PALO ALTO NETWORKS EDU-210

paloalto
NETWORKS

Lab 13: Active/Passive High Availability

Document Version: 2019-11-12

Contents

Introduction

The board and the executives have become worried that we could experience downtime with the current configuration. They have therefore approved the purchase of a second Palo Alto Networks firewall like the first one and to implement Active/Passive High Availability to prevent possible downtime. We are going to test the process of configuring the feature before the second device arrives. We will then be able to duplicate the process when the second device arrives and turn it on.
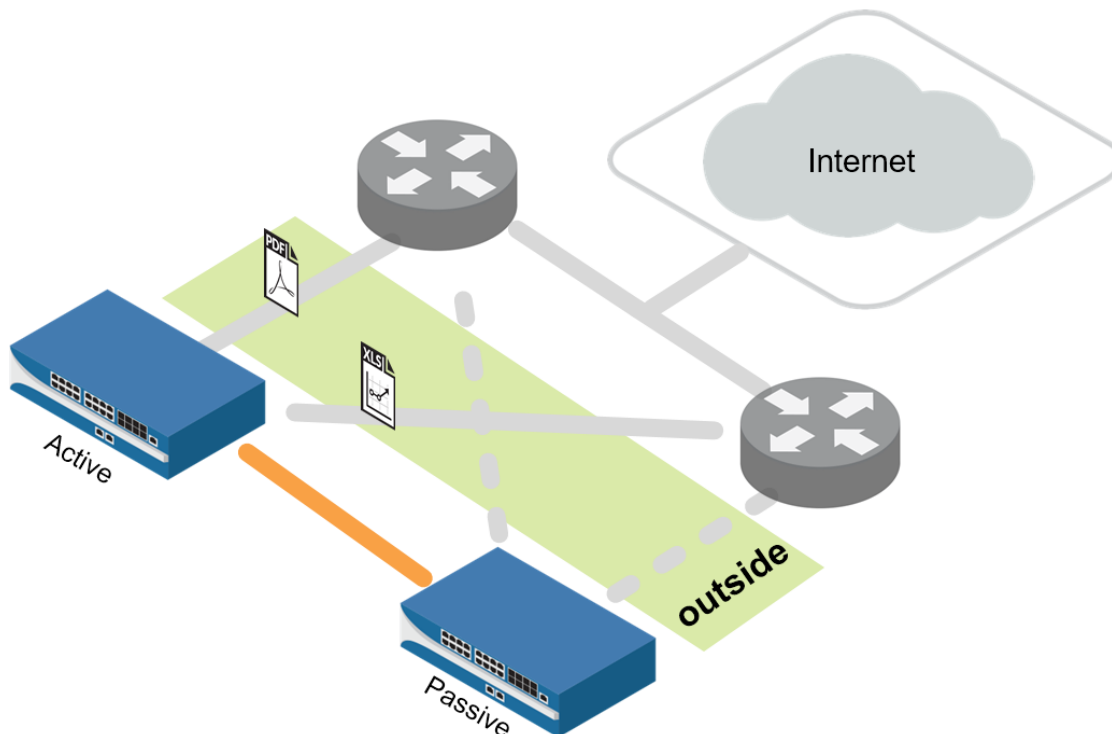
Objectives

- Display the Dashboard HA widget
- Configure a dedicated HA interface
- Configure active/passive HA
- Configure HA monitoring
- Observe the HA widget

