PALO ALTO NETWORKS - EDU-210

Lab 3: Security and NAT Policies

Document Version: 2020-06-26

Contents

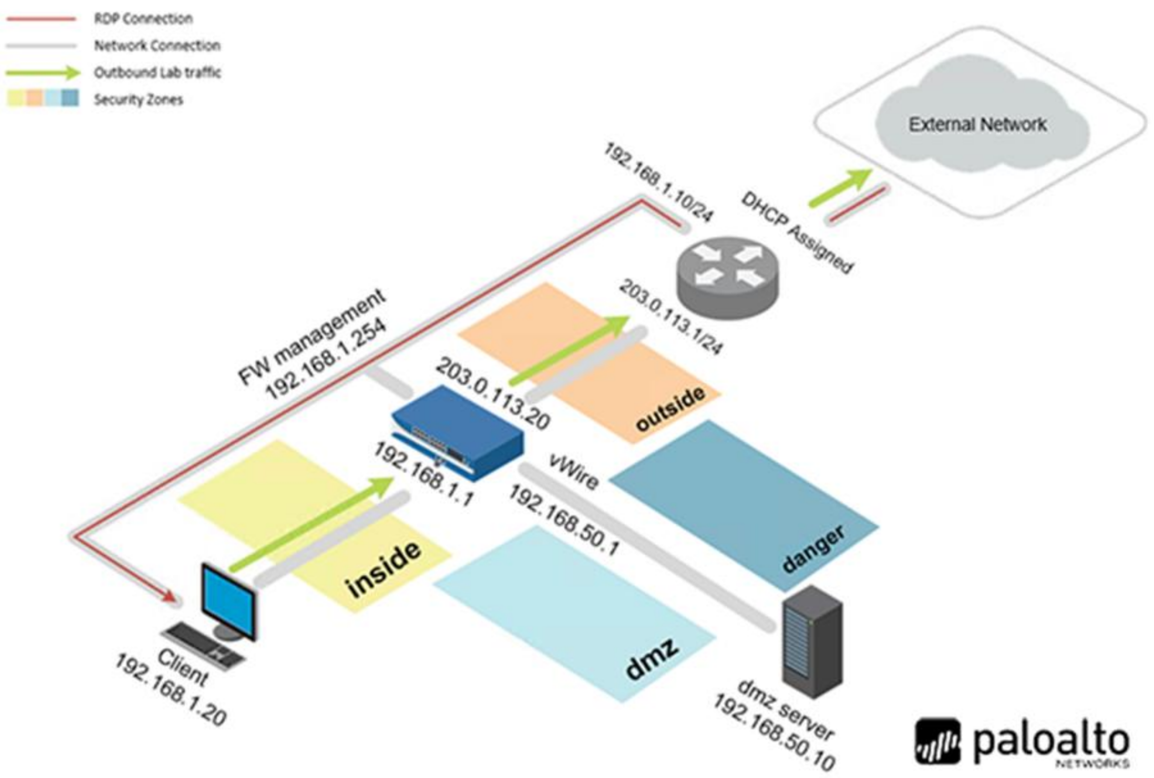
Introduction

The interfaces are configured and working, but we can't pass traffic through the appliance yet. That is because we need to set up our NAT and Security policies to allow our systems to communicate with the outside world. Now, we are going to configure those policies. We will have to revise them later as we grow, but this should get us to the internet.

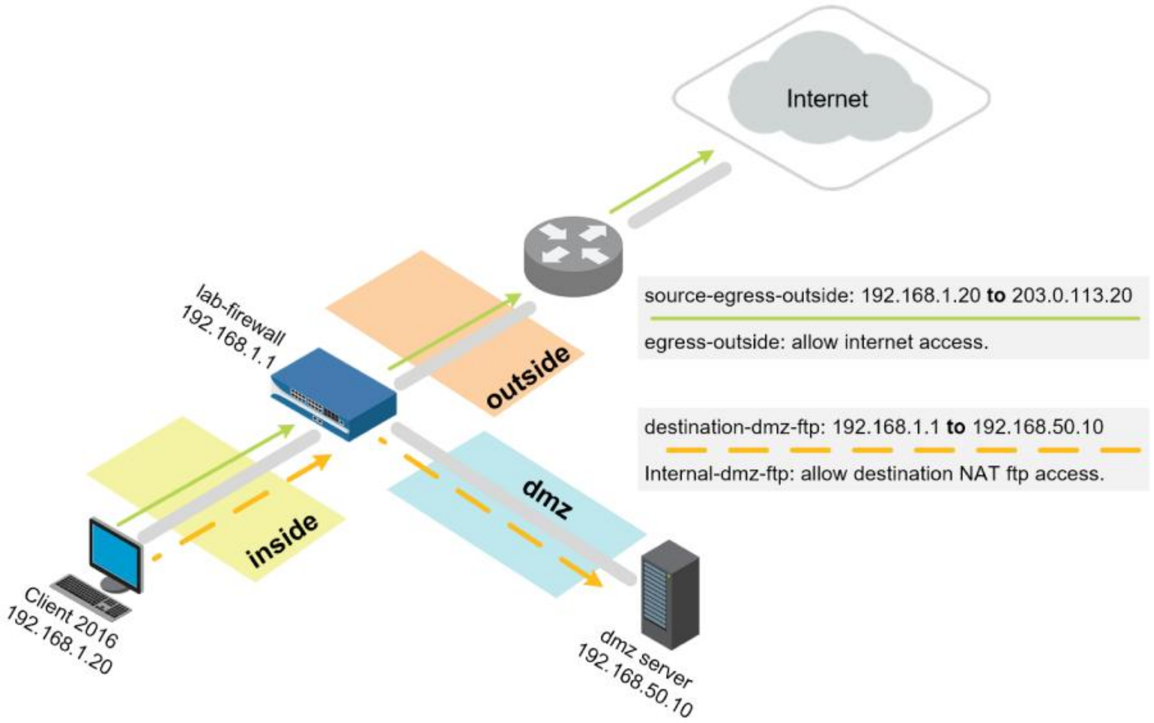
Objectives

- 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

Lab Topology



Theoretical Lab Topology



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 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$`
Firewall	192.168.1.254	`admin`	`Train1ng$`

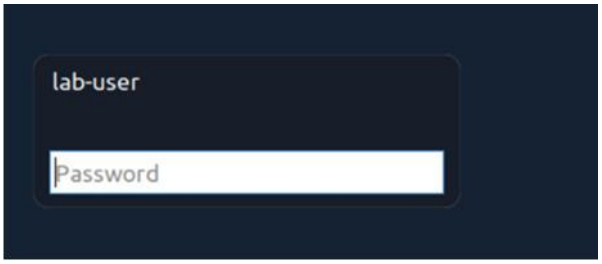
3 Security and NAT Policies

3.0 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.

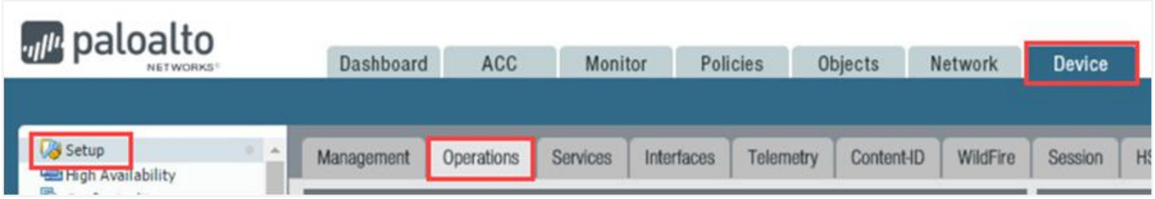
2. Log in as `lab-user` using the password `Train1ng$`.



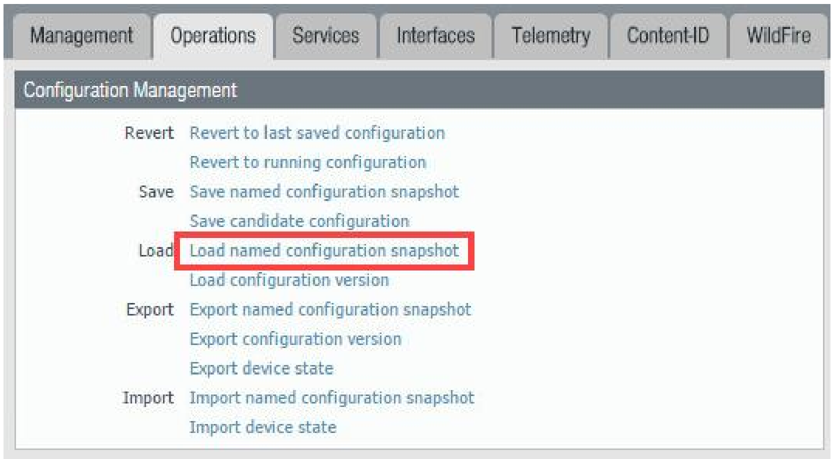
3. Launch the **Chromium Web Browser** and connect to `https://192.168.1.254.`
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	`admin`
Password	`Train1ng$`

6. In the firewall web interface, navigate to **Device > Setup > Operations**.



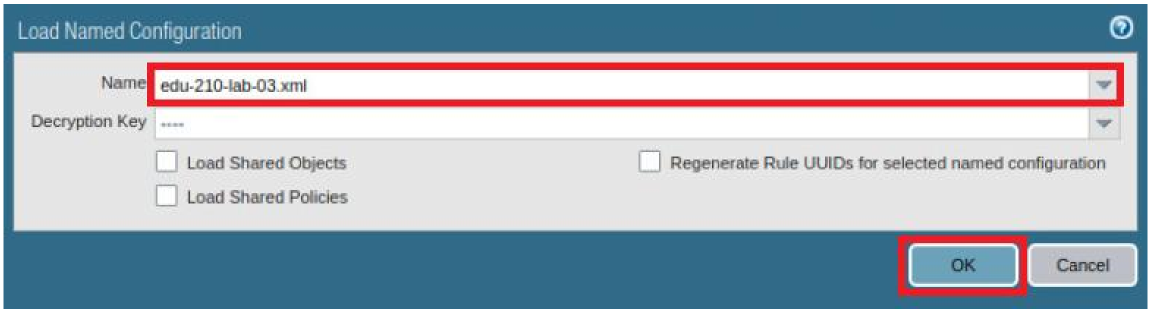
7. Click **Load named configuration snapshot**:



Configuration Management

Revert Revert to last saved configuration
Revert to running configuration
Save Save named configuration snapshot
Save candidate configuration
Load Load named configuration snapshot
Load configuration version
Export Export named configuration snapshot
Export configuration version
Export device state
Import Import named configuration snapshot
Import device state

8. Select **edu-210-lab-03.xml** and click **OK**.

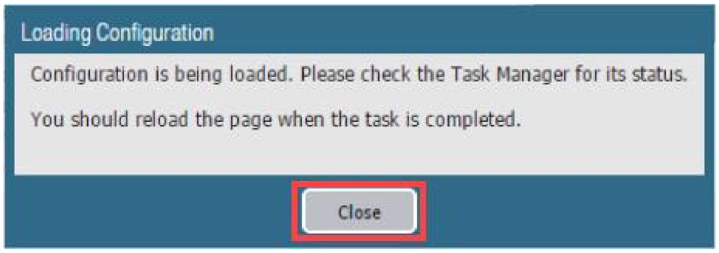

Load Named Configuration

Name edu-210-lab-03.xml

Decryption Key ••••

□ Load Shared Objects
□ Load Shared Policies
□ Regenerate Rule UUIDs for selected named configuration

9. Click **Close**.

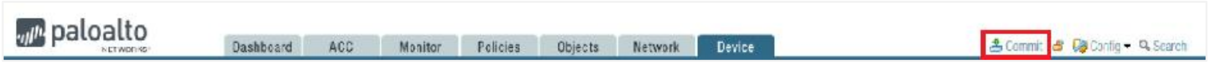

Loading Configuration

Configuration is being loaded. Please check the Task Manager for its status.

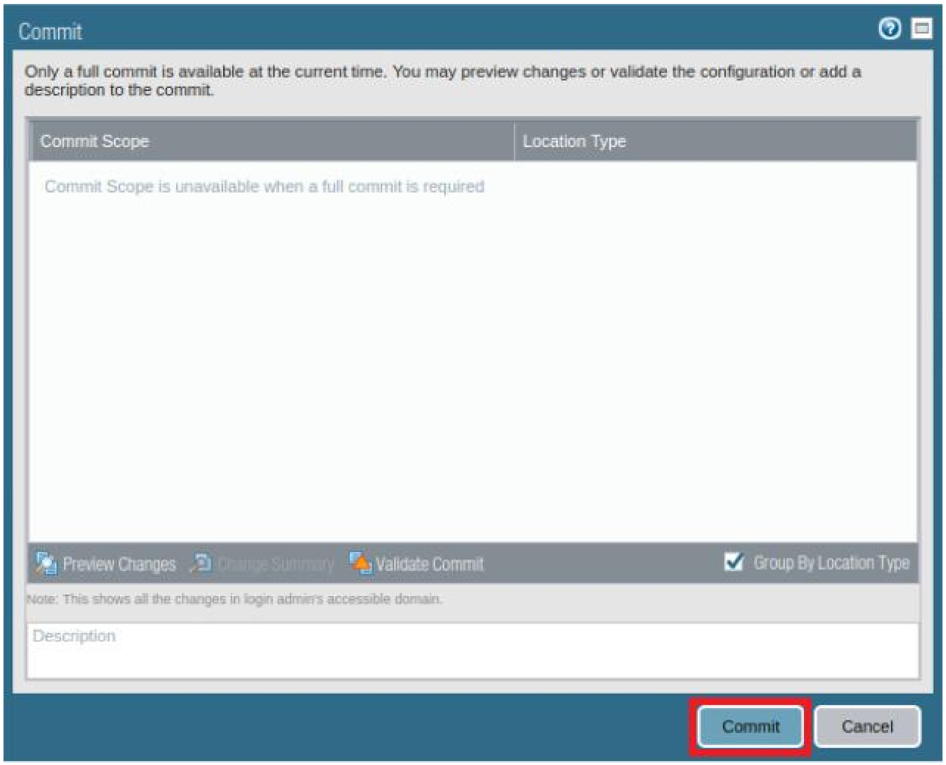
You should reload the page when the task is completed.

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.

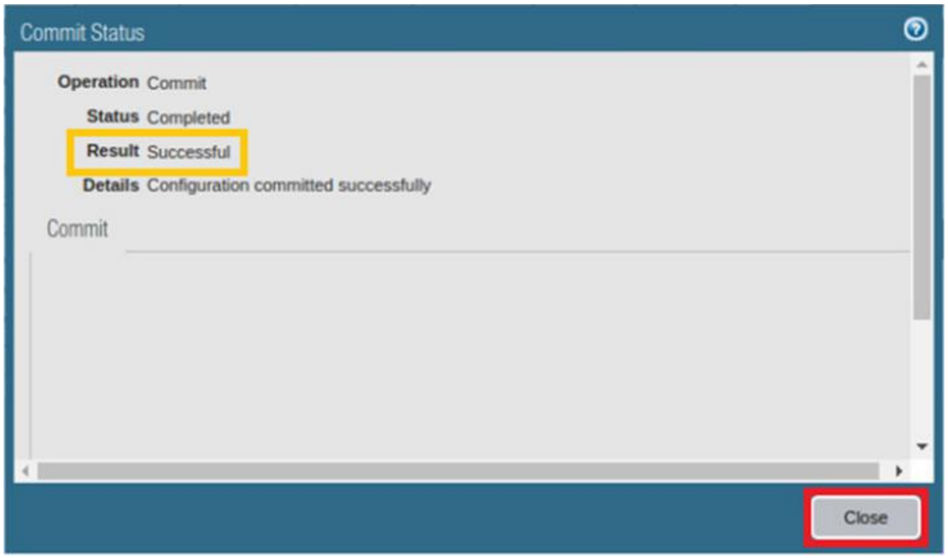


Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

Commit Scope is unavailable when a full commit is required

Note: This shows all the changes in login admin's accessible domain.

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



Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

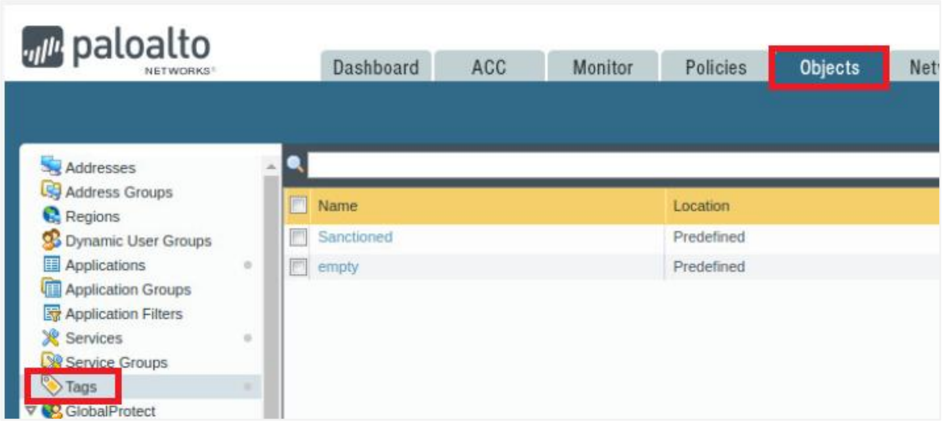
13. Leave the firewall web interface open to continue with the next task.

3.1 Create Tags

Tags are color-coded labels that enable you to group, sort, and filter objects using keywords or phrases. Tags can be applied to Address objects, Address Groups (static and dynamic), services, Service Groups, and policy rules. Tags can be assigned a color that makes the results of a search easier to find in the web interface.

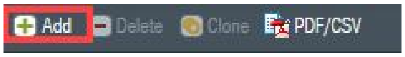
When used with Comments or Descriptions, Tags can help administrators to determine more easily how a firewall has been configured and the purpose of its various rules, objects, and entries. In the following steps, you will assign a description to a tag, assign a color to the tag, and apply the tag to different policies.

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



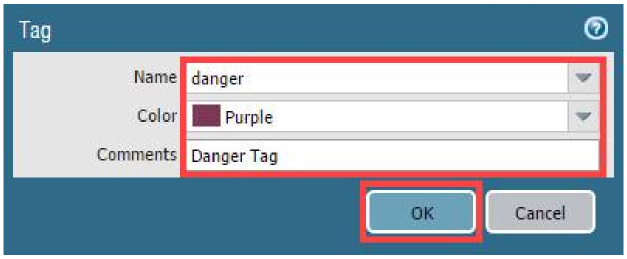
Name	Location
Sanctioned	Predefined
empty	Predefined

2. Click on **Add** located near the bottom to define a new tag**.**



3. In the *Tag* window, configure the following and then click **OK**.

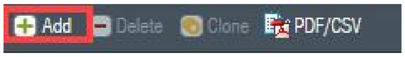
Parameter	Value
Name	Select **danger**
Color	**Purple**
Comments	`Danger Tag`



Name: danger
Color: Purple
Comments: Danger Tag

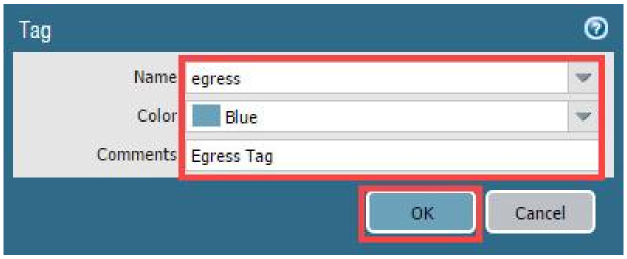
The firewall allows you to create tags based on existing Security zones, which is why *danger*, *dmz*, *outside*, and *inside* already appear in the dropdown list.

