

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC

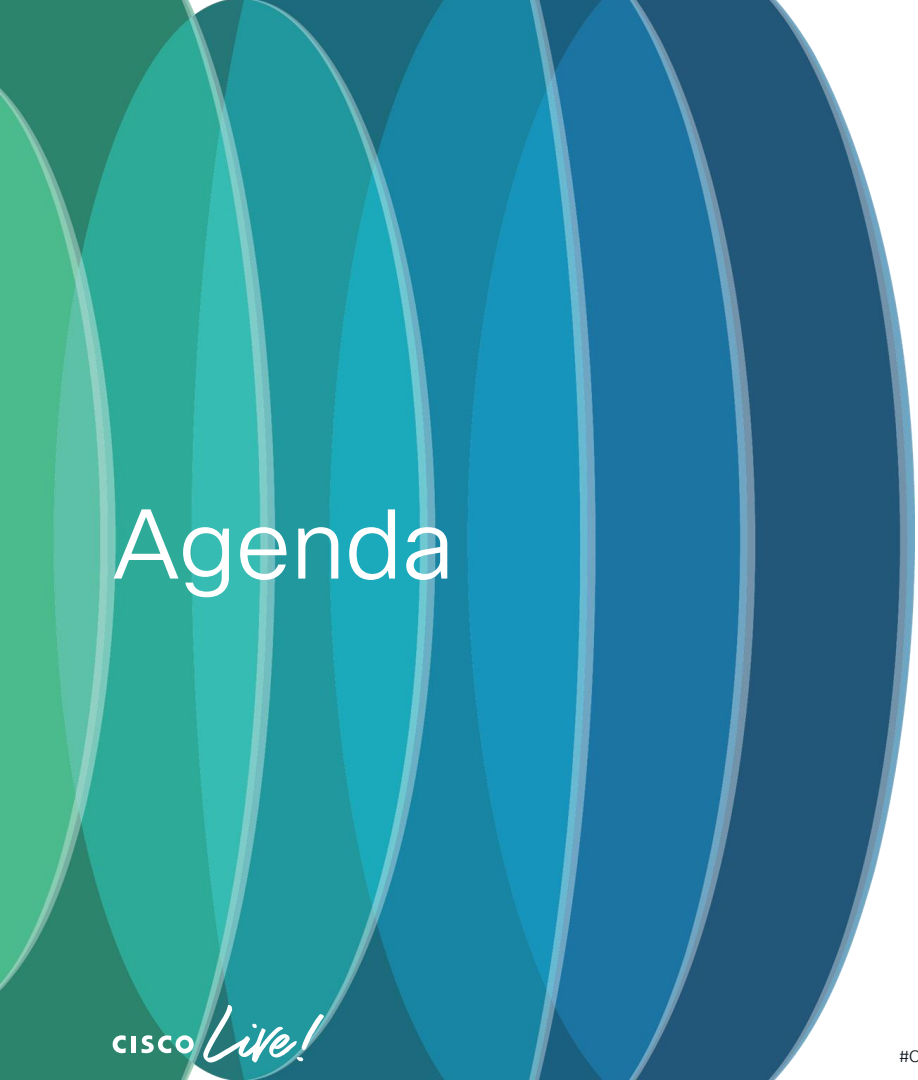


Building SDWANs with Cisco Firewall!

Jeff Fanelli
Distinguished Solutions Engineer
@jefanell
BRKSEC-2018

CISCO *Live!*

#CiscoLiveAPJC



Agenda

- Direct Internet Access (DIA)
- PBR with Path Monitoring
- Simplified Branch to Hub Communication using DVTI
- SASE / Security Service Edge integration
- Monitoring & Troubleshooting

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2018>



About me

Jeff Fanelli

- jefanell@cisco.com
- Distinguished Solutions Engineer
- 19 years @ Cisco
- 40+ Cisco Live & Cisco Connect Presenter
- Husband + father
- Instrument-rated pilot
- Sausage dog servant



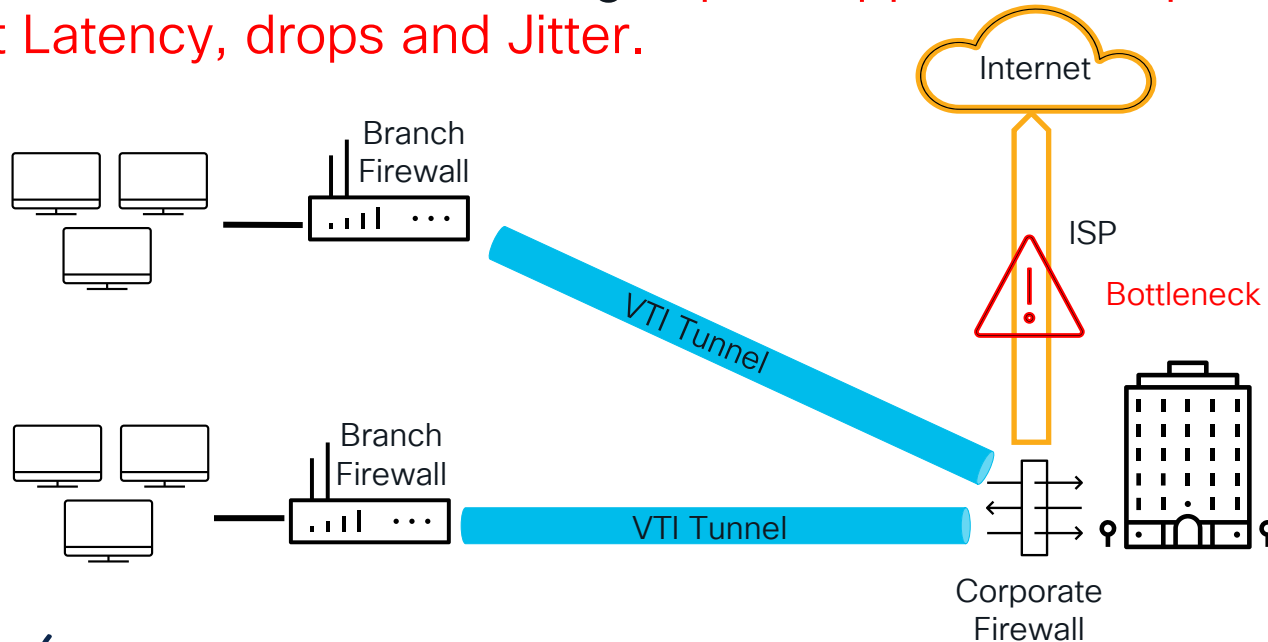
cisco *Live!*

Direct Internet Access Introduction

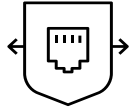
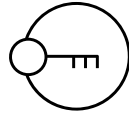
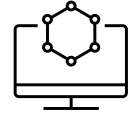


Traditional WAN Architecture

Traditional WAN topology backhauls all internet traffic to the enterprise Data center, resulting in **poor application experience, Packet Latency, drops and Jitter.**



Simplifying Branch Deployments



Secure Elastic Connectivity

- Route Based VPN VTI tunnels between branches (Spokes) to headquarters (Hubs)
- EIGRP and OSPF over VTI
- DVTI support DHCP

WAN Optimisation

- Dual ISP configuration
- Active-Standby Backup VTI tunnel configuration with SLA monitoring
- Optimal Path Selection based on interface Monitoring

Increased Usable Bandwidth

- Increased support for load-balancing across multiple ISPs
- ECMP Support for VTI
- Application based load balancing using Policy Based Routing (PBR)

Direct Internet Access for Public cloud

- SaaS Application detection (First Packet using AVC)
- DNS Snooping using trusted DNS Servers
- PBR using Application as matching criteria

Simplified Management

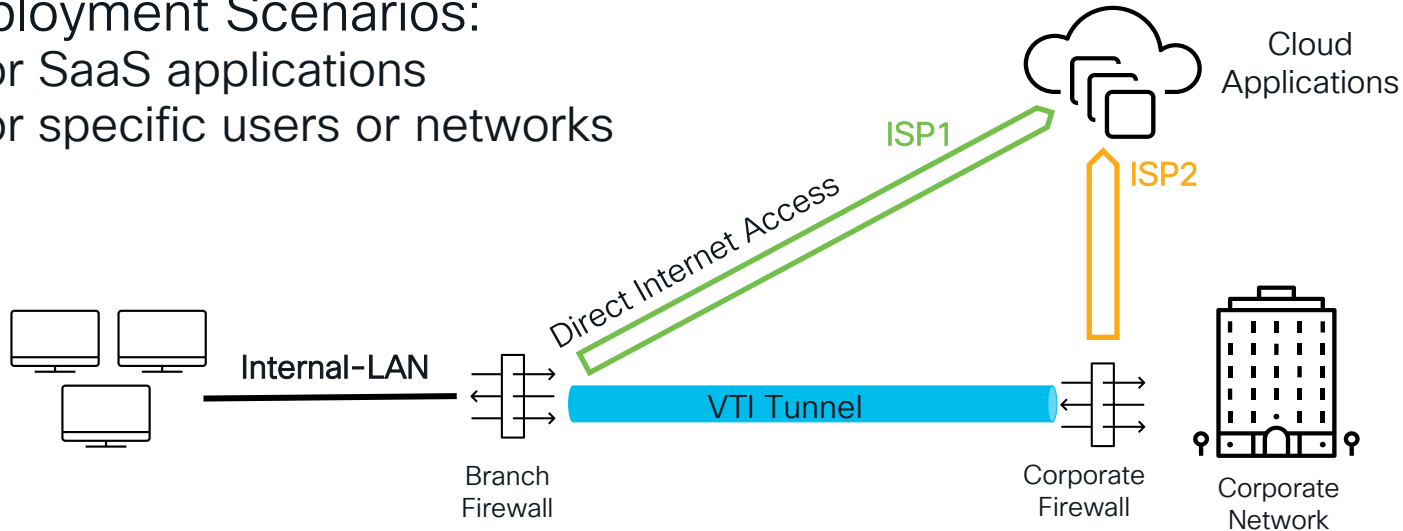
- Data Interface Management
- SASE: Umbrella Auto-Tunnel deployment
- DVTI Hub and Spoke topology simplification

Direct Internet Access (DIA)

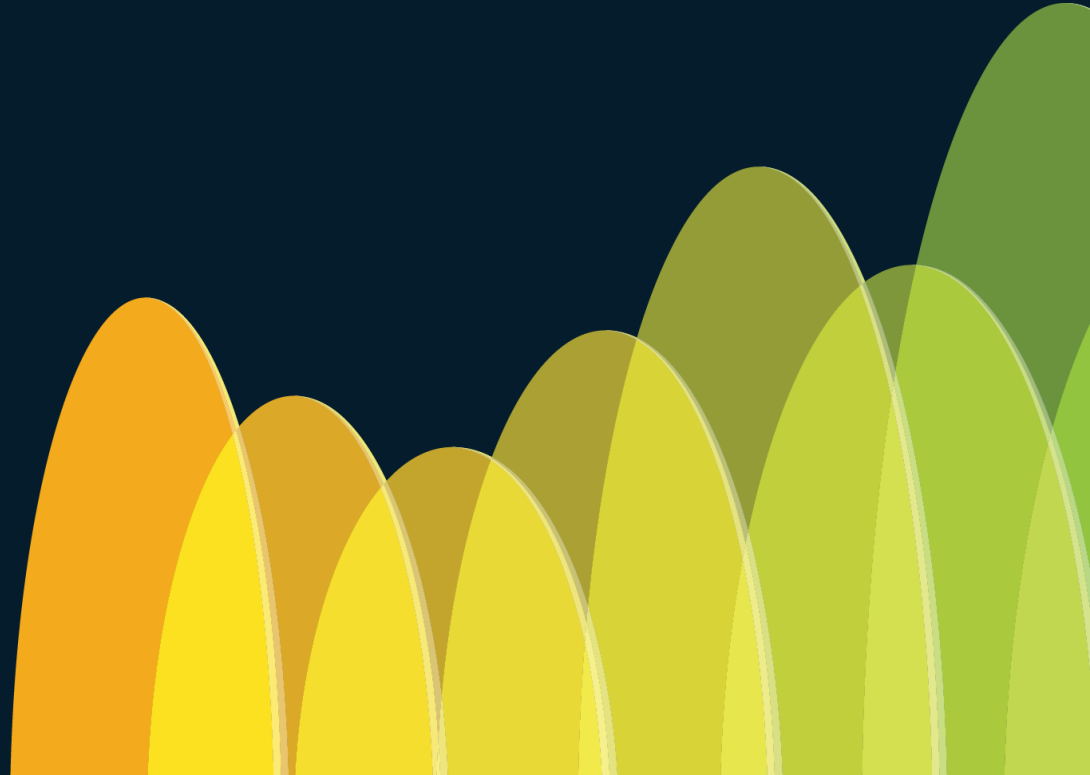
Routing traffic directly out to the internet rather than backhaul to central site

Deployment Scenarios:

- For SaaS applications
- For specific users or networks

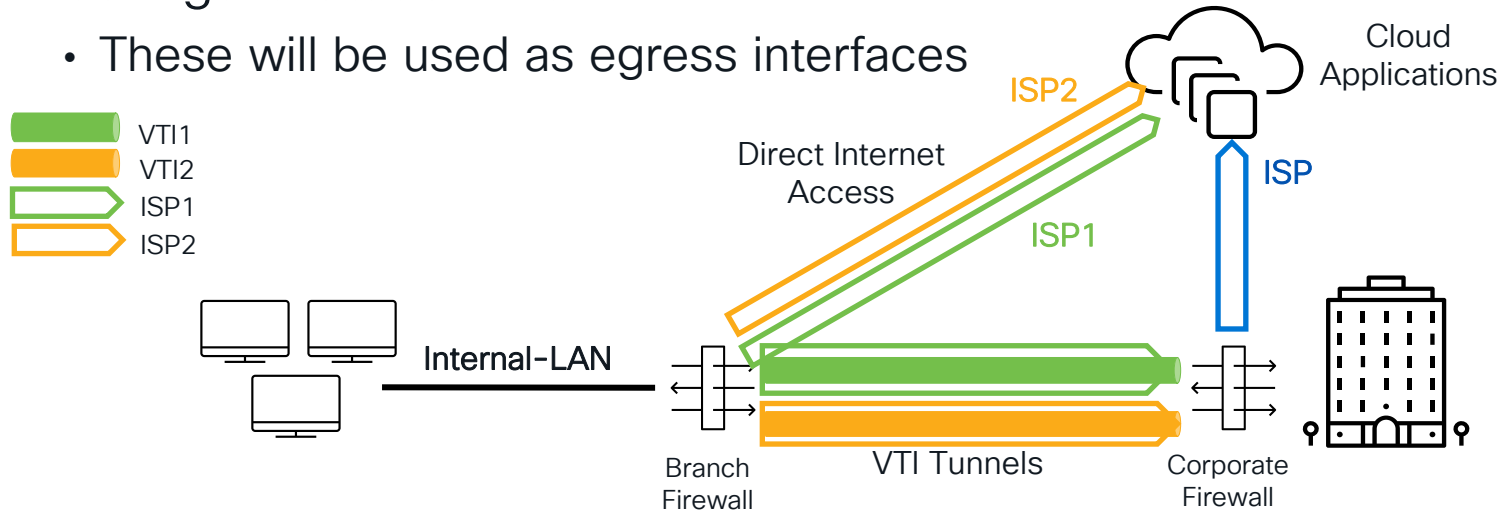


DIA Configuration Walkthrough



Configure Interfaces

- Define and configure interfaces to be used as ingress and egress
- To ensure that all traffic forwarded to the Central site is encrypted, configure Static VTIs
 - These will be used as egress interfaces



Configure Extended Access-list

- Configure Extended Access List for **Applications**
 - The selected applications (NSOs) in each of the Access Control entries form a NSG
 - This NSG is used in DIA to classify traffic based on the match criteria

The screenshot displays the Cisco configuration interface for an Extended Access List. On the left, a sidebar menu shows the navigation path: **Access List** > **Extended**. The main panel is titled "An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only." Below this, a table lists existing access lists: Email_Apps, SocialMediaTraffic, and VideoStreamingApps. A green arrow points from the "Email_Apps" entry to a detailed configuration window.

The detailed configuration window for "Email_Apps" shows the following details:

- Name:** Email_Apps
- Entries (1):**

Sequence	Action	Source	Source Port	Destination	Destination Port	Application
1	Allow	Any	Any	Any	Any	Gmail Outlook Microsoft Outlook Live

Configure Policy-Based Routing

Define Ingress interface

- PBR can be used to classify the network traffic based on applications
 - PBR policy enables to securely breakout traffic for specific applications

Policy Based Routing

Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

[Configure Interface Priority](#)[Add](#)



Edit Policy Based Route

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

Internal-LAN1 x

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

Match ACL Forwarding Action

Configure Policy-Based Routing

Match Traffic Criteria and Egress Interfaces

- Traffic will be forwarded through the Egress interfaces based on the **Interface Ordering** parameters:
 - Static parameters: By Order, By Priority
 - Dynamic parameters: Round Trip Time(RTT), Jitter, Mean Opinion Score (MOS) or Packet Loss

Edit Forwarding Actions

Match ACL:* **Email_Apps** +

Send To:* **Egress Interfaces**

Interface Ordering:* **Interface Priority**

Available Interfaces

Priority	Interface
0	Internal-LAN
0	vti-1
0	vti-2

Egress Interfaces*

Interface
ISP1
ISP2



Edit Policy Based Route

A policy based route consists of Ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

Internal-LAN1

Match Criteria and Egress Interface

Specify forward action for chosen match criteria. **Add**

Match ACL	Forwarding Action
Email_Apps	Send and load balance it through #4 ISP1 #4 ISP2
SocialMediaTraffic	Send through #4 ISP2 If above link fails, Send through #4 ISP1

Interface Priority

- Traffic is routed to the interface with the least priority first
 - If the priority value is the same for a group of interfaces, then traffic is load balanced among them
- There are 2 ways to configure interface priority:

Policy Based Routing
Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly.

Configure Interface Priority **Add**

Ingress Interfaces Match criteria and forward action

There are no PBR policies defined yet. Start by defining the first one.

