



PALO ALTO NETWORKS EDU 210

Lab 15: Implementing Day-One Best Practice Configuration

Document Version: **2022-07-18**

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark 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	3
Lab Topology.....	4
Lab Settings	5
1 Blocking Threats in Encrypted Traffic	6
1.1 Apply a Baseline Configuration to the Firewall.....	6
1.2 Generate Traffic Without Security Profiles	10
1.3 Modify Existing Security Policies.....	15
1.4 Create A Corporate Vulnerability Security Profile	17
1.5 Create A Corporate File Blocking Profile.....	20
1.6 Create Data Filtering Profiles	22
1.7 Create a Security Profile Group.....	25
1.8 Apply the Corp-Profiles-Group to a Security Policy	27
1.9 Generate Attack Traffic with Security Profiles.....	29
1.10 Create Tags	34
1.11 Apply Tags to Security Policy Rule.....	35
1.12 Enforce Rule Tags and Description Requirements	38
1.13 Test Rule Requirements.....	42

Introduction

You intend to cut over all production networks to use the Palo Alto Networks firewall this weekend during a maintenance window. Before the change, you want to implement as many of the best practices from Palo Alto Networks as you can before the firewall cut over. You realize that maintaining a secure network is a continuous process and that you will need to review logs, alerts, and reports each day to help you fine-tune the configuration.

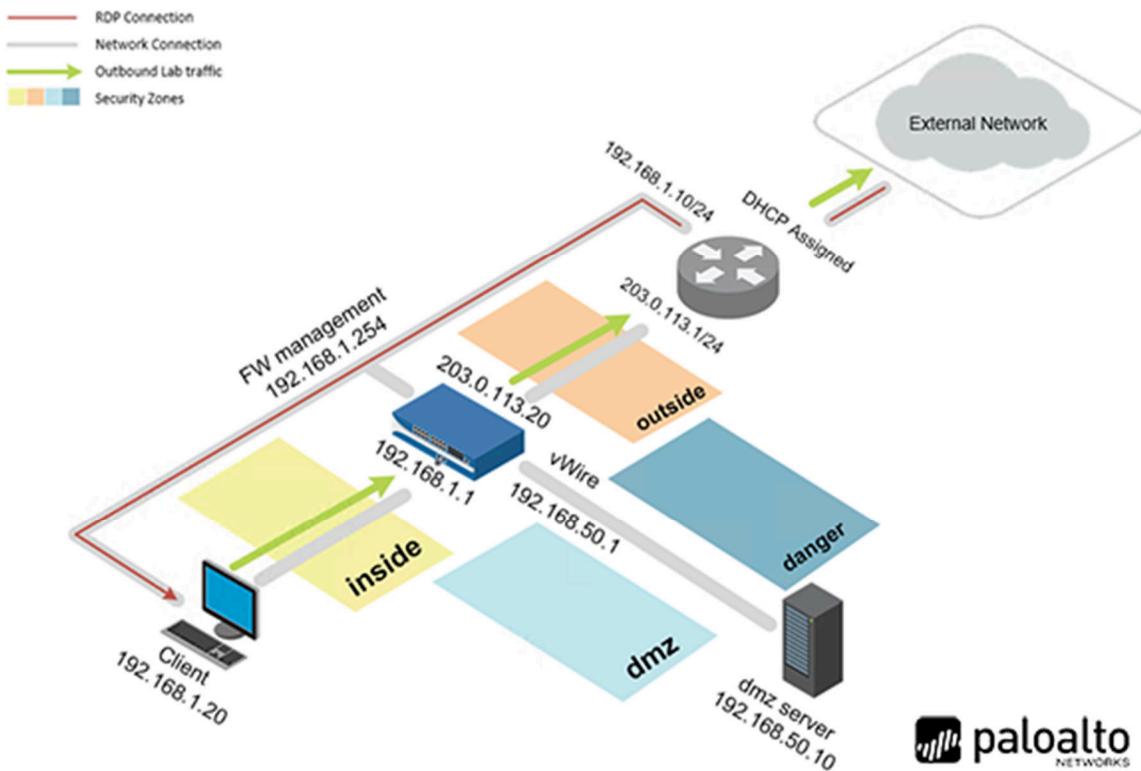
Nevertheless, there are several tasks that you can complete before the firewall goes into production so that you start with a solid, secure network.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Generate traffic without profiles and examine logs
- Create security profiles
- Create a security group
- Apply the security group to existing security policy rules
- Generate traffic with profiles and examine logs
- Create tags
- Enable policy rulebase settings and observe behavior

Lab Topology



Lab Settings

The information in the table below will be needed 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)
Client	192.168.1.20	lab-user	Pa10Alt0!
DMZ	192.168.50.10	root	Pa10Alt0!
Firewall	192.168.1.254	admin	Pa10Alt0!
VRouter	192.168.1.10	root	Pa10Alt0!

1 Blocking Threats in Encrypted Traffic

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the firewall configuration file.

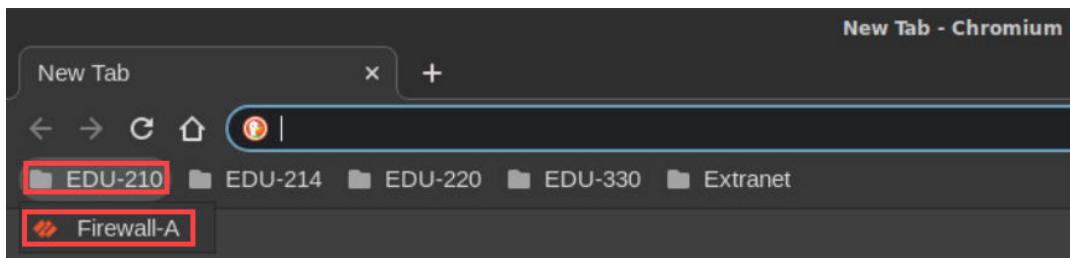
1. Click on the **Client** tab to access the Client PC.



2. Double-click the **Chromium Web Browser** icon located on the desktop.



3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.



4. You will see a "Your connection is not private" message. Next, click on the **ADVANCED** link.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

[Advanced](#)

[Back to safety](#)



If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

5. Click on **Proceed to 192.168.1.254 (unsafe)**.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

[Hide advanced](#)

[Back to safety](#)

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.1.254 \(unsafe\)](#)

6. Log in to the firewall web interface as username **admin**, password **Pa10Alt0!**.



The screenshot shows the login interface for a Palo Alto Networks device. The URL in the address bar is `http://192.168.1.254`. The page has a yellow border. At the top is the **paloalto® NETWORKS** logo. Below it is a login form with two fields: a text input for the username containing "admin" and a password input containing redacted dots. A blue "Log In" button is at the bottom. The entire form area is highlighted with a red box.

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

The screenshot shows the PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE link is highlighted with a red box. On the left, a sidebar menu under the 'Setup' heading lists various configuration options like High Availability, Config Audit, and Admin Roles. The main content area is titled 'Configuration Management'. It contains several buttons: 'Revert' (to last saved configuration), 'Save' (named configuration snapshot), 'Load' (load named configuration snapshot, which is highlighted with a red box), and 'Load configuration version'.

8. In the *Load Named Configuration* window, select **edu-210-lab-15.xml** from the *Name* dropdown box and click **OK**.

This screenshot shows the 'Load Named Configuration' dialog box. It has fields for 'Name' (set to 'edu-210-lab-15.xml'), 'Decryption Key' (containing '****'), and two checkboxes: 'Regenerate Rule UUIDs for selected named configuration' and 'Skip Validation'. At the bottom are 'OK' and 'Cancel' buttons, with 'OK' highlighted with a red box.

9. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

This screenshot shows the 'Loading Configuration' dialog box. It displays the message: 'Configuration is being loaded. Please check the Task Manager for its status.' and 'You should reload the page when the task is completed.' At the bottom is a 'Close' button, which is highlighted with a red box.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

The screenshot shows the bottom navigation bar of the web interface. It includes a 'Tasks' icon (highlighted with a red box), a 'Language' link, and the 'paloalto NETWORKS' logo.

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	08/05/21 00:03:04		
Load	Completed	08/05/21 00:01:59		
EDLRefresh	Completed	08/04/21 23:58:15		
EDLFetch	Completed	08/04/21 23:58:14		
Download	Completed	08/04/21 23:58:04		
Download	Completed	08/04/21 23:54:04		
EDLFetch	Completed	08/04/21 23:53:13		
Auto Commit	Completed	08/04/21 23:52:45		

Show All Tasks | Clear Commit Queue | Close

12. Click the **Commit** link located at the top-right of the web interface.



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

Commit

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

COMMIT SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

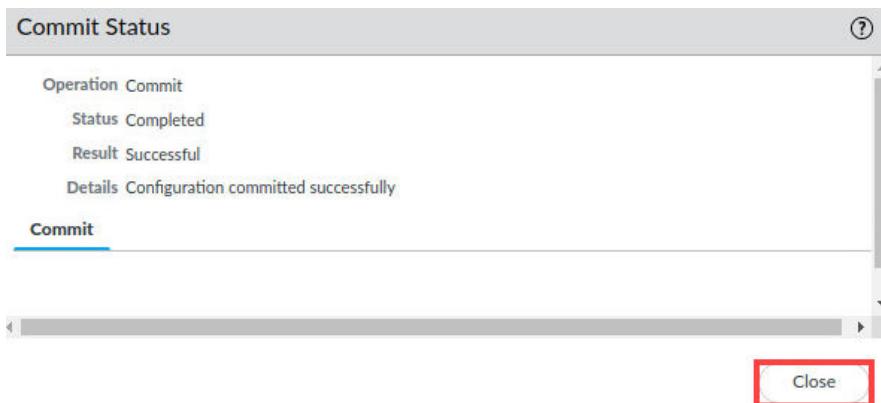
Preview Changes Change Summary Validate Commit Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

Commit Cancel

14. When the *Commit* operation successfully completes, click **Close** to continue.



The commit process takes changes made to the firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Minimize the *Palo Alto Networks Firewall* and continue to the next task.



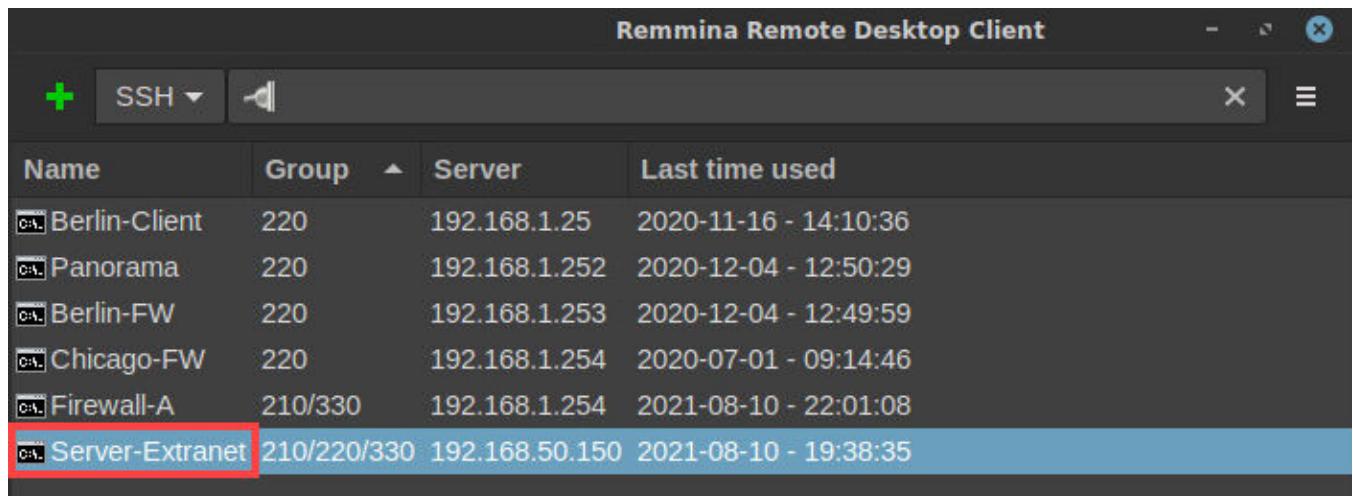
1.2 Generate Traffic Without Security Profiles

In this section, you will create a new security policy rule and attempt to leave out the description. This will let you see what happens when an administrator does not provide adequate information when creating a rule.

