PALO ALTO NETWORKS EDU-210

Lab 13: Active/Passive High Availability

Document Version: 2017-09-29

Copyright © 2017 Network Development Group, Inc.
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^2 is a registered trademark of EMC Corporation.

Contents

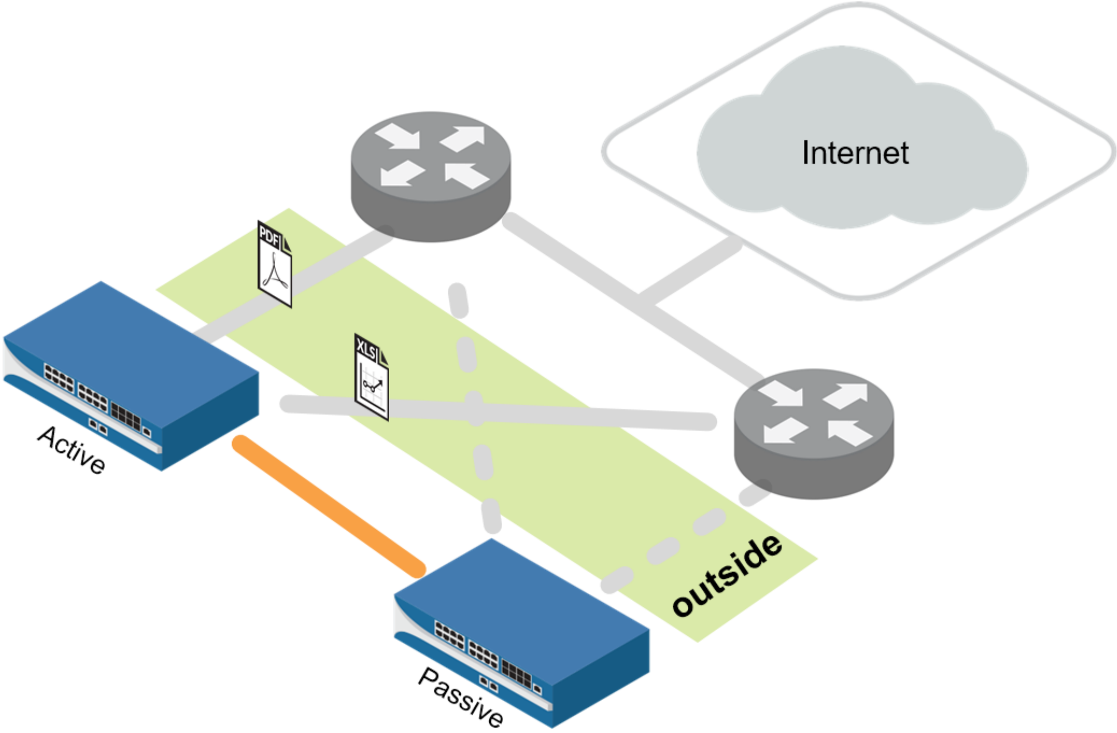
Introduction

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



Lab Settings

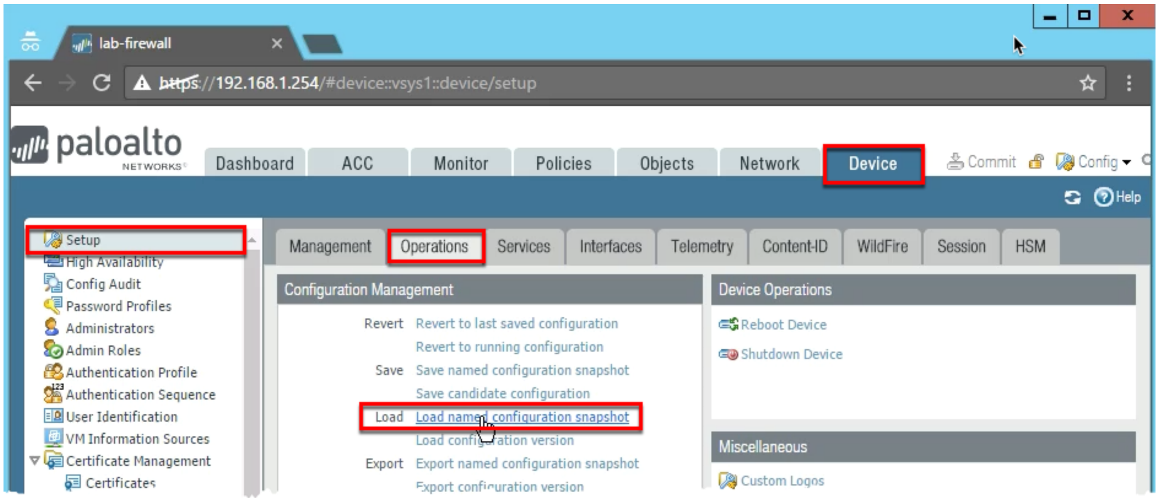
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

