Palo Alto Networks

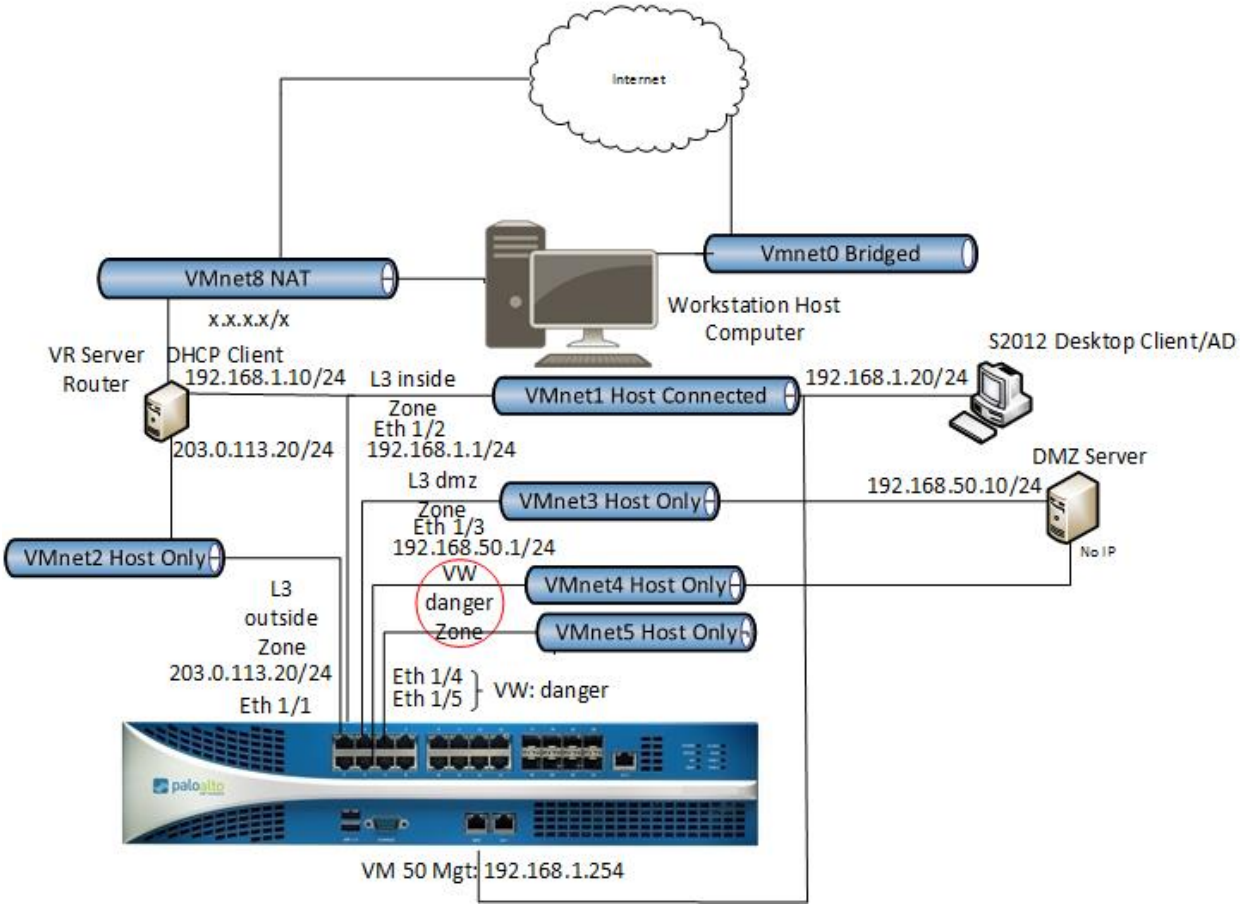
Academy Labs

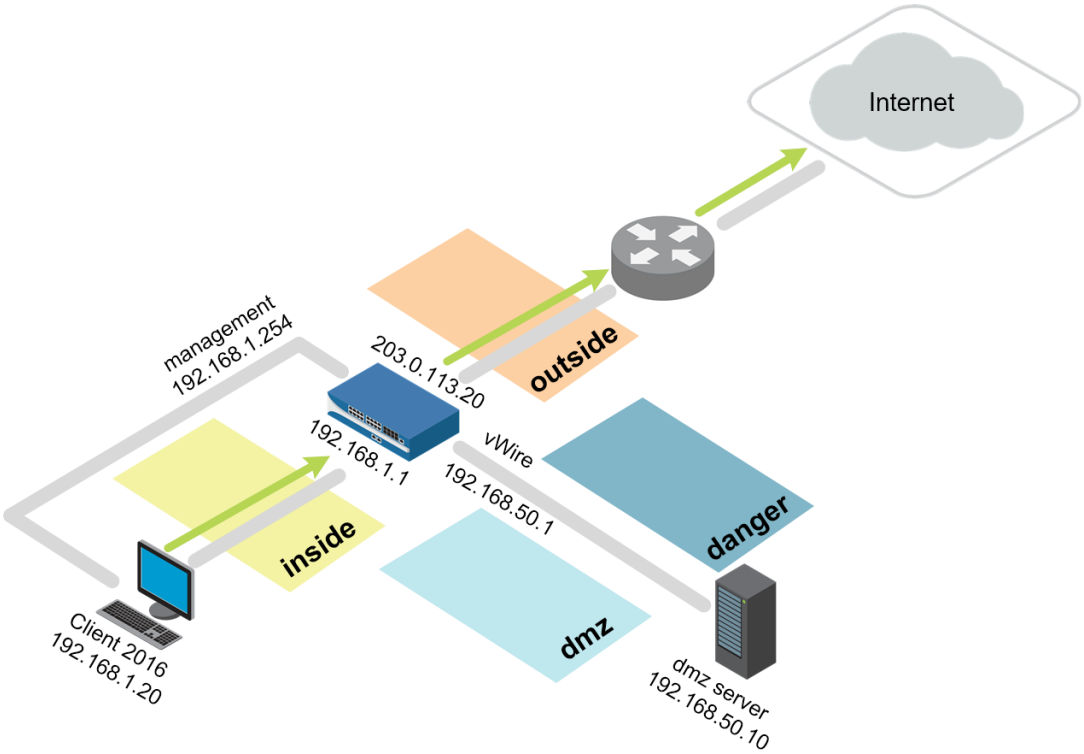
Lab 5 Content-ID

Document Version: 2018-11-10

www.paloaltonetworks.com

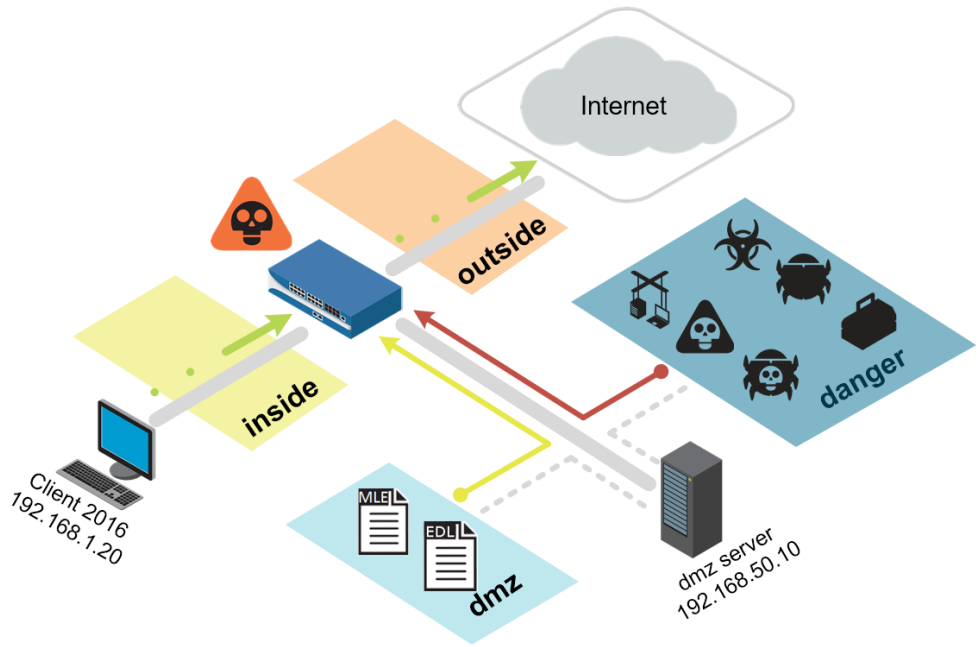
Lab Topology





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

Lab 5: Content-ID

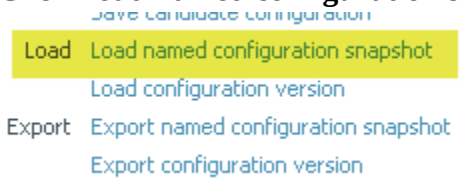


Lab Objectives

- 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.

5.0 Load Lab Configuration

1. In the web interface select **Device** > **Setup** > **Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-05** and click **OK**.
4. Click **Close**.
5. Commit all changes.

5.1 Create 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.

6. Select **Objects** > **Security Profiles** > **Antivirus**. 

7. Click 

to create an Antivirus Profile.
8. Configure the following:

Parameter	Value
Name	`lab-av`
Packet Capture	Packet Capture
Decoder	Set the Action column for http to **reset-server**

9. Click **OK** to close the **Antivirus Profile** configuration window.
10. Select **Policies** > **Security**. 

