SECURITY OPERATIONS FUNDAMENTALS V2

Lab 6: Securing Endpoints using Vulnerability Profiles

Document Version: 2023-12-22

Contents

Introduction

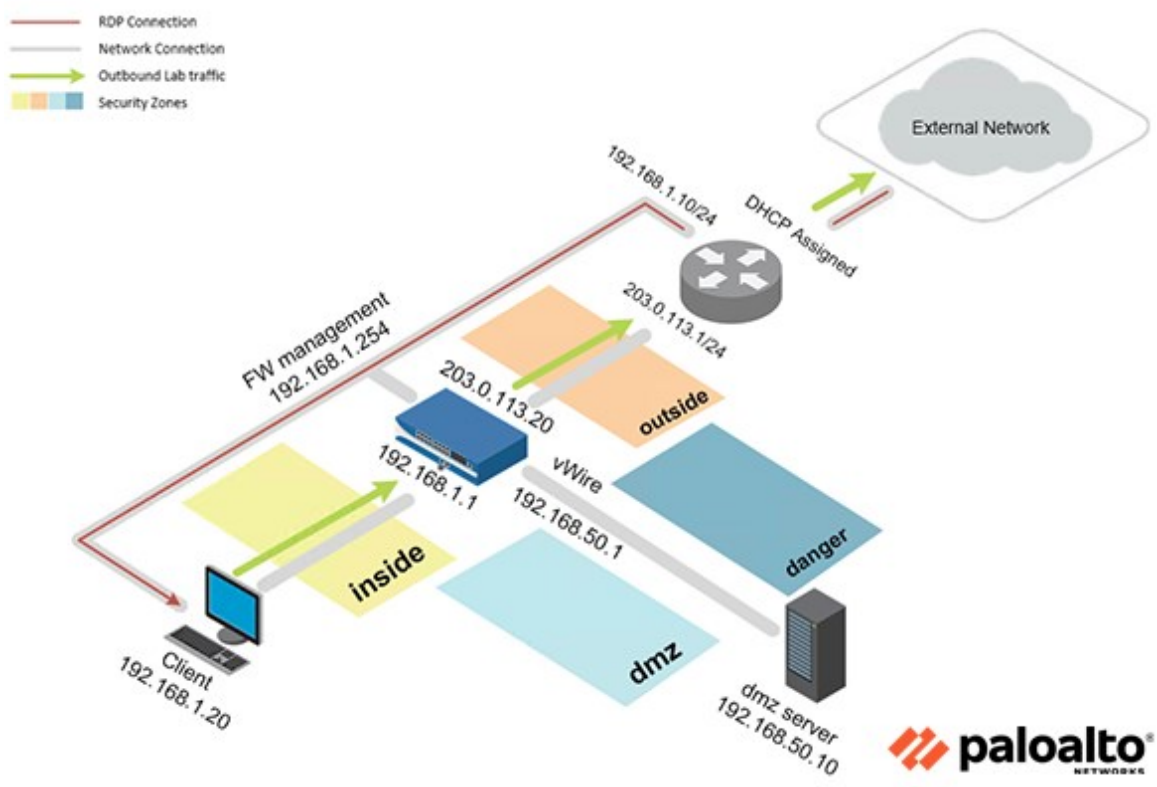
In this lab, you will secure an endpoint by blocking a PDF file with a Custom Vulnerability Object and Vulnerability Protection Profile. Palo Alto Networks Firewalls support the use of Custom Vulnerability Signatures that can be written with expression patterns to identify vulnerability exploits. Vulnerability 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.

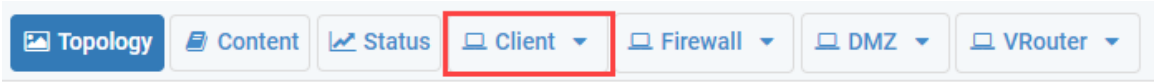
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Securing Endpoints Using Vulnerability Profiles

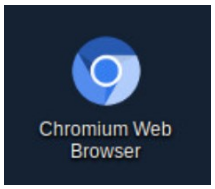
1.0 Load Lab Configuration

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

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

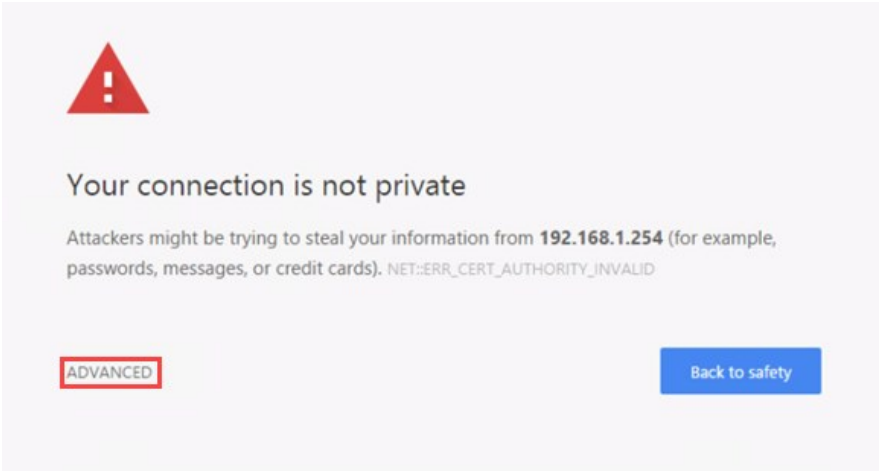


2. Log in to the client PC with username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



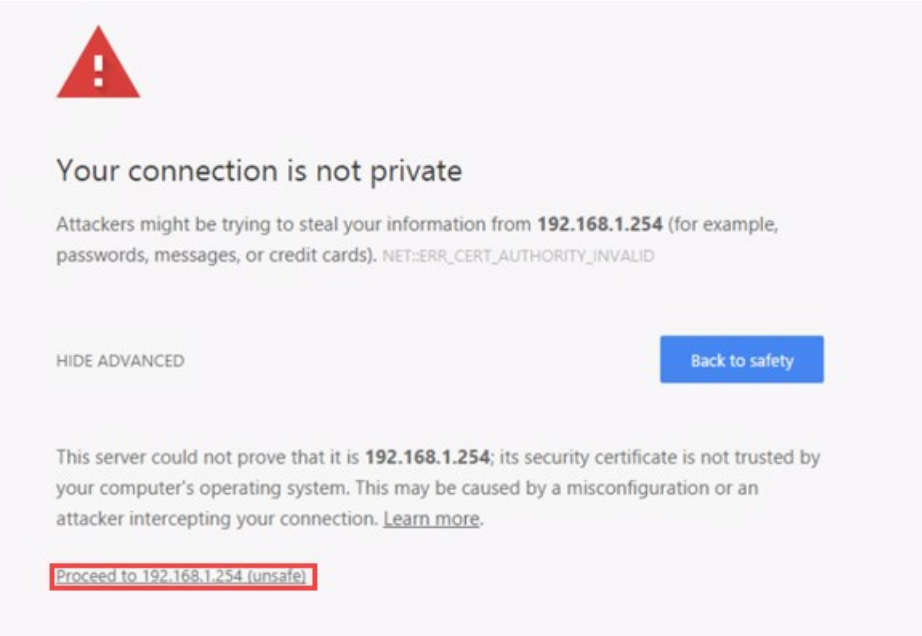
4. In the *Chromium address* field, type `https://192.168.1.254` and press **Enter**.

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



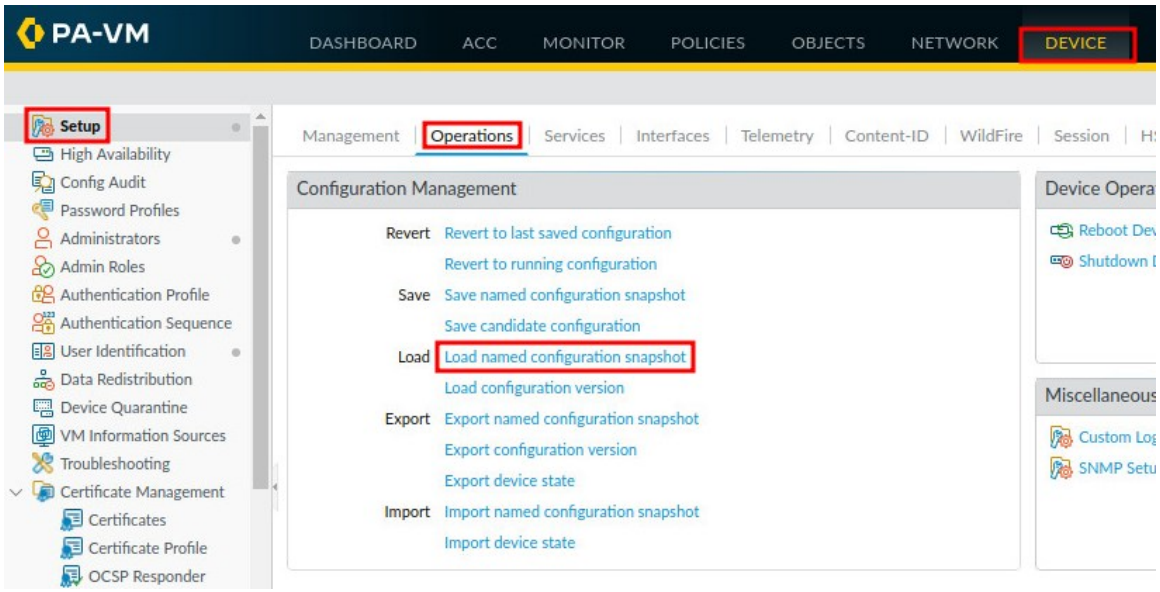
If you encounter the *"Unable to connect"* or *"502 Bad Gateway"* message while attempting to connect to the IP specified above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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



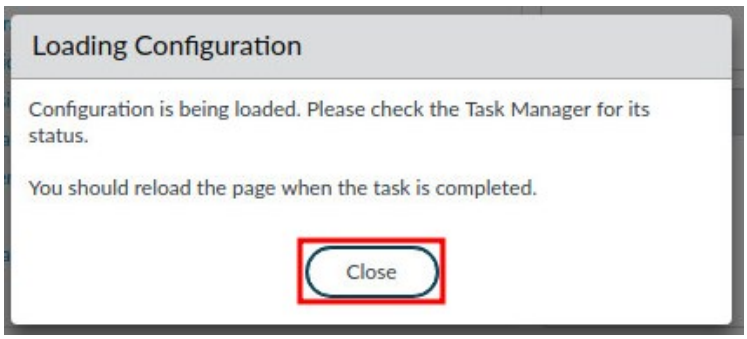
7. Log in to the Firewall web interface with username `admin`, password `Pal0Alt0!.`

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



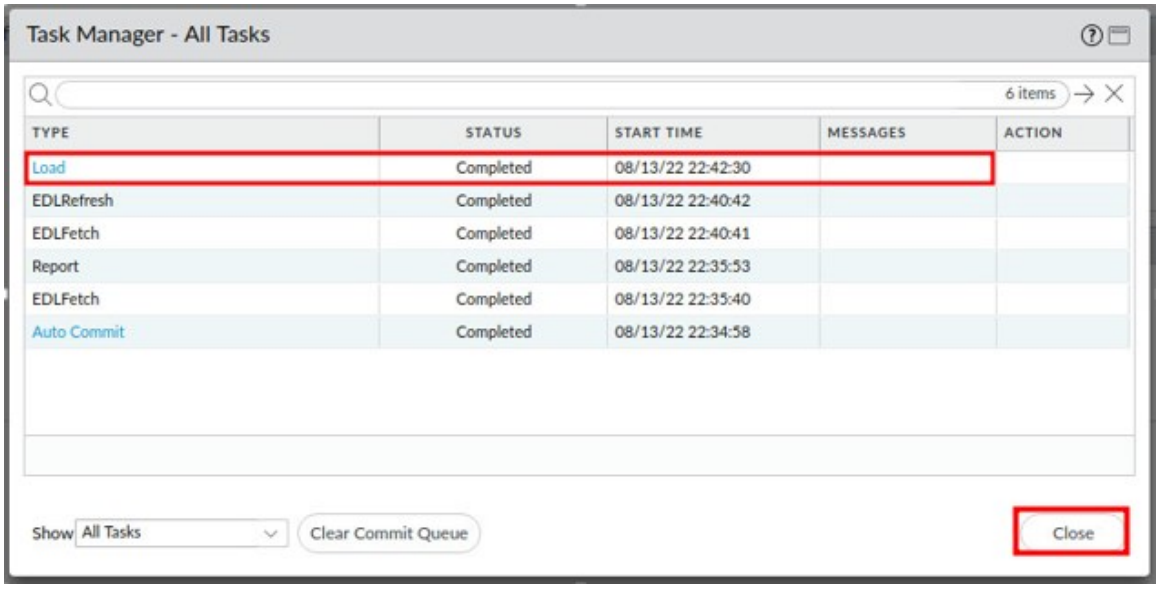
9. In the *Load Named Configuration* window, select **pan-sof-lab-06.xml** from the *Name* dropdown box and click **OK**.