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

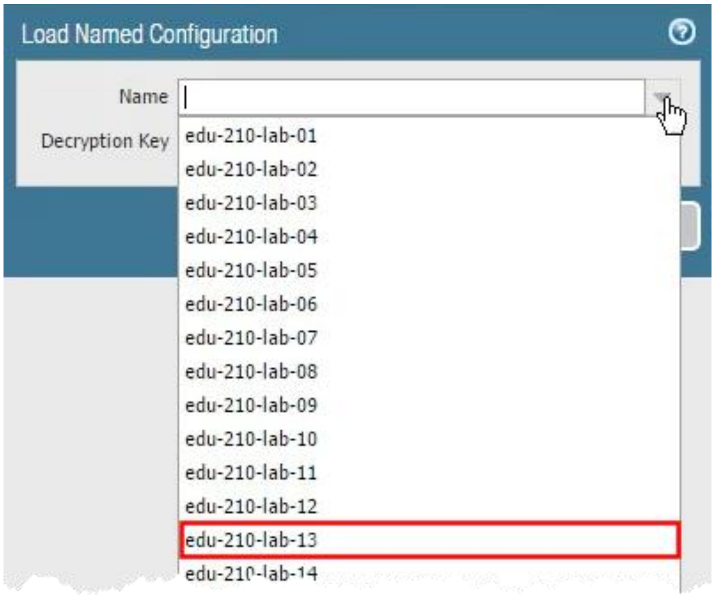
13 Lab: Active/Passive High Availability

13.0 Load Lab Configuration

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



3. Select **edu-210-lab-13** and click **OK**.

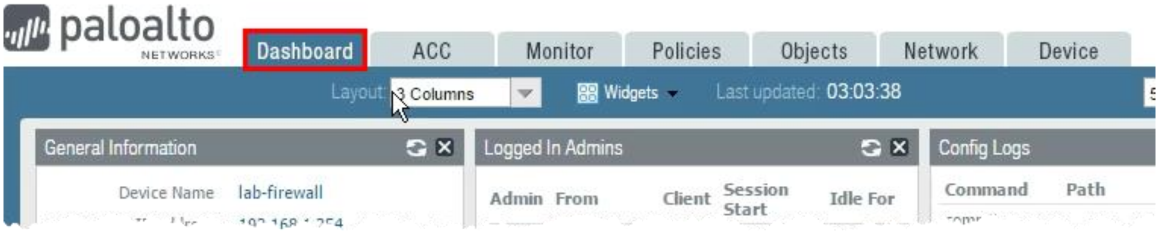


4. Click **Close**.
5. **Commit** all changes.

13.1 Display the HA Widget

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

1. In the WebUI click the **Dashboard** tab to display current firewall information.

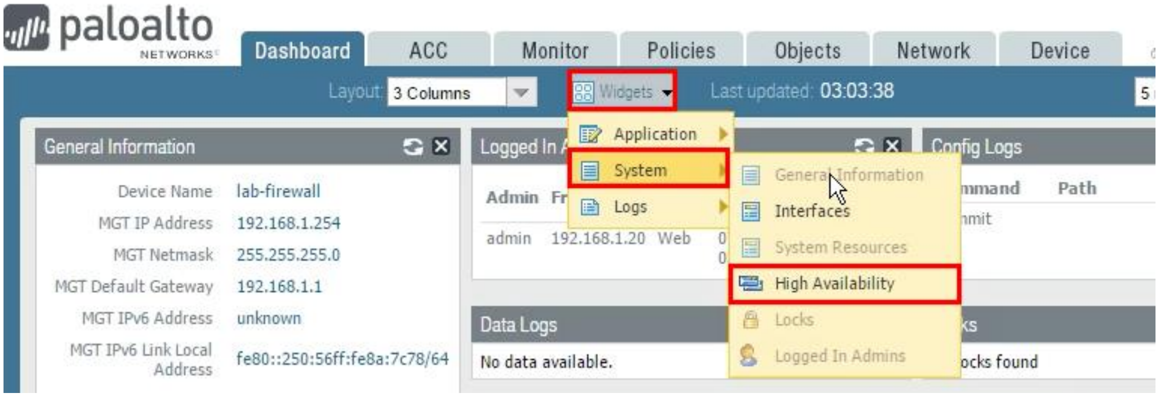


Layout: 3 Columns

Last updated: 03:03:38

Device Name lab-firewall

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



Layout: 3 Columns

Last updated: 03:03:38

General Information	
Device Name	lab-firewall
MGT IP Address	192.168.1.254
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.1.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::250:56ff:fe8a:7c78/64

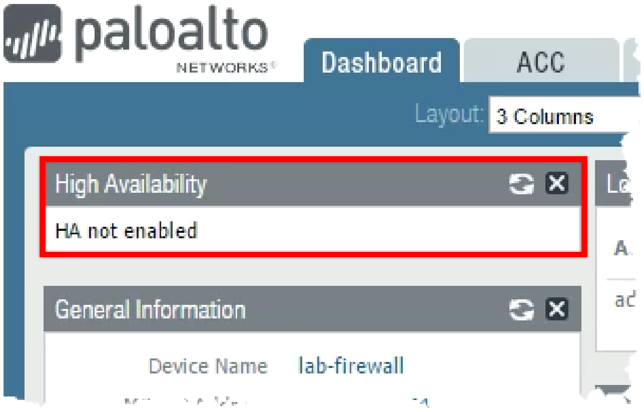
Admin Fr...

admin 192.168.1.20 Web

No data available.

