



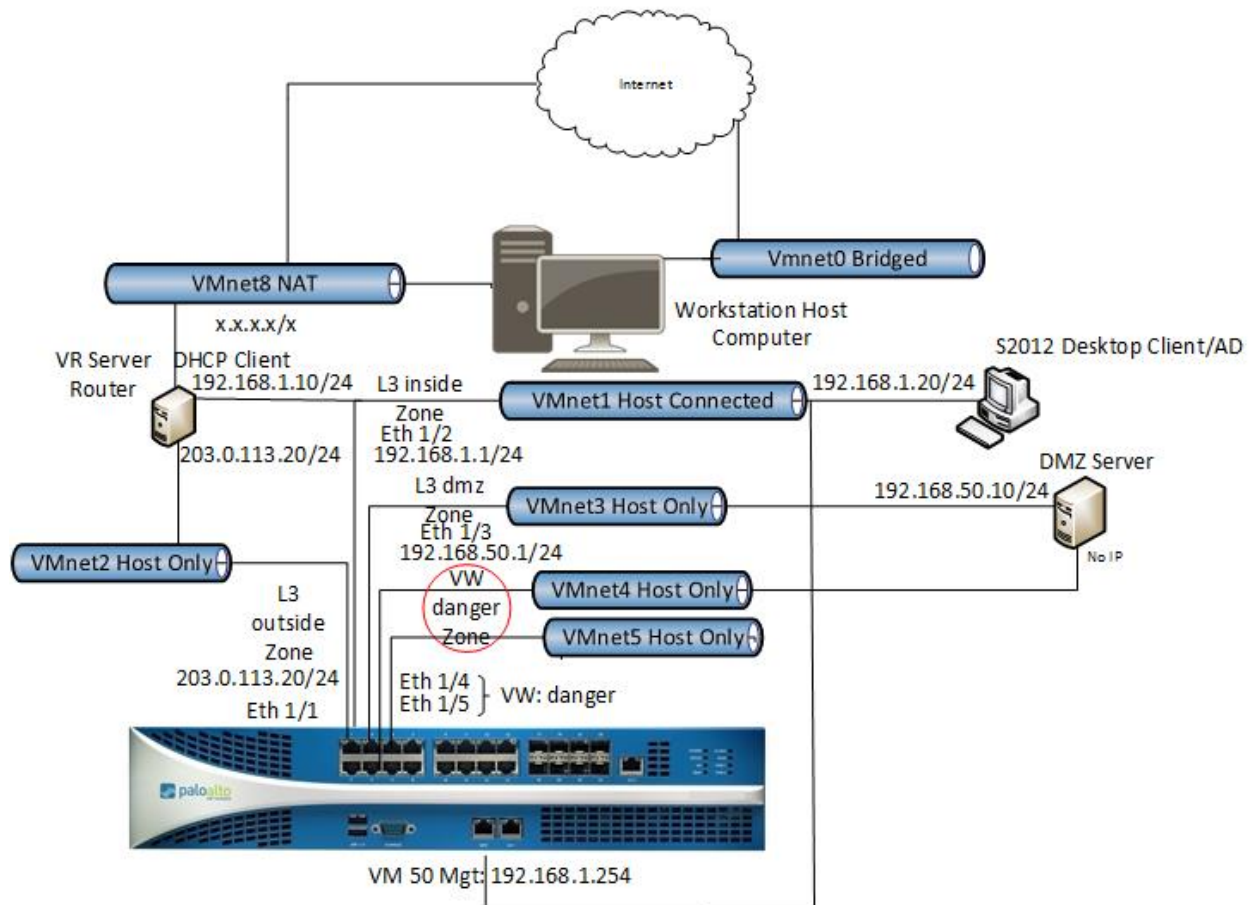
# **Palo Alto Networks Academy Labs Lab 4 App-ID**

