



Designing Networks with Palo Alto Networks Firewalls

Suggested Designs for Potential and Existing Customers

Table of Contents

Introduction	3
Section 1: Tap Mode Deployment Scenarios	7
1.1 Operation of Tap Interfaces	7
1.2 Example Scenarios: Tap Mode	7
Section 2: Virtual-wire Deployment Scenarios	13
2.1 Operation of Virtual Wire Interfaces	13
2.2 Example Scenario: Virtual Wire with Active/Passive HA	15
2.3 Example Scenario: Virtual Wire with Active/Active HA	24
2.4 Example Scenario: Virtual Wire with A/A HA and Link Aggregation on Adjacent Switches	33
2.5 Example Scenario: Virtual Wire with Bypass Switch (“fail-open” scenario)	45
2.6 Example Scenario: Horizontal Scaling with Load Balancers	52
Section 3: Layer2 Deployment Scenarios	59
3.1 Operation of L2 Interfaces	59
3.2 Example Scenario: Layer 2 Active/Passive HA	60
3.3 Example Scenario: Combination Layer 2 and Layer 3 Topology	68
Section 4: Layer3 Deployment Scenarios	75
4.1 Operation of L3 Interfaces	75
4.2 Example Scenario: Layer 3 Active/Passive HA with OSPF	76
4.3 Example Scenario: Layer 3 Active/Active HA with OSPF	77
4.4 Example Scenario: Layer 3 Active/Passive HA with BGP	78
4.5 Example Scenario: Layer 3 Active/Active HA with BGP	79
4.6 Example Scenario: Layer 3 Active/Passive with Link Aggregation	80
4.8 Example Scenario: Firewall on a Stick	99
Appendix A: Review of User-ID Operation	107
Revision History	110

Introduction

How to Use this Document

The purpose of this document is to help people choose how to deploy Palo Alto Networks devices into their network. Various scenarios are described, as well as their configuration. All of these scenarios were tested in the field, running PAN-OS 5.0.2.

Prerequisite knowledge

This document is not a step-by-step how-to document, but gives a summary of the configuration needed to implement each scenario. It is assumed that the reader has the knowledge to complete the following tasks on a PA firewall:

- Configure interface settings, such as interface type, duplex, speed, zone
- Create and configure zones
- Create and configure policies
- Create/delete virtual wires
- Configure virtual routers

Where do I start?

The best place to start is to review different deployment modes below, and then use the table of contents to determine which scenarios you might consider. The 4 interface modes/deployment scenarios are:

- Tap mode
- Virtual wire mode
- Layer 2 mode
- Layer 3 mode

Tap Mode Deployments

Whereas a network tap is a device that provides a way to access data flowing across a computer network, “tap mode deployment” of the Palo Alto Networks firewalls allows you to passively monitor traffic flows across a network by way of a tap or switch SPAN/ mirror port.

The SPAN or mirror port permits the copying of traffic from other ports on the switch. By designating an interface on the firewall as a tap mode interface and connecting it to a switch SPAN port, the switch SPAN port provides the firewall with the mirrored traffic. This provides application visibility within the network without being in the flow of network traffic.

Advantages:

- Visibility into the network traffic
- Easy to deploy
- Easy to implement for proof of concept testing
- Can be implemented without service interruption

Disadvantages

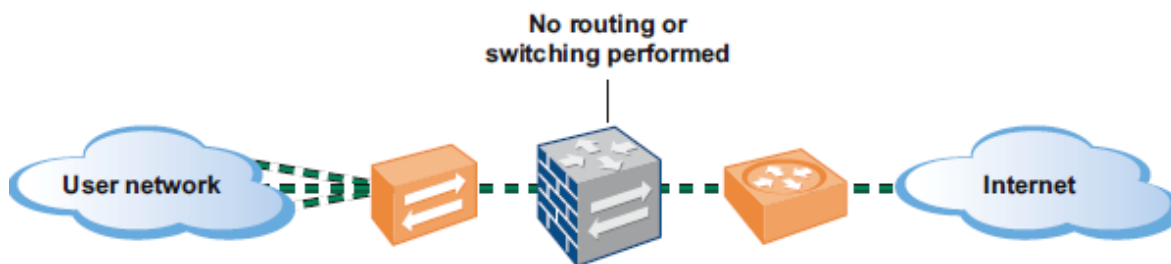
- Device is not able to take action, such as blocking traffic or applying QoS traffic control.

Virtual Wire Deployments

In a virtual wire (vwire) deployment, the firewall is installed transparently in the network (see figure below). This deployment mode is typically used when no switching or routing is needed or desired. A vwire deployment allows the firewall to be installed in any network environment without requiring any configuration changes to adjacent or surrounding network devices.

The vwire deployment mode binds any two Ethernet ports together placing the firewall inline on the wire and can be configured to block or allow traffic based on VLAN tags (VLAN tag "0" is untagged traffic). Multiple subinterfaces can be added to different security zones and classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet). This allows for granular policy control of the traffic traversing the vwire two interfaces for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet. Additional information on vwire subinterfaces can be found in the PAN-OS 5.0 Administrators Guide.

The default virtual wire "default-vwire" configuration as shipped from the factory, binds together Ethernet ports 1 (untrust) and 2 (trust) and allows all untagged traffic from the trust security zone to the untrust security zone.



Advantages:

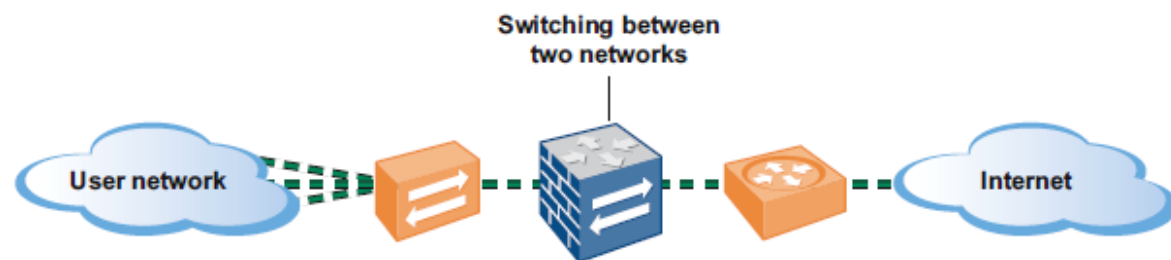
- Visibility into network traffic
- Simple to install and configure, no configuration changes required to surrounding network devices
- Easy to implement for proof of concept testing
- Device can take action on the traffic, such as allow, block or perform QoS
- Network Address Translation (NAT) is support in PAN-OS version 4.1 and later

Disadvantages:

- Cannot perform layer 3 functionality on the device, such as routing (NAT is support as of PAN-OS version 4.1)
- Cannot perform any switching on the device

Layer 2 Deployments

In a Layer 2 deployment, the firewall provides switching between two or more networks. Each group of interfaces must be assigned to a VLAN, and additional Layer 2 subinterfaces can be defined as needed. Choose this option when switching is required.



Advantages:

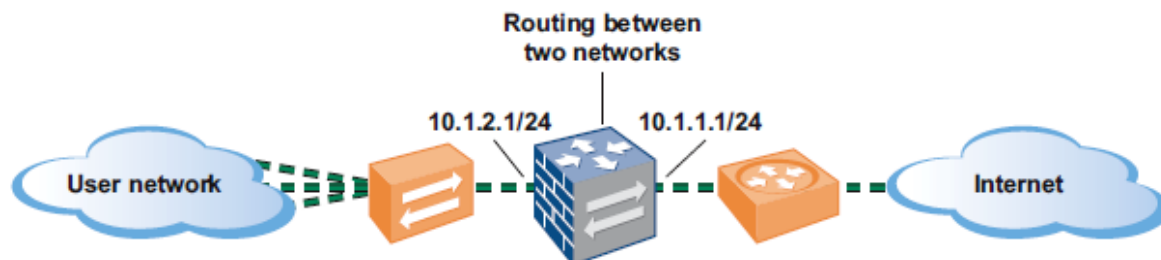
- o Visibility into network traffic
- o Device can take action on the traffic, such as block or perform QoS

Disadvantages:

- o The device does not participate in spanning tree

Layer 3 Deployments

In a Layer 3 deployment, the firewall routes traffic between multiple interfaces. An IP address must be assigned to each interface and a virtual router must be defined to route the traffic. Choose this option when routing or NAT is required.



Advantage:

- Full firewall functionality, such as traffic visibility, blocking traffic, rate limiting traffic, NAT, and routing, including support for common routing protocols

Disadvantage:

- Inserting device into network will require IP configuration changes on adjacent devices

After this document, where do I go next?

Document	Location
XML configs for all scenarios in this doc	attached
PPTs of all diagrams in this doc	attached
Layer 3 Deployment Guide	https://live.paloaltonetworks.com/docs/DOC-1861
Active/Passive HA	https://live.paloaltonetworks.com/docs/DOC-1160
Active/Active HA	https://live.paloaltonetworks.com/docs/DOC-1756
Admin guide	https://live.paloaltonetworks.com/docs/DOC-1753
User-ID tech note	https://live.paloaltonetworks.com/docs/DOC-1807
Virtual systems tech note	http://www.paloaltonetworks.com/literature/techbriefs/Virtual_Systems.pdf
OSPF tech note	https://live.paloaltonetworks.com/docs/DOC-1939
BGP tech note	https://live.paloaltonetworks.com/docs/DOC-1572

Section 1: Tap Mode Deployment Scenarios

1.1 Operation of Tap Interfaces

Interfaces in tap mode on Palo Alto Networks firewalls can be used in various ways:

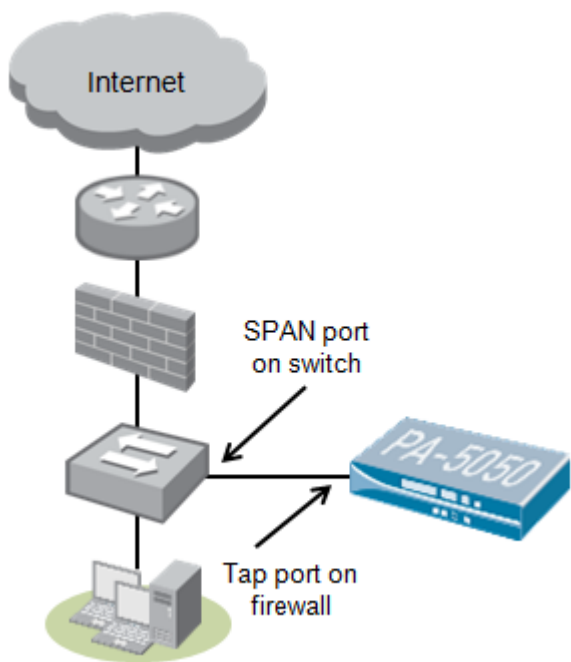
1. A non-intrusive way to get to know your network (detect applications, users and threats) and to get to know the firewall. It will use SPAN-ports on the switch or passive tap ports on the network to feed the tap ports on the firewall
2. A way to monitor internal flows (e.g. datacenter, Internet perimeter) without enforcing any security policies.

Advantage of tap mode: you will have visibility into the network applications, who is using them, and what threats are on the network without having to insert a device inline in the network.

1.2 Example Scenarios: Tap Mode

Tap ports on the Palo Alto Networks firewall can be deployed in any part of the network. Multiple tap ports can inspect data flows in concurrent network segments or keep track of asymmetric flows in the network. You can have separate reporting on these different segments by placing a segment's tap port in a separate security zone.

Here is a common deployment scenario for tap mode:

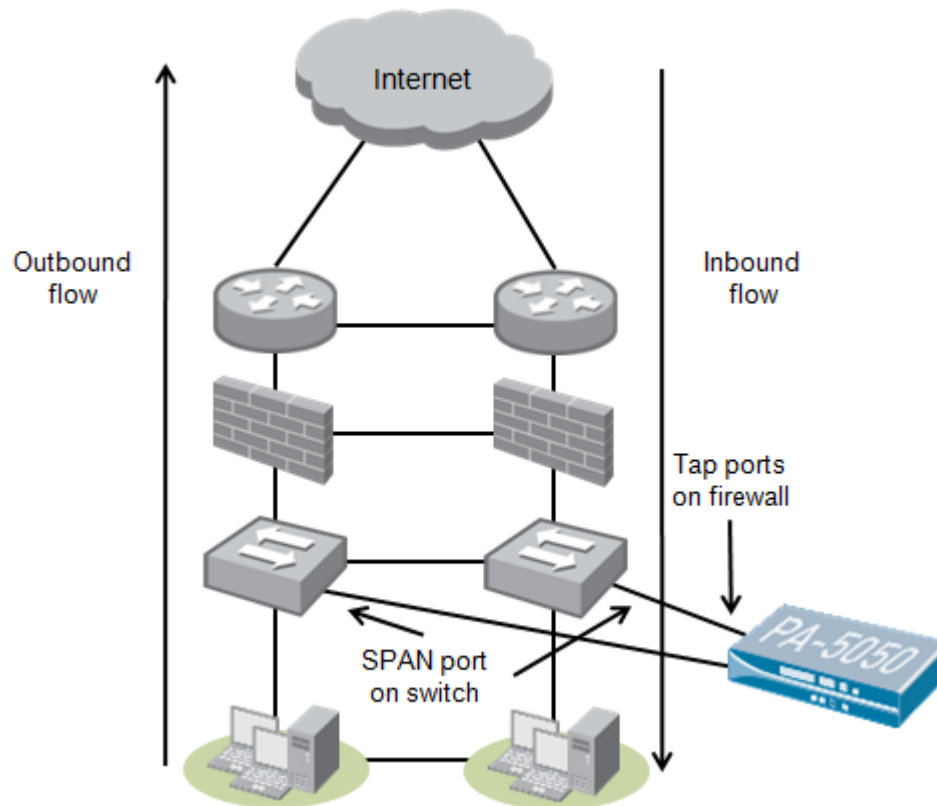


General Considerations

- When deploying tap ports make sure that concurrent sessions and performance are within the firewall's capabilities.

Tap ports in Asymmetric Flow Environment

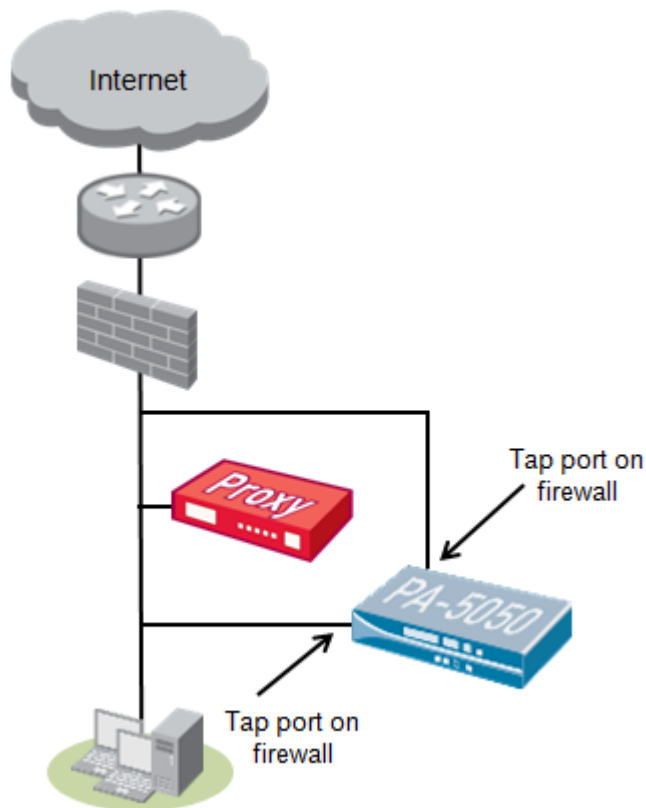
One of the challenges to place tap ports in an asymmetric flow network is that the firewall might not see all the packets in that session as they are routed through different segments in the network. In order for the firewall to see the complete packet flow, several tap ports will be required.



Note: When configuring multiple tap ports to work in an asymmetric environment, make sure that the tap ports are in the same security tap zone on the firewall. By placing them in the same security zone, the firewall will be able to match the session information and will have a complete view on the session.

Tap Ports in Proxy Environment

Preferably a Tap port is deployed south-side of an explicit proxy device. This will allow the firewall to see the original source IP addresses so user identification can be used while examining the flows from the internal network to the proxy. The firewall will recognize applications, URLs and threats inside the typical TCP port 8080 HTTP-PROXY tunnel.



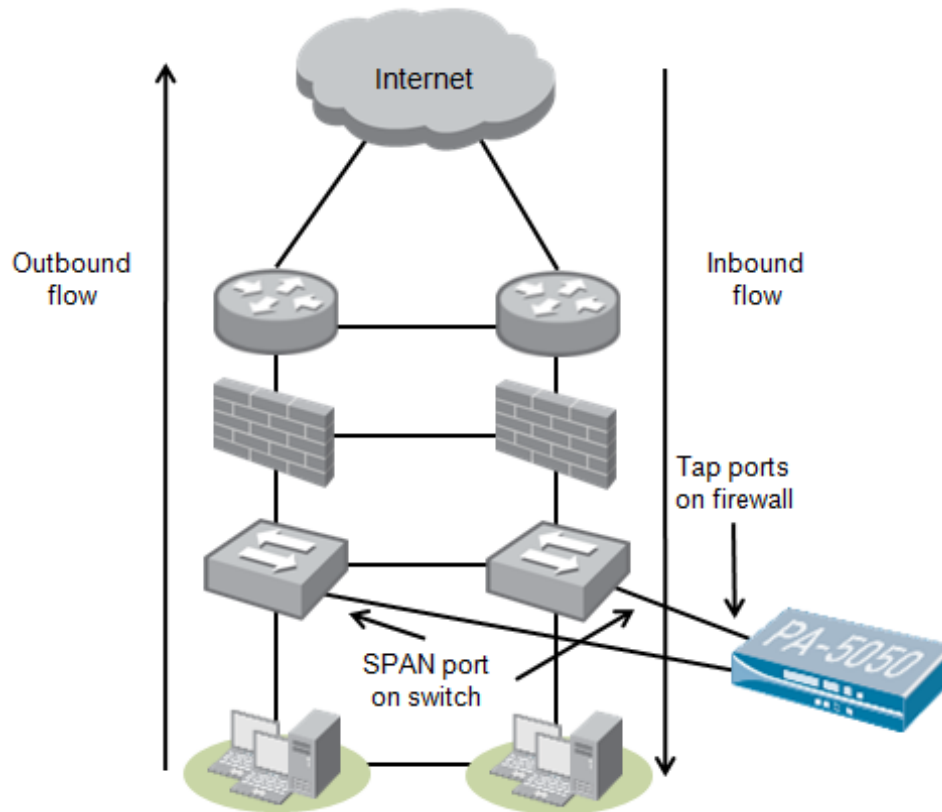
Note 1: Multiple tap ports can be deployed to check on the traffic going to (from the inside to the proxy) and coming from the proxy (proxy to the Internet). The second tap port will show the applications allowed by the proxy to the Internet.

Note 2: The second tap port north-side of the proxy should be configured in a different security tap zone on the firewall to filter on the reporting output. The second tap port could also be placed in a separate virtual system to allow for per tap reporting in the ACC.

Note 3: In case a hierarchical proxy environment is used (parent and child proxies), the firewall will capture the 'X-forwarded for' IP address of the original source.

Configuration Example

This example scenario was tested using two tap ports in the same security tap zone. This would be a scenario to capture asymmetric traffic. Of course if you only need to monitor one span port, just configure one tap interface.



GUI Configuration



The following screenshots are of a completed configuration.

Network tab -> Zones

	Name	Type	Interfaces / Virtual Systems	Protection Profile	Log Setting	Enable User Identification	User Id Include List	User Id Exclude List
<input type="checkbox"/>	tapzone	tap				✓		




Create one or more zones of type “tap”, and assign appropriate names. If you plan to implement user-ID, check the box to “enable user-identification”.

Network tab-> Interfaces

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
ethernet1/3	Tap							tapzone
ethernet1/4	Tap							tapzone

Configure one or more interfaces to be of type “tap”, and assign those interfaces to the tap zones you just created.

Policies tab-> Security

Source			Destination					
Zone	Address	User	Zone	Address	Application	Service	Action	Profile
 tapzone	any	any	 tapzone	any	any	any	✓	

Create a security policy to allow traffic from the tap zone to the tap zone. Assign security profiles to inspect for viruses/spyware/threats as appropriate. Note that different tap zones and security policies can be created to separate reporting afterwards.

Additional configuration

Attach one end of a cable to the span port on the switch or tap, and the other end to the tap interface on the PA firewall. Run additional cables to span ports as desired. Monitor the traffic log and ACC to confirm that you are detecting traffic.

CLI Configuration

The CLI commands used to configure this scenario are shown below: ¹

```
# Interface configuration
set network interface ethernet ethernet1/3 link-speed auto
set network interface ethernet ethernet1/3 link-duplex auto
set network interface ethernet ethernet1/3 link-state auto
set network interface ethernet ethernet1/4 link-speed auto
set network interface ethernet ethernet1/4 link-duplex auto
set network interface ethernet ethernet1/4 link-state auto

# Interface mode
set network interface ethernet ethernet1/3 tap
set network interface ethernet ethernet1/4 tap

# Zone configuration
set zone tapzone network tap ethernet1/3
set zone tapzone network tap ethernet1/4
set zone tapzone enable-user-identification yes

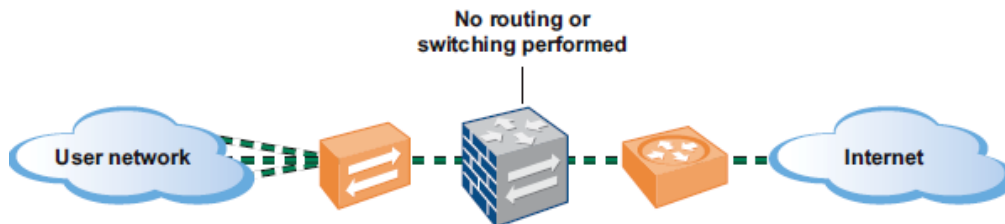
# Policy configuration
delete rulebase security rules rule1
set rulebase security rules rule1 from tapzone
set rulebase security rules rule1 to tapzone
set rulebase security rules rule1 source any
set rulebase security rules rule1 destination any
set rulebase security rules rule1 service any
set rulebase security rules rule1 application any
set rulebase security rules rule1 action allow
set rulebase security rules rule1 log-end yes
set rulebase security rules rule1 profile-setting profiles url-filtering default
set rulebase security rules rule1 profile-setting profiles virus default
set rulebase security rules rule1 profile-setting profiles spyware default
set rulebase security rules rule1 profile-setting profiles vulnerability default
```

¹ This output was obtained by running these three commands: “set cli config-output-format set”, “configure”, and “show”. Only commands relevant to this particular scenario are listed.

Section 2: Virtual-wire Deployment Scenarios

2.1 Operation of Virtual Wire Interfaces

An effective way of inserting the Palo Alto Networks firewalls into the network is using virtual wire (vwire) deployment mode. The vwire deployment mode offers the ideal solution when no switching or routing is needed or desired to be introduced to the network. A vwire configuration can be implemented in active-passive (A/P) or active-active (A/A) high availability (HA) to obtain redundancy for failover scenarios. As shown in the figure below, the firewalls are installed between Layer 3 devices. The firewalls are often deployed in conjunction with dynamic routing protocols on the surrounding network devices, which will fail traffic over to the other peer member and network path, if needed.



Advantages:

- Visibility into network traffic
- Simple to install and configure, no configuration changes required to surrounding network devices
- Easy to implement for proof of concept testing
- Device can take action on the traffic, such as allow, block or perform QoS
- Network Address Translation (NAT) is support in PAN-OS version 4.1 and later

Disadvantages:

- o Cannot perform layer 3 functionality on the device, such as routing (NAT is support as of PAN-OS version 4.1)
- o Cannot perform any switching on the device

A vwire deployment can be implemented either with or without HA. Implementing non-HA virtual wire is a simple configuration, which can be completed following the steps in section 2.2 and skipping the HA portion of the configuration that is outlined. The two basic HA configurations, A/P and A/A, are outlined in Sections 2.2 and 2.3. Sections 2.4 through 2.6 cover other common vwire configurations.

It is important to be aware that the Palo Alto Networks firewall maintains session state and by default will drop all packets that are not part of an existing session in the session table or where the session initialization (TCP 3-way handshake) is not seen. This is the default system wide session handling behavior and this dropped traffic will be logged as non-syn-tcp in the traffic logs.

This default behavior may not be desired, when implementing a transparent firewall. The firewall can be configured to ignore session state and allow traffic to flow (if allowed by the security policy) even if the session initialization has not been seen or it is not part of an existing session in the session table. However, security profiles will not be applied to this traffic as session initialization was not seen and the appropriate protocol decoder cannot be invoked. The behavior change can be enabled as a runtime parameter or in the device configuration itself.




Run-time Setting (will be fall back to the default behavior upon a firewall restart)

- CLI : `"set session tcp-reject-non-syn no"`

Device Configuration (will survive a firewall restart)

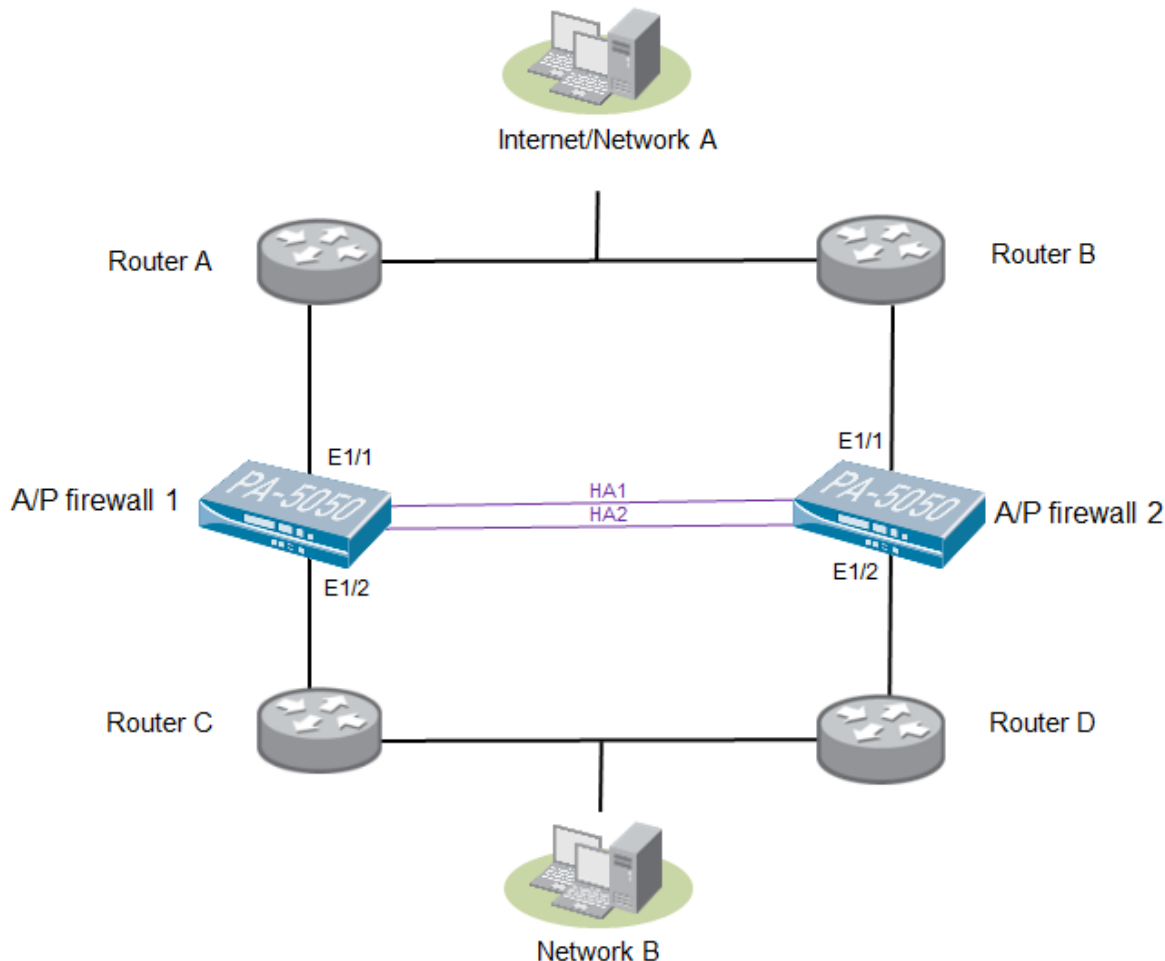
- CLI : `"set deviceconfig setting session tcp-reject-non-syn no"`

The screenshot below shows examples of non-syn-tcp traffic that can occur when the firewall is inserted inline in a vwire mode with the default behavior disabled.

<div>  <input type="text" value="(app eq non-syn-tcp)"/>      </div>										
	Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
	07/11 15:16:28	end	trust	untrust	192.168.10.91	64.124.57.10	443	non-syn-tcp	allow	Allow All Outbound
	07/11 15:15:24	end	trust	untrust	192.168.10.91	64.124.57.10	443	non-syn-tcp	allow	Allow All Outbound
	07/11 15:14:20	end	trust	untrust	192.168.10.91	64.124.57.10	443	non-syn-tcp	allow	Allow All Outbound

2.2 Example Scenario: Virtual Wire with Active/Passive HA

In this scenario, two Palo Alto Networks devices are used, with one device actively passing traffic, and the other device standing-by, waiting to take over if the active device fails.



