



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



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

**Document Version: 2020-01-22**

Copyright © 2020 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.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

## Contents

Introduction .....	3
Objectives.....	3
Lab Topology .....	4
Theoretical Lab Topology.....	4
Lab Settings .....	5
1 App-ID .....	6
1.0 Load Lab Configuration .....	6
1.1 Verify an FTP Service Object .....	8
1.2 Create an FTP Port-Based Security Policy Rule .....	10
1.3 Test the Port-Based Security Policy .....	14
1.4 Create an App-ID Security Policy Rule.....	15
1.5 Enable Interzone Logging .....	19
1.6 Enable the Application Block Page .....	20
1.7 Test Application Blocking .....	21
1.8 Review Logs .....	23
1.9 Test Application Blocking .....	23
1.10 Review Logs .....	24
1.11 Modify the App-ID Security Policy Rule.....	25
1.12 Test App-ID Changes.....	26
1.13 Observe the Application Command Center.....	27
1.14 Migrate Port-Based Rule to Application-Aware Rule .....	29

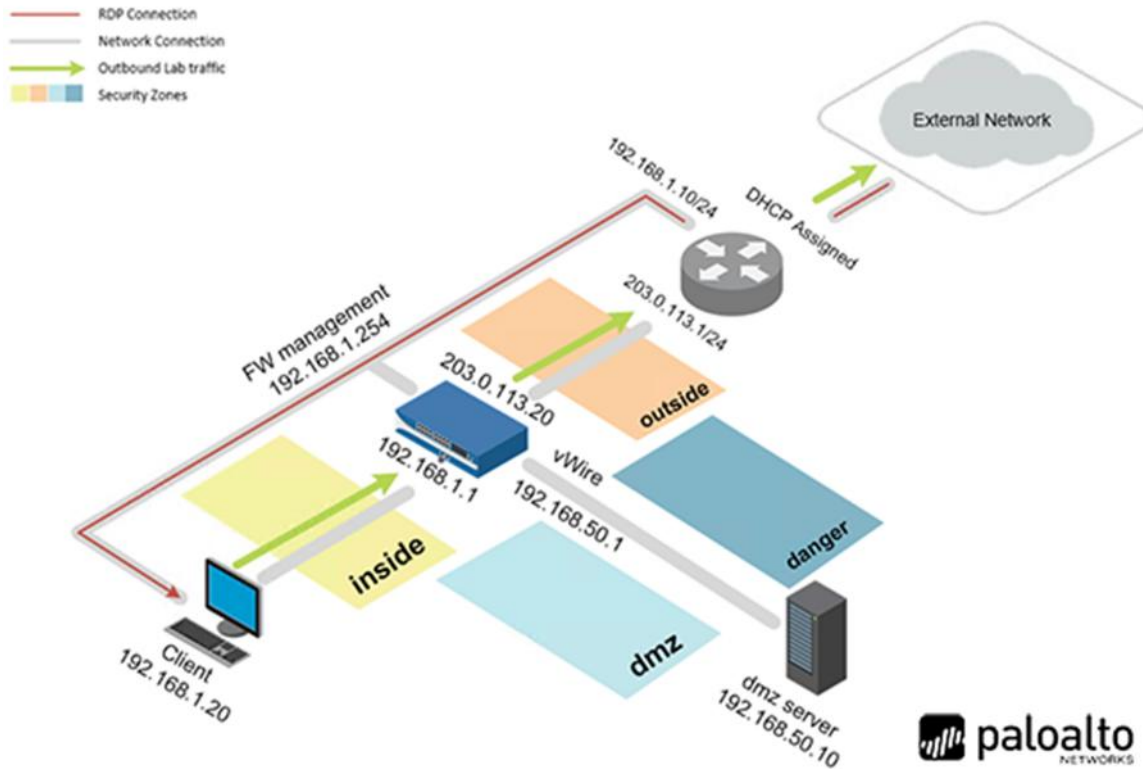
## Introduction

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.

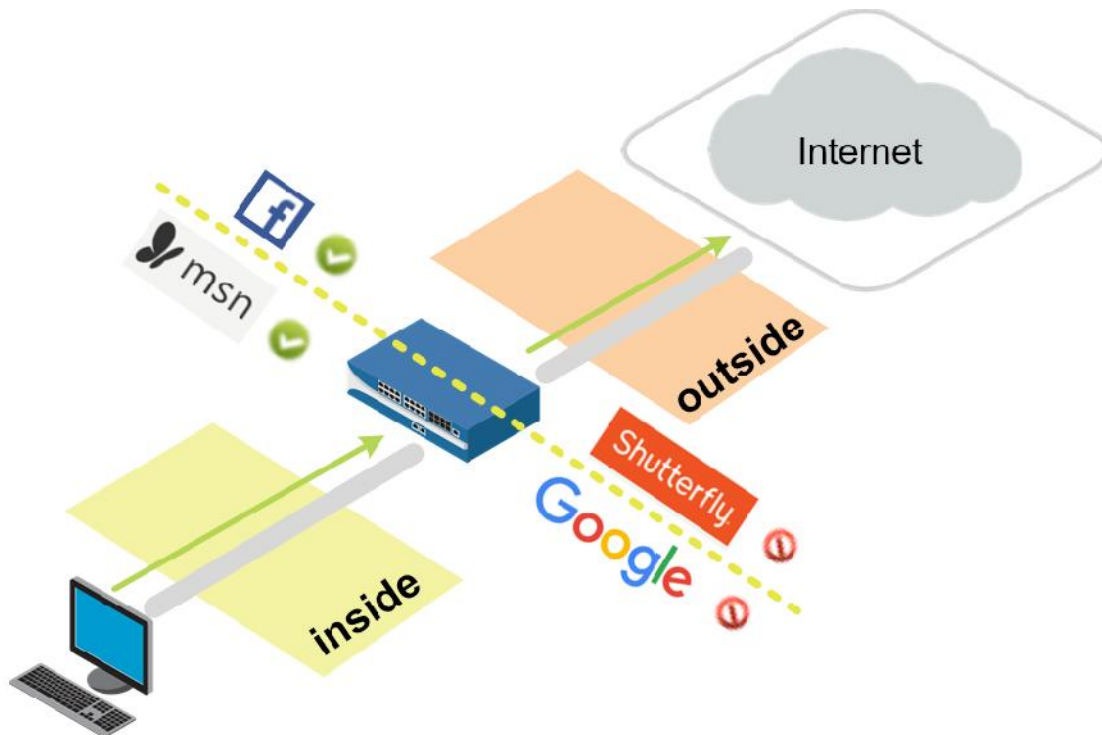
## Objectives

- ) Create an application-aware Security policy rule
- ) Enable interzone logging
- ) Enable the application 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 rule to application-aware policies
- ) Review logs associated with the traffic and browse the Application Command Center (ACC)

## Lab Topology



## Theoretical 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	192.168.1.20	lab-user	Pa10Alt0
Firewall	192.168.1.254	admin	admin

## 1 App-ID

### 1.0 Load Lab Configuration

1. Launch the **Client** virtual machine to access the graphical login screen.



To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

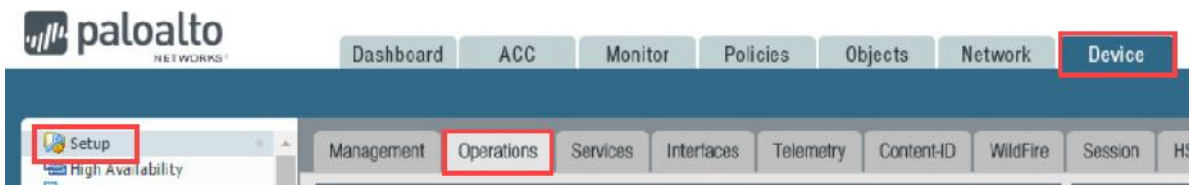
2. Click within the splash screen to bring up the login screen. Log in as **lab-user** using the password **Pa10A1t0**.



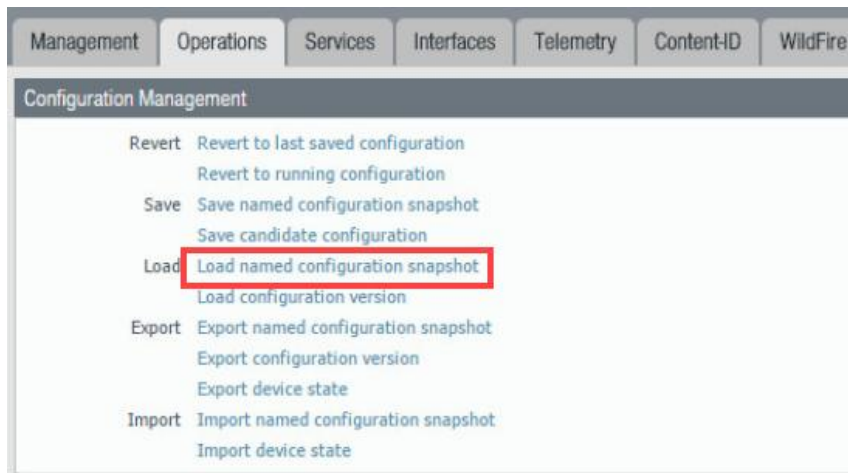
3. Launch the **Chrome** browser and connect to **https://192.168.1.254**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	admin
Password	admin

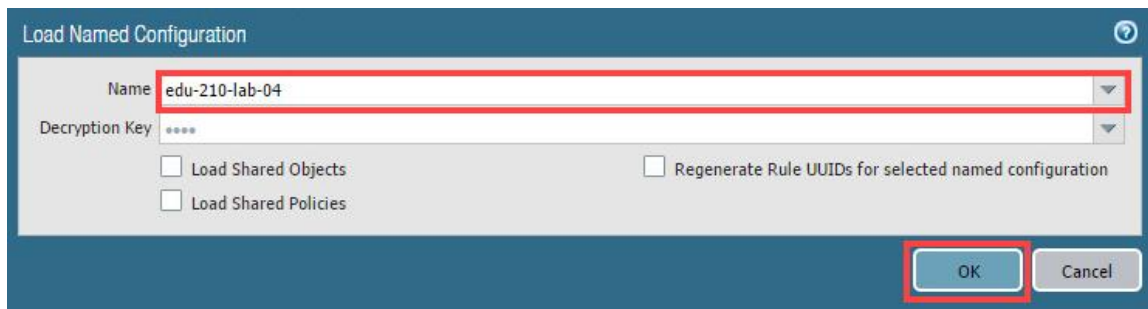
6. In the web interface, select **Device > Setup > Operations**.