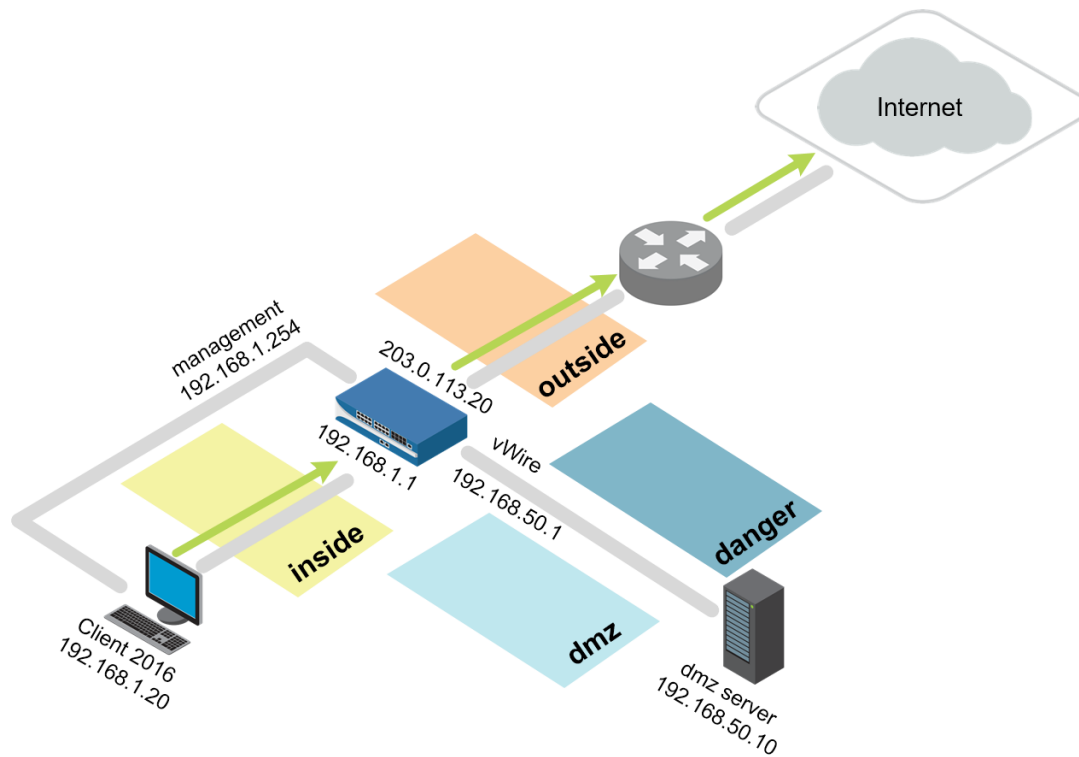
**Document Version: 2018-11-10**

Copyright © 2018 Palo Alto Networks, Inc.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

# Lab Topology

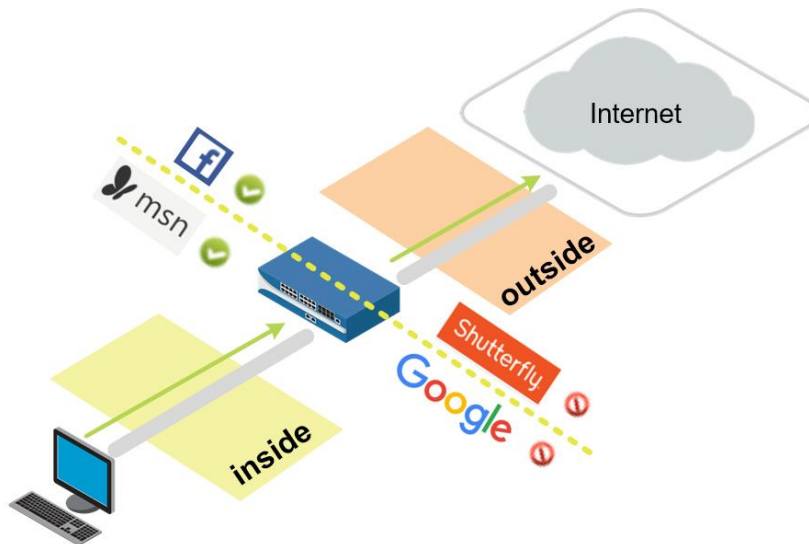




Virtual Machine	Username	Password
Firewall	admin	admin
Server 2012	lab-user	Pa10Alt0
Centos AAC DMZ	root	Pa10Alt0
Centos Virtual Router	root	Pa10Alt0

## Lab 4: App-ID

---

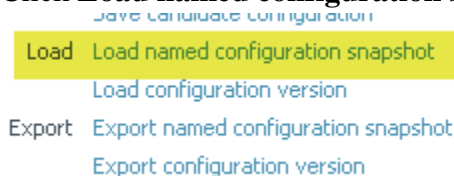



### Lab Objectives

- 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).

