



## **PALO ALTO NETWORKS - EDU-210**

### **Lab 4: App-ID**

**Document Version: 2017-09-29**

Copyright © 2017 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc. EMC<sup>2</sup> is a registered trademark of EMC Corporation.

## Contents

Introduction .....	3
Objectives.....	3
Lab Topology .....	4
Lab Settings .....	5
4 Lab: App-ID.....	6
4.1 Load Lab Configuration .....	6
4.2 Create App-ID Security Policy Rule .....	7
4.3 Enable Interzone Logging .....	9
4.4 Enable the Application Block Page .....	11
4.5 Test Application Blocking .....	12
4.6 Review Logs .....	13
4.7 Test Application Blocking .....	14
4.8 Review Logs .....	14
4.9 Modify the App-ID Security Policy Rule .....	16
4.10 Test App-ID Changes .....	17
4.11 Migrate Port-Based Rule to Application-Aware Rule .....	17
4.12 Observe the Application Command Center.....	19

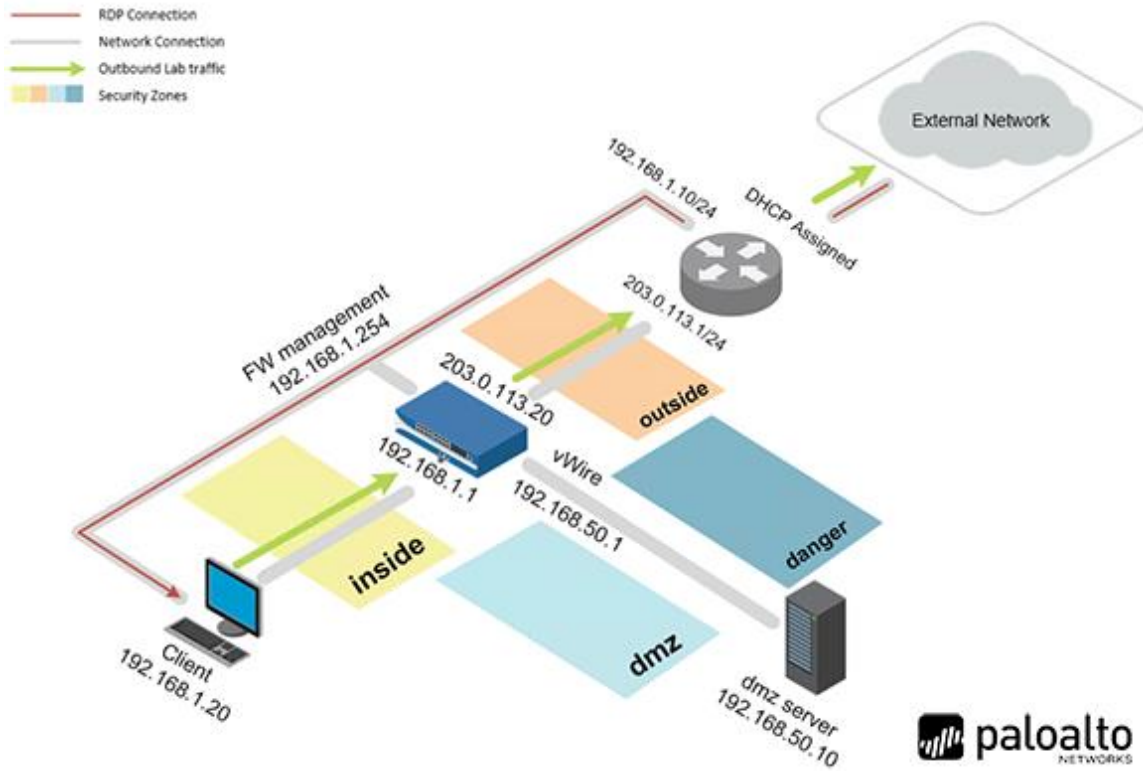
## Introduction

We have configured the interfaces and a basic security policy that allows any application. Since this is a next-generation firewall we want to allow only the applications that users need to complete their jobs. We will begin experimenting with the application id process to see how we can restrict these applications.

## Objectives

- Create an application-aware Security policy rule.
- Enable interzone logging.
- Enable the application block page for blocked applications.
- Test application blocking with different applications
- Understand what the signature web-browsing really matches.
- Migrate older port-based rule to application-aware.
- Review logs associated with the traffic and browse the Application Command Center (ACC).