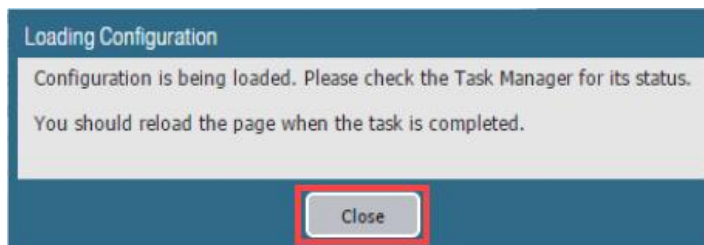
7. Click **Load named configuration snapshot**:



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



9. Click **Close**.

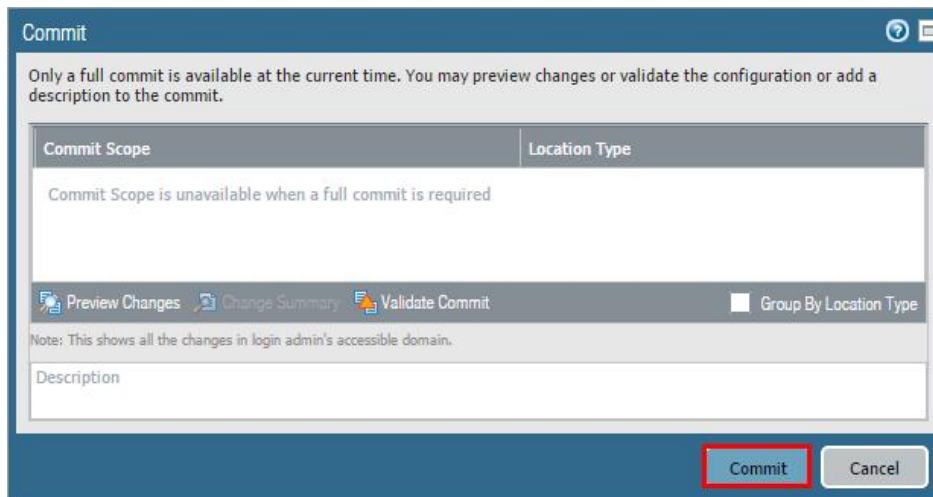


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

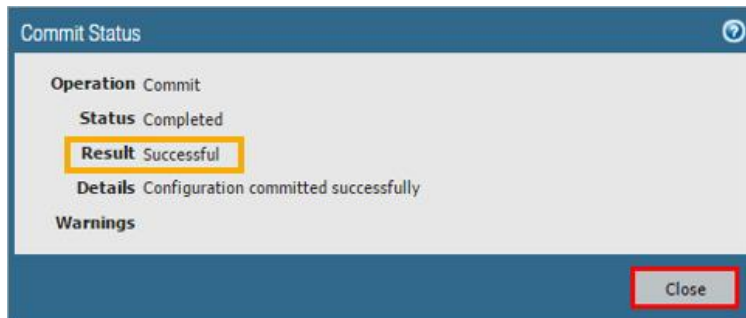
10. Click the **Commit** link at the top-right of the web interface.



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



12. Once completed successfully, click **Close** to continue.



13. Leave the firewall web interface open to continue with the next task.

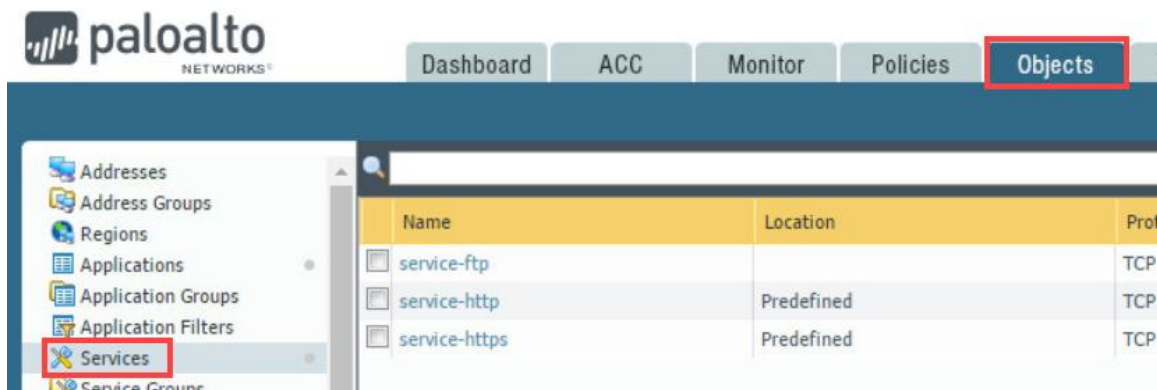
## 1.1 Verify an FTP Service Object

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 task.



1. In the web interface, navigate to **Objects > Services**.

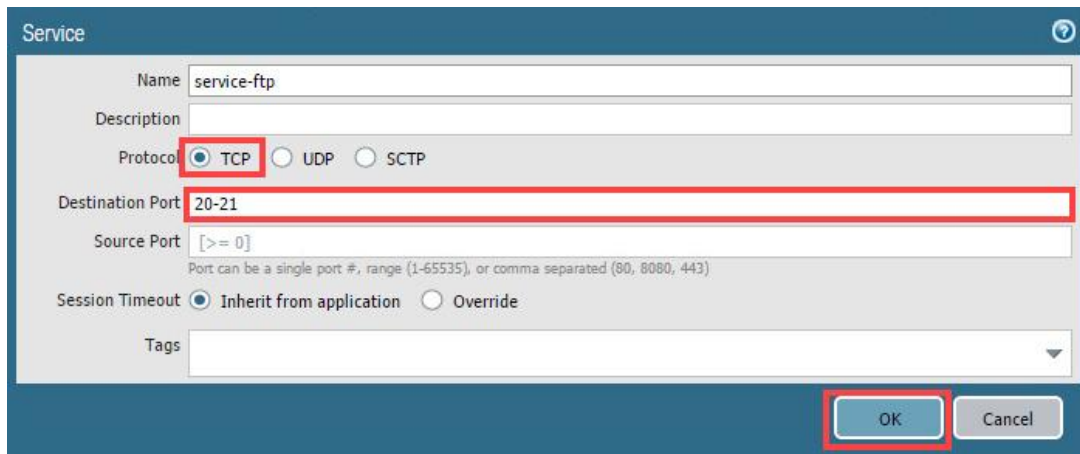


2. Click on the **service-ftp** object from the list to configure the service.

Name	Location
service-ftp	
service-http	Predefined
service-https	Predefined

3. In the *Service* window, verify the following configurations. Once finished, click **OK**.

Parameter	Value
Protocol	Verify <b>TCP</b> radio button is selected
Destination Port	Verify that the destination port entry is set to <b>20-21</b>



The screenshot shows the 'Service' configuration window for 'service-ftp'. The following fields are highlighted with red boxes to indicate the required configurations:

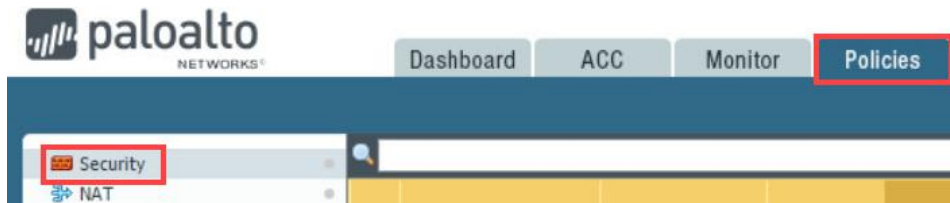
- Name:** service-ftp
- Protocol:** TCP (radio button selected)
- Destination Port:** 20-21
- Source Port:** [ >= 0 ]
- Session Timeout:** Inherit from application (radio button selected)
- Tags:** (empty dropdown menu)
- Buttons:** OK and Cancel

