PAN8 CYBERSECURITY ESSENTIALS

Lab 1: Creating a Zero Trust Environment

Document Version: 2018-07-02

Copyright © 2018 Network Development Group, Inc.
www.netdevgroup.com

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

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Lab: Creating a Zero Trust Environment 6
1.0 Load Lab Configuration 6
1.1 Create Zones and Associate the Zones to Interfaces 9
1.2 Create a Security Policy Rule 14
1.3 Create a NAT Policy 20
1.4 Commit and Test the Rules and Policies 22

 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

Introduction

In this lab, you will configure the Firewall with three zones: **inside**, **outside**, and **dmz**. Then, you will apply security policies to these zones to ensure all traffic between zones is being monitored by the Firewall.

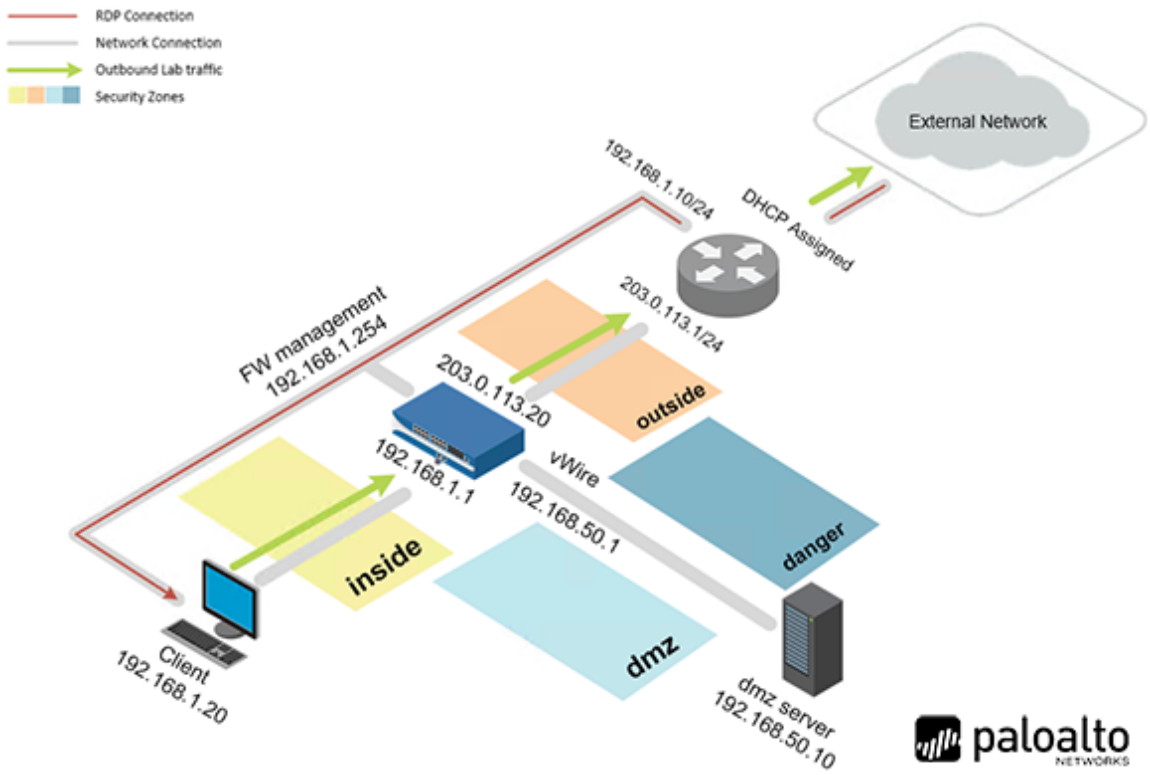
Objective

In this lab, you will perform the following tasks:

- Create Zones and Associate the Zones to Interfaces
- Create a Security Policy Rule
- Create a NAT Policy
- Commit and Test the Rules and Policies

 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

Lab Topology



 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

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	Pal0Alt0
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	admin

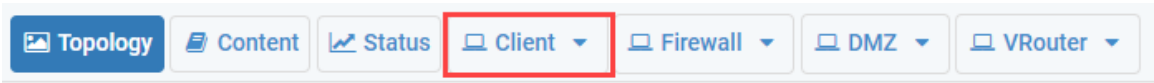
Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

1 Lab: Creating a Zero Trust Environment

1.0 Load Lab Configuration

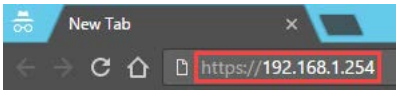
In this section, you will load the Firewall configuration file.

1. Click on the **Client** tab to access the Client machine.

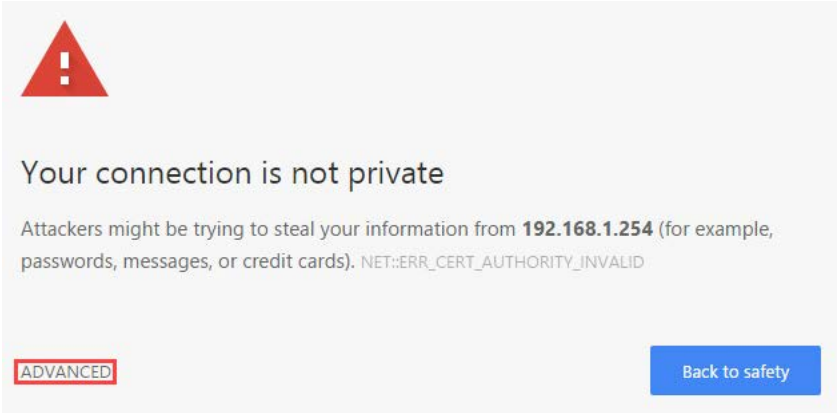


2. Login to the Client machine as username **lab-user**, password **`Pal0Alt0`**.
3. Double-click the **Google Chrome** icon located on the Desktop.

4. In the *Google Chrome* address field, type **https://192.168.1.254** and press **Enter**.



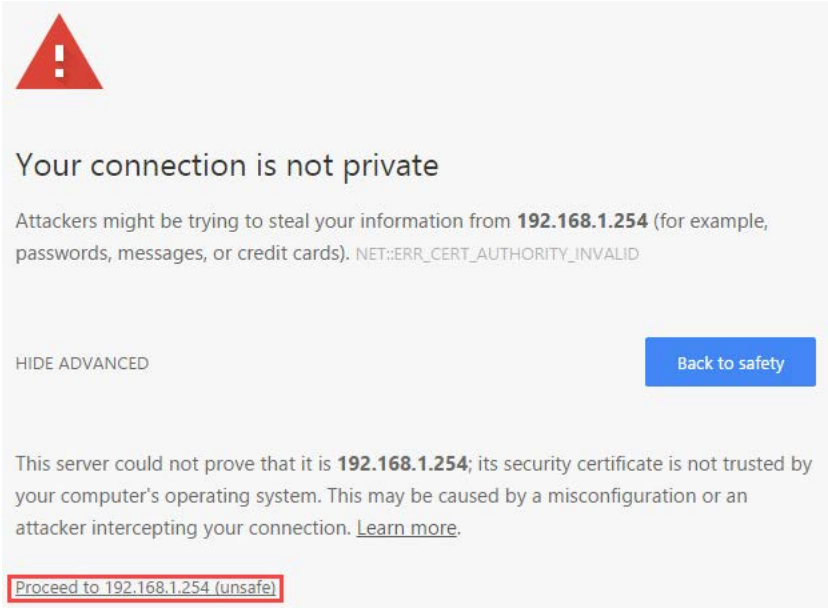
5. You will see a *"Your connection is not private"* message. Click on the **ADVANCED** link.



