PALO ALTO NETWORKS EDU-210

Lab 5B: Content-ID

Document Version: 2020-06-26

Contents

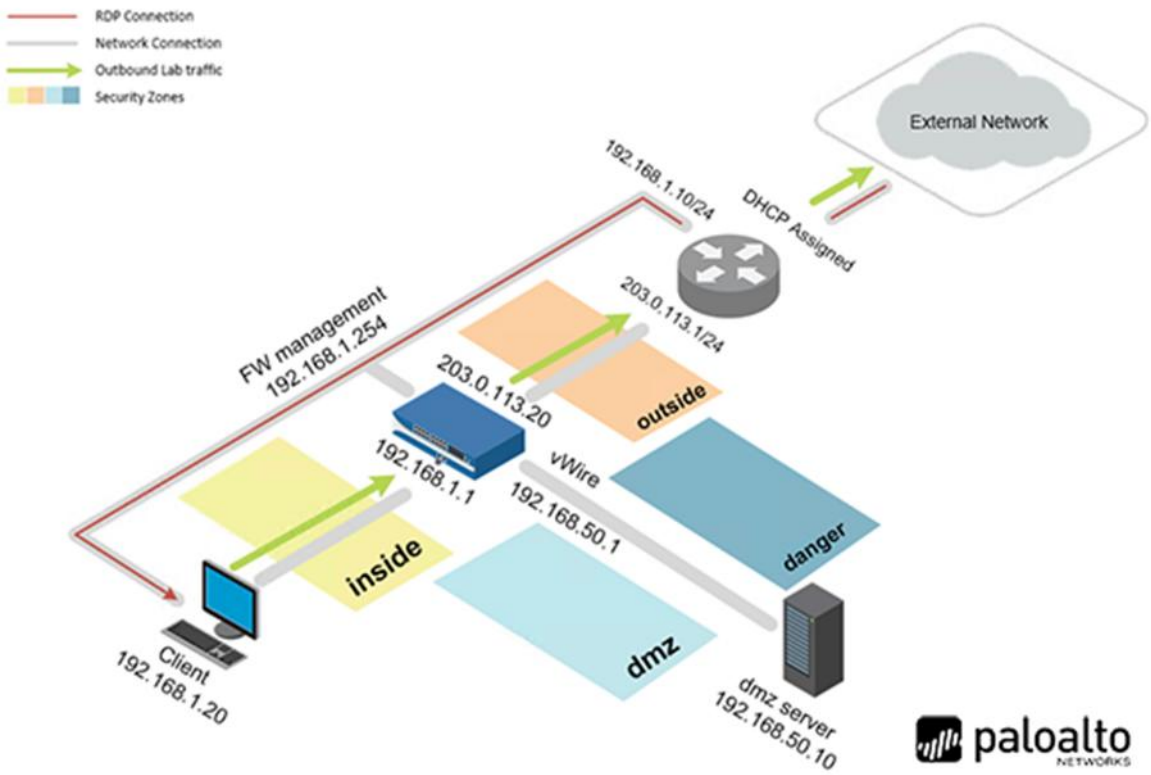
Introduction

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.

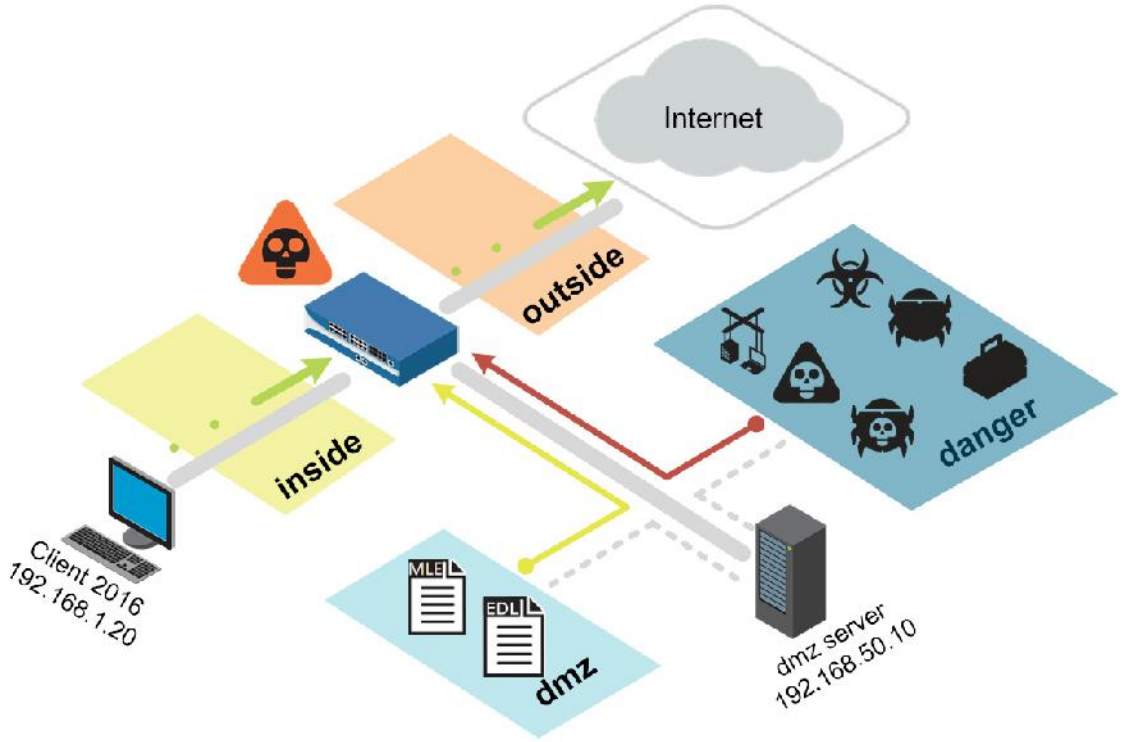
Objectives

- 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.

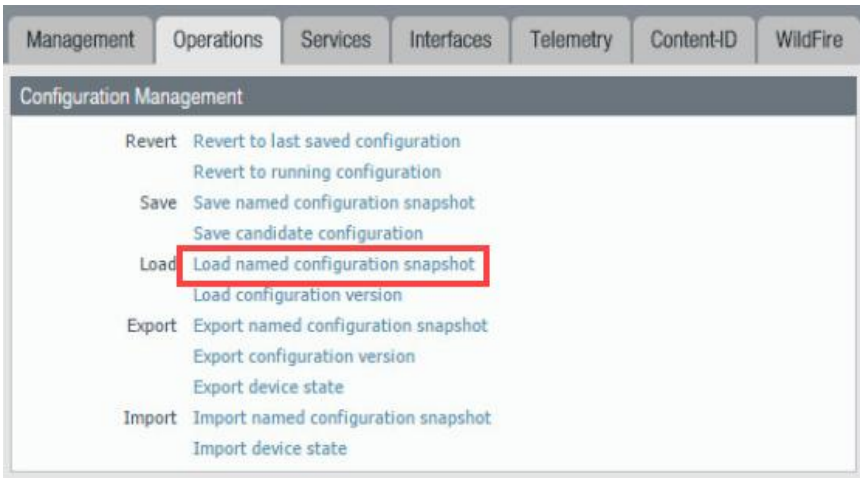
2. Log in as `lab-user` using the password `Train1ng$`.

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$`

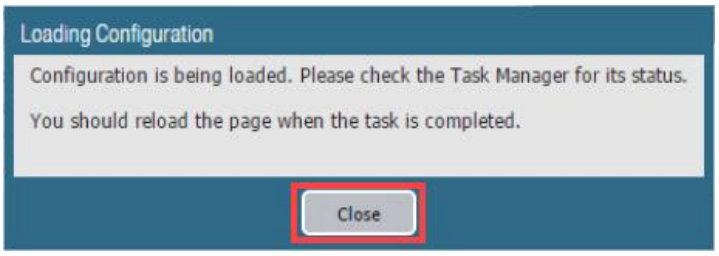
6. In the web interface, navigate to **Device > Setup > Operations**.

7. Click **Load named configuration snapshot**:



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

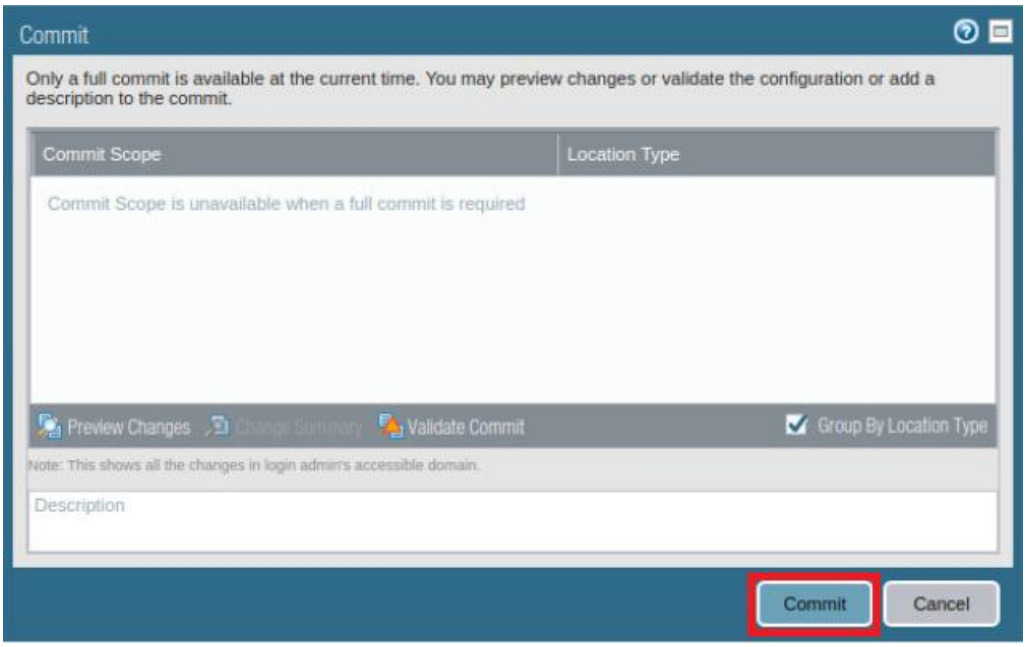
9. Click **Close**.