4. Leave the firewall web interface open to continue with the next task.

## 1.2 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.

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

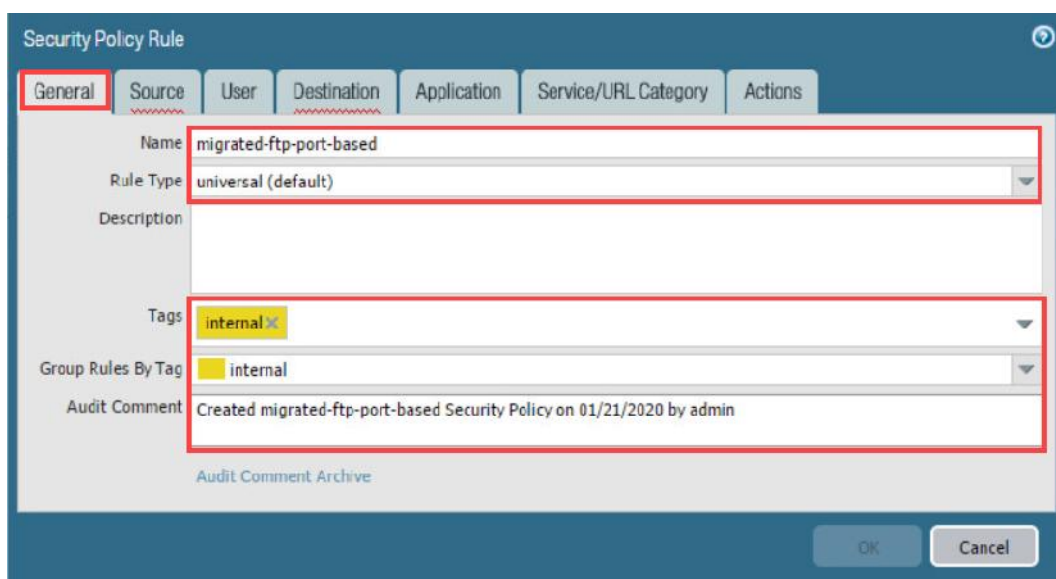


2. Click **Add** in the lower-left corner of the panel to create a new security policy rule.



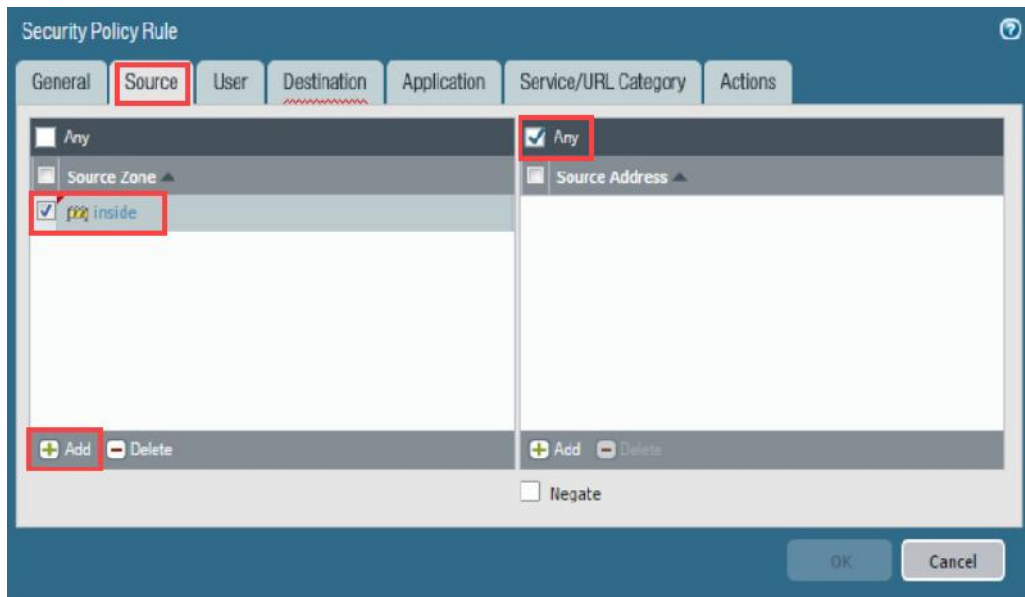
3. In the *Security Policy Rule* window, while on the *General* tab, configure the following:

Parameter	Value
Name	Type <code>migrated-ftp-port-based</code>
Rule Type	Verify that <b>universal (default)</b> is selected
Tags	Select <b>internal</b> from the drop-down list
Group Rules By Tag	Select <b>internal</b> from the drop-down list
Audit Comment	Type <code>Created migrated-ftp-port-based Security Policy on &lt;date&gt; by admin</code>



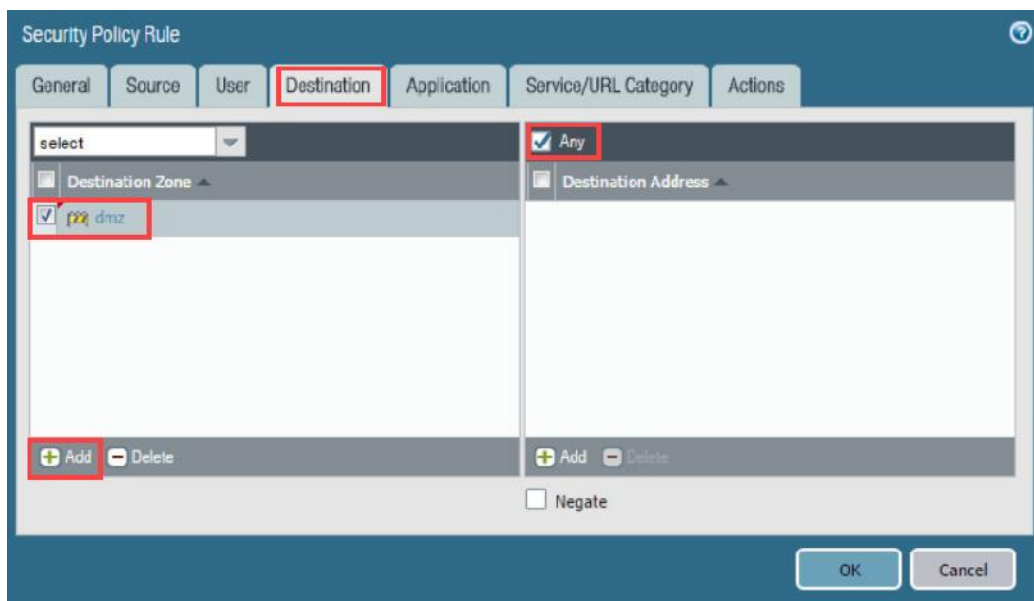
4. In the *Security Policy Rule* window, click on the **Source** tab and configure the following:

Parameter	Value
Source Zone	Click <b>Add</b> and select <b>inside</b>
Source Address	Verify that the <b>Any</b> checkbox is selected

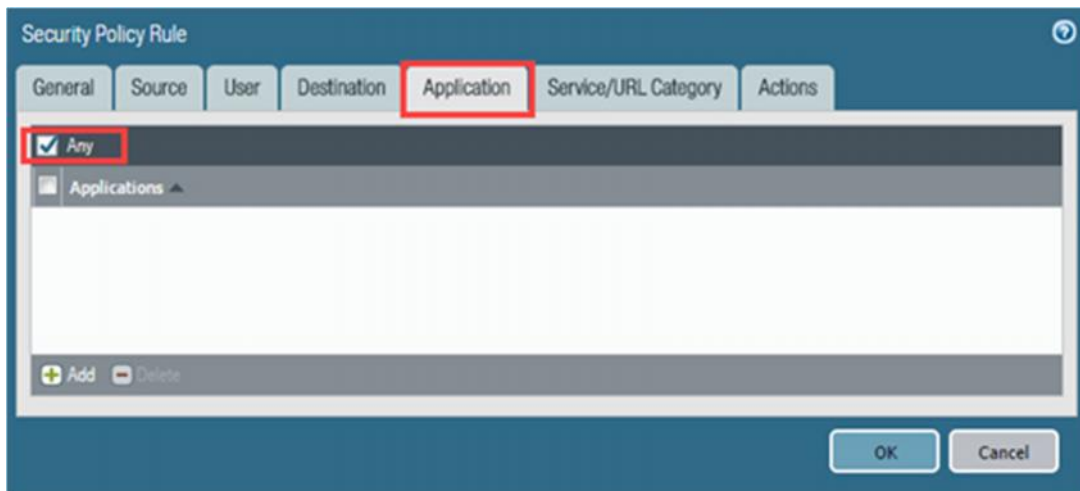


5. In the *Security Policy Rule* window, click on the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	Click <b>Add</b> and select <b>dmz</b>
Destination Address	Verify that the <b>Any</b> checkbox is selected

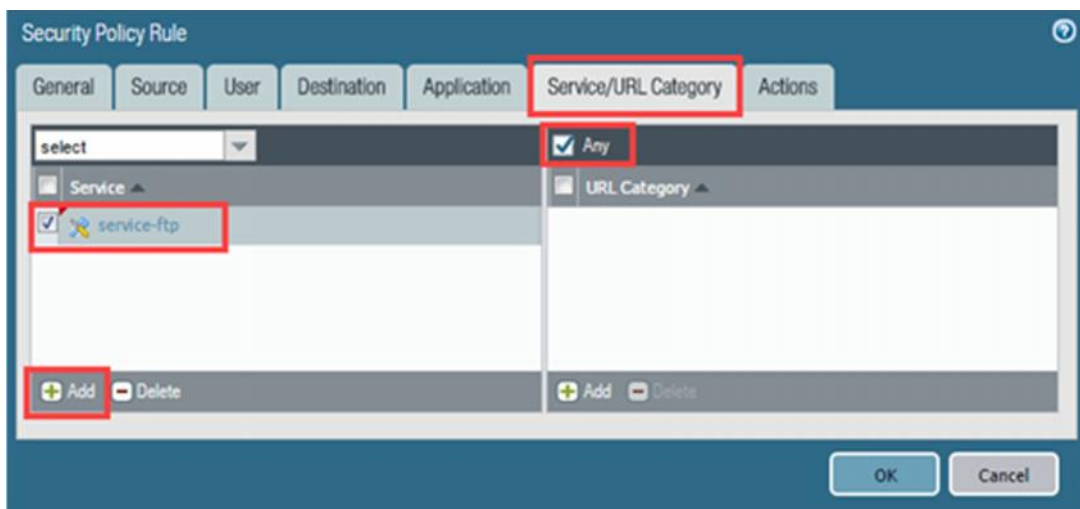


6. In the *Security Policy Rule* window, click on the **Application** tab and verify that the **Any** checkbox is selected.



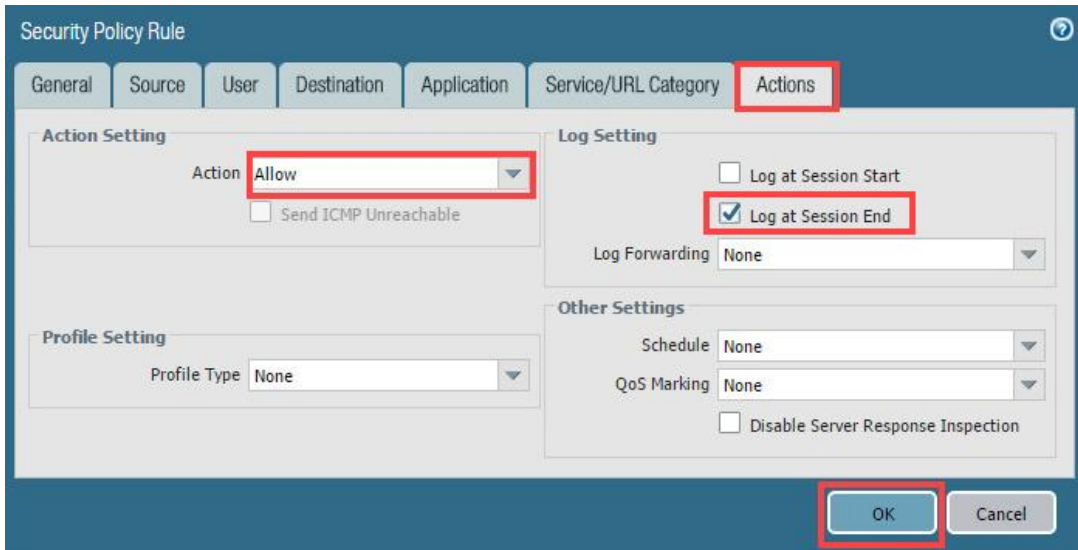
7. In the *Security Policy Rule* window, click on the **Service/URL Category** tab and configure the following:

Parameter	Value
Service	Click <b>Add</b> and select <b>service-ftp</b>
URL Category	Verify that the <b>Any</b> checkbox is selected



8. In the *Security Policy Rule* window, click on the **Actions** tab and verify the following. Once finished, click **OK**.