...ocks found

The High Availability Widget now displays on the Dashboard:



Layout: 3 Columns

High Availability

HA not enabled

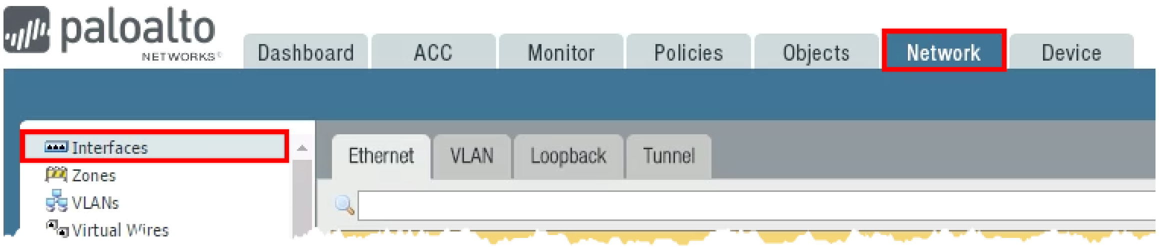
General Information

Device Name lab-firewall

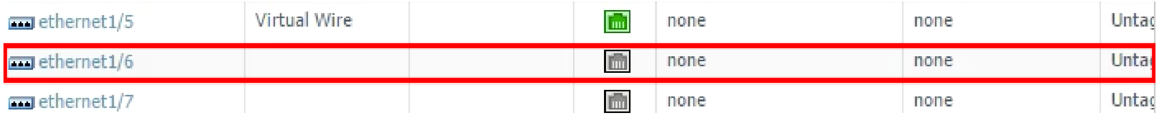
13.2 Configure the HA Interface

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 WebUI select **Network > Interfaces > Ethernet**.

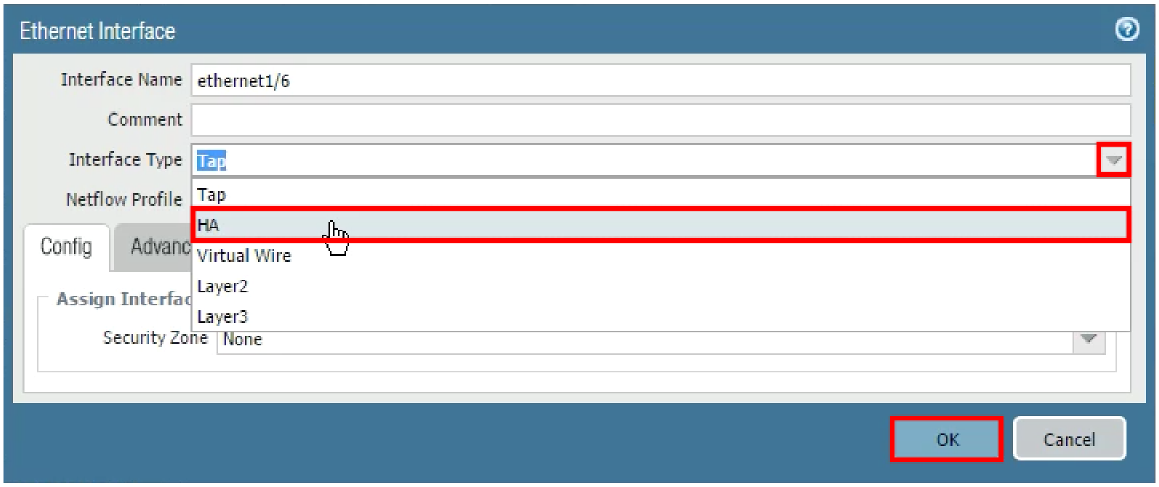


2. Click **ethernet1/6** to open the configuration window for that interface.



ethernet1/5	Virtual Wire		🟩	none	none	Untag
ethernet1/6			▨	none	none	Untag
ethernet1/7			▨	none	none	Untag

3. Select **HA** on the Interface Type drop-down list and click **OK**:



Ethernet Interface

Interface Name: ethernet1/6

Comment:

Interface Type: Tap

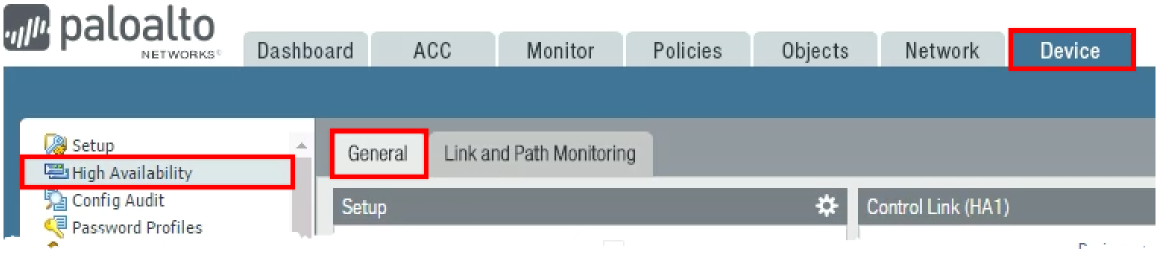
Netflow Profile:

Security Zone: None

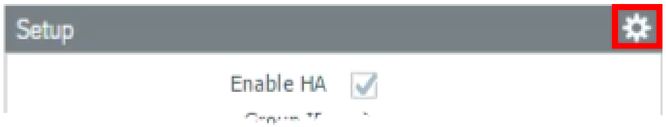
13.3 Configure Active/Passive HA

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 WebUI select **Device > High Availability > General**.



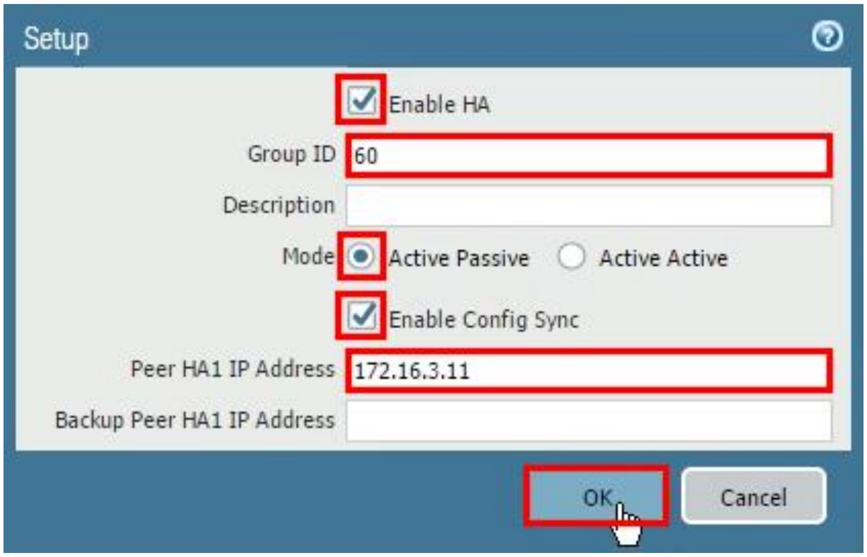
2. Click the **Edit** icon of the *Setup* panel to open the Setup configuration window.


Setup

Enable HA ☑

3. Configure the following:

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


Setup

☑ Enable HA

Group ID: 60

Description:

Mode: ● Active Passive ○ Active Active

☑ Enable Config Sync

Peer HA1 IP Address: 172.16.3.11

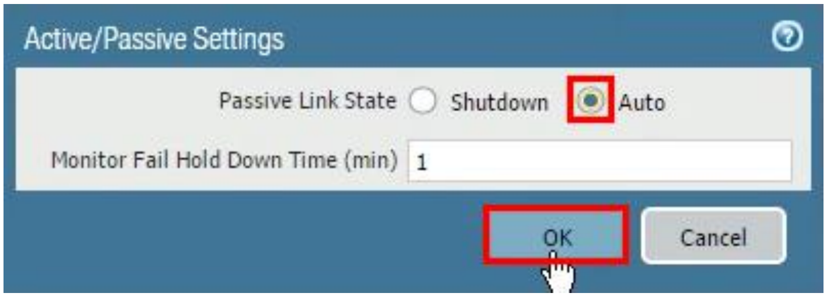
Backup Peer HA1 IP Address:

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

5. Click the **Edit** icon of the *Active/Passive Settings* panel:

   ⚙

6. Select the **Auto** radio button. 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.



Active/Passive Settings

Passive Link State ○ Shutdown ● Auto

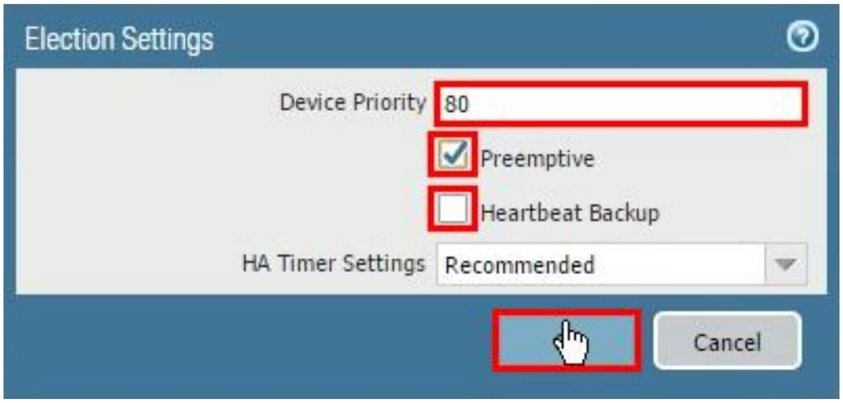
Monitor Fail Hold Down Time (min) 1

7. Click **OK** to close the *Active/Passive Settings* configuration window.

8. Click the **Edit** icon of the Election Settings panel to configure failover behavior:

Parameter	Value
Device Priority	`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	☑ Preemptive 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	□ Heartbeat Backup Uses the management ports on the HA firewalls to provide a backup path for heartbeat and hello messages

⚙



Election Settings

Device Priority: 80

☑ Preemptive

□ Heartbeat Backup

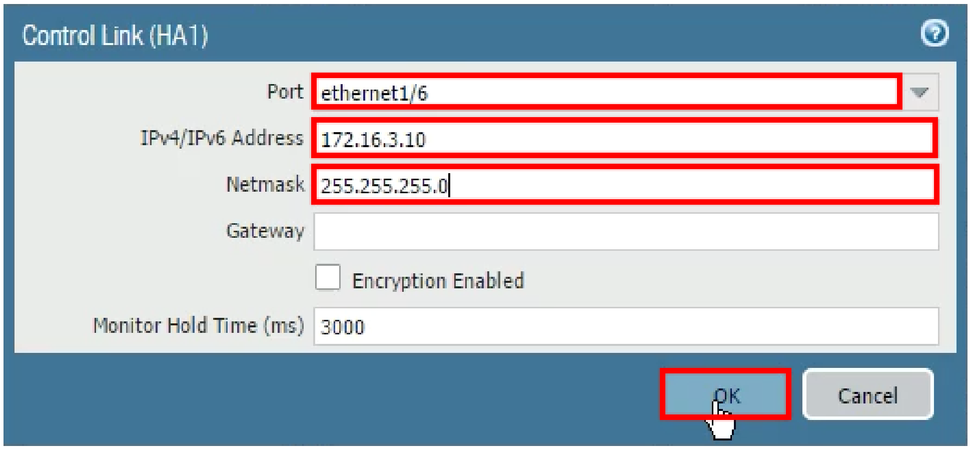
HA Timer Settings: Recommended

9. Click **OK** to close the *Election Settings* configuration window.

10. Click the **Edit** icon of 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:

Parameter	Value
Port	**ethernet1/6**
IP address	`172.16.3.10`
Netmask	`255.255.255.0`

⚙



Control Link (HA1)

Port: ethernet1/6

IPv4/IPv6 Address: 172.16.3.10

Netmask: 255.255.255.0

Gateway:

□ Encryption Enabled

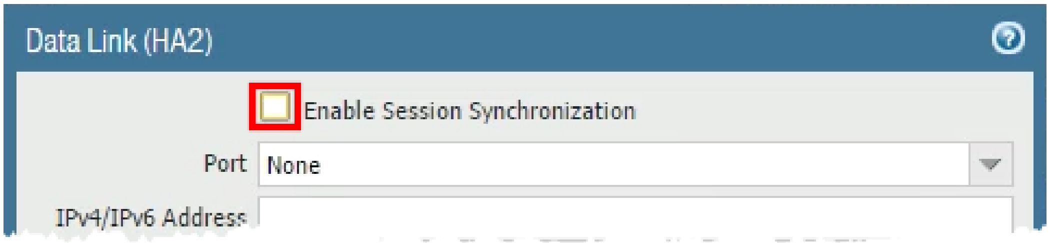
Monitor Hold Time (ms): 3000

11. Click **OK** to close the *Control Link (HA1)* configuration window.

12. Click the **Edit** icon of the *Data Link (HA2)* configuration window.

⚙

13. Deselect the **Enable Session Synchronization** check box:



Data Link (HA2)

□ Enable Session Synchronization

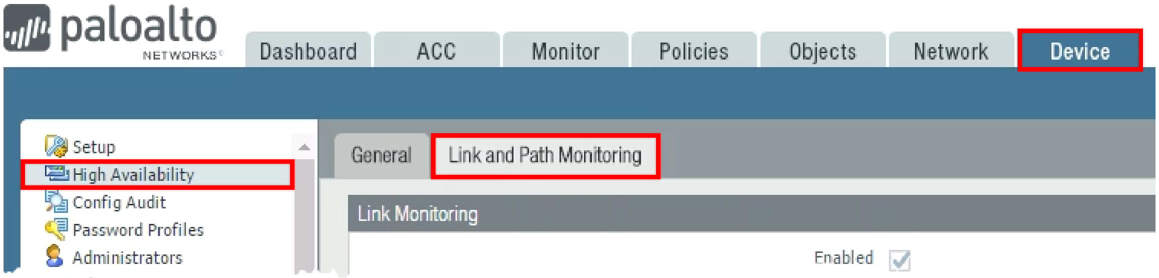
Port: None

IPv4/IPv6 Address:

14. Click **OK** to close the *Data Link (HA2)* configuration window.

13.4 Configure HA Monitoring

1. In the WebUI select **Device > High Availability > Link and Path Monitoring**.

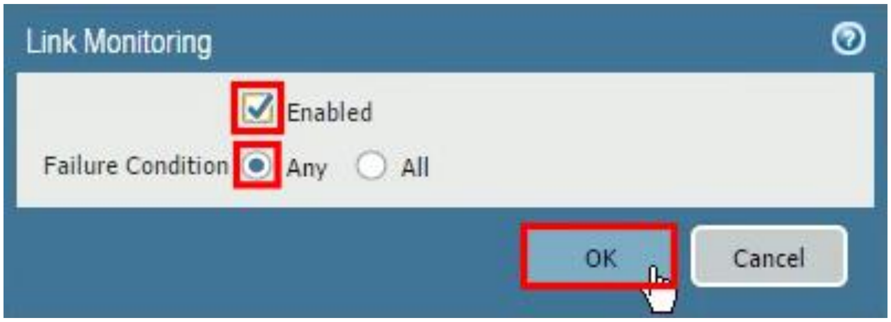


Link Monitoring

Enabled ☑

2. Click the **Edit** icon of 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.

Parameter	Value
Enabled	☑ Enabled
Failure Condition	**Any**



Link Monitoring

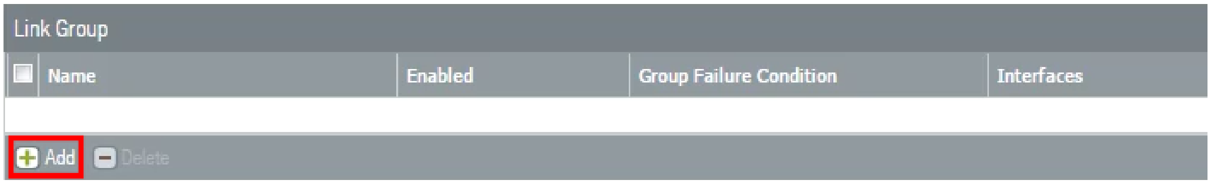
☑ Enabled

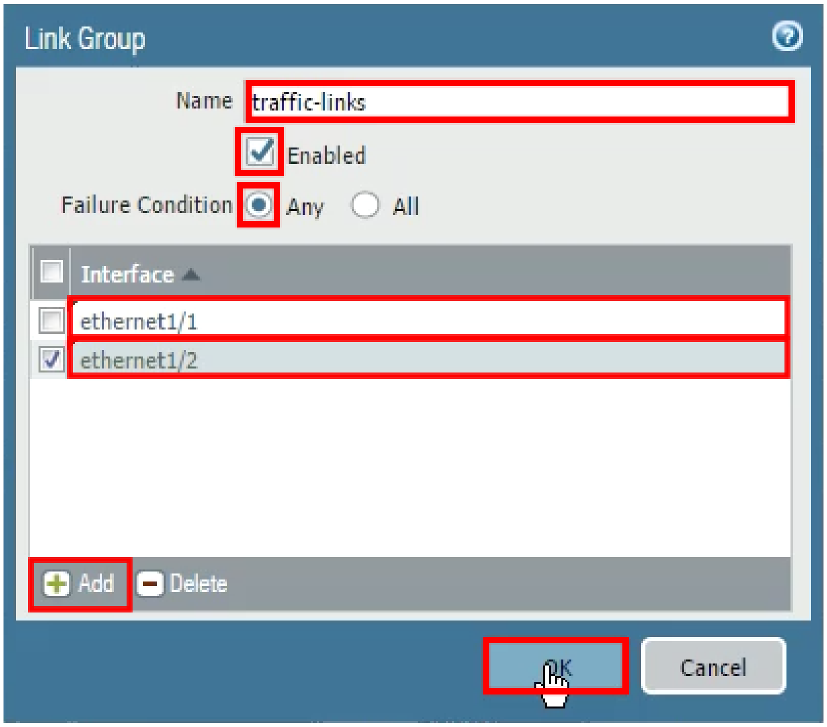
Failure Condition ● Any ○ All

3. Click **OK** to close the *Link Monitoring* configuration window.

4. Click **Add** in the Link Group panel to configure the traffic links to monitor:

Parameter	**Value**
Name	`traffic-links`
Enabled	☑ Enabled
Failure Condition	**Any**
Interface	**ethernet1/1** **ethernet1/2**




