



PALO ALTO NETWORKS EDU-210



Lab 5B: Content-ID

Document Version: 2020-06-26

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
Objectives.....	3
Lab Topology	4
Theoretical Lab Topology.....	4
Lab Settings	5
5 Content-ID.....	6
5.0 Load Lab Configuration	6
5.1 Create Security Policy Rule with a Vulnerability Protection Profile.....	9
5.2 Test the Security Policy Rule	13
5.3 Review the Logs.....	14
5.4 Update the Vulnerability Profile	16
5.5 Create a Security Profile Group.....	19
5.6 Create a File Blocking Profile.....	25
5.7 Modify a Security Profile Group	27
5.8 Test the File Blocking Profile	28
5.9 Create a File Blocking Profile to Block Multi-Level Encoded Files	29
5.10 Modify the Security Policy Rule	30
5.11 Test the File Blocking Profile with Multi-Level Encoding	31
5.12 Modify the Security Policy Rule	31
5.13 Test the File Blocking Profile with Multi-Level Encoding	32
5.14 Create a Danger Security Policy Rule	33
5.15 Generate Threats with File Blocking.....	35
5.16 Modify a Security Policy Group	37
5.17 Generate Threats without File Blocking	38

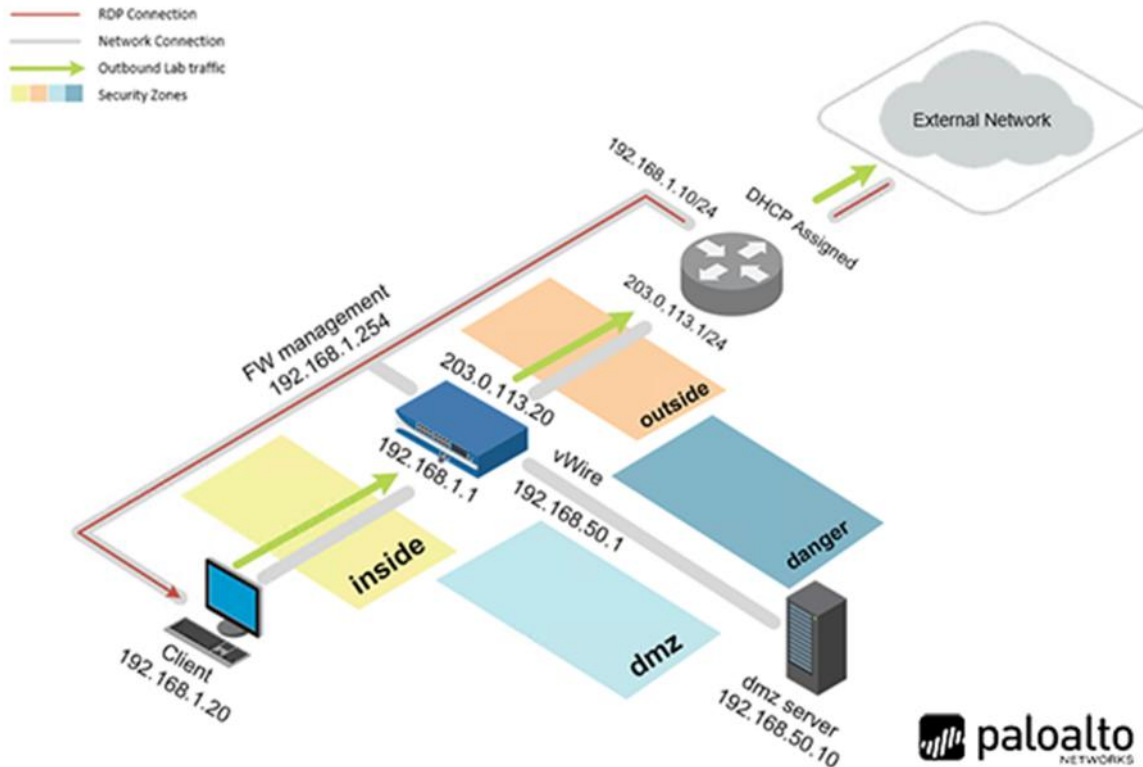
Introduction

The Palo Alto Networks next-generation firewall has been deployed. The company has set up policies to allow certain types of applications. Now, we need to begin scanning the traffic for threats as it passes through the firewall. We need to look for exploits, viruses, spyware, and other malicious threats.

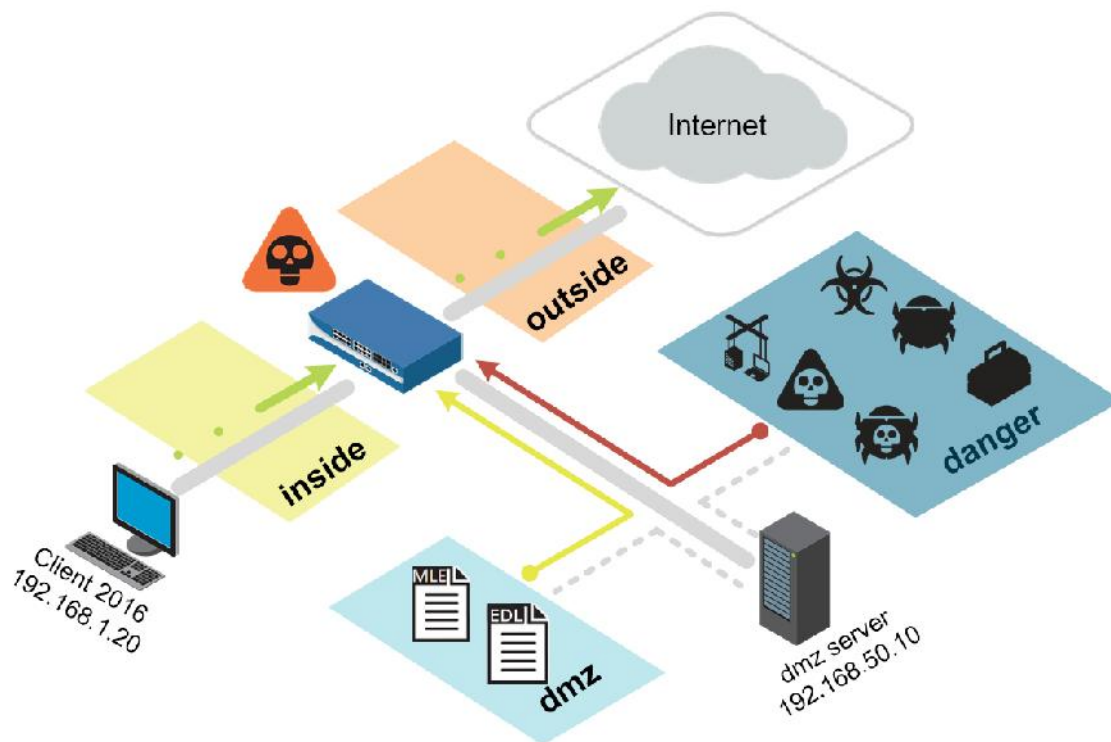
Objectives

-) Configure and test a Vulnerability Security Profile
-) Configure and test a File Blocking Security Profile
-) Use the Virtual Wire mode and configure the danger zone
-) Generate threats and observe the actions taken

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	Train1ng\$
Firewall	192.168.1.254	admin	Train1ng\$

5 Content-ID

5.0 Load Lab Configuration

1. Launch the **Client** virtual machine to access the graphical login screen.



To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

2. Log in as **lab-user** using the password **Train1ng\$**.



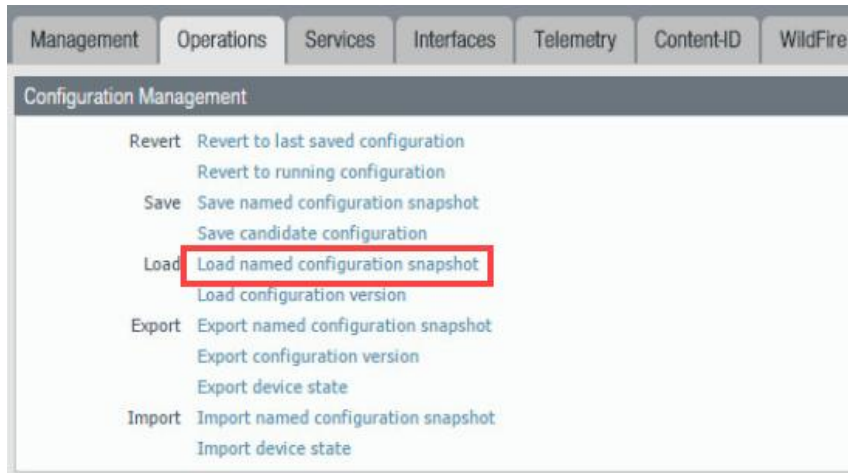
3. Launch the **Chromium Web Browser** and connect to **https://192.168.1.254**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	admin
Password	Train1ng\$

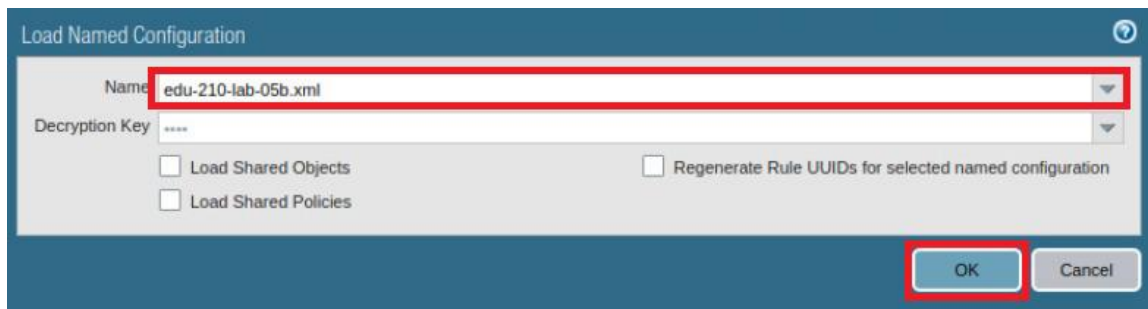
6. In the web interface, navigate to **Device > Setup > Operations**.



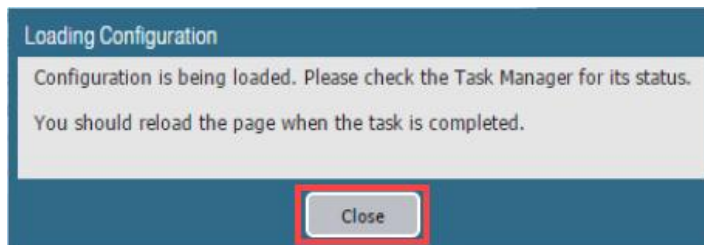
- Click **Load named configuration snapshot**:



- Click the dropdown list next to the *Name* text box and select **edu-210-lab-05b.xml**. Click **OK**.



- Click **Close**.

