PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 8: Blocking Known Threats Using Security Profiles

Document Version: 2025-10-13

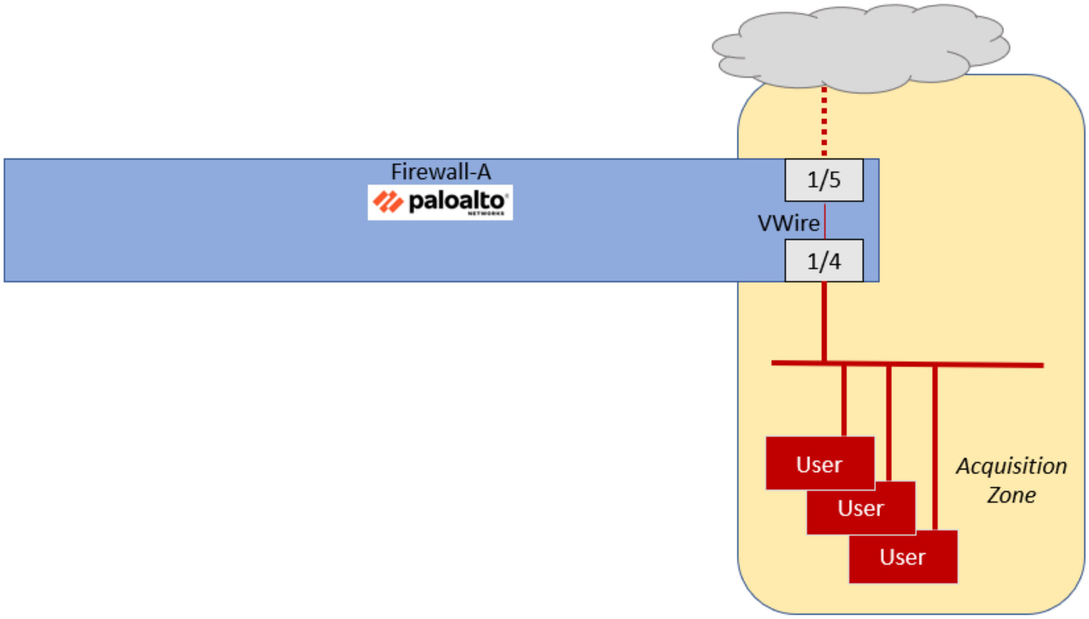
Contents

Introduction

Your organization recently acquired another company. Over the weekend one of your coworkers configured the firewall with a new security zone called Acquisition that contains all the users from this new company.

The coworker also configured the firewall with a Virtual Wire that allows traffic to the Internet from the users in the Acquisition security zone.

Traffic is now being forwarded from users in the acquisition company through the firewall.



The firewall has a Security Policy rule that allows users in the Acquisition zone to access any application on the Internet.

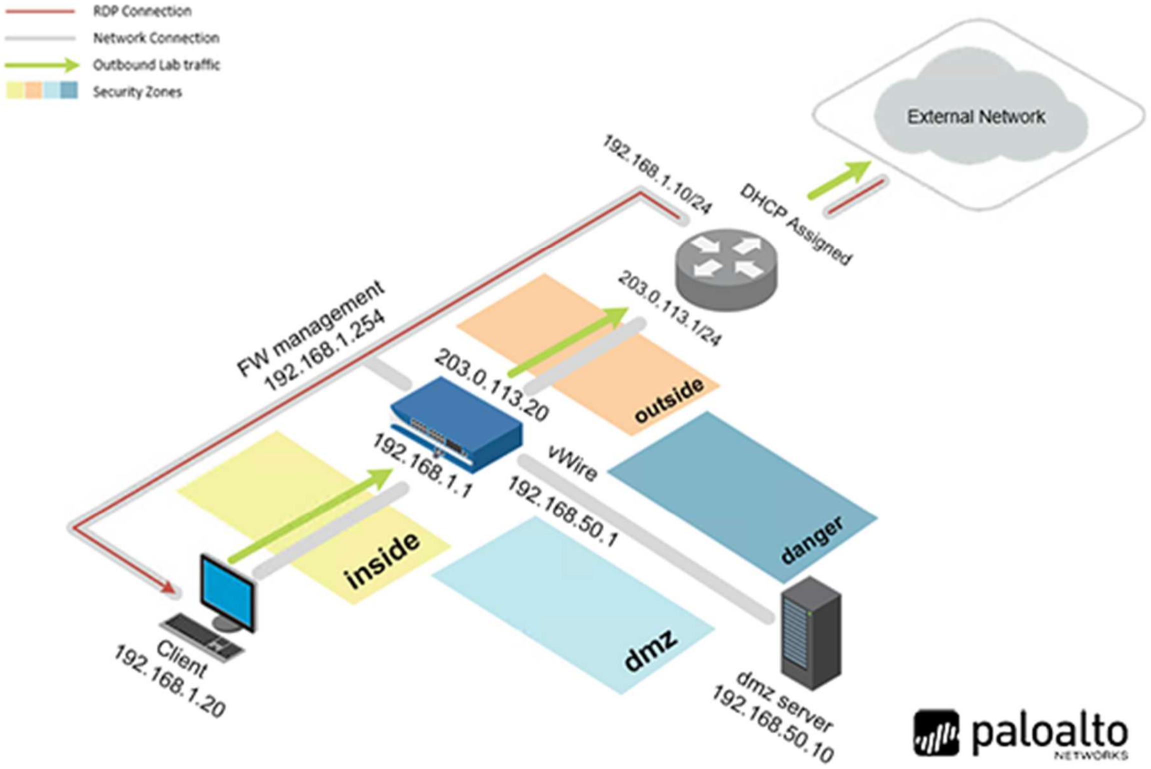
In this lab, you will build and apply a set of Security Profiles that will watch for, and block known threats from the users in this Acquisition zone.

Objective

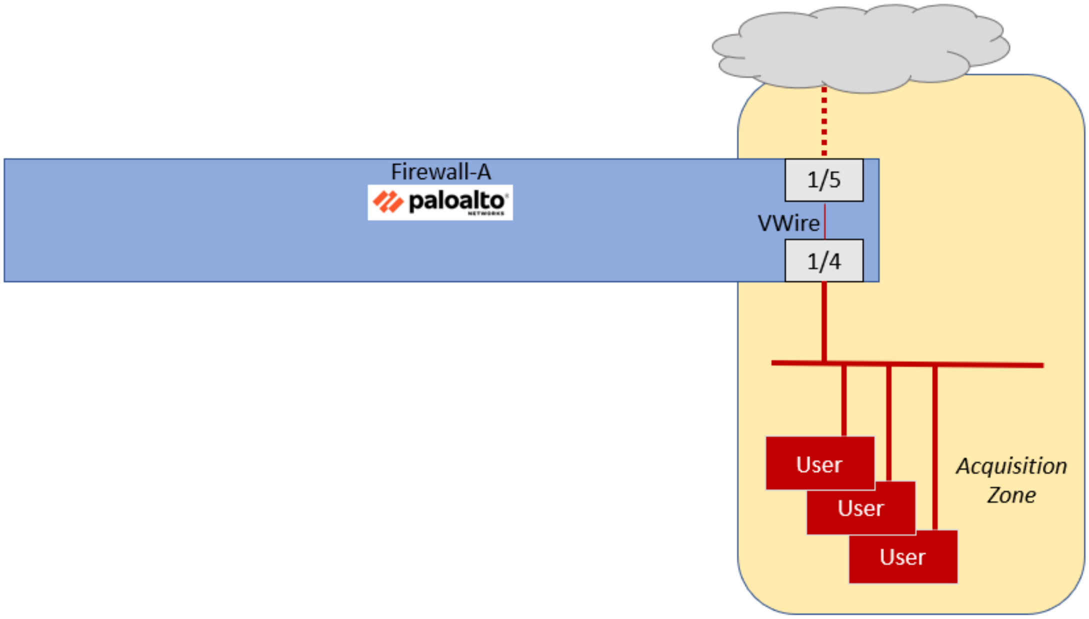
In this lab, you will perform the following tasks:

- 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.

Lab Topology



Theoretical Lab 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)
Client	**192.168.1.20**	`lab-user`	`Pal0Alt0!`
DMZ	**192.168.50.10**	`root`	`Pal0Alt0!`
Firewall	**192.168.1.254**	`admin`	`Pal0Alt0!`
vRouter	**192.168.1.10**	`root`	`Pal0Alt0`

Lab Guidance

There are two sections in this lab guide:

- High-Level Lab Steps
- Detailed Lab Steps

The High-Level Lab Steps section provides only general guidance and information about how to accomplish the lab objectives. This section is more challenging and is suited for students who have a working knowledge of Palo Alto Networks firewalls. If you have never worked with a Palo Alto Networks firewall, we strongly encourage you to use the Detailed Lab Steps section.

The instructions in the Detailed Lab Steps section provide guided, detailed steps and screenshots to accomplish the lab objectives.

If you decide to use the High-Level Lab Guide and get stuck, switch to the Detailed Lab Guide for guidance.

Please Note

You are not required to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Instead, please select the appropriate section based on your familiarity with Palo Alto Networks Firewalls.

1 Blocking Known Threats Using Security Profiles - High Level Lab Steps

It is recommended to use this section if you possess significant experience in working with Palo Alto Networks firewalls. In case you require more comprehensive instructions to achieve the objectives, please utilize the Detailed-Lab Steps section in Task 2.

1.1 Apply a Baseline Configuration to the Firewall

- On the Zorin desktop, select *lab-user*, enter **Pal0Alt0!** for the password.
- For the Palo Alto Firewall, enter **admin** for the user and **Pal0Alt0!** for the password.
- Load and commit the configuration file - **edu-210-11.0a-08.xml** to the Firewall.

1.2 Generate Traffic Without Security Profiles

- Use Remmina to connect to the **Server-Extranet** host.
- Change to the working directory.

  cd pcaps92019/attack.pcaps/ <Enter>

- Run the simulated attacks script.

  ./malwareattacks.sh <Enter>

  This script takes about 6 minutes to complete.

- Allow the script to run uninterrupted.
- Use Firefox on the Client-A workstation to connect to the following URI:

  http://192.168.50.80/badtarfile.tar

- Save the file to the **Downloads** folder when prompted.
- From a new tab in Firefox, browse to the following URI:

  http://192.168.50.80/companyssns.txt

  Note that the browser will display a file with employees and their Social Security Numbers.

- From a **Terminal** window on the Client-A host, use the following command to generate a DNS query using **dig** to resolve a URL to an IP address:

  dig @8.8.8.8 www.quora.com

  The command should return a public IP address, indicating that the URL is accessible.

- Leave the Terminal Emulator window open because you will use it again later in this lab.
- In the firewall web interface, examine the **Threat Log.**
- You should have ***<u>no</u>*** significant entries in the Threat Log.

1.3 Create a Corporate Antivirus Profile

- Clone the **default** Antivirus Profile.
- Rename the clone to **Corp-AV.**
- For the Corp-AV **Description**, enter **Standard antivirus profile for all security policy rules.**

1.4 Create A Corporate Vulnerability Security Profile

- Clone the **strict** Vulnerability Profile.
- Rename the clone to **Corp-Vuln.**
- For the Corp-Vuln **Description**, enter **Standard vulnerability profile for all security policy rules**.

1.5 Create a Corporate File Blocking Profile

- Clone the **strict file blocking** Profile.
- Rename the clone to **Corp-FileBlock**.
- For the Corp-FileBlock **Description**, enter **Standard file blocking profile for all security policy rules**.

1.6 Create a Corporate Data Filtering Profile

- Use the information below to create a Data Filtering Pattern that will identify US Social Security numbers with and without dash separators.

Parameter	**Value**
Name	**US-SSNs**
Description	**US Social Security Numbers**
Pattern Type	**Predefined Pattern**
First Pattern	**Social Security Numbers**
Second Pattern	**Social Security Numbers (without dash separator)**

- Use the information below to create a **Data Filtering** Profile.

Parameter	**Value**
Name	**Corp-DataFilter**
Description	**Standard data filtering profile for all security rules**
Data Pattern	**US-SSNs**
Alert Threshold	**1**
Block Threshold	**3**
Log Severity	**critical**

1.7 Create a Corporate Anti-Spyware Security Profile

- Clone the **strict** Anti-Spyware Profile.
- Rename the clone **Corp-AS.**
- For the Corp-AS **Description**, enter **Standard anti-spyware profile for all security policy rules.**

1.8 Create an External Dynamic List for Malicious Domains

- Use the information below to create an External Dynamic List

Parameter	Value
Name	malicious-domains-edl
Type	Domain List
Description	Custom list of bad domains maintained on Extranet server
Source	**http://192.168.50.80/malicious-domains.txt** (The EDL contains the domains quora.com and producthunt.com.)
Automatically expand to include subdomains	Checked
Check for updates	Every Five Minutes

1.9 Update the Anti-Spyware Profile with EDL

- Edit the **Corp-AS** Security and apply the DNS **sinkhole** action to the entry for **malicious-domains-edl.**

1.10 Commit the Configuration

- Commit the changes before proceeding.

1.11 Create a Security Profile Group

- Use the information below to create a Security Profile Group

Parameter	Value
Name	Corp-Profiles-Group
Antivirus Profile	Corp-AV
Anti-Spyware Profile	Corp-AS

Parameter	Value
Vulnerability Protection Profile	Corp-Vuln
URL Filtering Profile	none
File Blocking Profile	Corp-FileBlock
Data Filtering Profile	Corp-DataFilter
Wildfire Analysis Profile	none

Leave the URL Filtering Profile and the WildFire Analysis Profile set to none for this lab.

1.12 Apply the Corp-Profiles-Group to Security Policy Rules

- Individually edit each Security Policy rule that allows traffic and change the **Profile Setting** under the **Action** tab to use the **Corp-Profiles-Group.**
  - **Allow-PANW-Apps**
  - **Users_to_Extranet**
  - **Users_to_Internet**
  - **Extranet_to_Internet**
  - **Extranet_to_User_Net**
  - **Acquisition-Allow-All**

1.13 Commit the Configuration

- Commit the changes before proceeding.

1.14 Generate Attack Traffic to Test Security Profiles

- Use Remmina to connect to the **Server-Extranet** host.
- Change to the working directory.

  cd pcaps92019/attack.pcaps/ <Enter>

- Run the simulated attacks script.

  ./malwareattacks.sh <Enter>

  This script takes about 6 minutes to complete.

- Allow the script to run uninterrupted.
- Use Firefox on the Client-A workstation to connect to the following URI:

  http://192.168.50.80/badtarfile.tar

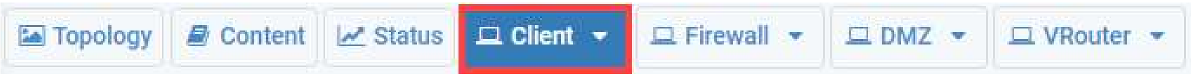
- You should receive a File Transfer Blocked page from the firewall.

2 Blocking known Threats Using Security Profiles – Detailed Lab Steps

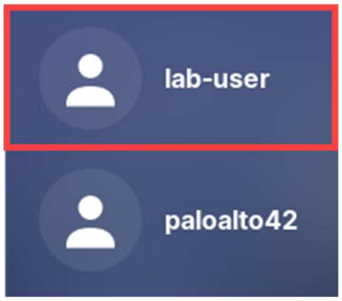
2.1 Apply a Baseline Configuration to the Firewall

In this section, you will connect to the Firewall and load the Firewall configuration file.

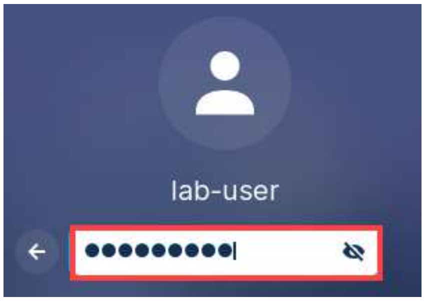
1. Click on the **Client** tab to access the Client PC.



2. On the *Zorin* desktop, click **lab-user.**

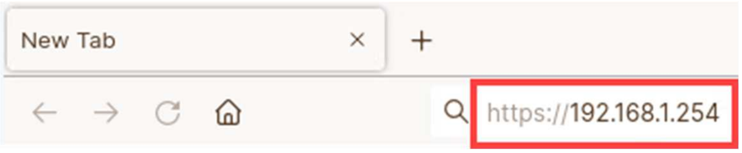


3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.

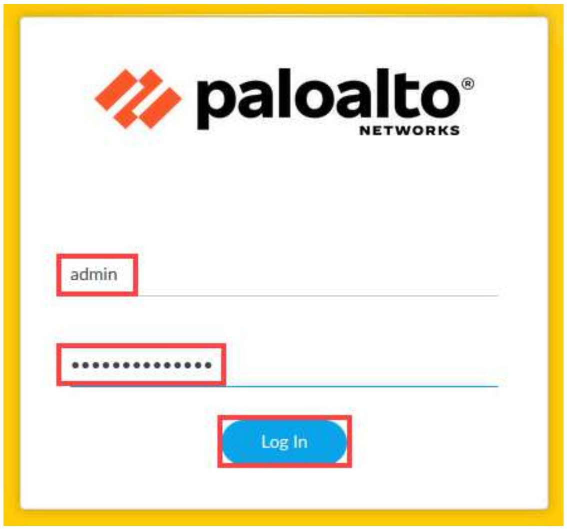


4. Double-click the **Firefox Web Browser** icon located on the *Desktop*.

5. In the *Firefox* address field, type **`https://192.168.1.254`** and press **Enter**.

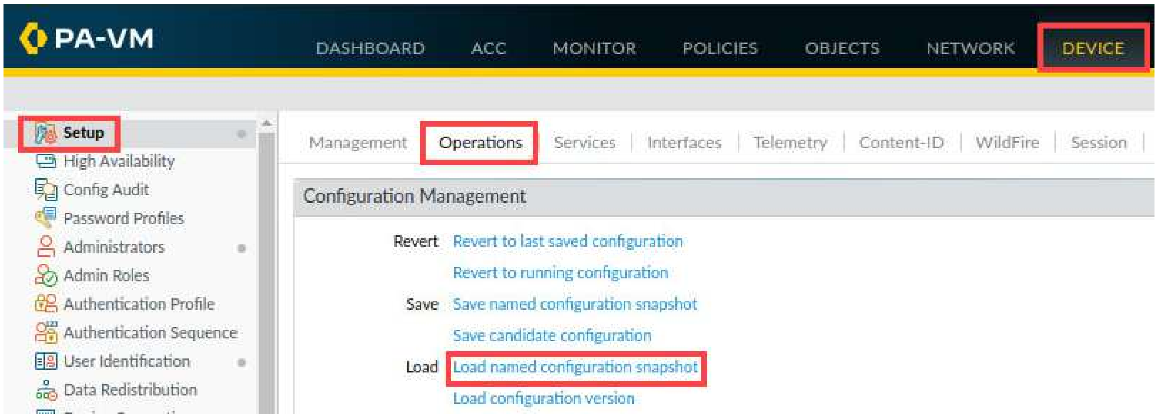


6. Log in to the Firewall web interface as username **admin**, password **`Pal0Alt0!`**.

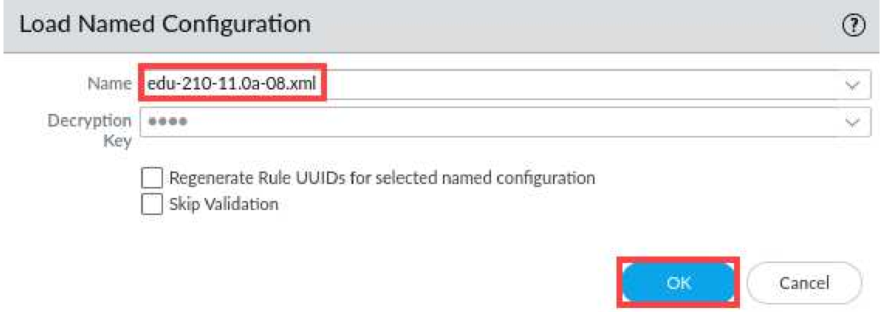


If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

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



8. In the *Load Named Configuration* window, select **edu-210-11.0a-08.xml** from the *Name* drop-down box and click **OK**.


