Palo Alto Networks Administrator's Guide

Release 3.0

paloalto NETWORKS

Palo Alto Networks, Inc.
www.paloaltonetworks.com

P/N 810-000044-00A

Table of Contents

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 11

Appendix A

Appendix B
Sample VPN Configuration 307

Appendix C
Application Categories, Subcategories, Technologies, and Characteristics 311

Appendix D
Open Source Licenses 315

Index 335

Preface

This preface contains the following sections:

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, "Firewall Installation"—**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. The firewall supports virtual wire, Layer 2, Layer 3, and combined Layer 2/ Layer 3 configurations.
- **Chapter 5, "Policies and Security Profiles"—**Describes how to configure security policies and profiles by zone, users, source/destination address, and application.

- **Chapter 6, "Reports and Logs"**—Describes how to view the reports and logs provided with the firewall.
- **Chapter 7, "Configuring SSL VPNs"**— Describes how configure virtual private networks (VPNs) using Secure Socket Layer (SSL).
- **Chapter 8, "Configuring IPSec Tunnels"**— Describes how to configure IP Security (IPSec) tunnels on the firewall.
- **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 Central 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, "Sample VPN Configuration"**—Provides a sample VPN configuration to establish a VPN tunnel between a central and branch office.
- **Appendix C, "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.

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

Notes and Cautions

This guide uses the following symbols for notes and cautions.

Symbol	Description
📝	NOTE Indicates helpful suggestions or supplementary information.
⚠	CAUTION Indicates actions that could cause loss of data.

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 website**—Go to *http://www.paloaltonetworks.com*.
- **Online help**—Click **Help** in the upper-right corner of the GUI to access the online help system.

Technical Support

For technical support, use the following methods:

- Go to *http://support.paloaltonetworks.com*.
- Call 1-866-898-9087 (U.S, Canada, and Mexico).
- Email us at: *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
- “Overview of Key Concepts” on page 15

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 "Defining Security Profiles" on page 164).

- **URL filtering** — Outbound connections can be filtered to prevent access to inappropriate web sites.

- **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 215).

- **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 "Configuring High Availability" on page 70).

- **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 central 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 281 for instructions on installing Panorama and "Central Management of Devices" on page 285 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 81). Remote configuration is not supported.
- **Syslog** — Provides message generation for one or more remote Syslog servers (refer to “Defining Syslog Servers” on page 83).

Overview of Key Concepts

For a description of some basic concepts that are key to understanding the capabilities of the firewall, refer to:

- “About Security Policies” in the next section
- “About Security Profiles” on page 16
- “About Virtual Systems” on page 16
- “About Virtual Routers and Routing Protocols” on page 16
- “About Virtual Private Networks” on page 17

About Security Policies

Security policies specify whether to block or allow network connections based on the application, the source and destination zones, users, and addresses, and the application service (such as UDP port 67 or TCP port 80). Zones identify the physical or logical interfaces that send or receive the traffic. By default an interface receiving traffic from the Internet is in an “untrusted” zone, while an interface receiving internal traffic is in a “trusted” zone.

Security policies can also specify security profiles that are used to protect against viruses, spyware, and other threats after the connection is established (refer to “About Security Profiles” in the next section). Security policies can be as general or specific as needed. The policy rules are processed in sequence, applying the first rule that matches the incoming traffic (refer to “Defining Policies” on page 144).

In addition to security policies, you can also define:

- Network Address Translation (NAT) policies to translate addresses and ports
- SSL Decryption policies to specify the SSL traffic to be decrypted so that security policies can be applied
- Application override policies to override the application definitions provided by the firewall
- Captive portal policies to request authentication of unidentified users

About Security Profiles

Each security policy can specify a number of security profiles to defend against known network threats, prevent access to specified web sites, and specify logging criteria. The security profiles include:

- Antivirus profiles to protect against worms and viruses
- Anti-spyware profiles to block known spyware
- Vulnerability protection profiles to stop attempts to exploit system flaws
- URL filtering profiles to deny access to inappropriate web sites
- File blocking profiles to block selected file types
- Data filtering profiles to prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall
- Log forwarding profiles to specify the severity level of the messages logged and where the messages are sent (Panorama, SNMP trap sinks, Syslog servers, and/or email addresses)

For more information about security profiles, refer to “Defining Security Profiles” on page 164.

About Virtual Systems

Virtual systems let you customize administration, networking, and security policies for the network traffic belonging to specific departments or customers. Each virtual system specifies a collection of physical and logical interfaces (including VLANs, and virtual wires), and security zones, for which you can tailor specific policies. Administrator accounts can be defined that are limited to the administration of a specific virtual system.

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

About Virtual Routers and Routing Protocols

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) and the Open Shortest Path First (OSPF) protocol.

RIP was designed for small IP networks and relies on hop count to determine routes; the best routes are deemed to be those with 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.

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.

About Virtual Private Networks

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. The Internet Key Exchange (IKE) protocols can be used to automatically generate security keys for communication through the tunnels.

Note: *The firewall also supports SSL VPNs which allow remote users to establish VPN connections through the firewall. Refer to Chapter 7, "Configuring SSL VPNs" for more information.*

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.

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.

VPN Tunnels

To set up the 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, route lookup can determine the appropriate tunnel to use. The tunnel interface appears to the system as if it is a normal interface, and the existing routing infrastructure can be applied.

There are two ways to secure 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 (refer to the next section).

Internet Key Exchange

IKE provides a standard mechanism for generating and maintaining security keys for identification and authentication of traffic through IPSec tunnels:

- **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.

IPSec and IKE Crypto Profiles

Crypto profiles are related to standard proposal fields in IKE negotiation. The IKE-crypto profile corresponds to IKE Security Association (SA) negotiation (IKEv1 Phase-1), while the IPSec crypto profile corresponds to 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 263 and "Defining IPSec Crypto Profiles" on page 264.

Setting Up VPNs

This section describes the process involved in setting up VPN tunnels. For detailed instructions, refer to the specified sections in this guide. For information about a sample configuration, refer to "Sample VPN Configuration" on page 307.

Note: *Before you begin, make sure that your Ethernet interfaces, virtual routers, and zones are configured properly. Refer to "Configuring Interfaces" on page 98, "Defining Virtual Routers" on page 122, and "Defining Security Zones" on page 116.*

To set up VPNs:

1. Plan the network topology and determine the required number of tunnels.
2. Create the tunnel interface, assigning a virtual router and zone to each. It is not necessary for the tunnel endpoints to be in the same virtual router or the same zone as the tunnel interface. Choose the auto or manual key option. Refer to "Setting Up IPSec Tunnels" on page 268.

   As part of the tunnel interface definition, you can select an existing IKE gateway or enter the IKE gateway information as part of the tunnel definition. If you are creating multiple tunnels, it is helpful to first create IKE gateways and then select them when defining the tunnel interfaces. Refer to "Setting Up IKE Gateways" on page 134.

   For multiple tunnels, you can add sub-interfaces to the tunnel interface.
3. Set up the tunnel interface and matching IKE settings for the peers at the other end of each tunnel.

4. 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 "Defining Virtual Routers" on page 122.

5. Set security policies to filter and inspect the traffic. 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. Refer to "Defining Security Profiles" on page 164.

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.*

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).

Chapter 2

Firewall Installation

This chapter describes how to install the firewall:

- "Pre-Installation Tasks" in the next section
- "Installation Procedure" on page 22
- "Post-Installation Tasks" on page 37

Note: *Refer to "Panorama Installation" on page 281 for instructions on installing the Panorama central management system.*

Pre-Installation Tasks

Before you install the firewall, perform the following tasks:

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. Get an RJ-45 Ethernet cable to connect your computer to the management port on the firewall.
5. Set your computer's IP address to 192.168.1.2 and the subnet mask to 255.255.255.0.

Installation Procedure

This section describes the procedure for installing the firewall:

1. Perform the initial setup (refer to “Performing the Initial Setup” in the next section).
2. Choose a deployment option (refer to “Choosing a Deployment Option” on page 23).
3. Perform the final setup (refer to “Performing the Final Setup” on page 33).

Performing the Initial Setup

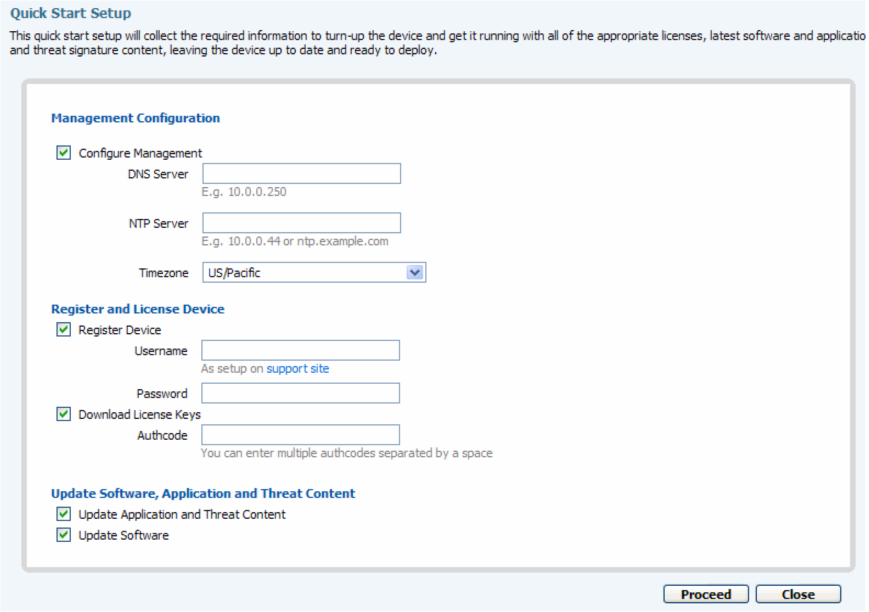
The first part of the installation procedure is to connect your computer to the management port on the firewall, log in to the firewall via a web browser, and change the default password.

To perform the initial 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 subnet (for example, 192.168.1.5).
3. Launch your preferred web browser and enter **https://192.168.1.1**.

   The browser automatically opens the Palo Alto Networks login page.
4. Enter **admin** in both the **Name** and **Password** fields, and click **Login**.

   The Quick Start page opens.



Quick Start Setup

This quick start setup will collect the required information to turn-up the device and get it running with all of the appropriate licenses, latest software and applicatio and threat signature content, leaving the device up to date and ready to deploy.

Management Configuration

☑ Configure Management

DNS Server
E.g. 10.0.0.250

NTP Server
E.g. 10.0.0.44 or ntp.example.com

Timezone: US/Pacific

Register and License Device

☑ Register Device

Username
As setup on support site

Password

☑ Download License Keys

Authcode
You can enter multiple authcodes separated by a space

Update Software, Application and Threat Content

☑ Update Application and Threat Content

☑ Update Software

Figure 1. Quick Start Setup Page

5. Perform these tasks on the Quick Start Setup page:
   a. 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 Setup page. Refer to “Performing the Final Setup” on page 33.
   b. If this is the first Palo Alto Networks firewall for your company, click the **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.
   c. Select the **Update Application and Threat Content** check box to automatically update the firewall with the latest application and threat data. Select the **Update Software** check box to update the firewall with the latest available software.
   d. Click **Proceed** to apply the settings and close the page.
6. Click **Administrators** under the **Devices** tab.
7. Click **admin**.
8. In the **New Password** and **Confirm New Password** fields, enter and confirm a case-sensitive password (up to 15 characters).
9. Click **OK** to submit the new password.

Choosing a Deployment Option

When deploying the firewall, choose one of the following deployment options:

- “Option A: Virtual Wire Deployment” in the next section
- “Option B: Layer 2 Deployment” on page 24
- “Option C: Layer 3 Deployment” on page 27
- “Option D: Tap Mode Deployment” on page 31

Option A: Virtual Wire Deployment

Choose this option to transparently place the firewall on a network segment where no routing, switching, or NAT is required.

This option is the default configuration. It allows the firewall to be a virtual wire that enforces security policies between ports 1 and 2.

If the default virtual wire configuration is suitable for your network topology, you do not need to perform any configuration. However, if you need to change the default virtual wire settings, refer to “Defining Virtual Wires” on page 120 for more information.

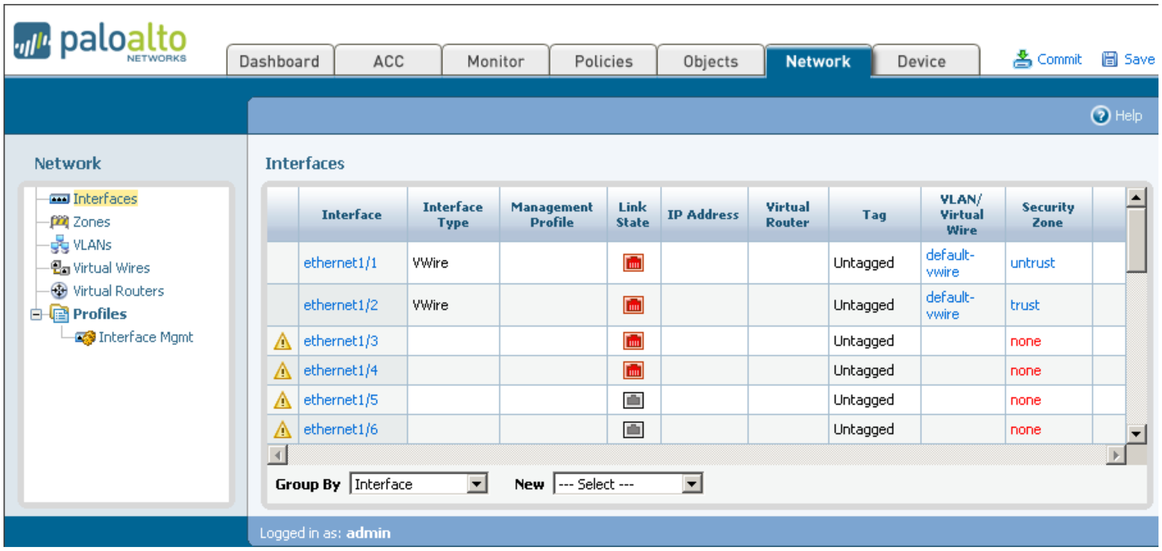
Option B: Layer 2 Deployment

Choose this option to deploy the firewall in a Layer 2 environment where switching is required.

To configure the firewall for a Layer 2 deployment:

1. Configure the Ethernet interfaces.

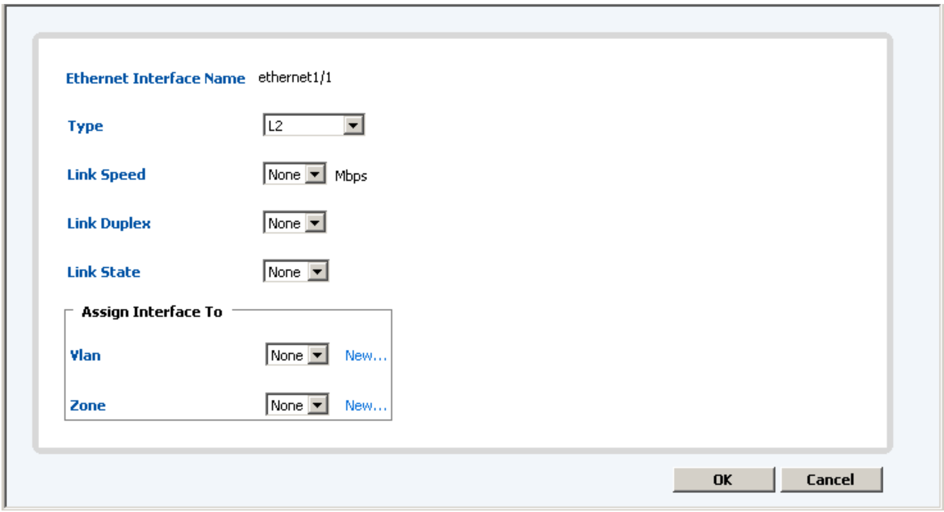
   a. Under the **Network** tab, click **Interfaces** to open the Interfaces page.



	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
	ethernet1/1	VWire		🟥			Untagged	default-vwire	untrust
	ethernet1/2	VWire		🟥			Untagged	default-vwire	trust
⚠	ethernet1/3			🟥			Untagged		none
⚠	ethernet1/4			🟥			Untagged		none
⚠	ethernet1/5			▨			Untagged		none
⚠	ethernet1/6			▨			Untagged		none

Figure 2. Interfaces Page

   b. Click **ethernet 1/1** to open the Edit Ethernet Interface page.



Ethernet Interface Name ethernet1/1

Type L2

Link Speed None Mbps

Link Duplex None

Link State None

Assign Interface To

Vlan None New...

Zone None New...

Figure 3. Edit Ethernet Interface Page

   c. Select **L2** from the **Type** drop-down list.

   d. Change any of the link settings, as needed, and click **OK** to submit the new interface.

   e. Click **OK** again when prompted.

f. Click ethernet 1/2 to open the Edit Ethernet Interface page.

g. Select **L2** from the **Type** drop-down list.

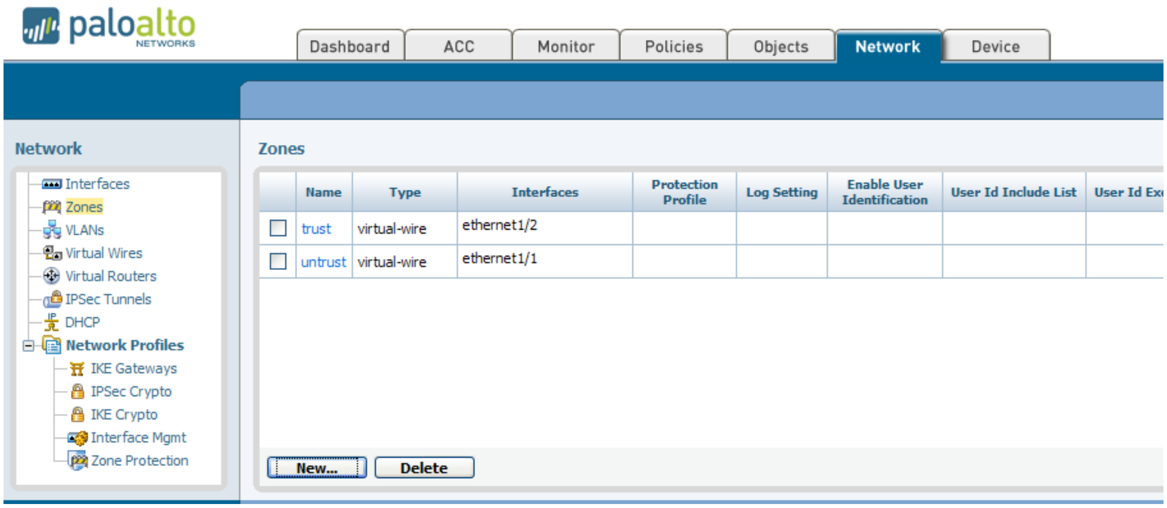
h. Click **OK** to submit the new interface.

i. Click **OK** again when prompted.

For more information about configuring the Ethernet interfaces, refer to “Configuring Interfaces” on page 98.

2. Configure the security zones.

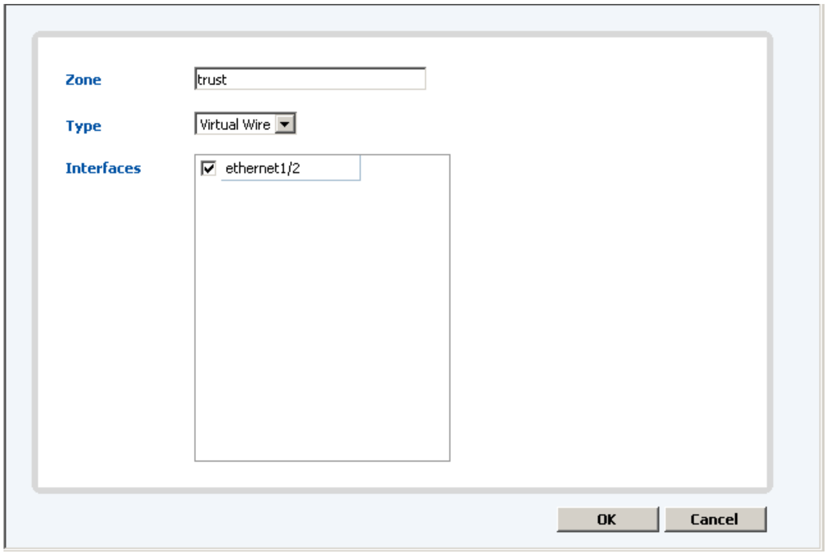
a. Click **Zones** to open the Zones page.



	Name	Type	Interfaces	Protection Profile	Log Setting	Enable User Identification	User Id Include List	User Id Ex
□	trust	virtual-wire	ethernet1/2					
□	untrust	virtual-wire	ethernet1/1					

Figure 4. Zones Page

b. Click **trust** to open the Edit Zone page.



Zone: trust

Type: Virtual Wire

Interfaces: ☑ ethernet1/2

Figure 5. Edit Zone Page

c. Select **Layer2** from the **Type** drop-down list.

d. Select the check box for ethernet1/2, and click **OK**.

e. Click **untrust** to open the Edit Zone page.

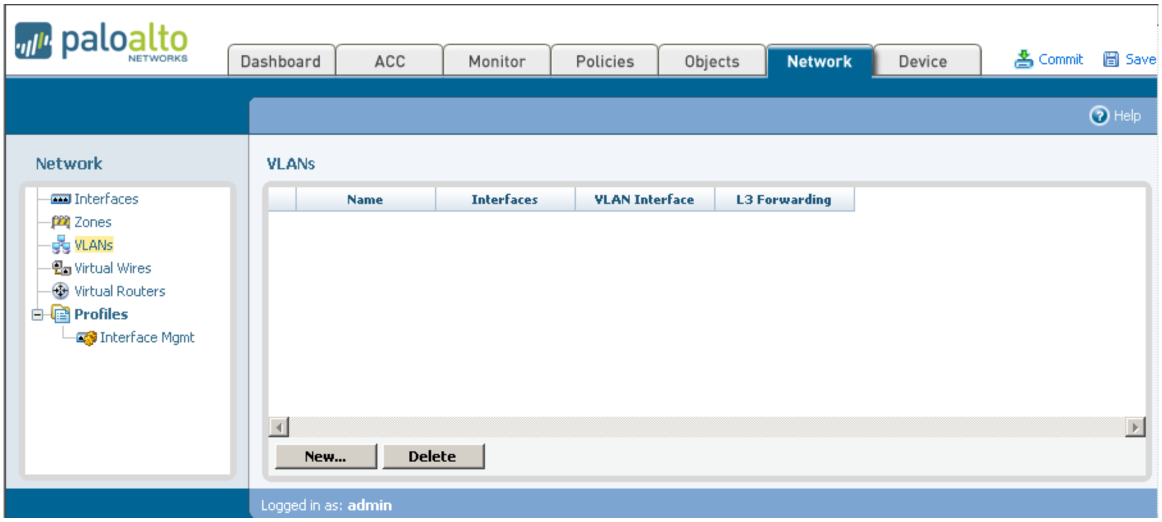
f. Select **Layer2** from the **Type** drop-down list.

g. Select the check box for ethernet1/1, and click **OK**.

For more information about configuring security zones, refer to “Defining Security Zones” on page 116.

3. Configure the VLANs.

a. Click **VLANs** to open the VLANs page.

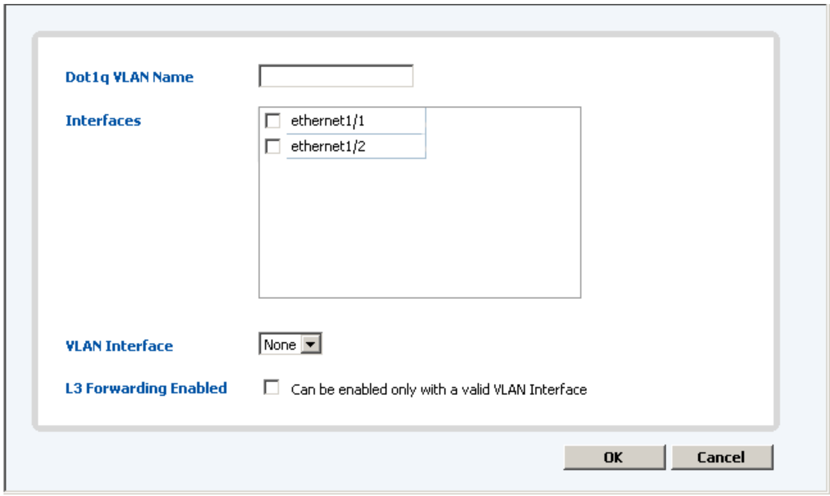


VLANs

Name	Interfaces	VLAN Interface	L3 Forwarding

Figure 6. VLANs Page

b. Click **New** to open the New Dot1q VLAN page.



Dot1q VLAN Name

Interfaces
□ ethernet1/1
□ ethernet1/2

VLAN Interface: None

L3 Forwarding Enabled: □ Can be enabled only with a valid VLAN Interface

Figure 7. New VLAN Page

c. Enter the name of the VLAN (up to 31 characters) in the **Dot1q VLAN Nam**e field.

The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.

d. Select the check boxes for ethernet1/1 and ethernet1/2 in the Interfaces list.

e. Click **OK** to submit the new VLAN.

4. Click **Commit** at the top-right of the page to activate your changes.

For more information about configuring VLANs, refer to “Defining VLANs” on page 119.

Option C: Layer 3 Deployment

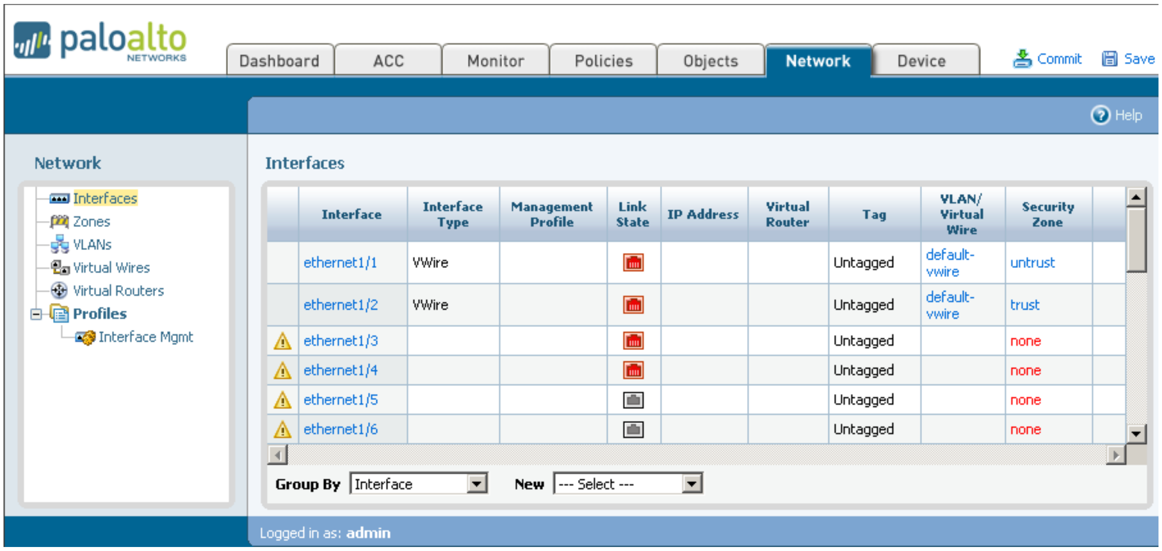
Choose this option to deploy the firewall in a Layer 3 environment where routing and NAT are required.

To configure the firewall for a Layer 3 deployment:

1. Configure the Ethernet interfaces.

a. Obtain two IP addresses for ports 1 and 2 on the firewall from your system administrator.

b. Under the **Network** tab, click **Interfaces** to open the Interfaces page.

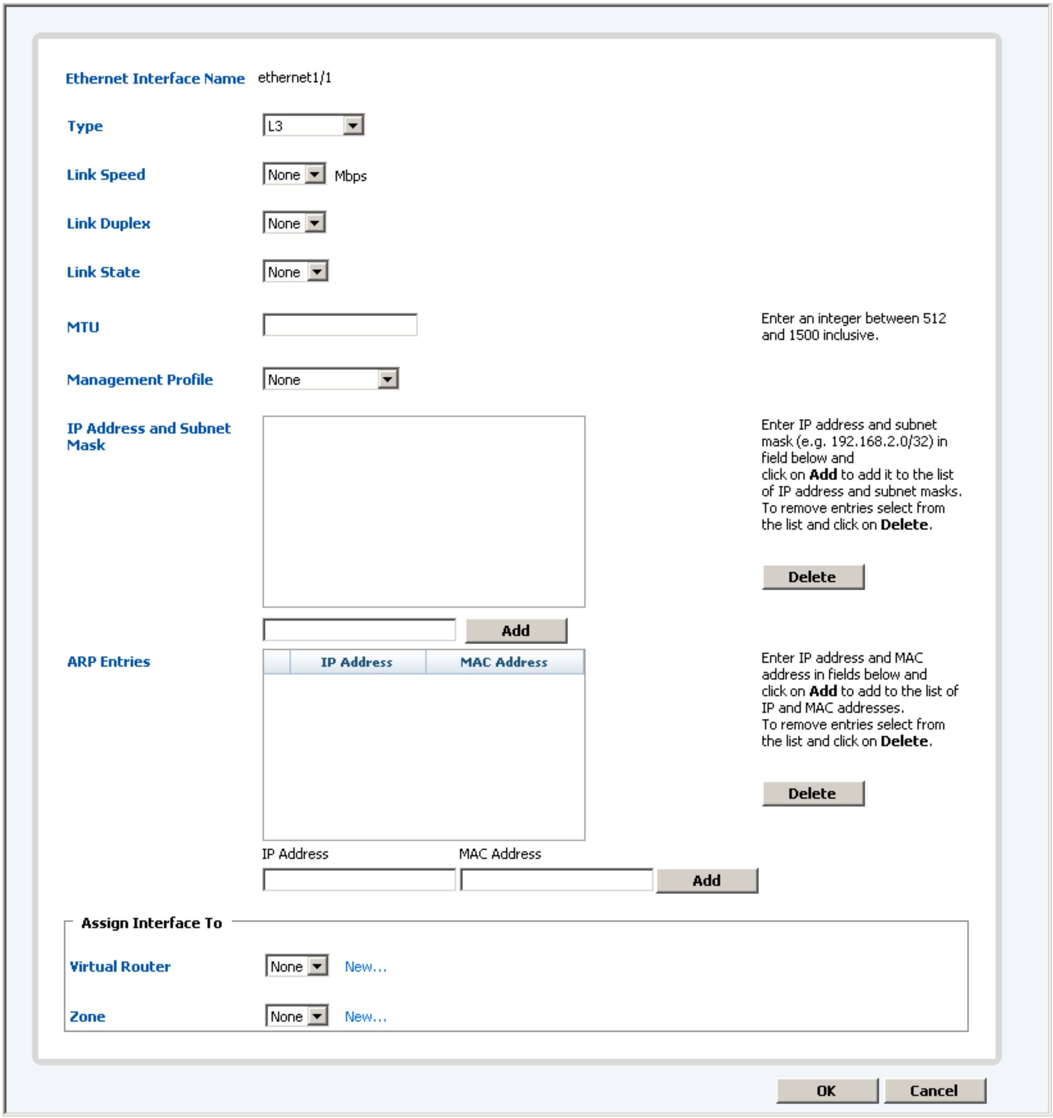


	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
	ethernet1/1	VWire		🟥			Untagged	default-vwire	untrust
	ethernet1/2	VWire		🟥			Untagged	default-vwire	trust
⚠	ethernet1/3			🟥			Untagged		none
⚠	ethernet1/4			🟥			Untagged		none
⚠	ethernet1/5			⬜			Untagged		none
⚠	ethernet1/6			⬜			Untagged		none

Figure 8. Interfaces Page

c. Click **ethernet 1/1** to open the Edit Ethernet Interface page.

d. Select **L3** from the **Type** drop-down list.



Ethernet Interface Name ethernet1/1

Type L3

Link Speed None Mbps

Link Duplex None

Link State None

MTU

Enter an integer between 512 and 1500 inclusive.

Management Profile None

IP Address and Subnet Mask

Enter IP address and subnet mask (e.g. 192.168.2.0/32) in field below and click on **Add** to add it to the list of IP address and subnet masks. To remove entries select from the list and click on **Delete**.

ARP Entries

IP Address	MAC Address

Enter IP address and MAC address in fields below and click on **Add** to add to the list of IP and MAC addresses. To remove entries select from the list and click on **Delete**.

IP Address MAC Address

Assign Interface To

Virtual Router None New...

Zone None New...

Figure 9. Edit Ethernet Interface Page

e. Enter the IP address and subnet mask for port 1 in the format *ip_address/mask* (for example, 10.1.1.1/24) in the **IP Address** and **Subnet Mask** field.

f. Click **Add**.

g. Click **OK** to submit the new interface.

h. Click **OK** again when prompted.

i. Click **ethernet1/2** to open the Edit Ethernet Interface page.

j. Select **L3** from the **Type** drop-down list.

k. Enter the IP address and subnet mask for port 2 in the format *ip_address/mask* (for example, 10.1.2.1/24) in the **IP Address** and **Subnet Mask** field.

l. Click **OK** to submit the new interface.

m. Click **OK** again when prompted.

For more information about configuring the Ethernet interfaces, refer to “Configuring Interfaces” on page 98.

2. Configure the security zones.

a. Click **Zones** to open the Zones page.

b. Click **trust** to open the Edit Zone page.

c. Select **Layer3** from the **Type** drop-down list.

d. Select the check box for ethernet1/2.

e. Click **OK**.

f. Click **untrust** to open the Edit Zone page.

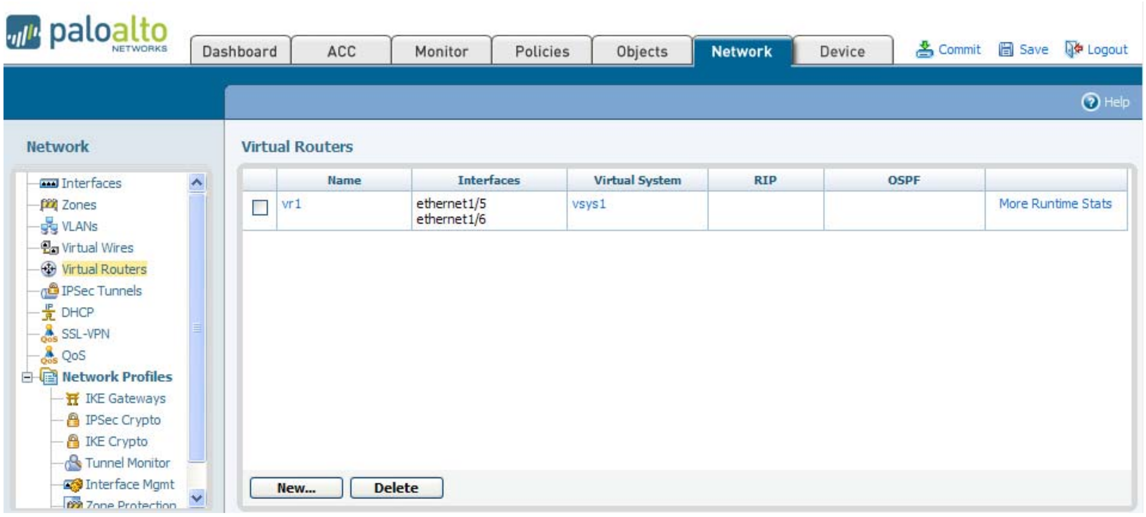
g. Select **Layer3** from the **Type** drop-down list.

h. Select the check box for ethernet1/1.

For more information about configuring security zones, refer to “Defining Security Zones” on page 116.

3. Configure the virtual routers.

a. Click **Virtual Routers** to open the virtual routers page.

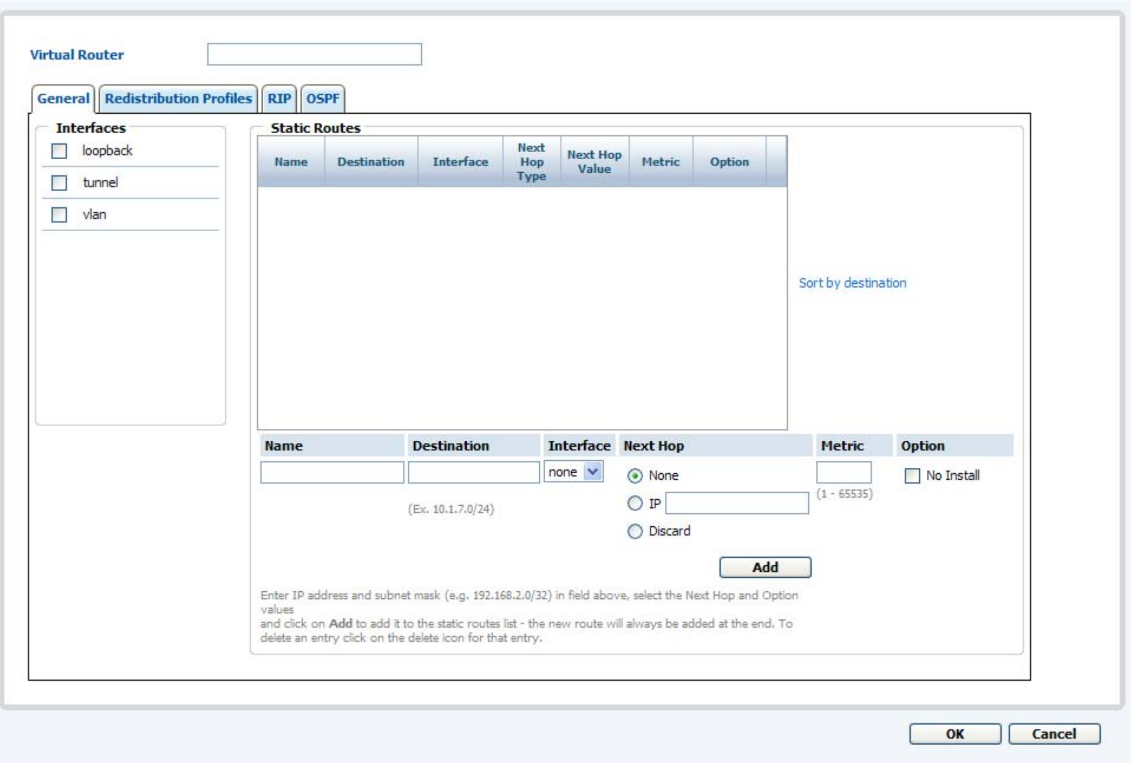


Virtual Routers

	Name	Interfaces	Virtual System	RIP	OSPF	
☐	vr1	ethernet1/5 ethernet1/6	vsys1			More Runtime Stats

Figure 10. Virtual Routers Page

b. Click **New** to open the New Virtual Router page.



Enter IP address and subnet mask (e.g. 192.168.2.0/32) in field above, select the Next Hop and Option values
and click on **Add** to add it to the static routes list - the new route will always be added at the end. To delete an entry click on the delete icon for that entry.

Figure 11. New Virtual Router Page

c. Enter the name of the virtual router (up to 20 characters) in the **Virtual Router** field.

The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.

d. Select the check boxes for ethernet1/1 and ethernet1/2 in the Interfaces list.

e. (Optional) Add static routes to the Static Routes list as described in “Defining Virtual Routers” on page 122.

f. Click **OK** to submit the new virtual router.

4. Click **Commit** at the top-right of the page to activate your changes.

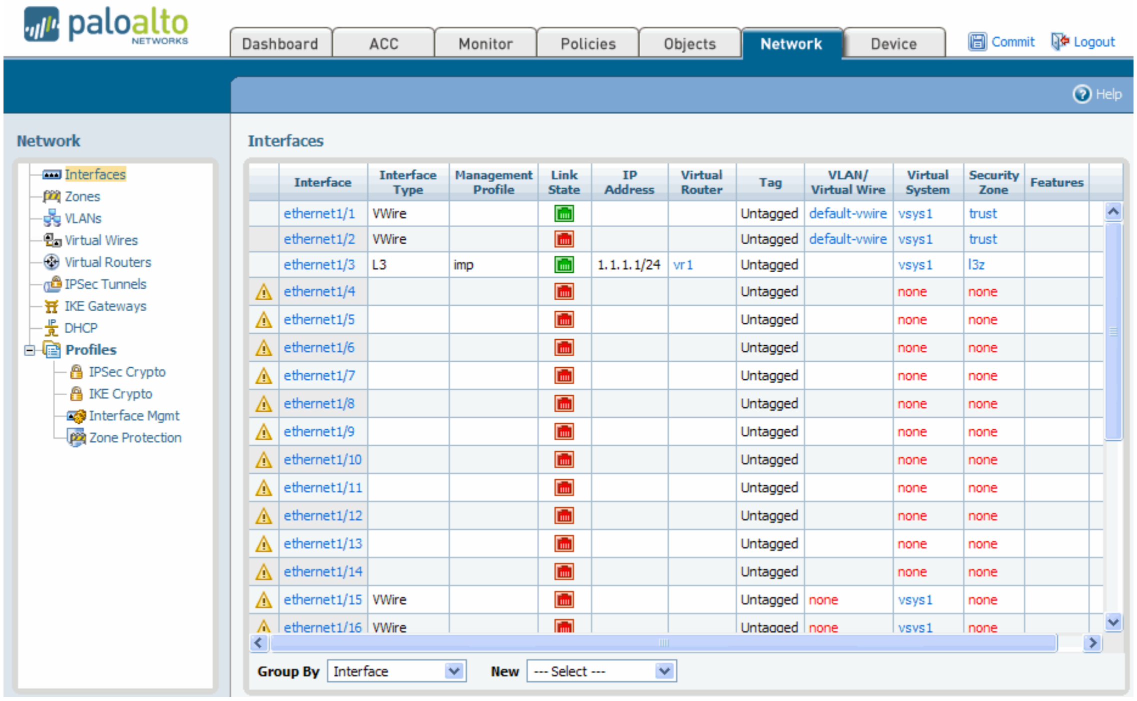
Option D: Tap Mode Deployment

Choose this option to passively monitor traffic flows across a network by way of a switch SPAN or mirror port.

To configure the firewall for tap mode:

1. Configure the Ethernet interface.

   a. Under the **Network** tab, click **Interfaces** to open the Interfaces page.



Interfaces

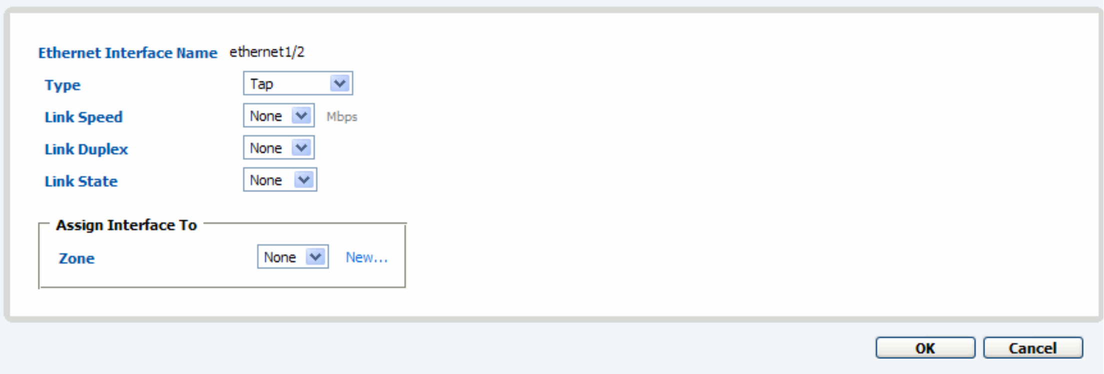
	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Virtual System	Security Zone	Features
	ethernet1/1	VWire		🟩			Untagged	default-vwire	vsys1	trust	
	ethernet1/2	VWire		🟥			Untagged	default-vwire	vsys1	trust	
	ethernet1/3	L3	imp	🟩	1.1.1.1/24	vr1	Untagged		vsys1	l3z	
⚠	ethernet1/4			🟥			Untagged		none	none	
⚠	ethernet1/5			🟥			Untagged		none	none	
⚠	ethernet1/6			🟥			Untagged		none	none	
⚠	ethernet1/7			🟥			Untagged		none	none	
⚠	ethernet1/8			🟥			Untagged		none	none	
⚠	ethernet1/9			🟥			Untagged		none	none	
⚠	ethernet1/10			🟥			Untagged		none	none	
⚠	ethernet1/11			🟥			Untagged		none	none	
⚠	ethernet1/12			🟥			Untagged		none	none	
⚠	ethernet1/13			🟥			Untagged		none	none	
⚠	ethernet1/14			🟥			Untagged		none	none	
⚠	ethernet1/15	VWire		🟥			Untagged	none	vsys1	none	
⚠	ethernet1/16	VWire		🟥			Untagged	none	vsys1	none	

Group By: Interface   New: --- Select ---

Figure 12. Interfaces Page

   b. Click the Ethernet interface that you want to use to connect to the switch SPAN port.

   c. Select **Tap** from the **Type** drop-down list.



Ethernet Interface Name	ethernet1/2
Type	Tap
Link Speed	None Mbps
Link Duplex	None
Link State	None

Assign Interface To

Zone: None New...

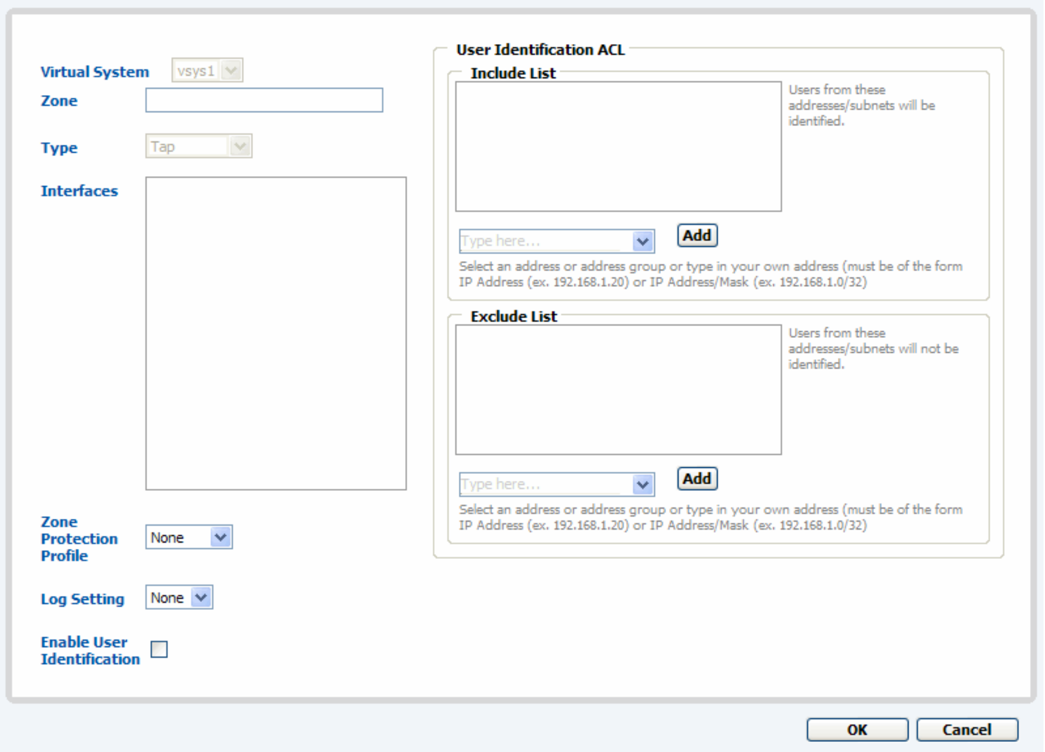
Figure 13. Edit Ethernet Interface Page

   d. Select the link speed, duplex setting, and state from the **Link** drop-down lists. Use the auto settings to have the settings determined automatically.

e. Select the VLAN and virtual system from the drop-down lists.

2. Create a zone.

a. Click **New** to open the New Zone page.



Virtual System: vsys1

Zone:

Type: Tap

Interfaces

Zone Protection Profile: None

Log Setting: None

Enable User Identification □

User Identification ACL

Include List

Users from these addresses/subnets will be identified.

Type here...

Select an address or address group or type in your own address (must be of the form IP Address (ex. 192.168.1.20) or IP Address/Mask (ex. 192.168.1.0/32)

Exclude List

Users from these addresses/subnets will not be identified.

Type here...

Select an address or address group or type in your own address (must be of the form IP Address (ex. 192.168.1.20) or IP Address/Mask (ex. 192.168.1.0/32)

Figure 14. Edit Zone Page - Tap Mode

b. Enter a name for the zone. Note that the type is automatically selected.

c. Select the check boxes for the interface that you configured for the zone.

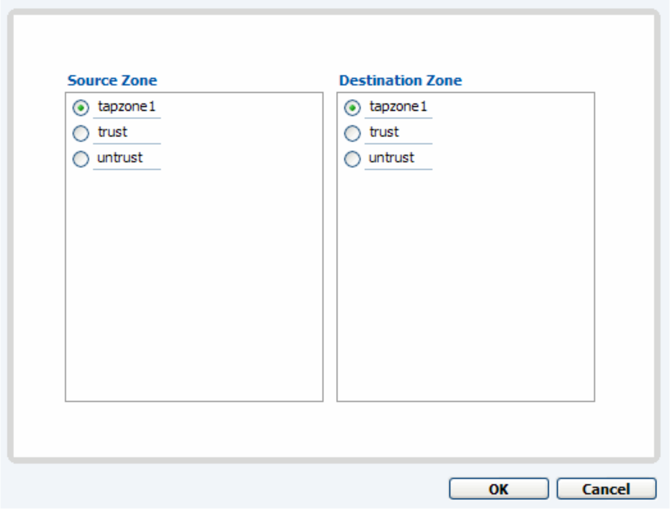
d. Click **OK**.

3. Create a tap mode policy.

a. Under the **Policies** tab, click **Security** to open the Security Rules page.

b. Click **Add Rule**.

c. For the source and destination zones, select the tap zone that was previously created.



Source Zone	Destination Zone
● tapzone1	● tapzone1
○ trust	○ trust
○ untrust	○ untrust

Figure 15. Edit Zone Page - Tap Mode

d. Click **OK**. The new rule is displayed on the Security Rules page.

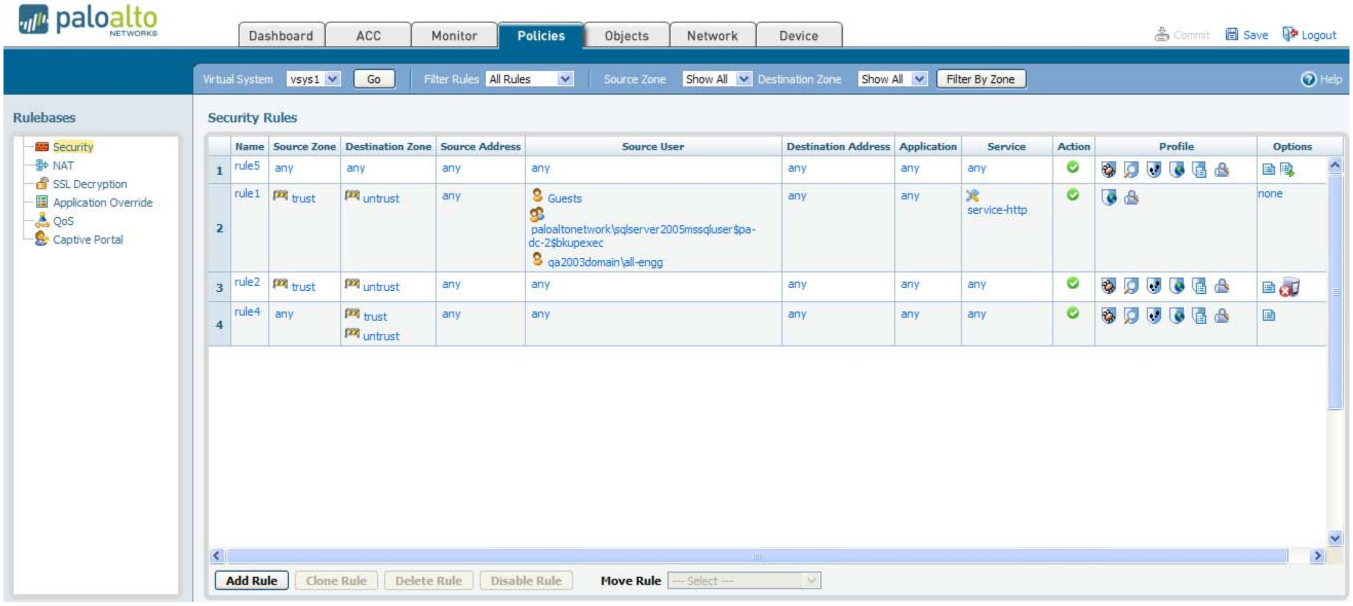
e. Click **Commit** to install the new settings and policy.

Performing the Final Setup

To perform the final setup of the firewall:

1. Configure the security policy.

   a. Under the **Policies** tab, click **Security** to open the Security Rules page.



Virtual System: vsys1 | Filter Rules: All Rules | Source Zone: Show All | Destination Zone: Show All | Filter By Zone

Security Rules

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1	rule5	any	any	any	any	any	any	any	✓		
2	rule1	trust	untrust	any	Guests paloaltonetwork\sqlserver2005mssqluser$pa-dc-2$bkupexec qa2003domain\all-engg	any	any	service-http	✓		none
3	rule2	trust	untrust	any	any	any	any	any	✓		
4	rule4	any	trust untrust	any	any	any	any	any	✓		

Figure 16. Security Rules Page

b. Review the default policies, which allow all traffic to flow from the trust zone to the untrust zone. To configure policies beyond the default settings, refer to “Defining Security Policies” on page 144.

2. Connect the firewall to your network and the Internet.

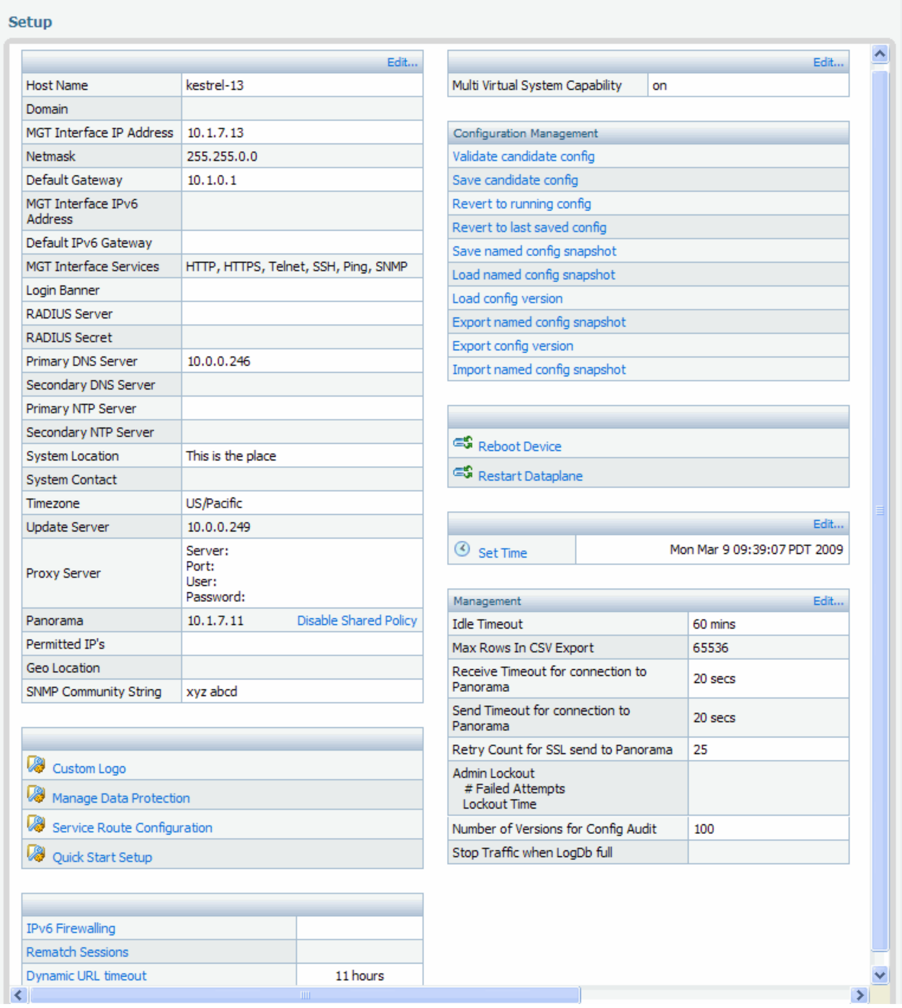
   a. Connect port 1 of the firewall to the Internet.

   b. Connect port 2 of the firewall to your network.

3. From a computer on your local network other than the computer you are using to configure the firewall, try to connect to the Internet to validate proper connectivity.

4. Configure the management interface.

   a. Under the **Device** tab, click **Setup** to open the Setup page.



Setup

	Edit...
Host Name	kestrel-13
Domain	
MGT Interface IP Address	10.1.7.13
Netmask	255.255.0.0
Default Gateway	10.1.0.1
MGT Interface IPv6 Address	
Default IPv6 Gateway	
MGT Interface Services	HTTP, HTTPS, Telnet, SSH, Ping, SNMP
Login Banner	
RADIUS Server	
RADIUS Secret	
Primary DNS Server	10.0.0.246
Secondary DNS Server	
Primary NTP Server	
Secondary NTP Server	
System Location	This is the place
System Contact	
Timezone	US/Pacific
Update Server	10.0.0.249
Proxy Server	Server: Port: User: Password:
Panorama	10.1.7.11 Disable Shared Policy
Permitted IP's	
Geo Location	
SNMP Community String	xyz abcd

Custom Logo
Manage Data Protection
Service Route Configuration
Quick Start Setup

IPv6 Firewalling	
Rematch Sessions	
Dynamic URL timeout	11 hours

	Edit...
Multi Virtual System Capability	on

Configuration Management
Validate candidate config
Save candidate config
Revert to running config
Revert to last saved config
Save named config snapshot
Load named config snapshot
Load config version
Export named config snapshot
Export config version
Import named config snapshot

Reboot Device
Restart Dataplane

	Edit...
Set Time	Mon Mar 9 09:39:07 PDT 2009

Management	Edit...
Idle Timeout	60 mins
Max Rows In CSV Export	65536
Receive Timeout for connection to Panorama	20 secs
Send Timeout for connection to Panorama	20 secs
Retry Count for SSL send to Panorama	25
Admin Lockout # Failed Attempts Lockout Time	
Number of Versions for Config Audit	100
Stop Traffic when LogDb full	

Figure 17. Setup Page

   b. Click **Edit** on the first table to open the Edit Setup page.

   c. Specify the following information.

Table 1. Host Name and Network Settings

Field	Description
Host Name	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.
Domain	Enter the domain name of the firewall (up to 31 characters).
MGT Interface IP Address	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.
Netmask	Enter the network mask for the IP address, such as "255.255.255.0".
Default Gateway	Enter the IP address of the default router (must be on the same subnet as the management port).
MGT Interface Services	Select the services enabled on the specified management interface address (HTTP, HTTPS, Telnet, SSH, and/or Ping).
RADIUS Server RADIUS Secret	Enter the IP address of the Remote Authentication Dial In User Service (RADIUS) server used for remote authentication (if any), and the secret key defined on the server.
Primary DNS Server Secondary DNS Server	Enter the IP address of the primary and secondary Domain Name Service (DNS) servers. The secondary server address is optional. ***Note:*** *If you entered a DNS server in the Quick Start Setup page, you do not need to reenter it here.*
Primary NTP Server Secondary NTP Server	Enter the IP address or name of the primary and secondary Network Time Protocol (NTP) servers, if any. If you do not use NTP servers, you can set the device time manually (refer to Step 5). ***Note:*** *If you entered an NTP server in the Quick Start Setup page, you do not need to reenter it here.*
System Location	Enter a description of where the firewall is located.
System Contact	Enter the name or email address of the person responsible for maintaining the firewall.
Timezone	Select the time zone of the firewall.
Update Server	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 (refer to "Updating Threat and Application Definitions" on page 88).
Panorama	Enter the IP address of Panorama, the Palo Alto Networks central 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**.
Login Banner	Enter custom text that will be displayed on the firewall login page. The text is displayed below the **Name** and **Password** fields.
MGT Interface Services	Select the services to be enabled on the management interface.

Table 1. Host Name and Network Settings (Continued)

Field	Description
Proxy Server: Server Port User Password	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.
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 SMMP community string.

d. Click **OK** to submit the new settings.

5. To change the current date and time:

a. Click **Set Time** to open the Edit Time page.

b. Specify the following information.

Table 2. Date and Time Settings

Field	Description
Date	Enter the current date: • Click 📅, and select a month and day. or • Enter the date directly (YYYY/MM/DD)
Time	Enter the current time in 24-hour format (HH:MM:SS).

c. Click **OK** to submit the new settings, or click **Cancel** to discard your changes. Changes to the date and time take effect immediately.

6. Click **Commit** at the top-right of the page to activate your changes.

7. Disconnect your computer from the MGT port of the firewall, and connect the MGT port to the enterprise management network.

8. Verify the management configuration.

a. Connect your computer to the enterprise management network.

b. Open a web browser window and enter:

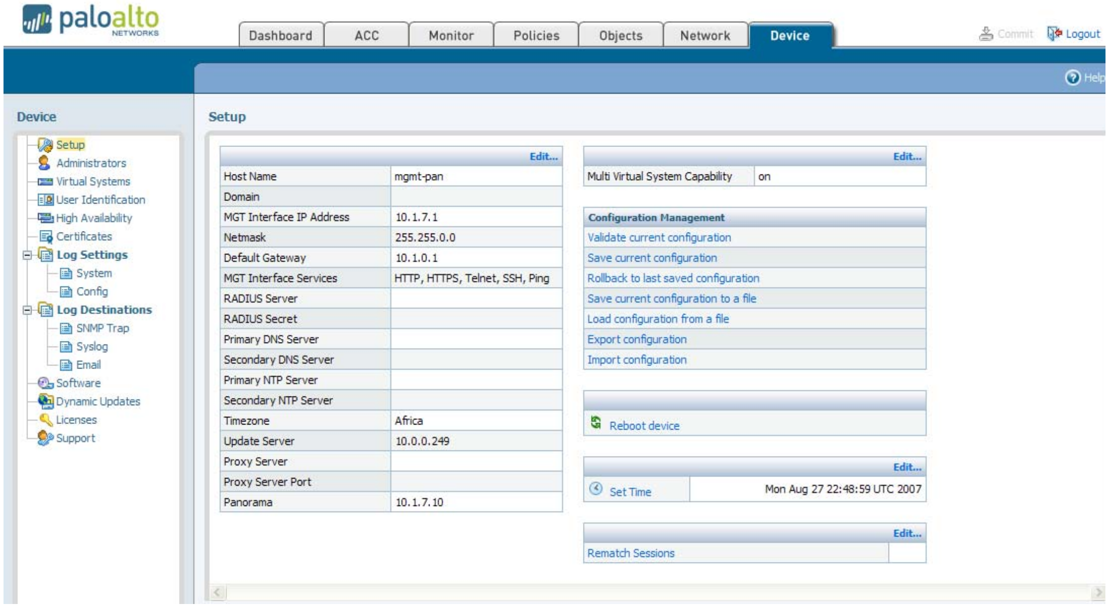
https:<MGT_interface_IP_address>

c. Log in to the web interface of the firewall.

Connecting to Panorama

To allow Panorama to manage your device, you must add the IP address of the Panorama server.

1. Under the **Device** tab, click **Setup** to open the Setup page.



Host Name	mgmt-pan
Domain	
MGT Interface IP Address	10.1.7.1
Netmask	255.255.0.0
Default Gateway	10.1.0.1
MGT Interface Services	HTTP, HTTPS, Telnet, SSH, Ping
RADIUS Server	
RADIUS Secret	
Primary DNS Server	
Secondary DNS Server	
Primary NTP Server	
Secondary NTP Server	
Timezone	Africa
Update Server	10.0.0.249
Proxy Server	
Proxy Server Port	
Panorama	10.1.7.10

Multi Virtual System Capability	on

Set Time	Mon Aug 27 22:48:59 UTC 2007

Figure 18. Setup Page

2. Click **Edit** on the first table to open the Edit Setup page.

3. In the **Panorama** field, enter the IP address of the Panorama server.

4. Click **OK**.

5. Click **Commit** at the top-right of the page to activate your changes.

Post-Installation Tasks

The following table summarizes the tasks performed by the firewall administrator.

Table 3. Summary of Administration Tasks

Task	Description
Monitor Performance	Monitor the status and performance of the firewall using the Dashboard, Application Command Center (ACC), device logs, and reports (refer to “Reports and Logs” on page 215).
Configure Interfaces and Zones	Configure additional interfaces, such as loopback, and VLAN interfaces (to route VLAN traffic), and define profiles to control management access on each interface, and responses to Denial of Service (DOS) attacks in each zone (refer to “Network Configuration” on page 95).

Table 3. Summary of Administration Tasks (Continued)

Task	Description
Identify Users	Obtain user information through a software user identification agent that you can install on your network (refer to “Configuring the User Identification Agent” on page 53).
Configure Policies and Profiles	Configure policies for security, NAT, SSL decryption, URL blocking, and application overrides, as well as the antivirus, anti-spyware, vulnerability, and log forwarding profiles used in security policies (refer to “Policies and Security Profiles” on page 143).
Manage Device Settings and Updates	Configure high availability, define administrator accounts, install licenses, update the PAN-OS software, malware signatures and application definitions, specify remote log destinations for system and configuration logs, enable multiple virtual systems (if supported on the firewall model), request support, and view support updates from Palo Alto Networks (refer to “Device Management” on page 39).

Chapter 3

Device Management

This chapter describes how to perform basic system configuration and maintenance for the firewall:

System Setup and Configuration 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 46
- "Managing Configurations" on page 47

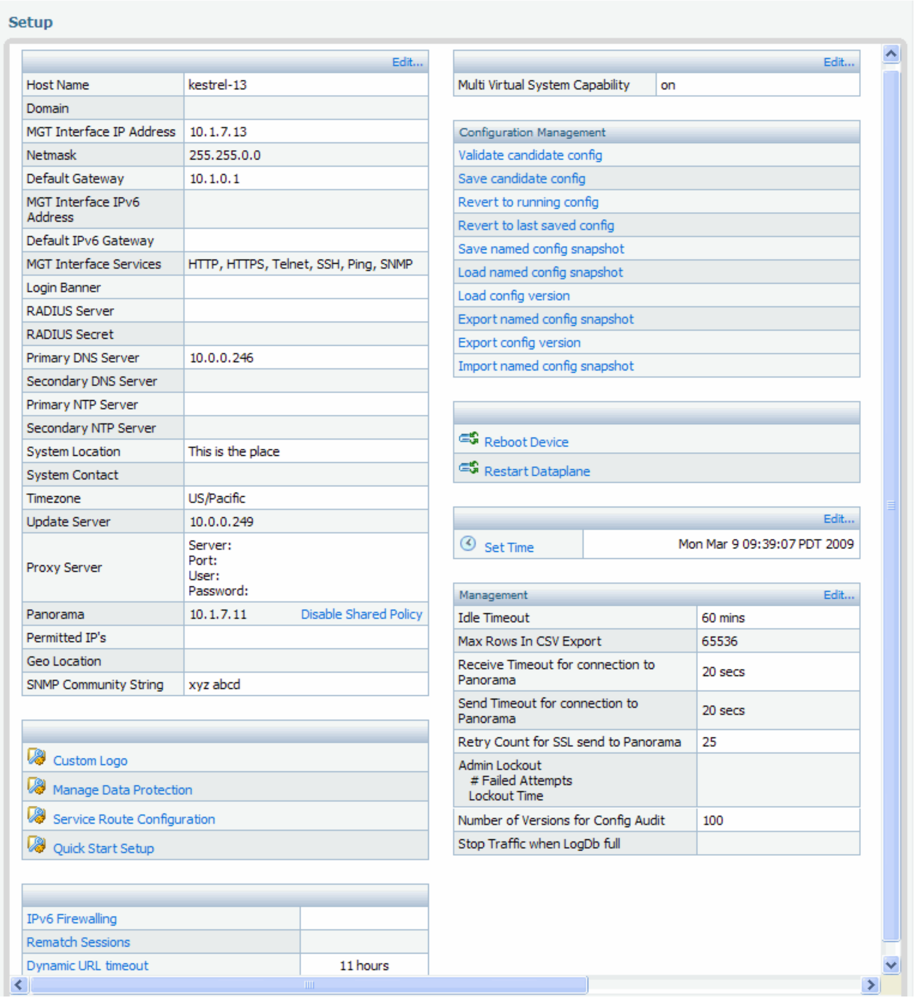
Defining the Host Name and Network Settings

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 112).

To access the Setup page:

1. Under the **Device** tab, click **Setup** to open the Setup page.



Setup

	Edit...
Host Name	kestrel-13
Domain	
MGT Interface IP Address	10.1.7.13
Netmask	255.255.0.0
Default Gateway	10.1.0.1
MGT Interface IPv6 Address	
Default IPv6 Gateway	
MGT Interface Services	HTTP, HTTPS, Telnet, SSH, Ping, SNMP
Login Banner	
RADIUS Server	
RADIUS Secret	
Primary DNS Server	10.0.0.246
Secondary DNS Server	
Primary NTP Server	
Secondary NTP Server	
System Location	This is the place
System Contact	
Timezone	US/Pacific
Update Server	10.0.0.249
Proxy Server	Server: Port: User: Password:
Panorama	10.1.7.11 Disable Shared Policy
Permitted IP's	
Geo Location	
SNMP Community String	xyz abcd

Custom Logo

Manage Data Protection

Service Route Configuration

Quick Start Setup

IPv6 Firewalling	
Rematch Sessions	
Dynamic URL timeout	11 hours

	Edit...
Multi Virtual System Capability	on

Configuration Management

Validate candidate config

Save candidate config

Revert to running config

Revert to last saved config

Save named config snapshot

Load named config snapshot

Load config version

Export named config snapshot

Export config version

Import named config snapshot

Reboot Device

Restart Dataplane

	Edit...
Set Time	Mon Mar 9 09:39:07 PDT 2009

Management	Edit...
Idle Timeout	60 mins
Max Rows In CSV Export	65536
Receive Timeout for connection to Panorama	20 secs
Send Timeout for connection to Panorama	20 secs
Retry Count for SSL send to Panorama	25
Admin Lockout # Failed Attempts Lockout Time	
Number of Versions for Config Audit	100
Stop Traffic when LogDb full	

Figure 19. Setup Page

2. To change the host name or network settings:

   a. Click **Edit** on the first table to open the Edit Setup page.

   b. Specify the following information.

Table 4. Host Name and Network Settings

Field	Description
Host Name	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.
Domain	Enter the domain name of the firewall (up to 31 characters).
MGT Interface IP Address	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.
Netmask	Enter the network mask for the IP address, such as "255.255.255.0".
Default Gateway	Enter the IP address of the default router (must be on the same subnet as the management port).
MGT Interface IPv6 Address	Enter an IPv6 address of the management interface if you want to support IPv6 on the interface.
IPv6 Default Gateway	Enter the address of the default IPv6 gateway if you want to support IPv6 on the management interface.
RADIUS Server RADIUS Secret	Enter the IP address of the RADIUS server used for remote authentication (if any), and the secret key defined on the server.
Primary DNS Server Secondary DNS Server	Enter the IP address of the primary and secondary Domain Name Service (DNS) servers. The secondary server address is optional.
Primary NTP Server Secondary NTP Server	Enter the IP address or name of the primary and secondary Network Time Protocol (NTP) servers, if any. If you do not use NTP servers, you can set the device time manually (refer to Step 5).
System Location	Enter a description of where the firewall is located.
System Contact	Enter the name or email address of the person responsible for maintaining the firewall.
Timezone	Select the time zone of the firewall.
Update Server	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 (refer to "Updating Threat and Application Definitions" on page 88).
Panorama	Enter the IP address of Panorama, the Palo Alto Networks central management system (if any). The server address is required to manage the device through Panorama.
SNMP Community String	Enter an SMMP community string.
MGT Interface Services	Select the services enabled on the specified management interface address (HTTP, HTTPS, Telnet, SSH, and/or Ping).
Login Banner	Enter custom text to display on the firewall login page. The text is displayed below the **Name** and **Password** fields.
Proxy Server: Server Port User Password	If you use a proxy server to provide updates to the firewall, enter the IP address, port number, user name, and password for the proxy server.

Table 4. Host Name and Network Settings (Continued)

Field	Description
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 port.
Geo Location	Enter the latitude (-90.0 to 90.0) and longitude (-180.0 to 180.0) of the firewall.

c. Click **OK** to submit the new settings, or click **Cancel** to discard your changes.

3. To 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 244.

4. To enable the use of multiple virtual systems (if supported on the firewall model), 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 “Defining Virtual Systems” on page 68.

5. To change the current date and time:

   a. Click **Set Time** to open the Edit Time page.

   b. Specify the following information.

Table 5. Date and Time Settings

Field	Description
Date	Enter the current date: • Click 📅, and select a month and day. or • Enter the date directly (YYYY/MM/DD)
Time	Enter the current time in 24-hour format (HH:MM:SS).

   c. Click **OK** to submit the new settings, or click **Cancel** to discard your changes. Changes to the date and time take effect immediately.

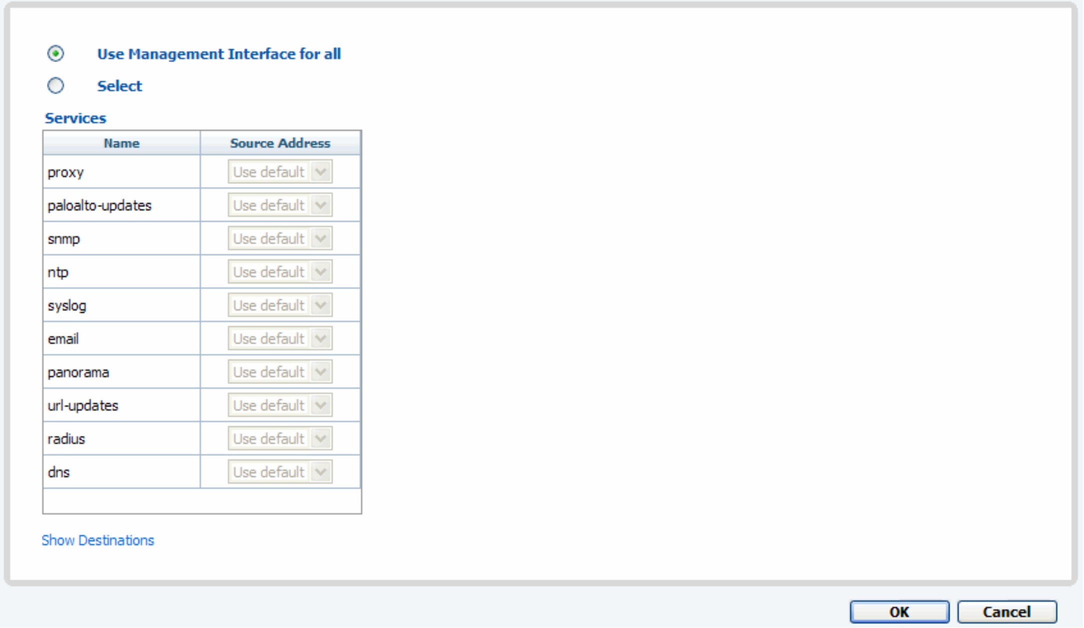
6. Click **Commit** to activate the changes. To save or roll back your configuration changes before activating them, as well as import, load, or export configurations, refer to “Managing Configurations” in the next section.

