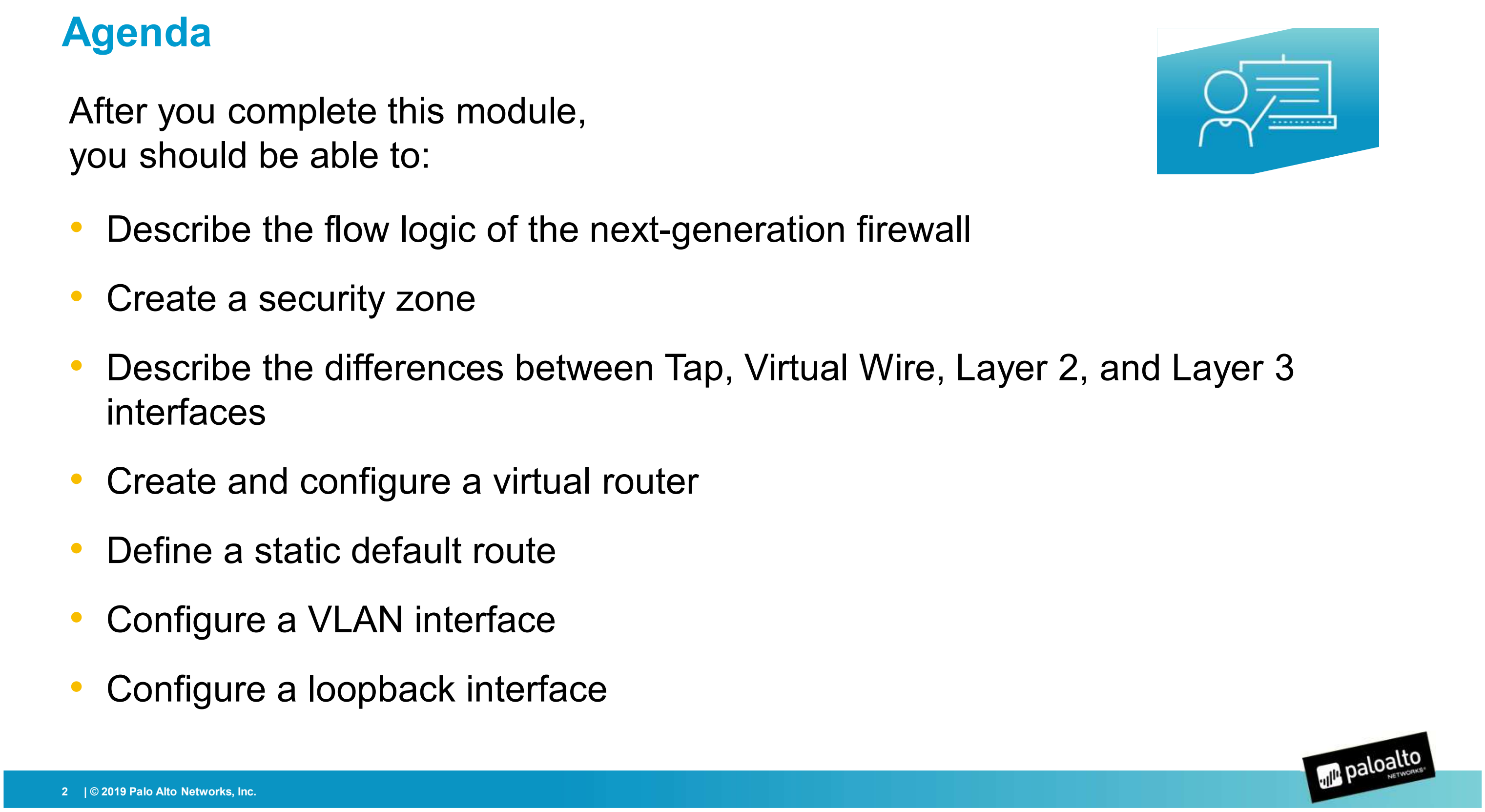
INTERFACE CONFIGURATION

EDU-210 Version A
PAN-OS® 9.0

DEPLOY TO MULTIPLE NETWORKS

- Security zones and interfaces
- Tap interfaces
- Virtual wire interfaces
- Layer 2 interfaces
- Layer 3 interfaces
- Virtual routers
- VLAN interfaces
- Loopback interfaces
- Policy-based forwarding



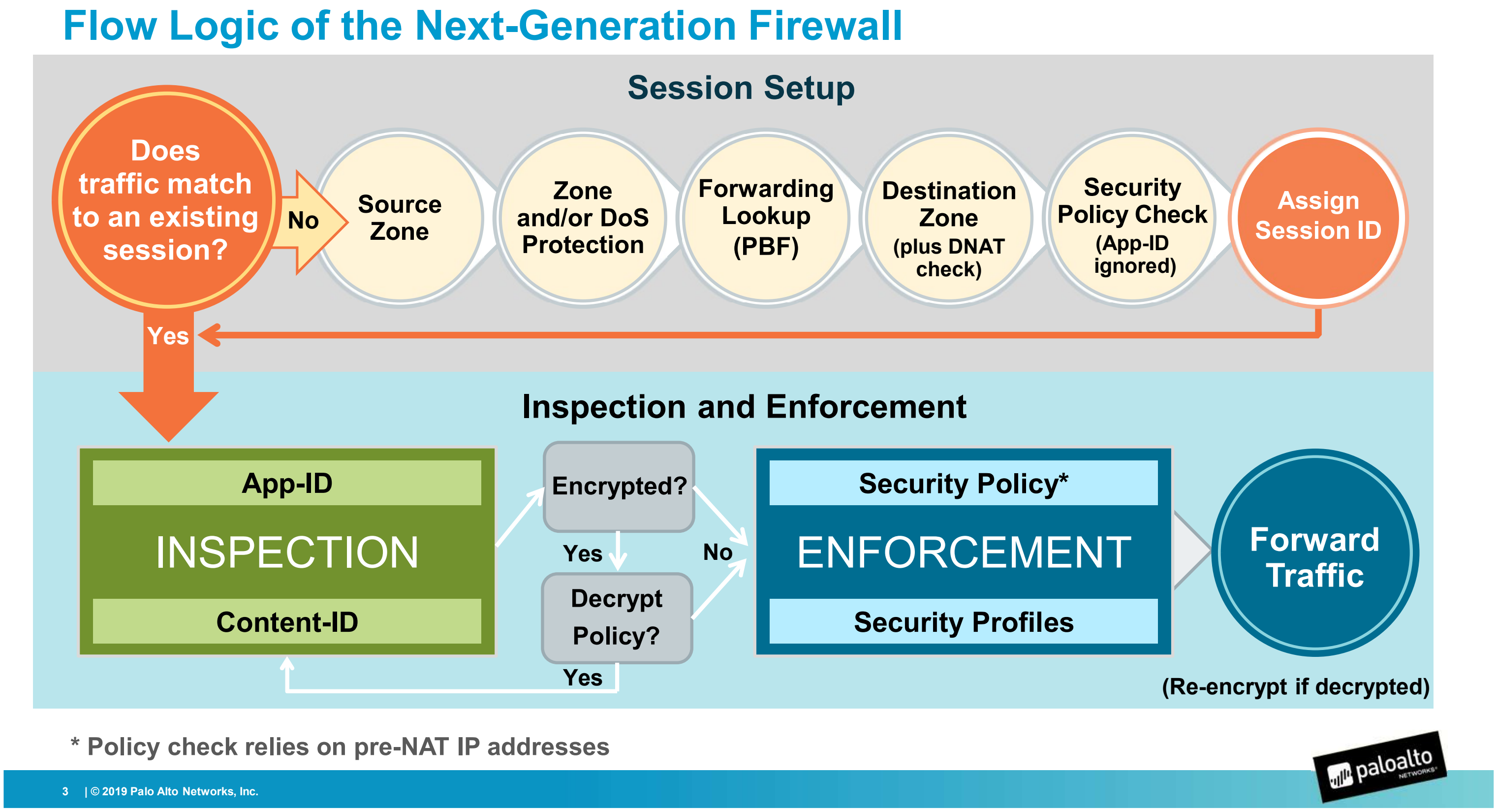
Agenda

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

- Describe the flow logic of the next-generation firewall
- Create a security zone
- Describe the differences between Tap, Virtual Wire, Layer 2, and Layer 3 interfaces
- Create and configure a virtual router
- Define a static default route
- Configure a VLAN interface
- Configure a loopback interface

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

- Describe the flow logic of the next-generation firewall
- Create a security zone
- Describe the differences between Tap, Virtual Wire, Layer 2, and Layer 3 interfaces
- Create and configure a virtual router
- Define a static default route
- Configure a VLAN interface
- Configure a loopback interface



Flow Logic of the Next-Generation Firewall

Session Setup

Does traffic match to an existing session?

No

Source Zone

Zone and/or DoS Protection

Forwarding Lookup (PBF)

Destination Zone (plus DNAT check)

Security Policy Check (App-ID ignored)

Assign Session ID

Yes

Inspection and Enforcement

App-ID

INSPECTION

Content-ID

Encrypted?

Yes

No

Decrypt Policy?

Yes

Security Policy*

ENFORCEMENT

Security Profiles

Forward Traffic

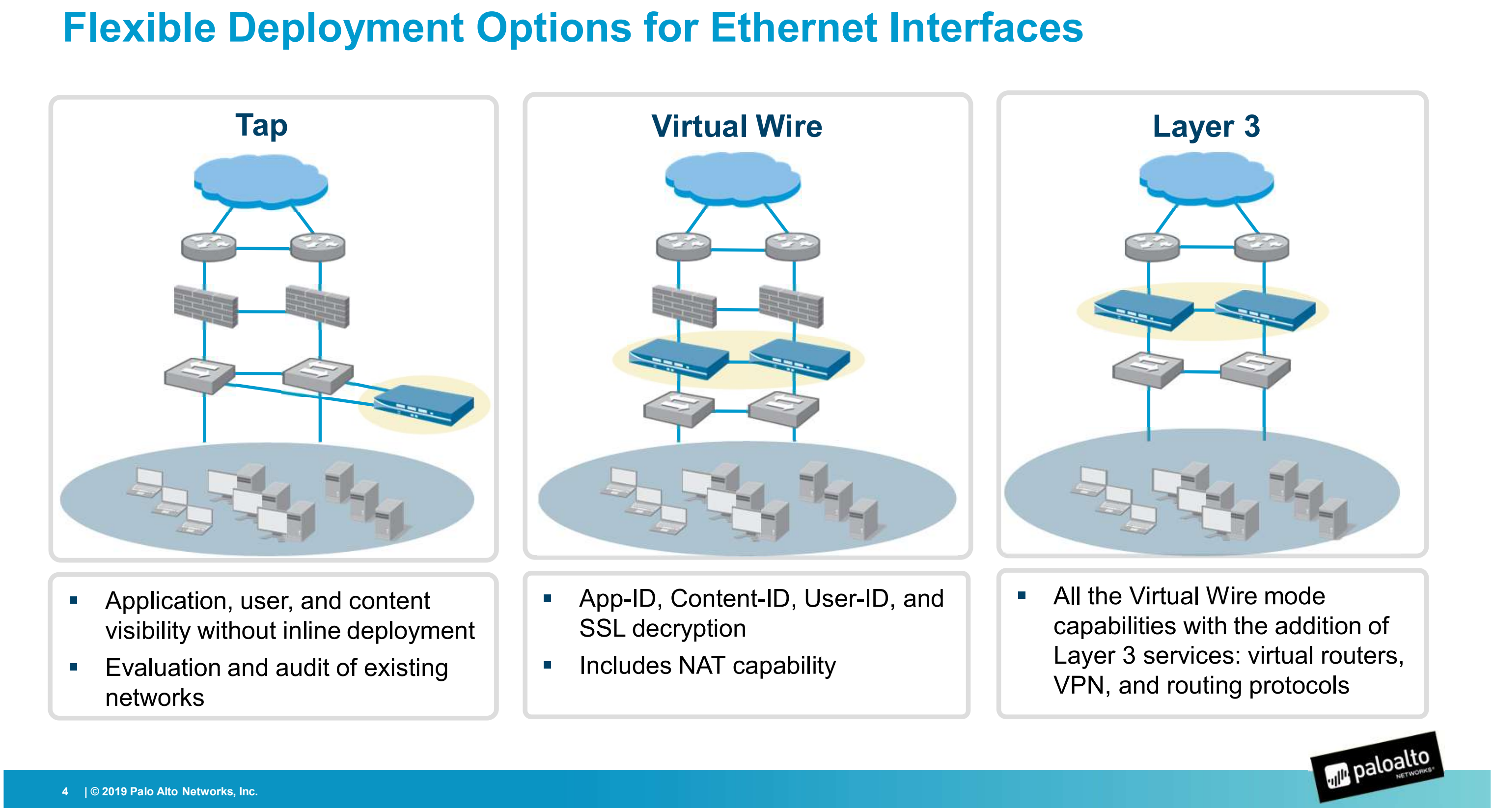
(Re-encrypt if decrypted)

* Policy check relies on pre-NAT IP addresses

3 | © 2019 Palo Alto Networks, Inc.

This diagram is a simplified version of the flow logic of a packet traveling through a Palo Alto Networks firewall.

For more information about the packet handling sequence inside of a PAN-OS® device, see the *Packet Flow Sequence in PAN-OS* document available on the Palo Alto Networks Support website at https://live.paloaltonetworks.com/docs/DOC-1628.



Flexible Deployment Options for Ethernet Interfaces

Tap

- Application, user, and content visibility without inline deployment
- Evaluation and audit of existing networks

Virtual Wire

- App-ID, Content-ID, User-ID, and SSL decryption
- Includes NAT capability

Layer 3

- All the Virtual Wire mode capabilities with the addition of Layer 3 services: virtual routers, VPN, and routing protocols

4 | © 2019 Palo Alto Networks, Inc.

