PAN-OS 7.0 FIREWALL ESSENTIALS LAB SERIES

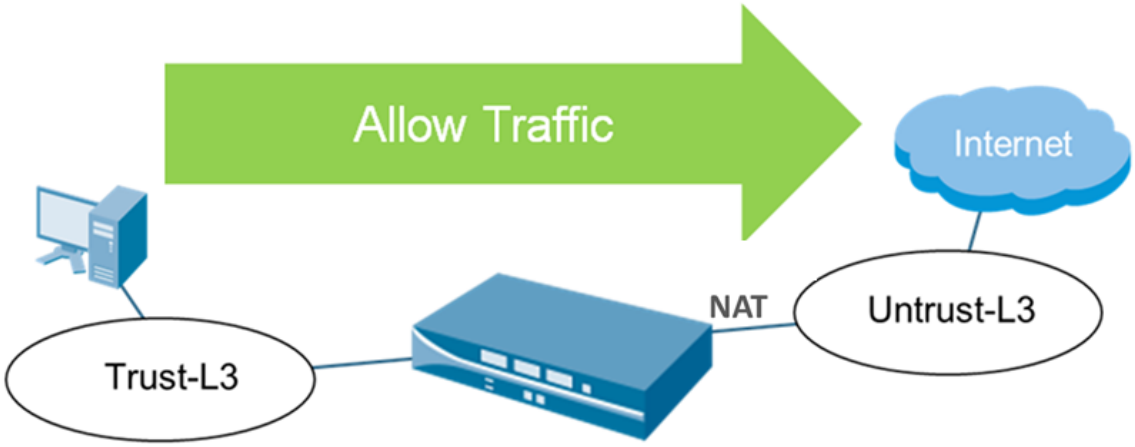
Lab 3: NAT and Security Policies

Document Version: 2016-04-19

Contents

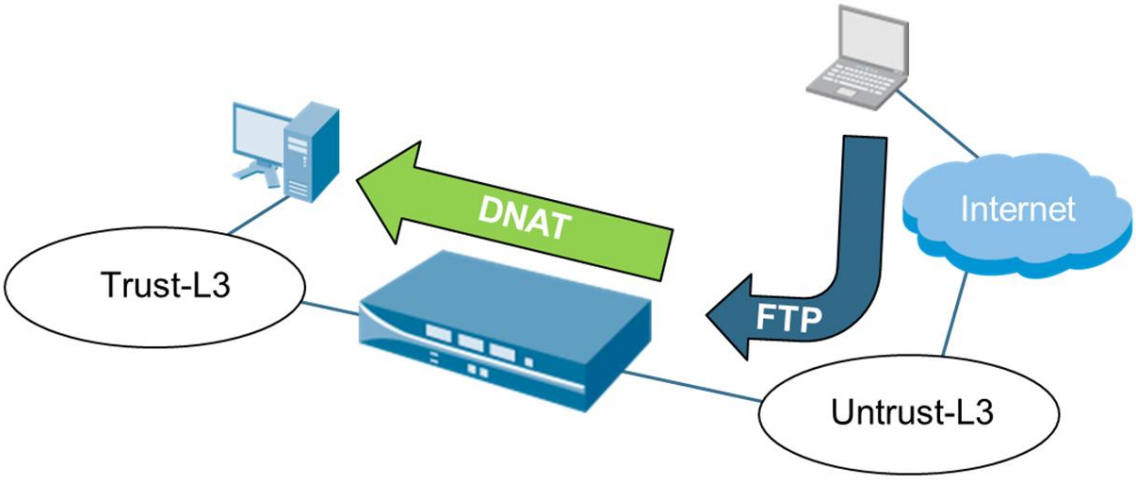
Introduction

Scenario 1



At this point, the firewall is configured but is unable to pass traffic between zones. NAT and Security Policies must be defined before traffic will flow between zones. In this lab, you will create a Source NAT Policy using the Untrust-L3 IP address as the source address for all outgoing traffic. Then you will create a Security Policy to allow traffic from the Trust-L3 Zone to the Untrust-L3 Zone, so that your workstation can access the outside world.

Scenario 2



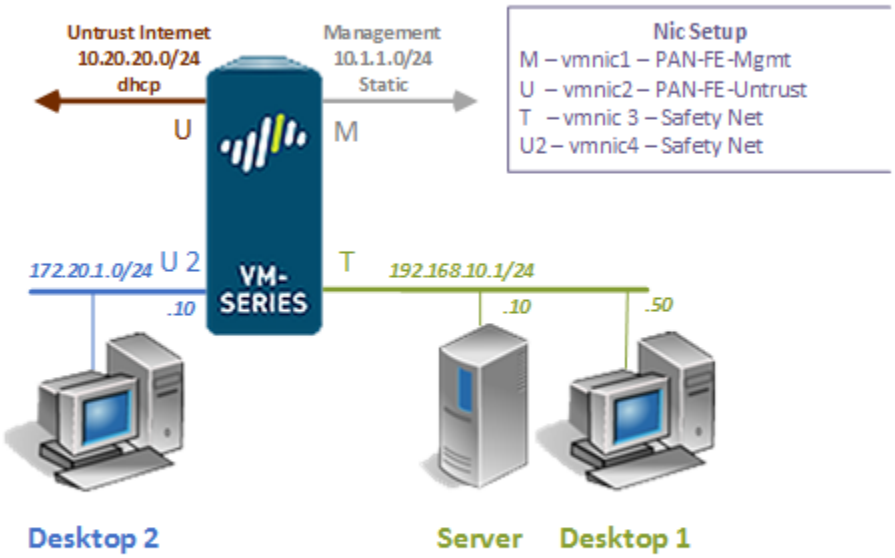
You need to allow access to the web server from outside resources. You also need to allow SSH access to the server for on-call personal remotely. Configure the firewall to accept Web and SSH traffic on its publicly facing interface then redirect the traffic to the server using Destination NAT. From Desktop 2, launch a web browser and terminal window to access the server via the web and SSH and connect to the Untrust2-L3.

Objective

In this lab, you will be utilizing Palo Alto technology to perform the following tasks:

1. Create a Source NAT policy
2. Create a Security Policy to allow connectivity from the Trust-L3 to the Untrust-L3 zone
3. Configure destination NAT to allow SSH and Web traffic to the internal server

Pod 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)
Ubuntu Desktop 1	192.168.10.50	sysadmin	Train1ng$
Ubuntu Server	192.168.10.10	sysadmin	Train1ng$
Ubuntu Desktop 2	172.30.1.10	sysadmin	Train1ng$
Palo Alto Firewall	192.168.10.1 172.30.1.1	admin	paloalto

1 Create a Source NAT Policy

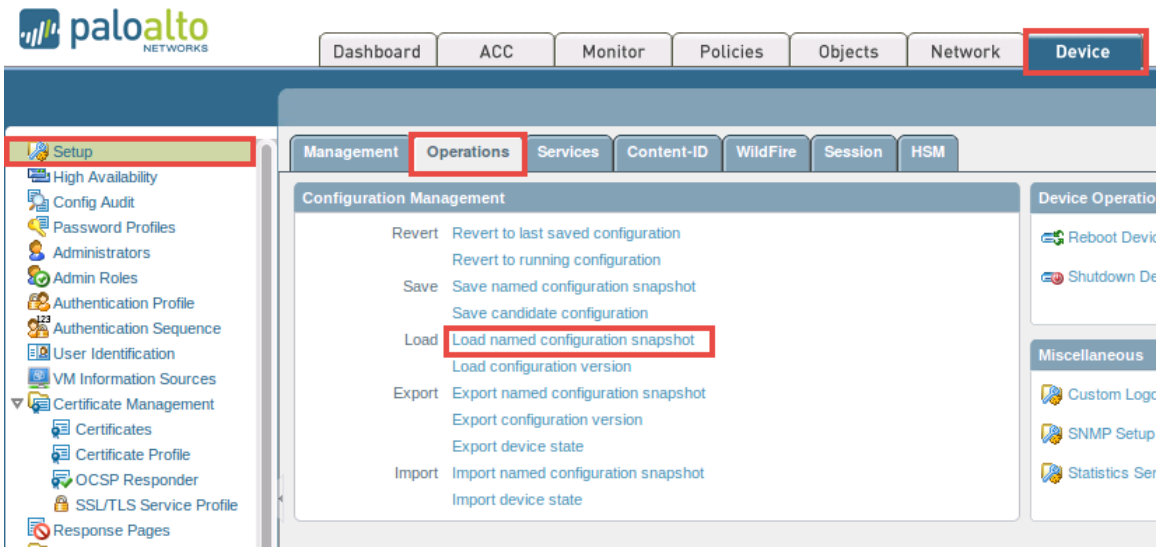
1. Click on the **Desktop 1** graphic found on the *topology page*.
2. Login using **`sysadmin`** as the *username* and **`Train1ng$`** as the *password*. Click **Log In**.
3. Double-click on the **Firefox Web Browser** icon located on the *Desktop*.