7. To specify how the firewall communicates with other servers, click **Service Route Configuration**.

   – 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, as shown in the next figure. Select the source from the **Source Address** drop-down list.

   – Click **OK**.



● Use Management Interface for all

○ Select

Services

Name	Source Address
proxy	Use default
paloalto-updates	Use default
snmp	Use default
ntp	Use default
syslog	Use default
email	Use default
panorama	Use default
url-updates	Use default
radius	Use default
dns	Use default

Figure 20. Service Route Configuration

8. To add additional protection for access to logs that may contain sensitive information, such as credit card numbers or social security numbers, click **Manage Data Protection**.

   – To set a new password if one has not already been set, click **Set data access password**. Enter and confirm the password, and click **OK**.

   – To change the password, click **Change data access password**. Enter the old password, enter and confirm the new password, and click **OK**.

   – To delete the password and the data that has been protected, click **Delete data access password and protected data**, and click **OK**. Click **OK** to confirm.

9. To restart the firewall or to restart the data plane without rebooting (traffic will be stopped during this operation):

   – Click **Reboot Device** to restart the firewall. Click **OK** to confirm. You will be logged out while the PAN-OS software and active configuration are reloaded. Any configuration changes that have not been saved or committed will be lost (refer to “Managing Configurations” in the next section).

   – Click **Restart Dataplane** to restart the data functions without rebooting. Click **OK** to confirm.

10. To enforce the new policy for existing sessions:
    a. Click **Rematch S**essions to open the Edit Rematch Sessions page.
    b. Select the check box and click **OK**.

    Rematch sessions 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.

11. To enable firewall capabilities for IPv6, click **Edit** for IPv6 Firewalling. Select the check box and click **OK**. IPv6 objects apply only to virtual wire policies. All IPv6-based configurations are ignored if IPv6 is not enabled.

12. To configure the timeout for the dynamic URL cache, click **Dynamic URL timeout**, enter the timeout (in hours), and click **OK**. 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. Refer to "Defining URL Filtering Profiles" on page 178 for information on URL filtering.

13. To set management parameters, including timeouts, CSV exports, and connections to Panorama, click **Edit** in the **Management** area and specify the following information.

Table 6. Management Settings

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

14. Click **OK**.

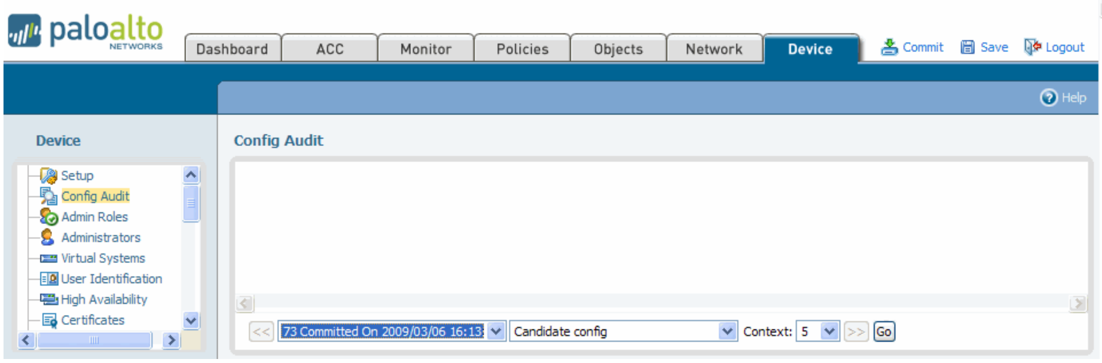
Comparing Configuration Files

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.

You can view and compare configuration files by using the Config Audit page.

To compare configuration files:

1. Under the **Device** tab, click **Config Audit** to open the Config Audit page.

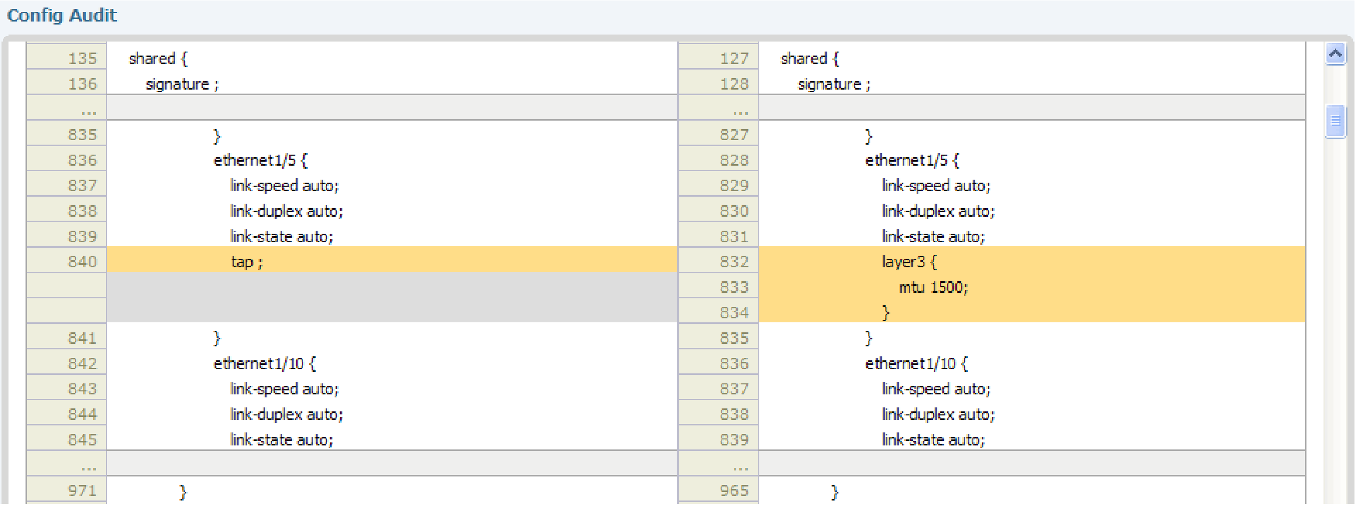


73 Committed On 2009/03/06 16:13 | Candidate config | Context: 5

Figure 21. Config Audit Page

2. From the drop-down lists, select the configurations that you want to compare.
3. Select whether to view the differences in a side-by-side display or as inline comparisons.
4. Select the number of lines that you want to include for context.
5. Click **Submit**.

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



```
135  shared {                         127  shared {
136    signature ;                    128    signature ;
...                                   ...
835            }                      827            }
836            ethernet1/5 {          828            ethernet1/5 {
837              link-speed auto;     829              link-speed auto;
838              link-duplex auto;    830              link-duplex auto;
839              link-state auto;     831              link-state auto;
840              tap ;                832              layer3 {
                                      833                mtu 1500;
                                      834              }
841            }                      835            }
842            ethernet1/10 {         836            ethernet1/10 {
843              link-speed auto;     837              link-speed auto;
844              link-duplex auto;    838              link-duplex auto;
845              link-state auto;     839              link-state auto;
...                                   ...
971        }                          965        }
```

Figure 22. Configuration Comparison

Managing Configurations

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. Activating multiple changes simultaneously helps avoid invalid configuration states that can occur when changes are applied in real-time, and allows the configuration to be reviewed before being activated.

You can save and roll back (restore) the candidate configuration as often as needed and also load, validate, import, and export configurations.

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:

1. Click **Setup** under the **Device** tab.
2. Select the appropriate configuration management functions.

Table 7. Configuration Management Functions

Function	Description
Validate candidate config	Checks the candidate configuration for errors.
Save candidate config	Saves the candidate configuration in flash memory (same as clicking **Save** at the top of the page).
Revert to running config	Restores the last running configuration. The current running configuration is overridden.
Revert to last saved config	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.
Save named config snapshot	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 (*running-config.xml*) cannot be overwritten.
Load named config snapshot	Loads a candidate configuration from the active configuration (*running-config.xml*) or from a previously imported or saved configuration. Select the configuration file to be loaded. The current candidate configuration is overwritten.
Load config version	Loads a specified version of the configuration.
Export named config snapshot	Exports the active configuration (*running-config.xml*) 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.
Export config version	Exports a specified version of the configuration.
Import named config spreadsheet	Imports a configuration file from any network location. Click **Browse** and select the configuration file to be imported.

Note: When you click ***Commit*** *or enter a* ***commit*** *CLI command, all changes made through the GUI and the CLI since the last commit are activated. To avoid possible conflicts, use only the GUI or CLI for most configuration changes.*

Managing Administrator Roles

You can specify the access and responsibilities that should be assigned to administrative users.

To define administrator roles:

1. Under the **Device** tab, click **Admin Roles** to open the Admin Roles page.

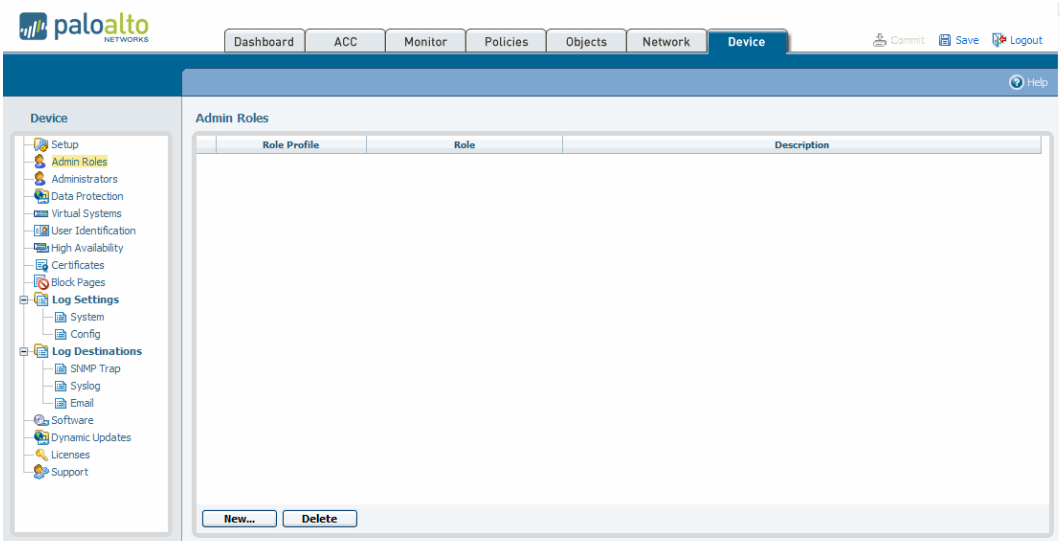
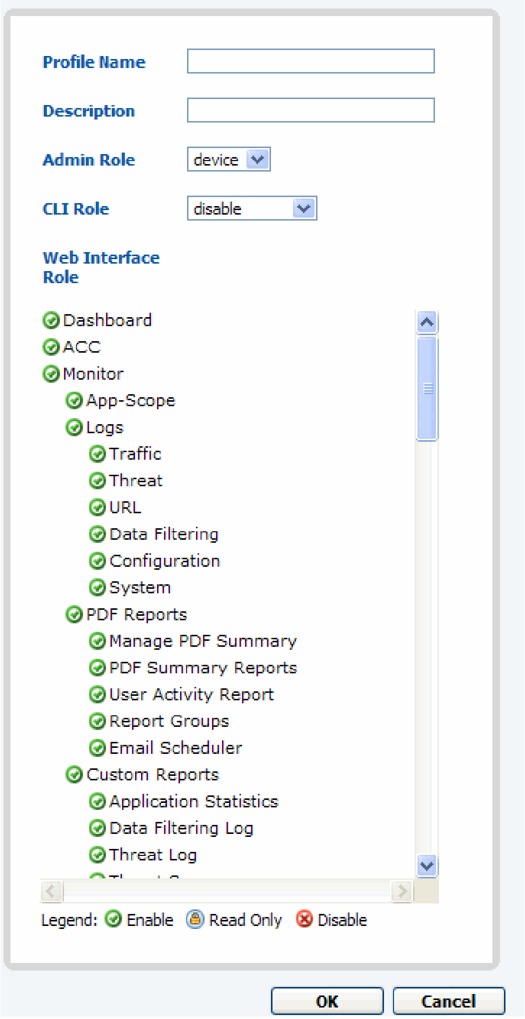


Figure 23. Admin Roles Page

2. To add a new administrator role:

   a. Click **New** to open the **New Administrator** page.



Profile Name

Description

Admin Role: device

CLI Role: disable

Web Interface Role

- ✓ Dashboard
- ✓ ACC
- ✓ Monitor
  - ✓ App-Scope
  - ✓ Logs
    - ✓ Traffic
    - ✓ Threat
    - ✓ URL
    - ✓ Data Filtering
    - ✓ Configuration
    - ✓ System
  - ✓ PDF Reports
    - ✓ Manage PDF Summary
    - ✓ PDF Summary Reports
    - ✓ User Activity Report
    - ✓ Report Groups
    - ✓ Email Scheduler
  - ✓ Custom Reports
    - ✓ Application Statistics
    - ✓ Data Filtering Log
    - ✓ Threat Log

Legend: ✓ Enable 🔒 Read Only ⊗ Disable

Figure 24. New Admin Role Page

   b. Specify the following information.

Table 8. New Administrator

Field	Description
Profile Name	Enter a name to identify this administrator role.
Description	Enter an optional description of the role.
Admin Role	Select the general scope of administrative responsibility from the drop-down list.

Table 8. New Administrator (Continued)

Field	Description
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. • **superreader** — Read-only access to the current device. • **deviceadmin** — Full access to a selected device, except for defining new accounts or virtual systems. • **devicereader**— Read-only access to a selected device.
WebUI Role	Click the icons for specified areas to indicate the type of access permitted in the GUI: • ✓ Read/write access to the indicated page. • 📄 Read only access to the indicated page. • ✖ No access to the indicated page.

c. Click **OK** to submit the new role, or click **Cancel** to discard your changes.

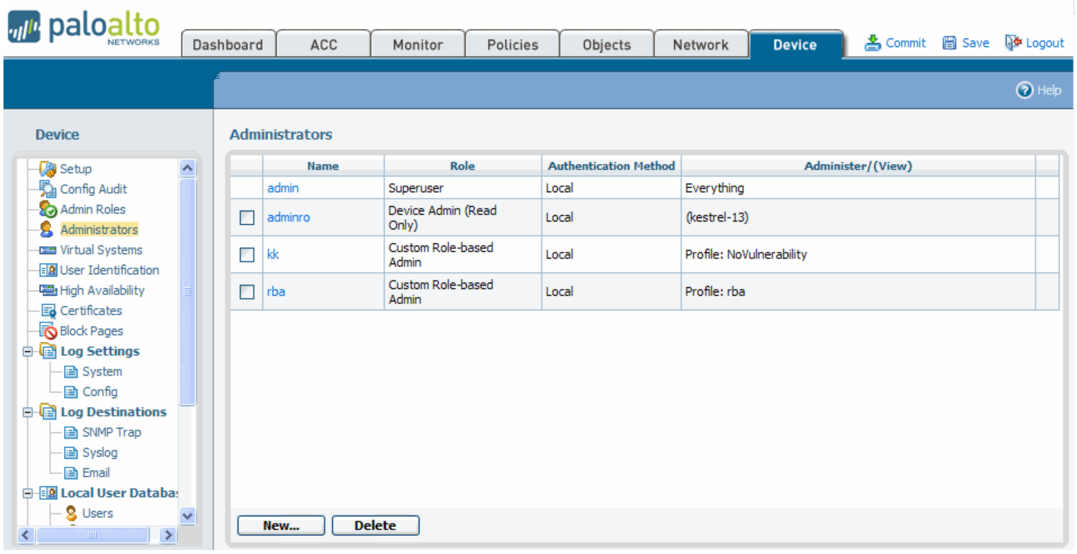
3. To change an administrator role, click the role as listed on the Administrators page, change the account settings, and click **OK**. To delete an account, select the account and click **Delete**.

Creating Administrative Accounts

Administrator accounts control access to the firewall. Each administrator can have full or read-only access to a single device, or a virtual system on a single device. The predefined **admin** account has full access to each device. 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 define local administrator accounts:

1. Under the **Device** tab, click **Administrators** to open the Administrators page.



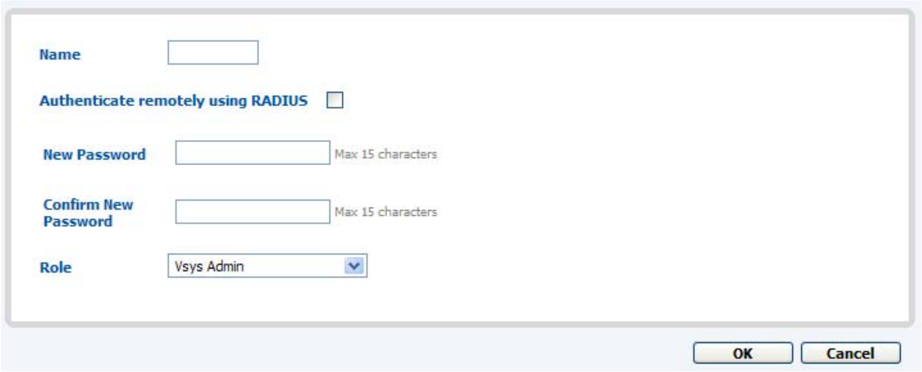
Administrators

	Name	Role	Authentication Method	Administer/(View)
	admin	Superuser	Local	Everything
□	adminro	Device Admin (Read Only)	Local	(kestrel-13)
□	kk	Custom Role-based Admin	Local	Profile: NoVulnerability
□	rba	Custom Role-based Admin	Local	Profile: rba

Figure 25. Administrators Page

2. To add a new administrator account:

   a. Click **New** to open the New Administrator page.



Name

Authenticate remotely using RADIUS □

New Password Max 15 characters

Confirm New Password Max 15 characters

Role Vsys Admin

Figure 26. New Administrators Page

b. Specify the following information.

Table 9. New Administrator

Field	Description
Name	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.
Authenticate remotely using RADIUS	Click the check box to use your RADIUS server to authenticate the user. To define the RADIUS server address, refer to “Defining the Host Name and Network Settings” on page 40.
New Password Confirm New Password	Enter and confirm a case-sensitive password for the user (up to 15 characters).
Role	Select a role to specify the user’s access and confirm if prompted. The roles are: • **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. • **Vsys Admin** — Full access to a selected virtual system on a specific device (if multiple virtual systems are enabled). • **Vsys Admin (Read Only)** — Read-only access to a selected virtual system on a specific device. • **Role Based Admin** — Access based on assigned roles, as defined in “Managing Administrator Roles” on page 48.

c. Click **OK** to submit the new account, or click **Cancel** to discard your changes.

3. To change an account, click the account name on the Administrators page, change the account settings, and click **OK**. To delete an account, select the check box next to the account and click **Delete**.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Note: *In Panorama, 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.*

Configuring User Identification

This section describes the Palo Alto Networks User Identification Agent , which identifies users who want to access the network, and the Terminal Services Agent (TS Agent), which allows the firewall to identify individual users that are supported by the same terminal server.

Configuring the User Identification Agent

The firewall can use any of the following methods for user identification:

- User Identification Agent with Active Directory
- Captive Portal with Windows NT LAN Manager (NTLM)
- Captive Portal with Web Forms

The User Identification Agent is available for download from Palo Alto Networks. The 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. This is the preferred method of user identification.

When the User Identification Agent with Active Directory is unable to associate a user with an IP address, the captive portal methods can take over to identify the user from a browser. If the NTLM method is unable to identify users from the captive portal, the last option is to solicit information directly from the user by way of a web form. The NTLM option is preferred to the web form option, because you can configure it to work without user intervention.

Each method initiates a process to map users to IP addresses. When the mapping is in place, all IP traffic from the mapped IP address is associated with the mapped user for the purposes of visibility and policy enforcement.

You can install the User Identification Agent on one or more Windows PCs on your network to obtain user-specific information. When user identification is configured, the firewall's Application Control Center, App-Scope, and logs all include the user name in addition to IP address. For policy enforcement, users and user groups can be selected in security and SSL decryption policies when Active Directory is used. However, if a RADIUS server is used without the User Identification Agent, you must manually add user names for enforcement.

Note: *If the multiple virtual system capability is on (PA-4000 Series only), 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. Refer to "Defining Virtual Systems" on page 68.*

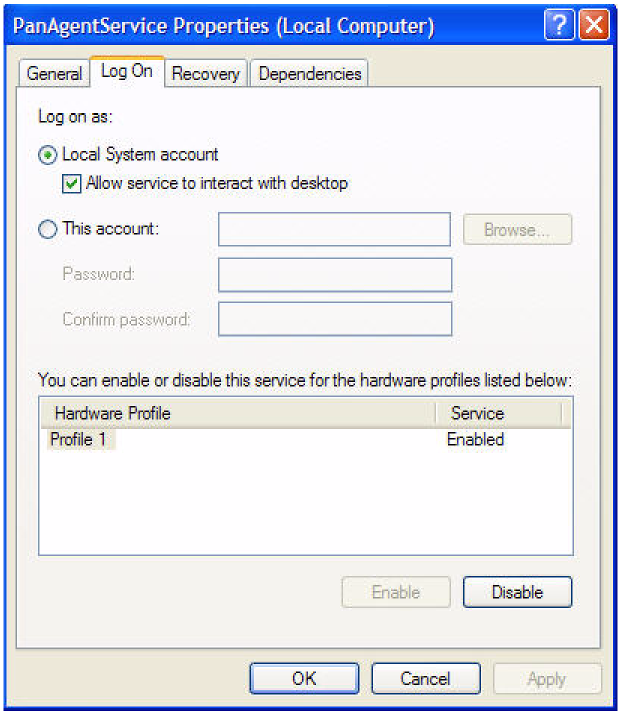
Follow the instructions in this section to install and configure the User Identification Agent.

Verifying Privileges for the PC User

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

To verify the privilege level of the PC user:

1. Choose **Control Panel > Administrative Tools > Services.**
2. Right-click **PANAgentService** and select **Properties**.
3. Open the **Log On** tab.



PanAgentService Properties (Local Computer)

Log on as:

● Local System account

☑ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

Figure 27. User Identification 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 Identification Agent

The user identification feature is designed for Active Directory deployments, and 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.

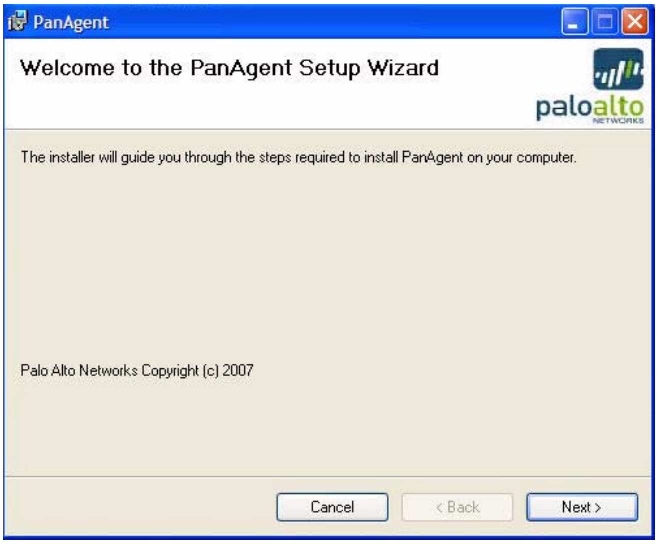
The system on which the User Identification Agent is installed must be running Windows 2008, Windows XP with Service Pack 2, or Windows Server 2003 with Service Pack 2.

Refer to these sections for additional information:

- "Defining Virtual Systems" on page 68—Describes how to enable captive portal and configure authentication.
- "Defining Captive Portal Policies" on page 160—Describes how to set up captive portal policies.

To install the User Identification Agent:

1. Open the installer file to display the Welcome page.



PanAgent

Welcome to the PanAgent Setup Wizard

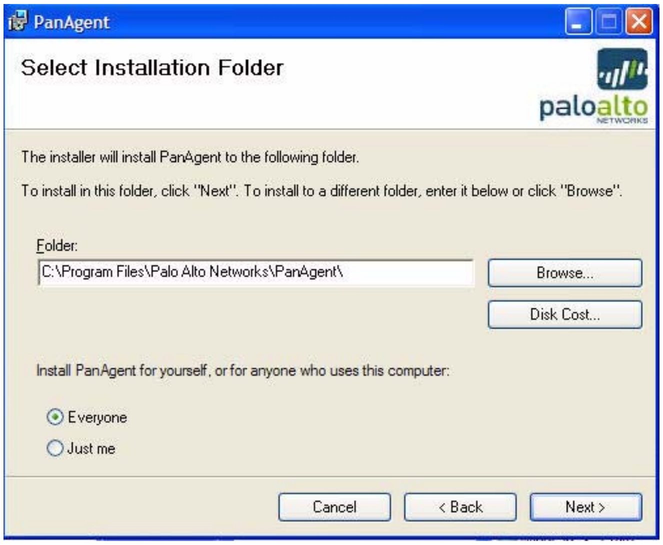
The installer will guide you through the steps required to install PanAgent on your computer.

Palo Alto Networks Copyright (c) 2007

Figure 28. User Identification Agent Wizard - Welcome

2. Click **Next**.

3. Choose an installation folder and disk and select whether to make the agent available just for you or for all users of this machine.



Select Installation Folder

The installer will install PanAgent to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\Palo Alto Networks\PanAgent\

Install PanAgent for yourself, or for anyone who uses this computer:

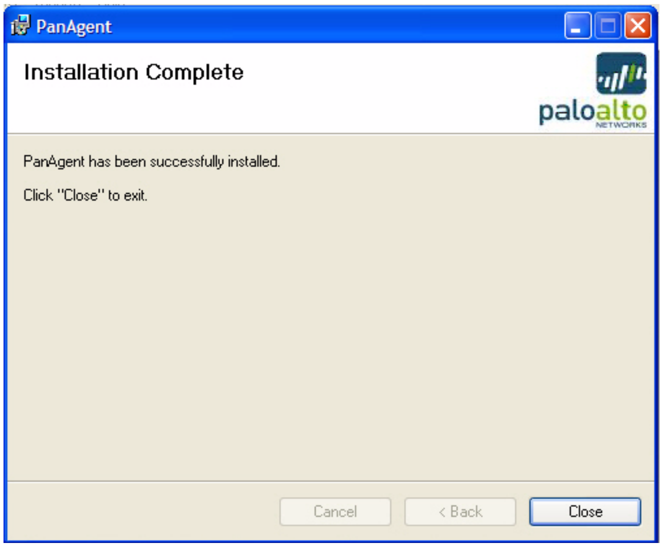
● Everyone
○ Just me

Figure 29. User Identification Agent Wizard - Select Installation Folder

4. Click **Next**.

5. Click **Next** to begin the installation.

6. A message is displayed when the installation is complete. Click **OK** to acknowledge the message, and then click **Close** to exit the installation wizard.



Installation Complete

PanAgent has been successfully installed.

Click "Close" to exit.

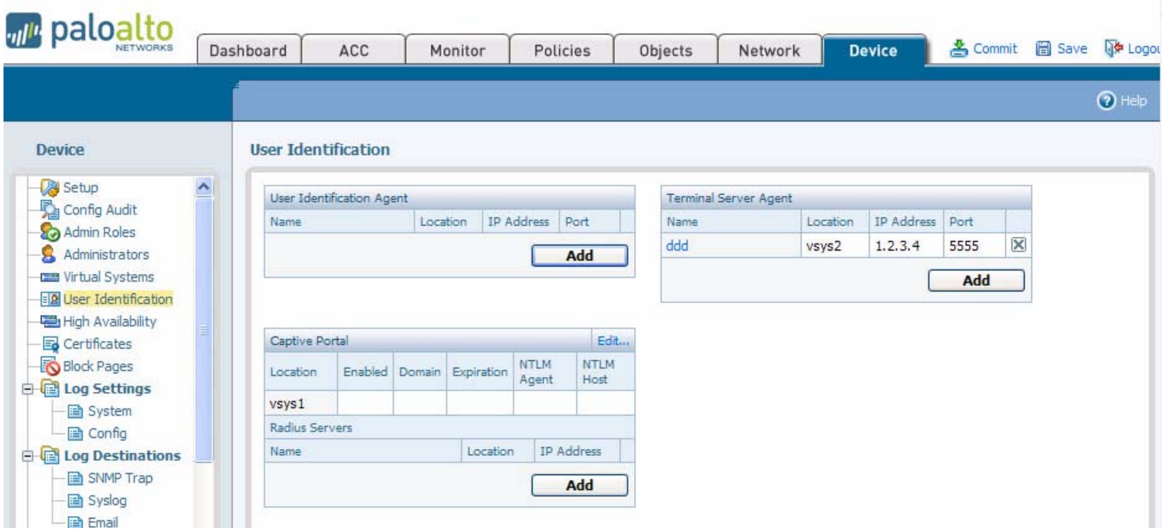
Figure 30. User Identification Agent Wizard - Installation Complete

Now that you have installed the User Identification Agent, the next step is to configure the firewall to communicate with the User Identification Agent, as described in the next section.

Configuring the Firewall to Communicate with the User Identification Agent

To configure the firewall to communicate with the User Identification Agent:

1. Under the **Device** tab, click **User Identification** to open the User Identification Agent page.



User Identification Agent

Name	Location	IP Address	Port

Terminal Server Agent

Name	Location	IP Address	Port
ddd	vsys2	1.2.3.4	5555

Captive Portal

Location	Enabled	Domain	Expiration	NTLM Agent	NTLM Host
vsys1					

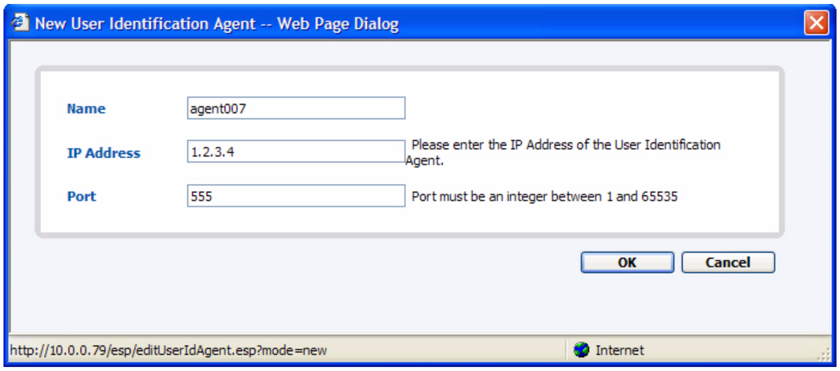
Radius Servers

Name	Location	IP Address

Figure 31. User Identification Agent Page

2. To add a new User Identification Agent:

   a. Click **New** to open the New User Identification page.



Name	agent007	
IP Address	1.2.3.4	Please enter the IP Address of the User Identification Agent.
Port	555	Port must be an integer between 1 and 65535

http://10.0.0.79/esp/editUserIdAgent.esp?mode=new

Figure 32. New User Identification Agent Page

b. Specify the following information.

Table 10. User Identification Agent Settings

Field	Description
Name	Enter a name to identify the User Identification Agent.
IP Address	Enter the IP address of the Windows PC on which the user identification is installed.
Port	Enter a port number of your choice for communication between the firewall and the agent.

c. Click **OK** to submit the information, or click **Cancel** to discard your changes.

d. Click **New** to add additional agents, as needed.

3. To enable captive portal and to configure RADIUS servers to authenticate users who enter through captive portals:

   a. Click the captive portal **Edit** link.

   b. Select **Enable Captive Portal** and click **OK**.

   c. Click **Add** in the captive portal area.

   d. Enter the RADIUS server name, IP address, and the shared secret code that authorizes communication between the firewall and server.

   e. Click **OK**. The server information is listed in the captive portal area. Click the **x** next to a server name if you need to delete the server. If you need to modify settings, delete the server and then add it again.

4. To change information for a User Identification Agent, click the agent name on the User Identification Agent page, change the account settings, and click **OK**. To delete a User Identification Agent, select the check box next to the account and click **Delete**.

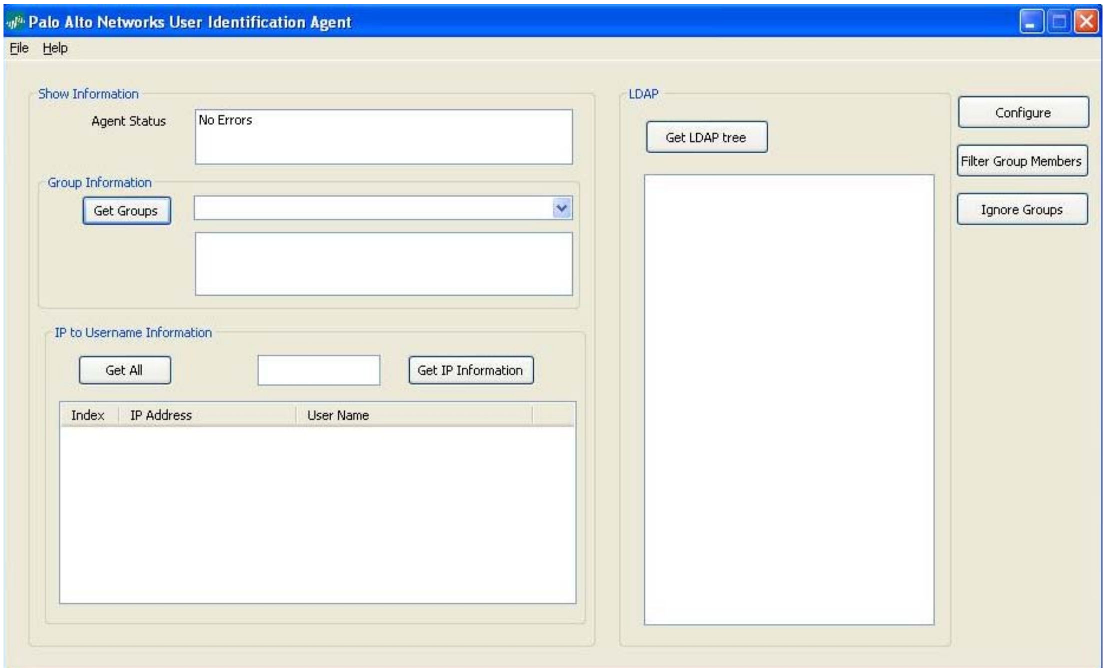
5. Click **Commit** to activate the changes.

The firewall now automatically collects information about user groups, users, and machines that are deployed on the network and incorporates that information into policies and the reports that are available on the Monitor and ACC tabs. Refer to "Policies and Security Profiles" on page 143 for information on policies and "Reports and Logs" on page 215 for information on the Monitor and ACC tabs.

Configuring the User Identification Agent

To open the User Identification Agent:

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



Agent Status No Errors

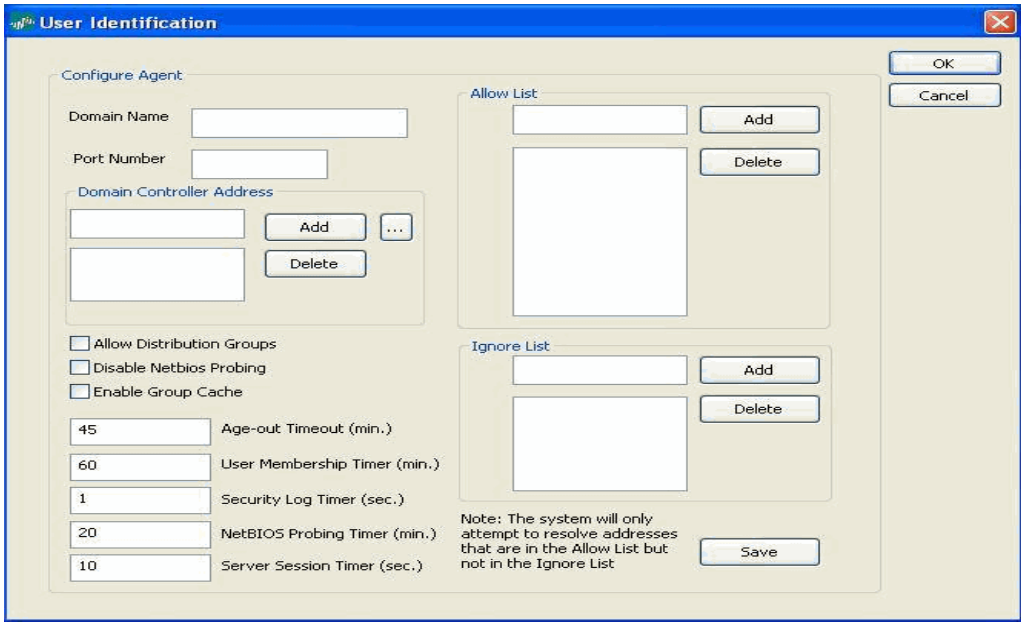
Figure 33. User Identification Agent Window

The window contains the following areas and functions:

- **Agent Status**—Displays the current status of the User Identification Agent.
- **Get Groups**—Lists the groups that were able to be 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 the Lightweight Directory Access Protocol (LDAP). Click **Get LDAP tree** to refresh this information.
- **Configure—**Allows you to configure settings for the User Identification Agent.
- **Filter Group Members—**Configures the groups from which the agent should extract users. Only the users that belong to the selected filtered groups will be read from the Domain Controller. This option can minimize the traffic between the User Identification Agent and the Domain Controller, and thereby improve overall performance. This approach is effective if there are numerous groups, but only a few are to be used in device policy.
- **Ignore Groups—**Configures the groups with users that the User Identification 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 Identification Agent.

To configure the User Identification Agent:

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



□ Allow Distribution Groups
□ Disable Netbios Probing
□ Enable Group Cache

45 Age-out Timeout (min.)
60 User Membership Timer (min.)
1 Security Log Timer (sec.)
20 NetBIOS Probing Timer (min.)
10 Server Session Timer (sec.)

Note: The system will only attempt to resolve addresses that are in the Allow List but not in the Ignore List

Figure 34. 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. 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.
6. 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.
7. Select the **Distribution Groups** check box to allow distribution groups to be part of the information sent to the firewall.
8. Select the **Disable Netbios Probing** check box to disable NETBIOS probing for each workstation. When this check box is selected, the User Identification Agent relies only on security logs and session information.
9. 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 Identification Agent is restarted, it first reloads the user-group membership from the cache to speed up the restart process.

10. Configure timer values as needed:

    – **Agent-out Timeout—**Timeout values for user entries. If this field is left blank, the default timeout value 45 minutes will be used. If Netbios Probing is disabled, entries do not time out.

    – **User Membership Timer—**Length of timer interval when the user-group membership will be updated. Default is 60 minutes.

    – **Security Log Timer—**Length of timer interval when the new domain controller security log will be read. Default is 1 second.

    – **NetBIOS Probing Timer—**Length of timer interval when the NetBIOS Probing will be started. Default is 20 minutes.

    – **Server Session Timer—**Length of timer interval when the domain controller server session will be read. Default is 10 seconds.

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

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

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

Configuring the Firewall to Support Terminal Servers

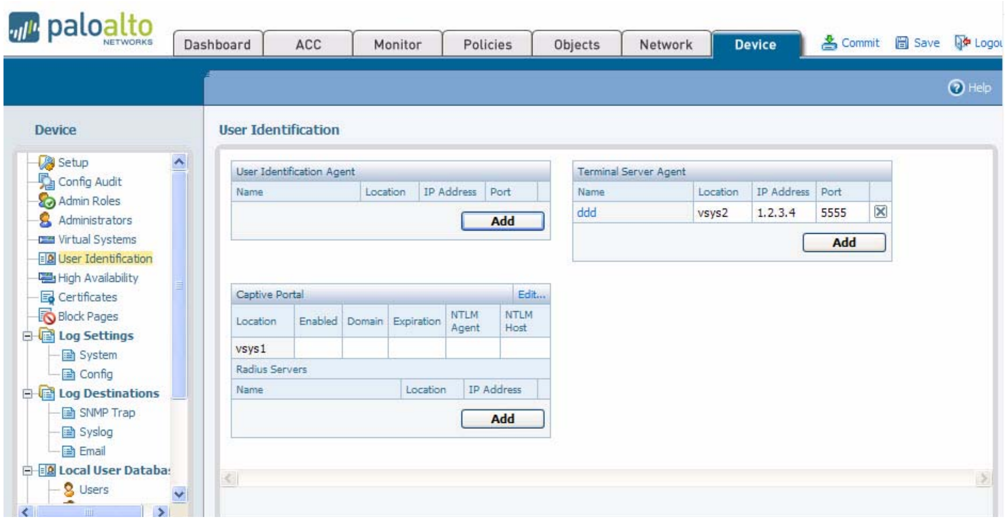
The firewall provides a Terminal Server Agent (TS agent) that runs on a terminal server and identifies individual users that the terminal server supports. This arrangement allows the firewall to support multiple users with the same source IP address. The TS agent monitors the remote user sessions and 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:

1. Under the **Device** tab, click **User Identification** to open the User Identification page.



User Identification

User Identification Agent

Name	Location	IP Address	Port

Terminal Server Agent

Name	Location	IP Address	Port
ddd	vsys2	1.2.3.4	5555

Captive Portal

Location	Enabled	Domain	Expiration	NTLM Agent	NTLM Host
vsys1					

Radius Servers

Name	Location	IP Address

Figure 35. Terminal Server Agent Setup

2. To add a TS agent:

   a. Click **Add** in the Terminal Server Agent area.

   b. Specify the following information.

Table 11. Terminal Server Agent Setup

Field	Description
Name	Enter a name to identify the TS agent.
Virtual system	Select the virtual system from the drop-down list (if supported on the firewall model).

Table 11. Terminal Server Agent Setup (Continued)

Field	Description
IP Address	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).
Port	Enter a port number of your choice for communication between the firewall and the TS agent.
Alternative IP Addresses	Enter additional IP addresses, if the server has multiple IP addresses that can appear as the source IP address for the outgoing traffic.

c. Click **OK**.

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. It 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.

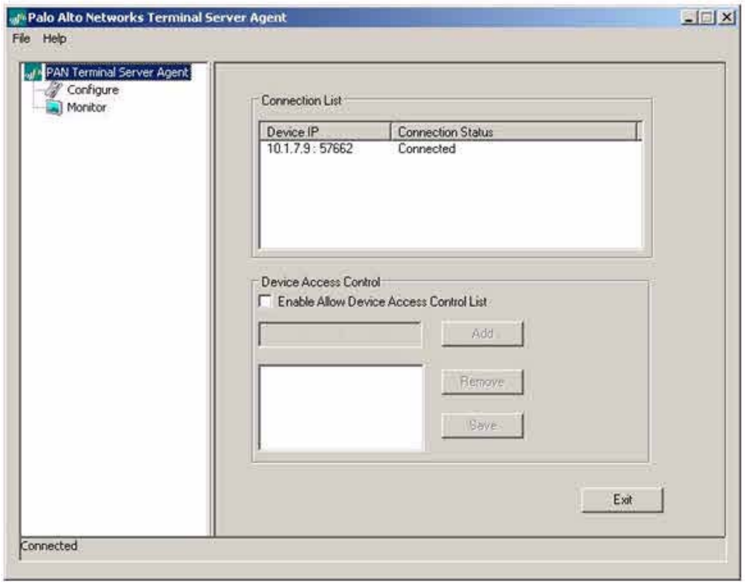
Uninstalling the Terminal Server Agent on the Terminal Server

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 either when you perform the uninstallation or at a later time.

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.



Device IP	Connection Status
10.1.7.9 : 57662	Connected

□ Enable Allow Device Access Control List

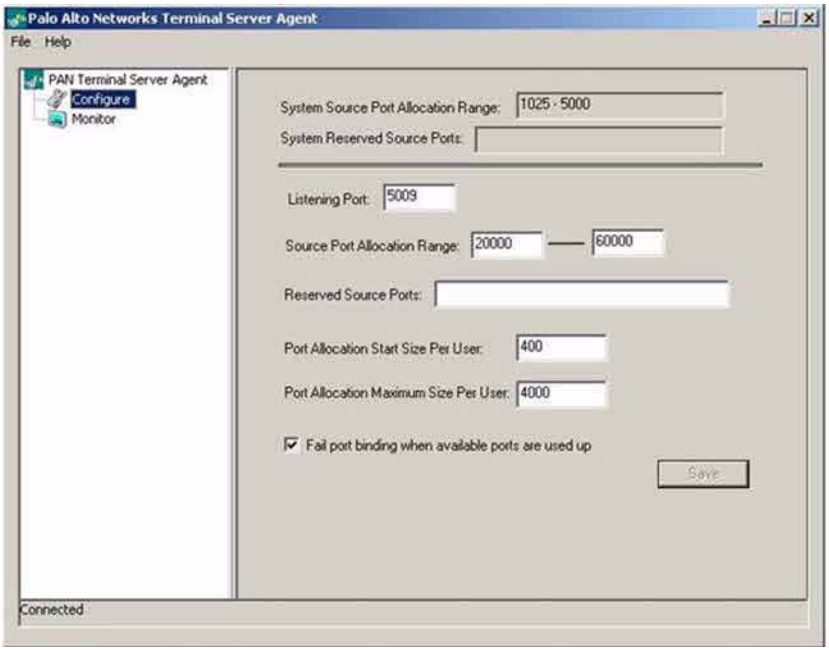
Connected

Figure 36. Terminal Server Agent Configuration - Main Panel

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.


Palo Alto Networks Terminal Server Agent
File Help
PAN Terminal Server Agent
Configure
Monitor
Save
Connected

System Source Port Allocation Range: 1025 - 5000

System Reserved Source Ports:

Listening Port: 5009

Source Port Allocation Range: 20000 — 60000

Reserved Source Ports:

Port Allocation Start Size Per User: 400

Port Allocation Maximum Size Per User: 4000

☑ Fail port binding when available ports are used up

Figure 37. Terminal Server Agent Configuration - Configure Panel

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.*

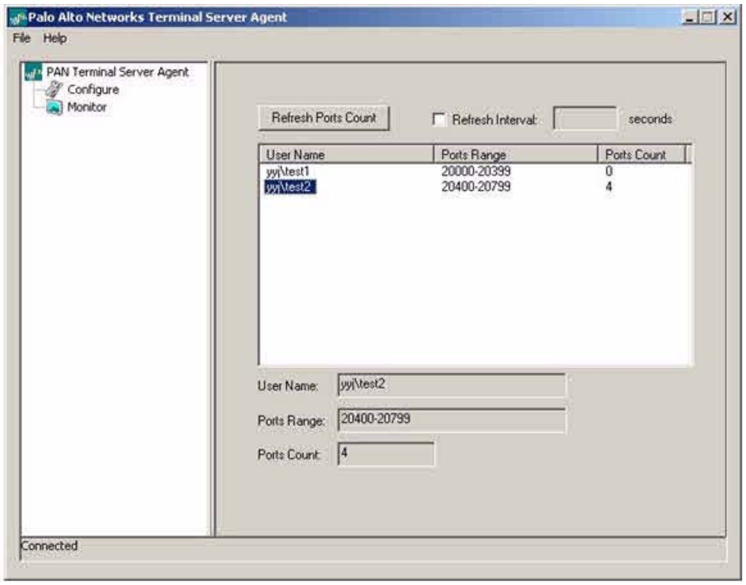
Table 12. Terminal Server Agent Configuration Settings

Field	Description
System Source Port Allocation Range	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*. The default is "1025-5000." ***Note:*** *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.* ***Note:*** *Modifying this value requires a Registry change and cannot be done from this panel.*
System Reserved Source Ports	Displays the port or ports to be excluded from the operating system source port allocation (because they may be used by other server processes). You can enter a range: *low-high* (no default). ***Note:*** *Modifying this value requires a Registry change and cannot be done from this panel.*

Table 12. Terminal Server Agent Configuration Settings (Continued)

Field	Description
Listening Port	Enter the port on which the terminal server will listen for communications from Palo Alto Networks firewalls. The default is "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. 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). The default is "20000-39999". ***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*. There is 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. 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. The default is "200".
Port Allocation Maximum Size Per User	Enter the maximum number of ports that the TS agent can allocate for a remote user session. 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. The default is "2000".
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.

6. Click **Monitor** to display the port allocation information for all terminal server users.


Palo Alto Networks Terminal Server Agent
File
Help
PAN Terminal Server Agent
Configure
Monitor
Refresh Ports Count

☐ Refresh Interval: seconds

User Name	Ports Range	Ports Count
yyj\test1	20000-20399	0
yyj\test2	20400-20799	4

User Name: yyj\test2

Ports Range: 20400-20799

Ports Count: 4

Connected

Figure 38. 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 13. Terminal Server Agent Monitor Information

Field	Description
User Name	Displays the user name.
Ports Range	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 12.
Ports Count	Indicates the number of ports in use by the user.

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 14. Terminal Server Agent Menu Options

Field	Description
Configure	Open the Configuration panel.
Monitor	Open the Monitor panel.
Restart Service	Restart the TS agent service. This option is not normally required and is reserved for troubleshooting.
Show Logs	Display the troubleshooting log.
Debug	Select debugging options (None, Error, Information, Debug, or Verbose).
Exit	Quit the TS agent application.
Help	Display TS agent version information.

Defining Virtual Systems

Interfaces and security zones can be grouped into virtual systems, and then managed independently of each other. For example, if you define virtual systems for the interfaces associated with specific departments or customers, you can then customize the administrative access, security policies, and logging for each department or customer. You can also define administrator accounts that provide administrative or view-only access to a single virtual system. Initially all interfaces, zones, and policies belong to the default virtual system (vsys1).

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

When you enable multiple virtual systems, note the following:

- Interfaces, zones, VLANs, virtual wires, and virtual routers must be assigned to a virtual system (a **Virtual System** column is added to the respective pages).
- A **Virtual System** drop-down list is added under the Policies and Objects tabs. Before defining a policy or policy object, you must select the appropriate virtual system.
- 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.

To define virtual systems:

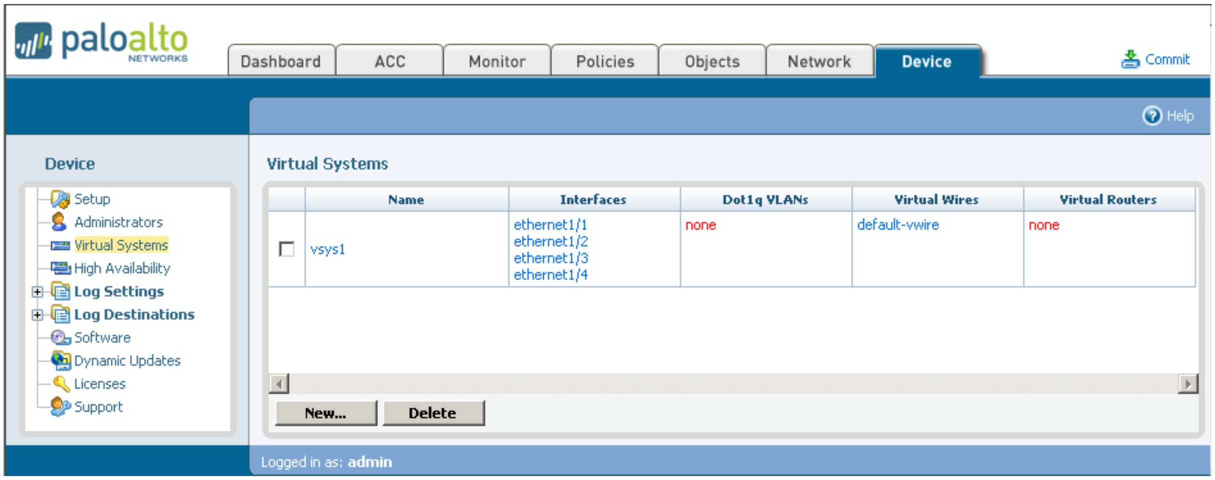
1. Enable the definition of multiple virtual systems:

   a. Under the **Device** tab, click **Setup** to open the Setup page.

   b. Click **Edit** on the second table, select the check box for Allow multiple virtual systems, and click **OK**.

   A Virtual Systems link is added to the left menu frame.

2. Click **Virtual Systems** to open the Virtual Systems page.



	Name	Interfaces	Dot1q VLANs	Virtual Wires	Virtual Routers
□	vsys1	ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/4	none	default-vwire	none

Figure 39. Virtual Systems Page

3. To add a new virtual system:

   a. Click **New** to open the New Virtual System page.

   b. Specify the following information.

Table 15. Host Name and Network Settings

Field	Description
Virtual System	Enter the virtual system name (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.
Interfaces Dot1q VLANs Virtual Wires Virtual Routers	Select the physical and logical interfaces, VLANs, virtual wires, and virtual routers that belong to the virtual system. Alternatively, you can select or change the virtual system when configuring each network component, as described in: • "Configuring Interfaces" on page 98 • "Defining VLANs" on page 119 • "Defining Virtual Wires" on page 120 • "Defining Virtual Routers" on page 122 Note that each interface, VLAN, virtual wire, and virtual router can belong to only one virtual system.

   c. Click **OK** to submit the new settings, or click **Cancel** to discard your changes.

4. To change a virtual system, click the virtual system name or the name of the interface, VLAN, virtual wire, or virtual router you want to change, make the appropriate changes, and click **OK**.
5. Click **Network > Zones** and define security zones for each new virtual system (refer to “Defining Security Zones” on page 116). When you define a new zone, you can now select a virtual system.
6. Click **Network > Interfaces** and verify that each interface has a virtual system and security zone.
7. To save or roll back your configuration changes before activating them, refer to “Managing Configurations” on page 47.

Configuring 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 one or more specified destinations cannot be reached by the active firewall.

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 HA interfaces.
- If the active firewall fails, then the passive firewall detects that heartbeats are lost and automatically becomes active.
- If one HA 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 switch-over; however, threat prevention functions do not continue.*

Note: *On the PA-2000 Series and PA-500 firewalls, you specify the data ports to be used for HA. On the PA-4000 Series, there are dedicated physical ports for HA.*

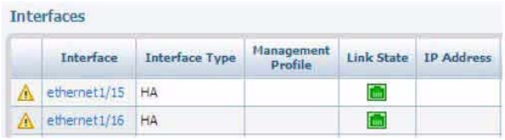
To configure high availability:

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, use the **request system** command to perform a factory reset, as described in 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 the two crossover RJ-45 Ethernet cables provided, 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 Series, you must use the traffic interfaces for HA. 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 HA links are up. Configure each to be of the type HA.



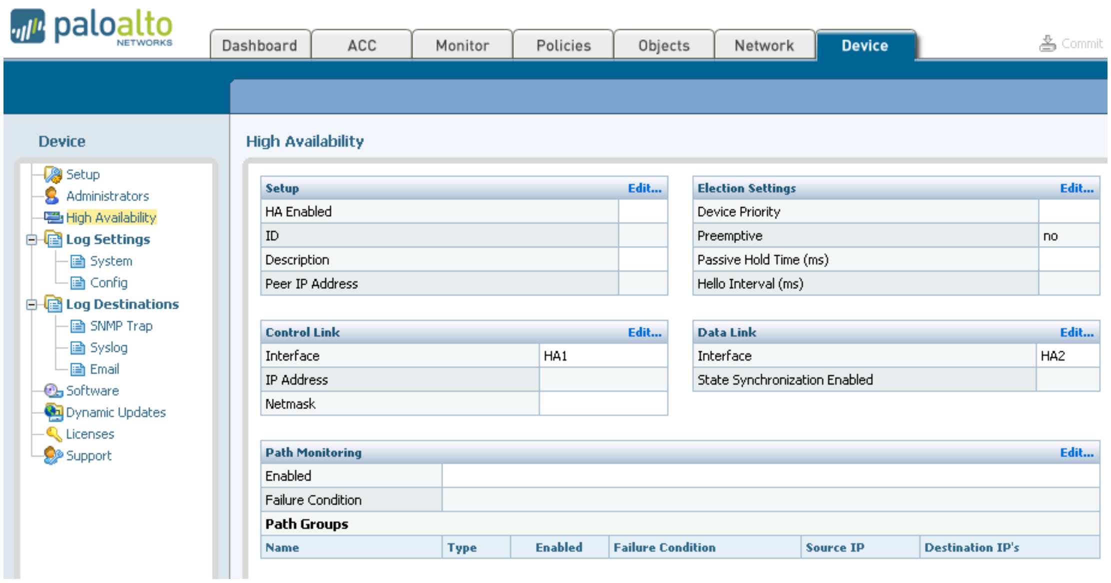
Interfaces

	Interface	Interface Type	Management Profile	Link State	IP Address
⚠	ethernet1/15	HA		🟩	
⚠	ethernet1/16	HA		🟩	

Figure 40. Verifying HA Interfaces

6. Enable high availability on both the active and passive firewall:

   a. Under the **Device** tab, click **High Availability** to open the High Availability page.



High Availability

Setup	Edit...
HA Enabled	
ID	
Description	
Peer IP Address	

Election Settings	Edit...
Device Priority	
Preemptive	no
Passive Hold Time (ms)	
Hello Interval (ms)	

Control Link	Edit...
Interface	HA1
IP Address	
Netmask	

Data Link	Edit...
Interface	HA2
State Synchronization Enabled	

Path Monitoring	Edit...
Enabled	
Failure Condition	

Path Groups

Name	Type	Enabled	Failure Condition	Source IP	Destination IP's

Figure 41. High Availability Page

b. For each section on the page, click **Edit** in the header, specify the corresponding information described below, and click **OK.**

Table 16. Availability Settings

Field	Description
Setup	
Enable HA	Select the check box to enable HA.
ID	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.
Description	Enter a description of the active/passive pair (optional).
Peer IP Address	Enter the IP address of the HA1 interface specified in the Control Link section of the other firewall.
Control Link	
Port	(If supported on your firewall model) Select the HA port.
IP Address	Enter the IP address of the HA1 interface for the current firewall.
Netmask	Enter the network mask for the IP address, such as “255.255.255.0”.
Encryption	Select the check box if you want to encrypt communications over the HA links, and enter a passphrase. The same passphrase must be entered in both firewalls.
Data Link	
Port	(If supported on your firewall model) Select the HA port.
Enable State Synchronization	Select the check box to enable synchronization of the configuration and session information with the passive firewall.
Election Settings	
Device Priority	Enter a priority value (0 to 255) to identify the active firewall. The firewall with the lower value (higher priority) becomes the active firewall.
Preemptive	Select the check box to enable the higher priority firewall to resume active operation after recovering from a failure.
Passive Hold Time	Enter the delay in milliseconds (0 to 60000) between the occurrence of a failover condition and the initiation of a failover.
Hello Interval	Enter the number of milliseconds (1000 to 60000) between the heartbeat packets sent to verify that the other firewall is operational.
Passive Link State	Choose from the following options: • **auto**—Causes the link status to reflect physical connectivity, but discards all packets received. It is supported for Layer 3 mode. The auto option is desirable, if it is feasible for your network. • **shutdown**—Forces the interface link to the down state. This is the default option, which ensures that loops are not created in the network.

Table 16. Availability Settings (Continued)

Field	Description
Path Monitoring	
Enabled	Select the check box to enable path monitoring.
Failure Condition	Select whether a failover occurs when any or all of the monitored path groups fail to respond.
Path Groups	Define one or more path groups to monitor specific destination addresses. To add a path group, specify the following and click **Add**: • **Type** — Select an interface type (Virtual Wire, VLAN, or Virtual Router). • **Name** — Select an interface of the specified type. • **Enabled** — Select the check box to enable the path group. • **Failure Condition** — Select whether a failure occurs when any or all of the specified destination addresses fails to respond. • **Source IP**—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. • **Destination IPs** — Enter one or more destination addresses to be monitored (multiple addresses must be separated by commas). To delete a path group, select the group, and click **Delete**.
Link Monitoring	
Enabled	Select the check box to enable link monitoring.
Failure Condition	Select whether a failover occurs when any or all of the monitored link groups fail.
Link Groups	Define one or more link groups to monitor specific Ethernet links. To add a link group, specify the following and click **Add**: • **Name** — Enter a link group name. • **Enabled** — Select the check box to enable the link group. • **Failure Condition** — Select whether a failure occurs when any or all of the selected links fail. • **Interfaces** — Select one or more Ethernet interfaces to be monitored (multiple addresses must be separated by commas). To delete a link group, select the group, and click **Delete**.

7. Click **Commit** to activate the changes. To save or roll back your configuration changes before activating them, as well as import, load, or export configurations, refer to “Managing Configurations” on page 47.

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 block pages.*

Table 17. Custom Response Page Types

Page Type	Description
Antivirus Block Page	Access blocked due to virus infection.
Application Block Page	Access blocked due to security policy.
File Blocking Block Page	Access blocked because access to the file is blocked.
SSL Decryption Opt-out Page	User warning page indicating that this session will be inspected.
URL Filtering Continue and Override Page	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.
Anti-spyware Download Block Page	Access blocked due to spyware activity.
Captive Portal Comfort Page	Page for users to verify their user name and password for machines that are not part of the Active Directory domain.
SSL Certificate Revoked Notify page	Notification that an SSL certificate has been revoked.
URL Filtering Block Page	Access blocked due to filtering applied to the URL being accessed.
SSL-VPN Custom Login Page	Page for users who attempt to access the SSL-VPN.

To manage custom response pages:

1. Under the **Device** tab, click **Response Pages** to open the page.

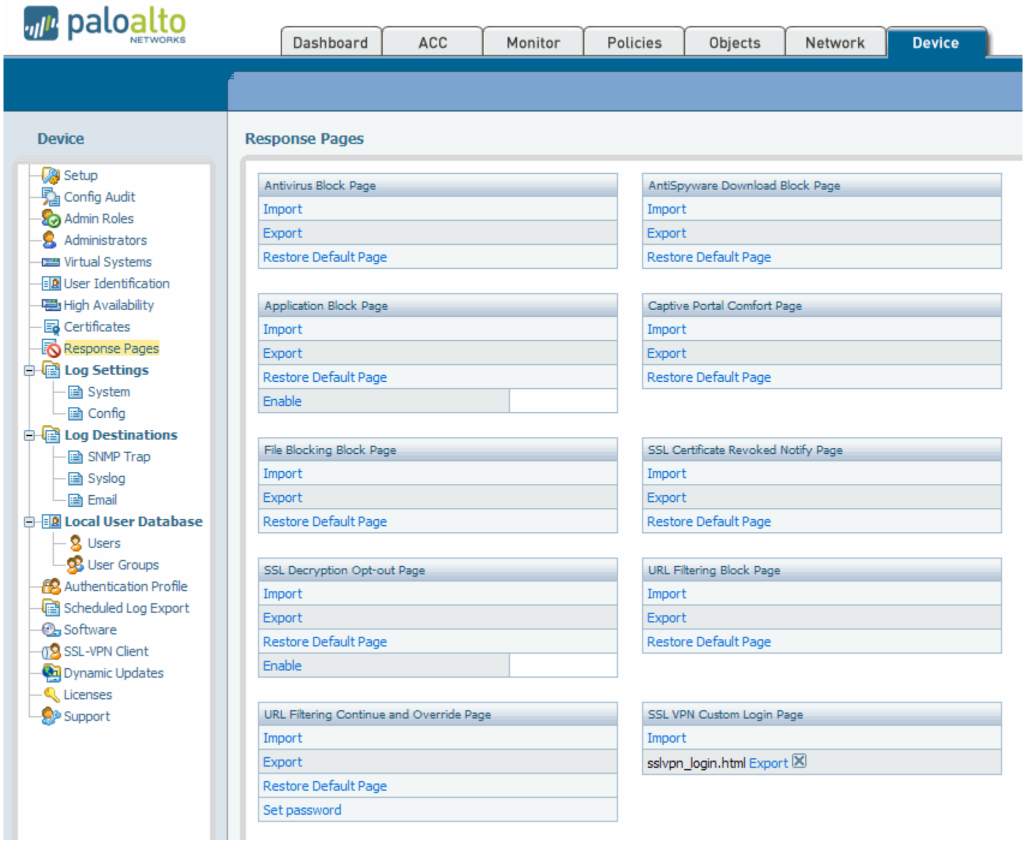


Figure 42. Responses Page

2. To import a custom HTML response page:

   a. Click the **Import** link for the type of page.

   b. Browse to locate the block page, and click **Open** to add the page.

   c. Click **OK** to import the file.

   A message is displayed to indicate whether the import succeeded. For the import to be successful, the file must be in HTML format.

   d. Click **Close** to close the pop-up window.

3. To export a custom HTML response page:

   a. Click the **Export** link for the type of page.

   b. Click **Export**.

   c. 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.

   d. Click **OK**.

4. To enable or disable the Application Block page or SSL Decryption Opt-out pages:

   a. Click the **Enable** link for the type of page.

   b. Select or deselect the **Enable** check box.

   c. Click **OK**.

5. To use the default block page instead of a previously uploaded page:

   a. Click the **Restore Block Page** link for the type of page.

   b. Click **Restore**.

   A message is displayed to indicate that the restoration succeeded.

Defining Configuration and System Log Settings

The following sections describe how to enable remote logging and email notification for the system and configuration logs. To enable remote logging for the threat and traffic logs, refer to "Defining Log Forwarding Profiles" on page 185.

- "About the Logs" in the next section
- "Defining Configuration Log Settings" on page 78
- "Defining System Log Settings" on page 79

About the Logs

The firewall provides logs that record configuration changes, system events, security threats, and traffic flows. Except for the traffic log, all logs are saved 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 18 Log Types and Settings

Log	Description
Configuration	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.
System	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.
Threat	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 "Defining Log Forwarding Profiles" on page 185). Threats are logged remotely only for the traffic that matches the security rules where the logging profile is assigned.
Traffic	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 also determines whether the locally logged entries are also logged remotely (refer to "Defining Log Forwarding Profiles" on page 185).
URL Filtering	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 proscribed web site is accessed (refer to "Defining URL Filtering Profiles" on page 178).
Data Filtering	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 188.

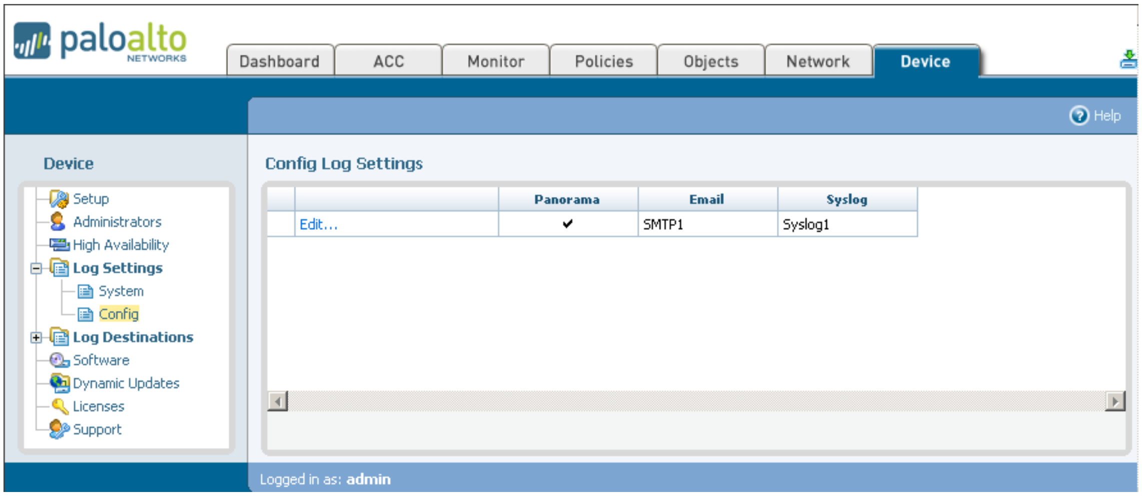
The threat and traffic logs are used to generate most of the information in the reports and the Application Command Center (refer to "Reports and Logs" on page 215).

Defining Configuration Log Settings

The configuration log settings specify the configuration log entries that are logged remotely with Panorama, and sent as Syslog messages and/or email notifications. Configuration logs record each configuration change, including the date and time and the name of the user who made the change. To view the configuration log, refer to “Identifying Unknown Applications and Taking Action” on page 246.

To define the configuration log settings:

1. Under the **Device** tab, click **Log Settings > Config** to open the Config Log Settings page.



Config Log Settings

	Panorama	Email	Syslog
Edit...	✓	SMTP1	Syslog1

Logged in as: admin

Figure 43. Configuration Log Settings Page

2. Click **Edit** to change the log settings:

   a. Specify the following information.

Table 19. System Log Settings

Field	Description
Panorama	Select the check box to enable sending configuration log entries to the Panorama central management system.
Email	To generate email notifications for configuration log entries, select the name of the email settings that specify the appropriate email addresses. To specify new email settings, refer to “Defining Email Notification Profiles” on page 84.
Syslog	To generate Syslog messages for configuration log entries, select the name of the Syslog server. To specify new Syslog servers, refer to “Defining Syslog Servers” on page 83.

   b. Click **OK** to change the log settings, or click **Cancel** to discard your changes.

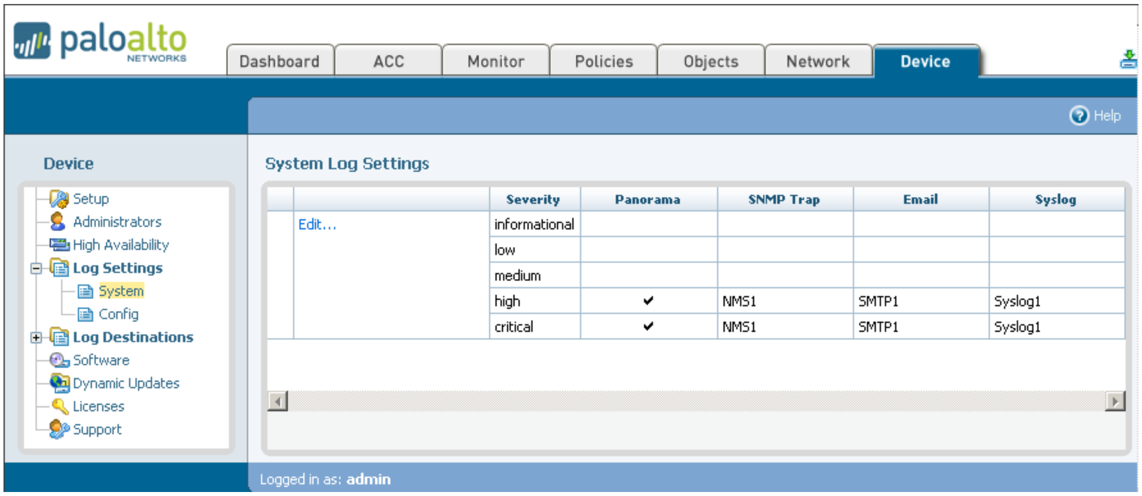
3. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Defining System Log Settings

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 view the system log, refer to “Identifying Unknown Applications and Taking Action” on page 246.

To define the system log settings:

1. Under the **Device** tab, click **Log Settings > System** to open the System Log Settings page.



System Log Settings

	Severity	Panorama	SNMP Trap	Email	Syslog
Edit...	informational				
	low				
	medium				
	high	✓	NMS1	SMTP1	Syslog1
	critical	✓	NMS1	SMTP1	Syslog1

Logged in as: admin

Figure 44. System Log Settings Page

2. Click **Edit** to change the log settings:

   a. Specify the following information.

Table 20. System Log Settings

Field	Description
Panorama	Click the check box for each severity level of the system log entries to be sent to the Panorama central management system. To define the Panorama server address, refer to “Defining the Host Name and Network Settings” on page 40. The severity levels are: • **Critical** — Hardware failures, including high availability (HA) 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.

Table 20. System Log Settings (Continued)

Field	Description
SNMP Trap Email Syslog	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 81. • "Defining Email Notification Profiles" on page 84 • "Defining Syslog Servers" on page 83

b. Click **OK** to change the log settings, or click **Cancel** to discard your changes.

3. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Defining Log Destinations

The following sections describe how to define SNMP trap sinks, Syslog servers, and email addresses where log entries can be sent.

- "About Log Destinations" in the next section
- "Defining SNMP Trap Destinations" on page 81
- "Defining Syslog Servers" on page 83
- "Defining Email Notification Profiles" on page 84

About Log Destinations

Log entries on the firewall can be sent to a Panorama central management system, SNMP trap sinks, Syslog servers, and email addresses.

The following table describes the remote log destinations.

Table 21 Remote Log Destinations

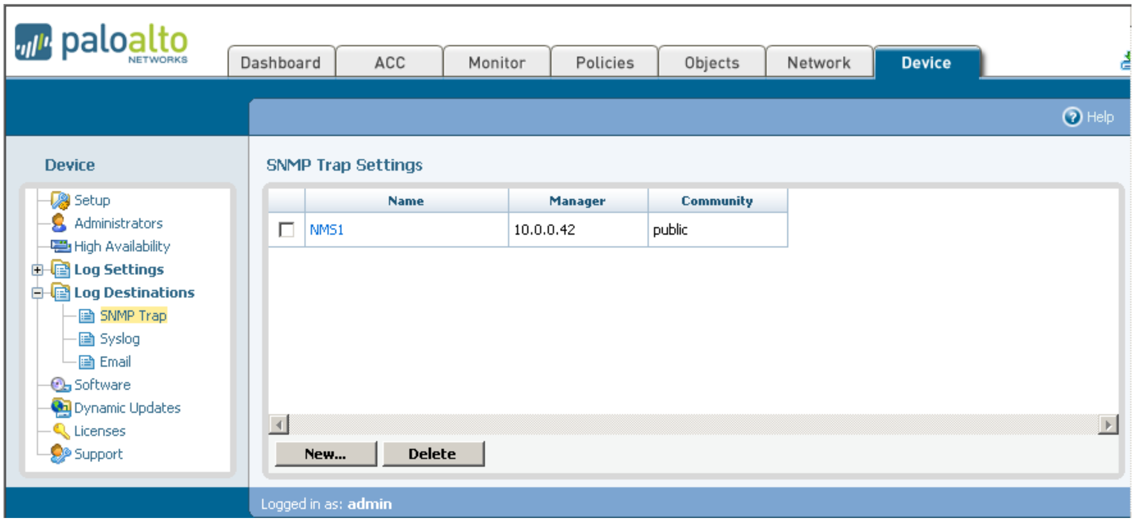
Destination	Description
Panorama	All log entries can be forwarded to a Panorama central management system. To specify the address of the Panorama server, refer to "Defining the Host Name and Network Settings" on page 40.
SNMP trap	SNMP traps can be generated by severity level for system, threat, and traffic log entries, but not for configuration log entries. To define the SNMP trap destinations, refer to "Defining SNMP Trap Destinations" on page 81.
Syslog	Syslog messages can be generated by severity level for system, threat, and traffic log entries, and for all configuration log entries. To define the Syslog destinations, refer to "Defining Syslog Servers" on page 83.
Email	Emails can be generated by severity level for system, threat, and traffic log entries, and for all configuration log entries. To define the email addresses and servers, refer to "Defining Email Notification Profiles" on page 84.

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 79) and for traffic and threat log entries (refer to “Defining Log Forwarding Profiles” on page 185).

To define SNMP trap destinations:

1. Under the **Device** tab, click **Log Destinations > SNMP Trap** to open the SNMP Trap Settings page.



	Name	Manager	Community
□	NMS1	10.0.0.42	public

Figure 45. SNMP Traps Page

2. To add a new SNMP trap destination:

    a. Click **New** to open the New SNMP Trap Setting page.

    b. Specify the following information.

