CONNECT TO PRODUCTION NETWORKS

NETWORK CONNECTIVITY IS NOT A LUXURY, IT IS A NECESSITY

- Block threats by using network segmentation
- Network interfaces and security zones
- Tap interfaces
- Virtual wire interfaces
- Layer 3 interfaces
- Virtual routers
- Loopback interfaces

EDU-210 Version B
PAN-OS® 10.0

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
- Configure a loopback interface to support external connections to internal firewall services

Block threats by using network segmentation

Network interfaces and security zones

Tap interfaces

Virtual wire interfaces

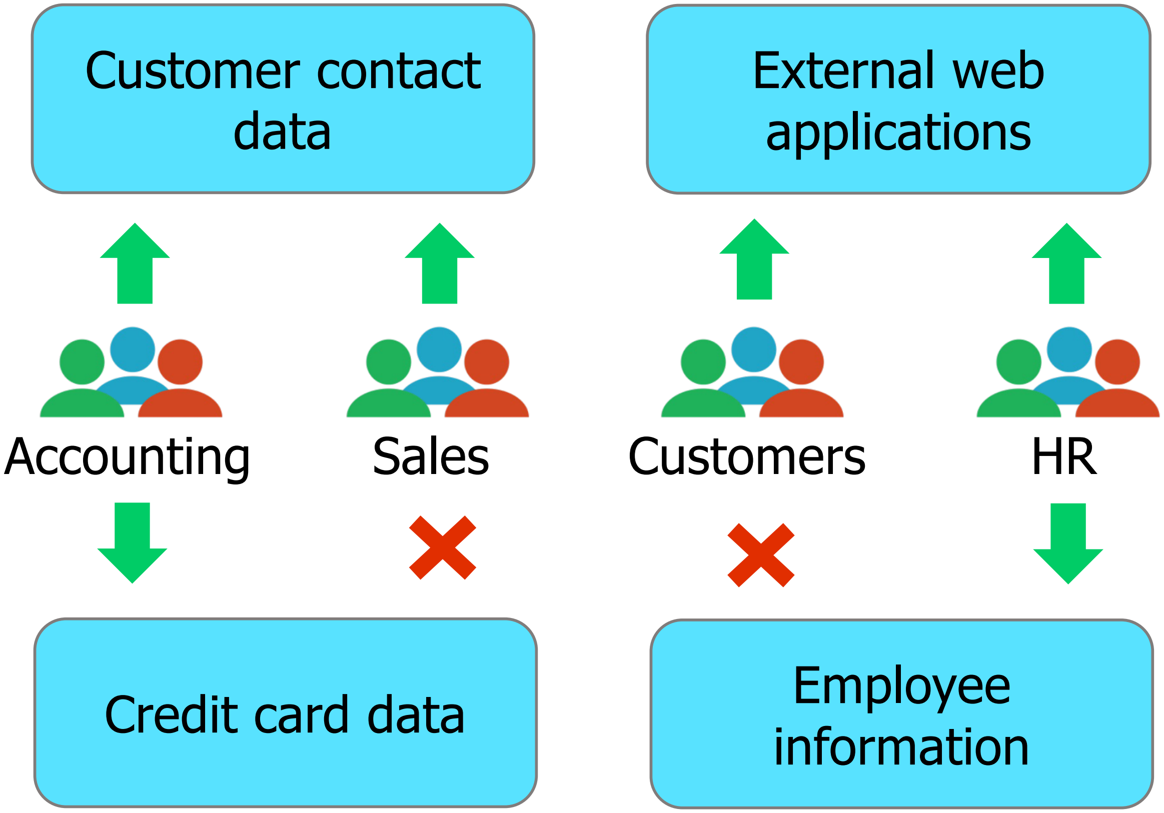
Layer 3 interfaces

Virtual routers

Loopback interfaces

Network Segmentation

- Use network segmentation to secure access to data.
- Understand your business and organizational drivers:
  - Who must access what?
  - Use the principle of least privilege.
  - Consider any regulatory requirements.



Customer contact data

External web applications

Accounting

Sales

Customers

HR

Credit card data

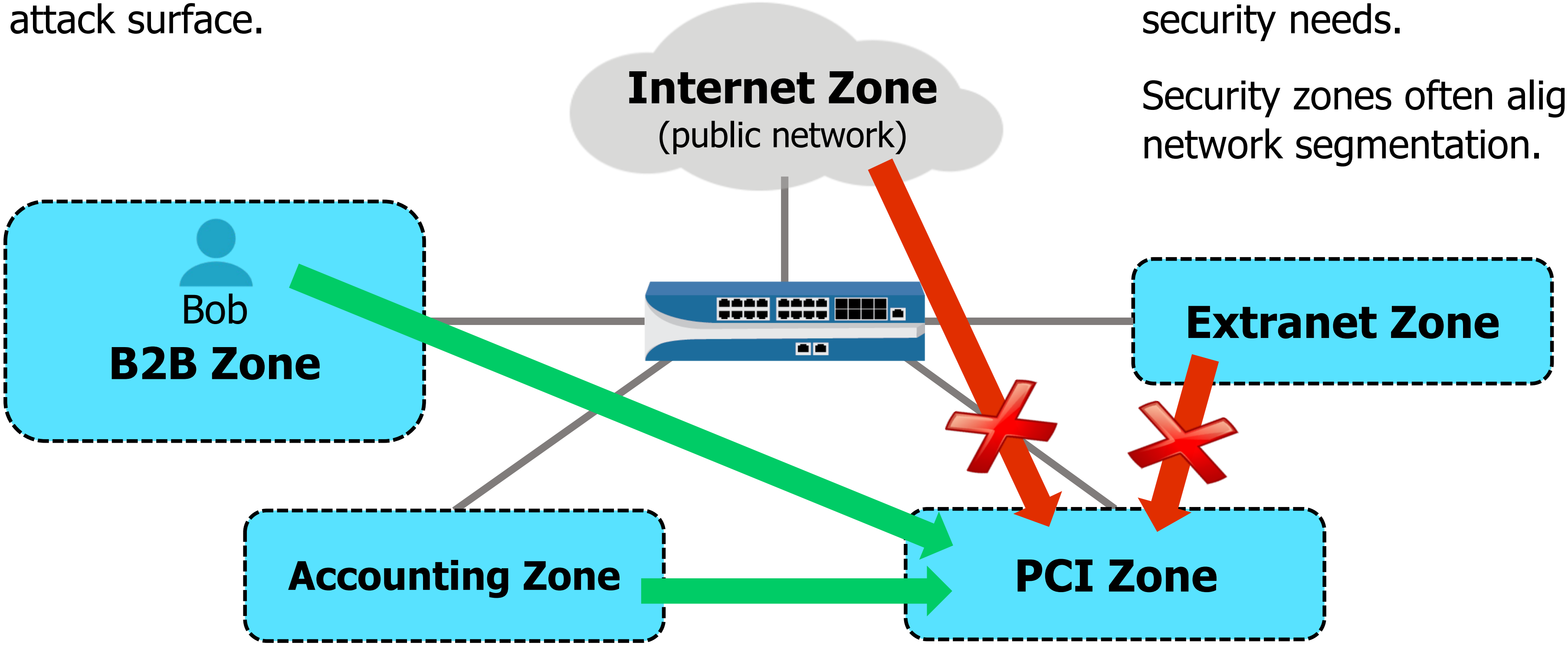
Employee information

Network Segmentation and Security Zones

Use network segmentation and security zones to reduce the attack surface.

Security zones group devices/users with similar security needs.

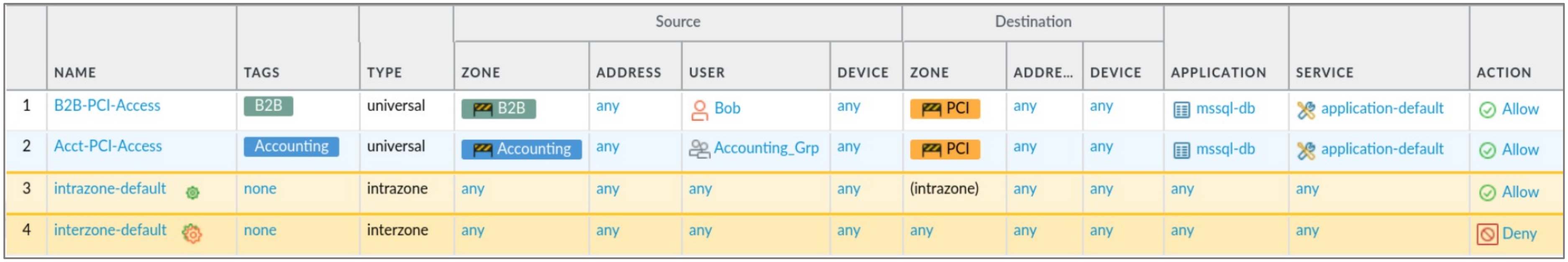
Security zones often align to network segmentation.



|

Configure Security Policy to Support Segmentation

Policies > Security

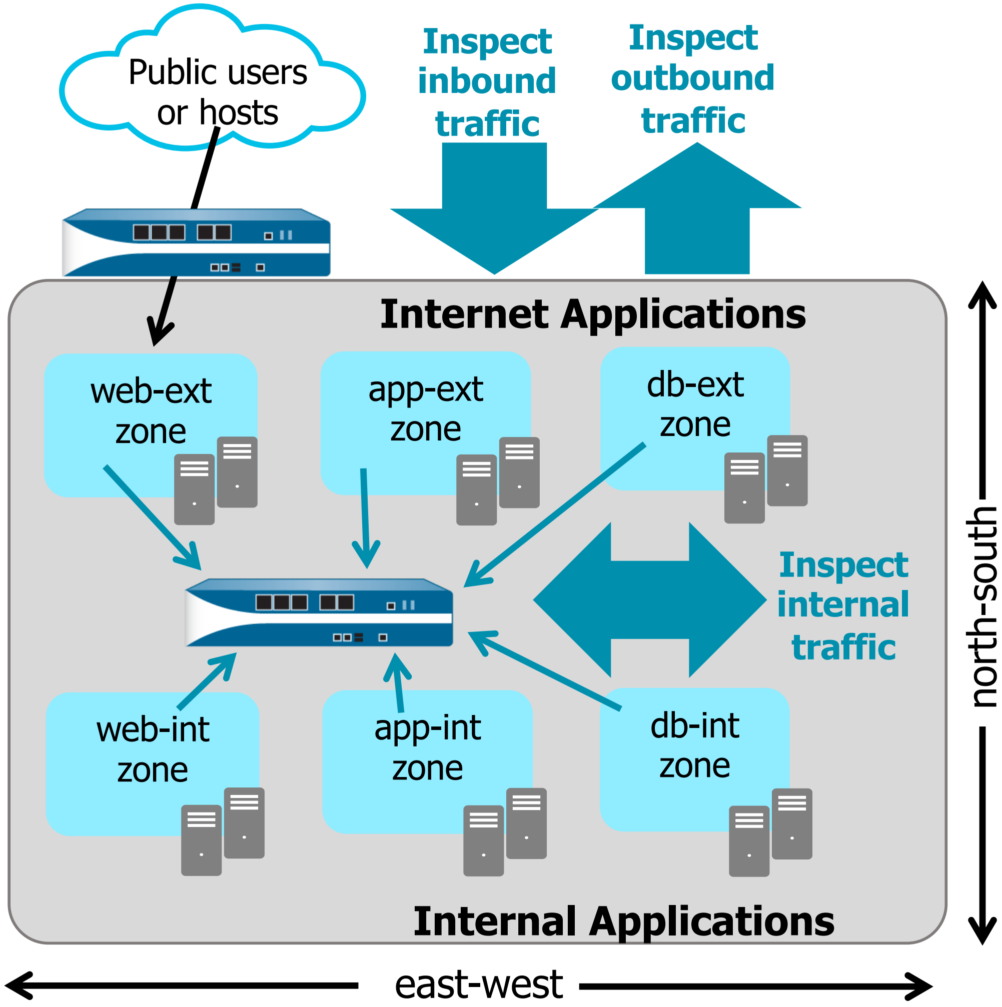


				Source				Destination					
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRE...	DEVICE	APPLICATION	SERVICE	ACTION
1	B2B-PCI-Access	B2B	universal	B2B	any	Bob	any	PCI	any	any	mssql-db	application-default	Allow
2	Acct-PCI-Access	Accounting	universal	Accounting	any	Accounting_Grp	any	PCI	any	any	mssql-db	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.

