



## **PAN-OS 7.0 FIREWALL ESSENTIALS LAB SERIES**

### **Lab 4: Basic App ID**

**Document Version: 2016-04-19**

Copyright © 2016 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

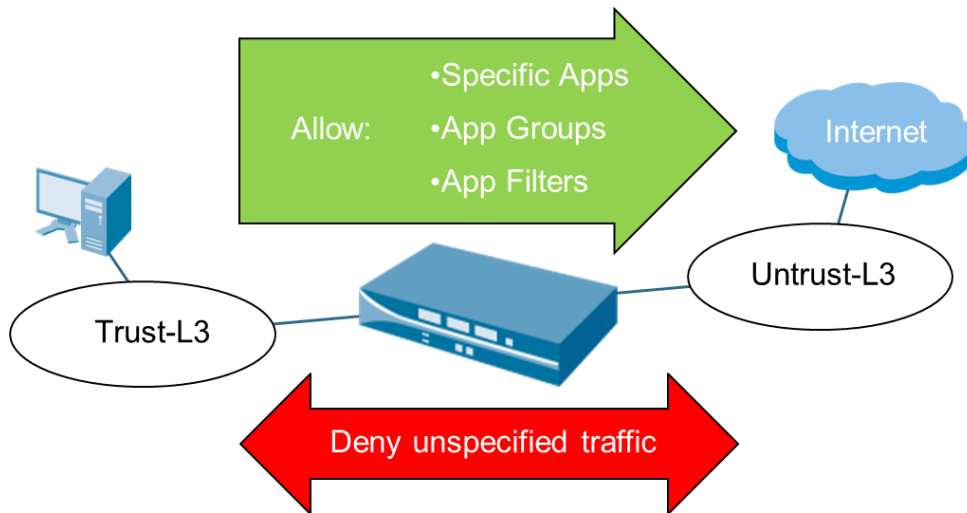
NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

## Contents

Introduction .....	3
Objective .....	4
Pod Topology .....	5
Lab Settings .....	6
1 Load Network Configuration.....	7
2 Create a General Internet Policy.....	10
3 Enable Interzone Logging.....	14
4 Enable the Application Block Page .....	16
5 Verify Internet Connectivity and Application Blocking.....	17

## Introduction



Now that you have confirmed that your workstation has connectivity to the Internet, you will delete the Allow All Out Security Rule and replace it with a more restrictive Security Rule. By default, the PAN Firewall will block any traffic between different Security Zones. You will create a Security Policy to selectively enable specific applications to pass from the Trust-L3 to the Untrust-L3 Zone. All other applications will be blocked.

Create a Rule named *General Internet*, which allows users in the Trust-L3 zone to use a set of commonly used applications such as dns, flash, ftp, ping, ssl, and web-browsing. The applications should only be permitted on an application's default port. All other traffic (inbound and outbound) between Zones will be blocked and logged so that you can identify what other applications are being used.

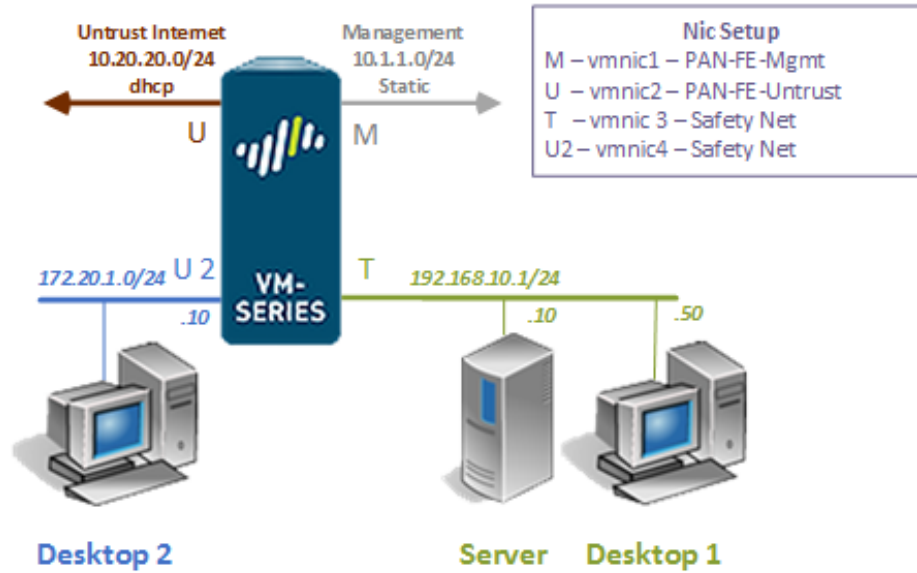
Next, you will configure the firewall to notify users when applications are blocked by a Rule.

