SECURITY OPERATIONS FUNDAMENTALS

Lab 6: Securing Endpoints using Vulnerability Profiles

Document Version: 2021-01-29

Contents

Introduction

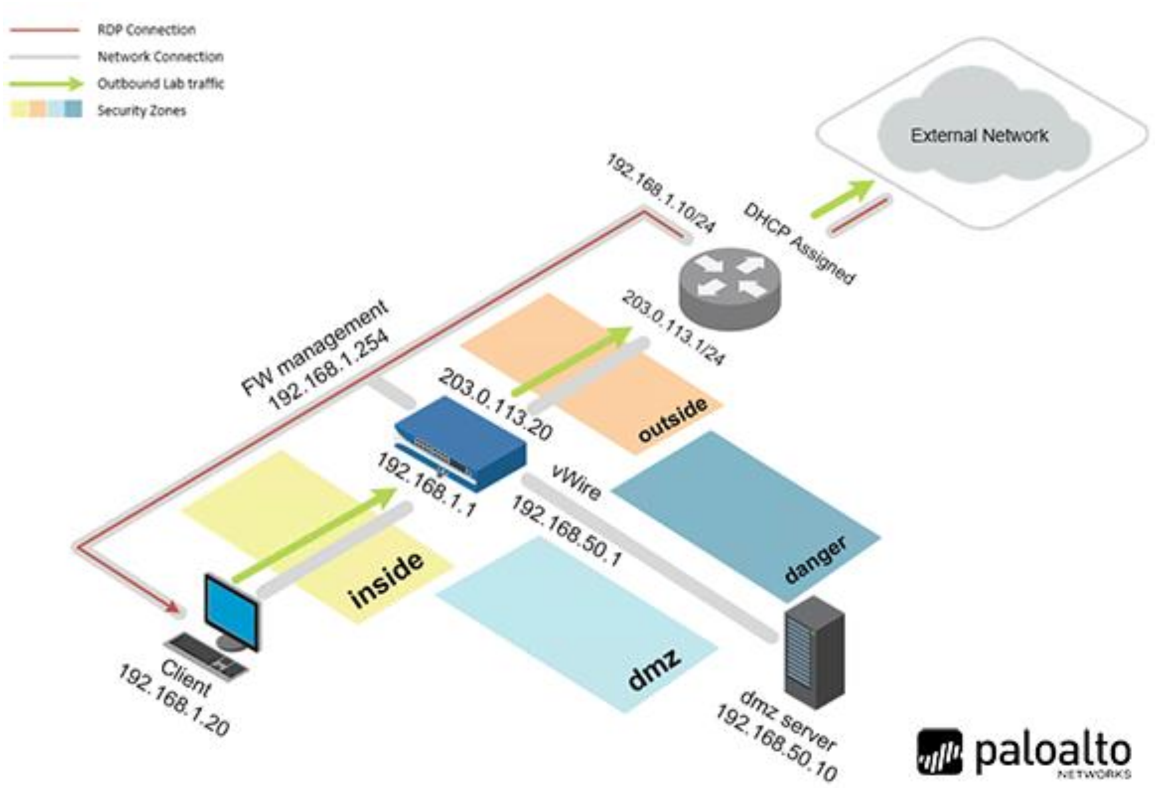
In this lab, you will secure an endpoint by blocking a PDF file with a Custom Vulnerability Object and Vulnerability Protection Profile. Palo Alto Networks Firewalls support the use of Custom Vulnerability Signatures that can be written with expression patterns to identify vulnerability exploits. Vulnerability Protection Profiles will stop any attempt to exploit system flaws so that unauthorized access cannot be gained to a targeted system.

Objective

In this lab, you will perform the following tasks:

- Install the latest Dynamic Updates of Antivirus
- Install Manual Update of Applications and Threats
- Create a Custom Vulnerability Signature
- Clone a Vulnerability Protection Profile
- Apply Custom Vulnerability Protection Profile to a Security Policy
- Commit and Test Vulnerability Protection

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.

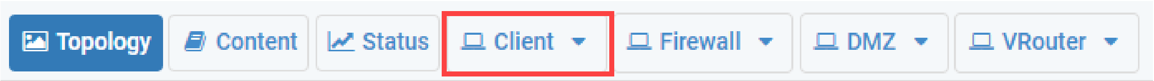
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng$

6 Securing Endpoints Using Vulnerability Profiles

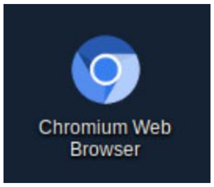
6.0 Load Lab Configuration

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

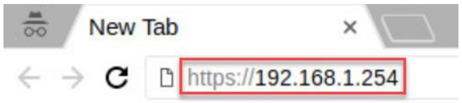
1. Click on the **Client** tab to access the client PC.



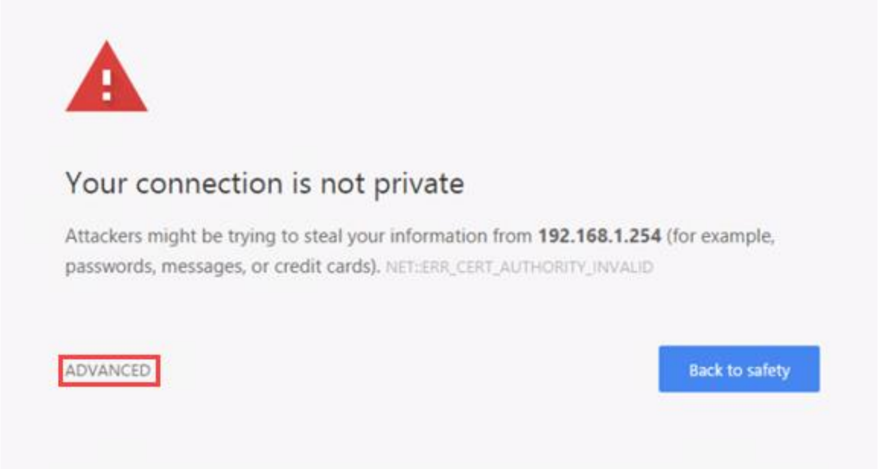
2. Log in to the client PC with username `lab-user`, password `Train1ng$`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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



5. You will see a *"Your connection is not private"* message. Click on the **ADVANCED** link.

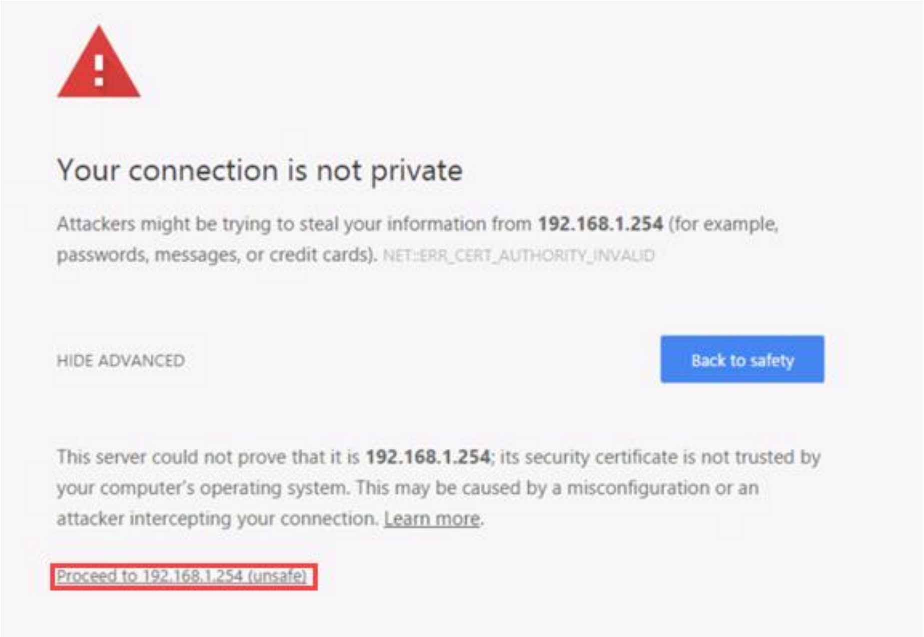


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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

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

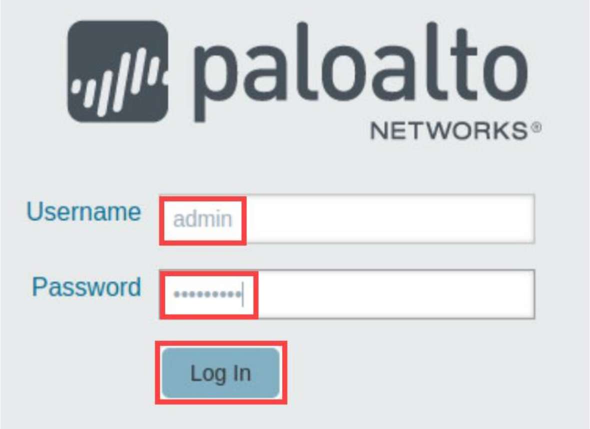


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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. Learn more.

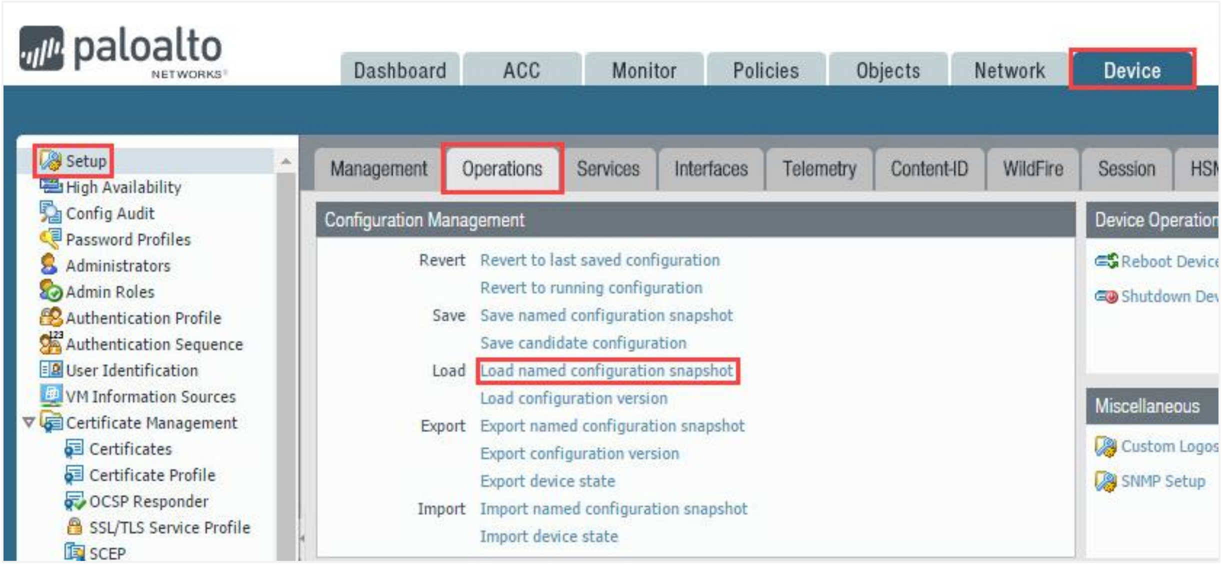
7. Log in to the Firewall web interface with username `admin`, password `Train1ng$`.



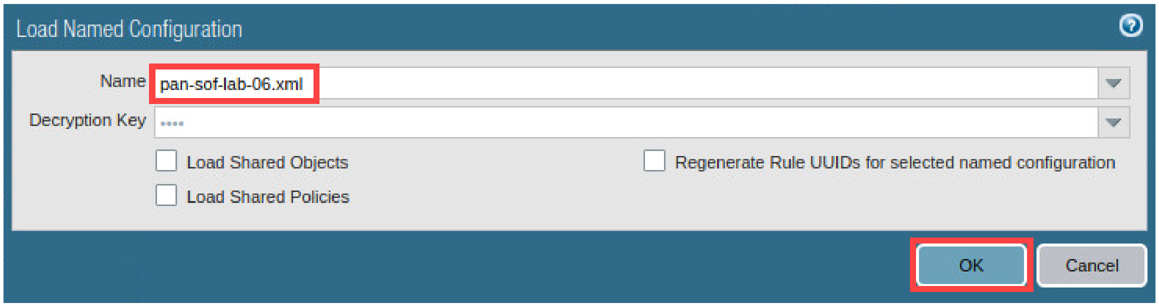
Username: admin

Password: •••••••••

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



9. In the *Load Named Configuration* window, select **pan-sof-lab-06.xml** from the *Name* dropdown box and click **OK**.


Load Named Configuration

Name pan-sof-lab-06.xml

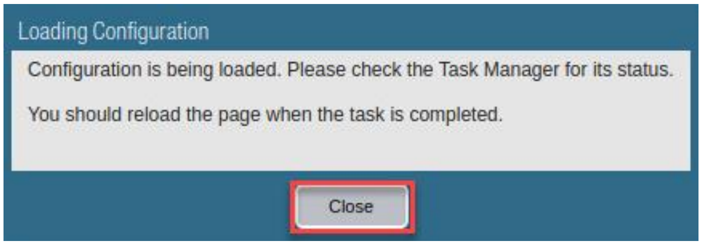
Decryption Key ••••

□ Load Shared Objects

□ Load Shared Policies

□ Regenerate Rule UUIDs for selected named configuration

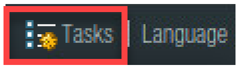
10. In the *Loading Configuration* window, a message will say *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.


