# Table of Contents

Preface ................................................................. 9
   About This Guide ................................................. 9
   Organization ..................................................... 9
   Typographical Conventions ...................................... 11
   Notes and Cautions ............................................. 11
   Related Documentation ......................................... 11
   Obtaining More Information .................................... 12
   Technical Support ............................................... 12

Chapter 1
Introduction ....................................................... 13
   About the Firewall ................................................ 13
   Features and Benefits ............................................ 14
   About the Management Interfaces ............................... 14

Chapter 2
Getting Started .................................................... 17
   Preparing the Firewall .......................................... 17
   Setting Up the Firewall .......................................... 17
   Using the Firewall Interface .................................... 19
      Navigating to Configuration Pages ............................ 21

Chapter 3
Device Management ............................................... 23
   About Virtual Systems .......................................... 24
      Communications Among Virtual Systems ...................... 25
      Shared Gateways ............................................... 26
      Defining Virtual Systems ...................................... 27
      Configuring Shared Gateways ................................. 28
   About High Availability ........................................ 28
      Setting Up High Availability ................................ 29
      Enabling High Availability on the Firewall ................. 30
   About User Identification Agents ............................... 33
Chapter 5
Policies and Security Profiles ................................................. 119

About Policies ........................................................................ 119
Guidelines on Defining Policies ................................................ 120
About Security Policies ............................................................. 122
About NAT Policies ................................................................... 125
About Policy-Based Forwarding Policies .................................... 128
About SSL Decryption Policies .................................................. 129
Specifying Users and Applications for Policies ............................ 130
About Application Override Policies ........................................... 131
About Captive Portal Policies ..................................................... 132

About Security Profiles .............................................................. 132
About Antivirus Profiles ............................................................ 133
Defining Anti-Spyware Profiles .................................................. 134
About Vulnerability Protection Profiles ...................................... 136
About URL Filtering Profiles ..................................................... 137
Defining File Blocking Profiles .................................................. 139
Defining Data Filtering Profiles .................................................. 139

About Other Policy Objects ....................................................... 141
About Addresses and Address Groups ....................................... 142
About Applications and Application Groups .............................. 143
About Application Filters .......................................................... 151
About Services and Service Groups .......................................... 152
About Data Patterns ................................................................. 153
About Custom URL Categories ................................................ 155
About Custom Threat Signatures .............................................. 155
About Security Profile Groups .................................................. 158
About Log Forwarding .............................................................. 159
About Schedules ....................................................................... 160
Chapter 6
Reports and Logs ................................. 161

Using the Dashboard. .......................... 162
Using the Application Command Center .... 163
Viewing App-Scope Reports .................... 167
  Summary Report ................................ 168
  Change Monitor Report ....................... 169
  Threat Monitor Report ....................... 170
  Threat Map Report ........................... 171
  Network Monitor Report ..................... 172
  Traffic Map Report .......................... 174
Viewing the Logs ............................... 175
Managing PDF Summary Reports ............. 179
Managing User Activity Reports ............. 181
Managing Report Groups ....................... 182
Scheduling Reports for Email Delivery .... 182
Viewing Reports ................................. 183
Generating Custom Reports ................... 183
Identifying Unknown Applications and Taking Action ............................... 187

Chapter 7
Configuring IPSec Tunnels .................... 189

About Virtual Private Networks ............ 190
  About IPSec VPNs and SSL VPNs .......... 191
  About VPN Tunnels .......................... 191
About IPSec and IKE ......................... 191
  About IPSec and IKE Crypto Profiles .... 192
Setting Up IPSec VPNs ....................... 193
Defining IKE Gateways ....................... 194
Defining IKE Crypto Profiles ............... 195
Defining IPSec Crypto Profiles ............. 195
Setting Up IPSec Tunnels .................... 196
Defining Tunnel Monitor Profiles .......... 199
Viewing IPSec Tunnel Status on the Firewall ............................................. 200
Sample VPN Configuration ..................... 201
  Existing Topology ......................... 201
  New Topology ................................ 201
  Configure the VPN Connection .......... 202
  VPN Connectivity Troubleshooting ...... 203

Chapter 8
Configuring SSL VPNs ......................... 205

About SSL VPNs ............................... 206
How the SSL VPN Works ....................... 206
Preface

This preface contains the following sections:

- “About This Guide” in the next section
- “Organization” on page 9
- “Typographical Conventions” on page 11
- “Notes and Cautions” on page 11
- “Related Documentation” on page 11
- “Obtaining More Information” on page 12
- “Technical Support” on page 12

About This Guide

This guide describes how to administer the Palo Alto Networks firewall using the device’s web interface.

This guide is intended for system administrators responsible for deploying, operating, and maintaining the firewall.

Organization

This guide is organized as follows:

- **Chapter 1, “Introduction”—Provides an overview of the firewall.**
- **Chapter 2, “Getting Started”—Describes how to install the firewall.**
- **Chapter 3, “Device Management”—Describes how to perform basic system configuration and maintenance for the firewall, including how to configure a pair of firewalls for high availability, define user accounts, update the software, and manage configurations.**
- **Chapter 4, “Network Configuration”—Describes how to configure the firewall for your network, including routing configuration.**
- **Chapter 5, “Policies and Security Profiles”—Describes how to configure security policies and profiles by zone, users, source/destination address, and application.**
Organization

• Chapter 6, “Reports and Logs”—Describes how to view the reports and logs provided with the firewall.

• Chapter 7, “Configuring IPSec Tunnels”—Describes how to configure IP Security (IPSec) tunnels on the firewall.

• Chapter 8, “Configuring SSL VPNs”—Describes how configure virtual private networks (VPNs) using Secure Socket Layer (SSL).

• Chapter 9, “Configuring Quality of Service”—Describes how to configure quality of service (QoS) on the firewall.

• Chapter 10, “Panorama Installation”—Describes how to install the centralized management system (CMS) for the High Definition Firewalls.

• Chapter 11, “Central Management of Devices”—Describes how to use Panorama to manage multiple firewalls.

• Appendix A, “Custom Pages”—Provides HTML code for custom response pages to notify end users of policy violations or special access conditions.

• Appendix B, “Application Categories, Subcategories, Technologies, and Characteristics”—Contains a list of the application categories defined by Palo Alto Networks.


• Appendix D, “Open Source Licenses”—Includes information on applicable open source licenses.
Typographical Conventions

This guide uses the following typographical conventions for special terms and instructions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Names of commands, keywords, and selectable items in the web interface</td>
<td>Click <strong>Security</strong> to open the Security Rules page.</td>
</tr>
<tr>
<td><em>italics</em></td>
<td>Name of parameters, files, directories, or Uniform Resource Locators (URLs)</td>
<td>The address of the Palo Alto Networks home page is <a href="http://www.paloaltonetworks.com">http://www.paloaltonetworks.com</a></td>
</tr>
<tr>
<td><strong>courier font</strong></td>
<td>Coding examples and text that you enter at the command prompt</td>
<td>Enter the following command: <code>a:\setup</code></td>
</tr>
<tr>
<td><strong>Click</strong></td>
<td>Click the left mouse button</td>
<td>Click <strong>Administrators</strong> under the <strong>Devices</strong> tab.</td>
</tr>
<tr>
<td><strong>Right-click</strong></td>
<td>Click the right mouse button.</td>
<td>Right-click on the number of a rule you want to copy, and select <strong>Clone Rule</strong>.</td>
</tr>
</tbody>
</table>

Notes and Cautions

This guide uses the following symbols for notes and cautions.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="NOTE" /></td>
<td>Indicates helpful suggestions or supplementary information.</td>
</tr>
<tr>
<td><img src="image" alt="CAUTION" /></td>
<td>Indicates actions that could cause loss of data.</td>
</tr>
</tbody>
</table>

Related Documentation

The following additional documentation is provided with the firewall:

- *Quick Start*
- *Hardware Reference Guide*
- *Command Line Interface Reference Guide*
Obtaining More Information

To obtain more information about the firewall, refer to:

- **Palo Alto Networks web site**—Go to [http://www.paloaltonetworks.com](http://www.paloaltonetworks.com).
- **Online help**—Click Help in the upper-right corner of the web interface to access the online help system.

Technical Support

For technical support, use the following methods:

- Go to [http://support.paloaltonetworks.com](http://support.paloaltonetworks.com).
- Call 1-866-898-9087 (U.S, Canada, and Mexico).
- Email us at: [support@paloaltonetworks.com](mailto:support@paloaltonetworks.com).
Chapter 1
Introduction

This chapter provides an overview of the firewall:

• “About the Firewall” in the next section
• “Features and Benefits” on page 14
• “About the Management Interfaces” on page 14

About the Firewall

The Palo Alto Networks firewall allows you to specify security policies based on a more accurate identification of each application seeking access to your network. Unlike traditional firewalls that identify applications only by protocol and port number, the firewall uses packet inspection and a library of application signatures to distinguish between applications that have the same protocol and port, and to identify potentially malicious applications that use non-standard ports.

For example, you can define security policies for specific applications, rather than rely on a single policy for all port 80 connections. For each identified application, you can specify a security policy to block or allow traffic based on the source and destination zones and addresses (IPv4 and IPv6). Each security policy can also specify security profiles to protect against viruses, spyware, and other threats.

IPv4 and IPv6 addresses are supported.
Features and Benefits

The firewall provides granular control over the traffic allowed to access your network. The primary features and benefits include:

- **Application-based policy enforcement**—Access control by application is far more effective when application identification is based on more than just protocol and port number. High risk applications can be blocked, as well as high risk behavior, such as file-sharing. Traffic encrypted with the Secure Socket Layer (SSL) can be decrypted and inspected.

- **Threat prevention**—Threat prevention services that protect the network from viruses, worms, spyware, and other malicious traffic can be varied by application and traffic source (refer to “About Security Profiles” on page 132).

- **URL filtering**—Outbound connections can be filtered to prevent access to inappropriate web sites (refer to “About URL Filtering Profiles” on page 137).

- **Traffic visibility**—Extensive reports, logs, and notification mechanisms provide detailed visibility into network application traffic and security events. The Application Command Center in the web interface identifies the applications with the most traffic and the highest security risk (refer to “Reports and Logs” on page 161).

- **Networking versatility and speed**—The firewall can augment or replace your existing firewall, and can be installed transparently in any network or configured to support a switched or routed environment. Multi-gigabit speeds and a single-pass architecture provide all services with little or no impact on network latency.

- **Fail-safe operation**—High availability support provides automatic failover in the event of any hardware or software disruption (refer to “Enabling High Availability on the Firewall” on page 30).

- **Easily managed**—Each firewall can be managed through an intuitive web interface or a command-line interface (CLI), or all devices can be centrally managed through the Panorama centralized management system, which has a web interface very similar to the device web interface.

About the Management Interfaces

The firewall supports the following management interfaces:

- **Web interface**—Configuration and monitoring over HTTP or HTTPS from an Internet Explorer (IE) or Firefox browser.

- **CLI**—Text-based configuration and monitoring over Telnet, Secure Shell (SSH), or the console port (refer to the **PAN-OS Command Line Interface Reference Guide**).

- **Panorama**—Palo Alto Networks product that provides web-based management for multiple firewalls. The Panorama interface is similar to the device web interface, with additional management functions included. Refer to “Panorama Installation” on page 219 for instructions on installing Panorama and “Central Management of Devices” on page 223 for information on using Panorama.
• **Simple Network Management Protocol (SNMP)**—Supports RFC 1213 (MIB-II) and RFC 2665 (Ethernet interfaces) for remote monitoring, and generates SNMP traps for one or more trap sinks (refer to “Defining SNMP Trap Destinations” on page 63 and “SNMP MIBs” on page 245.

• **Syslog**—Provides message generation for one or more remote syslog servers (refer to “Defining Syslog Servers” on page 64).
Chapter 2
Getting Started

This chapter describes how to set up and start using the firewall:
• “Preparing the Firewall” in the next section
• “Setting Up the Firewall” on page 17
• “Using the Firewall Interface” on page 19

Note: Refer to “Panorama Installation” on page 219 for instructions on installing the Panorama centralized management system.

Preparing the Firewall

Perform the following tasks to prepare the firewall for setup:
1. Mount the firewall in a rack and power it up as described in the Hardware Reference Guide.
2. Register your firewall at http://support.paloaltonetworks.com to obtain the latest software and App-ID updates, and to activate support or subscriptions.
3. Obtain an IP address from your system administrator for configuring the management port on the firewall.
4. Set the IP address on your computer to 192.168.1.2 and the subnet mask to 255.255.255.0.

Setting Up the Firewall

To perform the initial firewall setup:
1. Connect your computer to the management port (MGT) on the firewall using an RJ-45 Ethernet cable.
2. Start your computer. Assign a static IP address to your computer on the subnet 192.168.1.0 (for example, 192.168.1.5).
3. Launch a supported web browser and enter \texttt{https://192.168.1.1}.
   The browser automatically opens the Palo Alto Networks login page.

4. Enter \texttt{admin} in both the \texttt{Name} and \texttt{Password} fields, and click \texttt{Login}. The system presents a warning that the default password should be changed. Click \texttt{OK} to continue.

5. On the Device tab, click the \texttt{Quick Start Setup} link to open the Quick Start page.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{quick_start_setup.png}
\caption{Quick Start Setup Page}
\end{figure}

6. Perform these tasks on the Quick Start Setup page:
   \begin{enumerate}
   \item In the Management Configuration area, enter the IP address of the Domain Name Service (DNS) server. Enter the IP address or host and domain name of the Network Time Protocol (NTP) server and select your time zone. If you do not use NTP, you can enter a time manually on the \texttt{Setup} page. Refer to “About System Setup, Configuration, and License Management” on page 66.
   \item If this is the first Palo Alto Networks firewall for your company, click the \texttt{Support} link and register the firewall. If you have already registered a firewall, you have received a user name and password and the license authorization code for any optional features. Enter these on the page. Use a space to separate multiple authorization codes.
   \item Select the \texttt{Update Application and Threat Content} check box to automatically update the firewall with the latest application and threat data. Select the \texttt{Update Software} check box to update the firewall with the latest available software.
   \item Click \texttt{Proceed} to apply the settings and close the page.
   \end{enumerate}

7. Click \texttt{Administrators} under the \texttt{Devices} tab.

8. Click \texttt{admin}.

9. In the \texttt{New Password} and \texttt{Confirm New Password} fields, enter and confirm a case-sensitive password (up to 15 characters).
10. Click **OK** to submit the new password.

**Using the Firewall Interface**

Figure 2 shows the firewall web interface.

**Figure 2. Firewall Web Interface**
The following conventions apply when using the firewall interface.

- To display the menu items for a general functional category, click the tab, such as **Object** or **Devices**, near the top of the browser window.

- Click an item on the side menu to display a panel.

- To display submenu items, click the icon to the left of an item. To hide submenu items, click the icon to the left of the item.

- On most configuration pages, you can click **New** to create a new item.

- To delete one or more items, select their check boxes and click **Delete**. In most cases, the system prompts you to confirm by clicking **OK** or to cancel the deletion by clicking **Cancel**.

- On some configuration pages, you can select the check box for an item and click **Clone** to create a new item with the same information as the selected item.
• To modify an item, click its underlined link.

• After you configure settings, you must click **OK** or **Save** to store the changes. When you click **OK**, the current “candidate” configuration is updated. Clicking **Commit** at the top of the page applies the candidate configuration to the active configuration, which activates all configuration changes since the last commit. For more information about committing changes, refer to “Managing Configurations” on page 72.

• To view help information on a page, click the icon in upper right area of the page.

**Navigating to Configuration Pages**

Each configuration section in this guide shows the menu path to the configuration page. For example, to reach the Vulnerability Protection Profiles page, choose the **Objects** tab and then choose **Vulnerability Profiles** under **Security Profiles** in the side menu. This is indicated in this guide by the following path:

► **Objects > Security Profiles > Vulnerability Profiles**
Chapter 3
Device Management

This chapter describes how to perform basic system configuration and maintenance for the firewall and includes overviews of the virtual systems, high availability, and logging functions:

• “About Virtual Systems” in the next section
• “About High Availability” on page 28
• “About User Identification Agents” on page 33
• “About Administrator Roles, Profiles, and Accounts” on page 53
• “About Authentication Profiles” on page 54
• “About the Firewall Logs” on page 60
• “About System Setup, Configuration, and License Management” on page 66
• “Defining Custom Response Pages” on page 74
• “Upgrading the PAN-OS Software” on page 75
• “Updating Threat and Application Definitions” on page 76
• “Importing, Exporting and Generating Security Certificates” on page 77
• “Viewing Support Information” on page 80
A virtual system specifies a collection of physical and logical firewall interfaces (including VLANs, and virtual wires) and security zones. (For more information on security zones, refer to “Defining Security Zones” on page 97.) Virtual systems allow you to customize administration, networking, and security policies for the network traffic that is associated with specific departments or customers.

**Note:** The PA-4000 Series firewalls support multiple virtual systems. The PA-2000 firewalls can support multiple virtual systems if the appropriate license is installed. The PA-500 firewall does not support virtual systems.

For example, if you want to customize the security features for the traffic that is associated with your Finance department, you can define a Finance virtual system and then define security policies to apply only to that department.

Figure 3 illustrates the relationship between policies and virtual systems in the firewall. Policies are associated with individual virtual systems, by contrast with device and network level functions, which apply to the overall firewall.

To optimize policy administration, you can create virtual system administrator accounts that allow access to individual virtual systems, while maintaining separate administrator accounts for overall device and network functions. For example, a virtual system administrator in the Finance department can be assigned to manage the security policies only for that department.
Initially all interfaces, zones, and policies belong to the default virtual system (vsys1). When you enable multiple virtual systems, note the following:

- All items needed for policies are created and administered by a virtual systems administrator.
- Zones are objects within virtual systems. Before defining a policy or policy object, select the virtual system from the Virtual System drop-down list on the Policies or Objects tab.
- Interfaces, VLANs, virtual wires, and virtual routers can be assigned to virtual systems. Refer to “Defining Virtual Systems” on page 27.
- Remote logging destinations (SNMP, syslog, and email), as well as applications, services, and profiles, can be shared by all virtual systems or be limited to a selected virtual system.

Communications Among Virtual Systems

The virtual systems in the firewall are treated as separate entities. To support internal traffic flows between virtual systems, you must indicate which virtual systems are able to communicate with each other. You do so when configuring a virtual system by specifying the other virtual systems that are visible to it. Then when creating a zone, you can select the “external” type and specify the virtual systems to include in the zone. Refer to “Defining Security Zones” on page 97.

Each virtual system must have policies for sending and receiving traffic. For example, allowing Dept 1 VSYS to communicate with Dept 2 VSYS requires a policy in Dept 1 VSYS to allow traffic to go to Dept 2 VSYS and a policy in Dept 2 VSYS to accept incoming traffic from Dept 1 VSYS.
Shared Gateways

In a standard virtual system interface configuration, each virtual system uses a dedicated interface to the outside world. Each virtual system is autonomous, and there are no direct communication paths among the virtual systems that are internal to the firewall, unless such communications are explicitly configured (refer to “Communications Among Virtual Systems” on page 25). Because each virtual system has its own IP address, multiple addresses are required for external communications.

Shared gateways allow virtual systems to share a common interface for external communications. This is especially helpful in deployments where the Internet Service Provider (ISP) provides only a single IP address. All of the virtual systems communicate with the outside world through the physical interface using a single IP address (see Figure 6). A single virtual router is used to route the traffic for all of the virtual systems through the shared gateway.
About Virtual Systems

All policy rules are managed at the virtual system level. However, you can create NAT and policy-based forwarding rules through the shared gateway, if needed, by selecting the shared gateway from the Virtual System drop-down list on the policy screen.

Defining Virtual Systems

Device > Virtual Systems

To define virtual systems, you must first enable the definition of multiple virtual systems. To do so, open the Device > Setup page, click Edit in the Multi Virtual System Capability table, and select the Allow multiple virtual systems check box. This adds a Virtual Systems link to the side menu.

You can now open the Virtual Systems page, click New, and specify the following information.

Table 1. Virtual System Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Enter an integer identifier for the virtual system. Refer to the data sheet for your firewall model for information on the number of supported virtual systems.</td>
</tr>
<tr>
<td>Virtual System</td>
<td>Enter a virtual system name (up to 31 characters) that will be displayed in the web interface to identify the virtual system. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. Only the name is required.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Select the physical and logical interfaces, VLANs, virtual wires, and virtual routers that belong to the virtual system.</td>
</tr>
<tr>
<td>Dot1q VLANs</td>
<td></td>
</tr>
<tr>
<td>Virtual Wires</td>
<td></td>
</tr>
<tr>
<td>Virtual Routers</td>
<td></td>
</tr>
<tr>
<td>Visible Virtual Systems</td>
<td>Select check boxes for the virtual systems that will allow traffic from this virtual system. Each visible virtual system appears as a security zone that you can select when setting up policies.</td>
</tr>
</tbody>
</table>

After defining the virtual systems, you can perform any of the following additional tasks:

- To change a virtual system, click the virtual system name or the name of the interface, VLAN, virtual wire, virtual router, or visible virtual systems you want to change, make the appropriate changes, and click OK.

- To define security zones for the new virtual system, choose Network > Zones and define security zones for each new virtual system (refer to “Defining Security Zones” on page 97). When you define a new zone, you can now select a virtual system.

- Click Network > Interfaces and verify that each interface has a virtual system and security zone.
Configuring Shared Gateways

Shared gateways use Layer 3 interfaces, and at least one Layer 3 interface must be configured to configure a shared gateway. Refer to “Configuring Layer 3 Interfaces” on page 88.

To add a shared gateway, click New, and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identifier for the gateway (not used by firewall).</td>
</tr>
<tr>
<td>Virtual System</td>
<td>Enter a name for the shared gateway (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. Only the name is required.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Select check boxes for the interfaces that the shared gateway will use.</td>
</tr>
</tbody>
</table>

About High Availability

You can deploy firewalls in active/passive pairs so that if the active firewall fails for any reason, the passive firewall becomes active automatically with no loss of service. A failover can also occur if selected Ethernet links fail or if the active firewall cannot reach one or more of the specified destinations.

The following rules apply to high availability (HA) operation and failover:

- The active firewall continuously synchronizes its configuration and session information with the passive firewall over the high availability interfaces.
- If the active firewall fails, then the passive firewall detects that heartbeats are lost and automatically becomes active.
- If one high availability interface fails, synchronization continues over the remaining interface. If the state synchronization connection is lost, then no state synchronization occurs. If the configuration synchronization is lost, heartbeats are lost. Both devices determine that the other is down, and both become active.

**Note:** In an active/passive pair, both firewalls must be the same model and have the same licenses. If state synchronization is enabled, sessions continue after a switchover; however, threat prevention functions do not continue.

**Note:** On the PA-2000 Series and PA-500 firewalls, you specify the data ports to use for high availability. On the PA-4000 Series, there are dedicated physical ports for high availability.
Setting Up High Availability

To set up high availability, follow these steps:

1. Use two firewalls with the same model number.

2. Mount the passive firewall on a rack near the active firewall, and power it up as described in the Hardware Reference Guide. If this is an existing installation, perform a factory reset in maintenance mode by selecting the Factory Reset option from the main menu. Refer to the PAN-OS Command Line Interface Reference Guide.

3. Connect the passive firewall to your network and the Internet using the same physical ports as the active firewall.

4. Using two crossover RJ-45 Ethernet cables, connect the HA1 and HA2 ports on the passive firewall to the HA1 and HA2 ports on the active firewall, or connect the ports on both firewalls to a switch.

   Note: On the PA-2000 and PA-500 Series, you must use the traffic interfaces for high availability. For example, connect the ethernet1/15 interfaces to each other and the ethernet1/6 interfaces to each other.

5. Open the Network tab and verify that the high availability links are up. Configure each to be of the type high availability.

   ![Figure 7. Verifying high availability Interfaces](image)


Item to note when setting up high availability

Crossover cables are recommended when high availability links are directly connected.
Enabling High Availability on the Firewall

After setting up high availability as described in “Setting Up High Availability” on page 29, you can enable high availability on both the active and passive firewall. For each section on the High Availability page, click Edit in the header, and specify the corresponding information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Setup</strong></td>
<td></td>
</tr>
<tr>
<td>Enable HA</td>
<td>Select the check box to enable high availability.</td>
</tr>
<tr>
<td>ID</td>
<td>Enter a number to identify the active/passive pair (1 to 254). Allows multiple pairs of active/passive firewalls to reside on the same network.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the active/passive pair (optional).</td>
</tr>
<tr>
<td>Peer IP Address</td>
<td>Enter the IP address of the HA1 interface specified in the Control Link section of the other firewall.</td>
</tr>
<tr>
<td><strong>Control Link</strong></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>(If supported on your firewall model) Select the HA port.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the HA1 interface for the current firewall.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Enter the network mask for the IP address, such as “255.255.255.0”.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Select the check box if you want to encrypt communications over the high availability link, and enter a passphrase. The same passphrase must be entered in both firewalls.</td>
</tr>
<tr>
<td>Monitor Hold Time</td>
<td>Enter the length of time (milliseconds) that the system will wait before determining that the control link is down (1000-60000 ms, default 3000 ms).</td>
</tr>
<tr>
<td>Link Speed (PA-4000 only)</td>
<td>Select the speed for the data link between the active and passive firewalls.</td>
</tr>
<tr>
<td>Link Duplex (PA-4000 only)</td>
<td>Select a duplex option for the data link between the active and passive firewalls.</td>
</tr>
<tr>
<td><strong>Data Link</strong></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>(If supported on your firewall model) Select the high availability port.</td>
</tr>
<tr>
<td>Enable State Synchronization</td>
<td>Select the check box to enable synchronization of the configuration and session information with the passive firewall.</td>
</tr>
<tr>
<td>Link Speed (PA-4000 only)</td>
<td>Select the speed for the control link between the active and passive firewalls.</td>
</tr>
<tr>
<td>Link Duplex (PA-4000 only)</td>
<td>Select a duplex option for the control link between the active and passive firewalls.</td>
</tr>
</tbody>
</table>
### About High Availability

#### Election Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Priority</td>
<td>Enter a priority value to identify the active firewall. The firewall with the lower value (higher priority) becomes the active firewall (range 0-255).</td>
</tr>
<tr>
<td>Preemptive</td>
<td>Select the check box to enable the higher priority firewall to resume active operation after recovering from a failure. If this setting is off, then the lower priority firewall remains active even after the higher priority firewall recovers from a failure.</td>
</tr>
<tr>
<td>Passive Hold Time</td>
<td>Enter the delay between the occurrence of a failover condition and the initiation of a failover action (range 0-60000 ms, default 0 ms).</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Enter the number of milliseconds between the hello packets sent to verify that the other firewall is operational (ranges 1000-60000 ms for PA-4000 and 8000-60000 for PA-2000/PA-500, default 1000 ms on the PA-4000, 8000 ms on PA-2000/PA-500).</td>
</tr>
<tr>
<td>Heartbeat Interval</td>
<td>Specify how frequently the passive firewall checks for a response from the active firewall (range 1000-60000 ms, default 1000 ms).</td>
</tr>
<tr>
<td>Passive Link State</td>
<td>Choose from the following options:</td>
</tr>
<tr>
<td></td>
<td>• auto—Causes the link status to reflect physical connectivity, but discards all packets received. This option is supported in Layer 3 mode. The auto option is desirable, if it is feasible for your network.</td>
</tr>
<tr>
<td></td>
<td>• shutdown—Forces the interface link to the down state. This is the default option, which ensures that loops are not created in the network.</td>
</tr>
<tr>
<td>Maximum No. of Flaps</td>
<td>A flap is counted when the firewall leaves the active state within 15 minutes after it last left the active state. You can specify the maximum number of flaps that are permitted before the firewall is determined to be suspended and the passive firewall takes over (range 0-16, default 3). The value 0 means there is no maximum (an infinite number of flaps is required before the passive firewall takes over).</td>
</tr>
<tr>
<td>Monitor Fail Hold Time</td>
<td>Specify the interval that the firewall waits following a path monitor or link monitor failure before attempting to re-enter the passive state (default 1 min). During this period, the device is not available to take over for the active device in the event of failure.</td>
</tr>
<tr>
<td>Preemption Hold Time</td>
<td>Specify the interval during which the preempting device remains in the passive state before taking over as the active device (default 1 min).</td>
</tr>
</tbody>
</table>
**Issues to note when configuring high availability**

- The firewall that is assigned the lower device priority value is the higher priority device and becomes the active firewall in a high availability pair.

- The Preemptive option must be enabled on both devices for the higher priority firewall to resume active operation upon recovery following a failure.

- The subnet that is used for the local and peer IP should not be used anywhere else on the virtual router.

### Table 3. High Availability Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Monitoring</td>
<td>Select the check box to enable path monitoring. Path monitoring enables the firewall to monitor specified destination IP addresses by sending ICMP ping messages to make sure that they are responsive. Use path monitoring for virtual wire or Layer 3 configurations where monitoring of other network devices is required for failover and link monitoring alone may not be enough.</td>
</tr>
<tr>
<td>Failure Condition</td>
<td>Select whether a failover occurs when any or all of the monitored path groups fail to respond.</td>
</tr>
<tr>
<td>Path Groups</td>
<td>Define one or more path groups to monitor specific destination addresses. To add a path group, specify the following and click <strong>Add</strong>:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>—Select an interface type (Virtual Wire, VLAN, or Virtual Router).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Name</strong>—Select an interface of the specified type.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Enabled</strong>—Select the check box to enable the path group.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Failure Condition</strong>—Select whether a failure occurs when any or all of the specified destination addresses fail to respond.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Source IP</strong>—For virtual wire and VLAN interfaces, enter the source IP address used in the probe packets sent to the specified destination addresses. The local router must be able to route the address to the firewall.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Destination IPs</strong>—Enter one or more destination addresses to be monitored (multiple addresses must be separated by commas).</td>
</tr>
<tr>
<td></td>
<td>To delete a path group, select the group, and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Link Monitoring</th>
<th>Select the check box to enable link monitoring. Link monitoring allows failover to be triggered when a physical link or group of physical links fails. Use link monitoring for virtual wire or Layer 3 configurations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Condition</td>
<td>Select whether a failover occurs when any or all of the monitored link groups fail.</td>
</tr>
<tr>
<td>Link Groups</td>
<td>Define one or more link groups to monitor specific Ethernet links. To add a link group, specify the following and click <strong>Add</strong>:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Name</strong>—Enter a link group name.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Enabled</strong>—Select the check box to enable the link group.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Failure Condition</strong>—Select whether a failure occurs when any or all of the selected links fail.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Interfaces</strong>—Select one or more Ethernet interfaces to be monitored (multiple addresses must be separated by commas).</td>
</tr>
<tr>
<td></td>
<td>To delete a link group, select the group, and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>
• The OS and Content versions should be the same on each device. A mismatch can prevent the devices in the cluster from synchronizing.

• The HA1 MAC address for each firewall is unique, but the HA2 MAC address is the same on both devices.

• The LEDs are green on the high availability ports for the active firewall and amber on the passive firewall.

• To test failover, pull a cable on the active device, or put the active device into a suspend state by issuing the CLI command `request high-availability state suspend`. You can also suspend the active device by pressing the Suspend link at the top right corner of the High Availability configuration page on the Device tab.

• To place a suspended device back into a functional state, use the CLI command `request high-availability state functional`.

• To view detailed high availability information about the local firewall, use the CLI command `show high-availability all`.

• To compare the configuration of the local and peer firewalls, use the CLI command `show high-availability state` from either device. You can also compare the configurations on the local and peer firewalls using the Config Audit tool on the Device tab by selecting the desired local configuration in the left selection box and the peer configuration in the right selection box.

• Synchronize the firewalls from the web interface by pressing the Push Configuration button located in the high availability widget on the ACC tab. Note that the configuration on the device from which you push the configuration overwrites the configuration on the peer device. To synchronize the firewalls from the CLI on the active device, use the command `request high-availability sync-to-remote running-config`.

• To follow the status of the load, use the CLI command `show jobs processed`.

---

**About User Identification Agents**

A User Identification Agent (User-ID Agent) is a Palo Alto Networks application that is installed on your network to obtain needed mapping information between IP addresses and network users. The User-ID Agent collects user-to-IP address mapping information automatically and provides it to the firewall for use in security policies and logging. The IP address-to-user name mapping relies on the following mechanisms:

• For Active Directory, the security logs are continually monitored to detect user login events that contain user and IP address information.

• For Active Directory, a direct connection is required to all Domain Controllers to monitor user session activity and determine the user IP addresses.

• For eDirectory, when a user logs in, the IP address information is stored in eDirectory and retrieved by the User-ID Agent.

• For eDirectory, the host PC is polled to verify IP address and user information using WMI or NetBIOS. This occurs every 20 minutes to verify that the IP address-to-user name mapping is still correct and when an IP address is seen that does not have an associated user name.
The User-ID Agent API is used to send information on user IP addresses to the User-ID Agent.

The user-to-group mapping relies on the following mechanisms:

- For Active Directory, a direct connection to a Domain Controller that hosts user and group membership information. The group membership information is used to map users to groups and domains for the application of policies. This information is synchronized on an hourly basis (by default), regardless of whether the users are currently online. All group information for the domain is included.

- For eDirectory and other Lightweight Directory Access Protocol (LDAP) based directories, the device queries the directory directly for user and group information.

The following figure shows how the Active Directory and eDirectory/LDAP methods are applied. For Active Directory, the User-ID Agent associates users and groups and performs the user-IP address mapping. For eDirectory, the firewall associates the users and groups while the User-ID Agent performs the user-IP address mapping.

![Figure 8. User-ID Agents](image)

**Note:** User identification mapping requires that the firewall obtain the source IP address of the user before the IP address is translated with NAT. If multiple users appear to have the same source address, due to NAT or use of a proxy device, accurate user identification is not possible.

In addition to the User-ID Agents, the firewall supports a Terminal Services Agent (TS agent) that allows the firewall to identify individual users who are supported by the same terminal server. The firewall also supports captive portals for situations in which the User-ID Agent is unable to associate a user with an IP address.
Refer to the following sections for further information:

- “About Captive Portals” in the next section
- “Configuring the Firewall for User Identification” on page 35
- “About the User-ID Agent for Active Directory” on page 37
- “About the User-ID Agent for eDirectory or API” on page 42
- “About the Terminal Services Agent” on page 48

### About Captive Portals

If the User-ID Agent is unable to associate a user with an IP address, a captive portal can take over and authenticate the user with a web form or NTLM challenge. To receive the web form, users must be using a web browser and be in the process of connecting. Upon successful authentication, users are automatically directed to the originally requested web site. The firewall can now execute policies based on the user information for any applications passing through the firewall, not just for applications that use a web browser. The following rules apply to captive portals:

- Captive portal rules work only for web traffic (HTTP or HTTPS).
- If the action for the rule is “web form,” a web form is presented to the user to prompt for a password.
- If rule is “NTLM” and the browser is Internet Explorer or Firefox, the firewall performs an NTLM authentication challenge (transparent to the user). If another browser is used, the web form is presented.

If the above-mentioned captive portal rules do not apply because the traffic is not HTTP/HTTPS or there is no rule match, then the firewall applies its IP-based security policies (as opposed to user-based security policies).

### Configuring the Firewall for User Identification

▶ **Device > User Identification**

Follow the instructions in this section to configure the firewall for IP address-to-user mappings and to set up captive portals.

To specify the User-ID Agent for IP address-to-user mappings, click **Add** in the User Identification area and specify the following information.

### Table 4. User-ID Agent Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the User-ID Agent.</td>
</tr>
<tr>
<td>Virtual System</td>
<td>Select the virtual system from the drop-down list (if supported on the firewall model).</td>
</tr>
</tbody>
</table>
To enable captive portal and configure RADIUS servers to authenticate users who enter through captive portals, click **Edit** in the Captive Portal area and specify the following settings.

### Table 5. Captive Portal Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual System</td>
<td>Select the virtual system from the drop-down list (if supported on the firewall model).</td>
</tr>
<tr>
<td>Enable Captive Portal</td>
<td>Select to enable the captive port option for authentication.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain for the captive portal web page.</td>
</tr>
<tr>
<td>Idle Time</td>
<td>Enter the length of time after which the captive portal page times out (5-1440 minutes, default 5 minutes).</td>
</tr>
<tr>
<td>Expiration</td>
<td>Enter the length of time after which the captive portal page expires and must be reopened (5-1440 minutes, default 5 minutes).</td>
</tr>
<tr>
<td>Server Certificate</td>
<td>Select the certificate to use for authentication on the captive portal page.</td>
</tr>
<tr>
<td>User Identification Agent</td>
<td>Select the User-ID Agent to use for IP address-to-user mapping.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Specify the name of a host for HTTP redirection.</td>
</tr>
</tbody>
</table>
| Mode                | Choose whether the captive portal will use a redirection or be transparent to the user.  
                     | Redirection is required for NTLM and session cookie retention. With the redirection option, the firewall can set a cookie for future login requests. Future redirection then becomes transparent to the user if the browser has not been closed.  
                     | For redirection, specify the following settings:  
                     | • **Address**—Enter the IP address or host name to which the captive portal is redirected.  
                     | • **Enable**—Select the check box to configure an interval after which the redirection times out.  
                     | • **Timeout**—If **Enable** is selected, specify the timeout interval (range 60 - 10080 minutes, default 1440 minutes).  
                     | • **Roaming**—Select the check box if to retain the cookie if the IP address changes while the browser is open (for example, if the client moves from a wired to wireless network). The cookie is lost when the browser closes, whether or not **Roaming** is selected. |

To specify LDAP servers for user identification, click **Add** in the LDAP Server area and specify the following information.
About User Identification Agents

The User-ID Agent interfaces with Active Directory to communicate user group, user, and IP address information to the firewall for visibility only or visibility and policy enforcement. After it is installed, the agent initiates a process to map users to IP addresses.

The User-ID Agent is available for download from Palo Alto Networks. You can install the agent on one or more Windows PCs on your network to obtain user-specific information. When user identification is configured, the firewall’s Application Command Center, App-Scope, and logs all include the user name in addition to the user IP address. For policy enforcement, users and user groups can be selected in security and SSL decryption policies when Active Directory is used.

Follow the instructions in this section to install and configure the User-ID Agent.

Note: If the multiple virtual system capability is on, you can configure one or more agents per virtual system. This is useful to separate user identification in support of ISPs or other entities that maintain separate user records.

### Table 6. User-ID Agent Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual System</td>
<td>Select the virtual system from the drop-down list (if supported on the firewall model).</td>
</tr>
<tr>
<td>Enable</td>
<td>Select to enable LDAP user identification on the firewall.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name to identify the server in the firewall.</td>
</tr>
<tr>
<td>Server Profile</td>
<td>Select the profile from the drop-down list.</td>
</tr>
<tr>
<td>Domain</td>
<td>Specify the domain of the LDAP server.</td>
</tr>
<tr>
<td>Update Interval</td>
<td>(1-3600 seconds).</td>
</tr>
<tr>
<td>Group Filter</td>
<td>Specify an LDAP query that can be used to control which groups are retrieved and tracked. The query should be a filter that includes one group with all users in it and any other groups that you want to use in setting policy.</td>
</tr>
<tr>
<td>User Filter</td>
<td>Specify an LDAP query that can be used to control which users are retrieved and tracked.</td>
</tr>
<tr>
<td>Groups</td>
<td>Specify the definition of a group. For example, the default is objectClass=group, which means that the system retrieves all objects in the directory that match the group filter and have objectClass=group.</td>
</tr>
<tr>
<td>Users</td>
<td>Specify the definition of a user.</td>
</tr>
</tbody>
</table>

### About the User-ID Agent for Active Directory

The User-ID Agent interfaces with Active Directory to communicate user group, user, and IP address information to the firewall for visibility only or visibility and policy enforcement. After it is installed, the agent initiates a process to map users to IP addresses.

The User-ID Agent is available for download from Palo Alto Networks. You can install the agent on one or more Windows PCs on your network to obtain user-specific information. When user identification is configured, the firewall’s Application Command Center, App-Scope, and logs all include the user name in addition to the user IP address. For policy enforcement, users and user groups can be selected in security and SSL decryption policies when Active Directory is used.

Follow the instructions in this section to install and configure the User-ID Agent.
Verifying Privileges for the PC User

The PC user who configures the User-ID Agent must be a member of the Server Operator user group on the PC.

To verify the privilege level of the PC user:
2. Right-click PANAgentService and select Properties.
3. Open the Log On tab.

![User-ID Agent Service Properties](image)

Figure 9. User-ID Agent Service Properties

4. Choose a local system account with Server Operator privileges, or select This Account and browse or enter information for an account with Server Operator privileges.
5. Click OK and then close the Services window.

Installing the User-ID Agent

The system on which the User-ID Agent is installed must be running Windows 2008, Windows XP with Service Pack 2, or Windows Server 2003 with Service Pack 2.

Each PC that is included for user identification must be part of the Active Directory domain. For machines that are not part of the Active Directory domain, you can use the captive portal capability to screen users and verify user names and passwords.
About User Identification Agents

Refer to these sections for additional information:

- “Configuring the Firewall for User Identification” on page 35—Describes how to set up the firewall to communicate with the User-ID Agents and support captive portals.
- “About Security Profile Groups” on page 158—Describes how to set up captive portal policies.

To install the User-ID Agent, open the installer file and follow the on-screen instructions.

**Configuring the User-ID Agent**

To open the User-ID Agent:
1. Choose **Start > All Programs > Palo Alto Networks > User Identification Agent**.

![User-ID Agent Window](image)

**Figure 10. User-ID Agent Window**

The window contains the following areas and functions:

- **Agent Status**—Displays the current status of the User-ID Agent.
- **Get Groups**—Lists the groups that were retrieved from the directory. Select a group to display its individual members.
- **IP to Username Information**—Lists the mappings of user name to IP address. To retrieve information for a specific IP address, enter the address and click **Get IP Information**. To display all the available information, click **Get All**.
- **LDAP**—Displays the group and user hierarchy from the directory, based on LDAP. Click **Get LDAP tree** to refresh this information.
- **Configure**—Allows you to configure settings for the User-ID Agent.
About User Identification Agents

- **Filter Group Members**—Configures the groups from which the agent extracts users. Only the users that belong to the selected filtered groups are read from the Domain Controller. This option can minimize the traffic between the User-ID Agent and the Domain Controller, and thereby improve overall performance. This approach is effective if there are numerous groups but only a few are intended for use in device policy.

- **Ignore Groups**—Configures the groups with users that the User-ID Agent should ignore. If this option is set, then the users that belong to one of the selected ignored groups are added to the ignore user list for this User-ID Agent.

To configure the User-ID Agent:
1. Choose **Start > All Programs > Palo Alto Networks > User Identification Agent**.
2. Click **Configure** to open the configuration window.

![User Identification Configuration Window](image)

**Figure 11. User Identification Configuration Window**

3. Enter a fully qualified domain name and the port number that you want to assign for communications regarding user identification information. The port number should be higher than 1024.

4. In the Domain Controller Address area, enter the IP address of a domain controller (such as an Active Directory server) that hosts user identification information, and click **Add**. Repeat to add any additional domain controllers.

5. Select the **Allow Distribution Groups** check box to allow distribution groups to be part of the information sent to the firewall.

6. Select the **Disable NetBIOS Probing** check box if you want to disable WMI/NetBIOS probing for each workstation. When this check box is selected, the User-ID Agent relies only on security logs and session information. If you do not disable probing, select whether to use NetBIOS (default) or WMI.
7. Select the **Enable Group Cache** check box to enable the user-group membership cache. When this check box is selected, the user-group membership is cached; when the User-ID Agent is restarted, it first reloads the user-group membership from the cache to speed up the restart process.

8. Configure timer values as needed:
   - **Age-out Timeout**—Timeout value for user entries. If there are no successful polls, security logs, or other information during this interval to indicate that the user is still at this IP address, the IP-to-user mapping is removed. If this field is left blank, the default timeout value 45 minutes is used. If NetBIOS Probing is disabled, entries do not time out.
   - **User Membership Timer**—Frequency at which the user-group membership is updated. Default is 60 minutes.
   - **Security Log Timer**—Frequency at which the security log is read. Default is 1 second.
   - **NetBIOS Probing Timer**—Frequency at which the NetBIOS polling is done (each client is polled). Default is 20 minutes.
   - **Server Session Timer**—Frequency at which the server session table is read from the Domain Controller.

9. In the Allow List area, enter the IP address and network mask of a subnet that you want to scan for users and click **Add**. Use the format `ip_address/mask` (for example, `10.1.1.1/24`) in the **IP Address** and **Subnet Mask** field. Repeat to add additional subnets. You must specify at least one network.

10. In the Ignore List area, enter the IP address and network mask of any subnet that you want to explicitly exclude from scans, and click **Add**. Use the format `ip_address/mask` (for example, `10.1.1.1/24`) in the **IP Address** and **Subnet Mask** field. Repeat to exclude additional subnets.

11. Click **Save** to save the configuration.

   The User-ID Agent is restarted if the configuration is saved successfully. You can also click the **OK** button to save the configuration and restart the User-ID Agent. If you do not want to restart the User-ID Agent, click **Cancel** to close the dialog box.

   **Note:** During normal operation, the left side of the Palo Alto Networks User-ID Agent window displays information about users and groups. To display the detailed log information, choose **File > Show Logs**.

---

**Uninstalling and Upgrading the User-ID Agent**

To uninstall the User-ID Agent, open the Control Panel on the PC, select **Add or Remove Programs**, and remove the program **User Identification Agent**.
About User Identification Agents

If you install a new version of the agent and the installer detects an existing installation on your PC, the installer automatically removes the older version before performing the installation.

About the User-ID Agent for eDirectory or API

The User-ID Agent for eDirectory or API can identify users from eDirectory or through an API.

Follow the instructions in this section to install and configure the User-ID Agent. Before you begin, make sure that you have configured the firewall for user identification. Refer to “Configuring the Firewall for User Identification” on page 35.

To install the User-ID Agent, open the installer file and follow the on-screen instructions.

Configuring the User-ID Agent

To open the controller for the User-ID Agent, choose Start > All Programs > Palo Alto Networks > User-ID Agent.

![User-ID Agent - Main Panel]

Figure 12. User-ID Agent - Main Panel

The window contains a side menu for access to the Configuration and Monitor panels. The main panel contains the following areas:

- **Device Connection List**—Shows all firewalls that are connected to the User-Identification Agent. The Device IP column shows the firewall IP address and port, and the Connection Status column displays the current connection status: “Connected,” “Disconnected,” or “Connecting.” Disconnected items are removed from the Connection List box when you close and then reopen the controller.
• **User-ID Server Connection List**—Shows connection status for all configured User-ID servers. If a connection cannot be established successfully, the status is shown as “Connecting,” with a reason such as “Server Down” or “Credential invalid.”

To configure the User-ID Agent:

1. Choose **Start > All Programs > Palo Alto Networks > User Identification Agent.**

2. Click **Configure** to display the main configuration panel.

![User-ID Agent - Configuration Panel](image)

3. In the **Device Listening Port** field, enter the port on which the PC will listen for messages from the firewall (default 5007).

4. Select the **Entry Timeout** check box if you want to specify a timeout for User-ID Agent connections. Enter a timeout value after which all entries to the specified type of server are considered to be logged off and are removed (1 - 360000 seconds, default is disabled). If any connection comes up before the timeout is reached, the timeout count stops. The timing starts after all connections to eDirectory LDAP servers go down.

5. Select the **Enable Network Address Allow/Ignore List** check box to configure a list of allowed or ignored IP addresses. If you use this option, only the addresses in the Allowed List and not in the Ignore List are identified and recorded by the User-ID Agent. To add an address, enter the address and click **Add.** To remove entries, select them and click **Delete.** The format is x.x.x.x or x.x.x.x/y (default is disabled).
6. Select the **Device Access Control** check box to limit user access to an allowed set of firewalls. If the Enable Device Access Control List check box is selected, then the agent accepts incoming connections only from the firewalls in the allow list. To add a firewall to the allow list, enter its IP address in the entry field, and click **Add**. To remove entries, select them and click **Remove**.

7. If any item has been configured, the Commit button is enabled. Click **Commit** to save the configuration. When you commit, you are prompted to restart the User-ID Agent service. If you click **Cancel** when prompted to restart, the existing configuration remains as the running configuration. The new configuration can be applied only after the User-ID agent service is restarted.

