the To list, click Add. Click Add Other. Type 10.0.1.25 as the IP address of the Successful Company SMTP server on the trusted network. Click OK. Click OK again. Click Close.

**Edit an existing SMTP proxy policy**

If you would like to use the policy created in the “NAT” training module, then you need to edit a policy.

1. From Policy Manager, double-click the SMTP-proxy policy.
2. In the Name text box, type SMTP-Incoming-Proxy.
3. Select the Properties tab. Use the Proxy action drop-down box to select SMTP-Incoming.

4. Click .
   The SMTP Proxy Action Configuration dialog box appears.
5. In the Description text box, type Modified policy for email inbound.

Decrease maximum message size
The default maximum email message size is 10 MB. In the past, employees used email to exchange files with outside vendors. Now that Successful Company has a protected FTP server, the network administrator wants to discourage using the email server for large attachments. So, in this exercise we will reduce the maximum email size to 5 MB (5,000 kilobytes).

1. From the SMTP Proxy Action dialog box under the Categories list, select General > General Settings.
2. Find the Limits section. In the Set the maximum email size value box, type 5000.

Allow and deny content types and filenames
Successful Company employees complain that they cannot receive certain email attachments they need to do their jobs. By default, the SMTP incoming proxy is highly secure and allows very few types of email attachments. Because the network administrator does not have a comprehensive list of the MIME types that his organization’s employees use on a regular basis, he decides to turn content type filtering off but continue to filter email attachments by filename. He can do this until he understands better what content types are used. He understands this is a temporary reduction in security, but he accepts the business risk.

At the same time, the Successful Company network administrator realizes that it is very important to carefully restrict email attachments by filename. He accepted the default list of filenames denied by the SMTP-Incoming ruleset. Now he must make two changes to meet the needs of his organization. He must configure the Firebox® to allow Microsoft® Access database files to go through the SMTP proxy. He must also configure the Firebox to deny Apple® iTunes® MP4 files because of a recent vulnerability announced by Apple.

1. From the SMTP-Incoming Categories list, select Attachments > Content Types.
2. In the **Actions to take** section, use the **None Matched** drop-down list to select **Allow**. This allows all content types through Firebox to the SMTP server. After Successful Company is able to add in the specific content types they want to allow, they set this parameter to strip content type that does not match their list of allowed content types.

![Image of SMTP Proxy Action Configuration]

3. From the SMTP-Incoming **Categories** list, select **Attachments > Filenames**.

4. The filename extension for Microsoft Access databases is “.mdb”. In the list of filenames, find and select .mdb. Click **Remove**. Click **Yes** to confirm.
   If no rules match, the **Action to take** option is set to allow the attachment. In this example, MS Access files are now allowed through the Firebox.

5. In the **Pattern** text box, type ".mp4". Click **Add**. This rule configures the Firebox to deny all files with the Apple iTunes "mp4" file extension bound for the SMTP server.

**Control mail domain usage for incoming traffic**

Another way to protect your SMTP server is to restrict incoming traffic to only messages that use your company domain. In this example, we use the mywatchguard.com domain. You can use your own company domain.

1. From the SMTP-Incoming **Categories** list, select **Address > Rcpt To**.
2. In the Pattern text box, type *.mywatchguard.com. Click Add.
This denies any email messages with a Rcpt To address that does not match the company domain.

3. Click OK to close the SMTP Proxy Action Configuration dialog box.
Because SMTP-Incoming is a template, you cannot change it. You can only make a copy and use it for your policies.

4. Click OK to clone the template.
The default name for a clone is SMTP-proxy.1.

5. Click OK to close the Edit Policy Properties dialog box. Click Yes to confirm.
The SMTP-Incoming-Proxy policy appears in your policy list.

Exercise 4: Control Outgoing SMTP Connections

A network administrator at Successful Company has looked over the default rulesets that are included with the SMTP-Outgoing proxy action and wants to make these three changes:

- Remove the restriction on email size
- Make sure that all outgoing email is from the Successful Company domain
- Prevent users from sending email with Microsoft® Windows screensavers attached

Add an outgoing SMTP proxy policy
To configure all outgoing SMTP traffic, the Successful Company first adds an outgoing SMTP proxy policy.

1. From Policy Manager, click .
2. Expand the Proxies folder. Double-click SMTP-proxy.
The New Policy Properties dialog box appears.
3. In the Name text box, type SMTP-Server-Outgoing.
4. Under the From list, click Any-External. Click Remove. Click Add. Click Add Other. Type 10.0.1.25. Click OK. Click OK again.
These actions add the Successful Company SMTP server on the trusted network to the policy.
5. Under the To list, click Add. Double-click Any-External. Click OK.
Now the policy controls all traffic from the SMTP server to any computer on the external networks.
6. Click the **Properties** tab. Use the **Proxy action** drop-down list to select **SMTP-Outgoing**.

**Control email message size**
Successful Company management requests that there be no limit on the size of outgoing email. We will do this using outgoing SMTP rulesets.

1. From the **New Policy Properties** dialog box, click .
2. From the **Categories** list, select **General > General Settings**.
   Notice that the setting changes made for the SMTP incoming proxy due not appear here. This is policy controls only outgoing SMTP traffic.
3. Clear the **Set the maximum e-mail size to** check box.
   This removes any restriction on email size.

![SMTP Proxy Action Configuration (predefined)](image)

**Control mail domain use for outbound SMTP**
Successful Company’s network administrators want to make sure that only mail with a **Mail From** address in their domain is allowed out through the Firebox®. This is one measure that protects their mail server from abuse as a relay.

Another way to keep your server from being used as a relay is to use the **Rewrite As** feature included in this rule configuration dialog box. The Firebox changes the **From** and **To** components of your email address to a different value. This feature is also known as “SMTP masquerading.”

1. From the SMTP-Outgoing **Categories** list, select **Address > Mail From**.
2. In the **Pattern** text box, type `*mywatchguard.com`. Click **Add**.
   This denies any email messages with a **Mail From** address that does not match the company domain.
Restrict email by attachment filename

The Successful Company network administrators are also aware that Windows screensavers are sometimes associated with viruses and have no positive effect on their business. These screensavers, with a filename of “.scr”, are denied by default in the SMTP-Incoming proxy action. To make sure that their users do not accidentally send out a virus-infected email message, and to make sure that no virus forwards infected messages with the SCR filename as an attachment, they want to deny the “.scr” file extension for outgoing email. In addition, they want to make sure they are notified by email if anyone tries to send a Windows screensaver with the “.scr” file extension.

1. From the SMTP-Outgoing proxy action Categories list, select Attachments > Filenames.
2. In the Patterns text box, type *.scr*. Click Add.
   The asterisk at the end of the pattern makes sure that Windows screensavers with a trailing filename extension (such as *scr.txt) are also blocked.
3. In the Actions to take section, use the If Matched drop-down list to select Strip.
   This removes any attachment with “.scr” in the filename extension, but allows the rest of the email through.
4. Adjacent to the If matched drop-down list, select the Alarm check box and the Log check box.

5. From the Categories list, select Proxy and AV Alarms. Select the Send Notification check box and make sure that the Email button is selected.
6. Click **OK** to close the **SMTP Proxy Configuration** dialog box.

7. Click **OK** to clone the template.
   - The default name for a clone is SMTP-Outgoing.1. You can also give it a friendly name to help you recognize it.
   - The Edit Policy Properties dialog box appears.

8. Click **OK** to close the **New Policy Properties** dialog box. Click **Close**.
Exercise 5: Using a POP3 Client Policy

Successful Company network policy is to prohibit connections to all external POP3 servers. Unfortunately, the new CFO insists on downloading his personal mail from Impersonal ISP. He says he absolutely cannot do business without this service, and the CEO concurs though insists that even the CFO cannot get attachments via his POP3 account. In this exercise, we will use the POP3 proxy to open a tiny hole from the CFO to his service provider. While we cannot quarantine his attachments, we can lock them. There is a small hope this will prove so inconvenient, the CFO will switch to SMTP and our Exchange server.

Add a POP3 client policy

1. From Policy Manager, click .
2. Expand the Proxies folder. Double-click POP3-proxy.
   The New Policy Properties dialog box opens.
3. In the Name text box, type POP3-CFO.
   Click OK. Click OK again.
   These actions add the Successful Company CFO's desktop computer on the trusted network to the policy.
5. Under the To list, click Any-External. Click Remove. Click Add. Click Add Other. Use the Choose Type drop-down list to select Host Name (DNS Lookup). In the Value text box, type mail.impersonalips.com.
   Click OK. Click OK again. Policy Manager does a one-time DNS lookup for the host name "mail.impersonalips.com" and you see the IP address it finds in your policy.
   Now the policy controls all traffic from the CFO to the mail servers of Impersonal IPS.

6. Click the Properties tab. Use the Proxy action drop-down list to select POP3-Client.

Configure the POP3 policy to lock attachments

1. From the New Policy Properties dialog box, click .
2. From the Categories list, select Attachments > Content Types.
   Notice that by default Content Type detection is enabled and attachments are allowed.
3. In the **Actions to take** section, use the **If matched** drop-down list to select **Lock**.

   With this setting, the CFO receives locked attachments that match the content types listed. All other attachments are stripped.

4. Click **OK** to close the **POP3 Proxy Action Configuration** dialog box.

   Because POP3-Client is a template, you cannot change it. You can only make a copy and use it for your policies.

5. Click **OK** to clone the template.

   The default name for a clone is POP3-Client1.

6. Click **OK** to close the **New Policy Properties** dialog box. Click **Close** to close the **Add Policies** dialog box.

   The POP3-CFO policy appears in your policy list.

   ![POP3-CFO policy screenshot]

7. Save the configuration file as **EmailProxies-Done**.

   You can compare your results with the EmailProxies-Finish file included with the training.

### Related Courseware and Information

You can use these resources for more information on how to work with the email proxies.

**WatchGuard® System Manager User Guide**

Browse to [http://www.watchguard.com/help/documentation/](http://www.watchguard.com/help/documentation/) and download the **WSM User Guide**. See the chapters “Proxies” and “Signature-Based Security Services.”

**WatchGuard LiveSecurity® Online Resources**

Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/)

**RFC Archives**

To learn more about protocols used for email and controlled by the SMTP and POP3 proxies, browse to:

Test Your Knowledge

Use the questions below to practice what you have learned and exercise new skills.

1. Which of the following can an SMTP proxy check that an SMTP packet filter cannot (select all that apply):
   - [ ] A) Source IP Address
   - [ ] B) Content
   - [ ] C) RFC compliance
   - [ ] D) Packet Header
   - [ ] E) Attachment

Use the screen shot below to answer questions 2 - 4.

2. True or False: The Firebox will deny an email message with a 60-byte address.
3. Fill in the blank: The Firebox will allow up to ____ bytes in an email address before it denies a message.
4. True or False: The Firebox will remove an attachment that is 5 MB.
5. Select which SMTP proxy action would be the most appropriate:

<table>
<thead>
<tr>
<th>Task</th>
<th>SMTP-Incoming</th>
<th>SMTP-Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect your company network from the ILOVEYOU virus</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Reduce the number of very large files sent by email to your users</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Reduce spam</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Prevent your network from being used as a spam relay</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Block pornographic images being sent to your users</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Keep your users from sending MP3s to their friends</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

6. True or False: Many free, public email servers use POP3.

7. True or False: You can use the POP3-Client ruleset to deny an email message received through a POP3 server.
Test Your Knowledge

Email Proxies

ANSWERS

1. B, C, E
2. True
3. 50
4. True - A remove action removes an attachment from a message but allows the message itself. The rule defined in this screenshot makes the Firebox deny any message content that is greater than 4 MB.
5. True
6. True
7. False

Task
- Keep your users from sending MP3s to their friends
- Block pornographic images being sent to your users
- Prevent your network from being used as a spam relay
- Reduce spam
- Reduce the number of very large files sent by email to your users
- Protect your company network from the ILOVEYOU virus
- Block pornographic images being sent to your users
- Prevent your network from being used as a spam relay
- Keep your users from sending MP3s to their friends
- Reduce spam
- Reduce the number of very large files sent by email to your users
- Protect your company network from the ILOVEYOU virus
- Block pornographic images being sent to your users
- Prevent your network from being used as a spam relay
- Keep your users from sending MP3s to their friends
- Reduce spam
- Reduce the number of very large files sent by email to your users
- Protect your company network from the ILOVEYOU virus

5. This makes the Firebox deny any message content that is larger than 4 MB.

Email Proxies
Blocking Spam

Stopping Unwanted Email with spamBlocker

What You Will Learn

You can use the optional WatchGuard spamBlocker™ service to block unwanted email messages at your Internet gateway. In this module, you are shown how to:

- Activate and configure spamBlocker
- Specify the actions to take when spam is detected
- Exclude email messages from certain sources
- Monitor spamBlocker activity

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

In this module, you will configure an optional feature of the Firebox®. To view these settings, you must first purchase a license key for spamBlocker. In addition, to activate the key you must have access to a Firebox. If you take this course with a WatchGuard Certified Training Partner, your instructor will provide you with both a Firebox and a license key.

Stop Unwanted Email at the Network Edge

Unwanted email, also known as spam, fills the average inbox at an amazing rate. A large volume of spam decreases the bandwidth available to other applications, degrades employee productivity, and wastes network resources. The WatchGuard® spamBlocker™ service uses industry-leading pattern detection technology from Commtouch® to block spam at your Internet gateway. spamBlocker looks for patterns in spam traffic, instead of the contents of individual email messages. Because it looks for patterns, it can find spam in any language, format, or encoding method.
WatchGuard spamBlocker works with SMTP and POP3 proxy policies to examine up to 20,000 bytes of each inbound email message. You can configure the Firebox to take any of the following actions when spamBlocker determines that an email message processed by the SMTP proxy is spam:

- **Deny** — Stop the spam email message from being delivered to the mail server. The Firebox sends this message to the sending email server: “Delivery not authorized, message refused”.
- **Add subject tag** — Identify the email message as spam or not spam and allow spam email messages to go to the mail server. See the subsequent section for more information on spamBlocker tags.
- **Allow** — Let spam email messages go through the Firebox without a tag.
- **Drop** — Drop the connection immediately. Unlike the Deny option, the Firebox does not give any SMTP error message to the sending server.
- **Quarantine** — Send the message suspected to be spam to a Quarantine Server.

If you use spamBlocker with the POP3 proxy, you have only two actions to choose from: Add Subject Tag and Allow. You cannot use the Quarantine Server with the POP3 proxy in this release. You must configure at least one DNS server so the Firebox can resolve the IP addresses of the Commtouch servers. If you do not do this, spamBlocker will not operate.

**spamBlocker tags**

The Firebox can add spamBlocker tags to the subject line of the email message. You can also configure spamBlocker to customize the tag that it adds. This example shows the subject line of an email message that was classified as spam. The tag added is the default tag: ***SPAM***.

```
Subject: ***SPAM*** Free auto insurance quote
```

Here are some examples of other possible spamBlocker tags:

```
Subject: (SPAM) You've been approved!
Subject: [POSSIBLE SPAM] Save 75%
Subject: [JUNK EMAIL] Free shipping
Subject: *SPAM/BULK* 10 lbs in 10 days!
```

**spamBlocker categories**

spamBlocker puts potential spam email messages into these three categories based on classification of the mail envelope by the Commtouch classification server:

- **Spam** — Includes email messages that come from known spammers. We recommend you use the Deny action for this type of email if you use spamBlocker with the SMTP proxy, or the Add subject tag if you use spamBlocker with the POP3 proxy.
- **Bulk** — Includes email messages that do not come from known spammers, but do match some known spam structure patterns. We recommend that you use the Add subject tag action for this type of email, or the Quarantine action if you use spamBlocker with the SMTP proxy.
- **Suspect** — 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 use the Allow action for this type of email.

**spamBlocker exceptions**

The Firebox might sometimes identify a message as spam when it is not spam. If you know the address of the sender, you can configure the Firebox with an exception that tells it not to examine messages from that source address or domain.
Global spamBlocker settings
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 Firebox®, you must balance good spamBlocker performance with the needs of other Firebox functionality. To access these configuration settings, click Settings from the spamBlocker dialog box.

Maximum number of threads
spamBlocker creates a thread for each message it processes. The thread includes information about the message that is used to generate its spam score. The spam score is used by spamBlocker to decide if a message is spam or not. spamBlocker sets a default maximum number of threads that can be simultaneously buffered according to your Firebox appliance model. You can use the Maximum number of threads field 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 threads for spamBlocker without affecting performance. If you have memory problems related to your use of proxies on the Firebox, you might want to decrease the value in this field.

Maximum file size to scan
Use the Maximum file size to scan field to set the number of bytes of an email message to be passed to spamBlocker to be scanned. Usually, 20–40K is sufficient 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.

Cache size
In the Cache size field, 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 no network traffic to Commtouch is required. Usually, you do not have to change this value. You can set the Cache size field to 0 to force all email to be sent to Commtouch. This is generally used only for troubleshooting.

Proactive Patterns
Clear the Enabled check box next to Proactive Patterns if you want to disable the Commtouch CTEngine Proactive Patterns feature. The Proactive Patterns feature allows spamBlocker to identify and block new spam messages even before the recurrent pattern is added to the Commtouch database. For example, each day new types of spam tricks are introduced on the Internet. With Proactive Patterns enabled, spamBlocker blocks mails that use the newly identified spam methods. When clear patterns are established for these new attacks, the pattern is added to the Commtouch database. This feature is automatically enabled on e-Series and Firebox X Peak models. It requires large amounts of disk space while the local database is updated. If you have limited memory or processor resources, consider disabling this feature.

Connection string override
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.

Using an HTTP proxy server
Select the Contact the spamBlocker server using an HTTP proxy server check box if spamBlocker must use an HTTP proxy server to connect to the Commtouch server through the Internet. Use the remaining fields in this dialog box to set up parameters for the proxy server, which include the address of the proxy server, the port the Firebox must use to contact the proxy server, and authentication credentials for the Firebox to use for proxy server connections (if required by the proxy server).
Adding trusted email forwarders
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. With this feature, spamBlocker ignores the trusted email forwarder in the email message headers. The spam score is calculated using the IP address of the source email server.

Exercise 1: Activate and Configure a Quarantine Server
The Successful Company network administrator decides to start putting suspected mail into quarantine rather than simply locking and tagging it. He would also like to automatically remove messages from the SpamKing domain that he knows produces nothing but spam.

Prepare the Quarantine Server
The Quarantine Server must be a personal computer running a version of Microsoft Windows. For this course, we will use your training workstation.

1. From the Windows desktop, right-click the Quarantine Server icon in the WatchGuard toolbar. Select Setup Wizard. The Quarantine Server Setup Wizard appears.
2. Wait while it configures your workstation as a Quarantine Server. This can take a few minutes. Click Finish.
3. Right-click the Quarantine Server icon again. Select Configure. You are prompted to enter the Server Management Passphrase.
4. Type the Server Management Passphrase. Click OK. If you have been studying these modules sequentially, the passphrase is myservermanagementphrase. The Quarantine Server Configuration utility appears.
5. Click the Rules tab.
6. In the top section, select Auto-Remove messages from specific domains. The Rule description appears. Notice the blue underlined text.
7. Click specific domains. The Edit Auto-Remove Rule dialog box appears.
8. Type SpamKing.com. Click Add.
9. Click **OK**.

10. Click **OK** to close the Quarantine Server Configuration utility and apply the changes you made.

**Configure the Firebox to use the Quarantine Server**

The Firebox must be able to connect to the Quarantine Server. If they are not on the same network, be sure to create a policy which allows access from the management station to the Quarantine Server.

1. From Policy Manager, select **Tasks > Quarantine Server**.
   The Quarantine Server dialog box appears.
2. In the **IP Address** field, type the workstation IP address.

3. Click **OK**.
4. Save the configuration file to the Firebox.
Exercise 2: Activate spamBlocker

Successful Company decides to invest in spamBlocker to help get a handle on all the unwanted email its employees are receiving. In this exercise, we use the spamBlocker™ Wizard to activate the spamBlocker service.

1. From Policy Manager, select Tasks > spamBlocker > Activate. The Activate spamBlocker Wizard appears.

2. Click Next.
   If you are working through the training modules sequentially, using the BlockingSpam-Start configuration file, or taking the class with an instructor, you should have three email proxy policies configured.

3. Clear the POP3-CFO and SMTP-Server-Outgoing policies. Click Next.

4. Click Finish.
   If you do not have an SMTP or POP3 proxy policy, the wizard prompts you to create one.
Exercise 3: Configure the spamBlocker Service

After you use the activate spamBlocker™ wizard, you need to configure spamBlocker settings within your email proxy. In this exercise, you configure the spamBlocker service for SMTP. The procedure to configure spamBlocker for POP3 is the same.

Determine what happens to spam email

In this exercise, the Successful Company network administrator is new to this type of service and is a little nervous about losing valid messages. He decides to quarantine confirmed spam and tag the rest as spam, but send it to the intended recipients.

1. From Policy Manager, select Tasks > spamBlocker > Configure.
   The spamBlocker dialog box appears. It shows email proxy policies and whether spamBlocker is active for each policy.

2. Select SMTP-Incoming-Proxy. Click Configure.
   The spamBlocker configuration dialog box appears.

3. Use the Confirmed Spam drop-down list to select Quarantine.
   All email that spamBlocker confirms as spam will be held in quarantine. The network administrator will have to review these messages before they go to the final recipient.

4. Use the Suspect drop-down list to select Add subject tag.
   The text ***SUSPECT*** appears. You can replace this with any short text phrase.
5. Clear the Send a log message for each message classified as not spam check box. While a useful tool for troubleshooting, receiving a log message for each email message sent to your employees can quickly fill your log database.