Note for this configuration it is desired to have the passive link state configured to “auto” so the vwire interfaces on the passive firewall (A/P firewall 2) will be in a link up state, but will not pass traffic. The passive firewall vwire will pass traffic once the passive firewall becomes the active firewall member of the HA pair.

The Passive Link State is configured in the HA settings and can be configured to “auto” or “shutdown”.

- The “auto” setting causes the link status to reflect the physical connectivity, but still discards all packets received. This option allows the link state of the interface to be up on the passive firewall, decreasing the amount of time it takes for the passive firewall to become active during a failover, since link state negotiation does not need to occur with the connected devices.
- The “shutdown” setting forces the interface link to a down state. This is the default configuration, which ensures that loops are not created in the network.

Also note that if the routers A and B and routers C and D are also in a HA configuration, one may need to introduce Layer 2 switches between the routers and the Palo Alto Networks firewalls to allow any required HA communications between the HA pair of routers to properly function. Double check with the selected router vendor regarding their HA requirements.

GUI Configuration

The following screenshots are of a completed Active/Passive (A/P) High Availability (HA) virtual wire (vwire) configuration.

Network tab -> Zones

	Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	Enable User Identification	User ID Include List	User ID Exclude List
<input checked="" type="checkbox"/>	trust	virtual-wire	ethernet1/2			<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	untrust	virtual-wire	ethernet1/1			<input type="checkbox"/>		

The pre-defined vwire zones of “trust” and “untrust” are being used in this sample configuration. If you plan to implement User-ID, check the box to “enable user-identification” on the internal “trust” vwire zone.

Network tab-> Interfaces -> Ethernet subtab

Interface	Interface Type	Managem... Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features
ethernet1/1	Virtual Wire			none	none	Untagged	default-vwire	untrust	
ethernet1/2	Virtual Wire			none	none	Untagged	default-vwire	trust	

The factory-default configuration already has ethernet1/1 and ethernet1/2 in a virtual wire named “default-vwire”, with one interface in the “trust” zone and the other interface in the “untrust” zone. You can modify this sample configuration and use different vwire names or different zone names. Note for the vwire configuration that only two interfaces can be placed into the vwire definition - no more, no less. Additional vwires, using additional interfaces (and zones if needed) can be created to meet your specific design needs.

Network tab -> Virtual Wires

	Name	Interface1	Interface2	Tag Allowed	Multicast Firewalling	Link State Pass Through
<input checked="" type="checkbox"/>	default-vwire	ethernet1/1	ethernet1/2	0-4094	<input type="checkbox"/>	<input checked="" type="checkbox"/>

You can use the factory default vwire configuration on port ethernet1/1 and ethernet1/2 or create a new vwire configuration with another port pair.

Policies tab-> Security

Name	Tag	Source			Destination		Application	Service	Action	Profile	Options
		Zone	Address	User	Zone	Address					
rule1	none	trust	any	any	untrust	any	any	any	<input checked="" type="checkbox"/>		
rule2	none	untrust	any	any	trust	any	any	any	<input checked="" type="checkbox"/>		

Configure a security policy that allows traffic to flow between the vwire zones. Assign security profiles to inspect for viruses, spyware, vulnerabilities, files, data, and URLs as appropriate. In our sample security policy, “rule1” allows traffic to be initiated from the “trust” zone to the “untrust” zone and “rule2” allows traffic to be initiated from the “untrust” zone to the “trust” zone. After you have traffic flowing through the firewall using the wide-open policies above, you should modify your policies to limit the traffic flows through the device to those that are needed for the environment.

High-Availability

For a detailed description of how HA works and an explanation of the various settings, please refer to the following document in our knowledge base for Active/Passive HA, <https://live.paloaltonetworks.com/docs/DOC-1160>.

Note that in this example since it is from a PA-2050 and there are not dedicated HA links, the following interfaces are used for HA functions:

- Ethernet1/15 for the HA1 link
- Ethernet1/16 for the HA2 link
- Ethernet1/13 for the HA1 backup link

If this was a PA-Series device that had dedicated HA ports, then these dedicated HA1 and HA2 ports could be used instead of Ethernet port 1/15 and 1/16. An Ethernet interface would still be used for the HA1 backup link.

Device tab -> High Availability -> General subtab (A/P Firewall 1)

General	Link and Path Monitoring	Operational Commands
<div> <div> Setup <ul style="list-style-type: none"> Enable HA <input checked="" type="checkbox"/> Group ID 11 Description vwire Mode active-passive Enable Config Sync <input checked="" type="checkbox"/> Peer HA1 IP Address 1.1.1.2 Backup Peer HA1 IP Address 1.1.1.6 </div> <div> Active/Passive Settings <ul style="list-style-type: none"> Passive Link State auto Monitor Fail Hold Down Time 1 (min) </div> <div> Election Settings <ul style="list-style-type: none"> Heartbeat Backup <input type="checkbox"/> Preemptive <input checked="" type="checkbox"/> Promotion Hold Time (ms) 2000 Hello Interval (ms) 8000 Heartbeat Interval (ms) 1000 Maximum No. of Flaps 3 Preemption Hold Time (min) 1 Monitor Fail Hold Up Time (ms) 0 Additional Master Hold Up Time (ms) 500 Device Priority 10 </div> </div>		
<div> <div> Control Link (HA1) <ul style="list-style-type: none"> Port ethernet1/15 IPv4/IPv6 Address 1.1.1.1 Netmask 255.255.255.252 Gateway Encryption Enabled <input type="checkbox"/> Monitor Hold Time (ms) 3000 </div> <div> Control Link (HA1 Backup) <ul style="list-style-type: none"> Port ethernet1/13 IPv4/IPv6 Address 1.1.1.5 Netmask 255.255.255.252 Gateway </div> <div> Data Link (HA2) <ul style="list-style-type: none"> Enable Session Synchronization <input checked="" type="checkbox"/> Port ethernet1/16 IPv4/IPv6 Address Netmask Gateway Transport ethernet Action log-only Threshold (ms) 10000 </div> <div> Data Link (HA2 Backup) <ul style="list-style-type: none"> Port IPv4/IPv6 Address Netmask Gateway </div> </div>		

Device tab -> High Availability -> Link and Path Monitoring subtab (A/P Firewall 1)

General

Link and Path Monitoring

Operational Commands

Link Monitoring

Enabled ☒

Failure Condition any

Link Group

	Name	Enabled	Group Failure Condition	Interfaces
<input type="checkbox"/>	wire	<input checked="" type="checkbox"/>	any	ethernet1/1 ethernet1/2

+ Add

- Delete

Path Monitoring

Enabled ☐

Failure Condition any

Path Group

	Name	Type	Enabled	Failure Condition	Source IP	Destination IP	Ping Interval
--	------	------	---------	-------------------	-----------	----------------	---------------

+ Add Virtual Wire Path

+ Add VLAN Path

+ Add Virtual Router Path

- Delete

Device tab -> High Availability -> General subtab (A/P Firewall 2)

General	Link and Path Monitoring	Operational Commands
<div> <div> Setup </div> <div> <p>Enable HA <input checked="" type="checkbox"/></p> <p>Group ID 11</p> <p>Description vwire</p> <p>Mode active-passive</p> <p>Enable Config Sync <input checked="" type="checkbox"/></p> <p>Peer HA1 IP Address 1.1.1.1</p> <p>Backup Peer HA1 IP Address 1.1.1.5</p> </div> </div>		
<div> <div> Active/Passive Settings </div> <div> <p>Passive Link State auto</p> <p>Monitor Fail Hold Down Time 1 (min)</p> </div> </div>		
<div> <div> Election Settings </div> <div> <p>Heartbeat Backup <input type="checkbox"/></p> <p>Preemptive <input checked="" type="checkbox"/></p> <p>Promotion Hold Time (ms) 2000</p> <p>Hello Interval (ms) 8000</p> <p>Heartbeat Interval (ms) 1000</p> <p>Maximum No. of Flaps 3</p> <p>Preemption Hold Time (min) 1</p> <p>Monitor Fail Hold Up Time (ms) 0</p> <p>Additional Master Hold Up Time (ms) 500</p> <p>Device Priority 100</p> </div> </div>		
<div> <div> Control Link (HA1) </div> <div> <p>Port ethernet1/15</p> <p>IPv4/IPv6 Address 1.1.1.2</p> <p>Netmask 255.255.255.252</p> <p>Gateway</p> <p>Encryption Enabled <input type="checkbox"/></p> <p>Monitor Hold Time (ms) 3000</p> </div> </div>		
<div> <div> Control Link (HA1 Backup) </div> <div> <p>Port ethernet1/13</p> <p>IPv4/IPv6 Address 1.1.1.6</p> <p>Netmask 255.255.255.252</p> <p>Gateway</p> </div> </div>		
<div> <div> Data Link (HA2) </div> <div> <p>Enable Session Synchronization <input checked="" type="checkbox"/></p> <p>Port ethernet1/16</p> <p>IPv4/IPv6 Address</p> <p>Netmask</p> <p>Gateway</p> <p>Transport ethernet</p> <p>Action log-only</p> <p>Threshold (ms) 10000</p> </div> </div>		
<div> <div> Data Link (HA2 Backup) </div> <div> <p>Port</p> <p>IPv4/IPv6 Address</p> <p>Netmask</p> <p>Gateway</p> </div> </div>		

Device tab -> High Availability -> Link and Path Monitoring subtab (A/P Firewall 2)

General

Link and Path Monitoring

Operational Commands

Link Monitoring

Enabled ☒

Failure Condition any

Link Group

Name	Enabled	Group Failure Condition	Interfaces
<input type="checkbox"/> vwire	<input checked="" type="checkbox"/>	any	ethernet1/1 ethernet1/2

+ Add

- Delete

Path Monitoring

Enabled ☐

Failure Condition any

Path Group

Name	Type	Enabled	Failure Condition	Source IP	Destination IP	Ping Interval
------	------	---------	-------------------	-----------	----------------	---------------

+ Add Virtual Wire Path

+ Add VLAN Path

+ Add Virtual Router Path

- Delete

CLI Configuration

The CLI commands used to configure this scenario are shown below: ²

```
# Network configuration for a vwire called default-vwire on ports 1 and 2

set network virtual-wire default-vwire interface1 ethernet1/1
set network virtual-wire default-vwire interface2 ethernet1/2
set network virtual-wire default-vwire tag-allowed 0-4094
set network virtual-wire default-vwire multicast-firewalling enable no
set network virtual-wire default-vwire link-state-pass-through enable yes

# Zone configuration

set zone trust network virtual-wire ethernet1/2
set zone trust enable-user-identification yes
set zone untrust network virtual-wire ethernet1/1

# Policy configuration

set rulebase security rules rule1 from trust
set rulebase security rules rule1 to untrust
set rulebase security rules rule1 source any
set rulebase security rules rule1 destination any
set rulebase security rules rule1 service any
set rulebase security rules rule1 application any
set rulebase security rules rule1 action allow
set rulebase security rules rule1 log-end yes
set rulebase security rules rule1 profile-setting profiles url-filtering default
set rulebase security rules rule1 profile-setting profiles virus default
set rulebase security rules rule1 profile-setting profiles spyware default
set rulebase security rules rule1 profile-setting profiles vulnerability default
set rulebase security rules rule2 profile-setting profiles url-filtering default
set rulebase security rules rule2 profile-setting profiles virus default
set rulebase security rules rule2 profile-setting profiles spyware default
set rulebase security rules rule2 profile-setting profiles vulnerability default
set rulebase security rules rule2 option disable-server-response-inspection no
set rulebase security rules rule2 from untrust
set rulebase security rules rule2 to trust
set rulebase security rules rule2 source any
set rulebase security rules rule2 destination any
set rulebase security rules rule2 source-user any
set rulebase security rules rule2 application any
set rulebase security rules rule2 service any
set rulebase security rules rule2 hip-profiles any
set rulebase security rules rule2 log-start no
set rulebase security rules rule2 log-end yes
set rulebase security rules rule2 negate-source no
set rulebase security rules rule2 negate-destination no
set rulebase security rules rule2 action allow
```

² This output was obtained by running these three commands: “set cli config-output-format set” , “configure”, and “show”. Only commands relevant to this particular scenario are listed.

```

# High Availability
# A/P HA configurations for each of the firewalls are listed below.

# The sample CLI configuration for a HA pair of PA-2050 with HA1 as port 15, HA2 as port 16
and HA1 backup as port 13. The HA group ID was set to 11, link monitoring was configured for
both vwire interfaces, and the passive link state was set to auto.

# A/P Firewall 1

set deviceconfig high-availability enabled yes
set deviceconfig high-availability interface ha1 port ethernet1/15
set deviceconfig high-availability interface ha1 ip-address 1.1.1.1
set deviceconfig high-availability interface ha1 netmask 255.255.255.252
set deviceconfig high-availability interface ha1 monitor-hold-time 3000
set deviceconfig high-availability interface ha1-backup port ethernet1/13
set deviceconfig high-availability interface ha1-backup ip-address 1.1.1.5
set deviceconfig high-availability interface ha1-backup netmask 255.255.255.252
set deviceconfig high-availability interface ha2 port ethernet1/16
set deviceconfig high-availability group 11 description vwire
set deviceconfig high-availability group 11 peer-ip 1.1.1.2
set deviceconfig high-availability group 11 peer-ip-backup 1.1.1.6
set deviceconfig high-availability group 11 election-option device-priority 10
set deviceconfig high-availability group 11 election-option heartbeat-backup no
set deviceconfig high-availability group 11 election-option preemptive yes
set deviceconfig high-availability group 11 election-option promotion-hold-time 2000
set deviceconfig high-availability group 11 election-option hello-interval 8000
set deviceconfig high-availability group 11 election-option heartbeat-interval 1000
set deviceconfig high-availability group 11 election-option flap-max 3
set deviceconfig high-availability group 11 election-option preemption-hold-time 1
set deviceconfig high-availability group 11 election-option monitor-fail-hold-up-time 0
set deviceconfig high-availability group 11 election-option additional-master-hold-up-time 500
set deviceconfig high-availability group 11 state-synchronization enabled yes
set deviceconfig high-availability group 11 state-synchronization transport ethernet
set deviceconfig high-availability group 11 configuration-synchronization enabled yes
set deviceconfig high-availability group 11 mode active-passive passive-link-state auto
set deviceconfig high-availability group 11 mode active-passive monitor-fail-hold-down-time 1
set deviceconfig high-availability group 11 monitoring path-monitoring enabled no
set deviceconfig high-availability group 11 monitoring link-monitoring enabled yes
set deviceconfig high-availability group 11 monitoring link-monitoring failure-condition any
set deviceconfig high-availability group 11 monitoring link-monitoring link-group vwire
enabled yes
set deviceconfig high-availability group 11 monitoring link-monitoring link-group vwire
failure-condition any
set deviceconfig high-availability group 11 monitoring link-monitoring link-group vwire
interface ethernet1/1
set deviceconfig high-availability group 11 monitoring link-monitoring link-group vwire
interface ethernet1/2

# A/P Firewall 2

set deviceconfig high-availability enabled yes
set deviceconfig high-availability interface ha1 port ethernet1/15
set deviceconfig high-availability interface ha1 ip-address 1.1.1.2
set deviceconfig high-availability interface ha1 netmask 255.255.255.252
set deviceconfig high-availability interface ha1 monitor-hold-time 3000
set deviceconfig high-availability interface ha1-backup port ethernet1/13
set deviceconfig high-availability interface ha1-backup ip-address 1.1.1.6
set deviceconfig high-availability interface ha1-backup netmask 255.255.255.252
set deviceconfig high-availability interface ha2 port ethernet1/16
set deviceconfig high-availability group 11 description vwire
set deviceconfig high-availability group 11 peer-ip 1.1.1.1

```

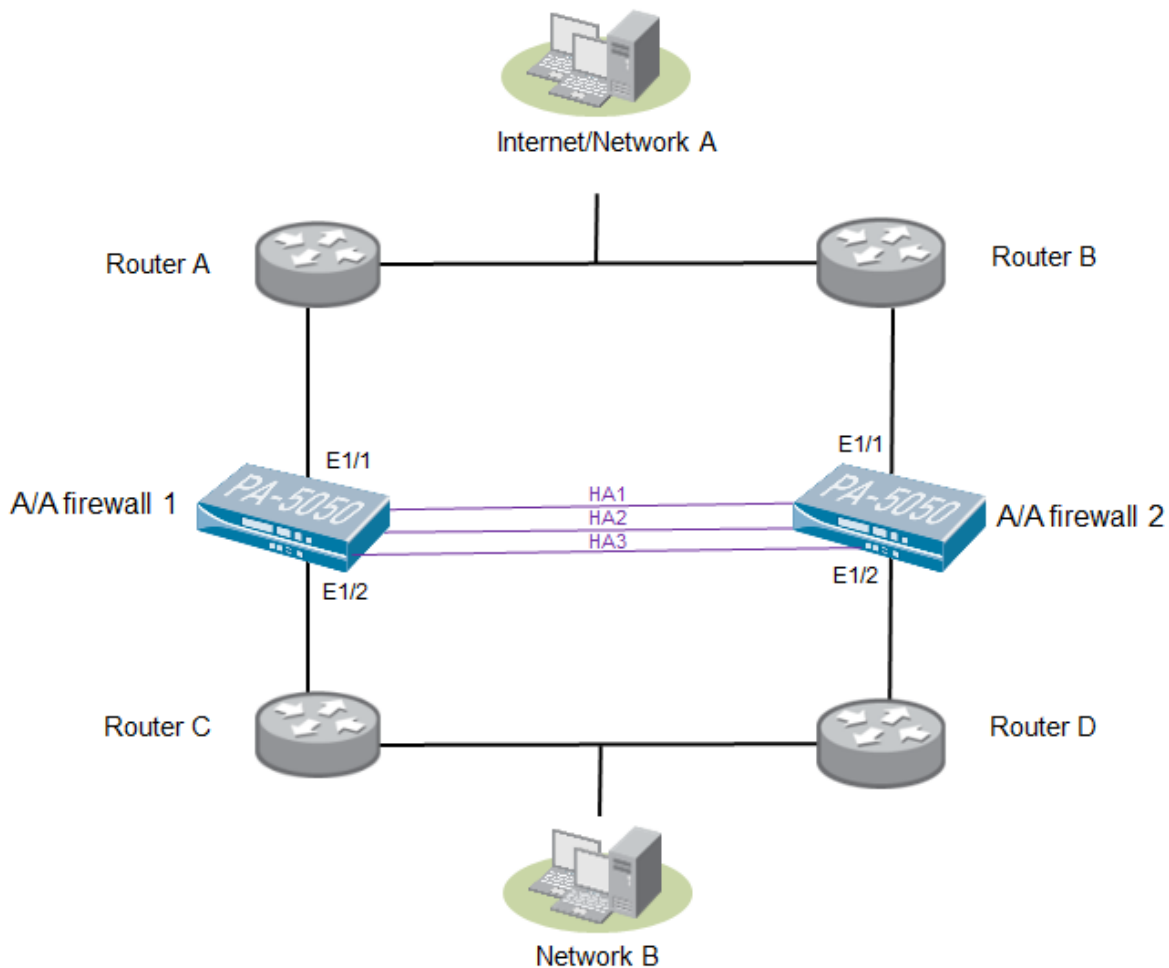
```

set deviceconfig high-availability group 11 peer-ip-backup 1.1.1.5
set deviceconfig high-availability group 11 election-option device-priority 100
set deviceconfig high-availability group 11 election-option heartbeat-backup no
set deviceconfig high-availability group 11 election-option preemptive yes
set deviceconfig high-availability group 11 election-option promotion-hold-time 2000
set deviceconfig high-availability group 11 election-option hello-interval 8000
set deviceconfig high-availability group 11 election-option heartbeat-interval 1000
set deviceconfig high-availability group 11 election-option flap-max 3
set deviceconfig high-availability group 11 election-option preemption-hold-time 1
set deviceconfig high-availability group 11 election-option monitor-fail-hold-up-time 0
set deviceconfig high-availability group 11 election-option additional-master-hold-up-time 500
set deviceconfig high-availability group 11 state-synchronization enabled yes
set deviceconfig high-availability group 11 state-synchronization transport ethernet
set deviceconfig high-availability group 11 configuration-synchronization enabled yes
set deviceconfig high-availability group 11 mode active-passive passive-link-state auto
set deviceconfig high-availability group 11 mode active-passive monitor-fail-hold-down-time 1
set deviceconfig high-availability group 11 monitoring path-monitoring enabled no
set deviceconfig high-availability group 11 monitoring link-monitoring enabled yes
set deviceconfig high-availability group 11 monitoring link-monitoring failure-condition any
set deviceconfig high-availability group 11 monitoring link-monitoring link-group vwire
enabled yes
set deviceconfig high-availability group 11 monitoring link-monitoring link-group vwire
failure-condition any
set deviceconfig high-availability group 11 monitoring link-monitoring link-group vwire
interface ethernet1/1
set deviceconfig high-availability group 11 monitoring link-monitoring link-group vwire
interface ethernet1/2

```

2.3 Example Scenario: Virtual Wire with Active/Active HA

The advantage of implementing virtual wire with Active/Active (A/A) HA is that both paths are active, and asymmetric traffic can be sent through the network with no issues.



Note: Implementing A/A HA in vwire mode in a Layer 2 sandwich will result in switching loops if Spanning Tree Protocol is not enabled on the switches. It is recommended to deploy A/A HA in vwire in a Layer 3 topology where the paths router A – router C and router B – router D are point-to-point.

GUI Configuration

The following screenshots are of a completed Active/Active HA virtual wire configuration.

Network tab -> Zones

	Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	Enable User Identification	User ID Include List	User ID Exclude List
<input checked="" type="checkbox"/>	trust	virtual-wire	ethernet1/2			<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	untrust	virtual-wire	ethernet1/1			<input type="checkbox"/>		

The pre-defined virtual-wire zones of “trust” and “untrust” are being used in this sample configuration. If you plan to implement User-ID, check the box to “enable user-identification” on the internal “trust” zone.

Network tab-> Interfaces -> Ethernet

Interface	Interface Type	Managem... Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features
ethernet1/1	Virtual Wire			none	none	Untagged	default-vwire	untrust	
ethernet1/2	Virtual Wire			none	none	Untagged	default-vwire	trust	

The factory-default configuration already has ethernet1/1 and ethernet1/2 in a virtual wire named “default-vwire”, with one interface in the “trust” zone and the other interface in the “untrust” zone. You can modify this sample configuration and use different vwire names or different zone names. Note for the vwire configuration that only two interfaces can be placed into the vwire definition - no more, no less. Additional vwires, using additional interfaces (and zones if needed) can be created to meet your specific design needs.

Network tab -> Virtual Wires

	Name	Interface1	Interface2	Tag Allowed	Multicast Firewalling	Link State Pass Through
<input checked="" type="checkbox"/>	default-vwire	ethernet1/1	ethernet1/2	0-4094	<input type="checkbox"/>	<input checked="" type="checkbox"/>

The factory-default configuration already has ethernet1/1 and ethernet1/2 in a virtual wire named “default-vwire”, with one interface in the “trust” zone and the other interface in the “untrust” zone. You can modify this sample configuration and use different vwire names or different zone names. Note for the vwire configuration that only two interfaces can be placed into the vwire definition - no more, no less. Additional vwires, using additional interfaces (and zones if needed) can be created to meet your specific design needs.

Policies tab-> Security

		Source			Destination						
Name	Tag	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
rule1	none	trust	any	any	untrust	any	any	any	<input checked="" type="checkbox"/>		
rule2	none	untrust	any	any	trust	any	any	any	<input checked="" type="checkbox"/>		

Configure a security policy that allows traffic to flow between the vwire zones. Assign security profiles to inspect for viruses, spyware, vulnerabilities, files, data, and URLs as appropriate. In our sample security policy, “rule1” allows traffic to be initiated from the “trust” zone to the “untrust” zone and “rule2” allows traffic to be initiated from the “untrust” zone to the “trust” zone. After you have traffic flowing through the firewall using the wide-open policies above, you should modify your policies to limit the traffic flows through the device to those that are needed for the environment.

High-Availability

For a detailed description of how HA works and the various settings, please refer to the following document in our knowledge base for the A/A HA, <https://live.paloaltonetworks.com/docs/DOC-1756>.

Note that in this example since it is from a PA-2050 and there are not dedicated HA links, the following interfaces are used for HA functions:

- o Ethernet1/15 for the HA1 link
- o Ethernet1/16 for the HA2 link
- o Ethernet1/14 for the HA3 link
- o Ethernet1/13 for the HA1 backup link

If this was a PA-Series device that had dedicated HA ports, then these dedicated HA1 and HA2 ports could be used instead of Ethernet port 1/15 and 1/16. An Ethernet interface would still be used for the HA1 backup link and the HA3 link.

Device tab -> High Availability -> General subtab (A/A Firewall 1)

General | **Link and Path Monitoring** | **Active/Active Config** | **Operational Commands**

Setup

- Enable HA ☒
- Group ID **1**
- Description **vwire**
- Mode **active-active**
- Device ID **0**
- Enable Config Sync ☒
- Peer HA1 IP Address **192.168.1.1**
- Backup Peer HA1 IP Address **1.1.1.6**

Election Settings

- Heartbeat Backup ☒
- Preemptive ☐
- Promotion Hold Time (ms) **0**
- Hello Interval (ms) **8000**
- Heartbeat Interval (ms) **1000**
- Maximum No. of Flaps **0**
- Preemption Hold Time (min) **1**
- Monitor Fail Hold Up Time (ms) **0**
- Additional Master Hold Up Time (ms) **0**
- Device Priority **1**

Control Link (HA1)

- Port **ethernet1/15**
- IPv4/IPv6 Address **192.168.1.2**
- Netmask **255.255.255.252**
- Gateway
- Encryption Enabled ☐
- Monitor Hold Time (ms) **3000**

Control Link (HA1 Backup)

- Port **ethernet1/13**
- IPv4/IPv6 Address **1.1.1.5**
- Netmask **255.255.255.252**
- Gateway

Data Link (HA2)

- Enable Session Synchronization ☒
- Port **ethernet1/16**
- IPv4/IPv6 Address
- Netmask
- Gateway
- Transport **ethernet**
- Action **log-only**
- Threshold (ms) **10000**

Data Link (HA2 Backup)

- Port
- IPv4/IPv6 Address
- Netmask
- Gateway

Device tab -> High Availability -> Active/Active Config subtab (A/A Firewall 1)

General
Link and Path Monitoring
Active/Active Config
Operational Commands

Packet Forwarding

Enable ☒
HA3 Interface ethernet1/14
VR Sync ☐
QoS Sync ☐
Tentative Hold Time (sec) 60
Session Owner Selection first-packet
Session Setup primary-device

Virtual Address

Name	Address	Type	Details
<div> + Add - Delete </div>			

Device tab -> High Availability -> Link and Path Monitoring subtab (A/A Firewall 1)

General
Link and Path Monitoring
Active/Active Config
Operational Commands

Link Monitoring

Enabled ☒
Failure Condition any

Link Group

	Name	Enabled	Group Failure Condition	Interfaces
<input type="checkbox"/>	wwire	<input checked="" type="checkbox"/>	any	ethernet1/1 ethernet1/2
<div> + Add - Delete </div>				

Path Monitoring

Enabled ☐
Failure Condition any

Path Group

	Name	Type	Enabled	Failure Condition	Source IP	Destination IP	Ping Interval
<div> + Add Virtual Wire Path + Add VLAN Path + Add Virtual Router Path - Delete </div>							

Device tab -> High Availability -> General subtab (A/A Firewall 2)

General	Link and Path Monitoring	Active/Active Config	Operational Commands
<div> <div> Setup </div> <div> <p>Enable HA <input checked="" type="checkbox"/></p> <p>Group ID 1</p> <p>Description vwire</p> <p>Mode active-active</p> <p>Device ID 1</p> <p>Enable Config Sync <input checked="" type="checkbox"/></p> <p>Peer HA1 IP Address 192.168.1.2</p> <p>Backup Peer HA1 IP Address 1.1.1.5</p> </div> </div>			
<div> <div> Election Settings </div> <div> <p>Heartbeat Backup <input type="checkbox"/></p> <p>Preemptive <input type="checkbox"/></p> <p>Promotion Hold Time (ms) 0</p> <p>Hello Interval (ms) 8000</p> <p>Heartbeat Interval (ms) 1000</p> <p>Maximum No. of Flaps 0</p> <p>Preemption Hold Time (min) 1</p> <p>Monitor Fail Hold Up Time (ms) 0</p> <p>Additional Master Hold Up Time (ms) 0</p> <p>Device Priority 100</p> </div> </div>			
<div> <div> Control Link (HA1) </div> <div> <p>Port ethernet1/15</p> <p>IPv4/IPv6 Address 192.168.1.1</p> <p>Netmask 255.255.255.252</p> <p>Gateway</p> <p>Encryption Enabled <input type="checkbox"/></p> <p>Monitor Hold Time (ms) 3000</p> </div> </div>			
<div> <div> Control Link (HA1 Backup) </div> <div> <p>Port ethernet1/13</p> <p>IPv4/IPv6 Address 1.1.1.6</p> <p>Netmask 255.255.255.252</p> <p>Gateway</p> </div> </div>			
<div> <div> Data Link (HA2) </div> <div> <p>Enable Session Synchronization <input checked="" type="checkbox"/></p> <p>Port ethernet1/16</p> <p>IPv4/IPv6 Address</p> <p>Netmask</p> <p>Gateway</p> <p>Transport ethernet</p> <p>Action log-only</p> <p>Threshold (ms) 10000</p> </div> </div>			
<div> <div> Data Link (HA2 Backup) </div> <div> <p>Port</p> <p>IPv4/IPv6 Address</p> <p>Netmask</p> <p>Gateway</p> </div> </div>			

Device tab -> High Availability -> Active/Active Config subtab (A/A Firewall 2)

General Link and Path Monitoring **Active/Active Config** Operational Commands

Packet Forwarding

Enable ☒

HA3 Interface ethernet1/14

VR Sync ☐

QoS Sync ☐

Tentative Hold Time (sec) 60

Session Owner Selection first-packet

Session Setup primary-device

Virtual Address

Name	Address	Type	Details
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>			

Device tab -> High Availability -> Link and Path Monitoring subtab (A/A Firewall 2)

General **Link and Path Monitoring** Active/Active Config Operational Commands

Link Monitoring

Enabled ☒

Failure Condition any

Link Group

Name	Enabled	Group Failure Condition	Interfaces
<input type="checkbox"/> vwire	<input checked="" type="checkbox"/>	any	ethernet1/1 ethernet1/2
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>			

Path Monitoring

Enabled ☐

Failure Condition any

Path Group

Name	Type	Enabled	Failure Condition	Source IP	Destination IP	Ping Interval
<input type="button" value="+ Add Virtual Wire Path"/> <input type="button" value="+ Add VLAN Path"/> <input type="button" value="+ Add Virtual Router Path"/> <input type="button" value="- Delete"/>						

CLI Configuration

The CLI commands used to configure this scenario are shown below: ³

```
# Network configuration for a vwire called default-vwire on ethernet ports 1 and 2

set network virtual-wire default-vwire interface1 ethernet1/1
set network virtual-wire default-vwire interface2 ethernet1/2
set network virtual-wire default-vwire tag-allowed 0-4094
set network virtual-wire default-vwire multicast-firewalling enable no
set network virtual-wire default-vwire link-state-pass-through enable yes

# Zone Configuration

set zone trust network virtual-wire ethernet1/2
set zone trust enable-user-identification yes
set zone untrust network virtual-wire ethernet1/1

# Policy Configuration

set rulebase security rules rule1 from trust
set rulebase security rules rule1 to untrust
set rulebase security rules rule1 source any
set rulebase security rules rule1 destination any
set rulebase security rules rule1 service any
set rulebase security rules rule1 application any
set rulebase security rules rule1 action allow
set rulebase security rules rule1 log-end yes
set rulebase security rules rule1 profile-setting profiles url-filtering default
set rulebase security rules rule1 profile-setting profiles virus default
set rulebase security rules rule1 profile-setting profiles spyware default
set rulebase security rules rule1 profile-setting profiles vulnerability default
set rulebase security rules rule2 profile-setting profiles url-filtering default
set rulebase security rules rule2 profile-setting profiles virus default
set rulebase security rules rule2 profile-setting profiles spyware default
set rulebase security rules rule2 profile-setting profiles vulnerability default
set rulebase security rules rule2 option disable-server-response-inspection no
set rulebase security rules rule2 from untrust
set rulebase security rules rule2 to trust
set rulebase security rules rule2 source any
set rulebase security rules rule2 destination any
set rulebase security rules rule2 source-user any
set rulebase security rules rule2 application any
set rulebase security rules rule2 service any
set rulebase security rules rule2 hip-profiles any
set rulebase security rules rule2 log-start no
set rulebase security rules rule2 log-end yes
set rulebase security rules rule2 negate-source no
set rulebase security rules rule2 negate-destination no
set rulebase security rules rule2 action allow

# High Availability
# A/A HA configurations for each of the firewalls are listed below.

# The sample CLI configuration for a HA pair of PA-2050 with HA1 as port 15, HA2 as port 16,
HA3 as port 14, and HA1 backup as port 13. The HA group ID was set to 1, link monitoring was
configured for both vwire interfaces, and A/A Firewall 1 has lowest 'device priority'.
```

³ This output was obtained by running these three commands: "set cli config-output-format set", "configure", and "show". Only commands relevant to this particular scenario are listed.