## Objective

In this lab, you will be utilizing Palo Alto technology to perform the following tasks:

1. Create a new Security Policy to allow internet connectivity
2. Enable Application Block pages

## Pod Topology



## Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Ubuntu Desktop 1	192.168.10.50	sysadmin	Train1ng\$
Ubuntu Server	192.168.10.10	sysadmin	Train1ng\$
Ubuntu Desktop 2	172.30.1.10	sysadmin	Train1ng\$
Palo Alto Firewall	192.168.10.1 172.30.1.1	admin	paloalto

## 1 Load Network Configuration

1. Click on the **Desktop 1** graphic found on the *topology page*.
2. Login using **sysadmin** as the *username* and **Training\$** as the *password*. Click **Log In**.
3. Double-click on the **Firefox Web Browser** icon located on the *Desktop*.



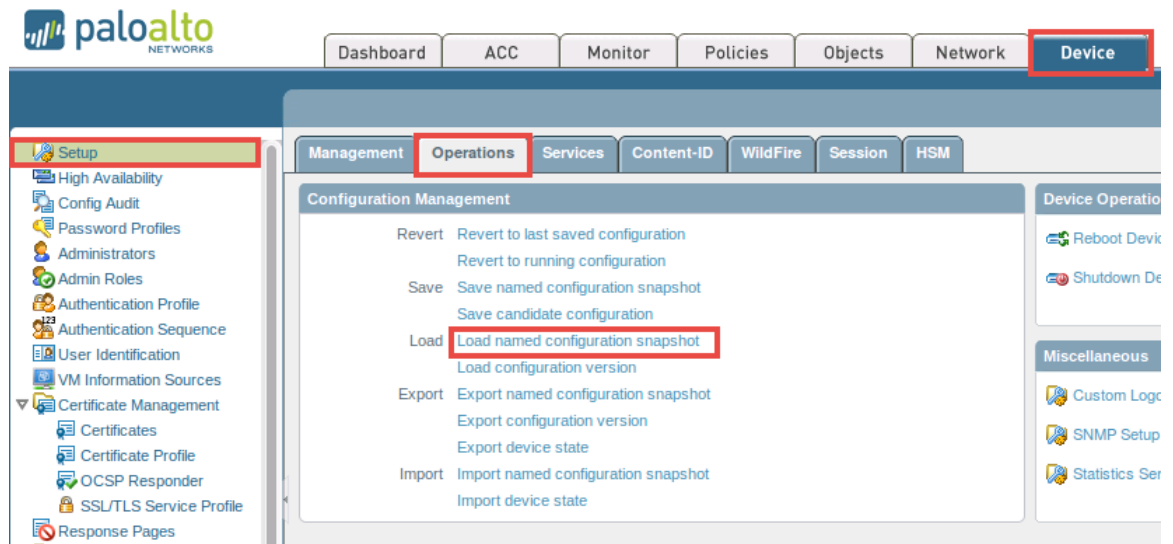
4. In the address field, type **https://192.168.10.1** and press **Enter**.

If you experience the “Unable to connect” message while attempting to connect to the specified IP above, please wait an additional 3-5 minutes for the PA VM to fully initialize and refresh the page to continue.

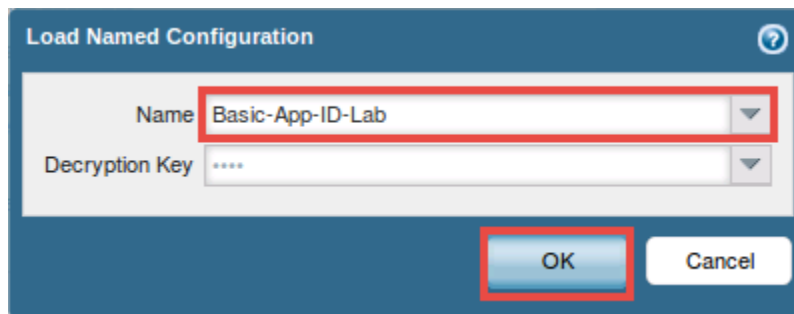
5. Login with the *username* **admin** and *password* **paloalto** on the firewall web interface.



- Using the *Palo Alto WebUI*, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



- In the *Load Named Configuration* window, select **Basic-App-ID-Lab** from the *Name* drop-down box. Click **OK**.