Configure Interface Priority

Interface priority is useful to create back up interface or load balancing by specifying ascending or same values on multiple interfaces

Interface	Priority
Internal-LAN1	0
ISP1	4
ISP2	4
vdi-1	0
vdi-2	0

Edit Physical Interface

General IPv4 IPv6

Name: ISP1

☒ Enabled
☐ Management Only

Description:

Mode: None

Security Zone: Outside-Zone

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

Priority: 4

Configure Policy-Based Routing

Match Traffic Criteria and Egress Interface

- Multiple PBR Rules configured on different set of ingress interfaces

Policy Based Routing
Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

[Configure Interface Priority](#) [Add](#)

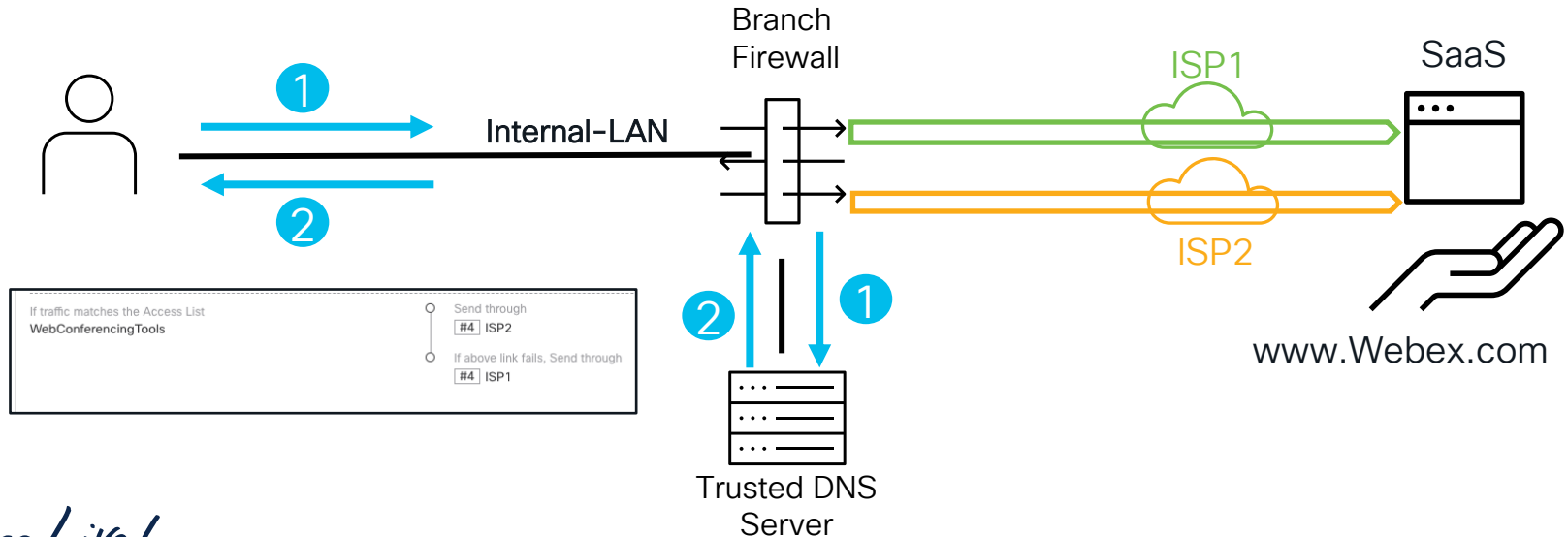
Ingress Interfaces	Match criteria and forward action	
Internal-LAN1 Internal-LAN2	<p>If traffic matches the Access List Email_Apps</p> <p>Send and load balance it through</p> <div><div>#4</div> SP1</div> <div><div>#4</div> SP2</div> <p>Interface Priority</p>	 
	<p>If traffic matches the Access List SocialMediaTraffic</p> <p>Send through</p> <div><div>#4</div> SP2</div> <p>If above link fails, Send through</p> <div><div>#4</div> SP1</div>	

Interface Ordering By Priority

Interface Ordering By Order

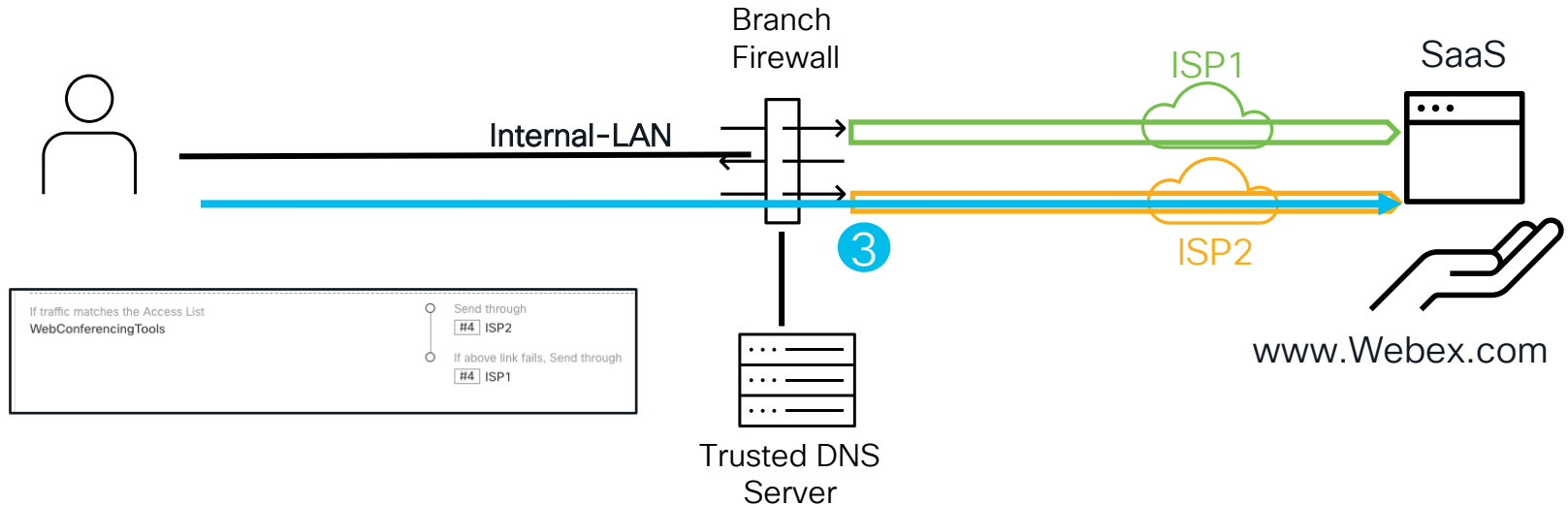
DIA End to End Flow

1. User initiates DNS Request for a particular application
2. Firewall snoops the DNS response and stores the domain information along with the IP address



DIA End to End Flow

3. Application traffic will be sent among the egress interfaces based on the **Interface Ordering** configuration in the PBR policy

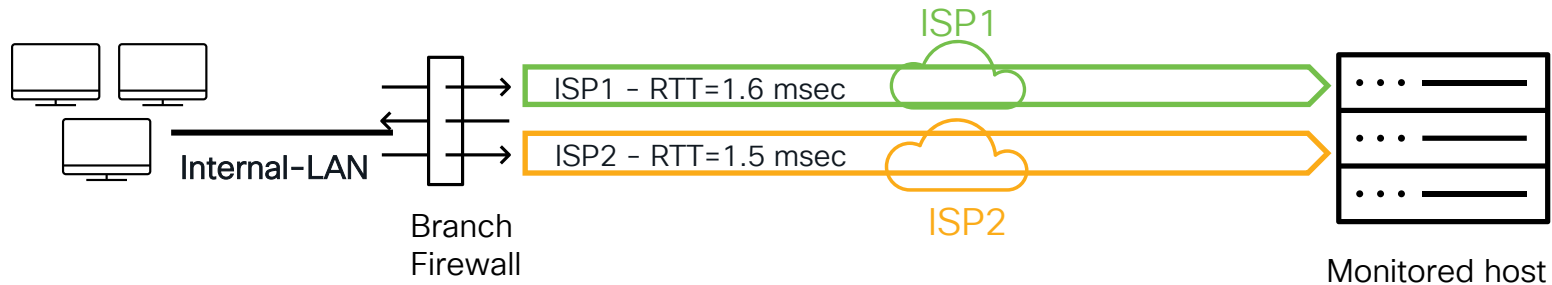


PBR with Path Monitoring (From FTD 7.2+)

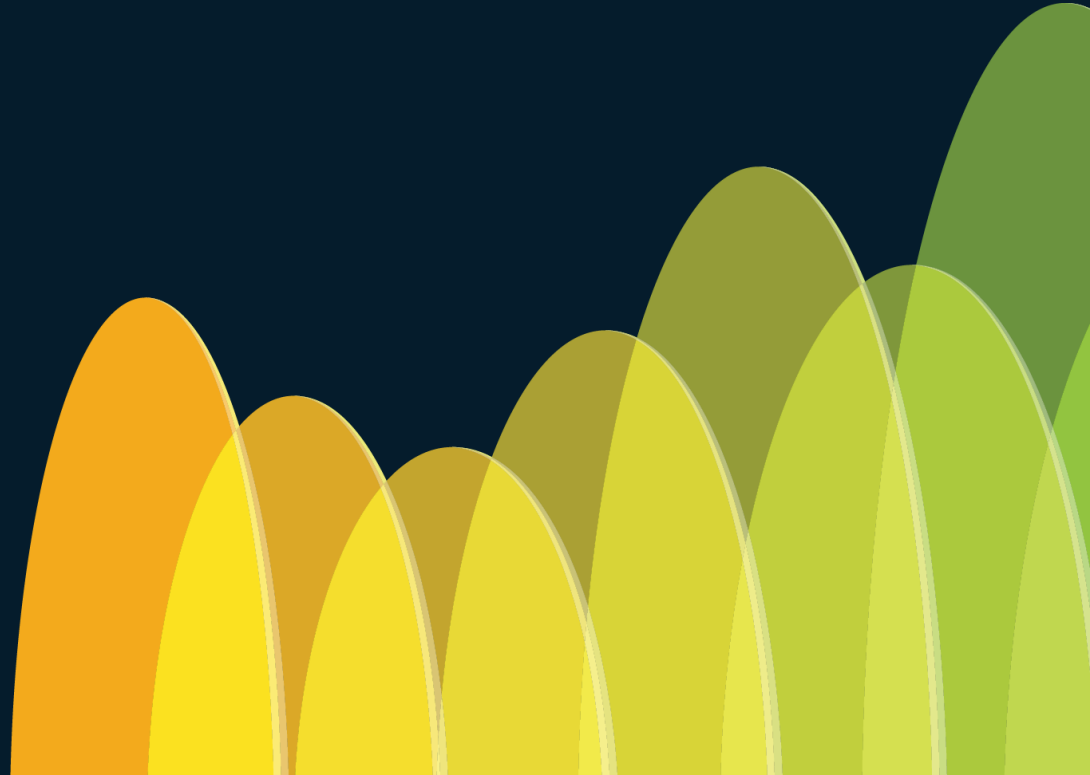


PBR with Path Monitoring

- PBR with Path Monitoring steers traffic based on dynamically monitored interface statistics such as **RTT, Jitter, MOS and packet loss**
- These metrics are collected dynamically using ICMP/HTTP Probe messages

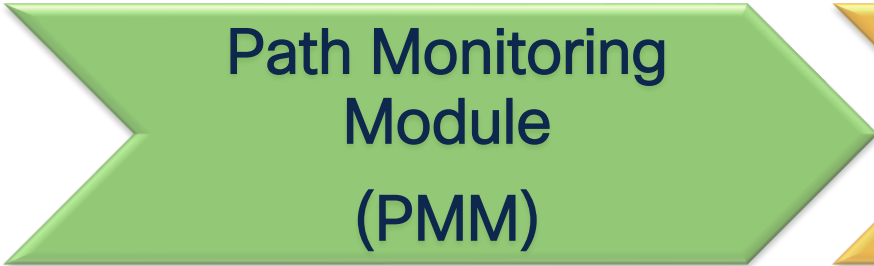


ICMP Path Monitoring



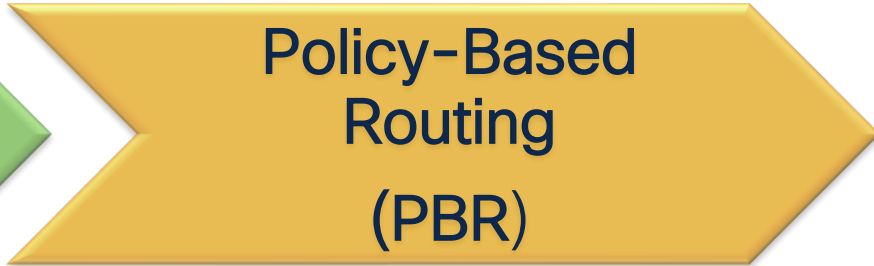
ICMP Path Monitoring

Components



Path Monitoring Module (PMM)

Responsible for
collecting the Link
metrics using ICMP
probes



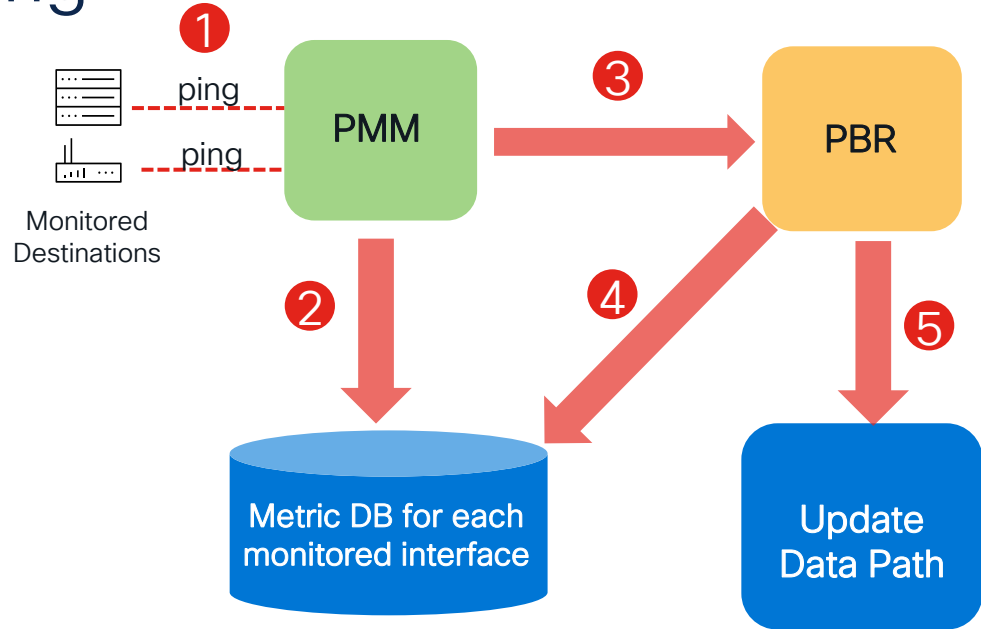
Policy-Based Routing (PBR)

Responsible for routing
the traffic using egress
interface as per the best
metric reported by the
PMM

ICMP Path Monitoring

Architecture Overview

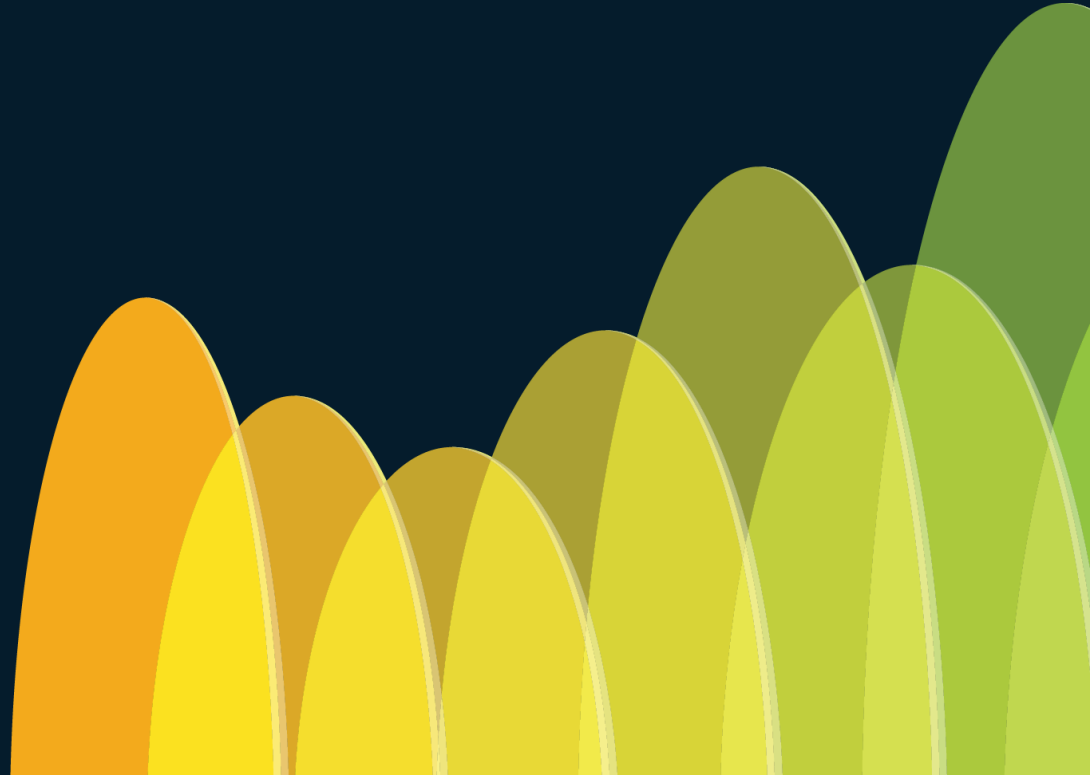
1. PMM sends ICMP probes to Monitored destinations
2. PMM computes and stores interface metrics
3. PMM pushes the list of interfaces that have updates to PBR
4. PBR fetches the latest available metrics from PMM internal DB
5. PBR pushes the routing updates



Interface: ISP1
RTT average: 1474 microsecond(s)
Jitter: 261 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 10 second(s) ago

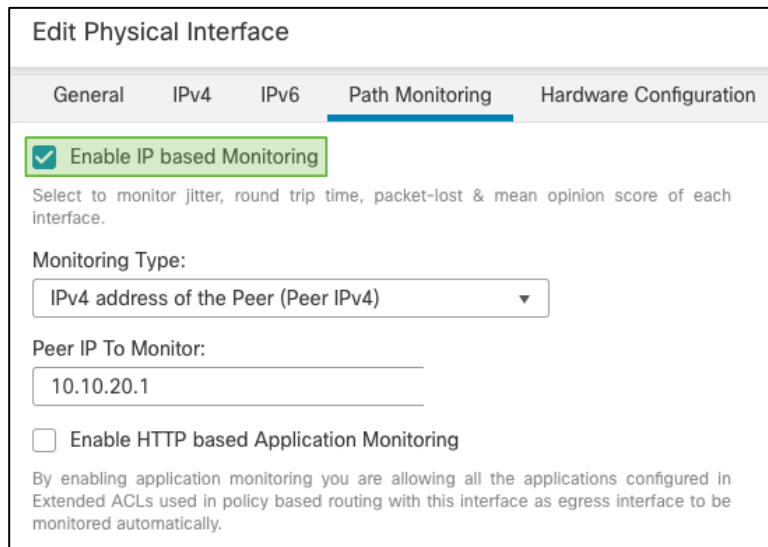
Interface: ISP2
RTT average: 883 microsecond(s)
Jitter: 158 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 10 second(s) ago

ICMP Path Monitoring Configuration Walkthrough



ICMP Path Monitoring Configuration

- Enable Path Monitoring at the interface level
 - Link metrics determined using ICMP to either Next Hop (auto, auto4, auto6) or to the explicit IP



The screenshot shows the 'Edit Physical Interface' configuration page with the 'Path Monitoring' tab selected. The 'Enable IP based Monitoring' checkbox is checked and highlighted with a green box. Below it, the 'Monitoring Type' is set to 'IPv4 address of the Peer (Peer IPv4)' and the 'Peer IP To Monitor' is set to '10.10.20.1'. The 'Enable HTTP based Application Monitoring' checkbox is unchecked.