Zero Trust Architecture

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



Blocking threats by using network segmentation

Network interfaces and security zones

Tap interfaces

Virtual wire interfaces

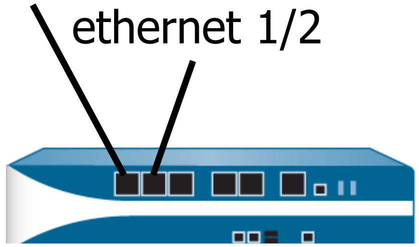
Layer 3 interfaces

Virtual routers

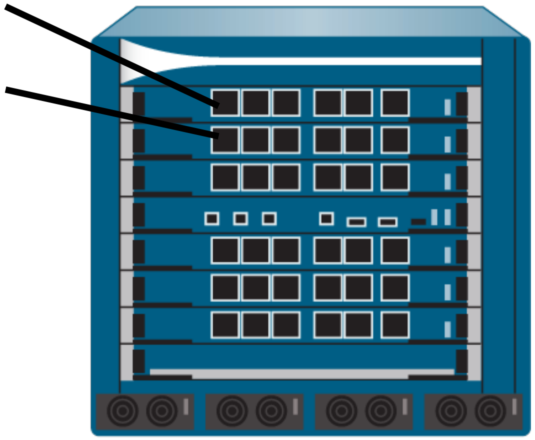
Loopback interfaces

Network Interfaces

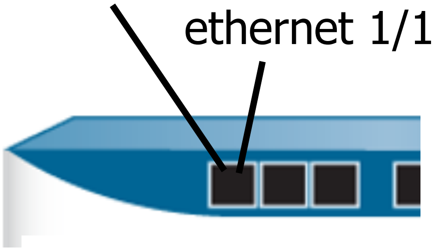
- The firewall data plane controls *in-band* network interfaces.
- Each interface is assigned to a single zone.
- A zone can include multiple physical or logical interfaces.



Single-Slot Firewall



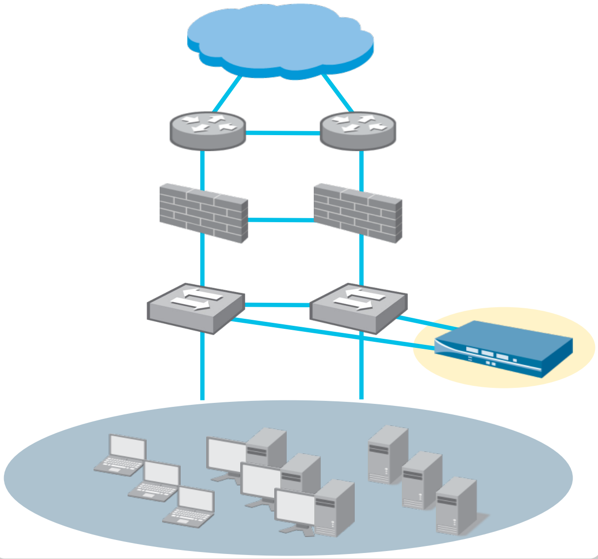
Multi-Slot Firewall



Logical Interfaces

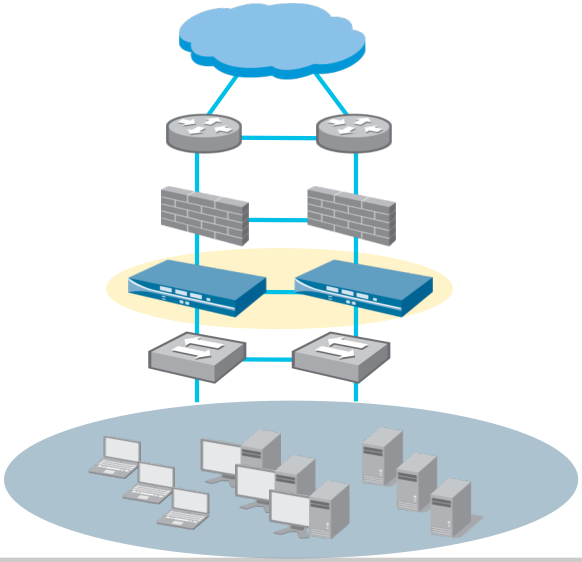
Flexible Deployment Options for Ethernet Interfaces

Tap



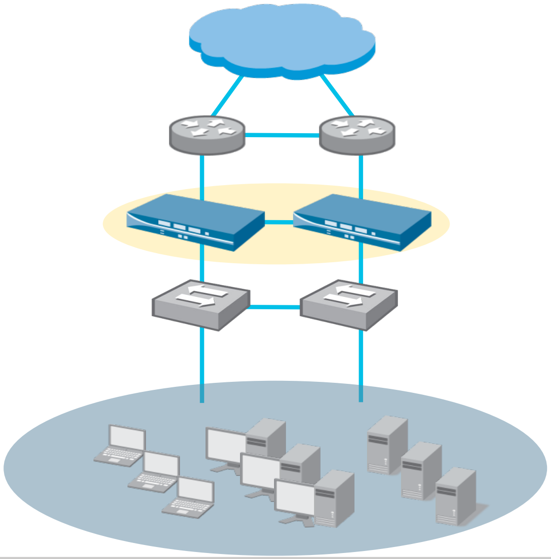
- Application, user, and content visibility without inline deployment
- Used for evaluation and audit of existing networks

Virtual Wire



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

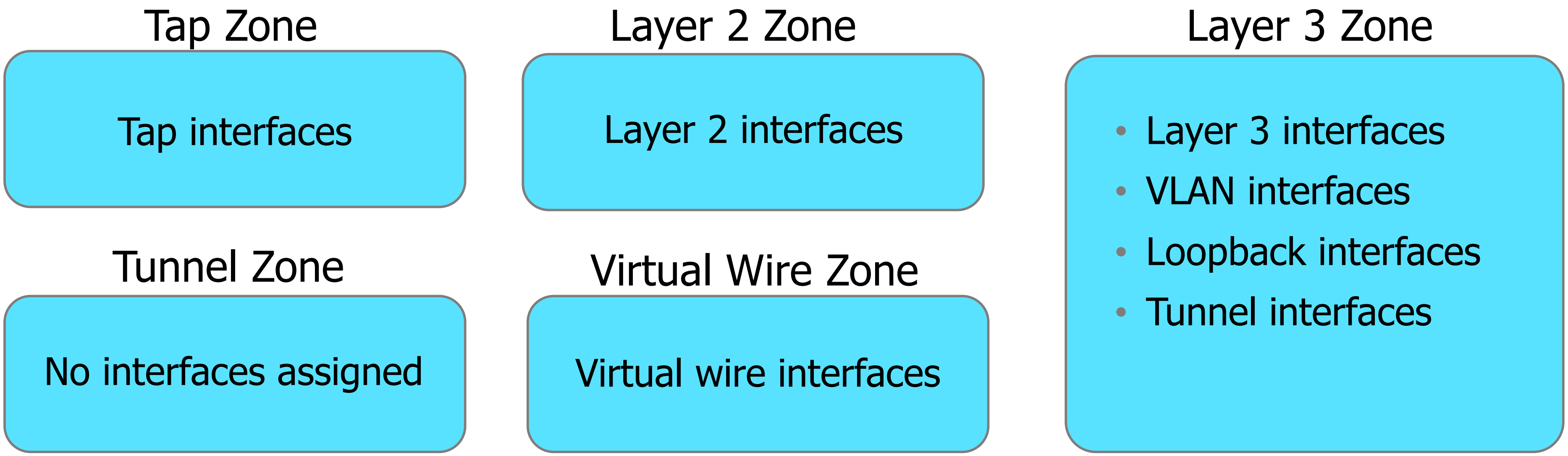
Layer 3



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

Interface Types and Zone Types

Different zone types support only specific interface 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

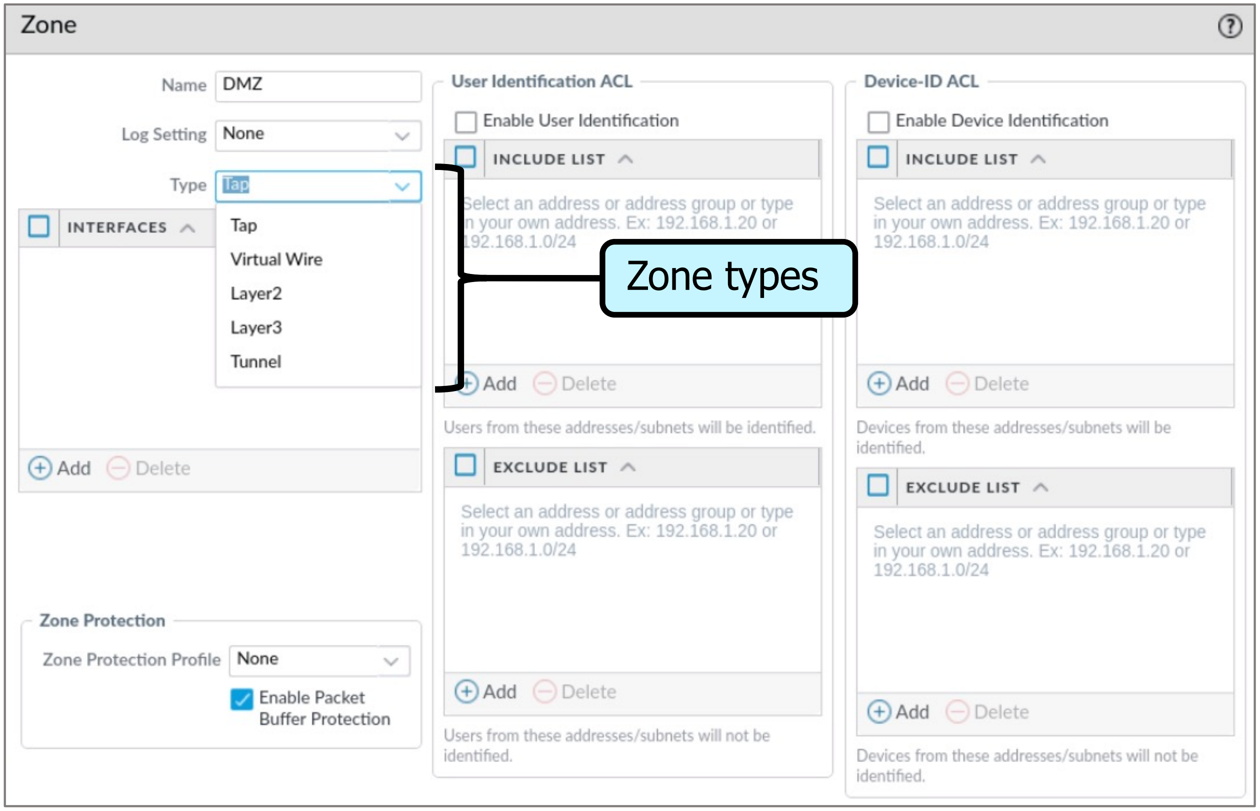
Virtual Wire Zone

Virtual wire interfaces

MGT and HA interfaces are not assigned to a zone.

Create a Security Zone

Network > Zones > Add



Zone

Name: DMZ

Log Setting: None

Type: Tap

Zone types

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.

Device-ID ACL

☐ Enable Device Identification

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

Devices 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

Devices 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.