Add spamBlocker exceptions

The network administration team at Successful Company all subscribe to the Security Now podcasts from TWIT.tv. However, like many companies that send useful newsletters and announcements to their customers, TWIT uses a bulk mail application. In this exercise, we configure the Successful Company spamBlocker service to allow messages as an exception.

1. From the spamBlocker Configuration dialog box, click the Exceptions tab.
   Notice that spamBlocker is already configured to allow bulk messages from the WatchGuard LiveSecurity service. This ensures that you can receive important announcements, security alerts, and threat responses.
2. Click Add.
   The Add Exception Rule dialog box opens.
3. Use the Action drop-down list to select Allow. In the Sender text box, type *@twit.tv. In the Recipient text box, type *@successfulcompany.com.
   This excludes all messages originating from the TWIT.tv domain from spamBlocker actions.
4. Click OK to close the Add Exception Rule dialog box.
**Turn on alarms when a virus is detected**

One selling point of spamBlocker for the security team at Successful Company was the ability to receive alarms when a virus is detected. In this exercise, we enable the alarm feature.

1. From the spamBlocker Configuration dialog box, click the **Virus Outbreak Detection** tab.
2. Use the **When a virus is detected** drop-down list to select **Drop**. Next to this option, select the **Alarm** check box.

3. Click **OK** to close the spamBlocker configuration dialog box. Click **OK** again to close the spamBlocker dialog box.
4. Save the configuration file to the Firebox.
Exercise 4: Monitor spamBlocker activity

You can use Firebox System Manager to monitor spamBlocker activity.

1. From WatchGuard System Manager, select the Firebox whose spamBlocker activity you want to monitor.
2. Select **Tools > Firebox System Manager**.
3. From Firebox System Manager, click the **Security Services** tab.
   The statistics for spamBlocker appear at the bottom of the screen.
Related Courseware and Information

You can use these resources for more information on how to enable and configure spamBlocker™:

**WatchGuard® System Manager User Guide**

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/) and locate this FAQ:

“How do I set up spamBlocker?”

“How do I report False Positives and False Negatives from spamBlocker?”

“What happens when my subscription services expire?”

“How do I set up rules to send spam or bulk email to special folders in Outlook?”

“How do I set up and use the Quarantine Server with spamBlocker?”
Test Your Knowledge

1. The actions spamBlocker can take when you configure spamBlocker to work with SMTP are (select all that apply):
   - ☐ A) Deny  Stop the spam message without a reply
   - ☐ B) Tag  Add a “spam” tag to the email subject line and allow spam messages to go to the recipient
   - ☐ C) Ignore  Do not send the email to spamBlocker to process
   - ☐ D) Allow  Let spam messages go through the Firebox without a tag
   - ☐ E) Drop  Drop the connection immediately and send no error messages back to sending email server.
   - ☐ F) Quarantine  Isolate the email on a Quarantine Server

2. True or False: The Spam category includes email messages that come from known spammers.

3. Which proxy works with spamBlocker (select all that apply):
   - ☐ A) HTTP
   - ☐ B) SMTP
   - ☐ C) POP3
   - ☐ D) FTP

4. True or False: When you use spamBlocker with the POP3 proxy, the Firebox can deny, drop, allow, or add a subject tag to any suspected spam message.

5. True or False: You must configure a Quarantine Server to use spamBlocker.

† A) Deny - Stop the spam message without a reply
† B) Tag - Add a “spam” tag to the email subject line and allow spam messages to go to the recipient
† C) Ignore - Do not send the email to spamBlocker to process
† D) Allow - Let spam messages go through the Firebox without a tag
† E) Drop - Drop the connection immediately and send no error messages back to sending email server.
† F) Quarantine - Isolate the email on a Quarantine Server

ANSWERS
1. A, B, D, E, F
2. True
3. B and C
4. False - Only the SMTP proxy can deny a message.
5. False - The Quarantine Server is optional.
DNS Proxy

Using the DNS Proxy

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox X Core / Firebox X Core e-Series / Firebox X Peak /Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>DNS Proxy</td>
</tr>
</tbody>
</table>

**What You Will Learn**

The DNS proxy can protect your DNS server as well as control outgoing connections to external DNS servers. In this training module, you are shown how to:

- Understand the purpose of the DNS proxy
- Configure the DNS proxy to protect your DNS server
- Use the DNS proxy for outgoing connections to external DNS servers

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

[http://www.watchguard.com/training/courses.asp](http://www.watchguard.com/training/courses.asp)

**Protect a DNS Server On Your Trusted Network**

The Domain Name System (DNS) is a network system of servers that translates numeric IP addresses into readable, hierarchical Internet addresses, and vice versa. This is what allows your computer network to understand that you want to reach the server at 200.253.208.100 or type into your browser a domain name such as www.watchguard.com.

With Fireware®, you have two methods to control DNS traffic through your firewall: the DNS packet filter and the DNS proxy policy. A packet filter examines the header information while a proxy examines the contents at the application layer and validates that the packet meets RFC compliance for DNS traffic. In this training module, we concentrate on the higher level of security available through a DNS proxy policy. It is important to understand that the DNS proxy settings are useful only if the DNS request is routed through the firewall.

To simplify configuration of your DNS policy, the default configuration includes two template proxy actions for DNS. You can use these rulesets without changing them, or you can use the rulesets as a base for a ruleset to meet the needs of your organization.

**DNS-Incoming**

This proxy action includes rulesets to protect your DNS server from DNS queries that are not correctly formed and certain query types that could be a risk to the security of your DNS server.

**DNS-Outgoing**

This proxy action includes rulesets to control outgoing DNS requests from your trusted users.
DNS-Incoming rulesets
You control incoming DNS connections to a DNS server on your optional or trusted network with the DNS-Incoming proxy action rulesets. The default configuration includes rules that examine the structure and syntax of incoming DNS requests to restrict known, deliberate attempts to compromise the security of your locally hosted DNS server.

Six default rulesets are included with the DNS-Incoming proxy action. These rulesets are shown in the Categories list on the left side of the DNS Proxy Configuration dialog box.

**General**
The General ruleset includes the basic DNS protocol anomaly detection rules to deny malformed and non-standard DNS queries. We recommend that you do not change the default settings for these rules.

**OpCodes**
OPcodes (operational codes) are commands sent to a DNS server, such as query, update, or status requests. They operate on items such as registers, values in memory, values stored on the stack, I/O ports, and the bus. 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. You use the OpCodes ruleset to allow or deny specific DNS OPcodes.

**Query Types**
You use the Query Types ruleset to allow or deny DNS connections based on the type of DNS query sent in the connection.

**Query Names**
You use the Query Names ruleset to allow or deny DNS connections based on the fully qualified domain name sent in the connection.
Intrusion Prevention
Although you can use the proxy definition screens to activate and configure IPS, it is easier to use the Tasks menu in Policy Manager to do this. The Intrusion Prevention ruleset lets you turn on the Intrusion Prevention Service’s monitoring of incoming DNS requests to look for signatures that match those in the IPS database. For more information on the optional IPS feature, see the “Threat Protection” training module.

Proxy Alarm
The Proxy Alarm ruleset lets you define the type of alarm that is sent any time a notification is triggered by a DNS-Incoming ruleset.

Using the DNS-Outgoing proxy action
When you make a new configuration file with Policy Manager or the Quick Setup Wizard, 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 using 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-Outgoing proxy action 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.

The same six rulesets in the DNS-Incoming proxy action are included with the DNS-Outgoing proxy action. These rulesets are shown in the Categories list on the left side of the DNS Proxy Configuration dialog box.

Exercise 1: Configure a DNS-Incoming Proxy Action
Successful Company has two DNS servers, one on the trusted network and a secondary on the optional network. After reading a LiveSecurity alert about a DNS exploit, the network administrator decides that he needs to create a DNS incoming proxy policy using static NAT to control traffic to the DNS server on his optional network.
Add a DNS incoming proxy policy

First, the network administrator adds a DNS proxy policy and configures it to examine traffic from external network to the DNS server on the optional network.

1. From Policy Manager, open the configuration file you are editing for these exercises.

2. Click .
   You can also select Edit > Add Policy. The Add Policies dialog box appears.

3. Expand the Proxies folder. Click DNS-proxy and click Add.
   The New Policy Properties dialog box appears.

4. In the Name text box, type DNS-Incoming-Proxy.

5. Under the From list, click Add. Click Add Other. Double-click Any-External. Click OK. Click Any-External. Click Remove.
   The policy now controls DNS traffic from the external network.

6. Under the To list, click Any-External. Click Remove. Click Add.

7. Click Add NAT. In the Internal IP Address box, type 10.0.2.53 as the IP address of the Successful Company primary DNS server on the optional network. Click OK. Click OK again.

8. Select the Properties tab. Use the Proxy drop-down box to select DNS-Incoming.

Log denials for reporting

Successful Company’s network administrator is having trouble with her DNS server on the trusted network. For a brief time, she uses the Firebox® to log all incoming DNS requests which she can then view in Historical Reports.

1. Click .
   The DNS Proxy Action Configuration dialog box appears.

2. From the Categories list, select General.
3. Check **Turn on logging for reports.**
   This feature records every DNS transaction. It is used primarily for troubleshooting.

![DNS Proxy Action Configuration (predefined)](image1)

**Allow a DNS query type**

After she does some research, Successful Company’s network administrator learns that SIP user agents must use the DNS query type SRV (also known as service) to perform SRV record lookups to the DNS servers. We must edit the DNS proxy policy to allow SRV requests to the DNS server.

1. From the **Categories** list, select **Query Types**.
2. Select the query type **SRV record** in the list. Click **Edit**.
   The Edit Query Types dialog box appears.
3. In the **Rule Actions** section, use the **Action** drop-down list to select **Allow**.

![Edit Query Types Rule](image2)
4. Click **OK**. Find the SRV query type in the list and make sure the **Enabled** check box is selected. The SRV query type should now appear as allowed and enabled.

5. Click **OK** to close the **DNS Proxy Action Configuration** dialog box. Because DNS-Incoming is a template, you cannot change it. You can only make a copy and use it for your policies.

6. Click **OK** to clone the template. The default name for a clone is DNS-Incoming.1.

7. Click **OK** to close the **New Policy Properties** dialog box. Click **Close** to close the **Add Policy** dialog box. The DNS-Incoming-Proxy policy appears in your policy list.
Exercise 2: Use the DNS-Outgoing Proxy Action

Because of problems associated with adware accidently downloaded into their network, the Successful Company network administrator would like to block DNS requests to messenger.yahoo.com. This site has been associated with shareware programs that also install adware, such as Gator. Adware is a software application that can display advertising banners while the program is running or through some other triggering mechanism. It can waste bandwidth and other system resources. It can also give attackers a way to get to your resources.

Add a DNS outgoing proxy policy

First, we add a policy to control outgoing DNS requests from our trusted users.

1. From Policy Manager, click.
2. Expand the Proxies folder. Click DNS-proxy and click Add.
   The New Policy Properties dialog box appears.
3. In the Name text box, type DNS-Outgoing-Proxy.
   We do not need to change the From and To as they are already set from our trusted networks to any computer on the external network.
4. Click the Properties tab. Use the Proxy Action drop-down list to select DNS-Outgoing.

Block a DNS request by query name

Now, we block DNS requests for a specific domain.

1. Click.
   The DNS Proxy Action Configuration dialog box appears for the DNS-outgoing actions.
2. From the Categories list, select Query Names.
   You see that messenger.yahoo.com already appears in the list of query names, but it is not active. This is an example of a case where WatchGuard provided a rule for your use, but it is not active in the default configuration.
3. To activate the rule, click Change View. Select the check box adjacent to messenger.yahoo.com.
   The default DNS proxy configuration does not deny DNS requests that contain messenger.yahoo.com. If you wanted to edit the properties of this rule, you would click Edit.
   Once you edit the Query Names settings in the Advanced View, Basic View is no longer available.
4. Click OK to close the DNS Proxy Action Configuration dialog box.
   Because DNS-Outgoing is a template, you cannot change it. You can only make a copy and use it for your policies.
5. Click OK to clone the template.
   The default name for a clone is DNS-Outgoing.1.
6. Click **OK** to close the **New Policy Properties** dialog box. Click **Close** to close the **Add Policy** dialog box. The DNS-Outgoing-Proxy policy appears in your policy list.

![Firewall Policy Table](image)

**Related Courseware and Information**

You can use these resources for more information on how to work with the DNS proxy.

**WatchGuard® System Manager User Guide**
Browse to [https://www.watchguard.com/help/documentation/](https://www.watchguard.com/help/documentation/) and download the **WSM User Guide**. See the chapters “Proxies” and “Signature-Based Security Services.”

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/)
Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. True or false: A default configuration file includes a DNS proxy policy that uses the DNS-Incoming ruleset.

2. Fill in the blank: To protect your DNS server from attacks, you configure a DNS proxy policy with this proxy action: _____________________

3. The function of a DNS server is to:
   - A) Distribute IP addresses to computers when they connect to a network
   - B) Assign domain names to individual networks
   - C) Translate numeric IP address into readable Internet addresses
   - D) All of the above
   - E) None of the above

4. Use the screenshot below and circle the correct answer to these questions:

   ![Edit DNS Proxy Action Configuration](image)

   A) This policy protects your users from an external DNS server.  
   B) The IPS service is enabled for this policy.  
   C) This policy blocks all incoming TXT record requests.  
   D) This policy allows all outgoing MX record requests.  
   E) You can add a new query type to the Rules list.
1. False - The default configuration does not have any DNS proxy policy. DNS traffic is allowed through the default Outgoing policy.
2. DNS-Incoming
3. C
4. A. False - This is a DNS-Incoming policy. You use the DNS-Incoming policy to protect a locally hosted DNS server on your trusted or optional network.
   B. Can't be determined - Although Intrusion Prevention always appears in the list of categories, you can enable the feature only if you have installed and configured the IPS service.
   C. True
   D. Can't be determined. You must look at the DNS-Outgoing ruleset to find this information.
   E. True
Web Traffic

Managing Web Traffic Through the Firewall

What You Will Learn

The HTTP proxy can protect your private and public web servers. It can also be used to both protect your user community from viruses as well as restrict unauthorized web use. In this module, you are shown how to:

- Enable a log message for each HTTP client connection
- Block HTTP client connections by URL path
- Allow files through the HTTP proxy by type
- Customize the deny message a user receives
- Strip headers that specify a certain type of authentication
- Activate WebBlocker
- Select categories of web sites to block
- Override WebBlocker rules for specific sites

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

Control Web Traffic Through Your Firewall

HTTP (Hypertext Transfer Protocol) is a protocol used to send and display text, graphic images, sound, video, and other multimedia files on the Internet. The WatchGuard® HTTP proxy is a high performance content filter. It examines web traffic to identify suspicious content, which can be spyware, malformed content, or another type of attack. It can also protect your web server from attacks from the external network using protocol anomaly detection rules to identify and deny suspicious packets.

The HTTP proxy operates between the sending web server and your receiving web client. It processes the HTTP protocol line-by-line for any potentially harmful content before sending it to an internal web client. It also acts as a buffer between your web server and potentially harmful web clients by enforcing HTTP RFC compliance and preventing potential buffer overflow attacks.

When you add an HTTP proxy policy to your Firebox® configuration, you get access to two proxy actions that are included with the product: an HTTP server ruleset template and an HTTP client ruleset template. You can use these rulesets without changing them, or you can use the rulesets as a base for a ruleset to meet the needs of your organization. This module shows you how to customize the rulesets in these two proxy actions.
HTTP-Client
The HTTP-Client proxy action is configured to give comprehensive protection to your network from the content your trusted users download from web servers.

HTTP-Server
The HTTP-Server proxy action is configured by default to allow most HTTP connections through to your public web server, but stop any attempts to put files on your web server or delete files from your web server.

Both the HTTP-Client and HTTP-Server proxy actions can use optional services that further protect your network.

WebBlocker
Controls the web sites trusted users are allowed to browse to at different times of the day. WebBlocker is only available for the HTTP-Client proxy action.

Gateway AntiVirus (Gateway AV)
Scans HTTP traffic and can stop viruses before they get to the client computers and HTTP servers on your network.

Intrusion Prevention Service (IPS)
Scans HTTP traffic for attempts to cause damage to your network, get sensitive information, or use your client computers and servers to attack other networks.

Controlling outgoing HTTP requests
You control outgoing HTTP connections from HTTP client applications to prevent your user community from downloading many of the dangerous files types that have been used by hackers to introduce viruses, trojans, and worms onto your network.

The many settings of the HTTP-Client proxy give you a high degree of control over the HTTP connections of your trusted users. You can strip files by file name or MIME content type. You can also restrict the use of cookies, ActiveX, Java, and other potential vectors for trojans and worms.

Protecting your web server
Web servers are popular targets for attackers. Although vendors try to patch web server applications quickly, attackers have a window of vulnerability between the time an attack is discovered and the opportunity you have to patch it. You can use the HTTP-Server proxy action as a way to prevent the attack until a patch is available.
If you host a public web server, you must also make sure that people can get access to it while protecting it against attacks. The default HTTP-Server ruleset allows most types of connections through the Firebox while it blocks the most common attacks. You can customize this ruleset to meet your business requirements.

**HTTP rulesets**

The ruleset functions are the same for both HTTP-Client and HTTP-Server proxy actions, but the default rules are different. These rulesets are shown in the **Categories** list to the left of the **HTTP Proxy Configuration** dialog box.

**HTTP Request — General Settings**

Use this ruleset to control the basic HTTP parameters of idle time out and maximum URL length. A very important rule you can enable in this ruleset is an option to send a log message with summary information for each HTTP connection request. **Turn on logging for reports** must be active to get bandwidth usage information in HostWatch and reports.

**HTTP Request — Request Methods**

The Request Method ruleset lets you control the types of HTTP request methods allowed through the Firebox as part of an HTTP request. By default, only HEAD, GET, POST, OPTIONS, PUT, and DELETE request methods are allowed from the client through the Firebox. Some applications such as Google Desktop and FrontPage use HTTP as a transport to require additional request methods. webDAV is used for collaborative online authoring and has a large number of additional request methods. The HTTP proxy supports webDAV request method extensions according to the specifications in RFC 2518.

**HTTP Request — URL Paths**

Use the URL Path ruleset to filter the content of the host and path of a URL. For best results, use URL path filtering together with file header and content type filtering.

**HTTP Request — Header Fields**

This ruleset supplies content filtering for the full HTTP header name and its value. By default, the Firebox uses exact matching rules to strip Via and From headers, and allows all other headers. The Via header can be added to a client request by a proxy server to track message forwards and avoid request loops. Stripping the Via header can protect client privacy. The From header passes the client users’ email address to the server, which can be harvested by bulk mail recipient lists. Stripping this header helps reduce the chance of receiving spam and maintains client anonymity and privacy.

**HTTP Request — Authorization**

This ruleset 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. With a default configuration, the Firebox allows Basic, Digest, NTLM, and Passport 1.4 authentication.
HTTP Response - General Settings
Use this ruleset to configure basic HTTP response parameters, including idle time out, maximum line length, and maximum total length of an HTTP response header. If you set a value control to 0 bytes, the Firebox ignores the size completely.

HTTP Response - Header Fields
This ruleset controls which HTTP response header fields the Firebox allows. Response headers can be used for specifying cookies, to supply modification dates for caching, to instruct the browser to reload the page after a specified time interval, and for several other tasks.

HTTP Response - Content Types
This ruleset controls the types of MIME content allowed through the Firebox in HTTP response headers. By default, the Firebox allows some safe content types and denies MIME content that has no specified content type. This is a common way of restricting the types of files that users can download from web sites.

HTTP Response - Cookies
Use this ruleset to control cookies included in HTTP responses. The default ruleset allows all cookies. HTTP cookies are used for tracking and storing information about users lengthy visit particular sites.

HTTP Response - Body Content Types
This ruleset gives you control of the content in an HTTP response. The Firebox is configured to deny Java applets, Zip archives, Windows EXE/DLL files, and Windows CAB files by default. It is a good idea to examine the file types used in your organization and allow only those file types that are necessary for your business.

HTTP Proxy Exceptions
All traffic to a domain listed in this ruleset will bypass the proxy completely. Only trusted sites that supply needed files that would be denied by other parts of the HTTP proxy should be listed here.

Antivirus
This ruleset sets the actions necessary if a virus is found. Although you can use the proxy definition screens to activate and configure Gateway AntiVirus, it is easier to use the Tasks menu in Policy Manager to do this. For more information, see the “Signature Services” training module.

Deny Message
This ruleset lets you customize the default deny message that your trusted users will see if the Firebox denies some HTML content they have tried to download with their web client.

Intrusion Prevention
The Intrusion Prevention ruleset lets you turn on the Intrusion Prevention Service’s monitoring of the HTTP client connections to look for signatures that match those in the Intrusion Prevention Service database (if you have purchased the optional Intrusion Prevention Service). Although you can use the proxy definition screens to activate and configure IPS, we recommend that you use the Tasks menu in Policy Manager to do this. For more information about IPS, see the “Signature Services” training module.

Proxy and AV Alarms
This ruleset lets you define the type of alarm that is sent any time a notification is triggered by an HTTP ruleset.

Restrict Web Access with WebBlocker
WebBlocker uses a database of web sites, organized into distinct categories. The content of this database is maintained by SurfControl®—an industry leader in web filtering software. You store a local copy of this database on a Windows computer on your trusted or optional network. This computer is known as the WebBlocker Server.

