PALO ALTO NETWORKS - EDU-210

Lab 4: App-ID

Document Version: 2020-06-26

Contents

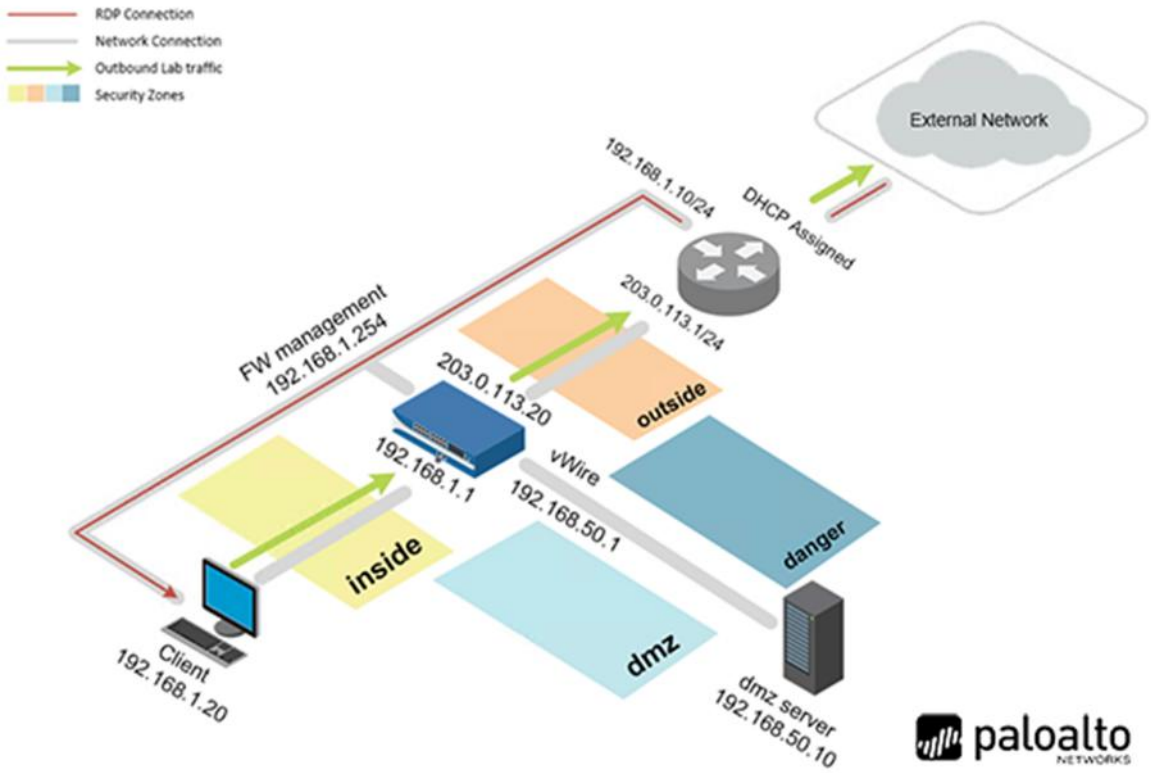
Introduction

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.

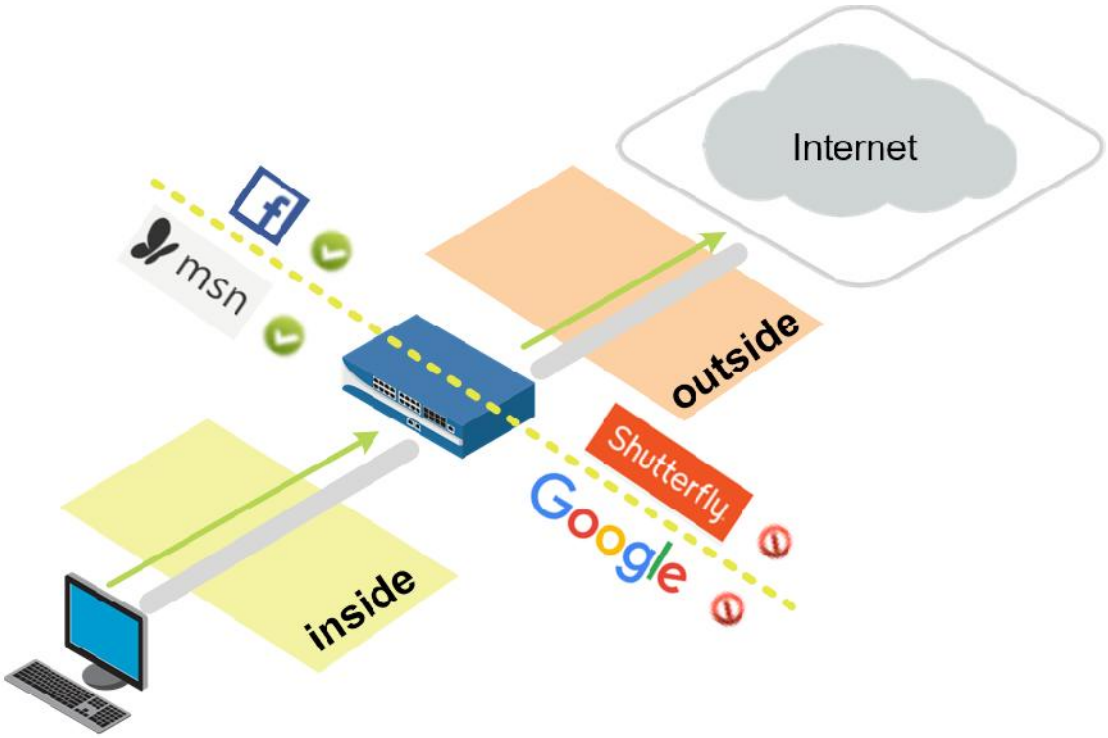
Objectives

- 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`	`Train1ng$`
Firewall	192.168.1.254	`admin`	`Train1ng$`

4 App-ID

4.0 Load Lab Configuration

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

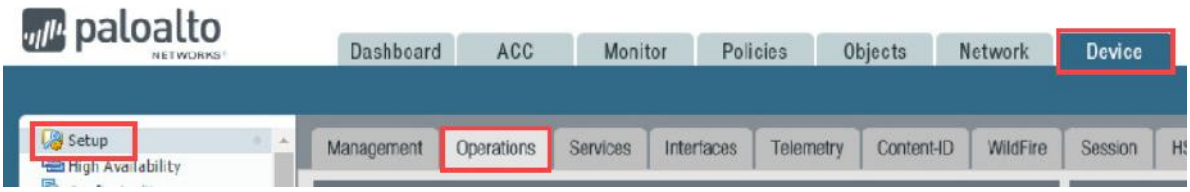
> To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

2. Log in as `lab-user` using the password `Train1ng$`.

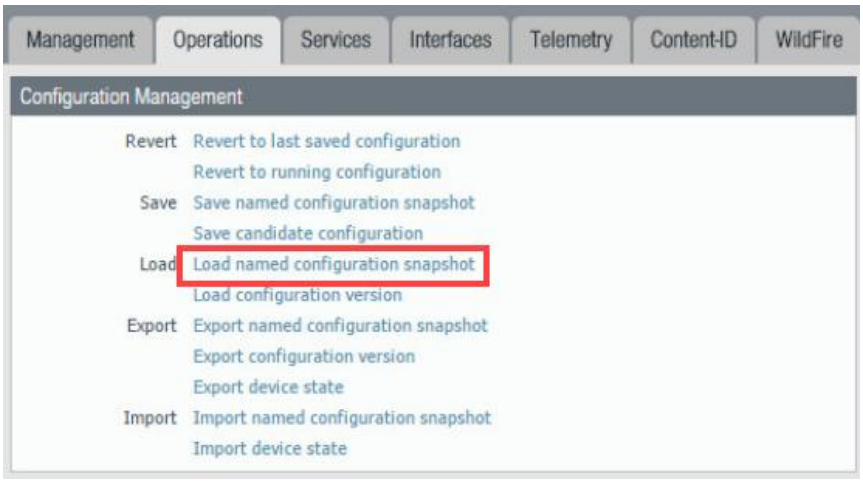
3. Launch the **Chromium Web Browser** and connect to `https://192.168.1.254`.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	`admin`
Password	`Train1ng$`

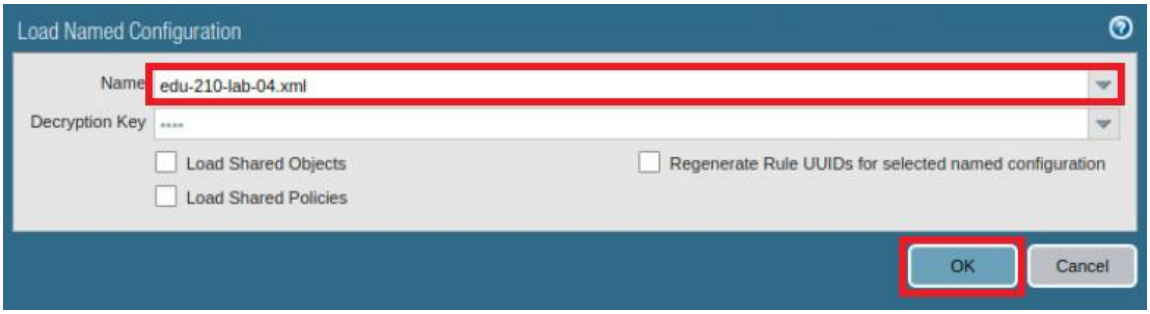
6. In the web interface, select **Device > Setup > Operations**.



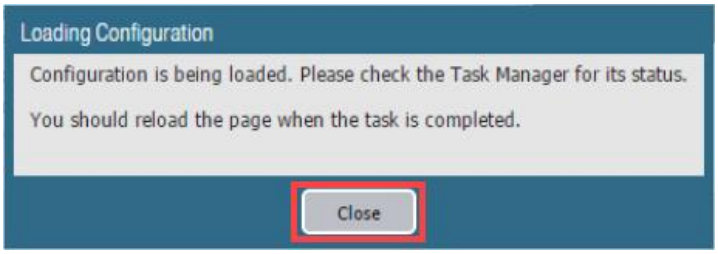
7. Click **Load named configuration snapshot**:



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



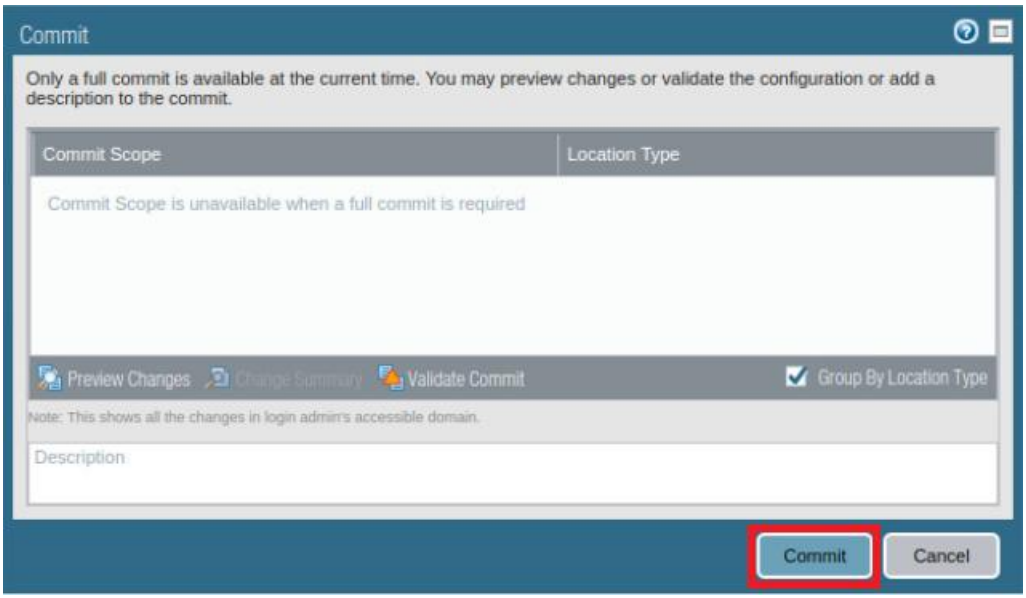
9. Click **Close**.



