How to Configure OSPF

Tech Note

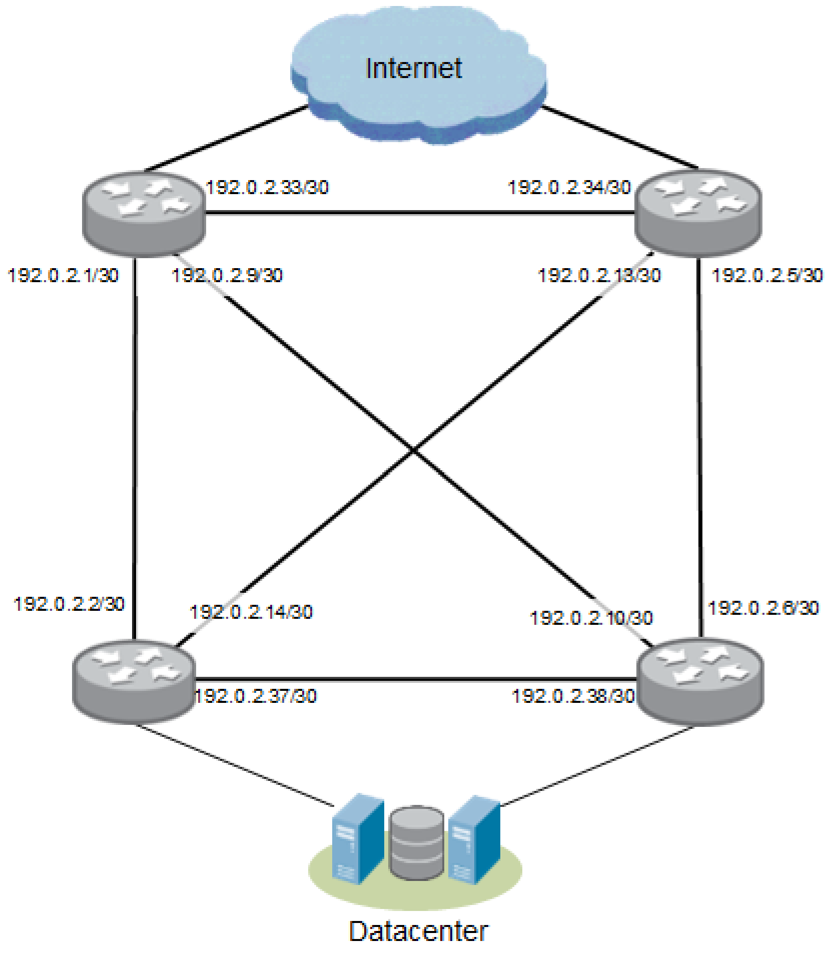
Revision A

This document gives step by step instructions for configuring and testing OSPF using Palo Alto Networks devices in both an Active/Passive and Active/Active scenario. The configuration examples that follow were performed on devices running PAN-OS 4.0.

Typical Topology

A common architecture for a datacenter edge utilizes BGP at the internet border and OSPF down to the access layer. Integrating a security solution into this model can present many problems, as it often requires breaking the architecture model by introducing Layer 2 elements, proprietary HA protocols, and floating IP addresses, all of which can make troubleshooting and tuning difficult.

Below is a sample diagram of a highly available routed infrastructure for an Internet datacenter. This design uses BGP at the Internet edge and OSPF to the distribution layer.



Design Objective

The primary objective of this design is to maintain the existing level of performance and availability without adding complexity. As it is well understood, OSPF is easy to implement and troubleshoot, provides the ability to perform traffic engineering, and has near-universal support among network vendors. By avoiding the addition of any layer 2 elements or new proprietary failover mechanisms, we can minimize the operational impact for both the network and security engineers

To meet these design objectives, Palo Alto Networks Next Generation Firewalls can be integrated with the existing OSPF architecture as an additional HA hop.

This document will discuss two scenarios:

Scenario 1: OSPF with Active/Passive High Availability
Scenario 2: OSPF with Active/Active High Availability

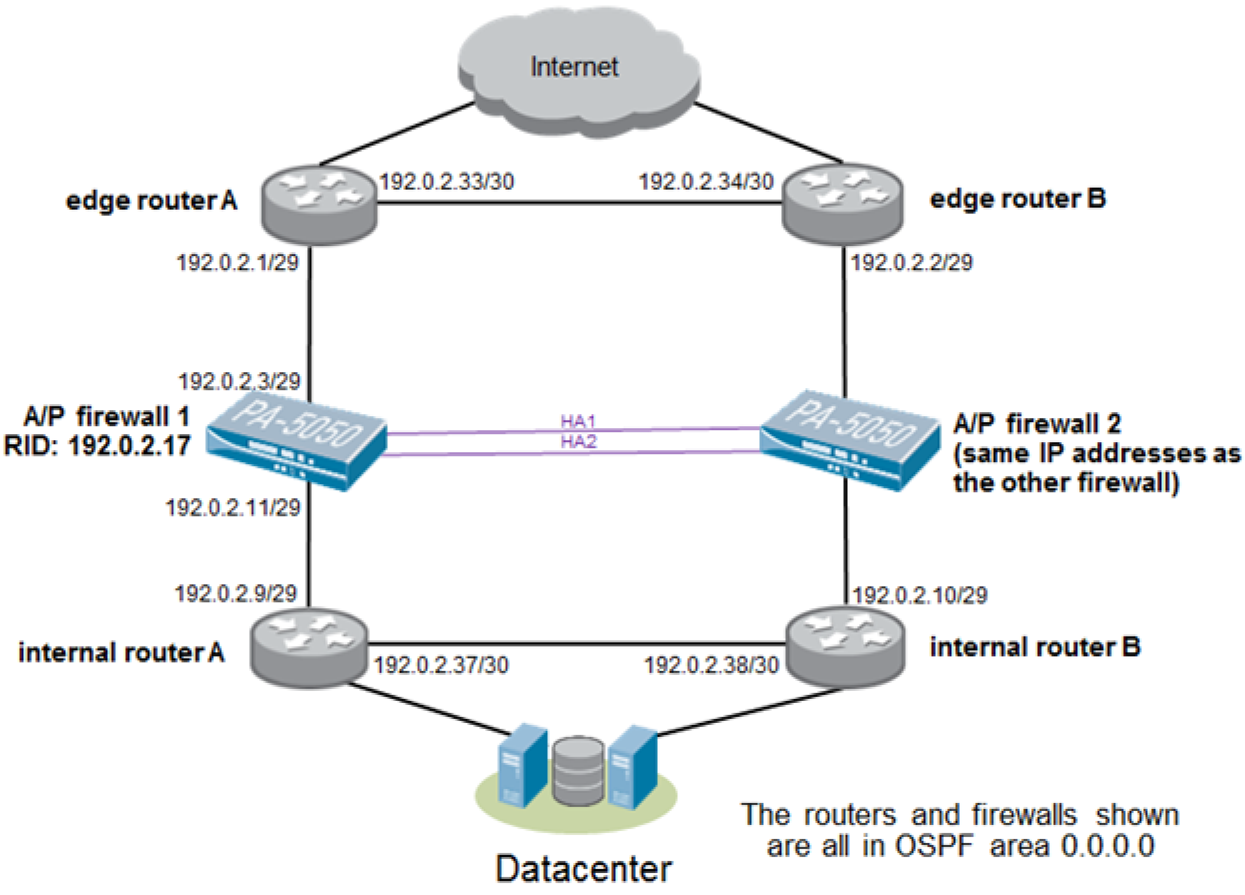
Preparation Steps

- You should have two Palo Alto Networks devices that will be used in the HA pair that are the same model and have the same version of the PAN-OS.

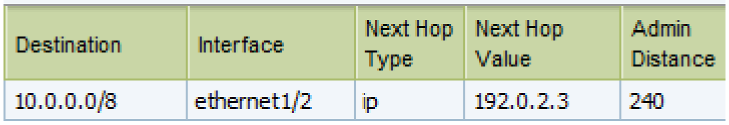
- You will need the following information:
  - IP addresses for your interfaces
  - IP addresses for your HA configuration
  - Your OSPF area number

Scenario 1: OSPF with Active/Passive High Availability

The following is a diagram of what will be implemented for scenario #1:

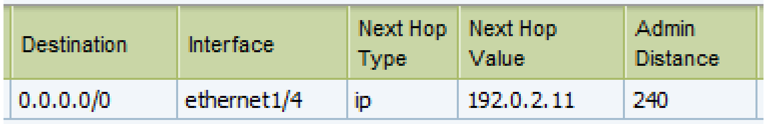


Note: In the above scenario, floating static routes should be configured on the upstream and downstream routers, to prevent a firewall failure from being noticed by users. For example, the upstream router would have a route to the datacenter networks that shows the following:



Destination	Interface	Next Hop Type	Next Hop Value	Admin Distance
10.0.0.0/8	ethernet1/2	ip	192.0.2.3	240

Notice that the cost of this route is set to a higher value than the OSPF route for the same destination network. Same would be true on the internal routers, configure a route as follows:



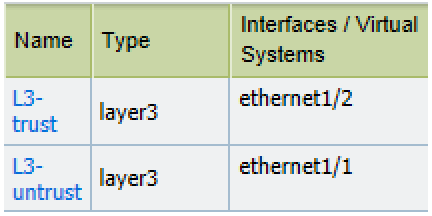
Destination	Interface	Next Hop Type	Next Hop Value	Admin Distance
0.0.0.0/0	ethernet1/4	ip	192.0.2.11	240

With these two routes in place, if the active firewall fails, that route will be used during the time needed for OSPF to re-converge. Once OSPF re-converges, the OSPF routes will take effect as designed.

Configuration for the Active/Passive Pair

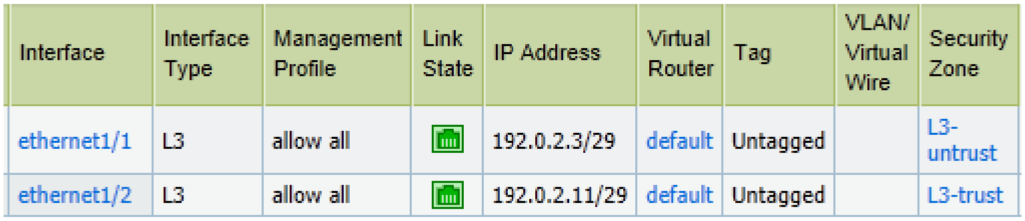
First, you will configure the zones, interfaces, policies, as well as HA.