Loading Configuration

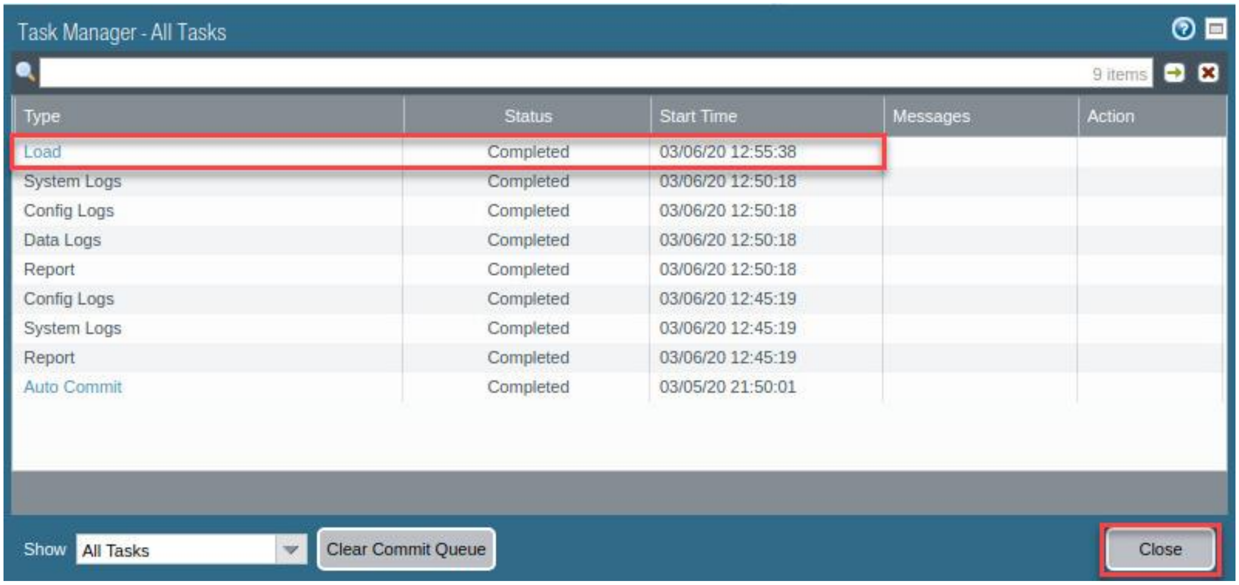
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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



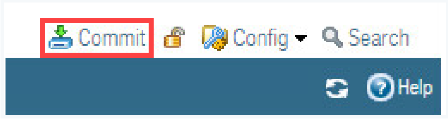
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**



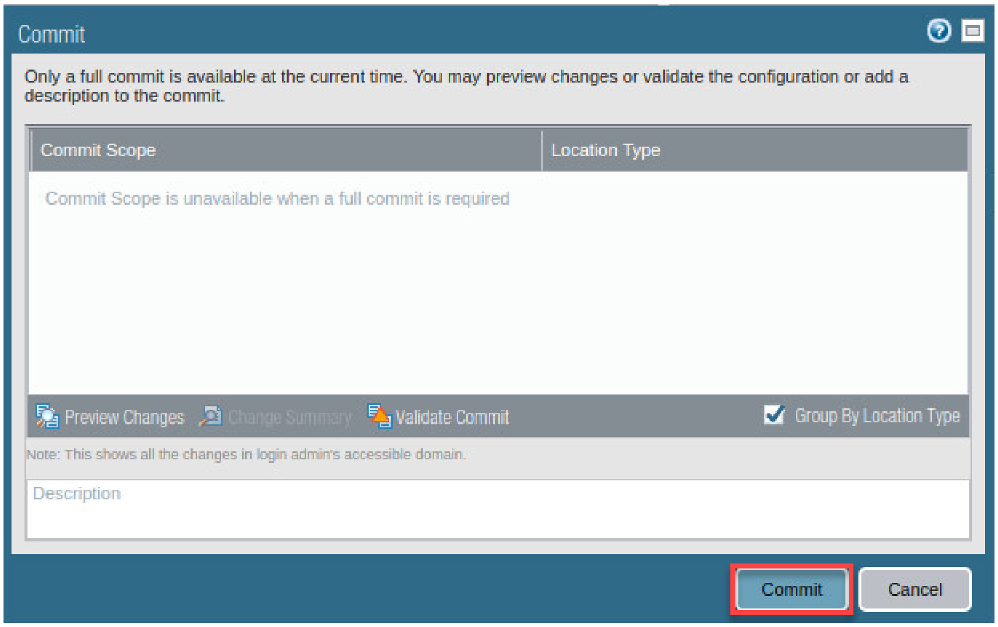
Task Manager - All Tasks

Type	Status	Start Time	Messages	Action
Load	Completed	03/06/20 12:55:38		
System Logs	Completed	03/06/20 12:50:18		
Config Logs	Completed	03/06/20 12:50:18		
Data Logs	Completed	03/06/20 12:50:18		
Report	Completed	03/06/20 12:50:18		
Config Logs	Completed	03/06/20 12:45:19		
System Logs	Completed	03/06/20 12:45:19		
Report	Completed	03/06/20 12:45:19		
Auto Commit	Completed	03/05/20 21:50:01		

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



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



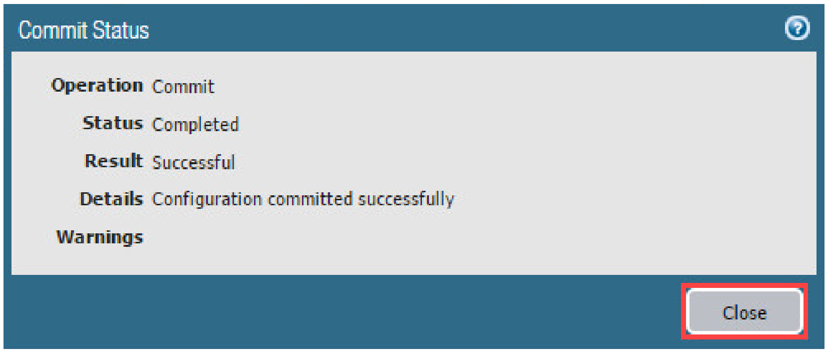
Commit

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	

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

15. When the commit operation successfully completes, click **Close** to continue.



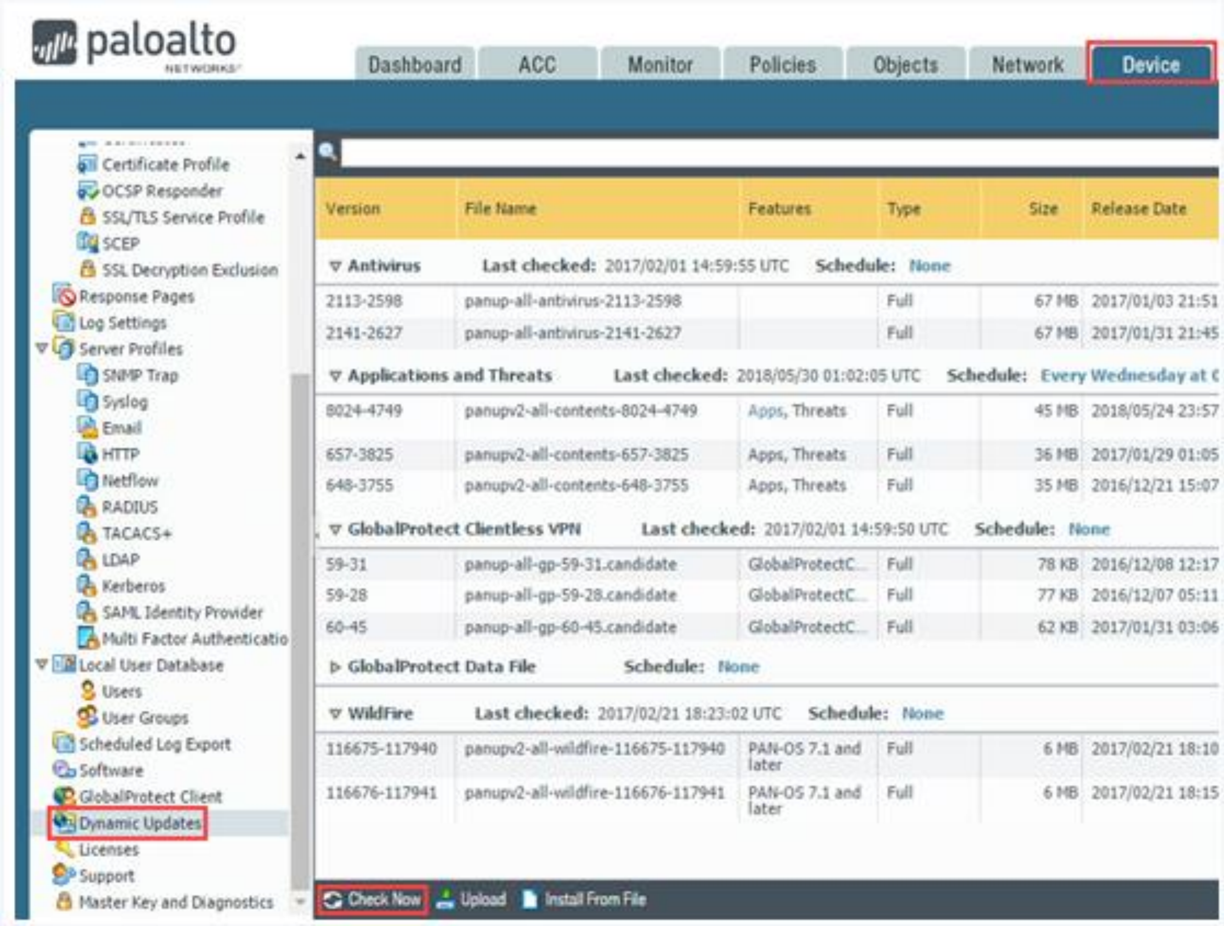
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

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.

6.1 Install the Latest Dynamic Updates of Antivirus

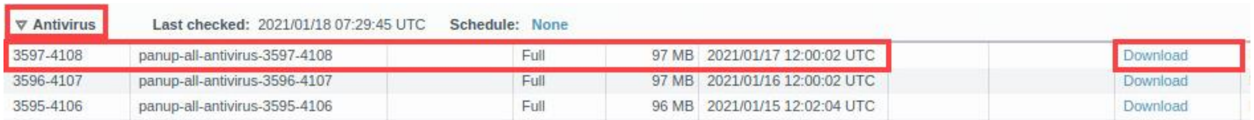
In this section, you will perform Dynamic Updates. Dynamic Updates ensure policy enforcement on a Palo Alto Networks Firewall of new threat signatures and applications**.**

1. Navigate to **Device > Dynamic Updates > Check Now**. You may need to scroll down in the left pane.



Version	File Name	Features	Type	Size	Release Date
▽ Antivirus	Last checked: 2017/02/01 14:59:55 UTC	Schedule: None			
2113-2598	panup-all-antivirus-2113-2598		Full	67 MB	2017/01/03 21:51
2141-2627	panup-all-antivirus-2141-2627		Full	67 MB	2017/01/31 21:45
▽ Applications and Threats	Last checked: 2018/05/30 01:02:05 UTC	Schedule: Every Wednesday at 0			
8024-4749	panupv2-all-contents-8024-4749	Apps, Threats	Full	45 MB	2018/05/24 23:57
657-3825	panupv2-all-contents-657-3825	Apps, Threats	Full	36 MB	2017/01/29 01:05
648-3755	panupv2-all-contents-648-3755	Apps, Threats	Full	35 MB	2016/12/21 15:07
▽ GlobalProtect Clientless VPN	Last checked: 2017/02/01 14:59:50 UTC	Schedule: None			
59-31	panup-all-gp-59-31.candidate	GlobalProtectC...	Full	78 KB	2016/12/08 12:17
59-28	panup-all-gp-59-28.candidate	GlobalProtectC...	Full	77 KB	2016/12/07 05:11
60-45	panup-all-gp-60-45.candidate	GlobalProtectC...	Full	62 KB	2017/01/31 03:06
▷ GlobalProtect Data File	Schedule: None				
▽ WildFire	Last checked: 2017/02/21 18:23:02 UTC	Schedule: None			
116675-117940	panupv2-all-wildfire-116675-117940	PAN-OS 7.1 and later	Full	6 MB	2017/02/21 18:10
116676-117941	panupv2-all-wildfire-116676-117941	PAN-OS 7.1 and later	Full	6 MB	2017/02/21 18:15

2. Under the *Antivirus* update, click **Download** on the latest update.

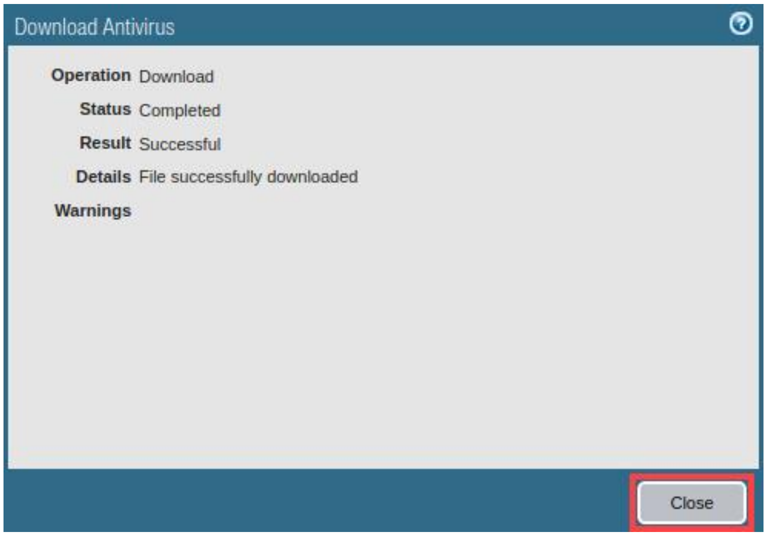


▽ Antivirus Last checked: 2021/01/18 07:29:45 UTC Schedule: None

3597-4108	panup-all-antivirus-3597-4108		Full	97 MB	2021/01/17 12:00:02 UTC	Download
3596-4107	panup-all-antivirus-3596-4107		Full	97 MB	2021/01/16 12:00:02 UTC	Download
3595-4106	panup-all-antivirus-3595-4106		Full	96 MB	2021/01/15 12:02:04 UTC	Download

This lab environment connects to a live update server. Therefore, screenshots are subject to change. Please select the latest update.