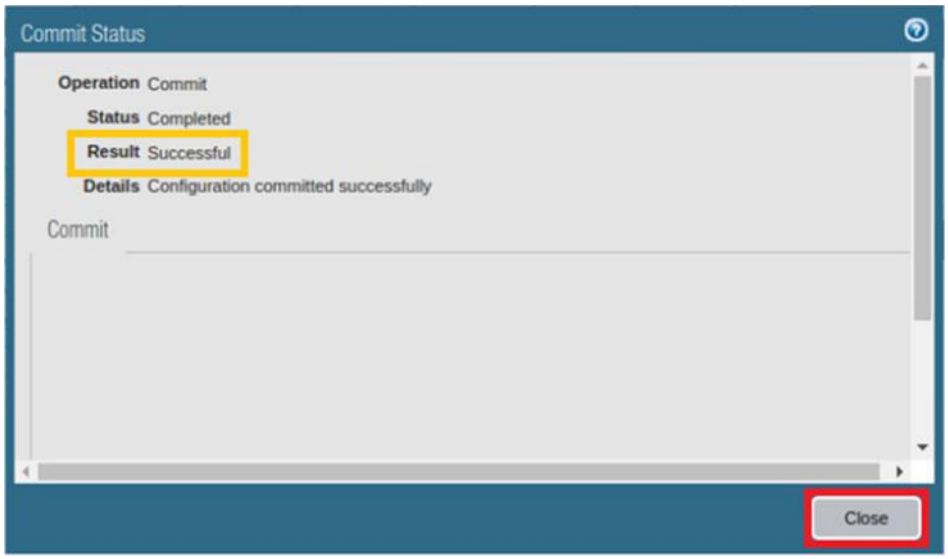
The following instructions are the steps to execute a **"Commit All"** as you will perform many times throughout these labs.

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.



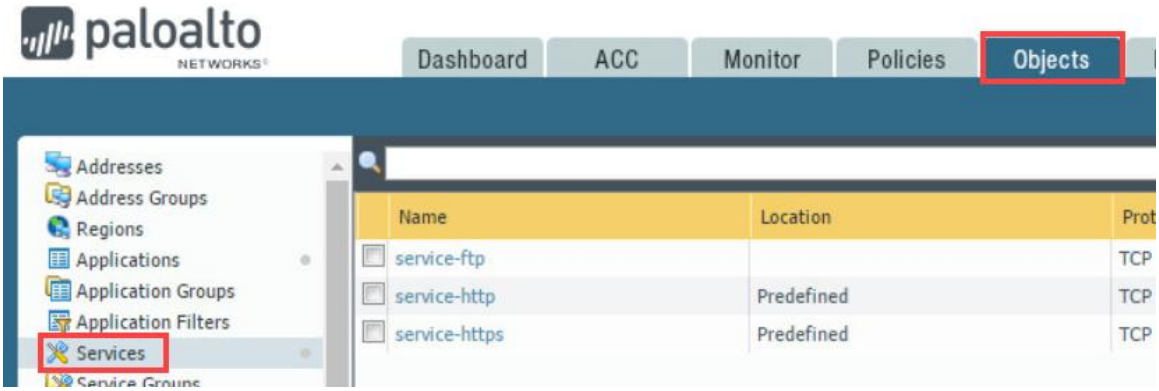
13. Leave the firewall web interface open to continue with the next task.

4.1 Verify an FTP Service Object

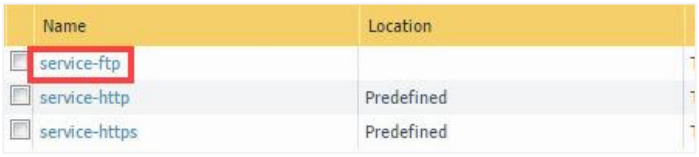
At the end of this lab, you will use the *Policy Optimizer* tool to migrate an FTP port-based rule to an FTP application-based rule. However, to prepare for that part of the lab exercise, you now will configure and use an FTP port-based Security Policy Rule. You will perform this activity now because 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**.

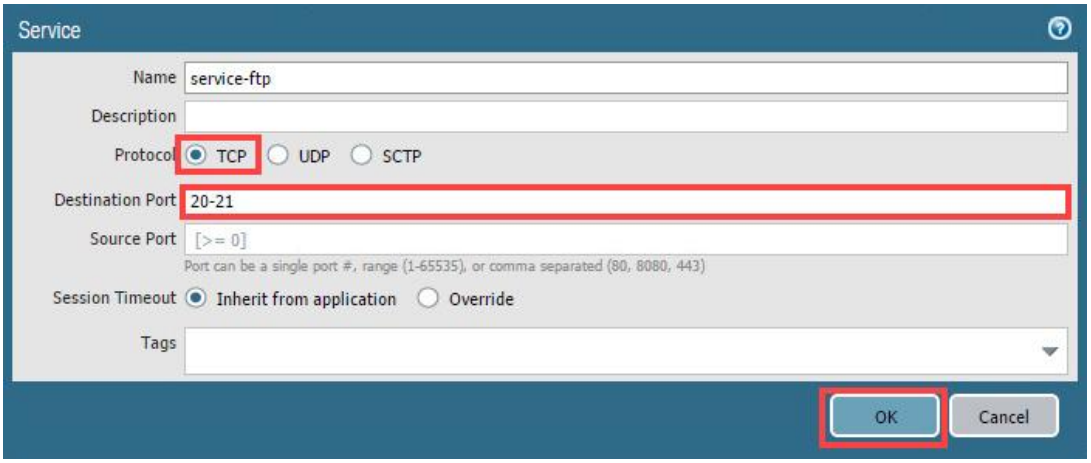


2. Click on the **service-ftp** object from the list to configure the Service.



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

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

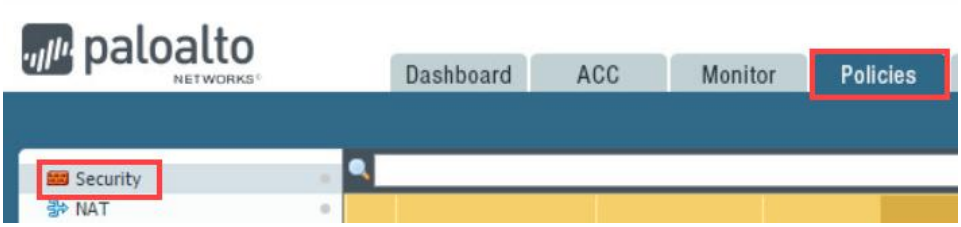


4. Leave the firewall web interface open to continue with the next task.

4.2 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.

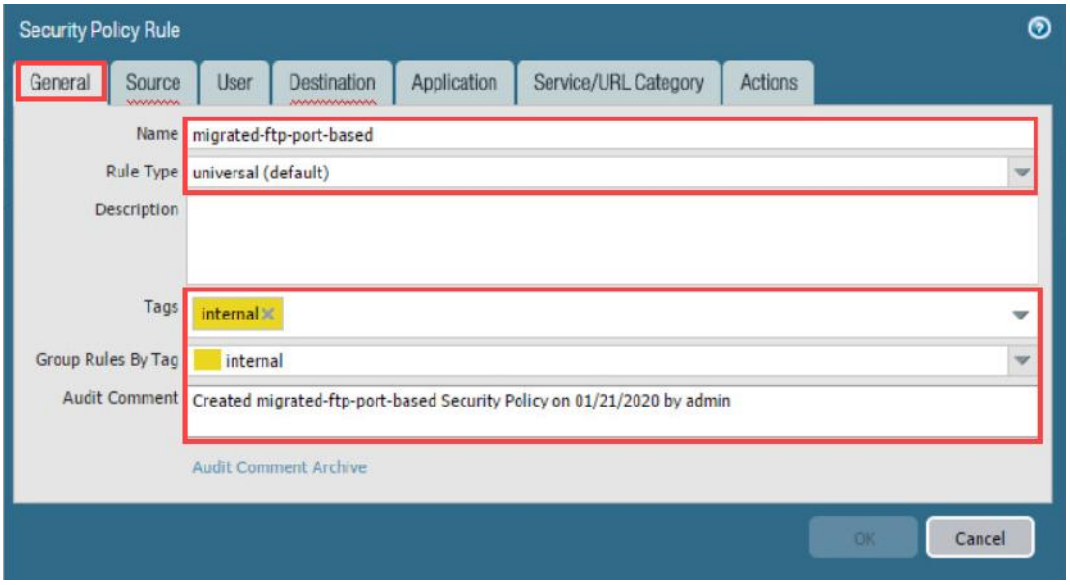
1. In the web interface, select **Policies > Security**.



