Palo Alto Networks

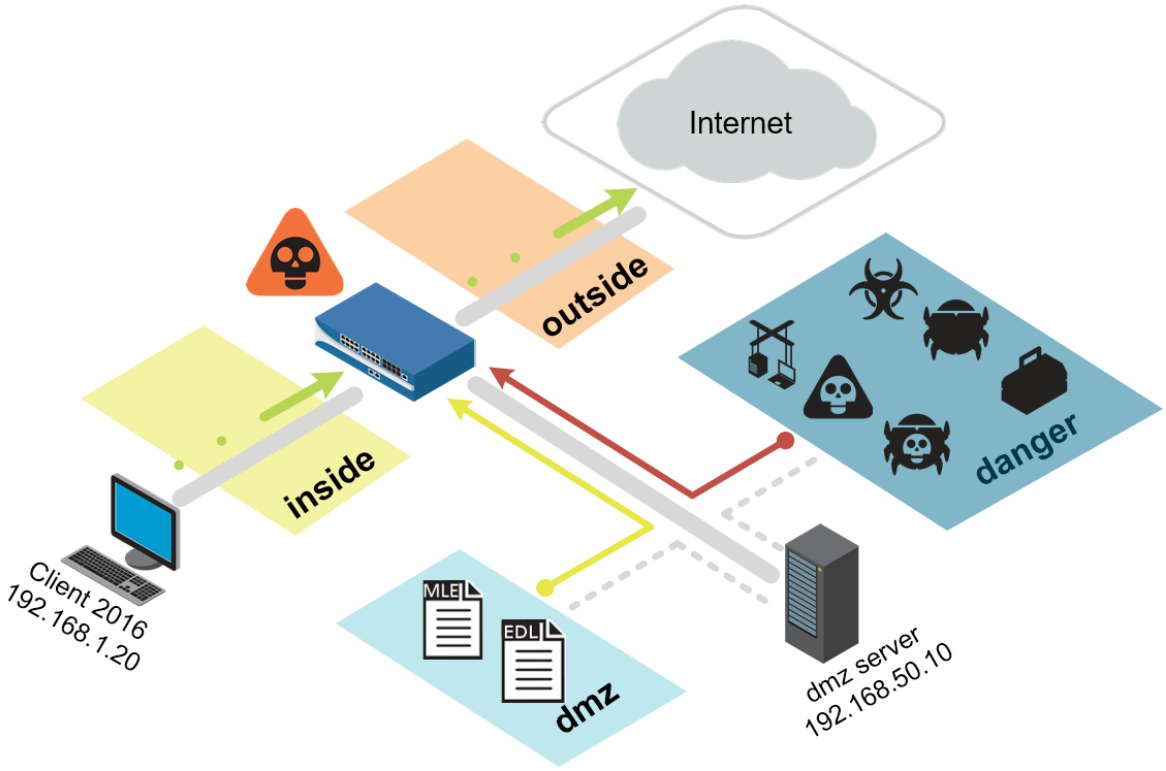
Academy Labs

Lab Content-ID

Document Version: 10-Dec-19

www.paloaltonetworks.com

Lab Topology



Virtual Machine	Username	Password
Firewall	admin	admin
Server 2012	lab-user	Pal0Alt0
Centos AAC DMZ	root	Pal0Alt0
Centos Virtual Router	root	Pal0Alt0

Powering Down Your VMware Workstation VM-50 firewall appliance:

If after powering off your VM-50 firewall appliance via VMware Workstation it remains powered on, please shut it down by accessing the CLI via SSH and entering the following command: "request shutdown system". You can access the firewall appliance via ssh from the Windows 2016 client virtual machine using PuTTY and 192.168.1.254 as the destination IP address or from your host computer using PuTTY and the Centos VR virtual machine's external interface's (ens160) IP address as the destination ssh address.

Lab: Content-ID

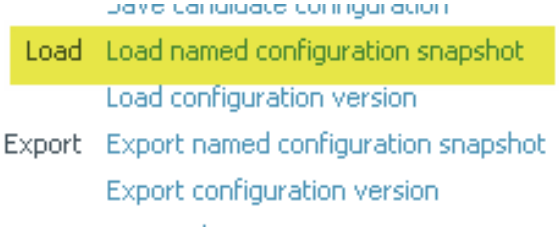
Lab Objectives

- **Configure and test an Antivirus Security Profile.**
- **Configure and test an Anti-Spyware Security Profile.**
- **Configure and test the DNS Sinkhole feature with an External Dynamic List.**
- **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.**

1.0 Load a Lab Configuration

To start this lab exercise, you will load a preconfigured firewall configuration file.

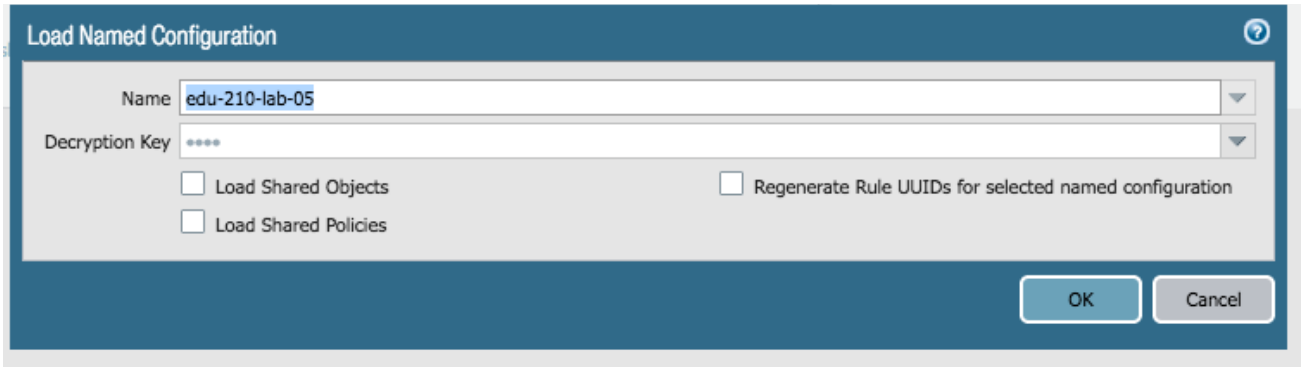
1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



A **Load Named Configuration** dialog box appears.

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

Note: Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers:



4. Click **OK** to close the **Load Named Configuration** window.

A window should appear that confirms that the configuration is being loaded.

5. Click **Close** to close the **Loading Configuration** window.

6. Click the **Commit** link at the upper right of the web interface:

A **Commit** window should appear.

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

A **Commit Status** window should appear that confirms the configuration was committed successfully.

8. Click **Close** to continue.

1.1 Create a Security Policy Rule with an Antivirus Profile

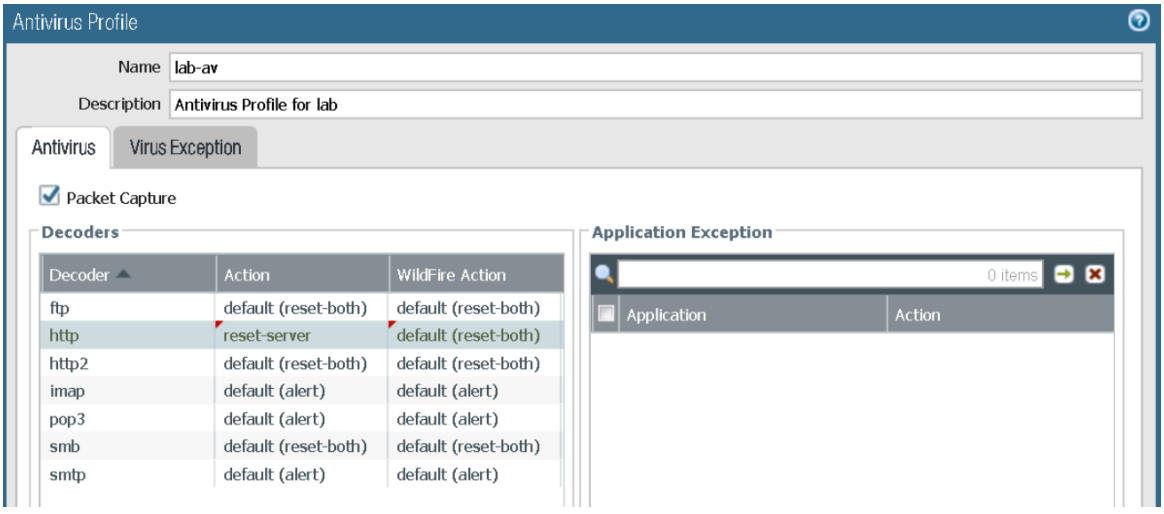
Use an Antivirus Profile object to configure options to have the firewall scan for viruses on traffic matching a Security policy rule. Set the applications that should be inspected for viruses and the action to take when a virus is detected.

9. In the web interface, select **Objects > Security Profiles > Antivirus**.
10. Click **Add** to create an **Antivirus Profile**.

An **Antivirus Profile** configuration window should appear.

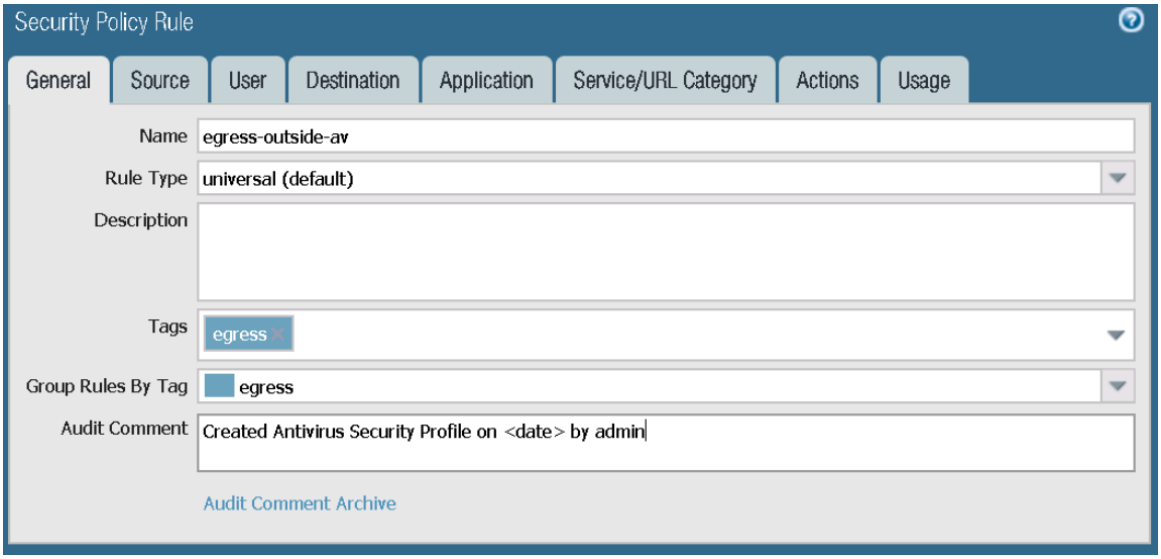
11. Configure the following:

Parameter	Value
Name	**Type `lab-av`**
Description	**Type `Antivirus profile for lab`**
Packet Capture	Select **Packet Capture check box**
Decoder	Set the **Action** column for **http** to **reset-server**



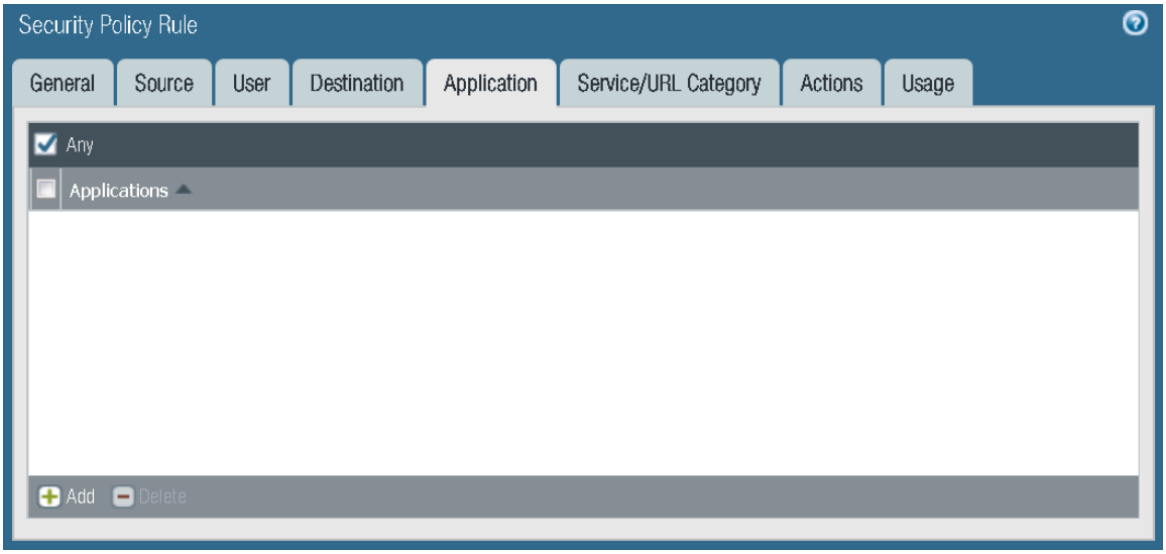
12. Click **OK** to close the **Antivirus Profile** configuration window.
    A new Antivirus Profile should appear in the web interface.
13. In the web interface, select **Policies** > **Security**.
14. Select the **egress-outside-app-id** Security policy rule.
    The **Security Policy Rule** configuration window should appear.
15. Configure the following:

Parameter	Value
Name	**Rename policy to `egress-outside-av`**
Audit Comment	**Type `Created Antivirus Security Policy on <date> by <Your-Role>`**



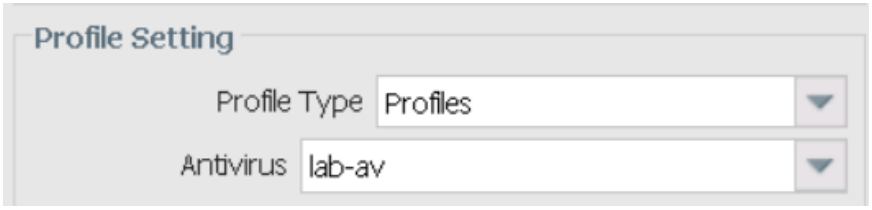
16. Click the **Application** tab and configure the following:

Parameter	Value
Applications	Select the **Applications** check box and click Delete
Applications	Verify that the **Any** check box is selected.



17. Click the **Actions** tab and configure the following:

Parameter	Value
Profile Type	Select **Profiles** from the drop-down list
Antivirus	Select **lab-av** from the drop-down list



18. Click **OK** to close the **Security Policy Rule** configuration window.
19. Verify that your configuration is like the following:

	Name	Tags	Type	Source				Destination		Application	Service	Action	Profile
				Zone	Addr...	Us...	HIP Pro...	Zone	Address				
1	egress-outside-av	egress	universal	inside	any	any	any	outside	any	any	application-default	Allow	
2	egress-outside	egress	universal	inside	any	any	any	outside	any	any	application-default	Allow	none
3	internal-dmz-ftp	internal	universal	inside	any	any	any	dmz	19...	ftp	application-default	Allow	none
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none
5	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none

20. **Commit** all changes.

