Palo Alto Networks

Academy Labs

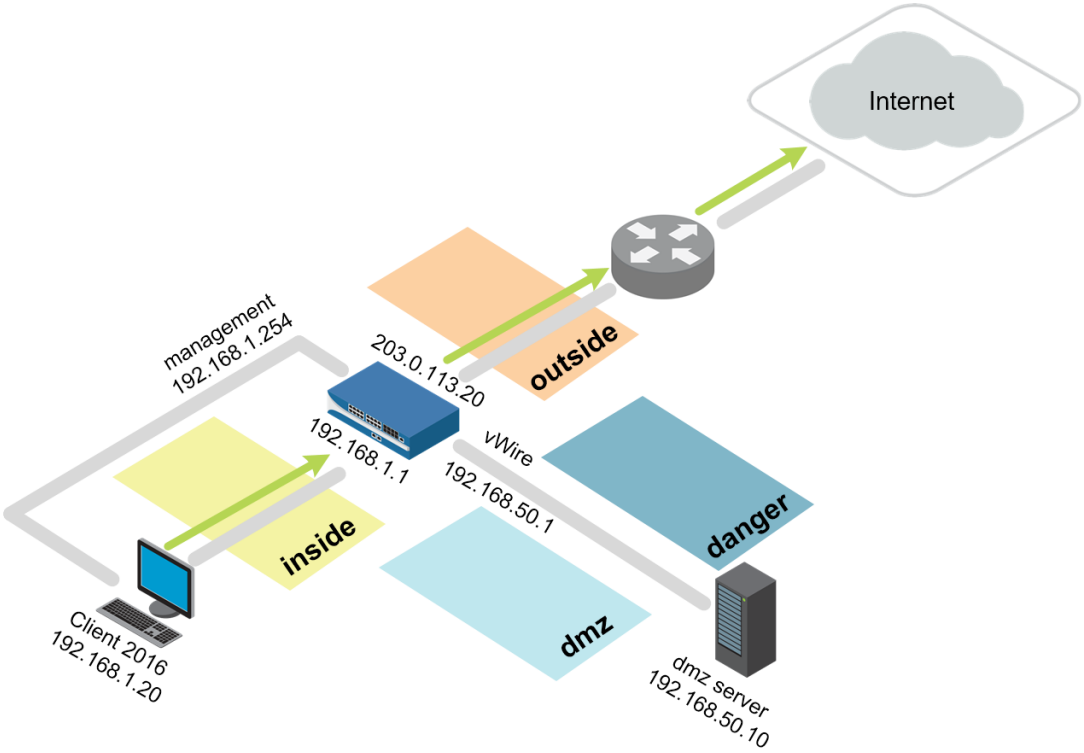
Lab App-ID

Document Version: 10-Dec-19

Copyright © 2018 Palo Alto Networks, Inc.

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

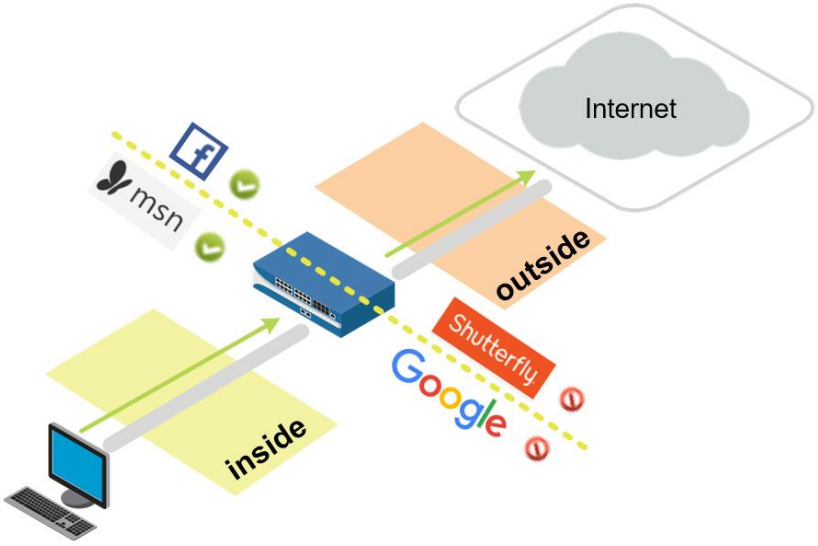
Powering Down Your VMware Workstation VM-50 firewall appliance:

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.

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

Lab: App-ID



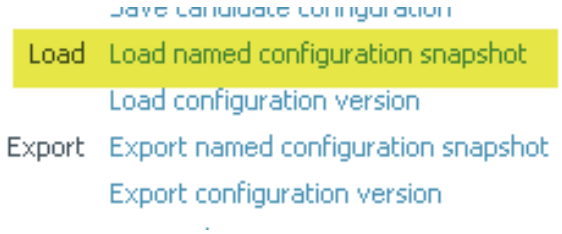
Lab Objectives

- **Create an application-aware Security policy rule.**
- **Enable interzone logging.**
- **Enable the Application Blocked page for blocked applications.**
- **Test application blocking with different applications**
- **Find the categories that match to the signature *web-browsing***
- **Migrate older port-based rules to application-aware policies.**
- **Review logs associated with the traffic and browse the Application Command Center (ACC).**

5.0 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**:

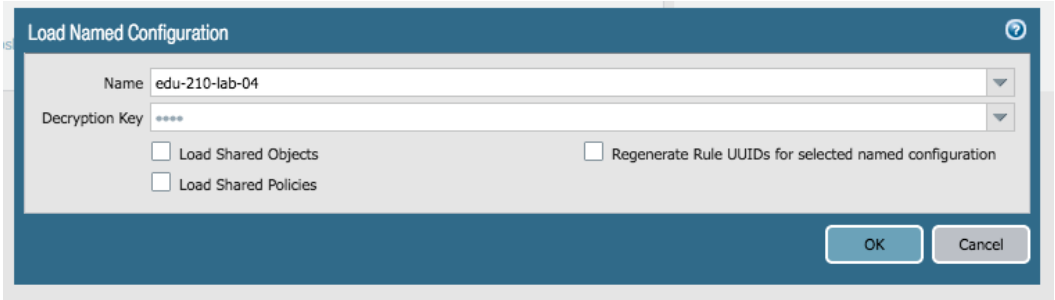


A **Load Named Configuration** dialog box appears.

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

3. Click the drop-down list next to the **Name** text box and select **edu-210-lab-04**.

   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.

5.1 Verify an FTP Service Object

At the end of this lab you will use the Policy Optimizer tool to migrate an FTP *port-based* rule to an FTP *application-based* rule. However, to prepare for that part of the lab exercise you now will configure and use an FTP *port-based* Security policy rule. You will perform this activity now because the Policy Optimizer tool processes logged traffic only at the beginning of each hour. If you generate port-based traffic now, the Policy Optimizer tool should be populated with data by the time you get to that portion of the lab.

In this section, you will start by verifying an FTP Service object that defines the FTP port. You will use this Service object in the FTP port-based Security policy rule that you will create in the next lab task.

9. In the web interface, select **Objects** > **Services**.
10. Click the **service-ftp** object to configure the service.

    The **Service** configuration window should appear.

11. Verify the following configuration:

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

Parameter	Value
Protocol	Verify **TCP** radio button is selected
Destination Port	Verify the destination port entry is set to **20-21**

12. Click **OK** to close the **Service** configuration window.

5.2 Create an FTP Port-Based Security Policy Rule

In this section, you will create a port-based Security policy rule that will enable you to simulate part of the process of migrating from a legacy, port-based Security policy to a next-generation, application-based Security policy.

