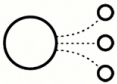
CONNECTING THE FIREWALL TO PRODUCTION NETWORKS WITH SECURITY ZONES



NETWORK CONNECTIVITY IS NOT A LUXURY, IT IS A NECESSITY

- Security Zones Overview
- Network interfaces and security zones
- Interfaces Types
- Virtual routers and Layer 3 interfaces

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

Learning Objectives

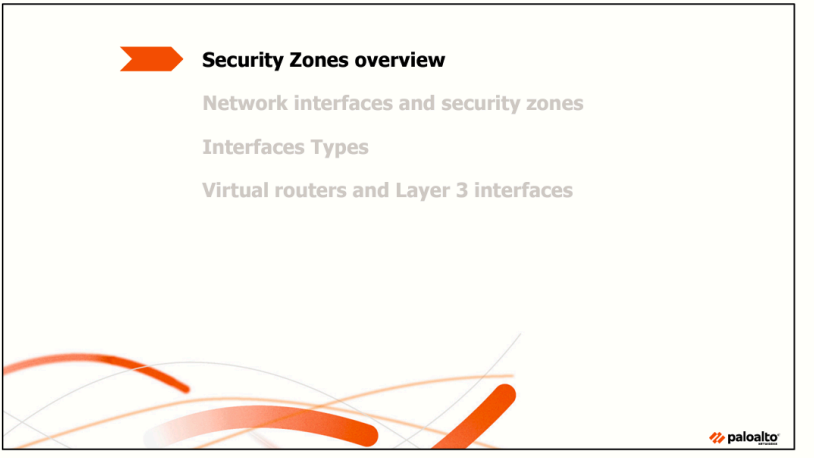
After you complete this module, you should be able to:

- Describe firewall network segmentation components used to block threats
- Configure firewall security zones to implement network segmentation
- Configure tap interfaces to collect network traffic for later analysis
- Configure virtual wire interfaces to control network traffic traversing between two firewall interfaces
- Configure Layer 3 interfaces to control network traffic traversing Layer 3 networks
- Configure a virtual router to support Layer 3 interfaces

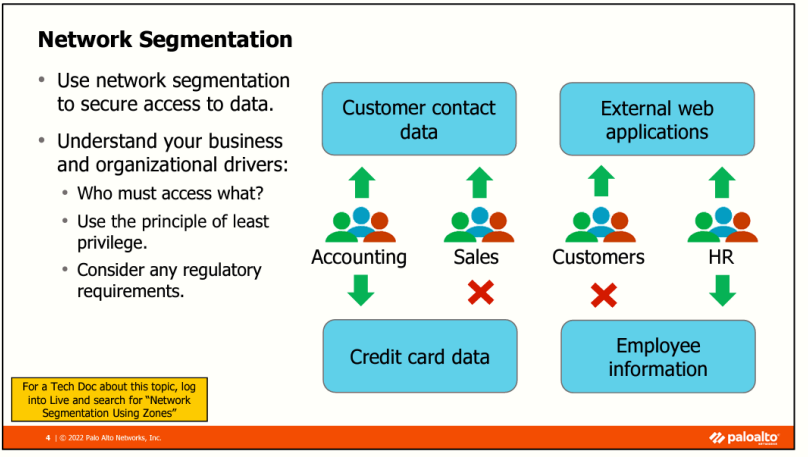
This module covers the topics listed here. Read through the list before proceeding.

After you complete this module, you should be able to:

- Describe firewall network segmentation components used to block threats
- Configure firewall security zones to implement network segmentation
- Configure tap interfaces to collect network traffic for later analysis
- Configure virtual wire interfaces to control network traffic traversing between two firewall interfaces
- Configure Layer 3 interfaces to control network traffic traversing Layer 3 networks
- Configure a virtual router to support Layer 3 interfaces



This section introduces how to block threats by using network segmentation.

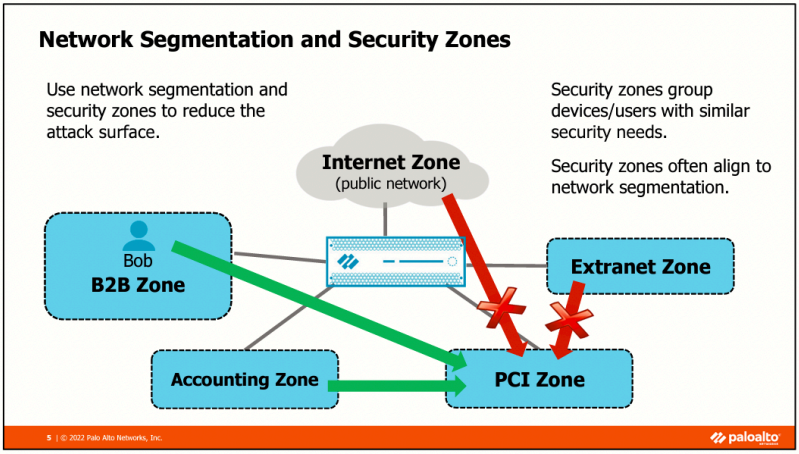


Use network segmentation to secure access to data. Network segmentation divides the network into multiple areas or zones, each protected by a firewall that controls access to the data and resources in that area. Network segmentation helps prevent attackers from accessing critical resources if they compromise one network area.

Before securely segmenting your network, you must first understand how various departments and users interact with applications and data. Network security must support and not hinder the business. It would help consider how the loss or compromise of data might affect your business. For example, business-critical data should reside in the most protected network segments.

Your user-to-data access requirements are a primary factor in how you decide to segment your network to meet your security requirements. Apply the principle of least privilege when segmenting your network. For example, a third-party vendor might need access to some resources in your network, but it most likely does not need access to all resources.

Another segmentation factor will be any data security regulations or standards that apply to your business. Such measures include requirements concerning data location and access. Failure to adhere to these requirements can result in data loss, fines, diminished customer confidence, or even the loss of the business.



Palo Alto Networks firewalls use the concept of security zones to secure and manage your networks. Security zones are a logical way to group physical and virtual interfaces on the firewall to control and log the traffic that travels across specific interfaces on your network. Systems with similar security needs are grouped into zones. The more granular you make your zones and the corresponding Security policy rules that control traffic between zones, the more you reduce your organization's attack surface. This reduction is possible because the smaller you make each zone, the greater the control over the traffic that accesses each zone and the more difficulty the malware has in moving laterally between zones.

For example, you might want to segment your network to control access to the database servers that store your consumer credit card data. Configure your database servers into a zone called PCI. Then define a Security policy rule that permits access to the PCI zone from only users in the Accounting zone and from only a single user named Bob in the B2B zone. If there is no Security policy rule to allow access, other users in the B2B zone or users in the Extranet or Internet zones cannot access the credit card data in the PCI zone.

Configure Security Policy to Support Segmentation

Policies > Security

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRE...	Destination DEVICE	APPLICATION	SERVICE	ACTION
1	B2B-PCI-Access	B2B	universal	B2B	any	Bob	any	PCI	any	any	mssql-db	application-default	Allow
2	Acct-PCI-Access	Accounting	universal	Accounting	any	Accounting_Grp	any	PCI	any	any	mssql-db	application-default	Allow
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
4	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

- Create a Security policy rule to allow required interzone traffic:
  - *Bob* in the *B2B* zone is allowed to access the *PCI* zone.
  - The *Accounting-Grp* in the *Accounting* zone is allowed to access the *PCI* zone.
- Any other interzone traffic is blocked, by default.

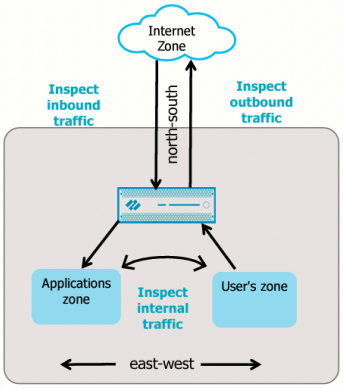
After you have segmented your network and grouped your network nodes into security zones, configure firewall Security policy rules to control network access between zones. Policy rules on the firewall use security zones to identify where the traffic comes from and where it is going. Traffic can flow freely within a zone, but traffic cannot flow between different zones until you define a Security policy rule that allows it.

The example Security policy is based on a previous illustration in this module. Rule 1 allows only *Eob* in the *B2B* zone to access the database application in the *PCI* zone. Rule 2 allows only members of the *Accounting-Grp* in the *Accounting* zone to access the database servers in the *PCI* zone. This configuration reduces the attack surface of the *PCI* zone.

Because the Security policy rules include a username and a group name as match criteria, you must enable and configure User-ID on the *B2B* and *Accounting* zones.

Zero Trust Architecture

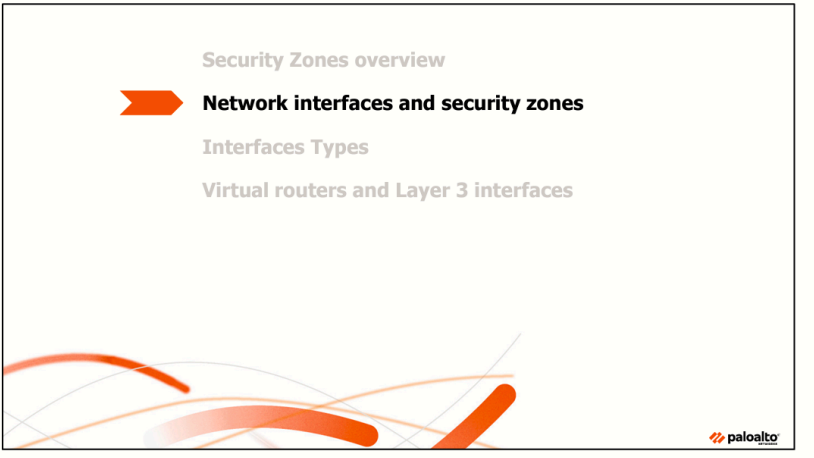
- Never trust, always verify.
- Inspect perimeter traffic:
  - Inbound traffic
  - Outbound traffic
- Also inspect internal traffic.



For a Tech Doc about this topic, log into Live and search for "What is Zero Trust Architecture"

The Zero Trust architecture remedies the deficiencies of the perimeter-only architecture. Zero Trust is based on the principle "never trust, always verify" rather than on the principle "trust but verify." After you segment your network, using subnets or VLANs, use firewalls and security zones to control traffic between network segments. A security zone is a grouping of physical or virtual interfaces representing a segment of your network connected to and controlled by the firewall.

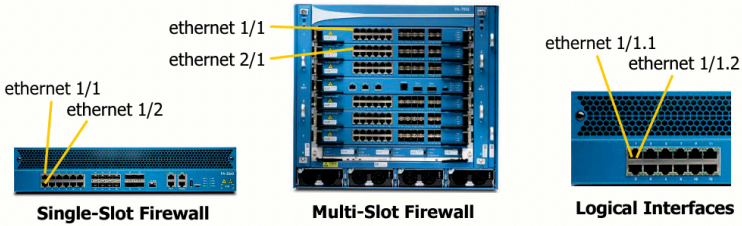
In complex network architectures, you can simplify traffic flows to inbound traffic from the internet, outbound traffic to the internet, and internal traffic between nodes in your data center. You accomplish inbound and outbound inspection by locating a firewall between your internal network segments and the internet. You achieve an internal traffic inspection by locating a firewall between your internal subnets and VLANs.



This section introduces the concept of security zones, which are used to segment your network for security reasons. This section also describes the purpose and configuration of various network interface types that enable a firewall to connect to a variety of network types.

Network Interfaces

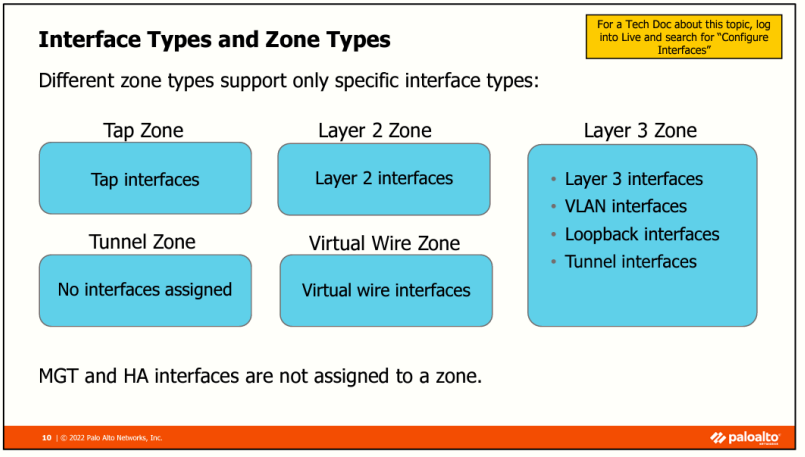
- The firewall data plane controls *in-band* network interfaces.
- Each interface is assigned to a single zone.
- A zone can include multiple physical or logical interfaces.



All firewall models include *in-band* interfaces used to control network traffic flowing across an enterprise. These interfaces are labeled in the web interface using the format "ethernet *n*/*n*." On a single-slot firewall, the first *n* is always 1, and the second *n* represents the number assigned to the in-band port. On a multi-slot firewall, the first *n* represents the slot number, and the second n represents the number assigned to the in-band port in that slot.

Each firewall interface supports multiple logical interfaces, called subinterfaces, in the web interface. Subinterfaces can be used to support VLANs, for example.

A physical port or a subinterface can be assigned to only a single security zone. However, a zone can contain multiple physical or logical interfaces.



You can use numerous methods to integrate Palo Alto Networks firewalls into your environment. Many deployments evolve and will transition from one configuration to another.

To support a wide variety of deployment options, PAN-OS® software includes different zone types and interface types. Each zone type supports specific interface types. The five-zone types and the interface types they support are illustrated here. Different zone and interface types can be used simultaneously on the same firewall if used on other physical firewall interfaces.

Notice that a Layer 3 zone supports several interface types. All these interface types are assigned IP addresses.

Tunnel zones became available starting in PAN-OS 8.0. They are used in a tunnel content inspection feature, specifically for a scenario involving tunnel-in-tunnel encapsulation. Tunnel zones are not described in this module. For more information about tunnel zones, log into Live and search for PAN-OS admin guide or see *PAN-OS 10.2 Administrator's Guide* at https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin.html.

HA interfaces are different from the other interface types because they do not control regular application traffic. HA interfaces are used to synchronize a pair of firewalls deployed in a high availability configuration. They are not placed in a security zone because they do not control regular network traffic.

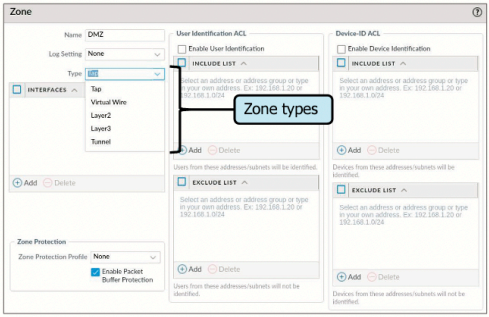
The MGT interface is used only for firewall management and is not assigned to a zone.

This module describes the purpose and configuration of the tap, virtual wire, Layer 2, and Layer 3 zone types, and the most common interface types.

Create a Security Zone

For a Tech Doc about this topic, log into Live and search for "Building Blocks of Security Zones"

Network > Zones > Add



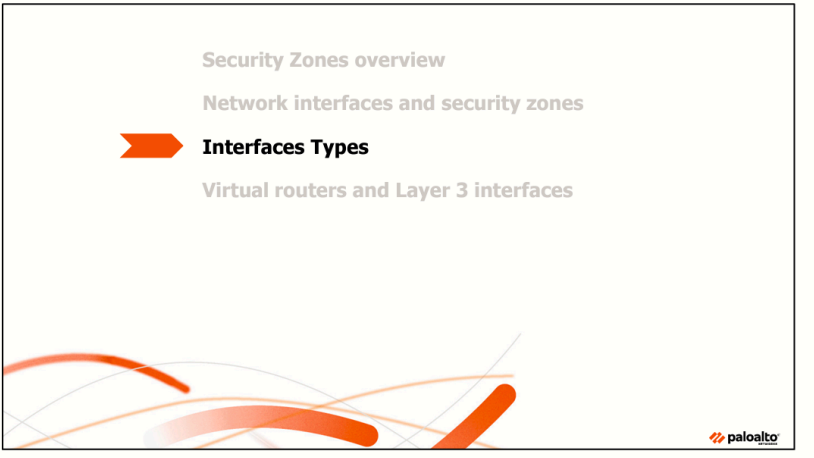
- Specify zone **Name**.
- Specify zone **Type**.
- Assign **Interfaces**:
  - Must be appropriate type.
  - Unassigned interfaces do not process traffic.

11 | © 2022 Palo Alto Networks, Inc.

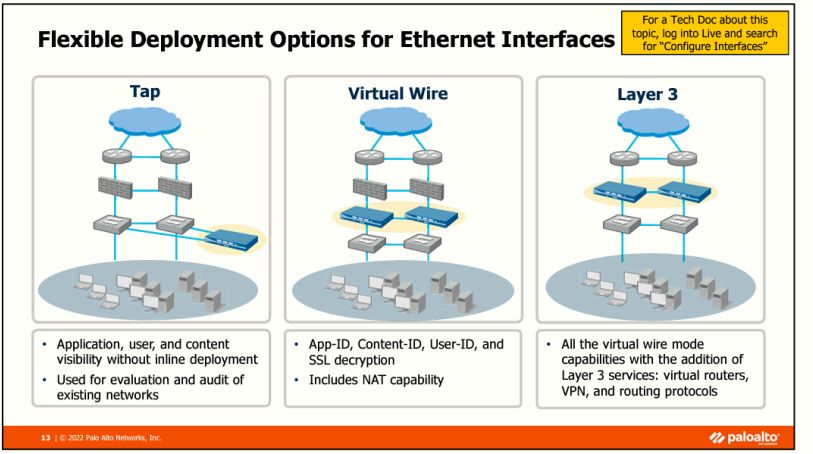
Because Security policy rules use zones to control and log traffic, one of the first tasks to perform is to create your zones by naming the zone and specifying the zone type. If interfaces of the appropriate type already have been configured, you can assign them to the zone. However, you can add interfaces to the zone later. Interfaces not assigned to a zone do not process traffic. Each interface can be assigned only to a single zone.

The zone name is case-sensitive. For example, DMZ and dmz would not be the same zone.

The five primary zone types are shown in the example: **Tap**, **Virtual Wire**, **Layer2**, **Layer3**, and **Tunnel**. A sixth zone type, external, is a special zone available only on some firewall models. The external zone allows traffic to pass between virtual systems when multiple virtual systems are configured on the same firewall. Virtual systems are supported only on the PA-3n00, PA-5n00, and PA-7000 Series firewalls. The **External** zone type is visible in the drop-down list only when a firewall with the virtual systems supports it feature enabled.



This section introduces tap interfaces. It describes what they are, what they are used for, and how to configure them.



You can use numerous methods to integrate Palo Alto Networks firewalls into your environment. Many deployments evolve, transitioning between some or all of these possible configurations. Palo Alto Networks firewalls support multiple interface types. The three most common implementations are illustrated here.

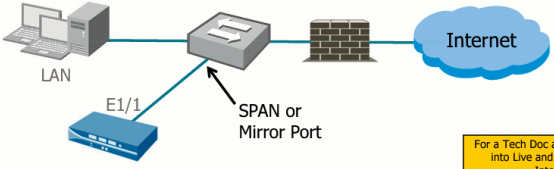
A brief overview of tap, virtual wire, and Layer 3 features follows:

- Tap: With tap interfaces, the firewall can be connected to a core switch's switch port analyzer (or SPAN) or mirror port to identify applications running on the network. This option requires no changes to the existing network design. In this mode, the firewall cannot block any traffic.
- Virtual wire: With virtual wire interfaces, the firewall can be inserted into an existing topology without requiring any re-allocation of network addresses or redesign on the network topology. In this mode, all the protection and decryption features of the device can be used. NAT functionality is provided in this mode.
- Layer 3: With Layer 3 interfaces, the firewall can replace any current enterprise firewall deployment.

A unique advantage is your ability to mix and match these interface types on a single device. For example, the same firewall can be deployed in tap mode for one portion of the network and virtual wire or Layer 3 mode for another.

Tap Interfaces

- Enable passive monitoring of switch traffic from a SPAN or mirror port
- Cannot control traffic or perform traffic shaping
- Must be assigned to a tap zone
- Use Traffic log information to configure Security policy rules



For a Tech Doc about this topic, log into Live and search for "Tap Interfaces"

You can use a tap interface to monitor traffic on a port. The firewall can use a tap interface to connect to a switch's SPAN or mirror port. Once connected to the switch, a tap interface passively collects and logs monitored traffic to the firewall's Traffic log. Tap mode deployment is often used to discover the application types and user traffic flowing across a network. An administrator can use the information recorded in the Traffic log to help configure appropriate Security policy rules to control traffic.

Because traffic is flowing to the firewall but is not flowing through the firewall, a tap interface cannot be used by a firewall to control traffic or perform traffic shaping.

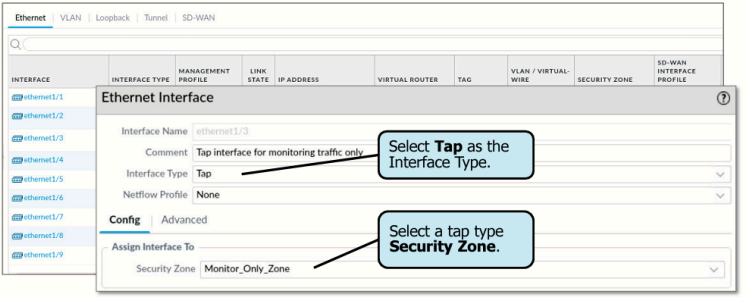
An advantage of using a tap interface to monitor network traffic flowing through a switch is that it does not require any network address changes.

If the SPAN or mirror port passes encrypted traffic, the tap interface supports only SSL inbound decryption. Decryption, including SSL inbound decryption, is described in another module.

Even though a firewall does not block traffic flowing into a tap interface, the firewall can still thoroughly identify the traffic. You can configure the firewall to perform App-ID, Content-ID, User-ID, and SSL inbound decryption. All these features are described in other modules.

Configure a Tap Interface

Network > Interfaces > Ethernet > <select_interface>



15 | © 2022 Palo Alto Networks, Inc.

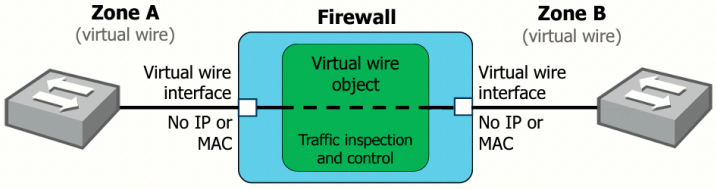
Even though a tap interface does not relay traffic as do the other interface types, you still must assign it to a zone. The zone that you assign the interface to must be a tap-type zone. You must assign the tap interface to a zone because Security policy rules are required to log network traffic, and Security policy rules require zones to process network traffic. To enable logging, you must configure a Security policy rule with the source and destination zones set to the zone that contains the tap interface.

The **Security Zone** drop-down list will list only zones of the type tap.

Virtual Wire Interfaces

For a Tech Doc about this topic, log into Live and search for "Virtual Wire Interfaces"

- Bind two firewall interfaces together through a virtual wire object
- Typically used when no switching or routing is needed
- No configuration changes for adjacent network devices



A virtual wire deployment binds two firewall interfaces together, allowing for all traffic to pass between the interfaces. It also is called a "bump in the wire" or transparent inline deployment. No MAC or IP address is assigned to either virtual wire interface. A virtual wire configuration is typically used when no switching or routing is required. A virtual wire requires no configuration changes for adjacent network devices, which means that you can insert the firewall into an existing topology without requiring any re-allocation of network addresses or redesign on the network topology.

A virtual wire configuration is defined in two steps: creating the virtual wire object and configuring the virtual wire interfaces that the object connects. You can perform these steps in any order. The virtual wire object provides the data path between the two virtual wire interfaces.

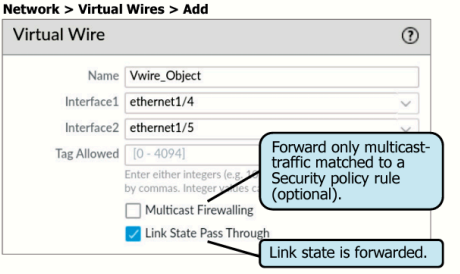
All firewalls shipped from the factory have Ethernet ports 1 and 2 preconfigured as virtual wire interfaces, and these interfaces allow all untagged traffic.

Network traffic flows through a firewall in a virtual wire, which means that the firewall can examine, traffic-shape, and block traffic. On the virtual wire, you can configure the firewall to perform App-ID, Content-ID, NAT, QoS, SSL decryption, and User-ID. All of these features except QoS are described in other modules.

A virtual wire does not support routing or firewall management traffic because no IP address is assigned to a virtual wire interface. A virtual wire cannot function as a termination point for an IPsec VPN tunnel.

Configure a Virtual Wire Object

- A virtual wire object connects to virtual wire interfaces.
- A virtual wire can accept traffic based on 802.1Q VLAN tags:
  - 0 = untagged traffic

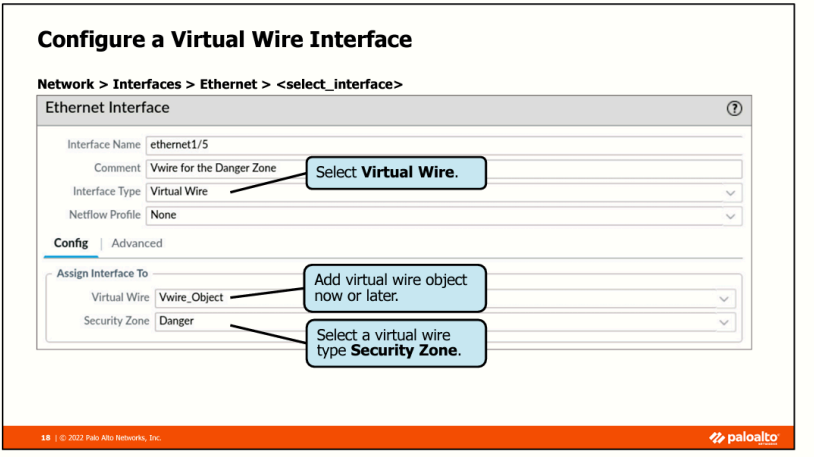


You must create a virtual wire object that connects the two virtual wire interfaces. A virtual wire interface must always connect two interfaces. If the virtual wire interfaces have not yet been configured, the interface fields can be left blank until the interfaces exist. Only interfaces configured as virtual wire interfaces appear on the interface drop-down lists.

A virtual wire object can block or allow traffic based on 802.1Q VLAN tag values. You can specify tag numbers in the range 0 to 4094. A tag value of 0 represents untagged traffic, and the firewall will pass untagged traffic allowed by a Security policy rule.

By default, all multicast traffic is passed through the virtual wire. Select the Multicast Firewalling check box to alter this behavior and apply Security policy rules to multicast traffic.

The link state of the devices on each side of the virtual wire is passed through the firewall because the **Link State Pass Through** field is pre-selected by default.



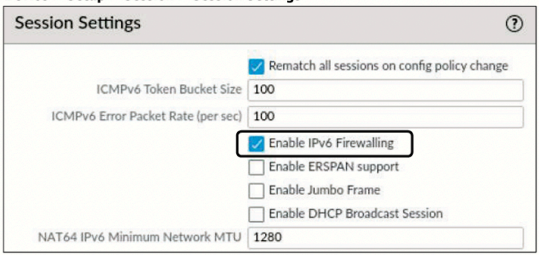
You must configure the virtual wire interfaces that the virtual wire object will connect. Choose an interface and select **Virtual Wire** from the **Interface Type** drop-down list. If the virtual wire object has not been configured, the **Virtual Wire** field can be left blank. The interface names can be specified when you create the virtual wire object.

A zone is required for each virtual wire interface because firewall Security policy rules are based on zones. Only zones of the type virtual wire will be listed on the **Security Zone** drop-down list.

Enable IPv4 and IPv6 Support

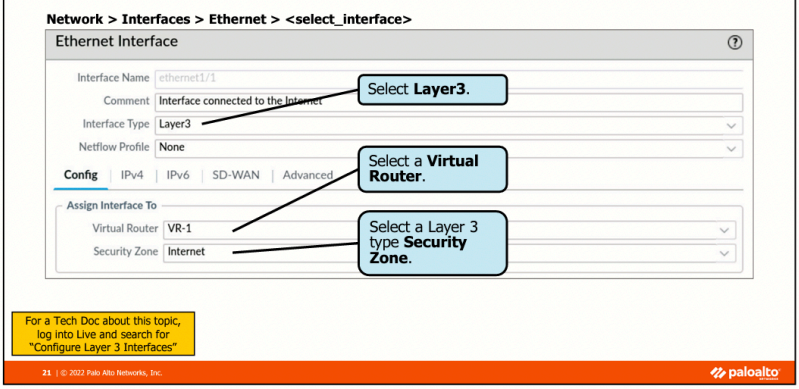
- Layer 3 interfaces support IPv4 and IPv6.
- To support IPv6 addresses, you must enable IPv6 on the firewall.

Device > Setup > Session > Session Settings



Layer 3 interfaces support both the IPv4 and the IPv6 protocols. These protocols can be deployed separately or in a dual-stack configuration. However, as shown here, before the firewall can support any feature that might use IPv6, including Layer 3 interfaces, you must enable IPv6 on the firewall.

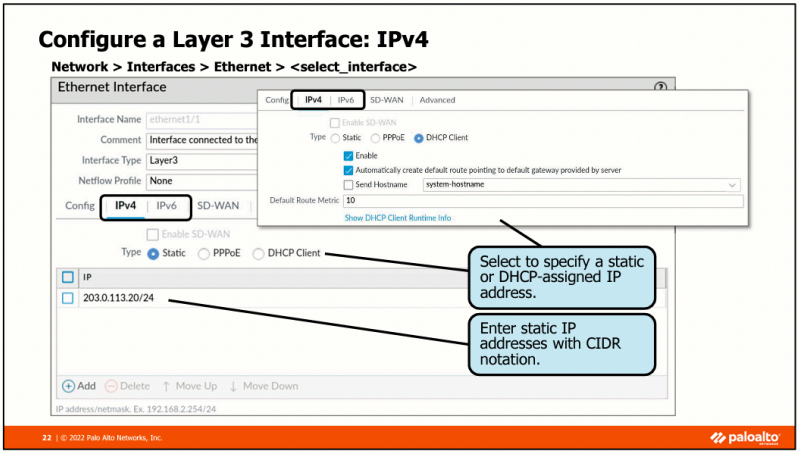
Configure a Layer 3 Interface: Config



To configure a Layer 3 interface, browse **Network > Interfaces > Ethernet** and select an interface. The minimum required properties for configuring a Layer 3 interface are **Interface Type**, **IP address**, and **Security Zone**.

Select the **Interface Type** of **Layer3**. If you want to route traffic to and from the interface, you will need to select a virtual router. If a virtual router has been configured on the firewall, select it from the **Virtual Router** drop-down list. A virtual router can be added later. All Layer 3 interfaces assigned to a specific virtual router share the same routing table.

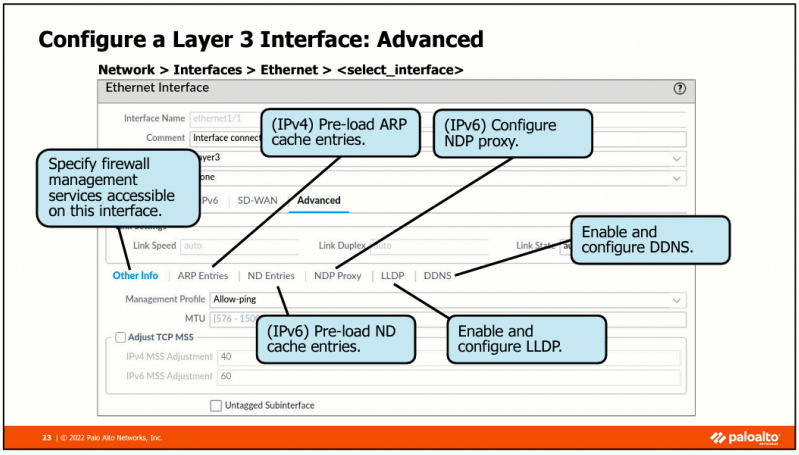
Finally, select a **Security Zone** from the drop-down list. Only zones configured as Layer 3 zones will appear on the drop-down list.



You can configure a Layer 3 interface with one or more static IPv4 addresses, IPv6 addresses, or as a DHCP client. To configure static IP addresses, select the **Static** radio button. You can assign multiple addresses to the same interface, although they should not be in the same subnet.

To configure an interface using DHCP, select the **DHCP Client** radio button. Configure an interface as a DHCP client for situations where the firewall must have a dynamically assigned IP address. Such cases might include the automatic deployment of a virtual firewall in a cloud environment. If the DHCP server provides a default route to the interface, you can configure the interface to propagate the default route to the interface's virtual router.

You can configure the firewall to be a Point-to-Point Protocol over Ethernet (or PPPoE) termination point to support a connection to a DSL modem.



The **Advanced** tab enables you to configure various Layer 3 interface settings. For example, you can modify each interface's link speed and duplex settings or change its MTU settings. Modifying the MTU settings here overrides the firewall's default jumbo frame and global MTU values configured in **Session Settings at Device > Setup > Session**. You also can adjust the TCP MSS to be a specified number of bytes less than the interface's MTU.

Use the **Management Profile** drop-down list to apply an Interface Management Profile to the interface. An Interface Management Profile defines the type of firewall management services accessible through the Layer 3 interface.

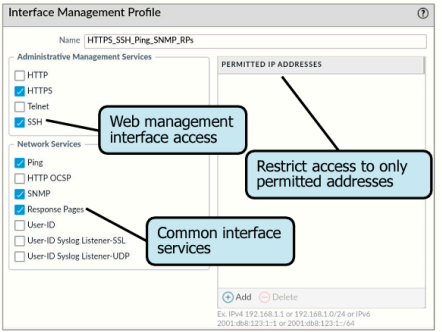
Use the **ARP Entries** tab to pre-load ARP table entries in the firewall's ARP cache or use the **ND Entries** tab to pre-load IPv6 Neighbor Discovery entries. If you need an IPv6 NDP proxy, the **NDP Proxy** tab lets you configure the interface as an NDP proxy that will respond to ND queries. This tab also enables you to configure the IPv6 addresses for which the NDP proxy will respond. Use the **LLDP** tab to enable LLDP on the interface and configure its behavior.

Use the **DDNS** tab to register the interface's IPv4 or IPv6 address changes with a dynamic DNS (or DDNS) service provider. The DDNS service automatically updates the domain name-to-IP address mappings to provide accurate IP addresses to DNS clients that will access the firewall and services behind the firewall. The firewall supports DDNS service providers DuckDNS, DynDNS, FreeDNS Afraid.org Dynamic API, and No-IP.

The **Untagged Subinterface** check box lets you create Layer 3 subinterfaces that are not assigned to a specific VLAN but carry untagged traffic. Layer 3 subinterfaces are described later in this module.

Interface Management Profile

Network > Network Profiles > Interface Mgmt > Add



- Defines which firewall management services are accessible from a traffic interface
- Can be applied to interfaces that support IP addresses:
  - Layer 3
  - Loopback
  - Tunnel

For a Tech Doc about this topic, log into Live and search for "Use Interface Management Profiles to Restrict Access"

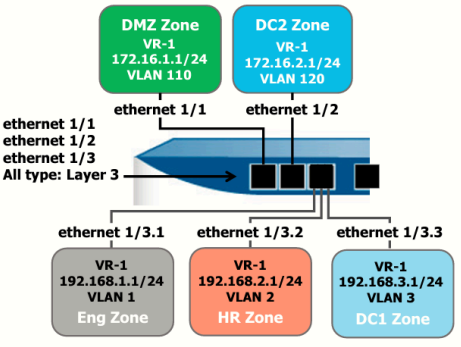
The out-of-band MGT port is designed to support firewall management functions and services by default. You can apply an Interface Management Profile to a Layer 3 interface to carry management traffic. An Interface Management Profile protects the firewall from unauthorized access by defining the protocols, services, and IP addresses that an in-band firewall interface permits for traffic to the firewall. Because a Layer 3 interface resides in a security zone, you must configure appropriate Security policy rules to allow the management traffic.

For example, you might want to prevent users from accessing the firewall web interface over the Layer 3 interface but allow that interface to receive ping queries from your network monitoring system. In this case, you would enable ping and disable HTTP/HTTPS. Ping will enable the firewall to respond to an ICMP echo request, which helps verify basic network connectivity to the interface. Response pages will allow a firewall to present information to users in response to their activity. For example, a response page might present an interactive web page to a user that asks them to verify a file transfer before the firewall allows the file transfer.

You can assign an Interface Management Profile to Layer 3 interfaces, subinterfaces, and logical interfaces such as VLAN, loopback, and tunnel interfaces. If you do not assign an Interface Management Profile to an interface, the firewall denies all firewall management services.

You can restrict management traffic enabled by a profile to one or more specific IP addresses by adding them to the **Permitted IP Addresses** field. If any permitted IP addresses are configured, only the listed IP addresses can access the selected functions and services. If the field is left blank, the profile allows any IP address to access the chosen functions and services, assuming that a Security policy rule does not block it.

Layer 3 Subinterfaces

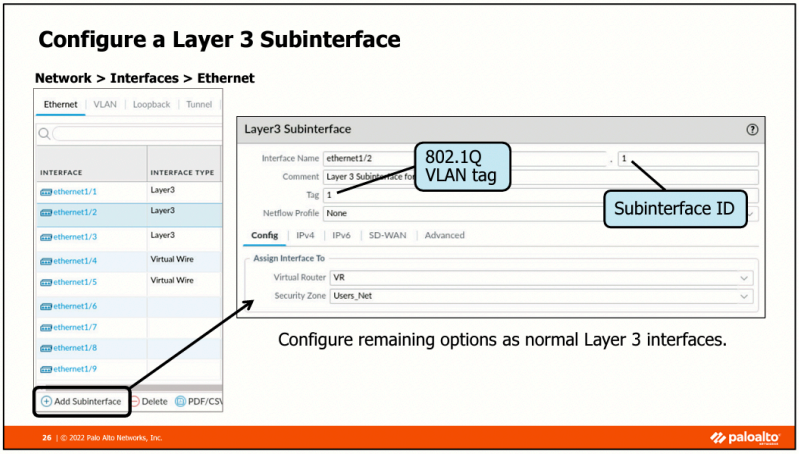


- Read and process traffic based on:
  - VLAN tags (1-4094)
  - VLAN tags and IP classifiers (source IP)
  - IP classifiers (untagged traffic, source IP)
- Common uses include:
  - More granular security rules
  - Logically splitting network traffic

For a Tech Doc about this topic, log into Live and search for "Layer 3 Subinterface"

paloalto

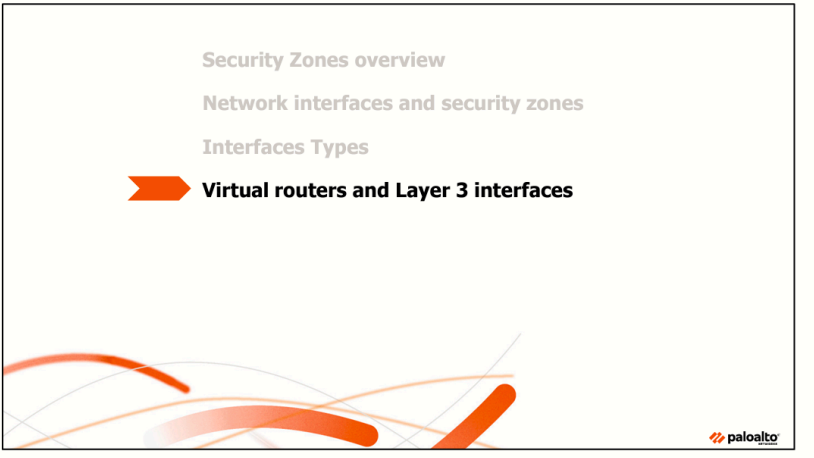
You can create Layer 3 subinterfaces and assign each subinterface to an 802.1Q VLAN. In this example, each VLAN is assigned to a unique zone. Traffic in different VLANs can share a common physical firewall port. However, traffic can be routed between one VLAN and another VLAN if a route exists between them in the routing table of the virtual router. Because Interzone traffic is blocked by default, you still need to configure Security policy rules to allow traffic to flow between different security zones.



To configure a Layer 3 subinterface, browse **Network > Interfaces > Ethernet** and select a Layer 3 interface. Then click **Add Subinterface**.

All the steps to configure Layer 3 interfaces apply to Layer 3 subinterfaces. The difference is your ability to assign a VLAN to a subinterface by entering a VLAN tag number in the **Tag** field.

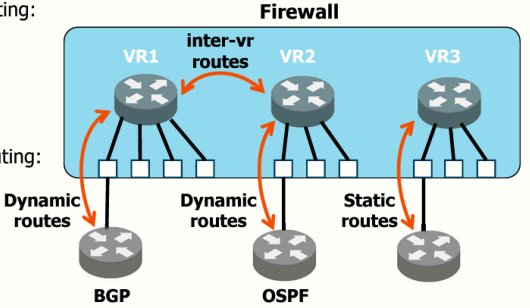
Untagged Layer 3 subinterfaces also can be used when the **Untagged Subinterface** option is enabled on the **Advanced** tab of the parent Layer 3 interface. Untagged subinterfaces are used in multi-tenant environments where traffic from each tenant must leave the firewall without VLAN tags. In this case, all traffic must be configured for source NAT, using the IP address of the untagged subinterface.



This section introduces virtual routers. It describes what they are, what they are used for, and how to configure them.

Virtual Routers

- Support one or more static routes
- Support dynamic routing:
  - BGPv4
  - OSPFv2
  - OSPFv3
  - RIPv2
- Support multicast routing:
  - PIM-SM
  - PIM-SSM

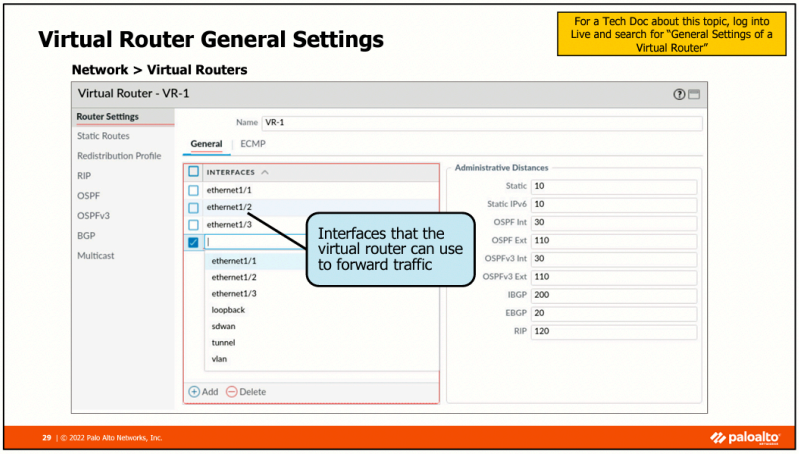


For a Tech Doc about this topic, log into Live and search for "Network > Virtual Routers"

A virtual router is a firewall function that participates in Layer 3 routing. The firewall uses virtual routers to obtain routes to other subnets by manually defining static routes or participating in one or more Layer 3 routing protocols (dynamic routes). The dynamic routing protocols supported on the firewall are BGP version 4, OSPF versions 2 and 3, and RIP version 2. The firewall supports Protocol Independent Multicast sparse mode (or PIM-SM) and PIM source-specific multicast (or PIM-SSM) for multicast routing. PIM version 2 is used for both multicast protocols. IGMPv1, v2, and v3 also are supported on host-facing interfaces.

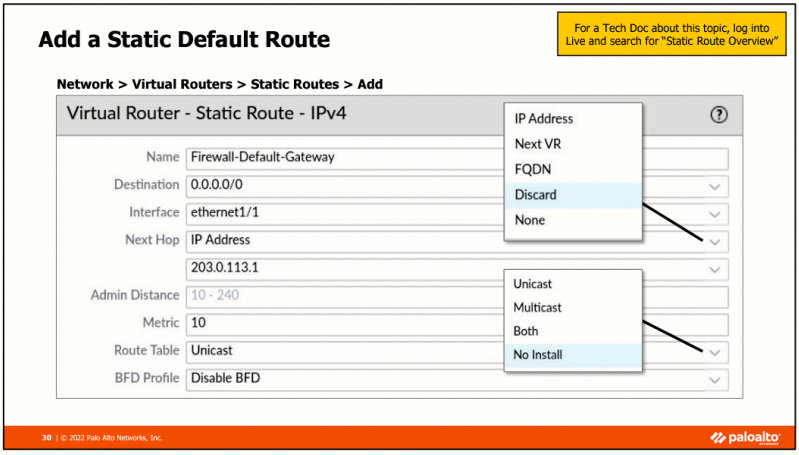
The routes that the firewall obtains through these methods populate the IP routing information base (RIB) on the firewall. When a packet is destined for a different subnet than the one it arrived on, the virtual router obtains the best route from the RIB, places it in the forwarding information base (FIB), and forwards the packet to the next-hop router defined in the FIB. The firewall uses Ethernet switching to reach other devices on the same IP subnet.

Virtual routers can also be linked so that traffic can be routed between them.



To configure a virtual router, browse to **Network > Virtual Routers**. Provide the virtual router with a unique name and then add one or more Layer 3, tunnel, or VLAN interfaces to the virtual router. After you add an interface, the interfaces-connected networks are automatically added to the virtual router's route table and can be used by the virtual router to forward traffic.

Set Administrative Distances for types of routes as required for your network. When the virtual router has two or more different ways to the same destination, it uses administrative distance to choose the best path from different routing protocols and static routes by preferring a lower distance. To display the installation default values or the acceptable ranges for each value, click the **help** icon (question mark icon) at the top right of the window.



Static routes are typically used in conjunction with dynamic routing protocols. You might configure a static route for a location that a dynamic routing protocol can not reach. Static routes require manual configuration on every router in the network, rather than the firewall entering dynamic routes in its route tables. A default route is a specific static route. When the virtual router has an incoming packet and finds no match for the packet's destination in its route table, the virtual router sends the packet to the default route. The default IPv4 route is 0.0.0.0/0; the default IPv6 route is::/0. You can configure both an IPv4 and IPv6 default route.

Browse to Network > Virtual Routers > Static Routes and click Add to add a static route. Enter the name for the static route. In the example, the static route is a default route, so the name chosen was default-route.

The destination address must include the netmask in CIDR notation. Select the firewall interface that will be used to forward packets that are assigned to the default route. You assign this interface to a security zone and define the Security policy rules that allow or block traffic for this zone.

The next-hop you choose can be a specific IP address or another virtual router. If you select **Discard**, the firewall discards traffic that matches the **Destination** address. This traffic would not appear in the Traffic log because it is discarded before a session is created. Select **None** if there is no next hop for the route.

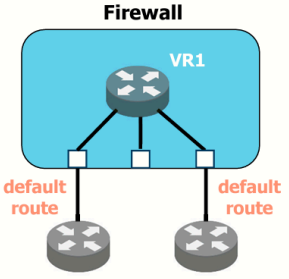
The **Admin Distance** field enables you to override the global administrative distance value configured on the **Router Settings** tab described on the previous page.

The **Metric** field helps the virtual router determine the best route to use when the same routing protocol offers multiple paths to the same destination. In this example, the metric value would help the router determine the best route between two static default routes if there were two static default routes.

You can select which route table to install the route into. You can install the entry in the **Unicast** or **Multicast** routing table, or **Both**. If you choose **No Install**, the route would be staged in the routing table, but the route would not be added to the forwarding table, so it would not be actively used.

A BFD Profile configures the firewall interface to use Bidirectional Forwarding Detection (or BFD). BFD is a vendor-independent mechanism used to detect a failed route between two interfaces. The firewall and the peer at the opposite end of the static route must support BFD sessions.

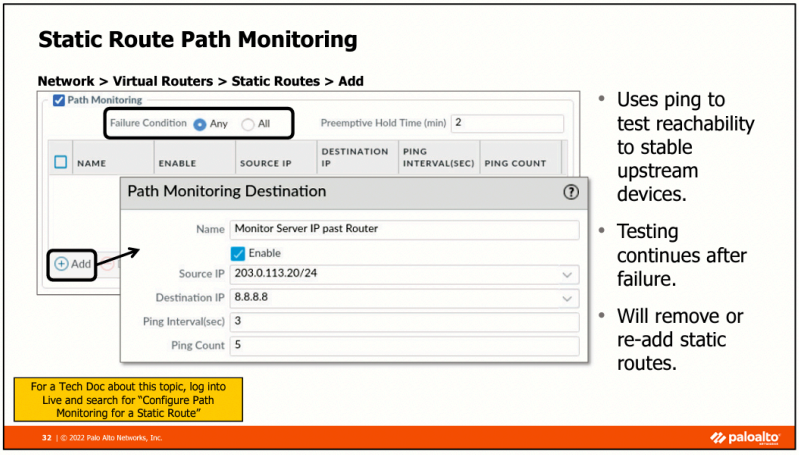
Multiple Static Default Routes



- Can configure multiple static default routes.
- Route with the lowest metric is used.
- Path monitoring determines if routes are usable.
- Firewall switches the default route during path failure.
- Supports failback.

You can configure multiple static default routes. By default, static routes have an administrative distance of 10. When the firewall has two or more routes to the same destination, it uses the route with the lowest administrative distance. Increasing the administrative distance of a static route to a value higher than a dynamic route allows you to use the static route as a backup route if the dynamic route is unavailable.

The firewall uses static route path monitoring to determine whether a static route is functioning. The firewall uses path monitoring to detect when the path to one or more monitored destinations has gone down. If path monitoring determines that a route no longer is working, the firewall switches to the static default route with the higher metric. Before PAN-OS 8.0, only the failure of a physical firewall interface would cause a failover between two static routes. Path monitoring continues to monitor all paths, even after a failure. Path monitoring that detects that the static default route with the lower metric is available again will cause the firewall to switch back to that route path.



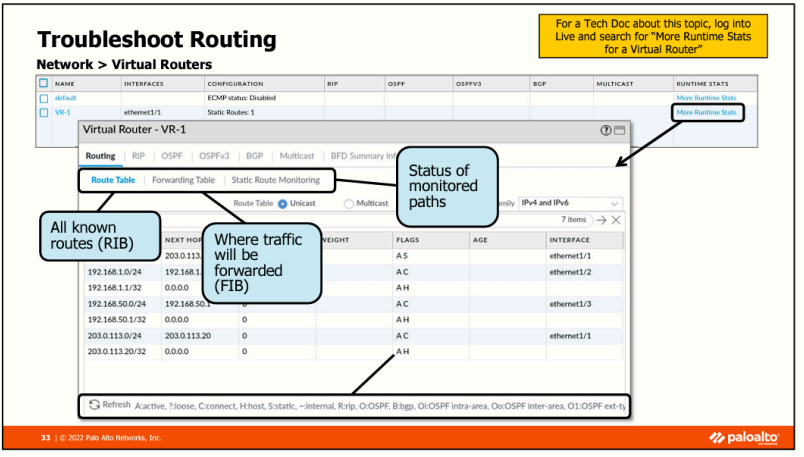
You can configure the firewall with path monitoring to remove static route table entries when a path failure occurs upstream from the firewall. To inform the firewall when a static route is down, use path monitoring to detect when the path to one or more monitored destinations no longer is reachable by ICMP pings. The firewall can then reroute traffic using an alternative route.

With firewall path monitoring:

- The firewall sends ICMP ping messages or heartbeat messages to one or more monitored destinations that you determine are robust and reflect the availability of the static route.
- If pings to any or all the monitored destinations become unreachable, the firewall considers the static route down and removes it from the routing information base (or RIB) and forwarding information base (or FIB). The firewall selects an alternative static route to the same destination (based on the route with the lowest metric) from the RIB and places it in the FIB.
- The firewall continues to monitor the failed route. The path monitor returns to the Up state when the monitored destination becomes reachable and the pre-emptive hold timer begins. If the path monitor remains in the Up state for the duration of the hold timer, then the firewall reinstates it into the RIB. The firewall then compares metrics of routes to the same destination to decide which route goes in the FIB.

To configure path monitoring, click the **Path Monitoring** check box and select a **Failure Condition**. **Any** condition means that a route path will be removed if at least one of the monitored paths fails. The **All** condition means that a route path will be removed only if all monitored paths fail.

Then enter a descriptive name for the path monitoring configuration and select the **Enable** check box. If the interface associated with the static route has multiple IP addresses, you can choose one for the **Source IP** address. By default, the first IP address assigned to the interface is chosen. Then select the **Destination IP** address of a stable device reachable through the default route. You also can adjust the default values for **Ping Interval** and **Ping Count**.



Click the **More Runtime Stats** link to display detailed information about a virtual router's current routing state and configuration.

The **Routing** tab contains three tabs: **Route Table**, **Forwarding Table**, and **Static Route Monitoring**. The **Route Table** tab displays the RIB that includes all currently known routes. The **Forwarding Table** tab displays the FIB derived from the RIB and contains the firewall interfaces and IP addresses presently used to forward all network traffic. The **Static Route Monitoring** tab displays the status of the monitor paths used to detail static route failures.

Module Summary

Now that you have completed this module, you should be able to:

- Describe firewall network segmentation components used to block threats
- Configure firewall security zones to implement network segmentation
- Configure tap interfaces to collect network traffic for later analysis
- Configure virtual wire interfaces to control network traffic traversing between two firewall interfaces
- Configure Layer 3 interfaces to control network traffic traversing Layer 3 networks
- Configure a virtual router to support Layer 3 interfaces

Now that you have completed the module, you should be able to perform the tasks listed.

Additional Resources

For a digital review of this module, log into Beacon and search for:

"Next-Generation Firewall Setup and Management Connection"

Review Questions

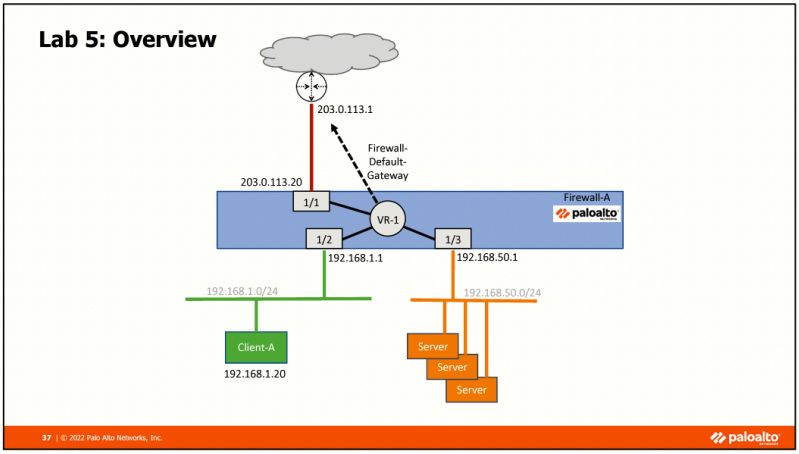
1. Which two items are supported routing protocols on a virtual router? (Choose two.)
   a. OSPF
   b. IGRP
   c. EGP
   d. BGP

2. Which three interface types are valid on a Palo Alto Networks firewall? (Choose three.)
   a. FC
   b. Layer3
   c. FCoE
   d. Tap
   e. Virtual wire

3. Which two firewall interface types can be added to a Layer3-type security zone? (Choose two.)
   a. Tunnel
   b. Virtual wire
   c. Tap
   d. Loopback

4. Which type of firewall interface enables passive monitoring of network traffic?
   a. Virtual wire
   b. Tap
   c. Loopback
   d. Tunnel

5. True or false? A Layer 3 interface can be configured as a dual-stack with IPv4 and IPv6 addresses.
   a. true
   b. false



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

Lab 5: Connecting the Firewall to Production Networks with Security Zones

- Load a baseline configuration
- Create Layer 3 interfaces
- Create a virtual router
- Segment your production network using security zones
- Test connectivity from firewall to hosts in each security zone
- Create Interface Management Profiles

Answers to Review Questions

1. a, d
2. b, d, e
3. a, d
4. b
5. a (true)