1. On the first firewall, go to the Network tab-> Zones screen. Create zones for the internal and external interfaces. This will be the same configuration for each firewall in the pair as follows:



Name	Type	Interfaces / Virtual Systems
L3-trust	layer3	ethernet1/2
L3-untrust	layer3	ethernet1/1

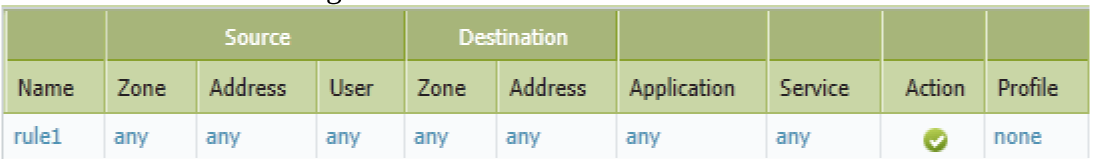
2. On the Network tab -> Interfaces screen, configure the interfaces as appropriate. An example configuration follows:



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
ethernet1/1	L3	allow all	🟩	192.0.2.3/29	default	Untagged		L3-untrust
ethernet1/2	L3	allow all	🟩	192.0.2.11/29	default	Untagged		L3-trust

Note: The device being used in this example has built-in HA interfaces, therefore no traffic ports were configured as interface type “HA”. If the device you are configuring does not have built-in HA interfaces, you must configure two interfaces to be type “HA”.

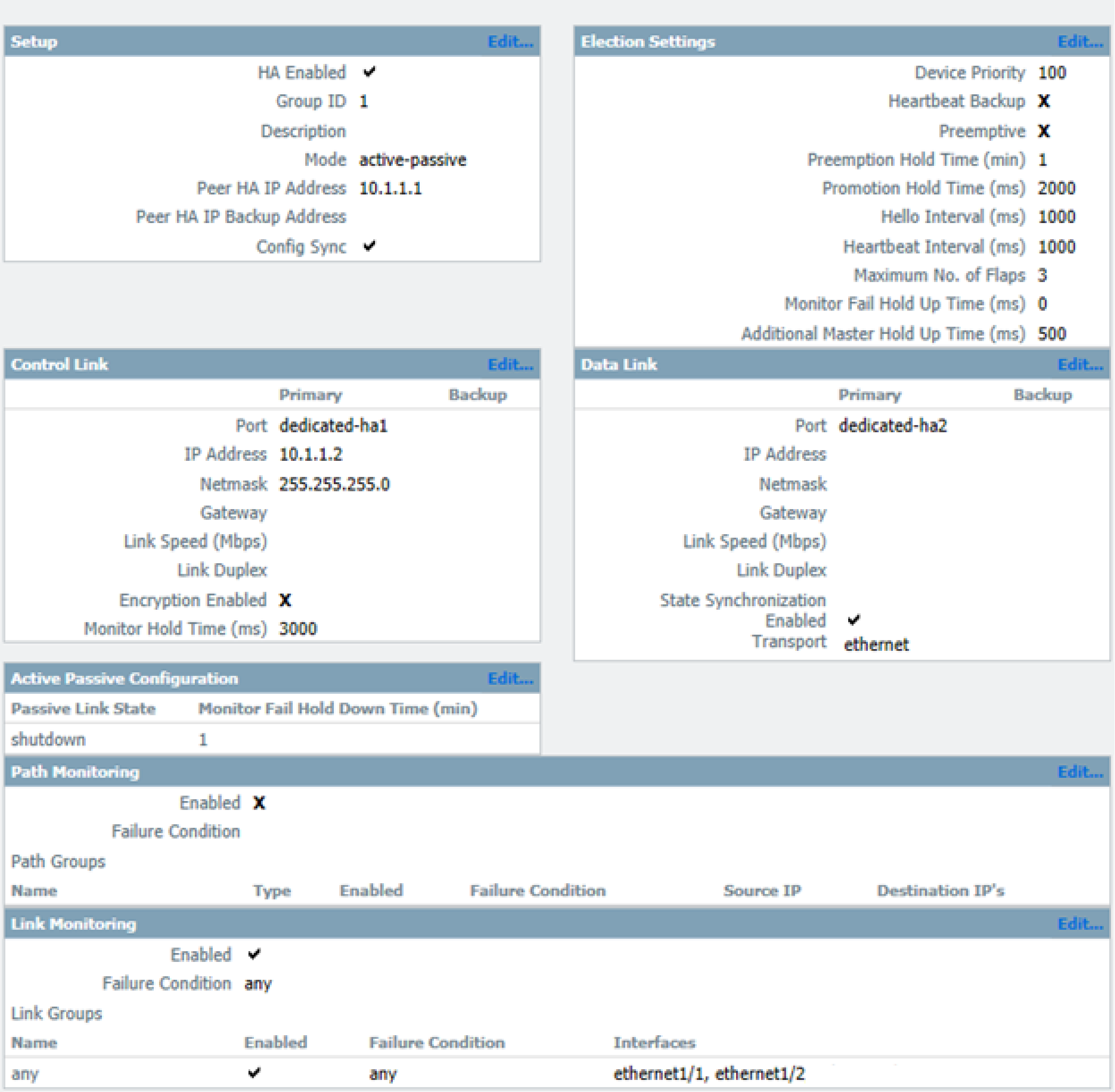
3. On the Policies tab -> Security screen, configure policies as you see fit. In this example, all traffic is allowed through the device as follows:



	Source			Destination					
Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile
rule1	any	any	any	any	any	any	any	✓	none

4. Now configure the devices as an Active/Passive HA pair. For these steps, refer to the following article on Active/Passive HA in the Palo Alto Networks Knowledgebase: https://live.paloaltonetworks.com/docs/DOC-1160

   Following is the HA configuration for the first firewall:



Setup Edit...

HA Enabled	✓
Group ID	1
Description	
Mode	active-passive
Peer HA IP Address	10.1.1.1
Peer HA IP Backup Address	
Config Sync	✓

Election Settings Edit...

Device Priority	100
Heartbeat Backup	X
Preemptive	X
Preemption Hold Time (min)	1
Promotion Hold Time (ms)	2000
Hello Interval (ms)	1000
Heartbeat Interval (ms)	1000
Maximum No. of Flaps	3
Monitor Fail Hold Up Time (ms)	0
Additional Master Hold Up Time (ms)	500

Control Link Edit...

	Primary	Backup
Port	dedicated-ha1	
IP Address	10.1.1.2	
Netmask	255.255.255.0	
Gateway		
Link Speed (Mbps)		
Link Duplex		
Encryption Enabled	X	
Monitor Hold Time (ms)	3000	

Data Link Edit...

	Primary	Backup
Port	dedicated-ha2	
IP Address		
Netmask		
Gateway		
Link Speed (Mbps)		
Link Duplex		
State Synchronization Enabled	✓	
Transport	ethernet	

Active Passive Configuration Edit...

Passive Link State	Monitor Fail Hold Down Time (min)
shutdown	1

Path Monitoring Edit...

Enabled	X
Failure Condition	

Path Groups

Name	Type	Enabled	Failure Condition	Source IP	Destination IP's

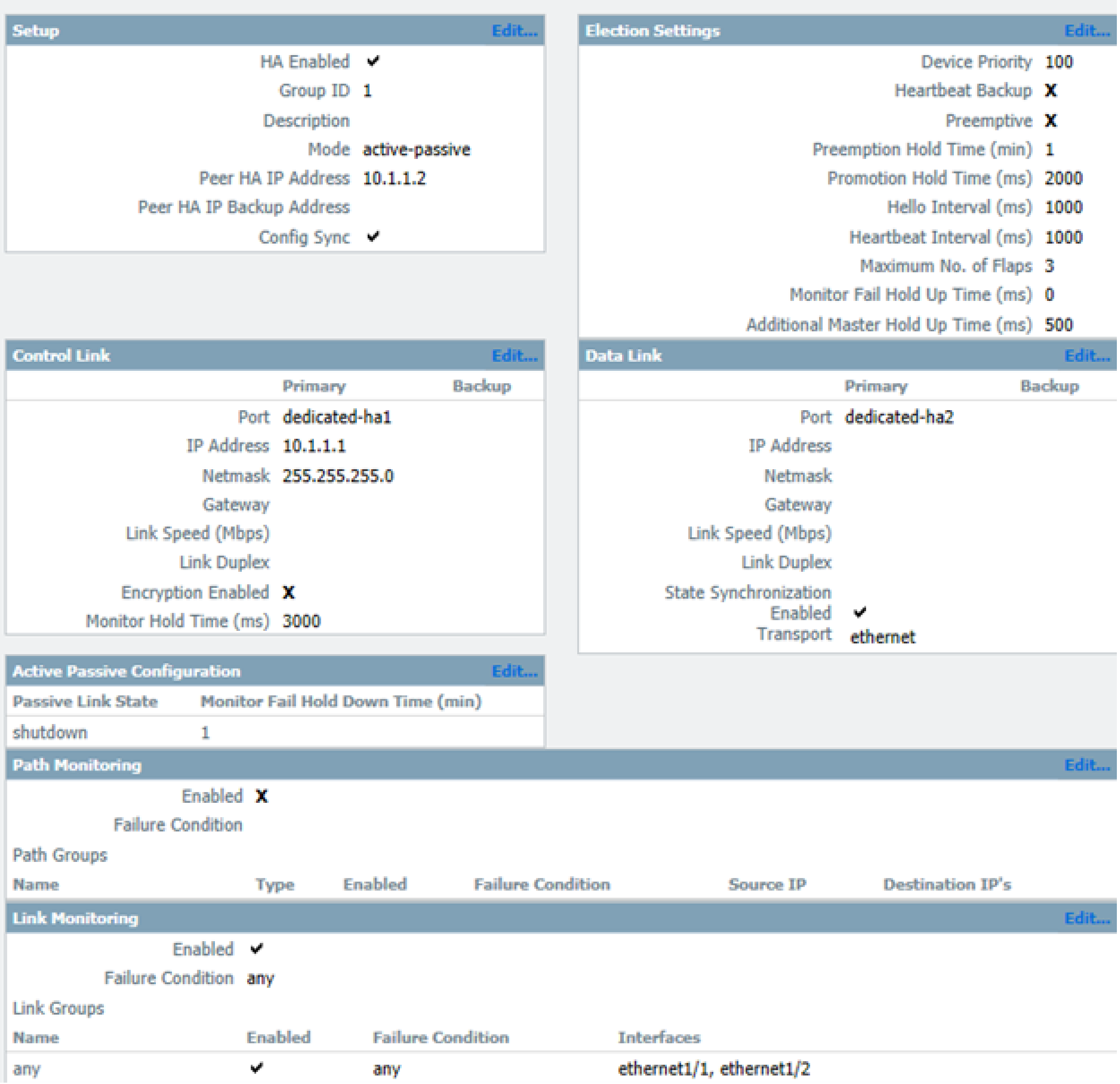
Link Monitoring Edit...

