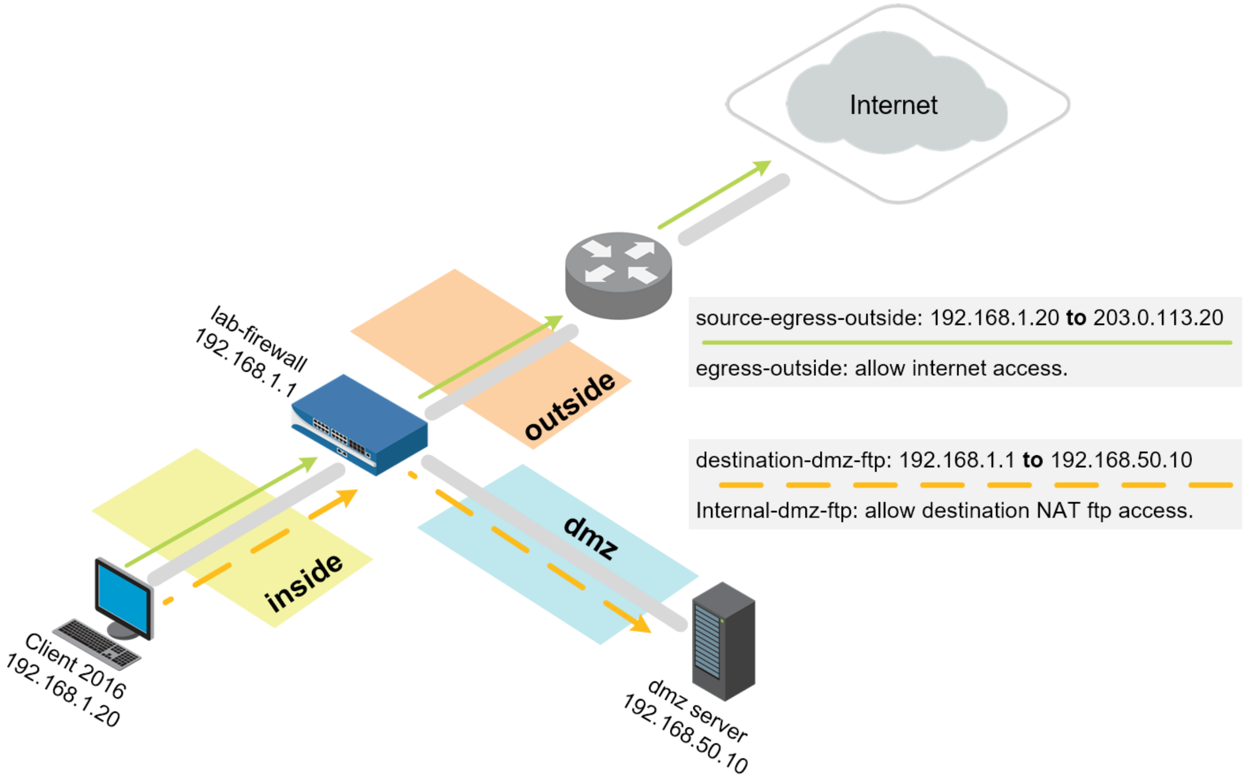
3. Lab: Security and NAT Policies



source-egress-outside: 192.168.1.20 **to** 203.0.113.20

egress-outside: allow internet access.

destination-dmz-ftp: 192.168.1.1 **to** 192.168.50.10

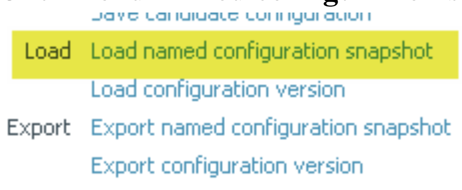
Internal-dmz-ftp: allow destination NAT ftp access.

Lab Objectives

- Create tags for later use with Security policy rules.
- Create a basic source NAT rule to allow outbound access and an associated Security policy rule to allow the traffic.
- Create a destination NAT rule for FTP server and an associated Security policy rule to allow the traffic.

3.0 Load Lab Configuration

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


Save candidate configuration
Load Load named configuration snapshot
Load configuration version
Export Export named configuration snapshot
Export configuration version

3. Select **edu-210-lab-03** and click **OK**.
4. Click **Close**.
5. all changes.

3.1 Create Tags

Tags allow you to group objects using keywords or phrases. Tags can be applied to Address objects, Address Groups (static and dynamic), zones, services, Service Groups, and policy rules. You can use a tag to sort or filter objects, and to visually distinguish objects because they can have color. When a color is applied to a tag, the Policies tab displays the object with a background color.

