

Configuring PA Firewalls for a Layer 3 Deployment

Configuring PAN Firewalls for a Layer 3 Deployment

Configuration Guide

January 2009

Introduction

The following document provides detailed step-by-step instructions for configuring PAN firewalls for a typical Layer 3 deployment. For additional information on any of the features listed in this document, please refer to the online help in the WebUI or the Administrator's Guide, which can be found on the Palo Alto Networks support site.

Device Registration

By default, all PAN firewalls retrieve licenses, content and software via the management interface. Before a device can download new content/software, the device must be registered on the support site. Follow the steps below to create a new support account and register your device.

1. Navigate to the Palo Alto Networks support site at <https://support.paloaltonetworks.com/>. If you have a support account login, otherwise click on the **Register** link to create a new support account.

Configuring PA Firewalls for a Layer 3 Deployment



2. On this page you will submit your contact information, create a user ID and register the firewall in the support database using the serial number located on the device. Complete the form and click the **Register** button.

Configuring PA Firewalls for a Layer 3 Deployment

The screenshot shows the Palo Alto Networks registration page. The browser address bar displays the URL: http://support.paloaltonetworks.com/ps-partner/next.php?option=com_registration-register. The page features a navigation menu with links for PRODUCTS, SOLUTIONS, INFO CENTER, SUPPORT, PARTNERS, NEWS & EVENTS, COMPANY, and APPLICATION RESEARCH CENTER. The main content area is titled 'New User Registration' and includes the following sections:

- User Information:** Fields for *First Name, *Last Name, *Company, Title, Address Line1, Address Line2, *City, *State, *Postal Code, *Country (dropdown menu), and *Telephone.
- User ID Creation:** Fields for *Login Name, *Your Email Address, *Password, and *Confirm Password.
- Device Registration:** Fields for Device Name, Device Serial Number, and Remarks.

Additional elements include a 'Remember me' checkbox, a 'Login' button, a 'Lost Password?' link, and a checkbox for 'By checking this box you are agreeing to the End User Service Agreement'. At the bottom, there is a '*Denotes required field' note, a 'Reset' button, and a 'Register' button.

Management Interface Configuration

By default, all PAN firewalls retrieve licenses and content/software updates via the management interface, so you will need to configure these settings first. All PAN firewalls ship with a serial cable and this is often the easiest way to configure these settings. By default, the management interface is configured with an IP address of 192.168.1.1/24, so you can connect directly using an Ethernet cable and then establish an SSH session to the device. Once connected and IP connectivity or serial connectivity is confirmed, follow the instructions below to configure the management interface.

Configuring PA Firewalls for a Layer 3 Deployment

1. Login to using default username/password of admin/admin

PA-2050 login: admin Password: admin

2. Enter configuration mode to configure the management interface. At a minimum, you will need to configure the IP Address, Subnet Mask, Default Gateway and Primary DNS as shown below.

```
admin@PA-2050> configure
```

Entering configuration mode

```
[edit]
```

```
admin@PA-2050# set deviceconfig system ip-address 192.168.1.2 netmask  
255.255.255.0 default-gateway 192.168.1.1 dns-primary 4.2.2.1 dns-secondary  
4.2.2.2
```

3. Commit the configuration to make it active and exit configuration mode.

```
admin@PA-2050# commit
```

```
.....98%.....100%
```

Configuration committed successfully

```
[edit]
```

```
admin@PA-2050# exit
```

Exiting configuration mode

4. To test IP connectivity and DNS, ping the default gateway and if successful, ping an address on the Internet using the Fully Qualified Domain Name (FQDN).

```
admin@PA-2050> ping host 192.168.1.1
```

```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
```

```
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.53 ms
```

```
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.47 ms
```

```
--- 192.168.1.1 ping statistics ---
```

```
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
```

```
rtt min/avg/max/mdev = 1.471/1.501/1.532/0.049 ms
```

```
admin@PA-2050> ping host google.com
```

```
PING google.com (72.14.205.100) 56(84) bytes of data.
```

```
64 bytes from qb-in-f100.google.com (72.14.205.100): icmp_seq=1 ttl=242 time=84.8 ms
```

```
64 bytes from qb-in-f100.google.com (72.14.205.100): icmp_seq=2 ttl=242 time=84.4 ms
```

```
--- google.com ping statistics ---
```

```
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
```

```
rtt min/avg/max/mdev = 84.447/84.660/84.873/0.213 ms
```

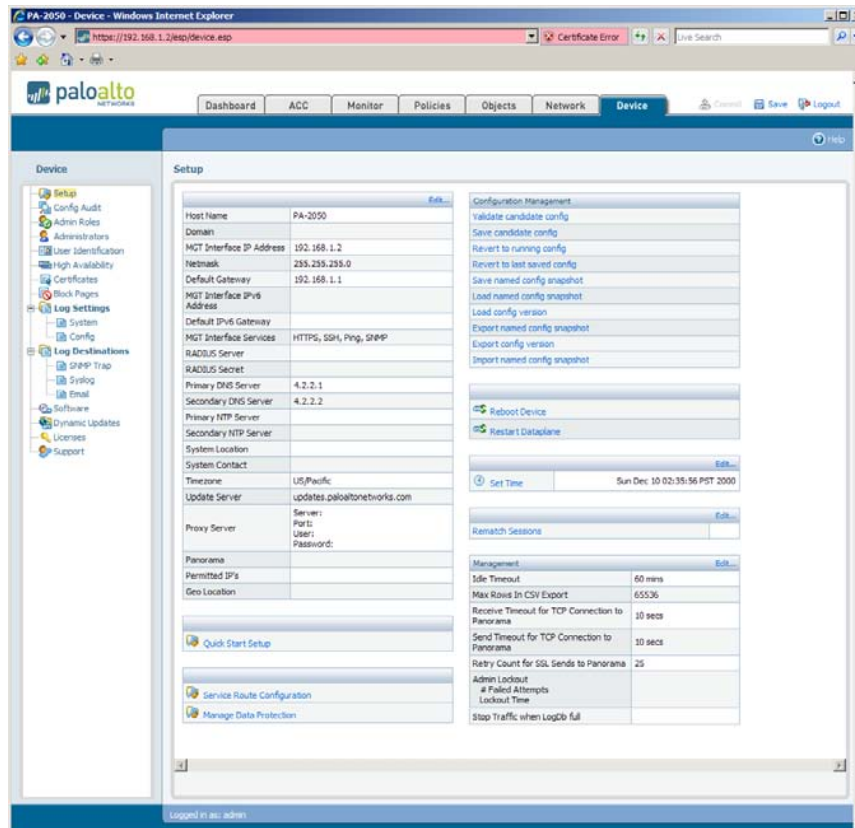
Download/Upgrade licenses, content and software

Once the management interface is configured, it is often easiest to configure the remaining settings via the WebUI. By default the management interface will respond using HTTPS, so point your browser to the management interface IP address and be sure to specify “https”.

Licensing

1. First configure the date and time. Once connected to the device, go to the **Device** tab and click on the **Set Time** link. Then fill in the required fields, no commit is needed to make the time change active.

Configuring PA Firewalls for a Layer 3 Deployment

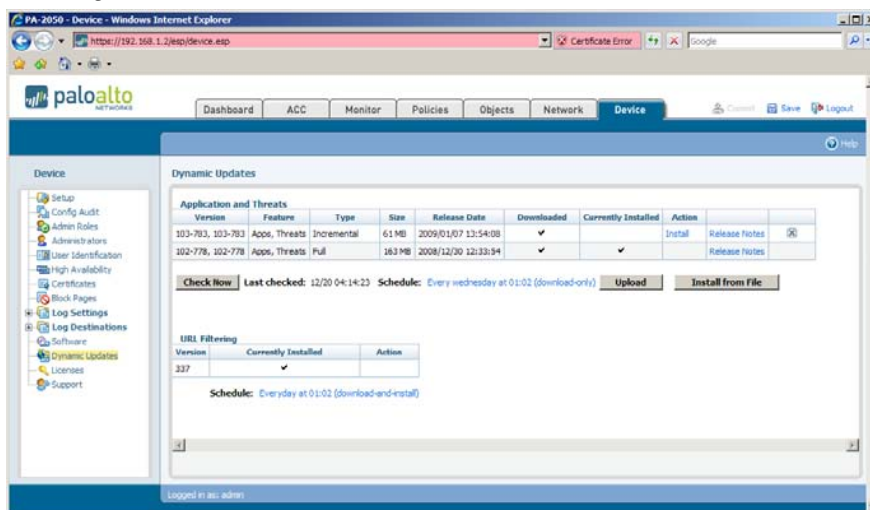


Note: Changing the system time does not change the original timestamps of existing log entries.

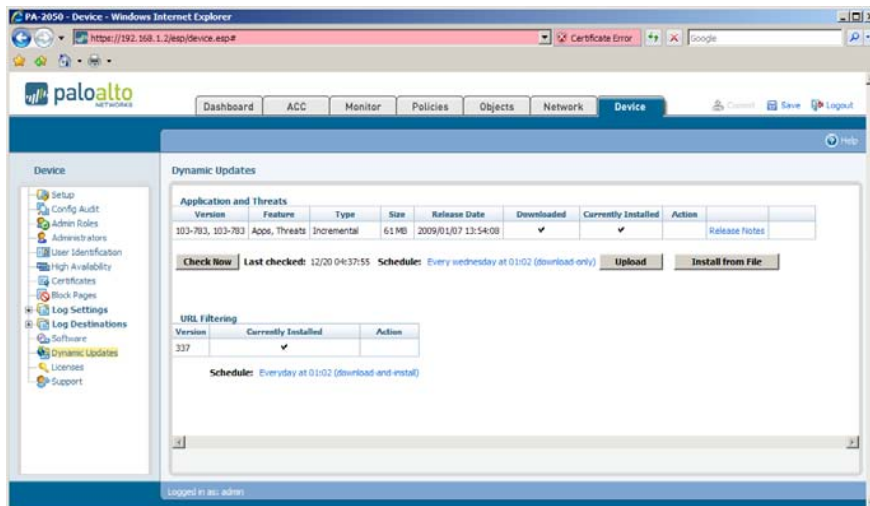
2. Navigate to the **Licenses** page in the left-hand navigation pane and click the **Retrieve license keys...** link. If the management interface is configured correctly and the device is registered, the firewall will pull down licenses from the Palo Alto Networks support site using SSL. If this fails, check for a device blocking TCP/443 between the firewall's MGT interface and the Internet. If the firewall is sitting behind a proxy server, you might need to configure the proxy settings on the **Device** tab.