3. In the *Download Antivirus* window, after the download completes, click the **Close** button.



Download Antivirus

Operation Download

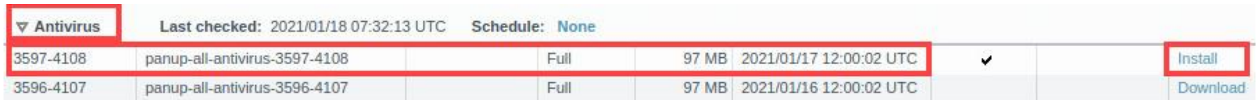
Status Completed

Result Successful

Details File successfully downloaded

Warnings

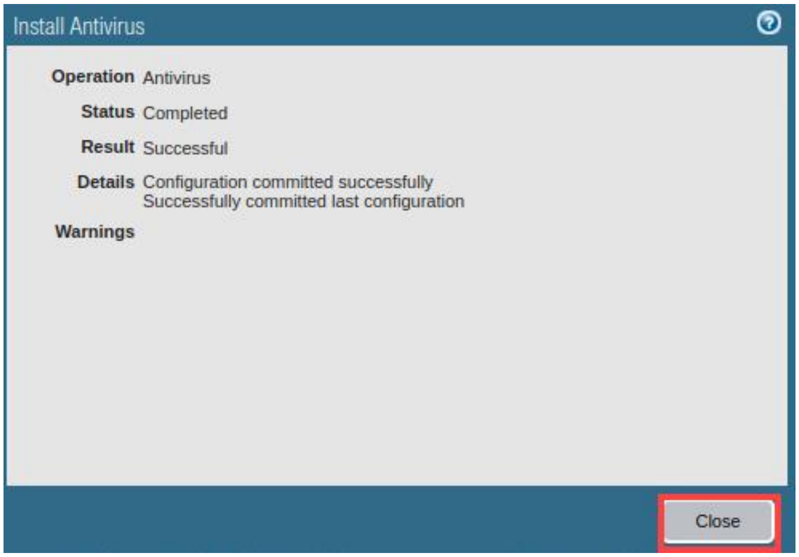
4. Under the *Antivirus* update, click **Install** on the latest update.



▽ Antivirus Last checked: 2021/01/18 07:32:13 UTC Schedule: None

3597-4108	panup-all-antivirus-3597-4108		Full	97 MB	2021/01/17 12:00:02 UTC	✓		Install
3596-4107	panup-all-antivirus-3596-4107		Full	97 MB	2021/01/16 12:00:02 UTC			Download

5. In the *Install Antivirus* window, after the update is successfully installed, click the **Close** button.



Install Antivirus

Operation Antivirus

Status Completed

Result Successful

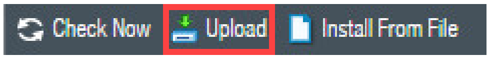
Details Configuration committed successfully
Successfully committed last configuration

Warnings

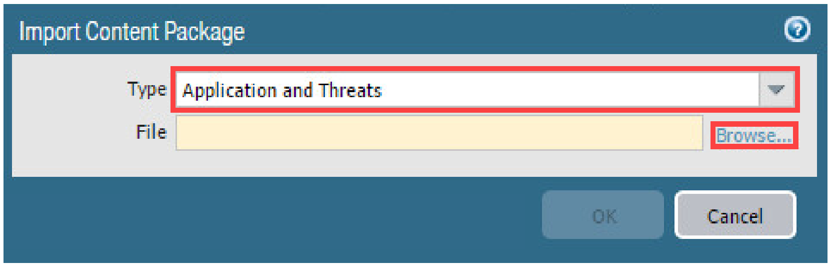
6.2 Install Manual Update of Applications and Threats

In this section, you will perform a Manual Update. There are times when the Firewall may not have Internet access to perform a Dynamic Update. Applications and Threats will be updated via a file that has been downloaded from the Palo Alto Networks Customer Support Portal.

1. To upload the file from the Customer Support Portal, click on the **Upload** button at the bottom.

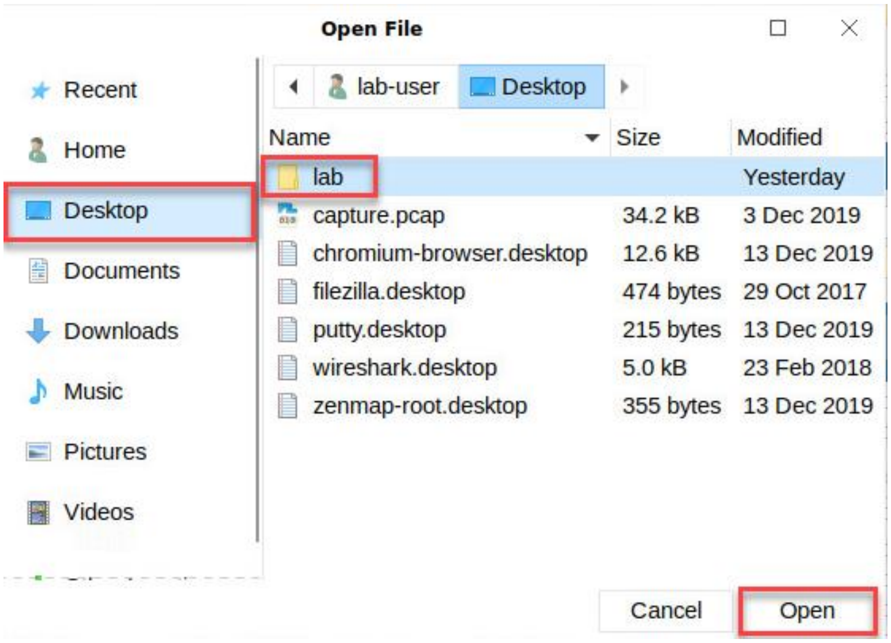


2. In the *Import Content Package* window, select **Application and Threats** from the *Type* dropdown. Then, click on **Browse…**



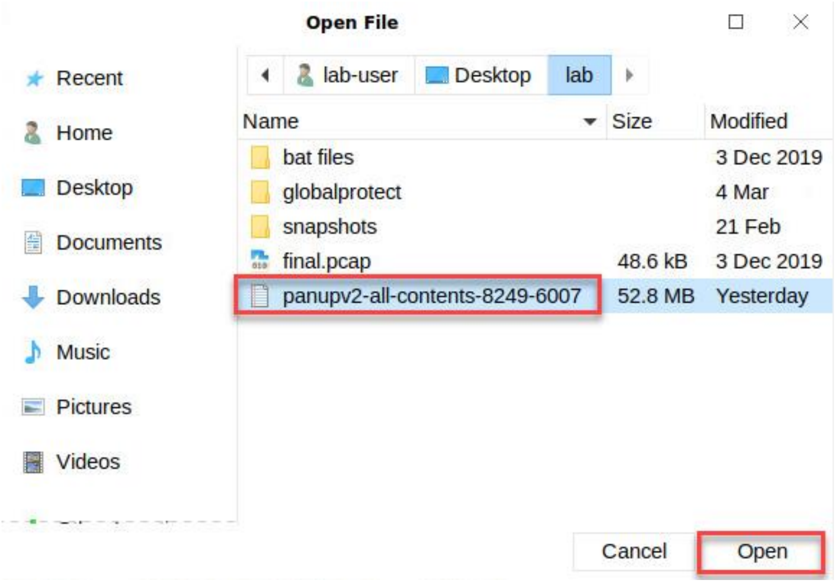
Type: Application and Threats
File:

3. In the *Open File* window, select **Desktop**, and click the **lab** folder. Lastly, click **Open**.



Name	Size	Modified
lab		Yesterday
capture.pcap	34.2 kB	3 Dec 2019
chromium-browser.desktop	12.6 kB	13 Dec 2019
filezilla.desktop	474 bytes	29 Oct 2017
putty.desktop	215 bytes	13 Dec 2019
wireshark.desktop	5.0 kB	23 Feb 2018
zenmap-root.desktop	355 bytes	13 Dec 2019

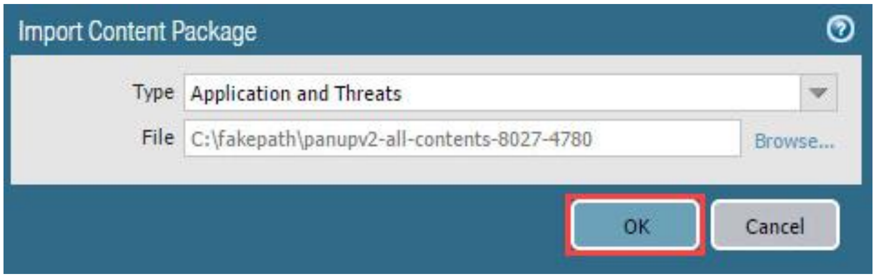
4. Click on the **panupv2-all-contents-8249-6007** file. Lastly, click **Open**.



Open File

Name	Size	Modified
bat files		3 Dec 2019
globalprotect		4 Mar
snapshots		21 Feb
final.pcap	48.6 kB	3 Dec 2019
panupv2-all-contents-8249-6007	52.8 MB	Yesterday

5. In the *Import Content Package* window, click on the **OK** button.



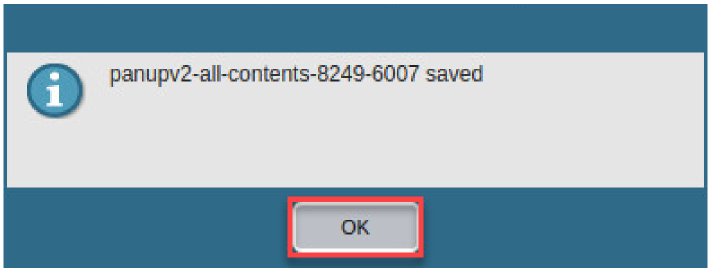
Import Content Package

Type: Application and Threats

File: C:\fakepath\panupv2-all-contents-8027-4780

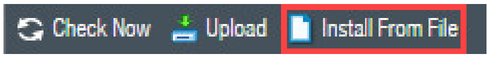
This may take several minutes to complete.

6. When completed, click on the **OK** button.

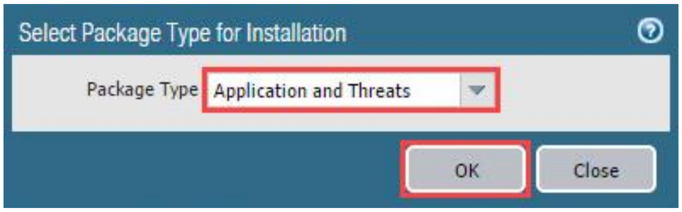


panupv2-all-contents-8249-6007 saved

7. With the file uploaded, you can begin the install. Click on **Install From File** at the bottom.

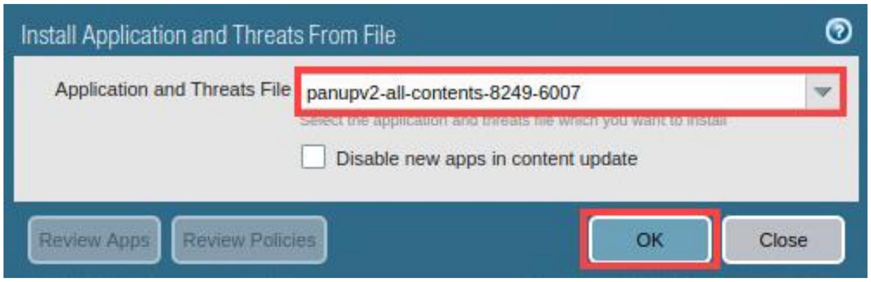


8. In the *Select Package Type for Installation* window, select **Application and Threats** from the *Package Type* dropdown. Then, click on the **OK** button.



Package Type: Application and Threats

9. In the *Install Application and Threats From File* window, select **panupv2-all-contents-8249-6007** from the *Application and Threats File* dropdown. Then, click on the **OK** button.



