



PALO ALTO NETWORKS EDU-210



Lab 5B: Content-ID

Document Version: 2019-11-12

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Theoretical Lab Topology.....	4
Lab Settings	5
1 Content-ID.....	6
1.0 Load Lab Configuration	6
1.1 Create Security Policy Rule with a Vulnerability Protection Profile.....	8
1.2 Test the Security Policy Rule	12
1.3 Review the Logs.....	13
1.4 Update the Vulnerability Profile	15
1.5 Create a Security Profile Group.....	17
1.6 Create a File Blocking Profile.....	22
1.7 Modify a Security Profile Group	25
1.8 Test the File Blocking Profile	26
1.9 Create a File Blocking Profile to Block Multi-Level Encoded Files	27
1.10 Modify the Security Policy Rule	28
1.11 Test the File Blocking Profile with Multi-Level Encoding	29
1.12 Modify the Security Policy Rule	30
1.13 Test the File Blocking Profile with Multi-Level Encoding	30
1.14 Create a Danger Security Policy Rule	31
1.15 Generate Threats.....	34
1.16 Modify a Security Policy Group	36
1.17 Modify the Security Policy Rule	37

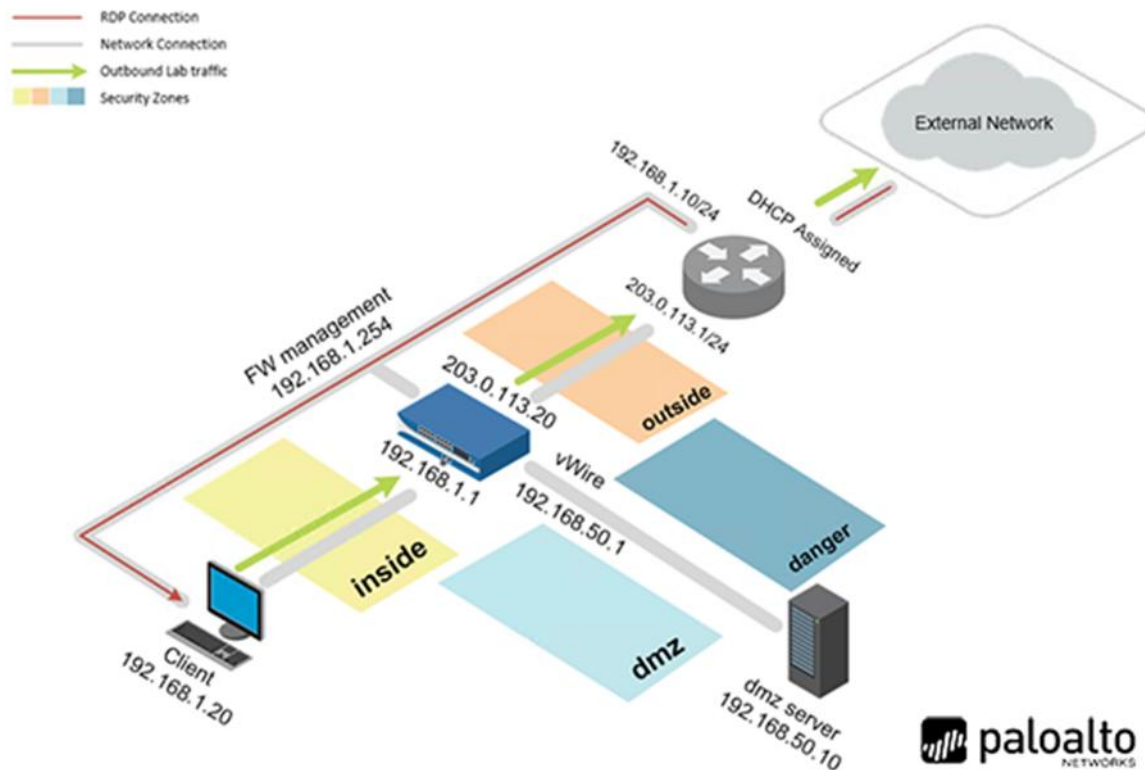
Introduction

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.

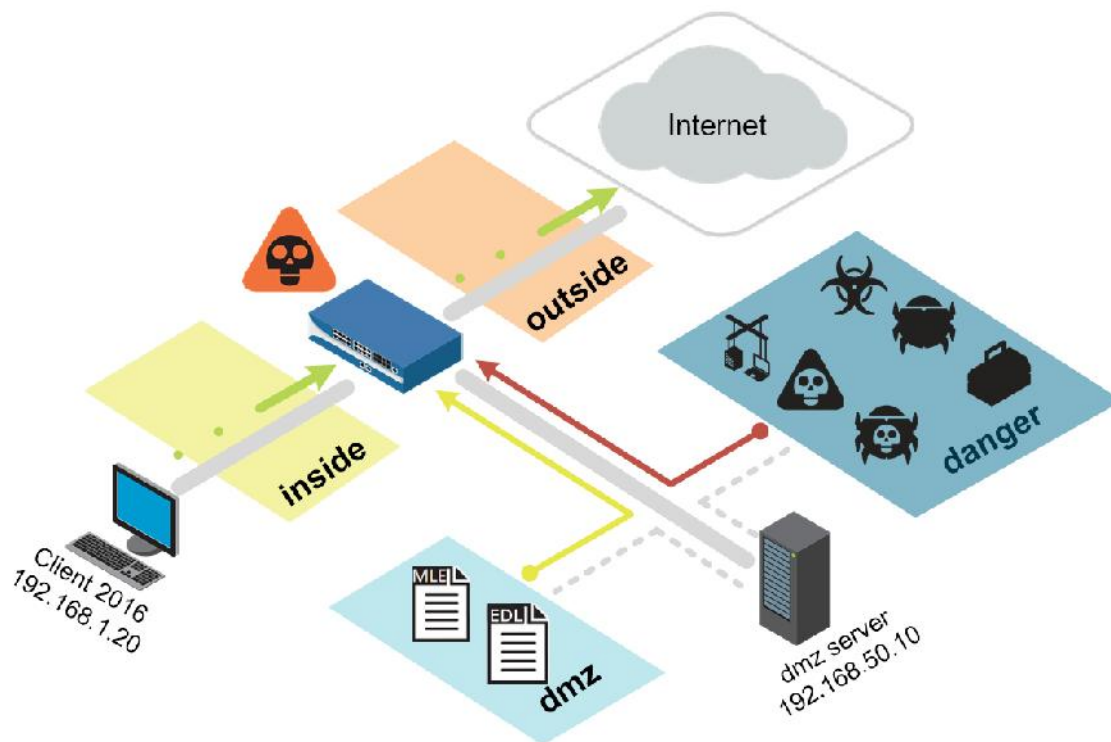
Objectives

-) 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	Pa10Alt0
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 **Pa10A1t0**.



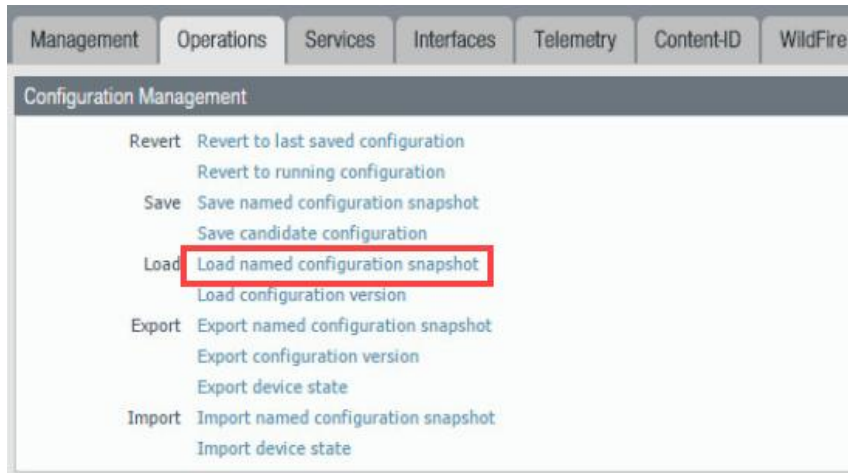
3. Launch the **Chrome** browser and connect to **https://192.168.1.254**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	admin
Password	admin

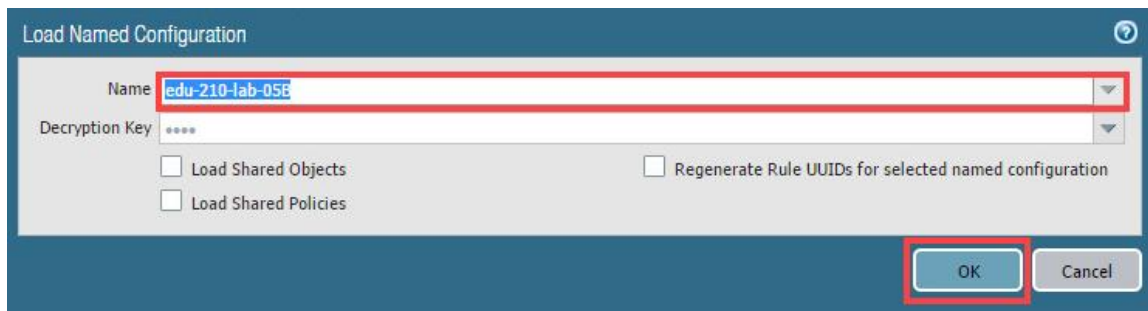
6. In the web interface, navigate to **Device > Setup > Operations**.