Blocking threats by using network segmentation

Network interfaces and security zones

Tap interfaces

Virtual wire interfaces

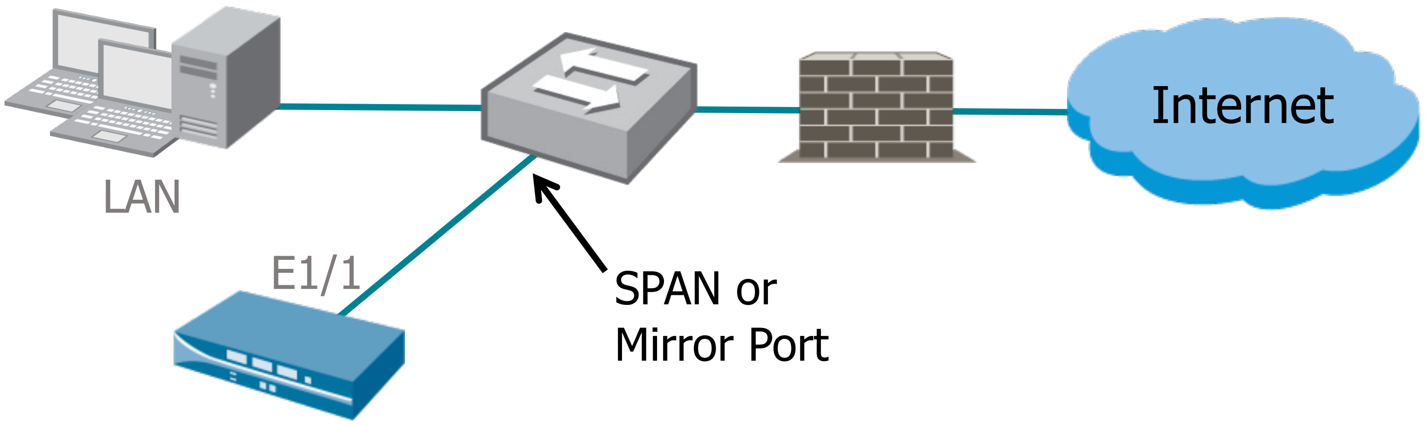
Layer 3 interfaces

Virtual routers

Loopback interfaces

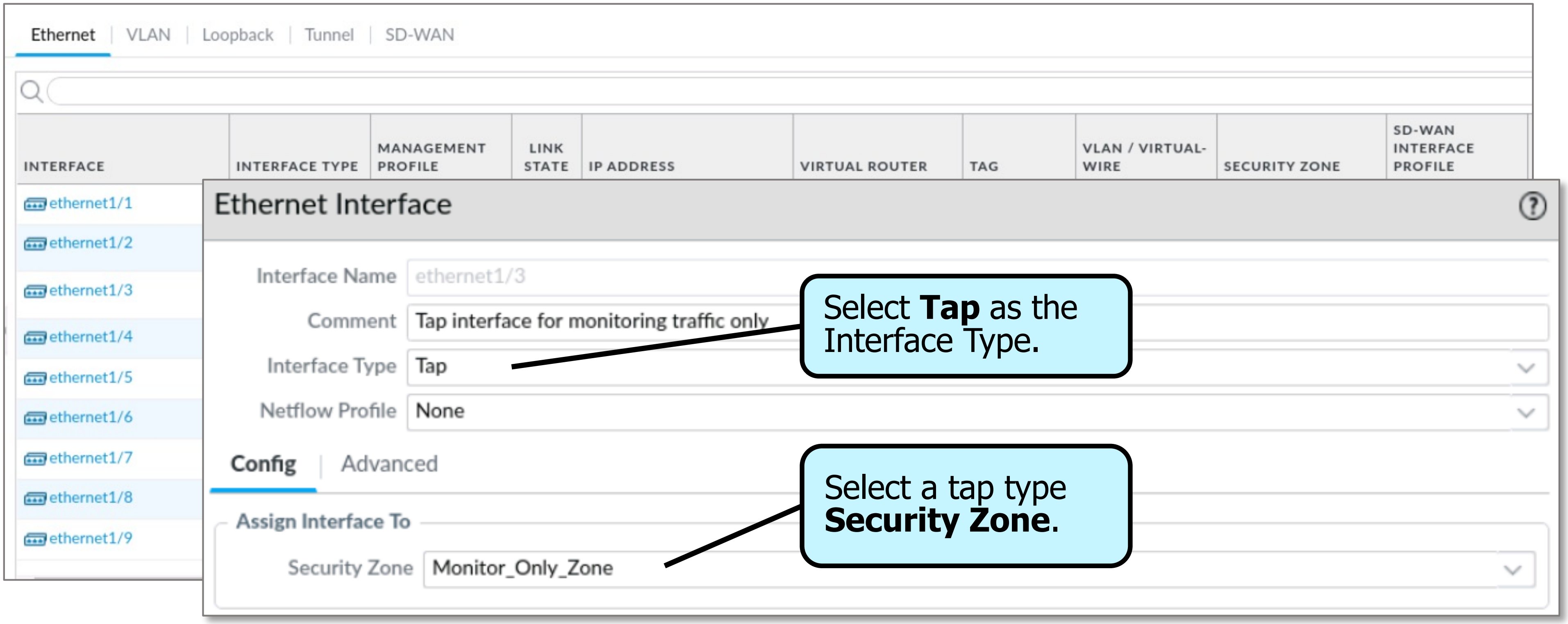
Tap Interfaces

- 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



Configure a Tap Interface

Network > Interfaces > Ethernet > <select_interface>



Ethernet | VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE
ethernet1/1									
ethernet1/2									
ethernet1/3									
ethernet1/4									
ethernet1/5									
ethernet1/6									
ethernet1/7									
ethernet1/8									
ethernet1/9									

Ethernet Interface

Interface Name: ethernet1/3

Comment: Tap interface for monitoring traffic only

Interface Type: Tap

Netflow Profile: None

Config | Advanced

Assign Interface To

Security Zone: Monitor_Only_Zone

Select **Tap** as the Interface Type.

Select a tap type **Security Zone.**

Blocking threats by using network segmentation

Network interfaces and security zones

Tap interfaces

Virtual wire interfaces

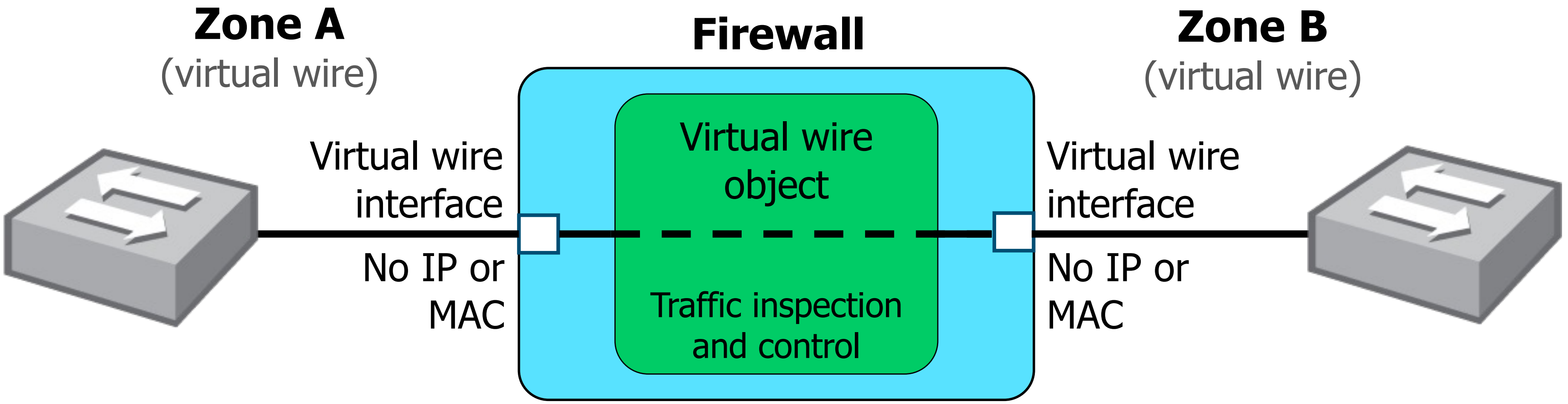
Layer 3 interfaces

Virtual routers

Loopback interfaces

Virtual Wire Interfaces

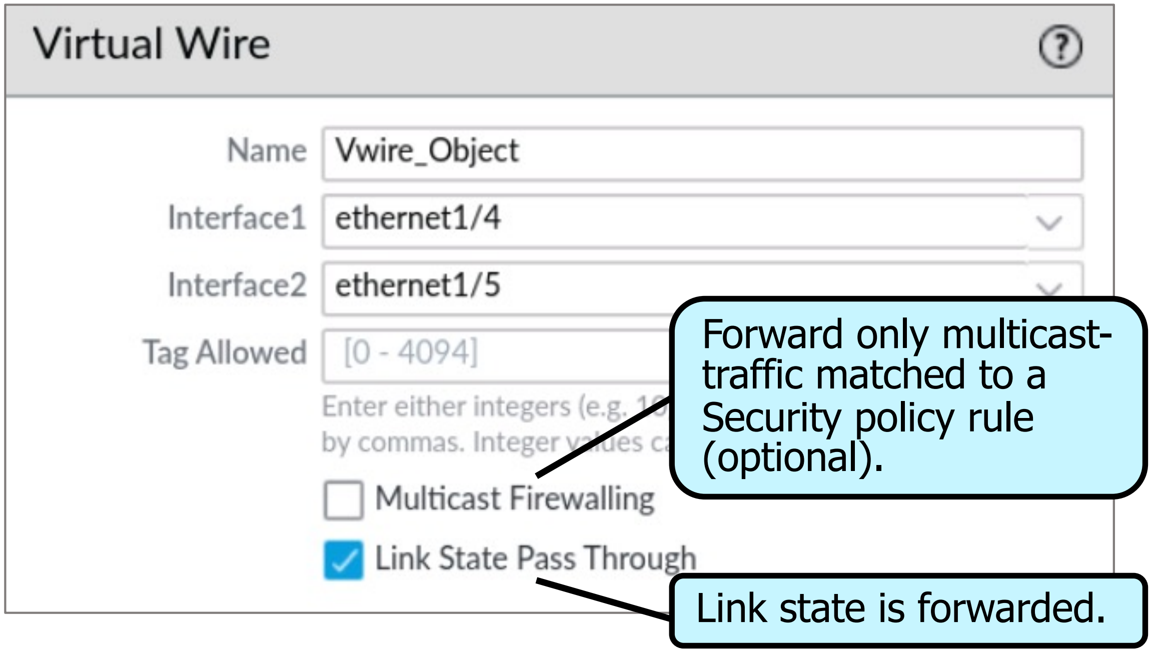
- Bind two firewall interfaces together through a virtual wire object
- Typically used when no switching or routing is needed
- No configuration changes for adjacent network devices



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

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
by commas. Integer values ca

□ Multicast Firewalling

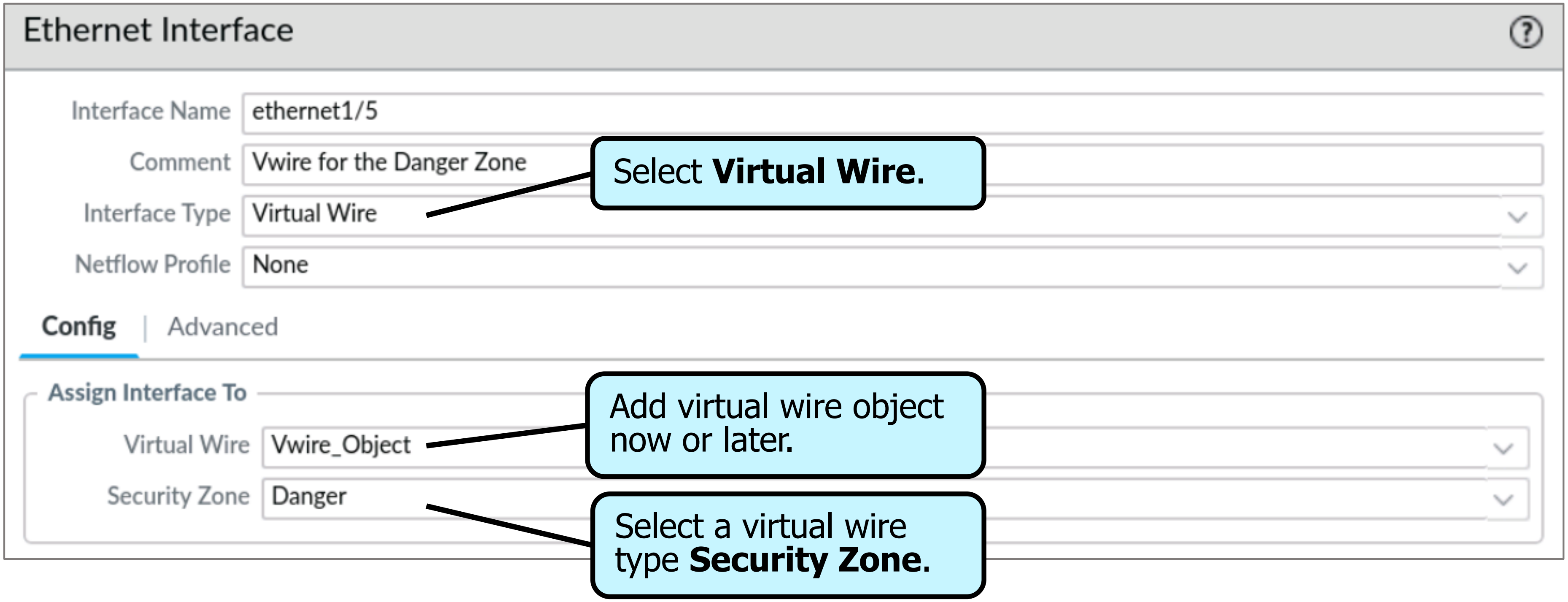
☑ Link State Pass Through

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

Link state is forwarded.