Parameter	Value
Action	Verify that <b>Allow</b> is selected
Log Setting	Verify that <b>Log at Session End</b> is selected



Security Policy Rule

General Source User Destination Application Service/URL Category **Actions**

**Action Setting**

Action: **Allow**

☐ Send ICMP Unreachable

**Log Setting**

☐ Log at Session Start

☒ **Log at Session End**

Log Forwarding: None

**Other Settings**

Schedule: None

QoS Marking: None

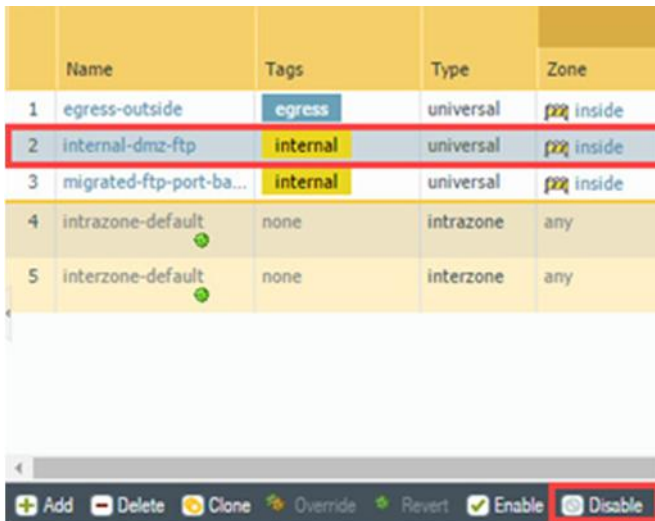
☐ Disable Server Response Inspection

**Profile Setting**

Profile Type: None

**OK** Cancel

9. Select the **internal-dmz-ftp** security policy rule without opening it and click **Disable**.



	Name	Tags	Type	Zone
1	egress-outside	egress	universal	inside
2	<b>internal-dmz-ftp</b>	internal	universal	inside
3	migrated-ftp-port-ba...	internal	universal	inside
4	intrazone-default	none	intrazone	any
5	interzone-default	none	interzone	any

+ Add    - Delete    Clone    Override    Revert    ☒ Enable    ☒ **Disable**

10. **Commit** all changes.

### 1.3 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 logs 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.

1. Launch the *Command Line Interface* by clicking on the **CMD** icon in the toolbar.



2. In the *CMD* window, type the command below, followed by pressing the **Enter** key in an attempt to connect to the FTP server.

```
C:\Windows\System32> ftp 192.168.50.10
```

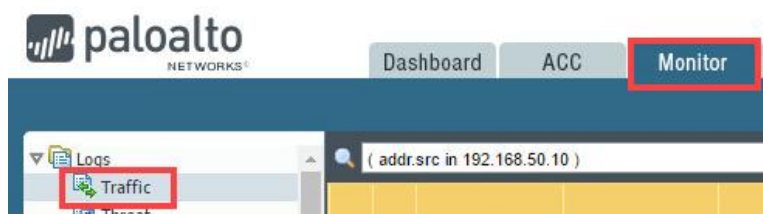
3. When prompted for user credentials, login as **lab-user** with the password **paloalto**. The login should succeed, although 30 seconds might pass until authentication completes.

```
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> _
```


4. Once successfully logged in, type **bye** followed by pressing the **Enter** key to end the FTP session.

```
ftp> bye
221 Goodbye.
C:\Windows\System32>_
```

5. Type **exit** followed by pressing the **Enter** key to close the *CMD* window.
6. Change focus to the firewall web interface and navigate to **Monitor > Logs > Traffic**.



- Make sure to clear any filters and locate the log entry for the FTP session.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
	01/21 21:57:21	end	inside	dmz	192.168.1.20		192.168.50.10	21	ftp	allow	migrated-ftp-port-based

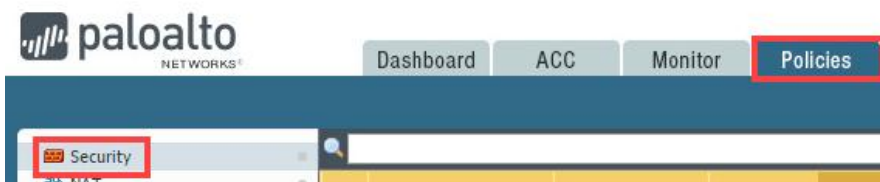


Notice the security policy rule matched the session with *migrated-ftp-port-based*.

- Leave the firewall web interface open to continue with the next task.








## 1.4 Create an App-ID Security Policy Rule

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



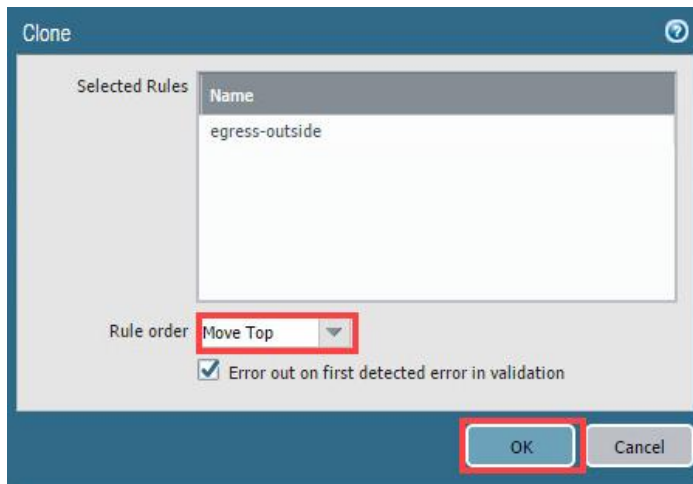
- Select the **egress-outside** Security policy rule without opening it. Click **Clone**. The *Clone* configuration window opens.

	Name	Tags	Type	Zone
1	egress-outside	egress	universal	inside
2	internal-dmz-ftp	internal	universal	inside
3	migrated-ftp-port-ba...	internal	universal	inside
4	intrazone-default	none	intrazone	any
5	interzone-default	none	interzone	any

 Add
  Delete
  Clone
  Override
  Revert
  Enable
  Disable



- In the *Clone* window, on the *Rule order* drop-down list, select **Move top**. Click **OK**.



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

- Notice a new Security policy rule named *egress-outside-1* is added to the top of the Policy order.

	Name	Tags	Type	Zone
1	egress-outside-1	egress	universal	inside
2	egress-outside	egress	universal	inside
3	internal-dmz-ftp	internal	universal	inside
4	migrated-ftp-port-ba...	internal	universal	inside
5	intrazone-default	none	intrazone	any
6	interzone-default	none	interzone	any

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

	Name	Tags	Type	Zone
1	egress-outside-1	egress	universal	inside
2	egress-outside	egress	universal	inside
3	internal-dmz-ftp	internal	universal	inside
4	migrated-ftp-port-ba...	internal	universal	inside
5	intrazone-default	none	intrazone	any
6	interzone-default	none	interzone	any

--	--	--	--	--	--	--	--

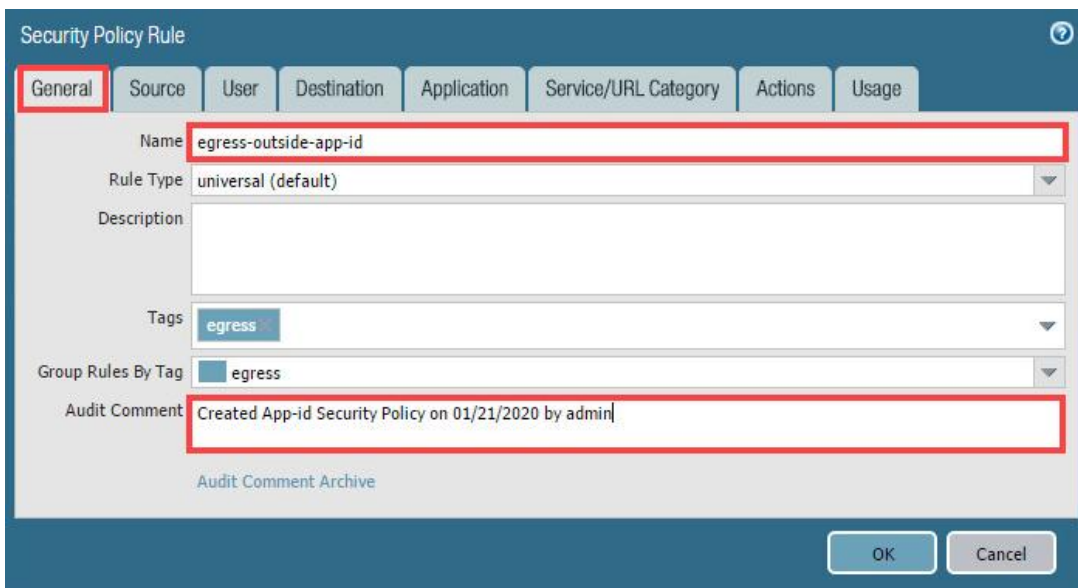


6. Click the cloned Security policy rule **egress-outside-1** to configure the policy.

	Name	Tags	Type	Zone
1	<b>egress-outside-1</b>	<b>egress</b>	universal	inside
2	egress-outside	egress	universal	inside
3	internal-dmz-ftp	internal	universal	inside
4	migrated-ftp-port-ba...	internal	universal	inside
5	intrazone-default	none	intrazone	any
6	interzone-default	none	interzone	any