You can use numerous methods to integrate Palo Alto Networks firewalls into your environment. Many implementations evolve over time, and they transition between some or all of these possible configurations. Three common deployments are illustrated here. Each deployment is described in more detail later in this module.

A brief overview of Tap, Virtual Wire, and Layer 2 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 reallocation 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 take the place of any current enterprise firewall deployment.

A unique advantage of the firewall 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 can be in Virtual Wire or Layer 3 mode for another.

Security zones and interfaces

Tap interfaces

Virtual wire interfaces

Layer 2 interfaces

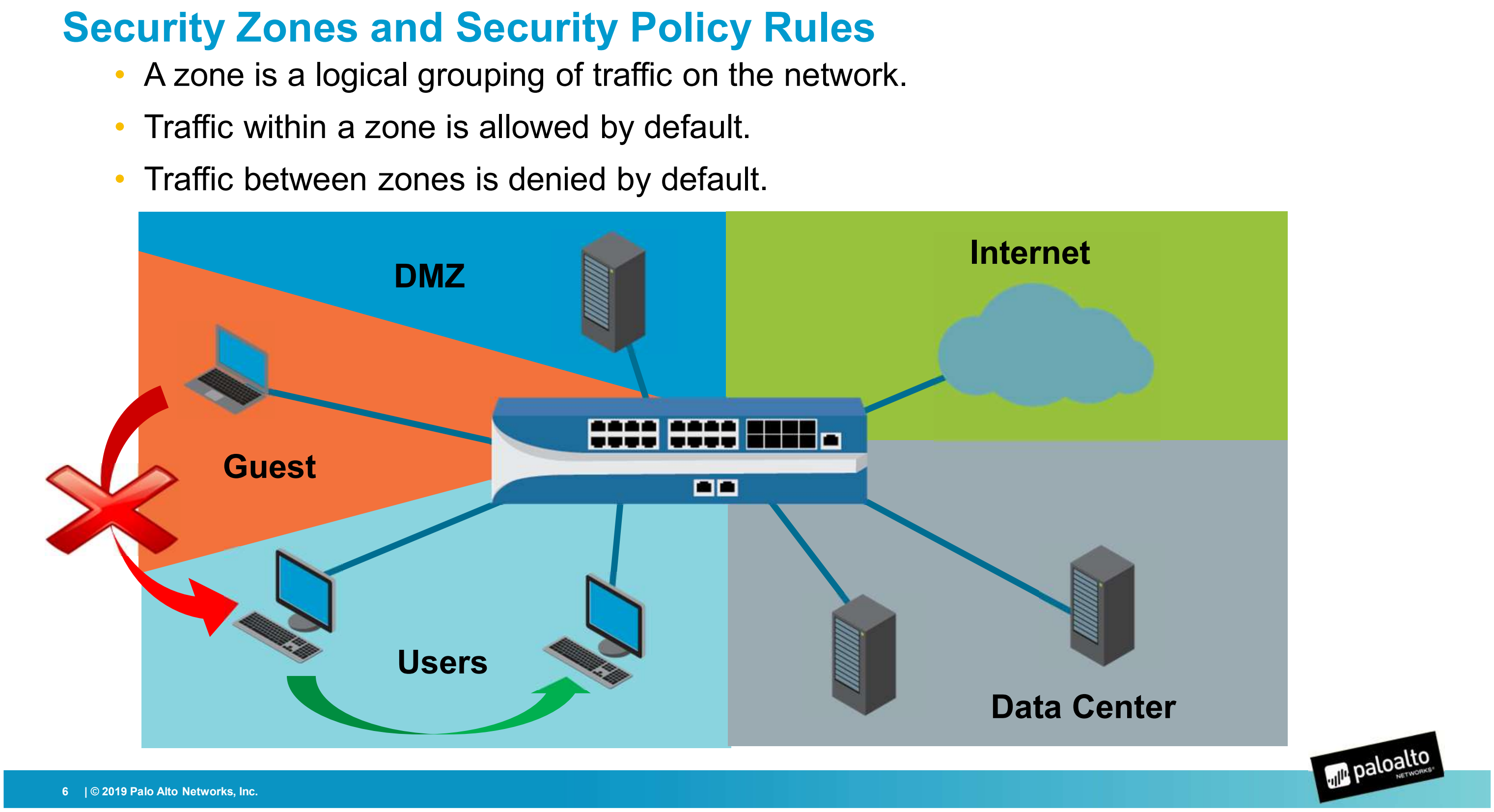
Layer 3 interfaces

Virtual routers

VLAN interfaces

Loopback interfaces

Policy-based forwarding



Security Zones and Security Policy Rules

- A zone is a logical grouping of traffic on the network.
- Traffic within a zone is allowed by default.
- Traffic between zones is denied by default.

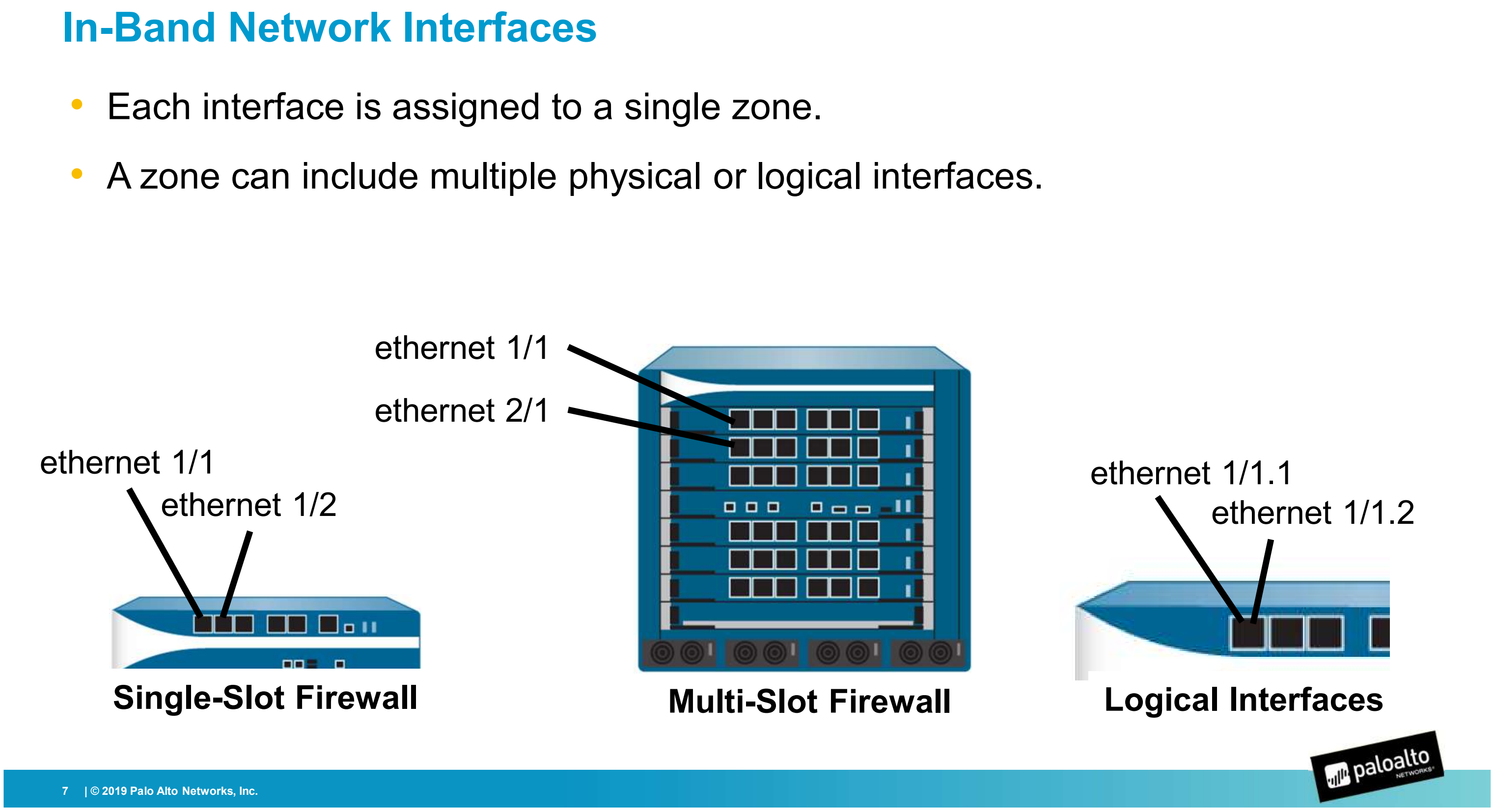
6 | © 2019 Palo Alto Networks, Inc.

Palo Alto Networks firewalls use the concept of security zones to secure and manage your networks. Systems with similar security needs are grouped into zones. For example, you would expect to see traffic initiated from the internet making connections into a DMZ network, but you would not expect to see internet traffic going into a data center network. To enforce this behavior, the DMZ network can be placed in one zone and the data center network can be placed in another zone. You can configure different firewall Security policy rules to control the traffic to and from each zone.

A zone is a logical grouping based on a particular type of traffic on your network. The physical location of a zone and its traffic is irrelevant. In fact, a single zone can reside at different locations throughout your enterprise.

Zone names have no predefined meaning or Security policy associations. You should choose descriptive zone names that help designate specific types of business functions, locations, or access privileges. In the example, the descriptive zone names are DMZ, Internet, Data Center, Users, and Guest.

By default, a PAN-OS Security policy allows intrazone traffic, which allows systems in the same zone to freely communicate with each other. However, interzone traffic is denied by default. For example, a server in the DMZ zone cannot communicate with a server in the Data Center zone unless you explicitly create a Security policy rule that allows communication. Security policy rules are described in another module.



In-Band Network Interfaces

- Each interface is assigned to a single zone.
- A zone can include multiple physical or logical interfaces.

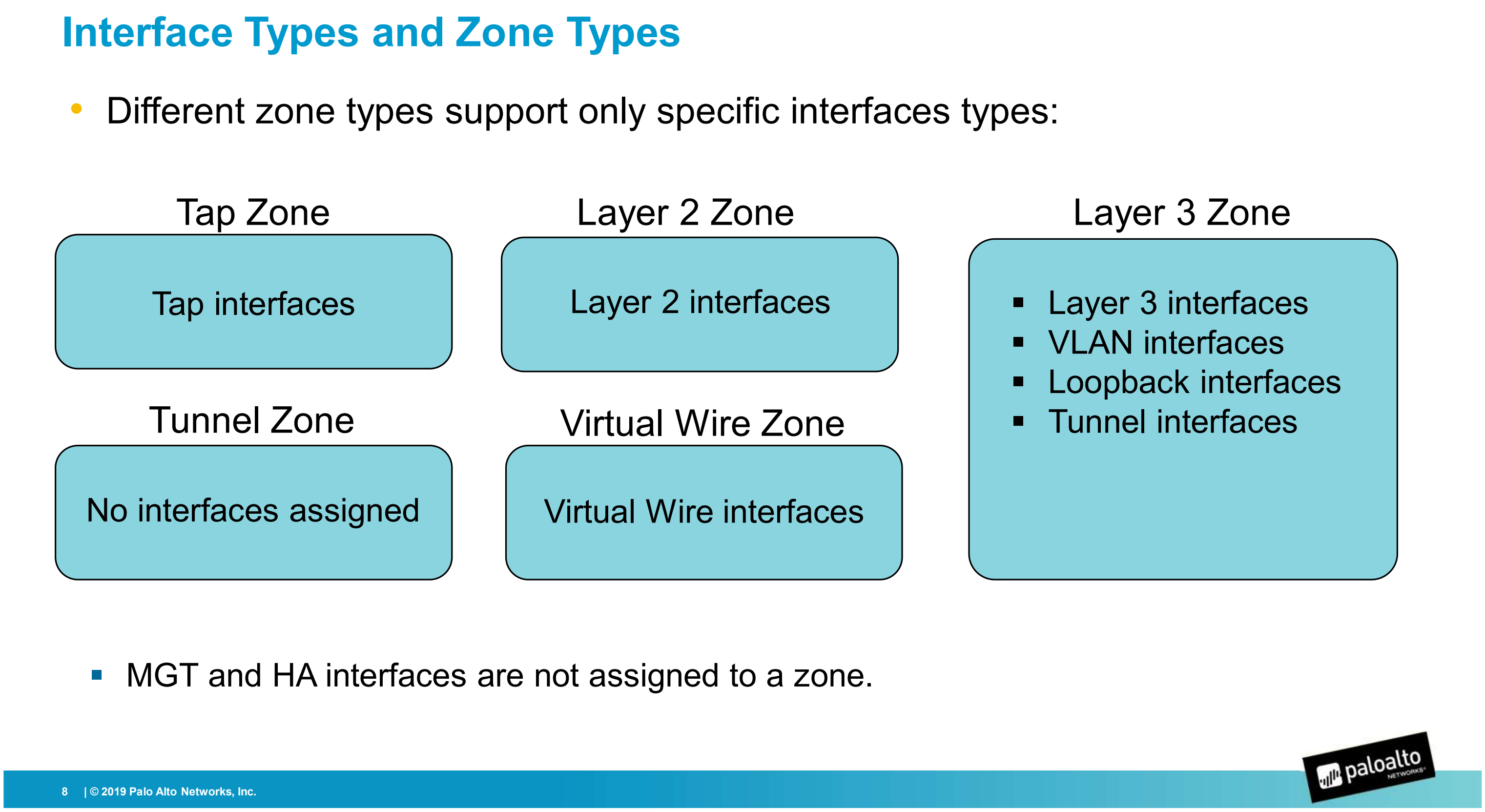
Single-Slot Firewall **Multi-Slot Firewall** **Logical Interfaces**

7 | © 2019 Palo Alto Networks, Inc.