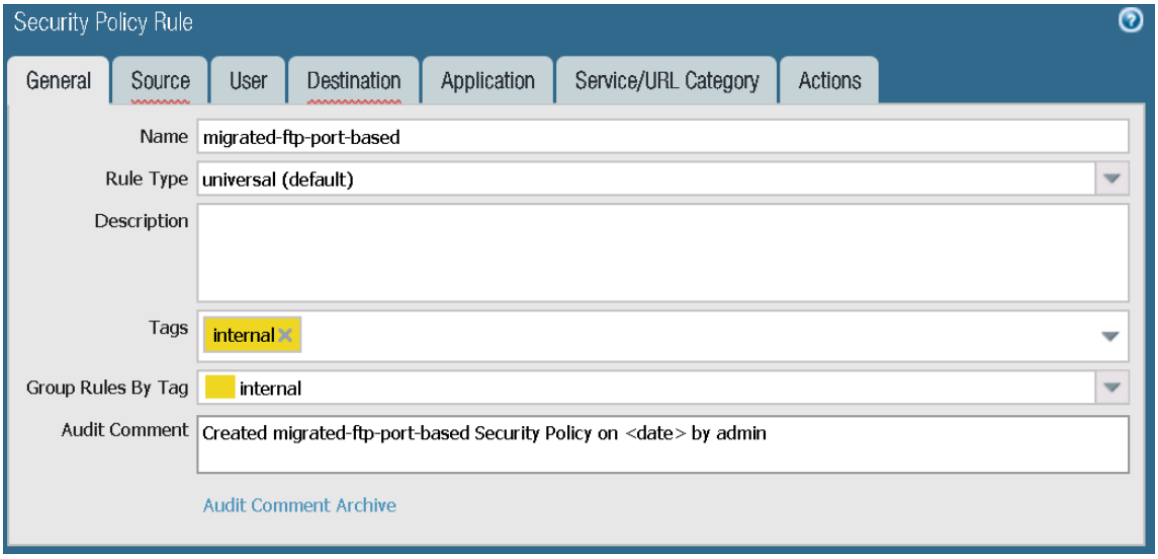
13. In the web interface, select **Policies** > **Security**.
14. Click **Add** to create a new Security policy rule.

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

15. Configure the following:

Parameter	Value
Name	Type `migrated-ftp-port-based`
Rule Type	Verify that **universal (default)** is selected
Tags	Select **internal** from the drop-down list
Group Rules By Tag	Select **internal** from the drop-down list
Audit Comment	`Type Created migrated-ftp-port-based Security Policy on <date> by <Your-Role>`

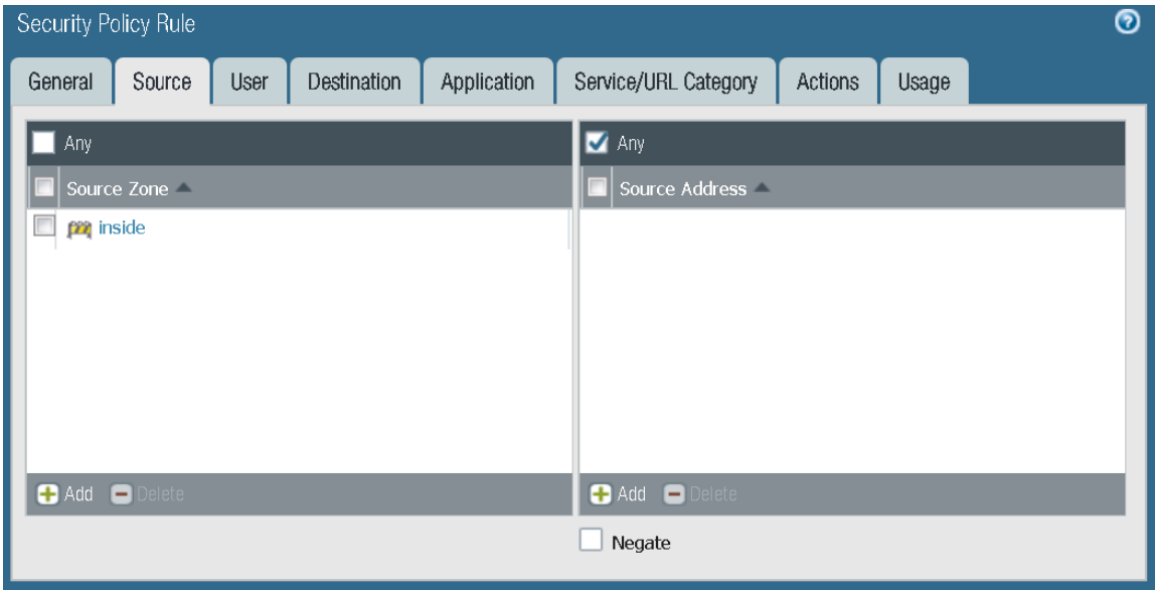
Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com



You are creating a rule that will simulate a port-based rule that was migrated from another vendor's firewall.

16. Click the **Source** tab and verify the following configuration:

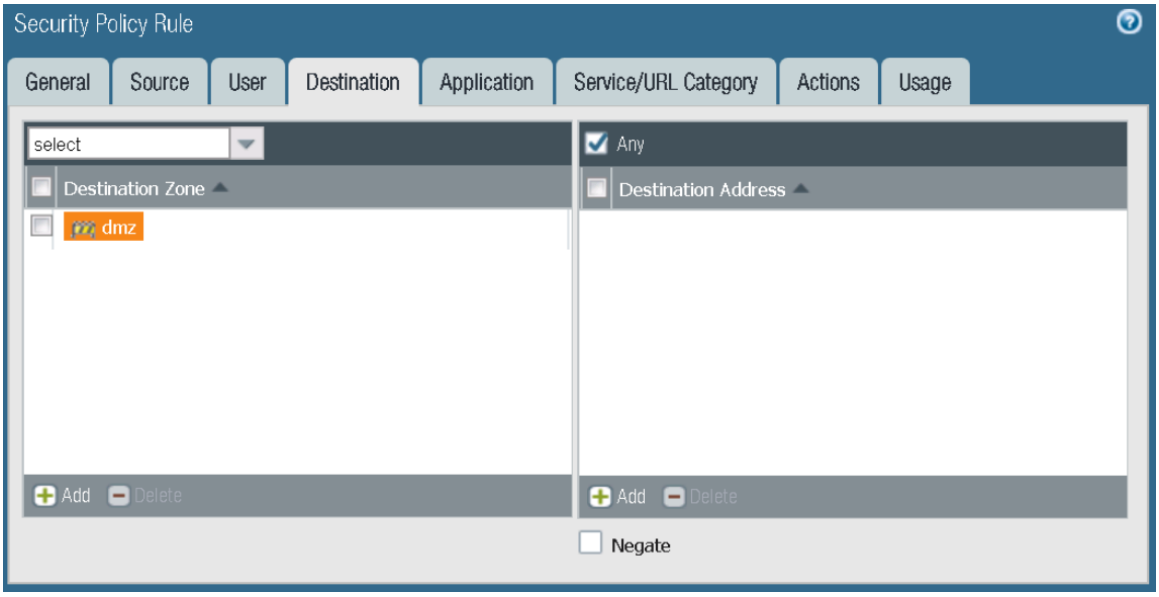
Parameter	Value
Source Zone	Click **Add** and select **inside**
Source Address	Verify that the **Any** check box is selected



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

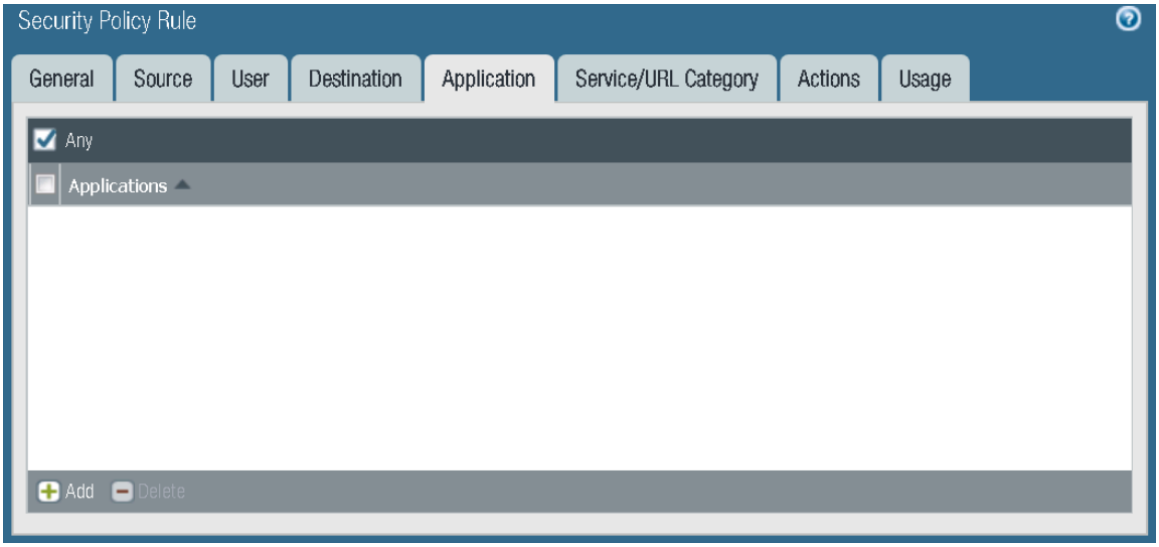
Parameter	Value
Destination Zone	Click **Add** and select **dmz**
Destination Address	Verify that the **Any** check box is selected