Edit Physical Interface

General IPv4 IPv6 **Path Monitoring** Hardware Configuration

☒ Enable IP based Monitoring

Select to monitor jitter, round trip time, packet-lost & mean opinion score of each interface.

Monitoring Type:

IPv4 address of the Peer (Peer IPv4) ▼

Peer IP To Monitor:

10.10.20.1

☐ Enable HTTP based Application Monitoring

By enabling application monitoring you are allowing all the applications configured in Extended ACLs used in policy based routing with this interface as egress interface to be monitored automatically.

PBR Policy Configuration

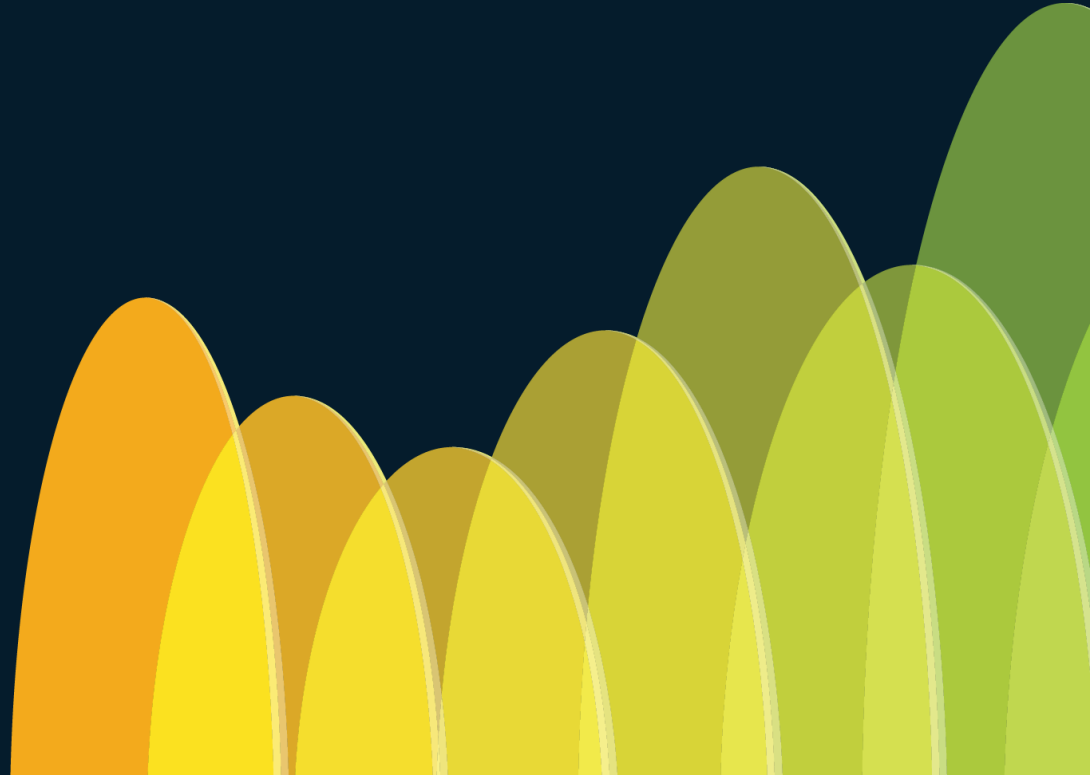
- **PBR Interface Ordering** enhanced to adaptively steers traffic based on the dynamically monitored metrics per egress interfaces

The screenshot shows the 'Edit Forwarding Actions' configuration window. The 'Match ACL:*' field is set to 'SocialMediaTraffic'. The 'Send To:*' field is set to 'Egress Interfaces'. The 'Interface Ordering:*' dropdown menu is open, showing options: 'Order' (selected), 'Interface Priority', 'Order', 'Minimal Jitter', 'Maximum Mean Opinion Score', 'Minimal Round-Trip Time', and 'Minimal Packet Loss'. Below the dropdown, there is a table of 'Available Interfaces' with columns 'Interface' and a '+' icon. The table lists: 'Internal-LAN1', 'Internal-LAN2', 'LAB-Network', 'vti-1', and 'vti-2'. To the right, there is a 'Selected Egress Interfaces*' section with a table listing 'WAN1' and 'WAN2'.

Interface
Internal-LAN1
Internal-LAN2
LAB-Network
vti-1
vti-2

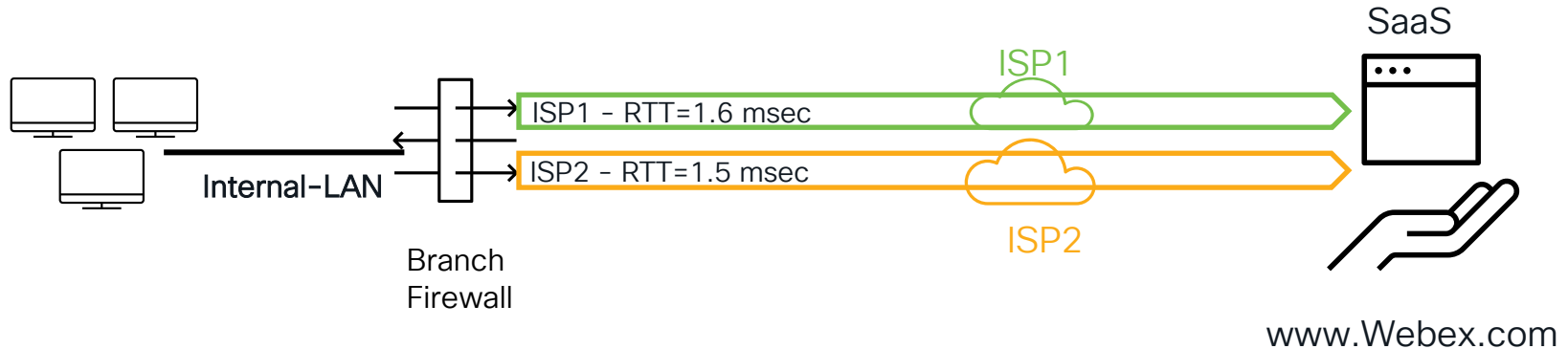
Interface
WAN1
WAN2

HTTP Path Monitoring (From FTD 7.4+)



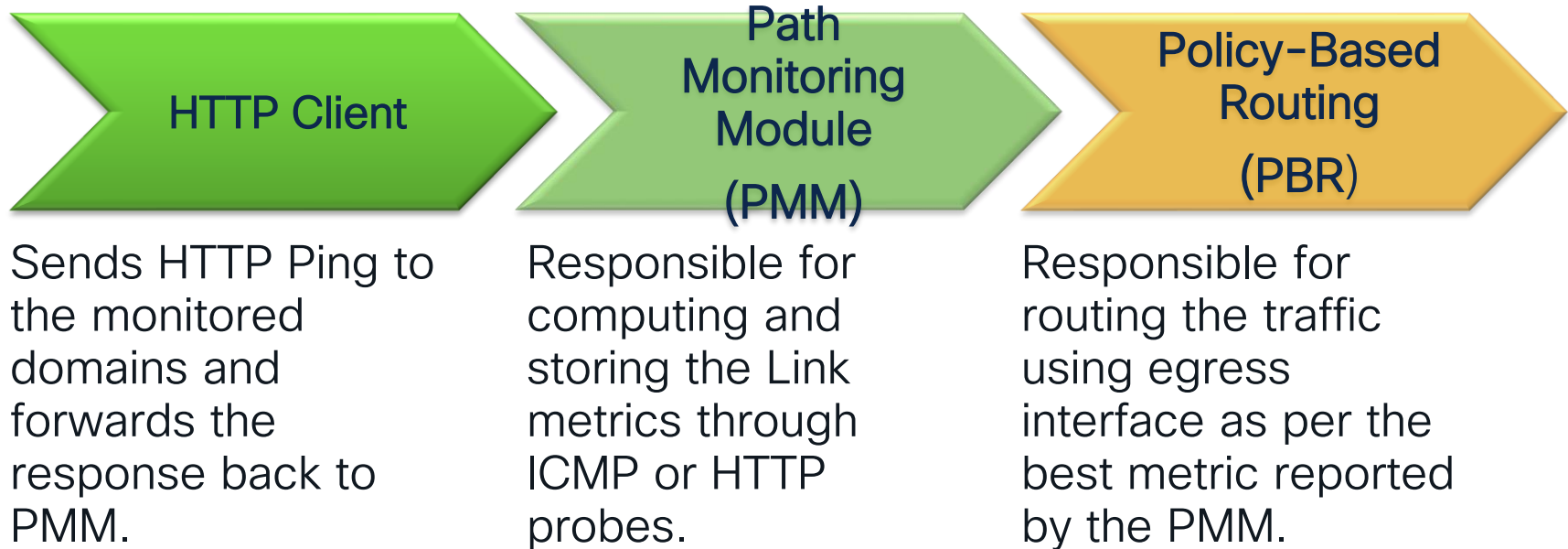
HTTP Path Monitoring

HTTP probes are sent to measure path metrics for selected applications across all egress interfaces configured for path monitoring.



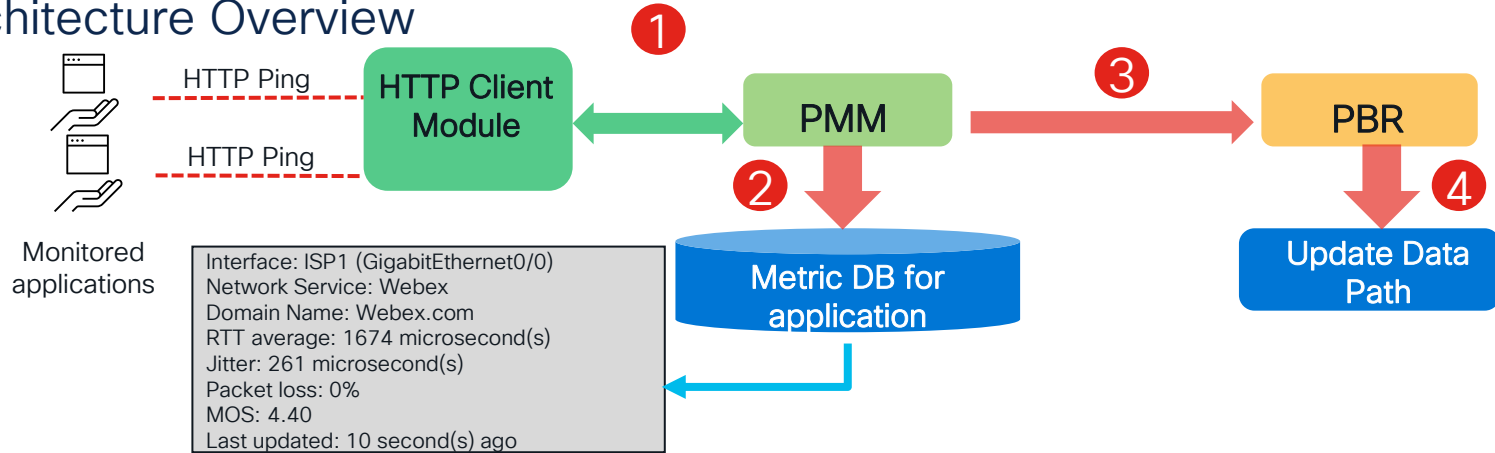
HTTP Path Monitoring

Components



HTTP Path Monitoring

Architecture Overview

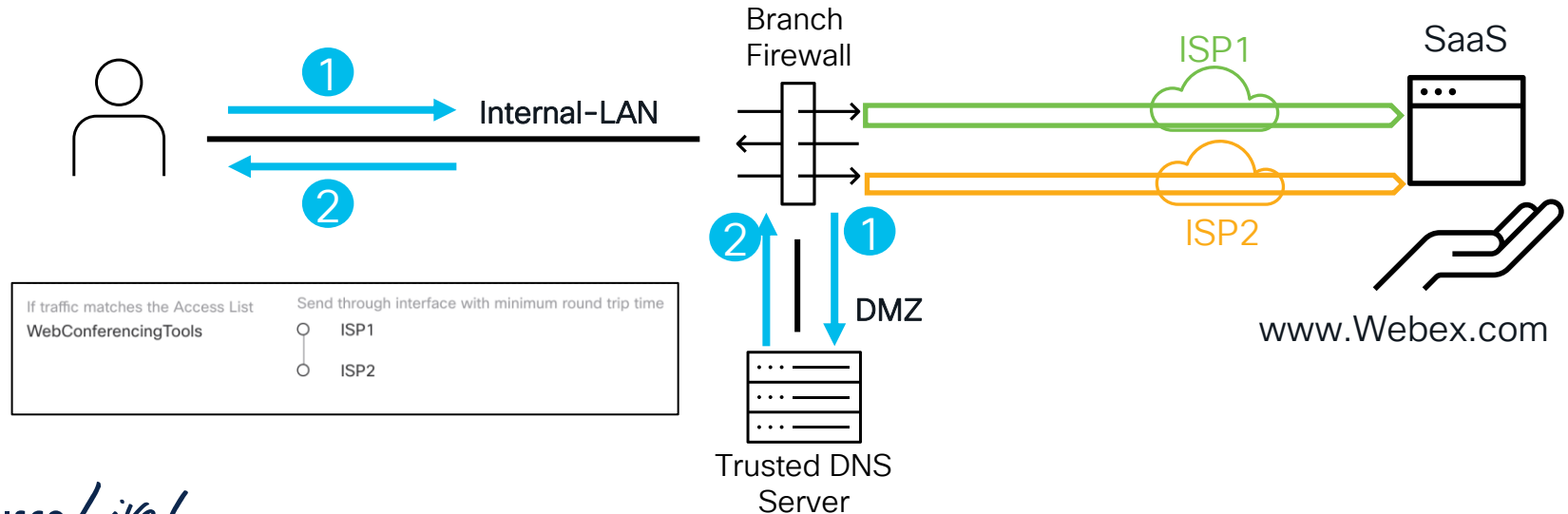


1. PMM will start application monitoring when a DNS entry is snooped for a domain
2. PMM computes and stores interface metrics
3. PMM pushes the metric values per domain and egress interfaces to PBR every 30 seconds
4. PBR pushes the routing updates

HTTP Path Monitoring

End to End Flow

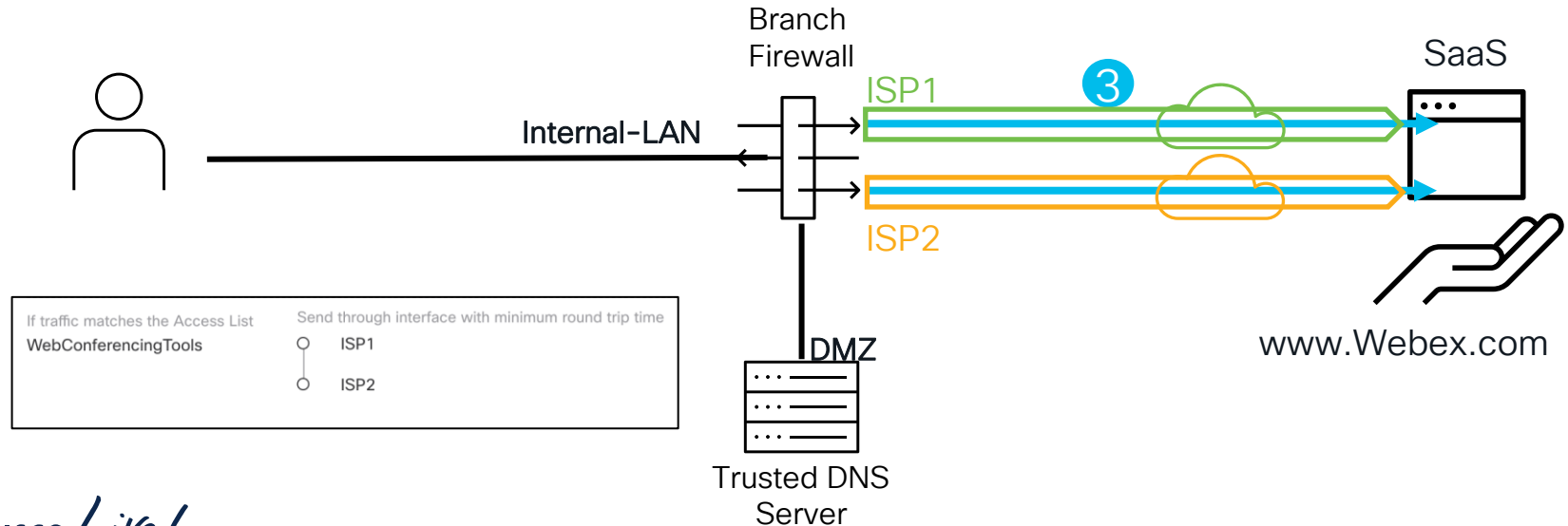
1. User initiates DNS Request for a particular domain
2. Firewall snoops the DNS response and stores the domain information along with the IP address