A/A High Availability Configuration - A/A Firewall 1

```
set deviceconfig high-availability enabled yes
set deviceconfig high-availability interface ha1 ip-address 192.168.1.2
set deviceconfig high-availability interface ha1 netmask 255.255.255.252
set deviceconfig high-availability interface ha1 monitor-hold-time 3000
set deviceconfig high-availability interface ha1 port ethernet1/15
set deviceconfig high-availability interface ha1-backup ip-address 1.1.1.5
set deviceconfig high-availability interface ha1-backup netmask 255.255.255.252
set deviceconfig high-availability interface ha1-backup port ethernet1/13
set deviceconfig high-availability interface ha2 port ethernet1/16
set deviceconfig high-availability interface ha3 port ethernet1/14
set deviceconfig high-availability group 1 description vwire
set deviceconfig high-availability group 1 peer-ip 192.168.1.1
set deviceconfig high-availability group 1 peer-ip-backup 1.1.1.6
set deviceconfig high-availability group 1 election-option device-priority 1
set deviceconfig high-availability group 1 election-option heartbeat-backup yes
set deviceconfig high-availability group 1 election-option preemptive no
set deviceconfig high-availability group 1 election-option promotion-hold-time 0
set deviceconfig high-availability group 1 election-option hello-interval 8000
set deviceconfig high-availability group 1 election-option heartbeat-interval 1000
set deviceconfig high-availability group 1 election-option flap-max 0
set deviceconfig high-availability group 1 election-option preemption-hold-time 1
set deviceconfig high-availability group 1 election-option monitor-fail-hold-up-time 0
set deviceconfig high-availability group 1 election-option additional-master-hold-up-time 0
set deviceconfig high-availability group 1 state-synchronization enabled yes
set deviceconfig high-availability group 1 state-synchronization transport ethernet
set deviceconfig high-availability group 1 configuration-synchronization enabled yes
set deviceconfig high-availability group 1 mode active-active device-id 0
set deviceconfig high-availability group 1 mode active-active network-configuration sync qos
no
set deviceconfig high-availability group 1 mode active-active network-configuration sync
virtual-router no
set deviceconfig high-availability group 1 mode active-active packet-forwarding yes
set deviceconfig high-availability group 1 mode active-active session-owner-selection first-
packet session-setup primary-device
set deviceconfig high-availability group 1 monitoring path-monitoring enabled no
set deviceconfig high-availability group 1 monitoring link-monitoring enabled yes
set deviceconfig high-availability group 1 monitoring link-monitoring failure-condition any
set deviceconfig high-availability group 1 monitoring link-monitoring link-group vwire enabled
yes
set deviceconfig high-availability group 1 monitoring link-monitoring link-group vwire
failure-condition any
set deviceconfig high-availability group 1 monitoring link-monitoring link-group vwire
interface [ ethernet1/1 ethernet1/2 ]
```

A/A High Availability Configuration - A/A Firewall 2

```
set deviceconfig high-availability enabled yes
set deviceconfig high-availability interface ha1 port ethernet1/15
set deviceconfig high-availability interface ha1 ip-address 192.168.1.1
set deviceconfig high-availability interface ha1 netmask 255.255.255.252
set deviceconfig high-availability interface ha1 monitor-hold-time 3000
set deviceconfig high-availability interface ha1-backup port ethernet1/13
set deviceconfig high-availability interface ha1-backup ip-address 1.1.1.6
set deviceconfig high-availability interface ha1-backup netmask 255.255.255.252
set deviceconfig high-availability interface ha2 port ethernet1/16
set deviceconfig high-availability interface ha2-backup
set deviceconfig high-availability interface ha3 port ethernet1/14
set deviceconfig high-availability group 1 description vwire
set deviceconfig high-availability group 1 peer-ip 192.168.1.2
```

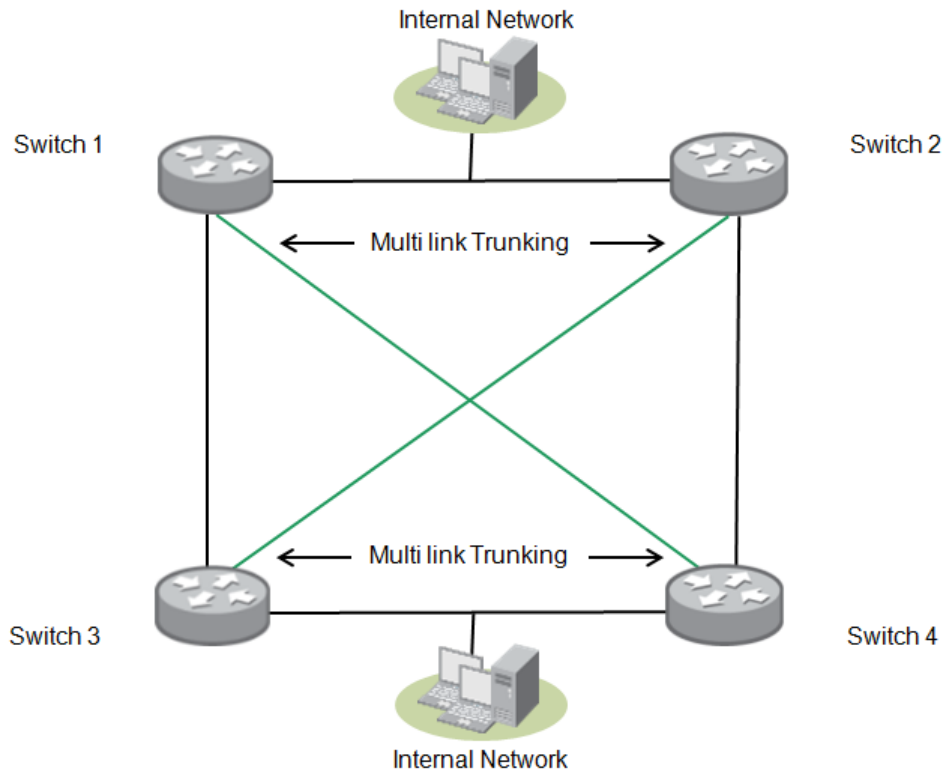
```

set deviceconfig high-availability group 1 mode active-active device-id 1
set deviceconfig high-availability group 1 configuration-synchronization enabled yes
set deviceconfig high-availability group 1 peer-ip-backup 1.1.1.5
set deviceconfig high-availability group 1 election-option device-priority 100
set deviceconfig high-availability group 1 election-option heartbeat-backup no
set deviceconfig high-availability group 1 election-option preemptive no
set deviceconfig high-availability group 1 election-option promotion-hold-time 0
set deviceconfig high-availability group 1 election-option hello-interval 8000
set deviceconfig high-availability group 1 election-option heartbeat-interval 1000
set deviceconfig high-availability group 1 election-option flap-max 0
set deviceconfig high-availability group 1 election-option preemption-hold-time 1
set deviceconfig high-availability group 1 election-option monitor-fail-hold-up-time 0
set deviceconfig high-availability group 1 election-option additional-master-hold-up-time 0
set deviceconfig high-availability group 1 state-synchronization enabled yes
set deviceconfig high-availability group 1 state-synchronization transport ethernet
set deviceconfig high-availability group 1 mode active-active network-configuration sync
virtual-router no
set deviceconfig high-availability group 1 mode active-active network-configuration sync qos
no
set deviceconfig high-availability group 1 mode active-active packet-forwarding yes
set deviceconfig high-availability group 1 mode active-active session-owner-selection first-
packet session-setup primary-device
set deviceconfig high-availability group 1 monitoring path-monitoring enabled no
set deviceconfig high-availability group 1 monitoring link-monitoring enabled yes
set deviceconfig high-availability group 1 monitoring link-monitoring failure-condition any
set deviceconfig high-availability group 1 monitoring link-monitoring link-group vwire enabled
yes
set deviceconfig high-availability group 1 monitoring link-monitoring link-group vwire
failure-condition any
set deviceconfig high-availability group 1 monitoring link-monitoring link-group vwire
interface [ ethernet1/1 ethernet1/2 ]

```

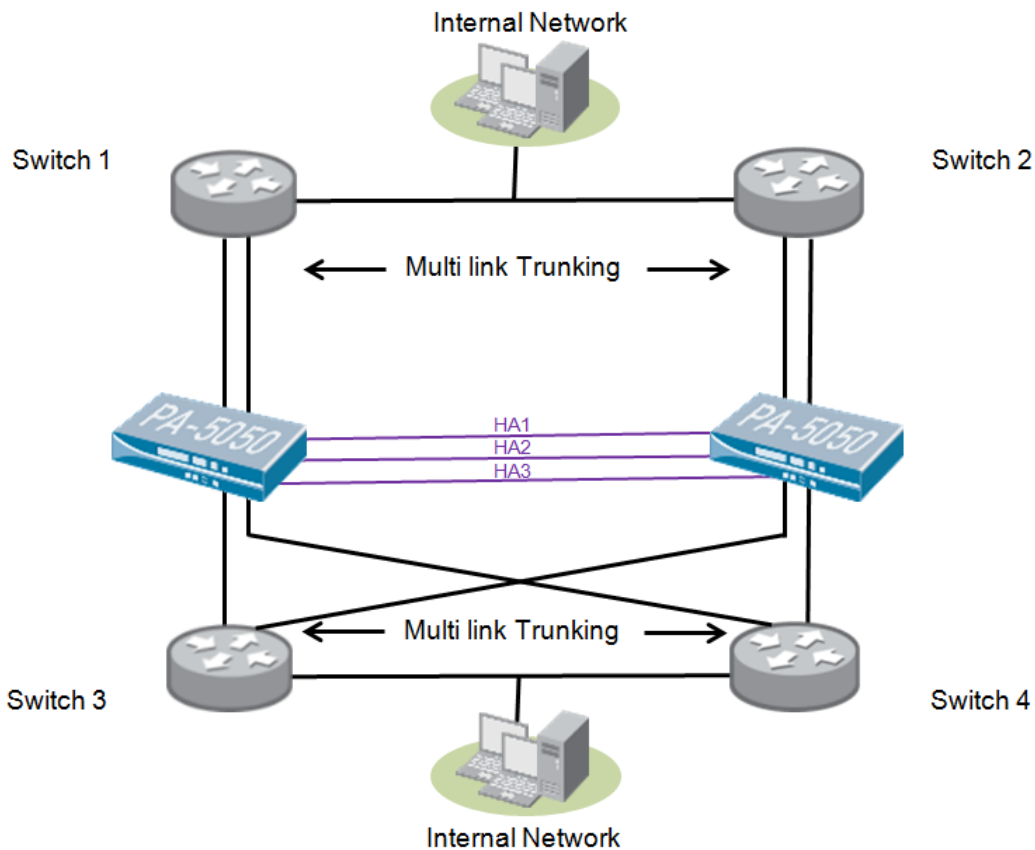

2.4 Example Scenario: Virtual Wire with A/A HA and Link Aggregation on Adjacent Switches

Below is a sample diagram of a network where security protection may be desired to provide protection between the two networks (top network and bottom network) where the switched environment is making use of link aggregation (802.3ad) and optimized redundancy such as Nortel SMLT, Cisco VSS, Cisco vPC or Juniper VC. In many of these configurations extensive VLAN trunking is used on top of link aggregation.



Suggested Network Design

As shown in the figure below, the Palo Alto Networks firewalls are installed between Layer 2/Layer 3 devices. These are often used in conjunction with dynamic routing protocols, which will fail traffic over to the other peer member, if needed.

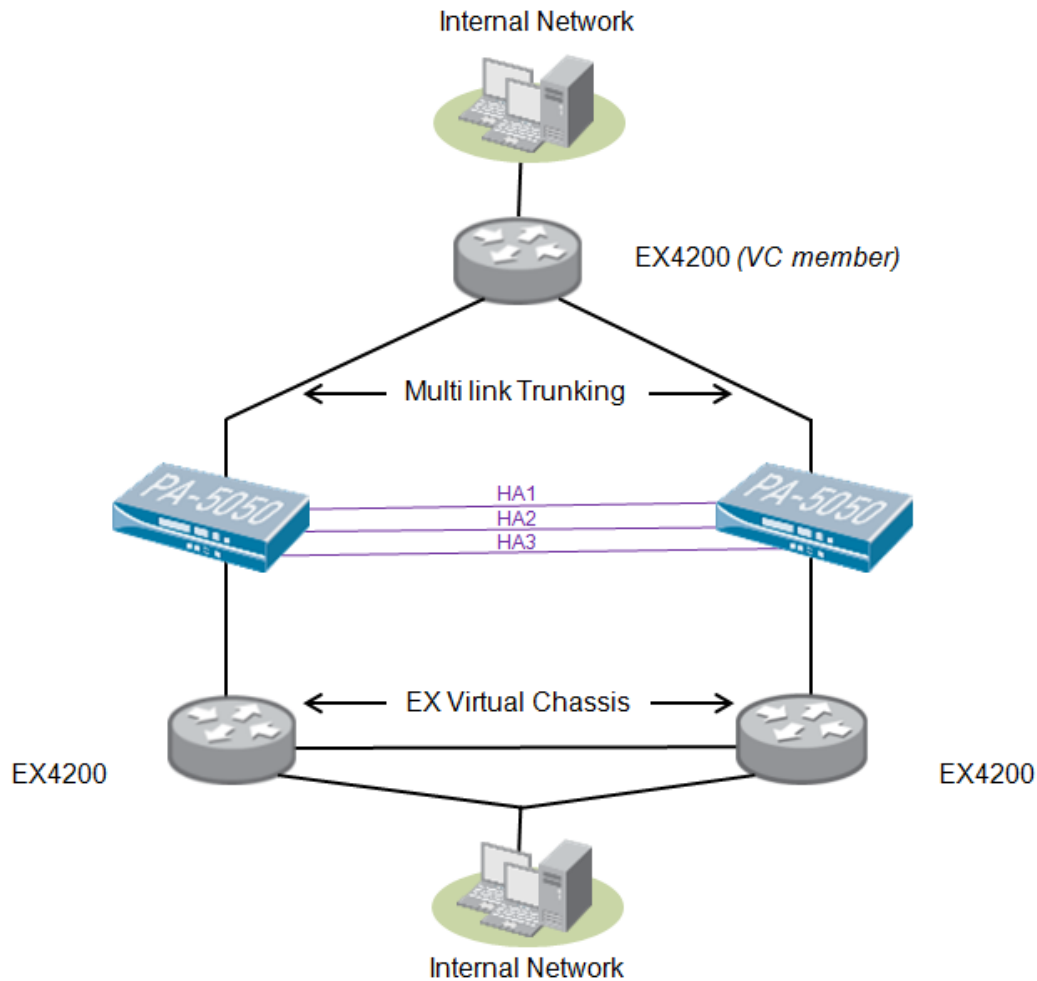


Note: Implementing A/A HA in vwire mode in a Layer 2 sandwich will result in switching loops if Spanning Tree Protocol is not enabled on the switches. It is recommended to deploy A/A HA in vwire in a layer3 topology. Using 802.3ad or a similar link aggregation technology will avoid potential loops while making use of the aggregate performance in an A/A environment.

Configuration Example

This setup was tested in combination with Juniper EX switches (EX4200 – Junos 10.4R3.4) where 2 of the switches are configured as a Virtual Chassis (VC). A similar setup can be constructed by using independent switches. A simplified configuration extract from the switches is included in this document.









Several failover scenarios were tested and all resulted in a sub-second failover when one of the firewalls or switches was failed. LACP configuration is recommended for the aggregate ports on the switches to avoid configuration mistakes and fast failover. LACP is transparent for the Palo Alto Networks firewall in vwire mode and no additional configuration on the firewall is required for LACP.



GUI Configuration

The following screenshots are of a completed configuration.

Network tab-> Interfaces -> Ethernet subtab

Ethernet VLAN Loopback Tunnel									
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features
 ethernet1/1	Virtual Wire			none	none	Untagged	default-vwire	untrust	
 ethernet1/2	Virtual Wire			none	none	Untagged	default-vwire	trust	
 ethernet1/3	Virtual Wire			none	none	Untagged	second-vwire	untrust	
 ethernet1/4	Virtual Wire			none	none	Untagged	second-vwire	trust	

Network tab-> Virtual Wires

	Name	Interface1	Interface2	Tag Allowed	Multicast Firewalling	Link State Pass Through
<input type="checkbox"/>	default-vwire	ethernet1/1	ethernet1/2	0-4094	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	second-vwire	ethernet1/3	ethernet1/4	0-4094	<input type="checkbox"/>	<input checked="" type="checkbox"/>















The factory-default vwire (default-vwire) is used for interfaces ethernet1/1 and ethernet1/2 and a second vwire (second-vwire) is created for interfaces ethernet1/3 and ethernet1/4.

Network tab -> Zones

	Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	Enable User Identification	User ID Include List	User ID Exclude List
<input checked="" type="checkbox"/>	trust	virtual-wire	ethernet1/2 ethernet1/4			<input checked="" type="checkbox"/>		
<input type="checkbox"/>	untrust	virtual-wire	ethernet1/1 ethernet1/3			<input type="checkbox"/>		

The factory-default zones are used for both of the defined vwires. This allows traffic to flow across either vwire symmetrically or asymmetrically and still allow the firewall to track the session on the common zone boundaries.

Policies tab-> Security

		Source			Destination						
Name	Tag	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
rule1	none	 trust	any	any	 untrust	any	any	any	<input checked="" type="checkbox"/>	   	
rule2	none	 untrust	any	any	 trust	any	any	any	<input checked="" type="checkbox"/>	   	

Configure a security policy that allows traffic to flow between the vwire zones. Assign security profiles to inspect for viruses, spyware, vulnerabilities, files, data, and URLs as appropriate.

Device tab -> High Availability -> General subtab (A/A Firewall 1)

General	Link and Path Monitoring	Active/Active Config	Operational Commands
<div> <div> <h3>Setup</h3> <ul style="list-style-type: none"> Enable HA <input checked="" type="checkbox"/> Group ID 3 Description Mode active-active Device ID 0 Enable Config Sync <input checked="" type="checkbox"/> Peer HA1 IP Address 172.16.1.101 Backup Peer HA1 IP Address </div> <div> <h3>Election Settings</h3> <ul style="list-style-type: none"> Heartbeat Backup <input checked="" type="checkbox"/> Preemptive <input type="checkbox"/> Promotion Hold Time (ms) 2000 Hello Interval (ms) 8000 Heartbeat Interval (ms) 1000 Maximum No. of Flaps 3 Preemption Hold Time (min) 1 Monitor Fail Hold Up Time (ms) 0 Additional Master Hold Up Time (ms) 500 Device Priority 100 </div> </div>			
<div> <div> <h3>Control Link (HA1)</h3> <ul style="list-style-type: none"> Port ethernet1/13 IPv4/IPv6 Address 172.16.1.100 Netmask 255.255.255.0 Gateway Encryption Enabled <input type="checkbox"/> Monitor Hold Time (ms) 3000 </div> <div> <h3>Control Link (HA1 Backup)</h3> <ul style="list-style-type: none"> Port IPv4/IPv6 Address Netmask Gateway </div> <div> <h3>Data Link (HA2)</h3> <ul style="list-style-type: none"> Enable Session Synchronization <input checked="" type="checkbox"/> Port ethernet1/14 IPv4/IPv6 Address Netmask Gateway Transport ethernet Action log-only Threshold (ms) 10000 </div> <div> <h3>Data Link (HA2 Backup)</h3> <ul style="list-style-type: none"> Port IPv4/IPv6 Address Netmask Gateway </div> </div>			

Device tab -> High Availability -> Active/Active Config subtab (Device 1)

General

Link and Path Monitoring

Active/Active Config

Operational Commands

Packet Forwarding

Enable

☒

HA3 Interface

ethernet1/15

VR Sync

☐

QoS Sync

☐

Tentative Hold Time (sec)

60

Session Owner Selection

first-packet

Session Setup

ip-module

Virtual Address

Name	Address	Type	Details
------	---------	------	---------

+ Add

- Delete

Device tab -> High Availability -> General subtab (Device 2)

General	Link and Path Monitoring	Active/Active Config	Operational Commands
Setup			
Enable HA <input checked="" type="checkbox"/>			
Group ID 3			
Description			
Mode active-active			
Device ID 1			
Enable Config Sync <input checked="" type="checkbox"/>			
Peer HA1 IP Address 172.16.1.100			
Backup Peer HA1 IP Address			
Election Settings			
Heartbeat Backup <input checked="" type="checkbox"/>			
Preemptive <input type="checkbox"/>			
Promotion Hold Time (ms) 2000			
Hello Interval (ms) 8000			
Heartbeat Interval (ms) 1000			
Maximum No. of Flaps 3			
Preemption Hold Time (min) 1			
Monitor Fail Hold Up Time (ms) 0			
Additional Master Hold Up Time (ms) 500			
Device Priority 200			
Control Link (HA1)			
Port ethernet1/13			
IPv4/IPv6 Address 172.16.1.101			
Netmask 255.255.255.0			
Gateway			
Encryption Enabled <input type="checkbox"/>			
Monitor Hold Time (ms) 3000			
Control Link (HA1 Backup)			
Port			
IPv4/IPv6 Address			
Netmask			
Gateway			
Data Link (HA2)			
Enable Session Synchronization <input checked="" type="checkbox"/>			
Port ethernet1/14			
IPv4/IPv6 Address			
Netmask			
Gateway			
Transport ethernet			
Action log-only			
Threshold (ms) 10000			
Data Link (HA2 Backup)			
Port			
IPv4/IPv6 Address			
Netmask			
Gateway			

Device tab -> High Availability -> Active/Active Config subtab (Device 2)

General

Link and Path Monitoring

Active/Active Config

Operational Commands

Packet Forwarding

Enable

☒

HA3 Interface

ethernet1/15

VR Sync

☐

QoS Sync

☐

Tentative Hold Time (sec)

60

Session Owner Selection

first-packet

Session Setup

ip-modulo

Virtual Address

Name	Address	Type	Details
------	---------	------	---------

+ Add

- Delete

CLI Configuration

The CLI commands used to configure this scenario are shown below: ⁴

```
# Network configuration for a vwire on Port 3 and 4
# note that vwire on port 1 and 2 is factory default

set network interface ethernet ethernet1/1 virtual-wire
set network interface ethernet ethernet1/2 virtual-wire
set network interface ethernet ethernet1/3 link-state auto
set network interface ethernet ethernet1/3 link-duplex auto
set network interface ethernet ethernet1/3 link-speed auto
set network interface ethernet ethernet1/3 virtual-wire
set network interface ethernet ethernet1/4 link-state auto
set network interface ethernet ethernet1/4 link-duplex auto
set network interface ethernet ethernet1/4 link-speed auto
set network interface ethernet ethernet1/4 virtual-wire
set network virtual-wire default-vwire interface1 ethernet1/1
set network virtual-wire default-vwire interface2 ethernet1/2
set network virtual-wire default-vwire tag-allowed 0-4094
set network virtual-wire default-vwire multicast-firewalling enable no
set network virtual-wire default-vwire link-state-pass-through enable yes
set network virtual-wire second-vwire interface1 ethernet1/3
set network virtual-wire second-vwire interface2 ethernet1/4
set network virtual-wire second-vwire tag-allowed 0-4094
set network virtual-wire second-vwire multicast-firewalling enable no
set network virtual-wire second-vwire link-state-pass-through enable yes

# Zone configuration. Both vwires are in the same zones allowing session match on all
# ports belonging to the same security zone.

set zone trust network virtual-wire ethernet1/2
set zone trust network virtual-wire ethernet1/4
set zone untrust network virtual-wire ethernet1/1
set zone untrust network virtual-wire ethernet1/3

# Policy configuration. Allow traffic in any direction through the firewall.
# Rule1 is factory default allowing any traffic from trust to untrust (not shown)

set rulebase security rules rule1 from trust
set rulebase security rules rule1 to untrust
set rulebase security rules rule1 source any
set rulebase security rules rule1 destination any
set rulebase security rules rule1 service any
set rulebase security rules rule1 application any
set rulebase security rules rule1 action allow
set rulebase security rules rule1 log-end yes
set rulebase security rules rule1 profile-setting profiles url-filtering default
set rulebase security rules rule1 profile-setting profiles virus default
set rulebase security rules rule1 profile-setting profiles spyware default
set rulebase security rules rule1 profile-setting profiles vulnerability default
set rulebase security rules rule2 from untrust
set rulebase security rules rule2 to trust
set rulebase security rules rule2 source any
set rulebase security rules rule2 destination any
set rulebase security rules rule2 application any
set rulebase security rules rule2 service any
```