1. On the *client desktop*, open the **Remmina** application.



2. Double-click the entry for **Server-Extranet**.



Please
Note

This action will open an SSH connection to the server and automatically log you in with appropriate credentials.

3. In the CLI connection, enter the following command to change the working directory.

```
paloalto42@extranet1:~$ cd pcaps92019/attack.pcaps/ <Enter>
```

```
paloalto42@extranet1:~$ cd pcaps92019/attack.pcaps/
```

4. In the CLI connection, enter the following command to run the simulated attacks.

```
paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh <Enter>
```

```
paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh
```

Please
Note

This script takes about 6 minutes to complete. Allow the **malwareattacks** script to run uninterrupted.

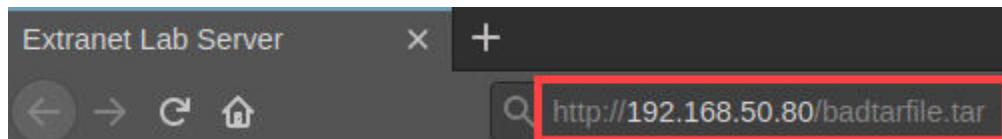
5. Minimize the *Remmina* connection window.



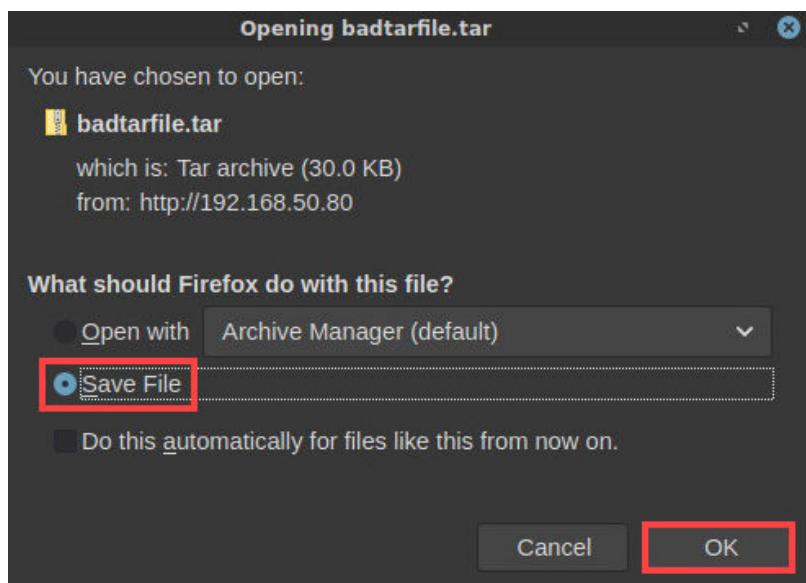
6. On the *client desktop*, open the **Firefox Web Browser** application.



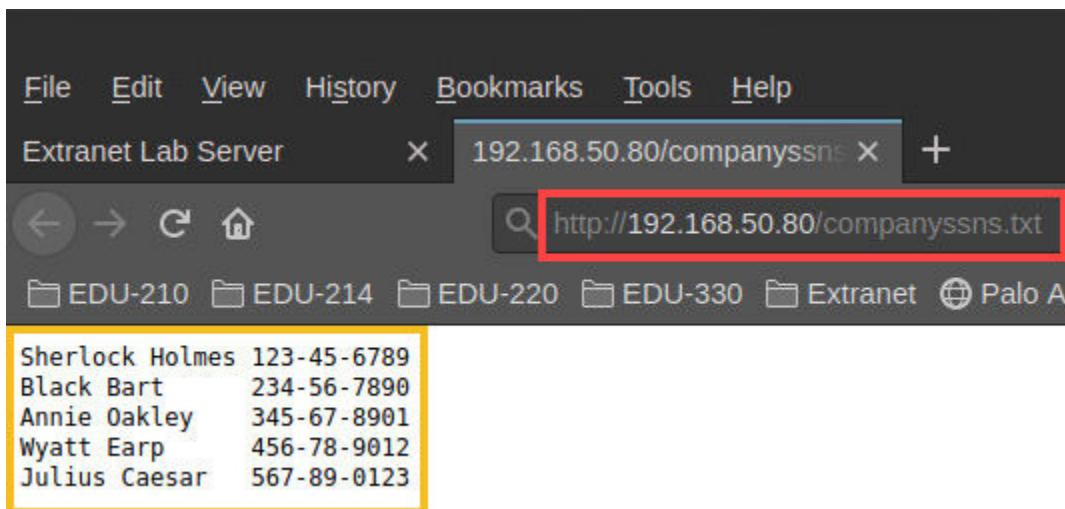
7. Type **http://192.168.50.80/badtarfile.tar** and press **Enter**.



8. In the *Opening badtarfile.tar* window, select **Save File**. Click **OK**.



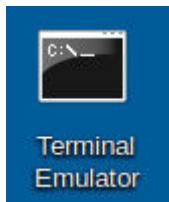
9. In the *Firefox Web Browser*, open a new tab. Type `http://192.168.50.80/companyssns.txt` and press **Enter**. The browser will display a file with *fictitious names* and *social security numbers*.



10. Close the *Firefox browser*.



11. On the *client desktop*, open **Terminal Emulator**.



12. Enter the following command to generate a DNS query using **dig** to resolve a URL to an IP address. The command returns a public IP address, indicating that the URL is accessible.

```
C:\home\lab-user\Desktop\Lab-Files> dig @8.8.8.8 www.quora.com
```

```
Terminal
C:\home\lab-user\Desktop\Lab-Files> dig @8.8.8.8 www.quora.com
; <>>> DiG 9.11.3-lubuntu1.12-Ubuntu <>>> @8.8.8.8 www.quora.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28718
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.quora.com.           IN      A
;;
;; ANSWER SECTION:
www.quora.com.        21195   IN      CNAME   quora.map.fastly.net.
quora.map.fastly.net. 4        IN      A       151.101.1.2
quora.map.fastly.net. 4        IN      A       151.101.65.2
quora.map.fastly.net. 4        IN      A       151.101.129.2
quora.map.fastly.net. 4        IN      A       151.101.193.2
;;
;; Query time: 61 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Aug 11 22:30:27 EDT 2021
;; MSG SIZE rcvd: 140
C:\home\lab-user\Desktop\Lab-Files>
```

Please
Note

Quora.com is one of the entries included in the malicious domains external dynamic list you configured in an earlier lab.

Also note that you may see a different IP address than what the screen shot shows.

13. Leave the Terminal Emulator window open because you will use it again later in this lab.
14. Reopen the *PA-VM firewall* by clicking on the **Chromium** icon in the taskbar.



15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.3 Modify Existing Security Policies

In previous labs, you created Security Profiles to inspect traffic for spyware and virus signatures. You created a Security Profile for WildFire that forwards unknown executable files to the WildFire cloud for inspection. And you created a URL Filtering Profile to prevent users from browsing to potentially harmful categories of websites.

In this section, you will review these profiles.

1. Select **Objects > Security Profiles > Antivirus**. Click **Corp-AV**.

The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. On the left, there is a sidebar with various object types: Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, and Application Filters. Below this, under 'Custom Objects', are External Dynamic Lists, Data Patterns, Spyware, Vulnerability, URL Category, Security Profiles, Antivirus, and Anti-Spyware. The 'Antivirus' item is highlighted with a red box. The main area displays a table for the 'Antivirus' profiles. The table has columns for NAME, LOCATION, PACKET CAPTURE, PROTOCOL, and SIGNATURE ACTION. One row is visible for the 'default' profile, which is Predefined, has PACKET CAPTURE checked, PROTOCOL set to http, and SIGNATURE ACTION set to default (reset-both). A second table below shows other security profiles: pop3 (default (alert)), ftp (default (reset-both)), smb (default (reset-both)), http (default (reset-both)), and http2 (default (reset-both)). The 'Corp-AV' profile is also highlighted with a red box in this table.

2. In the *Antivirus Profile* window, for *Description*, enter **Standard antivirus profile for all security policy rules**. Check the box for **Enable Packet Capture**.

The screenshot shows the 'Antivirus Profile' configuration window. At the top, it says 'Antivirus Profile'. Below that, there is a form with fields: 'Name' (set to 'Corp-AV'), 'Description' (set to 'Standard antivirus profile for all security policy rules'), and 'Action' (selected). Below the description field, there is a checkbox labeled 'Enable Packet Capture' which is checked and highlighted with a red box. There are also tabs for 'Signature Exceptions' and 'WildFire Inline ML'.

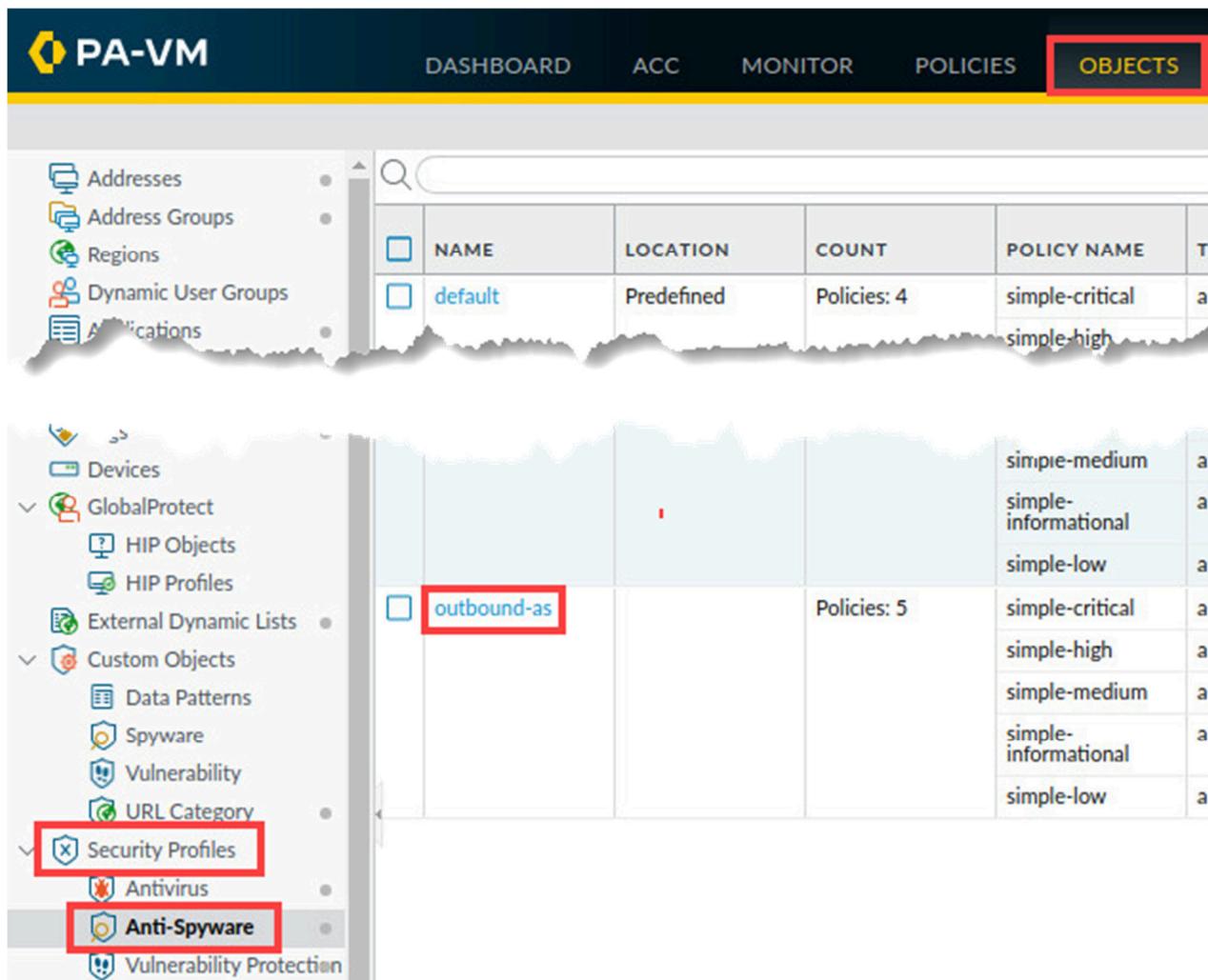
Please Note

Enabling Packet Capture instructs the firewall to take very small packet captures (more like packet snippets) that contains patterns in traffic which match the signatures used in the profile.