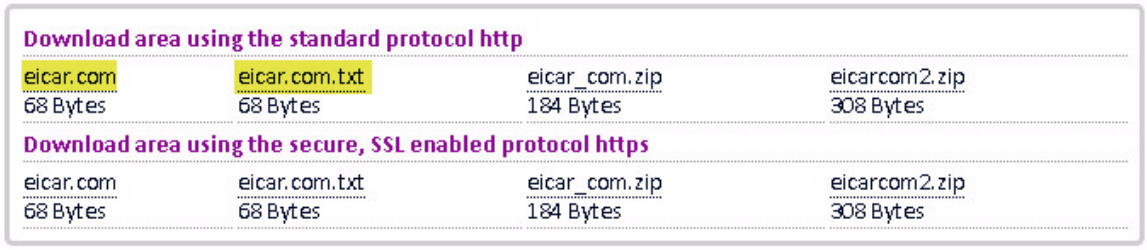
1.2 Test the Security Policy Rule

In this section, you will test your Antivirus Security Profile.

21. On your desktop, open a new browser window in private/incognito mode and browse to **`http://2016.eicar.org`**.
22. Click the **DOWNLOAD ANTI MALWARE TESTFILE** image in the upper-right corner:

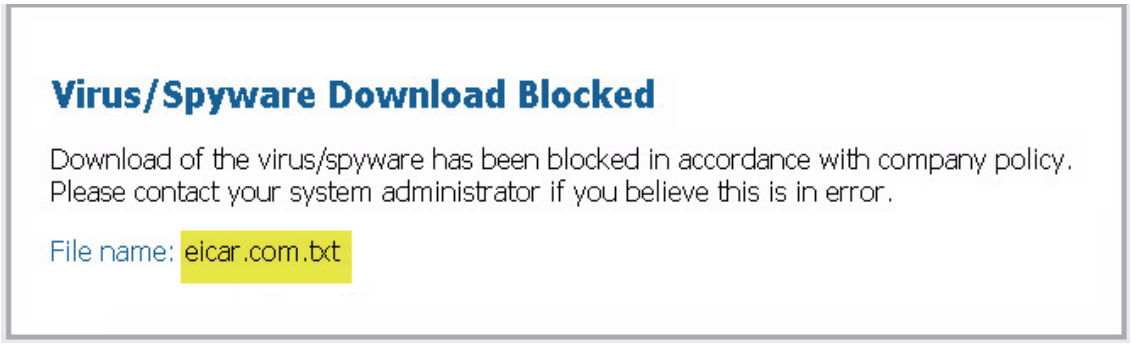
23. Click the **Download** link on the left of the webpage:

24. Within the **Download area using the standard protocol http** at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using standard HTTP and *not* SSL-enabled HTTPS.



The firewall will not be able to detect the viruses in an HTTPS connection until decryption is configured.

An **Virus/Spyware Download Blocked** page opens that shows that the file download was blocked:



25. Close the browser window.

1.3 Review the Logs

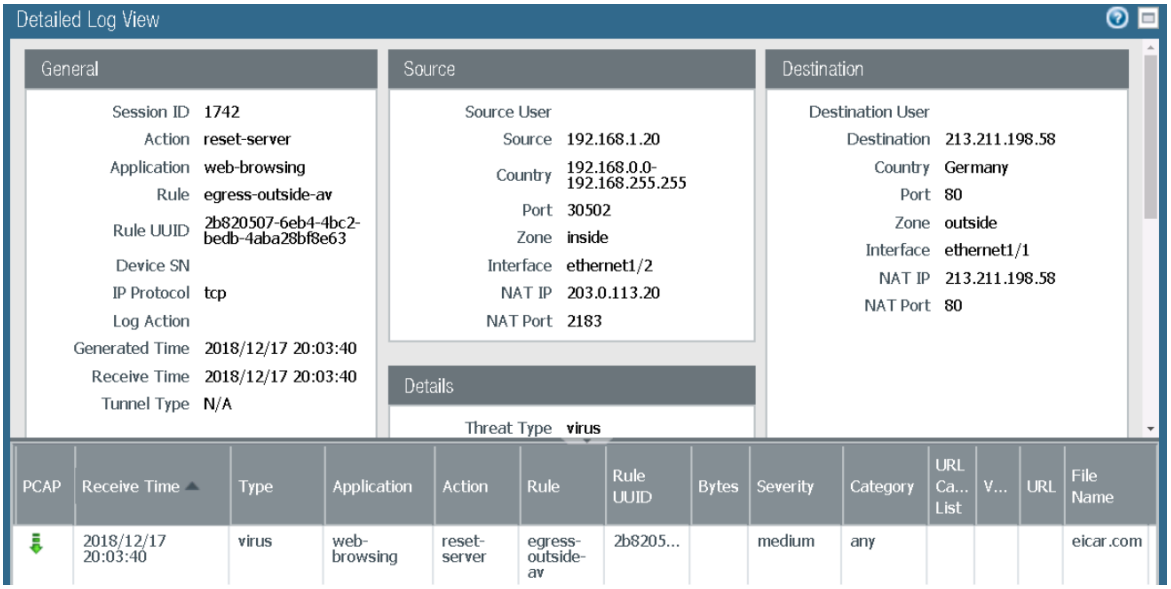
26. In the web interface, select **Monitor > Logs > Threat**.
27. Find the log message that detected the **Eicar Test File**. Notice that the action for the file is **reset-server**:

Destination address	To Port	Application	Action	Severity	File Name
213.211.198.58	80	web-browsing	reset-server	medium	eicar.com.txt

28. Notice the  icon on the left side of the entry for the **Eicar Test File**. It indicates that there is a packet capture (pcap):

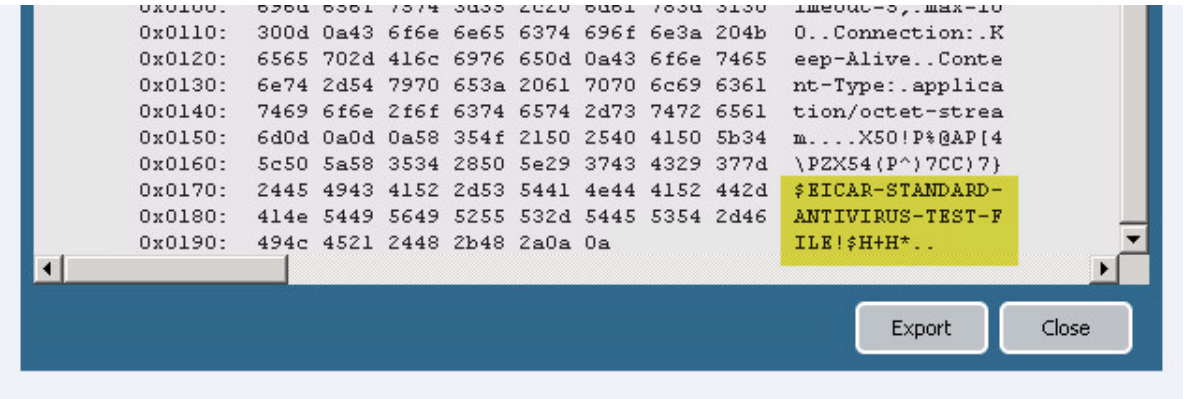
		Receive Time	Type	Name	From Zone	To Zone
		02/19 23:53:02	virus	Eicar Test File	inside	outside

29. To display the packet capture through the **Detailed Log View**, first click the **Detailed Log View** icon  to open the **Detailed Log View** of the threat entry:



30. From the **Detailed Log View**, click the icon to open the packet capture.

    Here is an example of what a pcap might look like:



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

31. After viewing the pcap, click **Close** to close the packet capture window.
32. Click **Close** to close the **Detailed Log View** window.

1.4 Create a Security Policy Rule with an Anti-Spyware Profile

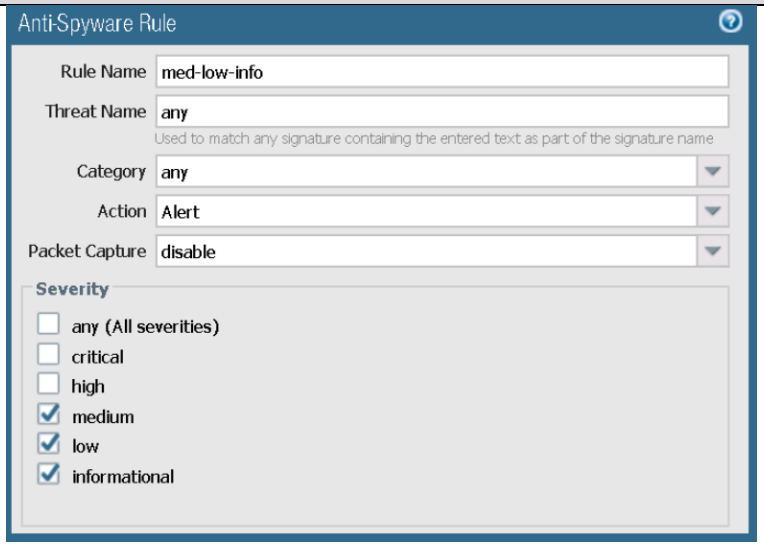
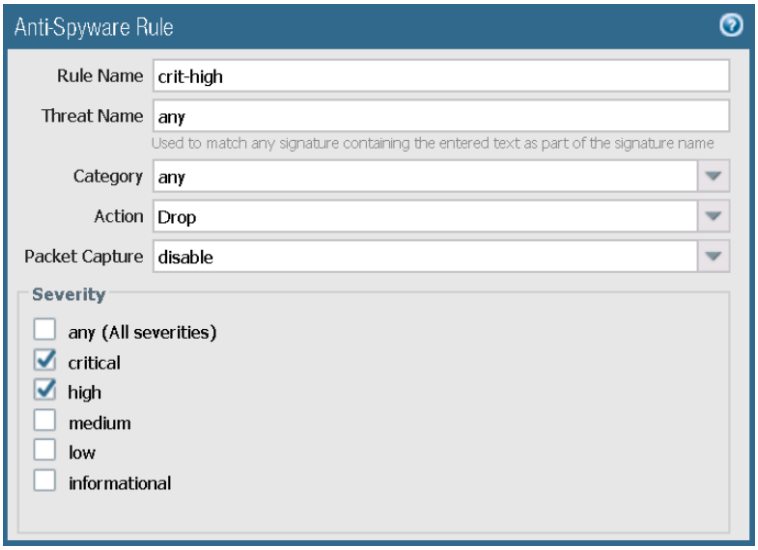
Anti-Spyware profiles block spyware on compromised hosts from trying to phone home or beacon out to external command-and-control (C2) servers, thus allowing you to detect malicious traffic leaving the network from infected clients.

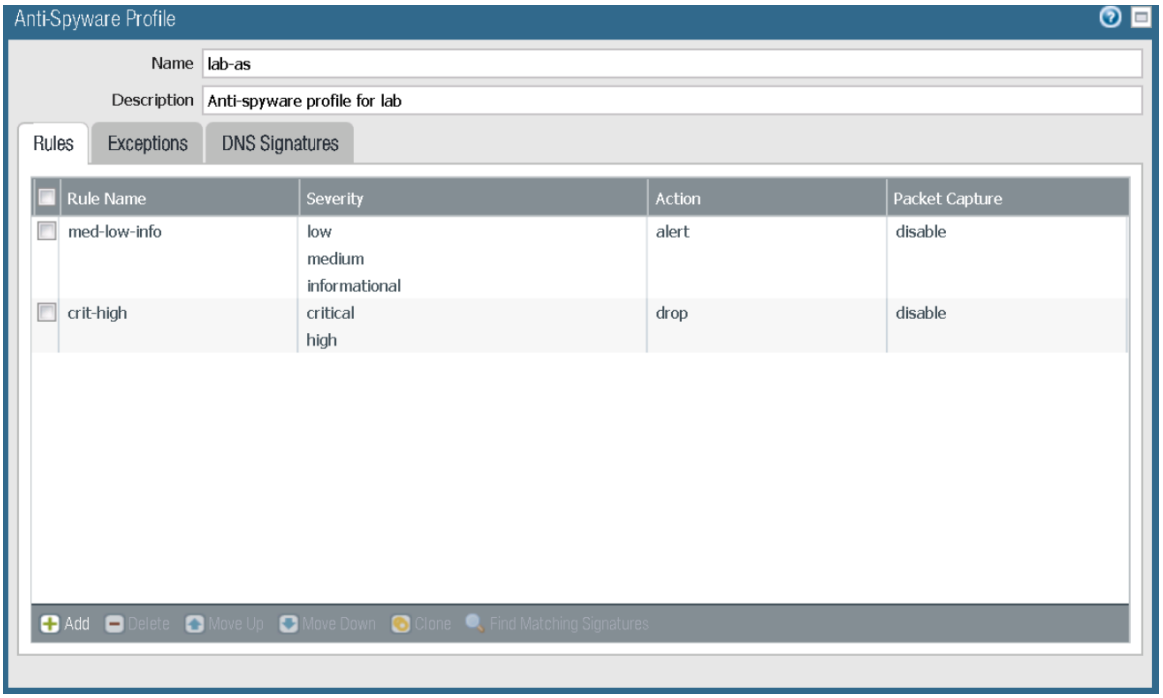
33. In the web interface, select **Objects** > **Security Profiles** > **Anti-Spyware**.
34. Click **Add** to create an Anti-Spyware Profile.

    An **Anti-Spyware Profile** configuration window should appear.

35. Configure the following:

Parameter	Value
Name	`lab-as`
Description	`Anti-spyware profile for lab`
Rules tab	Click **Add** and create a rule with these parameters: ▪ **Rule Name**: Type `med-low-info` ▪ **Action**: Select **Alert** from the drop-down list ▪ **Severity**: Select only the **medium**, **low**, and **informational** check boxes Click **OK** to save the rule.

Parameter	Value
	
Rules tab	Click **Add** and create another rule with these parameters: ▪ Rule Name: Type **`crit-high`** ▪ Action: Select **Drop** from the drop-down list ▪ Severity: Select only the **critical** and **high** check boxes Click **OK** to save the rule. 