All firewall models include in-band interfaces that are 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.



Interface Types and Zone Types

- Different zone types support only specific interfaces types:

Tap Zone

Tap interfaces

Layer 2 Zone

Layer 2 interfaces

Layer 3 Zone

- Layer 3 interfaces
- VLAN interfaces
- Loopback interfaces
- Tunnel interfaces

Tunnel Zone

No interfaces assigned

Virtual Wire Zone

Virtual Wire interfaces

- MGT and HA interfaces are not assigned to a zone.

8 | © 2019 Palo Alto Networks, Inc.

You can use numerous methods to integrate Palo Alto Networks firewalls into your environment. Many implementations 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 different physical firewall interfaces.

Notice that a Layer 3 zone supports a number of 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 feature named tunnel content inspection, and specifically for a particular scenario involving tunnel-in-tunnel encapsulation. Tunnel zones are not described in this module. For more information about tunnel zones, see the *PAN-OS 9.0 Administrator's Guide* at https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html.

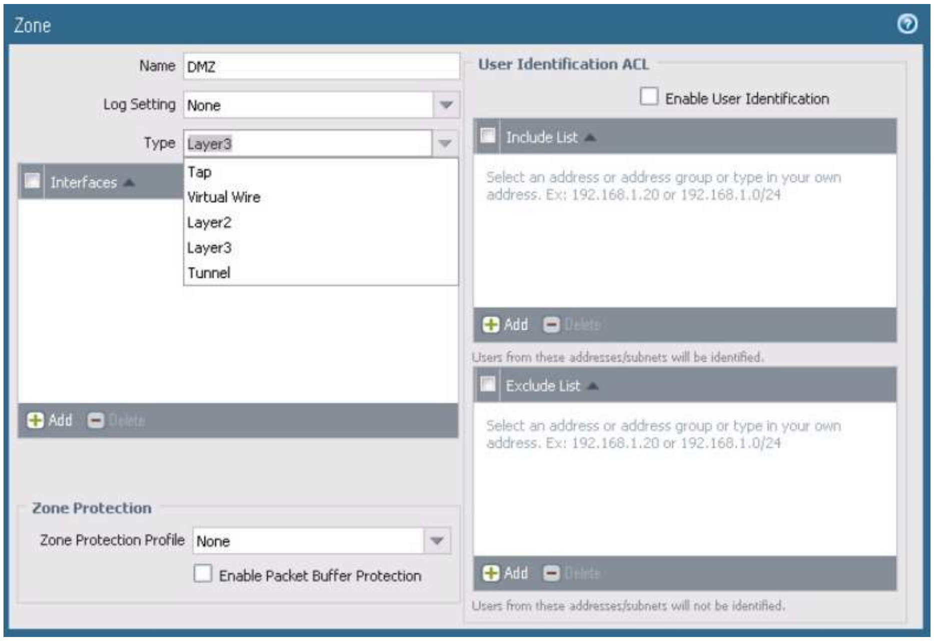
HA interfaces are different from the other interface types because they are not used to control normal network traffic. HA interfaces are used for synchronization of a pair of firewalls deployed in a High Availability configuration. Because they do not control normal network traffic, they are not placed in a security zone.

The MGT interface is used 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. Other interfaces types are described in other modules.

Creating a Security Zone

Network > Zones > Add



Zone

Name: DMZ

Log Setting: None

Type: Layer3

Zone Protection

Zone Protection Profile: None

□ Enable Packet Buffer Protection

User Identification ACL

□ Enable User Identification

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will be identified.

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

- Specify zone name
- Specify zone type
- Assign interfaces:
  - Must be appropriate type
  - Unassigned interfaces do not process traffic.

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 named External is a special zone that is 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-2000, -3000, -4000, -5000, and -7000 Series firewalls. The External zone type is visible in the drop-down list only when it is supported by a firewall with the virtual systems feature enabled.

Security zones and interfaces

Tap interfaces

Virtual wire interfaces

Layer 2 interfaces

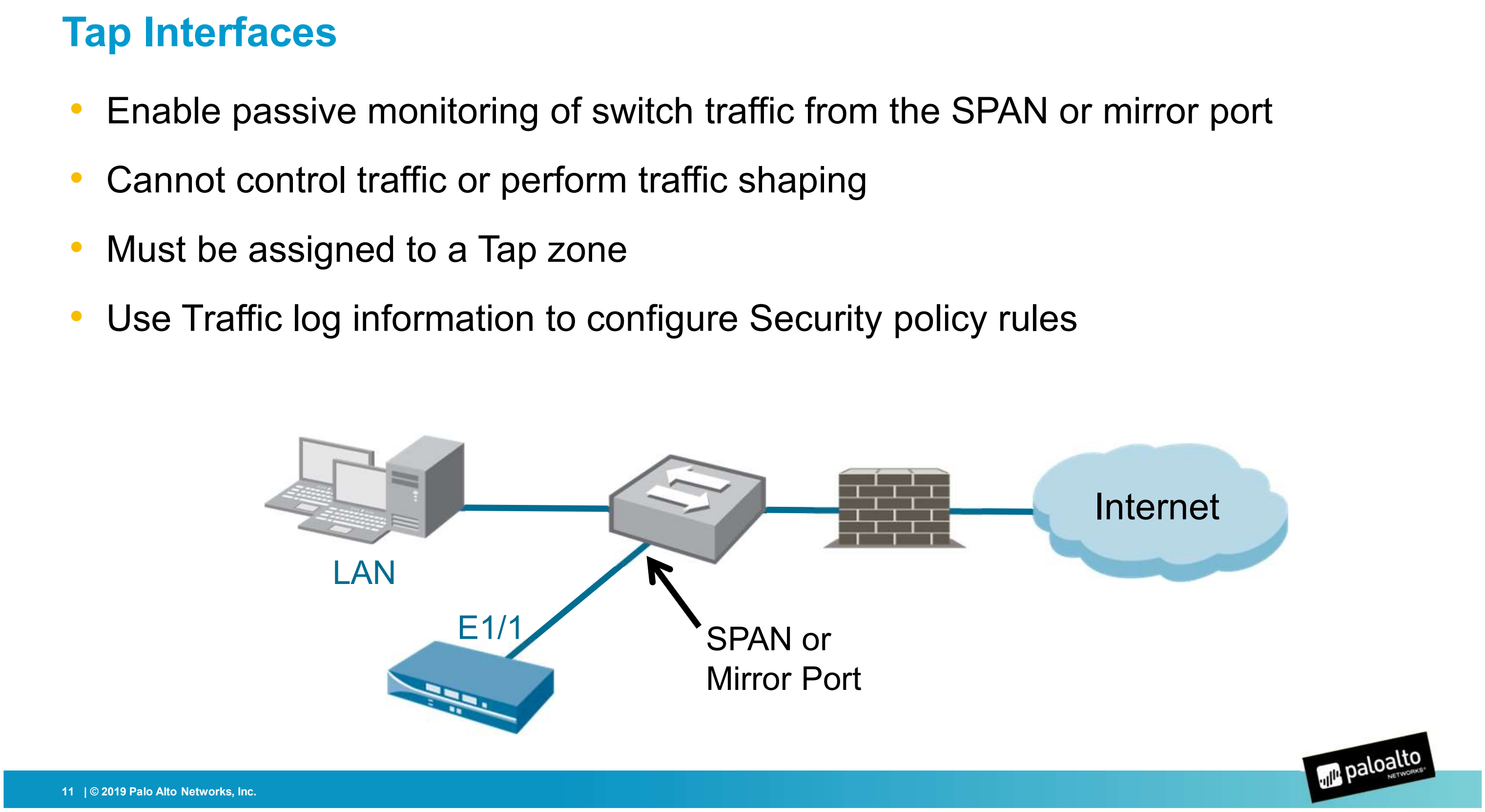
Layer 3 interfaces

Virtual routers

VLAN interfaces

Loopback interfaces

Policy-based forwarding



Tap Interfaces

- Enable passive monitoring of switch traffic from the 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

The firewall can use a Tap interface to connect to a switch’s SPAN or mirror port. A Tap interface passively collects and logs monitored traffic to the firewall’s Traffic log. Tap mode deployment often is used to initially discover the types of application and user traffic flowing across a network. The information recorded in the Traffic log can be used by an administrator to help configure appropriate Security policy rules to allow or block 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 block traffic or perform traffic shaping.

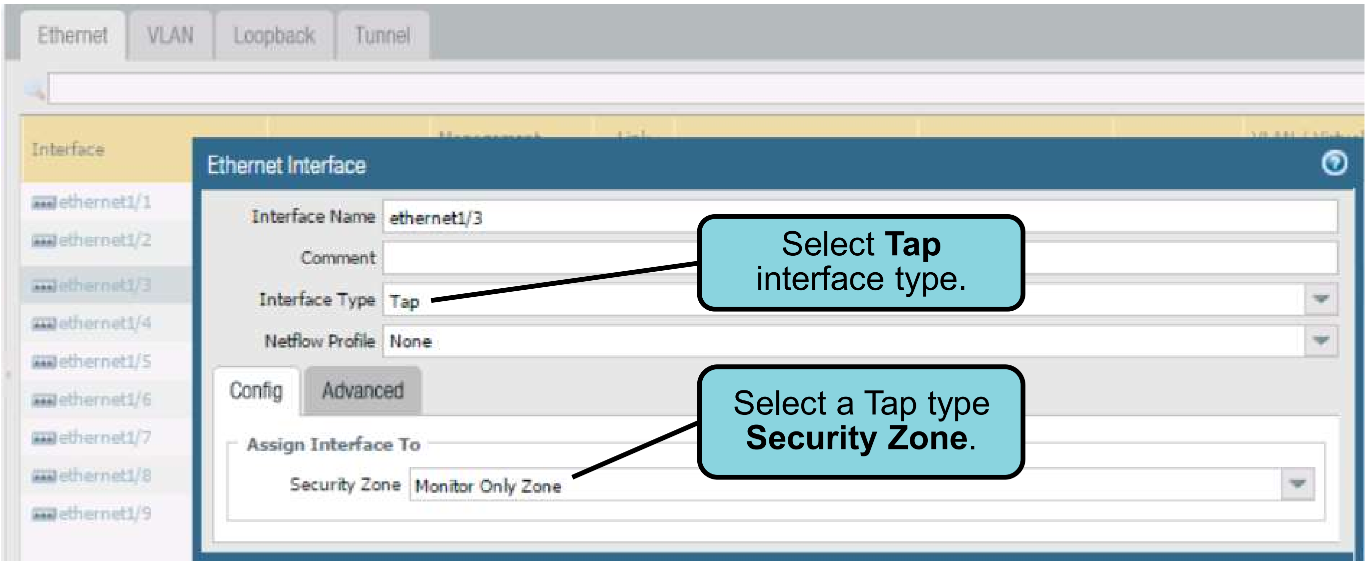
An advantage of using a Tap interface to monitor network traffic flowing through a switch is that it does not require any network address changes.

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 still can 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.

Configuring a Tap Interface

Network > Interfaces > Ethernet > <select_interface>



Interface Name: ethernet1/3

Comment:

Interface Type: Tap

Netflow Profile: None

Security Zone: Monitor Only Zone

Select **Tap** interface type.

Select a Tap type **Security Zone**.

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

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

The firewall can generate and export NetFlow Version 9 records to an outside NetFlow collector. The firewalls support only unidirectional NetFlow, not bidirectional. You can enable NetFlow exports on all interface types listed in this module except HA. The NetFlow feature is available on all firewalls except the PA-4000 Series models.