Table 22. New SNMP Trap Destination

Field	Description
Name	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.
Manager	Enter the IP address of the trap destination.
Community	Enter the community string required to send traps to the specified destination (default is “public”).

    c. Click **OK** to submit the new trap destination, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

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

4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

SNMP MIBs

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

- SNMPv2-MIB
- SNMPv2-SMI
- IF-MIB
- HOST-RESOURCES-MIB
- ENTITY-SENSOR-MIB
- PAN-COMMON-MIB

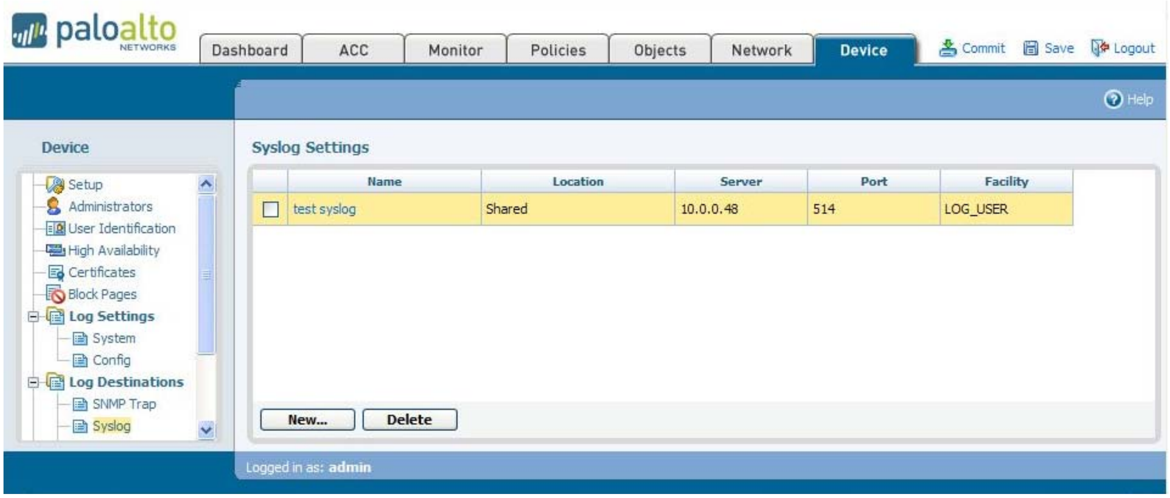
The full set of MIBs is available on the Palo Alto Networks support site: *http://support.paloaltonetworks.com*.

Defining Syslog Servers

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 Configuration and System Log Settings” on page 76) and for traffic and threat log entries (refer to “Defining Log Forwarding Profiles” on page 185).

To define Syslog servers:

1. Under the **Device** tab, click **Log Destinations > Syslog** to open the Syslog Settings page.



Syslog Settings

	Name	Location	Server	Port	Facility
□	test syslog	Shared	10.0.0.48	514	LOG_USER

Logged in as: admin

Figure 46. Syslog Settings Page

2. To add a new Syslog server:

   a. Click **New** to open the New Syslog Setting page.

   b. Specify the following information.

Table 23. New Syslog Server

Field	Description
Name	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.
Server	Enter the IP address of the Syslog server.
Port	Enter the port number of the Syslog server (the standard port is 514).
Facility	Choose a level from the drop-down list.

   c. Click **OK** to submit the new trap destination, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

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

4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

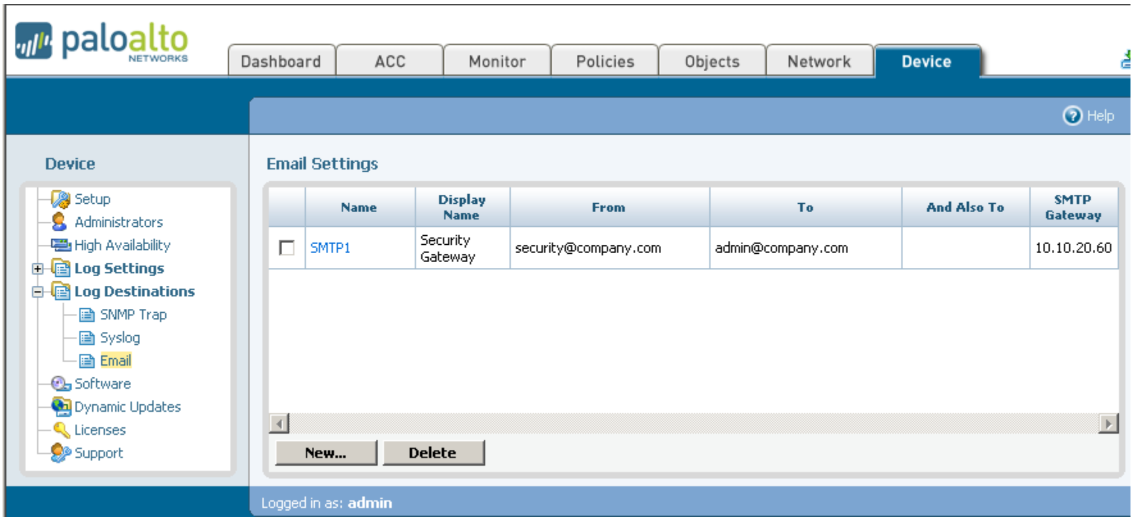
Defining Email Notification Profiles

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 Configuration and System Log Settings" on page 76) and traffic and threat log entries (refer to "Defining Log Forwarding Profiles" on page 185).

Refer to "Scheduling Reports for Email Delivery" on page 240 for information on scheduling email report delivery.

To define email settings:

1. Under the **Device** tab, click **Log Destinations > Email** to open the Email Settings page.



Email Settings

	Name	Display Name	From	To	And Also To	SMTP Gateway
□	SMTP1	Security Gateway	security@company.com	admin@company.com		10.10.20.60

Logged in as: admin

Figure 47. Email Settings Page

2. To add new email settings:

   a. Click **New** to open the New Email Setting page.

b. Specify the following information.

Table 24. New Email Address Settings

Field	Description
Name	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.
Display Name	Enter the name shown in the **From** field of the email.
From	Enter the From email address, such as "security_alert@company.com".
To	Enter the email address of the recipient.
And Also To	Optionally, enter the email address of another recipient.
SMTP Gateway	Enter the IP address or host name of the Simple Mail Transport Protocol (SMTP) server used to send the email.

c. Click **OK** to submit the new email setting, or click **Cancel** to discard your changes.

3. To change a Syslog server, click the name on the Email Settings page, change the name or addresses, and click **OK**. To delete email settings, select the check box next to the setting names and click **Delete**.

4. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

Note: *You cannot delete an email setting that is used in any system or configuration log settings or logging profiles.*

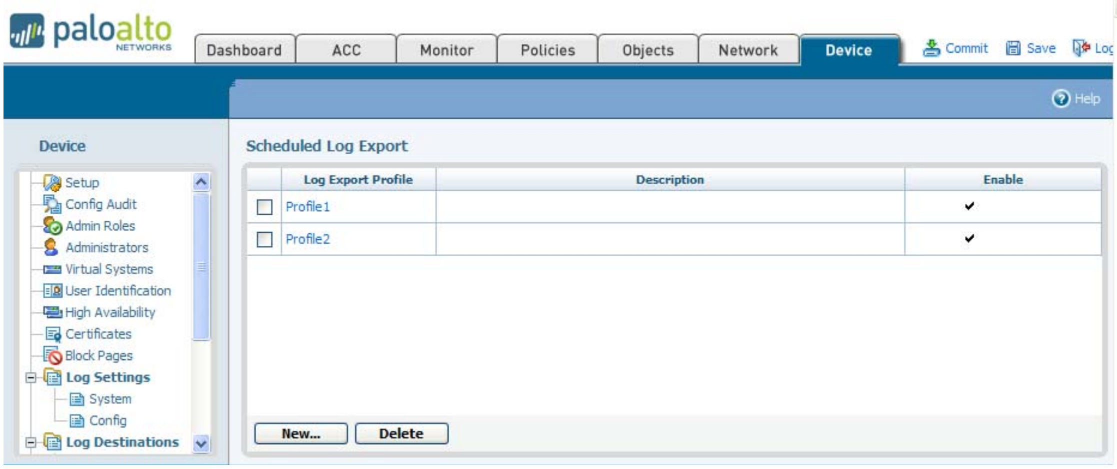
5. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Scheduling Log Exports

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:

1. Under the **Device** tab, click **Scheduled Log Export** to open the Scheduled Log Export page.



	Log Export Profile	Description	Enable
□	Profile1		✓
□	Profile2		✓

Figure 48. Scheduled Log Export Page

2. To create a new profile or configure an existing profile:

   a. Click **New** or click the profile link.

   b. Specify the following information.

Table 25. Scheduled Log Export Settings

Field	Description
Profile Name	Enter a name to identify the profile. The name cannot be changed after the profile is created.
Description	Enter an optional description.
Enabled	Select the check box to enable the scheduling of log exports.
Log Type	Select the type of log (traffic or threat). Default is traffic.
Scheduled export start time (daily)	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).
FTP Hostname	Enter the host name or IP address of the FTP server that will be used for the export.
FTP Port	Enter the port number that the FTP server will use. Default is 21.

Table 25. Scheduled Log Export Settings (Continued)

Field	Description
FTP Passive Mode	Select the check box to use passive mode for the export. By default, this option is selected.
FTP Username	Enter the user name for access to the FTP server. Default is anonymous.
FTP Password	Enter the password for access to the FTP server. A password is not required if the user is "anonymous."

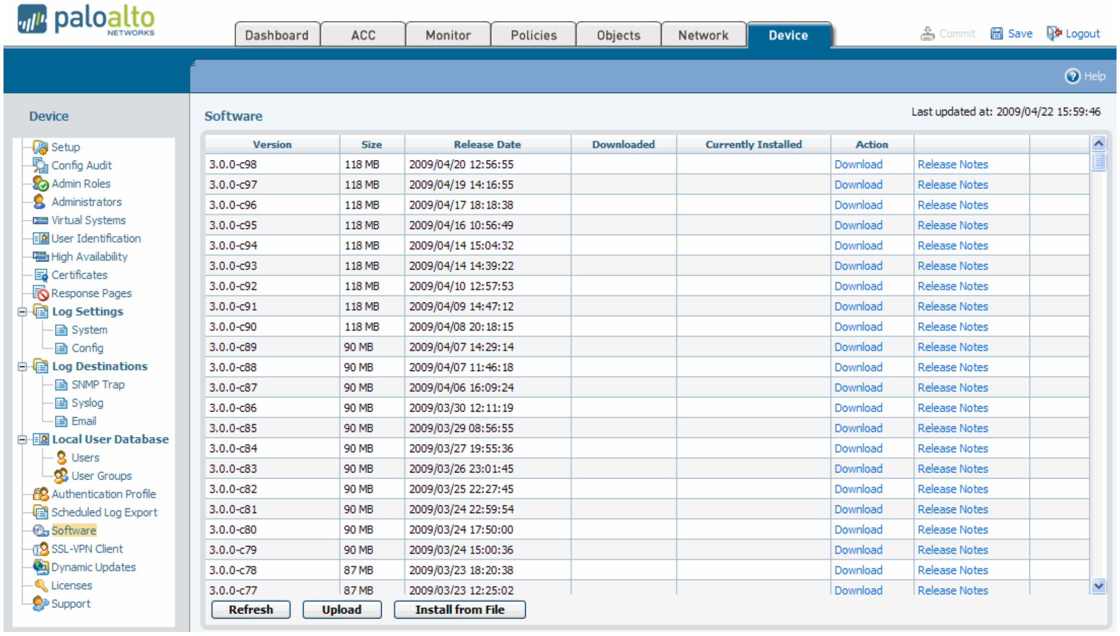
c. Click **OK**. The new profile is added to the Scheduled Log Export page, and the specified export is scheduled.

Upgrading the PAN-OS 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).

To upgrade the PAN-OS software:

1. Under the **Device** tab, click **Software** to open the Software page.



Software

Last updated at: 2009/04/22 15:59:46

Version	Size	Release Date	Downloaded	Currently Installed	Action	
3.0.0-c98	118 MB	2009/04/20 12:56:55			Download	Release Notes
3.0.0-c97	118 MB	2009/04/19 14:16:55			Download	Release Notes
3.0.0-c96	118 MB	2009/04/17 18:18:38			Download	Release Notes
3.0.0-c95	118 MB	2009/04/16 10:56:49			Download	Release Notes
3.0.0-c94	118 MB	2009/04/14 15:04:32			Download	Release Notes
3.0.0-c93	118 MB	2009/04/14 14:39:22			Download	Release Notes
3.0.0-c92	118 MB	2009/04/10 12:57:53			Download	Release Notes
3.0.0-c91	118 MB	2009/04/09 14:47:12			Download	Release Notes
3.0.0-c90	118 MB	2009/04/08 20:18:15			Download	Release Notes
3.0.0-c89	90 MB	2009/04/07 14:29:14			Download	Release Notes
3.0.0-c88	90 MB	2009/04/07 11:46:18			Download	Release Notes
3.0.0-c87	90 MB	2009/04/06 16:09:24			Download	Release Notes
3.0.0-c86	90 MB	2009/03/30 12:11:19			Download	Release Notes
3.0.0-c85	90 MB	2009/03/29 08:56:55			Download	Release Notes
3.0.0-c84	90 MB	2009/03/27 19:55:36			Download	Release Notes
3.0.0-c83	90 MB	2009/03/26 23:01:45			Download	Release Notes
3.0.0-c82	90 MB	2009/03/25 22:27:45			Download	Release Notes
3.0.0-c81	90 MB	2009/03/24 22:59:54			Download	Release Notes
3.0.0-c80	90 MB	2009/03/24 17:50:00			Download	Release Notes
3.0.0-c79	90 MB	2009/03/24 15:00:36			Download	Release Notes
3.0.0-c78	87 MB	2009/03/23 18:20:38			Download	Release Notes
3.0.0-c77	87 MB	2009/03/23 12:25:02			Download	Release Notes

Figure 49. Software Page

2. Click **Refresh** to view the latest software releases available from Palo Alto Networks.

3. To view a description of the changes in a release, click **Release Notes** next to the release.

4. To install a new release from the download site:

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.

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.

5. To install a release that you previously stored on your PC:

a. Click **Upload**.

b. Browse to locate the software package, and click **OK**.

c. Click **Install from File**.

d. Choose the file that you just selected from the drop-down list, and click **OK** to install the image.

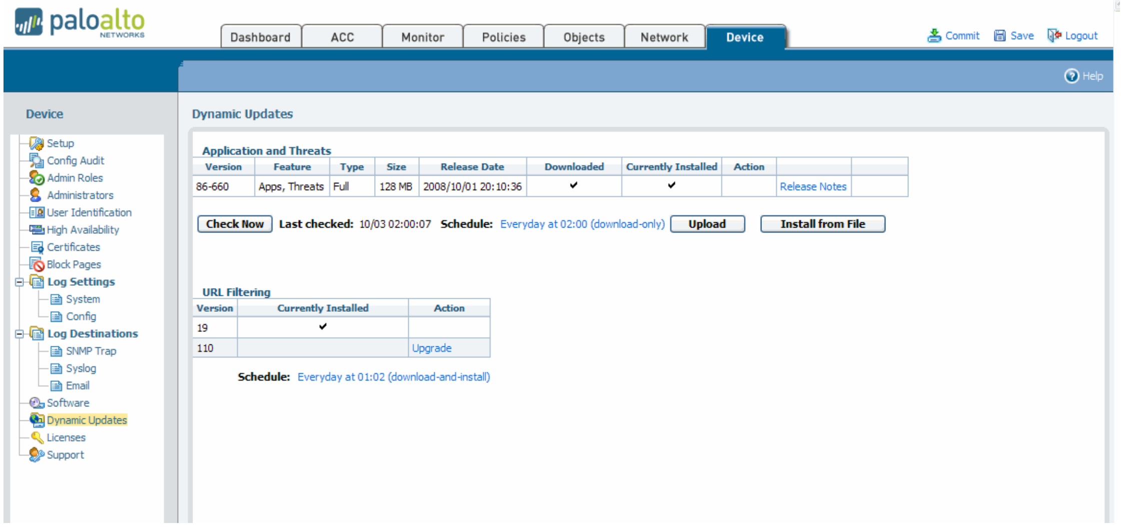
6. To delete an outdated release, click ☒ next to the release.

Updating Threat and Application Definitions

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.

To install threat and application updates:

1. Under the **Device** tab, click **Dynamic Updates** to open the Dynamic Updates page.



Dynamic Updates

Application and Threats

Version	Feature	Type	Size	Release Date	Downloaded	Currently Installed	Action		
86-660	Apps, Threats	Full	128 MB	2008/10/01 20:10:36	✓	✓		Release Notes	

Check Now **Last checked:** 10/03 02:00:07 **Schedule:** Everyday at 02:00 (download-only) Upload Install from File

URL Filtering

Version	Currently Installed	Action
19	✓	
110		Upgrade

Schedule: Everyday at 01:02 (download-and-install)

Figure 50. 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.

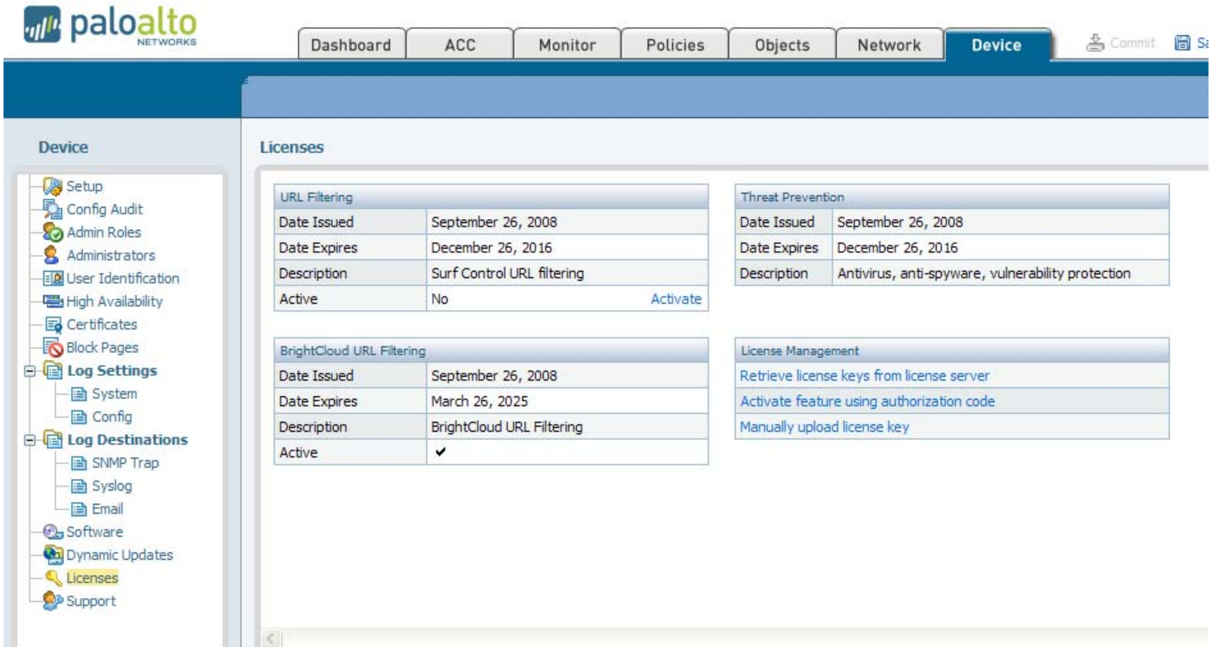
2. Click **Check Now** to view the latest threat and application definition updates available from Palo Alto Networks.
3. To view a description of an update, click **Release Notes** next to the update.
4. To install a new update:
   a. Click **Download** next to the update to be installed. When the download is complete, a checkmark is displayed in the **Downloaded** column.
   b. To install a downloaded content update, click **Install** next to the update.
5. To schedule automatic updates:
   a. Click the schedule link to open the Edit Update Schedule window.
   b. Select the frequency of the update.
   c. Select the day of the week and time of day.
   d. Select 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.
   e. Click **OK** to close the window and schedule the updates.
6. To install a file that you previously stored on your PC:
   a. Click **Upload**.
   b. Browse to locate the file, and click **OK**.
   c. Click **Install from File**.
   d. Choose the file that you just selected from the drop-down list, and click **OK** to install.
7. To delete an already downloaded update, click ☒ next to the update.

Installing a License

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.

To install a license:

1. Under the **Device** tab, click **Licenses** to open the Licenses page.



URL Filtering	
Date Issued	September 26, 2008
Date Expires	December 26, 2016
Description	Surf Control URL filtering
Active	No Activate

Threat Prevention	
Date Issued	September 26, 2008
Date Expires	December 26, 2016
Description	Antivirus, anti-spyware, vulnerability protection

BrightCloud URL Filtering	
Date Issued	September 26, 2008
Date Expires	March 26, 2025
Description	BrightCloud URL Filtering
Active	✓

License Management
Retrieve license keys from license server
Activate feature using authorization code
Manually upload license key

Figure 51. Licenses Page

2. You can activate licenses for standard URL filtering, BrightCloud URL filtering, and Threat Prevention. Click the **Activate** link to activate the license.

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

4. To activate 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, you can upload license keys manually:

a. Obtain a file of license keys from *http://support.paloaltonetworks.com*.

b. Save the license key file locally.

c. Click **Manually upload license key**, click **Browse** and select the file, and click **OK**.

Importing, Exporting and Generating Security 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.
- **Trusted CA certificate**—Import an additional intermediate certificate authority (CA) certificate to trust when doing SSL decryption. If the firewall encounters a certificate that is not signed by a trusted CA, then it uses its own untrusted CA to sign the certificate and generate the expected browser warning message.
- **SSL Forward Proxy certificate**—Import or generate an SSL forward proxy certificate.
- **SSL Inbound Inspection certificate**—Import or generate an SSL reverse proxy certificate.

To use certificates:

1. Under the **Device** tab, click **Certificates** to open the Certificates page.

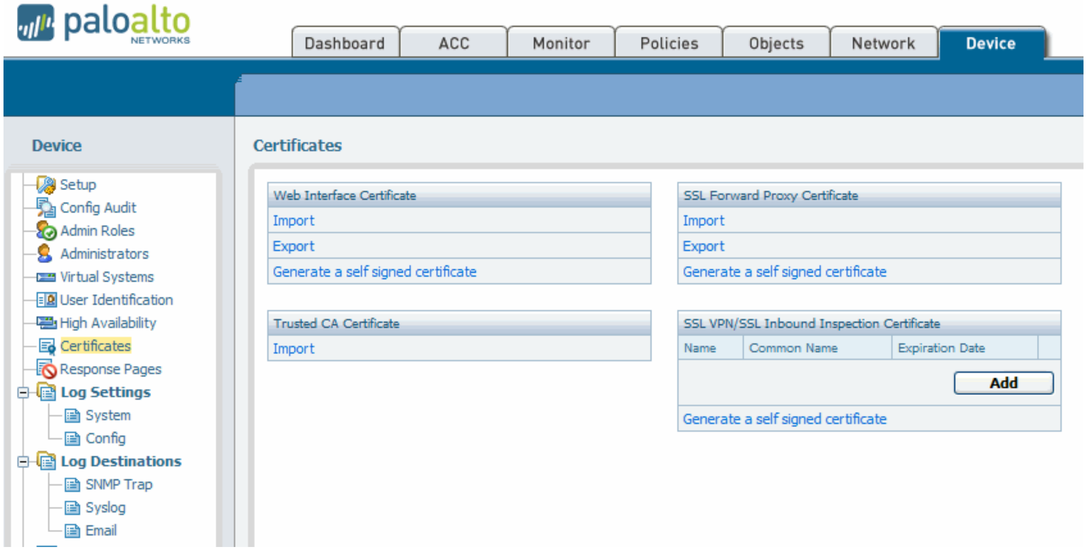


Figure 52. Certificates Page

2. 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. Click **OK**.

3. To export the web interface certificate:

   a. Click **Export**.

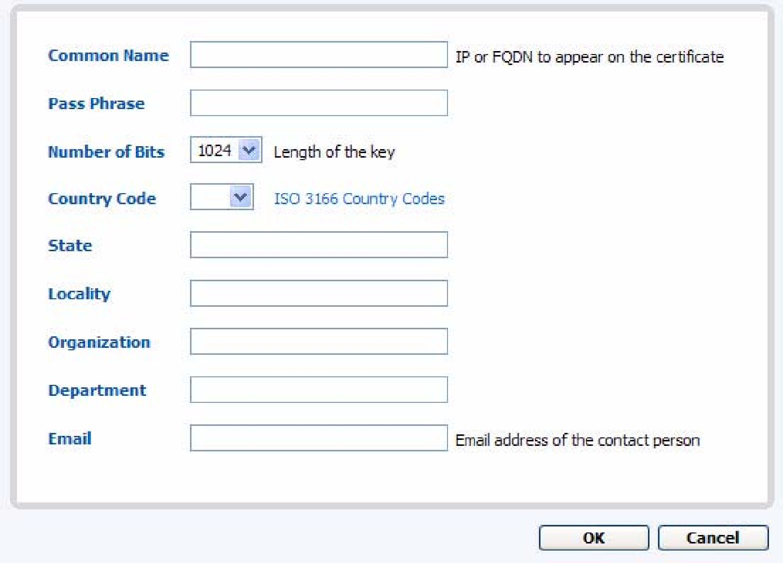
b. Click **Save** and then choose a location to copy the file to your local computer.

c. Click **Save**.

4. 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 285 for information on Panorama.*



Common Name		IP or FQDN to appear on the certificate
Pass Phrase		
Number of Bits	1024	Length of the key
Country Code		ISO 3166 Country Codes
State		
Locality		
Organization		
Department		
Email		Email address of the contact person

Figure 53. Generating a Self-Signed Certificate

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.

5. 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.

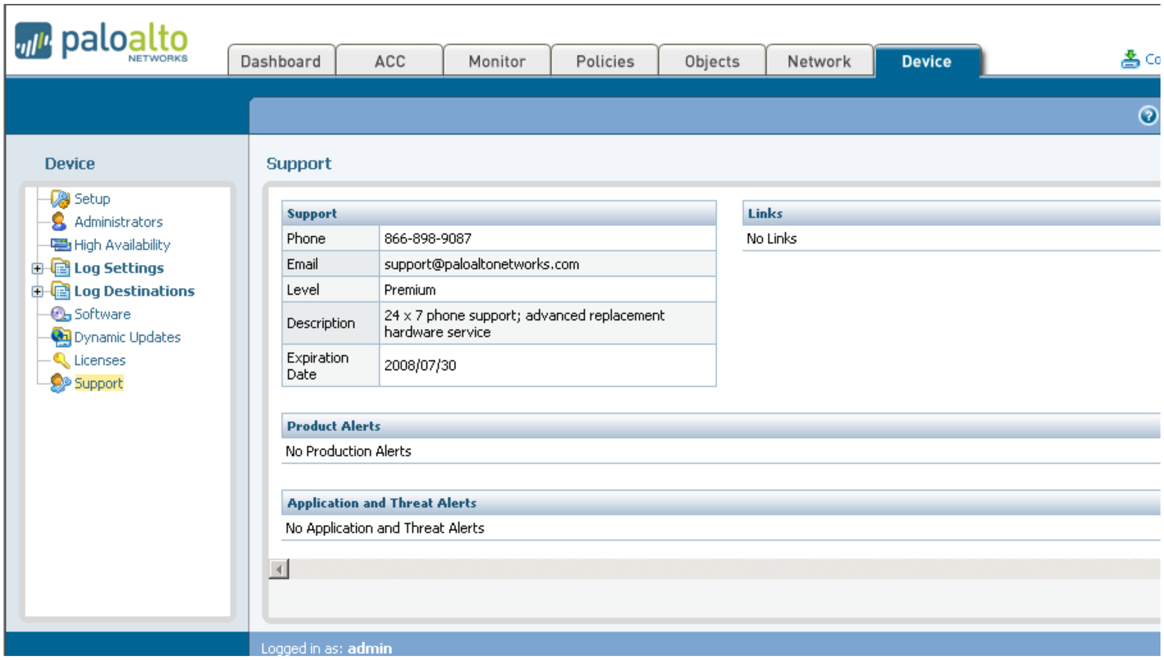
Refer to "Defining SSL Decryption Policies" on page 154 for instructions on creating policies for SSL forward proxy.

Viewing Support Information

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.

To access the Support page:

1. Under the **Device** tab, click **Support** to open the Support page.



Support	
Phone	866-898-9087
Email	support@paloaltonetworks.com
Level	Premium
Description	24 x 7 phone support; advanced replacement hardware service
Expiration Date	2008/07/30

Links
No Links

Product Alerts
No Production Alerts

Application and Threat Alerts
No Application and Threat Alerts

Logged in as: admin

Figure 54. Support Page

2. To view the details of an alert, click the alert name.

3. To enter a request for technical support, click **Create Ticket**. To view your current support requests, click **View Ticket**.

4. To generate a system file to assist Palo Alto Networks technical support in troubleshooting:

    a. Click **Generate Tech Support** file.

    b. Click **OK** to confirm.

    c. When the file is generated, click **Download Tech Support File** to download the file to your computer.

5. 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:

- "Networking Overview" in the next section
- "Deployment Types" on page 96
- "Configuring Interfaces" on page 98
- "Defining Security Zones" on page 116
- "Defining VLANs" on page 119
- "Defining Virtual Wires" on page 120
- "Defining Virtual Routers" on page 122
- "Defining DHCP Options" on page 130
- "Defining Network Profiles" on page 133

Networking Overview

The firewall can replace your existing firewall, and is typically installed between an edge router or other device facing the Internet and a switch or router connecting to your internal network. The Ethernet interfaces on the firewall can be configured to support virtually any network environment, including Layer 2 switching and VLAN environments, Layer 3 routing environments, and combinations of the two.

Deployment Types

The following sections describe the basic types of deployments and provide a summary of the supported interface types:

- "Virtual Wire Deployments" in the next section
- "Layer 2 Deployments" on page 96
- "Layer 3 Deployments" on page 97
- "Tap Mode Deployments" on page 97
- "Summary of Interface Types" on page 97

Virtual Wire Deployments

In a virtual wire deployment, the firewall is installed transparently on a network segment by binding two ports together (Figure 55). If necessary, you can allow only traffic that has specific virtual LAN (VLAN) tag values (or no tags). Choose this option to:

- Simplify installation and configuration.
- Avoid configuration changes to surrounding network devices.

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

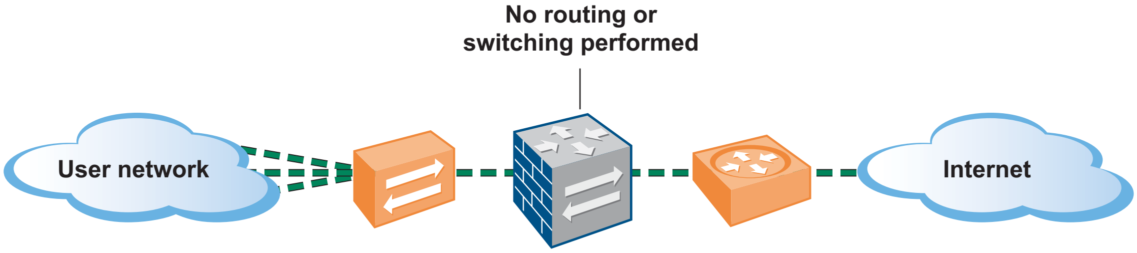


Figure 55. Virtual Wire Deployment

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 56).

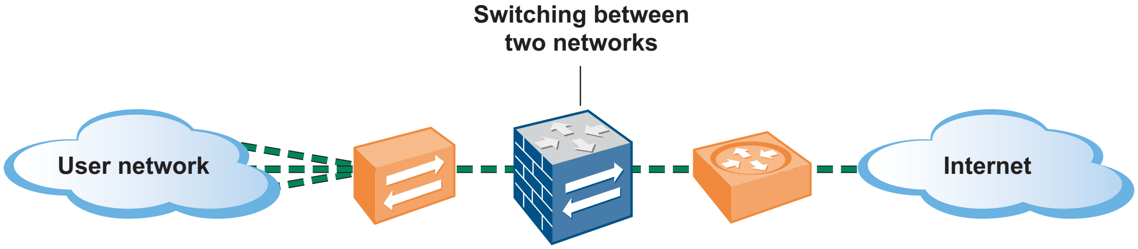


Figure 56. Layer 2 Deployment

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 57).

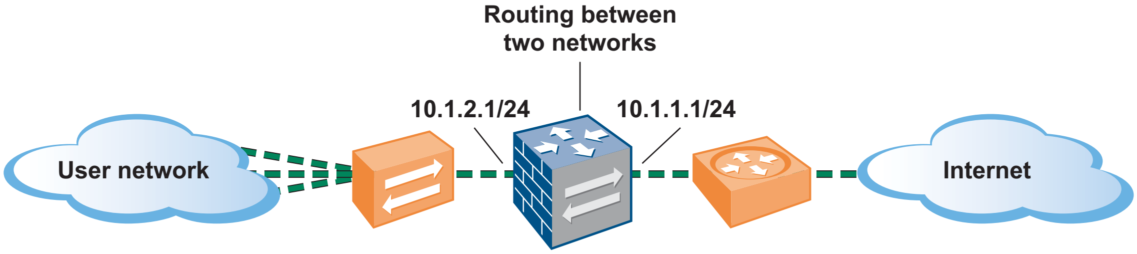


Figure 57. Layer 3 Deployment

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 any other port 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 an inline network traffic.

Note: When deployed in tap mode, the firewall is not able to take action, such as blocking traffic or decrypting SSL connections.

Summary of Interface Types

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

Table 26. Supported Interfaces

Interface	Description
Aggregate Ethernet	Two or more Ethernet ports can be combined into a group to increase the throughput for a Layer 2 or Layer 3 interface and its subinterfaces (refer to “Configuring Aggregate Ethernet Interfaces” on page 103).
Layer 2	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 100 and “Configuring Layer 2 Subinterfaces” on page 101).

Table 26. Supported Interfaces (Continued)

Interface	Description
Layer 3	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 102 and "Configuring Layer 3 Subinterfaces" on page 105).
Loopback	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 112).
Virtual Wire	A virtual wire binds two Ethernet ports together, which allows you to install the firewall transparently in the network with the 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 107).
VLAN Interface	VLAN interfaces provide Layer 3 routing of VLAN traffic to non-VLAN destinations (refer to "Configuring VLAN Interfaces" on page 110).
Tap	The Tap interface permits connection to a span port on a switch for traffic monitoring only. This mode does not support traffic blocking or SSL decryption.
HA	You can configure a data interface to be a high availability (HA) interface on some Palo Alto Networks firewalls.

Configuring Interfaces

For information about how to configure the Ethernet interfaces and define additional logical interfaces, refer to:

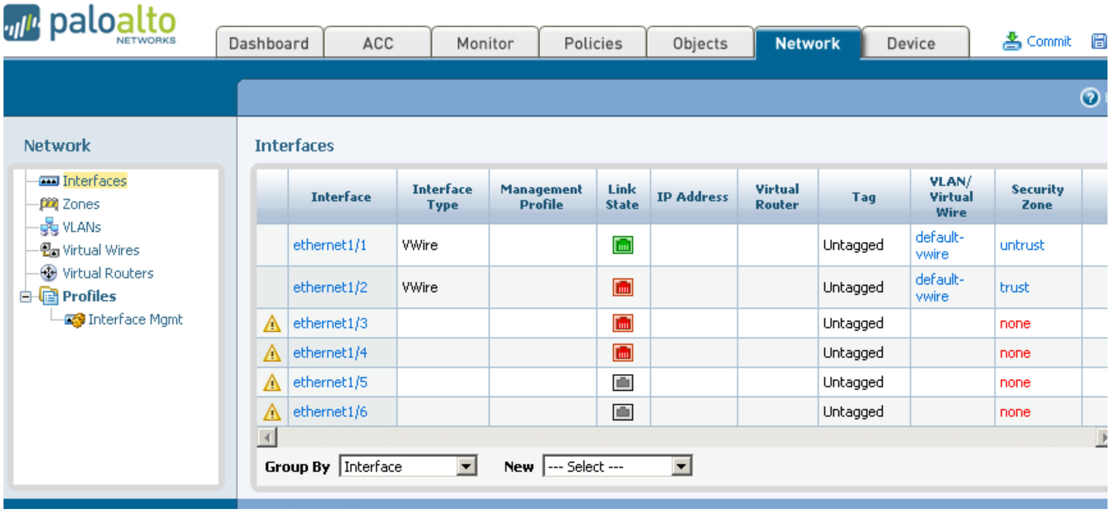
- "Viewing the Current Interfaces" in the next section
- "Configuring Layer 2 Interfaces" on page 100
- "Configuring Layer 2 Subinterfaces" on page 101
- "Configuring Layer 3 Interfaces" on page 102
- "Configuring Aggregate Ethernet Interfaces" on page 103
- "Configuring Layer 3 Subinterfaces" on page 105
- "Configuring Virtual Wire Interfaces" on page 107
- "Configuring Aggregate Interface Groups" on page 108
- "Configuring VLAN Interfaces" on page 110
- "Configuring Loopback Interfaces" on page 112
- "Configuring Tap Interfaces" on page 113
- "Configuring High Availability Interfaces" on page 115

Viewing the Current 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 view the current interfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.



Interfaces

	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
	ethernet1/1	VWire		🟩			Untagged	default-vwire	untrust
	ethernet1/2	VWire		🟥			Untagged	default-vwire	trust
⚠	ethernet1/3			🟥			Untagged		none
⚠	ethernet1/4			🟥			Untagged		none
⚠	ethernet1/5			▨			Untagged		none
⚠	ethernet1/6			▨			Untagged		none

Group By: Interface New: --- Select ---

Figure 58. Interfaces Page

2. 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.

   Note the following icons:

⚠	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, a "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

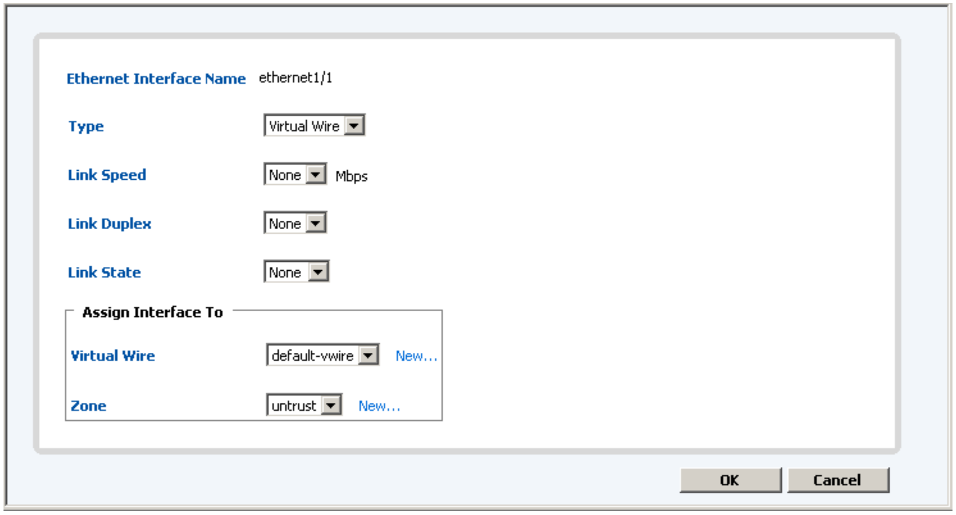
You can configure one or more Ethernet ports as a Layer 2 interface for untagged VLAN traffic. For each main Layer 2 interface, you can define multiple Layer 2 subinterfaces for traffic with specific VLAN tags (refer to “Configuring Layer 2 Subinterfaces” on page 101) and VLAN interfaces to provide Layer 3 routing of VLAN traffic (refer to “Configuring VLAN Interfaces” on page 110).

To configure Layer 2 interfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.
2. To change an Ethernet interface:
   a. To change an interface type, first 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**.

      In addition, to change a virtual wire to another interface type, delete the virtual wire definition shown in the **VLAN/Virtual Wire** column, if any (refer to “Defining Virtual Wires” on page 120).

   b. Click the interface name to open the Edit Ethernet Interface page.



Ethernet Interface Name ethernet1/1

Type: Virtual Wire

Link Speed: None Mbps

Link Duplex: None

Link State: None

Assign Interface To

Virtual Wire: default-vwire

Zone: untrust

Figure 59. Edit Ethernet Interface Page

   c. Specify the following information.

Table 27. Ethernet Interface Settings

Field	Description
Type	Select **L2** from the drop-down list.
Link Speed	Select the interface speed in Mbps (10, 100, or 1000).
Link Duplex	Select whether the interface transmission mode is full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
Link State	Select whether the interface status is enabled (Up), disabled (Down), or determined automatically (Auto).

Table 27. Ethernet Interface Settings (Continued)

Field	Description
Assign Interface To	
Vlan	Select a VLAN, or click **New** to define a new VLAN (refer to "Defining VLANs" on page 119).
Zone	Select a security zone for the interface, or click **New** to define a new zone (refer to "Defining Security Zones" on page 116).

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

3. To change the interface's VLAN or security zone, click the current value shown on the Interfaces page, and select (or create) a new VLAN or security zone.
4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

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 100.

To define Layer 2 subinterfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.
2. To add a Layer 2 subinterface:

a. Select **L2 Interface** from the **New** drop-down list at the bottom of the page.

b. Specify the following information.

Table 28. L2 Subinterface Settings

Field	Description
Physical Interface	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 100.
Logical Interface Name	Enter the number (1 to 9999) appended to the physical interface name to form the logical interface name. The general name format is: ethernet x/y.<1-9999>
Tag	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.
Assign Interface To	
Vlan	For a Layer 2 interface, select a VLAN, or click **New** to define a new VLAN (refer to "Defining VLANs" on page 119).
Zone	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 116).

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

3. To change an interface’s VLAN, or security zone, click the current value shown on the Interfaces page, and select (or create) a new VLAN or security zone.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Configuring Layer 3 Interfaces

You can configure one or more Ethernet ports as a Layer 3 interface 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 105).

To configure Layer 3 interfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.

2. To change an Ethernet interface:

   a. To change an interface type, first 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**.

      In addition, to change a virtual wire to another interface type, delete the virtual wire definition shown in the **VLAN/Virtual Wire** column, if any (refer to “Defining Virtual Wires” on page 120).

   b. Click the interface name to open the Edit Ethernet Interface page.

   c. Specify the following information.

Table 29. Ethernet Interface Settings

Field	Description
Type	Select **L3** from the drop-down list.
Link Speed	Select the interface speed in Mbps (10, 100, or 1000).
Link Duplex	Select whether the interface transmission mode is full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
Link State	Select whether the interface status is enabled (Up), disabled (Down), or determined automatically (Auto).
MTU	Enter the maximum transmission unit in bytes for packets sent on this Layer 3 interface (512 to 1500). The default is 1500.
Management Profile	Select a profile that specifies which protocols, if any, can be used to manage the firewall over this interface. To define new profiles, refer to “Defining Interface Management Profiles” on page 136.
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 Entries	To add one or more static Address Resolution Protocol (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**. Static ARP entries reduce ARP processing and preclude man-in-the-middle attacks for the specified addresses.

Table 29. 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 "Defining Virtual Routers" on page 122).
Zone	Select a security zone for the interface, or click **New** to define a new zone (refer to "Defining Security Zones" on page 116).

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

3. To change the interface's virtual router or security zone, click the current value shown on the Interfaces page, and select (or create) a new virtual router or security zone.

4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Configuring Aggregate Ethernet Interfaces

You can configure one or more interfaces as part of an aggregate Ethernet interface group. First define the group, as described in "Configuring Aggregate Interface Groups" on page 108, and then assign interfaces to the group.

Each aggregate Ethernet interface is assigned a name of the form ae.*number* 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:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.

2. Click the interface name to open the Edit Ethernet Interface page.

   a. Specify the following information.

Table 30. Aggregate Ethernet Interface Settings

Field	Description
Type	Select **Aggregate Ethernet** from the drop-down list.
Link Speed	Select the interface speed in Mbps (10, 100, or 1000).
Link Duplex	Select whether the interface transmission mode is full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
Link State	Select whether the interface status is enabled (Up), disabled (Down), or determined automatically (Auto).

Table 30. 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 "Defining Virtual Routers" on page 122).
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 108.

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

3. To change settings for an interface, click the current value shown on the Interfaces page, specify new settings, and click **OK**.

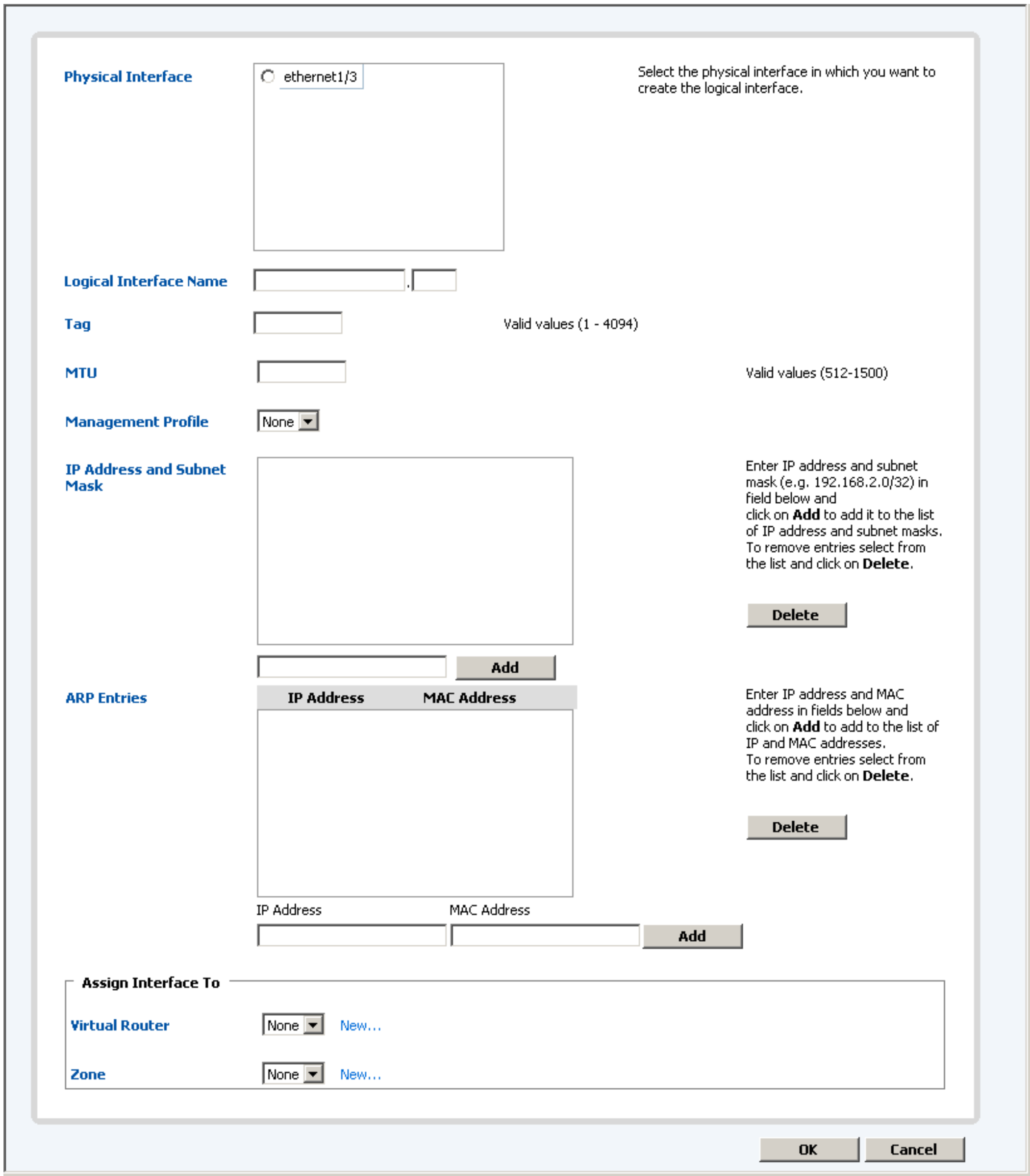
4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

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 102.

To define Layer 3 subinterfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.
2. To add a Layer 3 subinterface:
   a. Select **L3 Interface** from the **New** drop-down list at the bottom of the page.



Physical Interface: ○ ethernet1/3

Select the physical interface in which you want to create the logical interface.

Tag: Valid values (1 - 4094)

MTU: Valid values (512-1500)

Management Profile: None

Enter IP address and subnet mask (e.g. 192.168.2.0/32) in field below and click on **Add** to add it to the list of IP address and subnet masks. To remove entries select from the list and click on **Delete**.

Enter IP address and MAC address in fields below and click on **Add** to add to the list of IP and MAC addresses. To remove entries select from the list and click on **Delete**.

Virtual Router: None

Zone: None

Figure 60. New L3 Logical Interface Page

b. Specify the following information.

Table 31. L3 Subinterface Settings

Field	Description
Physical Interface	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 102.
Logical Interface Name	Enter the number (1 to 9999) appended to the physical interface name to form the logical interface name. The general name format is: ethernet x/y.<1-9999>
Tag	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.
MTU	Enter the maximum transmission unit in bytes for packets sent on this interface (512 to 1500). The default is 1500.
Management Profile	Select a profile that specifies which protocols, if any, can be used to manage the firewall over this interface. To define new profiles, refer to “Defining Interface Management Profiles” on page 136.
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 Entries	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**.
Assign Interface To	
Virtual Router	Select a virtual router, or click **New** to define a new virtual router (refer to “Defining Virtual Routers” on page 122).
Zone	Select a security zone for the interface, or click **New** to define a new zone (refer to “Defining Security Zones” on page 116).

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

3. To change an interface’s virtual router or security zone, click the current value shown on the Interfaces page, and select (or create) a new virtual router or security zone.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

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.

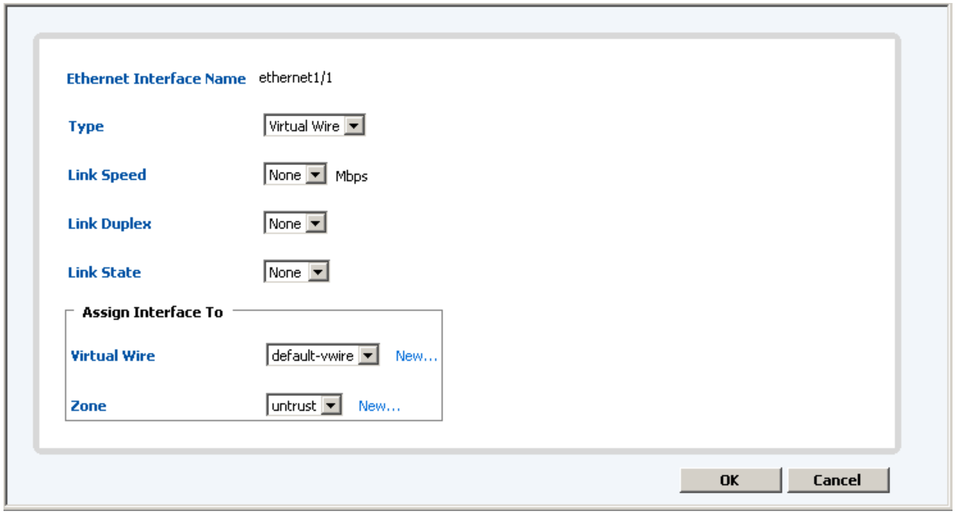
To configure virtual wire interfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.
2. To change an Ethernet interface:

   a. To change an interface type, first 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**.

   In addition, to change a virtual wire to another interface type, delete the virtual wire definition shown in the **VLAN/Virtual Wire** column, if any (refer to “Defining Virtual Wires” on page 120).

   b. Click the interface name to open the Edit Ethernet Interface page.



Ethernet Interface Name ethernet1/1

Type: Virtual Wire

Link Speed: None Mbps

Link Duplex: None

Link State: None

Assign Interface To

Virtual Wire: default-vwire

Zone: untrust

Figure 61. Edit Ethernet Interface Page

   c. Specify the following information.

Table 32. Ethernet Interface Settings

Field	Description
Type	Select **Virtual Wire** from the drop-down list.
Link Speed	Select the interface speed in Mbps (10, 100, or 1000).
Link Duplex	Select whether the interface transmission mode is full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
Link State	Select whether the interface status is enabled (Up), disabled (Down), or determined automatically (Auto).

Table 32. Ethernet Interface Settings (Continued)

Field	Description
Assign Interface To	
Virtual Wire	Select a virtual wire, or click **New** to define a new virtual wire (refer to "Defining Virtual Wires" on page 120).
Zone	Select a security zone for the interface, or click **New** to define a new zone (refer to "Defining Security Zones" on page 116).

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

3. To change the interface's virtual wire or security zone, click the current value shown on the Interfaces page, and select (or create) a new virtual wire or security zone.
4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Configuring 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. The aggregate interface that you create becomes a logical interface. Interface management, zone profiles, VPN interfaces, and VLAN sub-interfaces are all properties of the logical aggregate interface, not of the underlying physical interfaces.

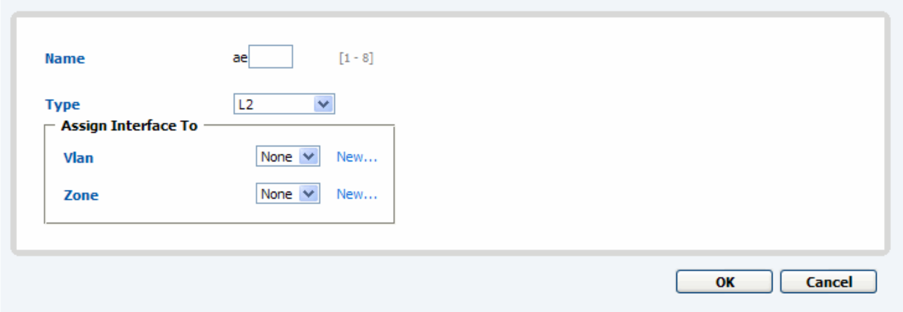
Each aggregate group can contain several physical interfaces of the type Aggregate Ethernet. After the group is created, you perform operations such as configuring Layer 2 or Layer 3 parameters on the Aggregate Group object rather than on the Aggregate Ethernet interfaces themselves.

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.

To create and configure aggregate group interfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.
2. Select **Aggregate Group** from the **New** drop-down list.



Name ae [1 - 8]

Type L2

Assign Interface To

Vlan None New...

Zone None New...

Figure 62. Edit Ethernet Interface Page

3. Specify the following information.

Table 33. Aggregate Group Interface Settings

Field	Description
Name	Enter a numeric suffix to identify the interface. The interface name is listed as ae.*n* where *n* is the suffix (1-8).
Type	Select the interface type (Layer 2, Layer 3, or virtual wire).
Assign Interface To	
Virtual Wire	Select a virtual wire, or click **New** to define a new virtual wire (refer to “Defining Virtual Wires” on page 120).
Zone	Select a security zone for the interface, or click **New** to define a new zone (refer to “Defining Security Zones” on page 116).

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

   The new group is listed on the Interfaces page.

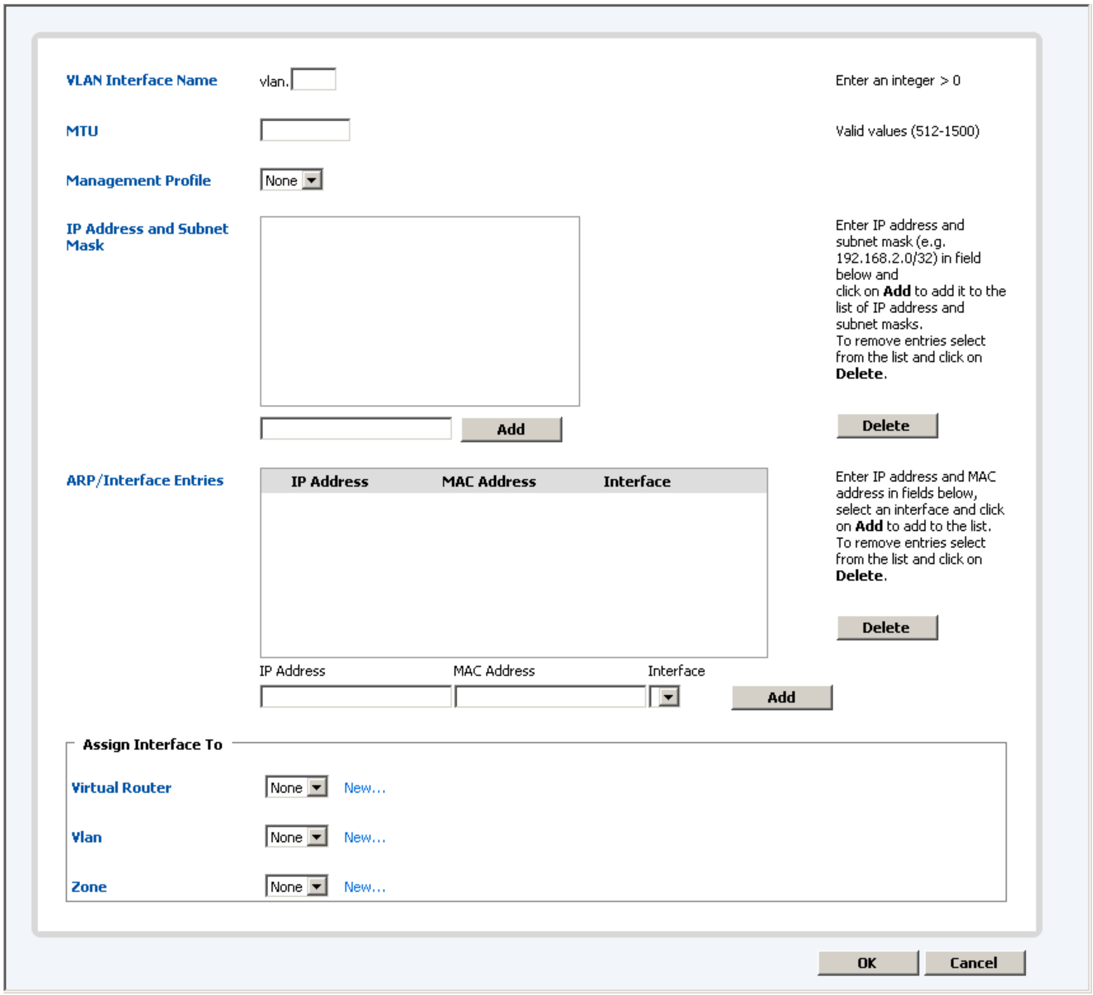
5. To modify the settings, click the interface link, make changes, and click **OK**. To delete the interface, click the ☒ icon in the column on the right of the interfaces list.
6. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.
7. Refer to “Configuring Aggregate Ethernet Interfaces” on page 103 for instructions on assigning interfaces to the group.

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 100.

To define VLAN interfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.
2. To add a VLAN interface:
   a. Select **VLAN Interface** from the **New** drop-down list at the bottom of the page.



VLAN Interface Name vlan. — Enter an integer > 0

MTU — Valid values (512-1500)

Management Profile: None

IP Address and Subnet Mask — Enter IP address and subnet mask (e.g. 192.168.2.0/32) in field below and click on **Add** to add it to the list of IP address and subnet masks. To remove entries select from the list and click on **Delete**.

ARP/Interface Entries — Enter IP address and MAC address in fields below, select an interface and click on **Add** to add to the list. To remove entries select from the list and click on **Delete**.

IP Address	MAC Address	Interface

Assign Interface To

Virtual Router: None

Vlan: None

Zone: None

Figure 63. New VLAN Interface Page

b. Specify the following information.

Table 34. VLAN Interface Settings

Field	Description
VLAN Interface Name	Enter the number (1 to 9999) appended to "vlan" to form the interface name. The general name format is: vlan.<1-9999>
MTU	Enter the maximum transmission unit in bytes for packets sent on this interface (512 to 1500). The default is 1500.
Management Profile	Select a profile that specifies which protocols, if any, can be used to manage the firewall over this interface. To define new profiles, refer to "Defining Interface Management Profiles" on page 136.
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 "Defining Virtual Routers" on page 122).
Vlan	Select a VLAN, or click **New** to define a new VLAN (refer to "Defining VLANs" on page 119).
Zone	Select a security zone for the interface, or click **New** to define a new zone (refer to "Defining Security Zones" on page 116).

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

3. To change an interface's virtual router, VLAN, or security zone, click the current value shown on the Interfaces page, and select (or create) a new virtual router, VLAN, or security zone.

4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

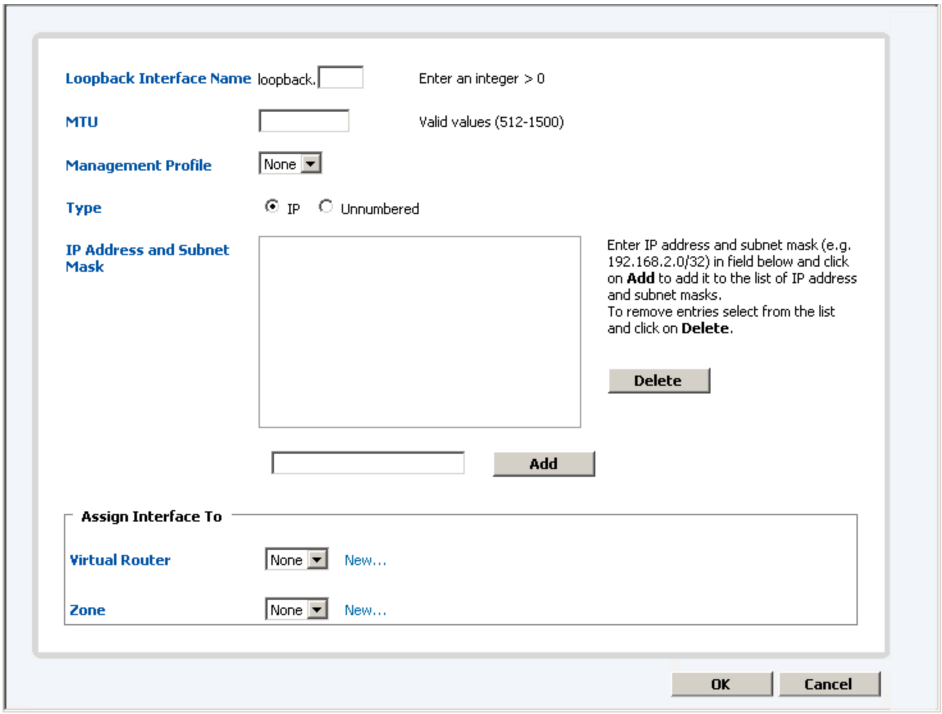
Configuring Loopback Interfaces

You can define one or more Layer 3 loopback interfaces, as needed. Each loopback interface can be associated with a Layer 3 interface (unnumbered) or have its own IP address. For example, you can define a loopback interface to manage the firewall, rather than use the management port.

To define loopback interfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.
2. To add a loopback interface:

   a. Select **Loopback Interface** from the **New** drop-down list at the bottom of the page.



Loopback Interface Name loopback. Enter an integer > 0

MTU Valid values (512-1500)

Management Profile None

Type ● IP ○ Unnumbered

IP Address and Subnet Mask

Enter IP address and subnet mask (e.g. 192.168.2.0/32) in field below and click on **Add** to add it to the list of IP address and subnet masks.
To remove entries select from the list and click on **Delete**.

Delete

Add

Assign Interface To

Virtual Router None New...

Zone None New...

OK Cancel

Figure 64. New Loopback Interface Page

   b. Specify the following information.

Table 35. Loopback Interface Settings

Field	Description
Loopback Interface Name	Enter the number (1 to 9999) appended to “loopback” to form the interface name. The general name format is: loopback.<1-9999>
MTU	Enter the maximum transmission unit in bytes for packets sent on this interface (512 to 1500). The default is 1500.
Management Profile	Select a profile that specifies which protocols, if any, can be used to manage the firewall over this interface. To define new profiles, refer to “Defining Interface Management Profiles” on page 136.
Type	Select **IP** to enter an IP address for the interface, or select **Unnumbered** to select the Layer 3 interface that acts as loopback interface.

Table 35. Loopback Interface Settings (Continued)

Field	Description
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**.
Source Interface	If you select Unnumbered as the type, select a Layer 3 interface from the drop-down list.
Assign Interface To	
Virtual Router	Select a virtual router, or click **New** to define a new virtual router (refer to "Defining Virtual Routers" on page 122).
Zone	Select a security zone for the interface, or click **New** to define a new zone (refer to "Defining Security Zones" on page 116).

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

3. To change an interface's virtual router or security zone, click the current value shown on the Interfaces page, and select (or create) a new virtual router or security zone.

4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

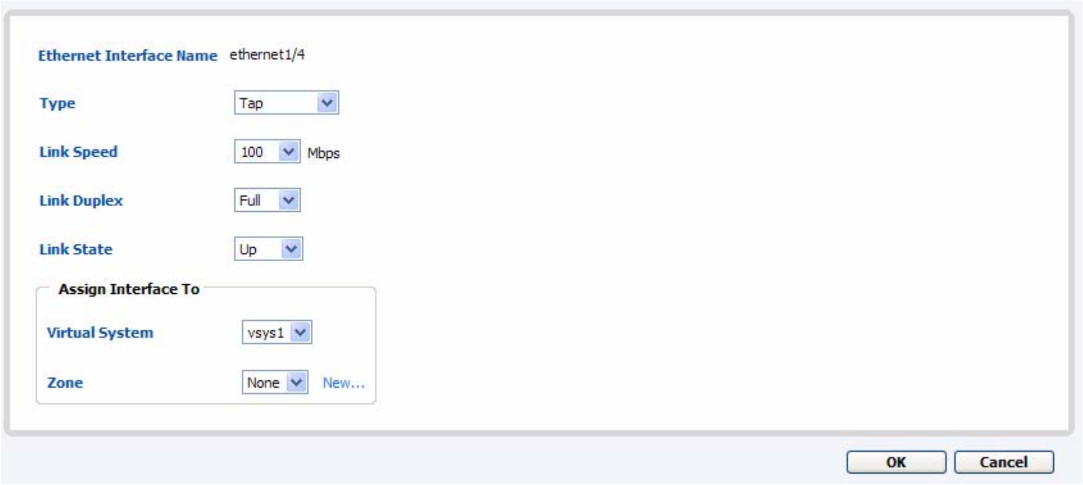
Configuring Tap Interfaces

You can define tap interfaces as needed to permit connection to a span port on a switch for traffic monitoring only. Refer to "Option D: Tap Mode Deployment" on page 31.

To define tap interfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.

2. Click an interface name to open the Edit Ethernet Interface page.



Ethernet Interface Name ethernet1/4

Type: Tap

Link Speed: 100 Mbps

Link Duplex: Full

Link State: Up

Assign Interface To

Virtual System: vsys1

Zone: None

Figure 65. Edit Ethernet Interface Page - Tap Interface

3. Specify the following information.

Table 36. Ethernet Interface Settings - Tap Interface

Field	Description
Type	Select **Tap** from the drop-down list.
Link Speed	Select the interface speed in Mbps (10, 100, or 1000).
Link Duplex	Select whether the interface transmission mode is full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
Link State	Select whether the interface status is enabled (Up), disabled (Down), or determined automatically (Auto).
Assign Interface To	
Virtual System	Select a virtual system
Zone	Select a security zone for the interface, or click **New** to define a new zone (refer to “Defining Security Zones” on page 116).

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

5. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Note: *Refer to “Option D: Tap Mode Deployment” on page 31 for information on defining a security policy for tap mode.*

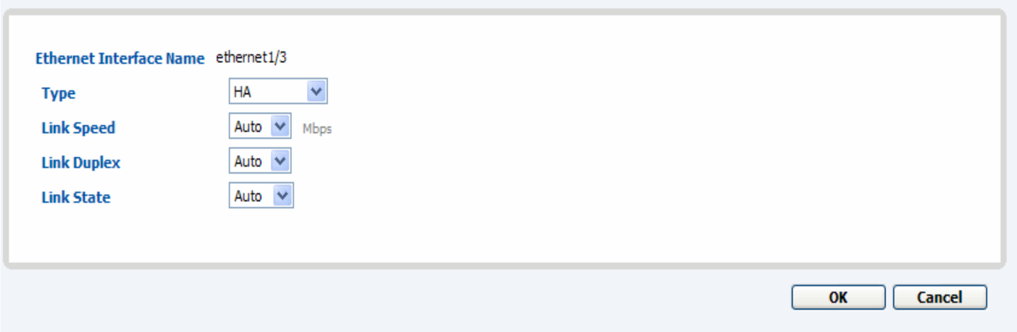
Configuring High Availability Interfaces

The firewall supports high availability (HA) interfaces. Each HA interface has a specific function: one for configuration synchronization and heartbeats and one 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 "Configuring High Availability" on page 70.*

To define HA interfaces:

1. Under the **Network** tab, click **Interfaces** to open the Interfaces page.
2. Click an interface name to open the Edit Ethernet Interface page.



Ethernet Interface Name ethernet1/3

Type: HA

Link Speed: Auto Mbps

Link Duplex: Auto

Link State: Auto

Figure 66. Edit Ethernet Interface Page

3. Specify the following information.

Table 37. Ethernet Interface Settings - HA Interface

Field	Description
Type	Select **HA** from the drop-down list.
Link Speed	Select the interface speed in Mbps (10, 100, or 1000).
Link Duplex	Select whether the interface transmission mode is full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
Link State	Select whether the interface status is enabled (Up), disabled (Down), or determined automatically (Auto).

4. Click **OK** to submit the new interface, or click **Cancel** to discard your changes.
5. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Defining Security Zones

To define each security policy rule, you must specify the source and destination zones of the traffic. Each zone identifies one or more interfaces on the firewall. 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.

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 67) has the same effect as applying policies between the Layer 2 and Layer 3 interface zones.

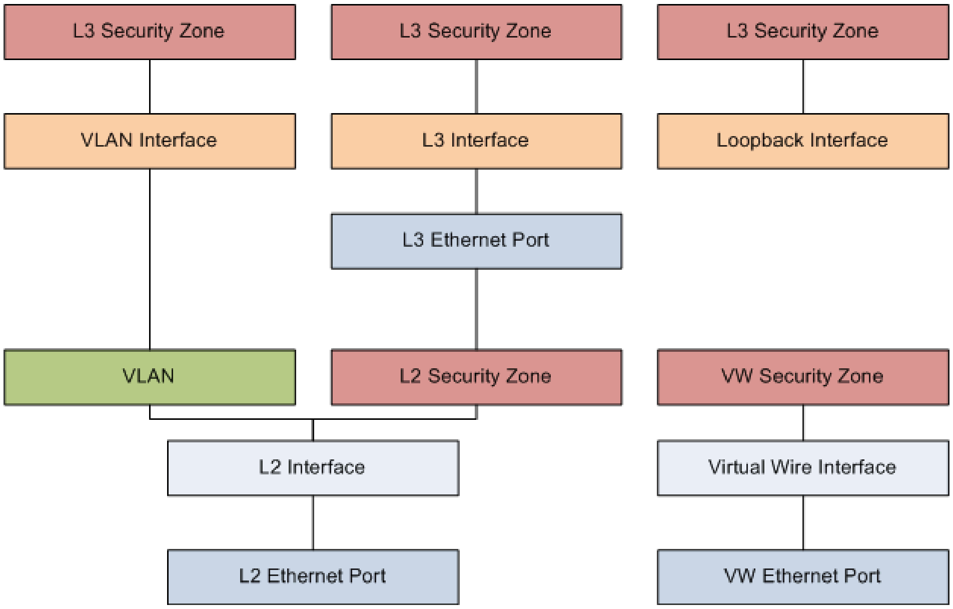
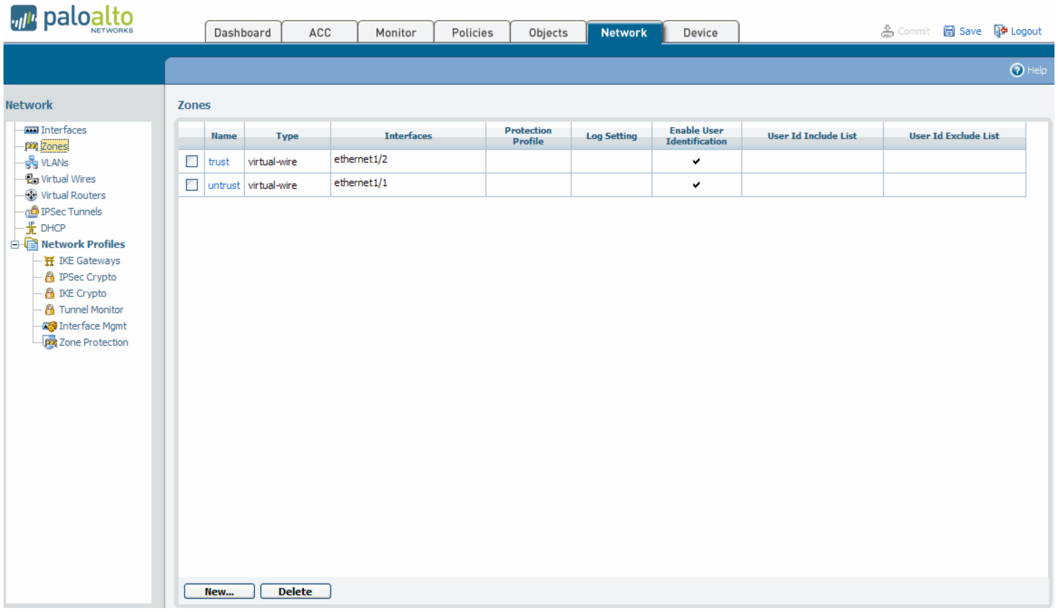


Figure 67. Zone and Interface Types

To apply zones to security policies, refer to "Defining Security Policies" on page 144.

To define security zones:

1. Under the **Network** tab, click **Zones** to open the Zones page.



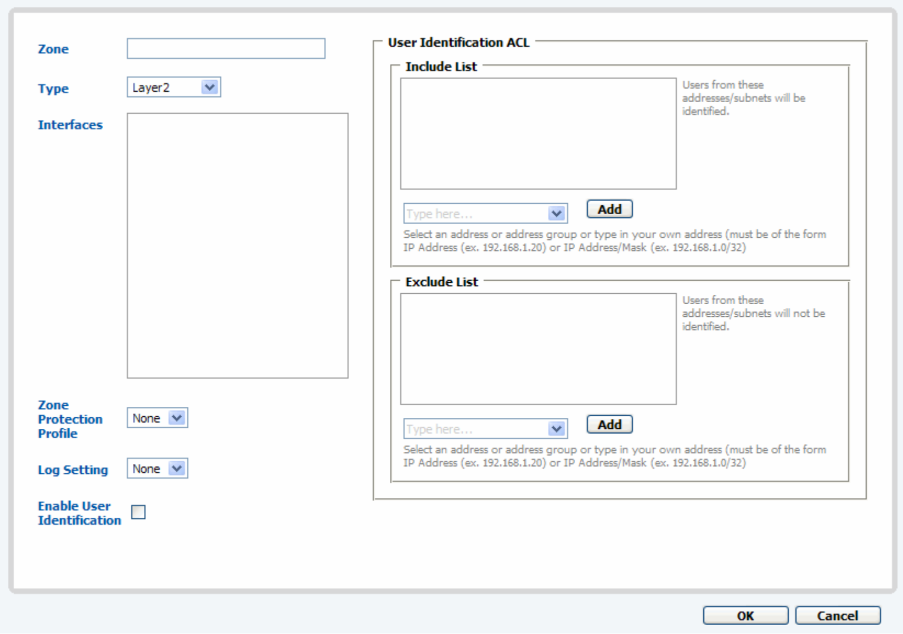
Zones

	Name	Type	Interfaces	Protection Profile	Log Setting	Enable User Identification	User Id Include List	User Id Exclude List
□	trust	virtual-wire	ethernet1/2			✓		
□	untrust	virtual-wire	ethernet1/1			✓		

Figure 68. Zones Page

2. To add a new zone:

   a. Click **New** to open the New Zone page.