7. In the *Security Policy Rule* window, while on the *General* tab, configure the following:

Parameter	Value
Name	Rename policy to <b>egress-outside-app-id</b>
Audit Comment	Type Created App-id Security Policy on <date> by admin



**Security Policy Rule**

**General** | Source | User | Destination | Application | Service/URL Category | Actions | Usage

Name: **egress-outside-app-id**

Rule Type: universal (default)

Description:

Tags: **egress**

Group Rules By Tag: **egress**

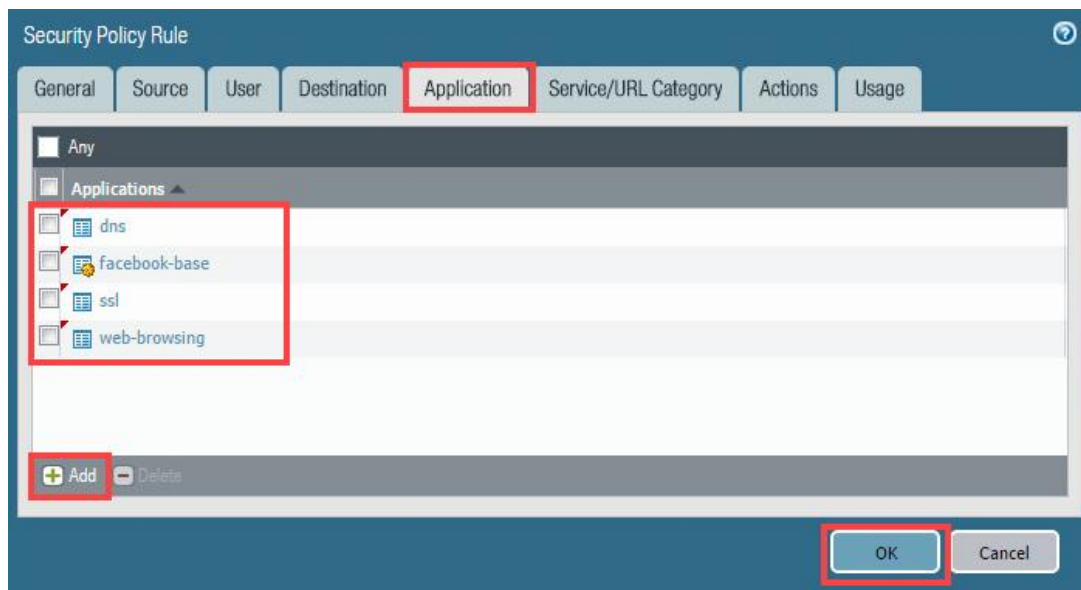
Audit Comment: **Created App-id Security Policy on 01/21/2020 by admin**

[Audit Comment Archive](#)

OK Cancel

8. In the *Security Policy Rule* window, click the **Application** tab and configure the following. Once finished, click **OK**.

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



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.

9. Leave the firewall web interface open to continue with the next task.

## 1.5 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.

1. In the web interface, click to open the **interzone-default** Security policy rule.

	Name	Tags	Type	Zone
1	egress-outside-app-id	egress	universal	inside
2	egress-outside	egress	universal	inside
3	internal-dmz-ftp	internal	universal	inside
4	migrated-ftp-port-ba...	internal	universal	inside
5	intrazone-default	none	intrazone	any
6	interzone-default	none	interzone	any

2. In the *Security Policy-Rule - predefined (Read Only)* window, click the **Actions** tab. Notice that *Log at Session Start* and *Log at Session End* are deselected, and cannot be edited. Click **Cancel**.

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

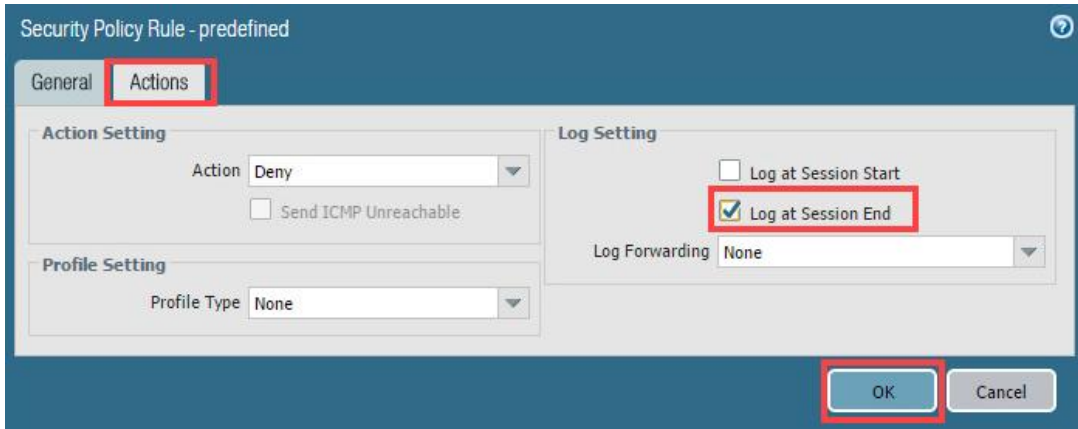
OK Cancel

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

5	intrazone-default	none	intrazone	any
6	interzone-default	none	interzone	any

 Add
  Delete
  Clone
  **Override**
 Revert
  Enable
  Disable

- In the *Security Policy Rule - predefined* window, click the **Actions** tab and select the **Log at Session End** checkbox. Click **OK**.



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

- Leave the firewall web interface open to continue with the next task.

## 1.6 Enable the Application Block Page

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

- In the web interface, select **Device > Response Pages**.



- Select **Application Block Page** without opening it and click the **Disabled** link to the right of the *Application Block Page* under the *Action* column.

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

3. In the *Application Block Page* window, select the **Enable Application Block Page** checkbox. Click **OK**.

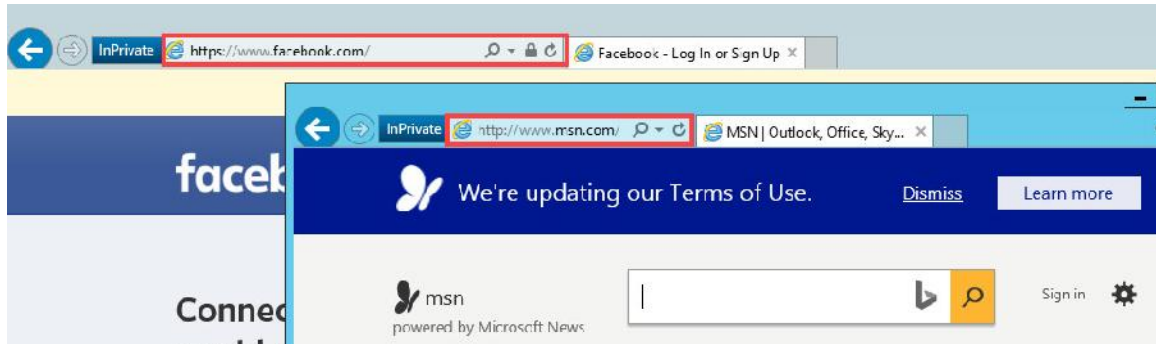


The firewall can present the *Application Block Page* only if it detects and blocks a web-based application. Blocked applications that do not use a web browser will be stopped but the user will not necessarily know why.

4. Notice the *Application Block Page* should now be enabled.
5. **Commit** all changes.

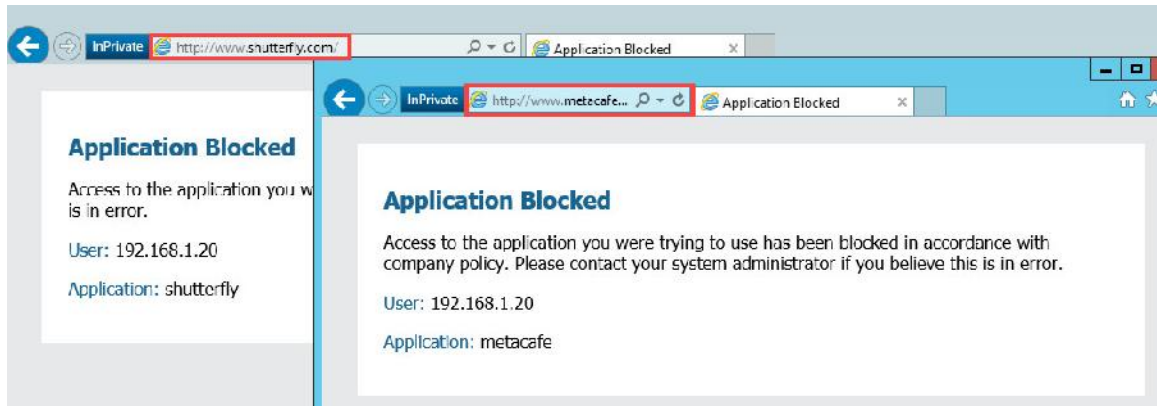
## 1.7 Test Application Blocking

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



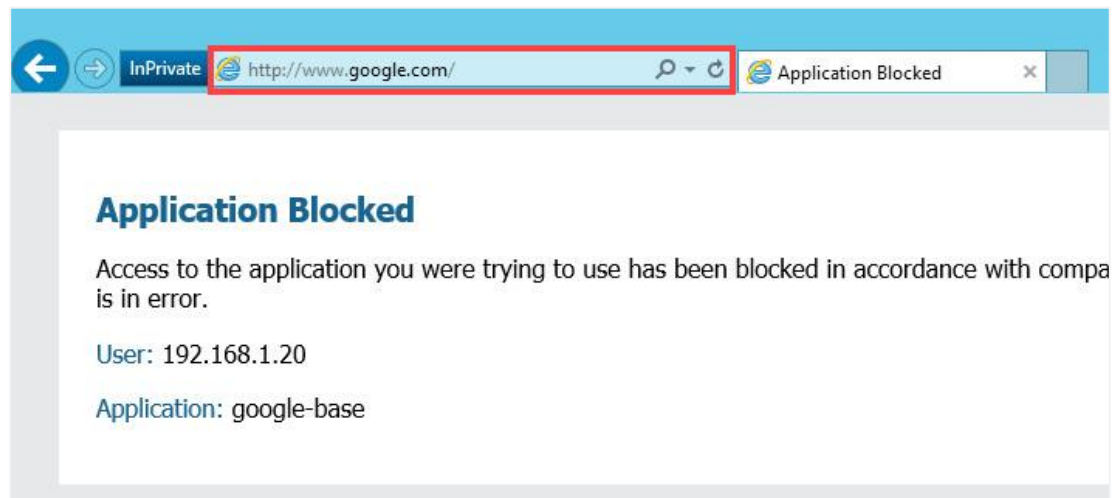
You should be able to successfully connect to the Facebook and MSN websites.