Enabled	✓
Failure Condition	any

Link Groups

Name	Enabled	Failure Condition	Interfaces
any	✓	any	ethernet1/1, ethernet1/2

HA configuration for the second firewall:



Setup

HA Enabled	✔
Group ID	1
Description	
Mode	active-passive
Peer HA IP Address	10.1.1.2
Peer HA IP Backup Address	
Config Sync	✔

Election Settings

Device Priority	100
Heartbeat Backup	X
Preemptive	X
Preemption Hold Time (min)	1
Promotion Hold Time (ms)	2000
Hello Interval (ms)	1000
Heartbeat Interval (ms)	1000
Maximum No. of Flaps	3
Monitor Fail Hold Up Time (ms)	0
Additional Master Hold Up Time (ms)	500

Control Link

	Primary	Backup
Port	dedicated-ha1	
IP Address	10.1.1.1	
Netmask	255.255.255.0	
Gateway		
Link Speed (Mbps)		
Link Duplex		
Encryption Enabled	X	
Monitor Hold Time (ms)	3000	

Data Link

	Primary	Backup
Port	dedicated-ha2	
IP Address		
Netmask		
Gateway		
Link Speed (Mbps)		
Link Duplex		
State Synchronization Enabled	✔	
Transport	ethernet	

Active Passive Configuration

Passive Link State	Monitor Fail Hold Down Time (min)
shutdown	1

Path Monitoring

Enabled	X
Failure Condition	

Path Groups

Name	Type	Enabled	Failure Condition	Source IP	Destination IP's

Link Monitoring

Enabled	✔
Failure Condition	any

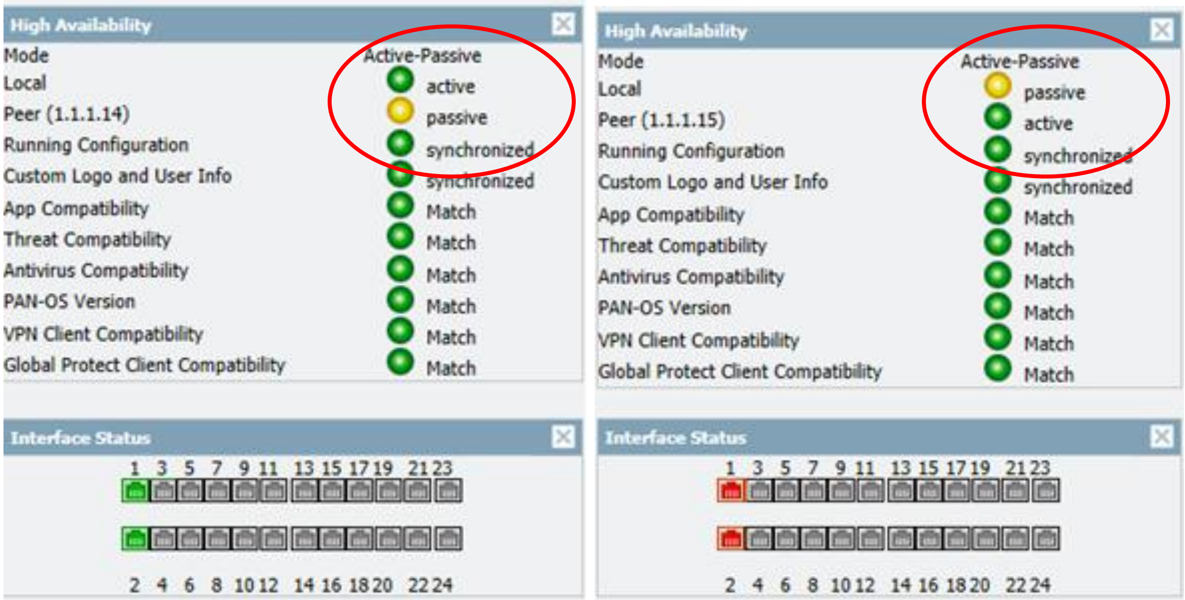
Link Groups

Name	Enabled	Failure Condition	Interfaces
any	✔	any	ethernet1/1, ethernet1/2

Note: For faster failover times, it is recommended that you configure the passive link state to "auto".

5. Commit the configuration.

6. Confirm that one device becomes active and the other device becomes passive. Also, push the configuration from one device to the other to sync the configurations of the HA pair. Here is a view of the High Availability widget from the Dashboard screen of each device:



High Availability

Mode	Active-Passive
Local	● active
Peer (1.1.1.14)	● passive
Running Configuration	● synchronized
Custom Logo and User Info	● synchronized
App Compatibility	● Match
Threat Compatibility	● Match
Antivirus Compatibility	● Match
PAN-OS Version	● Match
VPN Client Compatibility	● Match
Global Protect Client Compatibility	● Match

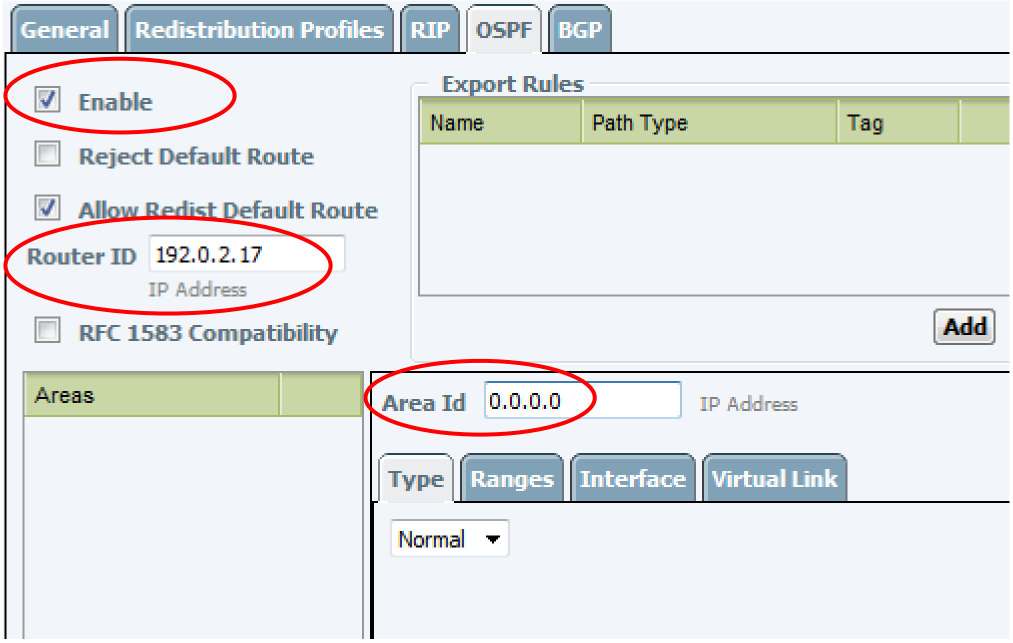
High Availability

Mode	Active-Passive
Local	● passive
Peer (1.1.1.15)	● active
Running Configuration	● synchronized
Custom Logo and User Info	● synchronized
App Compatibility	● Match
Threat Compatibility	● Match
Antivirus Compatibility	● Match
PAN-OS Version	● Match
VPN Client Compatibility	● Match
Global Protect Client Compatibility	● Match

If you have problems with High Availability, check the system log for errors.

Next, you will configure OSPF.

7. On one of the firewalls, go to the Network tab-> Virtual Routers screen. Edit the virtual router. On the OSPF tab, enable OSPF, configure the Router ID, and create a new OSPF area by entering the appropriate area ID. In this example, area ID 0.0.0.0 is used.



☑ Enable

□ Reject Default Route

☑ Allow Redist Default Route

Router ID 192.0.2.17
IP Address

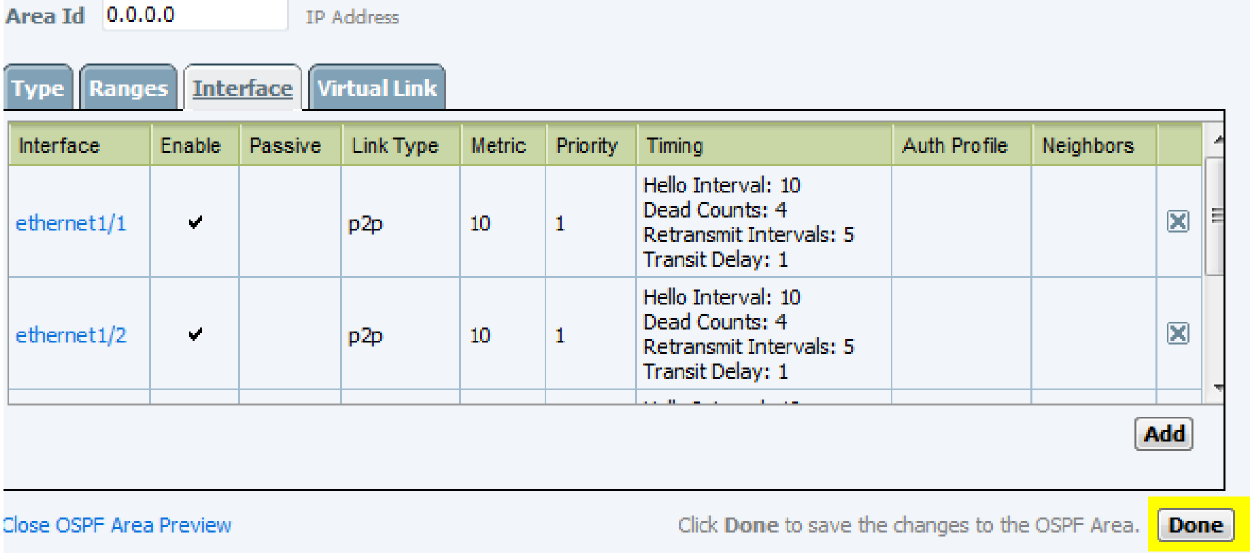
□ RFC 1583 Compatibility

Name	Path Type	Tag

Area Id 0.0.0.0 IP Address

Type: Normal

8. In the Area ID portion of the above screen, click on the Interface tab. Add all interfaces which you want to send/receive OSPF messages. In this example, all 4 traffic interfaces will be added. Configure the link type as “p2p”, since there is no need for a DR or BDR to be selected on that path. Once you add all the interfaces, click “Done” to complete the process of adding the area.



