# How to Configure BGP
Tech Note

This document gives step by step instructions for configuring and testing full-mesh multi-homed eBGP 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

Border Gateway Protocol (BGP) forms the routing backbone of the Internet and provides dynamic routing and resiliency for many public and private networks that require robust performance and fault tolerance. One of the many benefits of a BGP environment is the ability to route an IP space across multiple links simultaneously, allowing for both load sharing and redundancy. Many environments today have the need to connect to two disparate ISPs to achieve this functionality.

Below is a sample diagram of a network with dual homed eBGP connectivity.

Note: The BGP routed IP space is referred to as the "internal network".
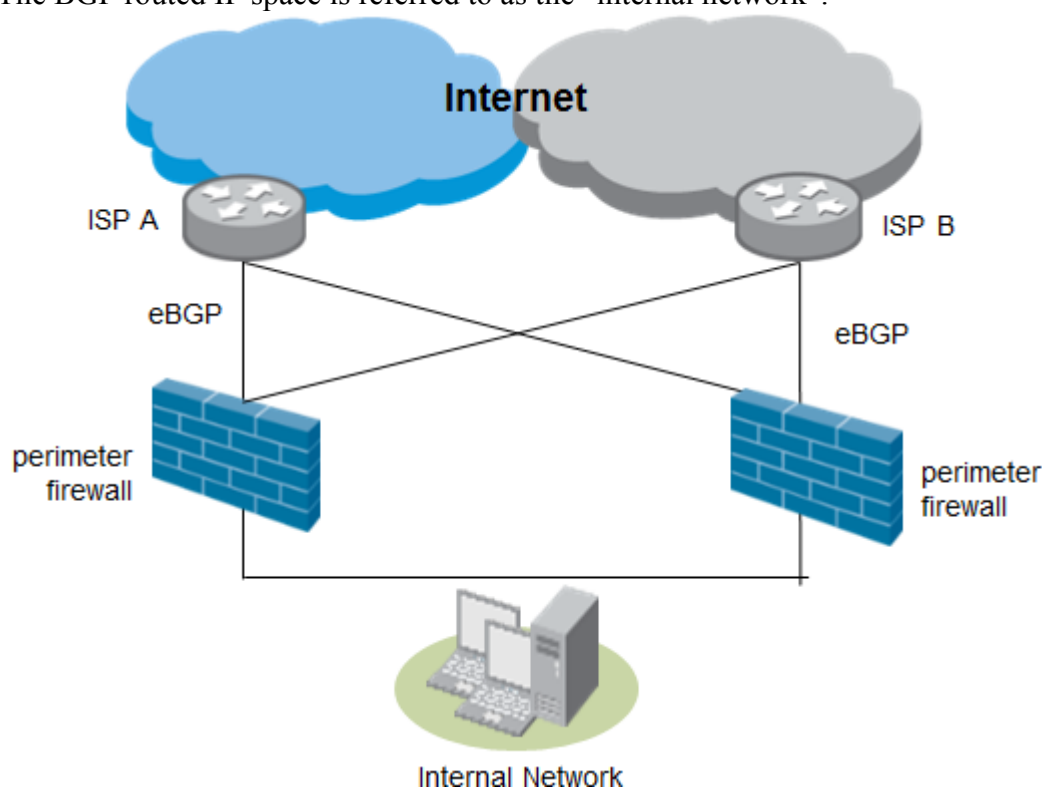
In this scenario, the Palo Alto Networks devices will become eBGP peers to their Internet Service Providers to provide redundancy and route redistribution.

[2]

This document will discuss two scenarios:
    Scenario 1: Full-mesh multi-homed eBGP with Active/Passive High Availability
    Scenario 2: Full-mesh multi-homed eBGP with Active/Active High Availability

Concerns about Redistributing Routes

You may have different thoughts on how you enable your redistribution rules for exporting your public IP space, or how you enable your import/export route filters. There isn't a specific best practice as each environment can be different and there are many ways and styles to implement BGP. In the scenario in this document, we assume that each ISP will give us a single default route and we will import that route into our RIB. We also assume that we want to redistribute a route to our 203.0.113.0/24 network to both ISPs. As such, you will see a redistribution profile for this route in the virtual router configuration.