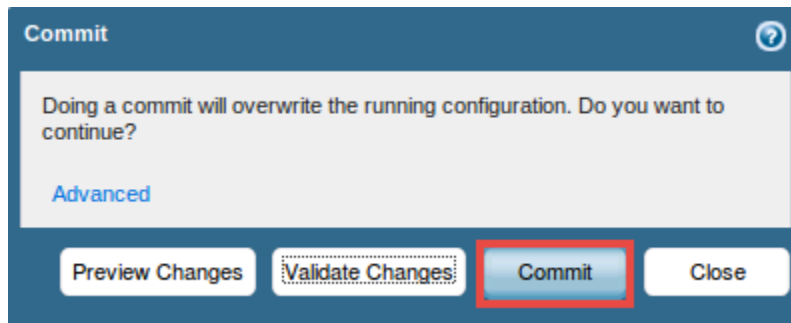


- When prompted with the config loaded message, click on the **Close** button to continue.
- Click on the **Commit** link located at the top-right of the *WebUI*.

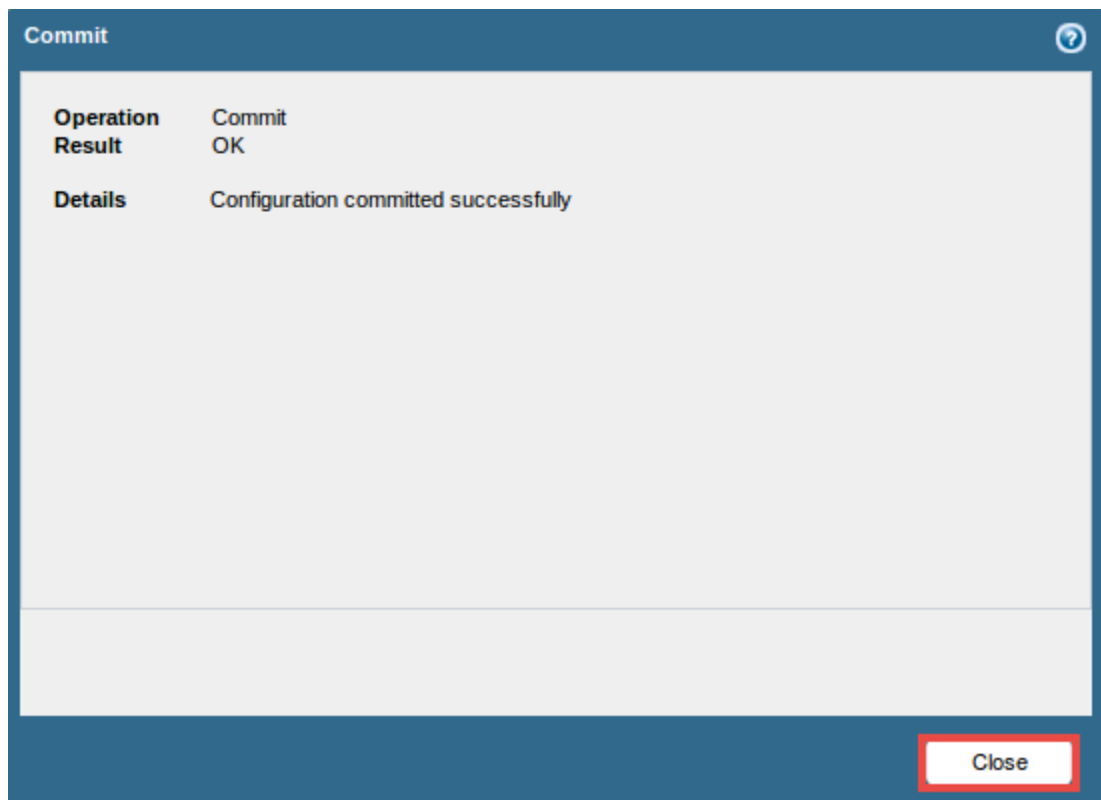




10. In the *Commit* window, click **Commit** to proceed with committing the changes.



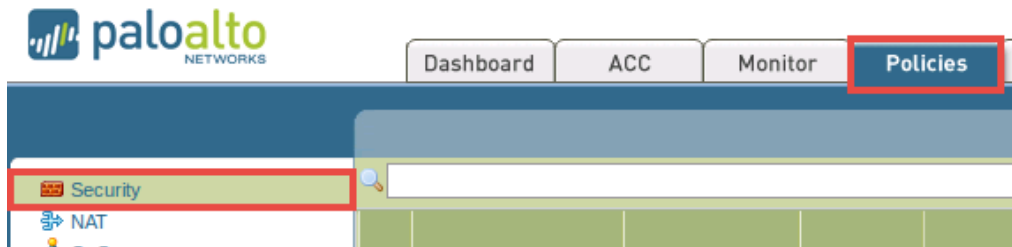
11. Once the operation successfully completes, click **Close** to continue.



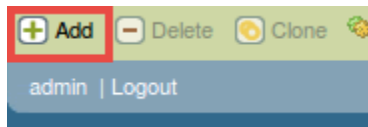
12. Leave the *WebUI* opened to continue with the next task.