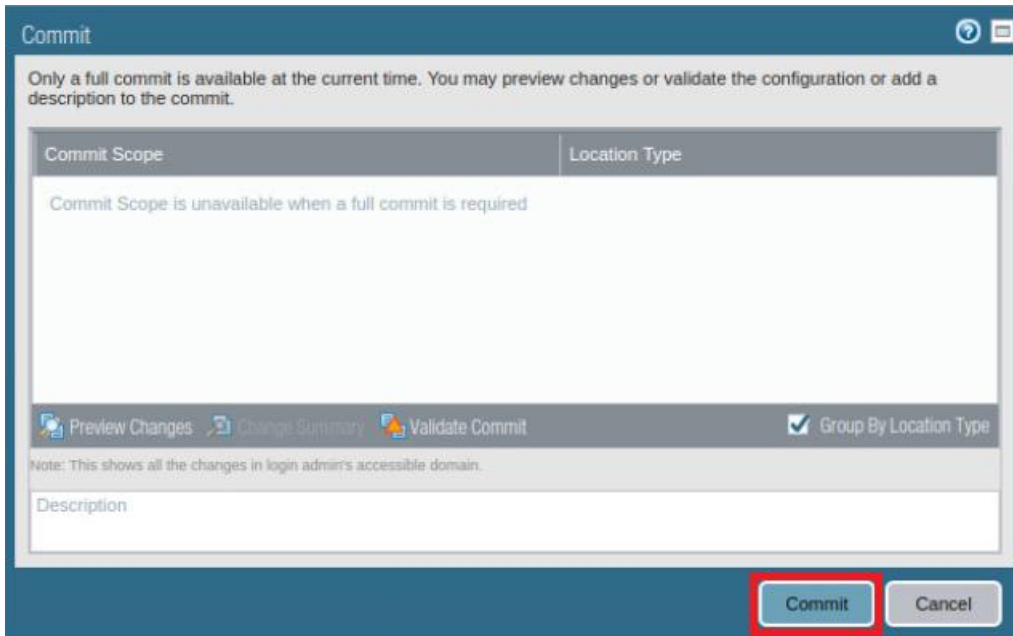


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

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

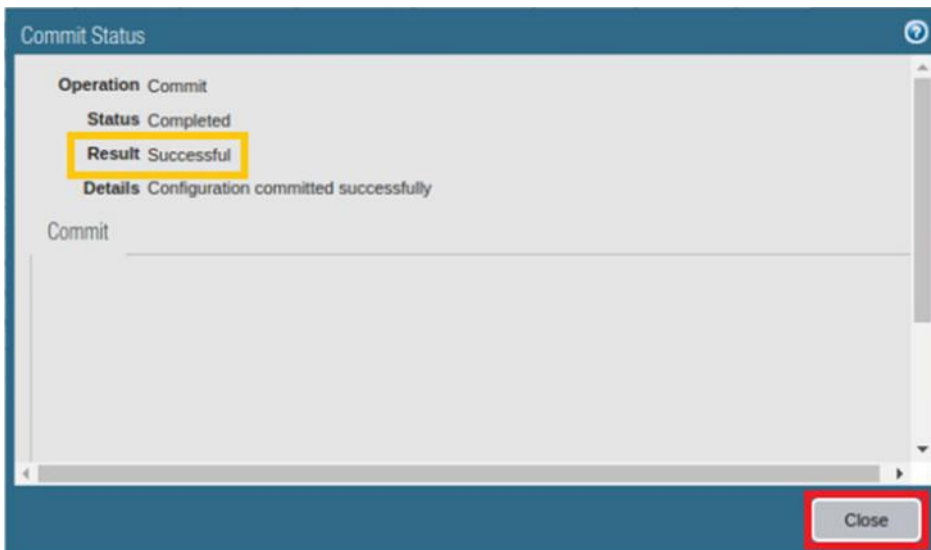


11. Click **Commit** and wait until the commit process is complete.



The 'Commit' dialog box has a title bar with a question mark icon and a close icon. The main content area contains a message: '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.' Below this is a table with two columns: 'Commit Scope' and 'Location Type'. The 'Commit Scope' column contains the text 'Commit Scope is unavailable when a full commit is required'. Below the table is a row of buttons: 'Preview Changes', 'Change Summary', 'Validate Commit', and a checked checkbox 'Group By Location Type'. Below the buttons is a note: 'Note: This shows all the changes in login admin's accessible domain.' At the bottom is a text input field labeled 'Description'. At the bottom right are two buttons: 'Commit' (highlighted with a red box) and 'Cancel'.

12. Once completed successfully, click **Close** to continue.



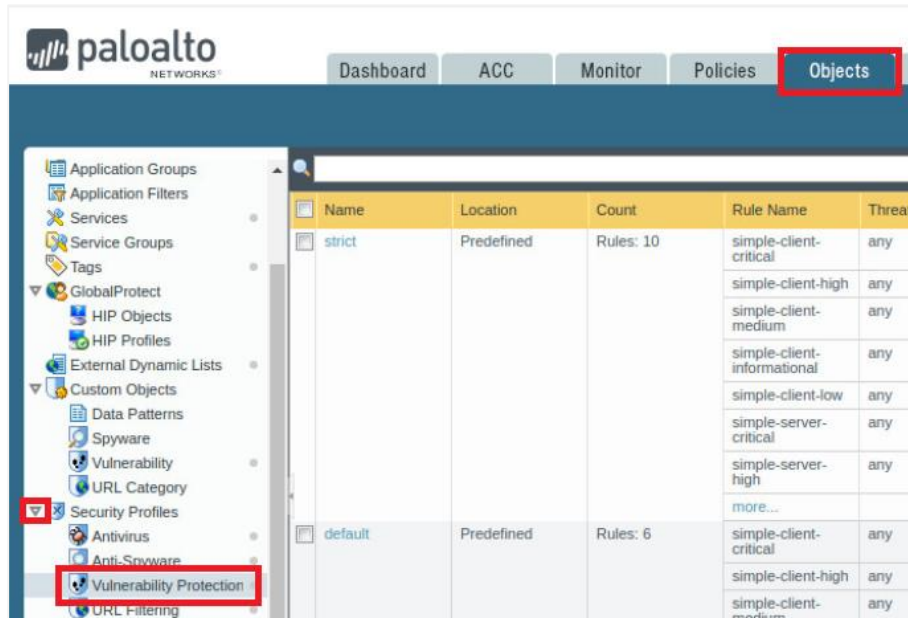
The 'Commit Status' dialog box has a title bar with a question mark icon. The main content area displays the following information: 'Operation Commit', 'Status Completed', 'Result Successful' (highlighted with a yellow box), and 'Details Configuration committed successfully'. Below this is a section labeled 'Commit' with a large text area. At the bottom right is a button labeled 'Close' (highlighted with a red box).

13. Leave the firewall web interface open to continue with the next task.

5.1 Create Security Policy Rule with a Vulnerability Protection Profile

A Security Policy Rule can include a *Vulnerability Protection Profile* that determines the level of protection against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.

1. In the web interface, select **Objects > Security Profiles > Vulnerability Protection**.

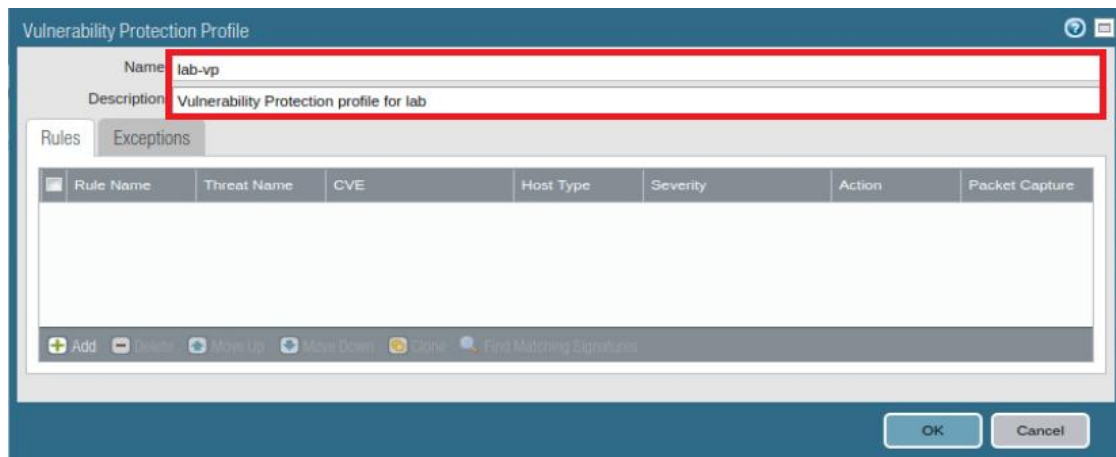


2. Click **Add** to create a *Vulnerability Protection Profile*.



3. In the *Vulnerability Protection Profile* window, configure the following.

Parameter	Value
Name	lab-vp
Description	Type vulnerability Protection profile for lab

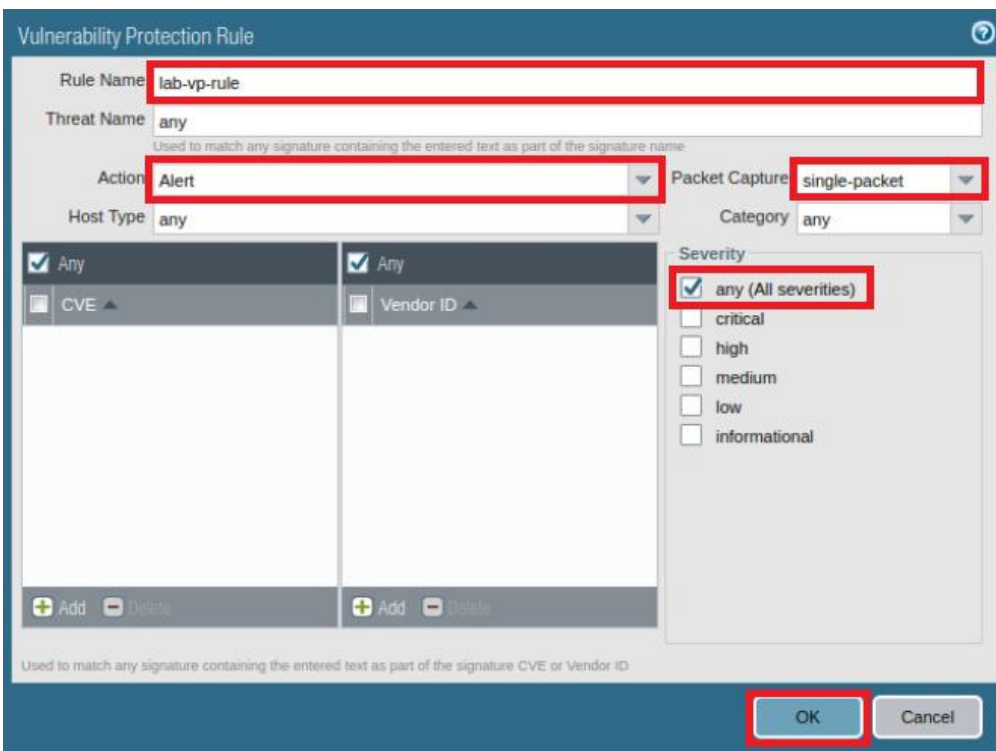


4. On the *Rules* tab, click **Add** to create a rule.

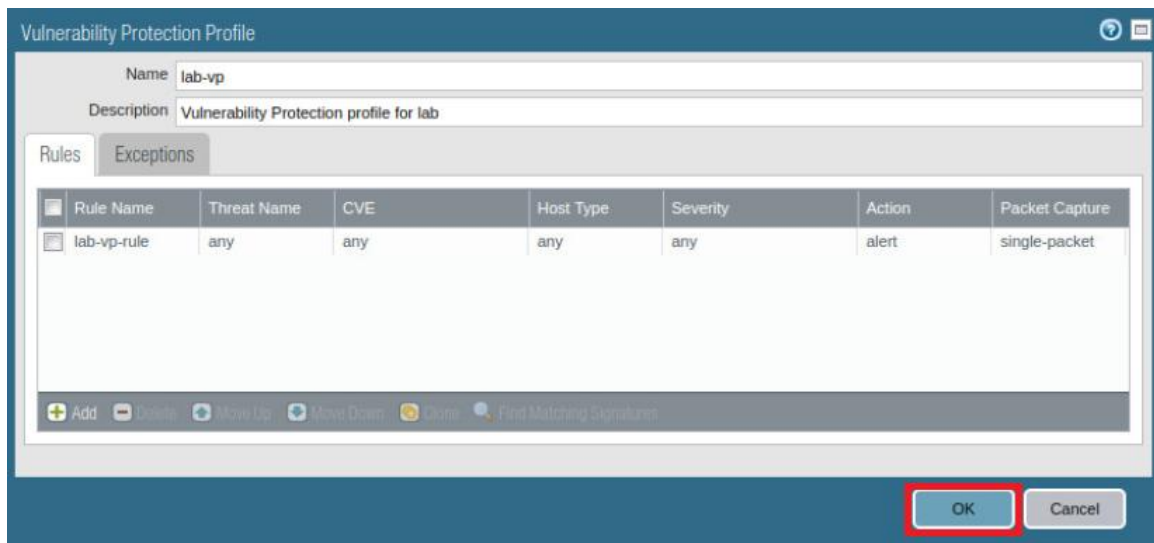


5. In the *Vulnerability Protection Rule* window, configure the following and then proceed to click **OK**.

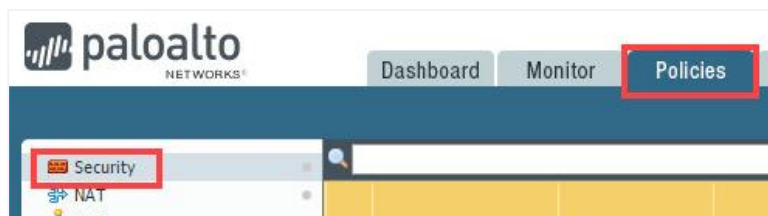
Parameter	Value
Name	lab-vp-rule
Action	Select Alert from the dropdown menu
Packet Capture	Select single-packet from the dropdown menu
Severity	Verify that the any (All severities) checkbox is selected



- Back on the *Vulnerability Protection Profile* window, ensure that the new rule appears and click **OK**.



- In the web interface, select **Policies > Security**.