1. Select **Objects > Tags**.
2. Click to define a new tag.
3. Configure the following:

Parameter	Value
Name	Select **danger**
Color	**Purple**

4. Click **OK** to close the Tag configuration window.
5. Click again to define another new tag.
6. Configure the following:

Parameter	Value
Name	`egress`
Color	**Blue**

7. Click **OK** to close the Tag configuration window.
8. Click again to define another new tag.
9. Configure the following:

Parameter	Value
Name	Select **dmz**
Color	**Orange**

10. Click **OK** to close the Tag configuration window.
11. Click again to define another new tag.
12. Configure the following:

Parameter	Value
Name	internal
Color	**Yellow**

13. Click **OK** to close the Tag configuration window.

3.2 Create a Source NAT Policy

1. Select **Policies** > **NAT**. NAT
2. Click Add to define a new source NAT policy.
3. Configure the following:

Parameter	**Value**
Name	`source-egress-outside`
Tags	**egress**

4. Click the **Original Packet** tab and configure the following:

Parameter	**Value**
Source Zone	**inside**
Destination Zone	**outside**
Destination Interface	**ethernet1/1**

5. Click the **Translated Packet** tab and configure the following:

Parameter	**Value**
Translation Type	**Dynamic IP And Port**
Address Type	**Interface Address**
Interface	**ethernet1/1**
IP Address	Select **203.0.113.20/24** (Make sure to *select* the interface IP address, do not *type* it.)

6. Click **OK** to close the NAT Policy Rule configuration window.

You will not be able to access the internet yet because you still need to configure a Security policy to allow traffic to flow between zones.

3.3 Create Security Policy Rules

Security policy rules reference Security zones and enable you to allow, restrict, and track traffic on your network based on the application, user or user group, and service (port and protocol).

1. Select **Policies** > **Security**. Security

2. Click Add to define a Security policy rule.
3. Configure the following:

Parameter	Value
Name	`egress-outside`
Rule Type	**universal (default)**
Tags	**egress**

4. Click the **Source** tab and configure the following:

Parameter	Value
Source Zone	**inside**
Source Address	**Any**

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

Parameter	Value
Destination Zone	**outside**
Destination Address	**Any**

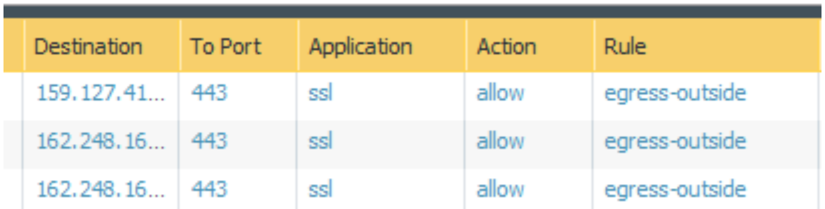
6. Click the **Application** tab and verify that ☑ Any is checked.
7. Click the **Service/URL Category** tab and verify that application-default ▾ is selected.
8. Click the **Actions** tab and verify the following:

Parameter	Value
Action Setting	**Allow**
Log Setting	**Log at Session End**

9. Click **OK** to close the Security Policy Rule configuration window.
10. Commit all changes.

3.4 Verify Internet Connectivity

1. Test internet connectivity by opening a different browser in private/incognito mode and browse to `msn.com` and `shutterfly.com`.
2. In the WebUI select **Monitor > Logs > Traffic**. Traffic
3. Traffic log entries should be present based on the internet test. Verify that there is allowed traffic that matches the Security policy rule **egress-outside**:



Destination	To Port	Application	Action	Rule
159.127.41...	443	ssl	allow	egress-outside
162.248.16...	443	ssl	allow	egress-outside
162.248.16...	443	ssl	allow	egress-outside

3.5 Create FTP Service

When you define Security policy rules for specific applications, you can select one or more services that limit the port numbers that the applications can use.

1. In the WebUI select **Objects** > **Services**. Services
2. Click Add to create a new service using the following:

Parameter	Value
Name	`service-ftp`
Destination Port	`20-21`

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

3.6 Create a Destination NAT Policy

You are configuring destination NAT in the lab to get familiar with how destination NAT works, not because it is necessary for the lab environment.

1. In the WebUI select **Policies** > **NAT**. NAT
2. Click Add to define a new destination NAT policy rule.
3. Configure the following:

Parameter	Value
Name	`destination-dmz-ftp`
Tags	**internal**

4. Click the **Original Packet** tab and configure the following:

Parameter	Value
Source Zone	**inside**
Destination Zone	**inside**
Destination Interface	**ethernet1/2**
Service	**service-ftp**

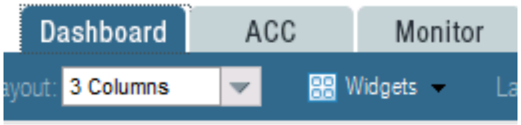
Parameter	Value
Destination Address	`192.168.1.1`

5. Click the **Translated Packet** tab and configure the following:

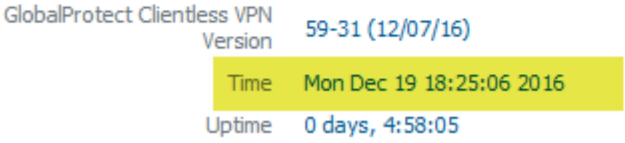
Parameter	Value
Destination Address Translation	Select the check box
Translated Address	`192.168.50.10` (address of DMZ Server)