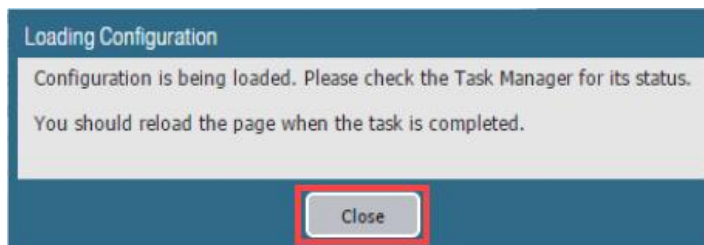
7. Click **Load named configuration snapshot**:



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



9. Click **Close**.

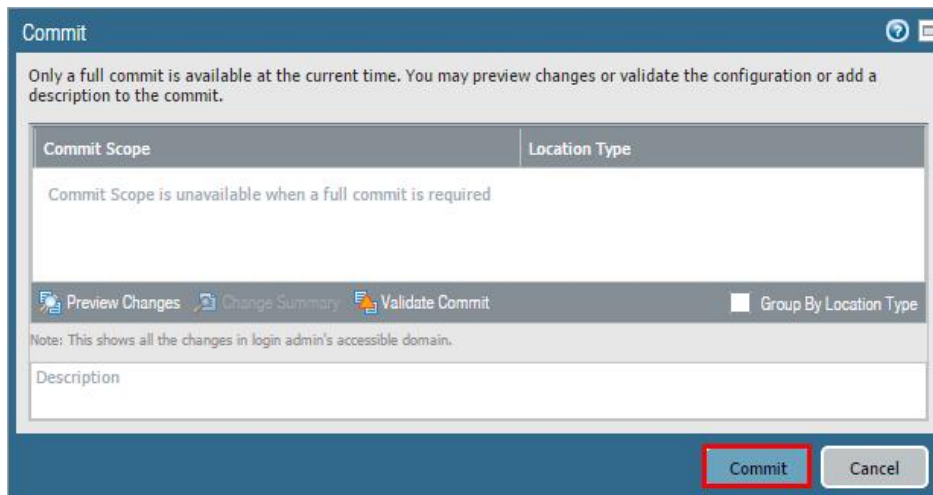


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

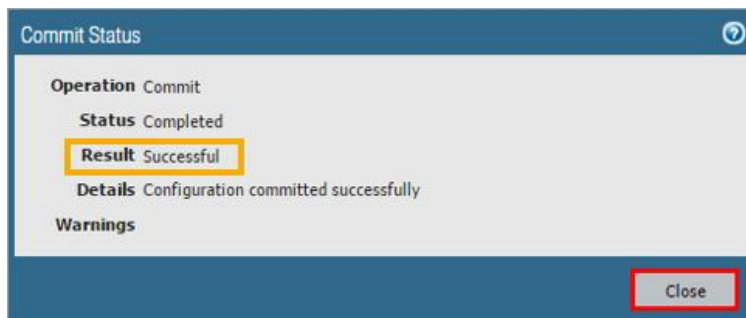
10. Click the **Commit** link at the top-right of the web interface.



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



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

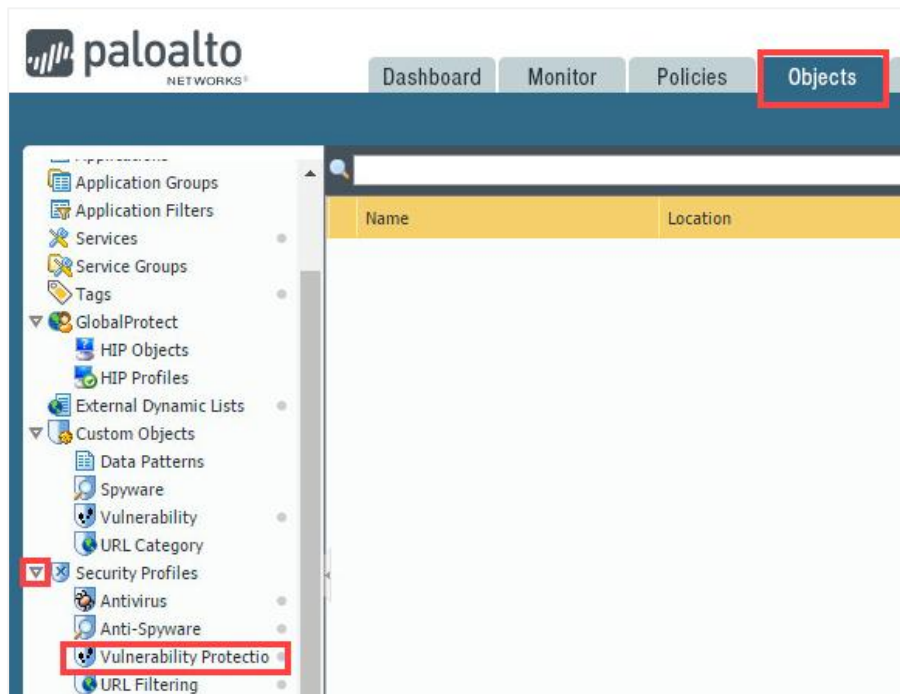


13. Leave the firewall web interface open to continue with the next task.

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**.

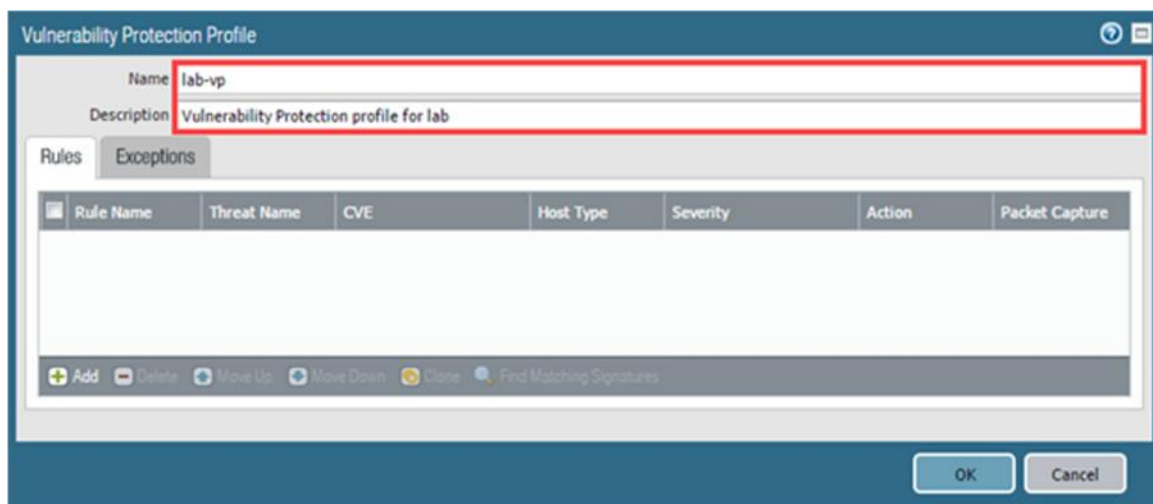


2. Click **Add** to create a *Vulnerability Protection Profile*.



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

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

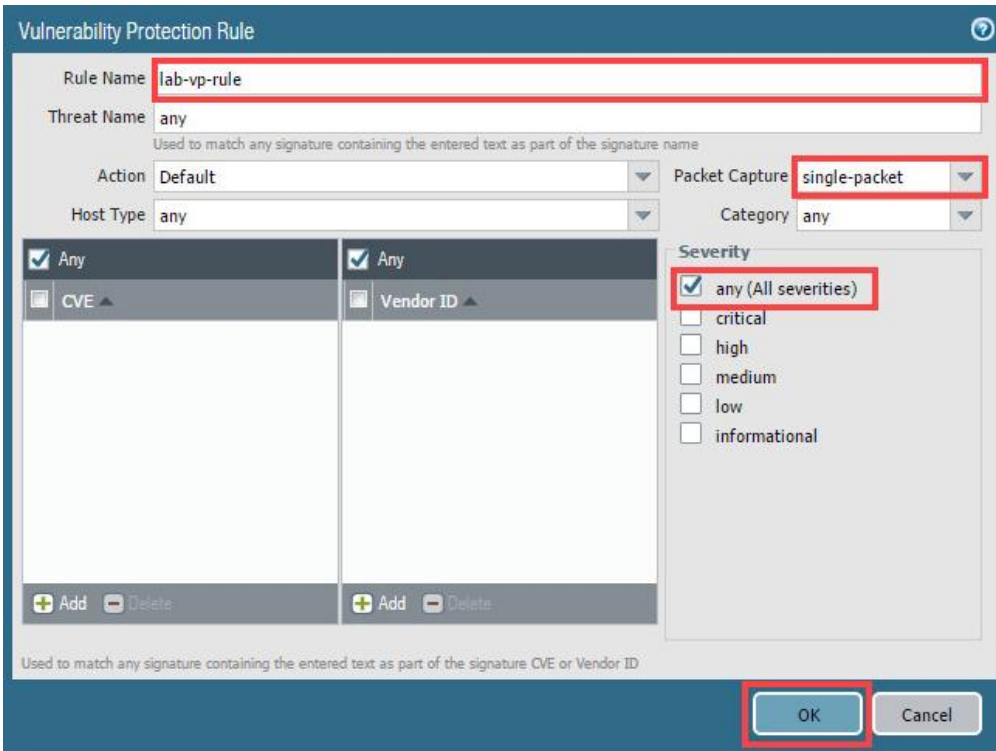


4. On the *Rules* tab, click **Add** to create a rule.



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

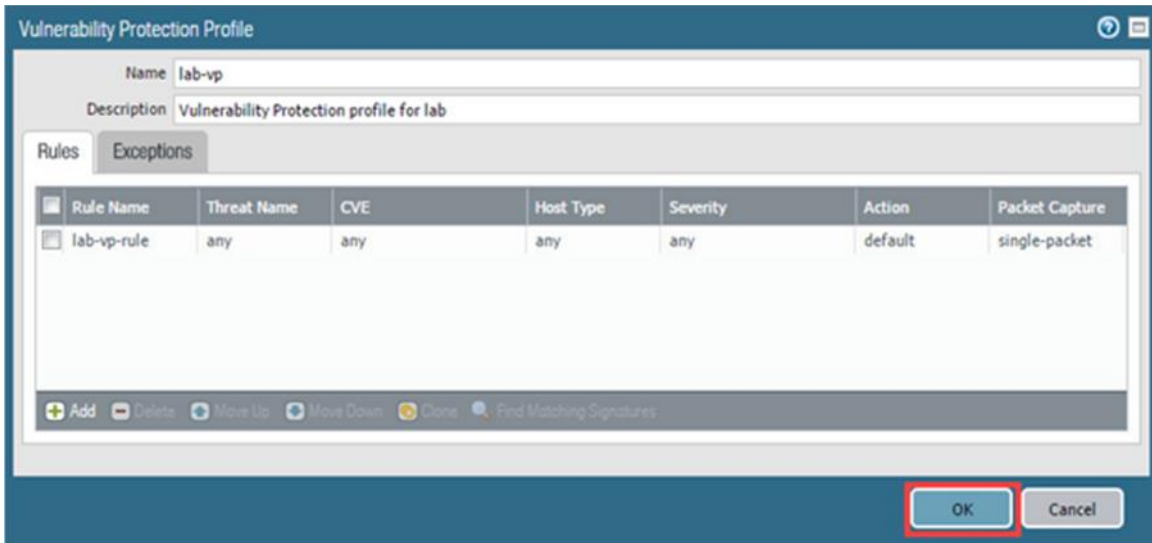


The screenshot shows the 'Vulnerability Protection Rule' configuration window. The following fields are highlighted with red boxes:

- Rule Name:** lab-vp-rule
- Threat Name:** any
- Packet Capture:** single-packet
- Severity:** any (All severities)
- OK button:** (highlighted with a red box)

The window also includes sections for 'Any' and 'Vendor ID' with 'Add' and 'Delete' buttons, and a 'Severity' section with checkboxes for 'critical', 'high', 'medium', 'low', and 'informational'.