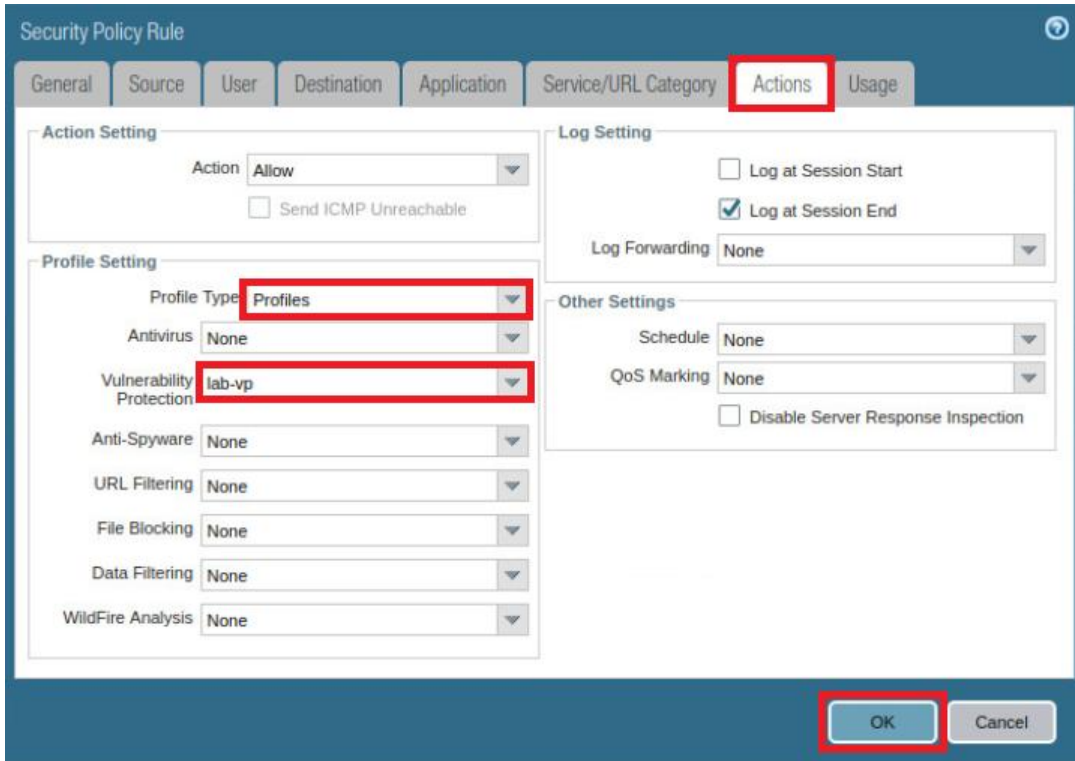


- Click on **internal-inside-dmz** to open the Security Policy Rule.

	Name	Tags	Type	Source		
				Zone	Address	User
1	egress-outside-av-as	egress	universal	inside	any	any
2	egress-outside	egress	universal	inside	any	any
3	internal-inside-dmz	internal	universal	inside	any	any
4	intrazone-default	none	intrazone	any	any	any
5	interzone-default	none	interzone	any	any	any

9. In the *Security Policy Rule* window, click the **Actions** tab and configure the following. When finished, click **OK**.

Parameter	Value
Profile Type	Select Profiles from the dropdown list
Vulnerability Protection	Select lab-vp from the dropdown list



The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action' is set to 'Allow'. Under 'Profile Setting', 'Profile Type' is set to 'Profiles' and 'Vulnerability Protection' is set to 'lab-vp'. Under 'Log Setting', 'Log at Session End' is checked. Under 'Other Settings', 'Schedule' and 'QoS Marking' are set to 'None'. The 'OK' button is highlighted.

10. **Commit** all changes.

5.2 Test the Security Policy Rule

1. Launch the *Terminal* window by clicking on the **Xfce Terminal** icon in the toolbar.



2. In the Terminal window, enter the command below, followed by pressing the **Enter**.

```
C:\home\lab-user> sudo nmap --script ftp-brute 192.168.50.10 -p 21
```

3. When prompted, enter **Train1ng\$** for the password and press **Enter**.

```
C:\home\lab-user> sudo nmap --script ftp-brute 192.168.50.10 -p 21
[sudo] password for lab-user: *****
```

4. This action launches an FTP brute force attack at the DMZ FTP server. After several minutes, you can press **CTRL+C** to terminate the command because sufficient log data will have been collected. The entire script will take greater than 10 minutes to complete, should you choose to wait for completion.

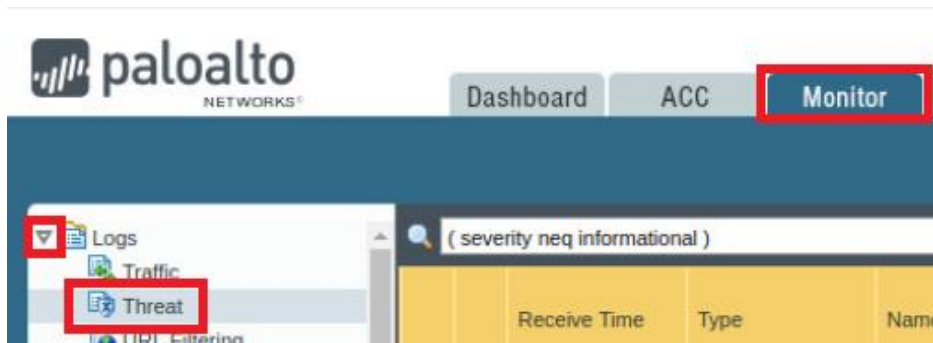
```
C:\home\lab-user> sudo nmap --script ftp-brute 192.168.50.10 -p 21
[sudo] password for lab-user:

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-04 22:04 UTC
```




5. After the script completes, type **exit** followed by pressing the **Enter** key to close the Terminal.

5.3 Review the Logs

1. Change focus to the firewall web interface and select **Monitor > Logs > Threat**.



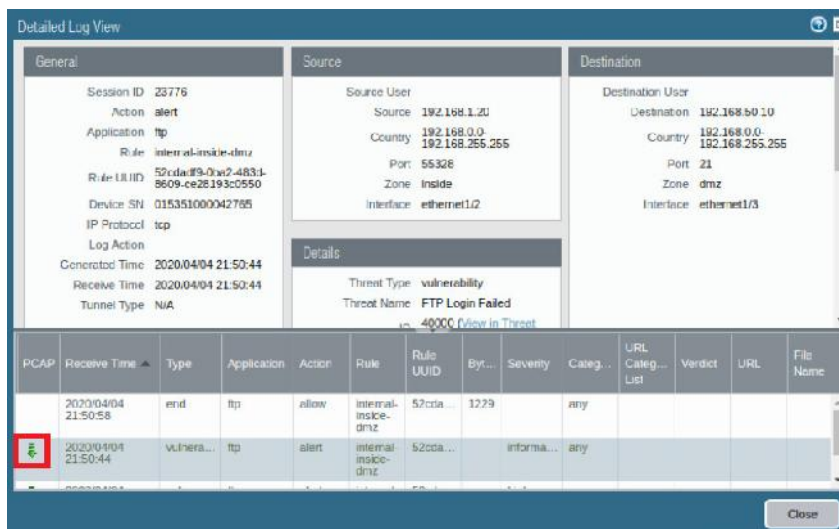
2. Make sure to clear the filter. Notice that you now have logs reflecting the FTP Brute Force attempt. However, the firewall is set only to alert. Open the **Detailed Log View** by clicking the **magnify** icon next to the most recent threat.

	Receive Time	Type	Name	From Zone	To Zone	Source address
	04/04 21:50:44	vulnerability	FTP Login Failed	inside	dmz	192.168.1.20
	04/04 21:50:43	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20
	04/04 21:50:43	vulnerability	FTP Login Failed	inside	dmz	192.168.1.20

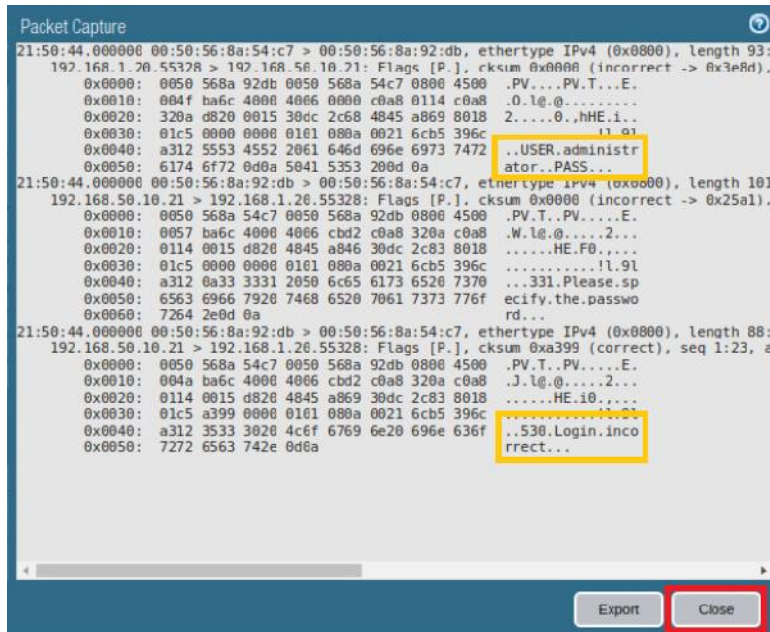


If there are no FTP: login Brute Force attempt events, the nmap command was not successful and you will need to rerun the nmap command.

3. From the *Detailed Log View* window, click the **download** icon underneath the **PCAP** column to open the packet capture.



- In the *Packet Capture* window, notice the username and password that were attempted, along with the 530 responses from the FTP server. After viewing the pcap, click **Close**.



Captured packets can be exported in pcap format and examined with an offline analyzer for further investigation.

- Back on the *Detailed Log View* window, click **Close**.
- Leave the firewall web interface open to continue with the next task.

5.4 Update the Vulnerability Profile

1. In the web interface, select **Objects > Security Profiles > Vulnerability Protection**.
2. Click on the **lab-vp** rule to open the profile.

<input type="checkbox"/>	Name	Location	Count	Rule Name	Threat Name
<input type="checkbox"/>	strict	Predefined	Rules: 10	simple-client-critical	any
				simple-client-high	any
				simple-client-medium	any
				simple-client-informational	any
				simple-client-low	any
				simple-server-critical	any
				simple-server-high	any
				more...	
<input type="checkbox"/>	default	Predefined	Rules: 6	simple-client-critical	any
				simple-client-high	any
				simple-client-medium	any
				simple-server-critical	any
				simple-server-high	any
				simple-server-medium	any
<input type="checkbox"/>	lab-vp		Rules: 1	lab-vp-rule	any

3. In the *Vulnerability Protection Profile* window, click on **lab-vp-rule** to open the rule.

Vulnerability Protection Profile

Name

lab-vp

Description

Vulnerability Protection profile for lab

Rules

Exceptions

<input type="checkbox"/>	Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packet Capture
<input type="checkbox"/>	lab-vp-rule	any	any	any	any	alert	single-packet

+

 Add

-

 Delete

↕

 Move Up

↕

 Move Down

📄

 Clone

🔍

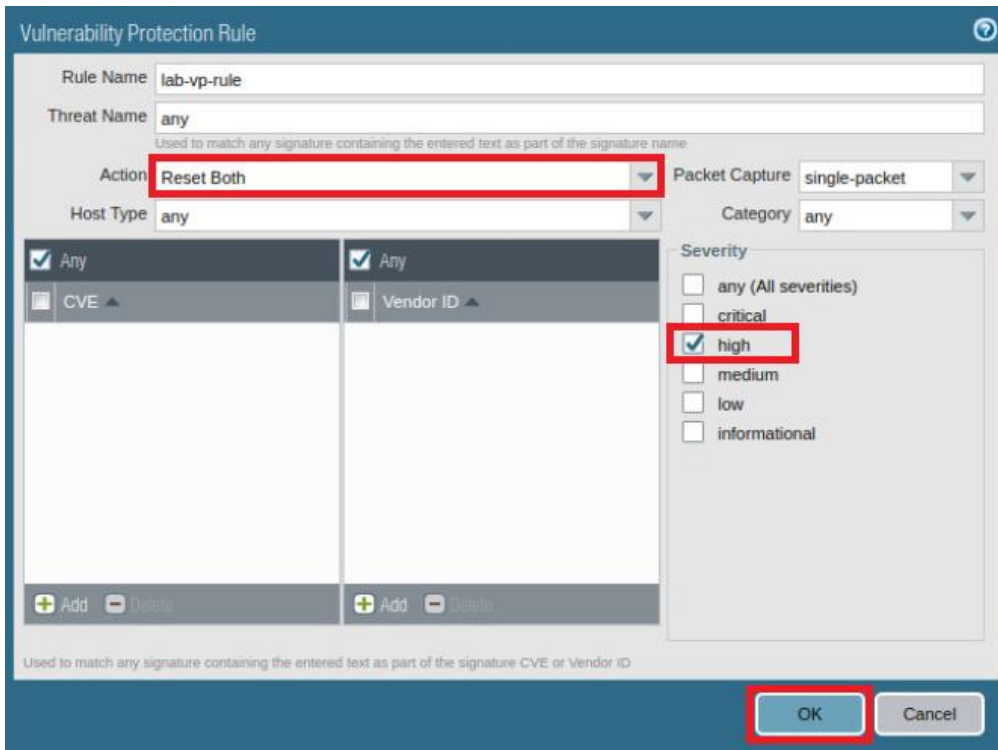
 Find Matching Signatures

OK

Cancel

4. In the *Vulnerability Protection Rule* window, configure the following. Once finished, click **OK**.

Parameter	Value
Action	Select the Reset Both option from the dropdown list
Severity	Select the high checkbox