8. Click **Configure** in the side menu to display the submenu, and then select **eDirectory** to display the eDirectory configuration panel.

9. Use the **LDAP Server Selection** area to specify the list of servers for EDirectory LDAP. The agent queries the servers in this IP list to collect the user-to-IP address mapping data. Enter an IP address and click **Add** to add it to the list. To remove entries, select them and click **Remove**.

10. If several servers have the same settings, you can select a server and click **Copy Settings** to copy settings from an already-configured server to the selected server. A dialog box opens to show a list of servers. Select the server from which you want to copy the settings, and click **OK**.
11. In the Basic Settings area, configure the following settings. (If the server list is empty or no server is selected, the Basic Settings and Advanced Settings areas are disabled.)
   - **Search Base**—Specify the starting point or root context for agent queries. Example: `dc=domain1, dc=example, dc=com`
   - **Bind Distinguished Name**—Specify the account to bind to the LDAP server. Example: `cn=admin, ou=IT, dc=domain1, dc=example, dc=com`
   - **Bind Password**—Specify the bind account password. The agent saves the encrypted password in the configuration file.
   - **Confirm Bind Password**—Reenter the bind account password to confirm.
   - **Server Domain Prefix**—Specify a prefix to uniquely identify the user. Use if there are overlapping name spaces. Example: Different users with the same name from two different directories
   - **Search Interval**—Specify the time interval between consecutive queries from the User-ID Agent (range 1-36000 secs, default 30 secs).

12. For most installations, the settings in the Advanced Settings area do not require modification. If modification is required to address specific conventions for your installation, configure the settings as follows (defaults are provided only for EDirectory; for Other, you must supply your own entries):
   - **Search Filter**—Specify the search query for LDAP entries (default is `objectClass=Person`).
   - **Login Address Attribute Names**—Specify the name of the attribute to store the login IP address (default is `networkAddress`).
   - **Login Time Attribute Name**—Specify the attribute to store the login time (default is `loginTime`).
   - **Login ID Attribute Name**—Specify the name of the attribute to store the login unique ID (default is `uniqueID`).
   - **Bind Port**—Specify the binding port (default is 636). If you select **Other**, enter the port number and/or select SSL. If SSL is not selected, a pop-up window warns that clear text will be used for the login account and password.
   - **Verify Server Certificate**—Select the check box to verify the eDirectory server certificate when using SSL (default is disabled).
13. Click **Configure** in the side menu, if necessary, to display the submenu, and then select **User-ID API** to display the User-ID API configuration panel.

![User ID-Agent Configuration - API Settings](image)

**Figure 15. User ID-Agent Configuration - API Settings**

a. Select the **Enable User-ID API** check box to activate the User-ID API functionality.

b. You must configure the listening port to be different from the listening port on the Configure panel that is used to communicate with the firewall. The default listening port for User-ID API is 5006.

c. Select the **Server Allow List** check box to configure a list of allowed server IP addresses. If you use this option, the User-ID Agent accepts incoming connections only from the User-ID API Servers that are in the list (default is disabled). To add an address, enter the address and click **Add**. To remove entries, select them and click **Remove**.

d. Click **Commit** to save and activate the configuration.
Uninstalling and Upgrading the User-ID Agent

To uninstall the User-ID Agent, open the Control Panel on the PC, select Add or Remove Programs, and remove the program User-ID Agent.

If you install a new version of the agent and the installer detects an existing installation on your PC, the installer automatically removes the older version before performing the installation.

Monitoring the User-ID Agent Status

The monitor panel shows all captured User-ID Agent data, including the login name, IP address, and name mapping.

To monitor the agent status:
1. Choose Start > All Programs > Palo Alto Networks > User Identification Agent.
2. Click Monitor to display the monitor panel.

3. To search for a specific firewall, select Search IP and enter an IP address, or select Search Name and enter a user login name.

   The panel displays the requested login information. When you click in the first column for an entry, the details are presented below the login information list.

   Note: The status bar at the bottom of the agent window shows the status of the User-ID Agent. If there are no errors, the status bar displays “Ready” or “Connected,” indicating that the controller has successfully connected to the agent service. If the connection is not successful, an error message is presented.
About the Terminal Services Agent

The firewall provides a Terminal Server Agent (TS agent) that runs on a terminal server and identifies individual users that the terminal server supports. This arrangement allows the firewall to support multiple users with the same source IP address. The TS agent monitors the remote user sessions and reserves a different TCP/UDP source port range for each user session. After a port range is allocated for the user session, the TS agent provides information to map the source port range to the user name.

In addition, the TS agent requests that the TCP/UDP transport driver in the terminal server allocate the TS-agent-specified source port instead of the operating system-determined ephemeral port for outbound TCP/UDP traffic. When the firewall receives the TCP/UDP traffic from the terminal server, it checks the source port and obtains the user ID in the ports-to-user map data for the terminal server.

Configuring the Terminal Server Agent

To configure the TS agent on the firewall, click Add in the Terminal Server Agent area of the User Identification page and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the TS agent.</td>
</tr>
<tr>
<td>Virtual system</td>
<td>Select the virtual system from the drop-down list (if supported on the firewall model).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the Windows PC on which the TS agent will be installed. You can also specify alternative IP addresses (see the last entry in this table).</td>
</tr>
<tr>
<td>Port</td>
<td>Enter a port number of your choice for communication between the firewall and the TS agent.</td>
</tr>
<tr>
<td>Alternative IP Addresses</td>
<td>Enter additional IP addresses, if the server has multiple IP addresses that can appear as the source IP address for the outgoing traffic.</td>
</tr>
</tbody>
</table>

Installing or Upgrading the Terminal Server Agent on the Terminal Server

You can install the TS agent on the following platforms:

- Microsoft Terminal Services 2003
- Citrix Metaframe Presentation Server 4.0
- Citrix Metaframe Presentation Server 4.5

To install the TS agent on the terminal server:

1. Download and open the installation file.
2. The installer first checks for platform compatibility. If the platform is not compatible, an error message is displayed.
3. The installer checks whether an existing TS agent exists on the system. If the installer detects that the TS agent already exists on the system (you are upgrading the TS agent), it first uninstalls the agent before running the installer.

- If you are installing a TS agent that has a newer driver than the existing installation, the installation wizard prompts you to reboot the system after upgrading in order to use the new driver.
- If you are installing a TS agent with the same driver version as the existing installation, you can perform the installation as prompted, and do not need to reboot the system afterwards.

4. Follow the installer instructions to specify an installation location and complete the installation.

   Note: If you specify a destination folder other than the default one, make sure that you use the same destination when you upgrade the TS agent in the future. If you do not, the existing configuration will be lost and the default configuration will be used.

5. Following installation, reboot the terminal server, if prompted to do so.

**Configuring the Terminal Server Agent on the Terminal Server**

To configure the TS agent on the terminal server:

1. Launch the TS agent application from the Start menu.

2. The configuration panel opens with Terminal Server Agent highlighted on the left side of the window.

![Figure 17. Terminal Server Agent Configuration - Main Panel](image)

The connection list box shows all the Palo Alto Networks devices that connect to the TS agent. The Device IP column shows the device IP and port; and the Connection Status column indicates whether the status is Connected, Disconnected, or Connecting. Disconnected items are removed from the Connection List box when you close and then reopen the TS agent configuration window.
3. Select the **Enable Device Access Control List** check box if you want to explicitly list the firewalls that the TS agent will accept. Add each device IP address and click **Add**. Click **Remove** to delete an address from the list. Click **Save** to save the allow list.

4. Click **Configure** to display the configuration settings.

![Figure 18. Terminal Server Agent Configuration - Configure Panel](image)

5. Configure settings as described in the following table, and then click **Save**.

   **Note:** If you enter an incorrect parameter and then attempt to save the configuration, a message is displayed to indicate that the configuration will not be saved unless you modify the parameter correctly.

### Table 8. Terminal Server Agent Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Source Port</td>
<td>Displays the port range for system processes that are not associated with individual users. When a server process opens a socket to send a UDP packet or set up a TCP connection, it must obtain a source port from the server operating system. The server automatically allocates a source port (an ephemeral port) for this process. Format is low-high (default 1025-5000). The system port range must not overlap with the Source Port Allocation Range. If they overlap, an application using the system ephemeral source port range could mistakenly be identified as a particular user if the operation system allocated source port falls within the port range allocated for that user. <strong>Note:</strong> Modifying this value requires a Registry change and cannot be done from this panel.</td>
</tr>
</tbody>
</table>
### About User Identification Agents

- **System Reserved Source Ports**
  - Displays the port or ports to be excluded from the operating system source port allocation (because other server processes may use them).
  - You can enter a range: low-high (no default).
  - **Note:** Modifying this value requires a Registry change and cannot be done from this panel.

- **Listening Port**
  - Enter the port on which the terminal server will listen for communications from Palo Alto Networks firewalls (default 5009).

- **Source Port Allocation Range**
  - Enter a port allocation range for user sessions.
  - This setting controls the source port allocation for processes belonging to remote users (default 20000-39999). If a port allocation request comes from system services that cannot be identified as a particular user process, the TS agent lets the system allocate the source port from the system port range, excluding system reserved source ports.
  - **Note:** Make sure that this port range does not overlap with the System Source Port Allocation Range. If they overlap, an application using the system ephemeral source port range could mistakenly be identified as a particular user if the operation system allocated source port falls within the port range allocated for that user.

- **Reserved Source Ports**
  - Enter the reserved port allocation range for user sessions. These ports are unavailable for user sessions.
  - To include multiple ranges, use commas with no spaces, as in this example: 2000-3000,3500,4000-5000.
  - Format is low-high (no default).

- **Port Allocation Start Size Per User**
  - Enter the number of ports that the TS agent will first allocate when the remote user logs in (default 200).
  - When the remote user logs on, the TS agent allocates a port range from the Source Port Allocation Range with this specified size. This allows identification of user traffic based on the source port.

- **Port Allocation Maximum Size Per User**
  - Enter the maximum number of ports that the TS agent can allocate for a remote user session (default 200).
  - If the **Port Allocation Start Size Per User** setting is not sufficient for the user session, the TS agent will allocate additional ports up to this maximum.

- **Fail port binding when available ports are used up**
  - Select the check box as appropriate:
    - If the check box is selected (default), the port request from this user’s application fails if the user application has used all available ports. As a result, the application may fail to send traffic.
    - If the check box is not selected, the port request from this user’s application is granted from the System Source Port Allocation Range even if the user application has used all the available ports. The application can send traffic; however, the user ID of the traffic is unknown.

### Table 8. Terminal Server Agent Configuration Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Reserved Source Ports</td>
<td>Displays the port or ports to be excluded from the operating system source port allocation (because other server processes may use them).</td>
</tr>
<tr>
<td></td>
<td>You can enter a range: low-high (no default).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Modifying this value requires a Registry change and cannot be done from this panel.</td>
</tr>
<tr>
<td>Listening Port</td>
<td>Enter the port on which the terminal server will listen for communications from Palo Alto Networks firewalls (default 5009).</td>
</tr>
<tr>
<td>Source Port Allocation Range</td>
<td>Enter a port allocation range for user sessions.</td>
</tr>
<tr>
<td></td>
<td>This setting controls the source port allocation for processes belonging to remote users (default 20000-39999). If a port allocation request comes</td>
</tr>
<tr>
<td></td>
<td>from system services that cannot be identified as a particular user process, the TS agent lets the system allocate the source port from the</td>
</tr>
<tr>
<td></td>
<td>system port range, excluding system reserved source ports.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Make sure that this port range does not overlap with the System Source Port Allocation Range. If they overlap, an application using</td>
</tr>
<tr>
<td></td>
<td>the system ephemeral source port range could mistakenly be identified as a particular user if the operation system allocated source port falls</td>
</tr>
<tr>
<td></td>
<td>within the port range allocated for that user.</td>
</tr>
<tr>
<td>Reserved Source Ports</td>
<td>Enter the reserved port allocation range for user sessions. These ports are unavailable for user sessions.</td>
</tr>
<tr>
<td></td>
<td>To include multiple ranges, use commas with no spaces, as in this example: 2000-3000,3500,4000-5000.</td>
</tr>
<tr>
<td></td>
<td>Format is low-high (no default).</td>
</tr>
<tr>
<td>Port Allocation Start Size Per User</td>
<td>Enter the number of ports that the TS agent will first allocate when the remote user logs in (default 200).</td>
</tr>
<tr>
<td></td>
<td>When the remote user logs on, the TS agent allocates a port range from the Source Port Allocation Range with this specified size. This allows</td>
</tr>
<tr>
<td></td>
<td>identification of user traffic based on the source port.</td>
</tr>
<tr>
<td>Port Allocation Maximum Size Per User</td>
<td>Enter the maximum number of ports that the TS agent can allocate for a remote user session (default 200).</td>
</tr>
<tr>
<td></td>
<td>If the <strong>Port Allocation Start Size Per User</strong> setting is not sufficient for the user session, the TS agent will allocate additional ports up to this maximum.</td>
</tr>
<tr>
<td>Fail port binding when available ports are used up</td>
<td>Select the check box as appropriate:</td>
</tr>
<tr>
<td></td>
<td>- If the check box is selected (default), the port request from this user’s application fails if the user application has used all available ports. As a result, the application may fail to send traffic.</td>
</tr>
<tr>
<td></td>
<td>- If the check box is not selected, the port request from this user’s application is granted from the System Source Port Allocation Range even if the user application has used all the available ports. The application can send traffic; however, the user ID of the traffic is unknown.</td>
</tr>
</tbody>
</table>
6. Click **Monitor** to display the port allocation information for all terminal server users.

![Terminal Server Agent Configuration - Monitor Panel](image)

**Figure 19. Terminal Server Agent Configuration - Monitor Panel**

7. View the displayed information. For a description of the type of information displayed, refer to the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Displays the user name.</td>
</tr>
<tr>
<td>Ports Range</td>
<td>Displays the current allocated source ports for this user. Multiple ranges are separated by commas (for example, “20400-20799, 20500-20599”). The size of the port ranges is limited by the “Port Allocation Start Size Per User” and “Port Allocation Maximum Size Per User” configuration parameters, as described in Table 8.</td>
</tr>
<tr>
<td>Ports Count</td>
<td>Indicates the number of ports in use.</td>
</tr>
</tbody>
</table>

8. Click the **Refresh Ports Count** button to update the **Ports Count** field manually, or select the **Refresh Interval** check box and configure a refresh interval to update this field automatically.

The following table lists the menu options available in the TS agent application window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure</td>
<td>Open the Configuration panel.</td>
</tr>
<tr>
<td>Monitor</td>
<td>Open the Monitor panel.</td>
</tr>
<tr>
<td>Restart Service</td>
<td>Restart the TS agent service. This option is not normally required and is reserved for troubleshooting.</td>
</tr>
<tr>
<td>Show Logs</td>
<td>Display the troubleshooting log.</td>
</tr>
</tbody>
</table>
Uninstalling the Terminal Server Agent on the Terminal Server

To uninstall the TS agent, use the Add/Remove Programs control panel on the server. Remove the “Terminal Server Agent” application. You must reboot the system to complete the uninstallation.

About Administrator Roles, Profiles, and Accounts

The firewall supports the following options to authenticate administrative users who attempt to log in to the firewall:

- **Local database**—The user login and password information is entered directly into the firewall database.

- **RADIUS**—Existing RADIUS servers are used to authenticate users.

- **LDAP**—Existing LDAP servers are used to authenticate users.

When you create an administrative account, you specify either local authentication (no authentication profile) or an authentication profile (RADIUS, LDAP, or local DB authentication). This setting indicates how the user password is checked.

Administrator roles determine the functions that the administrator is permitted to perform after logging in. You can assign roles directly to an administrator account, or define role profiles, which specify detailed privileges, and assign those to administrator accounts.

Refer to the following sections for additional information:

- For instructions on setting up authentication profiles, refer to “Setting Up Authentication Profiles” on page 55.

- For instructions on setting up role profiles, refer to “Defining Administrator Roles” on page 54.

- For instructions on setting up administrator accounts, refer to “Creating Administrative Accounts” on page 57.

- For information on SSL VPNs, refer to “Configuring SSL VPNs” on page 205.

- For instructions on defining virtual system domains for administrators, refer to “Specifying Access Domains for Administrators” on page 58.

### Table 10. Terminal Server Agent Menu Options (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug</td>
<td>Select debugging options (None, Error, Information, Debug, or Verbose).</td>
</tr>
<tr>
<td>Exit</td>
<td>Quit the TS agent application.</td>
</tr>
<tr>
<td>Help</td>
<td>Display TS agent version information.</td>
</tr>
</tbody>
</table>
About Authentication Profiles

Defining Administrator Roles

► Device > Admin Roles

Use the Admin Roles page to define role profiles that determine the access and responsibilities available for administrative users. To add a new administrator role, click New and specify the following information. For instructions on defining administrator accounts, refer to “Creating Administrative Accounts” on page 57.

Table 11. Administrator Role Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Enter a name to identify this administrator role.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description of the role.</td>
</tr>
<tr>
<td>Admin Role</td>
<td>Select the general scope of administrative responsibility from the drop-down list.</td>
</tr>
<tr>
<td>CLI Role</td>
<td>Select the type of role for CLI access:</td>
</tr>
<tr>
<td></td>
<td>• disable—Access to the device CLI not permitted.</td>
</tr>
<tr>
<td></td>
<td>• superuser—Full access to the current device.</td>
</tr>
<tr>
<td></td>
<td>• superreader—Read-only access to the current device.</td>
</tr>
<tr>
<td></td>
<td>• deviceadmin—Full access to a selected device, except for defining new accounts or virtual systems.</td>
</tr>
<tr>
<td></td>
<td>• devicereader—Read-only access to a selected device.</td>
</tr>
</tbody>
</table>

WebUI Role

Click the icons for specified areas to indicate the type of access permitted in the web interface:

• 📐 Read/write access to the indicated page.
• 🔖 Read only access to the indicated page.
• 🔴 No access to the indicated page.

About Authentication Profiles

Authentication profiles specify local database, RADIUS, or LDAP settings and can be assigned to administrator accounts, SSL VPN access, and captive portal. When an administrator attempts to log in to the firewall directly or through an SSL VPN or captive portal, the firewall checks the authentication profile that is assigned to the account and authenticates the user based on the authentication settings.

If the user does not have a local administrator account, the authentication profile that is specified on the device Setup page determines how the user is authenticated (refer to “Defining the Host Name and Network Settings” on page 66):

• If you specify RADIUS authentication settings on the Setup page and the user does not have a local account on the firewall, then the firewall requests authentication information for the user (including role) from the RADIUS server. The RADIUS directory file containing the attributes for the various roles is available at http://support.paloaltonetworks.com.

• If None is specified as the authentication profile on the Settings page, then the user must be authenticated locally by the firewall according to the authentication profile that is specified for the user.
Setting Up Authentication Profiles

Device > Authentication Profile

Use the Authentication Profile page to configure authentication profiles. To add a new authentication profile, click New and configure the following settings. To change an entry, click the link for the entry.

Table 12. Authentication Profile Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Enter a name to identify the profile.</td>
</tr>
<tr>
<td>Virtual System</td>
<td>Select the virtual system from the drop-down list.</td>
</tr>
<tr>
<td>Failed Attempts</td>
<td>Enter the number of failed login attempts that are allowed before the account is locked out (1-10, default 0). 0 means that there is no limit.</td>
</tr>
<tr>
<td>Lockout Time</td>
<td>Enter the number of minutes that a user is locked out if the number of failed attempts is reached (0-60 minutes, default 0). 0 means that the lockout is in effect until it is manually unlocked.</td>
</tr>
<tr>
<td>Allow List</td>
<td>Specify the users and groups that are explicitly allowed to authenticate. Click Edit Allow List and do any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Select the check box next to the appropriate user or user group in the Available column, and click Add to add your selections to the Selected column.</td>
</tr>
<tr>
<td></td>
<td>• Enter the first few characters of a name in the Search field to list all the users and user groups that start with those characters. Selecting an item in the list sets the check box in the Available column. Repeat this process as often as needed, and then click Add.</td>
</tr>
<tr>
<td></td>
<td>• To remove users or user groups, select the appropriate check boxes in the Selected column and click Remove, or select any to clear all users.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Choose the type of authentication:</td>
</tr>
<tr>
<td></td>
<td>• Local DB—Use the authentication database on the firewall.</td>
</tr>
<tr>
<td></td>
<td>• RADIUS—Use a Remote Authentication Dial In User Service (RADIUS) server for authentication.</td>
</tr>
<tr>
<td></td>
<td>• LDAP—Use LDAP as the authentication method.</td>
</tr>
<tr>
<td>Server</td>
<td>If you select RADIUS or LDAP as the authentication method, choose the authentication server from the drop-down list. Servers are configured on the Server pages. Refer to “Configuring RADIUS Server Settings” on page 56 and “Configuring LDAP Server Settings” on page 56.</td>
</tr>
<tr>
<td>Login Attribute</td>
<td>If you selected LDAP as the authentication method, enter the LDAP directory attribute that uniquely identifies the user.</td>
</tr>
</tbody>
</table>
Configuring RADIUS Server Settings

▶ Device > Server > RADIUS

Use the RADIUS page to configure settings for the RADIUS servers that are identified in the authentication profiles. To add a new server, click New and configure the following settings. To change an entry, click the link for the entry.

Table 13. RADIUS Server Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the server.</td>
</tr>
<tr>
<td>Shared</td>
<td>Select this check box to apply the server settings across all of the virtual systems.</td>
</tr>
<tr>
<td>Virtual System</td>
<td>If you do not choose the Shared option, select a specific virtual system.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the RADIUS server domain. The domain setting is used if the user does not specify a domain when logging in.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Enter an interval after which an authentication request times out (1-30 seconds, default 3 seconds).</td>
</tr>
<tr>
<td>Retries</td>
<td>Enter the number of automatic retries following a timeout before the request fails (1-5, default 3).</td>
</tr>
<tr>
<td>Retrieve User Group</td>
<td>Select the check box to use RADIUS vendor specific attribute (VSA) to define the group that has access to the firewall.</td>
</tr>
<tr>
<td>Servers</td>
<td>Configure information for each server in the preferred order.</td>
</tr>
<tr>
<td></td>
<td>• Name—Enter a name to identify the server.</td>
</tr>
<tr>
<td></td>
<td>• IP address—Enter the server IP address.</td>
</tr>
<tr>
<td></td>
<td>• Port—Enter the server port for authentication requests.</td>
</tr>
<tr>
<td></td>
<td>• Secret/Confirm Secret—Enter and confirm a key to verify and encrypt the connection between the firewall and the RADIUS server.</td>
</tr>
</tbody>
</table>

Configuring LDAP Server Settings

▶ Device > Server > LDAP

Use the LDAP page to configure settings for the LDAP servers to use for authentication by way of authentication profiles. To add a new server, click New and configure the following settings. To change an entry, click the link for the entry.

Table 14. LDAP Server Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the profile.</td>
</tr>
<tr>
<td>Shared</td>
<td>Select this check box to apply the server settings across all of the virtual systems.</td>
</tr>
<tr>
<td>Virtual System</td>
<td>If you do not choose the Shared option, select a specific virtual system.</td>
</tr>
<tr>
<td>Base</td>
<td>Specify the root context in the directory server to narrow the search for user or group information.</td>
</tr>
</tbody>
</table>
Creating Administrative Accounts

Device > Administrators

Administrator accounts control access to the firewall. Each administrator can have full or read-only access to a single device or to a virtual system on a single device. The predefined admin account has full access. To ensure that the device management interface remains secure, it is recommended that administrative passwords be changed periodically using a mixture of lower-case letters, upper-case letters, and numbers.

To add a new administrator account, click New and specify the following information.

Table 14. LDAP Server Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind DN</td>
<td>Specify the login name (Distinguished Name) for the directory server.</td>
</tr>
<tr>
<td>Bind Password/Confirm Bind Password</td>
<td>Specify the bind account password. The agent saves the encrypted password in the configuration file.</td>
</tr>
<tr>
<td>SSL</td>
<td>Select to use secure SSL or Transport Layer Security (TLS) communications between the Palo Alto Networks device and the directory server.</td>
</tr>
<tr>
<td>Time Limit</td>
<td>Specify the time limit imposed when performing directory searches (0 - 60 seconds, default 30 seconds).</td>
</tr>
<tr>
<td>Bind Time Limit</td>
<td>Specify the time limit imposed when connecting to the directory server (0 - 60 seconds, default 30 seconds).</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>Specify the interval after which the system will try to connect to the LDAP server after a previous failed attempt (1-3600 seconds).</td>
</tr>
<tr>
<td>Servers</td>
<td>Specify the host names, IP addresses, and ports of up to three LDAP servers.</td>
</tr>
</tbody>
</table>

Table 15. Administrator Account Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a login name for the user (up to 15 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.</td>
</tr>
<tr>
<td>Authentication Profile</td>
<td>Select an authentication profile for administrator authentication according to the settings in the specified authentication profile. This setting can be used for RADIUS, LDAP, or Local DB authentication. For instructions on setting up authentication profiles, refer to “Setting Up Authentication Profiles” on page 55.</td>
</tr>
<tr>
<td>New Password Confirm New Password</td>
<td>Enter and confirm a case-sensitive password for the user (up to 15 characters).</td>
</tr>
</tbody>
</table>
About Authentication Profiles

Specifying Access Domains for Administrators

Device > Access Domain

Use the Access Domain page to define virtual system domains for administrators. Click New and specify the following information.

Table 16. Access Domain Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the access domain (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.</td>
</tr>
<tr>
<td>Virtual Systems</td>
<td>Select virtual systems in the Available column and click Add to select them.</td>
</tr>
</tbody>
</table>

Note: On the Panorama Administrator’s page for “super user,” a lock icon is shown in the right column if an account is locked out. The administrator can click the icon to unlock the account.
Defining Client Certificate Profiles

You can create client certificate profiles and then attach a profile to an administrator login on the Setup page or to an SSL VPN login for authentication purposes. Refer to “Defining the Host Name and Network Settings” on page 66.

Table 17. Client Certificate Profile Settings

<table>
<thead>
<tr>
<th>Page Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Enter a name to identify the profile.</td>
</tr>
<tr>
<td>Shared</td>
<td>Select this check box to apply the settings across all of the virtual systems.</td>
</tr>
<tr>
<td>Virtual System</td>
<td>If you do not choose the shared option, select a specific virtual system.</td>
</tr>
<tr>
<td>Username Field</td>
<td>Choose a user name option from the drop-down list.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain for the profile.</td>
</tr>
<tr>
<td>CA Certificates</td>
<td>Choose a CA certificate from the drop-down list, specify the default Online Certificate Status Protocol (OCSP) URL, select an option to verify the CA certificate, and click Add. Repeat to add additional certificates.</td>
</tr>
<tr>
<td>Use CRL</td>
<td>Select the check box to use a certificate revocation list (CRL).</td>
</tr>
<tr>
<td>Use OCSP</td>
<td>Select the check box to use OCSP.</td>
</tr>
<tr>
<td>CRL Receive Timeout</td>
<td>Specify an interval after which CRL requests time out (1 - 60 secs).</td>
</tr>
<tr>
<td>OCSP Receive Timeout</td>
<td>Specify an interval after which OCSP requests time out (1 - 60 secs).</td>
</tr>
<tr>
<td>Certificate Status Timeout</td>
<td>Specify an interval after which requests for certificate status time out (1 - 60 secs).</td>
</tr>
<tr>
<td>Block Unknown Certificate</td>
<td>Select the check box to block a session if the certificate status is unknown.</td>
</tr>
<tr>
<td>Block Timeout Certificate</td>
<td>Select the check box to block a session if the certificate status cannot be retrieved within the timeout interval.</td>
</tr>
</tbody>
</table>
About the Firewall Logs

The firewall provides logs that record configuration changes, system events, security threats, and traffic flows. Except for the traffic log, the firewall saves all logs locally by default. For each log, you can enable remote logging to a Panorama server, and generate SNMP traps, syslog messages, and email notifications.

The following table describes the logs and logging options.

<table>
<thead>
<tr>
<th>Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>The configuration log records each configuration change, including the date and time, the administrator user name, and whether the change succeeded or failed. All configuration log entries can be sent to Panorama, syslog, and email servers, but they cannot generate SNMP traps.</td>
</tr>
<tr>
<td>System</td>
<td>The system log records each system event, such as high availability failures, link status changes, and administrators logging in and out. Each entry includes the date and time, the event severity, and an event description. System log entries can be logged remotely by severity level. For example, you can generate SNMP traps and email notifications for just critical and high-level events.</td>
</tr>
<tr>
<td>Threat</td>
<td>The threat log records each security alarm generated by the firewall. Each entry includes the date and time, the threat type, such as a virus or spyware/vulnerability filtering violation, the source and destination zones, addresses, and ports, the application name, and the action and severity. Threat log entries can be logged remotely by severity level by defining log forwarding profiles, and then assigning the profiles to security rules (refer to “About Security Policies” on page 122). Threats are logged remotely only for the traffic that matches the security rules where the logging profile is assigned. Threat logs are used in generating reports and in the Application Command Center (refer to “Reports and Logs” on page 161).</td>
</tr>
<tr>
<td>Traffic</td>
<td>The traffic log can record an entry for the start and end of each session. Each entry includes the date and time, the source and destination zones, addresses, and ports, the application name, the security rule applied to the session, the rule action (allow, deny, or drop), the ingress and egress interface, and the number of bytes. Each security rule specifies whether the start and/or end of each session is logged locally for traffic that matches the rule. The log forwarding profile assigned to the rule determines whether the locally logged entries are also logged remotely. Traffic logs are used in generating reports and in the Application Command Center (refer to “Reports and Logs” on page 161).</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>The URL filtering log records entries for URL filters, which block access to specific web sites and web site categories or generate an alert when a user accesses a proscribed web site (refer to “About URL Filtering Profiles” on page 137).</td>
</tr>
<tr>
<td>Data Filtering</td>
<td>The data filtering log records information on the security policies that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall (refer to “Defining Data Filtering Profiles” on page 139).</td>
</tr>
</tbody>
</table>
About Log Destinations

You can configure the firewall to send log entries to a Panorama centralized management system, SNMP trap sinks, syslog servers, and email addresses.

The following table describes the remote log destinations.

<table>
<thead>
<tr>
<th>Table 19  Remote Log Destinations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>Panorama</td>
</tr>
<tr>
<td>SNMP trap</td>
</tr>
<tr>
<td>Syslog</td>
</tr>
<tr>
<td>Email</td>
</tr>
</tbody>
</table>

Defining Configuration Log Settings

► Device > Log Settings > Config

The configuration log settings specify the configuration log entries that are logged remotely with Panorama, and sent as syslog messages and/or email notifications.

To define the configuration log settings, click Edit and specify the following information.

<table>
<thead>
<tr>
<th>Table 20. Configuration Log Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Panorama</td>
</tr>
<tr>
<td>Email</td>
</tr>
<tr>
<td>Syslog</td>
</tr>
</tbody>
</table>
Defining System Log Settings

Device > Log Settings > System

The system log settings specify the severity levels of the system log entries that are logged remotely with Panorama, and sent as SNMP traps, syslog messages, and/or email notifications. The system logs show system events, such as high availability failures, link status changes, and administrators logging in and out.

To define the system log settings, click **Edit and** specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Panorama       | Select the check box for each severity level of the system log entries to be sent to the Panorama centralized management system. To specify the Panorama server address, refer to “Defining the Host Name and Network Settings” on page 66. The severity levels are:  
  • **Critical**—Hardware failures, including high availability failover, and link failures.  
  • **High**—Serious issues, including dropped connections with external devices, such as syslog and RADIUS servers.  
  • **Medium**—Mid-level issues, such as user authentication failures.  
  • **Low**—Minor issues, such as user authentication failures.  
  • **Informational**—Login/logoff, administrator name or password change, any configuration change, and all other events not covered by the other severity levels. |
| SNMP Trap      | Under each severity level, select the SNMP, syslog, and/or email settings that specify additional destinations where the system log entries are sent. To define new destinations, refer to:  
  • “Defining SNMP Trap Destinations” on page 63.  
  • “Defining Syslog Servers” on page 64  
  • “Defining Email Notification Settings” on page 64 |
| Email          |                                                                                               |
| Syslog         |                                                                                               |
Defining SNMP Trap Destinations

To generate SNMP traps for system, traffic, or threat log entries, you must specify one or more SNMP trap destinations. After you define the trap destinations, you can use them for system log entries (refer to “Defining System Log Settings” on page 62).

To define SNMP trap destinations, click **New** and specify the following information.

### SNMP MIBs

The firewall supports the following SNMP Management Information Bases (MIBs):

- SNMPv2-MIB
- DISMAN-EVENT-MIB
- IF-MIB
- HOST-RESOURCES-MIB
- ENTITY-SENSOR-MIB
- PAN-COMMON-MIB

The full set of MIBs is available on the Palo Alto Networks support site: [http://support.paloaltonetworks.com](http://support.paloaltonetworks.com).

### Table 22. SNMP Trap Destination Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the SNMP trap destination name (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.</td>
</tr>
<tr>
<td>Manager</td>
<td>Enter the IP address of the trap destination.</td>
</tr>
<tr>
<td>Community</td>
<td>Enter the community string required to send traps to the specified destination (default “public”).</td>
</tr>
</tbody>
</table>

*Note: Do not delete a destination that is used in any system log settings or logging profile.*
Defining Syslog Servers

Device > Log Destinations > Syslog

To generate syslog messages for system, configuration, traffic, or threat log entries, you must specify one or more syslog servers. After you define the syslog servers, you can use them for system and configuration log entries (refer to “Defining System Log Settings” on page 62). To define syslog servers, click New and specify the following information.

Table 23. New Syslog Server

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the syslog server (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the IP address of the syslog server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the syslog server (the standard port is 514).</td>
</tr>
<tr>
<td>Facility</td>
<td>Choose a level from the drop-down list.</td>
</tr>
</tbody>
</table>

Note: You cannot delete a server that is used in any system or configuration log settings or logging profiles.

Defining Email Notification Settings

Device > Log Destinations > Email

To generate email messages for system, configuration, traffic, or threat log entries, you must specify the email settings. After you define the email settings, you can enable email notification for system and configuration log entries (refer to “Defining System Log Settings” on page 62). For information on scheduling email report delivery, refer to “Scheduling Reports for Email Delivery” on page 182. To define email settings, click New and specify the following information.

Table 24. Email Notification Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the email settings (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Enter the name shown in the From field of the email.</td>
</tr>
<tr>
<td>From</td>
<td>Enter the From email address, such as “<a href="mailto:security_alert@company.com">security_alert@company.com</a>”.</td>
</tr>
<tr>
<td>To</td>
<td>Enter the email address of the recipient.</td>
</tr>
</tbody>
</table>
You can schedule exports of logs and save them to a File Transfer Protocol (FTP) server in CSV format. Log profiles contain the schedule and FTP server information. For example, a profile may specify that the previous day’s logs are collected each day at 3AM and stored on a particular FTP server.

To create a log export profile and schedule exports, click New or click the profile link and specify the following information. When you click OK, the new profile is added to the Scheduled Log Export page, and the specified export is scheduled. No commit is required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Enter a name to identify the profile. The name cannot be changed after the profile is created.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the check box to enable the scheduling of log exports.</td>
</tr>
<tr>
<td>Log Type</td>
<td>Select the type of log (traffic or threat). Default is traffic.</td>
</tr>
<tr>
<td>Scheduled export start time (daily)</td>
<td>Enter the time of day (hh:mm) to start the export, using a 24-hour clock (00:00 - 23:59). Default is 3:00 (3:00 AM).</td>
</tr>
<tr>
<td>FTP Hostname</td>
<td>Enter the host name or IP address of the FTP server that will be used for the export.</td>
</tr>
<tr>
<td>FTP Port</td>
<td>Enter the port number that the FTP server will use. Default is 21.</td>
</tr>
<tr>
<td>FTP Passive Mode</td>
<td>Select the check box to use passive mode for the export. By default, this option is selected.</td>
</tr>
<tr>
<td>FTP Username</td>
<td>Enter the user name for access to the FTP server. Default is anonymous.</td>
</tr>
<tr>
<td>FTP Password</td>
<td>Enter the password for access to the FTP server. A password is not required if the user is “anonymous.”</td>
</tr>
</tbody>
</table>

Note: You cannot delete an email setting that is used in any system or configuration log settings or logging profiles.
About System Setup, Configuration, and License Management

The following sections describe how to define the network settings and manage configurations for the firewall:

- “Defining the Host Name and Network Settings” in the next section
- “Comparing Configuration Files” on page 71
- “Managing Configurations” on page 72
- “Installing a License” on page 73
- “Support for Certificate Revocation List and Online Certificate Status Protocol” on page 79

Defining the Host Name and Network Settings

▶ Device > Setup

The Setup page allows you to specify the host name of the firewall, the network settings of the management interface, and the IP addresses of various network servers (Panorama, DNS, NTP, and RADIUS). You can also enable the use of virtual systems (if supported on the firewall model), save, load, import, and export configurations, set the date and time manually, and reboot the device.

If you do not want to use the management port, you can define a loopback interface and manage the firewall through the IP address of the loopback interface (refer to “Configuring Loopback Interfaces” on page 94).

Perform any of the following operations on this page:

- To change the host name or network settings, click Edit on the first table on the page, and specify the following information.

Table 26. Host Name and Network Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Settings</td>
<td></td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter a host name (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain name of the firewall (up to 31 characters).</td>
</tr>
<tr>
<td>Mgt Interface Speed</td>
<td>Configure a data rate and duplex option for the management interface. The choices include 10Mbps, 100Mbps, and 1Gbps at full or half duplex. Use the default auto-negotiate setting to have the firewall determine the interface speed. This setting should match the port settings on the neighboring network equipment.</td>
</tr>
</tbody>
</table>
### Table 26. Host Name and Network Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT Interface IP Address</td>
<td>Enter the IP address of the management port. Alternatively, you can use the IP address of a loopback interface for device management. This address is used as the source address for remote logging.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Enter the network mask for the IP address, such as “255.255.255.0”.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the IP address of the default router (must be on the same subnet as the management port).</td>
</tr>
<tr>
<td>MGT Interface IPv6 Address</td>
<td>(Optional) Enter the IPv6 address of the management port.</td>
</tr>
<tr>
<td>Default IPv6 Gateway</td>
<td>Enter the IPv6 address of the default router (must be on the same subnet as the management port), if you assigned an IPv6 address to the management port.</td>
</tr>
<tr>
<td>MGT Interface Services</td>
<td>Select the services enabled on the specified management interface address (HTTP, HTTPS, Telnet, SSH, and/or Ping).</td>
</tr>
<tr>
<td>Login Banner</td>
<td>Enter custom text that will be displayed on the firewall login page. The text is displayed below the Name and Password fields.</td>
</tr>
<tr>
<td>Authentication Profile</td>
<td>Select the authentication profile to use for administrator access to the firewall. For instructions on configuring authentication profiles, refer to “Setting Up Authentication Profiles” on page 55.</td>
</tr>
<tr>
<td>Client Certificate Profile</td>
<td>Select the client certificate profile to use for administrator access to the firewall. For instructions on configuring client certificate profiles, refer to “Defining Client Certificate Profiles” on page 59.</td>
</tr>
<tr>
<td>Primary DNS Server</td>
<td>Enter the IP address of the primary and secondary Domain Name Service (DNS) servers. The secondary server address is optional.</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
<td>Note: If you entered a DNS server in the Quick Start Setup page, you do not need to reenter it here.</td>
</tr>
<tr>
<td>Primary NTP Server</td>
<td>Enter the IP address or name of the primary and secondary Network Time Protocol (NTP) servers, if any.</td>
</tr>
<tr>
<td>Secondary NTP Server</td>
<td>If you do not use NTP servers, you can set the device time manually.</td>
</tr>
<tr>
<td>System Location</td>
<td>Enter a description of where the firewall is located.</td>
</tr>
<tr>
<td>System Contact</td>
<td>Enter the name or email address of the person responsible for maintaining the firewall.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Select the time zone of the firewall.</td>
</tr>
<tr>
<td>Update Server</td>
<td>The default name of the server used to download updates from Palo Alto Networks is “updates.paloaltonetworks.com.” Do not change the server name unless instructed by technical support.</td>
</tr>
<tr>
<td>Proxy Server: Server Port</td>
<td>If the device needs to use a proxy server to reach Palo Alto Networks update services, enter the IP address, port number, user name, and password for the proxy server.</td>
</tr>
<tr>
<td>User</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>
Table 26. Host Name and Network Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Panorama                  | Enter the IP address of Panorama, the Palo Alto Networks centralized management system (if any). The server address is required to manage the device through Panorama.  
To remove any policies that Panorama propagates to managed firewalls, click the **Disabled Shared Policies** link. To move the policies to your local name space before removing them from Panorama, click the **Import shared policies from Panorama before disabling** check box in the dialog box that opens. Click **OK**. |
| Permitted IP Addresses    | Enter the IPv4 or IPv6 addresses of any external servers that are used to provide updates to the firewall through the management ports.                                                                         |
| Geo Location              | Enter the latitude (-90.0 to 90.0) and longitude (-180.0 to 180.0) of the firewall.                                                                                                                                                  |
| SNMP Community String     | Enter an SNMP community string.                                                                                                                                                                                                             |
| Configuration Links       |                                                                                                                                                                                                                                       |
| Include a logo on custom reports | Click **Custom Logo**. Click **Browse** to locate the logo file, and then **OK** to upload the file to the firewall. To remove a previously uploaded logo, click **Remove** and then click **OK**. Refer to “Generating Custom Reports” on page 183. |
| Add additional protection for access to logs that may contain sensitive information, such as credit card numbers or social security number | Click **Manage Data Protection** and configure the following:  
• To set a new password if one has not already been set, click **Set data access password**. Enter and confirm the password.  
• To change the password, click **Change data access password**. Enter the old password, and enter and confirm the new password.  
• To delete the password and the data that has been protected, click **Delete data access password and protected data**. |
| Specify how the firewall will communicate with other servers | Click **Service Route Configuration** and configure the following:  
• To communicate with all external servers through the management interface, select **Use Management Interface for all**.  
• Choose **Select** to choose options based on the type of service. Select the source from the **Source Address** drop-down list. |
| Configure settings for certificate validation | Click **CRL/OCSP Settings** and follow the instructions in “Support for Certificate Revocation List and Online Certificate Status Protocol” on page 79. |
| Access quick start screens for the firewall | Click **Quick Start**. Refer to “Setting Up the Firewall” on page 17. |
| Multi-Virtual Systems     | Click **Edit** for Multi Virtual System Capability near the top of the **Setup** page. Select the check box, and click **OK**. For more information about virtual systems, refer to “About Virtual Systems” on page 24. |
### Reboot/Restart

Restart the firewall

Click **Reboot Device**. You are logged out and the PAN-OS software and active configuration are reloaded. Any configuration changes that have not been saved or committed are lost (refer to “Managing Configurations” on page 72).

Restart the data functions of the firewall without rebooting

Click **Restart Dataplane**.

### Date and Time

Set the date and time

Click **Set Time**. Enter the current date in (YYYY/MM/DD) or click the calendar icon to select a month and day. Enter the current time in 24-hour format (HH:MM:SS).

### Settings

**IPv6 Firewalling**

Click **Edit** and select the IPv6 Firewalling check box.
IPv6 objects apply only to virtual wire policies. All IPv6-based configurations are ignored if IPv6 is not enabled.

**Rematch Sessions**

Click **Edit** and select the check box **Rematch all sessions on config policy change**.
For example, assume that Telnet was previously allowed and then changed to **Deny** in the last commit. The default behavior is for any Telnet sessions started before the commit to continue to be allowed. However, if Rematch Sessions is configured, those Telnet sessions are terminated.

**Jumbo Frame**

Select the check box and specify the Maximum Transmission Unit (MTU), excluding the Ethernet header (range 512-9192).

**Dynamic URL cache Timeout**

Click **Edit** and enter the timeout (in hours). This value is used in dynamic URL filtering to determine the length of time an entry remains in the cache after it is returned from the BrightCloud service. For information on URL filtering, refer to “About URL Filtering Profiles” on page 137.

**URL Continue Timeout**

Specify the interval following a user’s “continue” action before the user must press continue again for URLs in the same category (1 - 86400 minutes).

**URL Admin Override Timeout**

Specify the interval after the user enters the admin override password before the user must re-enter the admin override password for URLs in the same category (1 - 86400 minutes).

**URL Admin Lockout Timeout**

Specify the period of time that a user is locked out from attempting to use the URL Admin Override password following three unsuccessful attempts (1 - 86400 minutes).

### Management

**Idle Timeout**

Enter the timeout interval (1 - 1440 minutes). A value of 0 means that the management, web, or CLI session does not time out.

**Max. Rows in CSV Export**

Enter the maximum number of rows that is supported for CSV file exports (1-1048576, default 65535).

**Receive Timeout for connection to Panorama**

Enter the timeout for receiving TCP messages from Panorama (1-120 seconds, default 20).
### About System Setup, Configuration, and License Management

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Timeout for connection to Panorama</td>
<td>Enter the timeout for sending TCP communications to Panorama (1-120 seconds, default 20).</td>
</tr>
<tr>
<td>Retry Count for SSL send to Panorama</td>
<td>Enter the number of retries (1-64, default 25) for attempts to send SSL messages to Panorama.</td>
</tr>
<tr>
<td># Failed Attempts</td>
<td>Enter the number of failed login attempts that are allowed for the web interface and CLI before the account is locked. (1-10, default 0). 0 means that there is no limit.</td>
</tr>
<tr>
<td>Lockout Time</td>
<td>Enter the number of minutes that a user is locked out (0-60 minutes) if the number of failed attempts is reached. The default 0 means that there is no limit to the number of attempts.</td>
</tr>
<tr>
<td>Number of Versions for Config Audit</td>
<td>Enter the number of configuration audit versions to save before discarding the oldest ones (default 100).</td>
</tr>
<tr>
<td>Stop Traffic when LogDb full</td>
<td>Select the check box if you want traffic through the firewall to stop when the log database is full (default off).</td>
</tr>
<tr>
<td>Number of Versions for Config Backups</td>
<td>(Panorama only) Enter the number of configuration backups to save before discarding the oldest ones (default 100).</td>
</tr>
</tbody>
</table>

**URL Admin Override**

Specify the settings that are used when a page is blocked by the URL filtering profile and the Override action is specified. Refer to “About URL Filtering Profiles” on page 137.

- **Virtual system**—Select the virtual system from the drop-down list.
- **Password**—Enter the password that the user is required to enter to override the block page.
- **Server Certificate**—Select the server certificate to be used with SSL communications when redirecting through the specified server.
- **Mode**—Determines whether the block page is delivered transparently (it appears to originate at the blocked website) or redirected to the user to the specified server. If you choose Redirect, enter the IP address for redirection.

Click ✗ to delete an entry.
Comparing Configuration Files

Device > Config Audit

You can view and compare configuration files by using the Config Audit page. From the drop-down lists, select the configurations that you want to compare. Select whether to view the differences in a side-by-side display or as inline comparisons, and select the number of lines that you want to include for context. Click Submit.

The system presents the configurations and highlights the differences, as in the following side-by-side example.

![Figure 20. Configuration Comparison](image)

Panorama automatically saves all of the configuration files that are committed on each managed firewall, whether the changes are made through the Panorama interface or locally on the firewall.
Managing Configurations

- **Device > Setup**

When you change a configuration setting and click **OK**, the current “candidate” configuration is updated, not the active configuration. Clicking **Commit** at the top of the page applies the candidate configuration to the active configuration, which activates all configuration changes since the last commit.

This method allows you to review the configuration before activating it. Activating multiple changes simultaneously helps avoid invalid configuration states that can occur when changes are applied in real-time.

You can save and roll back (restore) the candidate configuration as often as needed and also load, validate, import, and export configurations. Pressing **Save** creates a copy of the current candidate configuration, whereas choosing **Commit** updates the active configuration with the contents of the candidate configuration.

**Note:** It is a good idea to periodically save the configuration settings you have entered by clicking the **Save** link in the upper-right corner of the screen.