Configure a Virtual Wire Interface

Network > Interfaces > Ethernet > <select_interface>



Ethernet Interface

Interface Name: ethernet1/5

Comment: Vwire for the Danger Zone

Interface Type: Virtual Wire

Netflow Profile: None

Virtual Wire: Vwire_Object

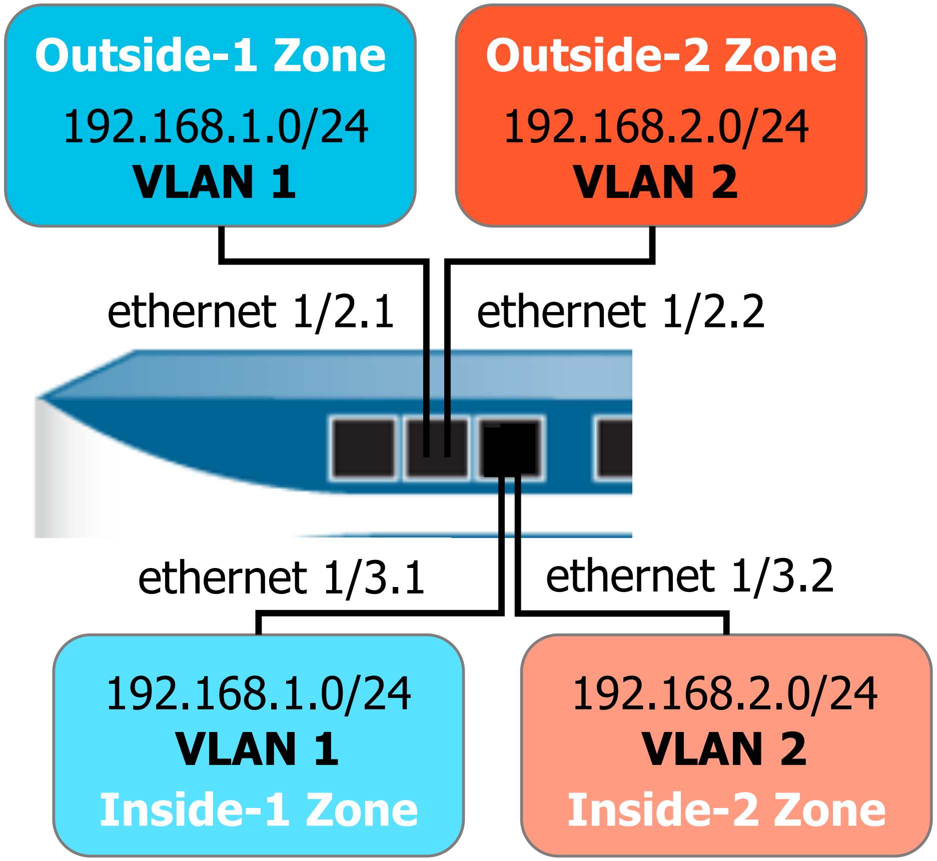
Security Zone: Danger

Select **Virtual Wire.**

Add virtual wire object now or later.

Select a virtual wire type **Security Zone**.

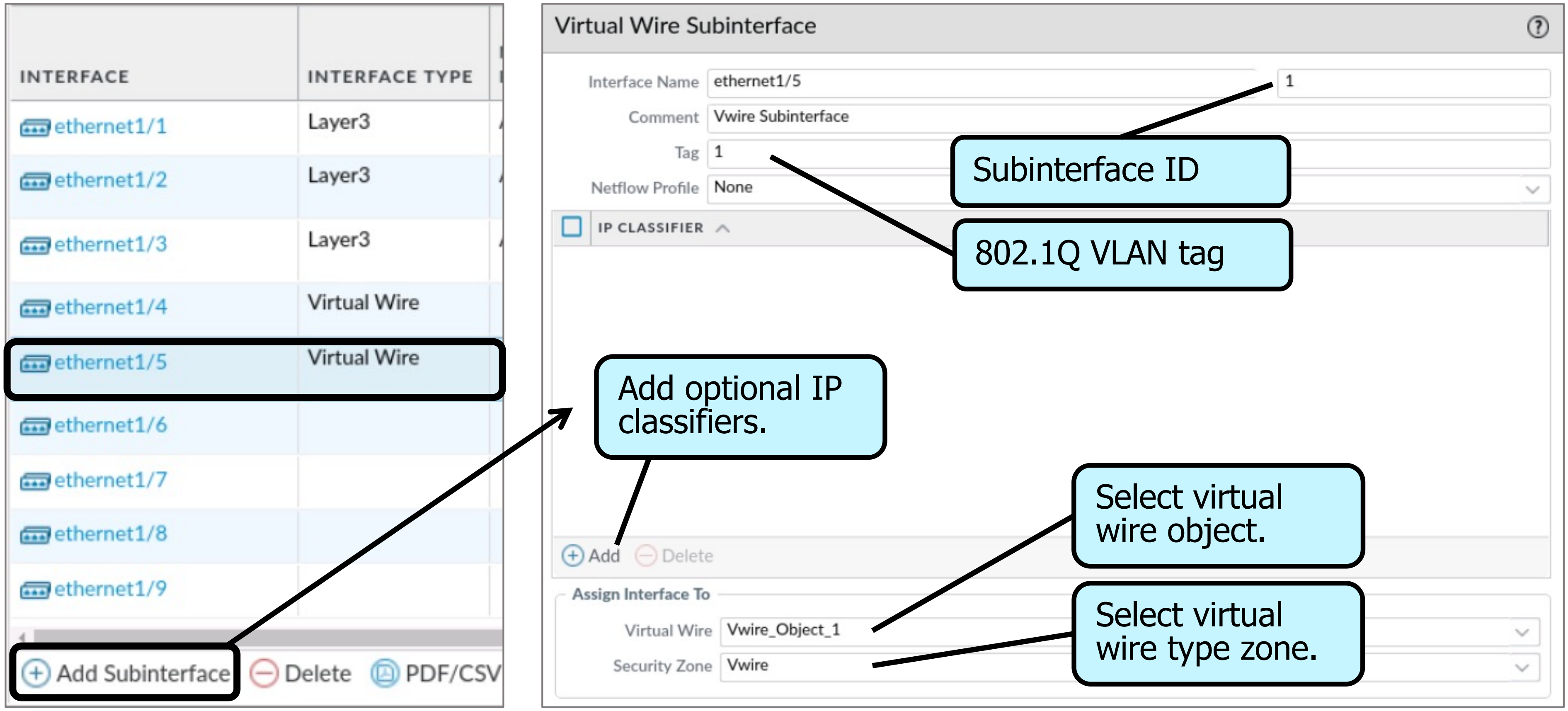
Virtual Wire Subinterfaces



- Assign subinterfaces to zones
- Security policy is required for interzone traffic
- Useful configuration for multi-tenant networks

Configure a Virtual Wire Subinterface

Network > Interfaces > Ethernet



INTERFACE	INTERFACE TYPE
ethernet1/1	Layer3
ethernet1/2	Layer3
ethernet1/3	Layer3
ethernet1/4	Virtual Wire
ethernet1/5	Virtual Wire
ethernet1/6	
ethernet1/7	
ethernet1/8	
ethernet1/9	

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.

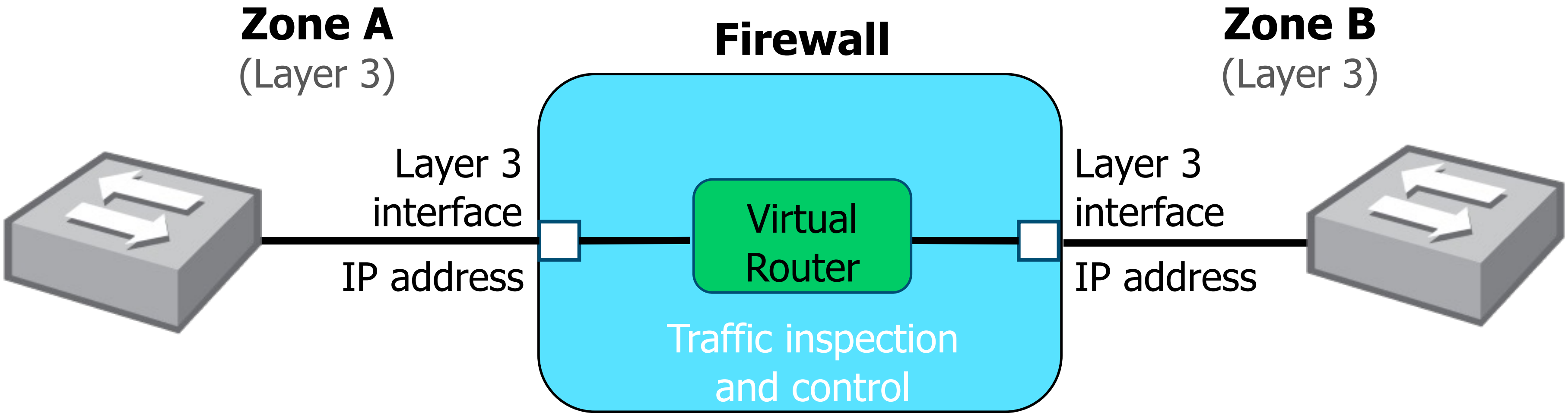
Select virtual wire object.

Select virtual wire type zone.

- Blocking threats by using network segmentation
- Network interfaces and security zones
- Tap interfaces
- Virtual wire interfaces
- **Layer 3 interfaces**
- Virtual routers
- Loopback interfaces

Layer 3 Interfaces

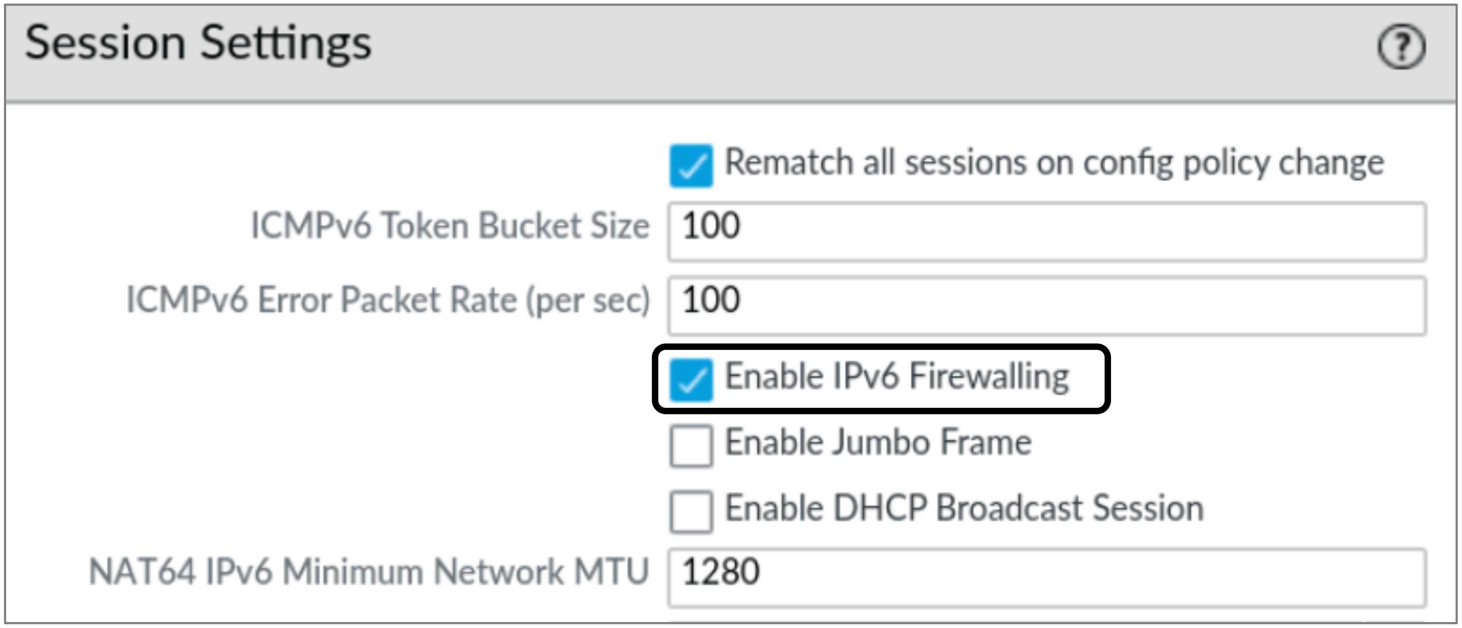
- Enables routing between multiple interfaces:
  - Requires a virtual router configuration
- Can require network configuration to accommodate new IP addresses