## 2 Create a General Internet Policy

1. Using the *Palo Alto WebUI*, navigate to **Policies > Security**.

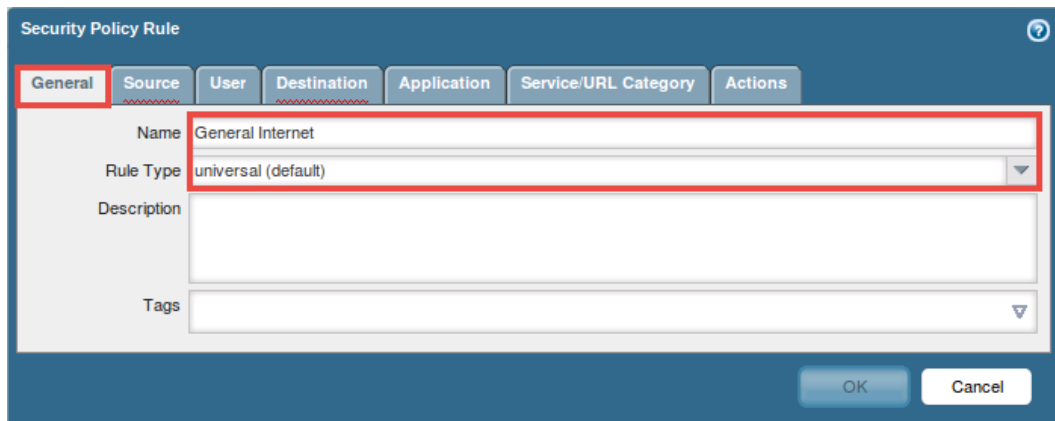


2. Click on **Add**, located near the bottom of the window, to define a new security policy.



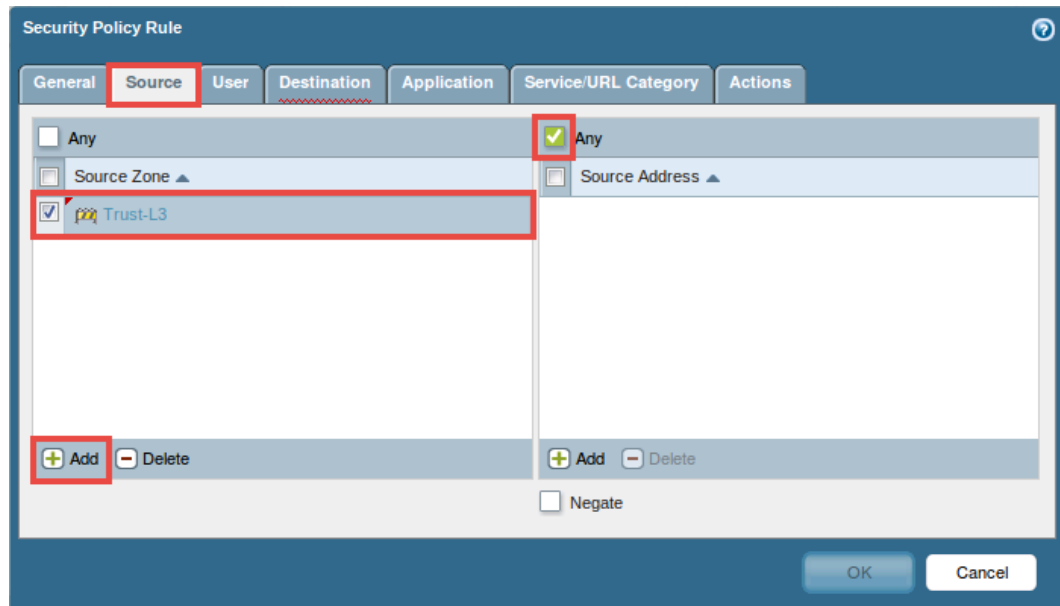
3. In the *Security Policy Rule* window, click on the **General** tab and use the information in the table below to configure the correct form fields.

Field	Data/Selection
Name	Enter <b>General Internet</b>
Rule Type	Select <b>universal (default)</b>



- In the *Security Policy Rule* window, click on the **Source** tab and use the information in the table below to configure the correct form fields.

