PALO ALTO NETWORKS EDU-210

Lab 5B: Content-ID

Document Version: 2019-11-12

Contents

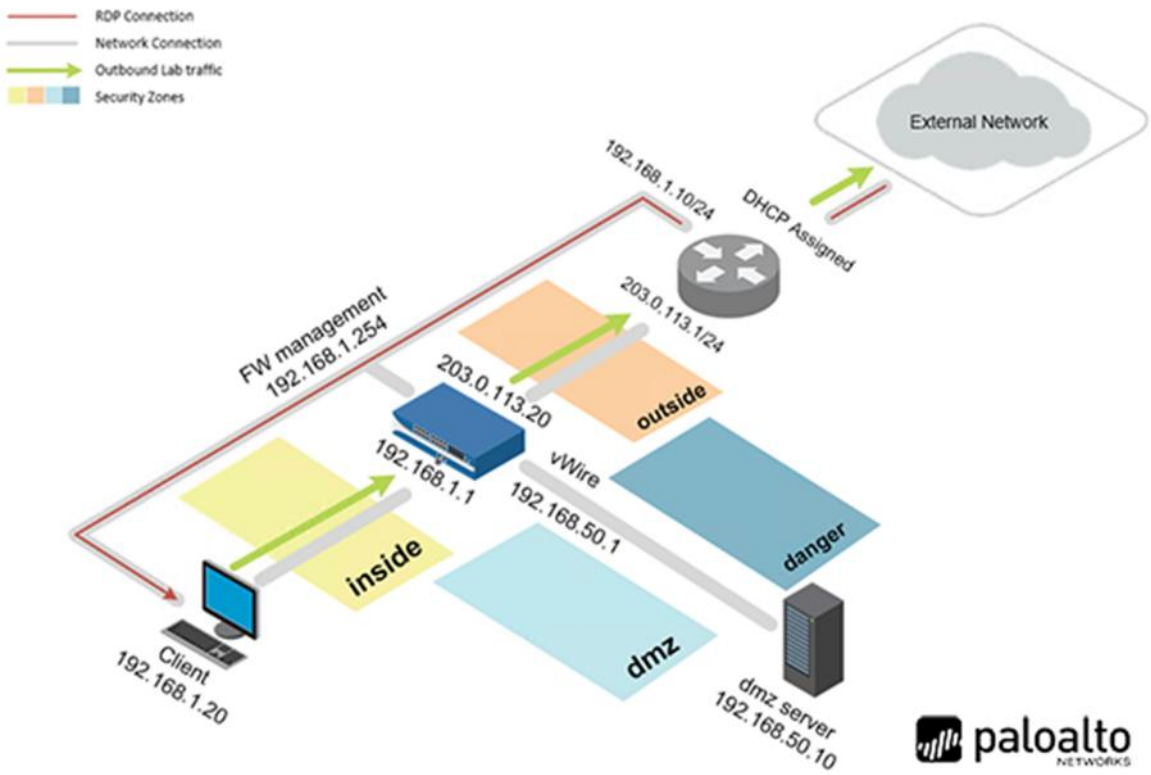
Introduction

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.

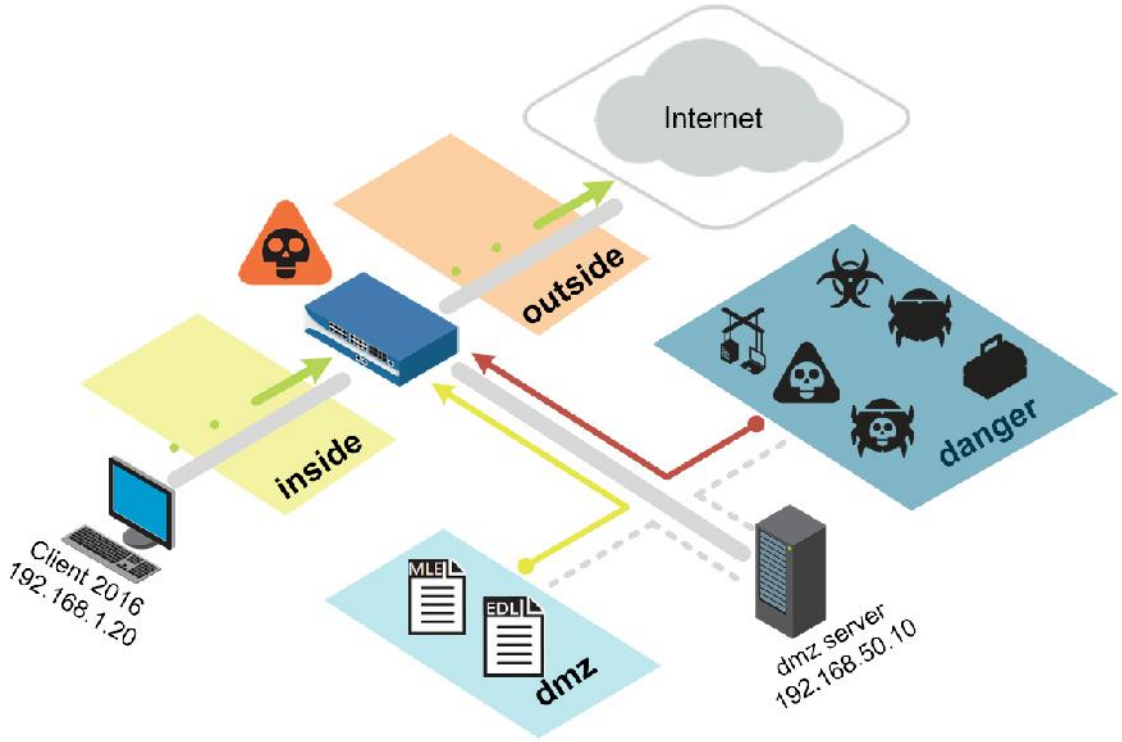
Objectives

- 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**	**Pal0Alt0**
Firewall	192.168.1.254	**admin**	**admin**

1 Content-ID

1.0 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.

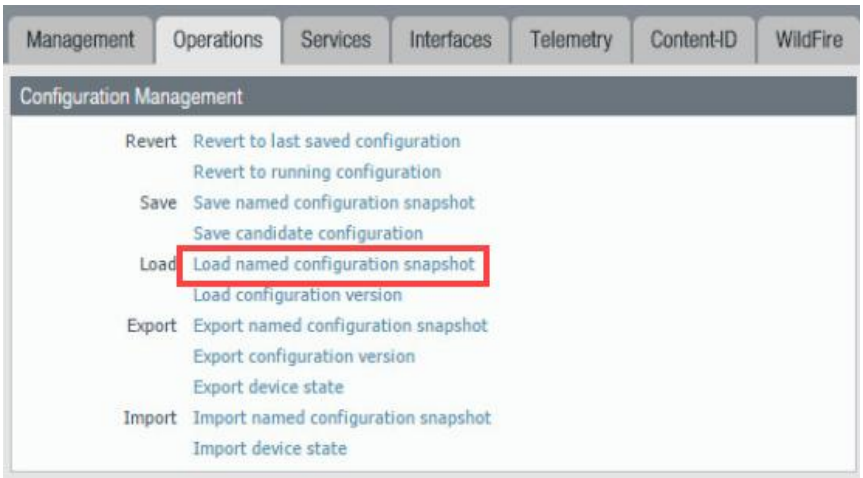
2. Click within the splash screen to bring up the login screen. Log in as **`lab-user`** using the password **`Pal0Alt0`**.

3. Launch the **Chrome** 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:

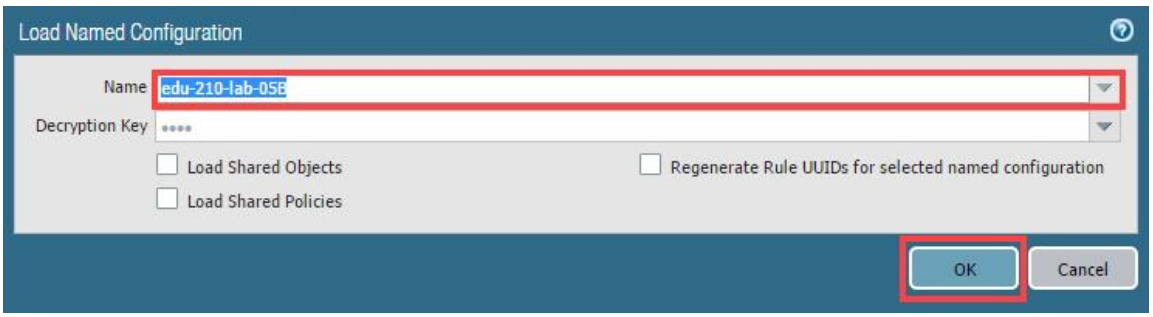
Parameter	Value
Name	**`admin`**
Password	**`admin`**

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

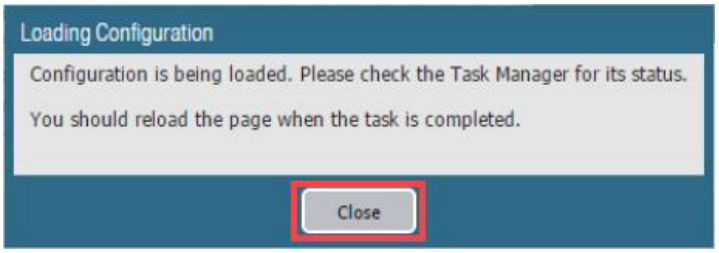
7. Click **Load named configuration snapshot**:



8. Click the drop-down list next to the *Name* text box and select **edu-210-lab-05B**. Click **OK**.



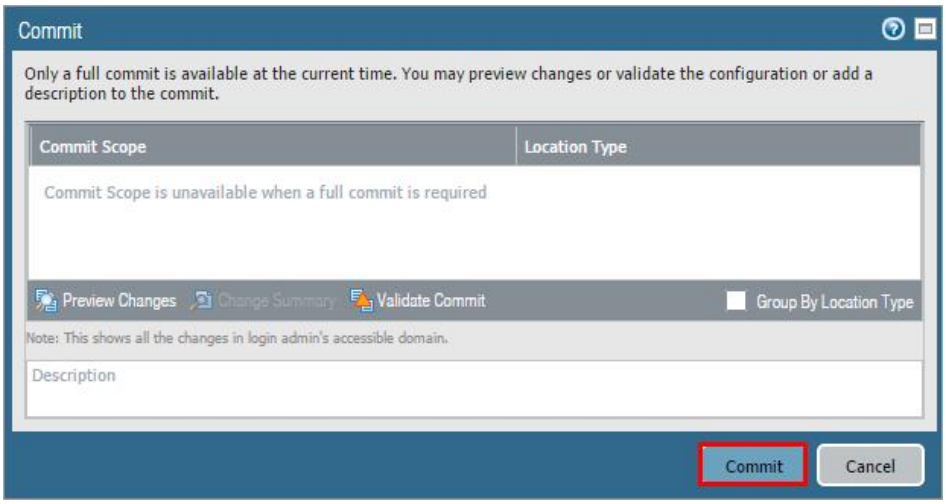
9. Click **Close**.



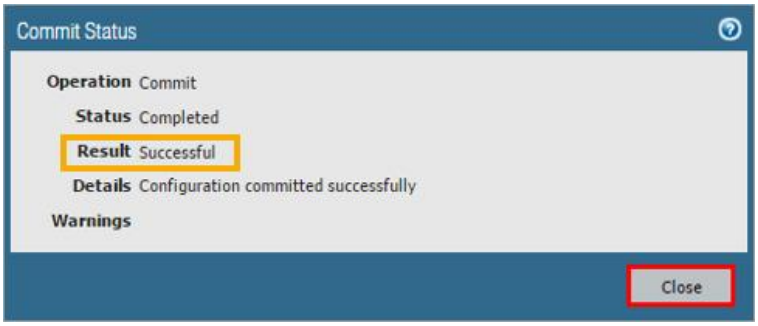
The following instructions are the steps to execute a **"Commit All"** as you will perform many times throughout these labs.

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.