Content Update

1. From the **Device** tab, click on the **Dynamic Updates** link in the left-hand navigation pane. Next, click the **Check Now** button to check for new application and/or threat content. If available, the action column will display a **Download** link. Click this link to begin downloading the latest content. Once completed, the link changes to an **Install** link. Click this link to begin installing the latest content. This could take several minutes depending on the platform. Later you can configure dynamic updates on a daily or weekly schedule to automate the process of downloading and installing new content.

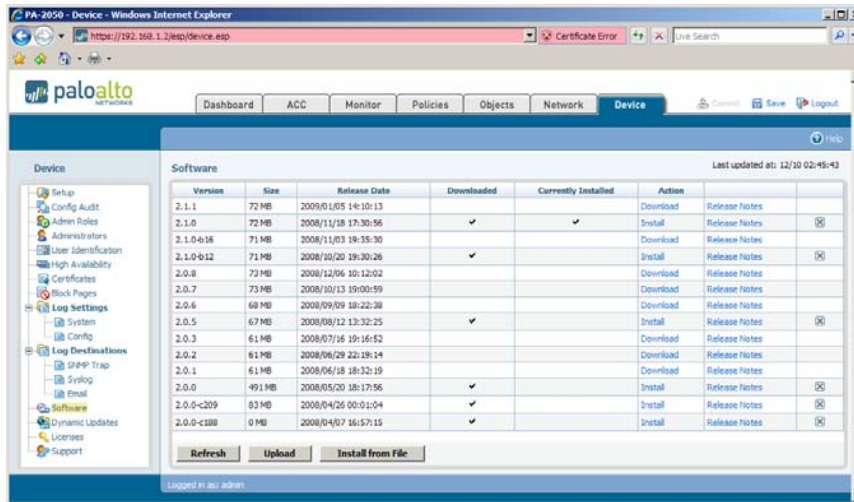


2. Once the installation is completed, you are finished with content updates and are ready to upgrade the software.

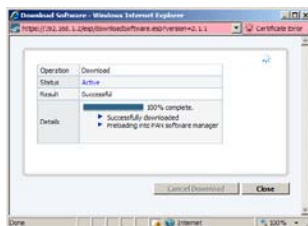


Software Update

1. Navigate to the **Software** page in the left-hand navigation pane and click the **Refresh** button to check for new system software.

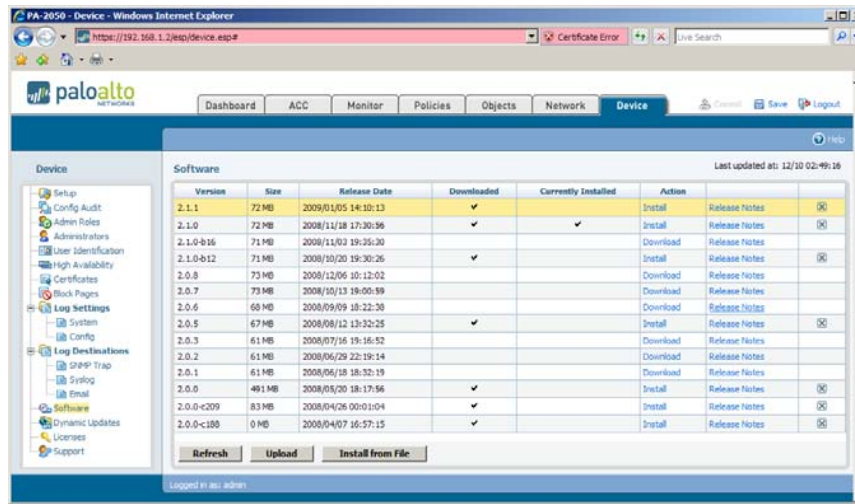


2. If new software is available, it should be listed at the top and the action column will display a **Download** link. Click this link to begin the software download.

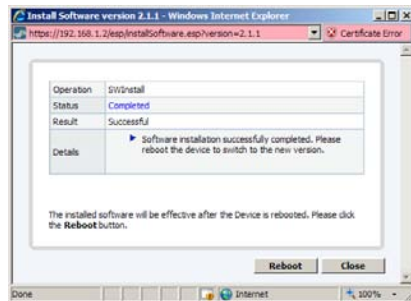


Configuring PA Firewalls for a Layer 3 Deployment

- Once the system software is downloaded, the action column for that software version will change to display an Install link, click the link to start the installation process. The amount of time this takes will depend on the hardware platform and the process will require a reboot of the firewall.



- Once the software is installed, you will have the option to reboot to complete the upgrade process. Click the Reboot button to force a reboot and to complete the upgrade process.



Note: When a device is rebooted, a job/process called an “Auto Commit” is performed to “push” the content and configuration from the management plane to the data plane. After an upgrade this may take several minutes and during this time, the device configuration cannot be committed. You can check the status of this job from the CLI using the following command:

The following shows an autocommit in-process:

```
admin@PA-2050> show jobs processed
```

Enqueued	ID	Type	Status	Result	Completed
----------	----	------	--------	--------	-----------

02:07:42	1	AutoCom	ACT	PEND	60%
----------	---	---------	-----	------	-----

The following shows an autocommit completed:

```
admin@PA-2050> show jobs processed
```

Enqueued	ID	Type	Status	Result	Completed
----------	----	------	--------	--------	-----------

02:07:42	1	AutoCom	FIN	OK	02:18:12
----------	---	---------	-----	----	----------

Note: After upgrading, close and reopen your browser. Most releases include updates to files that the browser may have cached so it is also a good idea to clear your browser cache. Skipping this step could cause the older files to be used and may lead to incorrect displays in the web interface.

5. Once software and content are both upgraded, you are ready to begin the configuration of the firewall.

Configure Interfaces, Zones and Virtual Routers

First it is important to understand the three key components to configuring a PAN firewall for a Layer 3 deployment. The building blocks for any Layer 3 deployment are zones, interfaces and virtual routers.

Zones: When it comes time to build your security policy, all security rules will be created based on a source zone and a destination zone. A typical perimeter firewall deployment will have three zones, a “Trust”, “DMZ” and an “Untrust” zone. To allow traffic to pass through the firewall from the internal network to the Internet, a policy permitting traffic between the “trust” and “untrust” zones would be required. PAN firewalls ship with predefined zones and firewall administrators can create their own custom zones to fit their environment. Zones are particularly useful for internal segmentation when you need to control traffic and protect resources between different groups/functions.

Interfaces: PAN firewalls support both physical and logical interfaces and all interfaces must be configured to belong to a zone before traffic can pass between two interfaces. Multiple interfaces can belong to a single zone but any physical or logical interface can only belong to a single zone. PAN devices support VLAN tagging (802.1q), so a single physical interface could have several logical subinterfaces, each in their own custom zone.

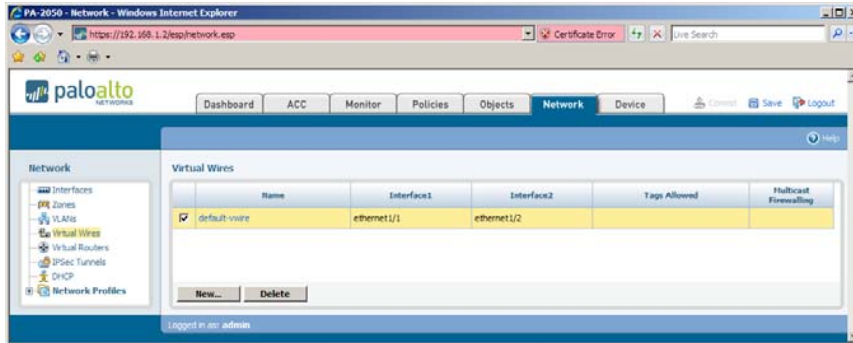
Virtual Routers: Virtual routers (VRs) are required for a Layer 3 deployment. This is where static routes are added and where dynamic routing protocols are configured. All Layer 3 interfaces must belong to a virtual router to function. For any Layer 3 deployment, a virtual router must be created and a default route added. Each virtual router maintains a separate set of routes that are not shared between VRs, giving administrators the ability to configure different routing behaviors for different interfaces.

Configuration Cleanup

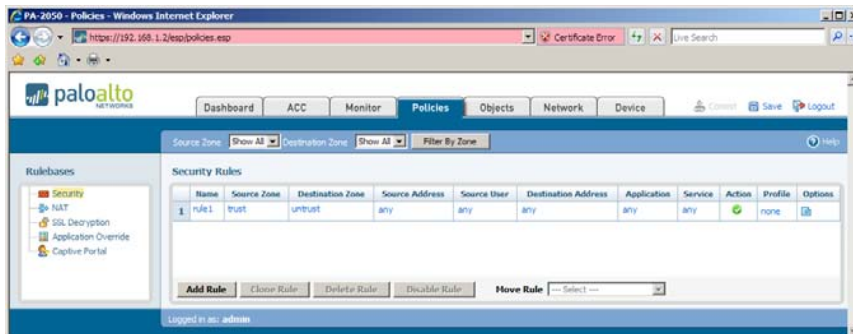
By default, all PAN firewalls ship to work in a Virtual Wire (transparent) mode right out of the box. Since this document only addresses Layer 3 deployment, we will want to delete some of the default configurations that are no longer needed.

Configuring PA Firewalls for a Layer 3 Deployment

1. First we will delete the default virtual wire. Navigate to the **Network** tab and click on the **Virtual Wires** link in the left navigation pane to see the configured virtual wire(s). Select the check box next to the “default-vwire” and click the **Delete** button.

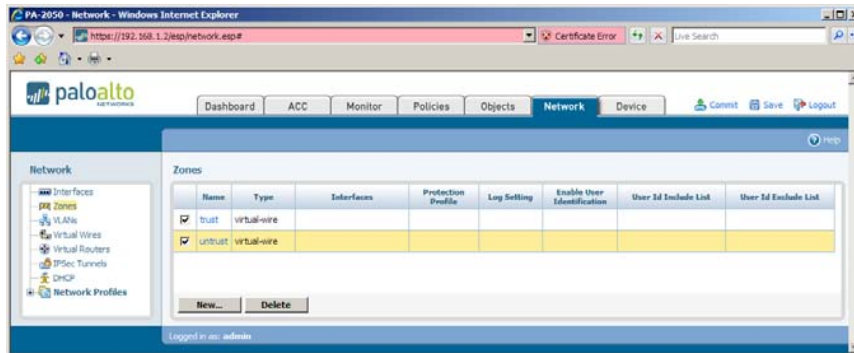


2. Next we will delete the default security policy since it is using zones only valid for a Virtual Wire deployment. . Navigate to the **Policy** tab and highlight the first rule and then click the **Delete Rule** button at the bottom of the page.