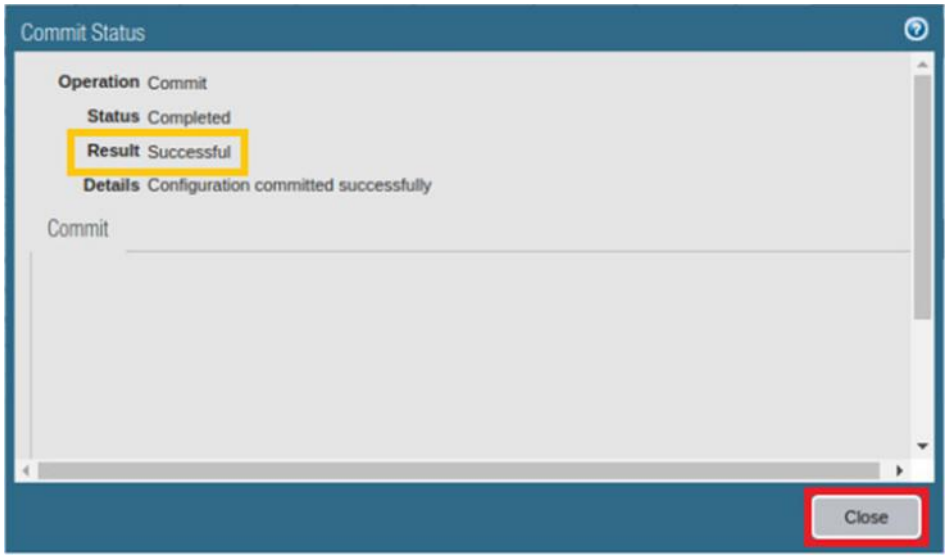
The following instructions are the steps to execute a **"Commit All"** as you will perform many times throughout these labs.

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

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



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

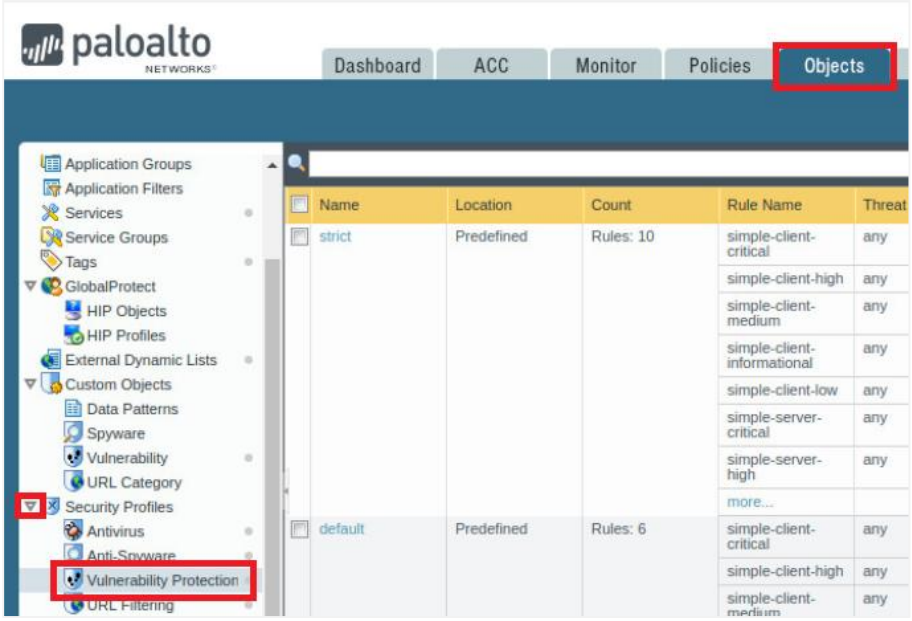


13. Leave the firewall web interface open to continue with the next task.

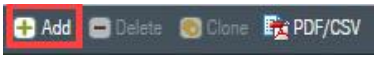
5.1 Create Security Policy Rule with a Vulnerability Protection Profile

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.**

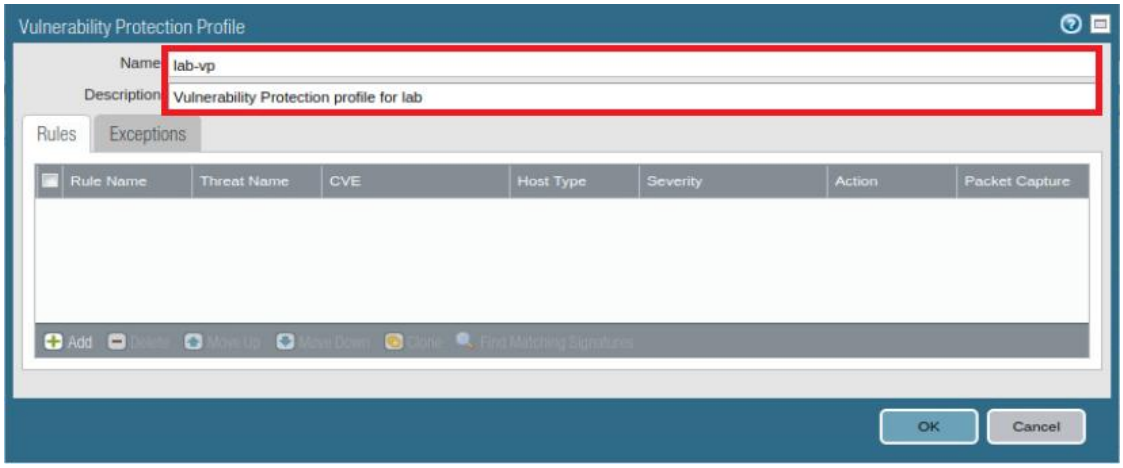


2. Click **Add** to create a *Vulnerability Protection Profile*.



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

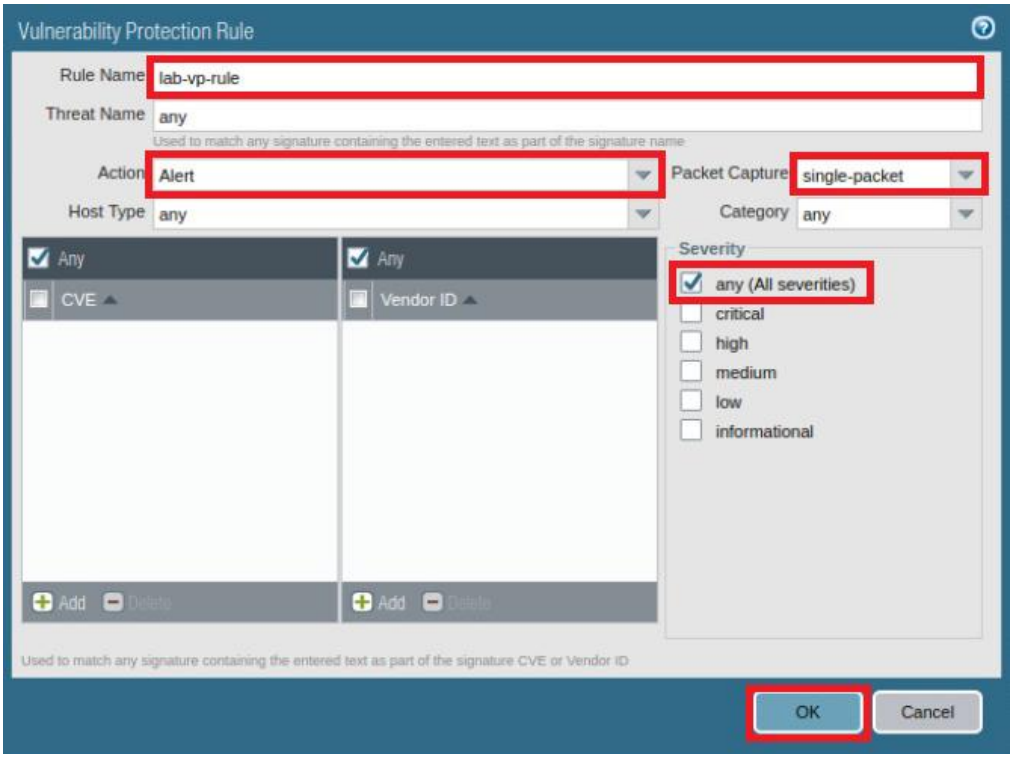
Parameter	Value
Name	`lab-vp`
Description	Type `Vulnerability Protection profile for lab`



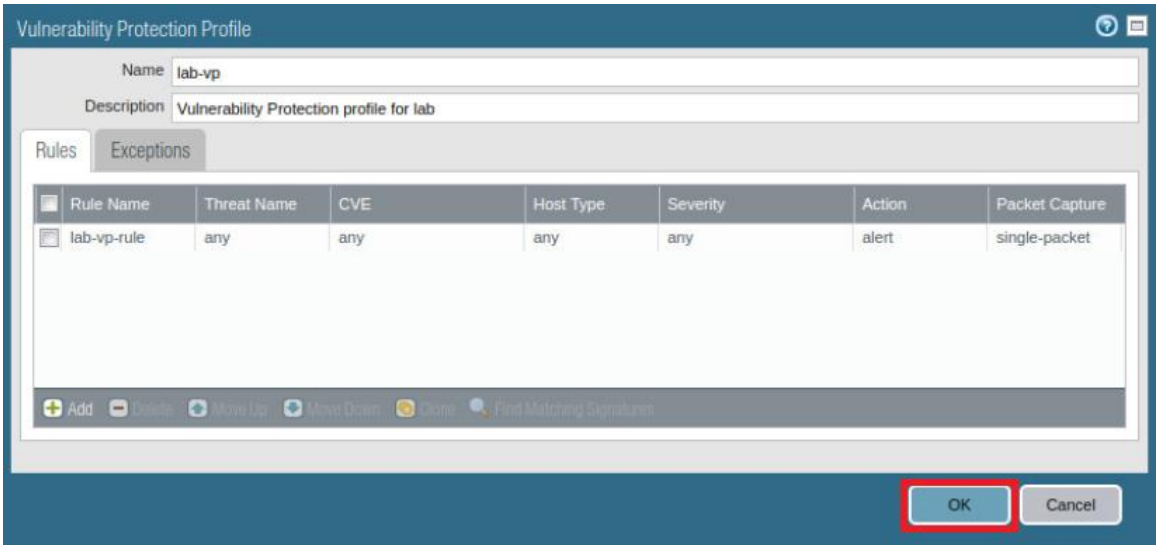
4. On the *Rules* tab, click **Add** to create a rule.