4. In the address field, type **`https://192.168.10.1`** and press **Enter**.

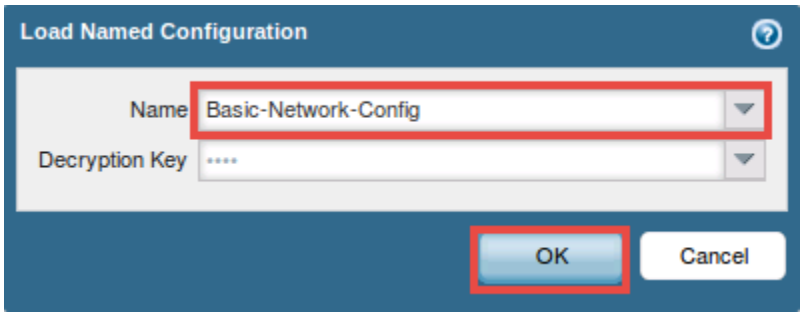
> If you experience the "*Unable to connect*" message while attempting to connect to the specified IP above, please wait an additional 3-5 minutes for the PA VM to fully initialize and refresh the page to continue.

5. Login with the *username* **`admin`** and *password* **`paloalto`** on the firewall web interface.

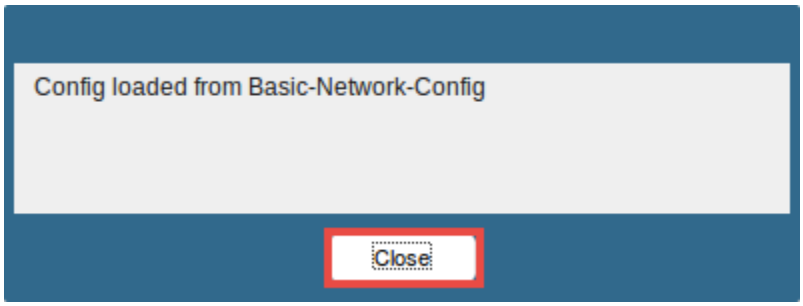
6. Using the *Palo Alto WebUI*, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



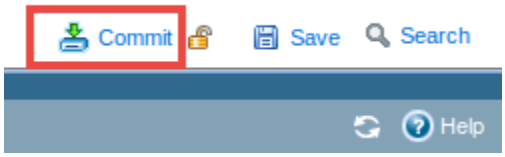
7. In the *Load Named Configuration* window, select **Basic-Network-Config** from the *Name* drop-down box. Click **OK**.



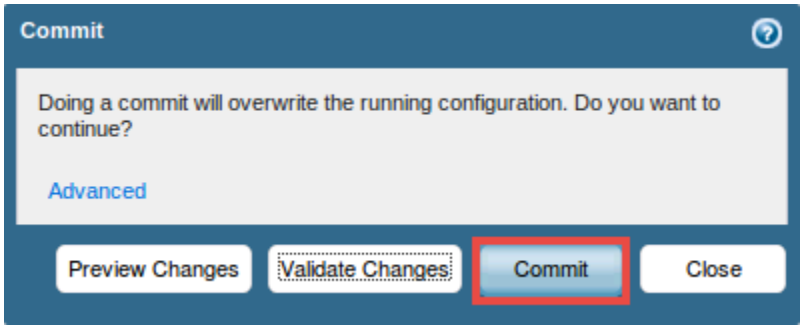
8. Notice the configuration is loaded, click **Close** to continue.



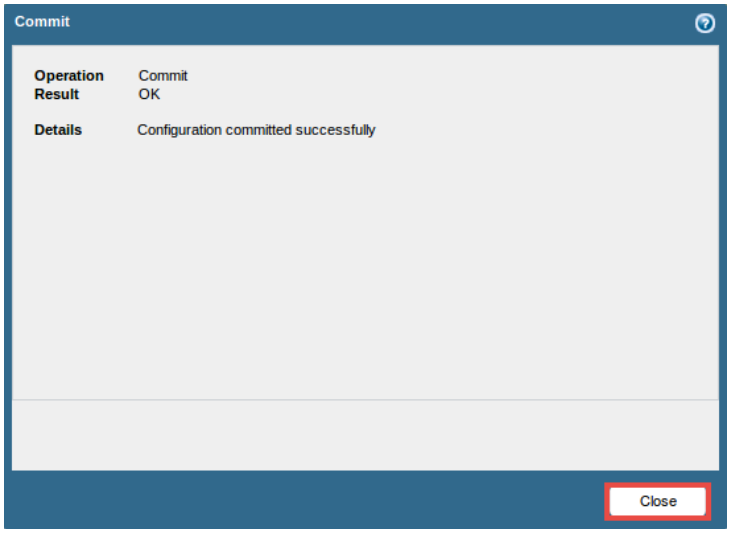
9. Click on the **Commit** link located at the top-right of the *WebUI*.



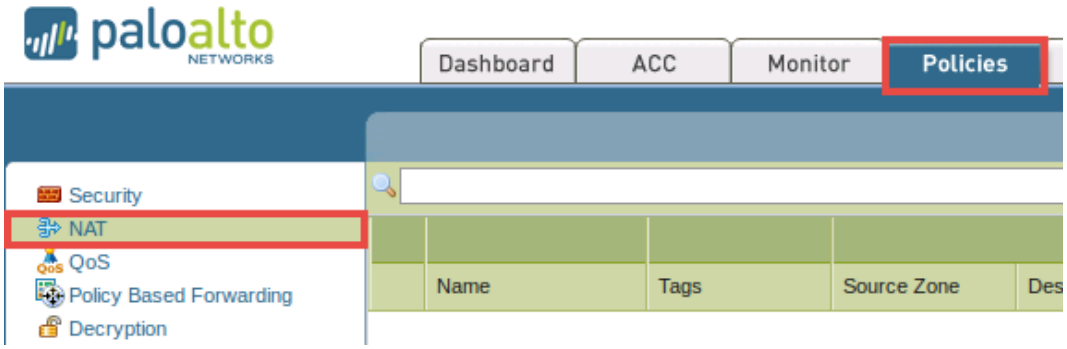
10. In the *Commit* window, click **Commit** to proceed with committing the changes.



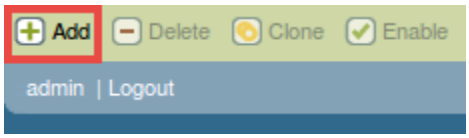
11. Once the operation successfully completes, click **Close** to continue.



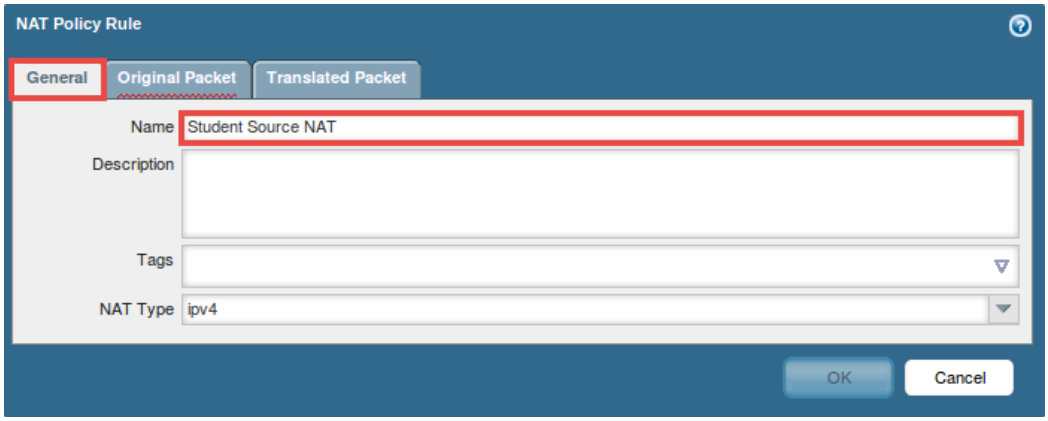
12. Using the *WebUI*, navigate to **Policies > NAT**.