3. Click **OK** to close the *Antivirus Profile* window.



4. Select **Objects > Security Profiles > Anti-Spyware**. Click **outbound-as**.

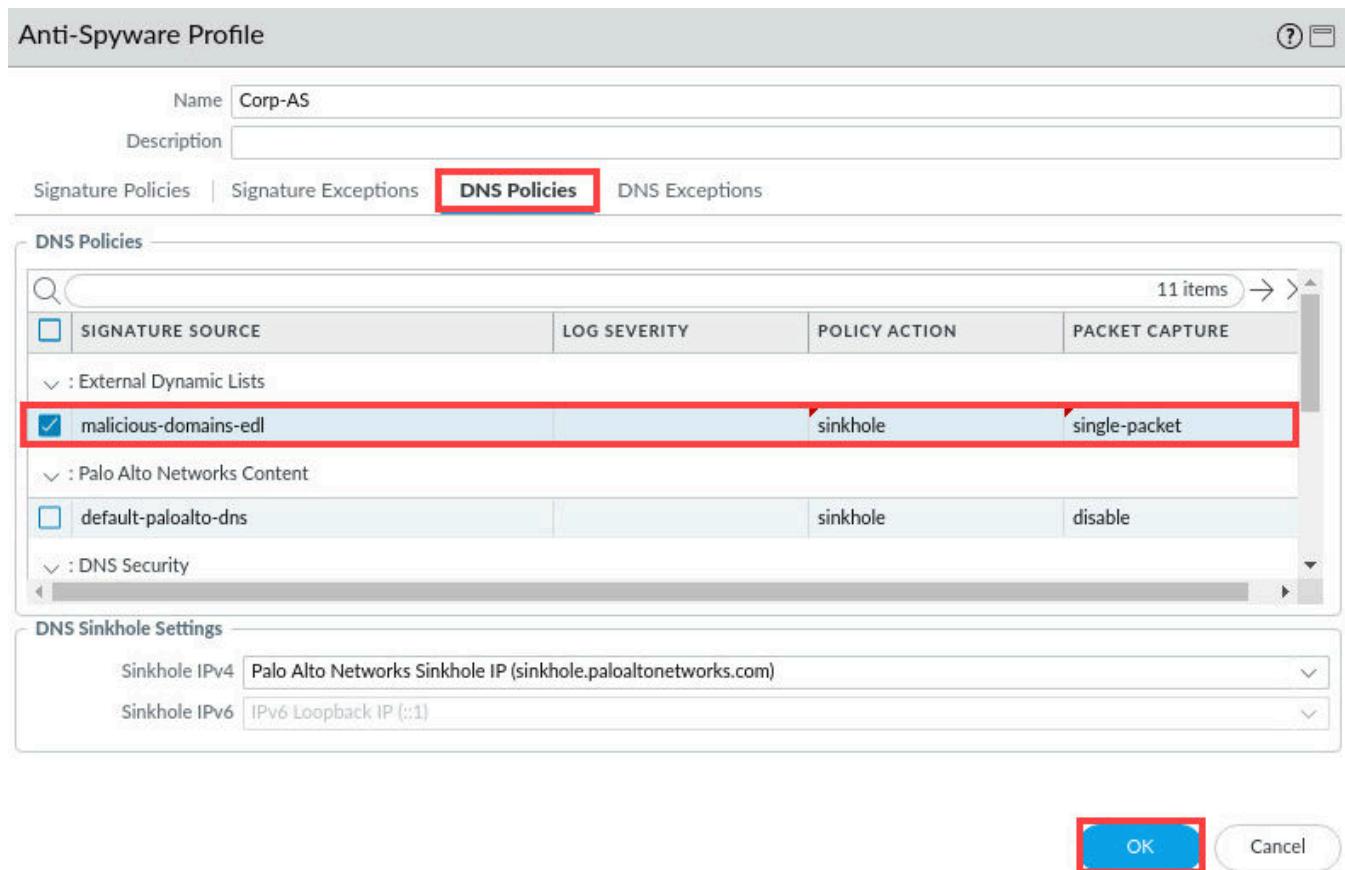


NAME	LOCATION	COUNT	POLICY NAME
default	Predefined	Policies: 4	simple-critical simple-high
outbound-as		Policies: 5	simple-medium simple-informational simple-low simple-critical simple-high simple-medium simple-informational simple-low

5. In the *Anti-Spyware Profile* window, change the *Name* to **Corp-AS**. Select the tab for **DNS Policies**.



6. On the *DNS Policies* tab, for the **malicious-domains-edl** entry, change the *Policy Action* to **sinkhole**. Change the *Packet Capture* to **single-packet**. Click **OK**.



7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Create A Corporate Vulnerability Security Profile

In this section, you will create a vulnerability Security Profile. Palo Alto Networks provides two vulnerability profiles which you can use as the basis for your own – strict and default.

- Select **Objects > Security Profiles > Vulnerability Protection**. Place a check in the box beside **strict**. Click **Clone**.

The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. In the left sidebar, under 'Security Profiles', the 'Vulnerability Protection' option is highlighted with a red box. In the main content area, a table lists security profiles. The 'strict' profile is selected, indicated by a checked checkbox in the 'NAME' column. The 'Clone' button at the bottom of the table is also highlighted with a red box.

NAME	LOCATION	COUNT	RULE NAME
<input checked="" type="checkbox"/> strict	Predefined	Rules: 10	simple-client-critical simple-client-high
			simple-client-medium
			simple-server-critical
			simple-server-high
			simple-server-medium

- In the *Clone* window, click **OK**.

The screenshot shows the 'Clone' dialog box. It has a table titled 'Selected Objects' with a single row containing the name 'strict'. At the bottom of the dialog, there is a checkbox labeled 'Error out on first detected error in validation' and two buttons: 'OK' and 'Cancel'. The 'OK' button is highlighted with a red box.

NAME
strict

3. Click the entry for **strict-1** to open it.

	NAME	LOCATION
<input type="checkbox"/>	default	Predefined
<input type="checkbox"/>	strict-1	

4. In the *Vulnerability Protection Profile* window, change the *Name* to **Corp-Vuln**. For *Description*, enter **Standard vulnerability profile for all security policy rules**. Click **OK**.

RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
simple-client-critical	any	any	client	critical	reset-both	disable
simple-client-high	any	any	client	high	reset-both	disable
simple-client-medium	any	any	client	medium	reset-both	disable
simple-client-informational	any	any	client	informational	default	disable
simple-client-low	any	any	client	low	default	disable
simple-server-critical	any	any	server	critical	reset-both	disable
simple-server-high	any	any	server	high	reset-both	disable

Add Delete Move Up Move Down Clone Find Matching Signatures OK Cancel

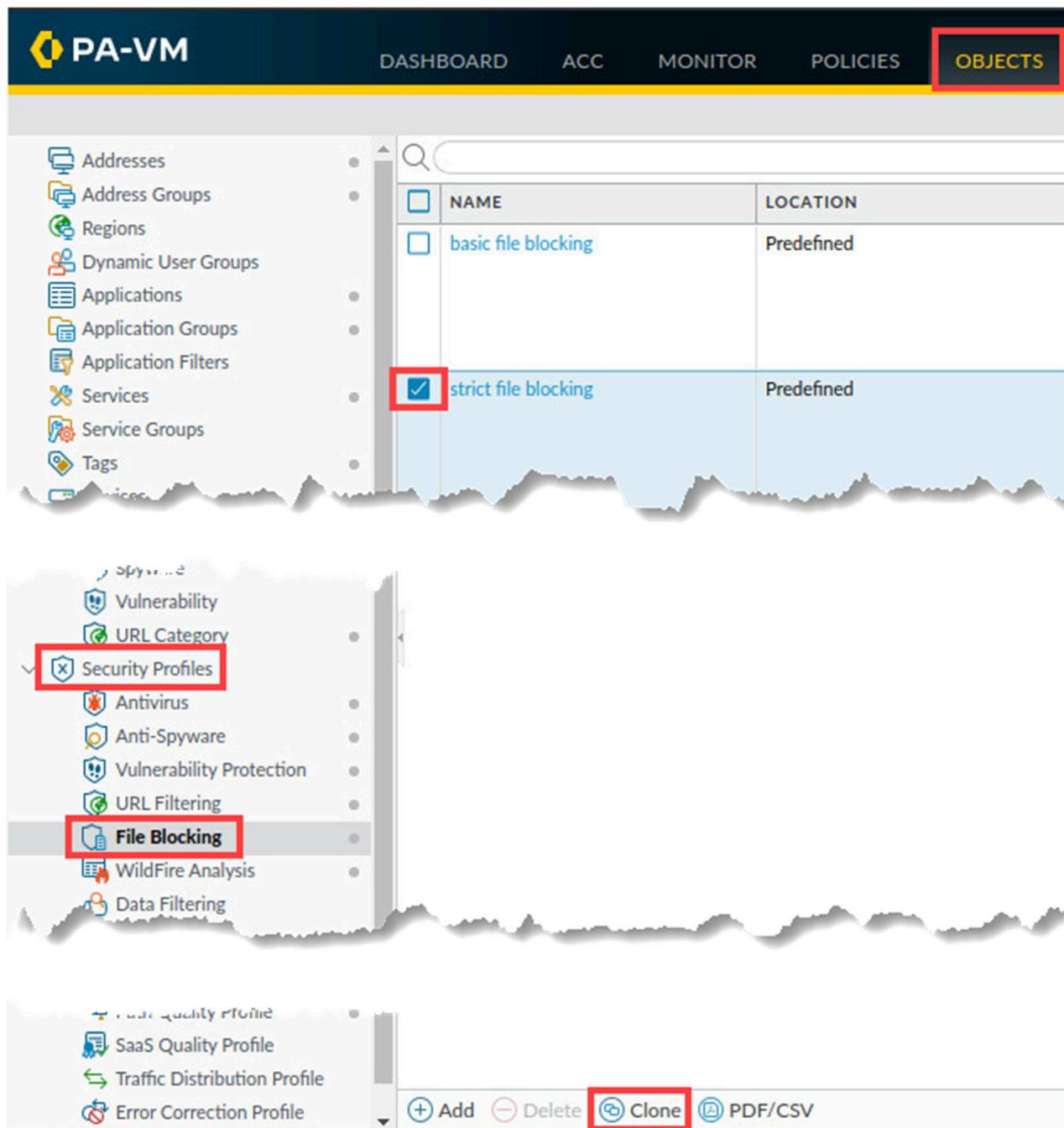
5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.5 Create A Corporate File Blocking Profile

In this section, you will configure a File Blocking Security Profile that the firewall will use to help detect, report, and block attempts to download potentially harmful filetypes. Palo Alto Networks provides two file blocking profiles that you can use as the basis for your own – basic file blocking and strict file blocking.