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.

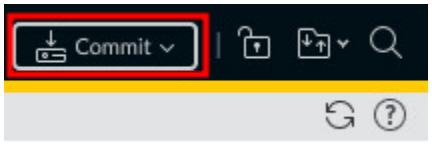


11. Click the **Tasks** icon located at the bottom-right of the web interface.

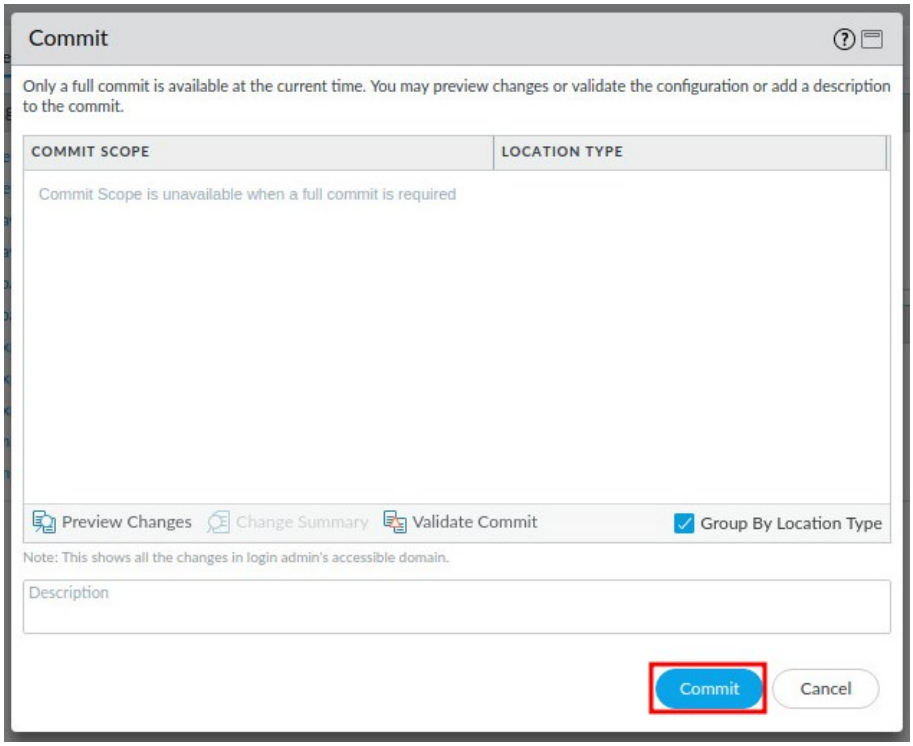
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**



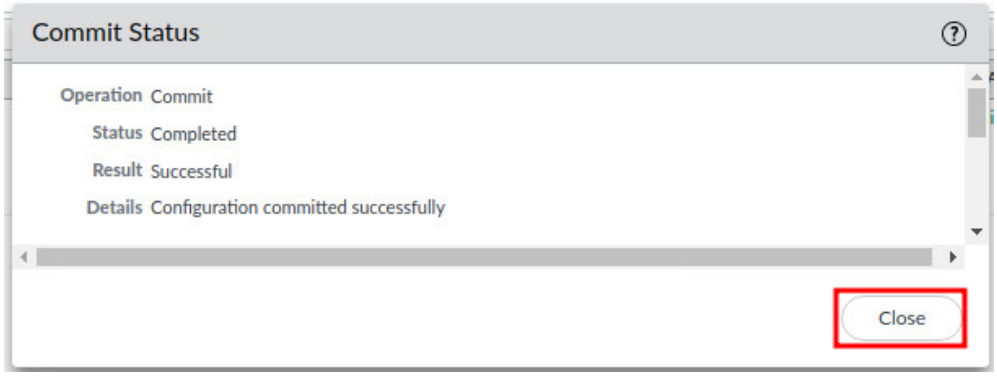
13. Click the **Commit** link located at the top-right of the web interface.



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



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

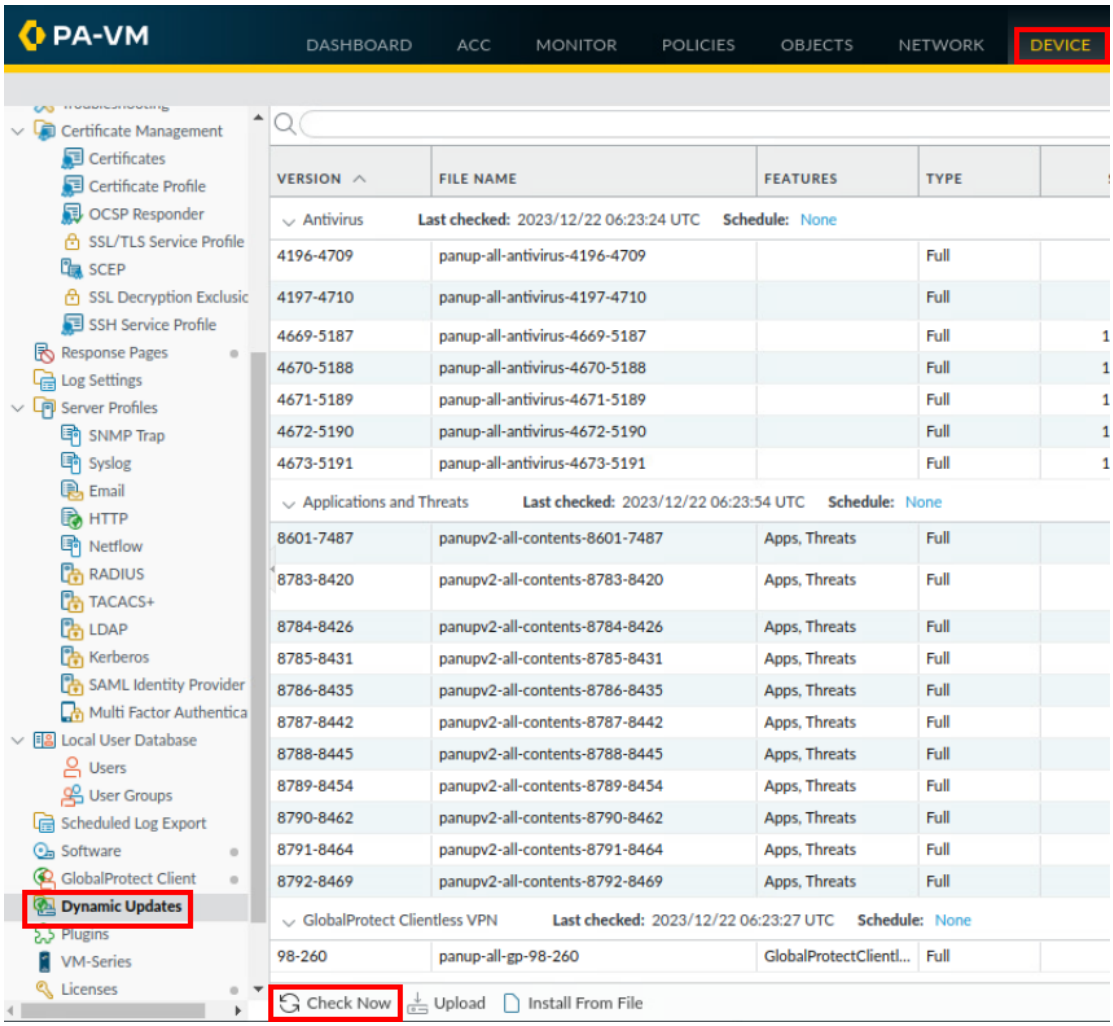


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

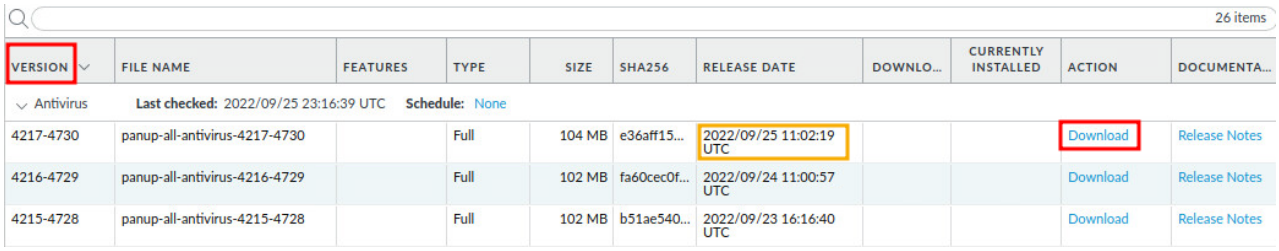
1.1 Install the Latest Dynamic Updates of Antivirus

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.

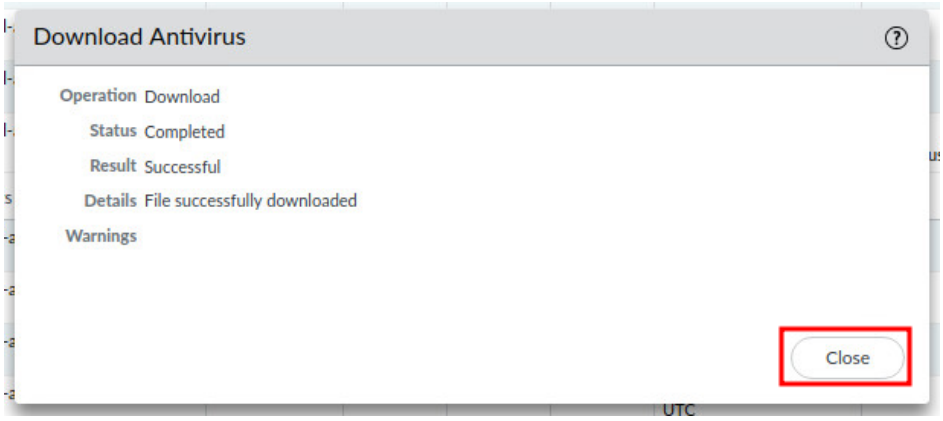


2. Click on *VERSION* to sort the entries such that the latest is at the top. Under the *Antivirus* update, click **Download** on the latest update.

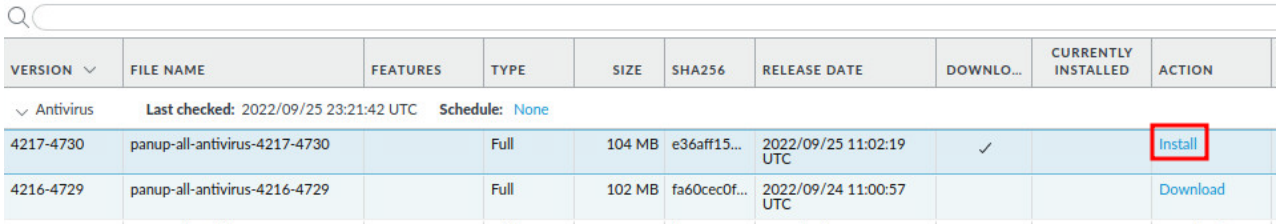


This lab environment connects to a live update server. Therefore, screenshots are subject to change. Please select the latest update.

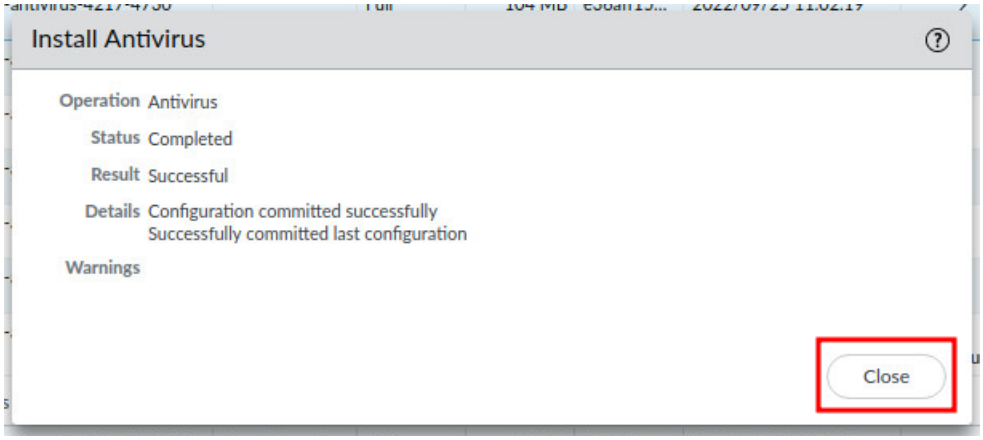
3. In the *Download Antivirus* window, after the download is completed, click the **Close** button.



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



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

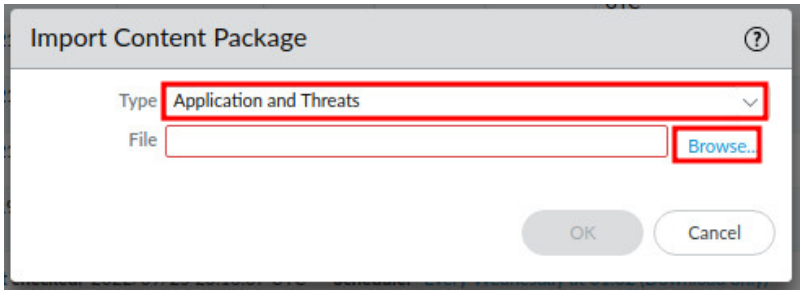


1.2 Install Manual Update of Applications and Threats

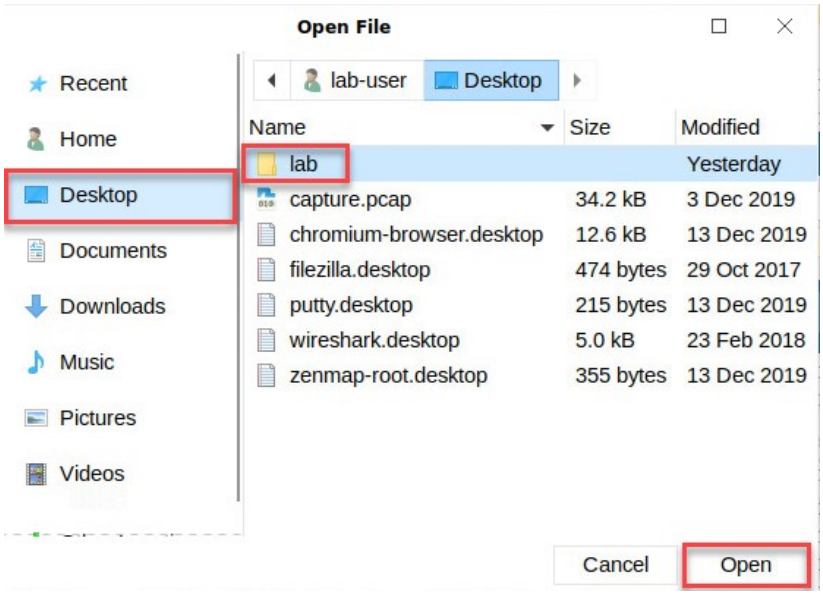
In this section, you will perform a Manual Update. There are times when the Firewall may not have Internet access to perform a Dynamic Update. Applications and Threats will be updated via a file that has been downloaded from the Palo Alto Networks Customer Support Portal.

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

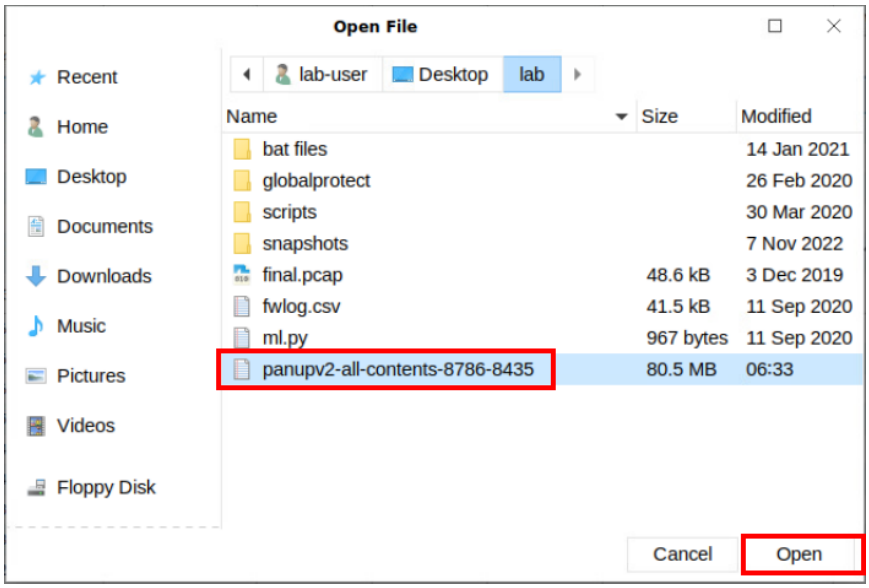
2. In the *Import Content Package* window, select **Application and Threats** from the *Type* dropdown. Then, click on **Browse…**



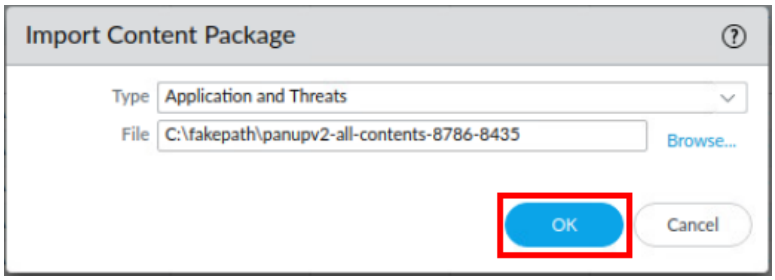
3. In the *Open File* window, select **Desktop**, and click the **lab** folder. Lastly, click **Open**.



4. Click on the **panupv2-all-contents-8786-8435** file. Lastly, click **Open**.

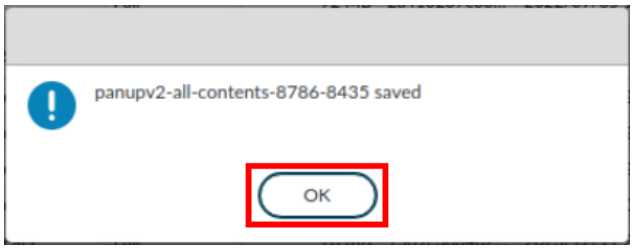


5. In the *Import Content Package* window, click on the **OK** button.



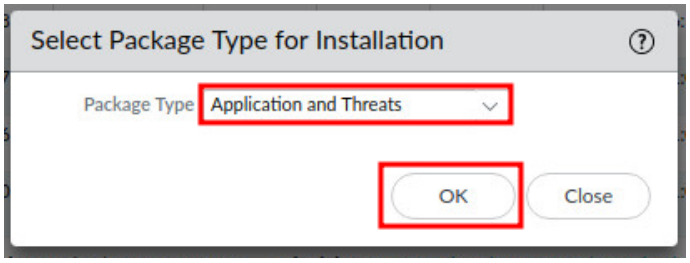
This may take several minutes to complete.

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

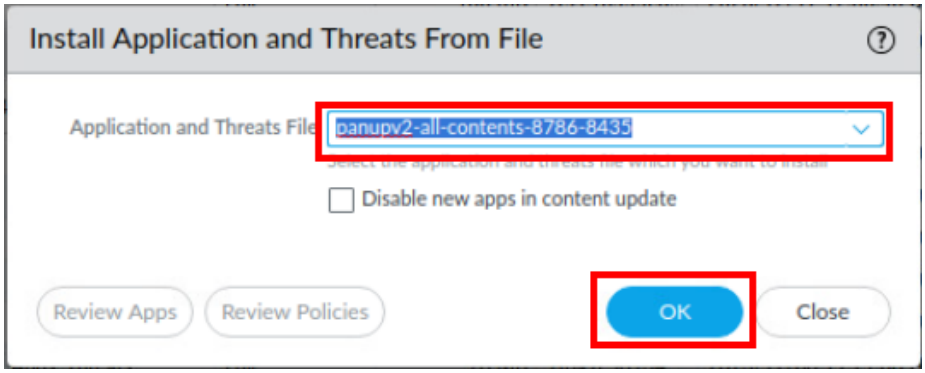


7. With the file uploaded, you can begin the install. Click on **Install From File** at the bottom.

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

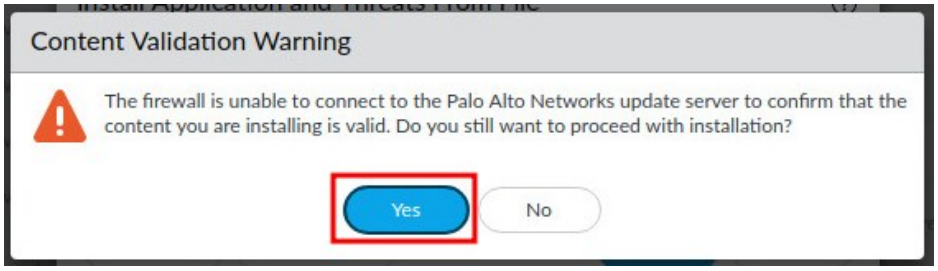


9. In the *Install Application and Threats From File* window, select **panupv2-all-contents-8786-8435** from the *Application and Threats File* dropdown. Then, click on the **OK** button.

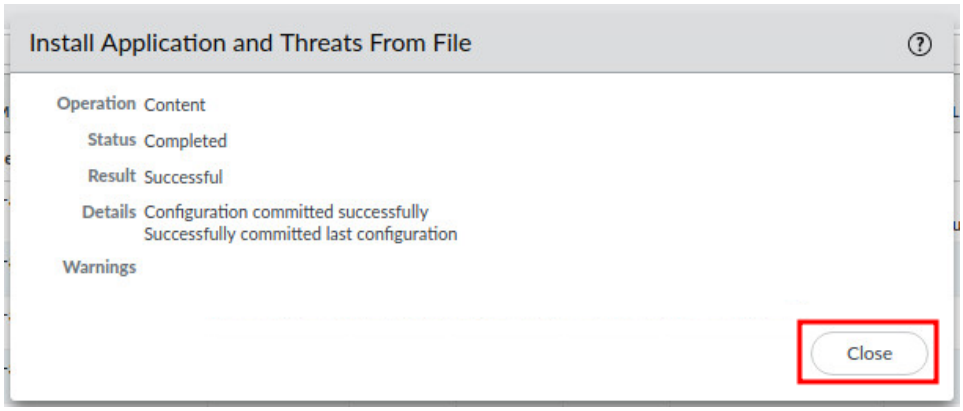


For the purpose of this lab, you will be manually installing the **Application and Threats** from a file already downloaded on the client machine. Normally you would download and install any updates from Palo Alto Networks via *Check Now*. Using *Check Now* retrieves the latest updates from Palo Alto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

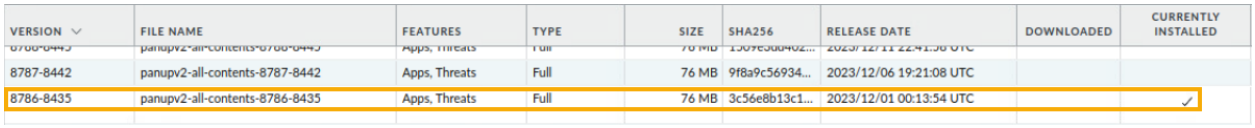
10. If you see a *Content Validation Warning* window popup, please click the **Yes** button to proceed.



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



12. Verify that the **panupv2-all-contents-8786-8435** version is now active.

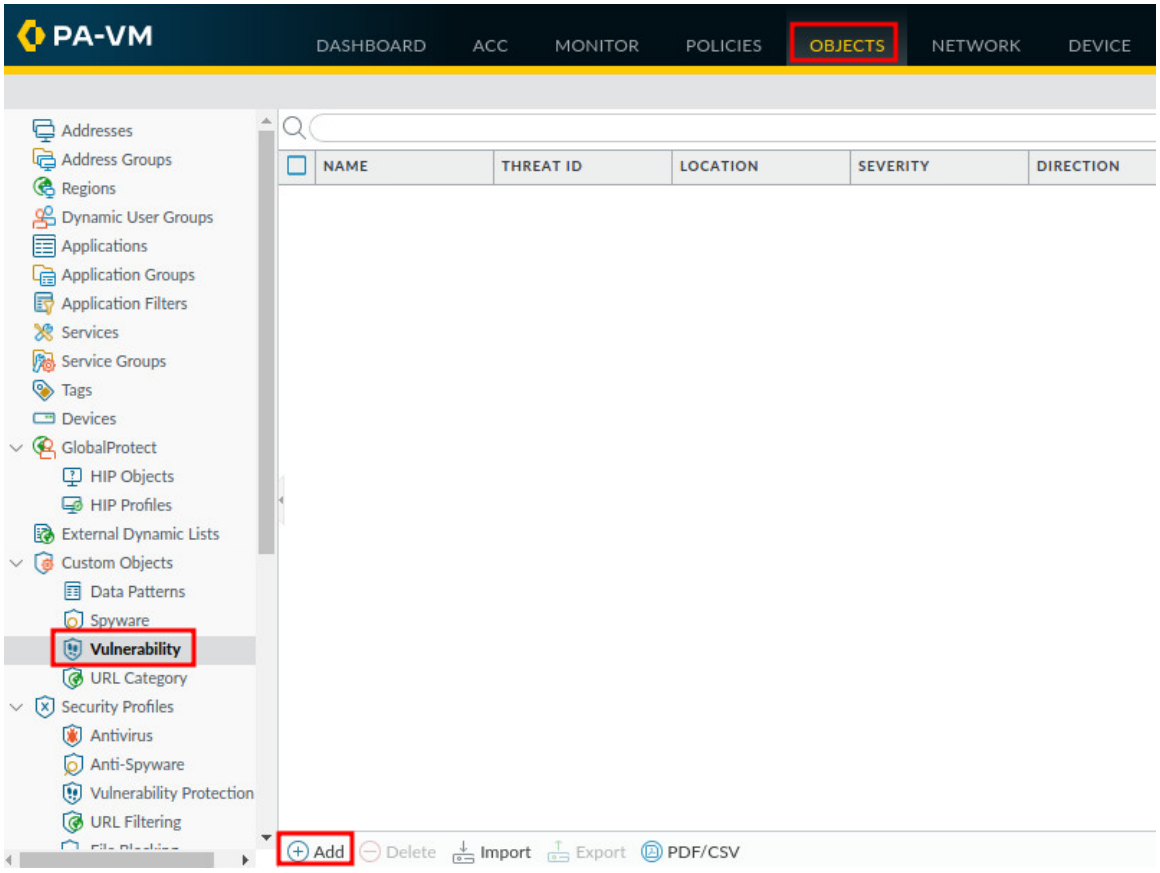


VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED
8787-8442	panupv2-all-contents-8787-8442	Apps, Threats	Full	76 MB	9f8a9c56934...	2023/12/06 19:21:08 UTC		
8786-8435	panupv2-all-contents-8786-8435	Apps, Threats	Full	76 MB	3c56e8b13c1...	2023/12/01 00:13:54 UTC		✓

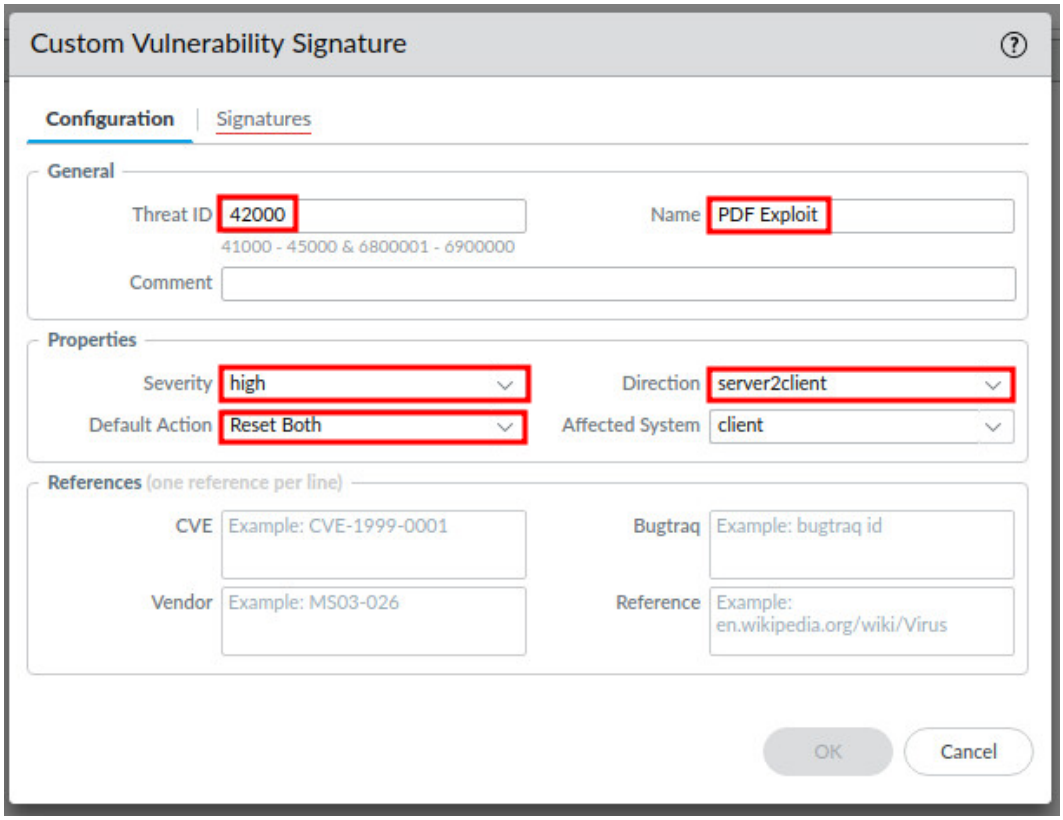
1.3 Create a Custom Vulnerability Signature

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**.

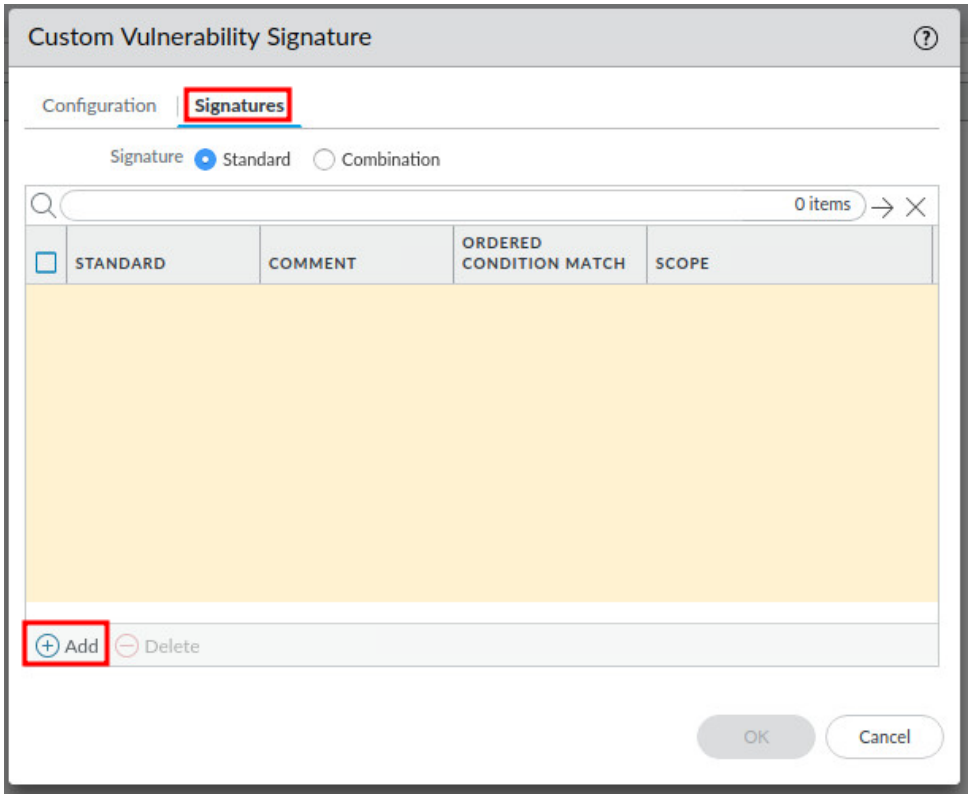


2. In the *Custom Vulnerability Signature* window, type `42000` in the *Threat ID* field. Then, type `PDF Exploit` in the *Name* field. Next, select **high** from the *Severity* dropdown. Then, select **server2client** from the *Direction* dropdown. Finally, select **Reset Both** from the *Default Action*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

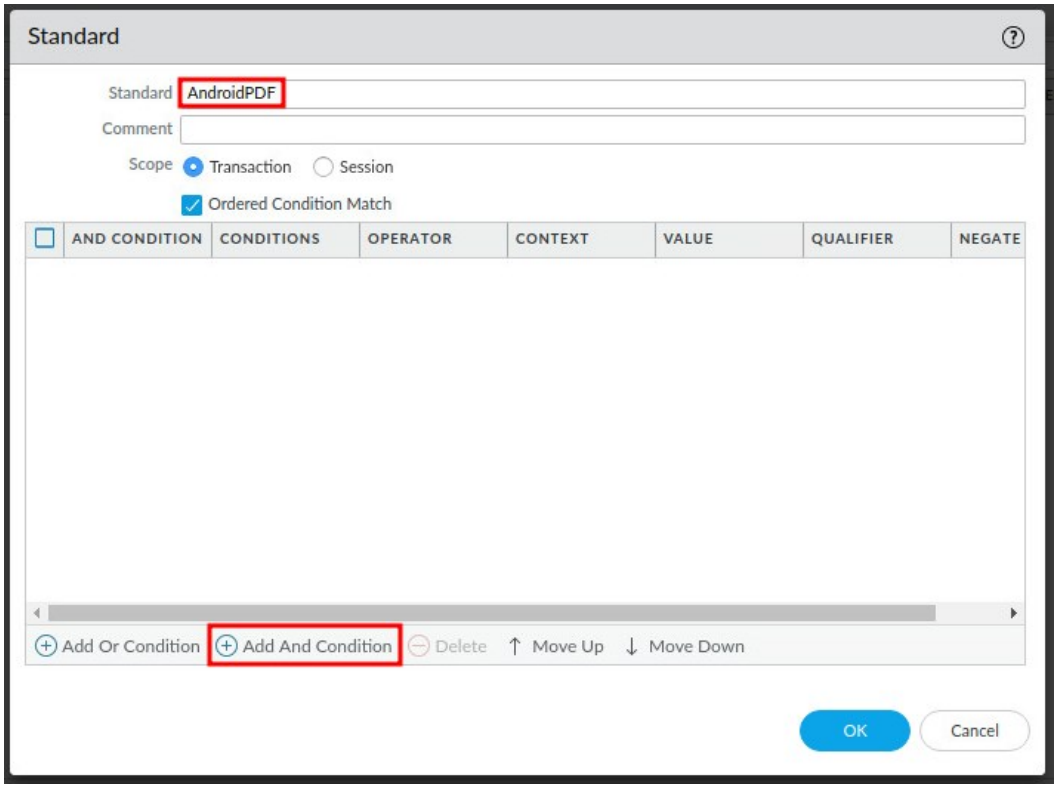


The Default Action, **Reset Both**, will be triggered when a match is detected to this Vulnerability Signature. For TCP, this will reset the connections on both the client and server ends. For UDP, the connection is dropped. This will effectively stop the traffic.

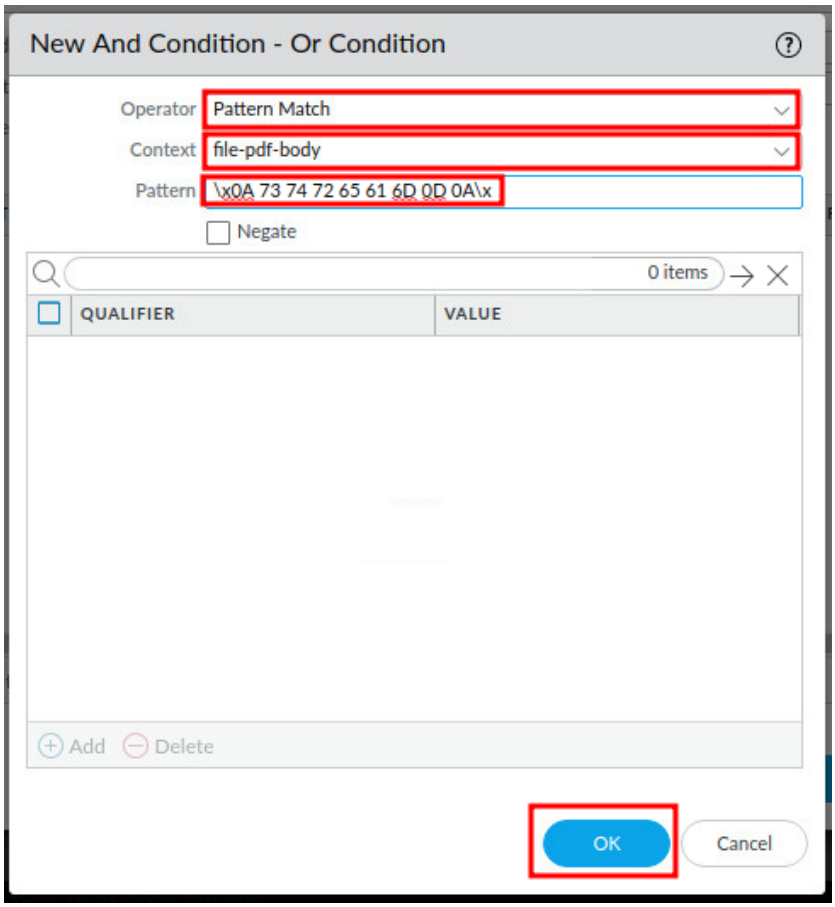
3. In the *Custom Vulnerability Signature* window, click on the **Signatures** tab. Then, click the **Add** button.



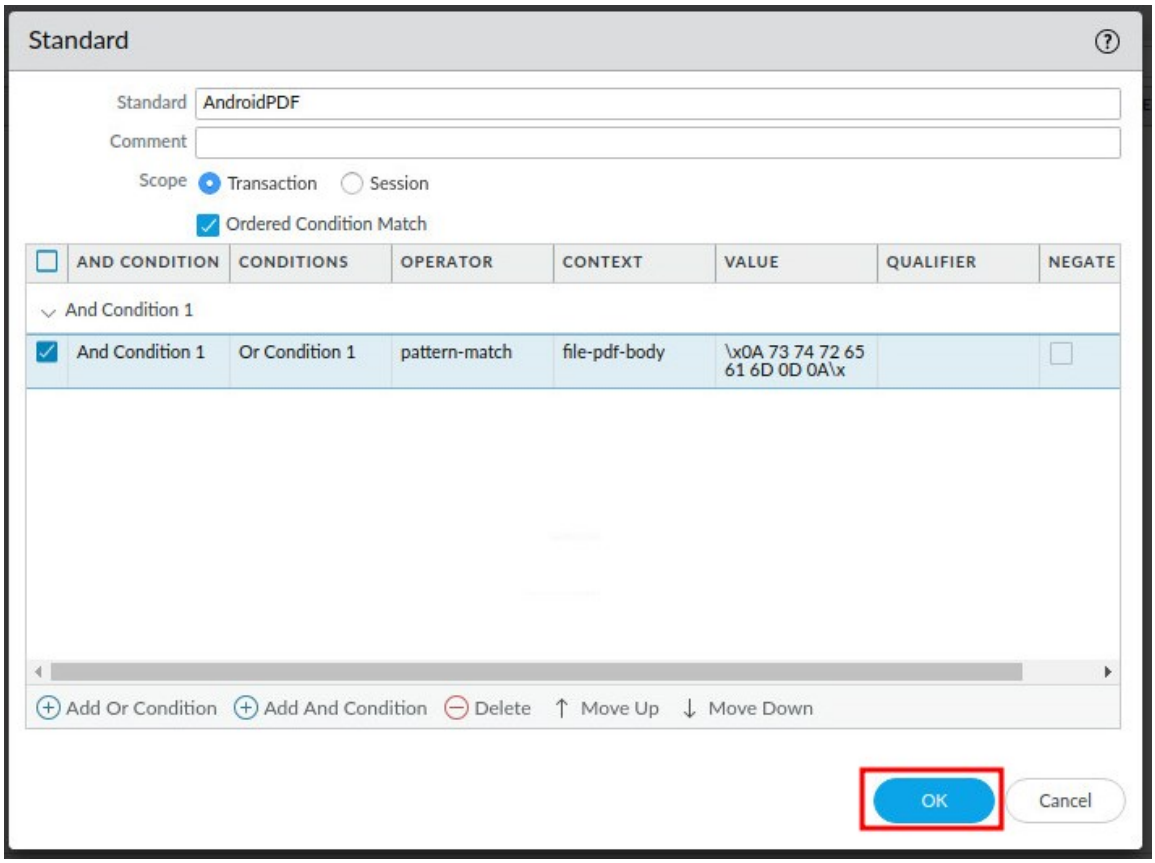
4. In the *Standard* window box, type `AndroidPDF` in the *Standard* field. Then**,** click **Add And Condition**.



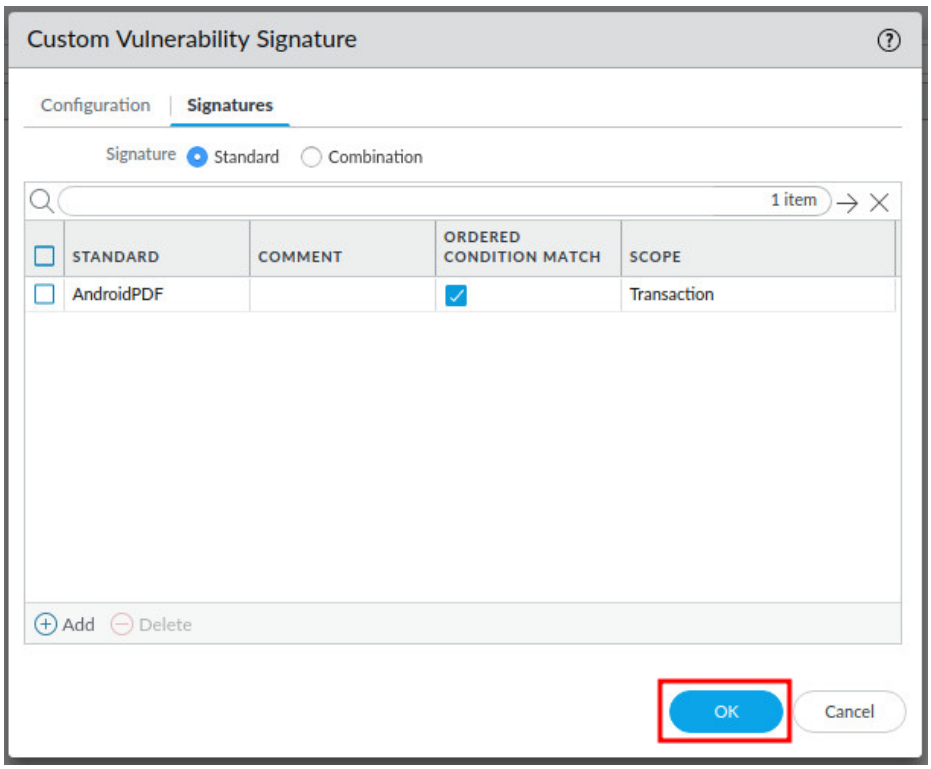
5. In the *New And Condition – Or Condition* window, select **Pattern Match** from the *Operator* dropdown. Then, select **file-pdf-body** from the *Context* dropdown. Next, type `\x0A 73 74 72 65 61 6D 0D 0A\x` in the *Pattern* field. Finally, click the **OK** button.



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



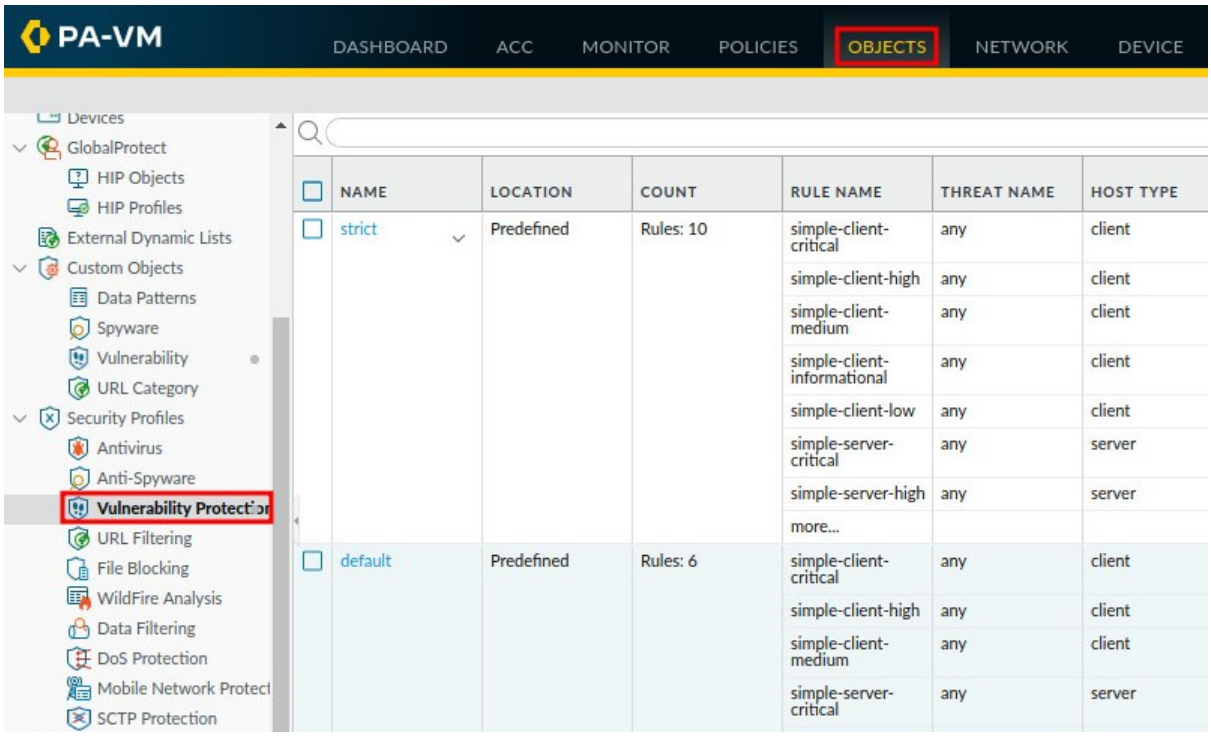
7. In the *Custom Vulnerability Signature* window, click the **OK** button.



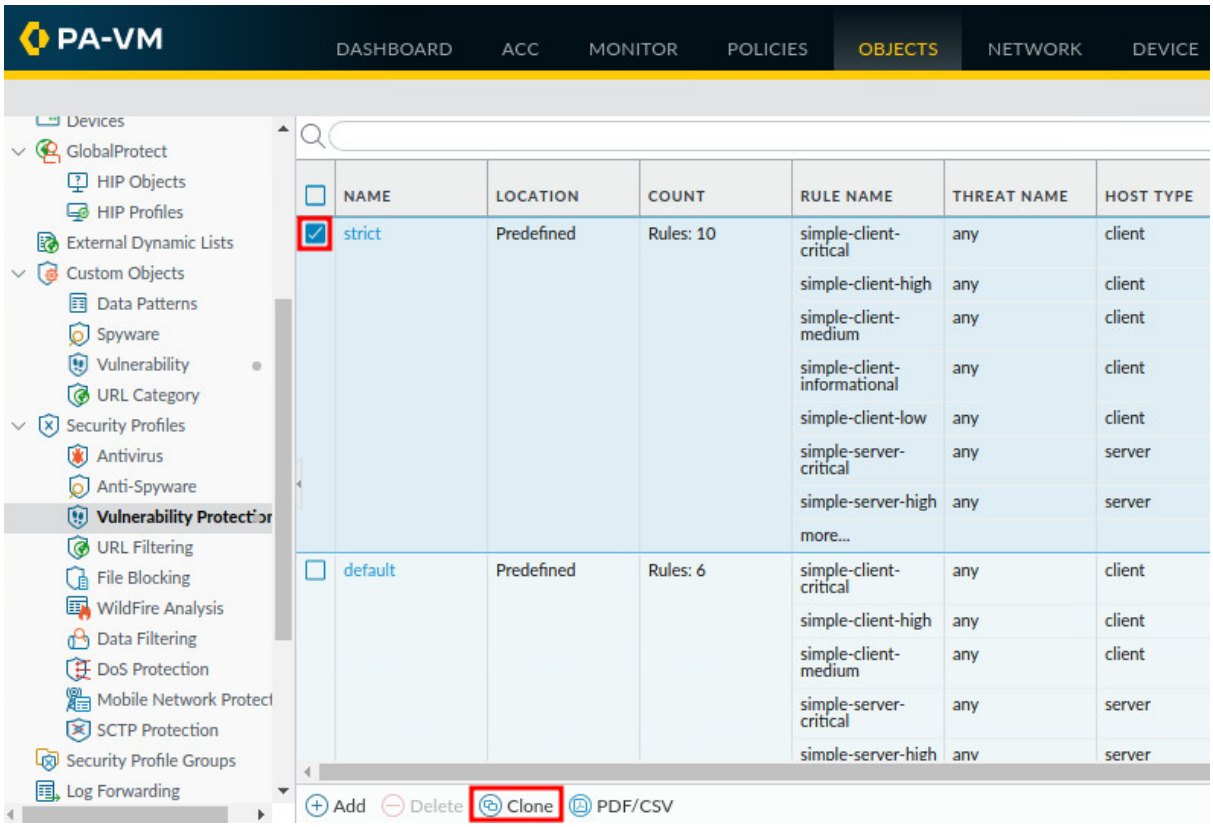
1.4 Clone a Vulnerability Protection Profile

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.

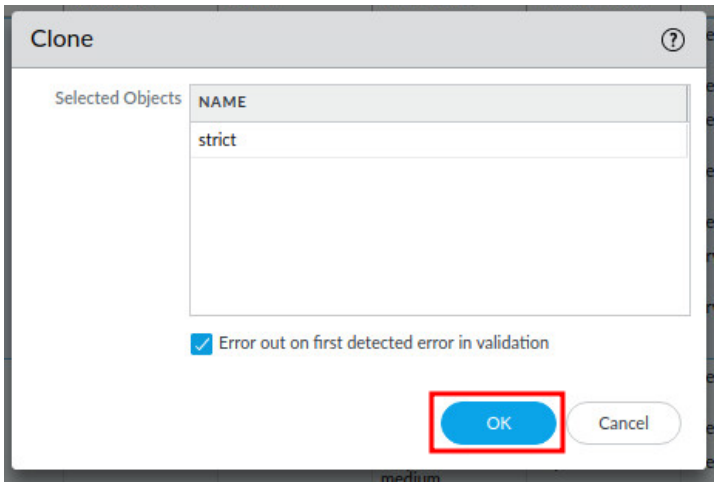
1. Navigate to **Objects > Security Profiles > Vulnerability Protection**.



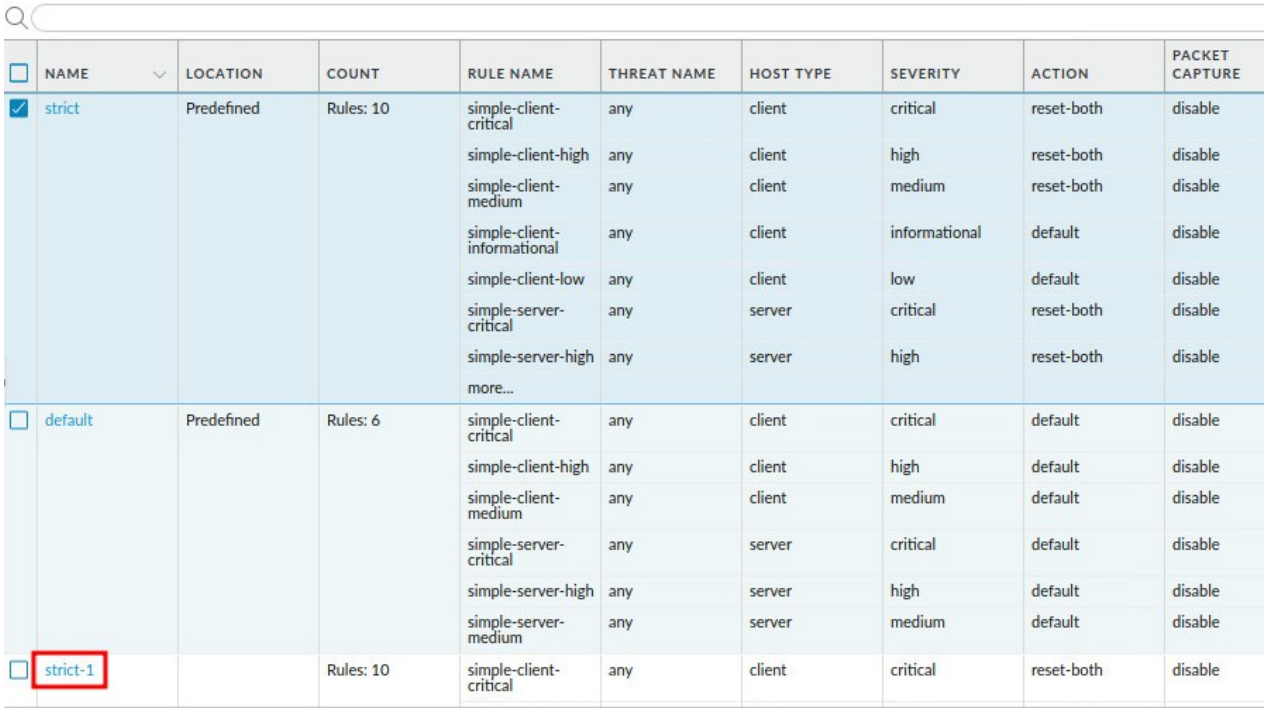
2. Click the checkbox on the **strict** profile. Then, click the **Clone** button.