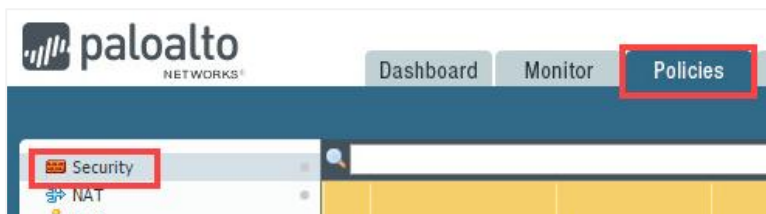
- Back on the *Vulnerability Protection Profile* window, ensure that the new rule appears and click **OK**.



The screenshot shows the 'Vulnerability Protection Profile' configuration window. The 'Name' field is 'lab-vp' and the 'Description' is 'Vulnerability Protection profile for lab'. The 'Rules' tab is active, showing a table with one rule: 'lab-vp-rule'. The rule has 'any' for Threat Name, CVE, Host Type, and Severity, and 'default' for Action and 'single-packet' for Packet Capture. At the bottom right, the 'OK' button is highlighted with a red box.

Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packet Capture
lab-vp-rule	any	any	any	any	default	single-packet

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

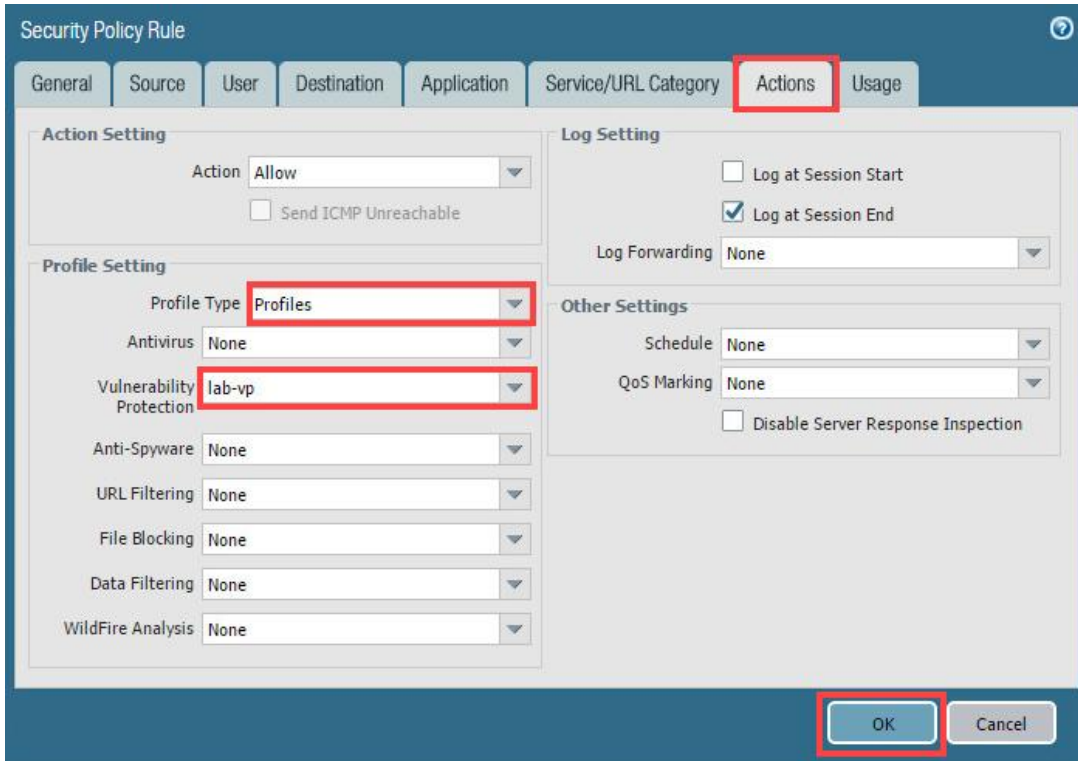


- Click on **internal-inside-dmz** to open the Security policy rule.

	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 drop-down list
Vulnerability Protection	Select lab-vp from the drop-down list



10. **Commit** all changes.

1.2 Test the Security Policy Rule

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

- 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 Universal 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 . . . _
```




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


1.3 Review the Logs

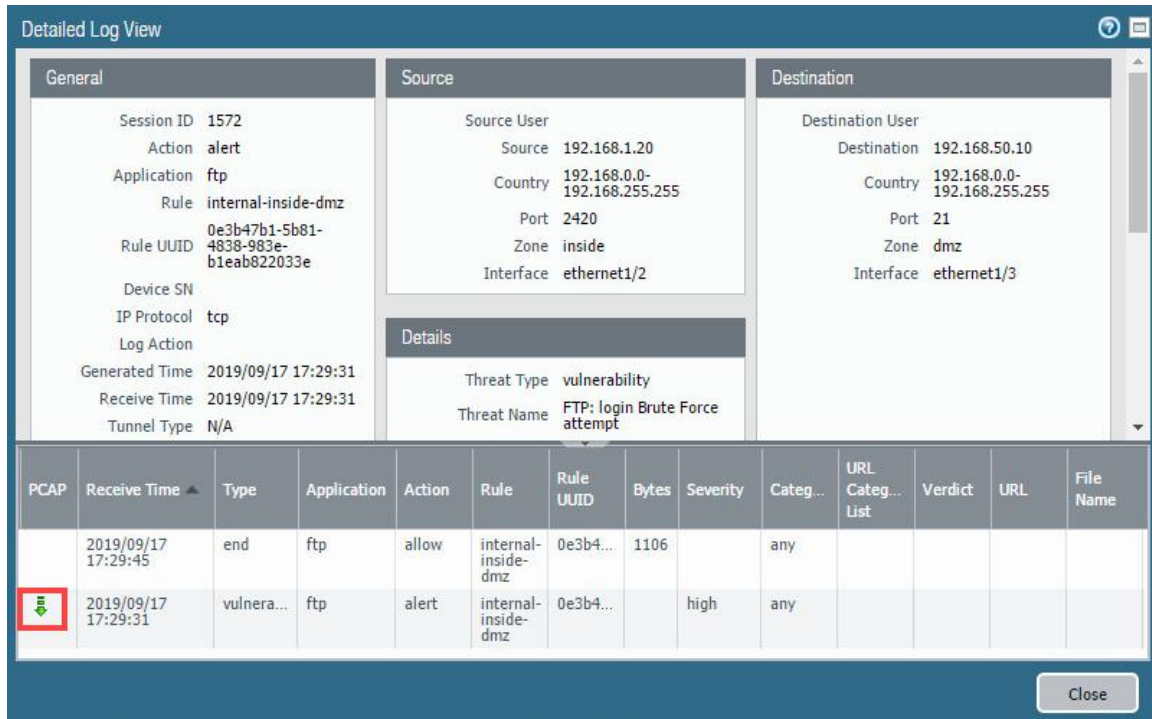
- Change focus to the firewall web interface and select **Monitor > Logs > Threat**.



- 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

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



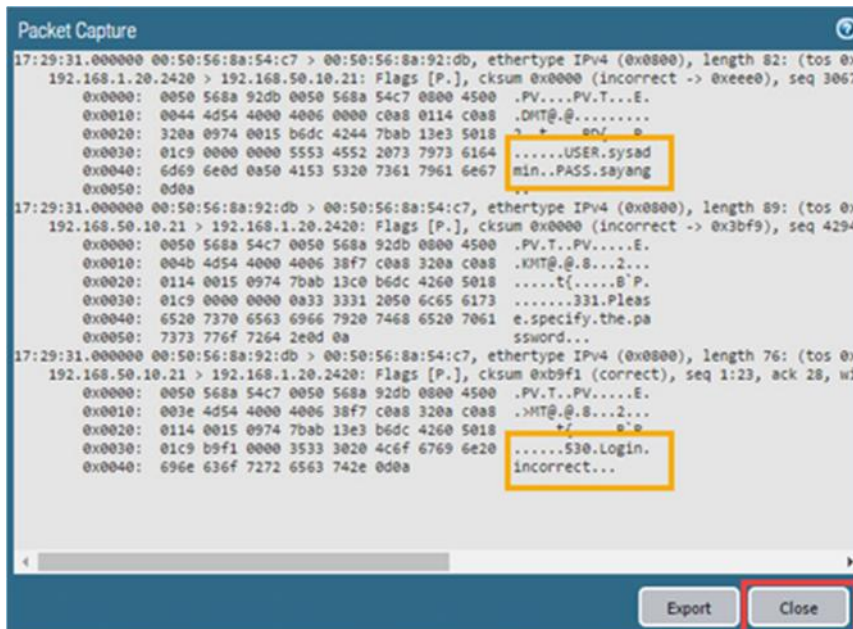
Detailed Log View

General	Source	Destination
Session ID 1572	Source User	Destination User
Action alert	Source 192.168.1.20	Destination 192.168.50.10
Application ftp	Country 192.168.0.0-192.168.255.255	Country 192.168.0.0-192.168.255.255
Rule internal-inside-dmz	Port 2420	Port 21
Rule UUID 0e3b47b1-5b81-4838-983e-b1eab822033e	Zone inside	Zone dmz
Device SN	Interface ethernet1/2	Interface ethernet1/3
IP Protocol tcp	Details	
Log Action	Threat Type vulnerability	
Generated Time 2019/09/17 17:29:31	Threat Name FTP: login Brute Force attempt	
Receive Time 2019/09/17 17:29:31		
Tunnel Type N/A		

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Bytes	Severity	Categ...	URL Categ...	Verdict	URL	File Name
	2019/09/17 17:29:45	end	ftp	allow	internal-inside-dmz	0e3b4...	1106		any				
	2019/09/17 17:29:31	vulnera...	ftp	alert	internal-inside-dmz	0e3b4...		high	any				

Close

- 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**.



Packet Capture

```

17:29:31.000000 00:50:56:8a:54:c7 > 00:50:56:8a:92:db, ethertype IPv4 (0x0800), length 82: (tos 0x0)
192.168.1.20.2420 > 192.168.50.10.21: Flags [P.], cksum 0x0000 (incorrect -> 0xeeee), seq 3067
0x0000: 0050 568a 92db 0050 568a 54c7 0800 4500 .PV...PV.T...E.
0x0010: 0044 4d54 4000 4006 0000 c0a8 0114 c0a8 .DMT@.@.....
0x0020: 320a 0974 0015 b6dc 4244 7bab 13e3 5018 .....+...enf e
0x0030: 01c9 0000 0000 5553 4552 2073 7973 6164 .....USER.sysad
0x0040: 6d69 6e0d 0a50 4153 5320 7361 7961 6e67 min..PASS.sayang
0x0050: 0d0a

17:29:31.000000 00:50:56:8a:92:db > 00:50:56:8a:54:c7, ethertype IPv4 (0x0800), length 89: (tos 0x0)
192.168.50.10.21 > 192.168.1.20.2420: Flags [P.], cksum 0x0000 (incorrect -> 0x3bf9), seq 4294
0x0000: 0050 568a 54c7 0050 568a 92db 0800 4500 .PV.T..PV....E.
0x0010: 004b 4d54 4000 4006 38f7 c0a8 320a c0a8 .KMT@.@.8...2...
0x0020: 0114 0015 0974 7bab 13c0 b6dc 4260 5018 .....t{....B'P.
0x0030: 01c9 0000 0000 0a33 2050 6c65 6173 .....331.Pleas
0x0040: 6520 7370 6563 6966 7920 7468 6520 7061 e.specify.the.pa
0x0050: 7373 776f 7264 2e0d 0a ssword...