If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

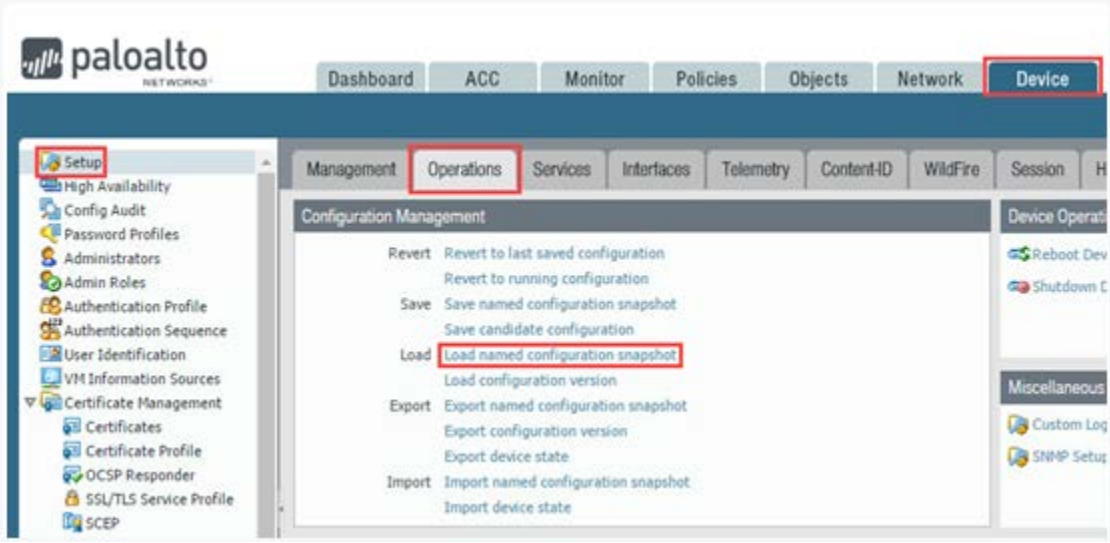
 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

6. Click on **Proceed to 192.168.1.254 (unsafe)**.



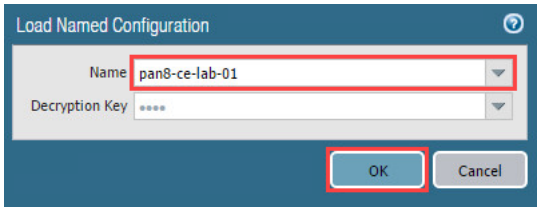
7. Login to the Firewall web interface as username **admin**, password **admin.**

8. Navigate to **Device > Setup > Operations > Load named configuration snapshot**.

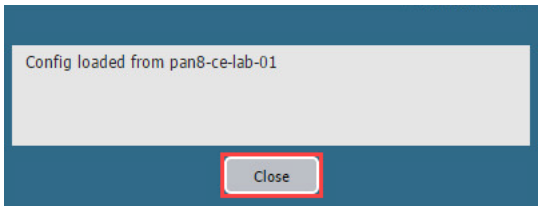


 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

9. In the *Load Named Configuration* window, select **pan8-ce-lab-01** from the *Name* dropdown box and click **OK**.

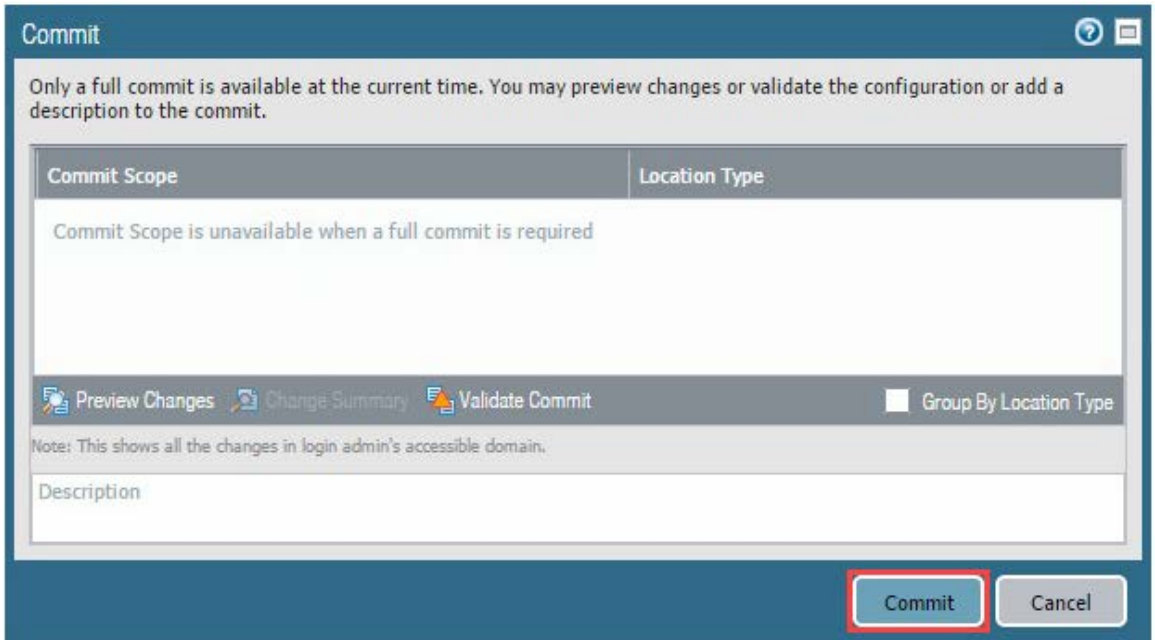


10. A message will confirm the configuration has loaded. Click **Close** to continue.



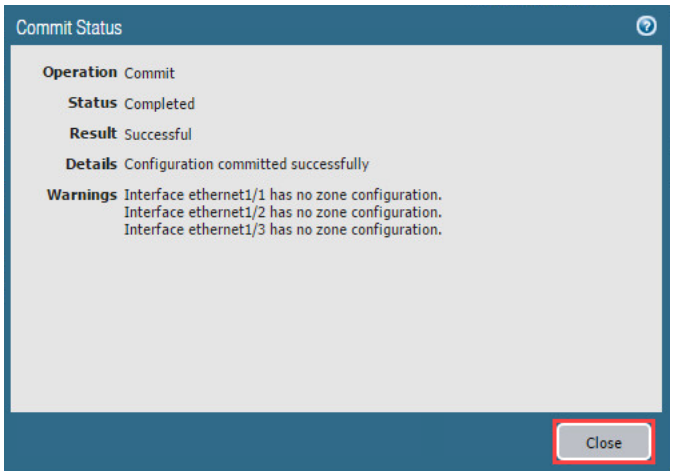
11. Click the **Commit** link located at the top-right of the web interface.

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



 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

13. When the commit operation successfully completes, click **Close** to continue.



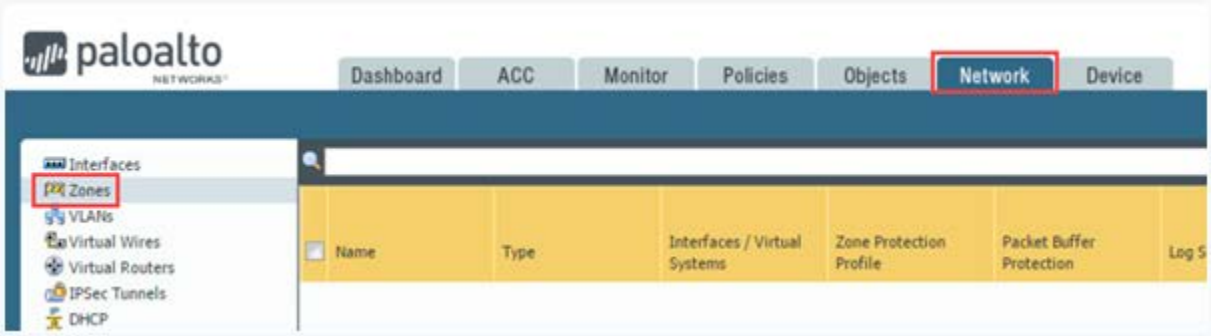
The **Warnings** displayed are normal. You will resolve those during this lab.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

1.1 Create Zones and Associate the Zones to Interfaces

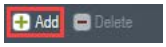
In this section, you will create three basic zones: **inside**, **outside**, and **dmz**. A security zone allows you to segregate traffic in the Firewall so that you can apply security policies later to limit the traffic between zones. Next, you will associate them to the appropriate interfaces.