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



Session Settings

☑ Rematch all sessions on config policy change

ICMPv6 Token Bucket Size: 100

ICMPv6 Error Packet Rate (per sec): 100

☑ Enable IPv6 Firewalling

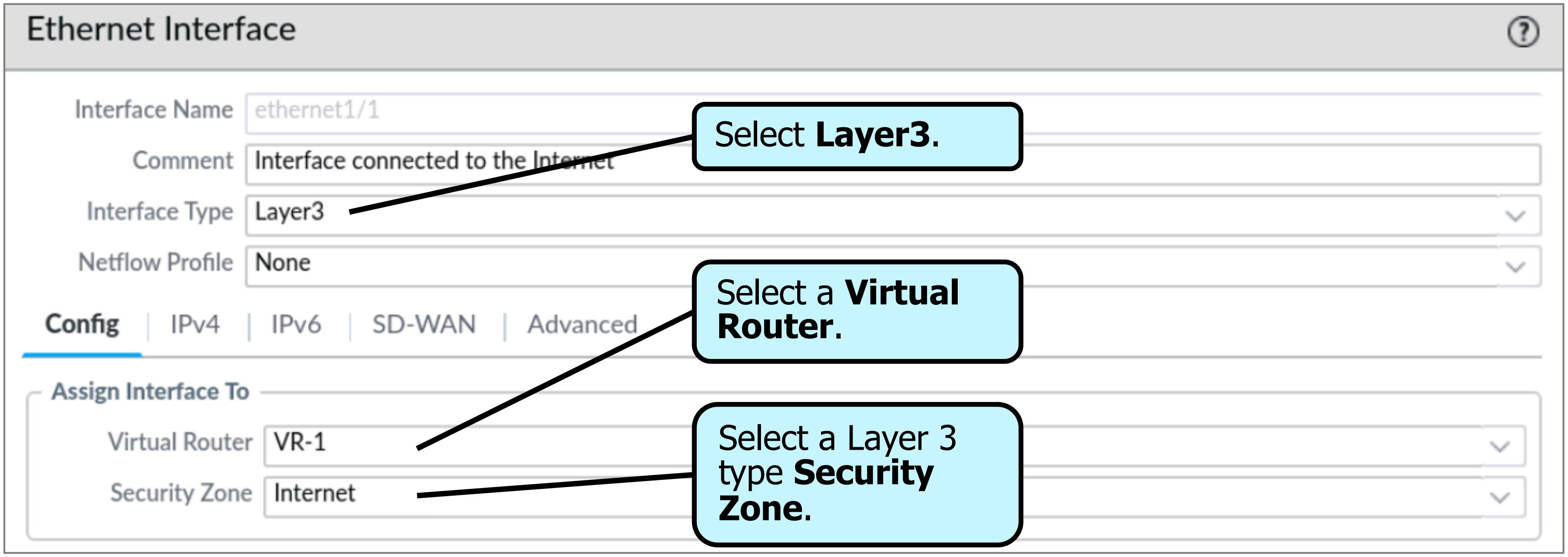
□ Enable Jumbo Frame

□ Enable DHCP Broadcast Session

NAT64 IPv6 Minimum Network MTU: 1280

Configure a Layer 3 Interface: Config

Network > Interfaces > Ethernet > <select_interface>



Ethernet Interface

Interface Name: ethernet1/1

Comment: Interface connected to the Internet

Interface Type: Layer3

Netflow Profile: None

Assign Interface To

Virtual Router: VR-1

Security Zone: Internet

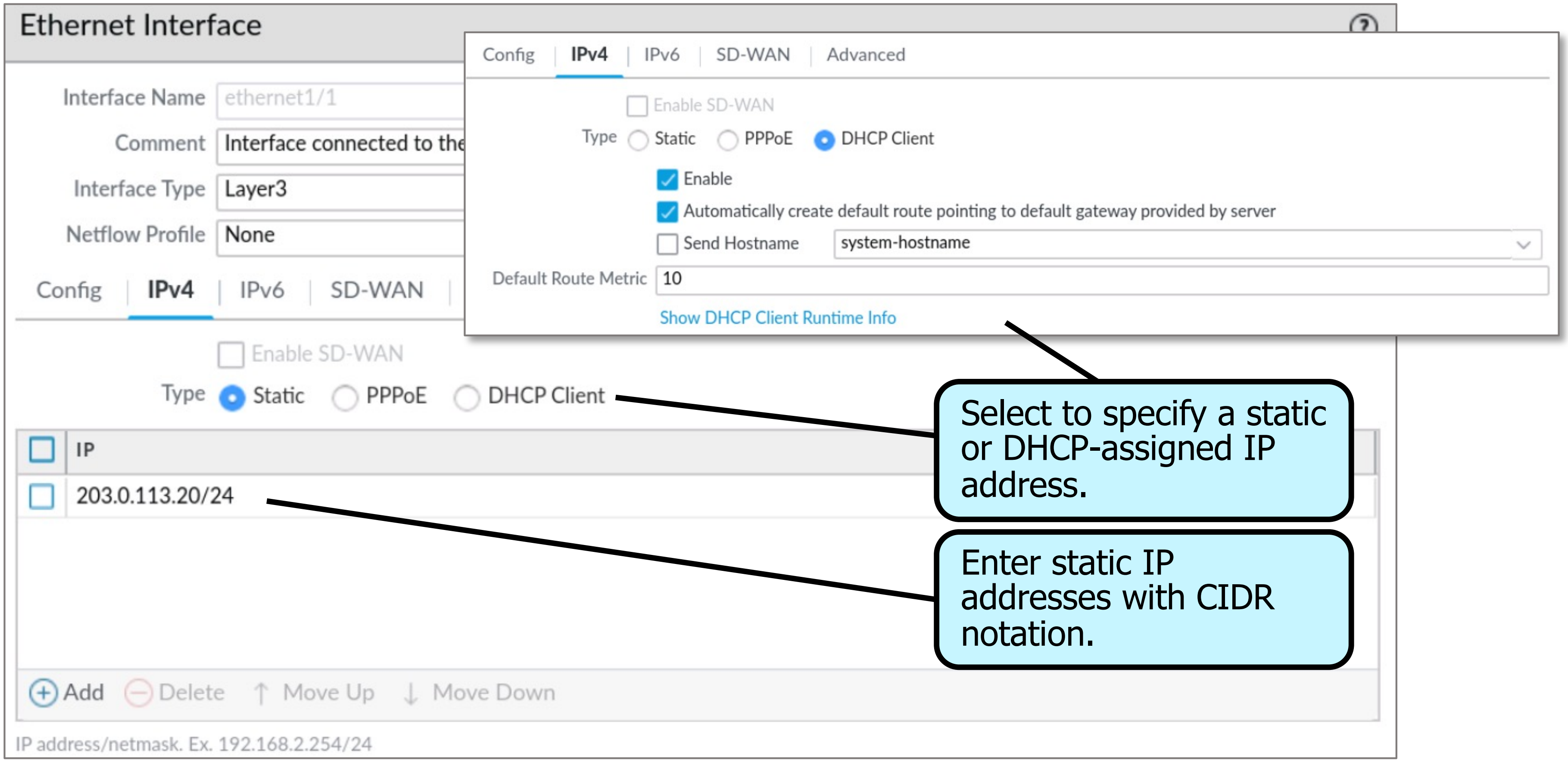
Select **Layer3**.

Select a **Virtual Router**.

Select a Layer 3 type **Security Zone**.

Configure a Layer 3 Interface: IPv4

Network > Interfaces > Ethernet > <select_interface>



Ethernet Interface

Interface Name: ethernet1/1

Comment: Interface connected to the

Interface Type: Layer3

Netflow Profile: None

Config | **IPv4** | IPv6 | SD-WAN

□ Enable SD-WAN

Type ● Static ○ PPPoE ○ DHCP Client

□	IP
□	203.0.113.20/24

IP address/netmask. Ex. 192.168.2.254/24

Config | **IPv4** | IPv6 | SD-WAN | Advanced

□ Enable SD-WAN

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

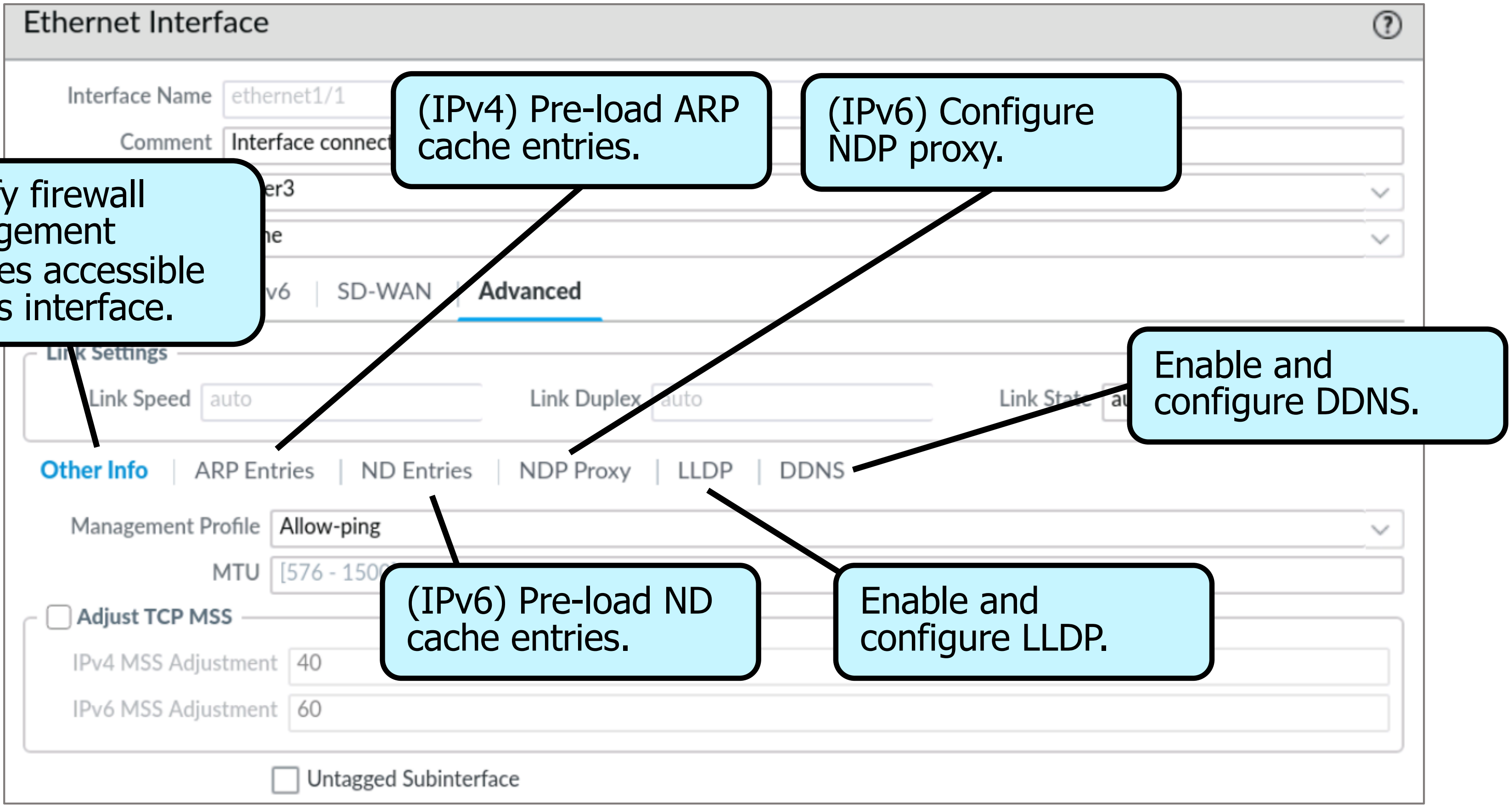
Show DHCP Client Runtime Info

Select to specify a static or DHCP-assigned IP address.

Enter static IP addresses with CIDR notation.

Configure a Layer 3 Interface: Advanced

Network > Interfaces > Ethernet > <select_interface>



Specify firewall management services accessible on this interface.

(IPv4) Pre-load ARP cache entries.

(IPv6) Configure NDP proxy.

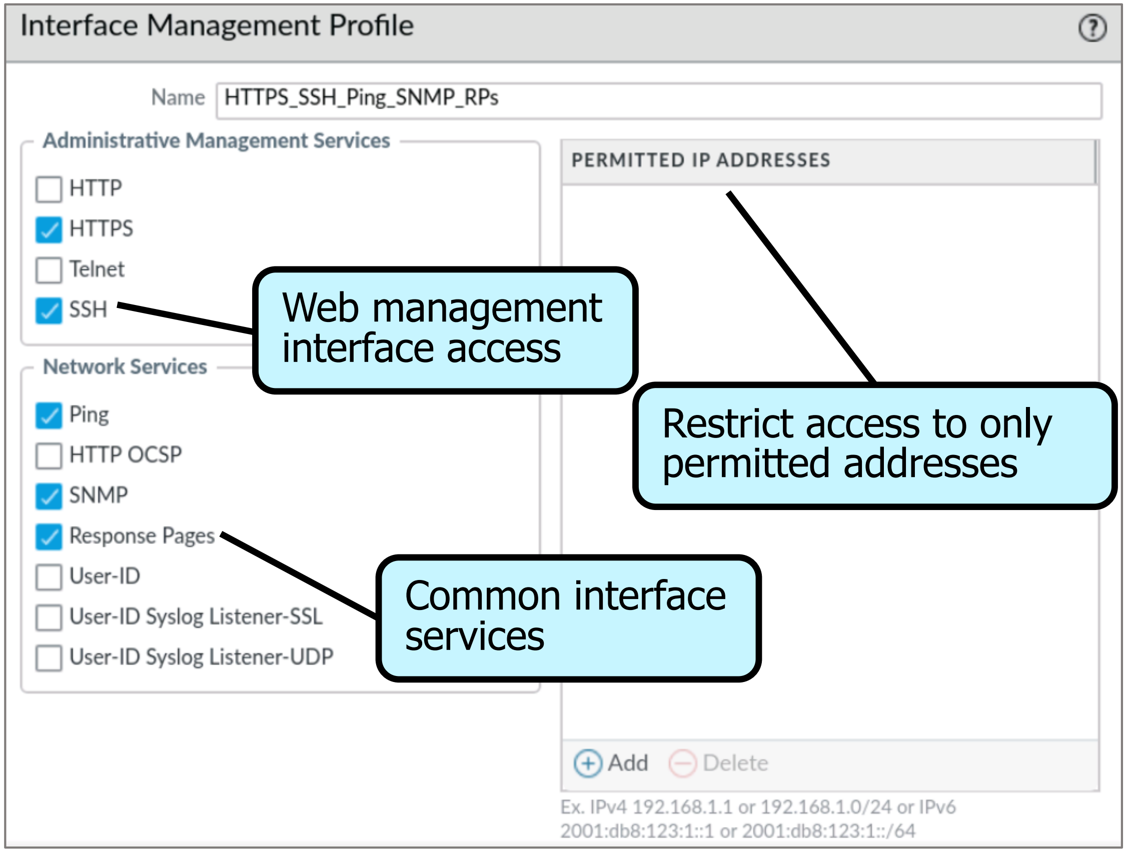
Enable and configure DDNS.