One common pitfall with configuring a redistribution profile is not checking the correct box in the Redistribution Profiles tab in the Filter Type section. You might be tempted to check the "bgp" checkbox here, but bear in mind that you are redistributing a route to a directly connected network, the 203.0.113.0/24 network. In this case, you will need to check the "connect" box instead. Follow the configuration as shown in the virtual router portion of this document.

Note: the firewall is not intended to be configured as a core BGP speaker importing and exporting hundreds of thousands of routes as is often found on the Internet. Only up to a few tens of thousands of entries are supported in the forwarding table of the largest Palo Alto Networks devices. It is recommended to only import the default route from the Internet, or perhaps selected partial routing information from one or more peers.

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 BGP neighbor peers (your two ISPs)
    - IP addresses for your HA configuration
    - If using active/active HA, an IP address for your virtual address (labeled VIP in the A/A diagram)
    - Your AS number
    - The AS numbers of your eBGP ISP peers

Scenario 1: Full-mesh multi-homed eBGP with Active/Passive High Availability

The following is a diagram of what will be implemented for scenario #1:
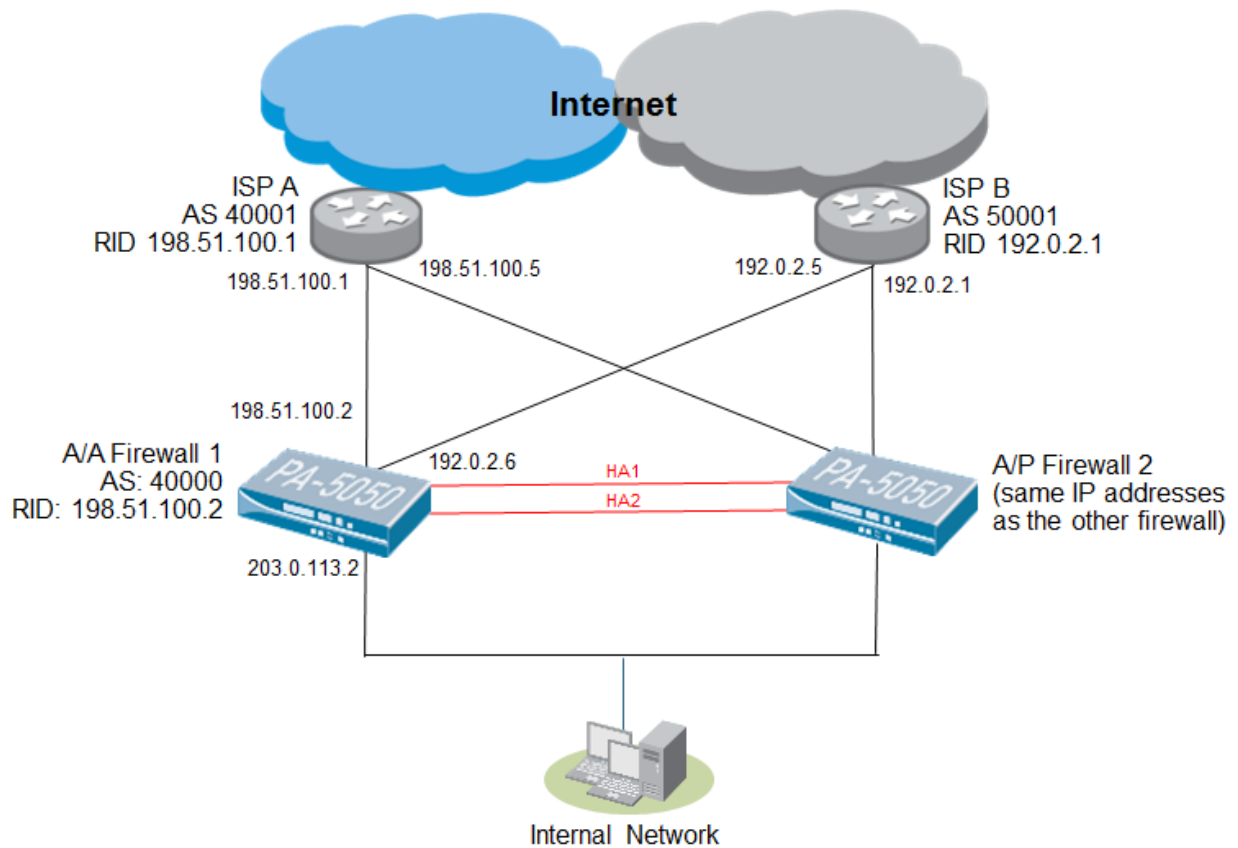
Note: To provide for full redundancy, you would need to insert L2 switches between the firewalls and the ISP routers.