- Using the same browser, browse to [www.shutterfly.com](http://www.shutterfly.com) and [www.metacafe.com](http://www.metacafe.com). An *Application Blocked* page appears, indicating that the *shutterfly* and *metacafe* application has been blocked:



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.

- Using the same *IE* browser, browse to [www.google.com](http://www.google.com) and verify that google-base is also being blocked.



- Close the *IE* browser.
- Leave the firewall web interface open to continue with the next task.

## 1.8 Review Logs

1. Change focus to the firewall's web interface and navigate to **Monitor > Logs > Traffic**



2. In the log filter text box, type `(app eq shutterfly)` and 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	Action	Rule
	01/21 22:06:38	deny	inside	outside	192.168.1.20		136.179.238.151	80	shutterfly	deny	interzone-default

## 1.9 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.

1. Using **Internet Explorer** in private/incognito mode in a browser, browse to **kproxy.com**.



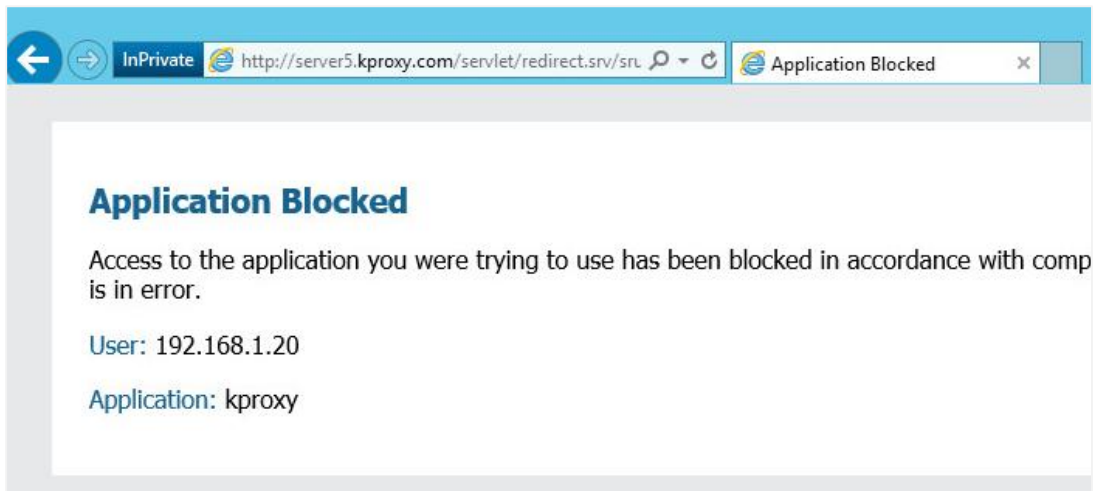
If *kproxy.com* is not available, try using *php-proxy.com*.

2. Enter **www.shutterfly.com** in the text box near the top and click **surf!**. An application block page opens showing that the **phproxy** application was blocked:





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



4. Close the **IE** browser.
5. Leave the firewall web interface open to continue with the next task.

### 1.10 Review Logs

1. In the web interface, select **Monitor > Logs > Traffic**.
2. Clear the exlog filter text box and type (**app eq kproxy**) followed by pressing the **Enter** key.



	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
	01/21 22:09:37	deny	inside	outside	192.168.1.20		167.114.102.230	80	kproxy	deny	interzone-default



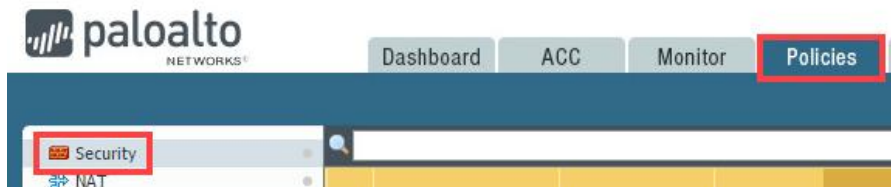
Based on the information from the Traffic log, *Shutterfly* and *kproxy* are denied by the *interzone-default* Security policy rule. If the logging functions of your *interzone-default* rule is not enabled, no information would be provided via the Traffic log.

3. Leave the firewall web interface open to continue with the next task.



## 1.11 Modify the App-ID Security Policy Rule

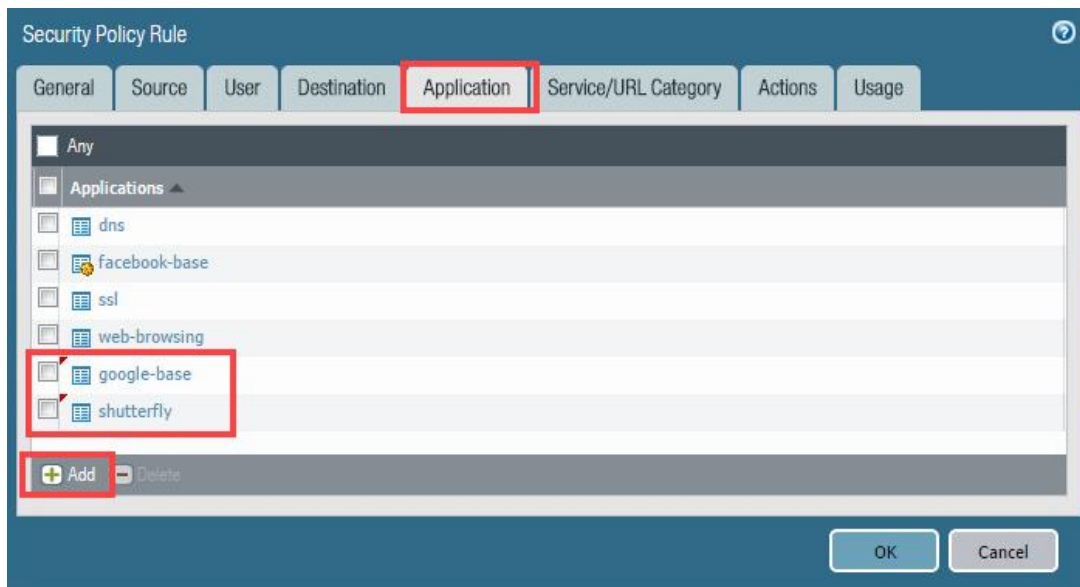
1. In the web interface, select **Policies > Security**.



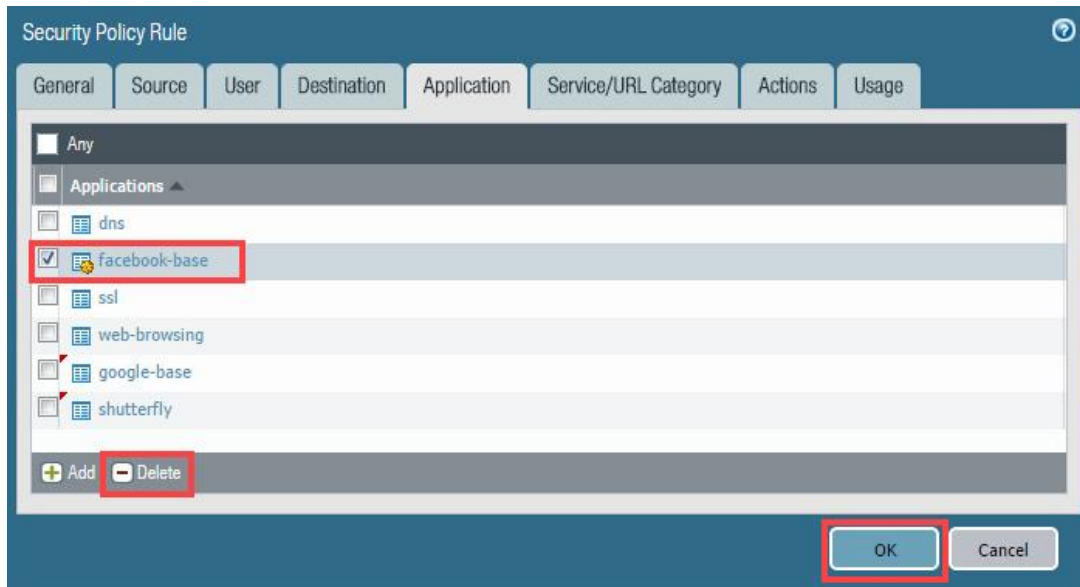
2. Click **egress-outside-app-id** to open the Security policy rule.

	Name	Tags	Type	Zone	Address
1	<b>egress-outside-app-id</b>	egress	universal	inside	any
2	egress-outside	egress	universal	inside	any
3	internal-dmz-ftp	internal	universal	inside	any
4	migrated-ftp-port-ba...	internal	universal	inside	any
5	intrazone-default	none	intrazone	any	any
6	interzone-default	none	interzone	any	any

3. In the *Security Policy Rule* window, click the **Application** tab and click the **Add** button. Select **google-base** from the list. Click the **Add** button once more to add **shutterfly**.