17:29:31.000000 00:50:56:8a:92:db > 00:50:56:8a:54:c7, ethertype IPv4 (0x0800), length 76: (tos 0x0)
192.168.50.10.21 > 192.168.1.20.2420: Flags [P.], cksum 0xb9f1 (correct), seq 1:23, ack 28, win
0x0000: 0050 568a 54c7 0050 568a 92db 0800 4500 .PV.T..PV....E.
0x0010: 003e 4d54 4000 4006 38f7 c0a8 320a c0a8 .>MT@.@.8...2...
0x0020: 0114 0015 0974 7bab 13e3 b6dc 4260 5018 .....+...e'e
0x0030: 01c9 b9f1 0000 3533 3020 4cef 6769 6e20 .....530.Login.
0x0040: 696e 636f 7272 6563 742e 0d0a incorrect...
  
```

Export Close



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

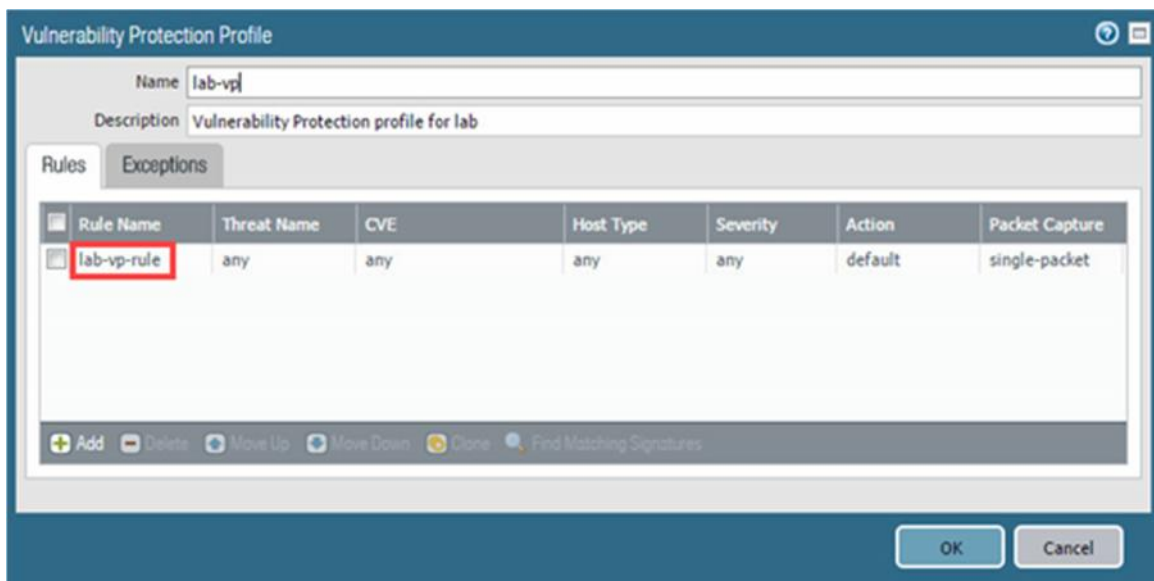
- Back on the *Detailed Log View* window, click **Close**.
- Leave the firewall web interface open to continue with the next task.

1.4 Update the Vulnerability Profile

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

- 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

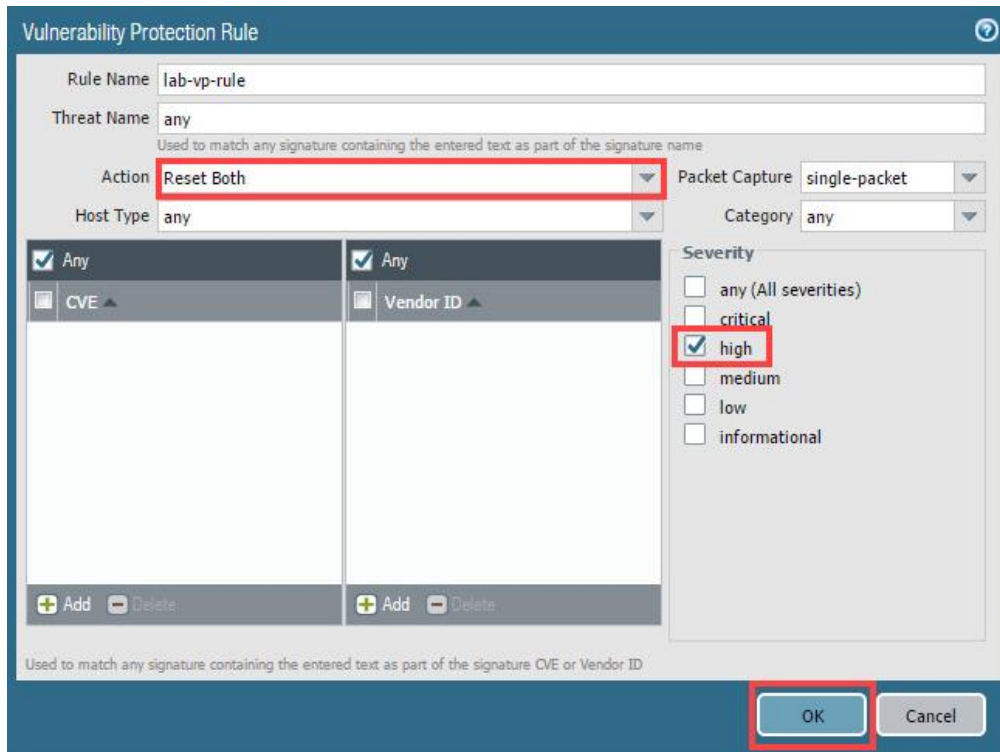
Rules Exceptions

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

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 drop-down 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

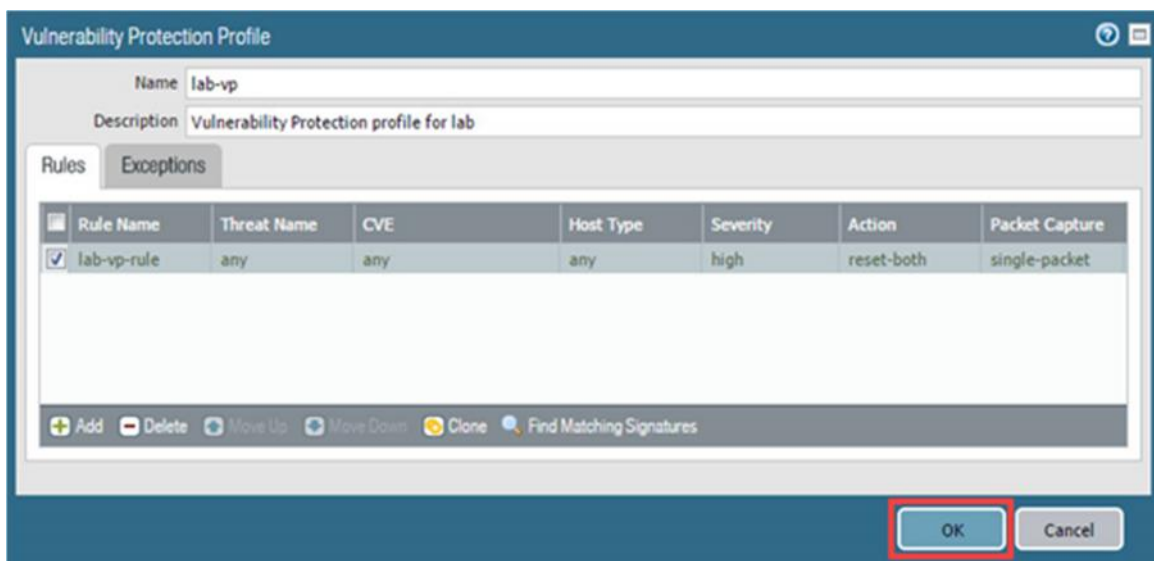
Severity:

- ☐ 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
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.

- 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.

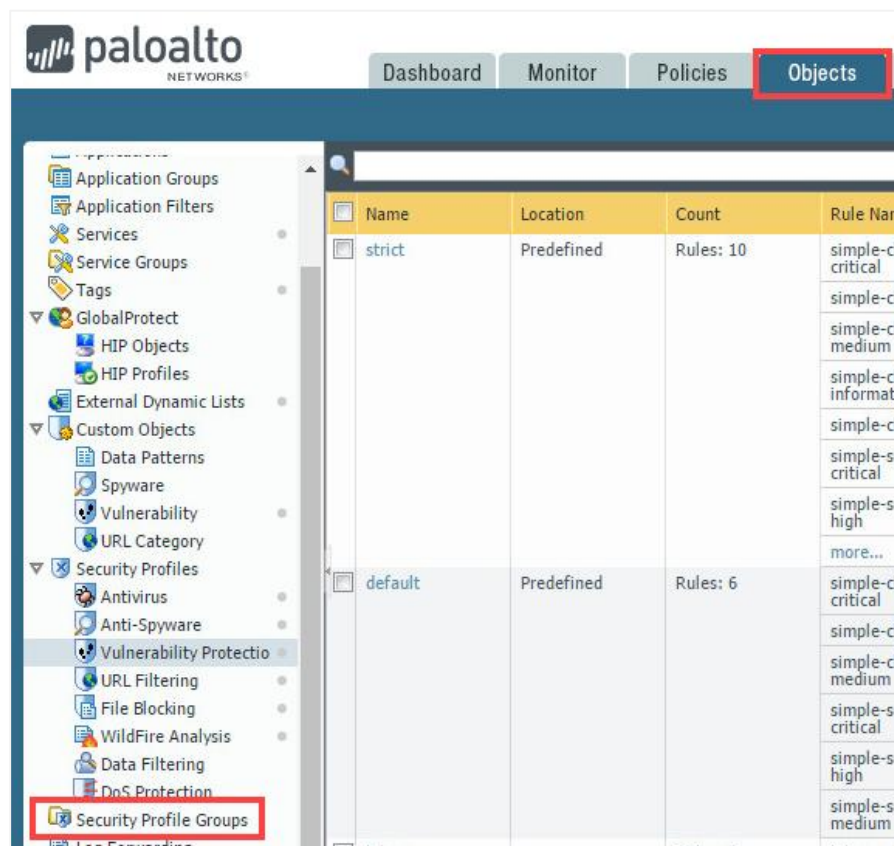
	Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	App...	Action
	09/17 18:26:51	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	reset-both
	09/17 18:26:51	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10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

- 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.

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

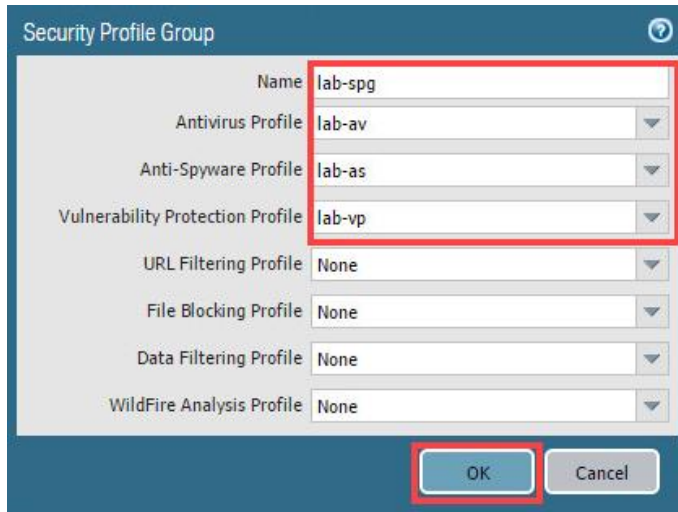


- Click **Add** to create a *Security Profile Group*.

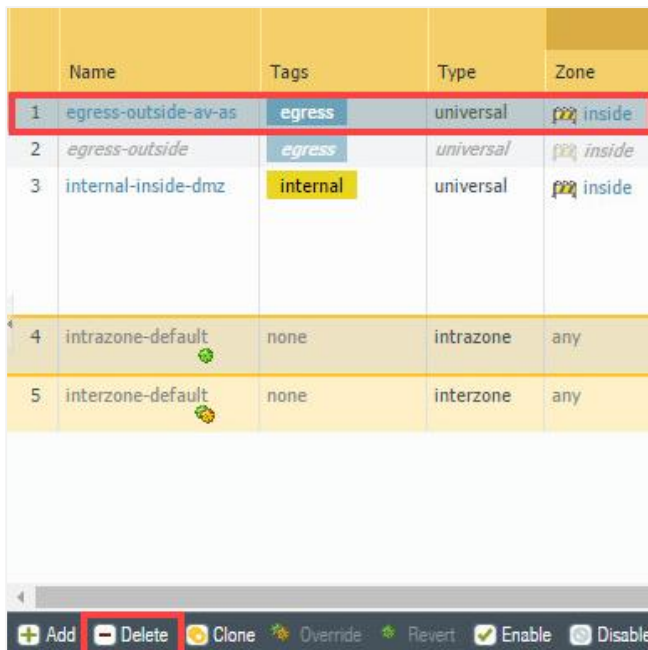


- In the *Security Profile Group* window, configure the following. Once finished, click **OK**.

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



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

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

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



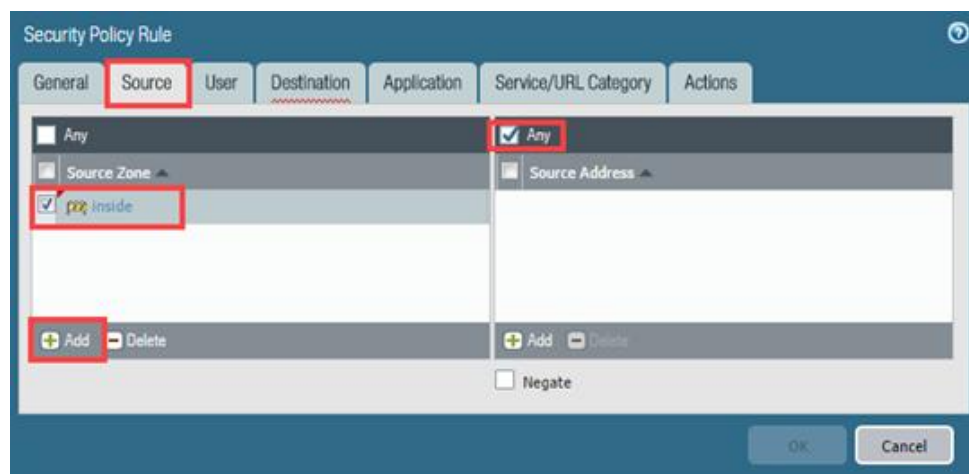
8. In the *Security Policy Rule* window, while on the *General* tab, configure the following.

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.



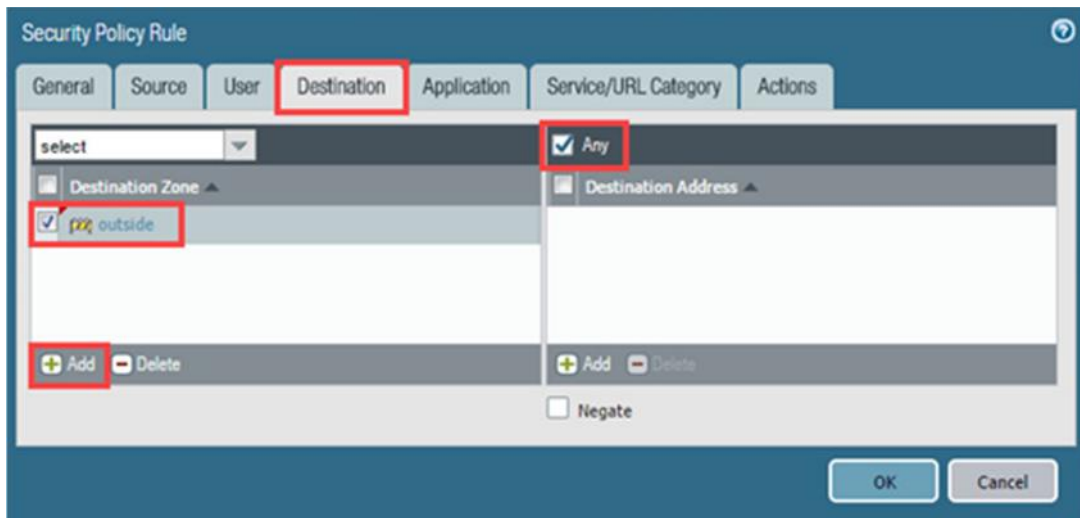