Vulnerability Protection Rule

Rule Name: lab-vp-rule

Threat Name: any
Used to match any signature containing the entered text as part of the signature name

Action: **Reset Both**

Host Type: any

Packet Capture: single-packet

Category: any

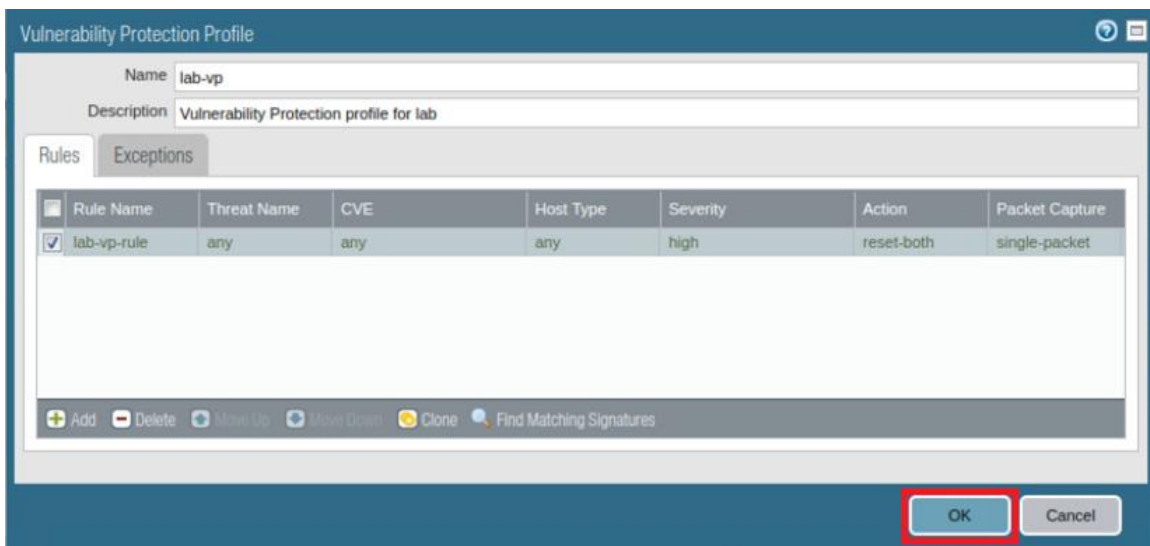
Severity:

- ☐ any (All severities)
- ☐ critical
- ☒ **high**
- ☐ medium
- ☐ low
- ☐ informational

Used to match any signature containing the entered text as part of the signature CVE or Vendor ID

OK Cancel

5. Back on the *Vulnerability Protection Profile* window, confirm the changes and click **OK**.



Vulnerability Protection Profile

Name: lab-vp

Description: Vulnerability Protection profile for lab

Rules Exceptions

Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packet Capture
<input checked="" type="checkbox"/> lab-vp-rule	any	any	any	high	reset-both	single-packet

Add Delete Move Up Move Down Clone Find Matching Signatures

OK Cancel

6. **Commit** all changes.

7. Rerun the **nmap** command and review the logs to confirm that the new FTP brute force attempts are reset. You can choose to run the script for at least a minute or the full 10 minutes for completion.

```
C:\home\lab-user> sudo nmap --script ftp-brute 192.168.50.10 -p 21
```

8. When prompted, enter **Train1ng\$** for the password and press **Enter**.
9. After several minutes, you can press **CTRL+C** to terminate the command because sufficient log data will have been collected. The entire script will take greater than 10 minutes to complete should you choose to wait for completion.

```
C:\home\lab-user> sudo nmap --script ftp-brute 192.168.50.10 -p 21
[sudo] password for lab-user:

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-04 22:04 UTC
```

10. After the script completes, type **exit** followed by pressing the **Enter** key to close the Terminal.
11. Change focus to the firewall web interface and select **Monitor > Logs > Threat**.

	Receive Time	Type	Name	From Zone	To Zone	Source address	S... U...	Destination address	Dy... User Gr...	To Port	Application	Action	Severity
	04/04 22:08:30	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10		21	ftp	reset-both	high
	04/04 22:08:30	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10		21	ftp	reset-both	high
	04/04 22:08:29	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10		21	ftp	reset-both	high
	04/04 22:08:29	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10		21	ftp	reset-both	high



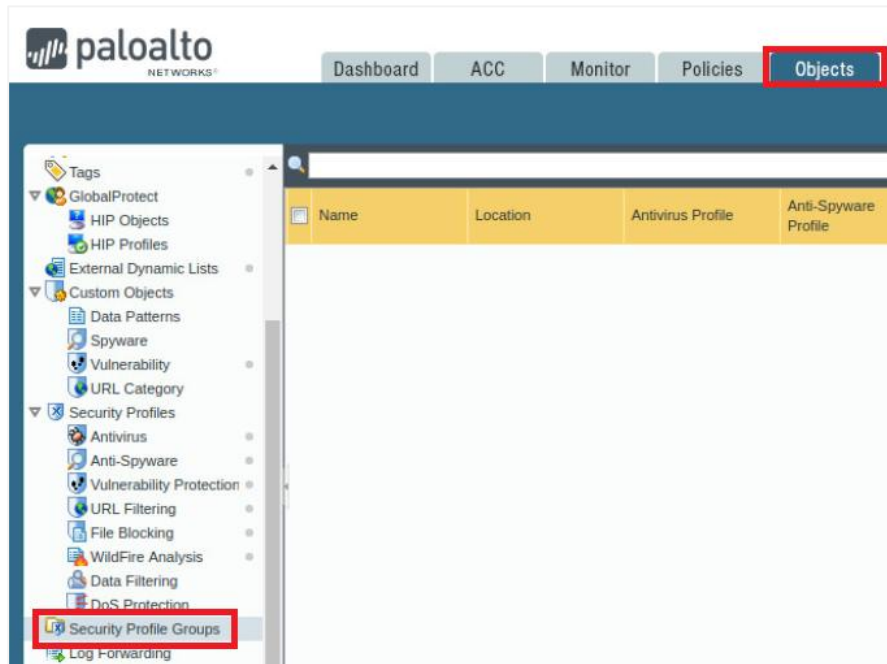
If there are no FTP: login Brute Force attempt events, the nmap command was not successful and you will need to rerun the nmap command.

12. Leave the firewall web interface open to continue with the next task.

5.5 Create a Security Profile Group

The firewall supports the ability to create *Security Profile Groups*, which specify sets of *Security Profiles* that can be treated as a unit and then added to Security policy rules.

1. In the web interface, navigate to **Objects > Security Profile Groups**.

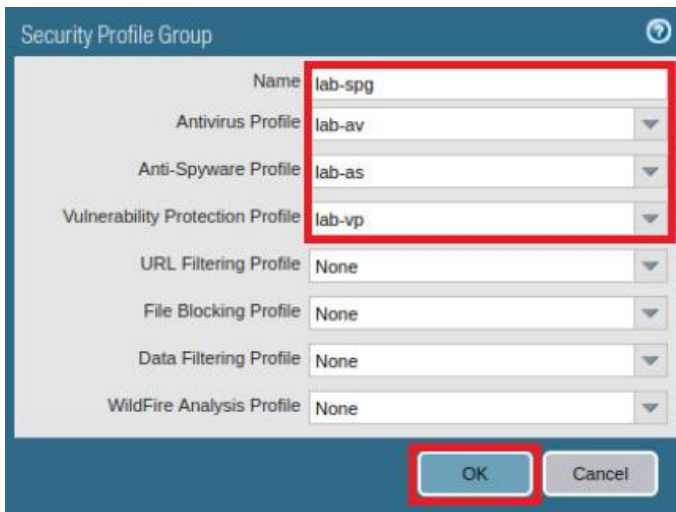


2. Click **Add** to create a *Security Profile Group*.



3. In the *Security Profile Group* window, configure the following. Once finished, click **OK**.

Parameter	Value
Name	lab-spg
Antivirus Profile	Select lab-av
Anti-Spyware Profile	Select lab-as
Vulnerability Protection Profile	Select lab-vp



Security Profile Group

Name: lab-spg

Antivirus Profile: lab-av

Anti-Spyware Profile: lab-as

Vulnerability Protection Profile: lab-vp

URL Filtering Profile: None

File Blocking Profile: None








Data Filtering Profile: None

WildFire Analysis Profile: None

OK Cancel

4. In the web interface, select **Policies > Security**.
5. Select the **egress-outside-av-as** rule and click **Delete**.

	Name	Tags	Type	Zone
1	egress-outside-av-as	egress	universal	inside
2	egress-outside	egress	universal	inside
3	internal-inside-dmz	internal	universal	inside
4	intrazone-default	none	intrazone	any
5	interzone-default	none	interzone	any

 Add
  Delete
  Clone
  Override
  Revert
  Enable
  Disable

6. When prompted, click **Yes** to continue with the deletion.
7. Click **Add** to define a new *Security Policy Rule*.



8. In the *Security Policy Rule* window, while on the *General* tab, configure the following.

Parameter	Value
Name	Type egress-outside-content-id
Rule Type	Verify that universal (default) is selected
Tags	Select egress from the dropdown list
Group Rules By Tag	Select egress from the dropdown list
Audit Comment	Type created Security Policy Rule for Security Profile Group on <date> by admin.



Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Name: egress-outside-content-id

Rule Type: universal (default)

Description:

Tags: egress

Group Rules By Tag: egress

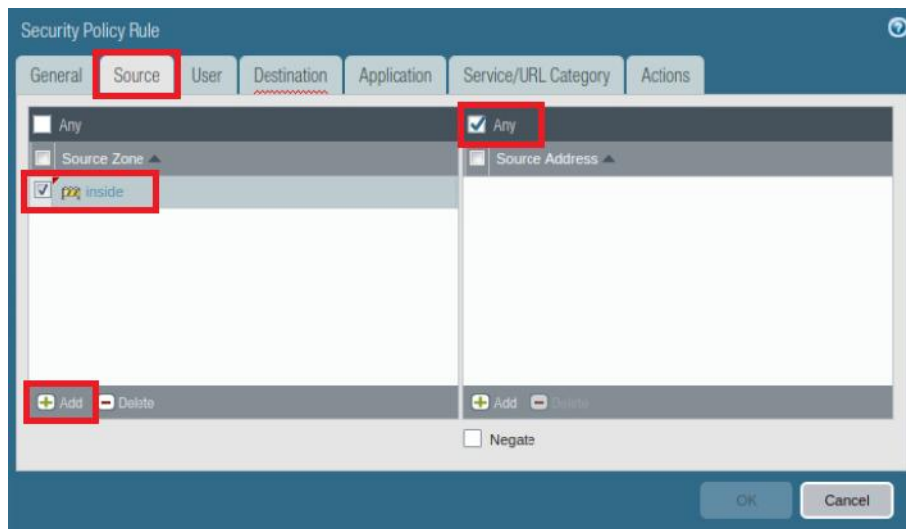
Audit Comment: Created Security Policy Rule for Security Profile Group on 04/04/2020 by admin

Audit Comment Archive

OK Cancel

9. In the *Security Policy Rule* window, click the **Source** tab to configure the following.

Parameter	Value
Source Zone	Click Add and select inside from the dropdown list
Source Address	Verify that the Any checkbox is selected



Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Any

Source Zone: inside

Source Address: Any

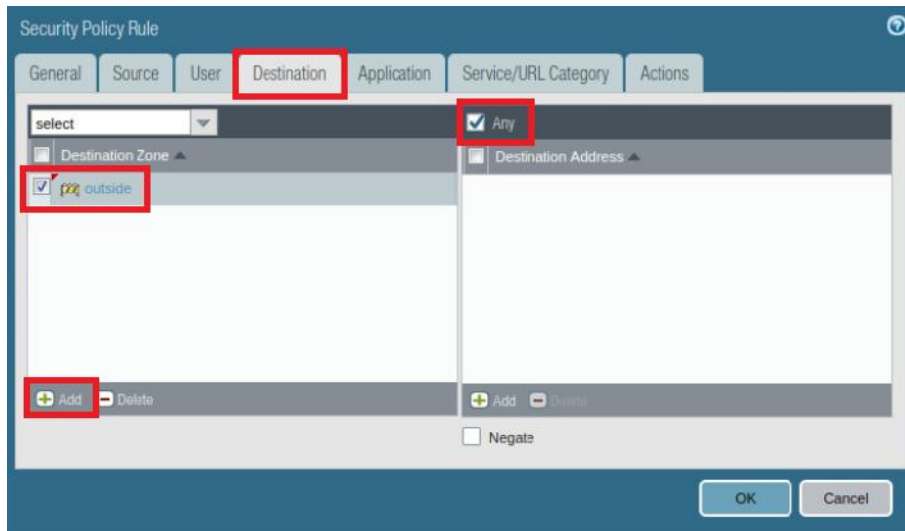
Add Delete

Negate

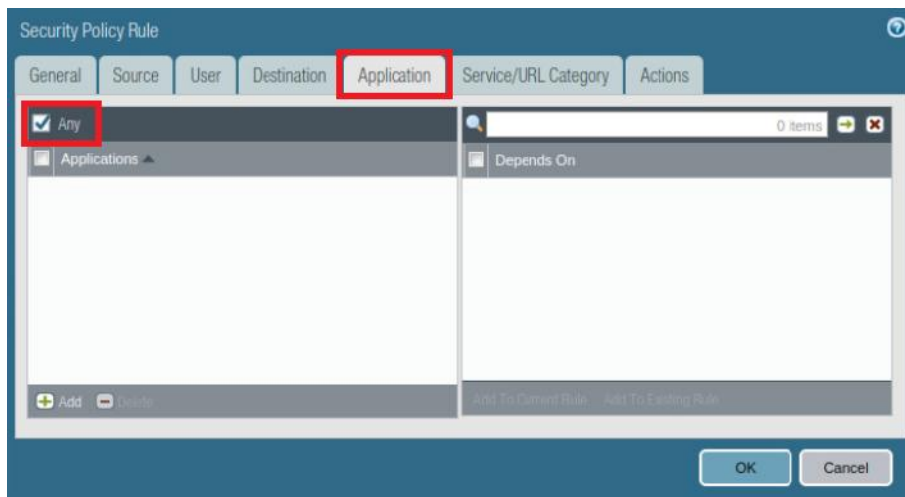
OK Cancel

10. In the *Security Policy Rule* window, click the **Destination** tab and configure the following.

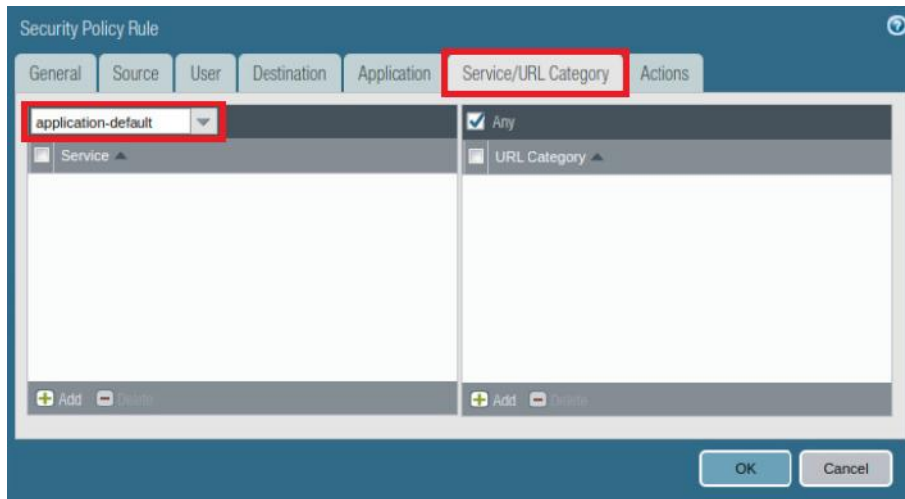
Parameter	Value
Destination Zone	Click Add and select outside from the dropdown list
Destination Address	Verify that the Any checkbox is selected



11. In the *Security Policy Rule* window, click the **Application** tab and verify that the **Any** checkbox is selected.

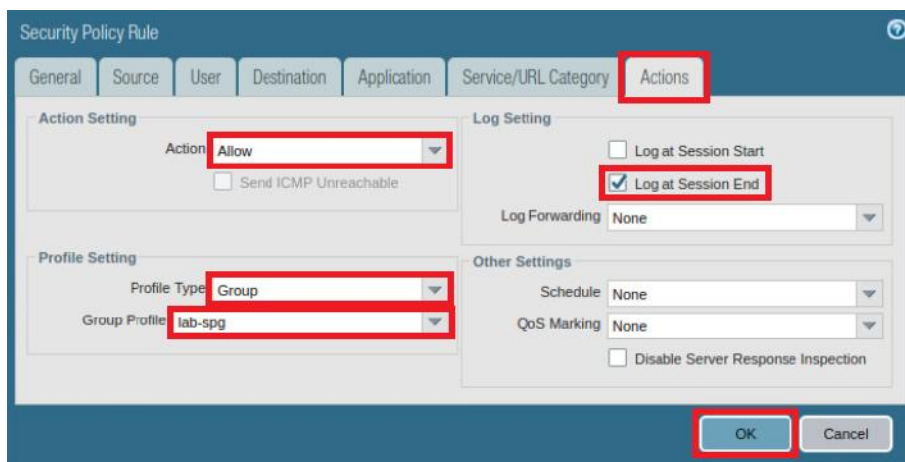


12. In the *Security Policy Rule* window, click the **Service/URL Category** tab and verify that **application-default** is selected.



13. In the *Security Policy Rule* window, click the **Actions** tab and configure the following. Once finished, click **OK**.

Parameter	Value
Action Setting	Verify that Allow is selected
Log Setting	Verify that Log at Session End is selected
Profile Type	Select Group from the dropdown list
Group Profile	Select lab-spg from the dropdown list



14. Verify that the new rule appears in the list. The *egress-outside-content-id* rule should be listed as the first Security policy rule to ensure that the next sections of the lab work properly. If it is not listed as the first Security policy rule, then highlight the rule and move the rule to the top of the list by click on **Move** and selecting **Move Top**.

	Name	Tags	Type	Zone	Address
1	<i>egress-outside</i>	<i>egress</i>	<i>universal</i>	<i>inside</i>	<i>any</i>
2	<i>internal-inside-dmz</i>	<i>internal</i>	<i>universal</i>	<i>inside</i>	<i>any</i>
3	<i>egress-outside-content-id</i>	<i>egress</i>	<i>universal</i>	<i>inside</i>	<i>any</i>
4	<i>intrazone-default</i>	<i>none</i>	<i>intrazone</i>	<i>any</i>	<i>any</i>
5	<i>interzone-default</i>	<i>none</i>	<i>interzone</i>	<i>any</i>	<i>any</i>

Move Top
Move Up
Move Down
Move Bottom

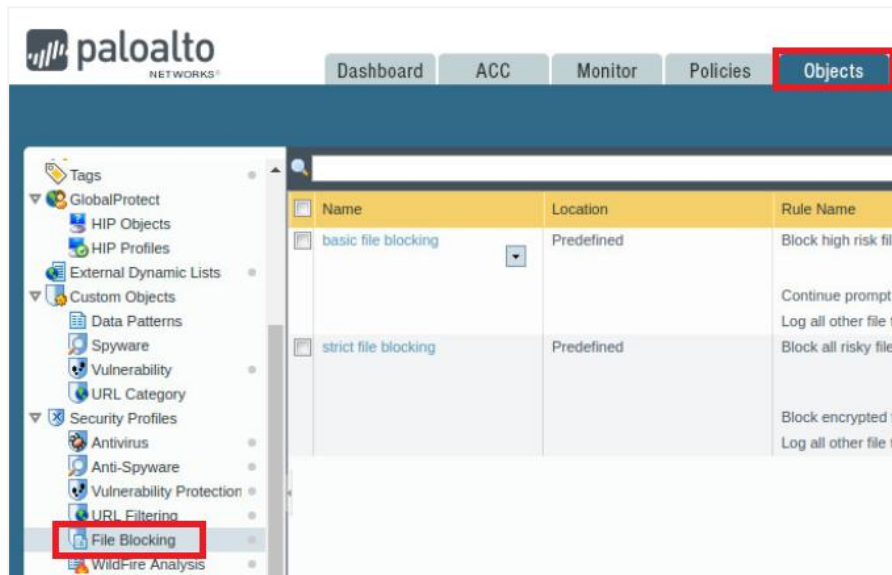
Add Delete Clone Override Revert Enable Disable Move PDF/CSV

15. Leave the firewall web interface open to continue with the next task.

5.6 Create a File Blocking Profile

A Security Policy Rule can include specifications of a *File Blocking Profile* that blocks selected file types from being uploaded or downloaded or generates an alert when the specified file types are detected.

1. In the web interface, select **Objects > Security Profiles > File Blocking**.

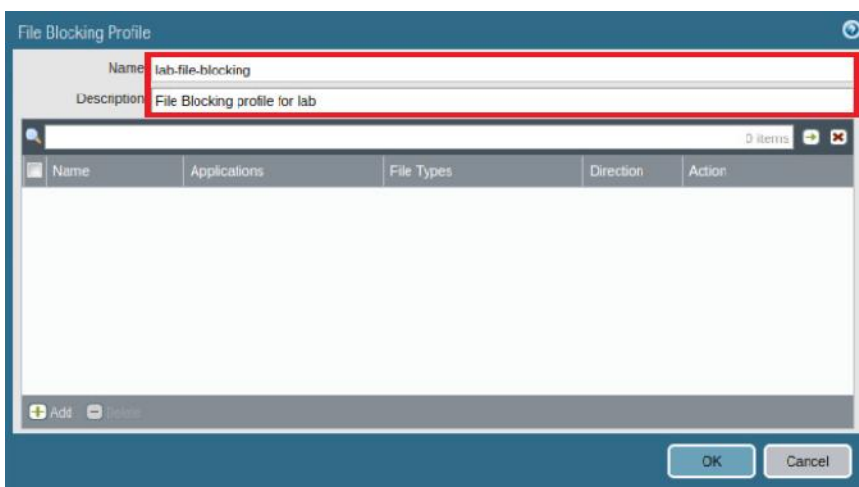


2. Click **Add** to open the *File Blocking Profile* configuration window.



3. In the *File Blocking Profile* window, configure the following.

Parameter	Value
Name	Type lab-file-blocking
Description	Type File Blocking profile for lab

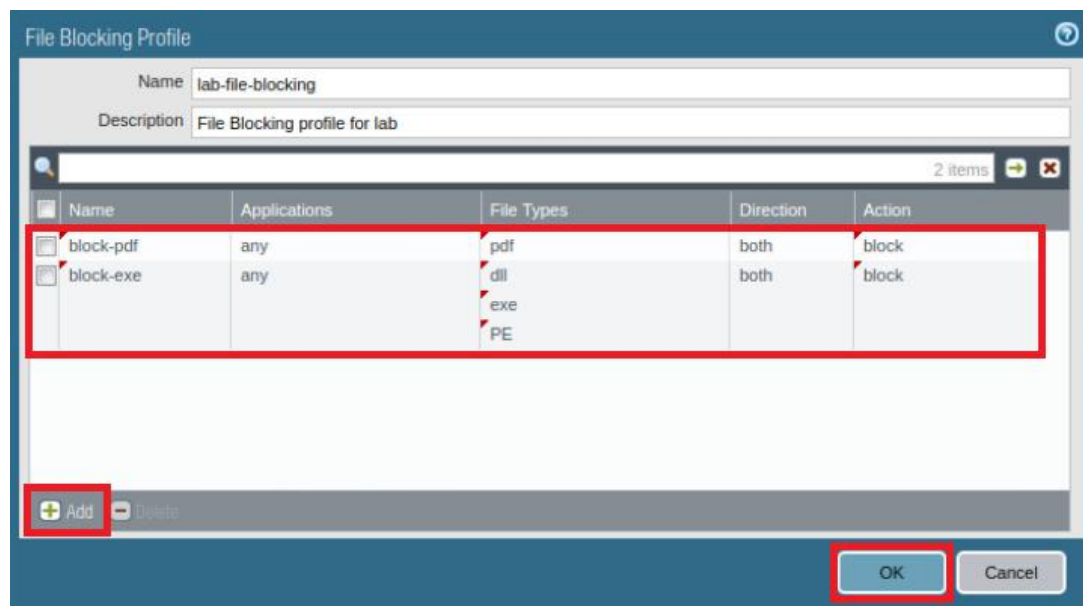


4. In the *File Blocking Profile* window, click **Add** and configure the following.

Parameter	Value
Name	Type block-pdf
Applications	Verify that any is selected
File Types	Click Add and select pdf from the dropdown list
Direction	Verify that both is selected
Action	Select block from the dropdown list

