



PAN9 CYBERSECURITY ESSENTIALS

Lab 8: Securing Endpoints using Vulnerability Profiles

Document Version: 2020-06-08

Copyright © 2020 Network Development Group, Inc.
www.netdevgroup.com

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

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

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
8 Lab: Securing Endpoints Using Vulnerability Profiles	6
8.0 Load Lab Configuration	6
8.1 Install the Latest Dynamic Updates of Antivirus	11
8.2 Install Manual Update of Applications and Threats.....	13
8.3 Create a Custom Vulnerability Signature	17
8.4 Clone a Vulnerability Protection Profile.....	21
8.5 Apply Custom Vulnerability Protection Profile to a Security Policy	24
8.6 Commit and Test Vulnerability Protection	25

Introduction

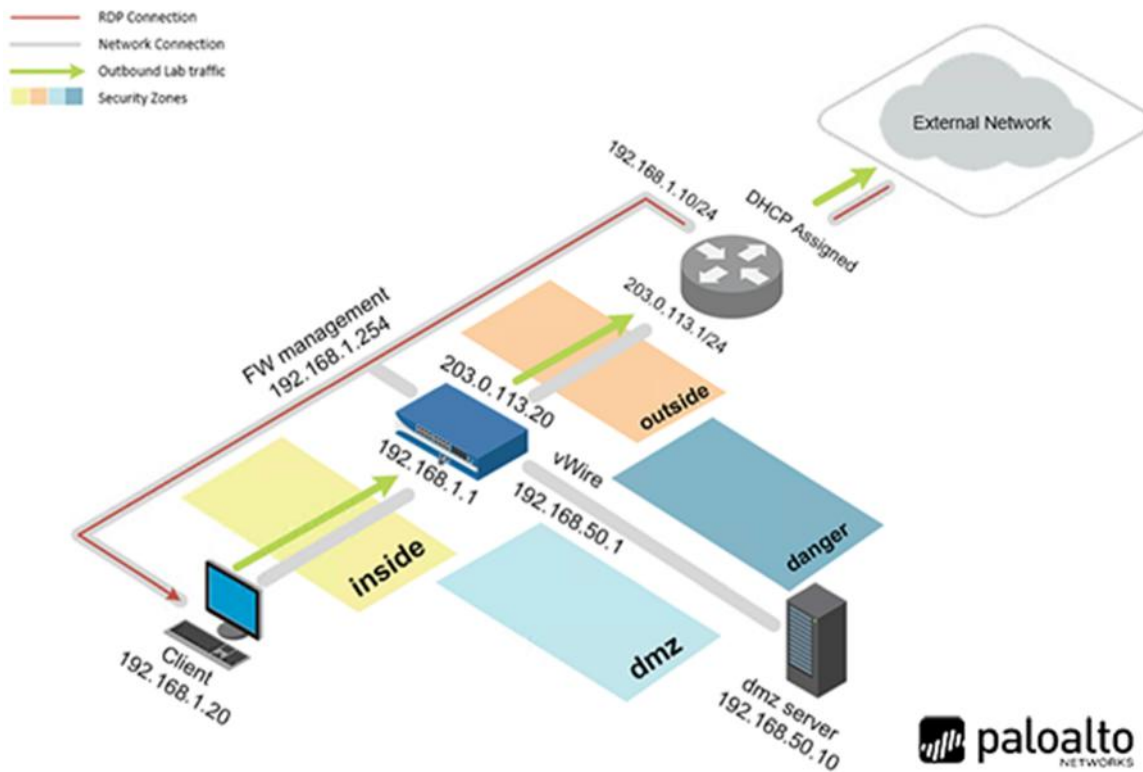
In this lab, you will secure an endpoint by blocking a PDF file with a Custom Vulnerability Object and Vulnerability Protection Profile. Palo Alto Networks Firewalls support the use of custom vulnerability signatures that can be written with expression patterns to identify vulnerability exploits. Vulnerability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

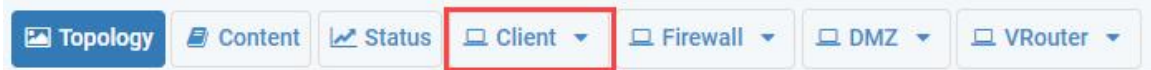
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng\$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng\$

8 Lab: Securing Endpoints Using Vulnerability Profiles

8.0 Load Lab Configuration

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

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



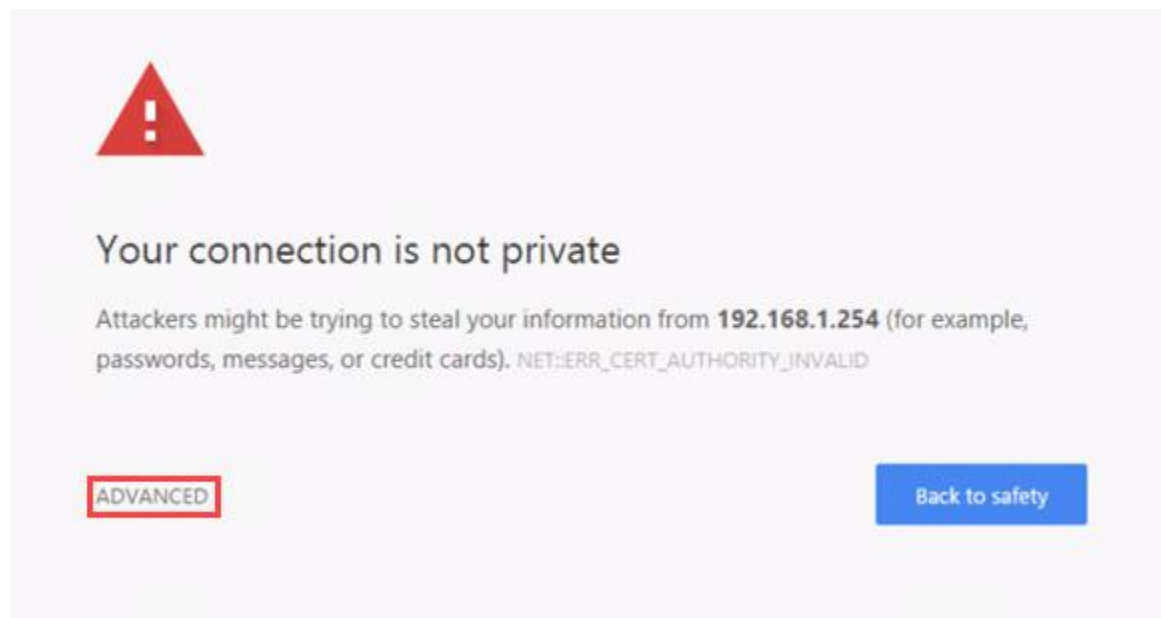
2. Log in to the Client PC as username **lab-user**, password **Train1ng\$**.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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.