9. In the *Security Policy Rule* window, click the **Source** tab to configure the following.

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

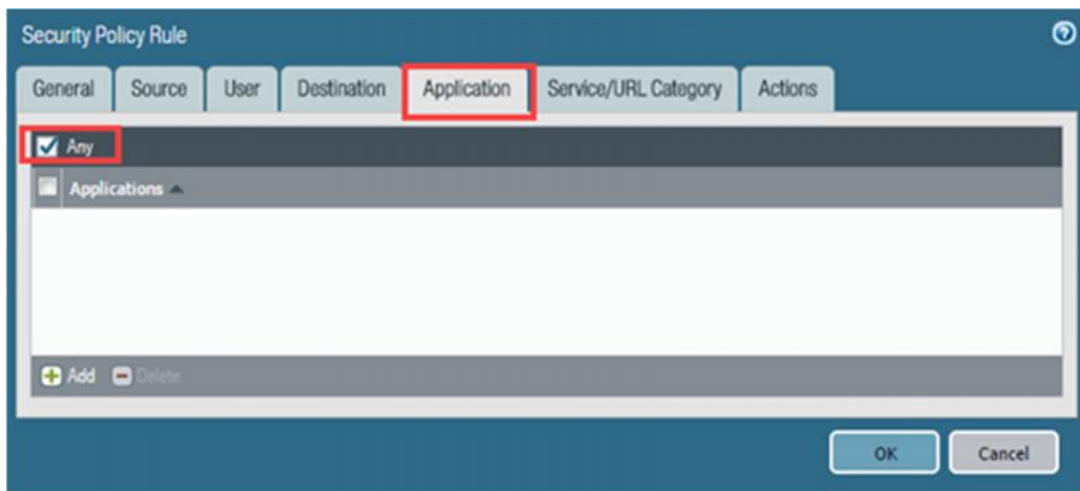


10. In the *Security Policy Rule* window, click the **Destination** tab and configure the following.

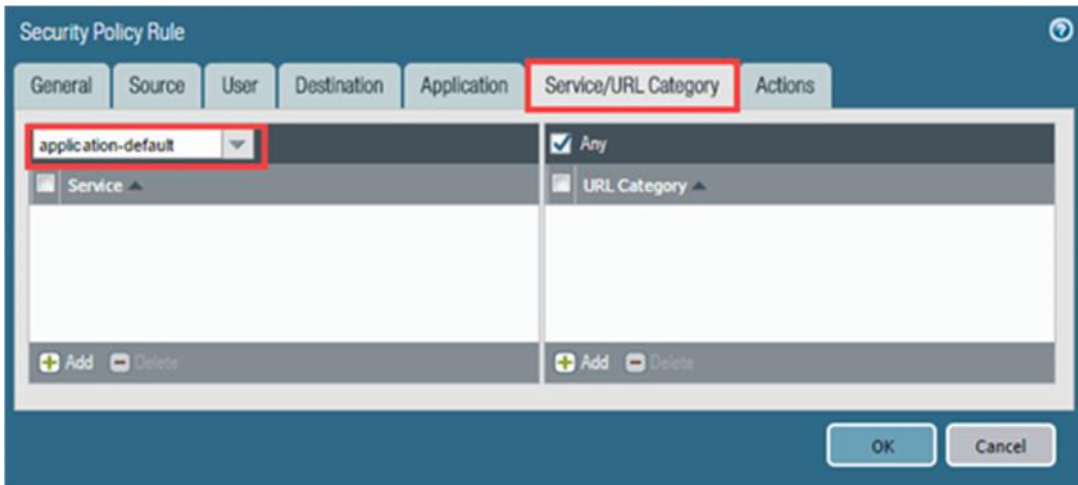
Parameter	Value
Destination Zone	Click Add and select outside from the drop-down list
Destination Address	Verify that the Any checkbox is selected



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

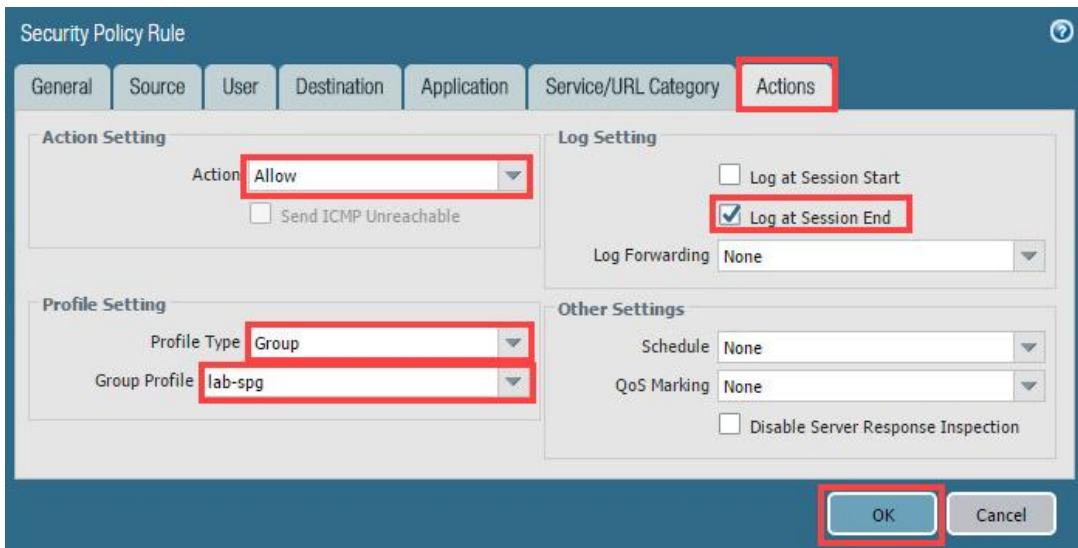


12. In the *Security Policy Rule* window, click the **Service/URL Category** tab and verify that **application-default** is selected.



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**.

	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

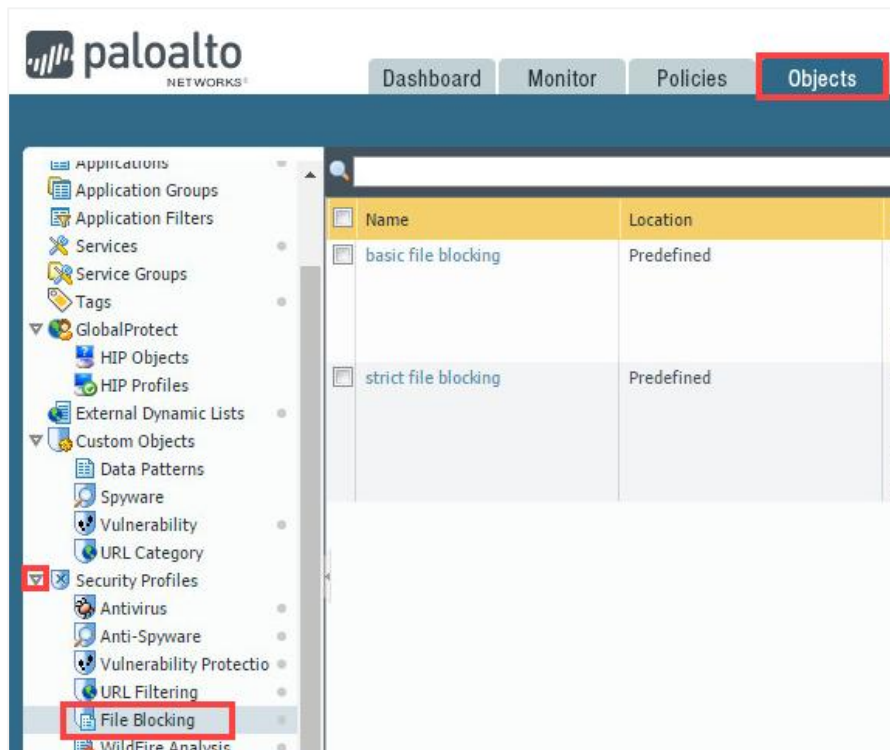
Add Delete Clone Override Revert Enable Disable Move PDF/CSV

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

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**.

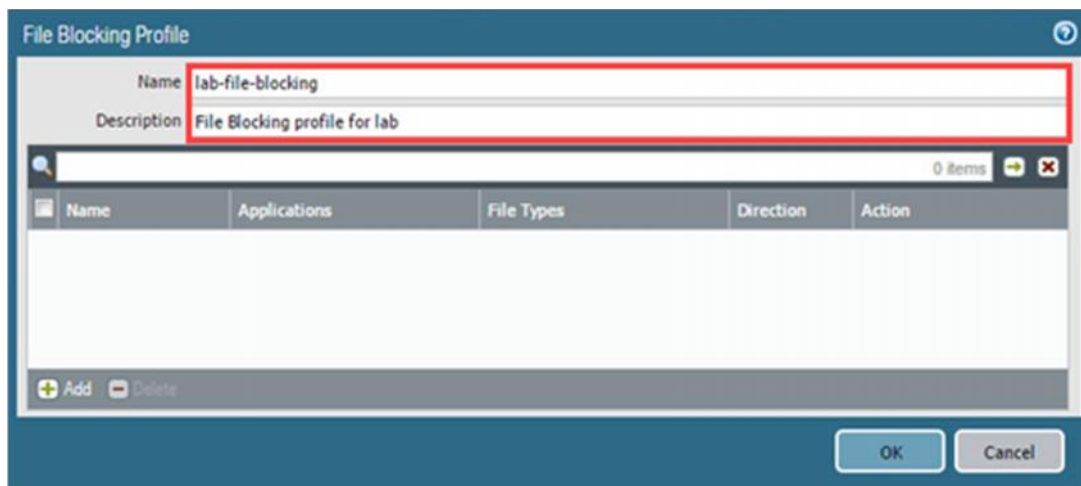


2. Click **Add** to open the *File Blocking Profile* configuration window.



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

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

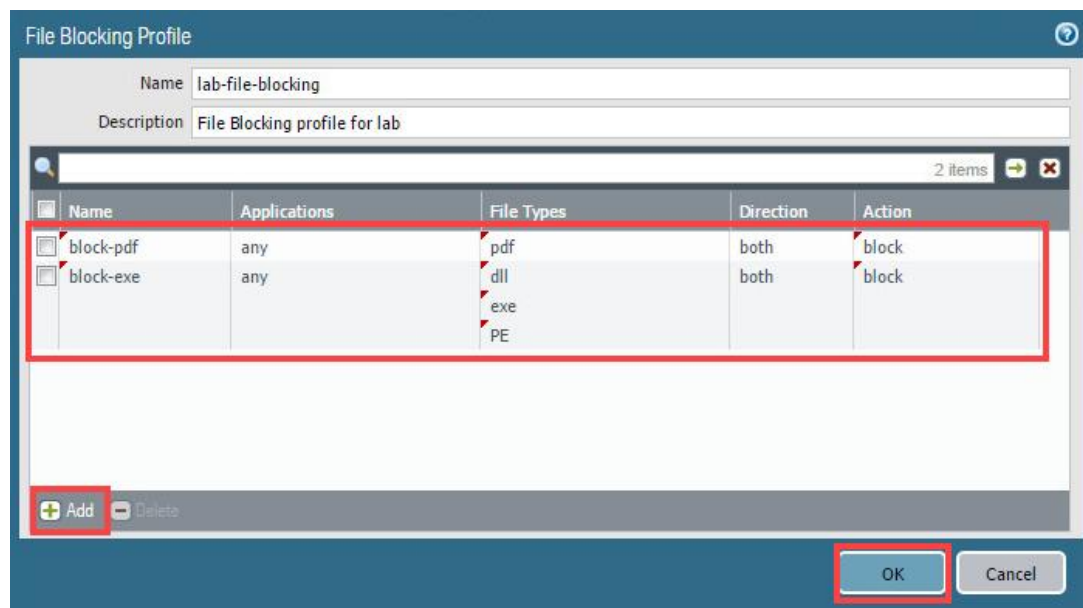


4. In the *File Blocking Profile* window, click **Add** and configure the following.

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**.

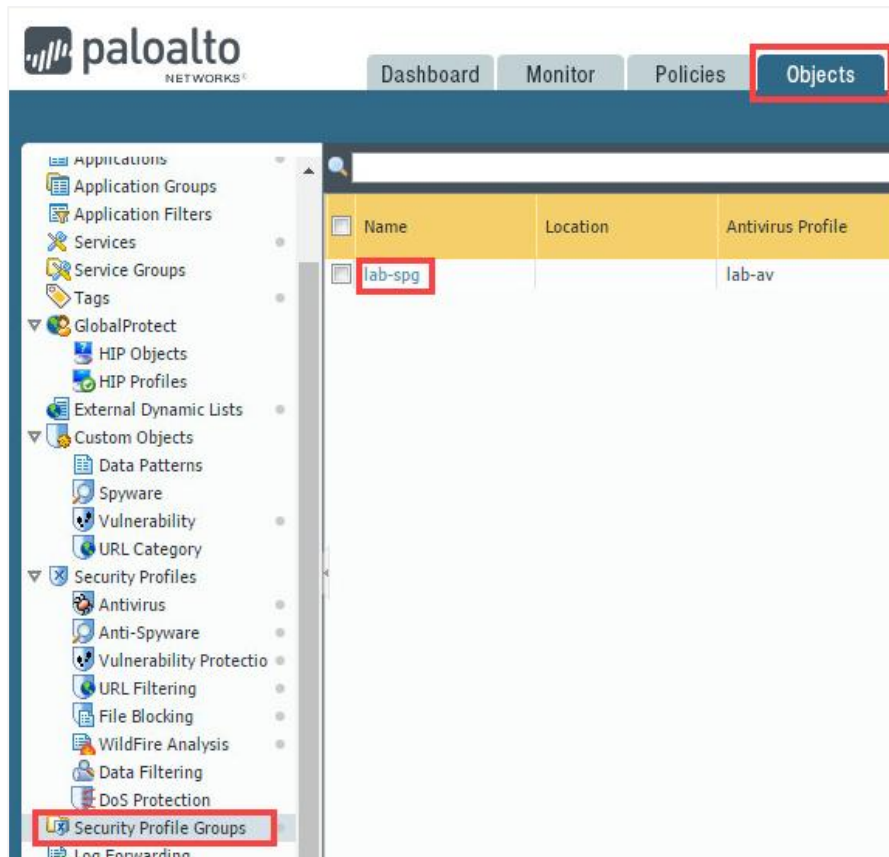
Parameter	Value
Name	Type block-exe
Applications	Verify that any is selected
File Types	Click Add and select the following from the drop-down list: dll exe PE
Direction	Verify that both is selected
Action	Select block from the drop-down list



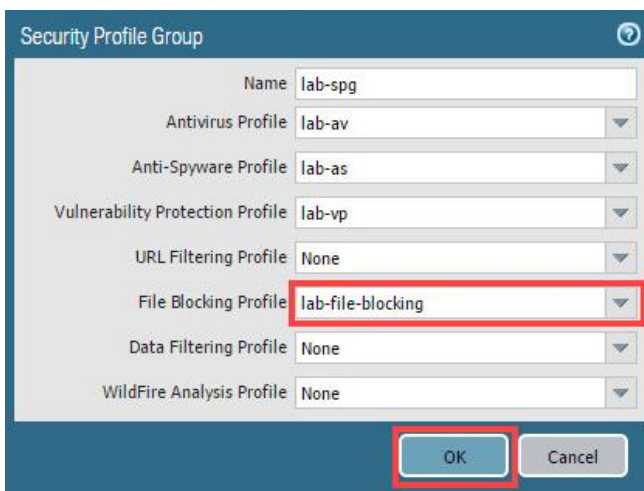
6. Verify that the new profile appears in the list. Leave the firewall web interface open to continue with the next task.

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**.



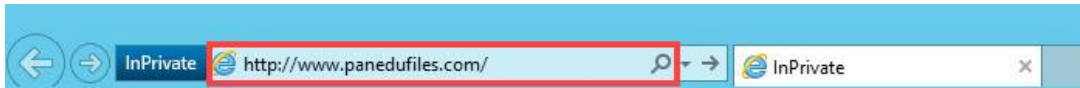
2. In the *Security Profile Group* window, select **lab-file-blocking** from the *File Blocking Profile* drop-down list and click **OK**.



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/>.



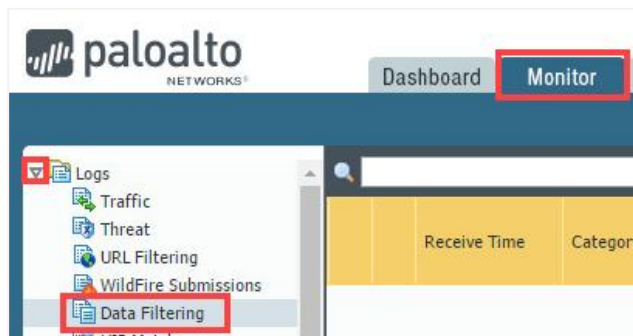
2. Once the webpage loads, click the **Panorama_AdminGuide.pdf** link.




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**.



- 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

- 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.