Link Group

Name: traffic-links

☑ Enabled

Failure Condition ● Any ○ All

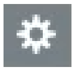
□	Interface ▲
□	ethernet1/1
☑	ethernet1/2

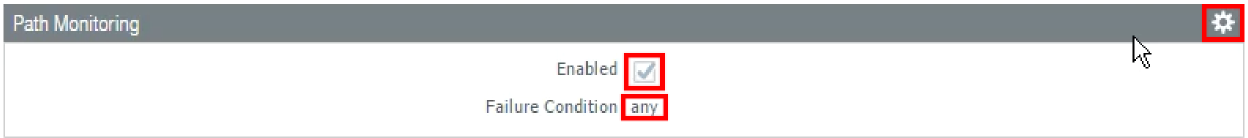
5. Click **OK** to close the *Link Group* configuration window.

6. Click the **Edit** icon of 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.

Parameter	**Value**
Enabled	☑ Enabled
Failure Condition	**Any**

Copyright © 2017 Network Development Group, Inc. www.netdevgroup.com





Path Monitoring

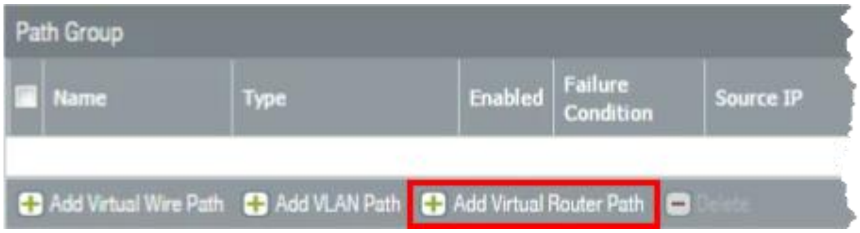
Enabled ☑

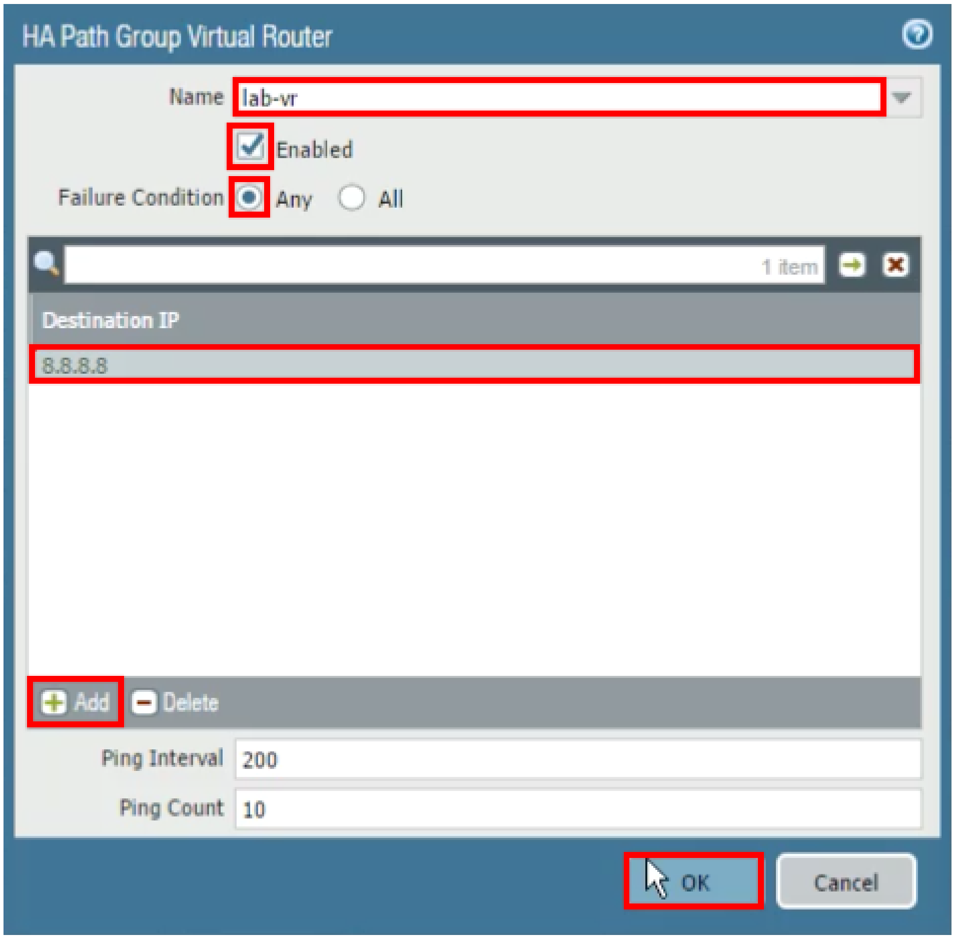
Failure Condition any

7. Click **OK** to close the *Path Monitoring* configuration window.

8. Find the Path Group panel and click **Add Virtual Router Path** to configure the path failure condition:

Parameter	**Value**
Name	`lab-vr`
Enabled	☑ Enabled
Failure Condition	**Any**
Destination IP	`8.8.8.8`