Load Named Configuration

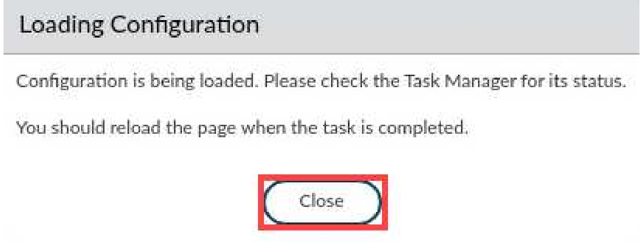
Name: edu-210-11.0a-08.xml

Decryption Key: ••••

☐ Regenerate Rule UUIDs for selected named configuration

☐ Skip Validation

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.

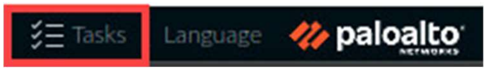


Loading Configuration

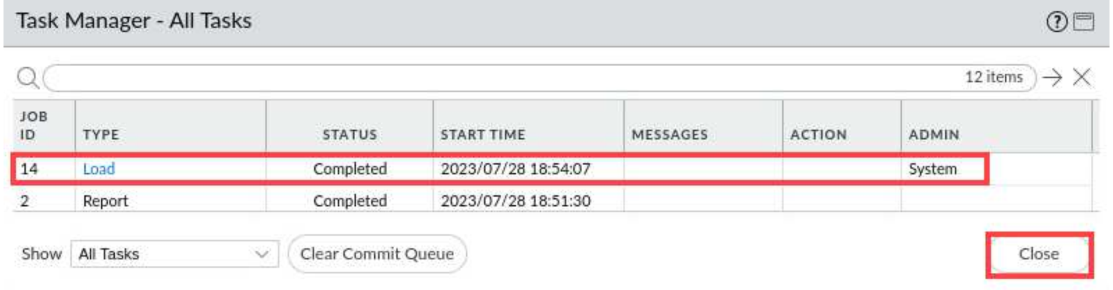
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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



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

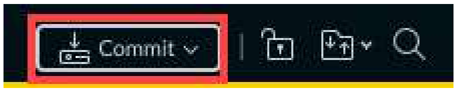


Task Manager - All Tasks

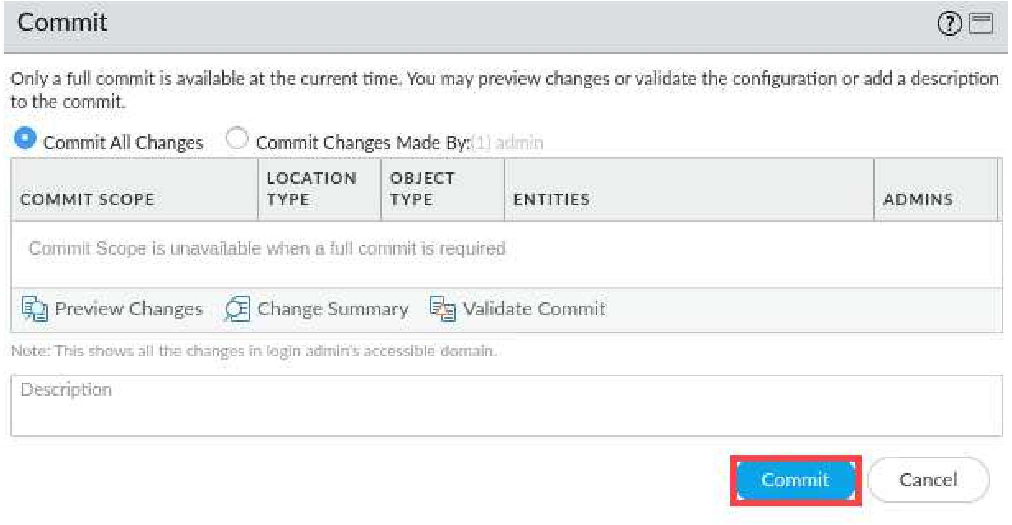
12 items

JOB ID	TYPE	STATUS	START TIME	MESSAGES	ACTION	ADMIN
14	Load	Completed	2023/07/28 18:54:07			System
2	Report	Completed	2023/07/28 18:51:30			

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

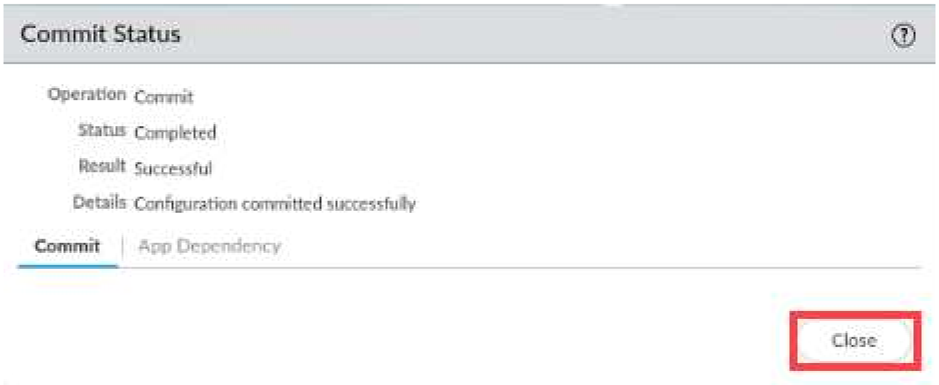
Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

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

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

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

14. When the commit operation is complete, click **Close** to continue.

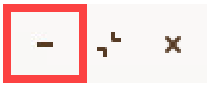


Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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.



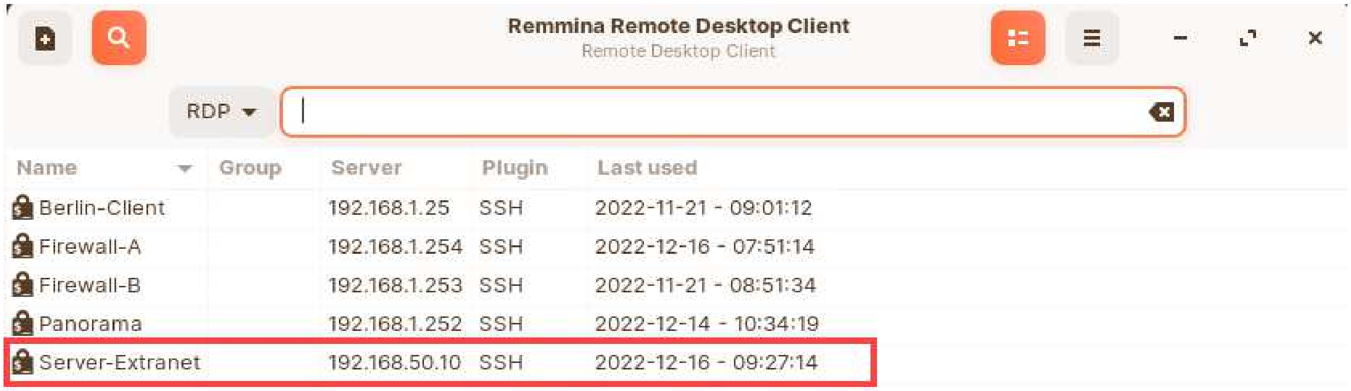
2.2 Generate Traffic Without Security Profiles

In this section, you will generate traffic that contains threats and malicious content. You will do so from the client workstation and from the Extranet server. Because you have not yet configured Security Profiles for your Security Policy, the firewall will allow this harmful traffic.

After the testing, you will examine the Threat Log to verify that this traffic was passed through the Palo Alto Networks Firewall.

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

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

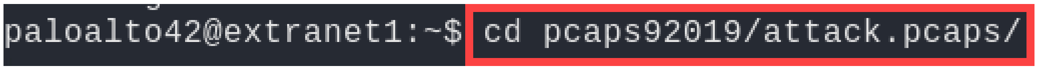


Name	Group	Server	Plugin	Last used
Berlin-Client		192.168.1.25	SSH	2022-11-21 - 09:01:12
Firewall-A		192.168.1.254	SSH	2022-12-16 - 07:51:14
Firewall-B		192.168.1.253	SSH	2022-11-21 - 08:51:34
Panorama		192.168.1.252	SSH	2022-12-14 - 10:34:19
Server-Extranet		192.168.50.10	SSH	2022-12-16 - 09:27:14

> **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.

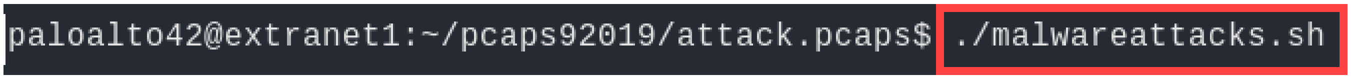
```
paloalto42@extranet1:~$ cd pcaps92019/attack.pcaps/ <Enter>
```



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

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

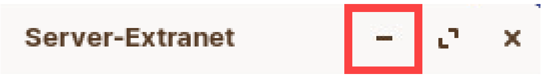
```
paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh <Enter>
```



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

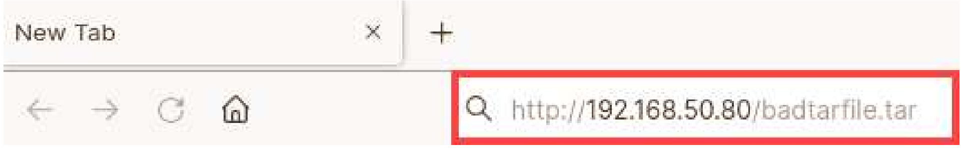
> **Please Note**
>
> This script takes about 6 minutes to complete. Allow the **malwareattacks** script to run uninterrupted.

5. Minimize the *Remmina* connection window.



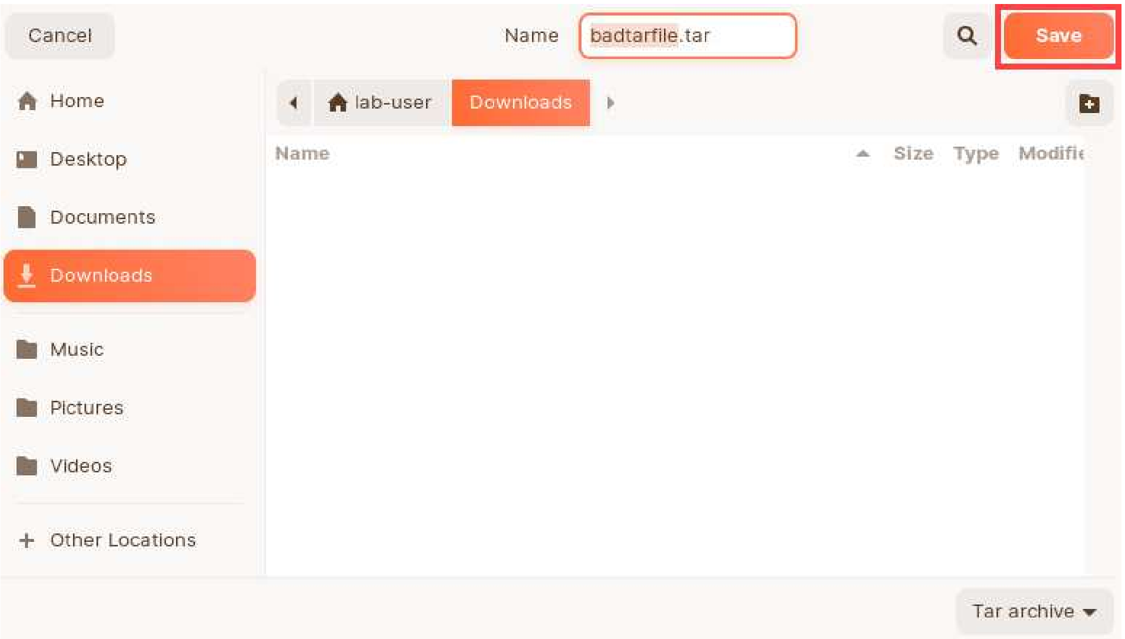
6. On the client desktop, open another **Firefox Web Browser** application.

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

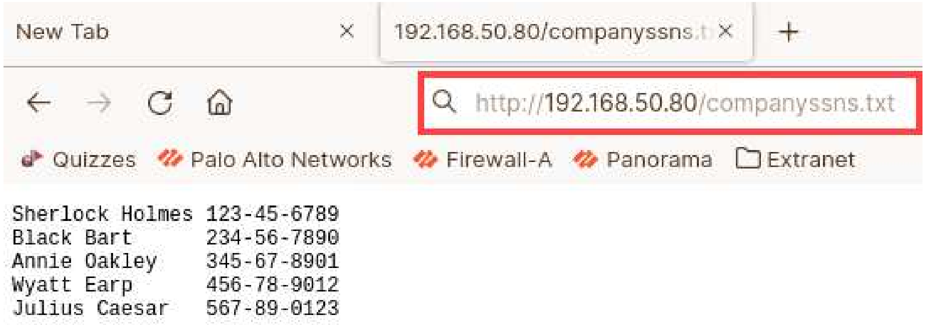


Please Note The download should succeed. This filetype is one that you will block when you configure the firewall with a File Blocking Profile.

8. When prompted, select **Save**.

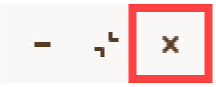


9. In the *Firefox Web Browser*, open a new tab. Type **`http://192.168.50.80/companyssns.txt`** and press **Enter.** The browser will display a file with *fictitious names* and *social security numbers.*


New Tab
192.168.50.80/companyssns.t
http://192.168.50.80/companyssns.txt
Quizzes
Palo Alto Networks
Firewall-A
Panorama
Extranet

```
Sherlock Holmes 123-45-6789
Black Bart      234-56-7890
Annie Oakley    345-67-8901
Wyatt Earp      456-78-9012
Julius Caesar   567-89-0123
```

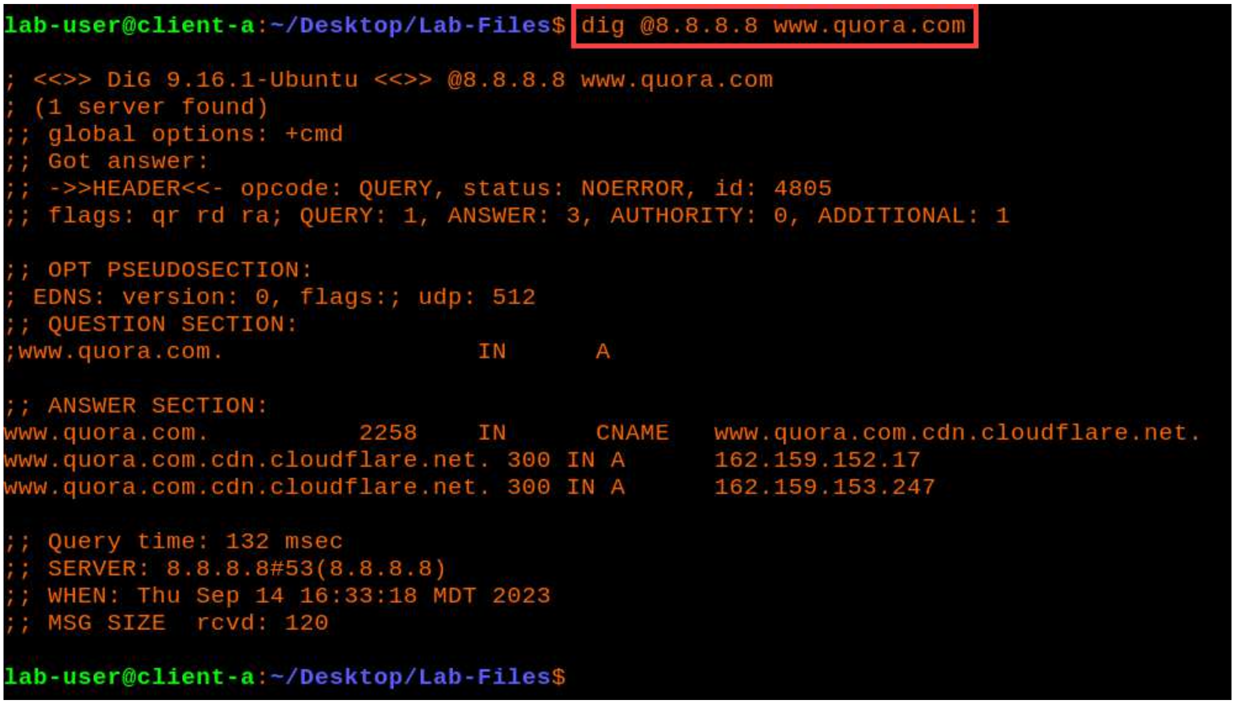
10. Close the *Firefox browser*.