Security zones and interfaces

Tap interfaces

Virtual wire interfaces

Layer 2 interfaces

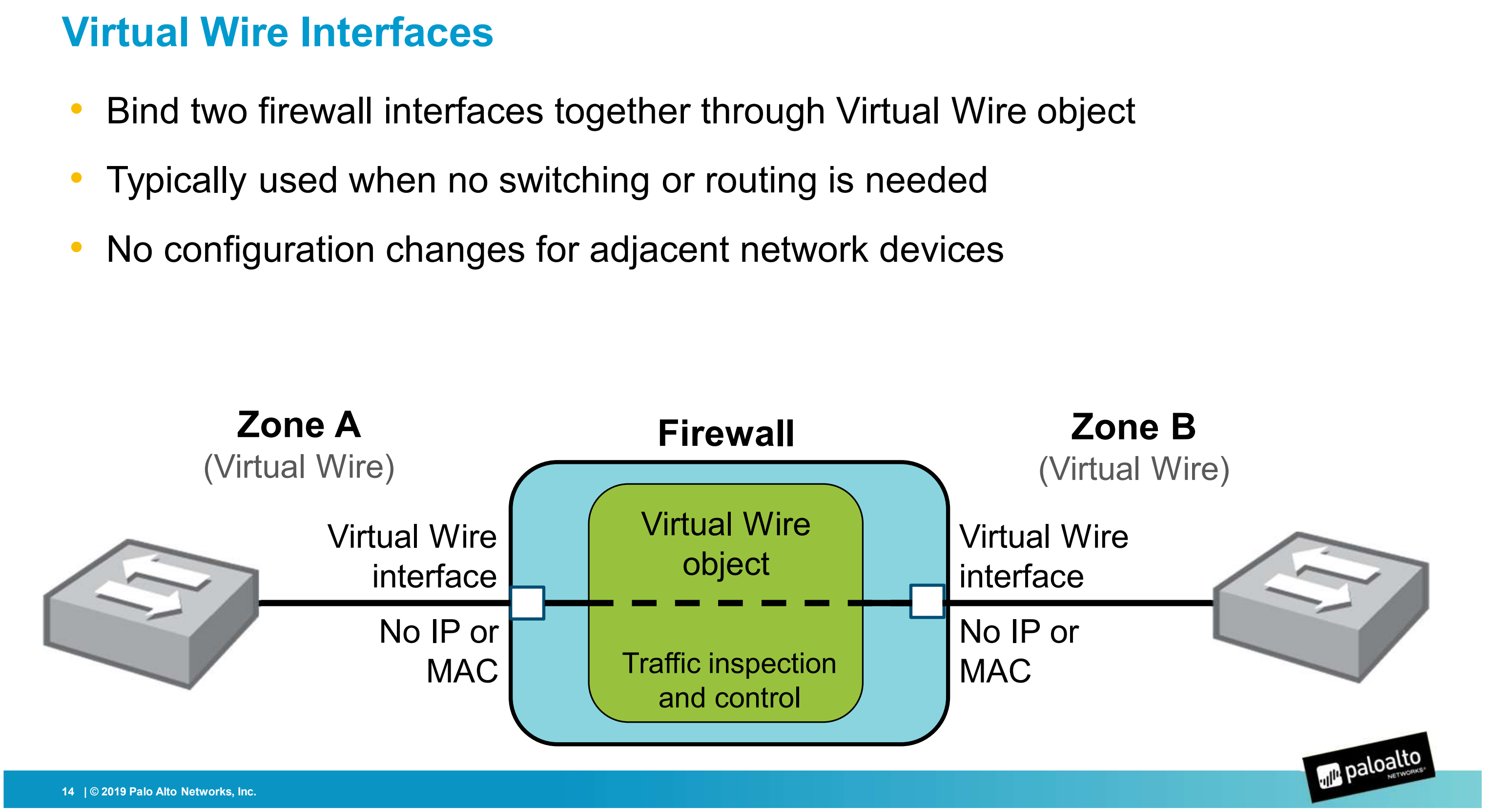
Layer 3 interfaces

Virtual routers

VLAN interfaces

Loopback interfaces

Policy-based forwarding



Virtual Wire Interfaces

- Bind two firewall interfaces together through 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. It also is referred to as a Bump in the Wire or Transparent In-Line deployment. No MAC or IP address is assigned to either Virtual Wire interface. A Virtual Wire configuration typically is used when no switching or routing is required. No configuration changes are required for adjacent network devices, which means that you can insert the firewall into an existing topology without requiring any reallocation 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 accomplish 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.

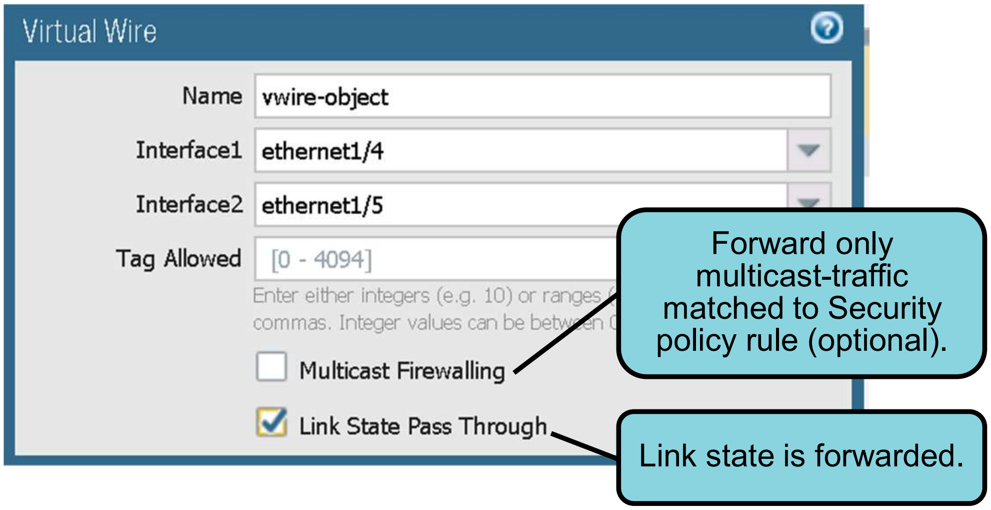
Network traffic flows through a firewall in a virtual wire, which means that the firewall can examine, traffic shape, and block traffic. You can configure the firewall to perform App-ID, Content-ID, NAT, QoS, SSL decryption, and User-ID on the virtual wire. All these features except QoS are described 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 also cannot function as a termination point for an IPsec VPN tunnel.

Configuring 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

Network > Virtual Wires > Add



Virtual Wire

Name	vwire-object
Interface1	ethernet1/4
Interface2	ethernet1/5
Tag Allowed	[0 - 4094]

Enter either integers (e.g. 10) or ranges (commas. Integer values can be between 0

□ Multicast Firewalling

☑ Link State Pass Through

Forward only multicast-traffic matched to Security policy rule (optional).

Link state is forwarded.

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.

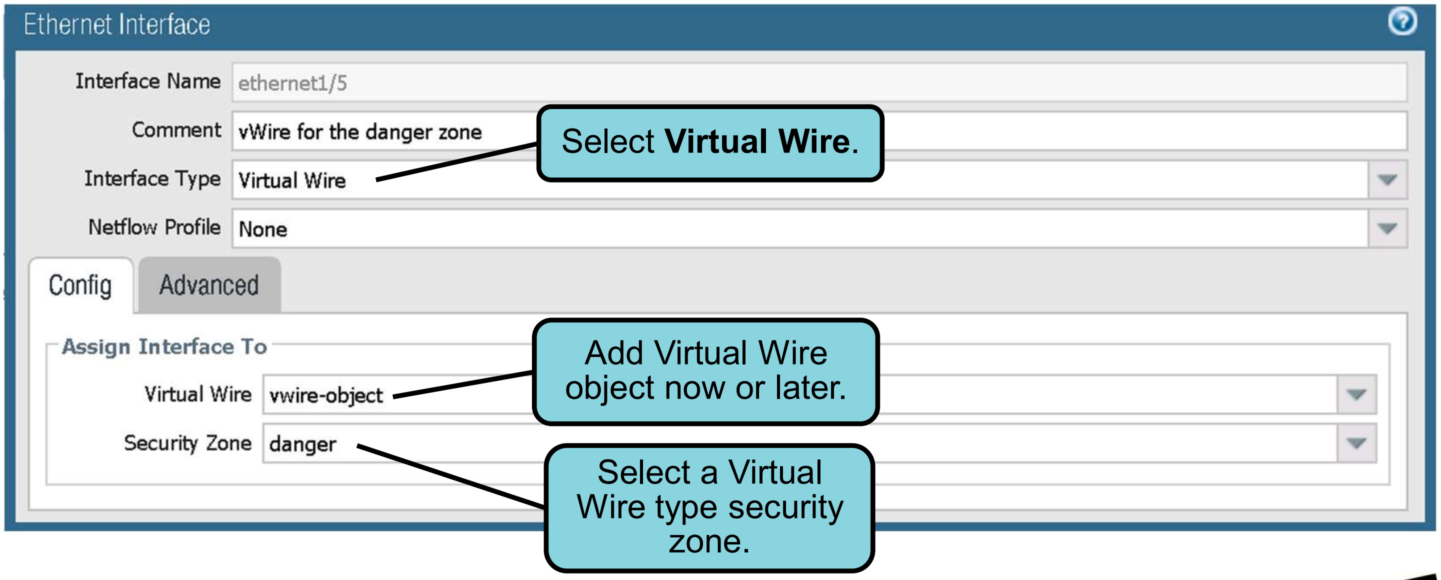
A Virtual Wire object can block or allow traffic based on 802.1Q VLAN tag values. You can specify tag numbers in the range 0 to 4094. A tag value of 0 represents untagged traffic, and the firewall will pass untagged traffic that is allowed by a Security policy rule. You also can specify VLAN tags or ranges of VLAN tags to allow. For example, 4,5,10-12,20-25 is a valid entry in the **Tags Allowed** field. The virtual wire will pass traffic on these VLANs as long as that traffic is allowed by the Security policy rules. To subject all tagged and untagged traffic to Security policy rule evaluation, set the **Tag Allowed** field to the value of **`[0-4094]`**.

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

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.

Configuring a Virtual Wire Interface

Network > Interfaces > Ethernet > <select_interface>



Interface Name: ethernet1/5

Comment: vWire for the danger zone

Interface Type: Virtual Wire

Netflow Profile: None

Assign Interface To

Virtual Wire: vwire-object

Security Zone: danger

Select **Virtual Wire**.

Add Virtual Wire object now or later.

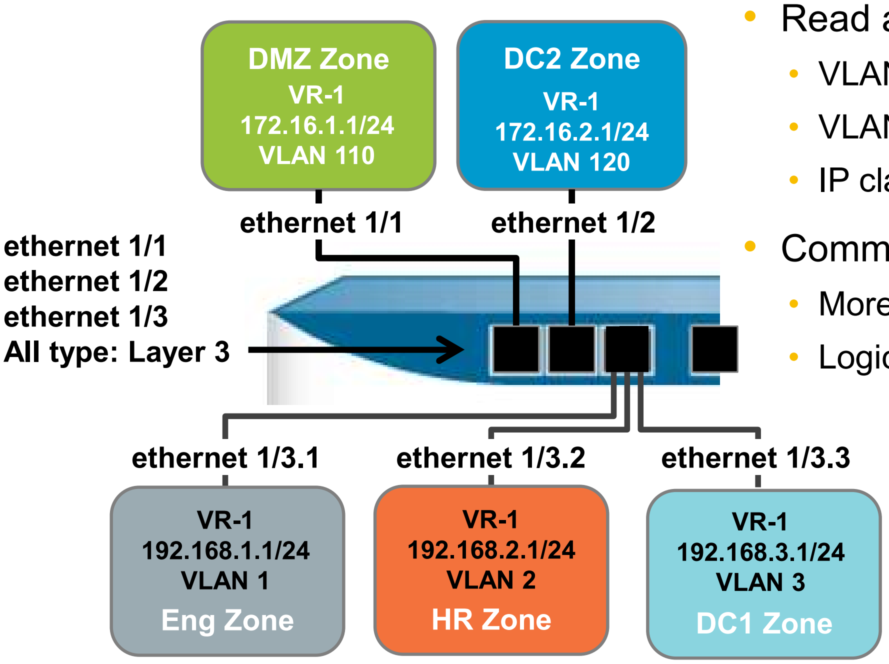
Select a Virtual Wire type security zone.

You must configure the Virtual Wire interfaces that will be connected by the Virtual Wire object. Choose an interface and select the **Interface Type Virtual Wire**. 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.

The firewall can generate and export NetFlow Version 9 records to an outside NetFlow collector. The firewalls support only unidirectional NetFlow, not bidirectional. You can enable NetFlow exports on all interface types listed in this module except HA. The NetFlow feature is available on all firewalls except the PA-4000 Series models.

Virtual Wire Subinterfaces



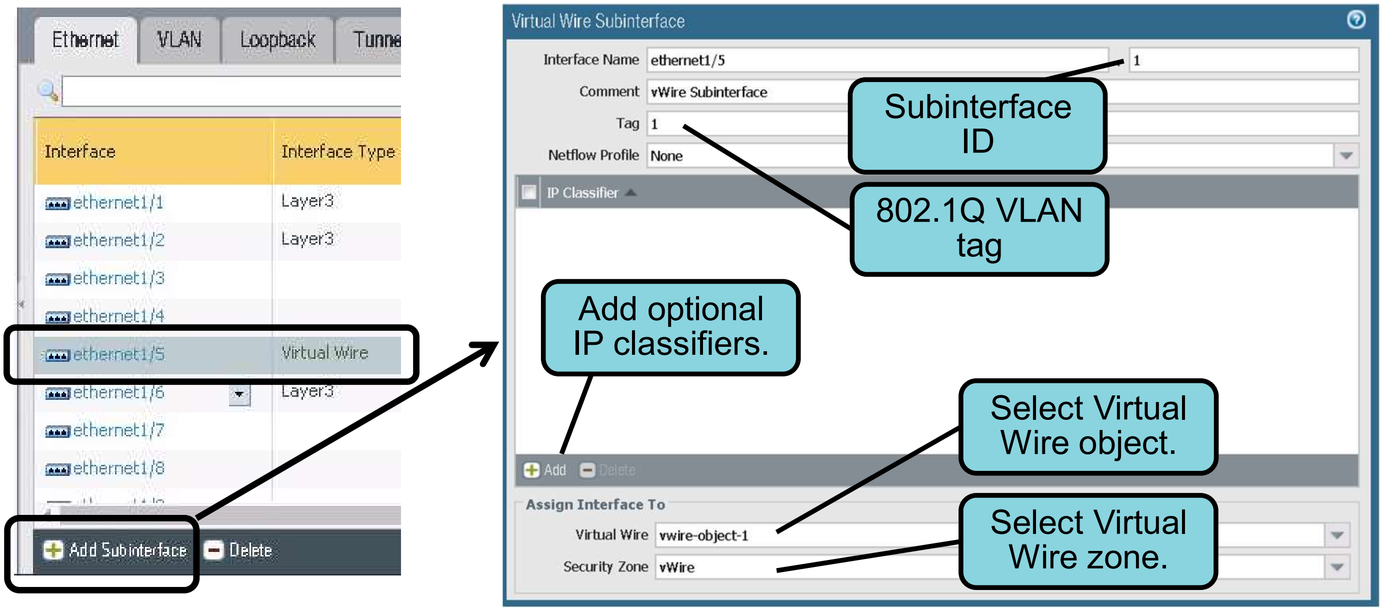
- Read and process traffic based on:
  - VLAN tags (1-4094)
  - VLAN tags and IP classifiers (source IP)
  - IP classifiers (untagged traffic, source IP)
- Common uses include:
  - More granular security rules
  - Logically splitting network traffic

You also can create multiple Virtual Wire subinterfaces that will read and classify traffic according to an administrator-defined VLAN tag, IP classifier, or both. An IP classifier can be a specific address, a range of addresses, or a subnet address. Assign each subinterface to a different security zone, which enables you to apply granular policy controls to different traffic flows arriving or leaving through the same physical firewall port.