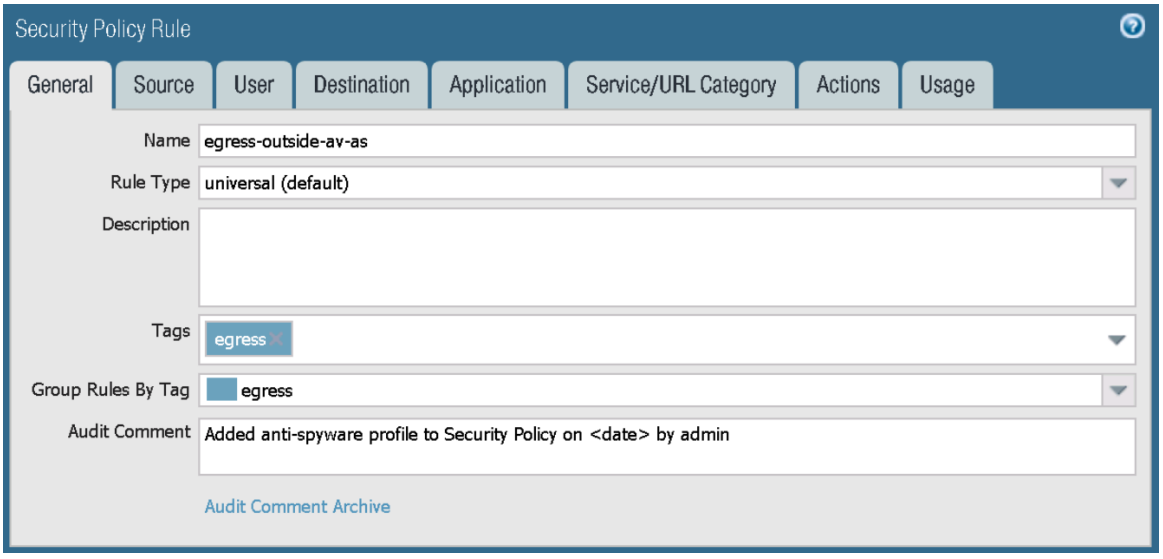


36. Click **OK** to close the **Anti-Spyware Profil**e configuration window.
37. Verify that your configuration is like the following:

Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture
default	Predefined	Rules: 4	simple-critical	any	critical	default	disable
			simple-high	any	high	default	disable
			simple-medium	any	medium	default	disable
			simple-low	any	low	default	disable
strict	Predefined	Rules: 5	simple-critical	any	critical	reset-both	disable
			simple-high	any	high	reset-both	disable
			simple-medium	any	medium	reset-both	disable
			simple-informational	any	informational	default	disable
			simple-low	any	low	default	disable
lab-as		Rules: 2	med-low-info	any	low,medium,inf...	alert	disable
			crit-high	any	critical,high	drop	disable

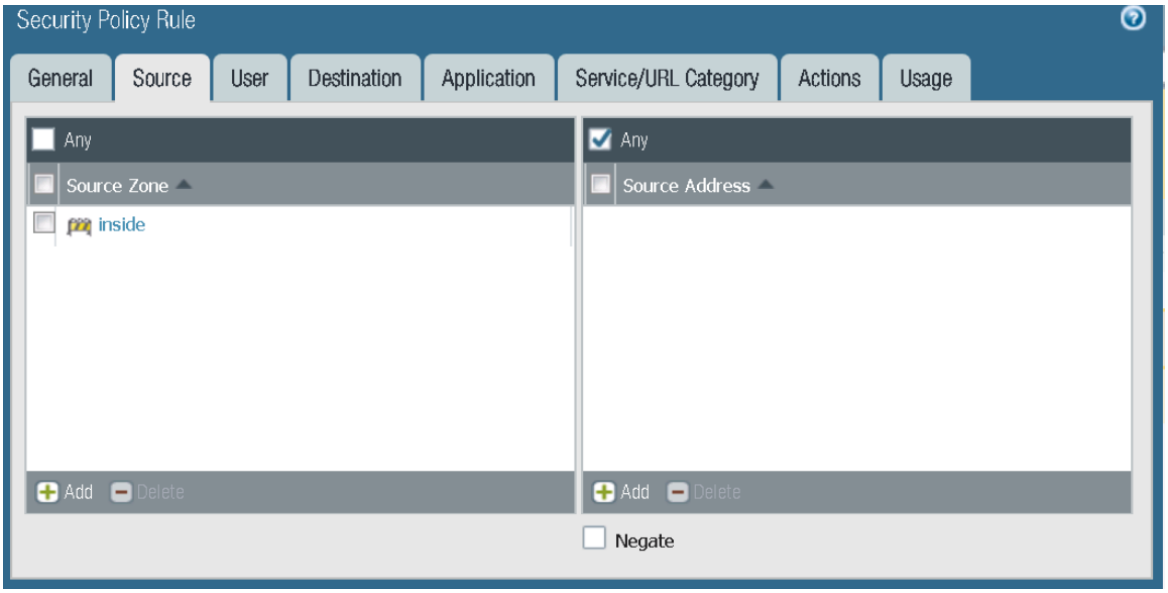
38. In the web interface, select **Policies** > **Security**.
39. Select the **egress-outside-av** Security policy rule.
    The **Security Policy Rule** configuration window should appear.
40. Configure the following:

Parameter	Value
Name	**Rename policy to `egress-outside-av-as`**
Audit Comment	**Type `Added anti-spyware profile to Security Policy on <date> by <Your-Role>`**



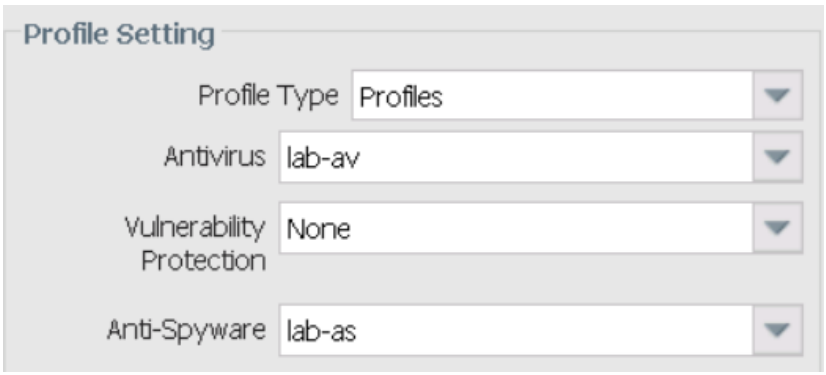
41. Verify that the **Source** tab is configured as follows:

Parameter	Value
Source Zone	Verify that **inside** is selected



42. Click the **Actions** tab and configure the following:

Parameter	Value
Profile Type	Verify that **Profiles** is selected
Anti-Spyware	Select **lab-as** from the drop-down list



43. Click **OK** to close the **Security Policy Rule** configuration window.
44. Verify that your configuration is like the following:

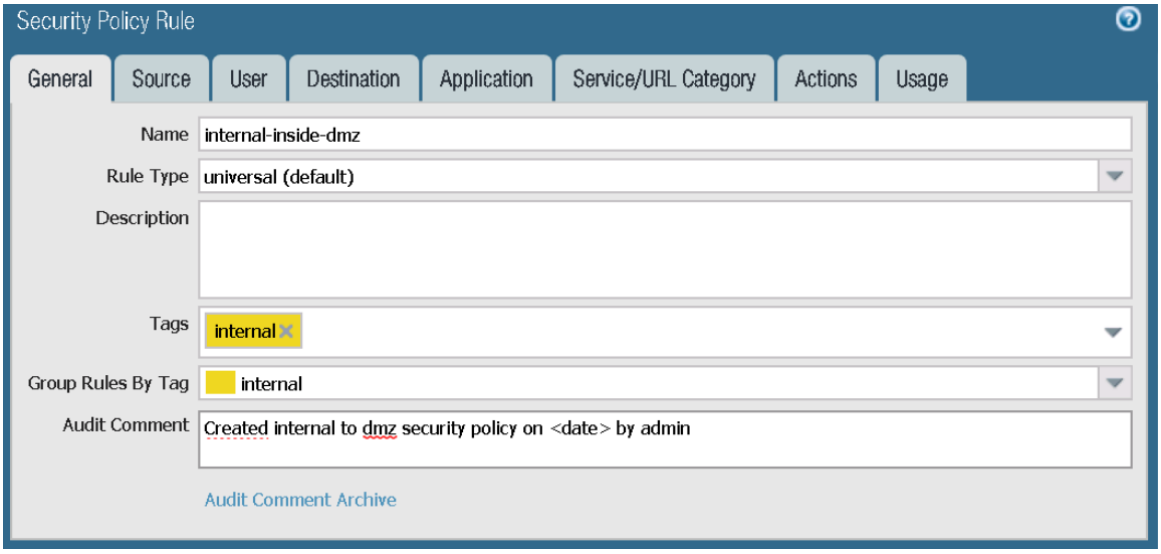
	Name	Tags	Type	Source				Destination		Application	Service	Action	Profile
				Zone	Addr...	Us...	HIP Pro...	Zone	Address				
1	egress-outside-as	egress	universal	inside	any	any	any	outside	any	any	application-default	Allow	
2	egress-outside	egress	universal	inside	any	any	any	outside	any	any	application-default	Allow	none
3	internal-dmz-ftp	internal	universal	inside	any	any	any	dmz	19...	ftp	application-default	Allow	none
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none
5	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none

1.5 Create a DMZ-Access Security Policy

In the next task, you will configure the firewall to download an External Dynamic List (EDL) of URLs from the DMZ server. You then will apply the EDL to the Anti-Spyware DNS Sinkhole configuration. Before the EDL and DNS Sinkhole configurations can work, you must create a Security policy that allows the management interface to connect to the DMZ server. The management interface establishes connections from the **inside** zone. The DMZ server responds to connection requests from the **dmz** zone.

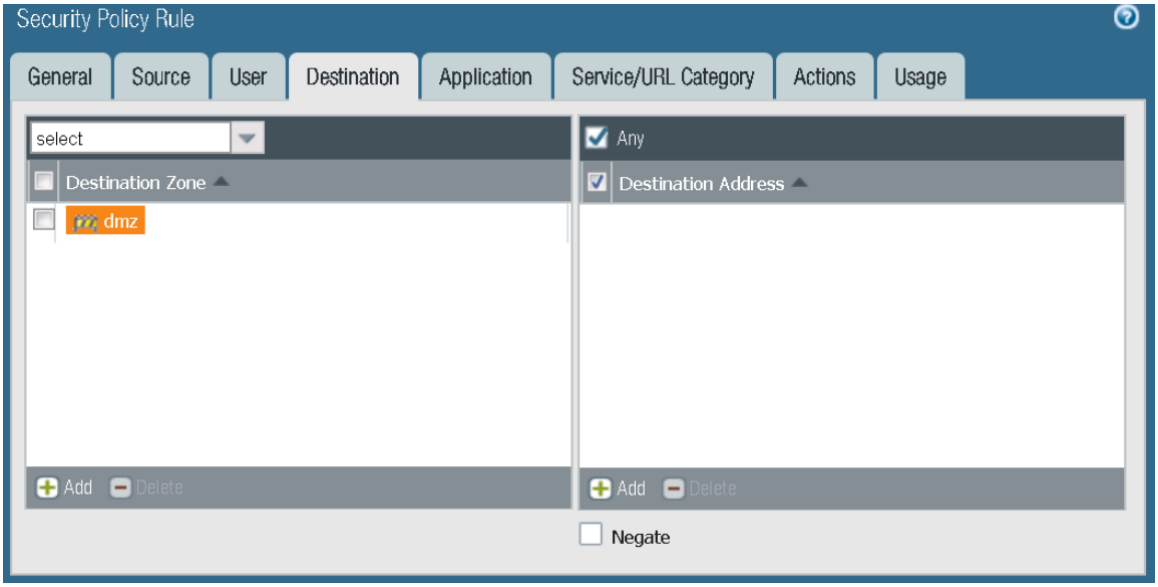
45. In the web interface, select the **internal-dmz-ftp** Security policy rule.
    The **Security Policy Rule** configuration window should appear.
46. Configure the following:

Parameter	Value
Name	**Rename the policy to `internal-inside-dmz`**
Audit Comment	Type **`Created internal to dmz security policy on <date> by <Your-Role>`**



47. Click the **Destination** tab and configure the following:

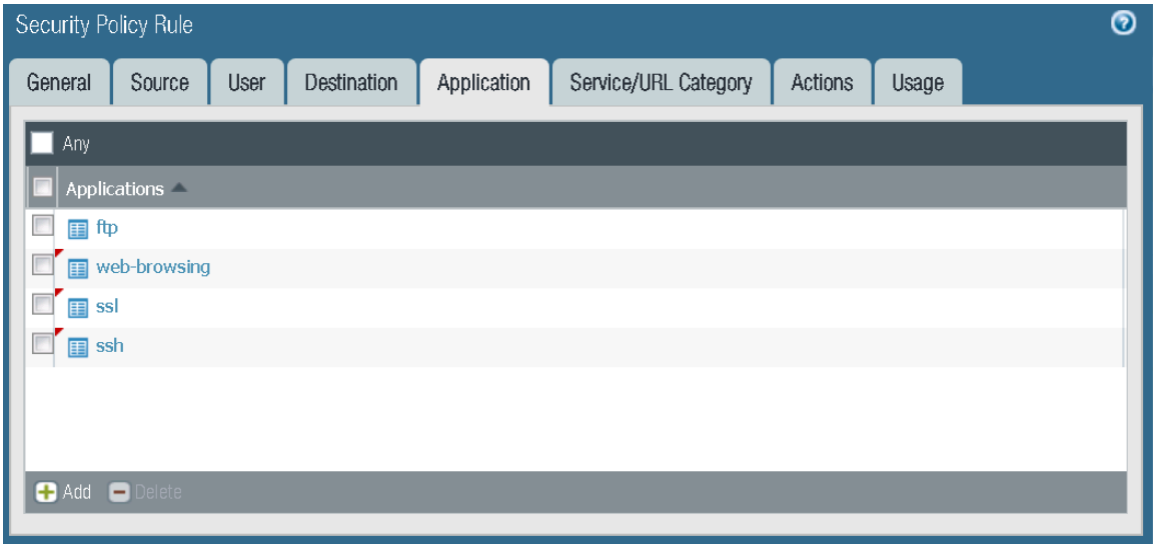
Parameter	Value
Destination Address	Select the **Destination Address** check box and click Delete
Destination Address	Verify that the **Any** check box is selected



48. Click the **Application** tab and configure the following:

Parameter	Value
Applications	**Click Add and select the following from the drop-down list:** **`ftp`**

Parameter	Value
	web-browsing **ssl** **ssh**



49. Click **OK** to close the **Security Policy Rule** configuration window.
50. Verify that your configuration is like the following:

	Name	Tags	Type	Source				Destination		Application	Service	Action	Profile
				Zone	Addr...	Us...	HIP Pro...	Zone	Address				
1	egress-outside-as	egress	universal	inside	any	any	any	outside	any	any	application-default	Allow	
2	egress-outside	egress	universal	inside	any	any	any	outside	any	any	application-default	Allow	none
3	internal-inside-dmz	internal	universal	inside	any	any	any	dmz	any	ftp ssh ssl web-...	application-default	Allow	none

51. In the web interface, select **Policies** > **NAT**.
52. Select the **destination-dmz-ftp** NAT policy rule without opening it.
53. Click **Disable**.
54. Verify that your configuration is like the following:

	Name	Tags	Original Packet						Translated Packet	
			Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	source-egress-outside	egress	inside	outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 203.0.113.20/24	none
2	destination-dmz-ftp	internal	inside	inside	ethernet1/2	any	192.168.1.1	service-ftp	none	destination-translation address: 192.168.50.10

55. **Commit** all changes.