To manage configurations, select the appropriate configuration management functions, as described in the following table.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate candidate config</td>
<td>Checks the candidate configuration for errors.</td>
</tr>
<tr>
<td>Save candidate config</td>
<td>Saves the candidate configuration in flash memory (same as clicking <strong>Save</strong> at the top of the page).</td>
</tr>
<tr>
<td>Revert to running config</td>
<td>Restores the last running configuration. The current running configuration is overridden.</td>
</tr>
<tr>
<td>Revert to last saved config</td>
<td>Restores the last saved candidate configuration from flash memory. The current candidate configuration is overwritten. An error occurs if the candidate configuration has not been saved.</td>
</tr>
<tr>
<td>Save named config snapshot</td>
<td>Saves the candidate configuration to a file. Enter a file name or select an existing file to be overwritten. Note that the current active configuration file (<em>running-config.xml</em>) cannot be overwritten.</td>
</tr>
<tr>
<td>Load named config snapshot</td>
<td>Loads a candidate configuration from the active configuration (<em>running-config.xml</em>) or from a previously imported or saved configuration. Select the configuration file to be loaded. The current candidate configuration is overwritten.</td>
</tr>
<tr>
<td>Load config version</td>
<td>Loads a specified version of the configuration.</td>
</tr>
<tr>
<td>Export named config snapshot</td>
<td>Exports the active configuration (<em>running-config.xml</em>) or a previously saved or imported configuration. Select the configuration file to be exported. You can open the file and/or save it in any network location.</td>
</tr>
<tr>
<td>Export config version</td>
<td>Exports a specified version of the configuration.</td>
</tr>
<tr>
<td>Import named config spreadsheet</td>
<td>Imports a configuration file from any network location. Click <strong>Browse</strong> and select the configuration file to be imported.</td>
</tr>
</tbody>
</table>
Note: When you click Commit or enter a commit CLI command, all changes made through the web interface and the CLI since the last commit are activated. To avoid possible conflicts, use only the web interface or CLI for most configuration changes.

Installing a License

► Device > Licenses

When you purchase a subscription from Palo Alto Networks, you receive an authorization code that can be used to activate one or more license keys. Perform any of these functions from the License page:

• To enable licenses for standard URL filtering, BrightCloud URL filtering, and Threat Prevention, click the Active link.

• To activate subscriptions that do not require an authorization code, such as for trial licenses, click Retrieve license keys from license server.

• To enable purchased subscriptions that require an authorization code, click Activate feature using authorization code. Enter your authorization code, and click OK.

• If the firewall does not have connectivity to the license server and you want to upload license keys manually, follow these steps:
  b. Save the license key file locally.
  c. Click Manually upload license key, click Browse and select the file, and click OK.

Issues to consider when installing a license

If you are unable to activate the URL filter using the web interface, you can load the database by using the following CLI command:
request url-filtering upgrade brightcloud

To track the progress of the load, use the following CLI command:
tail follow yes mp-log Pan_bc_download.log

You can now activate the BrightCloud URL filtering from the Licenses page.
Defining Custom Response Pages

Custom response pages are the web pages that are displayed when a user tries to access a URL. You can provide a custom HTML message that is downloaded and displayed instead of the requested web page or file.

Each virtual system can have its own custom response pages.

The following table describes the types of custom response pages that support customer messages.

Note: Refer to Appendix A, “Custom Pages” for examples of the default response pages.

<table>
<thead>
<tr>
<th>Page Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus Block Page</td>
<td>Access blocked due to virus infection.</td>
</tr>
<tr>
<td>Application Block Page</td>
<td>Access blocked due to security policy.</td>
</tr>
<tr>
<td>File Blocking Block Page</td>
<td>Access blocked because access to the file is blocked.</td>
</tr>
<tr>
<td>SSL Decryption Opt-out Page</td>
<td>User warning page indicating that this session will be inspected.</td>
</tr>
<tr>
<td>URL Filtering Continue and Override Page</td>
<td>Initial block policy that allows users to bypass the block. A user who thinks the page was blocked inappropriately can click the Continue button to proceed to the page. With the override page, a password is required for the user to override the policy that blocks this URL. See the “URL Admin Override” section of Table 26 for instructions on setting the override password.</td>
</tr>
<tr>
<td>Anti-spyware Download Block Page</td>
<td>Access blocked due to spyware activity.</td>
</tr>
<tr>
<td>Captive Portal Comfort Page</td>
<td>Page for users to verify their user name and password for machines that are not part of the Active Directory domain.</td>
</tr>
<tr>
<td>SSL Certificate Revoked Notify page</td>
<td>Notification that an SSL certificate has been revoked.</td>
</tr>
<tr>
<td>URL Filtering Block Page</td>
<td>Access blocked due to filtering applied to the URL being accessed.</td>
</tr>
<tr>
<td>SSL-VPN Custom Login Page</td>
<td>Page for users who attempt to access the SSL-VPN.</td>
</tr>
</tbody>
</table>

You can perform any of the following functions under **Response Pages**.

- To import a custom HTML response page, click the **Import** link for the type of page. Browse to locate the page. A message is displayed to indicate whether the import succeeded. For the import to be successful, the file must be in HTML format.

- To export a custom HTML response page, click the **Export** link for the type of page. Select whether to open the file or save it to disk, and select the check box if you want to always use the same option.
To enable or disable the Application Block page or SSL Decryption Opt-out pages, click the Enable link for the type of page. Select or deselect the Enable check box.

To use the default response page instead of a previously uploaded page, click the Restore Block Page link for the type of page, and click Restore. A message is displayed to indicate that the restoration succeeded.

### Upgrading the PAN-OS Software

► Device > Software

To upgrade to a new release of the PAN-OS software, you can view the latest versions of the PAN-OS software available from Palo Alto Networks, read the release notes for each version, and then select the release you want to download and install (a support license is required). Perform any of the following functions on the Software page:

- Click Refresh to view the latest software releases available from Palo Alto Networks.
- Click Release Notes to view a description of the changes in a release.
- Click Download to install a new release from the download site. When the download is complete, a checkmark is displayed in the Downloaded column. To install a downloaded release, click Install next to the release.

During installation, you are asked whether to reboot when installation is complete. When the installation is complete, you will be logged out while the firewall is restarted. The firewall will be rebooted, if that option was selected.

- Click Upload to install a release that you previously stored on your PC. Browse to select the software package, and click Install from File. Choose the file that you just selected from the drop-down list, and click OK to install the image.

- Click the Delete icon to delete an outdated release.

#### Items to note when upgrading the PAN-OS software

- When upgrading from a PAN-OS version earlier than Release 3.0.0, you must use the following migration path to reach the latest release: 2.1.2 > 2.1.4 - 2.1.6 > 3.0.0 > 3.0.x.

- The date and time settings on the firewall must be current. PAN-OS software is digitally signed and the signature checked by the device prior to installing a new version. If the date setting is not current, the device may perceive the signature to be erroneously in the future and display the message Decrypt failed: GnuPG edit non-zero, with code 171072 Failed to load into PAN software manager.
Updating Threat and Application Definitions

- **Device > Dynamic Updates**

Palo Alto Networks periodically posts updates with new or revised application definitions and information on new security threats, such as antivirus signatures (threat prevention license required). To upgrade the firewall, you can view the latest updates, read the release notes for each update, and then select the update you want to download and install.

On the **Dynamic Updates** page, you may see two entries listed in the Application and Threats or URL Filtering area, one for the currently installed version and one for the latest version available on the update server. If the latest version is already installed, there is only a single entry.

Perform any of the following functions on this page:

- Click **Check Now** to view the latest threat and application definition updates available from Palo Alto Networks.

- Click **Release Notes** to view a description of an update.

- Click **Download** next to an update to install it. When the download is complete, a checkmark is displayed in the **Downloaded** column.

- Click **Install** next to an update to install the downloaded content update.

- Click the **Schedule** link to schedule automatic updates, click the schedule link. Specify the frequency and timing for the updates and whether the update will be downloaded and installed or only downloaded. If you select **Download Only**, you can install the downloaded update by clicking the **Upgrade** link on the Dynamic Updates page. When you click **OK**, the update is schedule. No commit is required.

- Click **Upload** to install a file that you previously stored on your PC. Browse to select the file, and click **Install from File**. Choose the file that you just selected from the drop-down list, and click **OK** to install.

- Click the Delete icon next to the update to delete an entry.
Importing, Exporting and Generating Security Certificates

Device > Certificates

The Certificates page allows you to generate the following security certificates:

- **Web interface**—Import or export a certificate or generate a self-signed certificate to authenticate users for access to the web interface.

- **Trusted CA certificate**—Import an additional intermediate certificate authority (CA) certificate to trust when doing SSL decryption.

  When the firewall decrypts traffic, it checks the upstream certificate to see if it is issued by a trusted CA. If not, it uses a special untrusted CA certificate to sign the SSL decryption certificate. In this case, the user sees the usual certificate error page when accessing the firewall and must dismiss the warning to log in.

  The firewall has a large list of existing trusted CAs. The trusted CA certificate is for additional CAs that are trusted for your enterprise but are not part of the pre-installed trusted list.

- **SSL Forward Proxy certificate**—Import or generate an SSL forward proxy certificate.

- **SSL Inbound Inspection certificate**—Import or generate an SSL reverse proxy certificate.

  You can upload your own SSL server certificate to allow inspection of traffic coming to your SSL server.

Perform any of the following functions on the Certificates page:

- To import a web interface, trusted CA, or SSL Forward Proxy certificate:
  a. Click Import in the Web Interface Certificate, Trusted CA Certificate, or SSL Forward Proxy Certificate area
  b. Enter the certificate file name or click Browse to locate the file on your computer.
  c. (Web interface and SSL forward proxy only) Enter the key file name or click Browse to locate the file on your computer. Enter the certificate pass phrase. The key should be in Privacy Enhanced Mail (PEM) format.
  d. (SSL forward proxy only). Select the virtual system to which you want to import the certificate from the drop-down list.

- To export the web interface certificate:
  a. Click Export.
  b. (SSL forward proxy only). Select the virtual system from which you want to export the certificate from the drop-down list.
  c. Click Save and then choose a location to copy the file to your local computer.
To generate a self-signed web, SSL forward proxy, or SSL VPN/SSL inbound inspection certificate:

a. Click **Generate a Self-Signed Certificate** in the Web Interface Certificate or SSL Forward Proxy Certificate area to open the appropriate Self-Signed Certificate window.

   **Note:** If you are using Panorama, you also have the option of generating a self-signed certificate for the Panorama server. Refer to “Central Management of Devices” on page 223 for information on Panorama.

b. Enter the IP address or fully qualified domain name that will appear on the certificate in the **Name** field.

c. Enter a pass phrase.

d. Choose the key length in the **Number of Bits** field.

e. Select the country code from the drop-down list. To view a list of country code definitions, click the **ISO 3166 Country Codes** link.

f. Specify additional information to identify the certificate.

g. Click **OK** to save the settings and generate the certificate. After the certificate is saved, the web interface is restarted.

To add an SSL inbound inspection certificate (this is the private key and public certificate for the destination server):

a. Enter the IP address or fully qualified domain name that appears on the certificate in the **Name** field.

b. Enter the certificate file name or click **Browse** to locate the file on your computer.

c. Enter the key file name or click **Browse** to locate the file on your computer. Enter the certificate pass phrase. The key should be in Privacy Enhanced Mail (PEM) format.

d. Click **OK** to save the settings.

For instructions on creating policies for SSL forward proxy, refer to “About SSL Decryption Policies” on page 129.

**Items to note when importing, exporting, and generating certificates**

- If inspection of incoming traffic to a Microsoft Internet Information Server (IIS) server is required, the server's certificate and key can be separated into different files, converted from the .pfx file format to the .pem file format and imported to the firewall for inbound SSL inspection.
Importing, Exporting and Generating Security Certificates

- Use openssl, a text editor, and the following procedure to convert the files:

  1. Run the following command sequence:

```
> openssl -in file_from_IIS.pfx -out tempfile.pem
> openssl pkcs12 -in file_from_IIS.pfx -out tempfile.pem
```

  2. Open the `tempfile.pem` file with a text editor.

  3. Select the portion of the file that is delineated by
     
     ```
     -----BEGIN RSA PRIVATE KEY ----- and -----END RSA PRIVATE KEY-----
     ```

  4. Copy and paste this section into a new file named `server.key`.

  Select the portion of the `tempfile.pem` that is delineated with
  
  ```
  -----BEGIN CERTIFICATE-------and ------END CERTIFICATE
  ```

  5. Copy and paste this section into a new text document named `server.crt`.

Support for Certificate Revocation List and Online Certificate Status Protocol

- **Device > Setup**

Each trusted certificate authority (CA) maintains certificate revocation lists (CRLs) to
determine if an SSL certificate is valid (not revoked) for SSL decryption. The Online Certificate
Status Protocol (OCSP) can also be used to dynamically check the revocation status of a
certificate. For more information on SSL decryption, refer to “About SSL Decryption Policies”
on page 129.

To configure CRL and OCSP settings, click **CRL/OCSP Settings** on the **Setup** page, and
specify the following settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable CRL</td>
<td>Select the check box to use CRL to check the validity of SSL certificates.</td>
</tr>
</tbody>
</table>
| Receive Timeout        | Specify the interval after which the CRL request times out and the status is
determined to be unknown (1-60 seconds).                                   |
| Enable OCSP            | Select the check box to use OCSP to check the validity of SSL certificates. |
| Receive Timeout        | Specify the interval after which the OCSP requests times out and the status is
determined to be unknown (1-60 seconds).                                   |
| Block Unknown Certificate | Select the check box if you want to block certificates that cannot be validated. |
| Block Timeout Certificate | Select the check box if you want to block certificates when the request for certificate information times out. |
| Certificate Status Timeout | Specify the interval after which certificate status requests time out (1-60 seconds). |
Viewing Support Information

Device > Support

The Support page allows you to access product and security alerts from Palo Alto Networks, based on the serial number of your firewall. You can also view a technical knowledge base, and create and view “tickets” for technical support requests.

Perform any of the following functions on this page:

- To view the details of an alert, click the alert name.
- To enter a request for technical support, click Create Ticket. To view your current support requests, click View Ticket.
- To generate a system file to assist Palo Alto Networks technical support in troubleshooting, click Generate Tech Support file. When the file is generated, click Download Tech Support File to download the file to your computer.
- To search for information on a particular issue, click Knowledge Base.
Chapter 4
Network Configuration

This chapter describes how to configure the firewall to support your network architecture:

- “About Firewall Deployment” in the next section
- “About Firewall Interfaces” on page 85
- “About Security Zones” on page 97
- “About Virtual Routers and Routing Protocols” on page 98
- “About DHCP Options” on page 111
- “About VLAN Support” on page 113
- “About Network Profiles” on page 113

Note: For information about VPN support on the firewall, refer to “Configuring IPSec Tunnels” on page 189 and “Configuring IPSec Tunnels” on page 189. For information about quality of service (QoS) support, refer to “Configuring Quality of Service” on page 211
About Firewall Deployment

The firewall can replace your existing firewall when installed between an edge router (or other device that faces the Internet) and a switch or router that connects to your internal network. The firewall supports a wide range of deployment options and interface types that can be used simultaneously on different physical interfaces. They are described in the following sections:

- “About Virtual Wire Deployments” in the next section
- “About Layer 2 Deployments” on page 83
- “About Layer 3 Deployments” on page 83
- “About Tap Mode Deployments” on page 83
- “About Point-to-Point Protocol over Ethernet Support” on page 84
- “Defining Virtual Wires” on page 84

About Virtual Wire Deployments

In a virtual wire deployment, the firewall is installed transparently on a network segment by binding two ports together (Figure 21). You can install the firewall in any network environment with no configuration of adjacent network devices required. If necessary, a virtual wire can block or allow traffic based on the virtual LAN (VLAN) tag values. By default, the virtual wire “default-vwire” binds together Ethernet ports 1 and 2 and allows all untagged traffic.

Choose this option to:
- Simplify installation and configuration.
- Avoid configuration changes to surrounding network devices.

A virtual wire is the default configuration, and should be used only when no switching, routing, or Network Address Translation (NAT) is needed.

Figure 21. Virtual Wire Deployment

To set up virtual wires, refer to “Configuring Virtual Wire Interfaces” on page 91.
About Layer 2 Deployments

In a Layer 2 deployment, the firewall provides switching between two or more networks. Each pair of interfaces must be assigned to a VLAN, and additional Layer 2 subinterfaces can be defined as needed. Choose this option when switching is required (Figure 22).

Figure 22. Layer 2 Deployment

About Layer 3 Deployments

In a Layer 3 deployment, the firewall routes traffic between the two ports. An IP address must be assigned to each interface and a virtual router defined to route the traffic. Choose this option when routing or NAT is required (Figure 23).

Figure 23. Layer 3 Deployment

About Tap Mode Deployments

A network tap is a device that provides a way to access data flowing across a computer network. Tap mode deployment allows you to passively monitor traffic flows across a network by way of a switch SPAN or mirror port.

The SPAN or mirror port permits the copying of traffic from other ports on the switch. By dedicating an interface on the firewall as a tap mode interface and connecting it with a switch SPAN port, the switch SPAN port provides the firewall with the mirrored traffic. This provides application visibility within the network without being in the flow of network traffic.

Note: When deployed in tap mode, the firewall is not able to take action, such as blocking traffic or applying QoS traffic control.
About Point-to-Point Protocol over Ethernet Support

The firewall can be configured to be a Point-to-Point Protocol over Ethernet (PPPoE) termination point to support connectivity in a Digital Subscriber Line (DSL) environment where there is a DSL modem but no other PPPoE device to terminate the connection.

You can choose the PPPoE option and configure the associated settings when an interface is defined as a Layer 3 interface. For instructions, refer to “Configuring Layer 3 Interfaces” on page 88.

Defining Virtual Wires

Use this page to define virtual wires after you have specified two virtual wire interfaces on the firewall. For an overview of virtual wire deployments, refer to “About Virtual Wire Deployments” on page 82. For instructions on specifying interfaces as virtual wire, refer to “Configuring Virtual Wire Interfaces” on page 91.

To define virtual wires, click New and specify the following information.

Table 30. Virtual Wire Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Wire Name</td>
<td>Enter a virtual wire name (up to 31 characters). This name appears in the list of virtual wires when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Select two Ethernet interfaces from the displayed list for the virtual wire configuration. Interfaces are listed here only if they have the virtual wire interface type and have not been assigned to another virtual wire.</td>
</tr>
<tr>
<td>Tags Allowed</td>
<td>Enter the tag number (0 to 4094) or range of tag numbers (tag1-tag2) for the traffic allowed on the virtual wire. A tag value of zero indicates untagged traffic (the default). Multiple tags or ranges must be separated by commas. Traffic that has an excluded tag value is dropped. Note that tag values are not changed on incoming or outgoing packets.</td>
</tr>
<tr>
<td>Multicast Firewalling</td>
<td>Select the check box entitled Enable user of multicast IP addresses in security rules if you want to be able to apply security rules to multicast traffic.</td>
</tr>
<tr>
<td>Link State Pass Through</td>
<td>Select this check box if you want to bring down the other port in a virtual wire when a down link state is detected. If this check box is not selected, link status is not propagated across the virtual wire.</td>
</tr>
</tbody>
</table>

To change a virtual wire name or the allowed tags, click the virtual wire name on the Virtual Wires page, change the settings, and click OK. Virtual wires also can be changed from the Interfaces page (refer to “Configuring Virtual Wire Interfaces” on page 91).

To delete one or more virtual wires, select the check box next to the virtual wire names and click Delete. Note that deleting a virtual wire removes it from the associated virtual wire interfaces shown on the Interfaces page.
# About Firewall Interfaces

The following table describes the types of interfaces supported on the firewall and how to define them.

## Table 31. Supported Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aggregate Ethernet</strong></td>
<td>Two or more Ethernet ports can be combined into a group to increase the throughput and resiliency for a Layer 2, Layer 3, or virtual wire interface and its subinterfaces. Refer to “Configuring Aggregate Ethernet Interfaces” on page 92.</td>
</tr>
<tr>
<td><strong>Layer 2</strong></td>
<td>One or more Layer 2 interfaces can be configured for untagged VLAN traffic. You can then define Layer 2 subinterfaces for traffic with specific VLAN tags. Refer to “Configuring Layer 2 Interfaces” on page 87 and “Configuring Layer 2 Subinterfaces” on page 88.</td>
</tr>
<tr>
<td><strong>Layer 3</strong></td>
<td>One or more Layer 3 interfaces can be configured for untagged routed traffic. You can then define Layer 3 subinterfaces for traffic with specific VLAN tags. Each interface can have multiple IP addresses. Refer to “Configuring Layer 3 Interfaces” on page 88 and “Configuring Layer 3 Subinterfaces” on page 90.</td>
</tr>
<tr>
<td><strong>Loopback</strong></td>
<td>Loopback interfaces, which can be used to manage the firewall, can be associated with a Layer 3 interface (unnumbered) or have their own IP address. Refer to “Configuring Loopback Interfaces” on page 94.</td>
</tr>
<tr>
<td><strong>Virtual Wire</strong></td>
<td>A virtual wire binds two Ethernet ports together, which allows you to install the firewall transparently in the network with minimum configuration. A virtual wire accepts all traffic or traffic with selected VLAN tags, but provides no switching, routing, or NAT services. Refer to “Configuring Virtual Wire Interfaces” on page 91.</td>
</tr>
<tr>
<td><strong>VLAN Interface</strong></td>
<td>VLAN interfaces provide Layer 3 routing of VLAN traffic to non-VLAN destinations. Refer to “Configuring VLAN Interfaces” on page 93.</td>
</tr>
<tr>
<td><strong>Tap</strong></td>
<td>The Tap interface permits connection to a span port on a switch for traffic monitoring only. This mode does not support traffic blocking or URL filtering. Refer to “Configuring Tap Interfaces” on page 95.</td>
</tr>
<tr>
<td><strong>High Availability</strong></td>
<td>You can configure a data interface to be a high availability (HA) interface on some Palo Alto Networks firewalls. Refer to “Configuring High Availability Interfaces” on page 95.</td>
</tr>
</tbody>
</table>
About Aggregate Interface Groups

Aggregate interface groups allow you to generate more than 1 Gbps aggregate throughput by using 802.3ad link aggregation of multiple 1 Gbps links. Aggregation of 10Gbps XFP links is also supported. The aggregate interface that you create becomes a logical interface. Interface management, zone profiles, VPN interfaces, and VLAN subinterfaces are all properties of the logical aggregate interface, not of the underlying physical interfaces.

Each aggregate group can contain several physical interfaces of the type Aggregate Ethernet. After the group is created, you perform operations such as configuring Layer 2 or Layer 3 parameters on the Aggregate Group object rather than on the Aggregate Ethernet interfaces themselves.

The following rules apply to aggregate interface groups:

- The interfaces are compatible with virtual wire, Layer 2, and Layer 3 interfaces.
- Tap mode is not supported.
- The 1 Gig links in a group must be of the same type (all copper or all fiber).
- You can include up to eight aggregate interfaces in an aggregate interface.
- All of the members of an aggregate interface must be of the same type. This is validated during the commit operation.

Viewing the Current Interfaces

Network > Interfaces

The Interfaces page lists the interface type, link state, and security zone for each configured interface, along with the IP address, virtual router, VLAN tag, and VLAN or virtual wire name (as applicable).

By default, the interfaces are listed by interface name. To group the interfaces by another column, such as Security Zone, select the column name from the Group By drop-down list at the bottom of the page.

The following icons are used on the Interfaces page:

- Indicates one or more required interface properties are undefined, such as a security zone. Move the cursor over the icon to view the missing items. Also, “none” appears in the corresponding column for each missing item.

- Used to delete a logical interface (displayed in the last column). You can delete a logical interface by clicking the icon, but the interface type of a logical interface cannot be changed (and the physical Ethernet interfaces cannot be deleted).

- Indicates the link is up (green), down (red), or in an unknown state (gray).
Configuring Layer 2 Interfaces

You can configure one or more Ethernet ports as a Layer 2 interface for untagged VLAN traffic. For each main Layer 2 interface, you can define multiple Layer 2 subinterfaces for traffic with specific VLAN tags (refer to “Configuring Layer 2 Subinterfaces” on page 88) and VLAN interfaces to provide Layer 3 routing of VLAN traffic (refer to “Configuring VLAN Interfaces” on page 93).

To modify a Layer 2 Ethernet interface, follow these steps:

1. Remove the interface from the current security zone, if any. For the interface you want to change, click the name shown in the Security Zone column, select None, and click OK.

2. If you want to change a virtual wire to another interface type, click the virtual wire name shown in the VLAN/Virtual Wire column, if any, select None, and click OK.

3. Click the interface name and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select L2 from the drop-down list.</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Select the interface speed in Mbps (10, 100, or 1000).</td>
</tr>
<tr>
<td>Link Duplex</td>
<td>Select whether the interface transmission mode is full-duplex (Full), half-</td>
</tr>
<tr>
<td></td>
<td>duplex (Half), or negotiated automatically (Auto).</td>
</tr>
<tr>
<td>Link State</td>
<td>Select whether the interface status is enabled (Up), disabled (Down), or</td>
</tr>
<tr>
<td></td>
<td>determined automatically (Auto).</td>
</tr>
<tr>
<td>Assign Interface To</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>Select a VLAN, or click New to define a new VLAN (refer to “About VLAN</td>
</tr>
<tr>
<td></td>
<td>VLAN Support” on page 113).</td>
</tr>
<tr>
<td>Zone</td>
<td>Select a security zone for the interface, or click New to define a new zone</td>
</tr>
<tr>
<td></td>
<td>(refer to “Defining Security Zones” on page 97).</td>
</tr>
</tbody>
</table>
Configuring Layer 2 Subinterfaces

For each Ethernet port configured as a Layer 2 interface, you can define an additional logical Layer 2 interface (subinterface) for each VLAN tag that is used on the traffic received by the port. To configure the main Layer 2 interfaces, refer to “Configuring Layer 2 Interfaces” on page 87.

To add a Layer 2 Ethernet subinterface, select L2 Interface from the New drop-down list at the bottom of the Interfaces page, and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td>Select the Layer 2 interface where you want to add a subinterface. To configure the Layer 2 interfaces, refer to “Configuring Layer 2 Interfaces” on page 87.</td>
</tr>
<tr>
<td>Logical Interface Name</td>
<td>Enter the number (1 to 9999) appended to the physical interface name to form the logical interface name. The general name format is: ethernetx/y.&lt;1-9999&gt;</td>
</tr>
<tr>
<td>Tag</td>
<td>Enter the tag number (1 to 4094) of the traffic received on this interface. Outgoing traffic on this interface is also set to this tag value.</td>
</tr>
<tr>
<td>Assign Interface To</td>
<td>For a Layer 2 interface, select a VLAN, or click New to define a new VLAN (refer to “About VLAN Support” on page 113).</td>
</tr>
<tr>
<td>Zone</td>
<td>For all interfaces, select a security zone for the interface, or click New to define a new zone (refer to “Defining Security Zones” on page 97).</td>
</tr>
</tbody>
</table>

Configuring Layer 3 Interfaces

You can configure one or more Ethernet ports as Layer 3 interfaces for untagged routed traffic. You can then define Layer 3 subinterfaces for traffic with specific VLAN tags (refer to “Configuring Layer 3 Subinterfaces” on page 90). For information on configuring Layer 3 interfaces for PPPoE, refer to “About Point-to-Point Protocol over Ethernet Support” on page 84.

To modify a Layer 3 interface, follow these steps:

1. Remove the interface from the current security zone, if any. For the interface you want to change, click the name shown in the Security Zone column, select None, and click OK.

2. If you want to change a virtual wire to another interface type, click the virtual wire name shown in the VLAN/Virtual Wire column, if any, select None, and click OK.
3. Click the interface name and specify the following information.

<table>
<thead>
<tr>
<th>Table 34. Layer 3 Interface Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Link Speed</td>
</tr>
<tr>
<td>Link Duplex</td>
</tr>
<tr>
<td>Link State</td>
</tr>
<tr>
<td>MTU</td>
</tr>
<tr>
<td>Management Profile</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>ARP Entries</td>
</tr>
</tbody>
</table>
Configuring Layer 3 Subinterfaces

For each Ethernet port configured as a Layer 3 interface, you can define an additional logical Layer 3 interface (subinterface) for each VLAN tag that is used on the traffic received by the port. To configure the main Layer 3 interfaces, refer to “Configuring Layer 3 Interfaces” on page 88.

To add a Layer 3 Ethernet subinterface, select L3 Interface from the New drop-down list at the bottom of the Interfaces page, and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td>Select the Layer 3 interface where you want to add a subinterface. To configure the Layer 3 interfaces, refer to “Configuring Layer 3 Interfaces” on page 88.</td>
</tr>
<tr>
<td>Logical Interface Name</td>
<td>Enter the number (1 to 9999) appended to the physical interface name to form the logical interface name. The general name format is: ethernetx/y.&lt;1-9999&gt;</td>
</tr>
<tr>
<td>Tag</td>
<td>Enter the tag number (1 to 4094) of the traffic received on this interface. Outgoing traffic on this interface is also set to this tag value.</td>
</tr>
<tr>
<td>MTU</td>
<td>Enter the maximum transmission unit in bytes for packets sent on this interface (512 to 150, default 1500).</td>
</tr>
<tr>
<td>Management Profile</td>
<td>Select a profile that specifies which protocols, if any, can be used to manage the firewall over this interface.</td>
</tr>
<tr>
<td>IP Address and Subnet Mask</td>
<td>Enter an IP address and network mask for the interface in the format ip_address/mask, and click Add. You can enter multiple IP addresses for the interface. To delete an IP address, select the address and click Delete.</td>
</tr>
<tr>
<td>ARP Entries</td>
<td>To add one or more static ARP entries, enter an IP address and its associated hardware (MAC) address, and click Add. To delete a static entry, select the entry and click Delete.</td>
</tr>
<tr>
<td>Assign Interface To</td>
<td>Select a virtual router, or click New to define a new virtual router (refer to “About Virtual Routers and Routing Protocols” on page 98).</td>
</tr>
<tr>
<td>Zone</td>
<td>Select a security zone for the interface, or click New to define a new zone (refer to “Defining Security Zones” on page 97).</td>
</tr>
</tbody>
</table>
Configuring Virtual Wire Interfaces

You can bind two Ethernet ports together as a virtual wire, which allows all traffic to pass between the ports, or just traffic with selected VLAN tags (no other switching, routing, or NAT services are available). A virtual wire requires no changes to adjacent network devices. For an overview of virtual wire deployments, refer to “About Virtual Wire Deployments” on page 82.

To set up a virtual wire through the firewall, you must first define the in and out virtual wire interfaces, as described in the following procedure, and then create the virtual wire using the interfaces that you created.

To configure each virtual wire interface, follow these steps:

1. Identify the interface you want to use for the virtual wire, and remove it from the current security zone, if any. For the interface you want to change, click the name shown in the Security Zone column, select None, and click OK.

2. Click the interface name and specify the following information.

Table 36. Virtual Wire Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Virtual Wire from the drop-down list.</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Select the interface speed in Mbps (10, 100, or 1000).</td>
</tr>
<tr>
<td>Link Duplex</td>
<td>Select whether the interface transmission mode is full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).</td>
</tr>
<tr>
<td>Link State</td>
<td>Select whether the interface status is enabled (Up), disabled (Down), or determined automatically (Auto).</td>
</tr>
<tr>
<td>Assign Interface To</td>
<td>Select a virtual wire, or click New to define a new virtual wire (refer to “Defining Virtual Wires” on page 84).</td>
</tr>
<tr>
<td>Zone</td>
<td>Select a security zone for the interface, or click New to define a new zone (refer to “Defining Security Zones” on page 97).</td>
</tr>
</tbody>
</table>

If you want to change a virtual wire to another interface type, click the virtual wire name shown in the VLAN/Virtual Wire column, if any, select None, and click OK.
### Configuring Aggregate Interface Groups

**Network > Interfaces**

You can configure one or more interfaces as part of an aggregate Ethernet interface group. First define the group, as described in this section, and then assign interfaces to the group. For instructions on assigning interfaces to the group, refer to “Configuring Layer 3 Subinterfaces” on page 90.

To create and configure aggregate group interfaces, select **Aggregate Group** from the New drop-down list and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a numeric suffix to identify the interface. The interface name is listed as ae.&lt;i&gt;n&lt;/i&gt; where &lt;i&gt;n&lt;/i&gt; is the suffix (1-8).</td>
</tr>
<tr>
<td>Type</td>
<td>Select the interface type (Layer 2, Layer 3, or virtual wire).</td>
</tr>
<tr>
<td>Assign Interface To</td>
<td></td>
</tr>
<tr>
<td>Virtual Wire</td>
<td>Select a virtual wire, or click <strong>New</strong> to define a new virtual wire (refer to “Defining Virtual Wires” on page 84).</td>
</tr>
<tr>
<td>Zone</td>
<td>Select a security zone for the interface, or click <strong>New</strong> to define a new zone (refer to “Defining Security Zones” on page 97).</td>
</tr>
</tbody>
</table>

### Configuring Aggregate Ethernet Interfaces

**Network > Interfaces**

Each aggregate Ethernet interface is assigned a name of the form ae.<i>number</i> and can be of the type Layer 2, Layer 3, or virtual wire. After the assignment is made, the new interface functions in the same way as any other interface.

To configure aggregate Ethernet interfaces, click the interface name and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select <strong>Aggregate Ethernet</strong> from the drop-down list.</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Select the interface speed in Mbps (10, 100, or 1000).</td>
</tr>
<tr>
<td>Link Duplex</td>
<td>Select whether the interface transmission mode is full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).</td>
</tr>
<tr>
<td>Link State</td>
<td>Select whether the interface status is enabled (Up), disabled (Down), or determined automatically (Auto).</td>
</tr>
</tbody>
</table>
Configuring VLAN Interfaces

For each Ethernet port configured as a Layer 2 interface, you can define a VLAN interface to allow routing of the VLAN traffic to Layer 3 destinations outside the VLAN. To configure the main Layer 2 interfaces, refer to “Configuring Layer 2 Interfaces” on page 87.

To define VLAN interfaces, select VLAN Interface from the New drop-down list at the bottom of the page and specify the following information.

| Table 38. Aggregate Ethernet Interface Settings (Continued) |
|-------------------------------|---------------------------------|
| Field                        | Description                     |
| Assign Interface To          |                                 |
| Virtual Router               | Select a virtual router, or click New to define a new virtual router (refer to “About Virtual Routers and Routing Protocols” on page 98). |
| Aggregate Group              | Select an aggregate interface group. Each aggregate group (designated as ae.n) can contain several physical interfaces of the type Aggregate Ethernet. After the group is created, you perform operations such as configuring Layer 2 or Layer 3 parameters on the Aggregate Group object rather than on the Aggregate Ethernet interfaces themselves. Refer to “Configuring Aggregate Interface Groups” on page 92. |

| Table 39. VLAN Interface Settings |
|-------------------------------|---------------------------------|
| Field                        | Description                     |
| VLAN Interface Name          | Enter the number appended to “vlan” to form the interface name (1-9999). The general name format is: vlan.<1-9999> |
| MTU                          | Enter the maximum transmission unit in bytes for packets sent on this interface (512-1500, default 1500). |
| Management Profile           | Select a profile that specifies which protocols, if any, can be used to manage the firewall over this interface. |
| IP Address and Subnet Mask   | Enter an IP address and network mask for the interface in the format ip_address/mask, and click Add. You can enter multiple IP addresses for the interface. To delete an IP address, select the address and click Delete. |
| ARP/Interface Entries        | To add one or more static ARP entries, enter an IP address and its associated hardware (MAC) address, select the Layer 3 interface that can access the hardware address, and click Add. To delete a static entry, select the entry and click Delete. |
| Assign Interface To          |                                 |
| Virtual Router               | Select a virtual router, or click New to define a new virtual router (refer to “About Virtual Routers and Routing Protocols” on page 98). |
| VLAN                         | Select a VLAN, or click New to define a new VLAN (refer to “About VLAN Support” on page 113). |
| Zone                         | Select a security zone for the interface, or click New to define a new zone (refer to “Defining Security Zones” on page 97). |
Configuring Loopback Interfaces

To define loopback interfaces, select Loopback Interface from the New drop-down list at the bottom of the page, and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback Interface Name</td>
<td>Enter the number (1 to 9999) appended to “loopback” to form the interface name. The general name format is: loopback.&lt;1-9999&gt;</td>
</tr>
<tr>
<td>MTU</td>
<td>Enter the maximum transmission unit in bytes for packets sent on this interface (512 to 1500, default 1500).</td>
</tr>
<tr>
<td>Management Profile</td>
<td>Select a profile that specifies which protocols, if any, can be used to manage the firewall over this interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Select IP to enter an IP address for the interface, or select Unnumbered to select the Layer 3 interface that acts as loopback interface.</td>
</tr>
<tr>
<td>IP Address and Subnet Mask</td>
<td>Enter an IP address and network mask for the interface in the format ip_address / mask, and click Add. You can enter multiple IP addresses for the interface. To delete an IP address, select the address and click Delete.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>If you select Unnumbered as the type, select a Layer 3 interface from the drop-down list.</td>
</tr>
<tr>
<td>Assign Interface To</td>
<td>Select a virtual router, or click New to define a new virtual router (refer to “About Virtual Routers and Routing Protocols” on page 98).</td>
</tr>
<tr>
<td>Zone</td>
<td>Select a security zone for the interface, or click New to define a new zone (refer to “Defining Security Zones” on page 97).</td>
</tr>
</tbody>
</table>
Configuring Tap Interfaces

> Network > Interfaces

You can define tap interfaces as needed to permit connection to a span port on a switch for traffic monitoring only (refer to “About Tap Mode Deployments” on page 83).

To define tap interfaces, click an interface name to open the Edit Ethernet Interface page, and specify the following information.

Table 41. Tap Interface Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Tap from the drop-down list.</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Select the interface speed in Mbps (10, 100, or 1000).</td>
</tr>
<tr>
<td>Link Duplex</td>
<td>Select whether the interface transmission mode is full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).</td>
</tr>
<tr>
<td>Link State</td>
<td>Select whether the interface status is enabled (Up), disabled (Down), or determined automatically (Auto).</td>
</tr>
<tr>
<td>Assign Interface To</td>
<td>Select a virtual system.</td>
</tr>
<tr>
<td>Zone</td>
<td>Select a security zone for the interface, or click New to define a new zone (refer to “Defining Security Zones” on page 97).</td>
</tr>
</tbody>
</table>

1. Click OK to submit the new interface, or click Cancel to discard your changes.

2. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 72.

Configuring High Availability Interfaces

Each high availability (HA) interface has a specific function: one interface is for configuration synchronization and heartbeats and the other interface is for state synchronization.

Note: On the PA-2000 Series and PA-500 firewalls, you specify the data ports to be used for HA. The PA-4000 Series has dedicated physical ports for HA. For additional information on HA, refer to “Enabling High Availability on the Firewall” on page 30.

To define HA interface, click an interface name to open the Edit Ethernet Interface page, and specify the following information.

Table 42. High Availability Interface Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select HA from the drop-down list.</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Select the interface speed in Mbps (10, 100, or 1000).</td>
</tr>
</tbody>
</table>
### Table 42. High Availability Interface Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Duplex</td>
<td>Select whether the interface transmission mode is full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).</td>
</tr>
<tr>
<td>Link State</td>
<td>Select whether the interface status is enabled (Up), disabled (Down), or determined automatically (Auto).</td>
</tr>
</tbody>
</table>
About Security Zones

A security zone identifies one or more source or destination interfaces on the firewall. When you define a security policy rule, you must specify the source and destination security zones of the traffic. For example, an interface connected to the Internet is in an “untrusted” security zone, while an interface connected to the internal network is in a “trusted” security zone.

Separate zones must be created for each type of interface (Layer 2, Layer 3, or virtual wire), and each interface must be assigned to a zone before it can process traffic. Security policies can be defined only between zones of the same type. However, if you create a VLAN interface for one or more VLANs, applying security policies between the VLAN interface zone and a Layer 3 interface zone (Figure 24) has the same effect as applying policies between the Layer 2 and Layer 3 interface zones.

Figure 24. Zone and Interface Types

Defining Security Zones

Network > Zones

In order for a firewall interface to be able to process traffic, it must be assigned to a security zone. To define security zones, click New and specify the following information.

Table 43. Security Zone Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual System</td>
<td>Select the virtual system that applies to this zone.</td>
</tr>
<tr>
<td>Zone</td>
<td>Enter a zone name (up to 31 characters). This name appears in the list of zones when defining security policies and configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.</td>
</tr>
</tbody>
</table>
You can set up virtual routers to enable the firewall to route packets at Layer 3 by making packet forwarding decisions according to the destination address. The Ethernet interfaces, loopback interfaces, and VLAN interfaces defined on the firewall receive and forward the Layer 3 traffic. The destination zone is derived from the outgoing interface based on the forwarding criteria, and policy rules are consulted to identify the security policies to be applied.

Support is provided for static routing and dynamic routing using the Routing Information Protocol (RIP), Open Shortest Path First (OSPF) protocol, and Border Gateway Protocol (BGP).

**Routing Information Protocol**

RIP was designed for small IP networks and relies on hop count to determine routes; the best routes have the fewest number of hops. RIP is based on UDP and uses port 520 for route updates. By limiting routes to a maximum of 15 hops, the protocol helps prevent the development of routing loops, but also limits the supported network size. If more than 15 hops are required, traffic is not routed. RIP also can take longer to converge than OSPF and other routing protocols.
Open Shortest Path First

OSPF determines routes dynamically by obtaining information from other routers and advertising routes to other routers by way of Link State Advertisements (LSAs). The router keeps information about the links between it and the destination and can make highly efficient routing decisions. A cost is assigned to each router interface, and the best routes are determined to be those with the lowest costs, when summed over all the encountered outbound router interfaces and the interface receiving the LSA. Hierarchical techniques are used to limit the number of routes that must be advertised and the associated LSAs. Because OSPF dynamically processes a considerable amount of route information, it has greater processor and memory requirements than does RIP.

Border Gateway Protocol

The Border Gateway Protocol (BGP) is the primary Internet routing protocol. BGP determines network reachability based on IP prefixes that are available within autonomous systems (AS), where an AS is a set of IP prefixes that a network provider has designated to be part of a single routing policy.

In the routing process, connections are established between BGP peers (or neighbors). If a route is permitted by the policy, it is stored in the routing information base (RIB). Each time the local firewall RIB is updated, the firewall determines the optimal routes and sends an update to the external RIB, if export is enabled.

Conditional advertisement is used to control how BGP routes are advertised. The BGP routes must satisfy conditional advertisement rules before being advertised to peers.

BGP supports the specification of aggregates, which combine multiple routes into a single route. During the aggregation process, the first step is to find the corresponding aggregation rule by performing a longest match that compares the incoming route with the prefix values for other aggregation rules.

The firewall provides a complete BGP implementation that includes the following features:

- Specification of one BGP routing instance per virtual router.
- Routing policies based on route-map to control import, export and advertisement, prefix-based filtering, and address aggregation.
- Advanced BGP features that include route reflector, AS confederation, route flap dampening, and graceful restart.
- IGP-BGP interaction to inject routes to BGP using redistribution profiles.

BGP configuration consists of the following elements:

- Per-routing-instance settings, which include basic parameters such as local route ID and local AS and advanced options such as path selection, route reflector, AS confederation, route flap, and dampening profiles.
- Authentication profiles, which specify the MD5 authentication key for BGP connections.
- Peer group and neighbor settings, which include neighbor address and remote AS and advanced options such as neighbor attributes and connections.
- Routing policy, which specifies rule sets that peer groups and peers use to implement imports, exports, conditional advertisements, and address aggregation controls.
Redistribution Profiles

Redistribution profiles allow you to modify route redistribution filter, priority, and action based on desired network behavior.

Defining Virtual Routers

Network > Virtual Routers

Defining virtual routers allows you to set up forwarding rules for Layer 3 and enable the use of dynamic routing protocols. Each Layer 3 interface, loopback interface, and VLAN interface defined on the firewall should be associated with a virtual router. Each interface can belong to only one virtual router.

Note: To configure Ethernet ports as Layer 3 interfaces, refer to “Configuring Layer 3 Interfaces” on page 88. To define Layer 3 subinterfaces, refer to “Configuring Layer 3 Subinterfaces” on page 90. For an overview of virtual routers, refer to “About Virtual Routers and Routing Protocols” on page 98.

Define settings on the specified tabs, as appropriate.
• General—Select the interfaces to include in the virtual router and add any static routes. Refer to the following table.

Table 44. Virtual Router Settings - General Tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>Select the interfaces that you want to include in the virtual router. When you select an interface, it is included in the virtual router and can be used as an outgoing interface in the virtual router's routing tab. To specify the interface type, refer to “About Firewall Interfaces” on page 85. Note: When you add an interface, its connected routes are added automatically.</td>
</tr>
</tbody>
</table>
| Admin Distances | Specify the following administrative distances:  
• Static routes (10-240, default 10).  
• Internal OSPF (10-240, default 30).  
• External OSPF (10-240, default 110).  
• Internal BGP (IBGP) (10-240, default 200).  
• External BGP (EBGP) (10-240, default 20).  
• RIP (10-240, default 120). |
| Static Routes | In this section, optionally enter one or more static routes. Note: It is usually necessary to configure default routes (0.0.0.0/0) here. Default routes are applied for destinations that are otherwise not found in the virtual router’s routing table. Click Add after adding each route. The new route is added. Click the-trash icon to delete a route. |
| Name        | Enter a name to identify the static route. |
About Virtual Routers and Routing Protocols

Table 44. Virtual Router Settings - General Tab (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Enter an IP address and network mask in the format ip_address/mask.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface to forward packets to its destination, or configure the Next Hop field, or both.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Specify the Next Hop field, as follows, or the interface, or both:</td>
</tr>
<tr>
<td></td>
<td>• Interface—Select the interface to forward packets to its destination.</td>
</tr>
<tr>
<td></td>
<td>• IP—Specify the gateway IP address.</td>
</tr>
<tr>
<td></td>
<td>• Discard—Select if you want to drop the traffic that is sent to the specified IP addresses.</td>
</tr>
<tr>
<td>Admin Distance</td>
<td>Specify the administrative distance for the static route (10-240, default 10).</td>
</tr>
<tr>
<td>Metric</td>
<td>Specify a valid metric for the static route (1 - 65535).</td>
</tr>
<tr>
<td>No Install</td>
<td>Select if you do not want to install the route in the forwarding table. The route is retained in the configuration for future reference.</td>
</tr>
</tbody>
</table>
About Virtual Routers and Routing Protocols

- **Redistribution Profiles**—Modify route redistribution filter, priority, and action based on desired network behavior. Route redistribution allows static routes and routes that are acquired by other protocols to be advertised through specified routing protocols. Redistribution profiles must be applied to routing protocols in order to take effect. Without redistribution rules, each protocol runs separately and does not communicate outside its purview. Redistribution profiles can be added or modified after all routing protocols are configured and the resulting network topology is established. Apply redistribution profiles to the RIP and OSPF protocols by defining export rules. Apply redistribution profiles to BGP in the Redistribution Rules tab. Refer to the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Click Add to display the New Redistribution Profile page, and enter the profile name.</td>
</tr>
<tr>
<td>Priority</td>
<td>Enter a priority (range 1-255) for this profile. Profiles are matched in order (lowest number first).</td>
</tr>
<tr>
<td>Filter</td>
<td>Configure the following filter options.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>—Select check boxes to specify the route types of the candidate route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Interface</strong>—Select the interfaces to specify the forwarding interfaces of the candidate route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination</strong>—To specify the destination of the candidate route, enter the destination IP address or subnet (format x.x.x.x or x.x.x.x/n) and click Add. To remove an entry, click the icon associated with the entry.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Next Hop</strong>—To specify the gateway of the candidate route, enter the IP address or subnet (format x.x.x.x or x.x.x.x/n) that represents the next hop and click Add. To remove an entry, click the icon associated with the entry.</td>
</tr>
<tr>
<td>OSPF Params</td>
<td>Optionally configure these OSPF filter parameters.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Path Type</strong>—Select check boxes to specify the route types of the candidate OSPF route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Area</strong>—Specify the area identifier for the candidate OSPF route. Enter the OSPF area ID (format x.x.x.x), and click Add. To remove an entry, click the icon associated with the entry.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Tag</strong>—Specify OSPF tag values. Enter a numeric tag value (1-255), and click Add. To remove an entry, click the icon associated with the entry.</td>
</tr>
<tr>
<td>BGP Params</td>
<td>Configure parameters for community and extended community:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Community</strong>—Specify a community for BGP routing policy.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Extended Community</strong>—Specify an extended community for BGP routing policy.</td>
</tr>
<tr>
<td>Action</td>
<td>Select from the following actions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Redistribute</strong>—Select to redistribute matching candidate routes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Metric</strong>—Enter the new metric value when taking a redistribution action. A lower metric value means a more preferred route.</td>
</tr>
</tbody>
</table>
• **RIP**—Specify parameters for use of the Routing Information Protocol (RIP) on the selected interfaces. Although it is possible to configure both RIP and OSPF, it is generally recommended to choose only one of these protocols. Refer to the following table.