You will clone the strict file blocking profile and modify it to function as your Corp-FileBlock profile.

1. Select **Objects > Security Profiles > File Blocking**. Place a check beside the entry for **strict file blocking**. Click **Clone**.

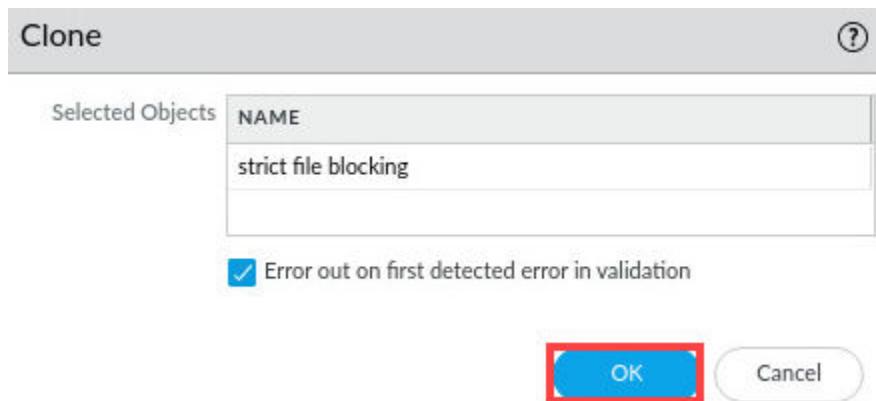


The screenshot shows the PA-VM interface with the following details:

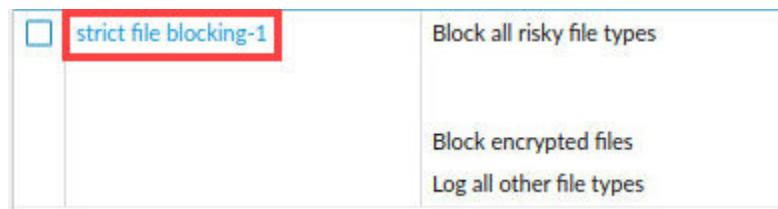
- Top Navigation Bar:** DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS (highlighted with a red box).
- Left Sidebar:** Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, Application Filters, Services, Service Groups, Tags, and a collapsed section starting with Spyware.
- Central Content Area:** A table listing security profiles:

NAME	LOCATION
basic file blocking	Predefined
<input checked="" type="checkbox"/> strict file blocking	Predefined
- Bottom Navigation Bar:** Add, Delete, Clone (highlighted with a red box), and PDF/CSV.
- Bottom Left Panel:** A sidebar showing Quality Profile, SaaS Quality Profile, Traffic Distribution Profile, and Error Correction Profile.
- Bottom Right Panel:** A sidebar showing the current configuration of the selected File Blocking profile, including Virus, URL Category, and File Blocking settings.

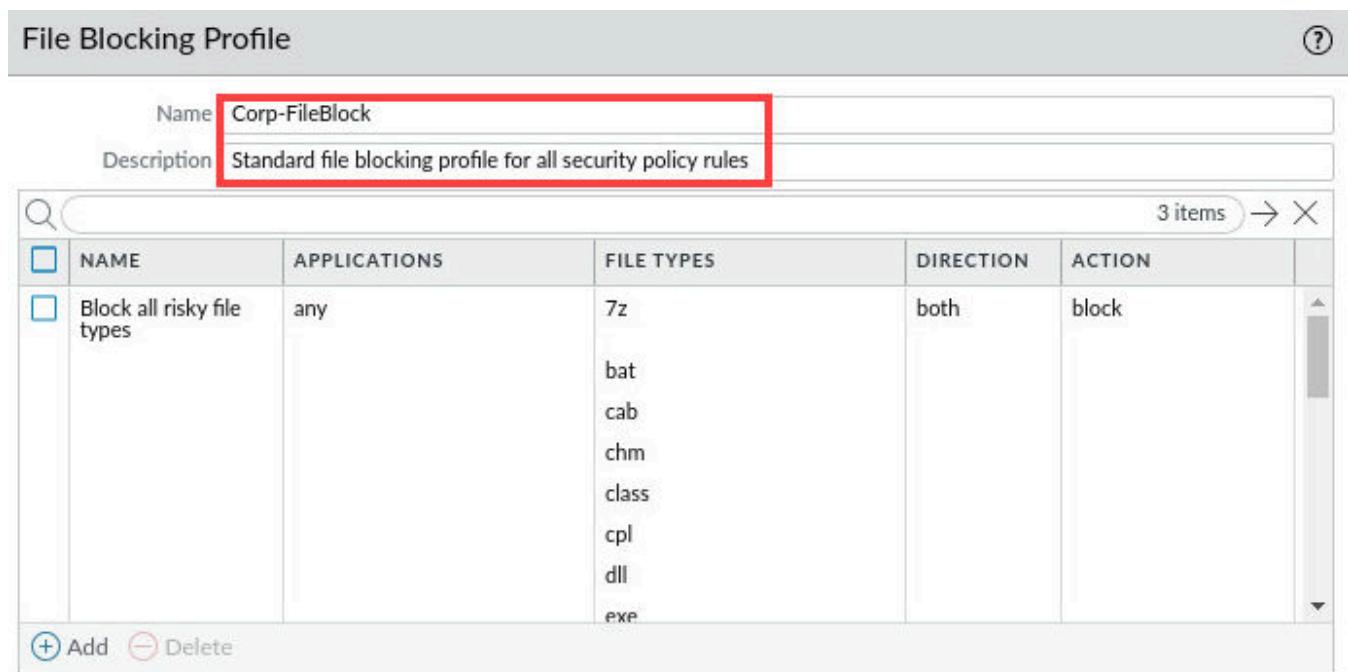
2. In the *Clone* window, click **OK**.



3. Click the entry for **strict file blocking-1** to open it.



4. Change the *Name* to **Corp-FileBlock**. For *Description*, enter **Standard file blocking profile for all security policy rules**. Click **OK**.

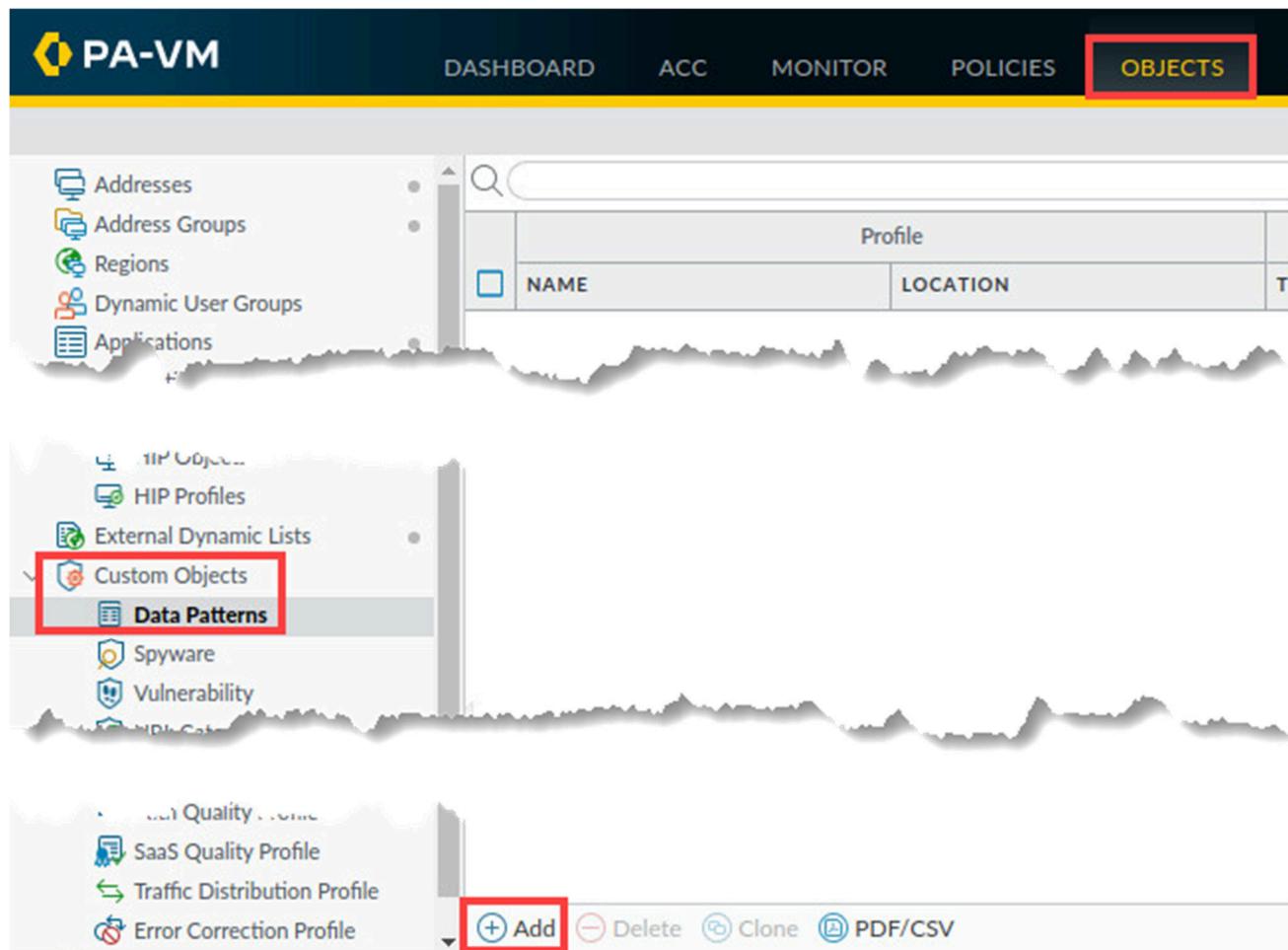


5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.6 Create Data Filtering Profiles

Create a data filtering profile to detect and block the transfer of files that contain more than three US social security numbers. Data Filtering Profiles are based on one or more Data Patterns, so you will need to first configure a Data Pattern that matches variations of US social security numbers.

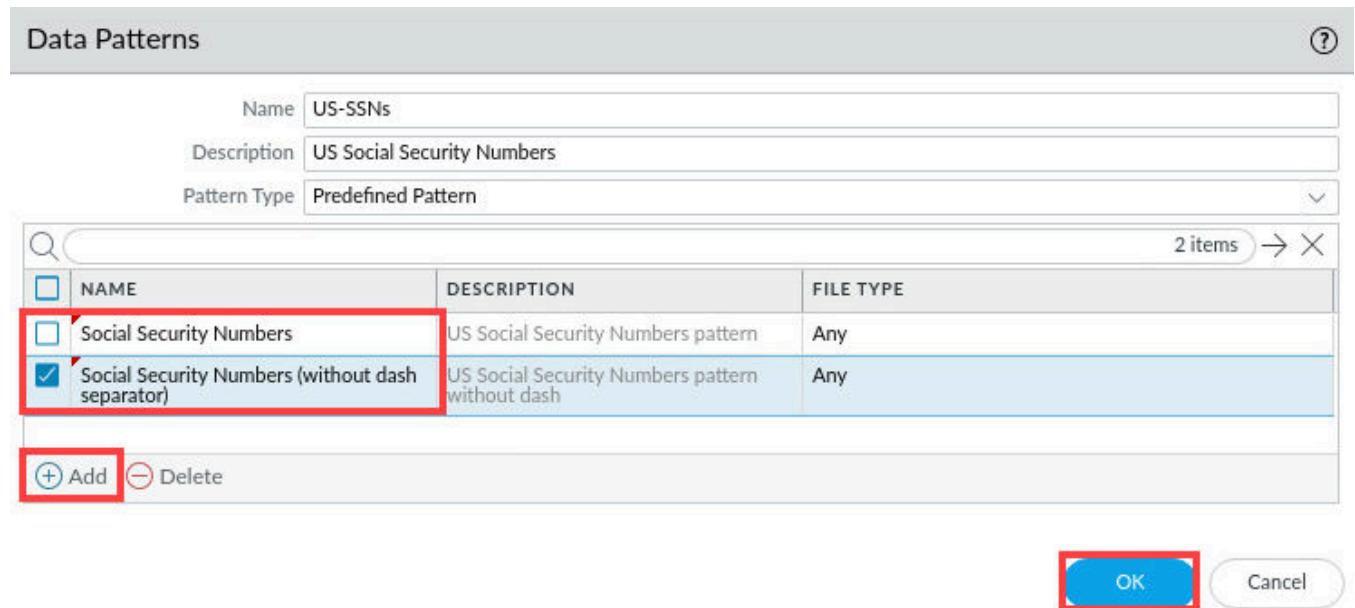
1. Select **Objects > Custom Objects > Data Patterns**. Click **Add**.