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.

```
lab-user@client-a:~\Desktop\Lab-Files$ dig @8.8.8.8 www.quora.com
```



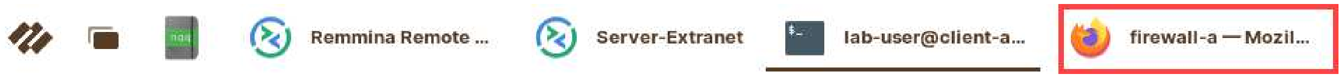
```
lab-user@client-a:~/Desktop/Lab-Files$ dig @8.8.8.8 www.quora.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 www.quora.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4805
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.quora.com.                 IN      A

;; ANSWER SECTION:
www.quora.com.          2258    IN      CNAME   www.quora.com.cdn.cloudflare.net.
www.quora.com.cdn.cloudflare.net. 300 IN A      162.159.152.17
www.quora.com.cdn.cloudflare.net. 300 IN A      162.159.153.247

;; Query time: 132 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Sep 14 16:33:18 MDT 2023
;; MSG SIZE  rcvd: 120

lab-user@client-a:~/Desktop/Lab-Files$
```

Please Note

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. Re-open the *PA-VM firewall* web interface by clicking on the **firewall-a – Mozilla Firefox** icon in the task bar.

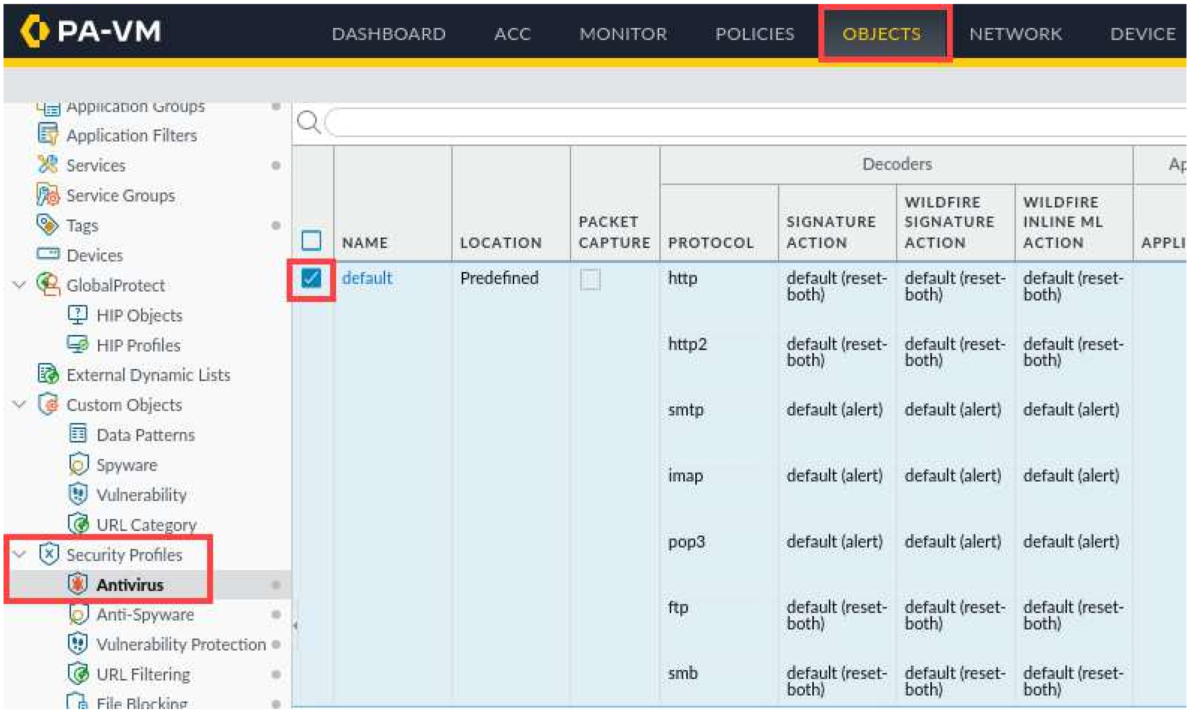


15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.3 Create a Corporate Antivirus Profile

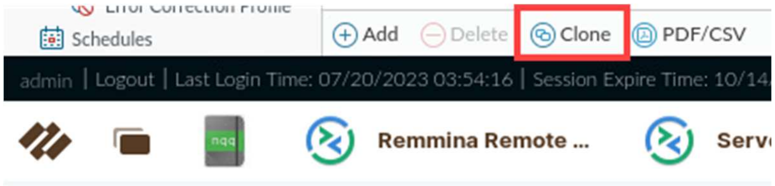
In this section, you will create the first of several Security Profiles. The Antivirus Profile you make will use signatures provided by Palo Alto Networks to watch for and block known threats from viruses.

1. Select **Objects > Security Profiles > Antivirus**. Place a check in the box next to the **default** entry.

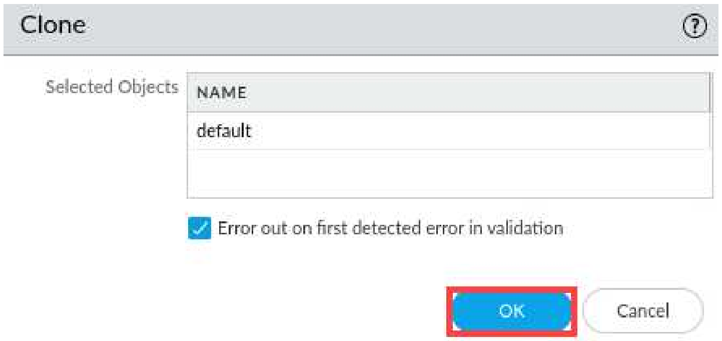


				Decoders				Ap
□	NAME	LOCATION	PACKET CAPTURE	PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	APPLI
☑	default	Predefined	□	http	default (reset-both)	default (reset-both)	default (reset-both)	
				http2	default (reset-both)	default (reset-both)	default (reset-both)	
				smtp	default (alert)	default (alert)	default (alert)	
				imap	default (alert)	default (alert)	default (alert)	
				pop3	default (alert)	default (alert)	default (alert)	
				ftp	default (reset-both)	default (reset-both)	default (reset-both)	
				smb	default (reset-both)	default (reset-both)	default (reset-both)	

2. At the bottom of the window, click the **Clone** button.


Error Correction Profile
Schedules
Add
Delete
Clone
PDF/CSV
admin | Logout | Last Login Time: 07/20/2023 03:54:16 | Session Expire Time: 10/14
Remmina Remote ...
Serv

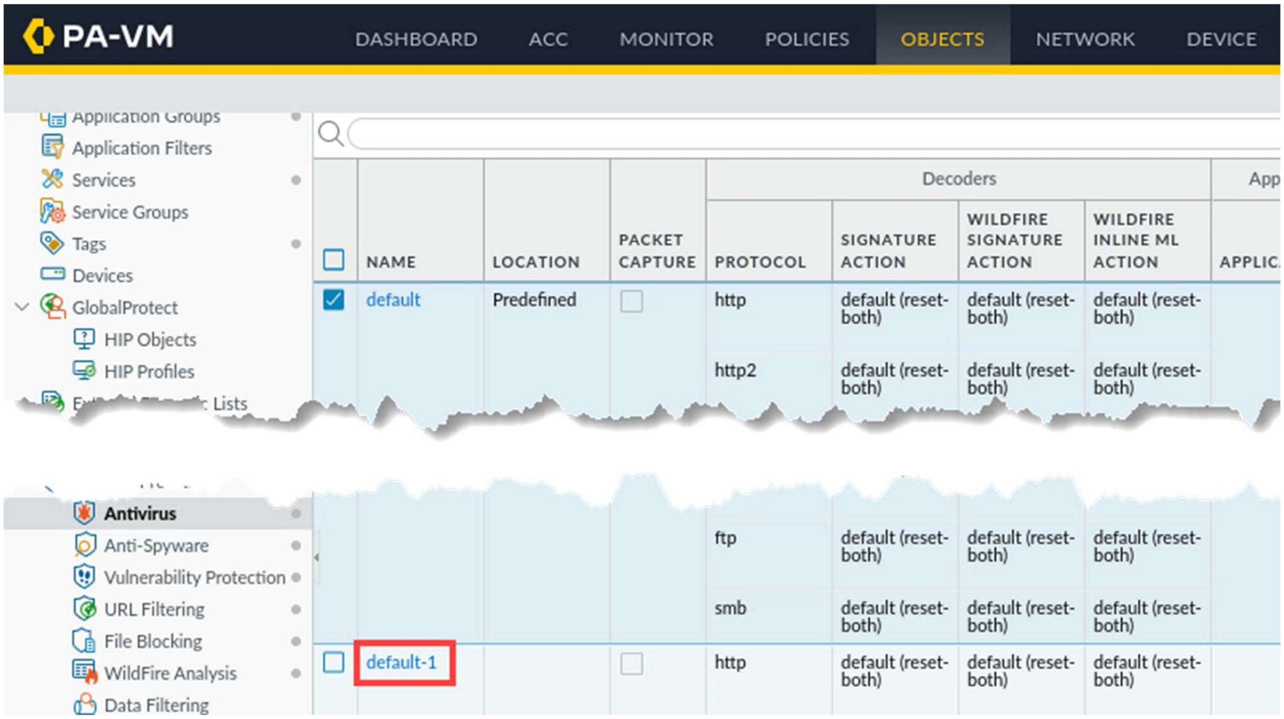
3. In the **Clone** window that appears, leave the settings unchanged. Click **OK**.



NAME
default

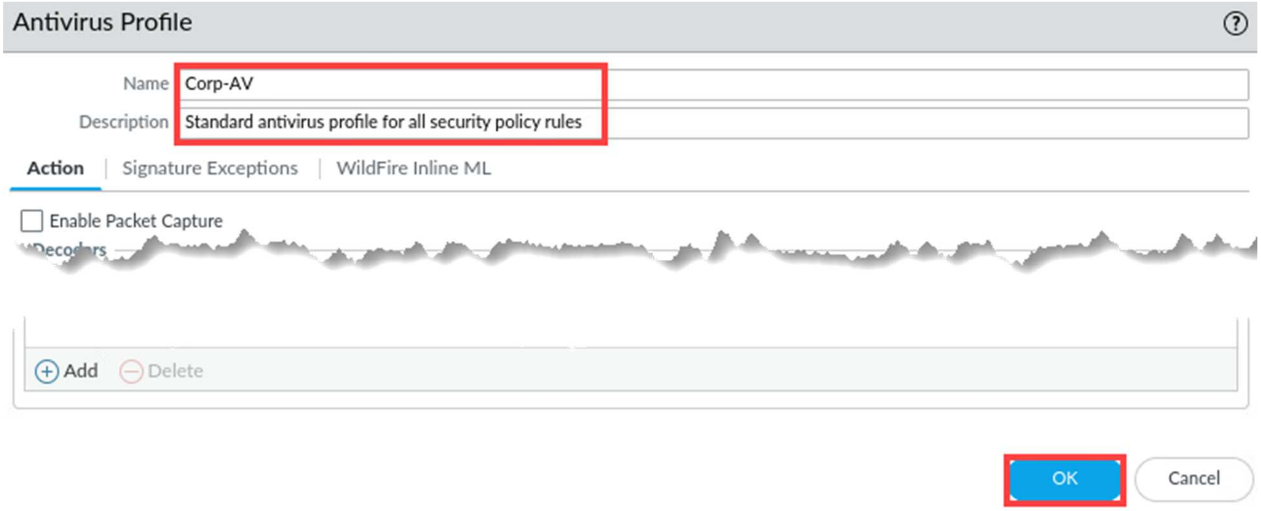
☑ Error out on first detected error in validation

4. A new entry called **default-1** will appear in the Antivirus list. Click the entry for **default-1** to edit it.



				Decoders				App
□	NAME	LOCATION	PACKET CAPTURE	PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	APPLIC
☑	default	Predefined	□	http	default (reset-both)	default (reset-both)	default (reset-both)	
				http2	default (reset-both)	default (reset-both)	default (reset-both)	
				ftp	default (reset-both)	default (reset-both)	default (reset-both)	
				smb	default (reset-both)	default (reset-both)	default (reset-both)	
□	default-1		□	http	default (reset-both)	default (reset-both)	default (reset-both)	

5. In the *Antivirus Profile* window, for the *Name*, enter **Corp-AV**. For *Description*, enter **`Standard antivirus profile for all security policy rules`**. Click **OK**.



Name: Corp-AV

Description: Standard antivirus profile for all security policy rules

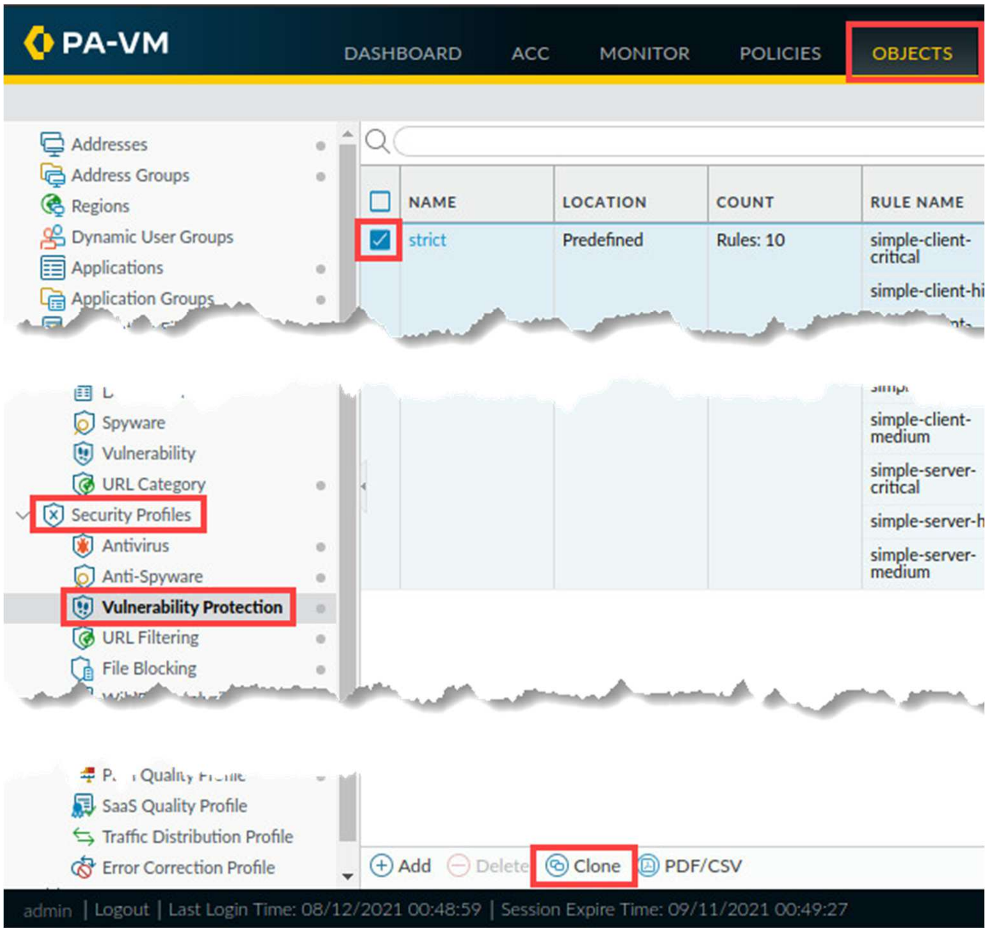
□ Enable Packet Capture

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

2.4 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.

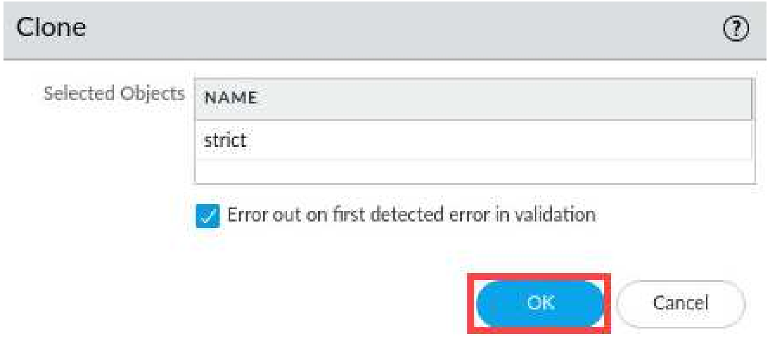
1. Select **Objects > Security Profiles > Vulnerability Protection**. Place a check in the box beside **strict.** Click **Clone.**



	NAME	LOCATION	COUNT	RULE NAME
☑	strict	Predefined	Rules: 10	simple-client-critical simple-client-hi simple-client-medium simple-server-critical simple-server-h simple-server-medium

admin | Logout | Last Login Time: 08/12/2021 00:48:59 | Session Expire Time: 09/11/2021 00:49:27

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

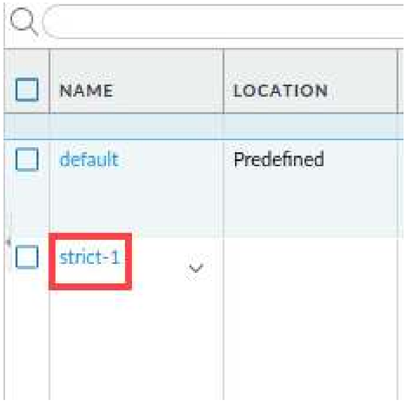


Selected Objects

NAME
strict

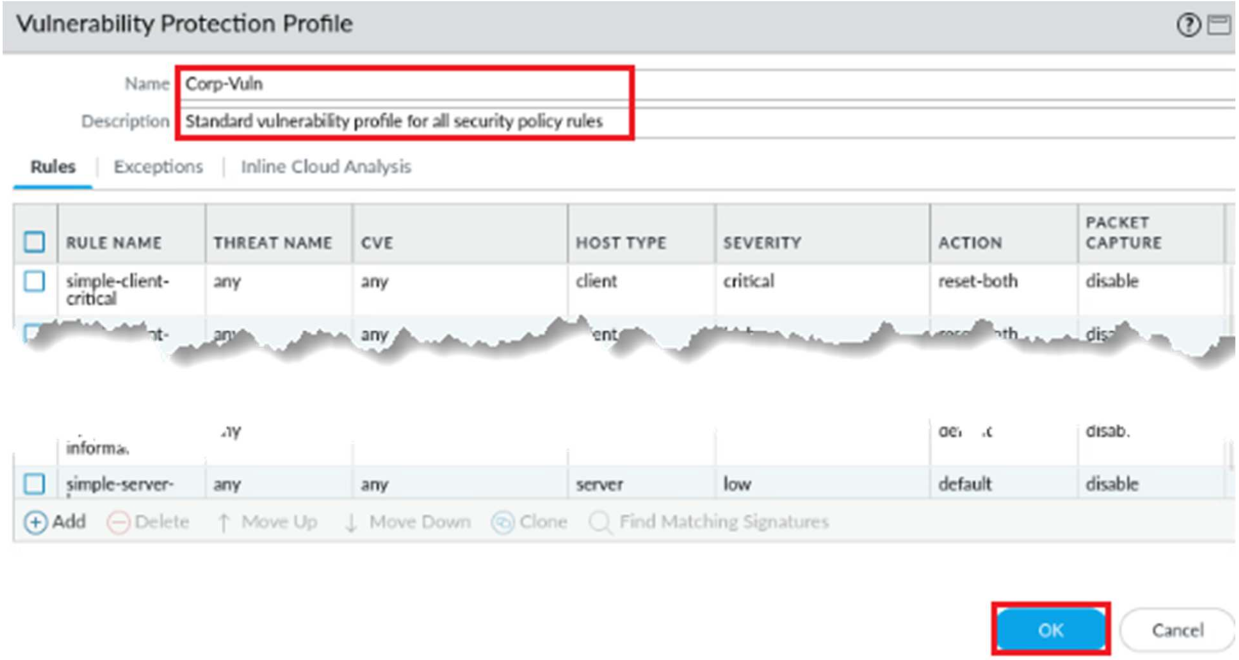
☑ Error out on first detected error in validation

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



□	NAME	LOCATION
□	default	Predefined
□	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**.