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com



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

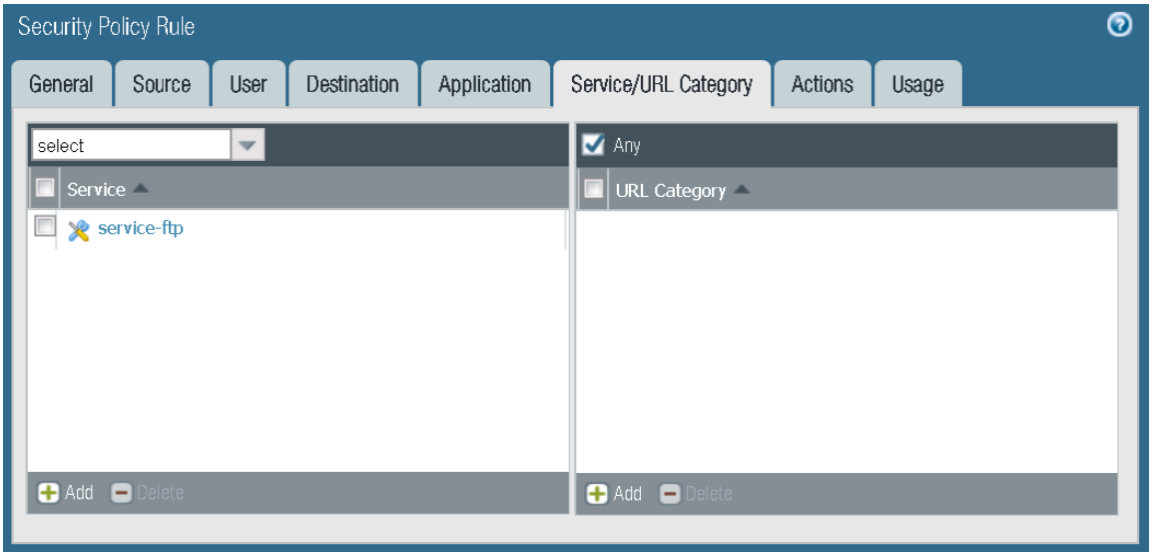
Parameter	Value
Applications	Verify that the **Any** check box is selected



19. Click the **Service/URL Category** tab and verify the following:

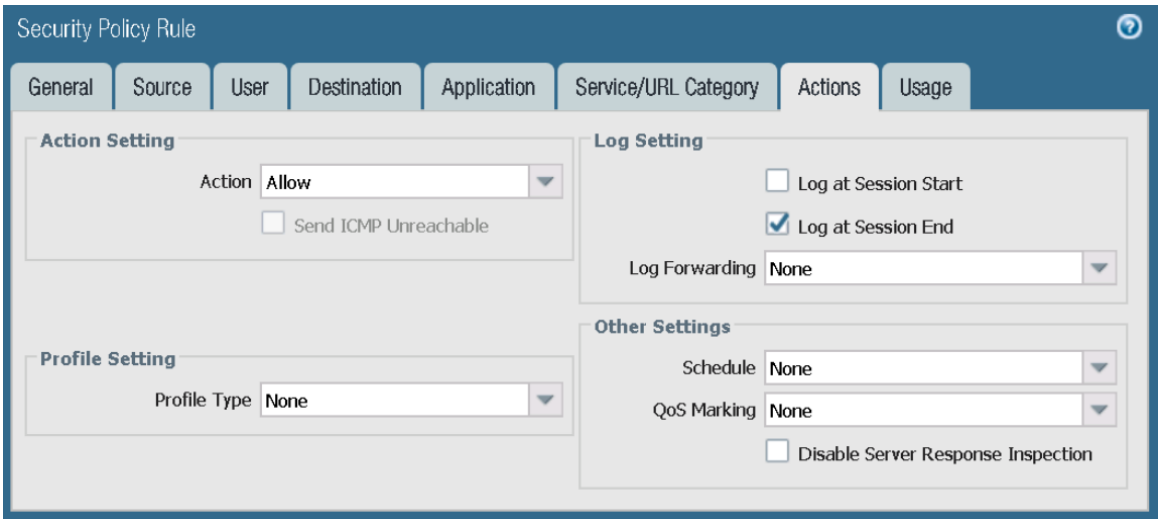
Parameter	Value
Service	Click **Add** and select **service-ftp** from the drop-down menu
URL Category	Verify that the **Any** check box is selected

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com



20. Click the **Actions** tab and verify the following:

Parameter	Value
Action	Verify that **Allow** is selected
Log Setting	Verify that **Log at Session End** is selected



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

    A new Security policy should appear in the web interface.

22. Select the **internal-dmz-ftp** Security policy rule without opening it and click **Disable**:

Notice that the **internal-dmz-ftp** rule now is grayed out and in italics:

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

23. Verify that your configuration is like the following:

	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Ap...	Service	Action
1	egress-outside	egress	universal	inside	any	any	any	outside	any	any	application-default	Allow
2	internal-dmz-ftp	internal	universal	inside	any	any	any	dmz	192.168.1.1	any	service-ftp	Allow
3	migrated-ftp-port-based	internal	universal	inside	any	any	any	dmz	any	any	service-ftp	Allow
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
5	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny

24. **Commit** your configuration changes.

5.3 Test the Port-Based Security Policy

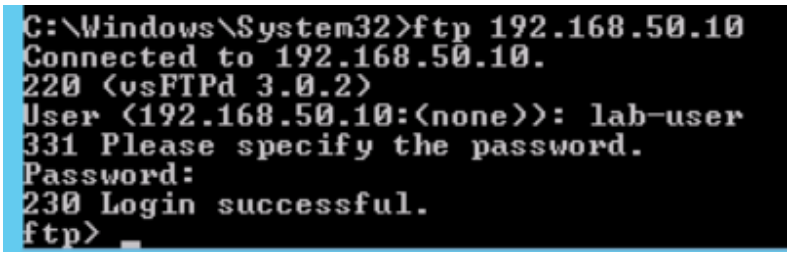
In this section, you will generate FTP traffic from the Windows host to the Linux host in the dmz zone. Then you will examine the Traffic log to view how the firewall processed the FTP traffic. After you complete this section, you will move on to other tasks related to App-ID. At the end of this lab you will return to the task of migrating the FTP port-based rule to an application-based rule. If the beginning of the next hour passes by the time you reach the end of this lab, the Policy Optimizer tool will have been populated with information about the FTP port-based rule.

25. On the Windows desktop, open a **CMD** window.
26. In the **CMD** window, type **`ftp 192.168.50.10`**

    You should be connected to the FTP server.
27. Log in using the following information:

Parameter	Value
Name	**`lab-user`**
Password	**`paloalto`**

The login should succeed, although 30 seconds might pass until authentication completes.



28. Type **`bye`** at the FTP command prompt.

    This command should end the FTP session. An FTP session will be logged on the firewall even though no data was transferred.
29. Type **`exit`** to close the **CMD** window.
30. In the web interface, select **Monitor** > **Logs** > **Traffic**.

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

You may need to manually refresh the log to view the current log entries.

31. Locate the log entry for the FTP session.

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
		02/19 21:56:10	end	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	allow	migrated-ftp-port-based

Which Security policy rule matched the session and allowed the FTP traffic?

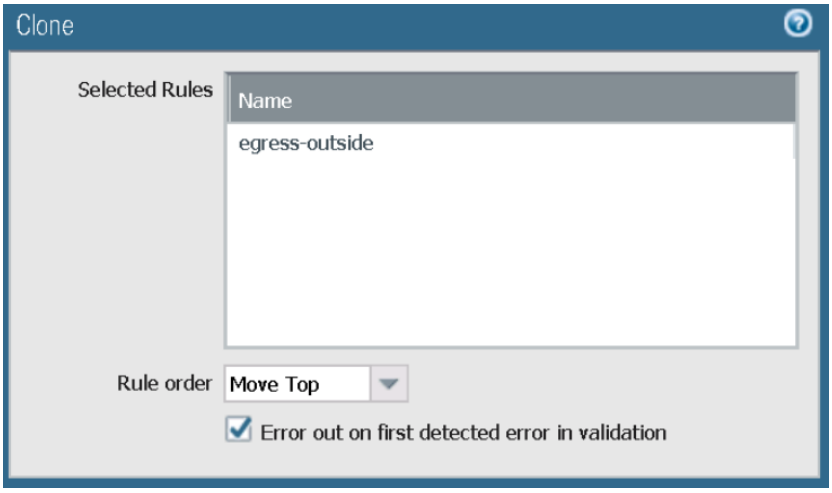
It should be "migrated-ftp-port-based."