11. Select the **egress-outside-app-id** Security policy rule without opening it:


12. Click 

. The **Clone** configuration window opens.
13. Verify that **Move top** is selected from the **Rule** order drop-down list.
14. Click **OK** to close the **Clone** configuration window.
15. With the original egress-outside-app-id still selected, click 

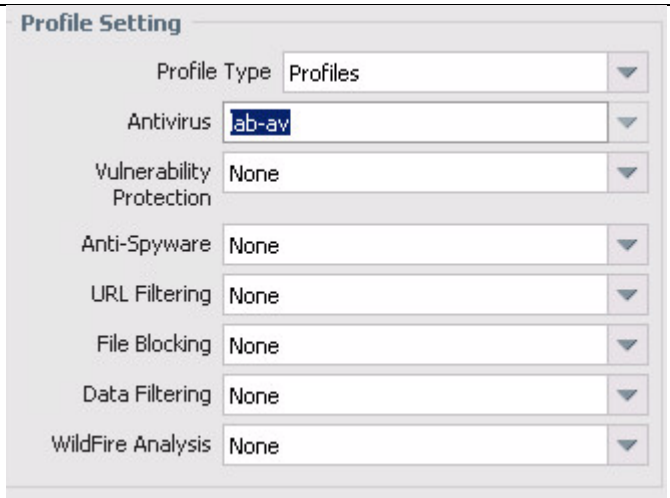
.
16. Click to open the cloned Security policy rule named **egress-outside-app-id-1**.
17. Configure the following:

Parameter	Value
Name	`egress-outside-av`
Tags	**egress**

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

Parameter	Value
Applications	Any

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

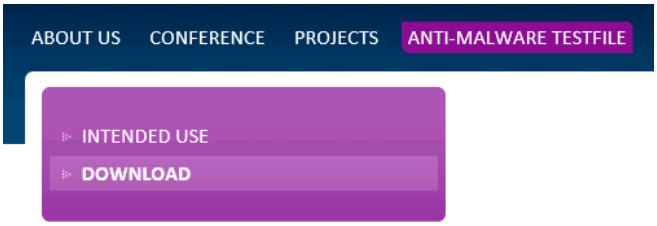
Parameter	Value
Profile Type	**Profiles**
Profile Setting	

20. Click **OK** to close the **Security Policy Rule** configuration window.
21. Commit all changes.

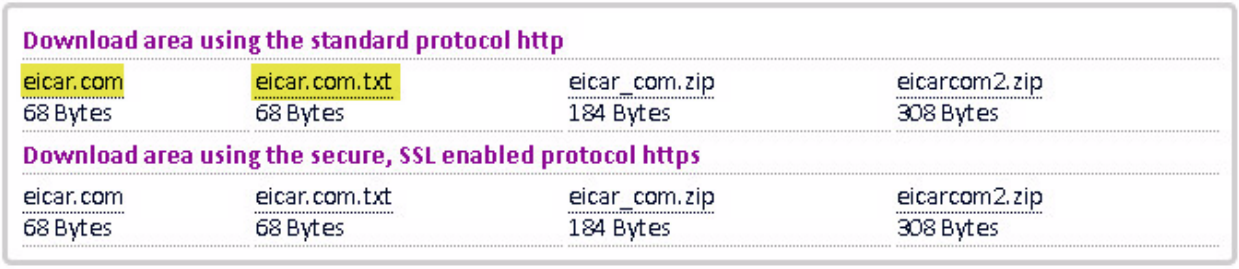
5.2 Test Security Policy Rule

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

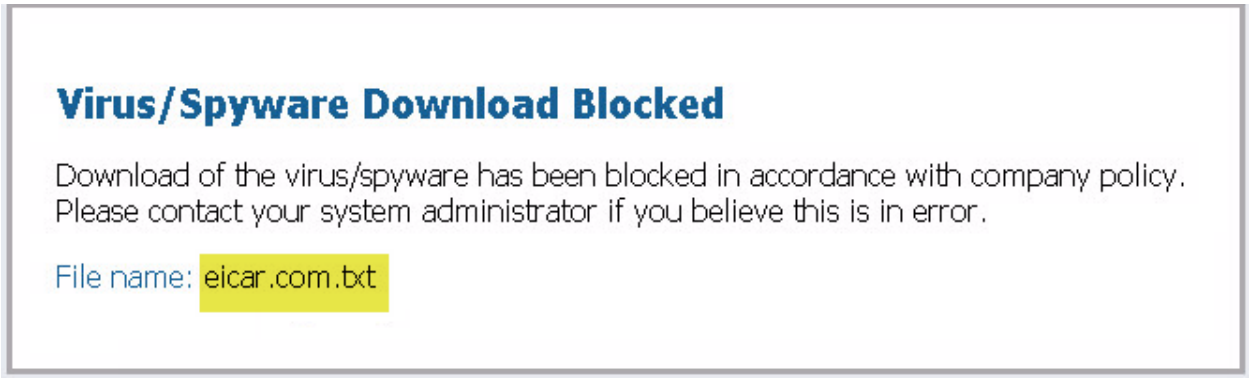
24. Click the **Download** link on the left of the web page:



25. Within the **Download** area 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.



26. If prompted, **Save** the file. Do *not* open or run the file.



27. Close the browser window.

5.3 Review Logs

28. In the web interface select **Monitor** > **Logs** > **Threat**. 

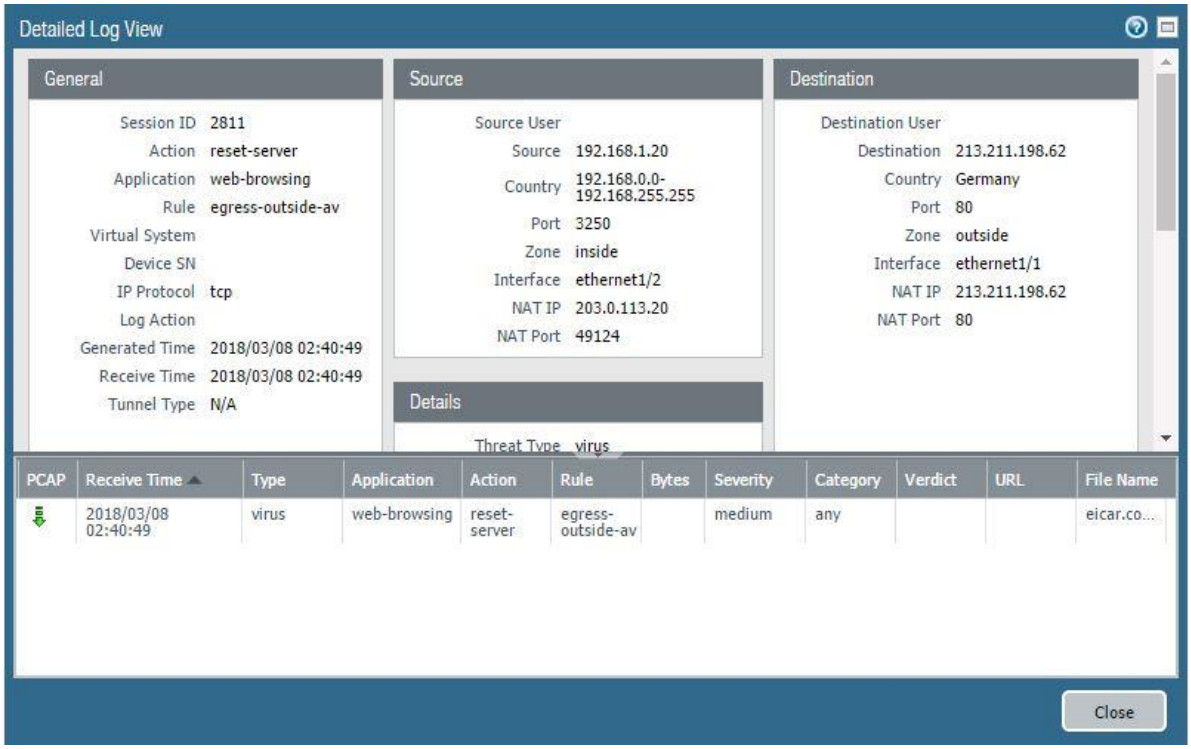
29. Find the log message that detected the **Eicar Test File**. Notice that the action for the file is **reset-server**:

To Port	Application	Action	Severity	File Name
56835	web-browsing	reset-server	medium	eicar.com.txt

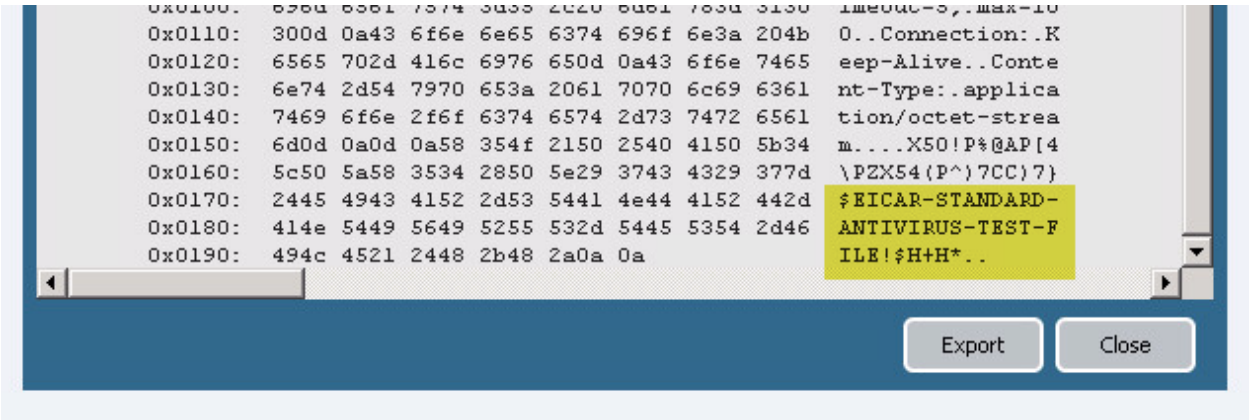
30. Notice the icon on the left side of the entry for the **Eicar Test File** indicating that there is a packet capture (pcap):

		Receive Time	Type	Name
		11/10 13:02:04	virus	Eicar Test File

To view 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:



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.

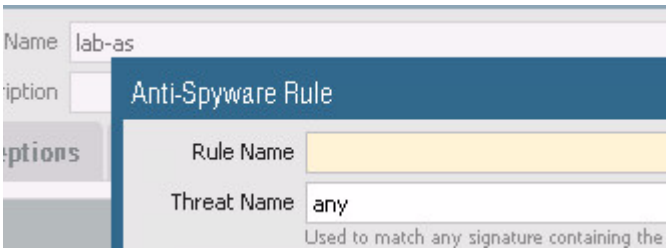
31. After viewing the pcap, click **Close**.

5.4 Create Security Policy Rule with an Anti-Spyware Profile

32. Select **Objects** > **Security Profiles** > **Anti-Spyware**.

33. Click Add to create an Anti-Spyware Profile.

34. Configure the following:

Parameter	Value
Name	`lab-as`
Rules tab	Click **Add** and create a rule with these parameters:  ▪ Rule Name: `med-low-info` ▪ Action: Select **Alert** ▪ Severity: Select only the **Medium**, **Low**, and **Informational** check boxes Click **OK** to save the rule. Click **Add** and create another rule with these parameters: ▪ Rule Name: `crit-high` ▪ Action: Select **Drop** ▪ Severity: Select only the **Critical** and **High** check boxes Click **OK** to save the rule.