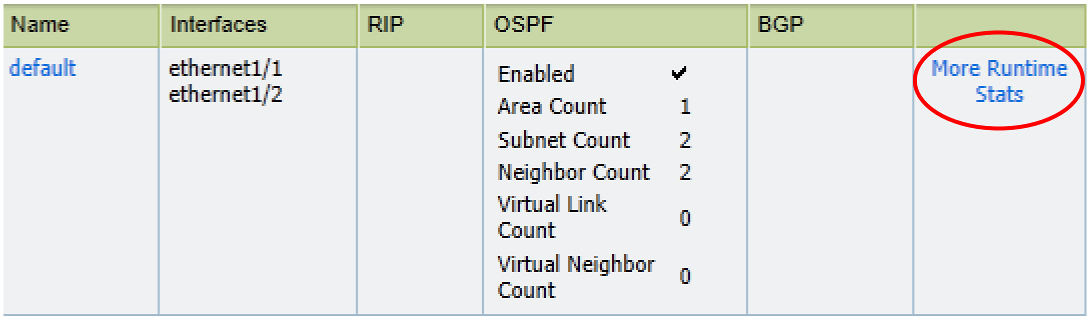
Area Id 0.0.0.0 IP Address

Interface	Enable	Passive	Link Type	Metric	Priority	Timing	Auth Profile	Neighbors
ethernet1/1	✔		p2p	10	1	Hello Interval: 10 Dead Counts: 4 Retransmit Intervals: 5 Transit Delay: 1		
ethernet1/2	✔		p2p	10	1	Hello Interval: 10 Dead Counts: 4 Retransmit Intervals: 5 Transit Delay: 1		

Click Done to save the changes to the OSPF Area.

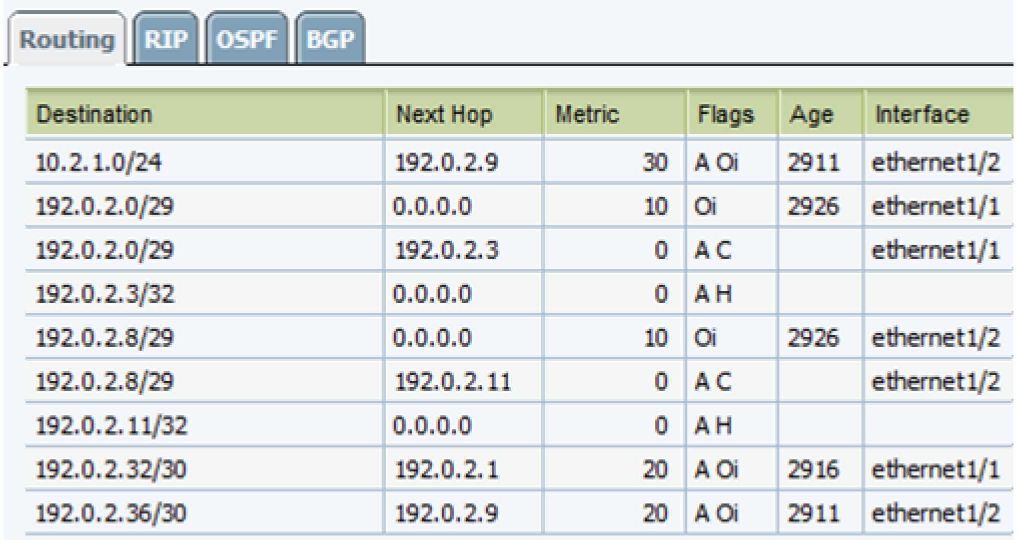
9. Commit the configuration on that device. During the commit process, the configuration will be synchronized with the other device.

10. Confirm that your OSPF peers are communicating with each other. On the active firewall, go to the Network tab -> Virtual Router screen and click on "More Runtime Stats":



Name	Interfaces	RIP	OSPF	BGP	
default	ethernet1/1 ethernet1/2		Enabled ✓ Area Count 1 Subnet Count 2 Neighbor Count 2 Virtual Link Count 0 Virtual Neighbor Count 0		More Runtime Stats

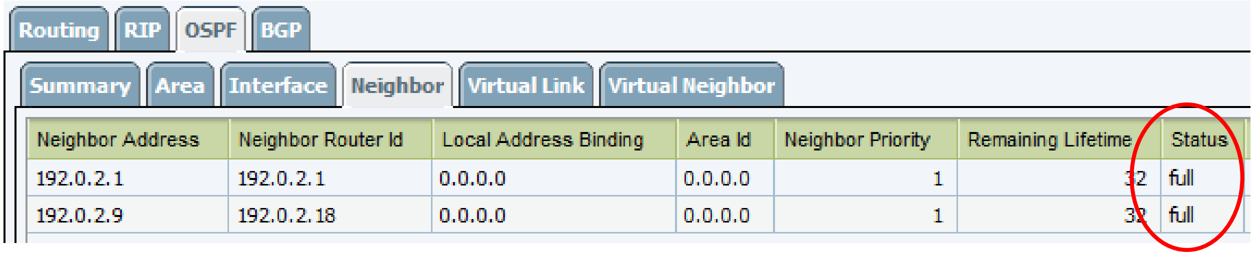
On the Routing tab, look for routes that were learned via OSPF ("O" flag). Routes that are inactive will not have the letter "A" in the Flags column.



Destination	Next Hop	Metric	Flags	Age	Interface
10.2.1.0/24	192.0.2.9	30	A Oi	2911	ethernet1/2
192.0.2.0/29	0.0.0.0	10	Oi	2926	ethernet1/1
192.0.2.0/29	192.0.2.3	0	A C		ethernet1/1
192.0.2.3/32	0.0.0.0	0	A H		
192.0.2.8/29	0.0.0.0	10	Oi	2926	ethernet1/2
192.0.2.8/29	192.0.2.11	0	A C		ethernet1/2
192.0.2.11/32	0.0.0.0	0	A H		
192.0.2.32/30	192.0.2.1	20	A Oi	2916	ethernet1/1
192.0.2.36/30	192.0.2.9	20	A Oi	2911	ethernet1/2

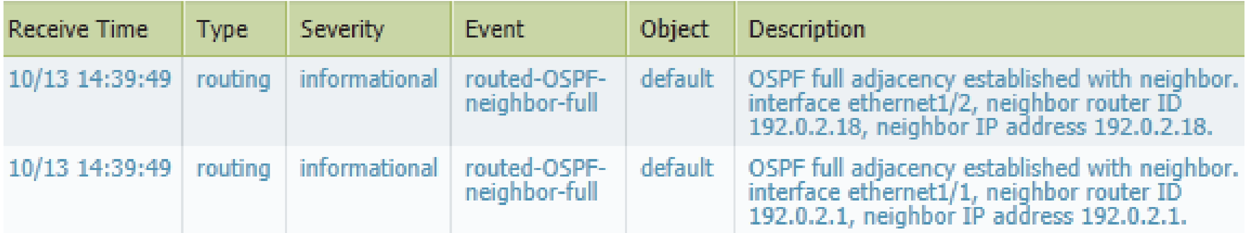
The routing table should also show internal network routes, as well as a default route propagated from the upstream routers.

11. Also go to OSPF -> Neighbor tab, and confirm the device has OSPF adjacencies established:



Neighbor Address	Neighbor Router Id	Local Address Binding	Area Id	Neighbor Priority	Remaining Lifetime	Status
192.0.2.1	192.0.2.1	0.0.0.0	0.0.0.0	1	32	full
192.0.2.9	192.0.2.18	0.0.0.0	0.0.0.0	1	32	full

You can also confirm that the OSPF connections are established by examining the Monitor tab -> System log:



Receive Time	Type	Severity	Event	Object	Description
10/13 14:39:49	routing	informational	routed-OSPF-neighbor-full	default	OSPF full adjacency established with neighbor. interface ethernet1/2, neighbor router ID 192.0.2.18, neighbor IP address 192.0.2.18.
10/13 14:39:49	routing	informational	routed-OSPF-neighbor-full	default	OSPF full adjacency established with neighbor. interface ethernet1/1, neighbor router ID 192.0.2.1, neighbor IP address 192.0.2.1.

12. On the upstream router, configure a floating static route to point traffic going to the internal subnet to use the gateway address 192.0.2.3. Configure the Administrative Distance on the static route to be higher than OSPF or other dynamic routing protocols in the network. This floating static route will need to be redistributed upstream, if not done so already.

13. On the downstream router, configure a floating static route to point traffic going to the Internet to use the gateway address 192.0.2.11. As in the last step, set a high Administrative Distance and redistribute this route downstream.