2. In the *Data Patterns* window, for *Name*, enter **US-SSNs**. For *Description*, enter **US Social Security Numbers**. Change the *Pattern Type* to **Predefined Pattern**.

Data Patterns	
Name	US-SSNs
Description	US Social Security Numbers
Pattern Type	Predefined Pattern

3. Click **Add** and scroll down the available list and select **Social Security Numbers**. Click **Add** again and select **Social Security Numbers (without dash separator)**. Click **OK**.



4. Select **Objects > Security Profiles > Data Filtering**. Click **Add**.

The screenshot shows the PA-VM interface with the following navigation path:

- Top navigation bar: DASHBOARD, ACC, MONITOR, POLICIES, **OBJECTS**
- Left sidebar under **Addressing**:
 - Vulnerability
 - URL Category
 - Security Profiles** (selected, highlighted with a red box)
 - Antivirus
 - Anti-Spyware
 - Vulnerability Protection
 - URL Filtering
 - File Blocking
 - WildFire Analysis
 - Data Filtering** (highlighted with a red box)
 - DoS Protection
 - Security Profile Groups
 - Log Forwarding
- Bottom right toolbar:
 - + Add** (highlighted with a red box)
 - Delete
 - Clone
 - PDF/CSV

5. In the *Data Filtering Profiles* window, for *Name*, enter **Corp-DataFilter**. For *Description*, enter **Standard data filtering profile for all security rules**.

Data Filtering Profile	
Name	Corp-DataFilter
Description	Standard data filtering profile for all security rules

6. Click **Add** and select the **US-SSNs** data pattern that you defined. Click in the **Alert Threshold** field and change the value to **1**. Click in the **Block Threshold** field and change the value to **3**. Change the **Log Severity** to **critical**. Click **OK**.

The screenshot shows the 'Data Filtering Profile' configuration window. At the top, there are fields for 'Name' (Corp-DataFilter) and 'Description' (Standard data filtering profile for all security rules). A 'Data Capture' checkbox is unchecked. Below is a table with columns: DATA PATTERN, APPLICATIONS, FILE TYPE, DIRECTION, ALERT THRESHOLD, BLOCK THRESHOLD, and LOG SEVERITY. A single row is present, showing 'US-SSNs' as the data pattern, 'any' as applications, 'Any' as file type, 'both' as direction, '1' as alert threshold, '3' as block threshold, and 'critical' as log severity. At the bottom left are 'Add' and 'Delete' buttons, with 'Add' being highlighted by a red box. At the bottom right are 'OK' and 'Cancel' buttons, with 'OK' being highlighted by a red box.

7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.7 Create a Security Profile Group

To simplify the process of applying Security Profiles to Security policy rules, you can create a Security Profile Group which contains individual Security Profiles.

You can then apply the Security Profile Group to a Security policy rule, rather than individually selecting each profile for each rule.

In this section, you will create a Security Profile Group called Corp-Profiles-Group. You will add each of your Corp-* Security Profiles to the group.

1. Select **Objects > Security Profile Groups**. Click Add.

The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. In the left sidebar, under 'SECURITY', the 'Security Profile Groups' option is highlighted with a red box. At the bottom of the sidebar, the '+ Add' button is also highlighted with a red box.

2. In the *Security Profile Group* window, enter **Corp-Profiles-Group** for the **Name**. For each of the available **Profiles**, use the dropdown list to select the **Corp-*** entry you have created. Click **OK**.

Name	Corp-Profiles-Group
Antivirus Profile	Corp-AV
Anti-Spyware Profile	Corp-AS
Vulnerability Protection Profile	Corp-Vuln
URL Filtering Profile	Corp-URL-Profile
File Blocking Profile	Corp-FileBlock
Data Filtering Profile	Corp-DataFilter
WildFire Analysis Profile	Corp-WF

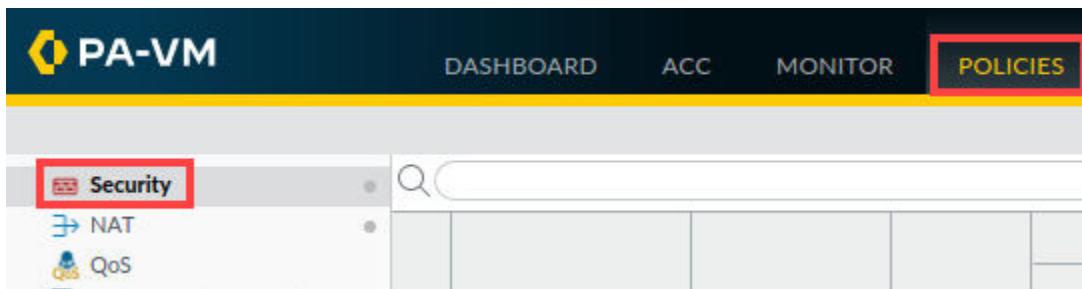
OK **Cancel**

3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

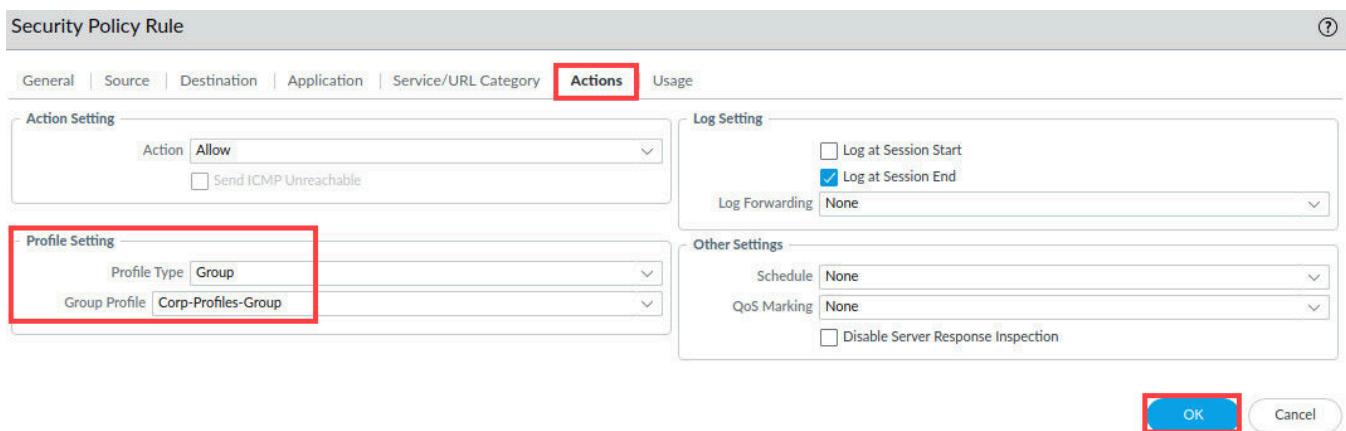
1.8 Apply the Corp-Profiles-Group to a Security Policy

In this section, you will apply the Corp-Profiles-Group to a security policy. With the Security Profiles in place, you can modify your security policy rules to use these protections.

1. Select Policies > Security.



2. Individually edit each security policy rule which allows traffic and change the **Profile Setting** under the **Action tab** to use the **Corp-Profiles-Group**. Be sure to edit and modify each of these rules.
 - **Users_to_Extranet** – Click **OK**.
 - **Users_to_Internet** – Click **OK**
 - **Extranet_to_Internet** – Click **OK**
 - **Extranet_to_Users_Net** – Click **OK**
 - **Allow-PANW-Apps** – Click **OK**
 - **Acquisition-Allow-All** – Click **OK**



3. Verify each of the rules you modified is showing the *Corp-Profiles-Group* by hovering over the **Profile** icon for each rule.

	NAME	TAGS	TYPE	Source ZONE	Destination ZONE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	Internet	any	application-...	Deny	none	grid	0
2	Users_to_Extranet	none	universal	Users_Net	Extranet	any	any	Allow	Profile Group: Corp-Profiles-Group	grid	10648
3	Users_to_Internet	none	universal	Users_Net	Internet	dns ping ssl web-browsing	application-...	Allow	Profile Group: Corp-Profiles-Group	grid	32431
4	Extranet_to_Internet	none	universal	Extranet	Internet	any	application-...	Allow	Profile Group: Corp-Profiles-Group	grid	61
5	Extranet_to_Users_N...	none	universal	Extranet	Users_Net	any	application-...	Allow	Profile Group: Corp-Profiles-Group	grid	2
6	Allow-PANW-Apps	none	universal	Users_Net	Internet	paloalto-apps	application-...	Allow	Profile Group: Corp-Profiles-Group	grid	187
7	Acquisition-Allow-All	none	universal	Acquisition	any	any	application-...	Allow	Profile Group: Corp-Profiles-Group	grid	580277
8	intrazone-default	none	intrazone	any	(intrazone)	any	any	Allow	none	grid	2728
9	interzone-default	none	interzone	any	any	any	any	Deny	none	grid	-

4. Click the **Commit** link located at the top-right of the web interface.



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

Commit

Doing a commit will overwrite the running configuration with the commit scope.

Commit All Changes Commit Changes Made By: [\(1\) admin](#)

COMMIT SCOPE	LOCATION TYPE
policy-and-objects	
shared-object	

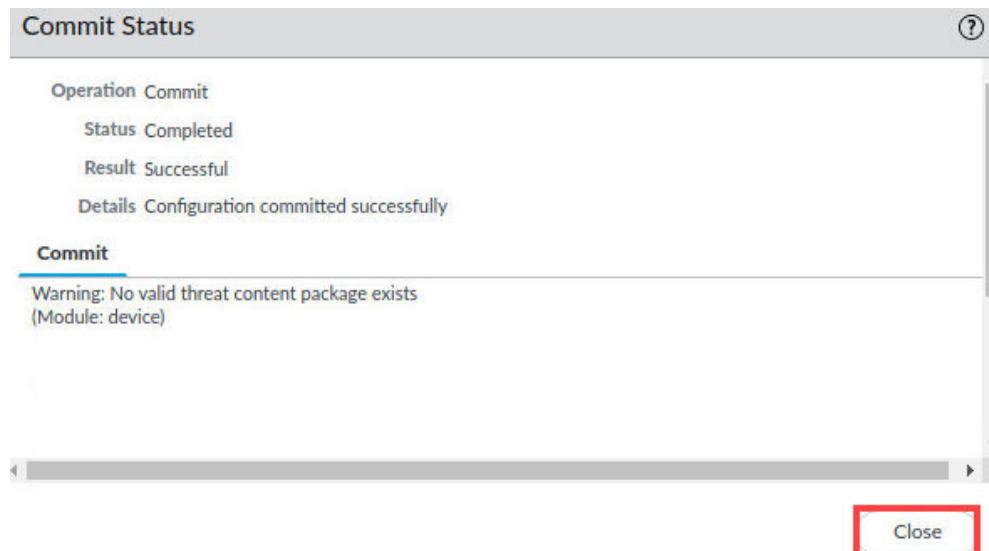
[Preview Changes](#) [Change Summary](#) [Validate Commit](#) Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

Commit **Cancel**

6. When the *Commit* operation successfully completes, click **Close** to continue.



7. Minimize the *Palo Alto Networks Firewall* and continue to the next task.



1.9 Generate Attack Traffic with Security Profiles

In this section, you will generate attack traffic with security policies.