(IPv6) Pre-load ND cache entries.

Enable and configure LLDP.

Interface Management Profile

Network > Network Profiles > Interface Mgmt > Add



Interface Management Profile

Name: HTTPS_SSH_Ping_SNMP_RPs

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

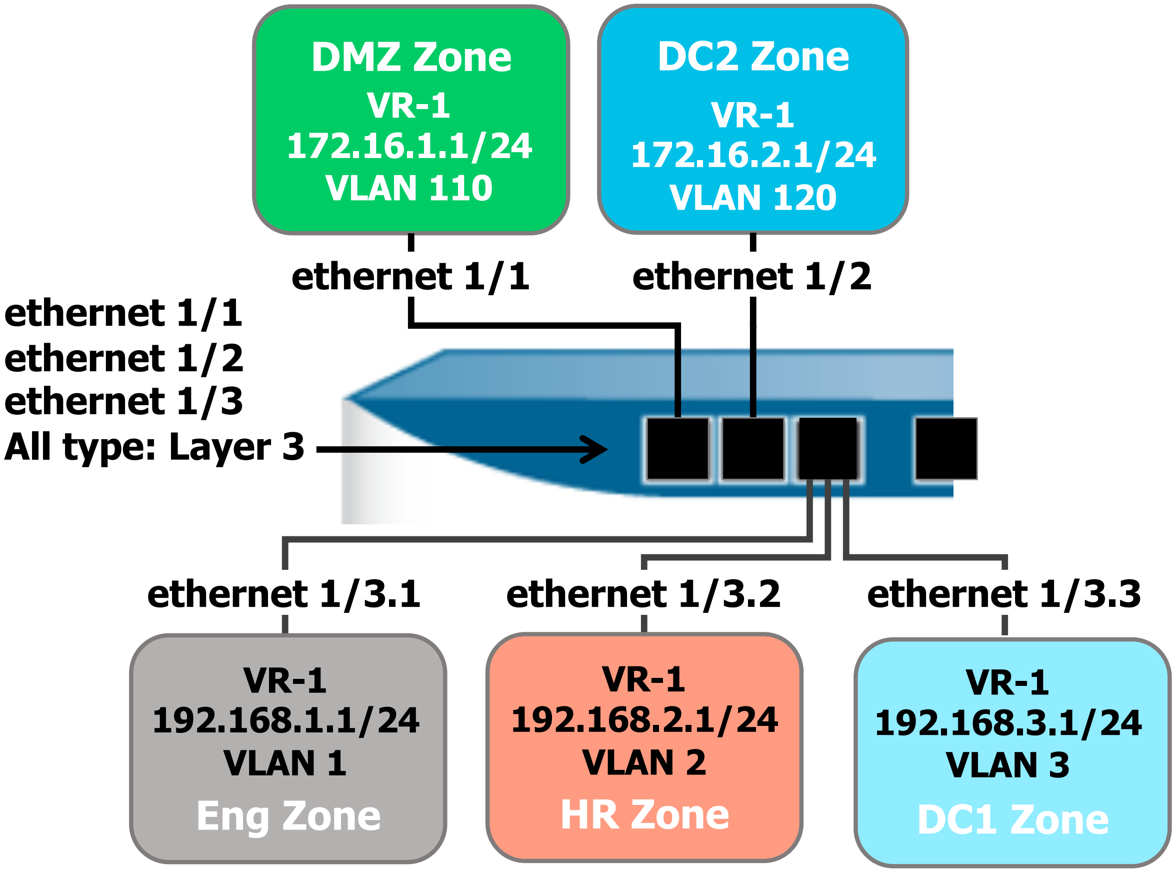
Web management interface access

Restrict access to only permitted addresses

Common interface services

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

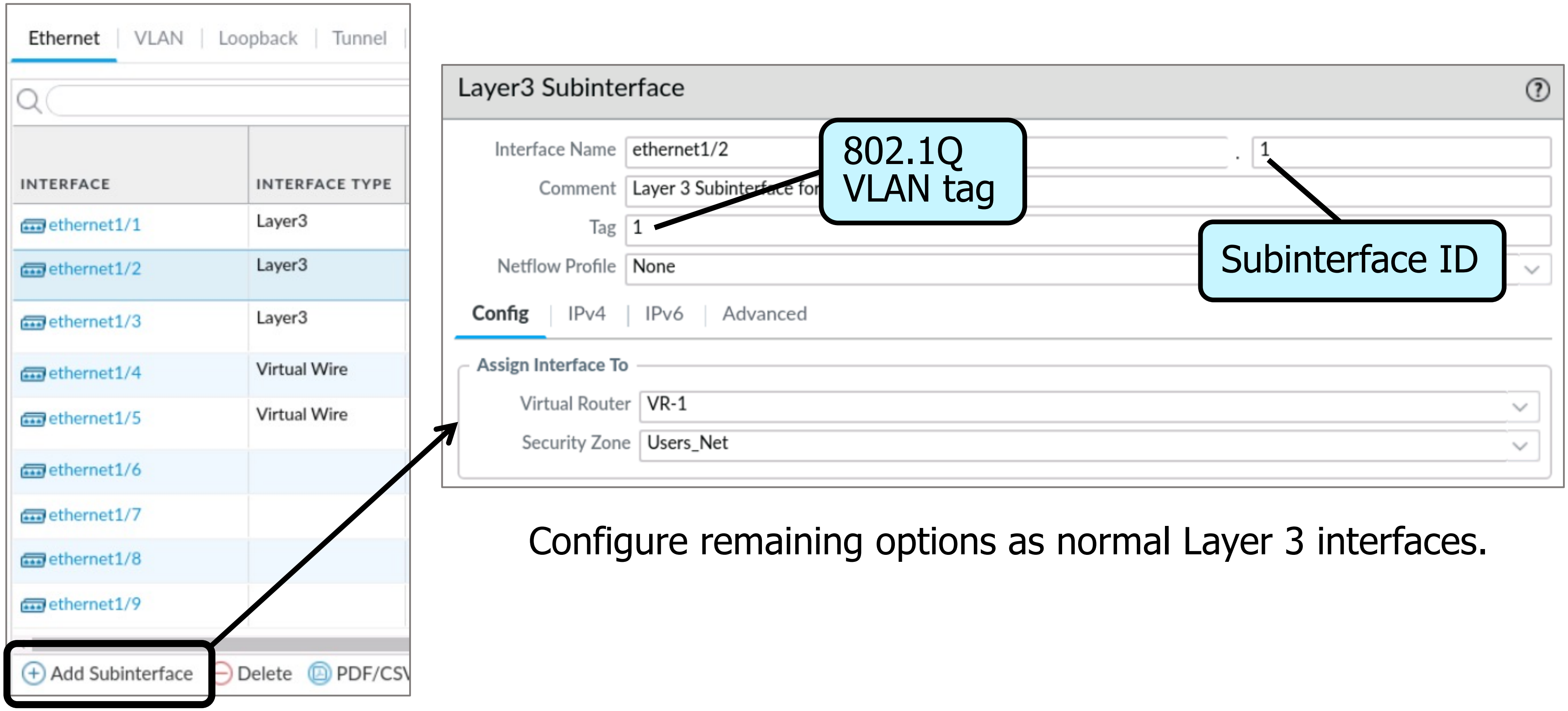
Layer 3 Subinterfaces



- 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

Configure a Layer 3 Subinterface

Network > Interfaces > Ethernet



Ethernet | VLAN | Loopback | Tunnel

INTERFACE	INTERFACE TYPE
ethernet1/1	Layer3
ethernet1/2	Layer3
ethernet1/3	Layer3
ethernet1/4	Virtual Wire
ethernet1/5	Virtual Wire
ethernet1/6	
ethernet1/7	
ethernet1/8	
ethernet1/9	

Add Subinterface
Delete
PDF/CSV

Layer3 Subinterface

Interface Name: ethernet1/2 . 1

Comment: Layer 3 Subinterface for

Tag: 1

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: VR-1

Security Zone: Users_Net

802.1Q VLAN tag

Subinterface ID

Configure remaining options as normal Layer 3 interfaces.