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

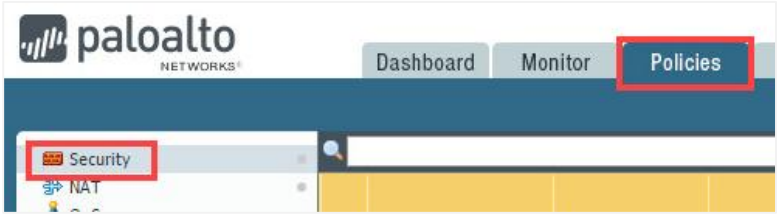
Parameter	Value
Name	`lab-vp-rule`
Action	Select **Alert** from the dropdown menu
Packet Capture	Select **single-packet** from the dropdown menu
Severity	Verify that the **any (All severities)** checkbox is selected



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



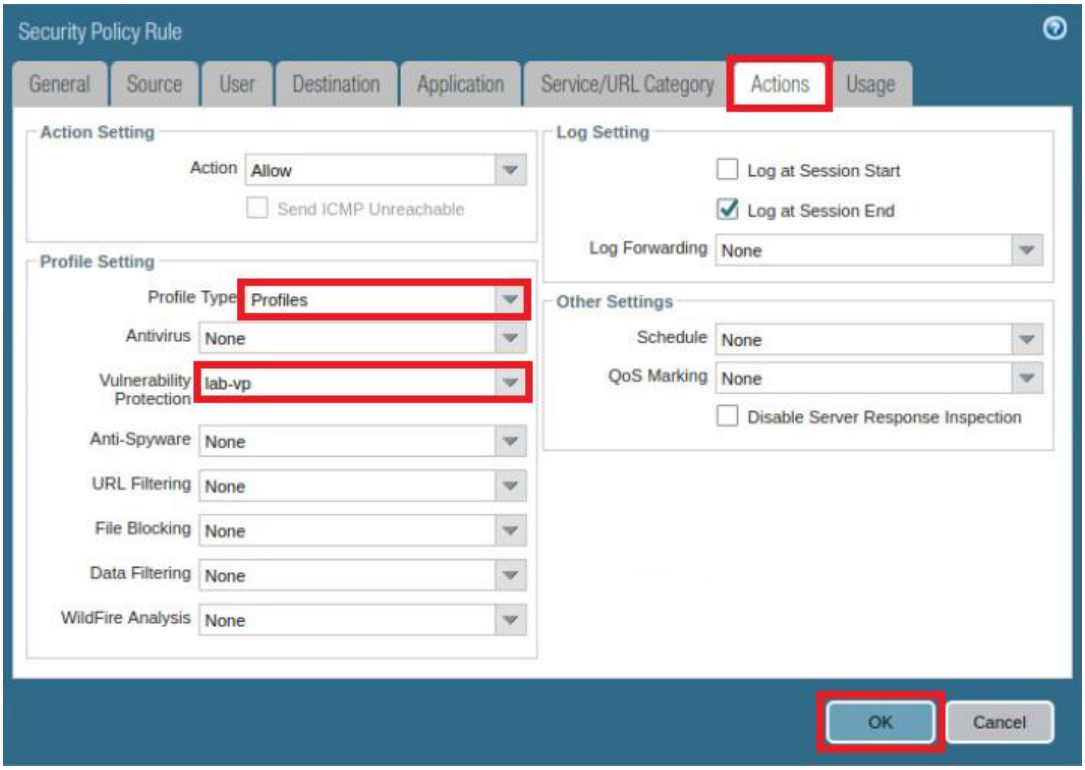
7. In the web interface, select **Policies > Security**.



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

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

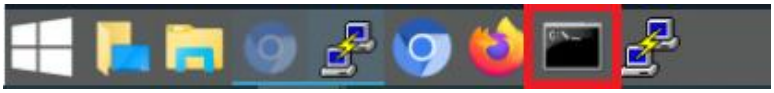
Parameter	Value
Profile Type	Select **Profiles** from the dropdown list
Vulnerability Protection	Select **lab-vp** from the dropdown list



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.