Configuration for the Active/Passive Pair

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

1. On the Network tab-> Zones screen, create zones for the internal and external interfaces.

   Note: There are two external interfaces, one for each ISP.

Name	Type	Interfaces / Virtual Systems	Protection Profile	Log Setting	Enable User Identification
ISP-A	layer3	ethernet1/1			
ISP-B	layer3	ethernet1/2			
L3-trust	layer3	ethernet1/3			

2. On the Network tab -> Interfaces screen, configure the 2 external interfaces and 1 internal interface as appropriate.

   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 of them to be type "HA".

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
ethernet1/1	L3	allow ping	🏢	198.51.100.2/24	default	Untagged		ISP-A
ethernet1/2	L3	allow ping	🏢	192.0.2.6/24	default	Untagged		ISP-B
ethernet1/3	L3	allow ping	🏢	203.0.113.2/24	default	Untagged		L3-trust

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

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

4. Now configure the devices as an Active/Passive HA pair. For the steps, refer to this 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	Primary	Backup	Edit...
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	Edit...
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, ethernet1/3

[6]

HA configuration for the second firewall:

Setup		Edit...
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		Edit...
Device Priority	100	
Heartbeat Backup	✗	
Preemptive	✗	
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	Edit...
Port	dedicated-ha1		
IP Address	10.1.1.1		
Netmask	255.255.255.0		
Gateway			
Link Speed (Mbps)			
Link Duplex			
Encryption Enabled	✗		
Monitor Hold Time (ms)	3000		

Data Link	Primary	Backup	Edit...
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	✗					
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, ethernet1/3	

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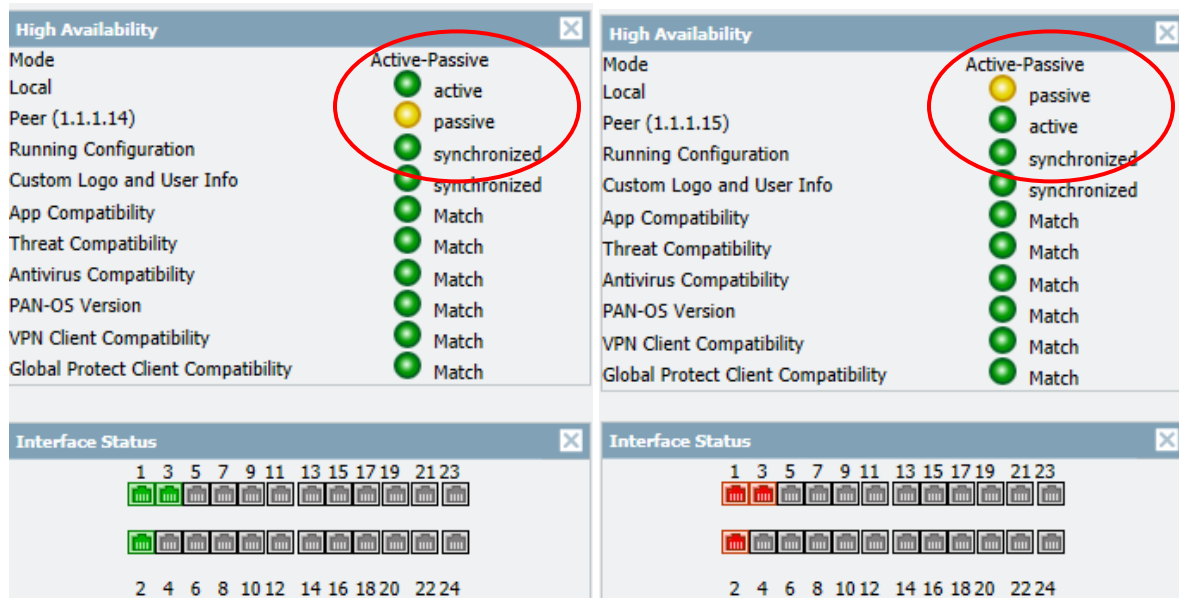
If you have problems with High Availability, check the system log for errors.