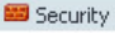


### 4.0 Load Lab Configuration

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



3. Select **edu-210-lab-04** and click **OK**.
4. Click **Close**.
5.  **Commit** all changes.

## 4.1 Create App-ID Security Policy Rule

6. Select **Policies > Security**. 
  7. Select the **egress-outside** Security policy rule without opening it.
  8. Click . The **Clone** configuration window opens.
  9. Verify that **Move top** is selected on the **Rule** order drop-down list.
  10. Click **OK** to close the **Clone** configuration window.
  11. With the original **egress-outside** Security policy rule still selected, click .
- Notice that the egress-public rule is now grayed out and in italics:



12. Click to open the cloned Security policy rule named **egress-outside-1**.
13. Configure the following:

Parameter	Value
Name	egress-outside-app-id

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

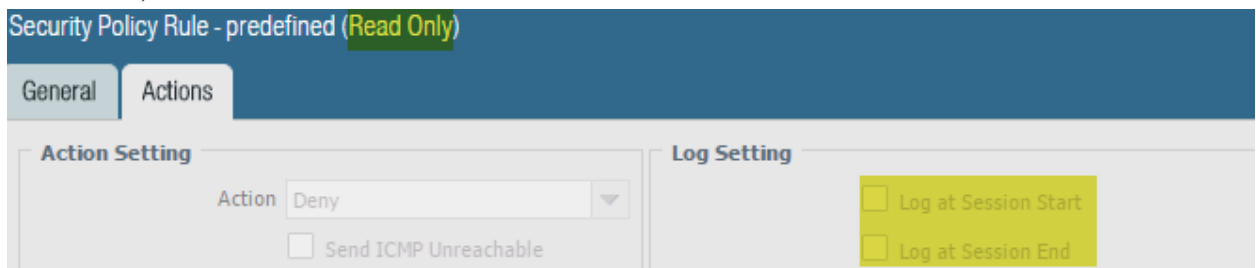
Parameter	Value
Applications	dns facebook-base ssl web-browsing


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

## 4.2 Enable Interzone Logging






The intrazone-default and interzone-default Security policy rules are read-only by default.

16. Click to open the **interzone-default** Security policy rule. 
17. Click the **Actions** tab. Note that **Log at Session Start** and **Log at Session End** are deselected, and cannot be edited:



18. Click **Cancel**.
19. With the **interzone-default** policy rule selected but not opened, click . The **Security Policy Rule – predefined** window opens.
20. Click the **Actions** tab.
21. Select **Log at Session End**.
22. Click **OK**.

## 4.3 Enable the Application Block Page

23. Select **Device > Response Pages**. 
24. Click **Disabled** to the right of **Application Block Page**:  

25. Select the **Enable Application Block Page** check box. 
26. Click **OK**. The **Application Block Page** should now be enabled:  

27.  **Commit** all changes.

## 4.4 Test Application Blocking

28. Open a new Internet Explorer browser window in private/incognito mode. You should be able to browse to [www.facebook.com](http://www.facebook.com) and [www.msn.com](http://www.msn.com).
29. Use private/incognito mode in a browser to connect to <http://www.shutterfly.com>. An **Application Blocked** page opens, indicating that the *shutterfly* application has been blocked:

### Application Blocked

Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 192.168.1.20

Application: shutterfly

Why could you browse to Facebook and MSN but not to Shutterfly? 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 currently it is not allowed in any of the firewall Security policy rules.

30. Browse to [www.google.com](http://www.google.com) using Internet Explorer and verify that google-base also is being blocked:

## Application Blocked

Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 192.168.1.20

Application: google-base

## 4.5 Review Logs


31. Go to the web interface and select **Monitor > Logs > Traffic**.



32. Type (app eq shutterfly) in the filter text box.

33. Press the **Enter** key.

Only log entries whose Application is shutterfly are displayed.