1. Navigate to **Network > Zones.**

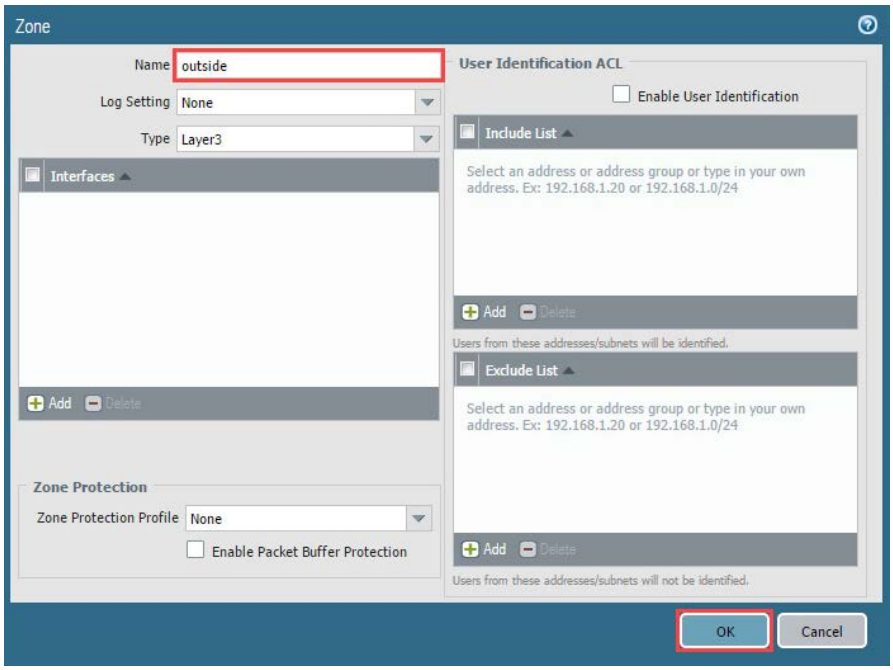


 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

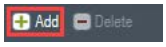
2. Click on the **Add** button at the bottom-left of the center section.



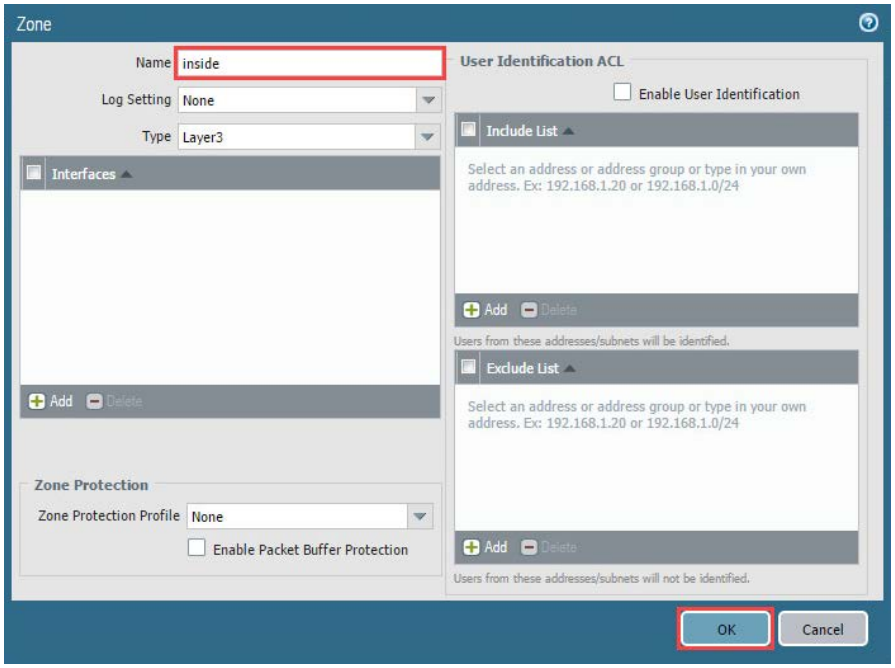
3. In the *Zone* window, type **outside** in the Name field. Then, click the **OK** button.



4. Click on the **Add** button at the bottom-left of the center section.

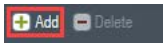


5. In the *Zone* window, type **inside** in the Name field. Then, click the **OK** button.

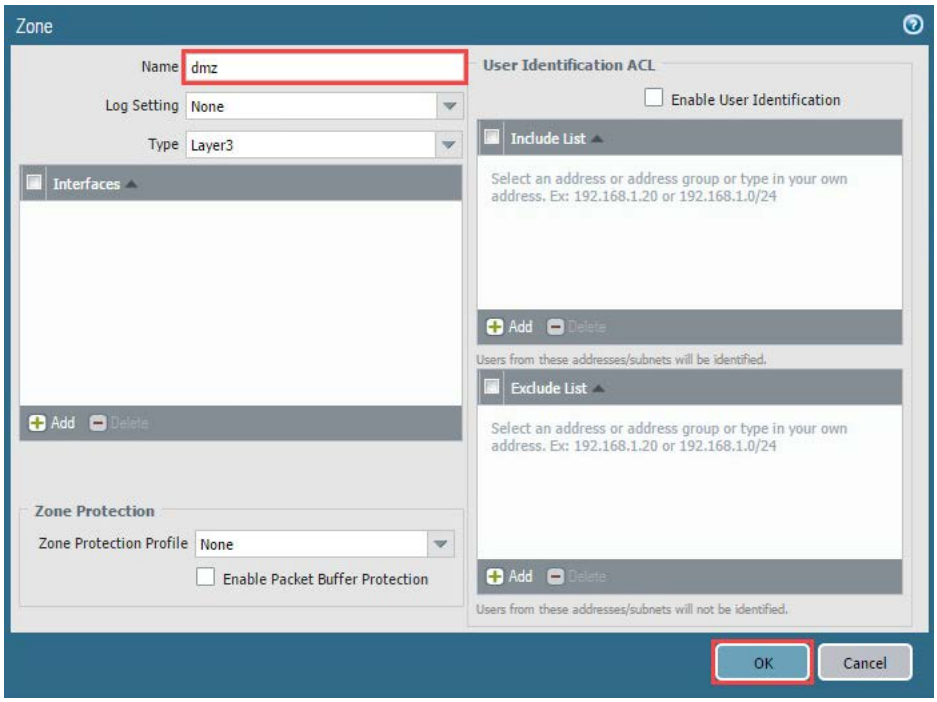


 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

6. Click the **Add** button at the bottom-left of the center section.

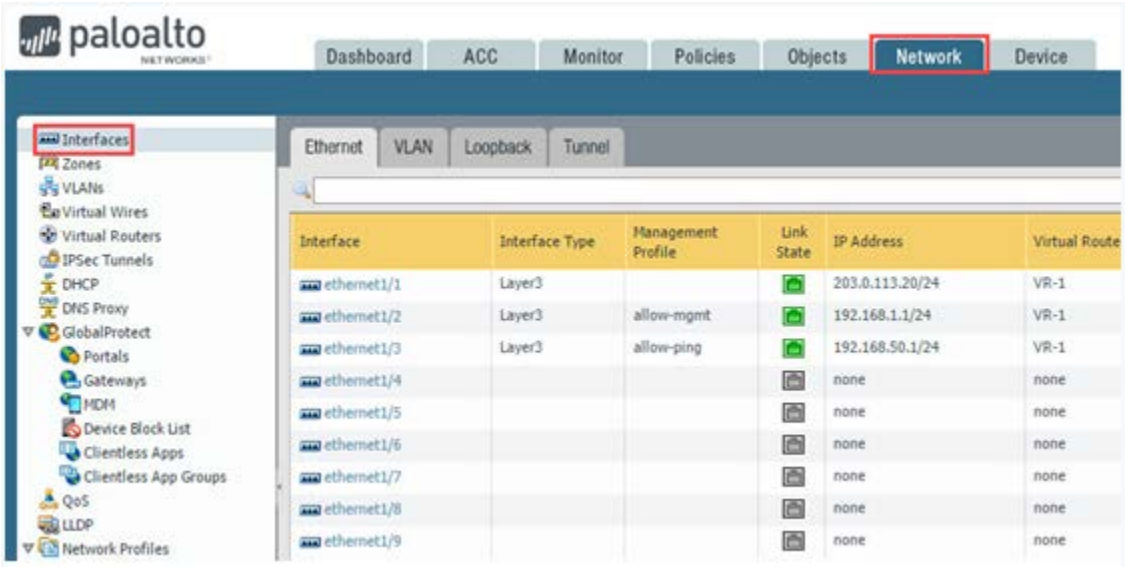


7. In the *Zone* window, type **dmz** in the Name field. Then, click the **OK** button.



You have now created a zone for each interface. This will keep the traffic between each interface in each zone. Next, you will associate each zone with an interface.