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

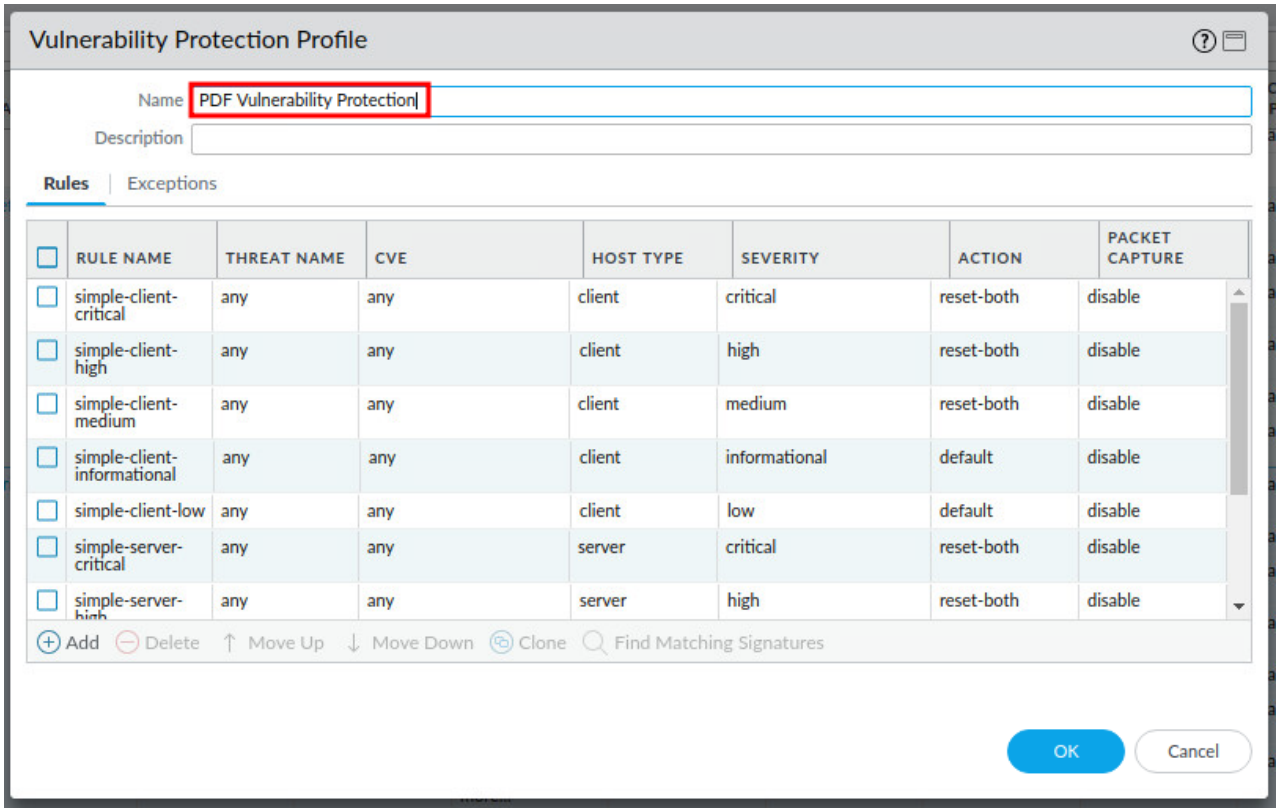


4. Click on **strict-1**.

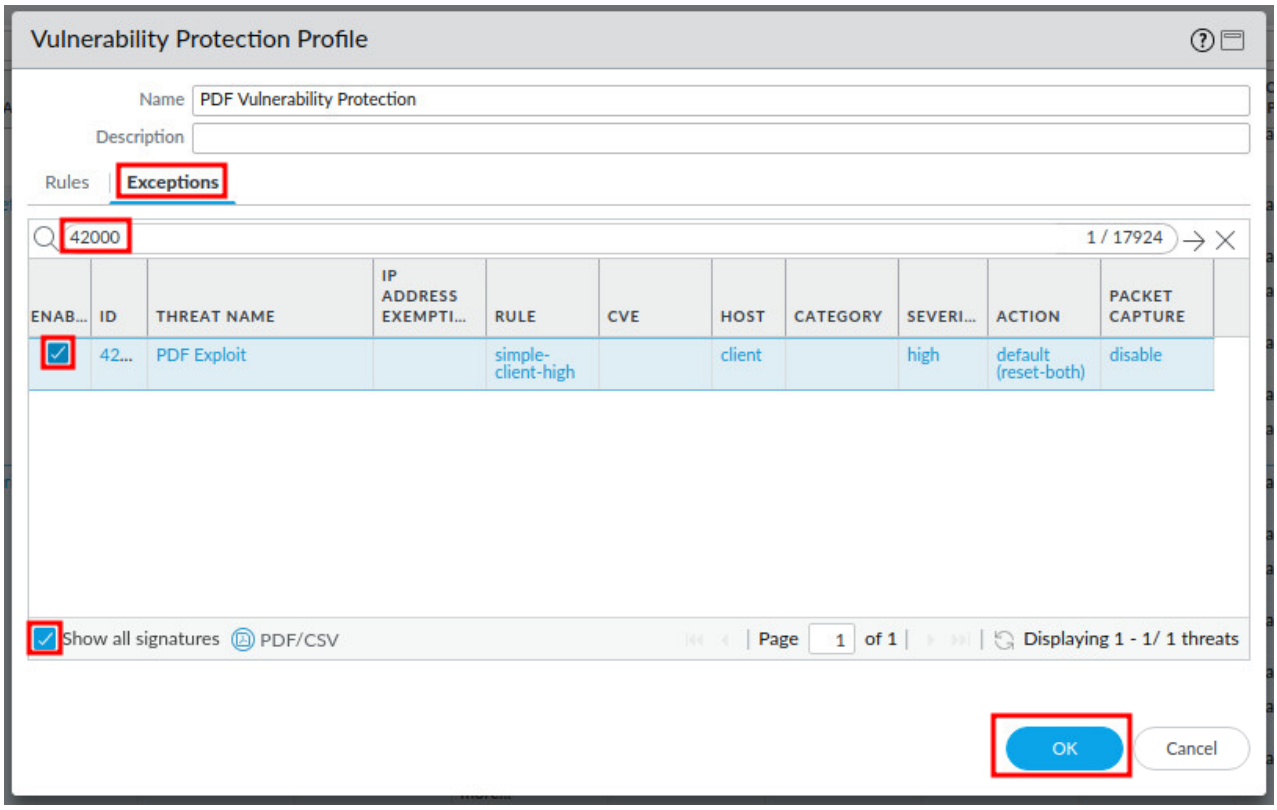


NAME	LOCATION	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
			simple-client-high	any	client	high	reset-both	disable
			simple-client-medium	any	client	medium	reset-both	disable
			simple-client-informational	any	client	informational	default	disable
			simple-client-low	any	client	low	default	disable
			simple-server-critical	any	server	critical	reset-both	disable
			simple-server-high	any	server	high	reset-both	disable
			more...					
default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable
			simple-client-high	any	client	high	default	disable
			simple-client-medium	any	client	medium	default	disable
			simple-server-critical	any	server	critical	default	disable
			simple-server-high	any	server	high	default	disable
			simple-server-medium	any	server	medium	default	disable
strict-1		Rules: 10	simple-client-critical	any	client	critical	reset-both	disable

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



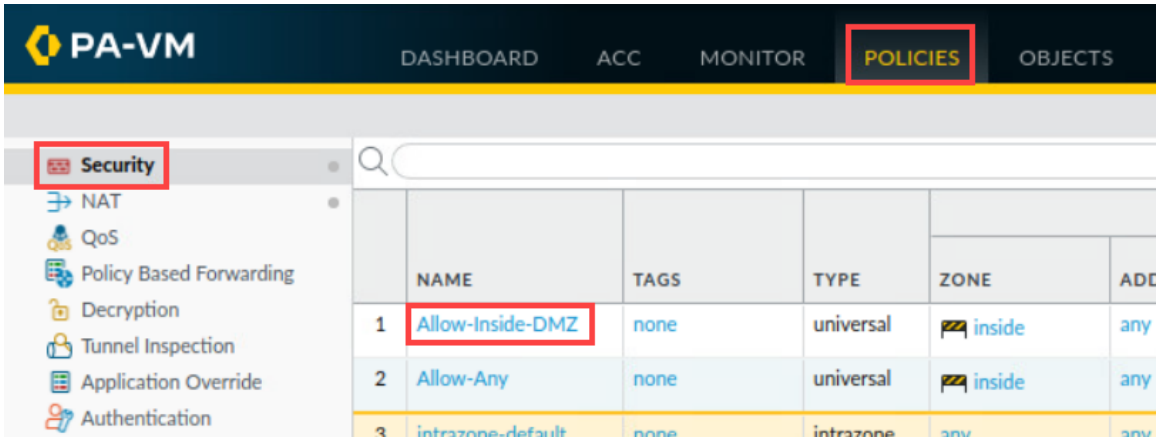
6. In the *Vulnerability Protection Profile* window, click the **Exceptions** tab. Type `42000` in the search box. Then, click the checkbox for **Show all signatures**. Next, click the **Enable** checkbox for the **PDF Exploit** signature. Finally, click the **OK** button.



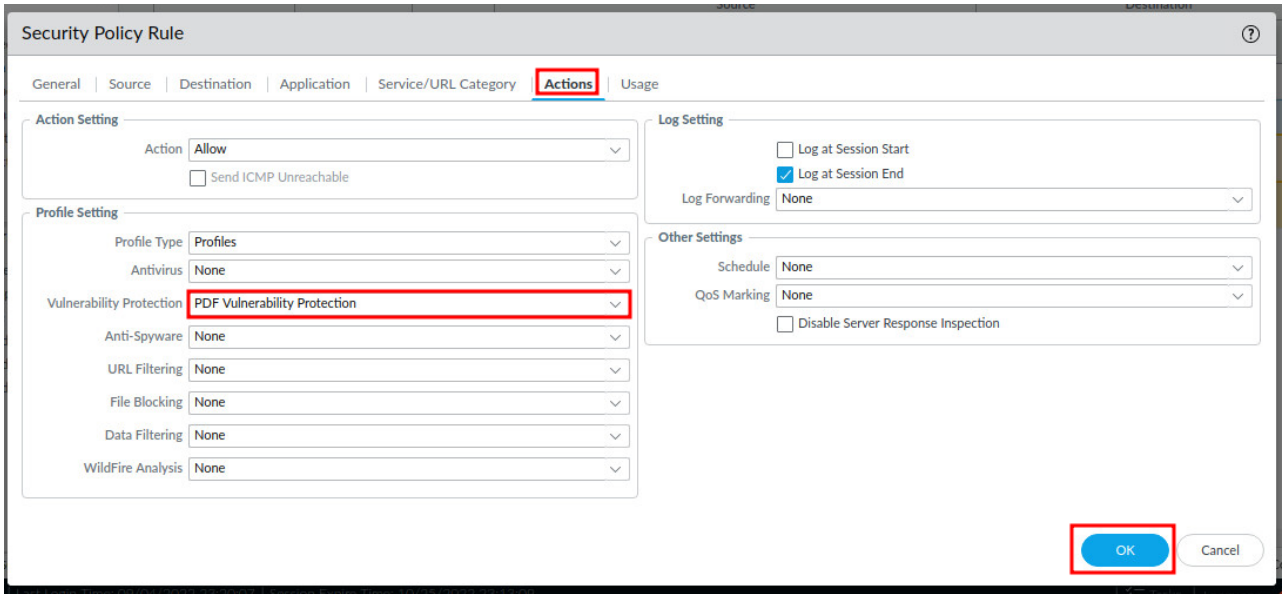
1.5 Apply Custom Vulnerability Protection Profile to a Security Policy

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

1. Navigate to **Policies > Security > Allow-Inside-DMZ**.



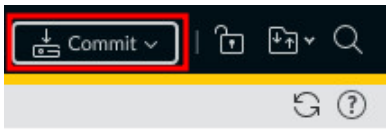
2. In the *Security Policy Rule* window, select the **Actions** tab. Then, select **Profiles** from the *Profile Type* dropdown. Next, select **PDF Vulnerability Protection** from the *Vulnerability Protection* dropdown. Finally, click on the **OK** button.



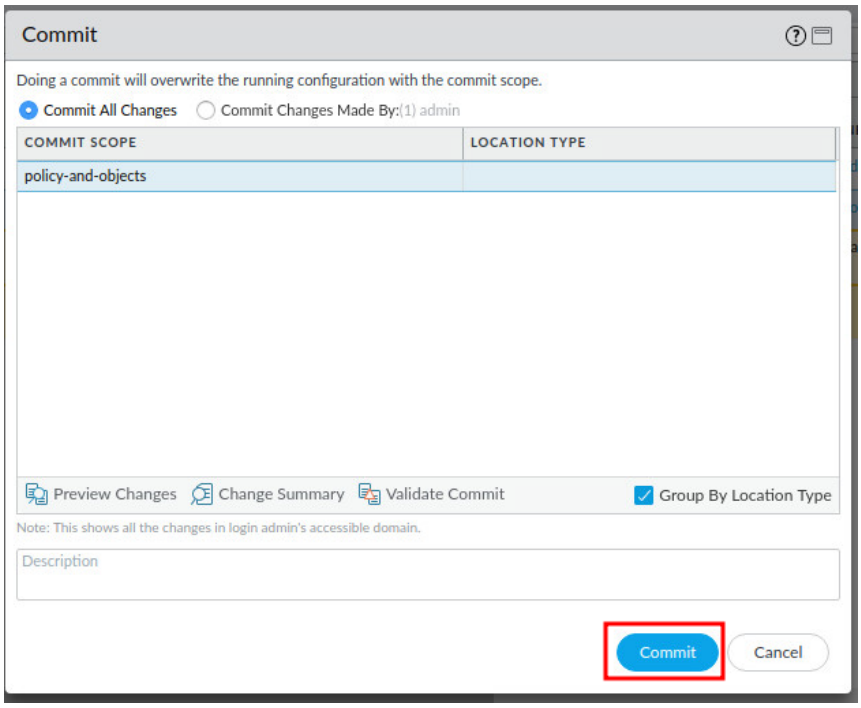
1.6 Commit and Test Vulnerability Protection

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.

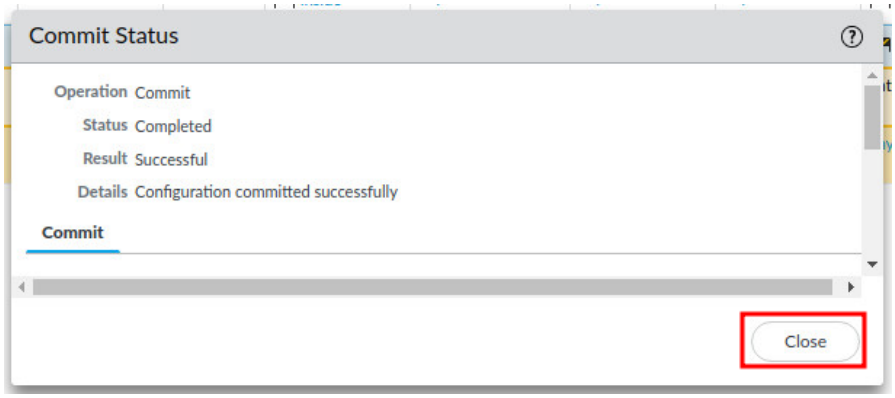
1. Click the **Commit** link located at the top-right of the web interface.



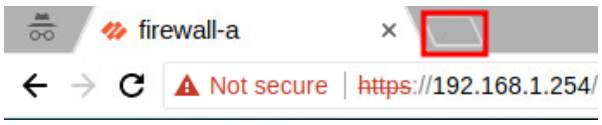
2. In the *Commit* window, click **Commit** to proceed with committing the changes.