### Table 46. Virtual Router Settings - RIP Tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Select the check box to enable the RIP protocol.</td>
</tr>
<tr>
<td>Reject Default Route</td>
<td>Select the check box if you do not want to learn any default routes through RIP. Selecting the check box is highly recommended.</td>
</tr>
<tr>
<td>Allow Redist Default Route</td>
<td>Select the check box to permit redistribution of default routes through RIP.</td>
</tr>
<tr>
<td>Auth Profiles</td>
<td>To authenticate RIP messages, first define the authentication profiles and then apply them to interfaces on the <strong>RIP</strong> tab. Click <strong>Add</strong>, enter the following values, and click <strong>OK</strong>:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>—Enter a name for the authentication profile.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password Type</strong>—Select the type of password (simple or MD5).</td>
</tr>
<tr>
<td></td>
<td>– If you select <strong>Simple</strong>, enter the password.</td>
</tr>
<tr>
<td></td>
<td>– If you select <strong>MD5</strong>, enter one or more password entries, including <strong>Key-ID</strong> (0-255), <strong>Key</strong>, and optional <strong>Preferred</strong> status. Click <strong>Add</strong> for each entry, and then click <strong>OK</strong>. To specify the key to be used to authenticate outgoing message, select the <strong>Preferred</strong> option.</td>
</tr>
<tr>
<td>Export Rules</td>
<td>(Read-only) Displays the rules that apply to routes sent by the virtual router to a receiving router.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Click <strong>Add</strong>, enter the following values, and click <strong>OK</strong>:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Interface</strong>—Select the interface that runs the RIP protocol.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong>—Select to enable these settings.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Advertise and Metric</strong>—Select to advertise a default route to RIP peers with the specified metric value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auth Profile</strong>—Select the profile.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mode</strong>—Select normal, passive, or send-only.</td>
</tr>
<tr>
<td>RIP Timing</td>
<td>Configure these timing settings:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Interval Duration</strong>—Define the length of the timer interval in seconds. This duration is used for the remaining <strong>RIP Timing</strong> fields (1 - 60).</td>
</tr>
<tr>
<td></td>
<td>• <strong># Update Intervals</strong>—Enter the number of intervals between route update announcements (1 - 3600).</td>
</tr>
<tr>
<td></td>
<td>• <strong># Expire Intervals</strong>—Enter the number of intervals between the time that the route was last updated to its expiration (1- 3600).</td>
</tr>
<tr>
<td></td>
<td>• <strong># Delete Intervals</strong>—Enter the number of intervals between the time that the route expires to its deletion (1- 3600).</td>
</tr>
</tbody>
</table>
• **OSPF**—Specify parameters for use of the Open Shortest Path First (OSPF) protocol on the selected interfaces. Although it is possible to configure both RIP and OSPF, it is generally recommended to choose only one of these protocols. Refer to the following table.

### Table 47. Virtual Router Settings - OSPF Tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Select the check box to enable the OSPF protocol.</td>
</tr>
<tr>
<td>Reject Default Route</td>
<td>Select the check box if you do not want to learn any default routes through OSPF. Selecting the check box is recommended, especially for static routes. Specify the router ID associated with the OSPF instance in this virtual router. The OSPF protocol uses the router ID to uniquely identify the OSPF instance.</td>
</tr>
<tr>
<td>Allow Redist Default Route</td>
<td>Select the check box to permit redistribution of default routes through OSPF. If you select the check box, enter the router ID.</td>
</tr>
<tr>
<td>RFC 1583 Compatibility</td>
<td>Select the check box to assure compatibility with RFC 1583.</td>
</tr>
<tr>
<td>Export Rules</td>
<td>To apply redistribution profiles for export routes to the OSPF instance, click <strong>Add</strong>, enter the following information, and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>—Select the name of a redistribution profile.</td>
</tr>
<tr>
<td></td>
<td>• <strong>New Metric Type</strong>—Select the metric type to apply.</td>
</tr>
<tr>
<td></td>
<td>• <strong>New Tag</strong>—Specify a tag for the matched route that has a 32-bit value.</td>
</tr>
<tr>
<td>Auth Profiles</td>
<td>To authenticate the OSPF messages, first define the authentication profiles and then apply them to interfaces on the OSPF tab. Click <strong>Add</strong> and enter the following values.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>—Enter a name for the authentication profile.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password Type</strong>—Select the type of password (simple or MD5).</td>
</tr>
<tr>
<td></td>
<td>– If you select <strong>Simple</strong>, enter the password.</td>
</tr>
<tr>
<td></td>
<td>– If you select <strong>MD5</strong>, enter one or more password entries, including <strong>Key-ID</strong> (0-255), <strong>Key</strong>, and optional <strong>Preferred</strong> status. Click <strong>Add</strong> for each entry, and then click <strong>OK</strong>. To specify the key to be used to authenticate outgoing message, select the <strong>Preferred</strong> option.</td>
</tr>
<tr>
<td>Areas</td>
<td>Use this section to configure the area over which the OSPF parameters can be applied. Click <strong>New</strong>, enter the following values, and click <strong>Done</strong>.</td>
</tr>
<tr>
<td>Area ID</td>
<td>Enter an identifier for the area in x.x.x.x format. This is the identifier that each neighbor must accept to be part of the same area.</td>
</tr>
</tbody>
</table>
About Virtual Routers and Routing Protocols

Table 47. Virtual Router Settings - OSPF Tab (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Type  | Select one of the following options.  
  - **Normal**—There are no restrictions; the area can carry all types of routes.  
  - **Stub**—There is no outlet from the area. To reach a destination outside of the area, it is necessary to go through the border, which connects to other areas. If you select this option, select **Accept Summary** if you want to accept this type of link state advertisement (LSA) from other areas. Also, specify whether to include a default route LSA in advertisements to the stub area along with the associated metric value (1-255).  
  - **NSSA** (not so stub area)—It is possible to leave the area directly, but only by routes other than OSPF routes. If you select this option, select **Accept Summary** if you want to accept this type of LSA. Specify whether to include a default route LSA in advertisements to the stub area along with the associated metric value (1-255). Also, select the route type used to advertise the default LSA. Click **Add** in the **External Ranges** section and enter ranges if you want to enable or suppress advertising external routes that are learned through NSSA to other areas. |
| Ranges | Click **Add** to aggregate LSA destination addresses in the area into subnets. Enable or suppress advertising LSAs that match the subnet, and click **OK**. Repeat to add additional ranges. |
| Interface | Click **Add** and enter the following information for each interface to be included in the area, and click **OK**.  
  - **Name**—Choose the interface.  
  - **Enable**—Cause the OSPF interface settings to take effect.  
  - **Passive**—Select the check box if you do not want the OSPF interface to send or receive OSPF packets. Although OSPF packets are not sent or received if you choose this option, the interface is included in the LSA database.  
  - **Link type**—Choose **broadcast** if you want all neighbors that are accessible through the interface to be discovered automatically by multicasting OSPF hello messages, such as an Ethernet interface. Choose **p2p** (point-to-point) to automatically discover the neighbor. Choose **p2mp** (point-to-multipoint) when neighbors must be defined manually. Defining neighbors manually is allowed only for p2mp mode.  
  - **Metric**—Enter the OSPF metric for this interface (0-65535).  
  - **Priority**—Enter the OSPF priority for this interface (0-255). It is the priority for the router to be elected as a designated router (DR) or as a backup DR (BDR) according to the OSPF protocol. When the value is zero, the router will not be elected as a DR or BDR.  
  - **Timing**—It is recommended that you keep the default timing settings.  
  - **Auth Profile**—Select a previously-defined authentication profile.  
  - **Neighbors**—For p2mp interfaces, enter the neighbor IP address for all neighbors that are reachable through this interface. |
About Virtual Routers and Routing Protocols

• **BGP**—Specify parameters for use of Border Gateway Protocol (BGP) on the selected interfaces. Refer to the following table.

| Table 47. Virtual Router Settings - OSPF Tab (Continued) |
|------------|-----------------|
| **Field**  | **Description**  |
| Virtual Link | Configure the virtual link settings to maintain or enhance backbone area connectivity. The settings must be defined for area borderer routers, and must be defined within the backbone area (0.0.0.0). Click **Add**, enter the following information for each virtual link to be included in the backbone area, and click **OK**.
  • **Name**—Enter a name for the virtual link.
  • **Neighbor ID**—Enter the router ID of the router (neighbor) on the other side of the virtual link.
  • **Transit Area**—Enter the area ID of the transit area that physically contains the virtual link.
  • **Enable**—Select to enable the virtual link.
  • **Timing**—It is recommended that you keep the default timing settings.
  • **Auth Profile**—Select a previously-defined authentication profile. |

| Table 48. Virtual Router Settings - BGP Tab |
|------------|-----------------|
| **Field**  | **Description**  |
| **General Tab** | |
| Enable | Select the check box to enable BGP. |
| Router ID | Enter the IP address to assign to the virtual router. |
| AS Number | Enter the number of the AS to which the virtual router belongs, based on the router ID. |
| Reject Default Route | Select the check box to ignore any default routes that are advertised by BGP peers. |
| Allow Redist Default Route | Select the check box to permit the firewall to redistribute its default route to BGP peers. |
| Install Route | Select the check box to install BGP routes in the global routing table. |
| Aggregate MED | Select to enable route aggregation even when routes have different Multi-Exit Discriminator (MED) values. |
| Reflector Cluster ID | Specify an IPv4 identifier to represent the reflector cluster. |
| Confederation Number AS | Specify the identifier for the AS confederation to be presented as a single AS to external BGP peers. |
| Auth Profiles | Click **Add** to include a new authentication profile and configure the following settings:
  • **Profile Name**—Enter a name to identify the profile.
  • **Secret/Confirm Secret**—Enter and confirm a passphrase for BGP peer communications.
  Click the **X** icon to delete a profile. |
About Virtual Routers and Routing Protocols

Dampening Profiles Settings include:

- **Profile Name**—Enter a name to identify the profile.
- **Enable**—Activate the profile.
- **Cutoff**—Specify a route withdrawal threshold above which a route advertisement is suppressed (range 0.0-1000.0, default 1.25).
- **Reuse**—Specify a route withdrawal threshold below which a suppressed route is used again (range 0.0-1000.0, default .5).
- **Max. Hold Time**—Specify the maximum length of time that a route can be suppressed, regardless of how unstable it has been (range 0-3600 seconds, default 900 seconds).
- **Decay Half Life Reachable**—Specify the length of time after which a route's stability metric is halved if the route is considered reachable (range 0-3600 seconds, default 300 seconds).
- **Decay Half Life Unreachable**—Specify the length of time after which a route's stability metric is halved if the route is considered unreachable (range 0-3600 seconds, default 300 seconds).

Click the icon to delete a profile.

Graceful Restart

Configure the following settings:

- **Enable**—Activate the graceful restart option.
- **Stale Route Time**—Specify the length of time that a route can stay in the stale state (range 1-3600 seconds, default 120 seconds).
- **Local Restart Time**—Specify the length of time that the local device takes to restart. This value is advertised to peers (range 1-3600 seconds, default 120 seconds).
- **Max Peer Restart Time**—Specify the maximum length of time that the local device accepts as a grace period restart time for peer devices (range 1-3600 seconds, default 120 seconds).

Path Selection

Configure the following settings:

- **Always Compare MED**—Enable MED comparison for paths from neighbors in different autonomous systems.
- **Deterministic MED comparison**—Enable MED comparison to choose between routes that are advertised by IBGP peers (BGP peers in the same autonomous system).

AS Format

Select the **2-byte** (default) or **4-byte** format. This setting is configurable for interoperability purposes.

---

**Table 48. Virtual Router Settings - BGP Tab (Continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Dampening Profiles | Settings include:  
- **Profile Name**—Enter a name to identify the profile.  
- **Enable**—Activate the profile.  
- **Cutoff**—Specify a route withdrawal threshold above which a route advertisement is suppressed (range 0.0-1000.0, default 1.25).  
- **Reuse**—Specify a route withdrawal threshold below which a suppressed route is used again (range 0.0-1000.0, default .5).  
- **Max. Hold Time**—Specify the maximum length of time that a route can be suppressed, regardless of how unstable it has been (range 0-3600 seconds, default 900 seconds).  
- **Decay Half Life Reachable**—Specify the length of time after which a route's stability metric is halved if the route is considered reachable (range 0-3600 seconds, default 300 seconds).  
- **Decay Half Life Unreachable**—Specify the length of time after which a route's stability metric is halved if the route is considered unreachable (range 0-3600 seconds, default 300 seconds). |
| Graceful Restart | ![General > Show Advanced]  
Configure the following settings:  
- **Enable**—Activate the graceful restart option.  
- **Stale Route Time**—Specify the length of time that a route can stay in the stale state (range 1-3600 seconds, default 120 seconds).  
- **Local Restart Time**—Specify the length of time that the local device takes to restart. This value is advertised to peers (range 1-3600 seconds, default 120 seconds).  
- **Max Peer Restart Time**—Specify the maximum length of time that the local device accepts as a grace period restart time for peer devices (range 1-3600 seconds, default 120 seconds). |
| Path Selection   | ![General > Show Advanced]  
Configure the following settings:  
- **Always Compare MED**—Enable MED comparison for paths from neighbors in different autonomous systems.  
- **Deterministic MED comparison**—Enable MED comparison to choose between routes that are advertised by IBGP peers (BGP peers in the same autonomous system). |
| AS Format        | ![General > Show Advanced]  
Select the **2-byte** (default) or **4-byte** format. This setting is configurable for interoperability purposes. |
### Table 48. Virtual Router Settings - BGP Tab (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Peer Group/Peer Tab</strong></td>
<td>To add a new group, click <strong>New</strong> and configure the following settings:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>—Enter a name to identify the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong>—Select to activate the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>—Specify the type of peer or group and configure the associated</td>
</tr>
<tr>
<td></td>
<td>settings.</td>
</tr>
<tr>
<td></td>
<td>- <strong>IBGP</strong>—Specify an option for <strong>Next Hop</strong>:</td>
</tr>
<tr>
<td></td>
<td>• <strong>original</strong>—Use the Next Hop address provided in the original route</td>
</tr>
<tr>
<td></td>
<td>advertisement.</td>
</tr>
<tr>
<td></td>
<td>• <strong>use-self</strong>—Replace the Next Hop address with this router’s IP</td>
</tr>
<tr>
<td></td>
<td>address to ensure that it will be in the forwarding path.</td>
</tr>
<tr>
<td></td>
<td>- <strong>EBGP</strong>—Specify options for <strong>Next Hop Import</strong>, <strong>Next Hop Export</strong>.</td>
</tr>
<tr>
<td></td>
<td>Select the <strong>Remove Private AS</strong> check box if you want to force BGP to</td>
</tr>
<tr>
<td></td>
<td>remove private AS numbers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>resolve</strong>—Resolve the Next Hop address using the local forwarding</td>
</tr>
<tr>
<td></td>
<td>table.</td>
</tr>
<tr>
<td></td>
<td>• <strong>use-self</strong>—Replace the Next Hop address with this router’s IP</td>
</tr>
<tr>
<td></td>
<td>address to ensure that it will be in the forwarding path.</td>
</tr>
<tr>
<td></td>
<td>• <strong>original</strong>—Use the Next Hop address provided in the original route</td>
</tr>
<tr>
<td></td>
<td>advertisement.</td>
</tr>
<tr>
<td></td>
<td>• <strong>use-peer</strong>—Use the peer’s IP address as the Next Hop address.</td>
</tr>
<tr>
<td></td>
<td>- <strong>IBGP-Confed</strong>—Specify an option for <strong>Next Hop Export</strong>:</td>
</tr>
<tr>
<td></td>
<td>• <strong>original</strong>—Use the Next Hop address provided in the original route</td>
</tr>
<tr>
<td></td>
<td>advertisement.</td>
</tr>
<tr>
<td></td>
<td>• <strong>use-self</strong>—Replace the Next Hop address with this router’s IP</td>
</tr>
<tr>
<td></td>
<td>address to ensure that it will be in the forwarding path.</td>
</tr>
<tr>
<td></td>
<td>- <strong>EBGP-Confed</strong>—Specify an option for <strong>Next Hop Export</strong>:</td>
</tr>
<tr>
<td></td>
<td>• <strong>original</strong>—Use the Next Hop address provided in the original route</td>
</tr>
<tr>
<td></td>
<td>advertisement.</td>
</tr>
<tr>
<td></td>
<td>• <strong>use-self</strong>—Replace the Next Hop address with this router’s IP</td>
</tr>
<tr>
<td></td>
<td>address to ensure that it will be in the forwarding path.</td>
</tr>
</tbody>
</table>
### About Virtual Routers and Routing Protocols

To add a new peer, click **New** and configure the following settings:

- **Name** — Enter a name to identify the peer.
- **Enable** — Select to activate the peer.
- **Peer AS** — Specify the AS of the peer.
- **Local Address** — Choose a firewall interface and local IP address.
- **Connection Options** — Specify the following options:
  - **Passive Connection** — Select to prevent the router from trying to establish a new connection.
  - **Auth Profile** — Select the profile.
  - **Keep Alive Interval** — Specify an interval after which routes from a peer are suppressed according to the hold time setting (range 0-1200 seconds or “disabled”, default 30 seconds).
  - **Multi Hop** — Set the time-to-live (TTL) value in the IP header (range 1-255, default 0). The default value of 0 means 2 for eBGP and 255 for iBGP.
  - **Open Delay Time** — Specify the delay time between opening the peer TCP connection and sending the first BGP open message (range 0-240 seconds, default 0 seconds).
  - **Hold Time** — Specify the period of time that may elapse between successive KEEPALIVE or UPDATE messages from a peer before the peer connection is closed. (range 3-3600 seconds or “disabled”, default 90 seconds).
  - **Idle Hold Time** — Specify the time to wait in the idle state before retrying connection to the peer (range 1-3600 seconds, default 15 seconds).
- **Peer Address** — Specify the IP address and port of the peer.
- **Advanced Options** — Configure the following settings:
  - **Reflector Client** — Select the type of reflector client (Non-Client, Client, or Meshed Client). Routes that are received from reflector clients are shared with all internal and external BGP peers.
  - **Aggregated Confed AS Path** — Select the check box to include a path to the configured aggregated confederation AS.
  - **Max. Prefixes** — Specify the maximum number of supported IP prefixes (1 - 100000 or unlimited).
  - **Soft Reset With Stored Info** — Select the check box to perform a soft reset of the firewall after updating the peer settings.

Click the ✗ icon to delete a group.

---

#### Table 48. Virtual Router Settings - BGP Tab (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peers Subtab</td>
<td>To add a new peer, click <strong>New</strong> and configure the following settings:</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name to identify the peer.</td>
</tr>
<tr>
<td><strong>Enable</strong></td>
<td>Select to activate the peer.</td>
</tr>
<tr>
<td><strong>Peer AS</strong></td>
<td>Specify the AS of the peer.</td>
</tr>
<tr>
<td><strong>Local Address</strong></td>
<td>Choose a firewall interface and local IP address.</td>
</tr>
<tr>
<td><strong>Connection Options</strong></td>
<td>Specify the following options:</td>
</tr>
<tr>
<td><strong>Passive Connection</strong></td>
<td>Select to prevent the router from trying to establish a new connection.</td>
</tr>
<tr>
<td><strong>Auth Profile</strong></td>
<td>Select the profile.</td>
</tr>
<tr>
<td><strong>Keep Alive Interval</strong></td>
<td>Specify an interval after which routes from a peer are suppressed according to the hold time setting (range 0-1200 seconds or “disabled”, default 30 seconds).</td>
</tr>
<tr>
<td><strong>Multi Hop</strong></td>
<td>Set the time-to-live (TTL) value in the IP header (range 1-255, default 0). The default value of 0 means 2 for eBGP and 255 for iBGP.</td>
</tr>
<tr>
<td><strong>Open Delay Time</strong></td>
<td>Specify the delay time between opening the peer TCP connection and sending the first BGP open message (range 0-240 seconds, default 0 seconds).</td>
</tr>
<tr>
<td><strong>Hold Time</strong></td>
<td>Specify the period of time that may elapse between successive KEEPALIVE or UPDATE messages from a peer before the peer connection is closed. (range 3-3600 seconds or “disabled”, default 90 seconds).</td>
</tr>
<tr>
<td><strong>Idle Hold Time</strong></td>
<td>Specify the time to wait in the idle state before retrying connection to the peer (range 1-3600 seconds, default 15 seconds).</td>
</tr>
<tr>
<td><strong>Peer Address</strong></td>
<td>Specify the IP address and port of the peer.</td>
</tr>
<tr>
<td><strong>Advanced Options</strong></td>
<td>Configure the following settings:</td>
</tr>
<tr>
<td><strong>Reflector Client</strong></td>
<td>Select the type of reflector client (Non-Client, Client, or Meshed Client). Routes that are received from reflector clients are shared with all internal and external BGP peers.</td>
</tr>
<tr>
<td><strong>Aggregated Confed AS Path</strong></td>
<td>Select the check box to include a path to the configured aggregated confederation AS.</td>
</tr>
<tr>
<td><strong>Max. Prefixes</strong></td>
<td>Specify the maximum number of supported IP prefixes (1 - 100000 or unlimited).</td>
</tr>
<tr>
<td><strong>Soft Reset With Stored Info</strong></td>
<td>Select the check box to perform a soft reset of the firewall after updating the peer settings.</td>
</tr>
</tbody>
</table>
Table 48. Virtual Router Settings - BGP Tab (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import Rules/Export</strong></td>
<td><strong>Rules Tabs</strong></td>
</tr>
<tr>
<td>Import Rules/Export</td>
<td>Click the BGP Import Rules or Export Rules subtab. To add a new rule,</td>
</tr>
<tr>
<td>Rules</td>
<td>click New and configure the following settings.</td>
</tr>
<tr>
<td></td>
<td>• General area:</td>
</tr>
<tr>
<td></td>
<td>– Name—Specify a name to identify the rule.</td>
</tr>
<tr>
<td></td>
<td>– Enable—Select to activate the rule.</td>
</tr>
<tr>
<td></td>
<td>– Used by—Select the peer groups that will use this rule.</td>
</tr>
<tr>
<td></td>
<td>• Match area:</td>
</tr>
<tr>
<td></td>
<td>– AS-Path Regular Expression—Specify a regular expression for</td>
</tr>
<tr>
<td></td>
<td>filtering of AS paths.</td>
</tr>
<tr>
<td></td>
<td>– Community Regular Expression—Specify a regular expression for</td>
</tr>
<tr>
<td></td>
<td>filtering of community strings.</td>
</tr>
<tr>
<td></td>
<td>– Extended Community Regular Expression—Specify a regular expression for</td>
</tr>
<tr>
<td></td>
<td>filtering of extended community strings.</td>
</tr>
<tr>
<td></td>
<td>– Address Prefix—Specify IP addresses or prefixes for route filtering.</td>
</tr>
<tr>
<td></td>
<td>– MED—Specify a MED value for route filtering.</td>
</tr>
<tr>
<td></td>
<td>– Next Hop—Specify next hop routers or subnets for route filtering.</td>
</tr>
<tr>
<td></td>
<td>– From Peer—Specify peer routers for route filtering.</td>
</tr>
<tr>
<td></td>
<td>• Action area:</td>
</tr>
<tr>
<td></td>
<td>– Action—Specify an action (Allow or Deny) to take when the match</td>
</tr>
<tr>
<td></td>
<td>conditions are met.</td>
</tr>
<tr>
<td></td>
<td>– Local Preference—Specify a local preference metric, only if the action</td>
</tr>
<tr>
<td></td>
<td>is Allow.</td>
</tr>
<tr>
<td></td>
<td>– MED—Specify a MED value, only if the action is Allow (0-65535).</td>
</tr>
<tr>
<td></td>
<td>– Weight—Specify a weight value, only if the action is Allow (0-65535).</td>
</tr>
<tr>
<td></td>
<td>– Next Hop—Specify a next hop router, only if the action is Allow.</td>
</tr>
<tr>
<td></td>
<td>– Origin—Specify the path type of the originating route: IGP, EGP, or</td>
</tr>
<tr>
<td></td>
<td>incomplete, only if the action is Allow.</td>
</tr>
<tr>
<td></td>
<td>– AS Path Limit—Specify an AS path limit, only if the action is Allow.</td>
</tr>
<tr>
<td></td>
<td>– AS Path—Specify an AS path: None, Remove, Prepend, Remove and Prepend,</td>
</tr>
<tr>
<td></td>
<td>only if the action is Allow.</td>
</tr>
<tr>
<td></td>
<td>– Community—Specify a community option: None, Remove All, Remove Regex,</td>
</tr>
<tr>
<td></td>
<td>Append, or Overwrite, only if the action is Allow.</td>
</tr>
<tr>
<td></td>
<td>– Extended Community—Specify a community option: None, Remove All, Remove</td>
</tr>
<tr>
<td></td>
<td>Regex, Append, or Overwrite, only if the action is Allow.</td>
</tr>
<tr>
<td></td>
<td>– Dampening—Specify the dampening parameter, only if the action is</td>
</tr>
<tr>
<td></td>
<td>Allow.</td>
</tr>
<tr>
<td></td>
<td>Click the icon to delete a group. Click Clone to add a new group with</td>
</tr>
<tr>
<td></td>
<td>the same settings as the selected group. A suffix is added to the new</td>
</tr>
<tr>
<td></td>
<td>group name to distinguish it from the original group.</td>
</tr>
</tbody>
</table>
### Displaying Runtime Statistics for Virtual Routers

**Network > Virtual Routers**

Detailed runtime statistics are available for the virtual router and dynamic routing protocols from the Virtual Routers page. Click the More Runtime Stats link to open a new window that contains the routing table as well as routing protocol-specific details. For an overview of virtual routers, refer to “About Virtual Routers and Routing Protocols” on page 98.

### About DHCP Options

**Network > DHCP**

The firewall supports the selection of DHCP servers or DHCP relay for IP address assignment on the Layer 3 interfaces. Multiple DHCP servers are supported. Client requests can be forwarded to all servers, with the first server response sent back to the client.

The DHCP assignment also works across an IPSec VPN, allowing clients to receive an IP address assignment from a DHCP server on the remote end of an IPSec tunnel. For information on IPSec VPN tunnels, refer to “Configuring IPSec Tunnels” on page 189.

Use this page to specify DHCP servers or DHCP relay for IP address assignment on the Layer 3 interfaces. You can specify multiple DHCP servers and configure them so that client requests are forwarded to all servers, with the first server response sent back to the client.
To configure DHCP settings, click New and specify the following information.

**Table 49. DHCP Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Select the firewall interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of DHCP request.</td>
</tr>
<tr>
<td>Mode</td>
<td>Select whether the settings on this page and enabled, disabled, or have</td>
</tr>
<tr>
<td></td>
<td>use determined automatically.</td>
</tr>
<tr>
<td>Lease</td>
<td>Enter any limitations on the DHCP lease interval. You can enter days, hours,</td>
</tr>
<tr>
<td></td>
<td>or minutes. For example, if you enter only hours, then the lease is</td>
</tr>
<tr>
<td></td>
<td>restricted to that number of hours.</td>
</tr>
<tr>
<td>Preferred DNS</td>
<td>Enter the IP address of the preferred and alternate Domain Name Service</td>
</tr>
<tr>
<td>Alternate DNS</td>
<td>(DNS) servers. The alternate server address is optional.</td>
</tr>
<tr>
<td>Preferred WINS</td>
<td>Enter the IP address of the preferred and alternate Windows Internet</td>
</tr>
<tr>
<td>Alternate WINS</td>
<td>Naming Service (WINS) servers. The alternate server address is optional.</td>
</tr>
<tr>
<td>Preferred NIS</td>
<td>Enter the IP address of the preferred and alternate Network Information</td>
</tr>
<tr>
<td>Alternate NIS</td>
<td>Service (NIS) servers. The alternate server address is optional.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Enter the IP address of the network gateway that is used to reach the</td>
</tr>
<tr>
<td></td>
<td>DHCP servers.</td>
</tr>
<tr>
<td>POP3 Server</td>
<td>Enter the IP address of the Post Office Protocol (POP3) server.</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>Enter the IP address of the Simple Mail Transfer Protocol (SMTP) server.</td>
</tr>
<tr>
<td>IP Pools</td>
<td>Specify the range of IP addresses to which this DHCP configuration applies</td>
</tr>
<tr>
<td></td>
<td>and click <strong>Add</strong>. You can enter an IP subnet and subnet mask (for example,</td>
</tr>
<tr>
<td></td>
<td>192.168.1.0/24) or a range of IP addresses (for example, 192.168.1.10-192.</td>
</tr>
<tr>
<td></td>
<td>168.1.20). Add multiple entries to specify multiple IP address pools.</td>
</tr>
<tr>
<td></td>
<td>To edit an existing entry, click <strong>Edit</strong>, make the changes, and click</td>
</tr>
<tr>
<td></td>
<td><strong>Done</strong>. To delete an entry, click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Reserved</td>
<td>Enter the IP address (format x.x.x.x) or MAC address (format xxxxxxxxxx:xx:xx) of any devices that you do not want to subject to DHCP address assignment.</td>
</tr>
<tr>
<td>Addresses</td>
<td>To edit an existing entry, click <strong>Edit</strong>, make the changes, and click <strong>Done</strong>. To delete an entry, click <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you leave this area blank, there will be no restrictions on the IP ranges.</td>
</tr>
<tr>
<td>Reserved</td>
<td>Enter the IP address (format x.x.x.x) or MAC address (format xxxxxxxxxx:xx:xx) of any devices that you do not want to subject to DHCP address assignment.</td>
</tr>
<tr>
<td>Addresses</td>
<td>To edit an existing entry, click <strong>Edit</strong>, make the changes, and click <strong>Done</strong>. To delete an entry, click <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you leave this area blank, then there will be no reserved IP addresses.</td>
</tr>
</tbody>
</table>
About VLAN Support

Network > VLANs

The firewall supports VLANs that conform to the IEEE 802.1Q standard. Each Layer 2 interface that is defined on the firewall must be associated with a VLAN. The same VLAN can be assigned to multiple Layer 2 interfaces, but each interface can belong to only one VLAN. Optionally, a VLAN can also specify a VLAN interface that can route traffic to Layer 3 destinations outside the VLAN.

Each Layer 2 interface defined on the firewall must be associated with a VLAN. The same VLAN can be assigned to multiple Layer 2 interfaces, but each interface can belong to only one VLAN. Optionally, a VLAN can also specify a VLAN interface that can route traffic to Layer 3 destinations outside the VLAN.

Table 50. VLAN Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dot1q VLAN Name</td>
<td>Enter a VLAN name (up to 31 characters). This name appears in the list of VLANs when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Select the interfaces from the displayed list that you want to include in the VLAN. Interfaces are listed here only if they have the Layer 2 interface type and have not been assigned to another VLAN. To specify the interface type, refer to “About Firewall Interfaces” on page 85.</td>
</tr>
<tr>
<td>VLAN Interface</td>
<td>Select a VLAN interface to allow traffic to be routed outside the VLAN. To define a VLAN interface, refer to “Configuring VLAN Interfaces” on page 93.</td>
</tr>
<tr>
<td>L3 Forwarding Enabled</td>
<td>If you select a VLAN interface, you can select the check box to enable Layer 3 routing over the selected interface.</td>
</tr>
</tbody>
</table>

About Network Profiles

Network profiles capture configuration information that the firewall can use to establish network connections and implement policies. The following types of network profiles are supported:

- **IKE gateways, IPSec crypto, IKE crypto, and tunnel monitor profiles**—These profiles support configuration and operation of IPSec VPNs. For information on the following profile types, refer to “Configuring IPSec Tunnels” on page 189.
  - IKE gateways include the configuration information that is necessary to perform IKE protocol negotiation with peer gateways when setting up IPSec VPN tunnels.
  - IKE crypto profiles specify the protocols and algorithms for Phase 1 identification, authentication, and encryption in VPN tunnels.
  - IPSec crypto profiles specify the protocols and algorithms for Phase 2 identification, authentication, and encryption in VPN tunnels.
  - Tunnel monitor profiles specify how the firewall monitors IPSec tunnels and the actions that are taken if the tunnel is not available.
About Network Profiles

- **Interface management profiles**—These profiles specify the protocols that can be used to manage the firewall for Layer 3 interface, including VLAN and loopback interfaces. Refer to “Defining Interface Management Profiles” on page 114.

- **Zone protection profiles**—These profiles determine how the firewall responds to attacks from individual security zones. Refer to “Defining Zone Protection Profiles” on page 115. The following types of protection are supported:
  - **Flood Protection**—Protects against SYN, ICMP, UDP, and other IP-based flooding attacks.
  - **Reconnaissance detection**—Allows you to detect and block commonly used port scans and IP address sweeps that attackers run to find potential attack targets.
  - **Packet-based attack protection**—Protects against large ICMP packets and ICMP fragment attacks.

- **QoS profiles**—These profiles determine how the QoS traffic classes are treated. You can set overall limits on bandwidth regardless of class and also set limits for individual classes. You can also assign priorities to different classes. Priorities determine how traffic is treated in the presence of contention. Refer to “Defining QoS Profiles” on page 214.

### Defining Interface Management Profiles

► *Network > Network Profiles > Interface Mgmt*

Use this page to specify the protocols that are used to manage the firewall. To assign management profiles to each interface, refer to “Configuring Layer 3 Interfaces” on page 88 and “Configuring Layer 3 Subinterfaces” on page 90.

To define interface management profiles, click New and specify the following information. For an overview of firewall interfaces, refer to “About Firewall Interfaces” on page 85.

**Table 51. Interface Management Profile Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a profile name (up to 31 characters). This name appears in the list of interface management profiles when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Ping</td>
<td>Select the check box for each service to be enabled on the interfaces where the profile is applied.</td>
</tr>
<tr>
<td>Telnet</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td>Permitted IP</td>
<td>Enter the IP addresses of any external servers that are used to manage the firewall (in-band management) through the data port.</td>
</tr>
</tbody>
</table>
About Network Profiles

Defining Zone Protection Profiles

- **Network > Network Profiles > Zone Protection**

Use this page to determine how the firewall responds to attacks from specified security zones. The same profile can be assigned to multiple zones. For an overview of security zones, refer to “About Security Zones” on page 97.

To define zone protection profiles, click **New** and specify the following information.

**Table 52. Zone Protection Profile Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a profile name (up to 31 characters). This name appears in the list of zone protection profiles when configuring zones. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, and underscores.</td>
</tr>
</tbody>
</table>

**Flood Protection Thresholds - SYN Flood**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Action | Select the action to take in response to a SYN flood attack.  
- **Random Early Drop**—Causes SYN packets to be dropped to mitigate a flood attack:  
  - When the flow exceeds the **Alert** threshold, an alert is generated.  
  - When the flow exceeds the **Activate** threshold, individual SYN packets are dropped randomly to restrict the flow.  
  - When the flow exceeds the **Maximum** threshold, all packets are dropped.  
- **SYN cookies**—Computes a sequence number for SYN-ACK packets that does not require pending connections to be stored in memory. This is the preferred method. |
| Alert | Enter the number of SYN packets received per second for the same destination that triggers an attack alarm. Alarms can be viewed on the Dashboard (refer to “Using the Dashboard” on page 162) and in the threat log (refer to “Identifying Unknown Applications and Taking Action” on page 185).  
Alarms can also generate SNMP traps and syslog messages (refer to “Defining SNMP Trap Destinations” on page 63 and “Defining Syslog Servers” on page 64). |
| Activate | Enter the number of SYN packets received per second for the same destination that causes subsequent ICMP packets to be dropped.  
Metering stops when the number of ICMP packets drops below the threshold. |
| Maximum | Enter the maximum number of SYN packets able to be received per second. Any number of packets exceeding the maximum will be dropped. |

**Flood Protection Thresholds - ICMP Flood**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Enter the number of ICMP echo requests (pings) received per second that triggers an attack alarm.</td>
</tr>
<tr>
<td>Activate</td>
<td>Enter the number of ICMP packets received per second for the same destination that causes subsequent ICMP packets to be dropped. Metering stops when the number of ICMP packets drops below the threshold.</td>
</tr>
</tbody>
</table>
### Table 52. Zone Protection Profile Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>Enter the maximum number of ICMP packets able to be received per second. Any number of packets exceeding the maximum will be dropped.</td>
</tr>
</tbody>
</table>

#### Flood Protection Thresholds - UDP Flood

<table>
<thead>
<tr>
<th>Alert</th>
<th>Enter the number of UDP packets received per second for the same destination that triggers an attack alarm.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate</td>
<td>Enter the number of UDP packets received per second for the same destination that triggers a response. The response is disabled when the number of UDP packets drops below the threshold.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Enter the maximum number of UDP packets able to be received per second. Any number of packets exceeding the maximum will be dropped.</td>
</tr>
</tbody>
</table>

#### Flood Protection Thresholds - Other IP Flood

<table>
<thead>
<tr>
<th>Alert</th>
<th>Enter the number of IP packets received per second for the same destination that triggers an attack alarm.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate</td>
<td>Enter the number of IP packets received per second for the same destination that triggers a response. The response is disabled when the number of IP packets drops below the threshold. Any number of packets exceeding the maximum will be dropped.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Enter the maximum number of IP packets able to be received per second. Any number of packets exceeding the maximum will be dropped.</td>
</tr>
</tbody>
</table>

#### Reconnaissance Protection - TCP Port Scan, UDP Port Scan, Host Sweep

<table>
<thead>
<tr>
<th>Interval</th>
<th>Enter the time interval for port scans and host sweep detection (seconds).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold</td>
<td>Enter the number of scanned ports within the specified time interval that will trigger this protection type (events).</td>
</tr>
<tr>
<td>Action</td>
<td>Enter the action that the system will take in response to this event type:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Allow</strong>—Permits the port scan of host sweep reconnaissance.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alert</strong>—Generates an alert for each scan or sweep that matches the threshold within the specified time interval.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Drop</strong>—Drops all further packets from the source to the destination for the remainder of the specified time interval.</td>
</tr>
</tbody>
</table>

#### Packet-Based Attack Protection

| IP address spoof        | Select the check box to enable protection against IP address spoofing.                                 |
| Block fragmented traffic| Discards fragmented IP packets.                                                                        |
| ICMP ping ID 0          | Discards packets with the ping ID 0.                                                                   |
| ICMP fragment           | Discards packets that consist of ICMP fragments.                                                       |
| ICMP large packet (>1024)| Discards ICMP packets that are larger than 1024 bytes.                                                 |
### Table 52. Zone Protection Profile Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppress ICMP TTL expired error</td>
<td>Does not display expired ICMP time-to-live (TTL) errors.</td>
</tr>
<tr>
<td>Suppress ICMP NEEDFRAG</td>
<td>Does not display information about ICMP need-to-fragment packets.</td>
</tr>
<tr>
<td>Reject non-SYN TCP Packet</td>
<td>Determines whether to reject the packet, if the first packet for the TCP session setup is not a SYN packet:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Global</strong>—Use system-wide setting that is assigned through the CLI.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Yes</strong>—Reject non-SYN TCP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No</strong>—Accept non-SYN TCP.</td>
</tr>
</tbody>
</table>
This chapter describes how to configure security policies and profiles:

- “About Policies” in the next section
- “About Security Profiles” on page 132
- “About Other Policy Objects” on page 141

### About Policies

Policies allow you to control firewall operation by enforcing rules and automatically taking action. The following types of policies are supported:

- Basic security policies to block or allow a network session based on the application, the source and destination zones and addresses, and optionally the service (port and protocol). Zones identify the physical or logical interfaces that send or receive the traffic. Refer to “About Security Policies” on page 122.

- Network Address Translation (NAT) policies to translate addresses and ports, as needed. Refer to “About NAT Policies” on page 125.

- Policy-based forwarding policies to determine the egress interface used following processing. Refer to “About Policy-Based Forwarding Policies” on page 128.

- SSL Decryption policies to specify SSL traffic decryption for security policies. Each policy can specify the categories of URLs for the traffic you want to decrypt. Refer to “About SSL Decryption Policies” on page 129.

- Application override policies to override the application definitions provided by the firewall. Refer to “About Application Override Policies” on page 131.

- Captive portal policies to request authentication of unidentified users. Refer to “About Captive Portal Policies” on page 132.

*Note: Shared policies pushed from Panorama are shown in green on the firewall web interface pages and cannot be edited at the device level.*
Guidelines on Defining Policies

For general guidelines on interacting with the firewall interface, refer to “Using the Firewall Interface” on page 19. The following specific guidelines apply when interacting with the pages on the Policies tab:

- To view just the rules for specific zones, select zones from the **Source Zone** and **Destination Zone** drop-down lists at the top of the page, and click **Filter by Zone**.

- To apply a filter to the list, select from the **Filter Rules** drop-down list.

- To add a new policy rule, do one of the following:
  - Click **Add Rule** at the bottom of the page. A new rule with the default settings is added to the bottom of the list, and given the next rule number. The source and destination zones must be for the same type of interfaces (Layer 2, Layer 3, or virtual wire). To define new zones, refer to “Defining Security Zones” on page 97.
  
  - Right-click on the number of a rule you want to copy, and select **Clone Rule**, or select a rule by clicking the white space of the rule, and select **Clone Rule** at the bottom of the page (a selected rule has a yellow background). The copied rule is inserted below the selected rule, and the subsequent rules are renumbered.

- To delete, disable, or move a rule up or down in the list, right-click on the rule number and select the appropriate action, or click the white space of a rule and select the action at the bottom of the page. Note that for disabled rules, the rule is grayed out and the **Disable Rule** option is changed to **Enable Rule**.
To specify source or destination addresses, click the address entry to open the pop-up window. Choose select and do any of the following:

- Select the check box next to the appropriate addresses and/or address groups in the Available column, and click Add to add your selections to the Selected column.

- Enter the first few characters of a name in the Search field to show the addresses and address groups that start with those characters. Selecting an item in the list will set the check box in the Available column. Repeat this process as often as needed, and then click Add.

- Enter one or more IP addresses (one per line), with or without a network mask. The general format is: `ip_address/mask`

- To remove source or destination addresses, select the appropriate check boxes in the Selected column and click Remove, or select any to clear all addresses and address groups.

- To disable source or destination addresses without removing them, click Negate. A line is drawn through each address and group on the SSL Decryption Rules page, which applies the rule to all addresses (same effect as any).

- To add new addresses that can be used in the current or other policies, click New Address (refer to “Defining Applications” on page 148). To define new address groups, refer to “Defining Address Groups” on page 143.

To specify source or destination users for a policy, click the user entry to open the pop-up window. Choose select and do any of the following:

- Select the check box next to the appropriate user or user group in the Available column, and click Add to add your selections to the Selected column.

- Enter the first few characters of a name in the Search field to list all users and user groups that start with those characters. Selecting an item in the list sets the check box in the Available column. Repeat this process as often as needed, and then click Add.

- To remove users or user groups, select the appropriate check boxes in the Selected column and click Remove, or select any to clear all users.

To select applications for the security rule, click the application entry to open the pop-up. The default of any should be used only in rules that specify the deny (block) action. To select specific applications, choose Select and do any of the following:

- To select according to the columns at the top of the page, click an entry in a column to display check boxes, and then select the check boxes. The filtering is successive: first category filters are applied, then sub category filters, then technology filters, then risk,
About Policies

filters, and finally characteristic filters. For a description of the choices in each column, refer to “Application Categories, Subcategories, Technologies, and Characteristics” on page 239.

– Enter the first few characters of a name in the Search field to list all applications, categories, and groups that start with those characters. Selecting an item in the list will set the check box in the Available column. Repeat this process as often as needed, and then click Add.

– Select a filter from the Filters drop-down list and click Add Filter.

– Select a group from the Groups drop-down list and click Add Group.

– Each time you make a selection the list of applications on the page is updated. When you have finished selecting applications, click OK.

– To define new applications, refer to “Defining Applications” on page 148. To define application groups, refer to “Defining Application Groups” on page 150.

– To select specific services for a policy, click the service entry to open the pop-up window. Choose Select and do any of the following:

  – Select the check box next to the appropriate services and/or service groups in the Available column, and click Add to add your selections to the Selected column.

  – Enter the first few characters of a name in the Search field to list all services and groups that start with those characters. Selecting an item in the list will set the check box in the Available column. Repeat this process as often as needed, and then click Add.

  – To remove services, clear the appropriate check boxes in the Selected column and click Remove, or select any to clear all individual services and groups.

  – To define new services, click New Service (refer to “Defining Services” on page 152). To define new service groups, refer to “Defining Service Groups” on page 153.

About Security Policies

Security policies can specify whether to block or allow a new network session based on traffic attributes, such as the application, source and destination security zones, the source and destination addresses, and the application service (such as HTTP). Security zones are used to group interfaces according to the relative risk of the traffic they carry. For example, an interface connected to the Internet is in an “untrusted” zone, while an interface connected to the internal network is in a “trusted” zone.

Note: By default, traffic between each pair of security zones is blocked until at least one rule is added to allow traffic between the two zones.

Intra-zone traffic is permitted by default and requires an explicit block rule.
Security policies can be as general or specific as needed. The policy rules are compared against the incoming traffic in sequence, and because the first rule that matches the traffic is applied, the more specific rules must precede the more general ones. For example, a rule for a single application must precede a rule for all applications if all other traffic-related settings are the same. If the traffic does not match any of the rules, the traffic is blocked.