13. Click **Add**, located towards the bottom of the window, to define a new source NAT Policy.

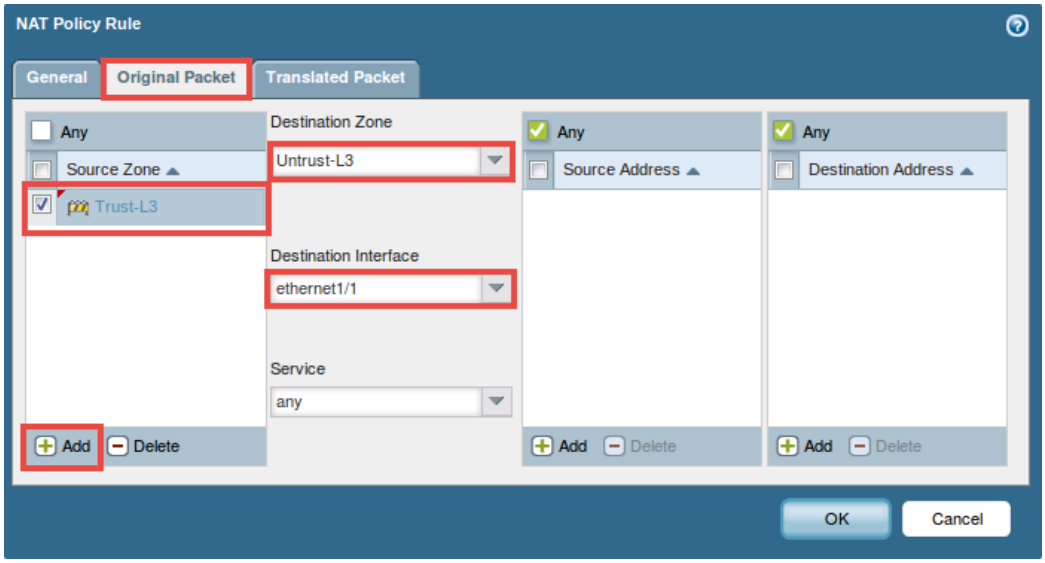


14. In the *NAT Policy Rule* window, verify that the **General** tab is selected and enter **`Student Source NAT`** into the *Name* field.



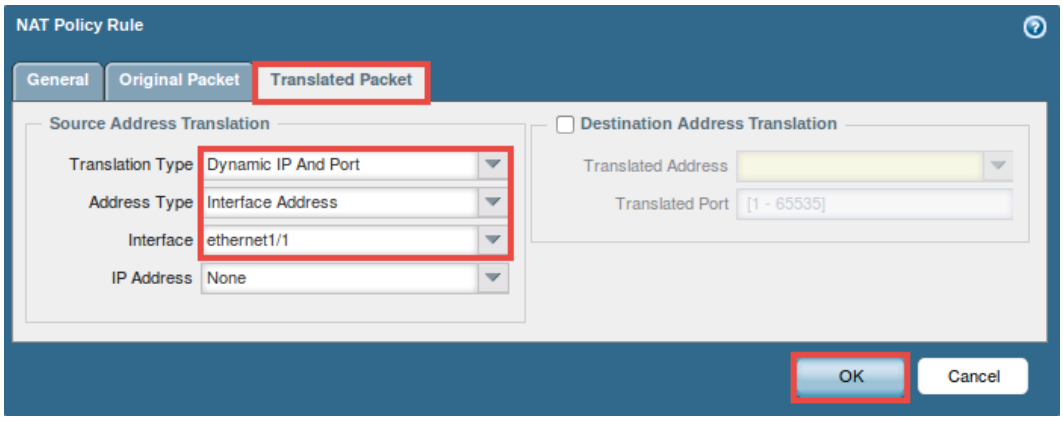
15. Click on the **Original Packet** tab and make the necessary configurations using the information from the table below.

Field	Data/Selection
Source Zone	Click **Add** and select **Trust-L3**
Destination Zone	Select **Untrust-L3**
Destination Interface	Select **ethernet1/1**



16. Click on the **Translated Packet** tab and make the necessary configurations using the information from the table below. Notice that you cannot select an IP address. This is because ethernet1/1 is configured for dhcp and therefore the policy will retrieve the current IP address from the interface when the NAT policy is applied.

Field	Data/Selection
Translation Type	Select **Dynamic IP and Port**
Address Type	Select **Interface Address**
Interface	Select **ethernet1/1**



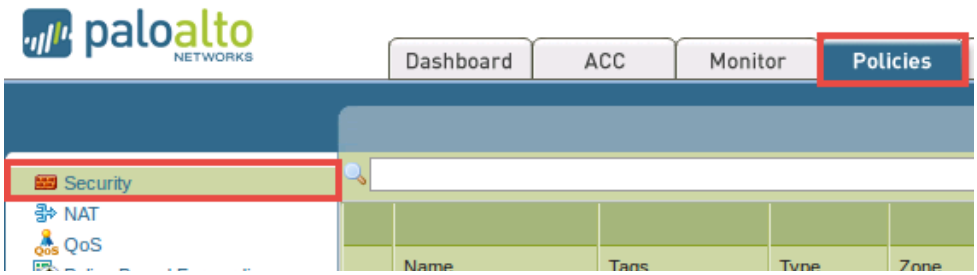
17. Click **OK** to continue.

The Internet will not be accessible just yet. A Security Policy will need to be configured to allow traffic to flow between zones.

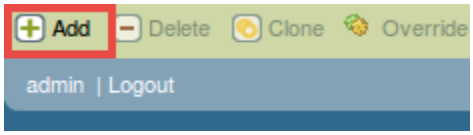
18. Leave the *WebUI* opened to continue with the next task.

2 Create the "Allow All Out" Policy

1. Using the WebUI, navigate to **Policies > Security**.

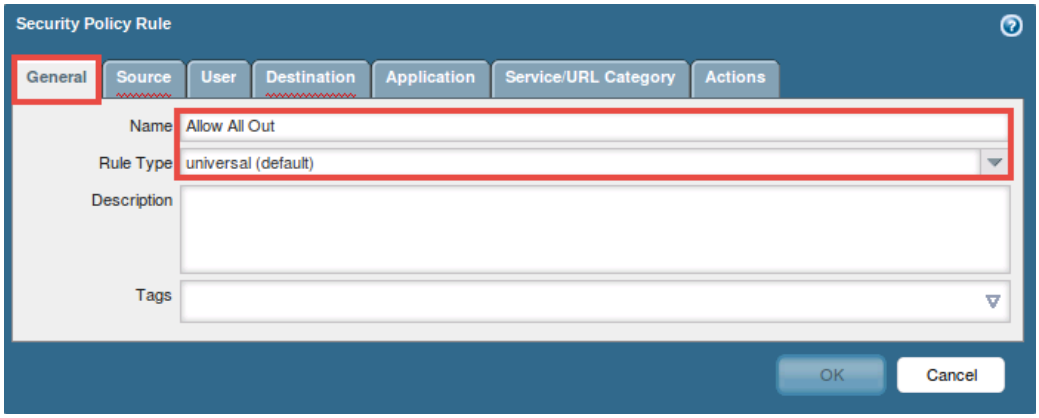


2. Click on **Add**, located near the bottom of the window, to define a *Security Policy*.



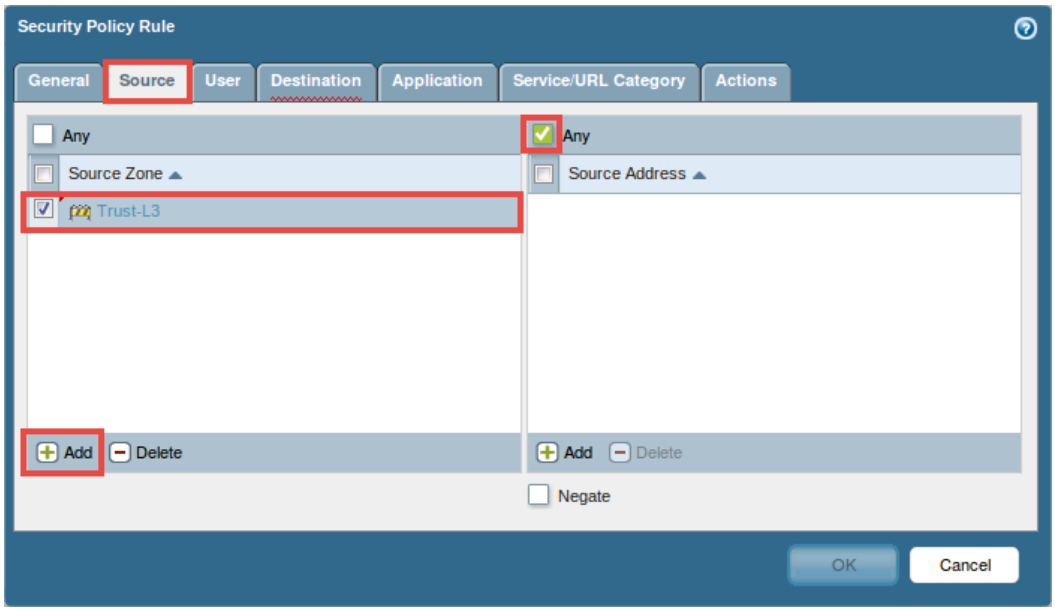
3. In the *Security Policy Rule* window, select the **General** tab and make the necessary configurations using the information from the table below.