5.4 Create an App-ID Security Policy Rule

32. In the web interface, select **Policies** > **Security**.
33. Select the **egress-outside** Security policy rule without opening it.
34. Click **Clone**:

The **Clone** configuration window should appear. Note that you do not have to use **Clone** to create new rules. You always can create them using the **Add** button.

35. On the **Rule order** drop-down list, select **Move top**:



Remember that rule order is important! The firewall compares a packet's characteristics to each rule in the Security Policy starting in order.

36. Click **OK** to close the **Clone** configuration window:

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

	Name	Tags	Type	Source				Destination		Ap...	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address			
1	egress-outside-1	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
3	*internal-dmz-ftp*	*internal*	*universal*	*inside*	*any*	*any*	*any*	*dmz*	*192.168.1.1*	*any*	*service-ftp*	*Allow*
4	migrated-ftp-port-based	internal	universal	inside	any	any	any	dmz	any	any	service-ftp	Allow
5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
6	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny

A new Security policy rule named **egress-outside-1** should be added to the top of the Policy order.

37. With the original **egress-outside** Security policy rule still selected, click **Disable**:

Notice that the egress-public rule now is grayed out and in italics:

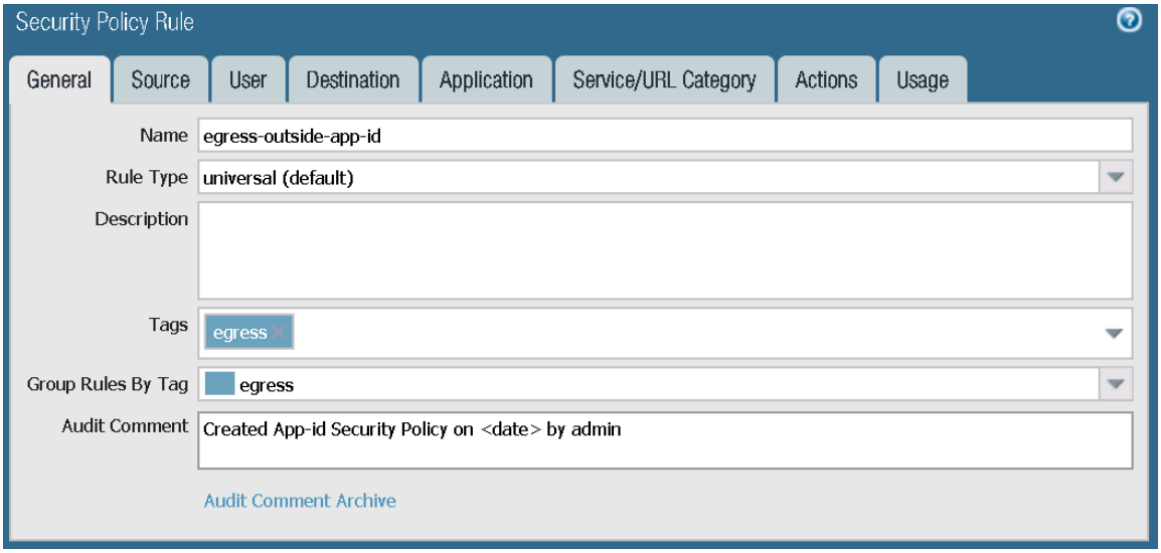
Be sure to disable this rule before proceeding.

38. Click the cloned Security policy rule **egress-outside-1** to configure the policy.

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

39. Configure the following:

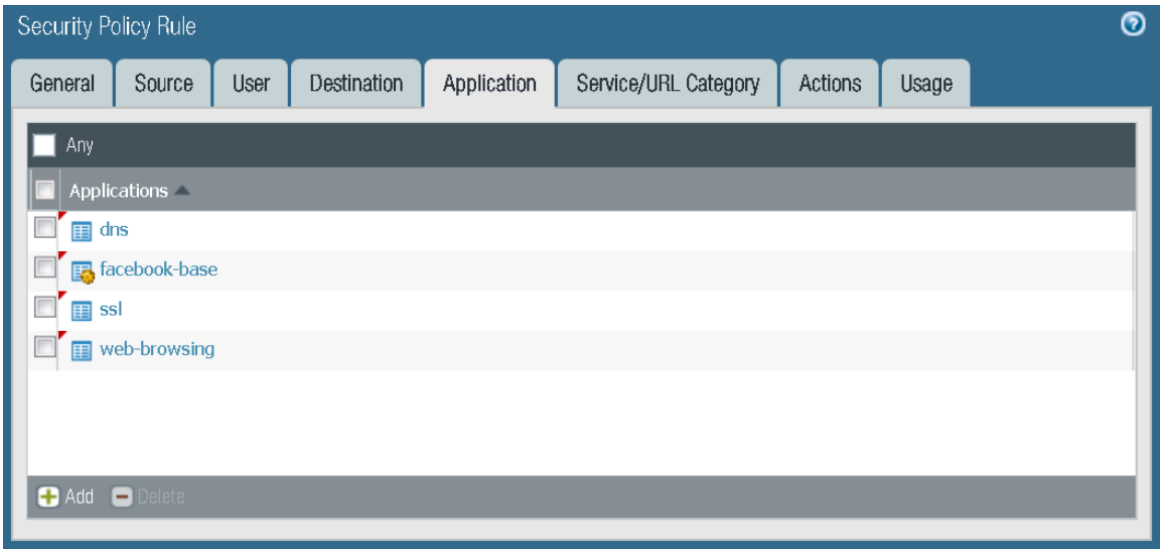
Parameter	Value
Name	**Rename policy to `egress-outside-app-id`**
Audit Comment	**Type `Created App-id Security Policy on <date> by <Your-Role>`**



Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

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

Parameter	Value
Applications	**Click Add and select the following from the drop-down list:** **dns** **facebook-base** **ssl** **web-browsing**



The firewall matches traffic to the list of applications in a Security policy rule. If the firewall detects a change in an application, or an application shift, the firewall will rematch the traffic to the list of applications in the Security policy.

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

5.5 Enable Interzone Logging

Two default security rules are in place: "intrazone-default" and "interzone-default." Both default security rules are read-only, but you can override them and make minimal changes. One change you should make is to enable **Log at Session End** on the "interzone-default" rule.

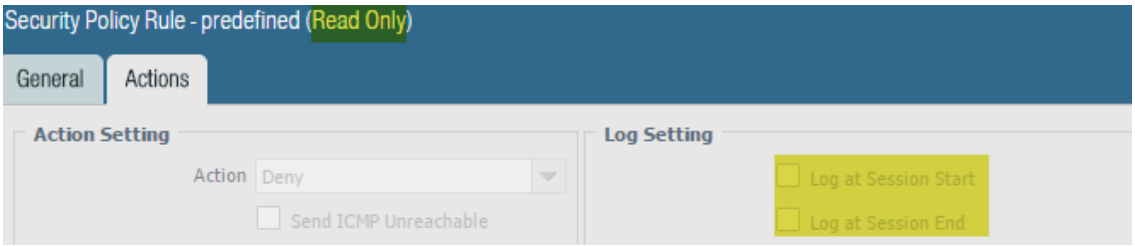
42. Click the Security policy rule **interzone-default** to configure the policy.

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

43. Click the **Actions** tab.

    Note that Security policy rule is in Read Only mode. In Read Only mode **Log at Session Start** and **Log at Session End** are deselected and cannot be edited:

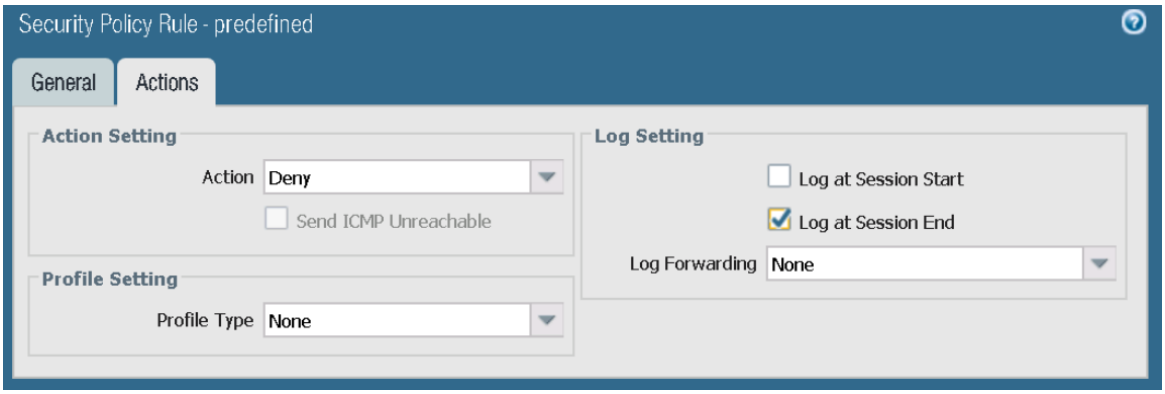
Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com



44. Click **Cancel**.
45. With the **interzone-default** policy rule selected but not opened, click **Override**:

The **Security Policy Rule – predefined** window should appear.