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

<input type="checkbox"/> Name	Location	Rule Name
<input type="checkbox"/> basic file blocking	Predefined	Block high risk file types Continue prompt encrypted files Log all other file types
<input type="checkbox"/> strict file blocking	Predefined	Block all risky file types Block encrypted files Log all other file types
<input type="checkbox"/> lab-file-blocking		block-pdf block-exe

- 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

File Blocking Profile

Name: lab-file-blocking

Description: File Blocking profile for lab

3 items

Name	Applications	File Types	Direction	Action
<input type="checkbox"/> block-pdf	any	pdf	both	block
<input type="checkbox"/> block-exe	any	dll exe PE	both	block
<input checked="" type="checkbox"/> block-multi-level	any	Multi-Level-Encoding	both	block

+ Add - Delete

OK Cancel

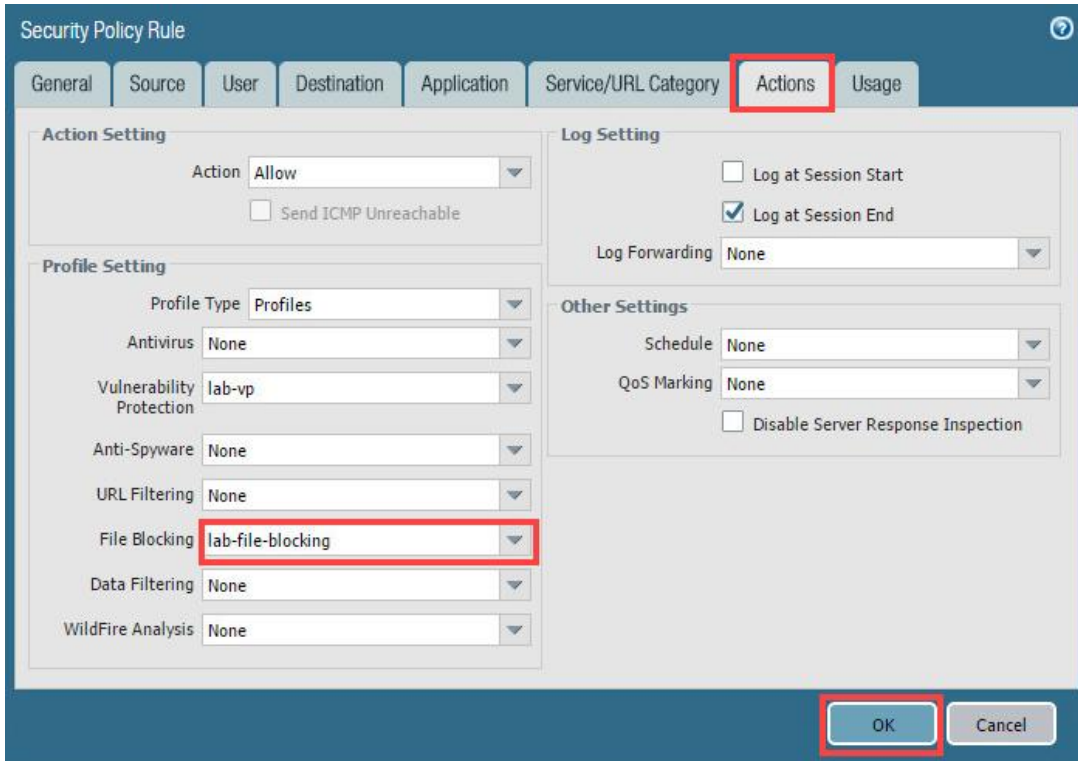
4. Leave the firewall web interface open to continue with the next task.

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.

	Name	Tags	Type	Zone	Addr
1	egress-outside-content-id	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

- 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**.

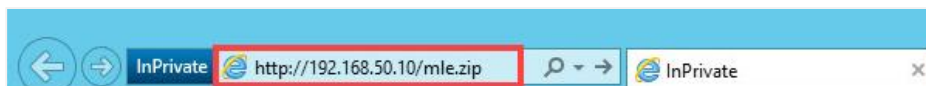


The screenshot shows the 'Security Policy Rule' configuration window. The 'Actions' tab is selected. Under 'Profile Setting', 'File Blocking' is set to 'lab-file-blocking'. The 'OK' button is at the bottom right.

- Commit** all changes.

1.11 Test the File Blocking Profile with Multi-Level Encoding

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



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

File Transfer Blocked

Transfer of the file you were trying to download or upload has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

File name: multi-level-encoded-file.zip

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.

<input type="checkbox"/> Name	Location	Rule Name
<input type="checkbox"/> basic file blocking	Predefined	Block high risk file types Continue prompt encrypted files Log all other file types
<input type="checkbox"/> strict file blocking	Predefined	Block all risky file types Block encrypted files Log all other file types
<input type="checkbox"/> 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**.

File Blocking Profile

Name lab-file-blocking

Description File Blocking profile for lab

3 items

<input type="checkbox"/> Name	Applications	File Types	Direction	Action