6. Click **OK** to close the NAT Policy configuration window.

3.7 Create a Security Policy Rule

1. Click the **Dashboard** tab. 

2. Annotate the current time referenced by the firewall:



GlobalProtect Clientless VPN Version	59-31 (12/07/16)
Time	Mon Dec 19 18:25:06 2016
Uptime	0 days, 4:58:05

3. Select **Policies** > **Security**.

4. Click to define a new Security policy rule.

5. Configure the following:

Parameter	Value
Name	`internal-dmz-ftp`
Rule Type	**universal (default)**
Tags	**internal**

6. Click the **Source** tab and configure the following:

Parameter	Value
Source Zone	**inside**

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

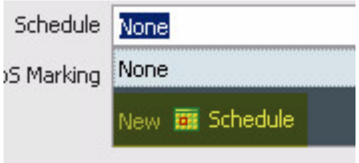
Parameter	Value
Destination Zone	**dmz**

Parameter	Value
Destination Address	`192.168.1.1`

8. Click the **Service/URL Category** tab and configure the following:

Parameter	Value
Service	**service-ftp**

9. Click the **Actions** tab and verify that **Allow** is selected.
10. Locate the **Schedule** drop-down list and select **New Schedule**:



By default, Security policy rules are always in effect (all dates and times). To limit a Security policy to specific times, you can define schedules and then apply them to the appropriate policy rules.

11. Configure the following:

Parameter	Value
Name	`internal-dmz-ftp`
Recurrence	**Daily**
Start Time	5 minutes from the time annotated in Step 2.
End time	2 hours from the current firewall time.

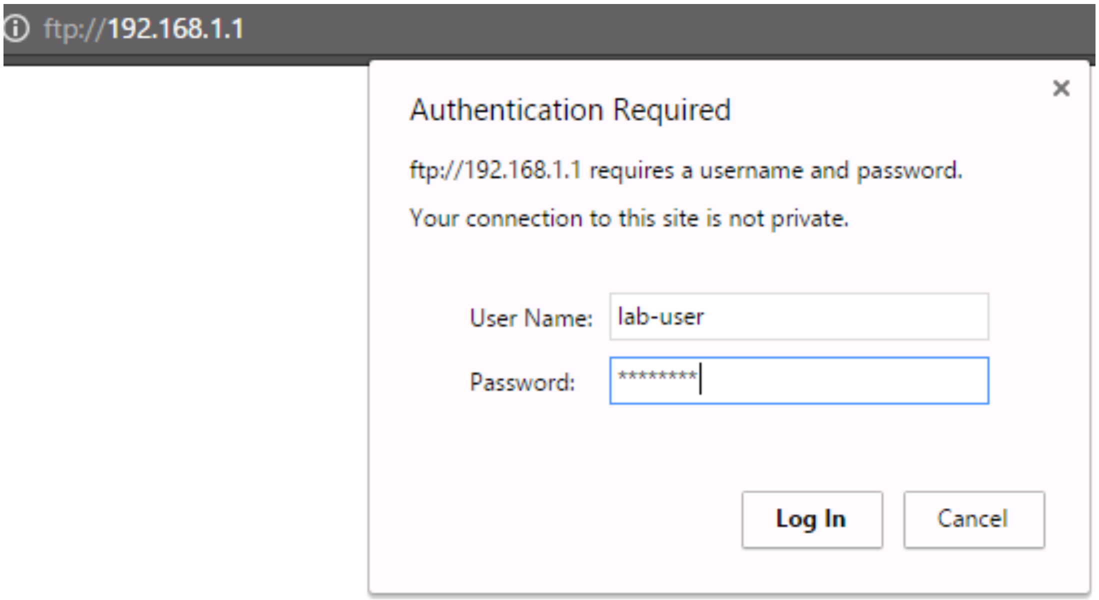
Note: Input time in a 24-hour format.

12. Click **OK** to close the Schedule configuration window.
13. Click **OK** to close the Security Policy Rule configuration window.
14. Commit all changes.

3.8 Test the Connection

1. Wait for the scheduled time to start for the internal-dmz-ftp Security policy rule.
2. Open a new Chrome browser window in private mode and browse to `ftp://192.168.1.1`.
3. At the prompt for login information, enter the following:

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



Authentication Required

ftp://192.168.1.1 requires a username and password.

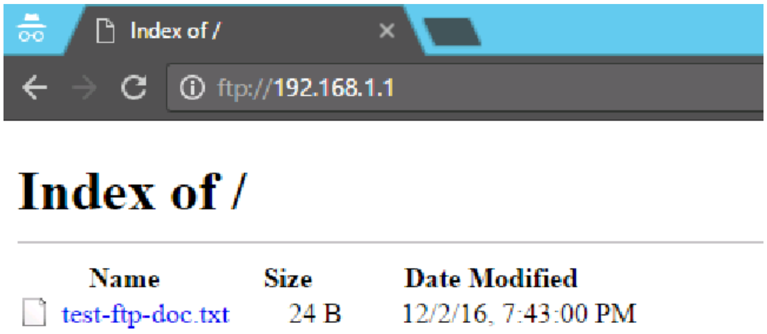
Your connection to this site is not private.