Next, you will configure BGP.

7. On the Network tab-> Virtual Routers screen, edit the virtual router. On the BGP General tab, enable BGP, and configure appropriate settings:

8. While still editing the BGP instance, go to the Peer Group tab. Create a new peer group for the first ISP. The General sub-tab for Provider A should look like the following:

The Peers sub-tab for Provider A should show the following:

Name	Enable	Peer AS	Local Address	Peer Address	Connection Options	Advanced
peerA	✔	40001	Interface: ethernet1/1 IP: 198.51.100.2/24	IP: 198.51.100.1	Multi Hop: 0 Hold Time: 90 Keep Alive Interval: 30 Open Delay Time: 0 Idle Hold Time: 15 Remote Port: 0 Allow Incoming: ✔ Local Port: 0 Allow Outgoing: ✔	Max Prefixes: 5000

9. Repeat the above step for ISP B:

General	Peers	
Name	Provider B	
Enable	☑	
Aggregated Confed AS Path	☐	
Soft Reset With Stored Info	☐	
Type	EBGP	
	Next Hop Import	original
	Next Hop Export	resolve
	Remove Private AS	☐

Name	Enable	Peer AS	Local Address	Peer Address	Connection Options	Advanced
peerB	✔	50001	Interface: ethernet1/2 IP: 192.0.2.6/24	IP: 192.0.2.1	Multi Hop: 0 Hold Time: 90 Keep Alive Interval: 30 Open Delay Time: 0 Idle Hold Time: 15 Remote Port: 0 Allow Incoming: ✔ Local Port: 0 Allow Outgoing: ✔	Max Prefixes: 5000

10. Commit the configuration.

11. Confirm that your BGP 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			Enabled	✔	More Runtime Stats
				Peer Count	2	
				Peer Group Count	2	
				Local RIB Prefix Count	0	

12. In the window that appears, go to the BGP -> Peer tab and confirm the BGP connections are established:

| Routing | RIP | OSPF | BGP |

| Summary | Peer | Peer Group | Local RIB | RIB Out |

Name	Group	Local IP	Peer IP	Peer AS	Password Set	Status	Status Duration (secs.)	Show/Hide
peerB	Provider B	192.0.2.6	192.0.2.1	50001	no	Established	259	Show details...
peerA	Provider A	198.51.100.2	198.51.100.1	40001	no	Established	259	Show details...

If the status shows "Connect", there are problems with establishing the BGP connection. Click on "Show details" to troubleshoot the connection.

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

Receive Time	Type	Severity	Event	Object	Description
09/28 11:08:28	routing	informational	routed-BGP-peer-enter-established	default	BGP peer session enters established state. peer IP: 198.51.100.1.
09/28 11:08:27	routing	informational	routed-BGP-peer-enter-established	default	BGP peer session enters established state. peer IP: 192.0.2.1.

13. Check to see what routes you are sending out (RIB Out tab), as well as accepting in (Local RIB). Both of those tabs will be empty since you haven't configured redistribution rules yet.

14. In the next 4 steps, you will configure redistribution rules, edit your virtual router, and then create a redistribution profile that distributes the internal network (in this example, network 203.0.113.0/24). First, create a redistribution profile as shown below.

General	Redistribution Profiles	RIP	OSPF	BGP					

Name	Priority	Filter						Action	
		Type	Interface	Destination	Next Hop	OSPF Params	BGP Params	Redistribute	Metric
redist-203net	1	connect	ethernet1/3					✔	1

15. While still editing your virtual router, edit the BGP instance. Configure the BGP instance to accept only the default route by adding a new import rule:

| General | Redistribution Profiles | RIP | OSPF | BGP |

| General | Peer Group/Peer | Import Rules | Export Rules | Conditional Advertisement | Aggregate | Redi |

	Name	Enable	Used By	Match				
				Prefixes	Next Hops	From Peers	Others	Action
☐	allow-default-route-in	✔	Provider A Provider B	0.0.0.0/0 (exact)				allow