2. Click **Add** in the lower-left corner of the panel to create a new Security Policy Rule.

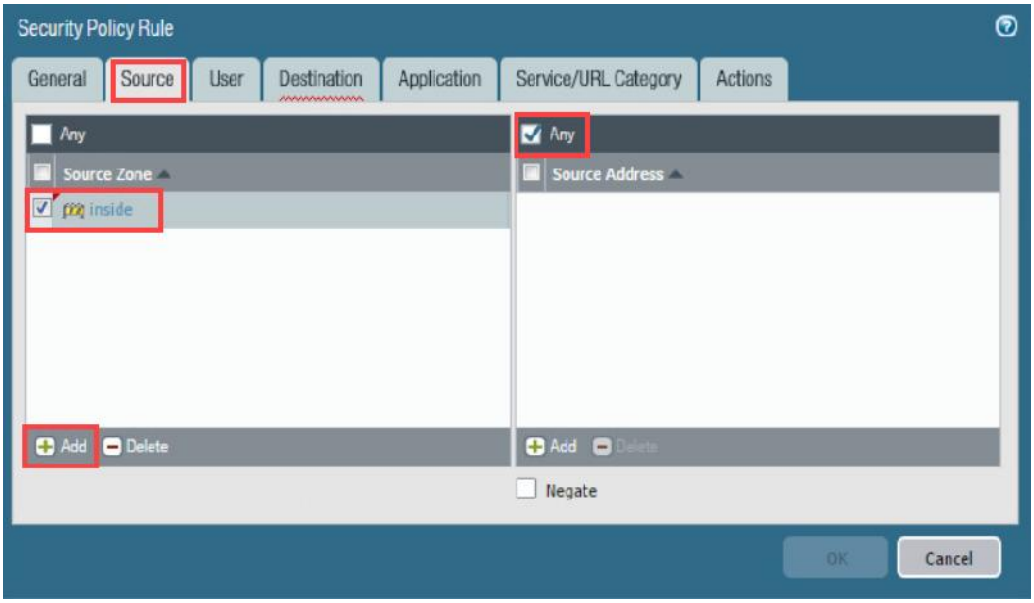
3. In the *Security Policy Rule* window, while on the *General* tab, configure the following:

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



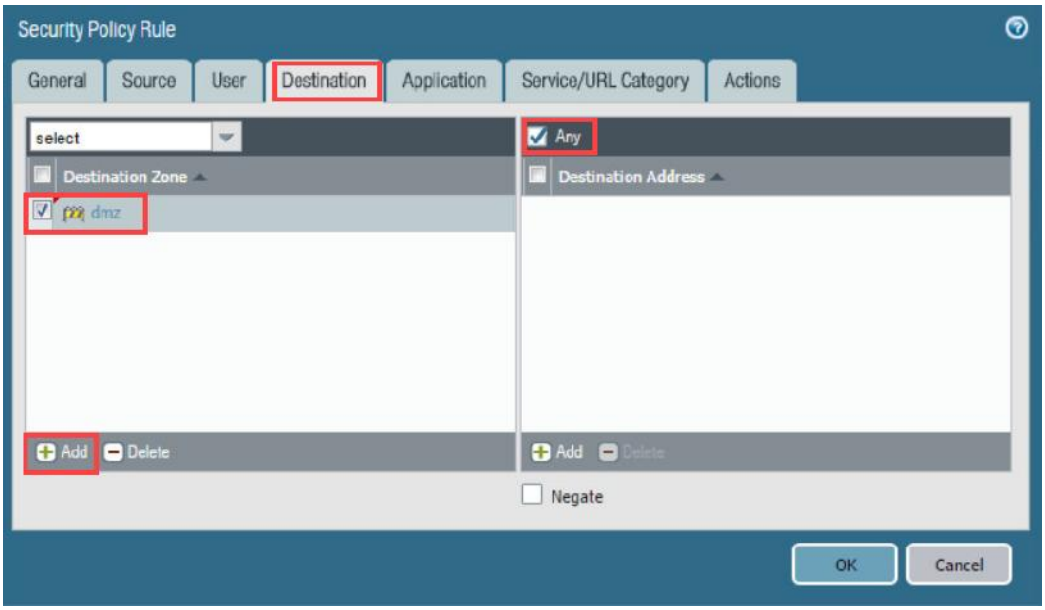
4. In the *Security Policy Rule* window, click on the **Source** tab and configure the following:

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

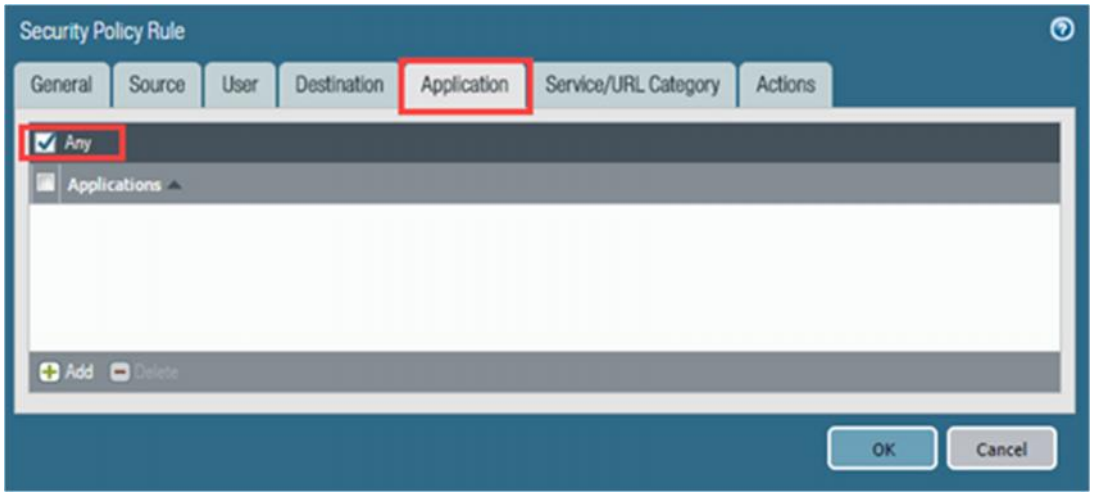


5. In the *Security Policy Rule* window, click on the **Destination** tab and configure the following:

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

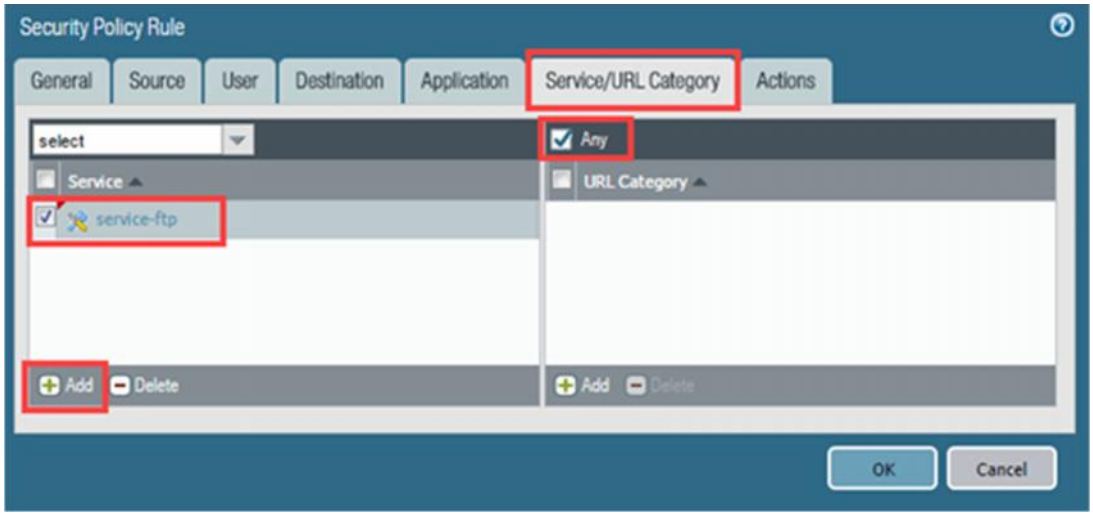


6. In the *Security Policy Rule* window, click on the **Application** tab and verify that the **Any** checkbox is selected.



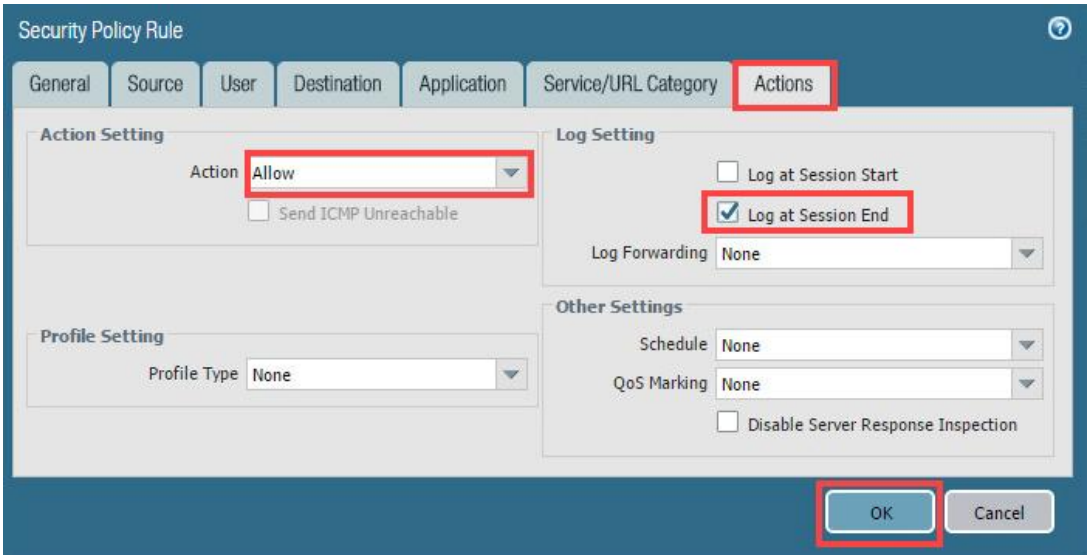
7. In the *Security Policy Rule* window, click on the **Service/URL Category** tab and configure the following:

Parameter	Value
Service	Click **Add** and select **service-ftp**
URL Category	Verify that the **Any** checkbox is selected

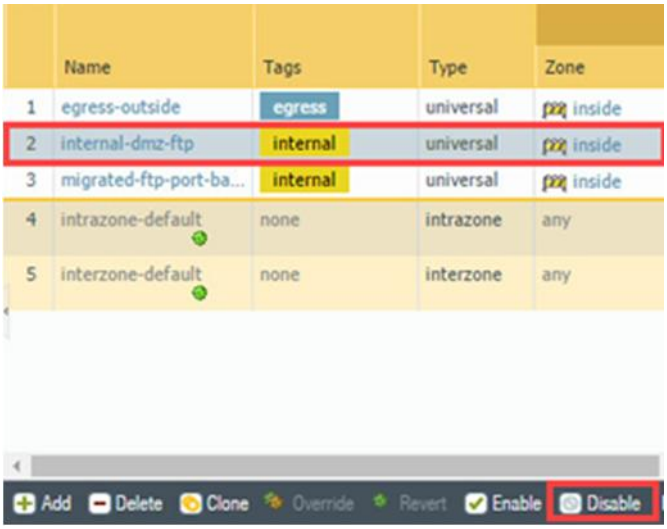


8. In the *Security Policy Rule* window, click on the **Actions** tab and verify the following. Once finished, click **OK**.

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



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

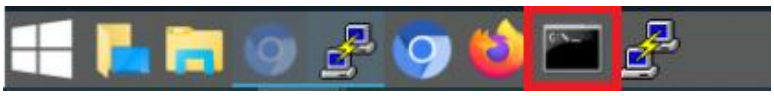


10. **Commit** all changes.

4.3 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 *Terminal* window by clicking on the **Xfce Terminal** icon in the toolbar.

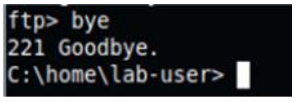


2. In the Terminal window, enter the command below, followed by pressing the **Enter** key to connect to the FTP server.

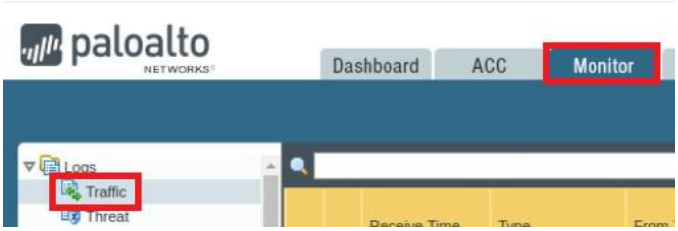
```
C:\home\lab-user> ftp 192.168.50.10
```

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

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



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



7. Make sure to clear any filters that may exist and locate the log entry for the FTP session.

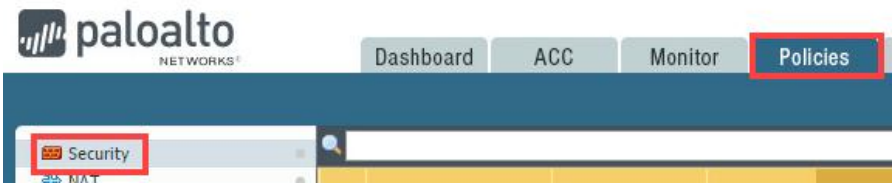
Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	Dynamic User Group	To Port	Application	Action	Rule
03/14 18:54:52	end	inside	dmz	192.168.1.20		192.168.50.10		21	ftp	allow	migrated-ftp-port-based

Notice the Security Policy Rule matched the session with *migrated-ftp-port-based*.