Lab Topology
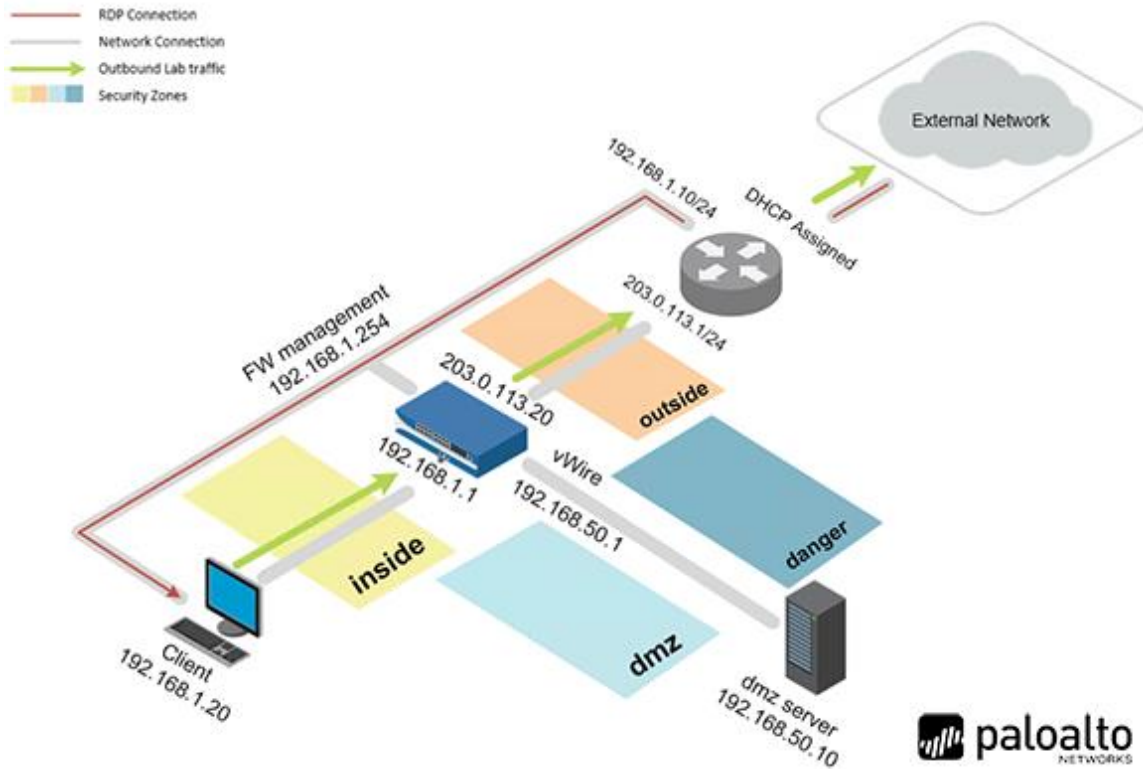
Theoretical Lab Topology

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	192.168.1.20	`lab-user`	`Pal0Alt0`
Firewall	192.168.1.254	`admin`	`admin`

1 Active/Passive High Availability

1.0 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. Click within the splash screen to bring up the login screen. Log in as `lab-user` using the password `Pal0Alt0`.
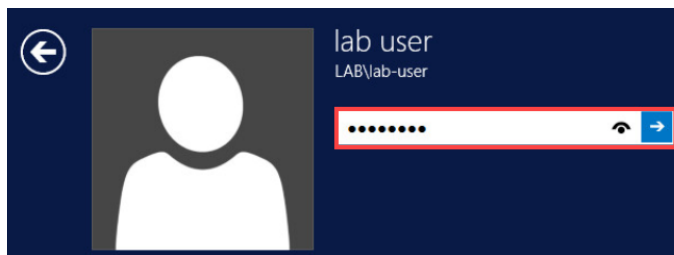

3. Launch the **Chrome** browser and connect to `https://192.168.1.254`.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

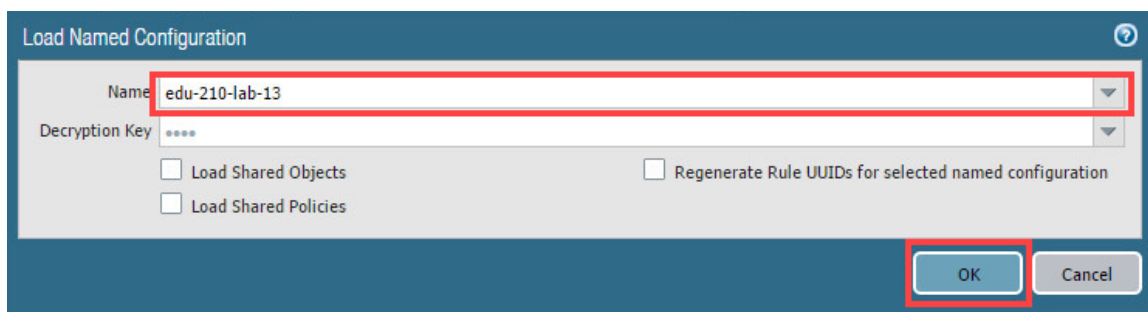| Parameter	Value
Name	`admin`
Password	`admin`