16. Configure the BGP instance to export the local route:

| General | Redistribution Profiles | RIP | OSPF | BGP |

| General | Peer Group/Peer | Import Rules | Export Rules | Conditional Advertisement | Aggregate |

	Name	Enable	Used By	Match				
				Prefixes	Next Hops	From Peers	Others	Action
☐	export-203-route	✔	Provider A Provider B	203.0.113.0/24 (exact)				allow

17. On the BGP -> Redistribution Rules tab, add a new rule. In the pull-down name field, select the redistribution rule you created earlier. Your completed rule will look like the following:

| General | Redistribution Profiles | RIP | OSPF | BGP |

| General | Peer Group/Peer | Import Rules | Export Rules | Conditional Advertisement | Aggregate | Redistribution Rules |

Name	Enable	Set Origin	Set MED	Set Local Preference	Set AS Path Limit	Set Communities	Set Extended Communities	
redist-203net	✔	incomplete						⊠

18. Commit the configuration.

19. View the runtime stats on the virtual router and look for the RIB Out tab as well as the Local RIB.

Routing	RIP	OSPF	BGP								

Summary	Peer	Peer Group	Local RIB	RIB Out

Prefix	Next Hop	Peer	Local Pref.	AS Path	Origin	MED	Adv. Status	Aggr. Status	Show/Hide
203.0.113.0/24	198.51.100.2	peerA	0	40000	N/A	0	advertised	no aggregate	Show details...
203.0.113.0/24	192.0.2.6	peerB	0	40000	N/A	0	advertised	no aggregate	Show details...

Routing	RIP	OSPF	BGP

Summary	Peer	Peer Group	Local RIB	RIB Out

Flag	Prefix	Next Hop	Peer	Weight	Local Pref.	AS Path	Origin	MED	Flap Count	Show/Hide
	0.0.0.0/0	198.51.100.1	peerA	0	100	40001	N/A	0	0	Show details...
*	0.0.0.0/0	192.0.2.5	peerB	0	100	50001	N/A	0	0	Show details...
*	203.0.113.0/24	203.0.113.2	Local	0	100		N/A	0	0	Show details...

Another way to confirm that BGP is operational is to look for routes in the routing table that were learned via BGP:

Routing	RIP	OSPF	BGP

Destination	Next Hop	Metric	Flags	Age	Interface
0.0.0.0/0	192.0.2.1		A?B	676	

Scenario 2: Full-mesh multi-homed eBGP with Active/Active High Availability

In an Active/Active environment, each device will be a separate eBGP peer to the ISP routers. Following is a diagram of what will be implemented:
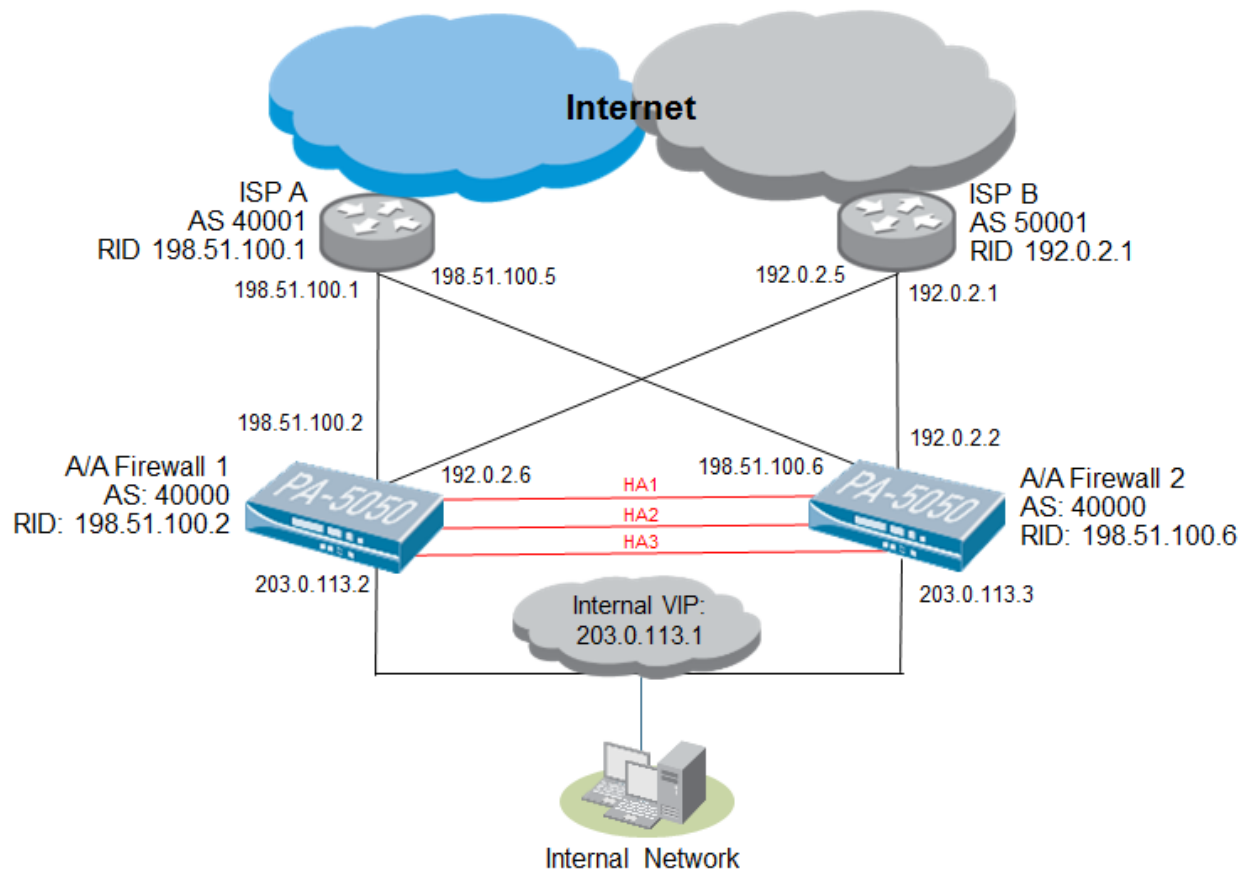
Note: To provide for full redundancy, you would need to insert L2 switches between the firewalls and the ISP routers.

Configuration for the Active/Active Pair

In steps 1 - 6 you will configure the zones, interfaces, 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:

	Name	Type	Interfaces / Virtual Systems
☐	internal	layer3	ethernet1/4
☐	internet	layer3	ethernet1/1 ethernet1/3

2. On the Network tab -> Interfaces screen, configure the interfaces as appropriate. Following are examples. Notice that this device does not have built-in HA interfaces, thus e1/6, e1/7, and e1/8 are configured as interface type HA and will be used for the HA1, HA2, and HA3 links.

Interface config of first firewall:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
ethernet1/1	L3			198.51.100.2/30	default	Untagged		internet
ethernet1/2						Untagged		none
ethernet1/3	L3			192.0.2.6/30	default	Untagged		internet
ethernet1/4	L3			203.0.113.2/24	default	Untagged		internal
ethernet1/5						Untagged		none
ethernet1/6	HA					Untagged		
ethernet1/7	HA					Untagged		
ethernet1/8	HA					Untagged		

Interface config of second firewall:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
ethernet1/1	L3			198.51.100.6/30	default	Untagged		internet
ethernet1/2						Untagged		none
ethernet1/3	L3			192.0.2.2/30	default	Untagged		internet
ethernet1/4	L3			203.0.113.3/24	default	Untagged		internal
ethernet1/5						Untagged		none
ethernet1/6	HA					Untagged		
ethernet1/7	HA					Untagged		
ethernet1/8	HA					Untagged		

[15]

3. Now configure HA as Active/Active. For details on the meanings of the settings, refer to this 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:

   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.