Field	Data/Selection
Name	Enter **Allow All Out**
Rule Type	universal (default)



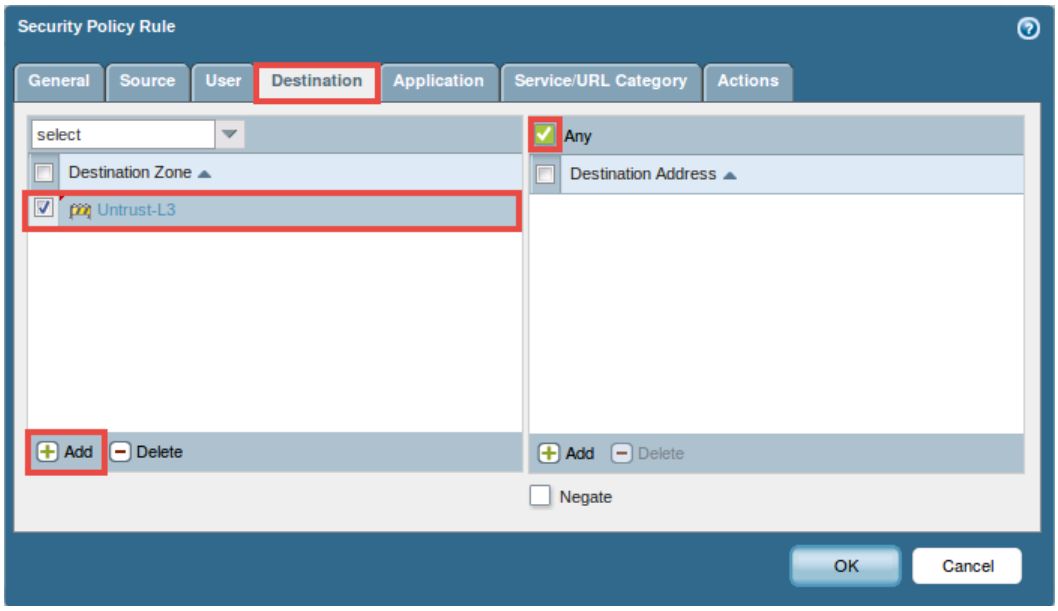
4. In the *Security Policy Rule* window, select the **Source** tab and make the necessary configurations using the information from the table below.

Field	Data/Selection
Source Zone	Click **Add** and select **Trust-L3**
Source Address	Select **Any**

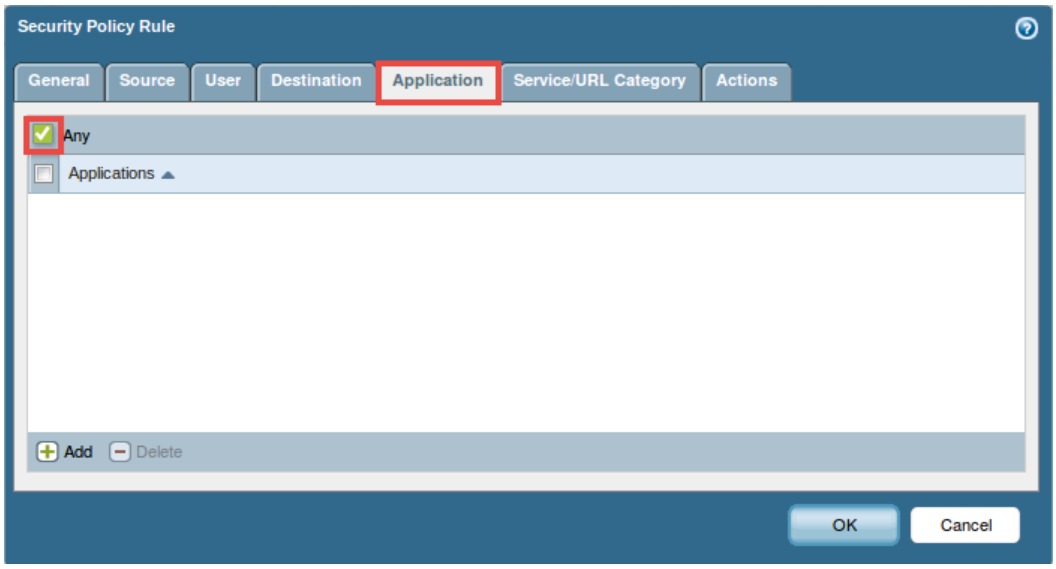


5. In the *Security Policy Rule* window, select the **Destination** tab and make the necessary configurations using the information from the table below.

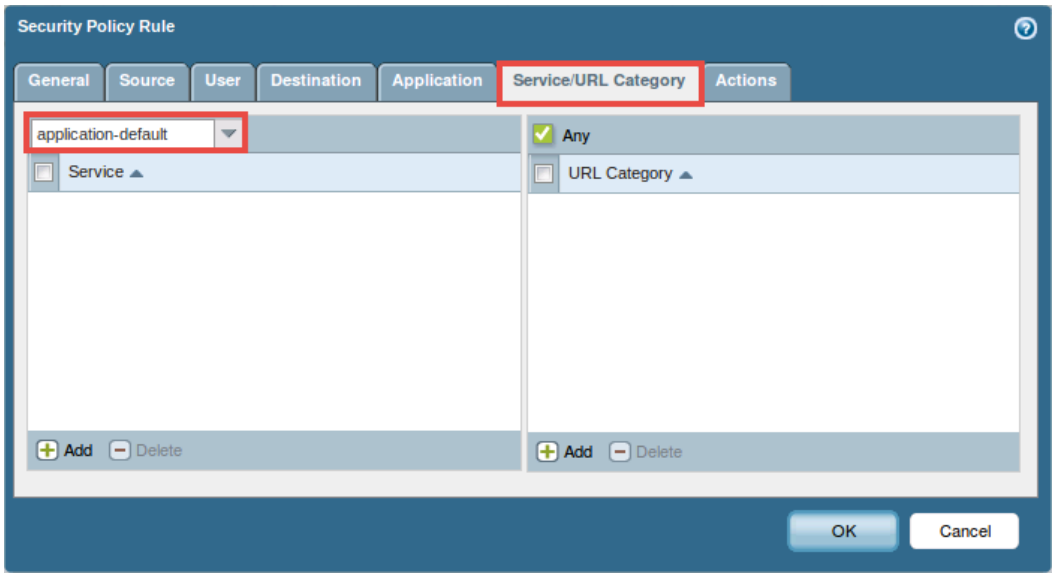
Field	Data/Selection
Destination Zone	Click **Add** and select **Untrust-L3**
Destination Address	Select **Any**



6. In the *Security Policy Rule* window, select the **Application** tab and make sure **Any** is checked

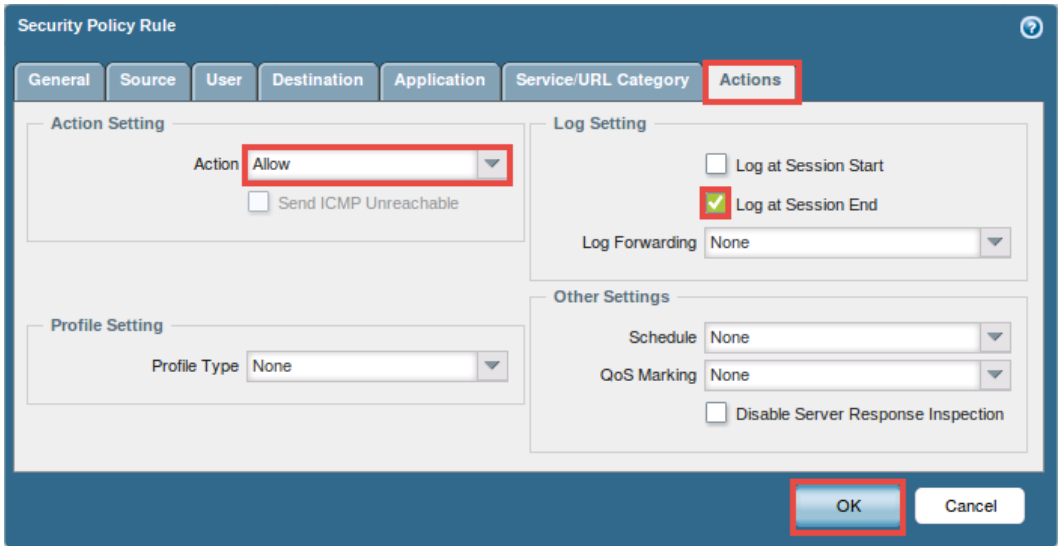


7. In the *Security Policy Rule* window, select the **Service/URL Category** tab and make sure **application-default** is selected from the drop-down menu.