8. Navigate to **Network > Interfaces**.

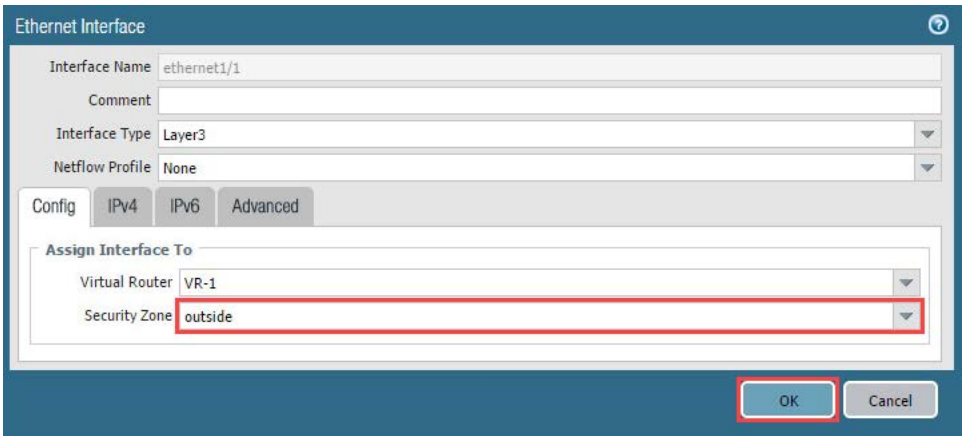


 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

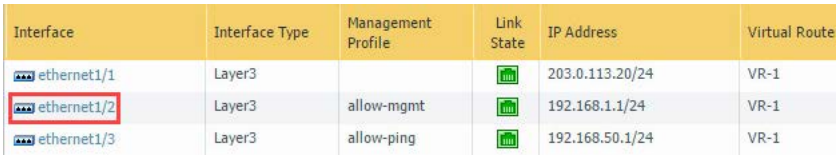
9. Click on the **ethernet1/1** interface.

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Route
ethernet1/1	Layer3			203.0.113.20/24	VR-1
ethernet1/2	Layer3	allow-mgmt		192.168.1.1/24	VR-1
ethernet1/3	Layer3	allow-ping		192.168.50.1/24	VR-1

10. In the *Ethernet Interface* window, select **outside** from the Security Zone dropdown. Then, click on the **OK** button.

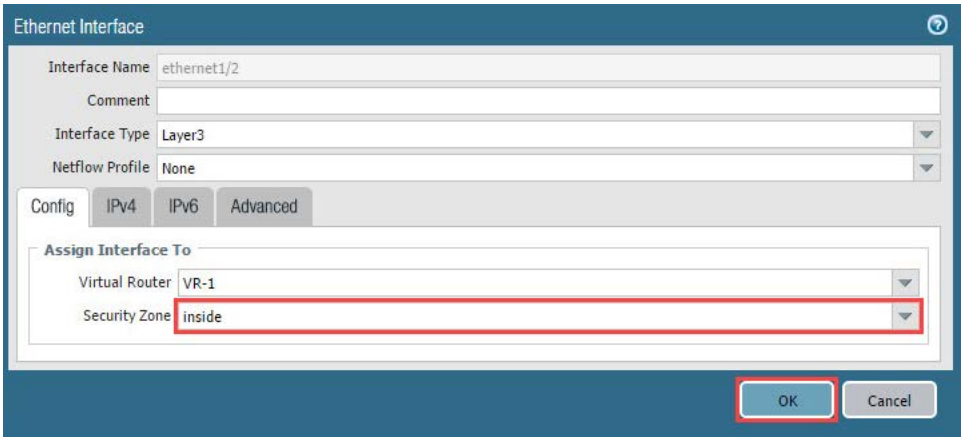


11. Click on the **ethernet1/2** interface.



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Route
ethernet1/1	Layer3			203.0.113.20/24	VR-1
ethernet1/2	Layer3	allow-mgmt		192.168.1.1/24	VR-1
ethernet1/3	Layer3	allow-ping		192.168.50.1/24	VR-1

12. In the *Ethernet Interface* window, select **inside** from the Security Zone dropdown. Then, click on the **OK** button.

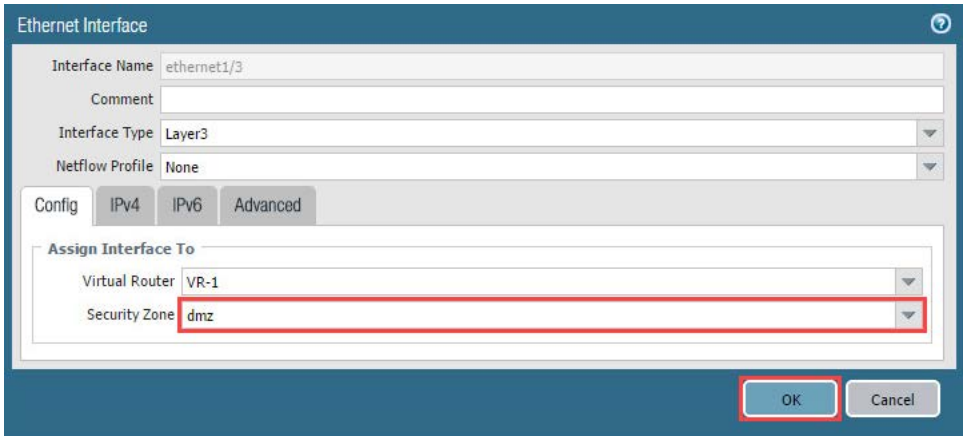


 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

13. Click on the **ethernet1/3** interface.

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Route
ethernet1/1	Layer3			203.0.113.20/24	VR-1
ethernet1/2	Layer3	allow-mgmt		192.168.1.1/24	VR-1
ethernet1/3	Layer3	allow-ping		192.168.50.1/24	VR-1

14. In the *Ethernet Interface* window, select the **dmz** in the Security Zone dropdown. Then, click on the **OK** button