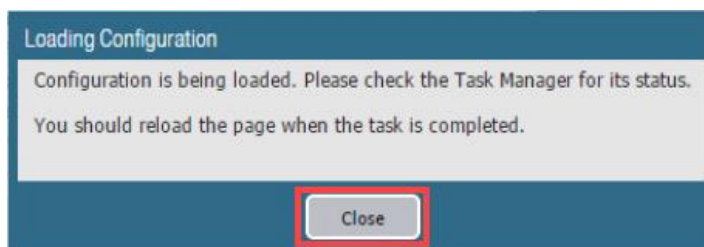6. In the web interface, navigate to **Device > Setup > Operations**.

7. Click **Load named configuration snapshot**:
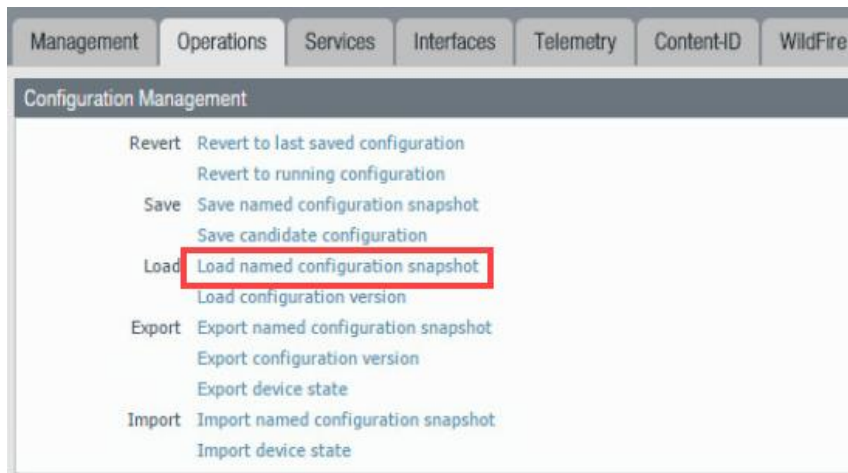
8. Click the drop-down list next to the *Name* text box and select **edu-210-lab-13**. Click **OK**.
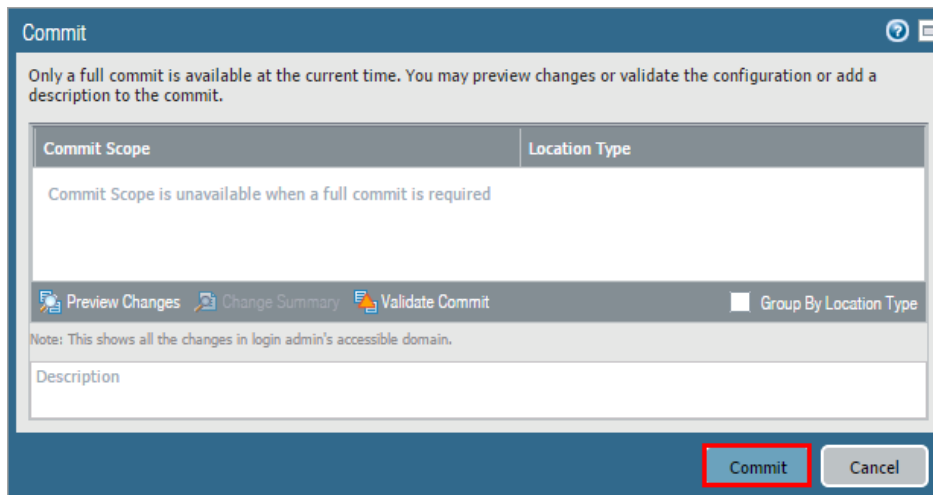

9. Click **Close**.

The following instructions are the steps to execute a **"Commit All"** as you will perform many times throughout these labs.
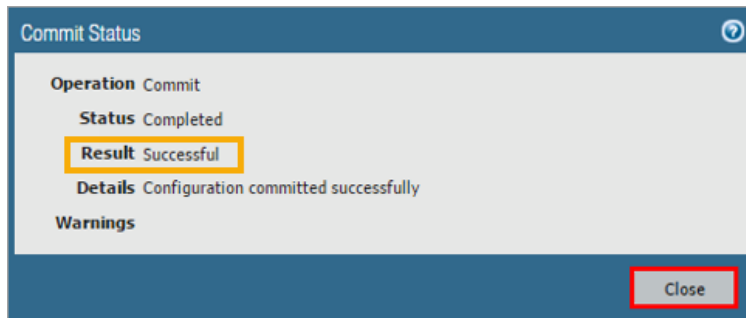
10. Click the **Commit** link at the top-right of the web interface.

11. Click **Commit** and wait until the commit process is complete.

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

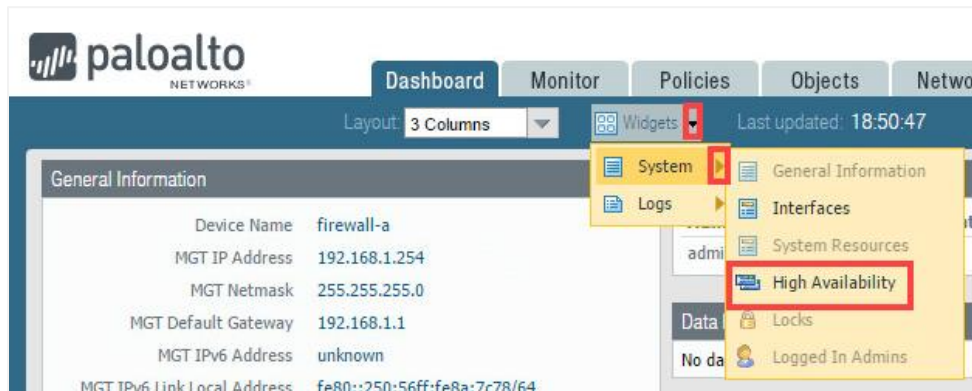13. Leave the firewall web interface open to continue with the next task.

1.1 Display the HA Widget

If high availability (HA) is enabled, the *High Availability* widget on the *Dashboard* indicates the HA status.

1. In the web interface, click the **Dashboard** tab to display current firewall information.

2. If the *High Availability* panel is not displayed, select **Widgets > System > High Availability** to enable the display.

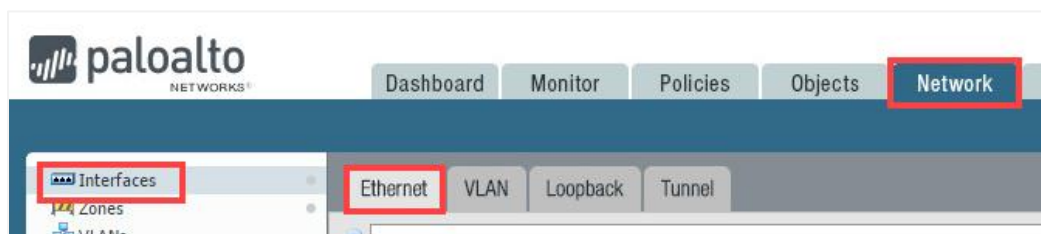3. Notice the *High Availability* widget now appears.

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

1.2   Configure the HA Interface

Each HA interface has a specific function: one interface is for configuration synchronization and heartbeats, and the other interface is for state synchronization (not configured in this lab).

1. In the web interface, navigate to **Network > Interfaces > Ethernet**.

2. Click **ethernet1/6** to open the configuration window for that interface.

3. In the Ethernet Interface window, select **HA** from the *Interface Type* drop-down list and click **OK**.

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

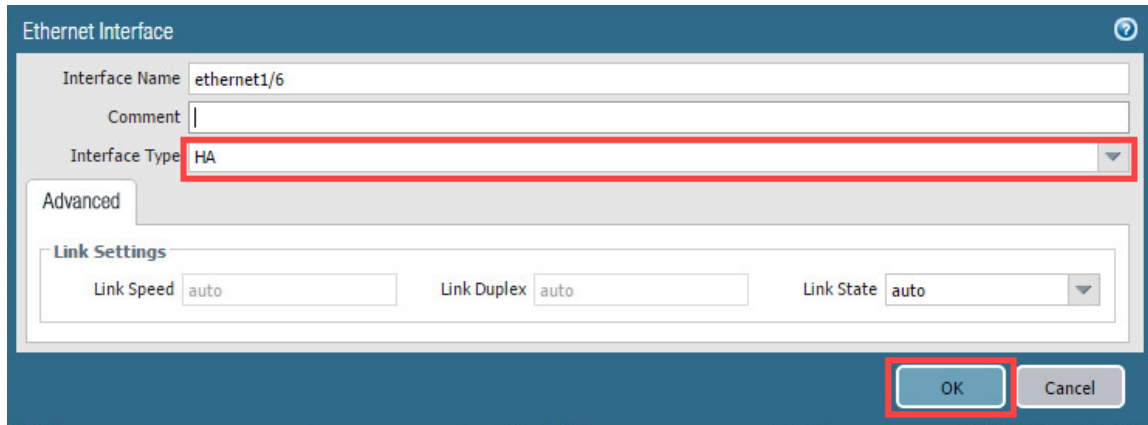## 1.3 Configure Active/Passive HA
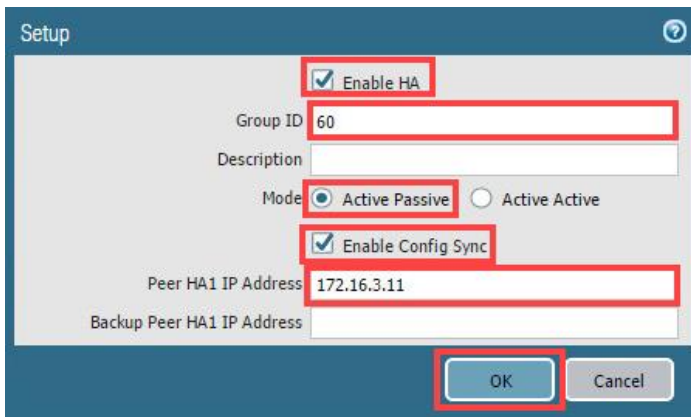
In this deployment, the active firewall continuously synchronizes its configuration and session information with the passive firewall over two dedicated interfaces. In the event of a hardware or software disruption on the active firewall, the passive firewall becomes active automatically without loss of service. Active/passive HA deployments are supported by the interface modes Virtual Wire, Layer 2, and Layer 3.

1. In the web interface, navigate to **Device > High Availability > General**.

2. Click the **Edit** ⚙ icon from the *Setup* panel to open the *Setup* configuration window.

3. In the *Setup* window, configure the following. Once finished, click **OK**.

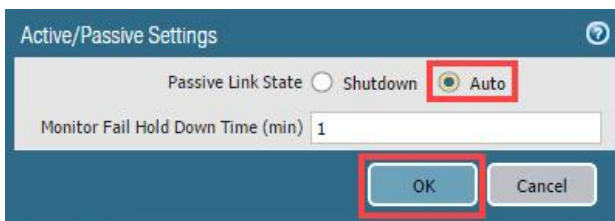| Parameter	Value
Enable HA	**Check** the checkbox
Group ID	Type 60 (This field is required and must be unique if multiple HA pairs reside on the same broadcast domain.)
Mode	Verify that the **Active Passive** radio button is selected
Enable Config Sync	**Check** the checkbox (Select this option to enable synchronization of configuration settings between the peers.)
Peer HA1 IP Address	Type 172.16.3.11

4. Click the **Edit** ⚙ icon from the *Active/Passive Settings* panel.

5. In the *Active/Passive Settings* window, select the **Auto** radio button and click **OK**.

> When *Auto* is selected, the links that have physical connectivity remain physically up but in a disabled state. They do not participate in ARP or packet forwarding. This configuration helps reduce convergence times during failover because no time is required to activate the links. To avoid network loops, do not select this option if the firewall has any Layer 2 interfaces configured.