HA Path Group Virtual Router

Name lab-vr

☑ Enabled

Failure Condition ● Any ○ All

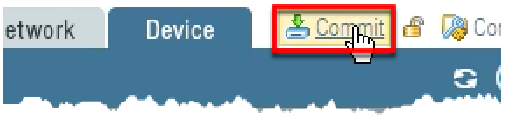
Destination IP
8.8.8.8

Ping Interval 200

Ping Count 10

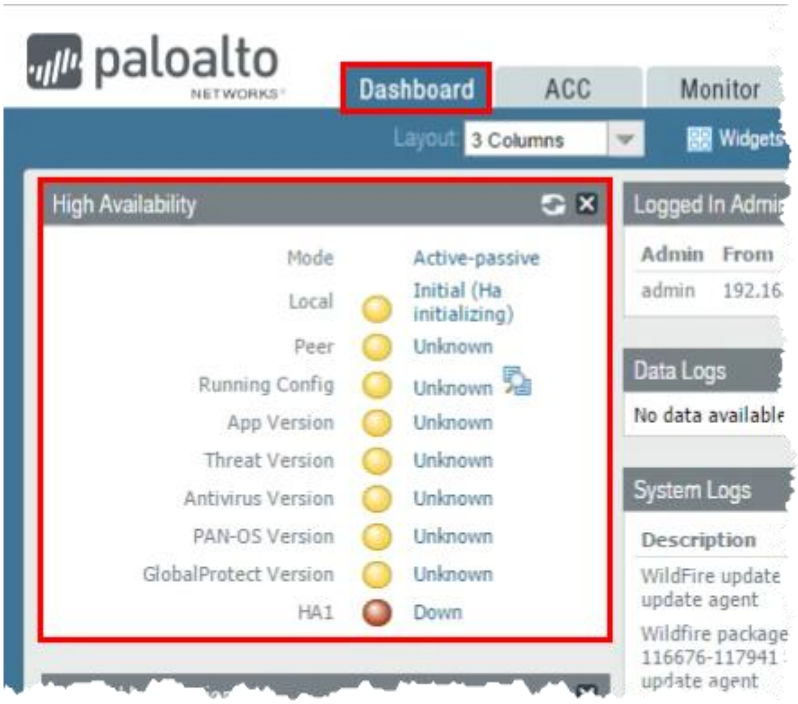
9. Click **OK** to close the HA Path Group Virtual Router configuration window.

10. **Commit** all changes.



13.5 Observe the HA Widget

1. In the WebUI 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). 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):



High Availability

Mode	Active-passive
Local	Initial (Ha initializing)
Peer	Unknown
Running Config	Unknown
App Version	Unknown
Threat Version	Unknown
Antivirus Version	Unknown
PAN-OS Version	Unknown
GlobalProtect Version	Unknown
HA1	Down

Logged In Admi

Admin	From
admin	192.16

Data Logs

No data available

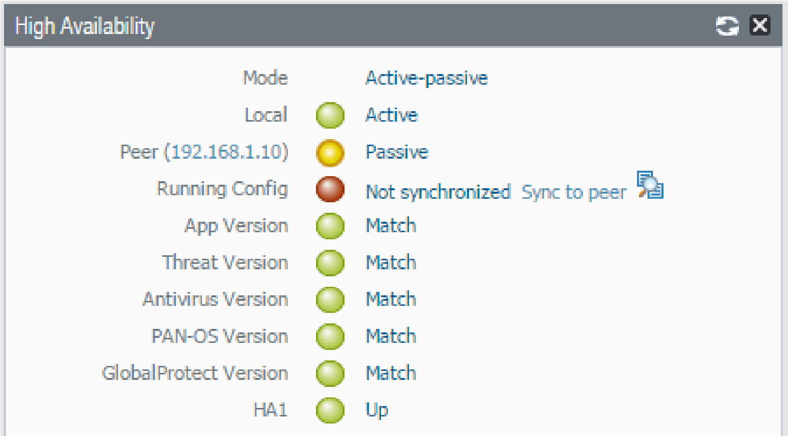
System Logs

Description

WildFire update
update agent

Wildfire package
116676-117941
update agent

2. If a peer was configured and was operating in passive mode, the High Availability widget on the Dashboard would appear as follows. In order 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.


High Availability

Mode	Active-passive
Local	Active
Peer (192.168.1.10)	Passive
Running Config	Not synchronized Sync to peer
App Version	Match
Threat Version	Match
Antivirus Version	Match
PAN-OS Version	Match
GlobalProtect Version	Match
HA1	Up

Stop. This is the end of the Active/Passive High Availability lab.