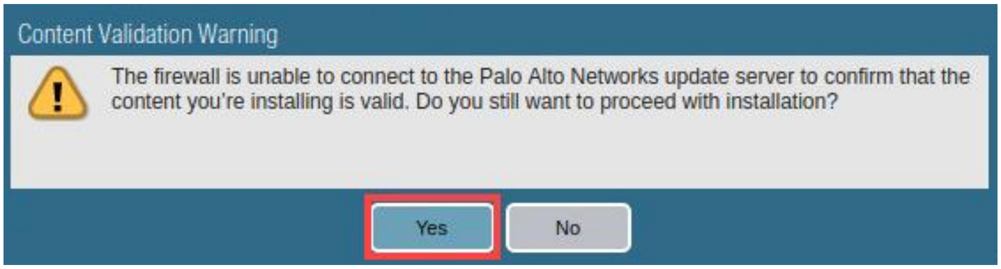
Application and Threats File: panupv2-all-contents-8249-6007

Select the application and threats file which you want to install

□ Disable new apps in content update

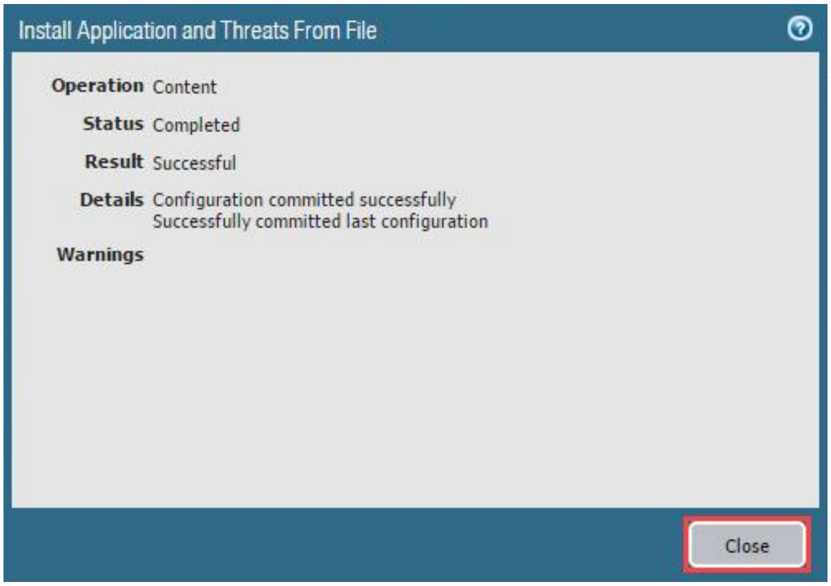
For the purpose of this lab, you will be manually installing the **Application and Threats** from a file already downloaded on the client machine. Normally you would download and install any updates from Palo Alto Networks via *Check Now*. Using *Check Now* retrieves the latest updates from Palo Alto Networks live update server.

10. If you see a *Content Validation Warning* window popup, please click the **Yes** button to proceed.



The firewall is unable to connect to the Palo Alto Networks update server to confirm that the content you're installing is valid. Do you still want to proceed with installation?

11. In the *Install Application and Threats From File* window, click on the **Close** button.



Operation Content

Status Completed

Result Successful

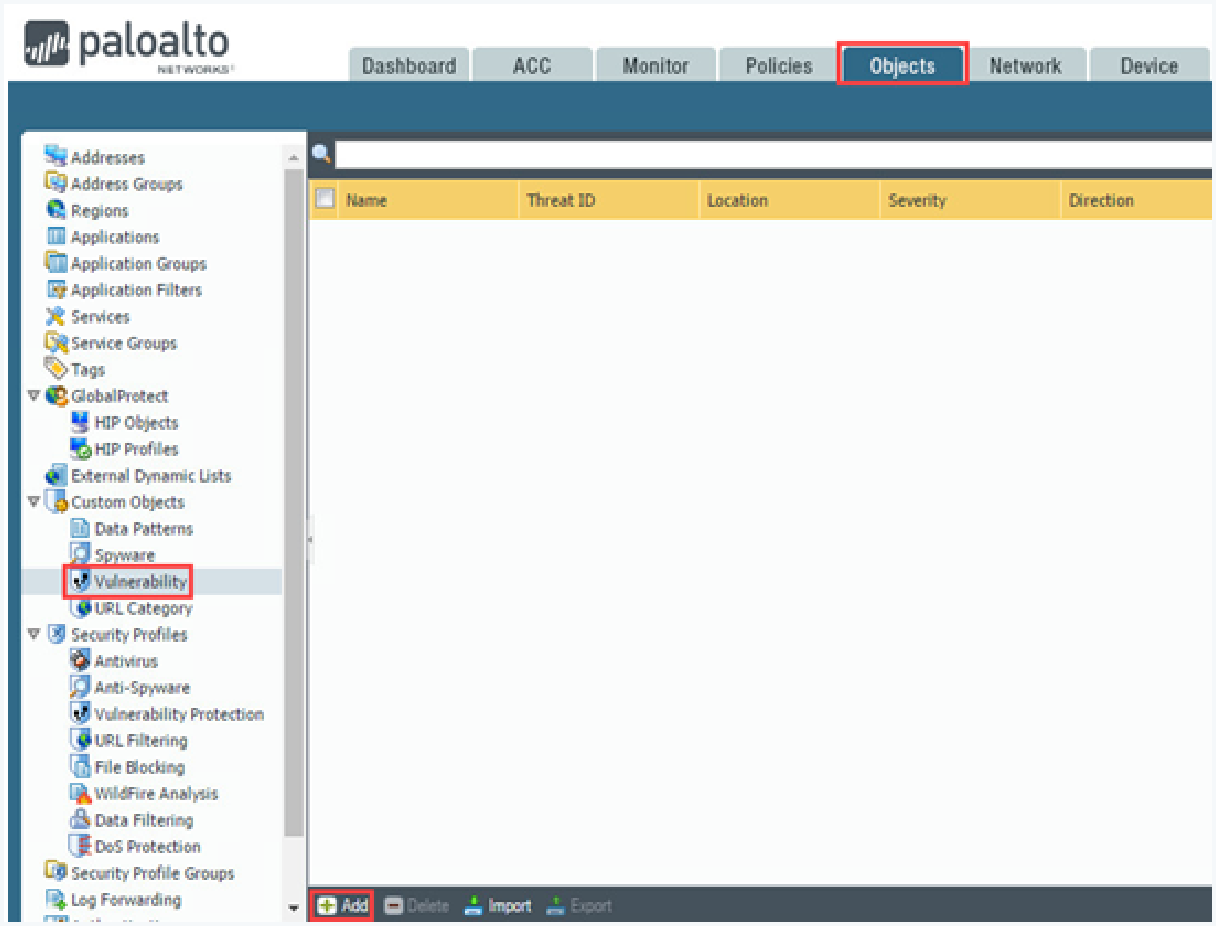
Details Configuration committed successfully
Successfully committed last configuration

Warnings

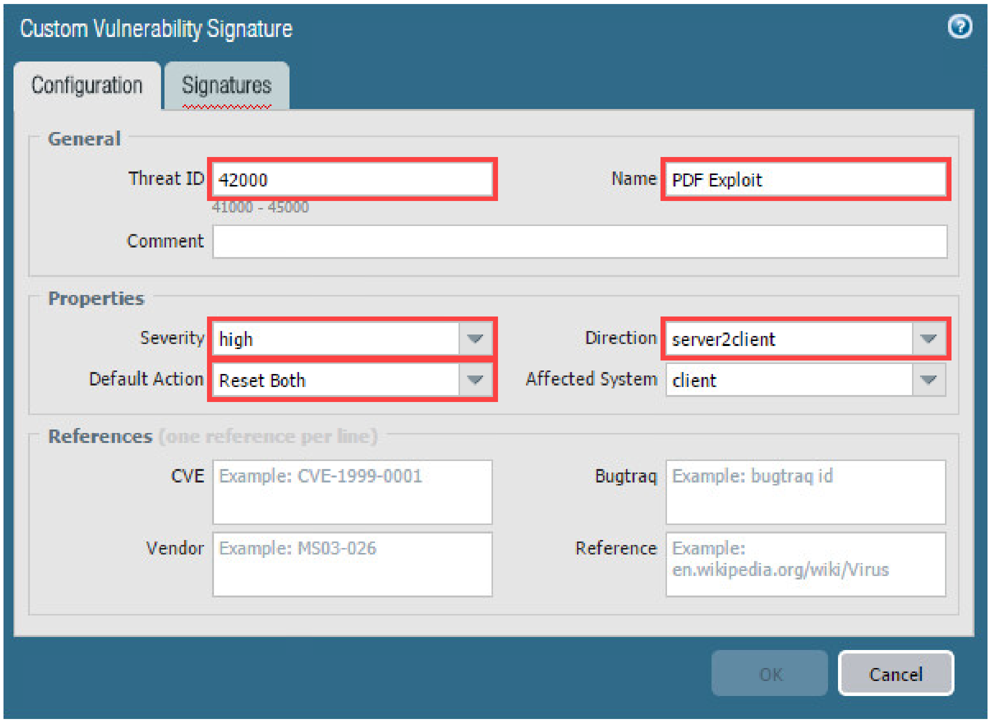
6.3 Create a Custom Vulnerability Signature

In this section, you will create a Custom Vulnerability Signature. Palo Alto Network Firewalls use Custom Vulnerability Signatures to identify vulnerability exploits by writing a custom regular expression. The Firewall then looks for the custom-defined pattern within the network traffic and takes the necessary action to identify and stop the vulnerability exploit.

1. Navigate to **Objects > Custom Objects > Vulnerability > Add**.



2. In the *Custom Vulnerability Signature* window, type `42000` in the *Threat ID* field. Then, type `PDF Exploit` in the *Name* field. Next, select **high** from the *Severity* dropdown. Then, select **server2client** from the *Direction* dropdown. Finally, select **Reset Both** from the *Default Action* dropdown.



General

Threat ID: 42000 (41000 - 45000)

Name: PDF Exploit

Comment:

Properties

Severity: high

Direction: server2client

Default Action: Reset Both

Affected System: client

References (one reference per line)

CVE: Example: CVE-1999-0001

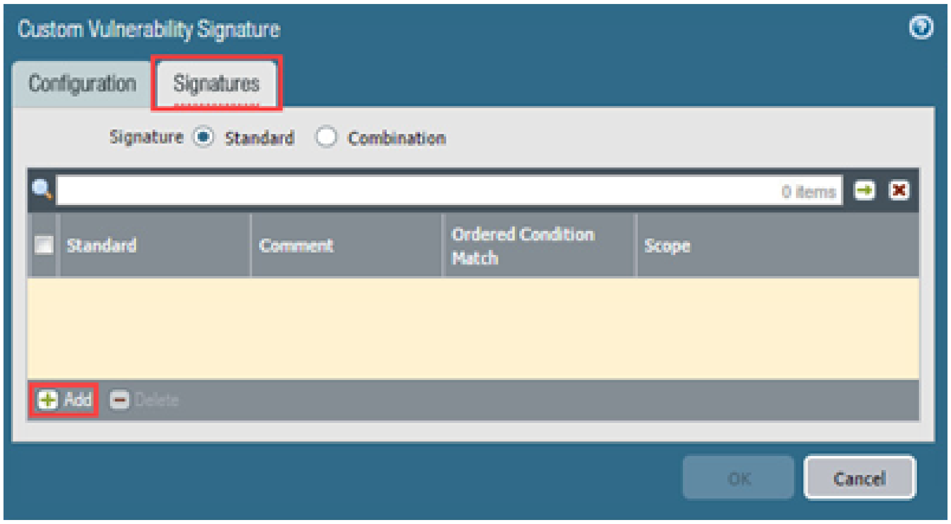
Bugtraq: Example: bugtraq id

Vendor: Example: MS03-026

Reference: Example: en.wikipedia.org/wiki/Virus

The Default Action, **Reset Both**, will be triggered when a match is detected to this Vulnerability Signature. For TCP, this will reset the connections on both the client and server ends. For UDP, the connection is dropped. This will effectively stop the traffic.

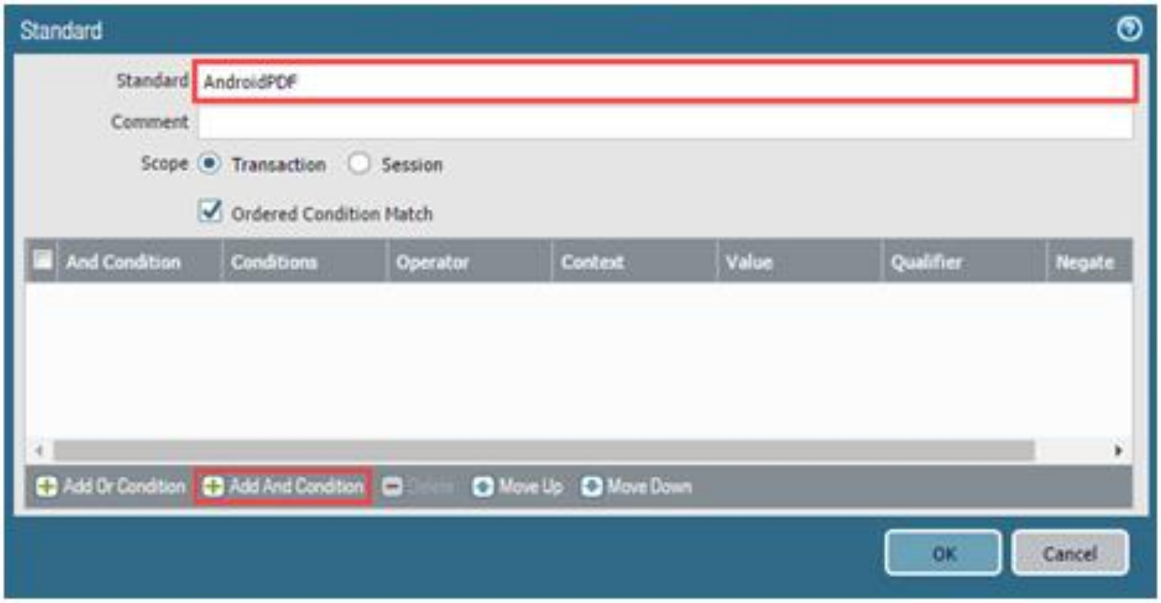
3. In the *Custom Vulnerability Signature* window, click on the **Signatures** tab. Then, click the **Add** button.