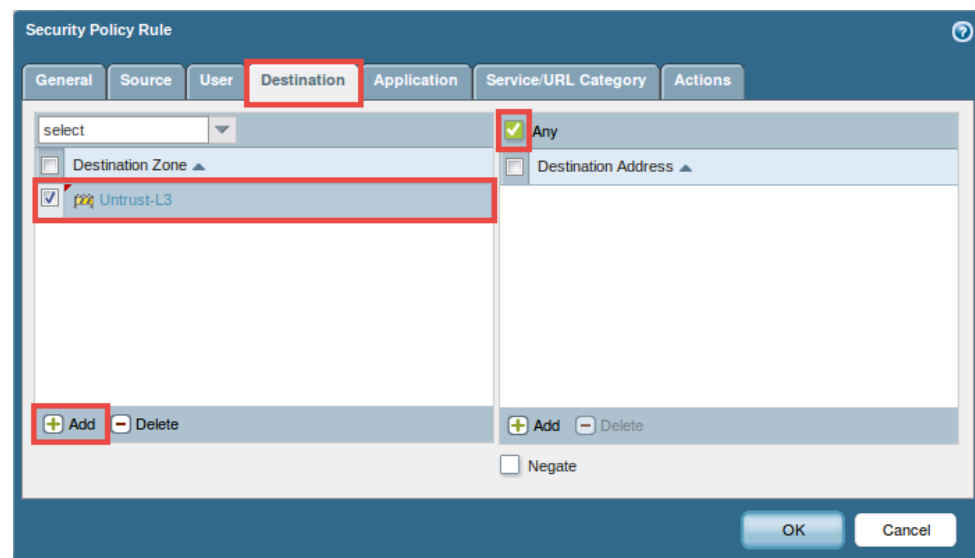
Field	Data/Selection
Source Zone	Click <b>Add</b> and select <b>Trust-L3</b>
Source Address	Select <b>Any</b>



The screenshot shows the 'Security Policy Rule' window with the 'Source' tab selected. The 'Source Zone' list on the left contains 'Trust-L3' with a checkmark, and the 'Source Address' list on the right contains 'Any' with a checkmark. The 'Add' button at the bottom left is highlighted with a red box. The 'Negate' checkbox is unchecked.

- In the *Security Policy Rule* window, click on the **Destination** tab and use the information in the table below to configure the correct form fields.

Field	Data/Selection
Destination Zone	Click <b>Add</b> and select <b>Untrust-L3</b>
Destination Address	Select <b>Any</b>



The screenshot shows the 'Security Policy Rule' window with the 'Destination' tab selected. The 'Destination Zone' list on the left contains 'Untrust-L3' with a checkmark, and the 'Destination Address' list on the right contains 'Any' with a checkmark. The 'Add' button at the bottom left is highlighted with a red box. The 'Negate' checkbox is unchecked.

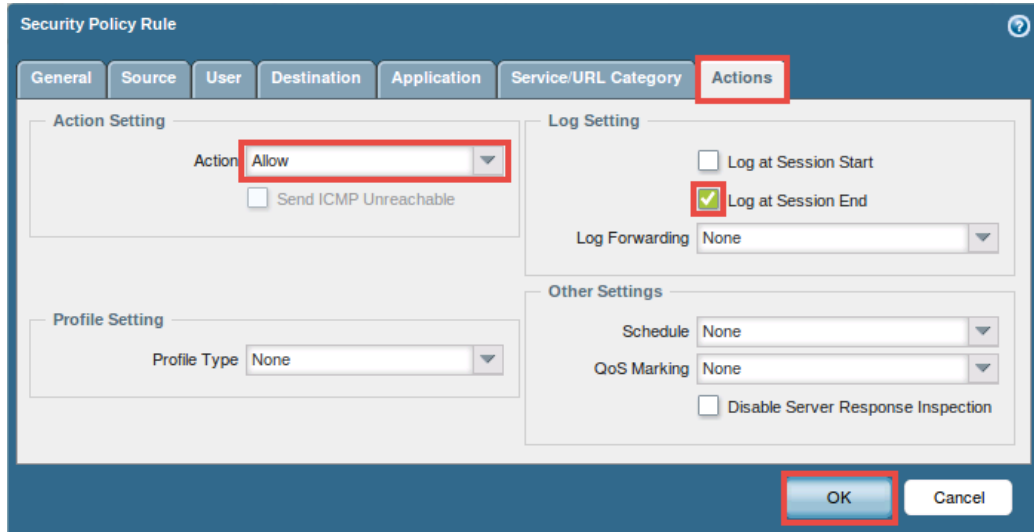
- In the *Security Policy Rule* window, click on the **Application** tab and use the information in the table below to configure the correct form fields.

Field	Data/Selection
<i>Applications</i>	Click <b>Add</b> and select each of the following: <ul style="list-style-type: none"> <li>• <b>dns</b></li> <li>• <b>flash</b></li> <li>• <b>ftp</b></li> <li>• <b>ping</b></li> <li>• <b>ssl</b></li> <li>• <b>web-browsing</b></li> </ul>



- In the *Security Policy Rule* window, click on the **Service/URL Category** tab and select **application-default** from the *Service* drop-down menu.
- In the *Security Policy Rule* window, click on the **Actions** tab and use the information in the table below to configure the correct form fields.