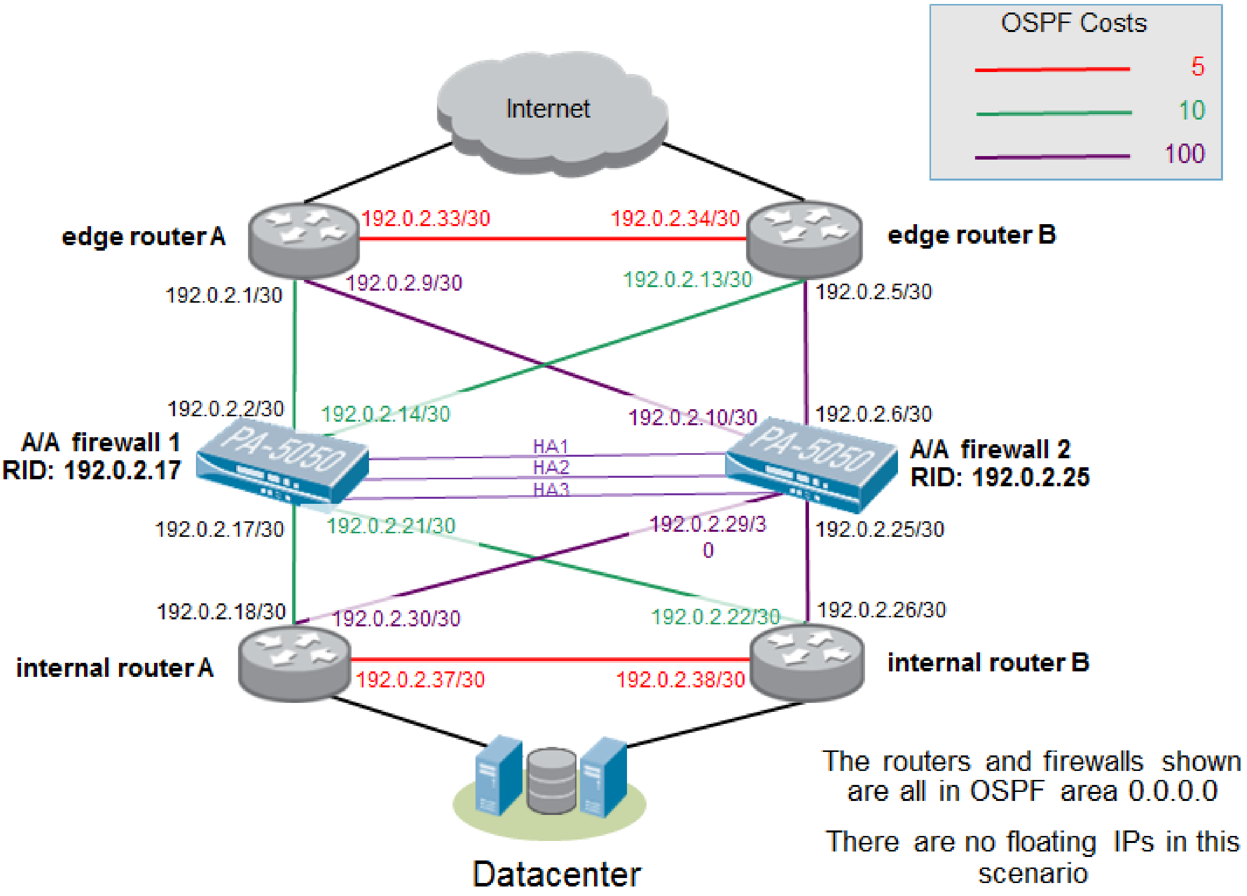
14. Examine the firewall’s routing table. Confirm that the floating static routes from the upstream and downstream routers appear. The floating static routes **will not** have an “A” in the flags column, as those routes are inactive. Those routes are ready to take over in case the OSPF routes disappear.

15. At this point, you can test your setup by sending pings through the network. Test with one firewall as the active device, put that device into a “suspended” HA state (Device tab -> High Availability screen), and watch the secondary take over. Confirm that pings flow through the second device. Make the original firewall functional, and fail the second device. Pings should still continue to flow.

Scenario 2: OSPF with Active/Active High Availability

In this scenario, the firewalls are deployed in Active/Active HA. This design supports asymmetric traffic, traffic engineering, and consistent deterministic failover behavior. In testing, this design proved to be highly resilient and fast to recover. This design can tolerate the loss of any two network connections without degrading performance or availability.

Following is a diagram of what will be implemented:



The routers and firewalls shown are all in OSPF area 0.0.0.0

There are no floating IPs in this scenario

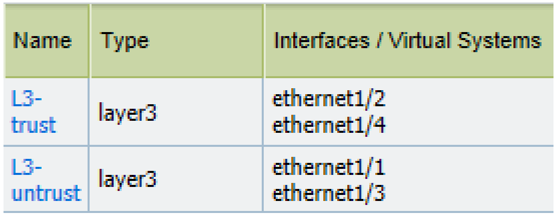
You should set the link costs such that certain routes will be preferred over other routes. The link costs are specified to keep the traffic routing symmetric. This also simplifies troubleshooting, packet captures, and firewall log monitoring.

Note: Floating IP addresses (“Virtual Address”) are typically used when the firewall is adjacent to end hosts. In this scenario, the firewall is directly connected to routers, so floating IP addresses are not used.

Configuration for the Active/Active Pair

In steps 1 - 7 you will configure the zones, interfaces, policies, as well as HA.

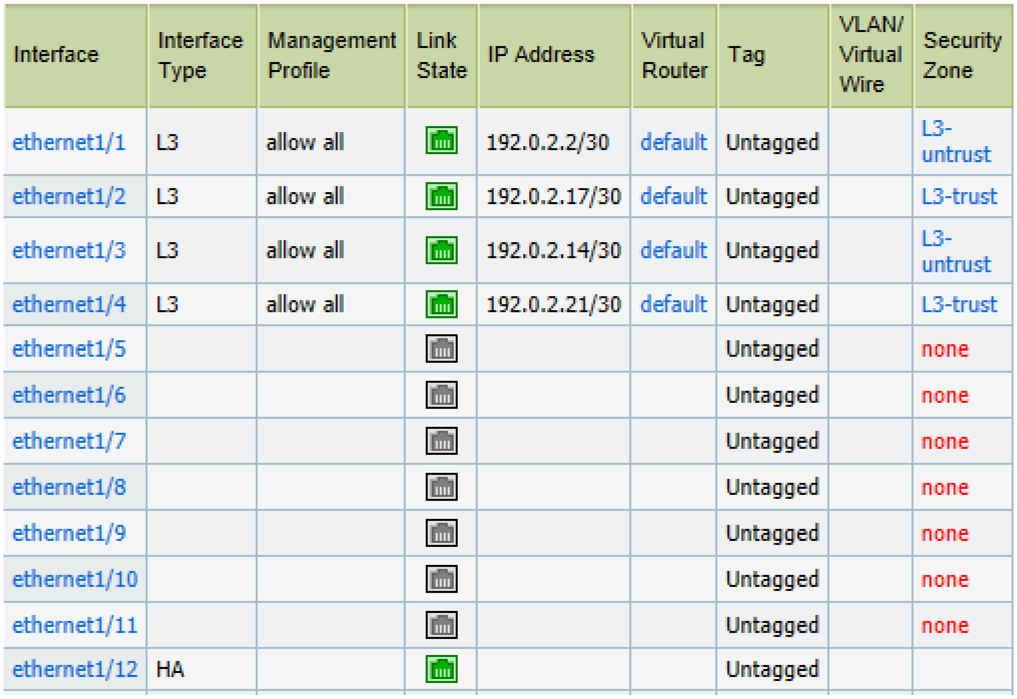
1. On the Network tab-> Zones screen of each firewall, create zones for the internal and external interfaces. This will be the same configuration for each firewall in the pair as follows:



Name	Type	Interfaces / Virtual Systems
L3-trust	layer3	ethernet1/2 ethernet1/4
L3-untrust	layer3	ethernet1/1 ethernet1/3

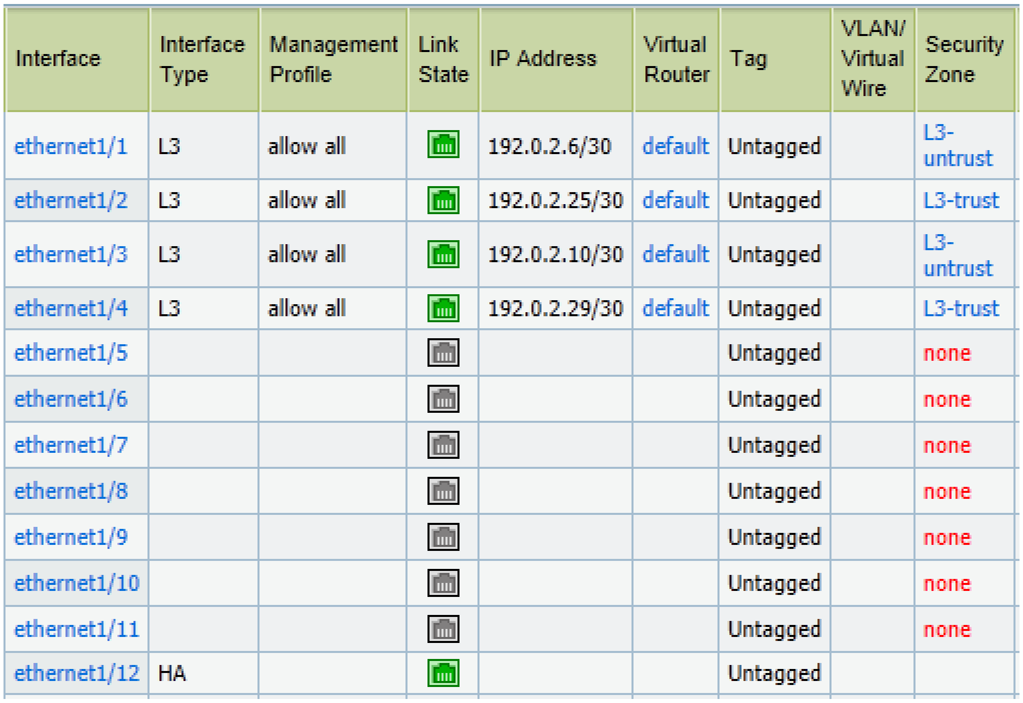
2. On the Network tab -> Interfaces screen, configure the interfaces as appropriate. Following are examples. The device shown has built-in HA1 and HA2 interfaces, and so a traffic port must be configured to be interface type HA (ethernet 1/12 in the example below). If your device does not have built-in HA interfaces, you must configure three traffic interfaces to be interface type HA, as those will be used for the HA1, HA2, and HA3 links.