Vulnerability Protection Profile

Name: Corp-Vuln

Description: Standard vulnerability profile for all security policy rules

□	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
□	simple-client-critical	any	any	client	critical	reset-both	disable
□	informa.	any				default	disable
□	simple-server-	any	any	server	low	default	disable

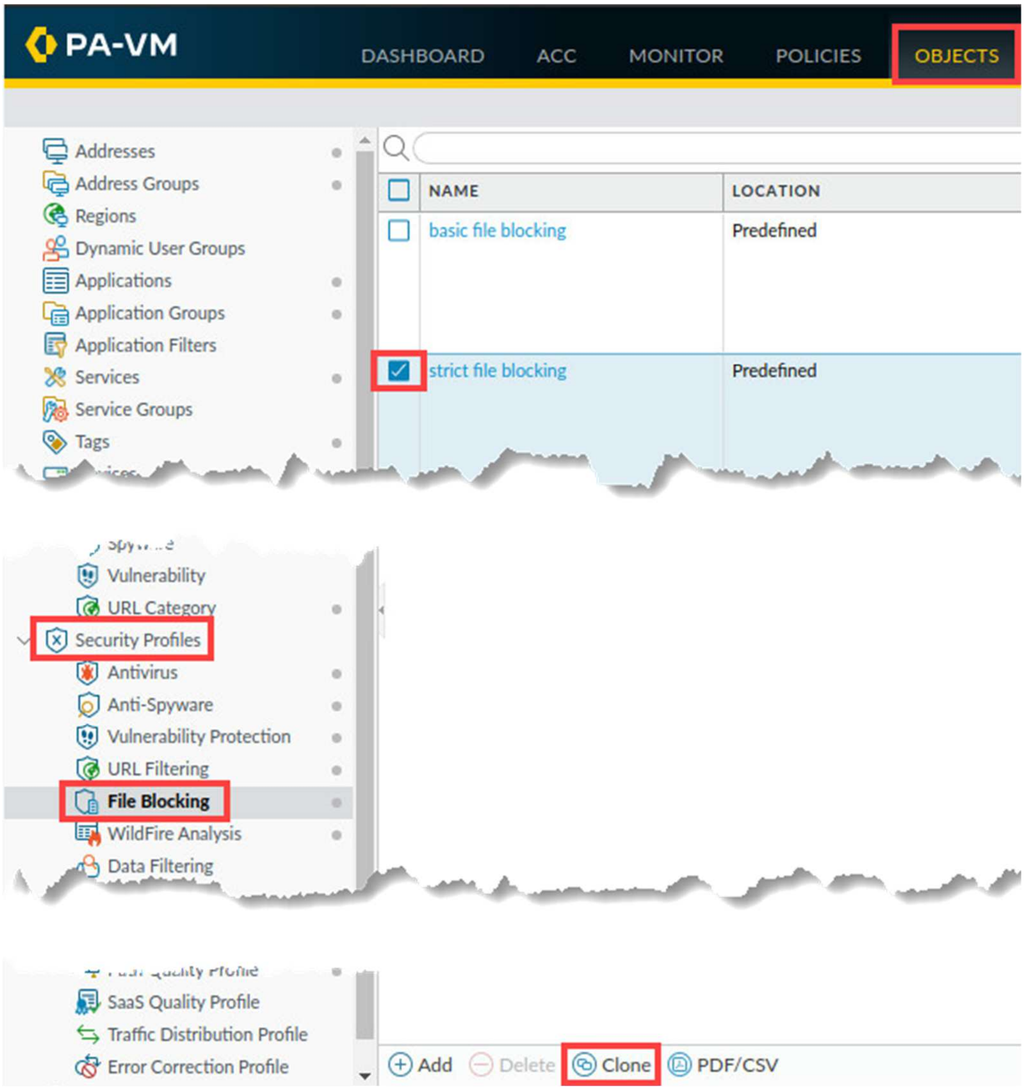
5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.5 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.

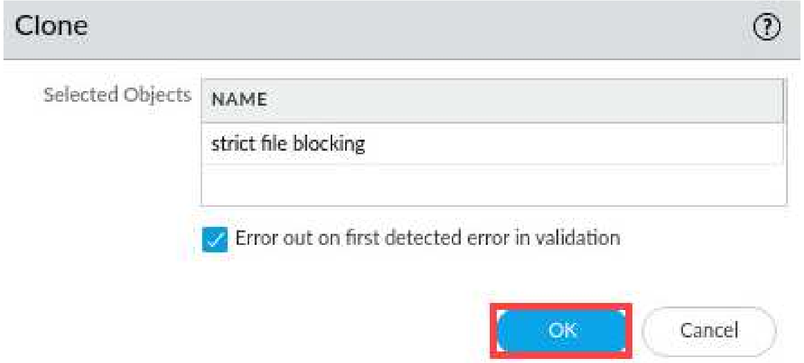
You will clone the strict file blocking Profile and modify it to function as your Corp-FileBlock Profile.

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



☐	NAME	LOCATION
☐	basic file blocking	Predefined
☑	strict file blocking	Predefined

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

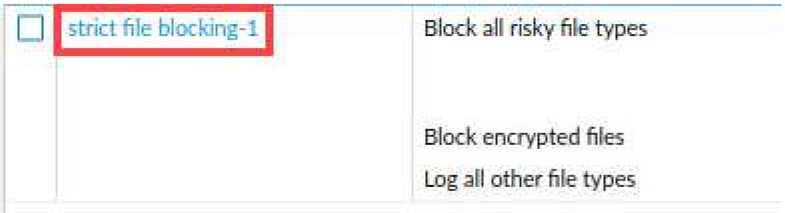


Selected Objects

NAME
strict file blocking

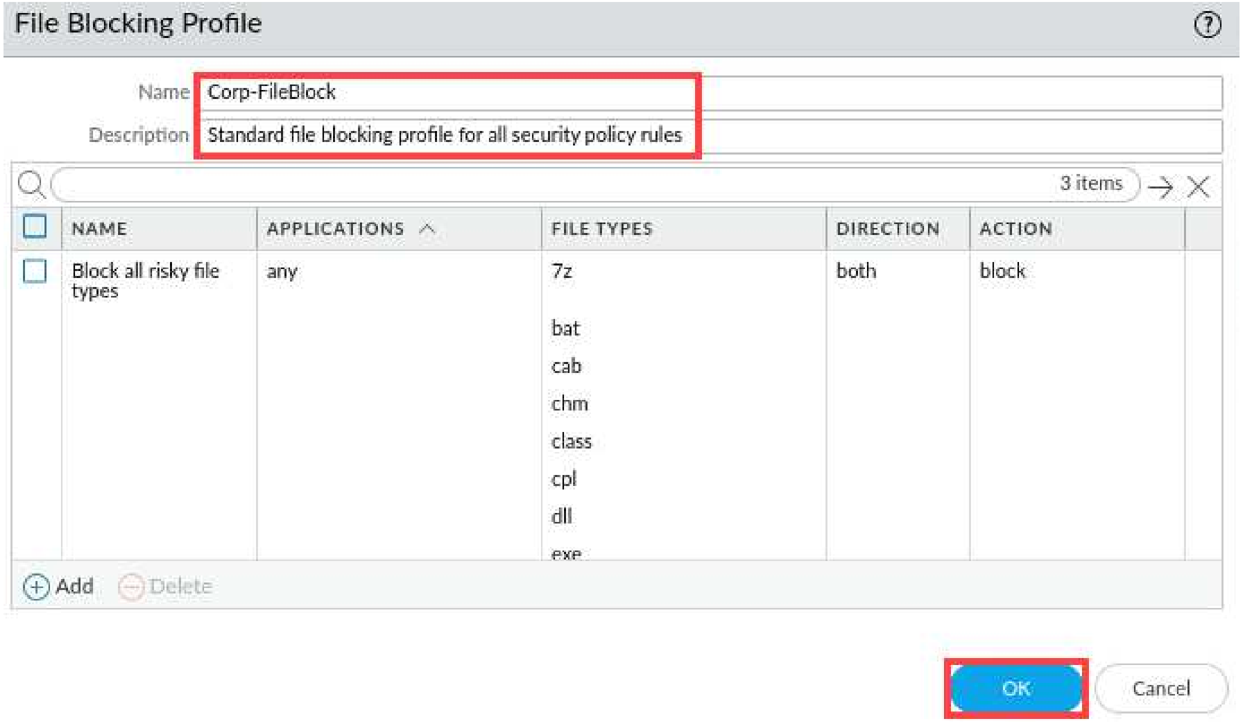
☑ Error out on first detected error in validation

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



□ strict file blocking-1	Block all risky file types Block encrypted files Log all other file types

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



File Blocking Profile

Name: Corp-FileBlock

Description: Standard file blocking profile for all security policy rules

3 items

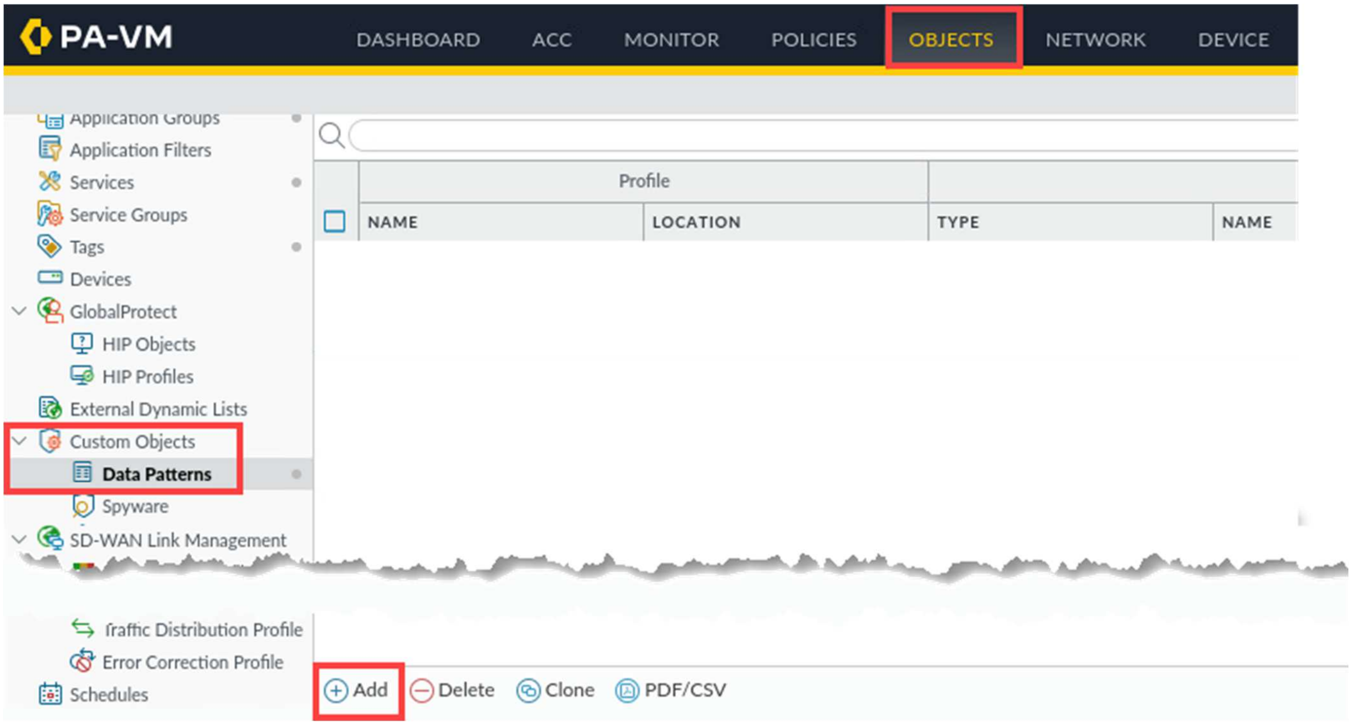
□	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
□	Block all risky file types	any	7z bat cab chm class cpl dll exe	both	block

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

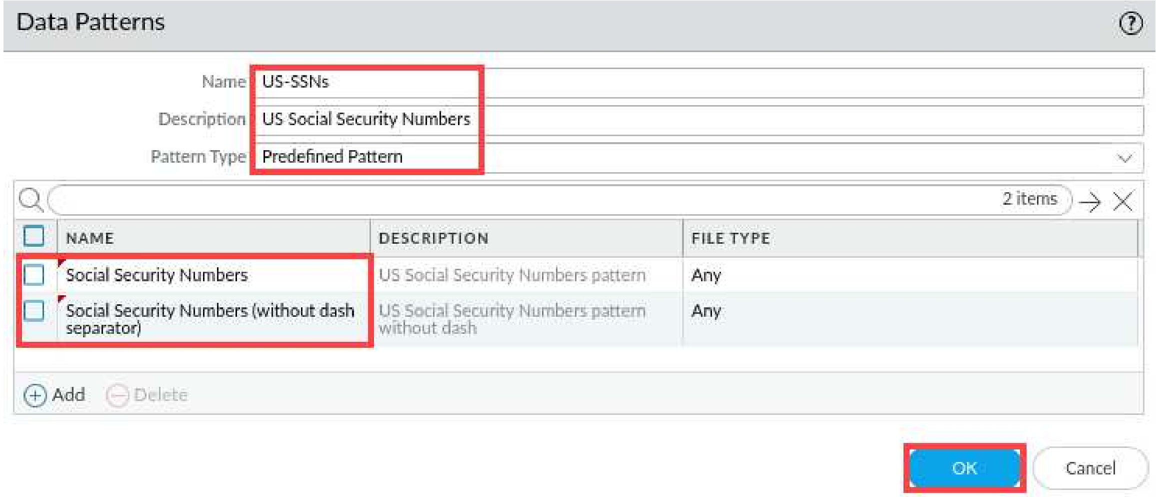
2.6 Create a Corporate Data Filtering Profile

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**. 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**.


Data Patterns

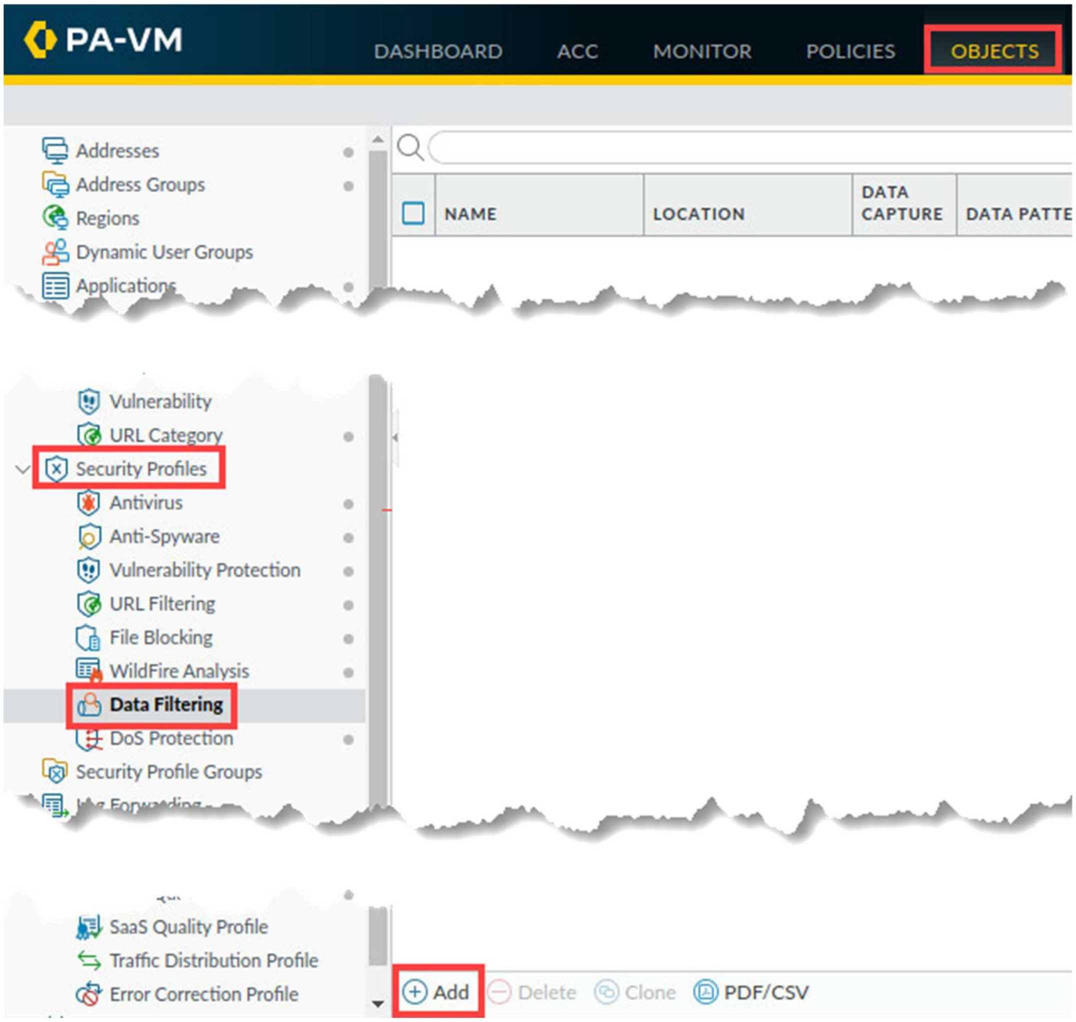
Name: US-SSNs

Description: US Social Security Numbers

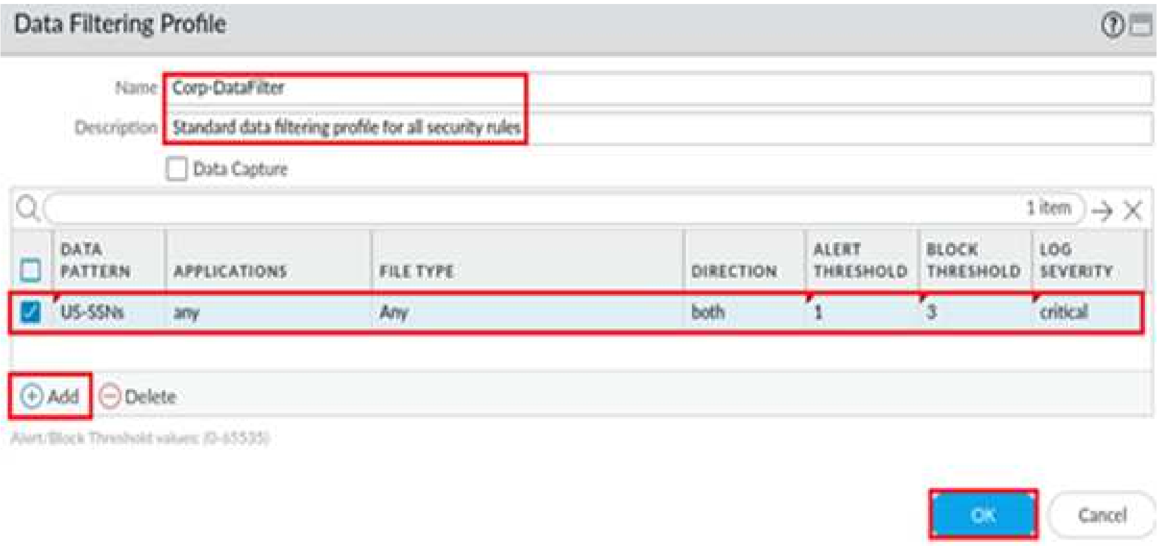
Pattern Type: Predefined Pattern

□	NAME	DESCRIPTION	FILE TYPE
□	Social Security Numbers	US Social Security Numbers pattern	Any
□	Social Security Numbers (without dash separator)	US Social Security Numbers pattern without dash	Any