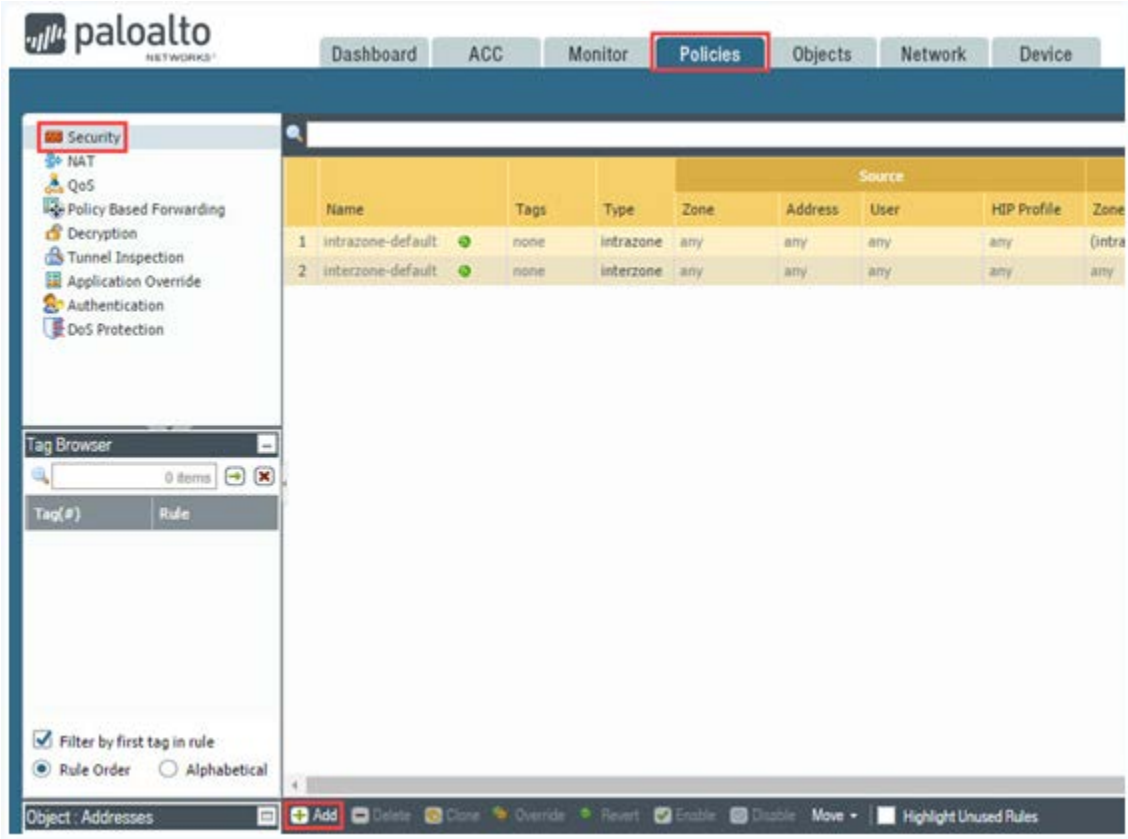


 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

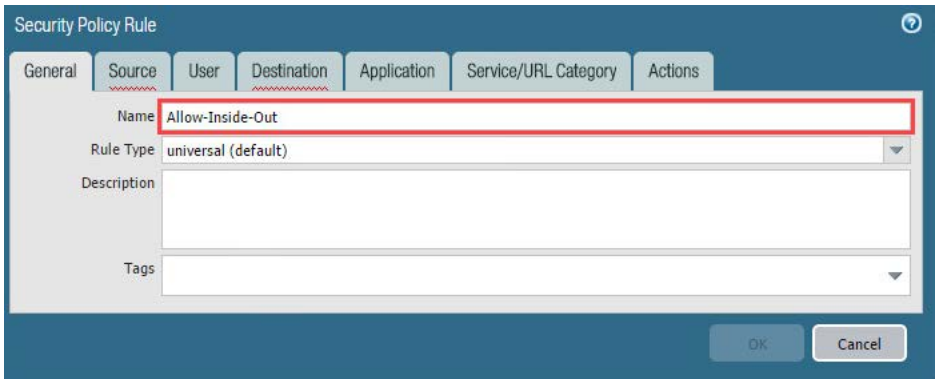
1.2 Create a Security Policy Rule

In this section, you will create a security policy rule that allows traffic from the inside zone to the outside zone.

1. Navigate to **Policies > Security > Add.**



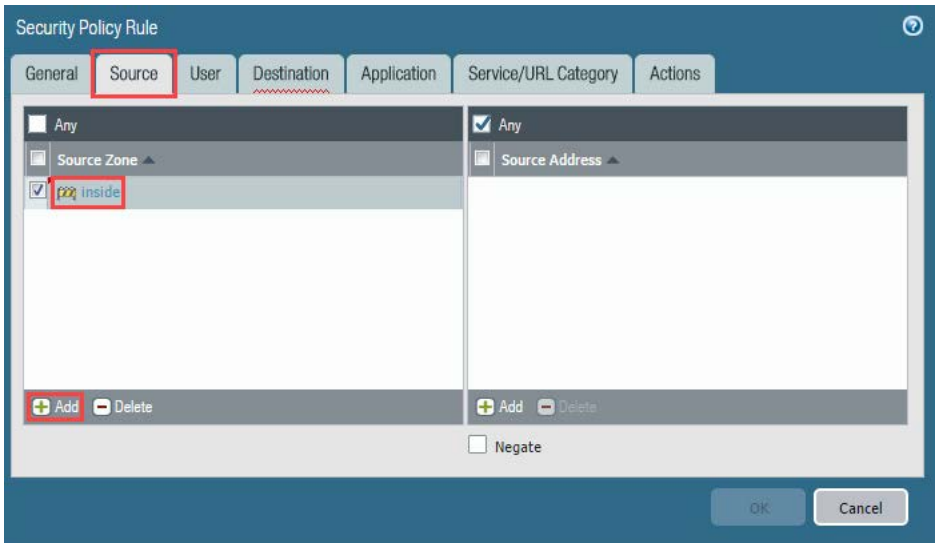
2. In the *Security Policy Rule* window, type **Allow-Inside-Out** in the Name field.



In a Security Policy Rule, there are three required sections. Note the initial red squiggle lines under General, Source, and Destination. These will go away as you fill out the required information.

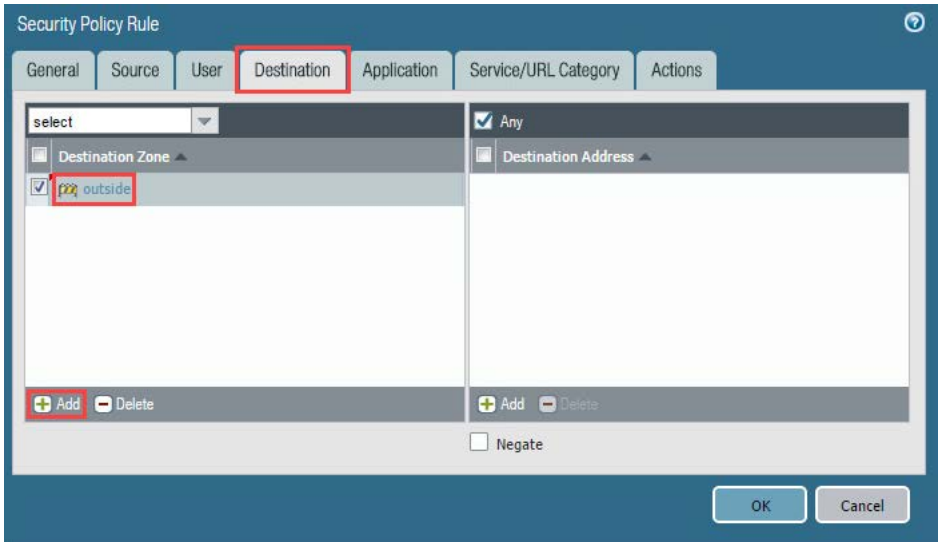
 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

3. In the *Security Policy Rule* window, click on the **Source** tab. Then, click the **Add** button in the Source Zone section. Next, select **inside** from the dropdown in the Source Zone column.



The **Source** tab allows you to select where traffic is coming from. In this rule, you select traffic coming from the *inside* zone. Note that you leave the default setting of *any* source address. This allows any address in the *inside* zone to pass through.

4. In the *Security Policy Rule* window, click on the **Destination** tab. Then, click the **Add** button in the Destination Zone section. Next, select **outside** from the dropdown in the Destination Zone column.



Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

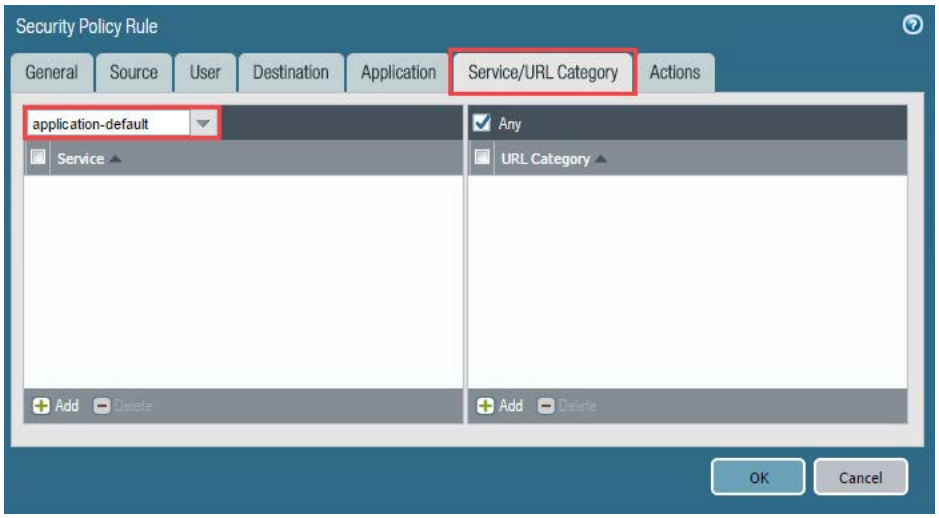
The **Destination** tab allows you to select where traffic is going to. In this rule, you select traffic destined to the *outside* zone. Note that you leave the default setting of *any* destination address. This allows the source traffic to communicate with any address in the destination zone.