## Lab Topology



## Lab Settings

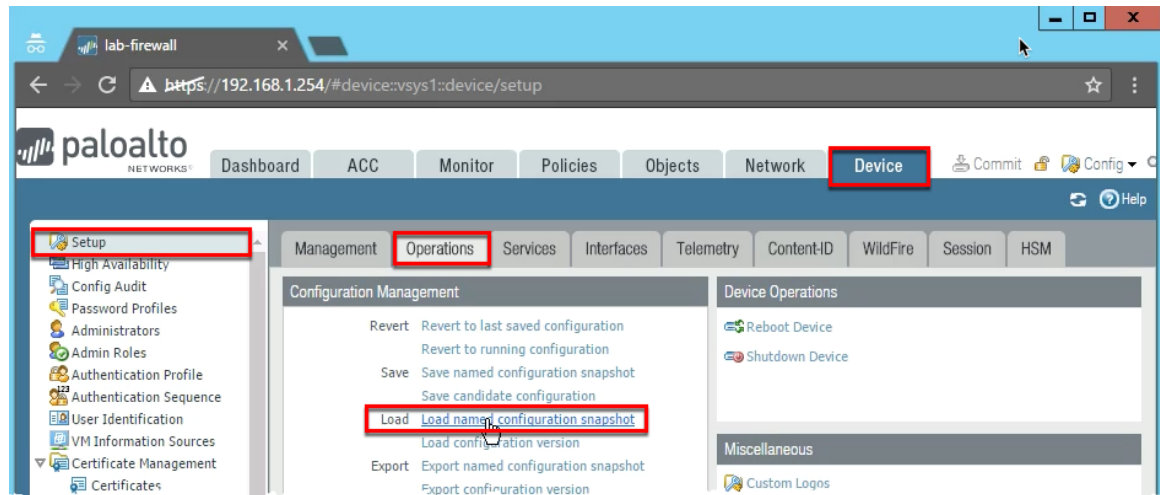
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client – Windows 2012 R2	192.168.1.20	lab-user	Pal0Alt0
Firewall – PA-VM	192.168.1.254	admin	admin

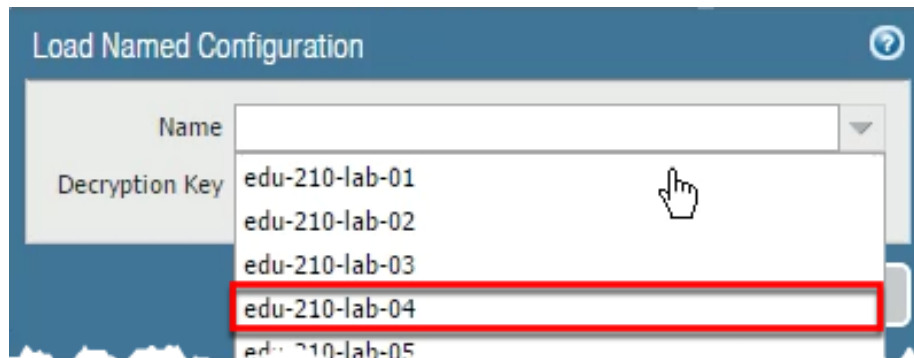
## 4 Lab: App-ID

### 4.0 Load Lab Configuration

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



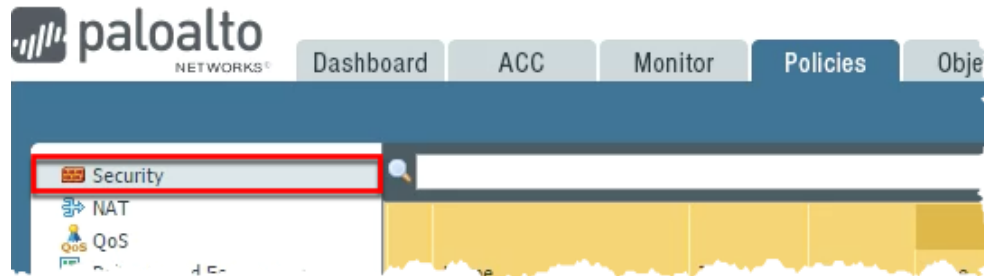
3. Select edu-210-lab-04 and click **OK**.



4. Click **Close**.
5. **Commit** all changes.

## 4.1 Create App-ID Security Policy Rule

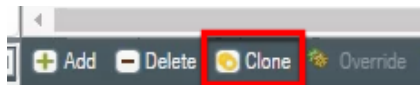
1. Select **Policies > Security**.



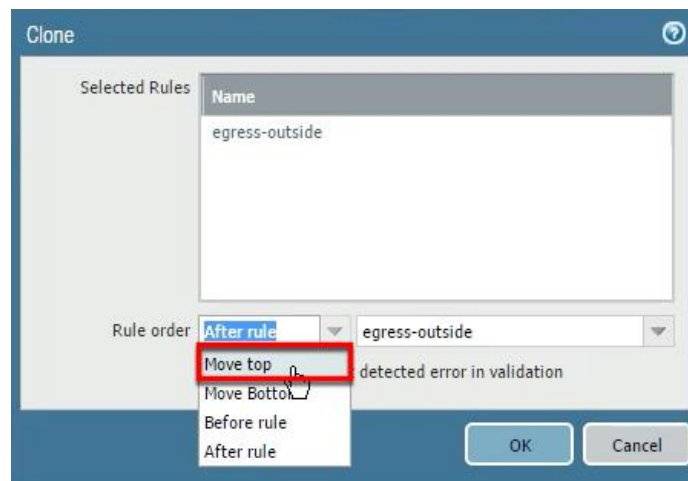
2. Select the **egress-outside** Security policy rule without opening it.

	Name	Tags	Type	Source				Destination	
				Zone	Address	User	HIP Profile	Zone	Address
1	egress-outside	egress	universal	inside	any	any	any	outside	any
2	internal-dmz-ftp	internal	universal	inside	any	any	any	dmz	192
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any
4									

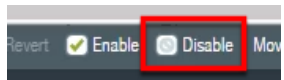
3. Click **Clone**. The Clone configuration window opens.



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



5. Click **OK** to close the **Clone** configuration window.
6. With the original **egress-outside** Security policy rule still selected, click **Disable**.