5. Click **Add** once more and configure the following and click **OK**.

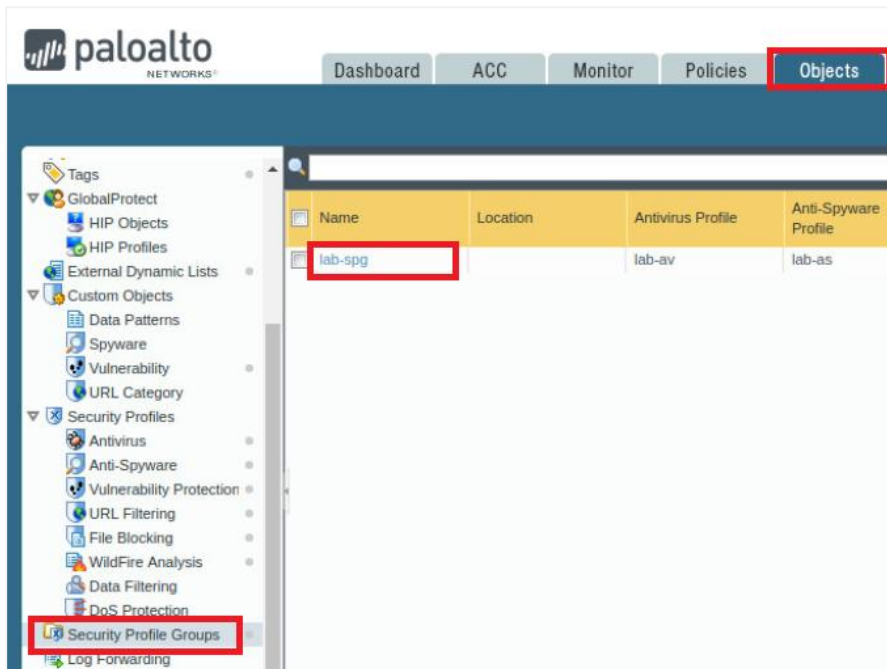
Parameter	Value
Name	Type block-exe
Applications	Verify that any is selected
File Types	Click Add and select the following from the dropdown list: dll exe PE
Direction	Verify that both is selected
Action	Select block from the dropdown list



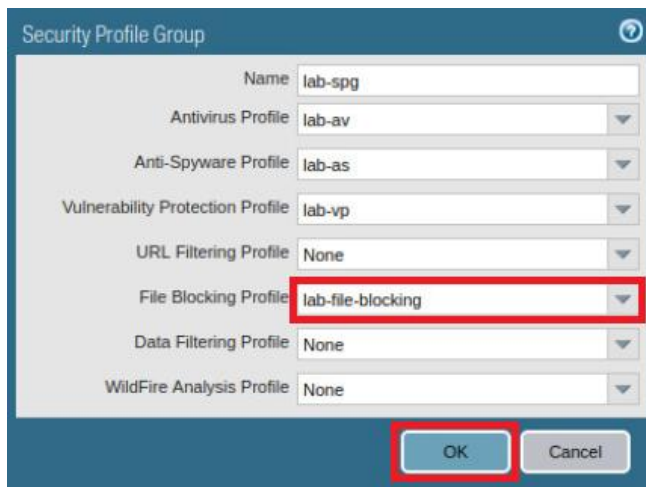
6. Verify that the new profile appears in the list. Leave the firewall web interface open to continue with the next task.

5.7 Modify a Security Profile Group

1. In the web interface, navigate to **Objects > Security Profiles Groups** and then click the *Security Profile Group* named **lab-spg**.



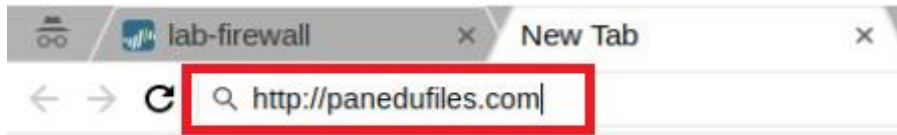
2. In the *Security Profile Group* window, select **lab-file-blocking** from the *File Blocking Profile* dropdown list and click **OK**.



3. **Commit** all changes.

5.8 Test the File Blocking Profile

1. Open a new tab in **Chromium Web Browser** and browse to <http://www.panedufiles.com/>.



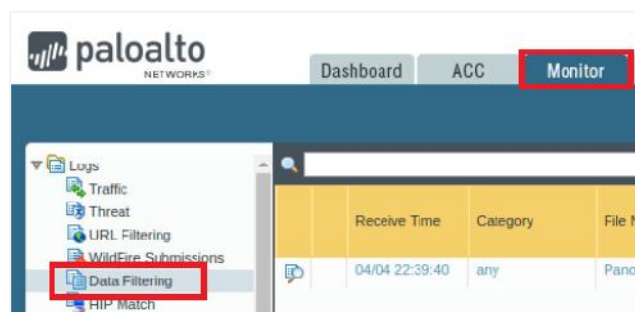
2. Once the webpage loads, click the **Panorama_AdminGuide.pdf** link.



3. Notice that the download is blocked. Close the browser tab.



4. Change focus back to the firewall web interface and select **Monitor > Logs > Data Filtering**.



5. Find the log entry for the PDF file that has been blocked.

	Receive Time	Category	File Name	File URL	Name	From Zone	To Zone	Source address	Source User	Destination address
	04/04 22:39:40	any	Panorama_AdminGuide70.pdf		Adobe Portable Document Format (PDF)	inside	outside	192.168.1.20		67.195.19

6. Leave the firewall web interface open to continue with the next task.

5.9 Create a File Blocking Profile to Block Multi-Level Encoded Files

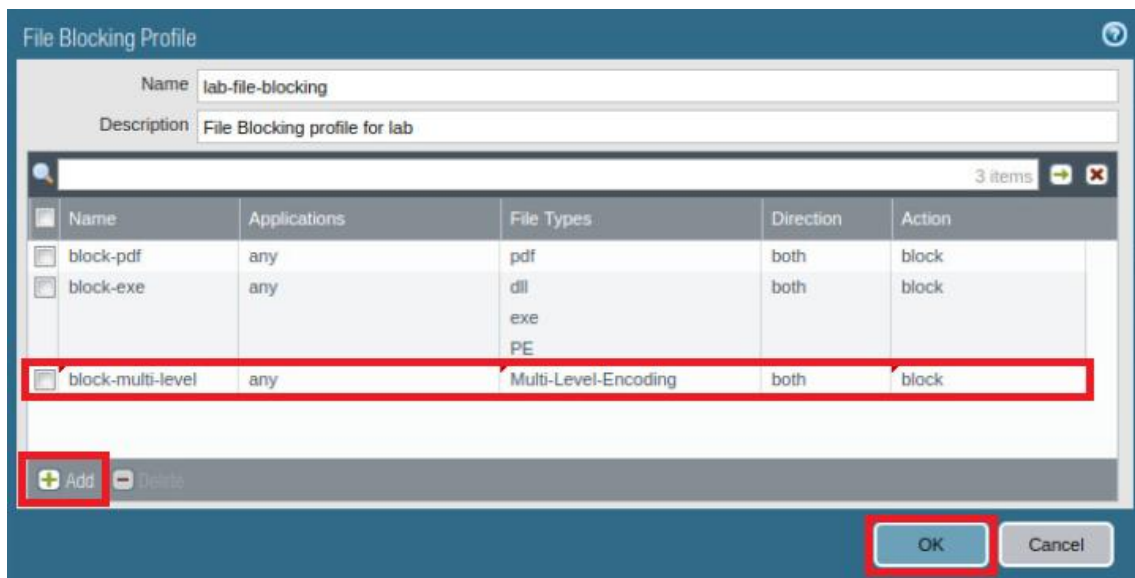
A file that is encoded five or more times cannot be inspected by the firewall. Multi-Level Encoding can be used to block this type of content.

1. In the web interface, navigate to **Objects > Security Profiles > File Blocking**.
2. Click **lab-file-blocking** to configure the profile.

Name	Location	Rule Name
basic file blocking	Predefined	Block high risk file types Continue prompt encrypted files Log all other file types
strict file blocking	Predefined	Block all risky file types Block encrypted files Log all other file types
lab-file-blocking		block-pdf block-exe

3. In the *File Blocking Profile* window, click **Add** and configure the following. Once finished, click **OK**.

Parameter	Value
Name	Type block-multi-level
Applications	Verify that any is selected
File Types	Click Add and select Multi-Level-Encoding from the dropdown list
Direction	Verify that both is selected
Action	Select block from the dropdown list



The screenshot shows the 'File Blocking Profile' configuration window. The 'Name' field is 'lab-file-blocking' and the 'Description' is 'File Blocking profile for lab'. Below these fields is a table with 5 columns: Name, Applications, File Types, Direction, and Action. The table contains three entries: 'block-pdf' (any, pdf, both, block), 'block-exe' (any, dll, exe, PE, both, block), and 'block-multi-level' (any, Multi-Level-Encoding, both, block). The 'block-multi-level' row is highlighted with a red box. At the bottom left, there is an 'Add' button with a green plus icon, also highlighted with a red box. At the bottom right, there are 'OK' and 'Cancel' buttons, with the 'OK' button highlighted by a red box.

Name	Applications	File Types	Direction	Action
block-pdf	any	pdf	both	block
block-exe	any	dll exe PE	both	block
block-multi-level	any	Multi-Level-Encoding	both	block

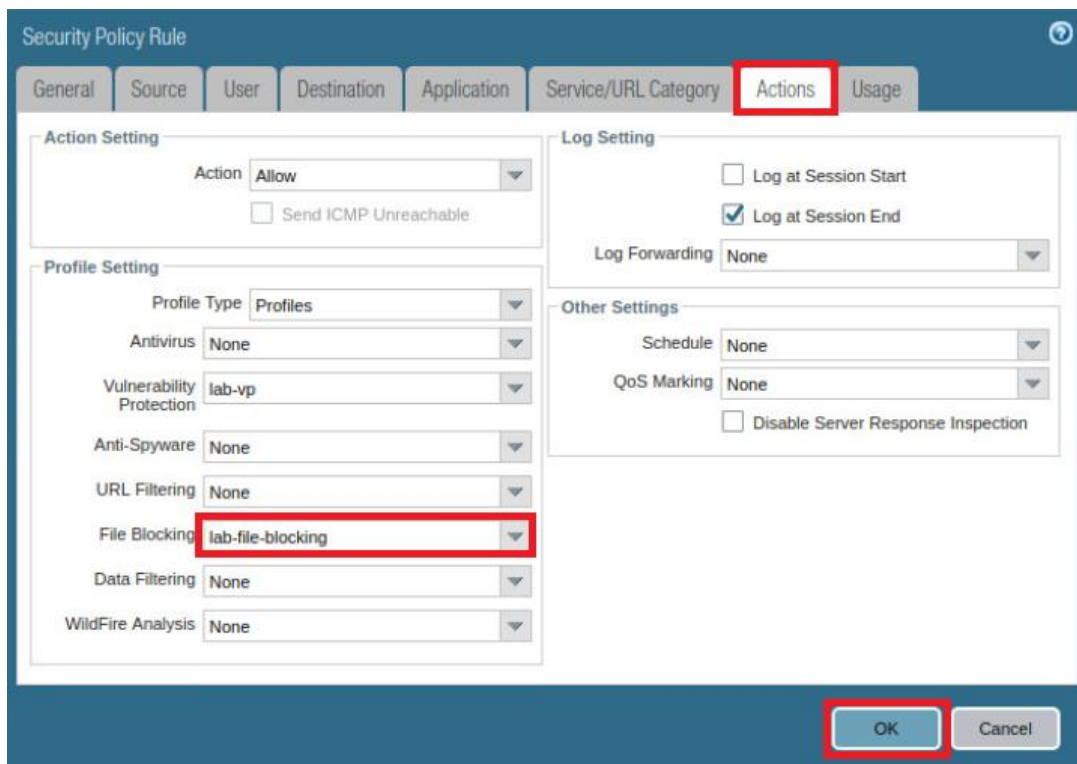
4. Leave the firewall web interface open to continue with the next task.