1.6 Configure a DNS-Sinkhole External Dynamic List

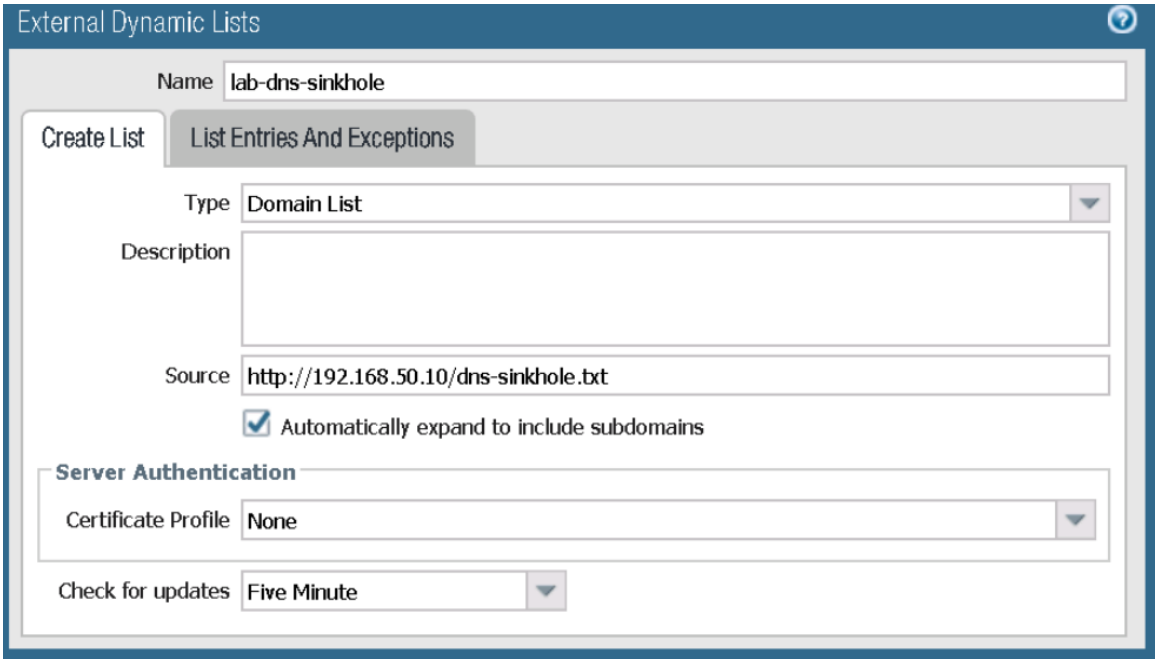
An EDL is an object that references an external list of IP addresses, URLs, or domain names that can be used in policy rules. You must create this list as a text file and save it to a web server that the firewall can access. By default, the firewall uses its management port to retrieve the list items.

56. In the web interface, select **Objects > External Dynamic Lists**.
57. Click **Add** to configure a new EDL.

    The **External Dynamic Lists** configuration window should appear.
58. Configure the following:

Parameter	Value
Name	**Type `lab-dns-sinkhole`**
Type	Select **Domain List** from the drop-down list
Source	**Type `http://192.168.50.10/dns-sinkhole.txt`** (This sinkhole file is hosted on the DMZ server.)
Automatically expand to include subdomains	**Select the check box**
Check for updates	Select **Five Minute** from the drop-down list

Note: This list currently contains "reddit.com" only.

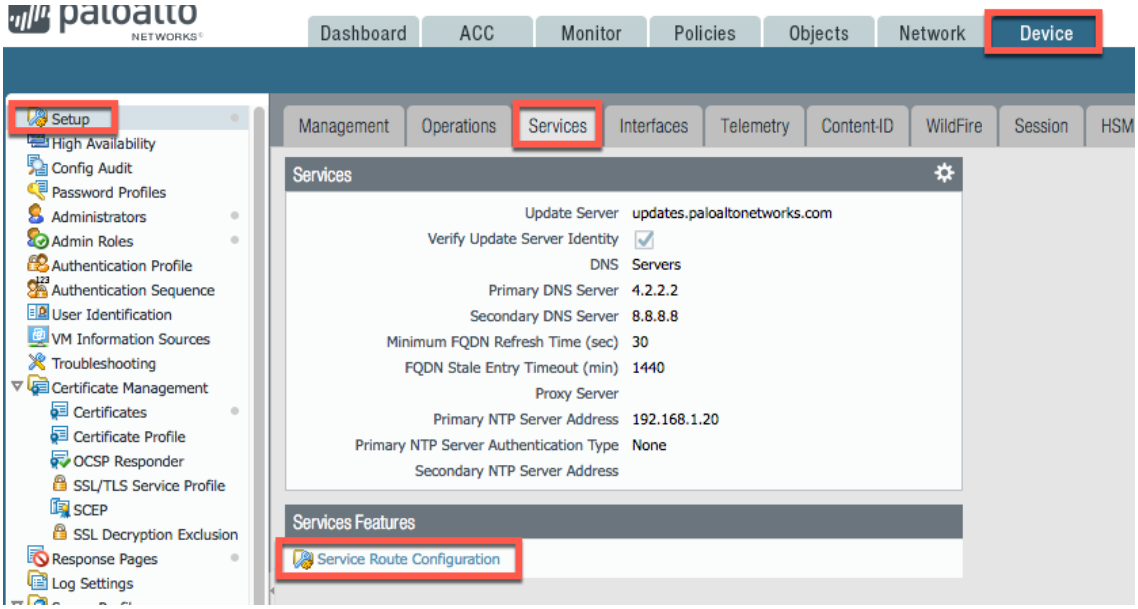


59. Click **OK** to close the External Dynamic Lists configuration window.

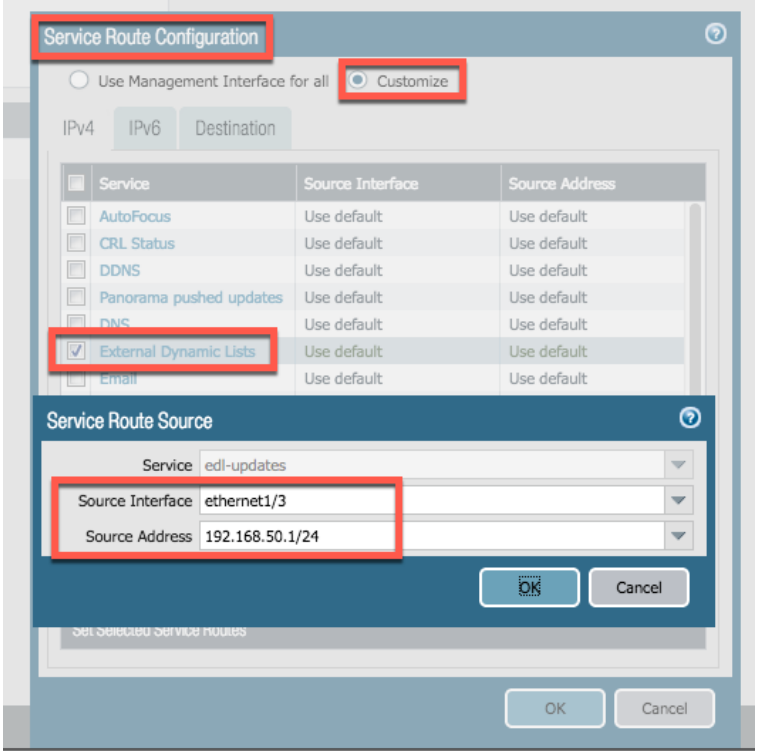
60. Verify that your configuration is like the following:

Name	Location	Description	Source	Certificate Profile	Frequency
Dynamic IP Lists					
Palo Alto Networks - High risk IP addresses	Predefined	High risk IP addresses, shared IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations, however Palo Alto Networks does not have direct evidence of maliciousness	Palo Alto Networks - High risk IP addresses		
Palo Alto Networks - Known malicious IP addresses	Predefined	Malicious IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, or for launching various attacks	Palo Alto Networks - Known malicious IP addresses		
Dynamic Domain Lists					
lab-dns-sinkhole			http://192.168.50.10/dns-sinkhole.txt	None	Five Minute

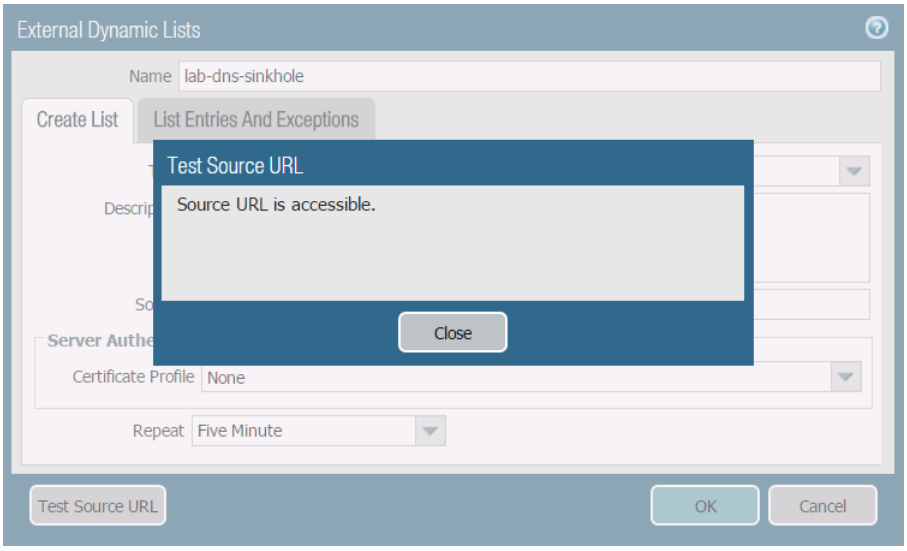
61. In the Web-UI, navigate to Device tab>Setup>Services tab and under Service Features click **Service Route Configuration.**



62. In the **Service Route Configuration** dialog box, select radial dial for **Customize**, select **External Dynamic Lists**. In the **Service Route Source** dialog box select **Source Interface** ethernet1/3 and **Source Address** 192.168.50.1/24.



63. **Click "OK" twice and Commit** all changes.
64. Open the **`lab-dns-sinkhole`** configuration you just created and click **Test Source URL**:



Confirm that the firewall reports that the "Source URL is accessible" and click **Close**. If the firewall reports a "URL access error," check the source address, correct any errors, and rerun the test.

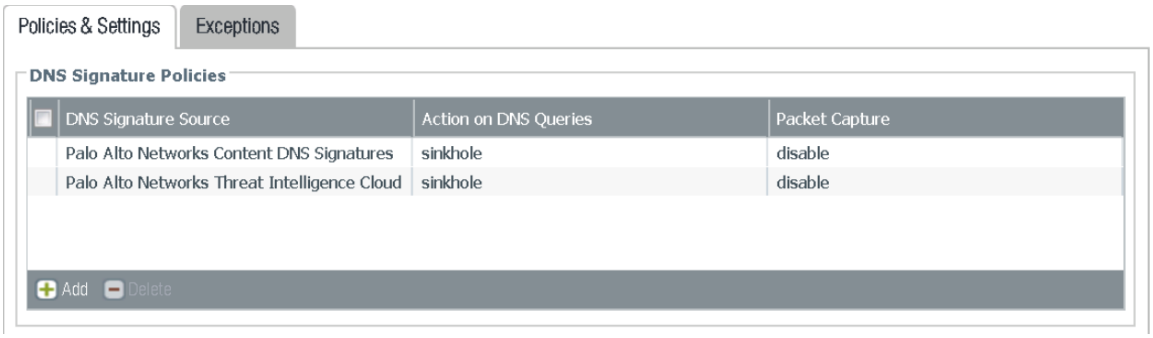
65. Click **Close** to close the **Test Source URL** dialog box.
66. Click **Cancel** to close the **External Dynamic Lists** configuration window.

1.7 Create an Anti-Spyware Profile with DNS Sinkhole

The DNS Sinkhole action provides administrators with a method of identifying infected hosts on the network using DNS traffic, even when the firewall cannot see the originator of the DNS query because the DNS server is not on the internal network.

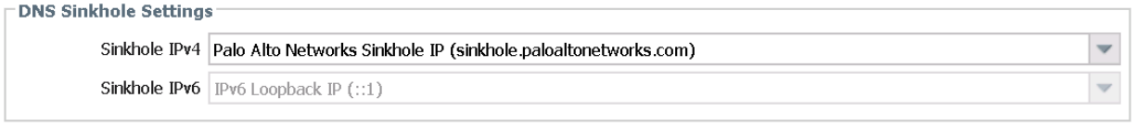
67. In the web interface, select **Objects > Security Profiles > Anti-Spyware**.
68. Click lab-as to open the Anti-Spyware Profile.

    The **Anti-Spyware Profile** configuration window should appear.
69. Click the **DNS Signatures** tab.
70. Locate the **DNS Signature Source** box and click **Add.**



71. Select lab-dns-sinkhole from the drop-down list.
72. Verify that the **Action on DNS Queries** is set to **sinkhole**:

73. Verify that the **Sinkhole IPv4** is set to **Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)** in the **DNS Sinkhole Settings** box.



74. Click **OK** to close the **Anti-Spyware Profile** configuration window.
75. **Commit** all changes.

1.8 Test the Security Policy Rule

76. From the Windows desktop, open a **CMD** window.
77. Type the **`nslookup`** command and press the **Enter** key.
78. Type the command **`server 8.8.8.8`** and press **Enter**:

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>nslookup
Default Server:  localhost
Address:  127.0.0.1

> server 8.8.8.8
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8
```

79. At the **`nslookup,`** type **`reddit.com`**. and press the **Enter** key:

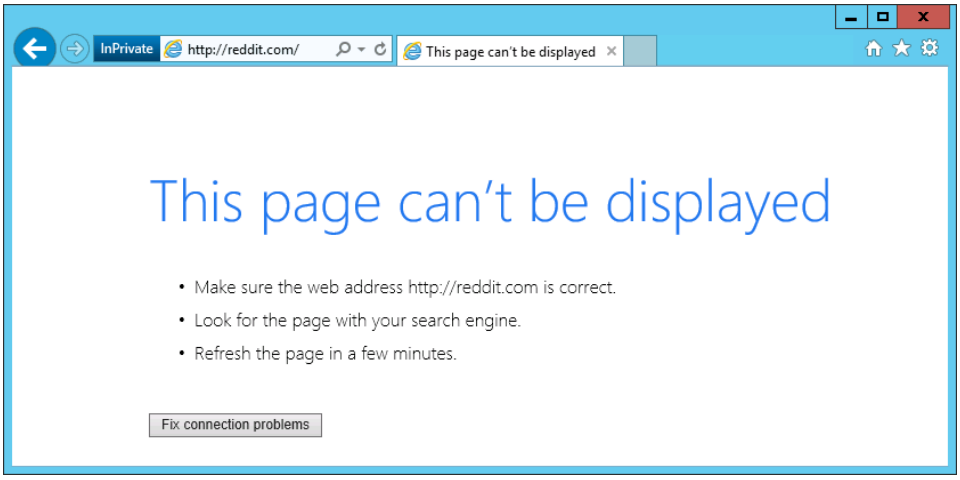
```
> reddit.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    reddit.com