Blocking threats by using network segmentation

Network interfaces and security zones

Tap interfaces

Virtual wire interfaces

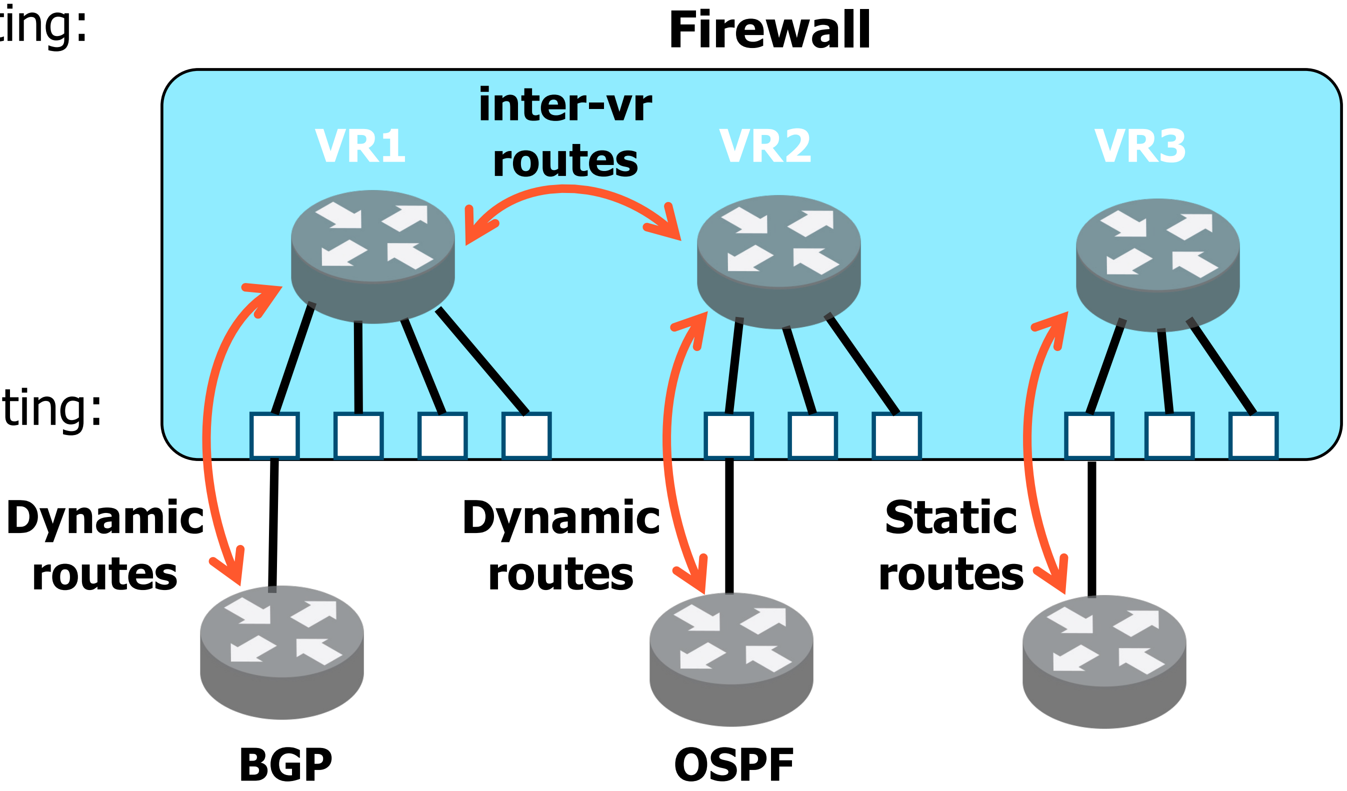
Layer 3 interfaces

Virtual routers

Loopback interfaces

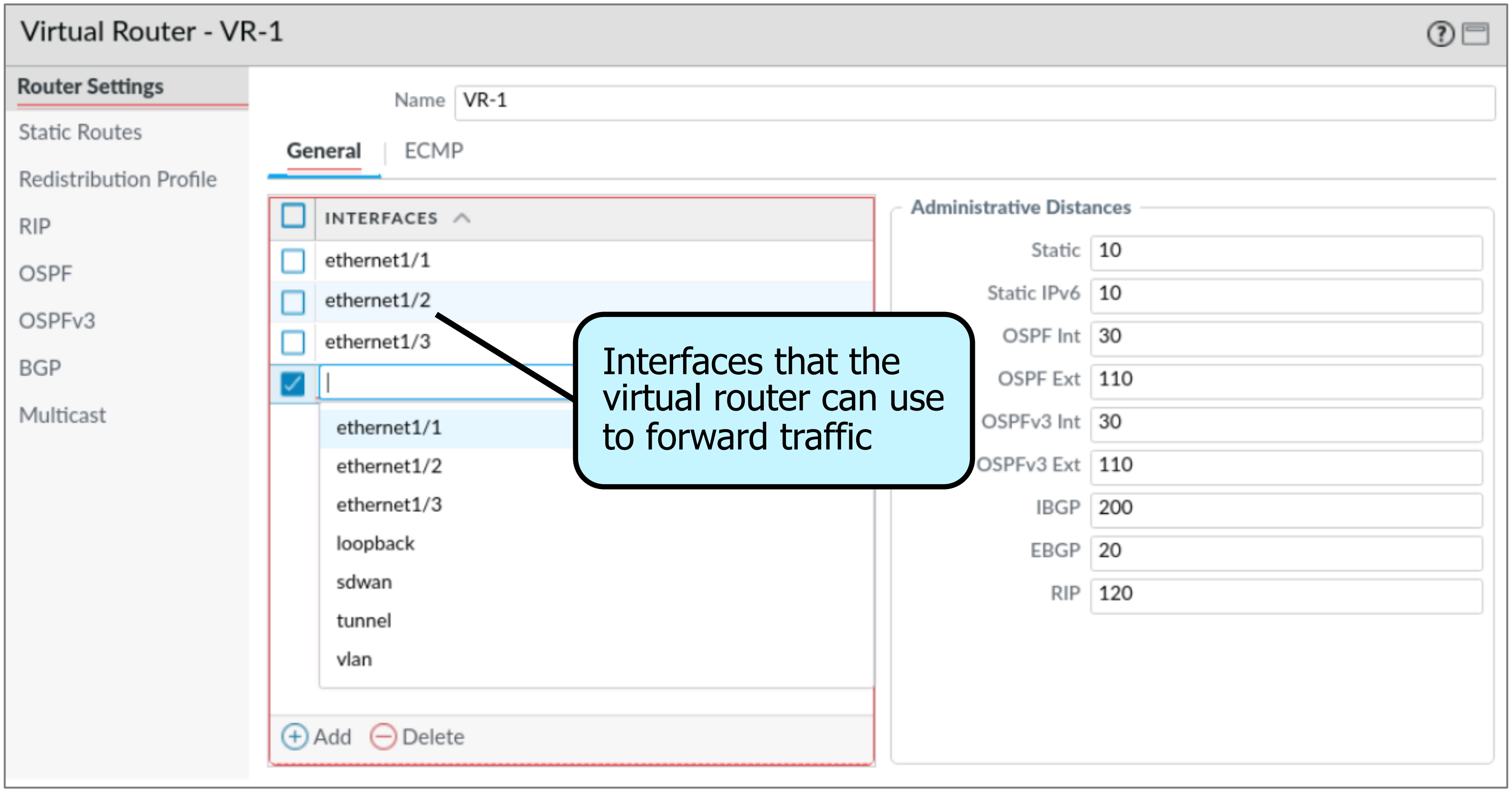
Virtual Routers

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



Virtual Router General Settings

Network > Virtual Routers



Name: VR-1

□	INTERFACES
□	ethernet1/1
□	ethernet1/2
□	ethernet1/3
☑	

Dropdown options: ethernet1/1, ethernet1/2, ethernet1/3, loopback, sdwan, tunnel, vlan

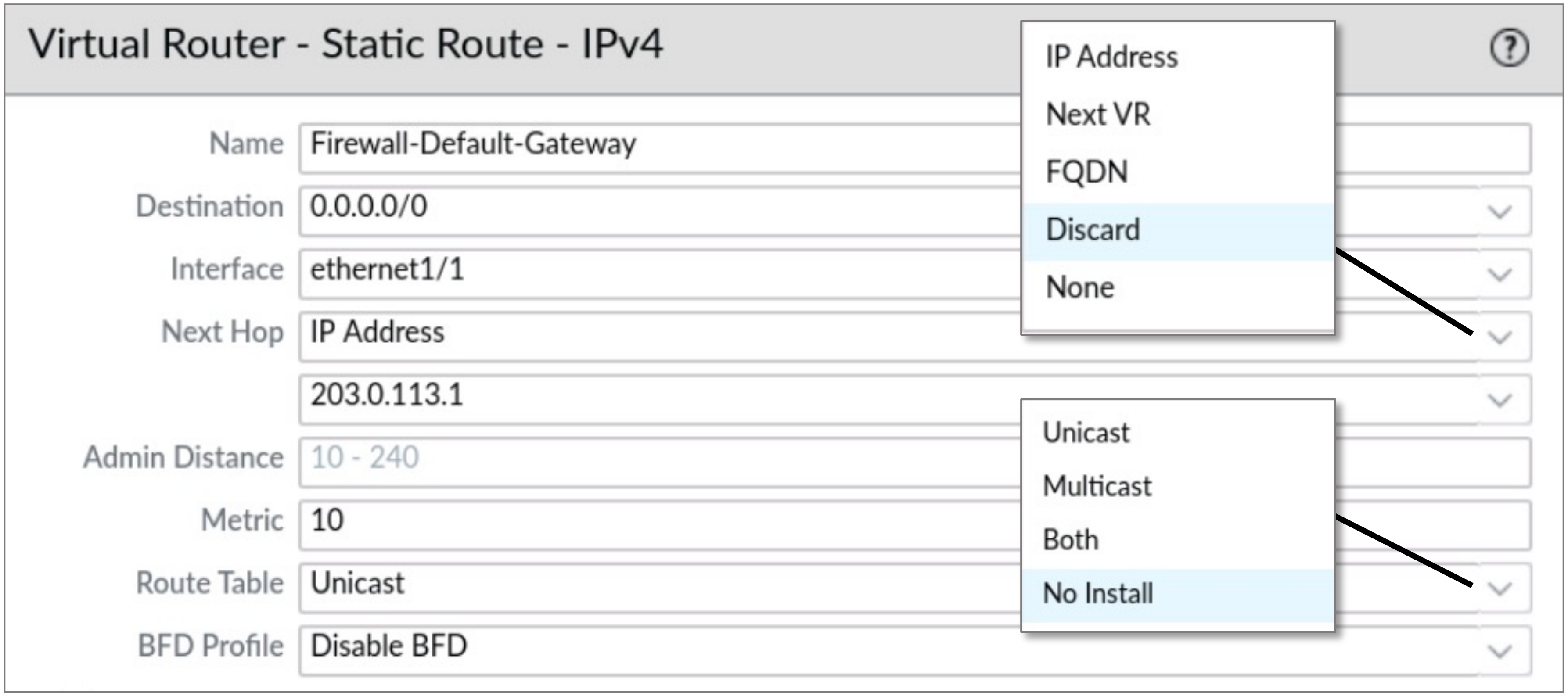
Administrative Distances

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

Add a Static Default Route

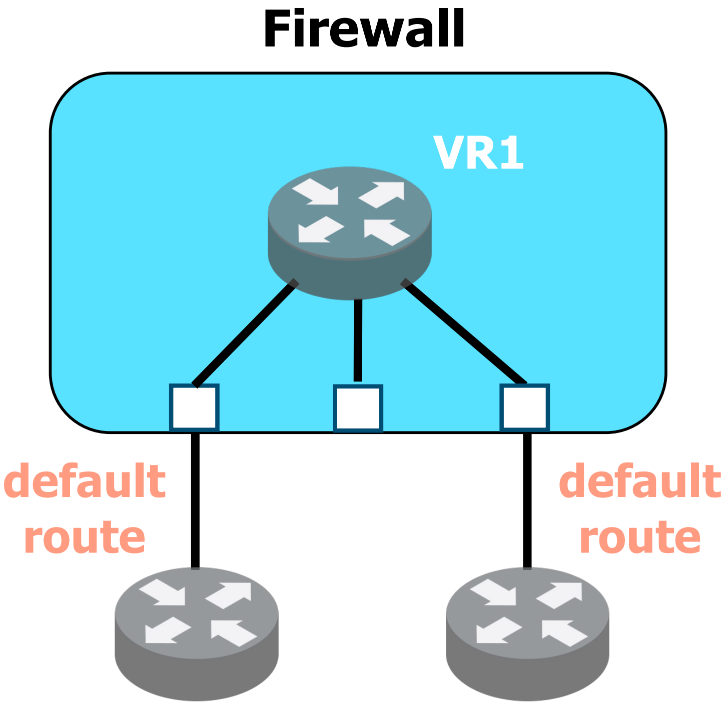
Network > Virtual Routers > Static Routes > Add



Virtual Router - Static Route - IPv4

Name	Firewall-Default-Gateway
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

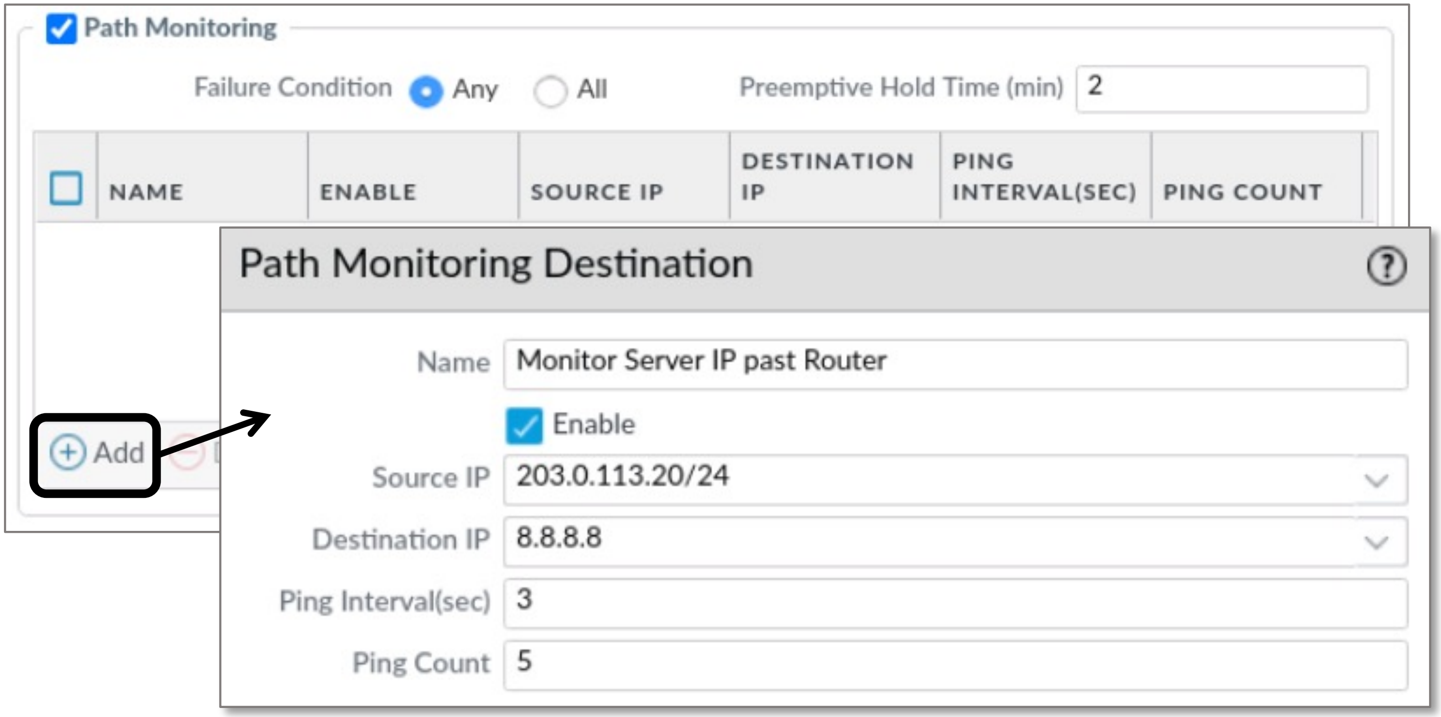
Multiple Static Default Routes



- 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.