HTTP Path Monitoring

End to End Flow

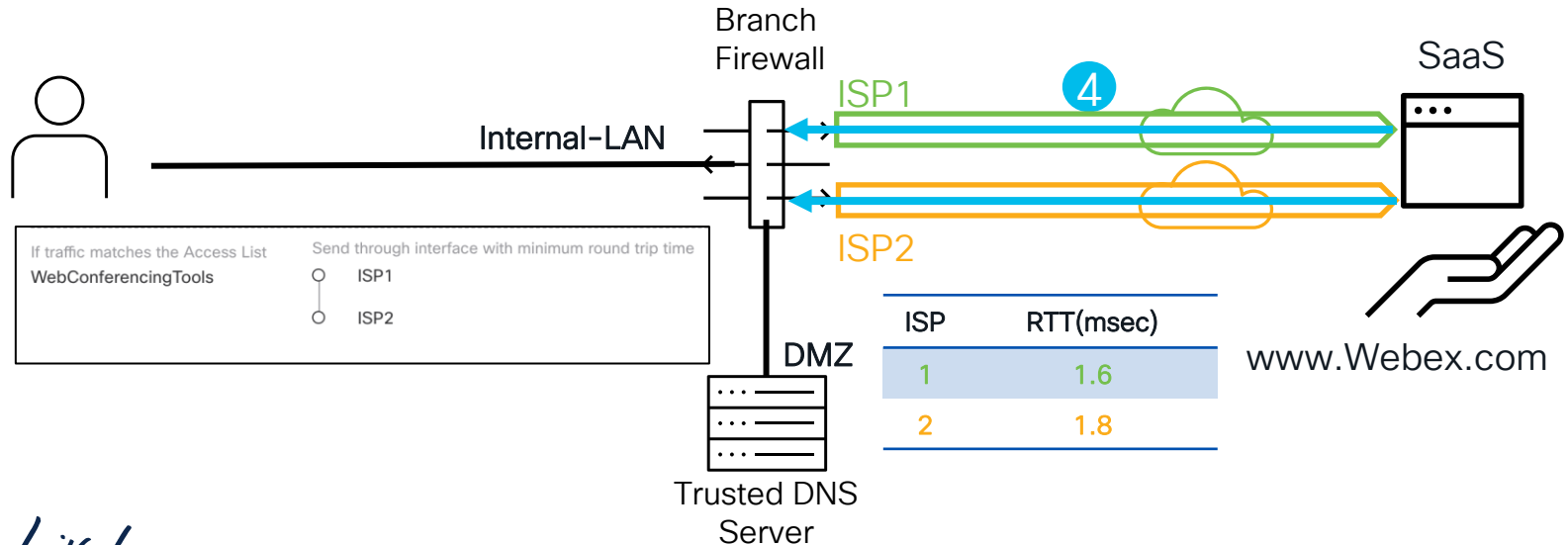
3. HTTP Client sends HTTP probes to the IP addresses for the monitored domains on the egress interfaces with Path Monitoring enabled



HTTP Path Monitoring

End to End Flow

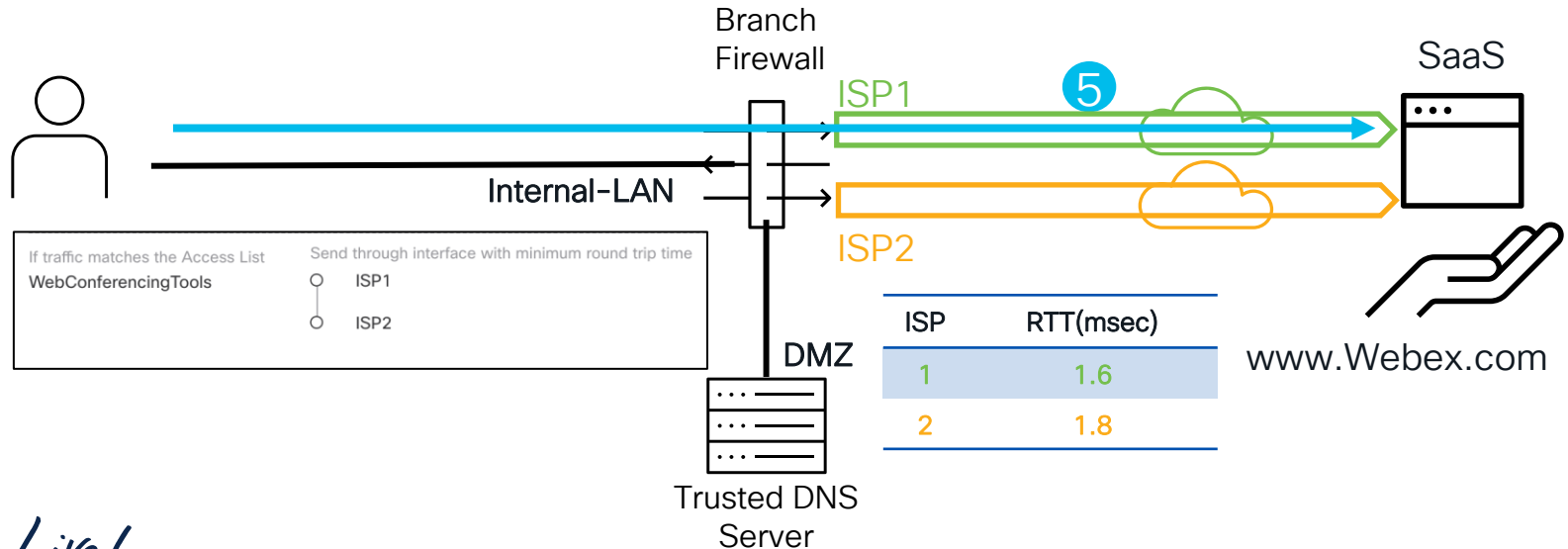
4. PMM computes and stores the metrics (Jitter, Packet Loss, RTT and MOS) which are then shared with the PBR module



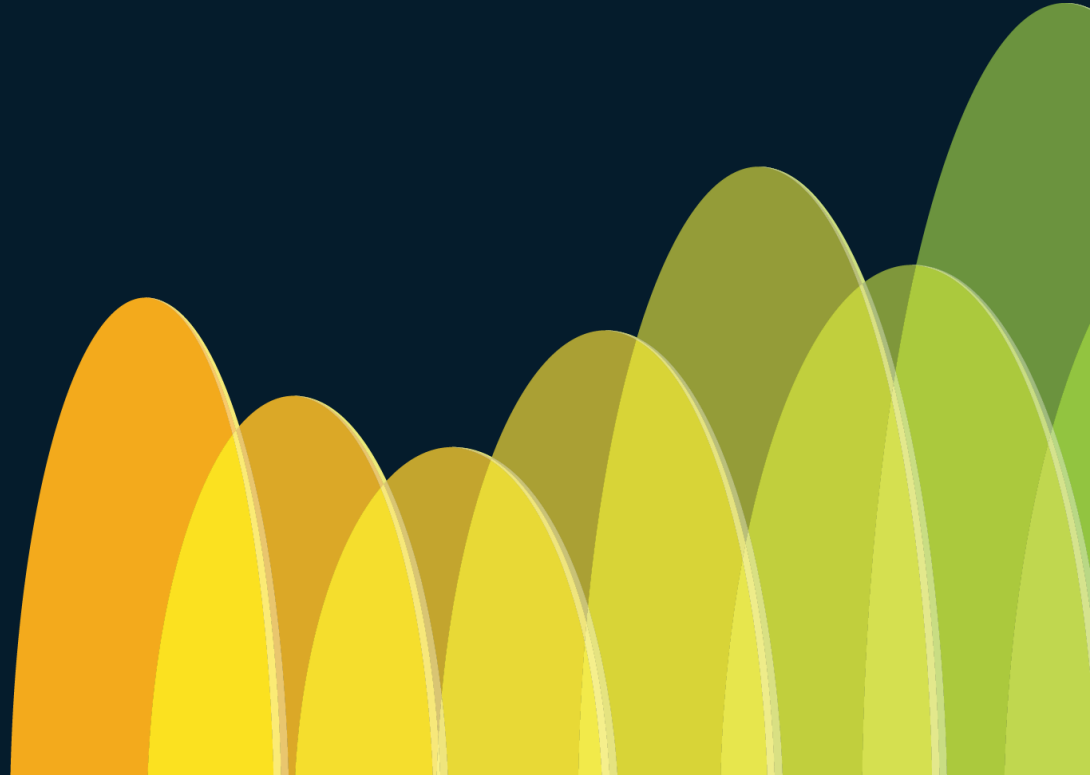
HTTP Path Monitoring

End to End Flow

5. Application traffic is sent through the selected interface based on whichever interface is better for the metric type configured



HTTP Path Monitoring Configuration Walkthrough



HTTP Path Monitoring Configuration

- Enable HTTP Path Monitoring at the interface level

Edit Physical Interface

General IPv4 IPv6 **Path Monitoring**

☐ Enable IP based Monitoring

Select to monitor jitter, round trip time, packet-lost & mea interface.

Monitoring Type:

Next-hop of default route out of interface (Auto)

System monitors the next hop of the interface. Tries IPv4 and th If the peer is unavailable, monitoring is not done.

☒ **Enable HTTP based Application Monitoring**

By enabling application monitoring you are allowing all the Extended ACLs used in policy based routing with this interface monitored automatically.

Applications

- Amazon Prime Video
- YouTube
- YouTube TV
- YouTubeMp3
- Youtube Upload



Read Only

Edit Forwarding Actions

Match ACL:* VideoStreamingApps +

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter

Available Interfaces

Search by interface name

Interface	
Internal-LAN1	+
vti-1	+
vti-2	+

Selected Egress Interfaces*

Interface	
ISP1	🗑
ISP2	🗑

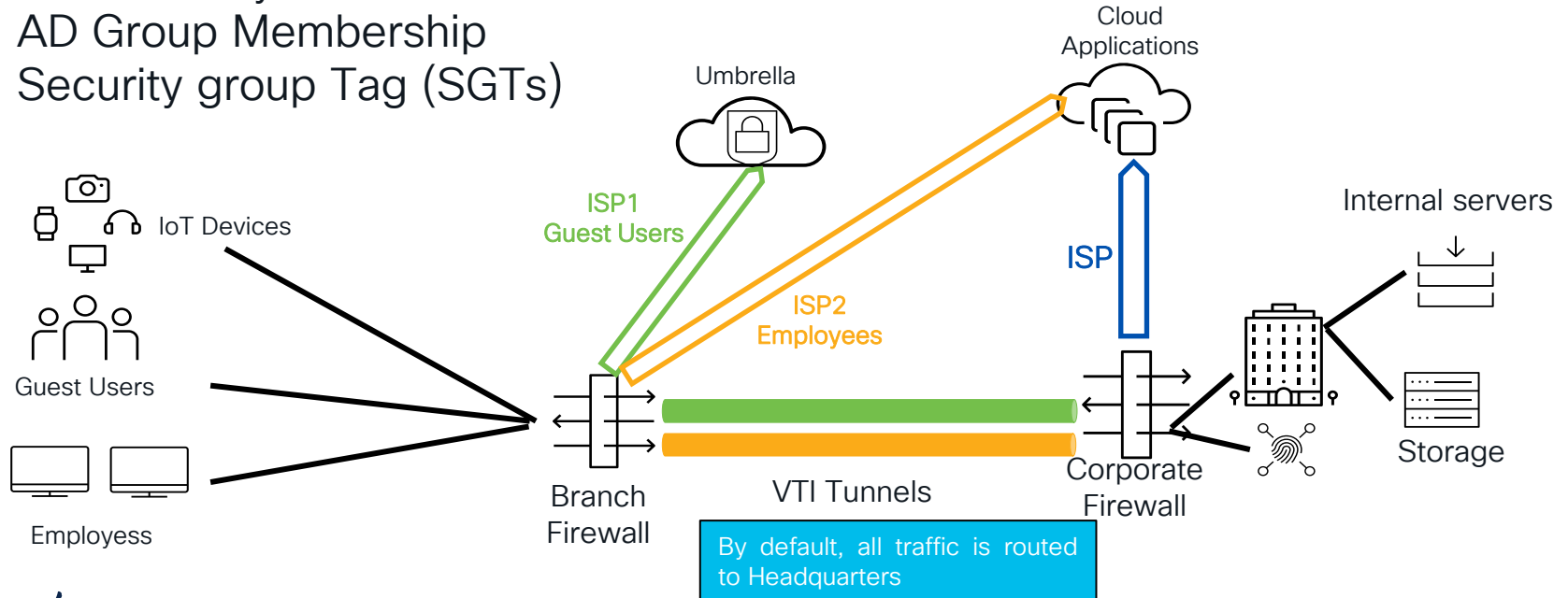
Identity and SGT Support (From FTD 7.4+)



PBR with User Identity and SGT

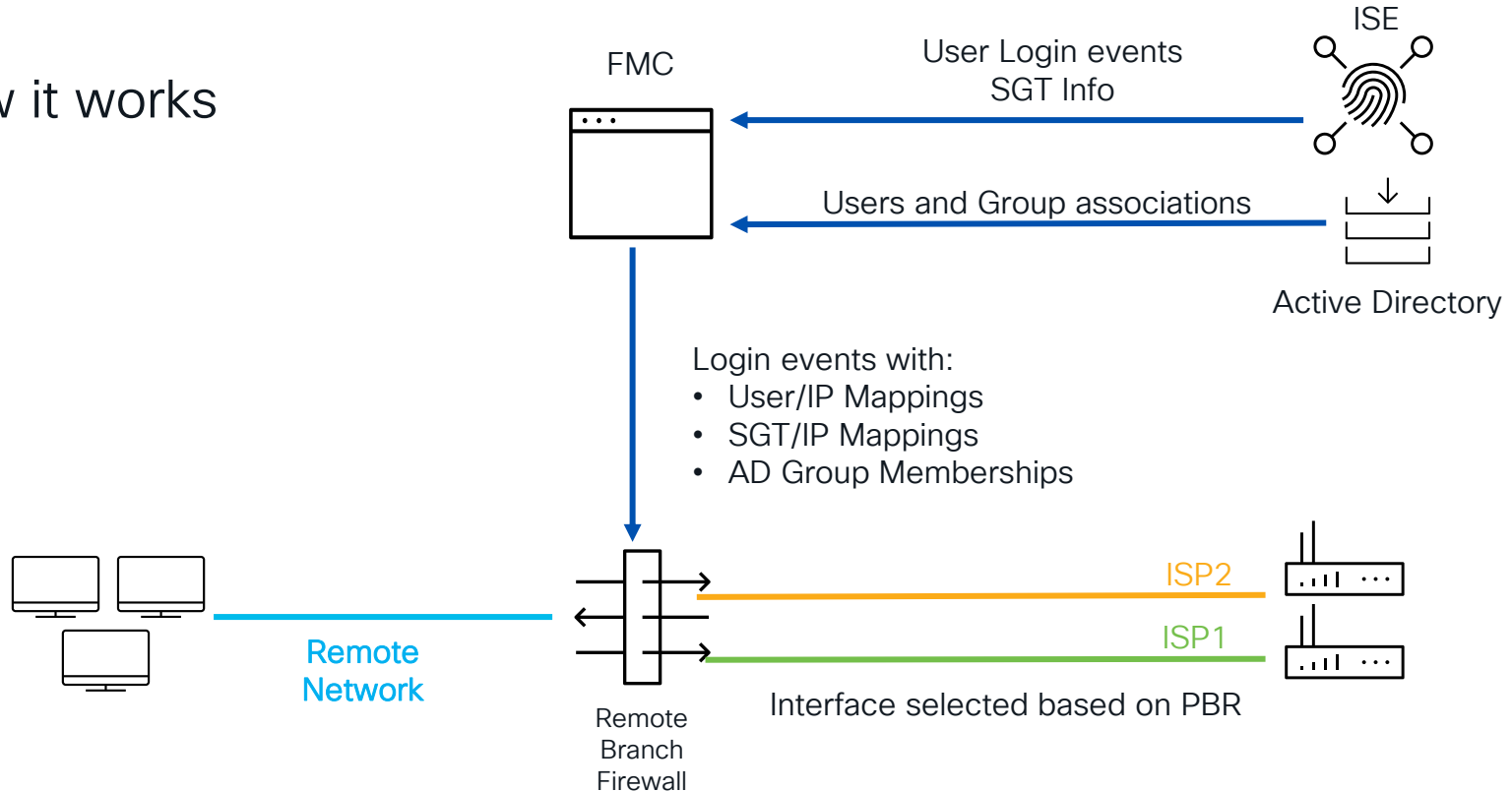
Additional attributes can be leveraged in the PBR policy:

- User Identity
- AD Group Membership
- Security group Tag (SGTs)



PBR with User Identity and SGT

- How it works



Configure Extended Access-list

- Configure Extended Access List with **User Identities and Security Group Tag (SGT)**

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only.

Name	Value	Override
Email_Apps		
SocialMediaTraffic		
VideoStreamingApps		

Name: Email_Apps

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	Any	Any	Any	Any	Gmail Outlook Microsoft Outlook Live	Any	Any	



View By:

Group

[Migrate](#) | [Deployment History](#)

All (2)

Error (0)

Warning (0)

Offline (0)

Normal (2)

Deployment Pending (0)

Upgrade (0)

Snort 3 (2)

Search Device

Add

[Collapse All](#)

[Download Device List Report](#)

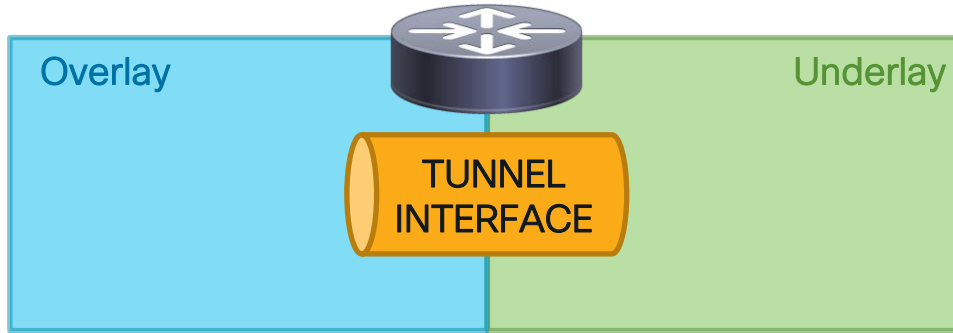
☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
☐	Ungrouped (2)							
☐	<div>Branch FTD Snort 3</div> <div>198.18.128.10 - Routed</div>	FTDv for VMware	7.4.1	N/A	Essentials	BranchPolicy		
☐	<div>Hub FTD Snort 3</div> <div>198.18.128.20 - Routed</div>	FTDv for VMware	7.4.1	N/A	Essentials	HQPolicy		

Firewall Management Center

Branch to Hub Communication using DVTI (From FTD 7.3+)



Tunnel Interface



- Tunnel Interface interconnects underlay and overlay network.
- Supports only native IPsec IPv4/IPv6 on ASA/FTD (no GRE)
- Main building block for ASA / FTD SDWAN VPNs.