When a user on your network browses to the Internet, the Firebox automatically checks the WebBlocker Server to see if the site is allowed. If the site is on the block list, the user receives a message that the site is not available.
To use WebBlocker you must:

- Install and set up the WebBlocker Server
- Activate a WebBlocker license
- Configure an HTTP Proxy policy to use WebBlocker

**WebBlocker categories**
The WebBlocker database is divided into 54 topic categories such as News, Gambling, or Adult/Sexually Explicit. You can find a list and description of the categories when you configure WebBlocker, or in the *WatchGuard System Manager Reference Guide*. You can also use a single check box to tell WebBlocker that you want to block all categories.

**WebBlocker exceptions**
You can override a WebBlocker action with an exception. You can add a web site that is allowed or denied as an exception to the WebBlocker categories. The exceptions are based on IP addresses or a pattern based on a URL. You can have the Firebox block a URL with an exact match. Usually, it is more convenient to have the Firebox look for URL patterns. To match a URL path on all web sites, the pattern must have a trailing "/*". The host in the URL can be the host name specified in the HTTP request, or the IP address of the server.

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*. Such broad wildcards should be used cautiously, however, since the rule just described would also unintentionally block access to a web site for the City of Middlesex.

You can also block ports in a URL. For example, http://www.hackerz.com/warez/index.html:8080 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.

**WebBlocker schedules**
You can set an operating schedule for a set of WebBlocker rules. You use time periods to set rules for when to block different web sites. For example, you can block sports web sites during usual business hours of operation, but allow users to browse at lunch time, evenings, and weekends. To do this, you add a schedule to the HTTP proxy policy that WebBlocker is assigned to. You can also configure two HTTP policies, but create a schedule for only one of them. Each policy uses one of the HTTP proxy actions. Each of these HTTP proxy actions points to one of at least two WebBlocker actions.

**WebBlocker Server**
The WebBlocker Server is installed and activated during the installation of WatchGuard System Manager. If you did not originally install the WebBlocker Server when installing WSM, you can do so at any time. Double-click the WSM installation file and modify the installed components by selecting the check box for WebBlocker. Then, continue installation.
Exercise 1: Configure HTTP Connections from Trusted Users

Successful Company network administrators are now ready to configure the Firebox® to enforce company policy on browsing the web. In this exercise, you edit the predefined HTTP-Client ruleset to limit the types of HTTP connections that Successful Company employees can start. Specifically, you will:

- Turn on logging of HTTP client requests
- Block HTTP client connections to YouTube®
- Enable the web download of Microsoft® Word, Excel, and PowerPoint documents, as well as Zip files
- Customize the message that users see when some of the content in their web requests is denied

Add an HTTP client proxy policy

The HTTP packet filter can not meet all the Successful Company web policy criteria. First, we must add a HTTP-Client proxy policy.

1. From Policy Manager, open the configuration file you are editing for these exercises.
2. Click .
   You can also select Edit > Add Policy. The Add Policies dialog box appears.
3. Expand the Proxies folder. Click HTTP-proxy and click Add.
   The New Policy Properties dialog box appears.
4. In the Name text box, type HTTP-Employees.
   By default, the HTTP-proxy policy is outgoing and controls traffic from any trusted network to any computer on the external network.
5. Select the Properties tab. Verify the Proxy action is set to HTTP-Client.
6. Select the Properties tab. Make sure that HTTP-Client is the selected proxy action.

Enable a log message for each HTTP client connection

Successful Company’s network administrator wants to make sure that the Firebox records each HTTP connection initiated by an employee. He plans to use this data to prove internal compliance with the
company’s Internet usage policy. It can also help to troubleshoot bandwidth problems if they occur in the future.

In the default HTTP-Client proxy action, as in other proxy rulesets, allowed connections do not create log entries unless you activate the log option. If you do not activate the option to send a log message for each HTTP client connection, you do not see any allowed HTTP traffic in the log file or in reports. You also do not see HTTP connections in HostWatch.

1. Click . The HTTP Proxy Action Configuration dialog box appears.
2. From the Categories list, select HTTP Request > General Settings.
3. Select the Turn on logging for reports check box.

Block HTTP client connections by URL path

Because of concerns about employee productivity and bandwidth use, Successful Company’s network administrator was asked to have the Firebox stop all HTTP client connection requests to YouTube. To block all client connections that include youtube.com in the URL path:

1. From the Categories list, click HTTP Request > URL Paths. The default configuration for the HTTP-Client proxy action allows all URL paths.
2. In the Patterns text box, type *.youtube.com. Click Add.
3. In the Actions to Take section, use the If matched drop-down list to select Deny.
4. To send a log message when this rule denies a connection, select the Log check box.

Allow Microsoft Office documents and Zip files through the HTTP proxy
The business needs of Successful Company require that users download certain Microsoft Office documents. Also, employees often use their browser to download files compressed using the ZIP file format, even though it is a security risk. After their network administrator educates users on the types of zipped files to avoid, it is decided to allow zipped content through the HTTP proxy as well. To allow these types of content, you must edit two of the HTTP Response rulesets:

1. From the Categories list, select HTTP Response > Content Types.
   The list of content types allowed by default includes PDF, XML, Flash, text, and image files. Many common MIME types are shown if you click the Predefined button. To find the MIME type for some content you want to allow or deny through the Firebox, refer to the WSM Reference Guide or go to http://www.iana.org/assignments/media-types/.

2. In the Pattern text box, type application/ms-excel. Click Add. Type application/mspowerpoint. Click Add. Type application/msword. Click Add. Type application/zip. Click Add.
3. Click application/*. Click **Remove**. Click **Yes**.

![HTTP Proxy Action Configuration (predefined)](image)

4. From the **Categories** list, select **HTTP Responses > Body Content Types**. Click **ZIP Archive**. Click **Remove**. This removes ZIP as a denied body content type.

**Customize the Deny message**

When a user on your network tries to browse to a site or to download a file that the HTTP Proxy action blocks, that user sees a Deny message. The default message includes the reason, method, host, and path. In this exercise, you edit the message to also include the email address for the Successful Company help desk.

1. From the **Categories** list, select **Deny Message**. The Deny Message uses HTML. The Firebox accepts most valid HTML code.

2. Highlight the phrase **WatchGuard HTTP proxy**. Type **Successful Company firewall**.

3. Click at the end of **"<b>Path: </b>%(url-path)%<br>** and press the Enter key. Type: **For more information, contact Dustin and Nandi at ITHelp@mywatchguard.com.<br>**
4. Click **OK** to close the **HTTP Proxy Action Configuration** dialog box. Because HTTP-Client is a template, you cannot change it. You can only make a copy and use it for your policies.

5. Click **OK** to clone the template. The default name for a clone is HTTP-Client.1.

6. Click **OK** to close the **New Policy Properties** dialog box. Click **Close** to close the **Add Policy** dialog box. The HTTP-Employees policy appears in your policy list.

---

**Exercise 2: Use HTTP Proxy Exceptions to allow Software Updates**

Frequently, software companies configure their software to “phone home” for software updates. This traffic can occur over HTTP. The update session can include many content types, file names and other properties that could cause the HTTP proxy to deny the traffic. At Successful Company, many employees use the Mozilla® Firefox® browser. To allow the clients to update their browsers automatically, the Firefox servers can be added to the list of HTTP Proxy Exceptions. All traffic to a domain listed in the HTTP Proxy Exceptions will bypass the proxy.

1. From Policy Manager, double-click the **HTTP-Employees** policy. The Edit Policy Properties dialog box appears.

2. Click the **Properties** tab. Adjacent to the **Proxy Action** text box, click ![Edit](image). The Edit HTTP Proxy Action Configuration dialog box appears.

3. From the **Categories** list, click **HTTP Proxy Exceptions**. Notice that the list already includes the domains used by Microsoft Windows to distribute updates to their software.

4. In the text box below the **Exceptions** list, type `*.mozilla.com`.

5. Click **OK** to close the **Edit HTTP Proxy Action Configuration** dialog box. Click **OK** again to close the **Edit Policy Properties** dialog box.
Exercise 3: Configure an HTTP-Server Proxy Action

Successful Company has a web server on the optional network at 10.0.2.80. Initially, their network administrators find the default settings of the HTTP-Server ruleset sufficiently robust to protect their server. Later we will learn that sometimes you need to change that ruleset to provide additional protection.

Add the HTTP-Server proxy policy

First, protect the Successful Company public web server. We will configure it to accept connections from both the trusted and external networks. This policy will use static NAT.

1. From Policy Manager, select Edit > Add Policy. Expand Proxies. Select HTTP-Proxy. Click Add.
2. In the Name text box, type HTTP-Public Server. It is useful to have a separate policy for each web server on your network.
3. Under the To list, click Any-External. Click Remove. Click Add. Click Add NAT. In the Internal IP Address box, type 10.0.2.80. Click OK. Click OK again. This restricts the policy to the Successful Company public web server on the optional network.
4. Under the From list, click Add. Double-click Any-External. Click OK.
   This expands the policy to include connections from the external as well as the trusted network.
5. Click the Properties tab. Use the Proxy action drop-down list to select HTTP-Server. Because we are going to accept the default ruleset, we do not need to click the View/Edit button.
6. Click OK. Click Close.
   The HTTP-Public-Server policy appears in the policy list.

Create a new proxy policy ruleset

Successful Company recently received a LiveSecurity alert that describes a vulnerability to Passport 1.4 authentication. In this exercise, you edit the HTTP-Server ruleset based upon this hypothetical LiveSecurity alert. Use the HTTP-Server proxy action rulesets to strip headers that specify Passport 1.4 authentication. This additional precaution can remain on the server until the network administrator applies and tests the patch the vendor provided, which was also described in the LiveSecurity Alert.

First, we clone the HTTP-Server ruleset and modify it to block the Passport 1.4 authentication. Then we apply it to our public server policy.

1. From Policy Manager, select Setup > Actions > Proxies.
   The Proxy Actions dialog box appears. This is a list of all the template rulesets available.
2. Select HTTP-Server and click Clone.
   The Clone HTTP Proxy Action Configuration dialog box appears.
4. Click Change View.
   In this view, we can change the settings for each rule rather than apply a global setting to all of them.
5. In the Rules list, click Passport 1.4. Click Edit.
   The Edit Authorization Rule dialog box appears.
6. In the **Rule Actions** section, use the **Action** drop-down list to select **Strip**. Select the **Log** check box. This rule strips all headers with Passport 1.4 authentication requests in them and sends a log message which can later be tracked using reports.

7. Click **OK** to return to the Authorization ruleset page. Click **OK** again to close the **Clone HTTP Proxy Action Configuration** dialog box.

8. In the **Name** text box, type **HTTP-Server-BlockPassport**. Click **OK**. Click **Close**. Click **OK** again. This will let us quickly apply this ruleset again in the future should it become necessary. You now have a ruleset which strips Passport 1.4 authorization requests.

9. Double-click the **HTTP-Public-Server** policy.

10. Click the **Properties** tab. Use the **Proxy Action** drop-down list to select **HTTP-Server-BlockPassport**. Click **OK**.
Exercise 4: Selectively Block Web Sites with WebBlocker

Successful Company is pleased with the results of their purchase of spamBlocker™. The network administrators decide to purchase the WebBlocker feature to enforce HR restrictions on what web content can be viewed during work hours.

Add a WebBlocker action
You can activate WebBlocker in two ways. The first is to use the global Actions menu. The second is to use the HTTP proxy. In this exercise, you use the first method to configure the WebBlocker policy for the Successful Company network.

1. From Policy Manager, select Setup > Actions > WebBlocker.
2. Click Add.

The WebBlocker Configurations dialog box appears.

3. In the Name text box, type General Employees. In the Description text box, type Everyone but the Executives and IT.

4. On the Servers tab, click Add.

The New WebBlocker Configuration dialog box appears.

5. Type the IP address of your workstation. Click OK.

When you use more than one WebBlocker Server, client computers try to connect to a server in the order the servers appear in the list. They keep trying until they connect successfully.

Select Categories to Block
Successful Company is very strict about sexual harassment, and about bias or intolerance regarding race, religion, or political beliefs. Obviously, the network administrator should block the sexual and hate speech categories. However, sites that belong to other categories might be a problem for the company as well.

1. Click the Categories tab.
2. Click the Adult check box.

This blocks all the subcategories for Adult.
3. Select the **Intolerance & Hate** check box. Scroll through the categories and click any categories you think might be blocked at your company. Many organizations, for example, also block Peer-to-Peer and Spam URLs as a way to help protect their networks from malware.

![WebBlocker Configuration Dialog Box](image)

### Create an exception

A web site on advertising principles that has a section on Ravel's Bolero is in the Adult/Sexually Explicit category. However, this is a useful site for the Successful Company Marketing department. The network administrator wants to create a WebBlocker exception for this site.

1. From the **New WebBlocker Configuration** dialog box, click the **Exceptions** tab.
2. Click **Add**. The New WebBlocker Exception dialog box appears.
3. In the **Pattern** text box, type `23.23.36.223`. Leave the defaults in the **Match Type** and **Type** fields. Click **OK**. WebBlocker asks if you want to add a “/” to the IP address to unblock all sites with this address. Click **Yes**. WebBlocker will now allow access to this site even though its IP address is in the Adult/Sexually Explicit category.
4. Click **OK** to close the **New WebBlocker Configuration** dialog box. Click **Close**.
   You can now apply the WebBlocker action to any policy that uses the HTTP proxy. You can apply the same WebBlocker action to more than one policy, or create different sets of WebBlocker rules for different groups in your organization.

5. From Policy Manager, select **Setup > Actions > Proxies**. Select **HTTP-Client.1**. Click **Edit**.
   In this exercise, we will add the General Employees WebBlocker action to our primary HTTP-Client ruleset.

6. Use the **WebBlocker** drop-down list to select **General employees**.

7. Click **OK** to close the **Edit HTTP Proxy Action Configuration** dialog box. Click **OK** again to close the **Proxy Actions** dialog box.
   The change is automatically applied to all policies which use the HTTP-Client.1 proxy action ruleset.

8. Save the configuration file as **WebTraffic-Done**.
   You can compare your results with the WebTraffic-Finish file included with the training.
Frequently Asked Questions

Can I get a report of HTTP traffic on my Firebox?
Yes. In the General Settings category for the HTTP proxy, select the Turn on logging for reports check box. The Firebox creates a log message for each HTTP transaction. You can use Report Manager to get detailed reports on HTTP traffic.

Related Courseware and Information

You can use these resources for more information on how to enable and configure the HTTP proxy:

**WatchGuard® System Manager User Guide**

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/)

**RFC Archives**
To learn more about protocols used for the web and controlled by the HTTP proxy, browse to:


**WatchGuard System Manager Reference Guide**

Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. Circle the proxy action you would use to do these tasks:
   A) Prevent users from downloading batch (*.bat) files from the Internet
   B) Strip Zip (*.zip) files from email messages
   C) Block incoming HTTP GET requests
   D) Apply WebBlocker to prevent users from browsing to web sites with profanity
   E) Configure the message users see when they browse to blocked URLs
   F) Resolve domain names for web sites

2. Fill in the blank: To use best security practices, you would place your public web server on the __________ network.

3. In the screen shot below, all of URL Path entries are set to Deny if matched. Using this configuration, which Web sites will the Firebox block (select all that apply):
   - A) terrificsex.com
   - B) allthemusic.bittorrent.com
   - C) sex.thegoodstuff.com
   - D) www.trumpets.org
   - E) prevent.pornography.org
4. True or False: WebBlocker adds URL filtering to the SMTP proxy.

5. Select the number of WebBlocker categories that are available:
   - A) 14
   - B) 24
   - C) 40
   - D) 54
   - E) None of the above

6. True or False: An exception to the WebBlocker rules allows a site that is normally blocked to be viewed, or a site that is normally viewed to be blocked.

7. The web site 10.0.1.19 is acceptable for employees to view except for its pages on politics. If the site’s pages on politics all have the word “politics” somewhere in the path, what do you type in the Pattern field? __________________

8. True or False: You can create new WebBlocker categories.
9. True or False: You can create a WebBlocker exception that blocks a specific port in a URL.
Threat Protection
Defending Your Network From Intruders

What You Will Learn

Firewalls provide both signature based and default threat protection measures. In this module, you are shown how to:

- Understand the different type of intrusion protection available for the Firebox
- Configure Firebox default packet handling options to stop many common attacks
- Block IP addresses and ports used by hackers to attack your network
- Automatically block IP addresses that send suspicious traffic

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

Default Threat Protection Measures Block Intruders

With Policy Manager, you can configure the Firebox® with very detailed control over access to your network. A strict access policy helps to keep hackers out of your network, however, a strict policy cannot defeat certain other types of attacks.

An Intrusion Prevention Service (IPS) detects attacks from hackers. With Fireware, you can use your Firebox as an IPS device to detect and prevent attacks automatically. There are two categories of IPS defenses:

Firewall-based IPS

The Firebox combines protocol anomaly detection with traffic analysis to proactively block many common attacks. Protocol anomaly detection is the examination of a packet for compliance with RFC guidelines. Attackers can make packets that are different from RFC standards in ways that allow them to bypass standard packet filters and get access to your network. If you block non-compliant packets, you can also block the attack. This allows your Firebox to proactively protect you against attacks that are as yet unknown.

Traffic pattern analysis examines a series of packets over time and matches them against known patterns of attack. For example, when an attacker launches a port space probe, they attempt to send packets through each port number until they identify which ports your firewall allows. If you can identify this pattern, you can block the source of the probe.
A firewall-based IPS can also protect your network from a “zero-day” threat. In other words, before the network security community is even aware that the vulnerability exists, broad categories of attack types are automatically identified and blocked by a strong firewall-based IPS.

**Signature-based IPS**

Fireware options such as the Gateway AntiVirus/Intrusion Prevention Service can be configured to compare the contents of packets against a database of character strings that are known to appear in attacks. Each unique character string is known as a signature. When there is a match, the Firebox can block the traffic and notify the network administrator. To remain protected, you must regularly update the signature database.

Signature-based approaches use less computer processing time than firewall-based IPS measures, however, they need a database update before they are current. As a result, signature-based IPS is good for maintaining efficient, high performance protection while firewall-based IPS catches the “zero-day” threats.

The rest of this training module focuses on the firewall-based IPS measures available with Fireware. For more information on signature based measures, see the “Signature Services” training module.

**Using Default Packet Handling Options**

Default packet handling is a set of pattern analysis rules to help protect your Firebox from attacks and also to instruct the Firebox how to process packets when no other rules are specified. With default packet handling, a firewall examines the source and destination of each packet it receives. The firewall looks at the IP address and port number and monitors the packets to look for patterns that show your network is at risk. If there is a risk and the Firebox is properly configured, it automatically blocks the possible attack.

The default configuration of the Firebox default packet handling options stops attacks such as SYN flood attacks, spoofing attacks, and port or address space probes. We do not recommend that you change the default packet handling settings in your Firebox configuration unless a particular setting interferes with the function of your network or you want a more stringent defense, like that available with the Block source of packets not handled option. The settings are carefully chosen to maximize security.

Default packet handling:

- Rejects packets that could be used to gain information about your network
- Automatically blocks all traffic to and from a source IP address when a configured limit is reached
- Adds an event to the log file
- Sends an SNMP trap to the SNMP management server (when configured)
- Sends a notification of possible security risks (when configured)
**Unhandled Packets**

Packets that are denied by the firewall because they do not match any of the firewall policies are blocked as “unhandled packets”. The Default Packet Handling options give you the option to block the source of any unhandled packet. This is an extremely aggressive security setting and is not enabled by default.

**Automatically Block the Source of Suspicious Traffic**

The Blocked Sites feature helps prevent network traffic from systems you know or think are a security risk. After you identify the source of suspicious traffic, you can block all the connections to and from that IP address. You can also configure the Firebox to send a log message each time the source tries to connect to your network.

A blocked site is an IP address that cannot make a connection through the Firebox, even if the IP address is usually allowed to connect as part of your policy configuration. If a packet comes from or is sent to a system that is blocked, it does not get through the Firebox. There are two types of blocked IP addresses:

- **Permanent Blocked Sites** — IP addresses that you manually add to the Firebox configuration file because you want all connections to and from the IP address blocked. You may want to add an IP address to the Permanent Blocked Sites list if it consistently and repeatedly tries to violate your security policies.

- **Auto-blocked sites** — IP addresses that the Firebox adds to, and removes from, a Temporary Blocked Sites list based upon the packet handling rules specified in your Firebox configuration. These IP addresses are blocked for a period of time you control. This feature is known as the Temporary Blocked Sites list. For example, you can configure the Firebox to add an IP address to the Temporary Blocked Sites list if you select the auto-block option in a policy set to deny traffic. If a connection is blocked by your default packet handling rules, the source IP address is also added to the Temporary Blocked Sites list.

You can use the Temporary Blocked Sites list with log messages to help make decisions about which IP addresses to block permanently.

**Block Ports Commonly Used by Attackers**

Another method to protect the network is to block all traffic on ports commonly used by attackers. As attackers become more creative, this method has become less effective. However, it can still be used to protect against some of the most obvious vulnerabilities. Because a blocked port overrides all other service configurations, it can protect you from errors to your Firebox configuration. It can also be used to make independent log entries for probes against sensitive services.