> _
```

Notice that the reply for reddit.com does not display an IP address. The request has been sinkholed.

80. Type **`exit`** and press **Enter** to exit **`nslookup`**.
81. Type **`exit`** and press **Enter** again to exit the command-prompt window.
82. On your desktop, open a new Internet Explorer browser window in private/incognito mode and browse to **`http://reddit.com`**. Wait for the connection to time out.



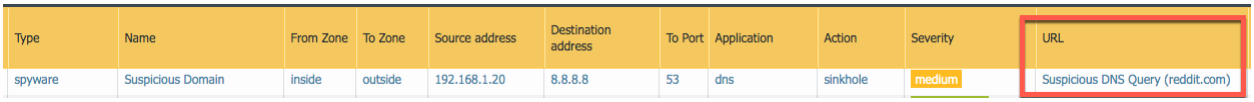
Note: Make sure that you do *not* include "**`www.`**" in the URL, because "www.reddit.com" is not in the EDL; "reddit.com" is currently the only entry in the list.

83. Close the browser window.

1.9 Review the Logs

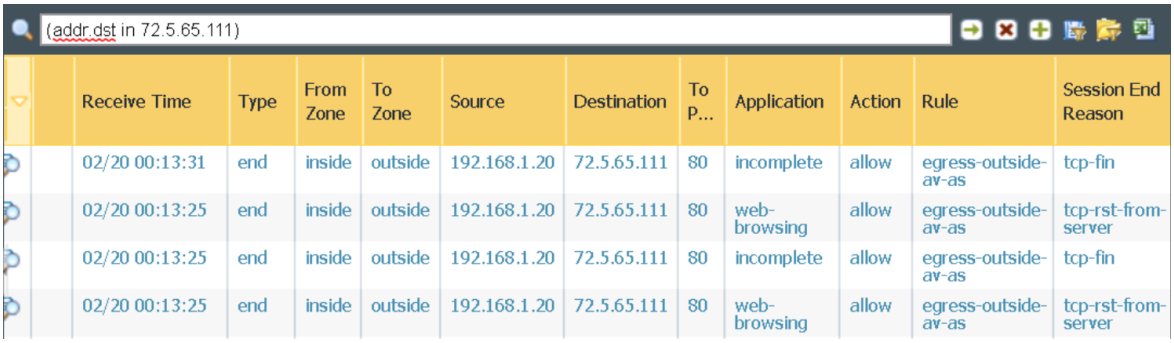
84. In the web interface, select **Monitor > Logs > Threat**.
85. Identify the **Suspicious Domain** log entry:

    Notice that the action is **sinkhole** and that the **URL** column includes the DNS FQDN that was queried (reddit.com).



Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity	URL
spyware	Suspicious Domain	inside	outside	192.168.1.20	8.8.8.8	53	dns	sinkhole	medium	Suspicious DNS Query (reddit.com)

86. In the web interface, select **Monitor > Logs > Traffic**.
87. Type the following filter statement **`(addr.dst in 72.5.65.111)`** and press **Enter**:

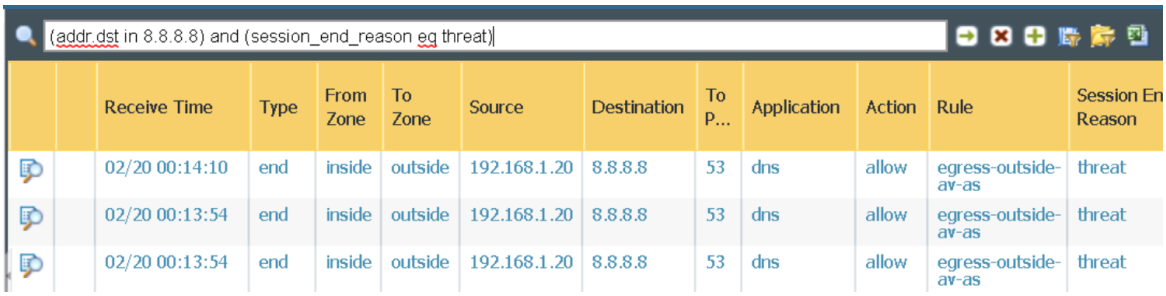


(addr.dst in 72.5.65.111)

Receive Time	Type	From Zone	To Zone	Source	Destination	To P...	Application	Action	Rule	Session End Reason
02/20 00:13:31	end	inside	outside	192.168.1.20	72.5.65.111	80	incomplete	allow	egress-outside-av-as	tcp-fin
02/20 00:13:25	end	inside	outside	192.168.1.20	72.5.65.111	80	web-browsing	allow	egress-outside-av-as	tcp-rst-from-server
02/20 00:13:25	end	inside	outside	192.168.1.20	72.5.65.111	80	incomplete	allow	egress-outside-av-as	tcp-fin
02/20 00:13:25	end	inside	outside	192.168.1.20	72.5.65.111	80	web-browsing	allow	egress-outside-av-as	tcp-rst-from-server

Notice that the **Application** type is "incomplete." This result occurs because the sinkhole address does not reply to the connection attempt made by the browser to reach reddit.com. The browser attempts to connect to the sinkhole address because the firewall is blocking the original DNS request. The firewall then returns a firewall-generated DNS reply that tells the browser that reddit.com is located at the sinkhole address.

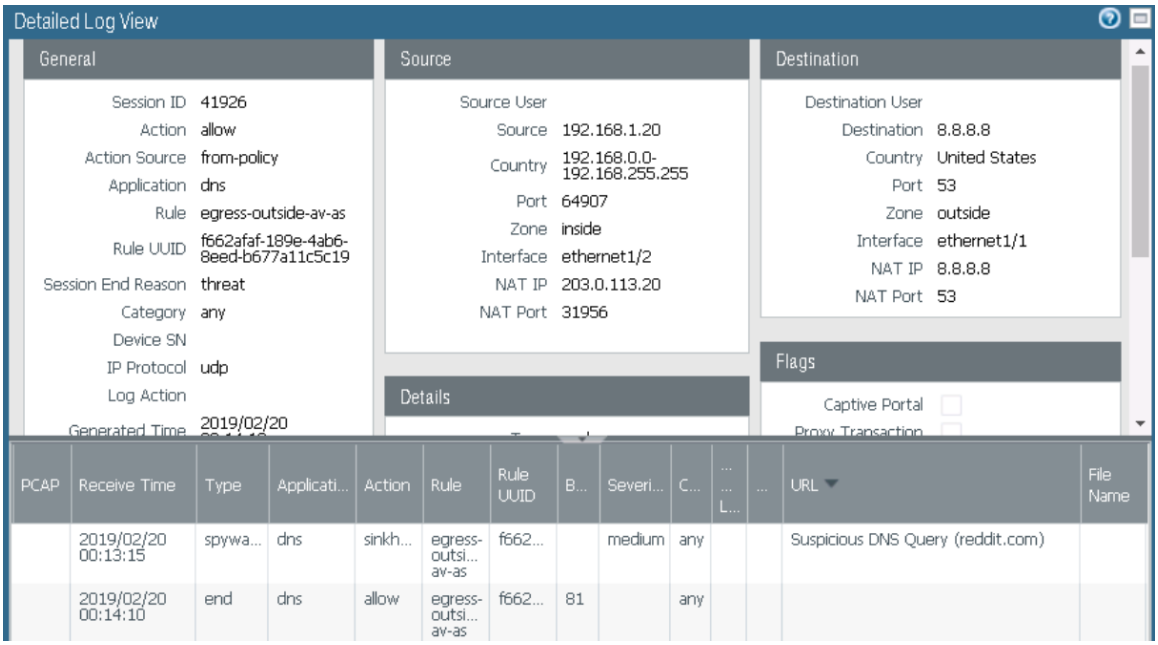
88. To find the original DNS request in the Traffic log, use the following filter statement **`(addr.dst in 8.8.8.8) and (session_end_reason eq threat)`**:



(addr.dst in 8.8.8.8) and (session_end_reason eq threat)

Receive Time	Type	From Zone	To Zone	Source	Destination	To P...	Application	Action	Rule	Session En Reason
02/20 00:14:10	end	inside	outside	192.168.1.20	8.8.8.8	53	dns	allow	egress-outside-av-as	threat
02/20 00:13:54	end	inside	outside	192.168.1.20	8.8.8.8	53	dns	allow	egress-outside-av-as	threat
02/20 00:13:54	end	inside	outside	192.168.1.20	8.8.8.8	53	dns	allow	egress-outside-av-as	threat

89. Click the **magnifying glass** icon  next to one of the entries to see the **Detailed Log View**:



In the **Detailed Log View**, you should notice the additional information that matches what you previously viewed in the Threat log. Next, scroll down and review the information in the **Details** section in the middle column of the main display area. Notice that the traffic log records only one packet. This packet is the original DNS query sent from the client. The DNS response packet with the sinkhole address is sent directly from the firewall itself.

90. Click **Close** to close the **Detailed Log View** window.

1.10 Create a 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.

91. In the web interface, select **Objects > Security Profiles > Vulnerability Protection**.
92. Click **Add** to create a Vulnerability Protection Profile.

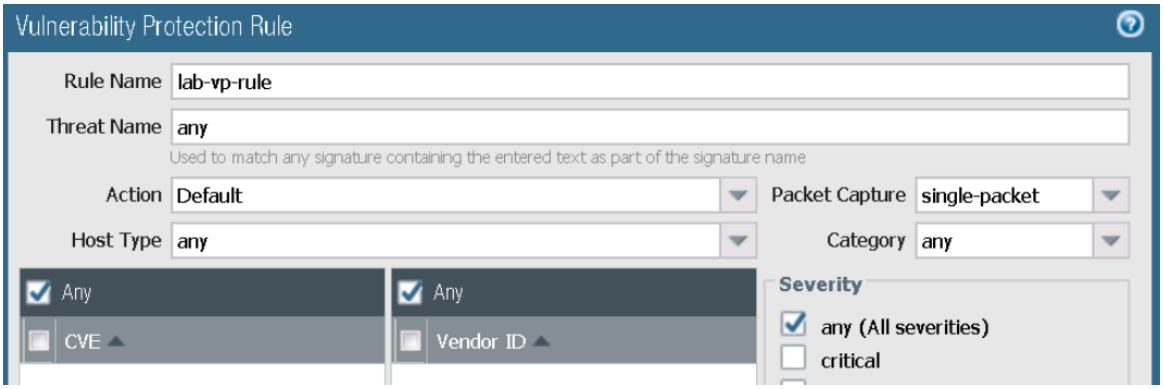
    The **Vulnerability Protection Profile** configuration window should appear.

93. Configure the following:

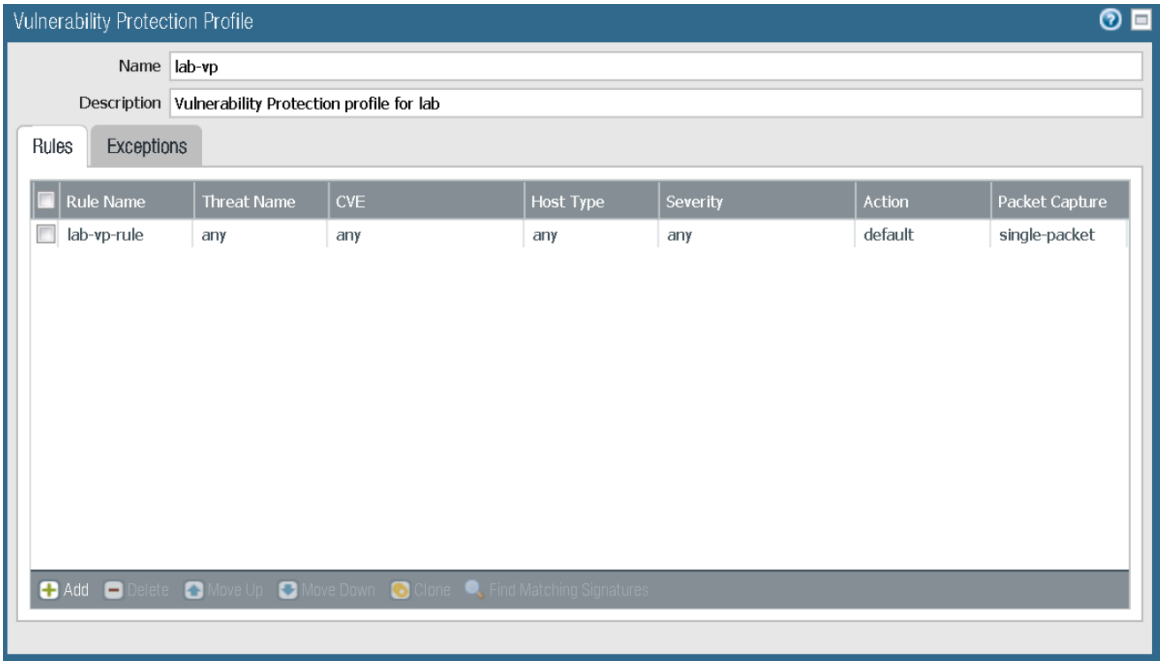
Parameter	Value
Name	**Type `lab-vp`**
Description	**Type `Vulnerability Protection profile for lab`**

94. On the **Rules** tab, click **Add** to create a rule.
    The **Vulnerability Protection Rule** configuration window should appear.
95. Configure the following:

Parameter	Value
Name	**Type `lab-vp-rule`**
Packet Capture	Select **single-packet** from the drop-down list
Severity	Verify that the **any (All severities)** check box is selected



96. Click **OK** to close the **Vulnerability Protection Rule** window:

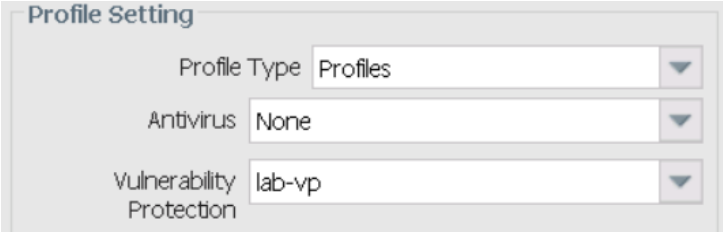


97. Click **OK** to close the **Vulnerability Protection Profile** window.
98. In the web interface, select **Policies > Security**.
99. Click to open the internal-inside-dmz Security policy rule.

The **Security Policy Rule** configuration window should appear.

100. Click the **Actions** tab and configure the following:

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



101. Click **OK** to close the **Security Policy Rule** configuration window.
102. **Commit** all changes.

1.11 Test the Security Policy Rule

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

Note: 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***.

```
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 2018-12-17 21:34 Coordinated Universa
l Time
Nmap scan report for test.lab (192.168.50.10)
Host is up (0.0020s latency).
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 1245 guesses in 604 seconds, average tps: 2.0

Nmap done: 1 IP address (1 host up) scanned in 605.96 seconds

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

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

1.12 Review the Logs

107. In the web interface, select **Monitor** > **Logs** > **Threat**.

Notice that you now have logs reflecting the FTP brute force attempt. However, the firewall is set only to alert:

		Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity
		02/20 00:34:05	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	alert	high
		02/20 00:34:05	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	alert	high
		02/20 00:34:05	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	alert	high
		02/20 00:34:05	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	alert	high

108. Open the **Detailed Log View** by clicking the icon.

109. From the **Detailed Log View**, click the icon to open the packet capture.

Notice the username and password that were attempted, along with the 530 responses from the FTP server.