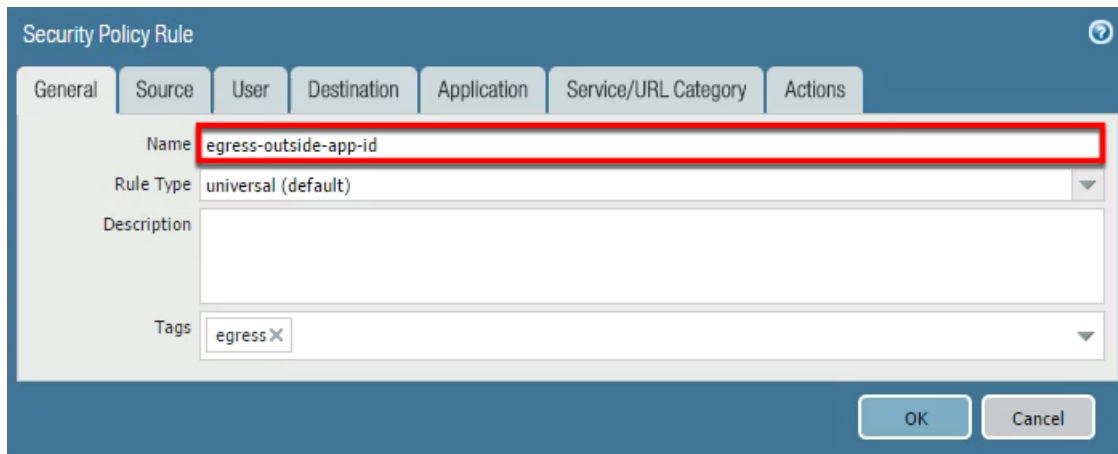


Notice that the egress-public rule is now grayed out and in italic fonts:

1	egress-outside-1	egress	universal	 inside	any
2	<i>egress-outside</i>	<i>egress</i>	<i>universal</i>	<i> inside</i>	<i>any</i>
3	internal-dmz-ftp	internal	universal	 inside	any

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

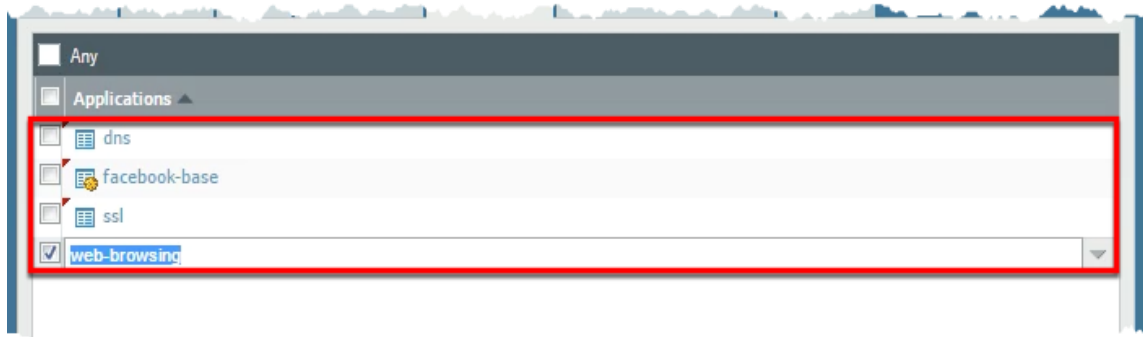
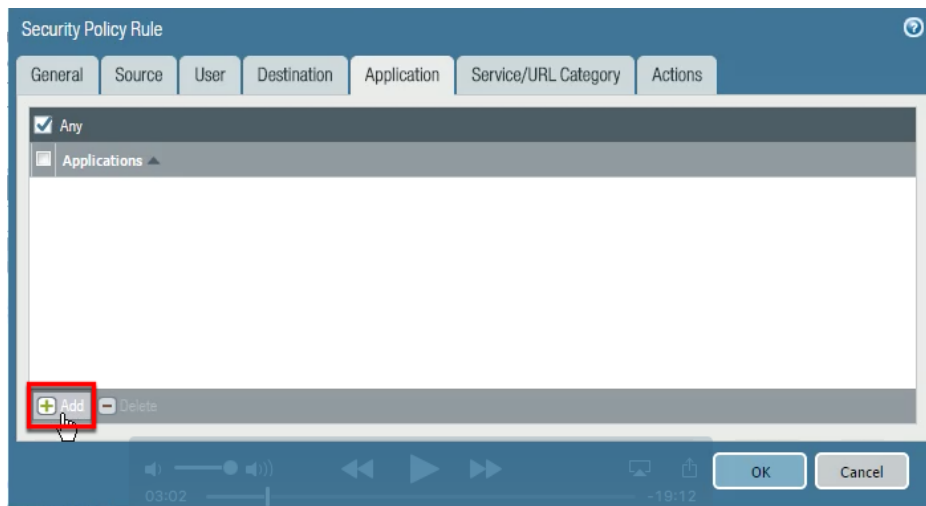
Parameter	Value
Name	egress-outside-app-id



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

Parameter	Value
Applications	dns facebook-base ssl web-browsing





10. 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.