Signature ● Standard ○ Combination

□	Standard	Comment	Ordered Condition Match	Scope

4. In the *Standard* window box, type `AndroidPDF` in the *Standard* field. Then**,** click **Add And Condition**.



Standard

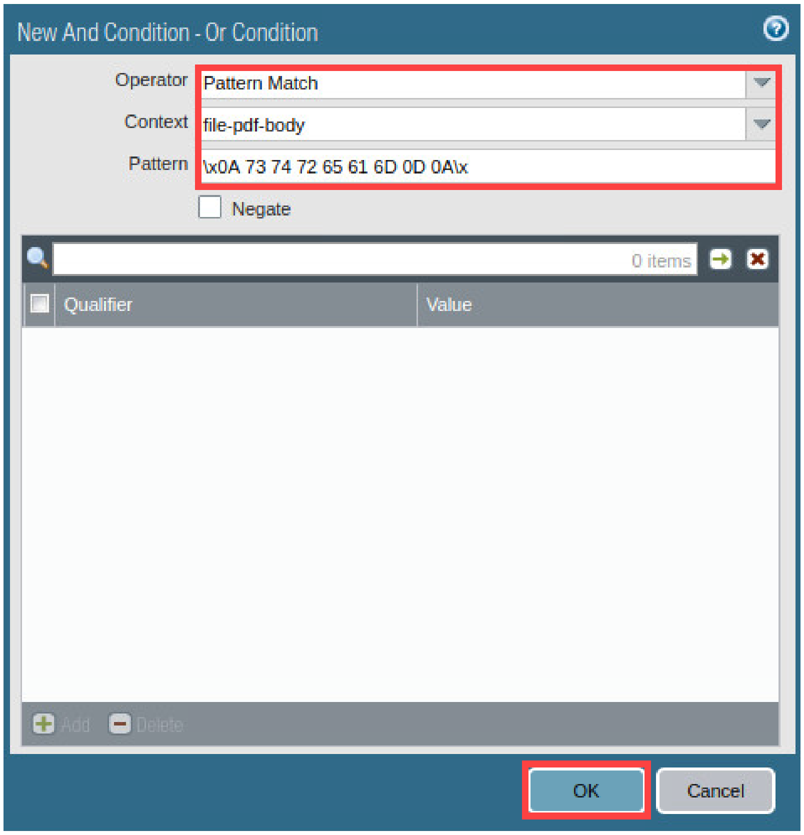
Standard: AndroidPDF

Comment:

Scope: ● Transaction ○ Session

☑ Ordered Condition Match

5. In the *New And Condition – Or Condition* window, select **Pattern Match** from the *Operator* dropdown. Then, select **file-pdf-body** from the *Context* dropdown. Next, type `\x0A 73 74 72 65 61 6D 0D 0A\x` in the *Pattern* field. Finally, click the **OK** button.



New And Condition - Or Condition

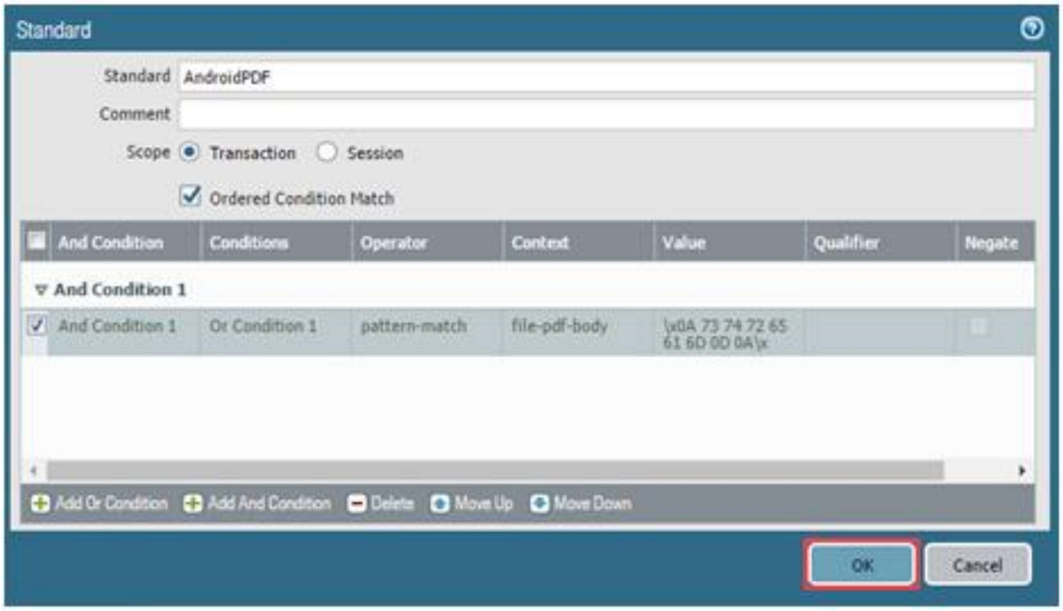
Operator: Pattern Match

Context: file-pdf-body

Pattern: \x0A 73 74 72 65 61 6D 0D 0A\x

□ Negate

6. In the *Standard* window, click the **OK** button.



Standard

Standard: AndroidPDF

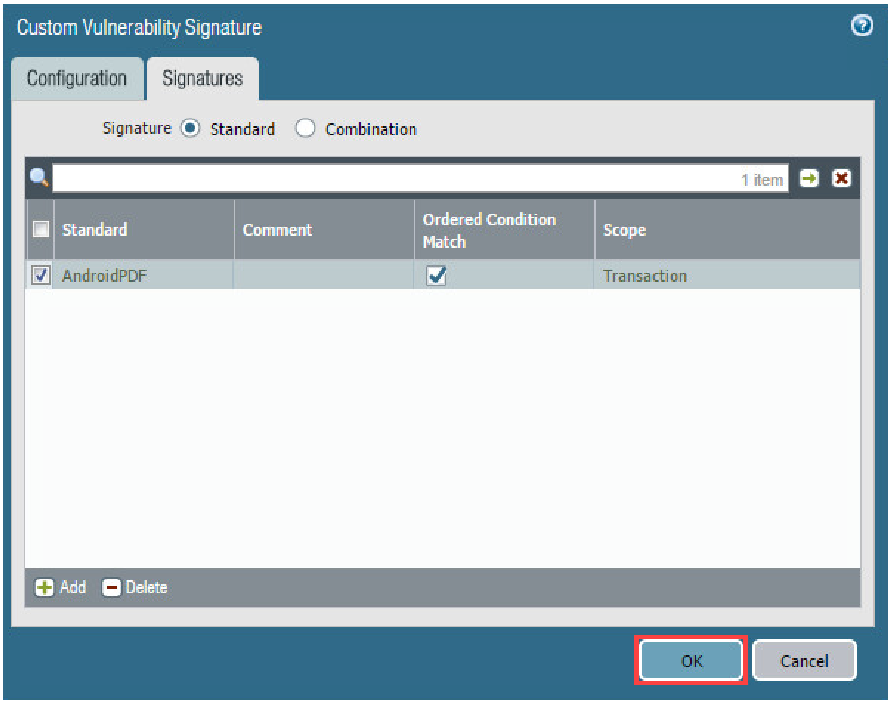
Comment:

Scope: ● Transaction ○ Session

☑ Ordered Condition Match

□	And Condition	Conditions	Operator	Context	Value	Qualifier	Negate
	▿ And Condition 1						
☑	And Condition 1	Or Condition 1	pattern-match	file-pdf-body	\x0A 73 74 72 65 61 6D 0D 0A\x		□

7. In the *Custom Vulnerability Signature* window, click the **OK** button.



Custom Vulnerability Signature

Configuration | Signatures

Signature: ● Standard ○ Combination

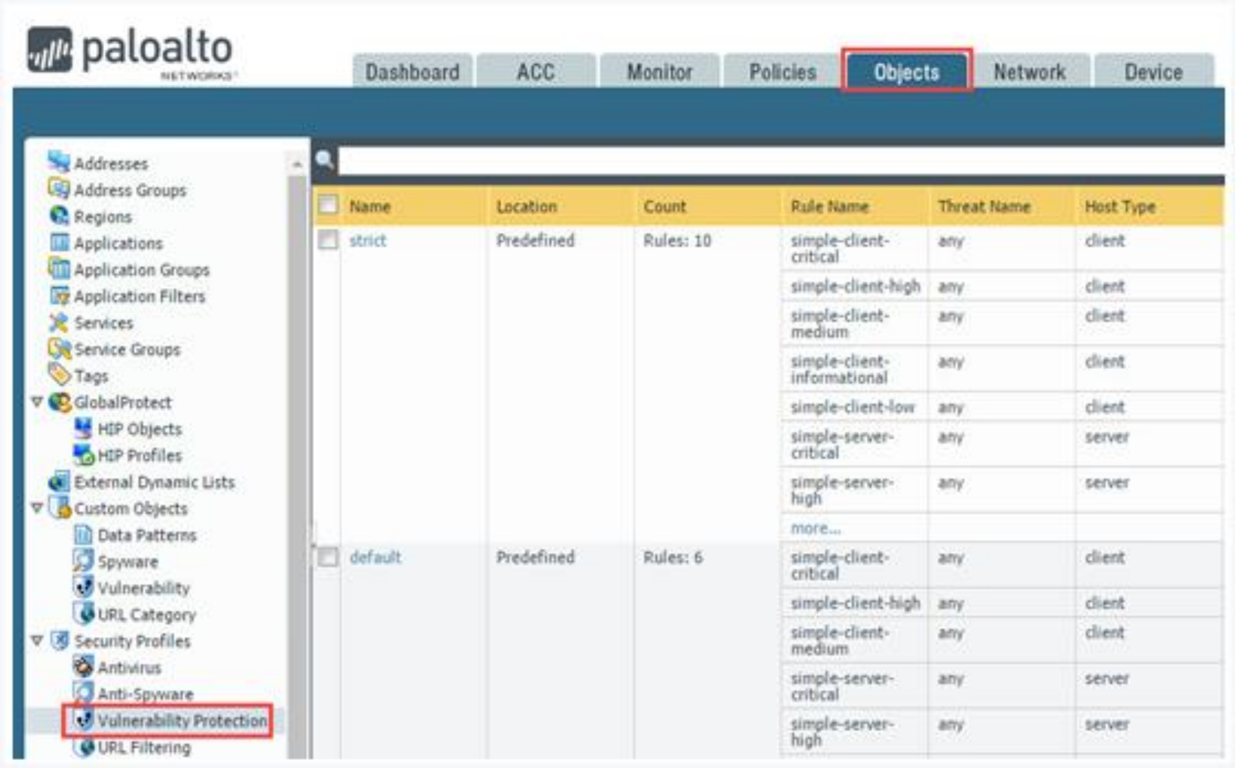
1 item

□	Standard	Comment	Ordered Condition Match	Scope
☑	AndroidPDF		✓	Transaction

6.4 Clone a Vulnerability Protection Profile

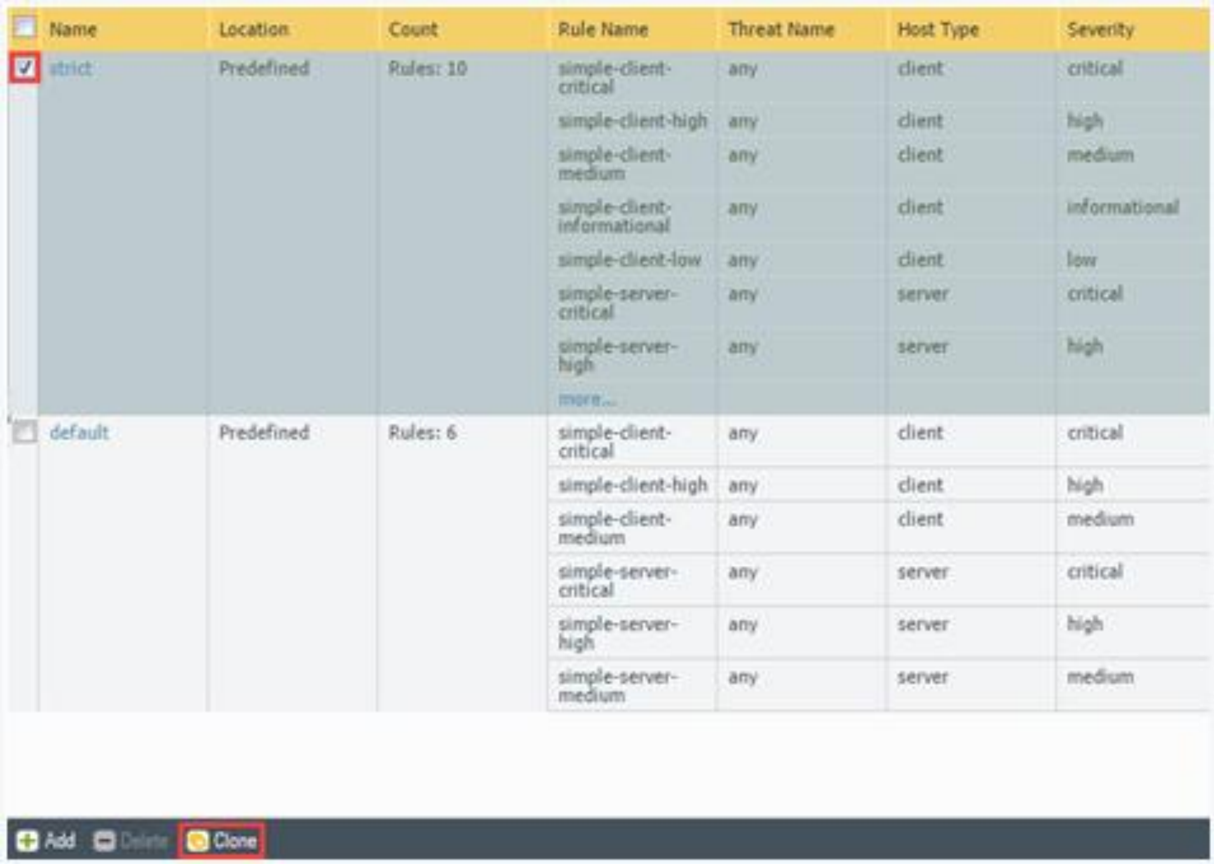
In this section, you will clone the **strict** Vulnerability Protection Profile. By creating a customized profile, you can minimize vulnerability-checking for traffic between trusted security zones, and maximize protection for traffic received from untrusted zones, such as the Internet. The **strict** profile applies the block response to all client and server critical, high, and medium severity events and uses the Default Action for low and informational vulnerability protection events.