In the example, frames tagged with VLAN ID 1 are assigned to the logical interface 1/3.1 and are considered part of the Eng security zone. You can define Security policy rules that control traffic going into or coming out of these zones.

Configuring a Virtual Wire Subinterface

Network > Interfaces > Ethernet



Interface	Interface Type
ethernet1/1	Layer3
ethernet1/2	Layer3
ethernet1/3	
ethernet1/4	
ethernet1/5	Virtual Wire
ethernet1/6	Layer3
ethernet1/7	
ethernet1/8	

Virtual Wire Subinterface

Interface Name	ethernet1/5 . 1
Comment	vWire Subinterface
Tag	1
Netflow Profile	None

Virtual Wire	vwire-object-1
Security Zone	vWire

Subinterface ID

802.1Q VLAN tag

Add optional IP classifiers.

Select Virtual Wire object.

Select Virtual Wire zone.

To create a virtual wire using subinterfaces, select a Virtual Wire interface and click Add Subinterface. You must assign a subinterface ID number to the subinterface. You also can assign an 802.1Q VLAN tag to the subinterface. The subinterface ID number and tag number do not have to match, but administration could be easier if they do match. Any VLAN tag assigned to the subinterface cannot be used by the Virtual Wire object used by the parent interfaces.

If you want to classify untagged traffic (Tag 0) you must use IP classifiers. If the traffic is tagged, then the use of IP classifiers is optional.

As with a physical Virtual Wire interface, you must assign the subinterface to a Virtual Wire object and to a security zone of type Virtual Wire.

Security zones and interfaces

Tap interfaces

Virtual wire interfaces

Layer 2 interfaces

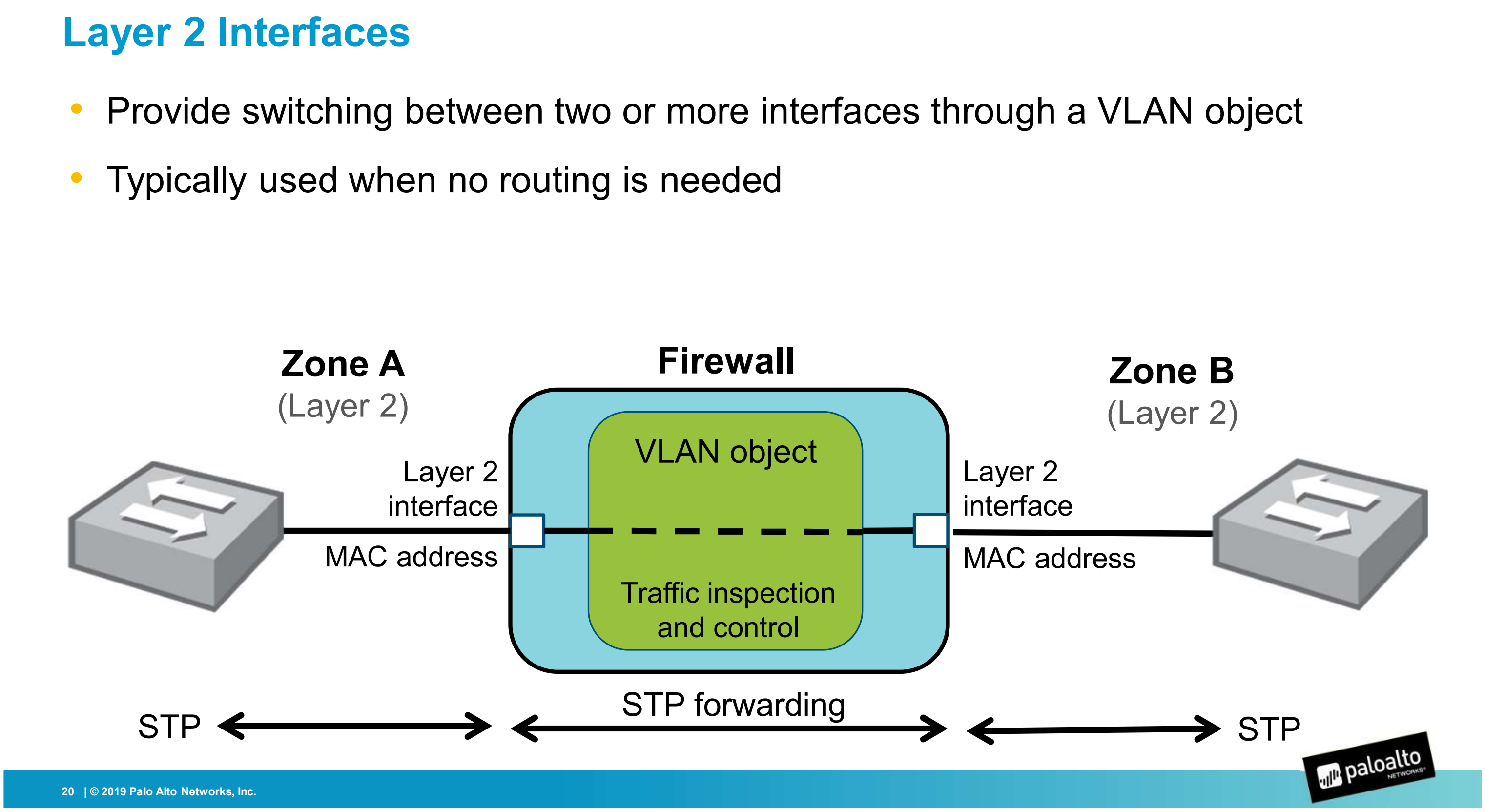
Layer 3 interfaces

Virtual routers

VLAN interfaces

Loopback interfaces

Policy-based forwarding



Layer 2 Interfaces

- Provide switching between two or more interfaces through a VLAN object
- Typically used when no routing is needed

20 | © 2019 Palo Alto Networks, Inc.

In a Layer 2 deployment, the firewall provides switching between two or more interfaces. You must assign a group of interfaces to a common VLAN object for the firewall to switch between them. The VLAN object connects the interfaces into a single Ethernet broadcast domain.

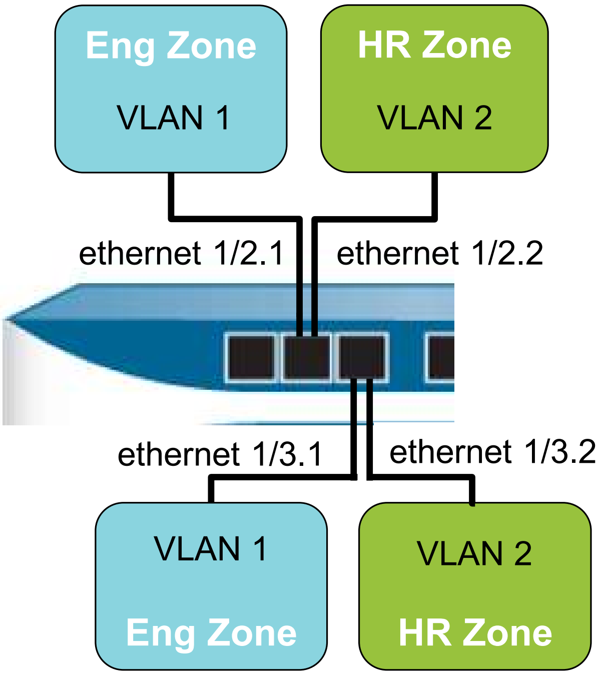
A Layer 2 configuration is defined in two steps: creating the VLAN object and configuring the Layer 2 interfaces that the VLAN object connects. You can accomplish these steps in any order. The VLAN object provides the switched data path between the Layer 2 interfaces.

The firewall is not a participant in the Spanning Tree Protocol, or STP. However, STP packets from external switches are forwarded through the VLAN object to other external switches.

Network traffic flows through a firewall between Layer 2 interfaces, which means that the firewall can examine, traffic shape, and block traffic. You can configure the firewall to perform App-ID, Content-ID, User-ID, SSL decryption, and QoS in a Layer 2 deployment. All these features except QoS are described in other modules.

A Layer 2 interface does not support routing or firewall management traffic because no IP addresses are assigned to a Layer 2 interface.

Layer 2 Subinterfaces



- Assign subinterfaces to zones
- VLAN traffic isolated by subinterfaces:
  - Need route between VLANs
  - Security policy blocks interzone traffic by default
- Useful configuration for multi-tenant networks

You can create Layer 2 subinterfaces and assign each subinterface to an 802.1Q VLAN. The firewall performs VLAN tag switching when Layer 2 subinterfaces are attached to a common VLAN object. Traffic in different VLANs can share a common physical firewall port but traffic between them is blocked by default. To enable traffic to flow between separate VLANs (for example, VLAN 1 and VLAN 2), you would have to configure a router and the appropriate Security policy rules.

Even though Layer 2 subinterfaces are available on the firewall, the best practice is to use Layer 3 subinterfaces with each Layer 3 subinterface assigned to a VLAN rather than to use VLAN objects and Layer 2 subinterfaces. Use of Layer 3 subinterfaces provides isolation at Layer 2 yet provides a routing path between networks at the IP layer. Layer 3 interfaces and subinterfaces are described later in this module.

Security zones and interfaces

Tap interfaces

Virtual wire interfaces

Layer 2 interfaces

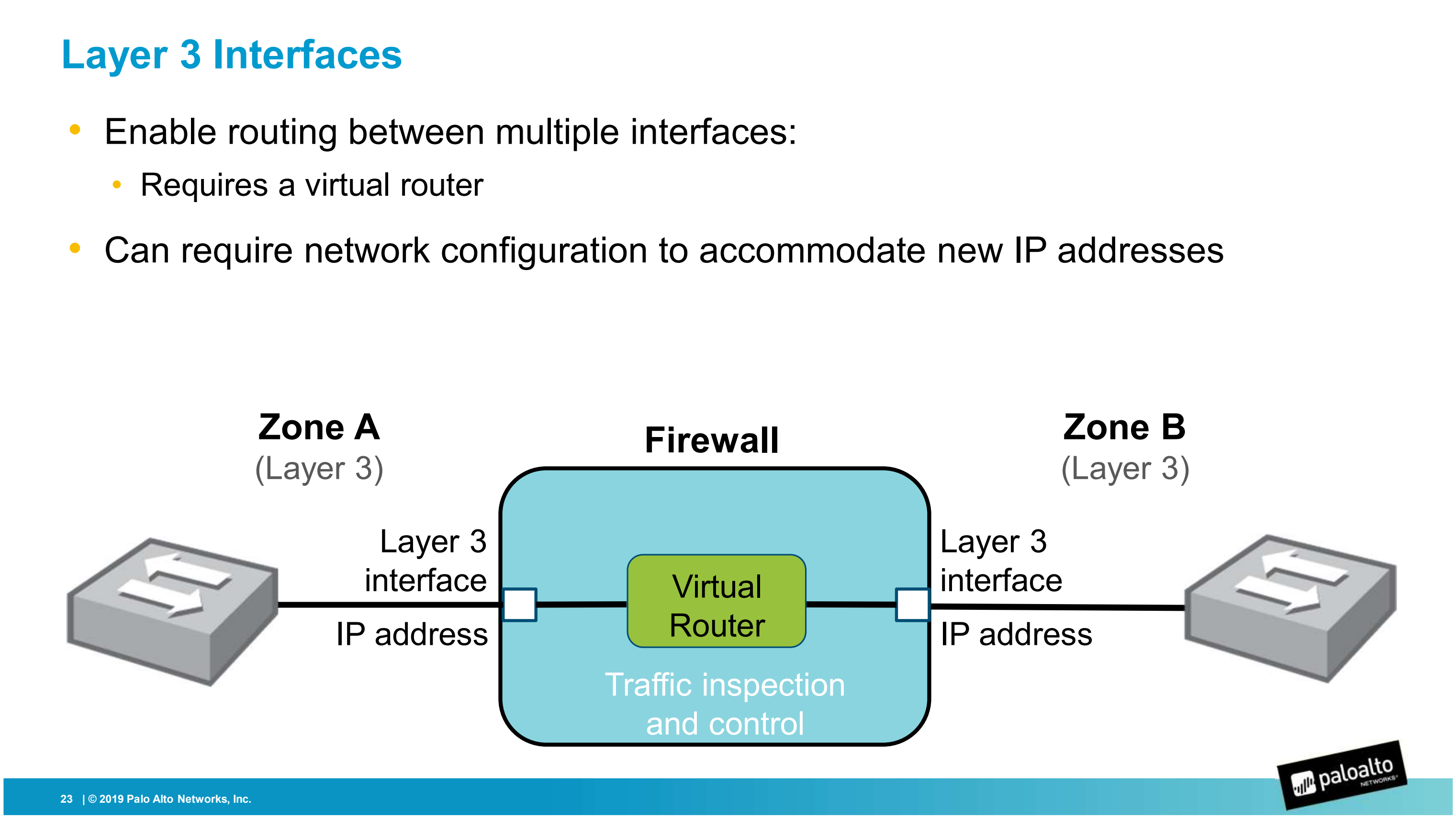
Layer 3 interfaces

Virtual routers

VLAN interfaces

Loopback interfaces

Policy-based forwarding



Layer 3 Interfaces

- Enable routing between multiple interfaces:
  - Requires a virtual router
- Can require network configuration to accommodate new IP addresses

Zone A
(Layer 3)

Firewall

Zone B
(Layer 3)

Layer 3
interface

IP address

Virtual
Router

Layer 3
interface

IP address

Traffic inspection
and control

A Layer 3 deployment enables routing traffic between multiple Layer 3 interfaces. You must assign an IP address to each Layer 3 interface. Because each Layer 3 interface consumes at least one IP address, a Layer 3 deployment can require network reconfiguration in your enterprise.

Routing between Layer 3 interfaces requires a router. In the example, an internal virtual router provides a routable connection between the Layer 3 interfaces.

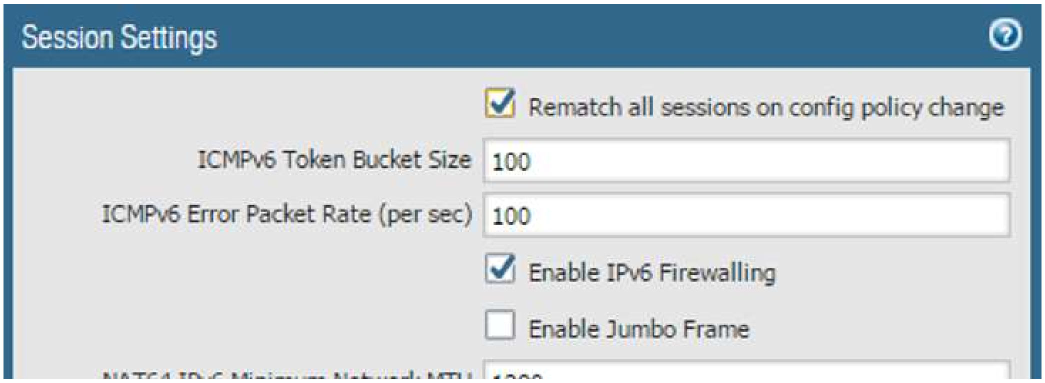
Network traffic can flow through a firewall between Layer 3 interfaces, which means that the firewall can examine, traffic shape, and block traffic. You can configure the firewall to perform App-ID, Content-ID, User-ID, SSL decryption, NAT, and QoS in a Layer 3 deployment. All these features except QoS are described in other modules.

A Layer 3 interface can support firewall management traffic because it is assigned an IP address.

IPv4 and IPv6

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

Device > Setup > Session > Session Settings



Session Settings

☑ Rematch all sessions on config policy change

ICMPv6 Token Bucket Size: 100

ICMPv6 Error Packet Rate (per sec): 100

☑ Enable IPv6 Firewalling

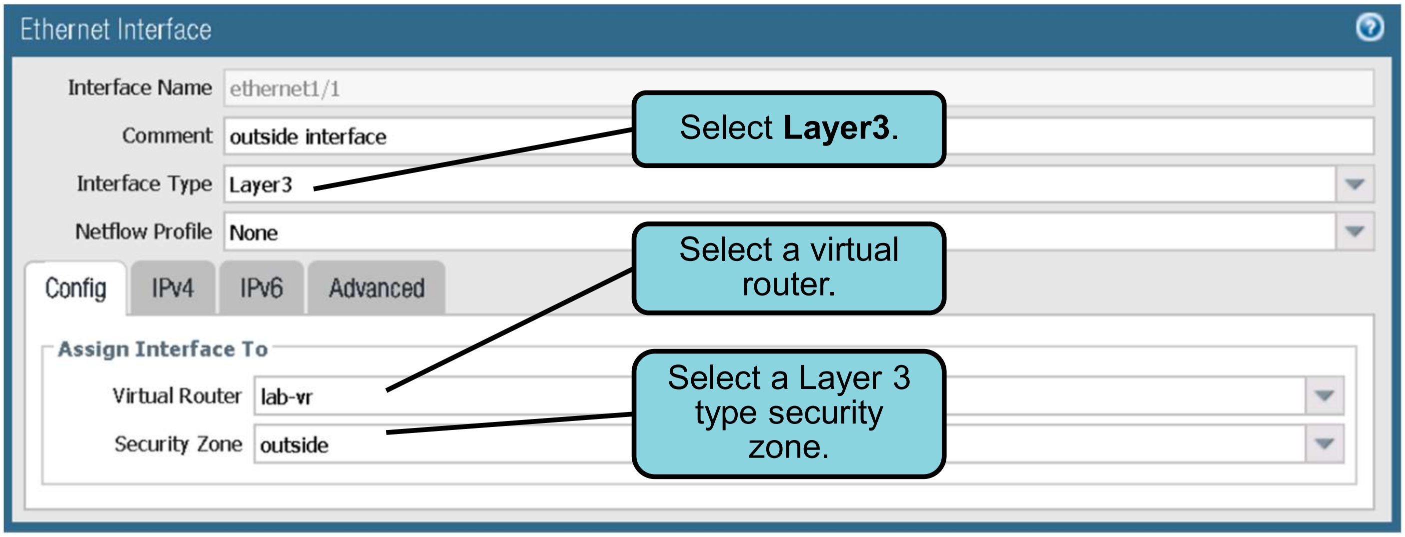
□ Enable Jumbo Frame

NAT64 IPv6 Minimum Network MTU: 1280

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

Configuring a Layer 3 Interface: Config

Network > Interfaces > Ethernet > <select_interface>



Interface Name: ethernet1/1
Comment: outside interface
Interface Type: Layer3
Netflow Profile: None
Virtual Router: lab-vr
Security Zone: outside

Select **Layer3**.

Select a virtual router.

Select a Layer 3 type security zone.

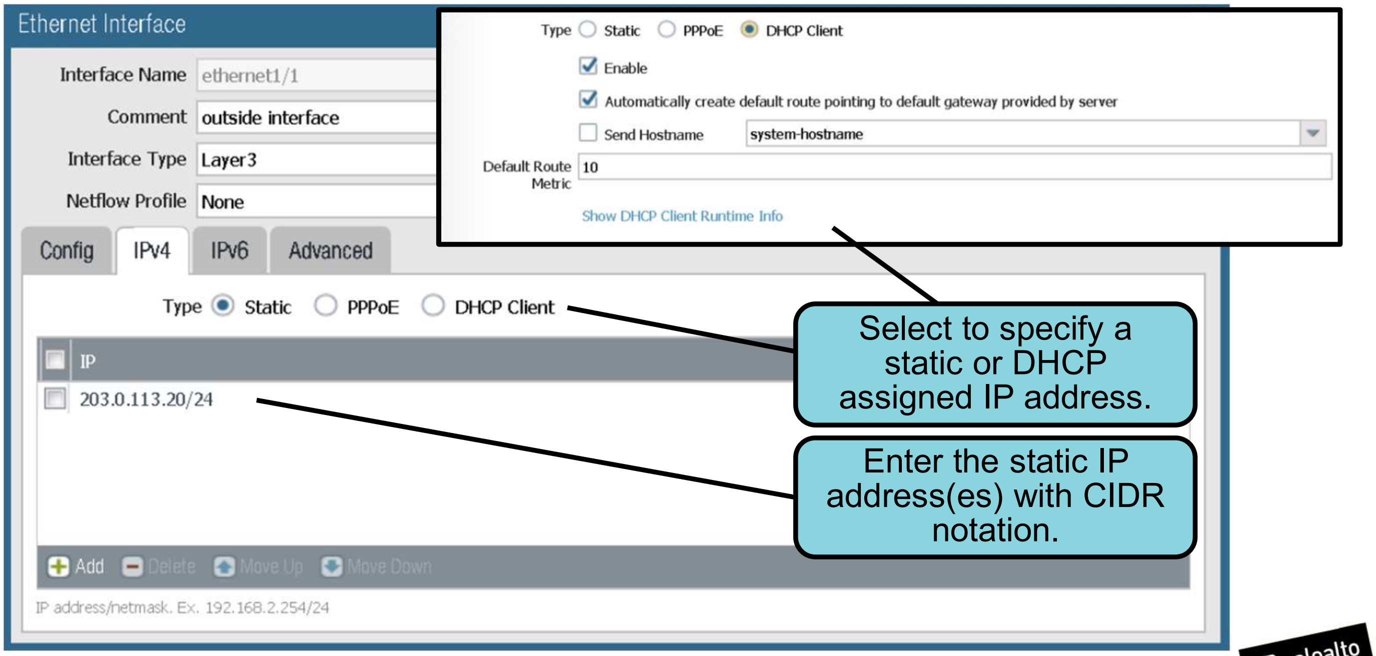
To configure a Layer 3 interface, browse to **Network** > **Interfaces** > **Ethernet** and select an interface. The minimum required properties for configuring a Layer 3 interface are the **Interface Type**, IP address, and **Security Zone**.

Select the **Interface Type** of **Layer3**. If you want to be able to route traffic to and from the interface, you will need to have a 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.

Then select a security zone from the **Security Zone** drop-down list. Only zones configured as Layer 3 zones appear on the drop-down list.

Configuring a Layer 3 Interface: IPv4

Network > Interfaces > Ethernet > <select_interface>



Ethernet Interface

Interface Name	ethernet1/1
Comment	outside interface
Interface Type	Layer3
Netflow Profile	None

Type ● Static ○ PPPoE ○ DHCP Client

□	IP
□	203.0.113.20/24

IP address/netmask. Ex. 192.168.2.254/24

Type ○ Static ○ PPPoE ● DHCP Client

☑ Enable

☑ Automatically create default route pointing to default gateway provided by server

□ Send Hostname system-hostname

Default Route Metric 10

Show DHCP Client Runtime Info

Select to specify a static or DHCP assigned IP address.

Enter the static IP address(es) with CIDR notation.

26 | © 2019 Palo Alto Networks, Inc.

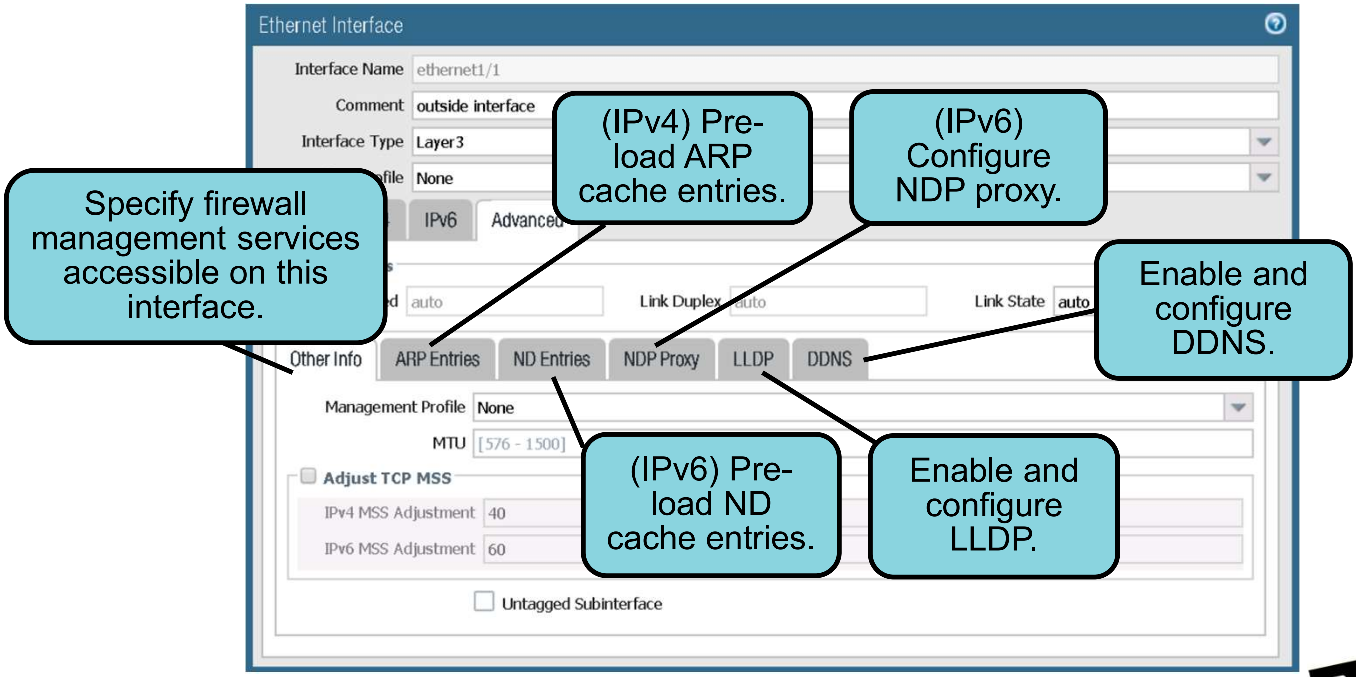
You can configure a Layer 3 interface with one or more static IPv4 addresses or as a DHCP client. To configure static IP addresses, select the **Static** radio button. You can assign multiple IPv4 addresses to the same interface, although they should not be in the same subnet.

To configure an interface using DHCP, click 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 situations might include 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.

Configuring a Layer 3 Interface: Advanced

Network > Interfaces > Ethernet > <select_interface>



Ethernet Interface

Interface Name: ethernet1/1

Comment: outside interface

Interface Type: Layer3

file: None

d: auto

Link Duplex: auto

Link State: auto

Management Profile: None

MTU: [576 - 1500]

□ Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

□ Untagged Subinterface

Specify firewall management services accessible on this interface.

(IPv4) Pre-load ARP cache entries.

(IPv6) Configure NDP proxy.

Enable and configure DDNS.

(IPv6) Pre-load ND cache entries.

Enable and configure LLDP.

The **Advanced** tab enables you to configure a variety of Layer 3 interface settings. For example, you can modify each individual interface’s link speed and duplex settings, or modify 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 that are accessible through the Layer 3 interface.

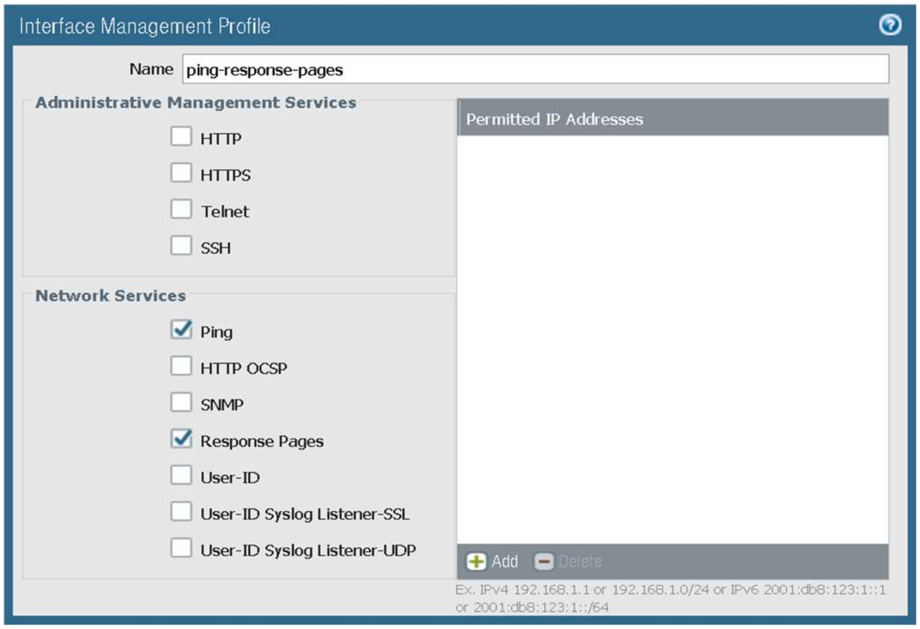
Use the **ARP Entries** tab to pre-load ARP table entries in the firewall’s ARP cache or use the **ND Entries** tab to pre-load IPv6 Neighbor Discovery entries. If you need an IPv6 NDP proxy, the **NDP Proxy** tab enables you to configure the interface as an NDP proxy that will respond to ND queries. 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 to 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, FreeDNS Afraid.org, and No-IP.

The **Untagged Subinterface** check box enables you to 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



Interface Management Profile

Name: ping-response-pages

Administrative Management Services

- □ HTTP
- □ HTTPS
- □ Telnet
- □ SSH

Network Services

- ☑ Ping
- □ HTTP OCSP
- □ SNMP
- ☑ Response Pages
- □ User-ID
- □ User-ID Syslog Listener-SSL
- □ User-ID Syslog Listener-UDP

Permitted IP Addresses

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

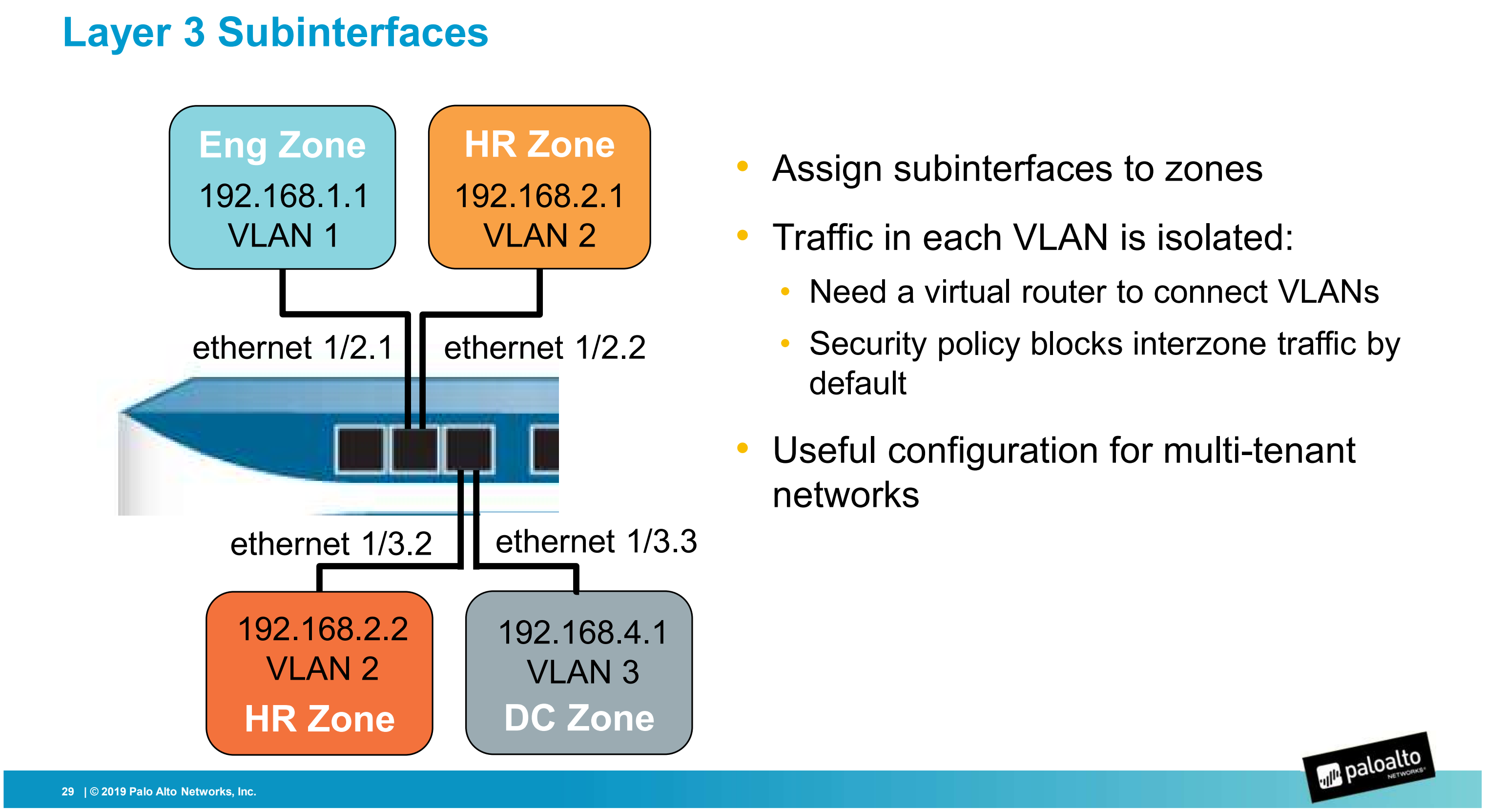
- Defines which firewall management services are accessible from a traffic interface
- Can be applied to Layer 3, loopback, and tunnel interfaces

By default, the out-of-band MGT port is designed to support firewall management functions and services. Alternatively, you can apply an Interface Management Profile to a Layer 3 interface to enable it 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 will need to 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 would enable the firewall to respond to an ICMP Echo Request, which is useful to verify basic network connectivity to the interface. Response Pages enable a firewall to present information to users in response to their activity. For example, a response page might be the presentation of an interactive webpage to a user asking them to verify a file transfer before the firewall will allow the file transfer.

You can assign an Interface Management Profile to Layer 3 interfaces and subinterfaces and to logical interfaces such as VLAN, loopback, and tunnel interfaces. If you do not assign an Interface Management Profile to an interface, the firewall denies access to 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, then only the IP addresses listed can access the selected functions and services. If the field is left blank, the profile allows any IP address to access the selected functions and services, assuming that it is not blocked by a Security policy rule.



Layer 3 Subinterfaces

- Assign subinterfaces to zones
- Traffic in each VLAN is isolated:
  - Need a virtual router to connect VLANs
  - Security policy blocks interzone traffic by default
- Useful configuration for multi-tenant networks

You can create Layer 3 subinterfaces and assign each subinterface to an 802.1Q VLAN. Traffic in different VLANs can share a common physical firewall port, but traffic between them is isolated at network Layer 2. However, traffic can be routed between the VLANs at network Layer 3 if a route exists between them at the IP network layer. You still will need to configure appropriate Security policy rules to allow traffic to flow between different security zones.

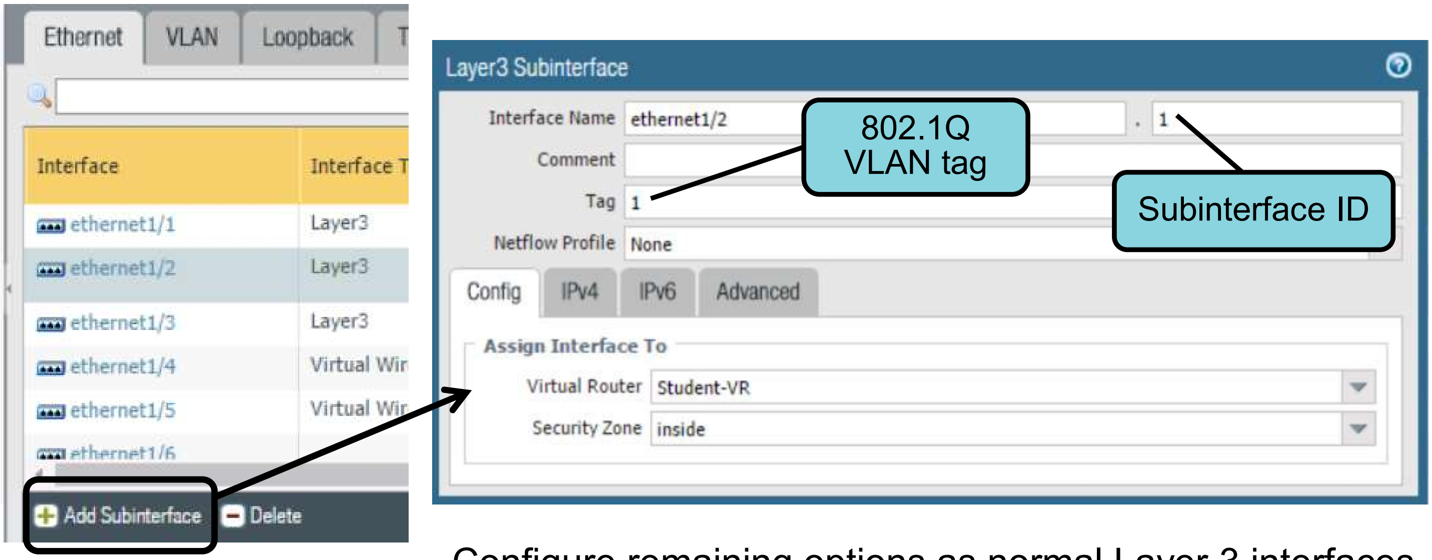
In the example, the subinterfaces 1/2.2 and 1/3.2 have been assigned to the same VLAN, and the firewall will use Ethernet switching to pass traffic between them.

The subinterfaces 1/2.1 and 1/3.3 are in different VLANs. Traffic could be passed between them only at the IP layer through a virtual router. Because these subinterfaces also are in different security zones and interzone traffic is blocked by default, you also would have to configure appropriate Security policy rules to pass traffic between these subinterfaces.

You also would need a virtual router and appropriate Security policy rules to pass traffic between the subinterfaces in VLANs 1 and 3. You also would need a virtual router and appropriate Security policy rules to pass traffic between the VLAN 2 subinterfaces and the subinterfaces in VLANs 1 or 3. Because the subinterfaces in VLAN 2 both are in the same zone, the firewall automatically will pass network traffic between them.

Configuring a Layer 3 Subinterface

Network > Interfaces > Ethernet



Interface	Interface T
ethernet1/1	Layer3
ethernet1/2	Layer3
ethernet1/3	Layer3
ethernet1/4	Virtual Wir
ethernet1/5	Virtual Wir
ethernet1/6	

Interface Name: ethernet1/2 . 1
Comment:
Tag: 1
Netflow Profile: None

Assign Interface To
Virtual Router: Student-VR
Security Zone: inside

Configure remaining options as normal Layer 3 interfaces.

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

All the steps to configure Layer 3 interfaces also 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.