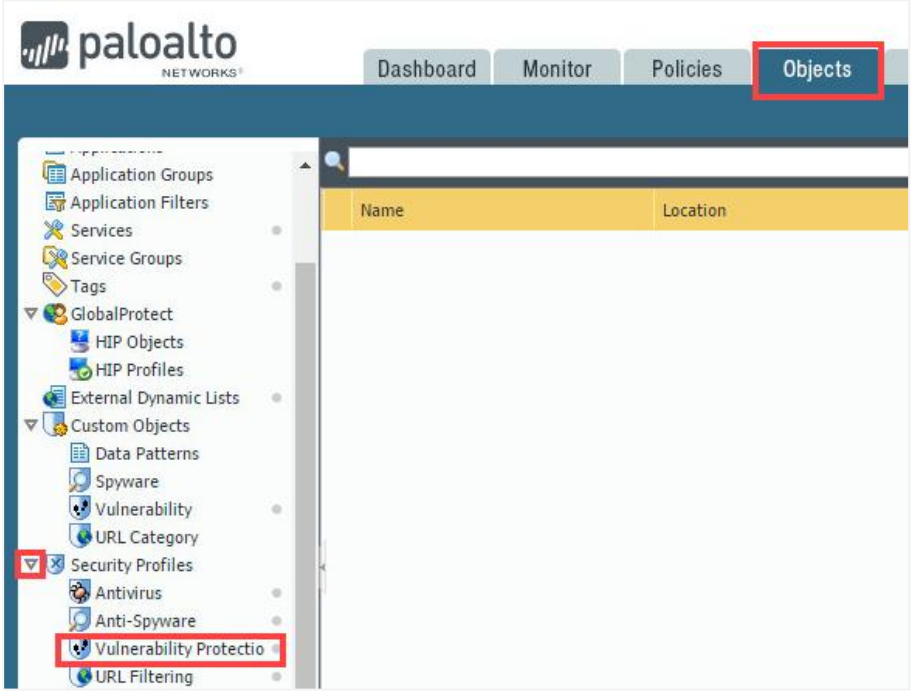


13. Leave the firewall web interface open to continue with the next task.

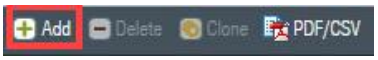
1.1 Create Security Policy Rule with a Vulnerability Protection Profile

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.**

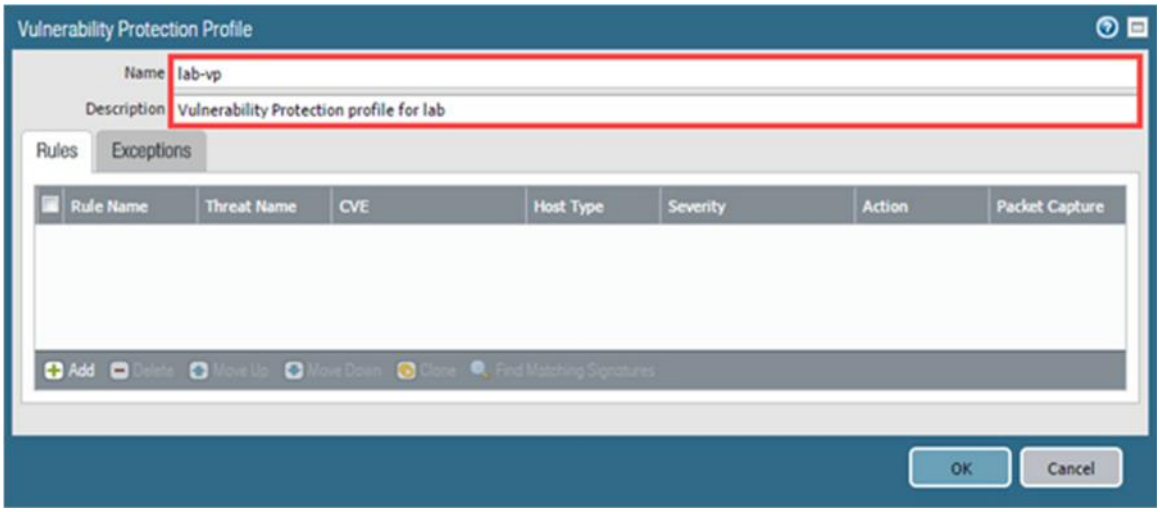


2. Click **Add** to create a *Vulnerability Protection Profile*.



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

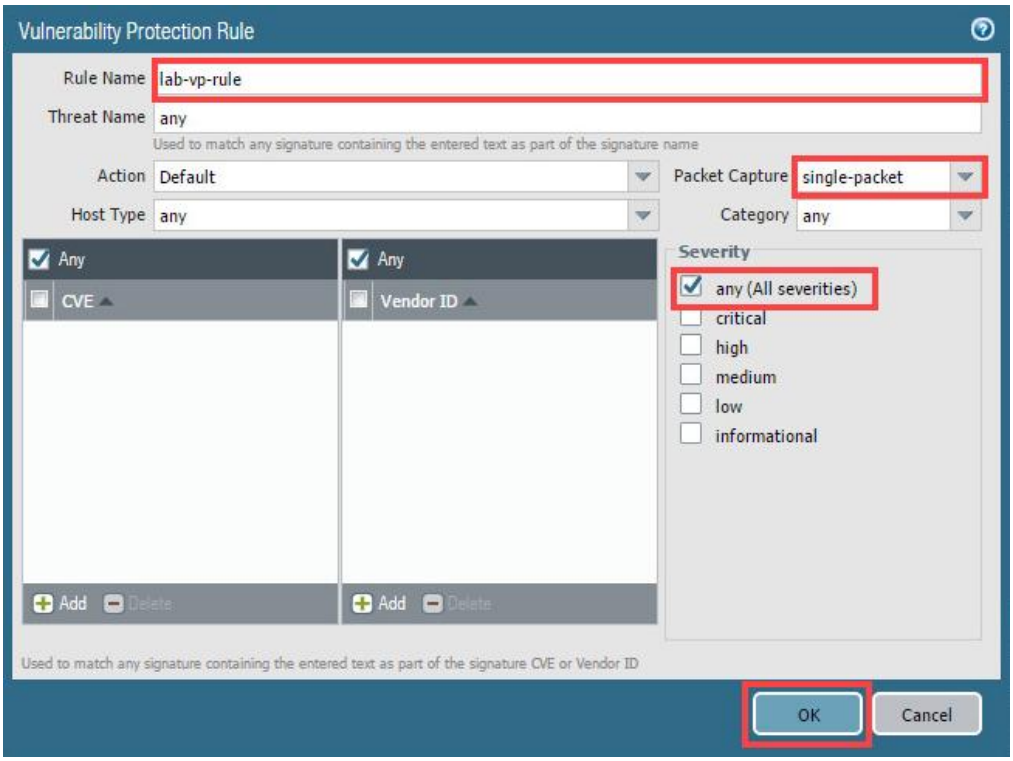
Parameter	Value
Name	**`lab-vp`**
Description	Type **`Vulnerability Protection profile for lab`**



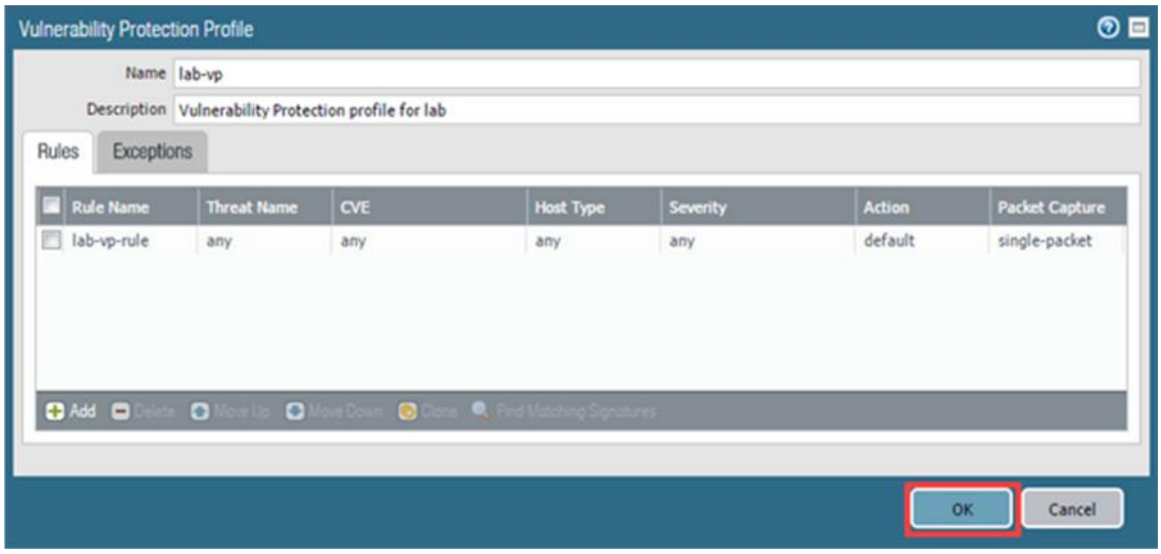
4. On the *Rules* tab, click **Add** to create a rule.

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

Parameter	Value
Name	`lab-vp-rule`
Packet Capture	Select **single-packet** from the drop-down 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**.

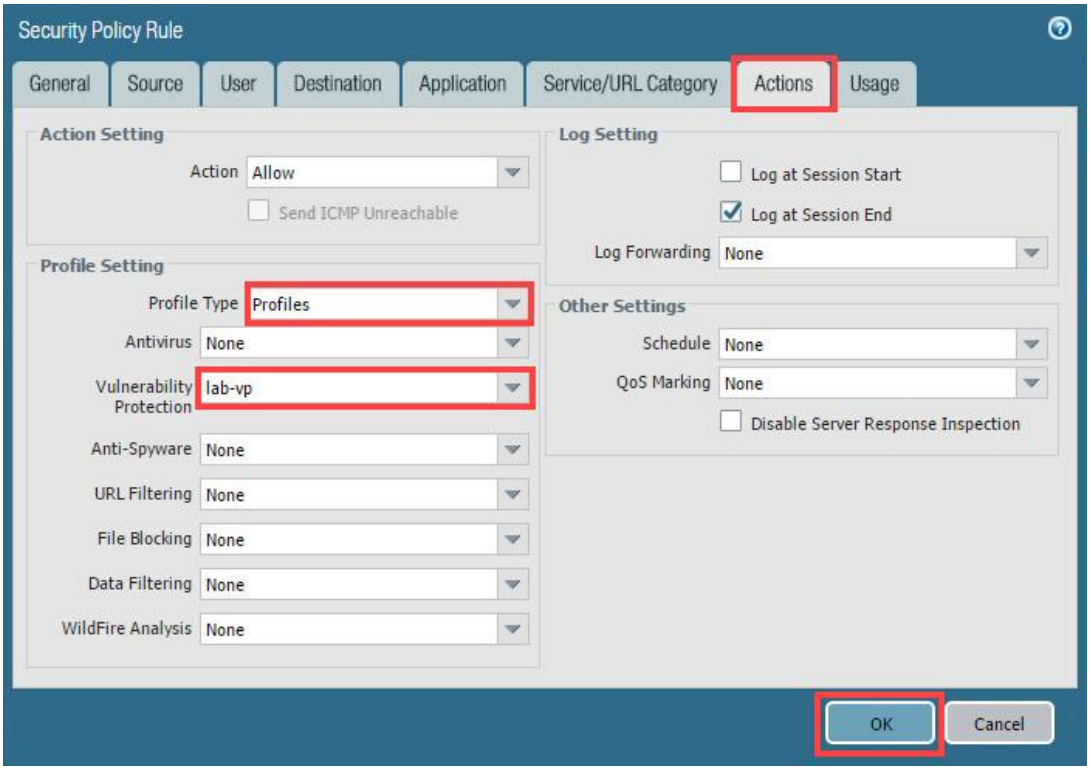


7. In the web interface, select **Policies > Security**.

8. Click on **internal-inside-dmz** to open the Security policy rule.

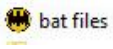
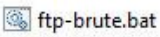
9. In the *Security Policy Rule* window, click the **Actions** tab and configure the following. When finished, click **OK**.

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



10. **Commit** all changes.

1.2 Test the Security Policy Rule

1. On the Windows desktop, double-click the **lab**  folder.
2. Within the *lab* folder, double-click the **bat files**  folder.
3. Double-click the **ftp-brute.bat**  file to launch the file.