1. Navigate to **Objects > Security Profiles > Vulnerability Protection**.



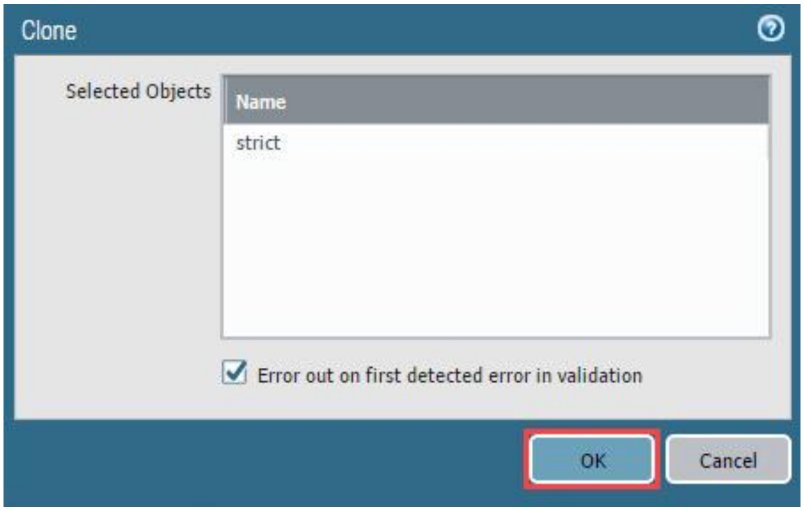
Name	Location	Count	Rule Name	Threat Name	Host Type
strict	Predefined	Rules: 10	simple-client-critical	any	client
			simple-client-high	any	client
			simple-client-medium	any	client
			simple-client-informational	any	client
			simple-client-low	any	client
			simple-server-critical	any	server
			simple-server-high	any	server
			more...		
default	Predefined	Rules: 6	simple-client-critical	any	client
			simple-client-high	any	client
			simple-client-medium	any	client
			simple-server-critical	any	server
			simple-server-high	any	server

2. Click the checkbox on the **strict** profile. Then, click the **Clone** button.



☐	Name	Location	Count	Rule Name	Threat Name	Host Type	Severity
☑	strict	Predefined	Rules: 10	simple-client-critical	any	client	critical
				simple-client-high	any	client	high
				simple-client-medium	any	client	medium
				simple-client-informational	any	client	informational
				simple-client-low	any	client	low
				simple-server-critical	any	server	critical
				simple-server-high	any	server	high
				more...			
☐	default	Predefined	Rules: 6	simple-client-critical	any	client	critical
				simple-client-high	any	client	high
				simple-client-medium	any	client	medium
				simple-server-critical	any	server	critical
				simple-server-high	any	server	high
				simple-server-medium	any	server	medium

3. In the *Clone* window, click the **OK** button.



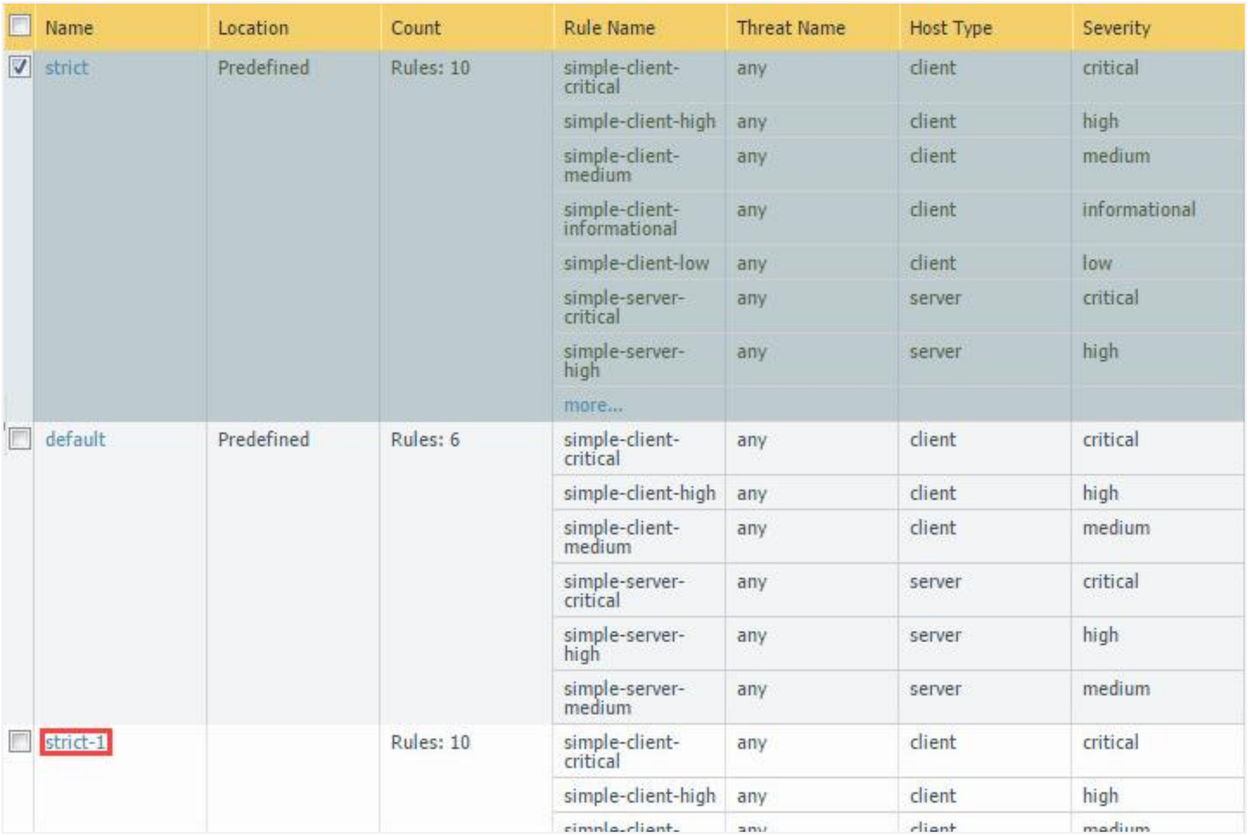
Clone

Selected Objects

Name
strict

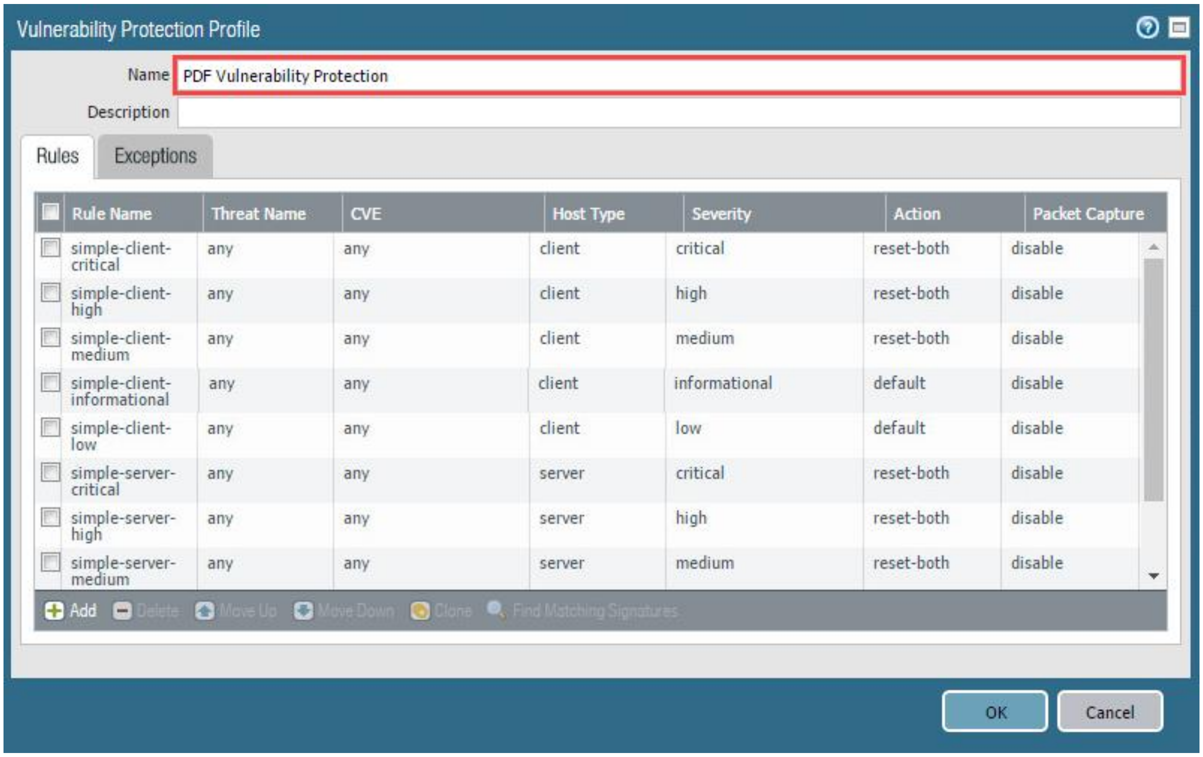
☑ Error out on first detected error in validation

4. Click on **strict-1**.



☐	Name	Location	Count	Rule Name	Threat Name	Host Type	Severity
☑	strict	Predefined	Rules: 10	simple-client-critical	any	client	critical
				simple-client-high	any	client	high
				simple-client-medium	any	client	medium
				simple-client-informational	any	client	informational
				simple-client-low	any	client	low
				simple-server-critical	any	server	critical
				simple-server-high	any	server	high
				more...			
☐	default	Predefined	Rules: 6	simple-client-critical	any	client	critical
				simple-client-high	any	client	high
				simple-client-medium	any	client	medium
				simple-server-critical	any	server	critical
				simple-server-high	any	server	high
				simple-server-medium	any	server	medium
☐	strict-1		Rules: 10	simple-client-critical	any	client	critical
				simple-client-high	any	client	high
				simple-client-	any	client	medium

5. In the *Vulnerability Protection Profile* window, type **`PDF Vulnerability Protection`** in the *Name* field.



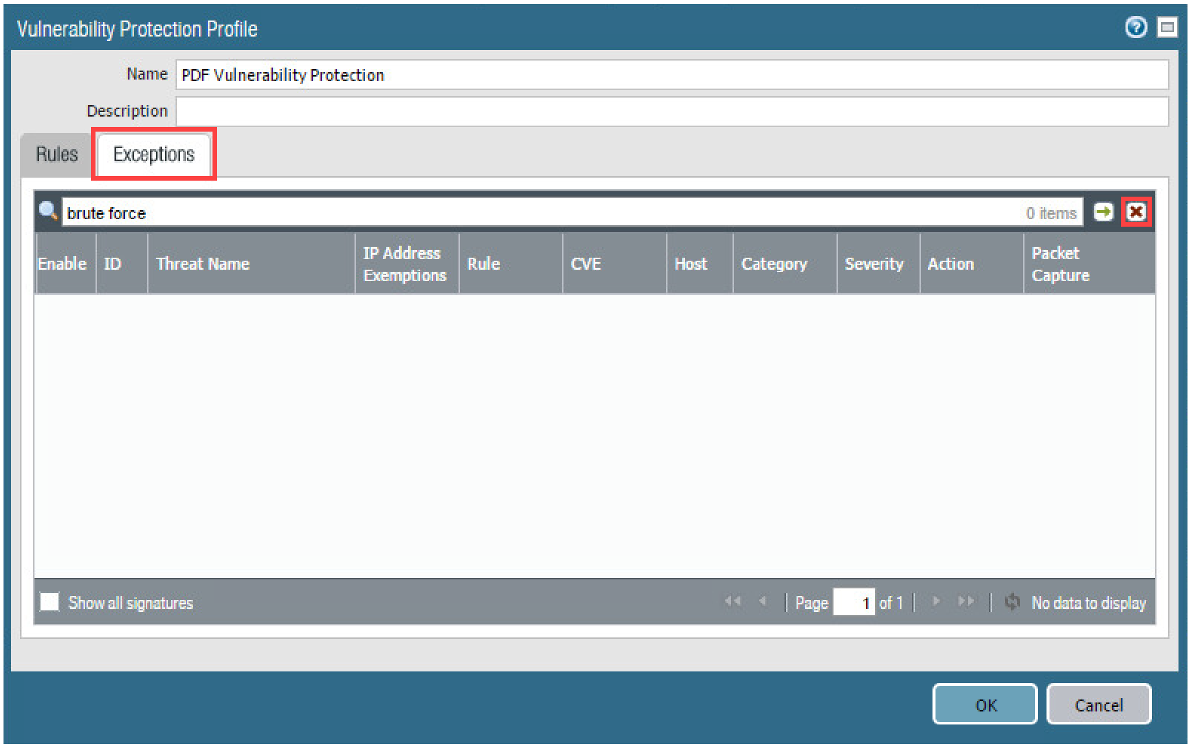
Vulnerability Protection Profile

Name: PDF Vulnerability Protection

Description:

☐	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
☐	simple-server-medium	any	any	server	medium	reset-both	disable

6. In the *Vulnerability Protection Profile* window, click the **Exceptions** tab. Click the red **X** button to clear the search box.



Name: PDF Vulnerability Protection

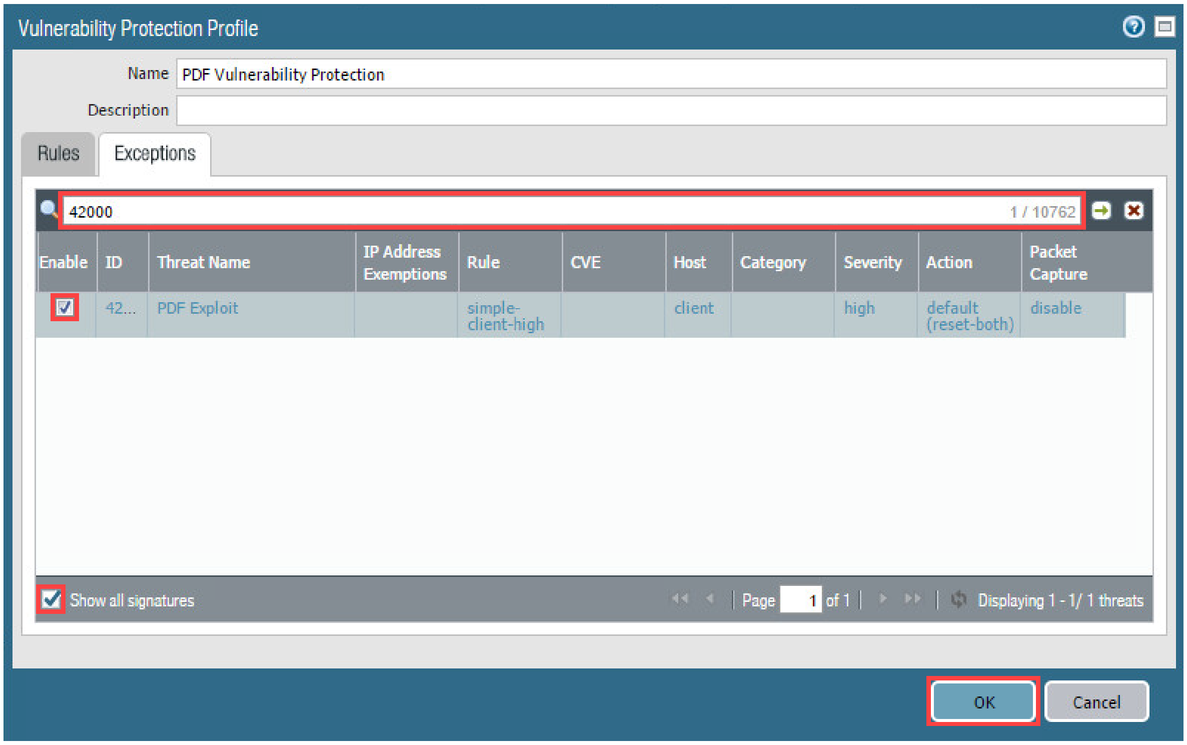
Description:

brute force — 0 items

Enable	ID	Threat Name	IP Address Exemptions	Rule	CVE	Host	Category	Severity	Action	Packet Capture

□ Show all signatures — Page 1 of 1 — No data to display

7. In the *Vulnerability Protection Profile* window, type **42000** in the search box. Then, click the checkbox for **Show all signatures**. Next, click the **Enable** checkbox for the **PDF Exploit** signature. Finally, click the **OK** button.



Name: PDF Vulnerability Protection

Description:

42000 — 1 / 10762

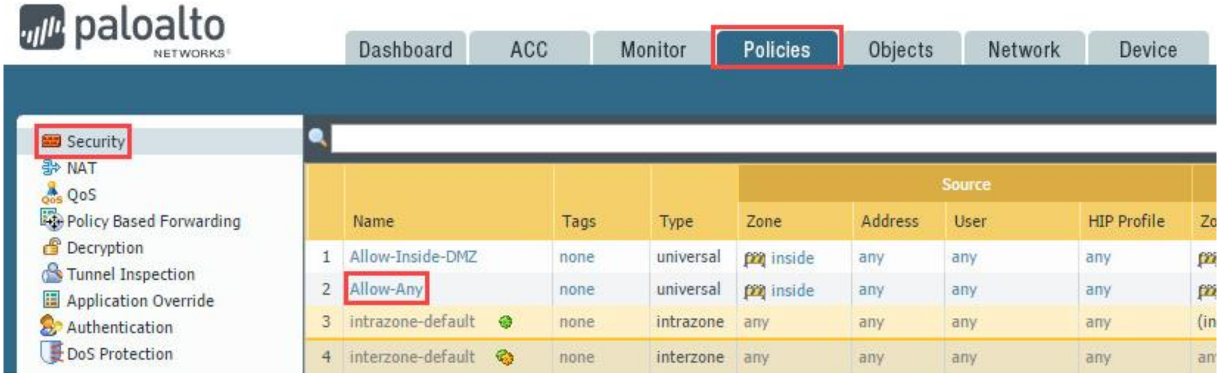
Enable	ID	Threat Name	IP Address Exemptions	Rule	CVE	Host	Category	Severity	Action	Packet Capture
☑	42...	PDF Exploit		simple-client-high		client		high	default (reset-both)	disable

☑ Show all signatures — Page 1 of 1 — Displaying 1 - 1/ 1 threats

6.5 Apply Custom Vulnerability Protection Profile to a Security Policy

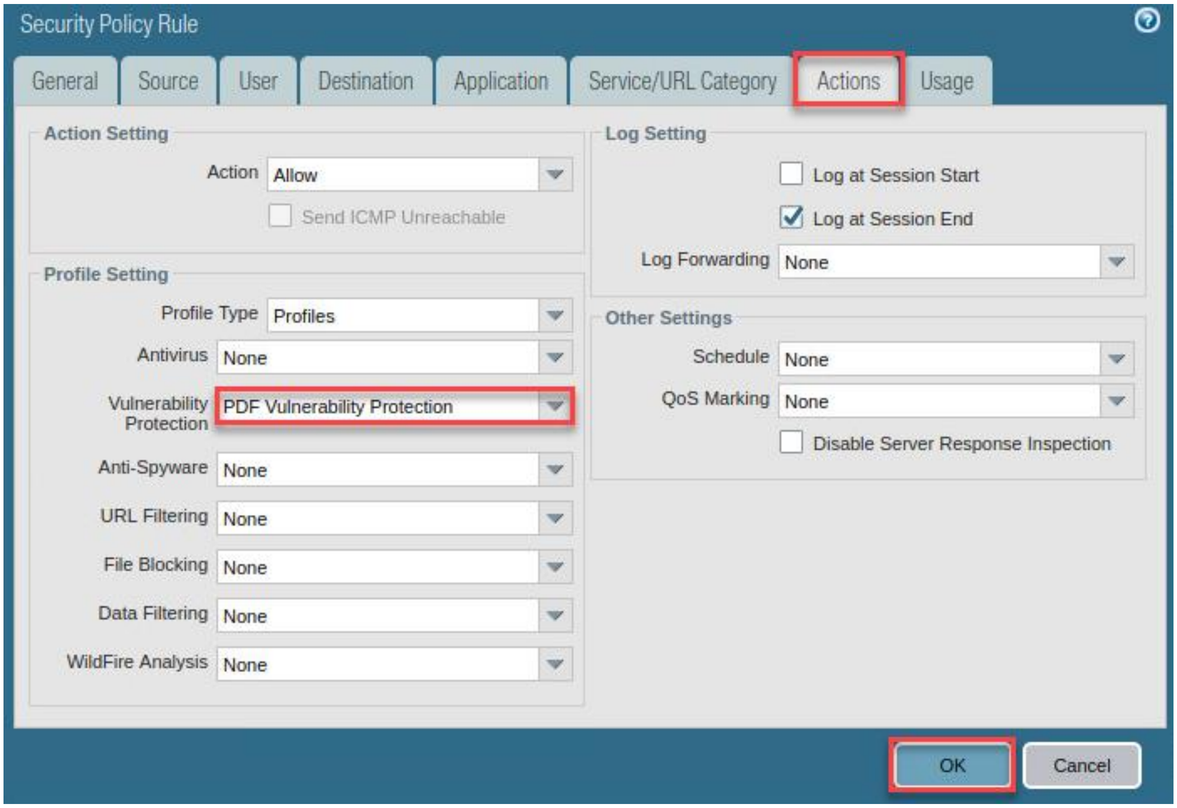
In this section, you will apply the Custom Vulnerability Protection Profile, **PDF Vulnerability Protection**, to the **Allow-Any** security policy for enforcement.

1. Navigate to **Policies > Security > Allow-Any**.



				Source				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zo
1	Allow-Inside-DMZ	none	universal	inside	any	any	any	
2	Allow-Any	none	universal	inside	any	any	any	
3	intrazone-default	none	intrazone	any	any	any	any	(in
4	interzone-default	none	interzone	any	any	any	any	an

2. In the *Security Policy Rule* window, select the **Actions** tab. Then, select **Profiles** from the *Profile Type* dropdown. Next, select **PDF Vulnerability Protection** from the *Vulnerability Protection* dropdown. Finally, click on the **OK** button.



Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: PDF Vulnerability Protection

Anti-Spyware: None

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

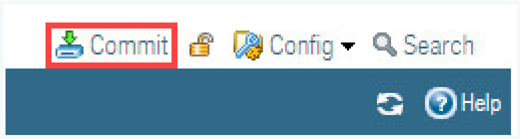
QoS Marking: None

□ Disable Server Response Inspection

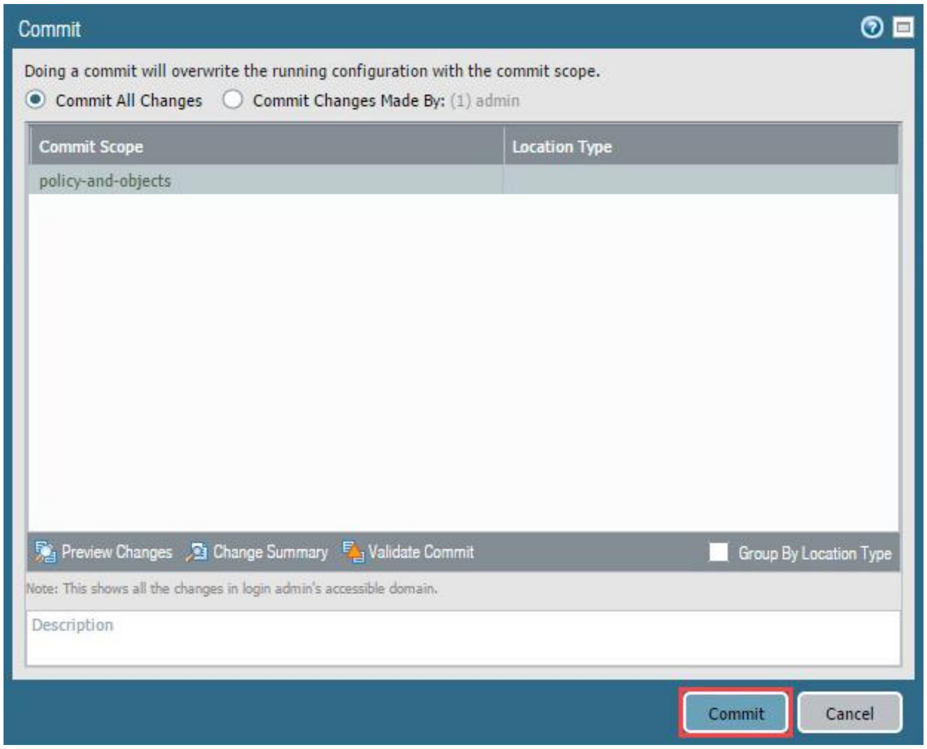
6.6 Commit and Test Vulnerability Protection

In this section, you will commit your changes to the Firewall. Then, you will attempt to download an infected PDF file and test the Vulnerability Protection. Next, you will verify it in the Threat Logs of the Palo Alto Networks Firewall.

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



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



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

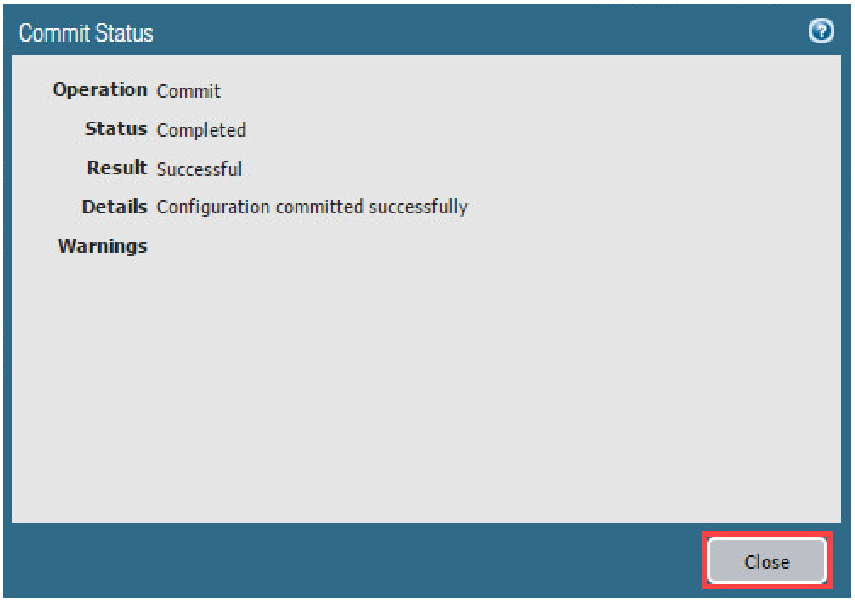
● Commit All Changes ○ Commit Changes Made By: (1) admin

Commit Scope	Location Type
policy-and-objects	

□ Group By Location Type

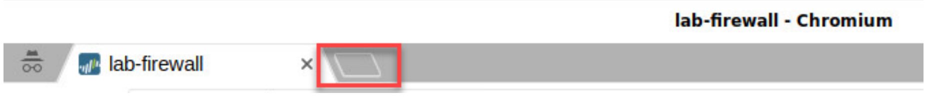
Note: This shows all the changes in login admin's accessible domain.