5. In the *Security Policy Rule* window, click on the **Application** tab. Then, make sure that the **Any** checkbox is checked.

The **Application** tab allows you to select predefined applications to allow through the Firewall. The Palo Alto Networks Firewall can be very precise on the traffic it allows. The **Any** checkbox allows any application through. In a real-world deployment, you may use a similar rule for testing traffic without any restrictions.

 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

6. In the *Security Policy Rule* window, click on the **Service/URL Category** tab. Then, make sure **application-default** is selected in the dropdown above the Service section.

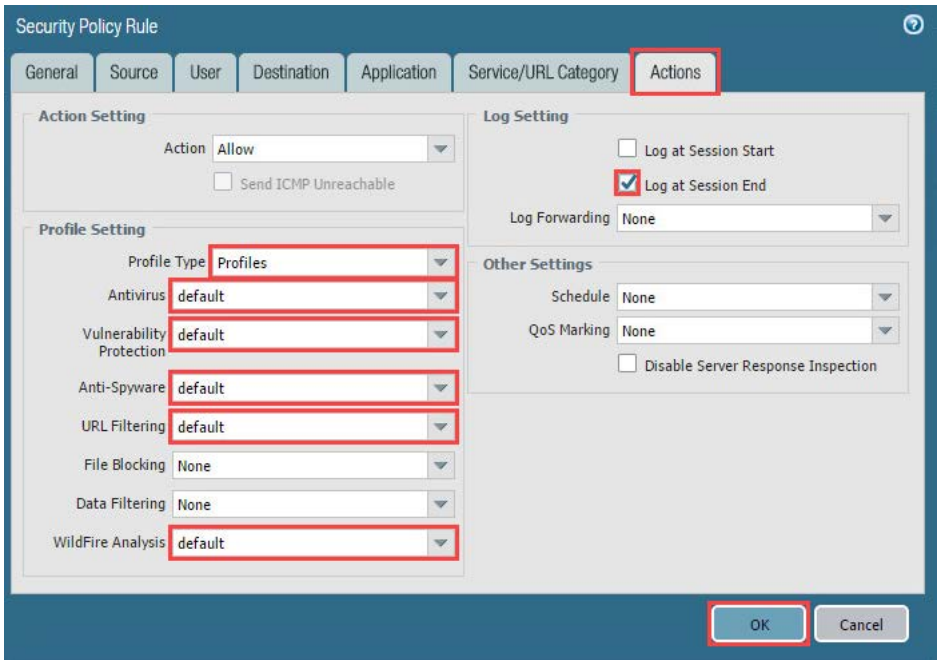


The **Service/URL Category** tab allows you to select predefined services or preset groups to allow through the Firewall. The **application-default** selection means that the selected applications are allowed or denied only on their default ports defined by Palo Alto Networks. This option is recommended for allowing policies because it prevents applications from running on unusual ports and protocols, which if not intentional, can be a sign of undesired application behavior and usage. When you use this option, the device still checks for all applications on all ports, but with this configuration, applications are only allowed on their default ports/protocols.

For example, if a web server is running on the standard port 80, traffic will be allowed to pass. However, if the web server is running on a non-standard port such as 5000, traffic will be blocked.

 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

7. In the *Security Policy Rule* window, click on the **Actions** tab. Then, make sure **Log at Session End** is checked under the Log Setting section. Next, select **Profiles** from the dropdown under the Profile Setting section. Then, select **default** for the Antivirus, Vulnerability Protection, Anti-Spyware, URL Filtering, and WildFire Analysis fields. Finally, click the **OK** button.

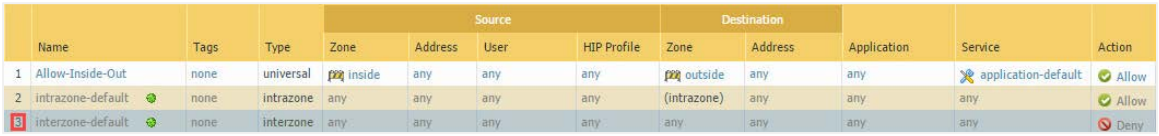


The **Actions** tab allows you to decide what to do with the traffic you have defined. In this rule, you use the default *Allow* action setting to permit traffic. Selecting *Log at Session End* is considered best practice as applications are likely to change throughout the lifespan of the session. Facebook, for example, will start as *web-browsing* and change to *Facebook-base* after the firewall recognized the application.

The various profile settings allow for predefined signatures and threats to be assessed by the Firewall. At a minimum it is best practice to select the *default* profiles. There are additional best practices for each individual profile defined in the technical documentation available at Palo Alto Networks.

 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

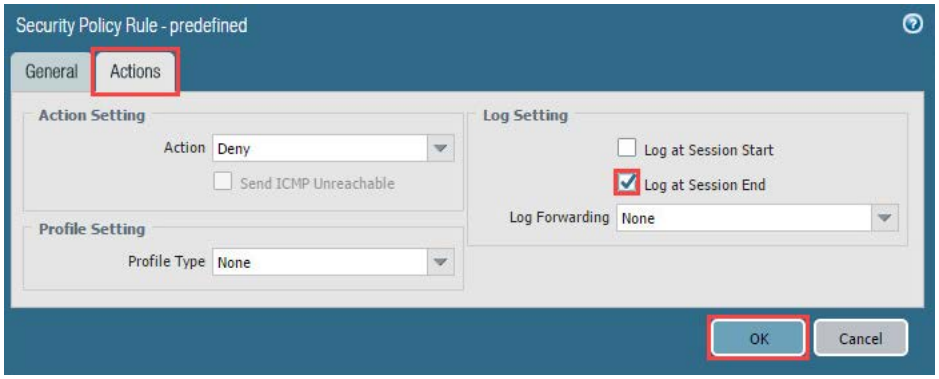
8. Click on the number **3,** to select but not open the **interzone-default** security policy.



	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Application	Service	Action
1	Allow-Inside-Out	none	universal	inside	any	any	any	outside	any	any	application-default	Allow
2	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
3	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny

9. With the interzone-default policy selected, click on the **Override** button at the bottom of the center section.

10. In the *Security Policy Rule – predefined* window, click on the **Actions** tab. Then, select **Log at Session End** checkbox under the Log Settings section. Finally, click the **OK** button.