46. Click the **Actions** tab.
47. Select **Log at Session End**:



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

5.6 Enable the Application Block Page

In this section you will enable the **Application Block Page**.

49. In the web interface, select **Device > Response Pages**.
50. Select the **Application Block Page** without opening it:

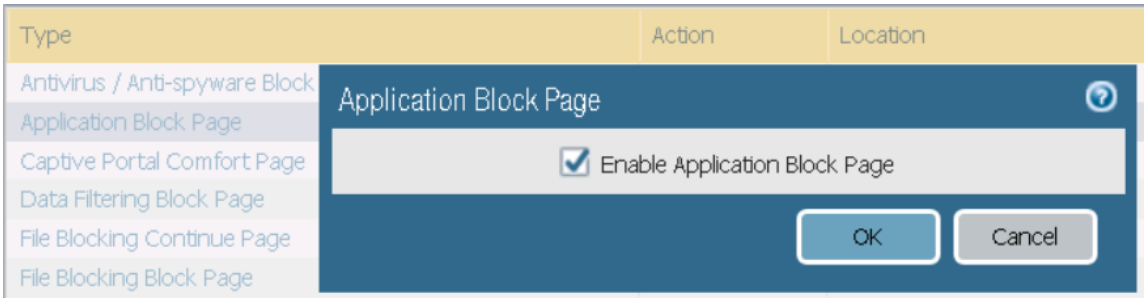
Type	Action	Location
Antivirus / Anti-spyware Block Page		Default
Application Block Page	Disabled	Default
Captive Portal Comfort Page		Default

51. Click the **Disabled** link to the right of the **Application Block Page**.

The **Application Block Page** window should appear.

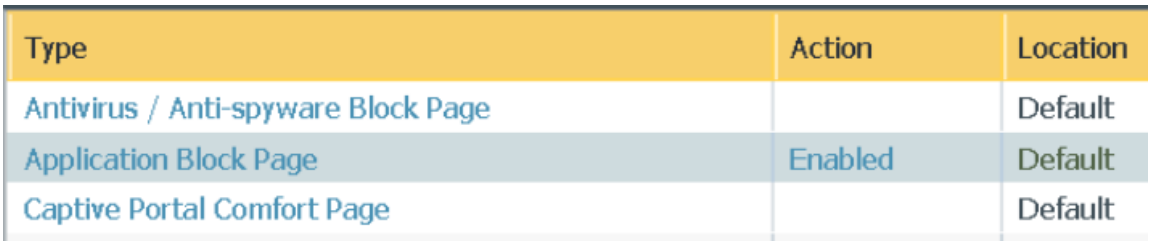
Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

52. Select the **Enable Application Block Page** check box:



The firewall can present the **Application Block Page** only if it detects and blocks a web-based application. Blocked applications that do not use a web browser will be stopped but the user will not necessarily know why.

53. Click **OK** to close the **Application Block Page** configuration window.



Type	Action	Location
Antivirus / Anti-spyware Block Page		Default
Application Block Page	Enabled	Default
Captive Portal Comfort Page		Default

The **Application Block Page** now should be enabled.

54. **Commit** all changes.

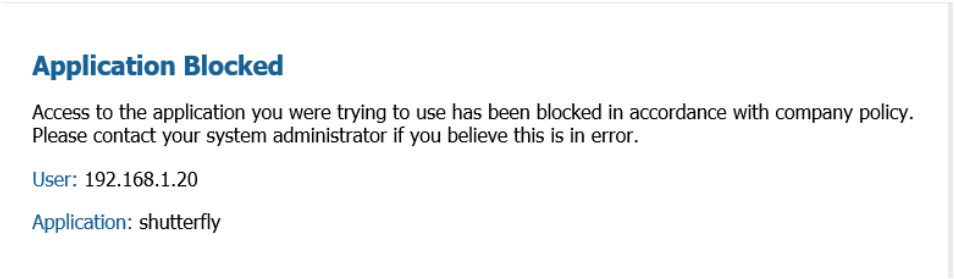
5.7 Test Application Blocking

55. Open a new Internet Explorer browser window in private/incognito mode and browse to **`www.facebook.com`** and **`www.msn.com`**.

    You should be able to successfully connect to the Facebook and MSN websites.

56. Using the same browser, browse to **`www.shutterfly.com`** and **`www.metacafe.com`**.

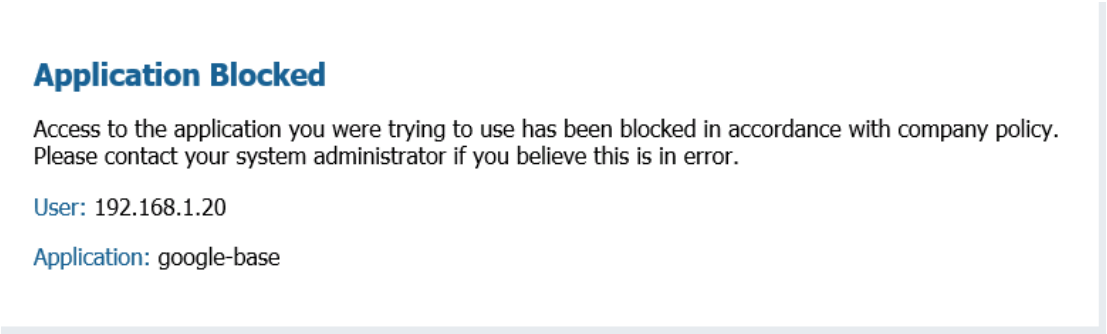
    An **Application Blocked** Page opens, which indicates that the *shutterfly* and *metacafe* applications have been blocked. If the Application Blocked page doesn't display, try a different browser. If the Application Blocked page still doesn't appear than disregard and proceed to Review Logs to confirm the application traffic was denied.



Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

Why could you browse to Facebook and MSN but not to Shutterfly or metacafe? MSN currently does not have a unique and specific Application signature. Therefore, App-ID identifies it using the Application signature web-browsing. However, an Application signature exists for Shutterfly and metacafe, and currently it is not allowed in any of the firewall Security policy rules.

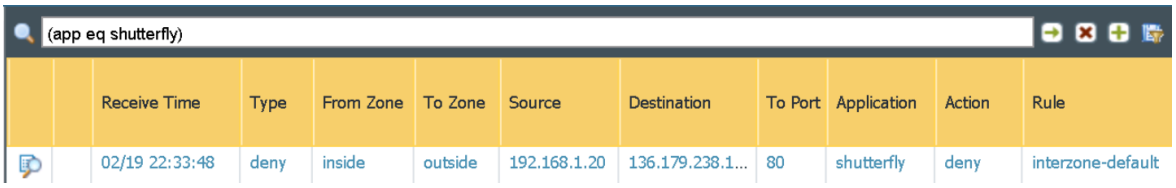
57. Browse to **`www.google.com`** using Internet Explorer and verify that google-base also is being blocked:



5.8 Review the Logs

58. In the web interface, select **Monitor** > **Logs** > **Traffic**.
59. In the log filter text box, type **`(app eq shutterfly) and`** press the **Enter** key.

    Only log entries whose Application is shutterfly should be displayed.



5.9 Test Application Blocking

In this section, you will attempt to work around the firewall's denial of access to Shutterfly by using a web proxy.