Field	Data/Selection
<i>Action Setting</i>	Select <b>Allow</b>
<i>Log Setting</i>	Select <b>Log at Session End</b>



The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action' dropdown is set to 'Allow'. The 'Log at Session End' checkbox is checked. The 'OK' button is highlighted.

**Security Policy Rule**

General Source User Destination Application Service/URL Category **Actions**

**Action Setting**

Action: **Allow**

☐ Send ICMP Unreachable

**Profile Setting**

Profile Type: None

**Log Setting**

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: None

**Other Settings**

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

**OK** Cancel

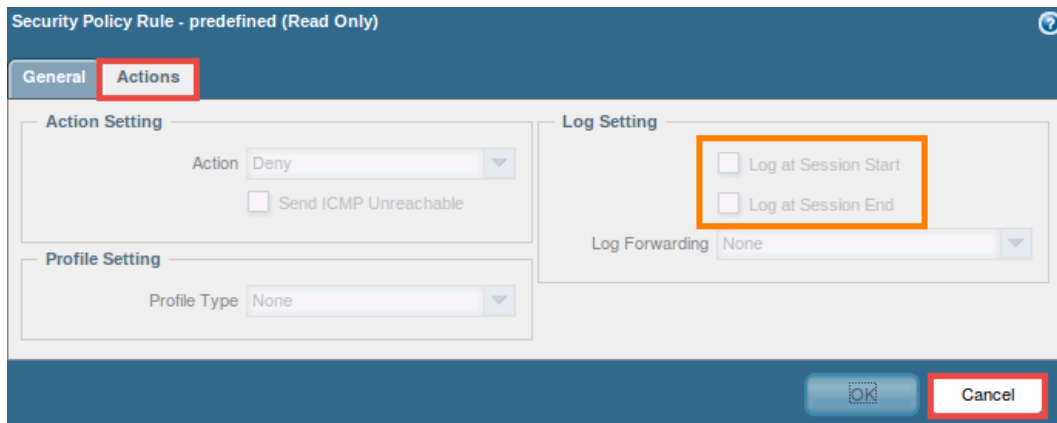
9. Click **OK** to save changes.
10. Verify that the new policy is listed.
11. Leave the *WebUI* opened to continue with the next task.

### 3 Enable Interzone Logging

1. Click on the **interzone-default** name underneath the *Name* column to open the policy. Make sure to click on the *interzone-default* policy with the **Deny** action (in the *Action* column) since there are two, identical *interzone-default* policies.

	Name	Tags	Type	Zone	Address
1	MGMT-PORT-OUT	none	universal	Mgmt-L3	192.168.1.1
2	General Internet	none	universal	Trust-L3	any
3	intrazone-default	none	intrazone	any	any
4	interzone-default	none	interzone	any	any

2. In the *Security Policy Rule – predefined (Read only)* window, click the **Actions** tab. Note that both *Log at Session Start* and *Log at Session End* are unchecked given no ability to check them.



Security Policy Rule - predefined (Read Only)

General Actions

Action Setting

Action: Deny

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☐ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: None

OK Cancel

3. Click **Cancel**.

4. Make sure the **interzone-default** policy with the **Deny** action (in the *Action* column) is selected (blue highlight), without opening the policy, and click **Override**.

	Name	Tags	Type	Zone	Address
1	MGMT-PORT-OUT	none	universal	Mgmt-L3	192.168.1.1
2	General Internet	none	universal	Trust-L3	any
3	intrazone-default	none	intrazone	any	any
4	interzone-default	none	interzone	any	any

+ Add
- Delete
Clone
Override
Revert
Enable
Disable
Move
High

admin | Logout

5. In the *Security Policy Rules – predefined* window, notice that the title does not display *Read Only*. Click on the **Actions** tab.
6. Check the **Log at Session End**.