⁴ This output was obtained by running these three commands: “set cli config-output-format set”, “configure”, and “show”. Only commands relevant to this particular scenario are listed.

```

set rulebase security rules rule2 log-end yes
set rulebase security rules rule2 action allow
set rulebase security rules rule2 profile-setting profiles url-filtering default
set rulebase security rules rule2 profile-setting profiles virus default
set rulebase security rules rule2 profile-setting profiles spyware default
set rulebase security rules rule2 profile-setting profiles vulnerability default

# High Availability
# A/A HA configurations for each of the firewalls are listed below.

# The sample CLI configuration for a HA pair of PA-2050 with HA1 as port 13, HA2 as port 14, and
# HA3 as port 15. The HA group ID was set to 3, link monitoring was configured for both vwire
# interfaces, and Device #1 has lowest 'device priority'.

# Device 1

set deviceconfig high-availability group 3 mode active-active device-id 0
set deviceconfig high-availability group 3 mode active-active network-configuration sync virtual-
router no
set deviceconfig high-availability group 3 mode active-active network-configuration sync qos no
set deviceconfig high-availability group 3 mode active-active packet-forwarding yes
set deviceconfig high-availability group 3 peer-ip 172.16.1.101
set deviceconfig high-availability group 3 election-option device-priority 100
set deviceconfig high-availability group 3 election-option heartbeat-backup yes
set deviceconfig high-availability group 3 election-option preemptive no
set deviceconfig high-availability group 3 election-option promotion-hold-time 2000
set deviceconfig high-availability group 3 election-option hello-interval 8000
set deviceconfig high-availability group 3 election-option heartbeat-interval 1000
set deviceconfig high-availability group 3 election-option flap-max 3
set deviceconfig high-availability group 3 election-option preemption-hold-time 1
set deviceconfig high-availability group 3 election-option monitor-fail-hold-up-time 0
set deviceconfig high-availability group 3 election-option additional-master-hold-up-time 500
set deviceconfig high-availability group 3 state-synchronization enabled yes
set deviceconfig high-availability group 3 state-synchronization transport ethernet
set deviceconfig high-availability group 3 configuration-synchronization enabled yes
set deviceconfig high-availability group 3 monitoring path-monitoring enabled no
set deviceconfig high-availability group 3 monitoring link-monitoring enabled no
set deviceconfig high-availability enabled yes
set deviceconfig high-availability interface ha1 port ethernet1/13
set deviceconfig high-availability interface ha1 ip-address 172.16.1.100
set deviceconfig high-availability interface ha1 netmask 255.255.255.0
set deviceconfig high-availability interface ha1 monitor-hold-time 3000
set deviceconfig high-availability interface ha2 port ethernet1/14
set deviceconfig high-availability interface ha3 port ethernet1/15

# Device 2

set deviceconfig high-availability group 3 mode active-active device-id 1
set deviceconfig high-availability group 3 mode active-active network-configuration sync virtual-
router no
set deviceconfig high-availability group 3 mode active-active network-configuration sync qos no
set deviceconfig high-availability group 3 mode active-active packet-forwarding yes
set deviceconfig high-availability group 3 peer-ip 172.16.1.100
set deviceconfig high-availability group 3 election-option device-priority 200
set deviceconfig high-availability group 3 election-option heartbeat-backup yes
set deviceconfig high-availability group 3 election-option preemptive no
set deviceconfig high-availability group 3 election-option promotion-hold-time 2000
set deviceconfig high-availability group 3 election-option hello-interval 8000
set deviceconfig high-availability group 3 election-option heartbeat-interval 1000
set deviceconfig high-availability group 3 election-option flap-max 3
set deviceconfig high-availability group 3 election-option preemption-hold-time 1

```

```

set deviceconfig high-availability group 3 election-option monitor-fail-hold-up-time 0
set deviceconfig high-availability group 3 election-option additional-master-hold-up-time 500
set deviceconfig high-availability group 3 state-synchronization enabled yes
set deviceconfig high-availability group 3 state-synchronization transport ethernet
set deviceconfig high-availability group 3 configuration-synchronization enabled yes
set deviceconfig high-availability group 3 monitoring path-monitoring enabled no
set deviceconfig high-availability group 3 monitoring link-monitoring enabled no
set deviceconfig high-availability enabled yes
set deviceconfig high-availability interface ha1 port ethernet1/13
set deviceconfig high-availability interface ha1 ip-address 172.16.1.101
set deviceconfig high-availability interface ha1 netmask 255.255.255.0
set deviceconfig high-availability interface ha1 monitor-hold-time 3000
set deviceconfig high-availability interface ha2 port ethernet1/14
set deviceconfig high-availability interface ha3 port ethernet1/15

```

Juniper EX configuration (EX 4200 series)

```

# Virtual Chassis of 2 members connected to a 1 member switch

# Virtual Chassis switches
### Make LAG interfaces ###
set chassis aggregated-devices ethernet device-count 2

### add members to LAG (ae0) ###
set interfaces ge-0/0/0 ether-options 802.3ad ae0
set interfaces ge-1/0/0 ether-options 802.3ad ae0

### Make LACP active on LAG interface ###
set interfaces ae0 aggregated-ether-options lacp active

### Add vlans on LAG interface ###
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members all

### Make vlans ###
set vlans vlan-100 vlan-id 100
set vlans vlan-200 vlan-id 200

### Add member to vlan (test station) ###
set vlans vlan-100 interface ge-0/0/22.0

### delete unit 0 for the LAG interfaces ###
Delete interfaces ge-0/0/0 unit 0
Delete interfaces ge-1/0/0 unit 0

#member switch
### Make LAG interfaces ###
set chassis aggregated-devices ethernet device-count 2

### add members to LAG (ae0) ###
set interfaces ge-0/0/0 ether-options 802.3ad ae0
set interfaces ge-0/0/2 ether-options 802.3ad ae0

### Make LACP active on LAG interface ###
set interfaces ae0 aggregated-ether-options lacp active

### Add vlans on LAG interface ###
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members all

```

```
### Make vlans ###
set vlans vlan-100 vlan-id 100
set vlans vlan-200 vlan-id 200

### Add member to vlan (test station) ###
set vlans vlan-100 interface ge-0/0/22.0

### delete unit 0 for the LAG interfaces ###
delete interfaces ge-0/0/0 unit 0
delete interfaces ge-2/0/0 unit 0
```

2.5 Example Scenario: Virtual Wire with Bypass Switch (“fail-open” scenario)

A single Palo Alto Networks firewall in a failure state will fail closed. In certain scenarios, failing closed may not be desirable:

- When two devices (HA pair) are not in the budget
- When a PA firewall is replacing an IPS, and the ability to fail open is still desired

In these scenarios, a bypass switch can be used to detect the state of the PA device, and send traffic around a failed PA device, essentially causing a fail-open state.

Description of Solution

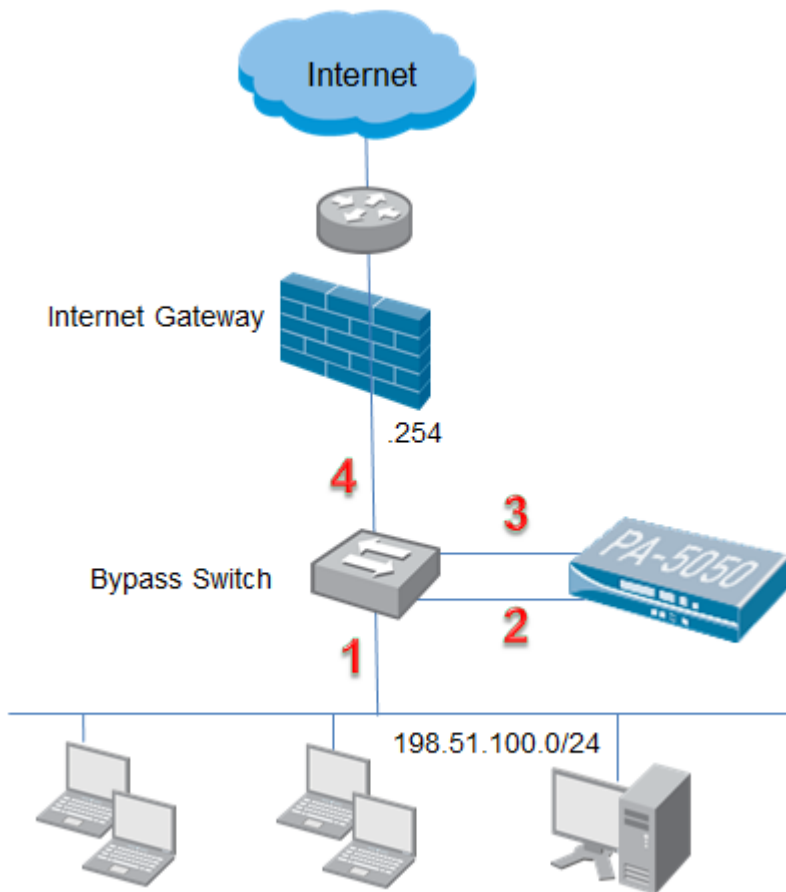
Bypass switches are hardware devices that allow for any transparent inline devices to be bypassed when a failure is experienced. This allows for network connectivity to remain constant but without the additional security services supplied by the security device. This solution requires that the firewall be deployed with an interface pair configured in vwire mode.

Vwire deployment mode is ideal for this solution because it is transparent and requires no routing decisions to be made within the firewall. Under normal operation the Palo Alto Networks firewall will impede traffic flow when a device failure is experienced in a non-HA deployment. But by augmenting the firewall with a bypass switch, network resiliency is maintained and communications will remain uninterrupted.

The purpose of the bypass switch is to transparently circumvent the Palo Alto Networks firewall should it experience a failure that causes communications between the two sides of the vwire to cease. Failures are constituted as health check (such as three missed consecutive pings), power and link state failures. The bypass switch can also be used to intentionally bypass a functional system during the troubleshooting or upgrade process to determine if the firewall is causing issues for flows during normal operation or to allow traffic to flow while the device is upgraded. The bypass switch utilized in this scenario is provided by NetOptics. The specific part number used for the test is BP-HBCU3. However bypass technology from other vendors should provide similar results.

Suggested Deployment

Here is how the PA device and bypass switch can be inserted in the network:



Normal Operation:

Traffic egressing the environment would take the following path in normal operation:

1. Traffic destined for the Internet would ingress the bypass switch.
2. The bypass switch would forward traffic to the Palo Alto Networks firewall's virtual-wire interface in the "internal" or "trust" zone.
3. Traffic that is allowed by the firewall would be forwarded out of the virtual-wire via the interface in the "external" or "untrust" zone back to the bypass switch.
4. The bypass switch would forward the traffic to the legacy firewall, which is the default route for the internal network.

Traffic ingressing the environment would take the inverse path (Steps 4, 3, 2, and 1 from above in this reverse order).

Bypass Operation:

Traffic egressing the environment would take the following path in a device failure condition:

1. Traffic destined for the Internet would ingress the bypass switch.
4. The bypass switch would detect the failure of the Palo Alto Networks firewall and would forward traffic to the legacy firewall directly.

Traffic ingressing the environment would take the inverse path (Steps 4 and 1 from above in this reverse order).

When the Palo Alto Networks firewall has recovered, traffic would return to the flow pattern associated with normal operation. However, special consideration needs to be taken when this type of recovery event occurs.

The Palo Alto Networks device maintains session state. Sessions seen by the appliance upon device initialization or service restoration that do not exist in the session table will be dropped by default. This may not be desired, especially if the goal is to not deny traffic if a device fails or recovers. The firewall does have the ability to be configured to ignore session state and allow traffic to flow even if the session initialization has not been seen. This setting can be leveraged to allow for traffic to always flow, however security profiles will not be applied to this traffic as session initialization was not seen and the appropriate protocol decoder cannot be invoked. The option can be enabled as a runtime parameter or in the device configuration itself. The latter is shown in the section Configuration Example (CLI). The screenshot below shows examples of non-syn-tcp traffic that can occur when the Palo Alto Networks firewall recovers from a failure and traffic that was in bypass then flows through the appliance.

Monitor tab -> Traffic Logs

To see any traffic that is being allowed by allowing non-syn-tcp traffic, set a filter of “app eq non-syn-tcp” in the traffic logs.



	Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
	07/11 15:16:28	end	trust	untrust	192.168.10.91	64.124.57.10	443	non-syn-tcp	allow	Allow All Outbound
	07/11 15:15:24	end	trust	untrust	192.168.10.91	64.124.57.10	443	non-syn-tcp	allow	Allow All Outbound
	07/11 15:14:20	end	trust	untrust	192.168.10.91	64.124.57.10	443	non-syn-tcp	allow	Allow All Outbound

GUI Configuration

The following screenshots are of a completed configuration.

Network tab-> Interfaces

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Virtual Wire			none	none	Untagged	default-vwire	untrust		
ethernet1/2	Virtual Wire			none	none	Untagged	default-vwire	trust		

Network tab-> Virtual Wires

	Name	Interface1	Interface2	Tag Allowed	Multicast Firewalling	Link State Pass Through
<input type="checkbox"/>	default-vwire	ethernet1/1	ethernet1/2	0-4094	<input type="checkbox"/>	<input checked="" type="checkbox"/>

You can use the factory default vwire configuration on port ethernet1/1 and ethernet1/2 or create a new vwire configuration with another port pair.

Note: be sure to set speed/duplex on all systems to match. For example, if the switched ports in the environment are set to 100/Full, the ports for the vwire interfaces as well as the bypass switch interfaces should be set to match. Not doing so will more than likely result in erratic or undesired behavior.

Network tab -> Zones

	Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	Enable User Identification	User ID Include List	User ID Exclude List
<input checked="" type="checkbox"/>	trust	virtual-wire	ethernet1/2			<input checked="" type="checkbox"/>		
<input type="checkbox"/>	untrust	virtual-wire	ethernet1/1			<input type="checkbox"/>		

The pre-defined virtual-wire zones of “trust” and “untrust” are being used in this example. If you plan to implement user-ID, check the box to “enable user-identification” on the “trust” zone.

Policies tab-> Security

		Source			Destination						
Name	Tag	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
Bypass Communications	none	trust	10.0.0.0/8	any	trust	10.0.0.0/8	icmp	application-default		none	
		untrust			untrust		ping				
Allow All Outbound	none	trust	any	any	untrust	any	any	any			
Allow All Inbound	none	untrust	any	any	trust	any	any	any			

The two rules at the bottom of this list allow traffic to flow in either direction on the vwire. The rule at the top of the list allows the bypass switch to evaluate the health of the system. This is typically accomplished by allowing ICMP and ping as the application to flow through the Palo Alto Networks device in both directions-- however this may vary and is dependent on the selected bypass switch used in the design⁵. Based upon the specific health check utilized by the selected bypass switch, you may be able to define the source and destination addresses and the applications used in rules to allow this communication in a more specific manor than the example above.

By default, the bypass switch will initiate communication from Monitor port 1 to Monitor port 2 once every second. A health check fails when three consecutive pings fail to reach Monitor port 2.

The traffic log will show log entries for the health check communications:

{ app eq ping }										
	Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
	07/11 15:01:36	end	untrust	trust	10.2.1.220	10.1.1.18	0	ping	allow	Bypass Communicat
	07/11 14:59:34	end	untrust	trust	10.2.1.220	10.1.1.18	0	ping	allow	Bypass Communicat

CLI Configuration

The CLI commands used to configure this scenario are shown below: ⁶

```
# The following configuration option ignores session state and allows a TCP session # to
pass through the system even if an entry does not exist in the session table.
```

```
set deviceconfig setting session tcp-reject-non-syn no
```

```
# Network Configuration
```

```
set network interface ethernet ethernet1/1 virtual-wire
set network interface ethernet ethernet1/1 link-speed auto
set network interface ethernet ethernet1/1 link-duplex auto
set network interface ethernet ethernet1/1 link-state auto
```

⁵ The BP-HBCU3 bypass switched used for this test scenario utilizes ping to determine the health of the inline system.

⁶ This output was obtained by running these three commands: “set cli config-output-format set” , “configure”, and “show”. Only commands relevant to this particular scenario are listed.


```

set network interface ethernet ethernet1/2 virtual-wire
set network interface ethernet ethernet1/2 link-speed auto
set network interface ethernet ethernet1/2 link-duplex auto
set network interface ethernet ethernet1/2 link-state auto

# Zone Configuration

set zone trust network virtual-wire ethernet1/2
set zone trust enable-user-identification yes
set zone untrust network virtual-wire ethernet1/1

# Vwire configuration

set network virtual-wire default-vwire interface1 ethernet1/1
set network virtual-wire default-vwire interface2 ethernet1/2
set network virtual-wire default-vwire tag-allowed 0-4094
set network virtual-wire default-vwire multicast-firewalling enable no
set network virtual-wire default-vwire link-state-pass-through enable yes

# Policy Configuration

set rulebase security rules "Bypass Communications" from [ trust untrust ]
set rulebase security rules "Bypass Communications" to [ trust untrust ]
set rulebase security rules "Bypass Communications" source 10.0.0.0/8
set rulebase security rules "Bypass Communications" destination 10.0.0.0/8
set rulebase security rules "Bypass Communications" service application-default
set rulebase security rules "Bypass Communications" application [ icmp ping ]
set rulebase security rules "Bypass Communications" action allow
set rulebase security rules "Bypass Communications" log-end yes
set rulebase security rules "Bypass Communications" option disable-server-response-inspection
no
set rulebase security rules "Bypass Communications" source-user any
set rulebase security rules "Bypass Communications" category any
set rulebase security rules "Bypass Communications" hip-profiles any
set rulebase security rules "Bypass Communications" log-start no
set rulebase security rules "Bypass Communications" negate-source no
set rulebase security rules "Bypass Communications" negate-destination no
set rulebase security rules "Allow All Outbound" from trust
set rulebase security rules "Allow All Outbound" to untrust
set rulebase security rules "Allow All Outbound" source any
set rulebase security rules "Allow All Outbound" destination any
set rulebase security rules "Allow All Outbound" service any
set rulebase security rules "Allow All Outbound" application any
set rulebase security rules "Allow All Outbound" action allow
set rulebase security rules "Allow All Outbound" log-end yes
set rulebase security rules "Allow All Outbound" profile-setting profiles url-filtering
default
set rulebase security rules "Allow All Outbound" profile-setting profiles virus default
set rulebase security rules "Allow All Outbound" profile-setting profiles spyware default
set rulebase security rules "Allow All Outbound" profile-setting profiles vulnerability
default
set rulebase security rules "Allow All Outbound" option disable-server-response-inspection no
set rulebase security rules "Allow All Outbound" source-user any
set rulebase security rules "Allow All Outbound" category any
set rulebase security rules "Allow All Outbound" hip-profiles any
set rulebase security rules "Allow All Outbound" log-start no
set rulebase security rules "Allow All Outbound" negate-source no
set rulebase security rules "Allow All Outbound" negate-destination no
set rulebase security rules "Allow All Inbound" from untrust
set rulebase security rules "Allow All Inbound" to trust
set rulebase security rules "Allow All Inbound" source any

```

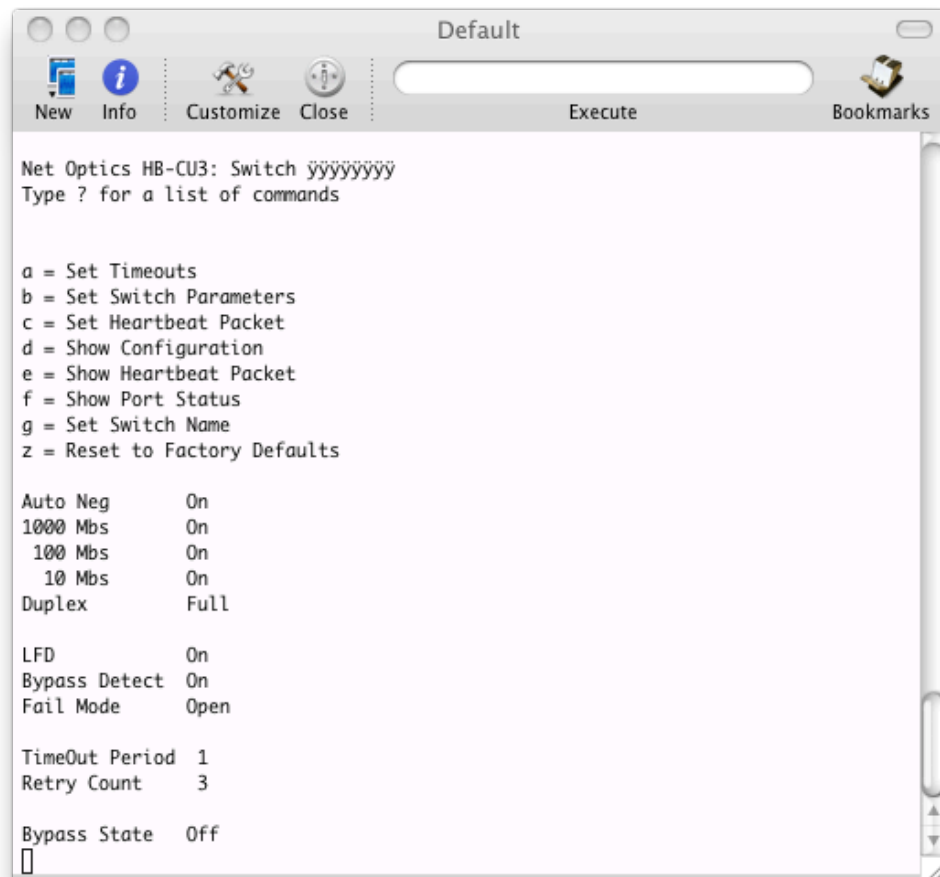
```

set rulebase security rules "Allow All Inbound" destination any
set rulebase security rules "Allow All Inbound" service any
set rulebase security rules "Allow All Inbound" application any
set rulebase security rules "Allow All Inbound" action allow
set rulebase security rules "Allow All Inbound" log-end yes
set rulebase security rules "Allow All Inbound" profile-setting profiles url-filtering default
set rulebase security rules "Allow All Inbound" profile-setting profiles virus default
set rulebase security rules "Allow All Inbound" profile-setting profiles spyware default
set rulebase security rules "Allow All Inbound" profile-setting profiles vulnerability default
set rulebase security rules "Allow All Inbound" option disable-server-response-inspection no
set rulebase security rules "Allow All Inbound" source-user any
set rulebase security rules "Allow All Inbound" category any
set rulebase security rules "Allow All Inbound" hip-profiles any
set rulebase security rules "Allow All Inbound" log-start no
set rulebase security rules "Allow All Inbound" negate-source no
set rulebase security rules "Allow All Inbound" negate-destination no

```

Bypass Switch Configuration

The NetOptics BP-HBCU3 used in this testing has very few configuration options. The default configuration was used for the test. The device was reset to factory defaults at the commencement of the test scenario. The device was configured to utilize IP packets as its default during the factory reset function.



There are very few options for the bypass switch utilized in this configuration. Typical options are LFD (Link Fault Detection) to find a failed interface, Bypass Detect to flap the IPS interfaces if possible to cause the IPS to trigger a monitoring alert, TimeOut Period to determine the time allocated for a health check to complete and the Retry Count to determine the number of consecutive failures that should occur before the device will go to bypass. The

Bypass State indicates the current state of the system. Off indicates that the inline device is functional. On indicates that the inline device is being circumvented.

2.6 Example Scenario: Horizontal Scaling with Load Balancers

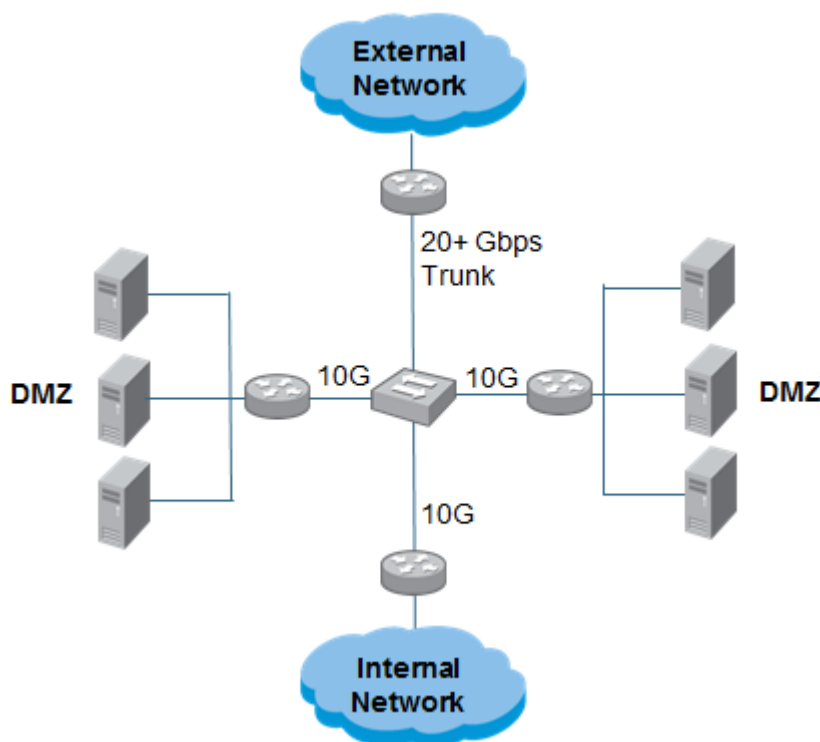
Overview of Challenge/Problem

In some cases network capacity requirements may exceed that of a single Palo Alto Networks device. In these cases there are a few options for sharing load across multiple devices in order to increase the scale of the solution.

Due to these issues and others, non-clustering solutions are desirable. The main objectives are maintenance of full state for each session, failure detection, and even load sharing. Maintaining full state requires that a single device process all packets for a given session. Failure detection requires that connectivity losses are identified and dynamically mitigated by offloading current and future sessions to the effected devices on to the other healthy devices. Equal load sharing requires an algorithm to distribute sessions to the devices such that all firewalls are loaded evenly.

Typical Topology

Below is a sample diagram of a network where security protection may be desired to provide protection between the external network and the internal networks as well as the DMZs.



Description of Solution

Using layer 3 stateful load balancers are a common and effective solution to horizontally scale firewall deployments. The load-balancing design allows traffic-flows to be split evenly over firewalls with different physical paths. Upstream and downstream load-balancers provide the ability to place multiple firewalls together creating a "cluster", where the traffic is split among the firewalls. The firewalls rely on the load-balancers to manage flows with whichever load-balancing algorithm is implemented. The benefit of this type of deployment is the ability to incrementally increase the bandwidth of the traffic that is being firewalled. If the cluster contains only two 10GB firewalls performing 20GB of inspection, another 20GB firewall can be added to the cluster to provide up to 40GB

of protection. Theoretically this can scale horizontally as long as the upstream and downstream load-balancing devices support the bandwidth of the connections and the firewalls follow suit.

This load-balancing model provides the capability to spread bandwidth between multiple firewalls. There are several algorithms available. The simplest algorithm is simple round-robin. Another relatively simple alternative is Equal Cost Load Balancing (ECLB), which works by hashing the source and destination IP addresses. The load balancers communicate with one another to ensure that sessions are “sticky” to a single firewall ensuring that state is maintained. The key is to ensure that return traffic associated with a session follows the same path as the initiating traffic.

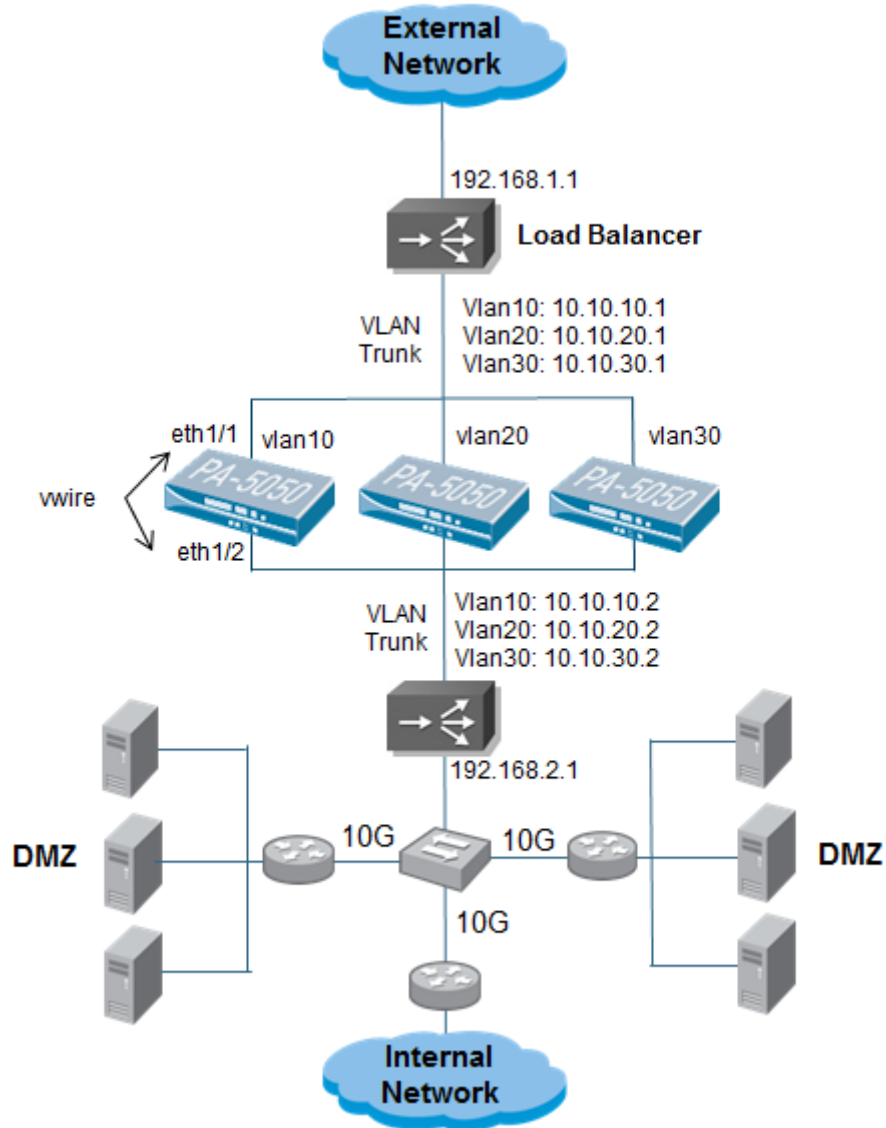
The load balancers also send keep-alives between themselves to ensure connectivity. If a firewall loses the ability to process traffic, the load-balancers will re-distribute the traffic over the remaining firewalls in the cluster. The failover time will vary depending on how the monitoring is configured on the load balancers. State is not synced between firewalls within the load-balanced cluster, so existing sessions will have to be re-established upon failure of a firewall.