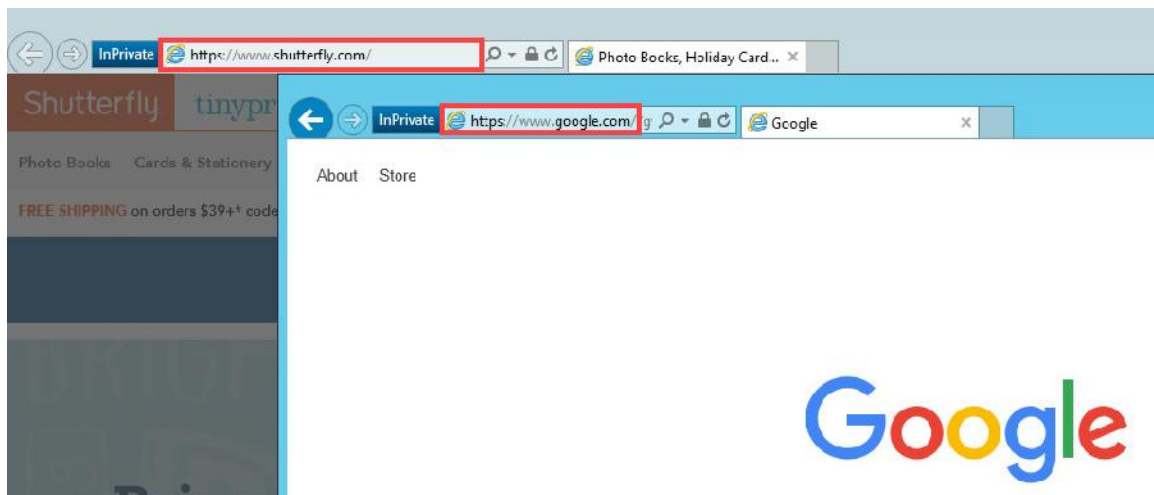
- Next, select **facebook-base** followed by clicking the **Delete** button to remove the application from the rule. Once finished, click **OK**.



- Commit** all changes.

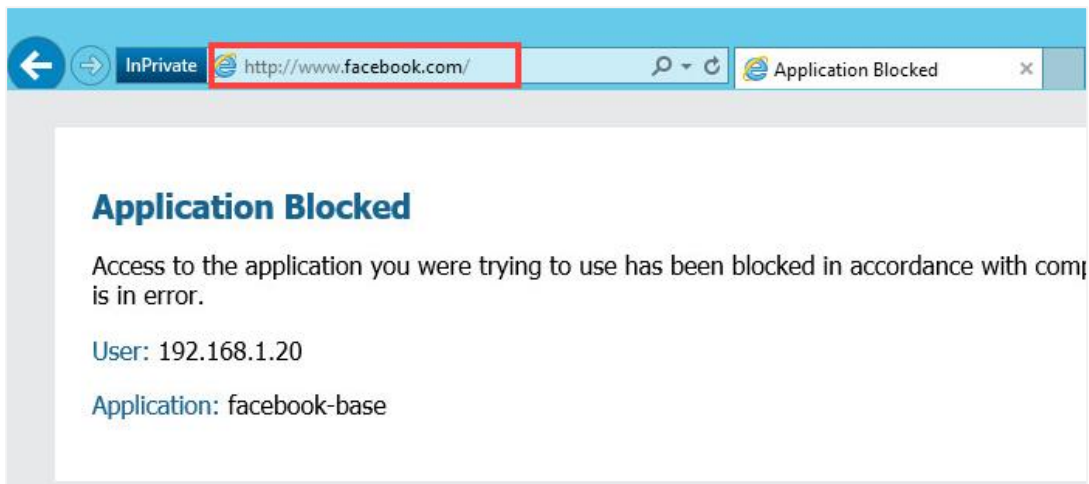
## 1.12 Test App-ID Changes

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



Notice the *Application Blocked Page* no longer displays for these applications.

- Using the same IE browser, browse to `www.facebook.com`.



Notice the *Application Blocked Page* now appears for *facebook-base*.

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



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

### 1.13 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 the 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.

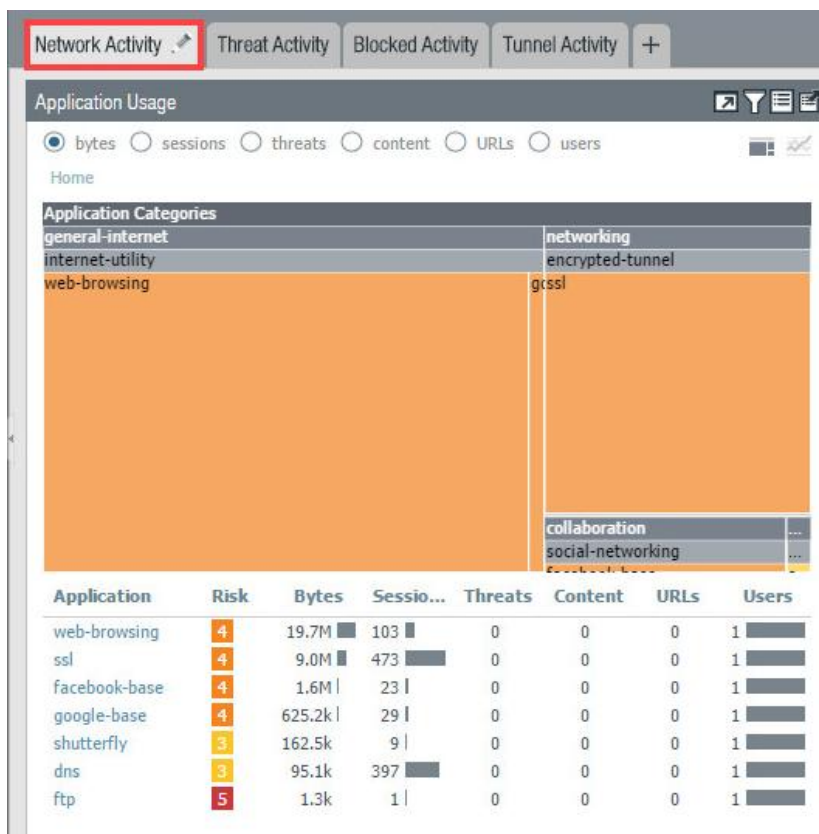
- Change focus to the firewall's web interface and click on the **ACC** tab to access the *Application Command Center*.



- 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:




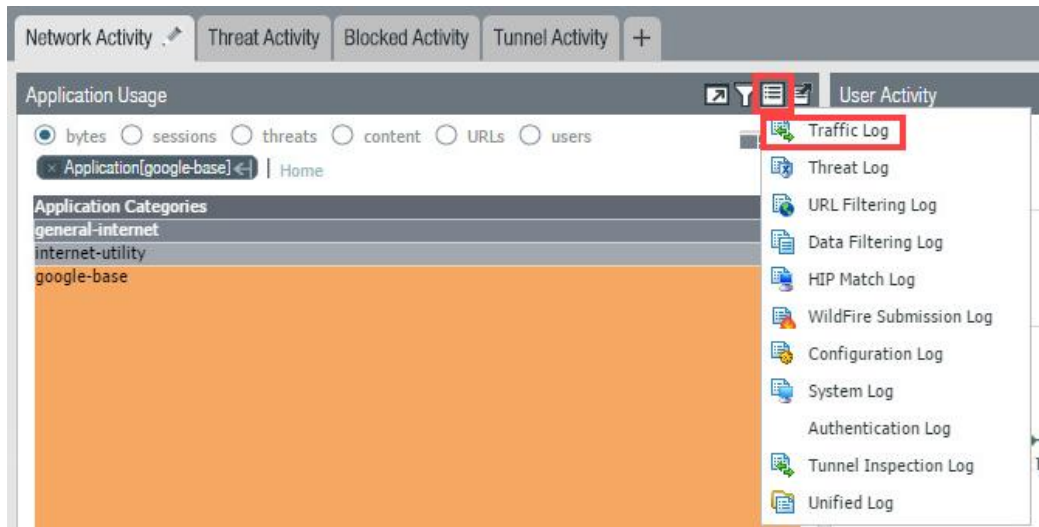
- On the **Network Activity** tab, the *Application Usage* pane shows application traffic generated so far (because the ACC relies on log aggregation, you may need to wait 15 minutes before the ACC displays all applications).



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

Application	Risk	Bytes	Sessio...	Threats	Content	URLs	Users
web-browsing	4	19.7M	103	0	0	0	1
ssl	4	9.0M	473	0	0	0	1
facebook-base	4	1.6M	23	0	0	0	1
google-base	4	625.2k	29	0	0	0	1
shutterfly	3	162.5k	9	0	0	0	1
dns	3	95.1k	397	0	0	0	1
ftp	5	1.3k	1	0	0	0	1

- Notice that the *Application Usage* pane updates to present only *google-base* information. In the *Application Usage* pane, click the **Jump to Logs** icon  and select **Traffic Log**.



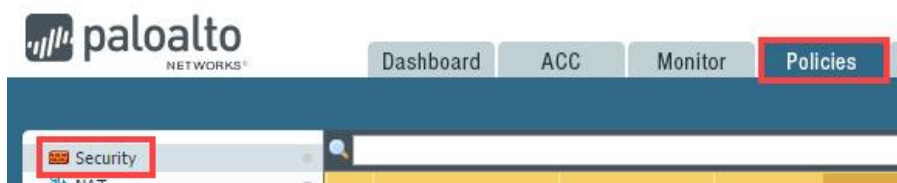
- After the *Traffic Log* is selected, a link automatically is made to the applicable log information with the filter set for a relevant time frame and for the *google-base* application.

(receive_time geq '2020/01/21 21:15:00') AND (receive_time leq '2020/01/21 22:14:59') AND ((app eq google-base))											
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
	01/21 22:14:22	end	inside	outside	192.168.1.20		172.217.15.66	443	google-base	allow	egress-outside-app-id
	01/21 22:14:22	end	inside	outside	192.168.1.20		172.217.15.66	443	google-base	allow	egress-outside-app-id
	01/21 22:14:22	end	inside	outside	192.168.1.20		172.217.15.66	443	google-base	allow	egress-outside-

- Leave the firewall web interface open to continue with the next task.

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

- In the firewall's web interface, select **Policies > Security**.