6. Click the **Edit** ⚙ icon from the *Election Settings* panel to configure failover behavior.

7. In the *Election Settings* window, configure the following. Once finished, click **OK**.

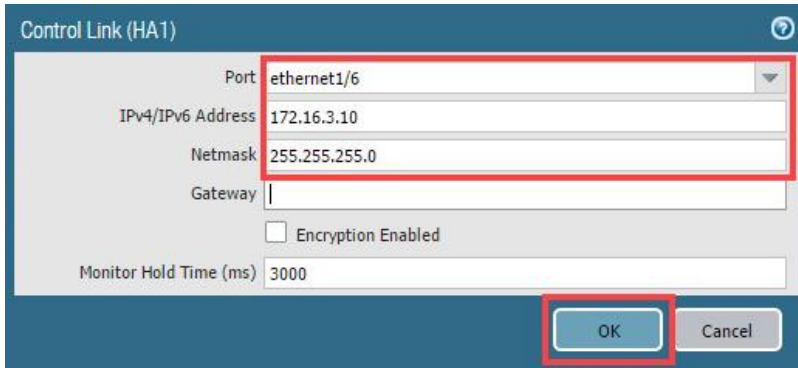| Parameter	Value
Device Priority	Type `80`
	(Enter a priority value (range is 0-255) to identify the active firewall. The firewall with the lower value (higher priority) becomes the active firewall when the *Preemptive* capability is enabled on both firewalls in the pair.)
Preemptive	**Check** the checkbox
	(Enables the higher priority firewall to resume active operation after recovering from a failure. This parameter must be enabled on both firewalls but is not always a recommended practice.)
Heartbeat Backup	**Uncheck** the checkbox
	(Uses the management ports on the HA firewalls to provide a backup path for heartbeat and hello messages.)
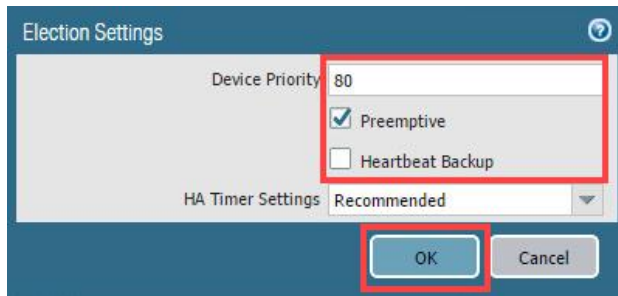
8. Click the **Edit** ⚙ icon from the *Control Link (HA1)* panel to configure the HA1 link. The firewalls in an HA pair use HA links to synchronize data and maintain state information.

9. In the *Control Link (HA1)* window, configure the following. Once finished, click **OK**.

Parameter	Value
Port	Select **ethernet1/6** from the drop-down list
IPv4/IPv6 Address	Type `172.16.3.10`
Netmask	Type `255.255.255.0`
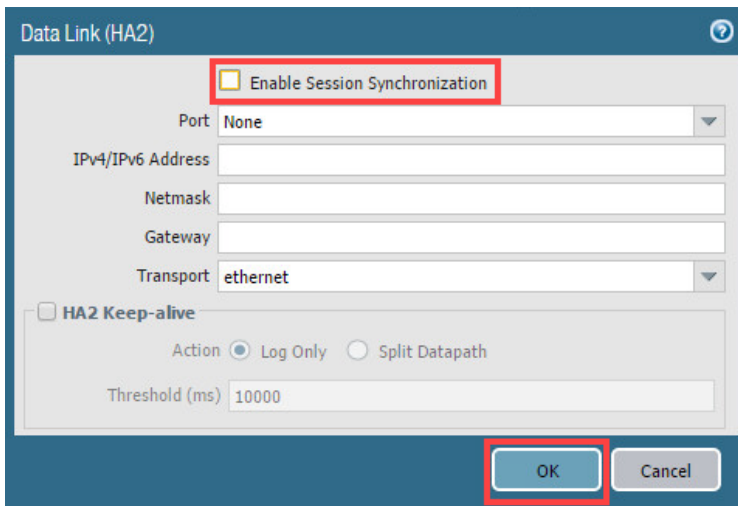
10. Click the **Edit** ⚙ icon from the *Data Link (HA2)* configuration window.
11. In the *Data Link (HA2)* windows, deselect the **Enable Session Synchronization** checkbox and click **OK**.