4. Click **Add** again to define another new tag.



5. In the *Tag* window, configure the following and then click **OK**.

Parameter	Value
Name	Type `egress`
Color	**Blue**
Comments	Type `Egress Tag`

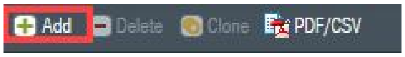


Name egress

Color Blue

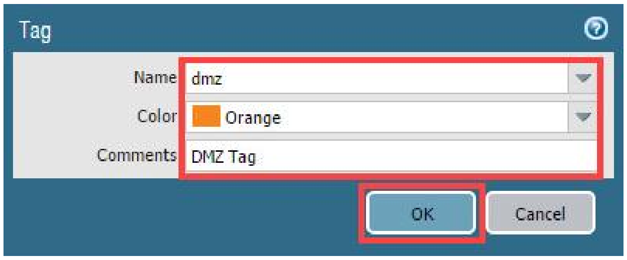
Comments Egress Tag

6. Click **Add** again to define another new tag.



7. In the *Tag* window, configure the following and then click **OK**.

Parameter	Value
Name	Select **dmz**
Color	**Orange**
Comments	`DMZ Tag`

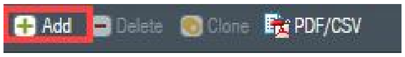


Name dmz

Color Orange

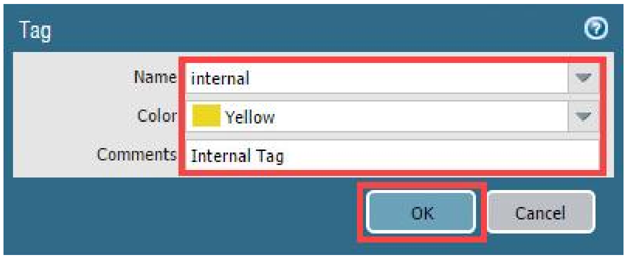
Comments DMZ Tag

8. Click **Add** again to define another.



9. In the *Tag* window, configure the following and then click **OK**.

Parameter	Value
Name	Type `internal`
Color	**Yellow**
Comments	`Internal Tag`

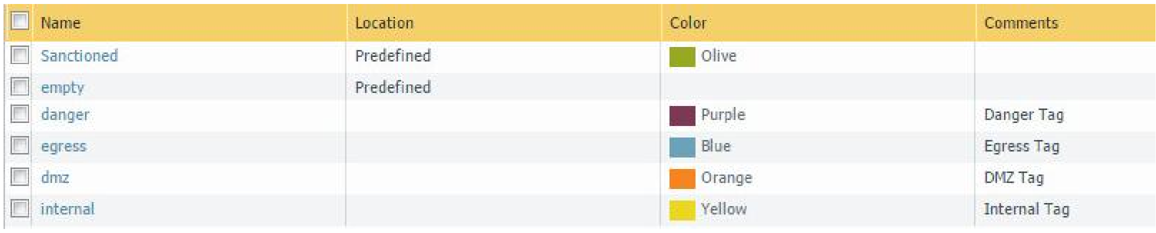

Tag

Name: internal

Color: 🟨 Yellow

Comments: Internal Tag

10. Verify that your configuration is like the following:



□	Name	Location	Color	Comments
□	Sanctioned	Predefined	🟩 Olive	
□	empty	Predefined		
□	danger		🟪 Purple	Danger Tag
□	egress		🟦 Blue	Egress Tag
□	dmz		🟧 Orange	DMZ Tag
□	internal		🟨 Yellow	Internal Tag

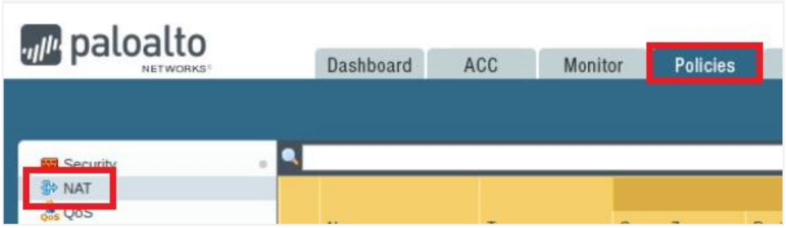
> If you create a Tag and use the same name you used for a Security zone, the firewall will apply that tag to the appropriate Security zone in any tables where zones are displayed. Note that the label you create for a zone must match exactly, including lowercase and uppercase.

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

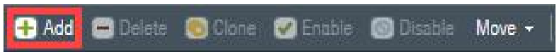
3.2 Create a Source NAT Policy

The firewall typically uses Source NAT to translate traffic from internal hosts (often on private networks) to a public, routable address (often an interface on the firewall itself). NAT rules provide address translation and are different from Security Policy Rules, which allow and deny packets. You can configure a NAT policy rule to match a packet's source and destination zone, destination interface, source and destination address, and service.

1. In the web interface, navigate to **Policies > NAT**.

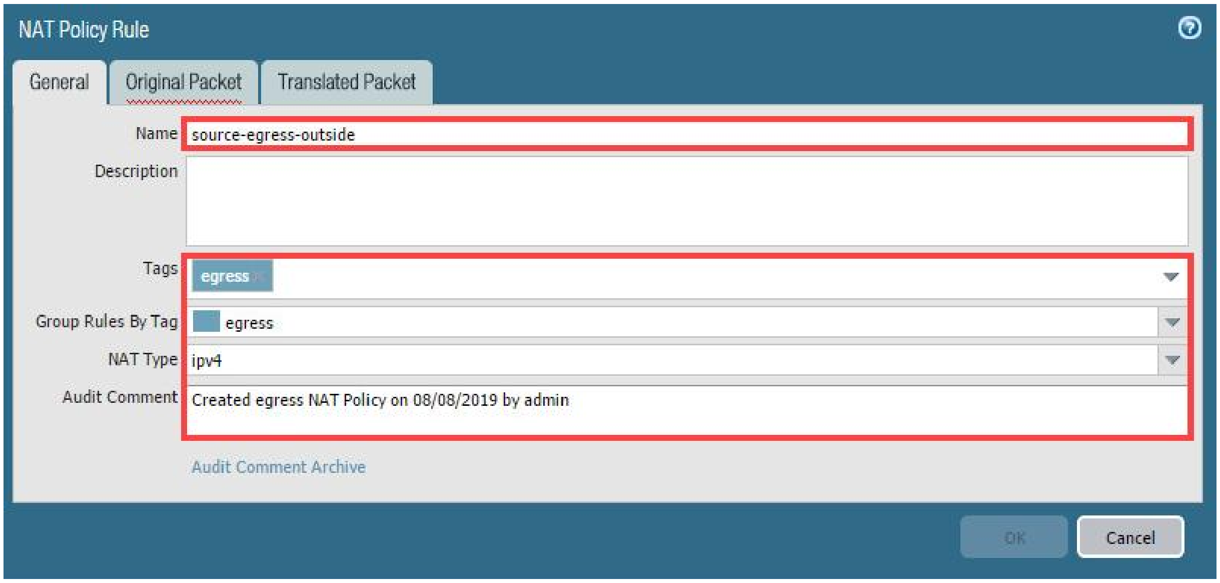


2. Located near the bottom, click **Add** to define a new source NAT policy.



3. In the *NAT Policy Rule* window, configure the following:

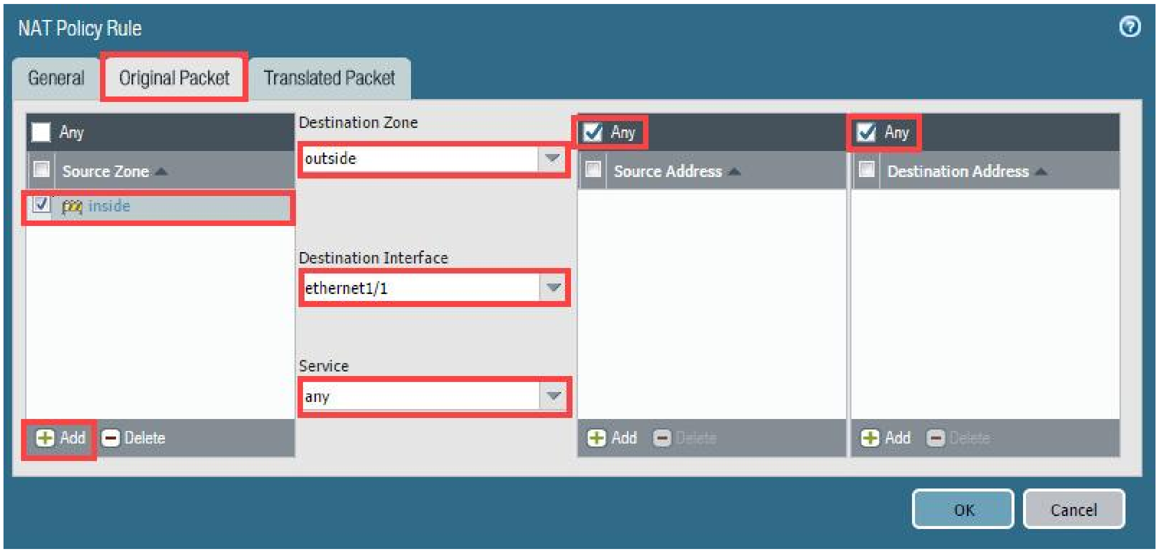
Parameter	Value
Name	`source-egress-outside`
Tags	Select **egress** from the dropdown list
Group Rules By Tag	Select **egress** from the dropdown list
NAT Type	Verify that **ipv4** is selected
Audit Comment	Type `Created egress NAT Policy on <date> by admin`



Name: source-egress-outside
Description:
Tags: egress
Group Rules By Tag: egress
NAT Type: ipv4
Audit Comment: Created egress NAT Policy on 08/08/2019 by admin

4. In the *NAT Policy Rule* window, click the **Original Packet** tab and configure the following:

Parameter	Value
Source Zone	Click **Add** and select the **inside** zone
Destination Zone	Select **outside** from the dropdown list
Destination Interface	Select **ethernet1/1** from the dropdown list
Service	Verify that **any** is selected
Source Address	Verify that the **Any** checkbox is selected
Destination Address	Verify that the **Any** checkbox is selected