3. Next we will delete the default zones. Navigate to the **Network** tab and check the boxes next to the “trust” and “untrust” zones. Then click the **Delete** button at the bottom of the page.

Configuring PA Firewalls for a Layer 3 Deployment



4. At this point, it is a good idea to click the Commit link located in the top right corner of the browser to verify, save and commit the changes made. No changes are saved to running configuration until the commit link is used.

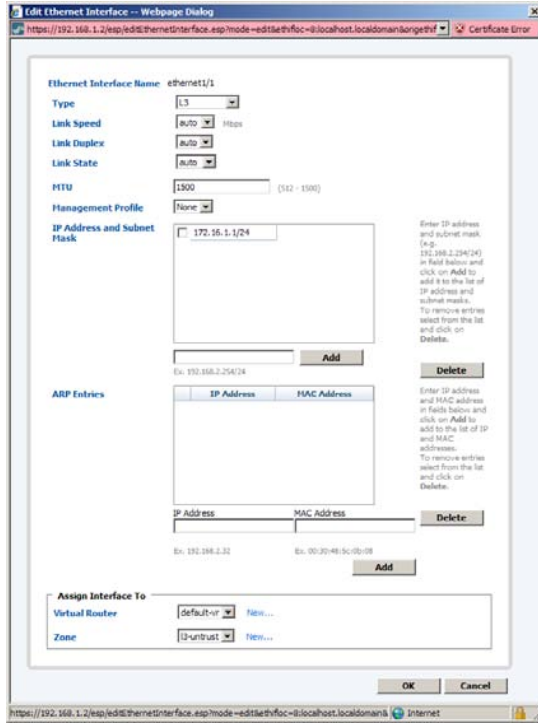
Interface, Zone and Virtual Router Configuration

First we will configure our interfaces, zones and virtual routers. One of the interfaces will be configured as the internal interface in the “I3-trust” zone and another will be configured as the external interface in the “I3-untrust” zone. Both interfaces will also be configured to belong to the “default-vr” virtual router. Follow the steps below to configure these interfaces, zones and VRs.

Configure Internal Interface

1. Navigate to the **Network** tab and click on the **ethernet1/1** link to edit the external interface. Enter an IP address and subnet mask in the appropriate field and click the **Add** button.

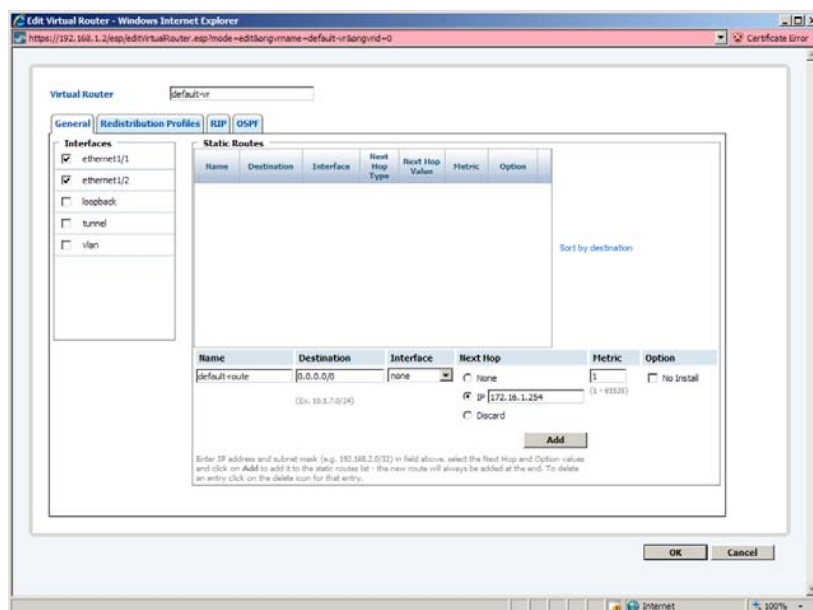
Configuring PA Firewalls for a Layer 3 Deployment



Configuring PA Firewalls for a Layer 3 Deployment

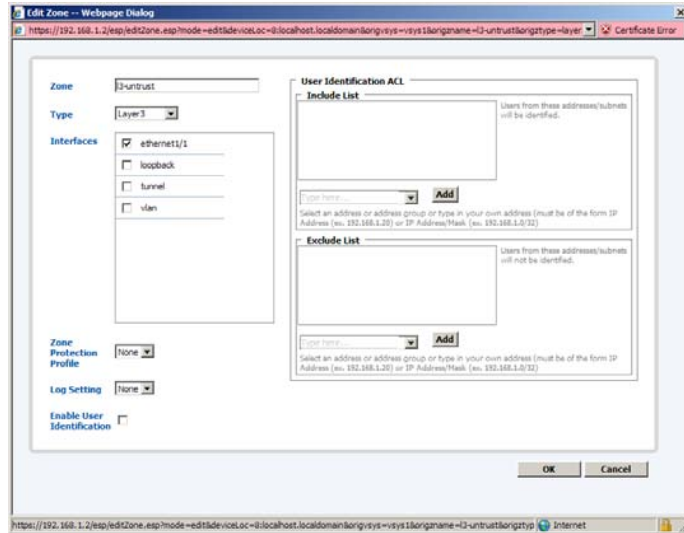
- At the bottom of the page you can assign the interface to the desired zone and virtual router. Next to the drop down menu for **Virtual Router** click the **New** link. You will be taken to the New Virtual Router configuration page. Give the virtual router a name of "default-vr" (can be any name) and configure a default route using the fields at the bottom of the page. In the example below, a new Virtual Router was created with a name of "default-vr" and a default route was added using the Internet router's IP address of "172.16.1.254" as the next hop and a metric value of "1". When adding a static default route, **DO NOT** select an interface in the **Interface** dropdown, leave this option set to "none".

Click the **Add** button to add the route and once added, verify that it is correct and click **OK** to be taken back to the interface configuration page.



- Next we need to create a new zone for this interface. Find the drop-down menu for **Zone** at the bottom of the page and click the **New** link to create a new zone. You will be taken to the New Zone configuration page. Give this zone a name of "I3-untrust" and click the **OK** button to return to the interface configuration page.

Configuring PA Firewalls for a Layer 3 Deployment

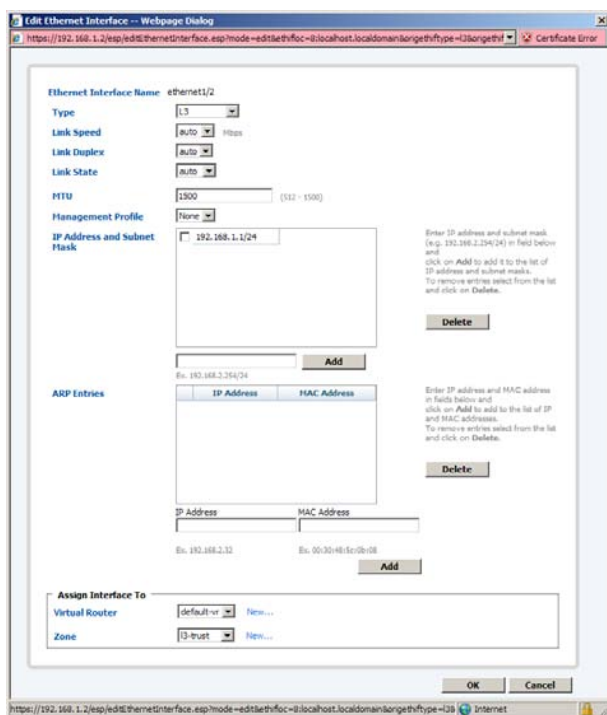


4. Make sure the new zone is selected in the drop-down and click the **OK** button to finish configuring the external interface.

Configure External Interface

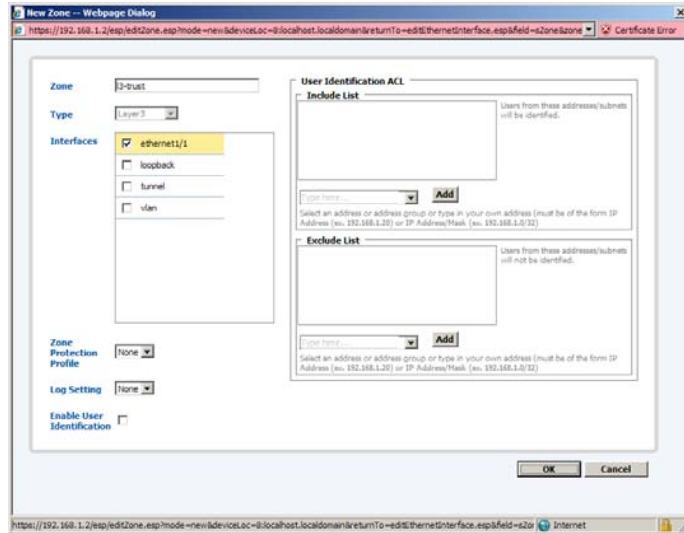
1. Now we will repeat the same steps for the internal interface. Navigate to the **Network** tab and click on the **ethernet1/2** link to edit the external interface. Enter an IP address and subnet mask in the appropriate field and click the **Add** button.

Configuring PA Firewalls for a Layer 3 Deployment



2. At the bottom of the page select "default-vr" in the **Virtual Router**, dropdown menu.
3. Next to the drop down menu for **Zone** at the bottom of the page, click the **New** link. You will be taken to the New Zone configuration page. Give the zone a name of "I3-trust" and click the **OK** button to return to the interface configuration page.

Configuring PA Firewalls for a Layer 3 Deployment



4. To finish configuring the internal interface, click the **OK** button.

Verify Network Configuration

Verify your interface, zone and virtual router configurations by comparing to the screenshots below:

Interfaces

Configuring PA Firewalls for a Layer 3 Deployment

The screenshot shows the Palo Alto Networks configuration interface for a PA-2050 device. The 'Network' tab is selected, and the 'Interfaces' section is active. A table lists various interfaces with their configurations.