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

1.4   Configure HA Monitoring

1. In the web interface, navigate to **Device > High Availability > Link and Path Monitoring**.

2. Click the **Edit** ⚙ icon from the *Link Monitoring* panel to configure link failure detection.

> Link monitoring enables failover to be triggered when a physical link or group of physical links fails.

3. In the *Link Monitoring* window, verify that the **Enabled** checkbox is checked and that the **Any** radio button is selected. Click **OK**.
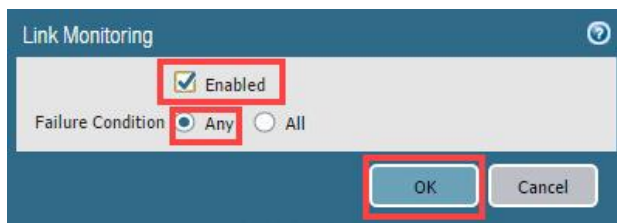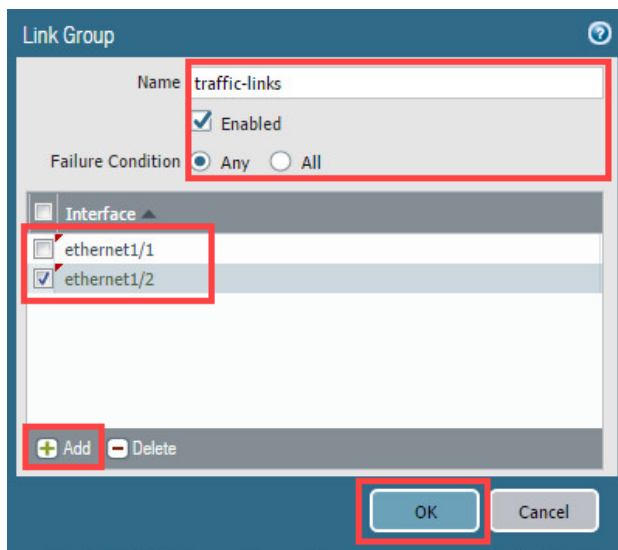

4. Click **Add** in the *Link Group* panel to configure the traffic links to monitor.
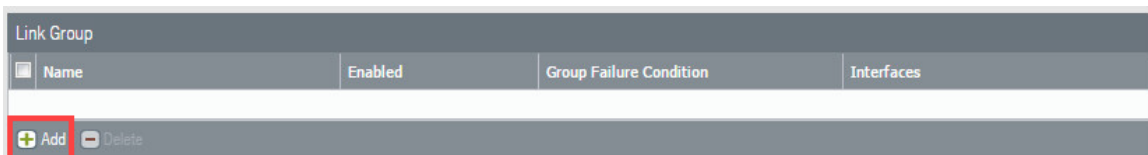
5. In the *Link Group* window, configure the following. Once finished, click **OK**.

Parameter	Value
Name	Type `traffic-links`
Enabled	Verify that **Enabled** is checked
	(Note: Not supported on VM-series on ESXi.)
Failure Condition	Verify that the **Any** radio button is selected
Interface	Click **Add** and select the following from the drop-down list:
	ethernet1/1
	ethernet1/2

6. Click the **Edit** ⚙ icon from the *Path Monitoring* panel to configure the *Path Failure* detection.

> Path monitoring enables the firewall to monitor specified destination IP addresses by sending ICMP ping messages to ensure that they are responsive.

7. In the *Path Monitoring* window, verify that the **Enabled** checkbox is checked and that the **Any** radio button is selected. Click **OK**.
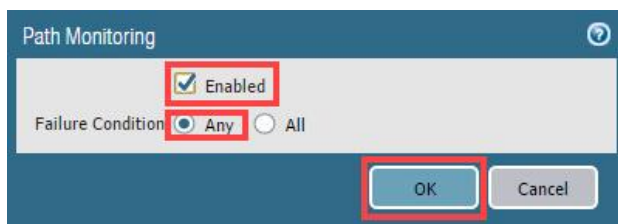
8. Find the *Path Group* panel and click **Add Virtual Router Path** to configure the path failure condition.