With the default configuration, the Firebox blocks some destination ports. This gives a basic configuration that you usually do not have to change. It blocks TCP and UDP packets for these ports:

<table>
<thead>
<tr>
<th>Port(s)</th>
<th>Service</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>NONE</td>
<td>Firebox always blocks this port and you cannot override this default.</td>
</tr>
<tr>
<td>1</td>
<td>TCPmux (infrequently)</td>
<td>Block to make it more difficult for port scanning tools.</td>
</tr>
<tr>
<td>111</td>
<td>RPC</td>
<td>Used by RPC Services to find out which ports a RPC server uses. These are easy to attack through the Internet.</td>
</tr>
<tr>
<td>513, 514</td>
<td>rlogin, rsh, rcp</td>
<td>Because they give remote access to other computers, many attackers probe for these services.</td>
</tr>
<tr>
<td>2049</td>
<td>NFS</td>
<td>New versions of NFS have important authentication and security problems.</td>
</tr>
<tr>
<td>6000 – 6005</td>
<td>X Window System</td>
<td>Client connection is not encrypted and dangerous to use over the Internet.</td>
</tr>
<tr>
<td>7100</td>
<td>X Font Server</td>
<td>X Font Servers operate as the super-user on some hosts.</td>
</tr>
<tr>
<td>8000</td>
<td></td>
<td>Used by many vendors whose software is vulnerable to a variety of attacks.</td>
</tr>
</tbody>
</table>
Exercise 1: Configure Default Packet Handling Options

Successful Company just signed a sponsorship of the popular podcast Diggnation. Surprisingly, the publicity generates an unusually high volume of traffic to their public web server. So high in fact that the Firebox® mistakenly interprets the requests as a Distributed Denial of Service (DDoS) attack. In this exercise, we increase the Per Server Quota threshold to prevent this problem.

1. From Policy Manager, open the configuration file you are editing for these exercises.
2. Select Setup > Default Threat Protection > Default Packet Handling. The Default Packet Handling dialog box appears.
3. Under the Distributed Denial-of-Service Prevention section in the Per Server Quota text box, type 200. This doubles the amount of connections that the Firebox allows before it triggers a DDoS block on additional connections.

4. Click OK.
Exercise 2: Block Potential Sources of Attacks

The network administrator at Successful Company is more and more confident that his Firebox® configuration policy is strong, strict, and effective at blocking most access to their network. However, the log files suggest that more can be done to reduce the impact of direct attacks on the performance of the firewall. He starts with blocking the potential sources of attacks.

Block a site permanently

The Successful Company network administrator has been driven to distraction recently by a script kiddy using addresses in the 192.136.15.0/24 network to run probes of the Successful network. In this exercise, we permanently block all connections from that network.

1. From Policy Manager, select Setup > Default Threat Protection > Blocked Sites.
   The Blocked Sites Configuration dialog box opens.
2. On the Blocked Sites tab, click Add.
   The Add Site dialog box opens.
3. Use the Choose Type drop-down list to select Network IP. In the Value text box, type 192.136.15.0/24. In the Comment field, you can type a comment if you want. The comment is optional.
   The member type shows if this is an IP address or a range of IP addresses. When you type an IP address, type all the numbers and the periods.
4. Click OK.
   The entry appears in the Blocked Sites list. With this configuration, the Firebox blocks all packets to and from the 192.136.15.0/24 network range.

Create exceptions to the Blocked Sites list

An exception is an entry for which all other rules do not apply. For blocked sites, an exception is an IP address or network address that is never blocked. The automatic rules do not apply for this host. The rule also takes precedence over the manually blocked sites list.

In this exercise, we will add an exception to the 192.136.15.0/24 network we blocked in the exercise above. We will configure the Firebox to allow connections to and from the single IP address: 192.136.15.22.

1. On the Blocked Site Configuration dialog box, click the Blocked Sites Exceptions tab.
2. Click Add.
   The Add Site dialog box appears.
3. Use the Choose Type drop-down list to select Host IP. In the Value text box, type 192.136.15.22. In the Comment field, type Joe’s home IP.
   The Comment is optional but it can help you—and further network administrators configuring your Firebox—to figure out why an exception was made.
4. Select **OK**.

5. Click **OK** again to close the **Blocked Sites Configuration** dialog box.
Exercise 3: Block sites automatically

After reading a LiveSecurity Foundations article, the Successful Company network administrator decides to deny all RSH (Remote Shell) connections. In addition, he would like to automatically block the source of any incoming attempts to use RSH.

1. From Policy Manager, select Edit > Add Policy. Expand the Packet Filters folder. Click RSH. Click Add.
   The New Policy Properties dialog box appears.

2. Use the RSH Connections are drop-down list to select Denied. Configure the policy to deny connections:
   - From: Any-External
   - To: Any-Trusted, Any-Optional, Any-BOVPN

3. Click the Properties tab. Select the Auto-block sites that attempt to connect check box.

4. Click OK.
   The Firebox now automatically adds the IP address of any source of RSH packets to the Blocked Sites list. With a default configuration, the IP address stays on the Blocked Sites list for 20 minutes.
Related Courseware and Information

You can use these resources for more information on how to work with the email proxies.

**WatchGuard® System Manager User Guide**

**WatchGuard LiveSecurity® Online Resources**
Browse to [https://www.watchguard.com/support/faqs/fireware/](https://www.watchguard.com/support/faqs/fireware/).
Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. True or False: A firewall-based IPS maintains a database of character strings that match known viruses and worms.

2. Select the type of intrusion prevention measure for each Fireware feature?
   - A) Gateway AntiVirus Firewall-Based | Signature-Based
   - B) Default Packet Handling Firewall-Based | Signature-Based
   - C) Blocked Sites Firewall-Based | Signature-Based
   - D) IPS Service Firewall-Based | Signature-Based
   - E) Blocked Ports Firewall-Based | Signature-Based

3. Which of these actions does the Firebox® perform when it looks for patterns that show if your network is at risk (select all that apply):
   - □ A) Looks for packets which are not RFC compliant
   - □ B) Automatically blocks all traffic to and from a source IP address
   - □ C) Sends a log message to the Log Server
   - □ D) Sends a notification of possible security risks
   - □ E) All of the above

4. True or False: An unhandled packet is a packet that does not match any rule created in Policy Manager.

5. Fill in the blank: To block all traffic to and from a network, you add the address to the Blocked ______ list.
ANSWERS

1. False - A signature-based IPS maintains a database.
2. Gateway AntiVirus - Signature; Default Packet Handling - Firewall; Blocked Sites - Firewall; IPS Service - Signature; Blocked ports - Firewall
3. All the above
4. True
5. Sites
Signature Services

Signature-based virus and intrusion prevention

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak /Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Signature Services</td>
</tr>
</tbody>
</table>

What You Will Learn

The WatchGuard® Gateway AntiVirus/Intrusion Prevention Service (Gateway AV/IPS) is a signature based intrusion prevention system that identifies and stops possible viruses and intrusions. In this module, you are shown how to:

- Understand how signature services work to protect your network
- Set up and configure Gateway AntiVirus
- Set up and configure the Intrusion Prevention Service

Before you do the exercises, be sure to read and become familiar with the information in the “Getting Started” and “Threat Protection” training modules found at:

http://www.watchguard.com/training/courses.asp

In this module, you will configure an optional feature of the Firebox®. To view these settings, you must first purchase a feature key for Gateway AntiVirus/Intrusion Protection Service. In addition, to activate the key you must have access to a Firebox. If you take this course with a WatchGuard Certified Training Partner, your instructor will provide you with both a Firebox and a feature key.

Identify and Stop Viruses at the Edge of Your Network

In the “Threat Protection“ training module, we learned that the Firebox® includes ways to secure your network from zero-day threats using tools such as blocked sites, blocked ports, and default packet handling options. Often, these threat protection measures protect your network but at the cost of closing off an entire port and protocol. In our example, we turned off all RSH traffic to protect the Successful Company network from an RSH exploit. While this method is very effective, it is not generally a good long term solution. Yet, it may be weeks, even months, before a vendor builds a patch to fix the vulnerability.

In the interim, you can use a signature-based service to identify and block the exploit code while otherwise allowing the traffic. Signature-based protection services are much quicker for a vendor to
WatchGuard Gateway AntiVirus/IPS protects against two categories of threats:

- **AntiVirus** — Identifies viruses and trojans brought into your network through email, web browsing, TCP connections, or FTP downloads.
- **IPS** — Identifies direct attacks on your network applications or operating system.

**AntiVirus Scans User Traffic for Viruses and Trojans**

WatchGuard® Gateway AntiVirus scans different types of traffic according to which proxy or proxies you use the feature with:

- Email — With the SMTP or POP3 proxy, Gateway AntiVirus finds viruses encoded with frequently used email attachment methods. These include base64, binary, 7-bit, 8-bit encoding, and uuencoding.
- Web — With the HTTP proxy, Gateway AntiVirus scans web pages and any files that are downloaded from web pages for viruses.
- TCP — With the TCP proxy, Gateway AntiVirus can scan HTTP traffic on dynamic ports. It recognizes that traffic and forwards it to the default or user-defined HTTP proxy to perform antivirus scanning.
- FTP — With the FTP proxy, Gateway AntiVirus finds viruses in uploaded or downloaded files.

Note: Signatures for Gateway AntiVirus are not automatically updated by default. To make sure Gateway AntiVirus has current signatures, either enable automatic updates for the Gateway AntiVirus server, or use the Security Services tab of Firebox System Manager to manually update the signatures.

**Configuring 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 or TCP proxies), or uploaded or downloaded files (FTP proxy). The options for antivirus actions are:

**Allow**

Allows the packet to go to the recipient, even if the content contains a virus.

**Lock (SMTP and POP3 proxies only)**

Locks the attachment. A file that is locked cannot be opened 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 on how to unlock a file locked by Gateway AntiVirus, see the *WSM User Guide*. 
Identify and Stop Viruses at the Edge of Your Network

**Remove (SMTP and POP3 proxies only)**
Removes the attachment and allows the message and any other safe attachments 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.

In addition, Gateway AntiVirus can scan traffic that matches rules in several categories in each proxy. From the Categories list on the left side of the Proxy Configuration window, click one of the following categories to get access to these rule sets:

<table>
<thead>
<tr>
<th>FTP Proxy</th>
<th>SMTP Proxy</th>
<th>POP3 Proxy</th>
<th>HTTP Proxy</th>
<th>TCP-UDP Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download</td>
<td>Content Types</td>
<td>Content Types</td>
<td>Requests:</td>
<td>Requests:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>URL Paths</td>
<td>URL Paths</td>
</tr>
<tr>
<td>Upload</td>
<td>File names</td>
<td>File names</td>
<td>Responses:</td>
<td>Responses:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Content Types</td>
<td>Content Types</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Responses:</td>
<td>Responses:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Body Content Types</td>
<td>Body Content Types</td>
</tr>
</tbody>
</table>

**Using Gateway AntiVirus with compressed files**
In the Gateway AntiVirus configuration settings, you can select the number of compression levels to scan in a file during virus scan. 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 Firebox could send traffic too slowly. Gateway AntiVirus supports the scanning of up to six compression levels. If Gateway AntiVirus detects that the archive depth is greater than the value set in this field, it generates a scan error for the content.

The Firebox cannot scan encrypted files or files that use a type of compression that we do not support such as password-protected Zip files.

**Intrusion Prevention Service Blocks Direct Attacks**
An intrusion is when someone launches a direct attack on your computer. Usually the attack exploits a vulnerability in an application or operating system. These attacks are created to cause damage to your network, get sensitive information, or use your computers to attack other networks.

The Intrusion Prevention Service includes a set of signatures associated with specific commands or text found in commands that could be harmful. The Intrusion Prevention Service works together with all Firebox proxies.

When you enable IPS in a proxy policy, you can select from the following actions:

- **Allow**
  Allows the packet to go to the recipient, even if the content matches a signature.

- **Deny**
  Drops the packet and sends a TCP reset packet to the sender.

- **Drop**
  Drops the packet and drops the connection. No information is sent to the sender.

- **Block**
  Blocks the packet, and adds the source of the IP address to the Blocked Sites list.

Before you use IPS in a proxy policy, you must run the Activate Intrusion Prevention wizard to activate this feature and create a basic configuration.
Exercise 1: Automate Gateway AntiVirus/IPS Status and Updates

Automatic updates for Gateway AntiVirus are not enabled by default. You can enable automatic updates for Gateway AntiVirus. You can also update signatures.

To enable automatic updates, go to Tasks > Gateway Antivirus > Configure. Click the Update Server button and select the Enable automatic update check box. You can choose to check for updates to the Gateway AntiVirus signatures, IPS signatures, and the GAV engine.

You can also update signatures or the engine manually from Firebox System Manager on the Security Services tab. On this same tab, you can see the status of Gateway AntiVirus/IPS and information about signature versions.

Exercise 2: Setup Gateway AntiVirus

The Successful Company CIO decides to invest in signature-based intrusion prevention measures. The network administrator recommends WatchGuard® Gateway AntiVirus/IPS. Because the service is both cost effective and the WatchGuard system familiar, the expense is approved. In this exercise, we will activate Gateway AntiVirus and configure it to automatically get updates.

Activate Gateway AntiVirus

After the network administrator adds the feature key and saves it to the Firebox, he opens Policy Manager to activate the service.

1. From Policy Manager, select Tasks > Gateway AntiVirus > Activate. The Activate Gateway AntiVirus Wizard appears.
2. Click Next.
   If you are working through the training modules sequentially, using the SignatureServices-Start configuration file, or taking the class with an instructor, you should have several email, web, and FTP policies configured.
3. Clear the HTTP-Public-Servers policy. Click Next.
4. Click Finish.
Configure Gateway AntiVirus
Now, we enable decompression and enter the location of the Gateway AntiVirus signature database.

1. When the wizard is complete, select **Tasks > Gateway AntiVirus > Configure**. The Gateway AntiVirus dialog box appears and shows your proxy policies and whether Gateway AntiVirus is enabled.

2. Click **Settings**. The Gateway AV Decompression Settings dialog box appears.

3. Select the **Enable Decompression** check box. Make sure the number of levels to scan to is set to 3.

4. Click **OK**. Click **Update Server**. The Update Server dialog box appears.

5. By default, the Firebox automatically updates signature database files every hour. Increase the **Interval** to 3 hours.
6. Click OK. Click OK again to close the Gateway AntiVirus dialog box.
You must save your changes to the Firebox before they take effect.

Exercise 3: Configure a SMTP proxy policy for Gateway AntiVirus

Now that the Gateway AntiVirus service is activated for all email proxies and the signature database updated every three hours, we must configure each the actions we want the Firebox® to take when an exploit is detected. If you have more than one proxy policy, you must configure each.

In this exercise, we will configure the Successful Company SMTP-Incoming-Proxy policy to:

- Drop emails with attachments that contain viruses
- Allow attachments that cannot be scanned
- Enable the automatic content type detection feature

Automatic content type detection can improve virus detection rates. Often, the content type value that appears in an email header is set incorrectly by email clients. With this feature enabled, the SMTP proxy tries to verify the content type of email attachments itself.

1. From Policy Manager, select Tasks > Gateway AntiVirus > Configure. The Gateway AntiVirus dialog box appears. Make sure there is an SMTP proxy policy present in your configuration. If not, close this dialog box and go to Edit > Add Policies and add an SMTP proxy policy to your configuration before you continue.


3. From the When a virus is detected drop-down list, select Remove.

4. From the When a scan error occurs drop-down list, select Allow. Select the Alarm check box.

5. From the Category list on the left, select Attachments > Content Types. Select the Enable content type auto detection check box.

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.
examines the content, it uses the value stated in the email header, as it would if content type auto detection were not enabled.

6. Click OK to close the Gateway AntiVirus Configuration dialog box. Click OK again to close the Gateway AntiVirus dialog box.

Exercise 4: Configure the Intrusion Prevention Service

The Successful Company network administrator is dismayed to learn that employees accidentally downloaded a nasty “bot” virus through the file sharing features of a popular instant messenger client. In this exercise, we will activate the Intrusion Prevention Service and then configure the employee HTTP policy to deny the use of instant messenger and peer-to-peer applications.

Activate Intrusion Prevention
1. From Policy Manager, select Tasks > Intrusion Prevention > Activate. The Activate Intrusion Prevention Wizard starts.
2. Click Next.
3. Clear all proxies except HTTP-Employees. Click Next. The Advanced Intrusion Prevention settings panel appears.
4. Click Finish.

Related Courseware and Information

You can use these resources for more information on how to work with the optional WatchGuard® signature services.

WatchGuard® System Manager User Guide
Browse to http://www.watchguard.com/help/documentation/ and download the WSM User Guide. See the “Gateway AntiVirus/IPS” and “Proxies” chapters.
WatchGuard LiveSecurity® Online Resources
Browse to https://www.watchguard.com/support/faqs/fireware/
Test Your Knowledge

1. Match the proxy action with the correct description of what the Firebox does:

   A) **Allow**  
   Delete the attachment, send nothing to the sender or recipient, and add the sender to the Blocked Sites list.

   B) **Lock**  
   Delete the attachment, send nothing to the recipient and send nothing to the sender.

   C) **Remove**  
   Not a Fireware proxy action.

   D) **Drop**  
   Let the attachment go to the recipient even if it contains a virus.

   E) **Block**  
   Remove the attachment and delete it while sending the message to the recipient.

   F) **Send**  
   Encode the attachment so that the recipient cannot open it without a network administrator.

2. True or False: Gateway AntiVirus can look for viruses in uuencoded email.
   - Answer: True

3. True or False: Gateway AntiVirus can look for viruses in password-protected Zip files.
   - Answer: False

4. True or False: The Intrusion Prevention Service works only with the HTTP and TCP proxies. It cannot look for possible intrusions in the SMTP, POP3, DNS, or FTP proxies.
   - Answer: False

5. True or False: By default, the Firebox checks for new Gateway AntiVirus/IPS signature updates every hour.
   - Answer: False
Mobile VPN

Securely Connect Mobile Users

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak / Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Mobile VPN</td>
</tr>
</tbody>
</table>

What You Will Learn

WatchGuard® System Manager offers three methods to securely connect mobile users to your corporate network. In this training module, you will be shown how to:

- Select the mobile VPN type(s) appropriate for your network
- Configure the Firebox to allow mobile VPN connections
- Prepare mobile VPN end-user profiles
- Install and use the Mobile VPN client on a remote device

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

In this module, you will connect to one or more Firebox devices. If you take this course with a WatchGuard Certified Training Partner, your instructor will provide the IP address and passphrases for devices used in the exercises. For self-instruction, you can safely connect to a Firebox on a production network. It is helpful to conduct a portion of this exercise from a computer connected to the external network.

Connect Remote Users Securely to the Corporate Network

Mobile VPN allows telecommuters and traveling employees to connect to the corporate network while maintaining privacy and security. WatchGuard® System Manager 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 must configure the Firebox® and then the remote client computers. You use Policy Manager to enter the settings for each end user or group of users. Policy Manager makes an end
user profile configuration file that includes all the settings necessary to connect to the Firebox. You also configure your policies to allow or deny traffic from Mobile VPN clients. Mobile VPN users authenticate either to the Firebox user database or to an external authentication server. This module uses the Firebox authentication server to illustrate the process.

**Types of Mobile VPN**

WatchGuard System Manager includes three types of mobile VPN based on the protocol used to establish and encrypt a connection:

- **IPSec** — Internet Protocol Security
- **PPTP** — Point-to-Point Tunneling Protocol
- **SSL** — Secure Sockets Layer

While there are subtle advantages and disadvantages to each method, the selection of Mobile VPN type largely depends on your existing infrastructure and your network policy preferences. Configuration and system requirements on both the Firebox and the client side are similar. The Firebox can manage all three types of mobile VPN simultaneously. A client computer can be configured with one or all three methods.

One consideration that may drive your selection of mobile VPN protocol is compatibility with types of authentication. This table summarizes the types of authentication supported by each form of mobile VPN:

<table>
<thead>
<tr>
<th>Mobile VPN</th>
<th>Firebox</th>
<th>RADIUS</th>
<th>Vasco RADIUS</th>
<th>Vasco Challenge Response</th>
<th>RSA SecurID</th>
<th>LDAP</th>
<th>Active Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes¹</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PPTP</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SSL²</td>
<td>Yes</td>
<td>Yes³</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. RADIUS Group Attribute currently not supported by Vasco. Work around available via Microsoft® IAS Radius plug-in.
3. Entering the wrong password might lock out a user.

**Enabling the Firebox for Mobile VPN**

To configure the Firebox to accept connections from remote users, you must complete these steps:

**Activate Mobile VPN**

By default, the Firebox does not allow remote users to connect to protected resources on the trusted and optional networks. To allow these types of connections, you must first activate the form of Mobile VPN on the Firebox. In the case of SSL and PPTP, this is a single checkbox. With IPSec, you must also create client configuration files.

**Define settings**

Each type of Mobile VPN includes settings such as encryption method and keep alive interval. These settings are unique for each type. For example, only PPTP requires the configuration of a range of IP addresses on the trusted network for PPTP clients.

**Select and configure authentication**

Before connecting to resources on the company network, remote users must authenticate. You can select an authentication method for each type of Mobile VPN.

**Configure policies**

Even though the Mobile VPN connection is secure, you may want to limit access to trusted and optional networks through the Mobile VPN tunnel. Remote users are automatically added to the groups SSLVPN-Users, PPTP-Users, or IPSec-Clients as appropriate. You can use these groups to configure Firebox policies.
Distribute client software
Mobile VPN with IPSec requires that you distribute client software and an end-user profile to each remote user. The end-user profiles generated by the Policy Manager when you configure the Firebox. The client software is available on the WatchGuard web site.

Exercise 1: Set Up Mobile User VPN with PPTP

Successful Company starts with just a few mobile users and decides to try the PPTP client built into the Windows operating system on their laptop computers. It requires more configuration than the alternatives, but it is a good way to start implementing a company network policy which includes remote users.

Activate PPTP on the Firebox

First, we must activate PPTP on the Firebox. During this process, you must also define an address pool which can be used by PPTP users while connected.