35. Click **OK** to close the **Anti-Spyware Profil**e configuration window.
36. Select **Policies** > **Security**. 

37. Select the **egress-outside-av** Security policy rule without opening it.
38. Click 

. The **Clone** configuration window opens.
39. Verify that **Move top** is selected from the **Rule** order drop-down list.
40. Click **OK** to close the **Clone** configuration window.
41. With the original egress-outside-av still selected, click 

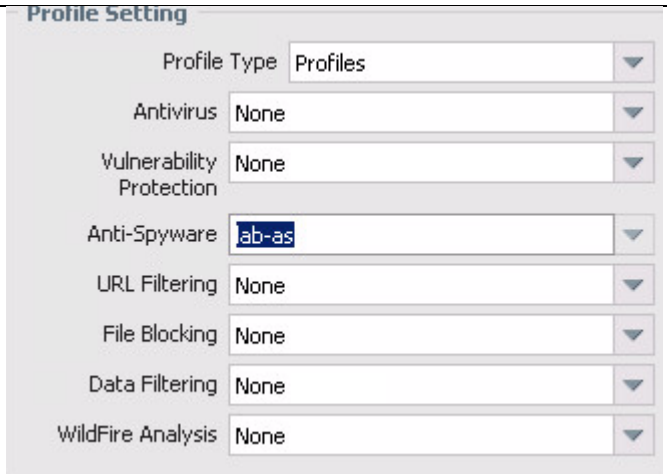
.
42. Click to open the cloned Security policy rule named **egress-outside-av-1**.
43. Configure the following:

Parameter	Value
Name	`egress-outside-as`
Tags	**egress**

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

Parameter	Value
Source Zone	inside

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

Parameter	Value
Profile Type	**Profiles**
Profile Setting	

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

5.5 Create DMZ-Access Security Policy

In the next section, 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. For the EDL and DNS Sinkhole configurations to 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.

47. Select the **internal-dmz-ftp** Security policy rule without opening it.
48. Click  . The **Clone** configuration window opens.
49. Verify that **Move top** is selected from the **Rule** order drop-down list.
50. Click **OK** to close the **Clone** configuration window.
51. With the original internal-dmz-ftp still selected, click  .

52. Click to open the cloned Security policy rule named **internal-dmz-ftp-1**.
53. Configure the following:

Parameter	Value
Name	`internal-inside-dmz`
Tags	**internal**

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

Parameter	Value
Destination Address	Any

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

Parameter	Value

Applications	`web-browsing`
	`ssl`
	`ssh`
	`ftp`

56. Click **OK** to close the **Security Policy Rule** configuration window.
57. Select **Policies** > **NAT**. NAT
58. Select the **destination-dmz-ftp** NAT policy rule without opening it.
59. Click Disable.
60. Commit all changes.

5.6 Configure DNS-Sinkhole External Dynamic List

An External Dynamic List (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.

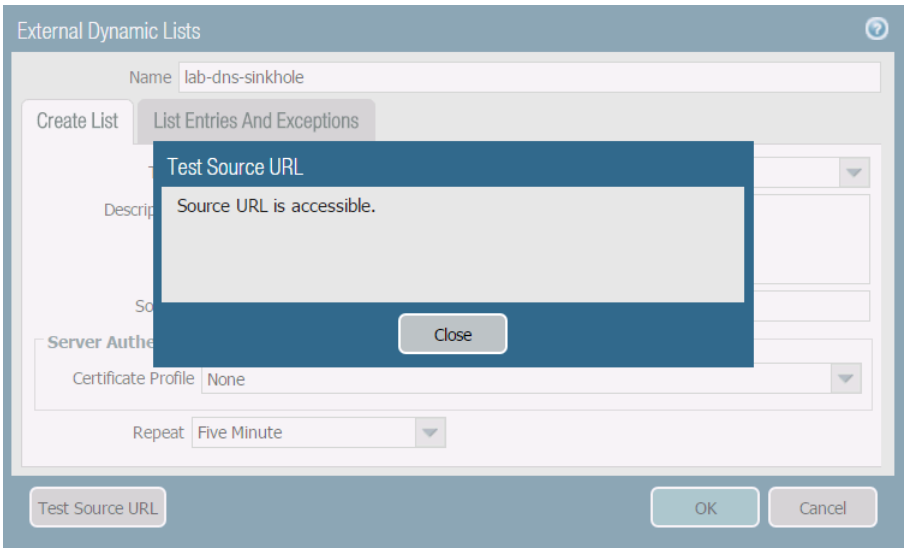
61. Select **Objects** > **External Dynamic Lists**. External Dynamic Lists
62. Click Add to configure a new EDL.
63. Configure the following:

Parameter	Value
Name	`lab-dns-sinkhole`

Parameter	Value
Type	**Domain List**
Source	`http://192.168.50.10/dns-sinkhole.txt` (This is hosted on the DMZ server.)
Repeat	**Five Minute**

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

64. Click **OK** to close the configuration window.
65. Commit all changes.
66. Open the `lab-dns-sinkhole` configuration you just created and click **Test Source URL**:



67. 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.
68. Click **OK** to close the **External Dynamic Lists** configuration window.

5.7 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.

69. Select **Objects** > **Security Profiles** > **Anti-Spyware**.
70. Click to open the Anti-Spyware Profile named lab-as.
71. Click the **DNS Signatures** tab.
72. Click Add and select lab-dns-sinkhole.

73. Verify that the **Action on DNS Queries** is set to **sinkhole**:

External Dynamic List Domains	Action on DNS Querie
Palo Alto Networks DNS Signatures	sinkhole
lab-dns-sinkhole	sinkhole

74. Verify that the **Sinkhole IPv4** is set to **72.5.65.111**.
75. Click **OK** to close the **Anti-Spyware Profile** configuration window.
76. Commit all changes.

5.8 Test Security Policy Rule

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

```
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

> _
```

80. At the `nslookup` command prompt, type `reddit.com`. and press the **Enter** key:

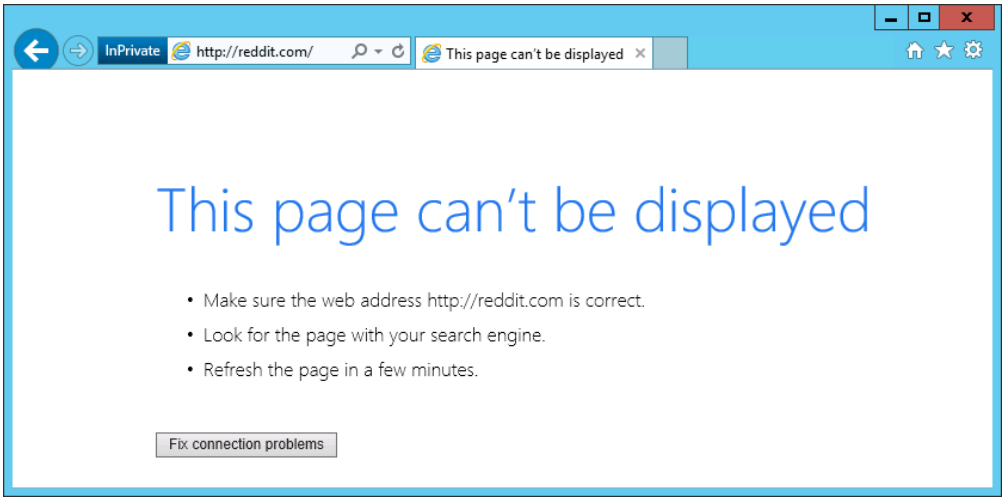
```
> reddit.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    reddit.com
Addresses:  ::1
          72.5.65.111

> _
```

Notice that the reply for reddit.com is 72.5.65.111. The request has been sinkholed.