**Defining Security Policies**

Use the Security page to determine whether to allow or block network session based on specified traffic attributes. After creating a new rule, configure the rule by clicking the current field values and specifying the appropriate information, as described in the following table. For configuration guidelines, refer to “Guidelines on Defining Policies” on page 120.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Change the default rule name and/or enter a rule description.</td>
</tr>
<tr>
<td>Source Zone</td>
<td>Select one or more source and destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to “Defining Security Zones” on page 97. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.</td>
</tr>
<tr>
<td>Destination Zone</td>
<td>Select one or more source and destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to “Defining Security Zones” on page 97. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Select the source and destination IPv4 or IPv6 addresses for which the security rule applies.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Select the source and destination IPv4 or IPv6 addresses for which the security rule applies.</td>
</tr>
<tr>
<td>Source User</td>
<td>Select the source users or groups of users subject to this policy.</td>
</tr>
<tr>
<td>Application</td>
<td>Select specific applications for the security rule. To define new applications, refer to “Defining Applications” on page 148. To define application groups, refer to “Defining Application Groups” on page 150. If an application has multiple functions, you can select the overall application or individual functions. If you select the overall application, all functions are included, and the application definition is automatically updated as future functions are added.</td>
</tr>
</tbody>
</table>
| Service            | Select services to limit the applications to specific TCP and/or UDP port numbers. You can select specific services and service groups, or one of the following:  
  • any—The selected applications are allowed or denied on any protocol or port. Use of “any” is recommended on deny policies.  
  • application-default—The selected applications are allowed or denied only on the default ports defined by Palo Alto Networks. Use of “application-default” is recommended on allow policies. Do not use for applications that are user-defined The predefined services (service-http and service-https) can be used to force applications to run over ports that are more easily forwarded to other security or control devices, such as web proxies. |
| Action             | Click allow or deny to allow or block a new network session for traffic that matches this rule. |
### Table 53. Security Policy Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>To specify the checking done by the default security profiles, select individual antivirus, anti-spyware, vulnerability protection, URL filtering, data filtering, and/or file blocking profiles. To specify a profile group, rather than individual profiles, select <strong>Profile Groups</strong> and select a profile group from the <strong>Group</strong> drop-down list. To define new profiles or profile groups, click <strong>New</strong> next to the appropriate profile or group (refer to “About Security Profile Groups” on page 158).</td>
</tr>
<tr>
<td>Options</td>
<td>Specify any combination of the following options:</td>
</tr>
<tr>
<td><strong>Log Setting</strong></td>
<td>• To generate entries in the local traffic log for traffic that matches this rule, select the following options:</td>
</tr>
<tr>
<td></td>
<td>– <strong>Send Traffic Log at session start</strong>. Generates a traffic log entry for the start of a session (disabled by default).</td>
</tr>
<tr>
<td></td>
<td>– <strong>Send Traffic Log at session end</strong>. Generates a traffic log entry for the end of a session (enabled by default).</td>
</tr>
<tr>
<td></td>
<td>If the session start or end entries are logged, “drop” and “deny” entries are also logged.</td>
</tr>
<tr>
<td></td>
<td>• To forward the local traffic log and threat log entries to remote destinations, such as Panorama and syslog servers, select a log profile from the <strong>Log Forwarding Profile</strong> drop-down list. Note that the generation of threat log entries is determined by the security profiles. To define new log profiles, click <strong>New</strong> (refer to “About Log Forwarding” on page 159).</td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
<td>To limit the days and times when the rule is in effect, select a schedule from the drop-down list. To define new schedules, click <strong>New</strong> (refer to “About Schedules” on page 160).</td>
</tr>
<tr>
<td><strong>QoS Marking</strong></td>
<td>To change the Quality of Service (QoS) setting on packets matching the rule, select <strong>IP DSCP</strong> or <strong>IP Precedence</strong> and enter the QoS value in binary or select a predefined value from the drop-down list. For more information on QoS, refer to “Configuring Quality of Service” on page 211.</td>
</tr>
<tr>
<td><strong>Disable Server Response Inspection</strong></td>
<td>To disable packet inspection from the server to the client, select this check box. This option may be useful under heavy server load conditions.</td>
</tr>
</tbody>
</table>
## About NAT Policies

If you define Layer 3 interfaces on the firewall, you can use Network Address Translation (NAT) policies to specify whether source or destination IP addresses and ports are converted between public and private addresses and ports. For example, private source addresses can be translated to public addresses on traffic sent from an internal (trusted) zone to a public (untrusted) zone.

The firewall supports the following types of address translation:

- **Dynamic IP/Port**—For outbound traffic. Multiple clients can use the same public IP addresses with different source port numbers.

  **Note:** Palo Alto Networks Dynamic IP/port NAT supports more NAT sessions than are supported by the number of available IP addresses and ports. The firewall can use IP address and port combinations up to two times (simultaneously) on the PA-2000 series, four times on the PA-4020, and eight times on the PA-4050/4060 devices when destination IP addresses are unique.

- **Dynamic IP**—For outbound traffic. Private source addresses translate to the next available address in a range.

- **Static IP**—For inbound or outbound traffic. You can use static IP to change the source or the destination IP address while leaving the source or destination port unchanged. When used to map a single public IP address to multiple private servers and services, destination ports can stay the same or be directed to different destination ports.

  **Note:** You may need to define static routes on the adjacent router and/or the firewall to ensure that traffic sent to a public IP address is routed to the appropriate private address. If the public address is the same as the firewall interface (or on the same subnet), then a static route is not required on the router for that address. When you specify service (TCP or UDP) ports for NAT, the pre-defined HTTP service (service-http) includes two TCP ports: 80 and 8080. To specify a single port, such as TCP 80, you must define a new service.

The next table summarizes the NAT types. The two dynamic methods map a range of client addresses (M) to a pool (N) of NAT addresses, where M and N are different numbers. N can also be 1. Dynamic IP/Port NAT differs from Dynamic IP NAT in that the TCP and UDP source ports are not preserved in Dynamic IP/Port, whereas they are unchanged with Dynamic IP NAT. There are also differing limits to the size of the translated IP pool, as noted below.

With Static IP NAT, there is a one-to-one mapping between each original address and its translated address. This can be expressed as 1-to-1 for a single mapped IP address, or M-to-M for a pool of many one-to-one, mapped IP addresses.

<table>
<thead>
<tr>
<th>PAN-OS NAT Type</th>
<th>Source Port Stays the Same</th>
<th>Destination Port Can Change</th>
<th>Mapping Type</th>
<th>Size of Translated Address Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic IP/Port</td>
<td>No</td>
<td>No</td>
<td>Many-to-1 M-to-N</td>
<td>Up to 254 consecutive addresses</td>
</tr>
<tr>
<td>Dynamic IP</td>
<td>Yes</td>
<td>No</td>
<td>M-to-N</td>
<td>Up to 16k consecutive addresses</td>
</tr>
</tbody>
</table>
About Policies

NAT Policy Examples
The following NAT policy rule translates a range of private source addresses (10.0.0.1 to 10.0.0.100) to a single public IP address (200.10.2.100) and a unique source port number (dynamic source translation). The rule applies only to traffic received on a Layer 3 interface in the “L3 trust” zone that is destined for an interface in the “L3 untrust” zone. Because the private addresses are hidden, network sessions cannot be initiated from the public network. If the public address is not a firewall interface address (or on the same subnet), the local router requires a static route to direct return traffic to the firewall.

Figure 25. Dynamic Source Address Translation

In the following example, the first NAT rule translates the private address of an internal mail server to a static public IP address. The rule applies only to outgoing email sent from the “L3 trust” zone to the “L3 untrust” zone. For traffic in the reverse direction (incoming email), the second rule translates the destination address from the server’s public address to its private address.

Figure 26. Static Source and Destination Address Translation

In both examples, if the public address is not the address of the firewall’s interface (or on the same subnet), you must add a static route to the local router to route traffic to the firewall.
Defining Network Address Translation Policies

Policies > NAT

NAT address translation rules are based on the source and destination zones, the source and destination addresses, and the application service (such as HTTP). Like security policies, the NAT policy rules are compared against the incoming traffic in sequence, and the first rule that matches the traffic is applied.

As needed, add static routes to the local router so that traffic to all public addresses is routed to the firewall. You may also need to add static routes to the receiving interface on the firewall to route traffic back to the private address (refer to “About Firewall Interfaces” on page 85). For configuration guidelines, refer to “Guidelines on Defining Policies” on page 120.

Table 55. NAT Rule Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Change the default rule name and/or enter a rule description.</td>
</tr>
<tr>
<td><strong>Original Packet</strong></td>
<td></td>
</tr>
<tr>
<td>Source Zone</td>
<td>Select one or more source and destination zones for the original (non-NAT) packet (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to “Defining Security Zones” on page 97. Multiple zones can be used to simplify management. For example, you can configure settings so that multiple internal NAT addresses are directed to the same external IP address.</td>
</tr>
<tr>
<td>Destination Zone</td>
<td></td>
</tr>
<tr>
<td><strong>Destination Interface</strong></td>
<td>Specify the type of interface (none, loopback, or vlan). Destination interface can be used to translate IP addresses differently in the case where the network is connected to two ISPs with different IP address pools.</td>
</tr>
<tr>
<td><strong>Source Address</strong></td>
<td>Specify a combination of source and destination addresses for which the source or destination address must be translated.</td>
</tr>
<tr>
<td><strong>Destination Address</strong></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Specify the services for which the source or destination address is translated. To define new service groups, refer to “Defining Service Groups” on page 153.</td>
</tr>
<tr>
<td><strong>Translated Packet</strong></td>
<td></td>
</tr>
<tr>
<td>Source Translation</td>
<td>Enter an IP address or address range (address1-address2) that the source address is translated to, and select a dynamic or static address pool. The size of the address range is limited by the type of address pool:</td>
</tr>
<tr>
<td>Dynamic IP/port</td>
<td>The next available address in the address range is used, and the source port number is changed. Up to 64K concurrent sessions are translated to the same public IP address, each with a different port number. Up to 254 consecutive IP addresses are supported. Port numbers are managed internally.</td>
</tr>
<tr>
<td>Dynamic IP</td>
<td>The next available address in the specified range is used, but the port number is unchanged. Up to 16K consecutive IP addresses are supported.</td>
</tr>
<tr>
<td>Static IP</td>
<td>The same address is always used, and the port is unchanged. For example, if the source range is 192.168.0.1-192.168.0.10 and the translation range is 10.0.0.1-10.0.0.10, address 192.168.0.2 is always translated to 10.0.0.2. The address range is virtually unlimited.</td>
</tr>
</tbody>
</table>
About Policy-Based Forwarding Policies

Normally, when traffic enters the firewall, the ingress interface virtual router dictates the route that determines the outgoing interface and destination security zone. With policy based forwarding, you can specify other information to determine the outgoing interface, including source and destination IP addresses, source and destination ports, and user ID. The initial session on a given destination IP address and port that is associated with an application will not match an application-specific rule and will be forwarded according to subsequent policy based forwarding rules (that do not specify an application) or the virtual router’s forwarding table. All subsequent sessions on that destination IP address and port for the same application will match an application-specific rule. To ensure forwarding through policy based forwarding rules, application-specific rules are not recommended.

Click New on this page to create a new rule. For configuration guidelines, refer to “Guidelines on Defining Policies” on page 120.

Table 55. NAT Rule Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Translation</td>
<td>Enter an IP address or range of IP addresses and a port number (1 to 65535) that the destination address and port number are translated to. If the port number field is blank, the destination port is not changed. Destination translation is typically used to allow an internal server, such as an email server, to be accessed from the public network.</td>
</tr>
</tbody>
</table>

Table 56. Policy-Based Forwarding Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Change the default rule name and/or enter a rule description.</td>
</tr>
<tr>
<td>Source Zone</td>
<td>Select one or more source and destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to “Defining Security Zones” on page 97.</td>
</tr>
<tr>
<td>Destination Zone</td>
<td>Select one or more source and destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to “Defining Security Zones” on page 97.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Select the source and destination addresses for the rule.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Select the source and destination addresses for the rule.</td>
</tr>
<tr>
<td>Source User</td>
<td>Select the source users or groups of users subject to this policy.</td>
</tr>
<tr>
<td>Application</td>
<td>Select specific applications for the security rule. To define new applications, refer to “Defining Applications” on page 148. To define application groups, refer to “Defining Application Groups” on page 150.</td>
</tr>
<tr>
<td>Service</td>
<td>Specify the services for which the source or destination address is translated. To define new service groups, refer to “Defining Service Groups” on page 153.</td>
</tr>
<tr>
<td>Action</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• no-pbf—Do not alter the path the packet will take.</td>
</tr>
<tr>
<td></td>
<td>• discard—Drop the packet.</td>
</tr>
<tr>
<td></td>
<td>• forward—Specify the next hop IP address and egress interface.</td>
</tr>
<tr>
<td>Forwarding</td>
<td>If the action is “forward,” the Egress I/f entry is the interface that the packet takes to get to the specified next hop.</td>
</tr>
</tbody>
</table>
Secure Socket Layer (SSL) decryption policies specify the SSL traffic to be decrypted so that security policies can be applied. Each policy specifies the categories of URLs whose traffic you want to decrypt or not decrypt.

You can configure the firewall to decrypt SSL traffic for visibility, control, and granular security. App-ID and the antivirus, vulnerability, anti-spyware, URL filtering, and file-blocking profiles are applied to decrypted traffic before it is re-encrypted as traffic exits the device. End-to-end SSL security between clients and servers is maintained, and the firewall acts as a trusted third party during the connection. No decrypted traffic leaves the device. The firewall inspects compliant SSL traffic, regardless of the protocols that are encapsulated.

Like security policies, SSL decryption policies can be as general or specific as needed. The policy rules are compared against the traffic in sequence, so the more specific rules must precede the more general ones.

Table 56. Policy-Based Forwarding Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>Specify profile actions:</td>
</tr>
<tr>
<td></td>
<td>• Wait-recover—Continue sending packets to the next hop (packets are lost if next hop goes down).</td>
</tr>
<tr>
<td></td>
<td>• Target IP Address—ICMP ping messages are sent periodically to determine the state of this policy based forwarding rule.</td>
</tr>
<tr>
<td></td>
<td>• failover—If failure occurs, any existing sessions revert to regular routing according to the virtual router at their ingress interface.</td>
</tr>
<tr>
<td></td>
<td>If Disable if unreachable is specified, this rule is ignored for all new sessions when the next hop router is unreachable.</td>
</tr>
<tr>
<td>Schedule</td>
<td>To limit the days and times when the rule is in effect, select a schedule from the drop-down list. To define new schedules, click New (refer to “About Schedules” on page 160).</td>
</tr>
</tbody>
</table>

About SSL Decryption Policies

Secure Socket Layer (SSL) decryption policies specify the SSL traffic to be decrypted so that security policies can be applied. Each policy specifies the categories of URLs whose traffic you want to decrypt or not decrypt.

You can configure the firewall to decrypt SSL traffic for visibility, control, and granular security. App-ID and the antivirus, vulnerability, anti-spyware, URL filtering, and file-blocking profiles are applied to decrypted traffic before it is re-encrypted as traffic exits the device. End-to-end SSL security between clients and servers is maintained, and the firewall acts as a trusted third party during the connection. No decrypted traffic leaves the device. The firewall inspects compliant SSL traffic, regardless of the protocols that are encapsulated.

Like security policies, SSL decryption policies can be as general or specific as needed. The policy rules are compared against the traffic in sequence, so the more specific rules must precede the more general ones.

Field Description

Note: Refer to the Palo Alto Networks Tech Note, “Controlling SSL Decryption,” for instructions on managing SSL certificates to avoid certificate mismatch errors, and “Controlling SSL Decryption” for guidelines on how to develop policies to handle non-standard SSL implementations.

Click New on this page to create a new rule. After creating a new rule, configure the rule by clicking the current field values and specifying the appropriate information, as described in the following table. For configuration guidelines, refer to “Guidelines on Defining Policies” on page 120.

Table 57. SSL Decryption Rule Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Change the default rule name and/or enter a rule description.</td>
</tr>
<tr>
<td>Source Zone</td>
<td>Select one or more source and destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to “Defining Security Zones” on page 97.</td>
</tr>
<tr>
<td>Destination Zone</td>
<td></td>
</tr>
</tbody>
</table>
You can restrict security policies to selected users or applications by clicking the user or application link on the Security or SSL Decryption device rules page. For information on restricting rules by application, refer to “Defining Applications” on page 148.

To restrict a policy to selected users, follow these steps:

1. On the Security or SSL Decryption device rules page, click the underlined link for the source or destination user to open the selection window.

   Note: If you are using a RADIUS server and not the User-ID Agent, the list of users is not displayed, and you must enter user information manually.

2. Choose the type of rule to apply:
   - any—Includes any user in the rule.
   - known-user—Includes all authenticated user.
   - unknown—Includes all unauthenticated users.
   - select—Includes selected users as determined by the selection in this window.

3. To add groups of users, select from the Available User Groups check boxes and click Add User Group. Alternatively, you can enter text to match one or more groups and click Add User Group.

4. To add individual users, enter search string in the User search field and click Find. You can then select users and click Add User. Alternatively, you can enter individual user names in the Additional Users area.

5. Click OK to save the selections and update the security or SSL decryption rule.
About Application Override Policies

To change how the firewall classifies network traffic into applications, you can specify application override policies. For example, if you want to control one of your custom applications, an application override policy can be used to identify traffic for that application according to zone, source and destination address, port, and protocol. If you have network applications that are classified as “unknown,” you can create new application definitions for them (refer to “Defining Applications” on page 148).

Like security policies, application override policies can be as general or specific as needed. The policy rules are compared against the traffic in sequence, so the more specific rules must precede the more general ones.

Custom Application Definition with Application Override

Because the App-ID engine in PAN-OS classifies traffic by identifying the application-specific content in network traffic, the custom application definition cannot simply use a port number to identify an application. The application definition must also include traffic (restricted by source zone, source IP address, destination zone, and destination IP address).

To create a custom application with application override:

1. Define the custom application, specifying the name, category, protocol numbers, port numbers, and timeout values. Refer to “Defining Applications” on page 148.

2. Define an application override policy that specifies when the custom application should be invoked. A policy typically includes the IP address of the server running the custom application and a restricted set of source IP addresses or a source zone.

Defining Application Override Policies

After creating a new rule, configure the rule by clicking the current field values and specifying the appropriate information, as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Change the default rule name and/or enter a rule description.</td>
</tr>
<tr>
<td>Source Zone</td>
<td>Select one or more source zones. Default is any. Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to “Defining Security Zones” on page 97.</td>
</tr>
<tr>
<td>Destination Zone</td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td>Specify a combination of source addresses for which the identified application can be overridden.</td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol for which the application can be overridden.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number (0 to 65535) or range of port numbers (port1-port2) for the specified source addresses. Multiple ports or ranges must be separated by commas.</td>
</tr>
<tr>
<td>Application</td>
<td>Select the override application for traffic flows that match the above rule criteria. To define new applications, click New Application (refer to “Defining Applications” on page 148).</td>
</tr>
</tbody>
</table>
About Captive Portal Policies

You can set up and customize a captive portal to direct user authentication by way of RADIUS, LDAP, or Local DB authentication. Captive portal is used in conjunction with the User-ID Agent to extend user identification functions beyond the Active Directory domain. Users are directed to the portal and authenticated, thereby creating a user-to-IP address mapping.

Defining Captive Portal Policies

> Policies > Captive Portal

Before you define captive portal policies, enable captive portal and configure captive portal settings on the User Identification page, as described in “Configuring the Firewall for User Identification” on page 35.

Click Add Rule to create new rule and add it to the list on the page. Configure the rule by clicking the current field values and specifying the appropriate information, as described in the following table.

<table>
<thead>
<tr>
<th>Table 59. Captive Portal Rule Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Source Zone</td>
</tr>
<tr>
<td>Destination Zone</td>
</tr>
<tr>
<td>Source Address</td>
</tr>
<tr>
<td>Destination Address</td>
</tr>
<tr>
<td>Method</td>
</tr>
</tbody>
</table>

About Security Profiles

Each security policy can include specification of one or more security profiles, which provide additional protection and control. You can choose from the following actions when defining security profiles:

- **Default**—Takes the default action that is specified internally for each threat.
- **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.
- **Block**—Drops the application traffic.
- **Allow**—Permits the application traffic.

You can choose from the following actions when defining threat-based policies:

- **None**—No action.
- **Default**—Takes the default action specified internally for each threat.
• **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.

• **Drop**—Drops the application traffic.

• **Drop-all-packets**—Keeps all packets from continuing past the firewall.

• **Reset-both**—Resets the client and server.

• **Reset-client**—Resets the client.

• **Reset-server**—Resets the server.

The following profile types are available:

• Antivirus profiles to protect against worms and viruses. Refer to “About Antivirus Profiles” in the next section.

• Anti-spyware profiles to block spyware downloads and attempts by spyware to access the network. Refer to “Defining Anti-Spyware Profiles” on page 134.

• Vulnerability protection profiles to stop attempts to exploit system flaws or gain unauthorized access to systems. Refer to “About Vulnerability Protection Profiles” on page 136.

• URL filtering profiles to restrict access to specific web sites and web site categories. Refer to “About URL Filtering Profiles” on page 137.

• File blocking profiles to block selected file types. Refer to “Defining File Blocking Profiles” on page 139.

• Data filtering profiles that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall. Refer to “Defining Data Filtering Profiles” on page 139.

In addition to individual profiles, you can create profile groups to combine profiles that are often applied together.

### About Antivirus Profiles

▶ **Objects > Security Profiles > Antivirus**

Each security policy can specify an antivirus profile that identifies which applications are inspected for viruses and the action taken when a virus is detected. The default profile inspects all of the listed protocol decoders for viruses, generates alerts for Simple Mail Transport Protocol (SMTP), Internet Message Access Protocol (IMAP), and Post Office Protocol Version 3 (POP3), and takes the default action for other applications (alert or deny), depending on the type of virus detected.

Customized profiles can be used to minimize antivirus inspection for traffic between trusted security zones, and to maximize the inspection of traffic received from untrusted zones, such as the Internet, as well as the traffic sent to highly sensitive destinations, such as server farms.
To define an antivirus profile, click **New** and specify the following information. For information on action types, refer to “About Security Profiles” on page 132.

### Table 60. Antivirus Profile Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a profile name (up to 31 characters). This name appears in the list of antivirus profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description.</td>
</tr>
</tbody>
</table>

**Anti-Virus Tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Capture</td>
<td>Select the check box if you want to capture identified packets.</td>
</tr>
<tr>
<td>Decoders and Actions</td>
<td>For each type of traffic that you want to inspect for viruses, select an action from the drop-down list.</td>
</tr>
<tr>
<td>Applications Exceptions</td>
<td>Identify applications that will be exceptions to the antivirus rule. For example, to block all HTTP traffic except for a specific application, you can define an antivirus profile for which the application is an exception. <strong>Block</strong> is the action for the HTTP decoder, and <strong>Allow</strong> is the exception for the application.</td>
</tr>
<tr>
<td></td>
<td>To find an application, start typing the application name in the text box. A matching list of applications is displayed, and you can make a selection. The application is added to the table, and you can assign an action. For each application exception, select the action to be taken when the threat is detected.</td>
</tr>
</tbody>
</table>

**Virus Exception Tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat ID</td>
<td>Use this tab if you want the system to ignore specific threats. Exceptions that are already specified are listed. You can add additional threats by entering the threat ID and clicking <strong>Add</strong>. Threat IDs are presented as part of the threat log information. Refer to “Viewing the Logs” on page 175.</td>
</tr>
</tbody>
</table>

### Defining Anti-Spyware Profiles

► **Objects > Security Profiles > Anti-Spyware**

Each security policy can specify an anti-spyware profile that determines the combination of methods used to combat spyware—download protection, web site blocking, and “phone home” detection (detection of traffic from installed spyware). The default anti-spyware profile provides download protection over all of the listed applications, and phone-home protection for all severity levels except the informational level.

Customized profiles can be used to minimize anti-spyware inspection for traffic between trusted security zones, and to maximize the inspection of traffic received from untrusted zones, such as the Internet, as well as the traffic sent to highly sensitive destinations, such as server farms.
To define anti-spyware profiles, click **New** and specify the following information.

**Table 61. Anti-Spyware Profile Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a profile name (up to 31 characters). This name appears in the list of anti-spyware profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter a text description of the profile.</td>
</tr>
<tr>
<td><strong>Download Protection Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Packet Capture</td>
<td>Select the check box capture spyware packets.</td>
</tr>
<tr>
<td>Decoders and Actions</td>
<td>For each type of traffic that you want to inspect for viruses, select an action from the drop-down list.</td>
</tr>
<tr>
<td>Applications Exceptions and Actions</td>
<td>Identify applications that will be exceptions to the spyware rule. For example, to block all HTTP traffic except for a specific application, you can define a spyware profile for which the application is an exception. <strong>Block</strong> is the action for the HTTP decoder, and <strong>Allow</strong> is the exception for the application. To find an application, start typing the application name in the text box. A matching list of applications is displayed, and you can make a selection. The application is added to the table, and you can assign an action. For each application exception, select the action to be taken when the threat is detected.</td>
</tr>
<tr>
<td><strong>Phone Home Protection Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>To use rule-based protection, select <strong>Simple</strong> from the <strong>Type</strong> drop-down list and select an action (<strong>None</strong>, default, <strong>Allow</strong>, <strong>Alert</strong>, or <strong>Block</strong>) for each severity level of spyware threats. To use threat-based protection, select <strong>Custom</strong> from the <strong>Type</strong> drop-down list.</td>
</tr>
<tr>
<td>Enable (Threat-based protection only)</td>
<td>Select the check box for each threat for which you want to assign an action, or select All to respond to all listed threats. The list depends on the selected host, category, and severity. If the list is empty, there are no threats for the current selections.</td>
</tr>
<tr>
<td>Actions (Threat-based protection only)</td>
<td>Choose an action from the drop-down list box, or choose from the <strong>Action</strong> drop-down at the top of the list to apply the same action to all threats.</td>
</tr>
<tr>
<td>Packet Capture</td>
<td>Select the check box to collect the traffic packets from the threat.</td>
</tr>
<tr>
<td><strong>Spyware Exception Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Threat ID</td>
<td>Use this tab if you want the system to ignore specific threats. Exceptions that are already specified are listed. You can add additional threats by entering the threat ID and clicking <strong>Add</strong>. Threat IDs are presented as part of the threat log information. Refer to “Viewing the Logs” on page 175.</td>
</tr>
</tbody>
</table>
About Vulnerability Protection Profiles

Each security policy can specify a vulnerability protection profile that determines the level of protection against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default profile protects clients and servers from all known critical, high-, and medium-severity threats.

Customized profiles can be used to minimize vulnerability checking for traffic between trusted security zones, and to maximize protection for traffic received from untrusted zones, such as the Internet, as well as the traffic sent to highly sensitive destinations, such as server farms. To apply vulnerability protection profiles to security policies, refer to “About Security Profiles” on page 132.

Note: You cannot delete a profile that is used in a security policy.

To define vulnerability protection profiles, click **New** and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a profile name (up to 31 characters). This name appears in the list of vulnerability protection profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a text description of the profile.</td>
</tr>
<tr>
<td>Shared</td>
<td>If the device is in Multiple Virtual System Mode, select this check box to allow the profile to be shared by all virtual systems.</td>
</tr>
</tbody>
</table>

**Vulnerability Tab**

- **Rule Type**
  - To use rule-based protection, select **Simple** from the Type drop-down list and select an action (**None**, **Default**, **Allow**, **Alert**, or **Block**) for each threat severity level.
  - To use threat-based protection, select **Custom** from the Type drop-down list and select threats and actions.

- **Threats**
  - Select the **Enable** check box for each threat for which you want to assign an action, or select **All** to respond to all listed threats. The list depends on the selected host, category, and severity. If the list is empty, there are no threats for the current selections.
  - Choose an action from the drop-down list box, or choose from the **Action** drop-down at the top of the list to apply the same action to all threats.

Note: The default action is shown in parentheses.

The **CVE** column shows identifiers for common vulnerabilities and exposures (CVE). These unique, common identifiers are for publicly known information security vulnerabilities.

- **Packet Capture**
  - Select the check box if you want to capture identified packets.
About Security Profiles

Each security policy can specify a URL filtering profile that blocks access to specific web sites and web site categories, or generates an alert when the specified web sites are accessed (a URL filtering license is required). You can also define a “block list” of web sites that are always blocked (or generate alerts) and an “allow list” of web sites that are always allowed. The web categories are predefined by Palo Alto Networks.

To apply URL filtering profiles to security policies, refer to “About Security Policies” on page 122. To create custom URL categories with your own lists of URLs, refer to “About Custom URL Categories” on page 155.

To define URL filtering profiles, click **New** and specify the following information.

**Table 62. Vulnerability Protection Profile Settings (Continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Exception Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Threat ID</td>
<td>Use this tab if you want the system to ignore specific threats. Exceptions that are already specified are listed. You can add additional threats by entering the threat ID and clicking <strong>Add</strong>. Threat IDs are presented as part of the threat log information. Refer to “Viewing the Logs” on page 175.</td>
</tr>
</tbody>
</table>

**About URL Filtering Profiles**

- **Objects > Security Profiles > URL Filtering**

Each security policy can specify a URL filtering profile that blocks access to specific web sites and web site categories, or generates an alert when the specified web sites are accessed (a URL filtering license is required). You can also define a “block list” of web sites that are always blocked (or generate alerts) and an “allow list” of web sites that are always allowed. The web categories are predefined by Palo Alto Networks.

To apply URL filtering profiles to security policies, refer to “About Security Policies” on page 122. To create custom URL categories with your own lists of URLs, refer to “About Custom URL Categories” on page 155.

To define URL filtering profiles, click **New** and specify the following information.

**Table 63. URL Filtering Profile Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a profile name (up to 31 characters). This name appears in the list of URL filtering profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the profile.</td>
</tr>
<tr>
<td>Shared</td>
<td>If the device is in Multiple Virtual System Mode, select this check box to allow the profile to be shared by all virtual systems.</td>
</tr>
</tbody>
</table>
| Action on License Expiration | Select the action to take if the URL filtering license expires:  
  * **Block**—Blocks access to all web sites in the block list or the selected categories.  
  * **Allow**—Allows access to all web sites.                                           |
| Enable dynamic categorization | Select to enable dynamic URL categorization. URL categorization takes advantage of a URL filtering database on the firewall that contains up to 20 million entries of the most popular URLs and other URLs for malicious categories. The BrightCloud URL filtering database has more than 100 million entries and may be able to resolve requests that the local database is unable to categorize.  
  To configure the system response when a URL remains unresolved after a 5 second timeout period, use the Category and Action settings in this window (see Category Action later in this table). Select the action for the category “Unresolved URL.” |
### About Security Profiles

#### Block List
Enter the IP addresses or URL path names of web sites that you want to block or generate alerts for (one per line). You can omit the “http[s]://” portion of the URLs. For example:

- www.ebay.com
- 198.133.219.25/en/US

**Note:** Block and allow lists support wildcard patterns. The following characters are considered separators:

. 
/ 
? 
& 
= 
; 
+

Every substring that is separated by the characters listed above is considered a token. A token can be any number of ASCII characters that does not contain any separator character or *. For example, the following patterns are valid:

- *.yahoo.com (Tokens are: "*", "yahoo" and "com")
- www.*.com (Tokens are: "www", "*" and "com")
- www.yahoo.com/search=*. (Tokens are: "www", "yahoo", "com", "search", "*"")

The following patterns are invalid because the character "*" is not the only character in the token.

- www.y*.com
- www.y*.com

---

### Table 63. URL Filtering Profile Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Block List** | Enter the IP addresses or URL path names of web sites that you want to block or generate alerts for (one per line). You can omit the “http[s]://” portion of the URLs. For example:  
- www.ebay.com  
- 198.133.219.25/en/US  

**Note:** Block and allow lists support wildcard patterns. The following characters are considered separators: . / ? & = ; +  

Every substring that is separated by the characters listed above is considered a token. A token can be any number of ASCII characters that does not contain any separator character or *. For example, the following patterns are valid:  
- *.yahoo.com (Tokens are: "*", "yahoo" and "com")  
- www.*.com (Tokens are: "www", "*" and "com")  
- www.yahoo.com/search=*. (Tokens are: "www", "yahoo", "com", "search", "*")  

The following patterns are invalid because the character "*" is not the only character in the token:  
- www.y*.com  
- www.y*.com |
| **Allow List** | Enter the IP addresses or URL path names of the web sites for which you want to allow access (one per line). This list takes precedence over the selected web site categories. The format is the same as for the block list. |
| **Category/Action** | For each category web site, select the action to take when a web site in the block list is accessed. To apply the same action to each category, select the action from the Set for all categories drop-down list.  
- **Allow**—Permit access to the web site.  
- **Block**—Block access to the web site.  
- **Continue**—Allow the user to access the blocked page by clicking Continue on the block page.  
- **Override**—Allow the user to access the blocked page after entering a password. The password and other override settings are specified in the URL Admin Override area of the Settings page. Refer to Table 26 in the “Defining the Host Name and Network Settings” on page 66.  
- **Alert**—Allow the user to access to the web site, but add an alert to the URL log. |
Defining File Blocking Profiles

Objects > Security Profiles > File Blocking

Each security policy can specify a file blocking profile that blocks selected file types from being uploaded and/or downloaded, or generates an alert when the specified file types are detected. To apply file blocking profiles to security policies, refer to “About Security Policies” on page 122.

To define file blocking profiles, click New and specify the following information.

Table 64. File Blocking Profile Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a profile name (up to 31 characters). This name appears in the list of file blocking profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
</tbody>
</table>
| Rules   | Define one or more rules to specify the action taken (if any) for the selected file types. To add a rule, specify the following and click Add:  
• Name—Enter a rule name (up to 31 characters).  
• Applications—Select the applications the rule applies to or select any.  
• File Types—Select the file types for which you want to block or generate alerts.  
• Direction—Select the direction of the file transfer (Upload, Download, or Both).  
• Action—Select the action taken when the selected file types are detected (Alert or Deny). Alerts are added to the threat log.  
The rules are processed in sequence. To change the position of a rule, select the rule and click Move Up or Move Down. To change a rule, click Edit next to the rule. To delete a rule, select the rule, and click Delete. |

Defining Data Filtering Profiles

Objects > Security Profiles > Data Filtering

You can define security policies that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall.

To apply data filtering profiles to security policies, refer to “About Security Policies” on page 122.

To define data filtering profiles, click New and specify the following information.

Table 65. Data Filtering Profile Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a profile name (up to 31 characters). This name appears in the list of log forwarding profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the profile.</td>
</tr>
</tbody>
</table>
To modify parameters for a data pattern in the list, click the item and specify information as described in the following table.

### Table 66. Data Pattern Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Applications** | Specify the applications to include in the filtering rule:  
  • Choose **any** to apply the filter to any applications with the sensitive date.  
  • Choose **Select** to specify individual applications. Select the check boxes for the applications, and click **Add** to include them in the selected list. To remove applications from the selected list, select the check boxes and click **Remove**. |
| **File Types** | Specify the file types to include in the filtering rule:  
  • Choose **any** to apply the filter to any file types that include the sensitive date.  
  • Choose **Select** to specify individual file types. Select the check boxes for the types, and click **Add** to include them in the selected list. To remove file types from the selected list, select the check boxes and click **Remove**. |
| **Direction** | Specify whether to apply the filter in the upload direction, download direction, or both. |
| **Alert Threshold** | Specify the number of times that the filter must be triggered in order to generate an alert. |
| **Block Threshold** | Specify the number of times that the filter must be triggered in order to block traffic. |
About Other Policy Objects

Policy objects are the elements that enable you to construct, schedule, and search for policies. The following element types are supported:

- Addresses and address groups to determine the scope of the policy. Refer to “About Addresses and Address Groups” in the next section.

- Applications and application groups that allow you to specify how software applications are treated in policies. Refer to “About Applications and Application Groups” on page 143.

- Application filters that allow you to simplify searches. Refer to “About Application Filters” on page 151.

- Services and service groups to limit the port numbers. Refer to “About Services and Service Groups” on page 152.

- Data patterns to define categories of sensitive information for data filtering policies. Refer to “About Data Patterns” on page 153.

- Custom URL categories that contain your own lists of URLs to include as a group in URL filtering profiles. Refer to “About Custom URL Categories” on page 155.

- Spyware and vulnerability threats to allow for detailed threat responses. Refer to “About Security Profile Groups” on page 158.

- Log forwarding to specify log settings. Refer to “About Log Forwarding” on page 159.

- Schedules to specify when policies are active. Refer to “About Schedules” on page 160.
About Addresses and Address Groups

To define security policies for specific source or destination addresses, you must first define the addresses and address ranges. Addresses requiring the same security settings can be combined into address groups that you can refer to as a unit.

Defining Address Ranges

To define security policies for specific source or destination addresses, you must first define the addresses and address ranges. Addresses requiring the same security settings can be combined into address groups to simplify policy creation (refer to “Defining Address Groups” on page 143).

To define an address range, click New and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Name</td>
<td>Enter a name that describes the addresses to be defined (up to 31 characters). This name appears in the address list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specify an IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>IPv4 address:</td>
<td>Enter the address or network using the following notation:</td>
</tr>
<tr>
<td>ip_address / mask</td>
<td>where the mask is the number of significant binary digits used for the network portion of the address.</td>
</tr>
<tr>
<td>Example:</td>
<td>“192.168.80.150/32” indicates one address, and “192.168.80.0/24” indicates all addresses from 192.168.80.0 through 192.168.80.255.</td>
</tr>
<tr>
<td>IPv6 address:</td>
<td>Enter the IPv6 address or address with prefix.</td>
</tr>
<tr>
<td>Example:</td>
<td>“2001:db8:123:1::1” or “2001:db8:123:1::/64”</td>
</tr>
<tr>
<td>IP Range</td>
<td>To specify an address range, select IP Range, and enter a range of addresses. The format is:</td>
</tr>
<tr>
<td>ip_address – ip_address</td>
<td>where each address can be IPv4 or IPv6.</td>
</tr>
</tbody>
</table>
Defining Address Groups

Objects > Address Groups

To simplify the creation of security policies, addresses requiring the same security settings can be combined into address groups.

To define address groups, click New and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Group Name</td>
<td>Enter a name that describes the address group (up to 31 characters). This name appears in the address list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>All Addresses &amp; Groups</td>
<td>Select the check box next to the addresses and/or other address groups to be included in this group.</td>
</tr>
</tbody>
</table>

About Applications and Application Groups

The Applications page lists various attributes of each application definition, such as the application’s relative security risk (1 to 5). The risk value is based on criteria such as whether the application can share files, is prone to misuse, or tries to evade firewalls. Higher values indicate higher risk.

The top application browser area of the page lists the attributes that you can use to filter the display. The number to the left of each entry represents the total number of applications with that attribute.

You can perform any of the following functions on this page:

- To apply application filters, click an item that you want to use as a basis for filtering. For example, to restrict the list to the Networking category, click Networking.

  The Attribute column is redisplayed with a highlighted check box for the column and the selected item. Use the column and item check boxes to select or deselect individual items or the full column.
To filter on additional columns, select an entry in the columns to display check boxes. The filtering is successive: first category filters are applied, then sub category filters, then technology filters, then risk, filters, and finally characteristic filters.

For example, the next figure shows the result of applying a category, sub category, and risk filter. In applying the first two filters, the **Technology** column is automatically restricted to the technologies that are consistent with the selected category and sub category, even though a technology filter has not been explicitly applied.

Each time a filter is applied, the list of applications in the lower part of the page is automatically updated, as shown in the following figure. Any saved filters can be viewed in Objects > Application Filters.

To search for a specific application, enter the application name or description in the **Search** field, and press Enter. The application is listed, and the filter columns are updated to show statistics for the applications that matched the search.

A search will match partial strings. When you define security policies, you can write rules that apply to all applications that match a saved filter. Such rules are dynamically updated when a new application is added through a content update that matches the filter.

Click an application name to view additional details about the application, as described in the following table. You can also customize risk and timeout values, as described in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Standard Ports</td>
<td>Ports that the application uses to communicate with the network.</td>
</tr>
<tr>
<td>Capable of File Transfer</td>
<td>Indication of whether the application is able to transfer files.</td>
</tr>
<tr>
<td>Used by Malware</td>
<td>Indication of whether the application is used by malware.</td>
</tr>
<tr>
<td>Excessive Bandwidth Use</td>
<td>Indication of whether the application uses too much bandwidth so that network performance may be compromise.</td>
</tr>
<tr>
<td>Evasive</td>
<td>Indication of whether the application attempts to evade firewalls.</td>
</tr>
<tr>
<td>Tunnels Other Applications</td>
<td>Indication of whether the application can carry other applications within the messages that it sends.</td>
</tr>
</tbody>
</table>
About Other Policy Objects

When the firewall is not able to identify an application using the application ID, the traffic is classified as unknown: unknown-tcp or unknown-udp. This behavior applies to all unknown applications except those that fully emulate HTTP. For more information, refer to “Identifying Unknown Applications and Taking Action” on page 185.

You can create new definitions for unknown applications and then define security policies for the new application definitions. In addition, applications that require the same security settings can be combined into application groups to simplify the creation of security policies.

Table 69. Application Details (Continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Information</td>
<td>Links to web sources (Wikipedia, Google, and Yahoo!) that contain additional information about the application.</td>
</tr>
<tr>
<td>Category</td>
<td>Application category.</td>
</tr>
<tr>
<td>Subcategory</td>
<td>Application sub category.</td>
</tr>
<tr>
<td>Technology</td>
<td>Application technology.</td>
</tr>
<tr>
<td>Risk</td>
<td>Assigned risk of the application. To customize this setting, click the Customize link, enter a value (1-5), and click OK.</td>
</tr>
<tr>
<td>Pervasive</td>
<td>Indication of whether the effects of the application are wide-ranging.</td>
</tr>
<tr>
<td>Has Known Vulnerabilities</td>
<td>Indication of whether the application has any currently known vulnerabilities.</td>
</tr>
<tr>
<td>Prone to Misuse</td>
<td>Indication of whether the application tends to attract misuse.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Period of time (seconds) required for the application to time out due to inactivity. To customize this setting, click the Customize link, enter a value (seconds), and click OK.</td>
</tr>
<tr>
<td>TCP Timeout (seconds)</td>
<td>Timeout for terminating a TCP application flow (1-604800 seconds). To customize this setting, click the Customize link, enter a value (seconds), and click OK.</td>
</tr>
<tr>
<td>UDP Timeout (seconds)</td>
<td>Timeout for terminating a UCP application flow (1-604800 seconds). To customize this setting, click the Customize link, enter a value (seconds), and click OK.</td>
</tr>
<tr>
<td>Description</td>
<td>Purpose of the application.</td>
</tr>
</tbody>
</table>
Custom Applications with Signatures

You can define custom applications with signatures. The examples in this section show how this can be done. Refer to the PAN-OS Command Line Interface Reference Guide for information on the show application command.

Example - Detect web traffic to a specified site

This example shows an application that detects web traffic going to www.specifiedsite.com.

Requests to the web site are of the following form:

GET /001/guest/viewprofile.act?fa=25&tg=M&mg=F&searchType=zipcode&type=QUICK&pict=true&context=addr&zip=94024&ta=34&sb=&item=0&pn=0 HTTP/1.1

Host: www.specifiedsite.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-us,en;q=0.5 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 300 Connection: keep-alive Referer: http://www.specifiedsite.com/001/guest/search.act?type=QUICK&pict=true&sb=&fa=25&ta=34&mg=F&tg=M&searchType=zipcode &context=addr&context=addr Cookie: JSESSIONID=A41B41A19B753589D688190B7F0BD.001; specifiedsite.com/jumpcookie=445461346*google.com/search?q=lava+life&locale=en_US;campaign=1;imageNum=2;cfTag_LogSid=9327803497943a1237780204643;_utmz=69052556.19488761363713500.1238193797.1238193797.1238193797.1;__utmb=69052556.2.10.1238193797;__utmc=69052556;__utmz=69052556.1238193797.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none) __utmv=69052556.gender%3Df;launch=1

The following signature can identify specifiedsite traffic if the host field is www.specifiedsite.com.

username@hostname# show application specifiedsite

specifiedsite {
    category collaboration;
    subcategory social-networking;
    technology browser-based;
    decoder http;
    signature {
        s1 {
            and-condition {
                al {
                    or-condition {
                        o1 {
                            context http-req-host-header;
                            pattern www\.specifiedsite\.com;
                        }
                    }
                }
            }
        }
    }
}

Example - Detect a post to a specified blog

This example shows an application that detects blog posting activity on www.specifiedblog.com.

In this example, it is not necessary to detect when somebody tries to read the blog, only to detect when an item is getting posted.
The post traffic request includes the following:

POST /wp-admin/post.php HTTP/1.1 Host: panqa100.specifiedblog.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.7)
Gecko/2009021910 Firefox/3.0.7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-us,en;q=0.5 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Cookie: utma=96731468.235424814.1238195613.1238195613.1238195613.1; _utmb=96731468; _utmz=96731468.1238195613.1.1._utmccn=(organic) _utmcsr=google|utmcmd=referral|utmctr=blog+host _utmc=96731468; __utmt=96731468.1238195613.1.1.utmccn=(organic) _utmcsr=google|utmcmd=referral|utmctr=blog+host
Content-Type: application/x-www-form-urlencoded Content-Length: 462

The host field includes the pattern specifiedblog.com. However, if a signature is written with that value in the host, it will match all traffic going to specifiedblog.com, including posting and viewing traffic. Therefore, it is necessary to look for more patterns.

One way to do this is to look for post_title and post-author patterns in the parameters of the post. The resulting signature detects postings to the web site:

username@hostname# show application specifiedblog_blog_posting
specifiedblog_blog_posting { category collaboration; subcategory web-posting; technology browser-based; decoder http; signature { s1 { and-condition {
  a1 {
    or-condition {
      o1 {
        context http-req-host-header;
        pattern specifiedblog\.com;
        method POST;
      } }
    }
  }
  a2 {
    or-condition {
      o2 {
        context http-req-params;
        pattern post_title;
        method POST;
      } }
    }
  }
  a3 {
    or-condition {
      o3 {
        context http-req-params;
        pattern post_author;
        method POST;
      } }
    }
  }
} }
Defining Applications

Objects > Applications

To add a new application, click **New** and specify the following information.

<table>
<thead>
<tr>
<th>Table 70. New Application Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td><strong>Configuration Tab</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Shared</td>
</tr>
<tr>
<td>Category</td>
</tr>
<tr>
<td>Sub Category</td>
</tr>
<tr>
<td>Technology</td>
</tr>
<tr>
<td>Risk</td>
</tr>
<tr>
<td>Characteristics</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td><strong>Advanced Tab</strong></td>
</tr>
<tr>
<td>Default Port</td>
</tr>
<tr>
<td>IP Protocol</td>
</tr>
</tbody>
</table>
About Other Policy Objects

Table 70. New Application Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>Enter the number of seconds before an idle application flow is terminated (0 to 7200). A zero indicates that there is no timeout (the default). This value is used for protocols other than TCP and UDP in all cases, and is used for TCP and UDP timeouts when the TCP timeout and UDP timeout are not specified.</td>
</tr>
<tr>
<td>TCP Timeout</td>
<td>Enter the number of seconds before an idle TCP or UDP application flow is terminated (0 to 604800). A zero indicates that there is no timeout (the default).</td>
</tr>
<tr>
<td>Decoder</td>
<td>Select the following options from the drop-down lists:</td>
</tr>
<tr>
<td>Parent App</td>
<td>• Decoder—Indicates the application protocol. Currently HTTP is supported.</td>
</tr>
<tr>
<td></td>
<td>• Parent App—Specifies a general classification for this application. For example, if you are writing a custom application for a specific Facebook application, you can set Facebook as the parent application. This setting is important only if you are specifying a new application that covers a subset of an existing application.</td>
</tr>
<tr>
<td>Scanning</td>
<td>Select check boxes for the scanning types that you want to allow, based on security profiles (file types, data patterns, and viruses).</td>
</tr>
<tr>
<td>Signature Tab</td>
<td>Click New to add a new signature, and specify the following information:</td>
</tr>
<tr>
<td></td>
<td>• Name—Enter a name to identify the signature.</td>
</tr>
<tr>
<td></td>
<td>• Comment—Enter an optional description.</td>
</tr>
<tr>
<td></td>
<td>• Scope—Select whether to apply this signature only to the current transaction or to the full user session.</td>
</tr>
<tr>
<td></td>
<td>• Order Matters—Select if the order in which signature conditions are defined is important.</td>
</tr>
<tr>
<td></td>
<td>Specify conditions to define signatures:</td>
</tr>
<tr>
<td></td>
<td>• Add a condition by clicking Add AND Condition or Add OR Condition. To add a condition within a group, select the group and then click Add Condition. Select from the Method and Context drop-down lists. Specify a regular expression in the Pattern field. Add additional patterns as needed.</td>
</tr>
<tr>
<td></td>
<td>• To move a condition within a group, select the condition and click the Move Up or Move Down arrow. To move a group, select the group and click the Move Up or Move Down arrow. You cannot move conditions from one group to another.</td>
</tr>
</tbody>
</table>
Defining Application Groups

To simplify the creation of security policies, applications requiring the same security settings can be combined into application groups. To define new applications, refer to “Defining Applications” on page 148.

To define an application group, click New and specify the following information.

Table 71. New Application Group

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name that describes the application group (up to 31 characters). This name appears in the application list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
</tbody>
</table>
| Applications | Select specific applications for the group. The default of any should be used only in rules that specify the deny (block) action. To select specific applications, choose Select and do any of the following:  
  • To select according to the columns at the top of the page, click an entry in a column to display check boxes, and then select the check boxes. The filtering is successive: first category filters are applied, then sub category filters, then technology filters, then risk filters, and finally characteristic filters. For a description of the choices in each column, refer to “Application Categories, Subcategories, Technologies, and Characteristics” on page 239.  
  • Enter the first few characters of a name in the Search field to list all applications, categories, and groups that start with those characters. Selecting an item in the list will set the check box in the Available column. Repeat this process as often as needed, and then click Add. Each time you make a selection the list of applications on the page is updated. |
| Filters   | To filter on the available applications, select from the Filters drop-down list and click Add Filter. The list of applications on the page is updated. |
| Groups    | To filter on the available groups, select from the Groups drop-down list and click Add Group. The list of applications on the page is updated. |
About Application Filters

You can define application filters to simplify repeated searches. To define application filters to simplify repeated searches, click **New** and enter a name for the filter.