1. From Policy Manager, open the configuration file you are editing for these exercises.
2. Select **VPN > Mobile VPN > PPTP**. The Mobile User VPN with PPTP Configuration dialog box appears.
3. Select the **Activate Mobile VPN with PPTP** checkbox.
4. Under the **IP Address Pool** list, click **Add**.
The Add Address dialog box appears.

5. Use the **Choose Type** drop-down list to select **Host Range**.
The dialog box changes to permit the entry of two IP addresses.

6. In the **Value** address field, type 10.0.1.50. In the **To** address field, type 10.0.1.74.
This sets a range of IP addresses for use by PPTP remote users while connected. You can configure 50 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. You must add at least two IP addresses for PPTP to operate correctly.

7. Click **OK**.

8. Click **OK** again to close the Mobile VPN with PPTP Configuration dialog box.

**Restrict PPTP users by policy**

When we activated Mobile VPN with PPTP, Policy Manager automatically created a policy to allow all traffic to resources on the trusted and optional networks. If you want to restrict the resources that PPTP users can connect to, you can create policies and use the PPTP-Users group name in your policies to allow specific types of traffic. There is an exercise in how to restrict traffic by policies in the Mobile VPN with SSL section to demonstrate this idea.

**Exercise 2: Configuring the Firebox for SSL VPN**

For security and ease of use, many organizations use Mobile VPN with SSL. With Mobile VPN with SSL, SSL users connect to the Firebox on TCP port 4100 and the client software and a client profile are automatically downloaded to their computer. The client software is also available on the WatchGuard web site. This is important for users who cannot access the Firebox on port 4100. A Firebox administrator can download the client software and make it available to those users as needed.

In this exercise, we activate the Firebox for Mobile VPN with SSL and create a policy to restrict SSL VPN user access.
Activate the Firebox for SSL VPN
1. From Policy Manager, select **VPN > Mobile VPN > SSL**. The Mobile VPN with SSL Configuration dialog box appears.

2. Select the **Activate Mobile User VPN with SSL** check box.
3. Use the **Authentication Server** drop-down list to select Firebox-DB.
4. Select the **Force all client traffic through the tunnel** check box.
   This ensures that all traffic both to and from the remote user laptop computers must pass through the Firebox. This method is more secure, however it uses more processing power and bandwidth on the Firebox.

Restrict SSL VPN users by policy
When we activated Mobile VPN with SSL, Policy Manager automatically created a policy to allow all traffic to resources on the trusted and optional networks. In this exercise, the Successful Company administrator decides to restrict this policy to allow traffic only to their email (SMTP) server. In a real world environment, the administrator might also want to open FTP and HTTP to internal servers.

1. From Policy Manager, click to select the **WatchGuard SSL VPN** policy.
   This policy was automatically created when we activated SSL VPN. This is an Any policy allowing all traffic from SSL VPN users to all resources on the trusted and optional networks.
2. On the toolbar, click **Delete Policy**. Click **Yes**.
   You can also select Edit > Delete Policy.
3. Select **Edit > Add Policy**. Expand the Proxies list and select **SMTP Proxy**. Click **Add**.
   You can use this policy to control access to the Successful Company SMTP server on the trusted network.
4. Under the From section, click Add. Click Add User. Use the Type drop-down list to select Firewall and Group. A list of Firebox authentication groups appears. Note that Policy Manager added both PPTP and SSL VPN.

5. Select SSL VPN-Users. Click OK.
6. Select Any-External and click Remove.
7. Click OK to close the Add Address dialog box.
8. Under the To section, click Add. Click Add Other. Use the Choose Type drop-down list to select Host IP.
9. Type the IP address of the SMTP server, 10.0.2.25. Click OK.

10. Click OK again to close the New Policy Properties dialog box.

Exercise 3: Prepare Mobile VPN End-User Profiles

With Mobile VPN with IPSec, the network security administrator controls end-user profiles. Policy Manager is used to configure a user group with Mobile VPN with IPSec access. For each user group with Mobile VPN with IPSec access, a Mobile VPN profile is created with the file extension *.wgx. The *.wgx file contains the shared key, user identification, IP addresses, and settings that are used to create a secure tunnel between the remote computer and the Firebox.
This file is encrypted with a key that is eight characters or greater in length. This key must be known by both the administrator and the remote user. When the *.wgx file is imported into the client software, the key is used to decrypt the *.wgx file.

The IPSec client allows you to deploy the software in a situation where the client does not have a static public IP address. This exercise shows you how to configure the Firebox and deploy the user profile for a new employee in the IT department of Successful Company.

As a member of the Marketing team force, Tim is constantly on the road. The Successful Company network administrator will make him a Mobile VPN profile so that he can connect securely to the Successful Company network.

1. From Policy Manager, select **VPN > Mobile VPN > IPSec**. The Mobile VPN with IPSec Configuration dialog box opens.
2. Click **Add**. The Add Mobile VPN with IPSec Wizard opens.
3. Click **Next**.
4. Select an authentication server from the **Authentication Server** drop-down list. You can authenticate users with the internal Firebox database (Firebox-DB) or with a RADIUS, VASCO, SecurID, LDAP, or Active Directory server. Make sure that this method of authentication is enabled in Policy Manager (select **Setup > Authentication > Authentication Servers**)
5. In the **Group Name** text box, type **Mobile Users**. The name can be an existing group that needs Mobile VPN access or a new group. Make sure the name is unique among VPN group names as well as all interface and tunnel names. With extended authentication, the group name must be identical to the group name on the external authentication server.
6. Click **Next**. For this tunnel, you authenticate using a passphrase. In the **Tunnel Passphrase** text box, type **successfulremote**. In the **Retype Passphrase** text box, type **successfulremote**.
7. Click **Next**. Click **Next** again to accept the default, less secure setting that allows your mobile users to bypass the VPN tunnel for Web traffic.
8. Click **Add**. In the **Add Address** dialog box, use the **Choose Type** drop-down list to select **Network IP**. In the **Value** text box, type 10.0.0.0/24. This will allow members of the Mobile Users group to access the Successful Company trusted network, 10.0.0.0/24.
9. Click **OK**. Click **Next**.
10. To enter the IP addresses that will be assigned to the mobile user connections, click **Add**.
11. Use the **Choose Type** drop-down list to select **Host IP** and enter 10.0.0.200. The IP address will be assigned to the Mobile VPN user when they connect to your network. The number of IP addresses should be the same as the number of Mobile VPN users. The IP addresses cannot be used by more than one Mobile VPN user at a time, or any device behind the Firebox.
12. Click **OK** and click **Next**.
13. Tim needs to be added to the Mobile Users group. Select **Add users to Mobile Users**. Click **Finish**. The Mobile VPN profile is saved in the folder: C:\Documents and Settings\All Users\Shared WatchGuard\muvpn\<IP address or name of Firebox>\Mobile Users\Mobile Users.wgx.
14. The **Authentication Servers** dialog box opens. Select the **Firebox** tab and click **Add** in the Users area. You can add or remove users at any time by selecting Setup > Authentication > Authentication Servers.
15. Enter Tim in the **User Information** area. You must enter a passphrase and confirm it.
16. Under **Available** in the **Firebox Authentication Groups** area, double-click **Mobile Users**. A user is a member of any group listed under **Member** in the Firebox Authentication Groups area.
17. Click **OK** to close the Setup Firebox User dialog box. Click **OK** again to close the Authentication Servers dialog box. In the **Mobile VPN with IPSec Configuration** dialog box, click **Advanced**.

### Setting Advanced Preferences
Advanced settings include assigning a virtual adapter rule and locking down the end-user profile so that users are able to see the settings but cannot change them. It is recommended that you lock down the profile...
because the VPN will fail if users make changes to the profile without corresponding changes made to the Firebox configuration.

To get name resolution for resources behind the Firebox, it is recommended that you configure WINS and DNS and require the virtual adapter. If you do not use a virtual adapter, the client will only have DNS from a static IP stack configuration or from the DHCP lease.

1. From the Remote Users Configuration dialog box, click Advanced.
2. To give mobile users only read-only access to their profiles, select the Make the security policy read-only in the MUVPN client check box.
3. Leave Virtual Adapter Settings of the Secure VPN Client as Required.
4. Click OK. Click OK again to close the Remote User Configuration dialog box. Policy Manager saves the changes to the Mobile Users *.wgx file.

**Exercise 4: Using the Mobile VPN with IPSec Client**

The Mobile VPN with IPSec client allows the remote computer to establish a secure, encrypted connection to a protected network over the Internet. To do this, you must first connect to the Internet and then use the Mobile VPN with IPSec client to connect to the protected network.

Before you install the client software, make sure the remote computer does not have any other IPSec mobile user VPN client software installed. You must also uninstall any desktop firewall software (other than Microsoft firewall software) from each remote computer. The Mobile VPN with IPSec client software includes firewall software for the remote computer and for the VPN connection.

In order to perform the installation process successfully, you must log into the remote computer with local administrator rights.

**Installing the Mobile VPN with IPSec Client**

The installation process consists of two parts: installing the client software on the remote computer and importing the end-user profile into the client. Before you start the installation, make sure you have the following installation components:

- The Mobile VPN with IPSec client installation file
- An end-user profile, with a file extension of .wgx
- Shared Key
- A .p12 certificate file (if you are connecting to a Firebox X Core or Peak and use certificates to authenticate)
- User name and password

**Install the Mobile VPN with IPSec client software**

1. Copy the Mobile VPN with IPSec client installation .zip file to the remote computer and extract the contents of the file.
2. Run the Mobile VPN executable file by double-clicking the .exe file extracted. This starts the WatchGuard Mobile VPN Installation wizard.
3. Restart your computer when the installation wizard completes.

When the computer restarts, the WatchGuard Mobile VPN Connection Monitor dialog box opens. 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 Assistant for generating a profile now?

Click No.
Import the end-user profile
1. Copy the end-user profile (the .wgx file) to the root directory on the remote (client or user) computer. If you use certificates to authenticate, copy the .p12 file to the root directory as well.
2. If it is not already running, start the WatchGuard Mobile VPN Monitor.
   In Windows, Start > All Programs > WatchGuard Mobile VPN, Mobile VPN Monitor.
3. Select **Configuration > Profile Import**. The Profile Import Wizard starts.
4. On the Select User Profile screen, browse to the location of the .wgx file. Click **Next**.
5. On the Decrypt User Profile screen, type the shared key. The shared key is case-sensitive. Click **Next**.
6. 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 re-import it. Click **Next**.
7. 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 type your user name and password here, the Firebox stores it and you do not have to enter this information each time you connect. However, this is a security risk. If you keep these fields clear, you are prompted to enter your user name and password the first time you connect. All future connections, the user name is saved from the last time a connection was made but the password must be entered. This can minimize the amount of data required for the VPN connection without creating a security risk. Click **Next**.

Connecting and Disconnecting the Mobile VPN with IPSec VPN
1. First, establish an Internet connection through either Dial-Up Networking or directly through a local area network (LAN) or wide area network (WAN).
2. If it is not already running, start the WatchGuard Mobile VPN Monitor.
   In Windows, Start > All Programs > WatchGuard Mobile VPN, Mobile VPN Monitor.
3. From the **Profile** drop-down list, select the name of the profile you created for your Mobile VPN connections to the Firebox. Click **Connect**.
4. To disconnect the VPN, click **Disconnect**.

Related Courseware and Information
You can use these resources for more information on how to use policies and proxies:

**WatchGuard System Manager User Guide**
Browse to [https://www.watchguard.com/help/documentation/](https://www.watchguard.com/help/documentation/) and download the *WSM User Guide*. See the chapters on “Authentication” and “Mobile VPN.”

**Reference Guide**
Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. True or False: Forcing all Internet traffic flow through an Mobile VPN tunnel consumes more processing power and bandwidth but makes the configuration more secure.

2. True or False: You are able to use the Mobile VPN client as soon as it is installed. There is no need to configure it.

3. A WGX file contains (select all that apply):
   - A) A shared key
   - B) User identification
   - C) IP addresses
   - D) Settings to create a secure tunnel
   - E) Administrator ID
   - F) All of the above

4. True or False: You can create policies that control Mobile VPN access.

5. Before installing the Mobile VPN with IPSec client software you must:
   - A) Authenticate to the Firebox to download the software.
   - B) Uninstall any existing VPN software of any kind.
   - C) Uninstall any existing IPSec client software.

6. Which of the following forms of mobile user VPN are supported by WatchGuard® System Manager (select all that apply):
   - A) Active Directory
   - B) IPSec
   - C) LDAP
   - D) PGP
   - E) PPTP
   - F) SCP IRC
   - G) SSH
   - H) SSL VPN
Manual BOVPN

Manually Creating Branch Office Tunnels

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak /Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware® and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Manual BOVPN</td>
</tr>
</tbody>
</table>

What You Will Learn

This module shows you how to create branch office VPN (BOVPN) tunnels. After you finish this section, you will know how to:

- Understand when to use Policy Manager to create BOVPNs
- Create a BOVPN gateway
- Create a BOVPN tunnel
- Make tunnel policies

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

About Manual BOVPNs

Virtual private networks (VPNs) use encryption technology to decrease security risks and to protect private information on the public Internet. A virtual private network lets data flow safely across the Internet between two networks. VPN tunnels are also secure connections between a host and a network. The networks and hosts at the endpoints of a VPN can be corporate headquarters, branch offices, and remote users.

VPN tunnels use authentication, which examines the sender and the recipient. If the authentication information is correct, the data is decrypted. Only the sender and the recipient of the message can read the data clearly. A branch office VPN (BOVPN) is an encrypted connection between two dedicated, hardware devices. It is used most frequently to make secure network communications between two offices. A remote user VPN is an encrypted connection between a dedicated hardware device and a laptop or desktop computer.

WatchGuard Fireware supports many types of virtual private networking. With Fireware, you can configure a branch office VPN manually with Policy Manager. You can also use WatchGuard System Manager to quickly create centrally managed VPNs. In this training module, you learn more about manually configured branch office VPN tunnels.
When to use Policy Manager to create BOVPNs

Although you can use an easy drag-and-drop procedure to create managed tunnels in WatchGuard System Manager, it is not possible or practical to do this in these situations:

- VPN tunnels where the other end of the BOVPN is not a WatchGuard Firebox. Instead, it is an IPSec-compliant firewall or VPN device manufactured by some other company.
- You do not have a computer to use as a Management Server.
- You have only a small number of VPN tunnels to create. The time to manually define the BOVPN is less than the time it takes to configure a Management Server and the Fireboxes to work with the Management Server.

Steps to make a BOVPN tunnel with Policy Manager

When you create a branch office VPN tunnel with Policy Manager, you must:

- Add and configure a VPN gateway
- Create a VPN tunnel
- Create a VPN tunnel policy
- Configure the other endpoint of the VPN tunnel with the same VPN gateway and tunnel parameters

In this training module, you create a BOVPN tunnel with Policy Manager for the company called My WatchGuard. The company recently opened an office in Beijing, which is protected by a Firebox X750e. The sales people in Beijing must connect to the My WatchGuard CRM (Customer Relations Management) database, which is accessible through a web client on port 80. For security reasons, they do not want the sales people to have full access to the network behind their My WatchGuard Firebox X8500e.

Exercise 1: Configure a VPN Gateway

A gateway is a connection point for one or more VPN tunnels. Internet Security Association and Key Management Protocol (ISAKMP) is a protocol to authenticate network traffic between two devices. The VPN gateway contains the Phase 1 ISAKMP settings, which include the information that a device needs to make an authenticated and encrypted VPN tunnel with another device.

To start IPSec tunnel negotiation, one VPN endpoint must connect to the other. To create a manual VPN tunnel, you create a VPN gateway at each endpoint.

In this exercise, you configure the VPN gateway on the My WatchGuard Firebox to look for the remote gateway at the new Beijing office. The Beijing Firebox has a static external IP address of 50.50.50.50.

1. Start WatchGuard System Manager and connect to the My WatchGuard Firebox. Start Policy Manager.
   For this training module, open or create a policy that has an external network IP address of 100.100.100.100/24 and an optional network IP of 10.0.2.1/24. The network interfaces must be configured to follow the instructions in this module.
2. Select **VPN > Branch Office Gateways**. Click **Add**.
The New Gateway dialog box opens.

![New Gateway dialog box]

3. In the **Gateway Name** text box, type **BeijingGateway**.
   This name identifies the gateway only in Policy Manager.

4. On the **General Settings** tab, in the **Credential Method** section, select **Pre-Shared Key**.
   Type **xtm8virus** as the pre-shared key. You must use the same pre-shared key in the configuration of the remote device gateway.
   If you select to authenticate with certificates, you must start the Certificate Authority on your WatchGuard Management Server. See the *WatchGuard System Manager User Guide* or online Help for more information.
5. In the **Gateway Endpoints** section, click **Add**.
The New Gateway Endpoints Settings dialog box opens.

6. Use the following information in the **Local Gateway** and **Remote Gateway** fields:

<table>
<thead>
<tr>
<th>Gateway Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Gateway</td>
<td>100.100.100.100</td>
</tr>
<tr>
<td>Remote Gateway</td>
<td>50.50.50.50</td>
</tr>
</tbody>
</table>

7. In the **Local Gateway** section, select **By IP Address**. Type the external IP address of the My WatchGuard Firebox: 100.100.100.100. You can also click the drop-down menu for a list of the IP addresses of all active interfaces on the Firebox. This is the IP Address that the Beijing office Firebox will use to connect. If you select to authenticate with certificates, you must start the Certificate Authority on your WatchGuard Management Server. See the *WatchGuard System Manager User Guide* or online Help for more information. WatchGuard does not support the use of third-party certificates at this time.

8. In the **Remote Gateway** section, select **Static IP address**. Type the external IP address of the Beijing office, 50.50.50.50. For **Specify the gateway ID for tunnel authentication**, select **By IP address**. Type the external IP address of the Beijing office.

9. Click **OK** to return to the **General Settings** dialog box.
10. Click the **Phase1 Settings** tab.

11. From the **Mode** drop-down list, select **Main**.
   Main Mode protects the identities of the VPN endpoints during negotiation, and is more secure than Aggressive Mode. Main Mode also supports Diffie-Hellman group 2. However, Main Mode causes more messages to be sent between endpoints and is slower than Aggressive Mode. You must use Aggressive Mode when you configure VPN tunnels with a dynamic IP address at one VPN endpoint.

12. Clear the **NAT Traversal** check box.
   NAT Traversal uses UDP encapsulation to allow traffic to get to the correct destinations, even if VPN endpoint device addresses are changed by NAT. Because each My WatchGuard Firebox has a public static IP address and the default gateway routers are not configured to NAT connections to the external interface of the Firebox, the NAT Traversal Feature is not necessary. To keep the packet header size as small as possible to maximize VPN throughput, disable NAT Traversal when possible.

13. Select **IKE Keep-alive** or **Dead Peer Detection (RFC3706)**.
   Both IKE Keep-alive and Dead Peer Detection are methods to keep a tunnel connected and to identify whether a tunnel has become disconnected. A new Phase 1 negotiation starts when they identify that a tunnel is disconnected. If you select both IKE Keep-alive and Dead Peer Detection, the Phase 1 renegotiation started by one can cause the other to identify the tunnel as disconnected and start another new Phase 1 negotiation. To improve tunnel stability, choose one or the other and choose the same option when you configure each endpoint.

   **IKE Keep-alive** 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 Firebox tries to renegotiate the Phase 1 connection.

   **Dead Peer Detection** monitors tunnel traffic. 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 Firebox sends a query. If there is no response after the number of Max retries, the Firebox renegotiates
the Phase 1 connection. For more information about Dead Peer Detection, read http://www.ietf.org/rfc/rfc3706.txt.

14. In the Transform Settings area, keep the default settings to enable SHA1 authentication, 3DES encryption, and Diffie-Hellman Group 1 for Phase 1 IKE negotiation.

15. Click OK to save the gateway you have created. Click Close to close the Gateways dialog box.

Exercise 2: Define a VPN Tunnel

When you define a VPN tunnel with Policy Manager, you set the Phase 2 ISAKMP parameters, which include the authentication and encryption methods used to encrypt the data between your VPN networks.

The administrator of the Beijing office and the administrator of the central My WatchGuard Firebox have reviewed all available settings and are happy with most of the default settings included in the Policy Manager BOVPN tunnel configuration. They want to define a VPN tunnel that uses these settings.

1. From Policy Manager, select **VPN > Branch Office Tunnels**.
   The Branch Office IPSec Tunnels dialog box appears.

2. Click **Add**.
   The New Tunnel dialog box appears.

3. In the **Tunnel Name** text box, type BeijingCRMAccess.

4. Make sure the **Gateway** drop-down list is set to BeijingGateway.

**Addresses tab**

1. Click the **Addresses** tab.
2. Click Add to add a pair of IP addresses that communicate through the tunnel. The Tunnel Route Settings dialog box appears.

![Tunnel Route Settings](image)

3. In the Local text box, type the IP address of the CRM database server, 10.0.2.80. This is the only IP address behind the My WatchGuard Firebox that can communicate through this VPN tunnel. You can type the IP address directly in the text box, or you can click the button adjacent to the text box, select Host IP, and type the IP address.

4. In the Remote text box, type the trusted network address for the Beijing office, 192.168.111.0/24.
5. Make sure the tunnel direction shows as bidirectional. The bidirectional symbol is <==>.
6. Click OK.

**Phase 2 Settings tab**

1. Click the Phase 2 Settings tab.

![New Tunnel](image)

2. In the Perfect Forward Secrecy section, select PFS and Diffie-Hellman Group 1. Perfect Forward Secrecy (PFS) is enabled by default when you create a BOVPN tunnel. If the remote device does not support PFS or does not have PFS configured, you must clear this check box or tunnel negotiations will fail.
The default Diffie-Hellman group for both Phase 1 and Phase 2 is Diffie-Hellman group 1. This group provides basic security without sacrificing performance.