An N+1 arrangement should be used for the FWs to ensure that sufficient capacity exists in the event of a FW failure. To protect against failure of a load balancer, they should be deployed in high availability.

A key benefit of this design provides the ability to upgrade or replace firewalls without taking significant network downtime. A FW can be removed from the pool so no new sessions are directed to it and after all existing sessions have ended, the FW can be upgraded without service impact.

Load Balancing Topology

In the example depicted below, each Palo Alto Networks firewall is configured with a single vwire. Firewall HA is not being used. The load balancer would distribute the load using a static round robin algorithm. For example, the first session would be forwarded on vlan 20, the second session would be forwarded on vlan 30, etc.



There are many variations of the topology, for example a single load balancer can be virtualized to serve as the inside and outside load balancers. In addition, a single switch can be utilized to provide all the connectivity.

GUI Configuration

The following screenshots are of a completed configuration.

Network tab -> Zones

	Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	Enable User Identification	User ID Include List	User ID Exclude List
<input type="checkbox"/>	trust	virtual-wire	ethernet1/2			<input checked="" type="checkbox"/>		
<input type="checkbox"/>	untrust	virtual-wire	ethernet1/1			<input type="checkbox"/>		

The pre-defined virtual-wire zones of “trust” and “untrust” are being used in this example. If you plan to implement user-ID, check the box to “enable user-identification” on the internal zone.

Network tab-> Interfaces

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Virtual Wire			none	none	Untagged	default-vwire	untrust		
ethernet1/2	Virtual Wire			none	none	Untagged	default-vwire	trust		

The factory-default configuration already has ethernet1/1 and ethernet1/2 in a virtual wire named “default-vwire”, with one interface in the “trust” zone and the other interface in the “untrust” zone. You can modify this sample configuration and use different vwire names or different zone names. Note for the vwire configuration that only two interfaces can be placed into the vwire definition - no more, no less. Additional vwires, using additional interfaces (and zones if needed) can be created to meet your specific design needs.

Network tab-> Virtual Wires

	Name	Interface1	Interface2	Tag Allowed	Multicast Firewalling	Link State Pass Through
<input type="checkbox"/>	default-vwire	ethernet1/1	ethernet1/2	0-4094	<input type="checkbox"/>	<input checked="" type="checkbox"/>

You can use the factory default vwire configuration on port ethernet1/1 and ethernet1/2 or create a new vwire configuration with another port pair.

Policies tab-> Security

Name	Tag	Source			Destination		Application	Service	Action	Profile	Options
		Zone	Address	User	Zone	Address					
rule1	none	trust	any	any	untrust	any	any	any			
rule2	none	untrust	any	any	trust	any	any	any			

Configure a security policy that allows traffic to flow between the vwire zones. Assign security profiles to inspect for viruses, spyware, vulnerabilities, files, data, and URLs as appropriate. In our sample security policy, “rule1” allows traffic to be initiated from the “trust” zone to the “untrust” zone and “rule2” allows traffic to be initiated from the “untrust” zone to the “trust” zone. After you have traffic flowing through the firewall using the wide-open policies above, you should modify your policies to limit the traffic flows through the firewall to those that are needed for the environment.

CLI Configuration

The CLI commands used to configure this scenario are shown below: ⁷

```
# Vwire called default-vwire on ports 1 and 2
# Network Configuration

set network interface ethernet ethernet1/1 virtual-wire
set network interface ethernet ethernet1/1 link-speed auto
set network interface ethernet ethernet1/1 link-duplex auto
set network interface ethernet ethernet1/1 link-state auto
set network interface ethernet ethernet1/2 virtual-wire
set network interface ethernet ethernet1/2 link-speed auto
set network interface ethernet ethernet1/2 link-duplex auto
set network interface ethernet ethernet1/2 link-state auto

# Zone Configuration

set zone trust network virtual-wire ethernet1/2
set zone trust enable-user-identification yes
set zone untrust network virtual-wire ethernet1/1

# Vwire configuration

set network virtual-wire default-vwire interface1 ethernet1/1
set network virtual-wire default-vwire interface2 ethernet1/2
set network virtual-wire default-vwire tag-allowed 0-4094
set network virtual-wire default-vwire multicast-firewalling enable no
set network virtual-wire default-vwire link-state-pass-through enable yes

# Policy configuration

set rulebase security rules rule1 from trust
set rulebase security rules rule1 to untrust
set rulebase security rules rule1 source any
set rulebase security rules rule1 destination any
set rulebase security rules rule1 service any
set rulebase security rules rule1 application any
set rulebase security rules rule1 action allow
set rulebase security rules rule1 log-end yes
set rulebase security rules rule1 profile-setting profiles url-filtering default
set rulebase security rules rule1 profile-setting profiles virus default
set rulebase security rules rule1 profile-setting profiles spyware default
set rulebase security rules rule1 profile-setting profiles vulnerability default
set rulebase security rules rule2 profile-setting profiles url-filtering default
set rulebase security rules rule2 profile-setting profiles virus default
set rulebase security rules rule2 profile-setting profiles spyware default
set rulebase security rules rule2 profile-setting profiles vulnerability default
set rulebase security rules rule2 option disable-server-response-inspection no
set rulebase security rules rule2 from untrust
set rulebase security rules rule2 to trust
set rulebase security rules rule2 source any
set rulebase security rules rule2 destination any
set rulebase security rules rule2 source-user any
set rulebase security rules rule2 application any
set rulebase security rules rule2 service any
set rulebase security rules rule2 hip-profiles any
```

⁷ This output was obtained by running these three commands: “set cli config-output-format set”, “configure”, and “show”. Only commands relevant to this particular scenario are listed.


```

set rulebase security rules rule2 log-start no
set rulebase security rules rule2 log-end yes
set rulebase security rules rule2 negate-source no
set rulebase security rules rule2 negate-destination no
set rulebase security rules rule2 action allow

```

F5 Config for this scenario:

Outside:

```

}
node 10.10.10.2 {}
node 10.10.20.2 {}
node 10.10.30.2 {}
node 192.168.1.2 {}
pool_Untrust_to_Trust {
    unit 1
    monitor all gateway_icmp
    members {
        10.10.10.2:any {}
        10.10.20.2:any {}
        10.10.20.2:any {}
    }
}
pool pool_Trust_to_Untrust {
    unit 1
    monitor all gateway_icmp
    #Gateway ICMP checks nodes in a pool that implements gateway failsafe for high
    #availability
    members 192.168.1.2:any {}
}
virtual vs_Untrust_to_Trust {
    pool pool_Untrust_to_Trust
    destination any:any
    mask 0.0.0.0
    profiles fastL4 {}
    #fastL4 profile used when no processing above L4 is required. Results in traffic being
    #processed in the PVA (the Packet Velocity Accelerator ASIC on LTM) which can increase
    #performance
}
virtual vs_Trust_to_Untrust {
    pool pool_Trust_to_Untrust
    destination any:any
    mask 0.0.0.0
    profiles fastL4 {}
    vlans {
        VLAN10
        VLAN20
        VLAN30
    } enable
}
}

```

Inside:

```

}
node 10.10.10.1 {}
node 10.10.20.1 {}
node 10.10.30.1 {}
node 192.168.2.2 {}
pool pool_Trust_to_Untrust {
    unit 1
    monitor all gateway_icmp
}

```

```

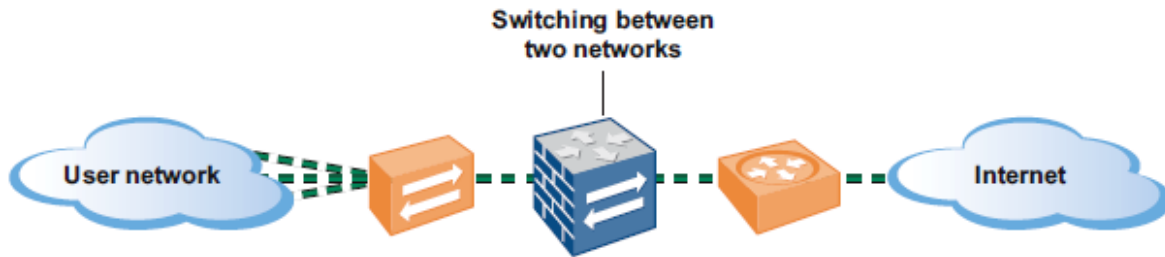
    members {
        10.10.10.4:any {}
        10.10.20.1:any {}
        10.10.30.1:any {}
    }
}
pool pool_Untrust_to_Trust {
    unit 1
    monitor all gateway_icmp
    #Gateway ICMP checks nodes in a pool that implements gateway failsafe for high
    #availability
    members 192.168.2.2:any {}
}
virtual vs_Trust_to_Untrust {
    pool pool_Trust_to_Untrust
    destination any:any
    mask 0.0.0.0
    profiles fastL4 {}
    #fastL4 profile used when no processing above L4 is required. Results in traffic being
    #processed in the PVA (the Packet Velocity Accelerator ASIC on LTM) which can increase
    #performance
}
virtual vs_Untrust_to_Trust {
    pool pool_Untrust_to_Trust
    destination any:any
    mask 0.0.0.0
    profiles fastL4 {}
    vlans {
        VLAN10
        VLAN20
        VLAN30
    } enable
}

```

Section 3: Layer2 Deployment Scenarios

3.1 Operation of L2 Interfaces

In a Layer2 deployment, the firewall provides MAC layer switching between two or more logical networks. The network provides L2 connectivity between networks where firewall segmentation is desired without changing the L3 topology. Each group of interfaces must be assigned to a VLAN, and additional Layer 2 subinterfaces can be defined as needed. Choose this option when switching is required.



Advantages:

- o Visibility into network traffic
- o Device can take action on the traffic, such as block or perform QoS

Disadvantages:

- o The device does not participate in spanning tree

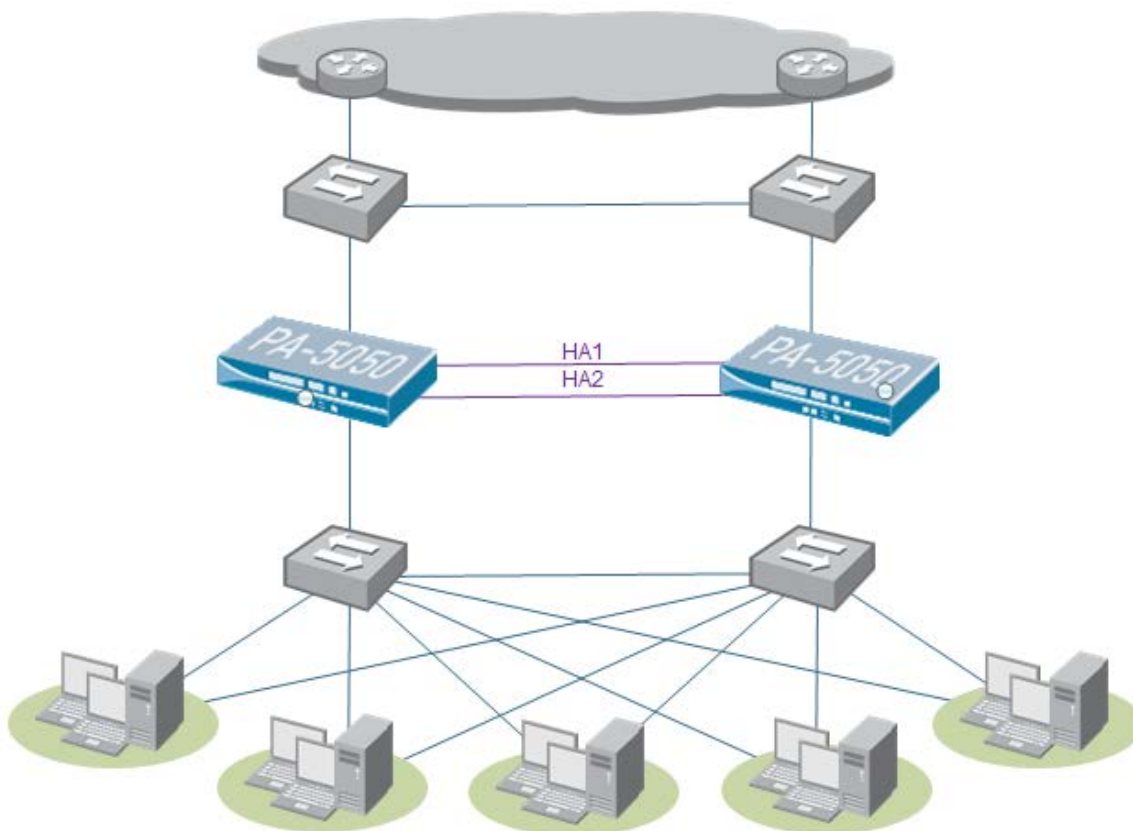
3.2 Example Scenario: Layer 2 Active/Passive HA

This suggested deployment below provides the design objective of firewall segmentation while maintaining the existing Layer3 topology. This solution may be used to segment internal logical domains as well as provide L2 connectivity for Internet services while providing the complete feature set of Palo Alto firewalls between these L2 segments. It is assumed both firewalls are within close physical proximity and the HA1 and HA2 links are direct crossover cables.

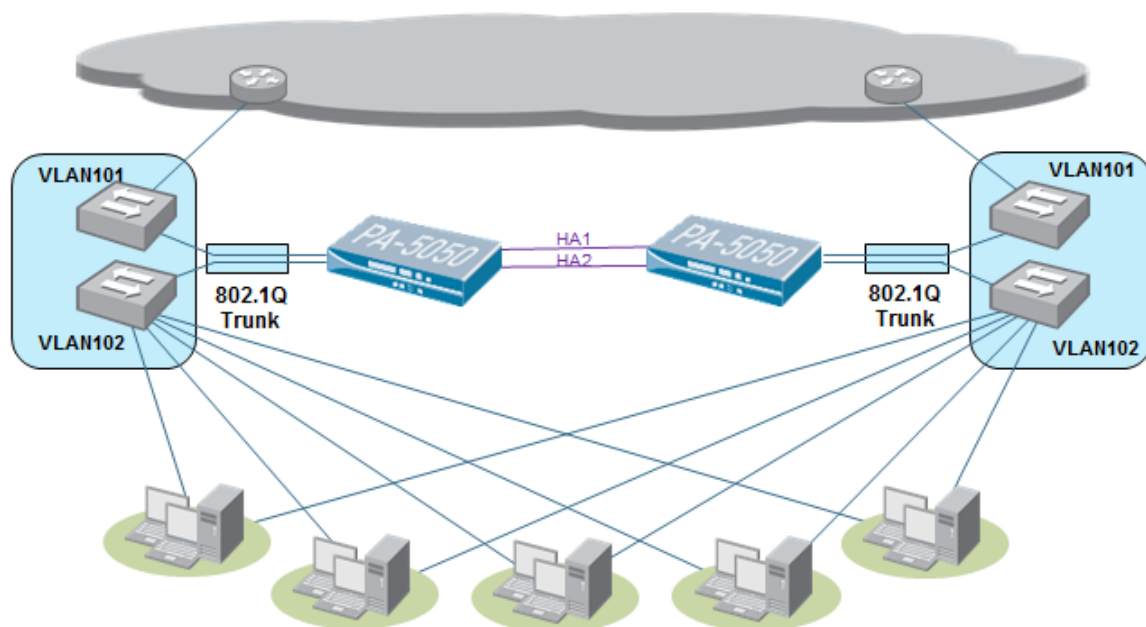
There are two options for network interface connectivity within L2 deployments:

- a) Simple L2 interfaces (non-trunked)
- b) VLAN Rewrite (trunked)

Here is an example of simple L2 firewall segmentation:



Here is an example of VLAN rewrite firewall segmentation using trunked interfaces:



Networking Considerations: Loop Prevention

An important component of L2 high availability design is multiple network paths. As the MAC layer packet provides no mechanism for loop detection the L2 network must ensure there is a single L2 path. Spanning Tree (802.1d) provides this loop detection role and should be employed within the adjacent L2 networks. The Active-Passive high availability solution provides a single L2 path across the Active firewall only, the Passive firewall interfaces are placed in a down state, so does not necessitate loop prevention across the firewall paths.

Networking Considerations: MAC Address Aging

L2 network switches maintain a table of MAC addresses and egress interfaces used to reach these MAC addresses; packets destined for an unknown MAC address must be flooded out all interfaces. To minimize flooding of packets to unknown MACs and provide for discovery of network topology changes L2 switches use a MAC Address Aging process: once a MAC address is learned the egress interface is placed in the forwarding table and an aging timer is set to the max aging time which is typically on the order of 5 minutes. Any changes in MAC address reachability will not be reflected in MAC forwarding tables until its entry ages out, traffic is once again flooded to the MAC address, and the destination interface discovered. To minimize network re-convergence after an HA state change, MAC Address Aging timers within the adjacent L2 network switches should be set to a value on the order of loop detection timers.

Networking Considerations: Spanning Tree

Note that PA firewalls do not participate in Spanning Tree Protocol, SPT BPDUs are passed through the HA cluster with no processing. Some network devices include L2 VLAN ID information to detect inadvertent inter-VLAN connectivity, these VLAN tagged BPDUs will cause an error condition on the adjacent L2 switches placing these ports in Blocking state. To prevent port blocking in such a scenario BPDUs with VLAN tagging must be

prevented from crossing L2 VLAN boundaries by disabling Spanning Tree Protocol BPDUs from being sent on these ports.

GUI Configuration

The below example configurations use e1/1 and e1/2 for a simple L2 scenario and ethernet1/3 for VLAN rewrite scenario using VLAN101 and VLAN102 for network connectivity.

1. Create zones as shown here:

Network tab -> Zones (simple L2 scenario)

Name	Type	Interfaces / Virtual Systems	Protection Profile	Log Setting	Enable User Identification	User Id Include List	User Id Exclude List
L2_Trust	layer2						
L2_Untrust	layer2						

Network tab -> Zones (VLAN rewrite scenario)

Name	Type	Interfaces / Virtual Systems	Protection Profile	Log Setting	Enable User Identification	User Id Include List	User Id Exclude List
L2-VLAN-Trust	layer2						
L2-VLAN-Untrust	layer2						

2. Create VLANs as shown here:

Network tab -> VLANs (simple L2 scenario)



Name	Interfaces	VLAN Interface	L3 Forwarding
VLAN			

Network tab -> VLANs (VLAN rewrite scenario)

Name	Interfaces	VLAN Interface	L3 Forwarding
VLAN-Rewrite			

3. Configure/create interfaces as shown here:

Network tab -> Interfaces (simple L2 scenario)

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
ethernet1/1	L2					Untagged	VLAN	L2_Untrust
ethernet1/2	L2					Untagged	VLAN	L2_Trust

Network tab -> Interfaces (VLAN rewrite scenario)

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
ethernet1/3	L2					Untagged	none	none
ethernet1/3.101	L2					101	VLAN-Rewrite	L2-VLAN-Untrust
ethernet1/3.102	L2					102	VLAN-Rewrite	L2-VLAN-Trust

In this scenario, you are creating new L2 interfaces (subinterfaces) associated with trunked link. Also assign VLAN tags, VLAN, and zone.

- Configure policies to allow the traffic to flow between the appropriate trusted and untrusted zones. The example below is using the zones in the Simple L2 scenario, change the zone names for the VLAN Rewrite scenario.

Policies tab -> Security

	Source			Destination					
Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile
rule1	L2_Trust	any	any	L2_Untrust	any	any	any		
rule2	L2_Untrust	any	any	L2_Trust	any	any	any		

- Configure High Availability as shown here:

Device tab -> High Availability (Device 1)

Setup [Edit...](#)

HA Enabled ☒

Group ID 1

Description

Mode active-passive

Peer HA IP Address 192.168.1.2

Peer HA IP Backup Address

Config Sync ☒

Control Link [Edit...](#)

Primary Backup

Port dedicated-ha1

IP Address 192.168.1.1

Netmask 255.255.255.0

Gateway

Link Speed (Mbps) auto

Link Duplex auto

Encryption Enabled ☒

Monitor Hold Time (ms) 3000

Active Passive Configuration [Edit...](#)

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

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

Data Link [Edit...](#)

Primary Backup

Port dedicated-ha2

IP Address 2.2.2.1

Netmask 255.255.255.0

Gateway

Link Speed (Mbps) auto

Link Duplex auto

State Synchronization Enabled ☒

Transport ethernet

Device tab -> High Availability (Device 2)

Setup	Election Settings
HA Enabled <input checked="" type="checkbox"/>	Device Priority 200
Group ID 1	Heartbeat Backup <input checked="" type="checkbox"/>
Description	Preemptive <input checked="" type="checkbox"/>
Mode active-passive	Preemption Hold Time (min) 1
Peer HA IP Address 192.168.1.1	Promotion Hold Time (ms) 2000
Peer HA IP Backup Address	Hello Interval (ms) 1000
Config Sync <input checked="" type="checkbox"/>	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	Data Link
Primary Backup	Primary Backup
Port dedicated-ha1	Port dedicated-ha2
IP Address 192.168.1.2	IP Address 2.2.2.2
Netmask 255.255.255.0	Netmask 255.255.255.0
Gateway	Gateway
Link Speed (Mbps) auto	Link Speed (Mbps) auto
Link Duplex auto	Link Duplex auto
Encryption Enabled <input checked="" type="checkbox"/>	State Synchronization Enabled <input checked="" type="checkbox"/>
Monitor Hold Time (ms) 3000	Transport ethernet

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

Note that in HA Setup, Group ID must be unique for multiple L2 HA pairs within the same L2 network domain.

For link monitoring, configure the following on each device:

Simple L2 scenario – Failure of any L2 link

Link Monitoring			
Enabled <input checked="" type="checkbox"/>			
Failure Condition any			
Link Groups			
Name	Enabled	Failure Condition	Interfaces
L2 links	<input checked="" type="checkbox"/>	any	ethernet1/1, ethernet1/2

VLAN Rewrite scenario – Failure of trunked link

Link Monitoring			
Enabled <input checked="" type="checkbox"/>			
Failure Condition any			
Link Groups			
Name	Enabled	Failure Condition	Interfaces
L2 trunk links	<input checked="" type="checkbox"/>	any	ethernet1/3

CLI Configuration

The CLI commands used to configure this scenario are shown below: ⁸

```
# Interface configuration (Simple L2 scenario)
set network interface ethernet ethernet1/1 link-state auto
set network interface ethernet ethernet1/1 link-duplex auto
set network interface ethernet ethernet1/1 link-speed auto
set network interface ethernet ethernet1/2 link-state auto
set network interface ethernet ethernet1/2 link-duplex auto
set network interface ethernet ethernet1/2 link-speed auto

# Interface configuration (VLAN rewrite scenario)
set network interface ethernet ethernet1/3 link-state auto
set network interface ethernet ethernet1/3 link-duplex auto
set network interface ethernet ethernet1/3 link-speed auto
set network interface ethernet ethernet1/3 layer2 units ethernet1/3.102 tag 102
set network interface ethernet ethernet1/3 layer2 units ethernet1/3.101 tag 101

# Interface mode
delete network virtual-wire default-vwire
delete zone trust
delete zone untrust
set network interface ethernet ethernet1/1 layer2
set network interface ethernet ethernet1/2 layer2
set network interface ethernet ethernet1/3 layer2

# Zone configuration (Simple L2 scenario)
set zone L2_Untrust network layer2 ethernet1/1
set zone L2_Untrust enable-user-identification no
set zone L2_Trust network layer2 ethernet1/2
set zone L2_Trust enable-user-identification no

# Zone configuration (VLAN rewrite scenario)
set zone L2-VLAN-Untrust network layer2 ethernet1/3.101
set zone L2-VLAN-Untrust enable-user-identification no
set zone L2-VLAN-Trust network layer2 ethernet1/3.102
set zone L2-VLAN-Trust enable-user-identification no

# VLAN configuration (Simple L2 scenario)
set network vlan VLAN interface ethernet1/1
set network vlan VLAN interface ethernet1/2

# VLAN configuration (VLAN rewrite scenario)
set network vlan VLAN-Rewrite interface ethernet1/3.101
set network vlan VLAN-Rewrite interface ethernet1/3.102

# Policy configuration
delete rulebase security rules rule1
delete rulebase security rules rule2
set rulebase security rules rule1 from L2_Untrust
set rulebase security rules rule1 to L2_Trust
set rulebase security rules rule1 source any
set rulebase security rules rule1 destination any
set rulebase security rules rule1 service any
set rulebase security rules rule1 application any
```

⁸ This output was obtained by running these three commands: “set cli config-output-format set”, “configure”, and “show”. Only commands relevant to this particular scenario are listed.

```

set rulebase security rules rule1 action allow
set rulebase security rules rule1 log-end yes
set rulebase security rules rule1 profile-setting profiles url-filtering default
set rulebase security rules rule1 profile-setting profiles virus default
set rulebase security rules rule1 profile-setting profiles spyware default
set rulebase security rules rule1 profile-setting profiles vulnerability default
set rulebase security rules rule2 from L2_Trust
set rulebase security rules rule2 to L2_Untrust
set rulebase security rules rule2 source any
set rulebase security rules rule2 destination any
set rulebase security rules rule2 service any
set rulebase security rules rule2 application any
set rulebase security rules rule2 action allow
set rulebase security rules rule2 log-end yes
set rulebase security rules rule2 profile-setting profiles url-filtering default
set rulebase security rules rule2 profile-setting profiles virus default
set rulebase security rules rule2 profile-setting profiles spyware default
set rulebase security rules rule2 profile-setting profiles vulnerability default

```

High Availability Configuration (Device #1):

```

set deviceconfig high-availability enabled yes
set deviceconfig high-availability interface ha1 port dedicated-ha1
set deviceconfig high-availability interface ha1 link-speed auto
set deviceconfig high-availability interface ha1 link-duplex auto
set deviceconfig high-availability interface ha1 ip-address 192.168.1.1
set deviceconfig high-availability interface ha1 netmask 255.255.255.0
set deviceconfig high-availability interface ha1 monitor-hold-time 3000
set deviceconfig high-availability interface ha2 port dedicated-ha2
set deviceconfig high-availability interface ha2 link-speed auto
set deviceconfig high-availability interface ha2 link-duplex auto
set deviceconfig high-availability interface ha2 ip-address 2.2.2.1
set deviceconfig high-availability interface ha2 netmask 255.255.255.0
set deviceconfig high-availability group 1 peer-ip 192.168.1.2
set deviceconfig high-availability group 1 election-option device-priority 100
set deviceconfig high-availability group 1 election-option heartbeat-backup no
set deviceconfig high-availability group 1 election-option preemptive yes
set deviceconfig high-availability group 1 election-option promotion-hold-time 2000
set deviceconfig high-availability group 1 election-option hello-interval 1000
set deviceconfig high-availability group 1 election-option heartbeat-interval 1000
set deviceconfig high-availability group 1 election-option flap-max 3
set deviceconfig high-availability group 1 election-option preemption-hold-time 1
set deviceconfig high-availability group 1 election-option monitor-fail-hold-up-time 0
set deviceconfig high-availability group 1 election-option additional-master-hold-up-time 500
set deviceconfig high-availability group 1 state-synchronization enabled yes
set deviceconfig high-availability group 1 state-synchronization transport ethernet
set deviceconfig high-availability group 1 configuration-synchronization enabled yes
set deviceconfig high-availability group 1 monitoring path-monitoring enabled no
set deviceconfig high-availability group 1 monitoring link-monitoring enabled yes
set deviceconfig high-availability group 1 monitoring link-monitoring failure-condition any

```

High Availability Configuration (Device #2):

```

set deviceconfig high-availability enabled yes
set deviceconfig high-availability interface ha1 port dedicated-ha1
set deviceconfig high-availability interface ha1 link-speed auto
set deviceconfig high-availability interface ha1 link-duplex auto
set deviceconfig high-availability interface ha1 ip-address 192.168.1.2
set deviceconfig high-availability interface ha1 netmask 255.255.255.0
set deviceconfig high-availability interface ha1 monitor-hold-time 3000
set deviceconfig high-availability interface ha2 port dedicated-ha2

```

```

set deviceconfig high-availability interface ha2 link-speed auto
set deviceconfig high-availability interface ha2 link-duplex auto
set deviceconfig high-availability interface ha2 ip-address 2.2.2.2
set deviceconfig high-availability interface ha2 netmask 255.255.255.0
set deviceconfig high-availability group 1 peer-ip 192.168.1.1
set deviceconfig high-availability group 1 election-option device-priority 200
set deviceconfig high-availability group 1 election-option heartbeat-backup no
set deviceconfig high-availability group 1 election-option preemptive yes
set deviceconfig high-availability group 1 election-option promotion-hold-time 2000
set deviceconfig high-availability group 1 election-option hello-interval 1000
set deviceconfig high-availability group 1 election-option heartbeat-interval 1000
set deviceconfig high-availability group 1 election-option flap-max 3
set deviceconfig high-availability group 1 election-option preemption-hold-time 1
set deviceconfig high-availability group 1 election-option monitor-fail-hold-up-time 0
set deviceconfig high-availability group 1 election-option additional-master-hold-up-time 500
set deviceconfig high-availability group 1 state-synchronization enabled yes
set deviceconfig high-availability group 1 state-synchronization transport ethernet
set deviceconfig high-availability group 1 configuration-synchronization enabled yes
set deviceconfig high-availability group 1 monitoring path-monitoring enabled no
set deviceconfig high-availability group 1 monitoring link-monitoring enabled yes
set deviceconfig high-availability group 1 monitoring link-monitoring failure-condition any

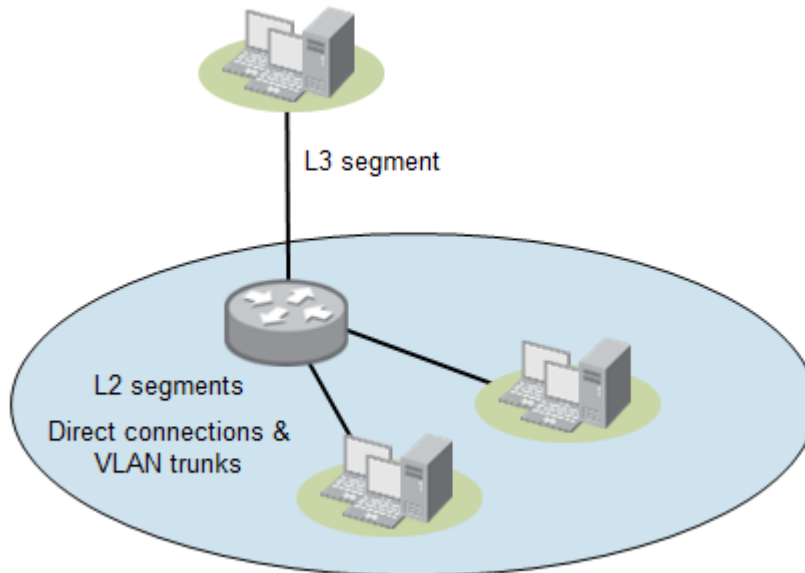
# HA link monitoring config (Simple L2 scenario)
set deviceconfig high-availability group 1 monitoring link-monitoring failure-condition any
set deviceconfig high-availability group 1 monitoring link-monitoring link-group "L2 links" enabled
yes
set deviceconfig high-availability group 1 monitoring link-monitoring link-group "L2 links" failure-
condition any
set deviceconfig high-availability group 1 monitoring link-monitoring link-group "L2 links" interface
ethernet1/1
set deviceconfig high-availability group 1 monitoring link-monitoring link-group "L2 links" interface
ethernet1/2

# HA link monitoring config (VLAN rewrite scenario)
set deviceconfig high-availability group 1 monitoring link-monitoring link-group "L2 trunk links"
enabled yes
set deviceconfig high-availability group 1 monitoring link-monitoring link-group "L2 trunk links"
failure-condition any
set deviceconfig high-availability group 1 monitoring link-monitoring link-group "L2 trunk links"
interface ethernet1/3

```

3.3 Example Scenario: Combination Layer 2 and Layer 3 Topology

Below is a sample diagram of a network where security protection may be desired to provide protection between L2 broadcast domains (direct physical connections or VLAN trunking) and a L3 domain (routing between the broadcast segments). Several variations on this topology exist but the goal is to provide firewall security within a broadcast domain and between broadcast domains.