5.10 Modify the Security Policy Rule

1. In the web interface, select **Policies > Security**.
2. Click **internal-inside-dmz** to configure the Security policy rule.

	Name	Tags	Type	Zone	Address
1	egress-outside-cont...	egress	universal	inside	any
2	egress-outside	egress	universal	inside	any
3	internal-inside-dmz	internal	universal	inside	any
4	intrazone-default	none	intrazone	any	any
5	interzone-default	none	interzone	any	any

3. In the *Security Policy Rule* window, click the **Actions** tab and then select **lab-file-blocking** from the *File Blocking* dropdown list. Click **OK**.



The image shows the 'Security Policy Rule' configuration window. The 'Actions' tab is selected. In the 'Action Setting' section, 'Action' is set to 'Allow'. In the 'Profile Setting' section, 'File Blocking' is set to 'lab-file-blocking'. In the 'Log Setting' section, 'Log at Session End' is checked. In the 'Other Settings' section, 'Schedule' and 'QoS Marking' are set to 'None'. The 'OK' button is highlighted with a red box.

4. **Commit** all changes.

5.11 Test the File Blocking Profile with Multi-Level Encoding

1. Open a new tab in **Chromium Web Browser** and browse **http://192.168.50.10/mle.zip**.



2. Notice that the file is blocked in accordance with the new file blocking rule. Close the browser tab.

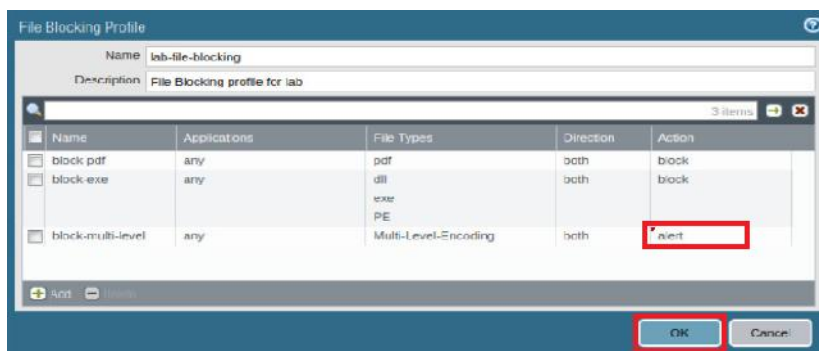


5.12 Modify the Security Policy Rule

1. In the web interface, select **Objects > Security Profiles > File Blocking**.
2. Click on **lab-file-blocking** to configure the profile.

Name	Location	Rule Name
basic file blocking	Predefined	Block high risk file types Continue prompt encrypted files Log all other file types
strict file blocking	Predefined	Block all risky file types Block encrypted files Log all other file types
lab-file-blocking		block-pdf block-exe block-multi-level

3. In the *File Blocking Profile* window, select the **block-multi-level** rule and change the **Action** to **alert**. Click **OK**.



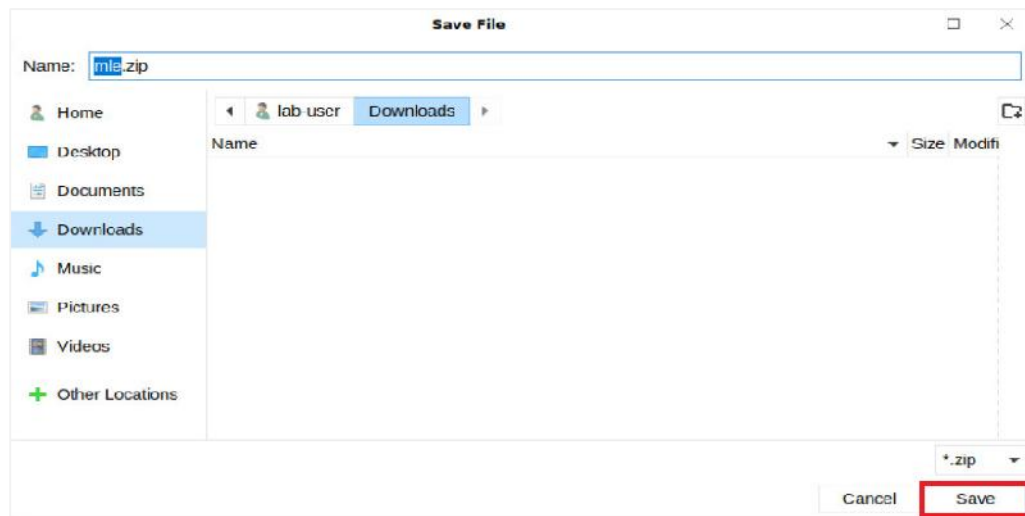
4. **Commit** all changes.

5.13 Test the File Blocking Profile with Multi-Level Encoding

1. Open a new tab in **Chromium Web Browser** and browse to **<http://192.168.50.10/mle.zip>**.



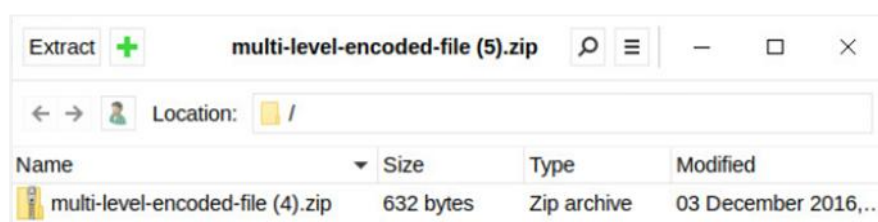
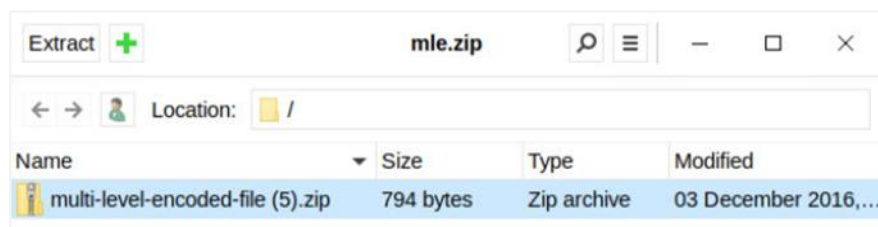
2. In the *Save File* window, save the report to the **Downloads** directory and click **Save**.



3. In the bottom-left corner of the *Chrome* browser window, click the file to open it.



4. Notice the recursive structure of the zip archive. Close the file browser and the browser tab.



5.14 Create a Danger Security Policy Rule

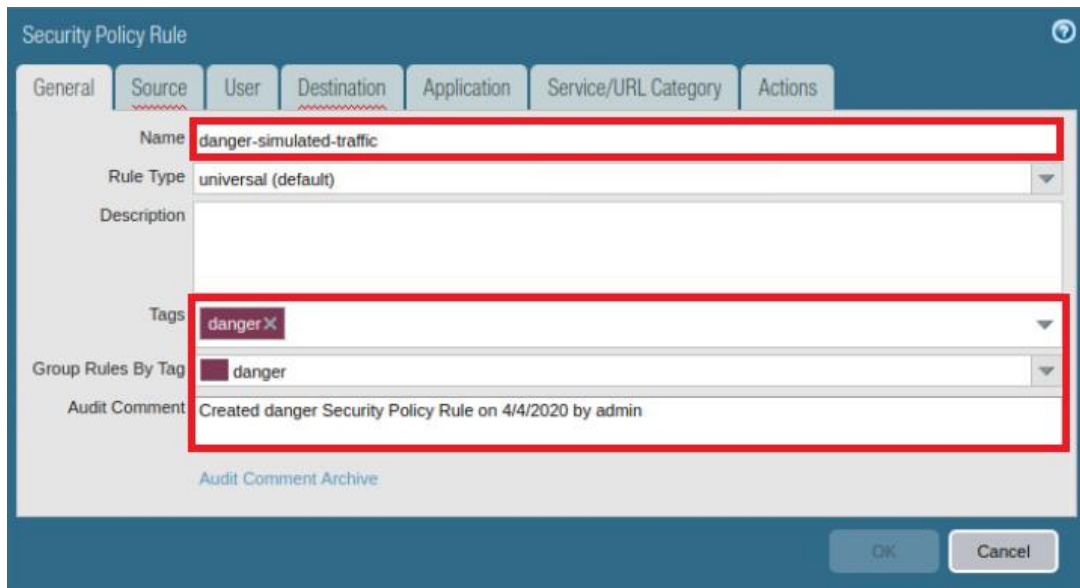
Create a Security Policy Rule that references the danger security zone for threat and traffic generation.

1. In the web interface, select **Policies > Security**.
2. Click **Add** to create a Security policy rule.



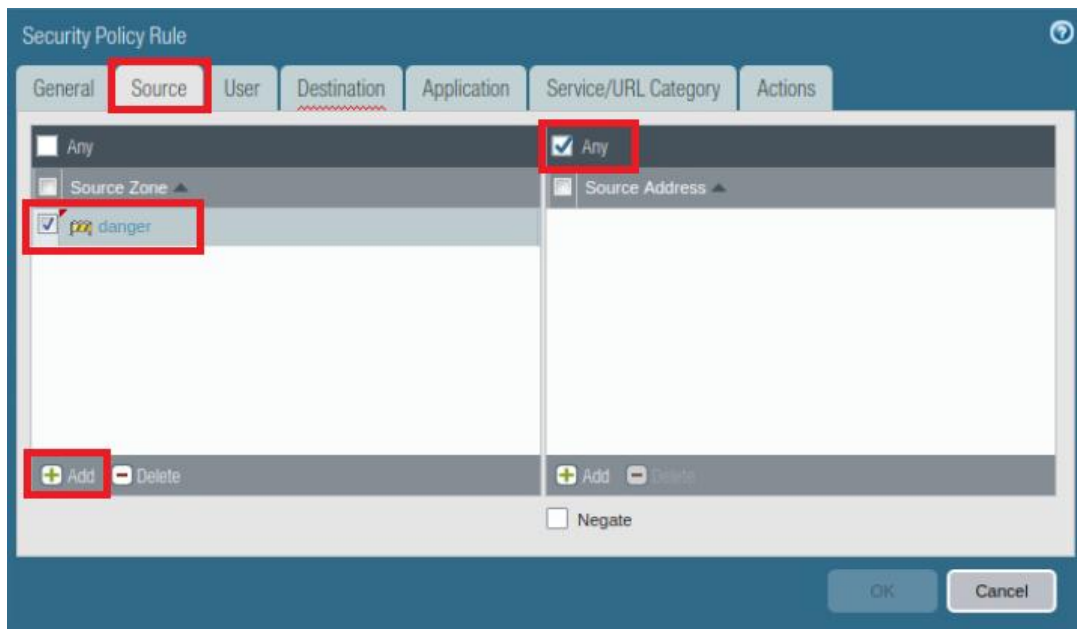
3. In the *Security Policy Rule* window, while on the *General* tab, configure the following.

Parameter	Value
Name	Type danger-simulated-traffic
Tags	Select danger from the dropdown list
Group Rules By Tag	Select danger from the dropdown list
Audit Comment	Type Created danger Security Policy Rule on <date> by admin



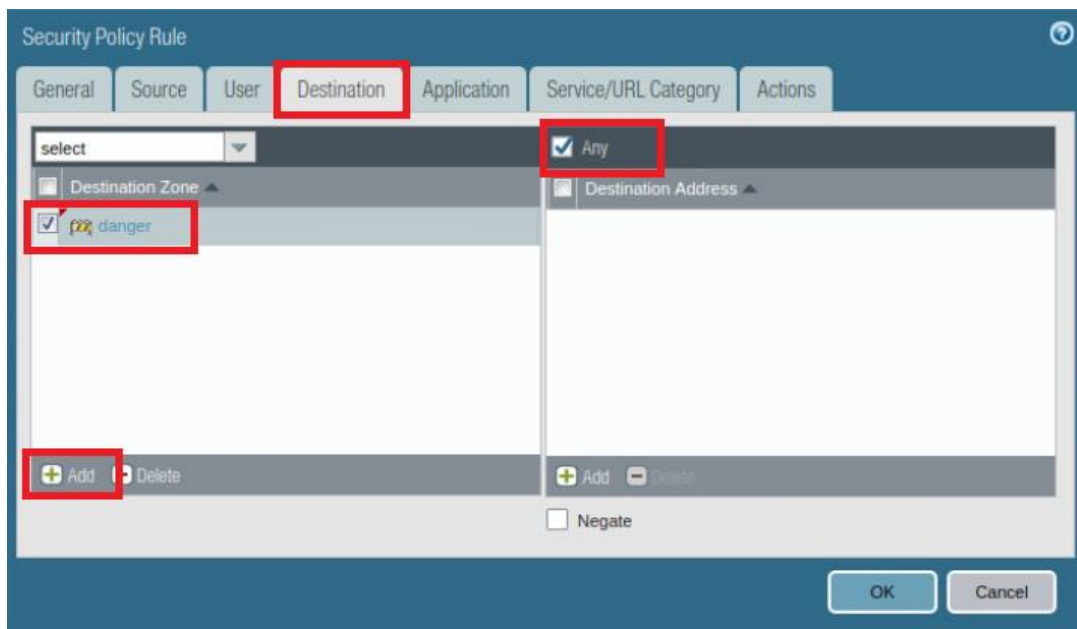
4. Click on the **Source** tab and configure the following.