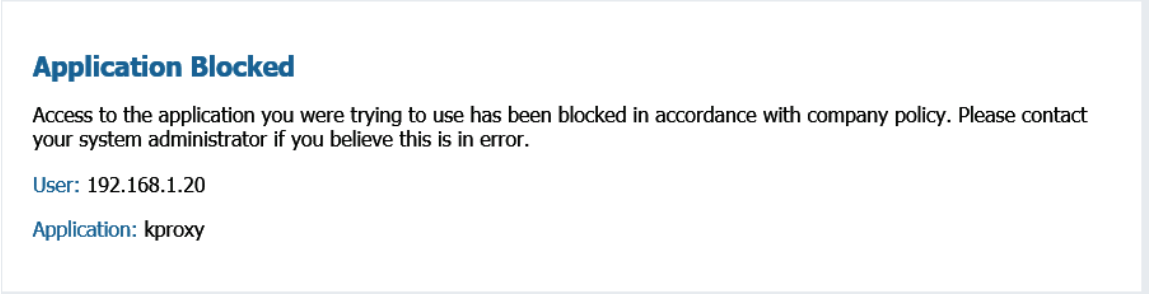
60. In Internet Explorer, browse to **`kproxy.com`**.

    Note: If kproxy.com is not available, try using php-proxy.com.

61. Enter **`www.shutterfly.com`** in the text box and click **surf!**:

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

An **Application Blocked** page opens that shows that the application was blocked:



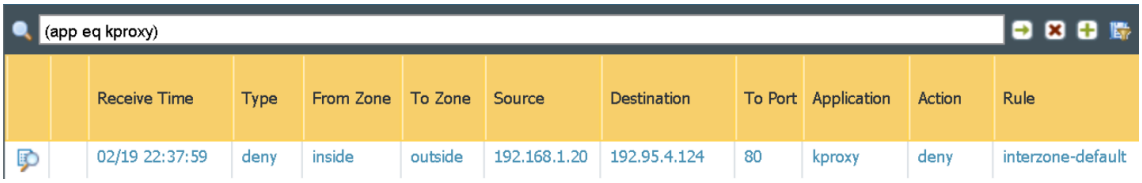
If the Application Blocked page doesn't display, try a different browser. If the Application Blocked page still doesn't appear than disregard and proceed to Review Logs to confirm the application traffic was denied.

62. Close all browser windows except for the firewall web interface.

5.10 Review the Logs

63. In the web interface, select **Monitor** > **Logs** > **Traffic**.
64. Clear the log filter text box and type **`(app eq kproxy) and`** press the **Enter** key.

    The Traffic log entries indicate that the kproxy application has been blocked:



(app eq kproxy)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
		02/19 22:37:59	deny	inside	outside	192.168.1.20	192.95.4.124	80	kproxy	deny	interzone-default

Based on the information from the Traffic log, Shutterfly and kproxy are denied by the "interzone-default": Security policy rule.

Note: If the logging function of your "interzone-default" rule is not enabled, no information would be provided via the Traffic log.

5.11 Modify the App-ID Security Policy Rule

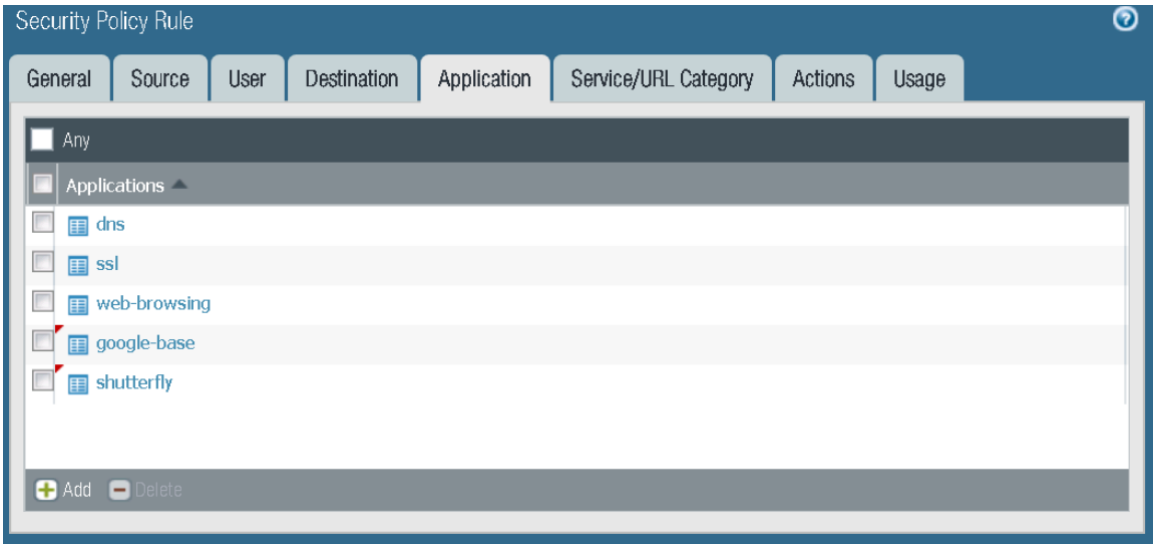
65. In the web interface, select **Policies** > **Security**.
66. Click to open the **egress-outside-app-id** Security policy rule.

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

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

Parameter	Value
Applications	**`Add google-base and shutterfly`**
Applications	**`Remove facebook-base`**

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com



68. Click **OK** to close the **Security Policy Rule** configuration window.
69. **Commit** all changes.

5.12 Test the App-ID Changes

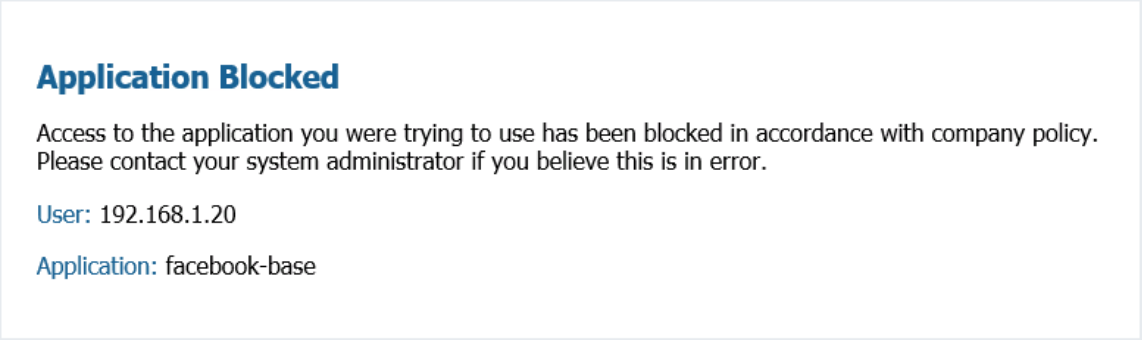
70. Open a new Internet Explorer browser in private/incognito mode and browse to **`www.shutterfly.com`** and **`www.google.com`**.

    The **Application Blocked Page** no longer should be displayed.

71. Browse to **`www.facebook.com`**.

    Note: Do not use any previously used browser windows because browser caching can cause incorrect results.

    The **Application Blocked Page** now appears for facebook-base.



72. Close all browser windows except for the firewall web interface.

    Note: The web-browsing Application signature applies only to browsing that does not match any other Application signature.

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

5.13 Observe the Application Command Center

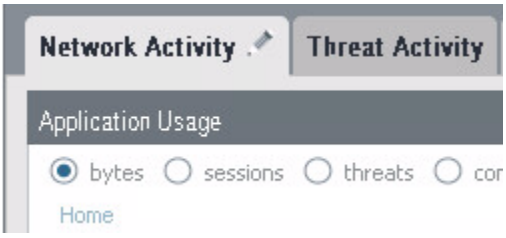
The Application Command Center, or ACC, is an analytical tool that provides useful intelligence on activity within your network. The ACC uses the firewall logs as the source for graphically depicting traffic trends on your network. The graphical representation enables you to interact with the data and visualize the relationships between events on the network, including network use patterns, traffic patterns, and suspicious activity and anomalies.

73. Click the **ACC** tab to access the Application Command Center:

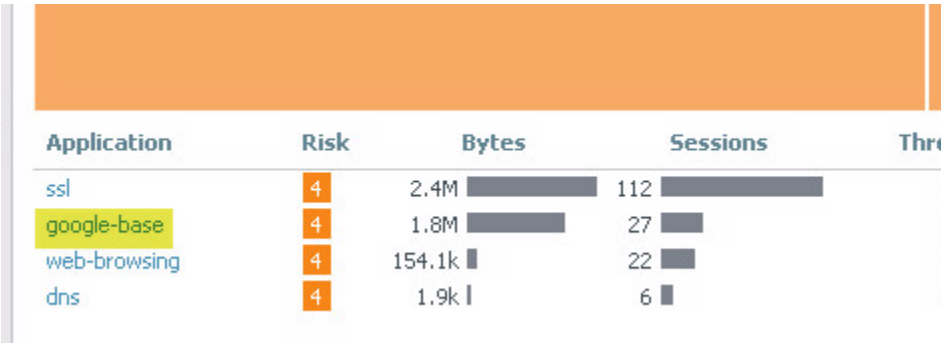
74. Note that the upper-right corner of the ACC displays the total risk level for all traffic that has passed through the firewall thus far:

Your results may differ from the score shown.