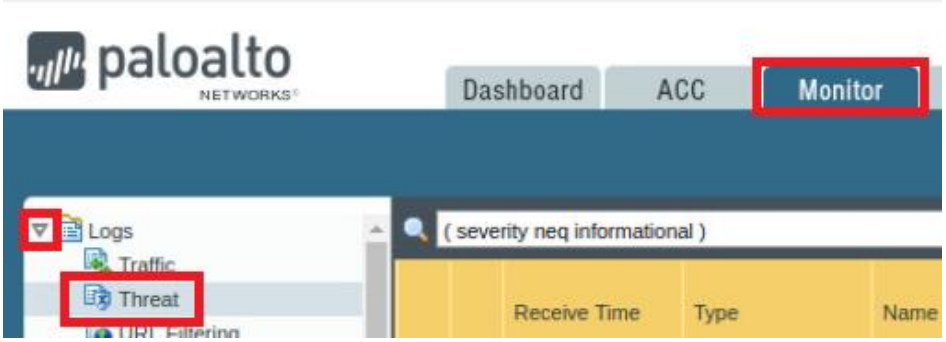
```
C:\home\lab-user> sudo nmap --script ftp-brute 192.168.50.10 -p 21
[sudo] password for lab-user:

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

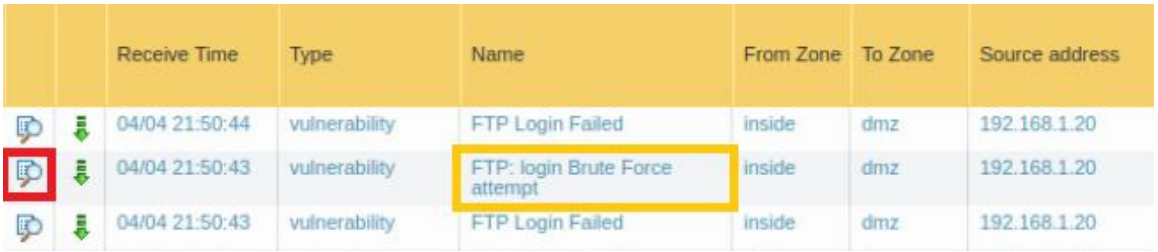
5. After the script completes, type **`exit`** followed by pressing the **Enter** key to close the Terminal.

5.3 Review the Logs

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

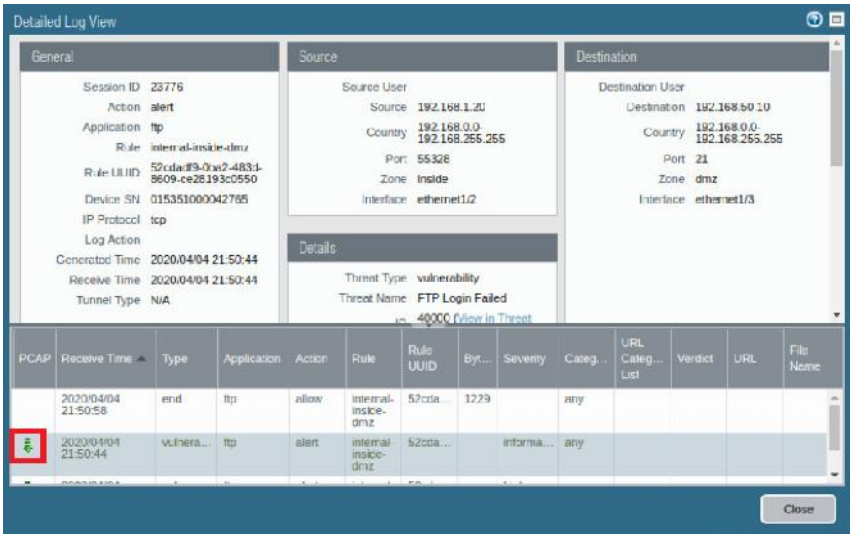


2. Make sure to clear the filter. Notice that you now have logs reflecting the FTP Brute Force attempt. However, the firewall is set only to alert. Open the **Detailed Log View** by clicking the **magnify** icon next to the most recent threat.

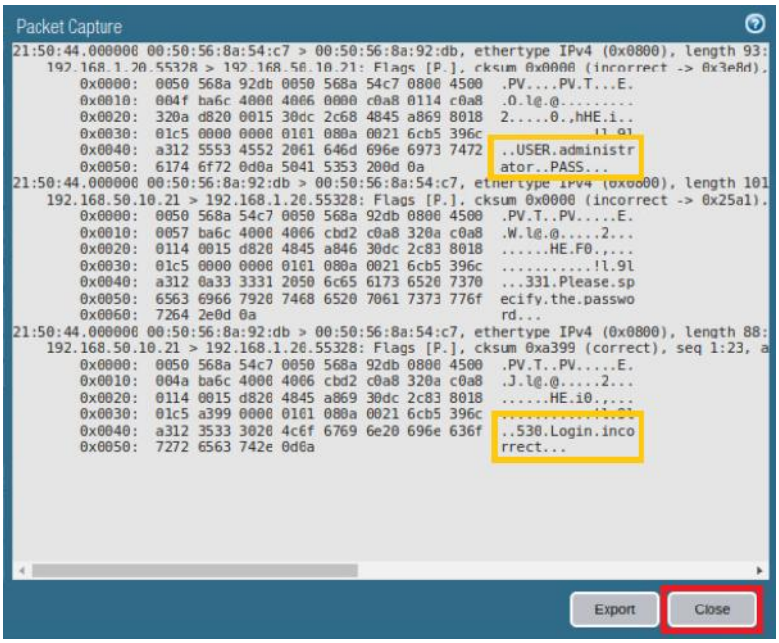


If there are no FTP: login Brute Force attempt events, the nmap command was not successful and you will need to rerun the nmap command.

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



4. 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**.

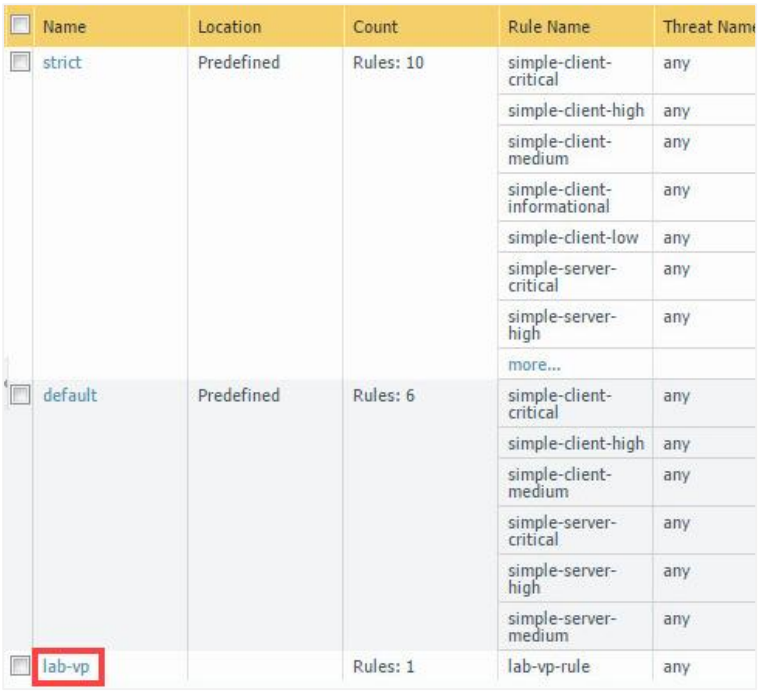


Captured packets can be exported in pcap format and examined with an offline analyzer for further investigation.

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

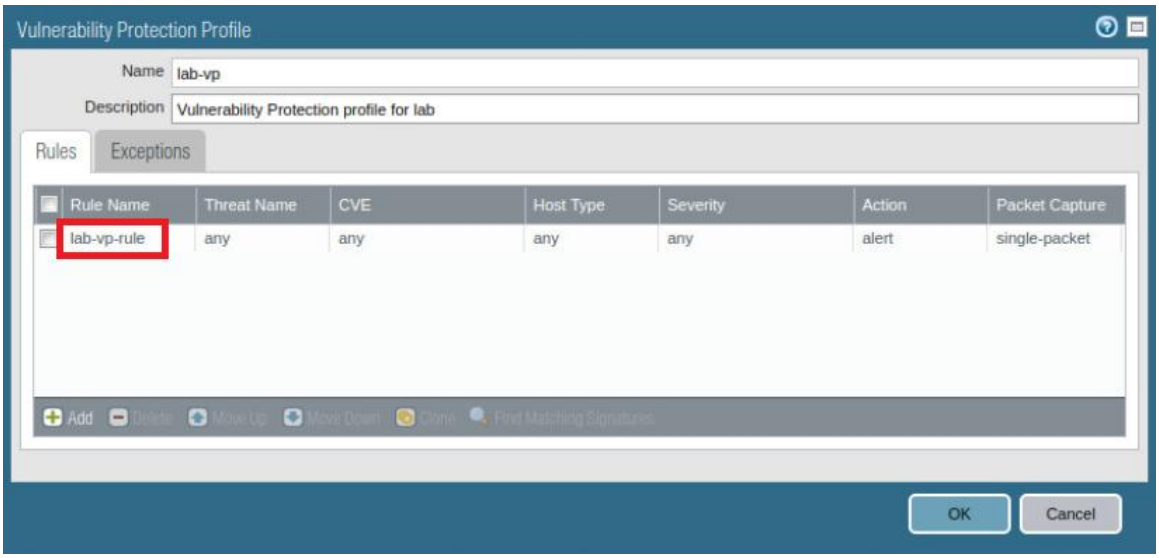
5.4 Update the Vulnerability Profile

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



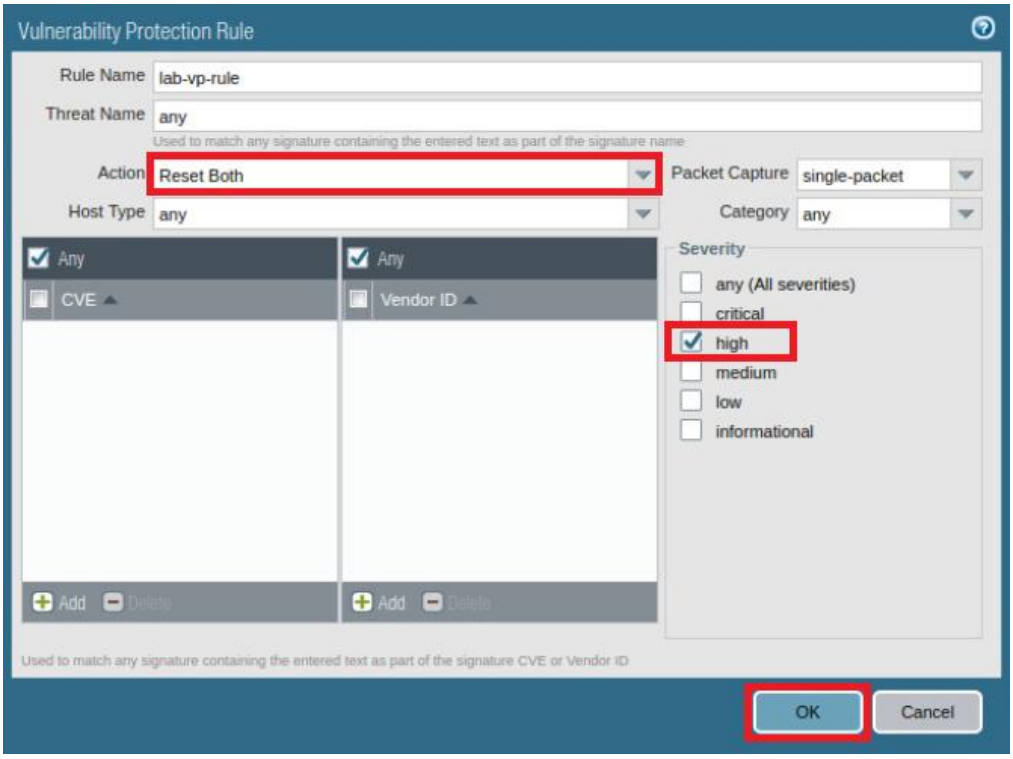
Name	Location	Count	Rule Name	Threat Name
strict	Predefined	Rules: 10	simple-client-critical	any
			simple-client-high	any
			simple-client-medium	any
			simple-client-informational	any
			simple-client-low	any
			simple-server-critical	any
			simple-server-high	any
			more...	
default	Predefined	Rules: 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
lab-vp		Rules: 1	lab-vp-rule	any

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

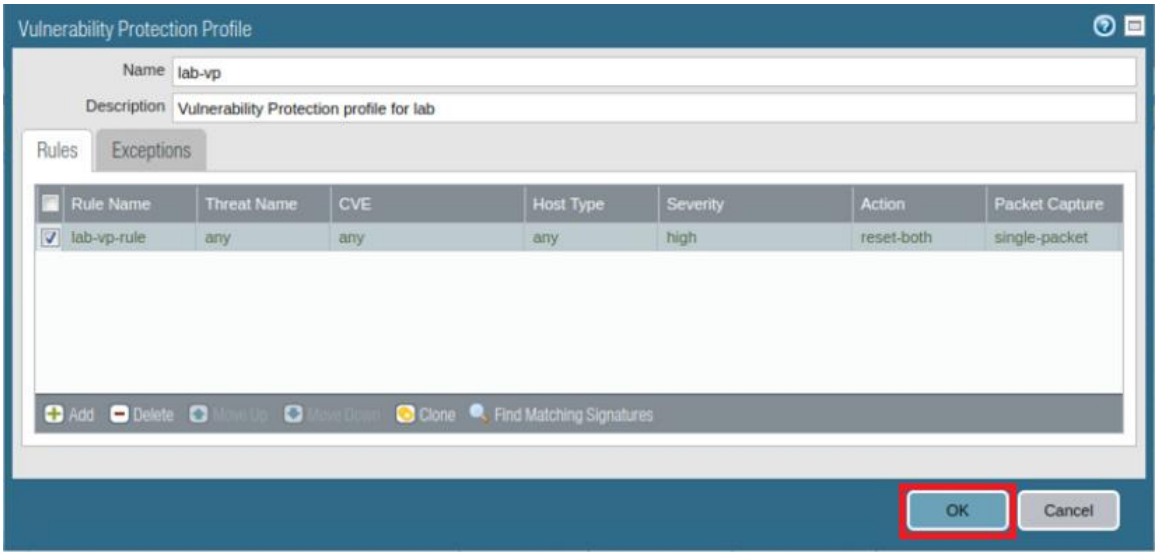


4. In the *Vulnerability Protection Rule* window, configure the following. Once finished, click **OK**.

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