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



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



Data Filtering Profile

Name: Corp-DataFilter

Description: Standard data filtering profile for all security rules

□ Data Capture

1 item

☐	DATA PATTERN	APPLICATIONS	FILE TYPE	DIRECTION	ALERT THRESHOLD	BLOCK THRESHOLD	LOG SEVERITY
☑	US-SSNs	any	Any	both	1	3	critical

⊕ Add ⊖ Delete

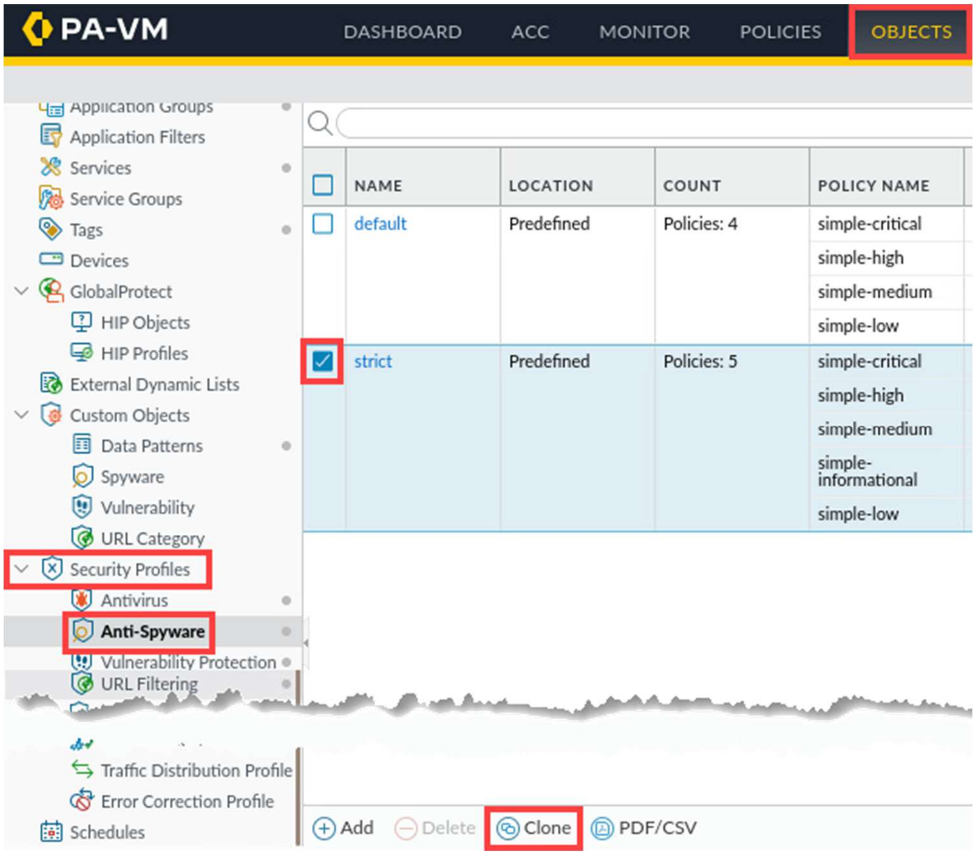
Alert/Block Threshold values: (0-65535)

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

2.7 Create a Corporate Anti Spyware Profile

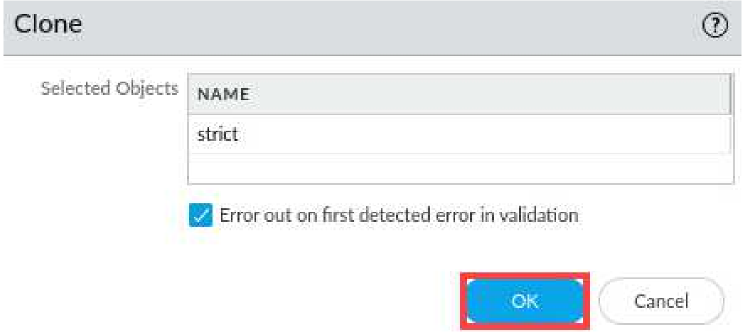
Create a Security Profile that will watch for and block known spyware.

1. Select **Objects > Security Profiles > Anti-Spyware**. Select the check box next to the **strict** Anti-Spyware Profile. Click **Clone**.



☐	NAME	LOCATION	COUNT	POLICY NAME
☐	default	Predefined	Policies: 4	simple-critical simple-high simple-medium simple-low
☑	strict	Predefined	Policies: 5	simple-critical simple-high simple-medium simple-informational simple-low

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

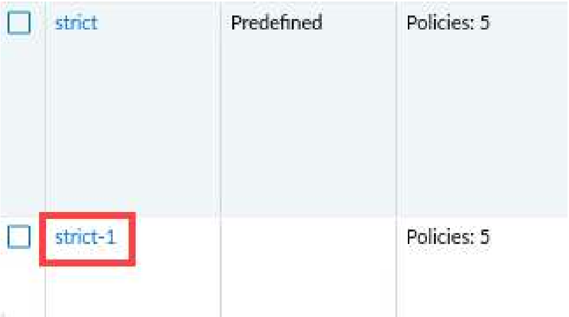


Selected Objects

NAME
strict

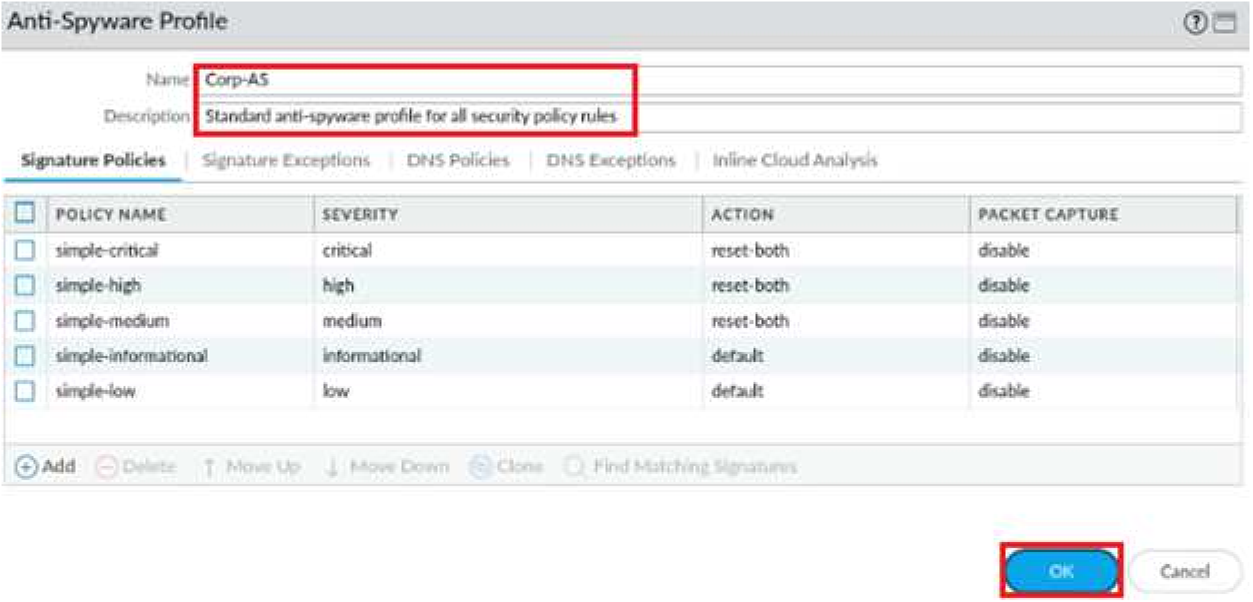
☑ Error out on first detected error in validation

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



□	strict	Predefined	Policies: 5
□	strict-1		Policies: 5

4. In the *Anti-Spyware Profile* window, for *Name*, enter **`Corp-AS`**. For *Description*, enter **Standard anti-spyware profile for all security policy rules.** Click **OK.**



Anti-Spyware Profile

Name: Corp-AS

Description: Standard anti-spyware profile for all security policy rules

□	POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
□	simple-critical	critical	reset-both	disable
□	simple-high	high	reset-both	disable
□	simple-medium	medium	reset-both	disable
□	simple-informational	informational	default	disable
□	simple-low	low	default	disable

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

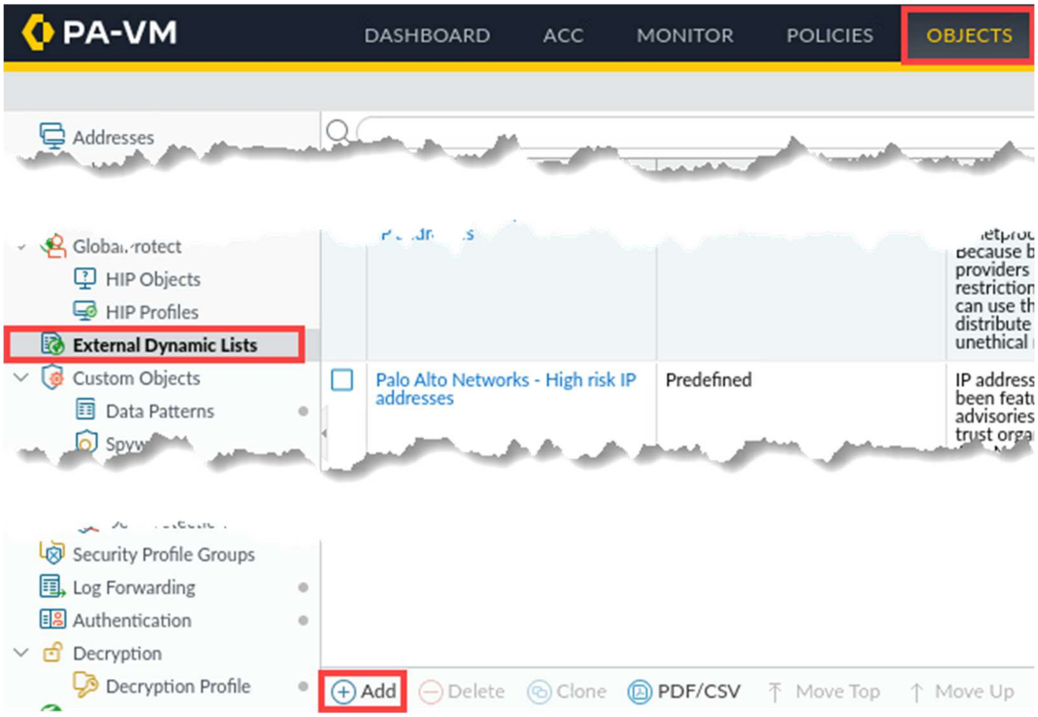
2.8 Create an External Dynamic List for Malicious Domains

You need to configure the firewall to ingest an external dynamic list that contains entries for several malicious domains that users should not access due to company restrictions. You have a list available on a local server that you can import to the firewall.

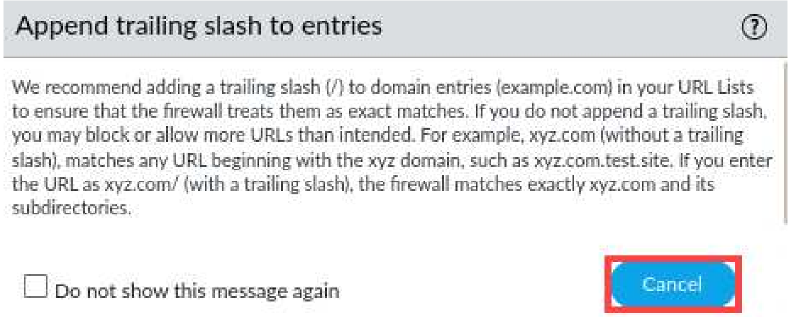
In this section, you will configure the firewall to import an External Dynamic List (EDL) from a server in the DMZ.

With the list configured on the firewall, you will update the Corporate-AS Anti-Spyware Profile to sinkhole entries in the EDL.

1. Select **Objects > External Dynamic Lists**. Click **Add**.



2. The firewall presents a notice about tokens for domain entries, read the notice and click **Cancel**.



Append trailing slash to entries

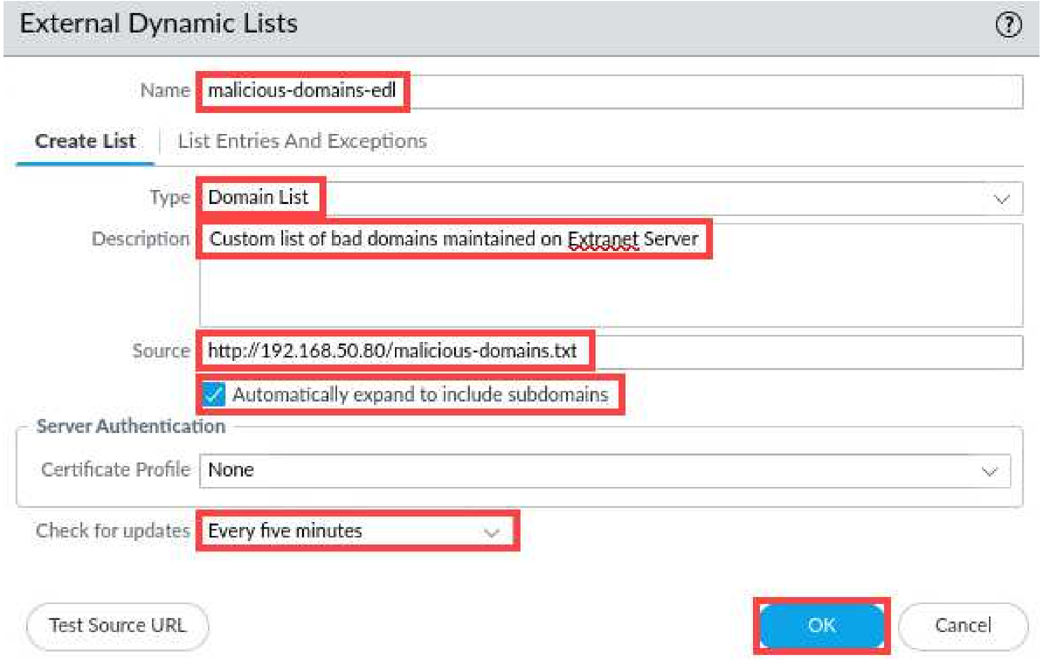
We recommend adding a trailing slash (/) to domain entries (example.com) in your URL Lists to ensure that the firewall treats them as exact matches. If you do not append a trailing slash, you may block or allow more URLs than intended. For example, xyz.com (without a trailing slash), matches any URL beginning with the xyz domain, such as xyz.com.test.site. If you enter the URL as xyz.com/ (with a trailing slash), the firewall matches exactly xyz.com and its subdirectories.