3. Do not change the **Security Associations (SA)** settings.
   You should not change the advanced SA settings unless the remote endpoint requires it. Some VPN endpoints need a separate SA for each tunnel route. The default setting for WatchGuard Fireboxes is one SA for all ports and protocols.

4. In the **IPSec Proposals** section, make sure **ESP-AES-SHA1** is listed. This default proposal is used for both Fireboxes.
   The Phase 2 IPSec proposals on each appliance must be identical. ESP-AES-SHA1 is the default Phase 2 IPSec proposal for Fireboxes that run current versions of Fireware.

5. Click **OK** to close the **New Tunnel** dialog box and return to the **Branch Office IPSec Tunnels** dialog box.

6. Click **Close**.

**Exercise 3: Make a Tunnel Policy**

Tunnel policies are sets of rules for tunnel connections. When you use Policy Manager to create a BOVPN tunnel, the software automatically adds an “Any” (BOVPN-Allow) policy. This policy allows connections using any port and any protocol between the two networks. You can delete this policy and create custom VPN policies to select the ports to allow, or to use a proxy policy to add more security.

**Allow only TCP port 80 through the BOVPN**

In this training exercise, the administrators want to restrict traffic through the VPN from the Beijing office to only HTTP connections to the company’s CRM database server. They want to use an HTTP packet filter to control the traffic on port 80 to the CRM server.

To restrict the traffic with an HTTP packet filter, you must first remove the tunnel from the default Any policies and then add the HTTP packet filter policy with the BOVPN Policy Wizard.

**Remove the tunnel from the Any policies**

1. In Policy Manager, select **VPN > Branch Office Tunnels**.
2. Select the BeijingCRM access tunnel and click **Edit**.
3. On the **Addresses** tab, clear the **Add this tunnel to the BOVPN-Allow policies** check box.
4. Click **OK**. Click **Close**.
   If there was more than one tunnel using the Any policies, the BeijingCRMAccess alias is removed from the policies. Because there is only the BeijingCRMAccess tunnel, the BOVPN-Allow.in and BOVPN-Allow.out policies are removed from the list of policies in Policy Manager.

**Add an HTTP policy with the BOVPN Policy Wizard**

1. In Policy Manager, select **VPN > Create BOVPN Policy**. Click **Next**.
   The BOVPN Policy Wizard starts.
2. The **Policy Name Base** will be the start of the names of the new policy. Choose a name that makes it easy for you to identify the policy and what it does. Type **BeijingCRMaccess-HTTP** and click **Next**.
3. In the **Select the policy type** dialog box, click **Choose**.
   The Select Policy Type dialog box appears.
4. Expand **Packet Filters**, select **HTTP** and click **Select**. Click **Next**.
   You can select only one policy in the BOVPN Policy Wizard. To add more policies to allow additional traffic, run the wizard again for each policy you want to add.
5. Click **Add**. Select the tunnel that the policy will allow traffic to pass through.
   To allow access to the CRM system from the Beijing office, select BeijingCRMAccess.
6. Click **OK**. The tunnel name is displayed. Click **Next**.

7. If you want to be able to use aliases for the tunnel traffic in other policies, select **Create aliases for the selected incoming and outgoing tunnels**. Click **Next**.
   Because only TCP port 80 traffic will pass through this tunnel to the CRM system, the aliases are not needed. Leave the check box clear.

8. The BOVPN Policy Wizard is complete and the policies created are listed. Click **Finish**.

The BOVPN Policy Wizard creates both an incoming (.in) and outgoing (.out) policy. The incoming policy applies to traffic when a device at the remote location starts a connection to a device on the local network. The outgoing policy applies to traffic when a local device starts a connection to a device at the remote location. You might not need both policies. You can delete any policy that the BOVPN Policy Wizard creates.

In the example, the My WatchGuard CRM system does not need to start connections out to client computers in the Beijing office. You can delete the BeijingCRMaccess-HTTP.out policy. The CRM system can respond to any connections from the Beijing office through the BeijingCRMaccess-HTTP.in policy.

**Related Courseware and Information**

You can use these resources for more information on how to create BOVPN tunnels:

- **WatchGuard System Manager User Guide**

- **WatchGuard Online FAQs**
  Browse to [http://www.watchguard.com/support/faqs/](http://www.watchguard.com/support/faqs/) and select the version of software you are using. See the “BOVPN Tunnels” section.

- **Reference Guide**
Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. True or False: When you create a BOVPN between a Firebox X700 and a Checkpoint firewall, you can use either a managed VPN tunnel created with the WatchGuard Management Server or a BOVPN tunnel created with Policy Manager.

2. Which BOVPN components must be configured exactly the same in the two endpoints of a BOVPN tunnel (select all that apply):
   - A) Remote gateway IP address
   - B) Pre-shared key
   - C) Gateway name
   - D) Authentication method
   - E) Encryption method
   - F) All of the above

3. True or False: You can import third-party certificates to use in BOVPN endpoint authentication.

4. When you configure the Phase 1 settings, what is the best way to help keep the tunnel connected and to identify if the tunnel has become disconnected?
   - A) Use IKE Keep-alives
   - B) Use Dead Peer Detection
   - C) Either A or B
   - D) Both A and B

5. True or False: The default configuration for a manual tunnel is to use an Any policy to allow all connections between the two endpoints.

6. Match the setting to the configuration task:
   1) Phase 1 authentication method  a) Configure a tunnel
   2) Restrict the protocols allowed through the tunnel  b) Configure a gateway
   3) Phase 2 encryption method  c) Edit Branch Office VPN policies
ANSWERS
1. False
2. B, D, E
3. False
4. C
5. True
6. 1=B, 2=C, 3=A
Managed BOVPN

Configure Managed VPN Tunnels

What You Will Learn

This module shows you how to create managed BOVPN tunnels. When you finish this section, you will know how to:

☐ Configure a Management Server
☐ Add Fireboxes to the Management Server configuration
☐ Create and use policy templates
☐ Create and use security templates
☐ Create a tunnel with the drag-and-drop method

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:

http://www.watchguard.com/training/courses.asp

In this module, you will connect to one or more Firebox devices. If you take this course with a WatchGuard Certified Training Partner, your instructor will provide the IP address and passphrases for devices used in the exercises. For self-instruction, you can safely connect to a Firebox on a production network. It is helpful to conduct a portion of this exercise from a computer connected to the external network.

Create Tunnels with the Management Server

With the WatchGuard Management Server, you can make fully authenticated and encrypted IPSec tunnels with a drag-and-drop or menu interface. The Management Server safely transmits IPSec VPN configuration information between Fireboxes and makes the task of creating IPSec VPN tunnels much easier than manual configuration.

With WatchGuard System Manager and a Management Server, you configure, manage, and monitor all WatchGuard devices across a company. You can create and manage VPN tunnels between Firebox X Peak, Firebox X Core, Firebox III, Firebox X Edge, and Firebox SOHO devices, even if the devices have dynamic IP addresses. The remote Fireboxes connect to the Management Server when they come online and download the VPN configuration information they need to configure their end of the VPN tunnel.

If you use certificates for tunnel authentication, you can configure the Management Server as a certificate authority to create certificates automatically.

Steps to create a managed VPN

• Set up a Management Server and (optional) certificate authority
• Add Fireboxes, or Firebox X Edge or SOHO devices to the Management Server configuration
• Configure the Fireboxes used in VPN tunnels as managed clients
In the following exercises, you create a managed branch office VPN (BOVPN) tunnel for My WatchGuard, a fictitious network security solutions company. My WatchGuard just purchased a Firebox X Edge for the vice president of the company. The VPN tunnel will connect the new Firebox X Edge to the primary My WatchGuard Firebox.

Here is the other information you must have to create a managed BOVPN tunnel:

- The vice president’s new Firebox X Edge is an X10e-W.
- The Edge gets its external IP through DHCP.

**Exercise 1: Set up a Management Server**

The WatchGuard Management Server keeps and distributes VPN configuration information for the Fireboxes it is configured to manage. It also acts as a certificate authority (CA) to issue certificates for VPN authentication. A certificate authority is an organization or application that issues and revokes certificates. In this case, the Management Server is a CA for all the Firebox devices that connect to it.

You install Management Server software using the WatchGuard System Manager installation files. It can be installed on your WatchGuard management station, or on a different computer on your network. Once installed, you use the Management Server Setup Wizard to complete the setup of the Management Server.

**Management Server passphrases**

When you use the Management Server Setup Wizard, you must give two different passphrases:

- **Master passphrase**
  This password is used to protect all the passphrases in the WatchGuard passphrase file on the hard drive of the Management Server. This prevents a person with access to this computer from getting the passphrases of all managed Fireboxes. This passphrase is not used frequently. We recommend that you write it down and lock it in a secure location.

- **Server management passphrase**
  This is the passphrase you use to connect to the Management Server from WatchGuard System Manager. This passphrase is used frequently.

**Management Server Setup Wizard**

1. On the WatchGuard toolbar, right-click the Management Server icon and select **Start Service**. The Management Server Setup Wizard starts.
2. Click **Next**.
3. Type the master passphrase `xtm8virus2`. Confirm the passphrase and click **Next**.
4. Type the server management passphrase `55555555`. Confirm the passphrase and click **Next**. The Identify the gateway Firebox dialog box appears.
5. Type the **IP Address**, **Status Passphrase**, and **Configuration Passphrase** for your gateway Firebox. Type the primary external IP address for **IP Address**. Click **Next**.
6. Type the license key for the Management Server. Click **Next**. Your instructor will give you this information.
7. Type the name of your organization as **My WatchGuard**. Click **Next**.
8. Click **Next**.
The wizard configures the Management Server.

9. Click **Finish**.

**Exercise 2: Add Fireboxes to the Management Server Configuration**

In order to create managed BOVPN tunnels between Fireboxes managed by the WatchGuard Management Server, you must register the Fireboxes in the Management Server configuration. To do this, you must connect to the Management Server from WatchGuard System Manager and add the information for the vice president’s Firebox X Edge.

1. Start WatchGuard System Manager and select **File > Connect to > Server**.
2. Type the **IP address**, **Name**, and **Passphrase** to connect to your Management Server. Click **Connect**. Your instructor has this information. The default name is admin.
3. From the **Device Management** tab, select **Edit > Insert Device**.
The WatchGuard Device Wizard starts.
4. Click **Next**.
The Enter the device’s IP address and passphrases dialog box opens.
5. Because the vice president’s Edge gets its external IP address through DHCP, you do not know the IP address. Select **I don't know the device's current dynamically allocated IP address (DHCP/PPPoE)**.
6. Click **Next**.
The Enter a name for the device dialog box appears.
7. Type **Vice_President-Home** as the client name for this device.
   This is a name that you select. It is not the same as the DNS name of the device.
8. From the **Device Type** drop-down list, select **Firebox X Edge (X10e, X10e-W,...)**.
9. Type **xtm8Uvirus** for the shared secret.
The Management Server will use the shared secret to authenticate to the managed Firebox X Edge. For authentication to work, you must type the same shared secret when you configure the Edge.
10. Click **Next**.
The **Enter the device’s status and configuration passphrase** dialog box appears. If the managed Firebox is a Firebox X Peak, Firebox X Core, or Firebox III, the passphrases you type here are the general WSM status and configuration passphrases for the Firebox. If the managed Firebox is a Firebox X Edge or SOHO, the passphrases you type here must be entered in the Edge/SOHO **Administration > VPN Manager** or **Administration > WSM Access** configuration page. Type these passphrases and click **Next**.

<table>
<thead>
<tr>
<th>Status passphrase</th>
<th>11111111</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration passphrase</td>
<td>22222222</td>
</tr>
</tbody>
</table>

11. Click **Next** to finish the wizard.

   If the external IP address of the Firebox is known, the Management Server connects to the Firebox, configures the Firebox and restarts it. Because we do not know the external IP address of the vice president’s Edge, the Edge will not be configured until it connects to the Management Server.

**Exercise 3: Configure a Firebox as a Managed Firebox Client**

To allow the Management Server to manage another Firebox, you must activate that Firebox as a managed client. The procedure to enable a Firebox as a managed client is different depending upon the type of Firebox. For Firebox III, Firebox X Core, and Firebox X Peak, you enable a Firebox as a managed client in Policy Manager. Select **VPN > Managed Client**. Identify the Management Server and set the shared secret.
In our example, My WatchGuard has a new Firebox X Edge to configure as a managed client. To do this:

1. Connect to the Edge System Status page by typing `https://` and the IP address of the Edge trusted interface in a Web browser address bar.
2. From the navigation bar on the left, select **Administration > WSM Access**. The WatchGuard Management Access page appears.
3. Select **Enable remote management**.
4. For **Management Type**, select **WatchGuard System Manager**.
5. Select **Use Centralized Management**.
6. Type and confirm the status and configuration passphrases to be used to allow the Management Server to make connections to the Firebox X Edge. These must match those you typed when you added the device to the Management Server configuration. These passphrases are:

<table>
<thead>
<tr>
<th>Status Passphrase</th>
<th>Configuration Passphrase</th>
</tr>
</thead>
<tbody>
<tr>
<td>11111111</td>
<td>22222222</td>
</tr>
</tbody>
</table>

7. Type the external IP of the Management Server’s gateway Firebox for the **Management Server Address**.
8. Type **Vice_President-Home** for the **Client Name**. This is a name that you select. It is not the same as the DNS name of the device.
9. Type **xtm8Uvirus** for the **Shared Secret**. This is the same shared secret you entered in the Management Server Setup Wizard.
10. Click **Submit**.

Before you continue with this set of exercises, the Firebox X Edge must be installed on the network external to the Firebox that protects the Management Server. If you look at WatchGuard System Manager while connected to the Management Server, the Edge must not have a red exclamation point next to it. A red exclamation point means that the Management Server cannot connect to the device.

**Exercise 4: Apply Policy Templates**

In a VPN, you configure (and limit) the networks that have access through the tunnel. To configure the networks available through a given VPN device, you make policy templates. A policy template defines the resources, networks, and services allowed through a VPN tunnel.

The WatchGuard Management Server adds a network policy template that gives access to the network behind a VPN device. This template is applied by default if a managed Firebox has a static IP address. If the device has a dynamic IP address, you can easily apply the template from WatchGuard System Manager after the managed device is available on the network.

In this exercise, the vice president’s Firebox X Edge has a dynamic IP address. As an officer of My WatchGuard, you allow the vice president full access to the computers protected by the Firebox.

1. On the WatchGuard System Manager **Device Management** tab, right-click **Vice_President-Home** and select **Update Device**.
   The Update Device dialog box appears.
2. Select the **Download Trusted and Optional Network Policies** check box.
3. Click **OK**.
4. Expand the **Devices** entries below **Vice_President-Home**. Right-click on **Trusted Network** or **Optional Network** and click **Properties**.
The Management Server copies the trusted and optional network ranges to its configuration as device resources for the managed Firebox. The resources for the managed Firebox are known collectively as a device template. Use the device template to create multiple VPN tunnels between this managed Firebox and other managed Fireboxes.

**Security templates**

A security template gives the encryption and authentication type for a tunnel. Security templates make it possible to set the encryption type and authentication type for the tunnel from the VPN wizard. WatchGuard recommends that you use the security template called Strong with Authentication when you create VPN tunnels. The properties of this security template are:

<table>
<thead>
<tr>
<th>Security Association Type</th>
<th>ESP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1 Encryption</td>
<td>DES-CBC</td>
</tr>
<tr>
<td>Phase 1 Authentication</td>
<td>MD5</td>
</tr>
<tr>
<td>Phase 2 Encryption</td>
<td>3DES-CBC</td>
</tr>
<tr>
<td>Phase 3 Authentication</td>
<td>SHA1-HMAC</td>
</tr>
</tbody>
</table>

You can also create your own security templates. Select **Edit > Insert Security Template** in WatchGuard System Manager.

**Exercise 5: Create Managed VPN Tunnels Between Fireboxes**

Now that the Management Server is able to connect to the vice president’s new Firebox X Edge, you can create a VPN tunnel between the Firebox X Edge and the My WatchGuard headquarters Firebox.

1. On the WatchGuard System Manager **Device Management** tab, click and hold down on the name of the first VPN endpoint: Vice_President-Home. Drag it to the device name of the My WatchGuard Firebox. The Add VPN Wizard starts.
2. The **Select the gateway devices** dialog box shows the two endpoint devices you selected. For each device, select the VPN resource you want to connect through the tunnel. In this exercise, select **Trusted Network** for both devices.
3. In the **Select the security template** dialog box, select **Strong with Authentication** from the **Security Template** drop-down list. Click **Next**.
4. In the **Select the VPN Firewall Policy Template** dialog box, select **Any** for the **VPN Firewall Policy Template**.
5. Click **Next**.
   The Add VPN Wizard is complete dialog box appears.
6. To save the settings for the new managed BOVPN to the Fireboxes, select **Restart devices now to download VPN configuration** and click **Finish**.

Related Courseware and Information

You can use these resources for more information on how to use policies and proxies:

**WatchGuard System Manager User Guide**

**WatchGuard Online FAQs**
Browse to [http://www.watchguard.com/support/faqs/](http://www.watchguard.com/support/faqs/) and select the version of software you are using. See the “BOVPN Tunnels” section.
Test Your Knowledge

Use these questions to practice what you have learned and to exercise new skills.

1. True or False: The master encryption passphrase is used to encrypt the connection between the Management Server and all managed devices.

2. Below is a list of steps to take when creating a managed VPN. Put them in order, from the first step to the last step, using the numbers 1 - 4:

   A) Use drag-and-drop to create a VPN tunnel
   B) Add devices to the Management Server configuration
   C) Complete the VPN Wizard
   D) Set up a Management Server

3. True or False: The Management Server also functions as a Certificate Authority.

4. True or False: You can use the Management Server to create a VPN tunnel between a Firebox X Core and an IPSec-compliant Checkpoint firewall.

5. Which of these security parameters are included in a security template (select all that apply):

   - A) Encryption algorithm
   - B) Security Association type
   - C) Shared Key
   - D) Authentication method
   - E) All of the above
ANSWERS

1. False
2. A=3, B=2, C=4, D=1
3. True
4. False
5. A, B, D
Traffic Management

Traffic Shaping and Prioritization

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak / Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware and Fireware Pro 10</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10</td>
</tr>
<tr>
<td>Training module</td>
<td>Traffic Management</td>
</tr>
</tbody>
</table>

What You Will Learn

Most organizations have mission-critical, real-time network applications that must take priority over other traffic. You can use bandwidth restrictions and reservations along with prioritization to make sure critical applications have the bandwidth they need. In this module, you are shown how to:

- Create Traffic Management actions
- Prioritize policies
- Guarantee and restrict bandwidth
- Use Service Watch to see your traffic management actions at work

Before you do the exercises, be sure to read and become familiar with the information in “Using the WSM/Fireware Training Modules,” available at:

http://www.watchguard.com/training/courses.asp

Control Bandwidth Use and Prioritize Traffic

Although the Firebox has no control over the rate at which packets arrive at a given interface, you can use traffic management settings to do the following:

- **Guarantee bandwidth.** A traffic management queue with reserved bandwidth and low priority can give bandwidth to real-time applications with higher priority when necessary to prevent connection timeout. Other traffic management queues can take advantage of unused reserved bandwidth when it becomes available.

- **Limit bandwidth.** Network traffic such as large file transfers can tolerate restricted bandwidth and delay. A traffic management queue that restricts bandwidth for these connections guarantees sufficient bandwidth for other applications. Maximum bandwidth limits can also help regulate total volume of data transfer over time to help your organization keep WAN usage within monthly quotas.

- **Assign different levels of priority to policies.** 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. If you use priorities correctly, you can make sure specific connections always succeed even when other applications also use the network.

Traffic prioritization in Fireware uses the configuration settings **Outgoing Interface Bandwidth, Traffic Management actions**, and, optionally, **Traffic Priority**. To use this advanced networking capability, you must understand how each setting works and how they can be used together.

### About Outgoing Interface Bandwidth

Before you use traffic management features, you must give each interface a bandwidth limit, known as Outgoing Interface Bandwidth, for traffic sent from that interface to the network segment to which it is connected. For example, you could set Outgoing Interface Bandwidth on the external interface when you upload files to a remote FTP server on the Internet. For downloads initiated from the trusted interface, you could set Outgoing Interface Bandwidth on the trusted interface. If you give an interface a bandwidth limit, Fireware refuses packets that exceed the limit. Also, Policy Manager gives a warning if you allocate too much bandwidth as you create or adjust Traffic Management actions.

When you set Outgoing Interface Bandwidth on the external interface, you should use your Internet connection upload speed (in Kbps rather than KBps) as the limit. Set your LAN interface bandwidth based on the minimum link speed supported by your LAN infrastructure.

### About Traffic Management actions

Traffic Management actions enforce an absolute maximum connection rate and bandwidth. They also guarantee minimum bandwidth per interface. All policies that use the same Traffic Management action share its connection rate and bandwidth settings.

Unused guaranteed bandwidth reserved by one Traffic Management action can be used by others. To plan your traffic management configuration, use these general steps:

- Identify three categories of applications based on priority and sensitivity to bandwidth restriction. You can add more at any time as necessary.
- Divide the Outgoing Interface Bandwidth for each interface based on anticipated need for each category. Make sure each division is large enough to accommodate all policies included in that queue.
- For each category, create one Traffic Management action with the bandwidth reservations you determined for each interface.
- Open each policy in your Firebox configuration and add it to the appropriate queue.