NAT Policy Rule

General | Original Packet | Translated Packet

☐ Any

Source Zone

☑ inside

Destination Zone: outside

Destination Interface: ethernet1/1

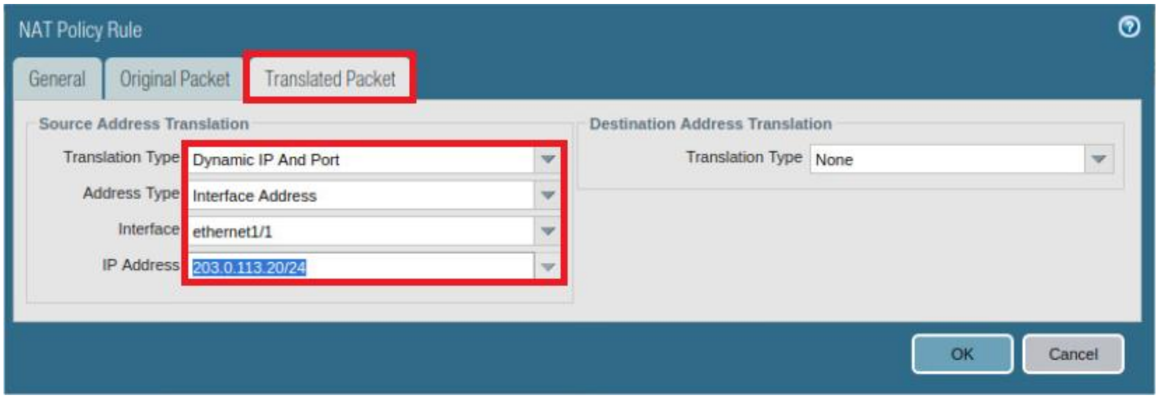
Service: any

☑ Any — Source Address

☑ Any — Destination Address

5. In the *NAT Policy Rule* window. Click the **Translated Packet** tab and configure the following. Click **OK** when finished.

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.)


NAT Policy Rule

General | Original Packet | Translated Packet

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

Interface: ethernet1/1

IP Address: 203.0.113.20/24

Destination Address Translation

Translation Type: None

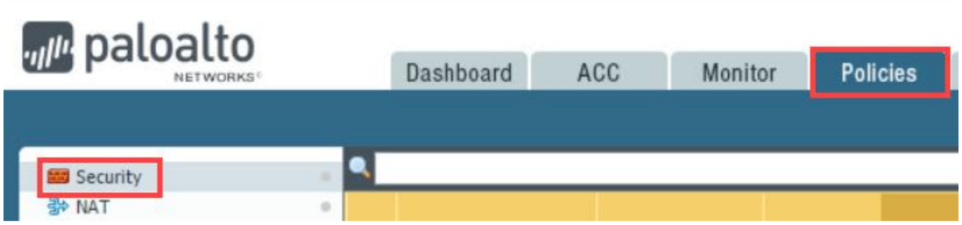
You will not be able to access the internet yet because you still need to configure a Security policy to allow traffic to flow between zones.

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

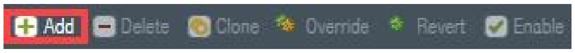
3.3 Create Security Policy Rules

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. In the web interface, navigate to **Policies > Security**.

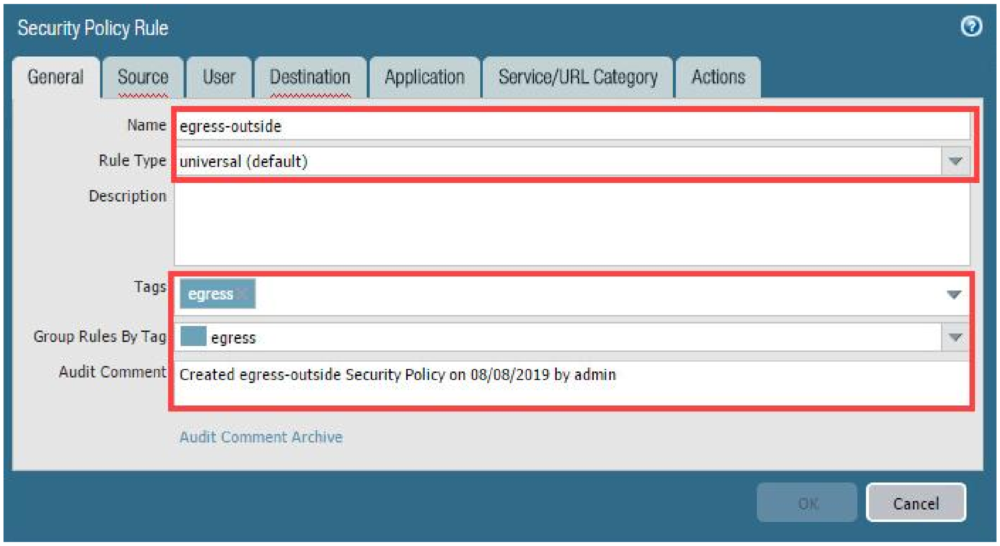


2. Click **Add** to define a Security Policy Rule (located near the bottom).



3. In the *Security Policy Rule* window, configure the following:

Parameter	Value
Name	`egress-outside`
Rule Type	**universal (default)**
Tags	**egress**
Group Rules By Tag	**egress**
Audit Comment	Type `Created egress-outside Security Policy on <date> by admin`



Name: egress-outside

Rule Type: universal (default)

Description:

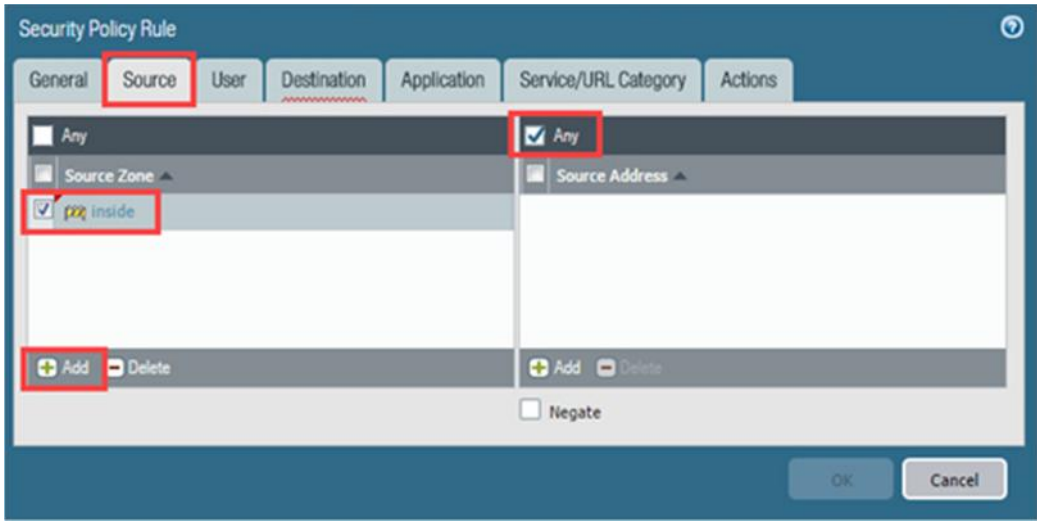
Tags: egress

Group Rules By Tag: egress

Audit Comment: Created egress-outside Security Policy on 08/08/2019 by admin

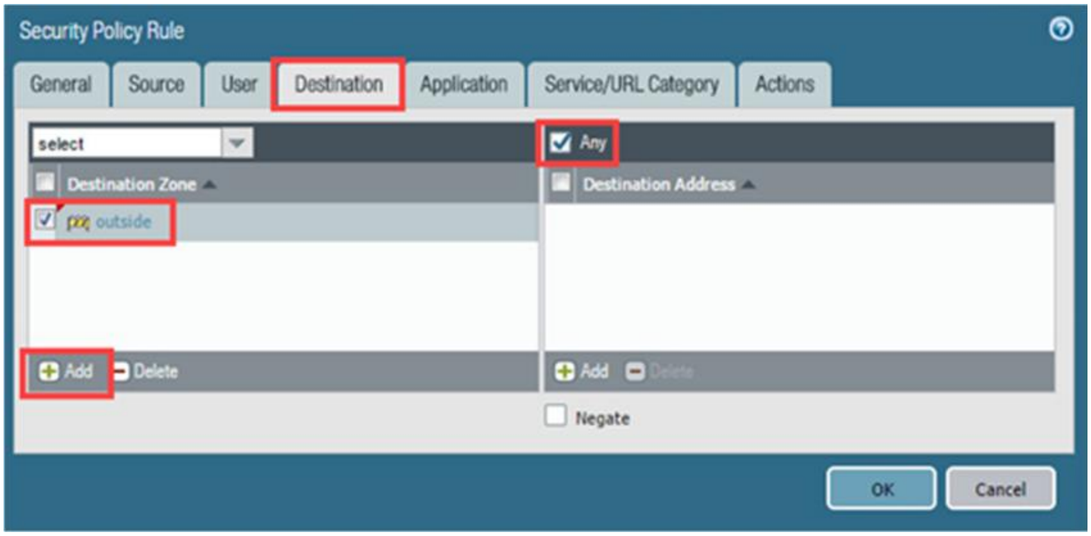
4. In the *Security Policy Rule* window, click the **Source** tab and configure the following:

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

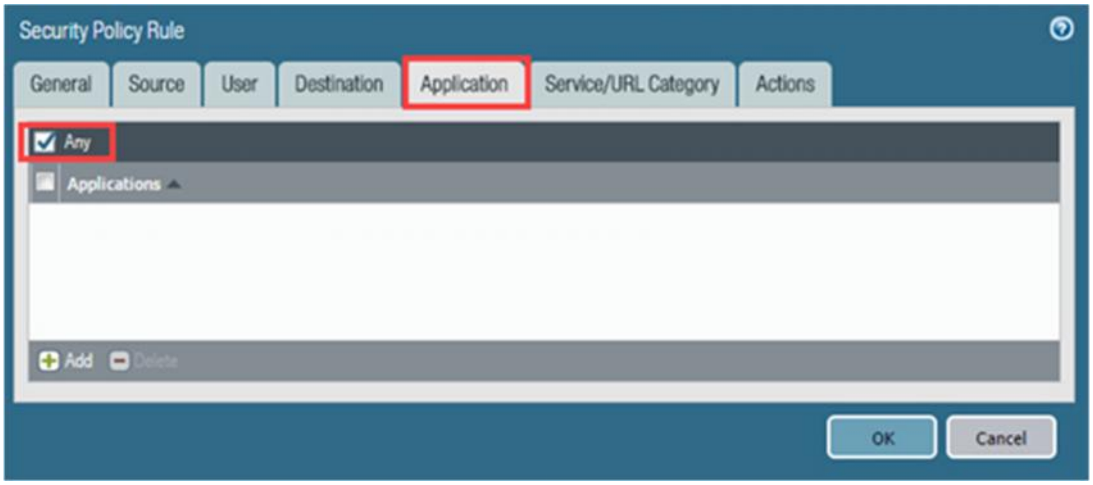


5. In the *Security Policy Rule* window, click the **Destination** tab and configure the following:

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

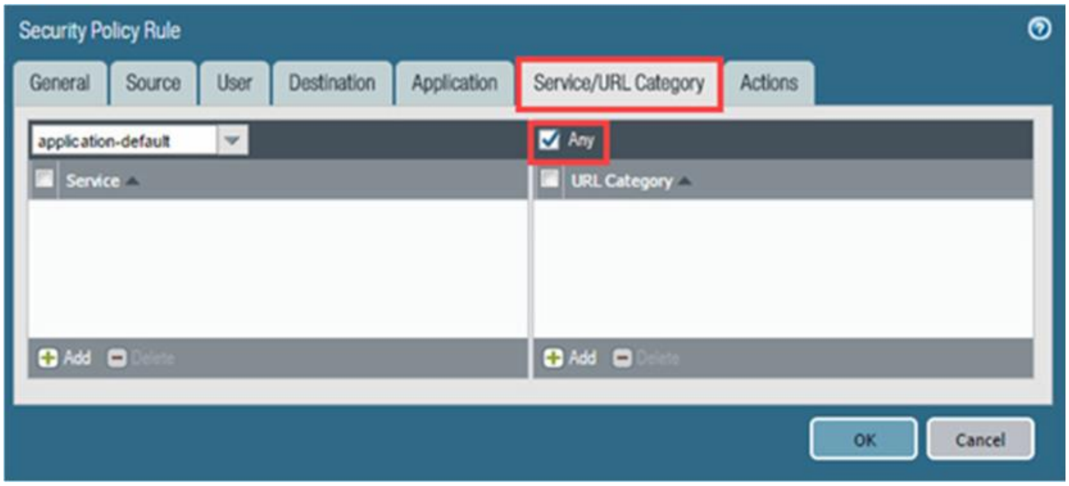


6. In the *Security Policy Rule* window, click the **Application** tab and verify that **Any** is checked.



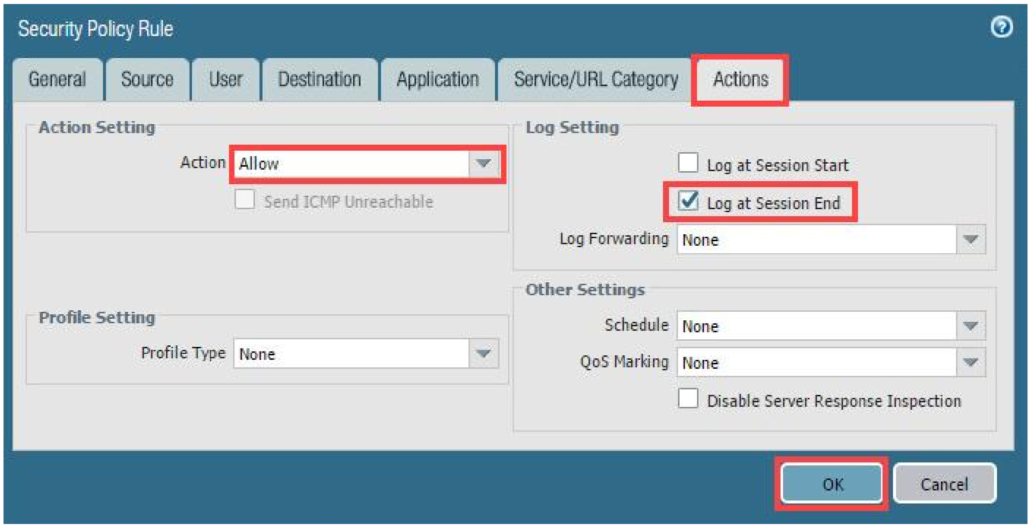
We will use the *Any* setting for this rule now because we have not discussed applications yet. Typically, your security rules will allow only those applications that you sanction for use in your network.

7. In the *Security Policy Rule* window, click the **Service/URL Category** tab and verify that **Any** is selected.



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

Parameter	Value
Action Setting	Verify that *Action* is set to **Allow**
Log Setting	Verify that the **Log at Session End** checkbox is selected


Action Setting

Action: Allow

□ Send ICMP Unreachable

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: None

Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

The setting for *Log at Session End* instructs the firewall to write an entry in the Traffic log after a session has dropped from the Session table. If you enable *Log at Session Start*, the firewall will create an entry when a session is established in the session table. *Log at Session End* is the recommended setting, though you can enable both simultaneously to help troubleshoot a specific rule.

9. **Commit** all changes.

3.4 Verify Internet Connectivity

In this section, you will test the configuration of your NAT and Security policies by accessing different websites on the internet.

1. Test internet connectivity by opening two new tabs in the **Chromium Web Browser** and browsing to **msn.com** and **shutterfly.com**.

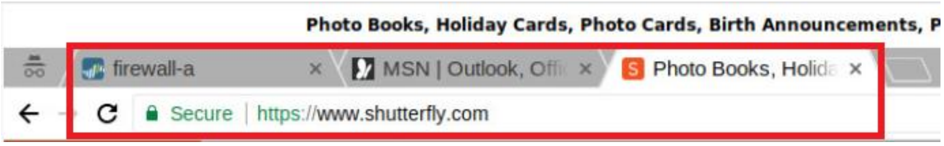
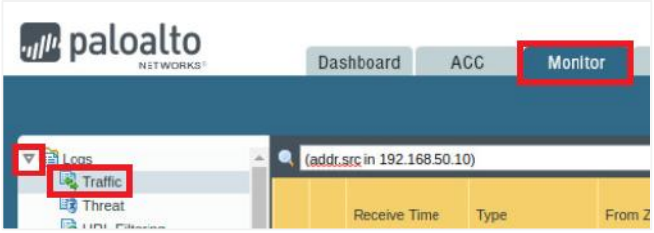


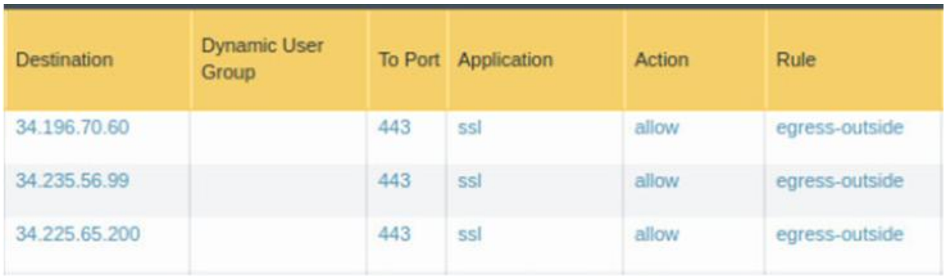
Photo Books, Holiday Cards, Photo Cards, Birth Announcements, P
firewall-a
MSN | Outlook, Offi
Photo Books, Holida
Secure
https://www.shutterfly.com

2. Change focus to the firewall web interface and navigate to **Monitor**, expand **Logs**, and click on **Traffic**.



(addr.src in 192.168.50.10)

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	Dynamic User Group	To Port	Application	Action	Rule
34.196.70.60		443	ssl	allow	egress-outside
34.235.56.99		443	ssl	allow	egress-outside
34.225.65.200		443	ssl	allow	egress-outside

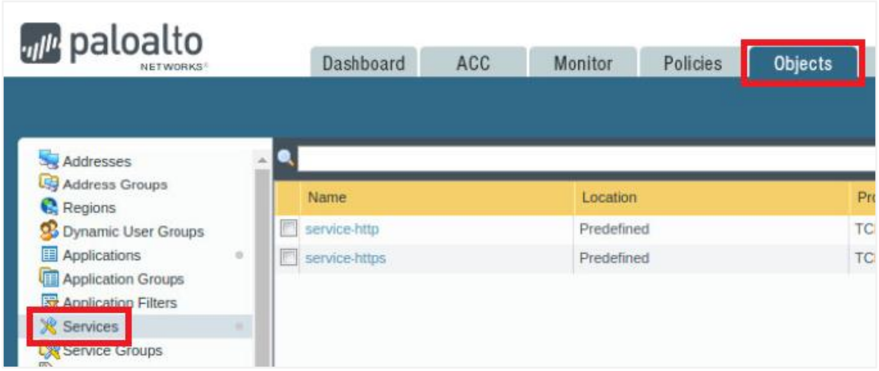
If a filter is in place, clear it to see all traffic. If entries are not present, click the refresh icon next to the *Help* icon.

4. Close the **msn.com** and **shutterfly.com** tabs in **Chromium Web Browser.**
5. Leave the firewall web interface open to continue with the next task.

3.5 Create FTP Service

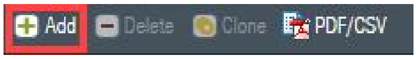
When you define Security policy rules for specific applications, you can select one or more services that limit the port numbers that the applications can use.