1. Reopen the **Remmina** application by clicking the icon in the taskbar.



2. In the CLI connection, enter the following command to change the working directory. If you are already in the *attack.pcaps* directory, please proceed to the next step.

```
paloalto42@extranet1:~$ cd pcaps92019/attack.pcap/ <Enter>
```

```
paloalto42@extranet1:~$ cd pcaps92019/attack.pcaps/
```

3. In the CLI connection, enter the following command to run the simulated attacks.

```
paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh <Enter>
```

```
paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh
```

Please Note

This script takes about 6 minutes to complete. Allow the **malwareattacks** script to run uninterrupted.

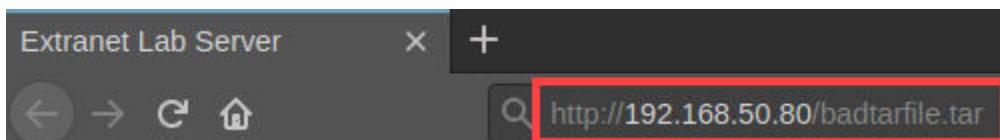
4. Minimize the *Remmina* connection window.



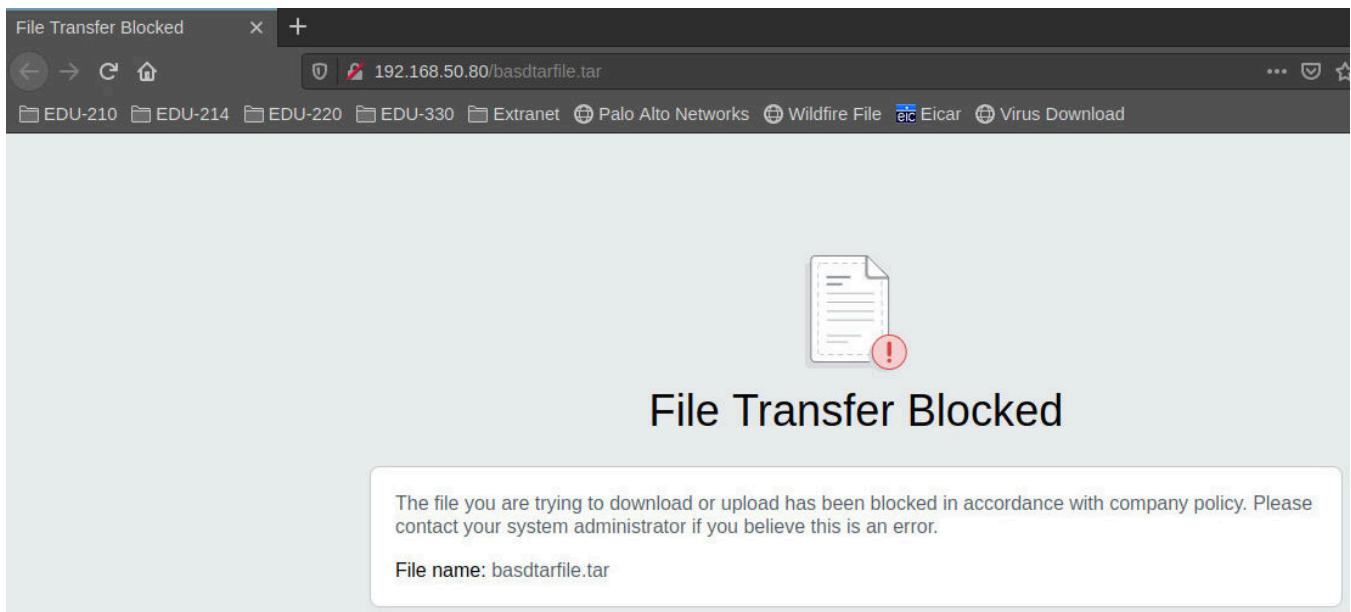
5. On the *client desktop*, open the **Firefox Web Browser** application.



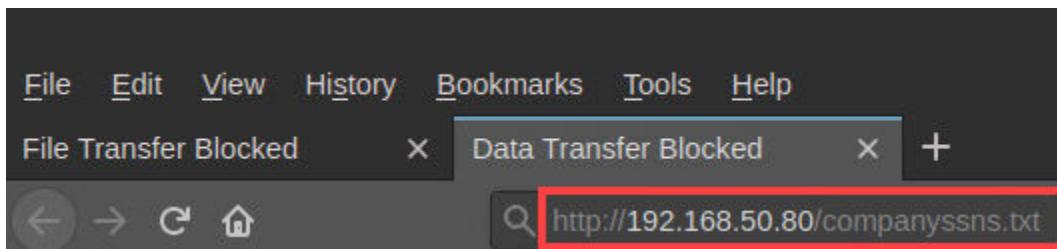
6. Type **http://192.168.50.80/badtarfile.tar** and press **Enter**.



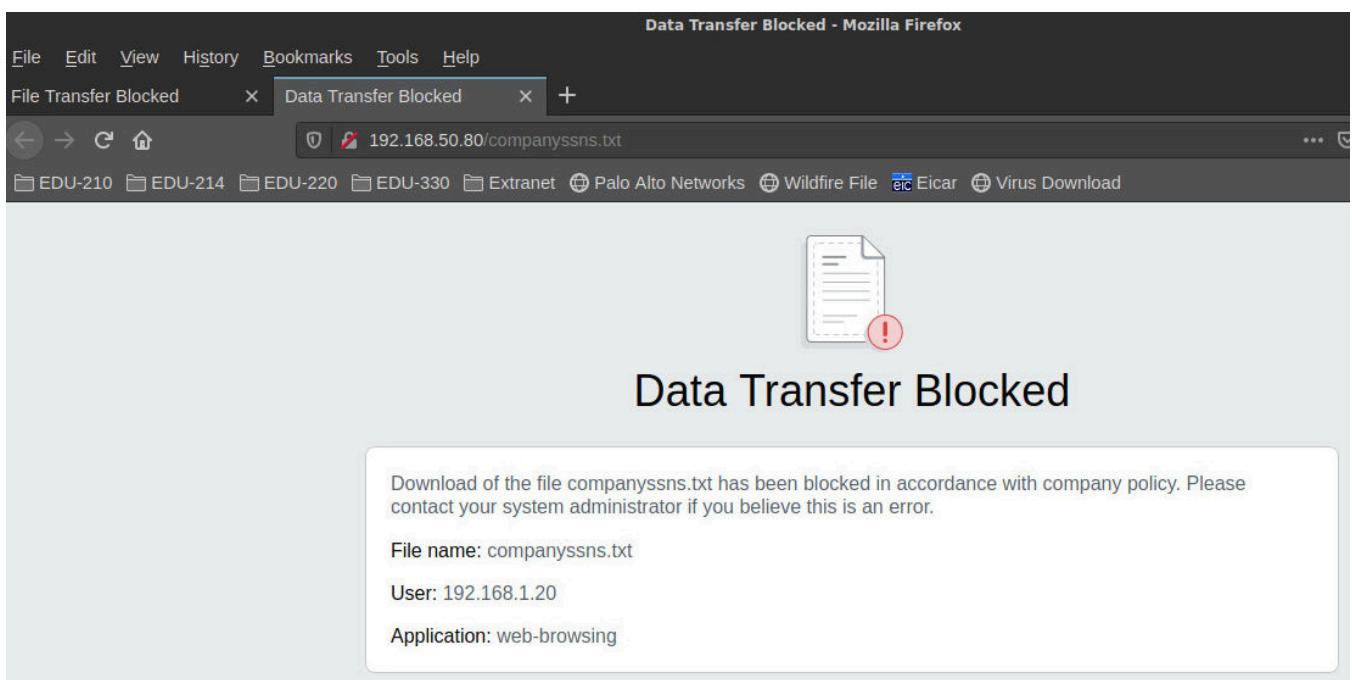
7. You should receive a **File Transfer Blocked** page from the firewall.



8. In *Firefox*, open a new tab. Type **http://192.168.50.80/companyssns.txt** and press **Enter**.



9. You should receive a **Data Transfer Blocked** page from the firewall.



Please Note

This page indicates that the firewall has blocked the transfer using the Data Filtering Profile and Data Pattern you defined for Social Security Numbers.

10. Close the *Firefox Web Browser* by clicking the **close** icon.

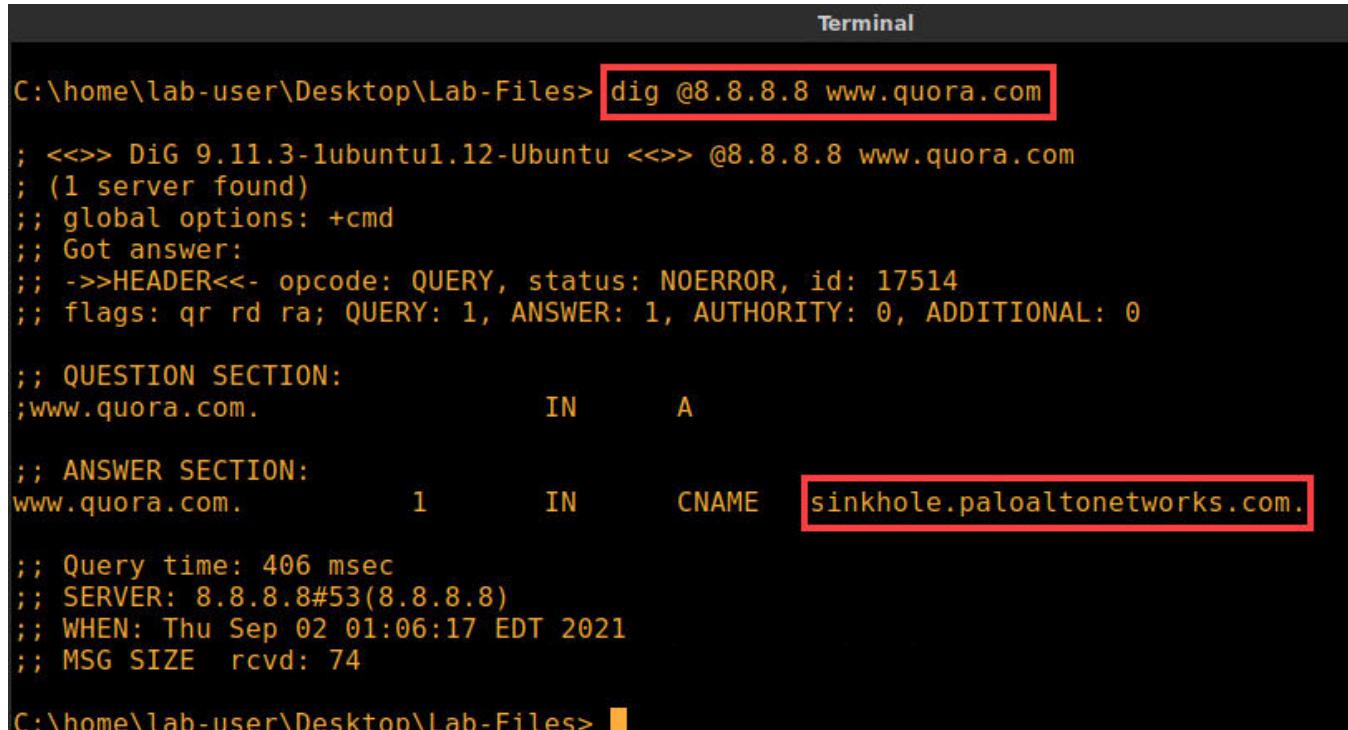


11. On the client workstation, locate the open Terminal Emulator window you used earlier in this lab. You can maximize by clicking the **Terminal** icon in the taskbar.