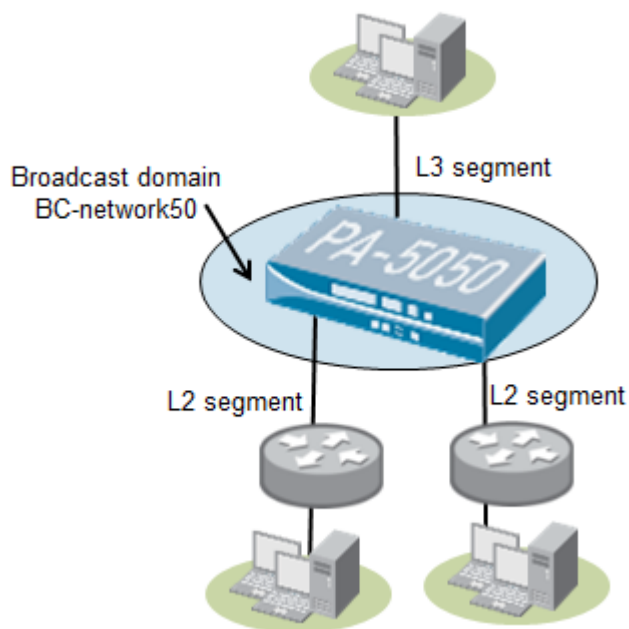


Description of Solution

Basic L2 configuration makes the Palo Alto Networks firewall act as one or more secure switches. Multiple physical ports (or 802.1Q subinterfaces) can be associated with the same broadcast domain using the VLAN object. Multiple L2 security zones can be configured for these VLANs. This allows the device to secure large flat networks without requiring a redesign. Servers can be in a separate security zone than users and the Internet even if they are all on the same subnet. A L3 subinterface can also be associated with a VLAN object (=broadcast domain) allowing route services to be delivered to exit the L2 broadcast domain.

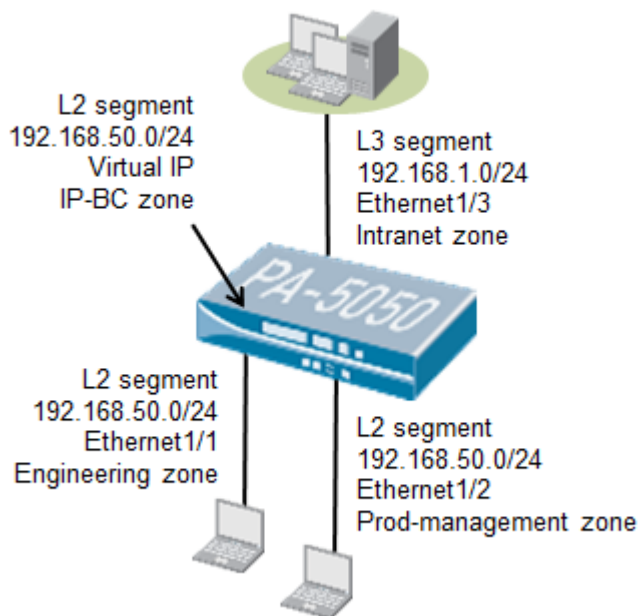
Note: This setup can also be used for VLAN rewriting where security policies (e.g. firewall, threats scanning, user identification, etc.) will be enforced between two 802.1Q VLAN's in the same broadcast domain.

Suggested Network Design



Configuration Example

This example scenario was tested using three directly connected devices. 2 devices were directly connected with each a dedicated L2 interface (ethernet1/1 and ethernet1/2). A third (logical) interface was added to the broadcast VLAN object allowing to route the L2 traffic from BC-network50 to another network. This third interface is represented by VLAN.100 which is assigned to the VLAN object.



GUI Configuration




1. Create the 4 security zones. The interfaces will be added to the zone when the interfaces are configured.

Name	Type	Interfaces / Virtual Systems	Protection Profile	Log Setting	Enable User Identification	User Id Include List	User Id Exclude List
engineering	layer2						
intranet	layer3						
IP-BC	layer3						
prod-management	layer2						

2. Create the VLAN object. Note that in this stage the L3 forwarding can't be configured yet as the VLAN interface doesn't exist yet. The VLAN object will need to be edited once the VLAN interface is configured. The Ethernet interfaces will also be added in a later stage.

Name	Interfaces	VLAN Interface	L3 Forwarding
BC-network50			

3. Assign the two Ethernet interfaces (ethernet1/1 and Ethernet1/2) to their respective zones and VLAN object. Note that the zone "intranet" represents an additional routed segment; ethernet1/3 will be assigned to that zone. Assign Ethernet1/3 to the 'default' virtual router instance. A management profile can also be created and assigned to ethernet1/3.

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
ethernet1/1	L2					Untagged	BC-network50	engineering
ethernet1/2	L2					Untagged	BC-network50	prod-management
ethernet1/3	L3	allow-all		196.168.1.111/24	default	Untagged		intranet

4. While still on the Interfaces screen, create a new VLAN interface with parameters as follows:
 - Name: vlan.100 (arbitrary number, doesn't refer to an 802.1q tag)
 - Management profile: allow all
 - IP address: 192.168.50.1/24 (an IP within the range of the L2 broadcast segment)
 - Vlan object: BC-network50
 - Virtual router: default
 - Zone: IP-BC

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone
vlan.100	VLAN	allow-all		192.168.50.1/24	default	Untagged	BC-network50	IP-BC

5. The 'default' virtual router instance will now have two interfaces assigned.

Name	Interfaces	RIP	OSPF	BGP
default	ethernet1/3 vlan.100			




6. Add the default route (or specific routing protocols) to the virtual router by editing the instance.

Static Routes						
IPv4		IPv6				
Name	Destination	Interface	Next Hop Type	Next Hop Value	Admin Distance	Metric
default route	0.0.0.0/0	ethernet1/3	ip	192.168.1.1		


7. Edit the VLAN object BC-network50. Enable L3 forwarding to result in:

Name	Interfaces	VLAN Interface	L3 Forwarding
BC-network50	ethernet1/1 ethernet1/2	vlan.100	yes

8. Now that we have the networking in place security policies must be added to allow traffic to flow between the different security zones. Although ethernet1/1 and ethernet1/2 are in the same broadcast domain, security policies must be in place to communicate between the two interfaces (or systems on those segments).

Name	Source			Destination		Application	Service	Action
	Zone	Address	User	Zone	Address			
rule1	 engineering	any	any	 prod-management	any	any	any	✓
rule2	 prod-management	any	any	 engineering	any	any	any	✓
rule3	 IP-BC	any	any	 intranet	any	any	any	✓

9. Create a NAT policy to allow network 192.168.50.0 to be translated to the “public” IP of e1/3, such that the internal network can reach the external network.

Original Packet						Translated Packet	
Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
 IP-BC	 intranet	any	any	any	any	dynamic-ip-and-port ethernet1/3 192.168.1.111/24	none

CLI Configuration

The CLI commands used to configure this scenario are shown below: ⁹

```
# Interface management profile
set network profiles interface-management-profile allow-all https yes ping yes ssh yes

# Interface configuration
set network interface ethernet ethernet1/1 link-speed auto
set network interface ethernet ethernet1/1 link-duplex auto
set network interface ethernet ethernet1/1 link-state auto
set network interface ethernet ethernet1/2 link-speed auto
set network interface ethernet ethernet1/2 link-duplex auto
set network interface ethernet ethernet1/2 link-state auto
set network interface ethernet ethernet1/3 link-speed auto
set network interface ethernet ethernet1/3 link-duplex auto
set network interface ethernet ethernet1/3 link-state auto
set network interface ethernet ethernet1/3 layer3 mtu 1500
set network interface ethernet ethernet1/3 layer3 interface-management-profile allow-all
set network interface ethernet ethernet1/3 layer3 ip 192.168.1.111/24
set network interface ethernet ethernet1/3 layer3 ipv6 enabled no
set network interface ethernet ethernet1/3 layer3 ipv6 neighbor-discovery enable-dad no
set network interface vlan units vlan.100 mtu 1500
set network interface vlan units vlan.100 interface-management-profile allow-all
set network interface vlan units vlan.100 ip 192.168.50.1/24
set network interface vlan units vlan.100 ipv6 enabled no
set network interface vlan units vlan.100 ipv6 neighbor-discovery enable-dad no

# Zone configuration
set zone engineering network layer2 ethernet1/1
set zone engineering enable-user-identification no
set zone intranet network layer3 ethernet1/3
set zone intranet enable-user-identification no
set zone IP-BC network layer3 vlan.100
set zone IP-BC enable-user-identification no
set zone prod-management network layer2 ethernet1/2
set zone prod-management enable-user-identification no

# VLAN configuration
set network vlan BC-network50 interface ethernet1/1
set network vlan BC-network50 interface ethernet1/2
set network vlan BC-network50 virtual-interface interface vlan.100
set network vlan BC-network50 virtual-interface l3-forwarding yes

# Virtual Router configuration
set network virtual-router default interface ethernet1/3
set network virtual-router default interface vlan.100
set network virtual-router default routing-table ip static-route "default route" destination
0.0.0.0/0 interface ethernet1/3 nexthop ip-address 192.168.1.1

# Policy configuration

delete rulebase security rules rule1
delete rulebase security rules rule2
delete rulebase security rules rule3
set rulebase security rules rule1 option disable-server-response-inspection no
```

⁹ This output was obtained by running these three commands: “set cli config-output-format set”, “configure”, and “show”. Only commands relevant to this particular scenario are listed.

```

set rulebase security rules rule1 from engineering
set rulebase security rules rule1 to prod-management
set rulebase security rules rule1 source any
set rulebase security rules rule1 destination any
set rulebase security rules rule1 source-user any
set rulebase security rules rule1 application any
set rulebase security rules rule1 service any
set rulebase security rules rule1 hip-profiles any
set rulebase security rules rule1 log-start no
set rulebase security rules rule1 log-end yes
set rulebase security rules rule1 negate-source no
set rulebase security rules rule1 negate-destination no
set rulebase security rules rule1 action allow
set rulebase security rules rule2 option disable-server-response-inspection no
set rulebase security rules rule2 from prod-management
set rulebase security rules rule2 to engineering
set rulebase security rules rule2 source any
set rulebase security rules rule2 destination any
set rulebase security rules rule2 source-user any
set rulebase security rules rule2 application any
set rulebase security rules rule2 service any
set rulebase security rules rule2 hip-profiles any
set rulebase security rules rule2 log-start no
set rulebase security rules rule2 log-end yes
set rulebase security rules rule2 negate-source no
set rulebase security rules rule2 negate-destination no
set rulebase security rules rule2 action allow
set rulebase security rules rule3 option disable-server-response-inspection no
set rulebase security rules rule3 from IP-BC
set rulebase security rules rule3 to intranet
set rulebase security rules rule3 source any
set rulebase security rules rule3 destination any
set rulebase security rules rule3 source-user any
set rulebase security rules rule3 application any
set rulebase security rules rule3 service any
set rulebase security rules rule3 hip-profiles any
set rulebase security rules rule3 log-start no
set rulebase security rules rule3 log-end yes
set rulebase security rules rule3 negate-source no
set rulebase security rules rule3 negate-destination no
set rulebase security rules rule3 action allow

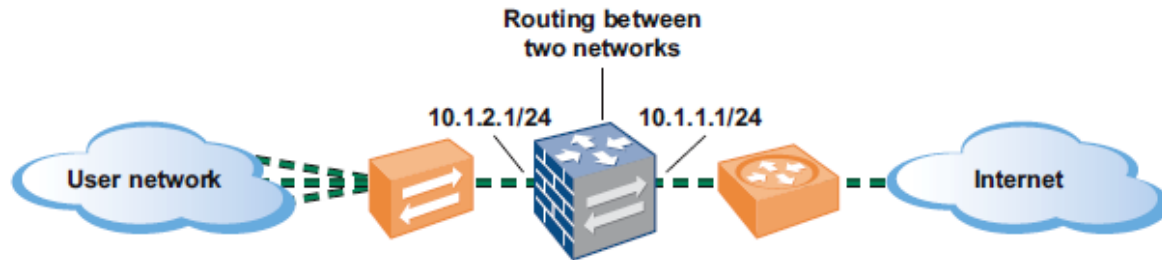
set rulebase nat rules Rule1 source-translation dynamic-ip-and-port interface-address interface
ethernet1/3 ip 192.168.1.111/24
set rulebase nat rules Rule1 to intranet
set rulebase nat rules Rule1 from IP-BC
set rulebase nat rules Rule1 source any
set rulebase nat rules Rule1 destination any
set rulebase nat rules Rule1 service any

```

Section 4: Layer3 Deployment Scenarios

4.1 Operation of L3 Interfaces

In a Layer 3 deployment, the firewall routes traffic between multiple interfaces. An IP address must be assigned to each interface and a virtual router must be defined to route the traffic. Choose this option when routing or NAT is required.



Advantages:

- o Full firewall functionality, such as traffic visibility, blocking traffic, rate limiting traffic, NAT, and routing, including support for common routing protocols

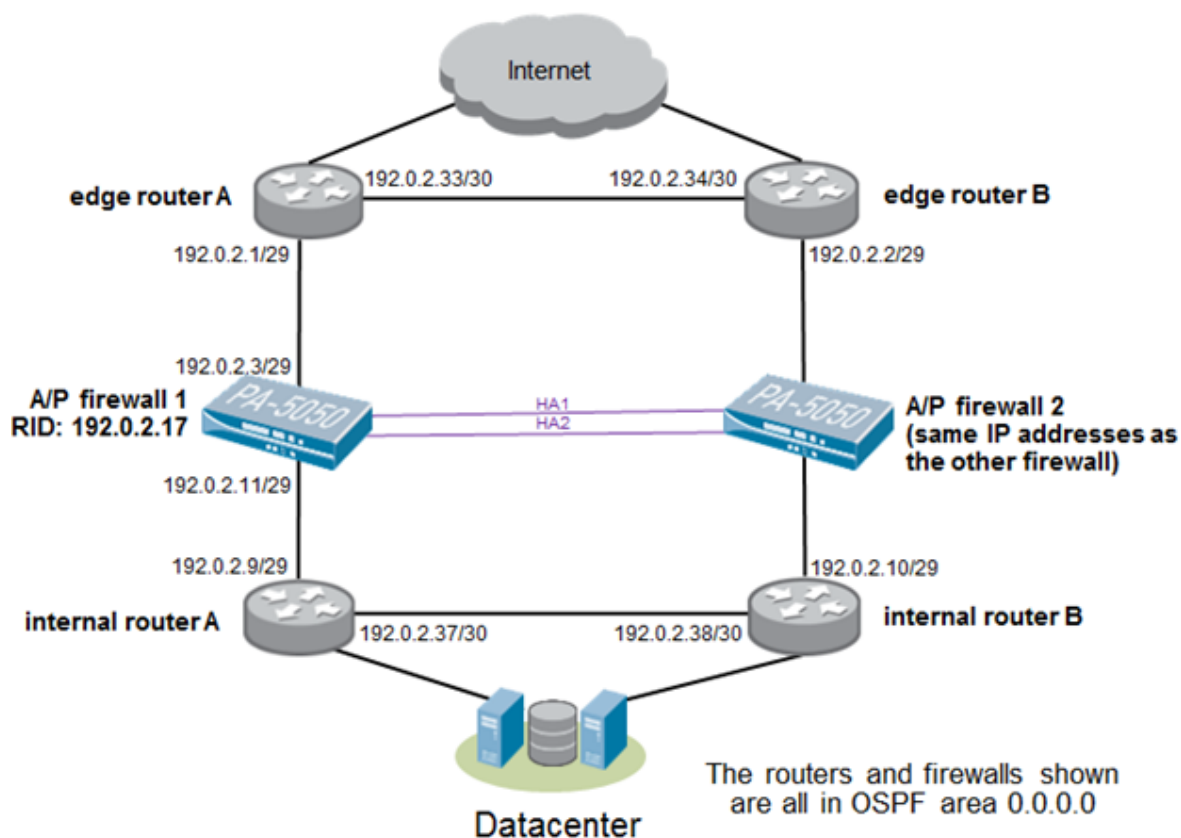
Disadvantages:

- o Inserting device into network will require IP configuration changes on adjacent devices

4.2 Example Scenario: Layer 3 Active/Passive HA with OSPF

The method for implementing OSPF on the Palo Alto Networks firewalls with Active/Passive HA is discussed in detail in the Palo Alto Networks Tech Note: <https://live.paloaltonetworks.com/docs/DOC-1939>.

Below is the network diagram that was implemented for this scenario:

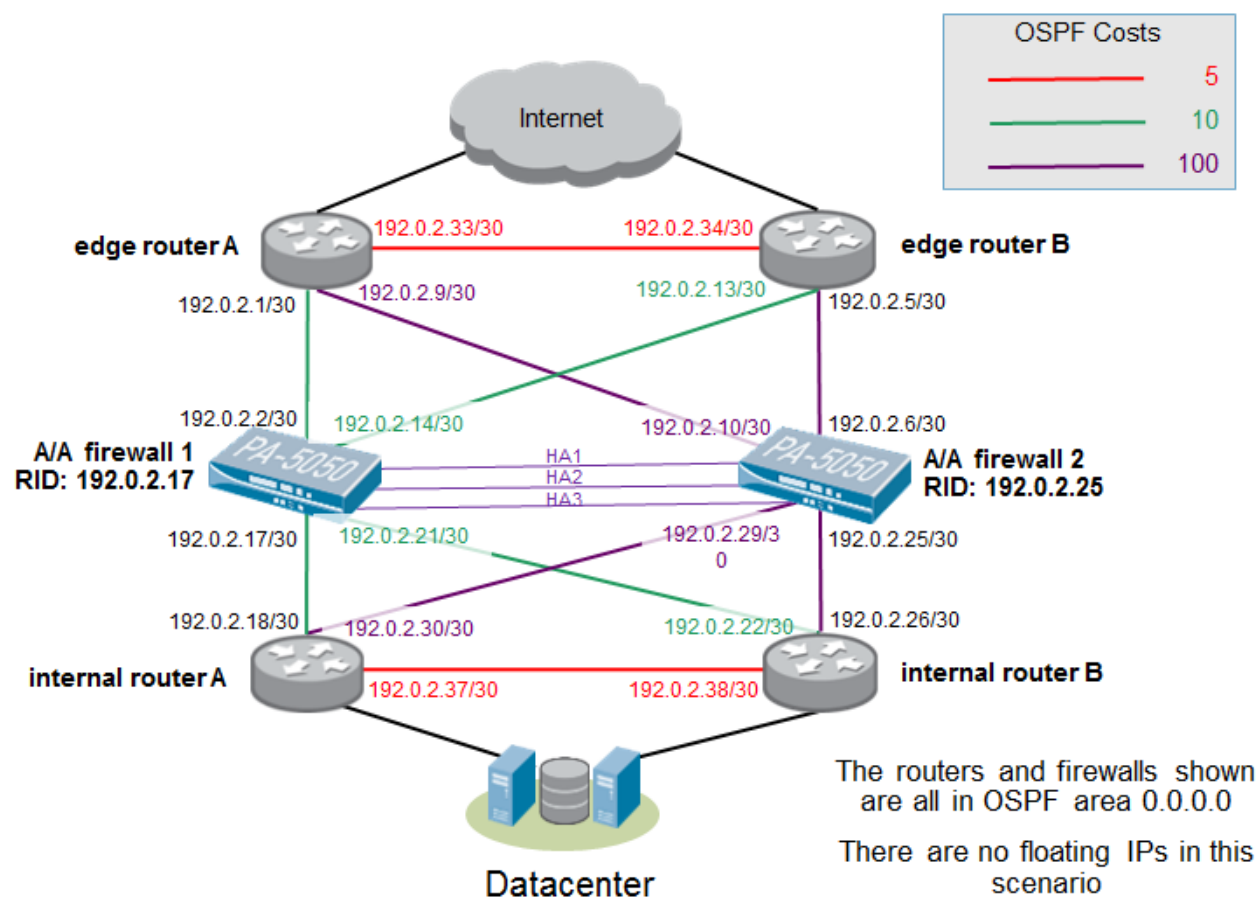


Please refer to that tech note for a discussion of this implementation, and GUI and CLI configuration.

4.3 Example Scenario: Layer 3 Active/Active HA with OSPF

The method for implementing OSPF on the Palo Alto Networks firewalls with Active/Active HA is discussed in detail in the Palo Alto Networks Tech Note: <https://live.paloaltonetworks.com/docs/DOC-1939>.

Below is the network diagram that was implemented for this scenario:

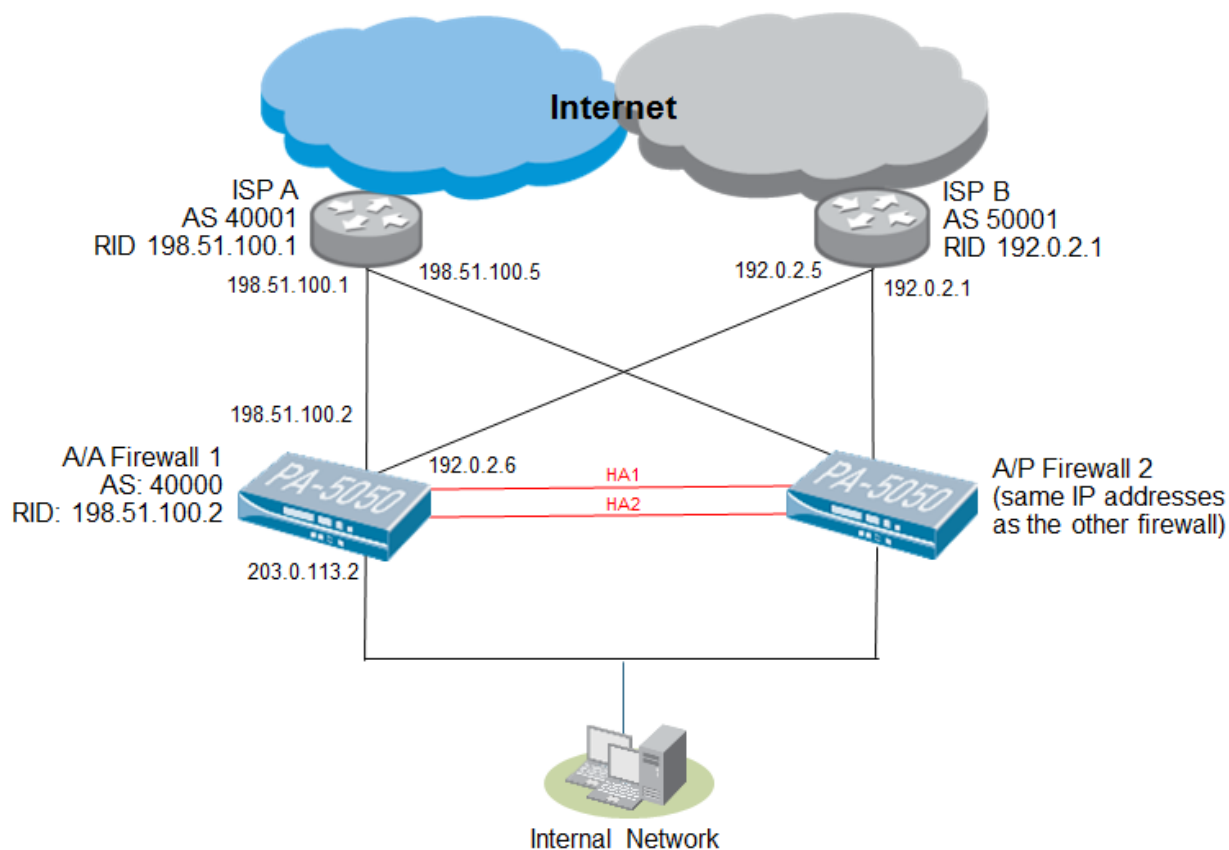


Please refer to that tech note for a discussion of this implementation, and GUI and CLI configuration.

4.4 Example Scenario: Layer 3 Active/Passive HA with BGP

The method for implementing BGP on the Palo Alto Networks firewalls with Active/Passive HA is discussed in detail in the Palo Alto Networks Tech Note: <https://live.paloaltonetworks.com/docs/DOC-1572>.

Below is the network diagram that was implemented for this scenario:

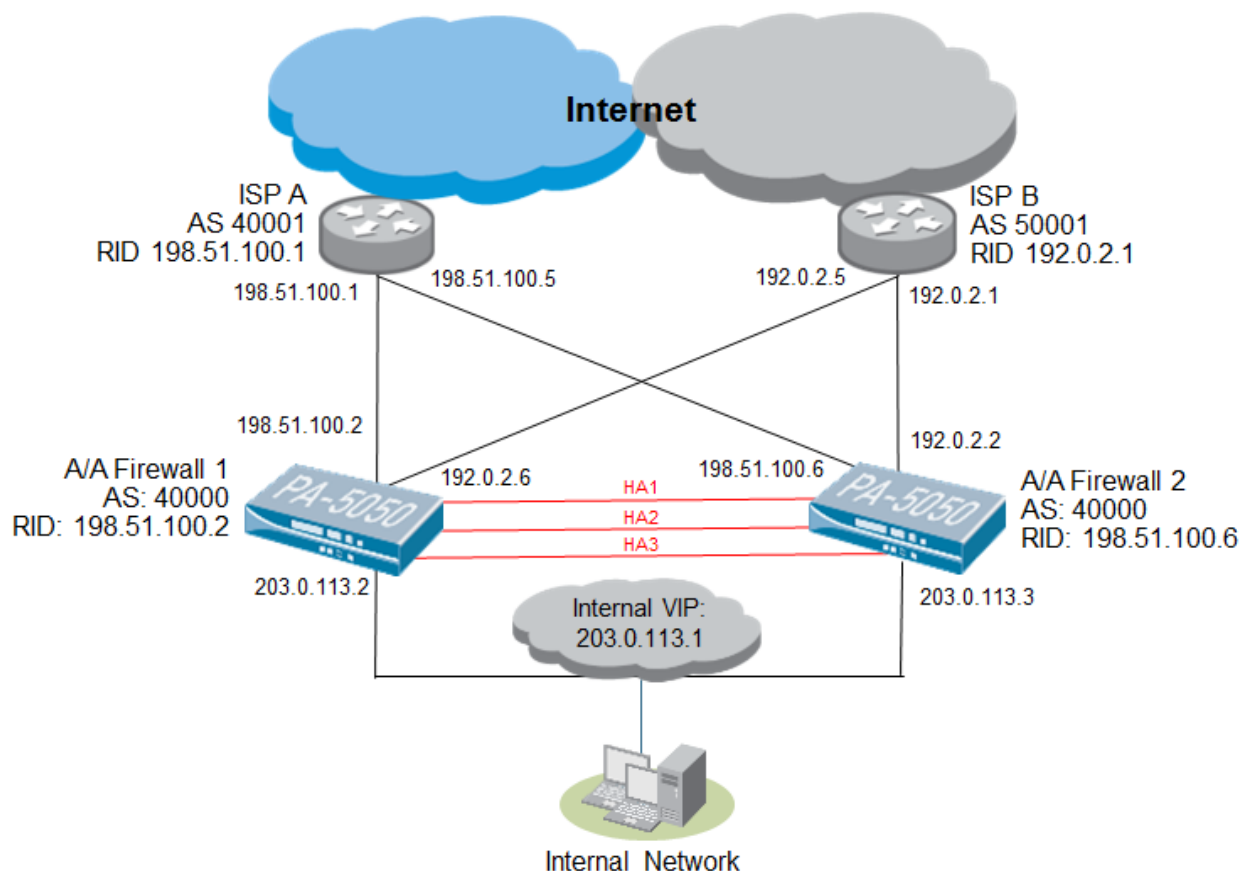


Please refer to that tech note for a discussion of this implementation, and GUI and CLI configuration.