Security Policy Rule - predefined

General Actions

Action Setting

Action Deny
Send ICMP Unreachable

Profile Setting

Profile Type None

Log Setting

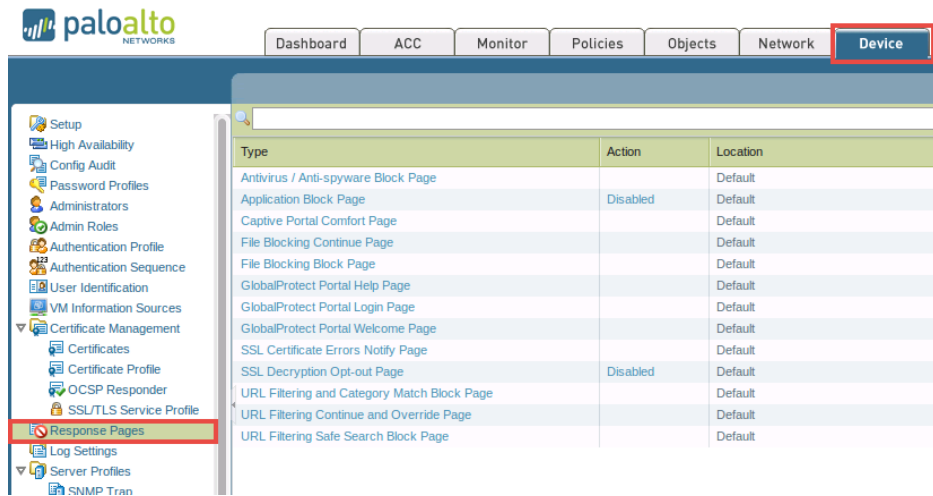
Log at Session Start
Log at Session End
Log Forwarding None

OK Cancel

7. Click **OK** to save changes.
8. Leave the *WebUI* to continue with the next task.

## 4 Enable the Application Block Page

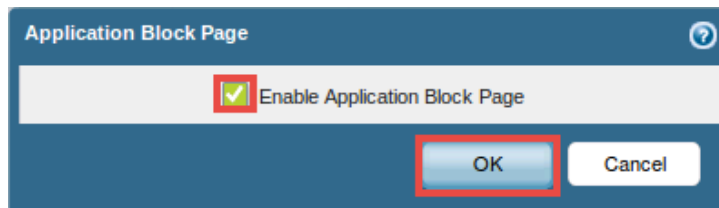
1. Using the WebUI, navigate to **Device > Response Pages**.



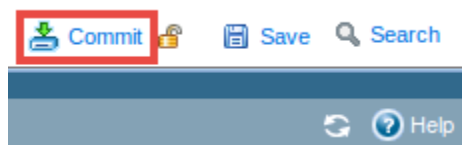
2. Identify **Application Block Page** from the list, and click on its respective *Action* column. In this case, it is the word **Disabled**.

Type	Action	Location
Antivirus / Anti-spyware Block Page		Default
Application Block Page	Disabled	Default
Captive Portal Comfort Page		Default
File Blocking Continue Page		Default
File Blocking Block Page		Default

3. In the *Application Block Page* window, check the box to **Enable Application Block Page**. Click **OK**.



4. Click on the **Commit** link, located at the top-right of the *WebUI*.

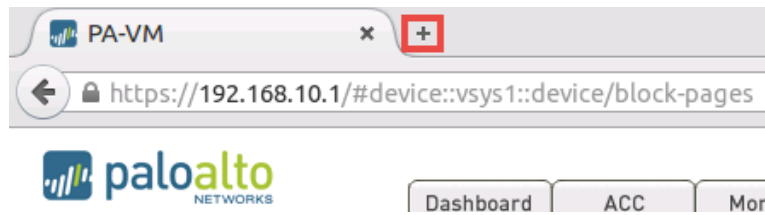


5. In the *Commit* window, click on the **Commit** button.
6. After the configuration successfully commits, click the **Close** button.
7. Leave the *Firefox* application opened to continue with the next task.



## 5 Verify Internet Connectivity and Application Blocking

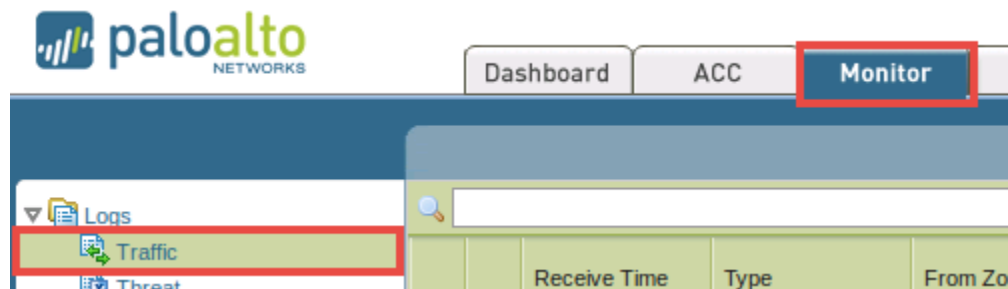
1. Using the *Firefox* web browser, open a new tab by clicking on the **(plus)** icon.



2. Type in **www.netdevgroup.com** in the address field followed by pressing **Enter** and verify that internet connectivity is present. You may also try common sites such as Google or Yahoo.
3. In the same tab, enter **www.depositfiles.com** in the address field followed by pressing **Enter**.

Notice that the *Application Blocked* page appears, indicating that the *depositfiles* application has been blocked.

4. Close the tab and navigate back to the first tab, **PA-VM**.
5. Using the *WebUI*, navigate to **Monitor > Logs > Traffic**.