1. Click to open the **interzone-default** Security policy rule.

3	internal-dmz-ftp	internal	universal	inside
4	intrazone-default	none	intrazone	any
5	interzone-default	none	interzone	any

- Click the **Actions** tab. Note that *Log at Session Start* and *Log at Session End* are deselected, and cannot be edited:

Security Policy Rule - predefined (Read Only)

General Actions

**Action Setting**

Action: Deny

☐ Send ICMP Unreachable

**Profile Setting**

Profile Type: None

**Log Setting**

☐ Log at Session Start

☐ Log at Session End

Log Forwarding: None

OK Cancel

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

3	internal-dmz-ftp	internal	universal	inside	any	any
4	intrazone-default	none	intrazone	any	any	any
5	interzone-default	none	interzone	any	any	any



The Security Policy Rule – predefined window opens.

- Click the **Actions** tab.
- Select *Log at Session End*.

Security Policy Rule - predefined

General Actions

Action Setting

Action: Deny

☐ Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

☐ Log at Session Start

☒ Log at Session End

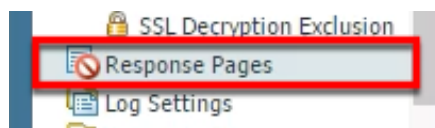
Log Forwarding: None

OK Cancel

- Click **OK**.

#### 4.3 Enable the Application Block Page

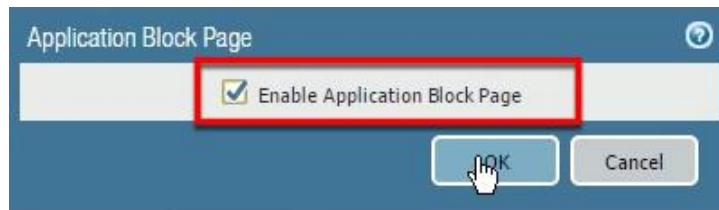
- Select **Device > Response Pages**.



- Click **Disabled** to the right of Application Block Page:

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

3. Select the **Enable Application Block Page** check box.



4. Click **OK**. The Application Block Page should now be enabled:

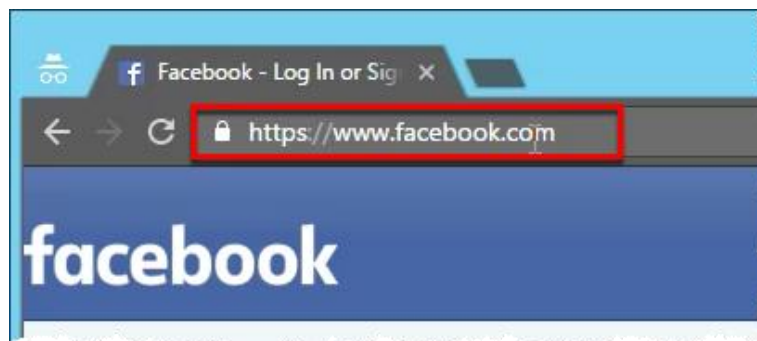
Type	Action	Location
Antivirus / Anti-spyware Block Page		Default
Application Block Page	Enabled	Default
Captive Portal Comfort Page		Default
Data Filtering Block Page		Default

5. **Commit** all changes.

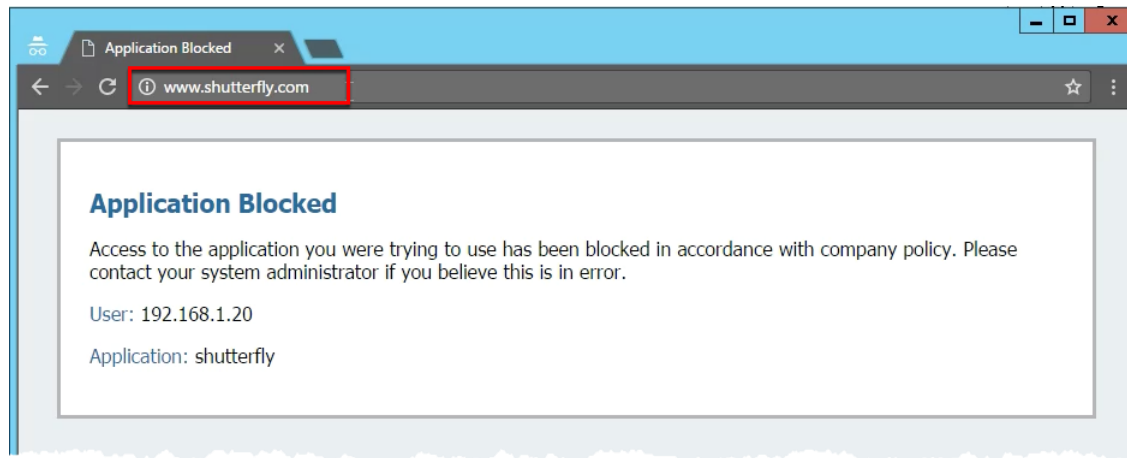


#### 4.4 Test Application Blocking

1. Open a new browser window in private/incognito mode. You should be able to browse to `www.facebook.com` and [www.msn.com](http://www.msn.com).