12. Enter the following command to generate a DNS query using **dig** to resolve a URL to an IP address. The command returns a public IP address, indicating that the URL is accessible. It will now show the **www.quora.com** *DNS query is now in the sinkhole.paloaltonetworks.com.*

```
C:\home\lab-user\Desktop\Lab-Files> dig @8.8.8.8 www.quora.com
```

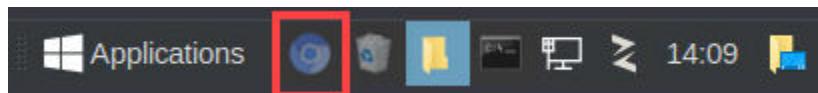


```
Terminal  
C:\home\lab-user\Desktop\Lab-Files> dig @8.8.8.8 www.quora.com  
; <>> DiG 9.11.3-1ubuntu1.12-Ubuntu <>> @8.8.8.8 www.quora.com  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17514  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;www.quora.com. IN A  
  
;; ANSWER SECTION:  
www.quora.com. 1 IN CNAME sinkhole.paloaltonetworks.com.  
  
;; Query time: 406 msec  
;; SERVER: 8.8.8.8#53(8.8.8.8)  
;; WHEN: Thu Sep 02 01:06:17 EDT 2021  
;; MSG SIZE rcvd: 74  
C:\home\lab-user\Desktop\Lab-Files>
```



This indicates that the firewall has intercepted and sinkholed the DNS query using the DNS Sinkholing function in your Anti-Spyware profile.

13. Reopen the *PA-VM firewall* by clicking on the **Chromium** icon in the *taskbar*.



14. In the firewall web interface, select **Monitor > Logs > Threat**. Clear any filters in place and press **Enter**. The Threat Log should contain numerous entries for *Spyware* and *Vulnerabilities*.

	RECEIVE TIME	SEVERITY	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS
	08/12 04:29:39	high	spyware	generic:aplattmesse.com	Acquisition	Acquisition	192.168.1.104
	08/12 04:29:26	medium	spyware	generic:crypto-pool.fr	Acquisition	Acquisition	10.10.17.102
	08/12 04:29:25	medium	spyware	Trojan.yakes:hellobro.bit	Acquisition	Acquisition	10.10.17.102
	08/12 04:29:15	medium	spyware	Trojan.yakes:hellobro.bit	Acquisition	Acquisition	10.10.17.102
	08/12 04:29:07	high	spyware	generic:31.smokemenowh...	Acquisition	Acquisition	10.11.2.102
	08/12 04:28:54	high	spyware	generic:31.smokemenowhhalala.bit	isition	Acquisition	10.11.2.102
	08/12 04:28:36	high	spyware	generic:31.smokemenowh...	Acquisition	Acquisition	10.11.2.102
	08/12 04:28:36	high	spyware	generic:31.smokemenowh...	Acquisition	Acquisition	10.11.2.102

Please Note

These entries indicate that the firewall has blocked malicious traffic using the Vulnerability and Anti-Spyware profiles that you defined. Note that the entries you see in the Threat Log may differ from the example shown here. The table may not contain very many entries until the malwareattacks script is finished. Use the refresh button periodically to update the table. Also, several Threat Log columns have been hidden in this example.

15. Select **Monitor > Logs > URL Filtering**. Note the numerous entries for blocked URLs.

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER
	08/12 04:29:28	malware	malware	159.203.185.4/...	Acquisition	Acquisition	10.3.30.101	
	08/12 04:29:23	malware	malware	hellobro.bit/	Acquisition	Acquisition	10.10.17.102	chicago\wearp
	08/12 04:28:26	command-and-control	command-and-control	n31.smokemeno...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge
	08/12 04:28:24	malware	malware	89.38.98.150/1...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge
	08/12 04:28:24	command-and-control	command-and-control	n31.smokemeno...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge
	08/12 04:28:24	malware	malware	89.38.98.150/1...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge
	08/12 04:28:23	command-and-control	command-and-control	n31.smokemeno...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge

Please Note

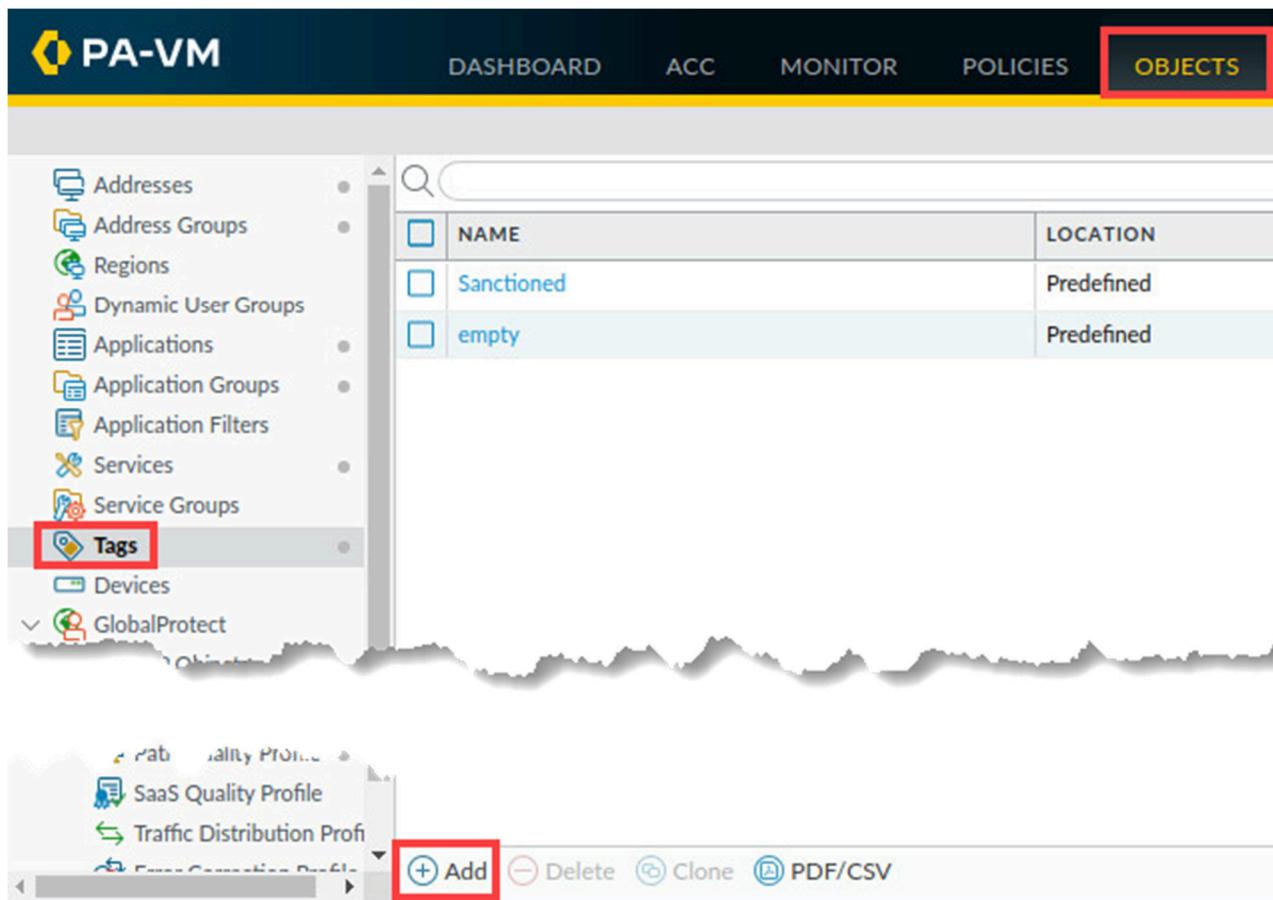
These entries indicate that the firewall has blocked access to dangerous URL categories using the URL Filtering profile you defined. Note that several default columns have been hidden in this example.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.10 Create Tags

You can create color-coded labels for use in various places within the firewall web configuration. These labels can be visual aids that help you more quickly locate information. In this section, you will create Tags to use with your security policy rules.

1. Select **Objects > Tags**. Click **Add**.

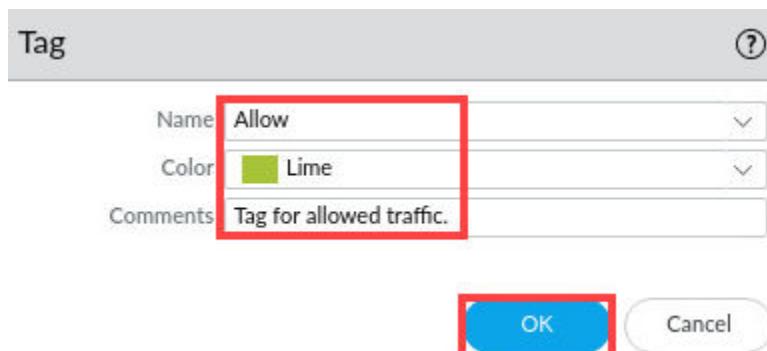


The screenshot shows the PA-VM interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, and OBJECTS, with OBJECTS highlighted. The left sidebar lists various object types: Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, Application Filters, Services, Service Groups, Tags (which is selected and highlighted with a red box), and Devices. Below the sidebar is a search bar and a table with two rows:

NAME	LOCATION
Sanctioned	Predefined
empty	Predefined

At the bottom of the screen, there is a toolbar with icons for SaaS Quality Profile, Traffic Distribution Profile, Add (highlighted with a red box), Delete, Clone, and PDF/CSV.

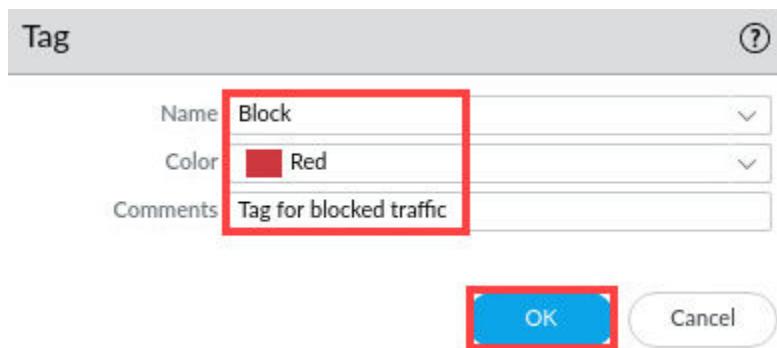
2. In the *Tag* window, Enter **Allow** for the *Name*. For *Color*, select **Lime**. For *Comments*, type **Tag for allowed traffic**. Click **OK**.



3. In the *Tags* window, click **Add** again.



4. In the *Tag* window, Enter **Block** for the *Name*. For *Color*, select **Red**. For *Comments*, type **Tag for blocked traffic**. Click **OK**.

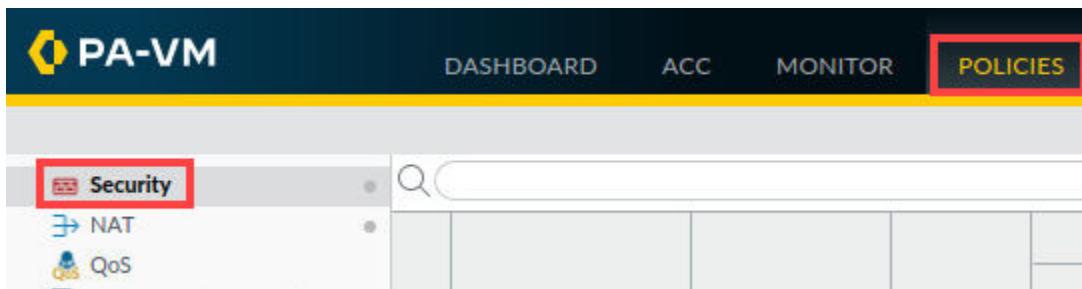


5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.11 Apply Tags to Security Policy Rule

With the Tags defined, you can assign them to your security rules. You will assign the Allow tag to all rules which have an action of Allow. You will assign the Blocked tag to all rules which have an action of Deny.