### About traffic priority

The networking industry has many different algorithms to prioritize network traffic. Fireware uses a high performance, class-based queueing method known Hierarchical Token Bucket. Prioritization in Fireware is equivalent to CoS levels 0 to 7, where 0 is routine priority (default) and 7 is the highest priority. You set traffic priority on the **QoS** tab of the **Advanced** tab of each policy. Use the table below as a guideline when you assign priorities.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Routine (HTTP, FTP)</td>
</tr>
<tr>
<td>1</td>
<td>Priority</td>
</tr>
<tr>
<td>2</td>
<td>Immediate (DNS)</td>
</tr>
<tr>
<td>3</td>
<td>Flash (Telnet, SSH, RDP)</td>
</tr>
<tr>
<td>4</td>
<td>Flash Override</td>
</tr>
<tr>
<td>5</td>
<td>Critical (VoIP)</td>
</tr>
<tr>
<td>6</td>
<td>Intemetwork Control (Remote router configuration)</td>
</tr>
<tr>
<td>7</td>
<td>Network Control (Firewall, router, switch management)</td>
</tr>
</tbody>
</table>

It is possible for high priority network traffic to interfere with system administration connections. Reserve the highest traffic priority levels only for network administration policies to make sure they are always available.
Exercise 1: Use a Traffic Management Action without Setting Priority

You might have circumstances when you must control minimum and maximum bandwidth for a group of policies, without concern for priority on an individual policy setting basis. These policies may represent less important or infrequently used ports that need bandwidth restrictions. Some applications rely on predictable, real-time data delivery to give a satisfactory user experience. Without prioritization, high-bandwidth applications can cause unacceptable delay if they are already transmitting when a more important application is launched.

Likewise, real-time connection reliability can be disrupted if other applications begin transmitting data. For example, a large FTP download could degrade or disrupt an HTTP session during bandwidth saturation, which results in, say, choppy video in a YouTube download. The following exercise shows how to guarantee minimum bandwidth that is shared between more than one policy, without setting priority in the policies. When configured this way, all policies compete for the same bandwidth.

Requirements for this exercise:

- One test computer connected to the Firebox trusted interface.
- One Windows 2003 Server computer connected to the external interface with a switch or hub (along with the Internet router). Windows 2003 Server includes IIS, which must be installed to run the FTP and HTTP server. You need both for this exercise.
- One computer running WSM version 10.x.
- Firebox running Fireware version 10.x.
- One hub or switch to connect the computers to the Firebox trusted interface.

All exercises in this course module were designed for a controlled environment using a LAN network. Real-world tests introduce volatility and latency associated with the Internet. Tests run in such an environment can produce unexpected results.

Put a default configuration on the Firebox

1. Run the Quick Setup Wizard to initialize your Firebox. Your instructor can help you with this process.
2. From Policy Manager, select the Outgoing policy. Click Delete.

Define Outgoing Interface Bandwidth

1. From Policy Manager, select Network > Configuration. Select Interface 1 (Trusted) and click Configure. Because your computers on the trusted network download files from a server on the external network, you define Outgoing Interface Bandwidth on the Firebox's trusted interface. You do not need to define Outgoing Interface Bandwidth on the external interface for this exercise.
2. On the Advanced tab under Traffic Management, set the Outgoing Interface Bandwidth limit to 1500 Kbps. Click OK.

3. Click OK again on the Network Configuration dialog box to return to Policy Manager.
**Create a Traffic Management action**

1. From the **Setup** menu, select **Actions > Traffic Management**.
2. Click **Add** to create a custom Traffic Management action. In the **Name** field, type the name “Min1000Kbps.”
   
   We will use this action to guarantee bandwidth for a group of policies.
3. From the **Maximum Bandwidth** drop-down list, select **No Limit**.
4. Under **Guaranteed Minimum Bandwidth**, click **Add**. Make sure the **Outgoing Interface** is set to **Trusted**. In the **Minimum Bandwidth** column, double-click **1000**. Click **OK**.
5. Click **Close** to return to Policy Manager.

**Add policies to the configuration**

1. From the **Edit** menu, select **Add Policy**.
2. Expand the **Packet Filters** folder and select **HTTP** from the list. Click **Add**.
3. At the top of the **Advanced** tab, from the **Traffic Management** drop-down list, click **Min1000Kbps**. Click **OK**.
4. From the **Add Policies** dialog box, select the DNS packet filter policy (not the proxy policy). Click **Add**.
5. Click **OK** to return to the **Add Policies** dialog box. Click **Close**.
6. From Policy Manager, select to edit the FTP policy. Repeat step 3.

Both policies now use the same Traffic Management action.

**Set up a server to host FTP and HTTP downloads**

1. Connect the server's network card to the same hub or switch that connects the Firebox external interface to the Internet router.
   
   Normally, you would connect your Firebox directly to the LAN interface of your Internet router. For this exercise, you must use a hub or switch to connect the Windows 2003 Server to the external network of the Firebox.
2. Set up the FTP server. For information on how to do this, see the following Microsoft article:
   
   [http://support.microsoft.com/kb/323384](http://support.microsoft.com/kb/323384)
3. Create a 350 MB text file called 350mbfile.txt and put it in the ftproot folder. The default location for this folder is c:\inetpub\ftproot. To create a file in Windows, use the fsutil command:
   
   `fsutil file createnew c:\inetpub\ftproot\350mbfile.txt 358400000`
4. Enable the web server on your Windows 200x Server. For information on how to do this, see the following Microsoft article:
   
   [http://support.microsoft.com/kb/324742](http://support.microsoft.com/kb/324742)
5. Copy the 350mbfile.txt from the c:\inetpub\ftproot to the c:\inetpub\wwwroot directory.

**Set up Service Watch**

1. From WatchGuard System Manager, connect to the Firebox. Start Firebox System Manager, and click the **Service Watch** tab.
2. Right-click anywhere in the window and select **Settings**. From the **Chart Type** drop-down list, select **Bandwidth**. Leave the **Graph Scale** settings at the default value (**auto-scale**).
3. From the **Show** box, select all policies not used in this exercise and click **Remove**. Only the FTP and HTTP policies should remain. The other policies should now appear in the **Hide** box.
4. Click **OK**.
See the results of the configuration

Both the FTP and the HTTP policy use the same Traffic Management action **Minimum1000k**. If you exceed your maximum allowed bandwidth, both policies will use the same minimum and maximum bandwidth restrictions.

1. On the computer you will use for the download, shut down all other applications. Results vary if other applications on the computer have access to the network.
2. From a computer that is connected to the trusted interface, start an FTP session. From either the command line, Internet Explorer, or an FTP client of your choice, make an FTP connection to your Windows 2003 Server on the external network. Download the 350MB file you created earlier.
3. Look at Service Watch. Notice that the FTP transfer takes all of the available bandwidth. This should be approximately equal to the value you set for Outgoing Interface Bandwidth on the trusted interface (1500 Kbps).
4. From the same computer you used for the FTP transfer, start the download of the 350MB file you copied into the c:\inetpub\wwwroot folder. If the instructor put the 350MB file in the root of c:\inetpub\wwwroot folder, use this URL:
   http://<web server.ip.addr>/350mbfile.txt
   Make sure the FTP transfer is still active before you start the HTTP transfer.
5. In Service Watch, look at the amount of bandwidth that is used by both policies. After you start the HTTP transfer, the amount of bandwidth used by the FTP transfer is reduced. The HTTP and FTP connections now compete for bandwidth, but they should now receive approximately equal amounts.

---

**Exercise 2: Use Traffic Management Actions with Traffic Priority**

All policies that share a Traffic Management action compete for the same slice of bandwidth. However, you can set a higher priority on specific types of traffic that are more important to your business functions. However, note that when traffic flows through all policies, those with the lowest priority settings might not be given any of the reserved bandwidth within that queue and will time out.
The requirements for this exercise are the same as for Exercise 1.

**When to reserve bandwidth and prioritize traffic in a policy**
Some applications rely on predictable, real-time data delivery to give a satisfactory user experience. Without prioritization, high bandwidth applications can cause unacceptable delay if they are already transmitting when a more important application is launched. Likewise, real-time connection reliability can be disrupted if other applications begin transmitting data. For example, a large FTP download could degrade or disrupt an HTTP download.

**Put a default configuration on the Firebox**
If you have not already done this, see the procedure in Exercise 1.

**Define Outgoing Interface Bandwidth**
If you have not already done this, see the procedure in Exercise 1.

**Create a Traffic Management action**
1. From the **Setup** menu, select **Actions > Traffic Management**.
2. Click **Add** to create a custom Traffic Management action. In the **Name** field, type the name “Min1000Kbps.”
   We will use this action to guarantee bandwidth for a group of policies.
3. From the **Maximum Bandwidth** drop-down list, select **No Limit**.
4. Under **Guaranteed Minimum Bandwidth**, click **Add**. Make sure the **Outgoing Interface** is set to **Trusted**. In the **Minimum Bandwidth** column, double-click **1000**. Click **OK**.
5. Click **Close** to return to Policy Manager.

**Add policies to the configuration**
1. From the **Edit** menu, select **Add Policy**.
2. Expand the **Packet Filters** folder and select **HTTP** from the list. Click **Add**.
3. At the top of the **Advanced** tab, from the **Traffic Management** drop-down list, click **Min1000Kbps**.
4. Select the **QoS** tab. Under **Traffic Priority**, select the **Override per-interface settings** check box. Change the **Value** setting to 5. Click **OK**.
   Now HTTP uses the custom Traffic Management action queue, and has a priority of 5.
5. From the **Add Policies** dialog box, select the DNS packet filter policy (not the proxy policy). Click **Add**.
6. Click **OK** to return to the **Add Policies** dialog box. Click **Close**.
7. From Policy Manager, select to edit the FTP policy. Repeat step 3. Do not set a priority in the **QoS** tab. Keep the default value of 0.
   FTP now uses the custom Traffic Management action queue with a priority of 0.

**Set up a server to host FTP and HTTP downloads**
If you have not already done this, see the procedure in Exercise 1.

**Define Service Watch**
If you have not already done this, see the procedure in Exercise 1.

**See the results of the configuration**
The HTTP policy has higher priority and guaranteed bandwidth. The FTP has only routine priority (0) and no guaranteed bandwidth. HTTP data will be handled at a predictable rate and some FTP traffic will be queued.
when HTTP connections are active. When no HTTP connections are active, the FTP policy can use all available bandwidth:

1. On the computer you will use for the download, shut down all other applications. Results vary if other applications on the computer have access to the network.

2. From a computer that is connected to the trusted interface, start an FTP session. From either the command line, Internet Explorer, or an FTP client of your choice, make an FTP connection to your Windows 2003 Server on the external network. Download the 350MB file you created earlier.

3. From the same computer you used for the FTP transfer, start the download of the 350MB file you copied into the c:\inetpub\wwwroot folder. If the instructor put the 350MB file in the root of c:\inetpub\wwwroot folder, use this URL:
   http://<web server.ip.addr>/350mbfile.txt
   Make sure the FTP transfer is still active before you start the HTTP transfer.

4. Look at Service Watch. The HTTP policy will use more bandwidth because its priority is higher than FTP.

5. Start additional HTTP sessions to the web server and download the same 350mb file to different locations on the test computer.
   You can expect results similar to the ones shown below when your connections exceed the maximum allowed bandwidth. The HTTP connections will use all available bandwidth, and none will be available for the FTP transfers. In this example, HTTP uses all 1.5 MB of our maximum allowed bandwidth.
Exercise 3: Use Guaranteed Bandwidth with Individual Traffic Management Actions

Bandwidth reservation prevents 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. With individual traffic management actions, and priorities, you can guarantee bandwidth on a more granular level on a per-policy basis. Our previous exercise demonstrated policies sharing the same Traffic Management actions; however, such configurations do not allow you to specify minimum bandwidths for each policy.

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 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.

The requirements for this exercise are the same as for Exercise 1.

Put a default configuration on the Firebox
If you have not already done this, see the procedure in Exercise 1.

Define Outgoing Interface Bandwidth
If you have not already done this, see the procedure in Exercise 1.

Create two Traffic Management actions
1. From the Setup menu, select Actions > Traffic Management.
2. Click Add to create a custom Traffic Management action. In the Name field, type the name “Min400Kbps.” We will use this action to guarantee bandwidth for a group of policies.

3. From the Maximum Bandwidth drop-down list, select No Limit.

4. Under Guaranteed Minimum Bandwidth, click Add. Make sure the Outgoing Interface is set to Trusted. In the Minimum Bandwidth column, double-click 400 to set it to that value. Click OK.

5. Click Close to return to Policy Manager.

6. Create another Traffic Management action for the HTTP policy. From the Setup menu, select Actions > Traffic Management.

7. Click Add to create a custom Traffic Management action. In the Name field, type the name “Min900Kbps.” We will use this action to guarantee bandwidth for a group of policies.

8. From the Maximum Bandwidth drop-down list, select No Limit.

9. Under Guaranteed Minimum Bandwidth, click Add. Make sure the Outgoing Interface is set to Trusted. In the Minimum Bandwidth column, double-click 900. Click OK.

10. Click Close to return to Policy Manager.

Add policies to the configuration
1. From the Edit menu, select Add Policy.

2. Expand the Packet Filters folder and select HTTP from the list. Click Add.

3. At the top of the Advanced tab, from the Traffic Management drop-down list, click Min900Kbps. HTTP now uses the Traffic Management action Min900Kbps.

4. From the Add Policies dialog box, select the DNS packet filter policy (not the proxy policy). Click Add.

5. Click OK to return to the Add Policies dialog box. Click Close.

6. From Policy Manager, select to edit the FTP policy.

7. At the top of the Advanced tab, from the Traffic Management drop-down list, click Min400Kbps. Click OK. FTP now uses the Traffic Management action Min400Kbps.

Set up a server to host FTP and HTTP downloads
If you have not already done this, see the procedure in Exercise 1.

Define Service Watch
If you have not already done this, see the procedure in Exercise 1.

See the results of the configuration
Both the HTTP and the FTP policies have guaranteed minimum and maximum bandwidths. These policies do not compete for bandwidth because they do not use the same Traffic Management action. This configuration is ideal when each policy must have a guaranteed minimum, maximum bandwidth, or both. This would not be possible if the policies shared a Traffic Management action.

1. On the computer you will use for the download, shut down all other applications. Results vary if other applications on the computer have access to the network.

2. From a computer that is connected to the trusted interface, start an FTP session. From either the command line, Internet Explorer, or an FTP client of your choice, make an FTP connection to your Windows 2003 Server on the external network. Download the 350MB file you created earlier.
3. Look at Service Watch. Results should be similar to those shown below.

4. From the same computer you used for the FTP transfer, start the download of the 350MB file you copied into the \c:\inetpub\wwwroot folder. If the instructor put the 350MB file in the root of \c:\inetpub\wwwroot folder, use this URL:
   http://<web server.ip.addr>/350mbfile.txt
   Make sure the FTP transfer is still active before you start the HTTP transfer.

5. Note the bandwidth used by the two policies in Service Watch. Although both connections are active, the HTTP policy will have more guaranteed bandwidth than the FTP policy, as shown below.
Related Courseware and Information

For more information on Firebox System Manager and how to use it, go to:
See the topics under “Firebox Status Monitoring.”

Or,
Go to https://www.watchguard.com/help/documentation/ and download the
WatchGuard System Manager User Guide. See the chapter “Firebox Status Monitoring.”

Test Your Knowledge

1. True or False: You cannot assign a Traffic Management action and set traffic priority together in one policy.

2. True or False: Bandwidth Meter is a FSM utility used to graph our HTTP and TCP connections in the exercises in this module.

3. Which priority level is generally recommended for latency-sensitive connections such as VoIP?
   A) □ 4 Flash Override
   B) □ 0 Routine
   C) □ 5 Critical
   D) □ 2 Immediate
   E) □ 1 Priority

4. True or False: You configure Outgoing Interface Bandwidth in the Advanced tab of each Firebox interface.

5. Which interface will you have to set the Outgoing Interface Bandwidth to guarantee bandwidth for downloads to an external FTP server initiated from a computer on the trusted interface?
   A) □ Trusted Interface
   B) □ Optional Interface
   C) □ External Interface
   D) □ None of the above
   E) □ All of the above

6. True or False: Before you use traffic management features, you must give each interface a bandwidth limit, known as Outgoing Interface Bandwidth, for traffic sent from that interface to the network segment to which it is connected.

[See next page for answers]
Answers
1. False
2. False. Service Watch is configured to graph bandwidth in this exercise.
3. C
4. True
5. A
6. True
Centralized Management

Managing the Firebox X Edge

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Firebox® X Core / Firebox X Core e-Series / Firebox X Peak /Firebox X Peak e-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance software versions</td>
<td>Fireware Pro 10.0</td>
</tr>
<tr>
<td>Management software versions</td>
<td>WatchGuard® System Manager 10.0</td>
</tr>
<tr>
<td>Training module</td>
<td>Centralized Management</td>
</tr>
</tbody>
</table>

What You Will Learn

WatchGuard System Manager (WSM) allows you to manage one or more Firebox X Edge legacy and e-Series Edge devices from a single Management Server. With centralized management, you can create Edge configuration templates that can be applied to multiple Edge devices. You can also use other tools that make Edge management easier from a central Management Server. In this training module, you learn how to:

- Define aliases for managed Firebox X Edge devices
- Configure the Firebox X Edge for centralized management
- Use Edge configuration templates to manage settings on multiple devices
- Schedule Edge firmware updates
- Create Firebox X Edge VPN tunnels

Before you do the exercises, be sure to read and become familiar with the information in the “Course Introduction” training module available at:
http://www.watchguard.com/training/courses.asp

In this module, you will connect to one or more Firebox devices. If you take this course with a WatchGuard Certified Training Partner, your instructor will provide the IP address and passphrases for devices used in the exercises.

Manage Edge Devices with WSM

WatchGuard System Manager includes several features specifically for centralized management of Firebox X Edge devices. You can easily manage many Firebox X Edge devices and make changes to the security policy for more than one Firebox X Edge device at one time, and still have individual control over the configuration of each Firebox X Edge device.

You can also manage Firebox SOHO 6 and SOHO 5 devices from WatchGuard System Manager. You cannot make configuration changes to the SOHO with WatchGuard System Manager other than making VPN tunnels to managed SOHO devices. However, you can see settings and VPN tunnels for a SOHO and launch configuration and monitoring tools.

When the Firebox X Edge is configured for centralized management, local access to the Firebox X Edge configuration pages is set to read-only. The only exception is access to the WSM Access configuration page. If you disable the remote management feature, you get read-write access to the Firebox X Edge configuration again.

If you use WatchGuard Management Server to create VPN tunnels only, you can enable remote management but disable centralized management. This lets you keep the ability to manage the Edge.
using the Edge web management interface. At the same time, you can make VPN tunnels using WSM’s easy
drag-and-drop tunnel wizard.

**Edge configuration templates**

An Edge configuration template is a collection of configuration settings that multiple Edge devices can use.
You configure and store an Edge configuration template on the Management Server. You then subscribe Firebox X Edge devices to the Edge configuration template by selecting devices from a list or with a drag-and-drop procedure. Although many Edge devices can use the same template, each Firebox X Edge can subscribe to only one Edge configuration template. You can make changes to an Edge configuration template or the list of subscribed devices at any time. The Management Server automatically makes the changes on all subscribed devices.

Edge configuration templates can include a number of settings for a Firebox X Edge. These settings include:

- Firewall policies that allow or deny traffic
- Standard or custom TCP, UDP, or IP protocols
- Blocked sites configuration
- Logging setup
- WebBlocker configuration

**Firmware updates**

When you manage Firebox X Edge devices with WSM, you can use a single operation to update firmware on
groups of Edge devices, either immediately or on a schedule. These firmware updates are downloaded from
LiveSecurity and installed on your Management Server.

Note that you can update the firmware from the Firebox X Edge e-Series configuration pages if you do not
use centralized management. This is a different procedure from the one used with centralized management.

**Aliases for template destinations**

You use aliases with managed Firebox X Edge devices to define a common destination for template configu-
ratin on the Management Server. You define aliases for an Edge when you configure the network settings
for that Edge.

For example, suppose you create an Edge configuration template for an email server and define that policy
to work with your mail server. Because the mail server can have a different IP address on each Firebox X Edge
network, you create an alias on the Management Server called MailServer. When you create the Edge
configuration template for the mail server, you use this alias as the destination. You would define that alias as
either the source or destination, depending on the direction of the policy. In this example, you would
configure an incoming SMTP Allow policy with MailServer as the destination.

To make the Edge configuration template work on the Fireboxes that subscribe to the policy, you configure
the MailServer alias in the network settings for each Firebox X Edge device.

**Exercise 1: Use Aliases with Managed Edge Devices**

In this exercise, you assign a name to an alias on the Management Server and define an alias IP address on
the Firebox X Edge.

**Give a name to an alias the Management Server**

1. In the **Device Management** tab in WatchGuard System Manager, select the Management Server.
2. Under **Server Information**, click **Manage Aliases**.
3. Select an alias and click **Edit** to change the default name.

4. Type a name for the alias and click **OK**.
Define an alias on the Edge
1. In the Device Management tab in WatchGuard System Manager, select the Firebox X Edge.
2. Under Network Settings for the Edge, click Configure. The Network Settings dialog box appears. This dialog box lists the current settings for each interface, in addition to other information. If this is the first time you click Configure in the Network Settings for an Edge, you are asked whether you are sure you want to download the network settings and enable global management.
3. Click Aliases. The aliases appear, including the alias you named on the Management Server.
4. Select an alias to define and click Edit.
Exercise 2: Set Up Centralized Management

This exercise shows you how to configure remote access from WatchGuard System Manager v8.2 or higher. These versions of WatchGuard System Manager support centralized management of Firebox X Edge devices.