81. Type `exit` and press the **Enter** key to exit `nslookup`. Then type `exit` and press the **Enter** key again to exit the command-prompt window.
82. On the desktop, open a browser and go to `http://reddit.com` and wait for the connection to timeout.



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.

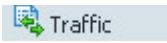
83. Close the browser window.

5.9 Review Logs

84. Select **Monitor** > **Logs** > **Threat**. 

85. Identify the **Suspicious Domain** log entry. Notice that the action is **sinkhole** and that the **File Name** column includes the DNS name that was queried (reddit.com):

Type	Name	Source address	Destination address	Application	Action	Severity	File Name
spyware	Suspicious Domain	192.168.1.20	8.8.8.8	dns	sinkhole	medium	Suspicious DNS Query (reddit.com)

86. Select **Monitor** > **Logs** > **Traffic**. 

87. Type the following filter statement `(addr.dst in 72.5.65.111)` and press the **Enter** key:

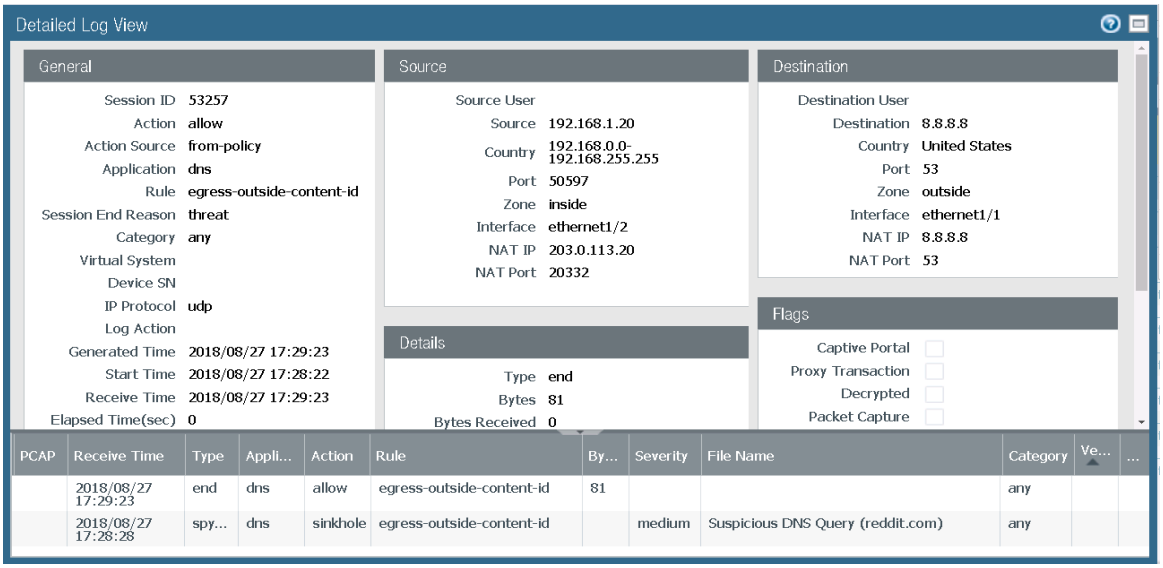
(addr.dst in 72.5.65.111)

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
	08/27 17:28:40	end	inside	outside	192.168.1.20		72.5.65.111	80	incomplete	allow	egress-outside-content-id	tcp-fin	432
	08/27 17:28:38	end	inside	outside	192.168.1.20		72.5.65.111	80	web-browsing	allow	egress-outside-content-id	tcp-rst-from-server	799

Notice that the **Application** type is "Incomplete" and the **Session End Reason** is "tcp-fin." These results occur 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)`.

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



90. In the **Detailed Log View** notice the additional information that matches what you saw 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.

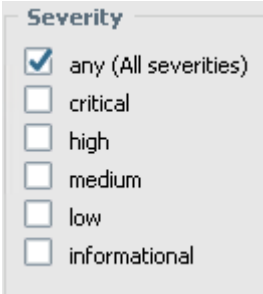
5.10 Create Security Policy Rule with a Vulnerability Protection Profile

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

91. Select **Objects** > **Security Profiles** > **Vulnerability Protection**. Vulnerability Protection
92. Click Add to create a Vulnerability Protection Profile.
93. Configure the following:

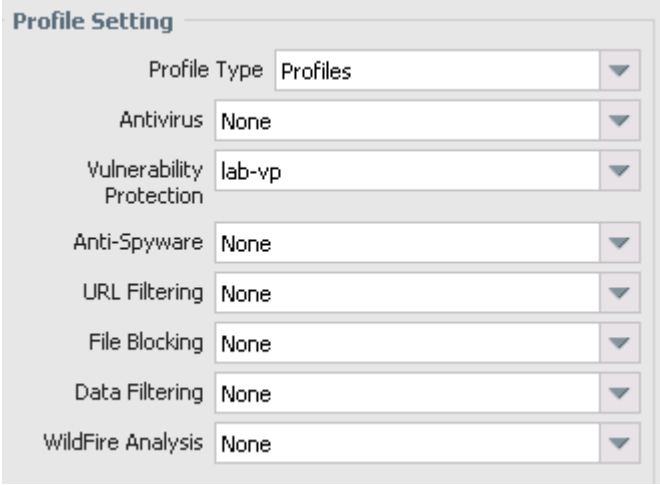
Parameter	Value
Name	`lab-vp`

94. On the **Rules** tab, click Add to create a rule.
95. Configure the following:

Parameter	Value
Name	`lab-vp-rule`
Packet Capture	
Severity	

96. Click **OK** twice.
97. Select **Policies** > **Security**. 

98. Click to open the internal-inside-dmz Security policy rule.
99. Click the **Actions** tab and configure the following:

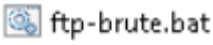
Parameter	Value
Profile Type	**Profiles**
Profile Setting	

100. Click **OK** to close the **Security Policy Rule** configuration window.
101. 

all changes.

5.11 Test Security Policy Rule

102. On the Windows desktop, double-click the **lab** folder and then the **bat files** folder.

103. Double-click 

.