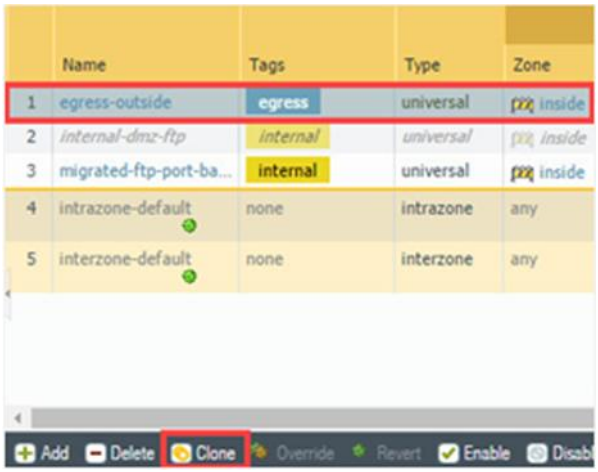
8. Leave the firewall web interface open to continue with the next task.

4.4 Create an App-ID Security Policy Rule

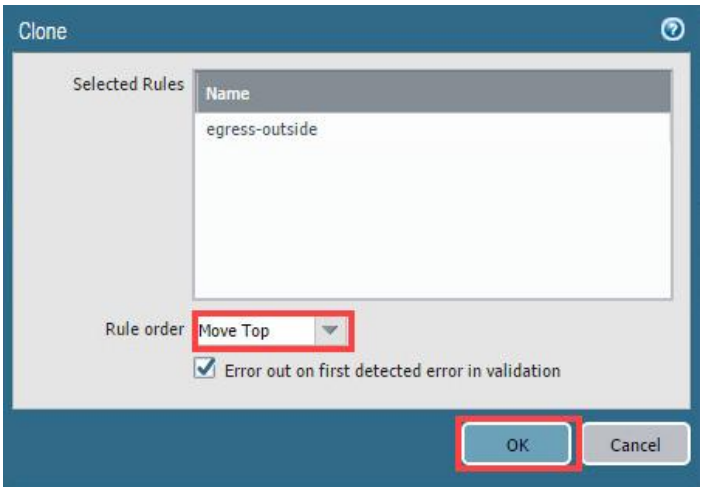
1. In the web interface, select **Policies > Security**.



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

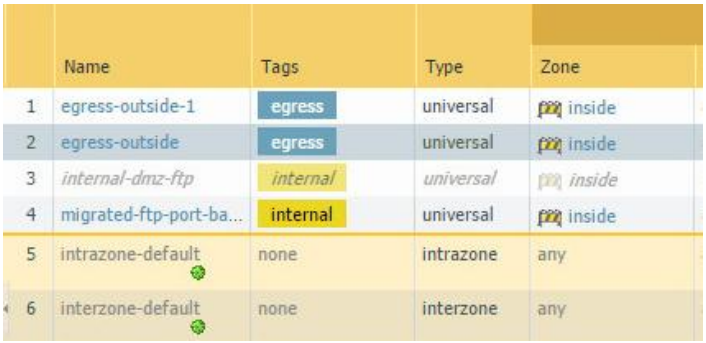


3. In the *Clone* window, on the *Rule order* dropdown list, select **Move top**. Click **OK**.



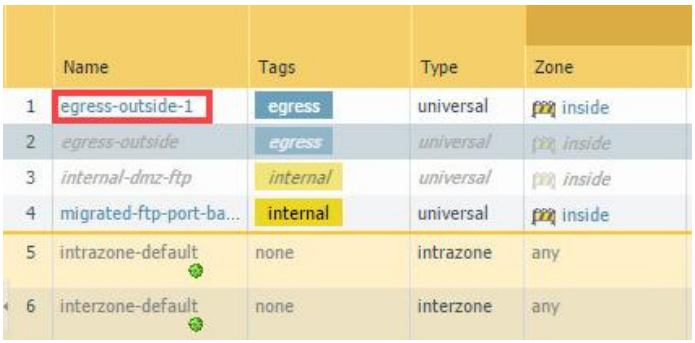
Remember that rule order is important. The firewall compares a packet's characteristics to each rule in the Security Policy starting in order.

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



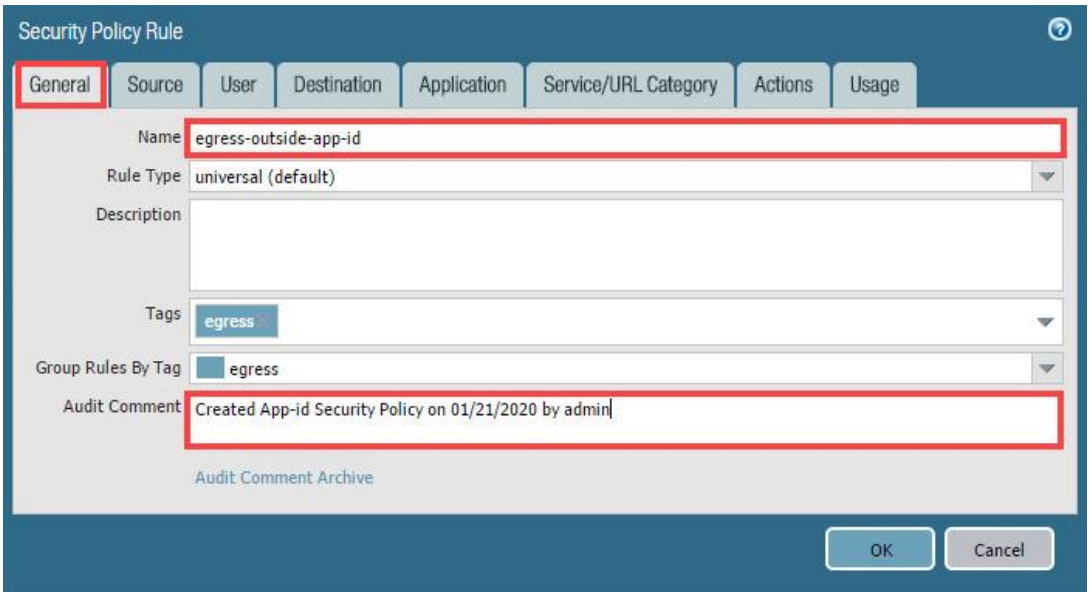
5. With the original **egress-outside** Security policy rule still selected, click **Disable**.

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



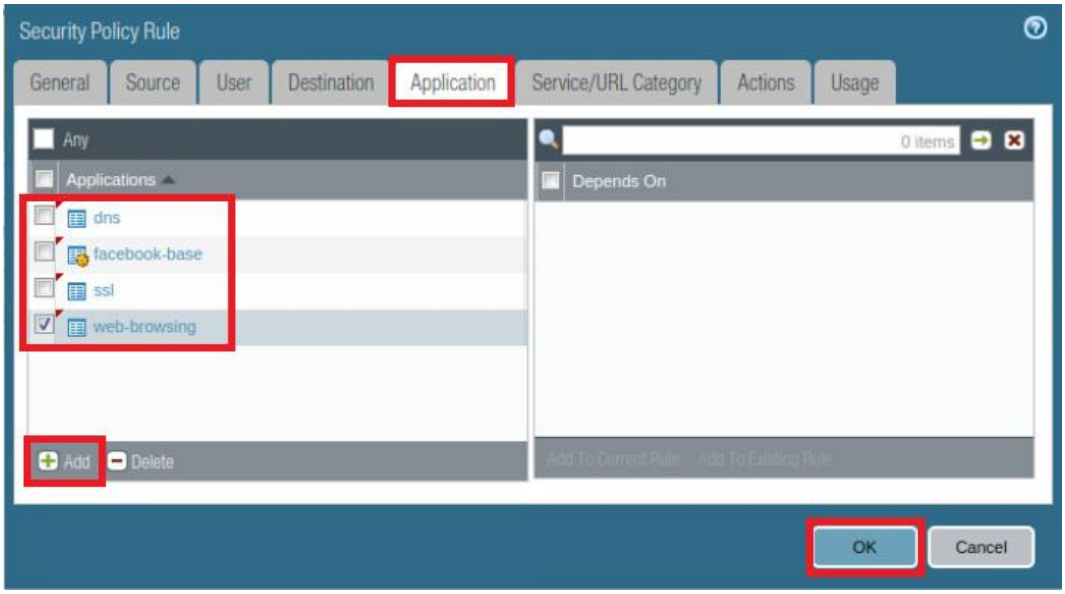
7. In the *Security Policy Rule* window, while on the *General* tab, configure the following:

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



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

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



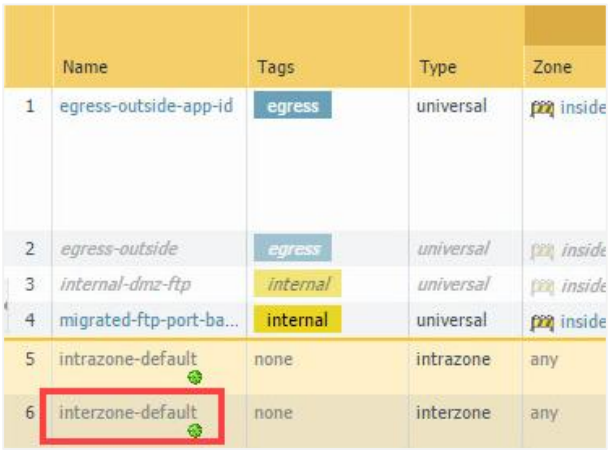
The firewall matches traffic to the list of applications in a Security Policy Rule. If the firewall detects a change in an application, or an application shift, the firewall will rematch the traffic to the list of applications in the Security policy.