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



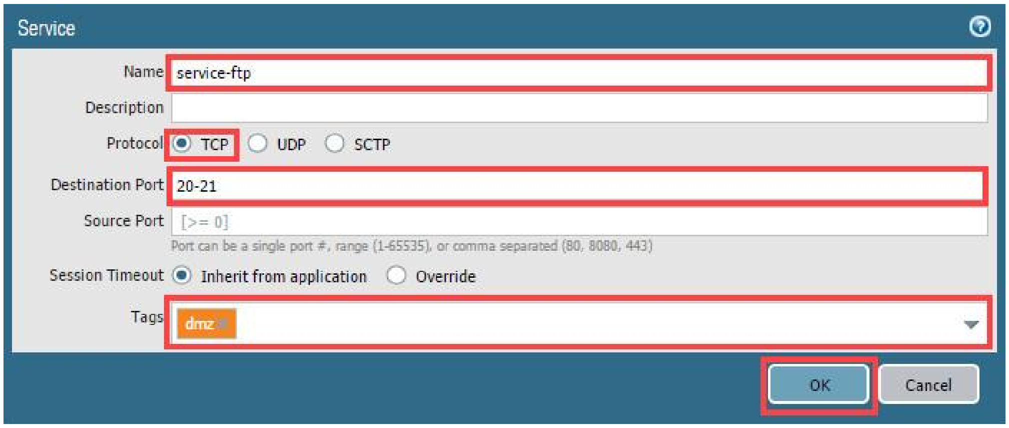
	Name	Location	Pr
□	service-http	Predefined	TC
□	service-https	Predefined	TC

2. Click **Add** to create a new service.



3. In the *Service* window, configure the following and then click **OK** when finished.

Parameter	Value
Name	`service-ftp`
Protocol	Verify that the **TCP** radio button is selected
Destination Port	Type `20-21`
Tags	Select **dmz** from the dropdown list



Name service-ftp

Description

Protocol ● TCP ○ UDP ○ SCTP

Destination Port 20-21

Source Port [>= 0]

Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)

Session Timeout ● Inherit from application ○ Override

Tags dmz

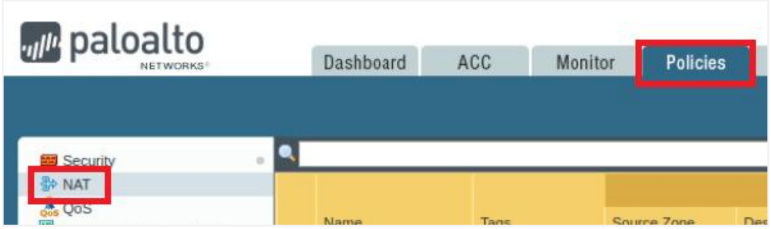
The host in the DMZ is preconfigured with an FTP server. This service matches the standard control and data ports for FTP.

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

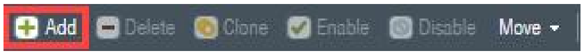
3.6 Create a Destination NAT Policy

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. You will connect from the Windows host (192.168.1.20) to an interface address on the firewall (192.168.1.1). The firewall will translate this connection to the DMZ server at 192.168.50.10.

1. In the web interface, navigate to **Policies > NAT**.

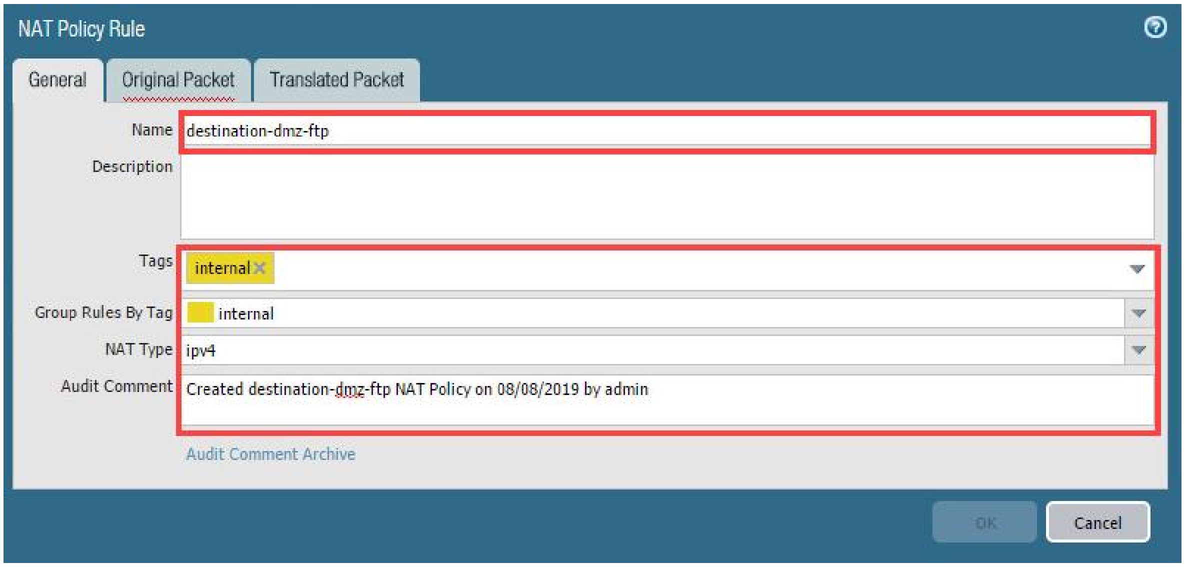


2. Click **Add** to define a new destination NAT Policy Rule.



3. In the *NAT Policy Rule* window, configure the following:

Parameter	Value
Name	`destination-dmz-ftp`
Tags	**internal**
Group Rules By Tag	Select **internal** from the dropdown list
NAT Type	Verify that **ipv4** is selected
Audit Comment	Type `Created destination-dmz-ftp NAT Policy on <date> by admin`

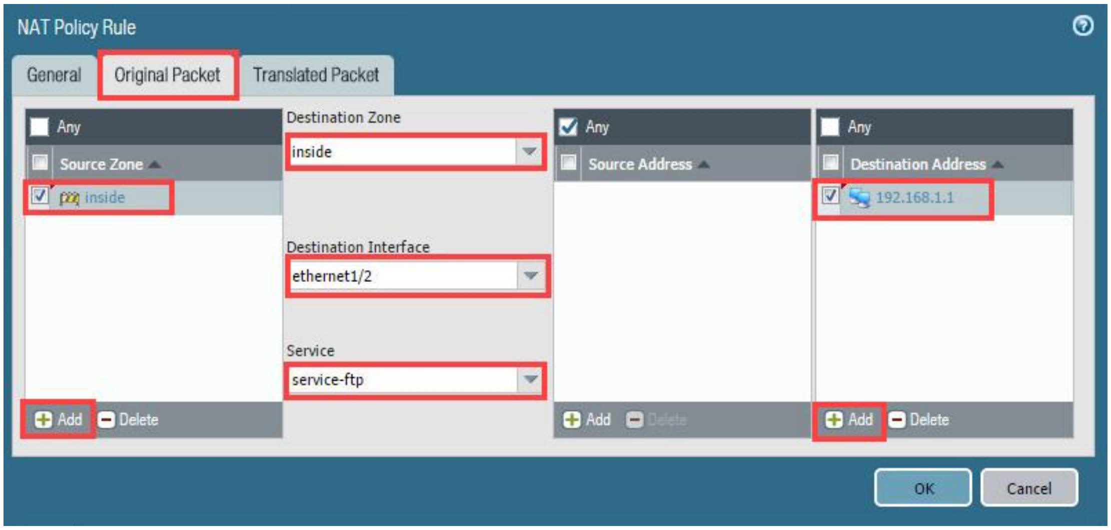


Name: destination-dmz-ftp
Description:
Tags: internal
Group Rules By Tag: internal
NAT Type: ipv4
Audit Comment: Created destination-dmz-ftp NAT Policy on 08/08/2019 by admin

The *Audit Comment* creates an audit trail where you can track the history of changes to the NAT Policy Rule.

4. In the *NAT Policy Rule* window, click the **Original Packet** tab and configure the following:

Parameter	**Value**
Source Zone	Click **Add** and select **inside**
Destination Zone	**inside**
Destination Interface	**ethernet1/2**
Service	**service-ftp**
Destination Address	Click **Add** and manually enter `192.168.1.1`



□ Any
Source Zone
☑ inside

Destination Zone: inside

Destination Interface: ethernet1/2

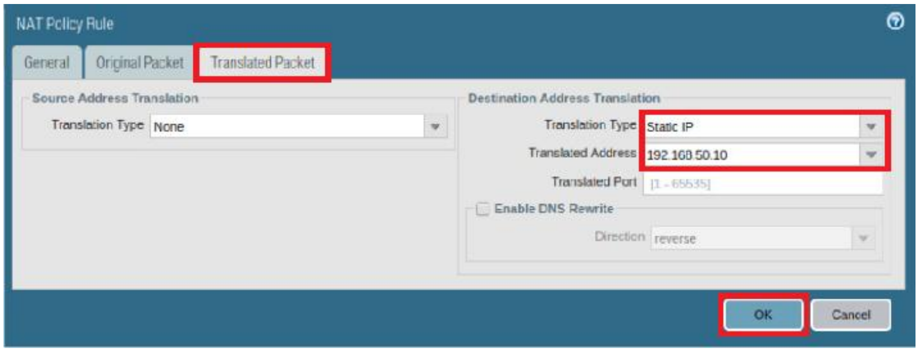
Service: service-ftp

☑ Any
Source Address

□ Any
Destination Address
☑ 192.168.1.1

5. In the *NAT Policy Rule* window, click the **Translated Packet** tab and configure the following. Once finished, click **OK**.

Parameter	**Value**
Destination Address Translation Type	**Static IP**
Translated Address	`192.168.50.10` (address of DMZ Server)



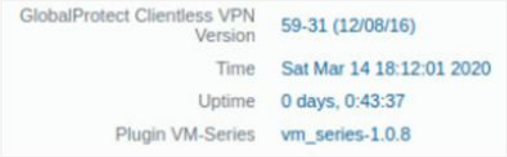
Source Address Translation
Translation Type: None

Destination Address Translation
Translation Type: Static IP
Translated Address: 192.168.50.10
Translated Port: [1 - 65535]
□ Enable DNS Rewrite
Direction: reverse

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

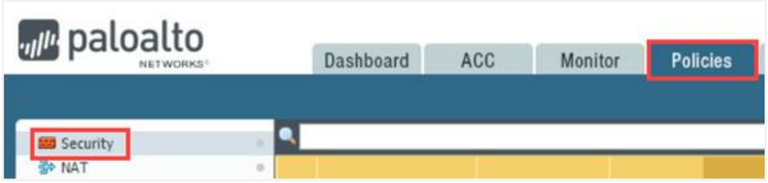
3.7 Create a Security Policy Rule

1. In the web interface, click the **Dashboard** tab.
2. Annotate the current time referenced by the firewall. Do note, however, that the times will be different.