Set up the Edge for management

1. To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface. The default URL is: https://192.168.111.1.
2. From the navigation bar, select **Administration > WSM Access**.

The Local Alias Setting dialog box appears.

5. Type the IP address of this Firebox X Edge.
6. Click **OK**.
3. Select the **Enable remote management** check box.

![Administration WatchGuard Management Access](image)

4. From the **Management Type** drop-down list, select **WatchGuard System Manager**.

5. To put the Firebox X Edge into the control of WatchGuard System Manager centralized management, select the **Use Centralized Management** check box.

6. Type a status passphrase for your Firebox X Edge. Type it again to confirm.

7. Type a configuration passphrase for your Edge. Type it again to confirm. These passphrases must match the passphrases you use when you add the device to WatchGuard System Manager, or the connection fails.

**NOTE:** Steps 8 – 10 are necessary only if the Edge has a dynamic IP address on its external interface. If your Edge has a static address, skip to step 7.

8. In the **Management Server Address** text box, type the IP address of the Management Server if it has a public IP address. If the Management Server has a private IP address, type the public IP address of the Firebox that protects the Management Server. The Firebox 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. No special configuration is necessary for this to occur.

9. Type the **Client Name** to give your Firebox X Edge. This is the name that identifies the Edge in the Management Server.

10. Type the **Shared Key**. The shared key is used to encrypt the connection between the Management Server and the Firebox X Edge. This shared key must be the same on the Edge and the Management Server.

11. Click **Submit**.

**Add the Edge to WSM**

This section shows you how to insert a Firebox X Edge into WSM and use the tools of centralized management to configure and manage the Edge.

1. Open WatchGuard System Manager (WSM), Connect to a Management Server.

2. Click the **Device Management** tab.
3. Select **Edit > Insert Device**. Or, right-click in the left frame of this window and select **Insert Device**. The Add Device Wizard starts.

4. Click **Next**. The Add Device wizard begins the process of identifying and inserting a Firebox into WSM.

1. Type the device name, then type the host name/IP address, and the passphrases for the Firebox Edge. These are the passphrases you defined when you configured the Edge for use with WSM. Click **Next**. This exercise uses a Firebox X Edge with a static IP address.
2. After the Management Server contacts the device, type a name for the Edge.

3. The Add Device wizard establishes a connection and adds a basic template to the Edge. Click **Next**.

4. The wizard proceeds through the verification process. When complete you see this screen. Click **Close**.
Exercise 3: Use an Edge Configuration Template

The Edge is now added to the Management Server and can be managed from WSM.

Exercise 3: Use an Edge Configuration Template

In this exercise you make an Edge configuration template for an Edge.

Add a policy to a configuration template
1. In WSM, select the Device Management tab.
2. In the left pane, expand Edge Configuration Templates.
3. Double-click a default configuration template. If you inserted a 10.0 Edge, you can select the Edge 10.0 default template.
4. In the field that appears, type a name for the policy. Click **OK**. You must change the name because you cannot edit a default template.

5. Under **Firewall Policies**, click **Configure**.

6. Click **Add**. This starts the Add Policy Wizard.

7. Click **Next**.
8. Select the type of policy to add. Click **Next**.

9. Select the traffic direction. Click **Next**.
10. Configure network resources. Click **Add** under **From**, **To**, or both to restrict the source or destination to specific hosts, networks, or aliases. Note that the alias you created in Exercise 1 appears. Click **Next**.

![Add Policy Wizard](image)

11. Click **Finish** to finish the wizard.
   
   You can see the policy in the Edge configuration template.

**Subscribe devices to a configuration template**

1. In the WatchGuard System Manager **Device Management** tab, expand the list of Edge configuration templates.

2. Select the template to add to a device.
   
   The Edge configuration template appears in the right frame of the window.
3. Click **Configure** under the **Devices** section.

4. Click **Add** to add a device to the list.

5. Select a Firebox X Edge device from the list.
6. Click **OK**, and then **Close**. The managed Edge device is added to the configuration template. You can see the device name in WSM as shown below.

![Image of WatchGuard System Manager interface showing Edge device added to configuration template]

**Exercise 4: Schedule Firmware Updates**

Before you start this exercise, you must make sure that Edge firmware for centralized management is already installed. Otherwise, you will get an error when you try to schedule a firmware update.

**Install firmware**

1. Log in to your LiveSecurity Service account.
2. Go to **Software Downloads**.
3. Select **Core** or **Peak**.
4. Double-click **Firebox Centralized Management** and run the installation program.

**Schedule an update**

1. In the **Device Management** tab in WatchGuard System Manager, select the Management Server. The Management Server settings page appears.
2. Scroll down to the **Firmware Update Status** section.
Exercise 4: Schedule Firmware Updates

3. Click **Schedule Firmware Update**. The Update Firmware Wizard starts.
4. Read the Welcome screen and click **Next**.
5. Select the device type from the list and click **Next**.
6. Select the check boxes for the devices on which to update firmware. Click **Next**.
7. Select the firmware version to use. Click **Next**. The Select the Time and Date page appears.
8. To update firmware immediately, select **Update firmware immediately**. To schedule the update for a time in the future, select **Schedule firmware update**.
9. If you selected **Schedule firmware update**, select the date from the **Date** field, and set the time in the **Time** field. Click **Next** to schedule the firmware update.
10. Click **Close**.
The firmware is updated if you selected **Update firmware immediately** or scheduled if you selected **Schedule firmware update**.

**See firmware updates**

1. From the **Device Management** tab, click **Scheduled Firmware Updates**.

All scheduled firmware updates are listed. Firmware updates are listed separately for each device, even if multiple devices are part of the same firmware update. For this reason, when you select a device, all devices included in that scheduled firmware update are also selected.

**Exercise 5: Define a VPN Tunnel**

The Firebox X Edge management page shows all tunnels that include the device in the Tunnels section. You can also add a VPN tunnel in this section.

You must have at least two managed devices inserted to make tunnels with the Management Server. At least one of them must have a static IP address. You cannot make a tunnel between two dynamic devices with the Management Server.

1. On the Firebox X Edge management page, find the VPN Tunnels section.

   ![VPN Tunnels](image)

   This section shows all tunnels that include this device.

2. Click **Add** to begin the process of adding a new VPN tunnel. The Add VPN wizard starts.
3. Select the devices to use in the tunnel from the drop-down menus for Device One and Device Two. Click **Next**.

![Add VPN Wizard](image)

1. Select a security template from the drop-down menu. A security template is a set of configuration information to be used when you create tunnels. When you use security templates, you do not need to individually create settings each time you create a tunnel. Click **Next**.

2. Select a VPN Firewall Policy Template. You use VPN Firewall Policy templates to create a set of one or more bidirectional firewall policies that restrict the type the traffic allowed across a VPN. Note that this step applies only to Fireware devices.

![Add VPN Wizard](image)

When the process is complete click **Finish**.

**Exercise 6: Start Firebox X Edge Tools**

The management page allows you to start four tools for Firebox X Edge configuration and monitoring:
- Edge Web Manager
- Firebox System Manager
- HostWatch
- Ping

1. From the Edge management page, find the Tools section.
2. To start any of these tools, click the link for the tool from the Tools section on the Firebox X Edge management page.

Related Courseware and Information

You can use these resources for more information on how to manage Edge devices with WSM:

**WatchGuard® System Manager User Guide**

Browse to [https://www.watchguard.com/help/documentation/](https://www.watchguard.com/help/documentation/) and download the User Guide. See the chapters “Firebox X Edge Centralized Management” and “Devices and VPNs in WatchGuard System Manager.”

Test Your Knowledge

Use these questions to practice what you have learned and exercise new skills.

1. You can apply Edge configuration templates to which of these Firebox devices:
   A) [ ] Firebox X Core  
   B) [ ] Firebox X Edge  
   C) [ ] Firebox X Peak  
   D) [ ] Firebox SSL VPN Gateway

2. Which of these settings can you modify using Edge Configuration Templates? (Select all that apply):
   A) [ ] Blocked sites  
   B) [ ] WebBlocker configuration  
   C) [ ] Logging setup  
   D) [ ] Policies to allow or deny TCP or UDP traffic  
   E) [ ] All of the above
3. You can apply Edge configuration templates to a Firebox Edge using these methods (select all that apply)?
   A) Drag-and-drop a policy onto an Edge listed in WSM
   B) Selecting the Edge from a list of managed devices
   C) A wireless broadcast from a Management Server to an Edge
   D) An SSH session from a Management Server to an Edge

4. True or false:
   ____ A Firebox Edge can be configured for management by more than one WatchGuard Management Server.
   ____ If you activate remote management on a Firebox Edge, you must always enable Centralized Management for that device.
   ____ The IP address of the WatchGuard Management Server can be either a static or dynamic IP address.
   ____ To add a managed device to the WatchGuard Management Server using the Add Device Wizard, the device must have a static IP address.
   ____ A Firebox Edge can subscribe to more than one Edge configuration template.
   ____ Firebox Edge firmware updates can be scheduled for automatic distribution from the WatchGuard Management Server.

5. Which of these items are tools that you can launch from WSM for a centrally managed Firebox X Edge? (Select all that apply):
   A) HostWatch
   B) Ping
   C) Edge Web Manager
   D) Firebox System Manager
   E) All of the above

6. Which of these network settings can you configure remotely for an Edge using WSM? (Select all that apply):
   A) External IP address
   B) WAN failover
   C) Static routes
   D) Trusted hosts
   E) All of the above
Answers

1. B
2. E
3. A and B
4. False
5. True
6. E
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-to-1 NAT</td>
<td>A form of NAT which changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses.</td>
</tr>
<tr>
<td>Active Mode</td>
<td>The FTP server establishes the data connection.</td>
</tr>
<tr>
<td>Adware</td>
<td>A software application that can display advertising banners while the program is running or via some other triggering mechanism. It can waste bandwidth and other system resources as well as be a vector for attacks.</td>
</tr>
<tr>
<td>Antivirus Software</td>
<td>Software that uses virus signatures to scan for the presence of malicious code.</td>
</tr>
<tr>
<td>Any</td>
<td>The Any alias includes any IP address on any network connected to an active Firebox interface.</td>
</tr>
<tr>
<td>Any-External</td>
<td>The Any-External alias includes any IP address on any network defined as an external-type interface, or the set of external interfaces themselves.</td>
</tr>
<tr>
<td>Any-Optional</td>
<td>The Any-Optional alias includes any IP address on any network defined as a optional-type interface, or the set of optional interfaces themselves.</td>
</tr>
<tr>
<td>Any-Trusted</td>
<td>The Any-Trusted alias includes any IP address on any network defined as a trusted-type interface, or the set of trusted interfaces themselves.</td>
</tr>
</tbody>
</table>
| Authentication              | 1. The process of identifying an individual, usually based on a user name and password. Authentication usually requires something a person has (such as a key, badge, or token), something a person knows (such as a password, ID number, or mother's maiden name), or something a person is (represented by a photo, fingerprint or retina scan, etc). When authentication requires two of those three things, it is considered strong authentication.  
  2. A method of associating a user name with a workstation IP address, allowing the tracking of connections based on name rather than IP address. With authentication, you can track users regardless of which machine a person chooses to work from. |
<p>| Configuration File          | A text file that contains the settings for a particular application or operating system.                                                                                                                      |
| Configuration Passphrase    | The read-write password that allows an administrator to edit the configuration file operating on the Firebox.                                                                                             |
| Consolidated Section        | A report section which includes data for more than one Firebox. See report section.                                                                                                                        |
| Default Packet Handling     | A set of rules that instruct the Firebox on how to process packets when no other rules have been specified. With default packet handling, 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 there is a risk, set the Firebox to automatically block against the possible attack. |
| DHCP (Dynamic Host Configuration Protocol) | A standard for transferring network configuration information from a central server to devices as the devices boot up. This data typically includes a computer’s IP address. |
| DHCP server                 | A device that automatically assigns IP addresses to networked computers from a defined pool of addresses, returning unused IP addresses to the pool. Using a DHCP server, an administrator normally does not have to get involved with the details of assigning IP addresses to individual clients. |
| DNS (Domain Name System)    | A network system of servers that translates numeric IP addresses into readable, hierarchical Internet addresses, and vice versa. This is what allows your computer network to understand that you want to reach the server at 192.168.100.1 (for example) when you type into your browser a domain name such as <a href="http://www.watchguard.com">www.watchguard.com</a>. |
| Download                    | To transfer (data or programs) from a server or host computer to one’s own computer or device.                                                                                                          |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop-in Configuration</td>
<td>In drop-in configuration mode, the trusted, external, and optional network interfaces on the Firebox are set to the same IP address. The Firebox uses automatic host mapping.</td>
</tr>
<tr>
<td>ESMTP (Extended Simple Mail Transfer Protocol)</td>
<td>This protocol allows for functional extensions to SMTP.</td>
</tr>
<tr>
<td>Exclude</td>
<td>To prevent or restrict (v). With Historical Reports, an exclude filter removes all log messages which match the criteria you set.</td>
</tr>
<tr>
<td>External</td>
<td>The External alias includes any IP address on any network attached to the external interface, or the external interface itself. If you configure more than one interface on the Firebox as external, you must select an alias to use for that external-type interface.</td>
</tr>
<tr>
<td>External Interface</td>
<td>On the Firebox, an Ethernet port intended for connecting to the portion of your network that presents the greatest security risk (typically the Internet).</td>
</tr>
<tr>
<td>Failover Logging</td>
<td>A logging procedure designed to decrease the possibility of missing log events. With failover logging, you configure more than one Log Server. When the primary Log Server fails, the Firebox automatically fails over, or sends log messages to the next Log Server on the list.</td>
</tr>
<tr>
<td>Filter</td>
<td>A filter rule you apply to a Historical Report to control the data included in the report. When you run a report against a WatchGuard log file, the report will include all relevant data from the log file, unless you include a report data filter. You can set a filter to include or exclude specific host, port, or user data.</td>
</tr>
<tr>
<td>Firebox</td>
<td>The Firebox alias includes any IP address that the Firebox has been assigned on any active interface.</td>
</tr>
<tr>
<td>Firebox backup image</td>
<td>A saved copy of the working image from the Firebox flash disk, including the Firebox appliance software and configuration file.</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol. The function of FTP is to enable access to another computer for the purposes of browsing directories and copying files.</td>
</tr>
<tr>
<td>Group</td>
<td>A collection of users who can share access authorities for protected resources. You can divide the users in your company into authentication groups.</td>
</tr>
<tr>
<td>HTML (Hypertext Markup Language)</td>
<td>The set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page. The markup tells the Web browser how to display a Web page’s words and images for the user.</td>
</tr>
<tr>
<td>HTTP (HyperText Transfer Protocol)</td>
<td>A protocol for sending and displaying files (text, graphic images, sound, video, and other multimedia files) on the Internet.</td>
</tr>
<tr>
<td>include</td>
<td>To contain or embrace (v). With Historical Reports, an include filter shows only those log messages which match the criteria you set.</td>
</tr>
<tr>
<td>Instant Messaging (IM)</td>
<td>Instant messaging is a type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet.</td>
</tr>
<tr>
<td>Intrusion Prevention System (IPS)</td>
<td>A hardware device or software application which detects attacks from hackers. Network-based intrusion detection systems examine the traffic on a network for signs of unauthorized access or attacks in progress, while host-based systems look at processes running on a local machine for activity an administrator has defined as “bad.”</td>
</tr>
<tr>
<td>Intrusion Prevention System (IPS)</td>
<td>An IPS, or intrusion prevention system provides policies and rules for network traffic.</td>
</tr>
<tr>
<td>LAN (Local Area Network)</td>
<td>A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).</td>
</tr>
<tr>
<td>Log Server</td>
<td>The computer to which your Firebox sends all log messages. It can be the same computer as your management station or you can use a second computer.</td>
</tr>
<tr>
<td>Management Server</td>
<td>A Management Server is a Windows computer with WatchGuard Firebox software installed. It is also a daemon running on a Management Server used to monitor multiple Fireboxes at once and simplify VPN configuration.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Address Translation (NAT)</td>
<td>NAT substitutes one IP address for one or more IP addresses from a different network. WatchGuard supports 1-to-1 and many-to-one NAT substitutions. 1-to-1 relationships allow bidirectional traffic initiation. Many-to-one, commonly known as masquerading or dynamic NAT, permits one way traffic from a privately addressed LAN of many hosts to other networks.</td>
</tr>
<tr>
<td>Operation Codes (also known as Opcodes)</td>
<td>An alphanumeric code value that tells a processor which operation to perform. DNS Opcodes are commands sent to a DNS server, such as query, update, or status requests.</td>
</tr>
<tr>
<td>Optional</td>
<td>The Optional alias includes any IP address on any network attached to the optional interface, or the optional interface itself. If you configure more than one interface on the Firebox optional, you must select an alias to use for that optional-type interface.</td>
</tr>
<tr>
<td>Optional Interface</td>
<td>The Ethernet port on the Firebox provided so you can connect a second secured network. This second network is often referred to as the “demilitarized zone” (DMZ), or the Optional network.</td>
</tr>
<tr>
<td>Packet Filter</td>
<td>Controls access to a network by analyzing the headers of incoming and outgoing packets, and letting them pass or halting them based on rules created by a network administrator. A packet filter allows or denies packets depending on where they are going, from whom they are sent, or what port they use. Packet filtering is one technique, among many, for implementing security firewalls.</td>
</tr>
<tr>
<td>Passive Mode</td>
<td>The client establishes the connection.</td>
</tr>
<tr>
<td>Peer-to-Peer (P2P)</td>
<td>Peer-to-peer is a method of distributing files over a network where all computers are treated as equals (in contrast to a client/server architecture). Using P2P client software, a client is able to receive files from another client. Some P2P file distribution systems require a centralized database of available files (such as Napster), while other distribution systems like Gnutella are decentralized.</td>
</tr>
<tr>
<td>Policy</td>
<td>A set of rules that describe how the Firebox manages packets that come to its interfaces.</td>
</tr>
<tr>
<td>Port Forwarding</td>
<td>Port forwarding allows connection initiation from external networks using one port or protocol to a dynamically NATed host. WatchGuard also uses the term Static NAT to describe port forwarding.</td>
</tr>
<tr>
<td>Precedence</td>
<td>The sequence in which the Firebox examines network traffic and applies a policy rule.</td>
</tr>
<tr>
<td>Protocol Anomaly Detection</td>
<td>The examination of a packet for compliance with RFC guidelines.</td>
</tr>
<tr>
<td>Proxy</td>
<td>A combination of stateful packet filtering with content inspection. Essentially, the Firebox intercepts traffic intended for another destination (for example, a Web server or an e-mail server) and imposes rigid access and routing rules with the defense of the internal networks and servers in mind. Dangerous traffic is discarded, while normal traffic is passed to the intended destination.</td>
</tr>
<tr>
<td>Related Hosts List</td>
<td>This list shows the hosts and interfaces on which the Firebox performs MAC discovery.</td>
</tr>
<tr>
<td>Secondary Network</td>
<td>A network on the same physical wire as a Firebox interface having a different IP network address. This technique allows you to add as many subnets as you want to a single Ethernet interface on a Firebox.</td>
</tr>
<tr>
<td>Signature</td>
<td>A unique string of bits, or the binary pattern, of a virus. The virus signature is like a fingerprint in that it can be used to detect and identify specific viruses.</td>
</tr>
<tr>
<td>SMTP (Simple Mail Transfer Protocol)</td>
<td>A protocol for sending electronic mail between servers.</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>A notification event issued by a managed device to the network management station when a significant event occurs.</td>
</tr>
<tr>
<td>Status Passphrase</td>
<td>The read-only password that allows you to see information about the Firebox but not make any changes to the configuration.</td>
</tr>
<tr>
<td>Traffic Pattern Analysis</td>
<td>The examination of a series of packets over time to match against known patterns of attack.</td>
</tr>
<tr>
<td>Trojan</td>
<td>A seemingly harmless program that hides a malicious virus, such as a password program that secretly records the passwords entered and sends them to the author of the virus.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trusted</td>
<td>The Trusted alias includes any IP address on any network attached to the trusted interface, or the trusted interface itself. If you configure more than interface on the Firebox as trusted, you must select an alias to use for that trusted-type interface.</td>
</tr>
<tr>
<td>Trusted Interface</td>
<td>The Ethernet port on the Firebox that connects it to your internal network.</td>
</tr>
<tr>
<td>Upload</td>
<td>To transfer (data or programs) from one's own computer or device to a server or host computer.</td>
</tr>
<tr>
<td>User</td>
<td>A person or entity with unique access permission to your network.</td>
</tr>
<tr>
<td>User Authentication</td>
<td>A process which allows a device to verify the identity of someone who connects to a network resource.</td>
</tr>
<tr>
<td>Virus</td>
<td>A self-replicating program that spreads by inserting copies of itself into other executable code or documents.</td>
</tr>
<tr>
<td>VPN (Virtual Private Network)</td>
<td>A means of having the security benefits of a private, dedicated, leased-line network, without the cost of actually owning one. VPN uses cryptography to scramble data so it's unreadable while traveling over the Internet, thus providing privacy over public lines. Companies with branch offices commonly use VPNs to connect multiple locations.</td>
</tr>
<tr>
<td>Worm</td>
<td>A self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers.</td>
</tr>
<tr>
<td>XML</td>
<td>XML is programming code designed especially for Web documents. It allows designers to create their own custom tags for the definition, transmission, validation, and interpretation of data between applications and between organizations.</td>
</tr>
</tbody>
</table>