Zone

Type: Layer2

Interfaces

Zone Protection Profile: None

Log Setting: None

Enable User Identification □

User Identification ACL

Include List

Users from these addresses/subnets will be identified.

Type here...

Select an address or address group or type in your own address (must be of the form IP Address (ex. 192.168.1.20) or IP Address/Mask (ex. 192.168.1.0/32)

Exclude List

Users from these addresses/subnets will not be identified.

Type here...

Select an address or address group or type in your own address (must be of the form IP Address (ex. 192.168.1.20) or IP Address/Mask (ex. 192.168.1.0/32)

Figure 69. Zones Page

b. Specify the following information.

Table 38. New Zone Settings

Field	Description
Zone	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.
Type	Select a zone type (Layer2, Layer3, or Virtual Wire) to list all the interfaces of that type that have not been assigned to a zone. The Layer 2 and Layer 3 zone types list all Ethernet interfaces and subinterfaces of that type. Each interface can belong to one zone in one virtual system.
Interfaces	Select the interfaces from the displayed list that you want to add to the zone. To add new interfaces, refer to “Configuring Interfaces” on page 98.
Zone Protection Profile	Select the zone protection profile. To add new zone protection profiles, refer to “Defining Zone Protection Profiles” on page 137.
Enable User Identification	Select to enable the user identification function on a per-zone basis.
User Identification ACL Include List	Enter the IP address or IP address/mask of a user or group to be identified (format *ip_address/mask*; for example, 10.1.1.1/24). Click **Add**. Repeat as needed.
User Identification ACL Exclude List	Enter the IP address or IP address/mask of a user or group that will explicitly not be identified (format *ip_address/mask*; for example, 10.1.1.1/24). Click **Add**. Repeat as needed.
Zone Protection Profile	Select a profile that specifies how the security gateway responds to attacks from this zone. To add new profiles, refer to “Defining Zone Protection Profiles” on page 137.
Enable User Identification	Select the check box to allow identification of users in this zone.
Log Setting	Select a log forwarding profile for forwarding zone protection logs to an external system.

c. Click **OK** to submit the new zone, or click **Cancel** to discard your changes.

3. To change a zone, click the zone name on the Zones page, change the settings, and click **OK**.

   To delete one or more zones, select the check box next to the zone names and click **Delete**. You cannot delete a zone that is used in a security policy. Note that deleting a zone or changing the zone type removes the associated interfaces from the zone.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

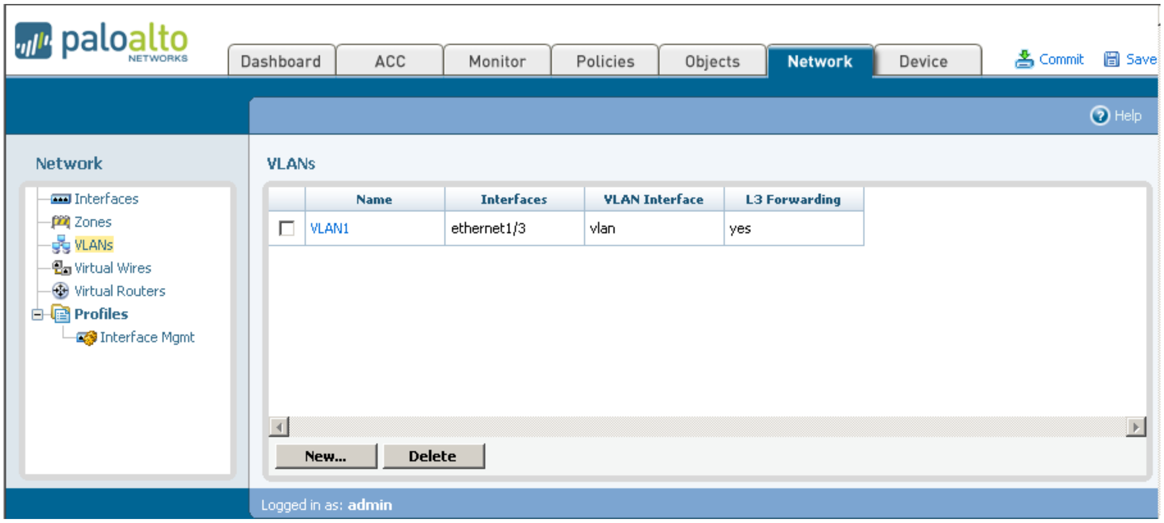
Defining VLANs

The firewall supports VLANs that conform to the IEEE 802.1Q standard. 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.

To configure Ethernet ports as Layer 2 interfaces, refer to "Configuring Layer 2 Interfaces" on page 100. To define Layer 2 subinterfaces, refer to "Configuring Layer 2 Subinterfaces" on page 101.

To define VLANs:

1. Under the **Network** tab, click **VLANs** to open the VLANs page.



VLANs

	Name	Interfaces	VLAN Interface	L3 Forwarding
□	VLAN1	ethernet1/3	vlan	yes

Figure 70. VLANs Page

2. To add a new VLAN:

    a. Click **New** to open the New VLAN page.

    b. Specify the following information.

Table 39. New VLAN Settings

Field	Description
Dot1q VLAN Name	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.
Interfaces	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 "Configuring Interfaces" on page 98.

Table 39. New VLAN Settings (Continued)

Field	Description
VLAN Interface	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 110.
L3 Forwarding Enabled	If you select a VLAN interface, you can select the check box to enable Layer 3 routing over the selected interface.

c. Click **OK** to submit the new VLAN, or click **Cancel** to discard your changes.

3. To change a VLAN, click the VLAN name on the VLANs page, change the settings, and click **OK**.

   To delete one or more VLANs, select the check box next to the VLAN names and click **Delete**. Note that deleting a VLAN removes it from the associated Layer 2 interfaces shown on the Interfaces page.

4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Defining Virtual Wires

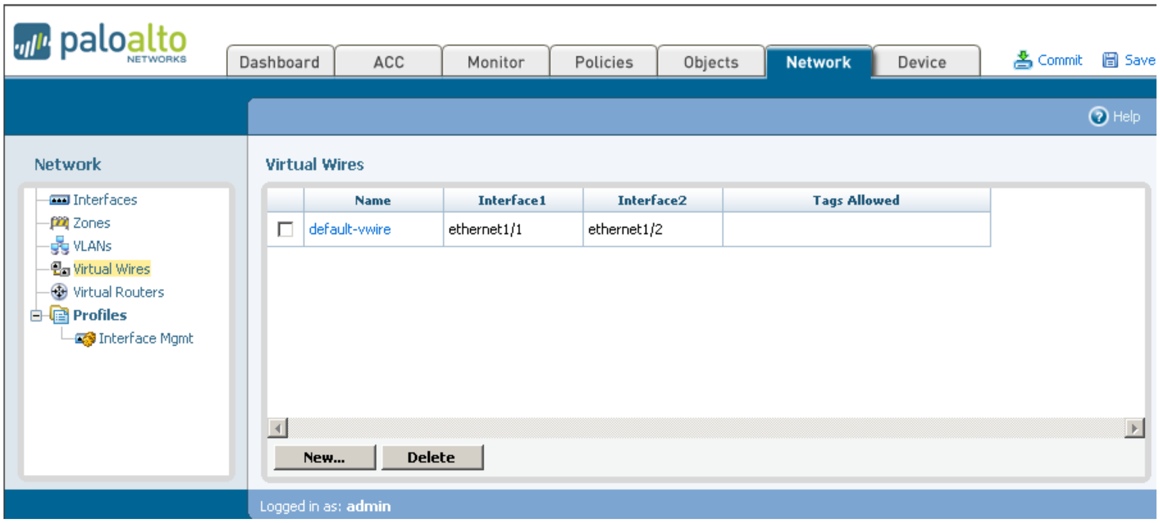
A virtual wire binds two Ethernet interfaces together so that you can install the firewall transparently in any network environment with no configuration of adjacent network devices required. If necessary, a virtual wire can block or allow traffic based on the virtual LAN (VLAN) tag values. By default, the virtual wire "default-vwire" binds together Ethernet ports 1 and 2 and allows all untagged traffic.

Use virtual wires only if:

- No routing or switching is required.
- No Network Address Translation (NAT) is required.

To define virtual wires:

1. Under the **Network** tab, click **Virtual Wires** to open the virtual wires page.



	Name	Interface1	Interface2	Tags Allowed
□	default-vwire	ethernet1/1	ethernet1/2	

Figure 71. Virtual Wires Page

2. To add a new virtual wire:

   a. Click **New** to open the New virtual wire page.

   b. Specify the following information.

Table 40. New Virtual Wire Settings

Field	Description
Virtual Wire Name	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.
Interfaces	Select two Ethernet interfaces from the displayed list that you want to configure as a virtual wire. Interfaces are listed here only if they have the virtual wire interface type and have not been assigned to another virtual wire. To specify the interface type, refer to “Configuring Virtual Wire Interfaces” on page 107.
Tags Allowed	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 will be dropped. Note that tag values are not changed on incoming or outgoing packets.
Multicast Firewalling	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.

   c. Click **OK** to submit the new virtual wire, or click **Cancel** to discard your changes.

3. 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 107).

   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.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Defining Virtual Routers

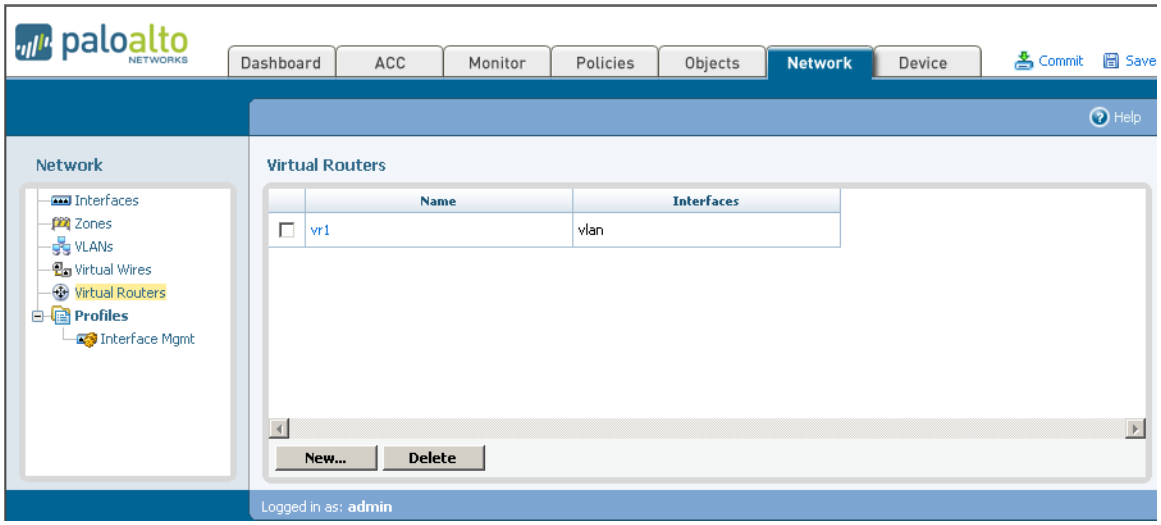
Defining virtual routers allows you to correctly set up forwarding rules for Layer 3 and enable the use of dynamic routing protocols.

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 102. To define Layer 3 subinterfaces, refer to “Configuring Layer 3 Subinterfaces” on page 105. For an overview of virtual routers, refer to “About Virtual Routers and Routing Protocols” on page 16.*

To add new virtual routers:

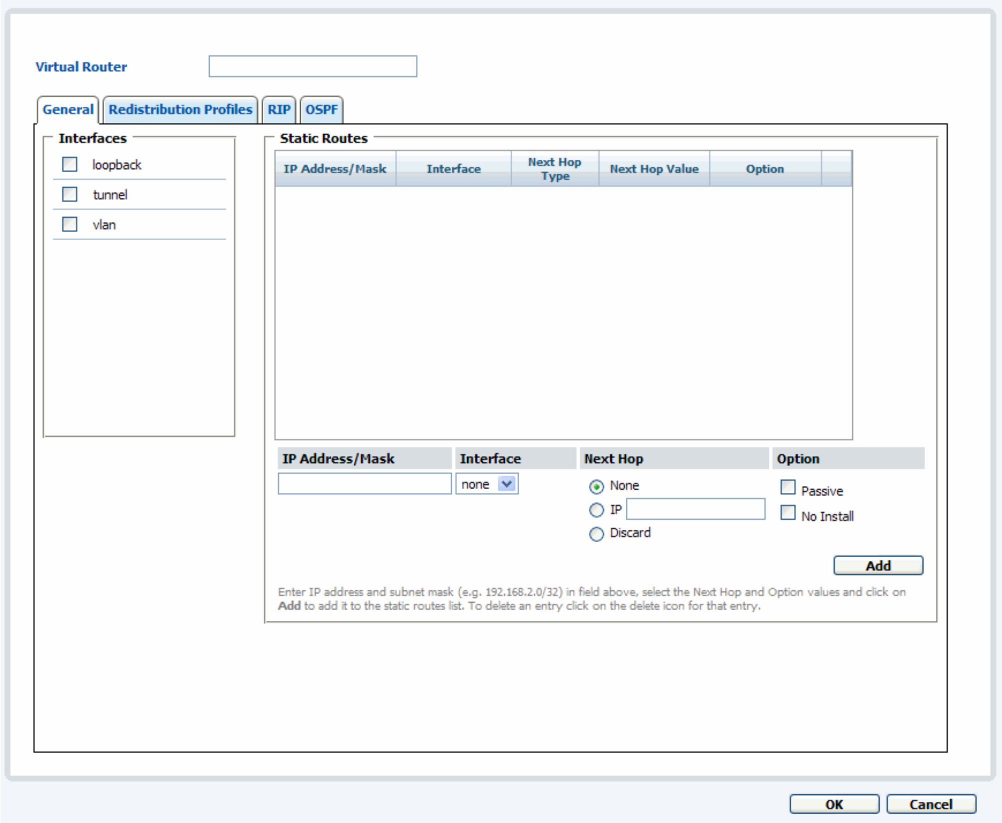
1. Under the **Network** tab, click **Virtual Routers** to open the Virtual Routers page.



	Name	Interfaces
□	vr1	vlan

Figure 72. Virtual Routers Page

2. Click **New** to open the New Virtual Router page.



Enter IP address and subnet mask (e.g. 192.168.2.0/32) in field above, select the Next Hop and Option values and click on **Add** to add it to the static routes list. To delete an entry click on the delete icon for that entry.

Figure 73. New Virtual Router Page

The page is divided into the following tabs.

Table 41. New Virtual Router Tabs

Field	Description
General	Select the interfaces to include in the virtual router and add any static routes.
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.

Table 41. New Virtual Router Tabs (Continued)

Field	Description
RIP	Specify parameters for use of the Routing Information Protocol (RIP) on the selected interfaces. ***Note:*** *Although it is possible to configure both RIP and OSPF, it is generally recommended to choose only one of these protocols.*
OSPF	Specify parameters for use of the Open Shortest Path First (OSPF) protocol on the selected interfaces. ***Note:*** *Although it is possible to configure both RIP and OSPF, it is generally recommended to choose only one of these protocols.*

3. Enter a name for the virtual router (up to 20 characters). This name appears in the list of virtual routers when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.

4. Follow this process to complete the virtual router definition:

   a. Complete the settings on the **General** tab as described in the following table.

Table 42. New Virtual Router Settings - General Tab

Field	Description
Interfaces	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 "Configuring Interfaces" on page 98. ***Note:*** *When you add an interface, its connect routes are added automatically.*
Static Routes	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.* • In the **IP Address/Mask** field, enter an IP address and network mask in the format *ip_address/mask*, configure additional options, and click **Add**. • Specify the forwarding interface or **Next Hop** field (or both): – **Interface**—Select the interface to forward packets to its destination. – **IP**—Specify the gateway IP address. – **Discard**—Select if you want to drop the traffic sent to the specified IP addresses. • Optionally, select one or both of the following options: – **Passive**—Install the route in the forwarding table even if the interface used to reach the gateway is down. By default, a route is not installed unless the associated interface is active. – **No Install**—Do not install the route in the forwarding table. The route is retained in the configuration for future reference.

b. If necessary, complete the settings for dynamic routing on the **RIP** or **OSPF** tab, as described in the following tables (Table 43 and Table 44).

Table 43. New Virtual Router Settings - RIP Tab

Field	Description
Enable	Select the check box to enable the RIP protocol.
Reject Default Route	Select the check box if you do not want to learn any default routes through RIP. Selecting the check box is highly recommended.
Auth Profiles	To authenticate RIP messages, first define the authentication profiles and then apply them to interfaces on the **RIP** tab. Click **Add** and enter the following values. • **Name**—Enter a name for the authentication profile. • **Password Type**—Select the type of password (simple or MD5). – If you select **Simple**, enter the password. – If you select **MD5**, enter one or more password entries, including **Key-ID** (0-255), **Key**, and optional **Preferred** status. Click **Add** for each entry, and then click **OK**. To specify the key to be used to authenticate outgoing message, select the **Preferred** option.
Interfaces	Click **Add**, enter the following values, and click **OK**. • **Interface**—Select the interface that runs the RIP protocol. • **Enable**—Select to enable these settings. • **Advertise** and **Metric**—Select to advertise a default route to RIP peers with the specified metric value. • **Auth Profile**—Select the profile. • **Mode**—Select **normal**, **passive**, or **send-only**.
RIP Timing	Configure these timing settings: • **Interval Duration**—Define the length of the timer interval in seconds. This duration is used for the remaining **RIP Timing** fields. Range (1 - 60) • **Update Intervals**—Enter the number of intervals between route update announcements. Range (1 - 3600) • **Expire Intervals**—Enter the number of intervals between the time that the route was last updated to its expiration. Range (1- 3600) • **Delete Intervals**—Enter the number of intervals between the time of route expiration to its deletion. Range (1- 3600)
Export Rules	To export redistribution profiles, select the profiles in the list.

Table 44. New Virtual Router Settings - OSPF Tab

Field	Description
Enable	Select the check box to enable the OSPF protocol.
Reject Default Route	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.
RFC 1583 Compatibility	Select the check box to assure compatibility with RFC 1583.
Auth Profiles	To authenticate the OSPF messages, first define the authentication profiles and then apply them to interfaces on the **OSPF** tab. Click **Add** and enter the following values. • **Name**—Enter a name for the authentication profile. • **Password Type**—Select the type of password (simple or MD5). – If you select **Simple**, enter the password. – If you select **MD5**, enter one or more password entries, including **Key-ID** (0-255), **Key**, and optional **Preferred** status. Click **Add** for each entry, and then click **OK**. To specify the key to be used to authenticate outgoing message, select the **Preferred** option.
Areas	OSPF areas indicate the scope over which the OSPF parameters can be applied. Click **New**, enter the following values, and click **Done**. *Note: You must click **Done** for your changes to take effect.* • **Area ID**—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. • **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 (range 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 (range 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 learned through NSSA to other areas. • **Range**—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.

Table 44. New Virtual Router Settings - OSPF Tab (Continued)

Field	Description
Areas (continued)	• **Interfaces**—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 to 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 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 (range 0-65535). – **Priority**—Enter the OSPF priority for this interface (range 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 p2pmp interfaces, enter the neighbor IP address for all neighbors reachable through this interface. • **Virtual Link**—Virtual links can be used to maintain or enhance backbone area connectivity. They must be defined between area boarder 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.
Export Rules	To apply redistribution profiles for export routes to the OSPF instance, click **Add**, enter the following information, and click **OK**. – **Name**—Select the name of a redistribution profile. – **New Metric Type**—Optionally select the metric type to apply. – **New Tag**—Optionally tag the matched route with a 32-bit value.

c. Check the status of the virtual router as described on page 129.

d. Define redistribution profiles as described in the following table.

Table 45. New Virtual Router Settings - Redistribution Profiles Tab

Field	Description
Profile Name	Click **Add** to display the New Redistribution Profile page, and enter the profile name.
Priority	Enter a priority (range 1-255) for this profile. Profiles are matched in order (lowest number first).
Filter	Configure the following filter options. • **Type**—Select check boxes to specify the route types of the candidate route. • **Interface**—Select the interfaces to specify the forwarding interfaces of the candidate route. • **Destination**—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 X associated with the entry. • **Next Hop**—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 X associated with the entry.
OSPF	Optionally configure these OSPF filter parameters. • **Metric Type**—Select check boxes to specify the route types of the candidate OSPF route. • **Area**—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 X associated with the entry.
Action	Select from the following actions. • **Redistribute**—Redistribute matching candidate routes. • **No-Redistribute**— Prevent redistribution of matching candidate routes. • **Metric**—Enter the new metric value when taking a redistribution action. A lower metric value means a more preferred route.

a. Apply the redistribution profiles to the RIP or OSPF protocol by selecting export rules in the Export Rules section on the **RIP** or **OSPF** tab.

b. Click **OK** to submit the new virtual router, or click **Cancel** to discard your changes.

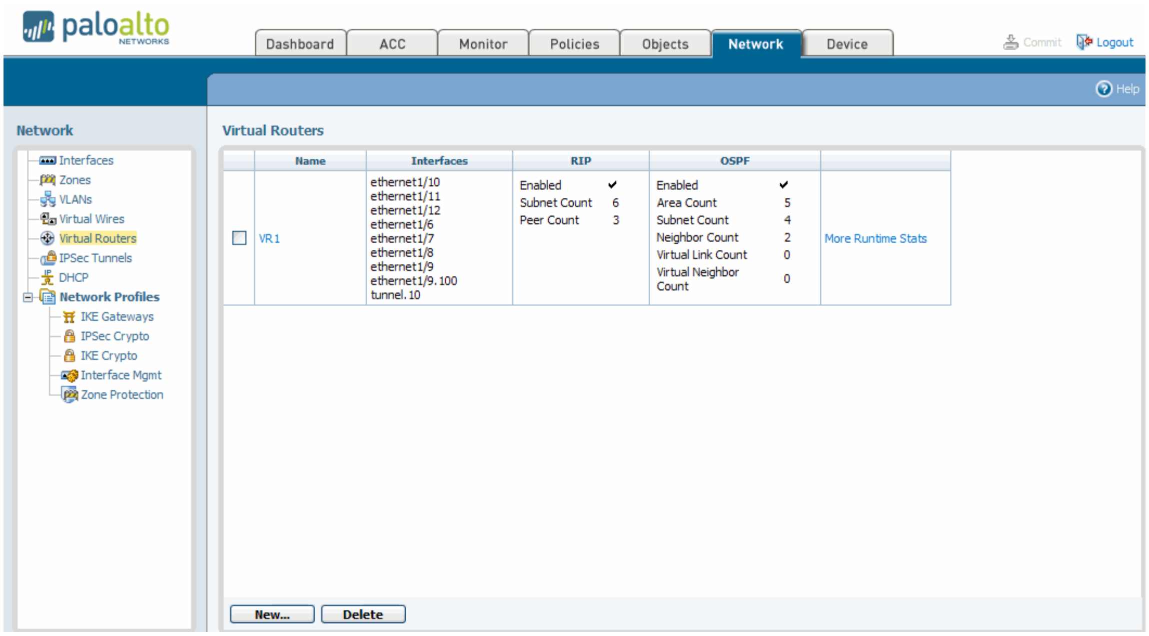
5. To change a virtual router, click the virtual router name on the Virtual Routers page, change the settings, and click **OK**. Virtual routers also can be changed from the Interfaces page (refer to “Configuring Layer 3 Interfaces” on page 102).

   To delete one or more virtual routers, select the check box next to the virtual router names and click **Delete**. Note that deleting a virtual router removes it from the associated interfaces shown on the Interfaces page.

6. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

To display runtime statistics for the virtual router and routing protocols:

1. Under the **Network** tab, click **Virtual Routers** to open the Virtual Routers page.



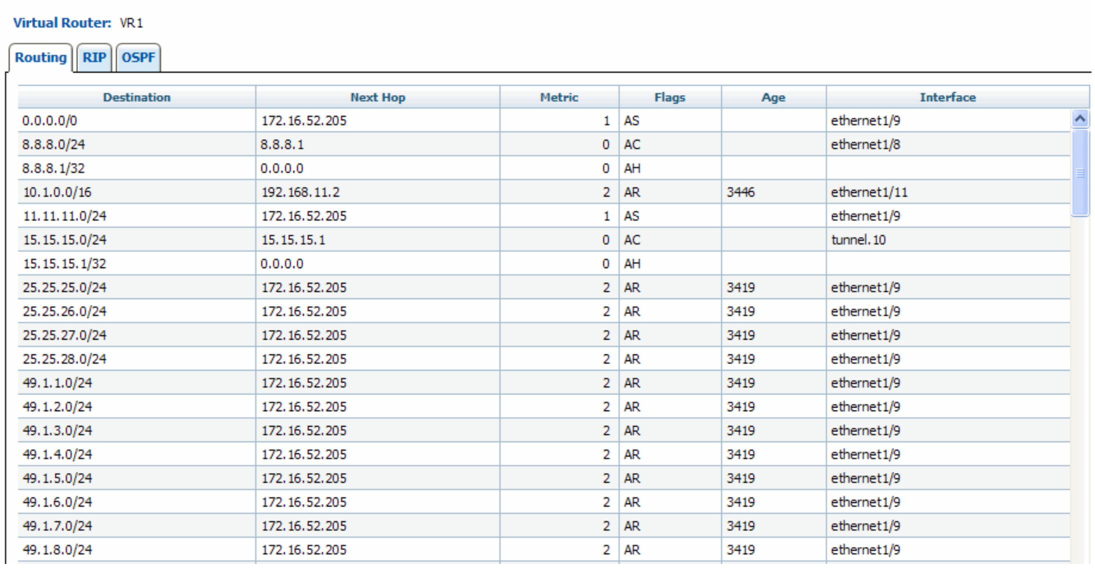
Virtual Routers

	Name	Interfaces	RIP	OSPF	
□	VR1	ethernet1/10 ethernet1/11 ethernet1/12 ethernet1/6 ethernet1/7 ethernet1/8 ethernet1/9 ethernet1/9.100 tunnel.10	Enabled ✓ Subnet Count 6 Peer Count 3	Enabled ✓ Area Count 5 Subnet Count 4 Neighbor Count 2 Virtual Link Count 0 Virtual Neighbor Count 0	More Runtime Stats

Figure 74. Virtual Routers Page

The page displays the interfaces currently in use and summary statistics for the RIP and OSPF protocols.

2. Click the **More Runtime Stats** link for a virtual router to open the statistics window.



Virtual Router: VR1

Destination	Next Hop	Metric	Flags	Age	Interface
0.0.0.0/0	172.16.52.205	1	AS		ethernet1/9
8.8.8.0/24	8.8.8.1	0	AC		ethernet1/8
8.8.8.1/32	0.0.0.0	0	AH		
10.1.0.0/16	192.168.11.2	2	AR	3446	ethernet1/11
11.11.11.0/24	172.16.52.205	1	AS		ethernet1/9
15.15.15.0/24	15.15.15.1	0	AC		tunnel.10
15.15.15.1/32	0.0.0.0	0	AH		
25.25.25.0/24	172.16.52.205	2	AR	3419	ethernet1/9
25.25.26.0/24	172.16.52.205	2	AR	3419	ethernet1/9
25.25.27.0/24	172.16.52.205	2	AR	3419	ethernet1/9
25.25.28.0/24	172.16.52.205	2	AR	3419	ethernet1/9
49.1.1.0/24	172.16.52.205	2	AR	3419	ethernet1/9
49.1.2.0/24	172.16.52.205	2	AR	3419	ethernet1/9
49.1.3.0/24	172.16.52.205	2	AR	3419	ethernet1/9
49.1.4.0/24	172.16.52.205	2	AR	3419	ethernet1/9
49.1.5.0/24	172.16.52.205	2	AR	3419	ethernet1/9
49.1.6.0/24	172.16.52.205	2	AR	3419	ethernet1/9
49.1.7.0/24	172.16.52.205	2	AR	3419	ethernet1/9
49.1.8.0/24	172.16.52.205	2	AR	3419	ethernet1/9

Figure 75. Virtual Routers Runtime Statistics

3. Click one of the following tabs to display runtime information.

Table 46. Virtual Router Runtime Statistics

Tab	Description
Routing	Runtime routing information.
RIP	Runtime information on RIP traffic. Includes tabs that present information in the following categories: • Summary • Interface • Peer
OSPF	Runtime information on OSPF traffic, including tabs that present information in the following categories: • Summary • Area • Interface • Neighbor • Virtual Link • Virtual Neighbors

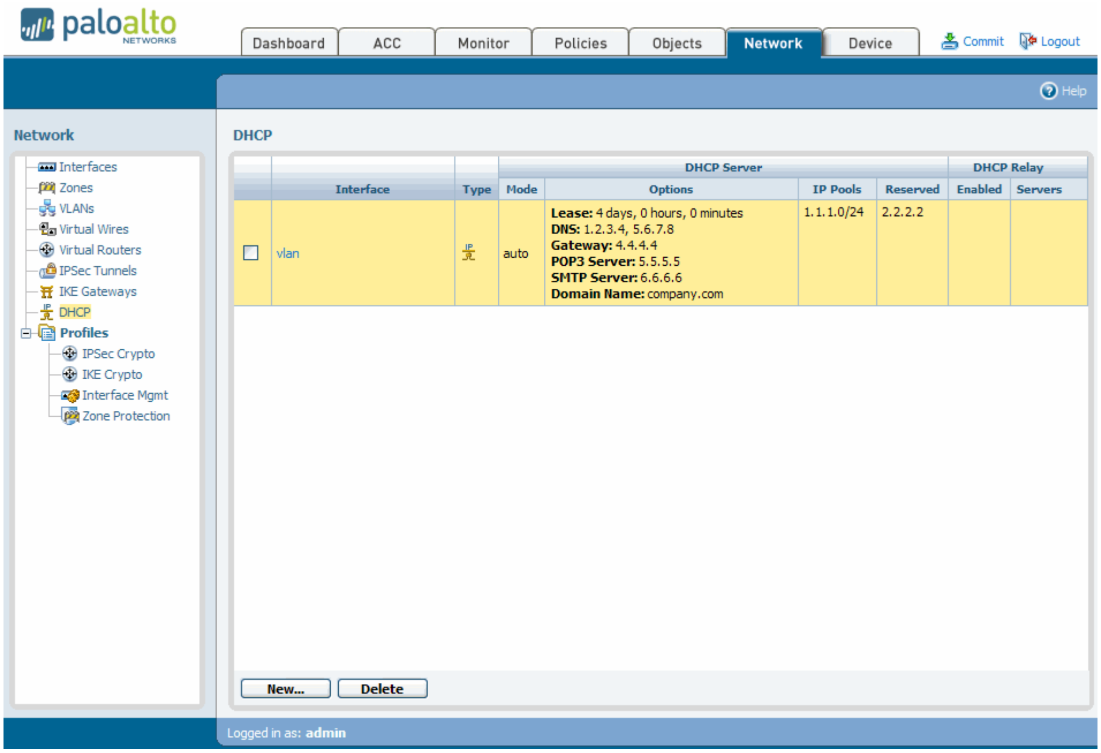
Defining DHCP Options

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 more information on IPSec VPN tunnels, refer to “Configuring IPSec Tunnels” on page 261.

To configure DHCP settings:

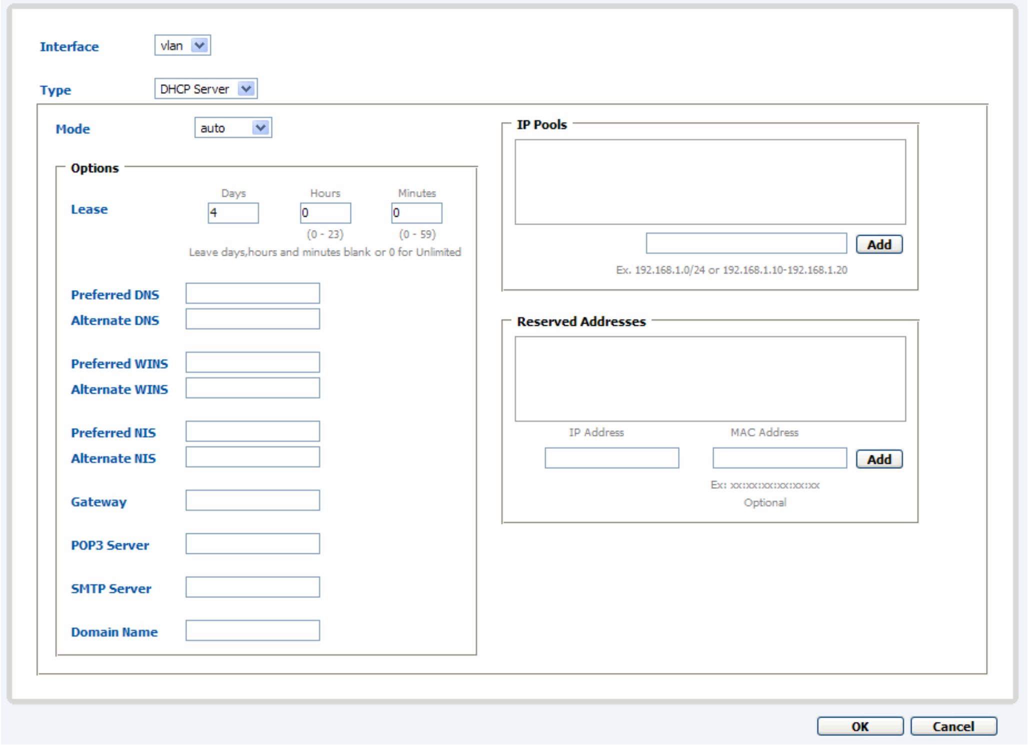
1. Under the **Network** tab, click **DHCP** to open the DHCP page.



			DHCP Server				DHCP Relay	
	Interface	Type	Mode	Options	IP Pools	Reserved	Enabled	Servers
☐	vlan		auto	**Lease:** 4 days, 0 hours, 0 minutes **DNS:** 1.2.3.4, 5.6.7.8 **Gateway:** 4.4.4.4 **POP3 Server:** 5.5.5.5 **SMTP Server:** 6.6.6.6 **Domain Name:** company.com	1.1.1.0/24	2.2.2.2		

Figure 76. DHCP Page

2. Click **New** to open the configuration page.



Interface vlan

Type DHCP Server

Mode auto

Lease Days 4 Hours 0 Minutes 0

Figure 77. Defining DHCP Settings

3. Specify the following information.

Table 47. DHCP Settings

Field	Description
Interface	Select the firewall interface.
Type	Select the type of DHCP request.
Mode	Select whether the settings on this page and enabled, disabled, or have use determined automatically.
Lease	Enter any limitations on the DHCP lease interval. You can enter days, hours, or minutes. For example, if you enter only hours, then the lease is restricted to that number of hours.
Preferred DNS Alternate DNS	Enter the IP address of the preferred and alternate Domain Name Service (DNS) servers. The alternate server address is optional.
Preferred WINS Alternate WINS	Enter the IP address of the preferred and alternate Windows Internet Naming Service (WINS) servers. The alternate server address is optional.
Preferred NIS Alternate NIS	Enter the IP address of the preferred and alternate Network Information Service (NIS) servers. The alternate server address is optional.
Gateway	Enter the IP address of the network gateway that is used to reach the DHCP servers.
POP3 Server	Enter the IP address of the Post Office Protocol (POP3) server.

Table 47. DHCP Settings (Continued)

Field	Description
SMTP Server	Enter the IP address of the Simple Mail Transfer Protocol (SMTP) server.
IP Pools	Specify the range of IP addresses to which this DHCP configuration applies and click **Add**. You can enter an IP subnet and subnet mask (for example, 192.168.1.0/24) or a range of IP addresses (for example, 192.168.1.10-192.168.1.20). Add multiple entries to specify multiple IP address pools. To edit an existing entry, click **Edit**, make the changes, and click **Done**. To delete an entry, click **Delete**. ***Note:*** *If you leave this area blank, there will be no restrictions on the IP ranges.*
Reserved Addresses	Enter the IP address (format x.x.x.x) or MAC address (format xx:xx:xx:xx:xx:xx) of any devices that you do not want to subject to DHCP address assignment. To edit an existing entry, click **Edit**, make the changes, and click **Done**. To delete an entry, click **Delete**. ***Note:*** *If you leave this area blank, then there will be no reserved IP addresses.*

4. Click **OK**.

   The DHCP page reopens to show the new entry.

5. To edit an existing entry, click the underlined link for the entry.

6. To delete an entry, select the entry and click **Delete**.

Defining Network Profiles

Refer to the following sections for information on defining network profiles:

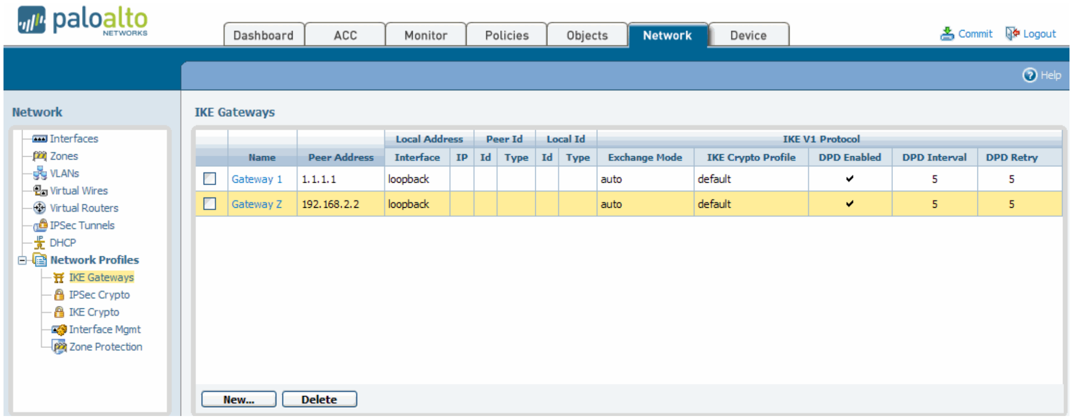
- “Setting Up IKE Gateways” in the next section
- “Defining Interface Management Profiles” on page 136
- “Defining Zone Protection Profiles” on page 137

Setting Up IKE Gateways

Use the IKE gateways page to define gateways that include the configuration information necessary to perform IKE protocol negotiation with peer gateways. Refer to “About Virtual Private Networks” on page 17 for more information, and refer to “Defining IKE Crypto Profiles” on page 263 for information on defining IKE crypto profiles.

To set up IKE gateways:

1. Under the **Network** tab, click **IKE Gateways** under **Network Profiles** to open the IKE Gateways page.

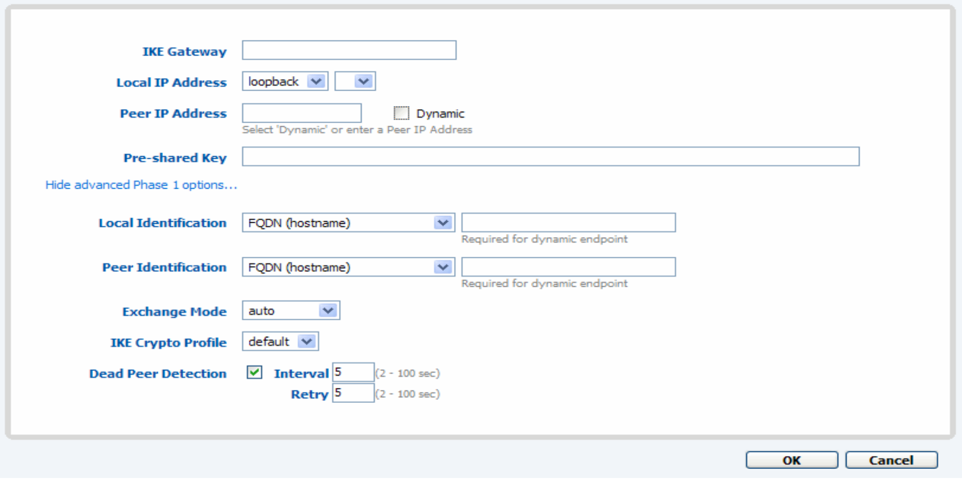


IKE Gateways

			Local Address		Peer Id		Local Id		IKE V1 Protocol				
	Name	Peer Address	Interface	IP	Id	Type	Id	Type	Exchange Mode	IKE Crypto Profile	DPD Enabled	DPD Interval	DPD Retry
□	Gateway 1	1.1.1.1	loopback						auto	default	✓	5	5
□	Gateway 2	192.168.2.2	loopback						auto	default	✓	5	5

Figure 78. IKE Gateways Page

2. Click **New** to open the configuration page.



IKE Gateway

Local IP Address: loopback

Peer IP Address: □ Dynamic
Select 'Dynamic' or enter a Peer IP Address

Pre-shared Key

Hide advanced Phase 1 options...

Local Identification: FQDN (hostname)
Required for dynamic endpoint

Peer Identification: FQDN (hostname)
Required for dynamic endpoint

Exchange Mode: auto

IKE Crypto Profile: default

Dead Peer Detection: ☑ Interval 5 (2 - 100 sec)
Retry 5 (2 - 100 sec)

Figure 79. Defining IKE Gateway Settings

3. Specify the following information.

Table 48. IKE Gateway Settings

Field	Description
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.
Peer IP Address	Static IP address or dynamic option for the peer on the far end of the tunnel.
Pre-shared key	Enter a security key to use for authentication across the tunnel.
Note: *The following advanced fields are visible if you click the* ***Show advanced Phase 1 options*** *link.*	
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: FQDN, key ID, or user FQDN (for the dynamic option)
Exchange Mode	Choose auto, aggressive, or main.
IKE Crypto Profile	Select an existing profile or keep the default profile. Select an existing profile or keep the default profile.
Dead Peer Detection	Select to enable. If enabled, enter an interval (2 - 100 seconds) and delay before retrying (2 - 100 seconds).

4. Click **OK**.

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.*

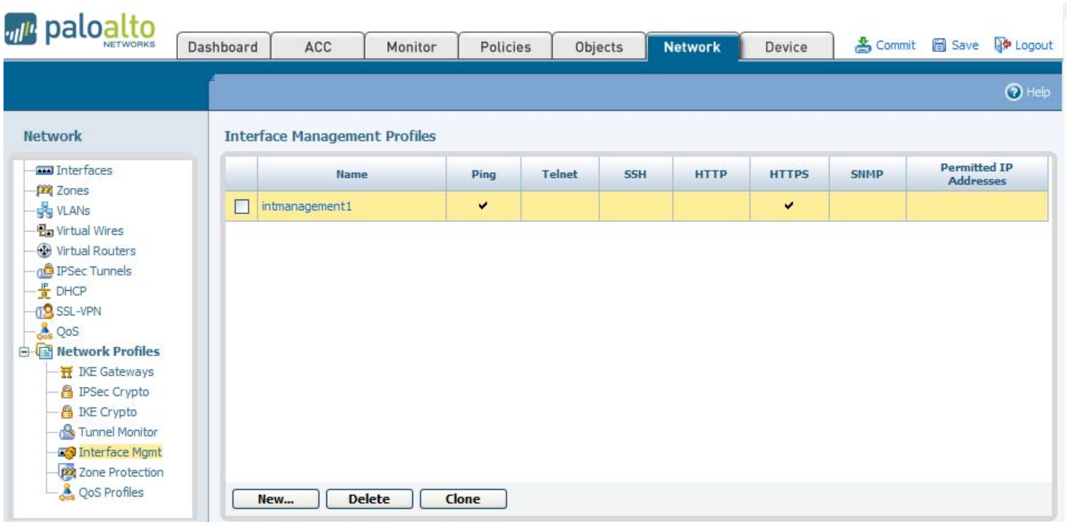
You must configure the peer device with the matching exchange mode to allow it to accept negotiation requests initiated from the first device.

Defining Interface Management Profiles

For each Layer 3 interface, including VLAN and loopback interfaces, you can define a management profile that specifies which protocols can be used to manage the firewall. To assign management profiles to each interface, refer to "Configuring Layer 3 Interfaces" on page 102 and "Configuring Layer 3 Subinterfaces" on page 105.

To define interface management profiles:

1. Under the **Network** tab, click **Interface Mgmt** under **Network Profiles** to open the Interface Management Profiles page.



	Name	Ping	Telnet	SSH	HTTP	HTTPS	SNMP	Permitted IP Addresses
□	intmanagement1	✓				✓		

Figure 80. Interface Management Profiles Page

2. To add a new interface management profile:

   a. Click **New** to open the New Interface Management Profile page.

   b. Specify the following information.

Table 49. New Interface Management Profile Settings

Field	Description
Name	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.
Ping Telnet SSH HTTP HTTPS SNMP	Select the check box for each service to be enabled on the interfaces where the profile is applied.
Permitted IP	Enter the IP addresses of any external servers that are used to manage the firewall (in-band management) through the data port.

   c. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Defining Zone Protection Profiles

For each security zone, you can define a zone protection profile that specifies how the security gateway responds to attacks from that zone. The same profile can be assigned to multiple zones. To assign zone protection profiles to each zone, refer to "Defining Security Zones" on page 116.

The following types of protection are supported:

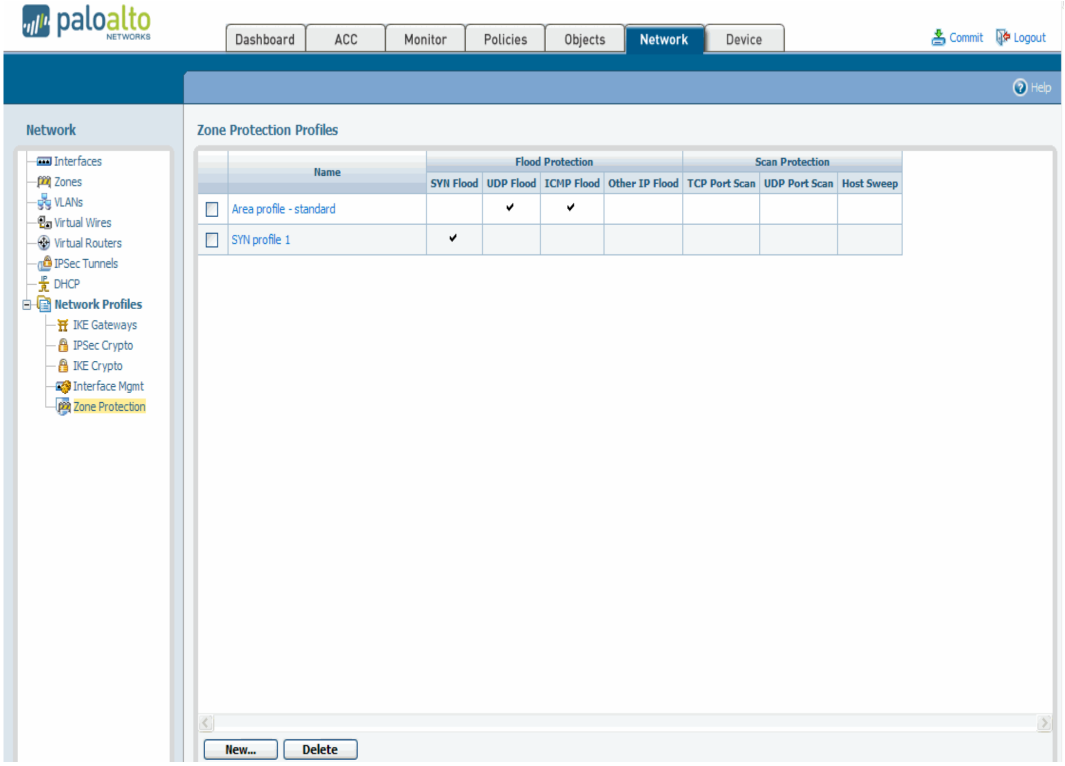
- **Flood Protection**—Protects against SYN, ICMP, UDP, and other IP-based flooding attacks.

- **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.

To define zone protection profiles:

1. Under the **Network** tab, click **Zone Protection** under **Network Profiles** to open the Zone Protection Profiles page.



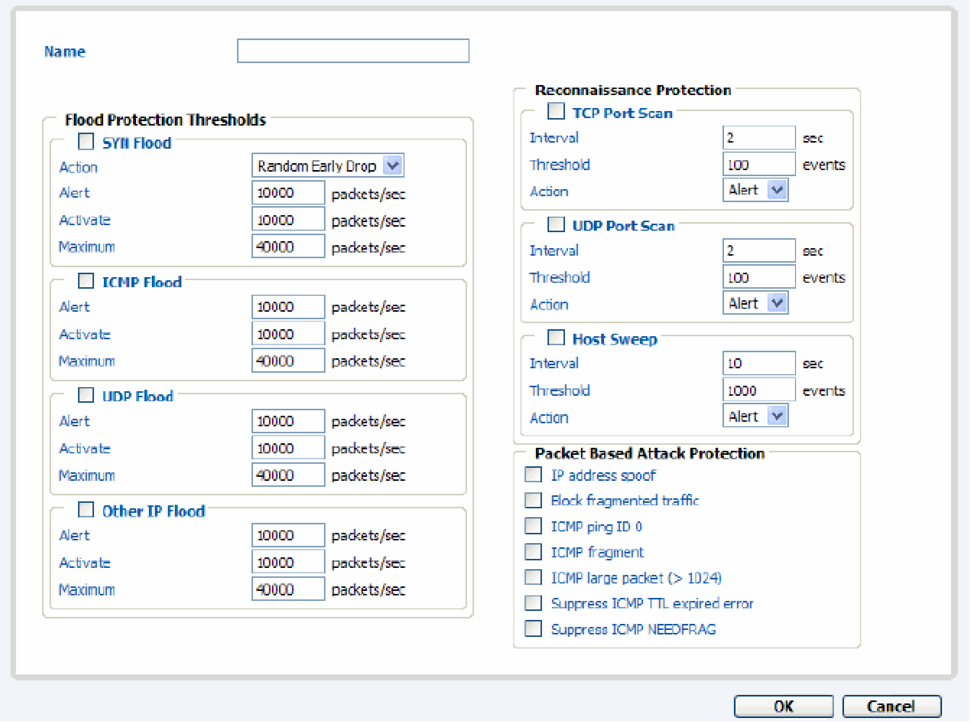
Zone Protection Profiles

	Name	Flood Protection				Scan Protection		
		SYN Flood	UDP Flood	ICMP Flood	Other IP Flood	TCP Port Scan	UDP Port Scan	Host Sweep
□	Area profile - standard		✓	✓				
□	SYN profile 1	✓						

Figure 81. Zone Protection Profiles Page

2. To add a new profile:

   a. Click **New**.



Name

Flood Protection Thresholds

□ SYN Flood

Action: Random Early Drop
Alert: 10000 packets/sec
Activate: 10000 packets/sec
Maximum: 40000 packets/sec

□ ICMP Flood

Alert: 10000 packets/sec
Activate: 10000 packets/sec
Maximum: 40000 packets/sec

□ UDP Flood

Alert: 10000 packets/sec
Activate: 10000 packets/sec
Maximum: 40000 packets/sec

□ Other IP Flood

Alert: 10000 packets/sec
Activate: 10000 packets/sec
Maximum: 40000 packets/sec

Reconnaissance Protection

□ TCP Port Scan

Interval: 2 sec
Threshold: 100 events
Action: Alert

□ UDP Port Scan

Interval: 2 sec
Threshold: 100 events
Action: Alert

□ Host Sweep

Interval: 10 sec
Threshold: 1000 events
Action: Alert

Packet Based Attack Protection

□ IP address spoof
□ Block fragmented traffic
□ ICMP ping ID 0
□ ICMP fragment
□ ICMP large packet (> 1024)
□ Suppress ICMP TTL expired error
□ Suppress ICMP NEEDFRAG

Figure 82. New Zone Protection Profile Page

   b. Select the check box for each type of protection you want to implement, and specify the following information.

Table 50. New Zone Protection Profile Settings

Field	Description
Name	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.
Flood Protection Thresholds - SYN Flood	
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 exceed 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.

Table 50. New Zone Protection Profile Settings (Continued)

Field	Description
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 216) and in the threat log (refer to "Identifying Unknown Applications and Taking Action" on page 246). Alarms can also generate SNMP traps and syslog messages (refer to "Defining SNMP Trap Destinations" on page 81 and "Defining Syslog Servers" on page 83).
Activate	Enter the number of SYN packets received per second for the same destination that triggers a response. The response is disabled when the number of SYN 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	
Alert	Enter the number of ICMP echo requests (pings) received per second that triggers an attack alarm.
Activate	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.
Maximum	Enter the maximum number of ICMP packets able to be received per second. Any number of packets exceeding the maximum will be dropped.
Flood Protection Thresholds - UDP Flood	
Alert	Enter the number of UDP packets received per second for the same destination that triggers an attack alarm.
Activate	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.
Maximum	Enter the maximum number of UDP packets able to be received per second. Any number of packets exceeding the maximum will be dropped.
Flood Protection Thresholds -Other IP Flood	
Alert	Enter the number of IP packets received per second for the same destination that triggers an attack alarm.
Activate	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.
Maximum	Enter the maximum number of IP packets able to be received per second. Any number of packets exceeding the maximum will be dropped.

Table 50. New Zone Protection Profile Settings (Continued)

Field	Description
Reconnaissance Protection - TCP Port Scan, UDP Port Scan, Host Sweep	
Interval	Enter the time interval for port scans and host sweep detection (seconds).
Threshold	Enter the number of scanned ports within the specified time interval that will trigger this protection type (events).
Action	Enter the action that the system will take in response to this event type: • **Allow**—Permits the port scan of host sweep reconnaissance. • **Alert**—Generates an alert for each scan or sweep that matches the threshold within the specified time interval. • **Drop**—Drops all further packets from the source to the destination for the remainder of the specified time interval.
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.
Suppress ICMP TTL expired error	Does not display expired ICMP time-to-live (TTL) errors.
Suppress ICMP NEEDFRAG	Does not display information about ICMP need-to-fragment packets.

c. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Chapter 5

Policies and Security Profiles

This chapter describes how to configure security policies and profiles:

- "About Policies and Profiles" in the next section
- "Defining Policies" on page 144
- "Defining Security Profiles" on page 164
- "Defining Policy Objects" on page 192

About Policies and Profiles

The operation of the firewall is controlled by several types of policies and profiles. The policies include:

- 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.
- Network Address Translation (NAT) policies to translate addresses and ports, as needed.
- SSL Decryption policies to specify the SSL traffic to be decrypted so that security policies can be applied. Each policy can specify the categories of URLs for the traffic you want to decrypt.
- Application override policies to override the application definitions provided by the firewall.

Each security policy can specify one or more security and logging profiles. Security profiles defend the network against viruses, spyware, and other known threats. The profiles include:

- Antivirus profiles to protect against worms and viruses.
- Anti-spyware profiles to block spyware downloads and attempts by spyware to access the network.
- Vulnerability protection profiles to stop attempts to exploit system flaws or gain unauthorized access to systems.
- URL filtering profiles to restrict access to specific web sites and web site categories.

- File blocking profiles to block selected file types.
- Data filtering profiles that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall.

Defining Policies

For information about defining policies, refer to:

- "Defining Security Policies" in the next section
- "Defining Network Address Translation Policies" on page 150
- "Defining SSL Decryption Policies" on page 154
- "Defining Application Override Policies" on page 158
- "Defining Captive Portal Policies" on page 160
- "Specifying Users and Applications for Policies" on page 163

Defining Security Policies

Security policies specify whether to block or allow a new network session based on the 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 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.

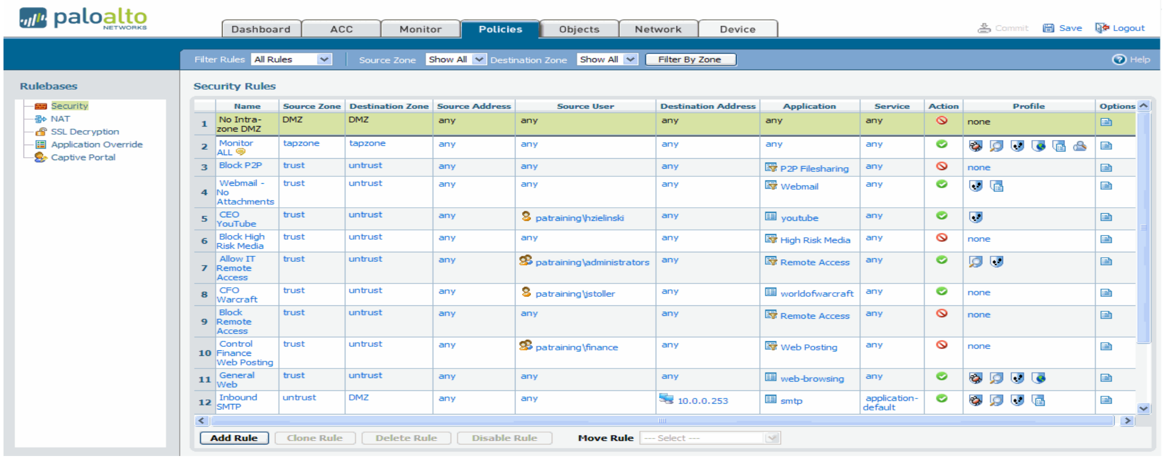
Note: *By default, traffic between each pair of security zones is blocked until at least one rule is added to allow traffic between the two zones.*

Each security policy can also specify security profiles that protect against viruses, spyware, and other threats, a log forwarding profile that enables remote logging for traffic sessions and security threats, and a schedule that determines the days and times when the policy is in effect.

Security policies can be as general or specific as needed. The policy rules are compared against the incoming traffic in sequence, and since 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.

To define security policies:

1. Under the **Policies** tab, click **Security** to open the Security Rules page.



Security Rules

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1	No Intra-zone DMZ	DMZ	DMZ	any	any	any	any	any	⊘	none	
2	Monitor ALL	tapzone	tapzone	any	any	any	any	any	✓		
3	Block P2P	trust	untrust	any	any	any	P2P Filesharing	any	⊘	none	
4	Webmail - No Attachments	trust	untrust	any	any	any	Webmail	any	✓		
5	CEO YouTube	trust	untrust	any	patraining\hzielinski	any	youtube	any	✓		
6	Block High Risk Media	trust	untrust	any	any	any	High Risk Media	any	⊘	none	
7	Allow IT Remote Access	trust	untrust	any	patraining\administrators	any	Remote Access	any	✓		
8	CFO Warcraft	trust	untrust	any	patraining\jstoller	any	worldofwarcraft	any	✓	none	
9	Block Remote Access	trust	untrust	any	any	any	Remote Access	any	⊘	none	
10	Control Finance Web Posting	trust	untrust	any	patraining\finance	any	Web Posting	any	⊘	none	
11	General Web	trust	untrust	any	any	any	web-browsing	any	✓		
12	Inbound SMTP	untrust	DMZ	any	any	10.0.0.253	smtp	application-default	✓		

Figure 83. Security Rules Page

2. 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**.

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

Note: *Shared polices pushed from Panorama are shown in green and cannot be edited at the device level.*

4. 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 highest 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 116.

   – 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.

5. To change a field in a new or existing rule, click the current field value, specify the appropriate information, as described below, and click **OK**.

Table 51. Security Rule Settings

Field	Description
Name	Change the default rule name and/or enter a rule description. If you add a rule description, a 💬 is added next to the rule name. By default, rules are named “rule<n>”, 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.
Source Zone Destination Zone	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 116. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, public relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.
Source Address Destination Address	Select the source and destination IPv4 or IPv6 addresses for which the security rule applies. To select specific addresses, 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 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_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 disable all addresses without removing them, click **Negate**. A line is drawn through each address and group on the Security Rules page, which applies the rule to all addresses (same effect as any). To add new addresses that can be used in this or other policies, click **New Address** (refer to “Defining Addresses” on page 193). To define new address groups, refer to “Defining Address Groups” on page 195.

Table 51. Security Rule Settings (Continued)

Field	Description
Source User	Select the source users or groups of users subject to this policy. Click the link 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 set up user identification, refer to "Configuring the User Identification Agent" on page 53.
Application	Select specific applications for the security rule. 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 311. • 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 196. To define application groups, refer to "Defining Application Groups" on page 202.

Table 51. Security Rule Settings (Continued)

Field	Description
Service	Select services to limit the application(s) to specific TCP and/or UDP port numbers. You can select specific services and service groups, or one of the following: • **any**. The selected application(s) are allowed or denied on any protocol or port. Use of "any" is recommended on deny policies. • **application-default**. The selected application(s) 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. To select specific services, 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. The predefined services are: – service-http (TCP port 80,8080) – service-https (TCP port 443) • 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 205). To define new service groups, refer to "Defining Service Groups" on page 207.
Action	Click **allow** or **deny** to allow or block a new network session for traffic that matches this rule.
Profile	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 **Profile Groups** and select a profile group from the **Group** drop-down list. To define new profiles or profile groups, click **New** next to the appropriate profile or group (refer to "Defining Security Profiles" on page 164).

Table 51. Security Rule Settings (Continued)

Field	Description
Options	Specify any combination of the following options: **Log Setting** • To generate entries in the local traffic log for traffic that matches this rule, select the following options: – **Send Traffic Log at session start**. Generates a traffic log entry for the start of a session (disabled by default). – **Send Traffic Log at session end**. Generates a traffic log entry for the end of a session (enabled by default). If the session start or end entries are logged, "drop" and "deny" entries are also logged (refer to "Identifying Unknown Applications and Taking Action" on page 246). • 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 **Log Forwarding Profile** drop-down list. Note that the generation of threat log entries is determined by the security profiles. To define new log profiles, click **New** (refer to "Defining Log Forwarding Profiles" on page 185). **Schedule** 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 "Defining Schedules" on page 212). **QoS Marking** To change the Quality of Service (QoS) setting on packets matching the rule, select **IP DSCP** or **IP Precedence** 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 271. **Disable Server Response Inspection** To disable packet inspection from the server to the client, select this check box. This option may be useful under heavy server load conditions.

6. 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 greyed out and the Disable Rule option is changed to **Enable Rule**.

7. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Defining Network Address Translation Policies

For information about defining NAT policies, refer to:

- "About NAT Policies" in the next section
- "NAT Examples" on page 151
- "Defining NAT Policies" on page 152

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.
- **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.

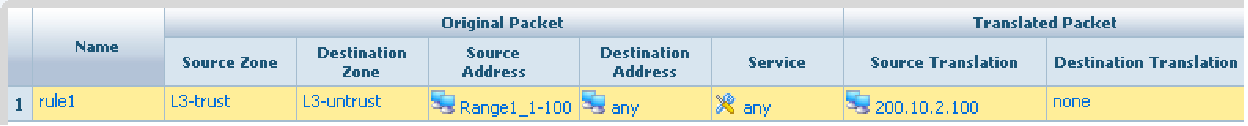
With Static IP NAT, there is a one-to-one mapping between each original address and its translated address. This can be expressed as 1-to-1 for a single mapped IP address, or M-to-M for a pool of many one-to-one, mapped IP addresses.

Table 52. NAT Types

PAN-OS NAT Type	Source Port Stays the Same	Destination Port Can Change	Mapping Type	Size of Translated Address Pool
Dynamic IP/ Port	No	No	Many-to-1 M-to-N	Up to three consecutive addresses
Dynamic IP	Yes	No	M-to-N	Up to 32 consecutive addresses
Static IP	Yes	No	1-to-1 M-to-M MIP	Unlimited
	Optional		1-to-Man VIP PAT	

NAT Examples

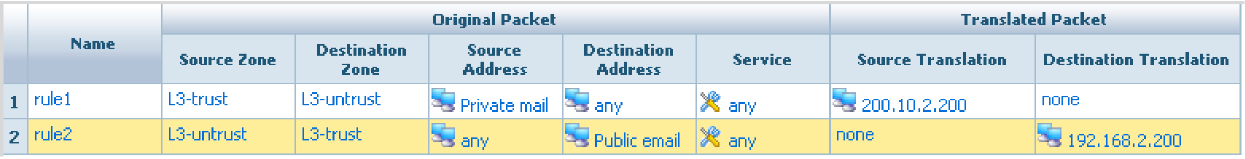
The following NAT policy rule translates a range of private source addresses (192.168.1.1 to 192.168.1.100) to a single public IP address (200.10.2.100) and a unique source port number (dynamic source translation). The rule applies only to traffic received on a Layer 3 interface in the "L3 trust" zone that is destined for an interface in the "L3 untrust" zone. Since 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.



	Name	Original Packet					Translated Packet	
		Source Zone	Destination Zone	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	rule1	L3-trust	L3-untrust	Range1_1-100	any	any	200.10.2.100	none

Figure 84. Dynamic Source Address Translation

In the following example, the first NAT rule translates the private address of an internal mail server (192.168.2.200) to a static public IP address (200.10.2.200). The source port number is not changed. 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.



	Name	Original Packet					Translated Packet	
		Source Zone	Destination Zone	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	rule1	L3-trust	L3-untrust	Private mail	any	any	200.10.2.200	none
2	rule2	L3-untrust	L3-trust	any	Public email	any	none	192.168.2.200

Figure 85. 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 NAT Policies

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.

To define NAT policies:

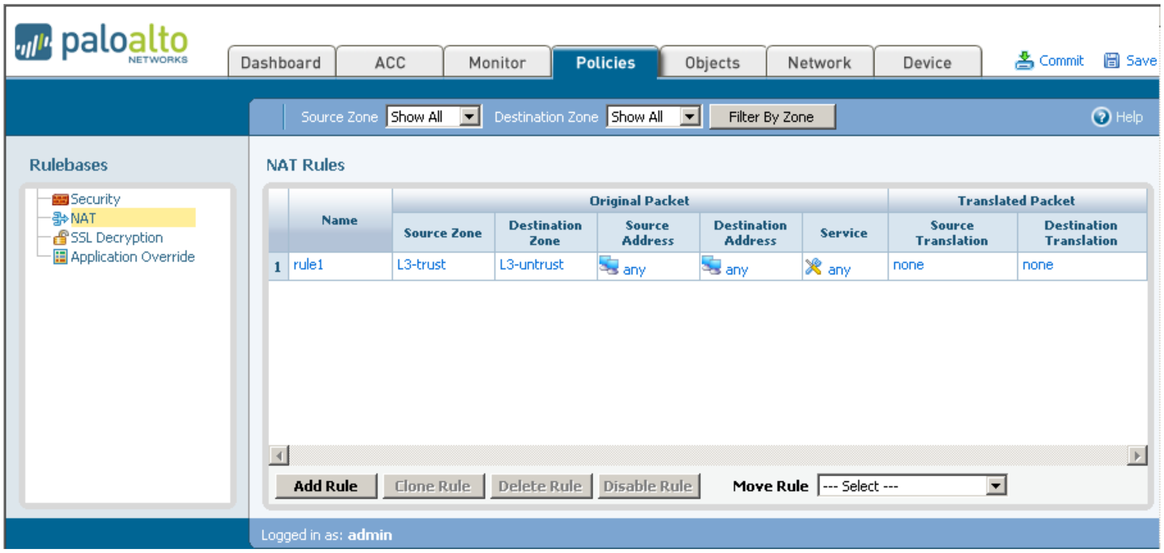
1. Under the **Policies** tab, click **NAT** to open the NAT Rules page.

2. 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.**

3. 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 highest rule number. The source and destination zones must be for Layer 3 interfaces. To define new Layer 3 zones, refer to "Defining Security Zones" on page 116.

   – 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.



Source Zone: Show All
Destination Zone: Show All

NAT Rules

	Name	Original Packet					Translated Packet	
		Source Zone	Destination Zone	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	rule1	L3-trust	L3-untrust	any	any	any	none	none

Move Rule: --- Select ---

Logged in as: admin

Figure 86. NAT Rules Page

4. To change a field in a new or existing rule, click the current field value, specify the appropriate information, as described below, and click **OK**.

Table 53. NAT Rule Settings

Field	Description
Name	Change the default rule name and/or enter a rule description. If you add a rule description, a 💬 is added next to the rule name. By default, rules are named “rule<n>”, 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.
Source Zone Destination Zone	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 116. 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.
Source Address Destination Address	Specify a combination of source and destination addresses for which the source or destination address must be translated. Select **any**, a predefined address or address range 🖧, or click **Additional Address** and enter an IP address, with or without a network mask. The general format is: <ip_address>/<mask> To add new addresses that can be used in this or other policies, click **New Address** (refer to “Defining Addresses” on page 193).
Service	Specify the services for which the source or destination address is translated. Select **any** or a service 🛠 or service group 🛠. To define new services, click **New Service** (refer to “Defining Services” on page 205). To define new service groups, refer to “Defining Service Groups” on page 207.
Source Translation	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: • **Dynamic IP/port**. 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. The address range is limited to three consecutive addresses. Port numbers are managed internally. • **Dynamic IP**. The next available address in the specified range is used, but the port number is unchanged. The address range is limited to 32 consecutive addresses. • **Static IP**. 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.
Destination Translation	Enter an IP address and 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.

5. 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 “Defining Virtual Routers” on page 122).

6. 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 greyed out and the Disable Rule option is changed to Enable Rule.

7. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Defining 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.

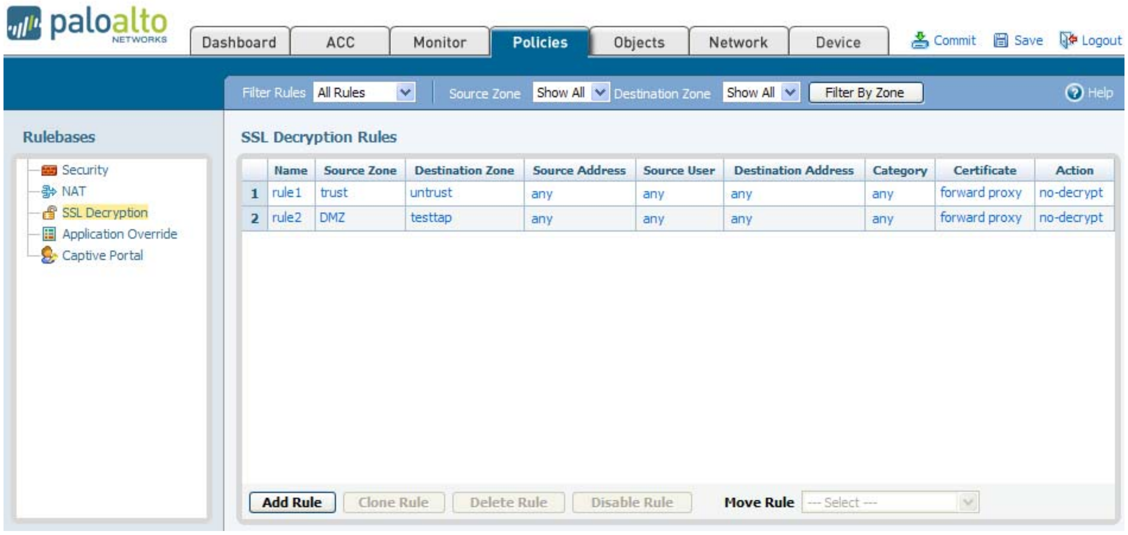
You can configure the firewall to decrypt SSL traffic for visibility, control, and granular security. App-ID and the antivirus, vulnerability, anti-spyware, URL filtering, and file-blocking profiles are applied to decrypted traffic before it is re-encrypted as traffic exits the device. End-to-end SSL 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.

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.*

To define SSL decryption policies:

1. Under the **Policies** tab, click **SSL Decryption** to open the SSL Decryption Rules page.



Filter Rules: All Rules · Source Zone: Show All · Destination Zone: Show All · Move Rule: --- Select ---

SSL Decryption Rules

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Category	Certificate	Action
1	rule1	trust	untrust	any	any	any	any	forward proxy	no-decrypt
2	rule2	DMZ	testtap	any	any	any	any	forward proxy	no-decrypt

Figure 87. SSL Decryption Rules Page

2. 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**.

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

Note: *Shared polices pushed from Panorama are shown in green and cannot be edited at the device level.*

4. 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 highest rule number. The source and destination zones must be for the same interface types (Layer 2, Layer 3, or virtual wire). To define new zones, refer to "Defining Security Zones" on page 116.

   – 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.

5. To change a field in a new or existing rule, click the current field value, specify the appropriate information, as described below, and click **OK**.

Table 54. SSL Decryption Rule Settings

Field	Description
Name	Change the default rule name and/or enter a rule description. If you add a rule description, a 💬 is added next to the rule name. By default, rules are named "rule<n>", 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.
Source Zone Destination Zone	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 116.
Source Address Destination Address	Select the source and destination addresses for which the SSL traffic can be decrypted. 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_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 disable all 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 this or other policies, click **New Address** (refer to "Defining Addresses" on page 193). To define new address groups, refer to "Defining Address Groups" on page 195.
Source User	Select the source users or groups of users subject to this policy: • 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 set up user identification, refer to "Configuring the User Identification Agent" on page 53.

Table 54. SSL Decryption Rule Settings (Continued)

Field	Description
Category	Choose **select** from the drop-down list, and select the check box next to the appropriate categories in the **Available** column, and click **Add**. You can also enter a few characters in the **Search** field to list all categories 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**.
Certificate	Select the certificate to apply to this rule. For SSL forward inspection, select **forward proxy**. For SSL inbound inspection, select one of the uploaded certificates.
Action	Select **decrypt** or **no-decrypt** for traffic to the selected URL categories.

6. 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 greyed out and the Disable Rule option is changed to Enable Rule.

7. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

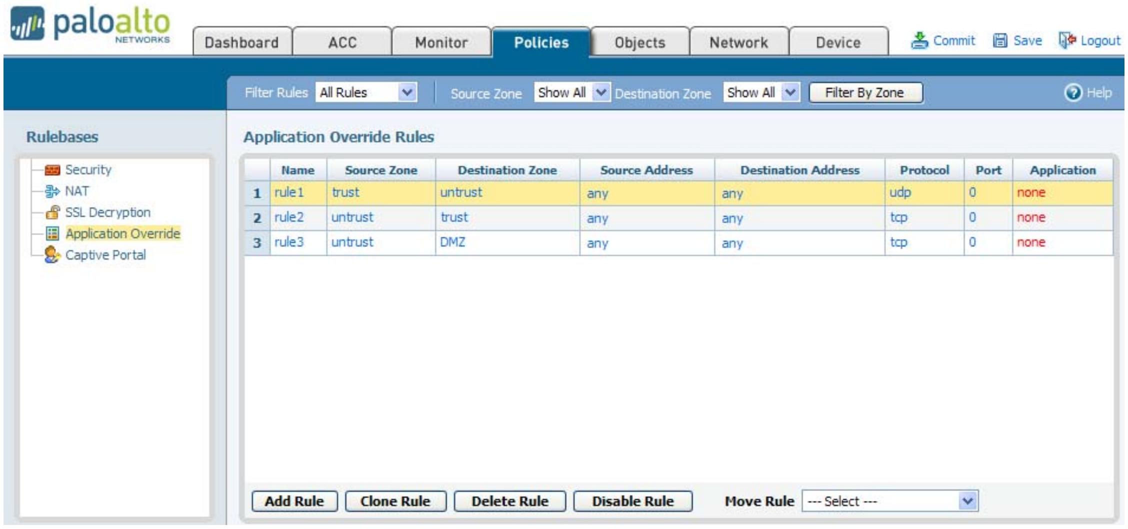
Defining Application Override Policies

To change how the firewall classifies network traffic into applications, you can specify application override policies. For example, if some of your network applications use nonstandard port numbers, you can specify application override rules to ensure that traffic to those ports are classified correctly. If you have network applications that are classified as “unknown,” you can create new application definitions for them (refer to “Defining Applications” on page 196).

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.

To define application override policies:

1. Under the **Policies** tab, click **Application Override** to open the Application Override Rules page.



Application Override Rules

	Name	Source Zone	Destination Zone	Source Address	Destination Address	Protocol	Port	Application
1	rule1	trust	untrust	any	any	udp	0	none
2	rule2	untrust	trust	any	any	tcp	0	none
3	rule3	untrust	DMZ	any	any	tcp	0	none

Figure 88. Application Override Rules Page

2. 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**.