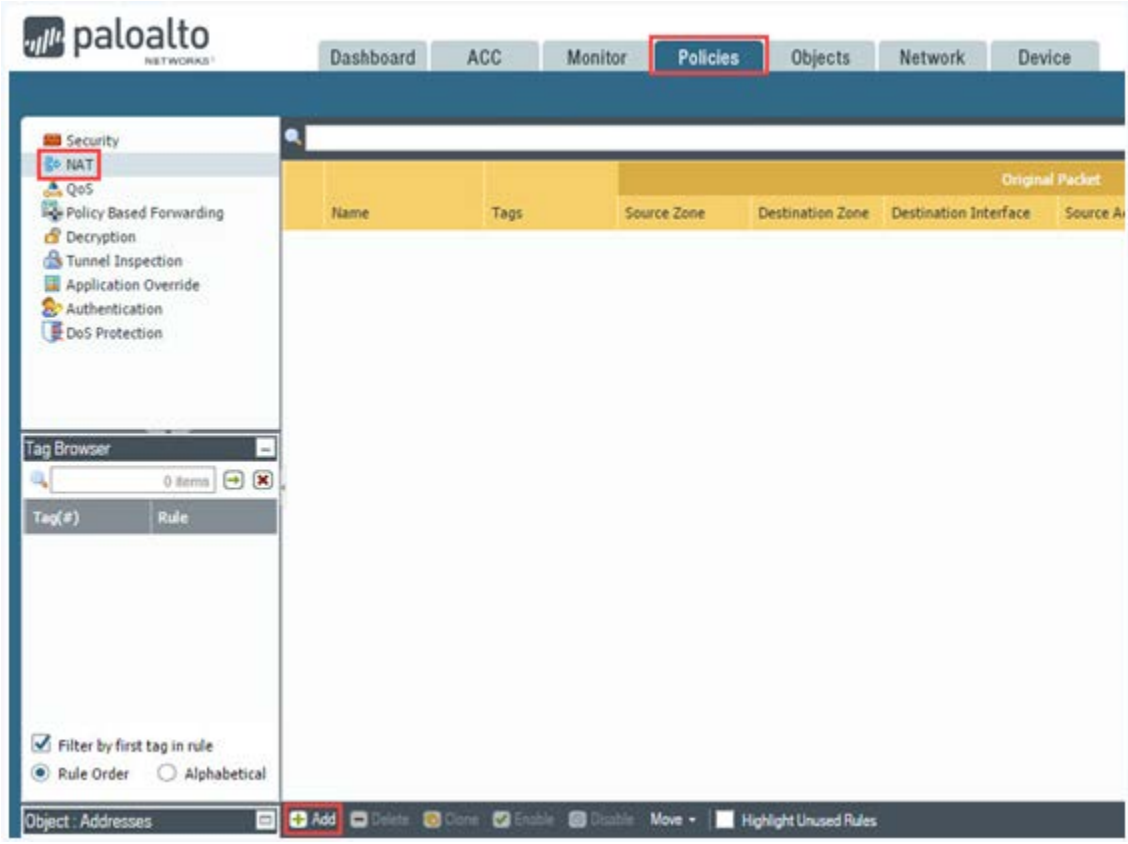


 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

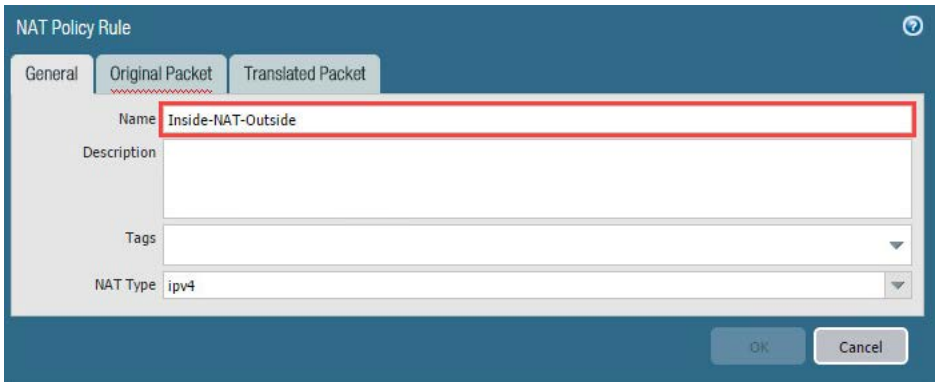
1.3 Create a NAT Policy

In this section, you will create a basic NAT policy to NAT traffic from the inside zone to the outside zone.

1. Navigate to **Policies > NAT > Add**.

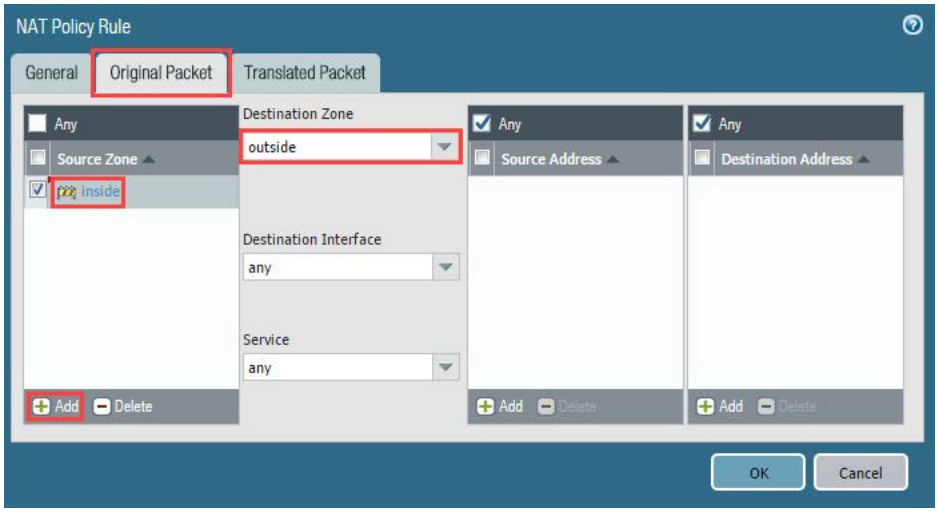


2. In the *NAT Policy Rule* window, type **Inside-NAT-Outside** in the Name field.

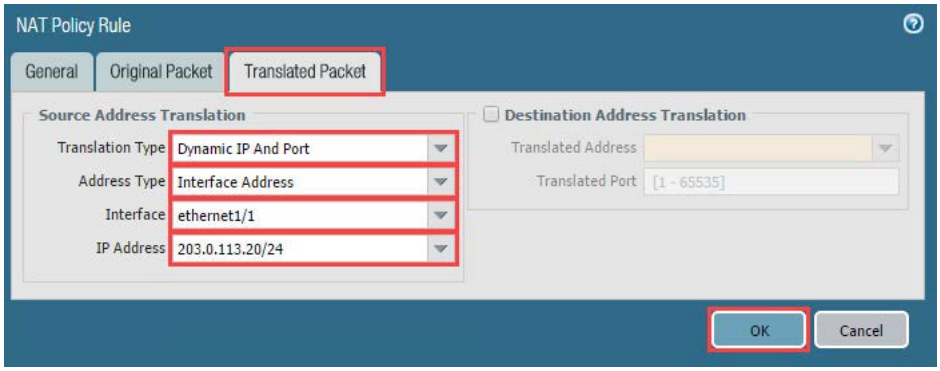


 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

3. In the *NAT Policy Rule* window, click on the **Original Packet** tab. Then, click the **Add** button at the bottom of the Source Zone section. Next, select **inside** in the dropdown of the Source Zone column. Finally, select **outside** in the Destination Zone dropdown.



4. In the *NAT Policy Rule* window, click on the **Translated Packet** tab. Then, select **Dynamic IP And Port** on the Translation Type dropdown. Next, select **Interface Address** on the Address Type dropdown. Then, select **ethernet1/1** for the Interface dropdown. Finally, select **203.0.113.20/24** on the IP Address dropdown and click the **OK** button.



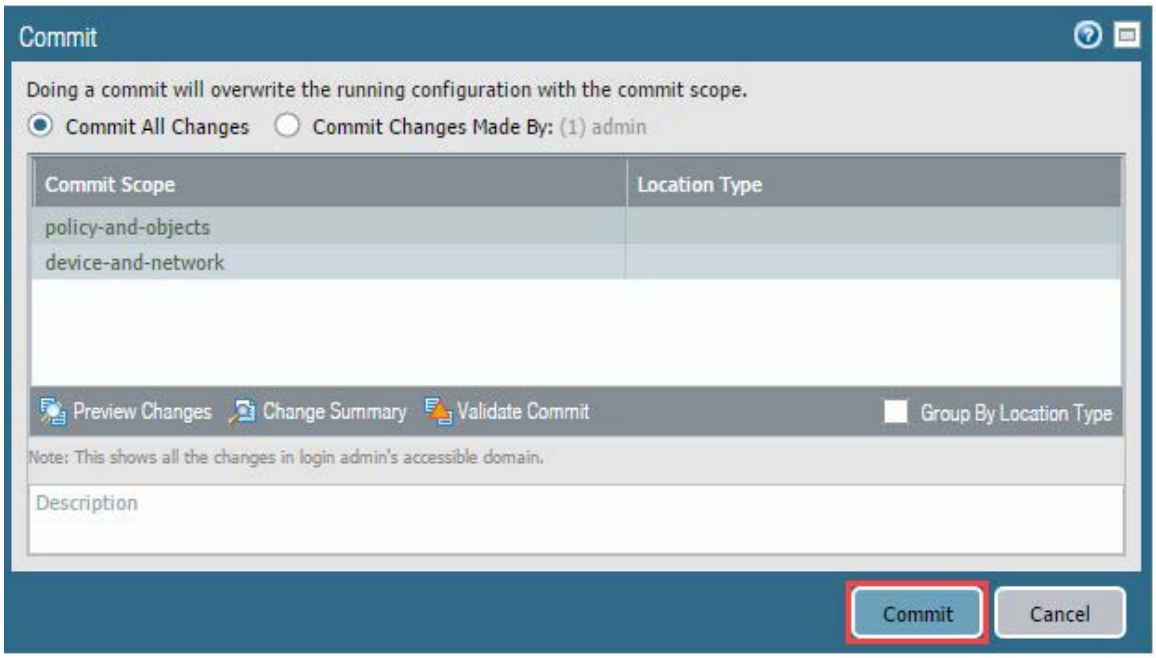
 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