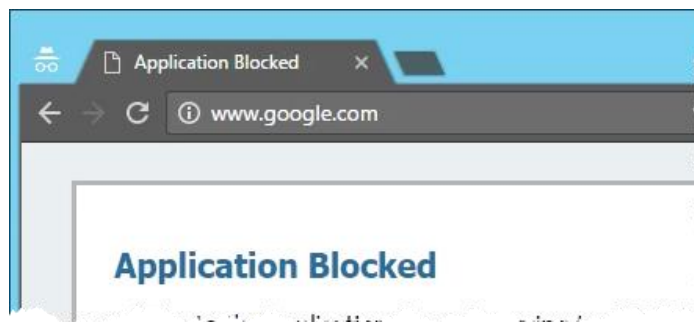


2. Use private/incognito mode in a browser to connect to `http://www.shutterfly.com`. An Application Blocked page opens, indicating that the *shutterfly* application has been blocked:



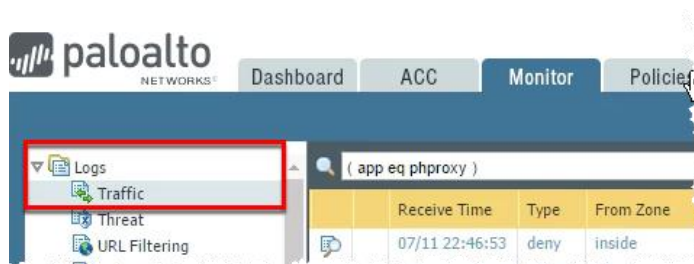
Why could you browse to Facebook and MSN but not to Shutterfly? MSN currently does not have an Application signature. Therefore, it falls under the Application signature web-browsing. However, an Application signature exists for Shutterfly and it is not currently allowed in any of the firewall Security policy rules.

3. Browse to `google.com` and verify that google-base is also being blocked:






## 4.5 Review Logs

1. Select **Monitor > Logs > Traffic**.



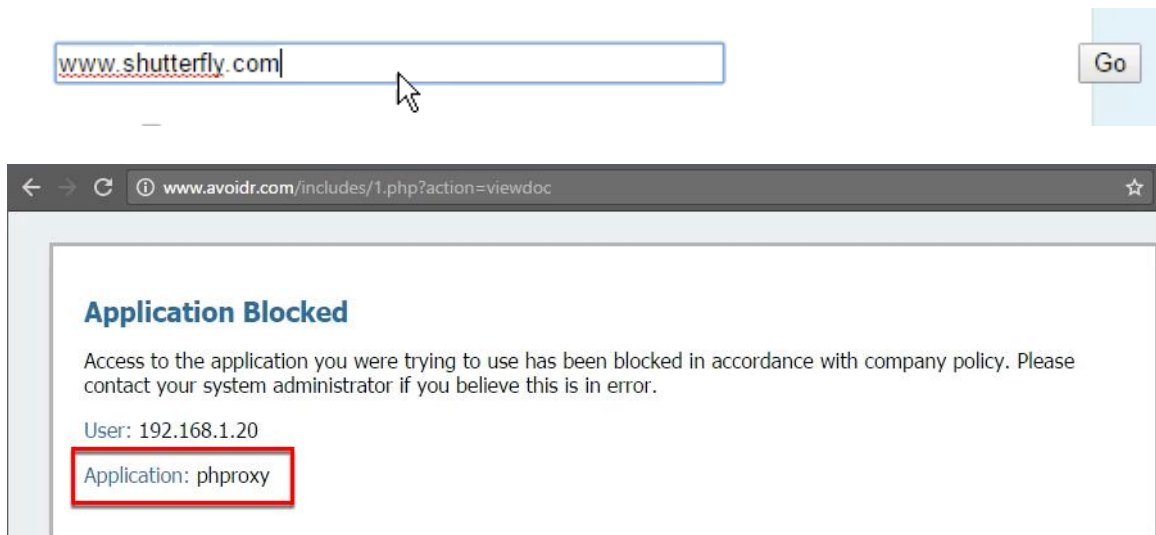
2. Type `( app eq shutterfly )` in the filter text box.
3. Press the **Enter** key.

Only log entries whose Application is shutterfly are displayed.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
	07/11 22:44:33	deny	inside	outside	192.168.1.20		136.179.236.72	80	shutterfly
	07/11 22:44:33	deny	inside	outside	192.168.1.20		136.179.236.72	80	shutterfly
	07/11 22:44:33	deny	inside	outside	192.168.1.20		136.179.236.72	80	shutterfly

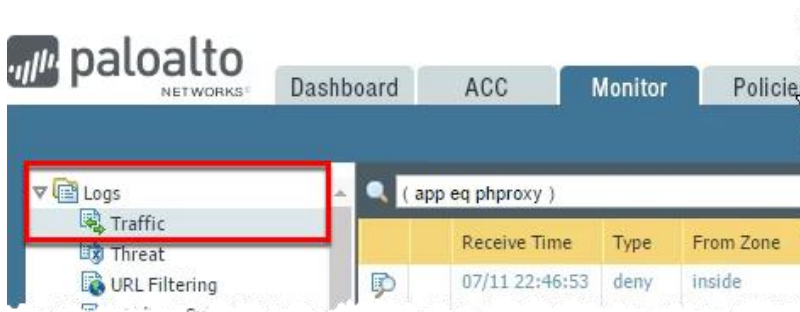
#### 4.6 Test Application Blocking

1. 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`.
2. Enter `www.shutterfly.com` in the text box near the bottom and click **Go**. An application block page opens showing that the phproxy application was blocked:





#### 4.7 Review Logs

1. Select **Monitor > Logs > Traffic**.



2. Type ( `app eq php proxy` ) in the filter text box. The Traffic log entries indicates that the php proxy application has been blocked:

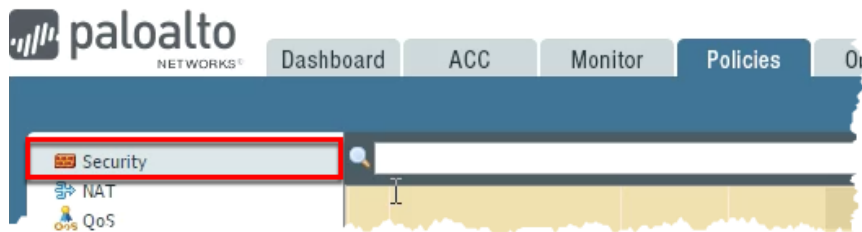
( <code>app eq php proxy</code> )												
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason
	12/02 12:01:31	deny	private	public	192.168.1.20		74.208.215...	80	php proxy	reset-both	interzone-default	policy-deny
	12/02 12:01:31	deny	private	public	192.168.1.20		74.208.215...	80	php proxy	reset-both	interzone-default	policy-deny

Based on the information from your log, Shutterfly and php proxy are denied by the interzone-default Security policy rule.

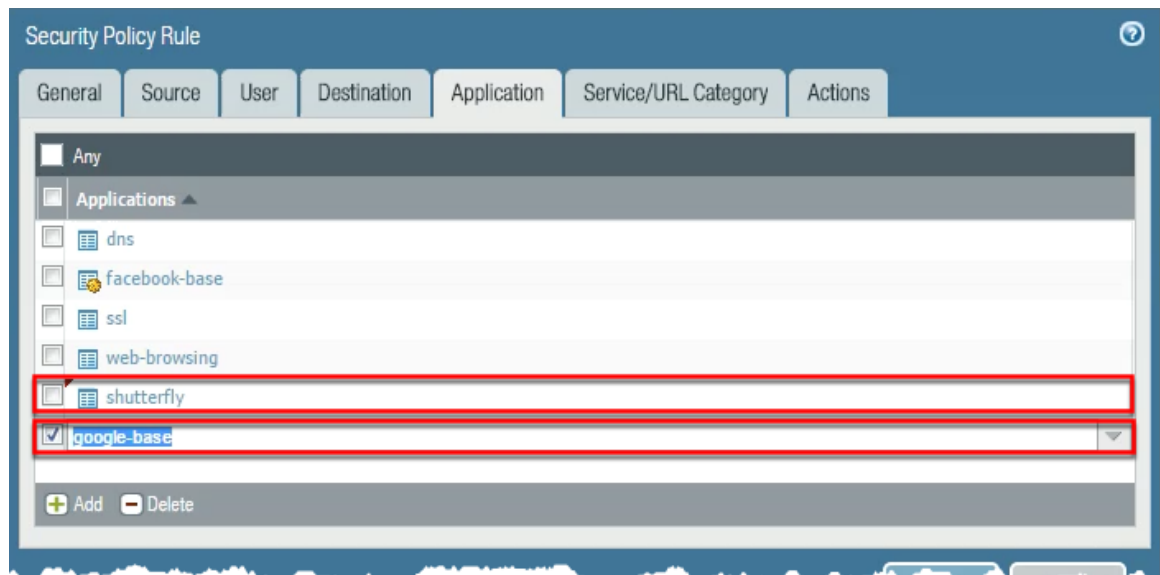
Note: If the logging function of your interzone-default rule is not enabled, no information would be provided via the Traffic log.

## 4.8 Modify the App-ID Security Policy Rule

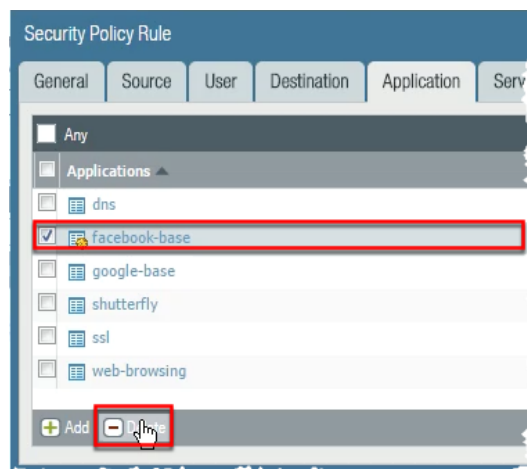
1. In the WebUI select **Policies > Security**.



2. Add `shutterfly` and `google-base` to the `egress-outside-app-id` Security policy rule.

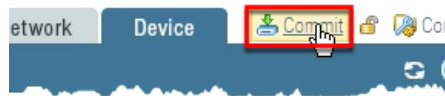


3. Remove `facebook-base` from the `egress-outside-app-id` Security policy rule.





4. **Commit** all changes.



#### 4.9 Test App-ID Changes

1. Open a browser in private/incognito mode and browse to `www.shutterfly.com` and `google.com`. The application block page is no longer presented.
2. Open a new browser in private/incognito mode and browse to `www.facebook.com`. The application block page now appears for facebook-base. Note: Do not use any previously used browser windows because browser caching can cause incorrect results.