   Interface configuration of the first firewall:



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
ethernet1/1	L3	allow all	🟩	192.0.2.2/30	default	Untagged		L3-untrust
ethernet1/2	L3	allow all	🟩	192.0.2.17/30	default	Untagged		L3-trust
ethernet1/3	L3	allow all	🟩	192.0.2.14/30	default	Untagged		L3-untrust
ethernet1/4	L3	allow all	🟩	192.0.2.21/30	default	Untagged		L3-trust
ethernet1/5			▨			Untagged		none
ethernet1/6			▨			Untagged		none
ethernet1/7			▨			Untagged		none
ethernet1/8			▨			Untagged		none
ethernet1/9			▨			Untagged		none
ethernet1/10			▨			Untagged		none
ethernet1/11			▨			Untagged		none
ethernet1/12	HA		🟩			Untagged		

Interface configuration of the second firewall:

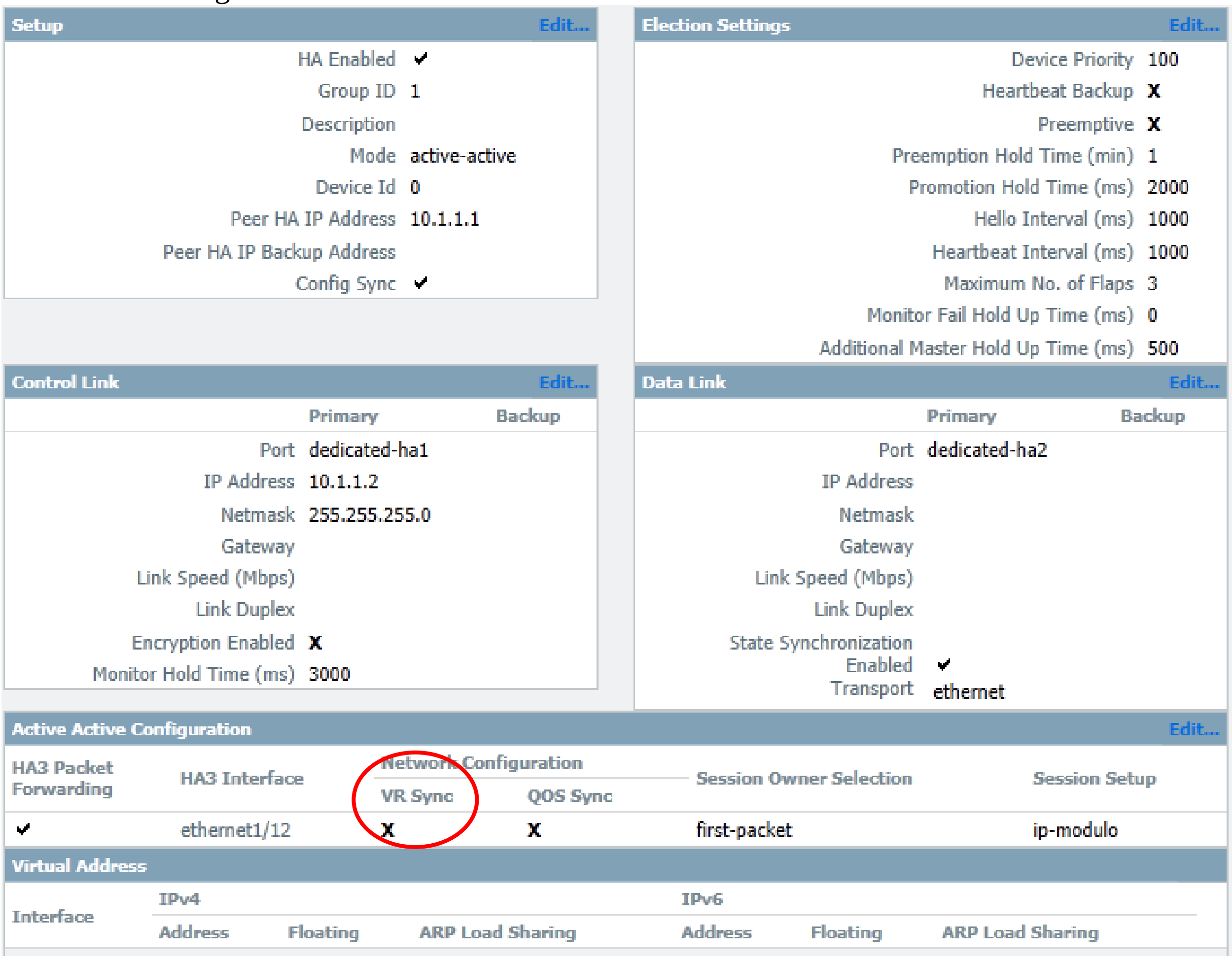


Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
ethernet1/1	L3	allow all	🟩	192.0.2.6/30	default	Untagged		L3-untrust
ethernet1/2	L3	allow all	🟩	192.0.2.25/30	default	Untagged		L3-trust
ethernet1/3	L3	allow all	🟩	192.0.2.10/30	default	Untagged		L3-untrust
ethernet1/4	L3	allow all	🟩	192.0.2.29/30	default	Untagged		L3-trust
ethernet1/5			◼			Untagged		none
ethernet1/6			◼			Untagged		none
ethernet1/7			◼			Untagged		none
ethernet1/8			◼			Untagged		none
ethernet1/9			◼			Untagged		none
ethernet1/10			◼			Untagged		none
ethernet1/11			◼			Untagged		none
ethernet1/12	HA		🟩			Untagged		

3. Now configure HA as Active/Active. For details on the meanings of the settings, refer to the following article on Active/Active HA in the Palo Alto Networks Knowledgebase: https://live.paloaltonetworks.com/docs/DOC-1765

   Note: The path monitoring and link monitoring configurations are not shown below, but you should make sure that you configure those appropriately. Refer to the document above for help on configuring those settings.

   HA config of the first firewall:



Setup

HA Enabled	✓
Group ID	1
Description	
Mode	active-active
Device Id	0
Peer HA IP Address	10.1.1.1
Peer HA IP Backup Address	
Config Sync	✓

Election Settings

Device Priority	100
Heartbeat Backup	X
Preemptive	X
Preemption Hold Time (min)	1
Promotion Hold Time (ms)	2000
Hello Interval (ms)	1000
Heartbeat Interval (ms)	1000
Maximum No. of Flaps	3
Monitor Fail Hold Up Time (ms)	0
Additional Master Hold Up Time (ms)	500

Control Link

	Primary	Backup
Port	dedicated-ha1	
IP Address	10.1.1.2	
Netmask	255.255.255.0	
Gateway		
Link Speed (Mbps)		
Link Duplex		
Encryption Enabled	X	
Monitor Hold Time (ms)	3000	

Data Link

	Primary	Backup
Port	dedicated-ha2	
IP Address		
Netmask		
Gateway		
Link Speed (Mbps)		
Link Duplex		
State Synchronization Enabled	✓	
Transport	ethernet	

Active Active Configuration

HA3 Packet Forwarding	HA3 Interface	Network Configuration		Session Owner Selection	Session Setup
		VR Sync	QOS Sync		
✓	ethernet1/12	X	X	first-packet	ip-modulo

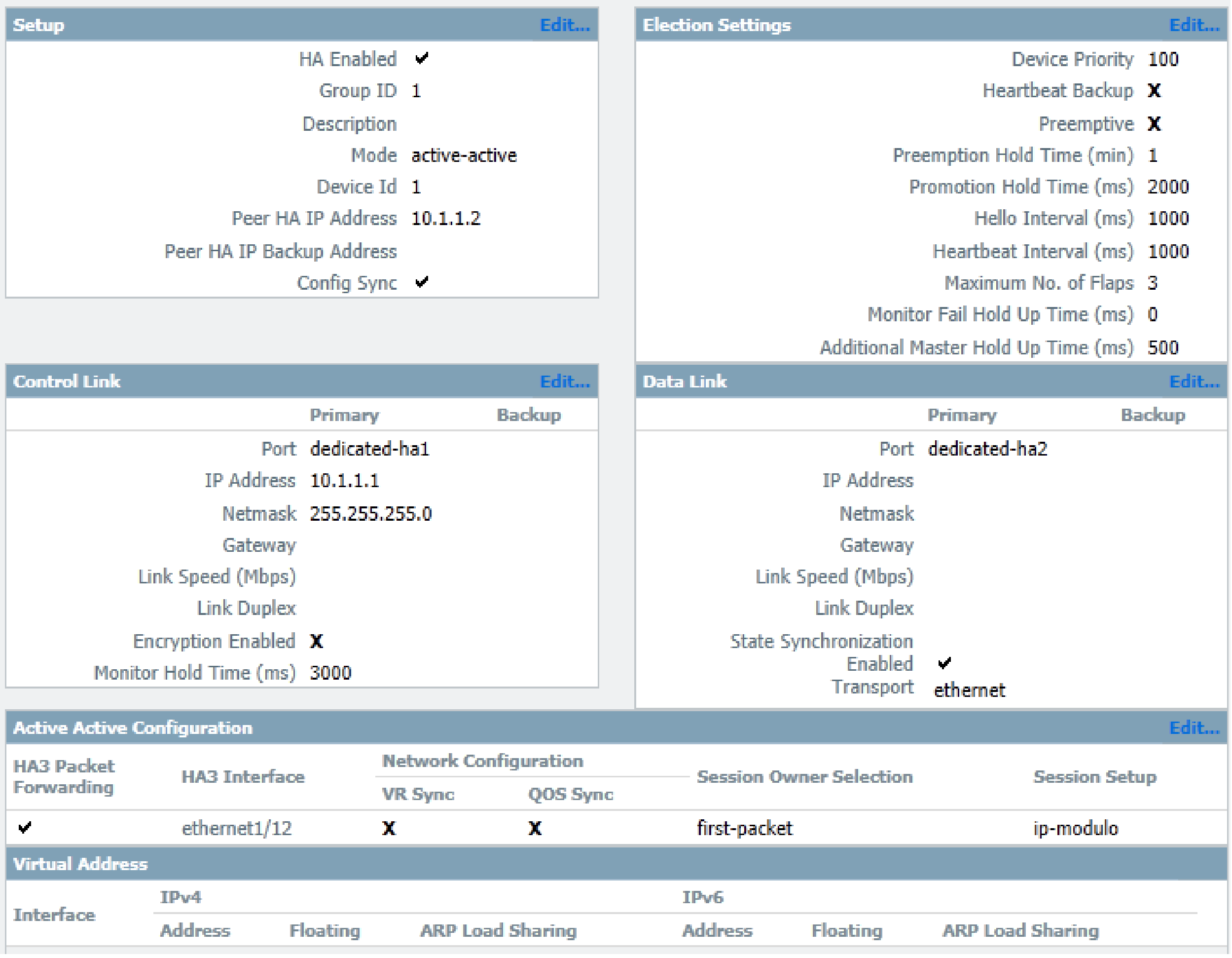
Virtual Address

Interface	IPv4			IPv6		
	Address	Floating	ARP Load Sharing	Address	Floating	ARP Load Sharing

   Notice that VR Sync is disabled. This setting is important for this type of configuration since both firewalls will be maintaining their own routing tables independently. This also allows the VR configuration to be unique on both firewalls in the HA pair.