User Name: lab-user

Password: ********

192.168.1.1 is the inside interface address on the firewall. The firewall is not hosting the FTP server. The fact that you were prompted for a username indicates that FTP was successfully passed through the firewall using destination NAT.

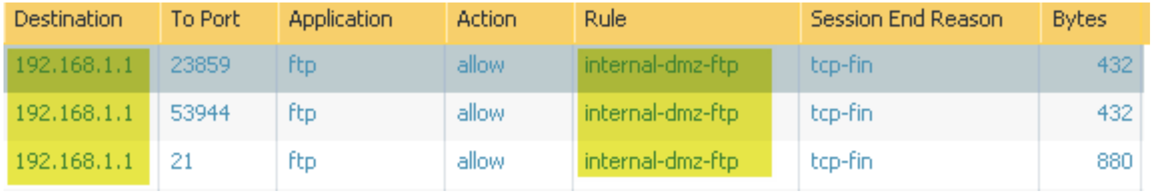
4. Verify that you can view the directory listing and then close the Chrome browser window:



Index of /

Name	Size	Date Modified
test-ftp-doc.txt	24 B	12/2/16, 7:43:00 PM

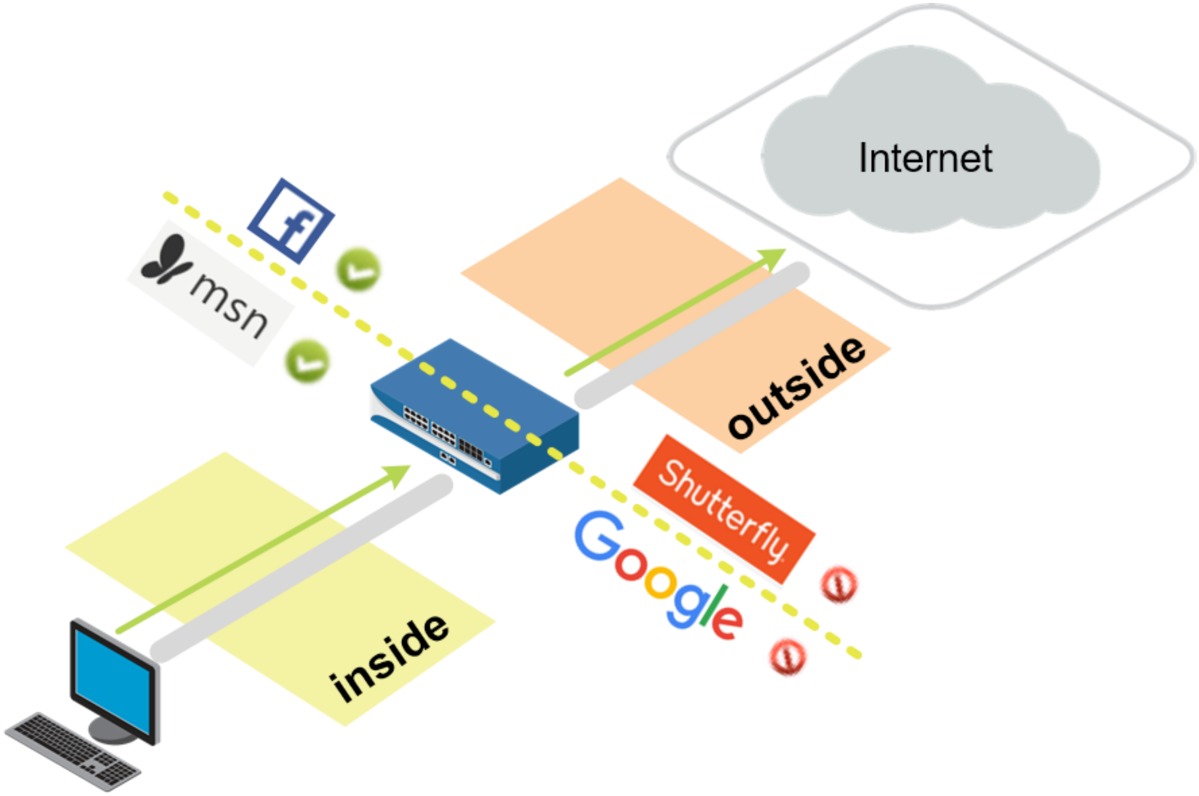
5. In the WebUI select **Monitor > Logs > Traffic**. Traffic
6. Find the entries where the application ftp has been allowed by rule internal-dmz-ftp. Notice the Destination address and rule matching:



Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
192.168.1.1	23859	ftp	allow	internal-dmz-ftp	tcp-fin	432
192.168.1.1	53944	ftp	allow	internal-dmz-ftp	tcp-fin	432
192.168.1.1	21	ftp	allow	internal-dmz-ftp	tcp-fin	880

Stop. This is the end of the Security and NAT Policies lab.

4. Lab: App-ID

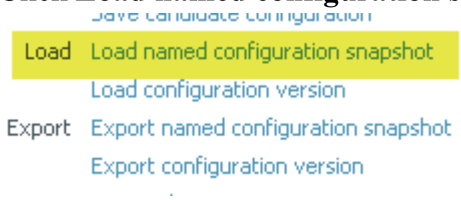


Lab Objectives

- 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).

4.0 Load Lab Configuration

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


Save candidate configuration
Load
Load named configuration snapshot
Load configuration version
Export
Export named configuration snapshot
Export configuration version

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

egress-outside *egress* *universal*

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

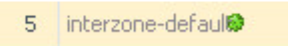
Applications	`dns`
	`facebook-base`
	`ssl`
	`web-browsing`

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

4.2 Enable Interzone Logging

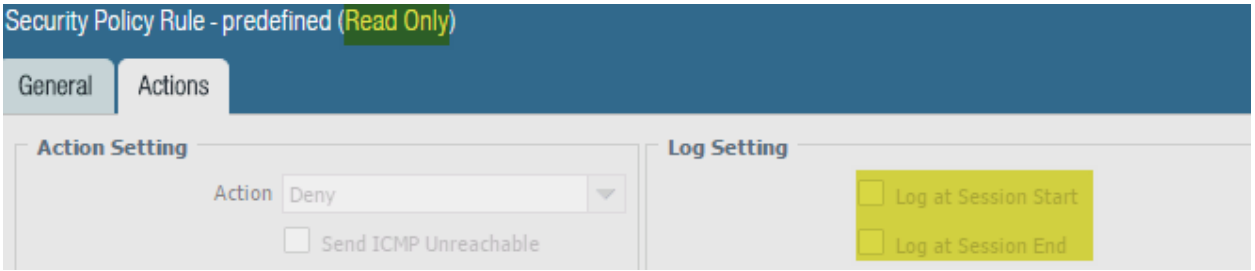
The intrazone-default and interzone-default Security policy rules are read-only by default.

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



5 interzone-default

2. 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)

Action Setting

Action: Deny

□ Send ICMP Unreachable

Log Setting

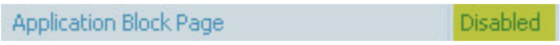
□ Log at Session Start

□ Log at Session End

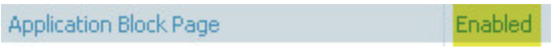
3. Click **Cancel**.
4. With the **interzone-default** policy rule selected but not opened, click Override. The Security Policy Rule – predefined window opens.
5. Click the **Actions** tab.
6. Select **Log at Session End**.
7. Click **OK**.

4.3 Enable the Application Block Page

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


Application Block Page | Disabled

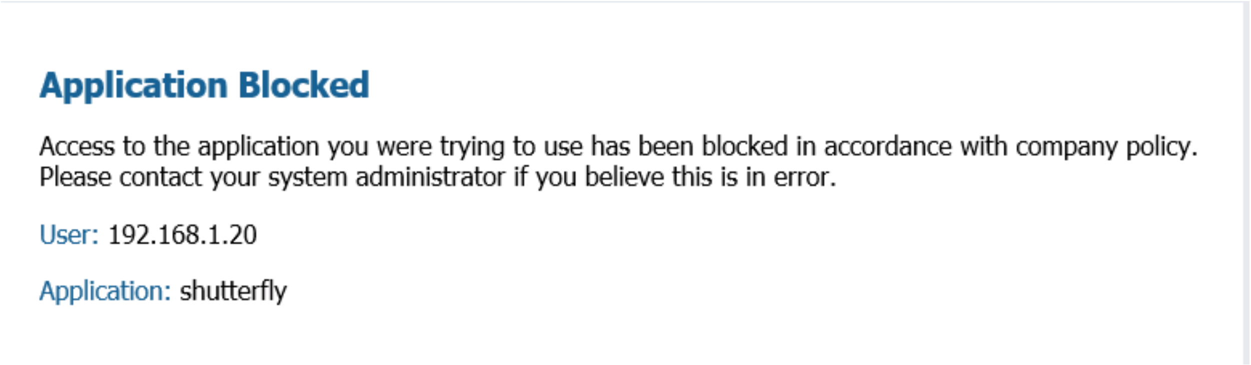
3. Select the **Enable Application Block Page** check box. ☑ Enable Application Block Page
4. Click **OK**. The Application Block Page should now be enabled:


Application Block Page | Enabled

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`.
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:


Application Blocked

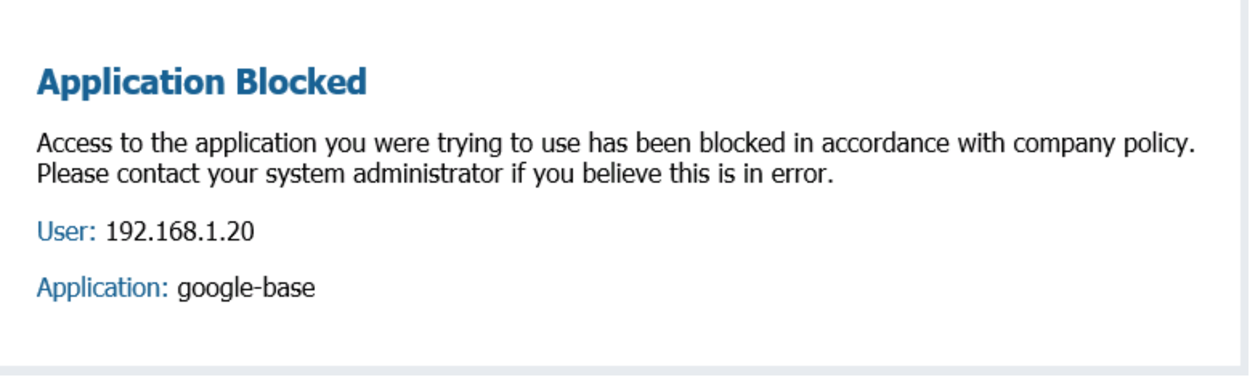
Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 192.168.1.20

Application: shutterfly

Why could you browse to Facebook and MSN but not to Shutterfly? MSN currently does not have 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:



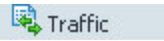
Application Blocked

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

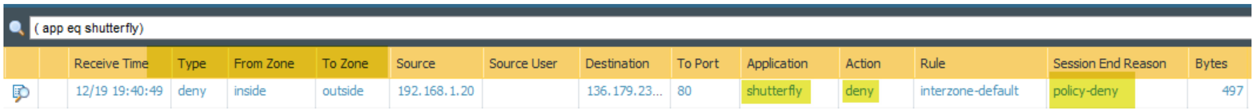
User: 192.168.1.20

Application: google-base

4.5 Review Logs

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.

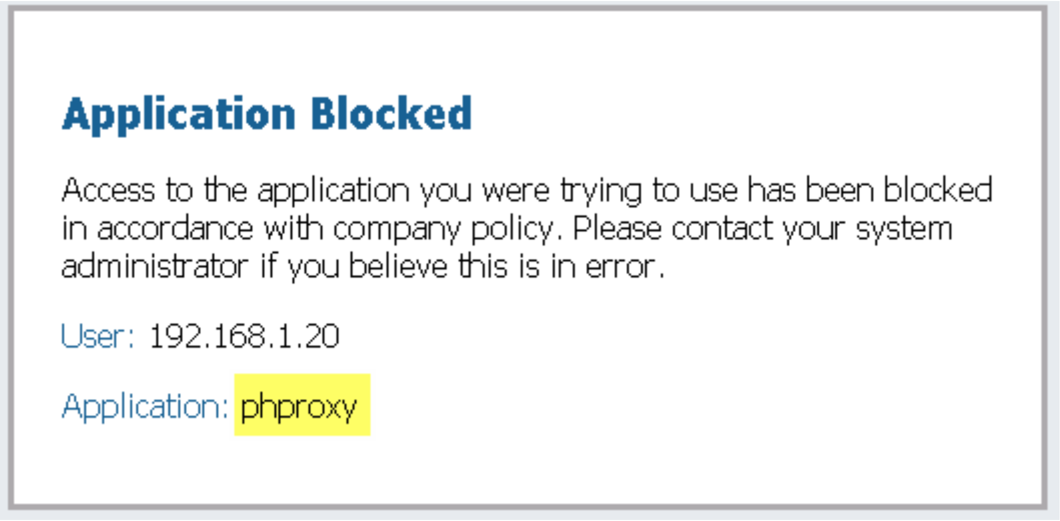


(app eq shutterfly)

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

4.6 Test Application Blocking

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:



Application Blocked

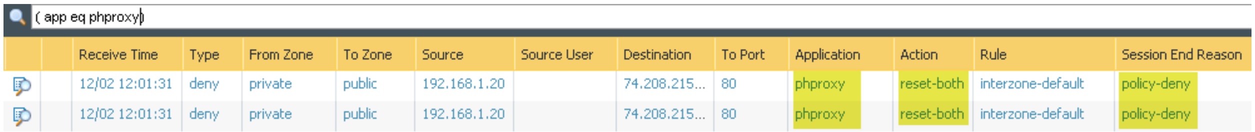
Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 192.168.1.20

Application: phproxy

4.7 Review Logs

1. Select **Monitor** > **Logs** > **Traffic**. Traffic
2. Type `( app eq phproxy )` in the filter text box. The Traffic log entries indicates that the phproxy application has been blocked:



(app eq phproxy)

		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	phproxy	reset-both	interzone-default	policy-deny
		12/02 12:01:31	deny	private	public	192.168.1.20		74.208.215...	80	phproxy	reset-both	interzone-default	policy-deny