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/Virtual Wire	Security Zone	Features
ethernet1/1	L3		🔴	172.16.1.1/24	default-vr	Untagged		🔵-untrust	
ethernet1/2	L3		🔴	192.168.1.1/24	default-vr	Untagged		🔵-trust	
ethernet1/3			🔴			Untagged		none	
ethernet1/4			🔴			Untagged		none	
ethernet1/5			🔴			Untagged		none	
ethernet1/6			🔴			Untagged		none	
ethernet1/7			🔴			Untagged		none	
ethernet1/8			🔴			Untagged		none	
ethernet1/9			🔴			Untagged		none	
ethernet1/10			🔴			Untagged		none	
ethernet1/11			🔴			Untagged		none	
ethernet1/12			🔴			Untagged		none	
ethernet1/13			🔴			Untagged		none	
ethernet1/14			🔴			Untagged		none	
ethernet1/15			🔴			Untagged		none	
ethernet1/16			🔴			Untagged		none	
ethernet1/17			🔴			Untagged		none	
ethernet1/18			🔴			Untagged		none	
ethernet1/19			🔴			Untagged		none	
ethernet1/20			🔴			Untagged		none	
vlan	VLAN		🟢		none	Untagged	none	none	
loopback	Loopback		🟢		none			none	
tunnel	Tunnel		🟢		none			none	

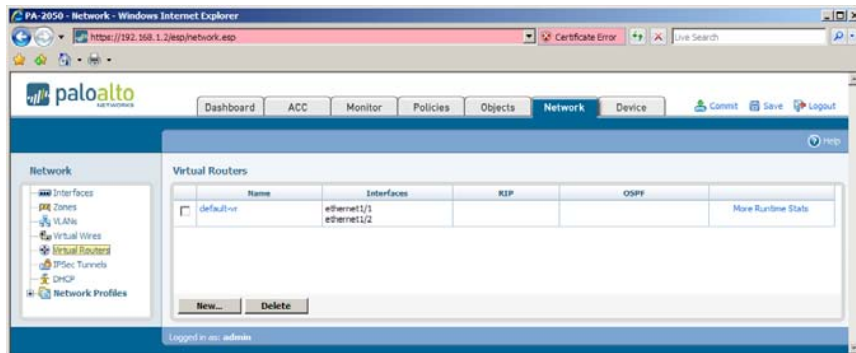
Zones

The screenshot shows the Palo Alto Networks configuration interface for a PA-2050 device. The 'Network' tab is selected, and the 'Zones' section is active. A table lists the configured zones.

Name	Type	Interfaces	Protection Profile	Log Setting	Enable User Identification	User Id Include List	User Id Exclude List
🔵-trust	layer3	ethernet1/2					
🔵-untrust	layer2	ethernet1/1					

Virtual Router

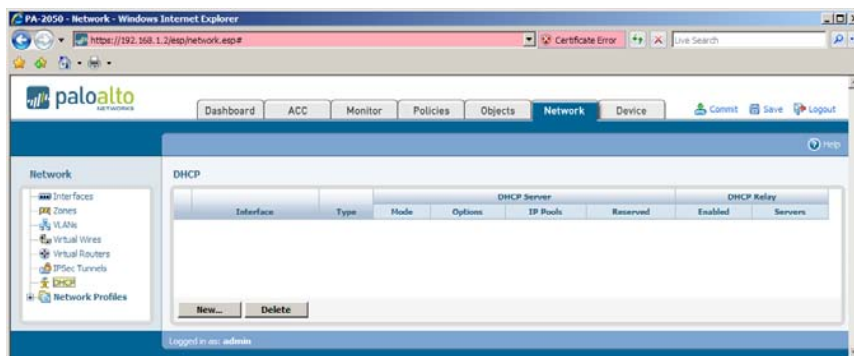
Configuring PA Firewalls for a Layer 3 Deployment



DHCP Server Configuration

PAN Firewalls support DHCP server functionality. Follow the steps below to configure a **DHCP** server for the internal (trust) interface.

1. Navigate to the **Network** tab and click on the DHCP link in the left navigation pane to see the configured DHCP options. Click on the New button to add a **new** DHCP server



2. On the New DHCP Interface configuration page select "ethernet 1/2" in the **Interface** dropdown menu and select "DHCP server" in the **Type** dropdown. Next, fill in the appropriate fields. At a minimum configure **Preferred DNS**, **Gateway** and an **IP Pool**. Use the example below as a reference.

Configuring PA Firewalls for a Layer 3 Deployment

The screenshot shows a web browser window titled "New DHCP Interface - Webpage Dialog". The URL is "https://192.168.1.2/esp/ed3DhcpInterface.asp?mode=new". The configuration is as follows:

- Interface: ethernet1/2
- Type: DHCP Server
- Mode: enabled
- Options:
 - Lease: 12 hours, 0 minutes
 - Preferred DNS: 4.2.2.1
 - Alternate DNS: 4.2.2.2
 - Preferred WINS: (empty)
 - Alternate WINS: (empty)
 - Preferred NIS: (empty)
 - Alternate NIS: (empty)
 - Gateway: 192.168.1.1
 - POP3 Server: (empty)
 - SMTTP Server: (empty)
 - Domain Name: parlab.com
- IP Pools: 192.168.1.200-192.168.1.210
- Reserved Addresses: (empty)

- Once completed with the DHCP configuration page click the OK button and verify the configuration looks similar to the screenshot below.

The screenshot shows the Palo Alto Networks management console. The "Network" tab is selected, and the "DHCP" configuration for interface "ethernet1/2" is displayed. The configuration is summarized in the following table:

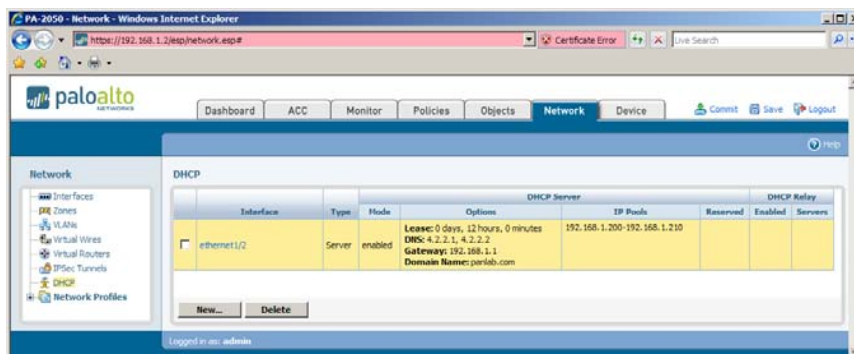
Interface	Type	Mode	Options	IP Pools	Reserved	Enabled	DHCP Relay Servers
ethernet1/2	Server	enabled	Lease: 0 days, 12 hours, 0 minutes DNS: 4.2.2.1, 4.2.2.2 Gateway: 192.168.1.1 Domain Name: parlab.com	192.168.1.200-192.168.1.210			

Outbound NAT Configuration

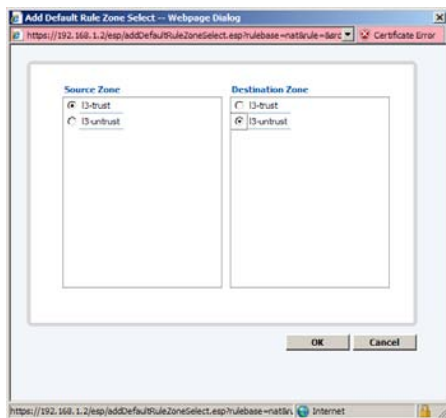
PAN firewalls support many types of Network Address Translation, this particular section is solely focused on configuring NAT for user traffic destined to the Internet. The following steps outline the configuration for outbound NAT using the external interface IP address and dynamic port address translation.

Configuring PA Firewalls for a Layer 3 Deployment

1. Navigate to the **Policies** tab and click on the **NAT** link in the left navigation pane to see the NAT policy. Click on the **Add Rule** button to add a new NAT rule.

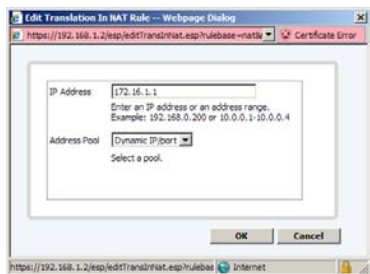


2. Next select the source and destination zones to be used as a match in the NAT rule. Select the "I3-trust" zone for the Source Zone and select the "I3-untrust" zone for the Destination Zone. In the following example, any traffic that enters the firewall on the "I3-trust" zone and leaves using the "I3-untrust" zone could be a match for this rule, depending on the address columns configured in the next steps. Click the **OK** button to return to the NAT rulebase.

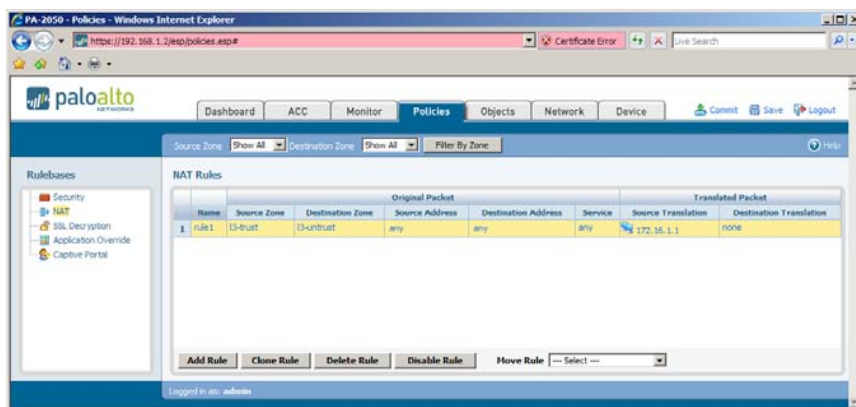


Configuring PA Firewalls for a Layer 3 Deployment

3. Click the “none” link in the **Source Translation** column to bring up a new window where you can select the source IP address you want to be used for traffic destined for the Internet. If you only have a single public IP address, you must enter the IP address of the external (untrust) interface. Select “Dynamic IP/port” and then click the **OK** button to return to the NAT rulebase.



4. Your NAT rulebase should now look like the example below, which will translate the source IP address of any internal user destined for the Internet.