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



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

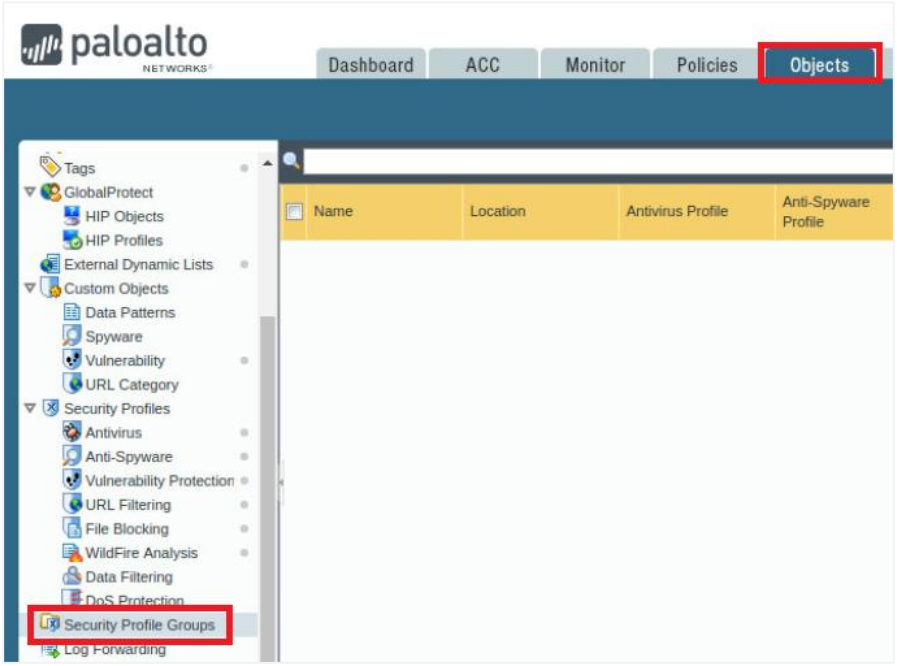
If there are no FTP: login Brute Force attempt events, the nmap command was not successful and you will need to rerun the nmap command.

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

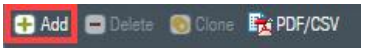
5.5 Create a Security Profile Group

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**.

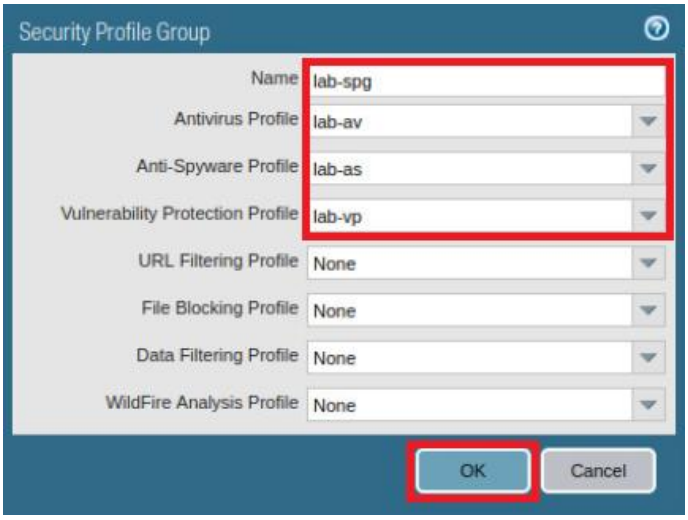


2. Click **Add** to create a *Security Profile Group*.

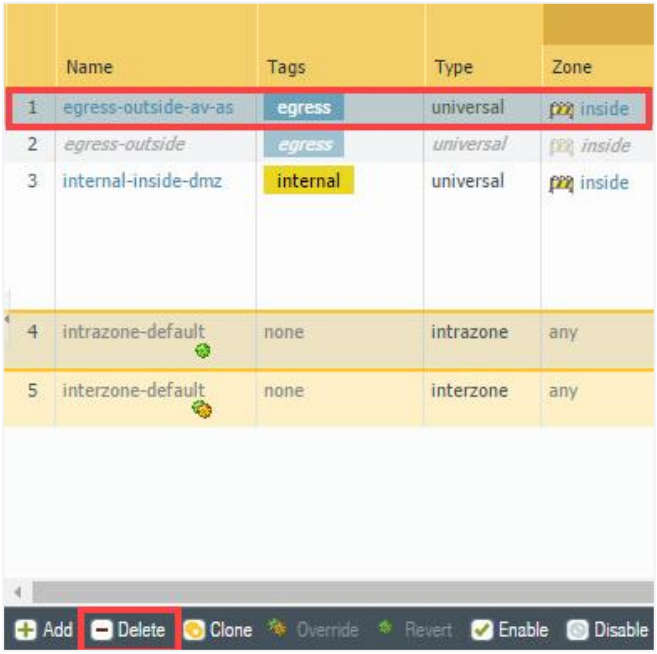


3. In the *Security Profile Group* window, configure the following. Once finished, click **OK**.

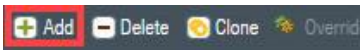
Parameter	Value
Name	`lab-spg`
Antivirus Profile	Select **lab-av**
Anti-Spyware Profile	Select **lab-as**
Vulnerability Protection Profile	Select **lab-vp**



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

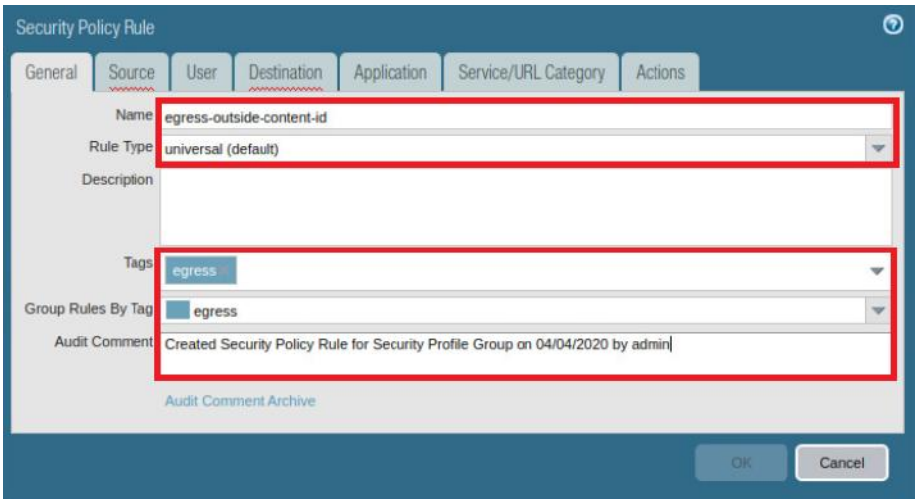


6. When prompted, click **Yes** to continue with the deletion.
7. Click **Add** to define a new *Security Policy Rule*.



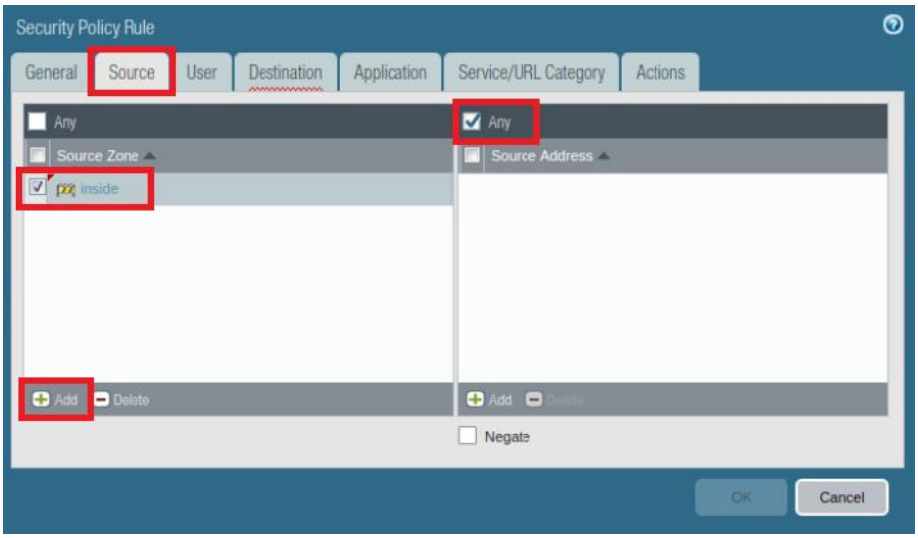
8. In the *Security Policy Rule* window, while on the *General* tab, configure the following.

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`.



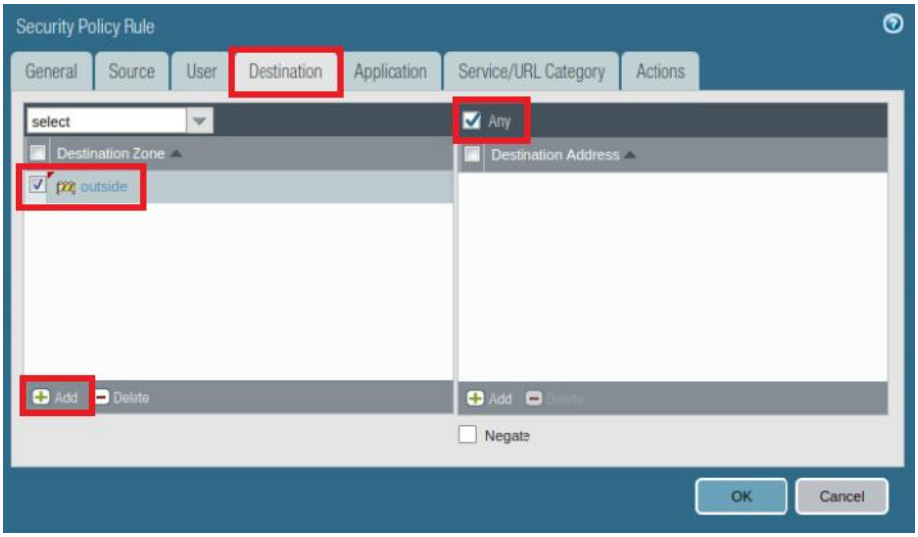
9. In the *Security Policy Rule* window, click the **Source** tab to configure the following.

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

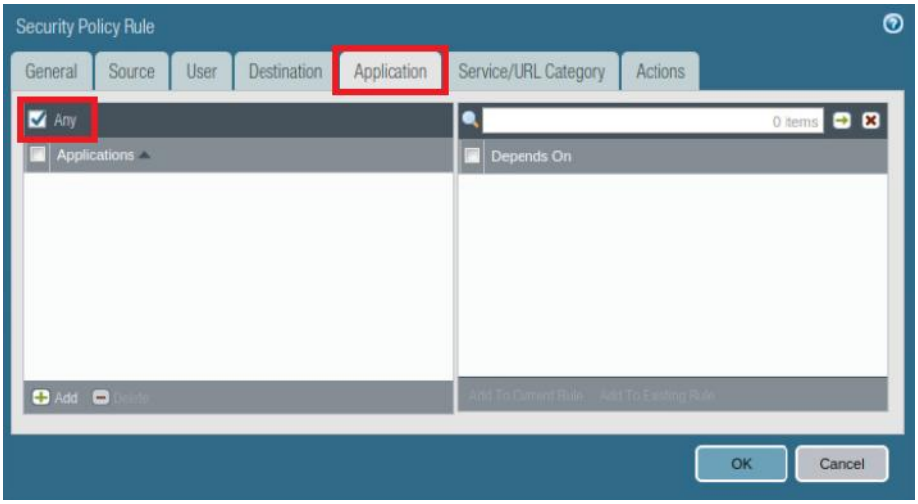


10. In the *Security Policy Rule* window, click the **Destination** tab and configure the following.

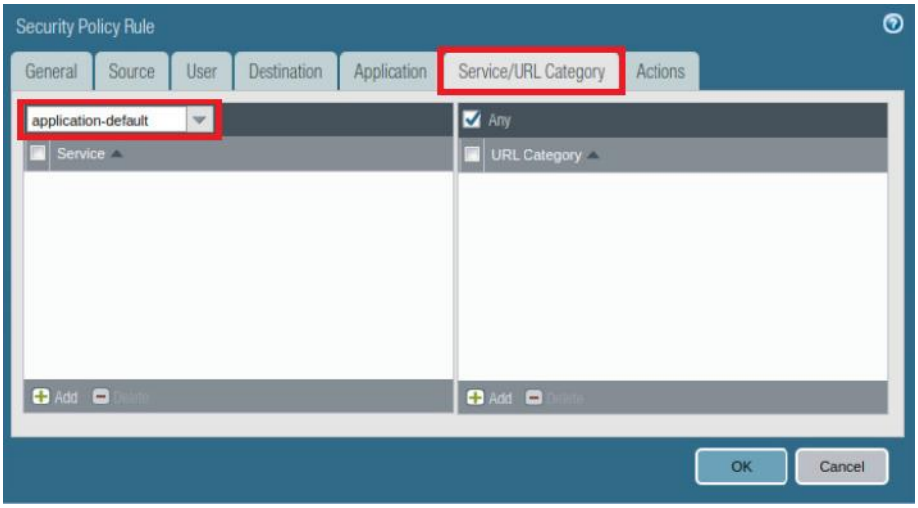
Parameter	Value
Destination Zone	Click **Add** and select **outside** from the dropdown list
Destination Address	Verify that the **Any** checkbox is selected



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

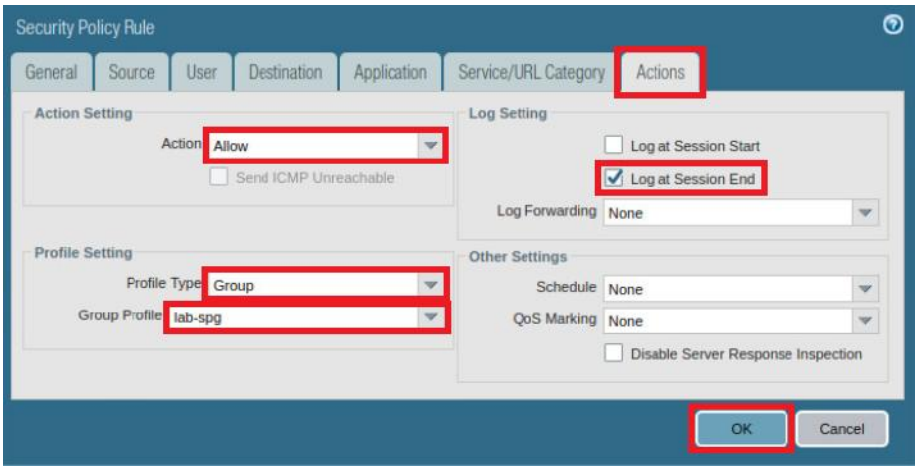


12. In the *Security Policy Rule* window, click the **Service/URL Category** tab and verify that **application-default** is selected.