##### 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

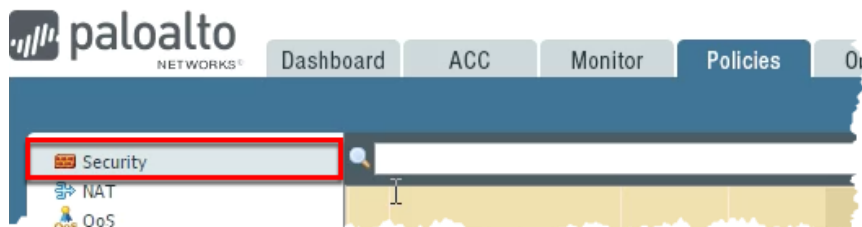
Application: facebook-base

3. Close all browser windows except for the firewall WebUI.

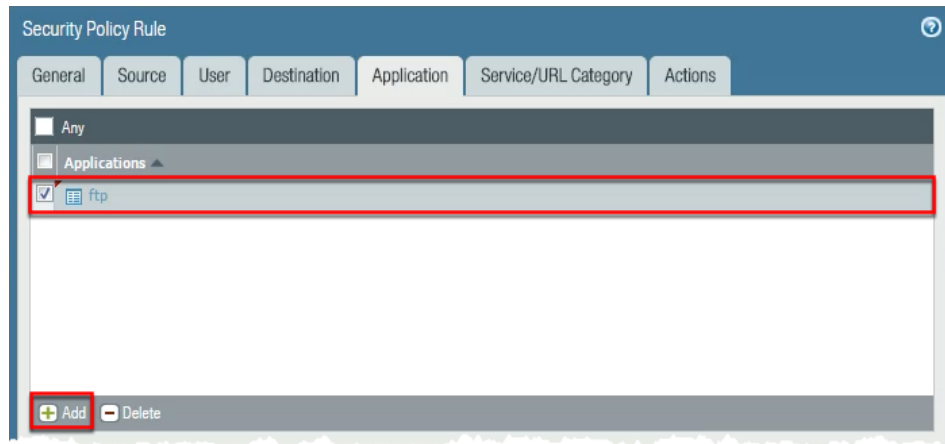
Note: The web-browsing Application signature only covers browsing that does not match any other Application signature.

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

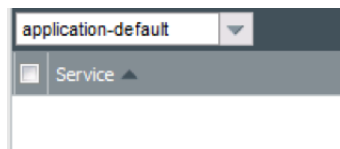
1. In the WebUI select **Policies > Security**.



2. Click to open the **internal-dmz-ftp** Security policy rule:
3. Click the **Application** tab and add ftp.

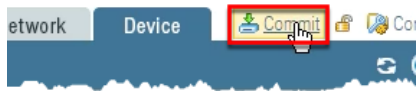


4. Click the **Service/URL Category** tab.
5. Delete service-ftp and select application-default.

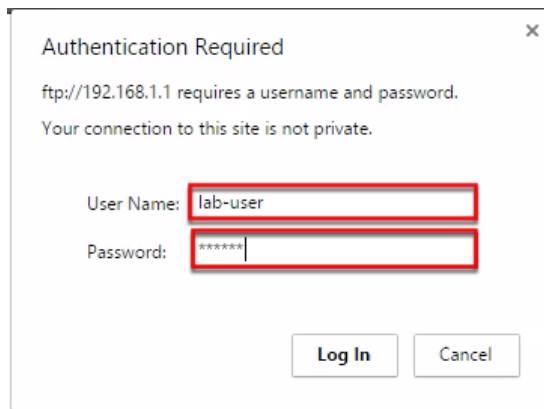


Selecting application-default does not change the service behavior because, in the application database, FTP is allowed only on ports 20 and 21 by default.

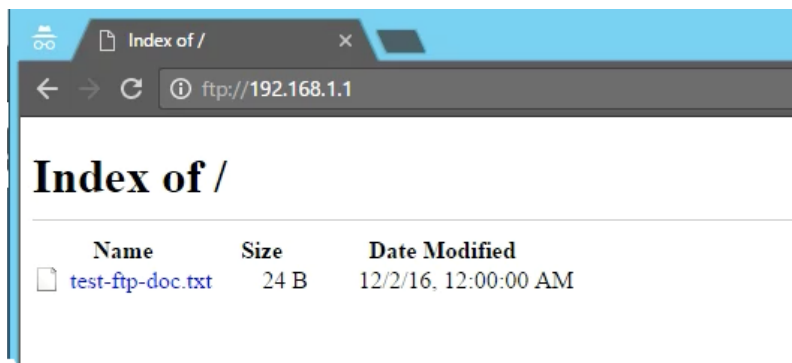
6. Click **OK**.
7. **Commit** all changes.