4. Notice that this action launches an FTP brute force attack at the DMZ FTP server. After one minute, you can press **CTRL+C** to terminate the batch file because sufficient log data will have been collected. The entire script should take about 10 minutes to complete should you choose to wait for completion.

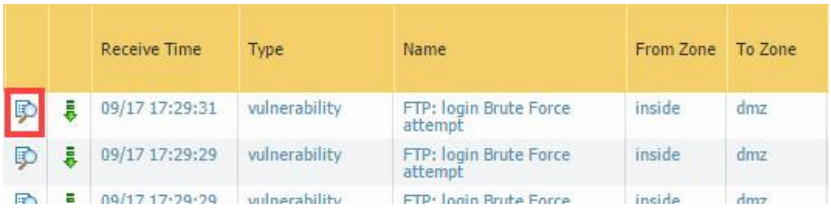
```
C:\Users\lab-user\Desktop\lab\bat files>nmap --script ftp-brute 192.168.50.10 -p
 21

Starting Nmap 7.31 ( https://nmap.org ) at 2019-09-17 17:19 Coordinated Universa
l Time
Nmap scan report for 192.168.50.10
Host is up (0.014s latency).
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 1245 guesses in 605 seconds, average tps: 2.0

Nmap done: 1 IP address (1 host up) scanned in 608.50 seconds

C:\Users\lab-user\Desktop\lab\bat files>pause
Press any key to continue . . .
```

5. After the script completes, press any key to close the command-prompt window.

1.3 Review the Logs

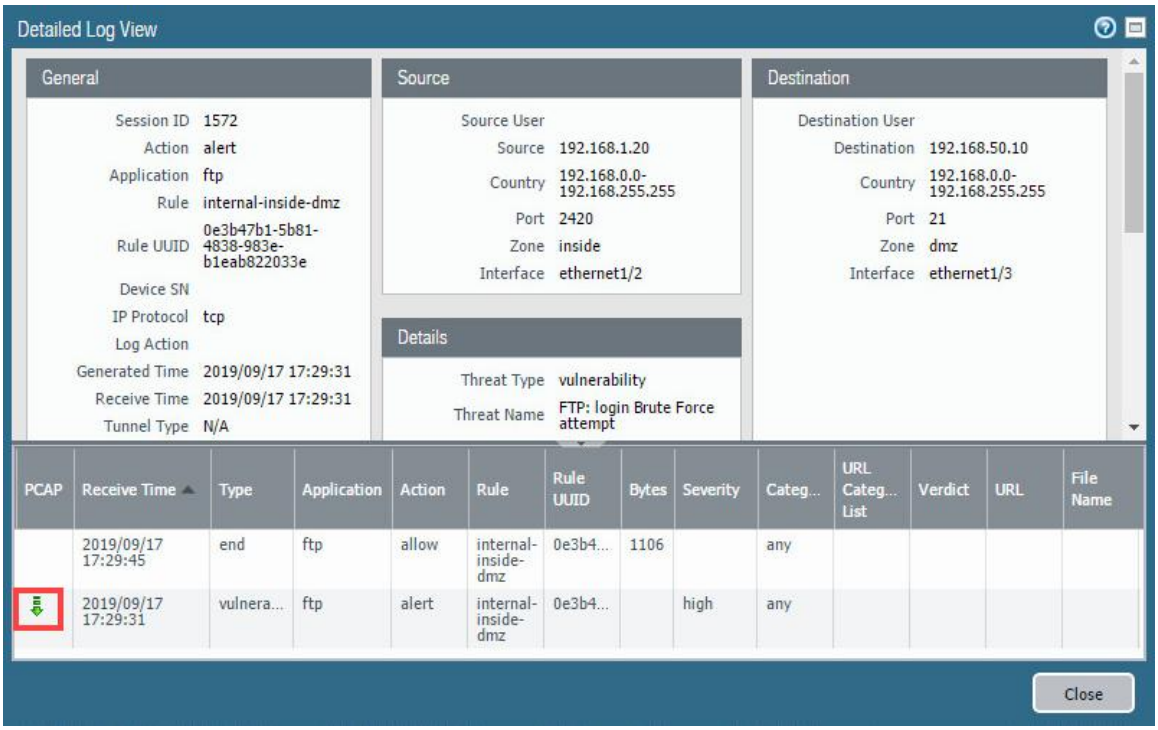
1. Change focus to the firewall web interface and select **Monitor > Logs > Threat**.

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.

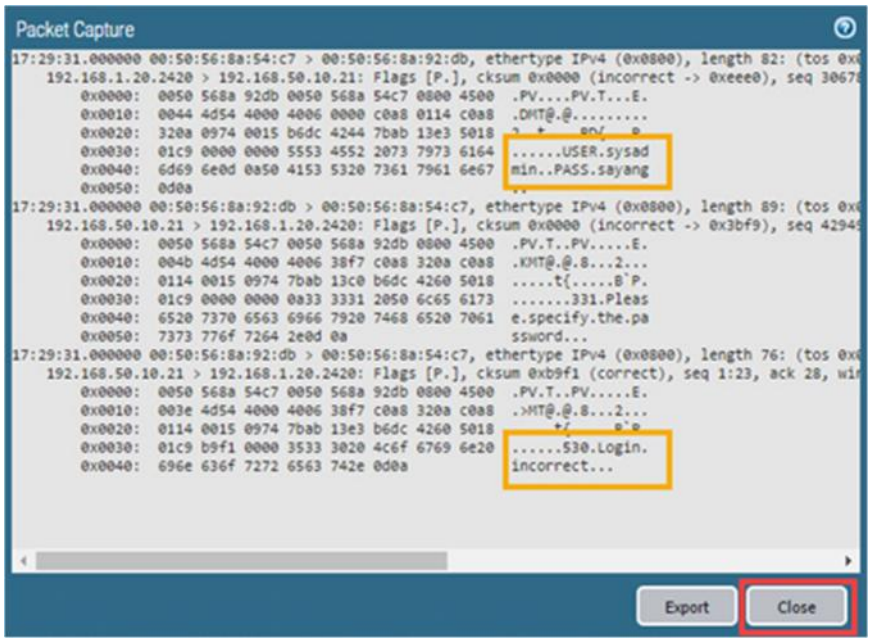


		Receive Time	Type	Name	From Zone	To Zone
		09/17 17:29:31	vulnerability	FTP: login Brute Force attempt	inside	dmz
		09/17 17:29:29	vulnerability	FTP: login Brute Force attempt	inside	dmz
		09/17 17:29:29	vulnerability	FTP: login Brute Force	inside	dmz

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**.

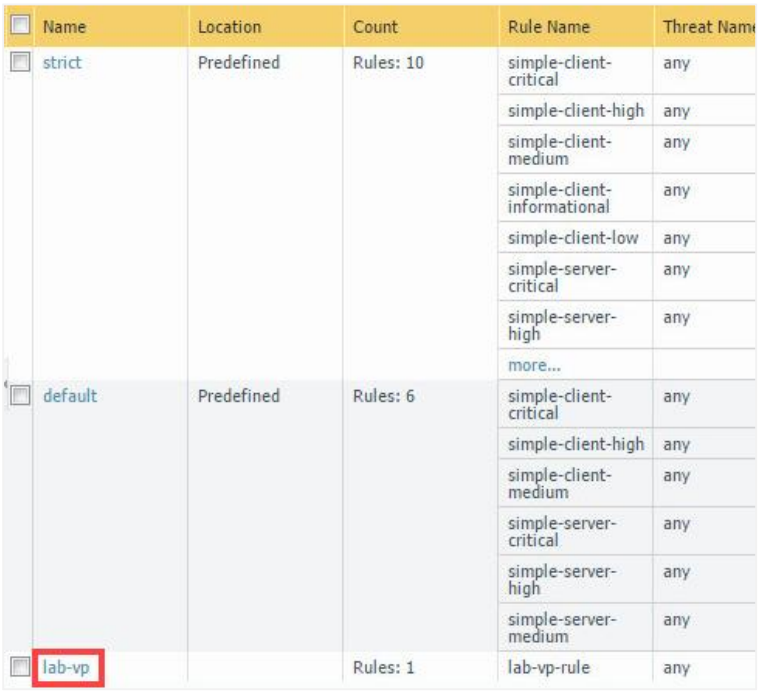


Captured packets can be exported in pcap format and examined with an offline analyzer for further investigation.

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

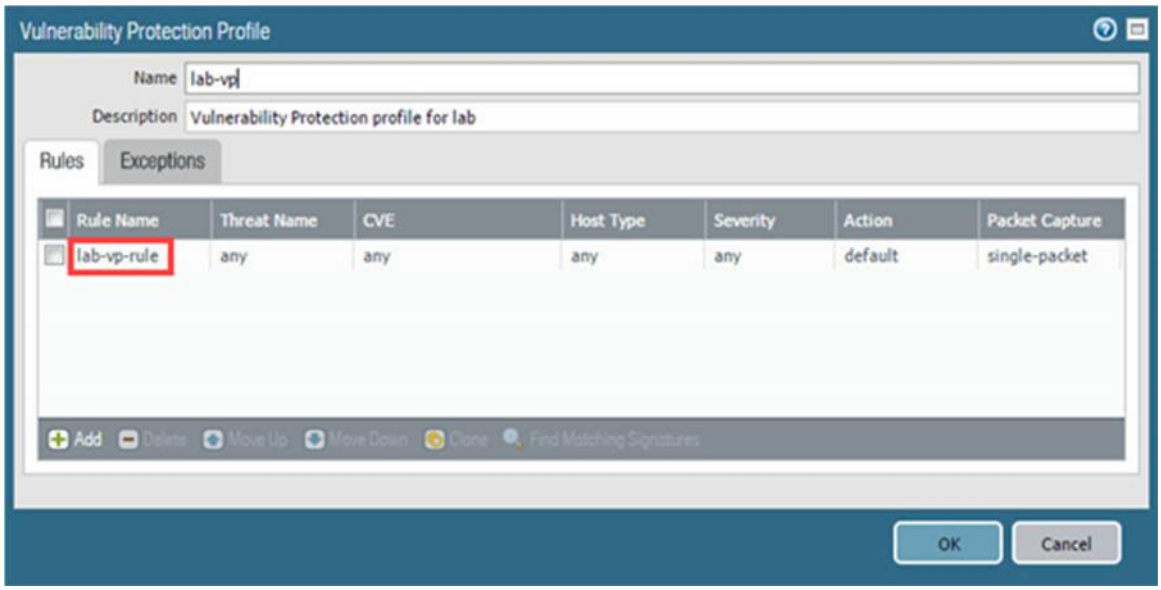
1.4 Update the Vulnerability Profile

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



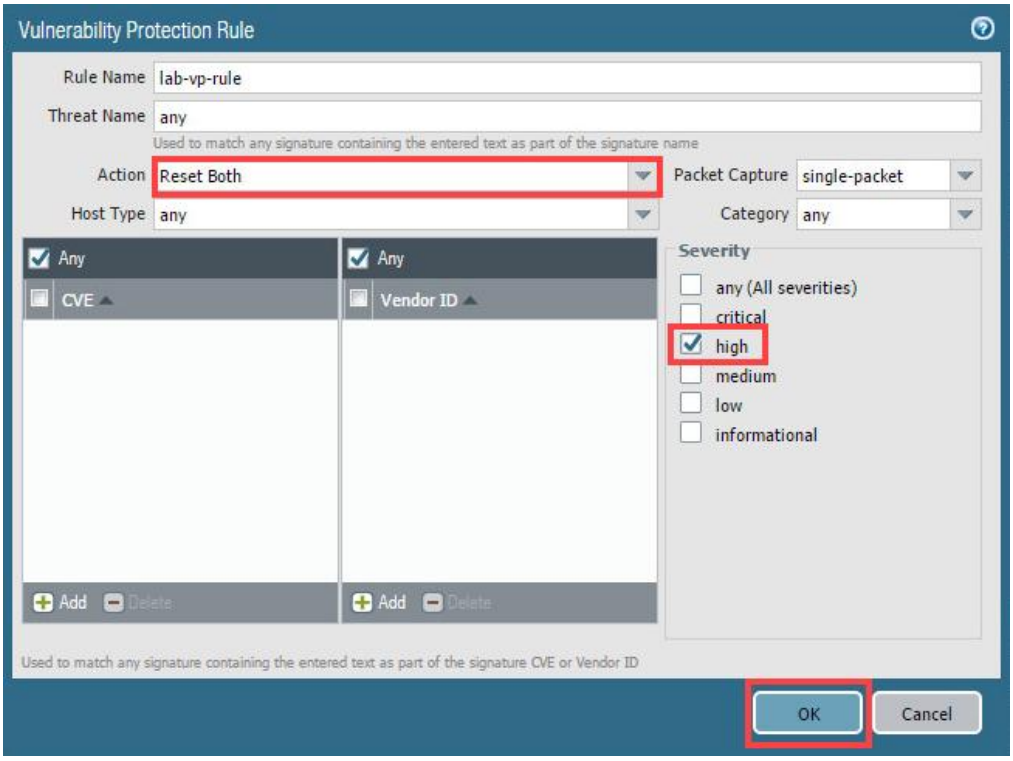
Name	Location	Count	Rule Name	Threat Name
strict	Predefined	Rules: 10	simple-client-critical	any
			simple-client-high	any
			simple-client-medium	any
			simple-client-informational	any
			simple-client-low	any
			simple-server-critical	any
			simple-server-high	any
			more...	
default	Predefined	Rules: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