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

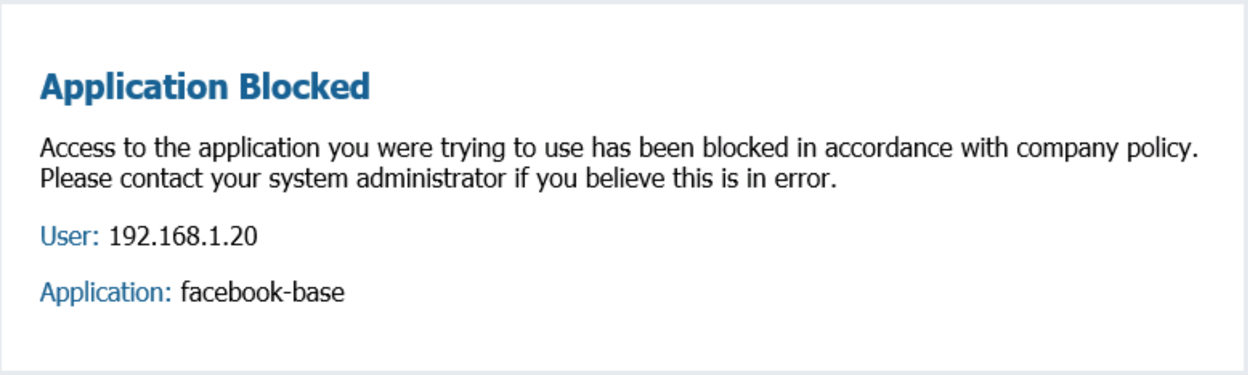
4.8 Modify the App-ID Security Policy Rule

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

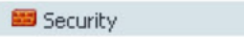
User: 192.168.1.20

Application: facebook-base

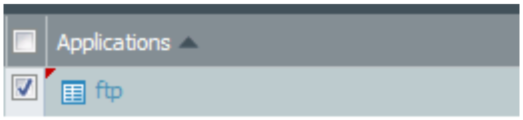
3. Close all browser windows except for the firewall WebUI.
   Note: The web-browsing Application signature only covers browsing that does not match any other Application signature.

4.10 Migrate Port-Based Rule to Application-Aware Rule

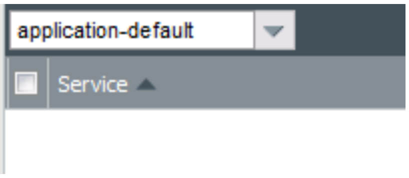
1. In the WebUI select **Policies** > **Security**.



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

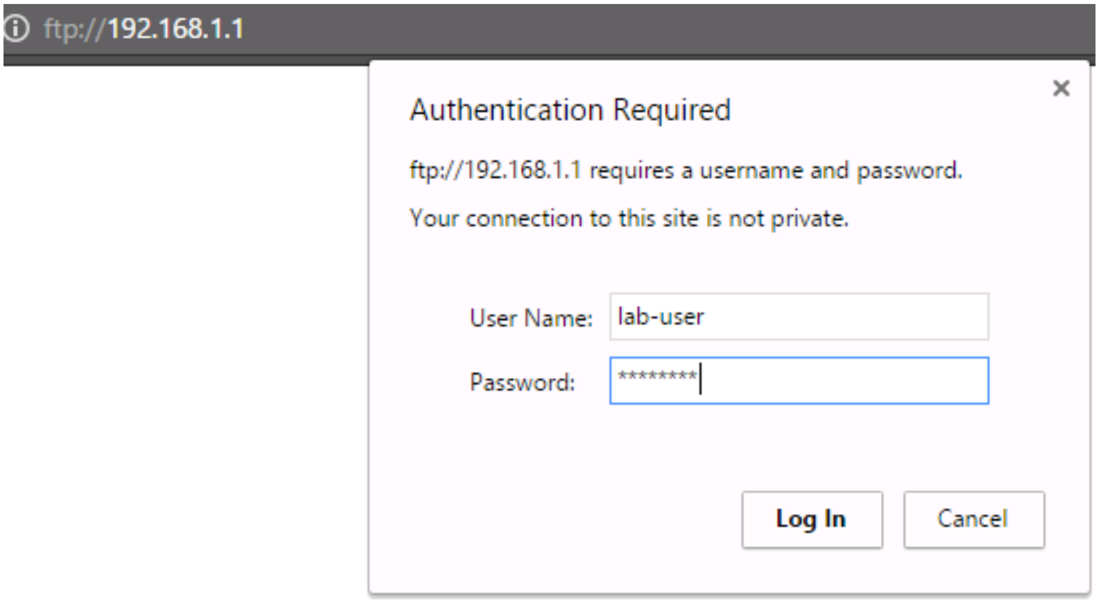


3. Click the **Application** tab and add `ftp`.
4. Click the **Service/URL Category** tab.
5. Delete **service-ftp** and select **application-default**.