2. Select the **migrated-ftp-port-based** Security policy rule without opening it and click **Disable**.

	Name	Tags	Type	Zone	
1	egress-outside-app-id	egress	universal	inside	
2	egress-outside	egress	universal	inside	
3	internal-dmz-ftp	internal	universal	inside	
4	migrated-ftp-port-based	internal	universal	inside	
5	intrazone-default	none	intrazone	any	
6	interzone-default	none	interzone	any	

Add Delete Clone Override Revert Enable Disable Move

3. Select the **internal-dmz-ftp** Security policy rule without opening it and click **Enable**.

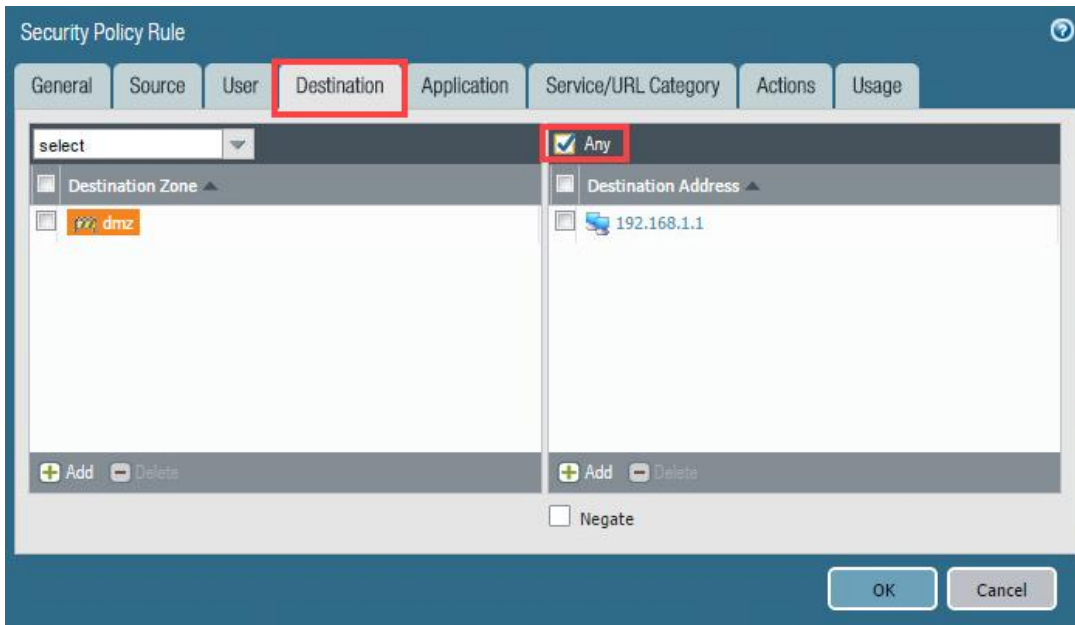
	Name	Tags	Type	Zone	
1	egress-outside-app-id	egress	universal	inside	
2	egress-outside	egress	universal	inside	
3	internal-dmz-ftp	internal	universal	inside	
4	migrated-ftp-port-based	internal	universal	inside	
5	intrazone-default	none	intrazone	any	
6	interzone-default	none	interzone	any	

Add Delete Clone Override Revert Enable Disable Move

- Click on **internal-dmz-ftp** to open the *Security policy rule* window.

	Name	Tags	Type	Zone
1	egress-outside-app-id	egress	universal	insid
2	egress-outside	egress	universal	insid
3	internal-dmz-ftp	internal	universal	insid
4	migrated-ftp-port-based	internal	universal	insid

- In the *Security Policy Rule* window, click the **Destination** tab and select the **Any** checkbox in the *Destination Address* pane.



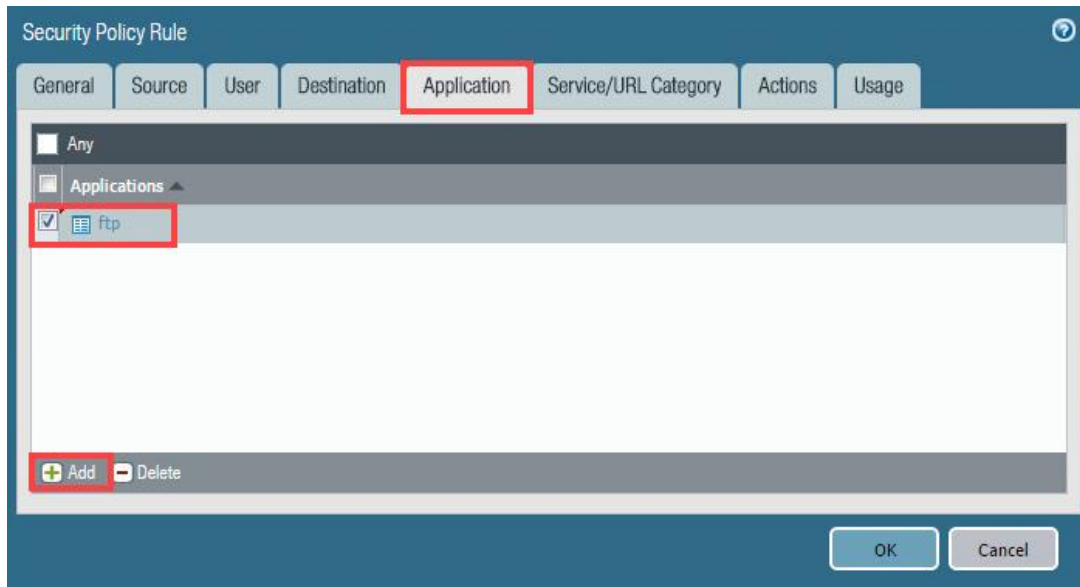
The screenshot shows the 'Security Policy Rule' window with the 'Destination' tab selected. The 'Destination Address' pane has the 'Any' checkbox checked. The 'Destination Zone' pane shows 'dmz' selected. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.



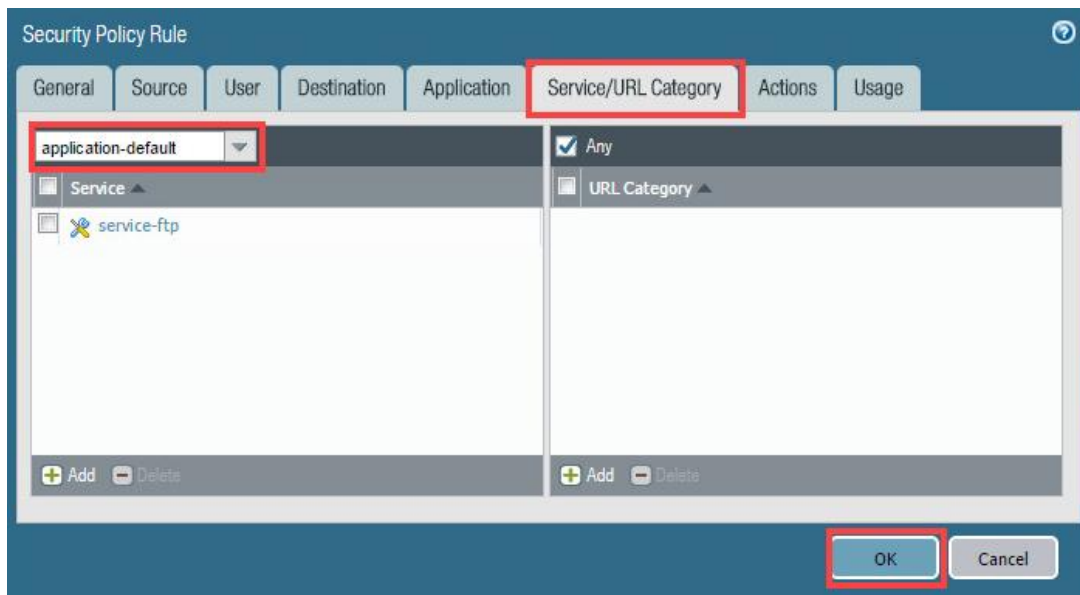
Selection of the *Any* checkbox will automatically remove the *192.168.1.1* entry when you click the *OK* button to save the configuration change.



6. In the *Security Policy Rule* window, click the **Application**. Click the **Add** button and select **ftp** from the list.



7. In the *Security Policy Rule* window, click the **Service/URL Category** tab. In the *Services* pane, select **application-default** from the drop-down menu. Click **OK**.



Selection of *application-default* does not change the service behavior because, in the application database, FTP is allowed only on port 21 by default. Selection of *application-default* from the services drop-down menu automatically will remove the *service-ftp* entry when you click the *OK* button to save the configuration change.

8. **Commit** all changes.



9. Open a *Command Line Interface* window by clicking on the **CMD** icon located in the toolbar.
10. In the *CMD* window, enter the command below, followed by pressing the **Enter** key.

```
C:\Windows\System32> ftp 192.168.50.10
```

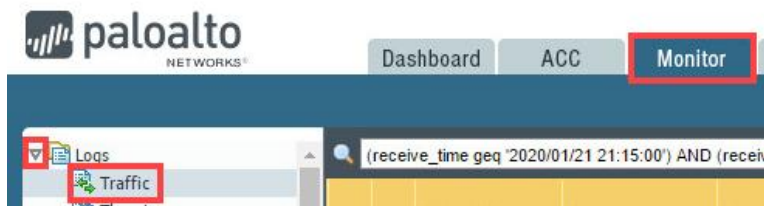
11. When prompted for user credentials, login as **lab-user** with the password of **paloalto**.

```
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>
```


12. Enter **bye** at the FTP prompt.

```
ftp> bye
221 Goodbye.
C:\Windows\System32>_
```

13. Enter **exit** to close the *CMD* window.
14. Change focus back to the firewall's web interface and navigate to **Monitor > Logs > Traffic**.



15. Clear any existing log filters and locate the log entry for the FTP session. Notice that the *internal-dmz-ftp* rule allowed the FTP traffic.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
	01/21 22:29:35	end	inside	dmz	192.168.1.20		192.168.50.10	21	ftp	allow	internal-dmz-ftp



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

16. The lab is now complete; you may end the reservation.