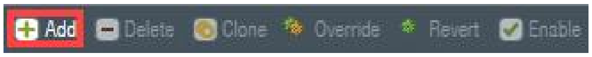


GlobalProtect Clientless VPN Version: 59-31 (12/08/16)
Time: Sat Mar 14 18:12:01 2020
Uptime: 0 days, 0:43:37
Plugin VM-Series: vm_series-1.0.8

3. Navigate to **Policies > Security**.

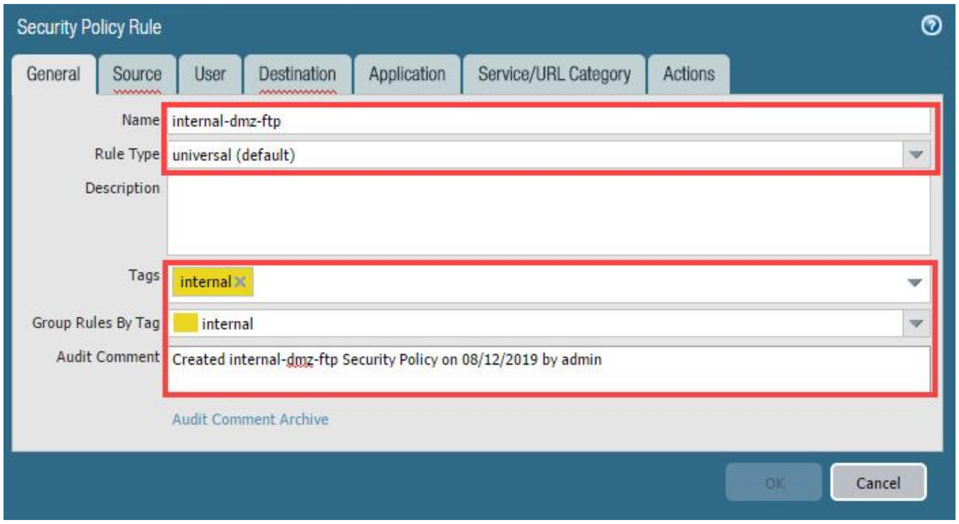


4. Click **Add** to define a new Security Policy Rule.



5. In the *Security Policy Rule* window, configure the following:

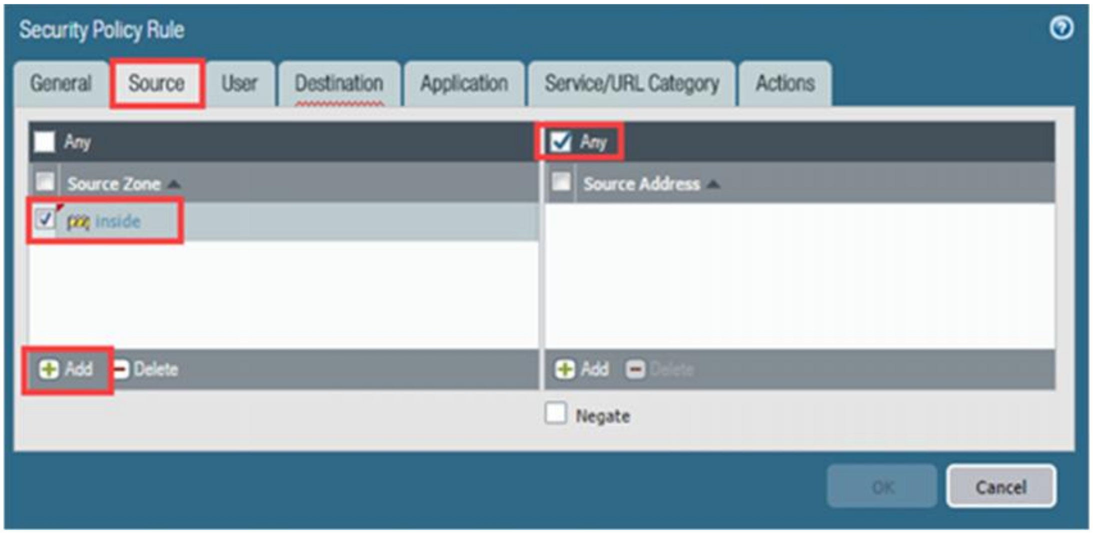
Parameter	Value
Name	`internal-dmz-ftp`
Rule Type	**universal (default)**
Tags	**internal**
Group Rules By Tag	Select **internal** from the dropdown list
Audit Comment	Type `Created internal-dmz-ftp Security Policy on <date> by admin`



Name: internal-dmz-ftp
Rule Type: universal (default)
Description:
Tags: internal
Group Rules By Tag: internal
Audit Comment: Created internal-dmz-ftp Security Policy on 08/12/2019 by admin

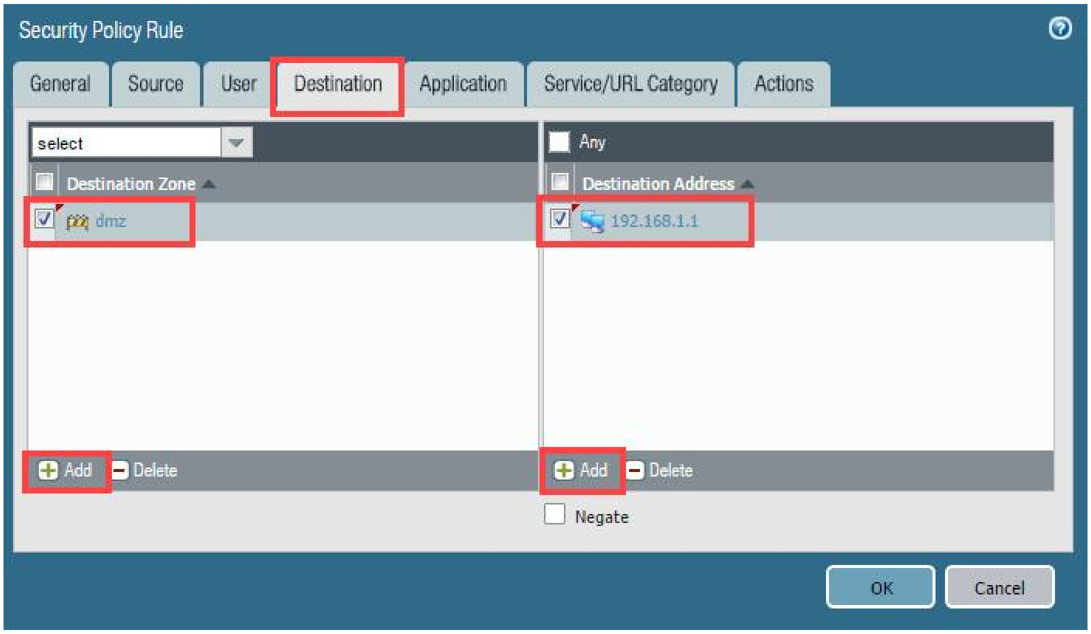
6. In the *Security Policy Rule* window, click the **Source** tab and configure the following:

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



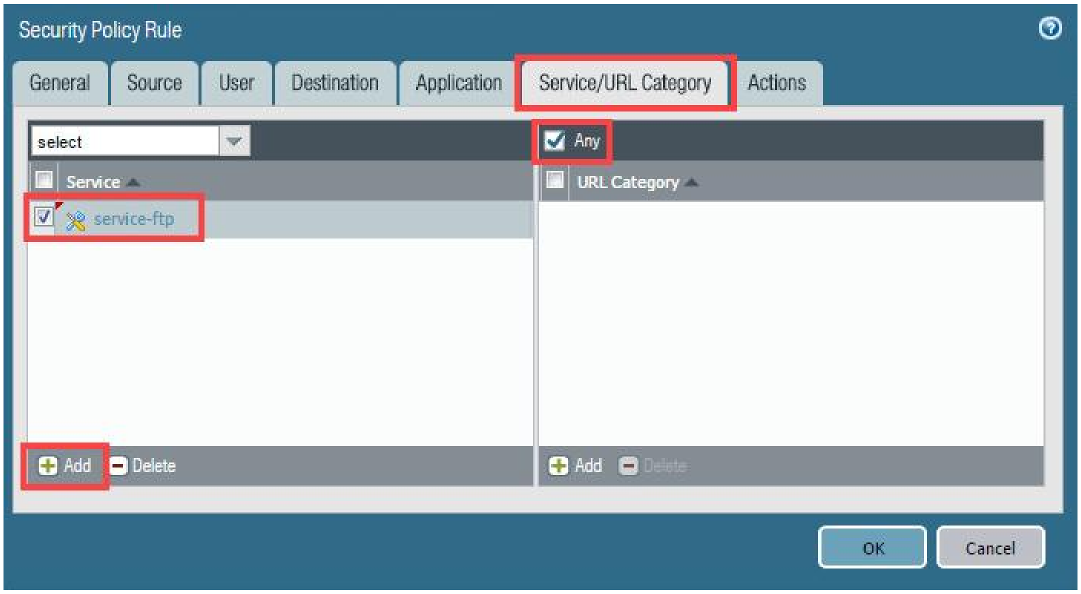
7. In the *Security Policy Rule* window, click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	Click **Add** and select **dmz**
Destination Address	Click **Add** and manually enter `192.168.1.1`