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

Note: *Shared polices pushed from Panorama are shown in green and cannot be edited at the device level.*

4. 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 highest 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 116.
   - 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.
5. To change a field in a new or existing rule, click the current field value, specify the appropriate information, as described below, and click **OK**.

Table 55. Application Override Rule Settings

Field	Description
Name	Change the default rule name and/or enter a rule description. If you add a rule description, a 💬 is added next to the rule name. By default, rules are named “rule<n>”, 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.
Source Zone Destination Zone	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 116.
Source Address Destination Address	Specify a combination of source and destination 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_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 Addresses” on page 193). To define new address groups, refer to “Defining Address Groups” on page 195.
Protocol	Select the protocol for which the application can be overridden.
Port	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.

Table 55. Application Override Rule Settings (Continued)

Field	Description
Application	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 196).

6. 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 greyed out and the Disable Rule option is changed to Enable Rule.

7. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

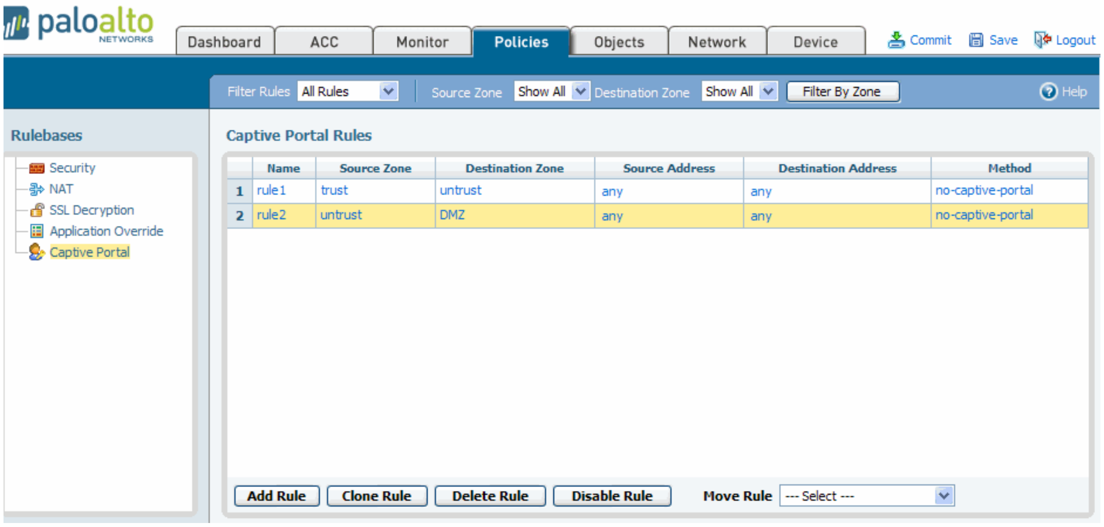
Defining Captive Portal Policies

You can set up and customize a captive portal to direct user authentication by way of a RADIUS server authentication. Captive portal is used in conjunction with the User Identification Agent to extend user identification functions beyond the Active Directory domain. Users are directed to the portal and authenticated by way of a RADIUS server.

To define captive portal policies:

1. Enable captive portal and configure RADIUS authentication on the User Identification page, as described in "Defining Virtual Systems" on page 68.

2. Under the **Policies** tab, click **Captive Portal** to open the Captive Portal Rules page.



Filter Rules: All Rules   Source Zone: Show All   Destination Zone: Show All

Captive Portal Rules

	Name	Source Zone	Destination Zone	Source Address	Destination Address	Method
1	rule1	trust	untrust	any	any	no-captive-portal
2	rule2	untrust	DMZ	any	any	no-captive-portal

Figure 89. Captive Portal Rules Page

3. 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**.

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

> ***Note:*** *Shared polices pushed from Panorama are shown in green and cannot be edited at the device level.*

5. To add a new 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. The source and destination zones must be for the same interface types (Layer 2, Layer 3, or virtual wire). Refer to “Defining Security Zones” on page 116.

   – 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.

6. To change a field in a new or existing rule, click the current field value, specify the appropriate information, as described below, and click **OK**.

Table 56. Captive Portal Rule Settings

Field	Description
Name	Change the default rule name and optionally enter a rule description (maximum 255 characters). If you add a rule description, a 💬 is added next to the rule name. By default, rules are named “rule<n>”, 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.
Source Zone Destination Zone	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 116.

Table 56. Captive Portal Rule Settings (Continued)

Field	Description
Source Address Destination Address	Select the source and destination addresses. 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_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 apply to all addresses except those that are entered, click **Negate**. To add new addresses that can be used in this or other policies, click **New Address** (refer to “Defining Addresses” on page 193). To define new address groups, refer to “Defining Address Groups” on page 195.
Method	Choose whether to use a captive portal for this rule.

7. 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 greyed out and the Disable Rule option is changed to Enable Rule.

8. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

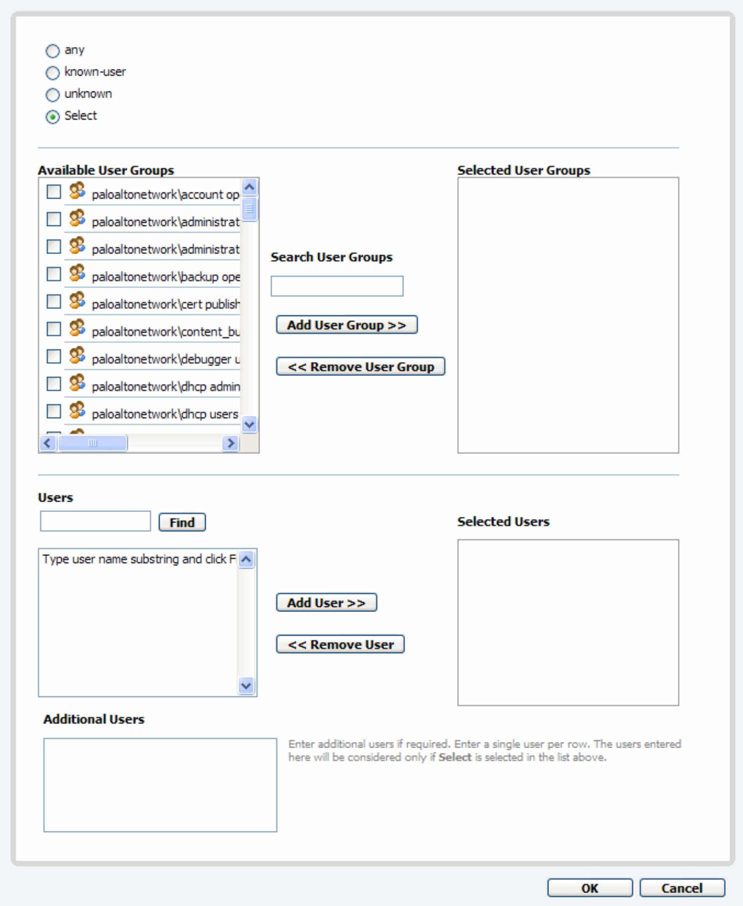
Specifying Users and Applications for Policies

You can restrict security policies (“Defining Security Policies” on page 144) and SSL decryption policies (“Defining SSL Decryption Policies” on page 154) to selected users or applications by clicking the user or application link on the Security Rules or SSL Decryption Policy page. For information on restricting rules by application, refer to “Defining Applications” on page 196.

To restrict a policy to selected users:

1. Under the **Policies** tab, click **Security** to open the Security Rules page.
2. Click an underlined user link to open the selection window.

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



○ any
○ known-user
○ unknown
● Select

Available User Groups

□ paloaltonetwork\account op
□ paloaltonetwork\administrat
□ paloaltonetwork\administrat
□ paloaltonetwork\backup ope
□ paloaltonetwork\cert publish
□ paloaltonetwork\content_bu
□ paloaltonetwork\debugger u
□ paloaltonetwork\dhcp admin
□ paloaltonetwork\dhcp users

Search User Groups

Selected User Groups

Users

Type user name substring and click F

Selected Users

Additional Users

Enter additional users if required. Enter a single user per row. The users entered here will be considered only if **Select** is selected in the list above.

Figure 90. Selecting Users for Security and SSL Decryption Rules

3. 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.
4. 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**.
5. 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.
6. Click **OK** to save the selections and update the security or SSL decryption rule.

Defining Security Profiles

Security profiles can be specified in each security policy to defend against known network threats, prevent access to specified web sites, and specify logging criteria. For information about defining security profiles, refer to:

- "Defining Antivirus Profiles" in the next section
- "Defining Anti-Spyware Profiles" on page 168
- "Defining Vulnerability Protection Profiles" on page 174
- "Defining URL Filtering Profiles" on page 178
- "Defining File Blocking Profiles" on page 182
- "Defining Log Forwarding Profiles" on page 185
- "Defining Data Filtering Profiles" on page 188
- "Defining Security Profile Groups" on page 191

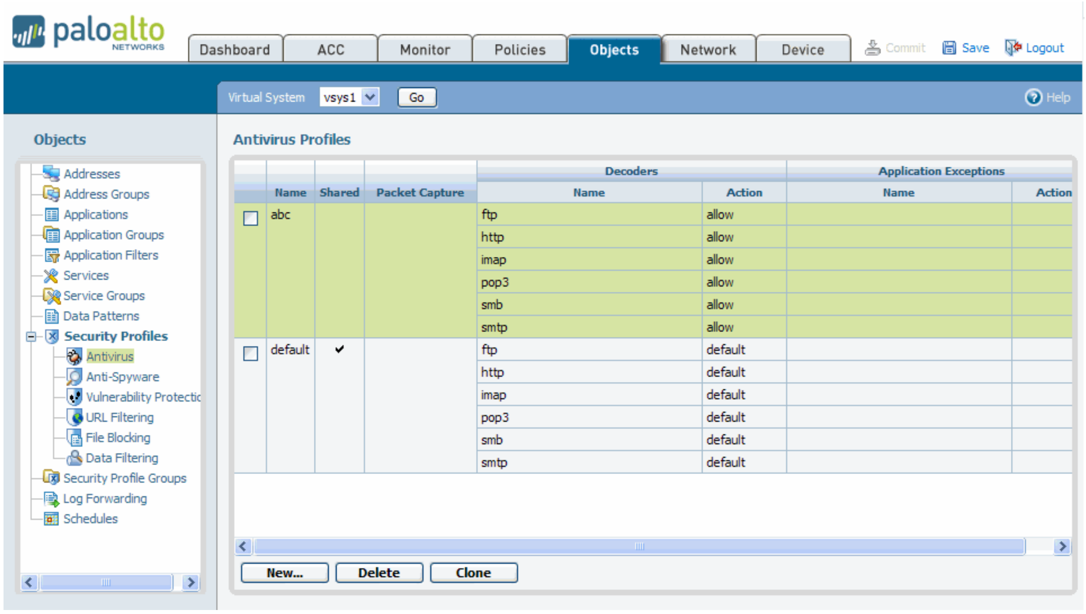
Defining Antivirus Profiles

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 applications for viruses, generates alerts for imap, pop3, and smtp, 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 apply antivirus profiles to security policies, refer to "Defining Security Policies" on page 144.

To define antivirus profiles:

1. Under the **Objects** tab, click **Security Profiles > Antivirus** to open the Antivirus Profiles page.

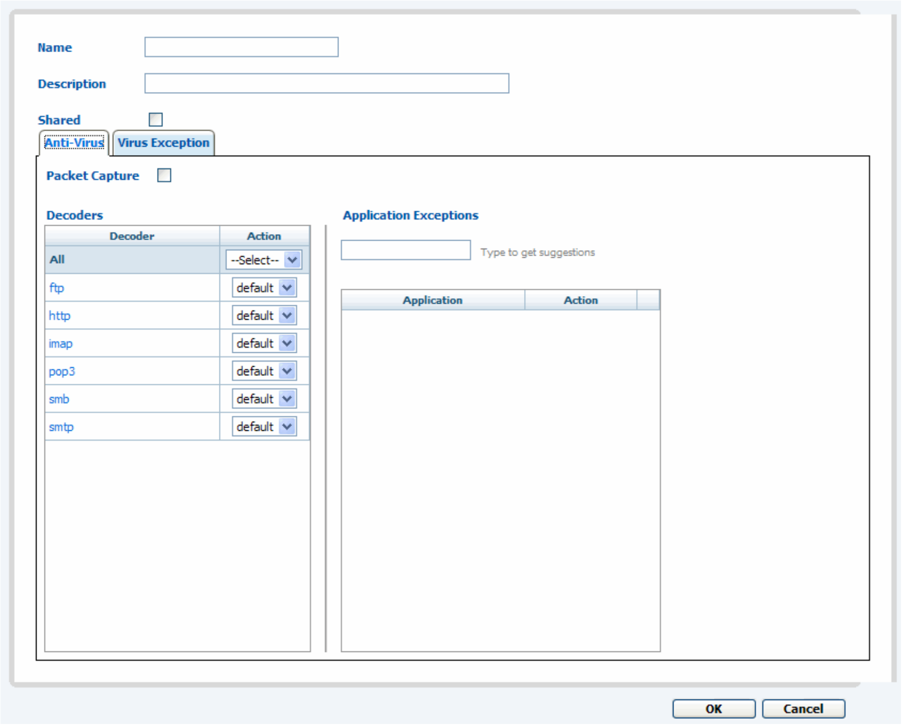


				Decoders		Application Exceptions	
	Name	Shared	Packet Capture	Name	Action	Name	Action
□	abc			ftp	allow		
				http	allow		
				imap	allow		
				pop3	allow		
				smb	allow		
				smtp	allow		
□	default	✓		ftp	default		
				http	default		
				imap	default		
				pop3	default		
				smb	default		
				smtp	default		

Figure 91. Antivirus Profiles Page

2. To add a new profile:

   a. Click **New** to open the New Antivirus Profile page.



Decoder	Action
All	--Select--
ftp	default
http	default
imap	default
pop3	default
smb	default
smtp	default

Figure 92. New Antivirus Profiles Page

   b. Specify the following information on the **Anti-Virus** tab.

Table 57. New Antivirus Profile Settings

Field	Description
Name	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.
Description	Enter an optional description.
Packet Capture	Select the check box if you want to capture identified packets.
Decoders and Actions	For each type of traffic that you want to inspect for viruses, select an action from the drop-down list. • **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. • **Block** — Drops the application traffic. • **Allow** — Permits the application traffic.

Table 57. New Antivirus Profile Settings (Continued)

Field	Description
Applications Exceptions and Actions	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. **Block** is the action for the HTTP decoder, and **Allow** 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: • **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. • **Block** — Drops the application traffic. • **Allow** — Permits the application traffic.

c. Use the **Virus Exception** 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 **Add**. Threat IDs are presented as part of the threat log information. Refer to “Viewing the Logs” on page 229.

d. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

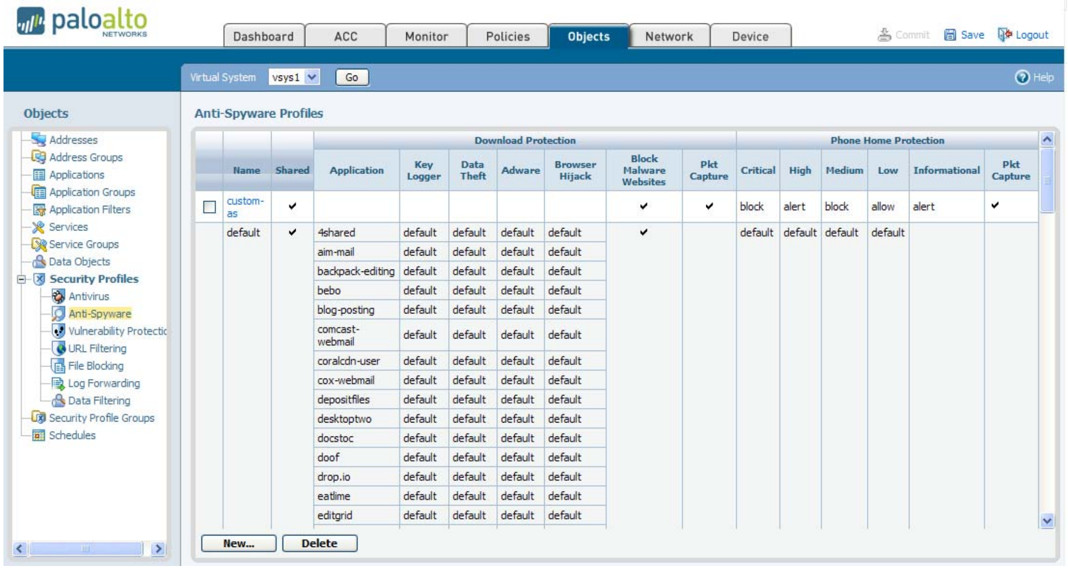
Defining Anti-Spyware Profiles

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 informational.

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 apply anti-spyware profiles to security policies, refer to “Defining Security Policies” on page 144.

To define anti-spyware profiles:

1. Under the **Objects** tab, click **Security Profiles > Anti-Spyware** to open the Anti-Spyware Profiles page.



Anti-Spyware Profiles

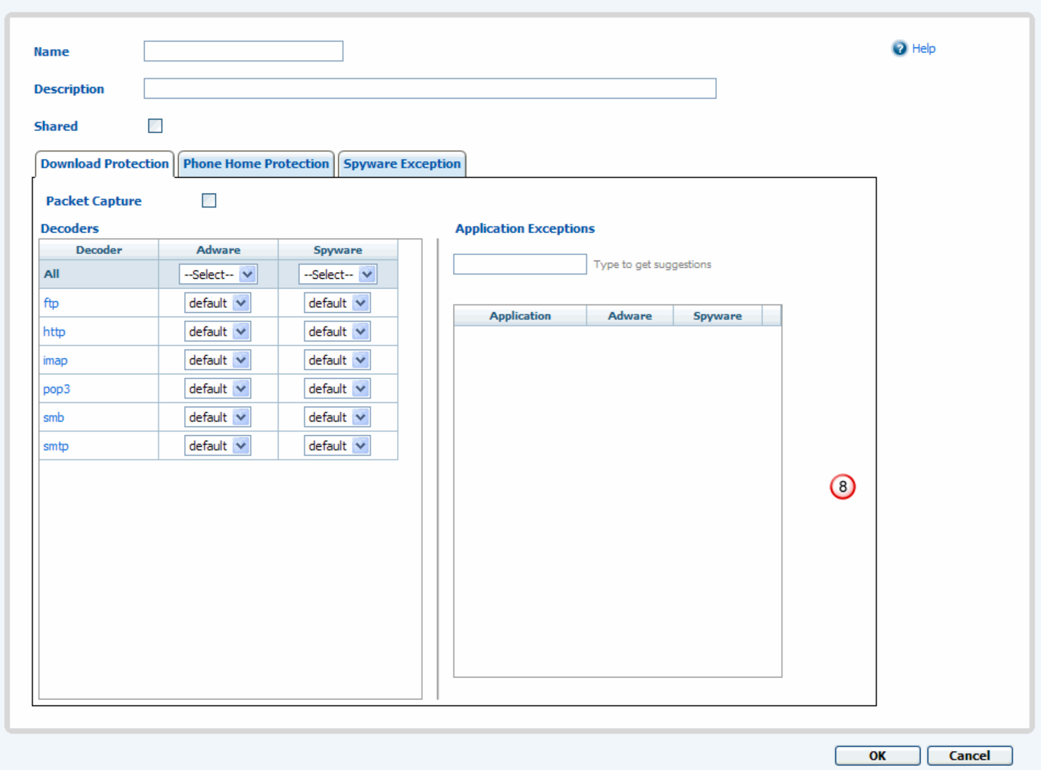
			Download Protection							Phone Home Protection					
	Name	Shared	Application	Key Logger	Data Theft	Adware	Browser Hijack	Block Malware Websites	Pkt Capture	Critical	High	Medium	Low	Informational	Pkt Capture
□	custom-as	✓						✓	✓	block	alert	block	allow	alert	✓
	default	✓	4shared	default	default	default	default	✓		default	default	default	default		
			aim-mail	default	default	default	default								
			backpack-editing	default	default	default	default								
			bebo	default	default	default	default								
			blog-posting	default	default	default	default								
			comcast-webmail	default	default	default	default								
			coralcdn-user	default	default	default	default								
			cox-webmail	default	default	default	default								
			depositfiles	default	default	default	default								
			desktoptwo	default	default	default	default								
			docstoc	default	default	default	default								
			doof	default	default	default	default								
			drop.io	default	default	default	default								
			eatlime	default	default	default	default								
			editgrid	default	default	default	default								

Figure 93. Anti-Spyware Profiles Page

2. To add a new profile:

   a. Click **New** to open the New Anti-Spyware Profile page.

      The page opens to show the anti-spyware **Download Protection** tab.



Name

Description

Shared □

Packet Capture □

Decoders

Decoder	Adware	Spyware
All	--Select--	--Select--
ftp	default	default
http	default	default
imap	default	default
pop3	default	default
smb	default	default
smtp	default	default

Application Exceptions

Type to get suggestions

Application	Adware	Spyware

Figure 94. New Anti-Spyware Profile Page - Download Protection Tab

   b. Specify the following information at the top of the page.

Table 58. New Anti-Spyware Profile Settings

Field	Description
Name	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.
Description	Enter a text description of the profile.

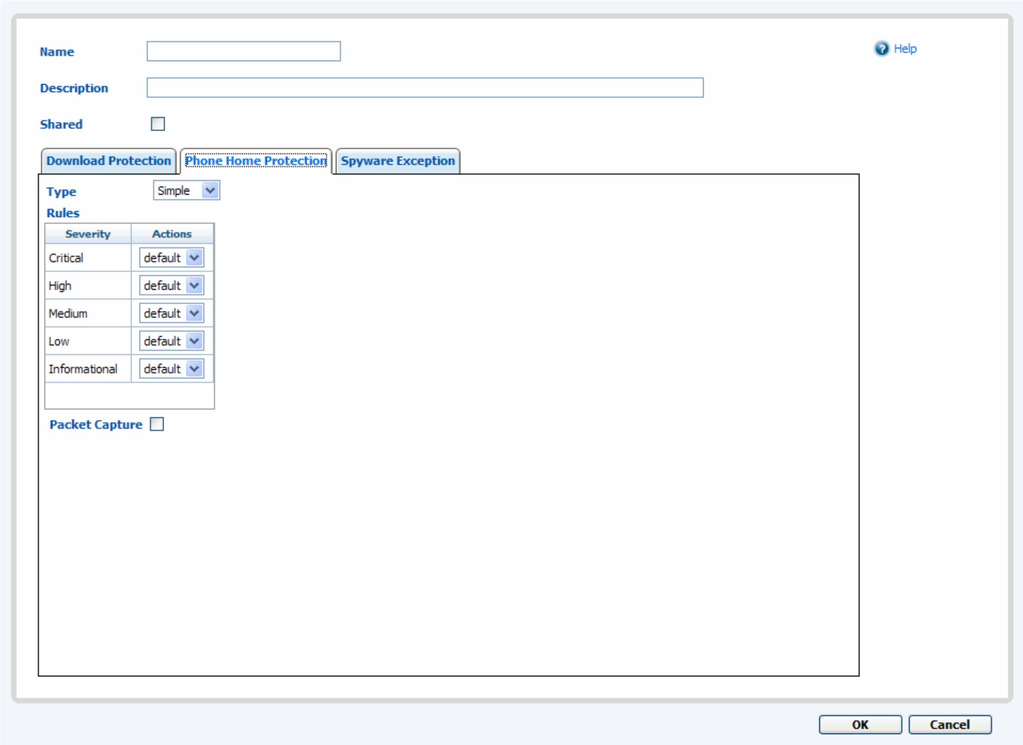
c. Specify the following information on the **Download Protection** tab.

Table 59. New Anti-Spyware Profile Settings - Download Protection

Field	Description
Packet Capture	Select the check box capture spyware packets.
Decoders and Actions	For each type of traffic that you want to inspect for viruses, select an action from the drop-down list. • **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. • **Block** — Drops the application traffic. • **Allow** — Permits the application traffic.
Applications Exceptions and Actions	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. **Block** is the action for the HTTP decoder, and **Allow** 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: • **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. • **Block** — Drops the application traffic. • **Allow** — Permits the application traffic.

d. Click the **Phone Home Protection** tab.

e. 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 severity level of spyware threats.



Name

Description

Shared □

Type: Simple

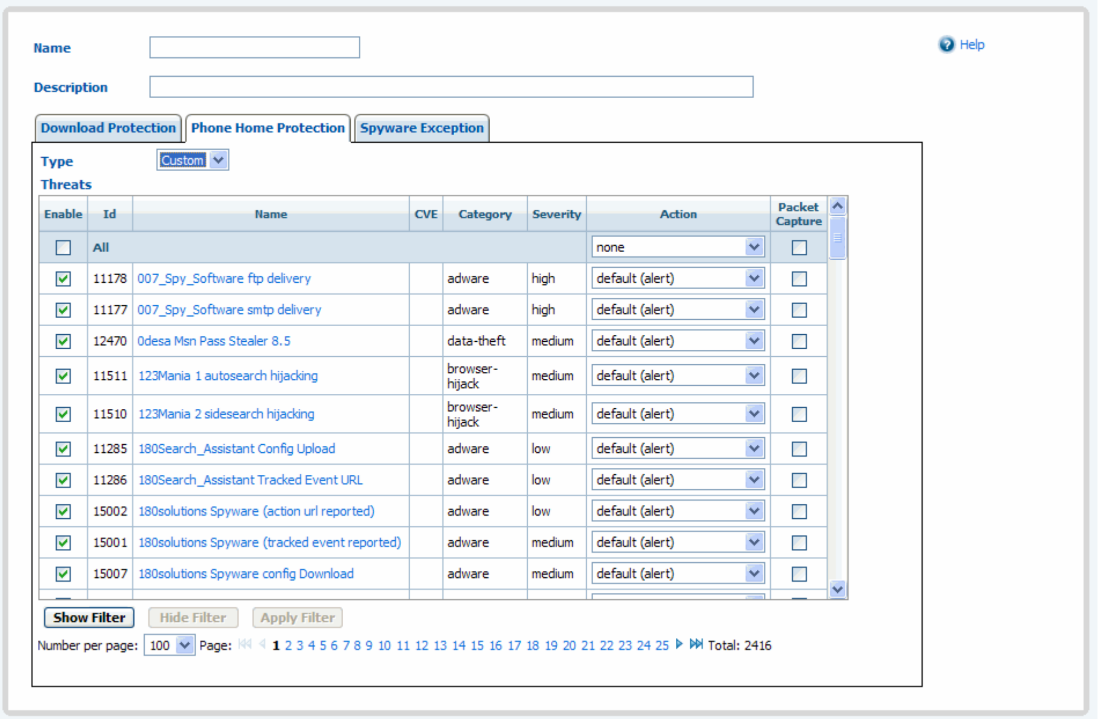
Rules

Severity	Actions
Critical	default
High	default
Medium	default
Low	default
Informational	default

Packet Capture □

Figure 95. Anti-Spyware Phone Home Protection - Simple

f. To use threat-based protection, select **Custom** from the **Type** drop-down list. The scroll bar at the right of the list allows you to display additional threats.



Name

Description

Type: Custom

Threats

Enable	Id	Name	CVE	Category	Severity	Action	Packet Capture
□	All					none	□
☑	11178	007_Spy_Software ftp delivery		adware	high	default (alert)	□
☑	11177	007_Spy_Software smtp delivery		adware	high	default (alert)	□
☑	12470	0desa Msn Pass Stealer 8.5		data-theft	medium	default (alert)	□
☑	11511	123Mania 1 autosearch hijacking		browser-hijack	medium	default (alert)	□
☑	11510	123Mania 2 sidesearch hijacking		browser-hijack	medium	default (alert)	□
☑	11285	180Search_Assistant Config Upload		adware	low	default (alert)	□
☑	11286	180Search_Assistant Tracked Event URL		adware	low	default (alert)	□
☑	15002	180solutions Spyware (action url reported)		adware	low	default (alert)	□
☑	15001	180solutions Spyware (tracked event reported)		adware	medium	default (alert)	□
☑	15007	180solutions Spyware config Download		adware	medium	default (alert)	□

Number per page: 100 Page: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 Total: 2416

Figure 96. Anti-Spyware Home Protection Tab - Custom

g. Specify the information in the following table.

Table 60. New Anti-Spyware Profile Settings

Field	Description
Enable	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.
Actions	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. The following actions are available. • **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.
Packet Capture	Select the check box to collect the traffic packets from the threat.

h. To apply filters to the list, click **Show Filter** to show the filter area near the top of the table. Enter the values and conditions and click **Apply filter**. Click **Hide Filter** to hide the filter settings.

i. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

j. Use the **Spyware Exception** tab if you want the system to ignore any specified threats. Exceptions that are already specified are listed. Add additional threats by entering the threat ID and clicking **Add**. Threat IDs are presented as part of the threat log information. Refer to “Viewing the Logs” on page 229.

3. Perform any of the following additional tasks:

a. To change an entry, click the link for the entry, specify changes, and click **OK**.

b. To delete entries, select their check boxes and click **Delete**.

c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

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

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

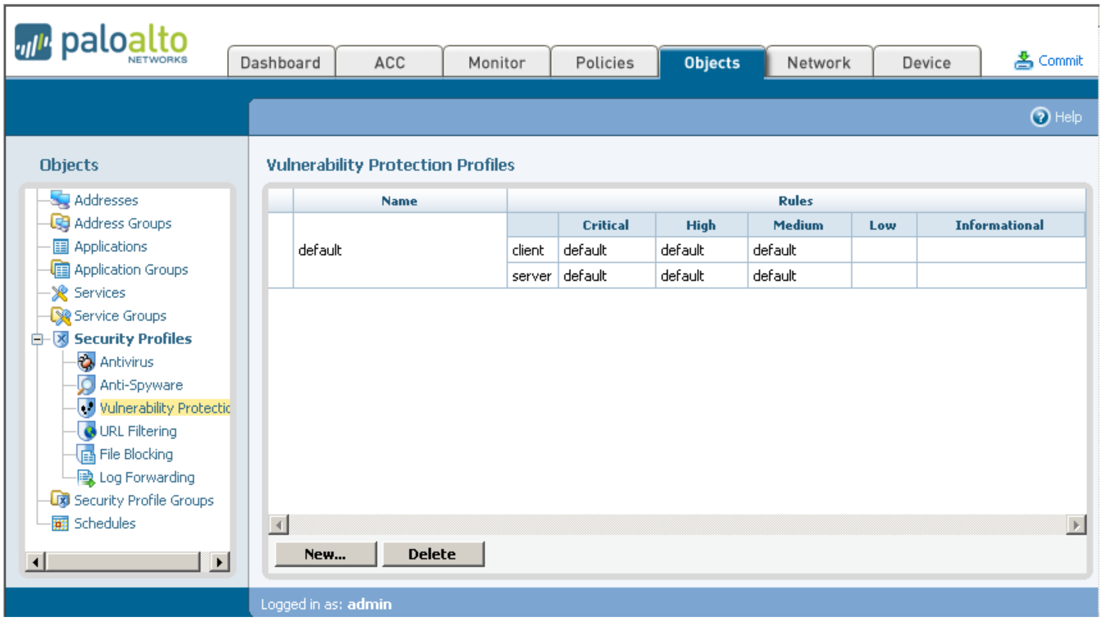
Defining Vulnerability Protection Profiles

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 “Defining Security Policies” on page 144.

To define vulnerability protection profiles:

1. Under the **Objects** tab, click **Security Profiles > Vulnerability Protection** to open the Vulnerability Protection Profiles page.



Name	Rules					
		Critical	High	Medium	Low	Informational
default	client	default	default	default		
	server	default	default	default		

Figure 97. Vulnerability Protection Profiles Page

2. To add a new profile:

   a. Click **New** to open the New Vulnerability Protection Profile page.

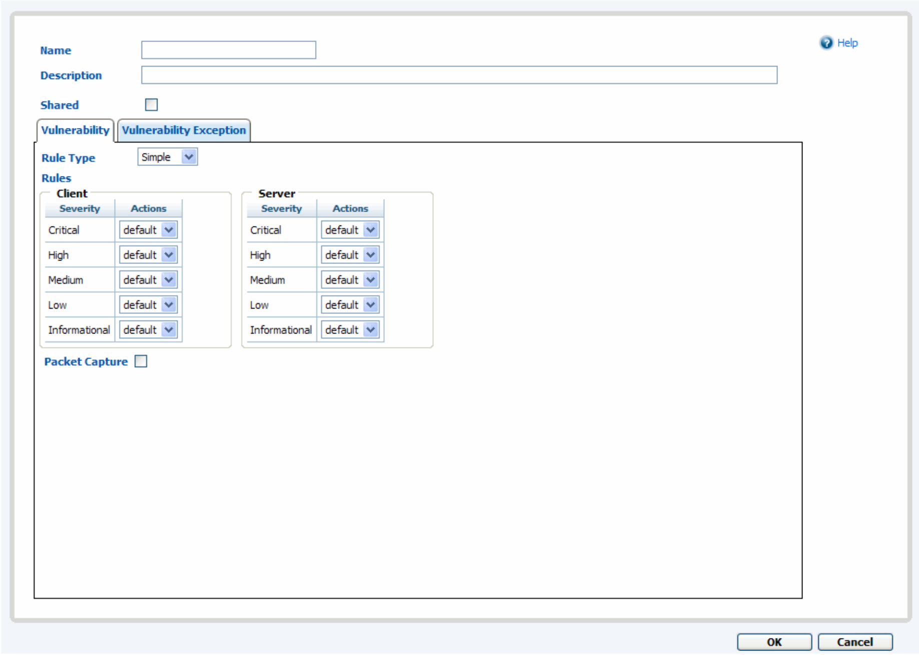
   b. Specify the following information at the top of the page.

Table 61. New Vulnerability Profile Settings

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of vulnerability profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Description	Enter a text description of the profile.

c. 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 severity level for client and server.

d. Select **Packet Capture** to collect the traffic packets from the threat.



Name

Description

Shared □

Rule Type: Simple

Rules

Client

Severity	Actions
Critical	default
High	default
Medium	default
Low	default
Informational	default

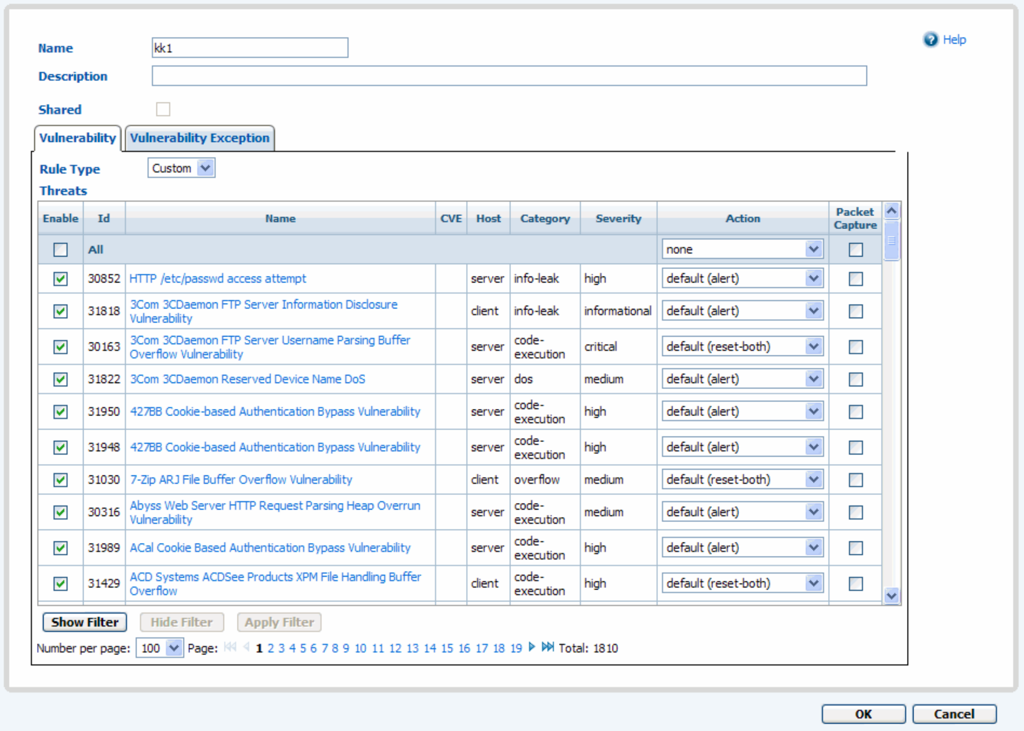
Server

Severity	Actions
Critical	default
High	default
Medium	default
Low	default
Informational	default

Packet Capture □

Figure 98. New Vulnerability Protection Profile Page - Simple

e. To use threat-based protection, select **Custom** from the **Type** drop-down list and specify the information in the following table. Use the scroll bar at the right of the list to display additional threats.



Name: kk1

Description:

Shared ☐

Rule Type: Custom

Threats

Enable	Id	Name	CVE	Host	Category	Severity	Action	Packet Capture
☐	All						none	☐
☑	30852	HTTP /etc/passwd access attempt		server	info-leak	high	default (alert)	☐
☑	31818	3Com 3CDaemon FTP Server Information Disclosure Vulnerability		client	info-leak	informational	default (alert)	☐
☑	30163	3Com 3CDaemon FTP Server Username Parsing Buffer Overflow Vulnerability		server	code-execution	critical	default (reset-both)	☐
☑	31822	3Com 3CDaemon Reserved Device Name DoS		server	dos	medium	default (alert)	☐
☑	31950	427BB Cookie-based Authentication Bypass Vulnerability		server	code-execution	high	default (alert)	☐
☑	31948	427BB Cookie-based Authentication Bypass Vulnerability		server	code-execution	high	default (alert)	☐
☑	31030	7-Zip ARJ File Buffer Overflow Vulnerability		client	overflow	medium	default (reset-both)	☐
☑	30316	Abyss Web Server HTTP Request Parsing Heap Overrun Vulnerability		server	code-execution	medium	default (alert)	☐
☑	31989	ACal Cookie Based Authentication Bypass Vulnerability		server	code-execution	high	default (alert)	☐
☑	31429	ACD Systems ACDSee Products XPM File Handling Buffer Overflow		client	code-execution	high	default (reset-both)	☐

Number per page: 100 Page: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 Total: 1810

Figure 99. New Vulnerability Protection Profile Page - Custom

Table 62. New Vulnerability Protection Profile Settings

Field	Description
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.* ***Note:*** *The* ***CVE*** *column shows identifiers for common vulnerabilities and exposures (CVE). These unique, common identifiers are for publicly known information security vulnerabilities.* The following actions are available. • **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 packet from continuing past the firewall. • **Reset-both**— Resets the client and server. • **Reset-client**— Resets the client. • **Reset-server**— Resets the server.

f. Select **Packet Capture** to collect the traffic packets from the threat.

g. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

3. Use the **Vulnerability Exception** tab if you want the system to ignore any specified threats. Exceptions that are already specified are listed. You can add additional threats by entering the threat ID and clicking **Add**. Threat IDs are presented as part of the threat log information. Refer to “Viewing the Logs” on page 229.

4. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

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

5. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

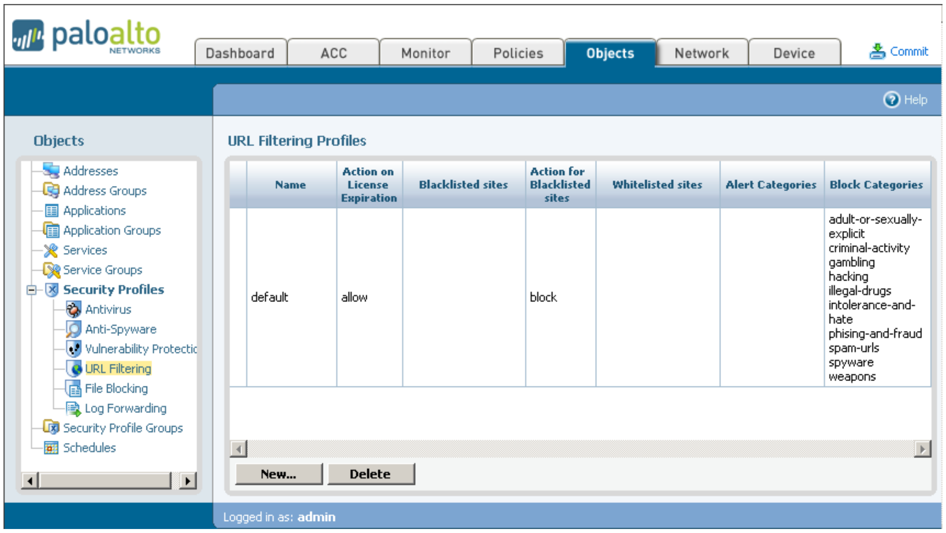
Defining URL Filtering Profiles

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 "Defining Security Policies" on page 144.

To define URL filtering profiles:

1. Under the **Objects** tab, click **Security Profiles > URL Filtering** to open the URL Filtering Profiles page.



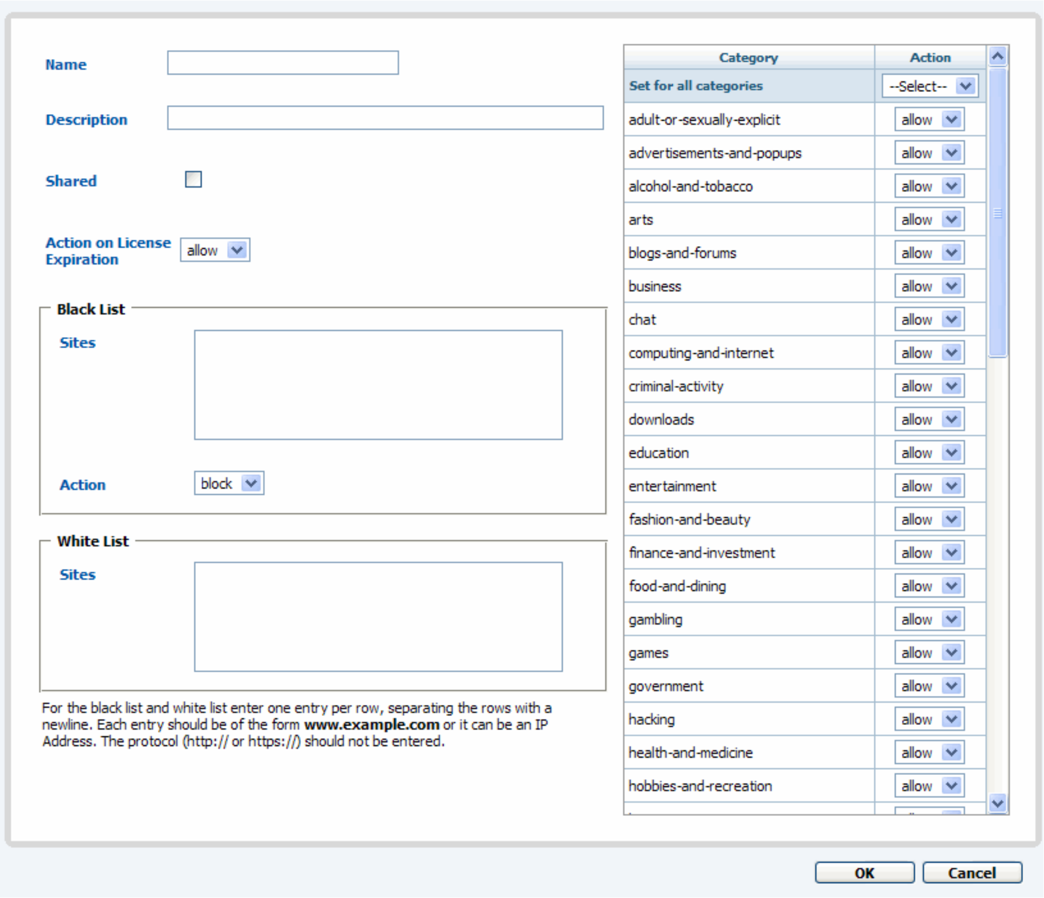
URL Filtering Profiles

Name	Action on License Expiration	Blacklisted sites	Action for Blacklisted sites	Whitelisted sites	Alert Categories	Block Categories
default	allow		block			adult-or-sexually-explicit criminal-activity gambling hacking illegal-drugs intolerance-and-hate phising-and-fraud spam-urls spyware weapons

Figure 100. URL Filtering Profiles Page

2. To add a new profile:

   a. Click **New** to open the New URL Filtering Profile page.



Name

Description

Shared □

Action on License Expiration: allow

Black List

Sites

Action: block

White List

Sites

For the black list and white list enter one entry per row, separating the rows with a newline. Each entry should be of the form **www.example.com** or it can be an IP Address. The protocol (http:// or https://) should not be entered.

Category	Action
Set for all categories	--Select--
adult-or-sexually-explicit	allow
advertisements-and-popups	allow
alcohol-and-tobacco	allow
arts	allow
blogs-and-forums	allow
business	allow
chat	allow
computing-and-internet	allow
criminal-activity	allow
downloads	allow
education	allow
entertainment	allow
fashion-and-beauty	allow
finance-and-investment	allow
food-and-dining	allow
gambling	allow
games	allow
government	allow
hacking	allow
health-and-medicine	allow
hobbies-and-recreation	allow

Figure 101. New URL Filtering Profile Page

b. Specify the following information.

Table 63. New URL Filtering Profile Settings

Field	Description
Name	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.
Description	Enter a description of the profile.
Shared	If the device is in Multiple Virtual System Mode, select this check box to allow the profile to be shared by all virtual systems.
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. The cache expiration option on the Setup page determines how long entries returned from BrightCloud remain in the cache. Refer to “Defining the Host Name and Network Settings” on page 40. 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.”
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:*** *The wildcard character “*” can represent any character. For example, *.site.com matches any URL for the web site site.com.* *A “/*” is implied after each URL so that all web pages with the same base URL are included.*

Table 63. New URL Filtering Profile Settings (Continued)

Field	Description
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. • **Alert** — Allow the user to access to the web site, but add an alert to the threat log.

c. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

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

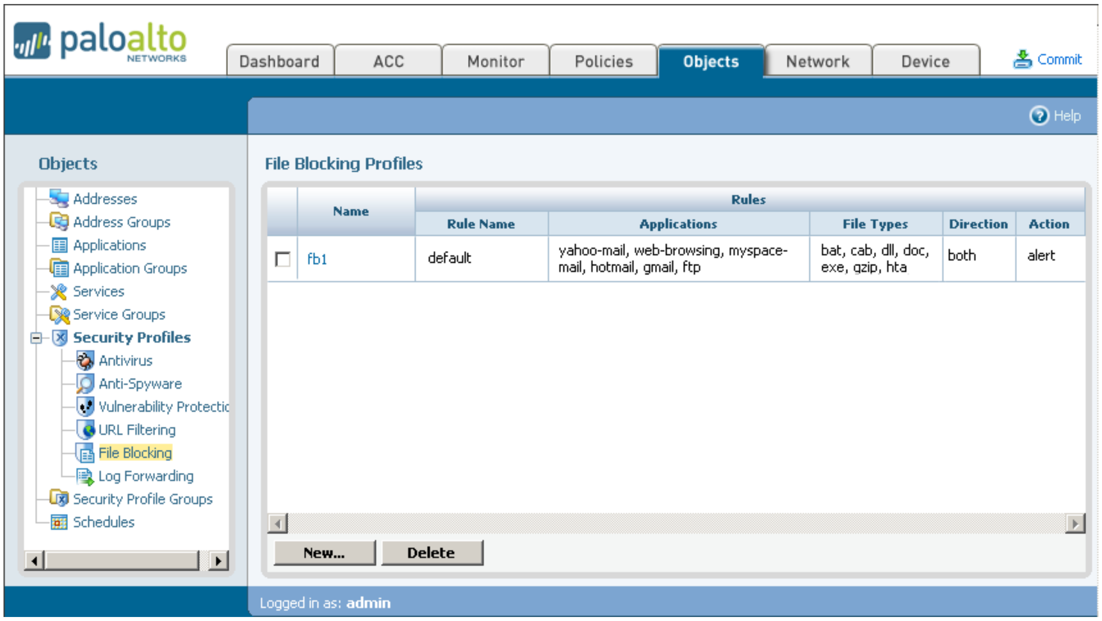
4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Defining File Blocking Profiles

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 “Defining Security Policies” on page 144.

To define file blocking profiles:

1. Under the **Objects** tab, click **Security Profiles > File Blocking** to open the File Blocking Profiles page.



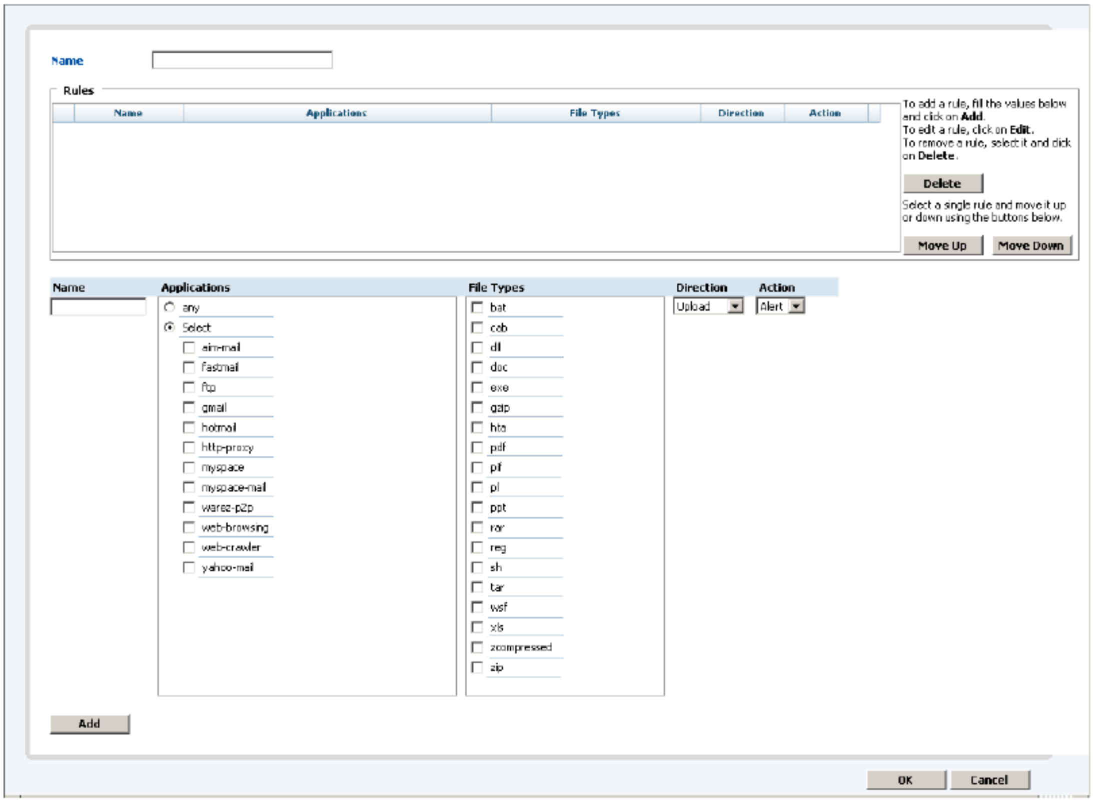
File Blocking Profiles

	Name	Rules				
		Rule Name	Applications	File Types	Direction	Action
□	fb1	default	yahoo-mail, web-browsing, myspace-mail, hotmail, gmail, ftp	bat, cab, dll, doc, exe, gzip, hta	both	alert

Figure 102. File Blocking Profiles Page

2. To add a new profile:

   a. Click **New** to open the New File Blocking Profile page.



To add a rule, fill the values below and click on **Add**.
To edit a rule, click on **Edit**.
To remove a rule, select it and click on **Delete**.

Select a single rule and move it up or down using the buttons below.

Applications: ○ any ● Select

Direction: Upload

Action: Alert

Figure 103. New File Blocking Profile Page

b. Specify the following information.

Table 64. New File Blocking Profile Settings

Field	Description
Name	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.
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**.

c. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

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

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

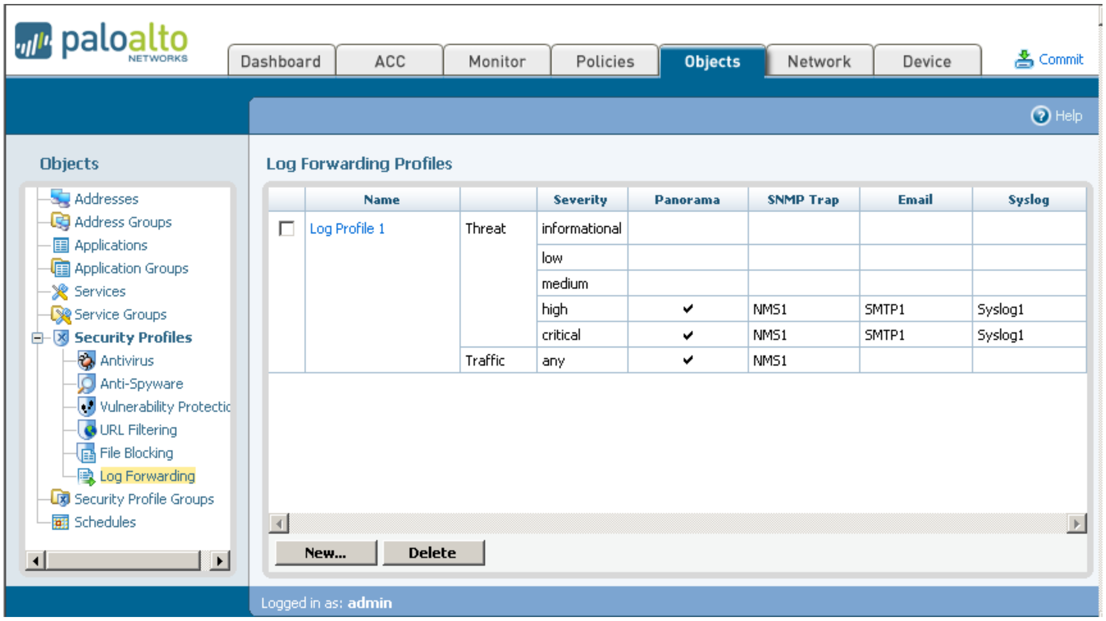
Defining Log Forwarding Profiles

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 "Defining Security Policies" on page 144.

To define log forwarding profiles:

1. Under the **Objects** tab, click **Security Profiles > Log Forwarding** to open the Logging Profiles page.



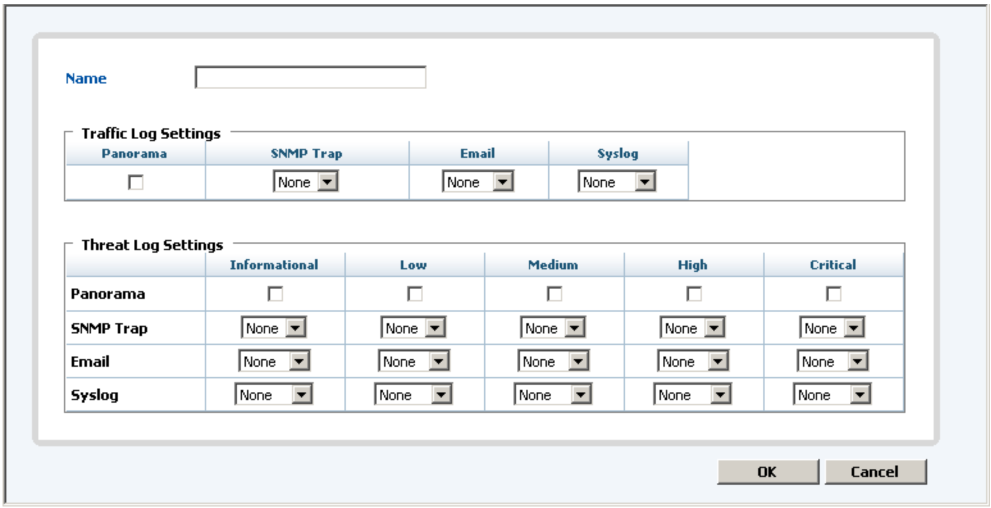
Log Forwarding Profiles

	Name		Severity	Panorama	SNMP Trap	Email	Syslog
□	Log Profile 1	Threat	informational				
			low				
			medium				
			high	✔	NMS1	SMTP1	Syslog1
			critical	✔	NMS1	SMTP1	Syslog1
		Traffic	any	✔	NMS1		

Figure 104. Log Forwarding Profiles Page

2. To add a new profile:

   a. Click **New** to open the New Log Forwarding Profile page.



Name

Traffic Log Settings

Panorama	SNMP Trap	Email	Syslog
□	None	None	None

Threat Log Settings

	Informational	Low	Medium	High	Critical
Panorama	□	□	□	□	□
SNMP Trap	None	None	None	None	None
Email	None	None	None	None	None
Syslog	None	None	None	None	None

Figure 105. New Log Forwarding Profile Page

   b. Specify the following information.

Table 65. New Log Forwarding Profile Settings

Field	Description
Name	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.
Traffic Log Settings	
Panorama	Select the check box to enable sending traffic log entries to the Panorama central management system. To define the Panorama server address, refer to “Defining the Host Name and Network Settings” on page 40.
SNMP Trap Setting Email Setting Syslog Setting	Select the SNMP, Syslog, and/or email settings that specify additional destinations where the traffic log entries are sent. To define new destinations, refer to: • “Defining SNMP Trap Destinations” on page 81. • “Defining Email Notification Profiles” on page 84 • “Defining Syslog Servers” on page 83

Table 65. New Log Forwarding Profile Settings (Continued)

Field	Description
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	Under each severity level, select the SNMP, Syslog, and/or email settings that specify additional destinations where the threat log entries are sent.

c. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

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

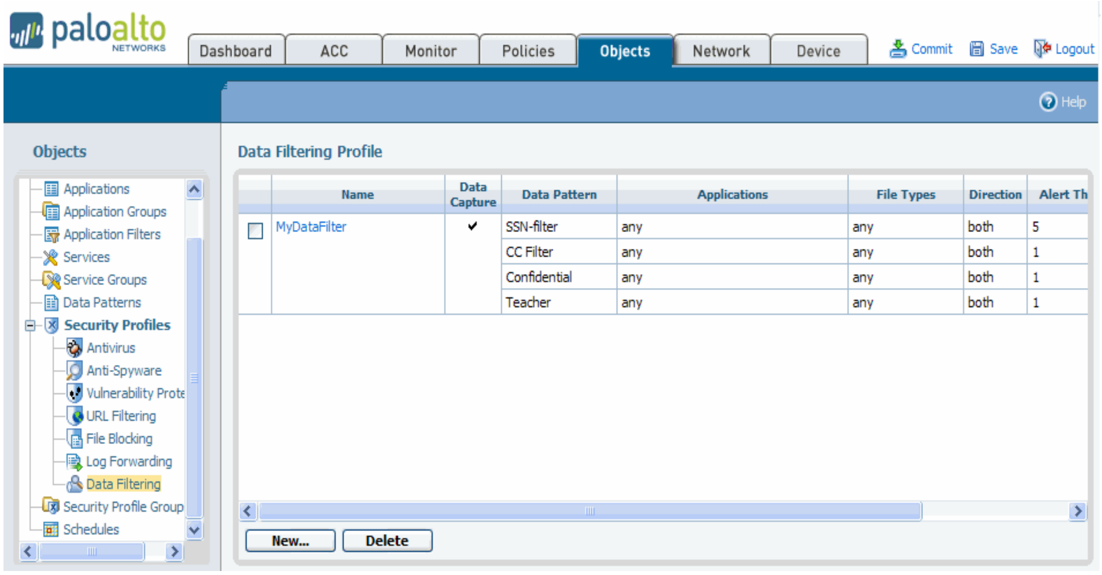
4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Defining Data Filtering Profiles

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 define data filtering profiles:

1. Under the **Objects** tab, click **Security Profiles > Data Filtering** to open the Data Filtering Profile page.

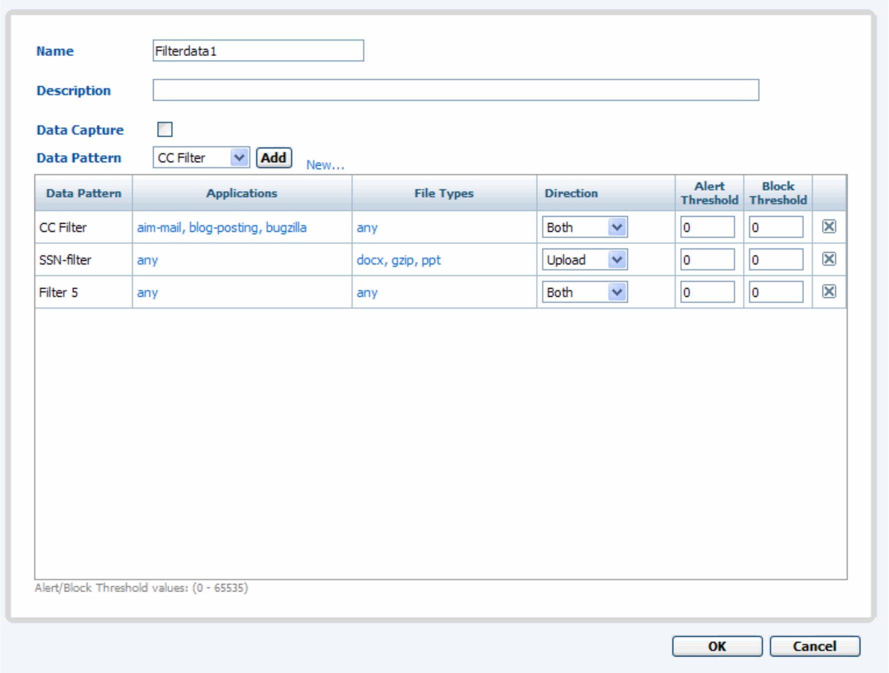


	Name	Data Capture	Data Pattern	Applications	File Types	Direction	Alert Th
□	MyDataFilter	✔	SSN-filter	any	any	both	5
			CC Filter	any	any	both	1
			Confidential	any	any	both	1
			Teacher	any	any	both	1

Figure 106. Data Filtering Profiles Page

2. To add a new profile:

   a. Click **New** to open the New Data Filtering Profile page.



Name	Filterdata1
Description	
Data Capture	□
Data Pattern	CC Filter

Data Pattern	Applications	File Types	Direction	Alert Threshold	Block Threshold	
CC Filter	aim-mail, blog-posting, bugzilla	any	Both	0	0	☒
SSN-filter	any	docx, gzip, ppt	Upload	0	0	☒
Filter 5	any	any	Both	0	0	☒

Alert/Block Threshold values: (0 - 65535)

Figure 107. New Data Filtering Profile Page

   b. Specify the following information.

Table 66. New Data Filtering Profile Settings

Field	Description
Name	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.
Description	Enter a description of the profile.
Shared	If the device is in Multiple Virtual System Mode, select this check box to allow the profile to be shared by all virtual systems.
Data Capture	Select the check box to automatically collect the data that is blocked by the filter.
Data Pattern	Select an existing data pattern for the rule, and click **Add** to the list of patterns. To define a new pattern, click **New**. Enter a name and description for the pattern, and click **OK**. To add a regular expression to the pattern, click **Add Pattern**, enter a pattern name, regular expression, and weight, and click **OK**.

c. To modify parameters for a data pattern in the list, click the item and specify information as described in the following table.

Table 67. New Data Filtering Profile Settings

Field	Description
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.

d. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

a. To change an entry, click the link for the entry, specify changes, and click **OK**.

b. To delete entries, select their check boxes and click **Delete**.

c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

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

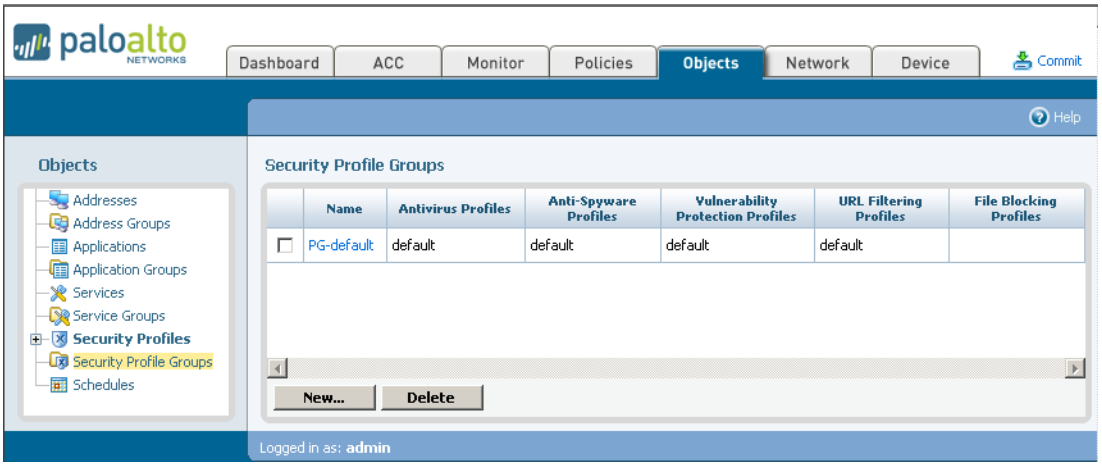
4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Defining Security Profile Groups

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 new security profiles, refer to “Defining Security Profiles” on page 164.

To define security profile groups:

1. Under the **Objects** tab, click **Security Profile Groups** to open the Security Profile Groups page.



	Name	Antivirus Profiles	Anti-Spyware Profiles	Vulnerability Protection Profiles	URL Filtering Profiles	File Blocking Profiles
□	PG-default	default	default	default	default	

Figure 108. Security Profile Groups Page

2. To add a new profile group:

   a. Click **New** to open the New Profile Group page.

   b. Specify the following information.

Table 68. New Security Profile Group

Field	Description
Profile Group Name	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.
Profiles	Select an antivirus, anti-spyware, vulnerability protection, URL filtering, and/or file blocking profile to be included in this group.

   c. Click **OK** to submit the new service group, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Defining Policy Objects

For information about defining the components of security policies, other than security profiles, refer to:

- “Defining Addresses” in the next section
- “Defining Address Groups” on page 195
- “Defining Applications” on page 196
- “Defining Application Groups” on page 202
- “Defining Application Filters” on page 204
- “Defining Services” on page 205
- “Defining Service Groups” on page 207
- “Defining Data Patterns” on page 209
- “Defining Schedules” on page 212

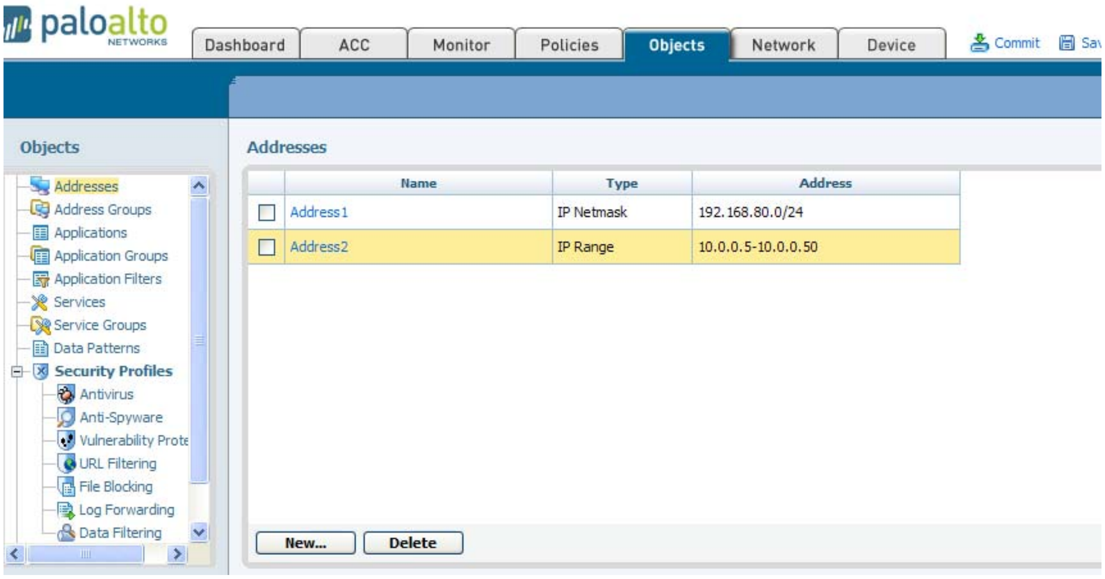
Note: *Shared polices pushed from Panorama are listed in green on the pages in the* ***Objects*** *tab.*

Defining Addresses

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 195).

To define addresses:

1. Under the **Objects** tab, click **Addresses** to open the Addresses page.



	Name	Type	Address
□	Address1	IP Netmask	192.168.80.0/24
□	Address2	IP Range	10.0.0.5-10.0.0.50

Figure 109. Addresses Page

2. To add a new IP address or address range:

   a. Click **New** to open the New Address page.

   b. Specify the following information.

Table 69. New Address

Field	Description
Address Name	Enter a name that describes the address(es) 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.

Table 69. New Address (Continued)

Field	Description
IP Address	Specify an IPv4 or IPv6 address. **IPv4 address:** Enter the address or network using the following notation: *ip_address/mask* or *ip_address* where the *mask* is the number of significant binary digits used for the network portion of the address. Example: "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. **IPv6 address:** Enter the IPv6 address or address with prefix. Example: "2001:db8:123:1::1" or "2001:db8:123:1::/64"
IP Range	To specify an address range, select **IP Range**, and enter a range of addresses. The format is: *ip_address–ip_address* where each address can be IPv4 or IPv6. Example: "2001:db8:123:1::1 - 2001:db8:123:1::22"

c. Click **OK** to submit the new address entry, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

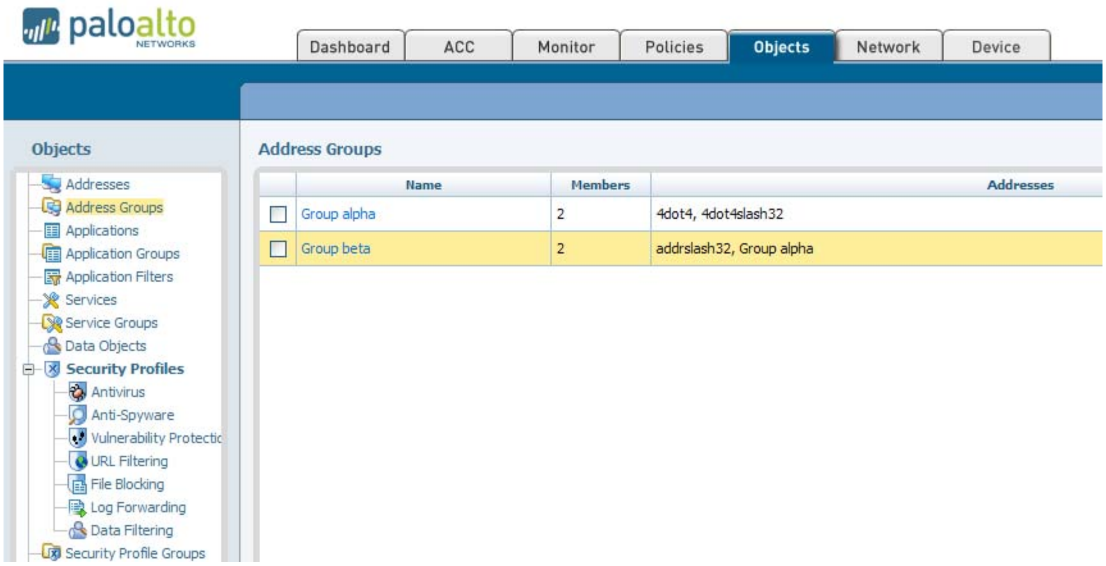
4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Defining Address Groups

To simplify the creation of security policies, addresses requiring the same security settings can be combined into address groups. To define addresses or address ranges, refer to "Defining Addresses" on page 193.

To define address groups:

1. Under the **Objects** tab, click **Address Groups** to open the Address Groups page.



	Name	Members	Addresses
□	Group alpha	2	4dot4, 4dot4slash32
□	Group beta	2	addrslash32, Group alpha

Figure 110. Address Groups Page

2. To add a new address group:

   a. Click **New** to open the New Address Group page.

   b. Specify the following information.

Table 70. New Address Group

Field	Description
Address Group Name	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.
All Addresses & Groups	Select the check box next to the addresses and/or other address groups to be included in this group.

   c. Click **OK** to submit the new address group, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

4. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Defining Applications

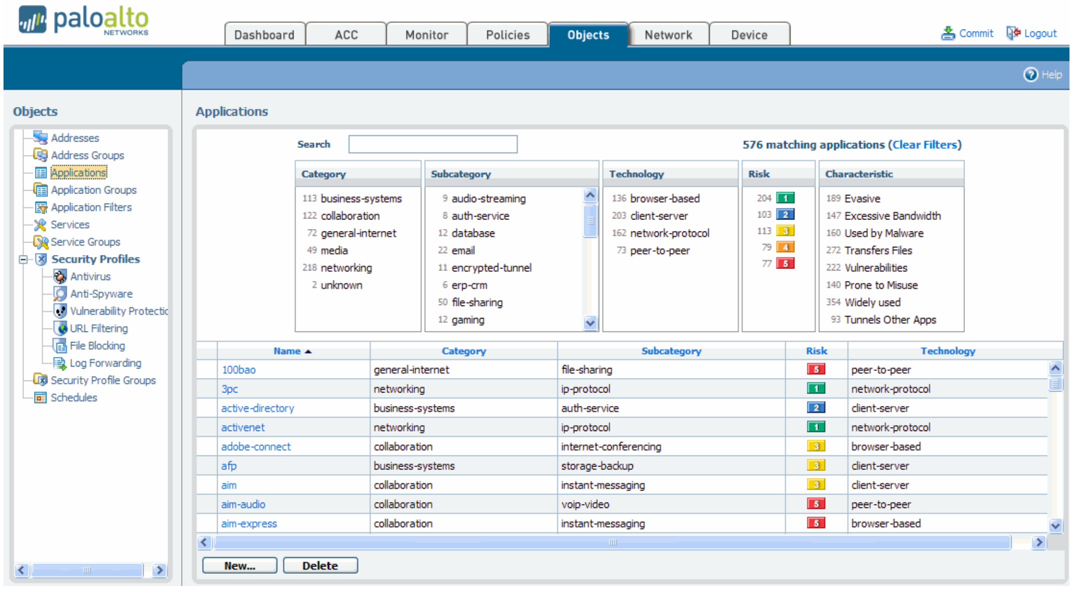
When the firewall is not able to identify an application using the application ID, the traffic is classified as unknown: unknown-tcp, unknown-udp, or tcp-no-syn. This behavior applies to all unknown applications except those that fully emulate HTTP. The HTTP emulation traffic is classified as web-browsing. For more information, refer to "Identifying Unknown Applications and Taking Action" on page 246.

You can create new definitions for unknown applications and then define security policies for the new application definitions (refer to "Defining Security Policies" on page 144).

Applications that require the same security settings can be combined into application groups to simplify the creation of security policies (refer to "Defining Application Groups" on page 202).