Static Route Path Monitoring

Network > Virtual Routers > Static Routes > Add



☑ Path Monitoring

Failure Condition ● Any ○ All

Preemptive Hold Time (min) 2

□	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

Path Monitoring Destination

Name: Monitor Server IP past Router

☑ Enable

Source IP: 203.0.113.20/24

Destination IP: 8.8.8.8

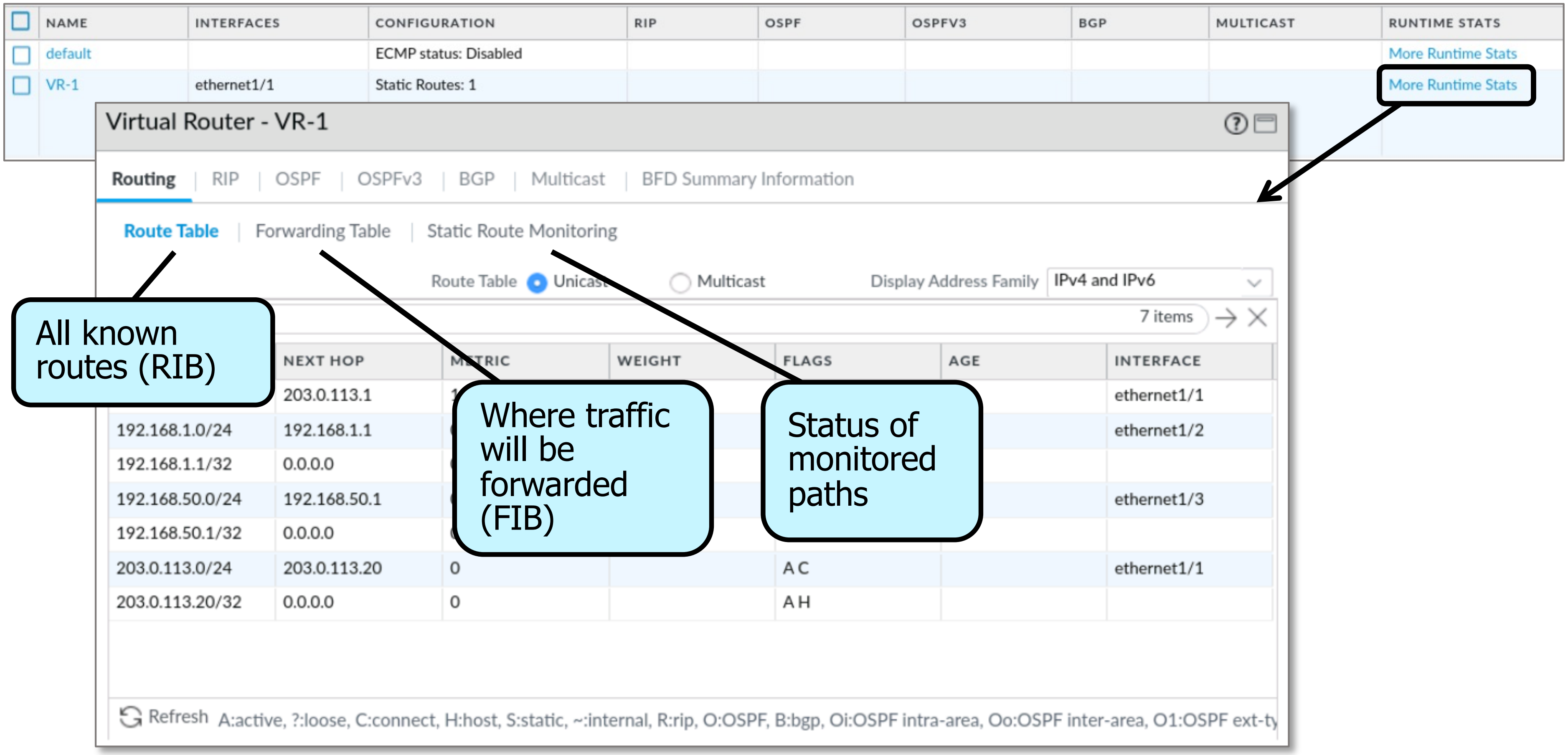
Ping Interval(sec): 3

Ping Count: 5

- Uses ping to test reachability to stable upstream devices.
- Testing continues after failure.
- Will remove or re-add static routes.

Troubleshoot Routing

Network > Virtual Routers



□	NAME	INTERFACES	CONFIGURATION	RIP	OSPF	OSPFV3	BGP	MULTICAST	RUNTIME STATS
□	default		ECMP status: Disabled						More Runtime Stats
□	VR-1	ethernet1/1	Static Routes: 1						More Runtime Stats

Virtual Router - VR-1

Routing | RIP | OSPF | OSPFv3 | BGP | Multicast | BFD Summary Information
Route Table | Forwarding Table | Static Route Monitoring

Route Table ● Unicast ○ Multicast   Display Address Family: IPv4 and IPv6

7 items

	NEXT HOP	METRIC	WEIGHT	FLAGS	AGE	INTERFACE
	203.0.113.1	1				ethernet1/1
192.168.1.0/24	192.168.1.1	0				ethernet1/2
192.168.1.1/32	0.0.0.0	0				
192.168.50.0/24	192.168.50.1	0				ethernet1/3
192.168.50.1/32	0.0.0.0	0				
203.0.113.0/24	203.0.113.20	0		A C		ethernet1/1
203.0.113.20/32	0.0.0.0	0		A H		

Refresh A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:OSPF, B:bgp, Oi:OSPF intra-area, Oo:OSPF inter-area, O1:OSPF ext-ty

All known routes (RIB)

Where traffic will be forwarded (FIB)

Status of monitored paths

Blocking threats by using network segmentation

Network interfaces and security zones

Tap interfaces

Virtual wire interfaces

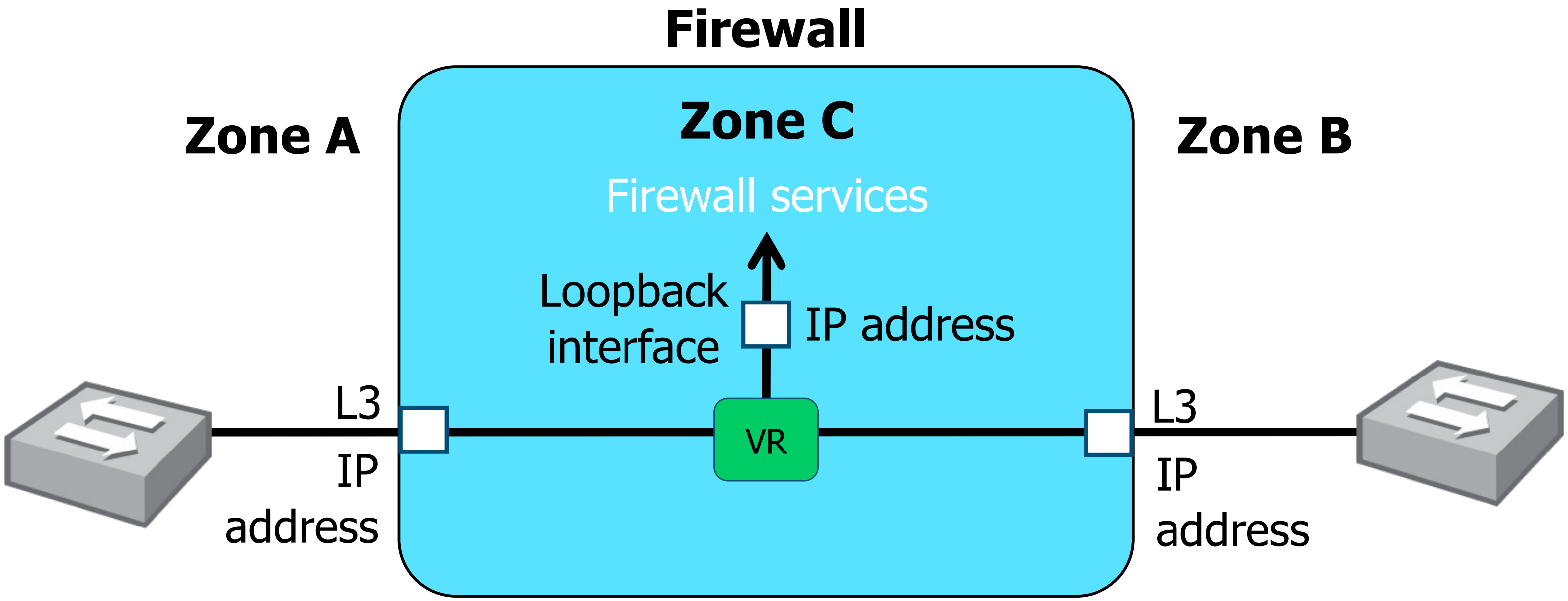
Layer 3 interfaces

Virtual routers

Loopback interfaces

Loopback Interface

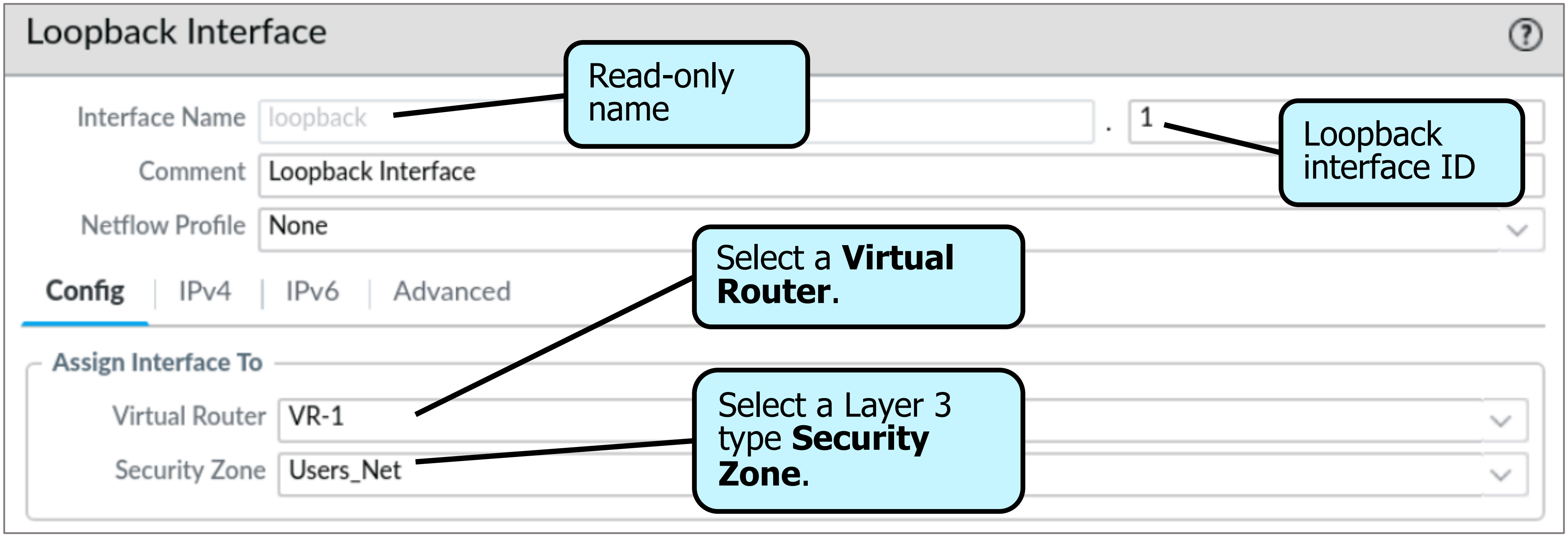
- Logical interface with an IP address
- Behaves like a host interface
- Used to provide access to firewall services



|

Configure a Loopback Interface

Network > Interfaces > Loopback > Add



Loopback Interface

Interface Name: loopback . 1

Comment: Loopback Interface

Netflow Profile: None

Assign Interface To

Virtual Router: VR-1

Security Zone: Users_Net

Read-only name

Loopback interface ID

Select a **Virtual Router**.

Select a Layer 3 type **Security Zone**.

Do not assign a netmask to the IP addresses.

|

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
- Configure a loopback interface to support external connections to internal firewall services

Questions

Lab 5: Connecting the Firewall to Production Networks

- Create Layer 3 Network Interfaces
- Create a Virtual Router
- Segment Your Production Network Using Security Zones
- Test Connectivity to Each Zone
- Create Interface Management Profiles
- Test Interface Access Before Management Profiles
- Define Interface Management Profiles
- Apply Interface Management Profiles
- Test Interface Access After Management Profiles

Protecting our digital way of life.