   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):

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



ftp://192.168.1.1

Authentication Required

ftp://192.168.1.1 requires a username and password.

Your connection to this site is not private.

User Name: lab-user

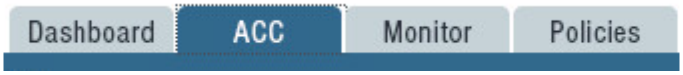
Password: ********

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

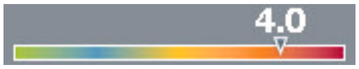
4.11 Observe the Application Command Center

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.

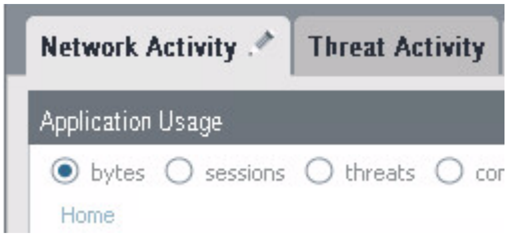
1. Click the **ACC** tab to access the Application Command Center:



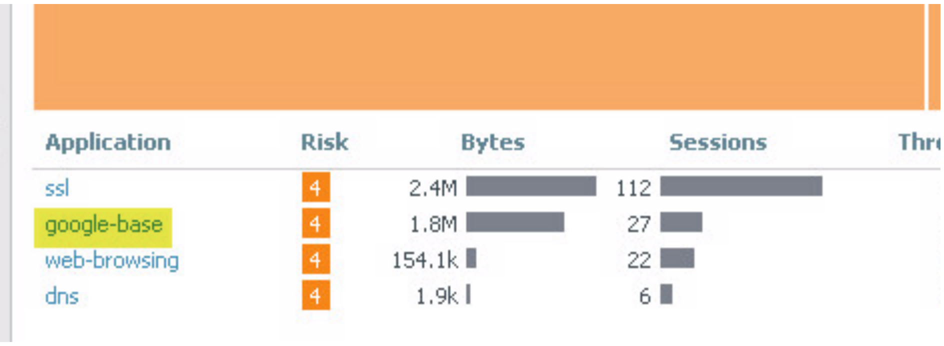
2. Note that the upper-right corner of the ACC displays the total risk level for all traffic that has passed through the firewall thus far:



3. 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).



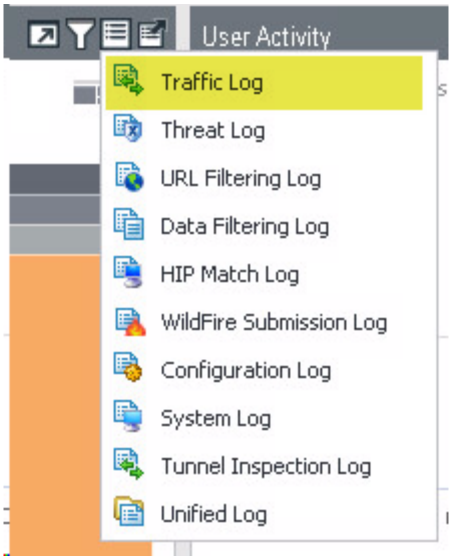
4. You can click any application listed in the Application Usage pane; *google-base* is used in this example:



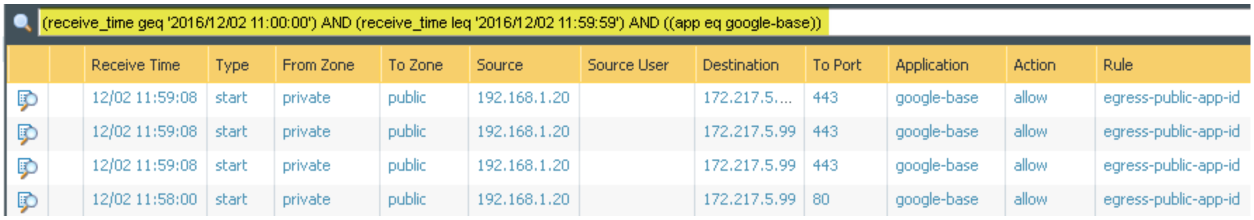
Application	Risk	Bytes	Sessions	Thr
ssl	4	2.4M	112	
google-base	4	1.8M	27	
web-browsing	4	154.1k	22	
dns	4	1.9k	6	

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

5. Click the ☰ 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:



```
(receive_time geq '2016/12/02 11:00:00') AND (receive_time leq '2016/12/02 11:59:59') AND ((app eq google-base))
```

		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
		12/02 11:59:08	start	private	public	192.168.1.20		172.217.5....	443	google-base	allow	egress-public-app-id
		12/02 11:59:08	start	private	public	192.168.1.20		172.217.5.99	443	google-base	allow	egress-public-app-id
		12/02 11:59:08	start	private	public	192.168.1.20		172.217.5.99	443	google-base	allow	egress-public-app-id
		12/02 11:58:00	start	private	public	192.168.1.20		172.217.5.99	80	google-base	allow	egress-public-app-id

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