( app eq shutterfly )														
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	
	12/19 19:40:49	deny	inside	outside	192.168.1.20		136.179.23...	80	shutterfly	deny	interzone-default	policy-deny		497

## 4.6 Test Application Blocking

34. Try to work around the firewall's denial of access to Shutterfly by using a web proxy. In private/incognito mode in a browser, browse to **avoidr.com**.

35. Enter **www.shutterfly.com** in the text box near the bottom and click **Go**. An

**Application Blocked** page opens showing that the avoidr application was blocked:

### Application Blocked

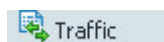
Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 192.168.1.20




Application: avoidr

## 4.7 Review Logs

36. Select **Monitor > Logs > Traffic**.



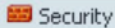

37. Type (app eq avoidr) in the filter text box. The Traffic log entries indicate that the avoidr application has been blocked:

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason
	03/08 02:17:20	deny	inside	outside	192.168.1.20		5.63.151.30	80	avoidr	deny	interzone-default	policy-deny
	03/08 02:16:23	deny	inside	outside	192.168.1.20		5.63.151.30	80	avoidr	deny	interzone-default	policy-deny
	03/08 02:15:52	deny	inside	outside	192.168.1.20		5.63.151.30	80	avoidr	deny	interzone-default	policy-deny

Based on the information from your log, Shutterfly and avoidr 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.

## 4.8 Modify the App-ID Security Policy Rule

38. In the web interface select **Policies > Security**. 
39. Add shutterfly and google-base to the egress-outside-app-id Security policy rule.
40. Remove facebook-base from the egress-outside-app-id Security policy rule.
41.  **Commit** all changes.

## 4.9 Test App-ID Changes

42. Open a new Internet Explorer browser in private/incognito mode and browse to [www.shutterfly.com](http://www.shutterfly.com) and [www.google.com](http://www.google.com). The **Application Blocked** page no longer is presented.
43. Open a new Internet Explorer browser window in private/incognito mode and browse to [www.facebook.com](http://www.facebook.com). **Note:** Do not use any previously used browser windows because browser caching can cause incorrect results.
44. The **Application Blocked** page now appears for facebook-base.

### Application Blocked

Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

**User:** 192.168.1.20

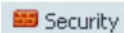
**Application:** facebook-base

45. Close all browser windows except for the firewall web interface.  
**Note:** The web-browsing Application signature applies to only browsing that does not match any other Application signature.



## 4.10 Migrate Port-Based Rule to Application-Aware Rule

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



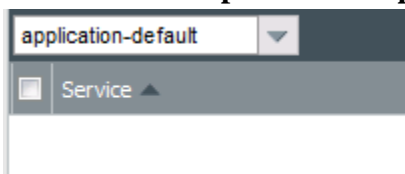
47. Click to open the **internal-dmz-ftp** Security policy rule:



48. Click the **Application** tab and add ftp.

49. Click the **Service/URL Category** tab.

50. Delete **service-ftp** and select **application-default**:



Selecting application-default does not change the service behavior because, in the application database, FTP is allowed only on port 21 by default.