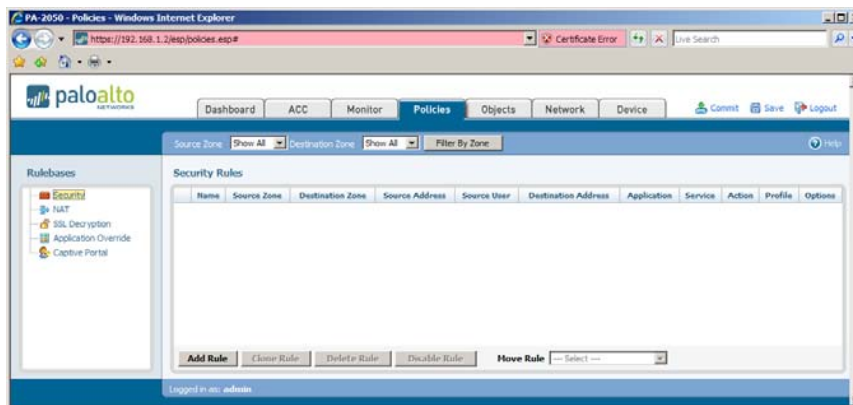
Security Policy Configuration

By default PAN firewalls drop any traffic that is not specifically allowed. The following steps outline the configuration for a basic security policy to allow

internal users to access the Internet and log all of their traffic. Like most firewalls, traffic is checked against the security policy from top to bottom and once a match is made, the action in the Action column is performed. If the action for the security rule is not “deny”, then all traffic is processed against the configured security profiles in the *Profile* column (covered in next section).

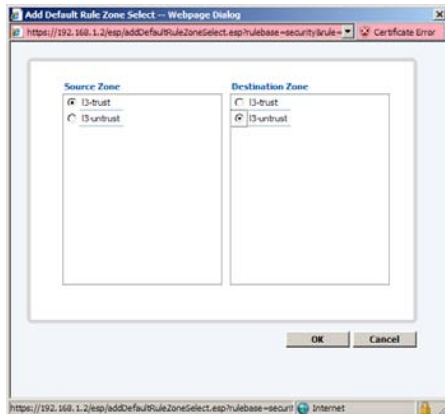
Controlling Application Usage

1. Navigate to the **Policies** tab and click on the **Security** link in the left navigation pane to see the Security policy. Click on the **Add Rule** button at the bottom of the page to add a new security rule.



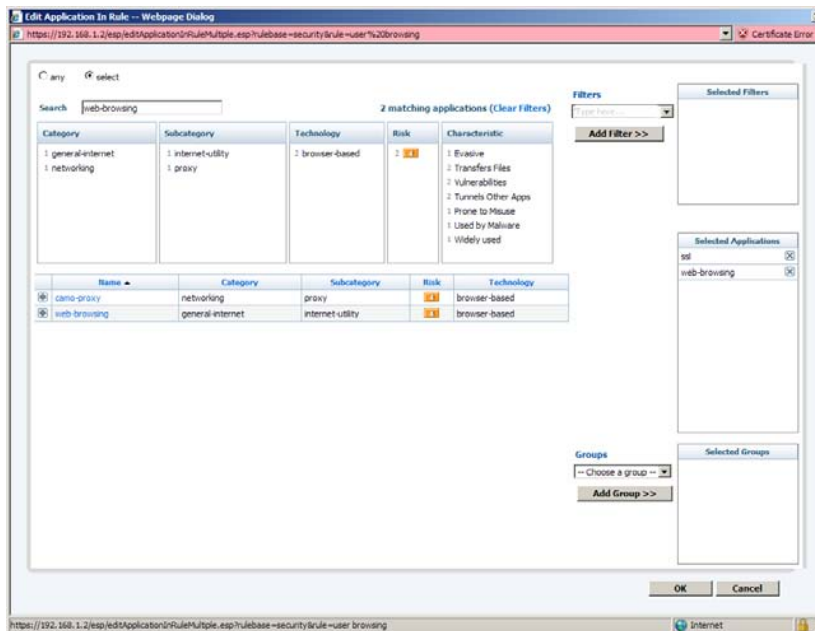
2. Next select the source and destination zones to be used as a match in the Security rule. Select the “I3-trust” zone for the **Source Zone** and select the “I3-untrust” zone for the **Destination Zone**. In the example below, any traffic that enters the firewall on the “I3-trust” zone and leaves using the “I3-untrust” zone could be a match for this rule, depending on the columns configured in the next steps. Click the **OK** button to return to the security rulebase.

Configuring PA Firewalls for a Layer 3 Deployment

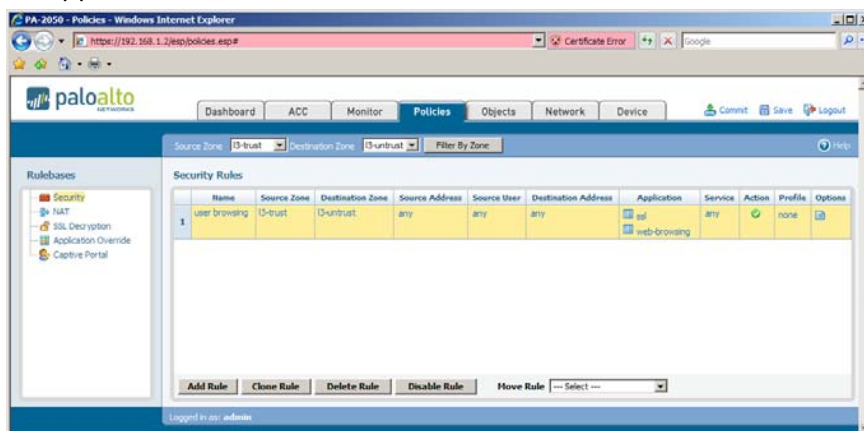


3. Since we are building a generic rule for web-browsing, we will leave the **Source Address, Source User** and **Destination Address** columns set to “any”. Later we can make changes to select IP addresses, subnets or even AD users/groups if the User Identification feature is used.
4. Next, click the “any” link in the **Application** column to open a new window where you can select the applications you want to be used as a match in this security rule. At the top of this page you will notice five fields that can be used to filter applications to be selected for this security rule. For example, if you only wanted to see applications that were “media” related, you could select the “media” category in the first box that is labeled **Category**. Once filtered on “media”, you could add another filter and select a **Subcategory** of “photo-video” to only see applications that are photo or video related. For this rule we are just concerned with web browsing and SSL traffic so it is easiest just to type the name of the application in the Search field and then click the “+” symbol (next to the application in the list) to add the application to the **Selected Applications** field.

Configuring PA Firewalls for a Layer 3 Deployment



5. Select the “web-browsing” and “ssl” applications and click the **OK** button to return to the security rulebase. Note, this example assumes DNS is located on the internal network. If you are using a DNS server located on the Internet, be sure to add DNS as an application.



Note: All security rules can be labeled to aid in troubleshooting later. Any description entered in the Name column will be shown as a column in the logs. For the example above, we used the label “web browsing”.

6. At this point it is a good idea to click the Commit link located in the top right corner of the browser to verify, save and commit the changes made. No changes are saved to running configuration until the commit link is clicked.

Controlling Threats

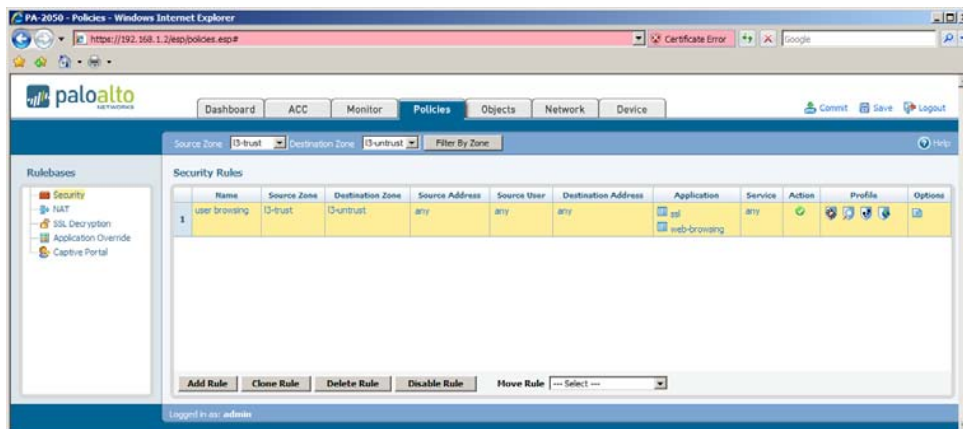
In addition to controlling application usage, PAN firewalls can provide URL filtering, Threat Prevention and Data filtering capabilities. PAN uses the concept of “Security Profiles” for each type of content inspection performed and for each security rule created, the following types of Security Profiles can be added to perform additional content inspection:

- Antivirus: The ability to detect/block viruses in files
- Vulnerability Protection: The ability to detect/block client or server exploits.
- Anti-Spyware: Includes download and phone-home protection against spyware.
- URL Filtering: The ability to detect/block URL’s accessed by users.
- File Blocking: The ability to block file types on a per-application basis.
- Data Filtering: The ability to detect/block Credit Card numbers, Social Security numbers and documents containing specific keywords.

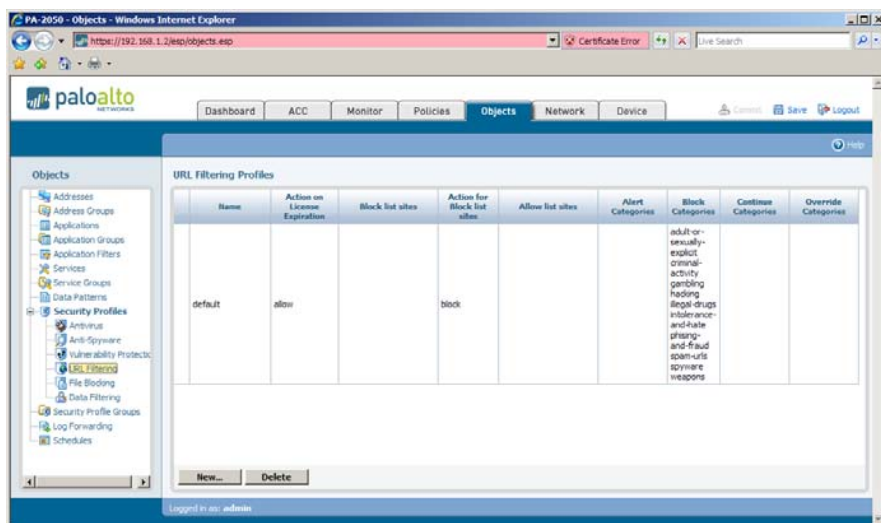
All traffic is checked against the security policy from top to bottom and once a match is made, the action in the **Action** column is performed. If the action is not “deny” and one or more security profiles are configured for a rule, traffic is further inspected by each configured security profile that each have their own configured actions. All PAN firewalls come with default profiles that are a good starting point for a security policy. Follow the steps below to apply default security profiles for Antivirus, Vulnerability Protection, Anti-Spyware and URL filtering. Once you are comfortable with the concept of security profiles, you can create your own custom profiles.