☐ Do not show this message again

Cancel

3. In the *External Dynamic Lists* window, configure the following and click **OK**.

Parameter	**Value**
Name	**malicious-domains-edl**
Type	**Domain List**
Description	**Custom list of bad domains maintained on Extranet server**
Source	**http://192.168.50.80/malicious-domains.txt** (The EDL contains the domains quora.com and producthunt.com.)
Automatically expand to include subdomains	**Checked**
Check for updates	**Every Five Minutes**



External Dynamic Lists

Name: malicious-domains-edl

Type: Domain List

Description: Custom list of bad domains maintained on Extranet Server

Source: http://192.168.50.80/malicious-domains.txt

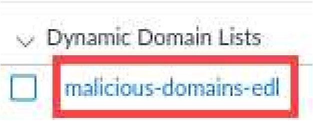
☑ Automatically expand to include subdomains

Server Authentication

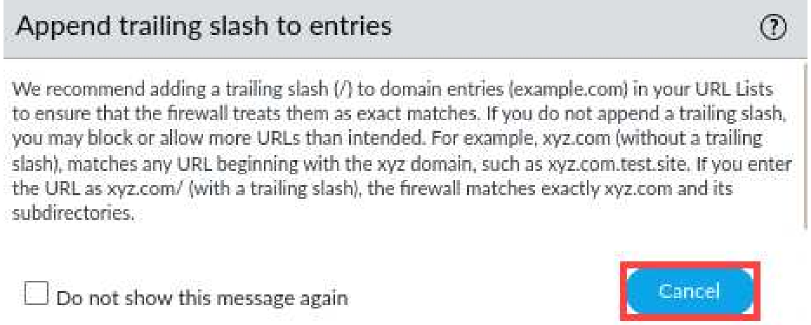
Certificate Profile: None

Check for updates: Every five minutes

4. Click **malicious-domains-edl.**



5. The firewall presents a notice about tokens for domain entries, click **Cancel**.

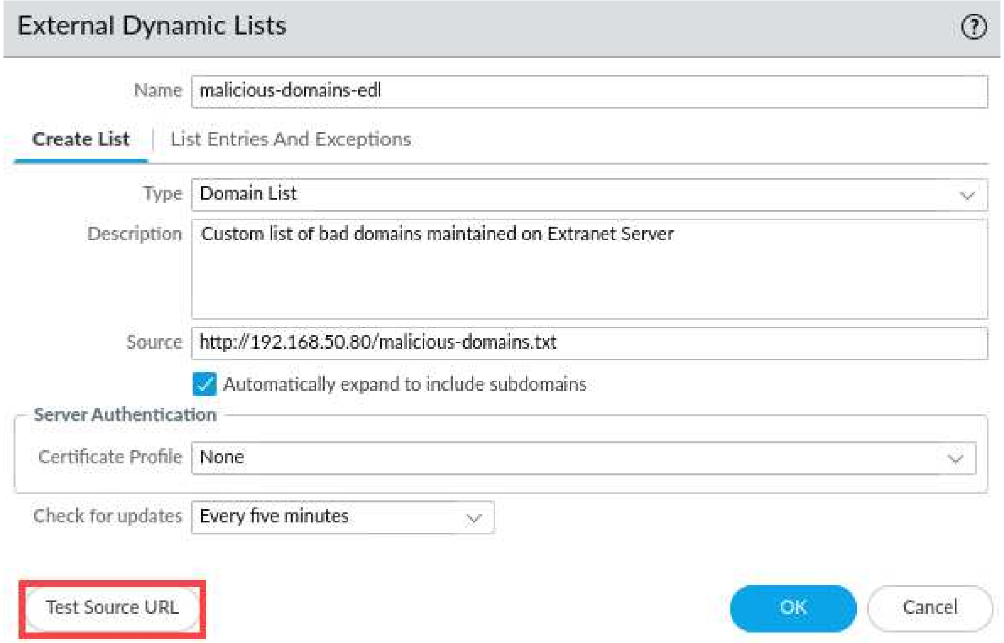


Append trailing slash to entries

We recommend adding a trailing slash (/) to domain entries (example.com) in your URL Lists to ensure that the firewall treats them as exact matches. If you do not append a trailing slash, you may block or allow more URLs than intended. For example, xyz.com (without a trailing slash), matches any URL beginning with the xyz domain, such as xyz.com.test.site. If you enter the URL as xyz.com/ (with a trailing slash), the firewall matches exactly xyz.com and its subdirectories.

□ Do not show this message again

6. Click **Test Source URL** to verify that the firewall can access the EDL URL.


External Dynamic Lists

Name: malicious-domains-edl

Create List | List Entries And Exceptions

Type: Domain List

Description: Custom list of bad domains maintained on Extranet Server

Source: http://192.168.50.80/malicious-domains.txt

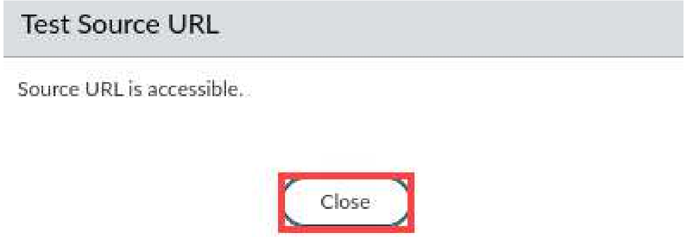
☑ Automatically expand to include subdomains

Server Authentication

Certificate Profile: None

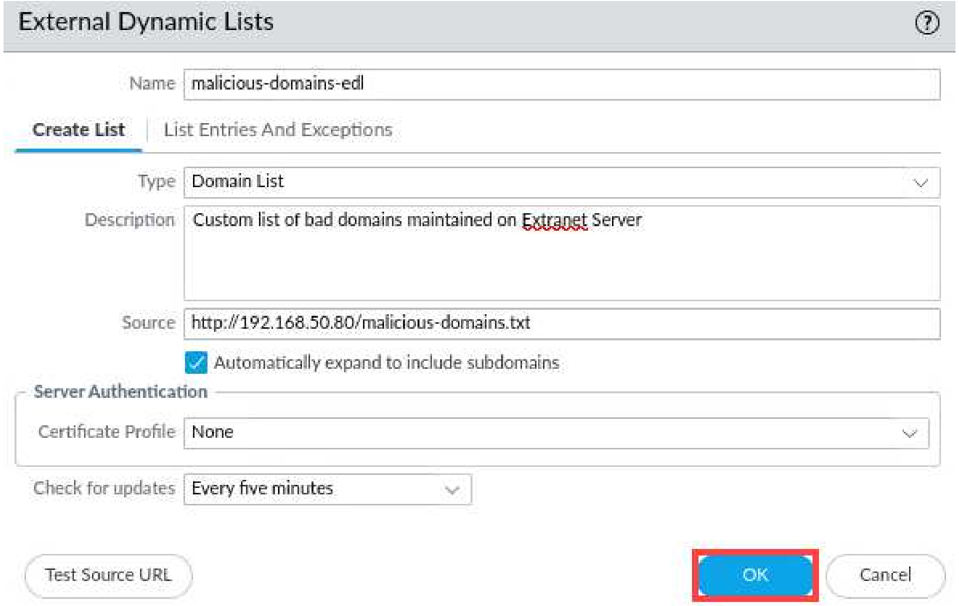
Check for updates: Every five minutes

7. A message window should open and state that the source URL is accessible. Click **Close**.


Test Source URL

Source URL is accessible.

8. Click **OK** to close the **External Dynamic Lists** window.


External Dynamic Lists

Name: malicious-domains-edl

Create List | List Entries And Exceptions

Type: Domain List

Description: Custom list of bad domains maintained on Extranet Server

Source: http://192.168.50.80/malicious-domains.txt

☑ Automatically expand to include subdomains

Server Authentication

Certificate Profile: None

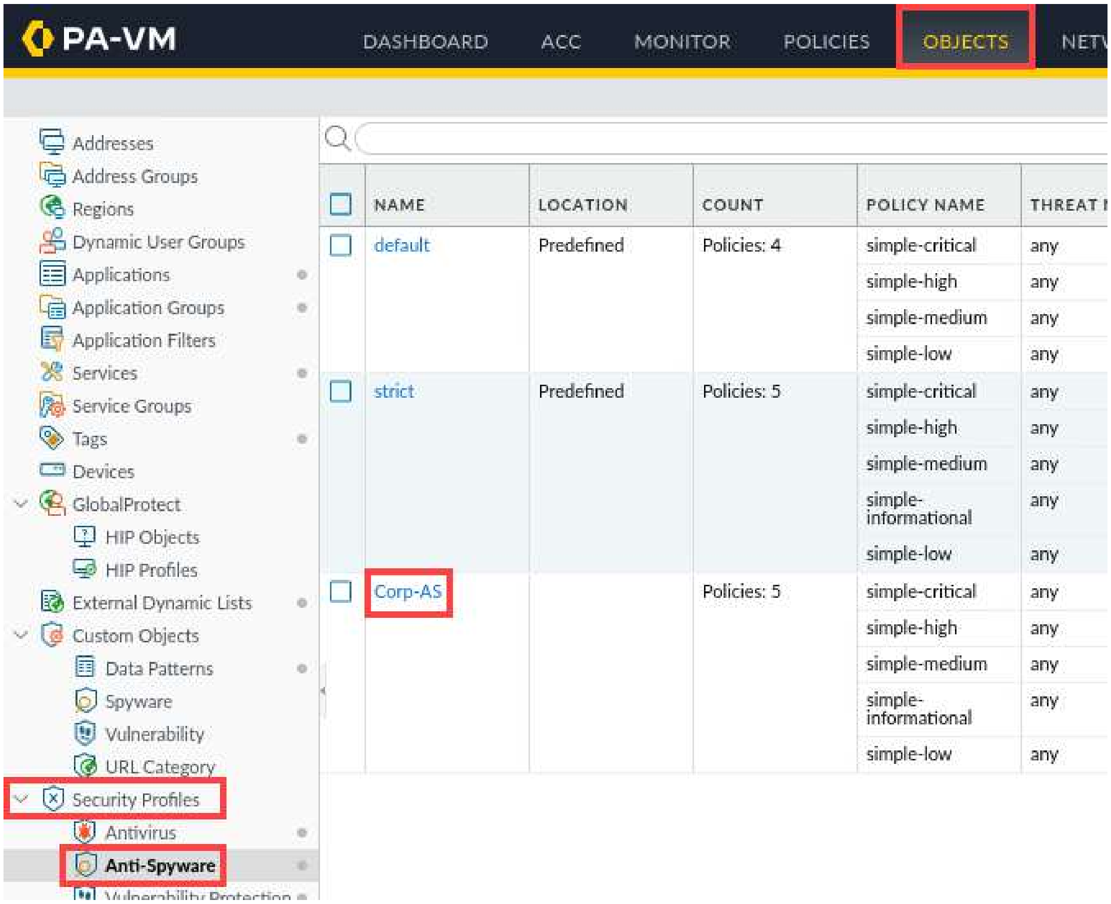
Check for updates: Every five minutes

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

2.9 Update the Anti-Spyware Profile with EDL

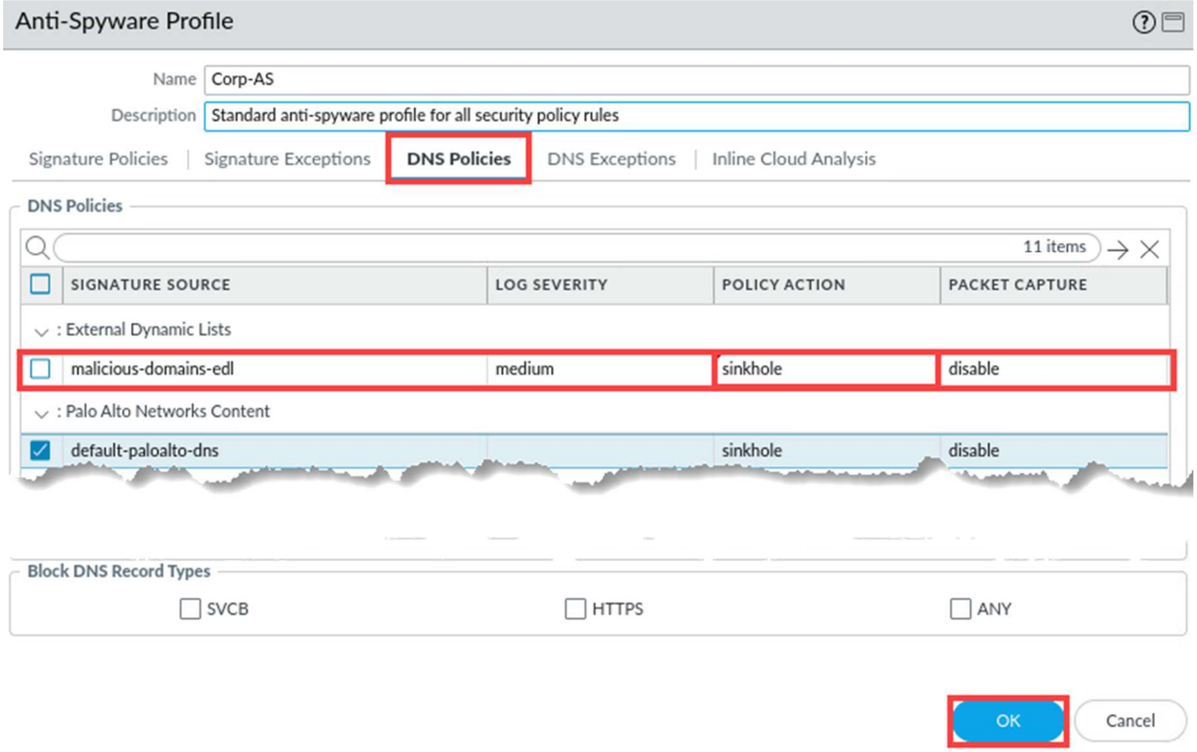
Now that you have configured the firewall with the External Dynamic List for custom malicious domains, you can update the Anti-Spyware Profile to use the list for sinkholing.

1. Select **Objects > Security Profiles > Anti-Spyware.** Click **Corp-AS** to edit the Profile.



☐	NAME	LOCATION	COUNT	POLICY NAME	THREAT N
☐	default	Predefined	Policies: 4	simple-critical	any
				simple-high	any
				simple-medium	any
				simple-low	any
☐	strict	Predefined	Policies: 5	simple-critical	any
				simple-high	any
				simple-medium	any
				simple-informational	any
				simple-low	any
☐	Corp-AS		Policies: 5	simple-critical	any
				simple-high	any
				simple-medium	any
				simple-informational	any
				simple-low	any

2. In the *Anti-Spyware Profile* window, click the **DNS Policies** tab. Under the **External Dynamic Lists** section, change the **Policy Action** drop-down list to **sinkhole** for the **malicious-domains-edl** entry. Click **OK.**



Anti-Spyware Profile

Name: Corp-AS

Description: Standard anti-spyware profile for all security policy rules

DNS Policies

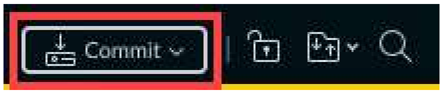
11 items

	SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
	: External Dynamic Lists			
□	malicious-domains-edl	medium	sinkhole	disable
	: Palo Alto Networks Content			
☑	default-paloalto-dns		sinkhole	disable

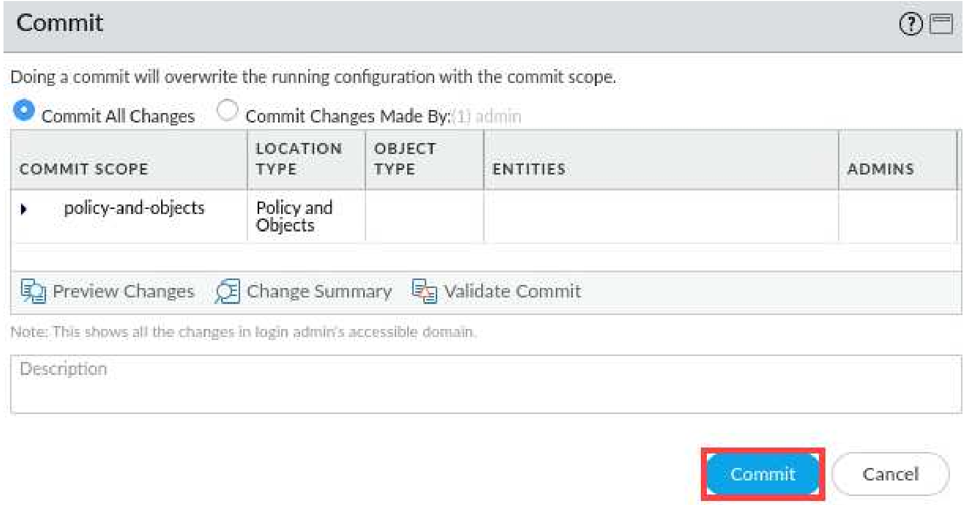
Block DNS Record Types

□ SVCB □ HTTPS □ ANY

3. Click the **Commit** button at the upper right of the web interface.



4. In the *Commit* window, click **Commit.**



Commit

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

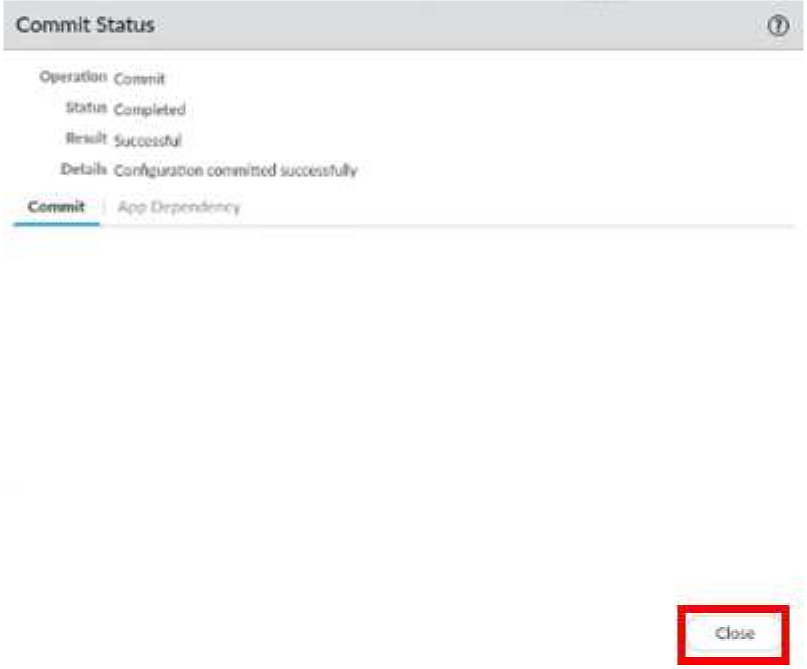
● Commit All Changes ○ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
policy-and-objects	Policy and Objects			

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

Description

5. Wait until the *Commit* process is complete. Click **Close**.



Commit Status

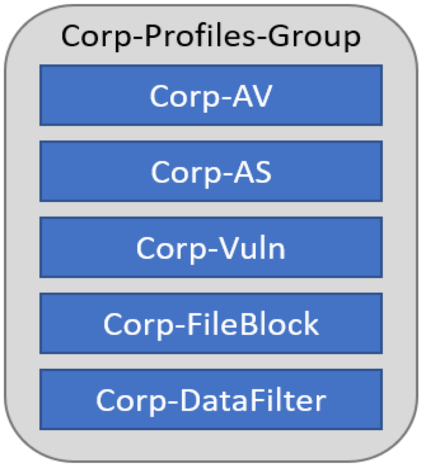
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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

2.10 Create a Security Profile Group

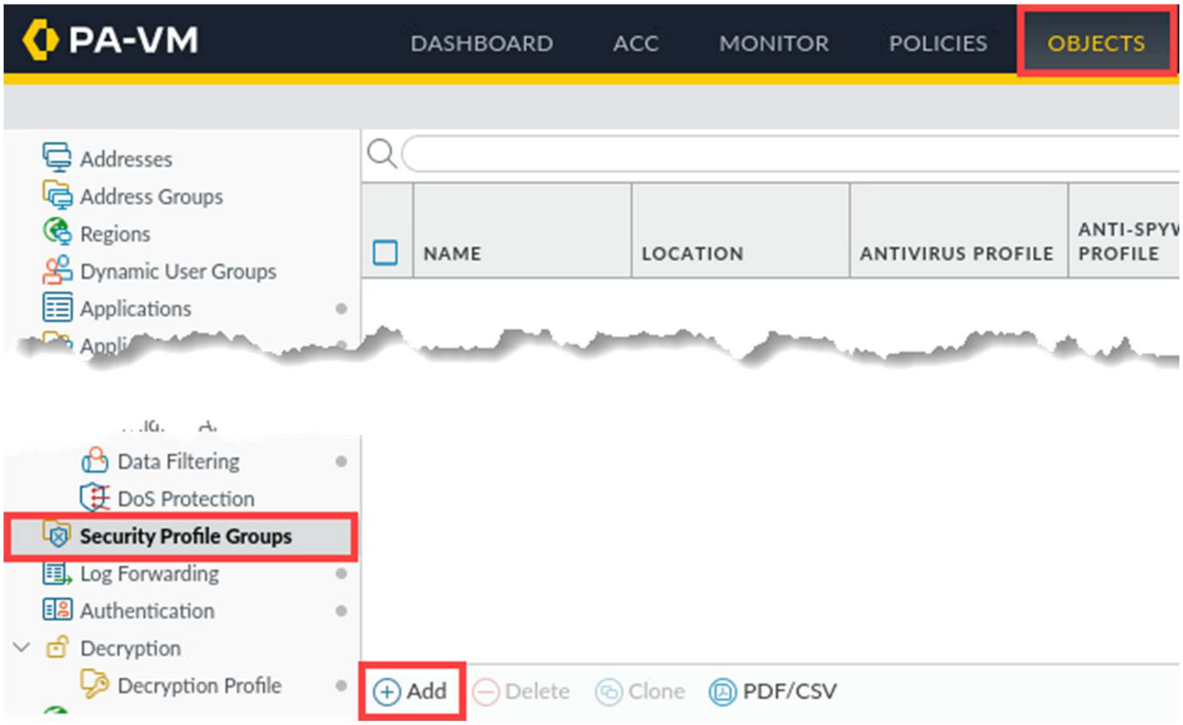
To simplify the process of applying Security Profiles to Security policy rules, you can create a Security Profile Group which contains individual Security Profiles.