HA config for the second firewall:

Setup		Edit...
HA Enabled	✔	
Group ID	63	
Description		
Mode	active-active	
Device Id	1	
Peer HA IP Address	1.2.3.4	
Peer HA IP Backup Address		
Config Sync	✔	

Election Settings		Edit...
Device Priority	0	
Heartbeat Backup	✗	
Preemptive	✗	
Preemption Hold Time (min)	1	
Promotion Hold Time (ms)	2000	
Hello Interval (ms)	8000	
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	ethernet1/6	
IP Address	1.2.3.5	
Netmask	255.255.255.0	
Gateway		
Encryption Enabled	✗	
Monitor Hold Time (ms)	3000	

Data Link	Primary	Backup
Port	ethernet1/7	
IP Address	4.3.2.2	
Netmask	255.255.255.0	
Gateway		
State Synchronization Enabled	✔	
Transport	ethernet	

Active Active Configuration					Edit...
HA3 Packet Forwarding	HA3 Interface	VR Sync	QOS Sync	Session Owner Selection	Session Setup
✔	ethernet1/8	✗	✔	first-packet	ip-modulo

| Virtual Address	IPv4			IPv6			
Interface	Address	Floating	ARP Load Sharing	Address	Floating	ARP Load Sharing	
ethernet1/4	203.0.113.1		ip-modulo				☒

Add

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:
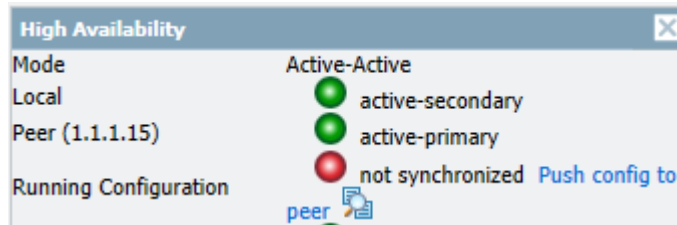
If the second comes up as non-functional as shown in the following screenshot, then check the system log for errors.
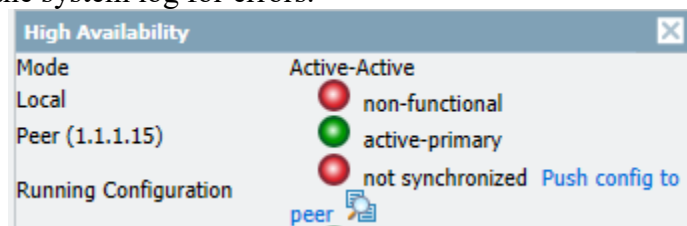
6. View the HA widget on the active-primary firewall. Click "Push config to peer". After the synchronization completes, you will see the following:
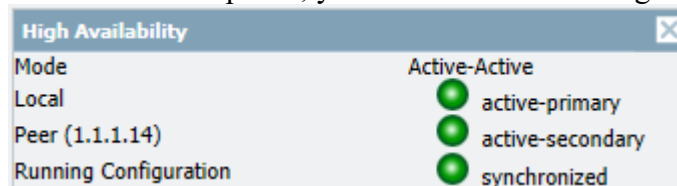
At this point, the HA configuration is complete. The next steps will be to configure policies and BGP.

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

| Name | Source | | | Destination | | | | | |
	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.

[18]

Next, you will configure BGP. Remember that in Active-Active the Virtual Router on each firewall is a separate independent BGP peer using the same AS number. In this example, we have two ISPs and will import the default route from each using an import rule. We will also redistribute a route to our public IP address space, the 203.0.113.0/24 network.

8. On the Active-Primary firewall, go to the Network tab-> Virtual Routers screen. Edit the virtual router. On the BGP General tab, enable BGP, and configure appropriate settings:

Revision A
©2011, Palo Alto Networks, Inc.

10. While still editing the BGP instance, go to the Peer Group tab. Create a new peer group for the first ISP. The General sub-tab for ISP A should look like the following:
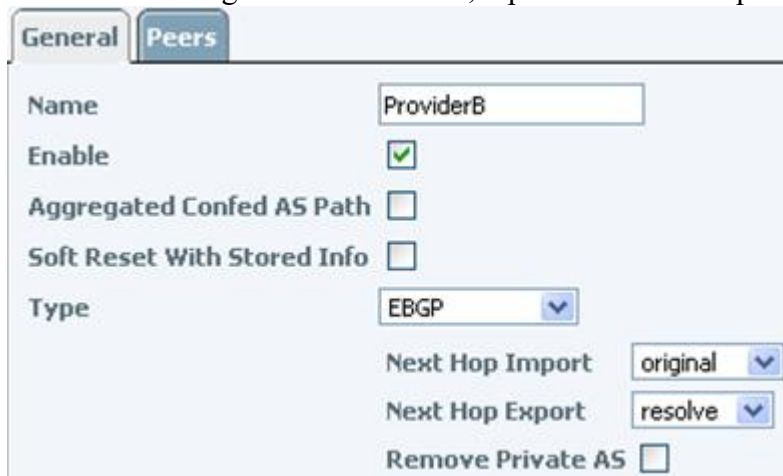

The Peers sub-tab for ISP A should look like the following:

11. While still editing the BGP instance, repeat the above step for ISP B:

12. Since the VR part of the configuration are not synchronized, repeat steps 8 – 11 on the Active-Secondary firewall using the correct IP addresses for the local and remote peer configuration.