Parameter	Value
Source Zone	Click Add and select danger from the dropdown list
Source Address	Verify that the Any checkbox is selected



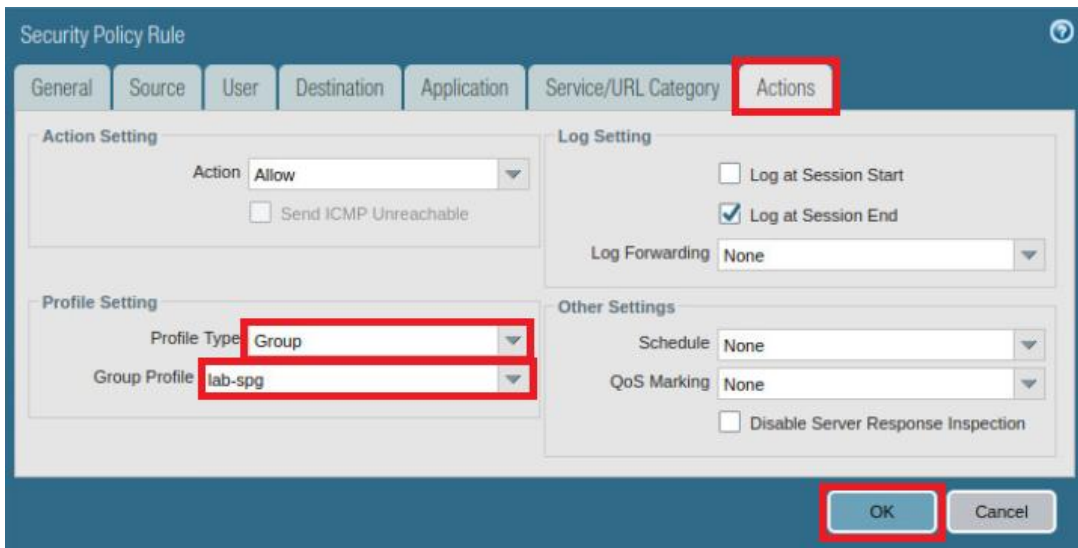
5. Click on the **Destination** tab and configure the following.

Parameter	Value
Destination Zone	Click Add and select danger from the dropdown list
Destination Address	Verify that the Any checkbox is selected



6. Click on the **Actions** tab and configure the following. Once finished, click **OK**.

Parameter	Value
Profile Type	Select Group from the dropdown list
Group Profile	Select lab-spg from the dropdown list



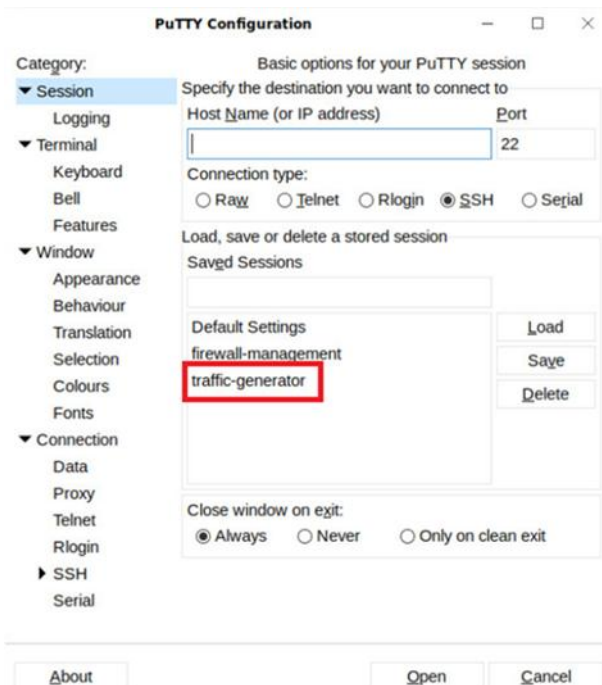
The image shows the 'Security Policy Rule' configuration window. The 'Actions' tab is selected and highlighted with a red box. Within this tab, the 'Action' is set to 'Allow'. The 'Log Setting' section has 'Log at Session End' checked. The 'Profile Setting' section has 'Profile Type' set to 'Group' and 'Group Profile' set to 'lab-spg', both highlighted with red boxes. The 'Other Settings' section has 'Schedule' and 'QoS Marking' both set to 'None'. The 'OK' button at the bottom right is also highlighted with a red box.

7. **Commit** all changes.

5.15 Generate Threats with File Blocking



1. On the Client desktop, double-click the **PuTTY** icon.
2. In *PuTTY Configuration* window, double-click **traffic-generator**.



The image shows the 'PuTTY Configuration' window. The 'Session' category is selected in the left sidebar. The 'Host Name (or IP address)' field is empty, and the 'Port' is set to 22. The 'Connection type' is set to 'SSH'. The 'Saved Sessions' list shows 'firewall-management' and 'traffic-generator', with 'traffic-generator' highlighted by a red box. The 'Load', 'Save', and 'Delete' buttons are visible next to the session list. The 'Close window on exit' options are 'Always' (selected), 'Never', and 'Only on clean exit'.

- Log in as **root** with **Pa10A1t0** as the password.





```
login as: root
root@192.168.50.10's password:
Last login: Mon Mar 30 16:35:53 2020 from 192.168.1.20
[root@pod-dmz ~]#
```

- In the *PuTTY* window, enter the command below and wait for the script to complete.

```
[root@pod-dmz ~]# sh /tg/malware.sh
```

```
Successful packets:      67
Failed packets:         0
Truncated packets:      0
Retried packets (ENOBUFFS): 0
Retried packets (EAGAIN): 0
Actual: 372 packets (264661 bytes) sent in 0.269919 seconds.
Rated: 980500.0 Bps, 7.84 Mbps, 1378.19 pps
Flows: 2 flows, 7.40 fps, 372 flow packets, 0 non-flow
Statistics for network device: ens224
Successful packets:      372
Failed packets:         0
Truncated packets:      0
Retried packets (ENOBUFFS): 0
Retried packets (EAGAIN): 0
Actual: 44 packets (11666 bytes) sent in 0.118679 seconds.
Rated: 98200.0 Bps, 0.785 Mbps, 370.74 pps
Flows: 2 flows, 16.85 fps, 44 flow packets, 0 non-flow
Statistics for network device: ens224
Successful packets:      44
Failed packets:         0
Truncated packets:      0
Retried packets (ENOBUFFS): 0
Retried packets (EAGAIN): 0
[root@pod-dmz ~]#
```

- Leave the *PuTTY* window open and change focus to the firewall web interface.
- In the web interface, navigate to **Monitor > Logs > Threat**.
- Notice the threats currently listed from the generated traffic. The threat log entries that you see in your lab may not match exactly the image shown. Threat signatures, names, categorizations, and verdicts may change over time to ensure that the firewall will consistently detect the packet captures. Two custom *Vulnerability* signatures are included in the lab configurations that you loaded at the start of this lab. In your lab, at a minimum, you should see the *Vulnerability* detections named *Trojan-Win32.swrort.dfap* and *Ransom-Win32.locky.pe*.

	Receive Time	Type	Name	From Zone	To Zone	Source address	S... U...	Destination address	Dy... User Gr...	To Port	Application	Action	Severity
	04/04 23:17:48	vulnerability	Trojan-Win32.swrort.dfap	danger	danger	10.10.10.10		192.168.1.121		25	smtp	reset-both	high
	04/04 23:17:47	vulnerability	Ransom-Win32.locky.pe	danger	danger	10.10.10.10		192.168.1.121		25	smtp	reset-both	high
	04/04 23:17:36	spyware	Bredolab Gen Command and Control Traffic	danger	danger	192.168.0.2		112.137.162.134		80	web-browsing	alert	critical
	04/04 22:38:18	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		172.217.154.174		443	google-play	alert	informal

- In the web interface, navigate to **Monitor > Logs > Data Filtering**.

9. Notice the blocked files.

	Receive Time	Category	File Name	File URL	Name	From Zone	To Zone	Source address
	04/04 23:17:53	any	CV.Cindy.Nero.pdf ...		Adobe Portable Document Format (PDF)	danger	danger	10.10.10.10
	04/04 23:17:53	any	locky.exe		Windows Executable (EXE)	danger	danger	10.10.10.10
	04/04 23:17:53	any	locky.exe		Microsoft PE File	danger	danger	10.10.10.10
	04/04 23:15:18	any	onus.dll		Microsoft PE File	danger	danger	192.168.204.134

10. Leave the firewall web interface open to continue with the next task.

5.16 Modify a Security Policy Group

1. In the web interface, select **Objects > Security Profile Groups**.
2. Click on **lab-spg** to edit the Security Profile Group.

<input type="checkbox"/>	Name	Location	Antivirus Profile	Anti-Spyware Profile	Vulnerability Protection Profile
<input type="checkbox"/>	lab-spg		lab-av	lab-as	lab-vp

3. Remove the *File Blocking Profile* by selecting **None** from the dropdown list and click **OK**.

Security Profile Group

Name: lab-spg

Antivirus Profile: lab-av

Anti-Spyware Profile: lab-as

Vulnerability Protection Profile: lab-vp

URL Filtering Profile: None

File Blocking Profile: None

Data Filtering Profile: None

WildFire Analysis Profile: None

OK Cancel

4. **Commit** all changes.

5.17 Generate Threats without File Blocking

1. Change focus to the **PutTY** window and enter the command below. Wait for the shell script to complete.

```
[root@pod-dmz ~]# sh /tg/malware.sh
```

```

Successful packets:      67
Failed packets:         0
Truncated packets:      0
Retried packets (ENOBUFS): 0
Retried packets (EAGAIN): 0
Actual: 372 packets (264661 bytes) sent in 0.215155 seconds.
Rated: 1230000.0 Bps, 9.84 Mbps, 1728.98 pps
Flows: 2 flows, 9.29 fps, 372 flow packets, 0 non-flow
Statistics for network device: ens224
Successful packets:      372
Failed packets:         0
Truncated packets:      0
Retried packets (ENOBUFS): 0
Retried packets (EAGAIN): 0
Actual: 44 packets (11666 bytes) sent in 0.118145 seconds.
Rated: 98700.0 Bps, 0.789 Mbps, 372.42 pps
Flows: 2 flows, 16.92 fps, 44 flow packets, 0 non-flow
Statistics for network device: ens224
Successful packets:      44
Failed packets:         0
Truncated packets:      0
Retried packets (ENOBUFS): 0
Retried packets (EAGAIN): 0
[root@pod-dmz ~]#
```

2. Close the **PutTY** window.
3. In the web interface, navigate to **Monitor > Logs > Threat**.
4. Notice the blocked files and whether any new threats were detected with the file blocking turned off. Some files that were being blocked based on file type alone now may be blocked based on the detection of malicious content.

	Receive Time	Type	Name	From Zone	To Zone	Source address	S... U...	Destination address	Dy... User Gr...	To Port	Application	Action	Severity
	04/04 23:27:56	vulnerability	Trojan-Win32.swort.dflap	danger	danger	10.10.10.10		192.168.1.121		25	smtp	reset-both	high
	04/04 23:27:56	vulnerability	Ransom-Win32.locky.pe	danger	danger	10.10.10.10		192.168.1.121		25	smtp	reset-both	high
	04/04 23:27:45	spyware	Bredolab.Gen Command and Control Traffic	danger	danger	192.168.0.2		112.137.162.134		80	web-browsing	alert	critical
	04/04 23:17:48	vulnerability	Trojan-Win32.swort.dflap	danger	danger	10.10.10.10		192.168.1.121		25	smtp	reset-both	high
	04/04 23:17:47	vulnerability	Ransom-Win32.locky.pe	danger	danger	10.10.10.10		192.168.1.121		25	smtp	reset-both	high
	04/04 23:17:36	spyware	Bredolab.Gen Command and Control Traffic	danger	danger	192.168.0.2		112.137.162.134		80	web-browsing	alert	critical



Because threat signatures, names, categorizations, and verdicts may change over time, the log entries that you see in your lab may not match exactly with the image shown.

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