Security zones and interfaces

Tap interfaces

Virtual wire interfaces

Layer 2 interfaces

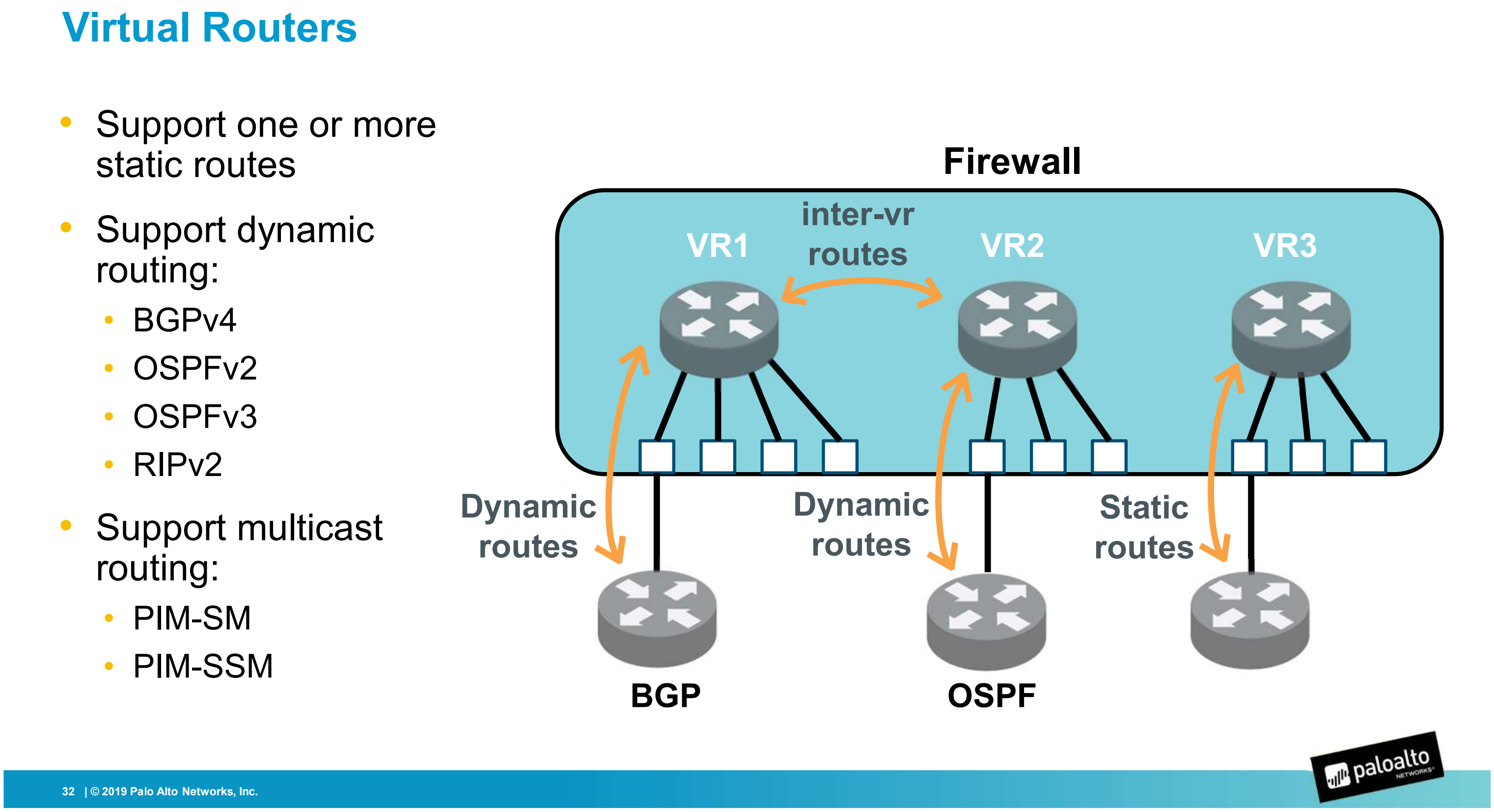
Layer 3 interfaces

Virtual routers

VLAN interfaces

Loopback interfaces

Policy-based forwarding



Virtual Routers

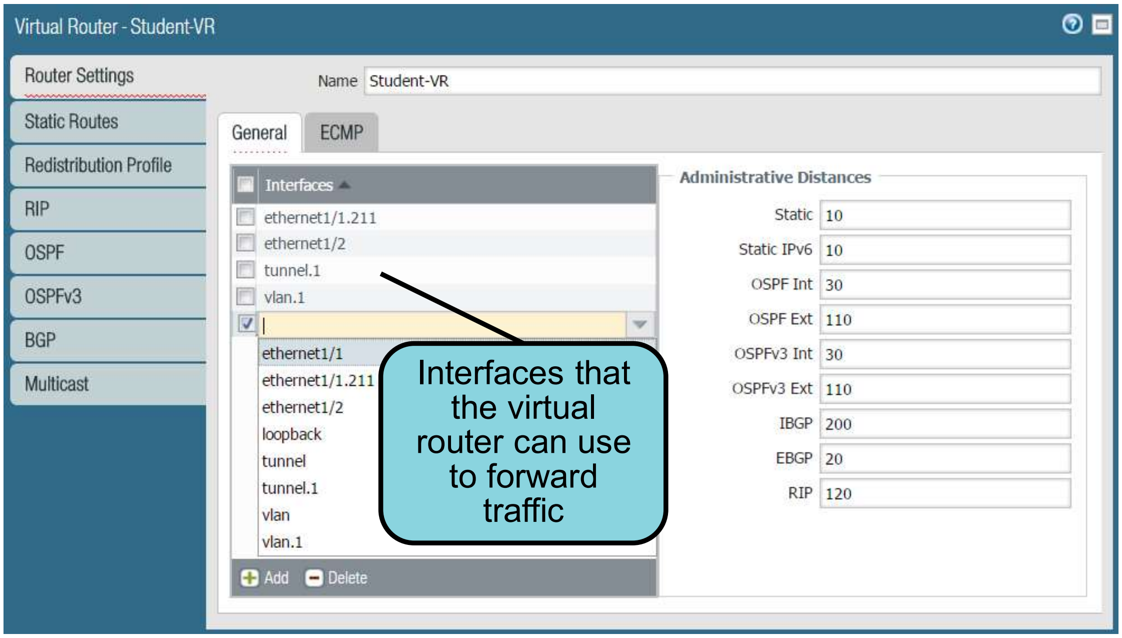
- Support one or more static routes
- Support dynamic routing:
  - BGPv4
  - OSPFv2
  - OSPFv3
  - RIPv2
- Support multicast routing:
  - PIM-SM
  - PIM-SSM

The firewall uses a virtual router to obtain routes to other subnets. You can manually define one or more static routes or configure a virtual router to participate in one or more dynamic routing protocols. The dynamic routing protocols supported on the firewall are BGP version 4, OSPF versions 2 and 3, and RIP version 2. For multicast routing, the firewall supports Protocol Independent Multicast sparse mode, or PIM-SM, and PIM source-specific multicast, or PIM-SSM. PIM version 2 is used for both multicast protocols. IGMPv1, v2, and v3 also are supported on host-facing interfaces.

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

Virtual Router General Settings

Network > Virtual Routers



Virtual Router - Student-VR

Name: Student-VR

□ Interfaces
□ ethernet1/1.211
□ ethernet1/2
□ tunnel.1
□ vlan.1
☑

ethernet1/1
ethernet1/1.211
ethernet1/2
loopback
tunnel
tunnel.1
vlan
vlan.1

Administrative Distances

Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

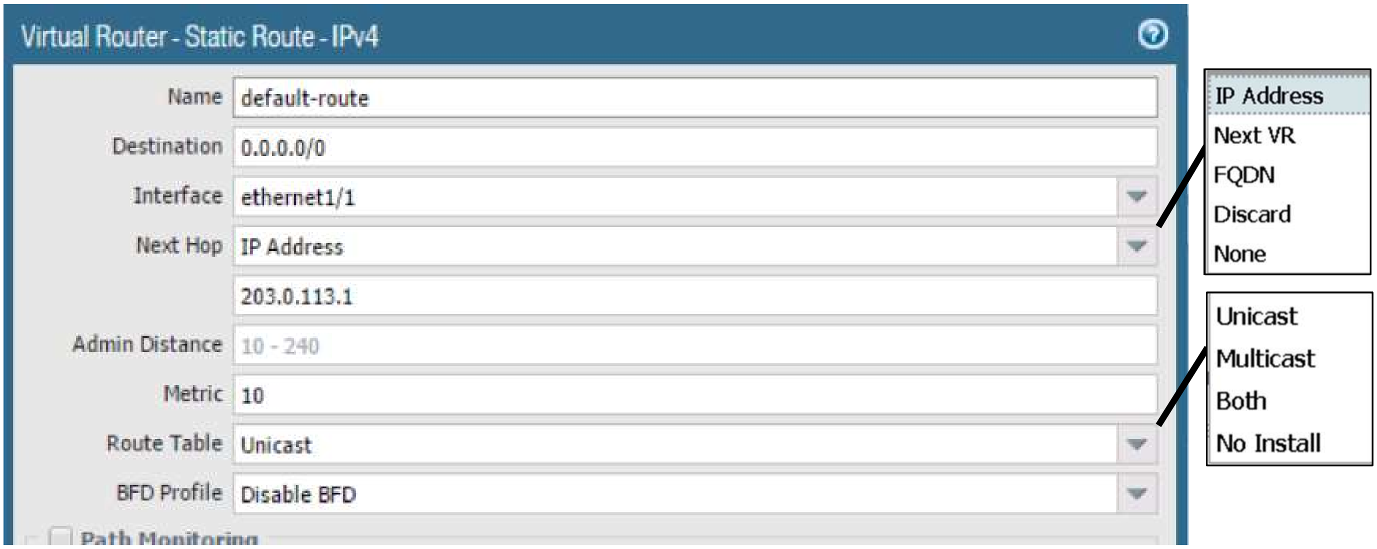
Interfaces that the virtual router can use to forward traffic

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

Administrative distances help the virtual router to determine the best route to use when multiple routes to the same destination are offered by two different routing protocols. 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.

Adding a Static Default Route

Network > Virtual Routers > Static Routes > Add



Virtual Router - Static Route - IPv4

Name	default-route
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address
	203.0.113.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

□ Path Monitoring

To add a static route, browse to **Network** > **Virtual Routers** > **Static Routes** and click **Add**. 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. An address of 0.0.0.0/0 is a default route for any destination IP address that does not match another address in the route table. 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.

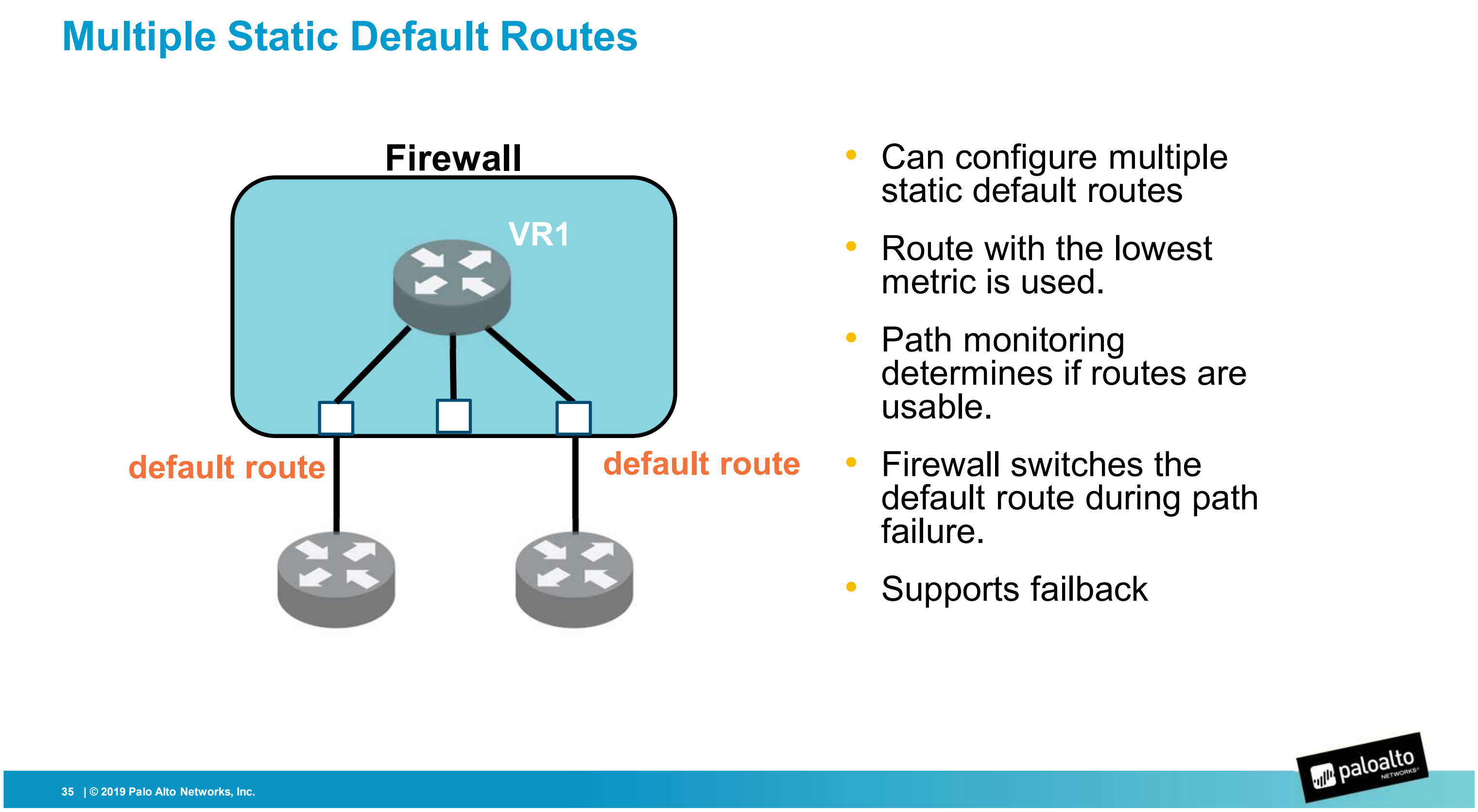
The next hop that you choose can be a specific IP address or another virtual router. If you select **Discard**, the firewall discards traffic that matches the **Destination** address. This traffic would not appear in the Traffic log because it is discarded before a session is created. Select **None** 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, which was described on the previous page.

The **Metric** field helps the virtual router to determine the best route to use when multiple routes to the same destination are offered by the same routing protocol. 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 select **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 between two interfaces to detect a failed route. 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. Each default route is assigned a different metric, with the lowest metric used to determine the route that is actively used. Static route path monitoring is used by the firewall to determine whether a static route is functioning. If path monitoring determines that a route no longer is working, the firewall switches to the static default route with the higher metric. Prior to 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.