3. When the commit operation successfully completes, click **Close** to continue.

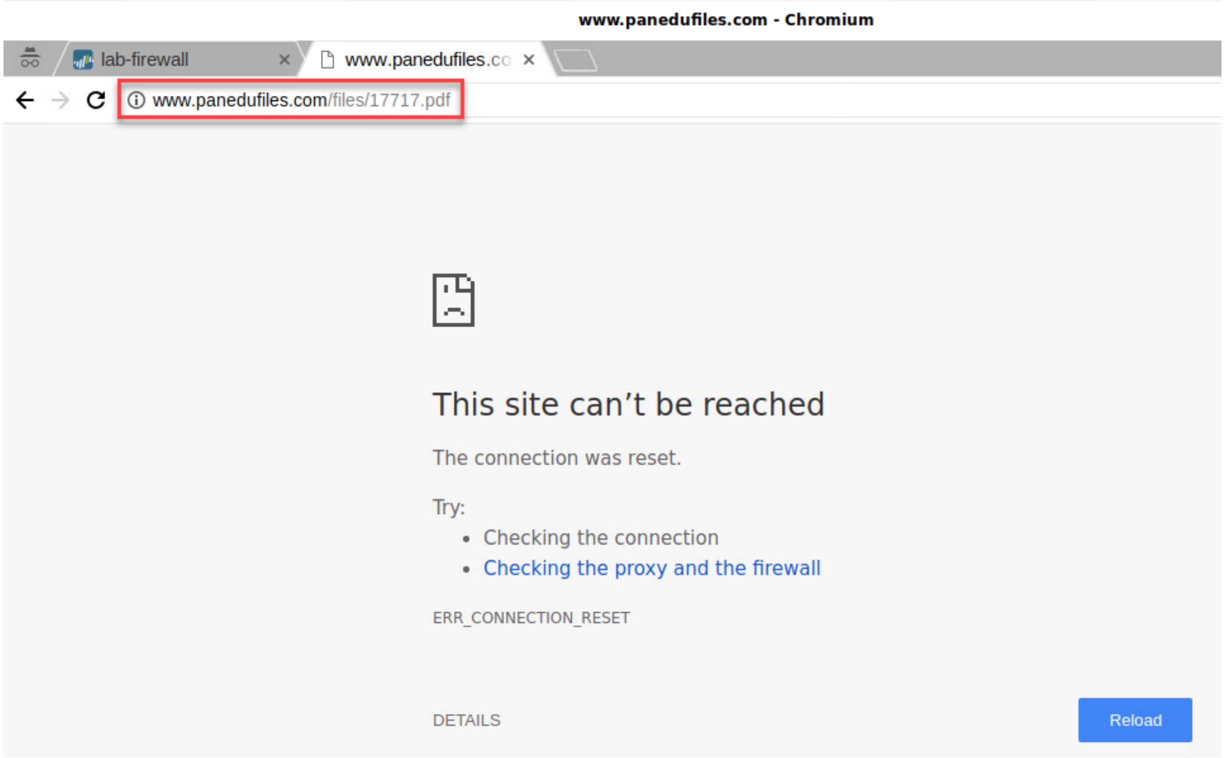


Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

4. Click on the **New tab** button in the upper-left.



5. In the address bar, type `http://www.panedufiles.com/files/17717.pdf` and press **Enter**.



www.panedufiles.com - Chromium

This site can’t be reached

The connection was reset.

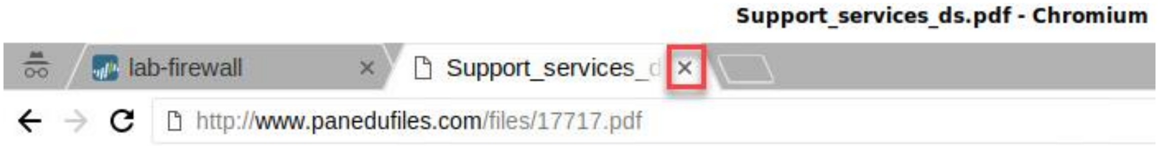
Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_RESET

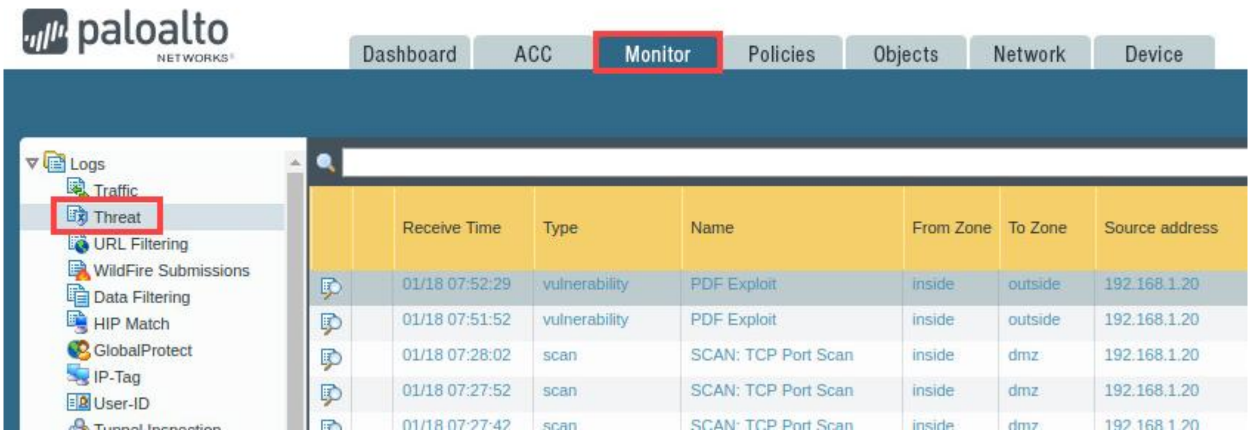
Notice the error message, *This site can’t be reached.* This is because the connection was reset by the Firewall to stop the exploit.

6. Click the **X** on the *www.panedufiles.com* tab.



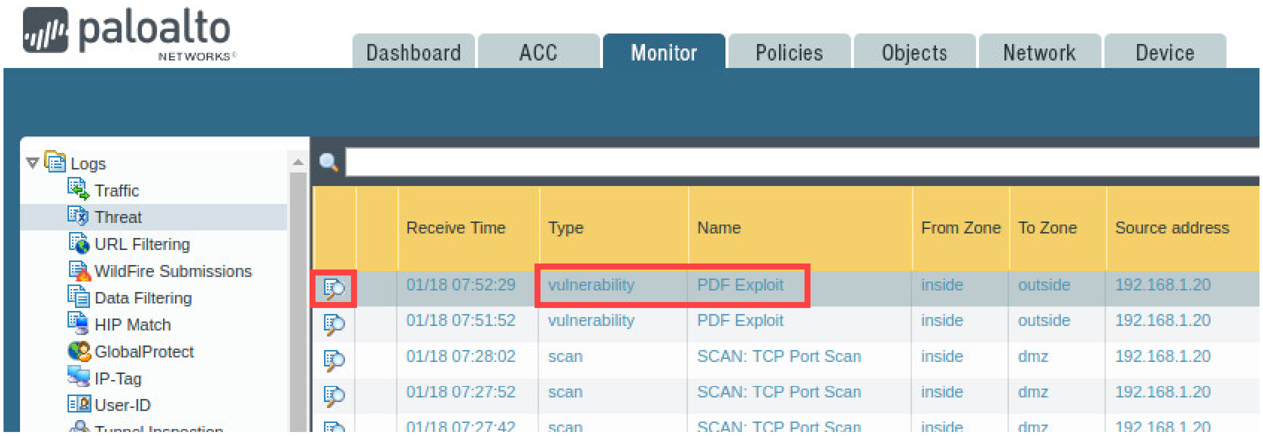
Support_services_ds.pdf - Chromium

7. Navigate to **Monitor > Logs > Threat**.



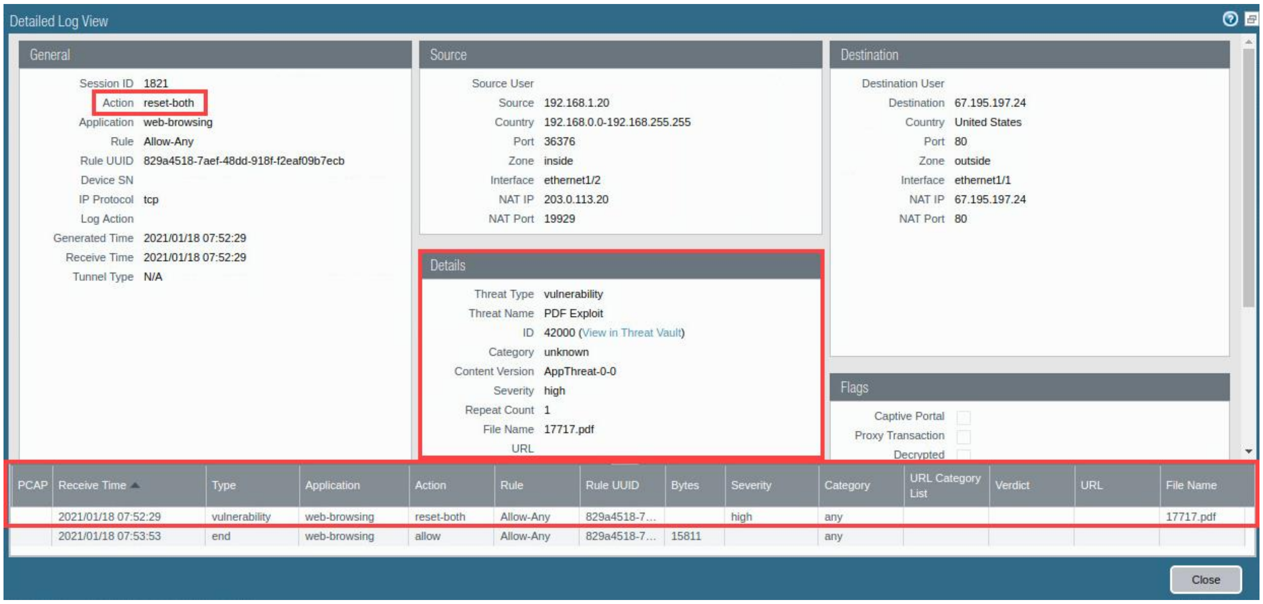
Receive Time	Type	Name	From Zone	To Zone	Source address
01/18 07:52:29	vulnerability	PDF Exploit	inside	outside	192.168.1.20
01/18 07:51:52	vulnerability	PDF Exploit	inside	outside	192.168.1.20
01/18 07:28:02	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20
01/18 07:27:52	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20
01/18 07:27:42	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20

8. Notice the threats listed (make sure that the search filter is cleared). Click on the **Detailed Log View** button.



Receive Time	Type	Name	From Zone	To Zone	Source address
01/18 07:52:29	vulnerability	PDF Exploit	inside	outside	192.168.1.20
01/18 07:51:52	vulnerability	PDF Exploit	inside	outside	192.168.1.20
01/18 07:28:02	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20
01/18 07:27:52	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20
01/18 07:27:42	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20

9. In the *Detailed Log View* window, analyze the threat, reviewing the information. In the *General* section, notice the *Action* taken. In the *Details* section, notice the *Threat Type*, *Threat Name,* and *ID*. At the bottom, you can see a list of all the sessions related to this log entry.



Detailed Log View

General

Session ID 1821
Action reset-both
Application web-browsing
Rule Allow-Any
Rule UUID 829a4518-7aef-48dd-918f-f2eaf09b7ecb
Device SN
IP Protocol tcp
Log Action
Generated Time 2021/01/18 07:52:29
Receive Time 2021/01/18 07:52:29
Tunnel Type N/A

Source

Source User
Source 192.168.1.20
Country 192.168.0.0-192.168.255.255
Port 36376
Zone inside
Interface ethernet1/2
NAT IP 203.0.113.20
NAT Port 19929

Destination

Destination User
Destination 67.195.197.24
Country United States
Port 80
Zone outside
Interface ethernet1/1
NAT IP 67.195.197.24
NAT Port 80

Details

Threat Type vulnerability
Threat Name PDF Exploit
ID 42000 (View in Threat Vault)
Category unknown
Content Version AppThreat-0-0
Severity high
Repeat Count 1
File Name 17717.pdf
URL

Flags

Captive Portal □
Proxy Transaction □
Decrypted □

PCAP	Receive Time ▲	Type	Application	Action	Rule	Rule UUID	Bytes	Severity	Category	URL Category List	Verdict	URL	File Name
	2021/01/18 07:52:29	vulnerability	web-browsing	reset-both	Allow-Any	829a4518-7…		high	any				17717.pdf
	2021/01/18 07:53:53	end	web-browsing	allow	Allow-Any	829a4518-7…	15811		any				

10. The lab is now complete; you may end the reservation.