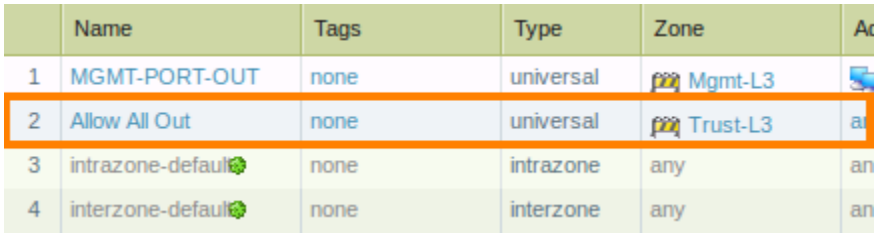


8. In the *Security Policy Rule* window, select the **Actions** tab and make the necessary configurations using the information from the table below.

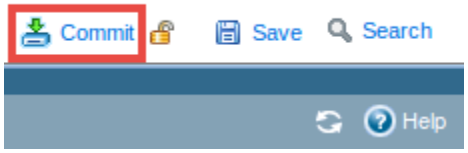
Field	Data/Selection
Action Setting	Select **Allow**
Log Setting	Check **Log at Session End**



9. Click **OK** to save changes and to close the *Security Policy Configuration* window.
10. Verify that the new *Allow All Out* security policy appears in the list.



11. Click **Commit**, located near the top-right.



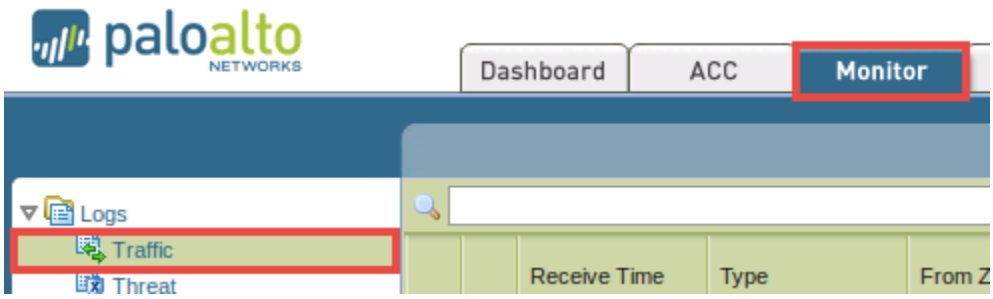
12. In the *Commit* window, click the **Commit** button to continue.
13. Once the commit process successfully completes, click the **Close** button.
14. Leave the *Firefox* web browser opened to continue with the next task.

3 Verify Internet Connectivity

1. Using the *Firefox* web browser, open a **new tab**.
2. In the new tab, type `www.google.com` into the address bar followed by pressing the **Enter** key.

Notice that an Internet connection is available.

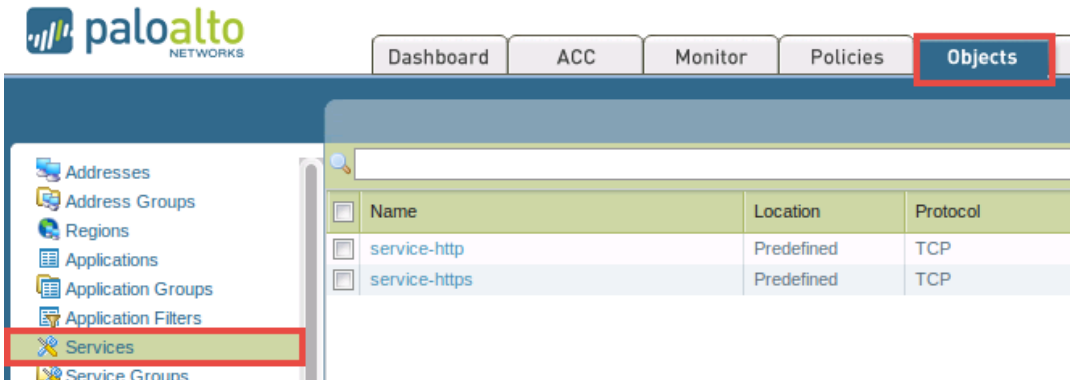
3. Close the **second tab**.
4. Using the *WebUI*, navigate to **Monitor > Traffic** to view traffic logs. Here, you can see what traffic has passed through the *Allow All Out* policy.



5. Leave the *WebUI* opened to continue with the next task.

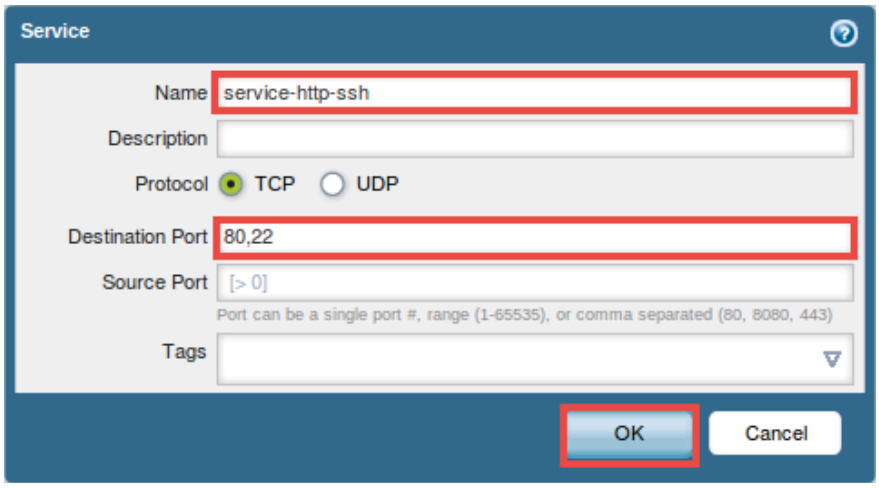
4 Create a Destination NAT Policy

1. Using the *WebUI*, navigate to **Objects > Services**.



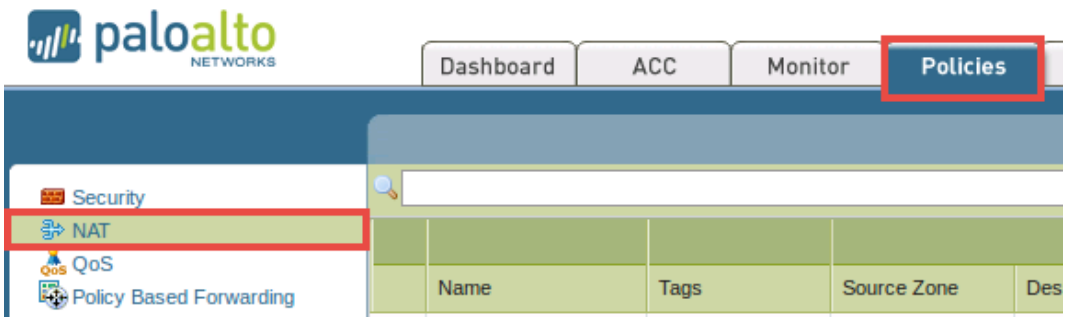
2. Click **Add**, located near the bottom of the window, to add a new service.
3. In the *Service* window, use the information from the table below to configure a new service.

Field	Data/Selection
Name	Enter **service-http-ssh**
Destination Port	Enter **80,22**

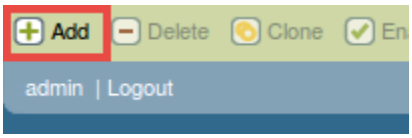


4. Click **OK** to save changes.
5. Verify that the *service-http-ssh* service appears in the list.

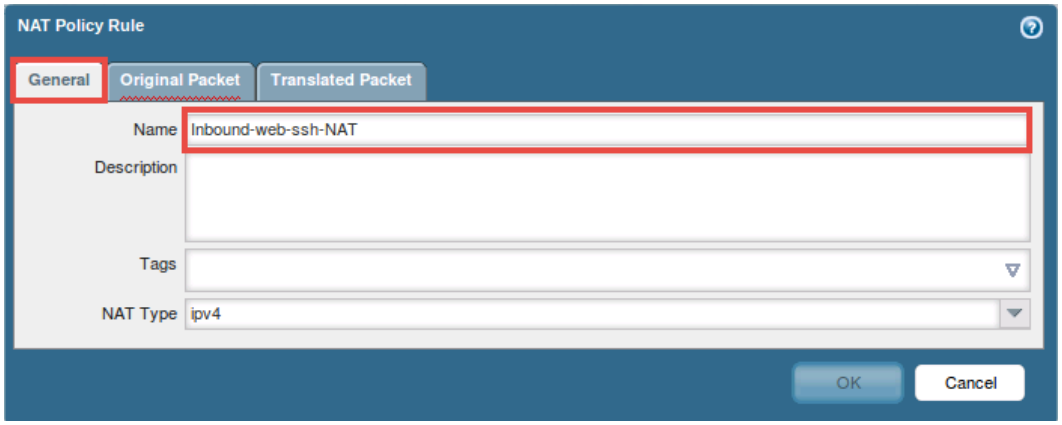
6. Navigate to **Policies > NAT**.