75. On the **Network Activity** tab, the **Application Usage** pane shows application traffic generated so far (because the ACC relies on log aggregation, you may need to wait 15 minutes before the ACC displays all applications):



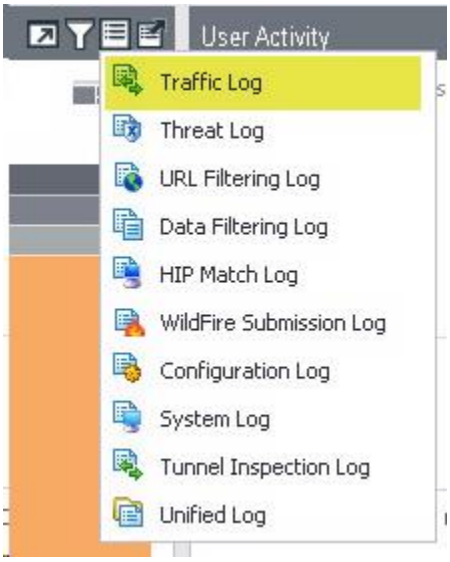
76. You can click any application listed in the **Application Usage** pane; *google-base* is used in this example:



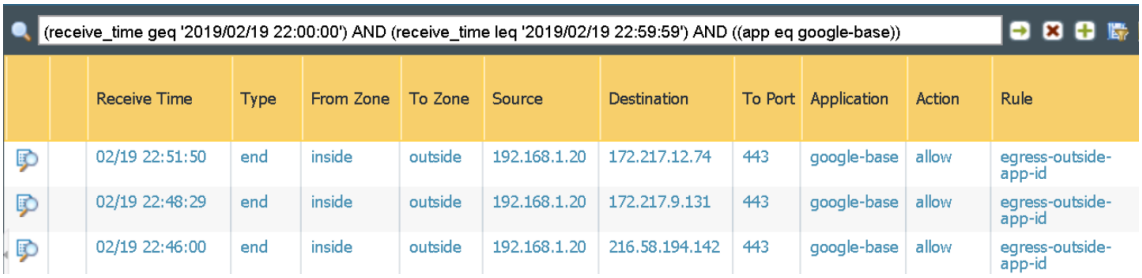
Notice that the **Application Usage** pane updates to present only google-base information.

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

77. Click the icon and select **Traffic Log**:



After the **Traffic Log** is selected, a link automatically is made to the applicable log information with the filter set for a relevant time frame and for the google-base application. It may take 15 minutes or longer for the traffic to appear in your firewall appliance running on VMware Workstation.



Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
02/19 22:51:50	end	inside	outside	192.168.1.20	172.217.12.74	443	google-base	allow	egress-outside-app-id
02/19 22:48:29	end	inside	outside	192.168.1.20	172.217.9.131	443	google-base	allow	egress-outside-app-id
02/19 22:46:00	end	inside	outside	192.168.1.20	216.58.194.142	443	google-base	allow	egress-outside-app-id

5.14 Create an FTP Application-Based Security Policy Rule

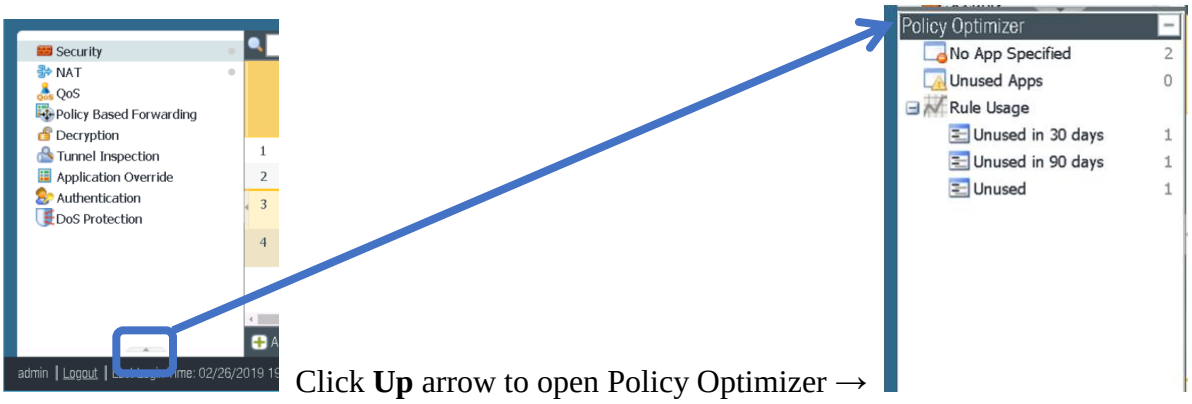
The goal of this exercise is to simulate the process of migrating from a port-based rule to an application-based rule. At the beginning of this lab exercise you created a port-based rule that allowed FTP traffic from the inside zone to the dmz zone and then opened an FTP session to the dmz zone. By now the beginning of the hour has passed so the Policy Optimizer tool should have recorded the FTP traffic through the port-based FTP rule, which will enable you to use the Policy Optimizer tool to migrate from the port-based rule to an application-based rule.

In this section, you will use the Policy Optimizer tool's cloning method to create an application-based rule to match and allow FTP traffic from the inside zone to the dmz zone.

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

 Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

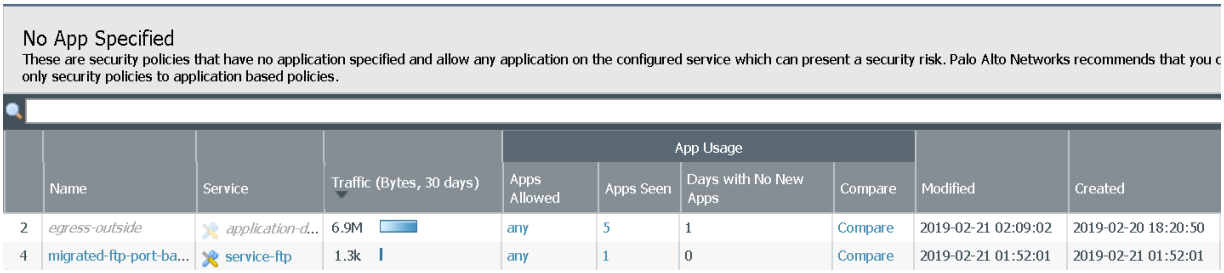
79. If necessary, open the **Policy Optimizer** panel by clicking the **up-arrow** beneath the list of policies on the left side of the web interface.



Click **Up** arrow to open Policy Optimizer →

80. Select **Policy Optimizer** > **No App Specified**.

The **No App Specified** window should open.



81. How many applications have been seen by the "migrated-ftp-port-based" rule?

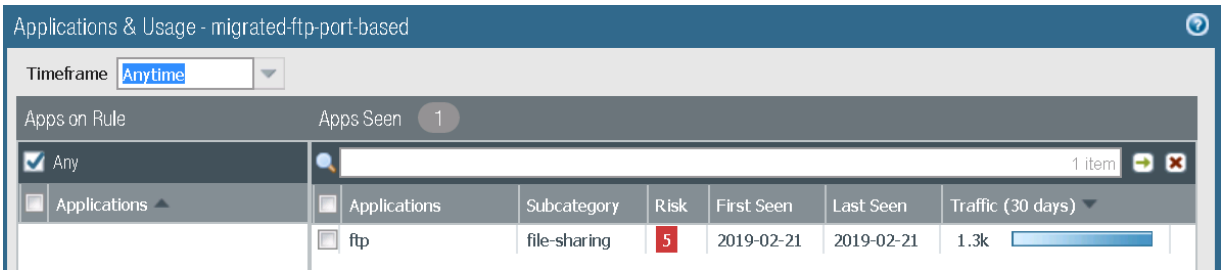
The number **1** in the **Apps Seen** column indicates that only a single application has been seen by this port-based rule. However, this window does not tell you which application. Please make sure you have allowed enough time in step 77 above for your traffic to show up in your logs. This may take up to 30 minutes.

82. Click **Compare** in the "migrated-ftp-port-based" rule's row.

The **Applications & Usage – migrated-ftp-port-based** window should open.