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

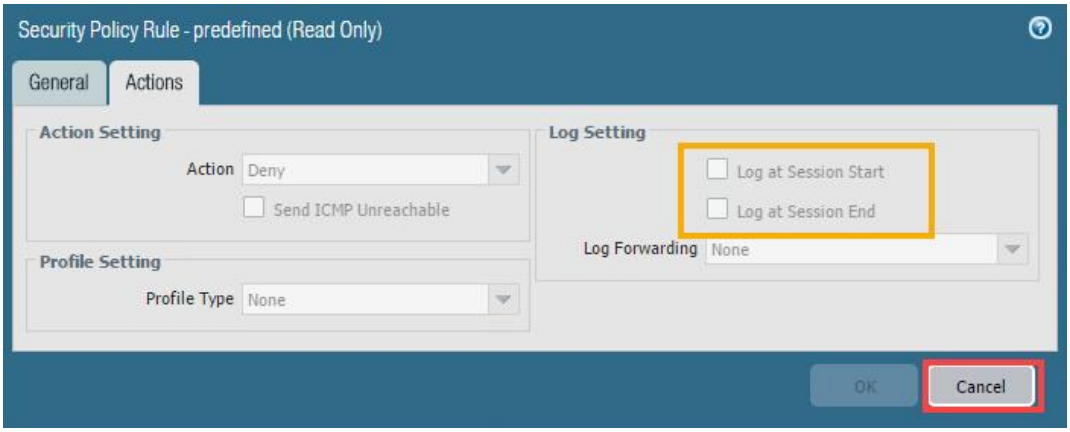
4.5 Enable Interzone Logging

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.

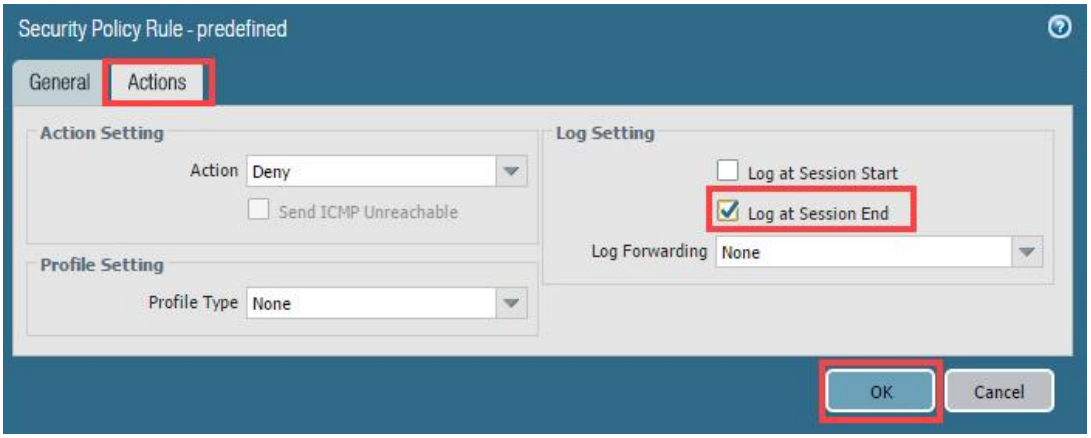


2. In the *Security Policy-Rule - predefined (Read Only)* window, click the **Actions** tab. Notice that *Log at Session Start* and *Log at Session End* are deselected, and cannot be edited. Click **Cancel**.



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

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

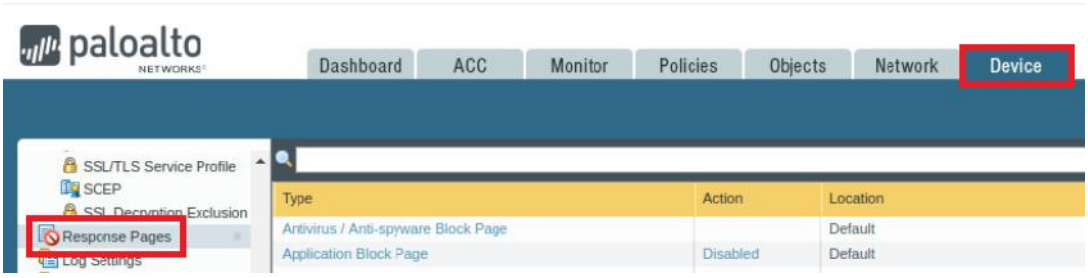


5. Leave the firewall web interface open to continue with the next task.

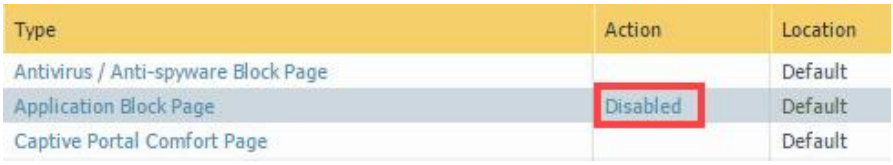
4.6 Enable the Application Block Page

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

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



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



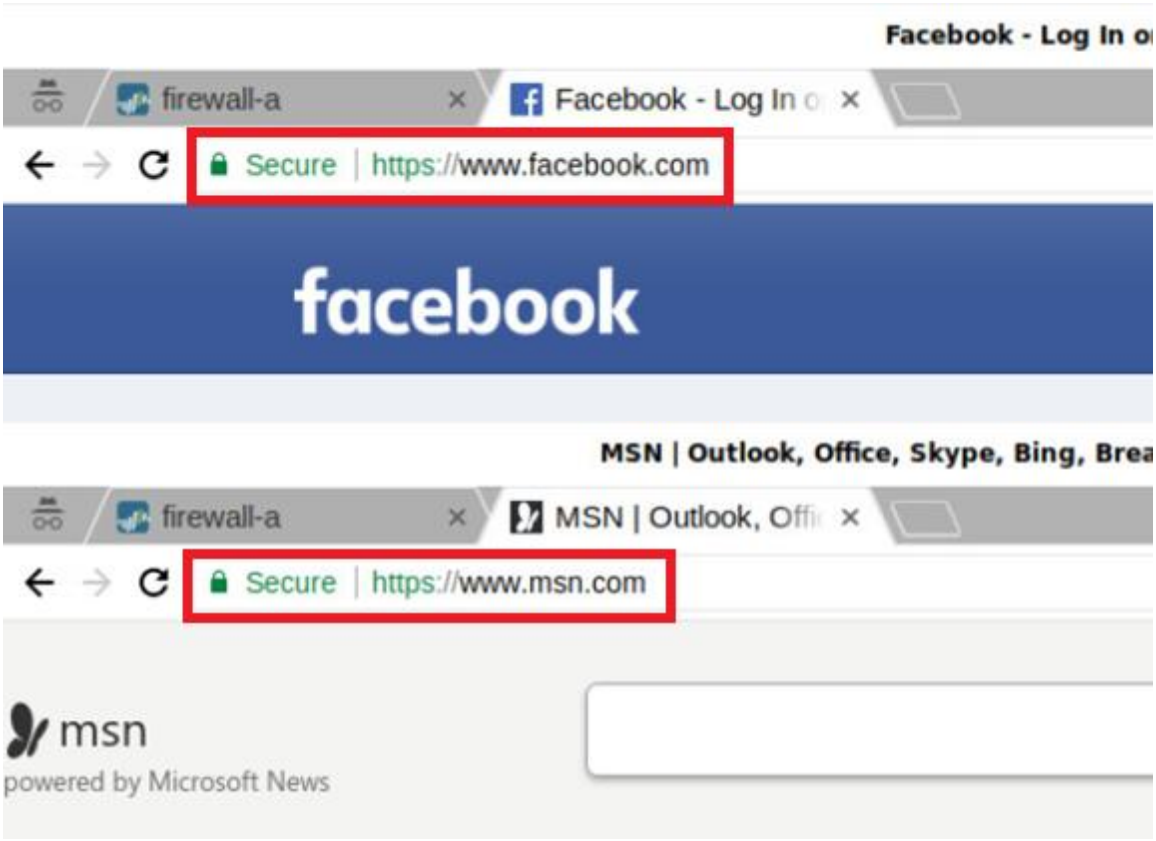
3. In the *Application Block Page* window, select the **Enable Application Block Page** checkbox. Click **OK**.

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.