9. In the *HA Path Group Virtual Router* window, configure the following. Once finished, click **OK**.

| Parameter	Value
Name	Select **lab-vr** from the drop-down list
Enabled	Verify that the **Enabled** checkbox is checked
Failure Condition	Verify that the **Any** radio button is selected
Destination IP	Click **Add** and type `8.8.8.8`
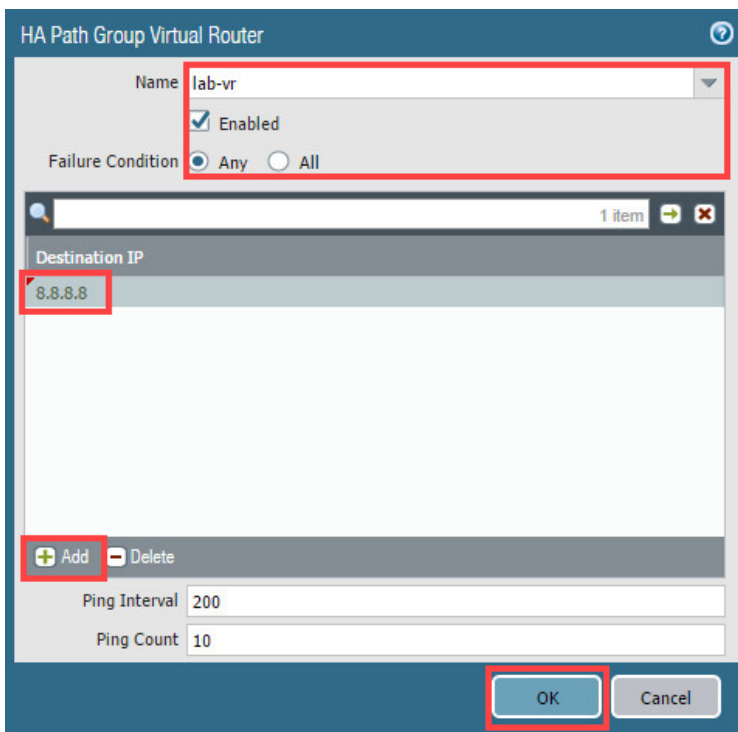
10. **Commit** all changes.

1.5 Observe the HA Widget

1. In the web interface, click the **Dashboard tab** and view the *High Availability* status widget for the firewall.

> Active-passive mode should be enabled, and the local firewall should be active (green). You may need to refresh the High Availability pane if the local firewall still shows that it is initializing. However, because there is no peer firewall, the status of most monitored items is unknown (yellow). Because HA1 has no peer, its state is down (red).

2. If a peer was configured and was operating in passive mode, the *High Availability* widget on the *Dashboard* would appear as follows.
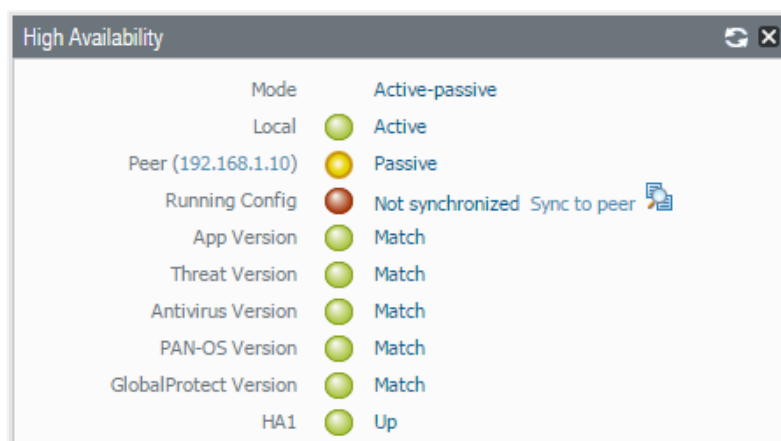
To avoid overwriting the wrong firewall configuration, the firewalls are not automatically synchronized. You must manually synchronize a firewall to the firewall with the "valid" configuration by clicking *Sync to peer*.

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