In the upper area of the window, click an item that you want to use as a basis for filtering. For example, to restrict the list to the Networking category, click **Networking**.

The column is redisplayed with a highlighted check box for the column and the selected item. Use the column and item check boxes to select or deselect individual items or the full column.

To filter on additional columns, select an entry in the columns to display check boxes. The filtering is successive: first category filters are applied, then sub category filters, then technology filters, then risk, filters, and finally characteristic filters.

For example, the next figure shows the result of choosing a category, sub category, and risk filter. In applying the first two filters, the **Technology** column is automatically restricted to the technologies that are consistent with the selected category and sub category, even though a technology filter has not been explicitly applied.

As you select options, the list of applications in the lower part of the page is automatically updated, as shown in the figure.
About Services and Service Groups

When you define security policies for specific applications, you can select one or more services to limit the port numbers the application(s) can use. The default service is any, which allows all TCP and UDP ports.

The HTTP and HTTPS services are predefined, but you can add additional service definitions. Services that are often assigned together can be combined into service groups to simplify the creation of security policies.

Defining Services

Objects > Services

When you define security policies for specific applications, you can select one or more services to limit the port numbers the applications can use. The default service is any, which allows all TCP and UDP ports.

The HTTP and HTTPS services are predefined, but you can add additional service definitions. Services that are often assigned together can be combined into service groups to simplify the creation of security policies (refer to “Defining Service Groups” on page 153).

To define services, click New and specify the following information.

Table 72. Service Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>Enter the service name (up to 31 characters). This name appears in the services list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Shared</td>
<td>If the device is in Multiple Virtual System Mode, select this check box to allow the profile to be shared by all virtual systems.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol used by the service (TCP or UDP).</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number (0 to 65535) or range of port numbers (port1-port2) used by the service. Multiple ports or ranges must be separated by commas.</td>
</tr>
</tbody>
</table>
Defining Service Groups

Objects > Services Groups

To simplify the creation of security policies, you can combine services that have the same security settings into service groups. To define new services, refer to “Defining Services” on page 152.

To define service groups, click New and specify the following information.

Table 73. Service Group Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Group Name</td>
<td>Enter the service group name (up to 31 characters). This name appears in the services list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>All Services &amp; Groups</td>
<td>Select the check box next to the services and/or other service groups to be included in this group.</td>
</tr>
</tbody>
</table>

About Data Patterns

Data pattern support allows you to specify categories of sensitive information that you may want to subject to filtering using data filtering security policies. For instructions on configuring data patterns, refer to “Defining Data Patterns” on page 157.

When adding a new pattern (regular expression), the following general requirements apply:

- The pattern must have string of at least 7 bytes to match. It can contain more than 7 bytes, but not fewer.

- The string match is case-sensitive, as with most regular expression engines. Looking for “confidential” is different than looking for “Confidential” or “CONFIDENTIAL.”

The regular expression syntax in PAN-OS is similar to traditional regular expression engines, but every engine is unique. The following table describes the syntax supported in PAN-OS.

Table 74. Pattern Rules

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Match any single character.</td>
</tr>
<tr>
<td>?</td>
<td>Match the preceding character or expression 0 or 1 time. The general expression MUST be inside a pair of parentheses. Example: (abc)?</td>
</tr>
<tr>
<td>*</td>
<td>Match the preceding character or expression 0 or more times. The general expression MUST be inside a pair of parentheses. Example: (abc)*</td>
</tr>
<tr>
<td>+</td>
<td>Match the preceding character or regular expression 1 or more times. The general expression MUST be inside a pair of parentheses. Example: (abc)+</td>
</tr>
</tbody>
</table>
### About Other Policy Objects

#### Table 74. Pattern Rules

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Equivalent to “or”. Example: ((bif)</td>
</tr>
<tr>
<td>-</td>
<td>Used to create range expressions. Example: [c-z] matches any character between c and z, inclusive.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Match any. Example: [abz]: matches any of the characters a, b, or z.</td>
</tr>
<tr>
<td>^</td>
<td>Match any except. Example: [^abz] matches any character except a, b, or z.</td>
</tr>
<tr>
<td>{ }</td>
<td>Min/Max number of bytes. Example: [10,20] matches any string that is between 10 and 20 bytes. This must be directly in front of fixed string, and only supports “.”.</td>
</tr>
<tr>
<td>\</td>
<td>To perform a literal match on any one of the special characters above, it MUST be escaped by preceding them with a ‘\’ (backslash).</td>
</tr>
<tr>
<td>&amp;amp</td>
<td>&amp; is a special character, so to look for the “&amp;” in a string you must use “&amp;amp” instead.</td>
</tr>
</tbody>
</table>

#### Data Patterns Examples

The following are examples of valid custom patterns:

- `.*(Confidential) | (CONFIDENTIAL)`
  - Looks for the word “Confidential” or “CONFIDENTIAL” anywhere
  - “.*” at the beginning specifies to look anywhere in the stream
  - Does not match “confidential” (all lower case)

- `.*(Proprietary & Confidential) | (Proprietary and Confidential)`
  - Looks for either “Proprietary & Confidential” or “Proprietary and Confidential”
  - More precise than looking for “Confidential”

- `.*(Press Release).*((Draft) | (DRAFT) | (draft))`
  - Looks for “Press Release” followed by various forms of the word draft, which may indicate that the press release isn’t ready to be sent outside the company

- `.*(Trinidad)`
  - Looks for a project code name, such as “Trinidad”
About Custom URL Categories

**Objects > Custom URL Categories**

The custom URL categories feature allows you to create your own lists of URLs that can be selected in any URL filtering profile. Each custom category can be controlled independently and will have an action associated with it in each URL filtering profile (allow, block, continue, override, or alert).

Before you begin, create a text file that contains the URLs to include, with one URL per line. Each URL can be in the format “www.example.com,” and can contain * as a wildcard, such as “www.ex*.com.” For additional information on wildcards, refer to the description of Block List in Table 63.

Click New and specify the following information. For instructions on setting up URL filtering profiles, refer to “About URL Filtering Profiles” on page 137.

<table>
<thead>
<tr>
<th>Table 75. Custom URL Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Shared</td>
</tr>
<tr>
<td>Members</td>
</tr>
</tbody>
</table>

About Custom Threat Signatures

**Objects > Threats > Spyware and Objects > Threats > Vulnerability**

The firewall supports the ability to create custom spyware and vulnerability signatures using the firewall threat engine. You can write custom regular expression patterns to identify spyware phone home communication or vulnerability exploits. The resulting spyware and vulnerability patterns become available for use in any custom vulnerability profiles. The firewall looks for the custom-defined patterns in network traffic and takes the specified action for the vulnerability exploit. Support is provided for creation of custom signatures using HTTP, SMTP, IMAP, FTP, and POP3.

Use the Custom Threat Signatures page to define signatures for vulnerability profiles. Click New and specify the following information.

<table>
<thead>
<tr>
<th>Table 76. Custom Threat Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Configuration Tab</td>
</tr>
<tr>
<td>ID</td>
</tr>
</tbody>
</table>
Table 76. Custom Threat Signatures (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared</td>
<td>If the device is in Multiple Virtual System Mode, select this check box to</td>
</tr>
<tr>
<td></td>
<td>allow the profile to be shared by all virtual systems.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter an optional comment.</td>
</tr>
<tr>
<td>Severity</td>
<td>Assign a level that indicates the seriousness of the threat.</td>
</tr>
<tr>
<td>Default Action</td>
<td>Assign the default action to take if the threat conditions are met.</td>
</tr>
<tr>
<td>Direction</td>
<td>Indicate whether the threat is assessed from the client to server, server to</td>
</tr>
<tr>
<td></td>
<td>client, or both.</td>
</tr>
<tr>
<td>Affected System</td>
<td>Indicate whether the threat involves the client, server, either, or both.</td>
</tr>
<tr>
<td>CVE</td>
<td>Specify the common vulnerability enumeration (CVE) as an external</td>
</tr>
<tr>
<td></td>
<td>reference for additional background and analysis.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Specify the vendor identifier for the vulnerability as an external</td>
</tr>
<tr>
<td></td>
<td>reference for additional background and analysis.</td>
</tr>
<tr>
<td>Bugtrap</td>
<td>Specify the bugtrap (similar to CVE) as an external reference for</td>
</tr>
<tr>
<td></td>
<td>additional background and analysis.</td>
</tr>
<tr>
<td>URL</td>
<td>Add any links to additional analysis or background information. The</td>
</tr>
<tr>
<td></td>
<td>information is shown when a user clicks on the threat from the ACC, logs,</td>
</tr>
<tr>
<td></td>
<td>or vulnerability profile.</td>
</tr>
</tbody>
</table>

**Signatures Tab**

Click **New** to add a new signature, and specify the following information:

- **Name**—Enter a name to identify the signature.
- **Comment**—Enter an optional description.
- **Scope**—Select whether to apply this signature only to the current transaction or to the full user session.
- **Order Matters**—Select if the order in which signature conditions are defined is important.

Specify conditions to define signatures:

- Add a condition by clicking **Add AND Condition** or **Add OR Condition**. To add a condition within a group, select the group and then click **Add Condition**. Select from the **Method** and **Context** drop-down lists. Specify a regular expression in the **Pattern** field. Add additional patterns as needed.

To move a condition within a group, select the condition and click the **Move Up** or **Move Down** arrow. To move a group, select the group and click the **Move Up** or **Move Down** arrow. You cannot move conditions from one group to another.
Defining Data Patterns

Objects > Data Patterns

Use the Data Patterns page to define the categories of sensitive information that you may want to subject to filtering using data filtering security policies. For information on defining data filtering profiles, refer to “Defining Data Filtering Profiles” on page 139.

To define a data object, click New and specify the following information.

Table 77. Data Pattern Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the data pattern name (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description.</td>
</tr>
<tr>
<td>Shared</td>
<td>If the device is in Multiple Virtual System Mode, select this check box to allow the profile to be shared by all virtual systems.</td>
</tr>
<tr>
<td>Add Pattern</td>
<td>The pre-defined patterns include credit card number and social security number (with and without dashes). Click to add a new pattern. Specify a name for the pattern, enter the regular expression that defines the pattern, and enter a weight to assign to the pattern. Add additional patterns as needed, or click X to delete an object.</td>
</tr>
<tr>
<td>Weight</td>
<td>Enter weights for pre-specified pattern types. The weight is a number between 1 and 255. Alert and Block thresholds specified in the Data Filtering Profile are a function of this weight.</td>
</tr>
</tbody>
</table>
About Security Profile Groups

The firewall supports the ability to create security profile groups, which specify sets of security profiles that can be treated as a unit and then added to security policies. For example, you can create a “threats” security profile group that includes profiles for antivirus, anti-spyware, and vulnerability and then create a security policy that includes the “threats” profile.

Antivirus, anti-spyware, vulnerability protection, URL filtering, and file blocking profiles that are often assigned together can be combined into profile groups to simplify the creation of security policies.

To define security profile groups, click New and specify the following information. To define new security profiles, refer to “About Security Profile Groups” on page 158.

Table 78. Security Profile Group Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Group Name</td>
<td>Enter the profile group name (up to 31 characters). This name appears in the profiles list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Profiles</td>
<td>Select an antivirus, anti-spyware, vulnerability protection, URL filtering, and/or file blocking profile to be included in this group. Data filtering profiles can also be specified in security profile groups. Refer to “Defining Data Filtering Profiles” on page 139.</td>
</tr>
</tbody>
</table>
### About Log Forwarding

Objects > Log Forwarding

Each security policy can specify a log forwarding profile that determines whether traffic and threat log entries are logged remotely with Panorama, and/or sent as SNMP traps, syslog messages, or email notifications. By default, only local logging is performed.

Traffic logs record information about each traffic flow, and threat logs record the threats or problems with the network traffic, such as virus or spyware detection. Note that the antivirus, anti-spyware, and vulnerability protection profiles associated with each rule determine which threats are logged (locally or remotely). To apply logging profiles to security policies, refer to “About Security Policies” on page 122.

To define log forwarding profiles, click **New** and specify the following information.

<table>
<thead>
<tr>
<th>Table 79. Log Forwarding Profile Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Name</td>
</tr>
</tbody>
</table>

**Traffic Log Settings**

- **Panorama**: Select the check box to enable sending traffic log entries to the Panorama centralized management system. To define the Panorama server address, refer to “Defining the Host Name and Network Settings” on page 66.

**SNMP Trap Setting**

- Under each severity level, select the SNMP, syslog, and/or email settings that specify additional destinations where the threat log entries are sent. Under each severity level, select the SNMP, syslog, and/or email settings that specify additional destinations where the traffic log entries are sent.

**Email Setting**

- Under each severity level, select the SNMP, syslog, and/or email settings that specify additional destinations where the threat log entries are sent.

**Syslog Setting**

- Under each severity level, select the SNMP, syslog, and/or email settings that specify additional destinations where the threat log entries are sent.

**Threat Log Settings**

- **Panorama**: Click the check box for each severity level of the threat log entries to be sent to Panorama. The severity levels are:
  - **Critical**: Very serious attacks detected by the threat security engine.
  - **High**: Major attacks detected by the threat security engine.
  - **Medium**: Minor attacks detected by the threat security engine, including URL blocking.
  - **Low**: Warning-level attacks detected by the threat security engine.
  - **Informational**: All other events not covered by the other severity levels, including informational attack object matches.

- **SNMP Trap Setting**
- **Email Setting**
- **Syslog Setting**
About Schedules

Objects > Schedules

By default, each security policy applies to all dates and times. To limit a security policy to specific times, you can define schedules, and then apply them to the appropriate policies. For each schedule, you can specify a fixed date and time range or a recurring daily or weekly schedule. To apply schedules to security policies, refer to “About Security Policies” on page 122.

To define schedule, click New and specify the following information.

### Table 80. Schedule Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a schedule name (up to 31 characters). This name appears in the schedule list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>Select the type of schedule (Daily, Weekly, or Non-Recurring).</td>
</tr>
<tr>
<td>Times</td>
<td>Enter a time range for the selected schedule type, and click Add. Each schedule can have multiple time ranges. For example, a weekly schedule can have one or more time ranges for each day of the week. To remove a time range, select the check box next to the range and click Delete.</td>
</tr>
<tr>
<td>Day of Week</td>
<td>If the schedule type is Weekly, select a day of the week.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Specify a start and end time in 24-hour format (HH:MM).</td>
</tr>
<tr>
<td>End Time</td>
<td></td>
</tr>
<tr>
<td>Start Date</td>
<td>If the schedule type is Non-Recurring, enter a start and end date:</td>
</tr>
<tr>
<td>End Date</td>
<td>• Click , and select a month and day.</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>• Enter the date directly (YYYY/MM/DD)</td>
</tr>
</tbody>
</table>
Chapter 6
Reports and Logs

This chapter describes how to view the reports and logs provided with the firewall:

- “Using the Dashboard” in the next section
- “Using the Application Command Center” on page 163
- “Viewing App-Scope Reports” on page 167
- “Viewing the Logs” on page 175
- “Managing PDF Summary Reports” on page 179
- “Managing User Activity Reports” on page 181
- “Managing Report Groups” on page 182
- “Scheduling Reports for Email Delivery” on page 182
- “Viewing Reports” on page 183
- “Generating Custom Reports” on page 183
- “Identifying Unknown Applications and Taking Action” on page 185
Using the Dashboard

Dashboard

The Dashboard page displays general device information, such as the software version, the operational status of each interface, resource utilization, and up to 10 of the most recent entries in the threat, configuration, and system logs. All of the available charts are displayed by default, but each user can remove and add individual charts, as needed.

Click Refresh to update the Dashboard. To change the automatic refresh interval, select an interval from the drop-down list (1 min, 2 mins, 5 mins, or Manual). To add a chart to the Dashboard, click the chart name on the left side of the page. To delete a chart, click \( \text{X} \) in the title bar of the chart.

Review the following information in each chart.

### Table 81. Dashboard Charts

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Applications</td>
<td>Displays the applications with the most sessions. The block size indicates the relative number of sessions (mouse-over the block to view the number), and the color indicates the security risk—from green (lowest) to red (highest). Click an application to view its application profile.</td>
</tr>
<tr>
<td>Top High Risk Applications</td>
<td>Similar to Top Applications, except that it displays the highest-risk applications with the most sessions.</td>
</tr>
<tr>
<td>General Information</td>
<td>Displays the device name, model, PAN-OS software version, the application, threat, and URL filtering definition versions, the current date and time, and the length of time since the last restart.</td>
</tr>
<tr>
<td>Interface Status</td>
<td>Indicates whether each interface is up (green), down (red), or in an unknown state (gray).</td>
</tr>
<tr>
<td>Threat Logs</td>
<td>Displays the threat ID, application, and date and time for the last 10 entries in the Threat log. The threat ID is a malware description or URL that violates the URL filtering profile.</td>
</tr>
<tr>
<td>Config Logs</td>
<td>Displays the administrator user name, client (Web or CLI), and date and time for the last 10 entries in the Configuration log.</td>
</tr>
<tr>
<td>Data Filtering Logs</td>
<td>Displays the description and date and time for the last 60 minutes in the Data Filtering log.</td>
</tr>
<tr>
<td>URL Filtering Logs</td>
<td>Displays the description and date and time for the last 60 minutes in the URL Filtering log.</td>
</tr>
<tr>
<td>System Logs</td>
<td>Displays the description and date and time for the last 10 entries in the System log. Note that a “Config installed” entry indicates configuration changes were committed successfully.</td>
</tr>
<tr>
<td>Resource Information</td>
<td>Displays the current CPU, memory, and disk utilization, and the number of sessions established through the firewall.</td>
</tr>
<tr>
<td>Logged In Admins</td>
<td>Displays the source IP address, session type (Web or CLI), and session start time for each administrator who is currently logged in.</td>
</tr>
</tbody>
</table>
Using the Application Command Center

Table 81. Dashboard Charts (Continued)

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACC Risk Factor</td>
<td>Displays the average risk factor (1 to 5) for the network traffic processed over the past week. Higher values indicate higher risk.</td>
</tr>
<tr>
<td>High Availability</td>
<td>If High Availability is enabled, indicates the HA status of the local and peer device—green (active), yellow (passive), or black (other). For more information about High Availability, refer to “Enabling High Availability on the Firewall” on page 30.</td>
</tr>
</tbody>
</table>

Using the Application Command Center

ACC

The Application Command Center (ACC) page displays the overall risk level for your network traffic, the risk levels and number of threats detected for the most active and highest-risk applications on your network, and the number of threats detected from the busiest application categories and from all applications at each risk level. The ACC can be viewed for the past hour, day, week, month, or any custom-defined time frame.

Risk levels (1=lowest to 5=highest) indicate the application’s relative security risk based on criteria such as whether the application can share files, is prone to misuse, or tries to evade firewalls.

To view the Application Command Center:

1. Under the ACC tab, change one or more of the following settings at the top of the page, and click Go:
   a. Select a virtual system, if virtual systems are defined.
   b. Select a time period from the Time Frame drop-down list. The default is Last Hour.
   c. Select a sorting method from the Sort By drop-down list. You can sort the charts in descending order by number of sessions, bytes, or threats. The default is by number of sessions.
d. For the selected sorting method, select the top number of applications and application categories shown in each chart from the Top N drop-down list. The default is the top 25.

![Application Command Center Page](image)

**Figure 27. Application Command Center Page**

2. To open log pages associated with the information on the page, use the log links in the upper-right corner of the page, as shown here. The context for the logs matches the information on the page.

![Traffic Log](image)

3. To filter the list, click Set Filter. Choose a filter type from the drop-down list, enter a value, and click OK.

4. Choose a view from the drop-down list for the area of interest, as described in the following table.

5. Use the drop-down lists for Applications, URL Filtering, and Threat to display the information described in the following table.
<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Displays information organized according to the menu selection. Information includes the number of sessions, bytes transmitted and received, number of threats, application category, application subcategories, application technology, and risk level, as applicable.</td>
</tr>
<tr>
<td></td>
<td>• Applications</td>
</tr>
<tr>
<td></td>
<td>• High risk applications</td>
</tr>
<tr>
<td></td>
<td>• Categories</td>
</tr>
<tr>
<td></td>
<td>• Sub Categories</td>
</tr>
<tr>
<td></td>
<td>• Technology</td>
</tr>
<tr>
<td></td>
<td>• Risk</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Displays information organized according to the menu selection. Information includes the URL, URL category, repeat count (number of times access was attempted), as applicable.</td>
</tr>
<tr>
<td></td>
<td>• URL Categories</td>
</tr>
<tr>
<td></td>
<td>• URLs</td>
</tr>
<tr>
<td></td>
<td>• Blocked URL Categories</td>
</tr>
<tr>
<td></td>
<td>• Blocked URLs</td>
</tr>
<tr>
<td>Threats</td>
<td>Displays information organized according to the menu selection. Information includes threat ID, count (number of occurrences), number of sessions, and subtype (such as vulnerability), as applicable.</td>
</tr>
<tr>
<td></td>
<td>• Threats</td>
</tr>
<tr>
<td></td>
<td>• Types</td>
</tr>
<tr>
<td></td>
<td>• Spyware</td>
</tr>
<tr>
<td></td>
<td>• Spyware Phone Home</td>
</tr>
<tr>
<td></td>
<td>• Spyware Downloads</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability</td>
</tr>
<tr>
<td></td>
<td>• Virus</td>
</tr>
<tr>
<td>Data Filtering</td>
<td>• Types</td>
</tr>
<tr>
<td></td>
<td>• File Types</td>
</tr>
<tr>
<td></td>
<td>• File Names</td>
</tr>
</tbody>
</table>
6. To view additional details, click any of the links. A details page opens to show information about the item at the top and additional lists for related items.

**Application Information**

- **Name**: ssl
- **Description**: Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols which provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.
- **Category**: networking
- **Subcategory**: encrypted-tunnel
- **Technology**: browser-based
- **Risk**: High
- **Widely Used**: Yes
- **Has Known Vulnerabilities**: Yes
- **Prone to Misuse**: No
- **Session Timeout (seconds)**: 1800
- **TCP Timeout (seconds)**: 
- **UDP Timeout (seconds)**: 

**Additional Information**: Wikipedia, Google, Yahoo!

**Top Applications**

<table>
<thead>
<tr>
<th>Risk</th>
<th>Application</th>
<th>Sessions</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ssl</td>
<td>30,863</td>
<td>415,338,178</td>
</tr>
</tbody>
</table>

**Top Sources**

<table>
<thead>
<tr>
<th>Source address</th>
<th>Source Host Name</th>
<th>Source User</th>
<th>Bytes</th>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.154.1.37</td>
<td>engr37.net1.bigedu.local</td>
<td>panacademo</td>
<td>gloria.wilker</td>
<td>9,123,112</td>
</tr>
<tr>
<td>10.154.4.42</td>
<td>engr42.net4.bigedu.local</td>
<td>panacademo</td>
<td>edgar.gray</td>
<td>4,896,933</td>
</tr>
<tr>
<td>10.154.1.64</td>
<td>engr64.net1.bigedu.local</td>
<td>panacademo</td>
<td>online.london</td>
<td>4,051,269</td>
</tr>
<tr>
<td>10.154.2.1</td>
<td>engr1.net2.bigedu.local</td>
<td>panacademo</td>
<td>javier.owens</td>
<td>963,202</td>
</tr>
</tbody>
</table>

*Figure 28. Application Command Center Page Drill Down Page*
Viewing App-Scope Reports

- **Monitor > App Scope**

The App-Scope reports introduce a visibility and analysis tools to help pinpoint problematic behavior, helping you understand the following aspects of your network:

- Changes in application usage and user activity
- Users and applications that take up most of the network bandwidth
- Network threats

With the App-Scope reports, you can quickly see if any behavior is unusual or unexpected. Each report provides a dynamic, user-customizable window into the network. The reports include options to select the data and ranges to display.

To view the reports, click the report name under **App-Scope** on the left side of the page in the Monitor tab. Select one of the report types lists below. Report options are available from the drop-down lists at the top and bottom of some of the pages.

**Table 83. Application Command Center Charts**

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>“Summary Report” on page 168</td>
</tr>
<tr>
<td>Change Monitor</td>
<td>“Change Monitor Report” on page 169</td>
</tr>
<tr>
<td>Threat Monitor</td>
<td>“Threat Monitor Report” on page 170</td>
</tr>
<tr>
<td>Threat Map</td>
<td>“Threat Monitor Report” on page 170</td>
</tr>
<tr>
<td>Network Monitor</td>
<td>“Network Monitor Report” on page 172</td>
</tr>
<tr>
<td>Traffic Map</td>
<td>“Traffic Map Report” on page 174</td>
</tr>
</tbody>
</table>
Summary Report

The Summary report (Figure 29) displays charts for the top five gainers, losers, and bandwidth consuming applications, application categories, users, and sources.

Figure 29. App-Scope Summary Report
Change Monitor Report

The Change Monitor report (Figure 30) displays changes over a specified time period.

![Change Monitor Report](image)

**Figure 30. App-Scope Change Monitor Report**

This report contains the following buttons and options.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Top 25" /></td>
<td>Determines the number of records with the highest measurement included in the chart: Top 25, Top 50, Top 75, or Top 100</td>
</tr>
<tr>
<td><img src="image" alt="Application" /></td>
<td>Determines the type of item reported: Application, Application Category, Source, or Destination.</td>
</tr>
<tr>
<td><img src="image" alt="Gainers" /></td>
<td>Displays measurements of items that have increased over the measured period.</td>
</tr>
<tr>
<td><img src="image" alt="Losers" /></td>
<td>Displays measurements of items that have decreased over the measured period.</td>
</tr>
<tr>
<td><img src="image" alt="Dropped" /></td>
<td>Displays measurements of items that were discontinued over the measure period.</td>
</tr>
<tr>
<td><img src="image" alt="Filter: None" /></td>
<td>Displays only the selected item.</td>
</tr>
<tr>
<td><img src="image" alt="Sessions" /></td>
<td>Determines whether sessions or bytes are displayed.</td>
</tr>
</tbody>
</table>
Viewing App-Scope Reports

Table 84. Change Monitor Report Buttons (Continued)

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Sort:" /></td>
<td>Determines whether data is sorted by number or percent.</td>
</tr>
<tr>
<td><img src="image" alt="Compare previous period" /></td>
<td>Indicates the period over which the change measurements are taken.</td>
</tr>
</tbody>
</table>

For example, in Figure 30 the figure displays the top 25 applications that gained in use for the 24-hour period ending with the last full hour today. The top applications are determined by session count and sorted by per cent.

**Threat Monitor Report**

The Threat Monitor report (Figure 31) displays a count of the top threats over the selected time period.

![Threat Monitor Report](image)

**Figure 31. App-Scope Threat Monitor Report**
Each threat type is color-coded as indicated in the legend below the chart. This report contains the following buttons and options.

**Table 85. Threat Monitor Report Buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Top10" /></td>
<td>Determines the number of records with the highest measurement included in the chart: Top 10 or Top 25.</td>
</tr>
<tr>
<td><img src="image" alt="Type" /></td>
<td>Determines the type of item measured: Threat, Threat Category, Source, or Destination.</td>
</tr>
<tr>
<td><img src="image" alt="Filter" /></td>
<td>Displays the selected threat type: All, Viruses, Spyware, or Vulnerabilities.</td>
</tr>
<tr>
<td><img src="image" alt="Period" /></td>
<td>Indicates the period over which the measurements are taken.</td>
</tr>
<tr>
<td><img src="image" alt="Chart" /></td>
<td>Determines whether the information is presented in a stacked column chart or a stacked area chart.</td>
</tr>
</tbody>
</table>

For example, Figure 31 the figure displays the top 10 threats over the past 24 hours.

**Threat Map Report**

The Threat Map report (Figure 32) shows a geographical view of threats, including severity.

![Figure 32. App-Scope Threat Monitor Report](image)
Each threat type is color-coded as indicated in the legend below the chart. Click a country on the map to zoom in. Click the Zoom Out button in the lower right corner of the screen to zoom out.

This report contains the following buttons and options.

### Table 86. Threat Map Report Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Top 10" /></td>
<td>Determines the number of records with the highest measurement included in the chart: Top 10 or Top 25.</td>
</tr>
<tr>
<td><img src="image" alt="Incoming threats" /></td>
<td>Determines whether incoming or outgoing threats are included.</td>
</tr>
<tr>
<td><img src="image" alt="Filter" /></td>
<td>Displays the selected threat type: All, Viruses, Spyware, or Vulnerabilities.</td>
</tr>
<tr>
<td><img src="image" alt="Dates" /></td>
<td>Indicates the period over which the measurements are taken.</td>
</tr>
</tbody>
</table>

### Network Monitor Report

The Network Monitor report (Figure 33) displays the bandwidth dedicated to different network functions over the specified period of time. Each network function is color-coded as indicated in the legend below the chart.
The report contains the following buttons and options.

**Table 87. Network Monitor Report Buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10</td>
<td>Determines the number of records with the highest measurement included in the chart: Top 10, Top 25, or Top 100.</td>
</tr>
<tr>
<td>Application</td>
<td>Determines the type of item measured: Application, Application Category, Source, or Destination.</td>
</tr>
<tr>
<td>Filter: None</td>
<td>Displays only the selected item.</td>
</tr>
<tr>
<td>Sessions or bytes</td>
<td>Determines whether sessions or bytes are plotted.</td>
</tr>
<tr>
<td>Last 24 hours Last 7 days Last 2 weeks Last 30 days</td>
<td>Indicates the period over which the measurements are taken.</td>
</tr>
<tr>
<td></td>
<td>Determines whether the information is presented in a stacked column chart or a stacked area chart.</td>
</tr>
</tbody>
</table>

For example, Figure 33 displays the top 10 applications over the past 6 hours, measured by the number of bytes transmitted and received.
Traffic Map Report

The Traffic Map report (Figure 34) shows a geographical view of traffic flows according to sessions or flows.

![Traffic Map Report](image)

**Figure 34. App-Scope Traffic Monitor Report**

Each traffic type is color-coded as indicated in the legend below the chart. This report contains the following buttons and options.

**Table 88. Threat Map Report Buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Top 10" /></td>
<td>Determines the number of records with the highest measurement included in the chart: Top 10 or Top 25.</td>
</tr>
<tr>
<td><img src="image" alt="Incoming threats" /></td>
<td>Determines whether incoming or outgoing traffic is included.</td>
</tr>
<tr>
<td><img src="image" alt="Sessions or Bytes" /></td>
<td>Determines whether sessions or bytes are plotted.</td>
</tr>
<tr>
<td><img src="image" alt="Period" /></td>
<td>Indicates the period over which the measurements are taken.</td>
</tr>
</tbody>
</table>
Viewing the Logs

Monitor > Logs

The firewall maintains logs for traffic flows, threats, configuration changes, and system events. You can view the current logs at any time. To locate specific entries, you can apply filters to most of the log fields.

Note: The firewall displays the information in logs so that role-based administration permissions are respected. When you display logs, only the information that you have permission to see is included. For information on administrator permissions, refer to “Defining Administrator Roles” on page 54.

To view the logs, click the log types on the left side of the page in the Monitor tab. Each log page has a filter area at the top of the page.

Use the filter area as follows:

- Click any of the underlined links in the log listing to add that item as a log filter option. For example, if you click the Host link in the log entry for 10.0.0.252 and Web Browsing in both items are added, and the search will find entries that match both (AND search).

- To define other search criteria, click the Add Filter Expression button to open the Expression pop-up window. Select the type of search (and/or), the attribute to include in the search, the matching operation, and the values for the match, if appropriate. Click Add to add the criterion to the filter area on the log page, and then click Close to close the pop-up window. Click the Apply Filter button to display the filtered list.

Note: You must use the Expression pop-up window to define AND and OR filters, or enter the desired filter directly.

You can combine filter expressions added on the Log page with those that you define in the Expression pop-up window. Each is added as an entry on the Filter line on the Log page.

If you set the “in” Received Time filter to Last 60 seconds, some of the page links on the log viewer may not show results because the number of pages may grow or shrink due to the dynamic nature of the selected time.

- To clear filters and redisplay the unfiltered list, click the Clear Filter button.

- To save your selections as a new filter, click the Save Filter button, enter a name for the filter, and click OK.

- To export the current log listing (as shown on the page, including any applied filters) click the Save Filter button. Select whether to open the file or save it to disk, and select the check box if you want to always use the same option. Click OK.
Click the **Refresh** link at the top of the page to update the log. To change the automatic refresh interval, select an interval from the drop-down list (1 min, 30 seconds, 10 seconds, or Manual). To change the number of log entries per page, select the number of rows from the **Rows** drop-down list.

Log entries are retrieved in blocks of 10 pages. To move between pages, click the page numbers or the left or right arrowhead icons at the bottom of the frame. To view the next block of pages, click ; to view the first block of pages, click .

If an entry has an underlined name link, you can click the link to display additional details. You can also specify exceptions if you want to ignore the log entry. **Select Current security profile** (the default) to disable the entry for the profile that caused it, or choose **Multiple security profiles** and select other profiles. Click **Add** to ignore the log entry for the specified profiles. Click **Close** to close the Details window.

When you create exceptions they appear in a tab on the vulnerability, anti-spyware, or antivirus profile. Refer to “About Security Profiles” on page 132.

![Figure 35. Log Entry Details](image)

If the source or destination has an IP address to name mapping defined in the Addresses page, the name is presented instead of the IP address. To view the associated IP address, move your cursor over the name.
Review the following information in each log.

### Table 89. Log Descriptions

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>Displays an entry for the start and end of each session. Each entry includes the date and time, the source and destination zones, addresses, and ports, the application name, the security rule name applied to the flow, the rule action (allow, deny, or drop), the ingress and egress interface, and the number of bytes. Click next to an entry to view additional details about the session, such as whether an ICMP entry aggregates multiple sessions between the same source and destination (the Count value will be greater than one). Note that the Type column indicates whether the entry is for the start or end of the session, or whether the session was denied or dropped. A “drop” indicates that the security rule that blocked the traffic specified “any” application, while a “deny” indicates the rule identified a specific application. If traffic is dropped before the application is identified, such as when a rule drops all traffic for a specific service, the application is shown as “not-applicable”.</td>
</tr>
<tr>
<td>Threat</td>
<td>Displays an entry for each security alarm generated by the firewall. Each entry includes the date and time, a threat name or URL, the source and destination zones, addresses, and ports, the application name, and the alarm action (allow or block) and severity. Click next to an entry to view additional details about the threat, such as whether the entry aggregates multiple threats of the same type between the same source and destination (the Count value will be greater than one). Note that the Type column indicates the type of threat, such as “virus” or “spyware.” The Name column is the threat description or URL, and the Category column is the threat category (such as “keylogger”) or URL category. If local packet captures are enabled, click next to an entry to access the captured packets, as in the following figure. To enable local packet captures, refer to “About URL Filtering Profiles” on page 137.</td>
</tr>
</tbody>
</table>
### Table 89. Log Descriptions (Continued)

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Filtering</td>
<td>Displays logs for URL filters, which block access to specific web sites and web site categories or generate an alert when a proscribed web site is accessed. Refer to “About URL Filtering Profiles” on page 137 for information on defining URL filtering profiles.</td>
</tr>
</tbody>
</table>
| Data Filtering | Displays logs for the security policies that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall. Refer to “Defining Data Filtering Profiles” on page 139 for information on defining data filtering profiles.  
To configure password protection for access the details for a log entry, click the icon. Enter the password and click OK. Refer to “About System Setup, Configuration, and License Management” on page 66 for instructions on changing or deleting the data protection password.  
*Note: The system prompts you to enter the password only once per session.* |
| Configuration | Displays an entry for each configuration change. Each entry includes the date and time, the administrator user name, the IP address from where the change was made, the type of client (Web or CLI), the type of command executed, whether the command succeeded or failed, and the configuration path. |
| System       | Displays an entry for each system event. Each entry includes the date and time, the event severity, and an event description.                                                                                                                                                 |
Managing PDF Summary Reports

Monitor > PDF Reports

PDF summary reports contain information compiled from existing reports, based on data for the top 5 in each category (instead of top 50). They also contain trend charts that are not available in other reports.

Figure 36. PDF Summary Report
To create PDF summary reports, click **New**. The Manage PDF Summary Reports page opens to show all of the available report elements.

*Figure 37. Managing PDF Reports*

Use one or more of these options to design the report:

- To remove an element from the report, click the *X* icon in the upper-right corner of the element’s icon box or remove the check box from the item in the appropriate drop-down list box near the top of the page.

- Select additional elements by choosing from the drop-down list boxes near the top of the page.

- Drag and drop an element’s icon box to move it to another area of the report.

*Note:* A maximum of 18 report elements is permitted. You may need to delete existing elements to add additional ones.

Click **Save**, enter a name for the report, as prompted, and click **OK**.

To display PDF reports, choose **PDF Summary Report**, and select a report type from the drop-down list at the bottom of the page to display the generated reports of that type. Click an underlined report link to open or save the report.
Managing User Activity Reports

To schedule email delivery of reports, choose Email Scheduler. Click the link for a report to display the email options, or click New to create a new email schedule. Specify the following information.

Table 90. Email Scheduler Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the schedule.</td>
</tr>
<tr>
<td>Report</td>
<td>Select the report to email from the drop-down list.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>Select a recurrence option from the drop-down list. You can order email delivery daily or weekly on a specified day of the week.</td>
</tr>
<tr>
<td>Email Profile</td>
<td>Select an email profile from the drop-down list, or click New to create a new profile. Follow the instructions in “Defining Email Notification Settings” on page 64.</td>
</tr>
<tr>
<td>Override Recipient Email(s)</td>
<td>Specify additional recipient email addresses that are not included in the email profile.</td>
</tr>
</tbody>
</table>

To send a test message to the recipients, click Send Test Message. The selected report will be sent at a standard time each day or week.

Managing User Activity Reports

▶ Monitor > PDF Reports > User Activity

Use this page to create reports that summarize the activity of individual users. Click New and specify the following information.

Table 91. User Activity Report Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the report.</td>
</tr>
<tr>
<td>User</td>
<td>Enter the user name or IP address (IPv4 or IPv6) of the user who will be the subject of the report.</td>
</tr>
<tr>
<td>Time frame</td>
<td>Select the time frame for the report from the drop-down list.</td>
</tr>
</tbody>
</table>

To run the report on demand, select the report and click Edit, and then click Run.
Managing Report Groups

- **Monitor > PDF Reports > Report Groups**

Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

To create a new report group, click **New** and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Group Name</td>
<td>Enter a name to identify the report.</td>
</tr>
<tr>
<td>Title Page</td>
<td>Select the check box to include a title page in the report.</td>
</tr>
<tr>
<td>Custom Title</td>
<td>Enter the name that will appear as the report title.</td>
</tr>
<tr>
<td>Report selection</td>
<td>Select reports from the left column and click <strong>Add</strong> to move each to the report group on the right.</td>
</tr>
</tbody>
</table>

To use the report group, refer to “Scheduling Reports for Email Delivery” in the next section.

Scheduling Reports for Email Delivery

- **Monitor > PDF Reports > Email Scheduler**

Use the Email scheduler to schedule reports for delivery by email. Before adding a schedule, you must define report groups and an email profile. Refer to “Managing Report Groups” on page 182 and “Defining Email Notification Settings” on page 64.

To schedule report delivery, click **New** and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the schedule.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>Select the frequency at which to generate and send the report. Adamit.</td>
</tr>
<tr>
<td>Email Profile</td>
<td>Select the profile that defines the email settings. Refer to “Defining Email Notification Settings” on page 64 for information on defining email profiles.</td>
</tr>
<tr>
<td>Override Recipient email(s)</td>
<td>Enter an optional email address to use instead of the recipient specified in the email profile.</td>
</tr>
</tbody>
</table>
Viewing Reports

Monitor

The firewall provides various “top 50” reports of the traffic statistics for the previous day or a selected day in the previous week.

To view the reports, click the report names on the left side of the page under the Monitor tab. By default, all reports are displayed for the previous calendar day. To view reports for any of the previous days, select a report generation date from the Select drop-down list at the bottom of the page.

The reports are listed in sections. You can view the information in each report for the selected time period. To export the log in CSV format, click Export to CSV. To open the log information in PDF format, click Export to PDF. The PDF file opens in a new window. Click the icons at the top of the window to print or save the file.

Generating Custom Reports

Monitor > Manage Custom Reports

You can customize most of the standard reports available from the Monitor tab by selecting fields to include in the report and applying filters.

To create a custom report, click New to open a new report. Alternatively, to use an existing report as a template, click Open to choose the report. Select the report and click Load to add the report settings as a template.

To define a custom report:

1. Enter a report title.
2. Choose the database for the report from the Database drop-down list.
3. Select the columns to include in the report from the Columns drop-down list.
   The available columns depend on the choice of database. When you add or remove columns, the column headers on the page are updated to reflect your choices.
4. Choose the amount of information to include in the report (top 5, 10, 25, or 50), and how to sort the report.
5. Click Save to save the report settings.

To generate a custom report:

1. Under the Monitor tab, click Manage Custom Reports in the Custom Reports section.
2. Click New, and select the report.
3. Choose from the following options:
   - Click Scheduled to run the report each night and make the results available in the Custom Report list on the side menu.
   - Click Run to run the report immediately and display the results in a new tab on the page. This option does not save the report results.
Generating Custom Reports

To add filters to custom reports:

1. Under the Monitor tab, click Manage Custom Reports in the Custom Reports section.
2. Click New if you are creating a new report or Open to choose an existing report.
3. Perform these operations to define a set of filters:
   - Add a condition by clicking Add Condition and selecting from the Attribute, Operation, and Value drop-down lists. Successive pairs of conditions are combined using the AND operator (both must be valid for the filter to apply).
   - Combine conditions by clicking Add Group. Select the type of operator to use between groups (AND, OR) and then drag the small yellow box for a condition to move it to the group.
   - Choose a time period from the Period drop-down list.

In the following example, the custom report filter will capture data that applies to the source IP subnet 10.1.1.0/24 AND destination IP address 10.0.0.5 OR to the destination user user1.

<table>
<thead>
<tr>
<th>Group</th>
<th>Attribute</th>
<th>Operation</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source IP</td>
<td></td>
<td>10.1.1.0/24</td>
</tr>
<tr>
<td>OR</td>
<td>Destination IP</td>
<td></td>
<td>10.0.0.5</td>
</tr>
<tr>
<td></td>
<td>Destination User</td>
<td></td>
<td>user1</td>
</tr>
</tbody>
</table>

Figure 38. Custom Report Filter Example

4. Configure any additional report settings, and click OK to save the report, including the specified filters.
Identifying Unknown Applications and Taking Action

There are several ways to view unknown applications using the web interface of the Palo Alto Networks devices:

- **Application Command Center (ACC)**—Unknown applications are sorted along with other applications in the ACC. Click a link for an unknown application to view the details of the application, including top sources and destinations. For top sources, click the link to look up the owner of the address.

![Unknown Applications in the ACC List](image)

**Figure 39. Unknown Applications in the ACC List**
• **Unknown application reports**—Unknown application reports are automatically run on a daily basis and stored in the Reports section of the Monitor tab. These reports can provide useful information to help identify unknown applications.

![Unknown Application Report Example](image)

**Figure 40. Unknown Application Report Example**

• **Detailed traffic logs**—You can use the detailed traffic logs to track down unknown applications. If logging is enabled for the start and end of session, the traffic log will provide specific information about the start and end of an unknown session. Use the filter option to restrict the display to entries that match “unknown-tcp,” as shown in the next figure.

![Unknown Applications in Traffic Logs](image)

**Figure 41. Unknown Applications in Traffic Logs**
Taking Action

You can take the following actions to deal with unknown applications:

- Use custom application definition with application override (refer to “Custom Application Definition with Application Override” on page 131).

- Use custom applications with signatures (refer to “Custom Applications with Signatures” on page 146).

- Request an App-ID from Palo Alto Networks (refer to “Requesting an App-ID from Palo Alto Networks” in the next section).

Policies can also be set to control unknown applications by unknown TCP, unknown UDP or by a combination of source zone, destination zone, and IP addresses. Refer to “About Application Override Policies” on page 131.

Note: You can use custom signatures in App-ID definitions.

Requesting an App-ID from Palo Alto Networks

If it is necessary to identify an application using application contents instead of port, protocol, and IP address, you can submit the application to Palo Alto Networks for classification. This is important for applications that run over the Internet and for which custom application does not work. You can submit the application to Palo Alto Networks in either of the following ways:

- If the application is a readily accessible on the Internet (for example, an instant messaging application), then submit the name of the application and the URL to your account team or to this web site: http://www.paloaltonetworks.com/arc/

- If the application is not easily accessible (for example, a customer relationship management application) you must submit a packet capture (PCAP) of the running application using the session packet capture function built into the firewall. For assistance, contact technical support at support@paloaltonetworks.com.
Chapter 7

Configuring IPSec Tunnels

This chapter describes virtual private networks (VPNs) in general and IP Security (IPSec) VPNs in detail, and describes how to configure IPSec tunnels for VPNs on the firewall. Refer to the following sections:

- “About Virtual Private Networks” in the next section
- “About IPSec and IKE” on page 191
- “Setting Up IPSec VPNs” on page 193
- “Defining IKE Gateways” on page 194
- “Defining IKE Crypto Profiles” on page 195
- “Defining IPSec Crypto Profiles” on page 195
- “Setting Up IPSec Tunnels” on page 196
- “Defining Tunnel Monitor Profiles” on page 199
- “Viewing IPSec Tunnel Status on the Firewall” on page 200
- “Sample VPN Configuration” on page 201
Virtual private networks (VPNs) allow systems to connect securely over a public wide area network (WAN) as if they were connecting over a local area network (LAN). The IP Security (IPSec) set of protocols is used to set up a secure tunnel for the VPN traffic, and the private information in the TCP/IP packets is encrypted when sent through the IPSec tunnel.

Note: In addition to IPSec VPNs, the firewall also supports Secure Socket Layer (SSL) VPNs, which allow remote users to establish VPN connections through the firewall. Refer to Chapter 8, “Configuring SSL VPNs” for more information.

The following figure shows a standard IPSec tunnel between two devices. The configuration can include a tunnel monitor on each side to alert the device administrator of tunnel failure and provide automatic failover. Tunnel monitors are useful if you want to be able to provide failover of IPSec traffic to another interface.

Figure 42. IPSec Standard Configuration

You can configure route-based VPNs to connect Palo Alto Networks firewalls at central and remote sites or to connect Palo Alto Networks firewalls with third party security devices at other locations. With route-based VPNs, the firewall makes a routing decision based on the destination IP address. If traffic is routed through a VPN tunnel, then it is encrypted as VPN traffic. It is not necessary to define special rules or to make explicit reference to a VPN tunnel; routing and encryption decisions are determined only by the destination IP address.

The firewall can also interoperate with a policy-based VPN. To connect with a policy-based VPN, configure the Proxy ID for the tunnel. If multiple phase 2 tunnels are required, configure different Proxy IDs on each. Refer to “Setting Up IPSec Tunnels” on page 196.

For the IPSec connection between the firewalls, the full IP packet (header and payload) is embedded in another IP payload, and a new header is applied. The new header uses the IP address of the outgoing firewall interface as the source IP address and the incoming firewall interface at the far end of the tunnel as the destination IP address. When the packet reaches the firewall at the far end of the tunnel, the original packet is reconstructed and sent to the actual destination host.
IPSec Security Associations (SAs) are defined at each end of the IPSec tunnel to apply all of the parameters that are required for secure transmission, including the security parameter index (SPI), security protocol, cryptographic keys, and the destination IP address. Encryption, data authentication, are all handled by the SAs.

**About IPSec and IKE**

There are two ways to secure IPSec VPN tunnels:

- Configure the tunnel using manual security keys.
- Generate keys using Internet Key Exchange (IKE)

The same method must be applied to both ends of the IPSec tunnel. In the case of manual keys, the same key is entered at both ends; in the case of IKE, the same methods and attributes are applied at both ends.

**About IPSec VPNs and SSL VPNs**

The firewall supports both IPSec VPNs, described in this chapter, and SSL VPNs, described in “Configuring SSL VPNs” on page 205.