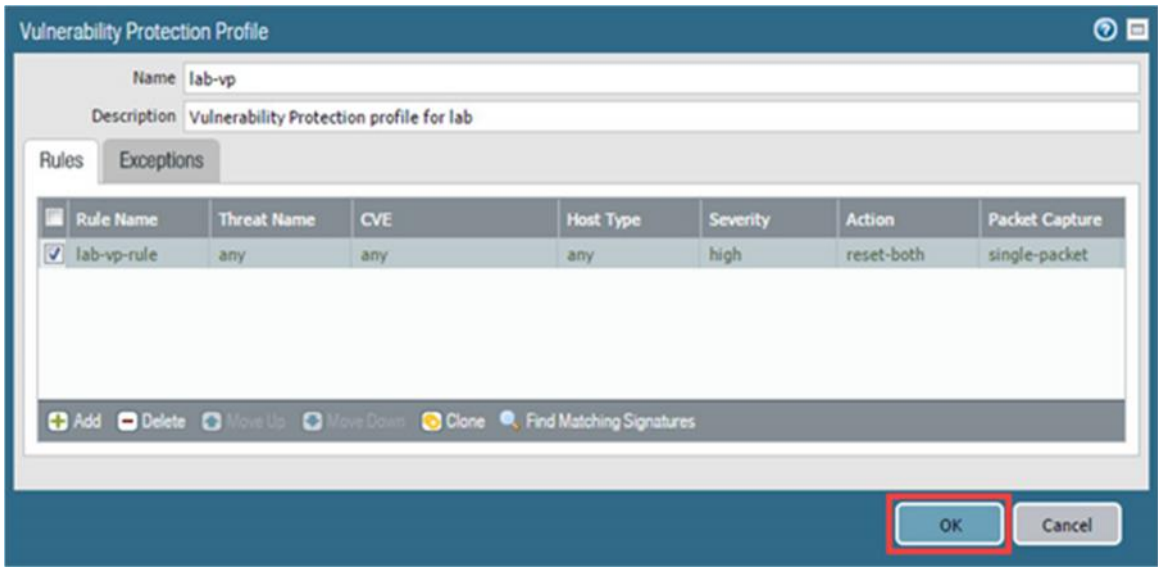


4. In the *Vulnerability Protection Rule* window, configure the following. Once finished, click **OK**.

Parameter	Value
Action	Select the **Reset Both** option from the drop-down 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 **ftp-brute.bat** 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.

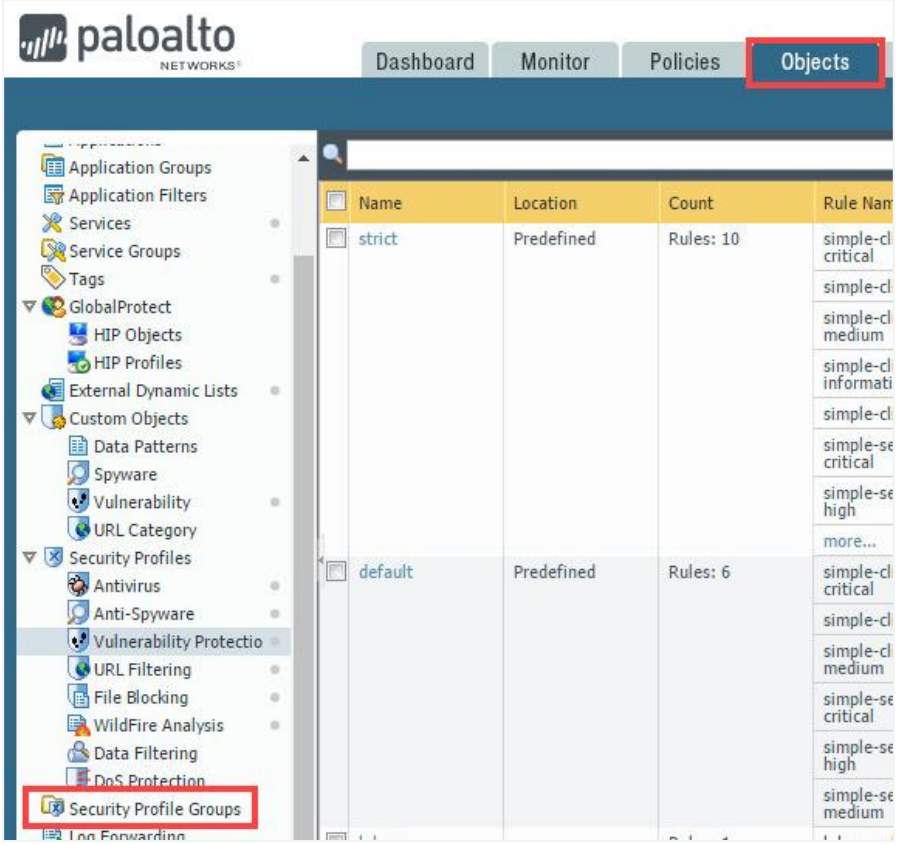
		Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	App...	Action
		09/17 18:26:51	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	reset-both
		09/17 18:26:51	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	reset-both
		09/17 18:26:51	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	reset-both
		09/17 18:26:51	vulnerability	FTP: login Brute Force	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	reset-both

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

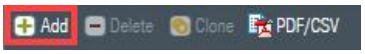
1.5 Create a Security Profile Group

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**.

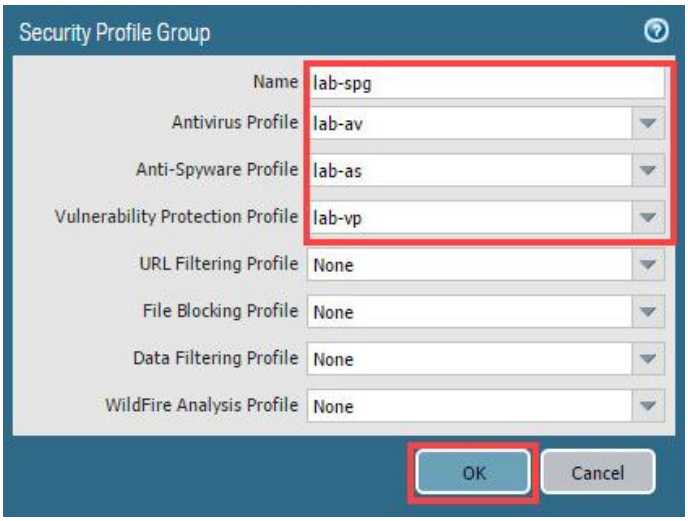


2. Click **Add** to create a *Security Profile Group*.

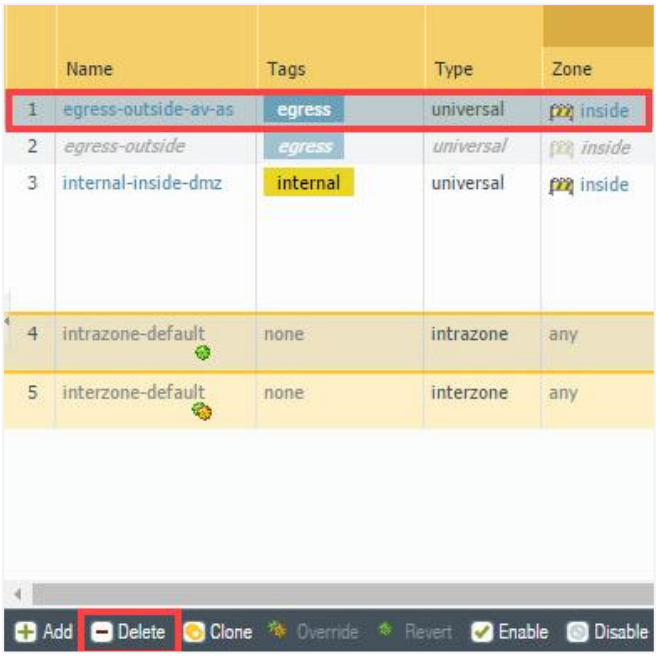


3. In the *Security Profile Group* window, configure the following. Once finished, click **OK**.

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

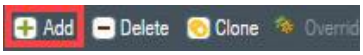


4. In the web interface, select **Policies > Security**.
5. Select the **egress-outside-av-as** rule and click **Delete**.



6. When prompted, click **Yes** to continue with the deletion.

7. Click **Add** to define a new *Security Policy Rule*.

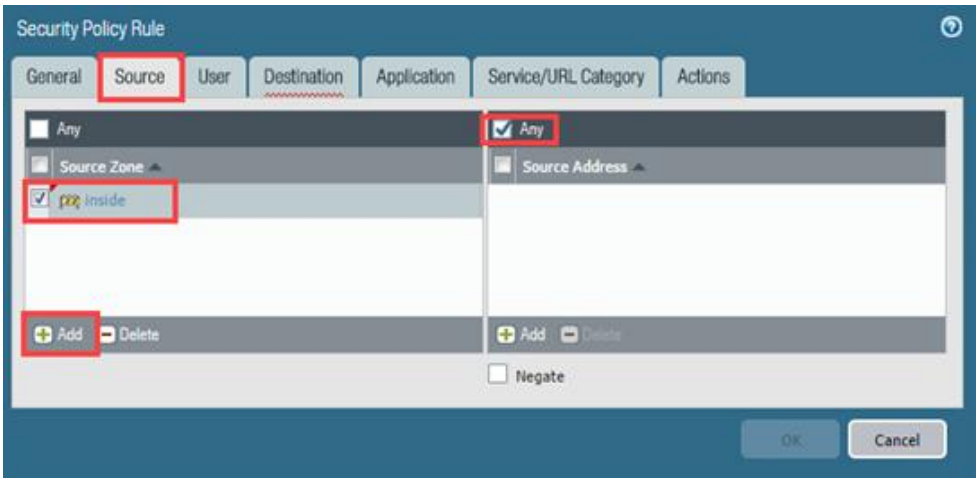


8. In the *Security Policy Rule* window, while on the *General* tab, configure the following.

Parameter	Value
Name	Type **`egress-outside-content-id`**
Rule Type	Verify that **universal (default)** is selected
Tags	Select **egress** from the drop-down list
Group Rules By Tag	Select **egress** from the drop-down list
Audit Comment	Type **`Created Security policy rule for Security Profile Group on <date> by admin`**.