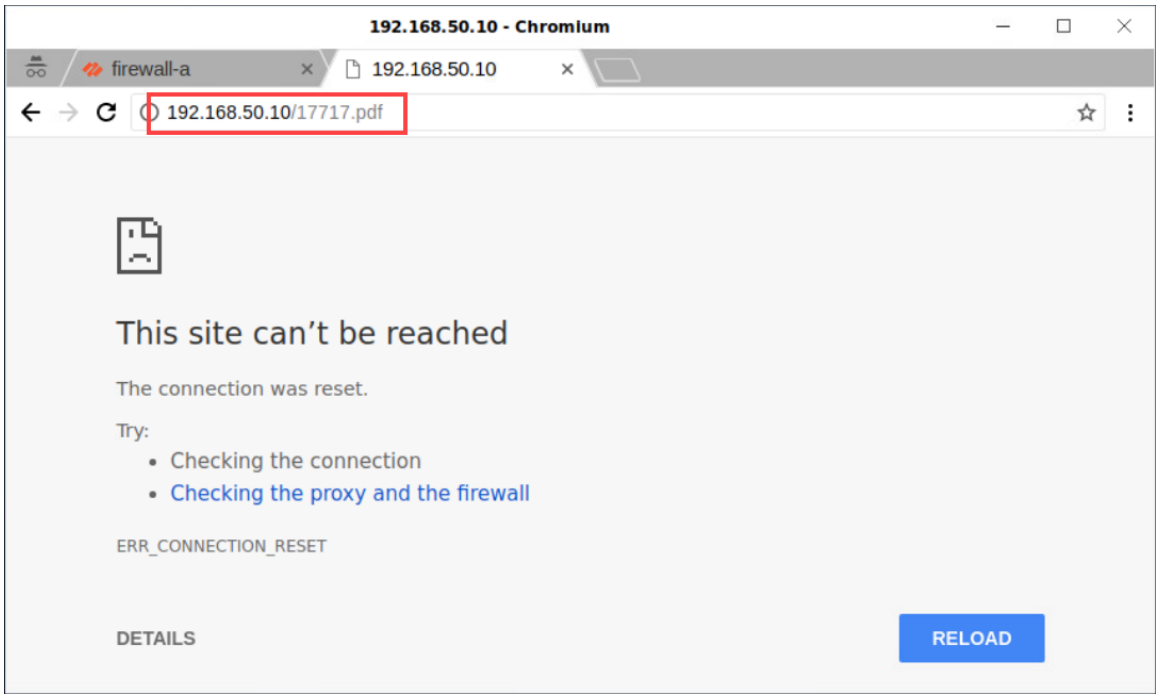
3. When the commit operation successfully completes, click **Close** to continue.



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

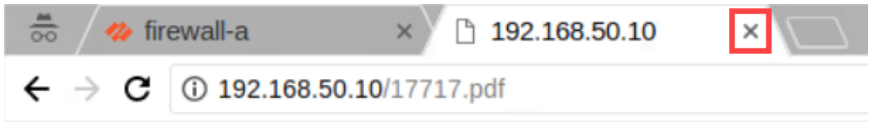


5. In the address bar, type `http://192.168.50.10/17717.pdf` and press **Enter**.

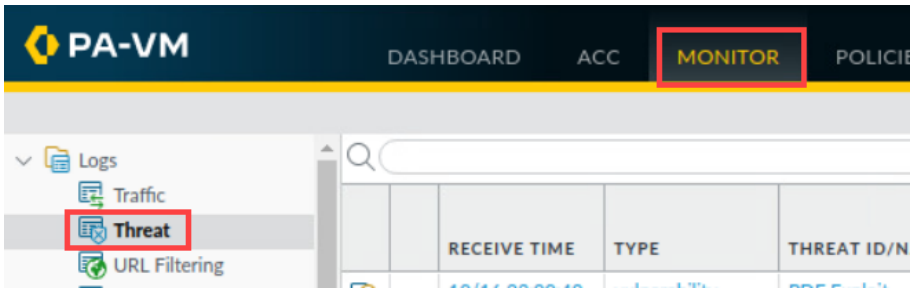


Notice the error message, *This site can't be reached.* This is because the connection was reset by the Firewall to stop the exploit.

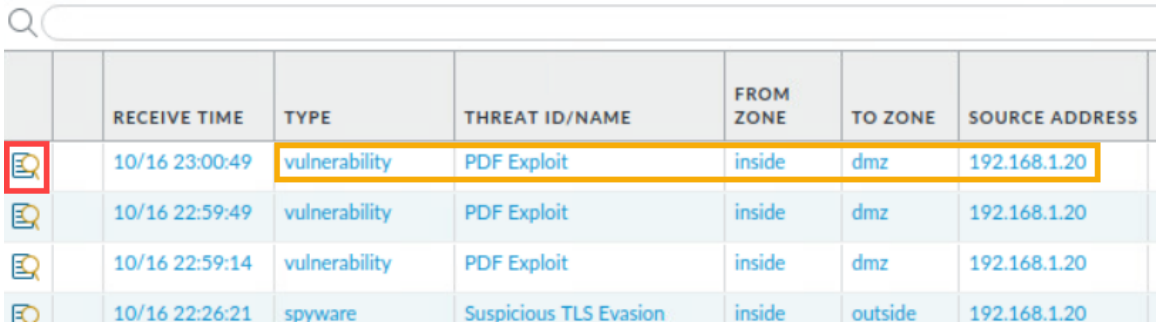
6. Click the **X** on the *192.168.50.10* tab.



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

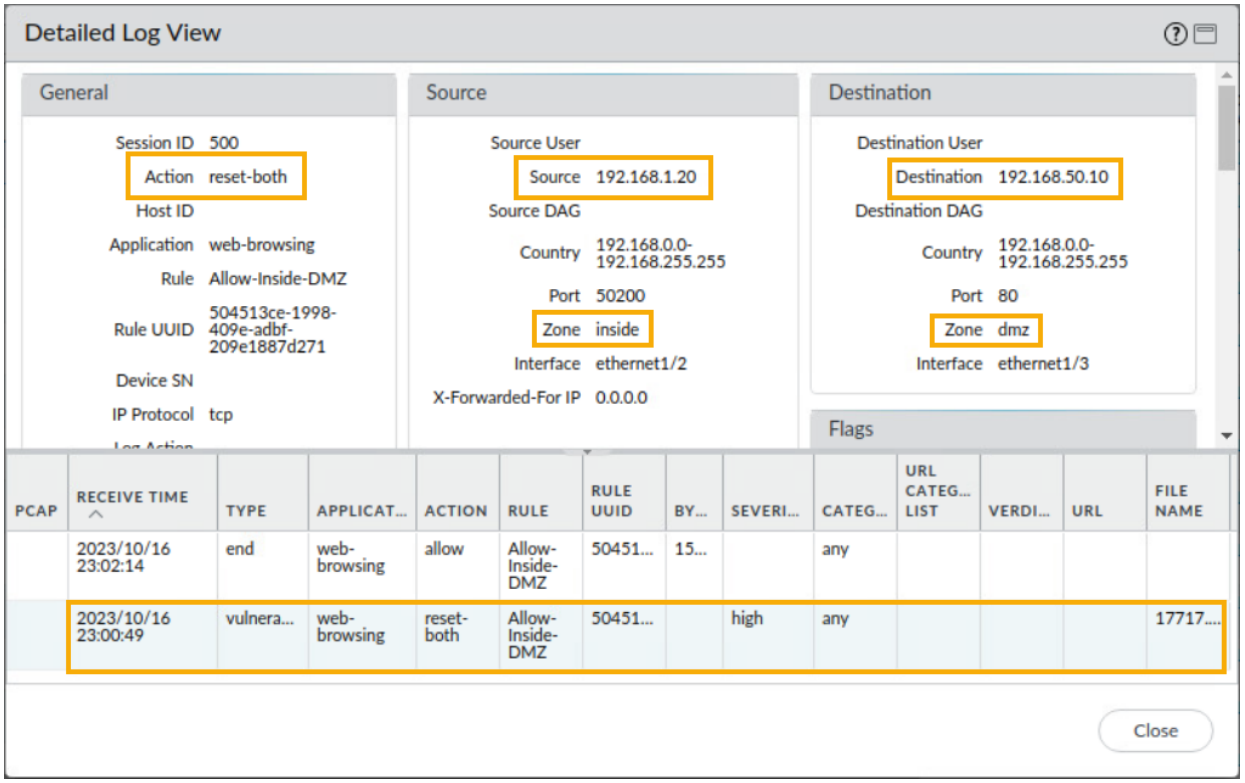


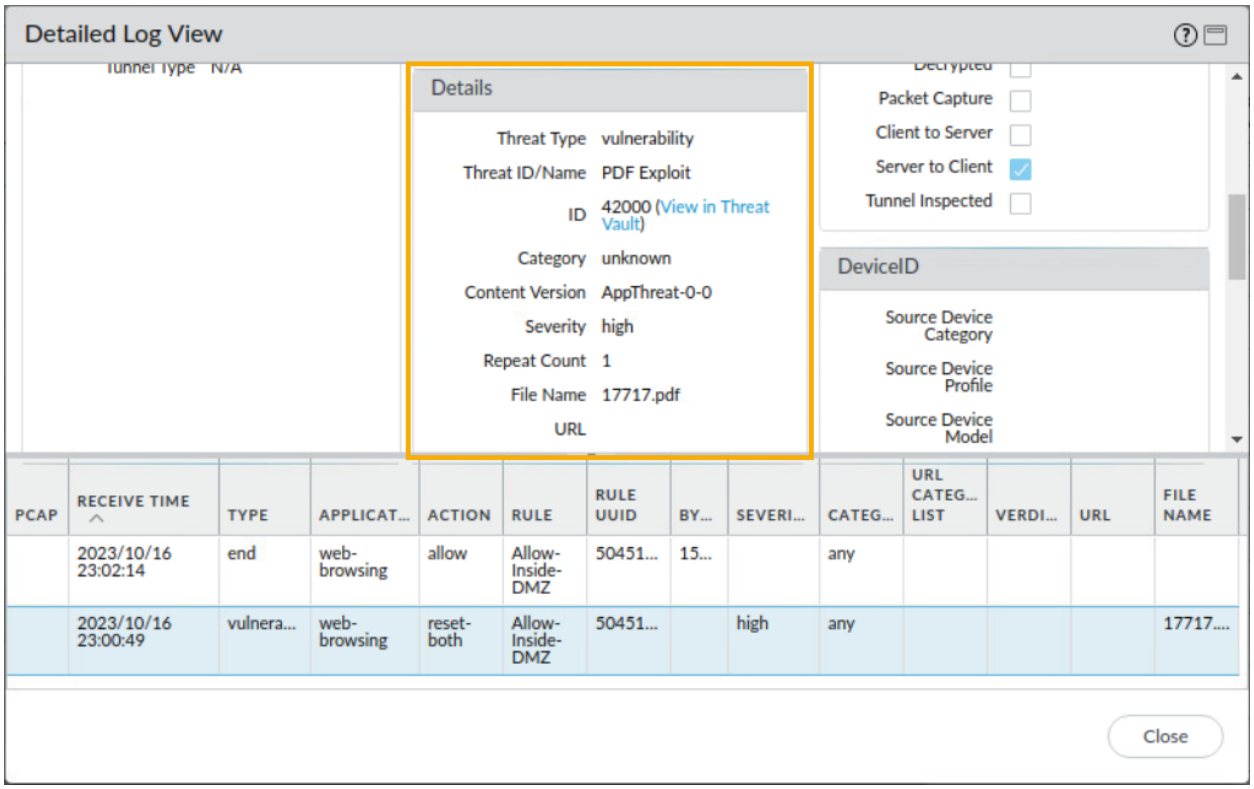
8. Notice the threats listed (make sure that the search filter is cleared). Click on the **Detailed Log View** button.



	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS
	10/16 23:00:49	vulnerability	PDF Exploit	inside	dmz	192.168.1.20
	10/16 22:59:49	vulnerability	PDF Exploit	inside	dmz	192.168.1.20
	10/16 22:59:14	vulnerability	PDF Exploit	inside	dmz	192.168.1.20
	10/16 22:26:21	spyware	Suspicious TLS Evasion	inside	outside	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. Scroll down and 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.





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