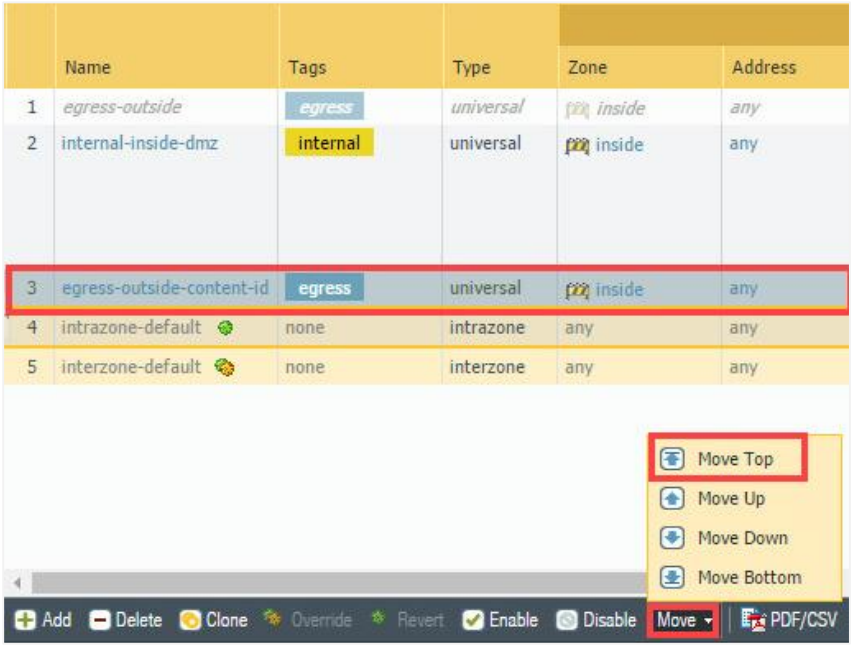


13. In the *Security Policy Rule* window, click the **Actions** tab and configure the following. Once finished, click **OK**.

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**.

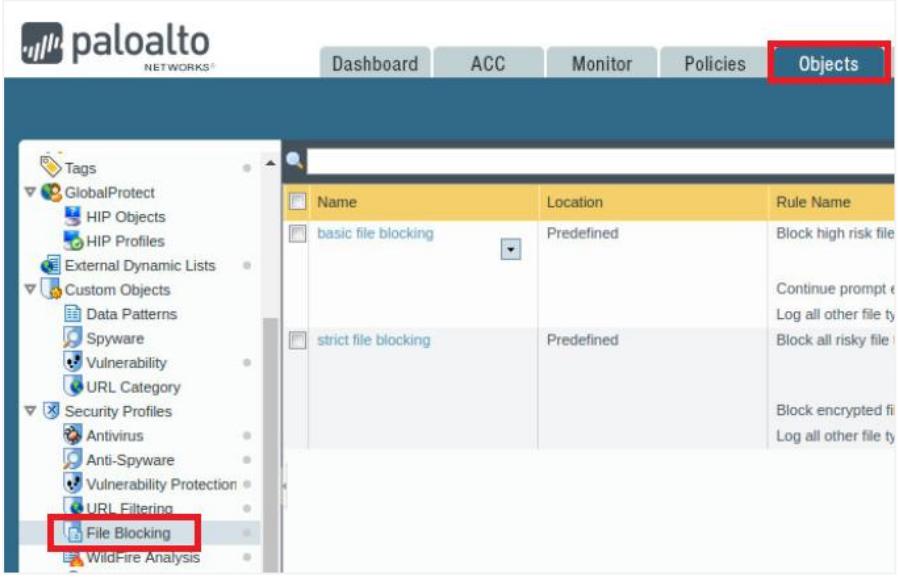


15. Leave the firewall web interface open to continue with the next task.

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.

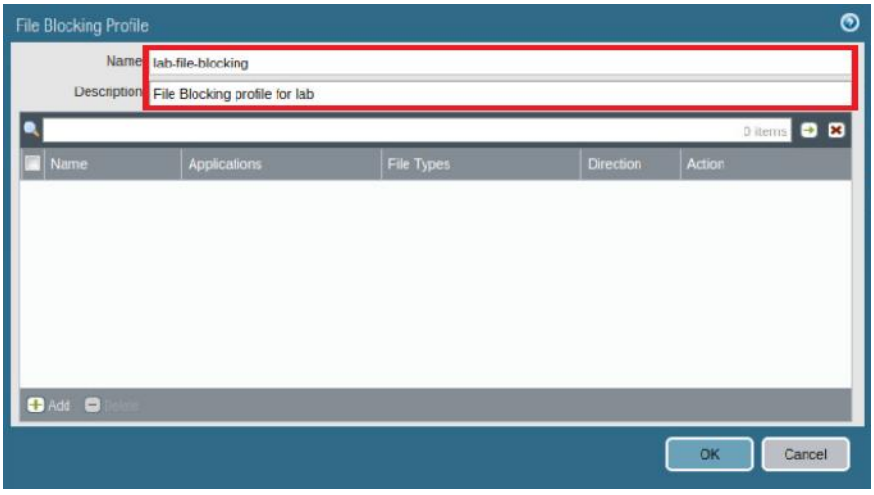
1. In the web interface, select **Objects > Security Profiles > File Blocking**.



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`

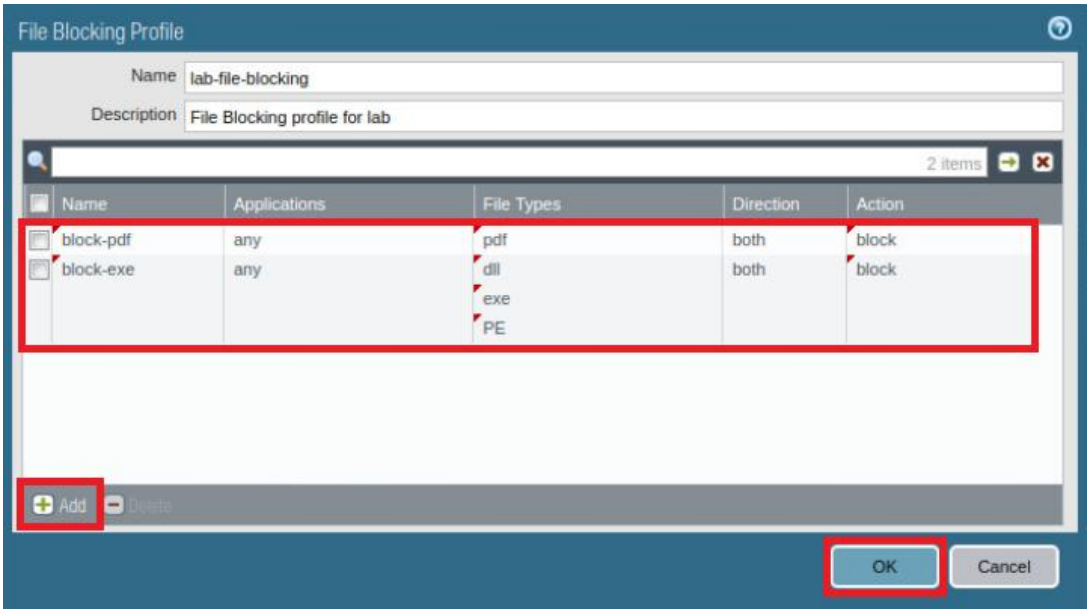


4. In the *File Blocking Profile* window, click **Add** and configure the following.

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**.

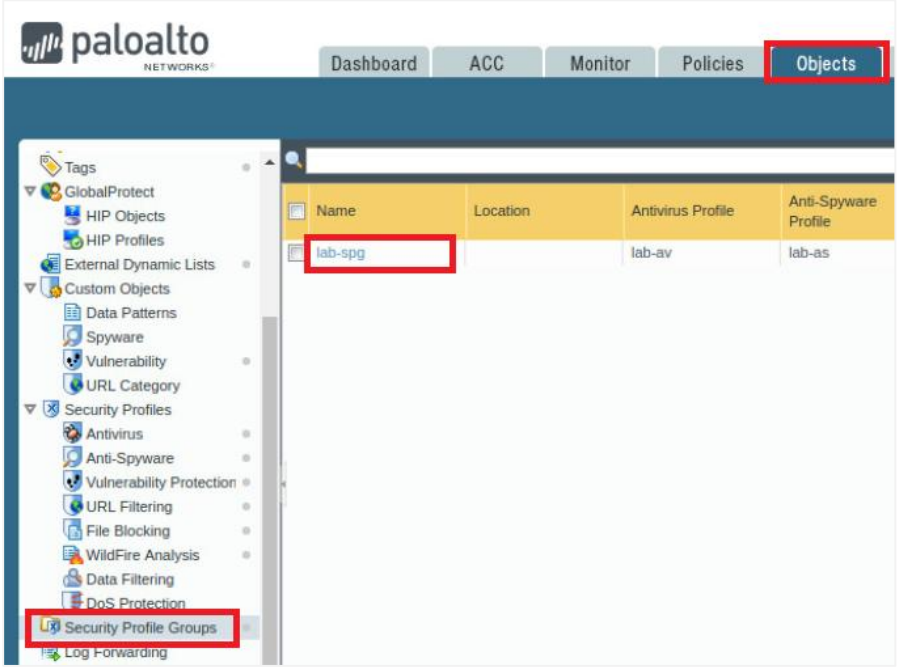
Parameter	Value
Name	Type `block-exe`
Applications	Verify that **any** is selected
File Types	Click **Add** and select the following from the dropdown list: **dll** **exe** **PE**
Direction	Verify that **both** is selected
Action	Select **block** from the dropdown list



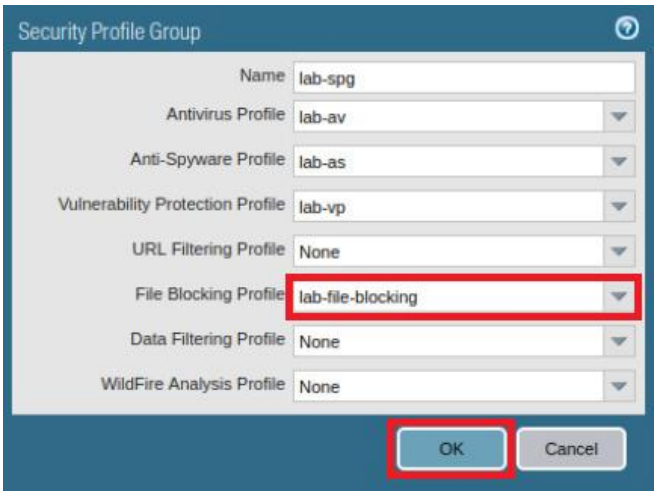
6. Verify that the new profile appears in the list. Leave the firewall web interface open to continue with the next task.

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**.



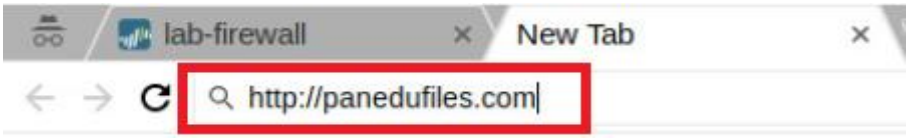
2. In the *Security Profile Group* window, select **lab-file-blocking** from the *File Blocking Profile* dropdown list and click **OK**.



3. **Commit** all changes.

5.8 Test the File Blocking Profile

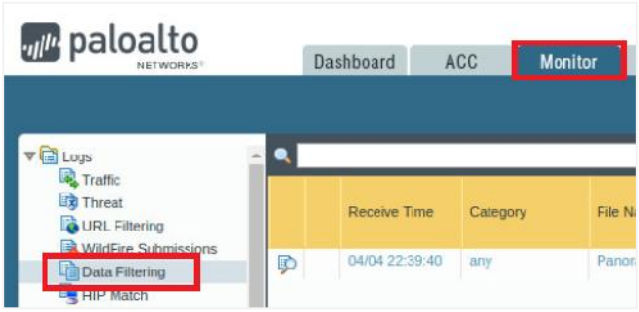
1. Open a new tab in **Chromium Web Browser** and browse to `http://www.panedufiles.com/`.



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	Destinatio 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.

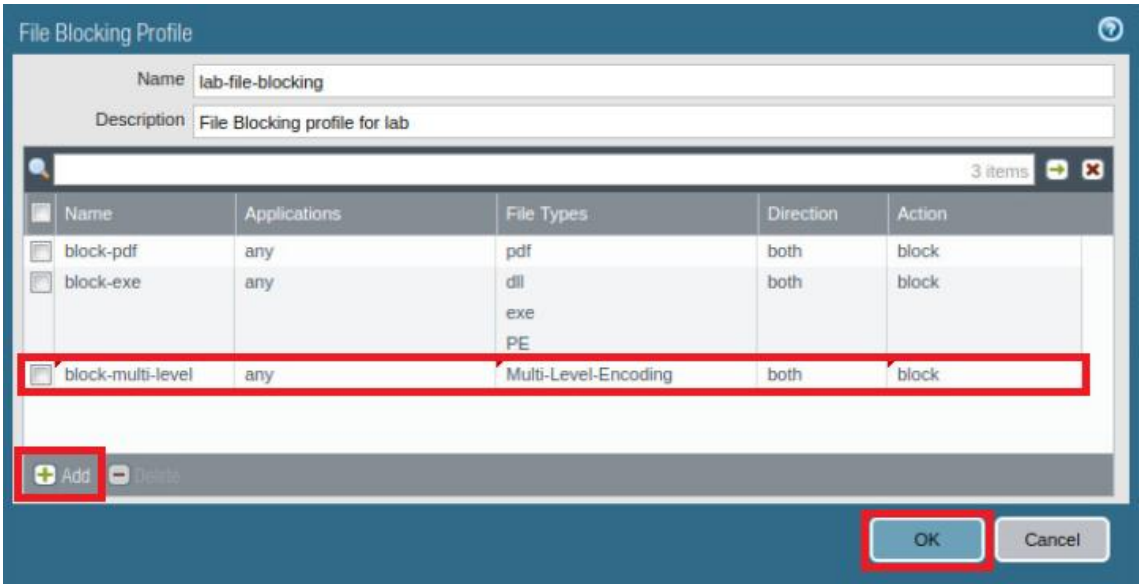
5.9 Create a File Blocking Profile to Block Multi-Level Encoded Files

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.

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