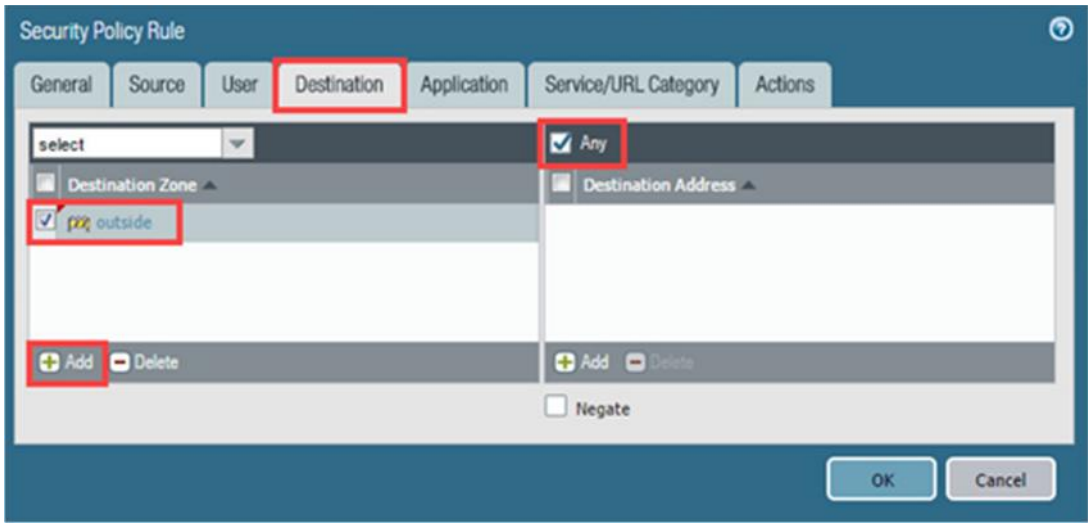
9. In the *Security Policy Rule* window, click the **Source** tab to configure the following.

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

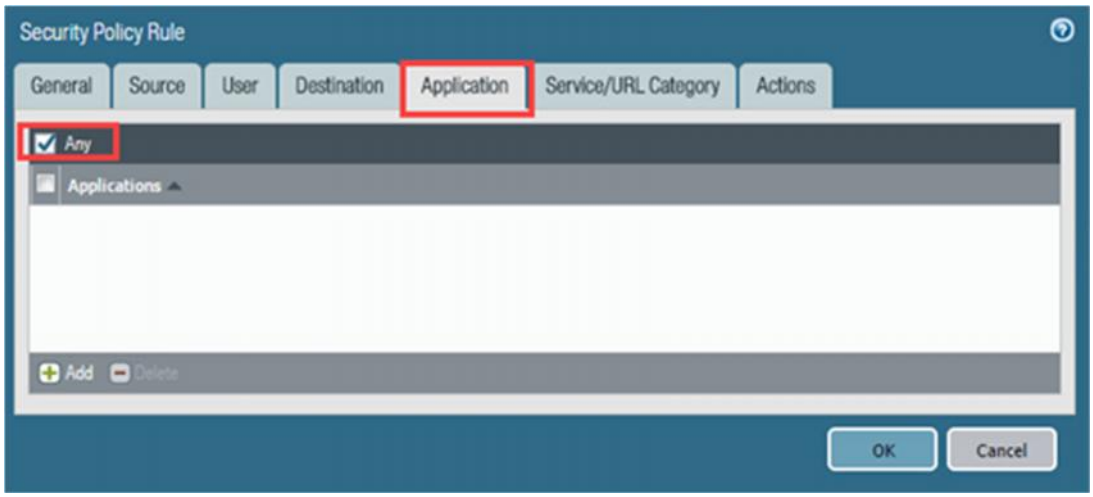


10. In the *Security Policy Rule* window, click the **Destination** tab and configure the following.

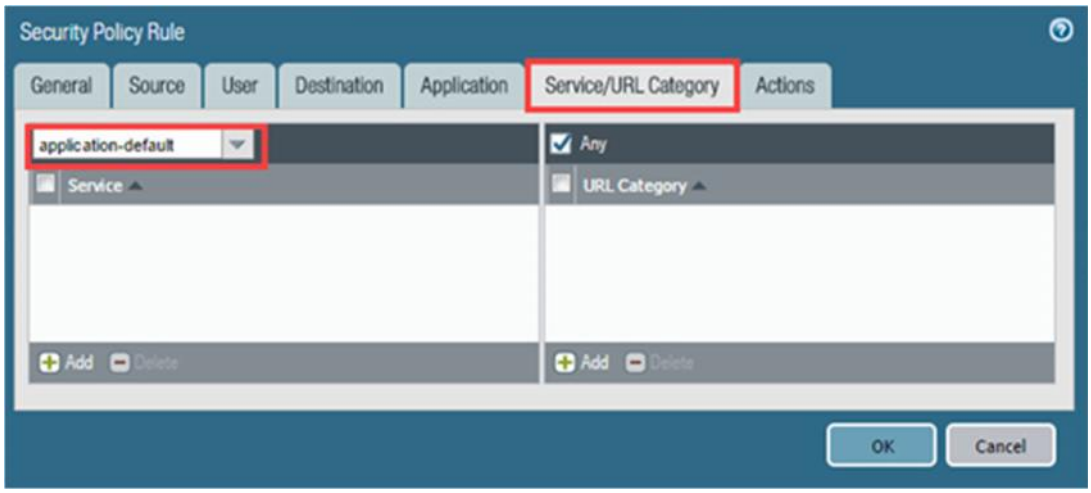
Parameter	Value
Destination Zone	Click **Add** and select **outside** from the drop-down list
Destination Address	Verify that the **Any** checkbox is selected



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

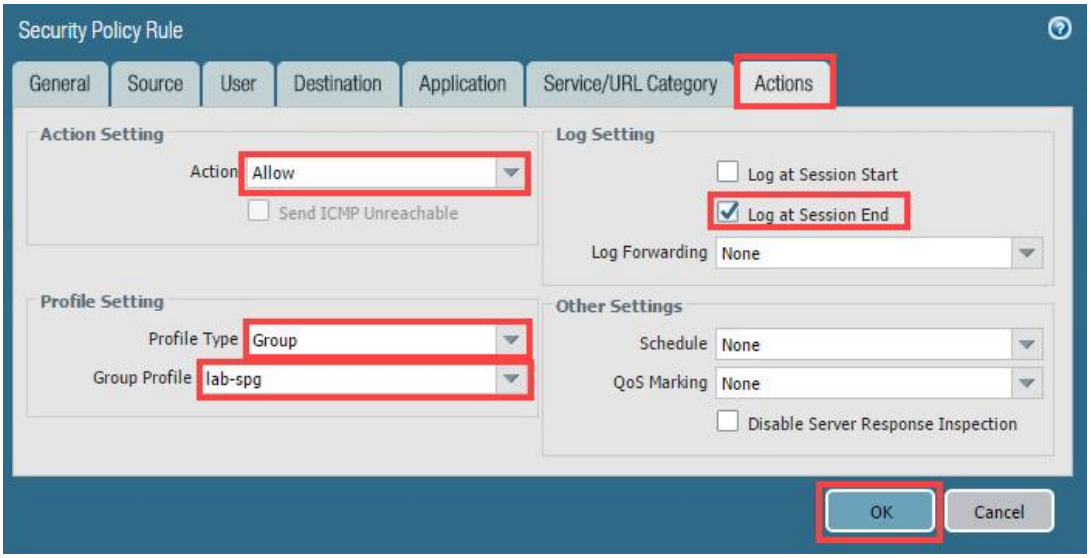


12. In the *Security Policy Rule* window, click the **Service/URL Category** tab and verify that **application-default** is selected.

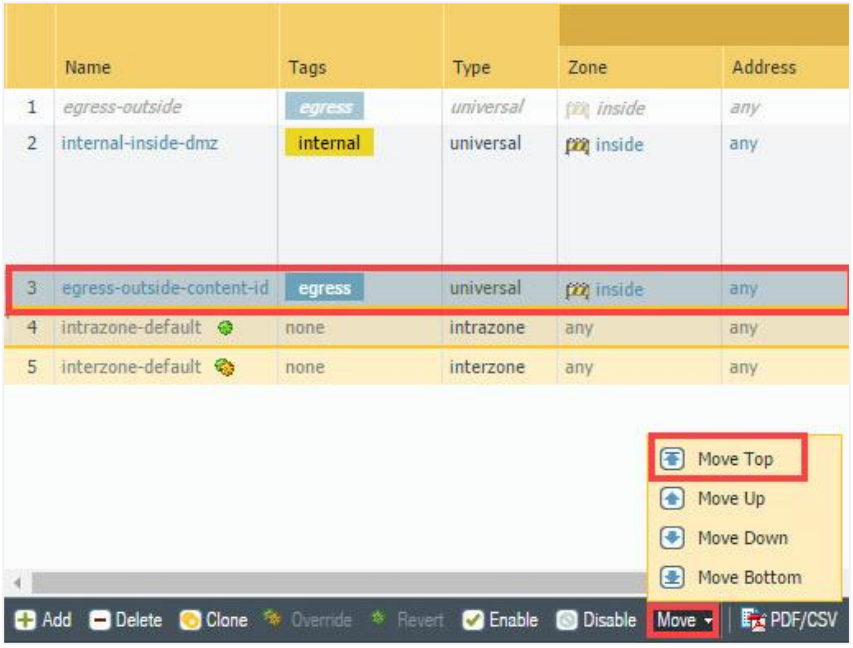


13. In the *Security Policy Rule* window, click the **Actions** tab and configure the following. Once finished, click **OK**.

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 drop-down list
Group Profile	Select **lab-spg** from the drop-down 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**.

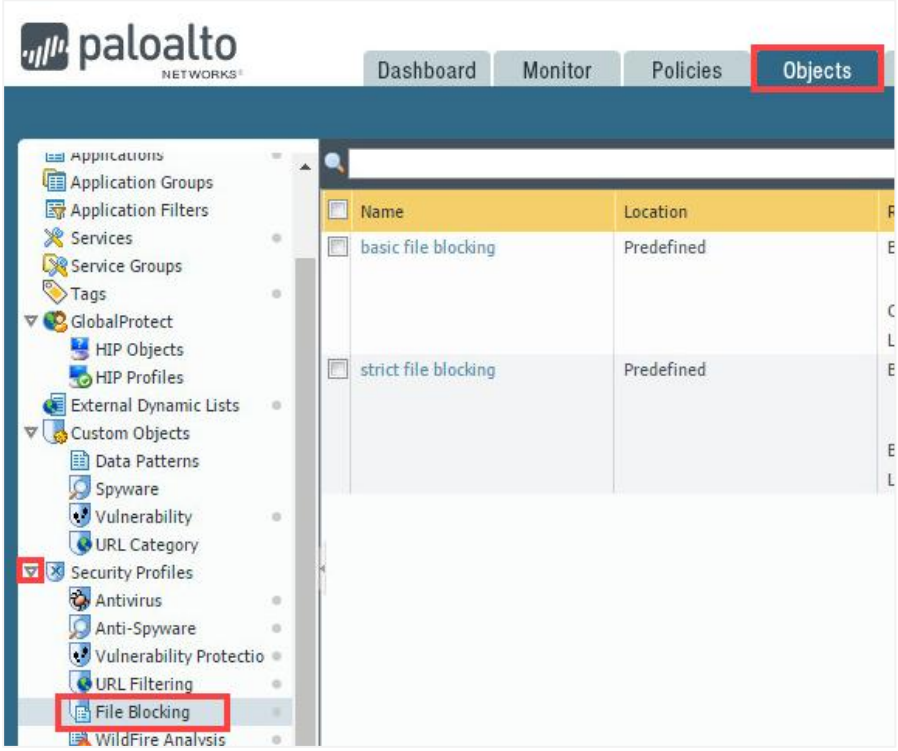


15. Leave the firewall web interface open to continue with the next task.

1.6 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.

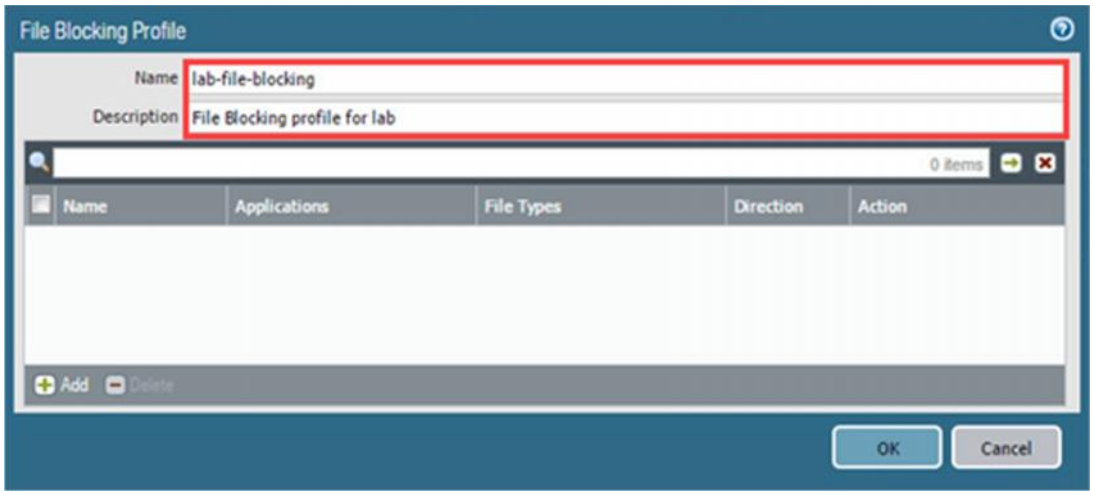
1. In the web interface, select **Objects > Security Profiles > File Blocking**.