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

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

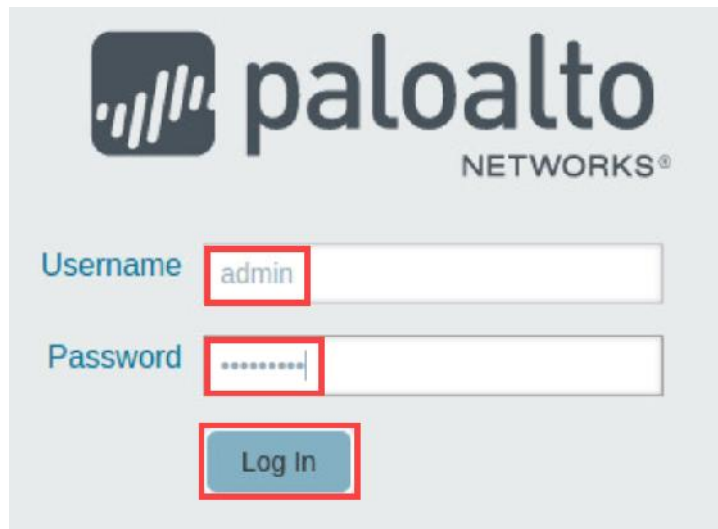
HIDE ADVANCED

Back to safety

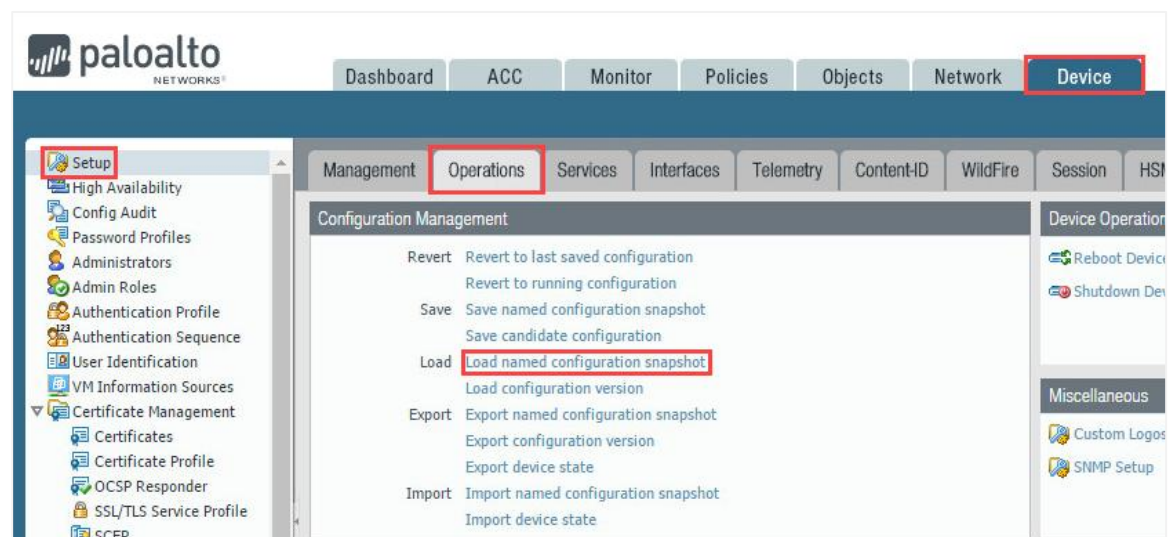
This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. [Learn more](#).

Proceed to 192.168.1.254 (unsafe)

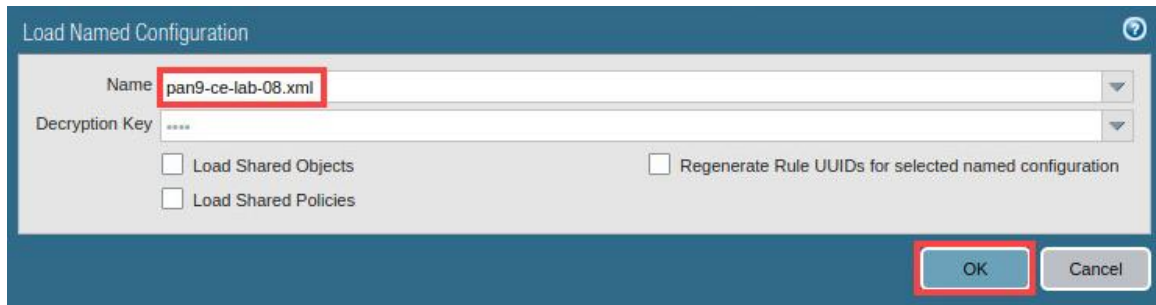
7. Log in to the Firewall web interface as username **admin**, password **Train1ng\$**.



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

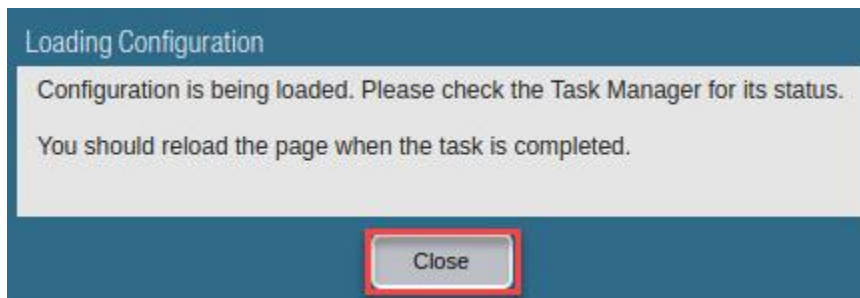


9. In the *Load Named Configuration* window, select **pan9-ce-lab-08.xml** from the *Name* dropdown box and click **OK**.



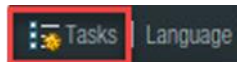
The dialog box titled "Load Named Configuration" has a "Name" dropdown menu with "pan9-ce-lab-08.xml" selected. Below it is a "Decryption Key" field with four asterisks. There are two checkboxes: "Load Shared Objects" and "Load Shared Policies", both of which are unchecked. To the right, there is a checkbox labeled "Regenerate Rule UUIDs for selected named configuration", which is also unchecked. At the bottom right, there are "OK" and "Cancel" buttons.

10. 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.

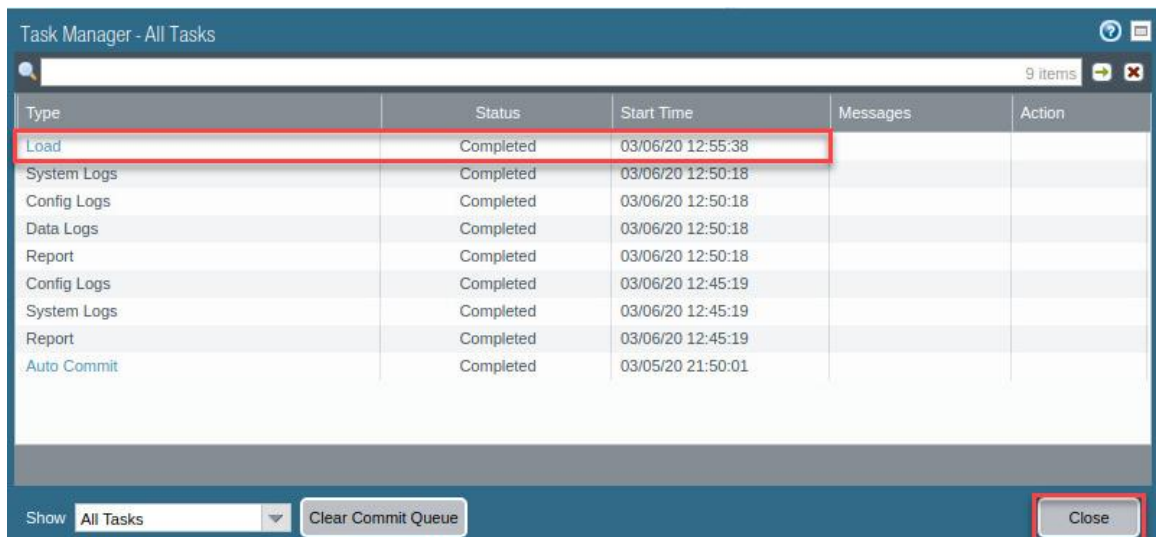


The "Loading Configuration" message box contains the text: "Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed." At the bottom center, there is a "Close" button.

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**.



The "Task Manager - All Tasks" window displays a table with the following data:

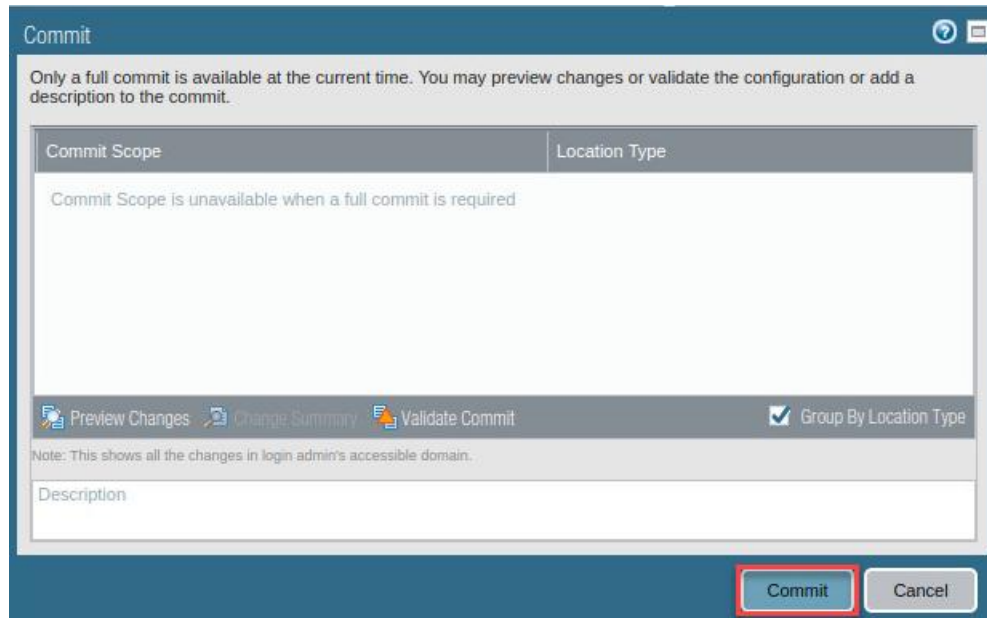
Type	Status	Start Time	Messages	Action
Load	Completed	03/06/20 12:55:38		
System Logs	Completed	03/06/20 12:50:18		
Config Logs	Completed	03/06/20 12:50:18		
Data Logs	Completed	03/06/20 12:50:18		
Report	Completed	03/06/20 12:50:18		
Config Logs	Completed	03/06/20 12:45:19		
System Logs	Completed	03/06/20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

At the bottom of the window, there is a "Show" dropdown menu set to "All Tasks", a "Clear Commit Queue" button, and a "Close" button.