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

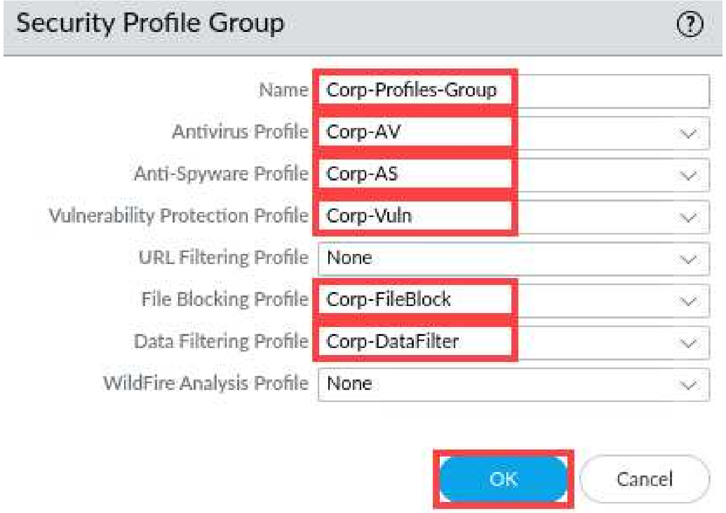


In this section, you will create a Security Profile Group called Corp-Profiles-Group. You will add each of your Corp-* Security Profiles to the group.

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



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


Security Profile Group

Name	Corp-Profiles-Group
Antivirus Profile	Corp-AV
Anti-Spyware Profile	Corp-AS
Vulnerability Protection Profile	Corp-Vuln
URL Filtering Profile	None
File Blocking Profile	Corp-FileBlock
Data Filtering Profile	Corp-DataFilter
WildFire Analysis Profile	None

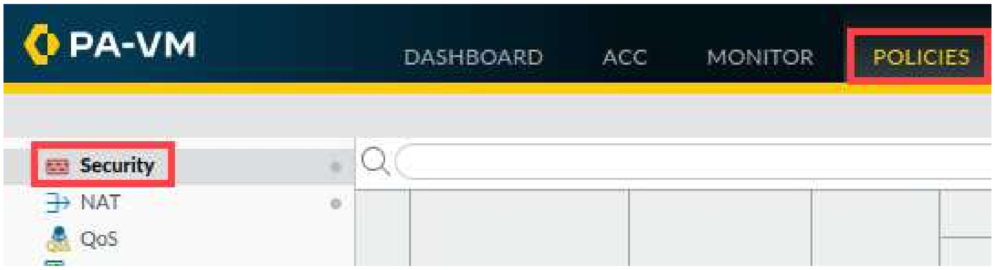
Leave the URL Filtering Profile and the WildFire Analysis Profile set to none for this lab.

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

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

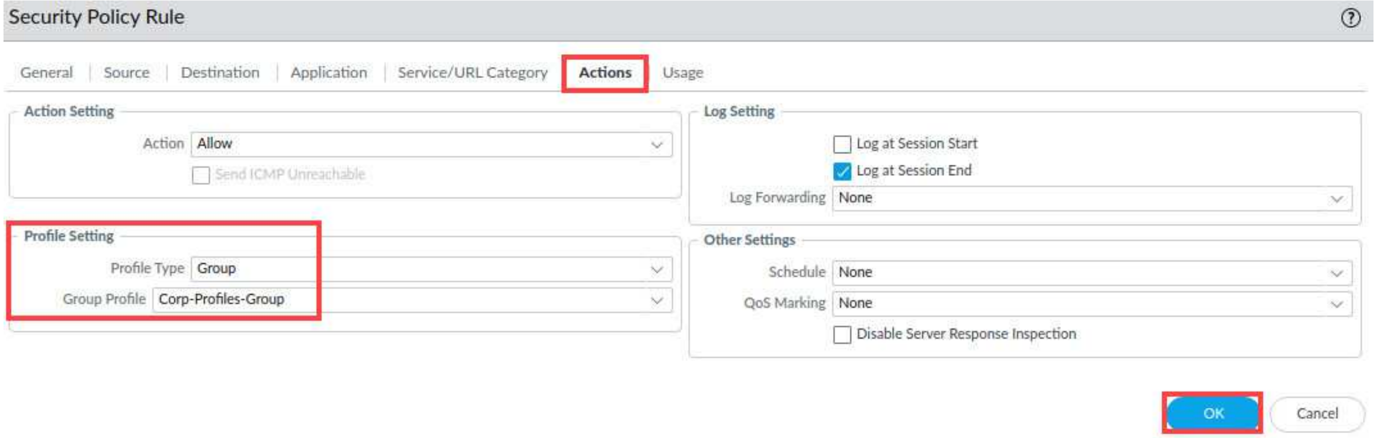
In this section, you will apply the Corp-Profiles-Group to a security policy. With the Security Profiles in place, you can modify your Security policy rules to use these protections.

1. Select **Policies > Security**.



2. Individually edit each Security Policy rule which allows traffic and change the **Profile Setting** under the **Actions** tab to use the **Corp-Profiles-Group**. Be sure to edit and modify each of these rules.

- **Allow-PANW-Apps**
- **Users_to_Extranet**
- **Users_to_Internet**
- **Extranet_to_Internet**
- **Extranet_to_User_Net**
- **Acquisition-Allow-All**



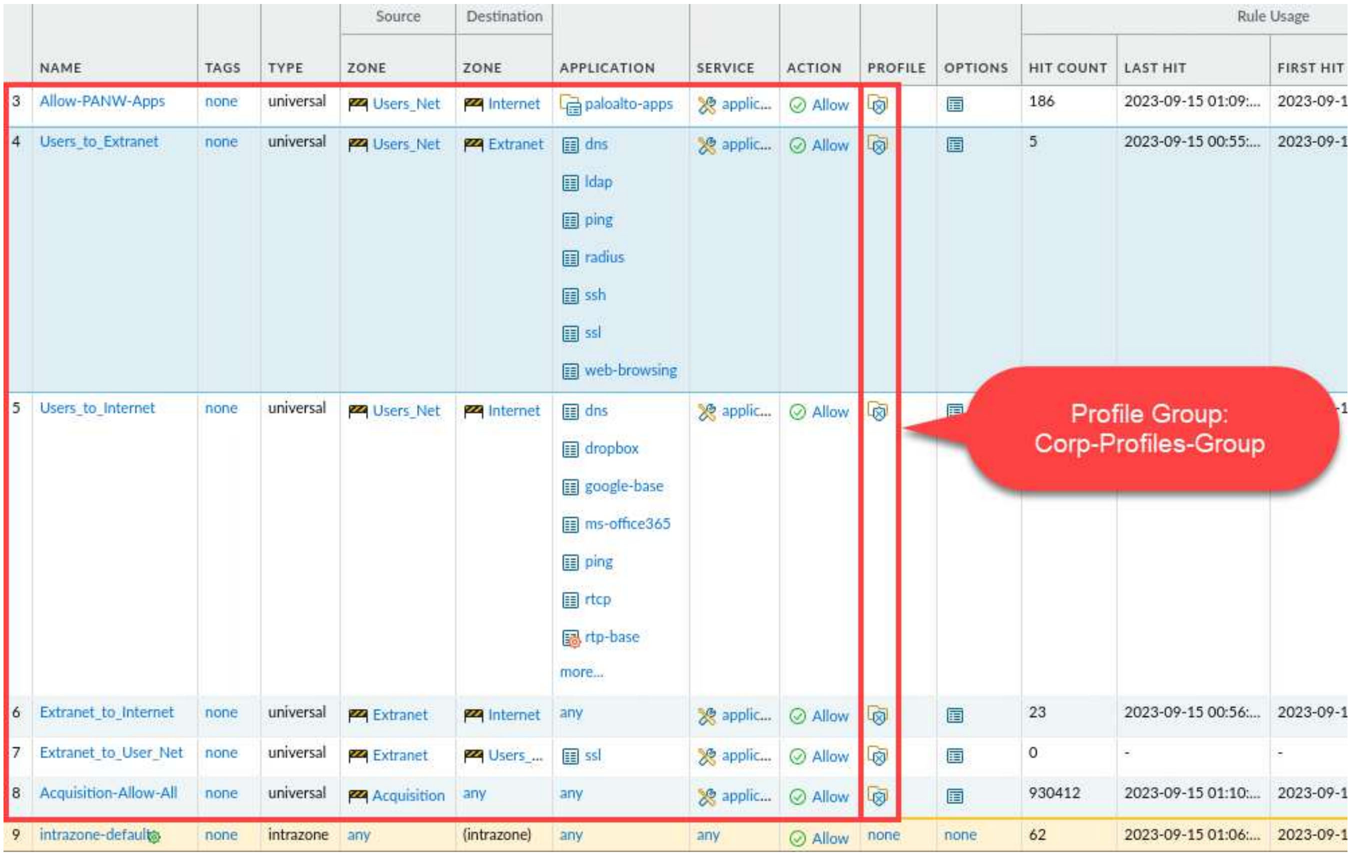
Action Setting
Action: Allow
□ Send ICMP Unreachable

Profile Setting
Profile Type: Group
Group Profile: Corp-Profiles-Group

Log Setting
□ Log at Session Start
☑ Log at Session End
Log Forwarding: None

Other Settings
Schedule: None
QoS Marking: None
□ Disable Server Response Inspection

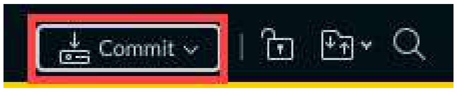
3. Verify each of the rules you modified are showing the *Corp-Profiles-Group* by hovering over the **Profile** icon for each rule.



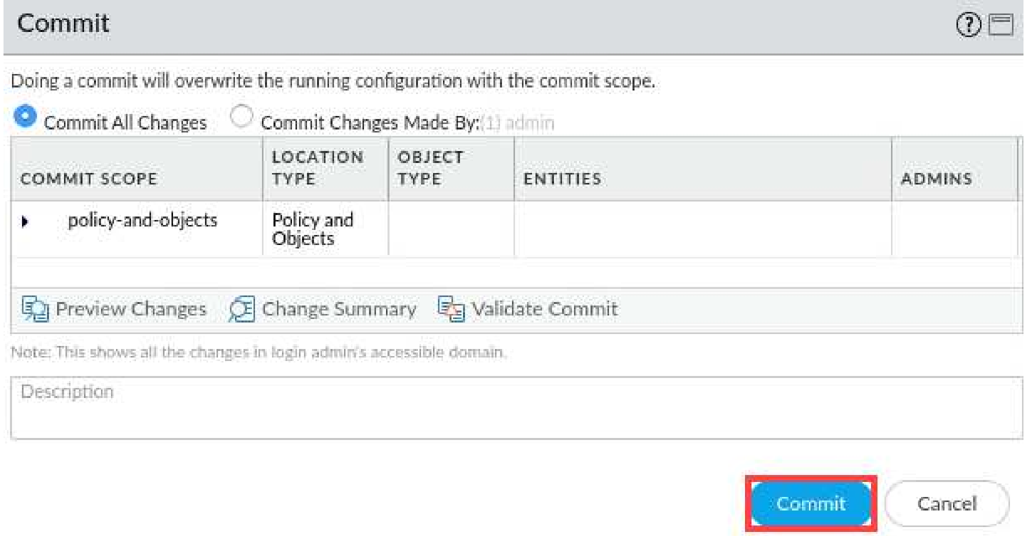
				Source	Destination						Rule Usage		
	NAME	TAGS	TYPE	ZONE	ZONE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT	LAST HIT	FIRST HIT
3	Allow-PANW-Apps	none	universal	Users_Net	Internet	paloalto-apps	applic...	Allow			186	2023-09-15 01:09:...	2023-09-1
4	Users_to_Extranet	none	universal	Users_Net	Extranet	dns ldap ping radius ssh ssl web-browsing	applic...	Allow			5	2023-09-15 00:55:...	2023-09-1
5	Users_to_Internet	none	universal	Users_Net	Internet	dns dropbox google-base ms-office365 ping rtcp rtp-base more...	applic...	Allow					-1
6	Extranet_to_Internet	none	universal	Extranet	Internet	any	applic...	Allow			23	2023-09-15 00:56:...	2023-09-1
7	Extranet_to_User_Net	none	universal	Extranet	Users_...	ssl	applic...	Allow			0	-	-
8	Acquisition-Allow-All	none	universal	Acquisition	any	any	applic...	Allow			930412	2023-09-15 01:10:...	2023-09-1
9	intrazone-default	none	intrazone	any	(intrazone)	any	any	Allow	none	none	62	2023-09-15 01:06:...	2023-09-1

Profile Group:
Corp-Profiles-Group

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	OBJECT TYPE	ENTITIES	ADMINS
policy-and-objects	Policy and Objects			

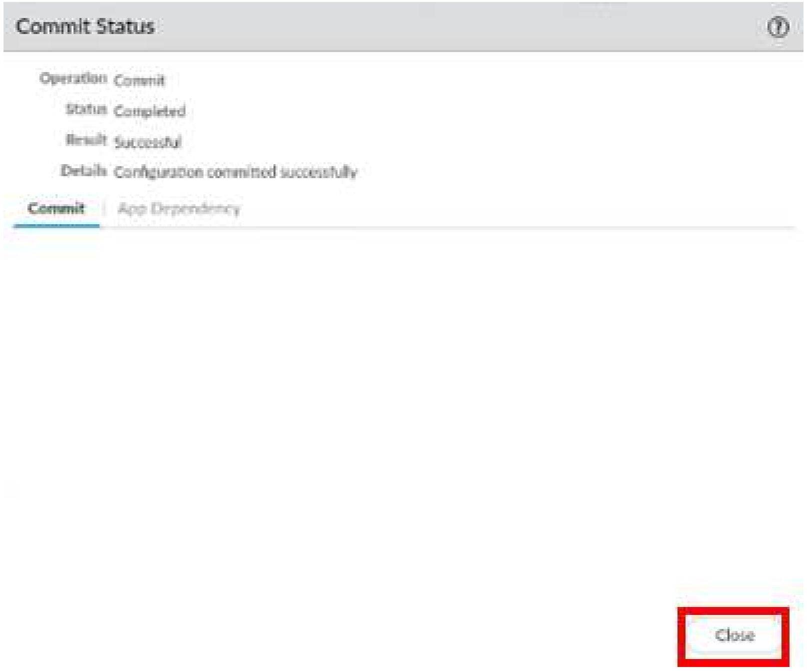
Preview Changes Change Summary Validate Commit

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.



Commit Status

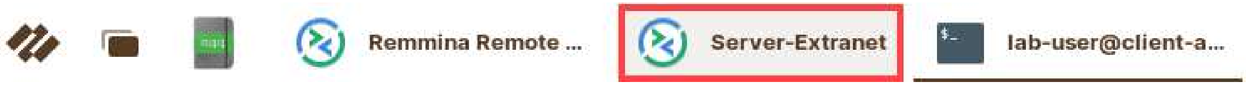
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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

2.12 Generate Attack Traffic with Security Profiles

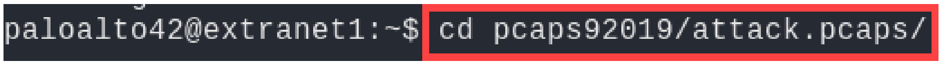
In this section, you will generate attack traffic with Security Profiles.