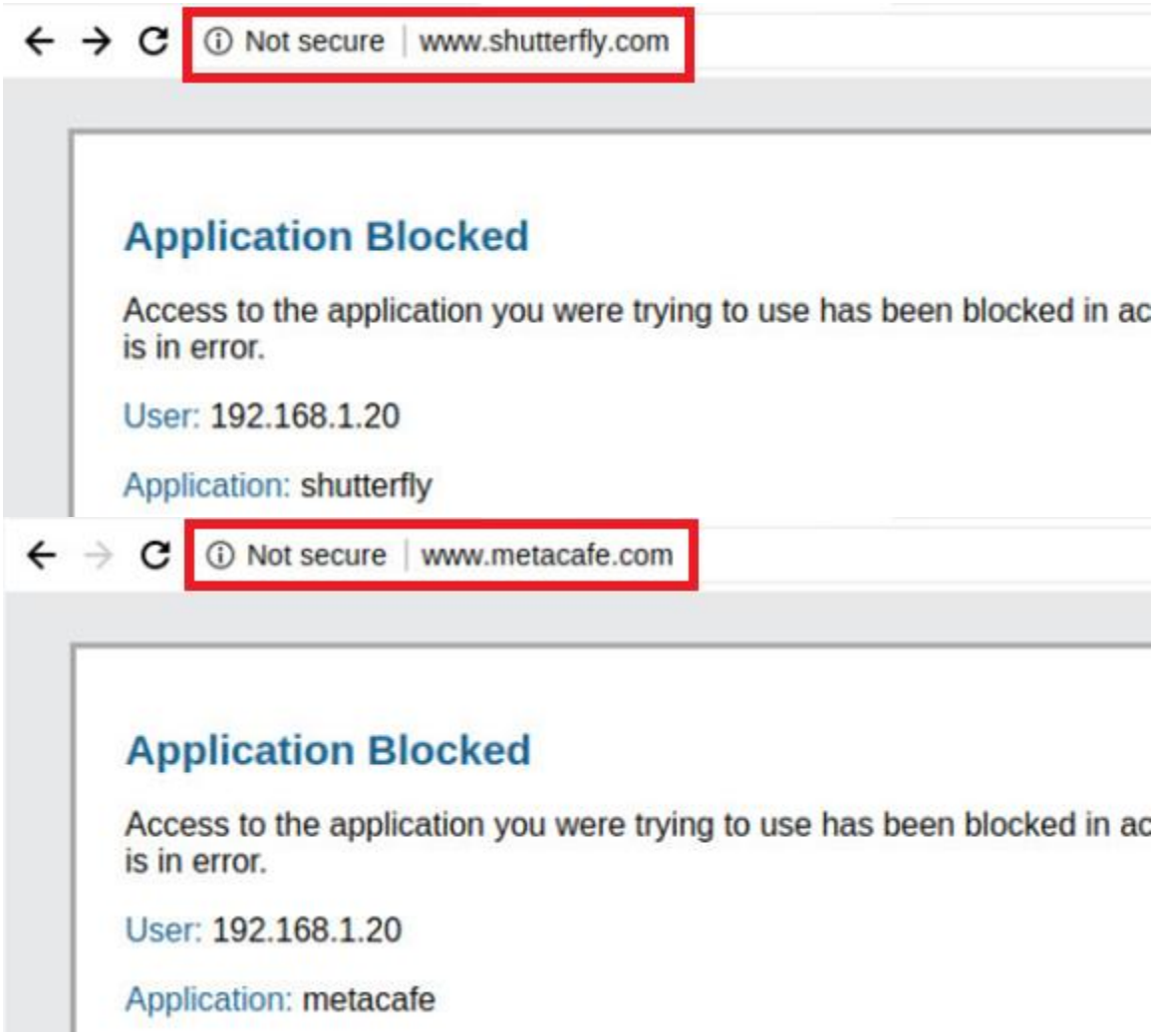
4.7 Test Application Blocking

1. Open a new tab in **Chromium Web Browser** and browse to `www.facebook.com` and `www.msn.com`.



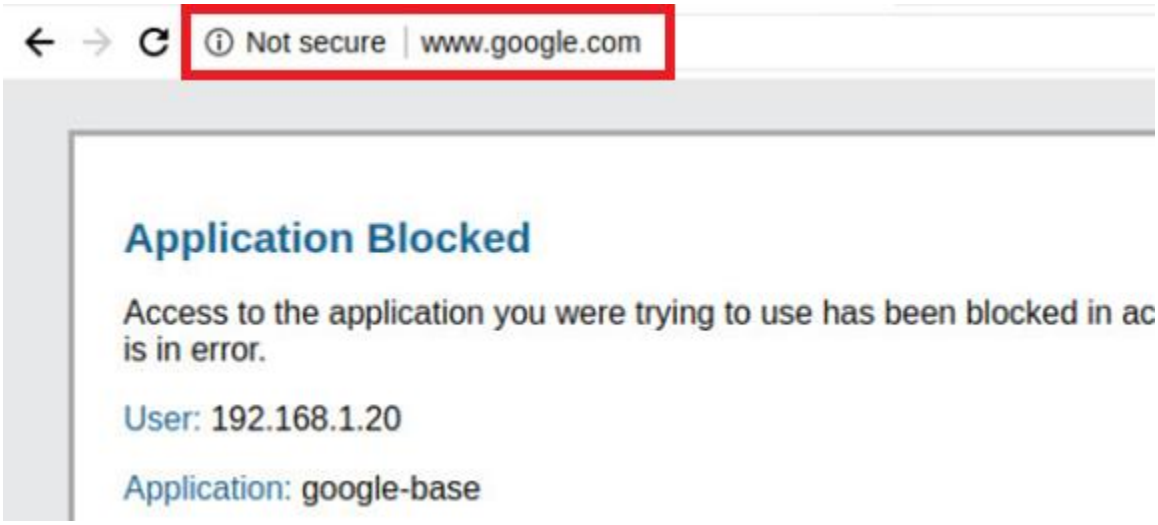
You should be able to successfully connect to the Facebook and MSN websites.

2. Using the same browser tab, browse to **`www.shutterfly.com`** and **`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 s*hutterfly* 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 s*hutterfly* and *metacafe*, and currently it is not allowed in any of the firewall Security Policy Rules.

3. Using the same *browser tab*, browse to **`www.google.com`** and verify that google-base is also being blocked.



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

4.8 Review Logs

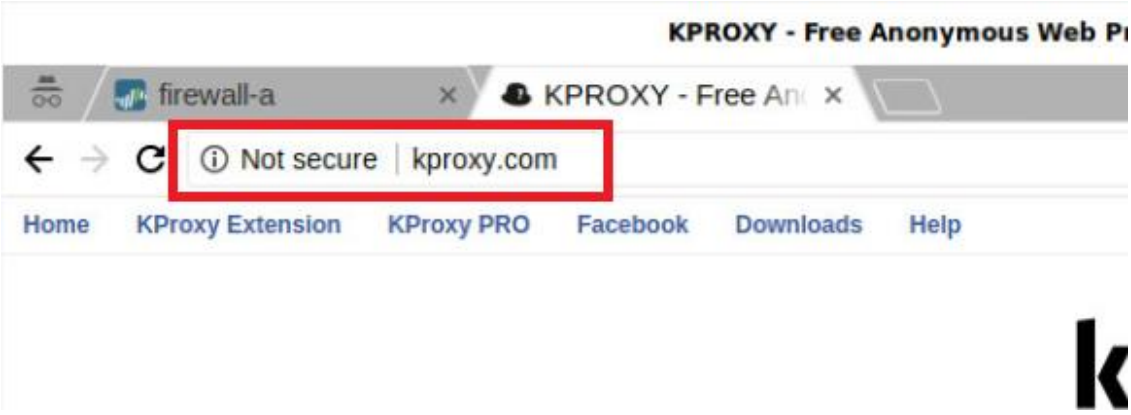
1. Change focus to the firewall's web interface and navigate to **Monitor > Logs > Traffic**

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.

4.9 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.

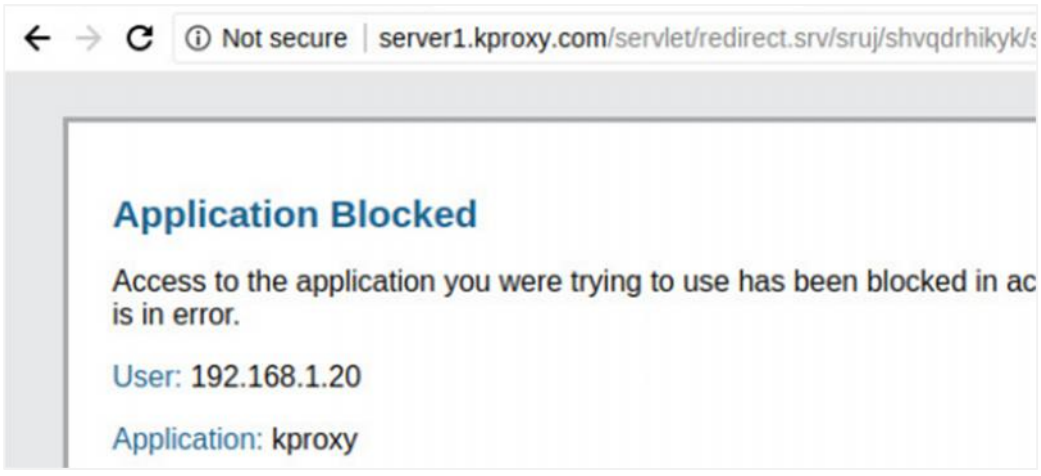
1. Open a new tab in **Chromium Web Browser** and browse to `kproxy.com`.



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!**.

3. An Application Blocked page opens, showing that the **kproxy** application was blocked.



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

4.10 Review Logs

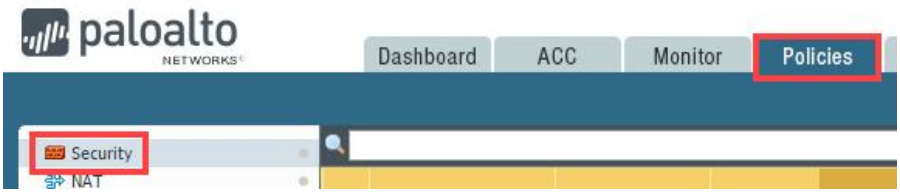
1. In the web interface, select **Monitor > Logs > Traffic**.
2. Clear the log filter text box and type **`(app eq kproxy)`** followed by pressing the **Enter** key.

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.

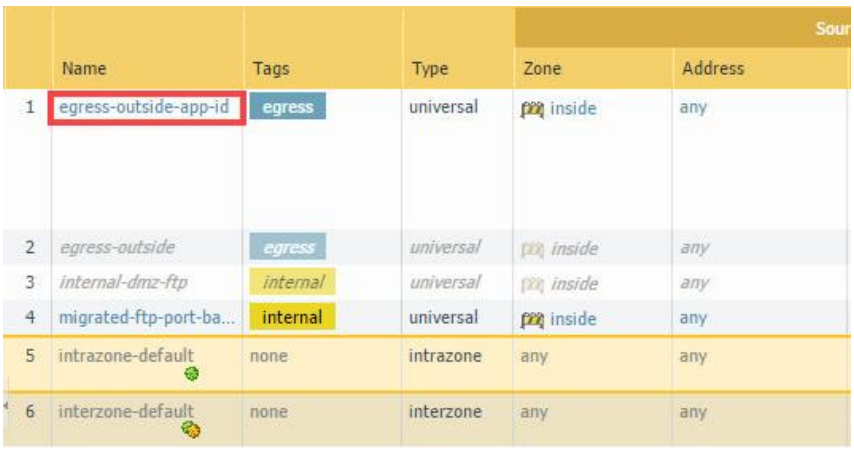
3. Leave the firewall web interface open to continue with the next task.

4.11 Modify the App-ID Security Policy Rule

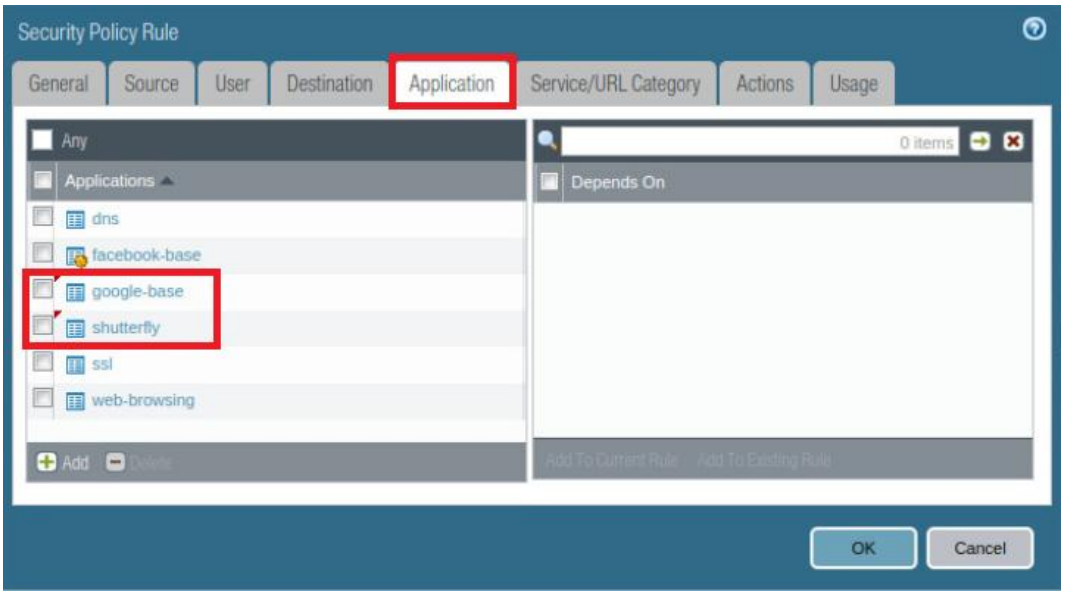
1. In the web interface, select **Policies > Security**.