1. In the firewall web browser, select **Policies > Security**.



2. If the *Tags* column is not showing, add the **Tags** column to the display. Click the small triangle in the column header for *Name*. Select **Columns** and check the box for **Tags**.

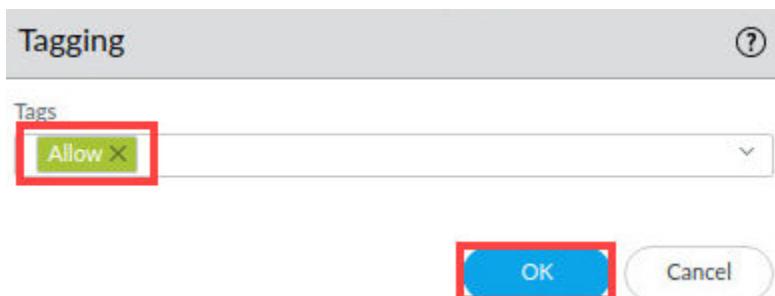
Please Note

Note that if you have already displayed the Tags column in the Security Policy Rule table, you can drag and drop it beside the Name column.

3. In the row for *Block-Known-Bad-IPs*, click the link for **none** under the *Tags* column. In the *Tagging* window, select **Block** from the dropdown box. Click **OK**.

4. Repeat this process for each remaining rule in the list, applying the appropriate **Allow** or **Blocked** tag, depending on the rule action.

- **Users_to_Extranet** – Click **OK**.
- **Users_to_Internet** – Click **OK**
- **Extranet_to_Internet** – Click **OK**
- **Extranet_to_Users_Net** – Click **OK**
- **Allow-PANW-Apps** – Click **OK**
- **Acquisition-Allow-All** – Click **OK**



5. When complete, your rules should match the following example.

	NAME	TAGS	TYPE
1	Block-Known-Bad-IPs	Block	universal
2	Users_to_Extranet	Allow	universal
3	Users_to_Internet	Allow	universal
4	Extranet_to_Internet	Allow	universal
5	Extranet_to_Users_N...	Allow	universal
6	Allow-PANW-Apps	Allow	universal
7	Acquisition-Allow-All	Allow	universal

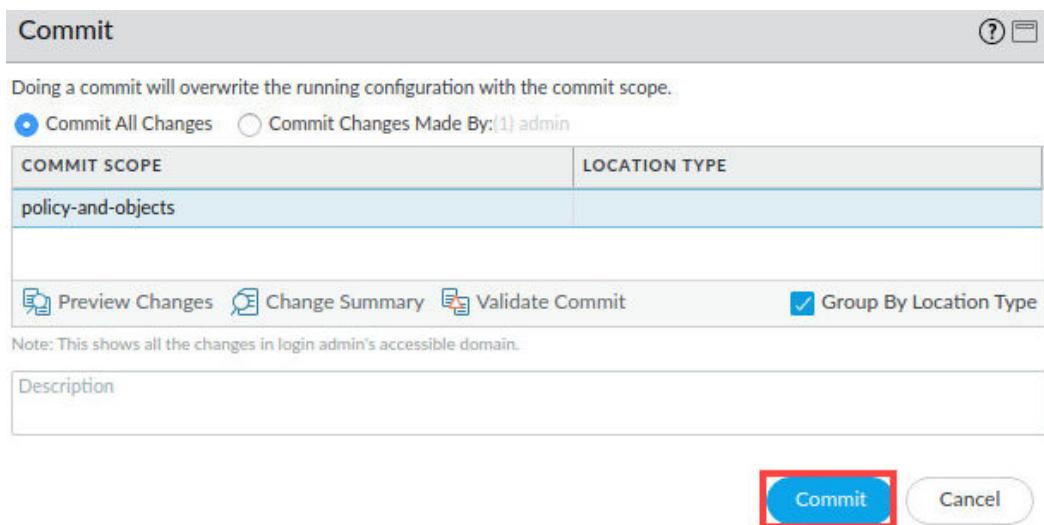
Please
Note

Note that this is a simple illustration of how to create and apply Tags to your security policy rules. You can also apply more than one Tag to your rules.

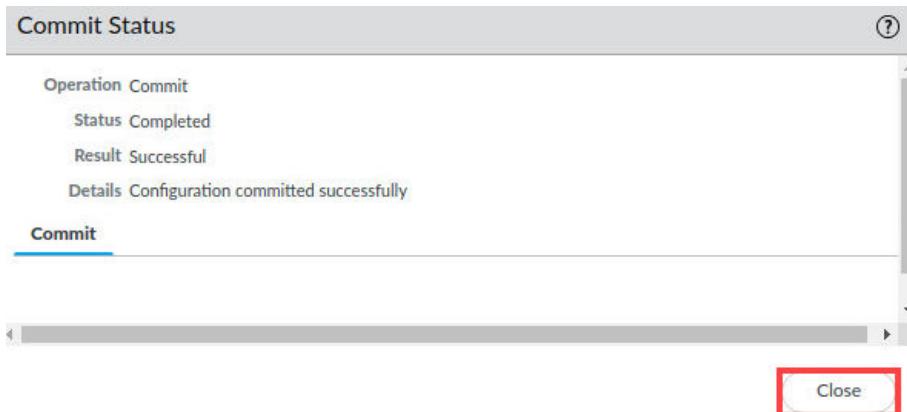
6. Click the **Commit** link located at the top-right of the web interface.



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



8. When the *Commit* operation successfully completes, click **Close** to continue.



9. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

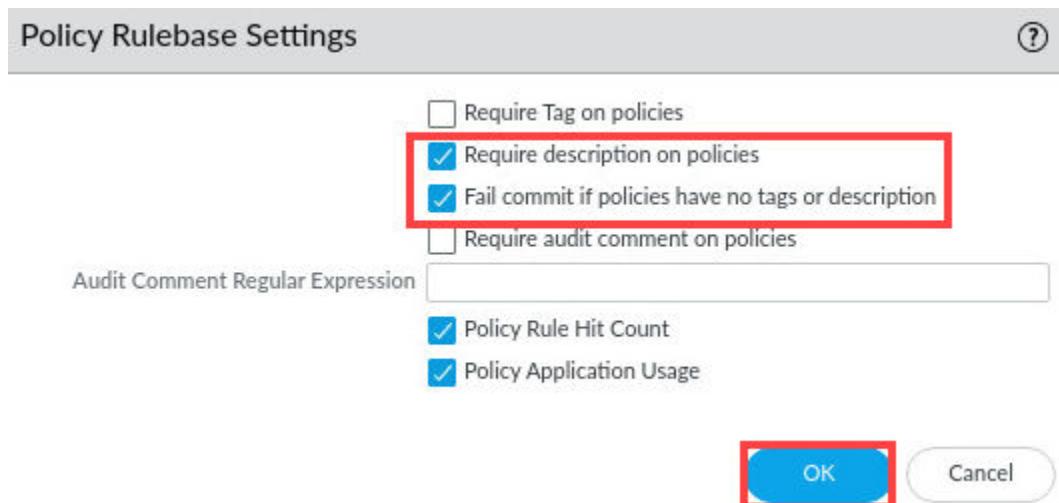
1.12 Enforce Rule Tags and Description Requirements

You can force firewall administrators to supply information in the *Description* field of security policy rules and to apply a **Tag** as well. This additional information can help you determine why a rule has been created and what it was meant to accomplish.

- Select **Device > Setup > Management**. Scroll down and locate the section for *Policy Rulebase Settings*. Click the gear icon to edit these settings.

The screenshot shows the PA-VM configuration interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE, with DEVICE highlighted by a red box. On the left, a sidebar under the 'Setup' heading lists various configuration options like High Availability, Config Audit, and Certificate Management, with Certificate Management expanded. The main content area shows the 'Management' tab selected. Below it is the 'Policy Rulebase Settings' section, which contains several configuration options with checkboxes. A red box highlights the 'Require description on policies' and 'Fail commit if policies have no tags or description' checkboxes, both of which are checked. Other options like 'Require Tag on policies' and 'Audit Comment Regular Expression' are shown but not highlighted.

- In the *Policy Rulebase Settings* window, check the boxes for **Require description on policies** and **Fail commit if policies have no tags or description**. Click **OK**.



Please Note

If you check the option for **Require Tag on policies**, you will need to modify your NAT Policy rules and assign a Tag to each of them.

3. Click the **Commit** link located at the top-right of the web interface.



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

Commit

Doing a commit will overwrite the running configuration with the commit scope.

Commit All Changes Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
device-and-network	

[Preview Changes](#) [Change Summary](#) [Validate Commit](#) Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

Commit **Cancel**

5. You should see a message indicating that one of the rules does not have a **Description**. When the commit operation successfully completes, click **Close** to continue.

Commit Status

Operation Commit

Status Completed

Result Failed

Details Validation Error:
rulebase -> security -> rules -> Acquisition-Allow-All is invalid. Description is missing for rule entry
rulebase -> security -> rules is invalid
Commit failed

Commit

Warning: No valid threat content package exists
(Module: device)

Close

6. Select **Policies > Security**. Click the **Acquisition-Allow-All** rule to open it.

	NAME	TAGS	TYPE	ZONE
1	Block-Known-Bad-IPs	Block	universal	E
2	Users_to_Extranet	Allow	universal	U
3	Users_to_Internet	Allow	universal	I
4	Extranet_to_Internet	Allow	universal	E
5	Extranet_to_Users_N...	Allow	universal	E
6	Allow-PANW-Apps	Allow	universal	U
7	Acquisition-Allow-All	Allow	universal	A

7. In the *Security Policy Rule* window, on the *General* tab, enter **Allows traffic from acquisition zone** for the *Description*. Click **OK**.

Security Policy Rule

General Source Destination Application Service/URL Category Actions Usage

Name: Acquisition-Allow-All
Rule Type: universal (default)
Description: Allows traffic from acquisition zone.
Tags: Allow
Group Rules By Tag: None
Audit Comment:

Audit Comment Archive

OK Cancel

8. Click the **Commit** link located at the top-right of the web interface.



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

Doing a commit will overwrite the running configuration with the commit scope.

Commit All Changes Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
policy-and-objects	
device-and-network	

Preview Changes Change Summary Validate Commit Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

Commit Cancel

10. When the *Commit* operation successfully completes, click **Close** to continue.

Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit

Close

11. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.13 Test Rule Requirements

In this section, you will create a new security policy rule and attempt to leave out the description. This will let you see what happens when an administrator does not provide adequate information when creating a rule.

1. Ensure you are at **Policies > Security**. Click **Add**.

The screenshot shows the PA-VM interface with the Policies tab selected. On the left, a sidebar under the Security section lists NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, and Application Override. In the main area, a table displays a single policy entry:

NAME	TAGS	TYPE	ZONE
Block-Known-Bad-IPs	Block	universal	Extranet Users_Net

At the bottom, there are buttons for Object : Addresses, (+) Add, Delete, Clone, Override, Revert, Enable, and Disable.

2. In the *Security Policy Rule* window, enter **Test-Policy** for the *Name*. Click inside the **Description** field and note the pop-up indicator. Click **Cancel**.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions

Name: **Test-Policy**

Rule Type: universal (default)

Description: ! This field is required

Tags:

Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

OK Cancel

3. The lab is now complete; you may end your reservation.