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.

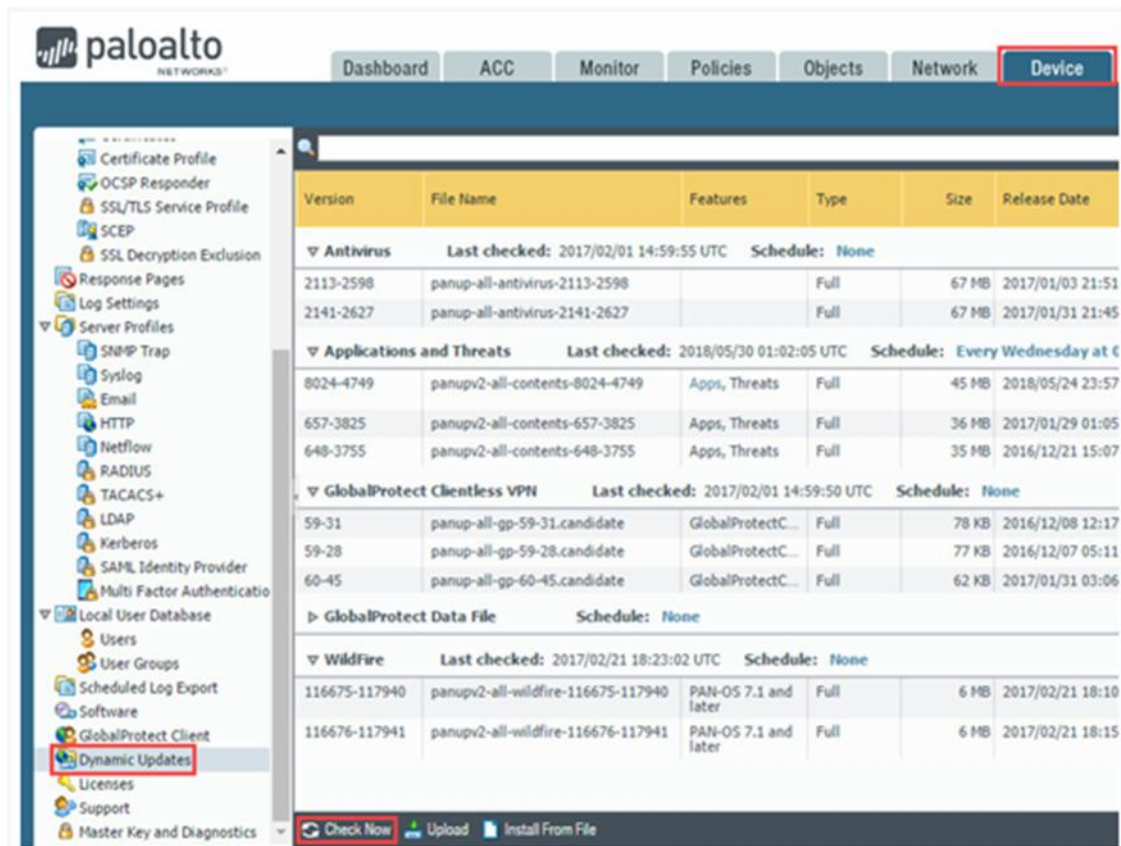


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

8.1 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.



The screenshot shows the Palo Alto Networks management console. The 'Device' tab is selected in the top navigation bar. In the left sidebar, 'Dynamic Updates' is highlighted under the 'Server Profiles' section. The main content area displays a table of updates for Antivirus, Applications and Threats, GlobalProtect Clientless VPN, and Wildfire. The 'Antivirus' section is expanded, showing a table of updates with columns: Version, File Name, Features, Type, Size, and Release Date. The 'Check Now' button is visible at the bottom of the update list.

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 6					
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

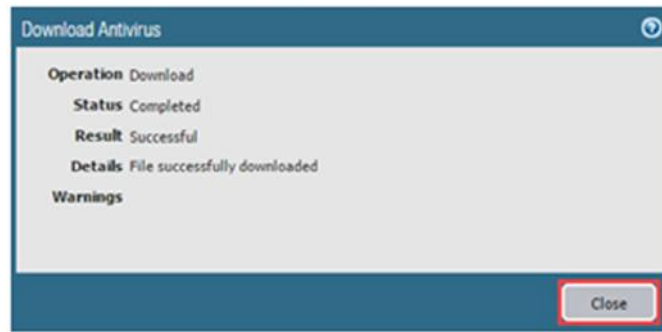
2. Under the Antivirus update, click **Download** on the latest update.

Antivirus Last checked: 2020/03/16 11:00:46 UTC Schedule: None							
3287-3798	panup-all-antivirus-3287-3798	Full	106 MB	2020/03/16 11:00:46 UTC		Download	Release Notes
3286-3797	panup-all-antivirus-3286-3797	Full	106 MB	2020/03/15 11:03:29 UTC		Download	Release Notes
3285-3796	panup-all-antivirus-3285-3796	Full	106 MB	2020/03/14 11:01:38 UTC		Download	Release Notes



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.



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

Antivirus		Last checked: 2020/03/15 18:14:16 UTC		Schedule: None					
3287-3798	panup-all-antivirus-3287-3798	Full	106 MB	2020/03/16 11:00:46 UTC	✓			Install	
3286-3797	panup-all-antivirus-3286-3797	Full	106 MB	2020/03/15 11:03:29 UTC				Download	

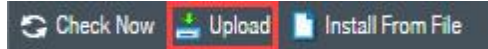
5. In the *Install Antivirus* window, after the update is successfully installed, click the **Close** button.



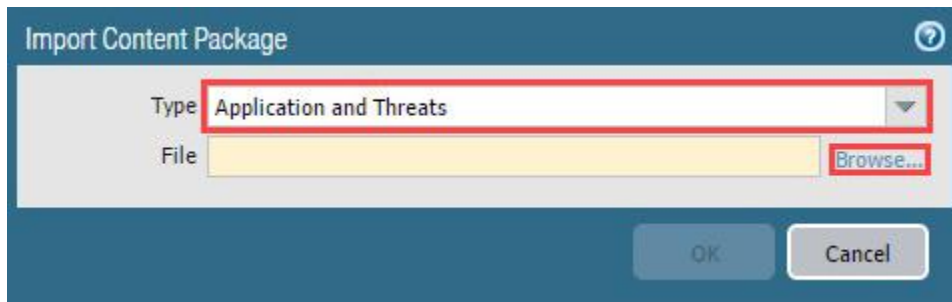
8.2 Install Manual Update of Applications and Threats

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.

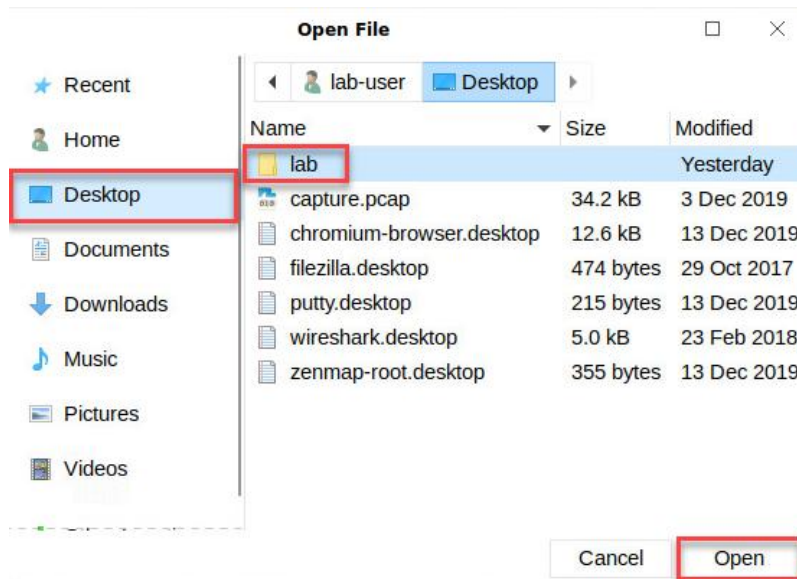
1. To upload the file from the Customer Support Portal, click on the **Upload** button at the bottom.