IPSec Virtual Tunnel Interface



- Provides a virtual **routable interface** for terminating IPsec tunnels
- **Simplifies the configuration** of IPsec for protection of remote links
- The **VTI tunnel is always up** (does not need “interesting traffic”)
- No multicast support on ASA / FTD over VTI

IPSec Tunnel Interface Types

Static Virtual Tunnel Interface (SVTI)



```
Interface tunnel1
nameif tunnel-to-dc
ip unnumbered loopback1
tunnel source GigabitEthernet1
tunnel destination 10.0.0.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile default
```

- Static Virtual Tunnel Interfaces (VTI) are introduced in [FTD 6.7](#)
- Static VTI is supported in HA and Multi-Instance
- VTI are not supported in clustering

IPSec Tunnel Interface Types

Dynamic Virtual Tunnel Interface (DVTI)



```
interface Virtual-Template101 type tunnel
 nameif dVTI101
 ip unnumbered Lo10
 tunnel source interface Corp-ISP1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC IPSEC PROFILE 2
```

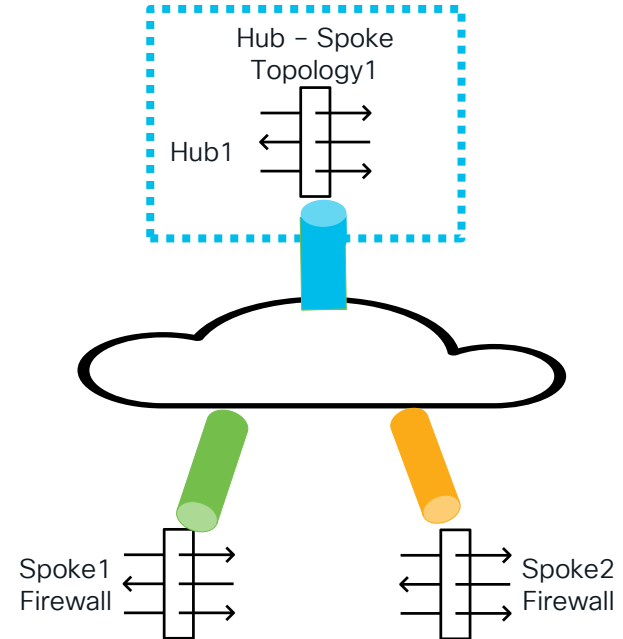
- Dynamic Virtual Tunnel Interfaces are introduced in [FTD 7.3](#)
- DVTI uses a virtual template for dynamic instantiation and management
- VPN Sessions using DVTIs only support IKEv2

```
> show interface Virtual-Access 1
Interface Virtual-Access1 "dVTI101_va3", is up, line protocol is up
Hardware is Virtual Access      MAC address N/A, MTU 1445
IP address 169.254.255.1, subnet mask 255.255.255.255
Vaccess Interface Information:
Source IP address: [REDACTED].9.20
Destination IP address: [REDACTED].7.10
Vaccess cloned from template 101
Mode: ipsec ipv4      IPsec profile: FMC_IPSEC_PROFILE_2
IPsec MTU Overhead : 55
```

Branch to Hub Communication

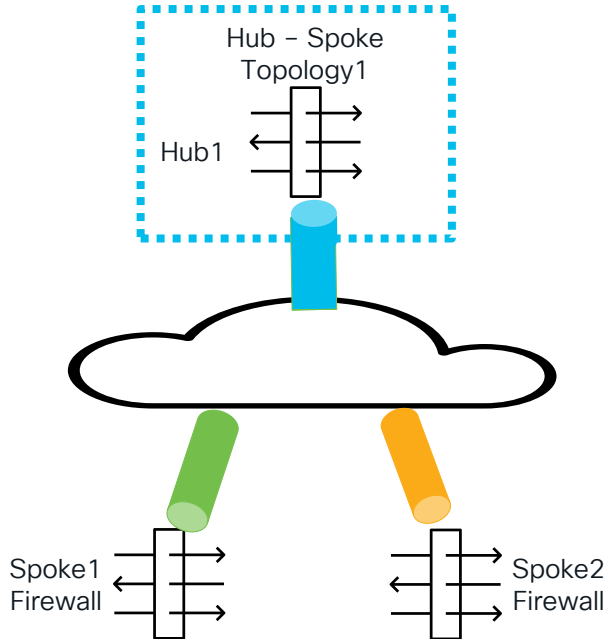
Why Dynamic Virtual Tunnel Interface (DVTI) ?

- High-scale, route-based VPN deployments
- No additional Hub configuration while adding new spokes
- No configuration change on Hub when the spoke's DHCP IP address changes



Hub and Spoke design using DVTIs

Single Hub Topology



Edit VPN Topology

Topology Name:*
dVTI-Hub-and-Spoke

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Hub Nodes: +

Device Name	VPN Interface	Traffic Match Criteria	
FTD Hub FTD	dVTI101 (169.254.255.1)	Routing Policy	

Spoke Nodes: +

Device Name	VPN Interface	Traffic Match Criteria	
FTD Branch FTD	VTI1 (169.254.255.2)	Routing Policy	

Single Hub Topology

Hub Interface Configuration

The screenshot displays the Cisco Firepower Threat Defense (FTD) configuration interface for a Hub FTD. The main configuration pane shows the 'Interfaces' tab, with a table listing the configured interfaces. A green box highlights the 'Virtual-Template101' interface, which is a VTI of type 'VTI' in the 'dVTI-Zone' security zone. A green line connects this interface to the detailed configuration pane on the right.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Management0/0	management	Phy...			
GigabitEthernet0/0	Corp-ISP1	Phy...	ISP1-Zone		9.20/255.255.255
Virtual-Template101	dVTI101	VTI	dVTI-Zone		

The detailed configuration pane for 'Virtual Tunnel Interface' shows the following settings:

- General:** Tunnel Type is set to 'Dynamic'. Name is 'dVTI101'. It is 'Enabled'.
- Security Zone:** Set to 'dVTI-Zone'.
- Virtual Tunnel Interface Details:** Template ID is '101'. Tunnel Source is 'GigabitEthernet0/0 (Corp-ISP1)' with IP '9.20'.
- IPsec Tunnel Details:** IPsec Tunnel Mode is set to 'IPv4'. IP Address is 'Configure IP' with a dropdown showing 'Borrow IP (IP unnumbered)' and 'Loopback10 (Lo10)'.
- VPN Topology Usage:** Shows 'cVTI-Hub-and-Spoke (Tunnel Destination IP - 198.18.6.10)'.

- DVTI is configured in the Hub
- Virtual Template interface must “borrow” loopback address
- Virtual Template interface is used to create ephemeral VTI interfaces as spokes connect

Single Hub Topology

Spoke Interface Configuration

Branch FTD

Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP VTEP

All Interfaces Virtual Tunnels

Search by

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Management0/0	management	Physical			
GigabitEthernet0/0	ISP-1	Physical	ISP1-Zone		6.10/24
Tunnel1	VTI1	VTI	sVTI-Zone		

Edit Virtual Tunnel Interface

General Path Monitoring

Tunnel Type

Static ☒ Dynamic ☐

Name:*

VTI1

☒ Enabled

Description:

Security Zone:

vTemplate-Zone

Priority:

0 (0 - 65536)

Virtual Tunnel Interface Details

An interface named Tunnel-ID is configured. Tunnel Source is a physical interface where

Tunnel ID:*

1 (0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (ISP-1) 6.10/24

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses as

IPsec Tunnel Mode:*

IPv4 ☒ IPv6 ☐

IP Address:*

Configure IP <Valid IPv4 address>/<Mask>

Borrow IP (IP unnumbered) Loopback1 (Lo1)

- SVTI is configured in the Spoke
- VTI can borrow the IP address from another interface, Loopback recommended (requires 7.3)

Single Hub Topology

VPN Topology

Hub FTD Configuration:

Device:*
Hub FTD

Dynamic Virtual Tunnel Interface
dVTI101 (IP: 169.254.255.1) +

Tunnel Source: Corp-ISP1 (IP: 198.18.9.20) [Edit VTI](#)

☐ Tunnel Source IP is Private

Additional Configuration ⓘ
Route traffic to the VTI : [Routing Policy](#)
Permit VPN traffic : [AC Policy](#)

▼ Advanced Settings

☐ Send Virtual Tunnel Interface IP to the peers

Protected Networks (To generate Access-list on the spoke): +

☒ Allow incoming IKEv2 routes from the peers

Connection Type:

It allows the device to send the VTI IP address to the peers.
Check this option, if BGP or static route is implemented

Spoke FTD Configuration:

Edit Endpoint ⓘ

Device:*
Branch FTD

Static Virtual Tunnel Interface
VTI1 (IP: 169.254.255.2) +

Tunnel Source: ISP-1 (IP: 198.18.6.10) [Edit VTI](#)

☐ Tunnel Source IP is Private

☐ Send Local Identity to Peers

+ Add Backup VTI (optional)

Additional Configuration ⓘ
Route traffic to the VTI : [Routing Policy](#)
Permit VPN traffic : [AC Policy](#)

▼ Advanced Settings

☒ Send Virtual Tunnel Interface IP to the peers

Single Hub Topology

Firewall Policy Configuration

HQPolicy

Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → More

Targeted: 1 device

Q Type to search

Total 3 rules

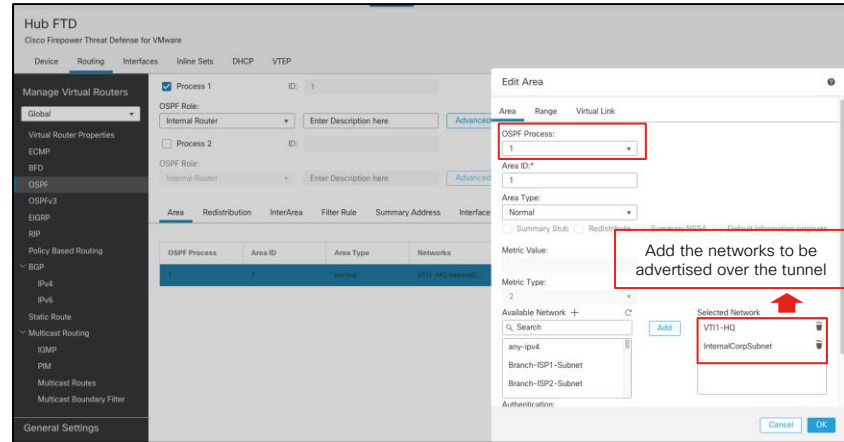
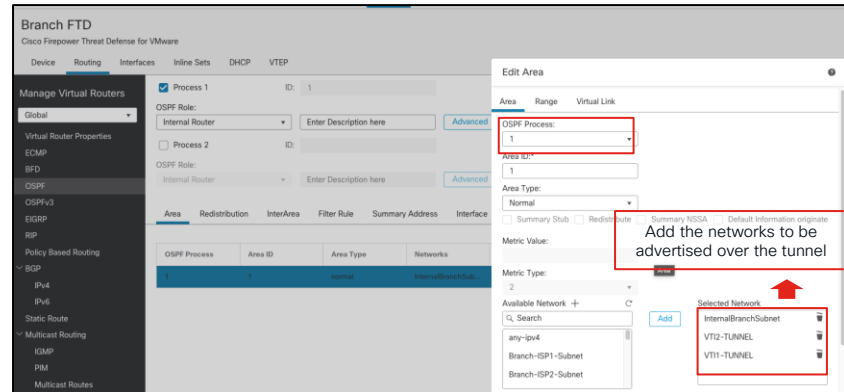
	Name	Action	Source			Destination			
			Zones	Networks	Ports	Zones	Networks	Ports	
Mandatory (1 - 3)									
☐	1 Allow-To-Branch-Over-Tu...	→ Allow	Internal-Z...	InternalCorpSu...	Any	dVTI-Zone	InternalSubnet	Any	
☐	2 Allow-To-Corp-Over-Tunnel	→ Allow	dVTI-Zone	InternalCorpSu...	Any	Internal-Zone	InternalBranchSub...	Any	
☐	3 Allow-To-Internet	→ Allow	dVTI-Zone	Any	Any	ISP1-Zone	Any	Any	
			Internal-Z...			ISP2-Zone			

- Assign a zone to the tunnel interfaces
- Use the same zone for tunnels to allow for asymmetric flows
- Use this zone in the Access Control Policy like any other interface zone for traffic control and inspection

Single Hub Topology

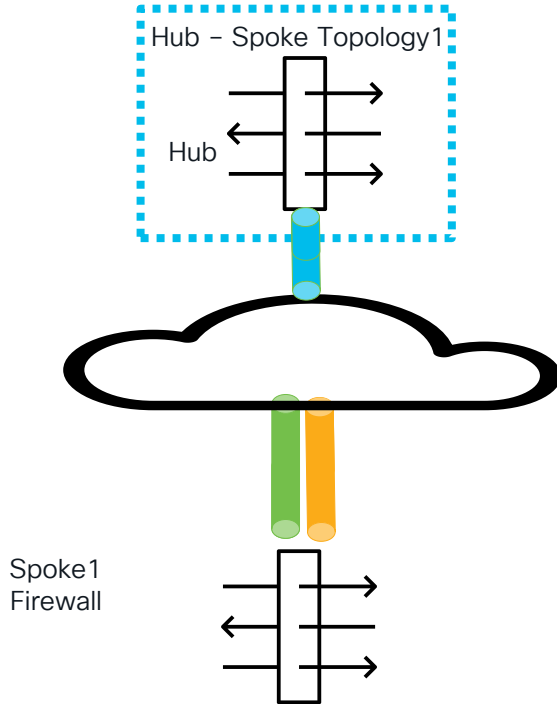
Routing Policy Configuration

- During the IKE exchange, the SVTI and VA interfaces IP addresses are advertised through the tunnel
- Routing protocol required on member devices to share routes
- For static routing, Protected RRI must be enabled



Single Hub Topology

Spoke with Dual WAN



Branch FTD

Cisco Firepower Threat Defense for VMware

Device

Routing

Interfaces

Inline Sets

DHCP

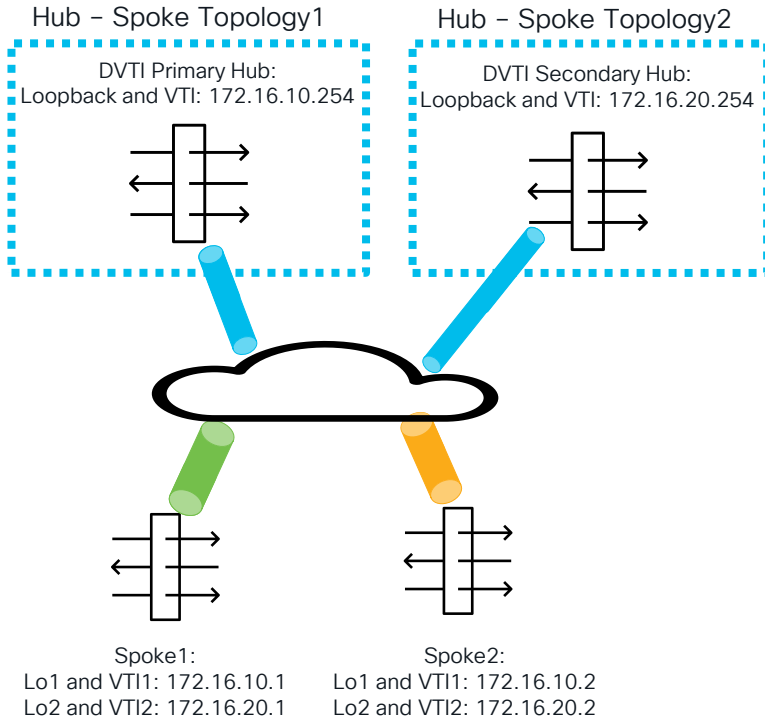
VTEP

All Interfaces

Virtual Tunnels

Interface	Logical Name	Type	Security Zones
Management0/0	management	Physical	
GigabitEthernet0/0	ISP-1	Physical	ISP1-Zone
Tunnel1	VTI1	VTI	sVTI-Zone
Tunnel3	VTI3	VTI	VTI-SSE
GigabitEthernet0/1	ISP-2	Physical	ISP2-Zone
Tunnel2	VTI2	VTI	sVTI-Zone
Tunnel5	VTI5	VTI	VTI-SSE

Dual Hub Topology



- VPN Topology can have multiple hubs for a set of spokes
 - With one hub as the Backup Hub
- Use a separate VPN topology configuration for each Hub
- Spokes require two loopback and two SVTI
 - Each spoke will have 2 VPN tunnels, one per Hub
- Dynamic Routing Protocol required

Site to Site VPN Dashboard Overview

 Firewall Management Center
Overview / Dashboards / Site to Site VPN

OverviewAnalysisPoliciesDevicesObjectsIntegrationDeploy

admin



Select...

Refresh

Refresh every 5 minutes

Node A	Node B	Topology	Status	Last Updated
Branch FTD (VPN IP: 198.18....)	Extranet (VPN IP: [REDACTED] 138....)	SecureAccess-I...	Active	2024-04-23 13...
Branch FTD (VPN IP: 198.18....)	Extranet (VPN IP: [REDACTED] .56)	SecureAccess-I...	Active	2024-04-23 13...
Branch FTD (VPN IP: 198.18....)	Hub FTD (VPN IP: [REDACTED] 9.20)	dVTI-PrimaryISP	Active	2024-04-23 13...
 Branch FTD (VPN IP: 198.18....)	Hub FTD (VPN IP: [REDACTED] 9.20)	dVTI-PrimaryISP	Active	2024-04-23 13...

View full information

A: Branch FTD ↔ B: Hub FTD

Topology: dVTI-PrimaryISP | Status: Active

GeneralCLI DetailsPacket Tracer

Topology

dVTI-PrimaryISP

Status

Active

Node A

Branch FTD

Node B

Hub FTD

Node A IP

[REDACTED] 7.10

Node B IP

[REDACTED] 9.20

Node A VPN Interface Name

ISP-2

Node B VPN Interface Name

Corp-ISP1

Last Updated

2024-04-23 13:30:56

SDWAN Updates in 7.6 release

- SDWAN Topology Wizard
- New capabilities for reference:
 - Policy Templates
 - Bulk Branch Onboarding Templates
 - Bulk Pre-Provisioning Templates for LTP
 - Tunnel/Route Setup Wizard



Secure Firewall 7.6 SD-WAN Topology Wizard

Firewall Management Center
Site To Site

Overview Analysis Policies Devices Objects Integration Deploy

admin

+ Add

Refresh

Select...