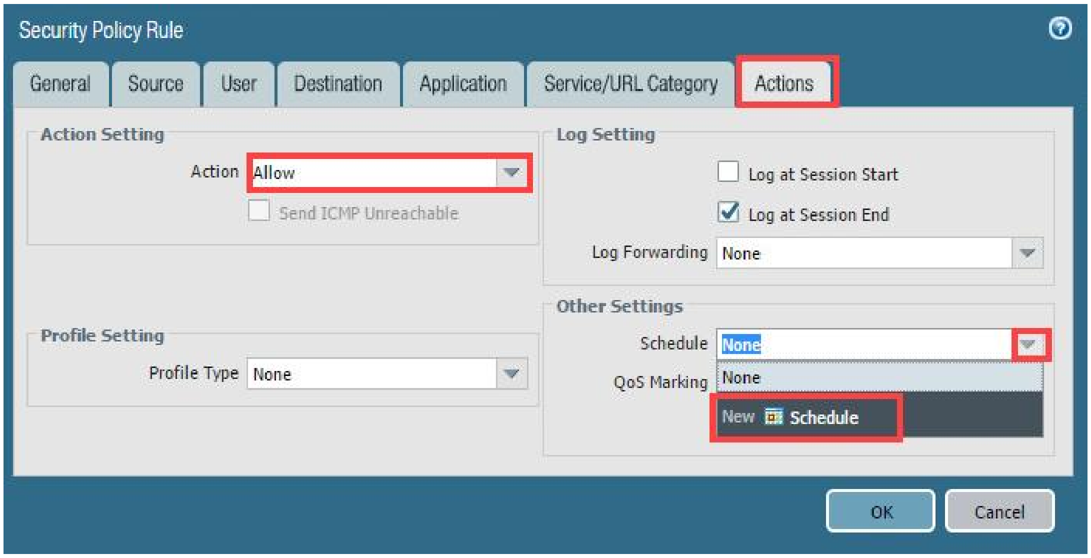


8. In the *Security Policy Rule* window, click the **Service/URL Category** tab and configure the following:

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



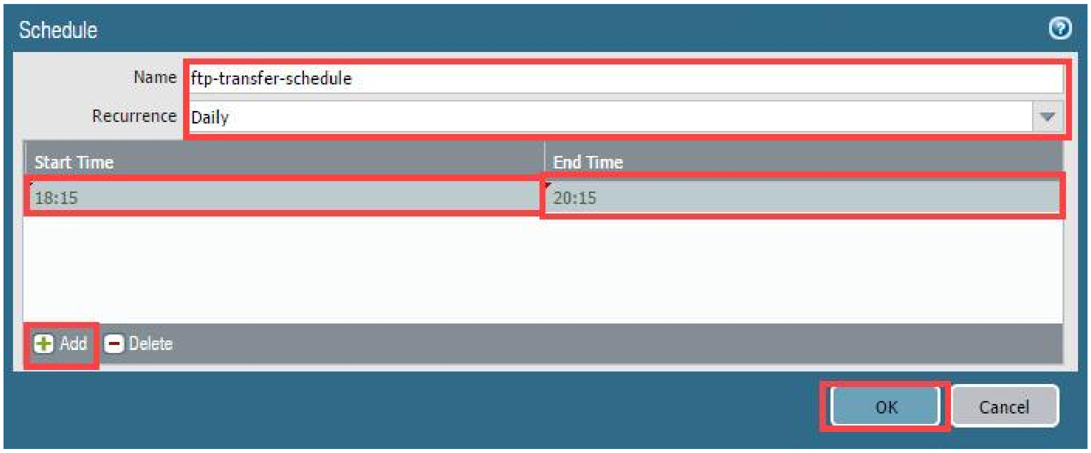
9. Click the **Actions** tab and verify that **Allow** is selected. Locate the *Schedule* dropdown list and select **New Schedule**.



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.

10. In the *Schedule* window, configure the following. Once finished, click **OK**.

Parameter	**Value**
Name	`ftp-transfer-schedule`
Recurrence	**Daily**
Start Time	**5 minutes** from the time annotated in Step 2 (if exceeded the time, enter a greater time)
End time	Add **2 hours** from the current firewall time.



Name: ftp-transfer-schedule
Recurrence: Daily

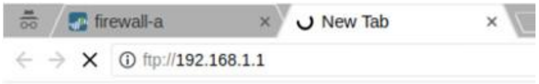
Start Time	End Time
18:15	20:15

Input the values for *Start Time* and *End Time* in 24-hour format.

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

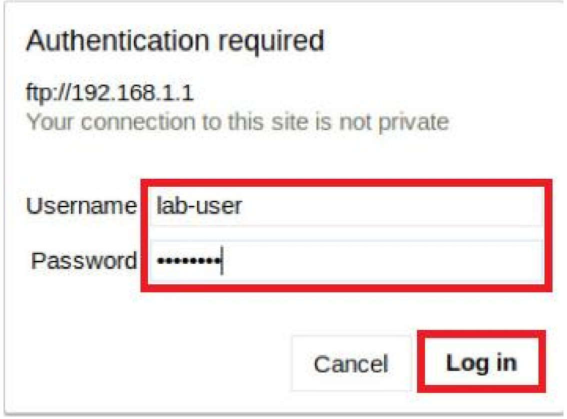
3.8 Test the Connection

1. Wait for the scheduled time to start (from *Task 1.7, Step 10*) for the *internal-dmz-ftp* Security Policy Rule.
2. Open a new tab in the **Chromium Web Browser** and browse to `ftp://192.168.1.1`.



3. At the prompt for login information, enter the following credentials and click **Log In**.

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



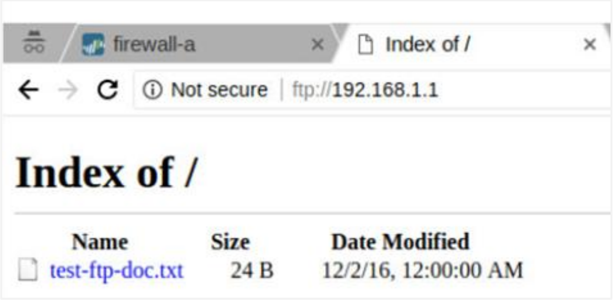
Authentication required

ftp://192.168.1.1
Your connection to this site is not private

Username: lab-user
Password: •••••••••

The *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.

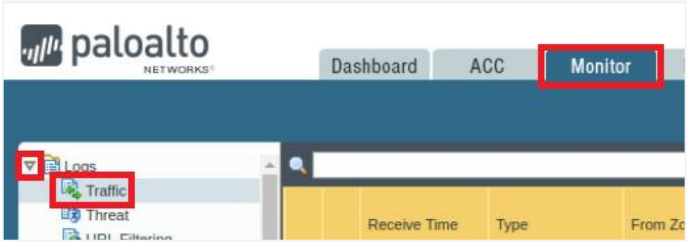
4. Verify that you can view the directory listing and then close the **Chrome** browser window:



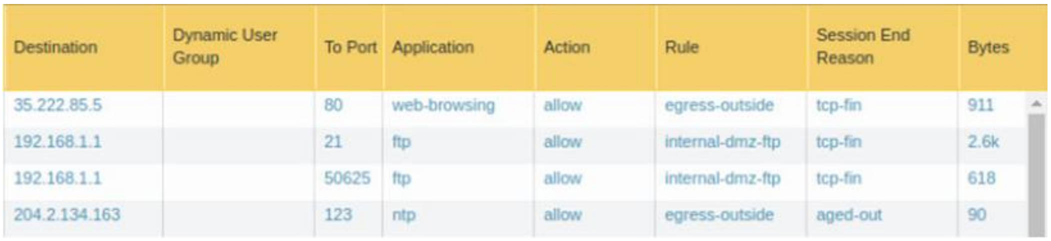
Index of /

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

5. Change focus to the firewall web interface and navigate to **Monitor > Logs > Traffic**.



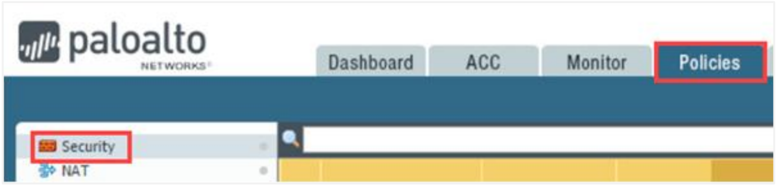
6. Find the entries where the application *ftp* has been allowed by rule *internal-dmz-ftp*.



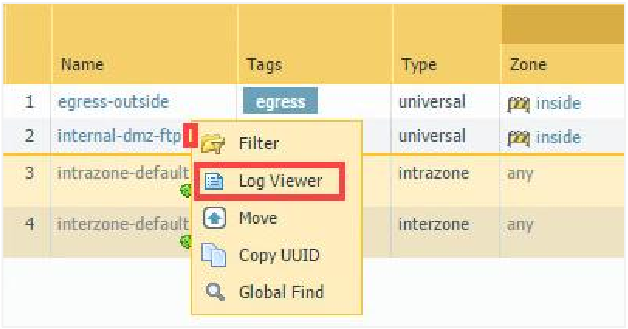
Destination	Dynamic User Group	To Port	Application	Action	Rule	Session End Reason	Bytes
35.222.85.5		80	web-browsing	allow	egress-outside	tcp-fin	911
192.168.1.1		21	ftp	allow	internal-dmz-ftp	tcp-fin	2.6k
192.168.1.1		50625	ftp	allow	internal-dmz-ftp	tcp-fin	618
204.2.134.163		123	ntp	allow	egress-outside	aged-out	90

Notice the *Destination* address and rule matching.

7. As an alternative method to accessing the Traffic log in the web interface, select **Policies > Security**.

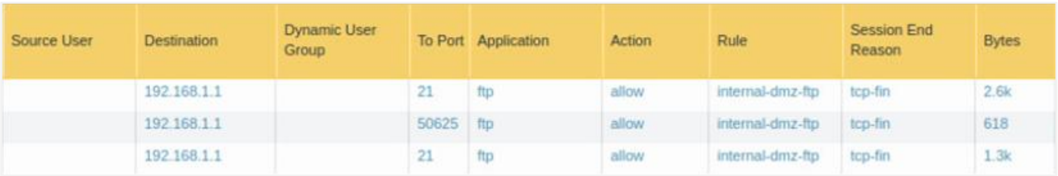


8. From the dropdown icon next to the rule name for *internal-dmz-ftp* (seen when the mouse is hovered over the rule name), select **Log Viewer**.



	Name	Tags	Type	Zone
1	egress-outside	egress	universal	inside
2	internal-dmz-ftp		universal	inside
3	intrazone-default		intrazone	any
4	interzone-default		interzone	any

9. You should see the following:



Source User	Destination	Dynamic User Group	To Port	Application	Action	Rule	Session End Reason	Bytes
	192.168.1.1		21	ftp	allow	internal-dmz-ftp	tcp-fin	2.6k
	192.168.1.1		50625	ftp	allow	internal-dmz-ftp	tcp-fin	618
	192.168.1.1		21	ftp	allow	internal-dmz-ftp	tcp-fin	1.3k

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