To search for applications:

1. Under the **Objects** tab, click **Applications** to open the Applications page.



Applications

Search

576 matching applications (Clear Filters)

Category	Subcategory	Technology	Risk	Characteristic
113 business-systems	9 audio-streaming	136 browser-based	204 1	189 Evasive
122 collaboration	8 auth-service	203 client-server	103 2	147 Excessive Bandwidth
72 general-internet	12 database	162 network-protocol	113 3	160 Used by Malware
49 media	22 email	73 peer-to-peer	79 4	272 Transfers Files
218 networking	11 encrypted-tunnel		77 5	222 Vulnerabilities
2 unknown	6 erp-crm			140 Prone to Misuse
	50 file-sharing			354 Widely used
	12 gaming			93 Tunnels Other Apps

Name ▲	Category	Subcategory	Risk	Technology
100bao	general-internet	file-sharing	5	peer-to-peer
3pc	networking	ip-protocol	1	network-protocol
active-directory	business-systems	auth-service	2	client-server
activenet	networking	ip-protocol	1	network-protocol
adobe-connect	collaboration	internet-conferencing	3	browser-based
afp	business-systems	storage-backup	3	client-server
aim	collaboration	instant-messaging	3	client-server
aim-audio	collaboration	voip-video	5	peer-to-peer
aim-express	collaboration	instant-messaging	5	browser-based

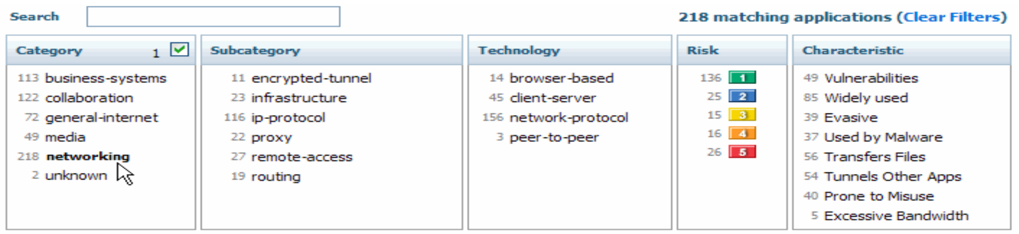
Figure 111. Applications Page

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 easy to misconfigure, 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.

2. 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.



Search

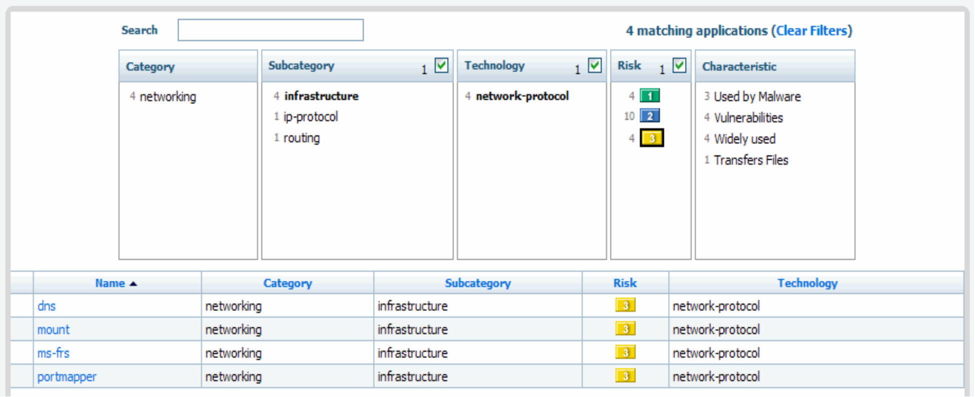
218 matching applications (Clear Filters)

Category 1 ☑	Subcategory	Technology	Risk	Characteristic
113 business-systems	11 encrypted-tunnel	14 browser-based	136 1	49 Vulnerabilities
122 collaboration	23 infrastructure	45 client-server	25 2	85 Widely used
72 general-internet	116 ip-protocol	156 network-protocol	15 3	39 Evasive
49 media	22 proxy	3 peer-to-peer	16 4	37 Used by Malware
218 **networking**	27 remote-access		26 5	56 Transfers Files
2 unknown	19 routing			54 Tunnels Other Apps
				40 Prone to Misuse
				5 Excessive Bandwidth

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**.



Search

4 matching applications (Clear Filters)

Category	Subcategory 1 ☑	Technology 1 ☑	Risk 1 ☑	Characteristic
4 networking	4 **infrastructure**	4 **network-protocol**	4 1	3 Used by Malware
	1 ip-protocol		10 2	4 Vulnerabilities
	1 routing		4 3	4 Widely used
				1 Transfers Files

Name ▲	Category	Subcategory	Risk	Technology
dns	networking	infrastructure	3	network-protocol
mount	networking	infrastructure	3	network-protocol
ms-frs	networking	infrastructure	3	network-protocol
portmapper	networking	infrastructure	3	network-protocol

3. 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.

4. 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 71. Application Details

Item	Description
Name	Name of the application.
Standard Ports	Ports that the application uses to communicate with the network.
Capable of File Transfer	Indication of whether the application is able to transfer files.
Used by Malware	Indication of whether the application is used by malware.
Excessive Bandwidth Use	Indication of whether the application uses too much bandwidth so that network performance may be compromise.
Evasive	Indication of whether the application attempts to evade firewalls.
Tunnels Other Applications	Indication of whether the application can carry other applications within the messages that it sends.
Additional Information	Links to web sources (Wikipedia, Google, and Yahoo!) that contain additional information about the application.
Category	Application category.
Subcategory	Application sub category.
Technology	Application technology.
Risk	Assigned risk of the application. To customize this setting, click the **Customize** link, enter a value (1-5), and click **OK**.
Pervasive	Indication of whether the effects of the application are wide-ranging.
Has Known Vulnerabilities	Indication of whether the application has any currently known vulnerabilities.
Prone to Misuse	Indication of whether the application tends to attract misuse.
Session Timeout	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**.
TCP Timeout (seconds)	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**.

Table 71. Application Details (Continued)

Item	Description
UDP Timeout (seconds):	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**.
Description	Purpose of the application.

To add a new application:

1. Under the **Objects** tab, click **Applications** to open the Applications page.
2. Click **New** to open the New Application page.

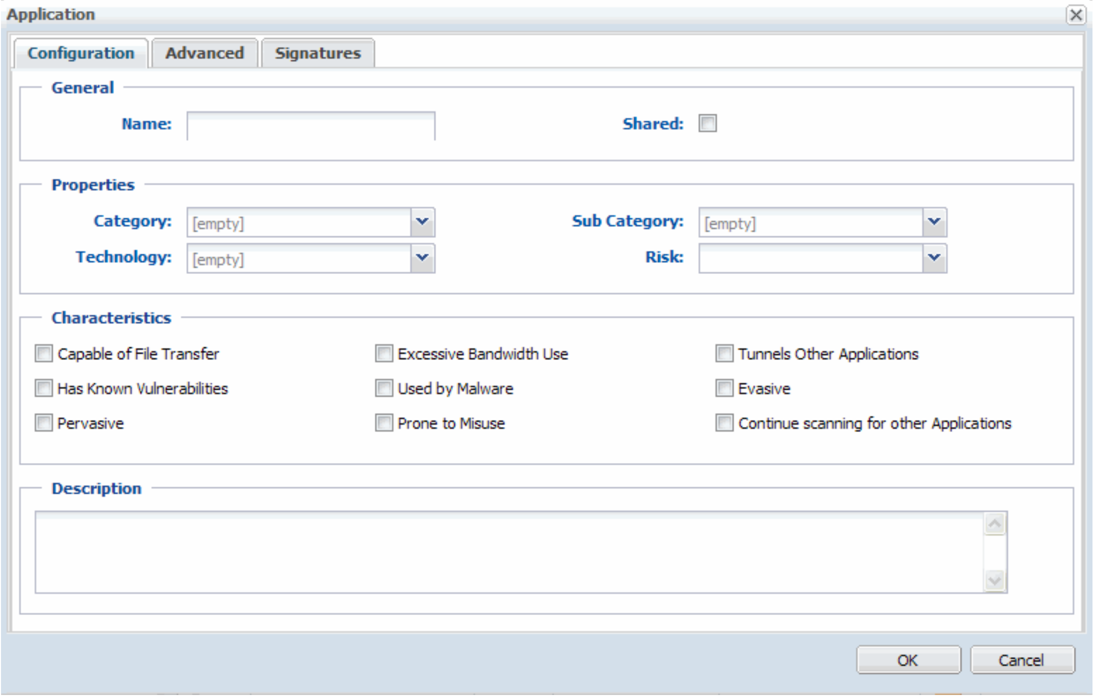


Figure 112. New Application Page

3. Specify the following information on the indicated tabs.

Table 72. New Application

Field	Description
Configuration Tab	
Name	Enter the application name (up to 31 characters). This name appears in the applications list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, periods, hyphens, and underscores. The first character must be a letter.
Shared	If the device is in Multiple Virtual System Mode, select this check box to allow the application to be shared by all virtual systems.
Category	Select the application category, such as email or database. For a description of each category, refer to "Application Categories and Subcategories" on page 311. The category is used to generate the Top Ten Application Categories chart and is available for filtering (refer to "Using the Application Command Center" on page 217).
Sub Category	Select the application sub category, such as email or database. For a description of each sub category, refer to "Application Categories and Subcategories" on page 311. The sub category is used to generate the Top Ten Application Categories chart and is available for filtering (refer to "Using the Application Command Center" on page 217).
Technology	Select the technology for the application. For a description of each technology, refer to "Application Technologies" on page 312.
Risk	Select the risk level associated with this application (1=lowest to 5=highest).
Characteristics	Select the application characteristics that may place the application at risk. For a description of each characteristic, refer to "Application Characteristics" on page 313.
Description	Enter an application description (for general reference only).
Advanced Tab	
Default Port	If the protocol used by the application is TCP and/or UDP, enter one or more combinations of the protocol and port number (one entry per line). The general format is: *<protocol>/<port>* where the *<port>* is a single port number, or **dynamic** for dynamic port assignment. Examples: TCP/dynamic or UDP/32. This setting applies when using **app-default** in the **Service** column of a security rule.
IP Protocol	To specify an IP protocol other than TCP or UDP, select **IP Protocol**, and enter the protocol number (1 to 255).
Timeout	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 if no TCP or UDP timeout is specified.
TCP Timeout UDP Timeout	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).

Table 72. New Application (Continued)

Field	Description
Engine	Select the following options from the drop-down lists: • **Decoder**—Indicates the application protocol. Currently HTTP is supported. • **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.
Scanning	Select check boxes for the scanning types that you want to allow, based on security profiles (file types, data patterns, and viruses).
Signature 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.

4. Click **OK** to submit the new definition, or click **Cancel** to discard your changes.

5. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

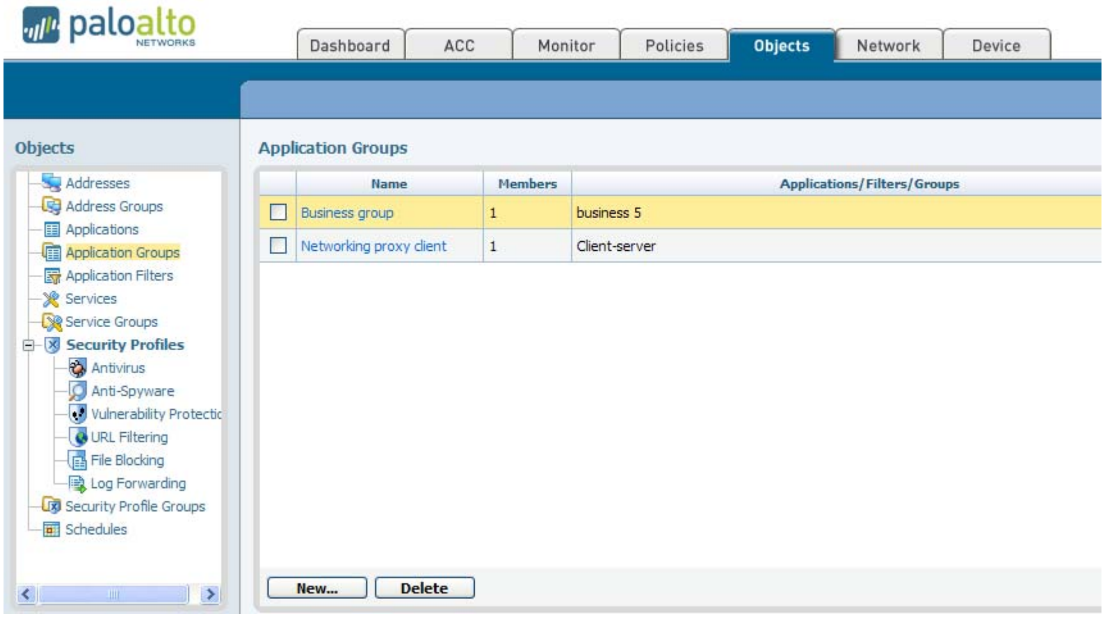
6. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

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 196.

To define application groups:

1. Under the **Objects** tab, click **Application Groups** to open the Application Groups page.



	Name	Members	Applications/Filters/Groups
□	Business group	1	business 5
□	Networking proxy client	1	Client-server

Figure 113. Application Groups Page

2. To add a new application group:

   a. Click **New** to open the New Application Group page.

   b. 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.

c. Use the following options to specify the applications to include in the group.

Table 73. New Application Group

Field	Description
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 311. • 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. To define new applications, refer to “Defining Applications” on page 196. To define application groups, refer to “Defining Application Groups” on page 202.
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.

d. Select check boxes for the desired applications, and click **Add Applications** to include the applications in the selected area.

e. Click **OK** to submit the new application group, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

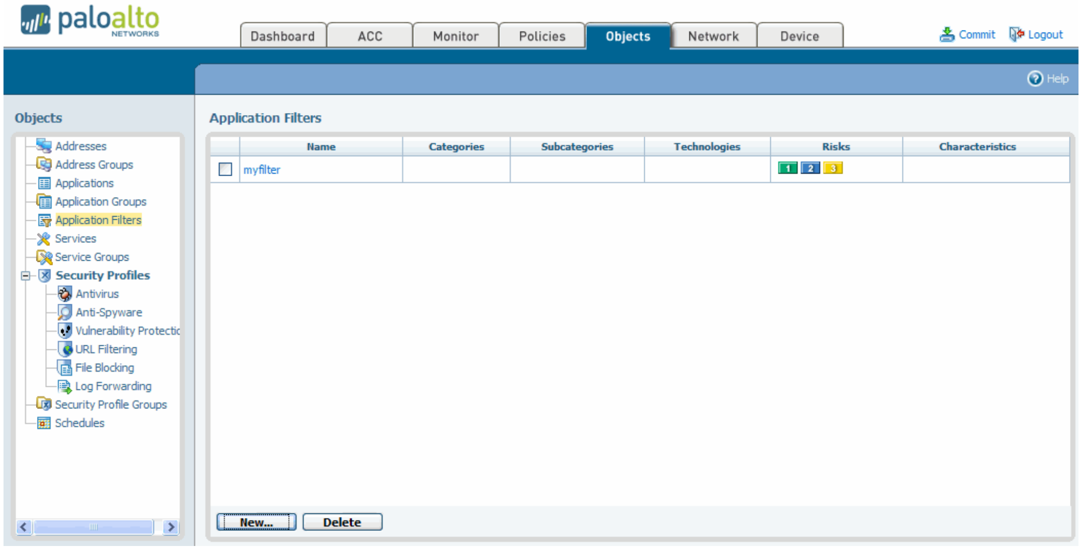
4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Defining Application Filters

You can define application filters to simplify repeated searches.

To define application filters:

1. Under the **Objects** tab, click **Application Filters** to open the Application Filters page.



	Name	Categories	Subcategories	Technologies	Risks	Characteristics
□	myfilter				1 2 3	

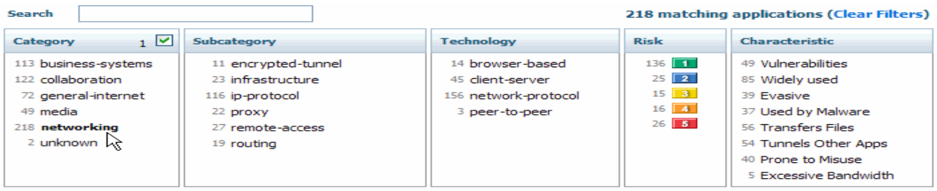
Figure 114. Application Filters Page

2. To define a new filters, click **New** to open the New Application Filters page.

   a. Enter a name for the filter.

   b. 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.

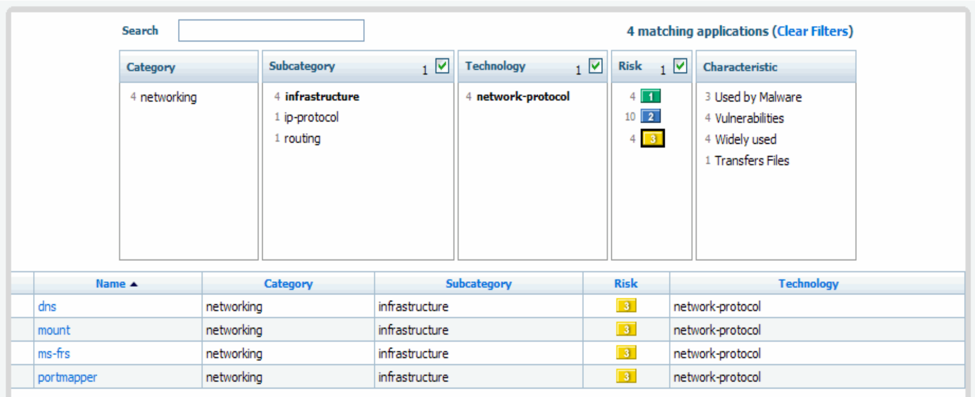


Category 1 ☑	Subcategory	Technology	Risk	Characteristic
113 business-systems	11 encrypted-tunnel	14 browser-based	136 1	49 Vulnerabilities
122 collaboration	23 infrastructure	45 client-server	25 2	85 Widely used
72 general-internet	116 ip-protocol	156 network-protocol	15 3	39 Evasive
49 media	22 proxy	3 peer-to-peer	16 4	37 Used by Malware
218 **networking**	27 remote-access		26 5	56 Transfers Files
2 unknown	19 routing			54 Tunnels Other Apps
				40 Prone to Misuse
				5 Excessive Bandwidth

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.



Search

4 matching applications (Clear Filters)

Category	Subcategory 1 ☑	Technology 1 ☑	Risk 1 ☑	Characteristic
4 networking	4 **infrastructure**	4 **network-protocol**	4 1	3 Used by Malware
	1 ip-protocol		10 2	4 Vulnerabilities
	1 routing		4 3	4 Widely used
				1 Transfers Files

Name ▲	Category	Subcategory	Risk	Technology
dns	networking	infrastructure	3	network-protocol
mount	networking	infrastructure	3	network-protocol
ms-frs	networking	infrastructure	3	network-protocol
portmapper	networking	infrastructure	3	network-protocol

c. Click **OK** to submit the new filter. The Application Filters page reopens to show the newly defined filter.

3. Perform any of the following additional tasks:

a. To change an entry, click the link for the entry, specify changes, and click **OK**.

b. To delete entries, select their check boxes and click **Delete**.

c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

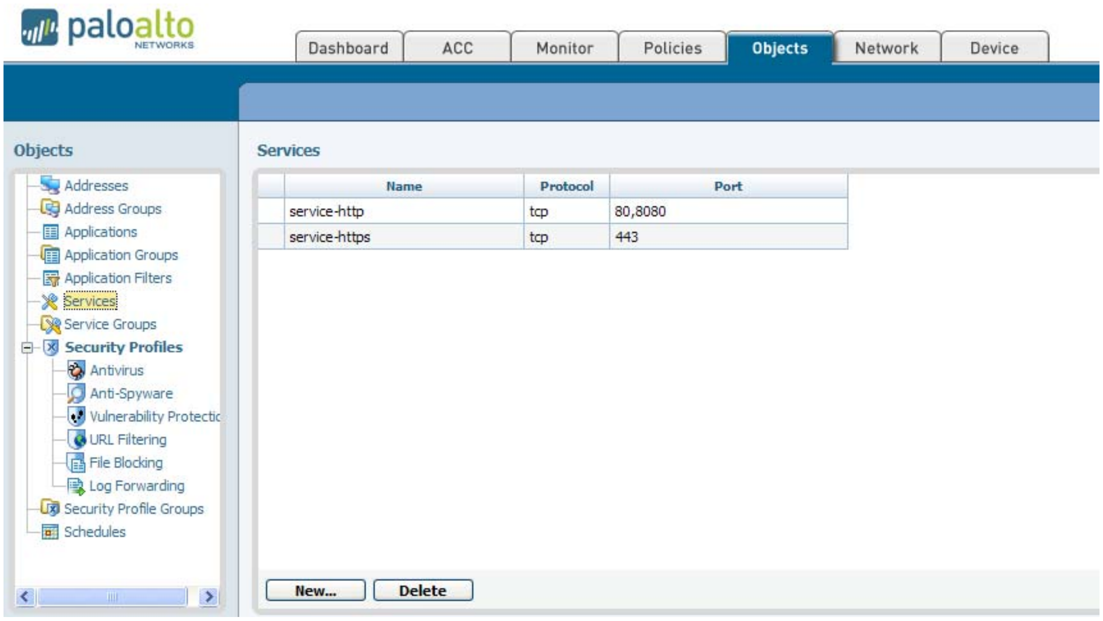
Defining Services

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 (refer to “Defining Service Groups” on page 207).

To define services:

1. Under the **Objects** tab, click **Services** to open the Services page.



Name	Protocol	Port
service-http	tcp	80,8080
service-https	tcp	443

Figure 115. Services Page

2. To add a new service:

   a. Click **New** to open the New Service page.

   b. Specify the following information.

Table 74. New Service

Field	Description
Service Name	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.
Shared	If the device is in Multiple Virtual System Mode, select this check box to allow the profile to be shared by all virtual systems.
Protocol	Select the protocol used by the service (TCP or UDP).
Port	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.

   c. Click **OK** to submit the new service, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

Note: *You cannot change or delete the predefined services.*

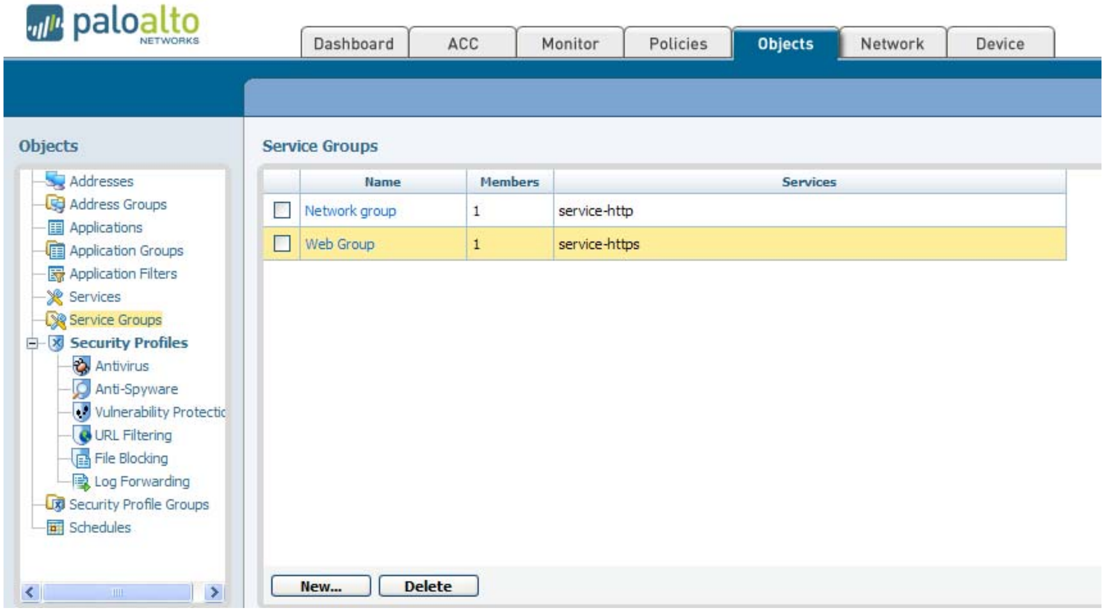
4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Defining Service Groups

To simplify the creation of security policies, services that often have the same security settings can be combined into service groups. To define new services, refer to “Defining Services” on page 205.

To define service groups:

1. Under the **Objects** tab, click **Service Groups** to open the Service Groups page.



	Name	Members	Services
□	Network group	1	service-http
□	Web Group	1	service-https

Figure 116. Service Groups Page

2. To add a new service group:

   a. Click **New** to open the New Service Group page.

   b. Specify the following information.

Table 75. New Service Group

Field	Description
Service Group Name	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.
All Services & Groups	Select the check box next to the services 🛠 and/or other service groups 📁 to be included in this group.

   c. Click **OK** to submit the new service group, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

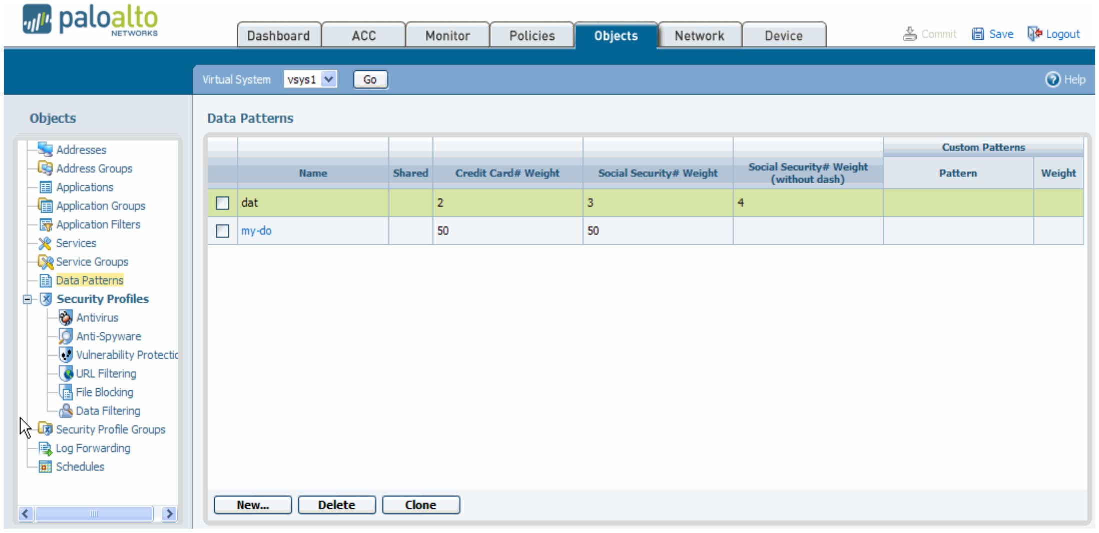
4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Defining 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. Refer to "Defining Data Filtering Profiles" on page 188 for information on defining data filtering policies.

To define data objects:

1. Under the **Objects** tab, click **Data Patterns** to open the Data Pattern page.



	Name	Shared	Credit Card# Weight	Social Security# Weight	Social Security# Weight (without dash)	Custom Patterns	
						Pattern	Weight
□	dat		2	3	4		
□	my-do		50	50			

Figure 117. Data Pattern Page

2. To add a object:

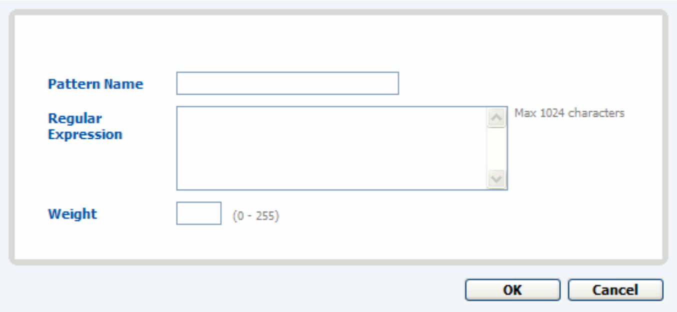
   a. Click **New** to open the New Data Pattern page.

   b. Specify the following information.

Table 76. New Data Pattern

Field	Description
Name	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.
Description	Enter an optional description.
Shared	If the device is in Multiple Virtual System Mode, select this check box to allow the profile to be shared by all virtual systems.

Table 76. New Data Pattern (Continued)

<table>
<thead>
<tr><th>Field</th><th>Description</th></tr>
</thead>
<tbody>
<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 ☒ to delete an object. See “Adding a New Pattern” in the next section.

</td></tr>
<tr><td>Weight</td><td>Enter weights for pre-specified pattern types. The weight is a number between 1 and 255.</td></tr>
</tbody>
</table>

   c. Click **OK** to submit the new data object, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Adding a New Pattern

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 77. Pattern Rules

Syntax	Description
.	Match any single character.
?	Match the preceding character or expression 0 or 1 time. The general expression MUST be inside a pair of parentheses. Example: (abc)?
*	Match the preceding character or expression 0 or more times. The general expression MUST be inside a pair of parentheses. Example: (abc)*
+	Match the preceding character or regular expression 1 or more times. The general expression MUST be inside a pair of parentheses. Example: (abc)+
|	Equivalent to “or”. Example: ((bif)|(scr)|(exe)) matches “bif”, “scr” or “exe”. Note that the alternative substrings must be in parentheses.
-	Used to create range expressions. Example: [c-z] matches any character between c and z, inclusive.
[ ]	Match any. Example: [abz]: matches any of the characters a, b, or z.
^	Match any except. Example: [^abz] matches any character except a, b, or z.
{ }	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 “.”.
\	To perform a literal match on any one of the special characters above, it MUST be escaped by preceding them with a ‘\’ (backslash).
&amp	& is a special character, so to look for the “&” in a string you must use “&amp” instead.

The following are examples of valid custom patterns:

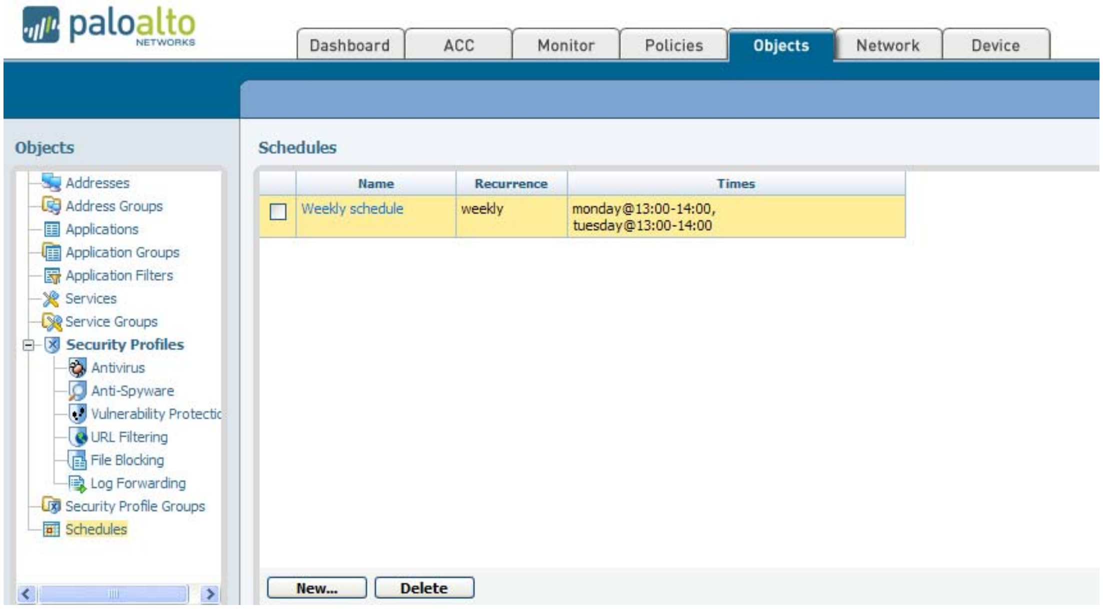
- .*((Confidential)|(CONFIDENTIAL))
  - Looks for the word “Confidential” or “CONFIDENTIAL” anywhere
  - “.*” at the beginning specifies to look anywhere in the stream
  - Does not match “confidential” (all lower case)
- .*((Proprietary &amp Confidential)|(Proprietary and Confidential))
  - Looks for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

Defining 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 “Defining Security Policies” on page 144.

To define schedules:

1. Under the **Objects** tab, click **Schedules** to open the Schedules page.

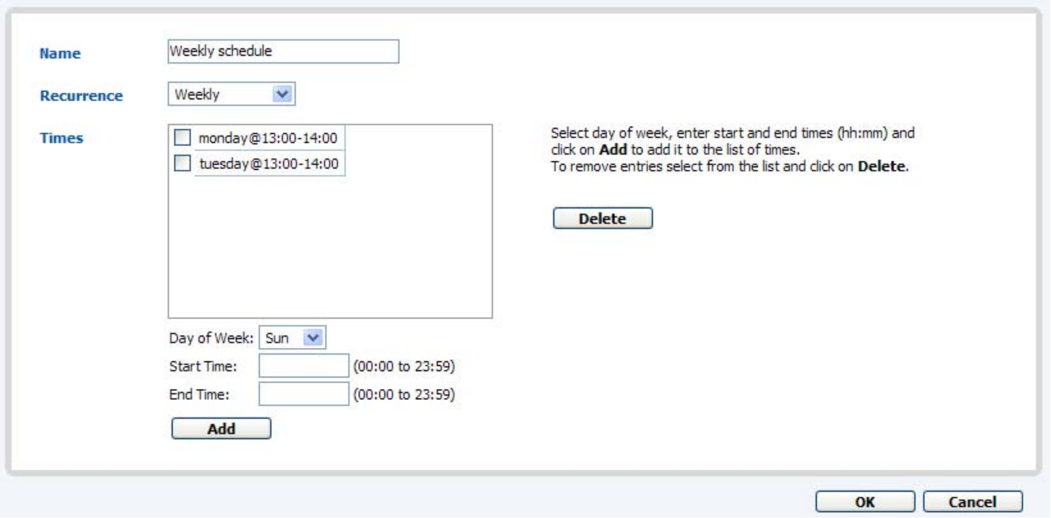


	Name	Recurrence	Times
□	Weekly schedule	weekly	monday@13:00-14:00, tuesday@13:00-14:00

Figure 118. Schedules Page

2. To add a new schedule:

   a. Click **New** to open the New Schedule page.



Name: Weekly schedule

Recurrence: Weekly

Times:

☐ monday@13:00-14:00

☐ tuesday@13:00-14:00

Select day of week, enter start and end times (hh:mm) and click on **Add** to add it to the list of times.
To remove entries select from the list and click on **Delete**.

Day of Week: Sun

Start Time: (00:00 to 23:59)

End Time: (00:00 to 23:59)

Figure 119. New Schedule Page

   b. Specify the following information.

Table 78. New Schedule Settings

Field	Description
Name	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.
Recurrence	Select the type of schedule (Daily, Weekly, or Non-Recurring).
Times	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**.
Day of Week	If the schedule type is Weekly, select a day of the week.
Start Time End Time	Specify a start and end time in 24-hour format (HH:MM).
Start Date End Date	If the schedule type is Non-Recurring, enter a start and end date: • Click 📅, and select a month and day. or • Enter the date directly (YYYY/MM/DD)

   c. Click **OK** to submit the new schedule, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Chapter 6

Reports and Logs

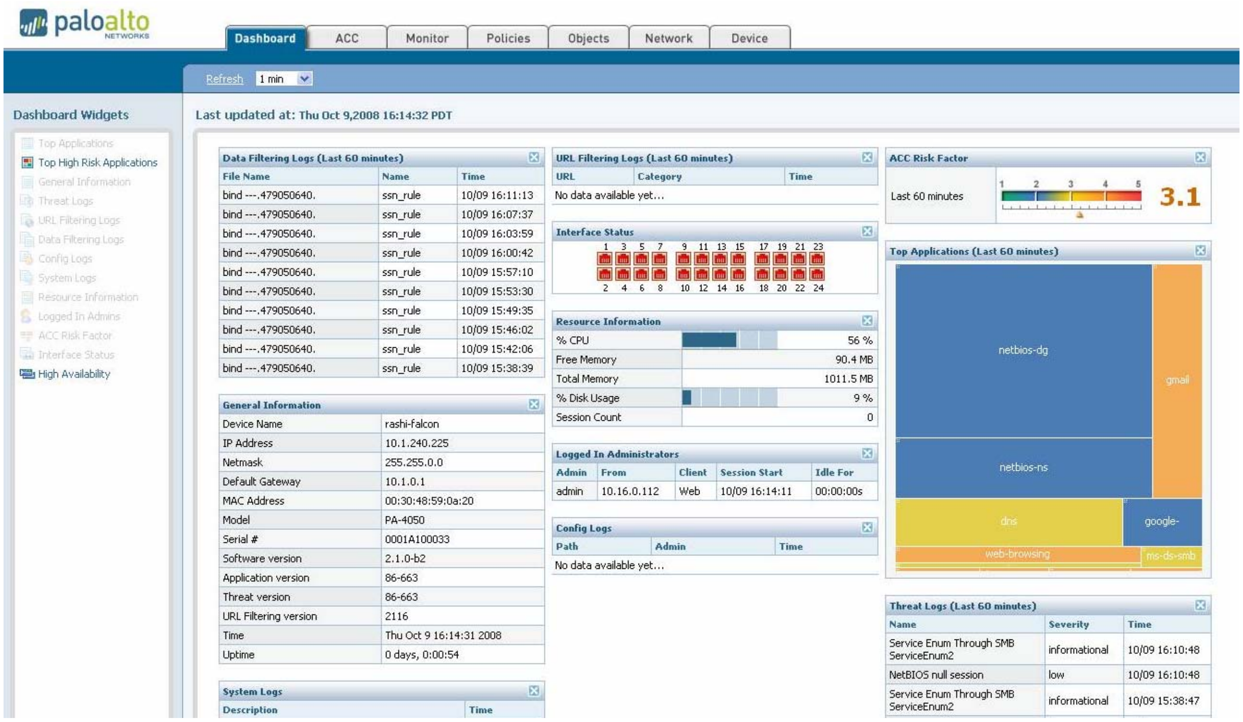
This chapter describes how to view the reports and logs provided with the firewall:

Using the 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.

To view or change the Dashboard:

1. Click the **Dashboard** tab to open the Dashboard page.
2. 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).



Last updated at: Thu Oct 9,2008 16:14:32 PDT

Data Filtering Logs (Last 60 minutes)

File Name	Name	Time
bind ---.479050640.	ssn_rule	10/09 16:11:13
bind ---.479050640.	ssn_rule	10/09 16:07:37
bind ---.479050640.	ssn_rule	10/09 16:03:59
bind ---.479050640.	ssn_rule	10/09 16:00:42
bind ---.479050640.	ssn_rule	10/09 15:57:10
bind ---.479050640.	ssn_rule	10/09 15:53:30
bind ---.479050640.	ssn_rule	10/09 15:49:35
bind ---.479050640.	ssn_rule	10/09 15:46:02
bind ---.479050640.	ssn_rule	10/09 15:42:06
bind ---.479050640.	ssn_rule	10/09 15:38:39

General Information

Device Name	rashi-falcon
IP Address	10.1.240.225
Netmask	255.255.0.0
Default Gateway	10.1.0.1
MAC Address	00:30:48:59:0a:20
Model	PA-4050
Serial #	0001A100033
Software version	2.1.0-b2
Application version	86-663
Threat version	86-663
URL Filtering version	2116
Time	Thu Oct 9 16:14:31 2008
Uptime	0 days, 0:00:54

System Logs

Description	Time

URL Filtering Logs (Last 60 minutes)

URL	Category	Time
No data available yet...		

Resource Information

% CPU	56 %
Free Memory	90.4 MB
Total Memory	1011.5 MB
% Disk Usage	9 %
Session Count	0

Logged In Administrators

Admin	From	Client	Session Start	Idle For
admin	10.16.0.112	Web	10/09 16:14:11	00:00:00s

Config Logs

Path	Admin	Time
No data available yet...		

ACC Risk Factor

Last 60 minutes 3.1

Threat Logs (Last 60 minutes)

Name	Severity	Time
Service Enum Through SMB ServiceEnum2	informational	10/09 16:10:48
NetBIOS null session	low	10/09 16:10:48
Service Enum Through SMB ServiceEnum2	informational	10/09 15:38:47

Figure 120. Dashboard Page

3. Review the following information in each chart.

Table 79. Dashboard Charts

Chart	Description
Top Applications	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 (refer to "Using the Application Command Center" on page 217).
Top High Risk Applications	Similar to Top Applications, except that it displays the highest-risk applications with the most sessions.

Table 79. Dashboard Charts (Continued)

Chart	Description
General Information	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.
Interface Status	Indicates whether each interface is up (green), down (red), or in an unknown state (gray).
Threat Logs	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 a URL that violates the URL filtering profile. To view the details of each threat. refer to “Identifying Unknown Applications and Taking Action” on page 246.
Config Logs	Displays the administrator user name, client (Web or CLI), and date and time for the last 10 entries in the Configuration log.
Data Filtering Logs	Displays the description and date and time for the last 60 minutes in the Data Filtering log.
URL Filtering Logs	Displays the description and date and time for the last 60 minutes in the URL Filtering log.
System Logs	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.
Resource Information	Displays the current CPU, memory, and disk utilization, and the number of sessions established through the firewall.
Logged In Admins	Displays the source IP address, session type (Web or CLI), and session start time for each administrator who is currently logged in.
ACC Risk Factor	Displays the average risk factor (1 to 5) for the network traffic processed over the past week. Higher values indicate higher risk.
High Availability	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 “Configuring High Availability” on page 70.

4. To add a chart to the Dashboard, click the chart name on the left side of the page. To delete a chart, click ✖ in the title bar of the chart.

Using the Application Command Center

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 easy to configure incorrectly, or tries to evade firewalls.

To view the Application Command Center:

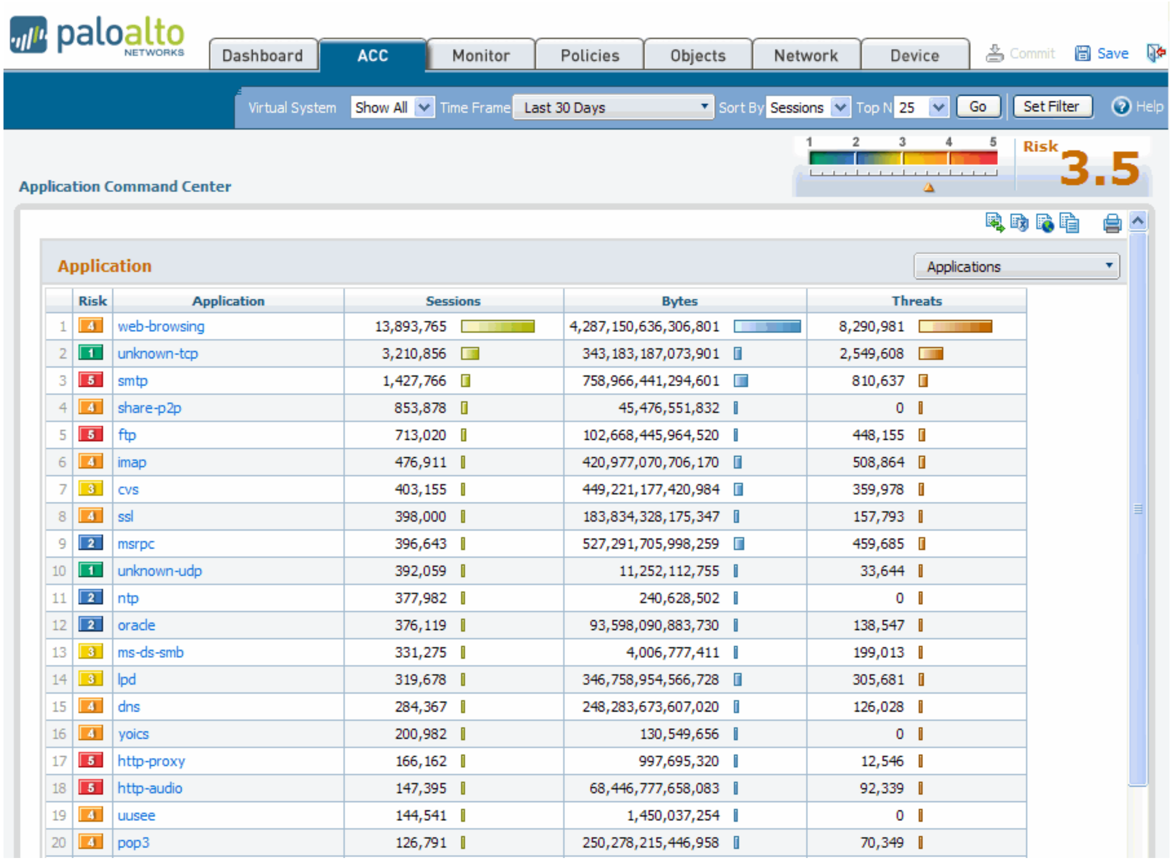
1. Under the **ACC** tab, change one or more of the following settings at the top of the page, and click **Go**:

   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.**



Virtual System: Show All
Time Frame: Last 30 Days
Sort By: Sessions
Top N: 25

Application Command Center

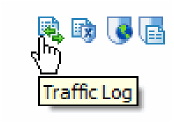
Risk 3.5

Application

	Risk	Application	Sessions	Bytes	Threats
1	4	web-browsing	13,893,765	4,287,150,636,306,801	8,290,981
2	1	unknown-tcp	3,210,856	343,183,187,073,901	2,549,608
3	5	smtp	1,427,766	758,966,441,294,601	810,637
4	4	share-p2p	853,878	45,476,551,832	0
5	5	ftp	713,020	102,668,445,964,520	448,155
6	4	imap	476,911	420,977,070,706,170	508,864
7	3	cvs	403,155	449,221,177,420,984	359,978
8	4	ssl	398,000	183,834,328,175,347	157,793
9	2	msrpc	396,643	527,291,705,998,259	459,685
10	1	unknown-udp	392,059	11,252,112,755	33,644
11	2	ntp	377,982	240,628,502	0
12	2	oracle	376,119	93,598,090,883,730	138,547
13	3	ms-ds-smb	331,275	4,006,777,411	199,013
14	3	lpd	319,678	346,758,954,566,728	305,681
15	4	dns	284,367	248,283,673,607,020	126,028
16	4	yoics	200,982	130,549,656	0
17	5	http-proxy	166,162	997,695,320	12,546
18	5	http-audio	147,395	68,446,777,658,083	92,339
19	4	uusee	144,541	1,450,037,254	0
20	4	pop3	126,791	250,278,215,446,958	70,349

Figure 121. 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.



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.

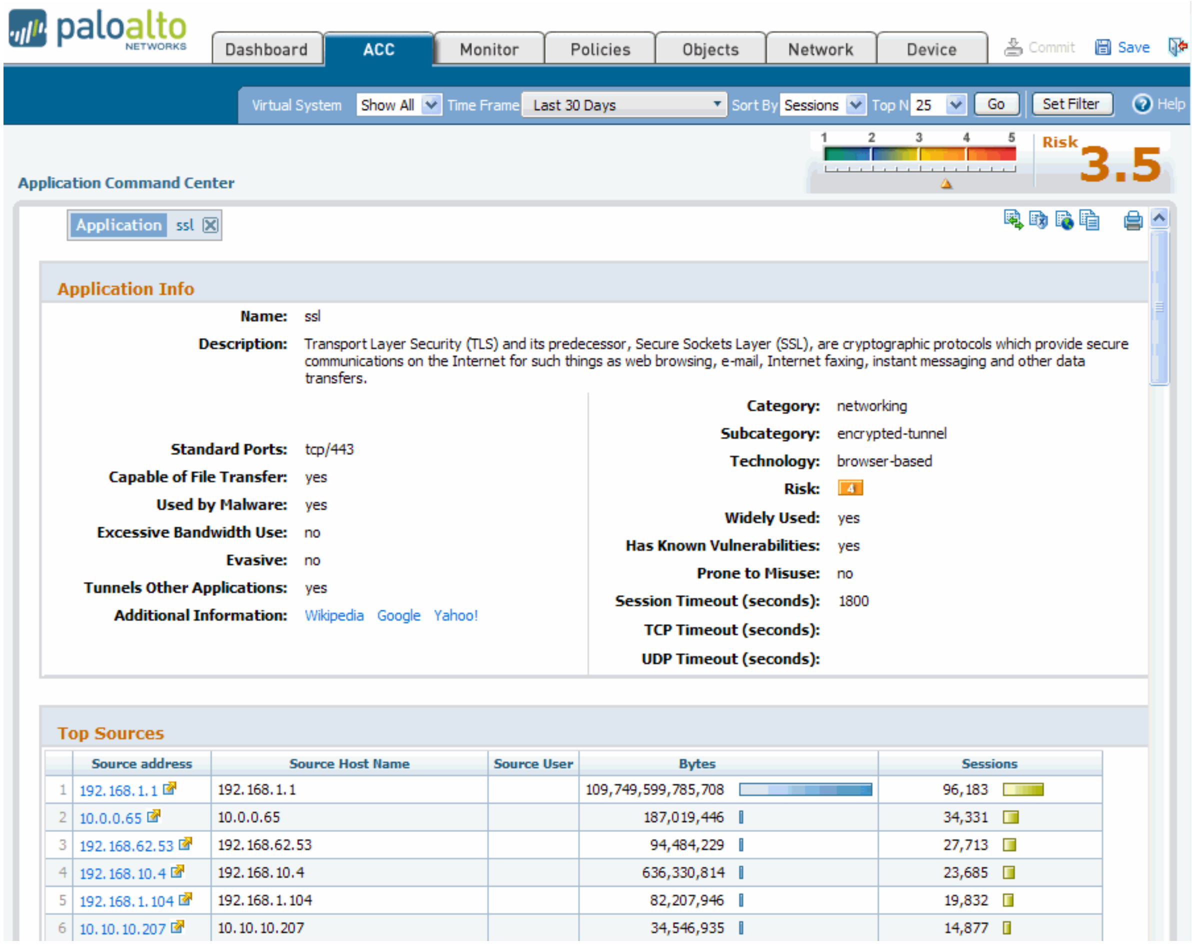
Table 80. Application Command Center Charts

Chart	Description
Applications	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. • Applications • High risk applications • Categories • Sub Categories • Technology • Risk
URL Filtering	Displays information organized according to the menu selection. Information includes the URL, URL category, repeat count (number of times access was attempted, as applicable. • URL Categories • URLs • Blocked URL Categories • Blocked URLs

Table 80. Application Command Center Charts (Continued)

Chart	Description
Threats	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. • Threats • Types • Spyware • Spyware Phone Home • Spyware Downloads • Vulnerability • Virus
Data Filtering	• Types • File Types • File Names

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 Info

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.

Standard Ports: tcp/443
Capable of File Transfer: yes
Used by Malware: yes
Excessive Bandwidth Use: no
Evasive: no
Tunnels Other Applications: yes
Additional Information: Wikipedia Google Yahoo!

Category: networking
Subcategory: encrypted-tunnel
Technology: browser-based
Risk: 4
Widely Used: yes
Has Known Vulnerabilities: yes
Prone to Misuse: no
Session Timeout (seconds): 1800
TCP Timeout (seconds):
UDP Timeout (seconds):

Top Sources

	Source address	Source Host Name	Source User	Bytes	Sessions
1	192.168.1.1	192.168.1.1		109,749,599,785,708	96,183
2	10.0.0.65	10.0.0.65		187,019,446	34,331
3	192.168.62.53	192.168.62.53		94,484,229	27,713
4	192.168.10.4	192.168.10.4		636,330,814	23,685
5	192.168.1.104	192.168.1.104		82,207,946	19,832
6	10.10.10.207	10.10.10.207		34,546,935	14,877

Figure 122. Application Command Center Page Drill Down Page

Viewing App-Scope Reports

The App-Scope reports introduce a new set of 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:

1. Under the **Monitor** tab, click the report name under App-Scope on the left side of the page.
2. 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 81. Application Command Center Charts

Chart	Description
Summary	"Summary Report" on page 222
Change Monitor	"Change Monitor Report" on page 223
Threat Monitor	"Threat Monitor Report" on page 224
Threat Map	"Threat Monitor Report" on page 224
Network Monitor	"Network Monitor Report" on page 227
Traffic Map	"Traffic Map Report" on page 228

Summary Report

The Summary report (Figure 123) displays charts for the top five gainers, losers, and bandwidth consuming applications, application categories, users, and sources.

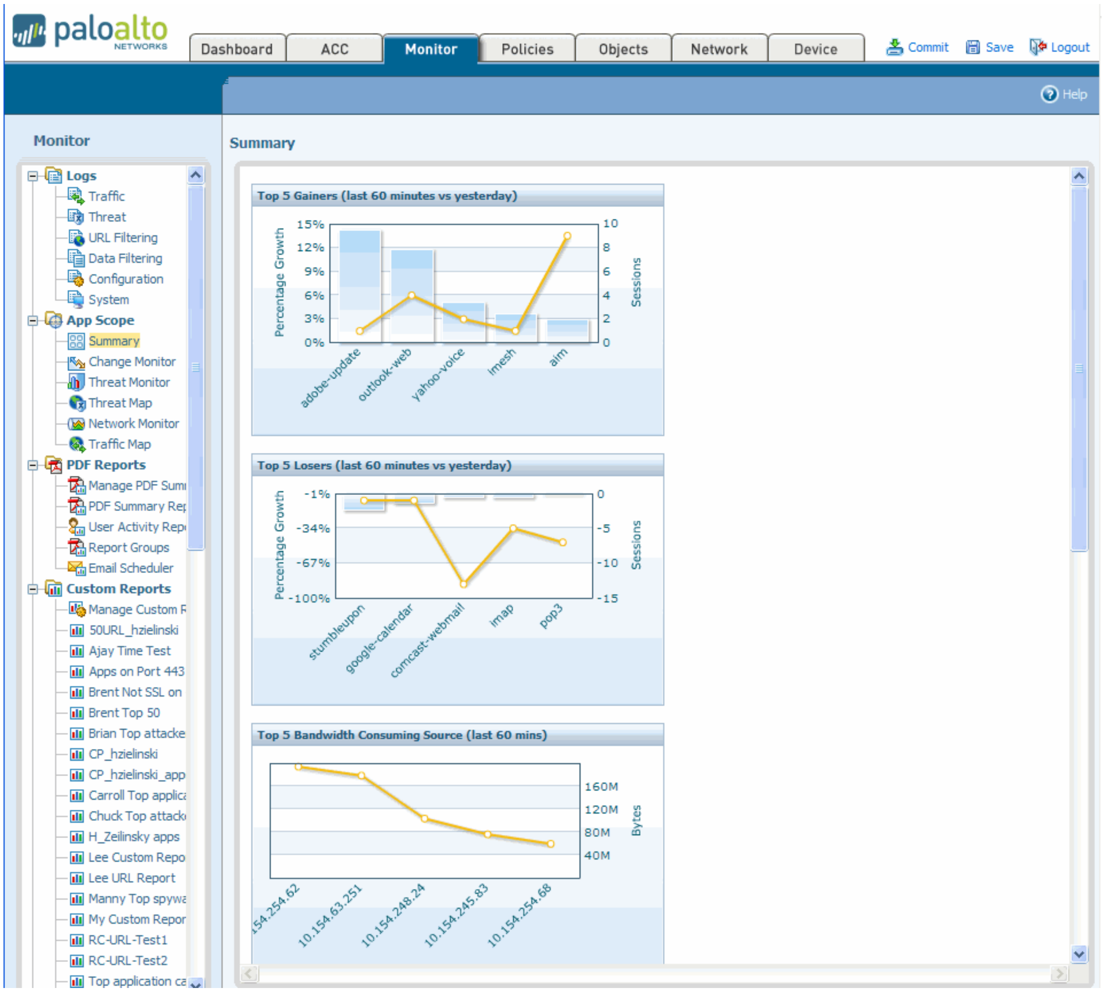


Figure 123. App-Scope Summary Report

Change Monitor Report

The Change Monitor report (Figure 124) displays changes over a specified time period.

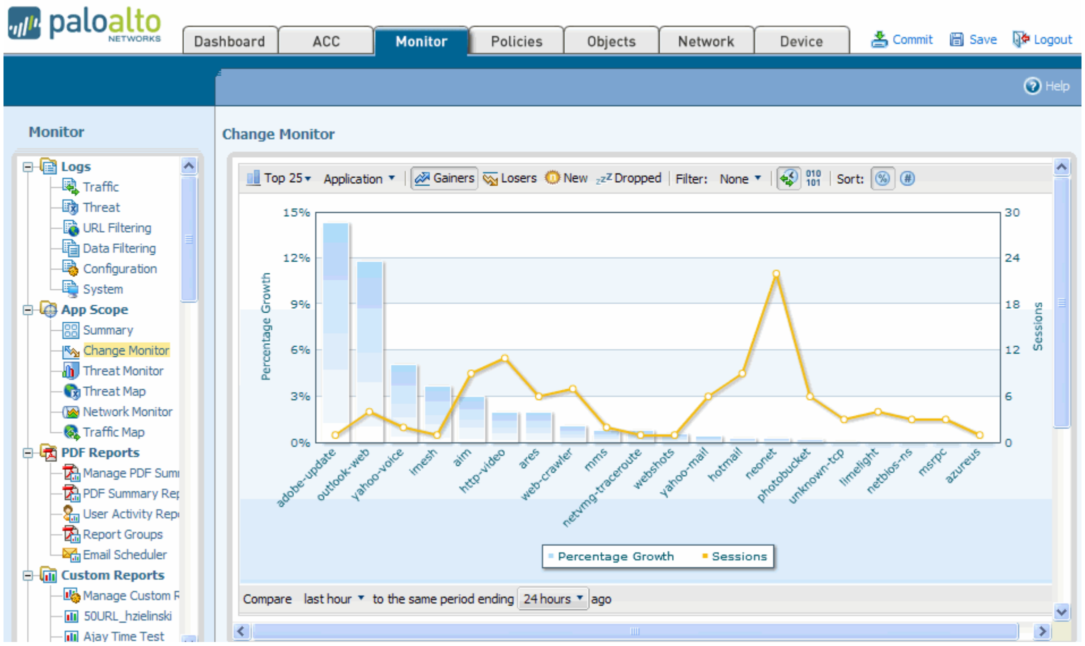


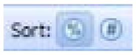
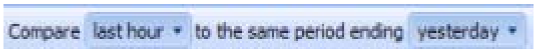
Figure 124. App-Scope Change Monitor Report

This report contains the following buttons and options.

Table 82. Change Monitor Report Buttons

Button	Description
Top 25	Determines the number of records with the highest measurement included in the chart: Top 25, Top 50, Top 75, or Top 100
Application ▾	Determines the type of item reported: Application, Application Category, Source, or Destination.
Gainers	Displays measurements of items that have increased over the measured period.
Losers	Displays measurements of items that have decreased over the measured period.
Dropped	Displays measurements of items that were discontinued over the measure period.
Filter: None ▾	Displays only the selected item.
010 101	Determines whether sessions or bytes are displayed.

Table 82. Change Monitor Report Buttons (Continued)

Button	Description
	Determines whether data is sorted by number or percent.
	Indicates the period over which the change measurements are taken.

For example, Figure 124 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 125) displays a count of the top threats over the selected time period.

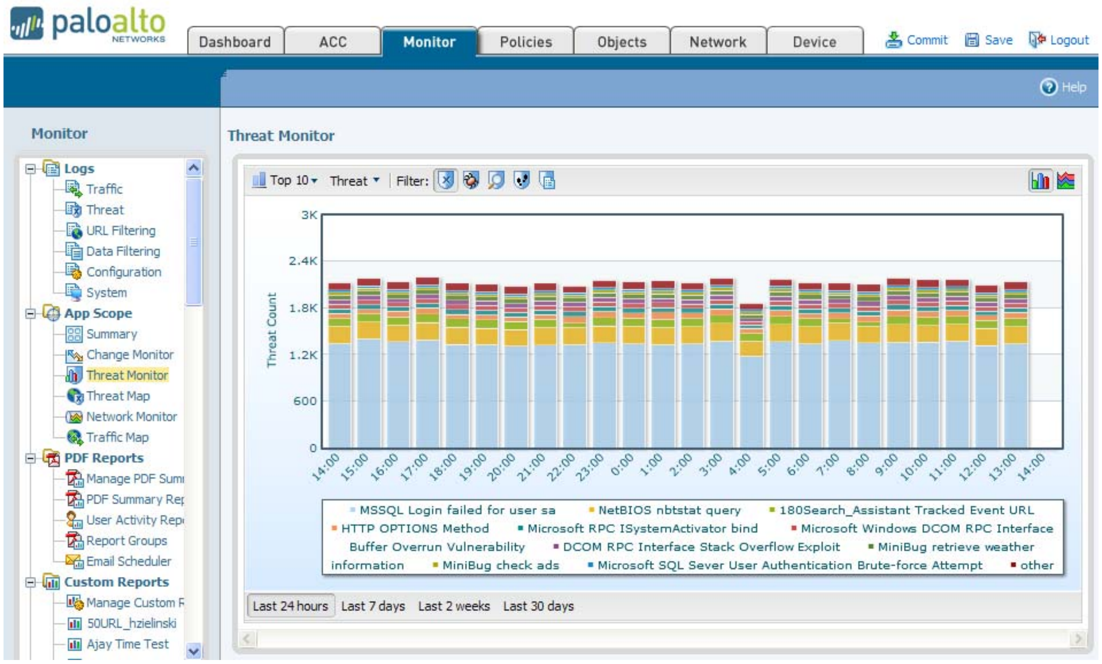


Figure 125. App-Scope Threat Monitor Report

Each threat type is color-coded as indicated in the legend below the chart. This report contains the following buttons and options.

Table 83. Threat Monitor Report Buttons

Button	Description
Top 10 ▾	Determines the number of records with the highest measurement included in the chart: Top 10 or Top 25.
Threat ▾	Determines the type of item measured: Threat, Threat Category, Source, or Destination.
Filter:	Displays the selected threat type: All, Viruses, Spyware, or Vulnerabilities.
Last 24 hours Last 7 days Last 2 weeks Last 30 days	Indicates the period over which the measurements are taken.
	Determines whether the information is presented in a stacked column chart or a stacked area chart.

For example, Figure 125 the figure displays the top 10 threats over the past 24 hours.

Threat Map Report

The Threat Map report (Figure 126) shows a geographical view of threats, including severity.

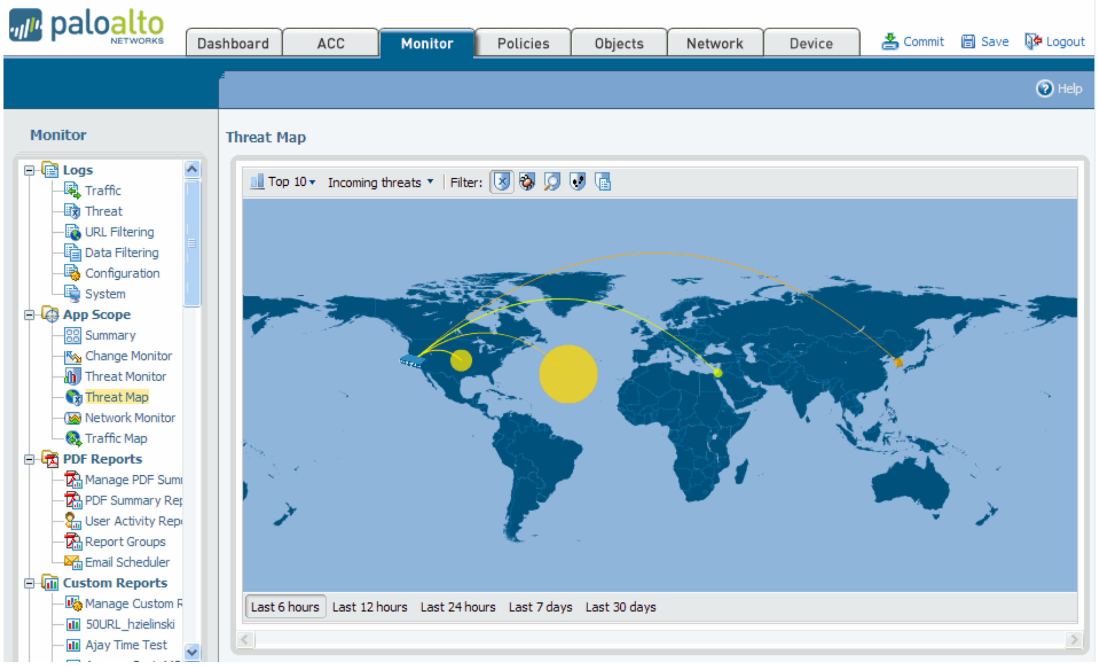
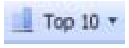
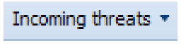
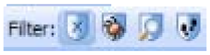
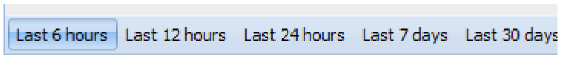


Figure 126. App-Scope Threat Monitor Report

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 84. Threat Map Report Buttons

Button	Description
	Determines the number of records with the highest measurement included in the chart: Top 10 or Top 25.
	Determines whether incoming or outgoing threats are included.
	Displays the selected threat type: All, Viruses, Spyware, or Vulnerabilities.
 Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Indicates the period over which the measurements are taken.

For example, Figure 126 displays the top 10 threats over the past 24 hours.

Network Monitor Report

The Network Monitor report (Figure 127) 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.

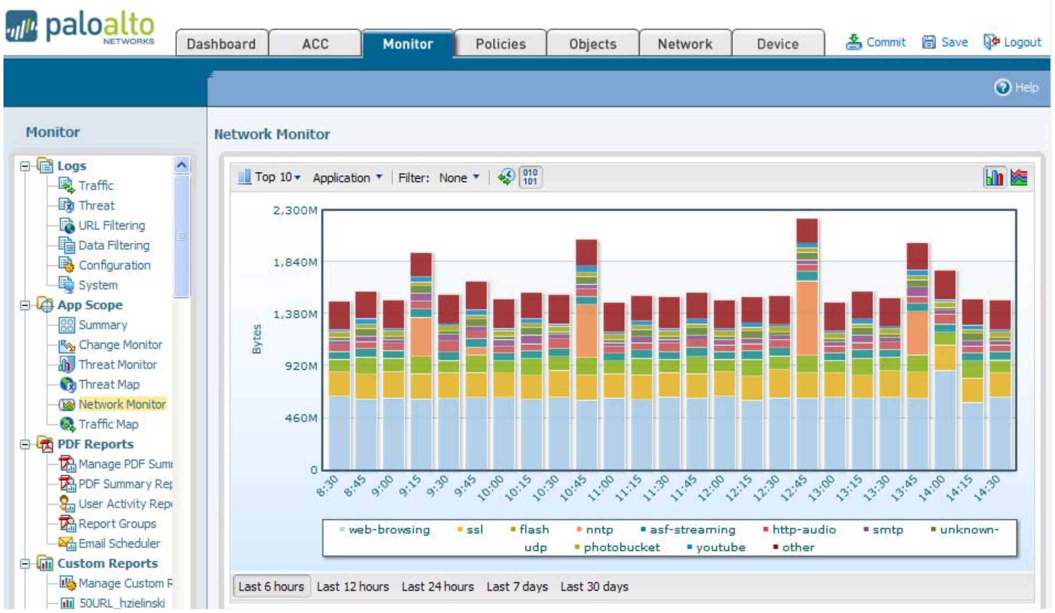


Figure 127. App-Scope Network Monitor Report

The report contains the following buttons and options.

Table 85. Network Monitor Report Buttons

Button	Description
Top 10	Determines the number of records with the highest measurement included in the chart: Top 10, Top 25, or Top 100.
Application	Determines the type of item measured: Application, Application Category, Source, or Destination.
Filter: None	Displays only the selected item.
010 101	Determines whether sessions or bytes are plotted.
Last 24 hours Last 7 days Last 2 weeks Last 30 days	Indicates the period over which the measurements are taken.
	Determines whether the information is presented in a stacked column chart or a stacked area chart.

For example, Figure 127 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 128) shows a geographical view of traffic flows according to sessions or flows.

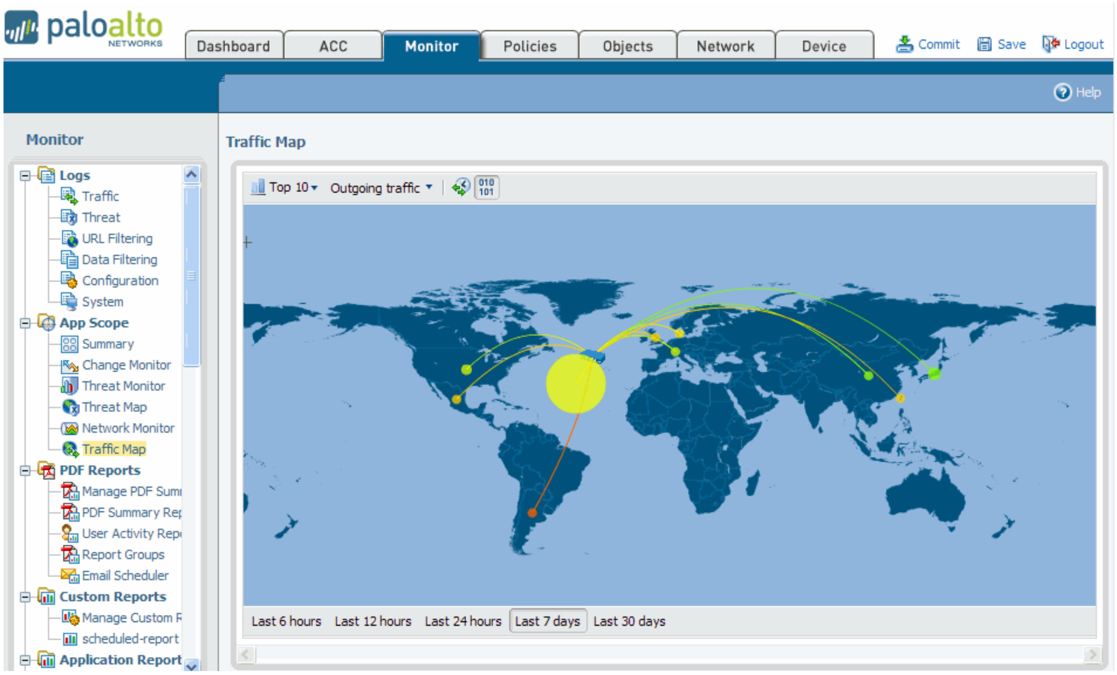


Figure 128. App-Scope Traffic Monitor Report

Each traffic type is color-coded as indicated in the legend below the chart. This report contains the following buttons and options.

Table 86. Threat Map Report Buttons

Button	Description
Top 10 ▾	Determines the number of records with the highest measurement included in the chart: Top 10 or Top 25.
Incoming threats ▾	Determines whether incoming or outgoing traffic is included.
010 101	Determines whether sessions or bytes are plotted.
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Indicates the period over which the measurements are taken.

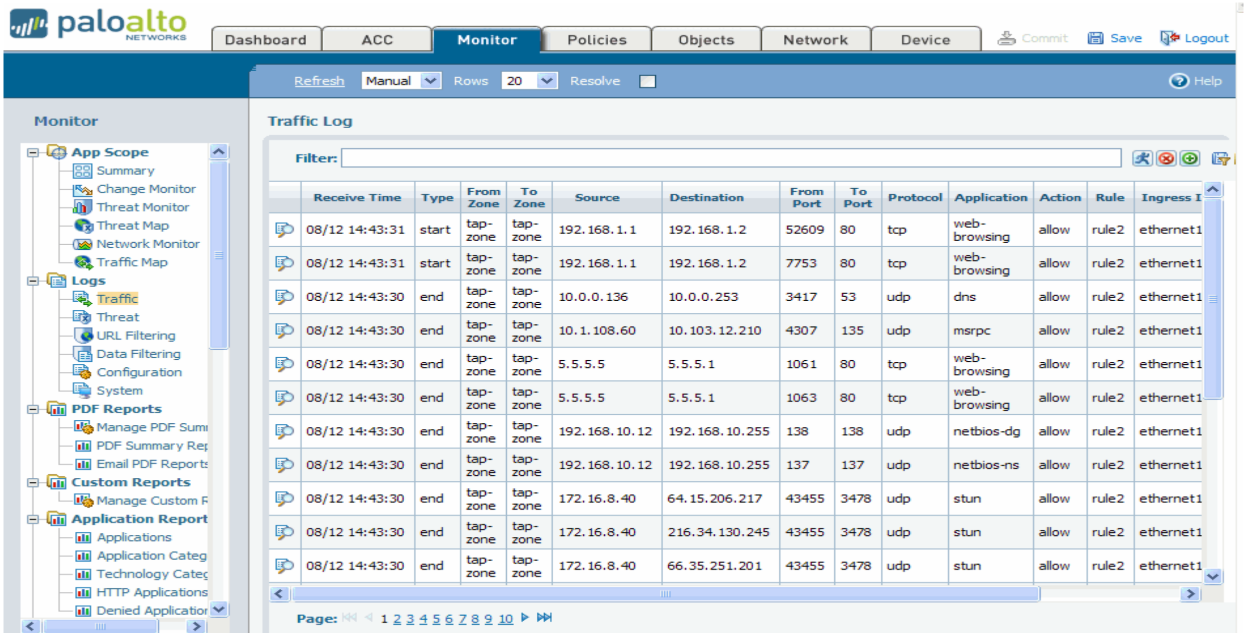
For example, Figure 128 displays the top 10 threats over the past 24 hours.

Viewing the 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.

To view the logs:

1. Under the **Monitor** tab, click the log types on the left side of the page. Figure 129 shows the Configuration Log page.

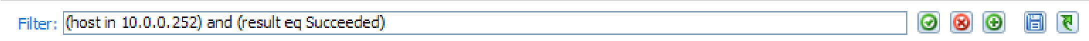


	Receive Time	Type	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Action	Rule	Ingress I
	08/12 14:43:31	start	tap-zone	tap-zone	192.168.1.1	192.168.1.2	52609	80	tcp	web-browsing	allow	rule2	ethernet1
	08/12 14:43:31	start	tap-zone	tap-zone	192.168.1.1	192.168.1.2	7753	80	tcp	web-browsing	allow	rule2	ethernet1
	08/12 14:43:30	end	tap-zone	tap-zone	10.0.0.136	10.0.0.253	3417	53	udp	dns	allow	rule2	ethernet1
	08/12 14:43:30	end	tap-zone	tap-zone	10.1.108.60	10.103.12.210	4307	135	udp	msrpc	allow	rule2	ethernet1
	08/12 14:43:30	end	tap-zone	tap-zone	5.5.5.5	5.5.5.1	1061	80	tcp	web-browsing	allow	rule2	ethernet1
	08/12 14:43:30	end	tap-zone	tap-zone	5.5.5.5	5.5.5.1	1063	80	tcp	web-browsing	allow	rule2	ethernet1
	08/12 14:43:30	end	tap-zone	tap-zone	192.168.10.12	192.168.10.255	138	138	udp	netbios-dg	allow	rule2	ethernet1
	08/12 14:43:30	end	tap-zone	tap-zone	192.168.10.12	192.168.10.255	137	137	udp	netbios-ns	allow	rule2	ethernet1
	08/12 14:43:30	end	tap-zone	tap-zone	172.16.8.40	64.15.206.217	43455	3478	udp	stun	allow	rule2	ethernet1
	08/12 14:43:30	end	tap-zone	tap-zone	172.16.8.40	216.34.130.245	43455	3478	udp	stun	allow	rule2	ethernet1
	08/12 14:43:30	end	tap-zone	tap-zone	172.16.8.40	66.35.251.201	43455	3478	udp	stun	allow	rule2	ethernet1

Page: 1 2 3 4 5 6 7 8 9 10

Figure 129. Configuration Log Page

Each log page has a filter area at the top of the page.



Filter: (host in 10.0.0.252) and (result eq Succeeded)

2. 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 **Succeeded** in the **Result** column in the Figure 129, both items are added, and the search will find entries that match both (AND search). Click the **Apply Filter** button to display the filtered list.