   Also notice that a Virtual Address is not configured.

HA config for the second firewall:



Setup Edit...

HA Enabled	✓
Group ID	1
Description	
Mode	active-active
Device Id	1
Peer HA IP Address	10.1.1.2
Peer HA IP Backup Address	
Config Sync	✓

Election Settings Edit...

Device Priority	100
Heartbeat Backup	X
Preemptive	X
Preemption Hold Time (min)	1
Promotion Hold Time (ms)	2000
Hello Interval (ms)	1000
Heartbeat Interval (ms)	1000
Maximum No. of Flaps	3
Monitor Fail Hold Up Time (ms)	0
Additional Master Hold Up Time (ms)	500

Control Link Edit...

	Primary	Backup
Port	dedicated-ha1	
IP Address	10.1.1.1	
Netmask	255.255.255.0	
Gateway		
Link Speed (Mbps)		
Link Duplex		
Encryption Enabled	X	
Monitor Hold Time (ms)	3000	

Data Link Edit...

	Primary	Backup
Port	dedicated-ha2	
IP Address		
Netmask		
Gateway		
Link Speed (Mbps)		
Link Duplex		
State Synchronization Enabled	✓	
Transport	ethernet	

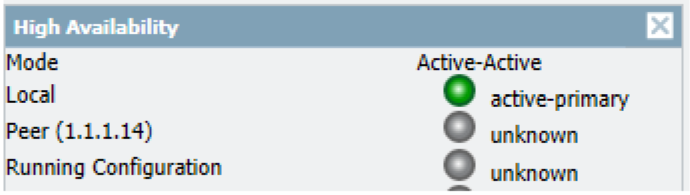
Active Active Configuration Edit...

HA3 Packet Forwarding	HA3 Interface	Network Configuration		Session Owner Selection	Session Setup
		VR Sync	QOS Sync		
✓	ethernet1/12	X	X	first-packet	ip-modulo

Virtual Address

Interface	IPv4			IPv6		
	Address	Floating	ARP Load Sharing	Address	Floating	ARP Load Sharing

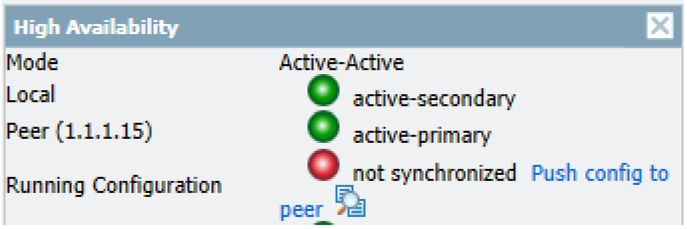
4. Commit the configuration on the first firewall. The first device that you perform commit on will become the active-primary firewall. You will push the config of the first firewall to the second firewall in a later step. Confirm that the first firewall is active-primary on the Dashboard screen:



High Availability

Mode	Active-Active
Local	● active-primary
Peer (1.1.1.14)	● unknown
Running Configuration	● unknown

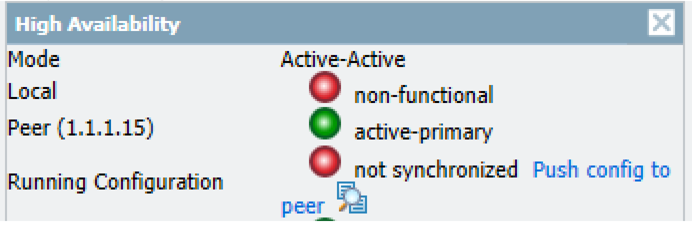
5. Commit the configuration on the second firewall. After the commit completes, you will see that the second firewall is in the active-secondary state and that the configs are not synchronized:



High Availability

Mode	Active-Active
Local	● active-secondary
Peer (1.1.1.15)	● active-primary
Running Configuration	● not synchronized Push config to peer

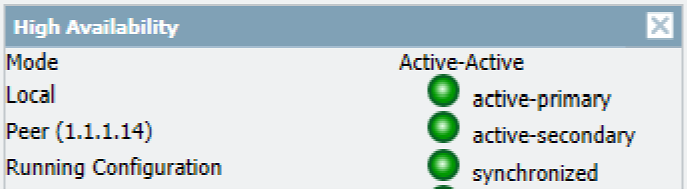
If the second comes up as non-functional as shown in the following screenshot, then check the system log for errors.



High Availability

Mode	Active-Active
Local	● non-functional
Peer (1.1.1.15)	● active-primary
Running Configuration	● not synchronized Push config to peer

6. View the HA widget on the active-primary firewall. Click "Push config to peer". After the synchronization completes, you will see the following:

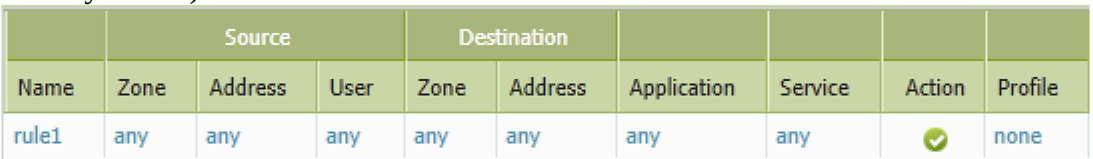


High Availability

Mode	Active-Active
Local	● active-primary
Peer (1.1.1.14)	● active-secondary
Running Configuration	● synchronized

At this point, the HA configuration is complete. The next steps will be to configure policies and OSPF.

7. Confirm that you have a policy that allows traffic through the device. (Policies tab -> Security screen)

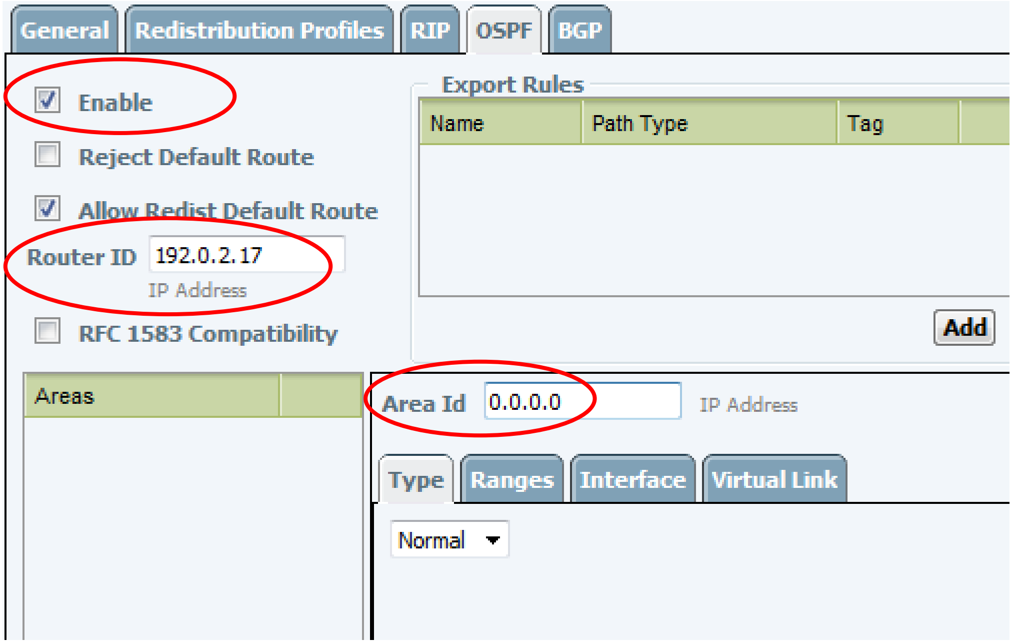


	Source			Destination					
Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile
rule1	any	any	any	any	any	any	any	✓	none

If you do not already have this policy in place, create one now on either firewall. The config change will be pushed to the other device during the commit process.

Next, you will configure OSPF.

8. On the Active-Primary firewall, go to the Network tab-> Virtual Routers screen. Edit the virtual router. On the OSPF tab, enable OSPF, configure the Router ID, and create a new OSPF area, entering the appropriate area ID. In this example, area ID 0.0.0.0 is used.



☑ Enable

□ Reject Default Route

☑ Allow Redist Default Route

Router ID 192.0.2.17 (IP Address)

□ RFC 1583 Compatibility

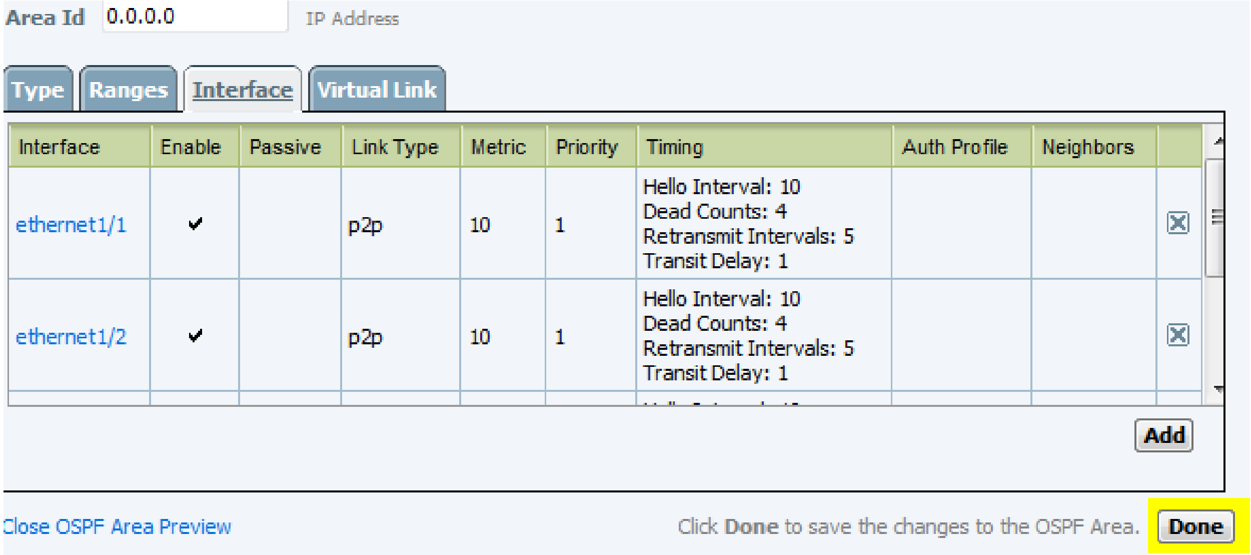
Name	Path Type	Tag

Areas

Area Id 0.0.0.0 (IP Address)

Type: Normal

9. In the Area ID portion of the above screen, click on the Interface tab. Add all interfaces which you want to send/receive OSPF messages. In this example, all 4 traffic interfaces will be added. Configure the link type as “p2p”, since there is no need for a DR or BDR to be selected on that path. Configure the costs as shown in the network diagram for this example. Once you add all the interfaces, click “Done” to complete the process of adding the area.