6. Identify the traffic log specifically for when connecting to **depositfiles**. You can do this by clicking in the search bar and entering (*app eq depositfiles*). Notice that the application has been denied because it is not listed in the allowed applications in the *General Internet Policy*.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action
	01/25 12:52:34	end	Trust-L3	Untrust-L3	192.168.10.50		8.8.4.4	53	dns	allow
	01/25 12:52:34	end	Trust-L3	Untrust-L3	192.168.10.50		8.8.8.8	53	dns	allow
	01/25 12:52:06	deny	Trust-L3	Untrust-L3	192.168.10.50		94.242.236.49	80	depositfiles	rese
	01/25 12:52:06	deny	Trust-L3	Untrust-L3	192.168.10.50		94.242.236.49	80	depositfiles	rese
	01/25 12:52:05	deny	Trust-L3	Untrust-L3	192.168.10.50		94.242.236.49	80	depositfiles	rese

7. Open a **new tab** in the *Firefox* application.








8. Try to work around the application block by using a proxy. Type **www.avoidr.com** into the address field and press the **Enter** key.

If *avoidr.com* is down, use another proxy like *php-proxy.net*.

9. Type **www.depositfiles.com** in the text box near the bottom of the page and click **Go**.

Notice that another *Application Blocked* page appears showing that the *phpproxy* application was blocked.

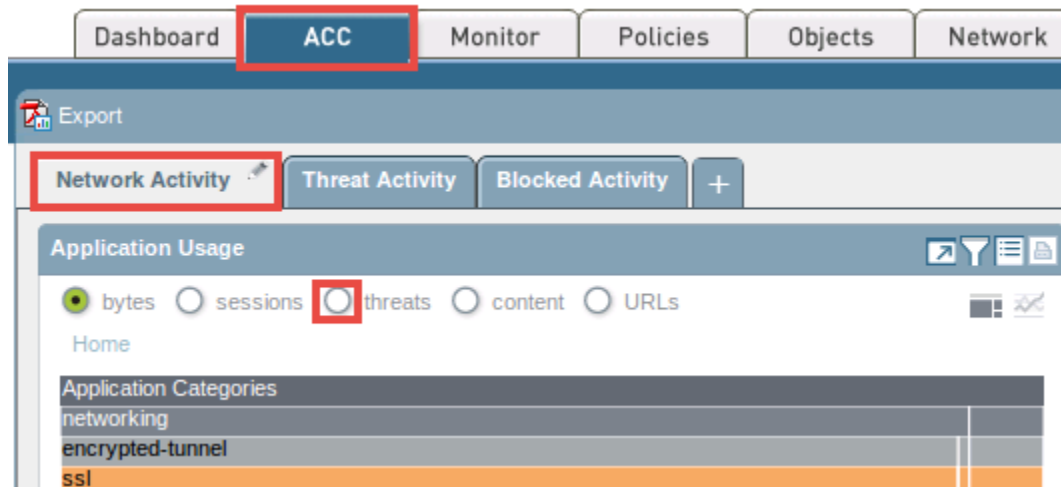
10. Close the second tab and navigate back to the first tab, **PA-VM**.
11. Using the *WebUI*, navigate to **Monitor > Logs > Traffic**.
12. Identify the corresponding log entry that indicates that the *phpproxy* application has been blocked. You can do this by clicking in the search bar and entering (*app eq phproxy*).

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Ac
	01/25 13:07:57	end	Trust-L3	Untrust-L3	192.168.10.50		8.8.4.4	53	dns	alc
	01/25 13:07:57	end	Trust-L3	Untrust-L3	192.168.10.50		8.8.4.4	53	dns	alc
	01/25 13:07:57	end	Trust-L3	Untrust-L3	192.168.10.50		8.8.4.4	53	dns	alc
	01/25 13:07:56	end	Trust-L3	Untrust-L3	192.168.10.50		8.8.4.4	53	dns	alc
	01/25 13:07:48	end	Trust-L3	Untrust-L3	192.168.10.50		5.63.151.30	80	incomplete	alc
	01/25 13:07:28	deny	Trust-L3	Untrust-L3	192.168.10.50		5.63.151.30	80	phpproxy	re
	01/25 13:07:19	drop	Trust-L3	Untrust-L3	192.168.10.50		91.189.94.4	123	not-applicable	der

13. Click on the **ACC** tab to access the *Application Command Center*.



14. Make sure to view the **Network Activity** tab from the ACC and fill in the radio button for **threats** in the *Application Usage* section to view more data about the recent traffic.



What is the total risk level for all traffic that has passed through the firewall thus far? \_\_\_\_\_

Notice that the *Threat Prevention* and *Data Filtering* sections within the ACC contain no matching records yet.

15. Close the **Desktop 1** PC viewer.