- 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.*

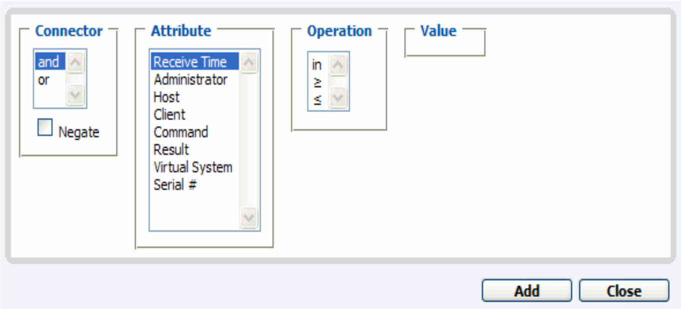


Figure 130. Add Filter Expression Page

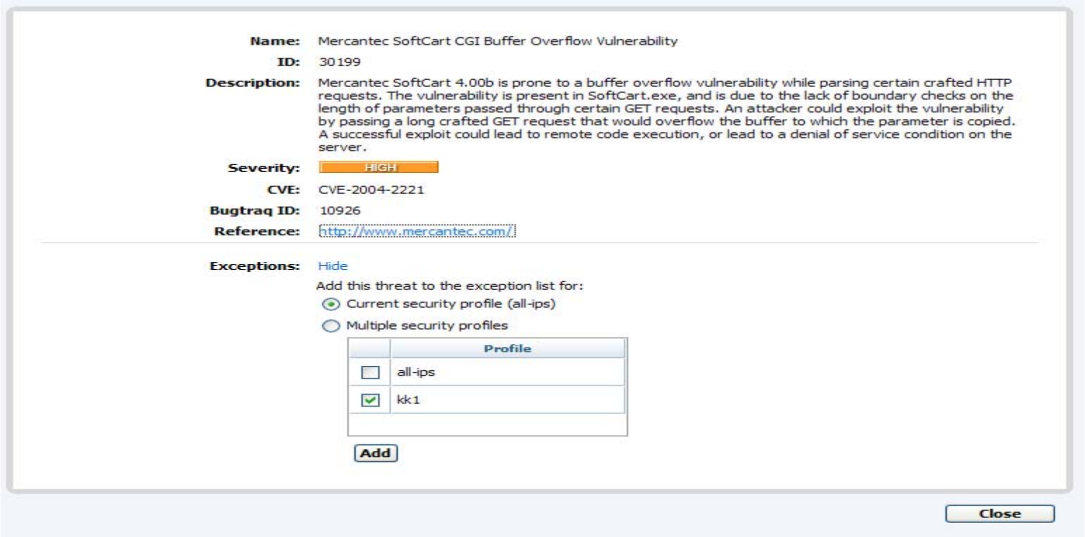
- To clear filters and redisplay the unfiltered list, click the **Clear Filter** button.
- To save your selections as a new filter, click the **Save Filter** button, enter a name for the filter, and click **OK**.
- To export the current log listing (as shown on the page, including any applied filters) 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**.

3. 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 secs, 10 secs, or Manual). To change the number of log entries per page, select the number of rows from the **Rows** drop-down list.

4. 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 ⏮.

5. 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 a**nd 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 “Defining Security Profiles” on page 164.



Name: Mercantec SoftCart CGI Buffer Overflow Vulnerability

ID: 30199

Description: Mercantec SoftCart 4.00b is prone to a buffer overflow vulnerability while parsing certain crafted HTTP requests. The vulnerability is present in SoftCart.exe, and is due to the lack of boundary checks on the length of parameters passed through certain GET requests. An attacker could exploit the vulnerability by passing a long crafted GET request that would overflow the buffer to which the parameter is copied. A successful exploit could lead to remote code execution, or lead to a denial of service condition on the server.

Severity: HIGH

CVE: CVE-2004-2221

Bugtraq ID: 10926

Reference: http://www.mercantec.com/

Exceptions: Hide

Add this threat to the exception list for:

● Current security profile (all-ips)

○ Multiple security profiles

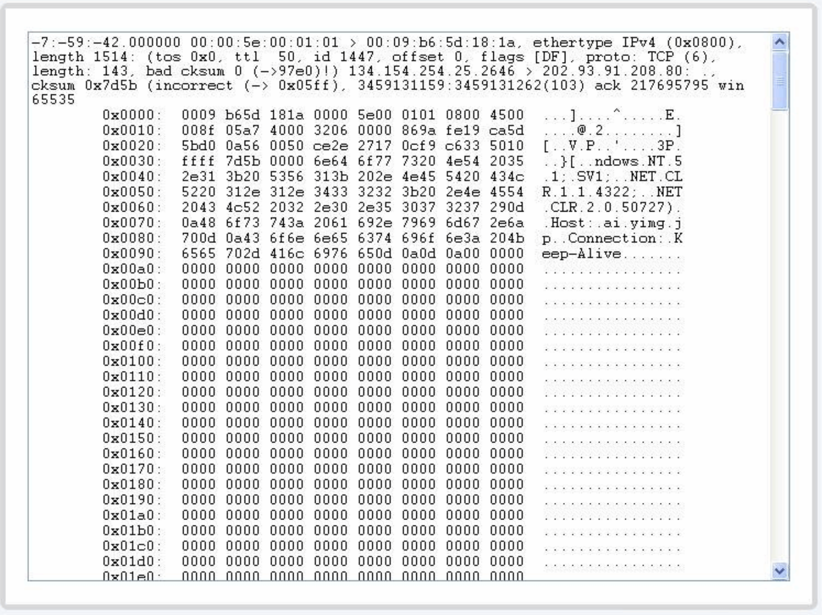
	Profile
□	all-ips
☑	kk1

Figure 131. Log Entry Details

6. 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. Refer to “Defining Addresses” on page 193 for information on assigning IP to address name mappings.

7. Review the following information in each log.

Table 87. Log Descriptions

Chart	Description
Traffic	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”.
Threat	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 “Defining Anti-Spyware Profiles” on page 168 and “Defining Vulnerability Protection Profiles” on page 174. 

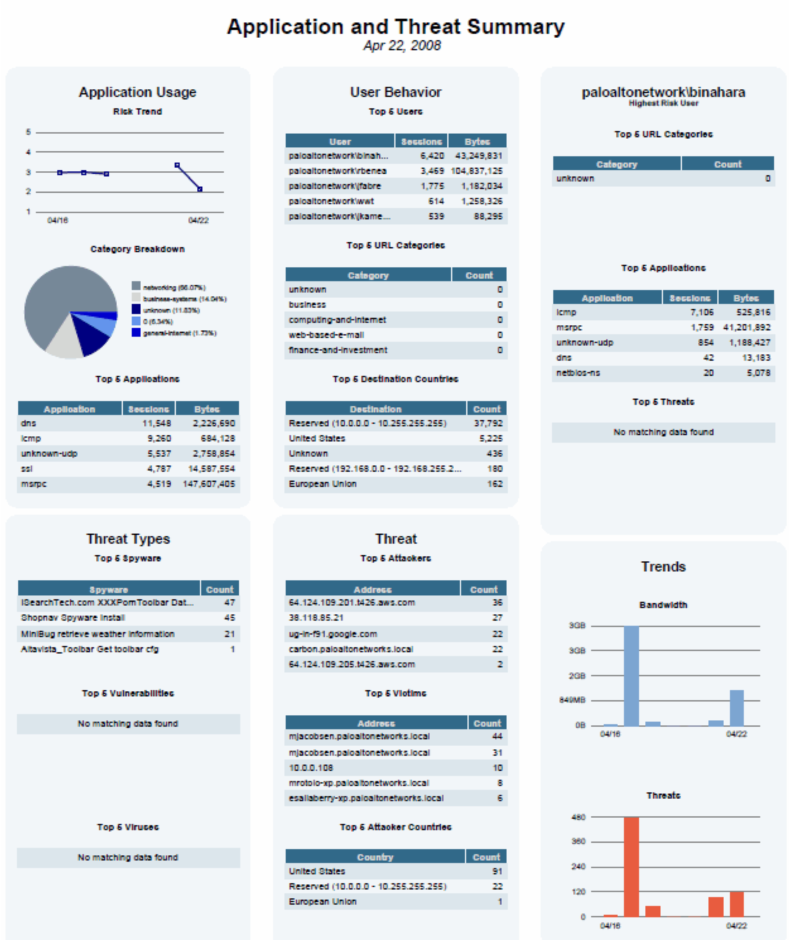
```
-7:-59:-42.000000 00:00:5e:00:01:01 > 00:09:b6:5d:18:1a, ethertype IPv4 (0x0800),
length 1514: (tos 0x0, ttl  50, id 1447, offset 0, flags [DF], proto: TCP (6),
length: 143, bad cksum 0 (->97e0)!) 134.154.254.25.2646 > 202.93.91.208.80: .,
cksum 0x7d5b (incorrect (-> 0x05ff), 3459131159:3459131262(103) ack 217695795 win
65535
        0x0000:  0009 b65d 181a 0000 5e00 0101 0800 4500  ...]....^.....E.
        0x0010:  008f 05a7 4000 3206 0000 869a fe19 ca5d  ....@.2........]
        0x0020:  5bd0 0a56 0050 ce2e 2717 0cf9 c633 5010  [..V.P..'....3P.
        0x0030:  ffff 7d5b 0000 6e64 6f77 7320 4e54 2035  ..}[..ndows.NT.5
        0x0040:  2e31 3b20 5356 313b 202e 4e45 5420 434c  .1;.SV1;..NET.CL
        0x0050:  5220 312e 312e 3433 3232 3b20 2e4e 4554  R.1.1.4322;..NET
        0x0060:  2043 4c52 2032 2e30 2e35 3037 3237 290d  .CLR.2.0.50727).
        0x0070:  0a48 6f73 743a 2061 692e 7969 6d67 2e6a  .Host:.ai.yimg.j
        0x0080:  700d 0a43 6f6e 6e65 6374 696f 6e3a 204b  p..Connection:.K
        0x0090:  6565 702d 416c 6976 650d 0a0d 0a00 0000  eep-Alive.......
        0x00a0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x00b0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x00c0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x00d0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x00e0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x00f0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0100:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0110:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0120:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0130:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0140:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0150:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0160:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0170:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0180:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0190:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x01a0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x01b0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x01c0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x01d0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x01e0:  0000 0000 0000 0000 0000 0000 0000 0000
```

Table 87. Log Descriptions (Continued)

Chart	Description
URL Filtering	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 “Defining URL Filtering Profiles” on page 178 for information on defining URL filtering profiles.
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 188 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 “System Setup and Configuration Management” on page 40 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

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.



Application and Threat Summary

Apr 22, 2008

Application Usage

Top 5 Applications

Application	Sessions	Bytes
dns	11,548	2,226,690
icmp	9,260	684,128
unknown-udp	5,537	2,758,854
ssl	4,787	14,587,554
msrpc	4,519	147,607,405

User Behavior

Top 5 Users

User	Sessions	Bytes
paloaltonetwork\binah...	6,420	43,249,831
paloaltonetwork\rbenea	3,469	104,837,125
paloaltonetwork\jfabre	1,775	1,182,034
paloaltonetwork\wwt	614	1,258,326
paloaltonetwork\jkame...	539	88,295

Top 5 URL Categories

Category	Count
unknown	0
business	0
computing-and-internet	0
web-based-e-mail	0
finance-and-investment	0

Top 5 Destination Countries

Destination	Count
Reserved (10.0.0.0 - 10.255.255.255)	37,792
United States	5,225
Unknown	436
Reserved (192.168.0.0 - 192.168.255.2...	180
European Union	162

paloaltonetwork\binahara

Highest Risk User

Top 5 URL Categories

Category	Count
unknown	0

Top 5 Applications

Application	Sessions	Bytes
icmp	7,106	525,816
msrpc	1,759	41,201,892
unknown-udp	854	1,188,427
dns	42	13,183
netbios-ns	20	5,078

Top 5 Threats

No matching data found

Threat Types

Top 5 Spyware

Spyware	Count
ISearchTech.com XXXPornToolbar Dat...	47
Shopnav Spyware Install	45
MiniBug retrieve weather information	21
Altavista_Toolbar Get toolbar cfg	1

Top 5 Vulnerabilities

No matching data found

Top 5 Viruses

No matching data found

Threat

Top 5 Attackers

Address	Count
64.124.109.201.t426.aws.com	36
38.118.85.21	27
ug-in-f91.google.com	22
carbon.paloaltonetworks.local	22
64.124.109.205.t426.aws.com	2

Top 5 Victims

Address	Count
mjacobsen.paloaltonetworks.local	44
mjacobsen.paloaltonetworks.local	31
10.0.0.108	10
mrotolo-xp.paloaltonetworks.local	8
esallaberry-xp.paloaltonetworks.local	6

Top 5 Attacker Countries

Country	Count
United States	91
Reserved (10.0.0.0 - 10.255.255.255)	22
European Union	1

Figure 132. PDF Summary Report

To create PDF summary reports:

1. Under the **Monitor** tab, click **Manage PDF Summary**.
2. Click **New**.

   The Manage PDF Summary Reports page opens to show all of the available report elements.

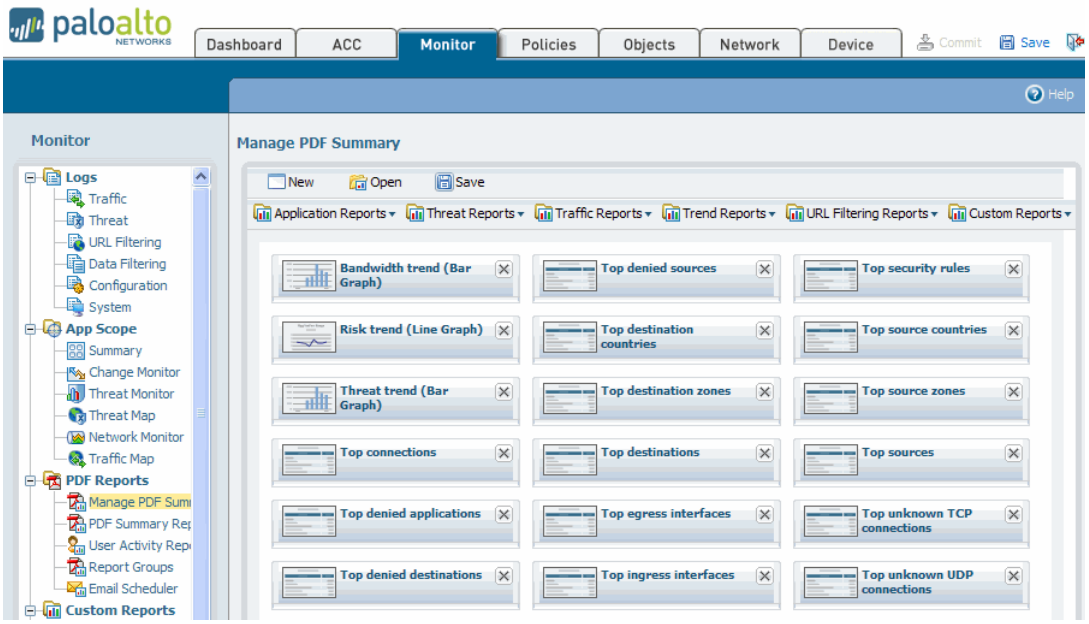


Figure 133. Managing PDF Reports

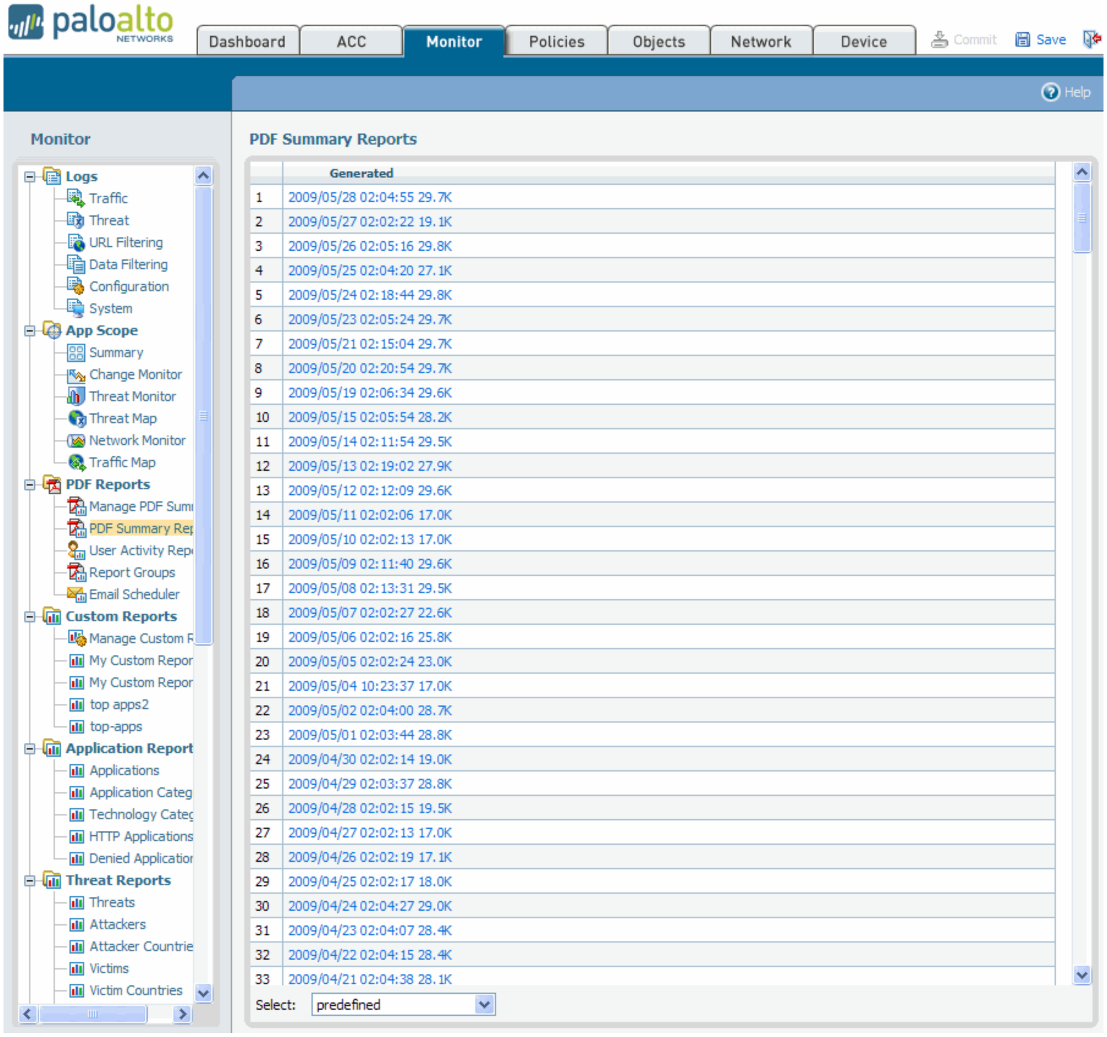
3. Use one or more of these options to design the report:
   - To remove an element from the report, click the **X** in the upper-right corner of the element’s icon box or remove the check box from the item in the appropriate drop-down list box near the top of the page.
   - Select additional elements 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.

4. Click **Save**.
5. Enter a name for the report, as prompted, and click **OK**.

To display PDF reports:

1. Under the **Monitor** tab, click **PDF Summary Report**.



PDF Summary Reports

	Generated
1	2009/05/28 02:04:55 29.7K
2	2009/05/27 02:02:22 19.1K
3	2009/05/26 02:05:16 29.8K
4	2009/05/25 02:04:20 27.1K
5	2009/05/24 02:18:44 29.8K
6	2009/05/23 02:05:24 29.7K
7	2009/05/21 02:15:04 29.7K
8	2009/05/20 02:20:54 29.7K
9	2009/05/19 02:06:34 29.6K
10	2009/05/15 02:05:54 28.2K
11	2009/05/14 02:11:54 29.5K
12	2009/05/13 02:19:02 27.9K
13	2009/05/12 02:12:09 29.6K
14	2009/05/11 02:02:06 17.0K
15	2009/05/10 02:02:13 17.0K
16	2009/05/09 02:11:40 29.6K
17	2009/05/08 02:13:31 29.5K
18	2009/05/07 02:02:27 22.6K
19	2009/05/06 02:02:16 25.8K
20	2009/05/05 02:02:24 23.0K
21	2009/05/04 10:23:37 17.0K
22	2009/05/02 02:04:00 28.7K
23	2009/05/01 02:03:44 28.8K
24	2009/04/30 02:02:14 19.0K
25	2009/04/29 02:03:37 28.8K
26	2009/04/28 02:02:15 19.5K
27	2009/04/27 02:02:13 17.0K
28	2009/04/26 02:02:19 17.1K
29	2009/04/25 02:02:17 18.0K
30	2009/04/24 02:04:27 29.0K
31	2009/04/23 02:04:07 28.4K
32	2009/04/22 02:04:15 28.4K
33	2009/04/21 02:04:38 28.1K

Select: predefined

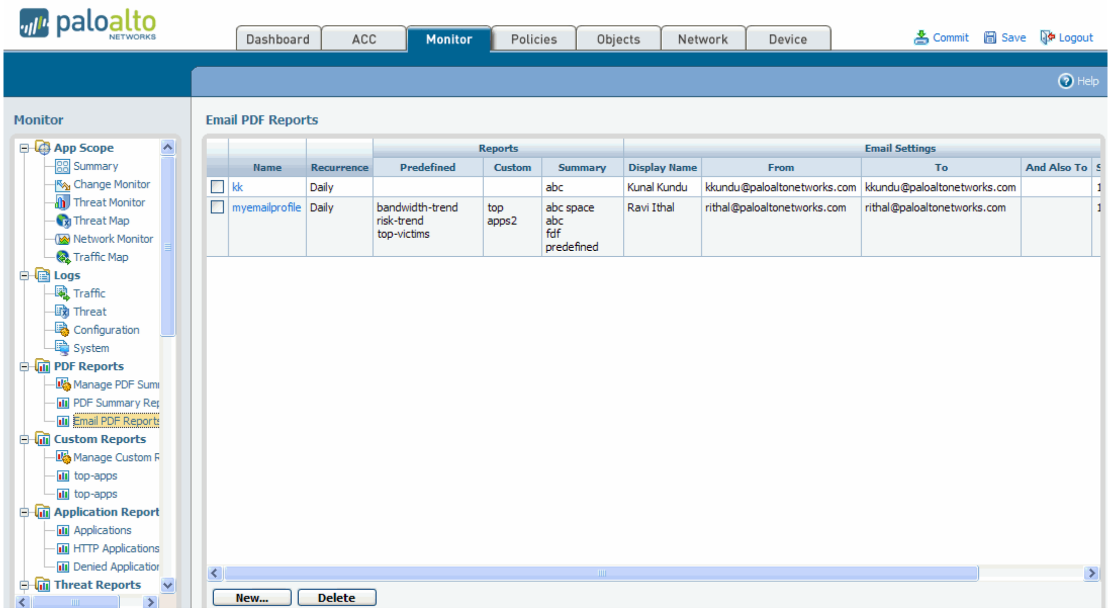
Figure 134. Selecting PDF Reports to Display

2. Select a report type from the drop-down list at the bottom of the page to display the generated reports of that type.

3. Click an underlined report link to open or save the report (see Figure 132 for a sample report).

To schedule email delivery of reports:

1. Under the **Monitor** tab, click **Email Scheduler**.



Email PDF Reports

			Reports			Email Settings				
	Name	Recurrence	Predefined	Custom	Summary	Display Name	From	To	And Also To	S
□	kk	Daily			abc	Kunal Kundu	kkundu@paloaltonetworks.com	kkundu@paloaltonetworks.com		1
□	myemailprofile	Daily	bandwidth-trend risk-trend top-victims	top apps2	abc space abc fdf predefined	Ravi Ithal	rithal@paloaltonetworks.com	rithal@paloaltonetworks.com		1

Figure 135. Email Scheduler Page

2. Click the link for a report to display the email options, or click **New** to create a new email schedule.

3. Specify the following information.

Table 88. Email Scheduler Settings

Field	Description
Name	Enter a name to identify the schedule.
Report	Select the report to email from the drop-down list.
Recurrence	Select a recurrence option from the drop-down list. You can order email delivery daily or weekly on a specified day of the week.
Email Profile	Select an email profile from the drop-down list, or click **New** to create a new profile. Follow the instructions in “Defining Email Notification Profiles” on page 84.
Override Recipient Email(s)	Specify additional recipient email addresses that are not included in the email profile.

4. Click **OK** to save and activate the schedule. 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.

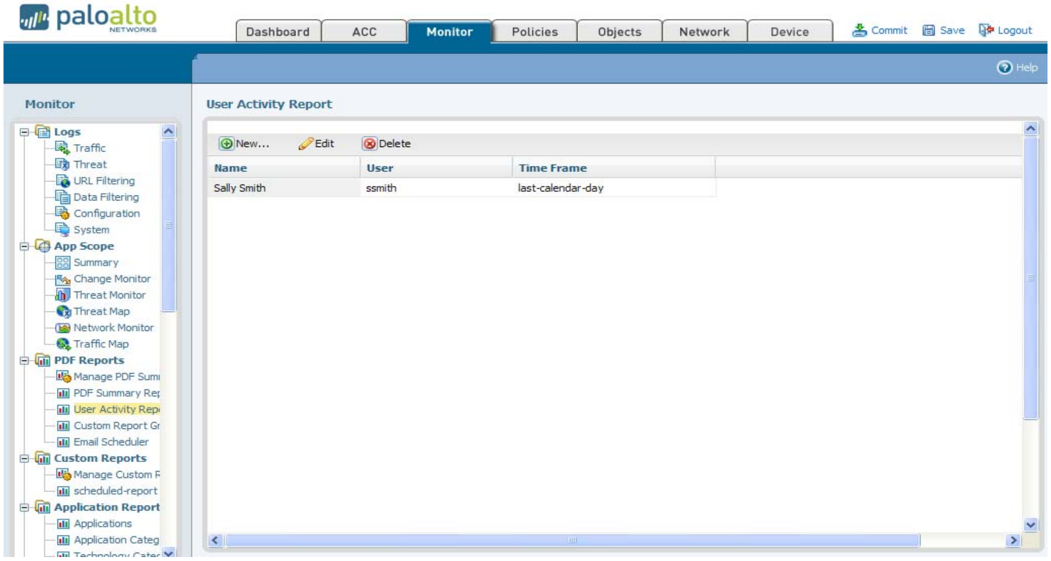
Managing User Activity Reports

You can define reports that summarize the activity of individual users.

To manage user activity reports:

1. Under the **Monitor** tab, click **User Activity Reports**.

   The User Activity Reports page opens to show all of the available report elements.



Name	User	Time Frame
Sally Smith	ssmith	last-calendar-day

Figure 136. Managing User Activity Reports

2. To create a new report:

   a. Click **New**.

   b. Specify the following information.

Table 89. User Activity Report Settings

Field	Description
Name	Enter a name to identify the report.
User	Enter the user name or IP address (IPv4 or IPv6) of the user who will be the subject of the report.
Time frame	Select the time frame for the report from the drop-down list.

   c. Click **OK** to add the report.

3. To run the report on demand, select the report and click **Edit**, and then click **Run**.

4. To delete the report, select the report and click **Delete**. Click **OK** to confirm.

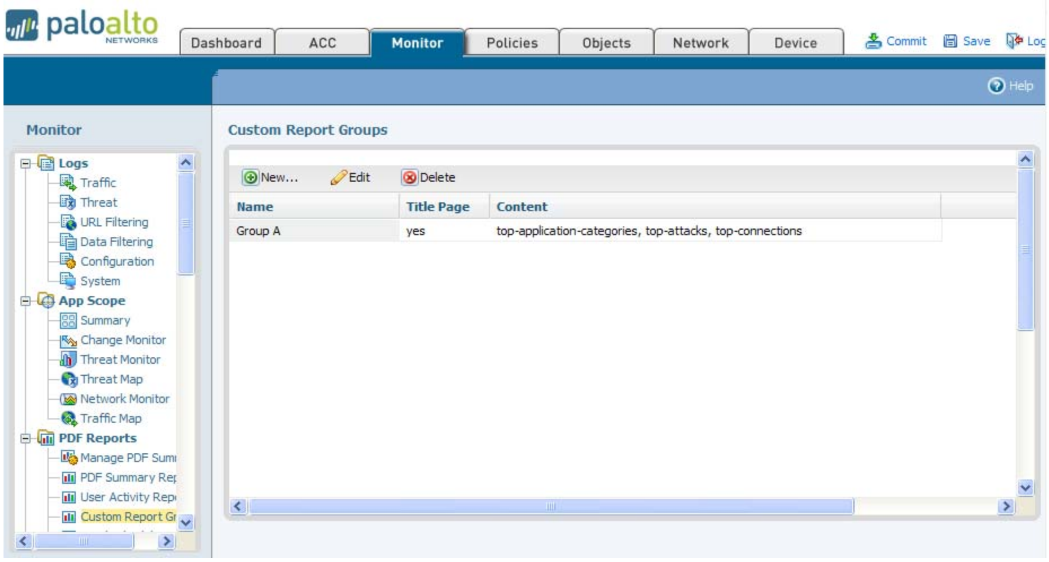
Managing Report Groups

Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with a optional title page and all the constituent reports included.

To manage user activity reports:

1. Under the **Monitor** tab, click **Report Groups**.

   The User Activity Reports page opens to show all of the available report elements.



Name	Title Page	Content
Group A	yes	top-application-categories, top-attacks, top-connections

Figure 137. Managing Custom Reports

2. To create a new report group:

   a. Click **New**.

   b. Specify the following information.

Table 90. Report Group Settings

Field	Description
Report Group Name	Enter a name to identify the report.
Title Page	Select the check box to include a title page in the report.
Custom Title	Enter the name that will appear as the report title.
Report selection	Select reports from the left column and click **Add** to move each to the report group on the right.

   c. Click **OK** to add the report group.

3. To edit a report group, select the group and click **Edit**.

4. To delete the report group, select the group and click **Delete**. Click **OK** to confirm.

To use the report group, refer to “Scheduling Reports for Email Delivery” in the next section.

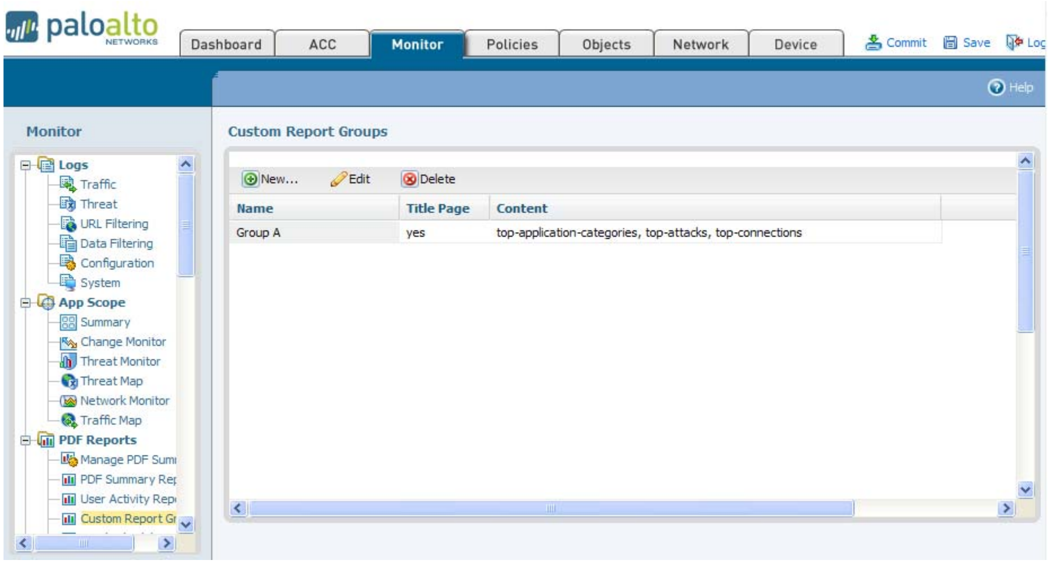
Scheduling Reports for Email Delivery

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 239 and “Defining Email Notification Profiles” on page 84.

To schedule report delivery:

1. Under the **Monitor** tab, click **Email Scheduler**

   The User Activity Reports page opens to show all of the available report elements.



Name	Title Page	Content
Group A	yes	top-application-categories, top-attacks, top-connections

Figure 138. Email Scheduler

2. To create a new report group:

   a. Click **New**.

   b. Specify the following information.

Table 91. Email Scheduler Settings

Field	Description
Name	Enter a name to identify the schedule.
Report Group	Select the report group (refer to “Managing Report Groups” on page 239).
Recurrence	Select the frequency at which to generate and send the report.
Email Profile	Select the profile that defines the email settings. Refer to “Defining Email Notification Profiles” on page 84 for information on defining email profiles.
Override Recipient email(s)	Enter an optional email address to use instead of the recipient specified in the email profile.

   c. Click **OK** to add the schedule.

3. To edit an email schedule, select the schedule and click **Edit**.

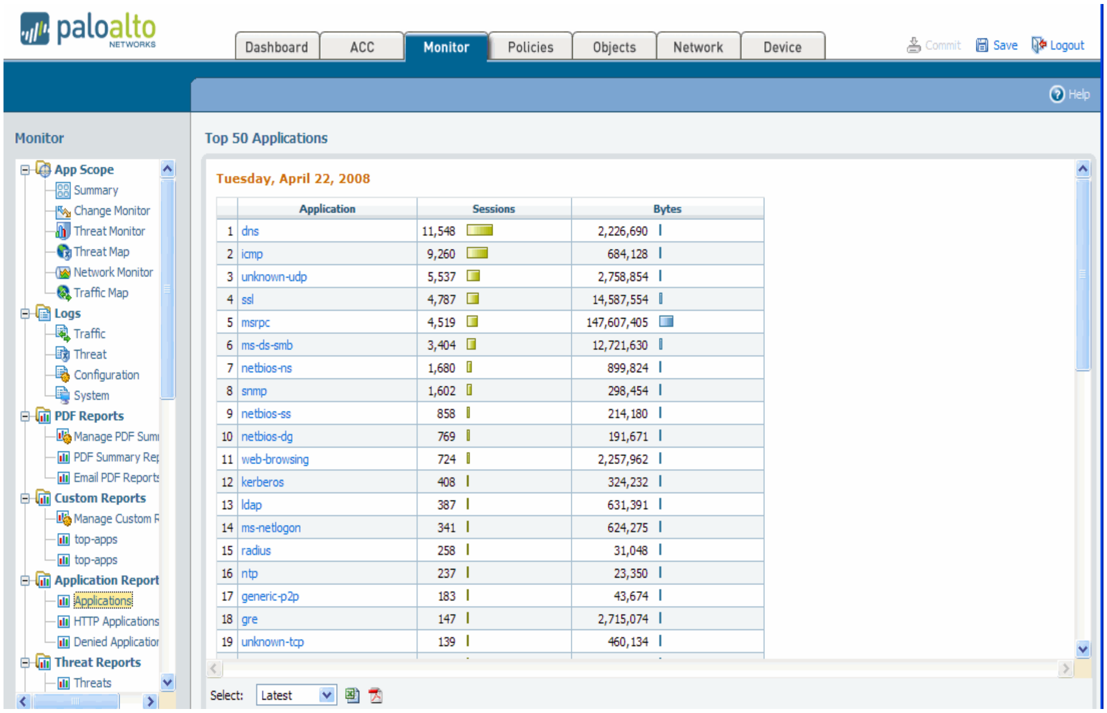
4. To delete an email schedule, select the schedule and click **Delete**. Click **OK** to confirm.

Viewing Reports

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:

1. Under the **Monitor** tab, click the report names on the left side of the page.



Top 50 Applications

Tuesday, April 22, 2008

	Application	Sessions	Bytes
1	dns	11,548	2,226,690
2	icmp	9,260	684,128
3	unknown-udp	5,537	2,758,854
4	ssl	4,787	14,587,554
5	msrpc	4,519	147,607,405
6	ms-ds-smb	3,404	12,721,630
7	netbios-ns	1,680	899,824
8	snmp	1,602	298,454
9	netbios-ss	858	214,180
10	netbios-dg	769	191,671
11	web-browsing	724	2,257,962
12	kerberos	408	324,232
13	ldap	387	631,391
14	ms-netlogon	341	624,275
15	radius	258	31,048
16	ntp	237	23,350
17	generic-p2p	183	43,674
18	gre	147	2,715,074
19	unknown-tcp	139	460,134

Figure 139. Top Applications Report Page

2. 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.

3. The reports are listed in sections. Review the following information in each report for the selected time period.

Table 92. Report Descriptions

Report	Description
Application Reports	
Applications	Number of sessions for each of the top 50 applications that had the most sessions.
HTTP Applications	Number of sessions for each of the top 50 HTTP applications that had the most sessions.
Denied Applications	Number of sessions denied for each of the top 50 denied applications.
Threat Reports	
Threats	Number of threats detected, if any, for each of the top 50 threats. Threats include malware attacks and URL filtering profile violations.
Attackers	Number of sessions for the top 50 attacking hosts.
Victims	Number of sessions for the top 50 attacked hosts.
Victim Countries	Number of sessions for the top 50 attacked countries.
Viruses	Number of sessions for the top 50 viruses detected.
Spyware	Number of sessions for the top 50 spyware programs detected.
Vulnerabilities	Number of sessions for the top 50 detected attempts to exploit known vulnerabilities.
URL Filtering Reports	
Security Rules	Number of times each of the top 50 security policy rules was applied to a session.
URL Categories	Number of sessions that accessed web sites in the top 50 URL categories (requires a URL filtering license).
URL Users	Number of sessions that accessed web sites in the top 50 URL categories according to user (requires a URL filtering license).
URL User Behavior	Number of sessions that accessed web sites in the top 50 URL categories according to user, with the type of activity (such as chat or web-based email) listed (requires a URL filtering license).
Web Sites	Number of sessions that accessed the top 50 web sites in URL filter categories that are blocked or generate alerts (requires a URL filtering license).
Blocked Categories	Number of sessions that were blocked from accessing web sites in the top 50 URL categories (requires a URL filtering license).
Blocked Users	Number of sessions that were blocked from accessing web sites in the top 50 URL categories according to user (requires a URL filtering license).
Blocked User Behavior	Number of sessions that were blocked from accessing web sites in the top 50 URL categories according to user, with the type of activity (such as chat or web-based email) listed (requires a URL filtering license).
Blocked Sites	Number of sessions that were blocked from accessing the top 50 web sites in URL filter categories (requires a URL filtering license).

Table 92. Report Descriptions (Continued)

Report	Description
Traffic Reports	
Security Rules	Number of sessions established according to each of the top 50 security rules.
Sources	Number of sessions established by each of the top 50 source IP addresses.
Source Countries	Number of sessions established by each of the top 50 source countries.
Destinations	Number of sessions established to each of the top 50 destination IP addresses.
Destination Countries	Number of sessions established to each of the top 50 destination countries.
Connections	Number of sessions established by each of the top 50 pairs of source and destination IP addresses.
Source Zones	Number of sessions established from each of the top 50 source zones.
Destination Zones	Number of sessions established to each of the top 50 destination zones.
Ingress Interfaces	Number of sessions established from each of the top 50 ingress interfaces.
Egress Interfaces	Number of sessions established to each of the top 50 egress interfaces.
Denied Sources	Number of sessions denied for each of the top 50 denied source IP addresses. The source host name is also shown, if available.
Denied Destinations	Number of sessions denied for each of the top 50 denied destination IP addresses. The destination host name is also shown, if available.
Attacker Countries	Number of sessions denied for each of the top 50 attacker countries
Unknown TCP Sessions	Number of sessions for the top 50 unknown TCP applications, including source and destination zones, addresses, and ports for each session.
Unknown UDP Sessions	Number of sessions for the top 50 unknown UDP applications, including source and destination zones, addresses, and ports for each session.

4. To export the log in CSV format, click **Export to CSV**. 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**.

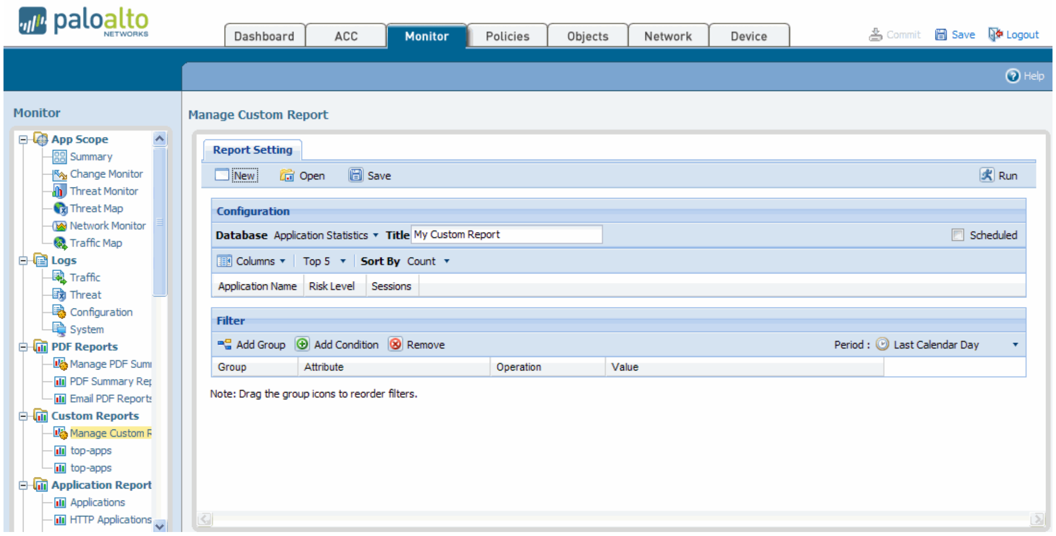
5. To open the log information in PDF format, click **Export to PDF**. The PDF file opens in a new window. Click the icons at the top of the window to print or save the file.

Generating Custom Reports

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:

1. Under the **Monitor** tab, click **Manage Custom Reports** in the Custom Reports section.
2. 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.



Manage Custom Report

Configuration

Database Application Statistics ▾ Title My Custom Report □ Scheduled

Columns ▾ Top 5 ▾ Sort By Count ▾

Application Name	Risk Level	Sessions

Filter

Period : Last Calendar Day ▾

Group	Attribute	Operation	Value

Note: Drag the group icons to reorder filters.

Figure 140. Creating a Custom Report

3. Enter a report title.
4. Choose the database for the report from the **Database** drop-down list.
5. 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.
6. Choose the amount of information to include in the report (top 5, 10, 25, or 50), and how to sort the report.
7. Click **Save** to save the report settings.

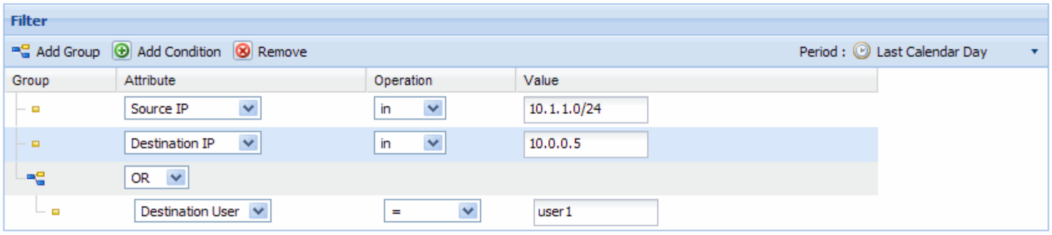
To generate a custom report:

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.

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.s

   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**.



Period : Last Calendar Day

Group	Attribute	Operation	Value
	Source IP	in	10.1.1.0/24
	Destination IP	in	10.0.0.5
	OR		
	Destination User	=	user1

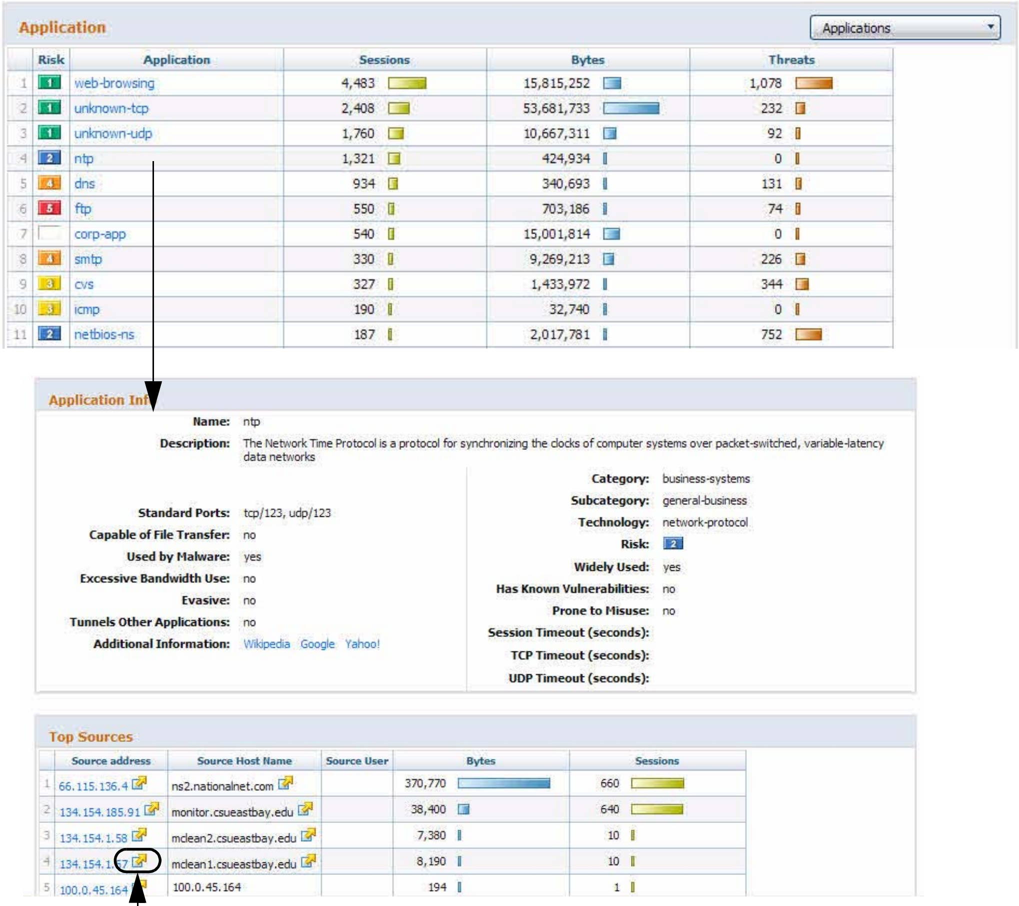
Figure 141. Custom Report Filter Example

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.



Application

Applications ▾

	Risk	Application	Sessions	Bytes	Threats
1	1	web-browsing	4,483	15,815,252	1,078
2	1	unknown-tcp	2,408	53,681,733	232
3	1	unknown-udp	1,760	10,667,311	92
4	2	ntp	1,321	424,934	0
5	4	dns	934	340,693	131
6	5	ftp	550	703,186	74
7		corp-app	540	15,001,814	0
8	4	smtp	330	9,269,213	226
9	3	cvs	327	1,433,972	344
10	3	icmp	190	32,740	0
11	2	netbios-ns	187	2,017,781	752

Application Inf

Name: ntp

Description: The Network Time Protocol is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks

Standard Ports: tcp/123, udp/123

Capable of File Transfer: no

Used by Malware: yes

Excessive Bandwidth Use: no

Evasive: no

Tunnels Other Applications: no

Additional Information: Wikipedia Google Yahoo!

Category: business-systems

Subcategory: general-business

Technology: network-protocol

Risk: 2

Widely Used: yes

Has Known Vulnerabilities: no

Prone to Misuse: no

Session Timeout (seconds):

TCP Timeout (seconds):

UDP Timeout (seconds):

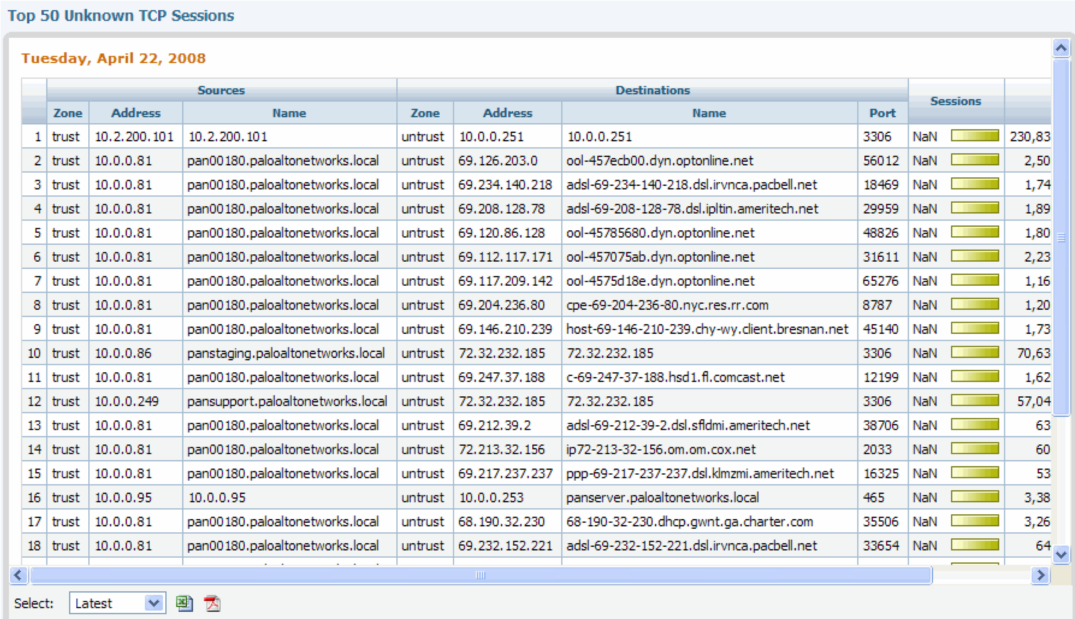
Top Sources

	Source address	Source Host Name	Source User	Bytes	Sessions
1	66.115.136.4	ns2.nationalnet.com		370,770	660
2	134.154.185.91	monitor.csueastbay.edu		38,400	640
3	134.154.1.58	mclean2.csueastbay.edu		7,380	10
4	134.154.1.[illegible]7	mclean1.csueastbay.edu		8,190	10
5	100.0.45.164	100.0.45.164		194	1

Link to look up owner of the address

Figure 142. 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.



Top 50 Unknown TCP Sessions

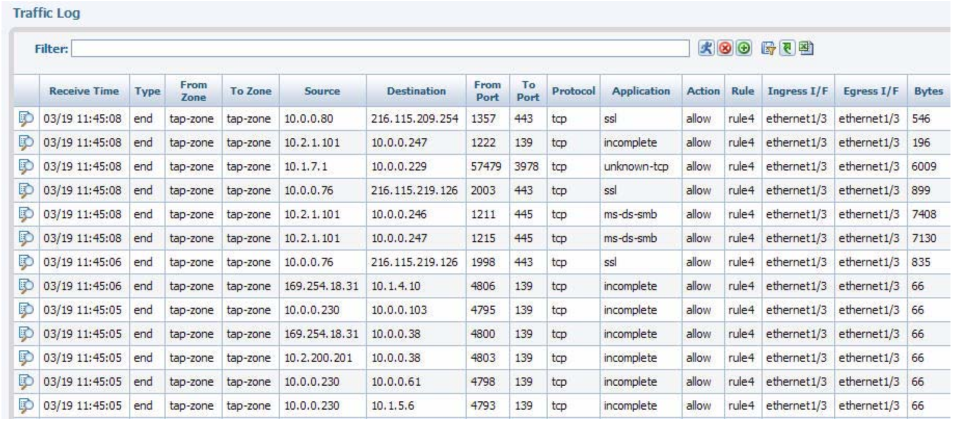
Tuesday, April 22, 2008

	Sources			Destinations				Sessions		
	Zone	Address	Name	Zone	Address	Name	Port			
1	trust	10.2.200.101	10.2.200.101	untrust	10.0.0.251	10.0.0.251	3306	NaN		230,83
2	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.126.203.0	ool-457ecb00.dyn.optonline.net	56012	NaN		2,50
3	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.234.140.218	adsl-69-234-140-218.dsl.irvnca.pacbell.net	18469	NaN		1,74
4	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.208.128.78	adsl-69-208-128-78.dsl.ipltin.ameritech.net	29959	NaN		1,89
5	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.120.86.128	ool-45785680.dyn.optonline.net	48826	NaN		1,80
6	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.112.117.171	ool-457075ab.dyn.optonline.net	31611	NaN		2,23
7	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.117.209.142	ool-4575d18e.dyn.optonline.net	65276	NaN		1,16
8	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.204.236.80	cpe-69-204-236-80.nyc.res.rr.com	8787	NaN		1,20
9	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.146.210.239	host-69-146-210-239.chy-wy.client.bresnan.net	45140	NaN		1,73
10	trust	10.0.0.86	panstaging.paloaltonetworks.local	untrust	72.32.232.185	72.32.232.185	3306	NaN		70,63
11	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.247.37.188	c-69-247-37-188.hsd1.fl.comcast.net	12199	NaN		1,62
12	trust	10.0.0.249	pansupport.paloaltonetworks.local	untrust	72.32.232.185	72.32.232.185	3306	NaN		57,04
13	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.212.39.2	adsl-69-212-39-2.dsl.sfldmi.ameritech.net	38706	NaN		63
14	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	72.213.32.156	ip72-213-32-156.om.om.cox.net	2033	NaN		60
15	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.217.237.237	ppp-69-217-237-237.dsl.klmzmi.ameritech.net	16325	NaN		53
16	trust	10.0.0.95	10.0.0.95	untrust	10.0.0.253	panserver.paloaltonetworks.local	465	NaN		3,38
17	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	68.190.32.230	68-190-32-230.dhcp.gwnt.ga.charter.com	35506	NaN		3,26
18	trust	10.0.0.81	pan00180.paloaltonetworks.local	untrust	69.232.152.221	adsl-69-232-152-221.dsl.irvnca.pacbell.net	33654	NaN		64

Select: Latest

Figure 143. 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.



Traffic Log

Filter:

Receive Time	Type	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Action	Rule	Ingress I/F	Egress I/F	Bytes
03/19 11:45:08	end	tap-zone	tap-zone	10.0.0.80	216.115.209.254	1357	443	tcp	ssl	allow	rule4	ethernet1/3	ethernet1/3	546
03/19 11:45:08	end	tap-zone	tap-zone	10.2.1.101	10.0.0.247	1222	139	tcp	incomplete	allow	rule4	ethernet1/3	ethernet1/3	196
03/19 11:45:08	end	tap-zone	tap-zone	10.1.7.1	10.0.0.229	57479	3978	tcp	unknown-tcp	allow	rule4	ethernet1/3	ethernet1/3	6009
03/19 11:45:08	end	tap-zone	tap-zone	10.0.0.76	216.115.219.126	2003	443	tcp	ssl	allow	rule4	ethernet1/3	ethernet1/3	899
03/19 11:45:08	end	tap-zone	tap-zone	10.2.1.101	10.0.0.246	1211	445	tcp	ms-ds-smb	allow	rule4	ethernet1/3	ethernet1/3	7408
03/19 11:45:08	end	tap-zone	tap-zone	10.2.1.101	10.0.0.247	1215	445	tcp	ms-ds-smb	allow	rule4	ethernet1/3	ethernet1/3	7130
03/19 11:45:06	end	tap-zone	tap-zone	10.0.0.76	216.115.219.126	1998	443	tcp	ssl	allow	rule4	ethernet1/3	ethernet1/3	835
03/19 11:45:06	end	tap-zone	tap-zone	169.254.18.31	10.1.4.10	4806	139	tcp	incomplete	allow	rule4	ethernet1/3	ethernet1/3	66
03/19 11:45:05	end	tap-zone	tap-zone	10.0.0.230	10.0.0.103	4795	139	tcp	incomplete	allow	rule4	ethernet1/3	ethernet1/3	66
03/19 11:45:05	end	tap-zone	tap-zone	169.254.18.31	10.0.0.38	4800	139	tcp	incomplete	allow	rule4	ethernet1/3	ethernet1/3	66
03/19 11:45:05	end	tap-zone	tap-zone	10.2.200.201	10.0.0.38	4803	139	tcp	incomplete	allow	rule4	ethernet1/3	ethernet1/3	66
03/19 11:45:05	end	tap-zone	tap-zone	10.0.0.230	10.0.0.61	4798	139	tcp	incomplete	allow	rule4	ethernet1/3	ethernet1/3	66
03/19 11:45:05	end	tap-zone	tap-zone	10.0.0.230	10.1.5.6	4793	139	tcp	incomplete	allow	rule4	ethernet1/3	ethernet1/3	66

Figure 144. 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
- Request an App-ID from Palo Alto Networks.

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.

Note: *You can use custom signatures in App-ID definitions.*

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 196.
2. Define an application override policy that specifies when the custom application should be invoked. The policy would typically include the IP address of the server running the custom application and a restricted set of source IP addresses or a source zone. Refer to "Defining Application Override Policies" on page 158.

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&cont
ext=adrr&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
&zip=94024&context=adrr&context=adrr Cookie:
JSESSIONID=A41B41A19B7533589D6E88190B7F0B3D.001; specifiedsite.com/
jumpcookie=445461346*google.com/search?q=lava+life&; locale=en_US;
campaign=1; imageNum=2; cfTag_LogSid=9327803497943a1237780204643;
__utma=69052556.1949878616336713500.1238193797.1238193797.1238193797.1;
```

```
__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 {
        a1 {
          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
Keep-Alive: 300 Connection: keep-alive Referer: http://
panqa100.specifiedblog.com/wp-admin/post.php?action=edit&post=1
Cookie: __utma=96731468.235424814.1238195613.1238195613.1238195613.1;
__utmb=96731468; __utmc=96731468;
__utmz=96731468.1238195613.1.1.utmccn=(organic)|utmcsr=google|utmctr=blog+ho
st|utmcmd=organic; wordpressuser_bfbaae4493589d9f388265e737a177c8=panqa100;
wordpresspass_bfbaae4493589d9f388265e737a177c8=c68a8c4eca4899017c58668eacc05
fc2
Content-Type: application/x-www-form-urlencoded Content-Length: 462
user_ID=1&action=editpost&post_author=1&post_ID=1&post_title=Hello+world%21&
post_category%5B%5D=1&advanced_view=1&comment_status=open&post_password=&exc
erpt=&content=Hello+world.%3Cbr+%2F%3E&use_instant_preview=1&post_pingback=1
&prev_status=publish&submit=Save&referredby=http%3A%2F%2Fpanqa100.specifiedb
log.com%2Fwp-admin%2F&post_status=publish&trackback_url=&post_name=hello-
world&post_author_override=1&mm=3&jj=27&aa=2009&hh=23&mn=14&ss=42&metakeyinp
ut=&metavalue=HTTP/1.1
```

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;
            }
          }
        }
      }
    }
  }
}
```

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 SSL VPNs

This chapter describes how configure virtual private networks (VPNs) using Secure Socket Layer (SSL).

- “About SSL VPNs” in the next section
- “Setting Up SSL VPNs” on page 252
- “Downloading and Activating the NetConnect SSL VPN Client” on page 255
- “Configuring Authentication” on page 256
- “Creating a Local User Database” on page 258

About SSL VPNs

The SSL VPN capability allows the firewall to support VPN connections for remote Windows XP and Vista 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.

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 an 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 17 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.*

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 security policies established. If if split tunneling is enabled on the client, the only 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 if split tunneling is enabled on the client, the only 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. Refer to the instructions in this section.
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 91.
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 255.
4. Set up user authentication rules for local or RADIUS authentication, as described in “Configuring Authentication” on page 256.
5. Identify the users that are allowed to access the VPN, as described in “Configuring Authentication” on page 256.
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 “Defining Security Policies” on page 144.

To set up a new SSL VPN:

1. Under the **Network** tab, click **SSL VPN** to open the SSL VPN page.

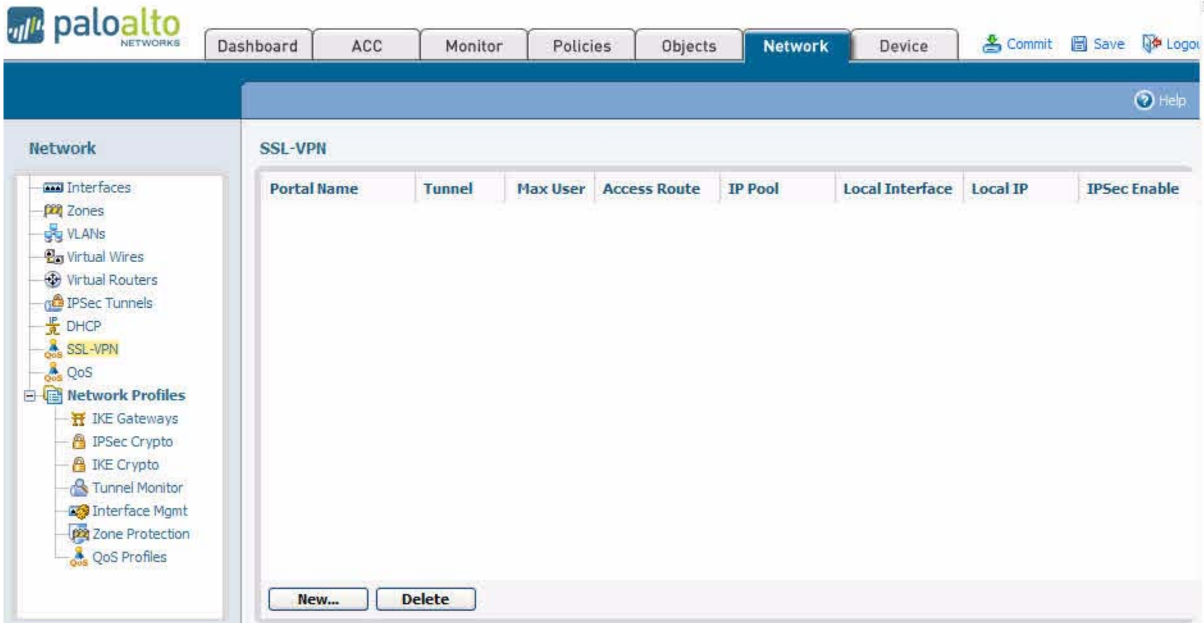


Figure 145. SSL VPN Page

2. To set up a new SSL VPN:

   a. Click **New**.

   b. Configure the following settings on the SSL and Client Configuration tabs. 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.

Table 93. SSL VPN Settings

Field	Description
SSL VPN Configuration	
Portal Name	Enter a name to identify the VPN.
Tunnel Interface	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.
Max User	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.
IPSec Enable	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.

Table 93. SSL VPN Settings (Continued)

Field	Description
Interface	Select the interface to be used for the connection.
IP Address	Choose the IP address that users will specify to access the VPN.
Client Configuration	
Primary DNS Secondary DNS	Enter the IP addresses of the primary and secondary Domain Name Service (DNS) servers that will be used on the clients.
Primary WINS Secondary WINS	Enter the IP addresses of the primary and secondary Windows Name Service (WINS) servers that will be used on the clients.
DNS Suffix	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**.
IP Pool - Subnet/Range	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.
Split Tunnel - Access Route	Use this section to add routes that will be pushed to the remote user's computer and therefore determine what the user's computer will send through the VPN connection. For example, you can set up split tunneling to allow remote users to access the Internet without going through the VPN tunnel. If no route is added, then every request is routed through the tunnel (no split tunneling). In this case, each Internet request passes through the firewall and then out to the network. This method can prevent a possibility of a external party accessing the user's computer and then gaining access to the internal network (with the user's computer acting as bridge). Click **Add** to enter a route. The route order is important because the PC/host will use a first match process. To change the order in which a route is listed, select an entry and click the **Move Up** and **Move Down** buttons. To delete an entry, select it and click **Remove**.

c. Click **OK**.

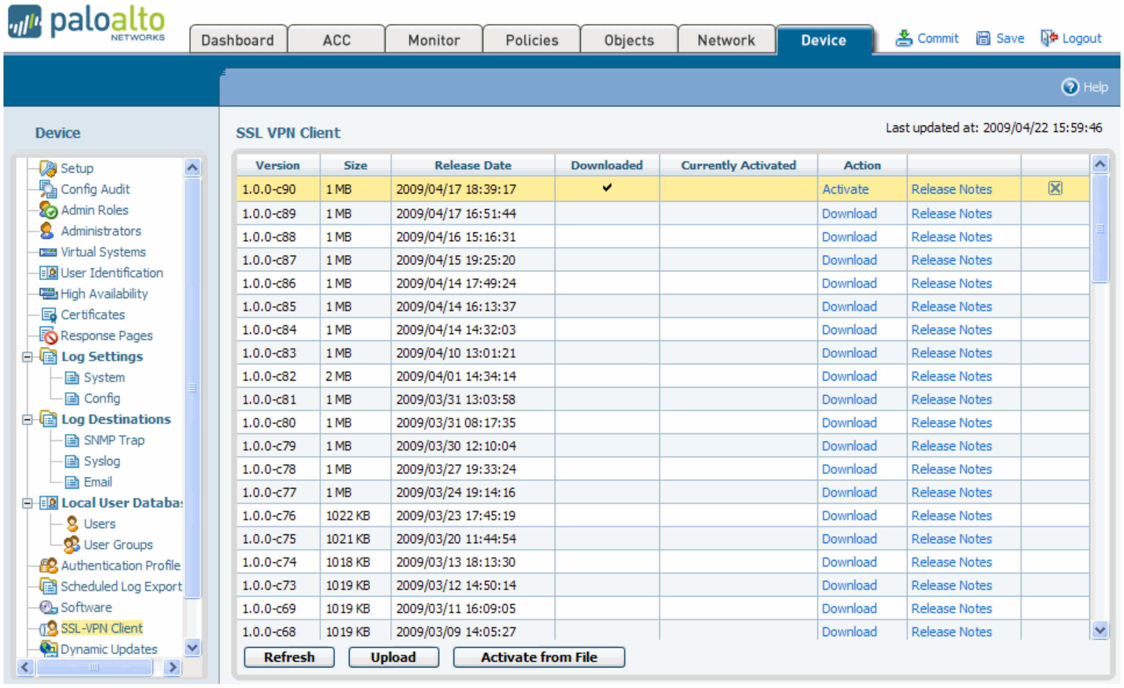
3. To modify the settings, click the user link, make changes, and click **OK**. To delete an entry, select the entry and click **Delete**.

Downloading and Activating the NetConnect SSL VPN Client

When a user 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.

To download and activate the NetConnect SSL VPN client:

1. Under the **Device** tab, click **SSL VPN Client** to display the list of available SSL VPN client releases.



SSL VPN Client

Last updated at: 2009/04/22 15:59:46

Version	Size	Release Date	Downloaded	Currently Activated	Action		
1.0.0-c90	1 MB	2009/04/17 18:39:17	✓		Activate	Release Notes	☒
1.0.0-c89	1 MB	2009/04/17 16:51:44			Download	Release Notes	
1.0.0-c88	1 MB	2009/04/16 15:16:31			Download	Release Notes	
1.0.0-c87	1 MB	2009/04/15 19:25:20			Download	Release Notes	
1.0.0-c86	1 MB	2009/04/14 17:49:24			Download	Release Notes	
1.0.0-c85	1 MB	2009/04/14 16:13:37			Download	Release Notes	
1.0.0-c84	1 MB	2009/04/14 14:32:03			Download	Release Notes	
1.0.0-c83	1 MB	2009/04/10 13:01:21			Download	Release Notes	
1.0.0-c82	2 MB	2009/04/01 14:34:14			Download	Release Notes	
1.0.0-c81	1 MB	2009/03/31 13:03:58			Download	Release Notes	
1.0.0-c80	1 MB	2009/03/31 08:17:35			Download	Release Notes	
1.0.0-c79	1 MB	2009/03/30 12:10:04			Download	Release Notes	
1.0.0-c78	1 MB	2009/03/27 19:33:24			Download	Release Notes	
1.0.0-c77	1 MB	2009/03/24 19:14:16			Download	Release Notes	
1.0.0-c76	1022 KB	2009/03/23 17:45:19			Download	Release Notes	
1.0.0-c75	1021 KB	2009/03/20 11:44:54			Download	Release Notes	
1.0.0-c74	1018 KB	2009/03/13 18:13:30			Download	Release Notes	
1.0.0-c73	1019 KB	2009/03/12 14:50:14			Download	Release Notes	
1.0.0-c69	1019 KB	2009/03/11 16:09:05			Download	Release Notes	
1.0.0-c68	1019 KB	2009/03/09 14:05:27			Download	Release Notes	

Figure 146. SSL VPN Page

2. 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**.

3. 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.

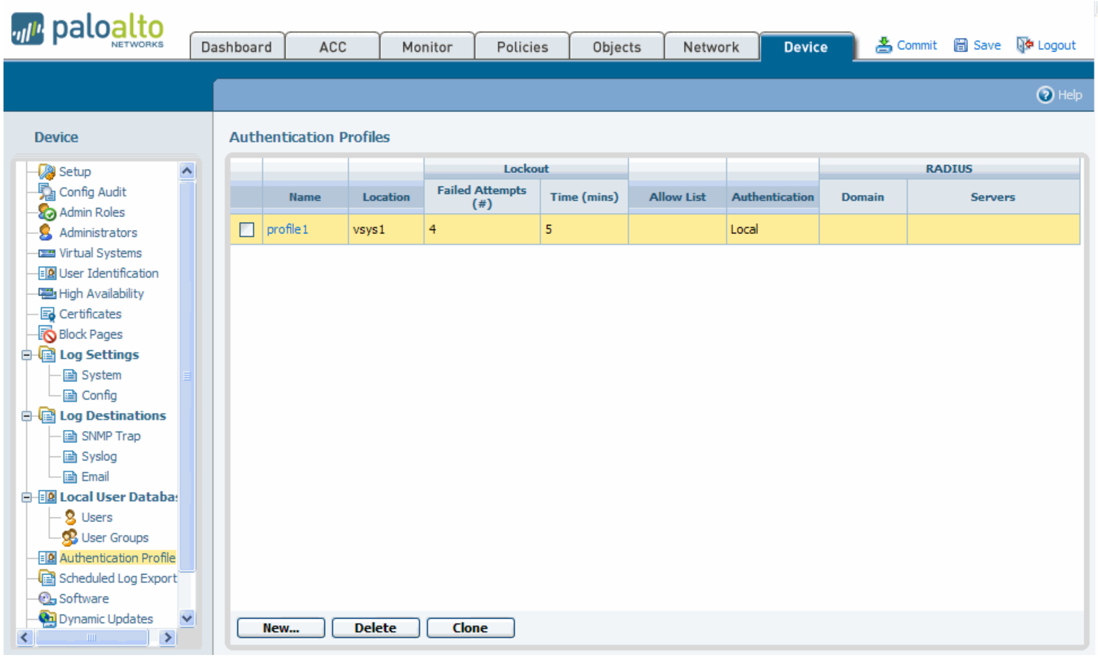
4. To activate the SSL VPN client that was previously uploaded by way of the **Upload** button, click the **Activate from File** button. A pop-up window opens. Select the file from the drop-down list and click **OK**.

5. 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.

Configuring Authentication

To configure authentication for the users who access the VPN:

1. Under the **Device** tab, click **Authentication Profile** to open the Authentication Profiles page.



Authentication Profiles

			Lockout				RADIUS	
	Name	Location	Failed Attempts (#)	Time (mins)	Allow List	Authentication	Domain	Servers
□	profile1	vsys1	4	5		Local		

Figure 147. Authentication Profiles Page

2. To add a new profile:

   a. Click **New**.

   b. Configure the following settings.

Table 94. Authentication Profile Settings

Field	Description
Profile Name	Enter a name to identify the profile.
Virtual System	Select the virtual system from the drop-down list.
Failed Attempts	Enter the number of failed login attempts that are allowed before the account is locked. (1-10, the default is 0). 0 means that there is no limit.
Lockout Time	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 the lockout is in effect until it is manually unlocked.

Table 94. Authentication Profile Settings (Continued)

Field	Description
Allow List	Specify the users and groups that will be explicitly allowed to authenticate. Click **Edit Allow List** 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.
Authentication	Choose the type of authentication to use. • **Local DB**—Use the authentication database on the firewall. • **RADIUS**—Use a Remote Authentication Dial In User Service (RADIUS) server. When you select this option, the following additional **RADIUS** fields are displayed. Enter the following information for each RADIUS server that will be used to provide authentication services (in the preferred order): – **Domain**—Enter the domain of the authentication database if you are connecting to an Active Directory-supported RADIUS server. The domain setting is used if the user does not specify a domain when logging in. – **Name**—Enter a name to identify the server. – **IP address**—Enter the server IP address. – **Secret**—Enter a key to verify and encrypt the connection between the firewall and the RADIUS server.

c. Click **OK**.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

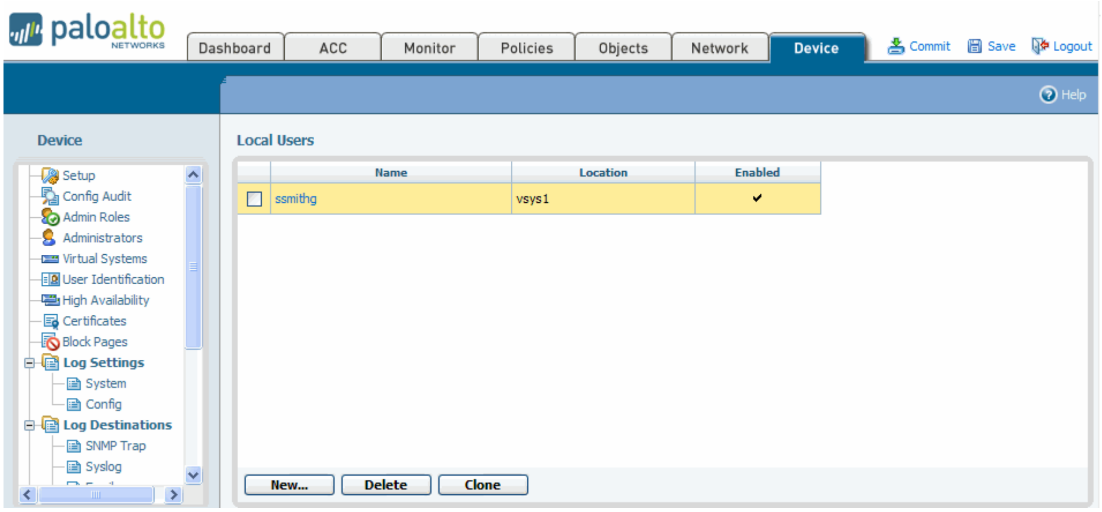
Creating a Local User Database

You can set up a database on the firewall to store authentication information for SSL VPN remote users. You can create users and user groups.

Adding Local Users

To add local users:

1. Under the **Device** tab, click **Local User Database > Users** to open the Local Users page.



	Name	Location	Enabled
□	ssmithg	vsys1	✓

Figure 148. Local Users Page

2. To add a new user:

   a. Click **New**.

   b. Configure the following settings.