Packet Capture

```
05:35:43.000000 00:0c:29:45:a2:c6 > 00:50:56:b0:2a:bc, ethertype IPv4 (0x0800), lengt
        0x0000:  0050 56b0 2abc 000c 2945 a2c6 0800 4500  .PV.*...)E....E.
        0x0010:  0041 e842 4000 4006 0000 c0a8 0114 c0a8  .A.B@.@.........
        0x0020:  320a 40ed 0015 ad95 eccb 0142 cd9b 5018  2.@........B..P.
        0x0030:  01c9 0000 0000 5553 4552 2077 6562 0d0a  ......USER.web..
        0x0040:  5041 5353 206d 6172 6970 6f73 610d 0a    PASS.mariposa..
05:35:43.000000 00:50:56:b0:2a:bc > 00:0c:29:45:a2:c6, ethertype IPv4 (0x0800), lengt
        0x0000:  000c 2945 a2c6 0050 56b0 2abc 0800 4500  ..)E...PV.*...E.
        0x0010:  004b e842 4000 4006 9e08 c0a8 320a c0a8  .K.B@.@.....2...
        0x0020:  0114 0015 40ed 0142 cd78 ad95 ece4 5018  ....@..B.x....P.
        0x0030:  01c9 0000 0000 0a33 3331 2050 6c65 6173  .......331.Pleas
        0x0040:  6520 7370 6563 6966 7920 7468 6520 2d20  e.specify.the.-.
        0x0050:  4733 006e 2065 4261 79                   G3.n.eBay
05:35:43.000000 00:50:56:b0:2a:bc > 00:0c:29:45:a2:c6, ethertype IPv4 (0x0800), lengt
        0x0000:  000c 2945 a2c6 0050 56b0 2abc 0800 4500  ..)E...PV.*...E.
        0x0010:  003e e842 4000 4006 9e08 c0a8 320a c0a8  .>.B@.@.....2...
        0x0020:  0114 0015 40ed 0142 cd9b ad95 ece4 5018  ....@..B......P.
        0x0030:  01c9 a1eb 0000 3533 3020 4c6f 6769 6e20  ......530.Login.
        0x0040:  696e 636f 7272 6563 742e 0d0a            incorrect...
```

110. After viewing the pcap, click **Close** to close the **Packet Capture** window.

111. Click **Close** to close the **Detailed Log View** window.

1.13 Update the Vulnerability Profile

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

113. Click **lab-vp** to open the profile.

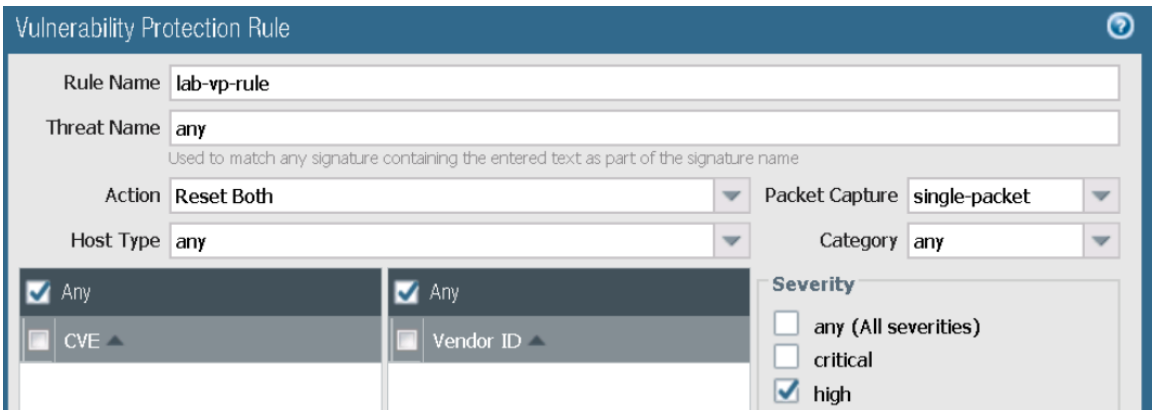
The **Vulnerability Protection Profile** configuration window should appear.

114. Click **lab-vp-rule** to open the rule.

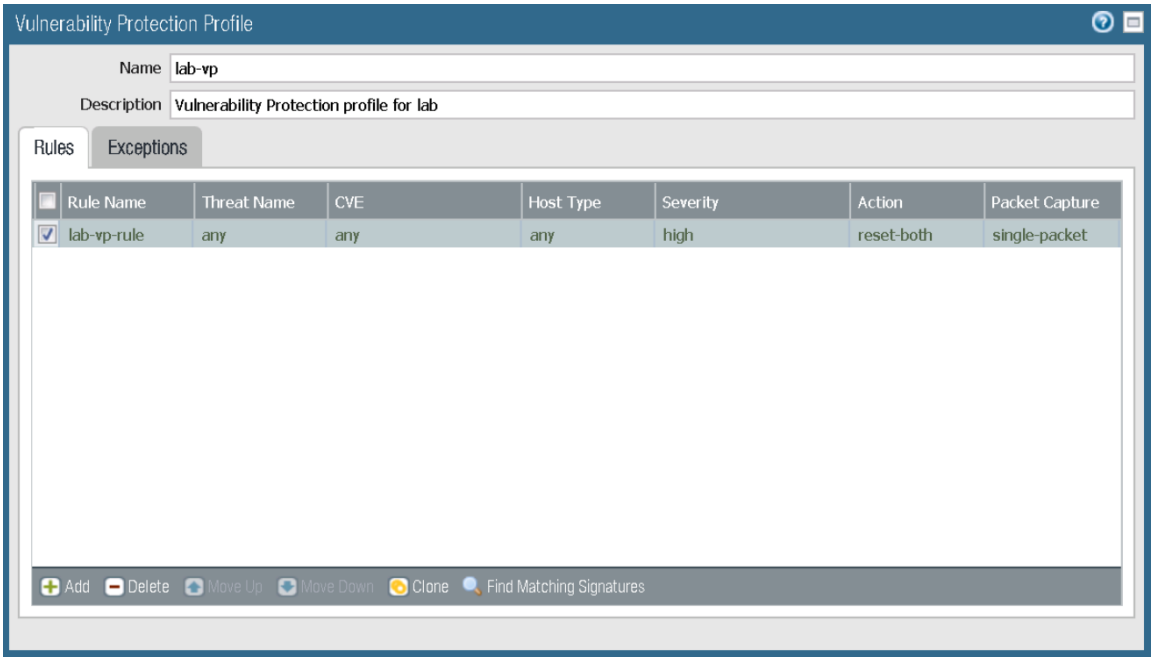
The **Vulnerability Protection Rule** configuration window should appear.

115. Configure the following:

Parameter	Value
Action	Select the **Reset Both** from the drop-down list
Severity	Select the **high** check box



116. Click **OK** to close the **Vulnerability Protection Rule** window:



117. Click **OK** to close the **Vulnerability Protection Profile** window.
118. **Commit** all changes.
119. Rerun **ftp-brute.bat** and review the logs to confirm that the new FTP brute force attempts are reset.

		Receive Time	Decryp...	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Ap...	Action	Severity
		12/17 21:59:57	no	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	reset-both	high
		12/17 21:59:57	no	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	reset-both	high
		12/17 21:59:57	no	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	reset-both	high

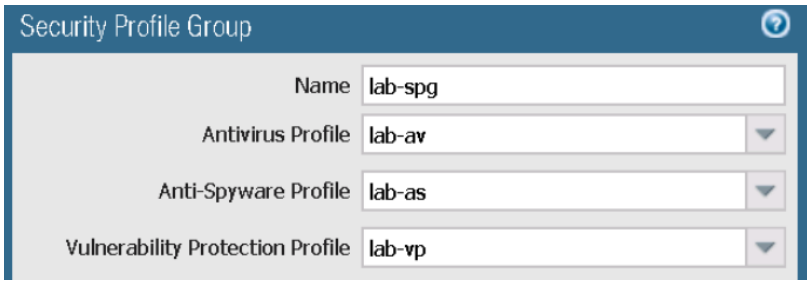
Note: This action launches an FTP brute force attack at the DMZ FTP server. After one minute, you can press **Ctrl+C** to terminate the batch file because sufficient log data will have been collected. The entire script should take about ***10 minutes to complete***.

1.14 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.

120. In the web interface, select **Objects > Security Profile Groups**.
121. Click **Add** to create a **Security Profile Group**.

    The **Security Profile Group** configuration window should appear.
122. Configure the following:

Parameter	Value
Name	**Type `lab-spg`**
Profiles	

123. Click **OK** to close the **Security Profile Group** window.

    The new Security Profile Group now should be listed.
124. In the web interface, select **Policies > Security**.
125. Delete the following rule:

Parameter	Value
Security Policy Rules	**egress-outside-av-as**

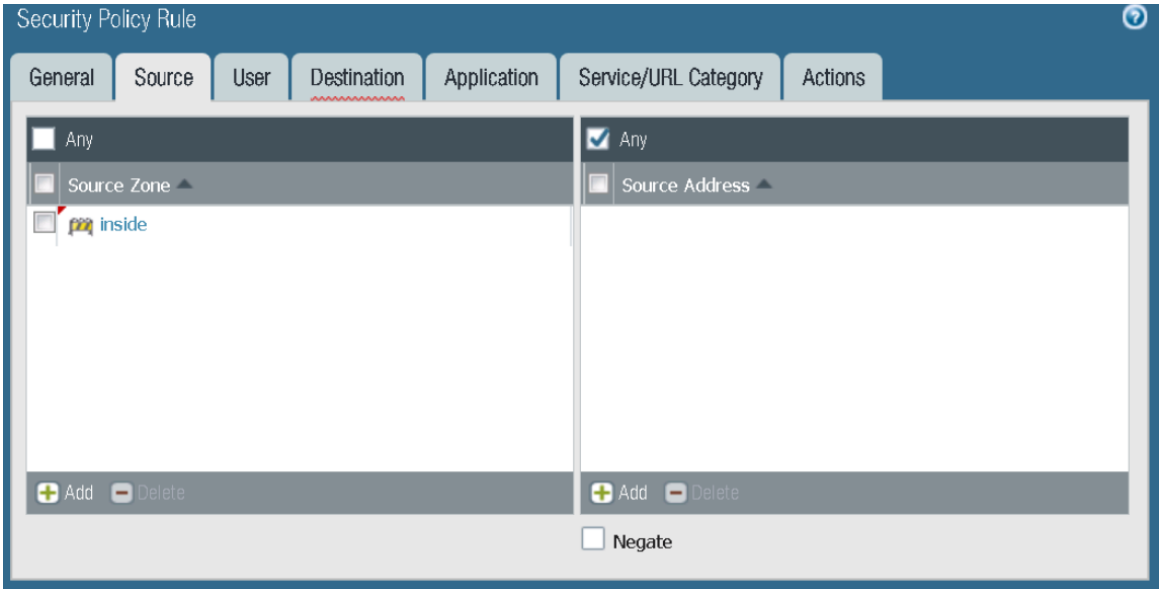
126. Click **Add** to define a new **Security policy rule**.

    The **Security Profile Rule** configuration window should appear.
127. 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 <Your-Role>`

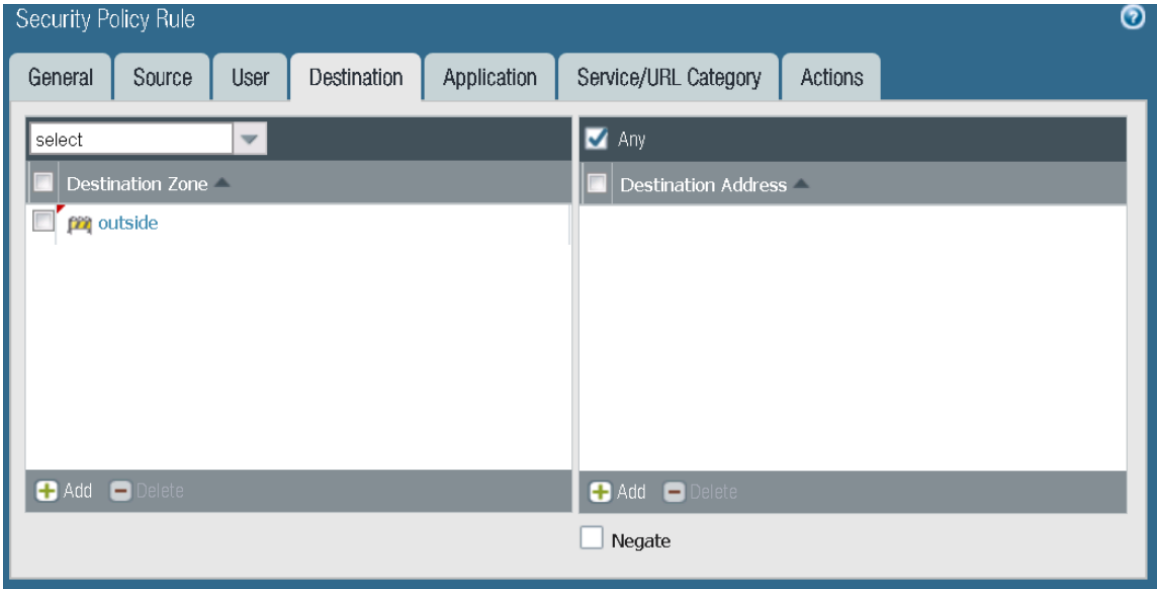
128. Click the **Source** tab and configure the following:

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



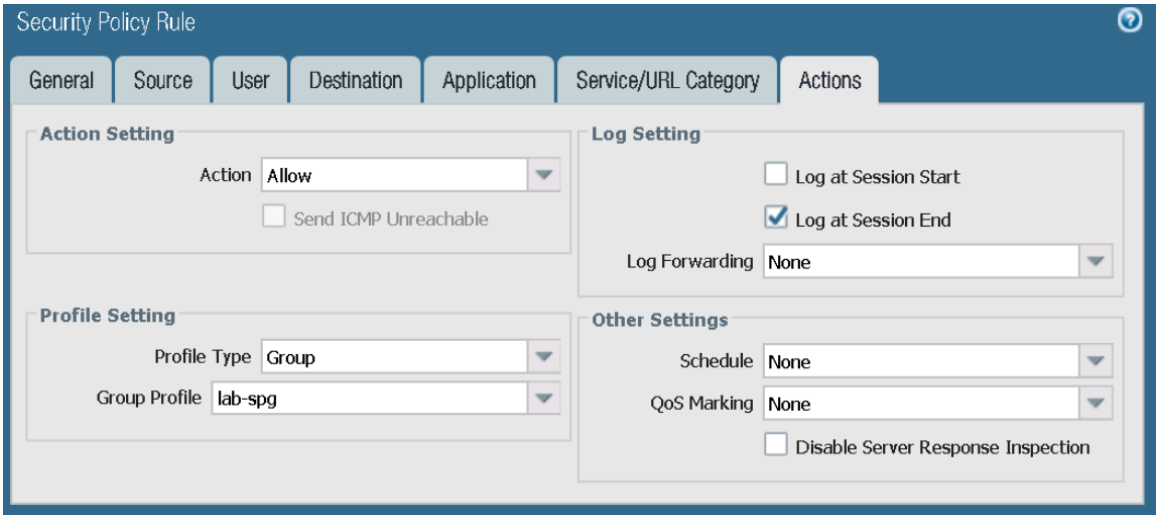
129. Click the **Destination** tab and configure the following:

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



130. Click the **Application** tab and verify that the **Any** check box is selected.
131. Click the **Service/URL Category** tab and verify that **application-default** is selected.
132. Click the **Actions** tab and configure the following:

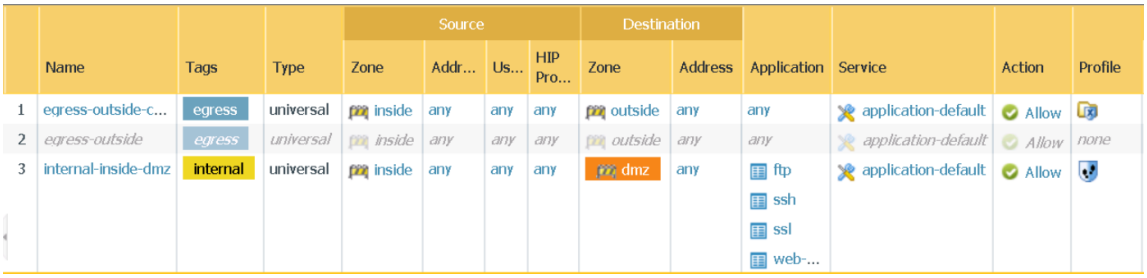
Parameter	Value
Action Setting	Verify that **Allow** is selected
Log Setting	Verify that **Log at Session End** is selected
Profile Type	**Select Group from the drop-down list**
Group Profile	**Select lab-spg from the drop-down list**



133. Click **OK** to close the **Security Policy Rule** configuration window.

The new Security Policy Rule now should be listed.