1. Navigate to the Policies tab and click on the **Security** link in the left navigation pane to see the Security policy. You should see the rule we created in the previous section. On the right side of the screen there is a **Profile** column, click on the “none” link to bring up a dialog to add security profiles to this security rule. Following the example below, select “default” for Antivirus, Vulnerability Protection, Anti-Spyware and URL filtering profiles. Once the “default” profiles are selected, click the OK button to return to the security rulebase.
2. As shown in the example below, your security policy should now have four icons in the **Profile** column representing the four security profiles we just added to the security rule:

Configuring PA Firewalls for a Layer 3 Deployment



3. If desired, you can view the default profiles but they cannot be edited. To view the default security profiles navigate to the **Objects** tab and expand the **Security Profiles** link in the left navigation pane. If you are using the default URL filtering profile, take a look at the example below see what categories are blocked by default:



Security Rule Options

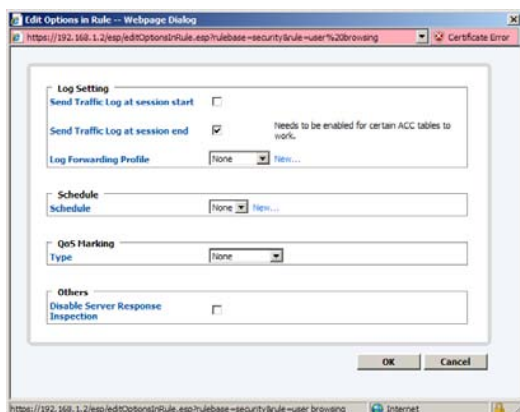
Each security rule has additional options that can be enabled. These include the following:

- Log at session start
- Log at session end
- Apply log forwarding profile

Configuring PA Firewalls for a Layer 3 Deployment

- Apply schedule
- Apply QoS Marking
- Disable Server Response Inspection

The default option is to log the session upon once it is closed but sometimes it is necessary to enable logging at session start for troubleshooting. Configuration of these options is beyond the scope of this document, so please refer to the online help in the User Interface for more information on the options shown below.

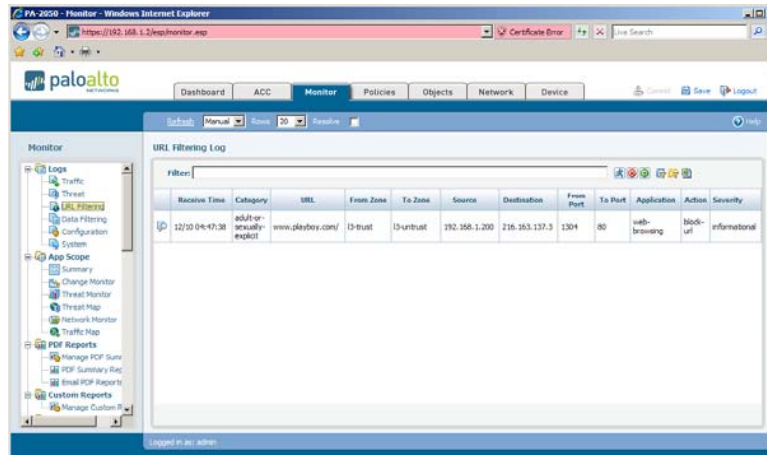


Test Connectivity

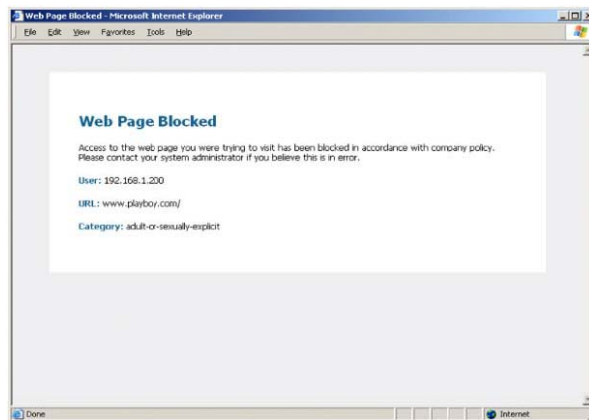
At this point, you should be able to connect a user workstation configured for DHCP to a network attached to interface ethernet1/2 and access any web site not blocked by the default URL filtering profile.

Configuring PA Firewalls for a Layer 3 Deployment

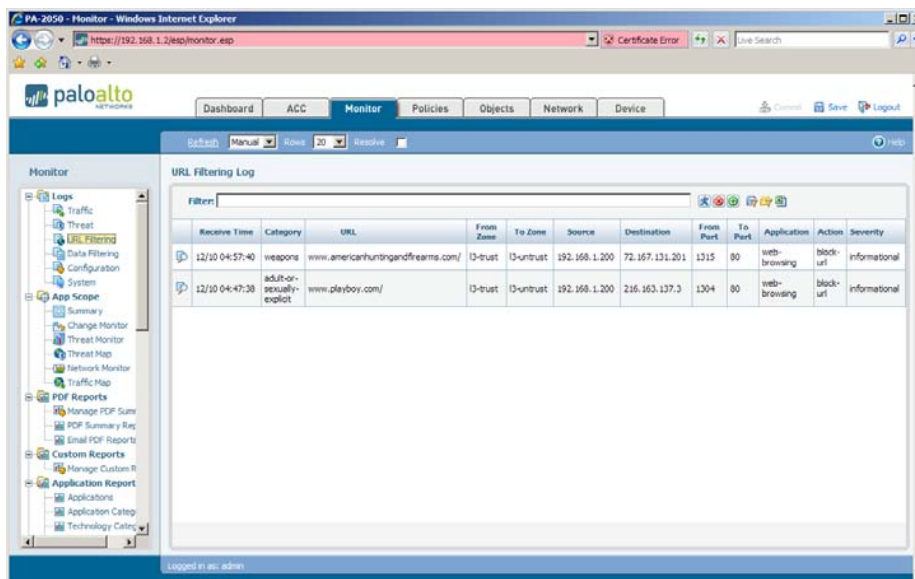
1. Below you can see a log entry for a user trying to access a website that was blocked by the default URL filtering profile.



The following is what an end-user accessing a blocked URL category would see. This is the default URL Filtering block page, custom block pages can also be configured.



2. The following is an example of a log entries generated from user activity using the default URL filtering profile.



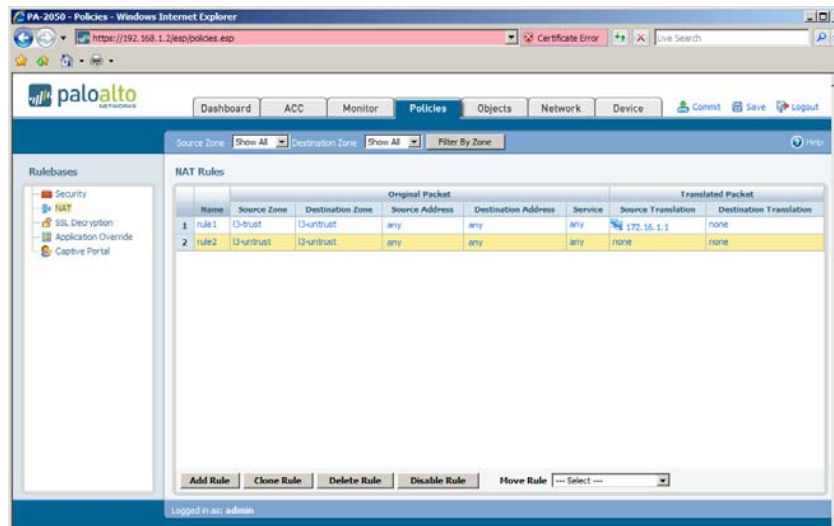
Configuring Inbound NAT

If you have an environment with internal servers using non-routable (RFC 1918) IP addresses, you will need to configure an inbound NAT rule to allow the outside world to reach these servers. The steps below detail the configuration to allow clients on the Internet to access an internal web server using HTTP (TCP/80).

Configure NAT Rule

1. Navigate to the **Policies** tab and click on the **NAT** link in the left navigation pane to see the NAT policy. Click on the **Add Rule** button to add a new NAT rule and then select the source and destination zones to be used as a match for this NAT rule. Since the source and destination IP address of this traffic both reside in the "I3-untrust" zone, you will need to select the "I3-untrust" zone as the Source Zone and as the Destination Zone for this NAT rule. Your NAT policy should now look like the example shown below.

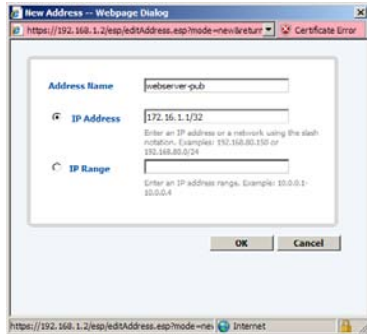
Configuring PA Firewalls for a Layer 3 Deployment



- Next, click the "any" link in the **Destination Address** column. This will bring up a new window where you can select or add IP address you want to be used as a match for this NAT rule. Since this is a new configuration there are no address object defined. To define a new address, click on the **New Address** button to configure an address object for the web server.
- Since external users are trying to reach this server on a public IP address, we will use this public address when configuring the new address object. In the **Address Name** field give the object a name you will recognize since this is how the new object will be represented in a NAT or Security rule. In the example below, we only have a single public IP address that is being used by the firewall's external interface, so it is necessary to specify the IP address of the external interface here. In the example below, the external interface is 172.16.1.1 so that is the IP address that needs to be configured. Be sure to give the object a name of "webserver-pub" and specify the subnet mask, which in this case is "/32" to represent a single host address.

Click the **OK** button to return to the address selection dialog.