Table 95. Local User Settings

Field	Description
Local User Name	Enter a name to identify the user.
Virtual System	Select the virtual system from the drop-down list.
Mode	Use this field to choose the authentication option: • **Password**—Enter and confirm a password for the user. • **Phash**—Enter a hashed password string.
Enabled	Select the check box to activate the user account.

   c. Click **OK**.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

Adding Local User Groups

To add local user groups:

1. Under the **Device** tab, click **Local User Database > User Groups** to open the Local User Groups page.

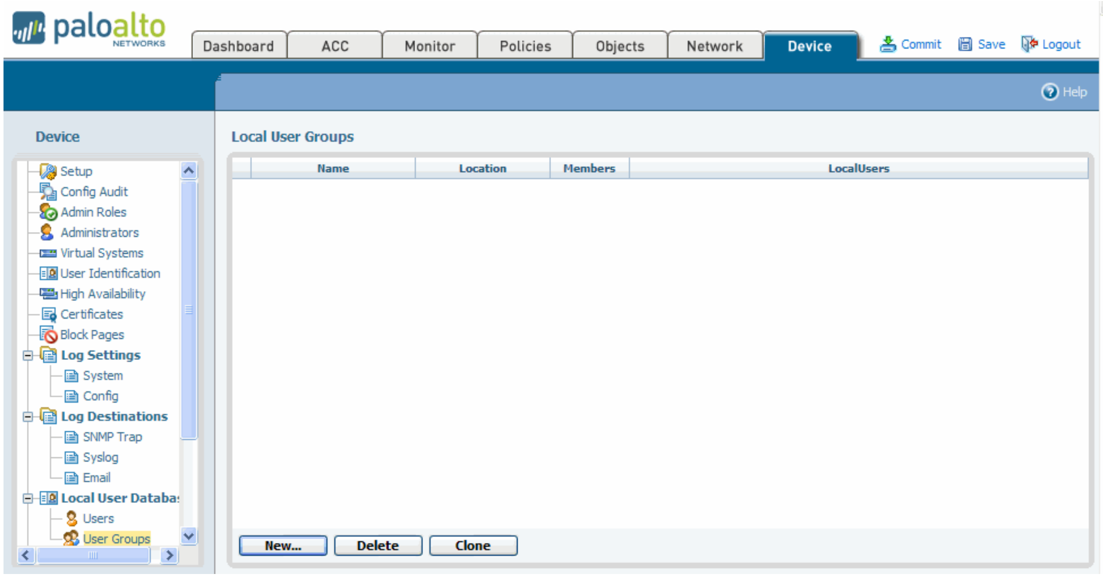


Figure 149. Local User Groups Page

2. To add a new user group:

   a. Click **New**.

   b. Configure the following settings.

Table 96. Local User Group Settings

Field	Description
Local User Group Name	Enter a name to identify the group.
Virtual System	Select the virtual system from the drop-down list.
All Local Users	Select check boxes for the users you want to add to the group.

   c. Click **OK**.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, specify changes, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

Chapter 8

Configuring IPSec Tunnels

This chapter describes how to configure IP Security (IPSec) tunnels on the firewall:

- "About IPSec VPN Support on the Firewall" in the next section
- "Defining IKE Crypto Profiles" on page 263
- "Defining IPSec Crypto Profiles" on page 264
- "Defining Tunnel Monitor Profiles" on page 266
- "Setting Up IPSec Tunnels" on page 268

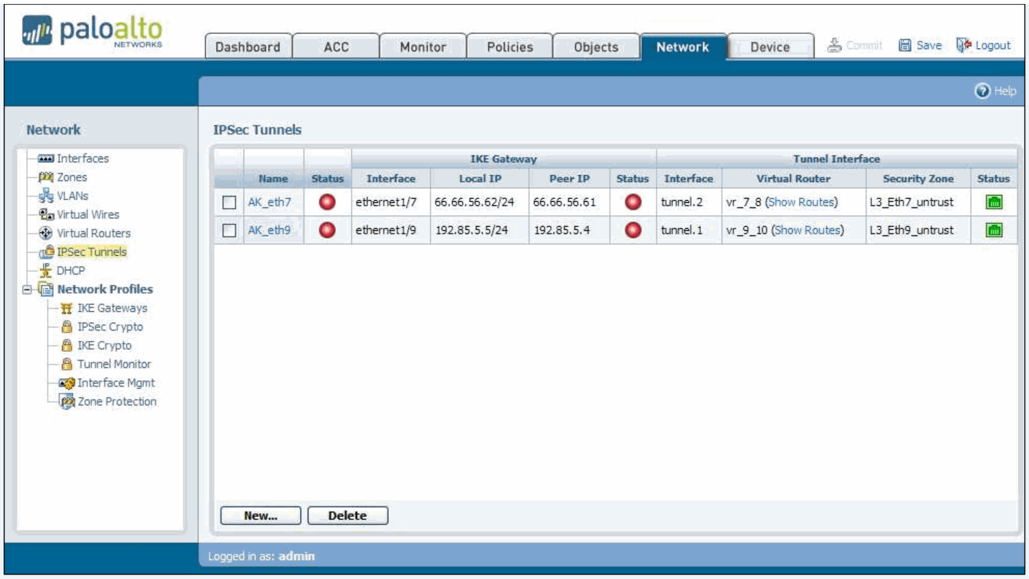
About IPSec VPN Support on the Firewall

IPSec is used in setting up secure tunnels for virtual private network (VPN) traffic, with encryption for TCP/IP packets that are sent through the tunnels.

Note: *Refer to "About Virtual Private Networks" on page 17 for general information on VPNs.*

You can view the status of currently defined IPSec tunnels by opening the IPSec Tunnels page (Figure 150). The following statuses are 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.



IPSec Tunnels

			IKE Gateway				Tunnel Interface			
	Name	Status	Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Security Zone	Status
□	AK_eth7	●	ethernet1/7	66.66.56.62/24	66.66.56.61	●	tunnel.2	vr_7_8 (Show Routes)	L3_Eth7_untrust	🟩
□	AK_eth9	●	ethernet1/9	192.85.5.5/24	192.85.5.4	●	tunnel.1	vr_9_10 (Show Routes)	L3_Eth9_untrust	🟩

Figure 150. IPSec Tunnels Page

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.

The following tasks are required to configure IPSec on the firewall:

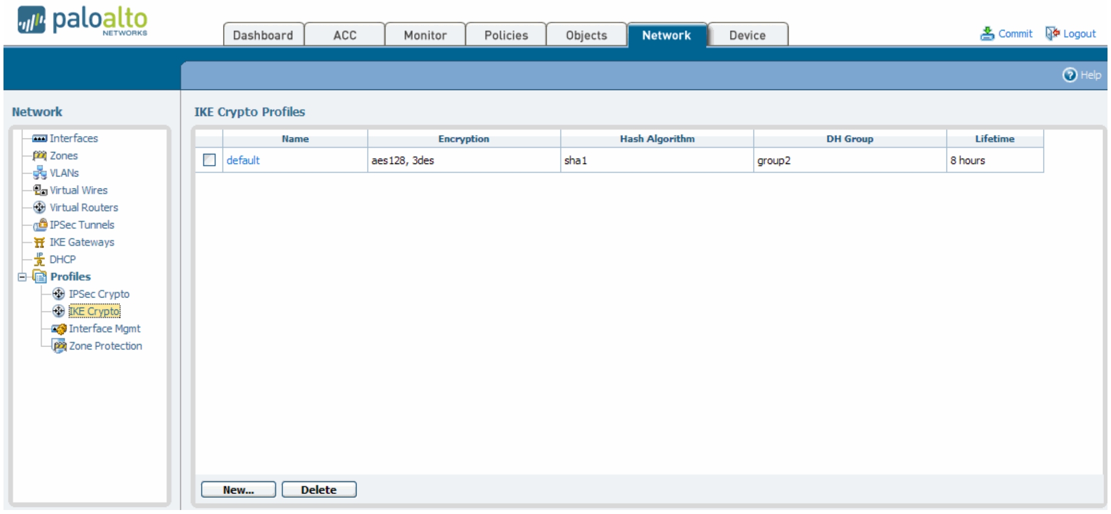
- **Create IKE crypto profiles**—Configure the protocols and algorithms for identification, authentication, and encryption in VPN tunnels using Internet Key Exchange (IKE) Security Association (SA) negotiation (IKEv1 Phase-1). Refer to “Defining IPSec Crypto Profiles” on page 264.
- **Create IPSec crypto profiles**—Configure the protocols and algorithms for identification, authentication, and encryption in the VPN tunnels using IPSec SA negotiation (IKEv1 Phase-2). Refer to “Defining IPSec Crypto Profiles” on page 264.
- **Set up IPSec tunnels**—Configure the parameters that are needed to establish IPSec VPN tunnels. Refer to “Setting Up IPSec Tunnels” on page 268.
- **Define tunnel monitoring profiles**—Specify how the firewall will monitor IPSec tunnels. Refer to “Defining Tunnel Monitor Profiles” on page 266.

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 17 for more information.

To set up IKE crypto profiles:

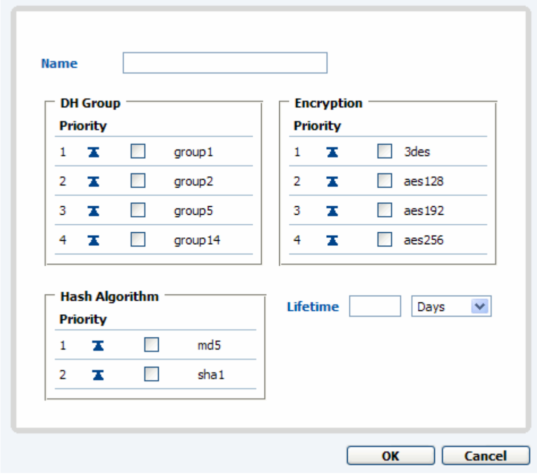
1. Under the **Network** tab, choose **IKE Crypto** under **Network Profiles** to open the IKE Crypto page.



	Name	Encryption	Hash Algorithm	DH Group	Lifetime
□	default	aes128, 3des	sha1	group2	8 hours

Figure 151. IKE Crypto Profile Page

2. Click **New** to open the configuration page.



DH Group

Priority			
1	⧗	□	group1
2	⧗	□	group2
3	⧗	□	group5
4	⧗	□	group14

Encryption

Priority			
1	⧗	□	3des
2	⧗	□	aes128
3	⧗	□	aes192
4	⧗	□	aes256

Hash Algorithm

Priority			
1	⧗	□	md5
2	⧗	□	sha1

Figure 152. Defining IKE Crypto Profile Settings

3. Specify the following information.

Table 97. IKE Crypto Profile Settings

Field	Description
DH Group Priority	Select the Diffie-Hellman (DH) groups.
Hash Algorithm Priority	Select the check boxes for the desired Authentication Header (AH) priority algorithms.
Encryption Priority	Select the check boxes for the desired ESP authentication options:
Lifetime	Select units and enter the length of time that the negotiated key will stay effective.

4. 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.

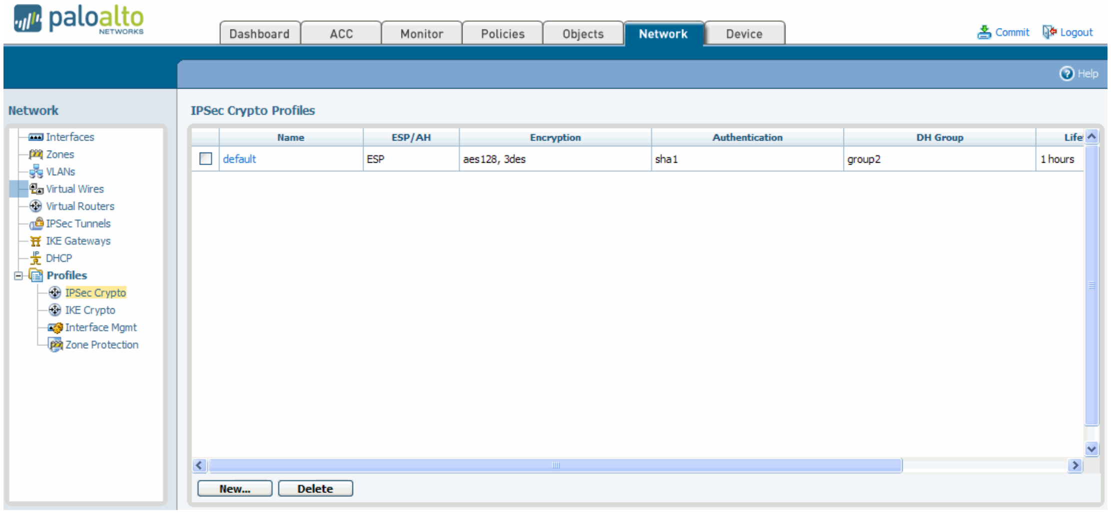
5. Click **OK**.

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 17 for more information.

To set up IPSec crypto profiles:

1. Under the **Network** tab, click **IPSec Crypto** under **Network Profiles** to open the IPSec Crypto Profiles page.

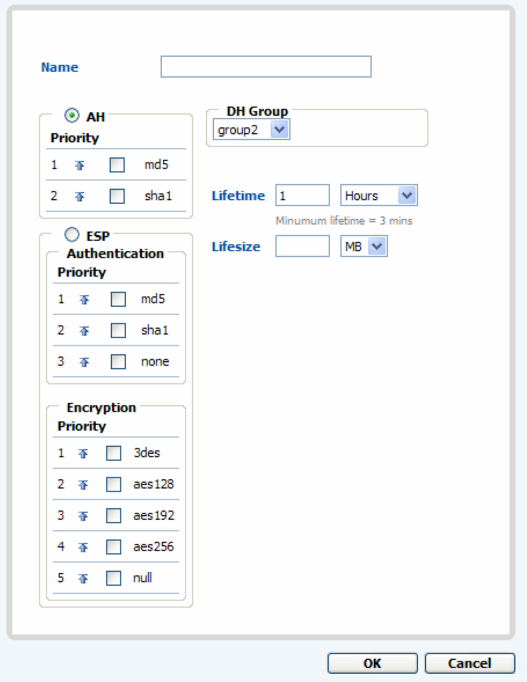


IPSec Crypto Profiles

	Name	ESP/AH	Encryption	Authentication	DH Group	Life
□	default	ESP	aes128, 3des	sha1	group2	1 hours

Figure 153. IPSec Crypto Profiles Page

2. Click **New** to open the configuration window.



Name

○ AH

Priority			
1	↑	□	md5
2	↑	□	sha1

○ ESP

Authentication

Priority			
1	↑	□	md5
2	↑	□	sha1
3	↑	□	none

Encryption

Priority			
1	↑	□	3des
2	↑	□	aes128
3	↑	□	aes192
4	↑	□	aes256
5	↑	□	null

DH Group: group2

Lifetime: 1 Hours

Minumum lifetime = 3 mins

Lifesize: MB

Figure 154. Defining IPSec Crypto Settings

3. Specify the following information.

Table 98. IPSec Crypto Profile Settings

Field	Description
Name	Enter a name to identify the profile.
AH Priority	Select the check boxes for the desired Authentication Header (AH) priority algorithms.
ESP Authentication	Select the check boxes for the desired ESP authentication algorithms.
ESP Encryption	Select the check boxes for the desired ESP encryption algorithms.
DH Group	Select the Diffie-Hellman (DH) group.
Lifetime	Select units and enter the length of time that the negotiated key will stay effective. The default is 1 hour.
Lifesize	Select optional units and enter the amount of data that the key can use for encryption.

4. 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.

5. Click **OK** to save the tunnels.

6. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, make change, and click **OK**.

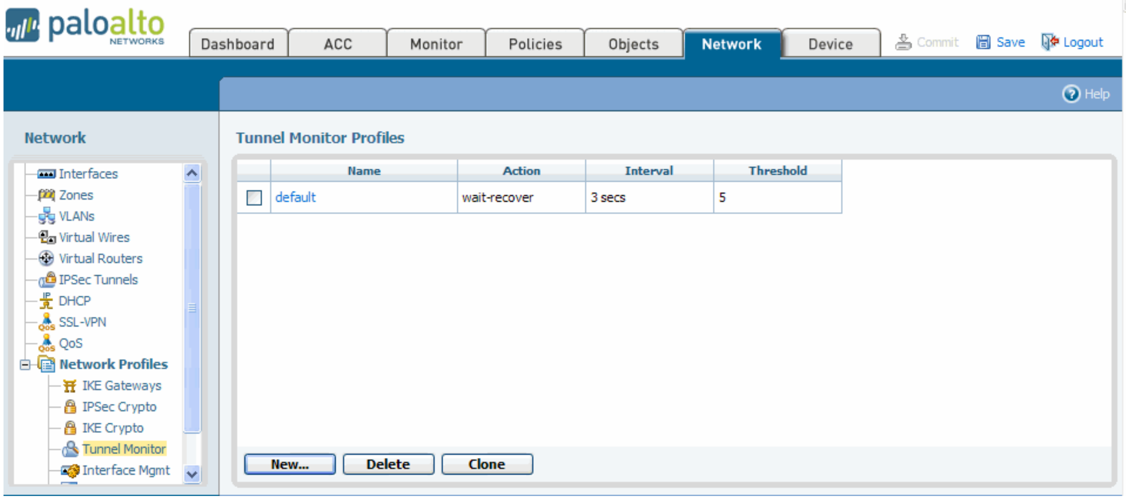
   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

Defining Tunnel Monitor Profiles

A tunnel monitor profile specifies how the firewall monitors IPSec tunnels. First you create a tunnel monitor profile, and then 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.

1. Under the **Network** tab, click **Tunnel Monitor** under **Network Profiles** to open the Tunnel Monitor page.



Tunnel Monitor Profiles

	Name	Action	Interval	Threshold
□	default	wait-recover	3 secs	5

Figure 155. Tunnel Monitor Profiles Page

2. To add a new tunnel monitor profile:

   a. Click **New** to open the New Tunnel Monitor Profile page.

   b. Specify the following information.

Table 99. New Interface Management Profile Settings

Field	Description
Name	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.
Action	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. • **wait-recover**—Wait for the tunnel to recover; do not take additional action. • **fail-over**—Cause traffic to fail over to a backup path, if one is available. In both cases, the firewall tries to negotiate new IPsec keys to accelerate the recovery.
Interval	Specify the time between heartbeats (range 2-10; default 3).
Threshold	Specify the number of heartbeats to be lost before the firewall takes the specified action (range 2-100; default 5).

   c. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, make change, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

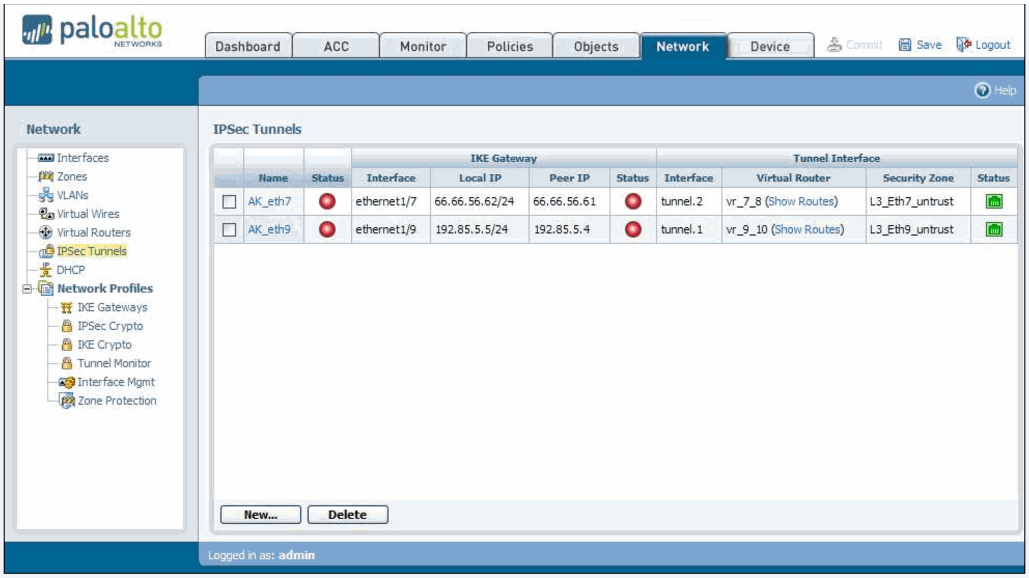
4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

Setting Up IPSec Tunnels

Use the IPSec Tunnels page to set up the parameters to establish IPSec VPN tunnels between firewalls.

To set up IPSec tunnels:

1. Under the **Network** tab, click **IPSec Tunnels** to open the IPSec Tunnels page.

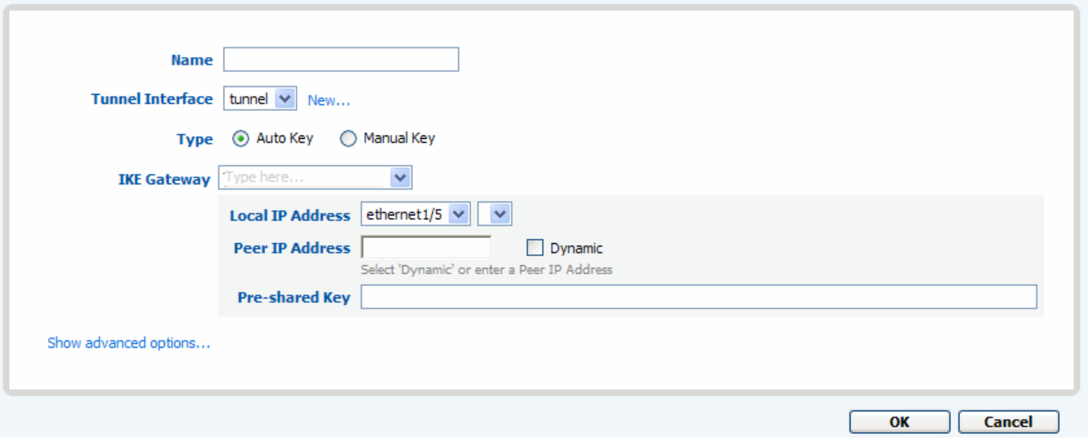


IPSec Tunnels

			IKE Gateway				Tunnel Interface			
	Name	Status	Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Security Zone	Status
□	AK_eth7	●	ethernet1/7	66.66.56.62/24	66.66.56.61	●	tunnel.2	vr_7_8 (Show Routes)	L3_Eth7_untrust	🟩
□	AK_eth9	●	ethernet1/9	192.85.5.5/24	192.85.5.4	●	tunnel.1	vr_9_10 (Show Routes)	L3_Eth9_untrust	🟩

Figure 156. IPSec Tunnels Page

2. Click **New** to open the configuration page.



Name	
Tunnel Interface	tunnel
Type	● Auto Key ○ Manual Key
IKE Gateway	Type here...
Local IP Address	ethernet1/5
Peer IP Address	□ Dynamic Select 'Dynamic' or enter a Peer IP Address
Pre-shared Key	

Figure 157. Defining IPSec Settings

3. Specify the following information.

Table 100. IPSec Tunnel Settings

Field	Description
IPSec Tunnel	Enter a name to identify the tunnel.
Tunnel Interface	Select an existing interface, or click **New**, enter the following information and click **OK**: • **Tunnel Interface Name**—Enter the new tunnel name. • **MTU**—Enter the maximum transmission unit in bytes for packets sent on this Layer 3 interface (512 to 1500). The default is 1500. ***Note:*** *The firewall automatically considers tunnel overhead when performing IP fragmentation and also adjusts the TCP maximum segment size (MSS) as needed.* • **IP Address**—Enter an IP address if dynamic routing is used. • **Management Profile**—Select the management profile to associate to this interface. • **Virtual Router**—Select a virtual router for this interface, or click **New** to configure a new virtual router. Refer to "Defining Virtual Routers" on page 122. • **Zone**—Select a security zone for this interface, or click **New** to configure a new zone. Refer to "Defining Security Zones" on page 116.
Type	Select whether to use an automatically generated or manually entered security key.
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.
Note: *The following advanced fields are displayed if you select the* ***Dynamic*** *check box to configure a dynamic endpoint or click the* ***Show Advanced Options*** *link.*	
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 (for the dynamic option)
Exchange Mode	Choose of 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 determine the mode.

Table 100. IPSec Tunnel Settings (Continued)

Field	Description
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 263.
Dead Peer Detection	Select to enable. If enabled, enter an interval (2 - 100 sec) and delay before retrying (2 - 100 sec).
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 264.
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).
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.

4. Click **OK** to save the tunnel.

Chapter 9

Configuring Quality of Service

This chapter describes how configure quality of service (QoS) on the firewall:

- “About Firewall Support for QoS” in the next section
- “Configuring QoS for Firewall Interfaces” on page 272
- “Defining QoS Profiles” on page 275
- “Defining QoS Policies” on page 277

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 interface to specify how traffic classes map to bandwidth (guaranteed, maximum) and priority. QoS classification is supported with all interface types except Aggregate Ethernet.

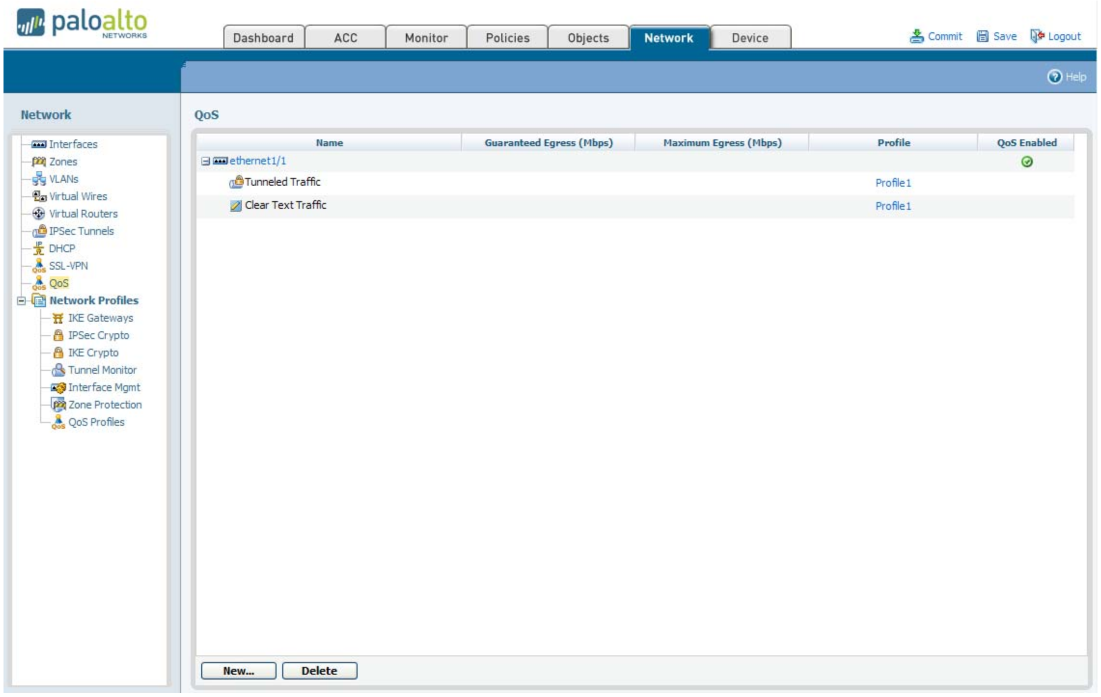
Use the following pages to define and apply QoS settings:

- QoS page (**Network** tab)—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 272.
- QoS profile (**Network** tab)—Configure QoS classes of service, as described in “Defining QoS Profiles” on page 275.
- QoS policies (**Policies** tab)—Configure the policies that will be used to active the QoS restrictions, as described in “Defining QoS Policies” on page 277.

Configuring QoS for Firewall Interfaces

To configure QoS settings for firewall interfaces:

1. Under the **Network** tab, click **QoS** to open the QoS page.

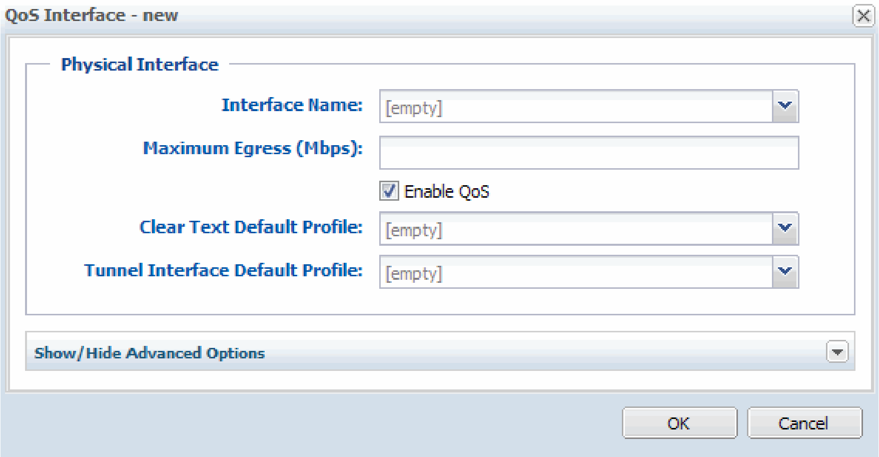


QoS

Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Profile	QoS Enabled
ethernet1/1				✓
Tunneled Traffic			Profile1	
Clear Text Traffic			Profile1	

Figure 158. QoS Page

2. Click **New** to open the configuration page.



QoS Interface - new

Physical Interface

Interface Name: [empty]

Maximum Egress (Mbps):

☑ Enable QoS

Clear Text Default Profile: [empty]

Tunnel Interface Default Profile: [empty]

Figure 159. Defining QoS Settings

3. Specify the following information.

Table 101. QoS Settings

Field	Description
Physical Interface	
Interface Name	Select the firewall interface.
Maximum Egress	Enter the limit on traffic leaving the firewall through this interface (Mbps).
Enable QoS	Select the check box to enable QoS features.
Clear Text Default Profile Tunnel Interface Default Profile	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. Refer to "Defining QoS Profiles" on page 275 for instructions on defining QoS profiles.
Advanced Options: Tunneled and Clear Text Traffic	Specify the following settings on the **Tunneled** and **Clear Text Traffic** tabs. These values apply unless they are overridden by setting in the Detail Configuration area, as described later in this table.
Guaranteed Egress	Enter the bandwidth that is guaranteed for tunneled traffic from this interface.
Maximum Egress	Enter the limit on traffic leaving the firewall through this interface (Mbps).

Table 101. QoS Settings (Continued)

Field	Description
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. Refer to "Defining QoS Profiles" on page 275 for instructions on defining QoS profiles. ***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**.

4. Click **OK**.

   The QoS page reopens to show the new entry.

5. To edit an existing entry, click the underlined link for the entry.

6. To delete an entry, select the entry and click **Delete**.

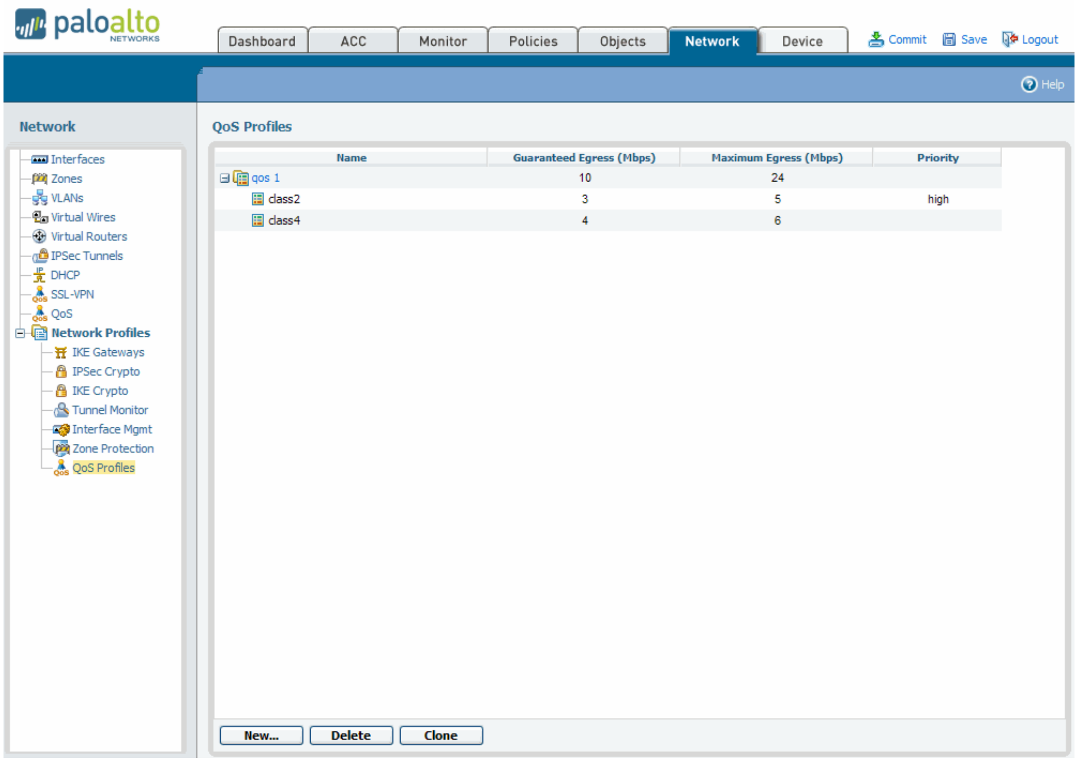
Defining QoS Profiles

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 272 for information on configuring firewall interfaces for QoS and refer to "Defining QoS Policies" on page 277 to configure the policies that will activate the QoS restrictions.*

To define QoS profiles:

1. Under the **Network** tab, click **QoS Profiles** under **Network Profiles** to open the QoS Profiles page.

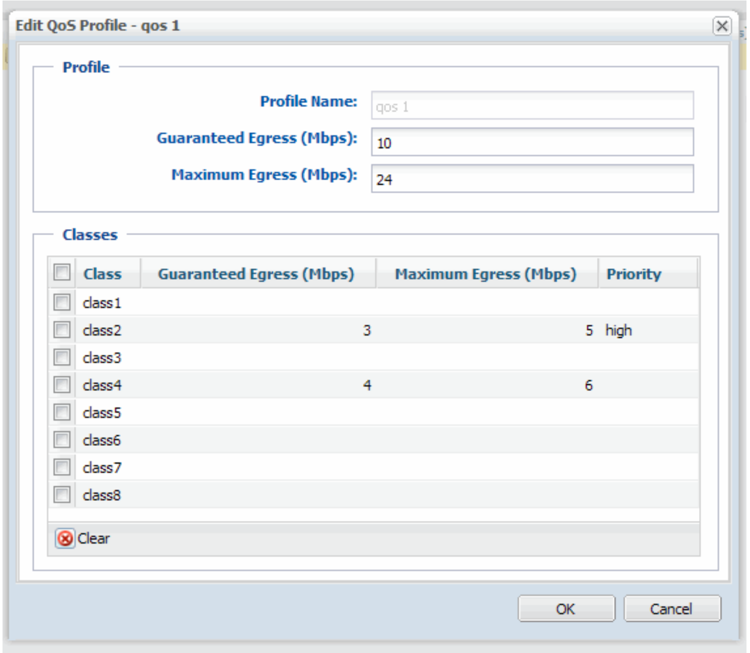


Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Priority
qos 1	10	24	
class2	3	5	high
class4	4	6	

Figure 160. QoS Profiles Page

2. To add a new profile:

   a. Click **New**.



Edit QoS Profile - qos 1

Profile

Profile Name: qos 1

Guaranteed Egress (Mbps): 10

Maximum Egress (Mbps): 24

Classes

☐	Class	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Priority
☐	class1			
☐	class2	3	5	high
☐	class3			
☐	class4	4	6	
☐	class5			
☐	class6			
☐	class7			
☐	class8			

Figure 161. New QoS Profile Page

   b. Specify the following information.

Table 102. New QoS Profile Settings

Field	Description
Profile Name	Enter a name to identify the profile.
Guaranteed Egress	Enter the bandwidth that is guaranteed for this profile (Mbps).
Maximum Egress	Enter the maximum bandwidth allowed for this profile (M.bps).
Classes	Specify how to treat individual QoS classes. You can select one or more classes to configure: • **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. • **Guaranteed Egress**—Click and enter a value (Mbps) for this class. • **Maximum Egress**—Click and enter a value (Mbps) for this class. • **Priority**—Click and select a priority to assign to this class. These are prioritized in the order listed (highest first): – Real-time – High – Medium – Low When contention occurs, traffic that is assigned a lower priority is dropped. Real-time priority uses its own separate queue.

c. Click **OK** to submit the new profile, or click **Cancel** to discard your changes.

3. Perform any of the following additional tasks:

   a. To change an entry, click the link for the entry, make change, and click **OK**.

   b. To delete entries, select their check boxes and click **Delete**.

   c. To create a new entry with the same information, select the check box for the entry and click **Clone**. The new entry is identical except for a sequence number that is added to the name.

4. To activate your changes immediately or save them for future activation, refer to “Managing Configurations” on page 47.

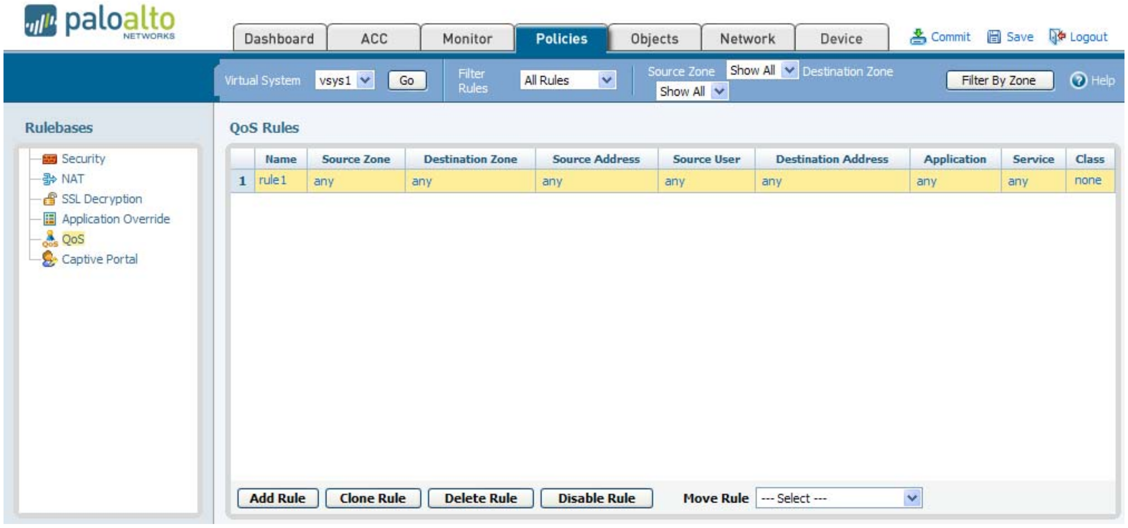
Defining QoS Policies

The Quality of Service (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 272 for information on configuring firewall interfaces for QoS and refer to “Defining QoS Profiles” on page 275 for information on configuring classes of service.*

To define QoS policies:

1. Under the **Policies** tab, click **QoS** to open the QoS Rules page.



Virtual System: vsys1
Filter Rules: All Rules
Source Zone: Show All
Destination Zone: Show All
Move Rule: --- Select ---

QoS Rules

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Class
1	rule1	any	any	any	any	any	any	any	none

Figure 162. QoS Rules Page

2. To view just the rules for a specific virtual system, select the system from the **Virtual System** drop-down list and click **Go**.

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

> ***Note:*** *Shared polices pushed from Panorama are shown in green and cannot be edited at the device level.*

4. 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**.

5. 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.

6. To change a field in a new or existing rule, click the current field value, specify the appropriate information, as described below, and click **OK.**

Table 103. QoS Rule Settings

Field	Description
Name	Change the default rule name and/or enter a rule description. If you add a rule description, a 💬 is added next to the rule name. By default, rules are named "rule<n>", 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.
Source Zone Destination Zone	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 116.

Table 103. QoS Rule Settings (Continued)

Field	Description
Source Address Destination 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_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 Addresses” on page 193). To define new address groups, refer to “Defining Address Groups” on page 195.
Source User	Click the link to identify the source users and groups to which the QoS policy will apply. Refer to “Specifying Users and Applications for Policies” on page 163 for instructions on specifying the source user and group settings.
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 196 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 205). To define new service groups, refer to “Defining Service Groups” on page 207.
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 275 for information on configuring settings for QoS classes.

7. 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 greyed out and the Disable Rule option is changed to Enable Rule.

8. To activate your changes immediately or save them for future activation, refer to "Managing Configurations" on page 47.

Chapter 10

Panorama Installation

This chapter describes how to install the Panorama central management system (CMS):

- "Installing Panorama" in the next section
- "Setting Up a Custom Virtual Disk" on page 282
- "Performing the Final Setup" on page 283
- "Accessing Panorama for the First Time" on page 283
- "Creating an SSL Certificate" on page 284

Note: *Refer to "Central Management of Devices" on page 285 for information on using Panorama and to "Connecting to Panorama" on page 37 for instructions on setting up the firewall so that it can be managed by 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 mgt-config 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 91.
8. Configure the serial numbers of the devices to be managed, as described in “Adding Devices” on page 289.
9. Verify that each managed device has the IP address of the Panorama server configured, as described in “Connecting to Panorama” on page 37.

Note: *Refer to "Central Management of Devices" on page 285 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 central management system to manage multiple firewalls:

- "Accessing the Panorama Interface" in the next section
- "Overview of the Panorama Interface" on page 286
- "Adding Devices" on page 289
- "Defining Device Groups" on page 291
- "Managing Administrator Roles" on page 293
- "Upgrading the Panorama Software" on page 295
- "Backing Up Firewall Configurations" on page 296

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**.

Overview of 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 163 shows the Panorama interface, which is similar to the interface for the firewall. The pages for each tab are listed in the left pane.

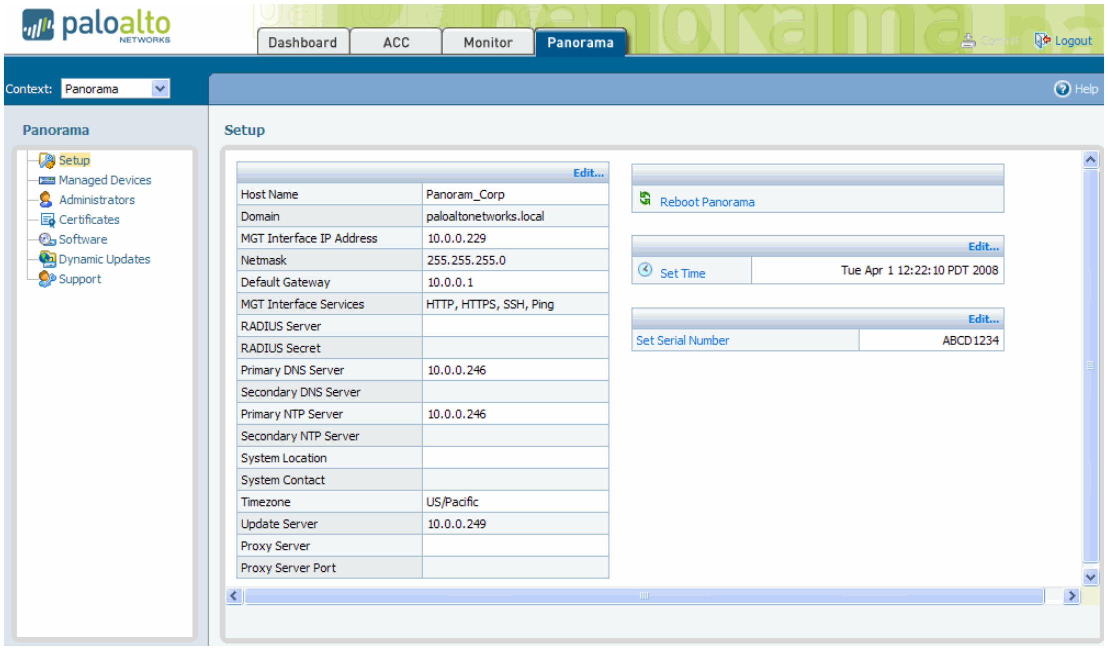
To display information regarding the Palo Alto Networks firewalls in the network, the devices must be connected to the Panorama server.

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 40.

2. Use the Panorama interface to add the devices. Refer to "Adding Devices" on page 289.

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.



Host Name	Panoram_Corp
Domain	paloaltonetworks.local
MGT Interface IP Address	10.0.0.229
Netmask	255.255.255.0
Default Gateway	10.0.0.1
MGT Interface Services	HTTP, HTTPS, SSH, Ping
RADIUS Server	
RADIUS Secret	
Primary DNS Server	10.0.0.246
Secondary DNS Server	
Primary NTP Server	10.0.0.246
Secondary NTP Server	
System Location	
System Contact	
Timezone	US/Pacific
Update Server	10.0.0.249
Proxy Server	
Proxy Server Port	

Set Time: Tue Apr 1 12:22:10 PDT 2008

Set Serial Number: ABCD1234

Figure 163. Panorama Interface

The Panorama tabs are listed in the following table.

Table 104. Summary of Panorama Tabs

Page	Description
Dashboard	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.
ACC	Displays the overall risk and threat levels for the managed devices. Refer to “Using the Application Command Center” on page 217 and “Identifying Unknown Applications and Taking Action” on page 246.
Monitor	Allows you to view logs and reports. Refer to “Viewing Reports” on page 241.
Objects	Allows you to define policy objects that are shared across the managed firewalls. Refer to “Defining Policy Objects” on page 192 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 “Defining Log Destinations” on page 80.
Policies	Allows you to define policies that are shared across the managed firewalls. Refer to “Defining Policies” on page 144 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 105. Summary of Panorama Pages

Page	Description
Setup	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 40 for information on using this page.
Config Audit	Allows you to view and compare firewall configuration files. Refer to "Comparing Configuration Files" on page 46 for information on using this page.
Managed Devices	Allows you to add devices for management by Panorama. Refer to "Adding Devices" on page 289 for information on using this page.
Device Groups	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 291 for information on using this page.
Admin Roles	Allows you to specify the privileges and responsibilities that are assigned to users who require access to Panorama. Refer to "Managing Administrator Roles" on page 48 for information on using this page.
Administrators	Allows you to define the accounts for users who require access to Panorama. Refer to "Creating Administrative Accounts" on page 51 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 91 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 "Defining Log Destinations" on page 80 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 295.
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 88 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 93.

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 289). 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.

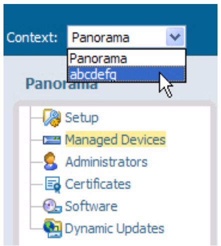


Figure 164. Choosing Device Context

Adding Devices

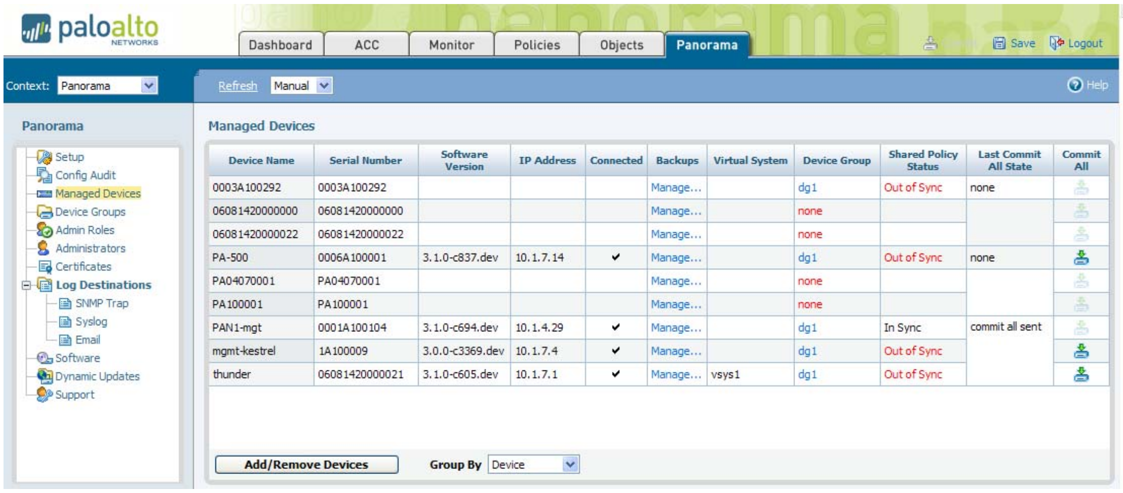
The Managed Devices page allows you to create a list of devices for centralized management.

Note: *The Panorama server communicates with managed devices via SSL through TCP port 3978.*

To add devices:

1. Under the **Panorama** tab, click **Managed Devices** to open the Managed Devices page.

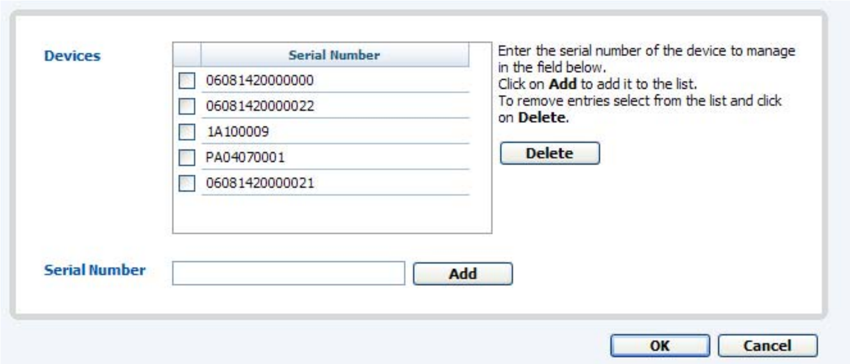
2. To group the devices according to device or device group, select from the **Group by** drop-down list.



Device Name	Serial Number	Software Version	IP Address	Connected	Backups	Virtual System	Device Group	Shared Policy Status	Last Commit All State	Commit All
0003A100292	0003A100292				Manage...		dg1	Out of Sync	none	
06081420000000	06081420000000				Manage...		none			
06081420000022	06081420000022				Manage...		none			
PA-500	0006A100001	3.1.0-c837.dev	10.1.7.14	✓	Manage...		dg1	Out of Sync	none	
PA04070001	PA04070001				Manage...		none			
PA100001	PA100001				Manage...		none			
PAN1-mgt	0001A100104	3.1.0-c694.dev	10.1.4.29	✓	Manage...		dg1	In Sync	commit all sent	
mgmt-kestrel	1A100009	3.0.0-c3369.dev	10.1.7.4	✓	Manage...		dg1	Out of Sync		
thunder	06081420000021	3.1.0-c605.dev	10.1.7.1	✓	Manage...	vsys1	dg1	Out of Sync		

Figure 165. Managed Devices Page

3. Click **Add/Remove Devices** to open an editing window.



	Serial Number
□	06081420000000
□	06081420000022
□	1A100009
□	PA04070001
□	06081420000021

Enter the serial number of the device to manage in the field below.
Click on **Add** to add it to the list.
To remove entries select from the list and click on **Delete**.

Figure 166. Managed Devices Page

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.

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**.

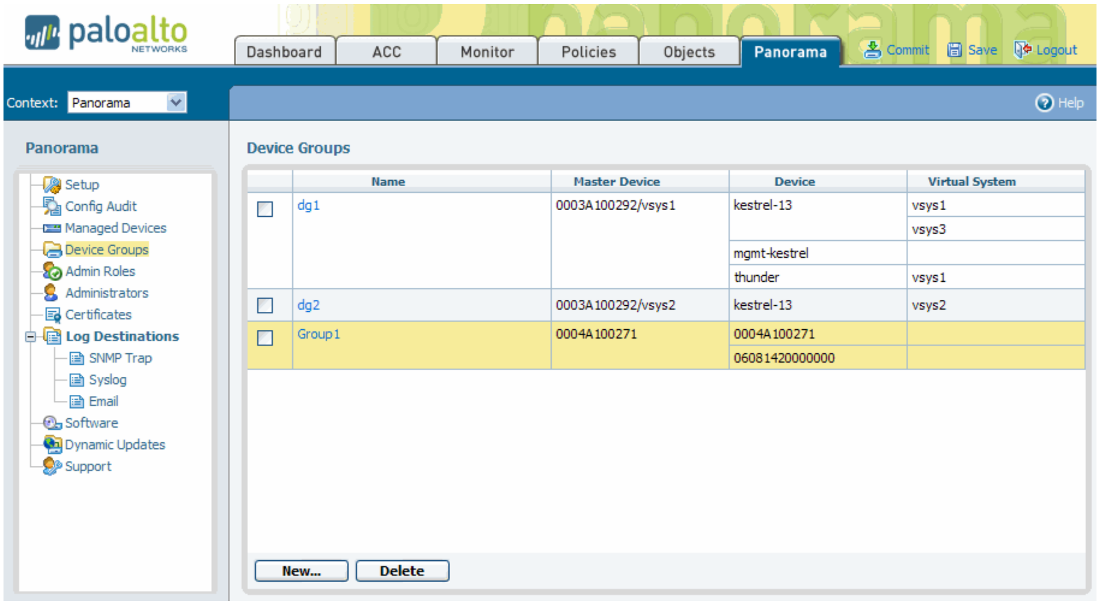
   c. Click **OK**.

Defining Device Groups

You can define device groups, which are treated as a single unit when applying policies in Panorama.

To manage device groups:

1. Under the **Panorama** tab, click **Device Groups** to open the Device Groups page.



	Name	Master Device	Device	Virtual System
□	dg1	0003A100292/vsys1	kestrel-13	vsys1
				vsys3
			mgmt-kestrel	
			thunder	vsys1
□	dg2	0003A100292/vsys2	kestrel-13	vsys2
□	Group1	0004A100271	0004A100271	
			06081420000000	

Figure 167. Device Groups Page

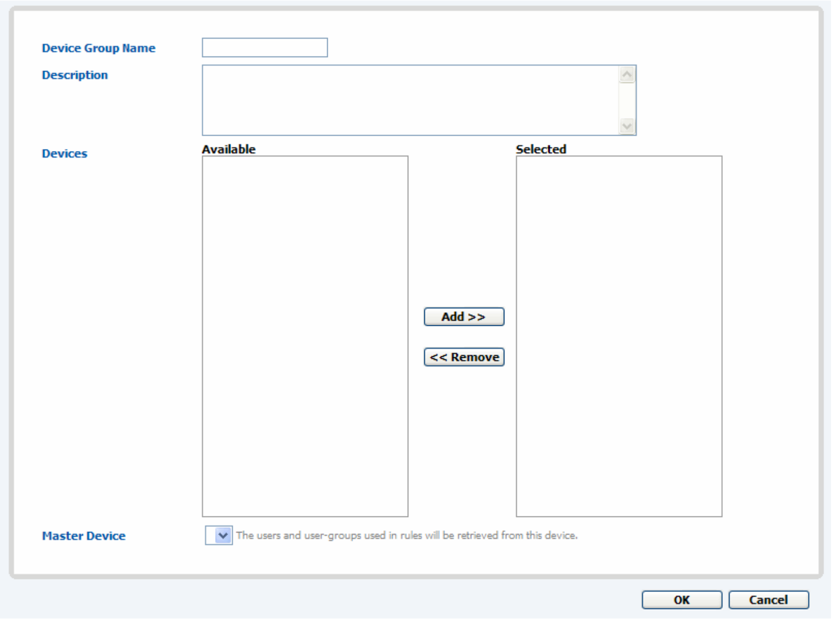
The page lists the device groups along with the following information.

Table 106. Device Group Information

Column	Description
Name	Name of the device group. Click the link to edit the group.
Master Device	Representative device from which the user information is gathered. The information is used for shared policy configuration.
Device	Devices included in the group.
Virtual Systems	Virtual systems for the devices included in the group.

2. To add a new device group:

   a. Click **New**.



The users and user-groups used in rules will be retrieved from this device.

Figure 168. Adding Device Groups

   b. Specify the following information.

Table 107. Device Groups Settings

Field	Description
Device Group Name	Enter a name to identify the group.
Description	Enter a description for the group.
Devices	Select devices from the available list and click **Add** to move them to the select list.
Master Device	Select the device from which the user information is gathered. The information is used for shared policy configuration.

   c. Click **OK**. The window closes and the Device Groups page refreshes to show the newly added group.

3. To edit a device group, click the underlined device link, make changes, and click **OK**.

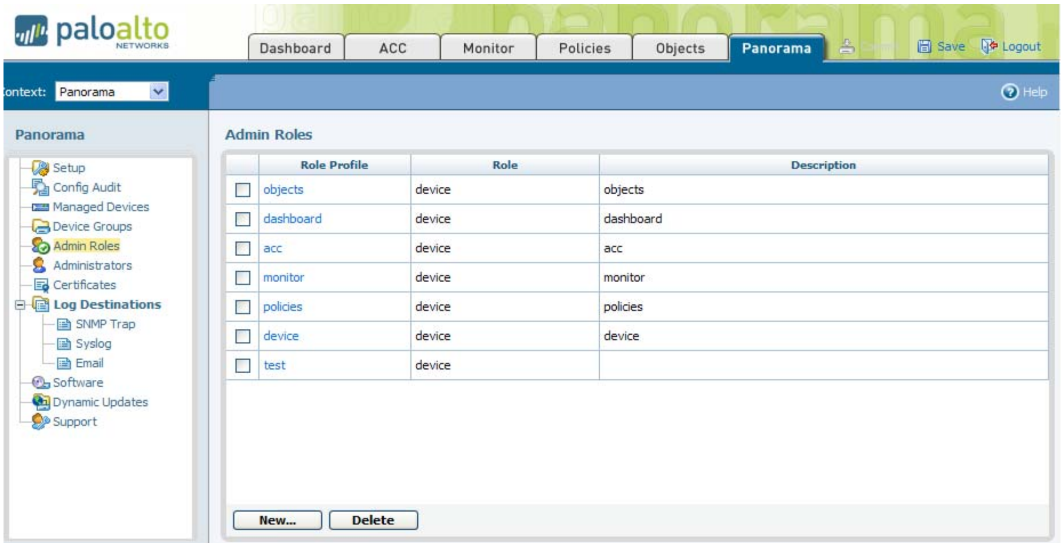
4. To delete a device group, select the check box for the group, and click **Delete**.

Managing Administrator Roles

You can specify the access and responsibilities that should be assigned to administrative users.

To define administrator roles:

1. Under the **Panorama** tab, click **Admin Roles** to open the Admin Roles page.



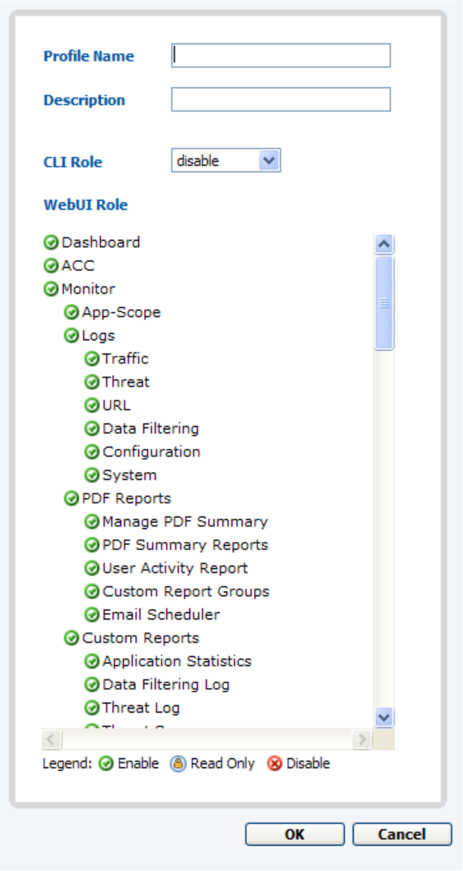
Admin Roles

	Role Profile	Role	Description
□	objects	device	objects
□	dashboard	device	dashboard
□	acc	device	acc
□	monitor	device	monitor
□	policies	device	policies
□	device	device	device
□	test	device	

Figure 169. Admin Roles Page

2. To add a new administrator role:

   a. Click **New** to open the New Administrator page.



Profile Name

Description

CLI Role: disable

WebUI Role

- ✓ Dashboard
- ✓ ACC
- ✓ Monitor
  - ✓ App-Scope
  - ✓ Logs
    - ✓ Traffic
    - ✓ Threat
    - ✓ URL
    - ✓ Data Filtering
    - ✓ Configuration
    - ✓ System
  - ✓ PDF Reports
    - ✓ Manage PDF Summary
    - ✓ PDF Summary Reports
    - ✓ User Activity Report
    - ✓ Custom Report Groups
    - ✓ Email Scheduler
  - ✓ Custom Reports
    - ✓ Application Statistics
    - ✓ Data Filtering Log
    - ✓ Threat Log

Legend: ✓ Enable 🔒 Read Only ✗ Disable

Figure 170. New Admin Role Page

   b. Specify the following information.

Table 108. New Administrator

Field	Description
Profile Name	Enter a name to identify this administrator role.
Description	Enter an optional description of the role.
Admin Role	Select the general scope of administrative responsibility from the drop-down list.

Table 108. New Administrator (Continued)

Field	Description
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 GUI: • ✓ Read/write access to the indicated page. • ▤ Read only access to the indicated page. • ✗ No access to the indicated page.

c. Click **OK** to submit the new role, or click **Cancel** to discard your changes.

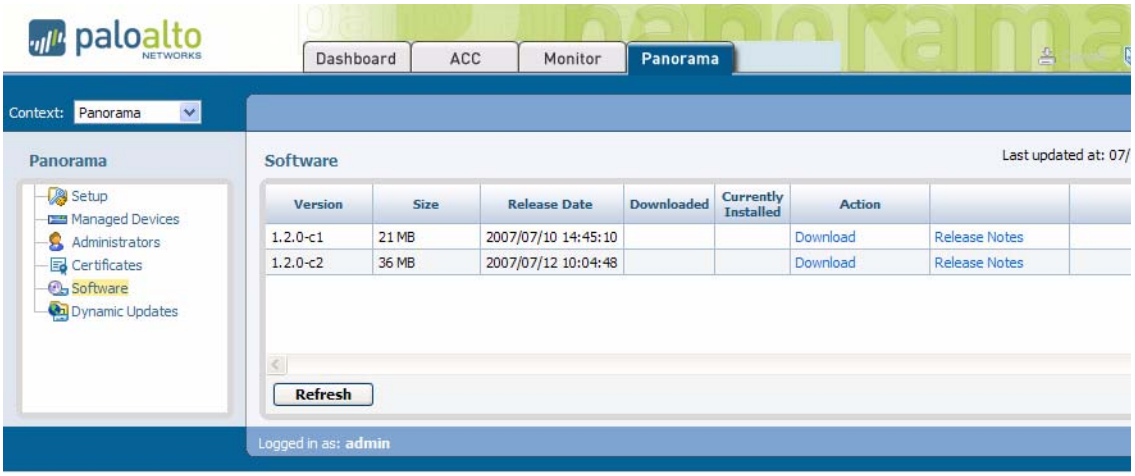
3. To change an administrator role, click the role as listed on the Admin Roles page, change the account settings, and click **OK**. To delete an account, select the account and click **Delete**.

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:

1. Under the **Device** tab, click **Software** to open the Software page.



Context: Panorama

Software

Last updated at: 07/

Version	Size	Release Date	Downloaded	Currently Installed	Action	
1.2.0-c1	21 MB	2007/07/10 14:45:10			Download	Release Notes
1.2.0-c2	36 MB	2007/07/12 10:04:48			Download	Release Notes

Logged in as: admin

Figure 171. Software Page

2. Click **Refresh** to view the latest software releases available from Palo Alto Networks.

3. To view a description of the changes in a release, click **Release Notes** next to the release.

4. 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.

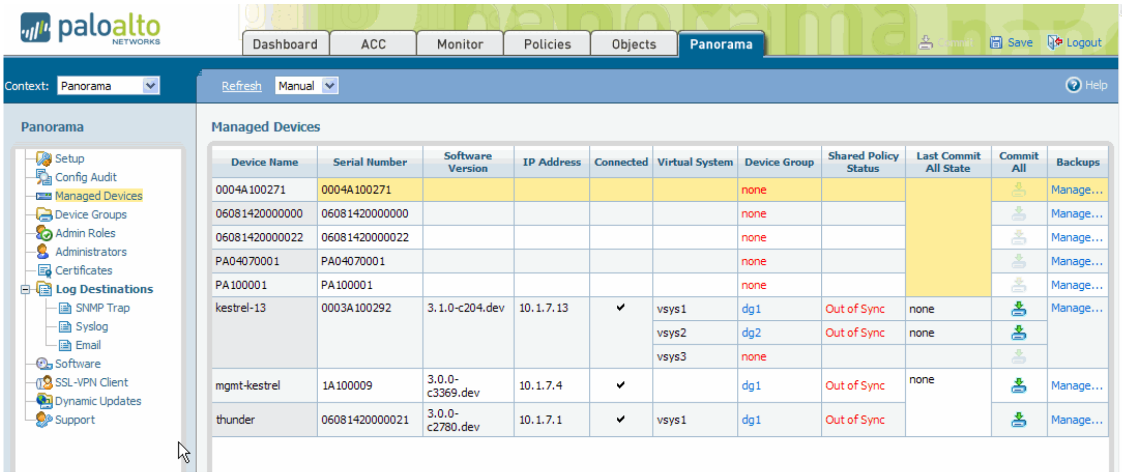
5. To delete an outdated release, click ☒ next to the release.

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. Refer to Table 6 in "Defining the Host Name and Network Settings" on page 40 for instructions on configuring the number of versions.

To manage backups on Panorama:

1. Under the **Panorama** tab, click **Managed Devices** to open the Managed Devices page.



Context: Panorama

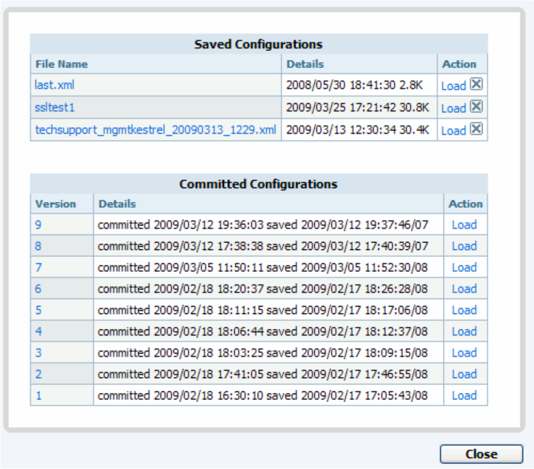
Manual

Managed Devices

Device Name	Serial Number	Software Version	IP Address	Connected	Virtual System	Device Group	Shared Policy Status	Last Commit All State	Commit All	Backups
0004A100271	0004A100271					none				Manage...
06081420000000	06081420000000					none				Manage...
06081420000022	06081420000022					none				Manage...
PA04070001	PA04070001					none				Manage...
PA100001	PA100001					none				Manage...
kestrel-13	0003A100292	3.1.0-c204.dev	10.1.7.13	✓	vsys1	dg1	Out of Sync	none		Manage...
					vsys2	dg2	Out of Sync	none		
					vsys3	none				
mgmt-kestrel	1A100009	3.0.0-c3369.dev	10.1.7.4	✓		dg1	Out of Sync	none		Manage...
thunder	06081420000021	3.0.0-c2780.dev	10.1.7.1	✓	vsys1	dg1	Out of Sync			Manage...

Figure 172. Managed Devices Page

2. Click **Manage** in the **Backups** column for a device. A window opens to show the saved and committed configurations for the device.



Saved Configurations		
File Name	Details	Action
last.xml	2008/05/30 18:41:30 2.8K	Load ☒
ssltest1	2009/03/25 17:21:42 30.8K	Load ☒
techsupport_mgmtkestrel_20090313_1229.xml	2009/03/13 12:30:34 30.4K	Load ☒

Committed Configurations		
Version	Details	Action
9	committed 2009/03/12 19:36:03 saved 2009/03/12 19:37:46/07	Load
8	committed 2009/03/12 17:38:38 saved 2009/03/12 17:40:39/07	Load
7	committed 2009/03/05 11:50:11 saved 2009/03/05 11:52:30/08	Load
6	committed 2009/02/18 18:20:37 saved 2009/02/17 18:26:28/08	Load
5	committed 2009/02/18 18:11:15 saved 2009/02/17 18:17:06/08	Load
4	committed 2009/02/18 18:06:44 saved 2009/02/17 18:12:37/08	Load
3	committed 2009/02/18 18:03:25 saved 2009/02/17 18:09:15/08	Load
2	committed 2009/02/18 17:41:05 saved 2009/02/17 17:46:55/08	Load
1	committed 2009/02/18 16:30:10 saved 2009/02/17 17:05:43/08	Load

Figure 173. Saved and Committed Configurations

3. 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 301
- "Default File Blocking Block Page" on page 301
- "Default URL Filtering Response Page" on page 302
- "Default Anti-Spyware Download Response Page" on page 303
- "Default SSL Decryption Opt-out Response Page" on page 303
- "Captive Portal Comfort Page" on page 304
- "URL Filtering Continue and Override Page" on page 304
- "SSL VPN Login Page" on page 305
- "SSL Certificate Revoked Notify Page" on page 305

***Note:** For information on importing and exporting custom response pages, refer to "Defining Custom Response Pages" on page 74.*

Default Antivirus Response Page

```
<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";
    panose-1:2 11 6 4 2 2 2 2 2 4;}
 /* Style Definitions */
 p.MsoNormal, li.MsoNormal, div.MsoNormal
    {margin:0in;
    margin-bottom:.0001pt;
    font-size:12.0pt;
    font-family:"Times New Roman";}
h4
    {margin-top:12.0pt;
    margin-right:0in;
    margin-bottom:3.0pt;
    margin-left:0in;
    page-break-after:avoid;
    font-size:14.0pt;
    font-family:"Times New Roman";}
p.SanSerifName, li.SanSerifName, div.SanSerifName
    {margin:0in;
    margin-bottom:.0001pt;
    text-autospace:none;
    font-size:10.0pt;
    font-family:"Microsoft Sans Serif";
    font-weight:bold;}
p.BoldNormal, li.BoldNormal, div.BoldNormal
    {margin:0in;
    margin-bottom:.0001pt;
    font-size:12.0pt;
    font-family:"Times New Roman";
    font-weight:bold;}
span.Heading10
    {color:black
    font-weight:bold;}
p.SubHeading1, li.SubHeading1, div.SubHeading1
    {margin-top:12.0pt;
    margin-right:0in;
    margin-bottom:3.0pt;
    margin-left:0in;
    page-break-after:avoid;
    font-size:12.0pt;
    font-family:"Times New Roman";
    font-weight:bold;}
@page Section1
    {size:8.5in 11.0in;
    margin:1.0in 1.25in 1.0in 1.25in;}
div.Section1
    {page:Section1;}
-->
</style>

</head>

<body lang=EN-US>

<div class=Section1>

<p class=MsoNormal>This is a test.</p>

</div>

</body>

</html>
```

Default Application Block Page

```
<html>
<head>
<title>Application 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;}
</style>
</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">
<meta name=Generator content="Microsoft Word 11 (filtered)">
<title>This is a test</title>
<style>
<!--
 /* Font Definitions */
 @font-face
    {font-family:"Microsoft Sans Serif";
    panose-1:2 11 6 4 2 2 2 2 2 4;}
 /* Style Definitions */
 p.MsoNormal, li.MsoNormal, div.MsoNormal
    {margin:0in;
    margin-bottom:.0001pt;
    font-size:12.0pt;
    font-family:"Times New Roman";}
h4
    {margin-top:12.0pt;
    margin-right:0in;
    margin-bottom:3.0pt;
    margin-left:0in;
    page-break-after:avoid;
    font-size:14.0pt;
    font-family:"Times New Roman";}
p.SanSerifName, li.SanSerifName, div.SanSerifName
    {margin:0in;
    margin-bottom:.0001pt;
    text-autospace:none;
    font-size:10.0pt;
    font-family:"Microsoft Sans Serif";
    font-weight:bold;}
p.BoldNormal, li.BoldNormal, div.BoldNormal
    {margin:0in;
    margin-bottom:.0001pt;
    font-size:12.0pt;
    font-family:"Times New Roman";
    font-weight:bold;}
```

```
span.Heading10
    {color:black
    font-weight:bold;}
p.SubHeading1, li.SubHeading1, div.SubHeading1
    {margin-top:12.0pt;
    margin-right:0in;
    margin-bottom:3.0pt;
    margin-left:0in;
    page-break-after:avoid;
    font-size:12.0pt;
    font-family:"Times New Roman";
    font-weight:bold;}
@page Section1
    {size:8.5in 11.0in;
    margin:1.0in 1.25in 1.0in 1.25in;}
div.Section1
    {page:Section1;}
-->
</style>

</head>

<body lang=EN-US>

<div class=Section1>

<p class=MsoNormal>This is a test.</p>

</div>

</body>

</html>
```

Default URL Filtering Response 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;}
</style>
</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><b>User:</b> <user/> </p>
<p><b>URL:</b> <url/> </p>
<p><b>Category:</b> <category/> </p>
</div>
</body>
</html>
```

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><b>IP:</b> <url/> </p>
<p><b>Category:</b> <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>

<pan_form/>
```

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><b>User:</b> <user/> </p>
<p><b>URL:</b> <url/> </p>
<p><b>Category:</b> <category/> </p>

<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 id="formdiv">
<pan_form/>
</div>
<a href="#" onclick="history.back();return false;">Return to previous page</
a>
</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=iso-8859-1">
<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">
        <h1>Palo Alto Networks - SSL VPN Portal</h1>
    </div>

<div id="formdiv">
<pan_form/>
</div>
</BODY>
</HTML>
```

SSL Certificate Revoked Notify Page

```
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<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

Sample VPN Configuration

This appendix 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.

The information is presented in the following sections:

- "Existing Topology" in the next section
- "New Topology" on page 308
- "Configure the VPN Connection" on page 308
- "VPN Connectivity Troubleshooting" on page 309

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 308.*

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.

Appendix C
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 312
- "Application Characteristics" on page 313

Application Categories and Subcategories

The following application categories and subcategories are supported:

- business-system
  - auth-service
  - database
  - erp-crm
  - general-business
  - management
  - office-program
  - software-update
  - storage-backup
- collaboration
  - voip-video
  - email
  - instant-messaging
  - internet-conferencing
  - social-networking

  - web-posting
- general-internet
  - file-sharing
  - internet-utility
- media
  - audio-streaming
  - gaming
  - photo-video
- networking
  - encrypted-tunnel
  - infrastructure
  - ip-protocol
  - proxy
  - remote-access
  - routing
- unknown

Application Technologies

The following application technologies are supported.

Table 109. Application Technologies

Item	Description
network-protocol	An application that is generally used for system to system communication that facilitates network operation. This includes most of the IP protocols.
client-server	An application that uses a client-server model where one or more clients communicate with a server in the network.
peer-to-peer	An application that communicates directly with other clients to transfer information instead of relying on a central server to facilitate the communication.
browser-based	An application that relies on a web browser to function.

Application Characteristics

The following application characteristics are supported.

Table 110. Application Characteristics

Item	Description
Capable of File Transfer	Has the capability to transfer a file from one system to another over a network.
Evasive	Uses a port or protocol for something other than its originally intended purpose with the hope that it will traverse a firewall.
Excessive Bandwidth Use	Consumes at least 1 Mbps on a regular basis through normal use.
Used by Malware	Malware has been known to use the application for propagation, attack, or data theft, or is distributed with malware.
Has Known Vulnerabilities	Has publicly reported vulnerabilities.
Prone to Misuse	Often used for nefarious purposes or is easily set up to expose more than the user intended.
Pervasive	Likely has more than 1,000,000 users.
Tunnels Other Applications	Is able to transport other applications inside its protocol.
Continue Scanning for Other Applications	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.

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 316
- "BSD" on page 317
- "GNU General Public License" on page 318
- "GNU Lesser General Public License" on page 322
- "MIT/X11" on page 328
- "OpenSSH" on page 328
- "PSF" on page 332
- "PHP" on page 332
- "Zlib" on page 333

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 documents 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 MERCHANTIBILITY 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

[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 Futoransky <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.

Copyright (c) 1983, 1990, 1992, 1993, 1995

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.

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>.

PHP includes the Zend Engine, freely available at <http://www.zend.com>.

Zlib

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

Index