<input type="checkbox"/> block-pdf	any	pdf	both	block
<input type="checkbox"/> block-exe	any	dll exe PE	both	block
<input checked="" type="checkbox"/> block-multi-level	any	Multi-Level-Encoding	both	alert

+

 Add

-

 Delete

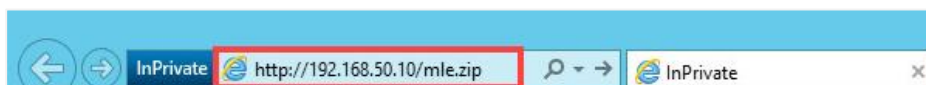
OK

Cancel

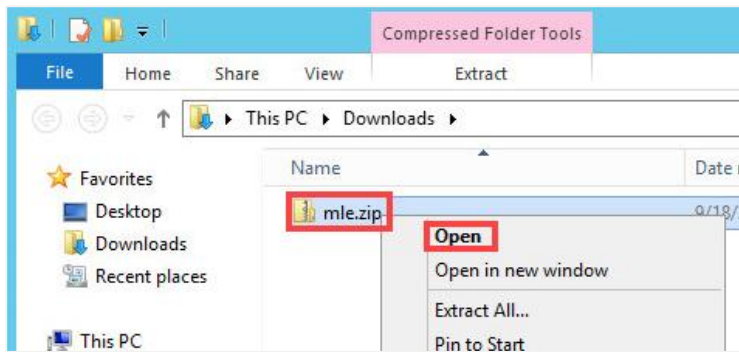
4. **Commit** all changes.

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**.



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



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

1.14 Create a Danger Security Policy Rule

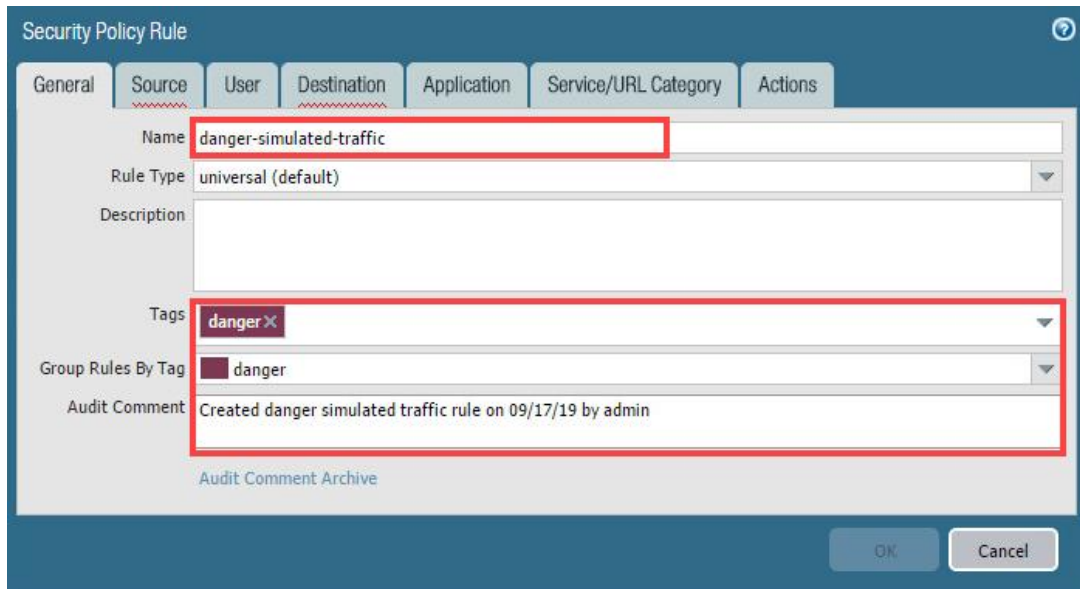
Create a Security Policy Rule that references the danger security zone for threat and traffic generation.

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



- 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



Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Name: danger-simulated-traffic

Rule Type: universal (default)

Description:

Tags: danger

Group Rules By Tag: danger

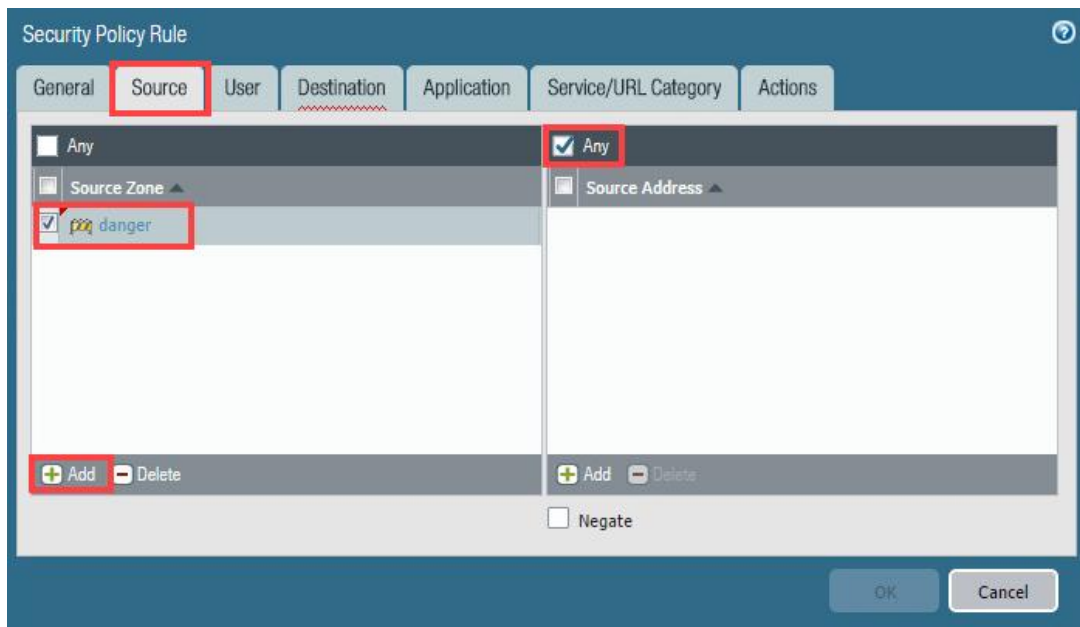
Audit Comment: Created danger simulated traffic rule on 09/17/19 by admin

Audit Comment Archive

OK Cancel

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



Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Any

Source Zone

Source Address

Any

danger

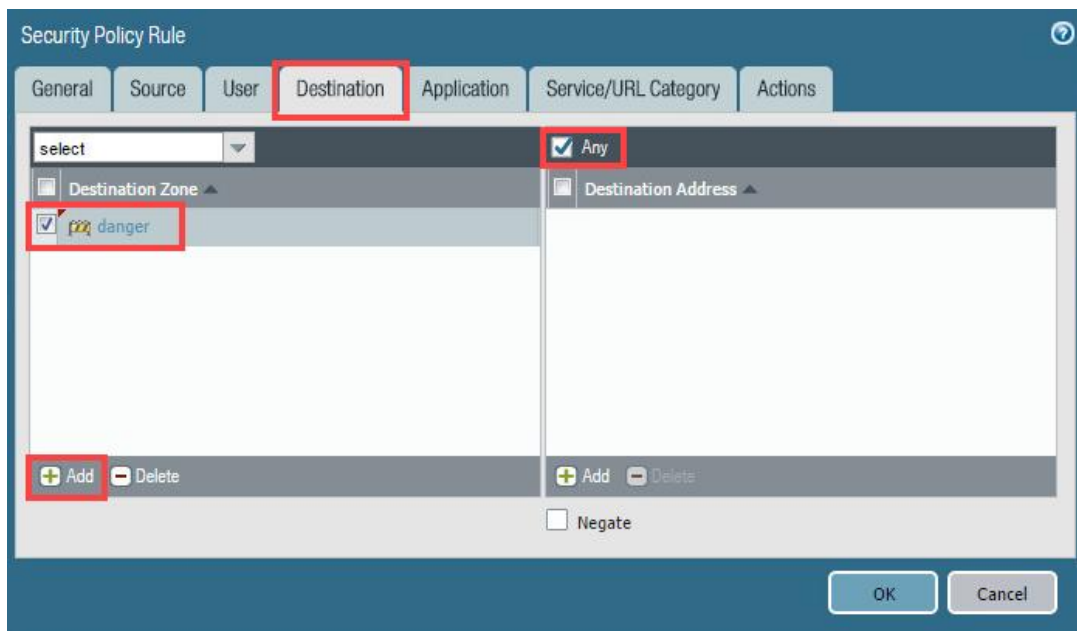
Add Delete

Negate

OK Cancel

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

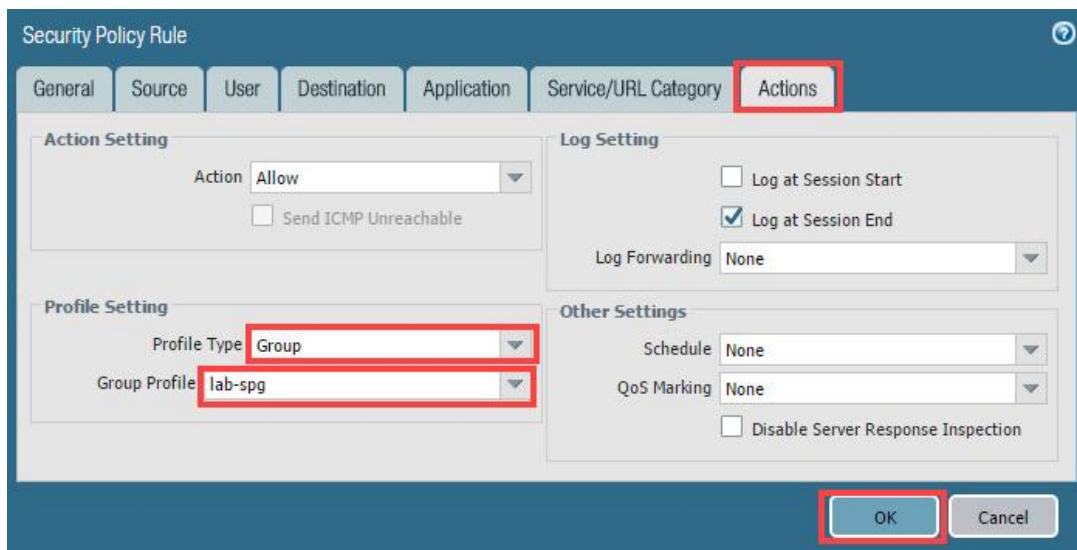
Parameter	Value
Destination Zone	Click Add and select danger from the drop-down list
Destination Address	Verify that the Any checkbox is selected



The screenshot shows the 'Security Policy Rule' configuration window with the 'Destination' tab selected. The 'Destination Zone' list contains one entry, 'danger', which is checked. The 'Destination Address' list is empty. The 'Any' checkbox is checked. The 'Add' button is highlighted with a red box. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

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



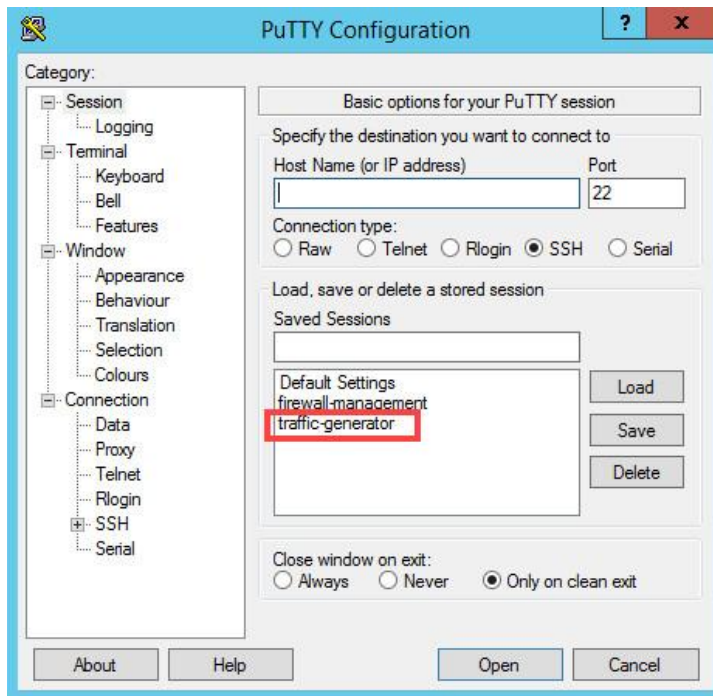
The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action Setting' section has 'Action' set to 'Allow'. The 'Profile Setting' section has 'Profile Type' set to 'Group' and 'Group Profile' set to 'lab-spg'. The 'Log Setting' section has 'Log at Session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

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 **Pa10A1t0** followed by pressing the **Enter** key.