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`**

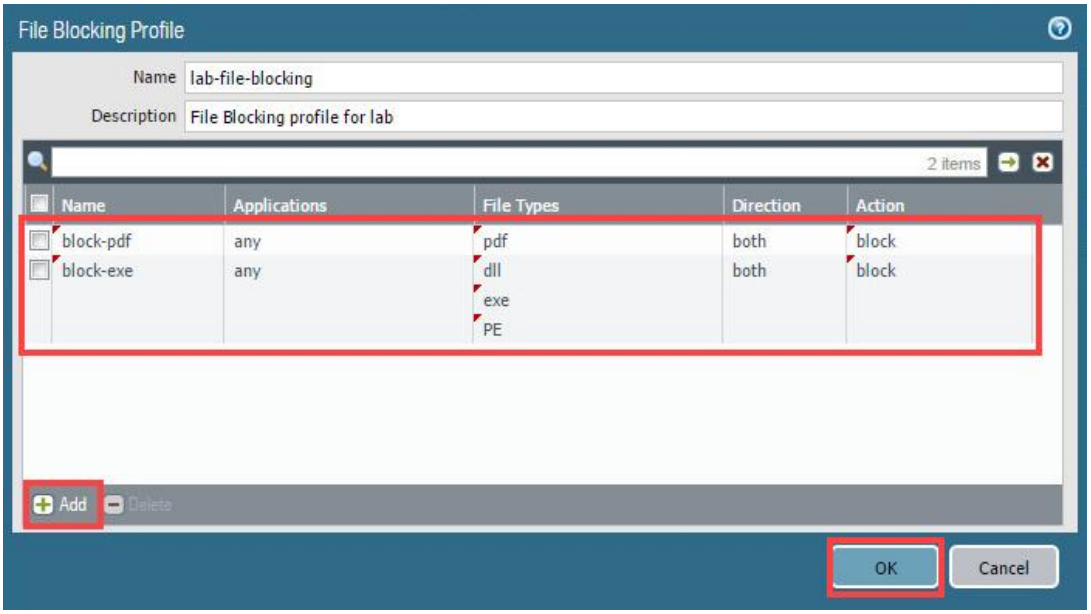


4. In the *File Blocking Profile* window, click **Add** and configure the following.

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

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

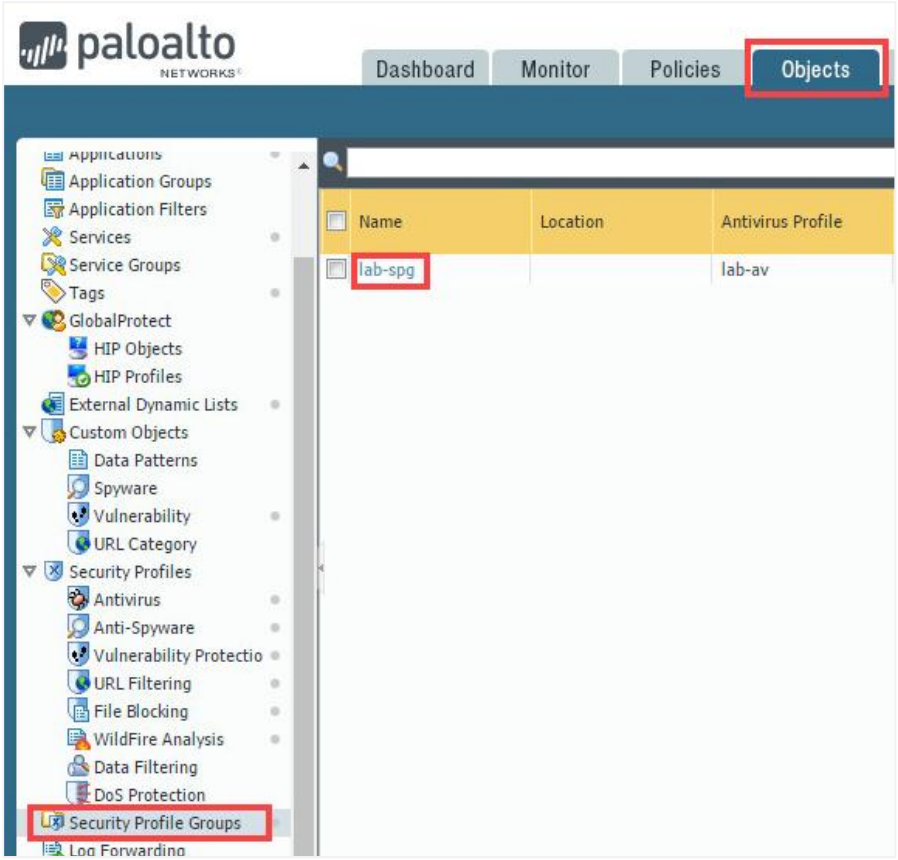
Parameter	Value
Name	Type `block-exe`
Applications	Verify that **any** is selected
File Types	Click **Add** and select the following from the drop-down list: **dll** **exe** **PE**
Direction	Verify that **both** is selected
Action	Select **block** from the drop-down list



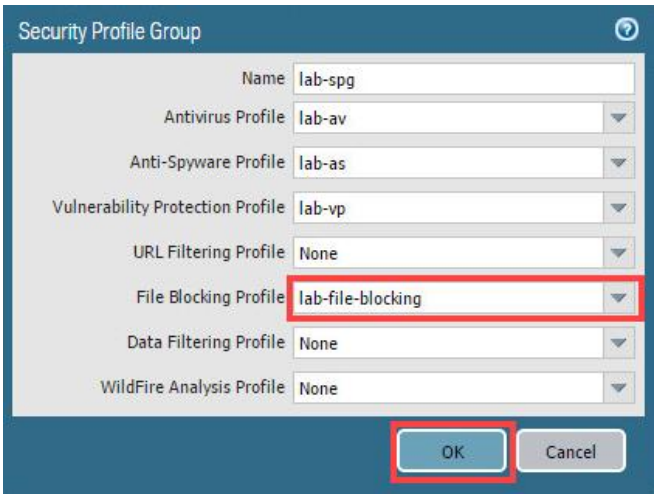
6. Verify that the new profile appears in the list. Leave the firewall web interface open to continue with the next task.

1.7 Modify a Security Profile Group

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



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



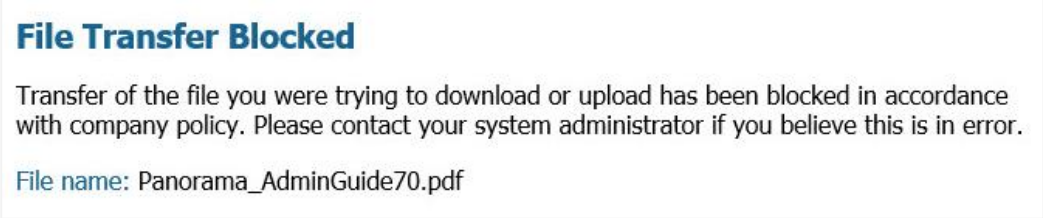
3. **Commit** all changes.

1.8 Test the File Blocking Profile

1. Open a new **Internet Explorer** browser window in **private/incognito** mode 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 **Internet Explorer** window.



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	Name	From Zone	To Zone	Source address	Destination address	Action
		09/17 19:33:36	any	Panorama_AdminGuide70.pdf	Adobe Portable Document Format (PDF)	inside	outside	192.168.1.20	67.195.197.75	deny

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

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

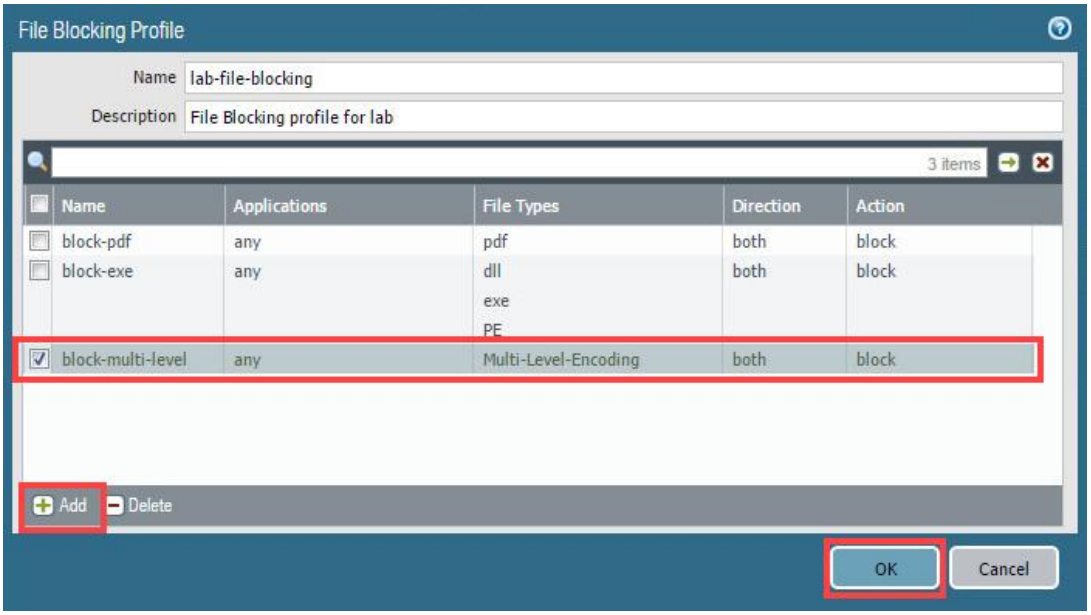
A file that is encoded five or more times cannot be inspected by the firewall. Multi-Level Encoding can be used to block this type of content.

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 drop-down list
Direction	Verify that **both** is selected
Action	Select **block** from the drop-down list

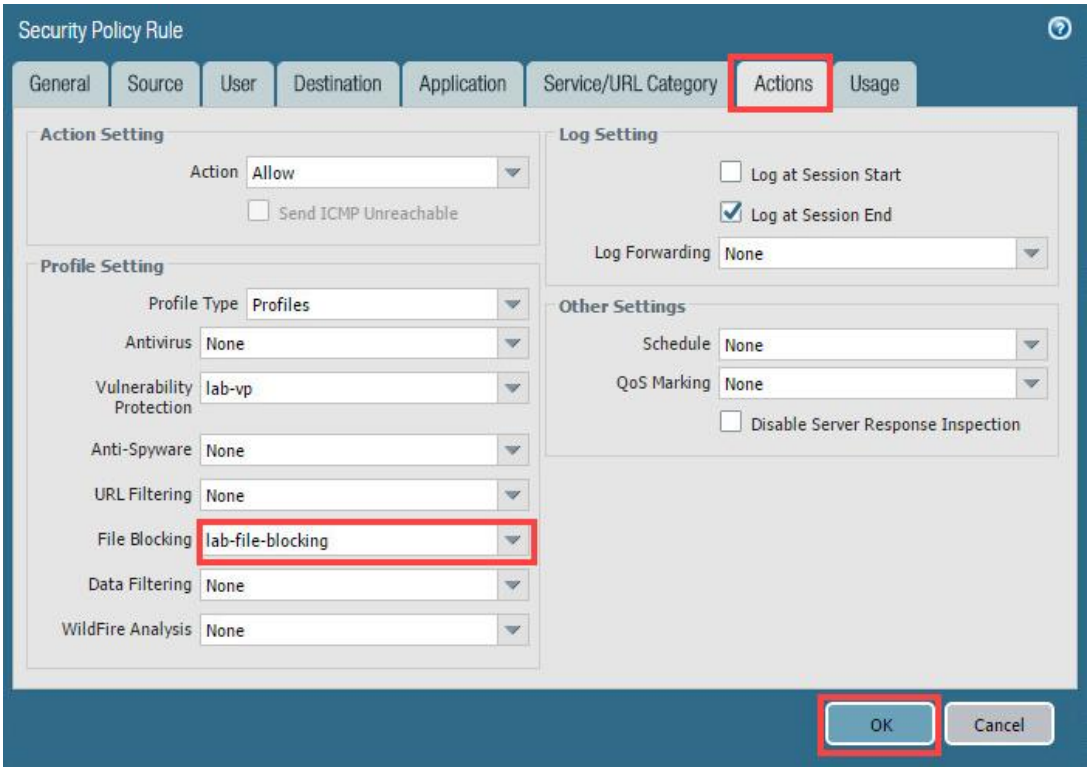


4. Leave the firewall web interface open to continue with the next task.

1.10 Modify the Security Policy Rule

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

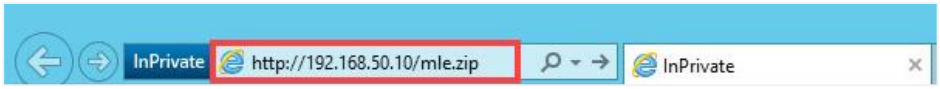
3. In the *Security Policy Rule* window, click the **Actions** tab and then select **lab-file-blocking** from the *File Blocking* drop-down list. Click **OK**.



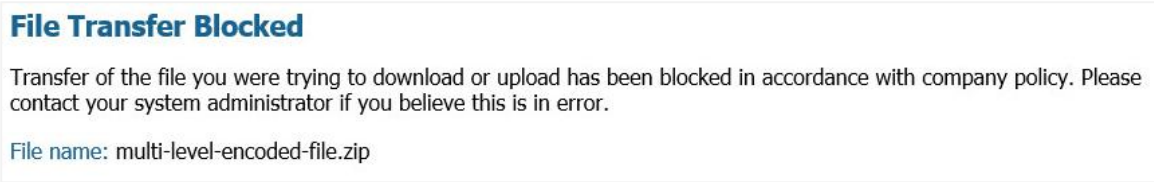
4. **Commit** all changes.

1.11 Test the File Blocking Profile with Multi-Level Encoding

1. Open the **Internet Explorer** browser in **private/incognito mode** and browse to **`http://192.168.50.10/mle.zip`**.

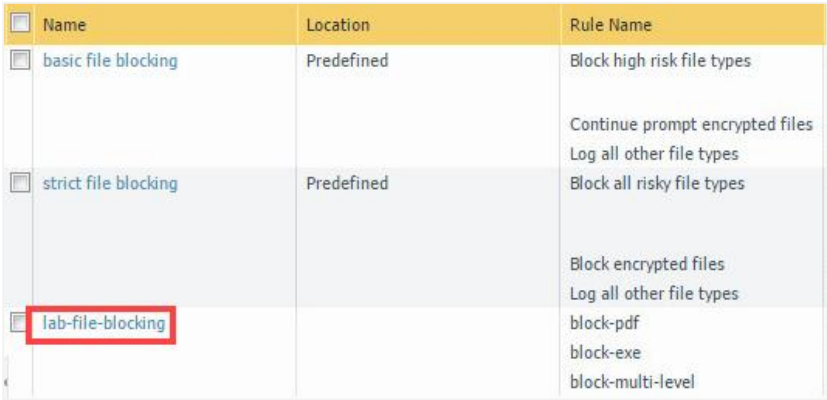


2. Notice that the file is blocked in accordance with the new file blocking rule. Close the browser window.

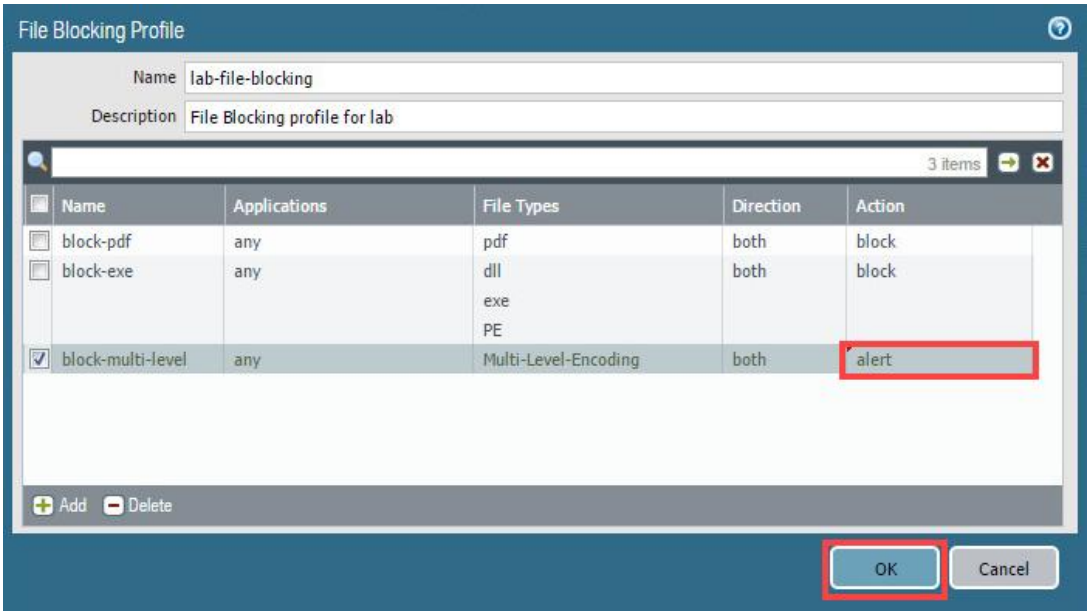


1.12 Modify the Security Policy Rule

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



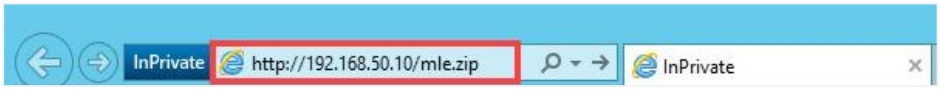
3. In the *File Blocking Profile* window, select the **block-multi-level** rule and change the *Action* to **alert**. Click **OK**.



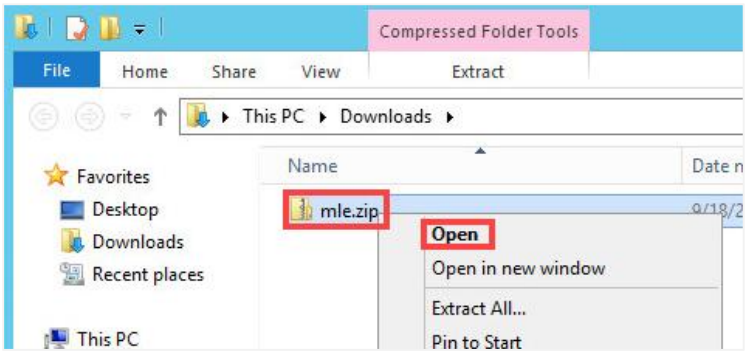
4. **Commit** all changes.

1.13 Test the File Blocking Profile with Multi-Level Encoding

1. Open the **Internet Explorer** browser in **private/incognito mode** and browse to **`http://192.168.50.10/mle.zip`**.



2. When prompted, save the file and open the file to examine the contents.



3. Notice the recursive structure of the zip archive. Close the file browser and IE browser.

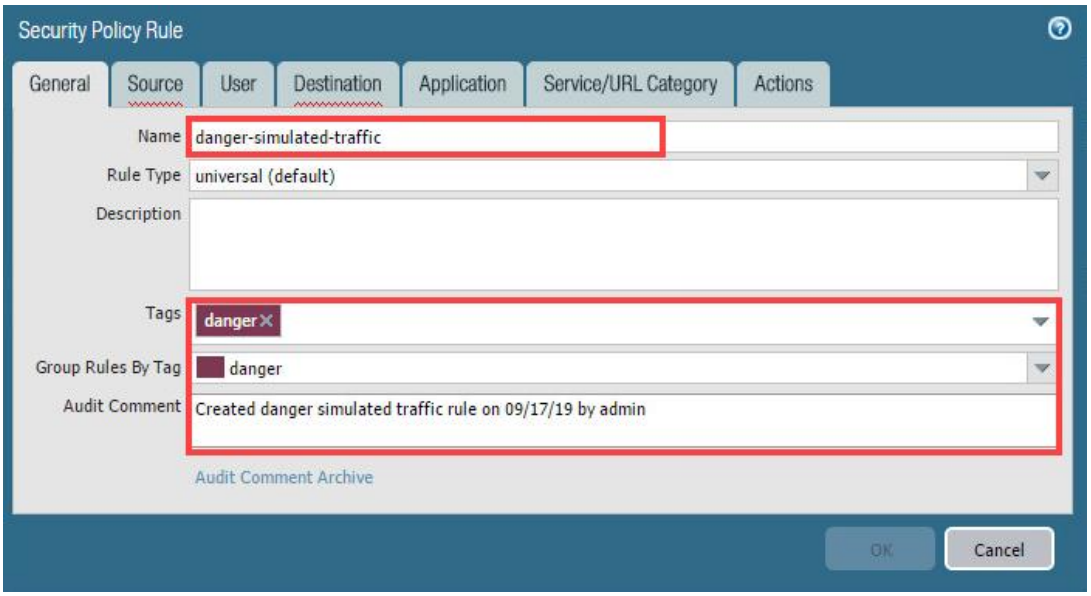
1.14 Create a Danger Security Policy Rule

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.

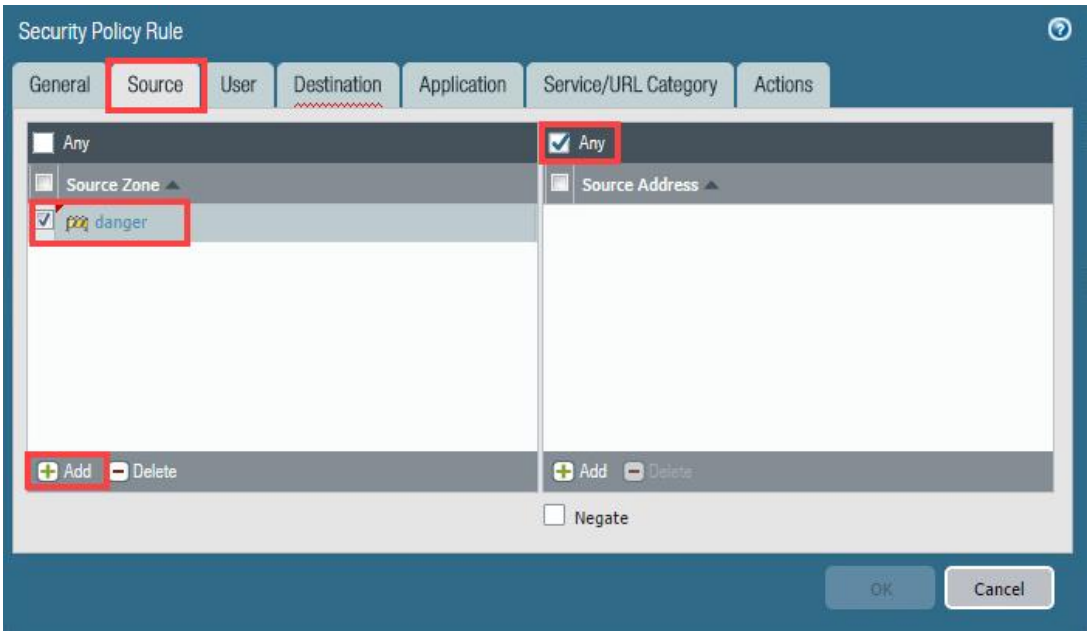
3. In the *Security Policy Rule* window, while on the *General* tab, configure the following.