Topology Name

Hub-Spoke-VPN

VPN Type

- ☒ **SD-WAN Topology** New
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.
Select VPN Topology
☒ Hub and Spoke
[Prerequisites](#)
- ☐ **Route-Based VPN**
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.
Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer
- ☐ **Policy-Based VPN**
Secures traffic between peers based on a static policy using protected networks.
Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer
☐ Full Mesh
- ☐ **SASE Topology**
Simplifies and orchestrates the auto tunnel configuration between the threat defense device and the Umbrella SIG gateway.
Select VPN Topology
☐ Hub and Spoke

Cancel Create

Full automated VPN deployment!

Why did we create this new SDWAN wizard?

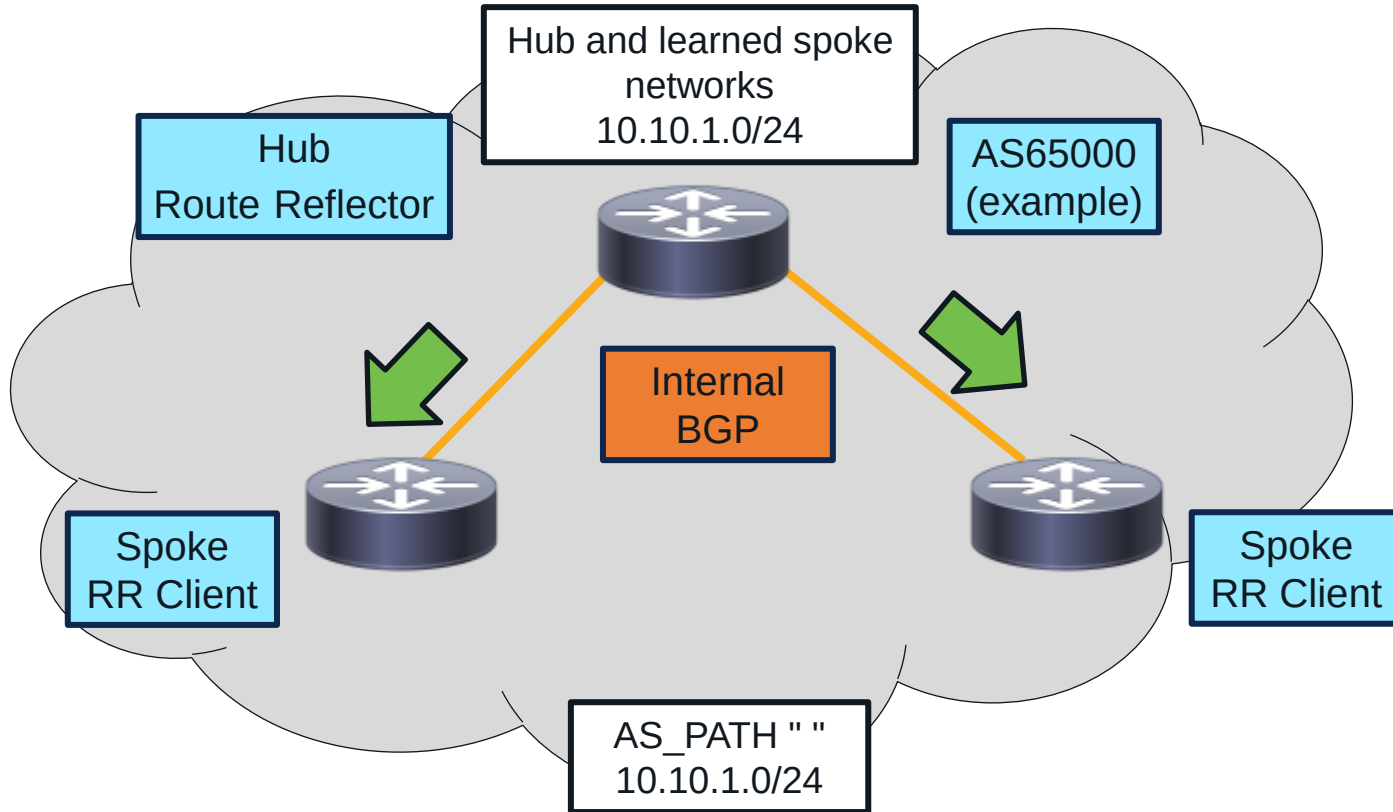
Pre-7.6 VPN deployment requirements:

- Manual & unique BGP configuration per spoke
- Manual assignment of spoke VTI interface IP address (and you have to keep track of these!)
- Easy but several steps for each spoke = time consuming

Starting with 7.6 SDWAN Topology automatically configures:

- VTI interface pool to auto-assign VTI interfaces of all spokes
- BGP configuration for all spokes using same BGP AS (iBGP)
- Fast and easy!

Why iBGP? How does it work? Route Reflection..



Secure Firewall 7.6 SD-WAN Topology Wizard

Firewall-Hub-Spoke

Hub and Spoke Route-Based (VTI) VPN Topology

Wizard configuration can be edited anytime to add more sites, make changes etc.

1

Hubs 

Device

ftdv-test-11
ftdv-test-12

DVTI

outside_dynamic_vti_1
outside_dynamic_vti_1

Gateway IP Address

64.100.14.211
64.100.14.212

Spoke Tunnel IP Address Pool

DVTI-IP-Pool
DVTI-IP-Pool-2

Edit

2

Spokes 

Device

ftdv-test-13
ftdv-test-14
ftdv-test-15
ftdv-test-16

VPN Interface

outside
outside
outside
outside

Local Tunnel (IKE) Identity

Key ID: Firewall-Hub-Spoke_ftdv-test-13
Key ID: Firewall-Hub-Spoke_ftdv-test-14
Key ID: Firewall-Hub-Spoke_ftdv-test-15
Key ID: Firewall-Hub-Spoke_ftdv-test-16

Edit

3

Authentication Settings 

Authentication

Pre-shared Automatic Key

Pre-shared Key Length

24

Edit

4

SD-WAN Settings

BGP enabled

true

Autonomous System Number

65100

Edit

Secure Firewall 7.6 SD-WAN Topology Wizard

4 SD-WAN Settings

Spoke Tunnel Interface Auto Generation

Static Virtual Tunnel Interfaces (SVTIs) are auto generated on each spoke using the spoke's VPN interface as tunnel source to establish a VPN to the DVTI on each of the hubs.

Spoke Tunnel Interface Security Zone ⓘ

VTI x v +

Overlay Routing Configuration

BGP can be enabled on the VPN overlay topology for seamless VPN connectivity from the spokes to the hub, and for spoke-to-spoke connectivity via the hub. [View more](#)

☒ Enable BGP on the VPN overlay topology

Autonomous System Number * ⓘ

65100

Community tag for local routes * ⓘ

2112

☒ Redistribute Connected Interfaces ⓘ

inside-interfaces x v +

☐ Secondary Hub is in different Autonomous System ⓘ

☒ Enable Multiple Paths for BGP

Allows multiple BGP routes to be used at the same time to reach the same destination. Enables BGP to load-balance traffic across multiple links.

- Automated iBGP configuration
- Auto-distribution of connected routes
- Community TAG support to tag routes



View By: Group

[All \(6\)](#)[Error \(0\)](#)[Warning \(0\)](#)[Offline \(0\)](#)[Normal \(6\)](#)[Deployment Pending \(6\)](#)[Upgrade \(0\)](#)[Snort 3 \(6\)](#)[Add](#)[Collapse All](#)[Download Device List Report](#)

☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
☐	Ungrouped (6)							
☐	ftdv-test-11 <small>Snort 3</small> 10.101.128.211 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	1 Edge Access Policy		
☐	ftdv-test-12 <small>Snort 3</small> 10.101.128.212 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	1 Edge Access Policy		
☐	ftdv-test-13 <small>Snort 3</small> 10.101.128.213 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	1 Edge Access Policy		
☐	ftdv-test-14 <small>Snort 3</small> 10.101.128.214 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	1 Edge Access Policy		
☐	ftdv-test-15 <small>Snort 3</small> 10.101.128.215 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	1 Edge Access Policy		
					Essentials, IPS (2 more...)	1 Edge Access Policy		

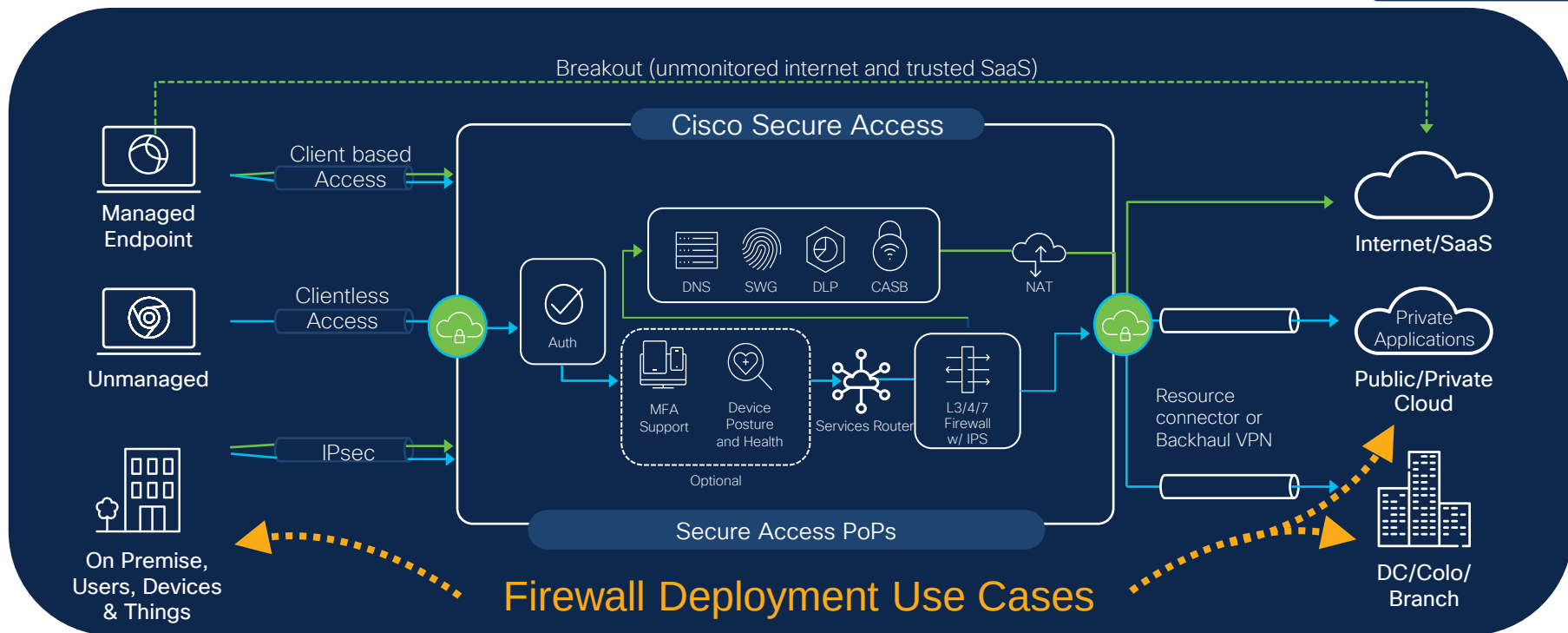
Firewall Management Center

Security Service Edge deployments

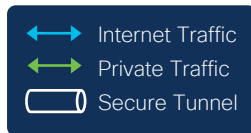
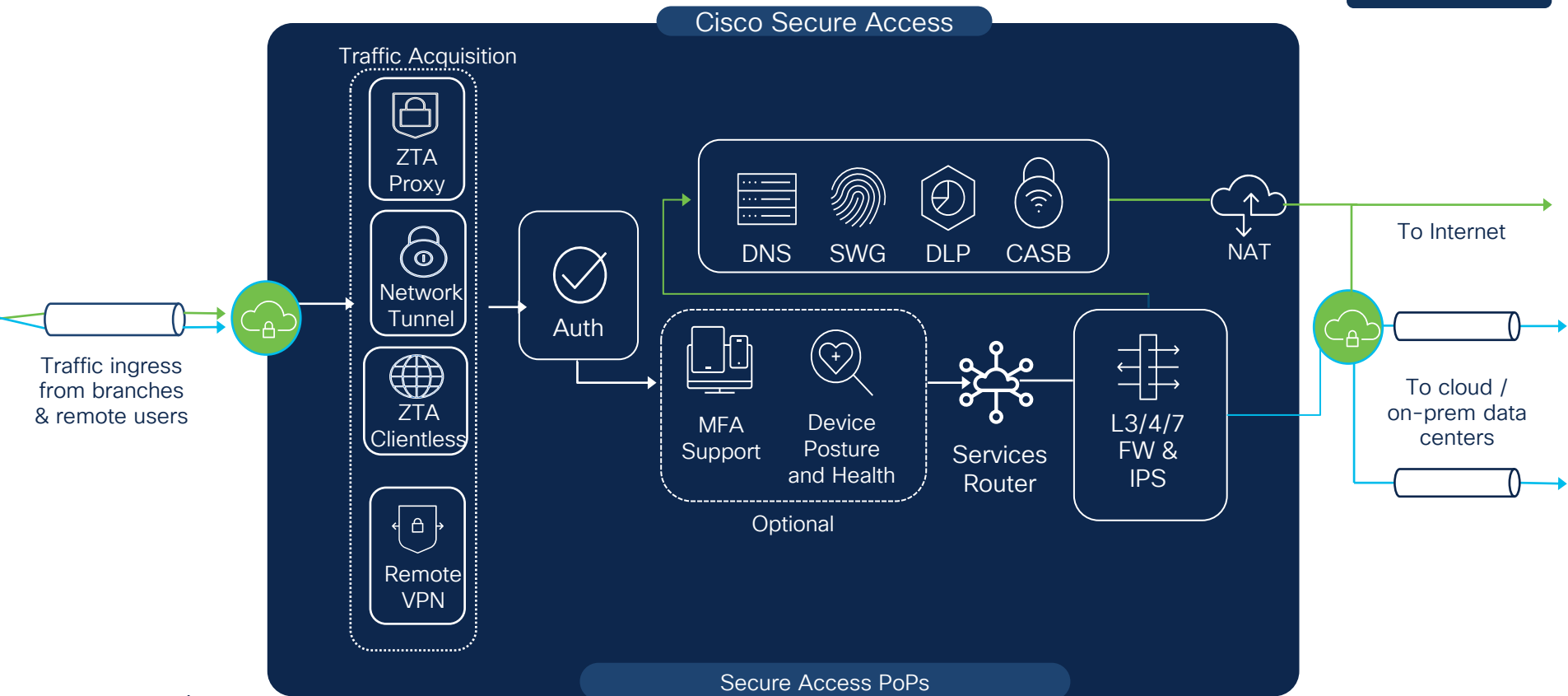
Featuring Cisco Secure Access



Secure Access (“Security Service Edge”)



Cloud Security Services



Why connect your branches to Secure Access?

Internet Security capabilities:

- Umbrella DNS protection
- DLP & CASB controls
- Web Application controls
- Microsoft & Google Tenant Controls
- Cloud malware protection, sandboxing, decryption.



Private application access:

- Connectivity to private apps protected by Secure Access
- Connectivity for private applications behind branch firewall
- Connectivity to cloud delivered RAVPN as a service subnets

Secure Access Branch Tunnels



Firewall Management Center
Site To Site

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy



admin ▾

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Hub-Spoke-Primary	Route Based (VTI)	Hub & Spoke	<div><div></div>4- Tunnels</div>	✓	
> Hub-Spoke-Secondary	Route Based (VTI)	Hub & Spoke	<div><div></div>4- Tunnels</div>	✓	
> Secure-Access-Virginia-Prim	Route Based (VTI)	Hub & Spoke	<div><div></div>3- Tunnels</div>	✓	
> Secure-Access-Virginia-Secr	Route Based (VTI)	Hub & Spoke	<div><div></div>3- Tunnels</div>	✓	

- Use Hub & Spoke VTI Tunnel topology for simplicity (not required)
- Dual topologies allow for redundant tunnels to backup DC
- eBGP or static routing to Secure Access data centers
 - Can assign “branch networks” to tunnel on Cloud Side if using static routing.