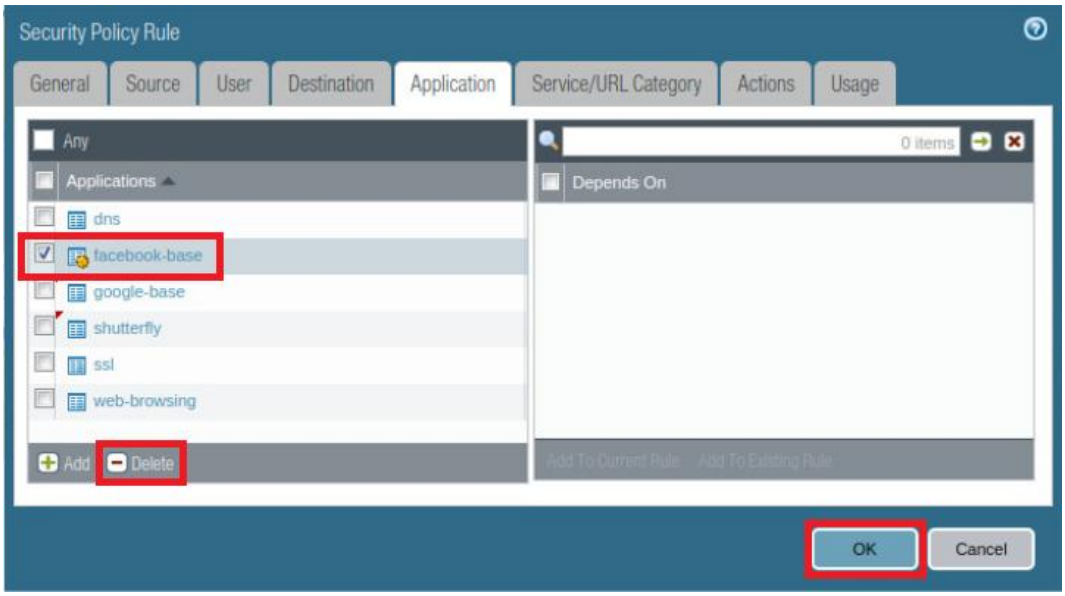
2. Click **egress-outside-app-id** to open the *Security Policy Rule*.



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**.



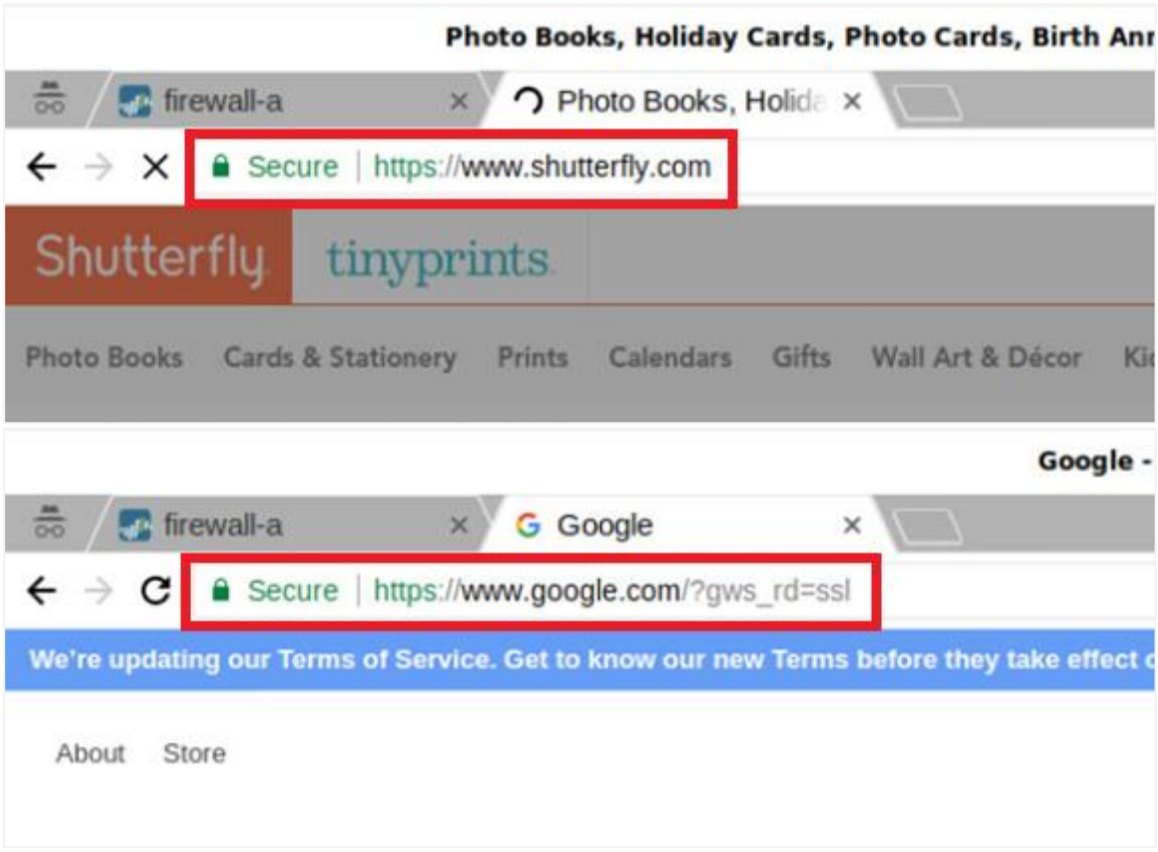
4. Next, select **facebook-base** followed by clicking the **Delete** button to remove the application from the rule. Once finished, click **OK**.



5. **Commit** all changes.

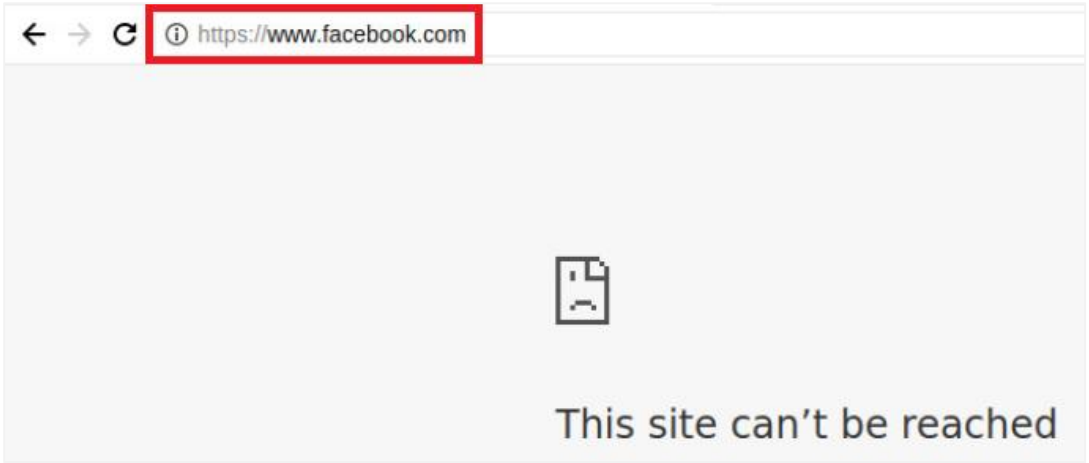
4.12 Test App-ID Changes

1. Open a new tab in **Chromium Web Browser** and browse to `www.shutterfly.com` and `www.google.com`.



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

2. Using the browser tab, browse to `www.facebook.com`.



Notice Facebook no longer loads. If the site didn't automatically redirect to https the *Application Blocked Page* would appear for *facebook-base*. Since it redirects to https the "This site can't be reached" error comes up instead.

3. Close all browser tabs except for the firewall web interface.

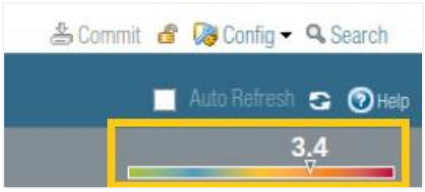
The web-browsing Application signature applies only to browsing that does not match any other Application signature.

4.13 Observe the Application Command Center

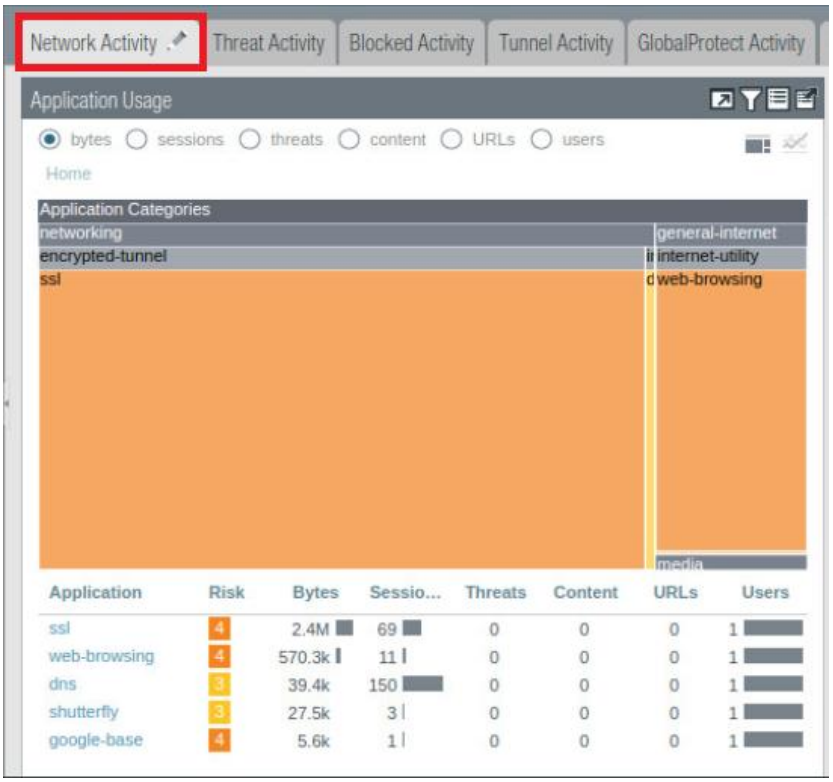
The *Application Command Center*, or *ACC*, is an analytical tool that provides useful intelligence on activity within your network. The *ACC* uses the firewall logs as the source for the graphically depicting traffic trends on your network. The graphical representation enables you to interact with the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

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

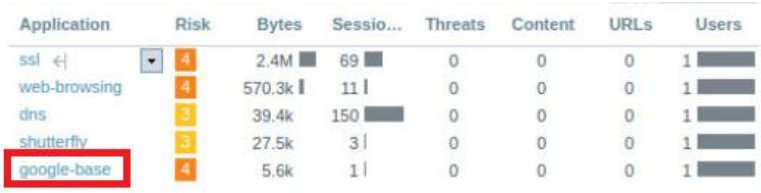
Note that the upper-right corner of the *ACC* displays the total risk level for all traffic that has passed through the firewall thus far:



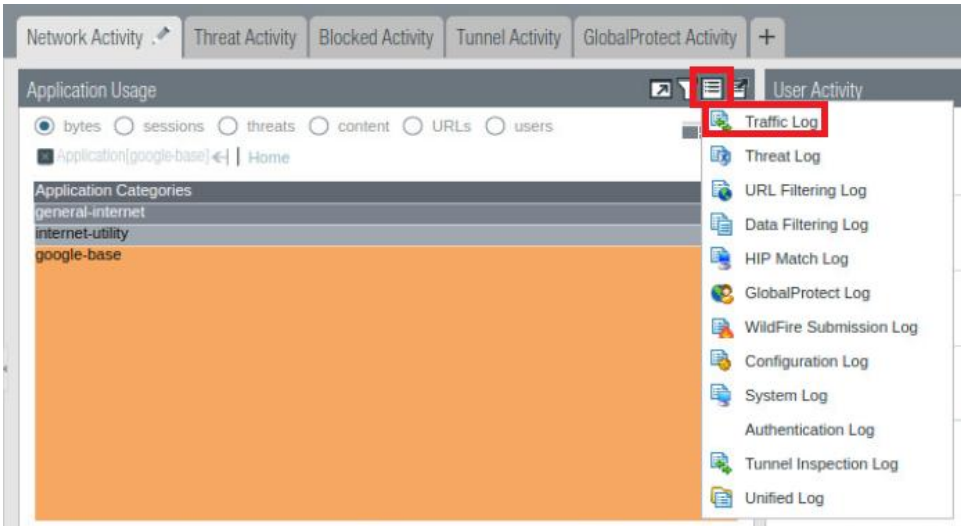
2. On the **Network Activity** tab, the *Application Usage* pane shows application traffic generated so far (because the *ACC* relies on log aggregation, you may need to wait 15 minutes before the *ACC* displays all applications).