1.4 Commit and Test the Rules and Policies

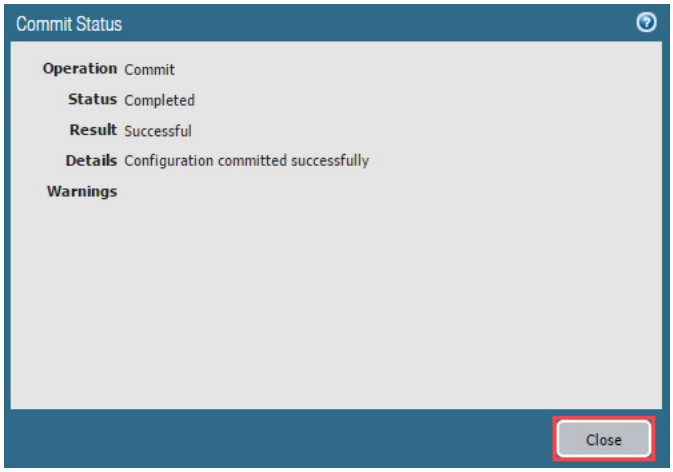
In this section, you will create a basic NAT policy to NAT traffic from the inside zone to the outside zone.

1. Click the **Commit** link located at the top-right of the web interface.

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



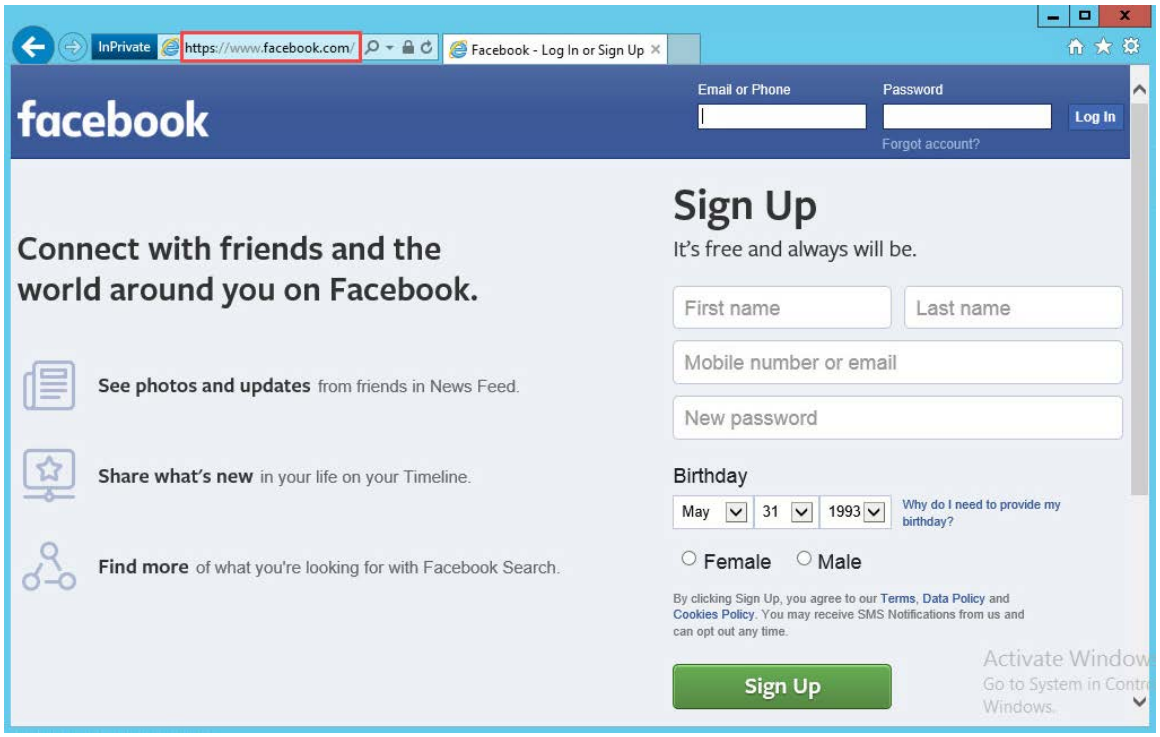
3. When the commit operation successfully completes, click **Close** to continue.



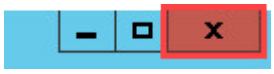
 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

4. Open **Internet Explorer** from the taskbar.

5. In the address bar, type **https://www.facebook.com** and press **Enter**.



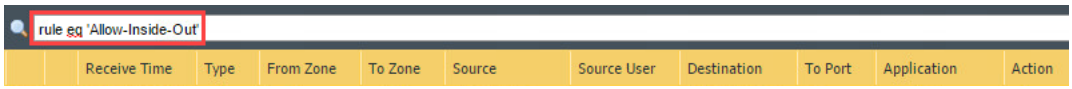
6. Click the **X** in the upper-right to close **Internet Explorer**.



7. Navigate to **Monitor > Logs > Traffic.**

 Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

8. In the filter text box, type **rule eq 'Allow-Inside-Out'** and press **Enter**.



9. You will see log entries allowing the **facebook-base** application.

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action
05/31 16:55:07	end	inside	outside	192.168.1.20		172.217.15.99	443	google-base	allow
05/31 16:54:13	end	inside	outside	192.168.1.20		172.217.15.99	443	google-base	allow
05/31 16:52:52	end	inside	outside	192.168.1.20		216.58.217.174	80	ocsp	allow
05/31 16:52:52	end	inside	outside	192.168.1.20		216.58.217.174	80	ocsp	allow
05/31 16:52:52	end	inside	outside	192.168.1.20		72.21.91.29	80	ocsp	allow
05/31 16:52:49	end	inside	outside	192.168.1.20		172.217.15.100	443	google-base	allow
05/31 16:52:49	end	inside	outside	192.168.1.20		172.217.7.130	443	google-base	allow
05/31 16:52:49	end	inside	outside	192.168.1.20		172.217.15.100	443	google-base	allow
05/31 16:52:48	end	inside	outside	192.168.1.20		31.13.69.193	443	ssl	allow
05/31 16:52:48	end	inside	outside	192.168.1.20		31.13.69.203	443	facebook-base	allow
05/31 16:52:48	end	inside	outside	192.168.1.20		31.13.71.36	443	ssl	allow
05/31 16:52:48	end	inside	outside	192.168.1.20		31.13.71.36	443	ssl	allow
05/31 16:52:48	end	inside	outside	192.168.1.20		31.13.69.228	443	facebook-base	allow
05/31 16:52:48	end	inside	outside	192.168.1.20		31.13.69.193	443	ssl	allow
05/31 16:52:48	end	inside	outside	192.168.1.20		31.13.69.203	443	facebook-base	allow
05/31 16:52:48	end	inside	outside	192.168.1.20		31.13.69.203	443	facebook-base	allow
05/31 16:52:48	end	inside	outside	192.168.1.20		31.13.69.203	443	facebook-base	allow

Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com