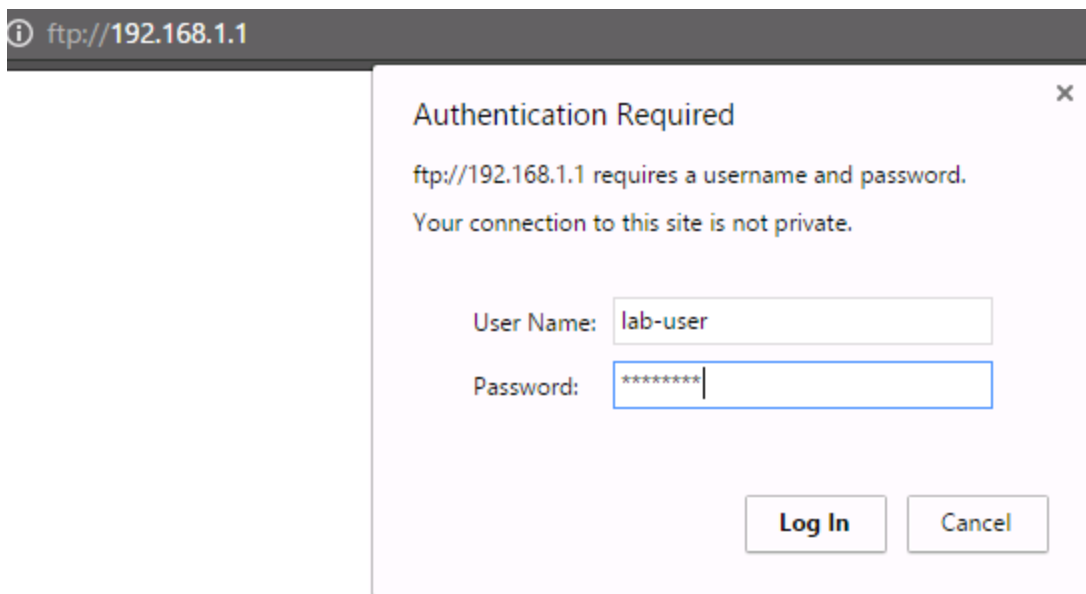
51. Click **OK**.

52.  **Commit** all changes.

53. Open a new Chrome browser window in incognito and browse to **ftp://192.168.1.1**.

54. At the prompt for login information, enter the following (credentials may be cached from a previous login):

Parameter	Value
User Name	lab-user
Password	paloalto



Notice that the connection succeeds and that you can log in to the FTP server with the updated Security policy rule.

## 4.11 Observe the Application Command Center

The Application Command Center (ACC) is an analytical tool that provides actionable 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.

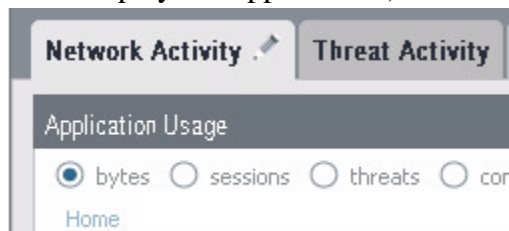
55. Click the **ACC** tab to access the Application Command Center:



56. 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:




57. On the **Network Activity** tab, the **Application Usage** pane shows application traffic generated so far (because log aggregation is required, 15 minutes might pass before the ACC displays all applications):

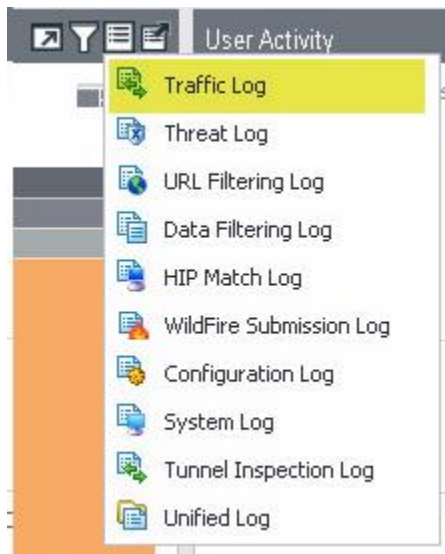


58. You can click any application listed in the **Application Usage** pane; *google-base* is used in this example:

Application	Risk	Bytes	Sessions	Thru
ssl	4	2.4M	112	
google-base	4	1.8M	27	
web-browsing	4	154.1k	22	
dns	4	1.9k	6	

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

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



Once the Traffic Log is selected, you automatically are linked to the applicable log information with the filter set for the google-base application:

(receive_time geq '2018/03/08 01:30:00') AND (receive_time leq '2018/03/08 02:29:59') AND ((app eq google-base))											
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
	03/08 02:29:01	end	inside	outside	192.168.1.20		216.58.194.46	443	google-base	allow	egress-outside-app-id
	03/08 02:26:41	end	inside	outside	192.168.1.20		216.58.194.36	443	google-base	allow	egress-outside-app-id
	03/08 02:26:37	end	inside	outside	192.168.1.20		216.58.194.36	443	google-base	allow	egress-outside-app-id
	03/08 02:26:37	end	inside	outside	192.168.1.20		172.217.12.34	443	google-base	allow	egress-outside-app-id



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