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



4. 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**.

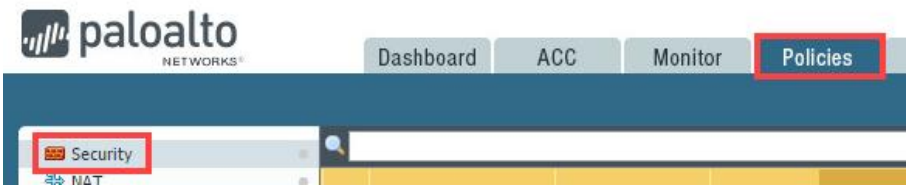


5. After the *Traffic Log* is selected, a link automatically is made to the applicable log information with the filter set for a relevant time frame and for the *google-base* application.

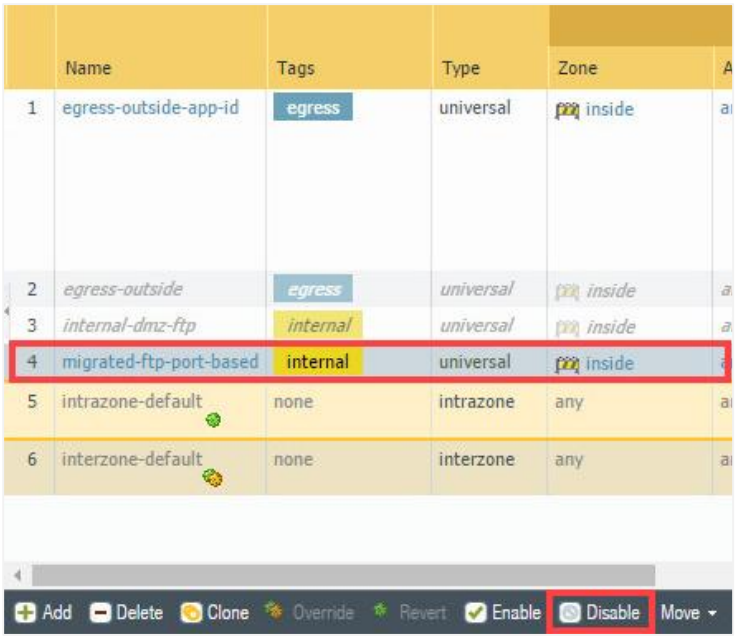
6. Leave the firewall web interface open to continue with the next task.

4.14 Migrate Port-Based Rule to Application-Aware Rule

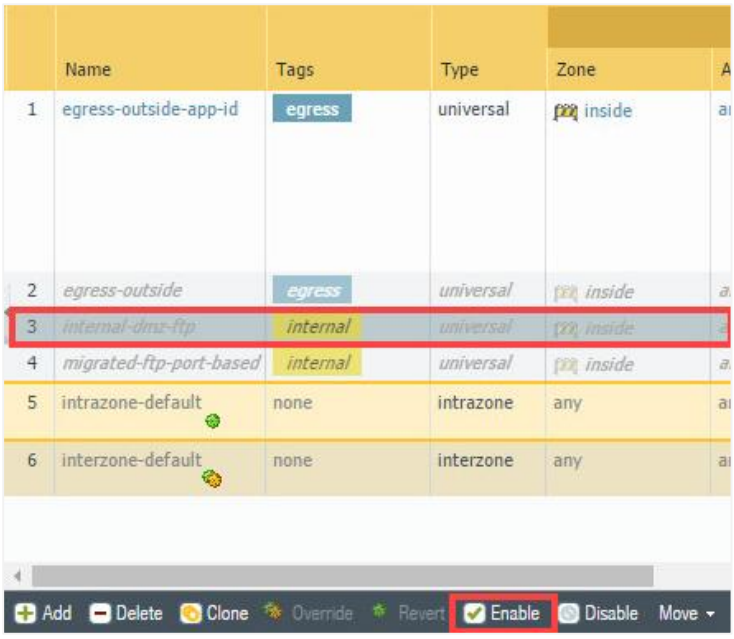
1. In the firewall's web interface, select **Policies > Security**.



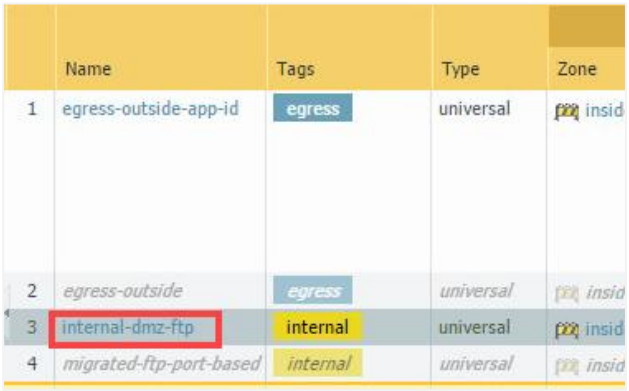
2. Select the **migrated-ftp-port-based** Security Policy Rule without opening it and click **Disable**.



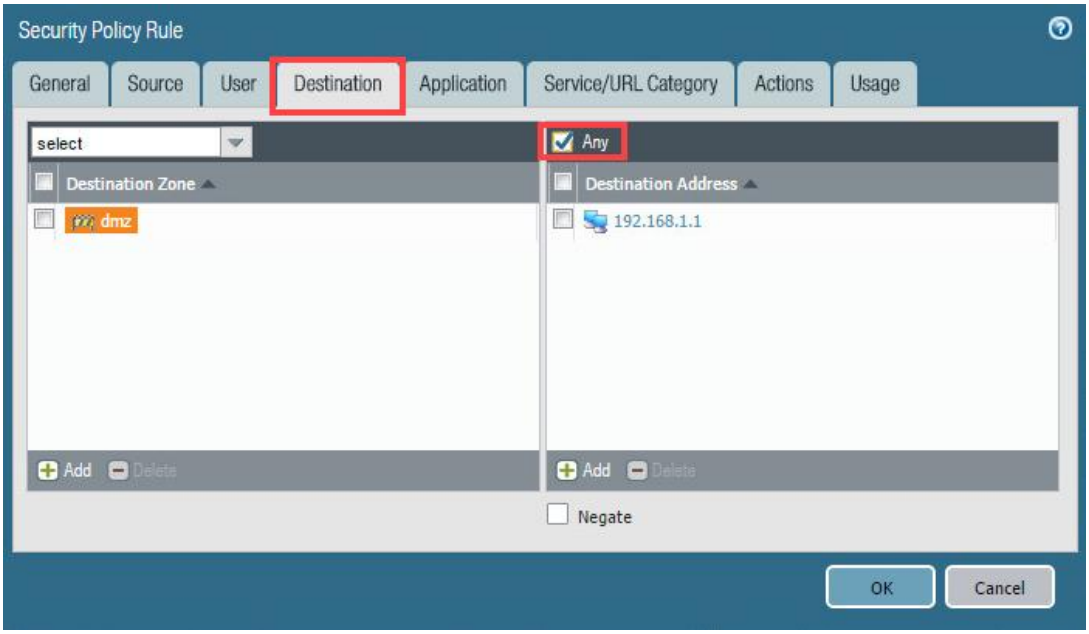
3. Select the **internal-dmz-ftp** Security Policy Rule without opening it and click **Enable**.



4. Click on **internal-dmz-ftp** to open the *Security Policy Rule* window.



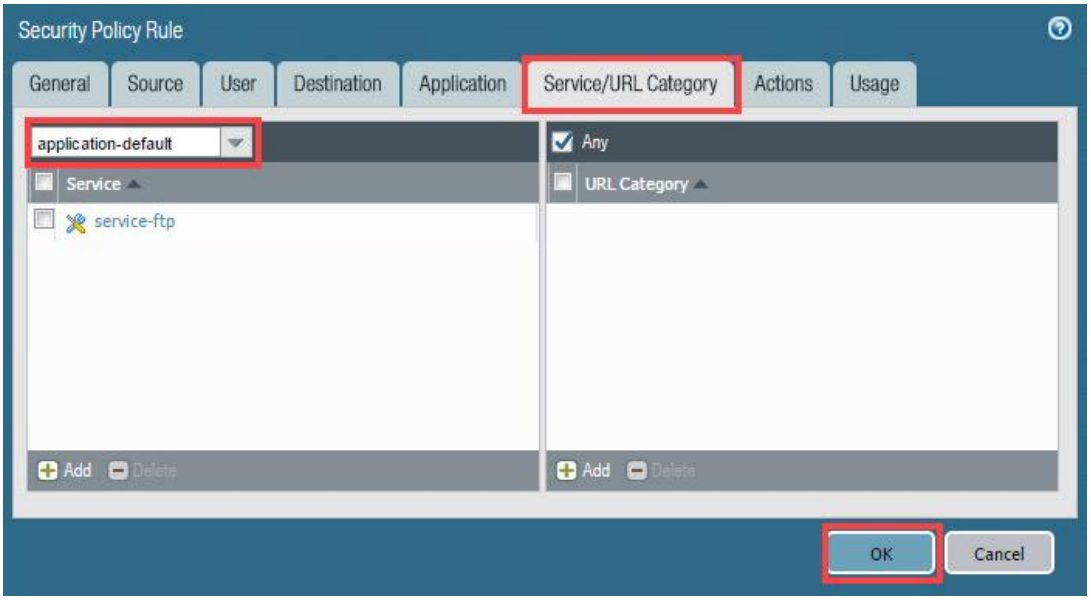
5. In the *Security Policy Rule* window, click the **Destination** tab and select the **Any** checkbox in the *Destination Address* pane.



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 **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 dropdown 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 dropdown menu automatically will remove the *service-ftp* entry when you click the *OK* button to save the configuration change.

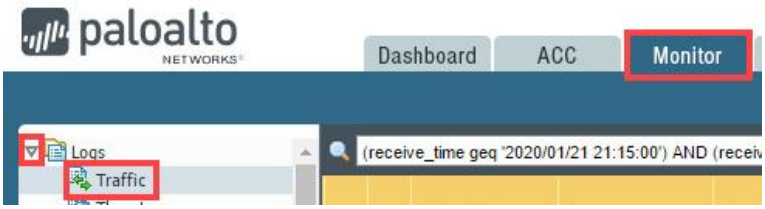
8. **Commit** all changes.
9. Open a *Terminal* window by clicking on the **Xfce Terminal** icon located in the toolbar.
10. In the *Terminal* window, enter the command below, followed by pressing the **Enter** key.

```
C:\home\lab-user> ftp 192.168.50.10
```

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

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

13. Enter **exit** to close the *Terminal* 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	Dynamic User Group	To Port	Application	Action	Rule
03/14 20:04:46	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.