Note: This action launches an FTP brute force attack at the DMZ FTP server. The script should take about *10 minutes* to complete.

```
Starting Nmap 7.31 ( https://nmap.org ) at 2018-01-22 02:44 Coordinated Universa
l Time
Nmap scan report for 192.168.50.10
Host is up (0.00013s latency).
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 1251 guesses in 604 seconds, average tps: 2.1

Nmap done: 1 IP address (1 host up) scanned in 604.58 seconds

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

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

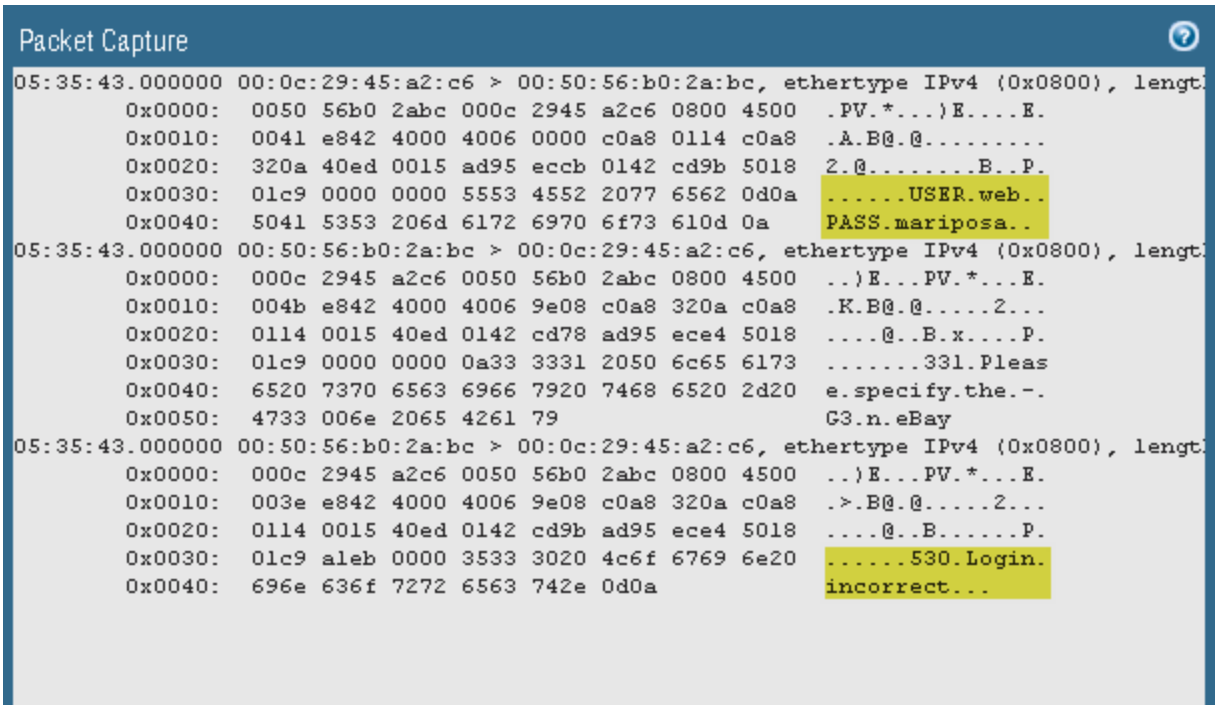
5.12 Review Logs

105. Select **Monitor** > **Logs** > **Threat**. 

106. 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	Source User	Destination address	To Port	Application	Action	Severity
		08/23 19:06:32	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	ftp	alert	high
		08/23 19:06:32	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	ftp	alert	high
		08/23 19:06:32	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	ftp	alert	high

107. Open the **Detailed Log View** by clicking on the  icon. From the **Detailed Log View**, click the  icon to open the packet capture.
108. Notice the username and password that were attempted along with the 530 responses from the FTP server.



5.13 Update Vulnerability Profile

109. Select **Objects** > **Security Profiles** > **Vulnerability Protection**. Vulnerability Protection
110. Click to open the **lab-vp** profile.
111. Click to open the **lab-vp-rule** rule and configure the following:

Parameter	Value
Action	**Reset Both**
Severity	**high**

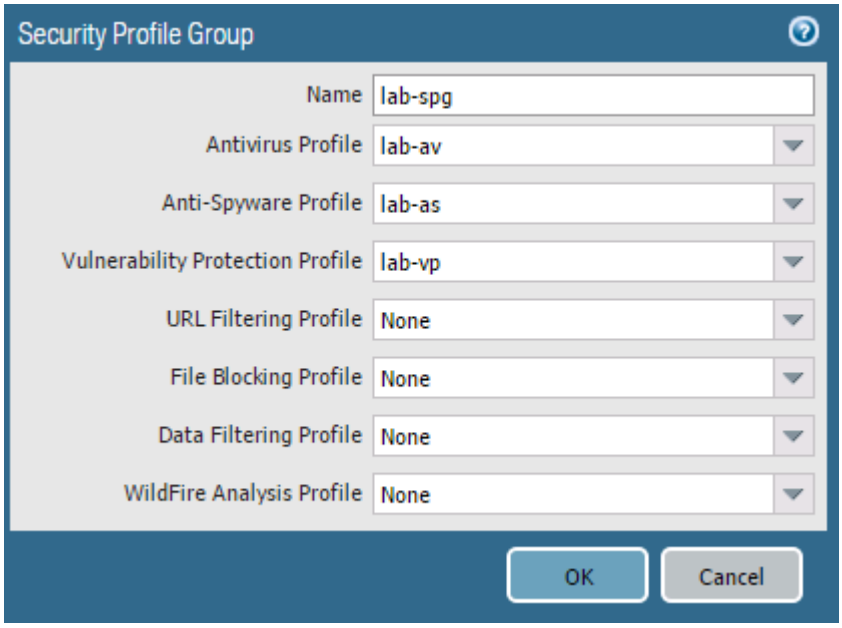
112. Click **OK** twice.
113. Commit all changes.
114. Rerun ftp-brute.bat and review the logs to confirm that the new FTP brute force attempts are reset.

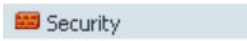
5.14 Create Group Security Profiles

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.

115. Select **Objects** > **Security Profile Groups**. Security Profile Groups
116. Click Add to open the **Security Profile Group** configuration window.

117. Configure the following:

Parameter	Value
Name	`lab-spg`
Profiles	

118. Click **OK**.
119. Select **Policies** > **Security**. 

120. 

the following rules:

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

121. Click 

to define a Security policy rule.
122. Configure the following:

Parameter	Value
Name	`egress-outside-content-id`
Rule Type	**universal (default)**
Tags	**egress**

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

Parameter	Value
Source Zone	**inside**
Source Address	**Any**

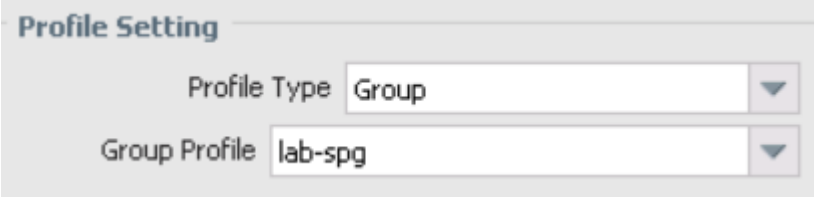
124. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	**outside**
Destination Address	**Any**

125. Click the **Application** tab and verify that  is checked.

126. Click the **Service/URL Category** tab and verify that  is selected.

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

Parameter	Value
Action Setting	**Allow**
Log Setting	**Log at Session End**
Profile Setting	

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

5.15 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.

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

130. Click  to open the **File Blocking Profile** configuration window.

131. Configure the following:

Parameter	Value
Name	`lab-file-blocking`

132. Click Add and configure the following.

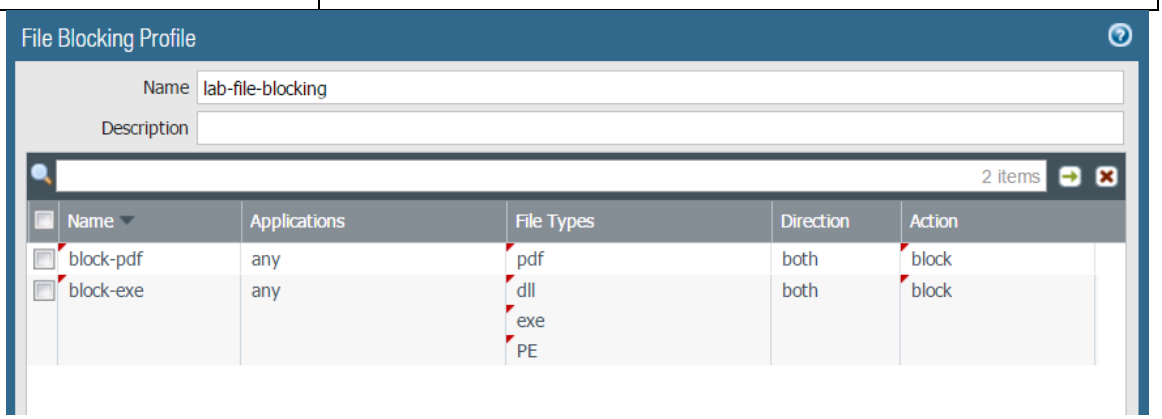
Parameter	Value
Name	`block-pdf`
Applications	**any**
File Types	`pdf`
Direction	**both**