Branch Configuration for Secure Access tunnels

Tunnel addressing best practices:

- No need for loopback interfaces
- Use these IP tunnel addresses
 - 169.254.0.6/30 for Primary
 - 169.254.0.10/30 for Secondary

IPSec best practices:

- Use “Email ID” for tunnel identity
- Default IKEv2 and IPSec settings
- If using Hub & Spoke topology, all branches use same pre-shared key

Device:*

ftdv-test-3

Static Virtual Tunnel Interface

outside_static_vti_3 (IP: 169.254.6.73)

Tunnel Source: outside (IP: 64.105.73.73)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration:*

Email ID

ftdv-test-3@[REDACTED]-618854070

Branch Configuration for Secure Access tunnels

BGP Peering to Secure Access:

- Remote AS 64512
- Unique AS for each branch
- Use BGP Route Maps to restrict inbound / outbound route advertisements
- FTD static default route should use metric of 254 if BGP default from Secure Access is desired
- Backup tunnel from Secure Access will use AS prepend to ensure primary tunnel preference

ftdv-test-3
Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

▼ BGP

IPv4

IPv6

Enable IPv4: ☒

AS Number 65073

General Neighbor Add Aggregate Address

Address	Remote AS Number
169.254.0.5	64512
169.254.0.9	64512

```
> show bgp 0.0.0.0
BGP routing table entry for 0.0.0.0/0, version 530
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
    64512 64512
      169.254.0.9 from 169.254.0.9 (169.254.0.9)
        Origin IGP, localpref 100, valid, external
    64512
      169.254.0.5 from 169.254.0.5 (169.254.0.5)
        Origin IGP, localpref 100, valid, external, best
```

FTD Branch with Secure Access

Routes from Secure Access:

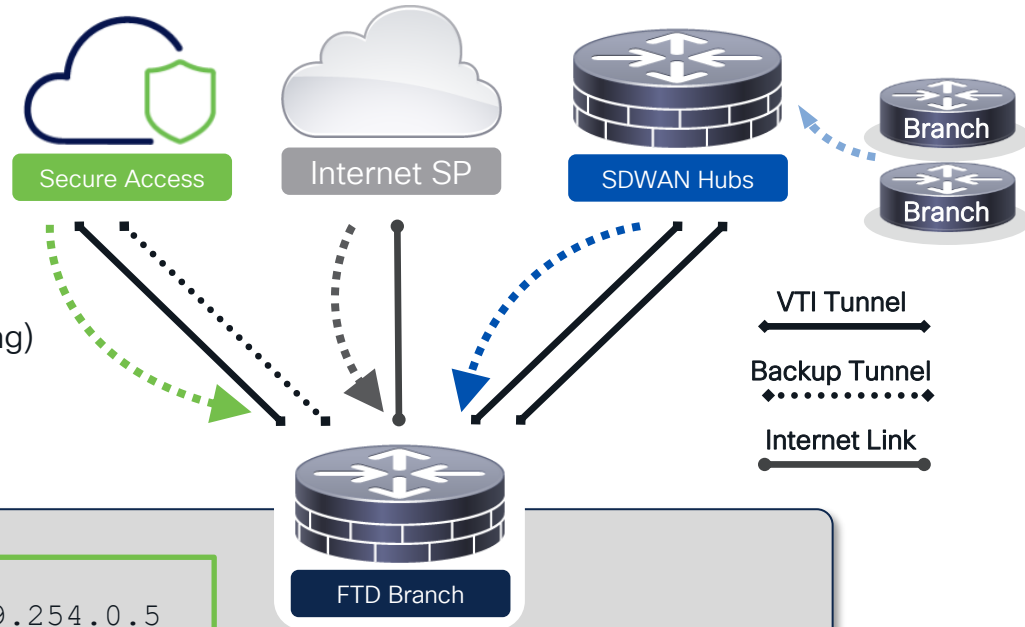
- Default Route* (Optional)
- RAVPN Subnets, Zero Trust enabled applications, Proxy Infrastructure

Static routes to ISP:

- Secure Access DC VPN Endpoint IPs (prevent flapping)

Routes from SDWAN Hubs:

- SDWAN HQ, branches, and data centers



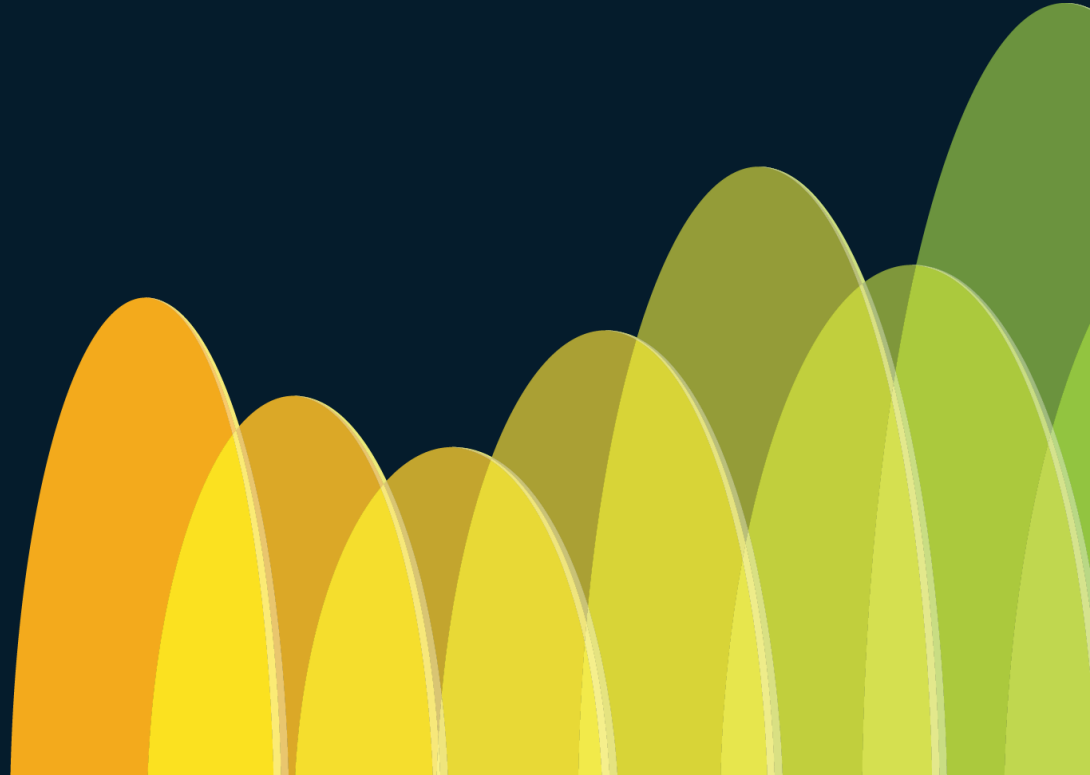
```
FTD-Spoke# show route
```

```
B* 0.0.0.0 0.0.0.0 [20/0] via 169.254.0.5
B 100.73.x.0 255.255.240.0 [20/0] via 169.254.0.5
```

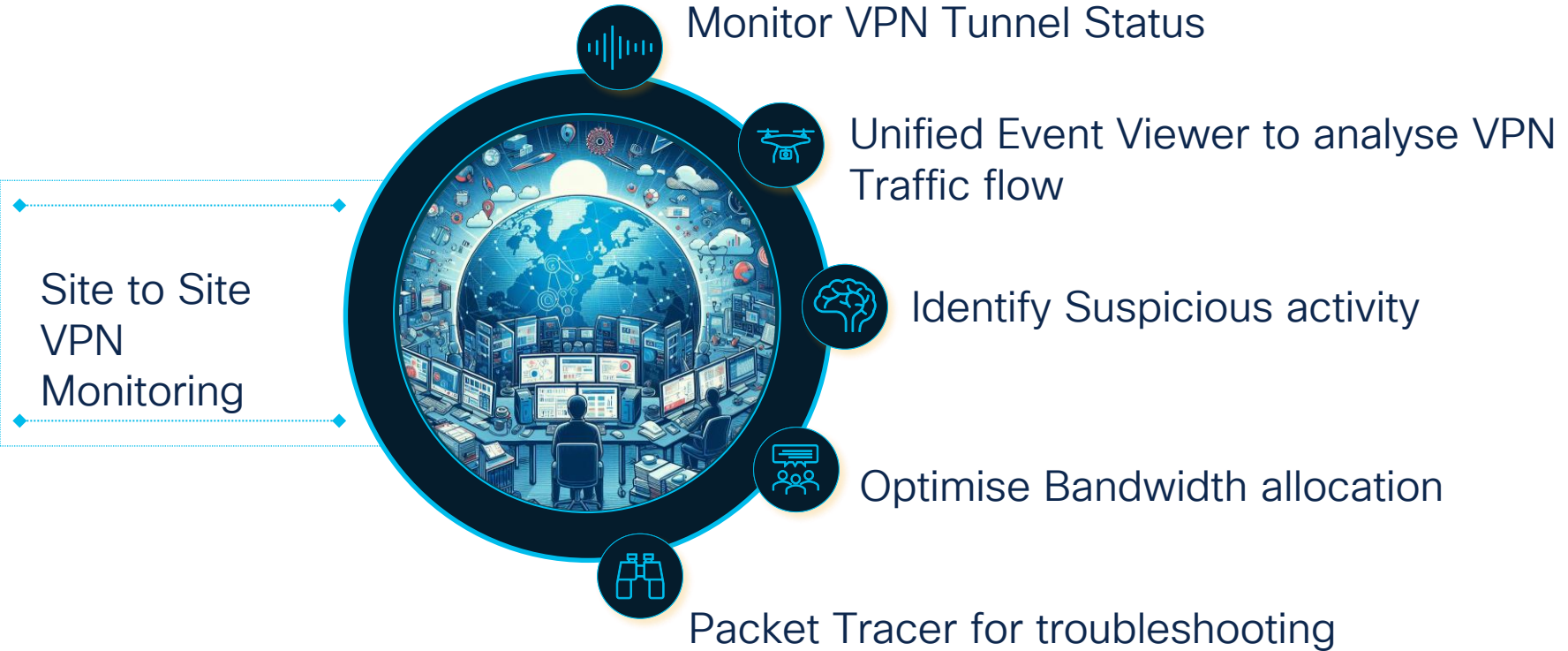
```
S 35.171.x.188 255.255.255.255 [1/0] via 64.x.14.254, outside
S 217.195.x.188 255.255.255.255 [1/0] via 64.x.14.254, outside
```

```
V 1.0.1.1 255.255.255.255 connected by VPN (advertised), outside_static_vti_1
V 1.0.2.1 255.255.255.255 connected by VPN (advertised), outside_static_vti_2
```

Monitoring & Troubleshooting



S2S VPN – Monitoring & Troubleshooting Insights



Site to Site Monitoring (7.4+)



Firewall Management Center

Overview / Dashboards / Site to Site VPN

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy



admin



Select...



Refresh

Refresh every 5 minutes



Node A	Node B	Topology	Status	Last Updated
10.10.1.19 (VPN IP: 10.10.1.39)	10.10.1.20 (VPN IP: 10.10.1.40)	VPN101-P2Pv4	Inactive	2023-01-30 12:48:49
10.10.1.19 (VPN IP: 9101::19)	10.10.1.20 (VPN IP: 9101::20)	VPN102-P2Pv6	No Active ...	N/A
10.10.1.19 (VPN IP: 10.10.1.69)	IOS99 (VPN IP: 192.168.102.99)	VPN103-HNSv4	No Active ...	N/A
10.10.1.19 (VPN IP: 10.10.1.69)	10.10.1.20 (VPN IP: 10.10.1.70)	VPN103-HNSv4	No Active ...	N/A
10.10.1.19 (VPN IP: 192.168.103.19)	10.10.1.20 (VPN IP: 192.168.103.20)	VPN104-SVTlv4	Active	2023-02-07 11:40:11
10.10.1.19 (VPN IP: 9104::19)	FTD02-EXTRANET (VPN IP: 9104::20)	VPN105-SVTlv6-FTD01	Active	2023-02-07 11:41:07
FTD02-EXTRANET (VPN IP: 9104::19)	10.10.1.20 (VPN IP: 9104::20)	VPN105-SVTlv6-FTD02	Active	2023-02-07 11:41:07
10.10.1.19 (VPN IP: 192.168.105.19)	10.10.1.20 (VPN IP: 192.168.105.20)	VPN106-DVTlv4	Active	2023-02-07 11:40:11
10.10.1.19 (VPN IP: 192.168.105.19)	IOS99 (VPN IP: 192.168.105.99)	VPN106-DVTlv4	No Active ...	N/A
10.10.1.19 (VPN IP: 9106::19)	10.10.1.20 (VPN IP: 9106::20)	VPN107-DVTlv6	Active	2023-02-07 11:40:11
10.10.1.19 (VPN IP: 9106::19)	IOS99 (VPN IP: 9106::99)	VPN107-DVTlv6	No Active ...	N/A

A: 10.10.1.19 ↔ B: 10.10.1.20

Topology: VPN106-DVTlv4 | Status: Active

General

CLI Details

Packet Tracer

Refresh

Maximize view

Summary

Node A (192.168.105.19/500)	Node B (192.168.105.20/500)
Transmitted: 560 Bytes (560 B)	Transmitted: 560 Bytes (560 B)
Received: 0 (0 B)	Received: 0 (0 B)

IPsec Security Associations (1)

192.168.15.0/255.255.255.0/0/0	192.168.25.0/255.255.255.0/0/0
L2L Tunnel PFS Group 21 IKEv2 VTI	
Encaps/Encrypt: 20 / 20 pkts	Encaps/Encrypt: 20 / 20 pkts
Dcaps/Decrypt: 0 / 0 pkts	Dcaps/Decrypt: 0 / 0 pkts
Remaining Lifetime for SPI ID: 0x2E5F96A1	
Outbound: 4.81 GB (5159999000 B) 09:09:05 (13145 sec)	Inbound: 5.03 GB (5400000000 B) 09:09:04 (13144 sec)
Remaining Lifetime for SPI ID: 0xE175D4C8	
Inbound: 4.97 GB (5340000000 B) 09:09:05 (13145 sec)	Outbound: 4.75 GB (5099999000 B) 09:09:04 (13144 sec)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

show crypto ipsec sa peer 192.168.105.20

show vpn-sessiondb detail 121 filter ipaddress 192.168.10...



Viewing 1-11 of 11



Site to Site Monitoring (7.4+)

Firewall Management Center
Overview / Dashboards / Site to Site VPN

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 ⚙️ ? admin ▾

SECURE

Select...

Node A

10.10.1.19

10.10.1.19

10.10.1.19

10.10.1.19

FTD02-EXT

10.10.1.19

10.10.1.19

10.10.1.19

10.10.1.19

Tunnel Details

?

×

Summary

Node A (192.168.105.19/500) ⓘ

Node B (192.168.105.20/500) ⓘ

Transmitted: 560 Bytes (560 B)

Received: 0 (0 B)

Transmitted: 560 Bytes (560 B)

Received: 0 (0 B)

IPsec Security Associations (1)

192.168.15.0/255.255.255.0/0/0

192.168.25.0/255.255.255.0/0/0

L2L Tunnel PFS Group 21 IKEv2 VTI

Encaps/Encrypt: 20 / 20 pkts

Dcaps/Decrypt: 0 / 0 pkts

Encaps/Encrypt: 20 / 20 pkts

Dcaps/Decrypt: 0 / 0 pkts

Remaining Lifetime for SPI ID: 0x2E5F96A1

Outbound: 4.81 GB (5159999000 B)

Inbound: 5.03 GB (5400000000 B)

08:53:49 (12229 sec)

08:53:48 (12228 sec)

Remaining Lifetime for SPI ID: 0xE175D4C8

Inbound: 4.97 GB (5340000000 B)

Outbound: 4.75 GB (5099999000 B)

08:53:49 (12229 sec)

08:53:48 (12228 sec)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

10.10.1.20 (VPN Interface IP: 192.168.105.20)

show crypto ipsec sa peer 192.168.105.20 ⓘ

peer address: 192.168.105.20

interface: DVTI105_va4

Crypto map tag: DVTI105_vtemplate_dyn_map, seq num: 1,

Protected vrf (ivrf): Global

local ident (addr/mask/prot/port): (192.168.15.0/255

show crypto ipsec sa peer 192.168.105.19 ⓘ

show vpn-sessiondb detail l2l filter ipaddress 192.1...

Close Refresh

×

Refresh

Refresh every 5 minutes

▶

A: 10.10.1.19 ↔ B: 10.10.1.20

Topology: VPN106-DVTiv4 | Status: Active

General CLI Details Packet Tracer

Refresh Maximize view

Summary

Node A (192.168.105.19/500) ⓘ

Node B (192.168.105.20/500) ⓘ

Transmitted: 560 Bytes (560 B)

Received: 0 (0 B)

Transmitted: 560 Bytes (560 B)

Received: 0 (0 B)

IPsec Security Associations (1)

192.168.15.0/255.255.255.0/0/0

192.168.25.0/255.255.255.0/0/0

L2L Tunnel PFS Group 21 IKEv2 VTI

Encaps/Encrypt: 20 / 20 pkts

Dcaps/Decrypt: 0 / 0 pkts

Encaps/Encrypt: 20 / 20 pkts

Dcaps/Decrypt: 0 / 0 pkts

Remaining Lifetime for SPI ID: 0x2E5F96A1

Outbound: 4.81 GB (5159999000 B)

Inbound: 5.03 GB (5400000000 B)

08:53:49 (12229 sec)

08:53:48 (12228 sec)

Remaining Lifetime for SPI ID: 0xE175D4C8

Inbound: 4.97 GB (5340000000 B)

Outbound: 4.75 GB (5099999000 B)

08:53:49 (12229 sec)

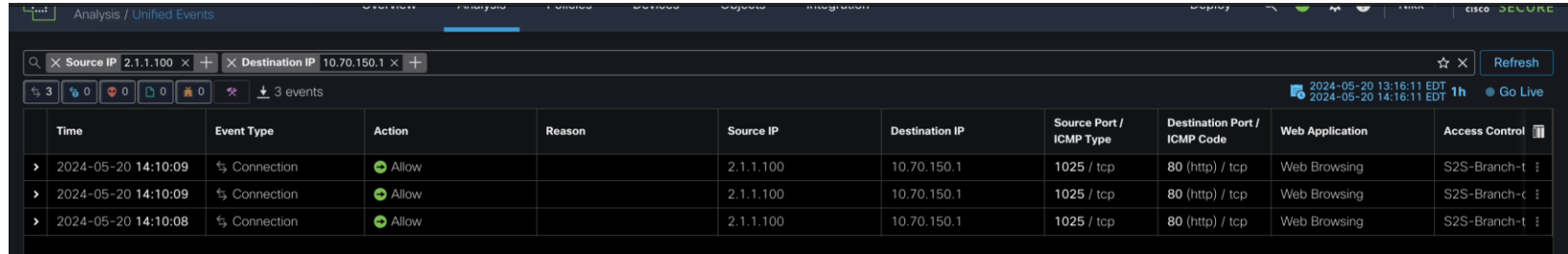
08:53:48 (12228 sec)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

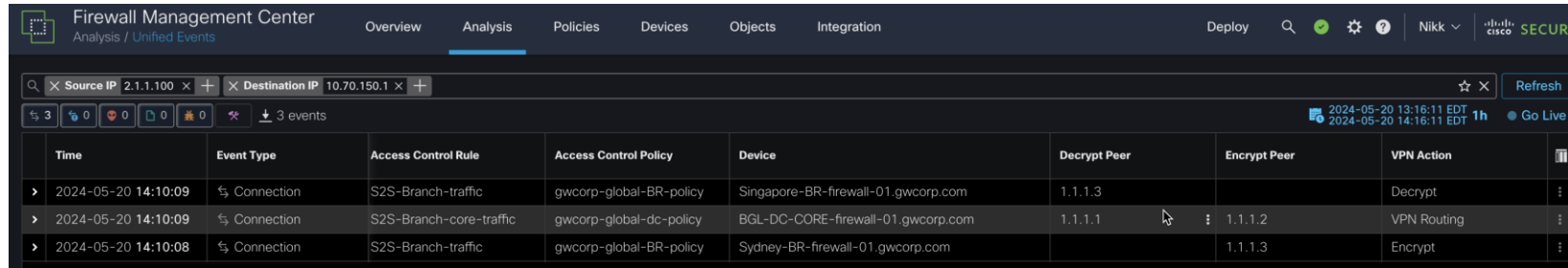
show crypto ipsec sa peer 192.168.105.20 ⓘ

show vpn-sessiondb detail l2l filter ipaddress 192.168.10...