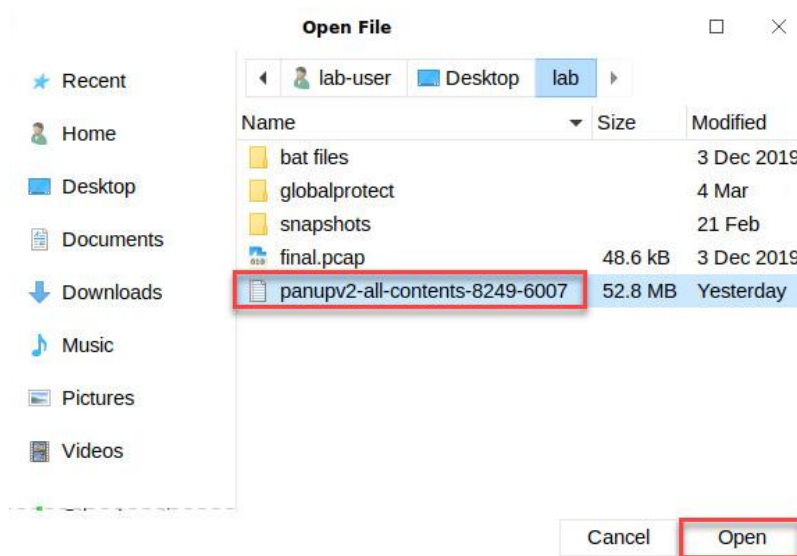
2. In the *Import Content Package* window, select **Application and Threats** from the *Type* dropdown. Then, click on **Browse...**



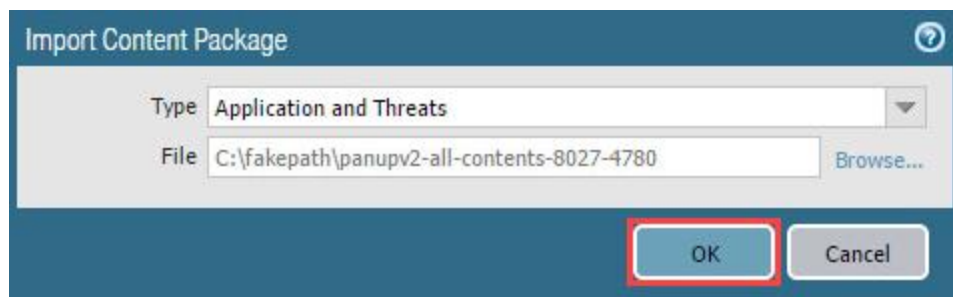
3. In the *Open File* window, select **Desktop**, click the **lab** folder. Lastly, click **Open**.



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



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



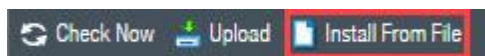


This may take several minutes to complete.

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



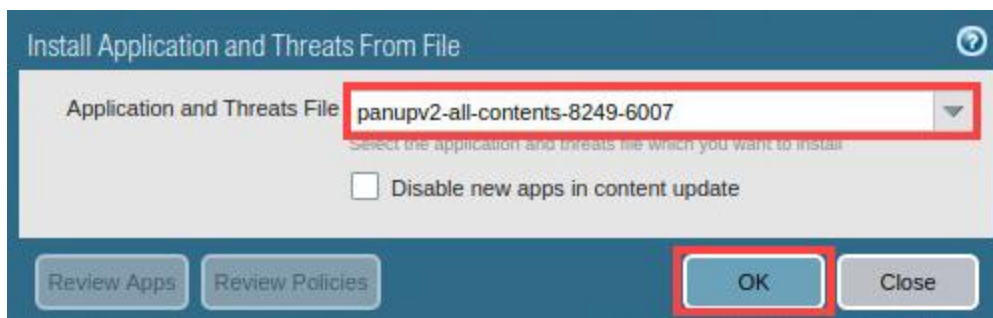
- With the file uploaded, you can begin the install. Click on **Install From File** at the bottom.



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



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





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.

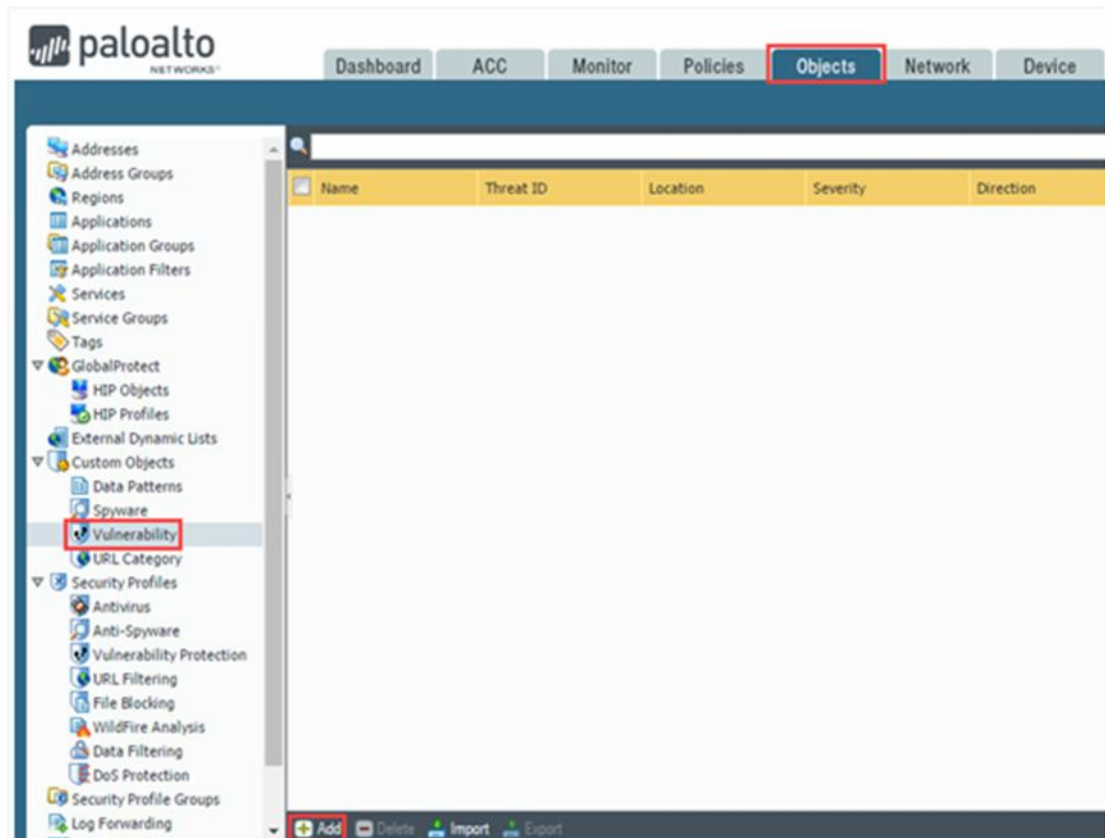
10. In the *Install Application and Threats From File* window, click on the **Close** button.



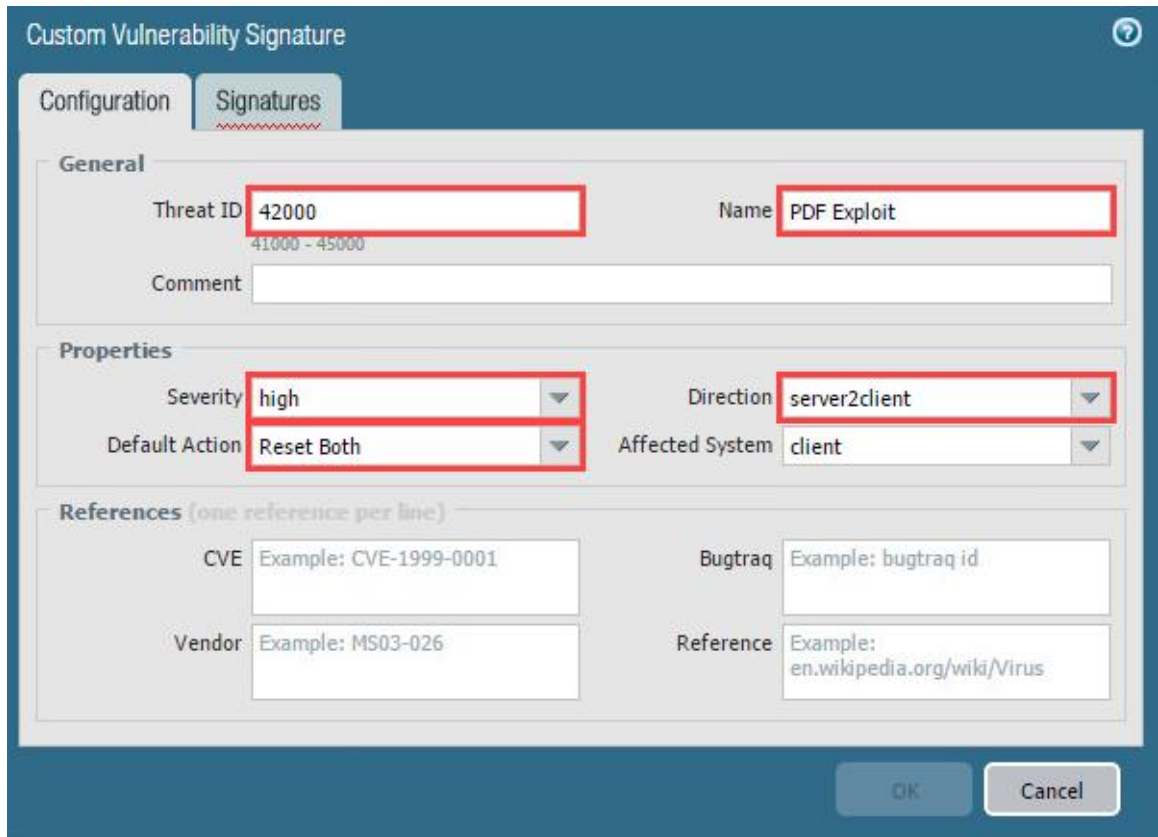
8.3 Create a Custom Vulnerability Signature

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**.



- 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.



Custom Vulnerability Signature

Configuration | **Signatures**

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

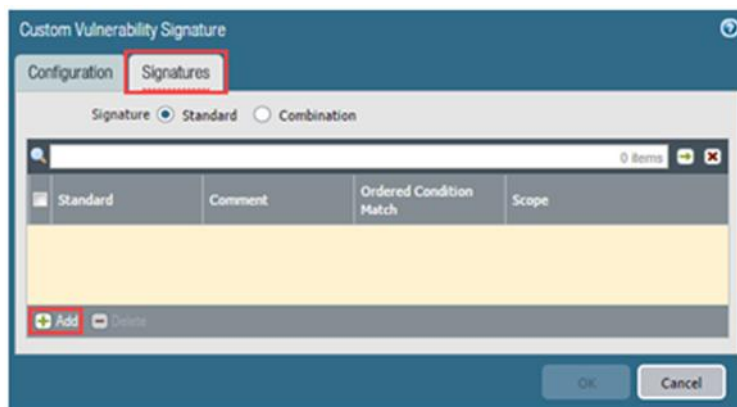
Reference: Example: en.wikipedia.org/wiki/Virus

OK Cancel



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.

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



Custom Vulnerability Signature

Configuration | **Signatures**

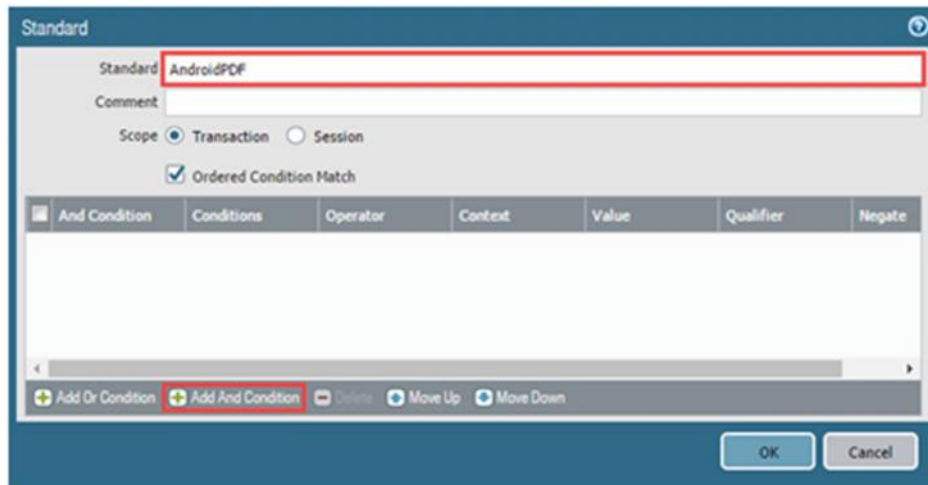
Signature: ☒ Standard ☐ Combination

Standard	Comment	Ordered Condition Match	Scope

Add **Delete**

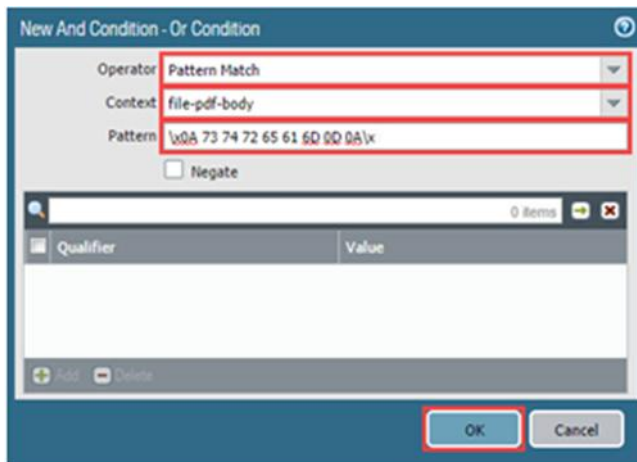
OK Cancel

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



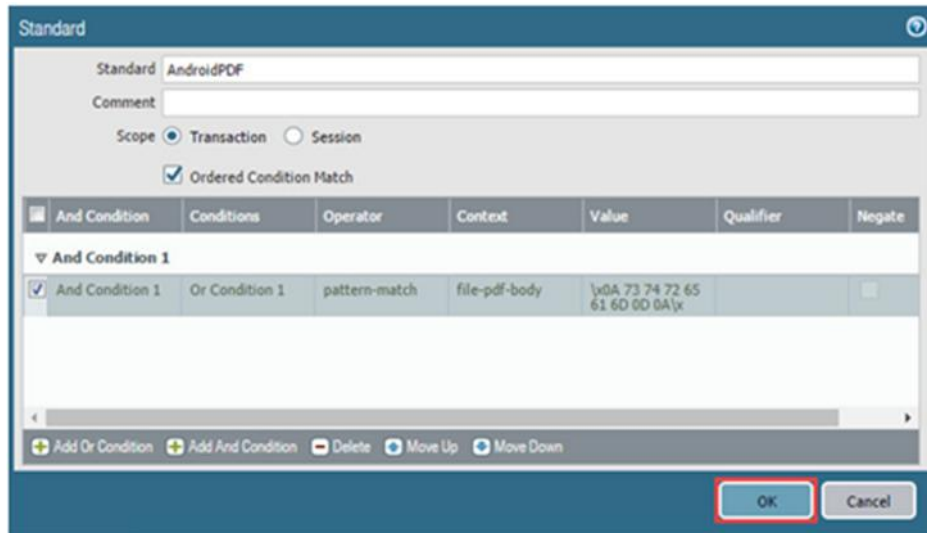
The screenshot shows the 'Standard' configuration window. The 'Standard' field is highlighted with a red box and contains the text 'AndroidPDF'. Below it, the 'Scope' is set to 'Transaction' and 'Ordered Condition Match' is checked. A table with columns 'And Condition', 'Conditions', 'Operator', 'Context', 'Value', 'Qualifier', and 'Negate' is visible. At the bottom, the 'Add And Condition' button is highlighted with a red box. 'OK' and 'Cancel' buttons are at the bottom right.

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.



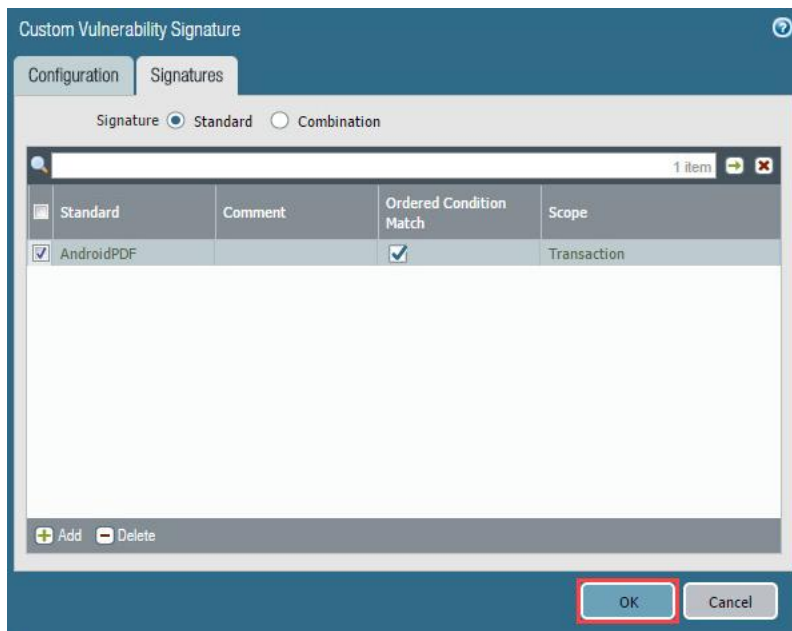
The screenshot shows the 'New And Condition - Or Condition' window. The 'Operator' dropdown is set to 'Pattern Match', the 'Context' dropdown is set to 'file-pdf-body', and the 'Pattern' field contains the hex string '\x0A 73 74 72 65 61 6D 0D 0A\x'. The 'Negate' checkbox is unchecked. Below these fields is a table with columns 'Qualifier' and 'Value'. At the bottom, the 'OK' button is highlighted with a red box. 'Add', 'Delete', 'OK', and 'Cancel' buttons are at the bottom.

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



The **Standard** window box is shown. It has a title bar with a question mark icon. Below the title bar, there is a text field labeled "Standard" containing "AndroidPDF". Below that is a text field labeled "Comment". Then, there are two radio buttons: "Transaction" (selected) and "Session". Below these is a checkbox labeled "Ordered Condition Match" which is checked. A table with 7 columns is shown: "And Condition", "Conditions", "Operator", "Context", "Value", "Qualifier", and "Negate". Under the "And Condition" column, there is a section titled "And Condition 1" with a dropdown arrow. Below this, there is a row with a checked checkbox, "And Condition 1", "Or Condition 1", "pattern-match", "file-pdf-body", a hex string value, and a checked checkbox in the "Negate" column. At the bottom of the table, there are five buttons: "Add Or Condition", "Add And Condition", "Delete", "Move Up", and "Move Down". At the bottom right of the window, there are two buttons: "OK" (highlighted with a red box) and "Cancel".

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

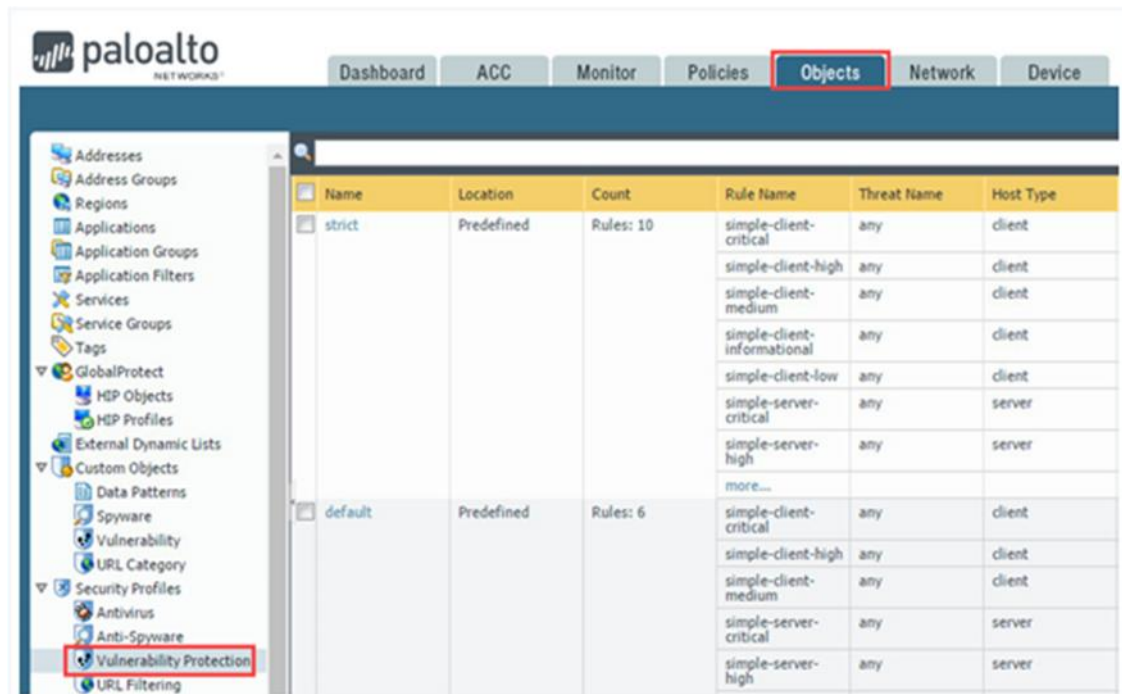


The **Custom Vulnerability Signature** window is shown. It has a title bar with a question mark icon. Below the title bar, there are two tabs: "Configuration" and "Signatures" (selected). Below the tabs, there are two radio buttons: "Standard" (selected) and "Combination". Below these is a list box with a search icon, a text field, and a "1 item" label. Below the list box is a table with 4 columns: "Standard", "Comment", "Ordered Condition Match", and "Scope". There is one row with a checked checkbox, "AndroidPDF", a checked checkbox, and "Transaction". At the bottom left of the table, there are two buttons: "Add" and "Delete". At the bottom right of the window, there are two buttons: "OK" (highlighted with a red box) and "Cancel".

8.4 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 to 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.

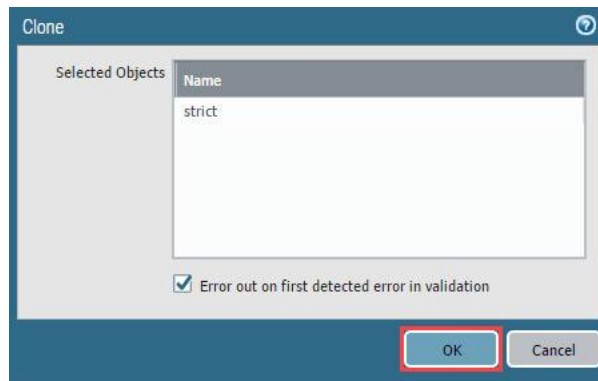
1. Navigate to **Objects > Security Profiles > Vulnerability Protection**.



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



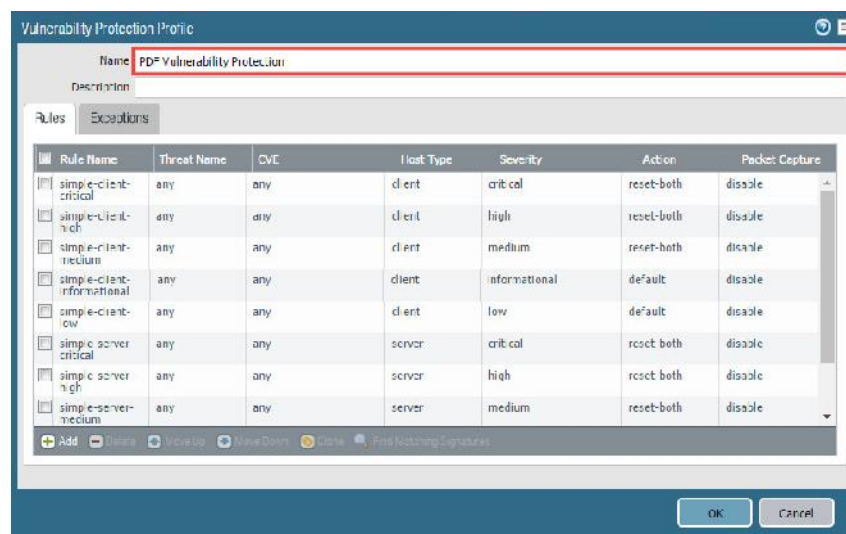
3. In the *Clone* window, click the **OK** button.



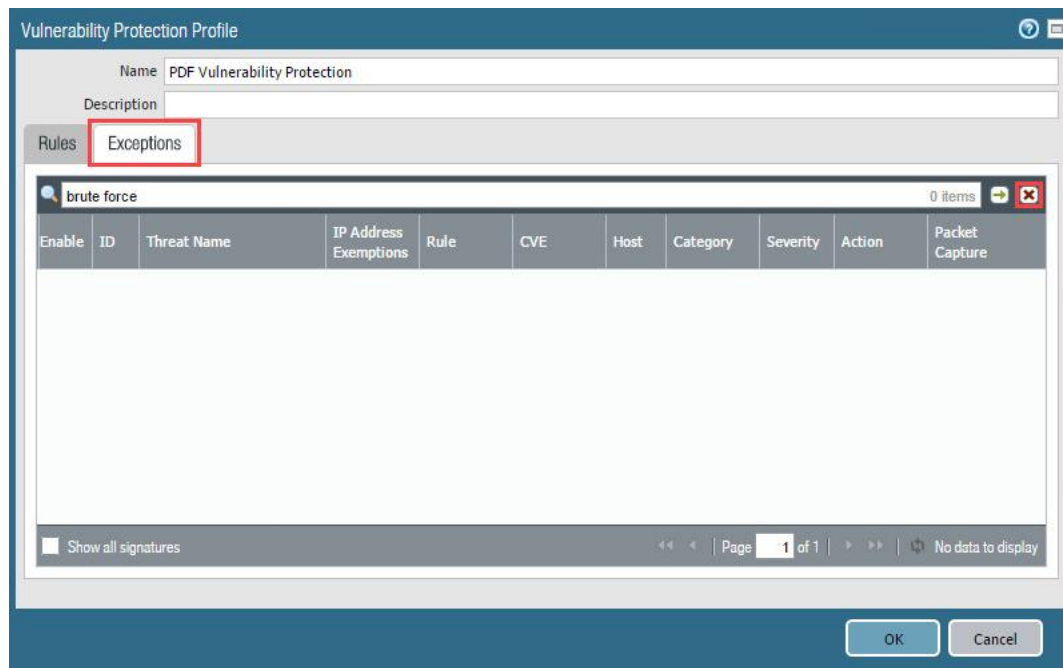
4. Click on **strict-1**.