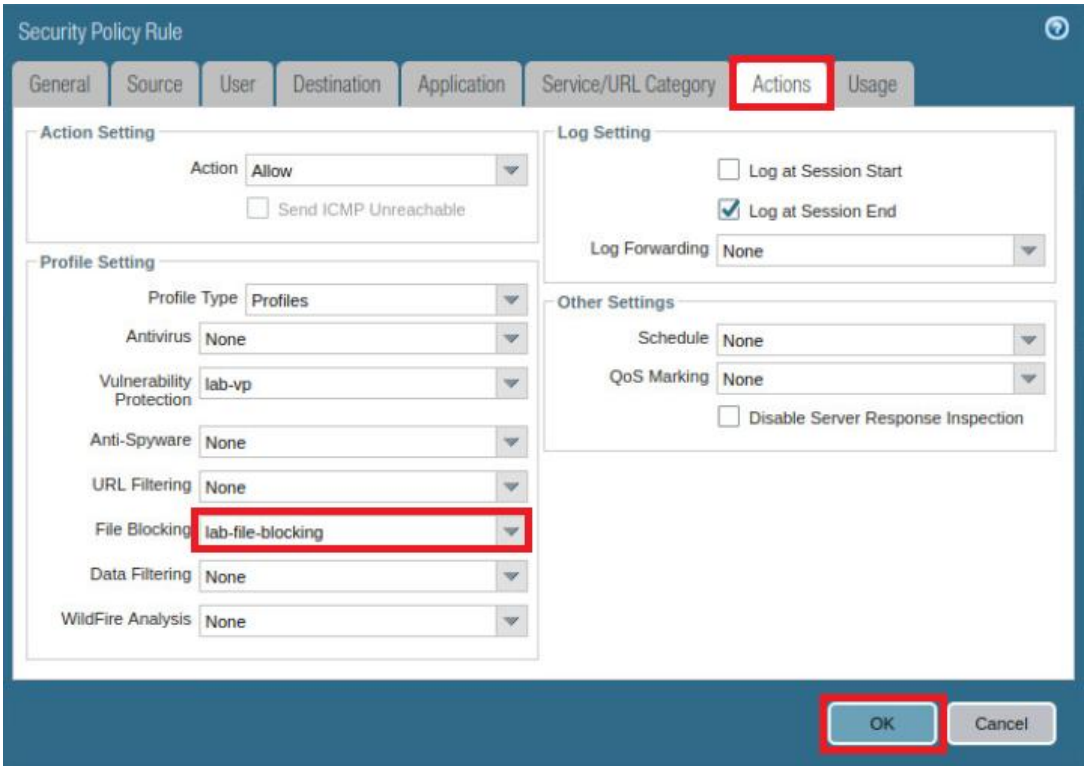


4. Leave the firewall web interface open to continue with the next task.

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.

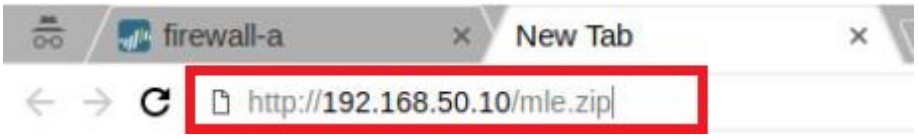
3. In the *Security Policy Rule* window, click the **Actions** tab and then select **lab-file-blocking** from the *File Blocking* dropdown list. Click **OK**.



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`.

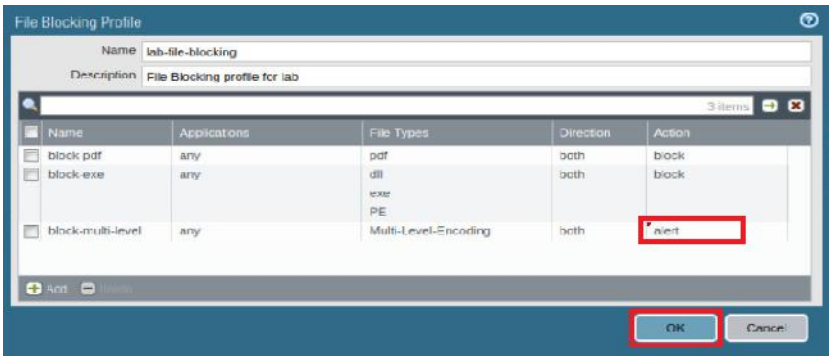


2. Notice that the file is blocked in accordance with the new file blocking rule. Close the browser tab.

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.

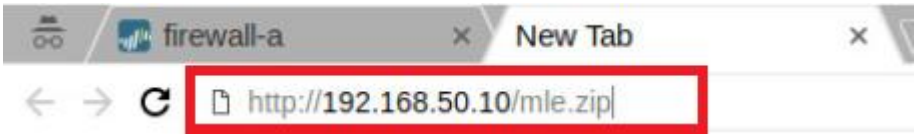
3. In the *File Blocking Profile* window, select the **block-multi-level** rule and change the *Action* to **alert**. Click **OK**.



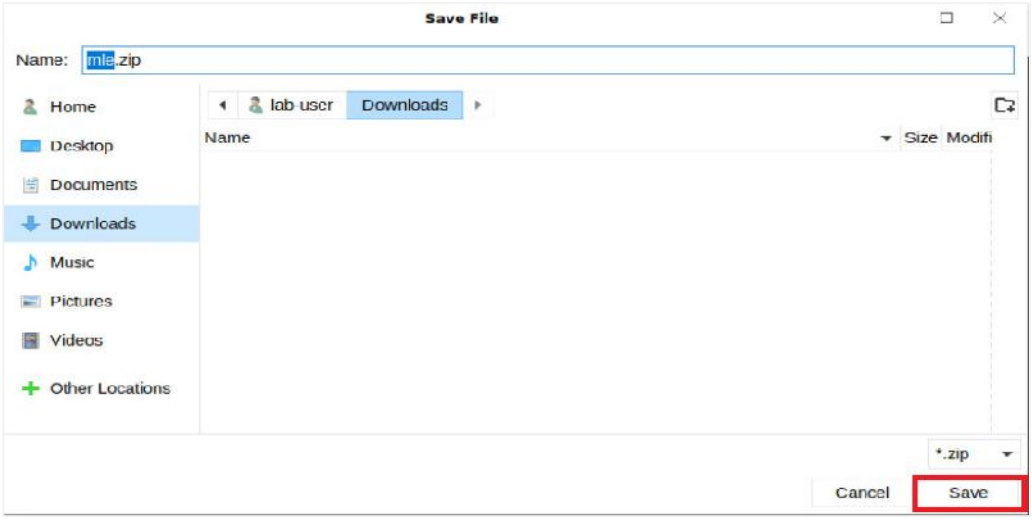
4. **Commit** all changes.

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`.

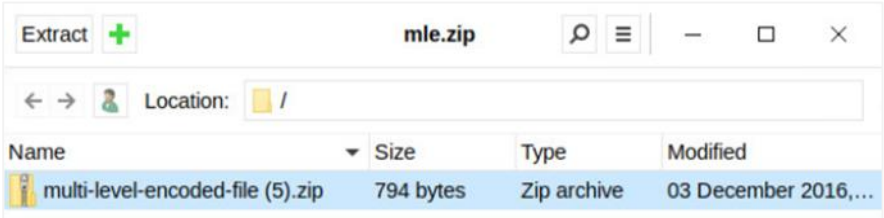


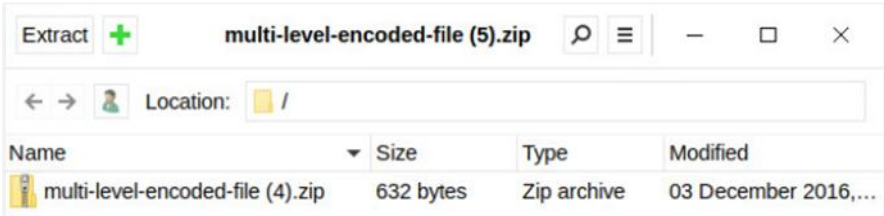
2. In the *Save File* window, save the report to the **Downloads** directory and click **Save**.



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.





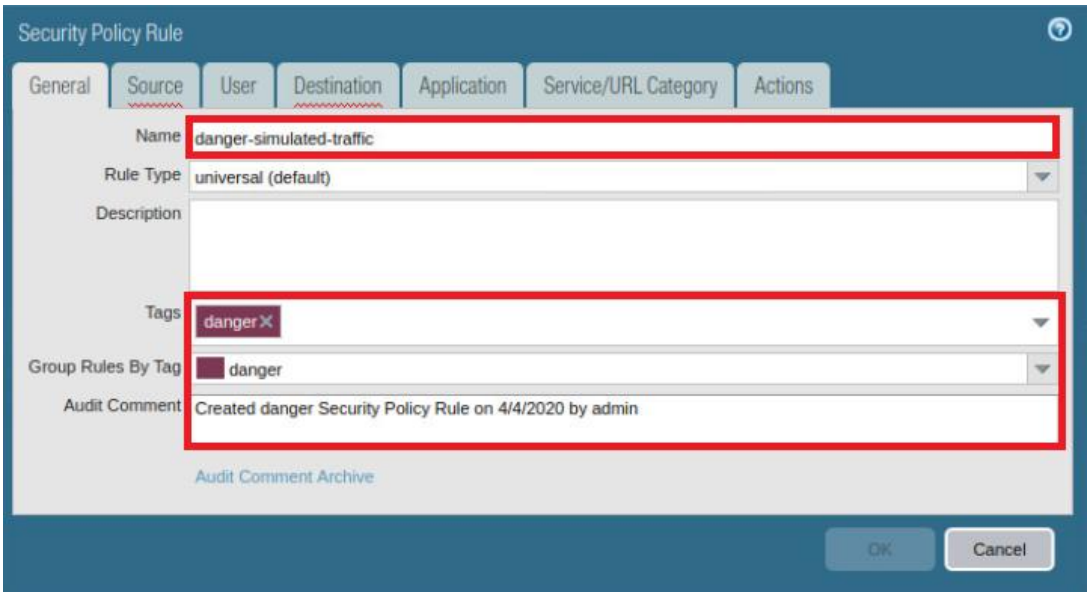
5.14 Create a Danger Security Policy Rule

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.

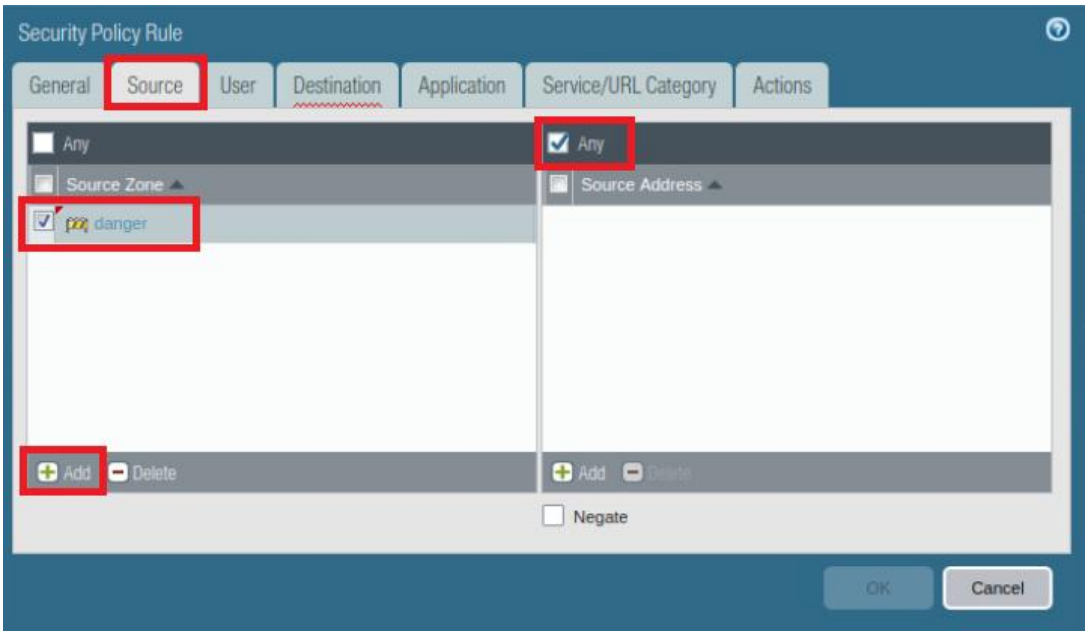
3. In the *Security Policy Rule* window, while on the *General* tab, configure the following.

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`



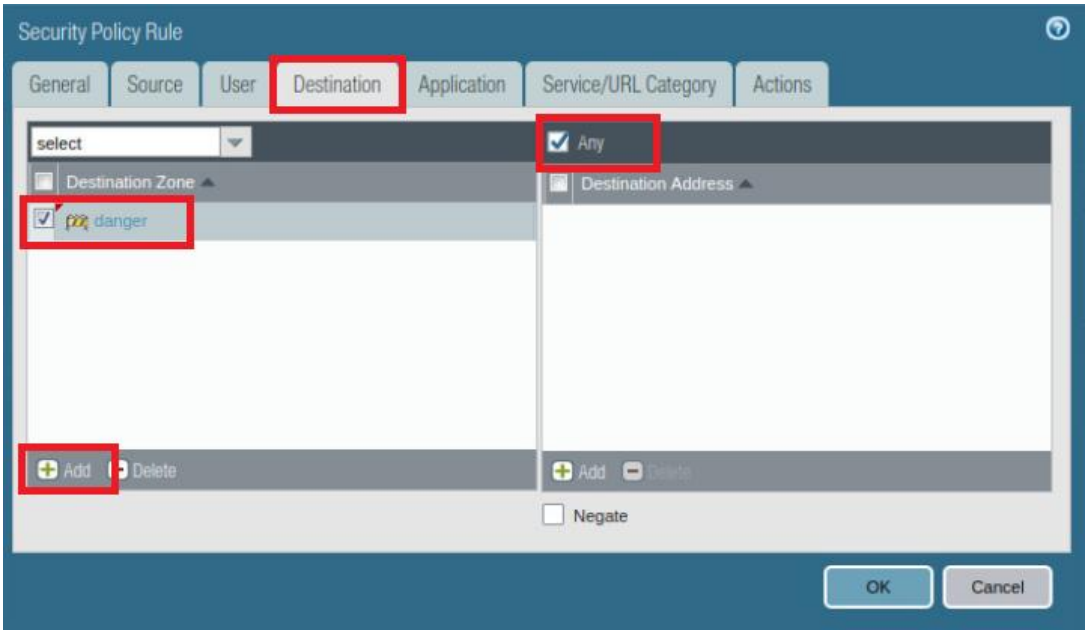
4. Click on the **Source** tab and configure the following.

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



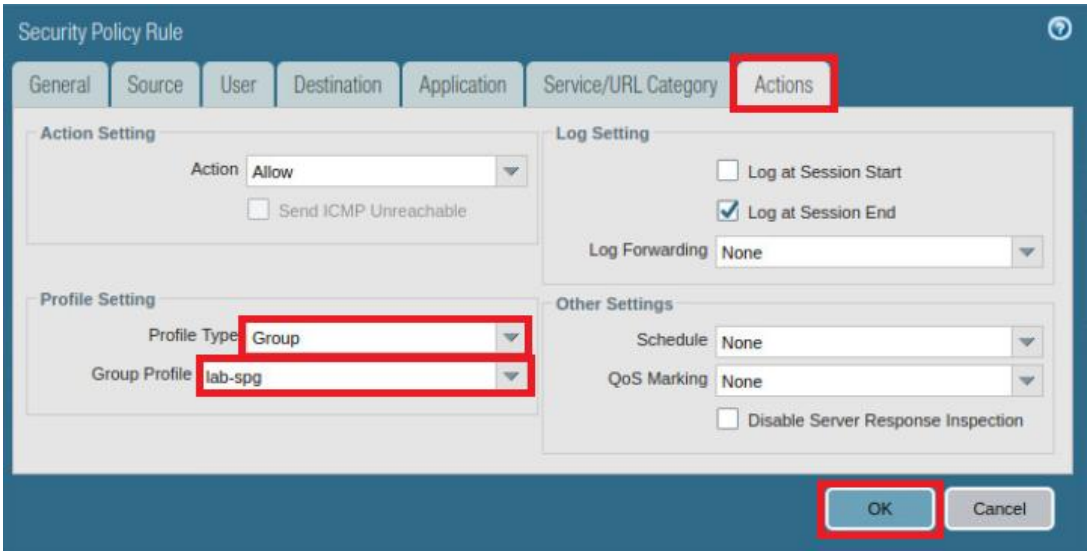
5. Click on the **Destination** tab and configure the following.

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

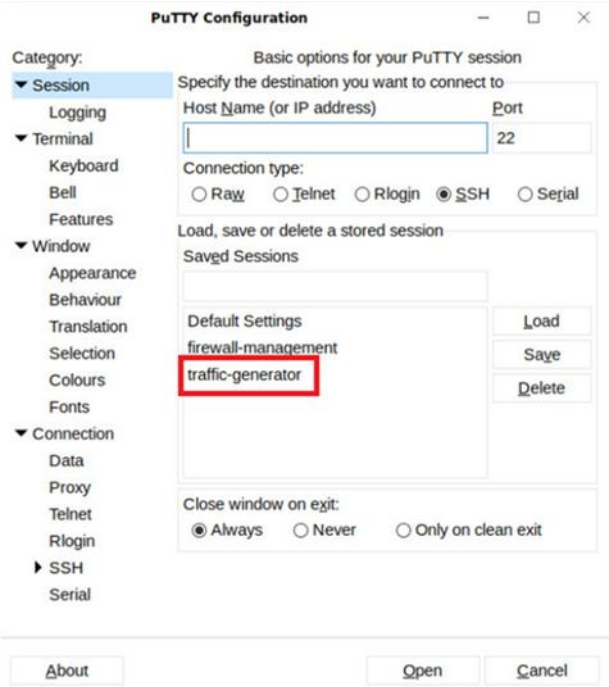


7. **Commit** all changes.

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**.



3. Log in as **root** with **Pal0Alt0** 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 ~]#
```