S2S VPN Monitoring Dashboard – Unified Viewer



Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control
2024-05-20 14:10:09	Connection	Allow		2.1.1.100	10.70.150.1	1025 / tcp	80 (http) / tcp	Web Browsing	S2S-Branch-t
2024-05-20 14:10:09	Connection	Allow		2.1.1.100	10.70.150.1	1025 / tcp	80 (http) / tcp	Web Browsing	S2S-Branch-c
2024-05-20 14:10:08	Connection	Allow		2.1.1.100	10.70.150.1	1025 / tcp	80 (http) / tcp	Web Browsing	S2S-Branch-t



Time	Event Type	Access Control Rule	Access Control Policy	Device	Decrypt Peer	Encrypt Peer	VPN Action
2024-05-20 14:10:09	Connection	S2S-Branch-traffic	gwcop-global-BR-policy	Singapore-BR-firewall-01.gwcop.com	1.1.1.3		Decrypt
2024-05-20 14:10:09	Connection	S2S-Branch-core-traffic	gwcop-global-dc-policy	BGL-DC-CORE-firewall-01.gwcop.com	1.1.1.1	1.1.1.2	VPN Routing
2024-05-20 14:10:08	Connection	S2S-Branch-traffic	gwcop-global-BR-policy	Sydney-BR-firewall-01.gwcop.com		1.1.1.3	Encrypt

Complete
connection log
available

WAN Summary Dashboard (7.4)

- 1 Application bandwidth consumption data
- 2 WAN interfaces status
- 3 VPN interfaces status
- 4 WAN interfaces throughput
- 5 Inventory of Devices part of WAN topology
- 6 Overall SDWAN Health

Detailed View in Health Monitoring



Enable SD-WAN Application Monitoring from Health Policy

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The main panel shows the 'Initial_Health_Policy' configuration page, dated 2023-08-03 06:00:29. The page is divided into sections for 'Appliance/Hardware', 'Disk', 'Processes', and 'High Availability'. The 'SD-WAN' section is highlighted with a red box, showing 'SD-WAN Monitoring' is enabled. An inset shows the navigation menu with 'Health' > 'Policy' selected.

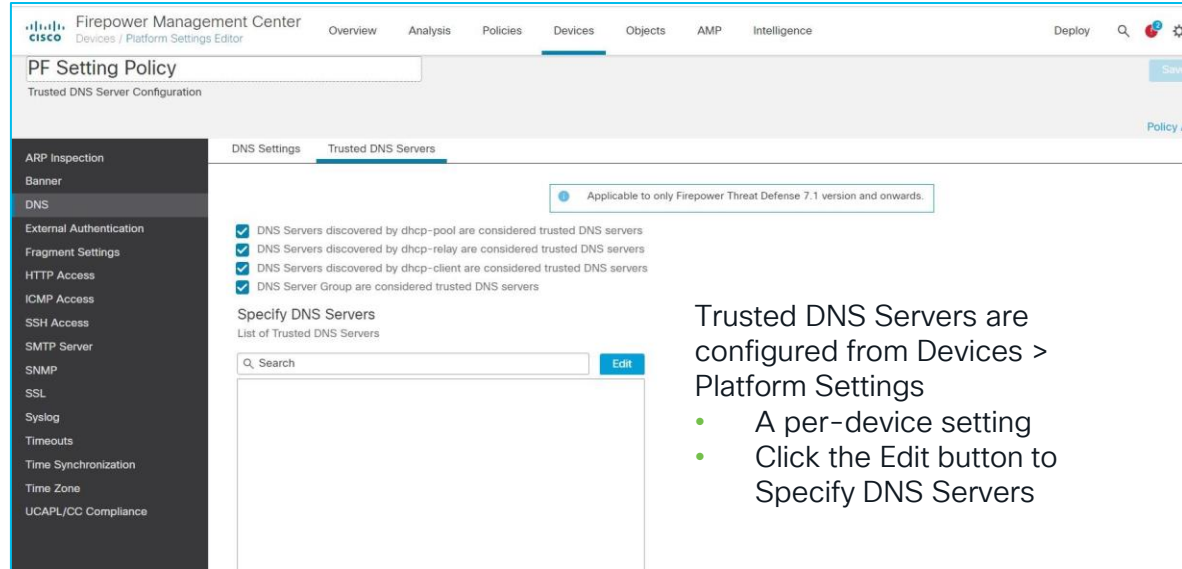
Navigation Menu:

- Configuration
 - Users
 - Domains
 - Content Updates
 - Licenses
 - Smart Licenses
 - Classic Licenses
- Health
 - Monitor
 - Policy**
 - Events
 - Exclude
 - Monitor Alerts
- Monitoring
 - Audit
 - Syslog
 - Statistics
 - Tools
 - Backup/Restore
 - Scheduling
 - Import/Export
 - Data Purge

1. User can enable/disable SD-WAN Monitoring feature from Settings -> Health -> Edit FTD Policy page
2. By default, SD-WAN Monitoring is enabled

SD-WAN Application Prerequisites

- DNS Server should be added as part of trusted sources in FMC.
- DNS Inspection *must* be enabled from FMC so FTD can do DNS Snooping.
- All egress paths should be in the same ECMP group for the PBR policy to get applied.



SD-WAN Application Monitoring – Path Monitoring

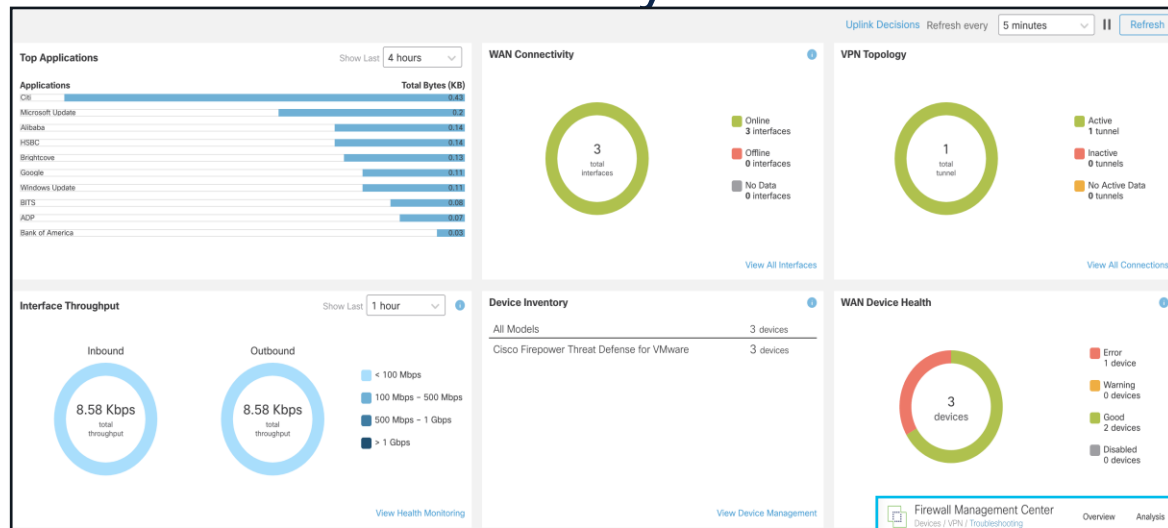
The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is selected, showing a list of interfaces. The 'Edit Physical Interface' dialog is open for 'GigabitEthernet0/2'. The 'Path Monitoring' tab is active, showing the following configuration:

- ☒ Enable IP based Monitoring
- Monitoring Type: Next-hop of default route out of interface (Auto)
- ☒ Enable HTTP based Application Monitoring
- Applications:
 - ADP
 - ADP GlobalView
 - ADP Resource

The background shows the 'Interfaces' page with a list of interfaces. The 'GigabitEthernet0/2' interface is highlighted in blue.

By default, HTTP-based monitoring is enabled and data for the same is seen in the Monitoring Dashboard if PBR is enabled with applications

SD-WAN Summary Dashboard



Uplink Decisions

- Launches the **VPN Troubleshooting Logs** page in a new tab filtered by PBR syslog ID FTD-6-880001.

PBR Syslog FTD-6-880001 shows uplink or egress interface decision changes by PBR due change in monitored metrics of the link/interface.

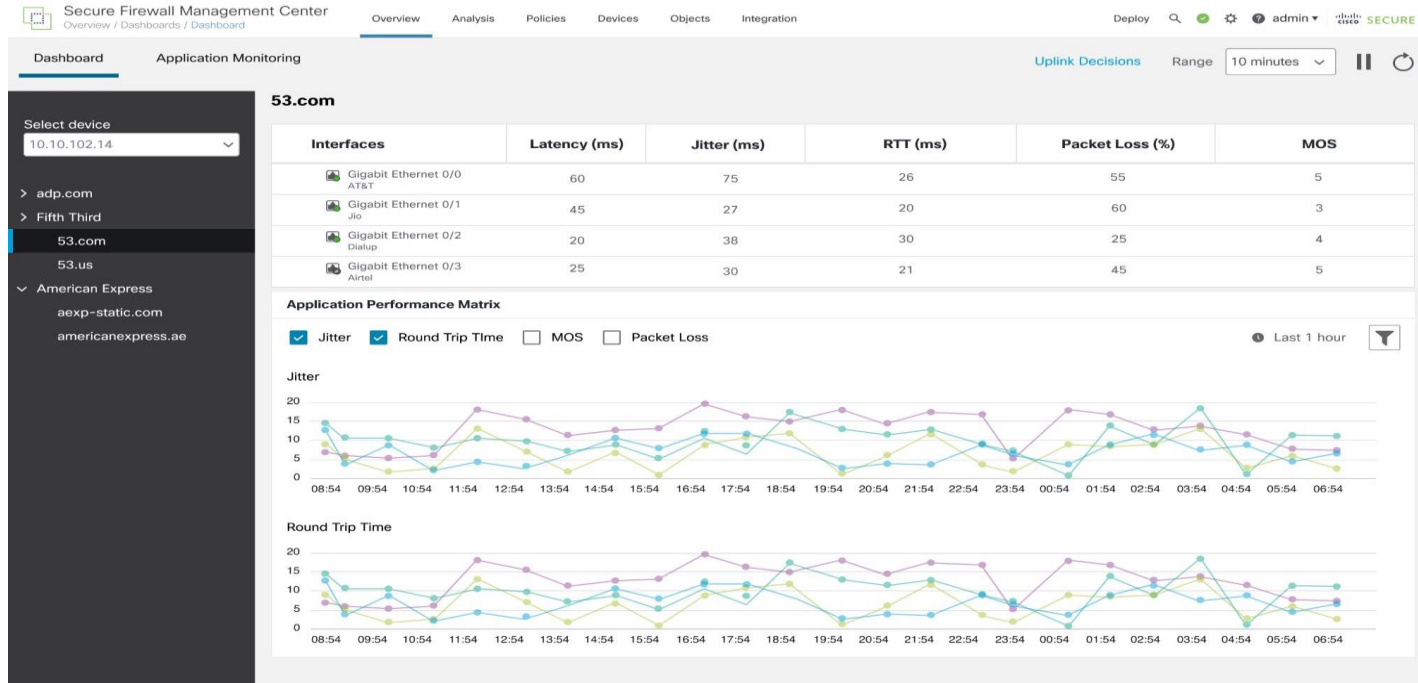
Overview Summary has following widgets for WAN Devices (Devices with Site-to-site VPN or PBR):

- Top Applications
- WAN Connectivity (WAN Link status)
- Interface Throughput on WAN Links
- VPN Topology (VPN Tunnel status)
- WAN Device Inventory and Device Health

The screenshot shows the Firewall Management Center (FTD) interface, specifically the VPN Troubleshooting logs. The logs are filtered by PBR syslog ID FTD-6-880001. The table displays the following columns: Time, Severity, Message, Message Class, Username, and Device.

Time	Severity	Message	Message Class	Username	Device
2023-08-28 07:03:56	Info	Ingress IFC inside-bo, For traffic [10.10.7.201->63.140.62.160], PBR picked outside-bo-lsp1 as its jitter metrics became better than outside-web-lsp3	pbr	admin	BoR-144
2023-08-28 07:03:07	Info	Ingress IFC inside-bo, For traffic [10.10.7.201->104.114.103.43], PBR picked outside-web-lsp3 as its jitter metrics became better than outside-bo-lsp1	pbr	admin	BoR-144
2023-08-28 06:33:26	Info	Ingress IFC inside-bo, For traffic [10.10.7.201->35.172.90.106], PBR picked outside-bo-lsp1 as its jitter metrics became better than outside-web-lsp3	pbr	admin	BoR-144
2023-08-28 06:33:02	Info	Ingress IFC inside-bo, For traffic [10.10.7.201->104.114.103.43], PBR picked outside-web-lsp3 as its jitter metrics became better than outside-bo-lsp1	pbr	admin	BoR-144
2023-08-28 06:32:25	Info	Ingress IFC inside-bo, For traffic [10.10.7.201->171.158.118.26], PBR picked outside-bo-lsp1 as its jitter metrics became better than outside-web-lsp3	pbr	admin	BoR-144
2023-08-28 06:31:58	Info	Ingress IFC inside-bo, For traffic [10.10.7.201->44.209.118.18], PBR picked outside-web-lsp3 as its jitter metrics became better than outside-bo-lsp1	pbr	admin	BoR-144
2023-08-28 05:15:49	Info	Ingress IFC inside-bo, For traffic [10.10.7.201->104.114.103.43], PBR picked outside-bo-lsp1 as its jitter metrics became better than outside-web-lsp3	pbr	admin	BoR-144
2023-08-28 05:08:35	Info	Ingress IFC inside-bo, For traffic [10.10.7.201->52.154.174.214], PBR picked outside-web-lsp3 as its jitter metrics became better than outside-bo-lsp1	pbr	admin	BoR-144
2023-08-28 04:59:34	Info	Ingress IFC inside-bo, For traffic [10.10.7.201->52.247.36.244], PBR picked outside-bo-lsp1 as its jitter metrics became better than outside-web-lsp3	pbr	admin	BoR-144

Enhanced WAN Application Monitoring



- Easily monitor all interfaces where Policy-Based Routing is enabled
- Detailed application performance metrics for Jitter, Round Trip Time, MOS and Packet Loss

VPN Packet Tracer (7.3+)

Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ? admin ✓ CISCO SECURE

Select... Refresh Refresh every 5 minutes ▶

Node A	Node B	Topology	Status	Last Updated
Branch1 (VPN IP: 10.10.0.202)	Branch2 (VPN IP: 10.10.0.203)	HnS-NATExempt	Inactive	2023-01-06 02:49...

- Policy and data plane tests for traffic across VTI tunnels
- Not supported from loopback or VTI interfaces (run from data interfaces only)
- Support for decrypted flows

A: Branch1 ↔ B: Branch2
Topology: HnS-NATExempt | Status: Inactive

General CLI Details **Packet Tracer**

SELECT TRACE



▼ See Trace Config

Node A Traces **Node B Traces**

Node A Traces:

- ✗ → Drop A: In → Out
- ✓ ROUTE-LOOKUP 175.06µs
- ✓ OBJECT-GROUP-SE... 0ms
- ✓ ACCESS-LIST 293ns
- ✓ CONN-SETTINGS 293ns
- ✓ NAT 293ns
- ✓ NAT 293ns
- ✓ IP-OPTIONS 293ns
- ✓ INSPECT 21.03µs
- ✓ INSPECT 2.93µs

Node B Traces:

- ✗ → Drop B (Decrypted): Out → In
- ✓ ROUTE-LOOKUP 137.41µs
- ✗ Result: Drop 137.41µs
- ✗ ← Drop B: Out ← In

Viewing 1-1 of 1

CLI configuration to onboard FTDv

Reference

Allows management on outside interface for cdFMC connectivity

```
> configure network management-data-interface

Data interface to use for management: GigabitEthernet0/0
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 38. .83
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 38. .1

Configuration done with option to allow FMC access from any network, if you wish
to change the FMC access network use the 'client' option in the command 'config
ure network management-data-interface'.
```

- Physical firewalls offer “Low Touch Provisioning” based on serial # to cdFMC
- Virtual firewalls offer CLI provisioning.
- “configure network management-data-interface” to manage firewall on outside interface

Get Security Cloud Control **free** for 1 year



http://cs.co/free_SCC



Offer includes:



Multicloud Defense
(max: 9,000 Gateway Hours)



Security Analytics and Logging
(Cloud logging 50Gb/day
with 90 days retention)



Cloud-delivered
Firewall Management Center

Offer available to first 500 customers

Get Security Cloud Control **free** for 1 year

For select customers with the following use cases
(terms and conditions apply):

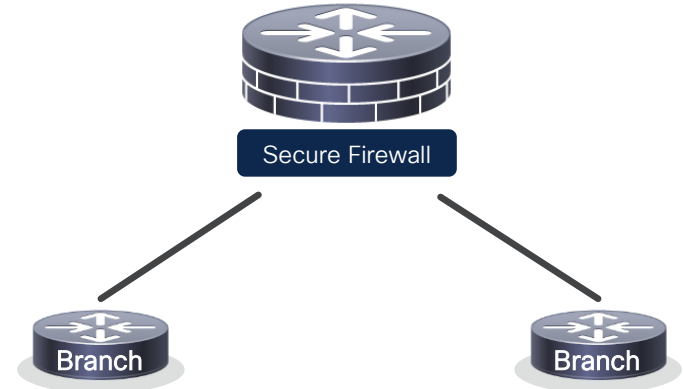


Capabilities	ASA Firewalls using CLI/CSM/ASDM	FTD Firewalls using FDM	FTD Firewalls using FMC
Multicloud Defense (max: 9,000 Gateway Hours)	•	•	•
Unified Event Viewer for easy monitoring & troubleshooting (50Gb/day with 90 days retention)	•	•	•
Manage firewalls of different form factors from the cloud	•	•	•
Migration path to FTD/cdFMC through Security Cloud Control	•	•	•
Cisco managed upgrades, updates, and uptime	•	•	•
Share objects across hybrid and multi-cloud environments	•	•	•
Streamlines policy management across diverse security firewall offerings	•		
Auto-scales to any size environment		•	•
Cloud assist capabilities - AI Assistant, AI Ops, Policy optimiser & Analyser (Future)		•	•
Early access to FMC features in cloud			•

Secure Firewall Threat Defense

Scalable hub and spoke VPNs for up to 1,000 sites (per topology!)

- Policy Based Routing on FTD to prioritise Internet links or tunnels to optimise security and end user experience!
- Use Virtual Tunnel Interface for all VPN tunnels including SASE deployments!
- Must use routing protocol for DVTI hub spoke topologies





Speaker Survey



cisco *Live!*



Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC