



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

### **Lab 3: Security and NAT Policies**

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

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

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

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

## Contents

Introduction .....	3
Objectives.....	3
Lab Topology .....	4
Lab Settings .....	5
3 Lab: Security and NAT Policies .....	6
3.0 Load Lab Configuration .....	6
3.1 Create Tags .....	7
3.2 Create a Source NAT Policy .....	10
3.3 Create Security Policy Rules .....	13
3.4 Verify Internet Connectivity .....	17
3.5 Create FTP Service .....	18
3.6 Create a Destination NAT Policy .....	19
3.7 Create a Security Policy Rule .....	21
3.8 Test the Connection .....	26

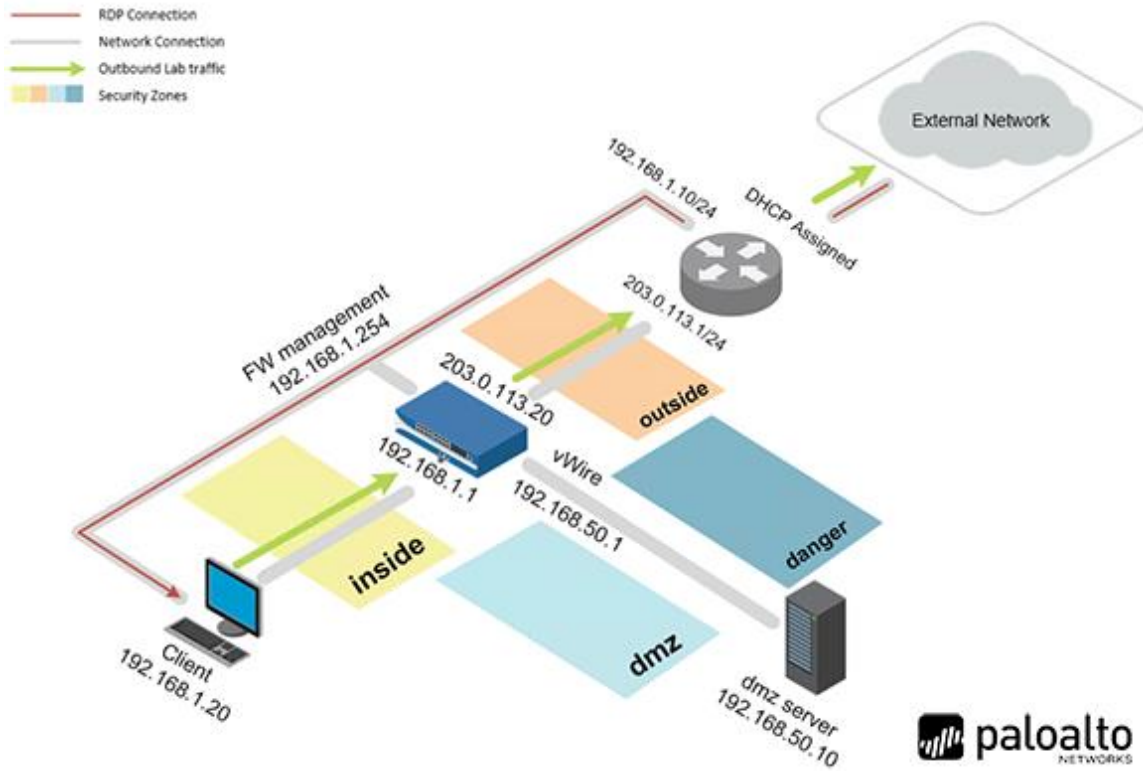
## Introduction

The interfaces are configured and working but we can't pass traffic through the appliance yet. That is because we need to setup 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



## Lab Settings

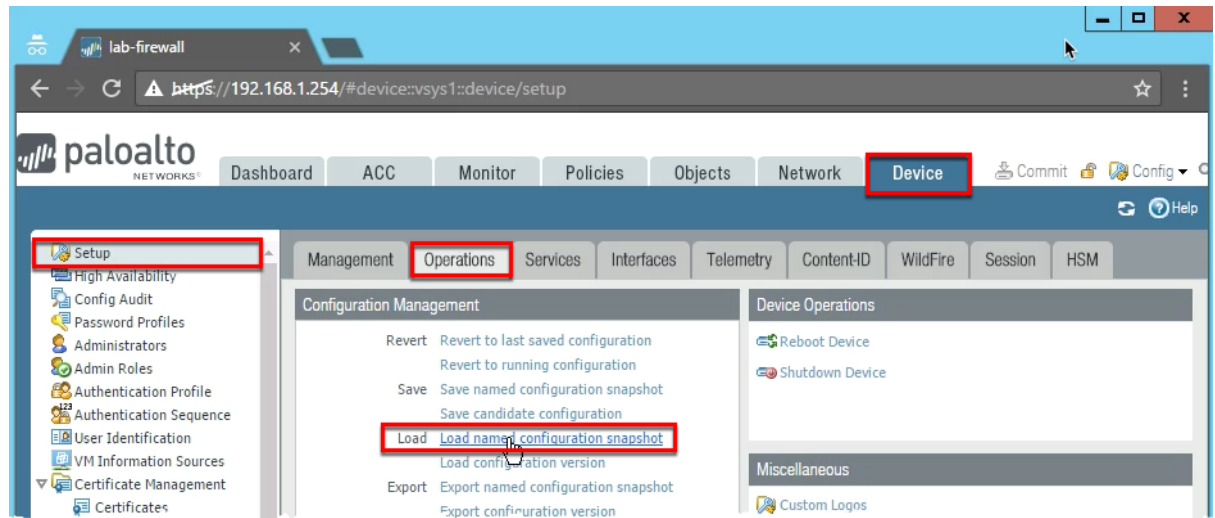
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

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

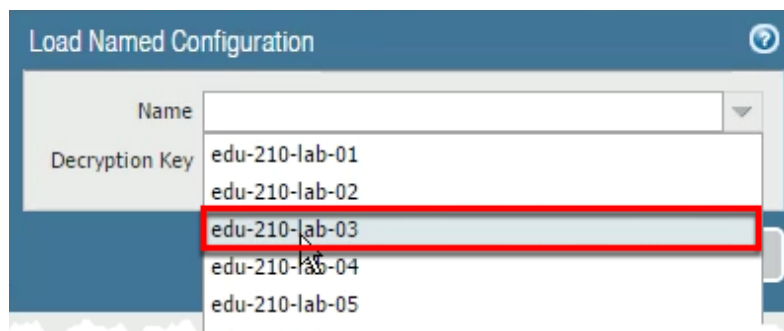
### 3 Lab: Security and NAT Policies

#### 3.0 Load Lab Configuration

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



3. Select **edu-210-lab-03** and click **OK**.

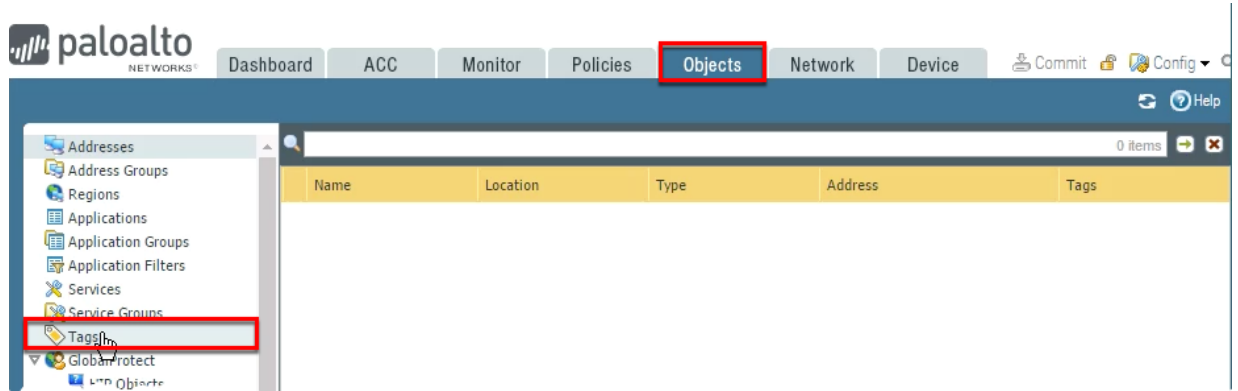


4. Click **Close**.
5. **Commit** all changes.

### 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**.



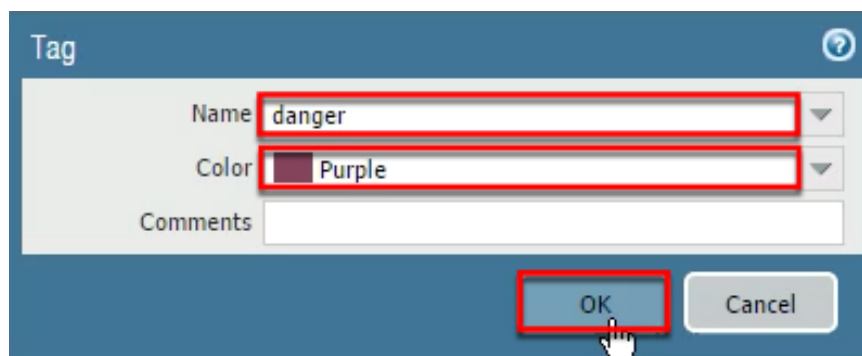
2. Click **Add** to define a new tag.



3. Configure the following:

Parameter	Value
Name	Select <b>danger</b>
Color	Purple

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

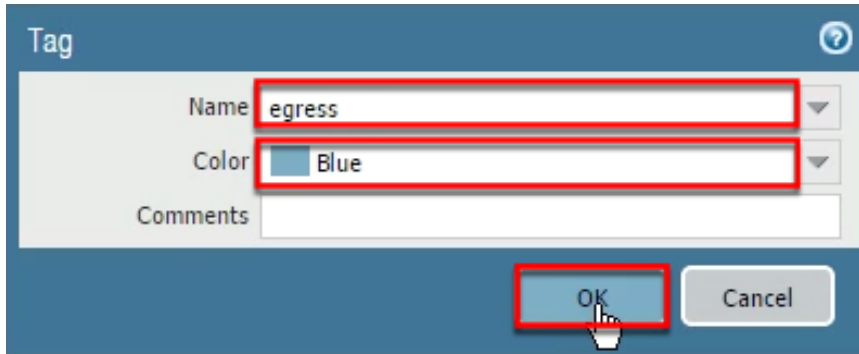


5. Click **Add** again to define another new tag.

6. Configure the following:

Parameter	Value
Name	egress
Color	Blue

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

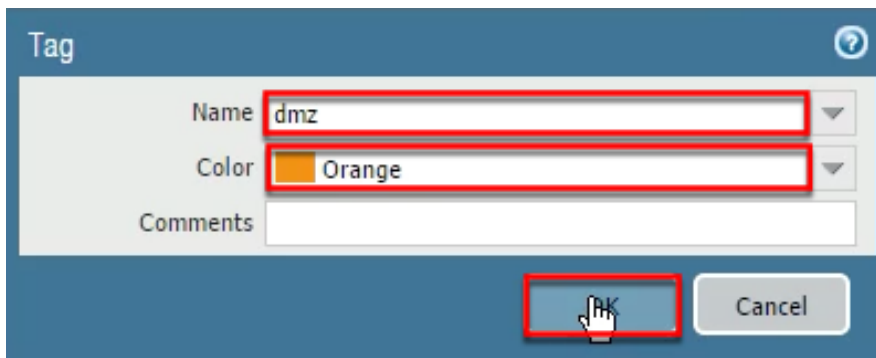


8. Click **Add** again to define another new tag.

9. Configure the following:

Parameter	Value
Name	Select <b>dmz</b>
Color	Orange

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

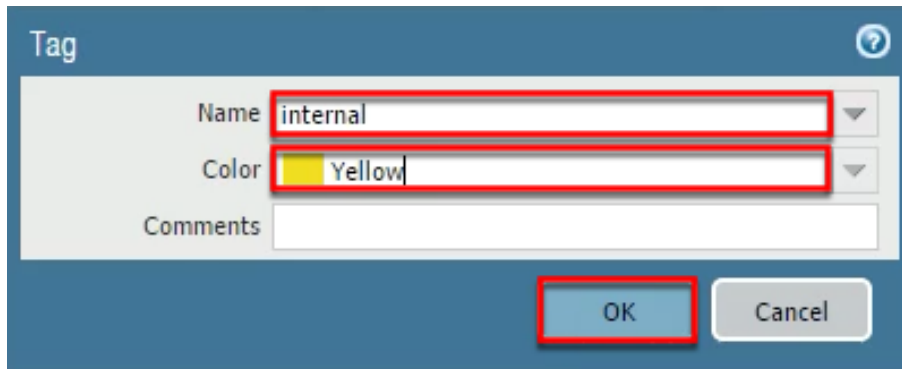


11. Click **Add** again to define another

12. Configure the following:

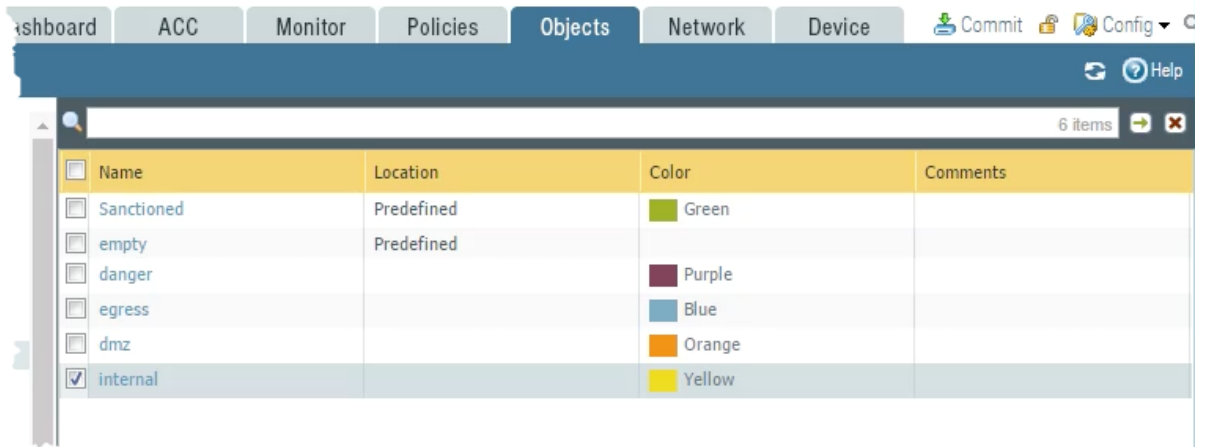
Parameter	Value
Name	internal
Color	Yellow





The image shows a 'Tag' configuration window. It has a title bar with a question mark icon. Inside, there are three fields: 'Name' with the value 'internal', 'Color' with a yellow swatch and the text 'Yellow', and 'Comments' which is empty. At the bottom right, there are 'OK' and 'Cancel' buttons. Red rectangles highlight the 'Name' field, the 'Color' field, and the 'OK' button.

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

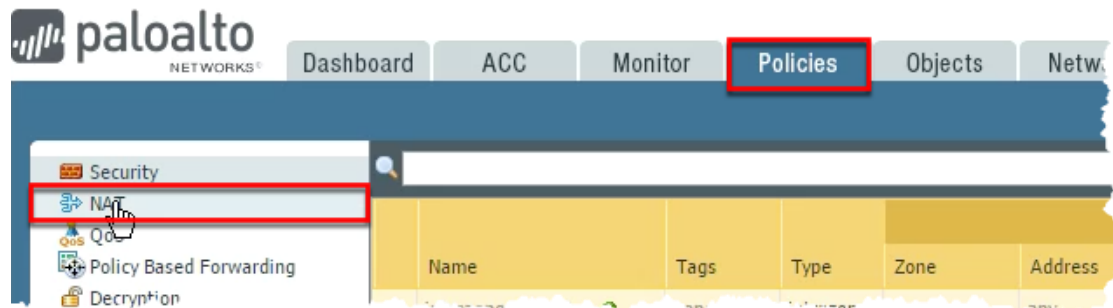


The image shows a screenshot of the NDG interface with the 'Objects' tab selected. A table lists several predefined tags. The 'internal' tag is selected with a checkmark in the first column.

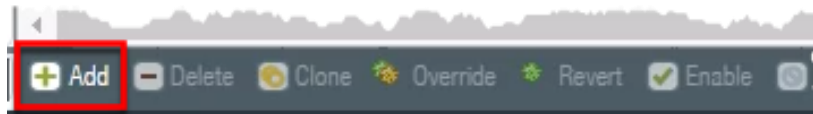
<input type="checkbox"/>	Name	Location	Color	Comments
<input type="checkbox"/>	Sanctioned	Predefined	Green	
<input type="checkbox"/>	empty	Predefined		
<input type="checkbox"/>	danger		Purple	
<input type="checkbox"/>	egress		Blue	
<input type="checkbox"/>	dmz		Orange	
<input checked="" type="checkbox"/>	internal		Yellow	

## 3.2 Create a Source NAT Policy

1. Select **Policies > NAT**.

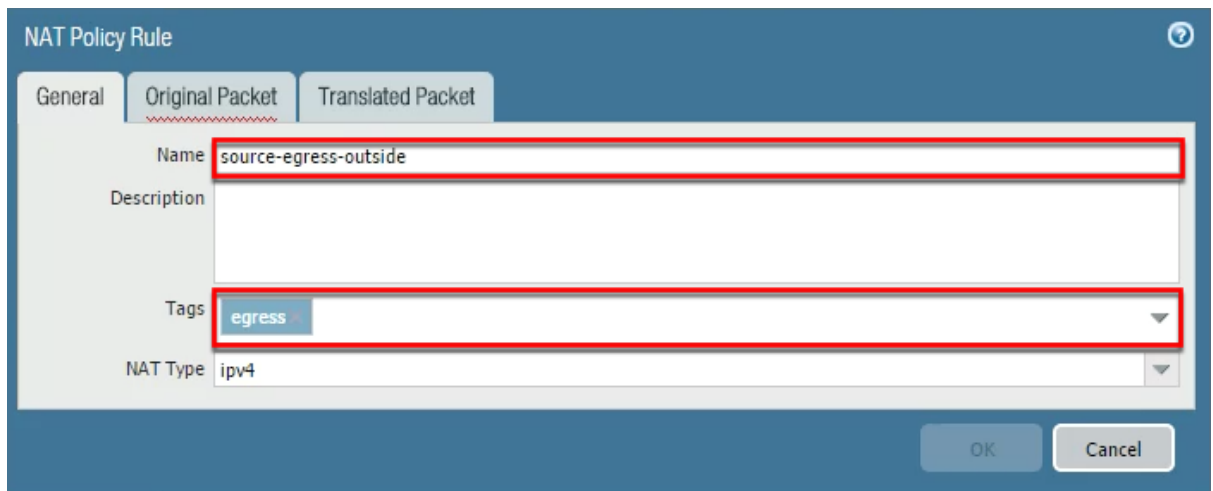


2. Click **Add** to define a new source NAT policy.



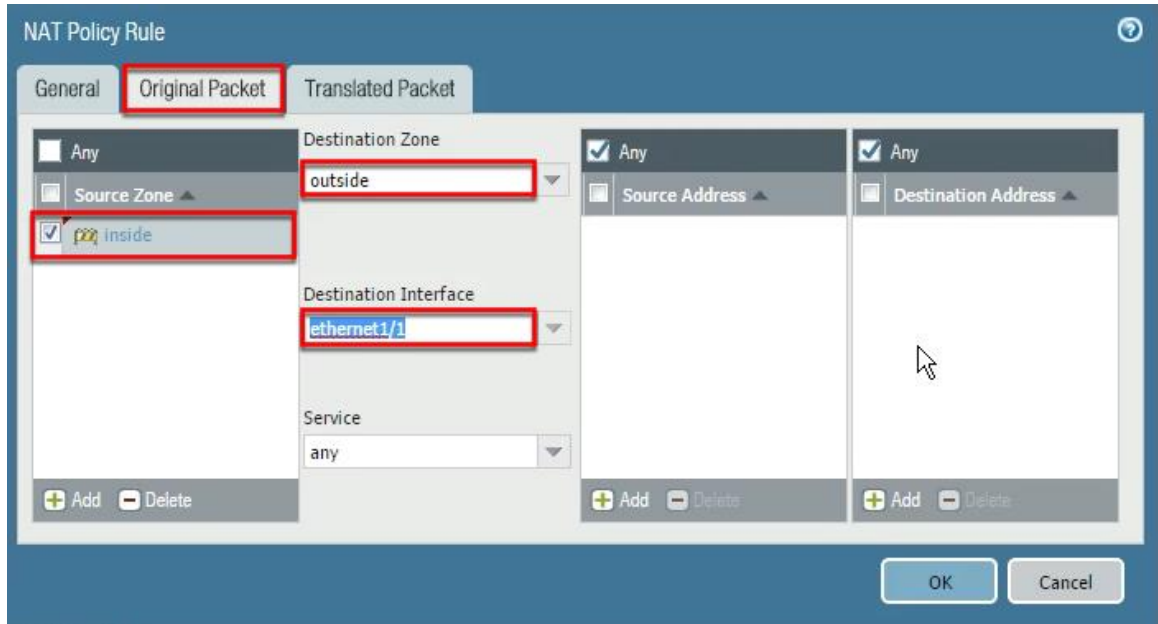
3. Configure the following:

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

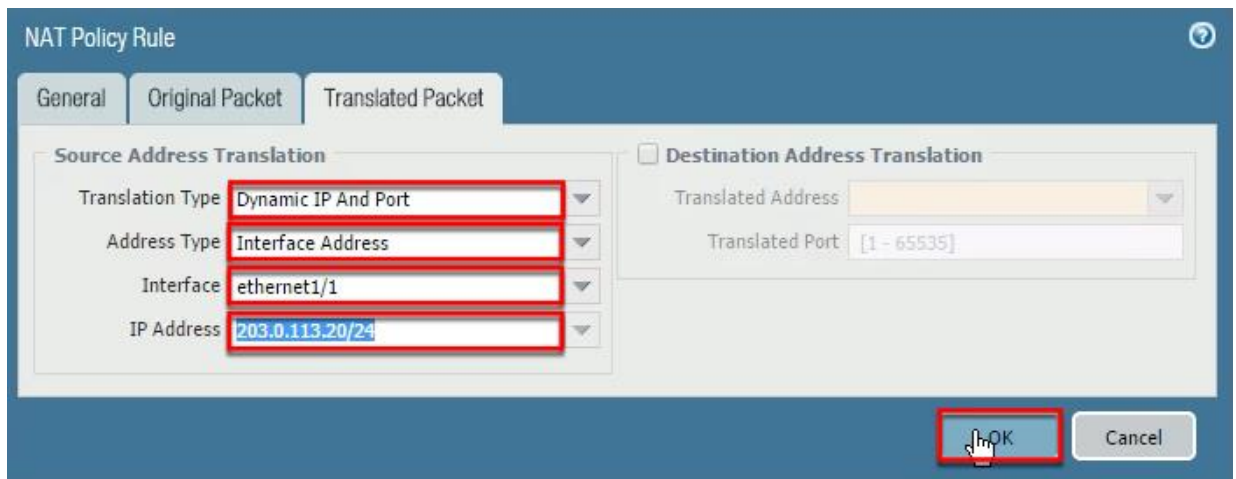


The screenshot shows the 'NAT Policy Rule' configuration window with the 'Original Packet' tab selected. The 'Source Zone' is set to 'inside' and the 'Destination Zone' is set to 'outside'. The 'Destination Interface' is set to 'ethernet1/1' and the 'Service' is set to 'any'. The 'Translated Packet' tab is also visible, showing 'Any' for both Source and Destination Address.

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

Parameter	Value
Translation Type	<b>Dynamic IP And Port</b>
Address Type	<b>Interface Address</b>
Interface	<b>ethernet1/1</b>
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.



The screenshot shows the 'NAT Policy Rule' configuration window with the 'Translated Packet' tab selected. The 'Source Address Translation' section is expanded, showing 'Dynamic IP And Port' for Translation Type, 'Interface Address' for Address Type, 'ethernet1/1' for Interface, and '203.0.113.20/24' for IP Address. The 'Destination Address Translation' section is collapsed. The 'OK' button is highlighted with a red box.

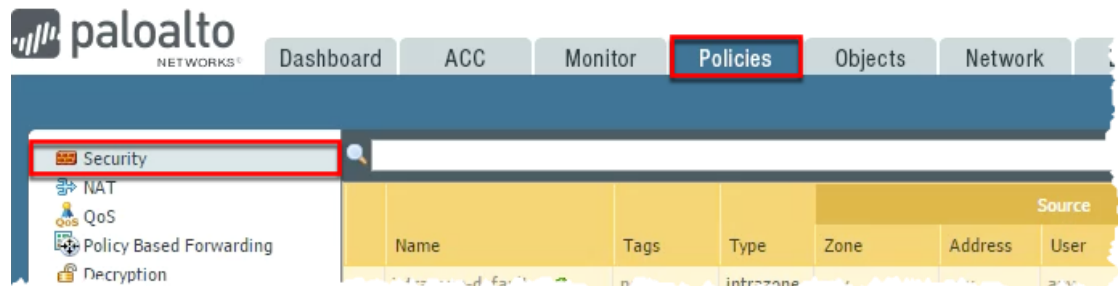
You will not be able to access the internet yet because you still need to configure a Security policy to allow traffic to flow between zones.



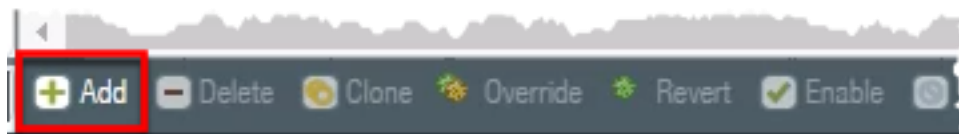
### 3.3 Create Security Policy Rules

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**.

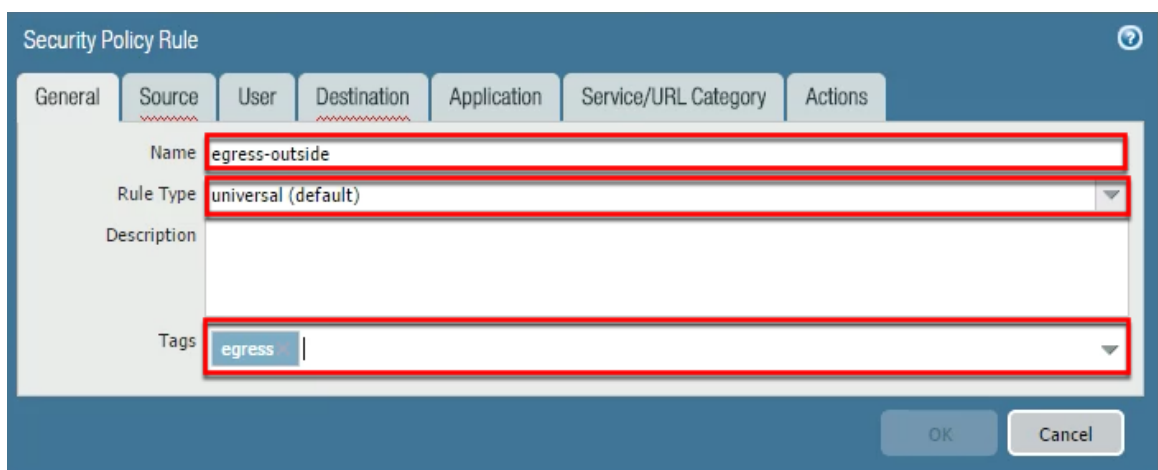


2. Click **Add** to define a Security policy rule.



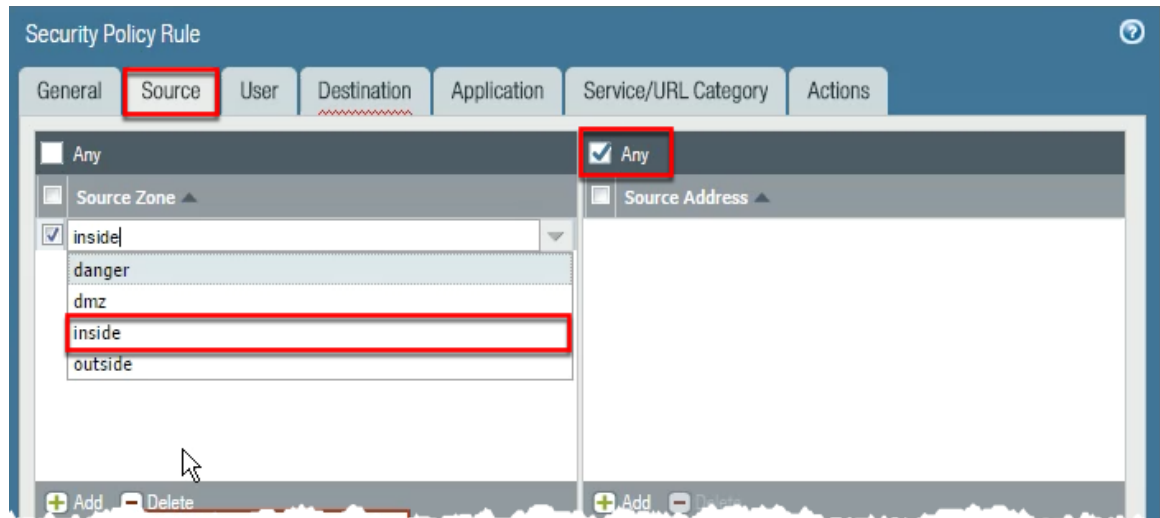
3. Configure the following:

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



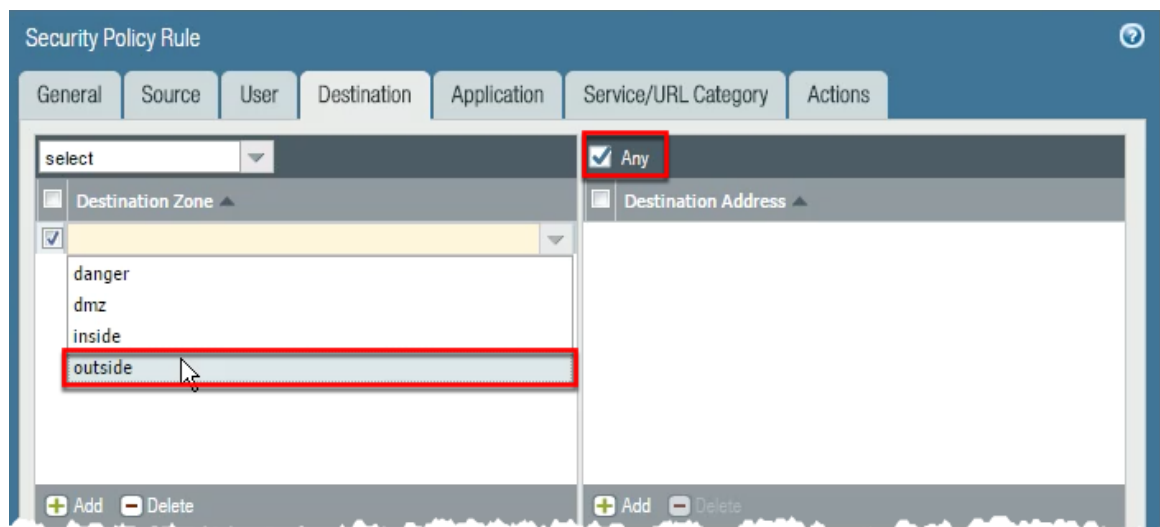
4. Click the **Source** tab and configure the following:

Parameter	Value
Source Zone	inside
Source Address	Any



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

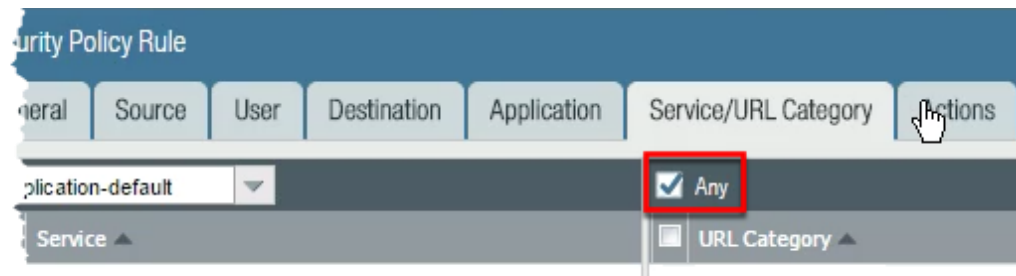
Parameter	Value
Destination Zone	outside
Destination Address	Any



6. Click the **Application** tab and verify that **Any** is checked.

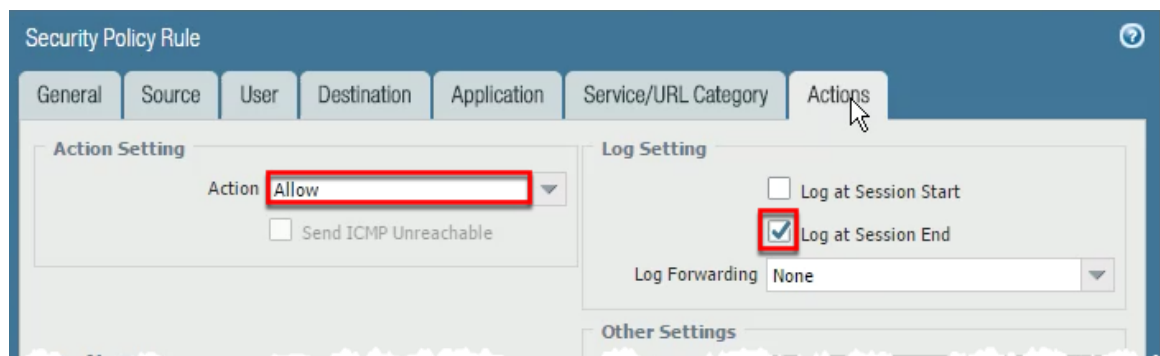


7. Click the **Service/URL Category** tab and verify that **Any** is selected.

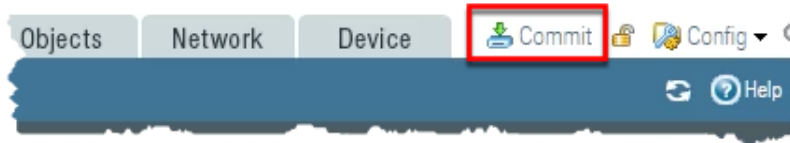


8. Click the **Actions** tab and verify the following:

Parameter	Value
Action Setting	<b>Allow</b>
Log Setting	<b>Log at Session End</b>



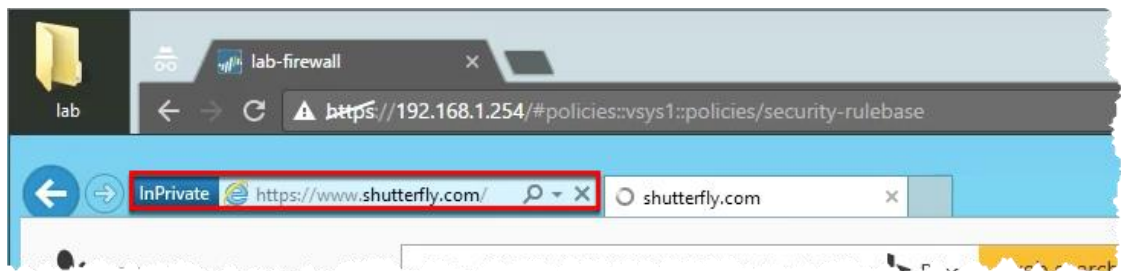
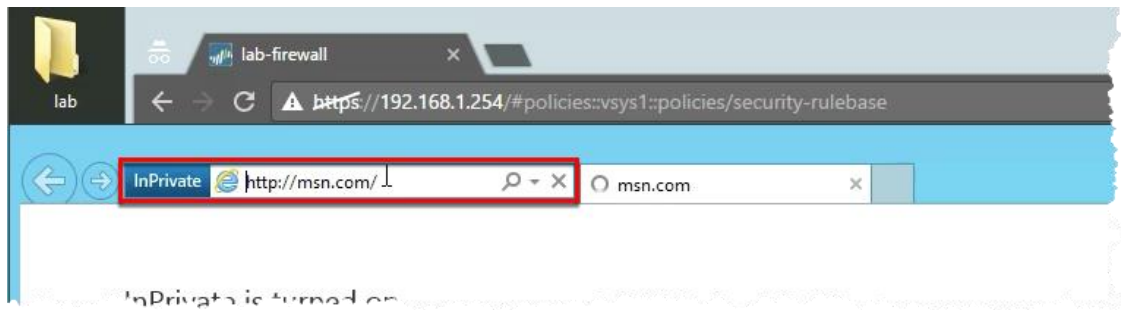
9. Click **OK** to close the **Security Policy Rule** configuration window.  
 10. **Commit** all changes.



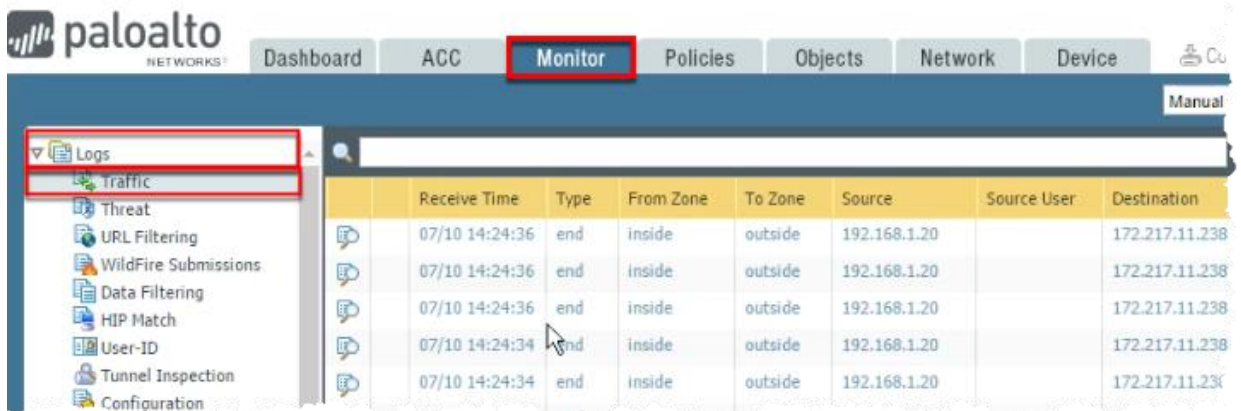


### 3.4 Verify Internet Connectivity

1. Test internet connectivity by opening a different browser in private/incognito mode and browse to `msn.com` and `shutterfly.com`.



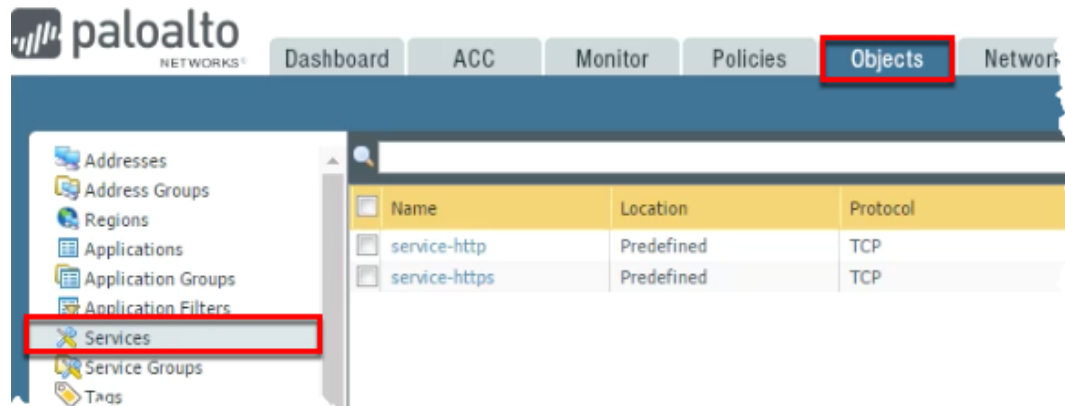
2. In the WebUI select **Monitor > Logs > Traffic**.
3. Traffic log entries should be present based on the internet test. Verify that there is allowed traffic that matches the Security policy rule *egress-outside*:



### 3.5 Create FTP Service

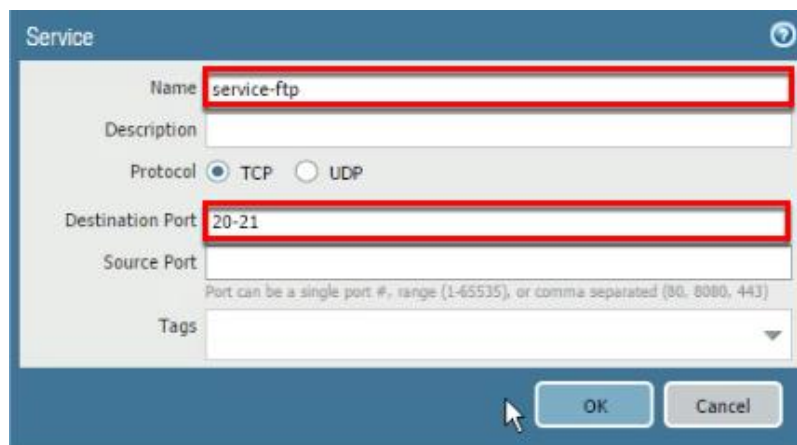
When you define Security policy rules for specific applications, you can select one or more services that limit the port numbers that the applications can use.

1. In the WebUI select **Objects > Services**.



2. Click **Add** to create a new service using the following:

Parameter	Value
Name	service-ftp
Destination Port	20-21



Service

Name: service-ftp

Description:

Protocol: ☒ TCP ☐ UDP

Destination Port: 20-21

Source Port:

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

Tags:

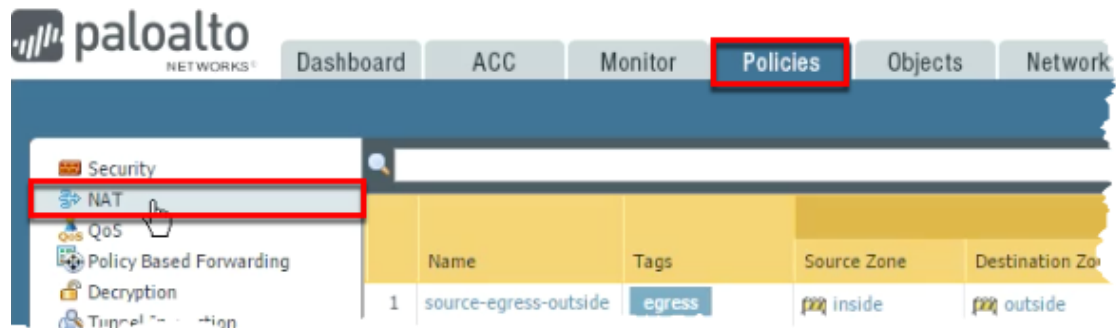
OK Cancel

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

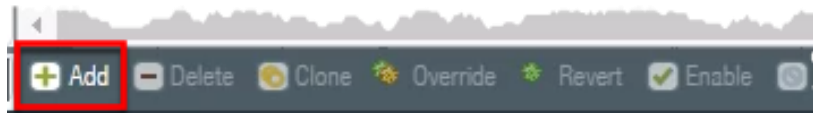
### 3.6 Create a Destination NAT Policy

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**.

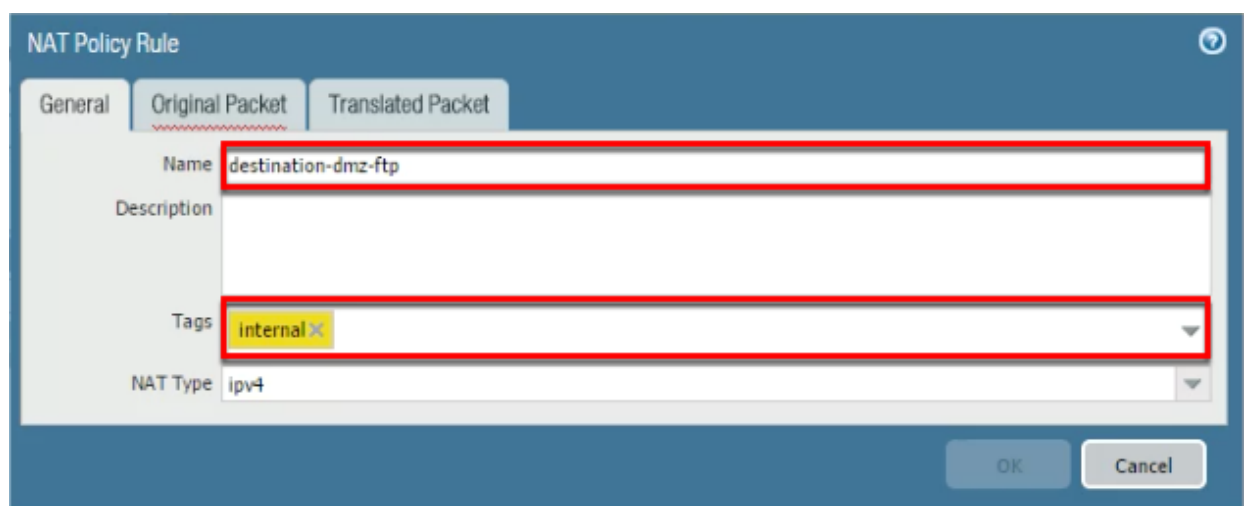


2. Click **Add** to define a new destination NAT policy rule.



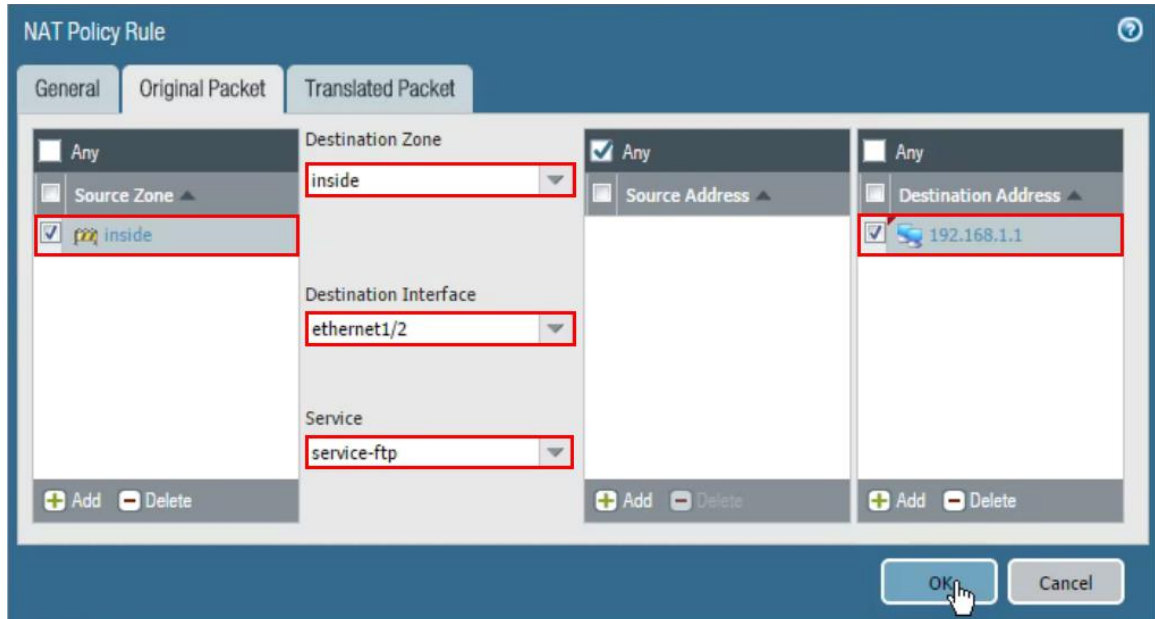
3. Configure the following:

Parameter	Value
Name	destination-dmz-ftp
Tags	internal



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

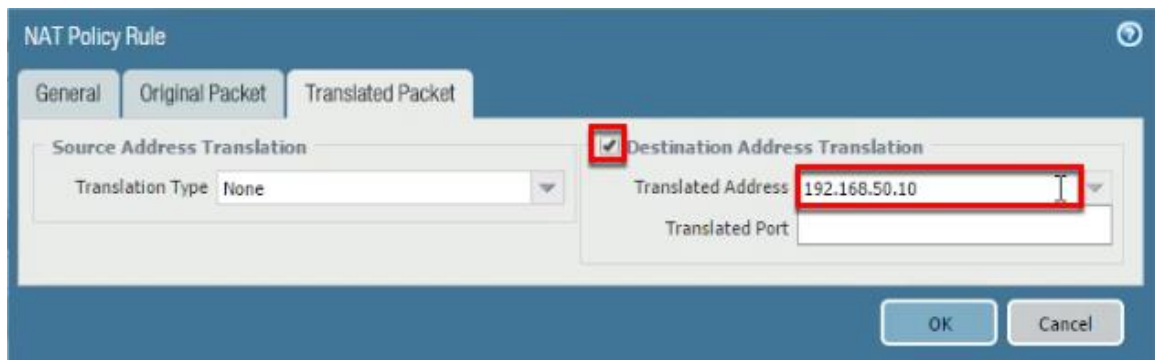
Parameter	Value
Source Zone	inside
Destination Zone	inside
Destination Interface	ethernet1/2
Service	service-ftp
Destination Address	192.168.1.1



The screenshot shows the 'NAT Policy Rule' configuration window with the 'Original Packet' tab selected. The 'Source Zone' is set to 'inside' (highlighted with a red box). The 'Destination Zone' is also set to 'inside' (highlighted with a red box). The 'Destination Interface' is set to 'ethernet1/2' (highlighted with a red box). The 'Service' is set to 'service-ftp' (highlighted with a red box). The 'Destination Address' is set to '192.168.1.1' (highlighted with a red box). The 'OK' button is highlighted with a red box and a mouse cursor.

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)



The screenshot shows the 'NAT Policy Rule' configuration window with the 'Translated Packet' tab selected. The 'Destination Address Translation' checkbox is checked (highlighted with a red box). The 'Translated Address' is set to '192.168.50.10' (highlighted with a red box). The 'Translated Port' is empty. The 'OK' button is highlighted with a red box.

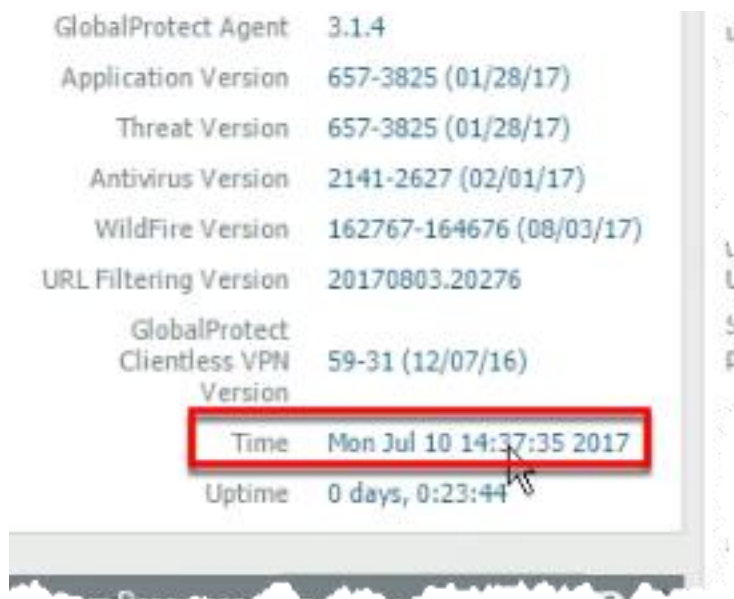
6. Click **OK** to close the **NAT Policy** configuration window.

### 3.7 Create a Security Policy Rule

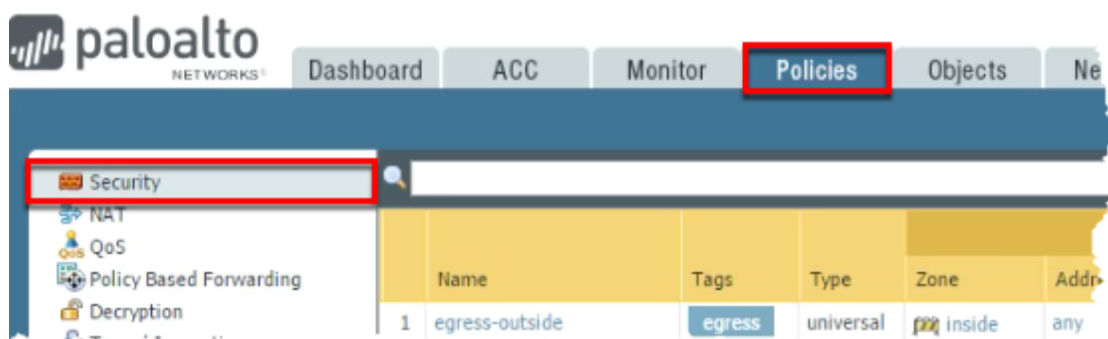
1. Click the **Dashboard** tab.



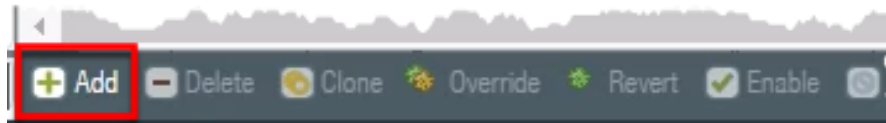
2. Annotate the current time referenced by the firewall:



3. Select **Policies > Security**.

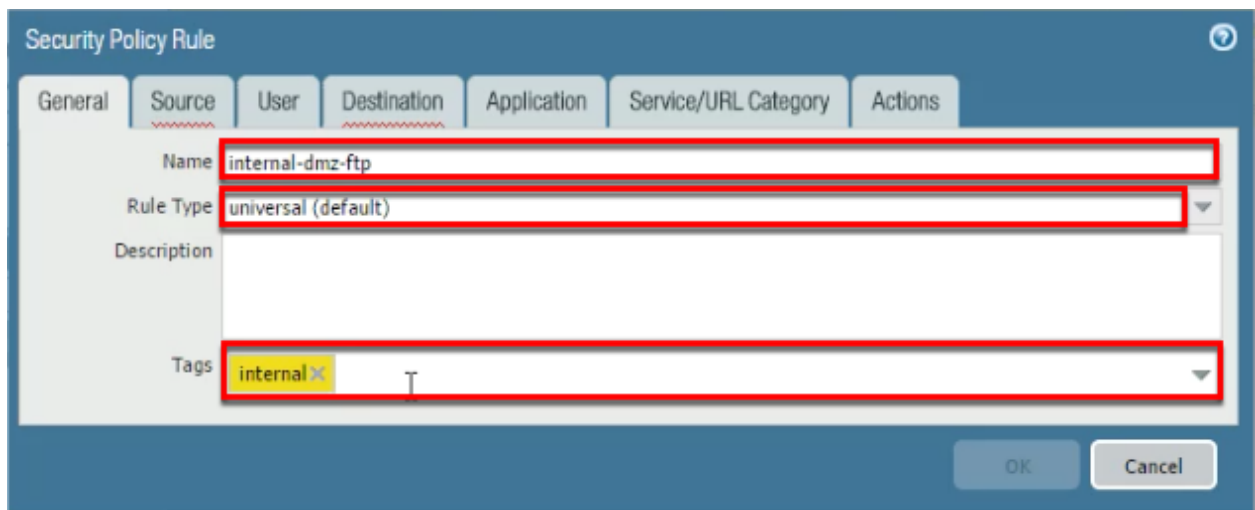


4. Click **Add** to define a new Security policy rule.



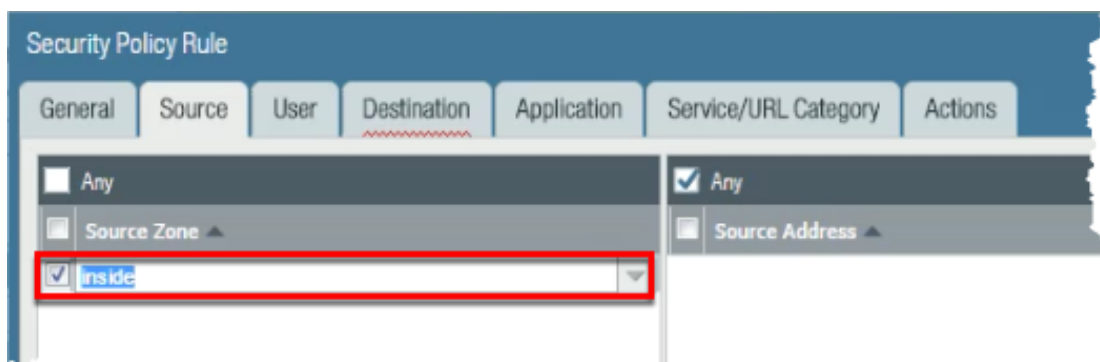
5. Configure the following:

Parameter	Value
Name	internal-dmz-ftp
Rule Type	<b>universal (default)</b>
Tags	<b>internal</b>



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

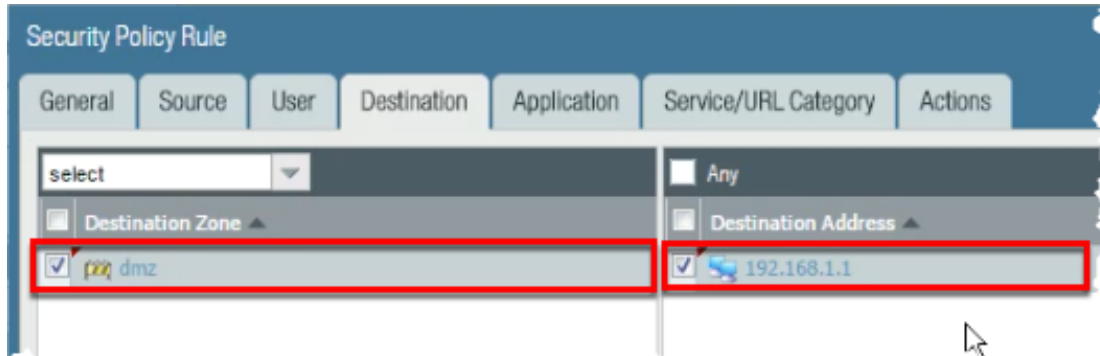
Parameter	Value
Source Zone	<b>inside</b>



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

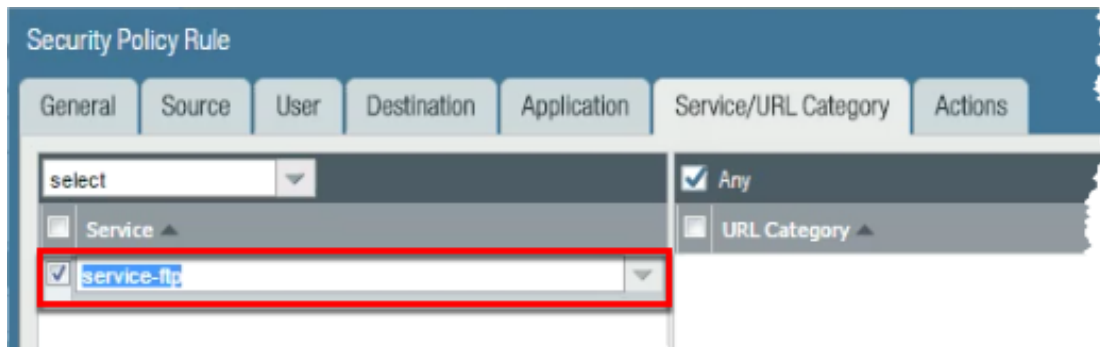
Parameter	Value
-----------	-------

Destination Zone	dmz
Destination Address	192.168.1.1

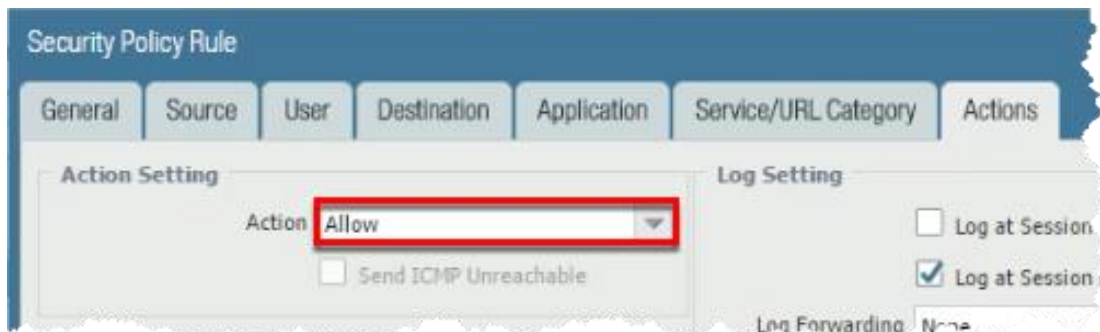


8. Click the **Service/URL Category** tab and configure the following:

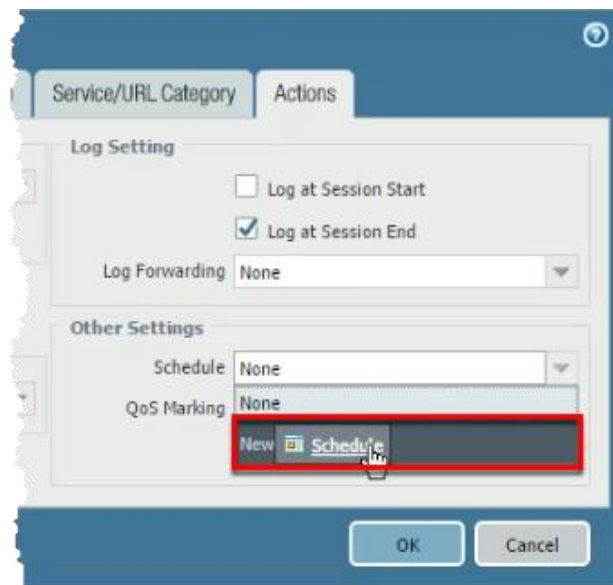
Parameter	Value
Service	service-ftp



9. Click the **Actions** tab and verify that Allow is selected.



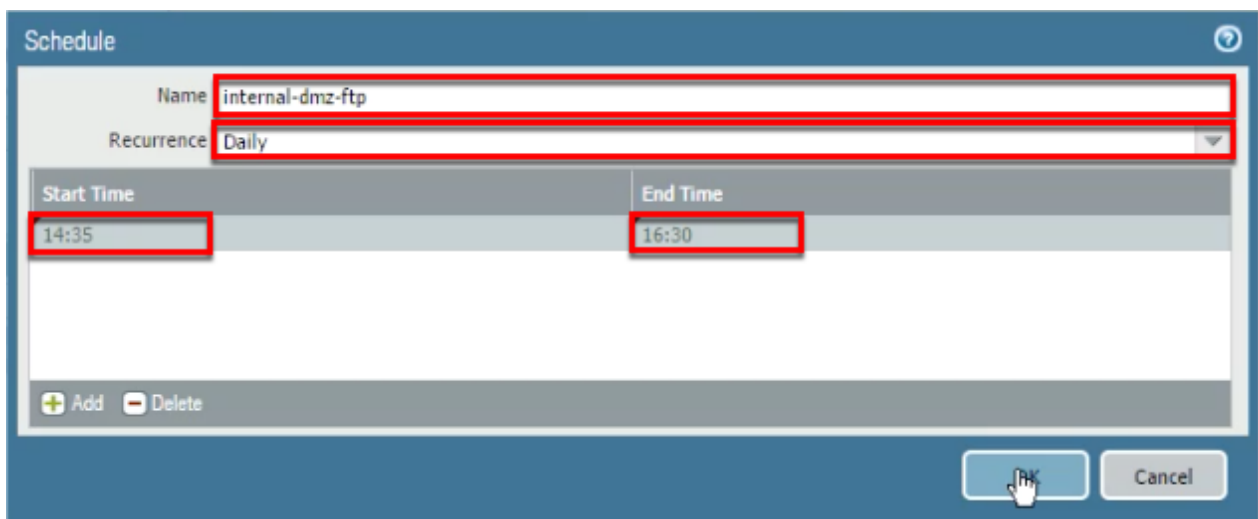
10. Locate the **Schedule** drop-down list and select *New Schedule*:



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:

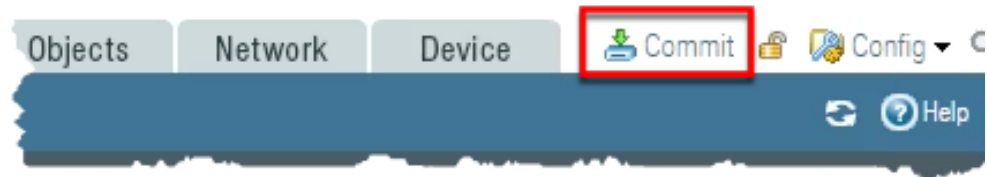
Parameter	Value
Name	internal-dmz-ftp
Recurrence	Daily
Start Time	5 minutes from the time annotated in Step 2.
End time	2 hours from the current firewall time.



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.



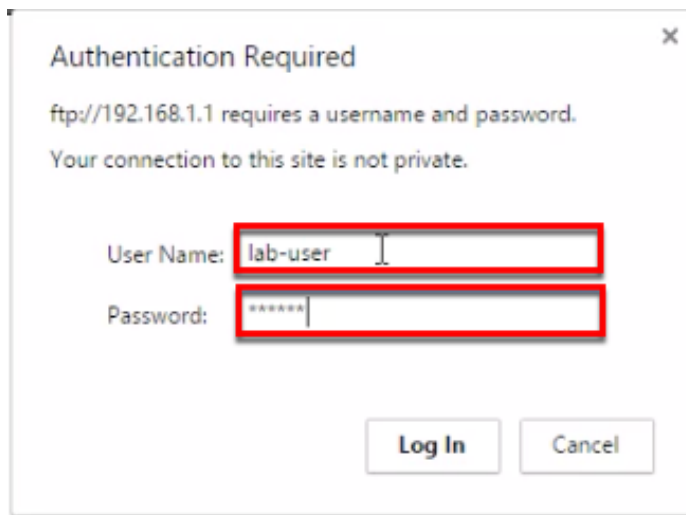
### 3.8 Test the Connection

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`.



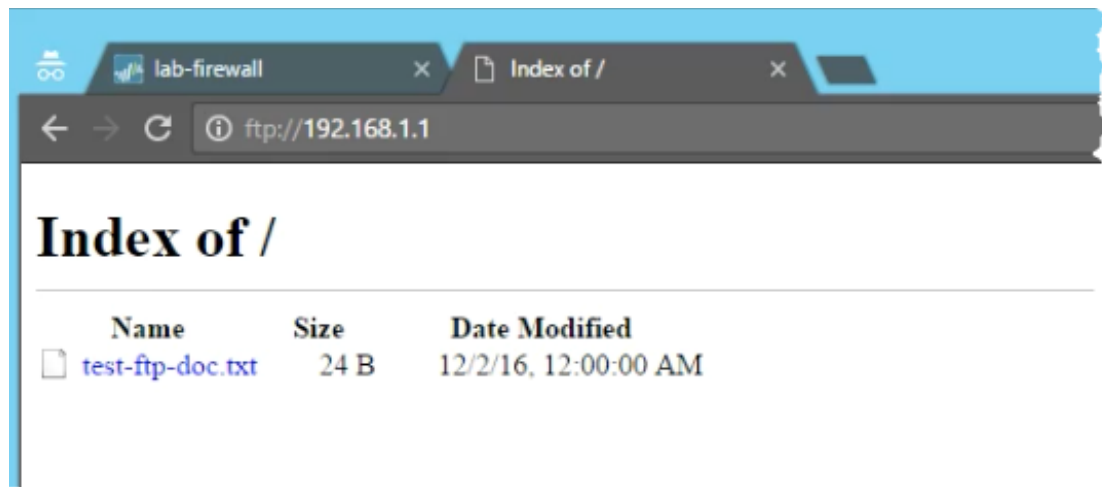
3. At the prompt for login information, enter the following:

Parameter	Value
User Name	lab-user
Password	paloalto



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:



5. In the WebUI select **Monitor > Logs > 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.