Action	**block**

133. Click Add and configure the following:

Parameter	Value
Name	`block-exe`
Applications	**any**

File Types	`dll`
	`exe`
	`PE`

Direction	**both**
Action	**block**

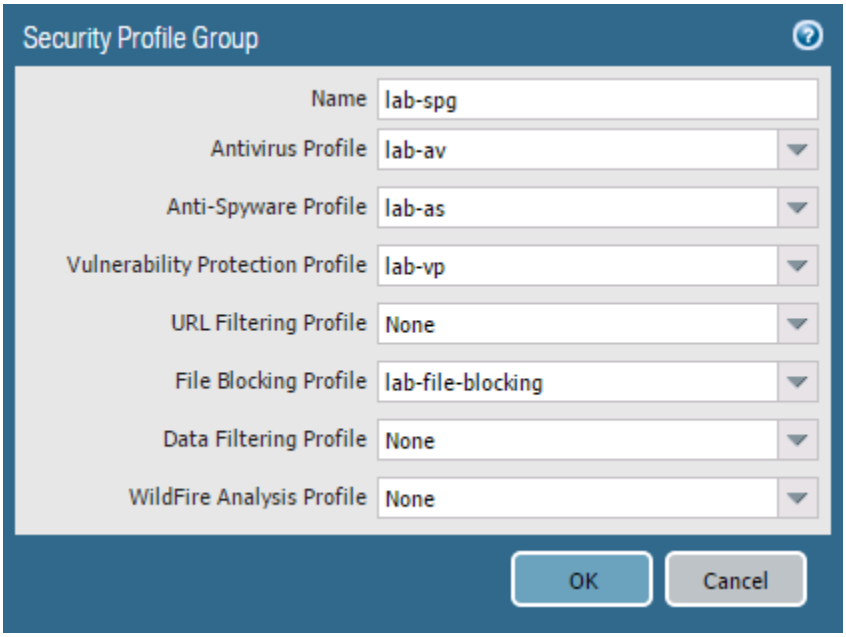


134. Click **OK** to close the **File Blocking Profile** configuration window.

5.16 Modify Security Profile Group

135. Select **Objects** > **Security Profile Groups**. 

136. Click to open the **lab-spg** Security Profile Group.
137. Add the newly created File Blocking Profile:



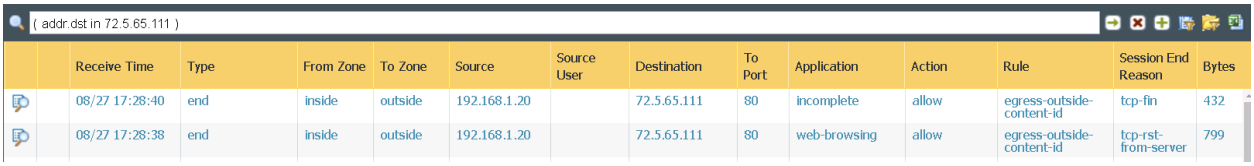
138. Click **OK**.
139. 

all changes.

5.17 Test the File Blocking Profile

140. Open a new browser window in private/incognito mode and browse to `http://www.panedufiles.com/`.

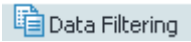
Note: Some recent updates to Google Chrome may allow the files to be successfully downloaded. If the files are not blocked, then use a different browser such as IE or Firefox, or do not open Google Chrome in incognito mode.



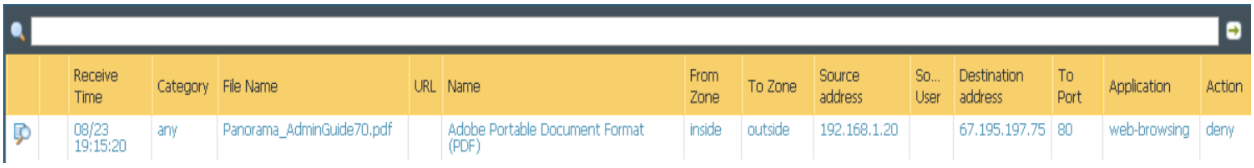
Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
08/27 17:28:40	end	inside	outside	192.168.1.20		72.5.65.111	80	incomplete	allow	egress-outside-content-id	tcp-fin	432
08/27 17:28:38	end	inside	outside	192.168.1.20		72.5.65.111	80	web-browsing	allow	egress-outside-content-id	tcp-rst-from-server	799

141. 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.

142. Close the browser window.
143. Select **Monitor** > **Logs** > **Data Filtering**. 

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



		Receive Time	Category	File Name	URL	Name	From Zone	To Zone	Source address	So... User	Destination address	To Port	Application	Action
		08/23 19:15:20	any	Panorama_AdminGuide70.pdf		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.

5.18 Multi-level Encoding

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.

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

146. Click to open the **lab-file-blocking** File Blocking Profile.
147. Click 

and configure the following:

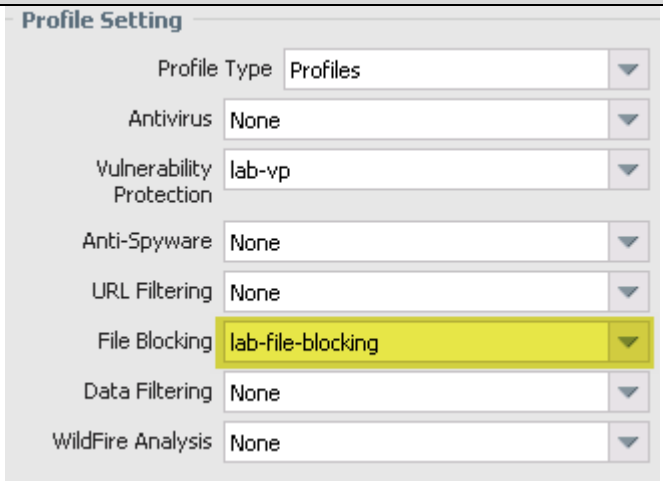
Parameter	Value
Name	`block-multi-level`
Applications	**any**
File Types	`Multi-Level-Encoding`
Direction	**both**
Action	**block**

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

5.19 Modify Security Policy Rule

149. In the web interface select **Policies** > **Security**. 

150. Click to open the **internal-inside-dmz** Security policy rule.
151. Click the **Actions** tab and configure the following:

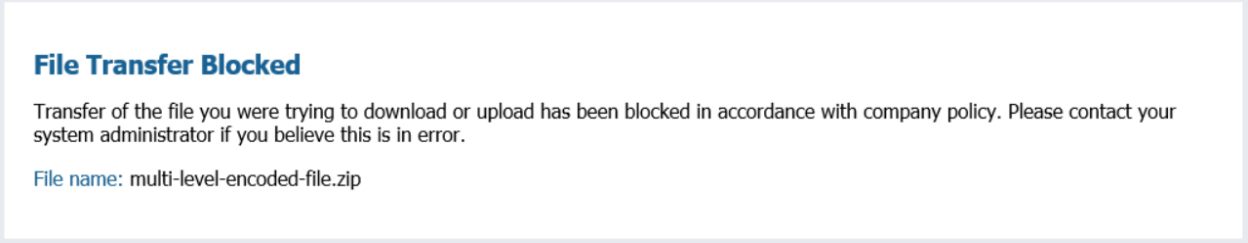
Parameter	Value
Profile Setting	

152. Click **OK** to close the **Security Policy Rule** configuration window.
153. 

all changes.

5.20 Test the File Blocking Profile with Multi-level Encoding

154. Open a new browser 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 is blocked in accordance with the new file blocking rule.

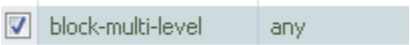
155. Close the browser window.

5.21 Modify Security Policy Rule

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

157. Click to open the **lab-file-blocking** File Blocking Profile.

158. Select the **block-multi-level** rule:

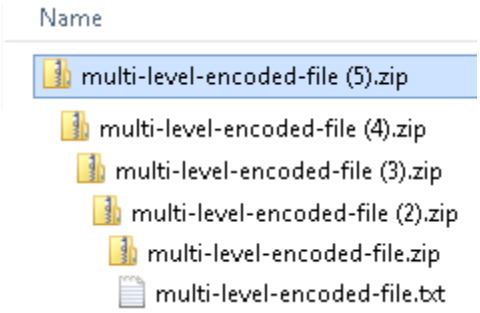


159. Change the **Action** to **alert**.
160. Click **OK** to close the **File Blocking Profile** configuration window.
161. 

all changes.

5.22 Test the File Blocking Profile with Multi-Level-Encoding

162. Open a new browser 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.
163. Save and open the file to examine the contents:



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

5.23 Create Danger Security Policy Rule

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

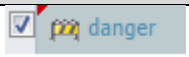
164. In the web interface select **Policies** > **Security**. 

165. Click 

and configure the following:

Parameter	Value
Name	`danger-simulated-traffic`

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

Parameter	Value
Source Zone	

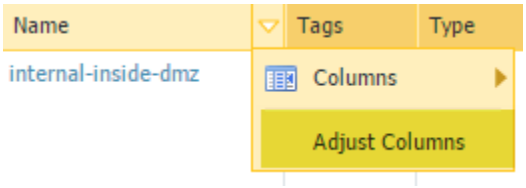
167. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	danger

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

Parameter	Value
Profile Setting	Profile Setting Profile Type: Group Group Profile: lab-spg

169. Click **OK** to close the **Security Policy Rule** configuration window.
170. 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.

171. Commit all changes.

5.24 Generate Threats

172. On the Windows desktop, open **PuTTY** and double-click **traffic-generator**.
173. Enter the following information when prompted:

Parameter	Value
Password	`Pal0Alt0`

174. In the **PuTTY** window, type the `sh /tg/malware.sh` command.
175. Wait for the shell script to complete. Leave the **PuTTY** window open.
176. In the web interface select **Monitor** > **Logs** > **Threat**. Threat
177. Type the filter `(severity neq informational)` and press the **Enter** key.
178. Notice the threats currently listed from the generated traffic:

		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	
		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-

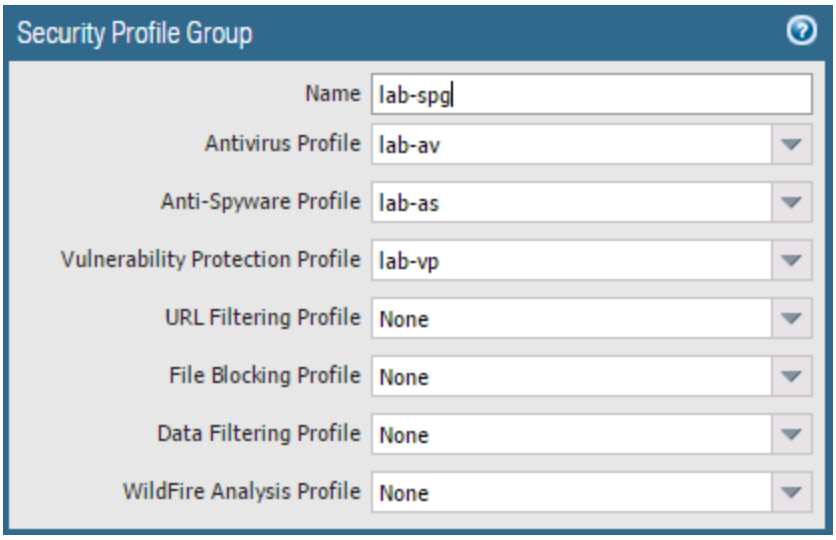
Note: The Threat log entries that you see in your lab may not match exactly the image above. Threat signatures, names, categorizations, and verdicts may change over time to ensure that the firewall will consistently detect the packet captures. Two custom Vulnerability signatures are included in the lab configuration that you loaded at the start of this module. In your lab, at a minimum, you should see the **Vulnerability** detections named **Trojan-Win32.swrort.dfap** and **Ransom-Win32.locky.pe**.

179. Select **Monitor** > **Logs** > **Data Filtering**. Data Filtering
180. Notice the blocked files:

		File Name	Name	Application	Action
		fix832922.ms	Microsoft PE File	web-browsing	deny
		cE7ZM5.exe	Microsoft PE File	web-browsing	deny
		89yg7g87byi	Microsoft PE File	web-browsing	deny
		89yg7g87byi	Microsoft PE File	web-browsing	deny
		8_pdTQ.exe	Microsoft PE File	web-browsing	deny
		Y2hNDK.exe	Microsoft PE File	web-browsing	deny
		5t3VMv.exe	Microsoft PE File	web-browsing	deny
		CV.Cindy.Nero.pdf	Adobe Portable Document Format (PDF)	smtp	deny
		locky.exe	Windows Executable (EXE)	smtp	deny
		locky.exe	Microsoft PE File	smtp	deny
		onus.dll	Microsoft PE File	silverlight	deny

5.25 Modify Security Profile Group

181. Select **Objects** > **Security Profile Groups**. Security Profile Groups
182. Click to open the **lab-spg** Security Profile Group.
183. Remove the File Blocking Profile:



184. Click **OK**.
185. Commit all changes.

5.26 Generate Threats

186. In the **PuTTY** window named **root@pod-dmz**, type the command `sh /tg/malware.sh`
187. Select **Monitor** > **Logs** > **Threat**. Threat
188. Verify that the filter `(severity neq informational)` is still active. If it is not, type it in and press the **Enter** key.
189. Notice the blocked files and whether any new threats were detected. Turn off File Blocking. 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 above.

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