Parameter	Value
Name	Type **`danger-simulated-traffic`**
Tags	Select **danger** from the drop-down list
Group Rules By Tag	Select **danger** from the drop-down list
Audit Comment	Type **`Created danger simulated traffic rule on <date> by admin`**



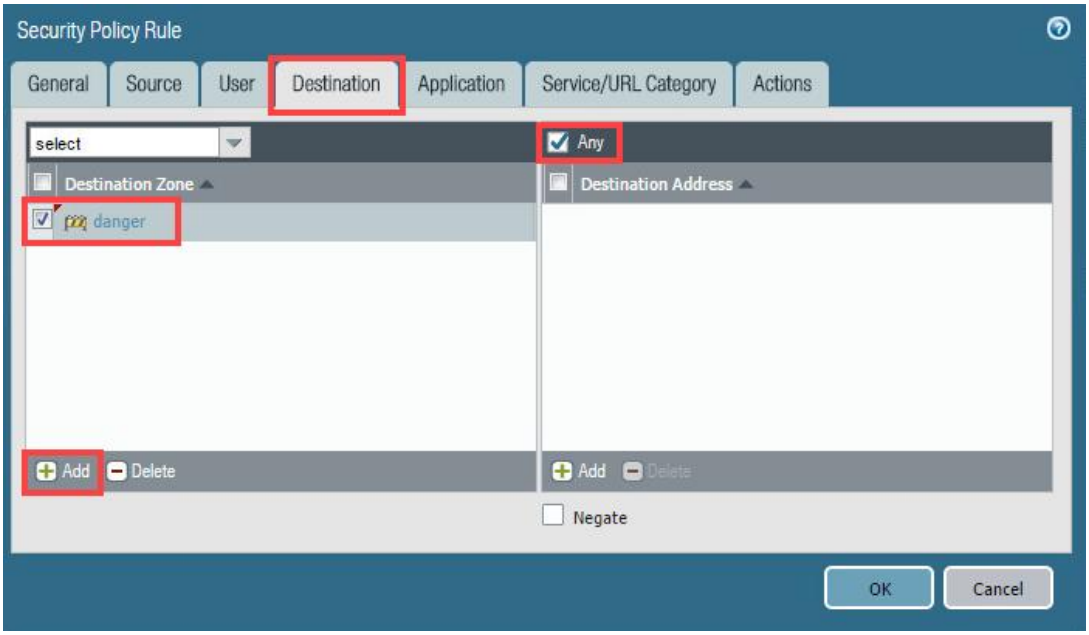
4. Click on the **Source** tab and configure the following.

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



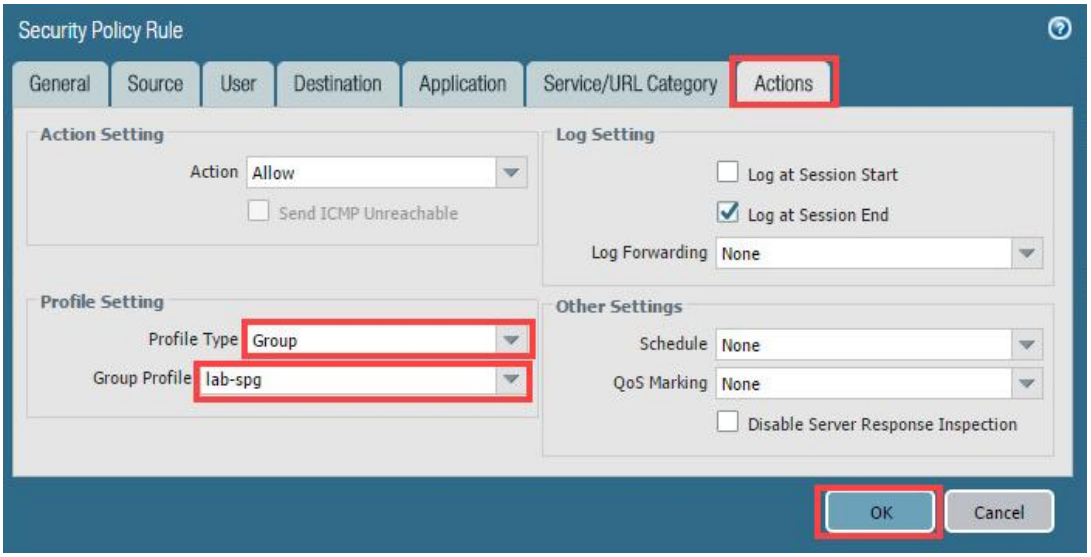
5. Click on the **Destination** tab and configure the following.

Parameter	Value
Destination Zone	Click **Add** and select **danger** from the drop-down 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 drop-down list
Group Profile	Select **lab-spg** from the drop-down list

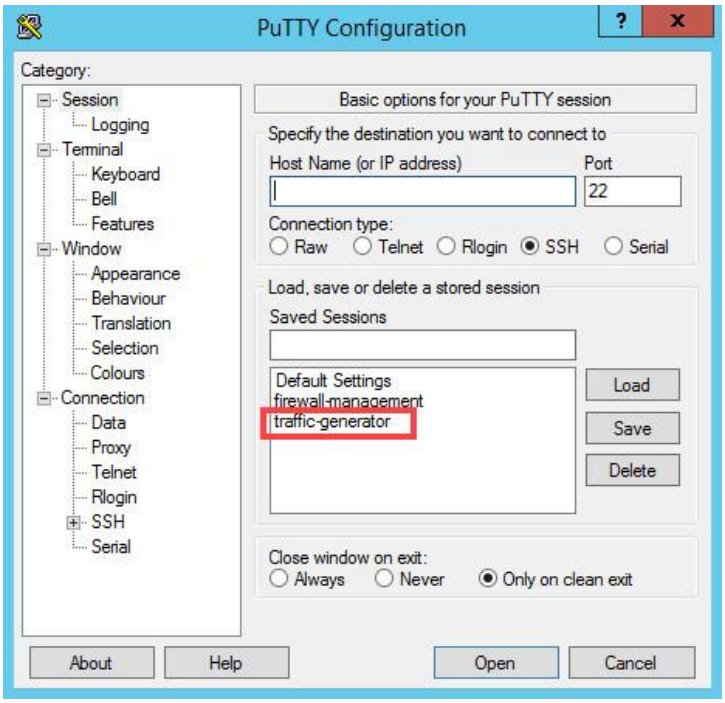


7. **Commit** all changes.

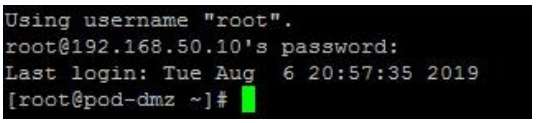
1.15 Generate Threats

1. On the Windows desktop, double-click the PuTTY 

icon.
2. In the *Saved Sessions* panes, double-click **traffic-generator**.



3. Notice a terminal appears. When prompted for a password, type **`Pal0Alt0`** followed by pressing the **Enter** key.



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

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

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


   THIS COULD TAKE UP TO 10 MINUTES

      Actual: 822 packets (735581 bytes) sent in 134.02 seconds.
Rated: 5400.0 Bps, 0.043 Mbps, 6.12 pps
Flows: 27 flows, 0.20 fps, 822 flow packets, 0 non-flow
Statistics for network device: ens224
        Successful packets:        822
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Actual: 67 packets (47535 bytes) sent in 17.04 seconds.
Rated: 2700.0 Bps, 0.021 Mbps, 3.84 pps
Flows: 6 flows, 0.34 fps, 67 flow packets, 0 non-flow
Statistics for network device: ens224
        Successful packets:        67
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Actual: 372 packets (264661 bytes) sent in 0.262919 seconds.
Rated: 1006600.0 Bps, 8.05 Mbps, 1414.88 pps
Flows: 2 flows, 7.60 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 0.118661 seconds.
Rated: 98300.0 Bps, 0.786 Mbps, 370.80 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	Destination address	To Port	Application	Action	Severity
		09/18 19:13:54	vulnerability	Trojan-Win32.swrort.dfap	danger	danger	10.10.10.10	192.168.1.121	25	smtp	reset-both	high
		09/18 19:13:54	vulnerability	Ransom-Win32.locky.pe	danger	danger	10.10.10.10	192.168.1.121	25	smtp	reset-both	high
		09/18 19:13:43	spyware	Bredolab.Gen Command and Control Traffic	danger	danger	192.168.0.2	112.137.162.134	80	web-browsing	alert	critical
		09/18 19:09:08	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20	172.217.5.238	443	google-base	alert	informational

8. In the web interface, navigate to **Monitor > Logs > Data Filtering**.
9. Notice the blocked files.

		Receive Time	Category	File Name	Name	From Zone	To Zone	Source address
		09/18 19:14:00	any	CV.Cindy.Nero.pdf	Adobe Portable Document Format (PDF)	danger	danger	10.10.10.10
		09/18 19:13:59	any	locky.exe	Windows Executable (EXE)	danger	danger	10.10.10.10
		09/18 19:13:59	any	locky.exe	Microsoft PE File	danger	danger	10.10.10.10
		09/18 19:11:33	any	onus.dll	Microsoft PE File	danger	danger	192.168.204.134
		09/18 19:08:29	any	multi-level-enco...	Multi-Level Encoding	inside	dmz	192.168.1.20

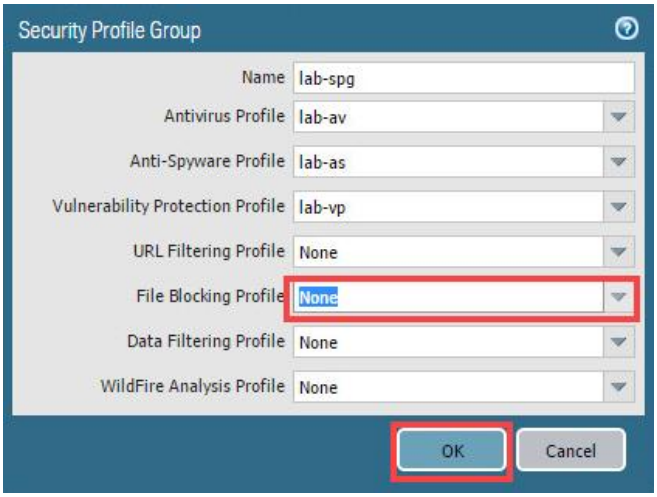
10. Leave the firewall web interface open to continue with the next task.

1.16 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 drop-down list and click **OK**.



4. **Commit** all changes.

1.17 Modify the Security Policy Rule

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
```

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


   THIS COULD TAKE UP TO 10 MINUTES

      Actual: 822 packets (735581 bytes) sent in 134.02 seconds.
Rated: 5400.0 Bps, 0.043 Mbps, 6.12 pps
Flows: 27 flows, 0.20 fps, 822 flow packets, 0 non-flow
Statistics for network device: ens224
        Successful packets:        822
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Actual: 67 packets (47535 bytes) sent in 17.04 seconds.
Rated: 2700.0 Bps, 0.021 Mbps, 3.84 pps
Flows: 6 flows, 0.34 fps, 67 flow packets, 0 non-flow
Statistics for network device: ens224
        Successful packets:        67
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Actual: 372 packets (264661 bytes) sent in 0.215220 seconds.
Rated: 1229700.0 Bps, 9.83 Mbps, 1728.46 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 0.118154 seconds.
Rated: 98700.0 Bps, 0.789 Mbps, 372.39 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	Destination address	To Port	Application	Action	Severity
		09/18 19:24:29	vulnerability	Trojan-Win32.swrort.dfap	danger	danger	10.10.10.10	192.168.1.121	25	smtp	reset-both	high
		09/18 19:24:29	vulnerability	Ransom-Win32.locky.pe	danger	danger	10.10.10.10	192.168.1.121	25	smtp	reset-both	high
		09/18 19:24:18	spyware	Bredolab.Gen Command and Control Traffic	danger	danger	192.168.0.2	112.137.162.134	80	web-browsing	alert	critical
		09/18 19:13:54	vulnerability	Trojan-Win32.swrort.dfap	danger	danger	10.10.10.10	192.168.1.121	25	smtp	reset-both	high
		09/18 19:13:54	vulnerability	Ransom-Win32.locky.pe	danger	danger	10.10.10.10	192.168.1.121	25	smtp	reset-both	high
		09/18 19:13:43	spyware	Bredolab.Gen Command and Control Traffic	danger	danger	192.168.0.2	112.137.162.134	80	web-browsing	alert	critical
		09/18 19:09:08	spyware	Suspicious TLS Evasion	inside	outside	192.168.1.20	172.217.5.238	443	google-base	alert	informational

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.