7. Click **Add**, located near the bottom of the window, to define a new destination NAT policy.

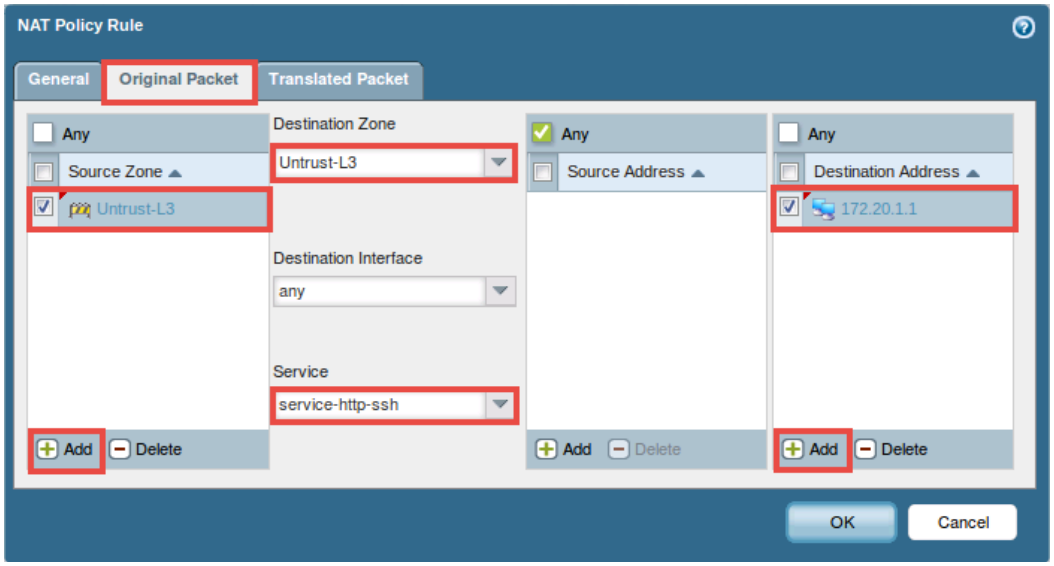


8. In the *NAT Policy Rule* window, click on the **General** tab and enter **`Inbound-web-ssh-NAT`** in the *Name* field.



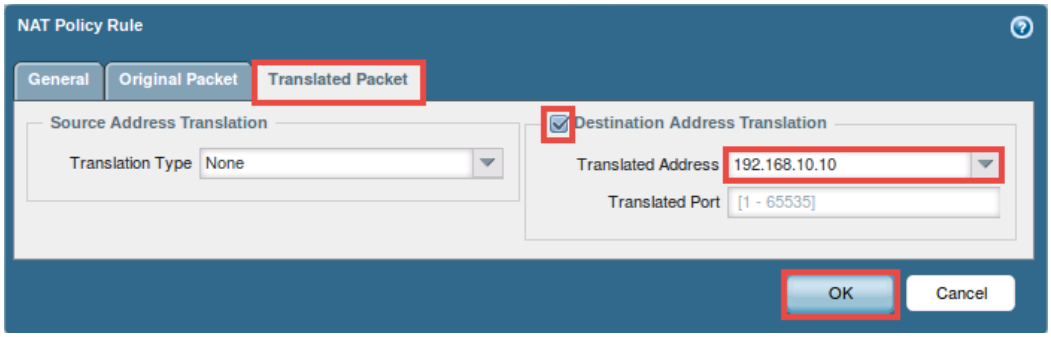
9. In the *NAT Policy Rule* window, click on the **Original Packet** tab and use the information in the table below to make the necessary configurations.

Field	Data/Selection
Source Zone	Click **Add** and select **Untrust-L3**
Destination Zone	Select **Untrust-L3**
Service	Select **service-http-ssh**
Destination Address	Click **Add** and enter **172.20.1.1**



10. In the *NAT Policy Rule* window, click on the **Translated Packet** tab and use the information in the table below to make the necessary configurations.

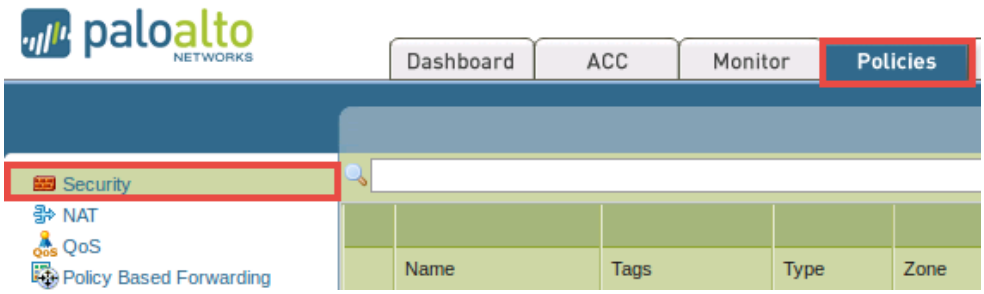
Field	Data/Selection
Destination Address Translation	Check the box
Translated Address	Enter **192.168.10.10**



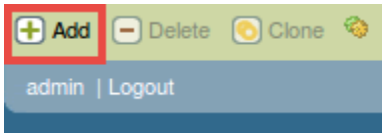
11. Click **OK** to save changes.
12. Verify that the new NAT policy appears in the list.
13. Leave the *WebUI* opened to continue with the next task.

5 Create a Security Policy Rule

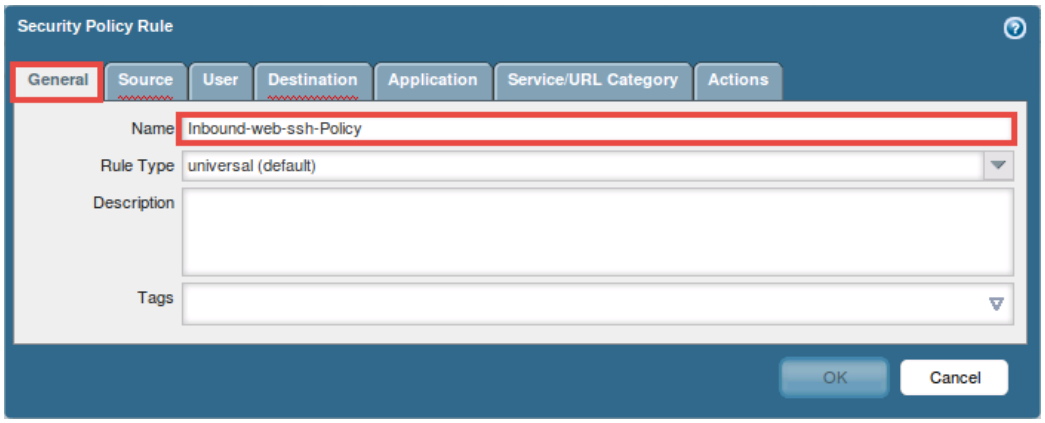
1. Using the *WebUI*, navigate to **Policies > Security**.