13. Commit the configuration on both devices.

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

Revision A
©2011, Palo Alto Networks, Inc.

15. In the window that appears, go to the BGP -> Peer tab, and confirm the BGP connections are established:

Name	Group	Local IP	Peer IP	Peer AS	Password Set	Status	Status Duration (secs.)	Show/Hide
peerB	Provider B	192.0.2.6	192.0.2.1	50001	no	Established	259	Show details...
peerA	Provider A	198.51.100.2	198.51.100.1	40001	no	Established	259	Show details...

If the status shows "Connect", there are problems with establishing the BGP connection. Click on "Show details" to troubleshoot the connection.

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

Receive Time	Type	Severity	Event	Object	Description
09/28 11:08:28	routing	informational	routed-BGP-peer-enter-established	default	BGP peer session enters established state. peer IP: 198.51.100.1.
09/28 11:08:27	routing	informational	routed-BGP-peer-enter-established	default	BGP peer session enters established state. peer IP: 192.0.2.1.

16. Check to see what routes you are sending out (RIB Out tab), as well as accepting in (Local RIB). Both of those tabs will be empty, since you haven't configured redistribution rules yet.

17. In the next 5 steps, you will configure redistribution rules on both the active-primary and active-secondary. On the active-primary firewall, edit your virtual router. Create a redistribution profile that distributes the internal network (in this example, network 203.0.113.0/24).

Name	Priority	Type	Interface	Destination	Next Hop	OSPF Params	BGP Params	Redistribute	Metric
redist-203net	1	connect	ethernet1/3					✔	1

18. While still editing your virtual router, edit the BGP instance. Configure the BGP instance to accept only the default route by adding a new import rule:

	Name	Enable	Used By	Prefixes	Next Hops	From Peers	Others	Action
						Match		
☐	allow-default-route-in	✔	Provider A Provider B	0.0.0.0/0 (exact)				allow

19. Configure the BGP instance to export the local route:

	Name	Enable	Used By	Prefixes	Next Hops	From Peers	Others	Action
						Match		
☐	export-203-route	✔	Provider A Provider B	203.0.113.0/24 (exact)				allow

20. On the BGP -> Redistribution Rules tab, add a new rule. In the pull-down name field, select the redistribution rule you created earlier. Your completed rule will look like the following:

Name	Enable	Set Origin	Set MED	Set Local Preference	Set AS Path Limit	Set Communities	Set Extended Communities	
redist-203net	✔	incomplete						☒

21. Repeat steps 17-20 on the active-secondary firewall.

22. Perform a commit on both devices.

23. View the runtime stats on the virtual router on each firewall and look for the RIB Out tab as well as Local RIB.

Prefix	Next Hop	Peer	Local Pref.	AS Path	Origin	MED	Adv. Status	Aggr. Status	Show/Hide
203.0.113.0/24	198.51.100.2	peerA	0	40000	N/A	0	advertised	no aggregate	Show details...
203.0.113.0/24	192.0.2.6	peerB	0	40000	N/A	0	advertised	no aggregate	Show details...

Flag	Prefix	Next Hop	Peer	Weight	Local Pref.	AS Path	Origin	MED	Flap Count	Show/ Hide
	0.0.0.0/0	198.51.100.1	peerA	0	100	40001	N/A	0	0	Show details...
*	0.0.0.0/0	192.0.2.5	peerB	0	100	50001	N/A	0	0	Show details...
*	203.0.113.0/24	203.0.113.2	Local	0	100		N/A	0	0	Show details...

Also examine the routing tables for routes that were learned via BGP:

Destination	Next Hop	Metric	Flags	Age	Interface
0.0.0.0/0	192.0.2.1		A?B	676	

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