1. Re-open the **Remmina Server-Extranet** application by clicking the icon in the taskbar.



2. If needed, in the CLI connection enter the following command to change the working directory.

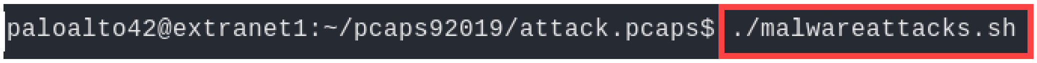
```
paloalto42@extranet1:~$ cd pcaps92019/attack.pcaps/ <Enter>
```



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

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

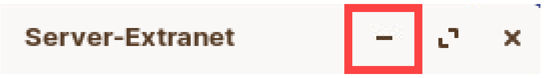
```
paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh <Enter>
```



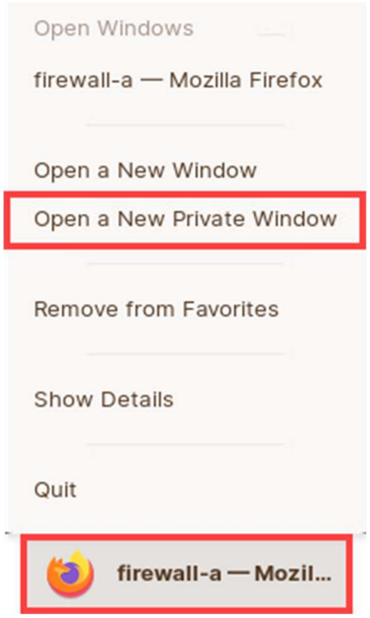
```
paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh
```

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

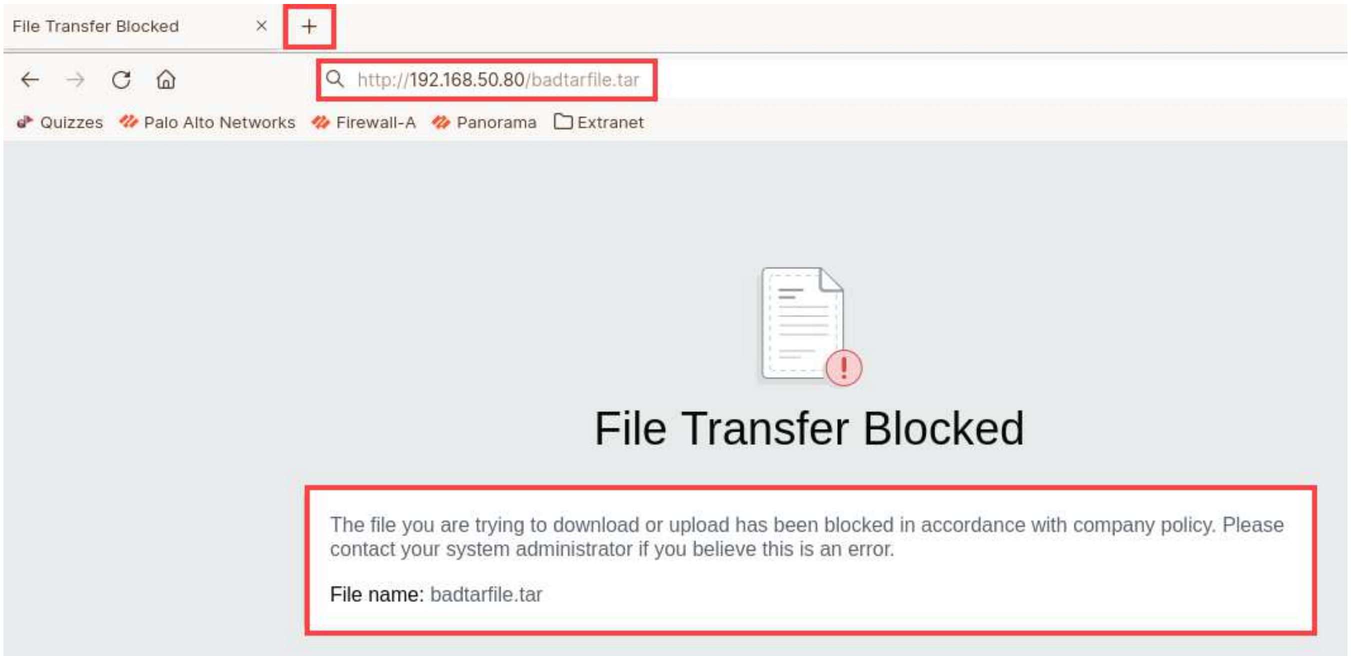
4. Minimize the *Remmina* connection window.



5. In the client taskbar, right-click the **firewall-a - Mozilla Firefox** Browser application. Select **Open a New Private Window**.



6. Type **`http://192.168.50.80/badtarfile.tar`** and press **Enter**. You should receive a **File Transfer Blocked** page from the firewall. Open a new tab in *Firefox*.



File Transfer Blocked

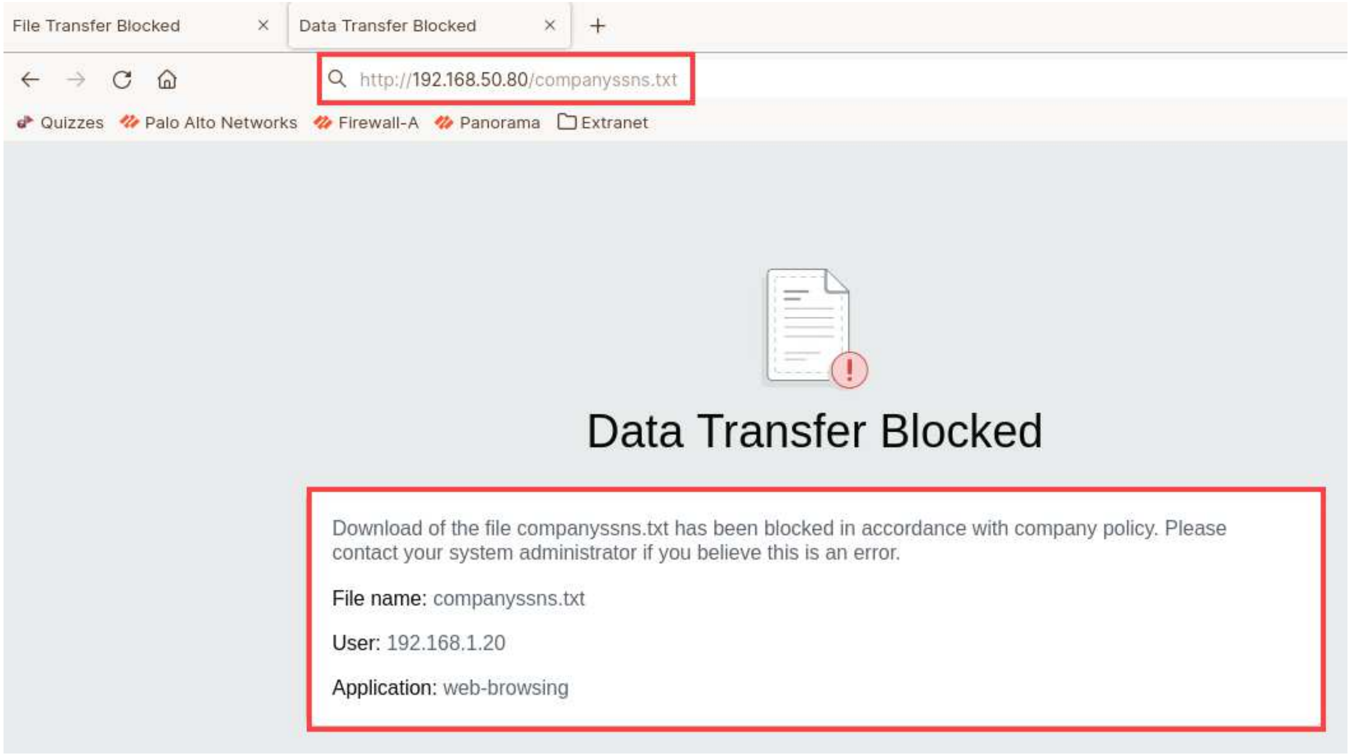
The file you are trying to download or upload has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

File name: badtarfile.tar

Please Note

This page indicates that the firewall has blocked the file using the File Blocking Profile you defined.

7. In the new *Firefox* browser tab, type **`http://192.168.50.80/companyssns.txt`**. Press **Enter.** You should receive a **Data Transfer Blocked** page from the firewall.



Data Transfer Blocked

Download of the file companyssns.txt has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

File name: companyssns.txt

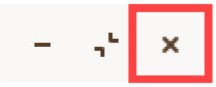
User: 192.168.1.20

Application: web-browsing

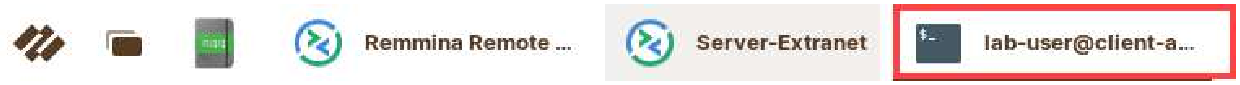
Please Note

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

8. Close the *Firefox browser*.

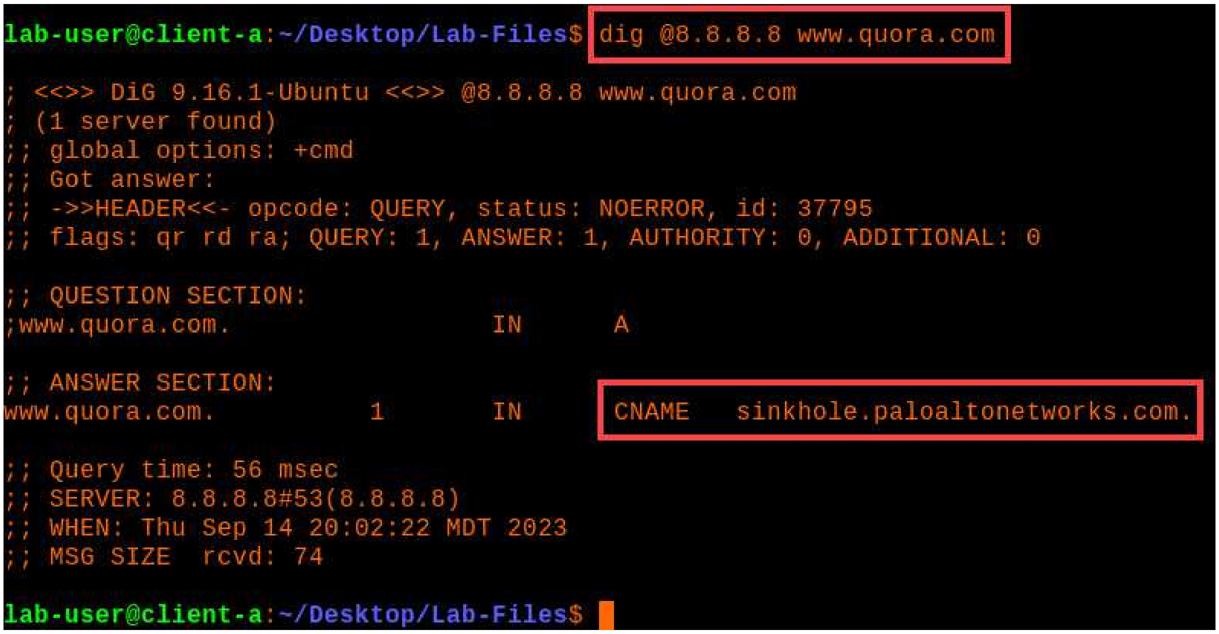


9. On the client taskbar, re-open the **lab-user@client-a** Terminal Emulator.



10. Enter the following command to generate a DNS query using **dig** to resolve a URL to an IP address. This time, the command returns **sinkhole.paloaltonetworks.com** instead of an IP address for the domain.

```
lab-user@client-a:~\Desktop\Lab-Files$ dig @8.8.8.8 www.quora.com
```

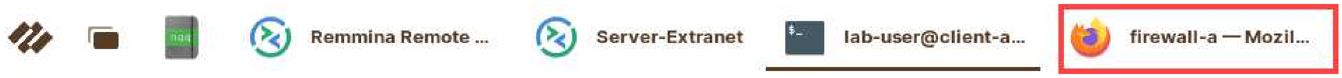


```
lab-user@client-a:~/Desktop/Lab-Files$ dig @8.8.8.8 www.quora.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 www.quora.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37795
;; 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: 56 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Sep 14 20:02:22 MDT 2023
;; MSG SIZE  rcvd: 74

lab-user@client-a:~/Desktop/Lab-Files$
```

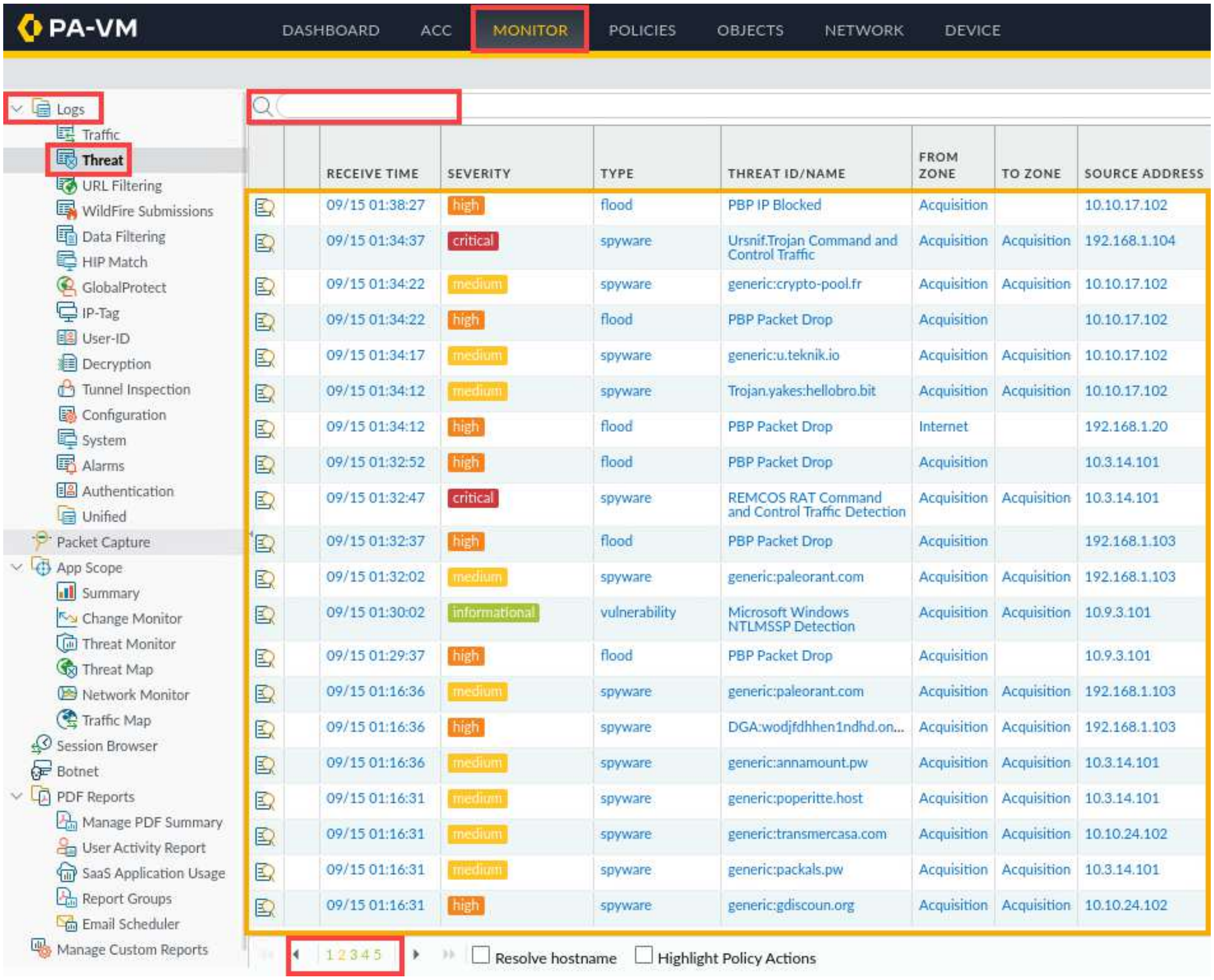
Please Note

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

11. Re-open the *PA-VM firewall* web interface by clicking on the **firewall-a – Mozilla Firefox** icon in the task bar.



12. In the firewall web interface, select **Monitor > Logs > Threat**. Clear any filters in place and press **Enter**. Scroll through the pages and notice the Threat Log will contain numerous entries for *Spyware* and *Vulnerabilities*. For the screenshot provided, notice it is on page two of the threat logs.



RECEIVE TIME	SEVERITY	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS
09/15 01:38:27	high	flood	PBP IP Blocked	Acquisition		10.10.17.102
09/15 01:34:37	critical	spyware	Ursnif.Trojan Command and Control Traffic	Acquisition	Acquisition	192.168.1.104
09/15 01:34:22	medium	spyware	generic:crypto-pool.fr	Acquisition	Acquisition	10.10.17.102
09/15 01:34:22	high	flood	PBP Packet Drop	Acquisition		10.10.17.102
09/15 01:34:17	medium	spyware	generic:u.teknik.io	Acquisition	Acquisition	10.10.17.102
09/15 01:34:12	medium	spyware	Trojan.yakes:hellobro.bit	Acquisition	Acquisition	10.10.17.102
09/15 01:34:12	high	flood	PBP Packet Drop	Internet		192.168.1.20
09/15 01:32:52	high	flood	PBP Packet Drop	Acquisition		10.3.14.101
09/15 01:32:47	critical	spyware	REMCOS RAT Command and Control Traffic Detection	Acquisition	Acquisition	10.3.14.101
09/15 01:32:37	high	flood	PBP Packet Drop	Acquisition		192.168.1.103
09/15 01:32:02	medium	spyware	generic:paleorant.com	Acquisition	Acquisition	192.168.1.103
09/15 01:30:02	informational	vulnerability	Microsoft Windows NTLMSSP Detection	Acquisition	Acquisition	10.9.3.101
09/15 01:29:37	high	flood	PBP Packet Drop	Acquisition		10.9.3.101
09/15 01:16:36	medium	spyware	generic:paleorant.com	Acquisition	Acquisition	192.168.1.103
09/15 01:16:36	high	spyware	DGA:wodjfdhhen1ndhd.on...	Acquisition	Acquisition	192.168.1.103
09/15 01:16:36	medium	spyware	generic:annamount.pw	Acquisition	Acquisition	10.3.14.101
09/15 01:16:31	medium	spyware	generic:poperitte.host	Acquisition	Acquisition	10.3.14.101
09/15 01:16:31	medium	spyware	generic:transmercasa.com	Acquisition	Acquisition	10.10.24.102
09/15 01:16:31	medium	spyware	generic:packals.pw	Acquisition	Acquisition	10.3.14.101
09/15 01:16:31	high	spyware	generic:gdiscoun.org	Acquisition	Acquisition	10.10.24.102

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.

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