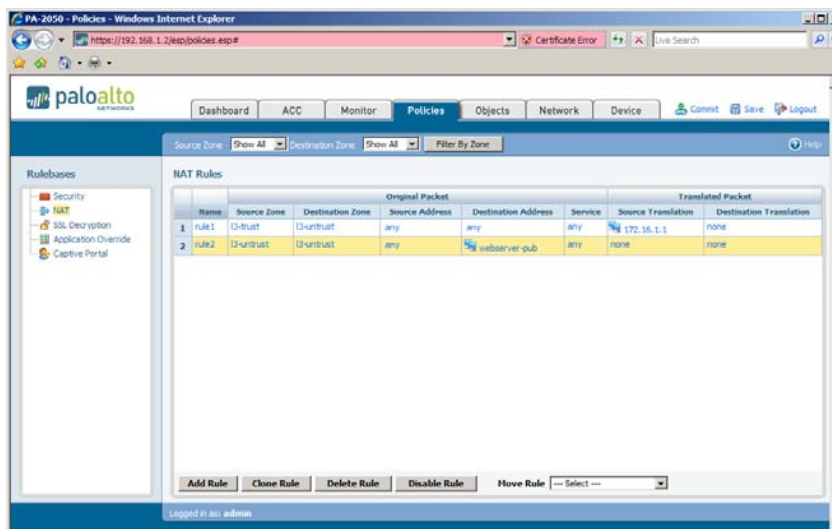
Configuring PA Firewalls for a Layer 3 Deployment



- Next, select the object "webserv-pub" and then click the **Add** button to use this address in this NAT rule. Click the **OK** button to return to the NAT rulebase.

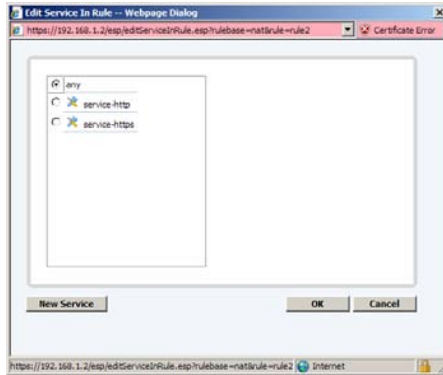


- At this point, your NAT rulebase should look like the example below:

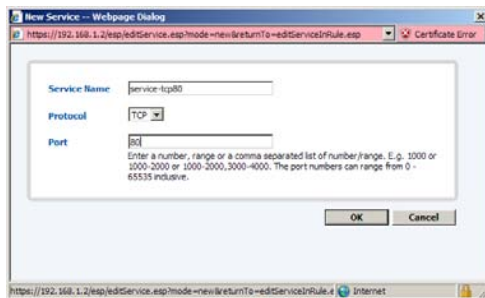


Configuring PA Firewalls for a Layer 3 Deployment

- Next we need to configure the service column to specify HTTP (TCP/80) as a match for this rule. Click the “any” link in the Service column to bring up a new window where you can select an existing service or create a new service. Click the **New Service** button at the bottom of the page to create a new service for our inbound HTTP.

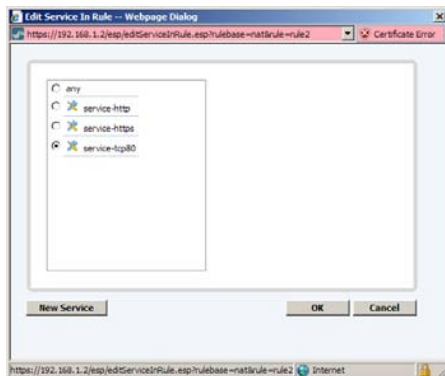


- To create a new service, first give the service a name of “service-tcp80”. Since we also have predefined applications that are based on signatures/decoders/heuristics, it is a good idea to give your port/protocol based services a name so they are easily distinguished from predefined application names. For example, for a service of TCP/80 use the name, “service-tcp80’. Click the Protocol dropdown and select “TCP” and enter 80 for the port number as shown in the example below. Click the **OK** button to return to the service selection dialog.

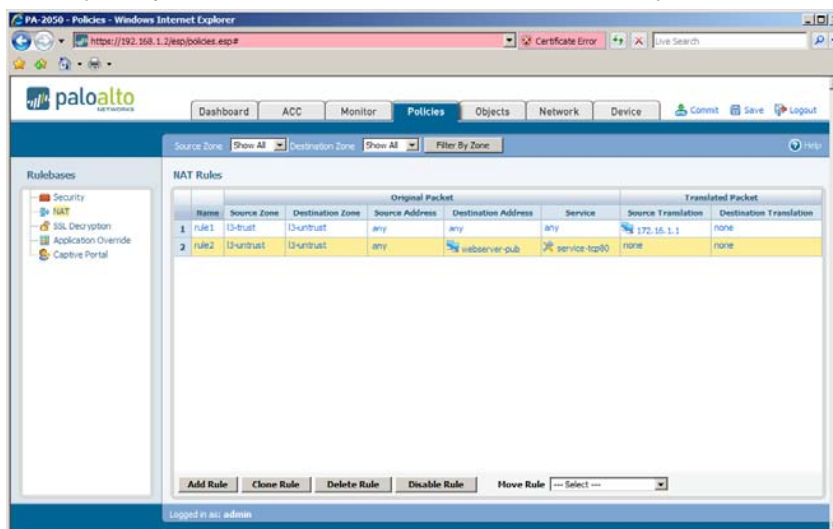


- Now you should see the service object you created in the previous step. Select “service-tcp80” and then click the **OK** button to return to the NAT rulebase.

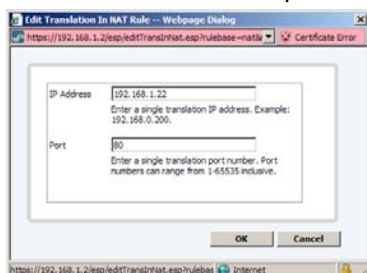
Configuring PA Firewalls for a Layer 3 Deployment



9. At this point, your NAT rulebase should look like the example below:

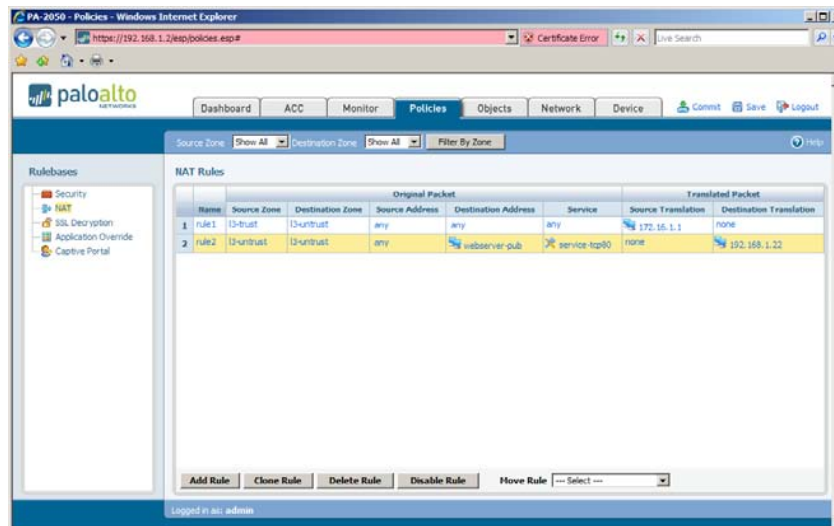


10. Next, we need to configure the rule to translate the destination IP address so traffic can reach the internal web server. Click on the “none” link in the **Destination Translation** column and then enter the IP address and port of the internal web server as shown in the example below:



11. Finally, your NAT rulebase should look like the example below. All that is left is to configure a security policy to allow the traffic to pass from the “I3-untrust” zone to the “I3-trust” zone. Optionally, a Vulnerability Protection profile can be added to protect the server.

Configuring PA Firewalls for a Layer 3 Deployment



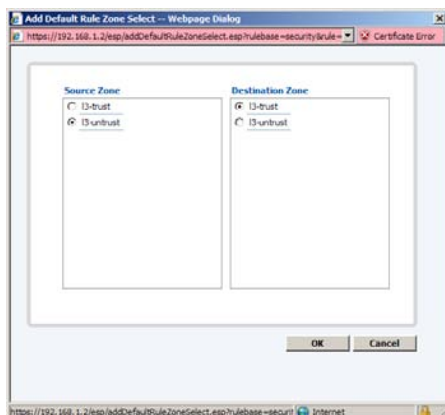
Note: Management profiles can be configured on any Layer 3 interface to allow administrators to remotely reach the CLI or WebUI of the firewall. You cannot have inbound NAT services that overlap management services enabled on a forwarding interface. For example, if you enable SSL management on the external interface, you would not be able to forward TCP/443 to an internal server since the firewall would respond on this port/protocol instead of performing NAT and forwarding.

Configure Security Rule for Inbound NAT

In addition to a NAT policy, a Security Policy is required to allow traffic to reach the internal web server. Follow the steps below to configure an inbound security policy to allow external users to reach an internal web server using HTTP.

1. Navigate to the Policies tab and click on the Security link in the left navigation pane to see the Security policy. Click on the Add Rule button to add a new security rule. Next select the source and destination zones to be used as a match in the Security rule. Since the client has a source IP address that resides on the external interface and the internal web server resides on the internal interface, select the "I3-untrust" zone for the Source Zone and select the "I3-trust" zone for the Destination Zone.

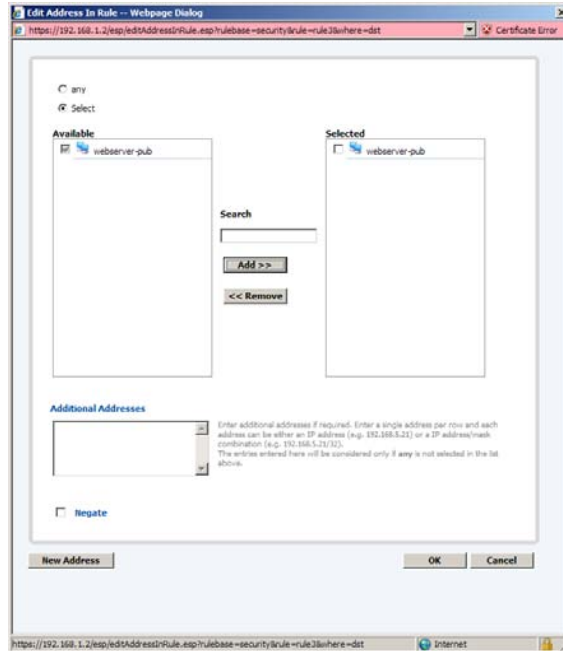
Click the **OK** button to return to the security rulebase.