134. Verify that your configuration is like the following:



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 it and move the rule to the top of the list:

1.15 Create a File Blocking Profile

A Security policy rule can include specification 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.

135. In the web interface, select **Objects** > **Security Profiles** > **File Blocking**.
136. Click **Add** to open the **File Blocking Profile** configuration window.

    The **File Blocking Profile** configuration window should appear.

137. Configure the following:

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

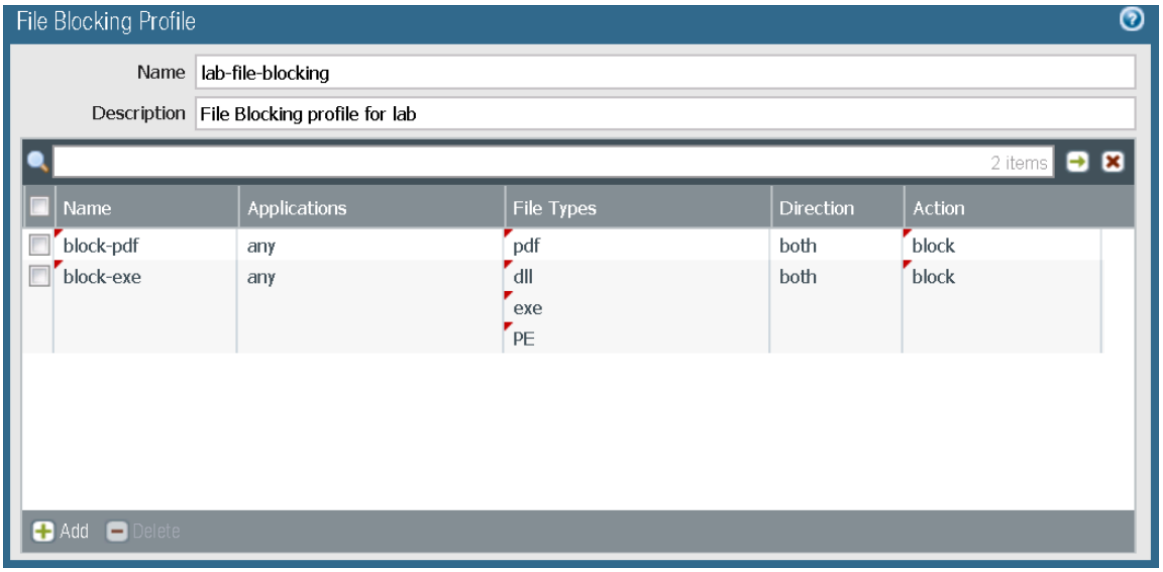
138. Click **Add** and configure the following.

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

139. Click **Add** and configure the following:

Parameter	Value
Name	Type **`block-exe`**
Applications	Verify that **any** is selected

Parameter	Value
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



140. Click **OK** to close the **File Blocking Profile** configuration window.

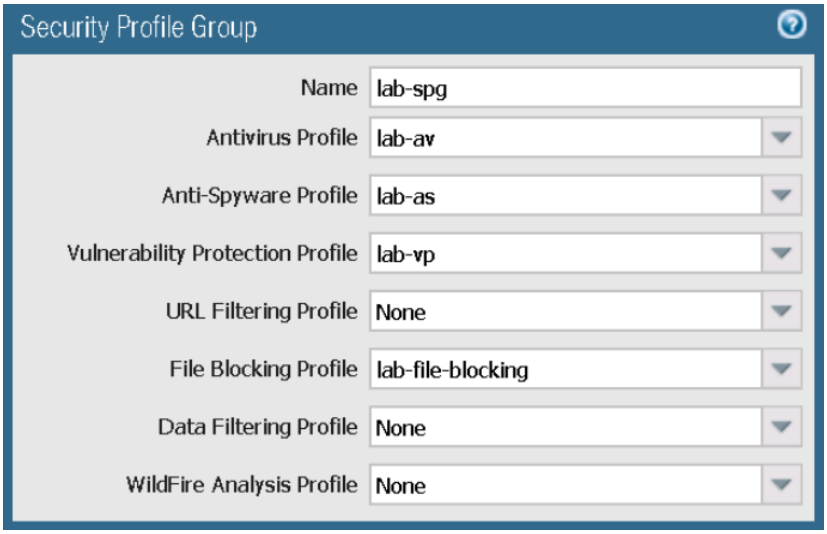
The new File Blocking Profile now should be listed.

1.16 Modify a Security Profile Group

141. In the web interface, select **Objects > Security Profile Groups**.
142. Click **lab-spg** to open the Security Profile Group.

The **Security Profile Group** configuration window should appear.

143. Add the newly created File Blocking Profile:



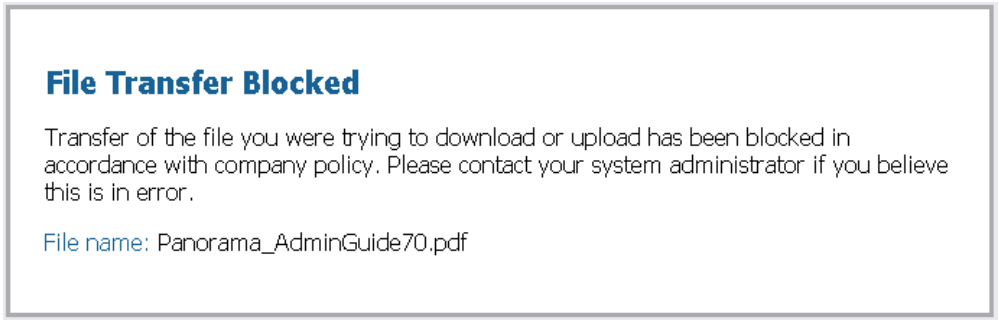
144. Click **OK** to close the **Security Profile Group** configuration window.
145. **Commit** all changes.

1.17 Test the File Blocking Profile

146. On your desktop, open a new browser window in private/incognito mode and browse to **`http://www.panedufiles.com/`**.

    Note: Some updates to Google Chrome may allow the files to be successfully downloaded. If the files are not blocked, then use a different browser such as IE or Firefox, or do not open Google Chrome in incognito mode.

147. Click the **Panorama_AdminGuide.pdf** link. The download fails:



    Note: If you get "failed to download pdf" and not the block page, then refresh the browser window.

148. Close the browser window.
149. In the web interface, select **Monitor > Logs > Data Filtering**.
150. Find the log entry for the PDF file that has been blocked:

Receive Time	Ca...	File Name	Name	From Zone	To Zone	Source address	Destination address	To Port	Application	Action
02/20 00:47:54	any	Panorama_AdminGuide...	Adobe Portable Document Format (PDF)	inside	outside	192.168.1.20	67.195.197.75	80	web-browsing	deny

Note: The **Action** column is located on the far right. You can move the column by using the mouse cursor to drag-and-drop it.

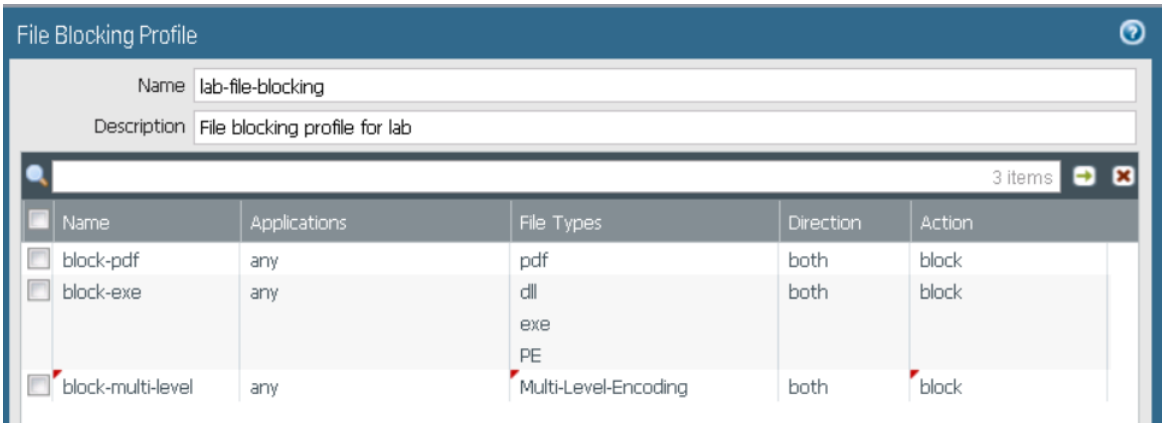
1.18 Create a File Blocking Profile to Block Multi-Level Encoded Files

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.

151. In the web interface, select **Objects** > **Security Profiles** > **File Blocking**.
152. Click **lab-file-blocking** to open the File Blocking Profile.

    The **File Blocking Profile** configuration window should appear.
153. Click **Add** and configure the following:

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



154. Click **OK** to close the **File Blocking Profile** configuration window.

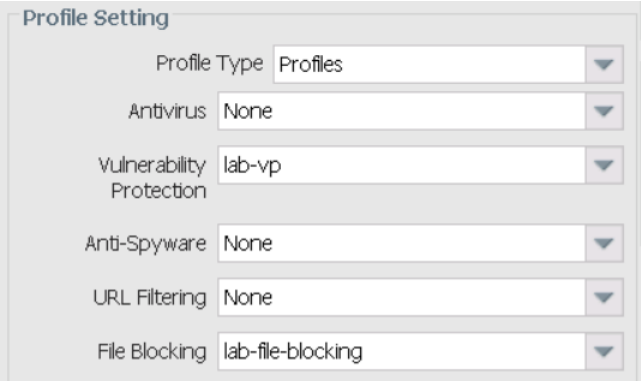
1.19 Modify the Security Policy Rule

155. In the web interface, select **Policies** > **Security**.
156. Click to open the **internal-inside-dmz** Security policy rule.

    The **Security Policy Rule** configuration window should appear.

157. Click the **Actions** tab and configure the following:

Parameter	Value
File Blocking	**Select lab-file-blocking from the drop-down list**

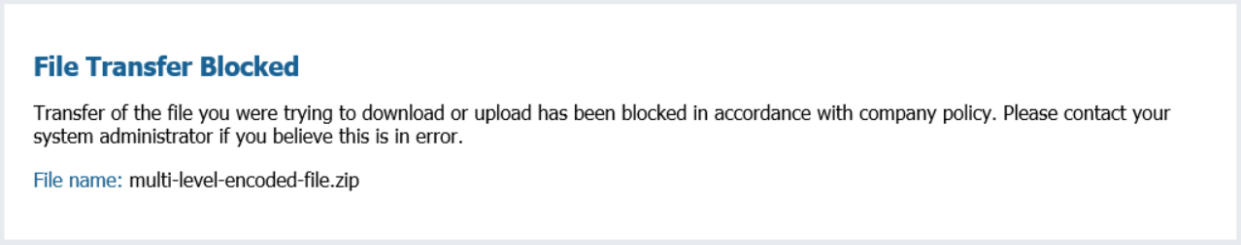


158. Click **OK** to close the **Security Policy Rule** configuration window.
159. **Commit** all changes.

1.20 Test the File Blocking Profile with Multi-Level Encoding

160. On your desktop, open a new browser window in private/incognito mode and browse to **http://192.168.50.10/mle.zip**.

The URL links to a zip file that was compressed five times.



The file should be blocked in accordance with the new file blocking rule.

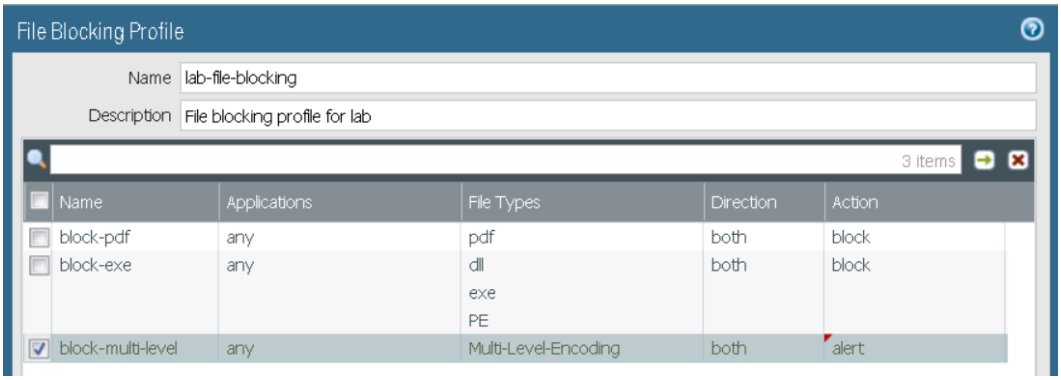
161. Close the browser window.

1.21 Modify the Security Policy Rule

162. In the web interface, select **Objects > Security Profiles > File Blocking**.
163. Click **lab-file-blocking** to open the File Blocking Profile.

The **File Blocking Profile** configuration window should appear.

164. Select the **block-multi-level** rule.
165. Change the **Action** to **alert**.



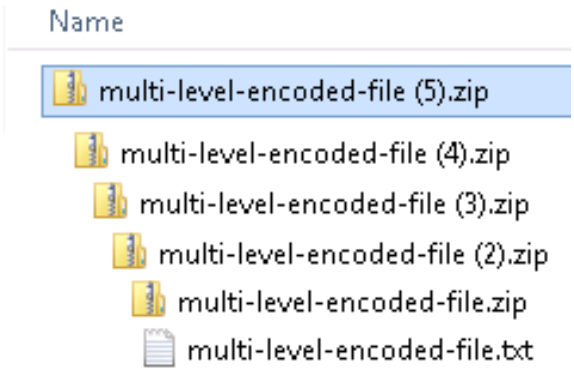
166. Click **OK** to close the **File Blocking Profile** configuration window.
167. **Commit** all changes.

1.22 Test the File Blocking Profile with Multi-Level Encoding

168. On your desktop, open a new browser window in private/incognito mode and browse to **http://192.168.50.10/mle.zip**.

    The URL links to a file that was compressed five times. The file no longer is blocked.

169. Save and open the file to examine the contents:



    Note: The screenshot shows the recursive structure of the zip archive. You cannot produce this view using Windows File Explorer.

170. Close the browser window.

1.23 Create a Danger Security Policy Rule

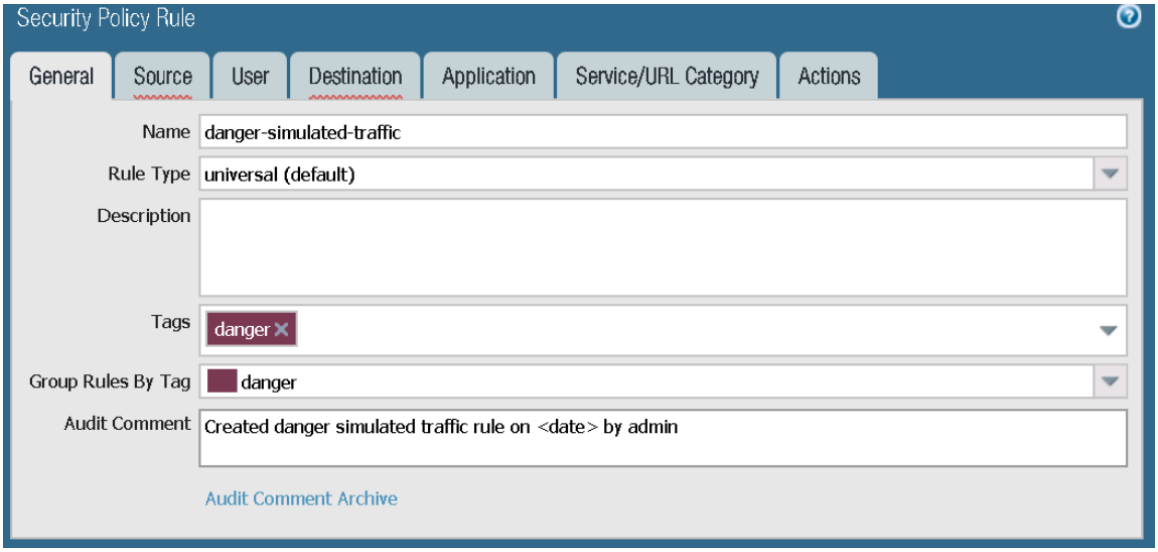
Create a Security policy rule that references the danger security zone for threat and traffic generation.