```
Using username "root".
root@192.168.50.10's password:
Last login: Tue Aug  6 20:57:35 2019
[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
```

```
[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 ~]#
```

- 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	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

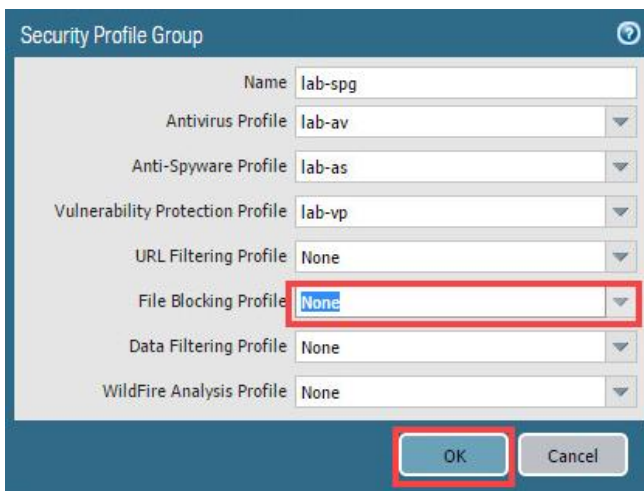
10. Leave the firewall web interface open to continue with the next task.

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.

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



The image shows the 'Security Profile Group' configuration window. It contains several dropdown menus for selecting profiles. The 'File Blocking Profile' dropdown is highlighted with a red box, and the word 'None' is selected within it. The 'OK' button at the bottom is also highlighted with a red box.

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

Buttons: OK, Cancel

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

2. Close the **PuTTY** window.
3. In the web interface, navigate to **Monitor > Logs > Threat**.

- 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.swroot.dfp	danger	danger	10.10.10.10	192.158.1.121	25	smtp	reset-both	high
		09/18 19:24:29	vulnerability	Ransom-Win32.ocky.pe	danger	danger	10.10.10.10	192.158.1.121	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.swroot.dfp	danger	danger	10.10.10.10	192.158.1.121	25	smtp	reset-both	high
		09/18 19:13:54	vulnerability	Ransom-Win32.ocky.pe	danger	danger	10.10.10.10	192.158.1.121	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 T.S 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.

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