Area Id 0.0.0.0 (IP Address)

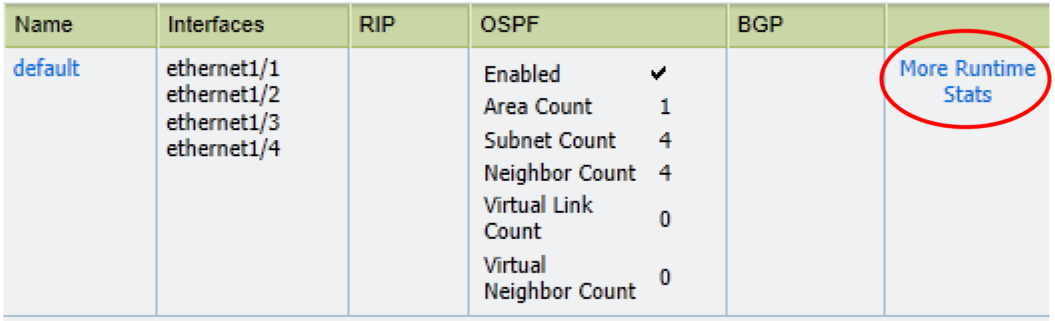
Interface	Enable	Passive	Link Type	Metric	Priority	Timing	Auth Profile	Neighbors
ethernet1/1	✓		p2p	10	1	Hello Interval: 10 Dead Counts: 4 Retransmit Intervals: 5 Transit Delay: 1		
ethernet1/2	✓		p2p	10	1	Hello Interval: 10 Dead Counts: 4 Retransmit Intervals: 5 Transit Delay: 1		

Click Done to save the changes to the OSPF Area.

10. Since the VR part of the configuration is not synchronized, repeat the previous two steps on the Active-Secondary firewall, specifying the proper router ID as well as a higher metric on the interfaces.

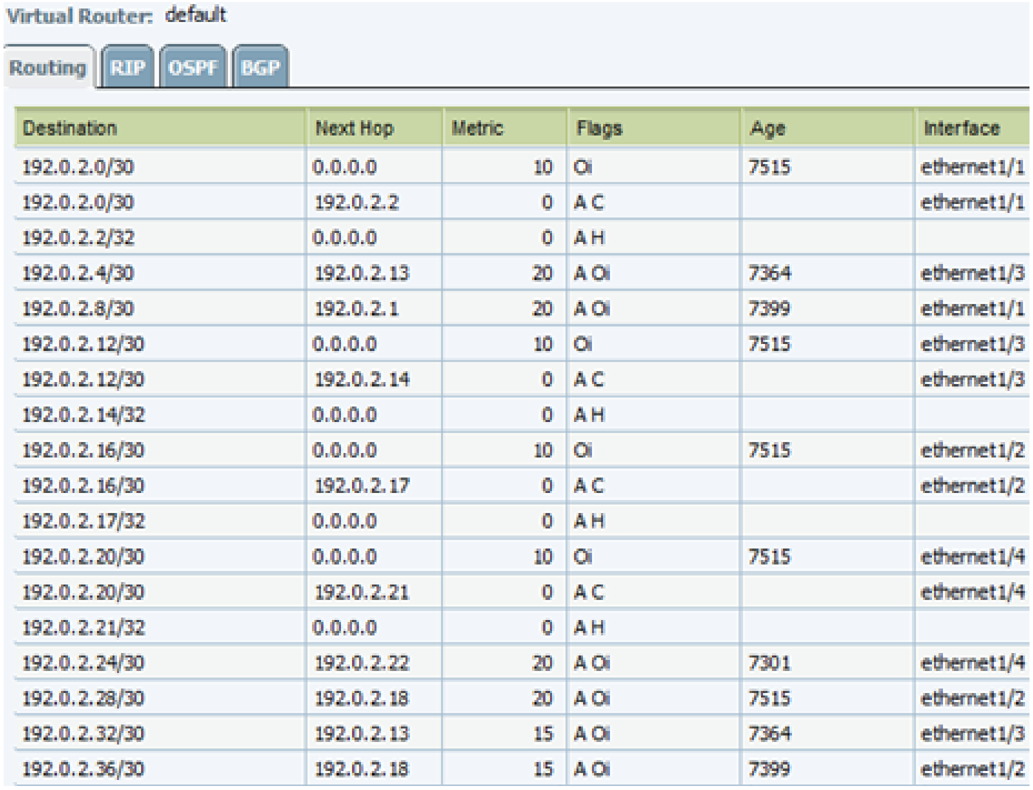
11. Commit the configuration on both devices since this part of the configuration is not synched automatically.

12. Confirm that your OSPF peers are communicating with each other. Go to the Network tab -> Virtual Router screen and click on "More Runtime Stats":



Name	Interfaces	RIP	OSPF	BGP	
default	ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/4		Enabled ✔ Area Count 1 Subnet Count 4 Neighbor Count 4 Virtual Link Count 0 Virtual Neighbor Count 0		More Runtime Stats

Examine the routing tables for routes that were learned via OSPF ("O" flag):

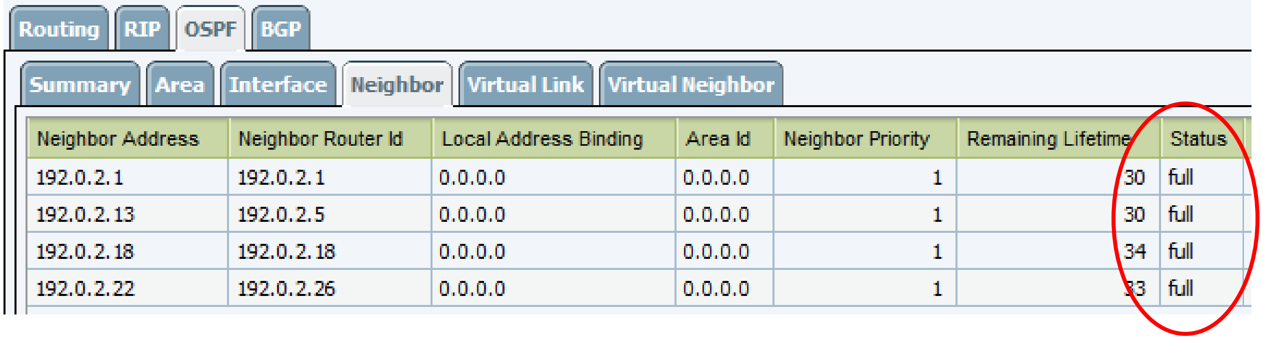


Virtual Router: default

Destination	Next Hop	Metric	Flags	Age	Interface
192.0.2.0/30	0.0.0.0	10	Oi	7515	ethernet1/1
192.0.2.0/30	192.0.2.2	0	A C		ethernet1/1
192.0.2.2/32	0.0.0.0	0	A H		
192.0.2.4/30	192.0.2.13	20	A Oi	7364	ethernet1/3
192.0.2.8/30	192.0.2.1	20	A Oi	7399	ethernet1/1
192.0.2.12/30	0.0.0.0	10	Oi	7515	ethernet1/3
192.0.2.12/30	192.0.2.14	0	A C		ethernet1/3
192.0.2.14/32	0.0.0.0	0	A H		
192.0.2.16/30	0.0.0.0	10	Oi	7515	ethernet1/2
192.0.2.16/30	192.0.2.17	0	A C		ethernet1/2
192.0.2.17/32	0.0.0.0	0	A H		
192.0.2.20/30	0.0.0.0	10	Oi	7515	ethernet1/4
192.0.2.20/30	192.0.2.21	0	A C		ethernet1/4
192.0.2.21/32	0.0.0.0	0	A H		
192.0.2.24/30	192.0.2.22	20	A Oi	7301	ethernet1/4
192.0.2.28/30	192.0.2.18	20	A Oi	7515	ethernet1/2
192.0.2.32/30	192.0.2.13	15	A Oi	7364	ethernet1/3
192.0.2.36/30	192.0.2.18	15	A Oi	7399	ethernet1/2

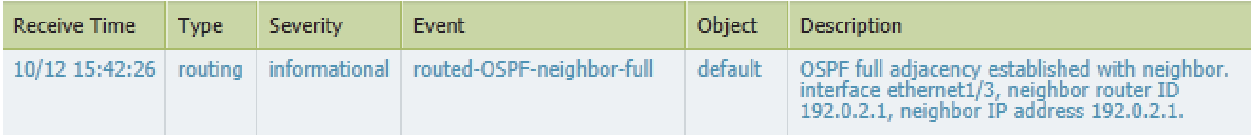
You should also see the internal network routes, as well as a default route propagated from the upstream routers.

13. Go to the OSPF -> Neighbor tab, and confirm the device has OSPF adjacencies established as follows:



Neighbor Address	Neighbor Router Id	Local Address Binding	Area Id	Neighbor Priority	Remaining Lifetime	Status
192.0.2.1	192.0.2.1	0.0.0.0	0.0.0.0	1	30	full
192.0.2.13	192.0.2.5	0.0.0.0	0.0.0.0	1	30	full
192.0.2.18	192.0.2.18	0.0.0.0	0.0.0.0	1	34	full
192.0.2.22	192.0.2.26	0.0.0.0	0.0.0.0	1	33	full

You can also confirm that the OSPF connections are established by examining the Monitor tab -> System log as follows:



Receive Time	Type	Severity	Event	Object	Description
10/12 15:42:26	routing	informational	routed-OSPF-neighbor-full	default	OSPF full adjacency established with neighbor. interface ethernet1/3, neighbor router ID 192.0.2.1, neighbor IP address 192.0.2.1.

16. At this point, you can test your setup by sending pings through the network. Put one firewall into a "suspended" HA state (Device tab -> High Availability screen), and confirm that pings still flow through the network.

This document gives you the basic steps needed to configure OSFP on Palo Alto Networks firewalls. From this point, you can configure additional OSPF features as is needed in your network.