- IPSec VPNs are used for site-to-site connections.
- SSL VPNs are used solely to connect remote users to the network and permit direct access through a web browser without requiring installation of a client application.

**About VPN Tunnels**

To set up VPNs, it is important to understand your network topology and be able to determine the required number of tunnels. For example:

- A single VPN tunnel may be sufficient for connection between a single central site and remote site.
- Connections between a central site and multiple remote sites require VPN tunnels for each central - remote site pair.

Each tunnel is bound to a tunnel interface. It is necessary to assign the tunnel interface to the same virtual router as the incoming (clear text) traffic. In this way, when a packet comes to the firewall, the route lookup function can determine the appropriate tunnel to use. The tunnel interface appears to the system as a normal interface, and the existing routing infrastructure can be applied.

Each tunnel interface can have a maximum of 10 IPSec tunnels. This allows you to set up IPSec tunnels for individual networks that are all associated with the same tunnel interface on the firewall.
IKE provides a standard mechanism for generating and maintaining security keys:

- **Identification**—The identification process involves recognition of the peers at both ends of the IPSec tunnel. Each peer is identified by IP address or peer ID (contained in the payload of the IP packet). The firewall or other security device at each end of the tunnel adds the identification of the peer at the other end into its local configuration.

- **Authentication**—There are two types of authentication methods: pre-shared key and PKI. Currently only the pre-shared key method is supported by Palo Alto Networks firewalls.

The firewall supports definition of IKE gateways, which specify the configuration information necessary to perform IKE protocol negotiation with peer gateways.

IKE configuration options include Diffie-Hellman Group for key agreement, Encryption algorithm, and hash for message authentication.

### About IPSec and IKE Crypto Profiles

Crypto profiles are related to standard proposal fields in IKE negotiation. The first phase involves the IKE-crypto profile for IKE security association (SA) negotiation (IKEv1 Phase-1), while the second phase involves IPSec crypto profile for IPSec SA negotiation (IKEv1 Phase-2).

You can define IPSec and IKE crypto profiles that determine the protocols and algorithms used to negotiate the IPSec and IKE SAs.

**Options for IKE SA:**
- **Diffie-Hellman (DH) Group**—Select DH groups to use when generating public keys for IKE.
- **Encryption**—Select encryption algorithms.
- **Hash Algorithm**—Select hash algorithms.
- **Lifetime**—Specify the length of time that the negotiated key will stay effective.

**Options for IPSec SA:**
- **Authentication Header (AH)**—Select options for authentication and data integrity.
- **Encapsulating Security Payload (ESP)**—Select options for authentication, data integrity, confidentiality, and encryption.
- **Perfect Forward Security (PFS) Diffie-Hellman (DH) group**—Select DH groups to use in generating independent keys for IPSec.
- **Lifetime**—Specify the length of time that the negotiated key will stay effective.

For details on the specific protocols and algorithms supported for IPSec and IKE crypto profiles, refer to “Defining IKE Crypto Profiles” on page 195 and “Defining IPSec Crypto Profiles” on page 195.
Setting Up IPSec VPNs

This section describes the multi-step process involved in setting up IPSec VPN tunnels. For detailed instructions, refer to the specified sections in this guide. For a sample configuration, refer to “Sample VPN Configuration” on page 239.

Note: Before you begin, make sure that your Ethernet interfaces, virtual routers, and zones are configured properly. Refer to “About Firewall Interfaces” on page 85, “About Virtual Routers and Routing Protocols” on page 98, and “Defining Security Zones” on page 97.

To set up IPSec VPNs:

1. Plan the network topology and determine the required number of tunnels.

2. Define IKE gateways with the configuration information for IKE protocol negotiation with peer gateways. Refer to “Defining IKE Gateways” on page 194.

3. Configure the protocols and algorithms for identification, authentication, and encryption in VPN tunnels using IKE SA negotiation:
   - For IKEv1 Phase-1, refer to “Defining IKE Crypto Profiles” on page 195.
   - For IKEv1 Phase-2, refer to “Defining IPSec Crypto Profiles” on page 195.

4. Configure the parameters that are needed to establish IPSec VPN tunnels. Refer to “Setting Up IPSec Tunnels” on page 196.

5. Specify how the firewall will monitor the IPSec tunnels. Refer to “Defining Tunnel Monitor Profiles” on page 199.

6. Set up static routes or assign routing protocols to redirect traffic into the newly established tunnels. The Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) options are supported; you can enable one or both of these protocols on the tunnel interface. Refer to “About Virtual Routers and Routing Protocols” on page 98.

7. Set security policies to filter and inspect the traffic as described in “About Security Policies” on page 122. Define the source and destination zones and specify the policy attributes as follows:
   - **Outgoing traffic**—For source, use the clear text zone. For destination, use the tunnel interface zone.
   - **Incoming traffic**—For source, use the tunnel interface zone. For destination, use the clear text zone.

After defining the rule, set the source and destination addresses.

Note: VPN traffic can reuse existing security policies that were intended for clear text, if that is appropriate for your network. You can put the tunnel interface in a special zone to ensure that VPN traffic is separated from clear text traffic.
Defining IKE Gateways

When these tasks are complete, the tunnel is ready for use. Traffic destined for the addresses defined for the tunnels is automatically routed properly and encrypted as VPN traffic.

**Note:** Without matching security rules, VPN traffic will be dropped by the firewall, when a security rule is required.

The IKE protocol will be triggered when necessary (for example, when traffic is routed to an IPSec tunnel with no keys or expired keys).

### Defining IKE Gateways

**Network > Network Profiles > IKE Gateways**

Use the IKE Gateways page to define gateways that include the configuration information necessary to perform IKE protocol negotiation with peer gateways. To set up IKE gateways, click **New** and specify the following information.

**Table 94. IKE Gateway Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Gateway</td>
<td>Enter a name to identify the gateway.</td>
</tr>
<tr>
<td>Local IP Address</td>
<td>Select the IP address for the local interface that is the endpoint of the tunnel.</td>
</tr>
<tr>
<td>Peer IP Address</td>
<td>Static IP address or dynamic option for the peer on the far end of the tunnel.</td>
</tr>
<tr>
<td>Pre-shared key</td>
<td>Enter a security key to use for authentication across the tunnel.</td>
</tr>
</tbody>
</table>

**Note:** The following advanced fields are visible if you click the **Show advanced Phase 1 options** link.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Identification</td>
<td>Choose from the following types and enter the value: Fully qualified domain name (FQDN), key ID, or user FQDN.</td>
</tr>
<tr>
<td>Peer Identification</td>
<td>Choose from the following types and enter the value: FQDN, key ID, or user FQDN (for the dynamic option)</td>
</tr>
<tr>
<td>Exchange Mode</td>
<td>Choose auto, aggressive, or main.</td>
</tr>
<tr>
<td>IKE Crypto Profile</td>
<td>Select an existing profile or keep the default profile.</td>
</tr>
<tr>
<td>Dead Peer Detection</td>
<td>Select the check box to enable and enter an interval (2 - 100 seconds) and delay before retrying (2 - 100 seconds). Dead peer detection identifies inactive or unavailable IKE peers through ICMP ping and can help restore resources that are lost when a peer is unavailable.</td>
</tr>
</tbody>
</table>

**Note:** When a device is set to use the **auto** exchange mode, it can accept both main mode and aggressive mode negotiation requests; however, whenever possible, it initiates negotiation and allows exchanges in main mode.

You must configure the peer device with the matching exchange mode to allow it to accept negotiation requests initiated from the first device.
Defining IKE Crypto Profiles

Use the IKE Crypto Profiles page to specify protocols and algorithms for identification, authentication, and encryption in VPN tunnels based on IPSec SA negotiation (IKEv1 Phase-1). Refer to “About Virtual Private Networks” on page 190 for more information.

To create a new configuration, click New and specify the following information. To change the ordering in which an algorithm or group is listed, click the icon. The ordering determines the first choice when settings are negotiated with a remote peer. The setting at the top of the list is attempted first, continuing down the list until an attempt is successful.

Table 95. IKE Crypto Profile Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DH Group Priority</td>
<td>Specify the priority for Diffie-Hellman (DH) groups. For highest security, use the arrows to move the groups with higher numeric identifiers to the top of the list. For example, move group14 above group2.</td>
</tr>
<tr>
<td>Hash Algorithm Priority</td>
<td>Specify the priority for hash algorithms. For highest security, use the arrows to move sha1 to the top of the list.</td>
</tr>
<tr>
<td>Encryption Priority</td>
<td>Select the check boxes for the desired Encapsulating Security Payload (ESP) authentication options. For highest security, use the arrows to change the order to the following: aes256, aes192, aes128, 3des.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>Select units and enter the length of time that the negotiated key will stay effective.</td>
</tr>
</tbody>
</table>

Defining IPSec Crypto Profiles

Use the IPSec Crypto Profiles page to specify protocols and algorithms for identification, authentication, and encryption in VPN tunnels based on IPSec SA negotiation (IKEv1 Phase-2). Refer to “About Virtual Private Networks” on page 190 for more information.

To create a new configuration, click New and specify the following information.

Table 96. IPSec Crypto Profile Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the profile.</td>
</tr>
<tr>
<td>HA Priority</td>
<td>Specify the priority for hash algorithms. For highest security, use the arrows to move sha1 to the top of the list.</td>
</tr>
<tr>
<td>ESP Authentication</td>
<td>Select the check boxes for the desired ESP authentication algorithms. For highest security, use the arrows to move sha1 to the top of the list and deselect None.</td>
</tr>
</tbody>
</table>
Setting Up IPSec Tunnels

To change the ordering in which an algorithm or group is listed, click the icon. The listed order determines the order in which the algorithms are applied and can affect tunnel performance.

Setting Up IPSec Tunnels

Network > IPSec Tunnels

Use the IPSec Tunnels page to set up the parameters to establish IPSec VPN tunnels between firewalls.

To create a new configuration, click New and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec Tunnel</td>
<td>Enter a name to identify the tunnel.</td>
</tr>
<tr>
<td>Tunnel Interface</td>
<td>Select an existing interface, or click New, enter the following information and click OK:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Tunnel Interface Name</strong>—Enter the new tunnel name.</td>
</tr>
<tr>
<td></td>
<td>• MTU—Enter the maximum transmission unit in bytes for packets sent on this Layer 3 interface (512-1500, default 1500).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The firewall automatically considers tunnel overhead when performing IP fragmentation and also adjusts the TCP maximum segment size (MSS) as needed.</td>
</tr>
<tr>
<td></td>
<td>• IP Address—Enter an IP address if dynamic routing is used.</td>
</tr>
<tr>
<td></td>
<td>• Management Profile—Select the management profile to associate to this interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Virtual Router</strong>—Select a virtual router for this interface, or click New to configure a new virtual router. Refer to “About Virtual Routers and Routing Protocols” on page 98.</td>
</tr>
<tr>
<td></td>
<td>• Zone—Select a security zone for this interface, or click New to configure a new zone. Refer to “Defining Security Zones” on page 97.</td>
</tr>
<tr>
<td>Type</td>
<td>Select whether to use an automatically generated or manually entered security key. <strong>Auto key</strong> is recommended.</td>
</tr>
</tbody>
</table>
## Setting Up IPSec Tunnels

**IKE Gateway**
Enter a name to identify the gateway.

**Local IP Address**
Select the IP address for the local interface that is the endpoint of the tunnel.
The second drop-down list displays all of the IP addresses that are assigned to the interface. If there are multiple IP addresses assigned to the interface, choose the one to use for the tunnel.

**Peer IP Address**
Enter a static IP address or select **Dynamic** for the peer IP address on the far end of the tunnel. If you select **Dynamic**, the additional fields described below in this table are displayed.

**Pre-shared key**
Enter a security key to use for authentication across the tunnel.

**Local Identification**
Choose from the following types and enter the value: Fully qualified domain name (FQDN), key ID, or user FQDN.

**Peer Identification**
Choose from the following types and enter the value: Fully qualified domain name (FQDN), key ID, or user FQDN.

**Exchange Mode**
Choose from the following modes:
- **main**—Specifies multiple two-way exchanges between the initiator and the receiver.
- **aggressive**—Specifies fewer exchanges than main mode. In this mode, both sides may exchange information before securing the channel.
- **auto**—Allows the firewall to connect to other machines that are configured to run in either main mode or aggressive mode.

As an initiator, the firewall will select aggressive mode if the local ID is configured to be anything other than the firewall’s IP address. Main mode will be used if the local ID is the firewall’s IP address.

**IKE Crypto Profile**
Select an existing profile or keep the default profile. To define a new profile, click **New** and follow the instructions in “Defining IKE Crypto Profiles” on page 195.

**Dead Peer Detection**
Select the check box to enable and enter an interval (2 - 100 sec) and delay before retrying (2 - 100 sec). Dead peer detection identifies inactive or unavailable IKE peers through ICMP ping and can help restore resources that are lost when a peer is unavailable.

**IPSec Crypto Profile**
Select an existing profile or keep the default profile. To define a new profile, click **New** and follow the instructions in “Defining IPSec Crypto Profiles” on page 195.

**Local Proxy ID**
Enter an IP address or subnet in the format `ip_address/mask` (for example, `10.1.2.1/24`).

**Remote Proxy ID**
If required by the peer, enter an IP address or subnet in the format `ip_address/mask` (for example, `10.1.1.1/24`).

---

### Table 97. IPSec Tunnel Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Gateway</td>
<td>Enter a name to identify the gateway.</td>
</tr>
<tr>
<td>Local IP Address</td>
<td>Select the IP address for the local interface that is the endpoint of the tunnel. The second drop-down list displays all of the IP addresses that are assigned to the interface. If there are multiple IP addresses assigned to the interface, choose the one to use for the tunnel.</td>
</tr>
<tr>
<td>Peer IP Address</td>
<td>Enter a static IP address or select <strong>Dynamic</strong> for the peer IP address on the far end of the tunnel. If you select <strong>Dynamic</strong>, the additional fields described below in this table are displayed.</td>
</tr>
<tr>
<td>Pre-shared key</td>
<td>Enter a security key to use for authentication across the tunnel.</td>
</tr>
<tr>
<td>Local Identification</td>
<td>Choose from the following types and enter the value: Fully qualified domain name (FQDN), key ID, or user FQDN.</td>
</tr>
<tr>
<td>Peer Identification</td>
<td>Choose from the following types and enter the value: Fully qualified domain name (FQDN), key ID, or user FQDN (for the dynamic option).</td>
</tr>
</tbody>
</table>
| Exchange Mode       | Choose from the following modes:  
  - **main**—Specifies multiple two-way exchanges between the initiator and the receiver.  
  - **aggressive**—Specifies fewer exchanges than main mode. In this mode, both sides may exchange information before securing the channel.  
  - **auto**—Allows the firewall to connect to other machines that are configured to run in either main mode or aggressive mode. As an initiator, the firewall will select aggressive mode if the local ID is configured to be anything other than the firewall’s IP address. Main mode will be used if the local ID is the firewall’s IP address. |
| IKE Crypto Profile  | Select an existing profile or keep the default profile. To define a new profile, click **New** and follow the instructions in “Defining IKE Crypto Profiles” on page 195. |
| Dead Peer Detection | Select the check box to enable and enter an interval (2 - 100 sec) and delay before retrying (2 - 100 sec). Dead peer detection identifies inactive or unavailable IKE peers through ICMP ping and can help restore resources that are lost when a peer is unavailable. |
| IPSec Crypto Profile| Select an existing profile or keep the default profile. To define a new profile, click **New** and follow the instructions in “Defining IPSec Crypto Profiles” on page 195. |
| Local Proxy ID      | Enter an IP address or subnet in the format `ip_address/mask` (for example, `10.1.2.1/24`). |
| Remote Proxy ID     | If required by the peer, enter an IP address or subnet in the format `ip_address/mask` (for example, `10.1.1.1/24`). |
Setting Up IPSec Tunnels

Keep the following in mind when configuring IPSec VPNs:

- There must be a route to the remote network that is being tunneled.

- Pre-shared keys may be entered incorrectly on one of the devices. Pre-shared keys must always match.

- Phase 1 negotiation mode (aggressive/main) may not match on the devices. The negotiation mode must always match.

- Perfect forward secrecy may be enabled on only one side. It must be enabled on both sides.

- If the dynamic routing protocols advertise routes to public IP addresses through the IPSec tunnel, the device establishing the tunnel may attempt phase 1 negotiation with the destination set to the public IP rather than the endpoint of the IPSec tunnel. As a result, the connection is never created and routing fails. To address this problem, ensure that only private IP addresses route through the tunnel and that no public IP addresses or default routes exist in the routing table that points to the tunnel.

### Table 97. IPSec Tunnel Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Protocol      | Configure the protocol and port numbers for the local and remote ports:  
  - any—Allow TCP and/or UDP traffic.  
  - TCP—Specify the local and remote TCP port numbers.  
  - UCP—Specify the local and remote UCP port numbers.  
  - Number—Specify the protocol number (used for interoperability with third-party devices). |
| Replay Protection | Select to detect and neutralize replay attacks on the decryption side. Replay attacks can be caused by attackers capturing and replaying legitimate IPSec packets or by malfunctioning network devices. |
| Copy TOS Header | Select this option to copy the Type of Service (TOS) value in the internal IP header to the outside IP header. This allows traffic to be processed by another networking device according to the original TOS value. |
| Tunnel Monitor | Configure these settings to monitor the state of the tunnel, including whether the peer is still responding to a heartbeat (and therefore has the correct runtime information) and the quality of the link (including average round trip time):  
  - Enable—Select to enable tunnel monitoring.  
  - Destination IP—Enter the IP address of the device that will receive the monitoring ICMP probe. If the peer device is another Palo Alto Networks firewall, use the IP address of the tunnel interface of the peer firewall as the destination IP address. If you do not do this, it may be necessary to configure a security policy on the peer firewall to permit the monitoring packets.  
  - Profile—Select a profile or click New to create a new tunnel monitoring profile. Enter a profile name, the type of action to take in response to state changes, the interval between ICMP probes, and a threshold, which is the number of failed probes indicating that the tunnel is down. |
Defining Tunnel Monitor Profiles

- A Proxy ID may be improperly entered for the device at the far end of the IPSec tunnel. This can occur because some vendors generate a default Proxy ID for IPSec communications that is not easily identified by the end user.

Defining Tunnel Monitor Profiles

► Network > Network Profiles > Monitor

A tunnel monitor profile specifies how the firewall monitors IPSec tunnels and the actions that are taken if the tunnel is not available. Tunnel monitor profiles are optional, but can be useful, for example, if you want to be able to provide failover in the event of tunnel failure.

After creating a tunnel monitor profile, you can select it in the advanced options section of the IPSec configuration page. The firewall then monitors the specified IP address through the tunnel to determine if the tunnel is working properly.

To create a new configuration, click New and specify the following information.

Table 98. Tunnel Monitor Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name (up to 31 characters) to identify the monitor profile.</td>
</tr>
<tr>
<td>Action</td>
<td>Specify an action to take if the tunnel is not available. If the threshold number of heartbeats is lost, the firewall takes the specified action.</td>
</tr>
<tr>
<td></td>
<td>• wait-recover — Wait for the tunnel to recover; do not take additional action.</td>
</tr>
<tr>
<td></td>
<td>• fail-over — Cause traffic to fail over to a backup path, if one is available.</td>
</tr>
<tr>
<td></td>
<td>In both cases, the firewall tries to negotiate new IPSec keys to accelerate the recovery.</td>
</tr>
<tr>
<td>Interval</td>
<td>Specify the time between heartbeats (range 2-10, default 3).</td>
</tr>
<tr>
<td>Threshold</td>
<td>Specify the number of heartbeats to be lost before the firewall takes the specified action (range 2-100, default 5).</td>
</tr>
</tbody>
</table>
Viewing IPSec Tunnel Status on the Firewall

Network > IPSec Tunnels

To view the status of currently defined IPSec VPN tunnels, open the IPSec Tunnels page (Figure 43).

![IPSec Tunnels Page]

The following status information is reported on the page:

- **Tunnel Status (first status column)**—Green indicates an IPSec SA tunnel. Red indicates that IPSec SA is not available or has expired.

- **IKE Gateway Status**—Green indicates a valid IKE phase-1 SA. Red indicates that IKE phase-1 SA is not available or has expired.

- **Tunnel Interface Status**—Green indicates that the tunnel interface is up (because tunnel monitor is disabled, or because tunnel monitor status is UP). Red indicates that the tunnel interface is down, because the tunnel monitor is enabled and the status is down.
Sample VPN Configuration

This section provides a sample VPN configuration. In this sample, a branch office is connected with a headquarters office and branch office users are allowed to access a central server farm. Refer to the following topics:

- “Existing Topology” in the next section
- “New Topology” on page 201
- “Configure the VPN Connection” on page 202
- “VPN Connectivity Troubleshooting” on page 203

Existing Topology

Headquarters:

- Firewall public IP 61.1.1.1, on interface ethernet1/1, which is in zone “ISP”, virtual-router “public”
- Server farm network is 10.100.0.0/16, connected through interface ethernet1/5 (IP 10.100.0.1), which is on zone “server”, virtual-router “internal”

Branch office:

- Firewall public IP is 202.101.1.1, on interface ethernet1/2, which is in zone “ISP-branch”, virtual-router “branch”
- A PC network of 192.168.20.0/24, connected through interface ethernet1/10, which is on zone “branch-office”, virtual-router “branch” (same as ethernet1/2)
- Security policy to allow traffic from zone “branch-office” to zone “ISP-branch” for internet access from the PC network

New Topology

Headquarters:

- Create a new security zone “branch-vpn.”
- Add a tunnel interface tunnel.1 to zone “branch-vpn” and assign an IP address from a private range (for example, 172.254.254.1/24)
- Add a static route to direct traffic to 192.168.20.0/24 (the branch office network) to the tunnel interface tunnel.1 and next hop 172.254.254.20 (the branch office tunnel interface IP).
- Add a security policy to allow traffic from zone “branch-vpn” to zone “server.”
Branch office:
- Create a new security zone “central-vpn.”
- Add a tunnel interface tunnel.2 to zone “central-vpn” and assign an IP address from private range (for example, 172.254.254.20/24).
- Add a static route to direct traffic to 10.100.0.0/16 (the server farm network) to the tunnel interface tunnel.2 and next-hop 172.254.254.1 (the headquarter tunnel interface IP).
- Add a security policy to allow traffic from zone “branch” to zone “central-vpn.”

Configure the VPN Connection

Headquarters:
- Create an IKE gateway “branch-1-gw” with these parameters:
  - Peer-address: dynamic (or 202.101.1.1)
  - Local-address: ethernet1/1
  - Peer-ID: type is FQDN: branch1.my.domain
  - Authentication: pre-shared-key newvpn
  - Protocol: keep default values
- Create an IPSec tunnel “branch-1-vpn” with these parameters:
  - ike-gateway-profile: “branch-1-gw”
  - ipsec-crypto-profile: leave as default
  - Tunnel interface: bind with tunnel.1
  - proxy-id: local 10.100.0.0/16, remote 192.168.20.0/24
- On servers in the server farm, check the routing table and verify that the destination 192.168.20.0/24 is reachable through 10.100.0.1.

Branch office:
- Create an IKE gateway “central-gw” with these parameters:
  - Peer-address: 61.1.1.1
  - Local-address: ethernet1/2
  - Local-ID: type is FQDN: “branch1.my.domain”
  - Authentication: pre-shared-key “newvpn”
  - Protocol: keep default values
• Create an IPSec tunnel “central -vpn” with these parameters:
  – ike-gateway-profile: “central -gw”
  – ipsec-crypto-profile: leave as default
  – Tunnel interface: bind with tunnel.2
  – proxy-id: local 192.168.20.0/24, remote 10.100.0.0/16

Configuration Notes:
• If 202.101.1.1 is set as the peer-address parameter in “branch-1-gw” on the central site, setting the local-id and peer-id parameters becomes unnecessary (the field can be left empty). Note that treatment of these two parameters must be the same, because these two fields are matched during IKE negotiation.

• The proxy-id can also be left empty on both sides (proxy-id is also matched during IKE negotiation).

After configuring the parameters and committing the configuration, the new VPN should work. If connectivity issues arise, refer to “VPN Connectivity Troubleshooting” in the next section.

VPN Connectivity Troubleshooting

Note: The parameter values in this section refer to the sample configuration. Refer to “Configure the VPN Connection” on page 202.

To troubleshoot issues regarding VPN connectivity:
1. Double check configurations on both sites.
2. Use the **ping** utility to verify connectivity between the central and branch offices (202.101.1.1 and 61.1.1.1).
3. Use the **ping** utility to verify connectivity between the server farm and the central firewall (ethernet1/5).
4. Use the **ping** utility to verify connectivity between the branch network and the branch firewall interface (ethernet1/10).
5. On the branch-office site, use the CLI commands **test vpn ike-sa gateway central-gw** and **show vpn ike-sa gateway central-gw** to verify that IKE phase-1 SA can be created from the branch office.
6. On the central site, use the CLI command **show vpn ike-sa gateway branch-1-gw** to verify that IKE phase-1 SA can be created from the branch office.
7. On the branch office site, use the CLI command **test vpn ipsec-sa tunnel central-vpn** and **show vpn ipsec-sa tunnel central-vpn** to verify that IKE phase-2 SA can be created from the branch office.
8. On the central site, use the CLI command **show vpn ipsec-sa tunnel branch-1-vpn** to verify that IKE phase-2 SA can be created from the branch office.
9. Check the server routing table in the server farm. The destination 192.169.20.0/24 must be reachable through the central firewall’s ethernet1/5 interface IP address.

10. To check the route setting, run the **traceroute** command from any PC in the branch office network, where the destination is one of servers in the server farm.

11. Run the **ping** utility from any PC in the branch office network, where the destination is one of servers in the server farm. Check the encryption and decryption counters shown in the output of the **show vpn flow** CLI command. Verify that these counters are incrementing and that none of the error counters are incrementing.

12. Examine the detailed error messages for IKE negotiation in the syslog or use the **debug ike pcap** command to capture IKE packets in PCAP format.
Chapter 8
Configuring SSL VPNs

This chapter describes how to configure virtual private networks (VPNs) using Secure Socket Layer (SSL).

- “About SSL VPNs” in the next section
- “How the SSL VPN Works” on page 206
- “Setting Up SSL VPNs” on page 207
- “Adding a new SSL VPN” on page 208
- “Downloading and Activating the NetConnect SSL VPN Client” on page 209
- “Creating a Local User Database” on page 210

Note: Refer to “Configuring IPSec Tunnels” on page 189 for general information on VPNs as well as information on IPSec VPNs.
About SSL VPNs

The SSL VPN capability allows the firewall to support VPN connections for remote Windows 7, Vista, and Windows XP users who require secure access to the corporate network. An SSL VPN establishes a secure connection between the remote user and the firewall. Users can access the SSL VPN through a web browser without having to first install a client application. This is in contrast with an IPSec VPN, which requires a previously-installed client application. For information on IPSec VPNs, refer to “Configuring IPSec Tunnels” on page 189.

To configure an SSL VPN, you define a profile and attach it as a virtual interface to a physical interface on the firewall. The SSL VPN virtual interface is mapped to a security zone, which can be subject to security policies. Configuration must be on a Layer 3 interface (it can be an aggregate interface). The user information for the SSL VPN sessions is added to the logs and security policies.

Note: Refer to “About Virtual Private Networks” on page 190 for information on setting up VPNs to connect Palo Alto Networks firewalls at central and remote sites or to connect Palo Alto Networks firewalls with third-party security devices at other locations.

How the SSL VPN Works

For a user who is connecting for the first time, the SSL VPN works as follows:

1. The user opens a browser and accesses the URL provided by the network administrator.

2. A login page opens and the user is prompted to enter a username and password.

3. After the user is successfully authenticated, the user can click the Start button to download the thin VPN client and install it on the user’s computer.

4. When the download is complete, the SSL VPN client automatically establishes a VPN tunnel connection. If possible, the tunnel will be established using IPSec; if this is not possible, the tunnel is established using SSL.

5. The tunnel is now established. Traffic is controlled at the gateway by use and application based on the established security policies. If split tunneling is enabled on the client, only the traffic bound for the network behind the gateway is sent through the firewall. All other traffic is sent directly to the Internet.

6. At the end of the session, the user can log off from the client, or simply shut down and let the VPN agent time out.

For a return user, the SSL VPN works as follows:

1. The user opens a browser and accesses the URL provided by the network administrator or launches the client that was previously installed.

2. The login page opens and the user is prompted to enter a username and password to authenticate successfully.
3. The tunnel is now established. Traffic is controlled at the gateway by use and application based on the security policies established. If split tunneling is enabled on the client, only the traffic bound for the network behind the gateway is sent through the firewall. All other traffic is sent directly to the Internet.

4. At the end of the session, the user can log off from the client, or simply shut down and let the VPN agent time out.

**Setting Up SSL VPNs**

The following tasks are required to set up and configure an SSL VPN:

1. Set up the SSL VPN on the firewall, as described in “Adding a new SSL VPN” on page 208.

2. Install or generate a self-signed security certificate for the SSL VPN client, as described in “Importing, Exporting and Generating Security Certificates” on page 77.

3. Download and activate the SSL VPN client on the client PC, as described in “Downloading and Activating the NetConnect SSL VPN Client” on page 209.

4. Set up user authentication rules for local or RADIUS authentication, as described in “Setting Up Authentication Profiles” on page 55.

5. Identify the users that are allowed to access the VPN, as described in “Creating a Local User Database” on page 210.

6. (Optional) Customize the response pages that users will see when using the VPN, as described in “Defining Custom Response Pages” on page 74.

7. Set up security policies for traffic flowing between the SSL VPN zone and other security zones, as described in “About Security Policies” on page 122.
Adding a new SSL VPN

Network > SSL VPN

The settings on the SSL VPN tab control the firewall configuration. The settings on the Client Configuration tab are pushed to the user’s computer to provide information on how to connect to the network. To change an entry, click the link for the entry.

Table 99. SSL VPN Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL VPN Configuration</td>
<td></td>
</tr>
<tr>
<td>Portal Name</td>
<td>Enter a name to identify the VPN.</td>
</tr>
<tr>
<td>Tunnel Interface</td>
<td>Choose the tunnel interface to use for the VPN from the drop-down list. This is the logical interface where the VPN tunnels will terminate, and the security zone for creating policy.</td>
</tr>
<tr>
<td>Max User</td>
<td>Enter the maximum number of users permitted to use the VPN simultaneously. Specifying a maximum number of users allows you to manage the load on the tunnel interface.</td>
</tr>
<tr>
<td>IPSec Enable</td>
<td>Select the check box if you want to try to use IPSec as the VPN protocol after the SSL VPN tunnel is established. This option can improve performance over the tunnel.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface to be used for the connection.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Choose the IP address that users will specify to access the VPN.</td>
</tr>
<tr>
<td>Client Configuration</td>
<td></td>
</tr>
<tr>
<td>Primary DNS</td>
<td>Enter the IP addresses of the primary and secondary Domain Name Service (DNS) servers that will be used on the clients.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td></td>
</tr>
<tr>
<td>Primary WINS</td>
<td>Enter the IP addresses of the primary and secondary Windows Name Service (WINS) servers that will be used on the clients.</td>
</tr>
<tr>
<td>Secondary WINS</td>
<td></td>
</tr>
<tr>
<td>DNS Suffix</td>
<td>Click Add to enter a suffix that the client should use locally when an unqualified hostname is entered that it cannot resolve. Suffixes are used in the order in which they are listed. To change the order in which a suffix is listed, select an entry and click the Move Up and Move Down buttons. To delete an entry, select it and click Remove.</td>
</tr>
<tr>
<td>IP Pool - Subnet/Range</td>
<td>Use this section to create a range of IP addresses to assign to remote users. When the tunnel is established, an interface is created on the remote user’s computer with an address in this range. Note: The IP pool must be large enough to support all concurrent connections. IP address assignment is dynamic and not retained after the user disconnects. Configuring multiple ranges from different subnets will allow the system to offer clients an IP address that does not conflict with other interfaces on the client. For example, for the 192.168.0.0/16 network, a remote user may be assigned the address 192.168.0.10.</td>
</tr>
</tbody>
</table>
Downloading and Activating the NetConnect SSL VPN Client

Device > SSL VPN Client

The SSL VPN Client page lists the available SSL VPN client releases. When the client connects, the system checks the NetConnect version and installs the currently activated version if it is different from the version that is on the client.

Note: For initial download and installation of the SSL VPN client, the user on the client system must be logged in with administrator rights. For subsequent upgrades of the SSL VPN client application, administrator rights are not required.

To download and activate the NetConnect SSL VPN client:

1. Click the Download link for the desired release. The download starts and a pop-up window opens to display the progress of the download. When the download is complete, click Close. To stop the download while it is in progress, click Cancel Download.

2. To activate a downloaded release, click the Activate link for the release. If an existing version of the SSL VPN client software has already been downloaded and activated, a pop-up message is displayed to indicate that the new version will be downloaded the next time that the clients connect. Click OK to continue or Cancel to cancel the request.

3. To activate the SSL VPN client that was previously uploaded by way of the Upload button, click the Activate from File button. A pop-up window opens. Select the file from the drop-down list and click OK.

4. To remove a downloaded release of the SSL VPN client software from the firewall, click the Remove icon in the rightmost column. Click Yes to confirm.
Creating a Local User Database

You can set up a database on the firewall to store authentication information for SSL VPN remote users and create users and user groups for database access.

Adding Local Users

Device > Local User Database > Users

Use the Local Users page to add user information. Click New and configure the following settings. To change an entry, click the link for the entry.

Table 100.  Local User Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local User Name</td>
<td>Enter a name to identify the user.</td>
</tr>
<tr>
<td>Virtual System</td>
<td>Select the virtual system from the drop-down list.</td>
</tr>
<tr>
<td>Mode</td>
<td>Use this field to choose the authentication option:</td>
</tr>
<tr>
<td></td>
<td>• Password—Enter and confirm a password for the user.</td>
</tr>
<tr>
<td></td>
<td>• Phash—Enter a hashed password string.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the check box to activate the user account.</td>
</tr>
</tbody>
</table>

Adding Local User Groups

Device > Local User Database > User Groups

Use the Local User Groups page to add user group information. Click New and configure the following settings. To change an entry, click the link for the entry.

Table 101.  Local User Group Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local User Group Name</td>
<td>Enter a name to identify the group.</td>
</tr>
<tr>
<td>Virtual System</td>
<td>Select the virtual system from the drop-down list.</td>
</tr>
<tr>
<td>All Local Users</td>
<td>Select check boxes for the users you want to add to the group.</td>
</tr>
</tbody>
</table>
Chapter 9
Configuring Quality of Service

This chapter describes how to configure quality of service (QoS) on the firewall:

- “About Firewall Support for QoS” in the next section
- “Configuring QoS for Firewall Interfaces” on page 212
- “Defining QoS Profiles” on page 214
- “Defining QoS Policies” on page 215
- “Displaying QoS Statistics” on page 217

About Firewall Support for QoS

The firewall supports fine grained QoS settings for clear text and tunneled traffic upon egress from the firewall. QoS profiles are attached to physical interfaces to specify how traffic classes map to bandwidth (guaranteed, maximum) and priority. QoS classification is supported with all interface types except Aggregate Ethernet.

The firewall supports the following QoS settings:

- On the QoS page (Network tab), you can configure QoS settings for firewall interfaces and the clear text and tunneled traffic that leaves the firewall through those interfaces, as described in “Configuring QoS for Firewall Interfaces” on page 212.

- For each interface, you can define QoS profiles that determine how the QoS traffic classes are treated. You can set overall limits on bandwidth regardless of class and also set limits for individual classes. You can also assign priorities to different classes. Priorities determine how traffic is treated when contention occurs. Refer to “Defining QoS Profiles” on page 214.

- On the QoS Policies page (Policies tab), you can configure the policies to activate the QoS restrictions. Refer to “Defining QoS Policies” on page 215.
Configuring QoS for Firewall Interfaces

**Issues to note when configuring firewall support for QoS**

- When setting up the QoS profile, the guaranteed and maximum egress settings defined for the classes must not exceed the guaranteed and maximum egress settings defined for the profile itself.

- Because traffic not marked by QoS defaults to Class 4, define Class 4 with a maximum guaranteed bandwidth and give it a higher priority than other classes.

- Each firewall model supports a maximum number of ports that can be configured with QoS:
  - PA-4060: 6 ports
  - PA-4050: 12 ports
  - PA4020: 12 ports
  - PA-2050: 6 ports
  - PA-2020: 6 ports
  - PA-500: 6 ports

**Configuring QoS for Firewall Interfaces**

- **Network > QoS**

  Use the QoS page to configure QoS settings for firewall interfaces. Click **New** and specify the following information.

**Table 102. QoS Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Interface</strong></td>
<td></td>
</tr>
<tr>
<td>Interface Name</td>
<td>Select the firewall interface.</td>
</tr>
<tr>
<td>Maximum Egress</td>
<td>Enter the limit on traffic leaving the firewall through this interface (Mbps).</td>
</tr>
<tr>
<td>Enable QoS</td>
<td>Select the check box to enable QoS features.</td>
</tr>
<tr>
<td>Clear Text Default Profile</td>
<td>Select the default QoS profiles for clear text and for tunneled traffic. You must specify a default profile for each. For clear text traffic, the default profile applies to all clear text traffic as an aggregate. For tunneled traffic, the default profile is applied individually to each tunnel that does not have a specific profile assignment in the detailed configuration section. For instructions on defining QoS profiles, refer to “Defining QoS Profiles” on page 214.</td>
</tr>
<tr>
<td>Tunnel Interface Default Profile</td>
<td></td>
</tr>
<tr>
<td>Guaranteed Egress</td>
<td>Enter the bandwidth that is guaranteed for tunneled traffic from this interface.</td>
</tr>
</tbody>
</table>
Configuring QoS for Firewall Interfaces

Maximum Egress
Enter the limit on traffic leaving the firewall through this interface (Mbps).

Detail Configuration
Use these settings to add additional granularity to the treatment of clear text traffic or to override the default profile assignment for specific tunnels. If this section is left blank, the values specified in Group Configuration are used.

For example, assume a configuration with two sites, one of which has a 45 Mbps connection and the other a T1 connection to the firewall. You can apply restrictive QoS settings to the T1 site so that the connection is not overloaded while also allowing more flexible settings for the site with the 45 Mbps connection.

To add granularity for clear text traffic, click the Clear Text tab, click Add, and then click individual entries to configure the following settings:

- **Name**—Enter a name to identify these settings.
- **Source Interface**—Select the firewall interface.
- **Source Subnet**—Select a subnet to restrict the settings to traffic coming from that source, or keep the default any to apply the settings to any traffic from the specified interface.
- **QoS Profile**—Select the QoS profile to apply to the specified interface and subnet. For instructions on defining QoS profiles, refer to “Defining QoS Profiles” on page 214.

*Note:* The QoS rules for clear text are applied in the specified order. To change the order, select the check box for the entry and click Move Up or Move Down.

To override the default profile for a specific tunnel, click the Tunneled Traffic tab, click Add, and then click individual entries to configure the following settings:

- **Tunnel Interface**—Select the tunnel interface on the firewall.
- **QoS Profile**—Select the QoS profile to apply to the specified tunnel interface.

To remove a clear text or tunneled traffic entry, select the check box for the entry and click Remove.

---

Table 102. QoS Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Egress</td>
<td>Enter the limit on traffic leaving the firewall through this interface (Mbps).</td>
</tr>
<tr>
<td>Detail Configuration</td>
<td>Use these settings to add additional granularity to the treatment of clear text traffic or to override the default profile assignment for specific tunnels. If this section is left blank, the values specified in Group Configuration are used.</td>
</tr>
</tbody>
</table>
Defining QoS Profiles

For each interface, you can define QoS profiles that determine how the QoS traffic classes are treated. You can set overall limits on bandwidth regardless of class and also set limits for individual classes. You can also assign priorities to different classes. Priorities determine how traffic is treated in the presence of contention.

**Note:** Refer to “Configuring QoS for Firewall Interfaces” on page 212 for information on configuring firewall interfaces for QoS and refer to “Defining QoS Policies” on page 215 to configure the policies that will activate the QoS restrictions.

To add a new profile, click **New** and specify the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Enter a name to identify the profile.</td>
</tr>
<tr>
<td>Guaranteed Egress</td>
<td>Enter the bandwidth that is guaranteed for this profile (Mbps).</td>
</tr>
<tr>
<td>Maximum Egress</td>
<td>Enter the maximum bandwidth allowed for this profile (Mbps).</td>
</tr>
<tr>
<td>Classes</td>
<td>Specify how to treat individual QoS classes. You can select one or more classes to configure:</td>
</tr>
<tr>
<td></td>
<td>• Class—If you do not configure a class, you can still include it in a QoS policy. In this case, the traffic is subject to overall QoS limits. The default class is 4.</td>
</tr>
<tr>
<td></td>
<td>• Guaranteed Egress—Click and enter a value (Mbps) for this class.</td>
</tr>
<tr>
<td></td>
<td>• Maximum Egress—Click and enter a value (Mbps) for this class.</td>
</tr>
<tr>
<td></td>
<td>• Priority—Click and select a priority to assign to this class. These are prioritized in the order listed (highest first):</td>
</tr>
<tr>
<td></td>
<td>− Real-time</td>
</tr>
<tr>
<td></td>
<td>− High</td>
</tr>
<tr>
<td></td>
<td>− Medium</td>
</tr>
<tr>
<td></td>
<td>− Low</td>
</tr>
<tr>
<td></td>
<td>When contention occurs, traffic that is assigned a lower priority is dropped. Real-time priority uses its own separate queue.</td>
</tr>
</tbody>
</table>

Table 103. QoS Profile Settings
Defining QoS Policies

The QoS policy determines how traffic is classified for treatment when it passes through an interface with QoS enabled. For each rule, you specify one of eight classes. You can also assign a schedule to specify which rule is active. Unclassified traffic is automatically assigned to class 4.

Note: Refer to “Configuring QoS for Firewall Interfaces” on page 212 for information on configuring firewall interfaces for QoS and refer to “Defining QoS Profiles” on page 214 for information on configuring classes of service.

To view just the rules for a specific virtual system, select the system from the Virtual System drop-down list and click Go. To apply a filter to the list, select from the Filter Rules drop-down list. To view just the rules for specific zones, select a zone from the Source Zone and/or Destination Zone drop-down lists, and click Filter by Zone.

Note: Shared policies pushed from Panorama are shown in green and cannot be edited at the device level.

To add a new QoS rule, do one of the following:

- Click Add Rule at the bottom of the page. A new rule with the default settings is added to the bottom of the list, and given the next highest rule number.

- Right-click on the number of a rule you want to copy, and select Clone Rule, or select a rule by clicking the white space of the rule, and select Clone Rule at the bottom of the page (a selected rule has a yellow background). The copied rule is inserted below the selected rule, and the subsequent rules are renumbered.

To configure a rule, click the entry in the table that you want to configure and specify changes, as described in the following table.

Table 104. QoS Rule Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Change the default rule name and/or enter a rule description. If you add a rule description, ☛ is added next to the rule name. By default, rules are named “rule&lt;n&gt;”, where n increases sequentially as rules are added. As rules are cloned, deleted, or moved, the rule names are not adjusted to match the rule numbers. Only the rule numbers in the first column determine the order in which the rules are compared against the network traffic.</td>
</tr>
<tr>
<td>Source Zone</td>
<td>Select one or more source and destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to “Defining Security Zones” on page 97.</td>
</tr>
<tr>
<td>Destination Zone</td>
<td>Select one or more source and destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to “Defining Security Zones” on page 97.</td>
</tr>
</tbody>
</table>
### Defining QoS Policies

**Source Address**
Specify a combination of source and destination IPv4 or IPv6 addresses for which the identified application can be overridden. To select specific addresses, choose select from the drop-down list and do any of the following:

- Select the check box next to the appropriate addresses and/or address groups in the Available column, and click Add to add your selections to the Selected column.
- Enter the first few characters of a name in the Search field to list all addresses and address groups that start with those characters. Selecting an item in the list will set the check box in the Available column. Repeat this process as often as needed, and then click Add.
- Enter one or more IP addresses (one per line), with or without a network mask. The general format is: \(<ip\textunderscore address>/<mask>\)
- To remove addresses, select the appropriate check boxes in the Selected column and click Remove, or select any to clear all addresses and address groups.

To add new addresses that can be used in this or other policies, click New Address (refer to “Defining Applications” on page 148). To define new address groups, refer to “Defining Address Groups” on page 143.

**Destination Address**

### Table 104. QoS Rule Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Specify a combination of source and destination IPv4 or IPv6 addresses for which the identified application can be overridden. To select specific addresses, choose select from the drop-down list and do any of the following:</td>
</tr>
<tr>
<td>Destination Address</td>
<td>• Select the check box next to the appropriate addresses and/or address groups in the Available column, and click Add to add your selections to the Selected column.</td>
</tr>
<tr>
<td></td>
<td>• Enter the first few characters of a name in the Search field to list all addresses and address groups that start with those characters. Selecting an item in the list will set the check box in the Available column. Repeat this process as often as needed, and then click Add.</td>
</tr>
<tr>
<td></td>
<td>• Enter one or more IP addresses (one per line), with or without a network mask. The general format is: (&lt;ip\textunderscore address&gt;/&lt;mask&gt;)</td>
</tr>
<tr>
<td></td>
<td>• To remove addresses, select the appropriate check boxes in the Selected column and click Remove, or select any to clear all addresses and address groups.</td>
</tr>
</tbody>
</table>

To add new addresses that can be used in this or other policies, click New Address (refer to “Defining Applications” on page 148). To define new address groups, refer to “Defining Address Groups” on page 143.

**Source User**
Click the link to identify the source users and groups to which the QoS policy will apply.

**Application**
Click the link to specify applications:

- Choose any to include all applications.
- Click Select to limit the applications. Select check boxes for the applications, and click Add to move the applications from the Available column to the Selected column. Click the + symbol to expand a listing or - to collapse the listing. To search for an application, enter all or part of the name in the Search field and press Enter. To remove an entry from the Selected column, select it and click Remove.
- To add a new application, click New Application. Refer to “Defining Applications” on page 148 for instructions on defining applications.
- Click OK.

**Service**
Click the link to specify the services to which this policy will apply.

To define new services, click New Service (refer to “Defining Services” on page 152). To define new service groups, refer to “Defining Service Groups” on page 153.

**Class**
Choose the QoS class to assign to the rule, and click OK. Class characteristics are defined in the QoS profile. Refer to “Defining QoS Profiles” on page 214 for information on configuring settings for QoS classes.
Displaying QoS Statistics

Network > QoS

The table on the QoS Policies page indicates when QoS is enabled, and includes a link to display QoS statistics. An example is shown in the following figure.

![QoS Statistics](image)

Figure 44. QoS Statistics

The left panel shows the QoS tree table, and the right panel shows data in the following tabs:

- **QoS Bandwidth**—Shows the real time bandwidth charts for the selected node and classes. The information is updated every two seconds.

- **Session Browser**—Lists the active sessions of the selected node and/or class.

- **Application View**—Lists all active applications for the selected QoS node and/or class.
Displaying QoS Statistics
This chapter describes how to install the Panorama centralized management system (CMS):

- “Installing Panorama” in the next section
- “Setting Up a Custom Virtual Disk” on page 220
- “Performing the Final Setup” on page 221
- “Accessing Panorama for the First Time” on page 221
- “Creating an SSL Certificate” on page 222

Note: Refer to “Central Management of Devices” on page 223 for information on using Panorama.

Installing Panorama

Follow these instructions to install Panorama on a Windows system.

To install Panorama on a Windows system:

1. If you do not already have VMware installed on the designated Panorama server, download and install VMware Player or VMware Server from http://www.vmware.com/download.
2. Insert the CD and copy the Panorama Appliance directory from the CD to the server.
3. Decompress the Panorama.zip file.
4. Launch VMware on the server.
5. Select File > Open within VMware and browse to the Panorama Appliance directory that was copied to the server.
6. Open the Panorama.vmdk file.
7. Click Start in VMware to start the Panorama application.
8. If you want to use less than 1G of memory for the guest OS that runs Panorama, select **Edit virtual machine settings** and adjust the amount of memory under the Memory device.