83. Which application has been seen by the "migrated-ftp-port-based" rule?

It should have been the *ftp* application.



84. Click the **ftp** check box to select the application:

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

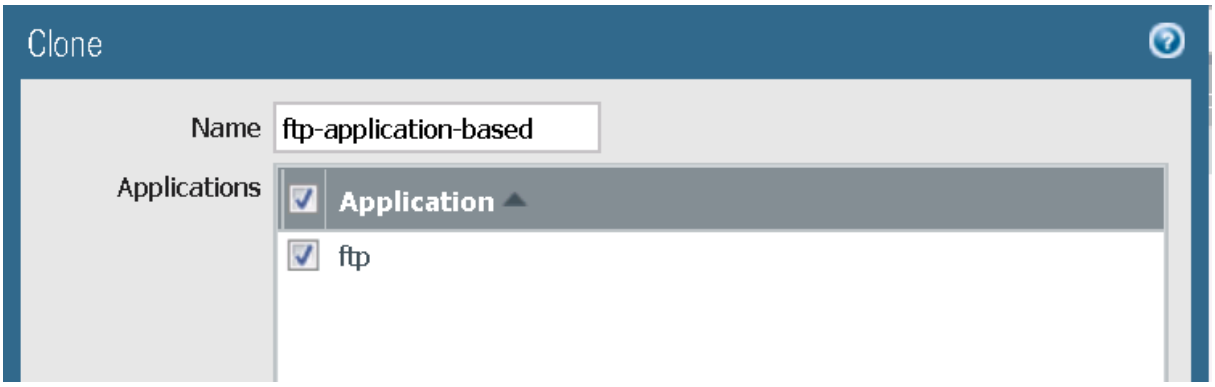
Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
ftp	file-sharing	5	2019-02-21	2019-02-21	1.3k

85. Click **Create Cloned Rule** to create an application-based FTP rule:

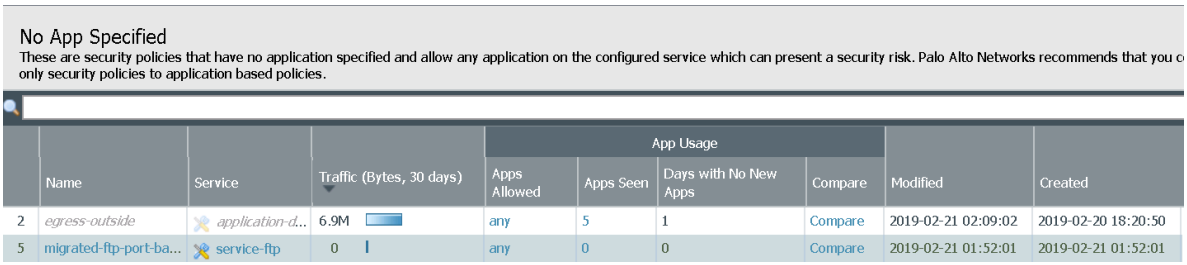
A **Clone** window should open.

86. Configure the following:

Parameter	Value
Name	Type **`ftp-application-based`**
Applications	Verify **ftp** is selected



87. Click **OK** to close the **Clone** window.
88. In the **No App Specified** window, now how many applications are listed in the **Apps Seen** column of the "migrated-ftp-port-based" rule?



The number should be **0** because the firewall has moved the ***ftp*** application from the migrated-ftp-port-based rule to the new ftp-application-based rule.

89. Select **Policies** > **Security** to redisplay the Security policy.

The **No App Specified** window should close.

90. Has a new "ftp-application-based" rule been added to your Security policy?

It should have been.

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

91. To which location in the Security policy rule hierarchy did the Policy Optimizer tool move the new “ftp-application-based” rule?

    It should directly precede the “migrated-ftp”-port-based rule and match FTP traffic before the “migrated-ftp”-port-based rule.

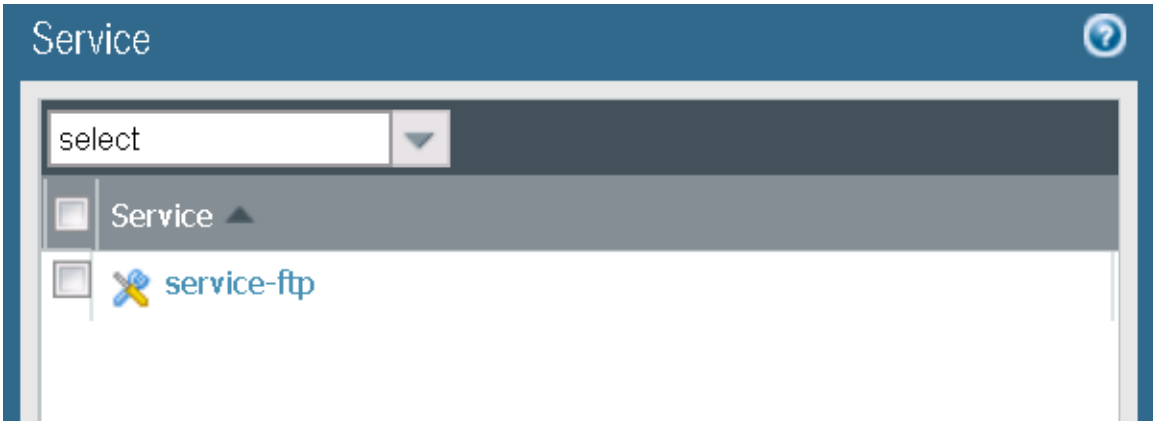
				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Ap...	Service	Action
1	egress-outside-app-id	egress	universal	inside	any	any	any	outside	any	... ...	application-default	Allow
2	egress-outside	egress	universal	inside	any	any	any	outside	any	any	application-default	Allow
3	internal-dmz-ftp	internal	universal	inside	any	any	any	dmz	192.168.1.1	any	service-ftp	Allow
4	ftp-application-based	internal	universal	inside	any	any	any	dmz	any	...	service-ftp	Allow
5	migrated-ftp-port-based	internal	universal	inside	any	any	any	dmz	any	any	service-ftp	Allow

92. Which service is listed in the **Service** column of the “ftp-application-based” rule?

    It should be the **service-ftp** service.

93. On the “ftp-application-based” rule, click “service-ftp” in the **Service** column.

    A **Service** window should open.



94. Select the **service-ftp** check box and then click **Delete** to delete the service.
95. Which service now is listed?
96. Click **OK** to close the **Service** window.

4	ftp-application-based	internal	universal	inside	any	any	any	dmz	any	...	application-default	Allow
5	migrated-ftp-port-based	internal	universal	inside	any	any	any	dmz	any	any	service-ftp	Allow

    It should be application-default.

97. **Commit** your configuration changes.

5.15 Test the Application-Based Security Policy

In this section, you will generate FTP traffic from the Windows host to the Linux host. Then you will examine the Traffic log to view how the firewall processed the FTP traffic. The FTP traffic should match the application-based rule and not the port-based rule.

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

98. On the Windows desktop, open a **CMD** window.
99. In the **CMD** window, type **`ftp 192.168.50.10.`**

    You should be connected to the FTP server.
100. Log in using the following information:

Parameter	Value
Name	**`lab-user`**
Password	**`paloalto`**

The login should succeed, although 30 seconds might pass until authentication completes.

```
C:\Windows\System32>ftp 192.168.50.10
Connected to 192.168.50.10.
220 (vsFTPd 3.0.2)
User (192.168.50.10:(none)): lab-user
331 Please specify the password.
Password:
230 Login successful.
ftp> _
```

101. Type **bye** at the FTP command prompt.

     This command should end the FTP session. An FTP session should be logged on the firewall even though no data was transferred.
102. Type **exit** to close the **CMD** window.
103. In the web interface, select **Monitor** > **Logs** > **Traffic**.
104. Clear any existing log filters. Locate the log entry for the FTP session.

     You also can apply a new log filter **`(app eq ftp)`** to help you find it.

     Which Security policy rule matched and allowed the FTP traffic?

     It should be the "ftp-application-based" rule. It may take more than 15 minutes for the traffic to show up in your firewall appliance traffic log running on VMware Workstation.

(app eq ftp)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
		02/21 04:40:33	end	inside	dmz	192.168.1.20	192.168.50.10	21	ftp	allow	ftp-application-based

Note: In a real migration, you would disable the port-based rule for a short period and wait to see if any FTP sessions are affected. After you are confident that the new application-based rule is matching all required FTP traffic, you would delete the port-based rule.

Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com

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

 Copyright © 2018 Palo Alto Networks, Inc. www.paloaltonetworks.com