4.5 Example Scenario: Layer 3 Active/Active HA with BGP

The method for implementing BGP on the Palo Alto Networks firewalls with Active/Active HA is discussed in detail in the Palo Alto Networks Tech Note: <https://live.paloaltonetworks.com/docs/DOC-1572>.

Below is the network diagram that was implemented for this scenario:



Please refer to that tech note for a discussion of this implementation, and GUI and CLI configuration.

4.6 Example Scenario: Layer 3 Active/Passive with Link Aggregation

Overview of Challenge

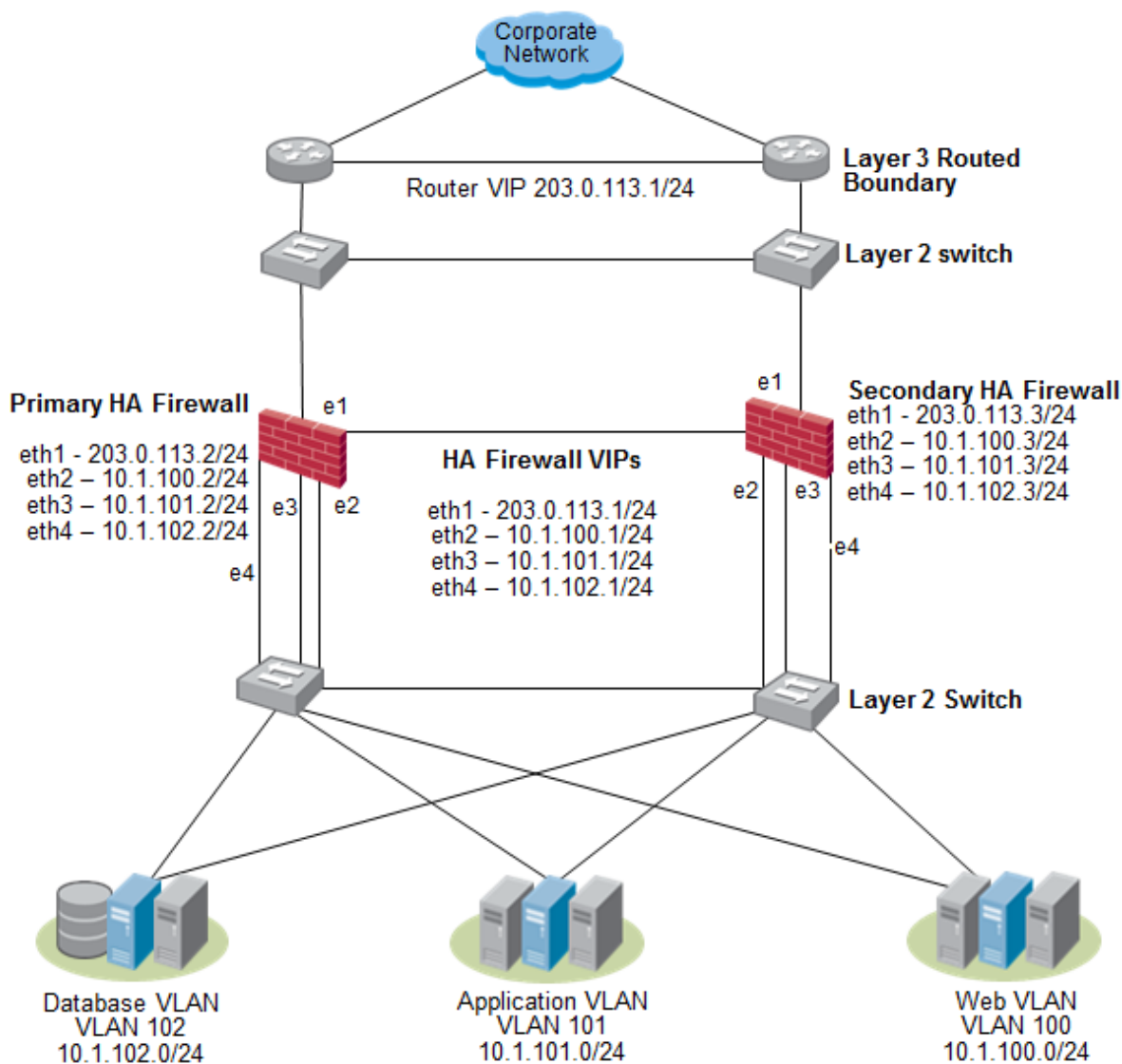
Many organizations today have the need to provide availability and redundancy with their network infrastructures without sacrificing any security controls. Within an application-hosting environment, it is desired to be able to enable security controls that segment applications (or their components), servers, and users while still providing a high-level of infrastructure availability.

A classic security objective is to separate the three major components of a web-based application between the web front-end servers, the application servers, and the database servers. This will be the focused design for the remainder of this document, but this concept can be expanded upon for other similar types of environments and network and security design needs.

This security segmentation desire gets blurred with multi-chassis virtual switch/router configurations and other network and datacenter redundancy solutions are introduced. Typically in this scenario, we are presented with redundant physical switches/routers but they are configured as a single virtual switch/router to help simplify the configuration but still providing network infrastructures with availability and redundancy. This type of switch and router availability can become a serious design challenge when introducing security devices, which typically require symmetric traffic flows to be able to provide effective security controls.

Typical Topology

A typical high availability network and security design that has been used in the past to achieve this level of security segmentation and control is a stacked hub and spoke design, which typically means that if any one component of the network and security design fails, the entire stack fails as well. Below is a sample network diagram of what this typical design might look like.



Classically, during a failure of either the Layer 2 switches before or after the firewall, the Layer 3 Routed Boundary routers, or the firewalls in the primary or secondary stack will cause the entire stack of the design to become unavailable and fail-over to the other stack even if only one of these components within the primary or secondary stack actually failed.

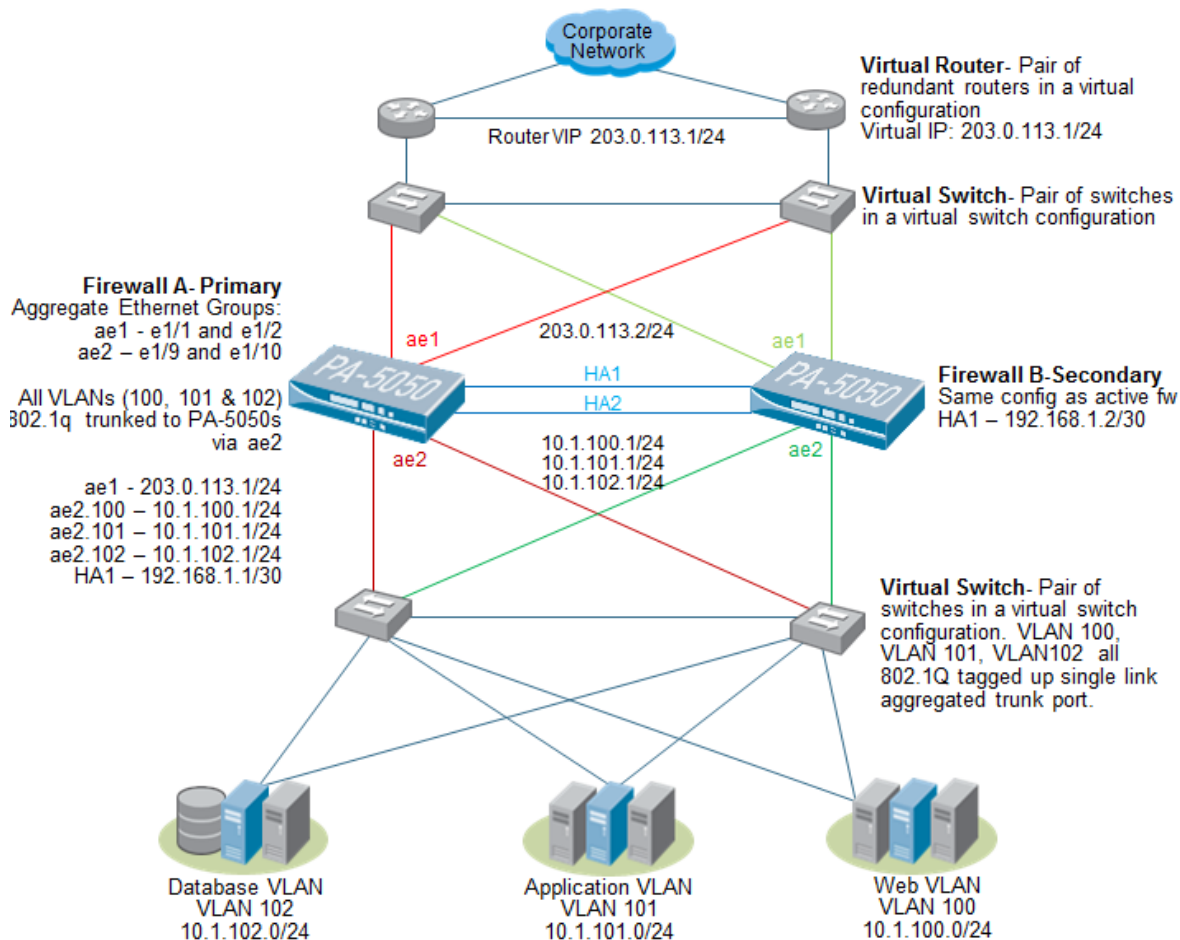
Description of Solution

Since Palo Alto Network's next generation firewalls support both high availability and link aggregation for layer 3 deployments, we can provide the desired segmentation in a more redundant and available fashion with multi-chassis virtual switch and router configurations. The virtual switch environment is making use of multi-chassis

etherchannel (MEC) or link aggregation (802.3ad). MEC or link aggregation is support by multiple different vendors through different technologies such as Cisco VSS (Cisco 6500 platform), Cisco vPC (Cisco Nexus platforms), Nortel (now Avaya) DSMLT, and Juniper MC-LAG. In many of these configurations extensive VLAN trunks and tags are leveraged on top of MEC or link aggregation ports.

The following is a sample configuration of how the above design would appear logically once each of the layer 2 boundaries surrounding the firewalls are configured as multi-chassis virtual switches supporting MEC or link aggregation.

Active/Passive Layer 3 High Availability with Multi-chassis Link Aggregation Topology



GUI Configuration

The following screenshots are of a completed configuration.

Network tab -> Zones

Name	Type	Interfaces / Virtual Systems
Web	layer3	ae2.100
Application	layer3	ae2.101
Database	layer3	ae2.102
CorpNet	layer3	ae1

Network tab -> Interfaces

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone
ethernet1/1	Aggregate (ae1)			none	none	Untagged	none	none
ethernet1/2	Aggregate (ae1)			none	none	Untagged	none	none
ethernet1/3				none	none	Untagged	none	none
ethernet1/4				none	none	Untagged	none	none
ethernet1/5				none	none	Untagged	none	none
ethernet1/6				none	none	Untagged	none	none
ethernet1/7				none	none	Untagged	none	none
ethernet1/8				none	none	Untagged	none	none
ethernet1/9	Aggregate (ae2)			none	none	Untagged	none	none
ethernet1/10	Aggregate (ae2)			none	none	Untagged	none	none
ae1	Layer3			203.0.113.2/24	VR1	Untagged	none	CorpNet
ae2	Layer3			none	none	Untagged	none	none
ae2.100	Layer3			10.1.100.1/24	VR1	100	none	Web
ae2.101	Layer3			10.1.101.1/24	VR1	101	none	Application
ae2.102	Layer3			10.1.102.1/24	VR1	102	none	Database

Network tab-> Virtual Routers

Virtual Router - VR1

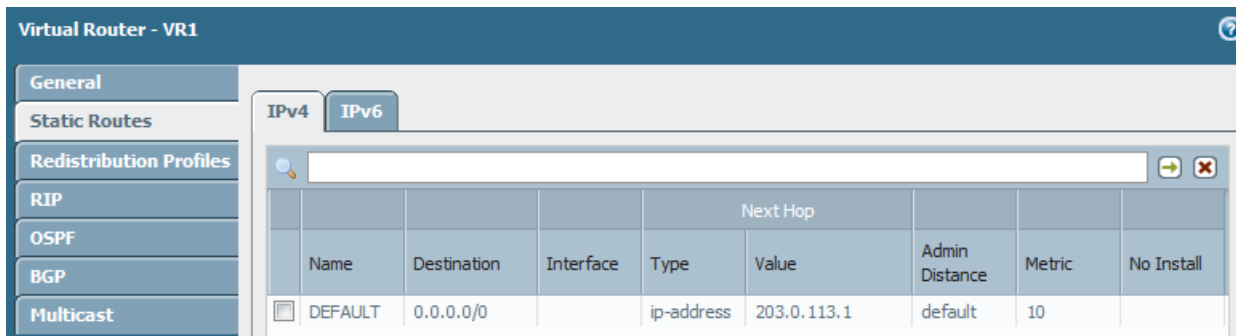
General

NameVR1

Static Routes**Redistribution Profiles****RIP****OSPF****BGP****Multicast**

Interfaces

☐ ae1☐ ae2.100☐ ae2.101☐ ae2.102



The virtual router is configured with the locally connected network routes for ae1, ae2.100, ae2.101, and ae2.102. The default route for our sample configuration points to the corporate network next hop of 203.0.113.1.

Policies tab -> Security

Name	Source			Destination		Application	Service	Action
	Zone	Address	User	Zone	Address			
Inbound Application Access	CorpNet	any	any	Application	any	any	any	✓
				Database				
				Web				
Outbound Application Access	Application	any	any	CorpNet	any	any	any	✓
	Database							
	Web							

Device tab-> High Availability

Primary firewall

General	Link and Path Monitoring	Operational Commands
Setup		
Enable HA <input checked="" type="checkbox"/>		
Group ID 1		
Description Corp HA Pair		
Mode active-passive		
Enable Config Sync <input checked="" type="checkbox"/>		
Peer HA1 IP Address 192.168.1.2		
Backup Peer HA1 IP Address		
Active/Passive Settings		
Passive Link State auto		
Monitor Fail Hold Down Time (min) 1		
Election Settings		
Heartbeat Backup <input checked="" type="checkbox"/>		
Preemptive <input checked="" type="checkbox"/>		
Promotion Hold Time (ms) 2000		
Hello Interval (ms) 8000		
Heartbeat Interval (ms) 1000		
Maximum No. of Flaps 3		
Preemption Hold Time (min) 1		
Monitor Fail Hold Up Time (ms) 0		
Additional Master Hold Up Time (ms) 500		
Device Priority 5		
Control Link (HA1)		
Port dedicated-ha1		
IPv4/IPv6 Address 192.168.1.1		
Netmask 255.255.255.252		
Gateway		
Link Speed auto		
Link Duplex auto		
Encryption Enabled <input type="checkbox"/>		
Monitor Hold Time (ms) 3000		
Control Link (HA1 Backup)		
Port management		
Data Link (HA2)		
Enable Session Synchronization <input checked="" type="checkbox"/>		
Port dedicated-ha2		
IPv4/IPv6 Address		
Netmask		
Gateway		
Link Speed auto		
Link Duplex auto		
Transport ethernet		
Action log-only		
Threshold (ms) 10000		
Data Link (HA2 Backup)		
Port		
IPv4/IPv6 Address		
Netmask		
Gateway		
Link Speed		
Link Duplex		

Secondary firewall

General	Link and Path Monitoring	Operational Commands
Setup		
Enable HA <input checked="" type="checkbox"/>		
Group ID 1		
Description Corp HA Pair		
Mode active-passive		
Enable Config Sync <input checked="" type="checkbox"/>		
Peer HA 1 IP Address 192.168.1.1		
Backup Peer HA 1 IP Address		
Active/Passive Settings		
Passive Link State auto		
Monitor Fail Hold Down Time (min) 1		
Election Settings		
Heartbeat Backup <input checked="" type="checkbox"/>		
Preemptive <input checked="" type="checkbox"/>		
Promotion Hold Time (ms) 2000		
Hello Interval (ms) 8000		
Heartbeat Interval (ms) 1000		
Maximum No. of Flaps 3		
Preemption Hold Time (min) 1		
Monitor Fail Hold Up Time (ms) 0		
Additional Master Hold Up Time (ms) 500		
Device Priority 10		
Control Link (HA1)		
Port dedicated-ha1		
IPv4/IPv6 Address 192.168.1.2		
Netmask 255.255.255.252		
Gateway		
Link Speed auto		
Link Duplex auto		
Encryption Enabled <input type="checkbox"/>		
Monitor Hold Time (ms) 3000		
Control Link (HA1 Backup)		
Port management		
Data Link (HA2)		
Enable Session Synchronization <input checked="" type="checkbox"/>		
Port dedicated-ha2		
IPv4/IPv6 Address		
Netmask		
Gateway		
Link Speed auto		
Link Duplex auto		
Transport ethernet		
Action log-only		
Threshold (ms) 10000		
Data Link (HA2 Backup)		
Port		
IPv4/IPv6 Address		
Netmask		
Gateway		
Link Speed		
Link Duplex		

Note that once the high availability configuration is completed on both PA-5050 appliances, configuration sync will need to be completed on the PA-5050-Primary to sync the running configuration from the PA-5050-Primary to the PA-5050-Secondary.

Link and Path Monitoring Configuration

General

Link and Path Monitoring

Operational Commands

Link Monitoring

Enabled ☒

Failure Condition any

Link Group

Name	Enabled	Group Failure Condition	Interfaces
<input type="checkbox"/> AE1 Monitor	<input checked="" type="checkbox"/>	all	ethernet1/1 ethernet1/2
<input type="checkbox"/> AE2 Monitor	<input checked="" type="checkbox"/>	all	ethernet1/10 ethernet1/9

Path Monitoring

Enabled ☐

Failure Condition any

Path Group

Name	Type	Enabled	Failure Condition	Source IP	Destination IP	Ping Interval	Ping Count
------	------	---------	-------------------	-----------	----------------	---------------	------------

In the above example we are only failing over to the PA-5050-Secondary device, if the PA-5050-Primary loses link state on both physical Ethernet ports associated with the ae1 or ae2. Alternatively, the link monitor could be configured so that if any physical Ethernet port fails the entire PA-5050-Primary device fails-over to the PA-5050-Secondary device. Here is a sample of this link monitor configuration:

General

Link and Path Monitoring

Operational Commands

Link Monitoring

Enabled ☒

Failure Condition any

Link Group

Name	Enabled	Group Failure Condition	Interfaces
<input type="checkbox"/> Any Ethernet	<input checked="" type="checkbox"/>	any	ethernet1/1 ethernet1/10 ethernet1/2 ethernet1/9

We can also configure appropriate path monitors to trigger a fail-over as well. During our testing in the lab, we did not notice any increase in high availability fail-over times when MEC and link aggregation was configured. We notice no more than a single ping packet being lost when a single link the in the Aggregate Ethernet group failed

using the first link monitor configuration and the high-availability did not fail-over from the primary PA-5050 to the secondary PA-5050.

CLI Configuration

The CLI commands used to configure this scenario are shown below: ¹⁰

Interface configuration

```
set network interface ethernet ethernet1/1 link-speed auto
set network interface ethernet ethernet1/1 link-duplex auto
set network interface ethernet ethernet1/1 link-state auto
set network interface ethernet ethernet1/1 aggregate-group ae1
set network interface ethernet ethernet1/2 link-speed auto
set network interface ethernet ethernet1/2 link-duplex auto
set network interface ethernet ethernet1/2 link-state auto
set network interface ethernet ethernet1/2 aggregate-group ae1
set network interface ethernet ethernet1/9 link-speed auto
set network interface ethernet ethernet1/9 link-duplex auto
set network interface ethernet ethernet1/9 link-state auto
set network interface ethernet ethernet1/9 aggregate-group ae2
set network interface ethernet ethernet1/10 link-speed auto
set network interface ethernet ethernet1/10 link-duplex auto
set network interface ethernet ethernet1/10 link-state auto
set network interface ethernet ethernet1/10 aggregate-group ae2

set network interface aggregate-ethernet ae1 layer3 mtu 1500
set network interface aggregate-ethernet ae1 layer3 ip 203.0.113.2/24
set network interface aggregate-ethernet ae1 layer3 ipv6 enabled no
set network interface aggregate-ethernet ae1 layer3 ipv6 neighbor-discovery enable-dad no
set network interface aggregate-ethernet ae2 layer3 mtu 1500
set network interface aggregate-ethernet ae2 layer3 ipv6 enabled no
set network interface aggregate-ethernet ae2 layer3 ipv6 neighbor-discovery enable-dad no
set network interface aggregate-ethernet ae2 layer3 units ae2.100 mtu 1500
set network interface aggregate-ethernet ae2 layer3 units ae2.100 tag 100
set network interface aggregate-ethernet ae2 layer3 units ae2.102 adjust-tcp-mss no
set network interface aggregate-ethernet ae2 layer3 units ae2.100 ip 10.1.100.1/24
set network interface aggregate-ethernet ae2 layer3 units ae2.100 ipv6 enabled no
set network interface aggregate-ethernet ae2 layer3 units ae2.100 ipv6 neighbor-discovery enable-dad no
set network interface aggregate-ethernet ae2 layer3 units ae2.101 mtu 1500
set network interface aggregate-ethernet ae2 layer3 units ae2.101 tag 101
set network interface aggregate-ethernet ae2 layer3 units ae2.102 adjust-tcp-mss no
set network interface aggregate-ethernet ae2 layer3 units ae2.101 ip 10.1.101.1/24
set network interface aggregate-ethernet ae2 layer3 units ae2.101 ipv6 enabled no
set network interface aggregate-ethernet ae2 layer3 units ae2.101 ipv6 neighbor-discovery enable-dad no
set network interface aggregate-ethernet ae2 layer3 units ae2.102 mtu 1500
set network interface aggregate-ethernet ae2 layer3 units ae2.102 tag 102
set network interface aggregate-ethernet ae2 layer3 units ae2.102 adjust-tcp-mss no
set network interface aggregate-ethernet ae2 layer3 units ae2.102 ip 10.1.102.1/24
set network interface aggregate-ethernet ae2 layer3 units ae2.102 ipv6 enabled no
```

¹⁰ This output was obtained by running these three commands: “set cli config-output-format set” , “configure”, and “show”. Only commands relevant to this particular scenario are listed.

```
set network interface aggregate-ethernet ae2 layer3 units ae2.102 ipv6 neighbor-  
discovery enable-dad no
```

Virtual Router configuration

```
set network virtual-router VR1 interface ae1  
set network virtual-router VR1 interface ae2.100  
set network virtual-router VR1 interface ae2.101  
set network virtual-router VR1 interface ae2.102  
set network virtual-router VR1 routing-table ip static-route DEFAULT destination  
0.0.0.0/0  
set network virtual-router VR1 routing-table ip static-route DEFAULT nexthop ip-  
address 203.0.113.1  
set network virtual-router VR1 protocol rip enable no  
set network virtual-router VR1 protocol rip reject-default-route yes  
set network virtual-router VR1 protocol rip allow-redist-default-route no  
set network virtual-router VR1 protocol rip timers interval-seconds 1  
set network virtual-router VR1 protocol rip timers update-intervals 30  
set network virtual-router VR1 protocol rip timers expire-intervals 30  
set network virtual-router VR1 protocol rip timers delete-intervals 120  
set network virtual-router VR1 protocol ospf enable no  
set network virtual-router VR1 protocol ospf reject-default-route yes  
set network virtual-router VR1 protocol ospf allow-redist-default-route no  
set network virtual-router VR1 protocol ospf rfc1583 no  
set network virtual-router VR1 protocol bgp enable no  
set network virtual-router VR1 protocol bgp reject-default-route no  
set network virtual-router VR1 protocol bgp routing-options as-format 2-byte  
set network virtual-router VR1 protocol bgp routing-options med deterministic-med-  
comparison no  
set network virtual-router VR1 protocol bgp routing-options default-local-  
preference 100  
set network virtual-router VR1 protocol bgp routing-options graceful-restart enable  
no  
set network virtual-router VR1 protocol bgp routing-options graceful-restart stale-  
route-time 120  
set network virtual-router VR1 protocol bgp routing-options graceful-restart local-  
restart-time 120  
set network virtual-router VR1 protocol bgp routing-options graceful-restart max-  
peer-restart-time 120  
set network virtual-router VR1 protocol bgp routing-options aggregate aggregate-med  
yes  
set network virtual-router VR1 admin-dists static 10  
set network virtual-router VR1 admin-dists ospf-int 30  
set network virtual-router VR1 admin-dists ospf-ext 110  
set network virtual-router VR1 admin-dists ibgp 200  
set network virtual-router VR1 admin-dists ebgp 20  
set network virtual-router VR1 admin-dists rip 120
```

Zone configuration

```
set zone CorpNet network layer3 ae1  
set zone CorpNet enable-user-identification no  
set zone Web network layer3 ae2.100  
set zone Web enable-user-identification no  
set zone Application network layer3 ae2.101
```

```
set zone Application enable-user-identification no
set zone Database network layer3 ae2.102
set zone Database enable-user-identification no
```

Policy configuration

```
set rulebase security rules "Inbound Application Access" from CorpNet
set rulebase security rules "Inbound Application Access" to Application
set rulebase security rules "Inbound Application Access" to Database
set rulebase security rules "Inbound Application Access" to Web
set rulebase security rules "Inbound Application Access" source any
set rulebase security rules "Inbound Application Access" destination any
set rulebase security rules "Inbound Application Access" service any
set rulebase security rules "Inbound Application Access" application any
set rulebase security rules "Inbound Application Access" action allow
set rulebase security rules "Inbound Application Access" log-end yes
set rulebase security rules "Inbound Application Access" option disable-server-
response-inspection no
set rulebase security rules "Inbound Application Access" source-user any
set rulebase security rules "Inbound Application Access" hip-profiles any
set rulebase security rules "Inbound Application Access" log-start no
set rulebase security rules "Inbound Application Access" negate-source no
set rulebase security rules "Inbound Application Access" negate-destination no
set rulebase security rules "Outbound Application Access" from Application
set rulebase security rules "Outbound Application Access" from Database
set rulebase security rules "Outbound Application Access" from Web
set rulebase security rules "Outbound Application Access" to CorpNet
set rulebase security rules "Outbound Application Access" source any
set rulebase security rules "Outbound Application Access" destination any
set rulebase security rules "Outbound Application Access" service any
set rulebase security rules "Outbound Application Access" application any
set rulebase security rules "Outbound Application Access" action allow
set rulebase security rules "Outbound Application Access" log-end yes
set rulebase security rules "Outbound Application Access" option disable-server-
response-inspection no
set rulebase security rules "Outbound Application Access" source-user any
set rulebase security rules "Outbound Application Access" hip-profiles any
set rulebase security rules "Outbound Application Access" log-start no
set rulebase security rules "Outbound Application Access" negate-source no
set rulebase security rules "Outbound Application Access" negate-destination no
```

High Availability configuration- primary firewall

```
set deviceconfig high-availability enabled yes
set deviceconfig high-availability interface ha1 port dedicated-ha1
set deviceconfig high-availability interface ha1 link-speed auto
set deviceconfig high-availability interface ha1 link-duplex auto
set deviceconfig high-availability interface ha1 ip-address 192.168.1.1
set deviceconfig high-availability interface ha1 netmask 255.255.255.252
set deviceconfig high-availability interface ha1 monitor-hold-time 3000
set deviceconfig high-availability interface ha2 port dedicated-ha2
set deviceconfig high-availability interface ha2 link-speed auto
set deviceconfig high-availability interface ha2 link-duplex auto
set deviceconfig high-availability group 1 description "Corp HA Pair"
set deviceconfig high-availability group 1 peer-ip 192.168.1.2
set deviceconfig high-availability group 1 election-option device-priority 5
```

```

set deviceconfig high-availability group 1 election-option heartbeat-backup yes
set deviceconfig high-availability group 1 election-option preemptive yes
set deviceconfig high-availability group 1 election-option promotion-hold-time 2000
set deviceconfig high-availability group 1 election-option hello-interval 1000
set deviceconfig high-availability group 1 election-option heartbeat-interval 1000
set deviceconfig high-availability group 1 election-option flap-max 3
set deviceconfig high-availability group 1 election-option preemption-hold-time 1
set deviceconfig high-availability group 1 election-option monitor-fail-hold-up-
time 0
set deviceconfig high-availability group 1 election-option additional-master-hold-
up-time 500
set deviceconfig high-availability group 1 state-synchronization enabled yes
set deviceconfig high-availability group 1 state-synchronization transport ethernet
set deviceconfig high-availability group 1 configuration-synchronization enabled
yes
set deviceconfig high-availability group 1 mode active-passive passive-link-state
auto
set deviceconfig high-availability group 1 mode active-passive monitor-fail-hold-
down-time 1

```

High Availability configuration- secondary firewall

```

set deviceconfig high-availability enabled yes
set deviceconfig high-availability interface ha1 port dedicated-ha1
set deviceconfig high-availability interface ha1 link-speed auto
set deviceconfig high-availability interface ha1 link-duplex auto
set deviceconfig high-availability interface ha1 ip-address 192.168.1.2
set deviceconfig high-availability interface ha1 netmask 255.255.255.252
set deviceconfig high-availability interface ha1 monitor-hold-time 3000
set deviceconfig high-availability interface ha2 port dedicated-ha2
set deviceconfig high-availability interface ha2 link-speed auto
set deviceconfig high-availability interface ha2 link-duplex auto
set deviceconfig high-availability group 1 description "Corp HA Pair"
set deviceconfig high-availability group 1 peer-ip 192.168.1.1
set deviceconfig high-availability group 1 election-option device-priority 10
set deviceconfig high-availability group 1 election-option heartbeat-backup yes
set deviceconfig high-availability group 1 election-option preemptive yes
set deviceconfig high-availability group 1 election-option promotion-hold-time 2000
set deviceconfig high-availability group 1 election-option hello-interval 1000
set deviceconfig high-availability group 1 election-option heartbeat-interval 1000
set deviceconfig high-availability group 1 election-option flap-max 3
set deviceconfig high-availability group 1 election-option preemption-hold-time 1
set deviceconfig high-availability group 1 election-option monitor-fail-hold-up-
time 0
set deviceconfig high-availability group 1 election-option additional-master-hold-
up-time 500
set deviceconfig high-availability group 1 state-synchronization enabled yes
set deviceconfig high-availability group 1 state-synchronization transport ethernet
set deviceconfig high-availability group 1 configuration-synchronization enabled
yes
set deviceconfig high-availability group 1 mode active-passive passive-link-state
auto
set deviceconfig high-availability group 1 mode active-passive monitor-fail-hold-
down-time 1

```

Link and Path Monitoring Configuration

The following commands configure the PA-5050 device for a high availability fail-over when any interface failure regardless of aggregate ethernet group health.

```
set deviceconfig high-availability group 1 monitoring path-monitoring enabled no
set deviceconfig high-availability group 1 monitoring link-monitoring enabled yes
set deviceconfig high-availability group 1 monitoring link-monitoring failure-
condition any
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"All Ethernet" enabled yes
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"All Ethernet" failure-condition any
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"All Ethernet" interface ethernet1/1
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"All Ethernet" interface ethernet1/10
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"All Ethernet" interface ethernet1/2
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"All Ethernet" interface ethernet1/9
```

The following commands configure the device for high availability fail-over when both interfaces in a single aggregate ethernet group fail.

```
set deviceconfig high-availability group 1 monitoring link-monitoring failure-
condition any
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"AE1 Monitor" enabled yes
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"AE1 Monitor" failure-condition all
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"AE1 Monitor" interface ethernet1/1
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"AE1 Monitor" interface ethernet1/2
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"AE2 Monitor" enabled yes
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"AE2 Monitor" failure-condition all
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"AE2 Monitor" interface ethernet1/10
set deviceconfig high-availability group 1 monitoring link-monitoring link-group
"AE2 Monitor" interface ethernet1/9
```

Sample Cisco 6500 VSS configuration with MEC

This is a sample partial configuration output from a pair of Cisco 6500 switches setup in a Virtual Switch System (VSS) configuration. Some of the unimportant configuration has been omitted for simplicity and readability.