9. Click **Start this virtual machine**.

10. A pop-up window opens for creating a new ID. Verify that Create a new identifier is checked and click **OK**.

   The Panorama system will boot and displays the login prompt.

11. Log in using the default login **admin** and password **admin**.

---

### Setting Up a Custom Virtual Disk

The default Panorama installation is configured with a single disk partition for all data. On this partition, 10 GB of space is allocated for log storage. If this amount is not sufficient for your environment, you can create a custom virtual disk that is up to 950 GB.

To create a custom virtual disk:

1. Open VMware and select the Panorama virtual machine.

2. Click **Edit virtual machine settings**.

3. Click **Add** to launch the Add Hardware Wizard.

4. Choose **Hard Disk** and click **Next**.

5. Choose **Create a new virtual disk** and click **Next**.

6. Choose **SCSI** and click **Next**.

7. Enter settings for the new virtual disk and click **Next**.

8. Choose a location for the virtual disk and click **Finish**.

   A new SCSI disk appears in the list of devices for the virtual machine.

9. Start the Panorama virtual machine.

On the first start after adding the new disk, Panorama will initialize the new disk for use. This process takes several minutes. When the system starts with the new disk, any existing logs on the default disk are moved to the new disk, and all future logs are written to the new disk. If the virtual disk is removed, Panorama sends logs back to the default internal 10GB disk.
Performing the Final Setup

After installing Panorama, you must configure the IP address, netmask, and default gateway for the Panorama machine and enable the http service.

To configure the network interface:
1. Log in to the server console using the login admin and password admin.
2. Type `configure` to enter configuration mode:
   
   ```
   username@hostname> configure
   username@hostname#
   ```
3. Enter the following commands to assign and commit the network configuration for the server:
   
   ```
   username@hostname# set deviceconfig system ip-address <Panorama IP address> netmask <netmask> default-gateway <gateway IP address>
   username@hostname# commit
   ```
4. Connect the server to your network.

Accessing Panorama for the First Time

To log in to Panorama for the first time:
1. Launch your preferred web browser and enter `https://<Panorama IP address>`.
   The browser automatically opens the Palo Alto Networks login page.
2. Enter admin in both the Name and Password fields, and click Login.
3. Choose Panorama > Administrators > admin.
4. Enter admin in the Old Password field.
5. Enter a new password (case-sensitive, up to 15 characters) in the New Password field and re-enter the password in the Confirm New Password field.
6. Click OK.
7. Generate a self-signed security certificate, as described in “Importing, Exporting and Generating Security Certificates” on page 77.
8. Configure the serial numbers of the devices to be managed, as described in “Adding Devices” on page 227.
9. Verify that each managed device has the IP address of the Panorama server configured. Refer to “Defining the Host Name and Network Settings” on page 66.

Note: Refer to “Central Management of Devices” on page 223 for information on using Panorama.

Creating an SSL Certificate

To create an SSL certificate to encrypt the management connection to Panorama:

1. Click Panorama > Certificates > Generate a self signed certificate.
2. Enter the desired certificate details and click OK.
3. Click Commit to make the changes active.
Chapter 11
Central Management of Devices

This chapter describes how to use the Panorama centralized management system (CMS) to manage multiple firewalls:

- “Accessing the Panorama Interface” in the next section
- “About the Panorama Interface” on page 224
- “Adding Devices” on page 227
- “Defining Device Groups” on page 228
- “Managing Administrator Roles” on page 229
- “Specifying Access Domains for Administrators” on page 229
- “Upgrading the Panorama Software” on page 230
- “Backing Up Firewall Configurations” on page 230

Accessing the Panorama Interface

To access the Panorama interface, log in to the server and click the Panorama tab.
1. Launch your preferred web browser and enter https://<Panorama IP address>
   The browser automatically opens the Palo Alto Networks login page.
2. Enter the login name and password and click Login.
About the Panorama Interface

Panorama allows you to view information about multiple devices in your network and to manage devices from a central web interface. Figure 45 shows the Panorama interface, which is similar to the interface for the firewall. The pages for each tab are listed in the left pane.

To display information regarding the Palo Alto Networks firewalls in the network, the devices must be connected to the Panorama server.

Perform these steps to allow the devices to connect:

1. Add the IP address of the Panorama server to each device. Refer to “Defining the Host Name and Network Settings” on page 66.

2. Use the Panorama interface to add the devices. Refer to “Adding Devices” on page 227.

You can access all of the Panorama tabs whether or not devices are connected to the Panorama server; however, you can only view device information on devices that are connected.

Figure 45. Panorama Interface
The Panorama tabs are listed in the following table.

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Displays general information about the managed devices, such as the software version, the operational status of each interface resource utilization, and up to 10 of the most recent entries in the threat, configuration, and system logs. All of the available charts are displayed by default, but each user can remove and add individual charts, as needed.</td>
</tr>
<tr>
<td>ACC</td>
<td>Displays the overall risk and threat levels for the managed devices. Refer to “Using the Application Command Center” on page 163 and “Identifying Unknown Applications and Taking Action” on page 185.</td>
</tr>
<tr>
<td>Monitor</td>
<td>Allows you to view logs and reports. Refer to “Viewing Reports” on page 183.</td>
</tr>
</tbody>
</table>
| Objects | Allows you to define policy objects that are shared across the managed firewalls. Refer to “About Security Profiles” on page 132 for information on the pages in this tab. The following modifications apply to the tab within Panorama:  
  • There is no select menu for the virtual system at the top.  
  • There is no Shared column or check box in any of the pages, because all Panorama objects are shared.  
  • Log destinations, which you specify under the Device tab for the firewall are included in the Objects tab in Panorama. Refer to “About Log Destinations” on page 61. |
| Policies | Allows you to define policies that are shared across the managed firewalls. Refer to “About Security Policies” on page 122 for information on the pages in this tab. The following modifications apply to the tab within Panorama:  
  • A Device Group drop-down list, which allows you to restrict the policy to a specified set of firewalls, replaces the Virtual System drop-down list.  
  • Zones are not created in Panorama; therefore, you must enter a zone name when you first create a rule. For subsequent rules, you can enter new zones or select from previously entered zones.  
  • Each policy type listed on the side menu includes pages to define pre-rules and post-rules. Click the Pre-Rule or Post-Rule link, enter the From and To zone, and click OK.   
    – A pre-rule that is assigned to specified firewalls always precedes any device-specific rules.  
    – A post-rule that is assigned to specified firewalls always follows any device-specific rules.  
  • You cannot manage Network Address Translation (NAT) policies from Panorama, because addresses in NAT rules are specific to the firewall and not typically shared.  
  • For SSL Decryption rules, only the forward-proxy option is available for the Certificates field. There are no shared certificates. |
| Panorama | Allows you to configure and supervise the managed devices. Refer to “Panorama Tab” in the next section                                                                                                       |
**Panorama Tab**

The Panorama tab is similar to the interface for the firewall and includes the pages described in the following table. To access a page, click the page name link on the left pane.

**Table 106. Summary of Panorama Pages**

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
<td>Allows you to specify the host name of the firewall, the network settings of the management interface, and the addresses of various network servers (Panorama, DNS, NTP, and RADIUS). Refer to “Defining the Host Name and Network Settings” on page 66 for information on using this page.</td>
</tr>
<tr>
<td>Config Audit</td>
<td>Allows you to view and compare firewall configuration files. Refer to “Comparing Configuration Files” on page 71 for information on using this page.</td>
</tr>
<tr>
<td>Managed Devices</td>
<td>Allows you to add devices for management by Panorama. Refer to “Adding Devices” on page 227 for information on using this page.</td>
</tr>
<tr>
<td>Device Groups</td>
<td>Allows you to define sets of devices that are treated as a unit when applying policies in Panorama. Refer to “Defining Device Groups” on page 228 for information on using this page.</td>
</tr>
<tr>
<td>Admin Roles</td>
<td>Allows you to specify the privileges and responsibilities that are assigned to users who require access to Panorama. Refer to “Defining Administrator Roles” on page 54 for information on using this page.</td>
</tr>
</tbody>
</table>
| Administrators     | Allows you to define the accounts for users who require access to Panorama. Refer to “Creating Administrative Accounts” on page 57 for information on using this page.  

*Note:* On the Administrator’s page for “super user,” a lock icon is shown in the right column if an account is locked out. The administrator can click the icon to unlock the account.

| Certificates        | Allows you to manage web interface and Panorama server certificates. Refer to “Importing, Exporting and Generating Security Certificates” on page 77 for information on using this page. |
| Log Destinations    | Allows you to define SNMP trap sinks, syslog servers, and email addresses for distributing log messages. Refer to “About Log Destinations” on page 61 for information on using this page. |
| Software            | Allows you to view the available Panorama software releases and download and install a selected software version. Refer to the instructions in “Upgrading the Panorama Software” on page 230. |
| Dynamic Updates     | Allows you to view the latest application definitions and information on new security threats, such as antivirus signatures (threat prevention license required) and update Panorama with the new definitions. Refer to “Updating Threat and Application Definitions” on page 76 for information on using this page. |
| Support             | Allows you to access product and security alerts from Palo Alto Networks. Refer to the information in “Viewing Support Information” on page 80. |
Adding Devices

Viewing Information on Individual Devices

Use the Context drop-down list above the left pane of the Panorama interface to choose an individual device or the full Panorama view. You can select the name of any device that has been added for management by Panorama (refer to “Adding Devices” on page 227). When you select a device, the web interface refreshes to show all the device tabs and options, allowing you to manage all aspects of the device from Panorama.

![Choosing Device Context](image)

Figure 46. Choosing Device Context

Adding Devices

1. Under the Panorama tab, click Managed Devices to open the Managed Devices page.
2. To group the devices according to device or device group, select from the Group by drop-down list.
3. Click Add/Remove Devices to open an editing window.
4. Enter the serial number of the device to be added, and click Add.
5. Add additional devices, as needed.
6. Click OK. The window closes and the Managed Devices page refreshes to show the newly added devices.
7. To commit all shared policies to a device, click the icon in the Commit All column. The devices initiate the connection with Panorama. When a communication link is established, the host name and IP address are automatically added to the list, and the Connected column indicates that the device is connected. The shared policies are pushed to the device and committed. The currently running configuration on the device is overridden.

Note: The Panorama server communicates with managed devices via SSL through TCP port 3978.
Defining Device Groups

8. To delete a device:
   a. Click **Add/Remove Devices** to open the editing window.
   b. Select the check box for the device, and click **Delete**.
   c. Click **OK**.

---

**Defining Device Groups**

▶ **Panorama > Device Groups**

You can define device groups, which are treated as a single unit when applying policies in Panorama. This page lists the device groups along with the following information.

**Table 107. Device Group Information**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device group. Click the link to edit the group.</td>
</tr>
<tr>
<td>Master Device</td>
<td>Representative device from which the user information is gathered. The</td>
</tr>
<tr>
<td></td>
<td>information is used for shared policy configuration.</td>
</tr>
<tr>
<td>Device</td>
<td>Devices included in the group.</td>
</tr>
<tr>
<td>Virtual Systems</td>
<td>Virtual systems for the devices included in the group.</td>
</tr>
</tbody>
</table>

To add a new device group, click **New** and specify the following information.

**Table 108. Device Groups Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Group Name</td>
<td>Enter a name to identify the group.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the group.</td>
</tr>
<tr>
<td>Devices</td>
<td>Select devices from the available list and click <strong>Add</strong> to move them to</td>
</tr>
<tr>
<td></td>
<td>the select list.</td>
</tr>
<tr>
<td>Master Device</td>
<td>Select the device from which the user information is gathered. The</td>
</tr>
<tr>
<td></td>
<td>information is used for shared policy configuration.</td>
</tr>
</tbody>
</table>
Managing Administrator Roles

- **Panorama > Admin Roles**

You can specify the access and responsibilities that should be assigned to administrative users.

To define administrator roles click **New** and specify the following information.

<table>
<thead>
<tr>
<th>Table 109. New Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Profile Name</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Admin Role</td>
</tr>
</tbody>
</table>
| CLI Role                    | Select the type of role for CLI access:  
  - **Disable**—Access to the device CLI not permitted.  
  - **Superuser**—Full access to the current device.  
  - **Superuser (Read Only)**—Read-only access to the current device.  
  - **Device Admin**—Full access to a selected device, except for defining new accounts or virtual systems.  
  - **Device Admin (Read Only)**—Read-only access to a selected device. |
| WebUI Role                  | Click the icons for specified areas to indicate the type of access permitted in the web interface:  
  - 🖨️ Read/write access to the indicated page.  
  - 🖼️ Read only access to the indicated page.  
  - ☠️ No access to the indicated page. |

Specifying Access Domains for Administrators

- **Panorama > Access Domain**

Use the Access Domain page to specify the domains for administrator access to devices and device groups. Click **New** and specify the following information.

<table>
<thead>
<tr>
<th>Table 110. Access Domain Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Devices</td>
</tr>
<tr>
<td>Device Groups</td>
</tr>
</tbody>
</table>
Upgrading the Panorama Software

To upgrade to a new release of Panorama software, you can view the latest versions of the Panorama software available from Palo Alto Networks, read the release notes for each version, and then select the release you want to download and install (a support license is required).

To upgrade the Panorama software, click Refresh to view the latest software releases available from Palo Alto Networks. To view a description of the changes in a release, click Release Notes next to the release.

1. To install a new release:
   a. Click Download next to the release to be installed. When the download is complete, a checkmark is displayed in the Downloaded column.
   b. To install a downloaded release, click Install next to the release.

   When the installation is complete, you will be logged out while the Panorama system is restarted.

2. To delete an outdated release, click  next to the release.

Backing Up Firewall Configurations

Panorama automatically saves every committed configured from the managed firewalls. You can configure the number of versions to keep on the Panorama device by using the Management settings under Setup on the Panorama tab. The default is 100. For instructions on configuring the number of versions, refer to “Defining the Host Name and Network Settings” on page 66.

To manage backups on Panorama, click Manage in the Backups column for a device. A window opens to show the saved and committed configurations for the device.

Click a Load to restore the selected configuration to the device. To remove a saved configuration, click the  icon.
Appendix A

Custom Pages

Custom response pages allow you to notify end users of policy violations and special access conditions. Each page can include references to the user’s IP address, the URL for which access is attempted, and the URL category. These parameters can also be used in links to trouble-ticketing systems.

This appendix provides HTML code for the following default custom response pages:

- “Default Antivirus Response Page” in the next section
- “Default Application Block Page” on page 233
- “Default File Blocking Block Page” on page 233
- “Default URL Filtering Response Page” on page 234
- “Default Anti-Spyware Download Response Page” on page 235
- “Default SSL Decryption Opt-out Response Page” on page 235
- “Captive Portal Comfort Page” on page 236
- “URL Filtering Continue and Override Page” on page 236
- “SSL VPN Login Page” on page 237
- “SSL Certificate Revoked Notify Page” on page 238

Note: For information on importing and exporting custom response pages, refer to “Defining Custom Response Pages” on page 74.

Default Antivirus Response Page

```html
<html>
<head>
<meta http-equiv=Content-Type content="text/html; charset=windows-1252">
<meta name=Generator content="Microsoft Word 11 (filtered)">
<title>This is a test</title>
<style>
<!--
/* Font Definitions */
@font-face
{font-family:"Microsoft Sans Serif";
```
This is a test.
Default Application Block Page

<html>
<head>
<title>Application Blocked</title>
</head>
<body bgcolor="#e7e8e9">
<div id="content">
<h1>Application Blocked</h1>
<p>Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.</p>
<p><b>User:</b> <user/> </p>
<p><b>Application:</b> <appname/> </p>
</div>
</body>
</html>

Default File Blocking Block Page

<html>
<head>
<meta http-equiv=Content-Type content="text/html; charset=windows-1252">
<title>This is a test</title>
</head>
<body>
<h4>This is a test</h4>
</body>
</html>
This is a test.

Default URL Filtering Response Page

Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User:

URL:

Category:
Default Anti-Spyware Download Response Page

<Application-type>
<Category>
  <Entry name="networking" id="1">
    <Subcategory>
      <Entry name="remote-access" id="1"/>
      <Entry name="proxy" id="2"/>
      <Entry name="encrypted-tunnel" id="3"/>
      <Entry name="routing" id="4"/>
      <Entry name="infrastructure" id="5"/>
      <Entry name="ip-protocol" id="6"/>
    </Subcategory>
  </Entry>
  <Entry name="collaboration" id="2">
    <Subcategory>
      <Entry name="email" id="7"/>
      <Entry name="instant-messaging" id="8"/>
      <Entry name="social-networking" id="9"/>
      <Entry name="internet-conferencing" id="10"/>
      <Entry name="voip-video" id="11"/>
    </Subcategory>
  </Entry>
  <Entry name="media" id="3">
    <Subcategory>
      <Entry name="video" id="12"/>
      <Entry name="gaming" id="13"/>
      <Entry name="audio-streaming" id="14"/>
    </Subcategory>
  </Entry>
  <Entry name="business-systems" id="4">
    <Subcategory>
      <Entry name="auth-service" id="15"/>
      <Entry name="database" id="16"/>
      <Entry name="erp-crm" id="17"/>
      <Entry name="general-business" id="18"/>
      <Entry name="management" id="19"/>
      <Entry name="office-programs" id="20"/>
      <Entry name="software-update" id="21"/>
      <Entry name="storage-backup" id="22"/>
    </Subcategory>
  </Entry>
  <Entry name="general-internet" id="5">
    <Subcategory>
      <Entry name="file-sharing" id="23"/>
      <Entry name="internet-utility" id="24"/>
    </Subcategory>
  </Entry>
</Category>
<Technology>
  <Entry name="network-protocol" id="1"/>
  <Entry name="client-server" id="2"/>
  <Entry name="peer-to-peer" id="3"/>
  <Entry name="web-browser" id="4"/>
</Technology>
</Application-type>

Default SSL Decryption Opt-out Response Page

<h1>SSL Inspection</h1>
<p>In accordance with company security policy, the SSL encrypted connection you have initiated will be temporarily unencrypted so that it can be inspected for viruses, spyware, and other malware.</p>
<p>After the connection is inspected it will be re-encrypted and sent to its destination. No data will be stored or made available for other purposes.</p>
<p>IP: <url/></p>
<p>Category: <category/></p>
Captive Portal Comfort Page

<h1 ALIGN=CENTER>Captive Portal</h1>

<h2 ALIGN=LEFT>In accordance with company security policy, you have to authenticate before accessing the network.</h2>

URL Filtering Continue and Override Page

<html>
<head>
<title>Web Page Blocked</title>
<style>
#content{border:3px solid#aaa;background-color:#fff;margin:40;padding:40;font-family:Tahoma,Helvetica,Arial,sans-serif;font-size:12px;}
  h1{font-size:20px;font-weight:bold;color:#196390;}
b{font-weight:bold;color:#196390;}
  form td, form input {
    font-size: 11px;
    font-weight: bold;
  }
  #formtable {
    height: 100%;
    width: 100%;
  }
  #formtd {
    vertical-align: middle;
  }
  #formdiv {
    margin-left: auto;
    margin-right: auto;
  }
</style>
<script type="text/javascript">
function pwdCheck() {
  if(document.getElementById("pwd")) {
    document.getElementById("continueText").innerHTML = "If you require access to this page, have an administrator enter the override password here:"
  }
}
</script>
</head>
<body bgcolor="#e7e8e9">
<div id="content">
<h1>Web Page Blocked</h1>
<p>Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.</p>
<p>User:</p><user/>
<p>URL:</p><url/>
<p>Category:</p><category/>
<hr>
<p id="continueText">If you feel this page has been incorrectly blocked, you may click Continue to proceed to the page. However, this action will be logged.</p>
</div>
</body>
</html>
SSL VPN Login Page

<html>
<head>
<title>Palo Alto Networks - SSL VPN</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link rel="stylesheet" type="text/css" href="/styles/falcon_content.css?v=@@version">
<style>
  td { 
    font-family: Verdana, Arial, Helvetica, sans-serif; 
    font-weight: bold; 
    color: black; /*#FFFFFF; */
  }
  .msg { 
    background-color: #ffff99; 
    border-width: 2px; 
    border-color: #ff0000; 
    border-style: solid; 
    padding-left: 20px; 
    padding-right: 20px; 
    max-height: 150px; 
    height: expression( this.scrollHeight > 150 ? "150px" : "auto" ); /* sets 
max-height for IE */ 
    overflow: auto; 
  }
  .alert {font-weight: bold; color: red;}
</style>
</head>
<body bgcolor="#F2F6FA">
<table style="background-color: white; width:100%; height:45px; border-bottom: 2px solid #888888;">
  <tr style="background-image:url(/images/logo_pan_158.gif); background-repeat: no-repeat;">
    <td align="left">&nbsp;</td>
  </tr>
</table>

<div align="center">
  &lt;h1&gt;Palo Alto Networks - SSL VPN Portal&lt;/h1&gt;
</div>

<div id="formdiv">
  &lt;pan_form/&gt;
</div>
</body>
</html>
SSL Certificate Revoked Notify Page

<html>
<head>
<title>Certificate Error</title>
<style>
#content{border:3px solid#aaa;background-color:#fff;margin:40;padding:40;font-family:Tahoma,Helvetica,Arial,sans-serif;font-size:12px;}

h1{font-size:20px;font-weight:bold;color:#196390;}

b{font-weight:bold;color:#196390;}
</style>
</head>
<body bgcolor="#e7e8e9">
<div id="content">
<h1>Certificate Error</h1>
<p>There is an issue with the SSL certificate of the server you are trying to contact.</p>
<p><b>Certificate Name:</b> <certname/> </p>
<p><b>IP:</b> <url/> </p>
<p><b>Issuer:</b> <issuer/> </p>
<p><b>Status:</b> <status/> </p>
<p><b>Reason:</b> <reason/> </p>
</div>
</body>
</html>
Appendix B

Application Categories, Subcategories, Technologies, and Characteristics

The appendix lists application-related categories defined by Palo Alto Networks:

- “Application Categories and Subcategories” in the next section
- “Application Technologies” on page 241
- “Application Characteristics” on page 241

Application Categories and Subcategories

The following application categories and subcategories are supported:

- business-system
  - auth-service
  - database
  - erp-crm
  - general-business
  - infrastructure
  - management
  - office-program
  - software-update
  - storage-backup

- collaboration
  - email
  - instant-messaging
  - internet-conferencing
  - internet-utility
Application Categories and Subcategories

- social-networking
- voip-video
- web-posting
- general-internet
  - email
  - file-sharing
  - internet-utility
- media
  - audio-streaming
  - gaming
  - photo-video
- networking
  - audio-streaming
  - encrypted-tunnel
  - infrastructure
  - ip-protocol
  - proxy
  - remote-access
  - routing
- unknown
Application Technologies

The following application technologies are supported.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-protocol</td>
<td>An application that is generally used for system to system communication that facilitates network operation. This includes most of the IP protocols.</td>
</tr>
<tr>
<td>client-server</td>
<td>An application that uses a client-server model where one or more clients communicate with a server in the network.</td>
</tr>
<tr>
<td>peer-to-peer</td>
<td>An application that communicates directly with other clients to transfer information instead of relying on a central server to facilitate the communication.</td>
</tr>
<tr>
<td>browser-based</td>
<td>An application that relies on a web browser to function.</td>
</tr>
</tbody>
</table>

Application Characteristics

The following application characteristics are supported.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfers Files</td>
<td>Has the capability to transfer a file from one system to another over a network.</td>
</tr>
<tr>
<td>Evasive</td>
<td>Uses a port or protocol for something other than its originally intended purpose with the hope that it will traverse a firewall.</td>
</tr>
<tr>
<td>Excessive Bandwidth</td>
<td>Consumes at least 1 Mbps on a regular basis through normal use.</td>
</tr>
<tr>
<td>Used by Malware</td>
<td>Malware has been known to use the application for propagation, attack, or data theft, or is distributed with malware.</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Has publicly reported vulnerabilities.</td>
</tr>
<tr>
<td>Prone to Misuse</td>
<td>Often used for nefarious purposes or is easily set up to expose more than the user intended.</td>
</tr>
<tr>
<td>Widely Used</td>
<td>Likely has more than 1,000,000 users.</td>
</tr>
<tr>
<td>Tunnels Other Applications</td>
<td>Is able to transport other applications inside its protocol.</td>
</tr>
<tr>
<td>Continue Scanning for Other Applications</td>
<td>Instructs the firewall to continue looking to see if other application signatures match. If this option is not selected, the first matching signature is reported and the firewall stops looking for additional matching applications.</td>
</tr>
</tbody>
</table>
Appendix C

Federal Information Processing Standards Support

You can configure the firewall to support the Federal Information Processing Standards 140-2 (FIPS 140-2), which are used by civilian U.S. government agencies and government contractors.

To enable FIPS mode on a software version that supports FIPS, boot the firewall into maintenance mode and then select Set FIPS Mode from the main menu.

For instructions on booting to maintenance mode, refer to the PAN-OS Command Line Interface Reference Guide.

When FIPS is enabled, the following apply:

- To log into the firewall, the browser must be TLS 1.0 compatible.
- All passwords on the firewall must be at least six characters.
- Accounts are locked after the number of failed attempts that is configured on the Device > Setup > Management page. If the firewall is not in FIPS mode, it can be configured so that it never locks out; however in FIPS mode, and lockout time is required.
- The firewall automatically determines the appropriate level of self-testing and enforces the appropriate level of strength in encryption algorithms and cipher suites.
- Non-FIPS approved algorithms are not decrypted and are thus ignored during SSL decryption.
- When configuring IPSec, a subset of the normally available cipher suites is available.
- Self-generated and imported certificates must contain public keys that are 2048 bits (or more).
- The serial port is disabled.
- Telnet, TFTP, and HTTP management connections are unavailable.
- Surf control is not supported.
- High availability encryption is required.
- PAP authentication is disabled.
- Log forwarding is not supported.
Appendix D
Open Source Licenses

The software included in this product contains copyrighted software that is licensed under the General Public License (GPL). A copy of that license is included in this document. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of this product by sending a money order or check for $5 to:

Palo Alto Networks
Open Source Request
232 E. Java Drive
Sunnyvale, CA

Some components of this product may be covered under one or more of the open source licenses listed in this appendix:

- “Artistic License” on page 246
- “BSD” on page 247
- “GNU General Public License” on page 248
- “GNU Lesser General Public License” on page 252
- “MIT/X11” on page 258
- “OpenSSH” on page 258
- “PSF” on page 262
- “PHP” on page 262
- “Zlib” on page 263
Artistic License

This document is freely plagiarised from the 'Artistic Licence', distributed as part of the Perl v4.0 kit by Larry Wall, which is available from most major archive sites.

This document's purpose is to state the conditions under which these Packages (see definition below) viz: "Crack", the Unix Password Cracker, and "CrackLib", the Unix Password Checking library, which are held in copyright by Alec David Edward Muffett, may be copied, such that the copyright holder maintains some semblance of artistic control over the development of the packages, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:
A "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification, or segments thereof.
"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.
"Copyright Holder" is whoever is named in the copyright or copyrights for the package.
"You" is you, if you're thinking about copying or distributing this Package.
"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)
"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.
2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.
3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when AND WHY you changed that file, and provided that you do at least ONE of the following:
a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.
b) use the modified Package only within your corporation or organization.
c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide separate documentation for each non-standard executable that clearly documents how it differs from the Standard Version.
d) make other distribution arrangements with the Copyright Holder.
4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:
a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.
b) accompany the distribution with the machine-readable source of the Package with your modifications.
c) accompany any non-standard executables with their corresponding Standard Version
executables, giving the non-standard executables non-standard names, and clearly
documenting the differences in manual pages (or equivalent), together with instructions on
where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may
charge any fee you choose for support of this Package. YOU MAY NOT CHARGE A FEE FOR
THIS PACKAGE ITSELF. However, you may distribute this Package in aggregate with other
(possibly commercial) programs as part of a larger (possibly commercial) software
distribution provided that YOU DO NOT ADVERTISE this package as a product of your own.

6. The name of the Copyright Holder may not be used to endorse or promote products
derived from this software without specific prior written permission.

7. THIS PACKAGE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

---

**BSD**

The following copyright holders provide software under the BSD license:

- Julian Steward
- Thai Open Source Software Center Ltd
- The Regents of the University of California
- Nick Mathewson
- Niels Provos
- Dug Song
- Todd C. Miller
- University of Cambridge
- Sony Computer Science Laboratories Inc.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions
and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
GNU General Public License

Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble:
The licenses for most software are designed to take away your freedom to share and change it.
By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.
This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
GNU Lesser General Public License

Version 2.1, February 1999
Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble:
The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author’s reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.
When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".) "Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.
1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) The modified work must itself be a software library.
   b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
   d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.
4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in
object code or executable form under the terms of Sections 1 and 2 above provided that you
accompany it with the complete corresponding machine-readable source code, which must be
distributed under the terms of Sections 1 and 2 above on a medium customarily used for
software interchange.

If distribution of object code is made by offering access to copy from a designated place, then
offering equivalent access to copy the source code from the same place satisfies the
requirement to distribute the source code, even though third parties are not compelled to copy
the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work
with the Library by being compiled or linked with it, is called a "work that uses the Library".
Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside
the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is
a derivative of the Library (because it contains portions of the Library), rather than a "work
that uses the library". The executable is therefore covered by this License. Section 6 states
terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library,
the object code for the work may be a derivative work of the Library even though the source
code is not. Whether this is true is especially significant if the work can be linked without the
Library, or if the work is itself a library. The threshold for this to be true is not precisely
defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors,
and small macros and small inline functions (ten lines or less in length), then the use of the
object file is unrestricted, regardless of whether it is legally a derivative work. (Executables
containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the
work under the terms of Section 6. Any executables containing that work also fall under
Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the
Library" with the Library to produce a work containing portions of the Library, and distribute
that work under terms of your choice, provided that the terms permit modification of the
work for the customer's own use and reverse engineering for debugging such modifications.
You must give prominent notice with each copy of the work that the Library is used in it and
that the Library and its use are covered by this License. You must supply a copy of this
License. If the work during execution displays copyright notices, you must include the
copyright notice for the Library among them, as well as a reference directing the user to the
copy of this License. Also, you must do one of these things:

* a) Accompany the work with the complete corresponding machine-readable source code
for the Library including whatever changes were used in the work (which must be distributed
under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with
the complete machine-readable "work that uses the Library", as object code and/or source
code, so that the user can modify the Library and then relink to produce a modified executable
containing the modified Library. (It is understood that the user who changes the contents of
definitions files in the Library will not necessarily be able to recompile the application to use
the modified definitions.)

* b) Use a suitable shared library mechanism for linking with the Library. A suitable
mechanism is one that (1) uses at run time a copy of the library already present on the user's
computer system, rather than copying library functions into the executable, and (2) will
operate properly with a modified version of the library, if the user installs one, as long as the
modified version is interface-compatible with the version that the work was made with.
* c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

* d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

* e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the “work that uses the Library” must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

* a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

* b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients’ exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license
would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A
FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF
SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
DAMAGES.

MIT/X11

Copyright (C) 2001-2002 Daniel Veillard. All Rights Reserved.
Copyright (C) 2001-2002 Thomas Broyer, Charlie Bozeman and Daniel Veillard. All Rights
Reserved.
Copyright (C) 1998 Bjorn Reese and Daniel Stenberg.
Copyright (C) 2000 Gary Pennington and Daniel Veillard.
Copyright (C) 2001 Bjorn Reese <breese@users.sourceforge.net>
Copyright (c) 2001, 2002, 2003 Python Software Foundation
Copyright (c) 2004-2008 Paramjit Oberoi <param.cs.wisc.edu>
Copyright (c) 2007 Tim Lauridsen <tla@rasmil.dk>
Permission is hereby granted, free of charge, to any person obtaining a copy of this software
and associated documentation files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or
substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER
IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.

OpenSSH

This file is part of the OpenSSH software.
The licences which components of this software fall under are as follows. First, we will
summarize and say that all components are under a BSD licence, or a licence more free than
that.
OpenSSH contains no GPL code.
1) Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved
As far as I am concerned, the code I have written for this software can be used freely for any
purpose. Any derived versions of this software must be clearly marked as such, and if the
derived work is incompatible with the protocol description in the RFC file, it must be called by
a name other than "ssh" or "Secure Shell".
[Tatu continues]
However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details. However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code
Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futornsky <futo@core-sdi.com> <http://www.core-sdi.com>

3) ssh-keyscan was contributed by David Mazieres under a BSD-style license.
Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)
Optimised ANSI C code for the Rijndael cipher (now AES)
@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
@author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5) One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

The Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6) Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

- Markus Friedl
- Theo de Raadt
- Niels Provos
- Dug Song
- Aaron Campbell
- Damien Miller
- Kevin Steves
- Daniel Kouril
- Wesley Griffin
- Per Allansson
- Nils Nordman
- Simon Wilkinson

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
PSF

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 2.3 software in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 2.3 alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003 Python Software Foundation; All Rights Reserved" are retained in Python 2.3 alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 2.3 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 2.3.

4. PSF is making Python 2.3 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 2.3 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 2.3 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 2.3, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python 2.3, Licensee agrees to be bound by the terms and conditions of this License Agreement.

PHP

The PHP License, version 3.01
Copyright (c) 1999 - 2009 The PHP Group. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo".

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP software, freely available from <http://www.php.net/software/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.
The PHP Group can be contacted via Email at group@php.net.
For more information on the PHP Group and the PHP project, please see <http://www.php.net>.


Zlib

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler
This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu
Index

A
access domains
firewall 53, 58
Panorama 229
accounts
and authentication profiles 54
creating administrator 57
active configuration, updating 72
Active Directory
configuring User-ID Agent 39
installing User-ID Agent 38
uninstalling and upgrading User-ID Agent 41
User-ID Agent 37
adding devices to CMS 224
address groups, defining 143
addresses
defining 142
defining address groups 143
defining group 143
defining ranges 142
administrator
accounts, about 53
accounts, creating 57
authentication options 53
page lockout 58, 226
profiles, about 53
roles, about 53
roles, defining 54, 229
agent
configuring terminal server 48
User-ID 33
aggregate Ethernet interfaces
configuring 92
groups 86
aggregate groups 86
alarm thresholds 115
allow list
URL filtering profile 138
wildcard patterns 138
anti-spyware profiles
about 134
defining 134
anti-spyware response page 74
antivirus profiles
defining 133
settings 134
antivirus response pages 231
App-ID, requesting 187
Application Command Center (ACC), using 163
application exception policies 158
application exceptions 134, 135
application groups, defining 150
application override policies
about 131
defining 131
applications
ACC page 165
attributes 143
categories 148, 239
characteristics 148, 241
custom with application override 131
defining 148
defining filters 151
defining groups 150
details 144
exceptions 134, 135
filters 143
identifying unknown 185
response page 233
searching 144
sub category 148
subcategories 239
technologies 241
updating threat definitions 76
applications list 165
App-Scope reports
change monitor report 169
network monitor report 172
summary report 168
threat map report 170, 171, 174
viewing 167
ARP entries
on L3 subinterfaces 90
on main L3 interfaces 89
on VLAN interfaces 93
AS
and BGP 99
description 99
attributes, application 143
audit, configuration 71
authentication
IKE 192
LDAP 53
local database 53
options for administrator 53
RADIUS 53
remote 66, 71
Authentication Header (AH) 192
authentication profiles
about 54
LDAP settings 56
RADIUS settings 56
setting up 55

B
BGP
about 98
custom group reports 182
custom reports
filters 184
generating 183

D
dashboard 162
data filtering
ACC page 165
and data patterns 157
defining policies 139
list 165
pattern settings 140
policies 139
profile settings 139
profiles and patterns 140
viewing logs 60, 178
data protection
adding 68
dead peer protection 194, 197
devices
adding 227
management 23
master 228
DHCP
firewall options 111
relay 111
servers 111
settings 112, 212
Diffie-Hellman (DH) group 192, 195
discard options, DOS profiles 116
disk utilization 162
DNS servers 67, 112
DNS with SSL VPNs 208
domain name 66
duplex settings 87, 95
dynamic updates
   about 76
   scheduling 76
dynamic URL timeout 69

eDisc
 about 76
setting 76

e-mail
   notification settings 64
   scheduling report delivery 182
email notification settings
   defining 64
   in logging profiles 159
   emailing PDF summary reports 181
Encapsulating Security Payload (ESP) 192
Ethernet interfaces, configuring 92
exchange mode 194, 197
exports
   certificates 77
   scheduling log 65

F
fail over 199
features and benefits 14
file blocking
   defining profiles 139
   profiles, defining 158
   settings 139
file blocking page 233
filters
   application 143, 151
   custom report 184
   report groups 184
   sub category 144
FIPS 243
firewall
   and User-ID Agent 35
   features and benefits 14
   introduction 13
   latitude and longitude 68
   navigating the user interface 21
flood protection 114
flood, zone protection settings 115, 214
FTP server, saving logs to 65

G
groups
   aggregate interface 86
   defining service 153, 160
device 228
   in filters 184

H
HA interfaces 95
HA1 and HA2 ports 30
hello interval, HA 31
high availability
   about 28
   active/passive pairs 28
   configuration notes 32
   configuring 30
   defining interfaces 95
   enabling 30
   interfaces 95
   notes about setting up 29
   rules for operation and failover 28
   setting up 29
hold time 31
host name, defining 66, 71
HTML block pages 231

I
ICMP flood 115
identification, IKE 192
IKE
   about 190, 192
   AH 192
   authentication 192
   crypto profile settings 195
   crypto profiles, about 192
   dead peer protection 194, 197
   defining crypto profiles 195
   DH group 192
   ESP 192
   exchange mode 194, 197
   identification 192
IKE gateways
   about 192
   setting up 113, 194
   settings 194
installation, Panorama 219
interface management profiles 114
interfaces
   aggregate groups 86
   configuring aggregate Ethernet 92
   high availability 95
   L2 subinterfaces 88, 95
   L2, main 87
   L3 subinterfaces 90
   L3, main 88
   summary of 85
   tap 95
viewing status 86, 162
IPSec
  AH 192
  crypto profile settings 195
defining crypto profiles 195
  DH group 192
  ESP 192
  lifetime 192
  number of tunnels 191
  setting up tunnels 196
IPv6 68
IPv6 addresses 142

J
jumbo frame MTU 69

K
knowledge base 80

L
L2 deployments, about 83
L2 interfaces
  configuring 87
  configuring subinterfaces 88
  main 87
  subinterfaces 88, 95
L3 deployments, about 83
L3 interfaces
  and shared gateways 28
  configuring 88
  configuring subinterfaces 90
  loopback 94
  main 88
  subinterfaces 90
latitude and longitude 68
Layer 88
LDAP 39
  authentication 53
  configuring server 36
  configuring server settings 56
licenses
  installing 73, 77
  open source 245
link
  duplex 87
  speed 87
  state 87
link groups, HA 32
link speed and duplex 95
link state
  setting 95
  viewing 162
local identification 194, 197
lockout on Administrator’s page 58, 226
log destinations
  about 61
  email 64
SNMP traps 63
syslog 64
log exports 65
log forwarding
  defining profiles 159
  profile settings 159
log page links 164
logs
  about 60
  configuration 60
  configuration settings 61
defining remote logging
  for the configuration 61
  for the system log 62
  for threat and traffic logs 158
email notification settings 64
links from ACC pages 164
saving to FTP server 65
scheduling exports 65
system 60
threat 60
viewing 175
viewing URL filtering 178
loopback interfaces
  and management port 66
defining 94
LSA 99

M
management interface
  CLI 14
  configuring 66, 71
  options 14
  Panorama 14
  web 14
managing configurations 72
master device 228
MD5 104
memory utilization 162
MIBs, SNMP 63
MTU 69
multiple virtual systems 25, 27, 68

N
NAT
  defining policies 127
  policies 125
  policy examples 126
  types 125
navigation 21
network profiles 113
network settings 66, 71
networking overview 82
NIS servers 112
NSSA (not so stub area) 105
NTP servers 67
objects, policy 141
OCSP 79
open source licenses 245
OSPF
  about 98
  configuring virtual router 104
  redistribution profiles 102
  virtual routers 104
packet captures, accessing 177
packet-based attack protection 114, 116
Panorama
  ACC tab 225
  access domains 229
  accessing 223
  adding devices 227
  configuring IP address 68
  dashboard 225
  enabling access 68
  installation 219
  interface description 224
  logging in 221
  monitor tab 225
  objects tab 225
  Panorama tab 225
  policies tab 225
  server certificate 78
  shared policies, defining 225
  tab 226
  tabs 225
  upgrading software 230
  user account lockout 58, 226
PAN-OS software
  upgrading 58, 75, 229
  version 162
PAN-OS, upgrading software 75
passive hold time, HA 31
passive link state 31
password
  data protection 68
  new 18
path groups, HA 32
PDF summary reports
  creating 180, 182
  designing 180
  displaying 180
  sending by email 181
  viewing 179
peer identification 194, 197
Perfect Forward Security (PFS) 192
policies
  about 119
  about NAT 125
  about policy-based forwarding 128
  about security 122
  and virtual systems 24, 25, 27
data filtering 139
data patterns 157
defining address objects 142
defining captive portal 132
defining NAT 127
defining SSL decryption 129
guidelines on defining 120
other policy objects 141
QoS 215
  shared 225
  specifying users and applications 130
types 119
policy objects, defining 160
policy-based forwarding
  about 128
  defining 128
PPPoE
  about 84
  deployments 84
  settings 89
profile groups, defining 158
profiles
  about security 132
  anti-spyware 134
  antivirus 133
  antivirus, application exceptions 134, 135
  antivirus, decoders and actions 134, 135
  defining log forwarding 159
  file blocking 139, 158
  flood protection 114
  IKE crypto 195
  IKE crypto profile settings 195
  interface management 114
  IPSec crypto 195
  IPSec crypto profile settings 195
  logging 158
  network 113
  packet-based attack 114
  QoS 211, 214
  reconnaissance detection 114
  redistribution 102
  security groups 133, 158
  tunnel monitor 199
  URL filtering 137
  vulnerability protection 136, 137
  zone protection 115, 214
proxy server 67
QoS
  classes 214, 215
  clear text traffic 212
  configuration instructions 211
  egress settings 214
  marking 124
  policies 215
  priority settings 214
  profiles 211, 214
settings 124
settings for firewall interfaces 211
tunneled traffic 212

R
RADIUS
and authentication profiles 54
authentication 53
defining server settings 56
random early drop 115
rebooting the device 66, 69, 71
rebooting the firewall 69
reconnaissance detection 114
redistribution profiles
about 102
configuring 102
regular expressions, and data patterns 153
rematching sessions 69
remote authentication 66, 71
reports
App-Scope 167
creating custom group 182
custom 183
groups in filters 184
PDF summary 179
scheduling email delivery 182
top 50 183
viewing 183
reports and logs
custom reports 183
identifying unknown applications 185
using the Application Command Center 163
using the dashboard 162
viewing App-Scope reports 167
viewing PDF summary reports 179
viewing reports 183
requesting support 80
response pages
anti-spyware 74
antivirus 74, 231
application block 74, 233
captive portal 74, 236
defining 74
file blocking 74, 233
SSL certificate revoked notify 74, 238
SSL decryption opt-out 74
SSL VPN custom login 74
types 59, 74
URL filtering continue and override 74, 236
response thresholds 115, 116
restarting the firewall 69
RFC 1583 Compatibility 104
RIP
about 98
configuring virtual router 103
redistribution profiles 102
virtual routers 103
roles
about 53
defining administrator 54, 229
rolling back a candidate configuration 72
routing protocols
about 98
and virtual routers 98
BGP 106
OSPF 104
RIP 103
rules
application exception policy 158
security policy 123
S
sample VPN configuration 201
saving a candidate configuration 72
schedules, defining 158
security
defining profile groups 133, 158
profile groups 158
security associations (SA) 191
security certificates 77
security policies
about 122
defining 123
security profile groups, defining 158
security profiles
about 132
actions 132
defining 158
security zones
about 97
and interfaces 97
defining 97
in NAT policies 127
in security policies 123
sensitive information, protecting 68
servers
defining LDAP 56
defining RADIUS 56
defining syslog 64
service groups
about 152
defining 153
service groups, defining 153, 160
services
about 152
defining 152
services, defining 160
shared gateways
about 26
and common interface 26
and L3 interfaces 28
configuring 28
shared policy
defining 225
master device 228
master device, 228
SNMP
  community string 68
  MIBs 63
SNMP trap destinations
  defining 63
  in logging profiles 159
software
  upgrading 58, 75, 229, 230
  upgrading Panorama 230
  version 162
speed, link 87, 95
SSL
  decryption policies 158
  decryption rule settings 128, 129
  defining decryption policies 129
  inbound inspection certificate 78
  tech notes reference 129
SSL VPNs
  about 205, 211
  and authentication profiles 54
  comfort page 74
  connection process 206
  local user database 210
  maximum number of users 208
  response page 74
  setting up 207
  split tunnels 209
  tunnel interface 208
state synchronization, HA 30
sub category
  application 148
  filtering 144
support information 80
support information, viewing 80
SYN flood 115
syslog servers
  defining 64
  in logging profiles 159
system log
  about 60
  defining remote logging 62
  viewing 178
system settings 66

T
tags
  on L2 subinterfaces 88
  on L3 subinterfaces 90
  on virtual wires 84
tap interfaces, defining 95
tap mode
  deployment option 83
  description 83
terminal server agent
  configuring 48
  configuring terminal server 49
  installing 48, 53
terminal server, configuring 49
threat list 165
threat log 159
  about 60
  defining remote logging 158
  viewing 177
threats
  ACC list 165
  updating definitions 76
thresholds, alarm 115
time
  setting 66, 71
  zone 67
traffic log 159
  defining remote logging 158
  viewing 177
Transport Layer Security (TLS) 57
TS agent
  configuring firewall to support 48
  installing 48
  uninstalling 53
  upgrading 48
tunnel interfaces 196
tunnel monitor
  fail over 199
  profiles 199
  wait-recover 199
tunneled traffic, and QoS 212
tunnels
  about VPN 191
  interface for SSL VPN 208
  number of IPSec 191
  setting up 196
  split for SSL VPNs 209
type of service (TOS) 198
types of deployments 82
typographical conventions 11

U
UDP flood 116
unknown applications
  identifying 185
  requesting App-ID 187
  taking action 187
unnumbered loopback interfaces 94
upgrading
  Panorama software 230
  PAN-OS software 58, 75, 229
  schedules 76
  threat and application definitions 76
URL filtering
  ACC page 165
  continue and override response page 74, 236
  defining profiles 137
  dynamic categorization 137
  list 165
  override settings 70
  profile settings 137
response pages 74
viewing log 178
viewing logs 60
user database, SSL VPN 210
user interface navigation 21
User-ID Agent
  configuring 42
  configuring for Active Directory 39
  for API, about 42
  for eDirectory, about 42
  installing for Active Directory 38
  monitoring status 47
  privileges for PC user 38
  timers for Active Directory 41
  uninstalling and upgrading 47
  uninstalling and upgrading for Active Directory 41
User-ID agent
  captive portal configuration 36
  configuring firewall for 35
  configuring LDAP server 36
  for Active Directory, about 37
users
  account lockout 58, 226
  connecting with SSL VPN 206
V
version, software 162
viewing devices 227
virtual routers
  and routing protocols 98
  configuring 100
  defining 100
  runtime statistics 111
virtual systems
  about 24
  and policies 24
  and security zones 24, 25
  communications among 25
  defining 24, 27, 28
  defining multiple 27
  enabling 68
  enabling multiple 68
  internal traffic flow 25
  multiple 25
  shared gateway common interface 26
  shared gateways 26
virtual wire 82
  defining 84
  interfaces 92
  interfaces, configuring 91
VLANs
  and L2 interfaces 93
  interfaces, defining 93
VPN
  about 190
  IPSec and IKE crypto profiles 192
  sample configuration 201
  setting up tunnels 191
  SSL, about 205, 211
VPN tunnels
  about 191
  IKE 191
  manual security keys 191
  securing 191
  setting up 193, 196
vulnerability protection profiles 136, 137
W
wildcard
  custom URL categories 155
  patterns for allow and block lists 138
Windows XP and Vista users 206
WINS
  for SSL VPNs 208
  servers 112
Z
zones
  defining 97
  in NAT policies 127
  in security policies 123
  protection profiles 115, 214