	Name	Location	Count	Rule Name	Threat Name	Host Type	Severity
<input checked="" type="checkbox"/>	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...			
<input type="checkbox"/>	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
<input type="checkbox"/>	strict-1		Rules: 10	simple-client-critical	any	client	critical
				simple-client-high	any	client	high
				simple-client-medium	any	client	medium

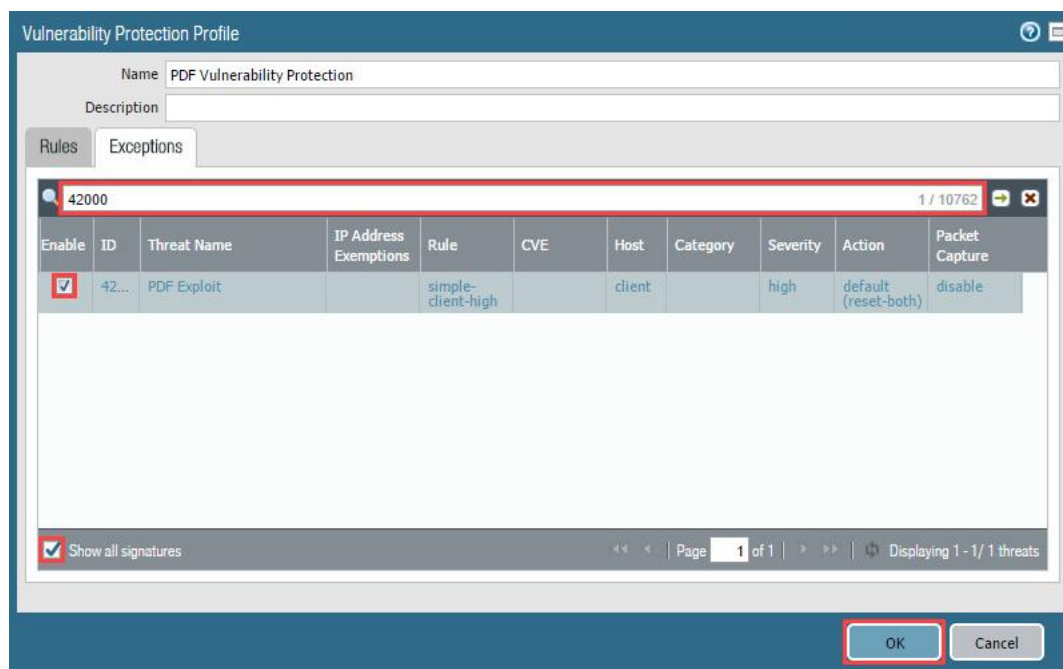
5. In the *Vulnerability Protection Profile* window, type **PDF vulnerability Protection** in the *Name* field.



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



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.



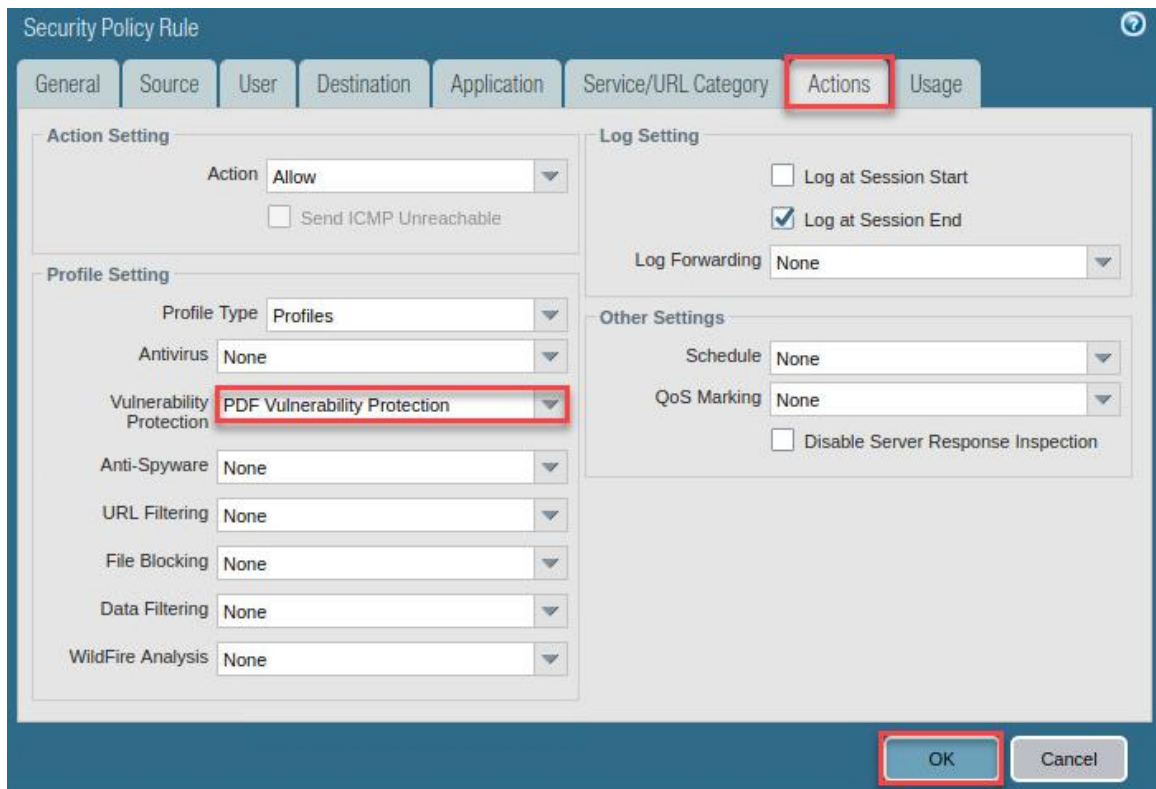
8.5 Apply Custom Vulnerability Protection Profile to a Security Policy

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**.



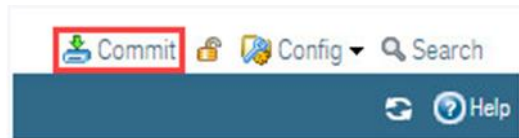
2. In the *Security Policy Rule* window, select the **Actions** tab. Then, select **Profiles** from the *Profile Type* dropdown. Next, select **PDF Vulnerability Protection** from the *Vulnerability Protection* dropdown. Finally, click on the **OK** button.



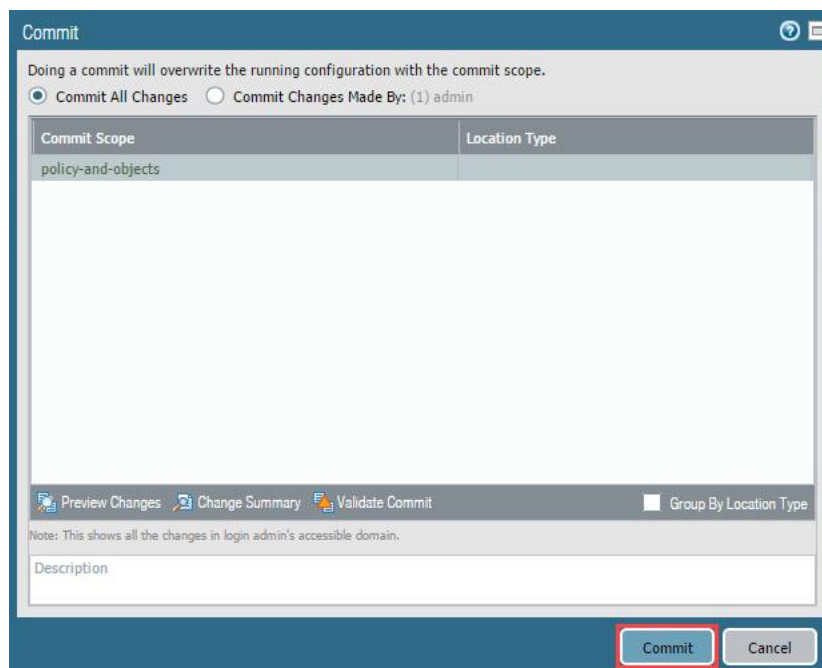
8.6 Commit and Test Vulnerability Protection

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.



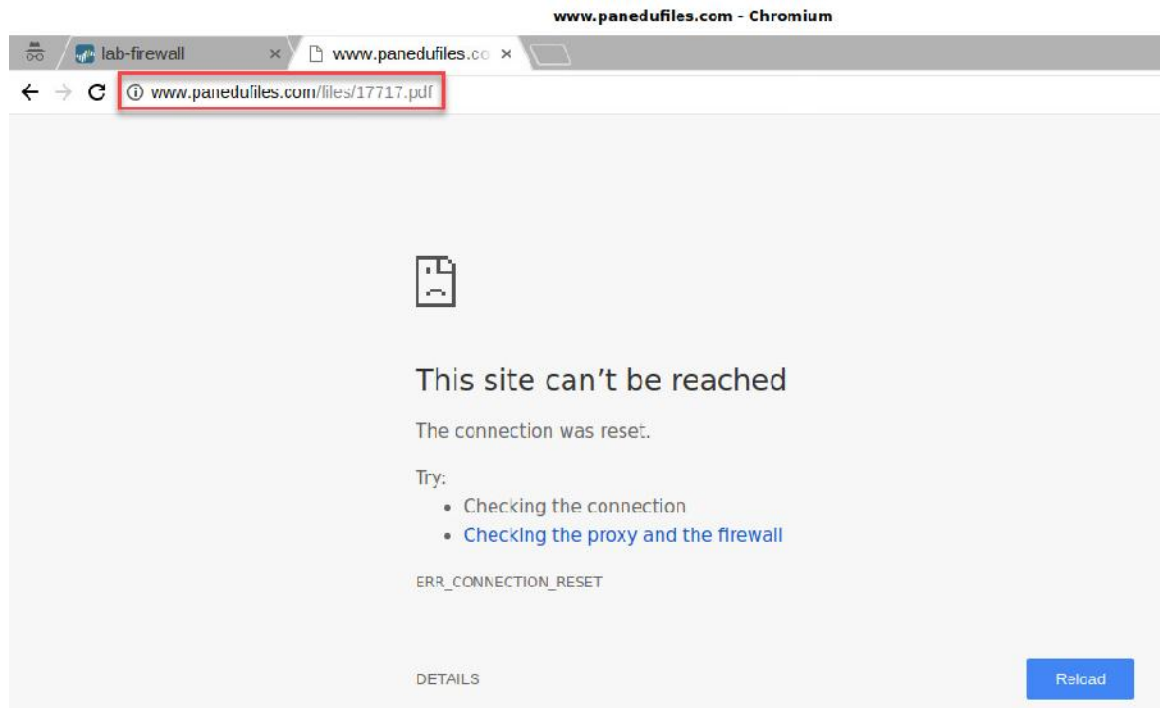
3. When the commit operation successfully completes, click **Close** to continue.



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



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

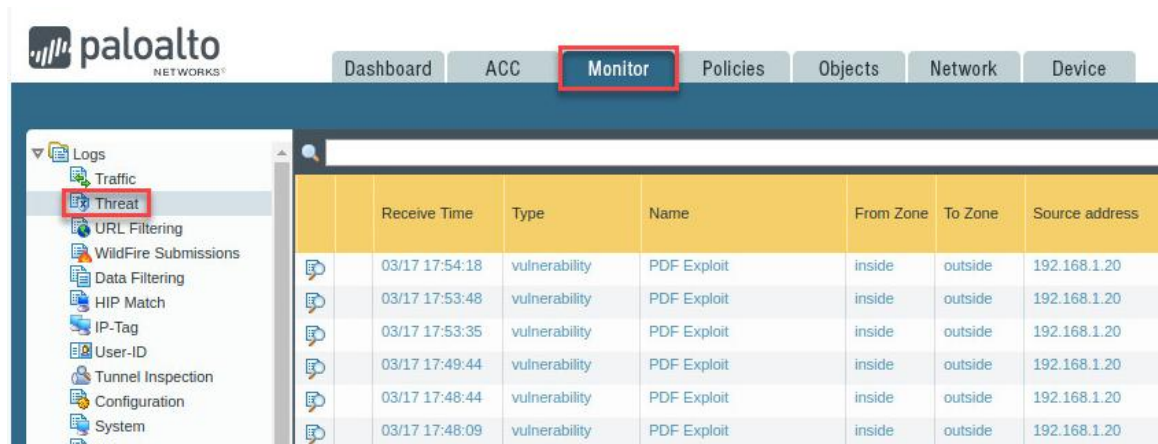


Notice the error message, *This site can't be reached*. This is because the connection was reset by the Firewall to stop the exploit.

- Click the **X** on the `www.panedufiles.com` tab.



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

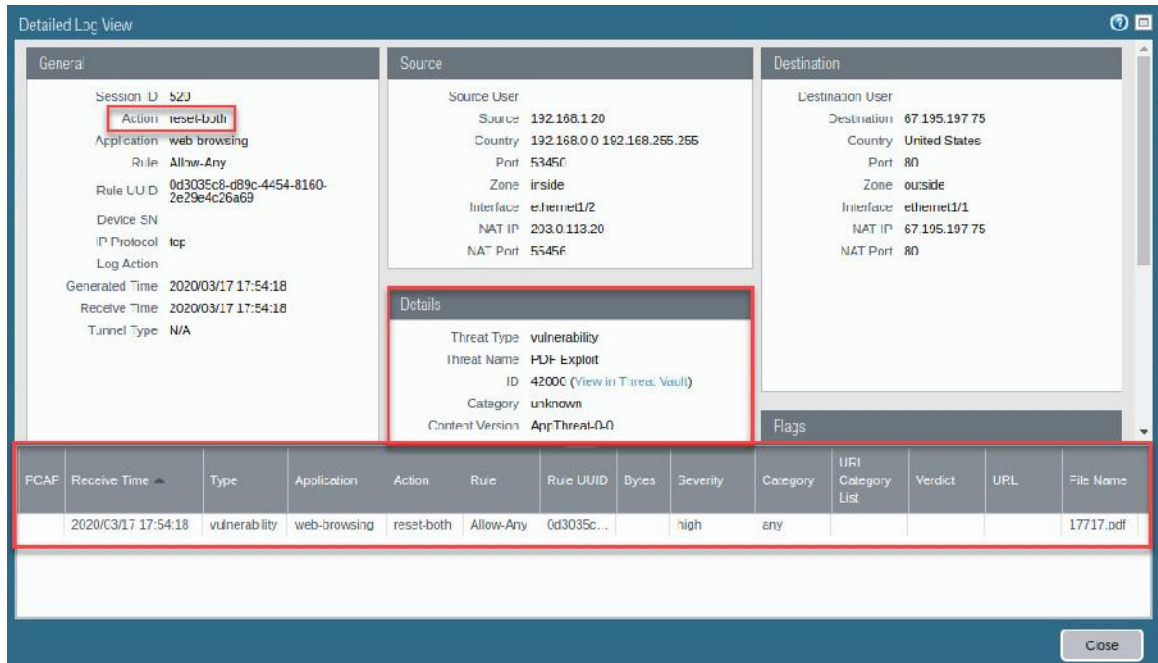


8. Notice the threats listed. Click on the **Detailed Log View** button.



	Receive Time	Type	Name	From Zone	To Zone	Source address
	03/17 17:54:18	vulnerability	PDF Exploit	inside	outside	192.168.1.20
	03/17 17:53:48	vulnerability	PDF Exploit	inside	outside	192.168.1.20
	03/17 17:53:35	vulnerability	PDF Exploit	inside	outside	192.168.1.20
	03/17 17:49:44	vulnerability	PDF Exploit	inside	outside	192.168.1.20
	03/17 17:48:44	vulnerability	PDF Exploit	inside	outside	192.168.1.20
	03/17 17:48:09	vulnerability	PDF Exploit	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. 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.



The screenshot shows the 'Detailed Log View' window with the following sections:

- General:**
 - Session ID: 52J
 - Action: **reset-both** (highlighted with a red box)
 - Application: web browsing
 - Rule: Allow-Any
 - Rule UUID: 0d3035c8-d89c-4454-8160-2e29e4c26a69
 - Device SN:
 - IP Protocol: tcp
 - Log Action:
 - Generated Time: 2020/03/17 17:54:18
 - Receive Time: 2020/03/17 17:54:18
 - Tunnel Type: N/A
- Source:**
 - Source User:
 - Source: 192.168.1.20
 - Country: 192.168.0.0 192.168.255.255
 - Port: 53450
 - Zone: inside
 - Interface: ethernet1/2
 - NAT IP: 203.0.113.20
 - NAT Port: 55456
- Destination:**
 - Destination User:
 - Destination: 67.195.197.75
 - Country: United States
 - Port: 80
 - Zone: outside
 - Interface: ethernet1/1
 - NAT IP: 67.195.197.75
 - NAT Port: 80
- Details:**
 - Threat Type: vulnerability
 - Threat Name: PDF-Exploit
 - ID: 42000C (View in Threat Vault)
 - Category: unknown
 - Content Version: AppThreat-0.0
- Flags:**

At the bottom, there is a table listing sessions related to this log entry:

FCAF	Receive Time	Type	Application	Action	Rule	Rule UUID	Dyes	Severity	Category	URI Category List	Verdict	URL	File Name
	2020/03/17 17:54:18	vulnerability	web-browsing	reset-both	Allow-Any	0d3035c...		high	any				17717.pdf

A 'Close' button is located at the bottom right of the window.

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