Note: The source and destination zones are different than what was configured in the NAT rulebase. This is because all policies (i.e. security, NAT, captive portal, etc.) use the IP addresses of the original packets as a match for all rules. However, it is important to note that the zones used for matching a rule can be different. In this example, a public address object is used in the **Destination Address** column but the internal "13-trust" zone is used in the **Destination Zone** column.

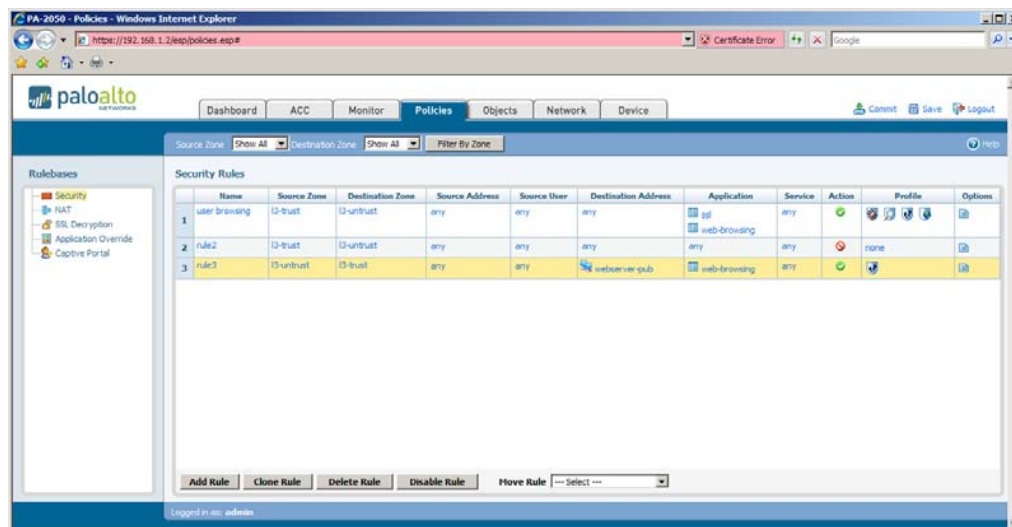
2. Next, click the "any" link in the **Destination Address** column. This will bring up a new window where you can select or add an IP address you want to be used as a match for this security rule. We created the object, "webserver-pub" for the web server in the previous NAT configuration, so all that is left to do here is select the "webserver-pub" object, click the **Add** button and then click the **OK** button to return to the security rulebase.

Configuring PA Firewalls for a Layer 3 Deployment



3. Next we need to specify the application/service, created previously, as a match for this inbound security rule. Click the “any” link in the **Application** column to bring up a window where we can select the applications to be used in this rule. For this example, we will also want to apply an inbound vulnerability protection profile, so it is necessary to select a predefined application instead of the custom service created previously. This is necessary because vulnerability signatures are logically assigned to application signatures to improve performance and increase accuracy. To apply the appropriate server protection signatures to this inbound traffic, we will need to select “web-browsing” as the application. Next, click the **OK** button to return to the security rulebase, your security rulebase should look like the example below:

Configuring PA Firewalls for a Layer 3 Deployment



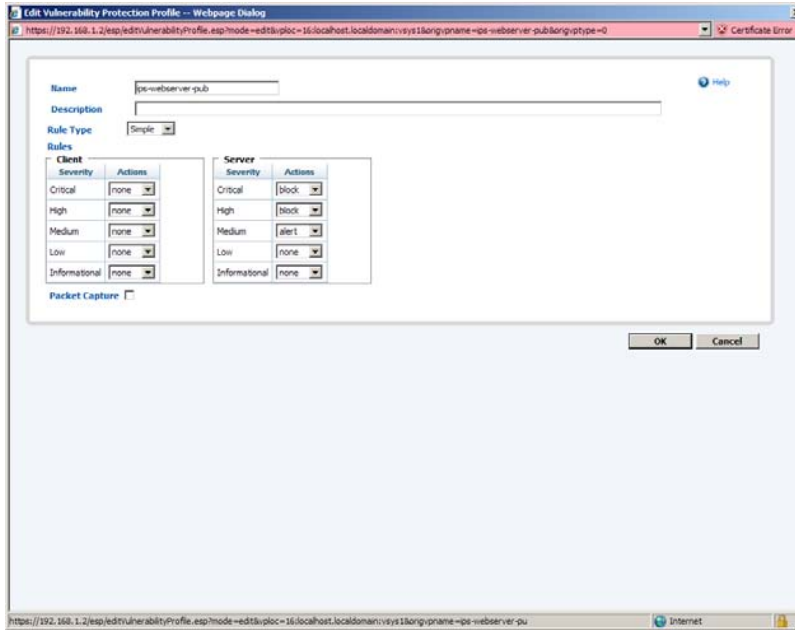
Configure Vulnerability Protection for Inbound NAT

Since this is a public-facing web server, it is recommended that a Vulnerability Protection profile be applied to protect the server. Follow the steps below to apply a default security profile for an internal web server.

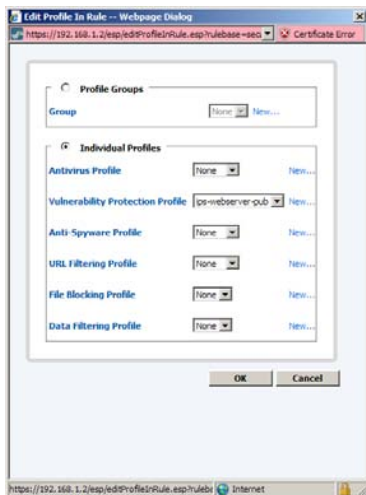
1. Navigate to the **Policies** tab and click on the **Security** link in the left navigation pane to see the Security policy. You should see the inbound security rule we created in the previous section. On the right side of the screen there is a **Profile** column, click on the “none” link to bring up a dialog to add a security profile to this rule. Since we only care about server vulnerabilities, we need to create a custom profile. Click the “New” link next to the **Vulnerability Protection Profile** dropdown. Following the example below, create a new profile with only server signatures enabled for Medium (alert), High (block) and Critical (block) severity vulnerabilities.

Click the **OK** button to return to the security profile selection dialog.

Configuring PA Firewalls for a Layer 3 Deployment

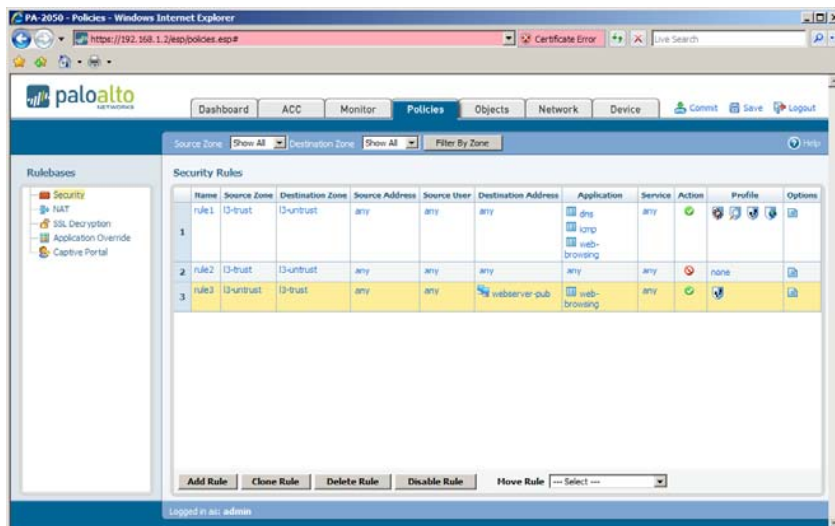


2. On the profile selection page, make sure the new profile is selected and click the **OK** button to return to the security rulebase.



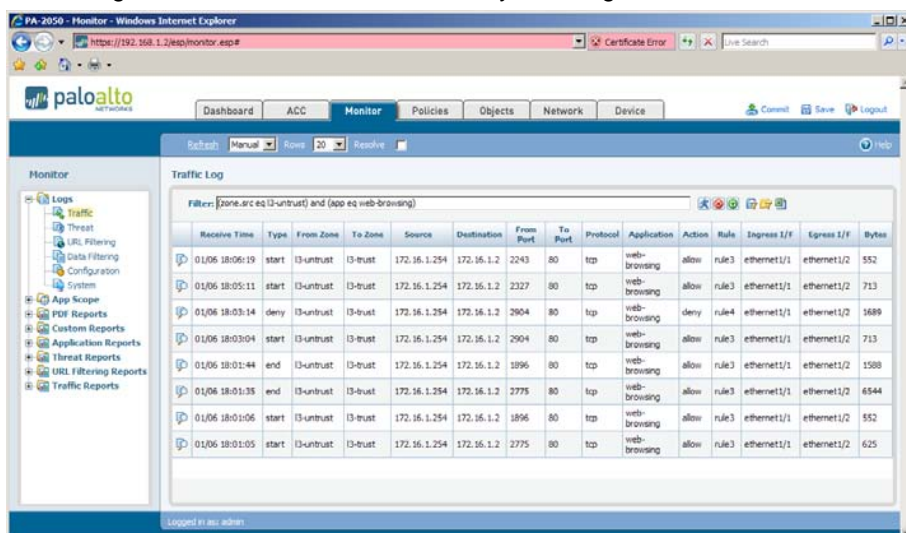
3. Your security policy should now look like the example below.

Configuring PA Firewalls for a Layer 3 Deployment



Note: Since the content being served by the web server is considered “trusted” content, it is a good idea to disable the inspection of the content in the web server responses. This setting can be found in the Options column of the security rulebase and this setting is disabled by default.

- At this point you should be able to test connectivity to the internal server from the Internet. The following Traffic Log entries show TCP/80 successfully reaching the internal web server.



Conclusion

Following the steps detailed in this document you should be able to configure any Palo Alto Networks firewall to serve as the perimeter firewall and provide secure inbound and outbound services to internal users and customers.

For additional information regarding any of the features and configurations covered in this document, please refer to the online help in the WebUI or the Administrator's Guide, which can be found on the support site. The support site also contains several documents that provide detailed concepts and configuration on the most commonly used features in PANOS.