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

    The **Security Policy Rule** configuration window should appear.

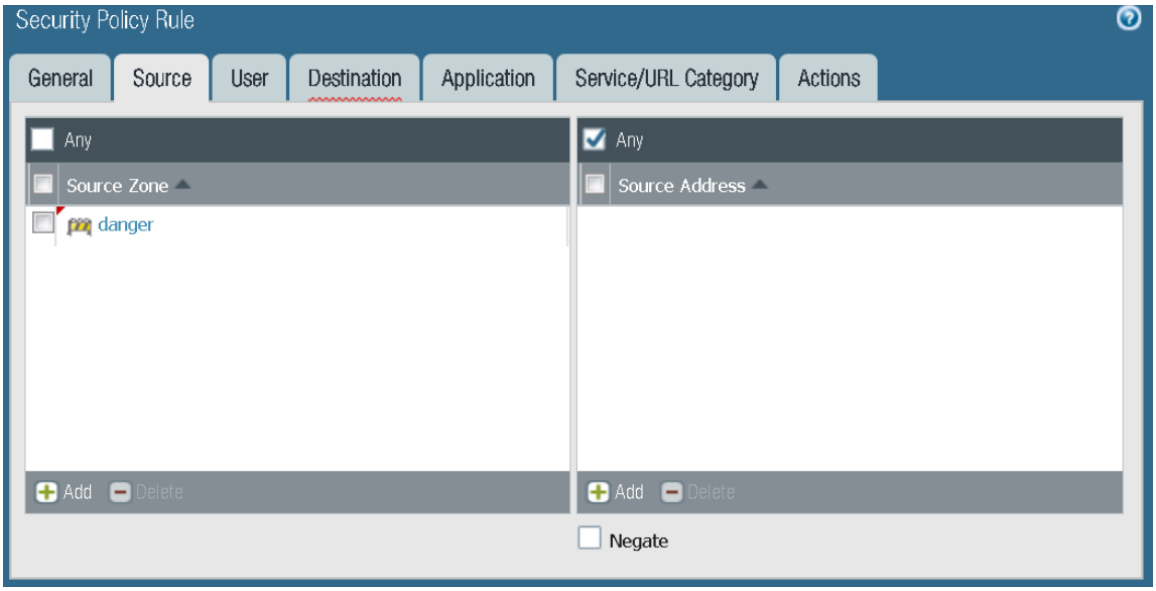
173. Configure the following:

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 <Your-Role>`



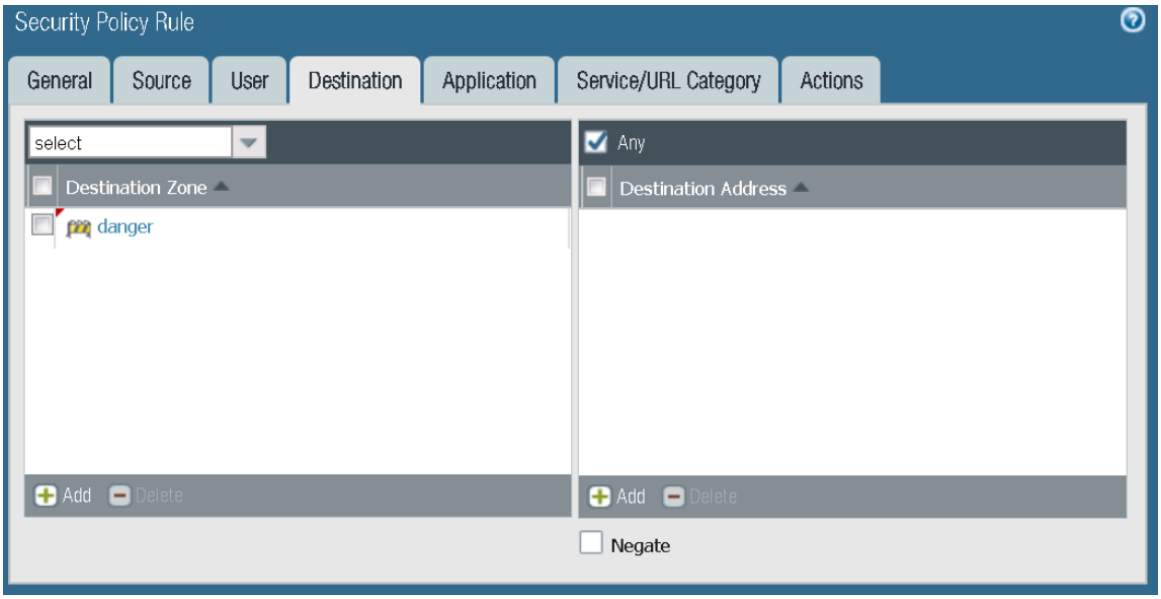
174. Click the **Source** tab and configure the following:

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



175. Click the **Destination** tab and configure the following:

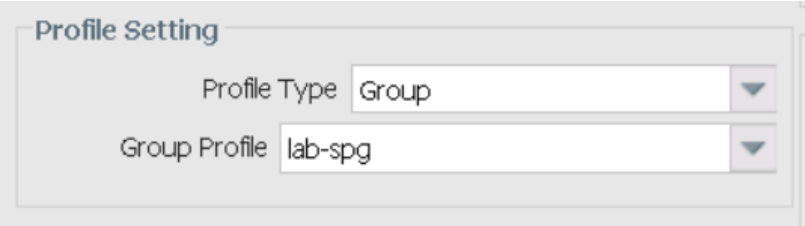
Parameter	Value
Destination Zone	Click **Add** and select **danger** from the drop-down list
Destination Address	Verify that the **Any** check box is selected



176. Click the **Actions** tab and configure the following:

Parameter	Value
Profile Type	Select **Group** from the drop-down list

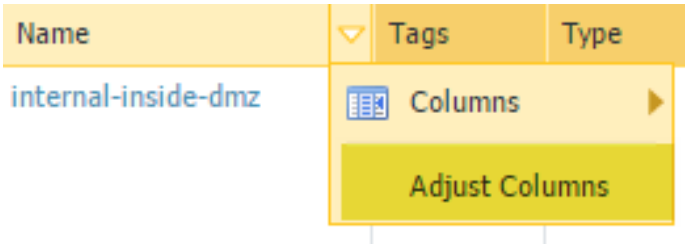
Parameter	Value
Group Profile	Select **lab-spg** from the drop-down list



177. Click **OK** to close the **Security Policy Rule** configuration window.

The new Security Policy Rule now should be listed.

178. Hover the mouse over the **Name** column header and select **Adjust Columns** from the drop-down list:

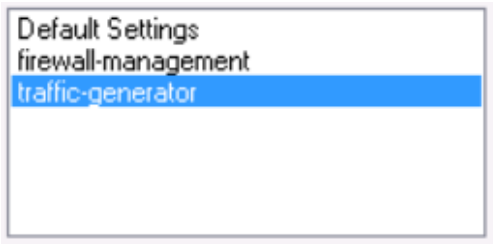


Notice that the width of all the columns was adjusted to fit the text in the columns.

179. **Commit** all changes.

1.24 Generate Threats

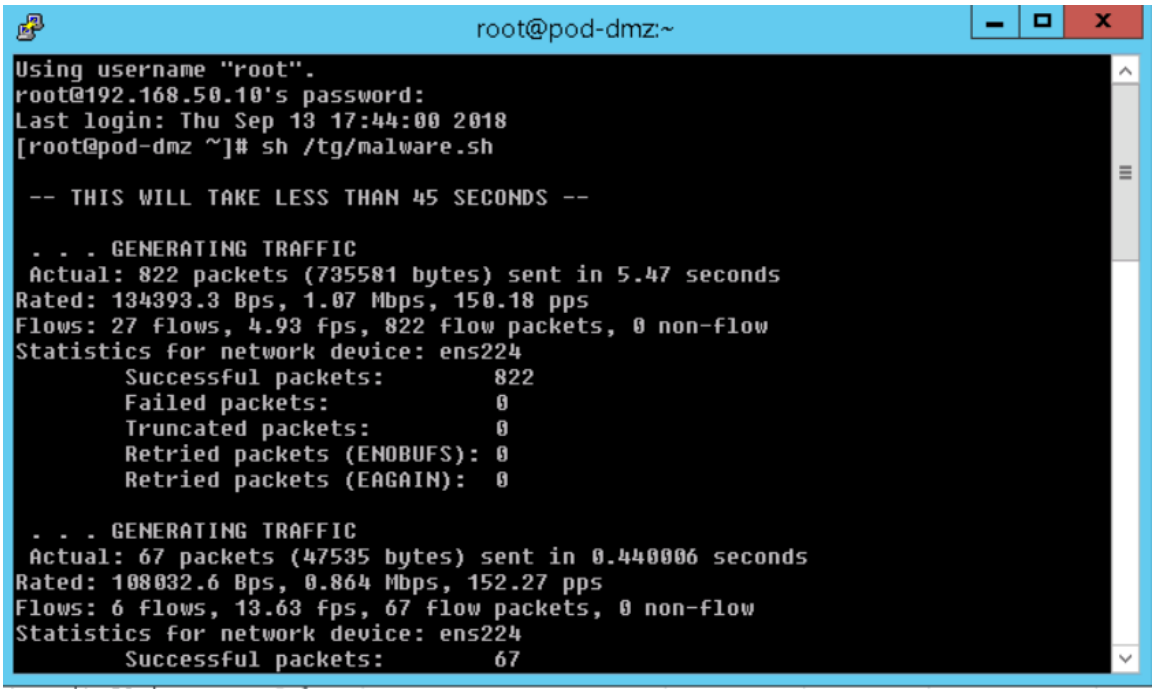
180. On the Windows desktop, double-click the **PuTTY** icon.
181. Double-click **traffic-generator**:



182. Enter the following information when prompted:

Parameter	Value
User	`root`
Password	`Pal0Alt0`

183. In the **PuTTY** window, type the **`sh /tg/malware.sh`** command:



Wait for the shell script to complete.

184. Leave the **PuTTY** window open.

185. In the web interface, select **Monitor > Logs > Threat**.

Notice the threats currently listed from the generated traffic:

Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity	File Name
02/20 00:59:01	spyware	Suspicious HTTP Evasion Found	danger	danger	10.12.1.101	134.0.116.201	80	web-browsing	alert	inform...	
02/20 00:58:35	spyware	Suspicious HTTP Evasion Found	danger	danger	192.168.0.2	112.137.162....	80	web-browsing	alert	inform...	
02/20 00:58:35	spyware	Bredolab.Gen Command and Control Traffic	danger	danger	192.168.0.2	112.137.162....	80	web-browsing	drop	critical	controller.php
02/20 00:58:32	vulnerability	Trojan-Win32.swrort.dfap	danger	danger	10.10.10.10	192.168.1.121	25	smtp	alert	high	CV.Cindy.Nero.p...
02/20 00:58:30	vulnerability	Ransom-Win32.locky.pe	danger	danger	10.10.10.10	192.168.1.121	25	smtp	alert	high	locky.exe..Cont...

Note: 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 configuration 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**.

186. In the web interface, select **Monitor > Logs > Data Filtering**.

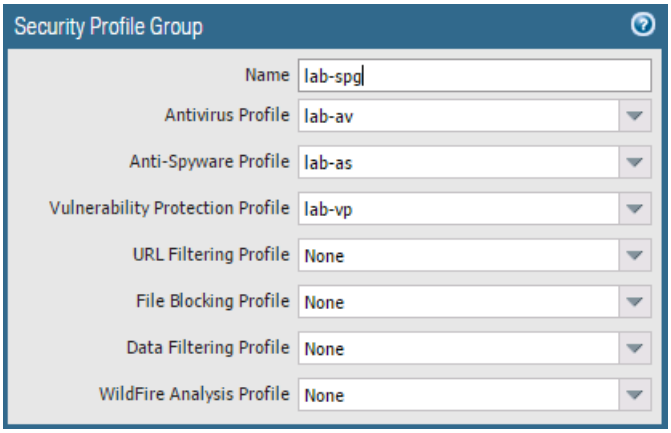
Notice the blocked files:

Receive Time	Ca...	File Name	Name	From Zone	To Zone	Source address	Destination address	Action
02/20 00:58:53	any	fix832922.ms	Microsoft PE File	danger	danger	10.12.1.101	194.58.100.59	deny
02/20 00:58:51	any	cE7ZM5.exe	Microsoft PE File	danger	danger	10.5.3.101	65.60.47.53	deny
02/20 00:58:48	any	89yg7g87byi	Microsoft PE File	danger	danger	10.5.3.101	72.52.179.2	deny
02/20 00:58:46	any	89yg7g87byi	Microsoft PE File	danger	danger	10.5.3.101	210.1.60.27	deny
02/20 00:58:44	any	8_pdTQ.exe	Microsoft PE File	danger	danger	10.5.3.101	185.104.45.34	deny

1.25 Modify a Security Profile Group

187. In the web interface, select **Objects > Security Profile Groups**.
188. Click to open the **lab-spg** Security Profile Group.

    The **Security Profile Group** configuration window should appear.
189. Remove the File Blocking Profile:



190. Click **OK** to close the **Security Profile Group** configuration window.
191. **Commit** all changes.

1.26 Generate Threats

192. In the **PuTTY** window named **root@pod-dmz**, type the command **`sh /tg/malware.sh`**.

    Wait for the shell script to complete.
193. Close the **PuTTY** window.
194. In the web interface, select **Monitor > Logs > Threat**.

    Notice the blocked files and whether any new threats were detected with 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:

		Type	Name	To Zone	Application	Action	Severity	File Name
		spyware	generic:tischlerei-kreiner.at	outside	dns	sinkhole	medium	
		spyware	generic:tischlerei-kreiner.at	danger	dns	sinkhole	medium	
		spyware	generic:evastrutzmann.at	outside	dns	sinkhole	medium	
		spyware	generic:evastrutzmann.at	danger	dns	sinkhole	medium	
		wildfire-virus	TrojanSpy/Win32.ursnif.bknt	danger	web-browsing	reset-server	medium	fix832922.ms
		wildfire-virus	Ransom/Win32.locky.mn	danger	web-browsing	reset-server	medium	89yg7g87byi
		wildfire-virus	Ransom/Win32.locky.mn	danger	web-browsing	reset-server	medium	89yg7g87byi
		spyware	Bredolab.Gen Command and Control Traffic	danger	web-browsing	drop	critical	controller.php
		vulnerability	Trojan-Win32.swrort.dfap	danger	smtp	reset-both	high	CV.Cindy.Nero.pdf
		vulnerability	Ransom-Win32.locky.pe	danger	smtp	reset-both	high	locky.exe..Content

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

Stop. This is the end of the Content-ID lab.