The following table is a summary of how the physical ports on the 6500, port channels on the 6500, the Aggregate Ethernet interfaces on the PA-5050, and the physical ports on the PA-5050s are all connected based on the sample configuration portions from above and below.

6500 port-channel	6500 Switch1 port	6500 Switch2 port	PA-5050 Aggregate Ethernet	PA-5050 Primary ports	PA-5050 Secondary ports
1	GigabitEthernet 1/1/3	GigabitEthernet 2/1/3	ae2 (ae2.100, ae2.101, and ae2.102)	ethernet1/9 ethernet1/10	None
2	GigabitEthernet 1/1/4	GigabitEthernet 2/1/4	ae2 (ae2.100, ae2.101, and ae2.102)	None	ethernet1/9 ethernet1/10
3	GigabitEthernet 1/1/1	GigabitEthernet 2/1/1	ae1	ethernet1/1 ethernet1/2	None
4	GigabitEthernet 1/1/2	GigabitEthernet 2/1/2	ae1	None	ethernet1/1 ethernet1/2

```
Current configuration : 17201 bytes
!
! Last configuration change at 22:34:50 GMT Mon Jul 18 2011
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service counters max age 5
!
hostname ciscoVSS
!
boot-start-marker
boot system flash sup-bootdisk:
boot-end-marker
!
security passwords min-length 1
logging buffered 61440
enable secret 5
!
username privilege 15 password 7
no aaa new-model
!
!
!
```

```

no ip domain-lookup
vtp mode transparent
!
switch virtual domain 255
  switch mode virtual
  switch 1 priority 200
!
mls netflow interface
mls cef error action reset
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
diagnostic bootup level minimal
port-channel load-balance dst-mac
!
redundancy
  main-cpu
  auto-sync running-config
  mode sso
!
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 14
  name CorpNet
!
vlan 100
  name Web
!
vlan 101
  name Applicaton
!
vlan 102
  name Database
!
!
!
interface Port-channel1
  description "VSS-Web-App-DB A"
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 100-102
  switchport mode trunk
  logging event link-status
  logging event trunk-status
  logging event bundle-status
!
interface Port-channel2
  description "VSS-Web-App-DB B"
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 100-102
  switchport mode trunk
  logging event link-status
  logging event trunk-status
  logging event bundle-status

```

```

!
interface Port-channel3
  description "VSS-CorpNet A"
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 14
  switchport trunk allowed vlan 14
  switchport mode trunk
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  spanning-tree bpdufilter disable
!
interface Port-channel4
  description "VSS-CorpNet B"
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 14
  switchport trunk allowed vlan 14
  switchport mode trunk
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  spanning-tree bpdufilter disable
!
interface Port-channel255
  no switchport
  no ip address
  switch virtual link 1
  mls qos trust cos
  no mls qos channel-consistency
!
interface Port-channel256
  no switchport
  no ip address
  switch virtual link 2
  mls qos trust cos
  no mls qos channel-consistency
!
interface GigabitEthernet1/1/1
  description "VSS-CorpNet-PAN-Primary"
  switchport
  switchport trunk native vlan 14
  switchport trunk allowed vlan 14
  switchport mode trunk
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  channel-group 3 mode on
!
interface GigabitEthernet1/1/2
  description "VSS-CorpNet-PAN-Secondary"
  switchport
  switchport trunk native vlan 14
  switchport trunk allowed vlan 14
  switchport mode trunk
  logging event link-status

```



```

logging event trunk-status
logging event bundle-status
channel-group 4 mode on
!
interface GigabitEthernet1/1/3
description "VSS-Web-App-DB-PAN-Primary"
switchport
switchport trunk allowed vlan 100-102
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
channel-group 1 mode on
!
interface GigabitEthernet1/1/4
description " VSS-Web-App-DB-PAN-Secondary"
switchport
switchport trunk allowed vlan 100-102
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
channel-group 2 mode on
!
...
Skipping additional interface configuration on the first 6500 in the VSS configuration.
...
!
interface TenGigabitEthernet1/5/4
no switchport
no ip address
mls qos trust cos
channel-group 255 mode on
!
interface TenGigabitEthernet1/5/5
no switchport
no ip address
mls qos trust cos
channel-group 256 mode on
!
interface GigabitEthernet2/1/1
description "VSS-CorpNet-PAN-Primary"
switchport
switchport trunk native vlan 14
switchport trunk allowed vlan 14
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
channel-group 3 mode on
!
interface GigabitEthernet2/1/2
description "VSS-CorpNet-PAN-Secondary"
switchport
switchport trunk native vlan 14
switchport trunk allowed vlan 14
switchport mode trunk

```

```

logging event link-status
logging event trunk-status
logging event bundle-status
channel-group 4 mode on
!
interface GigabitEthernet2/1/3
description "VSS-Web-App-DB-PAN-Primary"
switchport
switchport trunk allowed vlan 100-102
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
channel-group 1 mode on
!
interface GigabitEthernet2/1/4
description "VSS-Web-App-DB-PAN-Secondary"
switchport
switchport trunk allowed vlan 100-102
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
channel-group 2 mode on
!
...
Skipping additional interface configuration on the secondary 6500 in the VSS configuration.
...
!
interface TenGigabitEthernet2/5/4
no switchport
no ip address
mls qos trust cos
channel-group 255 mode on
!
interface TenGigabitEthernet2/5/5
no switchport
no ip address
mls qos trust cos
channel-group 256 mode on
!
interface Vlan14
ip address 203.0.113.1 255.255.255.0
no ip redirects
no ip unreachableables
!
...
Skipping Routing Configuration in Cisco VSS configuration
...
!
!
no ip http server
no ip http secure-server
!
!
!
!

```

```

control-plane
!
!
!
!
!
line con 0
line vty 0 4
  login local
!
mac-address-table aging-time 480
no event manager policy Mandatory.go_switchbus.tcl type system
!
!
module provision switch 1
  slot 1 slot-type 284 port-type 60 number 16  virtual-slot 17
  slot 2 slot-type 147 port-type 61 number 48  virtual-slot 18
  slot 5 slot-type 254 port-type 31 number 2 port-type 61 number 1 port-type 60
number 2  virtual-slot 21
!
module provision switch 2
  slot 1 slot-type 284 port-type 60 number 16  virtual-slot 33
  slot 2 slot-type 147 port-type 61 number 48  virtual-slot 34
  slot 5 slot-type 254 port-type 31 number 2 port-type 61 number 1 port-type 60
number 2  virtual-slot 37

!

end

```

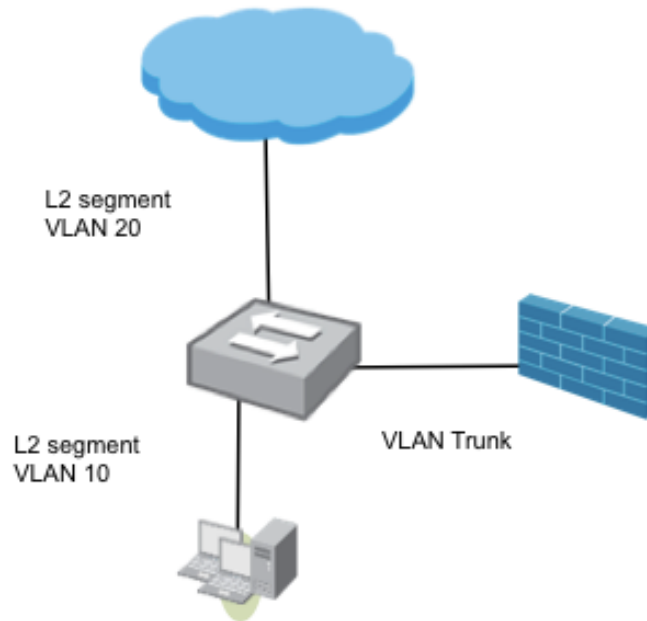
4.8 Example Scenario: Firewall on a Stick

Overview of Challenge/Problem

VLANs divide broadcast domains in a LAN environment and are used as an alternative solution to routers for broadcast containment. A Layer 2 switch can be configured to group subsets of its ports into virtual broadcast domains isolated from each other. These domains are commonly known as virtual LANs (VLANs). Using a VLAN not only offers the benefit of containing traffic within a LAN segment, but also provides security by restricting communication between hosts in different VLANs. Typical VLAN implementations will have hosts in each VLAN that use a unique IP subnet. In order for hosts in one VLAN to communicate with hosts in another VLAN, a router must be used to route traffic between the VLANs. This is known as inter-VLAN routing.

Typical Topology

Below is a sample diagram of a network where security protection may be desired to provide protection between the external network and the internal networks as well as the DMZs.



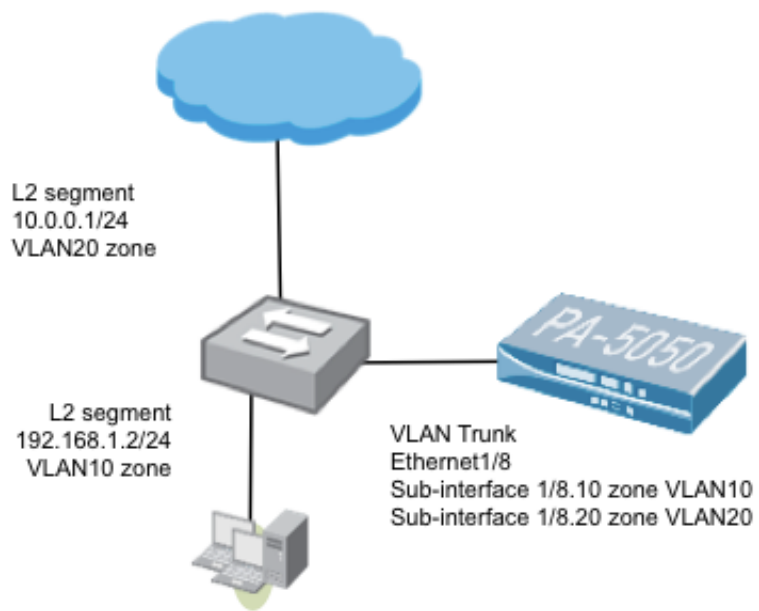
Description of Solution

In order for hosts in one VLAN to communicate with hosts in another VLAN, a router must be used to route traffic between the VLANs. This is known as inter-VLAN routing. A Palo Alto Networks firewall can be used to secure inter-VLAN traffic. This is also commonly called one arm routing or router on a stick.

The firewall configuration consists of a layer 3 interface and sub-interfaces corresponding to each one of the VLANs that are created off of the parent L3 interface. Each sub-interface is assigned a VLAN tag and an IP address that corresponds to the VLAN to which they provide connectivity. Sub-interfaces are assigned to separate zones to enforce security policy checks on inter-VLAN traffic.

Inter-VLAN routing and Router on a Stick Topology

Palo Alto Networks firewalls can be used to secure inter-VLAN traffic. Each VLAN has its own IP subnet and a single IP subnet spans multiple VLANs.



GUI Configuration





The following screenshots show a completed configuration:

Network tab -> Zones

Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	Enable User Identification
untagged	layer3	ethernet1/8			<input type="checkbox"/>
VLAN10	layer3	ethernet1/8.10			<input checked="" type="checkbox"/>
VLAN20	layer3	ethernet1/8.20			<input type="checkbox"/>





The physical interface Ethernet 1/8 is configured as the untagged zone. Sub-interface 1/8.10 is configured to VLAN10 zone and sub-interface 1/8.20 is configured to VLAN20 zone. If you plan to implement user-ID, check the box to “enable user-identification” on the internal zone.

Network tab-> Interfaces

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone
 ethernet1/8	Layer3			10.10.10.1/24	default	Untagged	none	untagged
 ethernet1/8.10	Layer3	allow ping		192.168.1.1/24	default	10	none	VLAN10
 ethernet1/8.20	Layer3	allow ping		10.0.0.1/24	default	20	none	VLAN20

In this example we are using Ethernet 1/8 as the trunk port. You can configure the physical interface with the untagged gateway IP address and add it to the Untagged zone. You can then select Ethernet 1/8 and using the drop down menu at the bottom select New → “L3 interface” for both tagged VLANs. You can then add them to their own security zone and select the same virtual router.

Policies tab-> Security

Source				Destination					
Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile
rule1	 VLAN10	any	any	 VLAN20	any	any	any		

Configure a security policy that allows traffic to flow between zones. Assign security profiles to inspect for viruses/spyware/threats as appropriate. After you have traffic flowing through the device using the wide-open policies above, you should modify policies to limit what traffic should flow through your device.

CLI Configuration

The CLI commands used to configure this scenario are shown below:

```
# Network configuration for Layer3 interface on port 8
set network interface ethernet ethernet1/8 link-speed auto
set network interface ethernet ethernet1/8 link-duplex auto
set network interface ethernet ethernet1/8 link-state auto
set network interface ethernet ethernet1/8 layer3 mtu 1500
set network interface ethernet ethernet1/8 layer3 ip 10.10.10.1/24
set network interface ethernet ethernet1/8 layer3 ipv6 enabled no
set network interface ethernet ethernet1/8 layer3 ipv6 neighbor-discovery enable-dad no
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.10 mtu 1500
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.10 interface-management-profile
"allow ping"
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.10 tag 10
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.10 ip 192.168.1.1/24
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.10 ipv6 enabled no
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.10 ipv6 neighbor-discovery
enable-dad no
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.20 mtu 1500
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.20 interface-management-profile
"allow ping"
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.20 tag 20
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.20 ip 10.0.0.1/24
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.20 ipv6 enabled no
set network interface ethernet ethernet1/8 layer3 units ethernet1/8.20 ipv6 neighbor-discovery
enable-dad no

# Virtual Router configuration
set network virtual-router default routing-table ip static-route Default-route destination 0.0.0.0/0
set network virtual-router default routing-table ip static-route Default-route nexthop ip-address
10.0.0.254
set network virtual-router default interface ethernet1/8
set network virtual-router default interface ethernet1/8.10
set network virtual-router default interface ethernet1/8.20

# Zone configuration
set zone VLAN10 network layer3 ethernet1/8.10
set zone VLAN10 enable-user-identification yes
set zone VLAN20 network layer3 ethernet1/8.20
set zone VLAN20 enable-user-identification no

# Policy configuration
set rulebase security rules rule1 from VLAN10
set rulebase security rules rule1 to VLAN20
set rulebase security rules rule1 source any
set rulebase security rules rule1 destination any
set rulebase security rules rule1 service any
set rulebase security rules rule1 application any
set rulebase security rules rule1 action allow
set rulebase security rules rule1 log-end yes
set rulebase security rules rule1 profile-setting profiles url-filtering "alert all URL"
set rulebase security rules rule1 profile-setting profiles virus "alert all AV"
set rulebase security rules rule1 profile-setting profiles spyware "alert all spyware"
set rulebase security rules rule1 profile-setting profiles vulnerability "alert all vulnerabilities"
```

Cisco Catalyst Config for this scenario:

Building configuration...

Current configuration: 1672 bytes

```
!  
version 12.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Example  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5  
enable password  
!  
no aaa new-model  
switch 1 provision ws-c3750g-24t  
system mtu routing 1500  
ip subnet-zero  
!  
!  
!  
!  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
!  
!  
interface GigabitEthernet1/0/1  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/2  
switchport trunk encapsulation dot1q  
switchport mode trunk  
!  
interface GigabitEthernet1/0/3  
switchport access vlan 20  
!  
interface GigabitEthernet1/0/4  
!  
interface GigabitEthernet1/0/5  
!  
interface GigabitEthernet1/0/6  
!  
interface GigabitEthernet1/0/7
```



```

!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan10
  no ip address
!
interface Vlan20
  no ip address
!
ip classless
ip http server
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0
line vty 0 4
  password ***

```

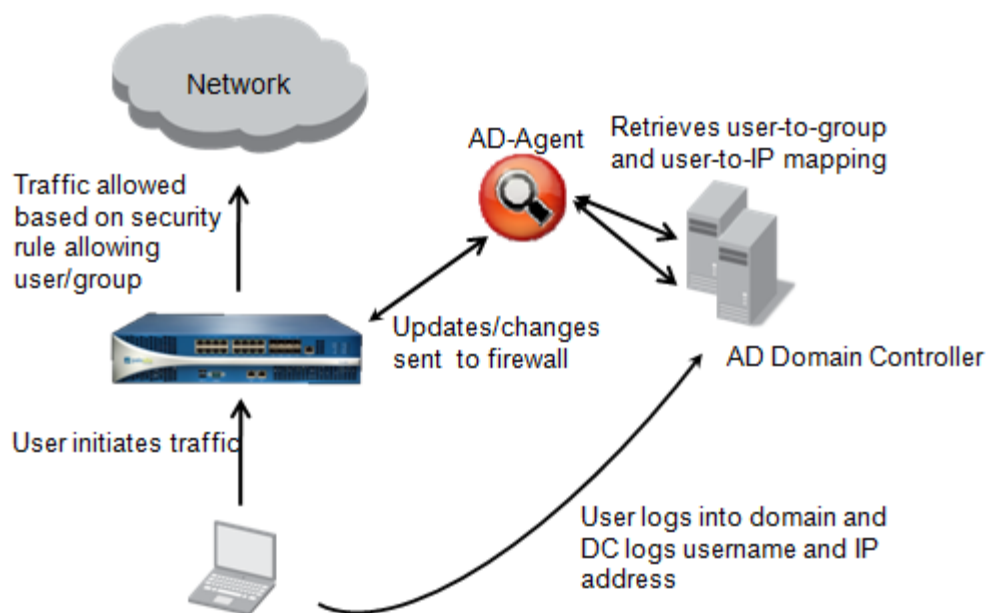
```
login
line vty 5 15
password ***
login
!
end
```

Appendix A: Review of User-ID Operation

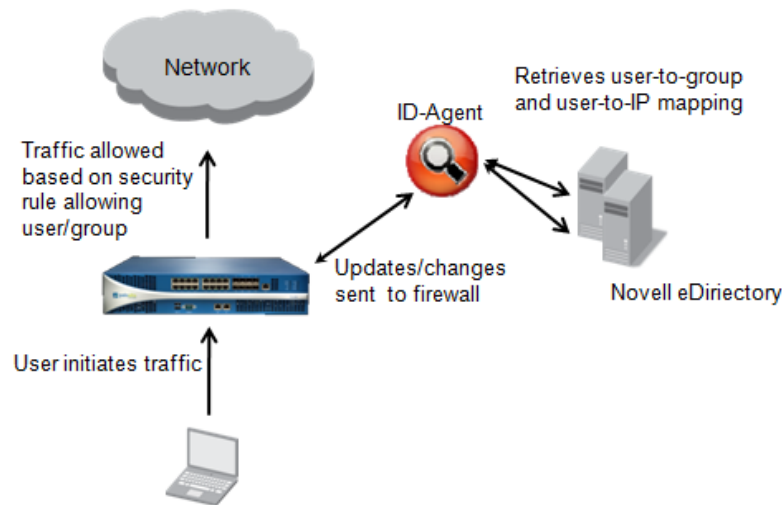
PAN-OS running on Palo Alto Networks firewalls is capable of leveraging user and user group information from Active Directory (AD), user information from Terminal Servers, LDAP servers and RADIUS servers for visibility and policy enforcement.

The User Identification Agent (UIA) interfaces with Active Directory to communicate user group, user, and IP address information to the Palo Alto Networks firewalls for visibility only, or visibility and policy enforcement.

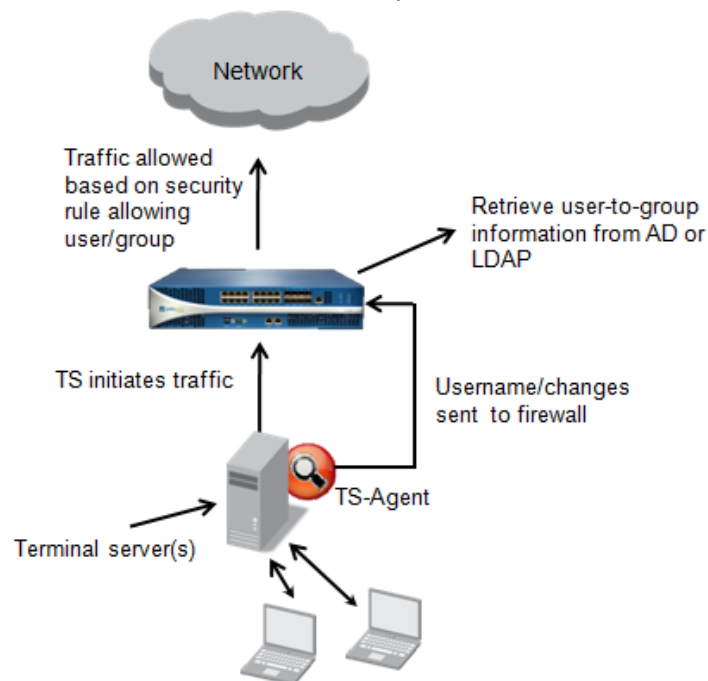
The agent runs on an external PC platform (Windows XP/2003/Vista/2008/Win7 32/64 bit platforms) and communicates with the AD Domain Controller(s). The agent can also be installed directly on a Domain Controller, which participates in the netlogon process. The AD agent is supported in all deployment modes and by default the firewall will communicate from the management port with the agent.



The User-ID Agent interfaces with Novell LDAP eDirectory where user group and user and IP address information can be retrieved. Other LDAP directories (e.g. OpenLDAP) can also be used, but only Novell LDAP can be used to retrieve the IP address in addition to the user to user-group mapping.



The Terminal Server Agent resides on the Terminal Server and communicates with the firewall providing username-mapping to source ports. This mapping allows user identification for any application (not only web applications) used from the Terminal Server when sessions pass between the client and the Terminal Server.

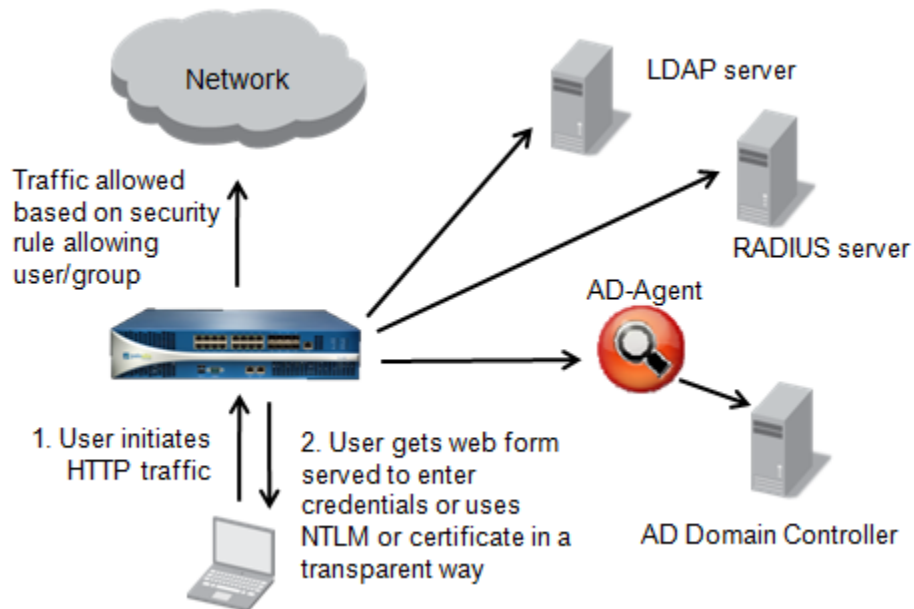


Captive Portal is an interactive way to authenticate users. This mechanism is intended for users which have not been authenticated through AD, LDAP, or Terminal Server before and are considered to be an 'unknown' user to

the firewall. As an example, it will also track roaming users in an AD environment when they roam between a fixed network connection and a wireless network.

The methods used to authenticate through the captive portal are:

- Local user database
- RADIUS server
- LDAP server
- NTLMv2 (automated for the user)
- Certificate on the end-user station (automated for the user)



The ACC, App-Scope, and logs will include the username and the IP address when user identification is configured, showing visibility into individual user activity. If used to enforce policy as well (in vwire, L2 or route mode), users and user groups can be selected in the security policies when Active Directory or LDAP is used. When only a RADIUS server is used, usernames must be manually entered into policy for enforcement unless LDAP is used to retrieve the group membership of each authenticated user.

Revision History

Date	Revision	Comment
4/08/2013	B	<ul style="list-style-type: none">• Section 1: Tap Mode Deployment Scenarios, minor updates to the CLI section in the Tap Ports in Proxy Environment section. Interface mode and Policy Configuration sections.• Section 2:<ul style="list-style-type: none">○ Updated all configuration screen shots and CLI commands for PAN-OS 5.0 from PAN-OS 4.0.○ Updated virtual wire references to new features such as NAT and virtual wire sub interfaces.○ Added some overview information for tcp-non-syn communications.○ Added link state to auto for virtual wire based on new feature in PAN-OS 5.0.○ Tested all configurations for PAN-OS 5.0.• Section 3.2 Example Scenario: Layer 2 Active/Passive HA section for the CLI updated the Interface mode and Policy configuration.• Section 3.3, Create a NAT policy step updated screenshot as well as the CLI Configuration section.
2/3/12	A	Initial release of this document.