4. 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 (ENOBUFS): 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 (ENOBUFS): 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 (ENOBUFS): 0
        Retried packets (EAGAIN):  0
[root@pod-dmz ~]#
```

5. Leave the *PuTTY* window open and change focus to the firewall web interface.
6. In the web interface, navigate to **Monitor > Logs > Threat**.
7. 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		172.217.164.174		443	google-play	alert	informa

8. 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

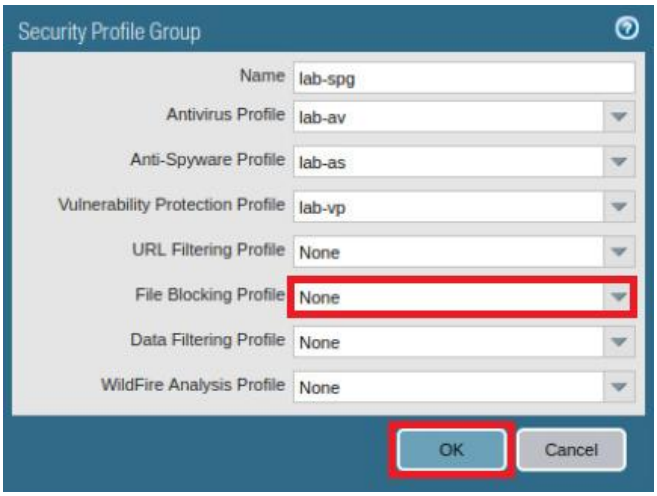
10. Leave the firewall web interface open to continue with the next task.

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.

Name	Location	Antivirus Profile	Anti-Spyware Profile
lab-spg		lab-av	lab-as

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



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.swrort.dfap	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.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

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.