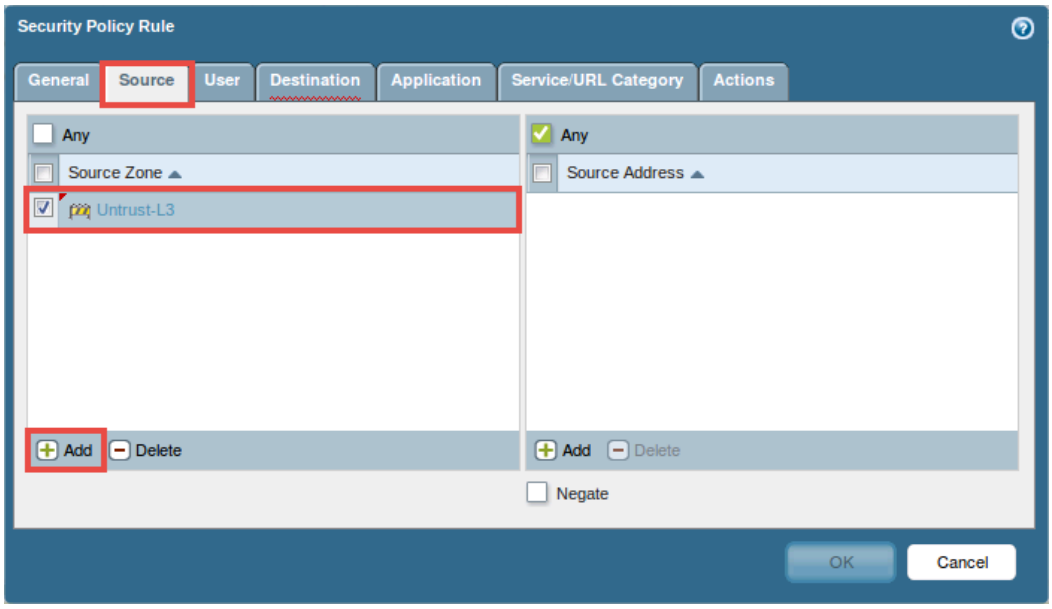
2. Click **Add**, located near the bottom of the window, to define a new security policy rule.



3. In the *Security Policy Rule* window, click on the **General** tab and enter **`Inbound-web-ssh-Policy`** in the *Name* text field.

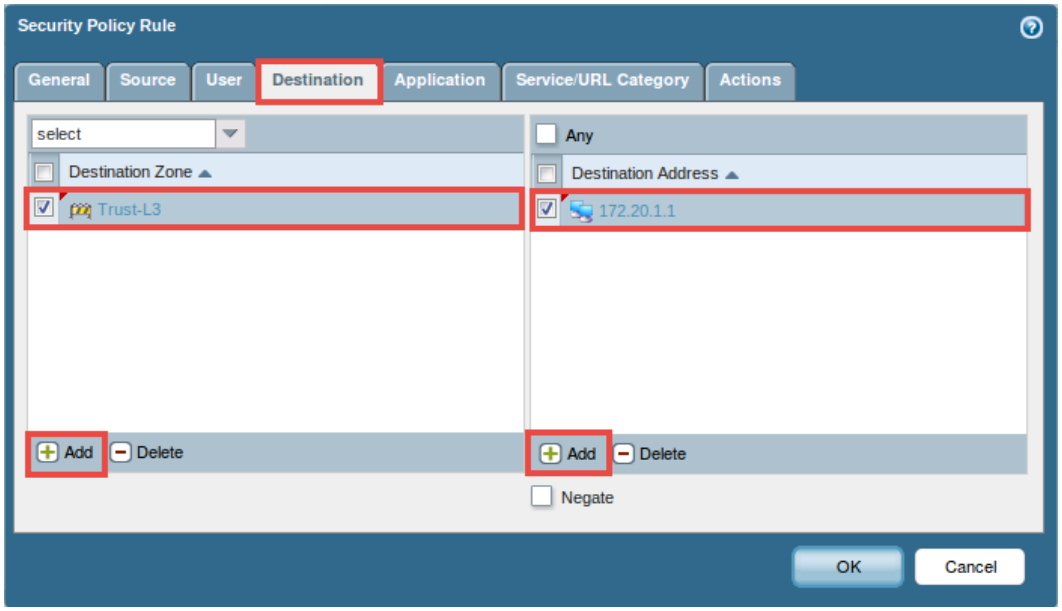


4. In the *Security Policy Rule* window, click on the **Source** tab and click **Add** for *Source Zone*. Select **Untrust-L3**.



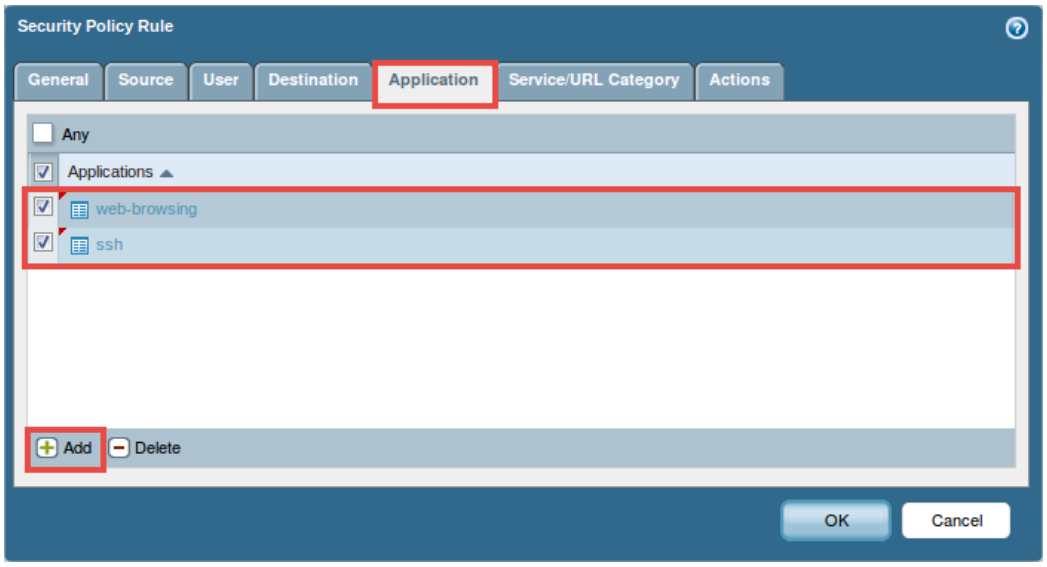
5. In the *Security Policy Rule* window, click on the **Destination** tab and use the information in the table below to make the necessary configurations.

Field	Data/Selection
Destination Zone	Click **Add** and select **Trust-L3**
Destination Address	Click **Add** and enter **172.20.1.1**

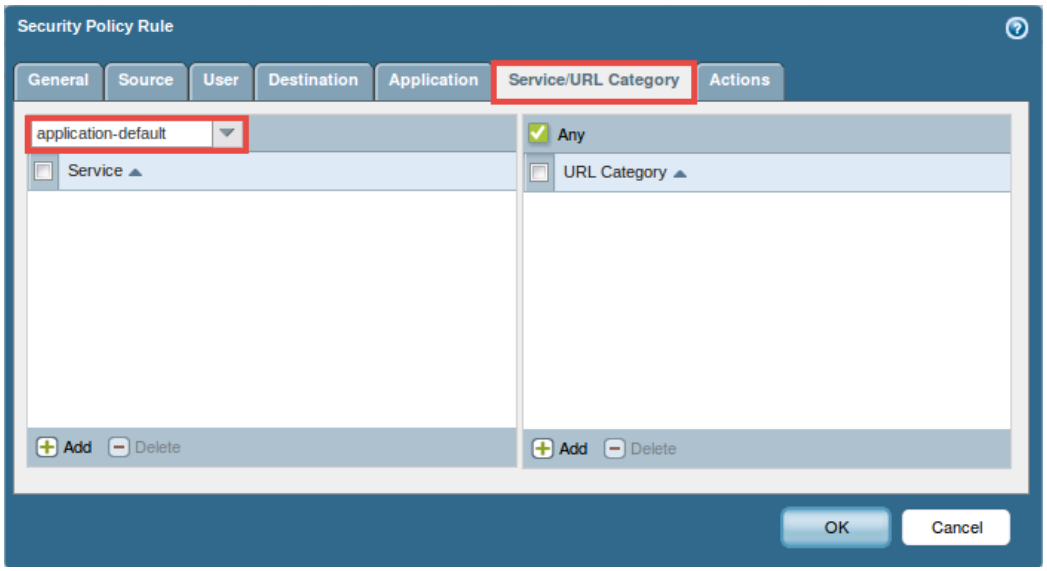


6. In the *Security Policy Rule* window, click on the **Application** tab and use the information in the table below to make the necessary configurations.