8. Open a new Chrome browser window in private mode and browse to <ftp://192.168.1.1>.
9. At the prompt for login information, enter the following (Credentials may be cached from previous login):



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



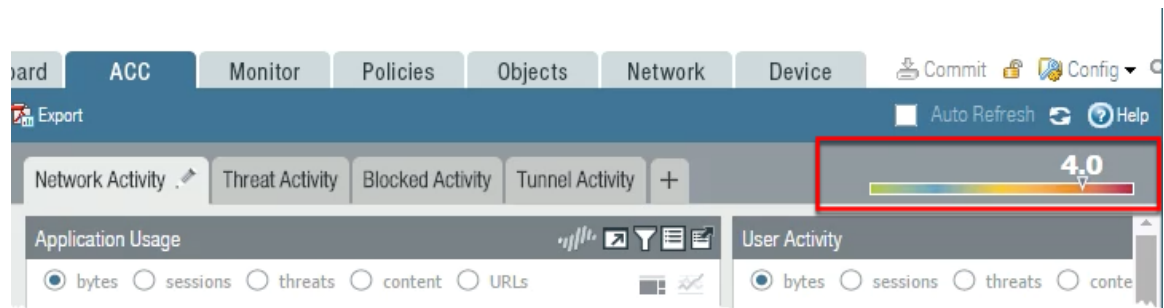
#### 4.11 Observe the Application Command Center

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.

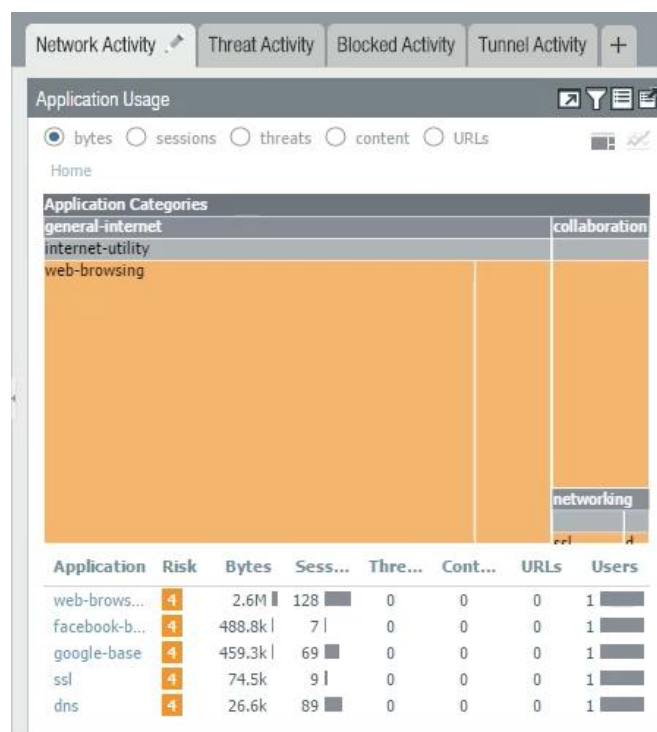
1. Click the **ACC** tab to access the Application Command Center:



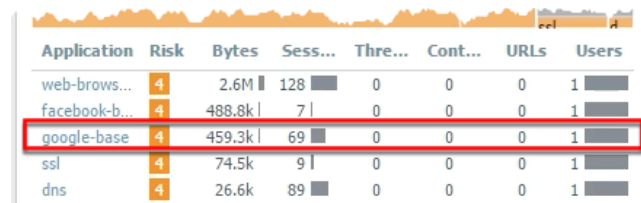
2. Note that the upper-right corner of the ACC displays the total risk level for all traffic that has passed through the firewall thus far:



- 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).

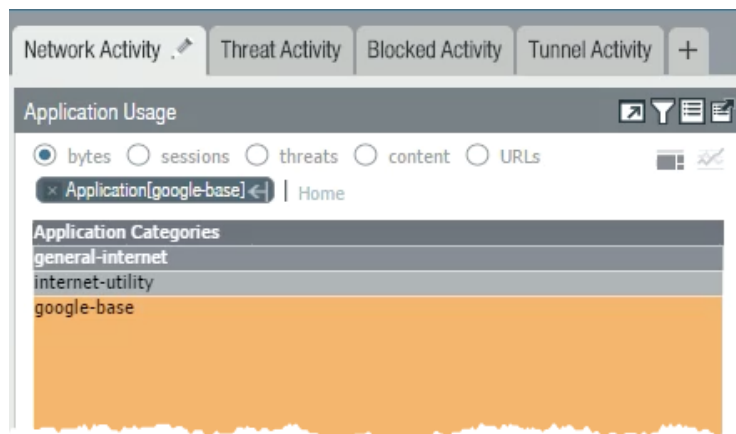


- You can click any application listed in the Application Usage pane; google-base is used in this example:

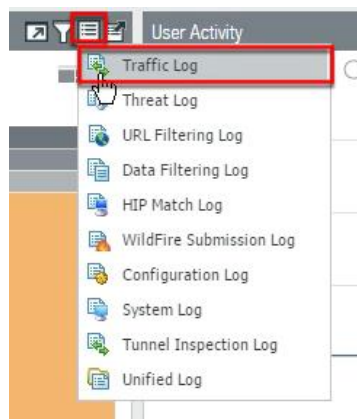


Application	Risk	Bytes	Sess...	Thre...	Cont...	URLs	Users
web-brows...	4	2.6M	128	0	0	0	1
facebook-b...	4	488.8k	7	0	0	0	1
google-base	4	459.3k	69	0	0	0	1
ssl	4	74.5k	9	0	0	0	1
dns	4	26.6k	89	0	0	0	1

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



5. Click the **Jump to logs** icon and select **Traffic Log**:



Notice that the WebUI generated the appropriate log filter and jumped to the applicable log information for the google-base application:

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