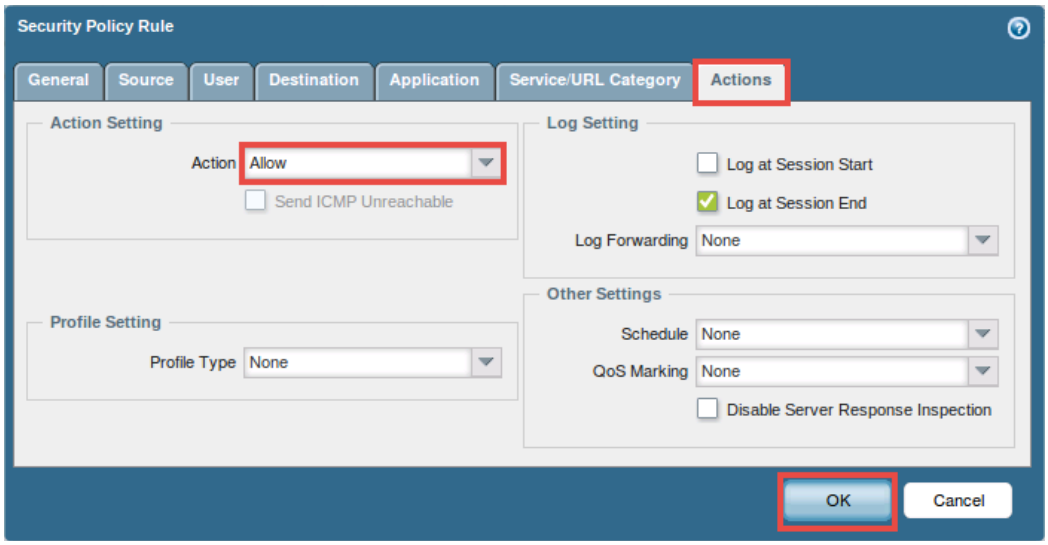
Field	Data/Selection
Applications	Click **Add** and select **web-browsing** Click **Add** and select **ssh**



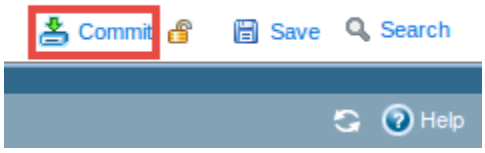
7. In the *Security Policy Rule* window, click on the **Service/URL Category** tab and select **application-default** from the drop-down menu.



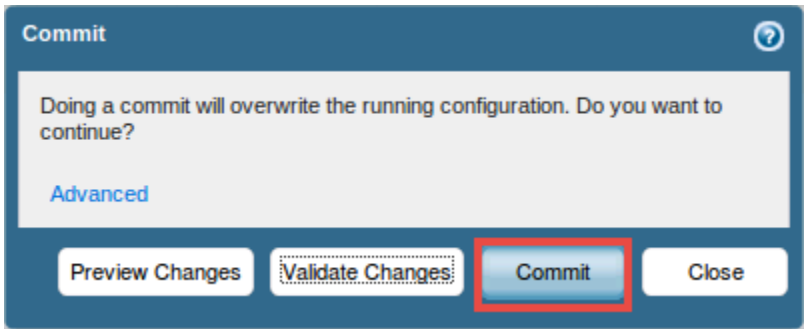
8. In the *Security Policy Rule* window, click on the **Actions** tab and select **Allow** for the *Action Setting*.



9. Click **OK** to save changes and to close the *Security Policy Rule* configuration window.
10. Verify that the new *Inbound-web-ssh-Policy* appears in the list.
11. Click on the **Commit** link located at the top-right of the *WebUI*.



12. In the *Commit* window, click **Commit**.



13. After the commit process completes successfully, click the **Close** button.

6 Test the Connection

1. Navigate to the **topology** page and click on the **Desktop 2** graphic.
2. Login using **`sysadmin`** as the *username* and **`Train1ng$`** as the *password*. Click **Log In**.
3. Click on the **LXTerminal** icon located on the bottom toolbar pane.

4. Using the terminal, type the command below followed by pressing the **Enter** key.

```
ssh 172.20.1.1
```

5. If asked to continue using the specified fingerprint, type **`yes`** followed by pressing the **Enter** key.

```
sysadmin@lubuntu:~$ ssh 172.20.1.1
The authenticity of host '172.20.1.1 (172.20.1.1)' can't be established.
ECDSA key fingerprint is 35:69:94:72:c5:75:7a:23:0c:a3:03:af:8e:9c:9f:f0.
Are you sure you want to continue connecting (yes/no)? yes
```

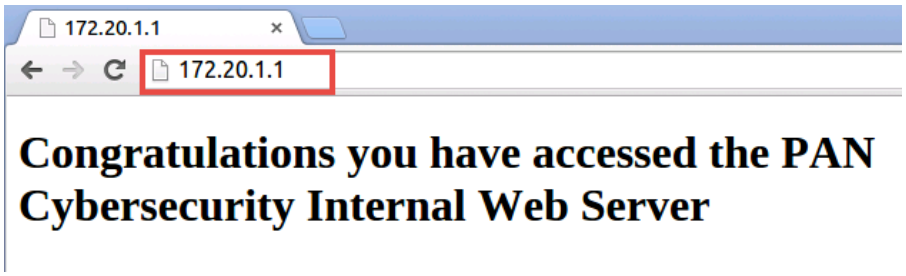
6. When prompted for a password, type **`Train1ng$`** followed by pressing the **Enter** key.

```
sysadmin@lubuntu:~$ ssh 172.20.1.1
sysadmin@172.20.1.1's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Fri Mar 18 13:54:45 EDT 2016

  System load:  0.0                Processes:           77
  Usage of /:   10.6% of 15.13GB   Users logged in:     0
  Memory usage: 11%                IP address for eth0: 192.168.10.10
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

205 packages can be updated.
0 updates are security updates.

Last login: Thu Feb 25 12:20:13 2016 from 192.168.10.50
sysadmin@ubuntu:~$
```

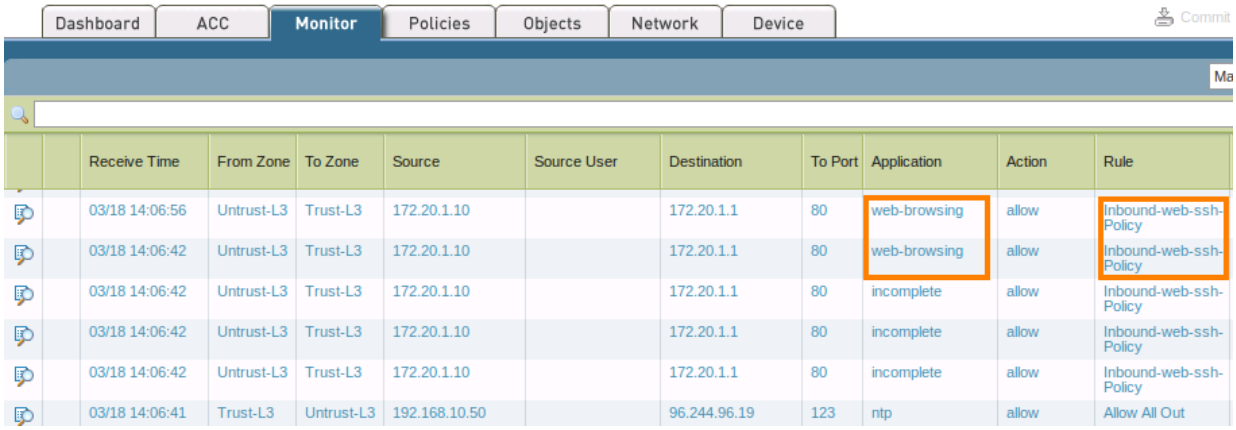
Notice the successful SSH connection.

7. While on the *Desktop 2* VM, open a web browser by clicking on the **Chrome** icon found on the bottom pane.

8. In the *Chrome* browser, type `http://172.20.1.1` into the address field. Press **Enter**.



9. Upon successfully loading of the web page on the internal web server, navigate back to the **Desktop 1** PC viewer.
10. Using the *WebUI*, navigate to **Monitor > Logs > Traffic** and find the entries where application *web-browsing* has been allowed by rule *Inbound-web-ssh-Policy*.



Receive Time	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
03/18 14:06:56	Untrust-L3	Trust-L3	172.20.1.10		172.20.1.1	80	web-browsing	allow	Inbound-web-ssh-Policy
03/18 14:06:42	Untrust-L3	Trust-L3	172.20.1.10		172.20.1.1	80	web-browsing	allow	Inbound-web-ssh-Policy
03/18 14:06:42	Untrust-L3	Trust-L3	172.20.1.10		172.20.1.1	80	incomplete	allow	Inbound-web-ssh-Policy
03/18 14:06:42	Untrust-L3	Trust-L3	172.20.1.10		172.20.1.1	80	incomplete	allow	Inbound-web-ssh-Policy
03/18 14:06:42	Untrust-L3	Trust-L3	172.20.1.10		172.20.1.1	80	incomplete	allow	Inbound-web-ssh-Policy
03/18 14:06:41	Trust-L3	Untrust-L3	192.168.10.50		96.244.96.19	123	ntp	allow	Allow All Out

Make sure that the filter is cleared so that all traffic results appear in the list.

11. Close both **Desktop 1 & 2** PC viewers.

