cisco The bridge to possible

Optimizing Security and Agility

Leveraging SD-WAN with Cisco Secure Firewall

Alejandra Páez Castro
Security Technical Leader, CX Americas

BRKSEC-2086

Session Abstract

As organizations expand their operations, ensuring secure and streamlined connectivity becomes paramount. To address the challenges related to secure connectivity, Cisco Secure Firewall Threat Defense introduces new SD-WAN capabilities that provide connectivity without compromising security. This session will cover the SD-WAN capabilities introduced in Cisco Secure Firewall Threat Defense, such as Firewall configuration to steer traffic directly to the Internet through multiple active WAN links based on either applications or users (DIA), firewall operation, and configuration to select the best egress interface based on link metrics (DIA with Path Monitoring) and SASE/SSE integration. By the end of the session, a live Demo will allow attendees to visualize how these features work and how to identify and troubleshoot potential issues

Some SDWAN Capabilities can be leveraged in the Secure Firewall to simplify branch deployments, optimize network performance, and ensure better user application experience while keeping the network secure.

Know your Presenter

Alejandra Páez Castro

- Venezuelan
  - Currently Living in Mexico
- Telecommunications Engineer
- 6 years as Technical Consulting Engineer in Firewall TAC
- 3 years+ as Security Technical Leader in CX
- Passionate about Network Security

cisco The bridge to possible
Implement Direc
Access with Sec
Threat Defense
Alejandra Páez Castro, Security Techn
cisco Live!

Cisco Webex App

Questions?

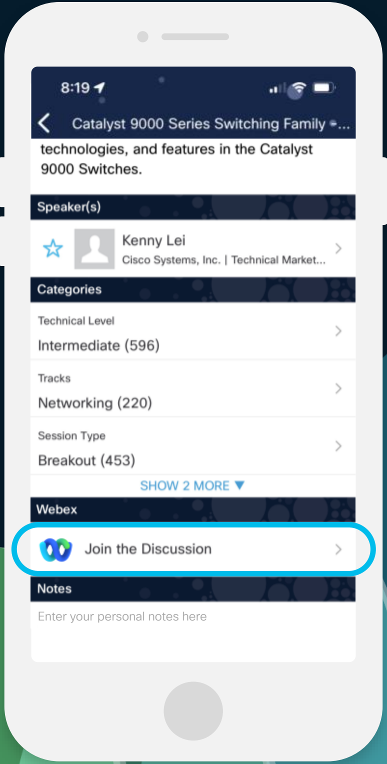
Use Cisco Webex App to chat
with the speaker after the session

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 June 7, 2024.

https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKSEC-2086



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

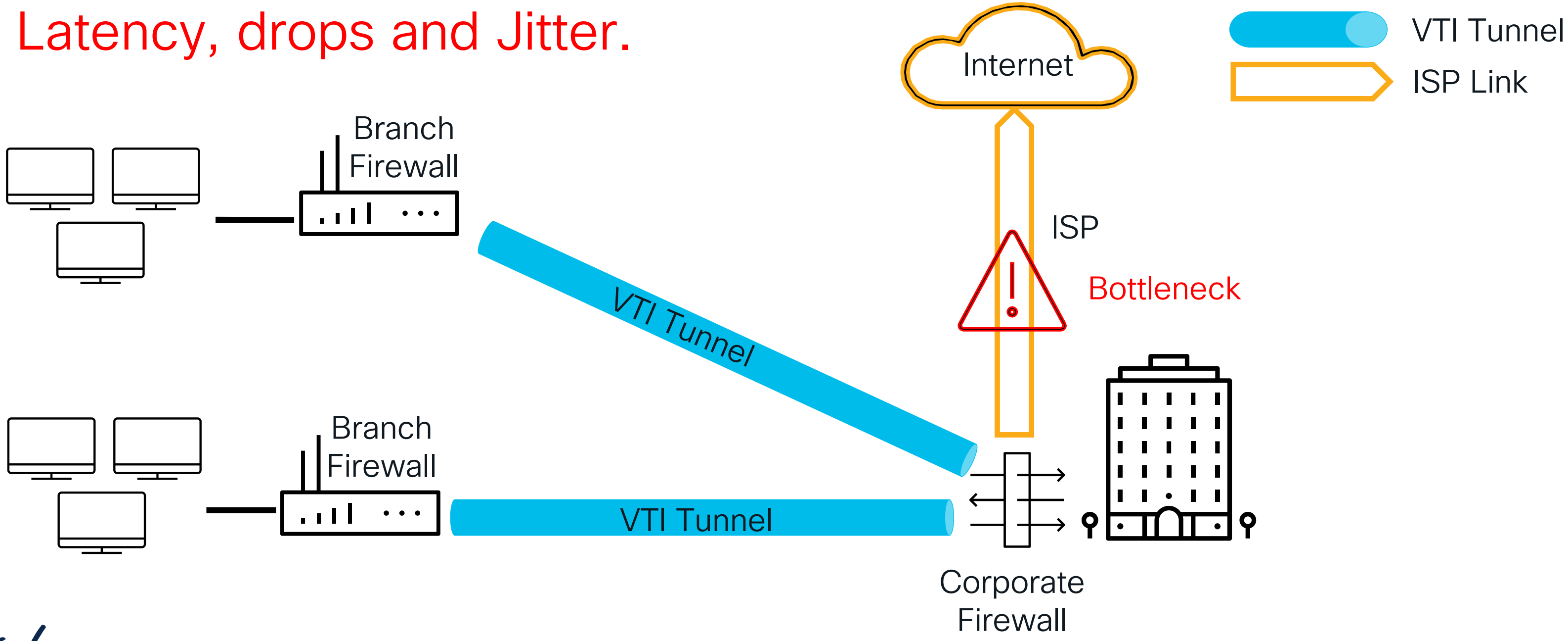
Agenda

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

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 to headquarters (6.7+)
- IPV6 VTI

WAN Optimization

- Active-Standby Backup VTI tunnel configuration
- Optimal Path selection based on interface monitoring

Increased Usable Bandwidth

- Increased support for load-balancing across multiple ISPs
- ECMP Support for sVTI
- Application based load balancing using Policy Based Routing (7.1+)

Direct Internet Access for Public cloud

- SaaS Application detection
- PBR using Application and users as matching criteria (7.4+)
- Optimal Path selection based on interface statistics(7.2+)

Simplified Management

- Data Interface Management
- SASE: Umbrella Auto-Tunnel deployment
- DVTI Hub and Spoke topology simplification (7.3+)

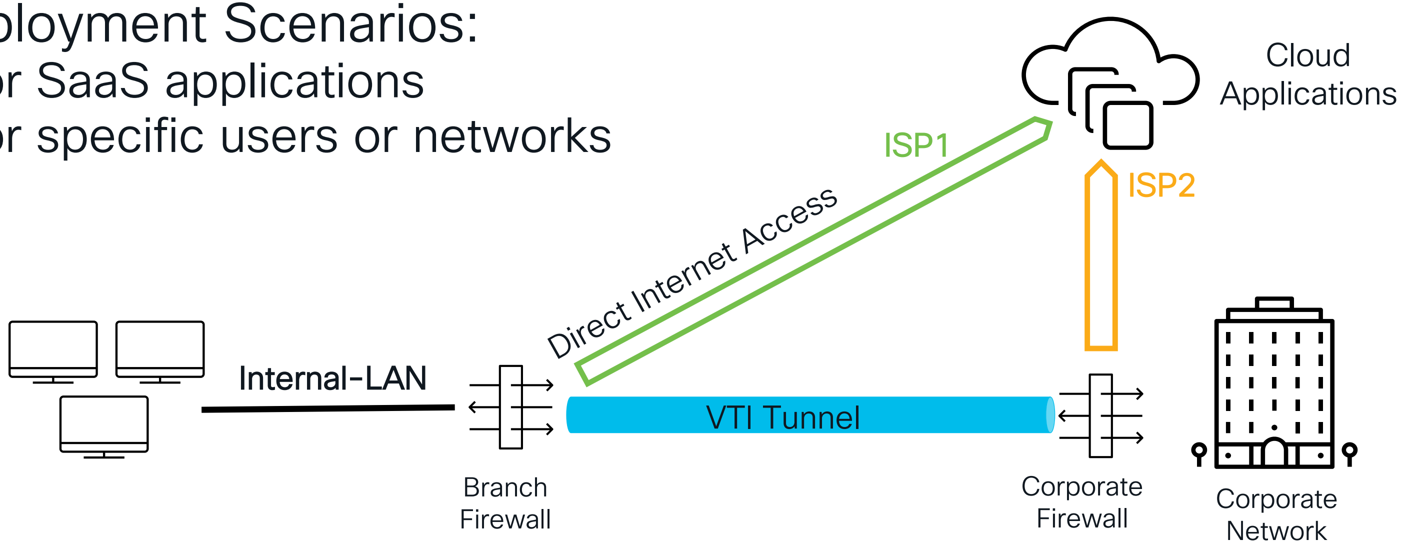
Direct Internet Access

Direct Internet Access (DIA)

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

Deployment Scenarios:

- For SaaS applications
- For specific users or networks



DIA Components (From FTD 7.1+)

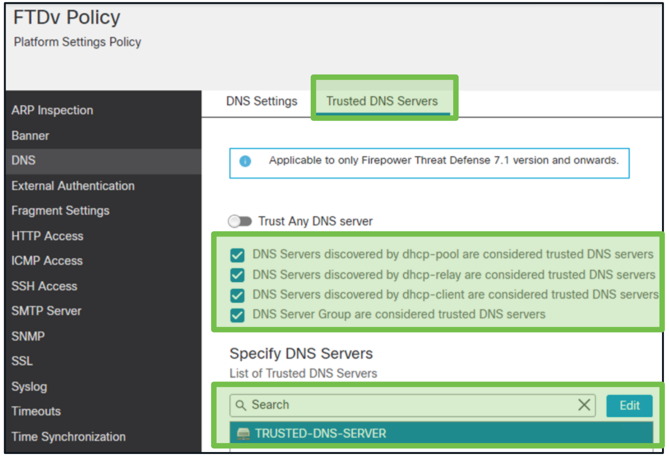
Vulnerability Database (VDB)

- VDB supplies the list of domains for application detection used by DIA
  - Keep the VDB version updated

```
firepower# show object network-service
[…]
object network-service "Cisco" dynamic
 description Official website for Cisco.
 app-id 2655
 domain cisco.com (bid=1851027941) ip (hitcnt=0)
object network-service "Duo Security" dynamic
 description A user-centric access security platform that provides two-factor
 authentication, endpoint security, remote access solutions and a
 subsidiary of Cisco.
 app-id 4648
 domain duosecurity.com (bid=-2050678515) ip (hitcnt=0)
 domain duo.com (bid=-2050510683) ip (hitcnt=0)
[…]
```

Trusted DNS Server

- Application-based Policy Based Routing (PBR) uses DNS Snooping to map the application domains to IP addresses
  - Ensure clear-text DNS traffic travels through Firewall



Applicable to only Firepower Threat Defense 7.1 version and onwards.

○ Trust Any DNS server

☑ DNS Servers discovered by dhcp-pool are considered trusted DNS servers
☑ DNS Servers discovered by dhcp-relay are considered trusted DNS servers
☑ DNS Servers discovered by dhcp-client are considered trusted DNS servers
☑ DNS Server Group are considered trusted DNS servers

Specify DNS Servers
List of Trusted DNS Servers

TRUSTED-DNS-SERVER

```
firepower# show runn dns
dns domain-lookup ISP1
dns domain-lookup ISP2
DNS server-group DNS-Server
    name-server 10.10.10.10
    domain-name cisco.com
dns-group DNS-Server
dns trusted-source 10.10.10.10
```

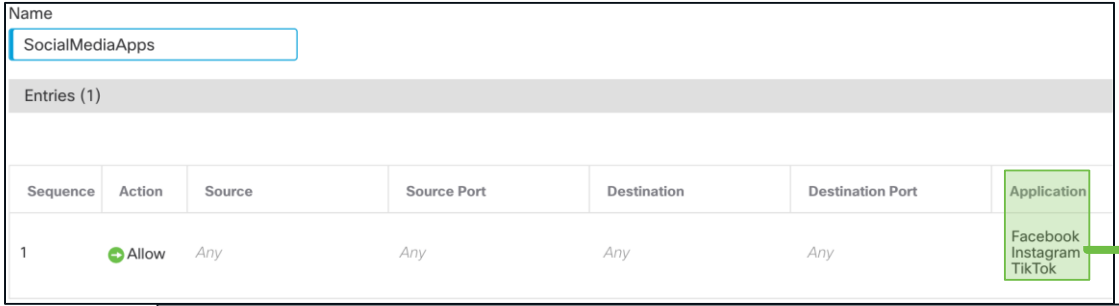
Network Service Object (NSO)

- Object associated with a particular application
  - NSOs are predefined and deployed to FTD from the FMC

```
firepower# show object id "Webex Teams"
object network-service "Webex Teams" dynamic
app-id 4080
 domain code.s4d.io (bid=839581615) ip (hitcnt=0)
 domain huron-dev.com (bid=839671741) ip (hitcnt=0)
 domain worklife.com (bid=839793477) ip (hitcnt=0)
 domain ciscospark.com (bid=839938715) ip (hitcnt=0)
 domain wbx2.com (bid=840165323) ip (hitcnt=0)
 domain idbroker.webex.com (bid=840285097) ip (hitcnt=0)
 domain teams.webex.com (bid=840320705) ip (hitcnt=0)
```

Network Service Group (NSG)

- FMC auto-generates NSGs based on the Extended Access Lists configured for PBR
  - Multiple NSOs can be part of a single NSG



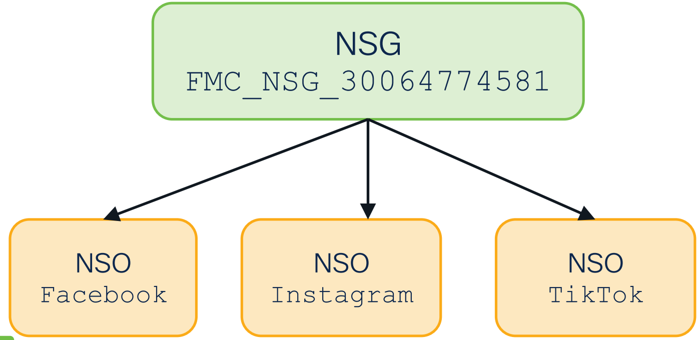
Name

SocialMediaApps

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application
1	Allow	Any	Any	Any	Any	Facebook Instagram TikTok

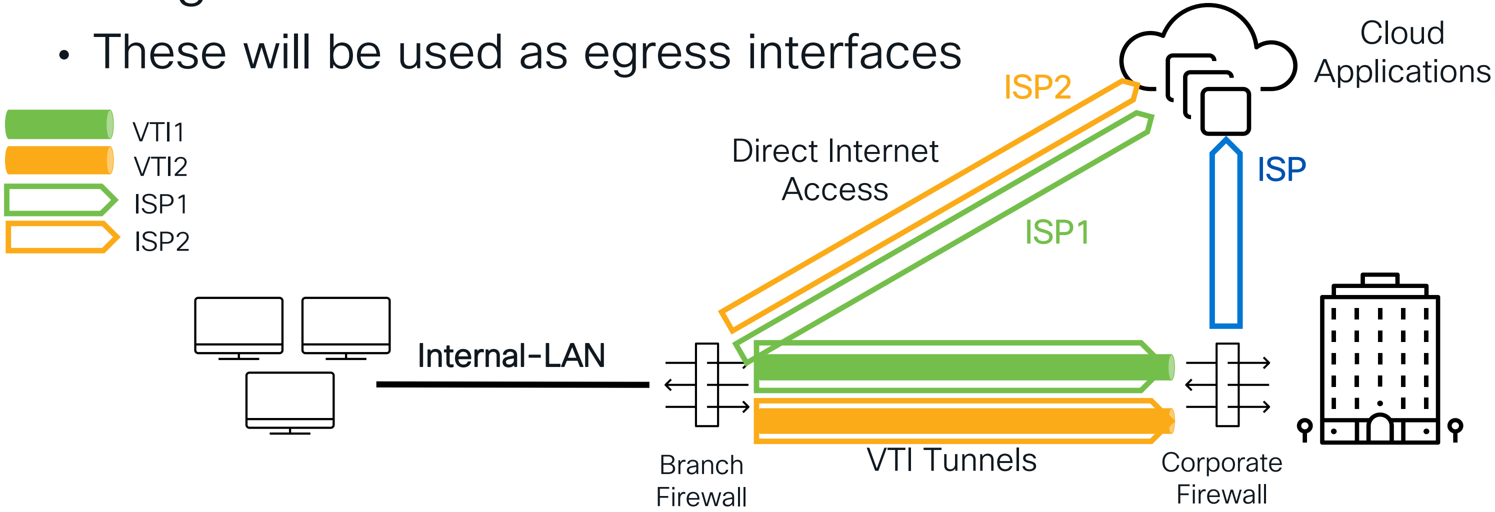
```
firepower# show runn access-list SocialMediaTraffic
access-list SocialMediaTraffic extended permit ip any object-group-network-service FMC_NSG_30064774581
firepower# show runn object-group network-service
object-group network-service FMC_NSG_30064774581
 network-service-member "Facebook"
 network-service-member "Instagram"
 network-service-member "TikTok"
```



DIA Configuration Walkthrough

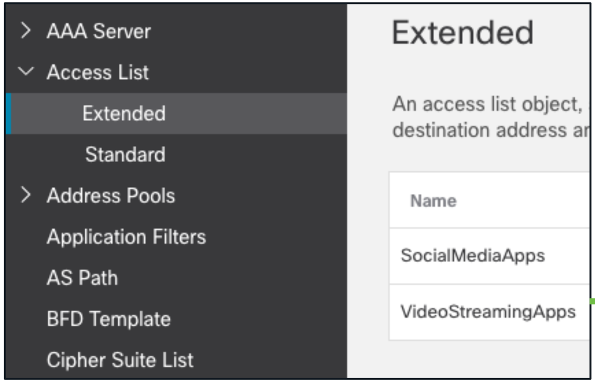
Configure Interfaces

- 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

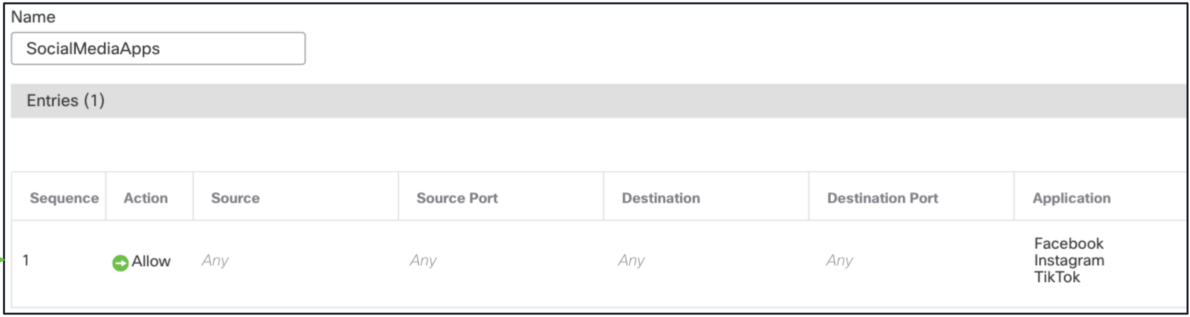
- Configure Extended Access List for Applications
  - The selected applications (NSOs) in each of the Access Control entries form a NSG
  - This NSG is used in DIA to classify traffic based on the match criteria



Extended

An access list object,
destination address ar

Name
SocialMediaApps
VideoStreamingApps



Name: SocialMediaApps

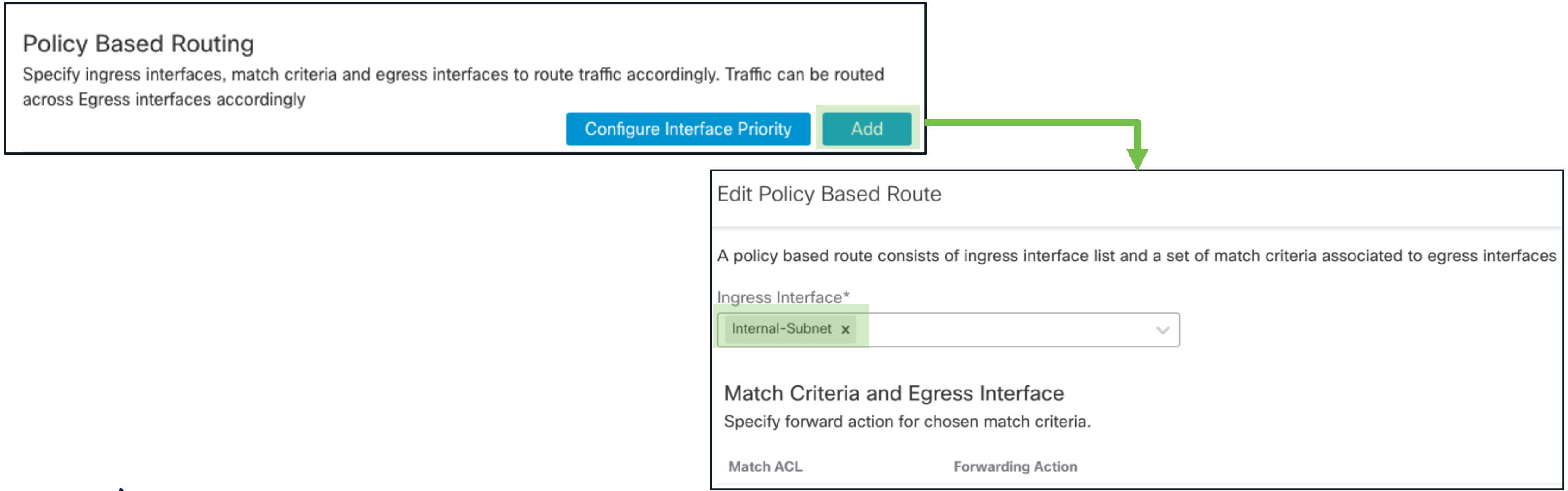
Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application
1	Allow	Any	Any	Any	Any	Facebook Instagram TikTok

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

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-Subnet

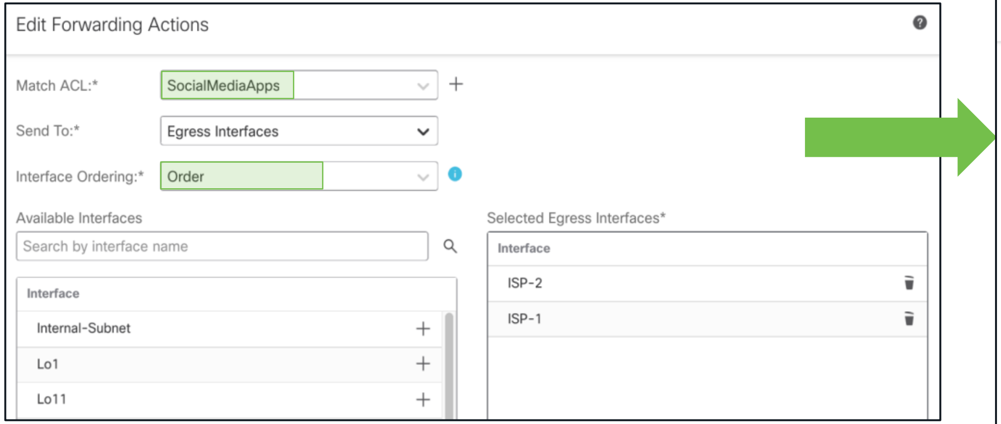
Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Configure Policy-Based Routing

Match Traffic Criteria and Egress Interfaces

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



Edit Forwarding Actions

Match ACL:* SocialMediaApps

Send To:* Egress Interfaces

Interface Ordering:* Order

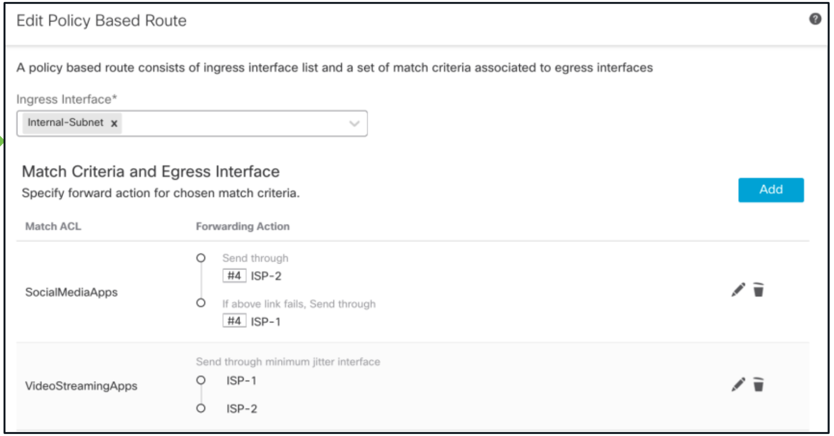
Available Interfaces

Search by interface name

Interface
Internal-Subnet
Lo1
Lo11

Selected Egress Interfaces*

Interface
ISP-2
ISP-1



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-Subnet

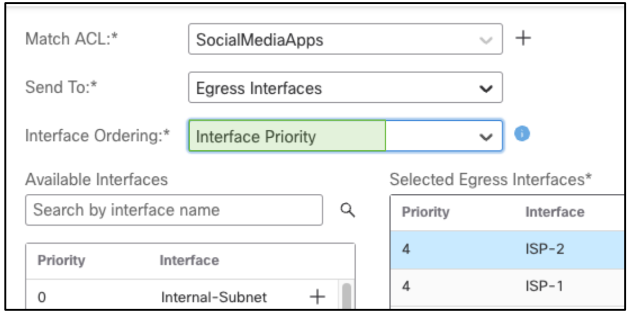
Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Match ACL	Forwarding Action
SocialMediaApps	○ Send through #4 ISP-2 ○ If above link fails, Send through #4 ISP-1
VideoStreamingApps	Send through minimum jitter interface ○ ISP-1 ○ ISP-2

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



Match ACL:* SocialMediaApps

Send To:* Egress Interfaces

Interface Ordering:* Interface Priority

Available Interfaces

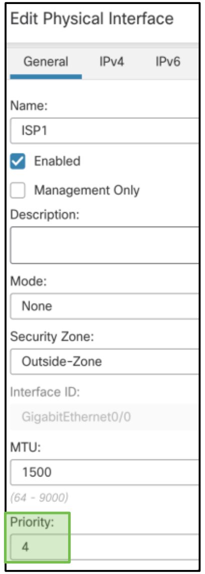
Search by interface name

Priority	Interface
0	Internal-Subnet

Selected Egress Interfaces*

Priority	Interface
4	ISP-2
4	ISP-1

1



Edit Physical Interface

Name: ISP1

☑ Enabled

□ Management Only

Description:

Mode: None

Security Zone: Outside-Zone

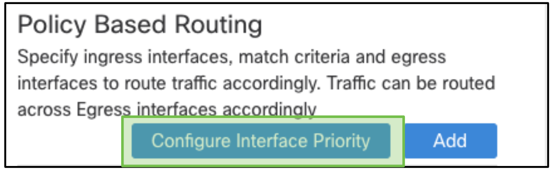
Interface ID: GigabitEthernet0/0

MTU: 1500

(64 - 9000)

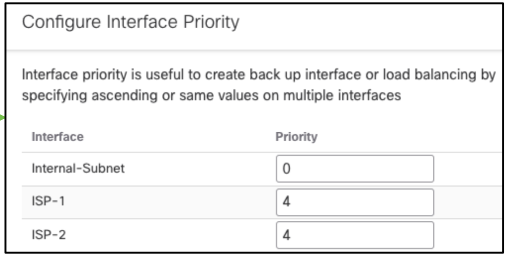
Priority: 4

2



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

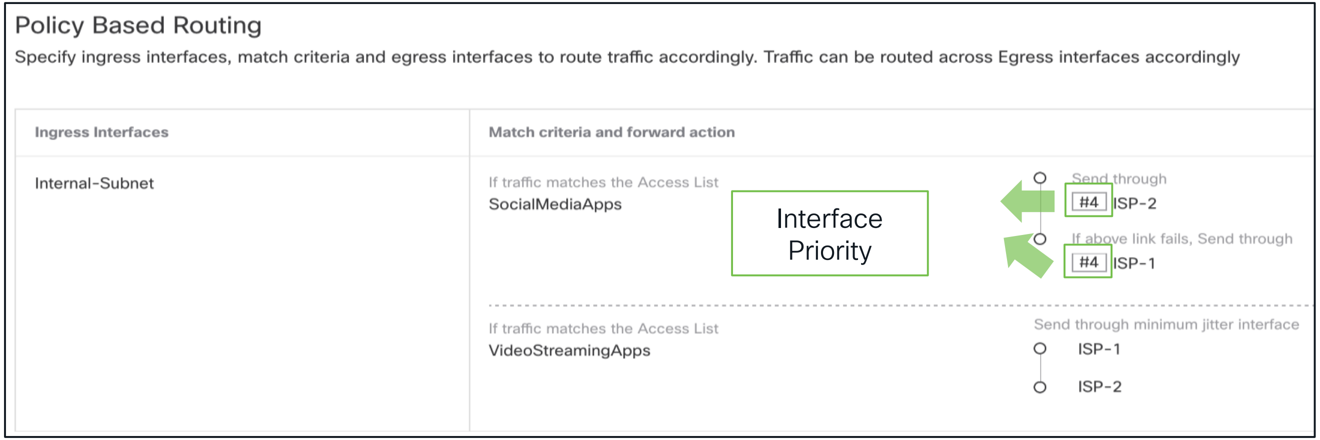
Interface priority is useful to create back up interface or load balancing by specifying ascending or same values on multiple interfaces

Interface	Priority
Internal-Subnet	0
ISP-1	4
ISP-2	4

Configure Policy-Based Routing

Match Traffic Criteria and Egress Interface

- Multiple PBR Rules configured on different set of ingress interfaces



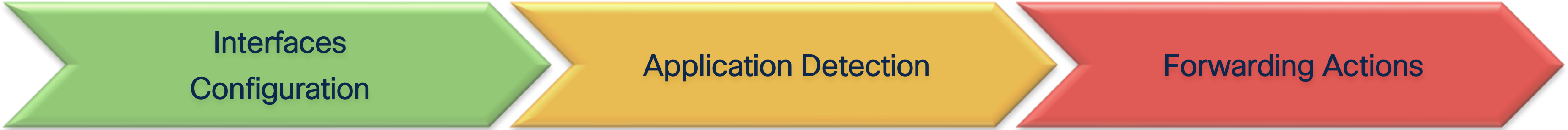
Policy Based Routing

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

Ingress Interfaces	Match criteria and forward action	
Internal-Subnet	If traffic matches the Access List SocialMediaApps	Send through #4 ISP-2 If above link fails, Send through #4 ISP-1
	If traffic matches the Access List VideoStreamingApps	Send through minimum jitter interface ISP-1 ISP-2

Interface Ordering **By Priority**

DIA Configuration Flow



Interfaces Configuration

Application Detection

Forwarding Actions

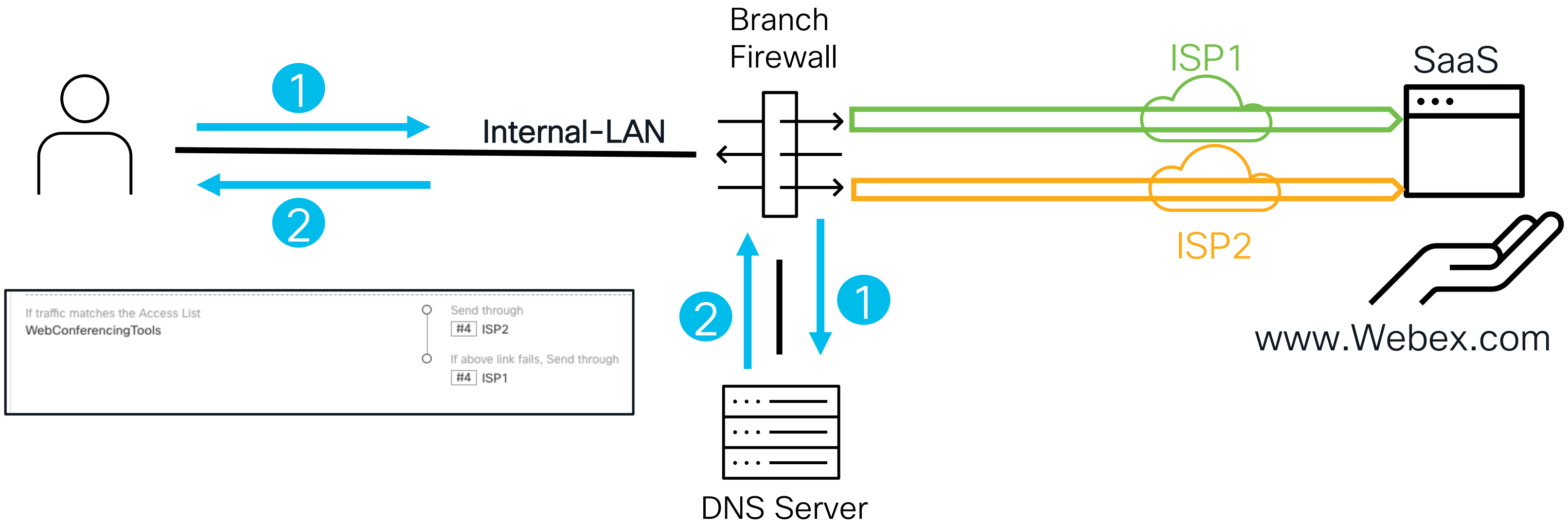
- Define Ingress and egress interfaces
  - Configure egress interfaces priorities

- VDB updated
- Trusted DNS
- Extended ACLs with Applications or users' definition

- Match ACL
- Egress Interface Selection by:
  - Order, Priority
  - RTT, Jitter, MOS and Packet Loss

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



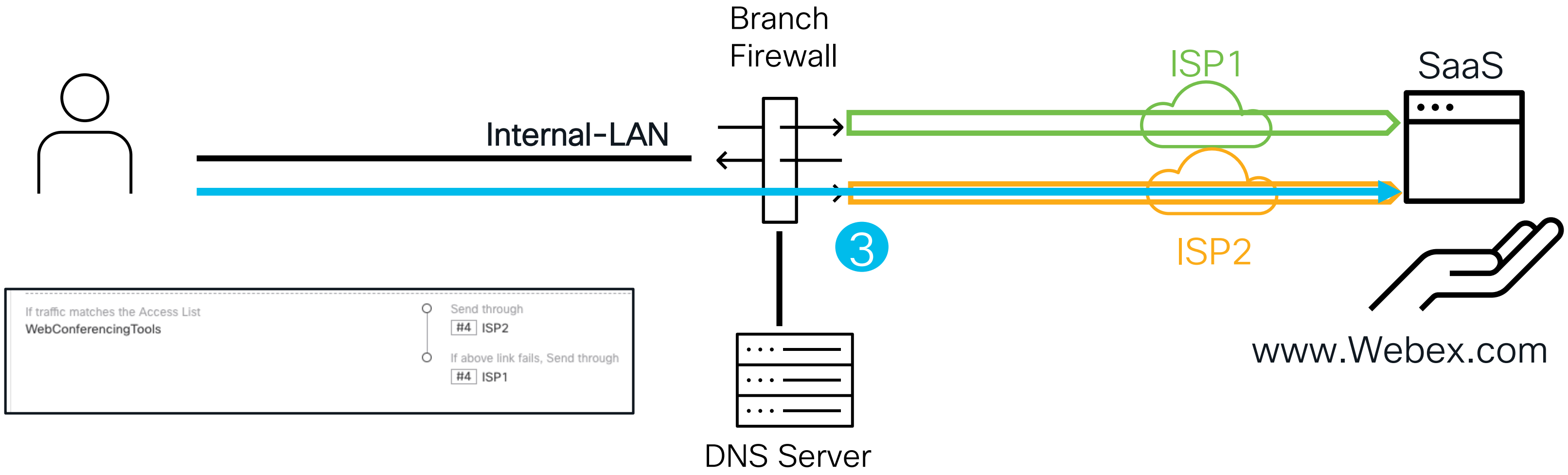
If traffic matches the Access List
WebConferencingTools

Send through
#4 ISP2

If above link fails, Send through
#4 ISP1

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



If traffic matches the Access List
WebConferencingTools

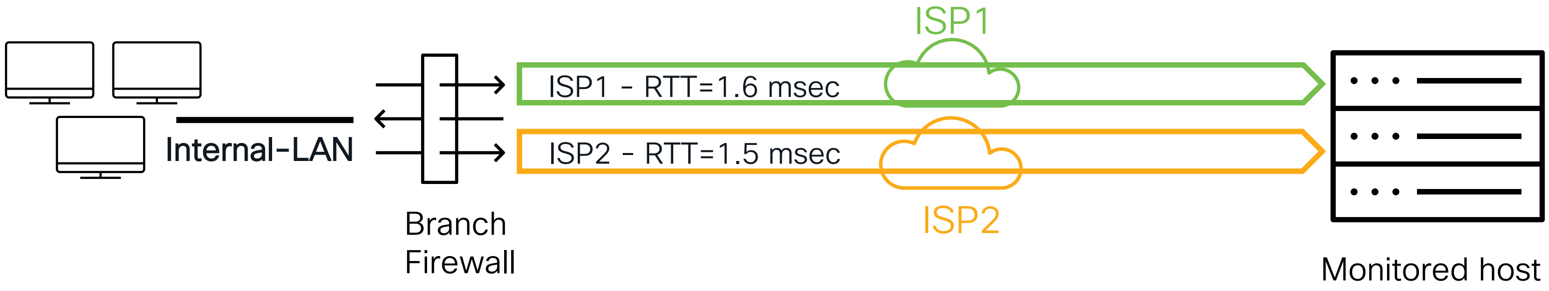
Send through
#4 ISP2

If above link fails, Send through
#4 ISP1

PBR with Path Monitoring (From FTD 7.2+)

PBR with Path Monitoring

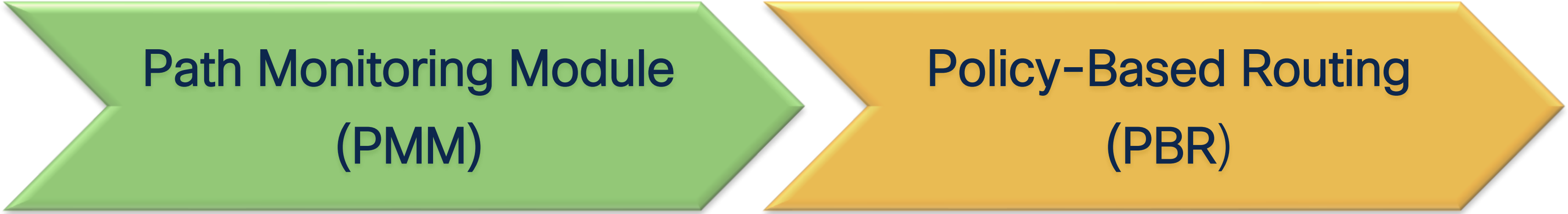
- PBR with Path Monitoring steers traffic based on dynamically monitored interface statistics such as RTT, Jitter, MOS and packet loss
  - These metrics are collected dynamically using ICMP/HTTP Probe messages



ICMP Path Monitoring

ICMP Path Monitoring

Internal FTD Components



Path Monitoring Module (PMM)

Policy-Based Routing (PBR)

Responsible for collecting the Link metrics using ICMP probes

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

ICMP Path Monitoring

Architecture Overview

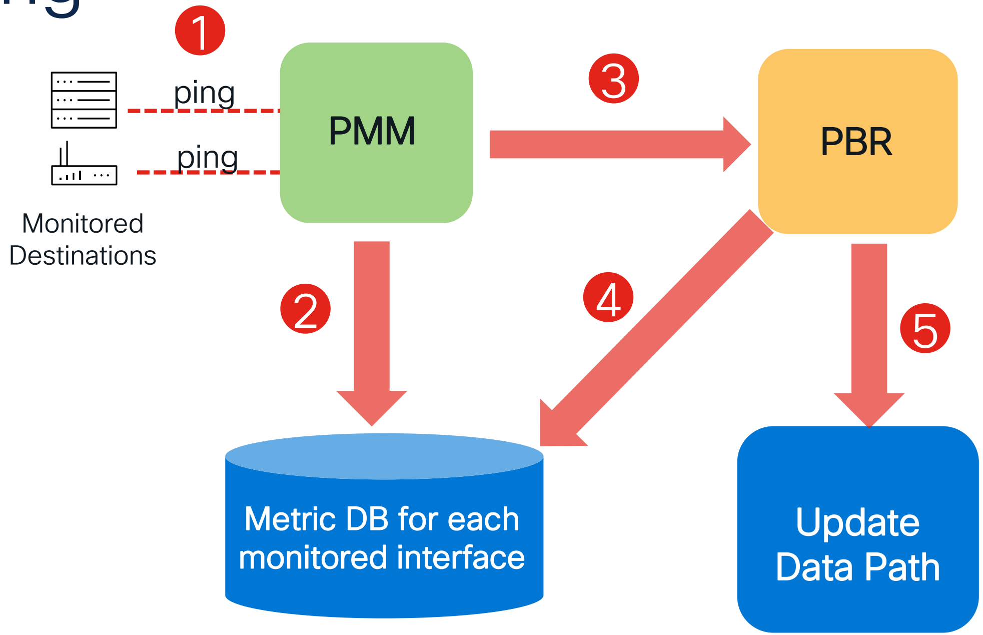
1. PMM sends ICMP probes to Monitored destinations

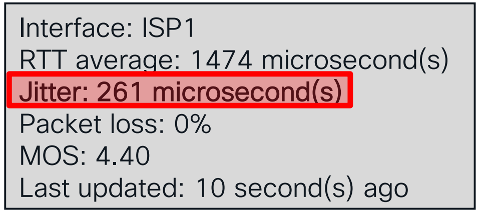
2. PMM computes and stores interface metrics

3. PMM pushes the list of interfaces that have updates to PBR

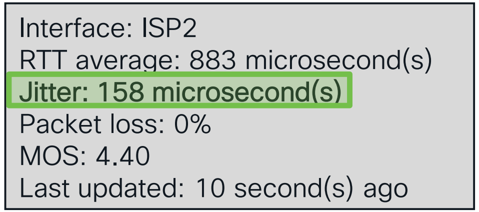
4. PBR fetches the latest available metrics from PMM internal DB

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
```

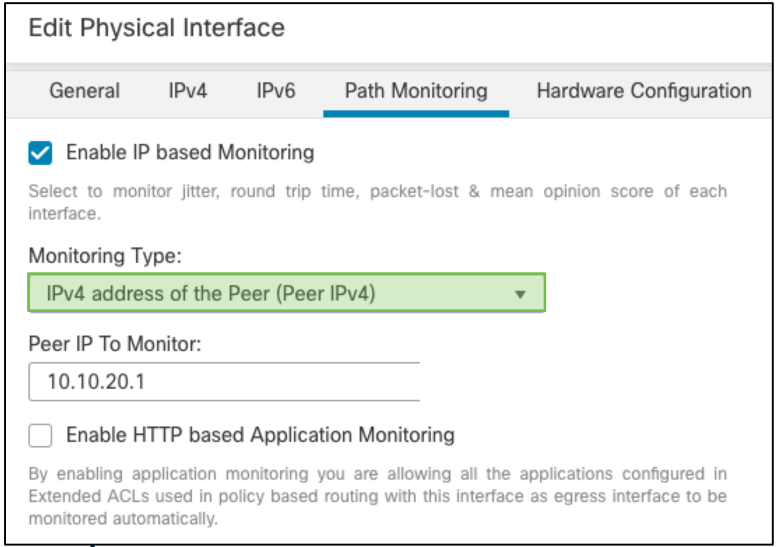


```
Interface: ISP2
RTT average: 883 microsecond(s)
Jitter: 158 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 10 second(s) ago
```

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



Edit Physical Interface

☑ Enable IP based Monitoring

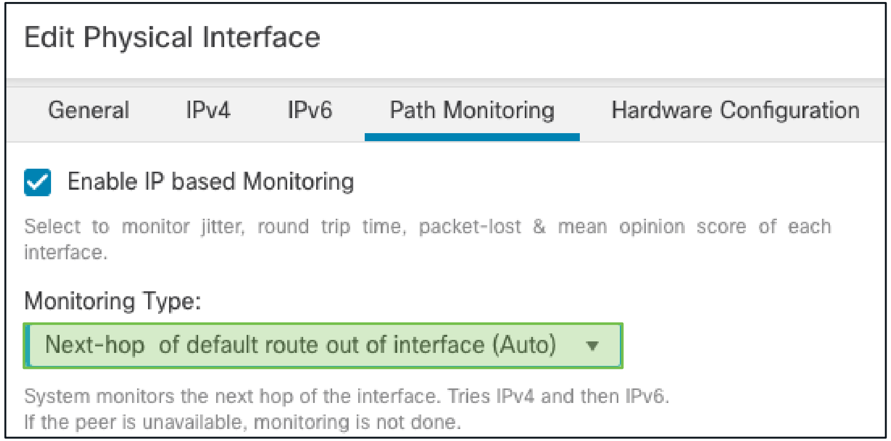
Select to monitor jitter, round trip time, packet-lost & mean opinion score of each interface.

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.



Edit Physical Interface

☑ Enable IP based Monitoring

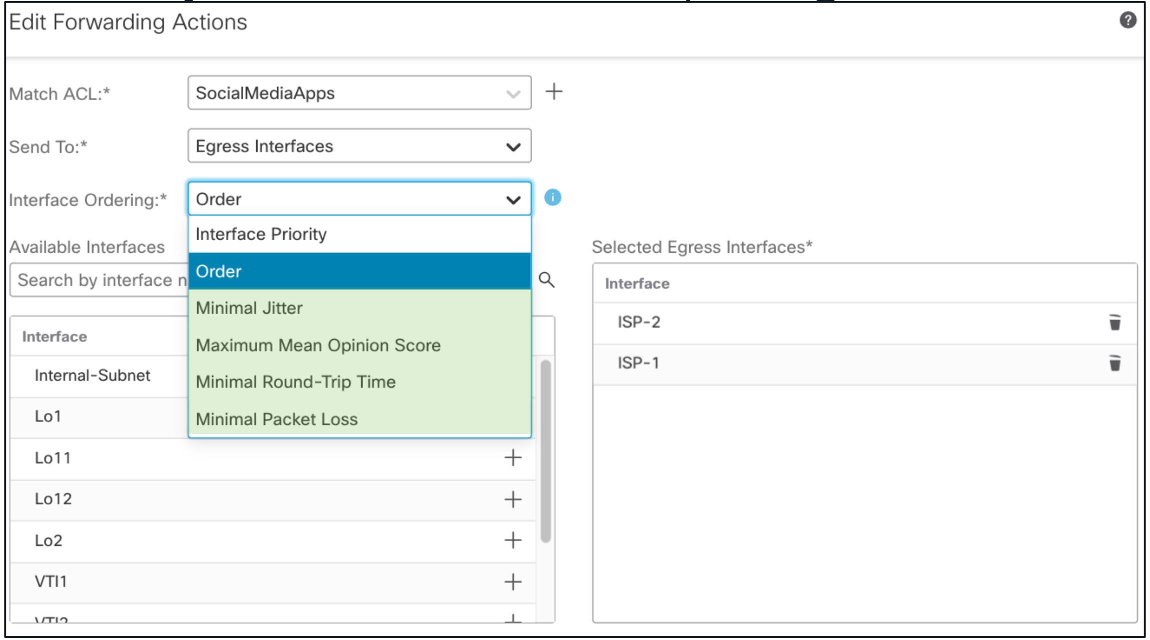
Select to monitor jitter, round trip time, packet-lost & mean opinion score of each interface.

Monitoring Type: Next-hop of default route out of interface (Auto) ▾

System monitors the next hop of the interface. Tries IPv4 and then IPv6.
If the peer is unavailable, monitoring is not done.

PBR Policy Configuration

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



Edit Forwarding Actions

Match ACL:* SocialMediaApps

Send To:* Egress Interfaces

Interface Ordering:* Order

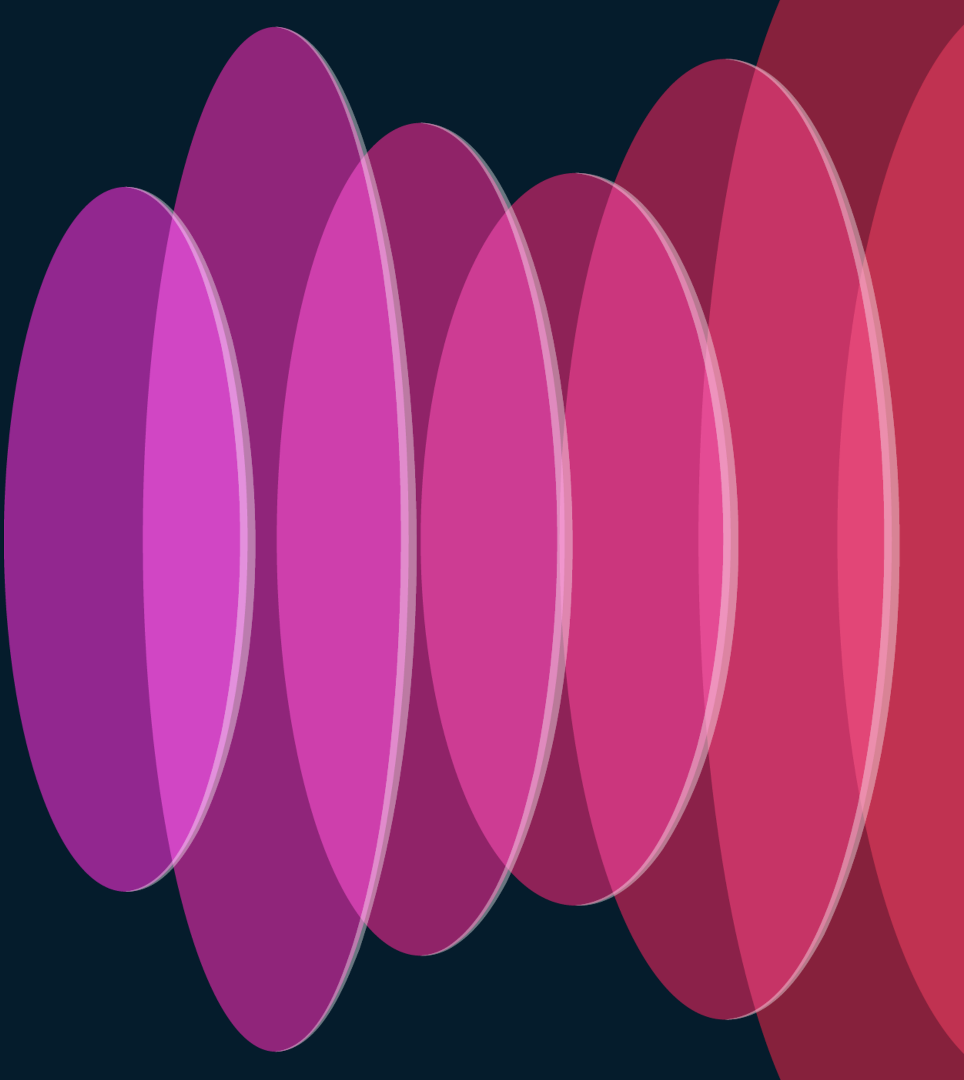
Available Interfaces

Interface
Internal-Subnet
Lo1
Lo11
Lo12
Lo2
VTI1

Selected Egress Interfaces*

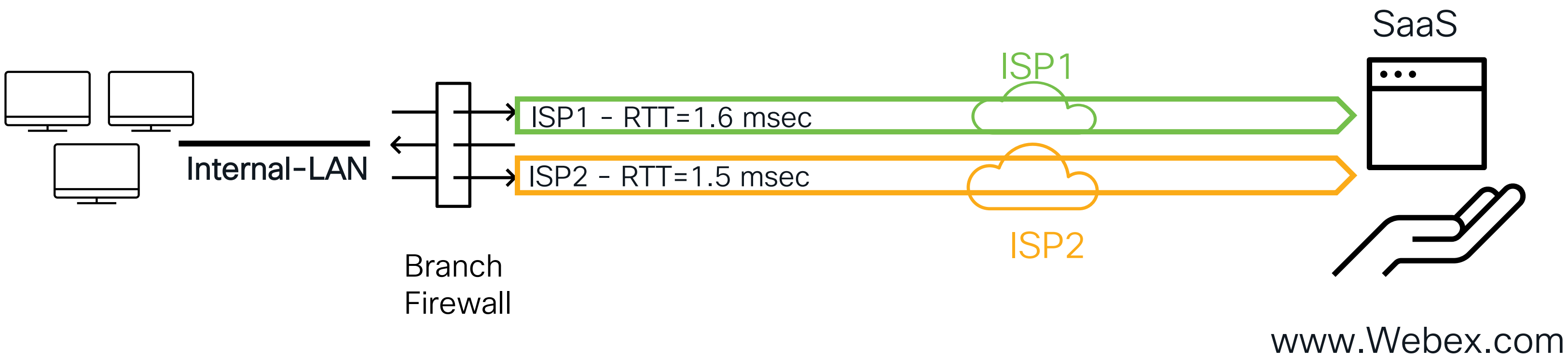
Interface
ISP-2
ISP-1

HTTP Path Monitoring (From FTD 7.4+)



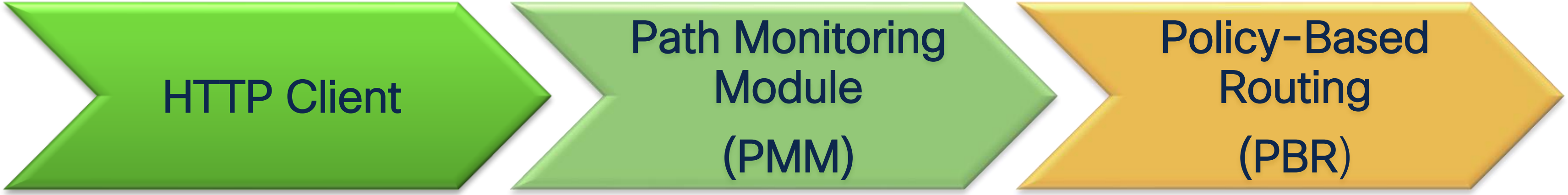
HTTP Path Monitoring

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



HTTP Path Monitoring

Internal FTD Components



HTTP Client

Path Monitoring Module (PMM)

Policy-Based Routing (PBR)

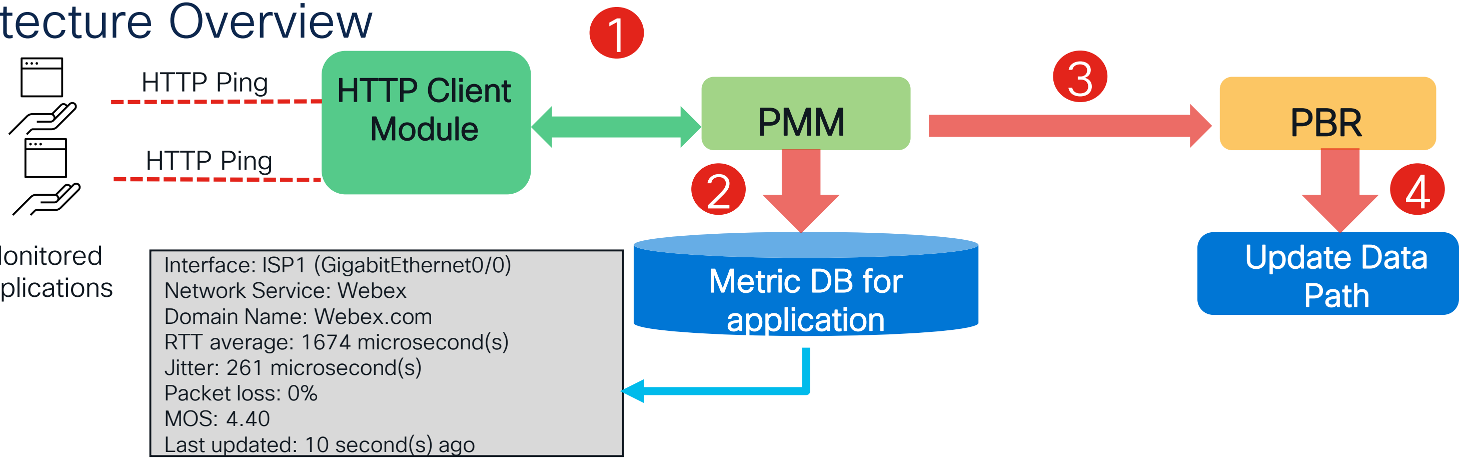
Sends HTTP Ping to the monitored domains and forwards the response back to PMM.

Responsible for computing and storing the Link metrics through ICMP or HTTP probes.

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

HTTP Path Monitoring

Architecture Overview



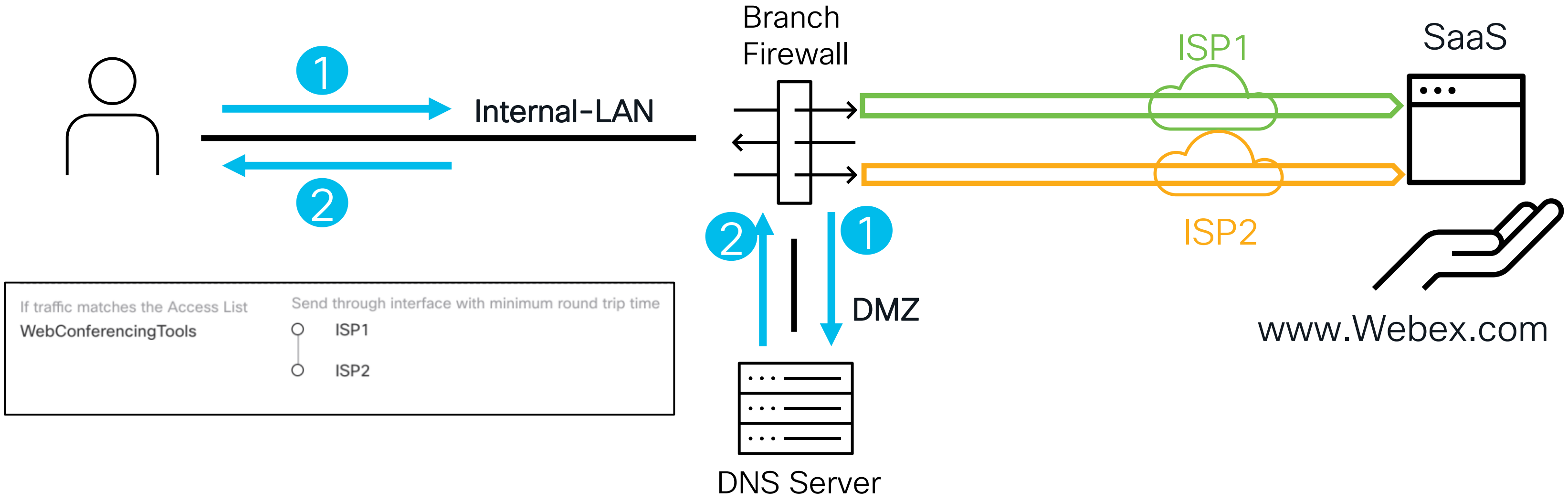
```
Interface: ISP1 (GigabitEthernet0/0)
Network Service: Webex
Domain Name: Webex.com
RTT average: 1674 microsecond(s)
Jitter: 261 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 10 second(s) ago
```

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



If traffic matches the Access List

WebConferencingTools

Send through interface with minimum round trip time

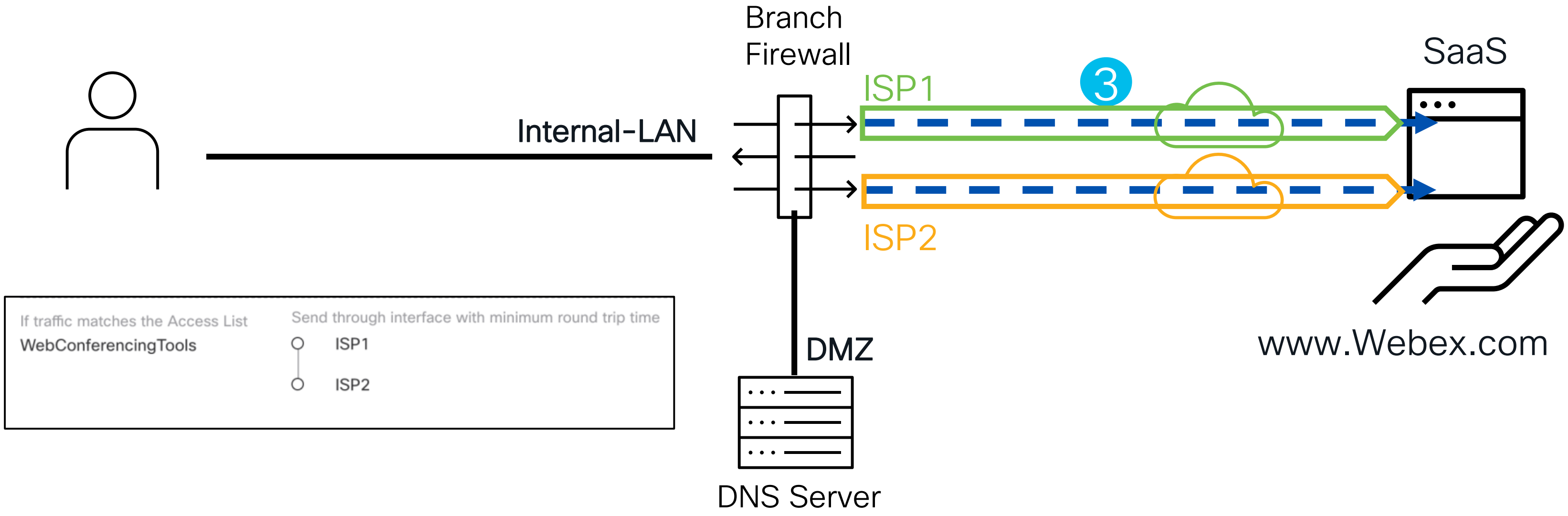
○ ISP1

○ ISP2

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

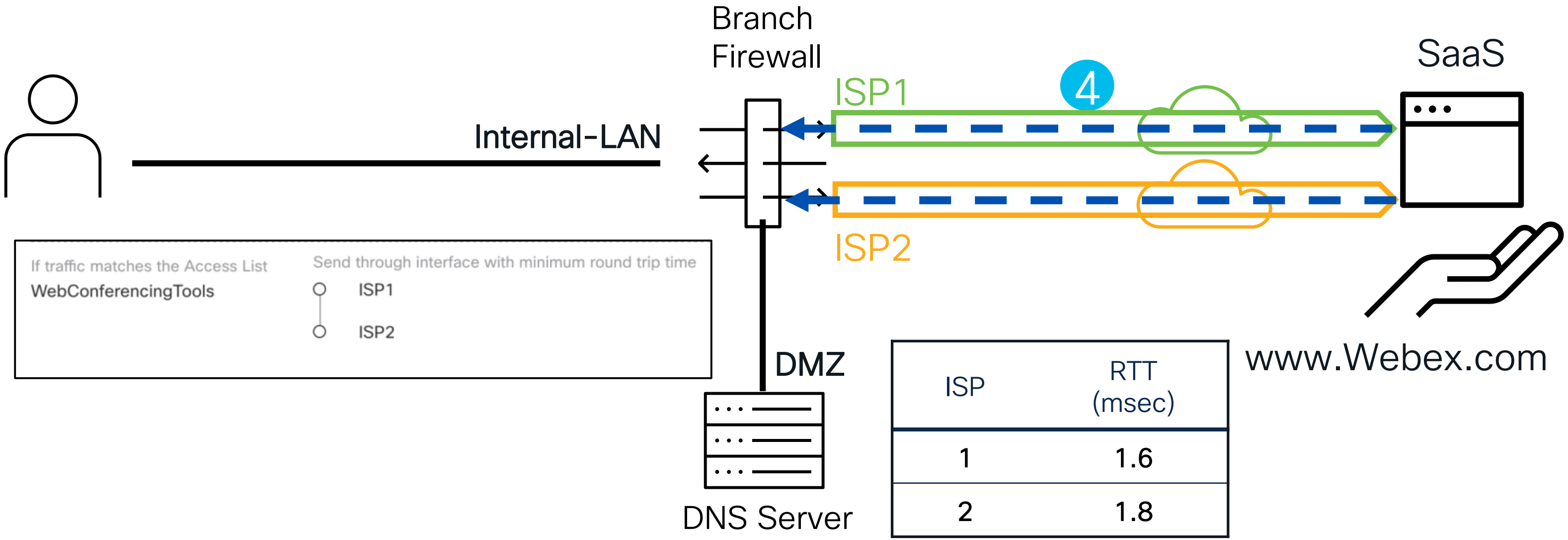


If traffic matches the Access List	Send through interface with minimum round trip time
WebConferencingTools	○ ISP1 ○ ISP2

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



If traffic matches the Access List
WebConferencingTools

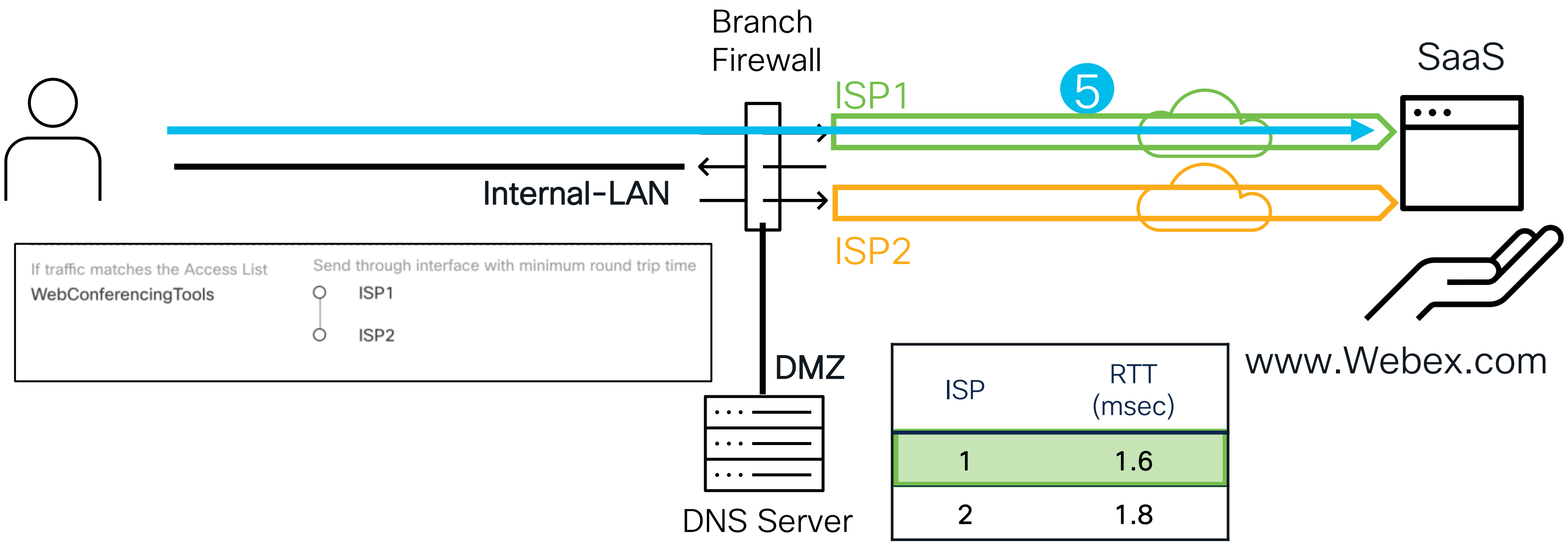
Send through interface with minimum round trip time
○ ISP1
○ ISP2

ISP	RTT (msec)
1	1.6
2	1.8

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



If traffic matches the Access List
WebConferencingTools

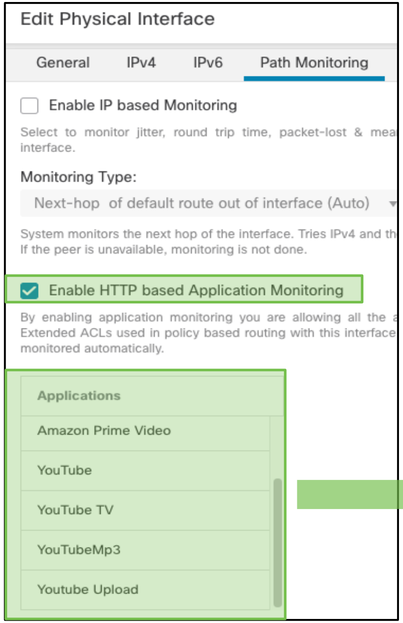
Send through interface with minimum round trip time
○ ISP1
○ ISP2

ISP	RTT (msec)
1	1.6
2	1.8

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)

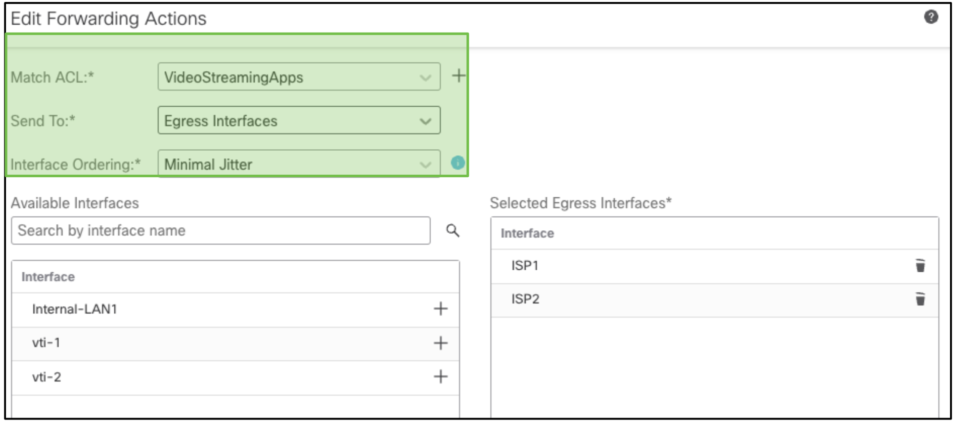
System monitors the next hop of the interface. Tries IPv4 and th
If the peer is unavailable, monitoring is not done.

☑ Enable HTTP based Application Monitoring

By enabling application monitoring you are allowing all the a 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*

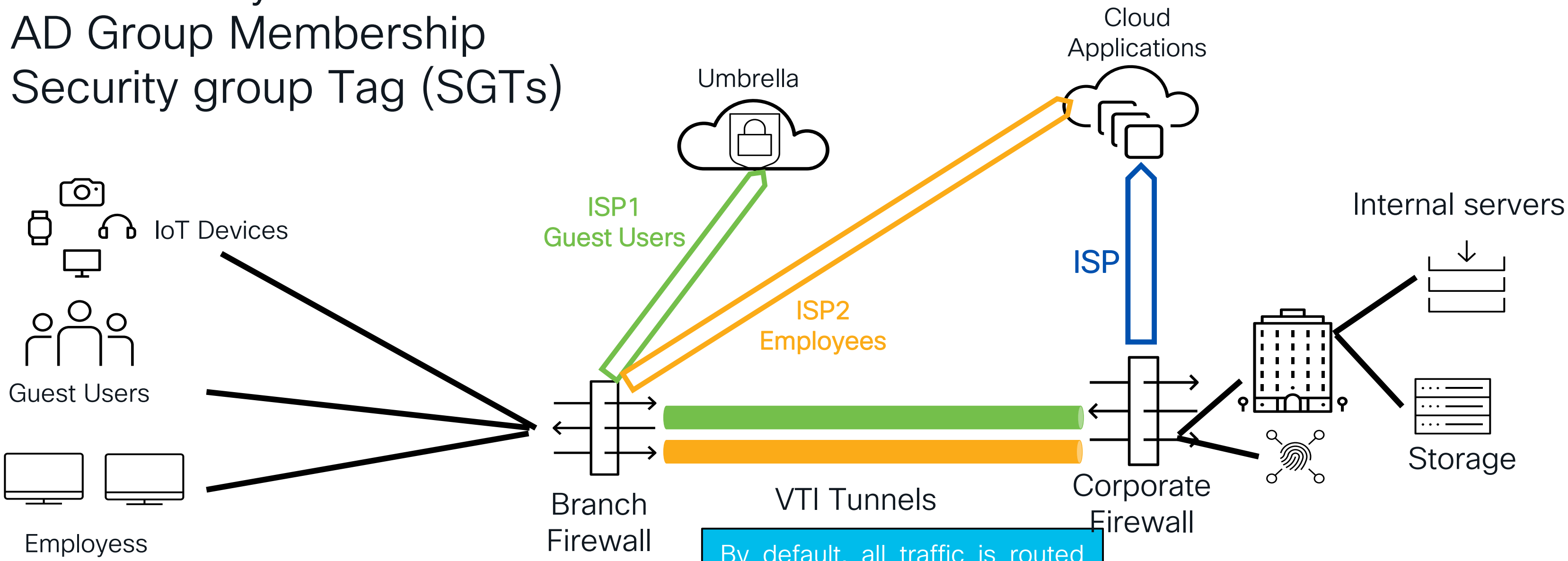
Interface
ISP1
ISP2

Identity and SGT Support (From FTD 7.4+)

PBR with User Identity and SGT

Additional attributes can be leveraged in the PBR policy:

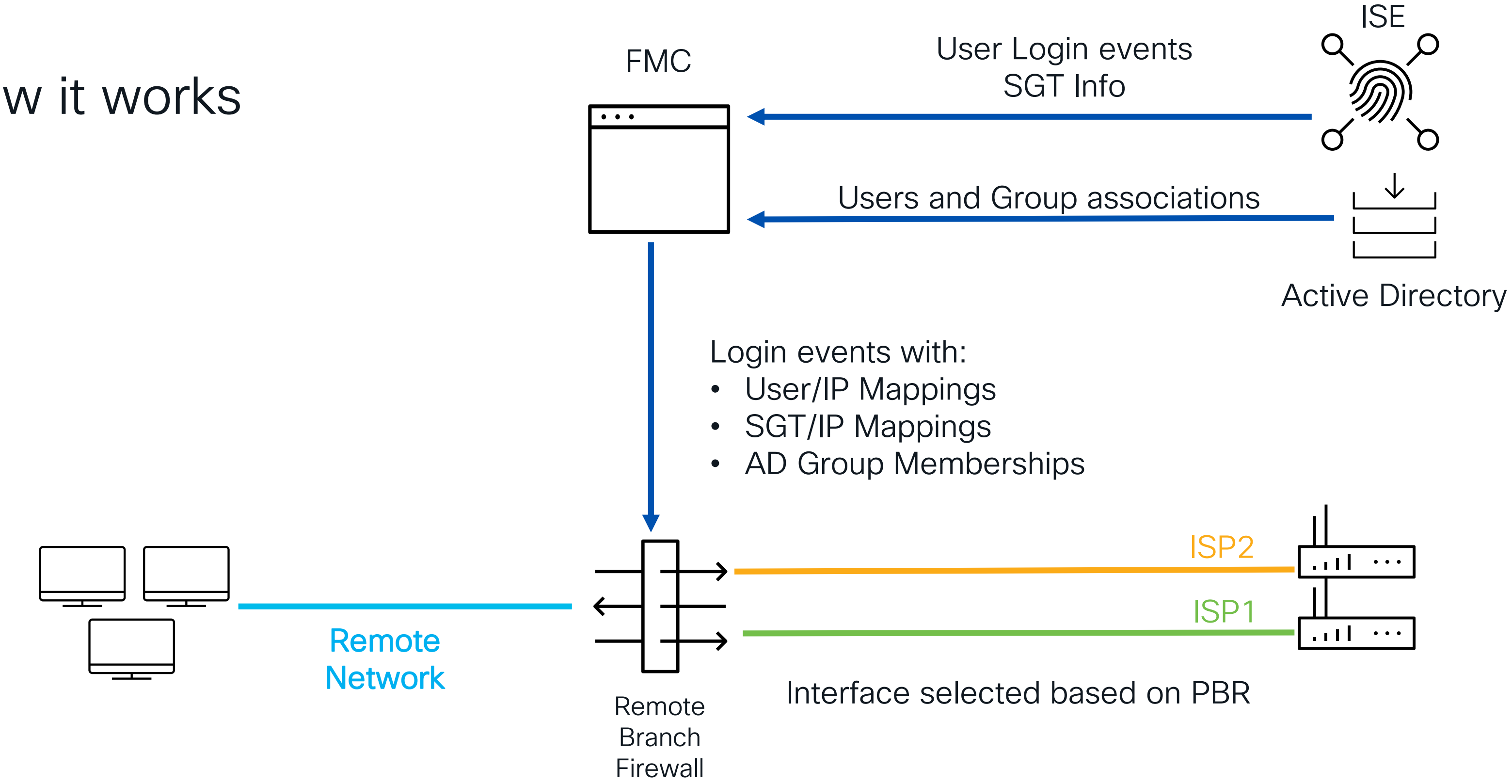
- User Identity
- AD Group Membership
- Security group Tag (SGTs)



By default, all traffic is routed to Headquarters

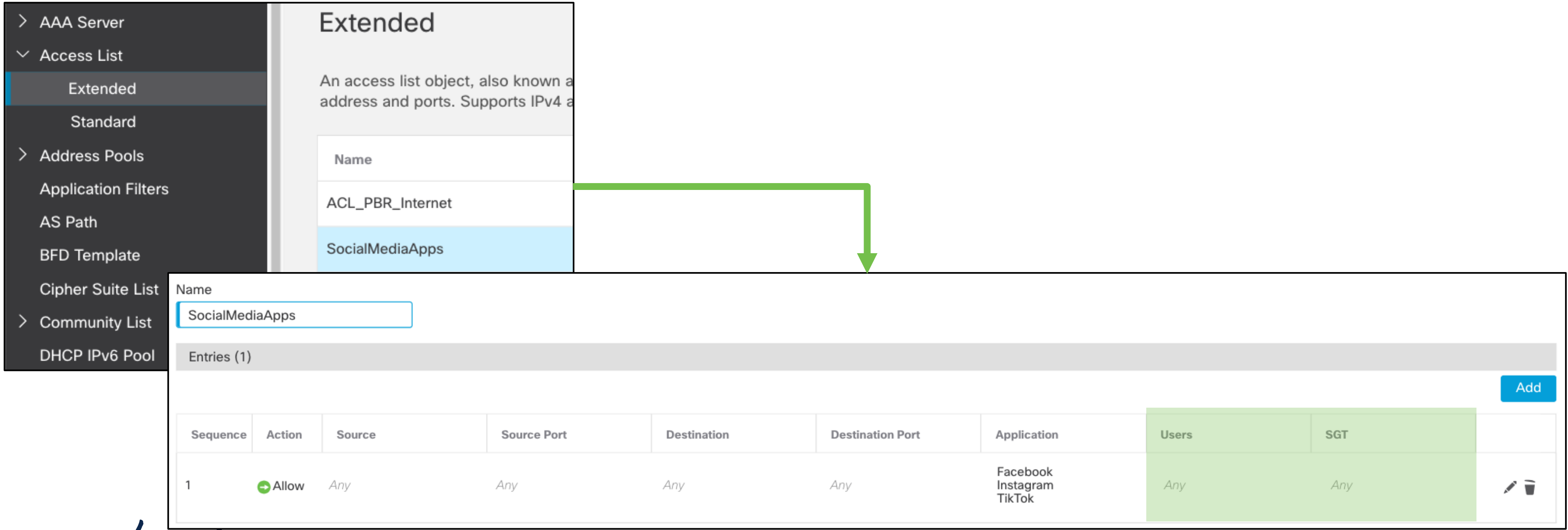
PBR with User Identity and SGT

- How it works



Configure Extended Access-list

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



Extended

An access list object, also known a
address and ports. Supports IPv4 a

Name
ACL_PBR_Internet
SocialMediaApps

Name: SocialMediaApps

Entries (1)

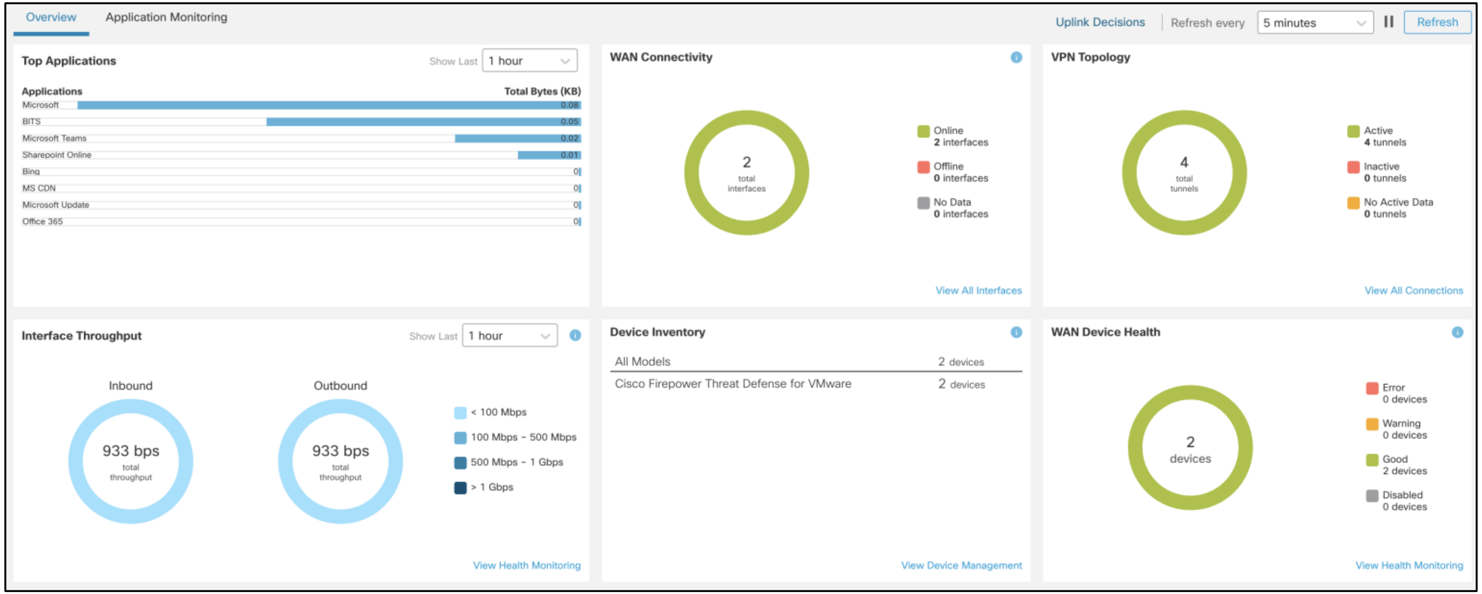
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	Any	Any	Any	Any	Facebook Instagram TikTok	Any	Any

SD-WAN Summary Dashboard (From FMC 7.4+)

SD-WAN Summary Dashboard

Overview

- It provides a holistic view of WAN devices and their associated interfaces in the deployment



Top Applications Show Last 1 hour

Applications	Total Bytes (KB)
Microsoft	0.08
BITS	0.05
Microsoft Teams	0.02
Sharepoint Online	0.01
Bing	0
MS CDN	0
Microsoft Update	0
Office 365	0

WAN Connectivity

2 total interfaces

- 🟩 Online 2 interfaces
- 🟥 Offline 0 interfaces
- ⬜ No Data 0 interfaces

View All Interfaces

VPN Topology

4 total tunnels

- 🟩 Active 4 tunnels
- 🟥 Inactive 0 tunnels
- 🟧 No Active Data 0 tunnels

View All Connections

Interface Throughput Show Last 1 hour

Inbound: 933 bps total throughput

Outbound: 933 bps total throughput

- < 100 Mbps
- 100 Mbps - 500 Mbps
- 500 Mbps - 1 Gbps
- > 1 Gbps

View Health Monitoring

Device Inventory

All Models	2 devices
Cisco Firepower Threat Defense for VMware	2 devices

View Device Management

WAN Device Health

2 devices

- 🟥 Error 0 devices
- 🟧 Warning 0 devices
- 🟩 Good 2 devices
- ⬜ Disabled 0 devices

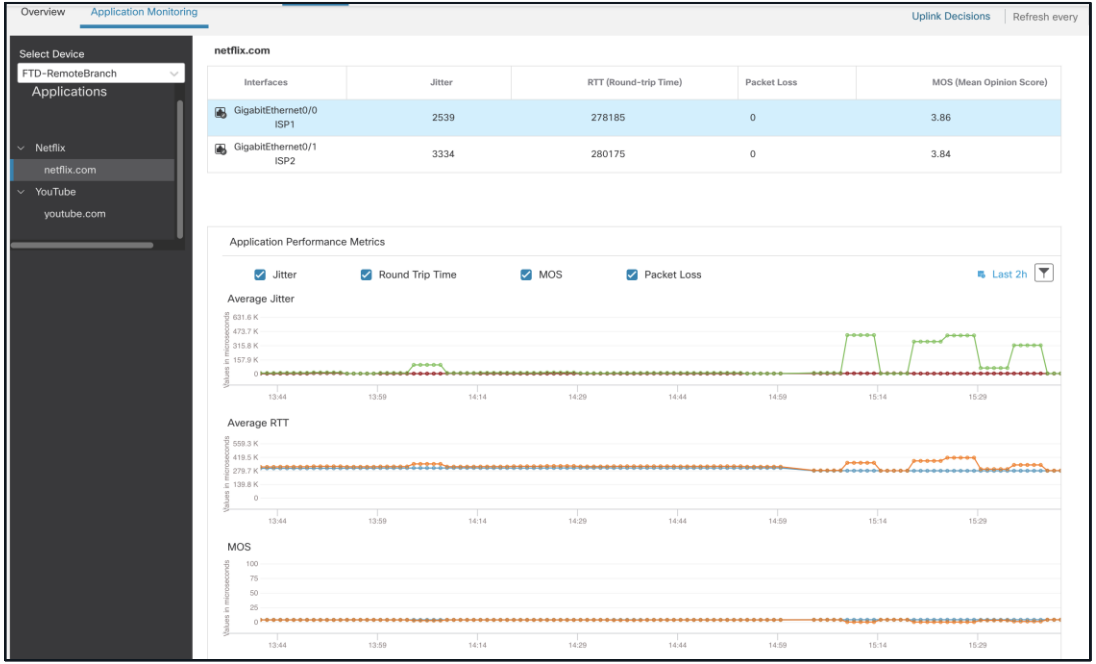
View Health Monitoring

SD-WAN Summary Dashboard

Application Monitoring

- Dashboards – SD-WAN Summary – Application Monitoring

It shows the Path Monitoring metrics per Egress interface and Domain



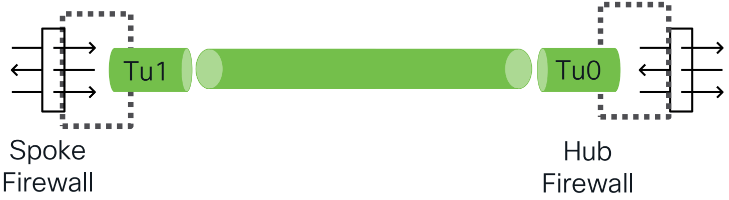
netflix.com

Interfaces	Jitter	RTT (Round-trip Time)	Packet Loss	MOS (Mean Opinion Score)
GigabitEthernet0/0 ISP1	2539	278185	0	3.86
GigabitEthernet0/1 ISP2	3334	280175	0	3.84

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

IPSec Tunnel Interface Types

Static Virtual Tunnel Interface (SVTI)

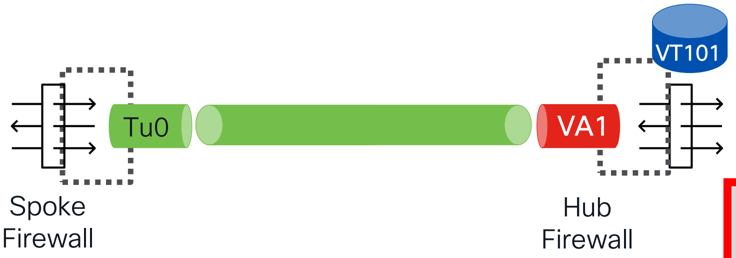


```
Interface tunnel1
 nameif VTI1
 zone-member VTI-ECMP
 ip unnumbered Lo1
 tunnel source interface ISP-1
 tunnel destination 198.18.9.20
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile
     FMC_IPSEC_PROFILE_2
```

- 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
```

```
> 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
```

- Dynamic Virtual Tunnel Interfaces are introduced in FTD 7.3
- DVTI uses a virtual template for dynamic instantiation
- VPN Sessions using DVTIs support IKEv2

Branch to Hub Communication

Dynamic Virtual Tunnel Interface (DVTI)

Features

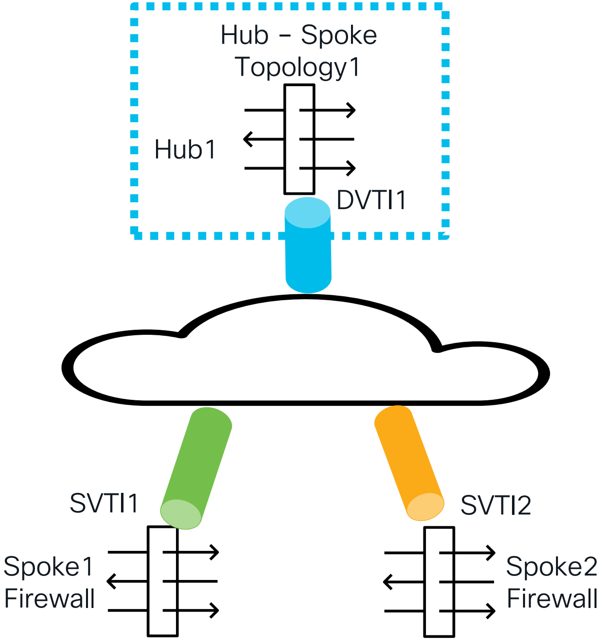
- Route-Based scalable and on-demand VPN deployment
- Enhanced spoke to hub communication
- Leveraging Virtual Template Interface – dynamic instantiation of VPN Tunnels on Hub

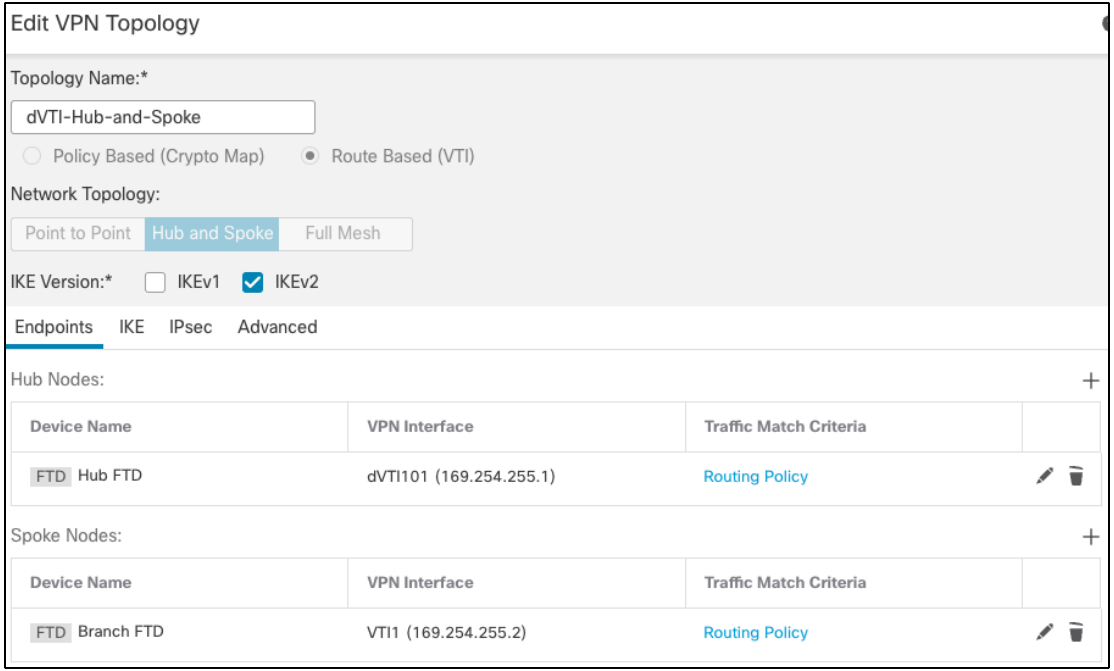
Benefits

- Simplifying tunnel management on Hub devices
- 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: Point to Point [✓ Hub and Spoke] Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

Hub Nodes:

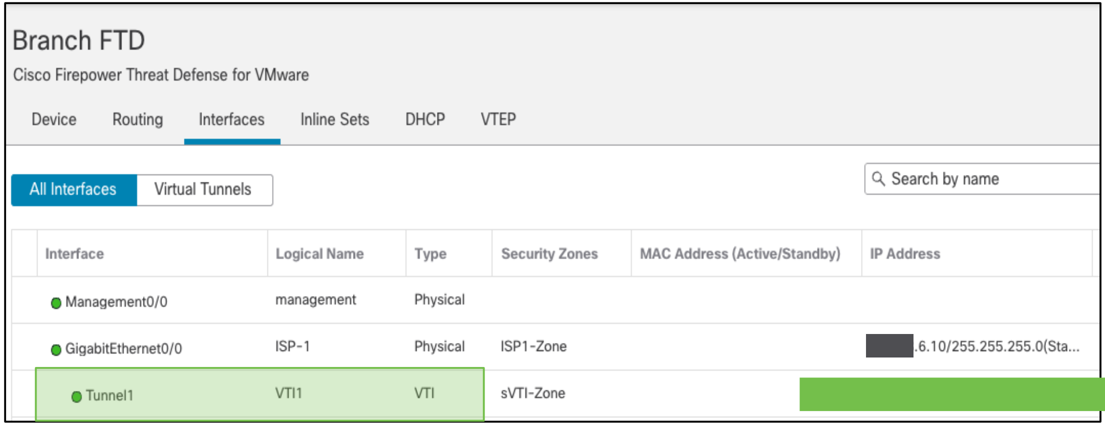
Device Name	VPN Interface	Traffic Match Criteria
FTD Hub FTD	dVTI101 (169.254.255.1)	Routing Policy

Spoke Nodes:

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

Single Hub Topology

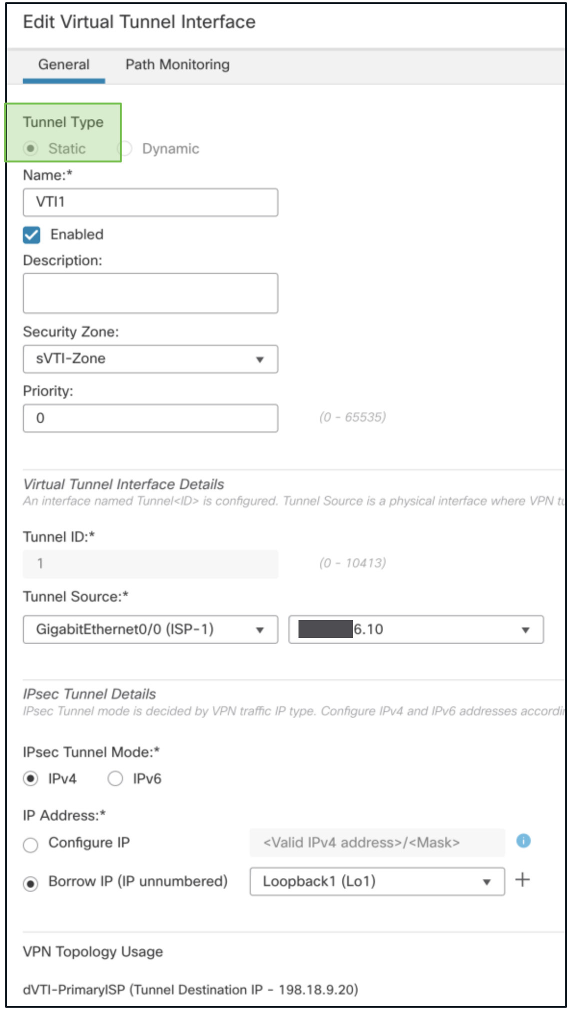
Spoke Interface Configuration



Branch FTD

Cisco Firepower Threat Defense for VMware

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
● Management0/0	management	Physical			
● GigabitEthernet0/0	ISP-1	Physical	ISP1-Zone		[redacted].6.10/255.255.255.0(Sta...
● Tunnel1	VTI1	VTI	sVTI-Zone		



Edit Virtual Tunnel Interface

Tunnel Type

● Static ○ Dynamic

Name:* VTI1

☑ Enabled

Description:

Security Zone: sVTI-Zone

Priority: 0 (0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tu

Tunnel ID:* 1 (0 - 10413)

Tunnel Source:* GigabitEthernet0/0 (ISP-1) [redacted]6.10

IPsec Tunnel Details

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

IPsec Tunnel Mode:*

● IPv4 ○ IPv6

IP Address:*

○ Configure IP <Valid IPv4 address>/<Mask>

● Borrow IP (IP unnumbered) Loopback1 (Lo1)

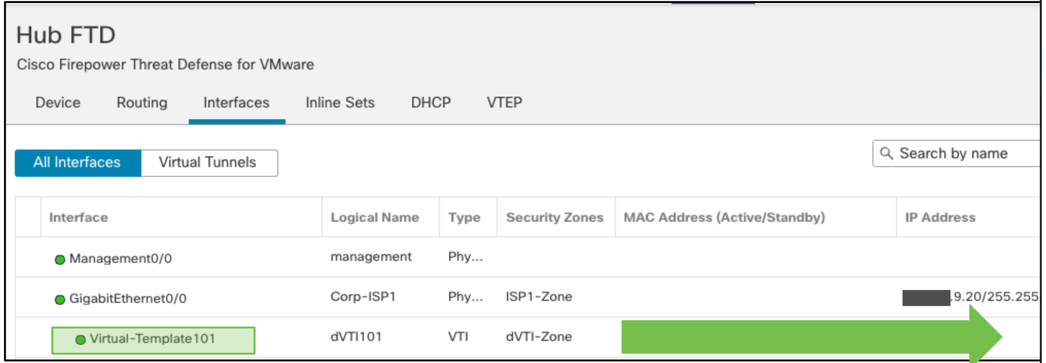
VPN Topology Usage

dVTI-PrimaryISP (Tunnel Destination IP - 198.18.9.20)

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

Single Hub Topology

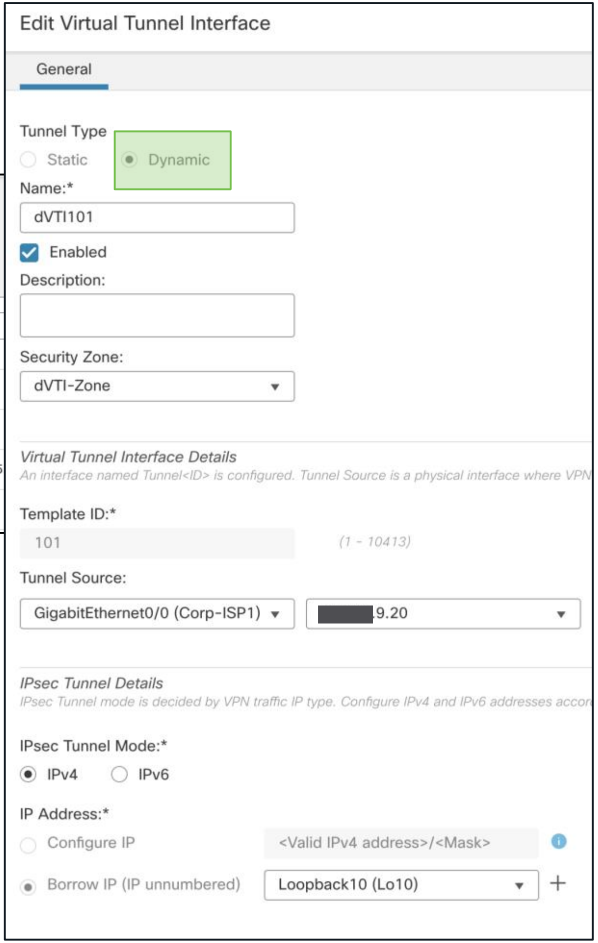
Hub Interface Configuration



Hub FTD

Cisco Firepower Threat Defense for VMware

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Management0/0	management	Phy...			
GigabitEthernet0/0	Corp-ISP1	Phy...	ISP1-Zone		[redacted]9.20/255.255
Virtual-Template101	dVTI101	VTI	dVTI-Zone		



Edit Virtual Tunnel Interface

Tunnel Type
○ Static ● Dynamic

Name:* dVTI101

☑ Enabled

Description:

Security Zone: dVTI-Zone

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN

Template ID:* 101 *(1 - 10413)*

Tunnel Source: GigabitEthernet0/0 (Corp-ISP1) [redacted]9.20

IPsec Tunnel Details

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

IPsec Tunnel Mode:*
● IPv4 ○ IPv6

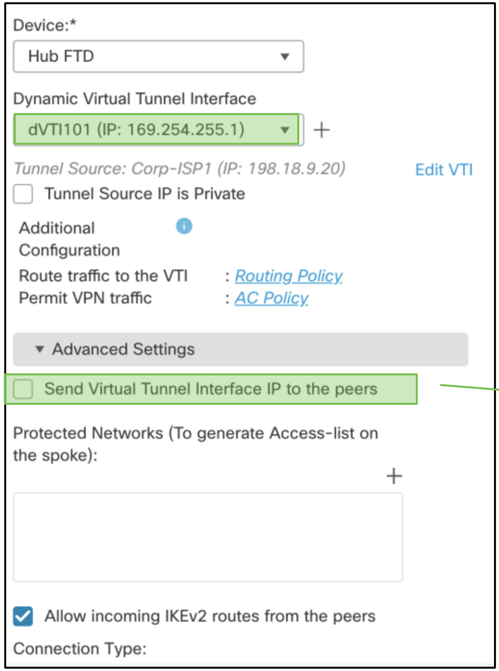
IP Address:*
○ Configure IP <Valid IPv4 address>/<Mask>
● Borrow IP (IP unnumbered) Loopback10 (Lo10)

- DVTI is configured in the Hub
- Virtual Template interface must "borrow" loopback address (recommended)
- Virtual Template interface is used to create ephemeral VTI interfaces as spokes connect

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):

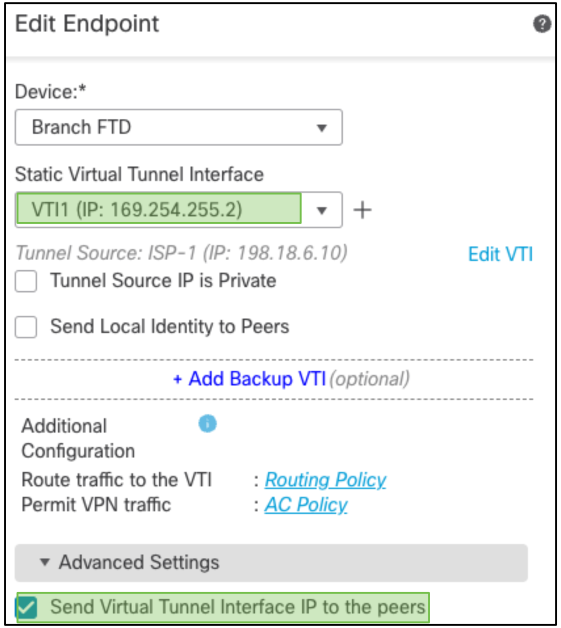
+

☑ 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

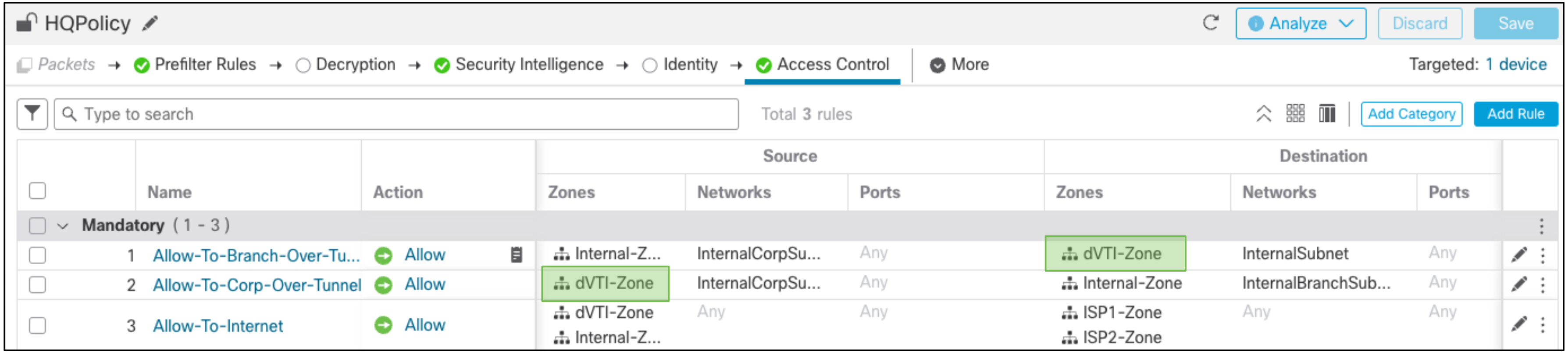
Permit VPN traffic : AC Policy

▾ Advanced Settings

☑ Send Virtual Tunnel Interface IP to the peers

Single Hub Topology

Firewall Policy Configuration



		Source			Destination		
Name	Action	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 Internal-Z...	Any	Any	ISP1-Zone ISP2-Zone	Any	Any

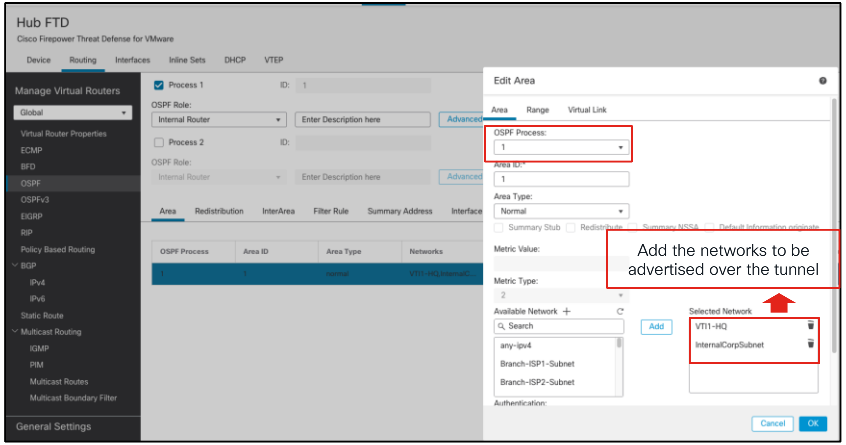
- Assign a zone to the tunnel interfaces
- Use the same zone for tunnels to allow for asymmetric flows
- Use this zone in the Access Control Policy like any other interface zone for traffic control and inspection

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 networks must be configured, and Reverse Route Injection must be enabled

OSPF Routing Configuration



Hub FTD
Cisco Firepower Threat Defense for VMware

Global

☑ Process 1 ID: 1
OSPF Role: Internal Router
Enter Description here

☐ Process 2 ID:
OSPF Role: Internal Router
Enter Description here

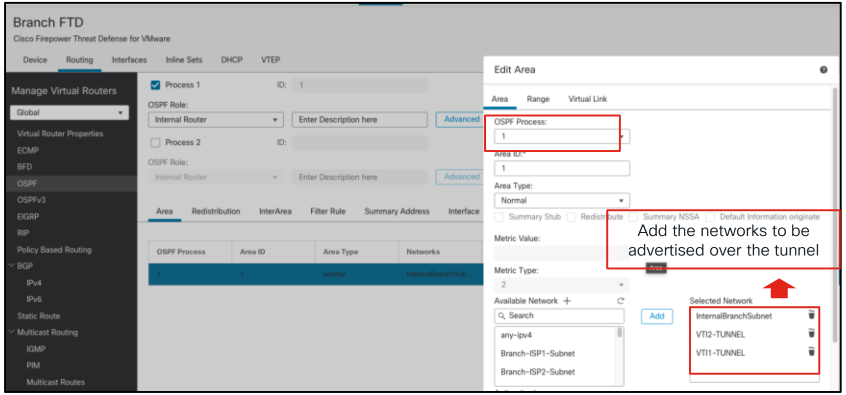
OSPF Process	Area ID	Area Type	Networks
1	1	normal	VTI1-HQ,InternalC...

Edit Area

OSPF Process: 1
Area ID:* 1
Area Type: Normal
☐ Summary Stub ☐ Redistribute ☐ Summary NSSA ☐ Default Information originate
Metric Value:
Metric Type: 2
Available Network: any-ipv4, Branch-ISP1-Subnet, Branch-ISP2-Subnet
Selected Network: VTI1-HQ, InternalCorpSubnet
Authentication:

Add the networks to be advertised over the tunnel

Hub FTD



Branch FTD
Cisco Firepower Threat Defense for VMware

Global

☑ Process 1 ID: 1
OSPF Role: Internal Router
Enter Description here

☐ Process 2 ID:
OSPF Role: Internal Router
Enter Description here

OSPF Process	Area ID	Area Type	Networks
1	1	normal	InternalBranchSub...

Edit Area

OSPF Process: 1
Area ID:* 1
Area Type: Normal
☐ Summary Stub ☐ Redistribute ☐ Summary NSSA ☐ Default Information originate
Metric Value:
Metric Type: 2
Available Network: any-ipv4, Branch-ISP1-Subnet, Branch-ISP2-Subnet
Selected Network: InternalBranchSubnet, VTI2-TUNNEL, VTI1-TUNNEL

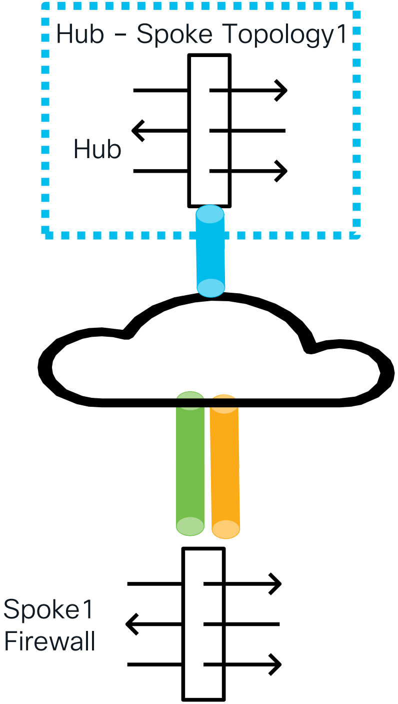
Add the networks to be advertised over the tunnel

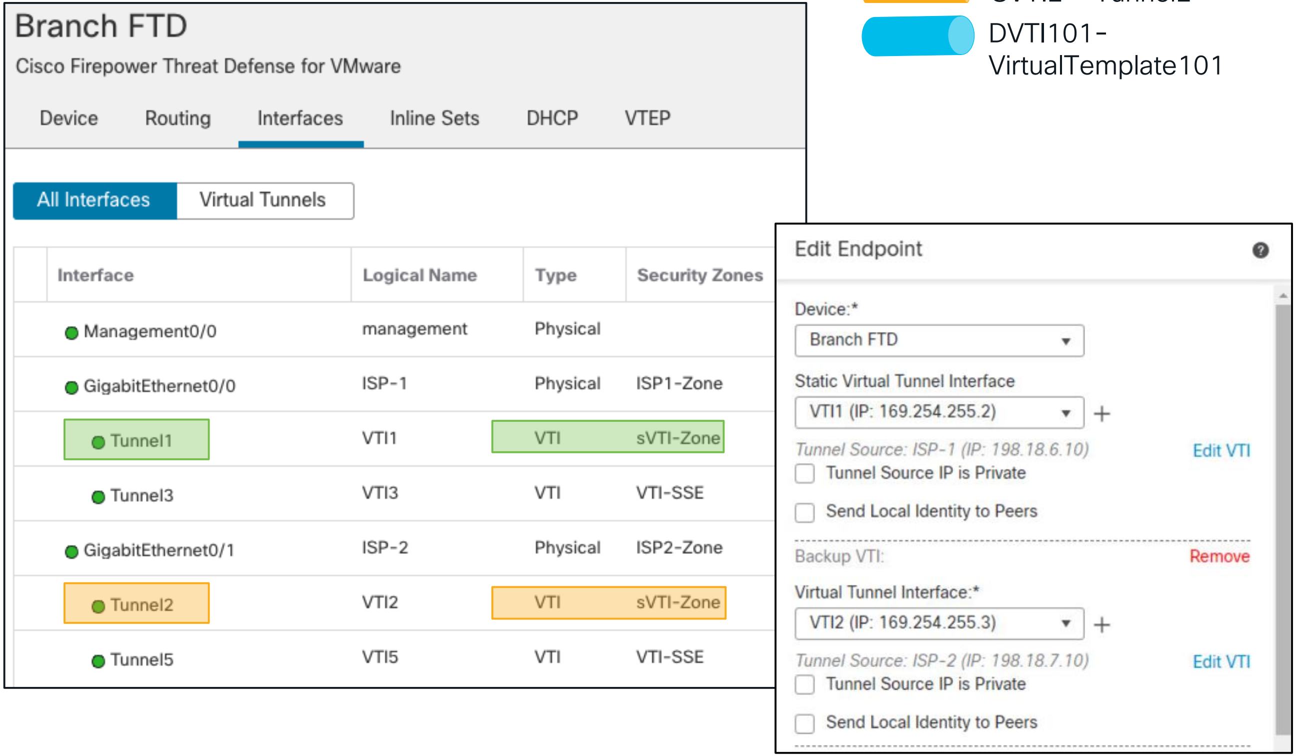
Spoke FTD

Single Hub Topology

Spoke with Dual WAN

🟩 SVTI1 – Tunnel1
🟧 SVTI2 – Tunnel2
🟦 DVTI101- VirtualTemplate101





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

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

Backup VTI: Remove

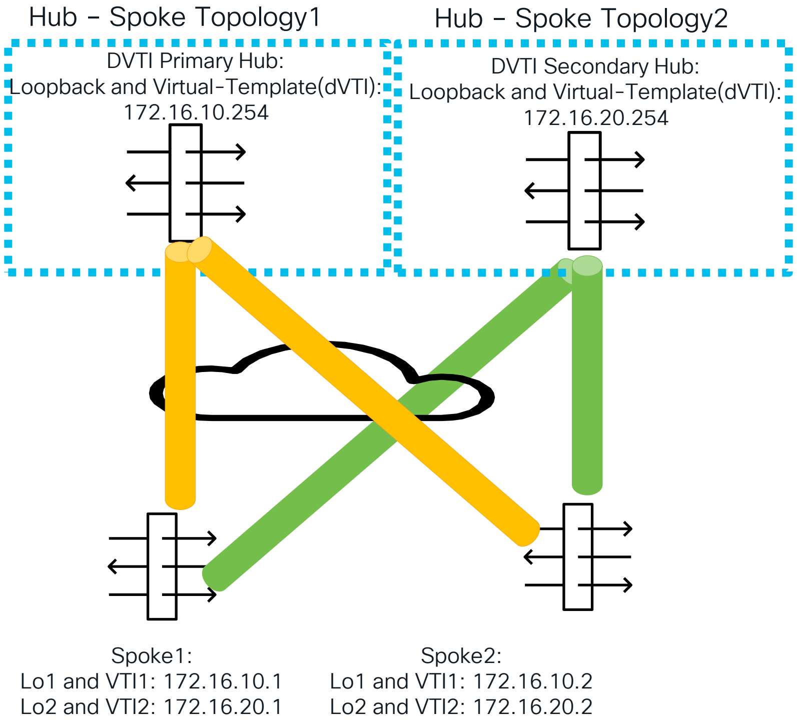
Virtual Tunnel Interface:* VTI2 (IP: 169.254.255.3) +

Tunnel Source: ISP-2 (IP: 198.18.7.10) Edit VTI

□ Tunnel Source IP is Private

□ Send Local Identity to Peers

Dual Hub Topology

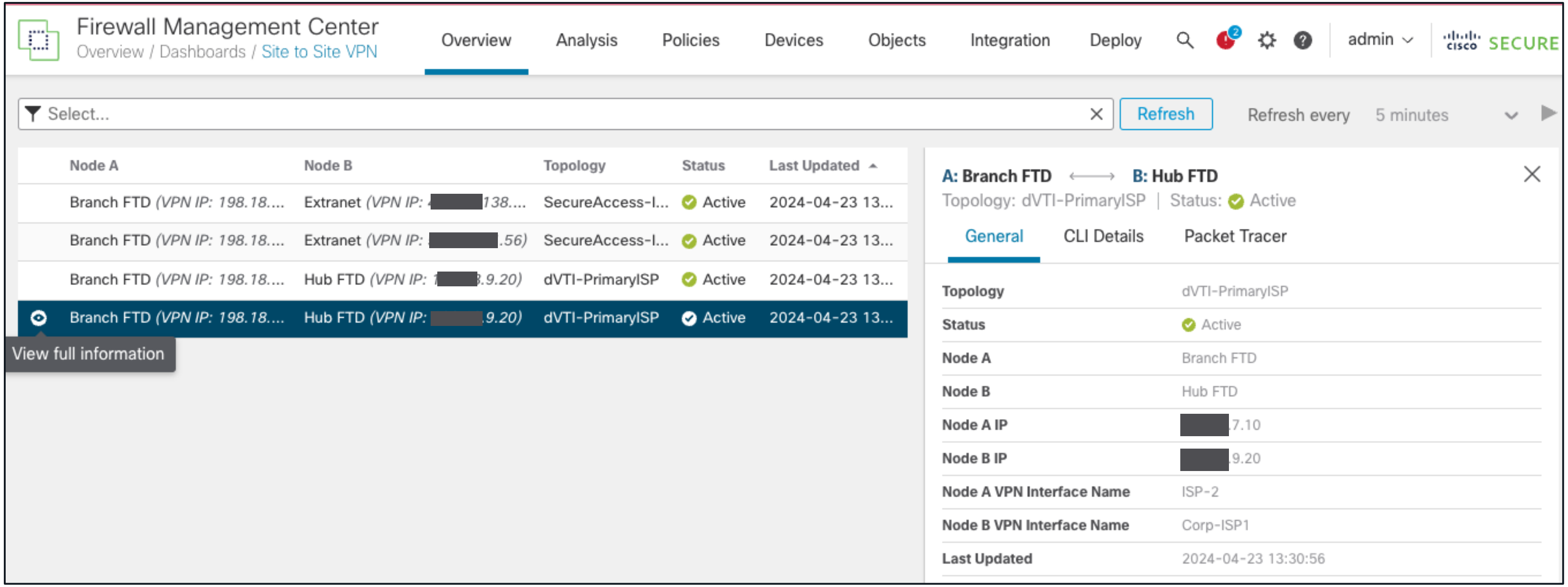


Hub – Spoke Topology1
Hub – Spoke Topology2
DVTI Primary Hub:
Loopback and Virtual-Template(dVTI):
172.16.10.254
DVTI Secondary Hub:
Loopback and Virtual-Template(dVTI):
172.16.20.254
Spoke1:
Lo1 and VTI1: 172.16.10.1
Lo2 and VTI2: 172.16.20.1
Spoke2:
Lo1 and VTI1: 172.16.10.2
Lo2 and VTI2: 172.16.20.2

- 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

Node A	Node B	Topology	Status	Last Updated
Branch FTD *(VPN IP: 198.18....*	Extranet *(VPN IP: [redacted]138....*	SecureAccess-l...	✓ Active	2024-04-23 13...
Branch FTD *(VPN IP: 198.18....*	Extranet *(VPN IP: [redacted].56)*	SecureAccess-l...	✓ 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

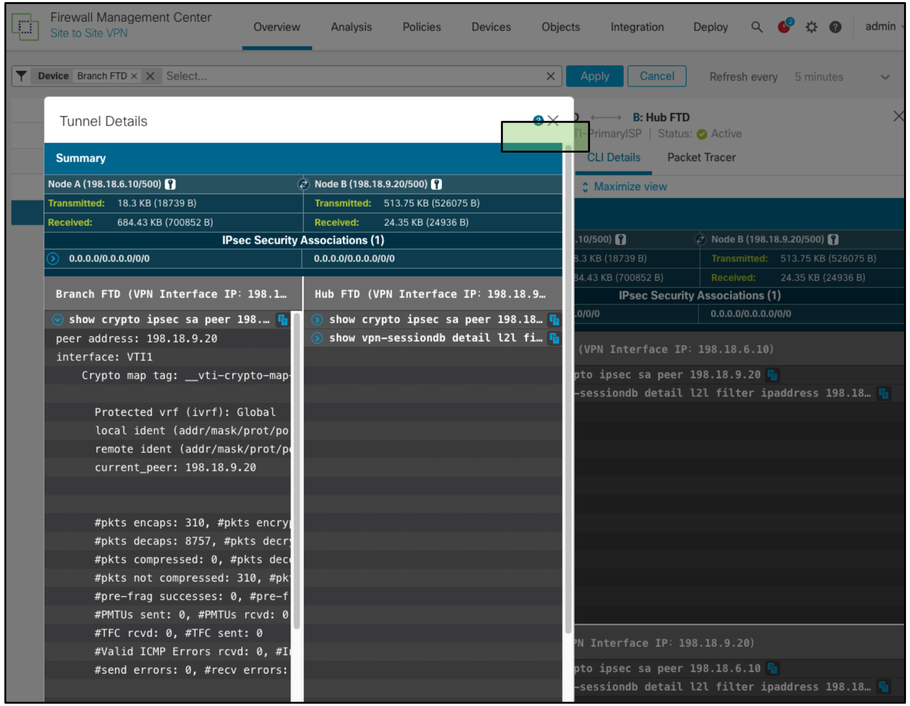
Topology	dVTI-PrimaryISP
Status	✓ Active
Node A	Branch FTD
Node B	Hub FTD
Node A IP	[redacted]7.10
Node B IP	[redacted]9.20
Node A VPN Interface Name	ISP-2
Node B VPN Interface Name	Corp-ISP1
Last Updated	2024-04-23 13:30:56

Site to Site VPN Dashboard

CLI Details

Displays the CLI outputs for the the following commands

```
Show crypto ipsec sa peer <ip_address>
show vpn-sessiondb l2l filter ipaddress <ip_address>
```



Node A (198.18.6.10/500)		Node B (198.18.9.20/500)	
Transmitted:	18.3 KB (18739 B)	Transmitted:	513.75 KB (526075 B)
Received:	684.43 KB (700852 B)	Received:	24.35 KB (24936 B)

IPsec Security Associations (1)

0.0.0.0/0.0.0.0/0/0	0.0.0.0/0.0.0.0/0/0

Branch FTD (VPN Interface IP: 198.1…

```
show crypto ipsec sa peer 198.…
peer address: 198.18.9.20
interface: VTI1
    Crypto map tag: __vti-crypto-map

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/po
      remote ident (addr/mask/prot/p
      current_peer: 198.18.9.20


      #pkts encaps: 310, #pkts encry
      #pkts decaps: 8757, #pkts decr
      #pkts compressed: 0, #pkts dec
      #pkts not compressed: 310, #pk
      #pre-frag successes: 0, #pre-f
      #PMTUs sent: 0, #PMTUs rcvd: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #I
      #send errors: 0, #recv errors:
```

Hub FTD (VPN Interface IP: 198.18.9…

```
show crypto ipsec sa peer 198.18…
show vpn-sessiondb detail l2l fi…
```

(VPN Interface IP: 198.18.6.10)

```
pto ipsec sa peer 198.18.9.20
-sessiondb detail l2l filter ipaddress 198.18…
```

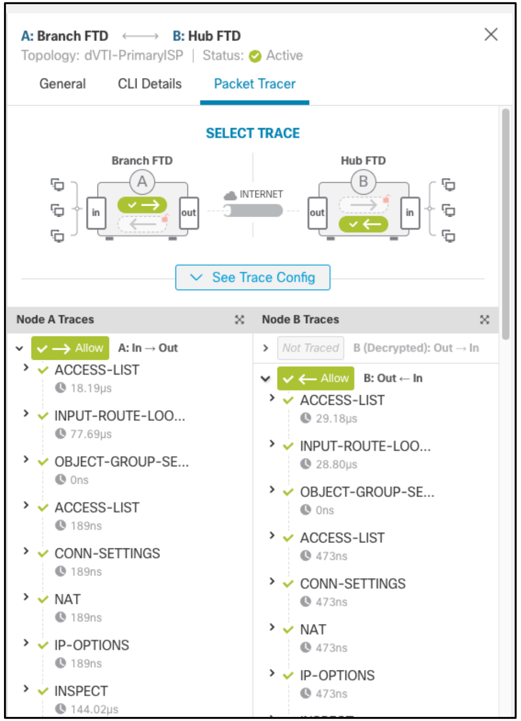
PN Interface IP: 198.18.9.20)

```
pto ipsec sa peer 198.18.6.10
-sessiondb detail l2l filter ipaddress 198.18…
```

Site to Site VPN Dashboard

Packet Tracer

- Packet tracer evaluates the packet against modules such as flow and route lookups, ACLs, protocol inspection, NAT, and QoS
- It shows the output of the trace with the results of each module
- You cannot run a decrypt trace for route-based (VTI-based) VPNs



A: Branch FTD ⟷ B: Hub FTD

Topology: dVTI-PrimaryISP | Status: ✓ Active

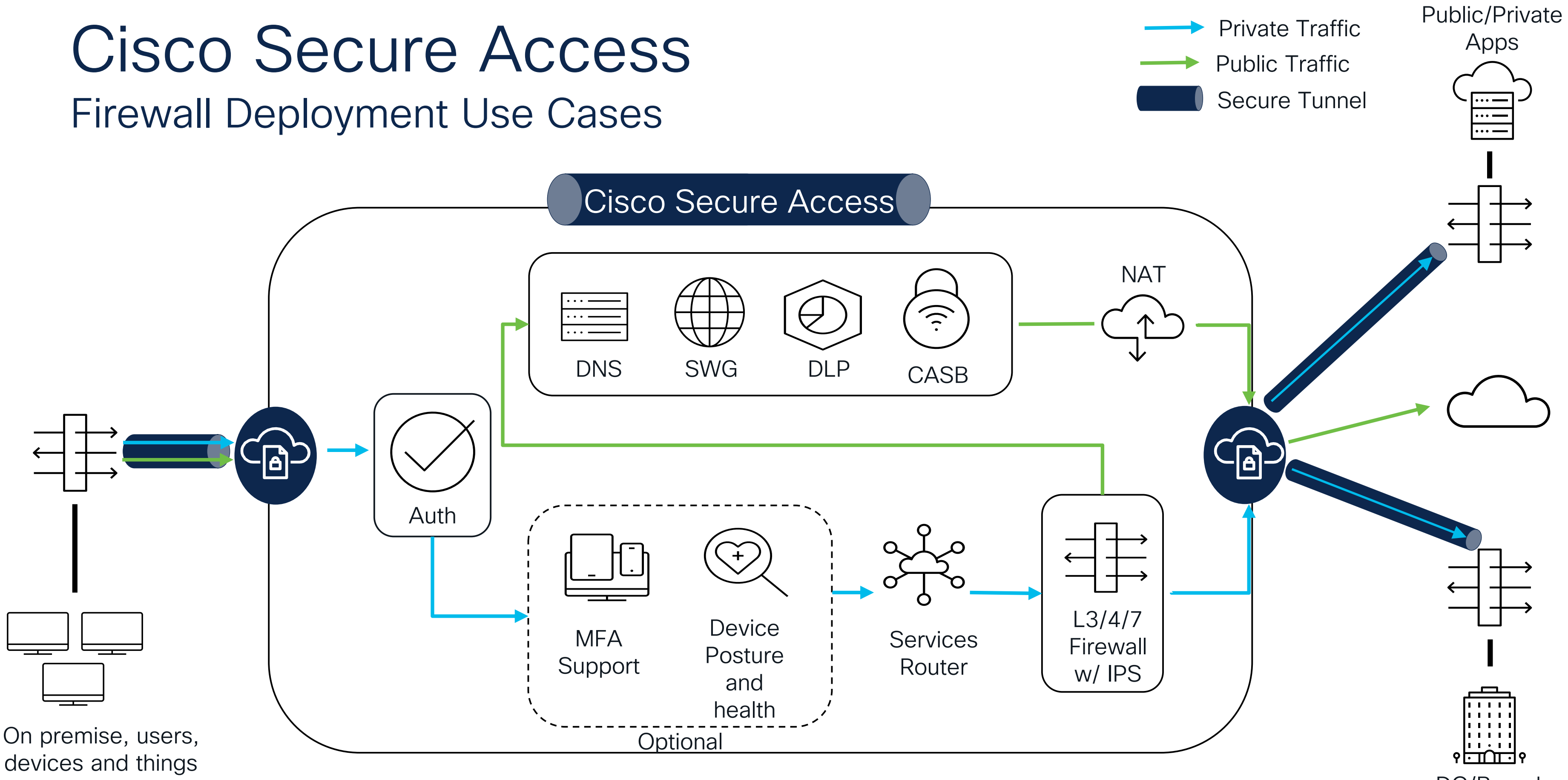
```
Node A Traces
✓ → Allow   A: In → Out
  ✓ ACCESS-LIST
    18.19μs
  ✓ INPUT-ROUTE-LOO...
    77.69μs
  ✓ OBJECT-GROUP-SE...
    0ns
  ✓ ACCESS-LIST
    189ns
  ✓ CONN-SETTINGS
    189ns
  ✓ NAT
    189ns
  ✓ IP-OPTIONS
    189ns
  ✓ INSPECT
    144.02μs
```

```
Node B Traces
Not Traced   B (Decrypted): Out → In
✓ ← Allow   B: Out ← In
  ✓ ACCESS-LIST
    29.18μs
  ✓ INPUT-ROUTE-LOO...
    28.80μs
  ✓ OBJECT-GROUP-SE...
    0ns
  ✓ ACCESS-LIST
    473ns
  ✓ CONN-SETTINGS
    473ns
  ✓ NAT
    473ns
  ✓ IP-OPTIONS
    473ns
```

FTD Integration with Cisco Secure Access

Cisco Secure Access

Firewall Deployment Use Cases

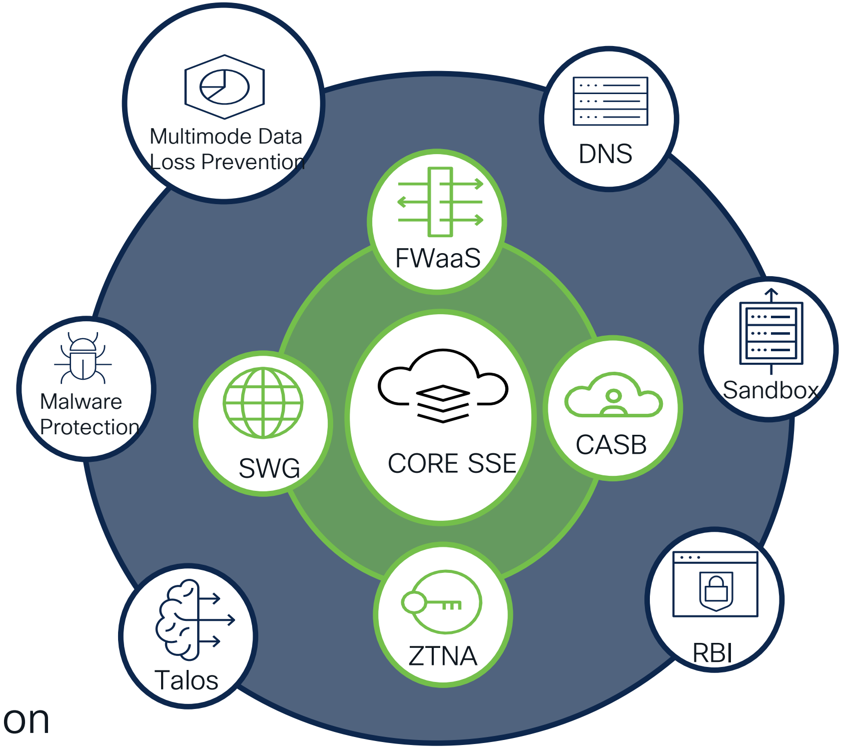


Cisco Secure Access

Benefits

Internet Security Capabilities:

- Umbrella DNS Protection
- DLP and CASB controls
- Web Application controls
- Cloud Malware Protection, sandboxing, decryption



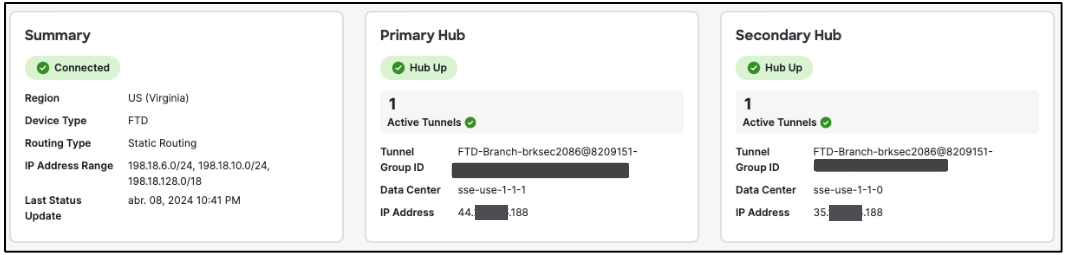
Private Application Access:

- Connectivity to private apps protected by Secure Access
- Connectivity for private applications behind branch firewall

Cisco Secure Access

FTD Tunnels Configuration

SSE Dashboard:



Summary

Connected

Region	US (Virginia)
Device Type	FTD
Routing Type	Static Routing
IP Address Range	198.18.6.0/24, 198.18.10.0/24, 198.18.128.0/18
Last Status Update	abr. 08, 2024 10:41 PM

Primary Hub

Hub Up

1
Active Tunnels

Tunnel Group ID	FTD-Branch-brksec2086@8209151-[redacted]
Data Center	sse-use-1-1-1
IP Address	44.[redacted].188

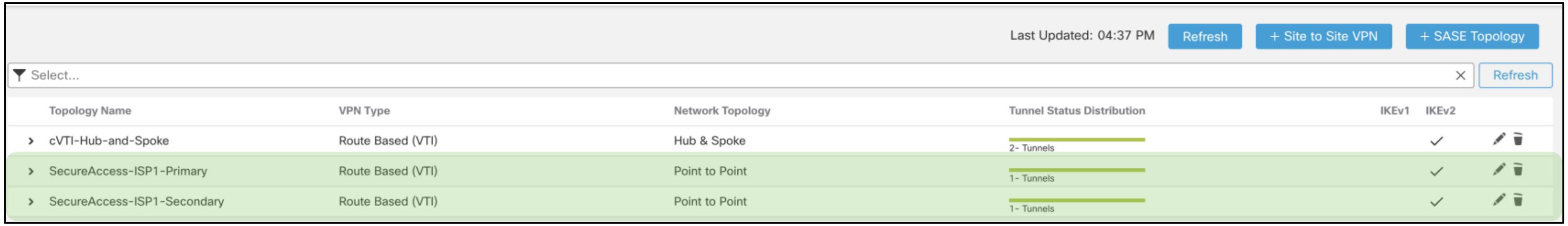
Secondary Hub

Hub Up

1
Active Tunnels

Tunnel Group ID	FTD-Branch-brksec2086@8209151-[redacted]
Data Center	sse-use-1-1-0
IP Address	35.[redacted].188

FMC VPN Topology:



Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
cVTI-Hub-and-Spoke	Route Based (VTI)	Hub & Spoke	2- Tunnels		✓
SecureAccess-ISP1-Primary	Route Based (VTI)	Point to Point	1- Tunnels		✓
SecureAccess-ISP1-Secondary	Route Based (VTI)	Point to Point	1- Tunnels		✓

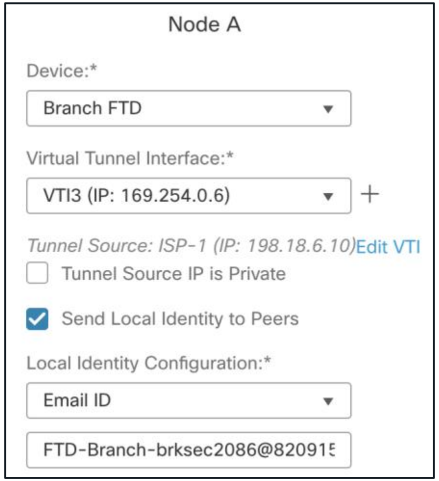
- Dual topologies allow for redundant tunnels to backup Secure Access Data Center

Cisco Secure Access

FTD Tunnels Configuration

- FTD Branch Details

Tunnel to Primary Datacenter



Node A

Device:* Branch FTD

Virtual Tunnel Interface:* VTI3 (IP: 169.254.0.6)

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

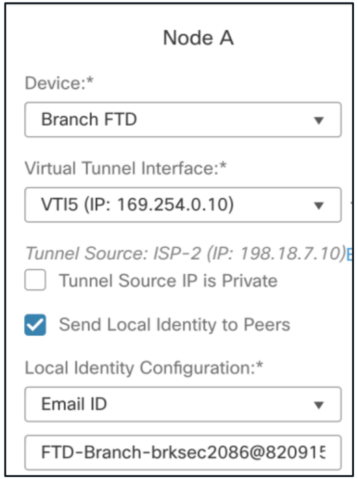
☐ Tunnel Source IP is Private

☑ Send Local Identity to Peers

Local Identity Configuration:* Email ID

FTD-Branch-brksec2086@82091

Tunnel to Secondary Datacenter



Node A

Device:* Branch FTD

Virtual Tunnel Interface:* VTI5 (IP: 169.254.0.10)

*Tunnel Source: ISP-2 (IP: 198.18.7.10)*E

☐ Tunnel Source IP is Private

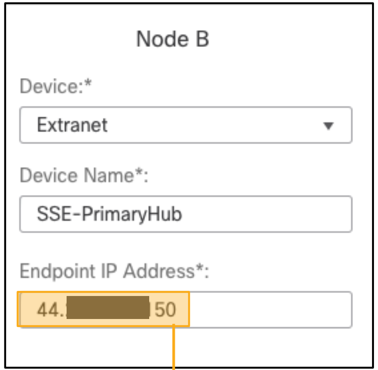
☑ Send Local Identity to Peers

Local Identity Configuration:* Email ID

FTD-Branch-brksec2086@82091

- Secure Access Data Centers

Primary Datacenter



Node B

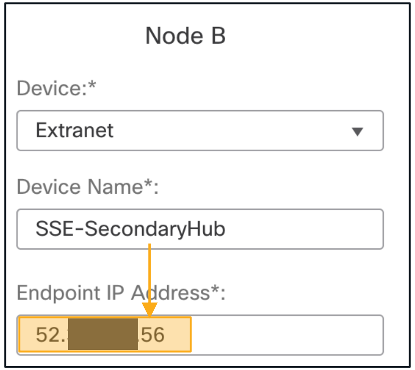
Device:* Extranet

Device Name*: SSE-PrimaryHub

Endpoint IP Address*: 44.[redacted]50

Primary Secure Access Data Center IP Address

Secondary Datacenter



Node B

Device:* Extranet

Device Name*: SSE-SecondaryHub

Endpoint IP Address*: 52.[redacted]56

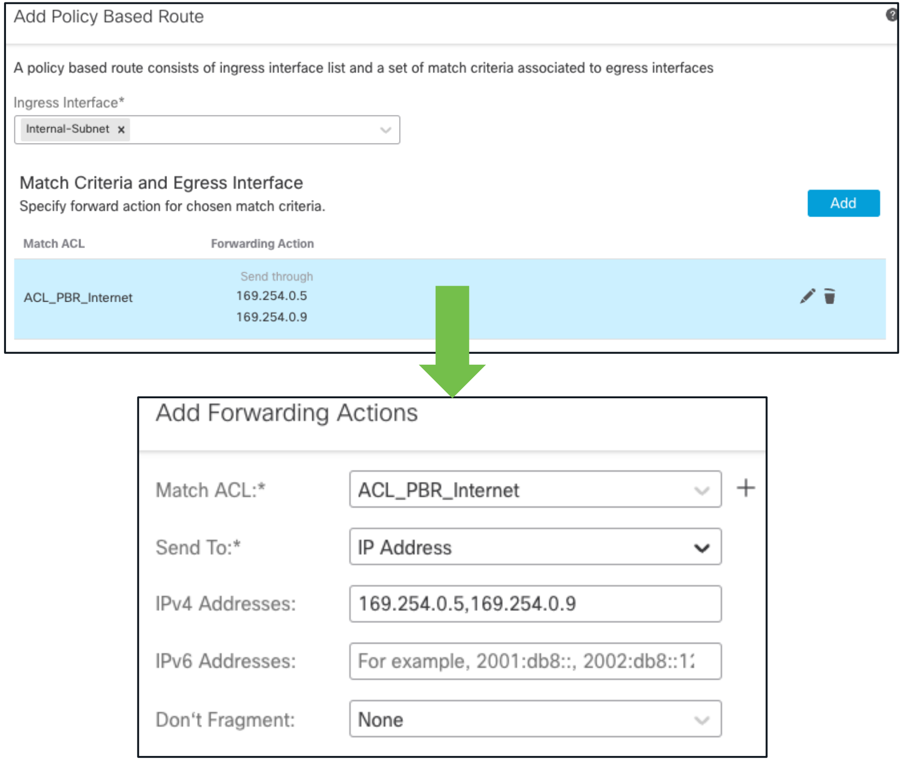
Secondary Secure Access Data Center IP Address

Cisco Secure Access

Routing Configuration

- BGP or Static routing can be used to route traffic to Secure Access Data centers
  a. Static Route considerations:
     - Set Next Hop as any IP address from within the VTI subnet
  b. BGP Routing considerations:
     - Remote AS 64512
     - Unique AS for each branch
     - Use BGP Route Maps to restrict inbound/outbound route advertisements

FTD PBR Configuration to send traffic to Secure Access Cloud



Add 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-Subnet

Match Criteria and Egress Interface

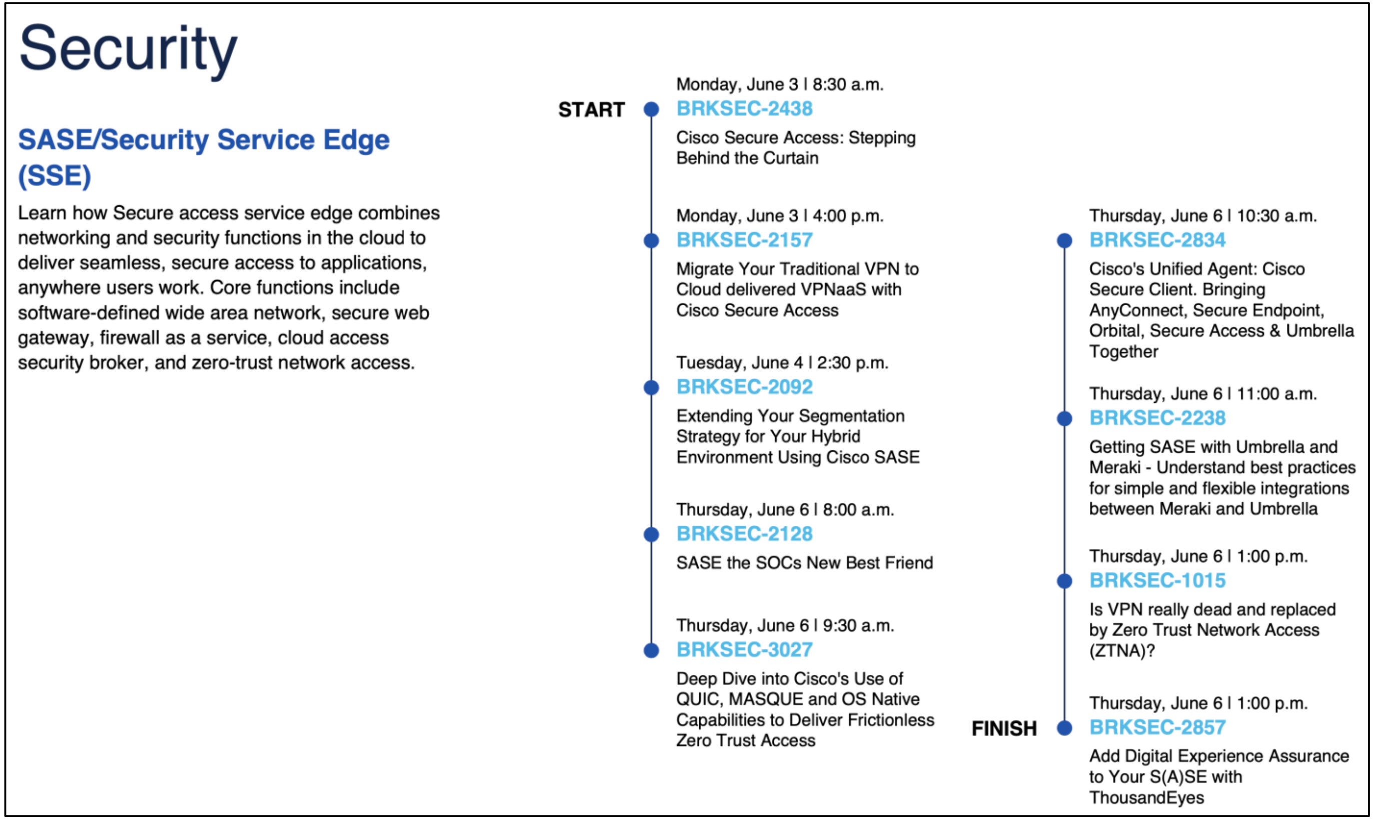
Specify forward action for chosen match criteria.

Match ACL	Forwarding Action
ACL_PBR_Internet	Send through 169.254.0.5 169.254.0.9

Add Forwarding Actions

Match ACL:*	ACL_PBR_Internet
Send To:*	IP Address
IPv4 Addresses:	169.254.0.5,169.254.0.9
IPv6 Addresses:	For example, 2001:db8::, 2002:db8::1:
Don't Fragment:	None

Secure Access Learning Maps



Security

SASE/Security Service Edge (SSE)

Learn how Secure access service edge combines networking and security functions in the cloud to deliver seamless, secure access to applications, anywhere users work. Core functions include software-defined wide area network, secure web gateway, firewall as a service, cloud access security broker, and zero-trust network access.

START

Monday, June 3 I 8:30 a.m.
BRKSEC-2438
Cisco Secure Access: Stepping Behind the Curtain

Monday, June 3 I 4:00 p.m.
BRKSEC-2157
Migrate Your Traditional VPN to Cloud delivered VPNaaS with Cisco Secure Access

Tuesday, June 4 I 2:30 p.m.
BRKSEC-2092
Extending Your Segmentation Strategy for Your Hybrid Environment Using Cisco SASE

Thursday, June 6 I 8:00 a.m.
BRKSEC-2128
SASE the SOCs New Best Friend

Thursday, June 6 I 9:30 a.m.
BRKSEC-3027
Deep Dive into Cisco's Use of QUIC, MASQUE and OS Native Capabilities to Deliver Frictionless Zero Trust Access

Thursday, June 6 I 10:30 a.m.
BRKSEC-2834
Cisco's Unified Agent: Cisco Secure Client. Bringing AnyConnect, Secure Endpoint, Orbital, Secure Access & Umbrella Together

Thursday, June 6 I 11:00 a.m.
BRKSEC-2238
Getting SASE with Umbrella and Meraki - Understand best practices for simple and flexible integrations between Meraki and Umbrella

Thursday, June 6 I 1:00 p.m.
BRKSEC-1015
Is VPN really dead and replaced by Zero Trust Network Access (ZTNA)?

FINISH

Thursday, June 6 I 1:00 p.m.
BRKSEC-2857
Add Digital Experience Assurance to Your S(A)SE with ThousandEyes

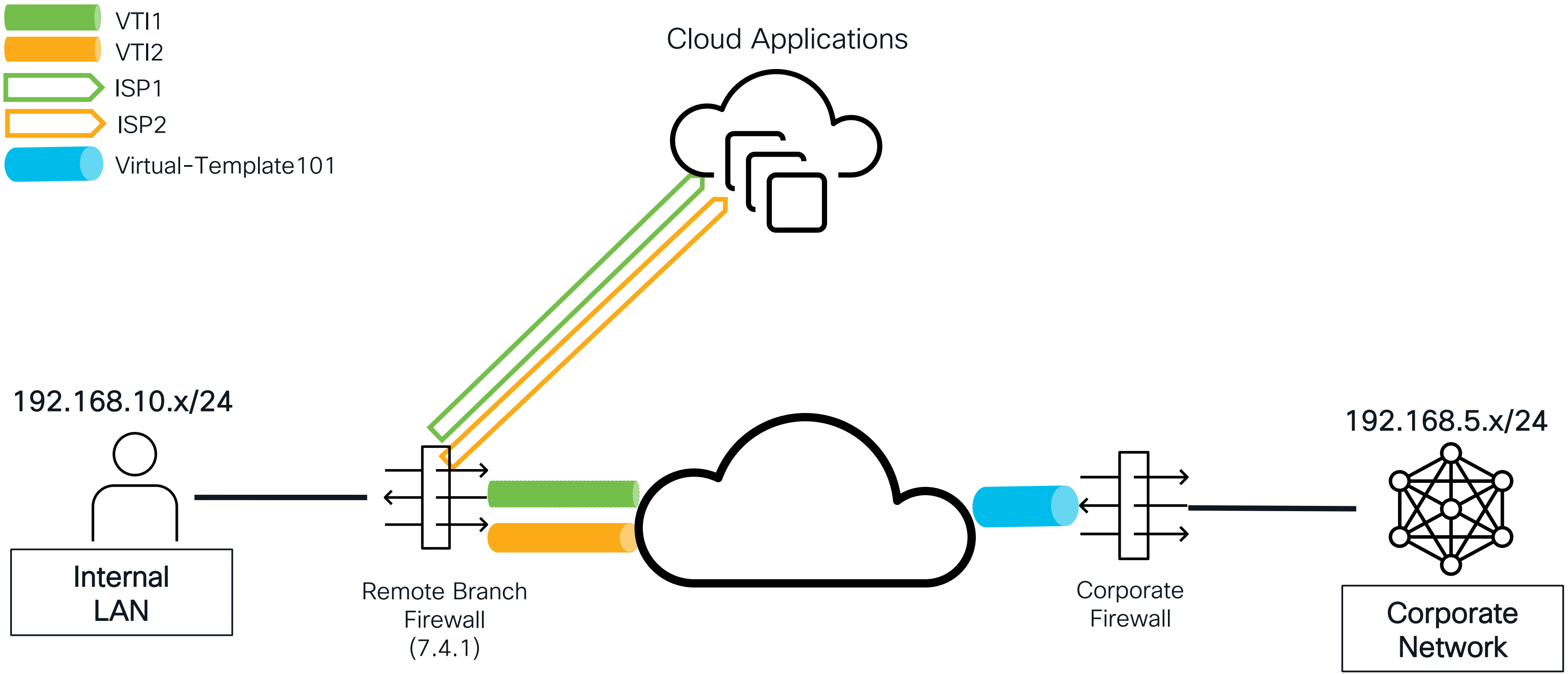
Demo

Demo 1: DIA configuration

In this Demo we will...

- Configure Trusted DNS server
- Configure ECMP for both sVTI and WAN interfaces
- Configure Extended Access List with Applications
- Configure PBR with Applications
- Initiate traffic from end user machine to both WAN links and VTI tunnels based on applications

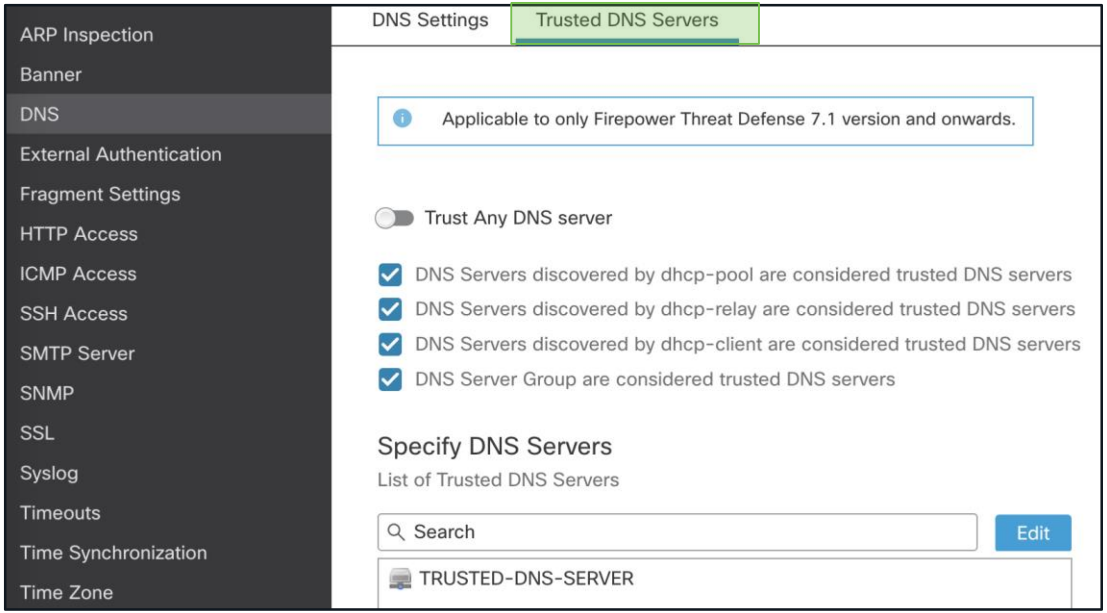
Demo 1 Topology



Remote Branch Firewall Configuration

Trusted DNS Server Configuration

- Devices > Platform Settings > DNS > Trusted DNS Servers



Applicable to only Firepower Threat Defense 7.1 version and onwards.

Trust Any DNS server

☑ DNS Servers discovered by dhcp-pool are considered trusted DNS servers

☑ DNS Servers discovered by dhcp-relay are considered trusted DNS servers

☑ DNS Servers discovered by dhcp-client are considered trusted DNS servers

☑ DNS Server Group are considered trusted DNS servers

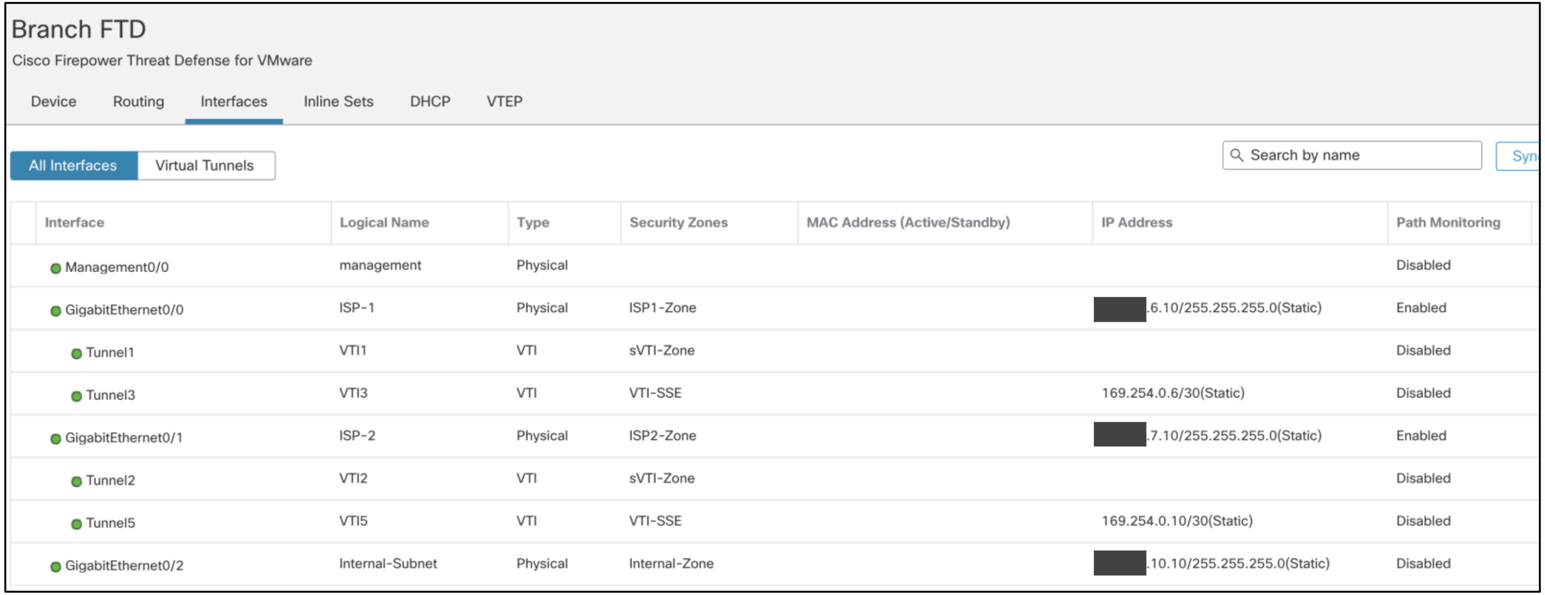
Specify DNS Servers

List of Trusted DNS Servers

TRUSTED-DNS-SERVER

Interfaces Configuration

- Devices > Interfaces



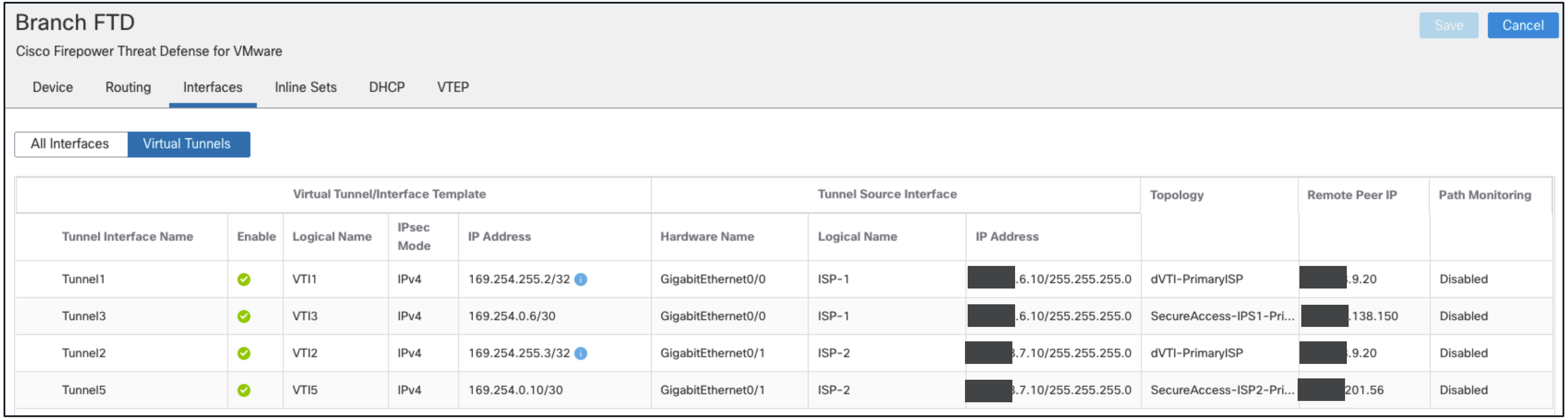
Branch FTD

Cisco Firepower Threat Defense for VMware

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring
● Management0/0	management	Physical				Disabled
● GigabitEthernet0/0	ISP-1	Physical	ISP1-Zone		[redacted].6.10/255.255.255.0(Static)	Enabled
● Tunnel1	VTI1	VTI	sVTI-Zone			Disabled
● Tunnel3	VTI3	VTI	VTI-SSE		169.254.0.6/30(Static)	Disabled
● GigabitEthernet0/1	ISP-2	Physical	ISP2-Zone		[redacted].7.10/255.255.255.0(Static)	Enabled
● Tunnel2	VTI2	VTI	sVTI-Zone			Disabled
● Tunnel5	VTI5	VTI	VTI-SSE		169.254.0.10/30(Static)	Disabled
● GigabitEthernet0/2	Internal-Subnet	Physical	Internal-Zone		[redacted].10.10/255.255.255.0(Static)	Disabled

VTIs Configuration

- Devices > Interfaces > Virtual Tunnels



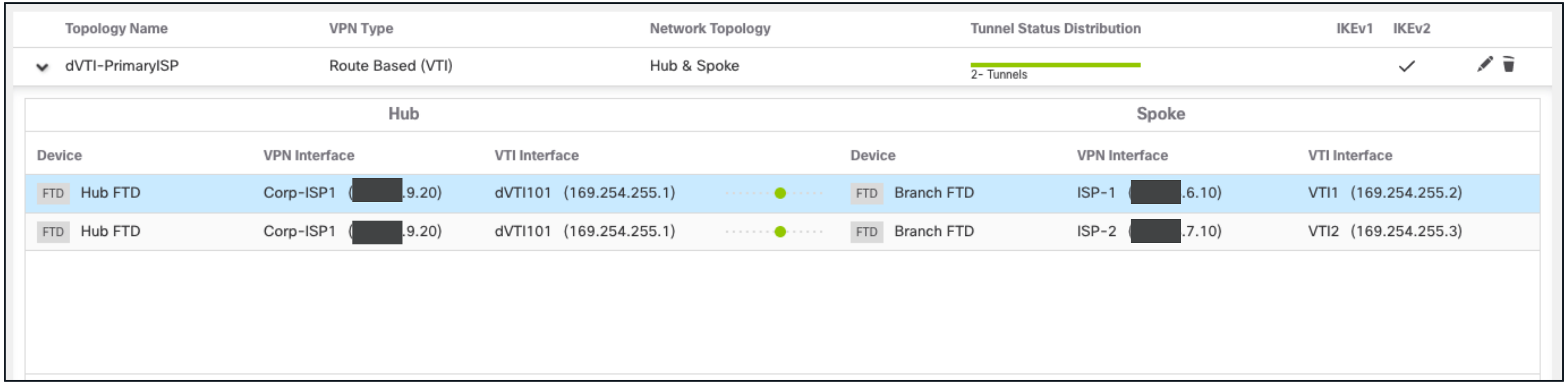
Branch FTD

Cisco Firepower Threat Defense for VMware

Virtual Tunnel/Interface Template					Tunnel Source Interface			Topology	Remote Peer IP	Path Monitoring
Tunnel Interface Name	Enable	Logical Name	IPsec Mode	IP Address	Hardware Name	Logical Name	IP Address			
Tunnel1	✓	VTI1	IPv4	169.254.255.2/32 ⓘ	GigabitEthernet0/0	ISP-1	[redacted].6.10/255.255.255.0	dVTI-PrimaryISP	[redacted].9.20	Disabled
Tunnel3	✓	VTI3	IPv4	169.254.0.6/30	GigabitEthernet0/0	ISP-1	[redacted].6.10/255.255.255.0	SecureAccess-IPS1-Pri...	[redacted].138.150	Disabled
Tunnel2	✓	VTI2	IPv4	169.254.255.3/32 ⓘ	GigabitEthernet0/1	ISP-2	[redacted].7.10/255.255.255.0	dVTI-PrimaryISP	[redacted].9.20	Disabled
Tunnel5	✓	VTI5	IPv4	169.254.0.10/30	GigabitEthernet0/1	ISP-2	[redacted].7.10/255.255.255.0	SecureAccess-ISP2-Pri...	[redacted]201.56	Disabled

VPN Topology

- Devices > VPN > Site to Site

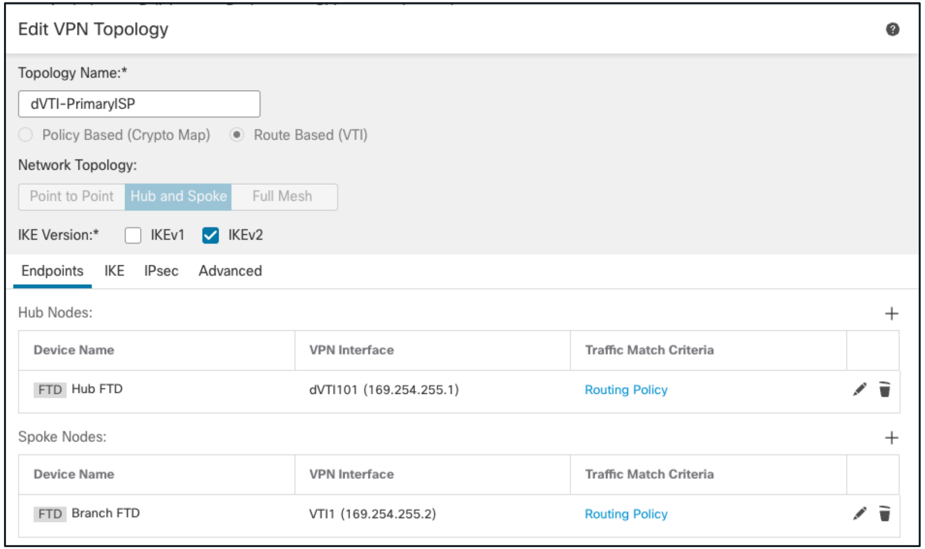


Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
dVTI-PrimaryISP	Route Based (VTI)	Hub & Spoke	2- Tunnels		✓

Hub			Spoke		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
FTD Hub FTD	Corp-ISP1 ([redacted].9.20)	dVTI101 (169.254.255.1)	FTD Branch FTD	ISP-1 ([redacted].6.10)	VTI1 (169.254.255.2)
FTD Hub FTD	Corp-ISP1 ([redacted].9.20)	dVTI101 (169.254.255.1)	FTD Branch FTD	ISP-2 ([redacted].7.10)	VTI2 (169.254.255.3)

VPN Topology

- Devices > VPN > Site to Site > dVTI-PrimaryISP



Edit VPN Topology

Topology Name:* dVTI-PrimaryISP

○ Policy Based (Crypto Map) ● Route Based (VTI)

Network Topology: Point to Point | **Hub and Spoke** | Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

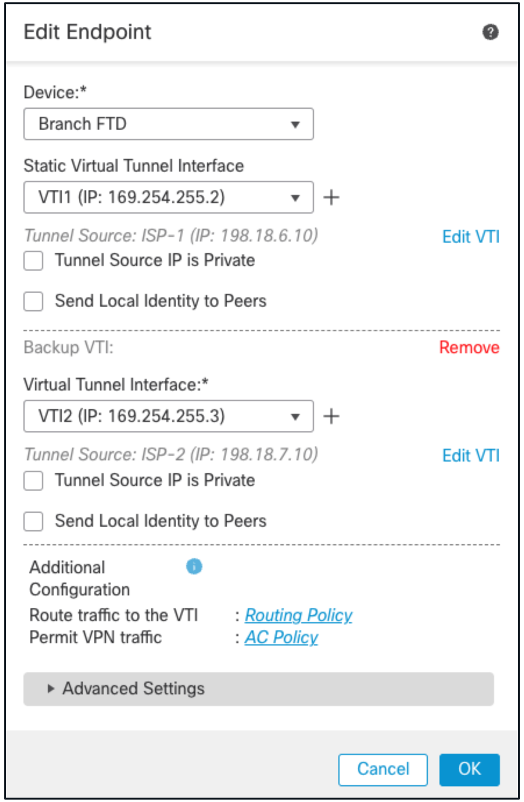
Endpoints | IKE | IPsec | Advanced

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



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

Backup VTI: Remove

Virtual Tunnel Interface:* VTI2 (IP: 169.254.255.3)

Tunnel Source: ISP-2 (IP: 198.18.7.10) Edit VTI

□ Tunnel Source IP is Private

□ Send Local Identity to Peers

Additional Configuration

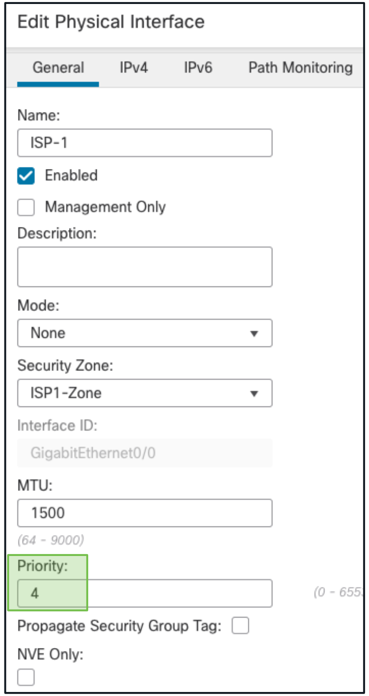
Route traffic to the VTI : Routing Policy

Permit VPN traffic : AC Policy

▸ Advanced Settings

Interfaces Priority Configuration

- Devices > Interfaces



Edit Physical Interface

Name: ISP-1

☑ Enabled

□ Management Only

Description:

Mode: None

Security Zone: ISP1-Zone

Interface ID: GigabitEthernet0/0

MTU: 1500

(64 - 9000)

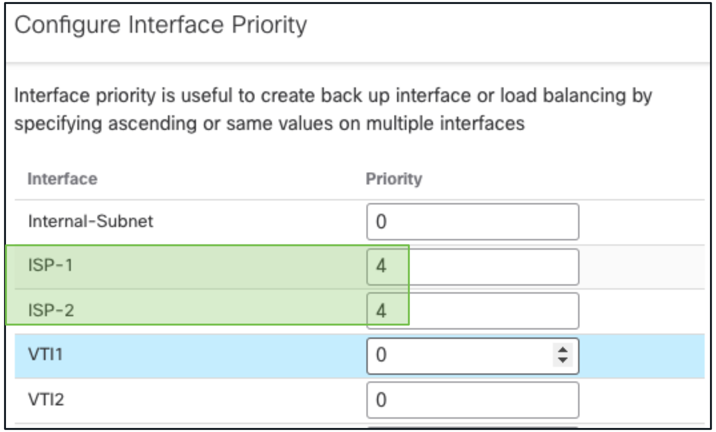
Priority: 4 (0 - 655

Propagate Security Group Tag: □

NVE Only:

□

- Devices > Routing > Policy Based Routing > Configure Interface Priority



Configure Interface Priority

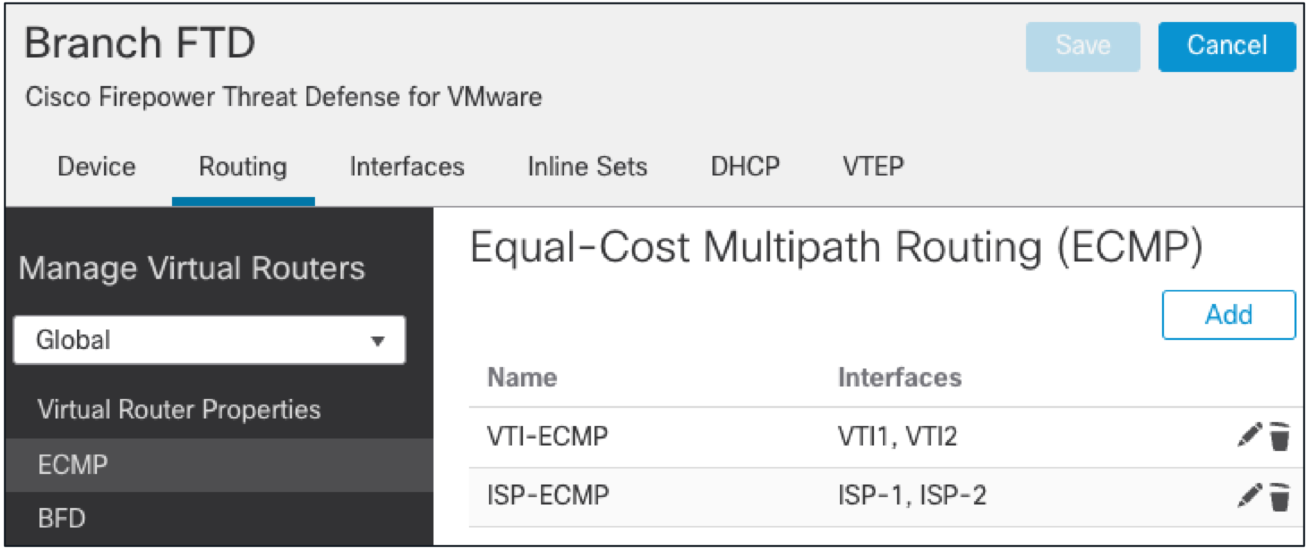
Interface priority is useful to create back up interface or load balancing by specifying ascending or same values on multiple interfaces

Interface	Priority
Internal-Subnet	0
ISP-1	4
ISP-2	4
VTI1	0
VTI2	0

Routing Configuration

ECMP Configuration

- Routing > ECMP



Cisco Firepower Threat Defense for VMware

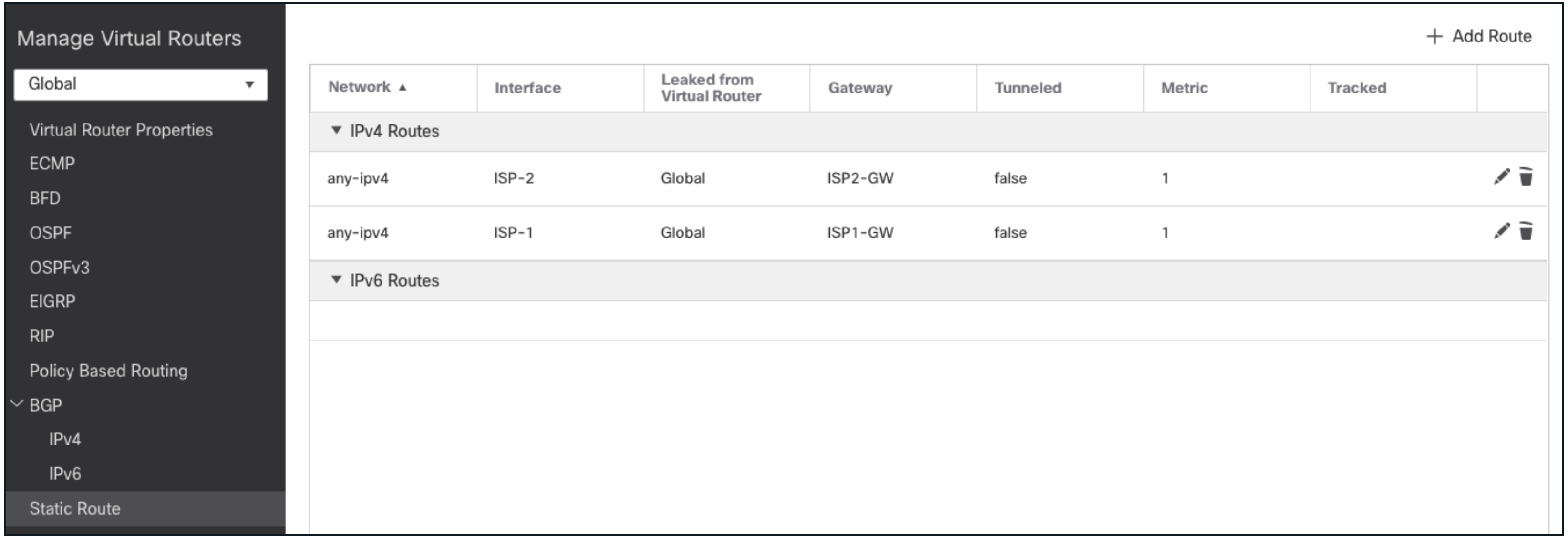
Equal-Cost Multipath Routing (ECMP)

Name	Interfaces
VTI-ECMP	VTI1, VTI2
ISP-ECMP	ISP-1, ISP-2

Routing Configuration

Static Routing Configuration

- Routing > Static Route

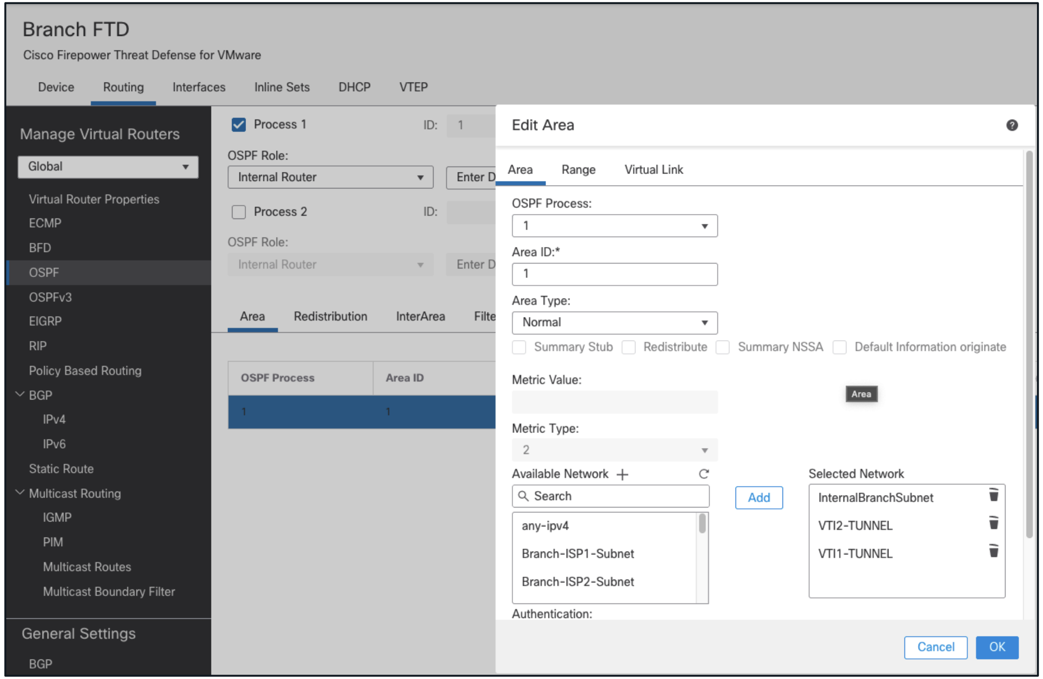


Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
any-ipv4	ISP-2	Global	ISP2-GW	false	1	
any-ipv4	ISP-1	Global	ISP1-GW	false	1	
▼ IPv6 Routes						

Routing Configuration

OSPF Configuration

- Routing > OSPF



Branch FTD

Cisco Firepower Threat Defense for VMware

Device | Routing | Interfaces | Inline Sets | DHCP | VTEP

Manage Virtual Routers

Global

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP
PIM
Multicast Routes
Multicast Boundary Filter

General Settings

BGP

☑ Process 1 ID: 1

OSPF Role: Internal Router

□ Process 2 ID:

OSPF Role: Internal Router

Area | Redistribution | InterArea | Filte

OSPF Process	Area ID
1	1

Edit Area

Area | Range | Virtual Link

OSPF Process: 1

Area ID:* 1

Area Type: Normal

□ Summary Stub □ Redistribute □ Summary NSSA □ Default Information originate

Metric Value:

Area

Metric Type: 2

Available Network: any-ipv4, Branch-ISP1-Subnet, Branch-ISP2-Subnet

Add

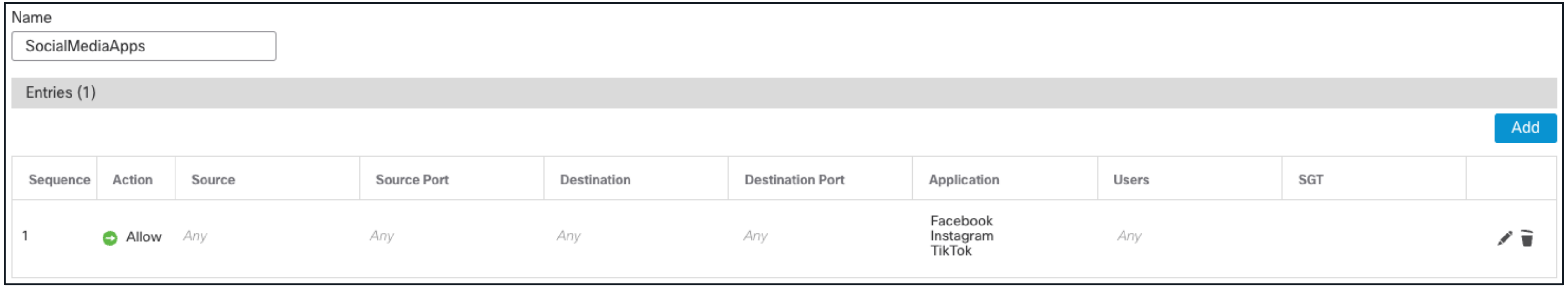
Selected Network: InternalBranchSubnet, VTI2-TUNNEL, VTI1-TUNNEL

Authentication:

Cancel | OK

Extended Access-List Configuration

- Objects > Object Management > Access-List > Extended



Name

SocialMediaApps

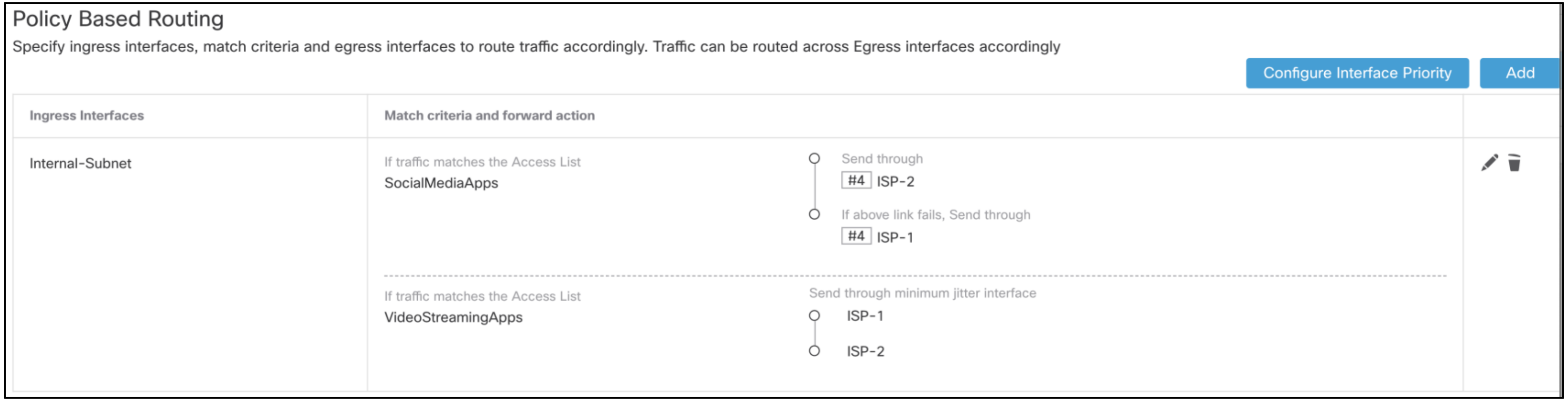
Entries (1)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	Any	Any	Any	Any	Facebook Instagram TikTok	Any		

DIA Configuration - PBR

- Device > Routing > Policy Based Routing

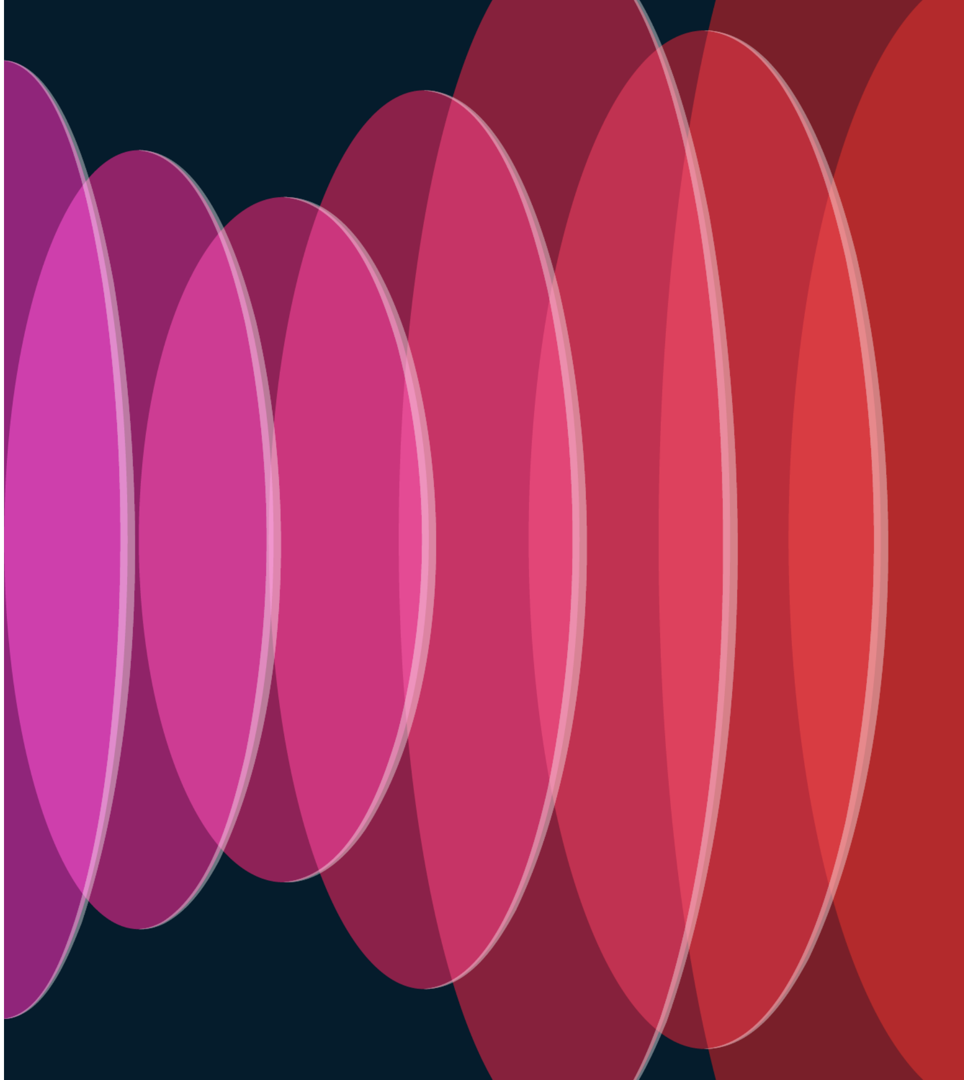


Policy Based Routing

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

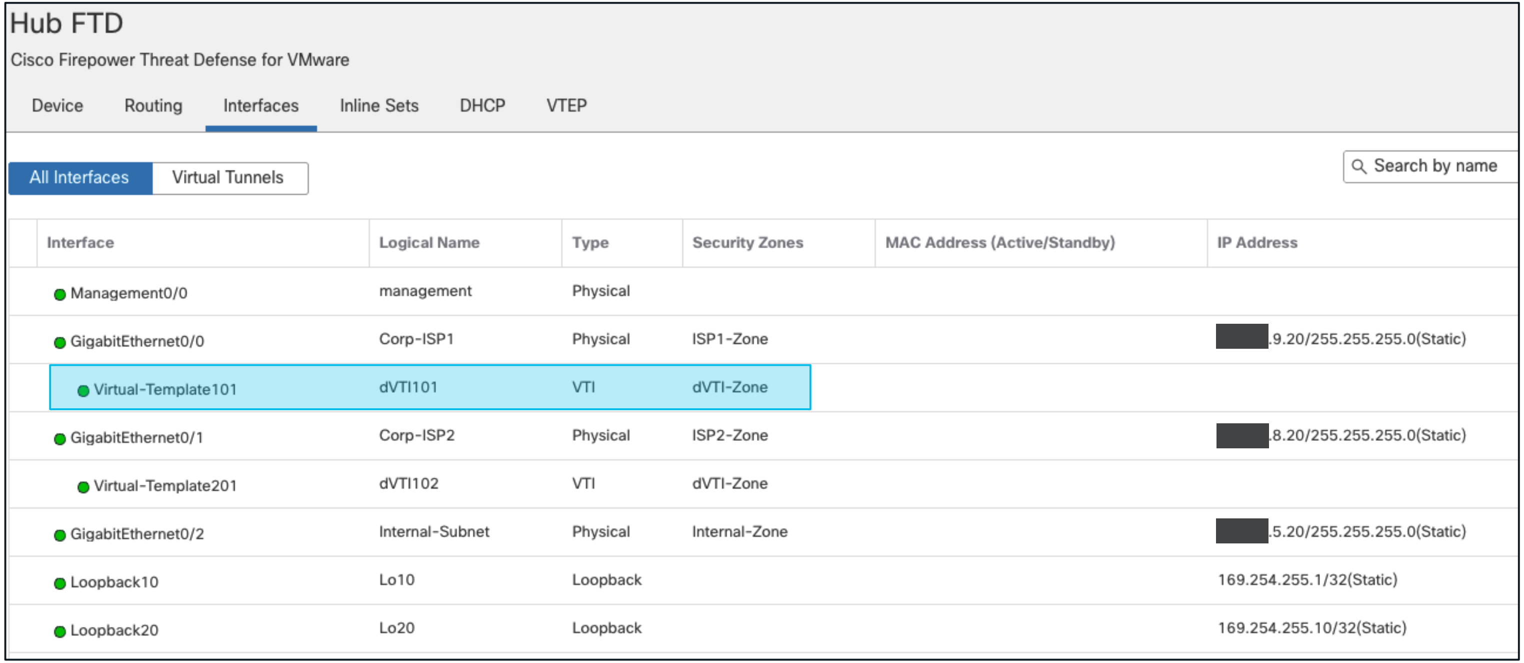
Ingress Interfaces	Match criteria and forward action	
Internal-Subnet	If traffic matches the Access List SocialMediaApps	Send through #4 ISP-2 If above link fails, Send through #4 ISP-1
	If traffic matches the Access List VideoStreamingApps	Send through minimum jitter interface ISP-1 ISP-2

Hub Firewall Configuration



Interfaces Configuration

- Devices > Interfaces



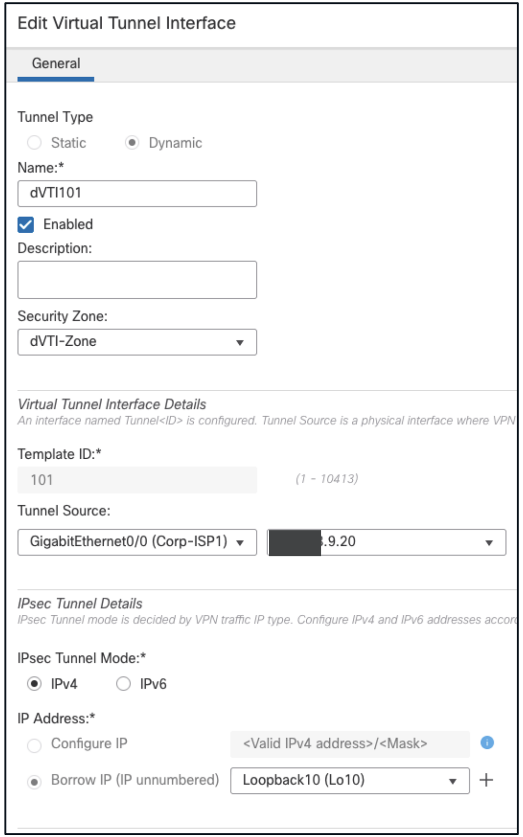
Hub FTD

Cisco Firepower Threat Defense for VMware

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
● Management0/0	management	Physical			
● GigabitEthernet0/0	Corp-ISP1	Physical	ISP1-Zone		[redacted].9.20/255.255.255.0(Static)
● Virtual-Template101	dVTI101	VTI	dVTI-Zone		
● GigabitEthernet0/1	Corp-ISP2	Physical	ISP2-Zone		[redacted].8.20/255.255.255.0(Static)
● Virtual-Template201	dVTI102	VTI	dVTI-Zone		
● GigabitEthernet0/2	Internal-Subnet	Physical	Internal-Zone		[redacted].5.20/255.255.255.0(Static)
● Loopback10	Lo10	Loopback			169.254.255.1/32(Static)
● Loopback20	Lo20	Loopback			169.254.255.10/32(Static)

Interfaces Configuration

- Devices > Interfaces > All Interfaces



Edit Virtual Tunnel Interface

General

Tunnel Type
○ Static ● Dynamic

Name:* dVTI101

☑ Enabled

Description:

Security Zone: dVTI-Zone

Virtual Tunnel Interface Details
An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN

Template ID:* 101 *(1 - 10413)*

Tunnel Source: GigabitEthernet0/0 (Corp-ISP1) [redacted].9.20

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

IPsec Tunnel Mode:*
● IPv4 ○ IPv6

IP Address:*
○ Configure IP <Valid IPv4 address>/<Mask>
● Borrow IP (IP unnumbered) Loopback10 (Lo10)

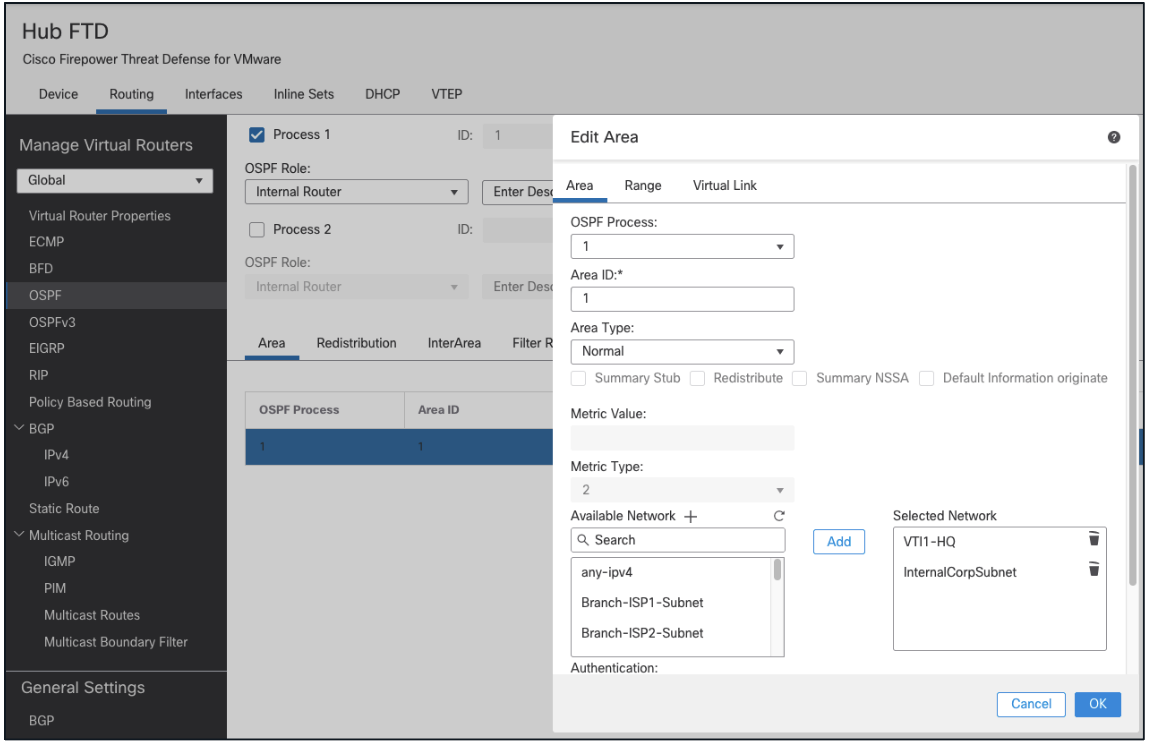
- FTD CLI

```
interface Virtual-Template101 type tunnel
 nameif dVTI101
 ip unnumbered Lo10
 ospf network point-to-point non-broadcast
 ospf authentication null
 tunnel source interface Corp-ISP1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_2
```

Routing Configuration

OSPF Configuration

- Routing > OSPF



Hub FTD

Cisco Firepower Threat Defense for VMware

Device | Routing | Interfaces | Inline Sets | DHCP | VTEP

Manage Virtual Routers

Global ▾

- Virtual Router Properties
- ECMP
- BFD
- OSPF
- OSPFv3
- EIGRP
- RIP
- Policy Based Routing
- BGP
  - IPv4
  - IPv6
- Static Route
- Multicast Routing
  - IGMP
  - PIM
  - Multicast Routes
  - Multicast Boundary Filter

General Settings

- BGP

☑ Process 1 ID: 1

OSPF Role: Internal Router ▾ Enter Desc

□ Process 2 ID:

OSPF Role: Internal Router ▾ Enter Desc

Area | Redistribution | InterArea | Filter R

OSPF Process	Area ID
1	1

Edit Area

Area | Range | Virtual Link

OSPF Process: 1

Area ID:* 1

Area Type: Normal

□ Summary Stub □ Redistribute □ Summary NSSA □ Default Information originate

Metric Value:

Metric Type: 2

Available Network +

Search

- any-ipv4
- Branch-ISP1-Subnet
- Branch-ISP2-Subnet

Add

Selected Network

- VTI1-HQ
- InternalCorpSubnet

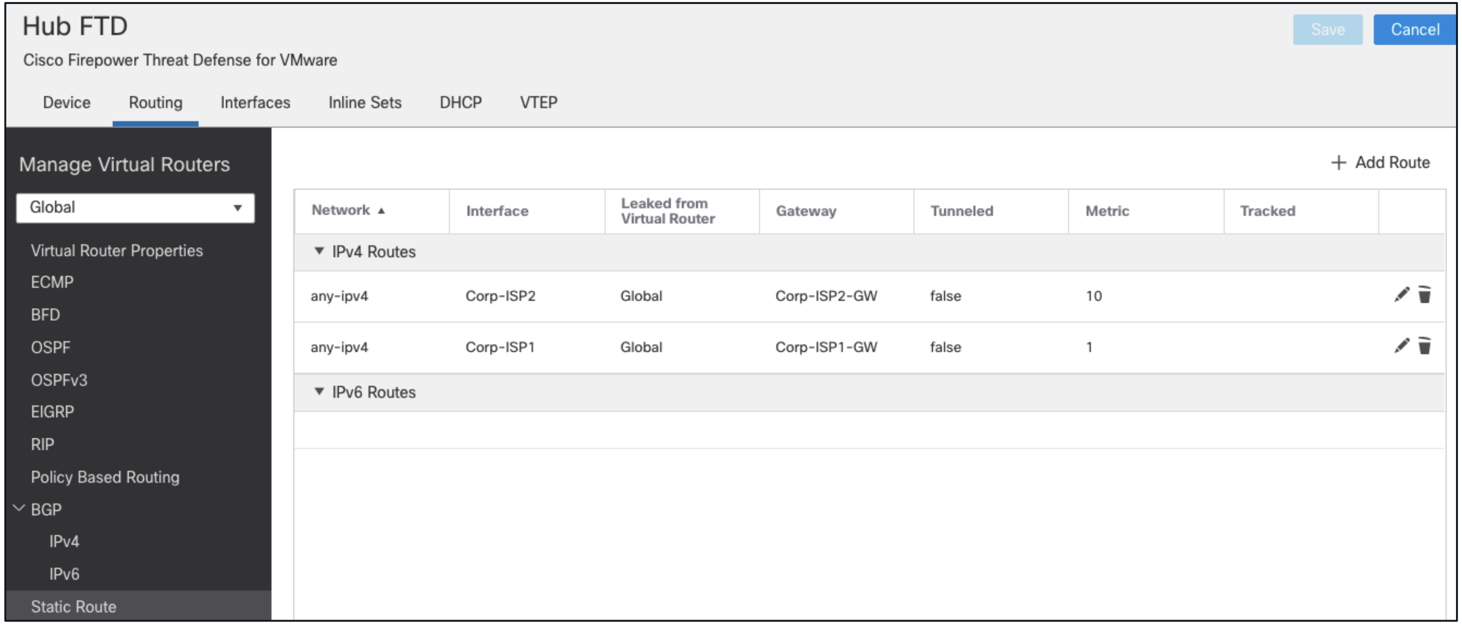
Authentication:

Cancel | OK

Routing Configuration

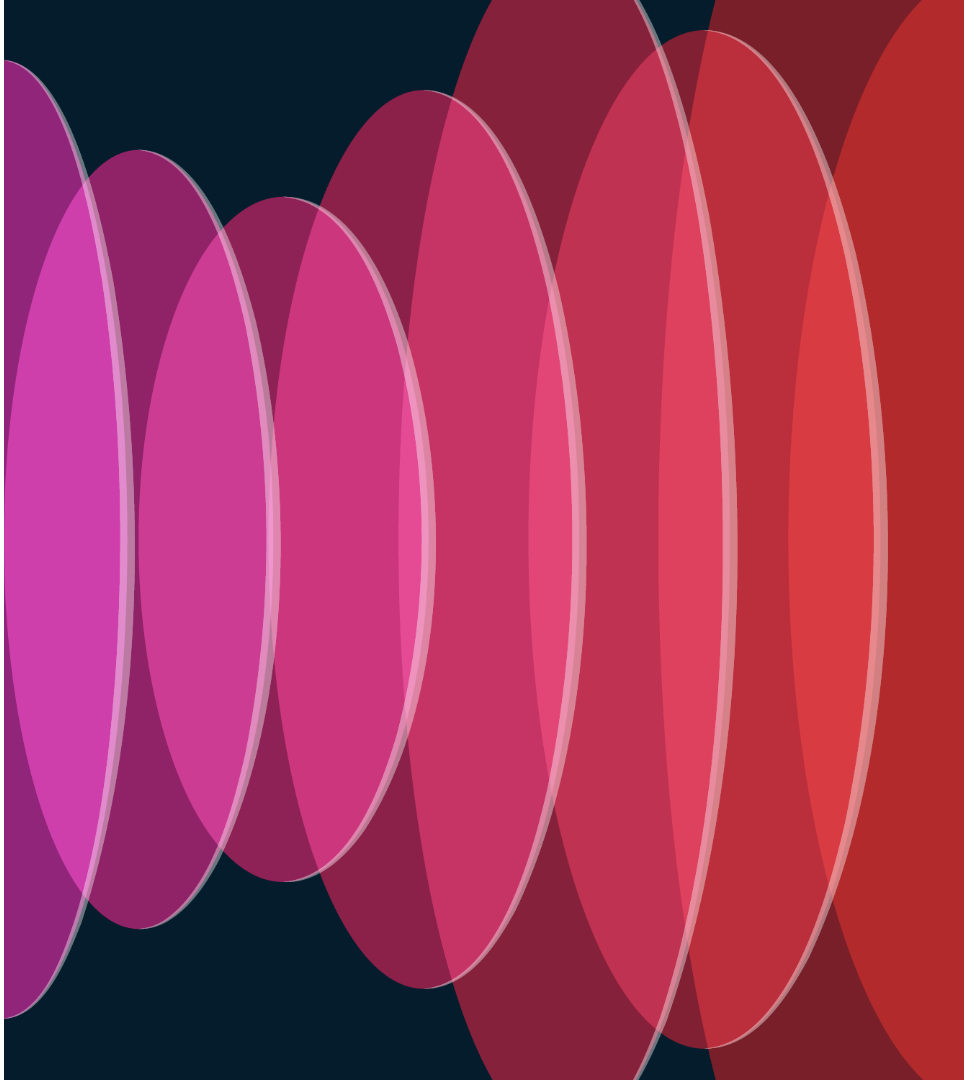
Static Routing Configuration

- Routing > Static Route



Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
▼ IPv4 Routes							
any-ipv4	Corp-ISP2	Global	Corp-ISP2-GW	false	10		
any-ipv4	Corp-ISP1	Global	Corp-ISP1-GW	false	1		
▼ IPv6 Routes							

Verification and Troubleshooting



Verification Commands

To show all the NSOs in the Firewall:

```
firepower# show object network-service
[…]
object network-service "Cisco" dynamic
 description Official website for Cisco.
 app-id 2655
 domain cisco.com (bid=1851027941) ip (hitcnt=0)
object network-service "Duo Security" dynamic
 description A user-centric access security platform that provides two-factor
 authentication, endpoint security, remote access solutions and a
 subsidiary of Cisco.
 app-id 4648
 domain duosecurity.com (bid=-2050678515) ip (hitcnt=0)
 domain duo.com (bid=-205510683) ip (hitcnt=0)
[…]
```

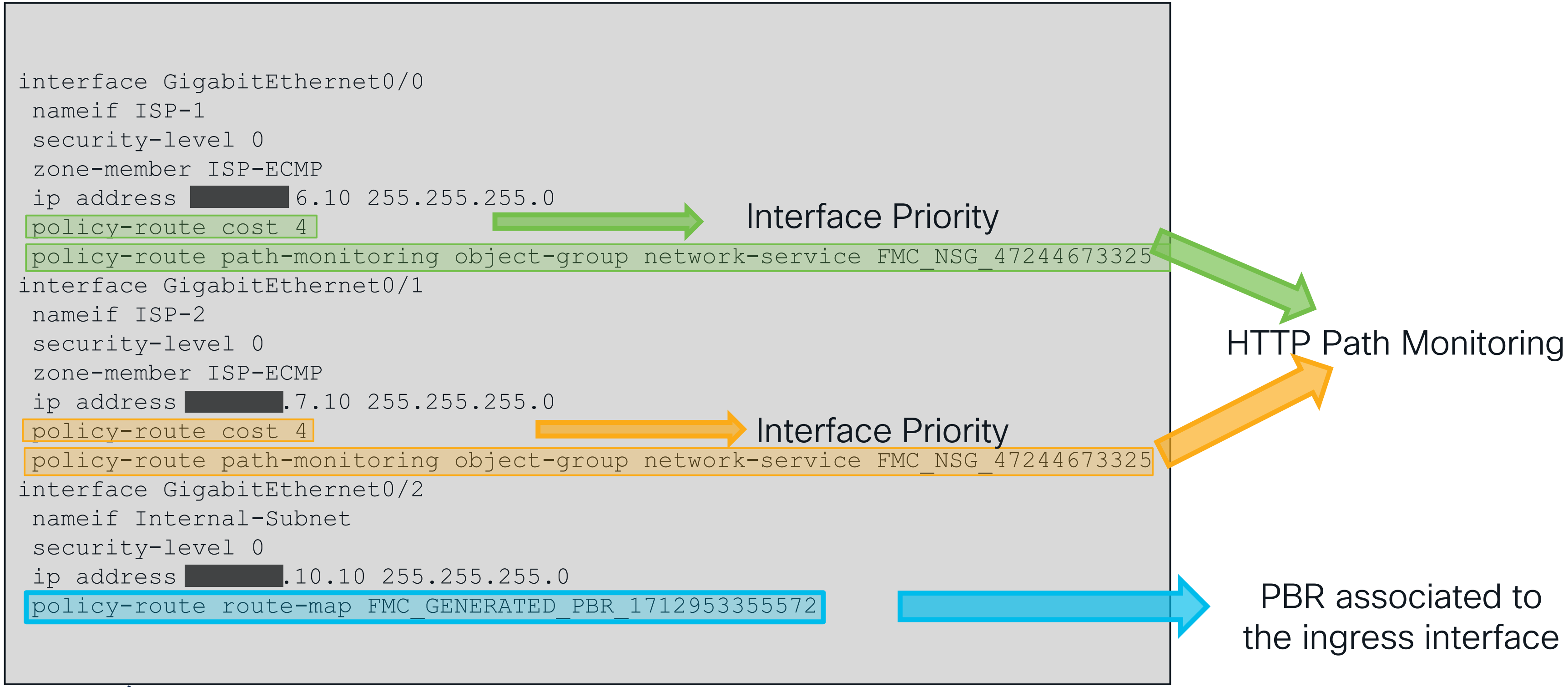
Verification Commands

To show a specific NSO:

```
firepower# show object id Cisco
object network-service "Cisco" dynamic
 description Official website for Cisco.
 app-id 2655
 domain cisco.com (bid=1851027941) ip (hitcnt=0)

firepower# show object id "Duo Security"
object network-service "Duo Security" dynamic
 description A user-centric access security platform that provides two-factor
 authentication, endpoint security, remote access solutions and a
 subsidiary of Cisco.
 app-id 4648
 domain duosecurity.com (bid=-2050678515) ip (hitcnt=0)
 domain duo.com (bid=-2050510683) ip (hitcnt=0)
```

Verification Commands

Spoke Interfaces configuration:



```
interface GigabitEthernet0/0
 nameif ISP-1
 security-level 0
 zone-member ISP-ECMP
 ip address [redacted]6.10 255.255.255.0
 policy-route cost 4
 policy-route path-monitoring object-group network-service FMC_NSG_47244673325
interface GigabitEthernet0/1
 nameif ISP-2
 security-level 0
 zone-member ISP-ECMP
 ip address [redacted].7.10 255.255.255.0
 policy-route cost 4
 policy-route path-monitoring object-group network-service FMC_NSG_47244673325
interface GigabitEthernet0/2
 nameif Internal-Subnet
 security-level 0
 ip address [redacted].10.10 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1712953355572
```

Interface Priority

HTTP Path Monitoring

Interface Priority

PBR associated to the ingress interface

Verification Commands

Spoke VTIs configuration:

```
interface Tunnel1
 nameif VTI1
 zone-member VTI-ECMP
 ip unnumbered Lo1
 tunnel source interface ISP-1
 tunnel destination [redacted]9.20
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_2

interface Tunnel2
 nameif VTI2
 zone-member VTI-ECMP
 ip unnumbered Lo2
 tunnel source interface ISP-2
 tunnel destination [redacted]9.20
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_2
```

```
interface Loopback1
 nameif Lo1
 ip address 169.254.255.2 255.255.255.255

interface Loopback2
 nameif Lo2
 ip address 169.254.255.3 255.255.255.255
```

Verification Commands

Route-Map configuration:

To show the route-map configuration:

```
Branch-FTD# show running-config route-map

route-map FMC_GENERATED_PBR_1712953355572 permit 5
 match ip address SocialMediaApps
 set interface ISP-2 ISP-1
route-map FMC_GENERATED_PBR_1712953355572 permit 10
 match ip address VideoStreamingApps
 set adaptive-interface jitter ISP-1 ISP-2
```

Per Interface Order

To show the To show the Access-Lists associated to the PBR:

```
Branch-FTD# show runn access-list SocialMediaApps
access-list SocialMediaApps extended permit ip any object-group-network-service FMC_NSG_47244673306

Branch-FTD# show runn access-list VideoStreamingApps
access-list VideoStreamingApps extended permit ip any object-group-network-service FMC_NSG_47244673325
```

Verification Commands

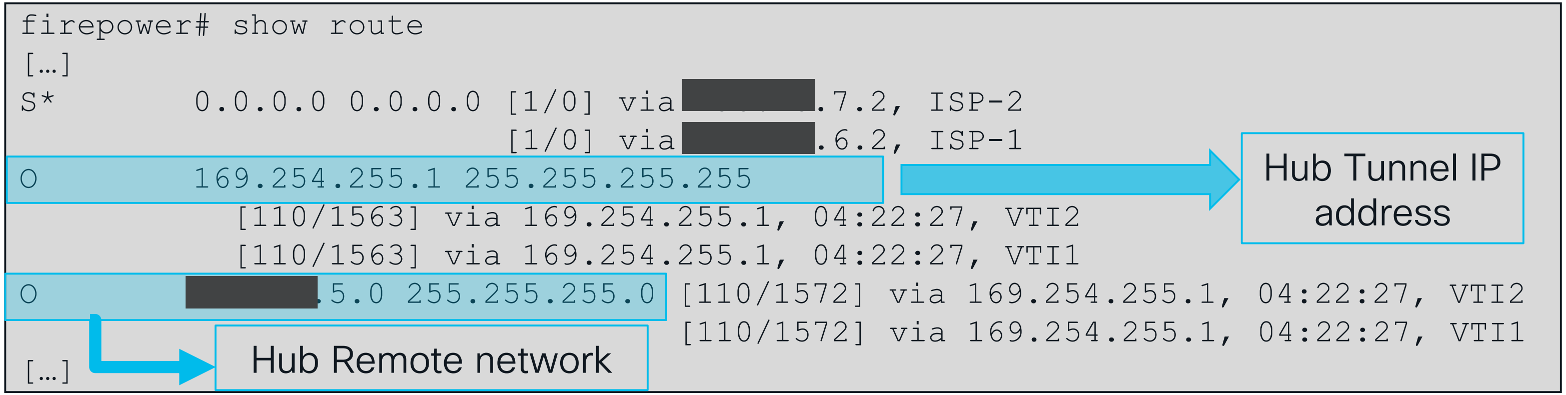
To show the NSGs associated to the acess lists:

```
Branch-FTD# show runn object-group network-service
object-group network-service FMC_NSG_47244673306
 network-service-member "Facebook"
 network-service-member "Instagram"
 network-service-member "TikTok"
object-group network-service FMC_NSG_47244673325
 network-service-member "Amazon Prime Video"
 network-service-member "Disney Plus"
 network-service-member "Netflix"
 network-service-member "Netflix stream”
[…]
```

Verification Commands

To show the routing configuration and routing table:

```
> show running-config route
route ISP-1 0.0.0.0 0.0.0.0 [redacted].6.2 1 track 1
route ISP-2 0.0.0.0 0.0.0.0 [redacted].7.2 1
> show running-config router ospf
router ospf 1
 network 169.254.255.2 255.255.255.255 area 1
 network 169.254.255.3 255.255.255.255 area 1
 network [redacted].10.0 255.255.255.0 area 1
```



```
firepower# show route
[…]
S*        0.0.0.0 0.0.0.0 [1/0] via [redacted].7.2, ISP-2
                          [1/0] via [redacted].6.2, ISP-1
O         169.254.255.1 255.255.255.255
                [110/1563] via 169.254.255.1, 04:22:27, VTI2
                [110/1563] via 169.254.255.1, 04:22:27, VTI1
O         [redacted].5.0 255.255.255.0 [110/1572] via 169.254.255.1, 04:22:27, VTI2
                                       [110/1572] via 169.254.255.1, 04:22:27, VTI1
[…]
```

Hub Tunnel IP address

Hub Remote network

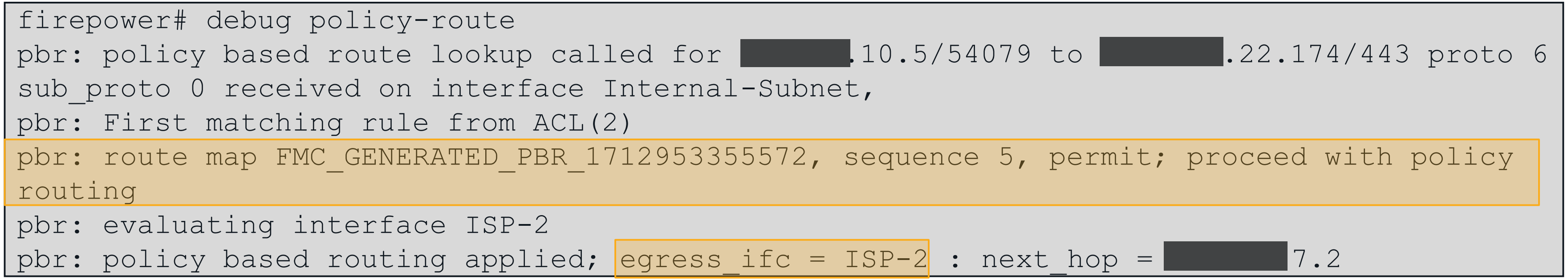
CLI Troubleshooting

TEST 1

In a production environment, debugs may generate a substantial volume of messages. It is advisable to use debug commands exclusively for troubleshooting specific issues and during times of low network traffic. Disable debugging once the troubleshooting is completed.

Client machine sends traffic to Social Media Application

PBR rule applied to Social Media application traffic

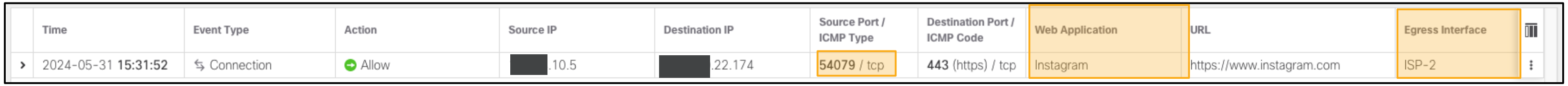


```
firepower# debug policy-route
pbr: policy based route lookup called for [redacted].10.5/54079 to [redacted].22.174/443 proto 6
sub_proto 0 received on interface Internal-Subnet,
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1712953355572, sequence 5, permit; proceed with policy
routing
pbr: evaluating interface ISP-2
pbr: policy based routing applied; egress_ifc = ISP-2 : next_hop = [redacted]7.2
```

FMC Troubleshooting

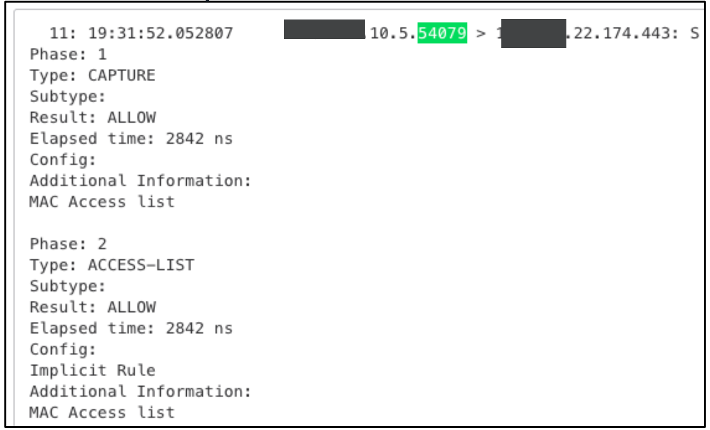
TEST 1

Unified Events:

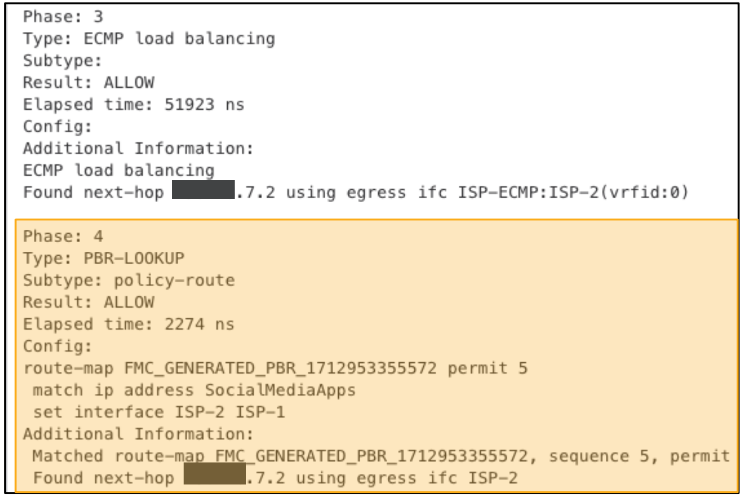


	Time	Event Type	Action	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	URL	Egress Interface
›	2024-05-31 15:31:52	⇆ Connection	● Allow	[redacted].10.5	[redacted].22.174	54079 / tcp	443 (https) / tcp	Instagram	https://www.instagram.com	ISP-2

Packet Captures:



```
  11: 19:31:52.052807       [redacted]10.5.54079 > [redacted].22.174.443: S
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 2842 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 2842 ns
Config:
Implicit Rule
Additional Information:
MAC Access list
```



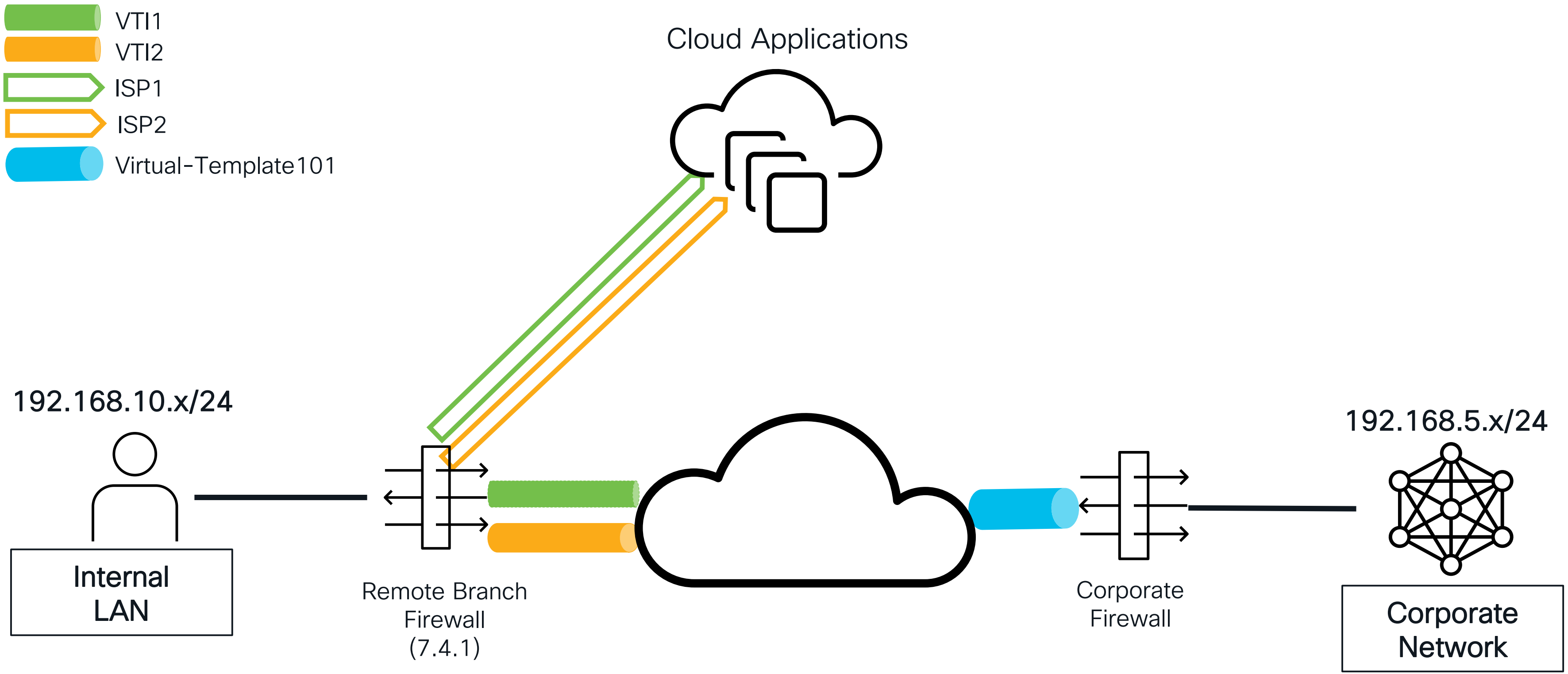
```
Phase: 3
Type: ECMP load balancing
Subtype:
Result: ALLOW
Elapsed time: 51923 ns
Config:
Additional Information:
ECMP load balancing
Found next-hop [redacted].7.2 using egress ifc ISP-ECMP:ISP-2(vrfid:0)

Phase: 4
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 2274 ns
Config:
route-map FMC_GENERATED_PBR_1712953355572 permit 5
 match ip address SocialMediaApps
 set interface ISP-2 ISP-1
Additional Information:
 Matched route-map FMC_GENERATED_PBR_1712953355572, sequence 5, permit
 Found next-hop [redacted].7.2 using egress ifc ISP-2
```

Demo 2: PBR with HTTP Path Monitoring

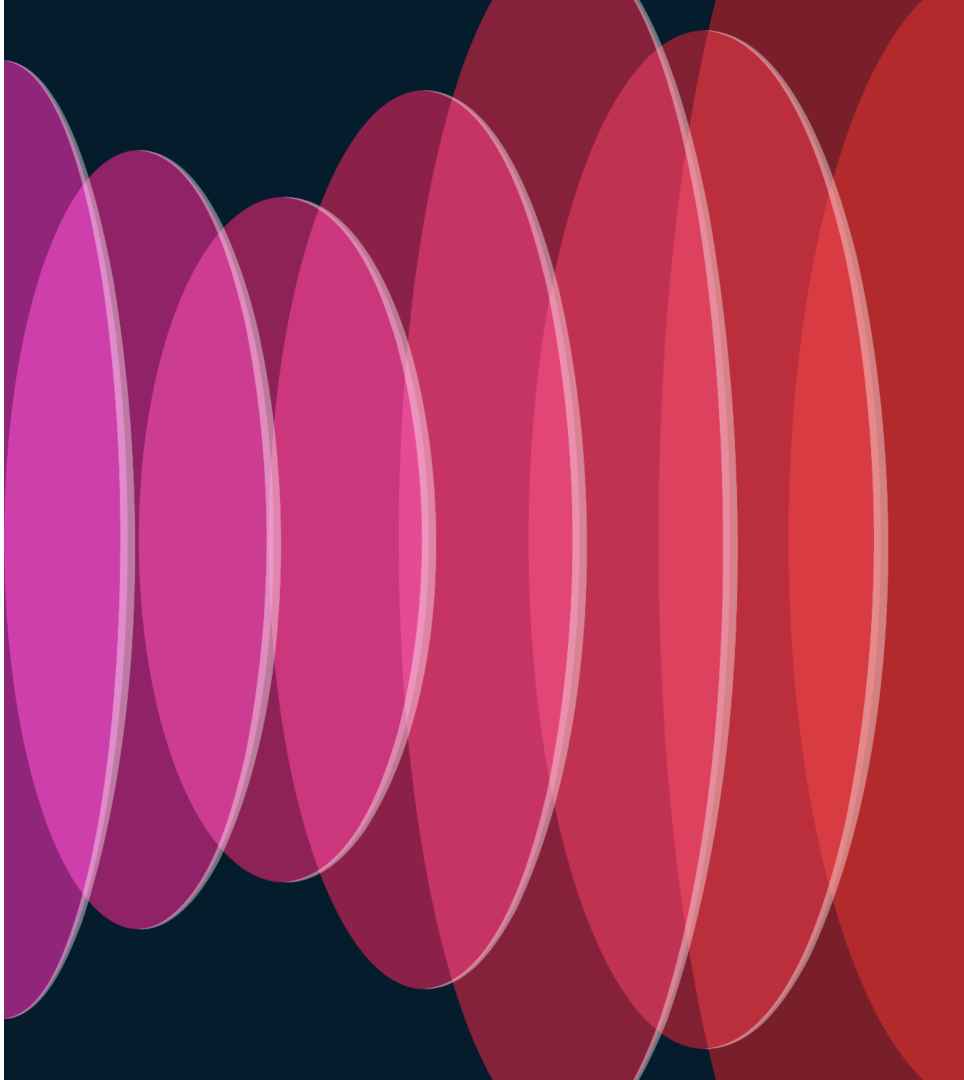
In this Demo we will…

- Configure Interface Path Monitoring
- Configure PBR with flexible metric ‘Jitter’ to steer Video Streaming traffic based on the link with Minimum Jitter

Demo 2 Topology

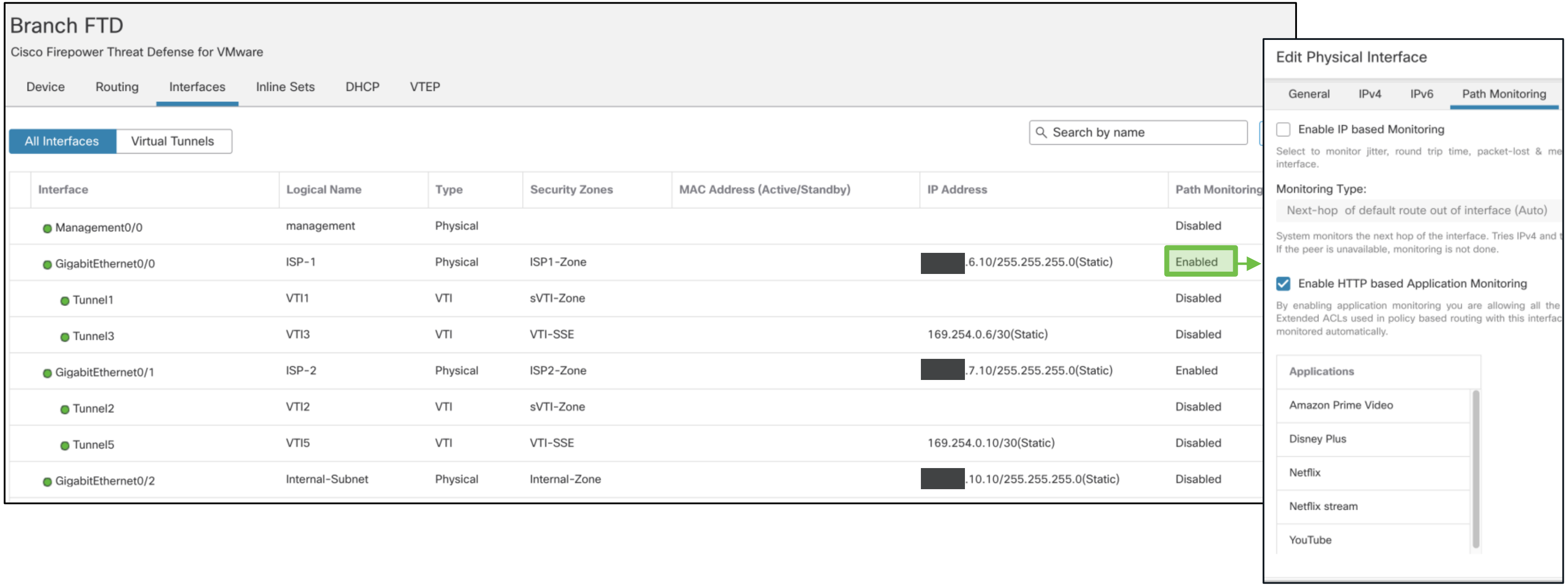


Remote Branch Firewall Configuration



Interface Configuration

- Devices > Interfaces



Branch FTD

Cisco Firepower Threat Defense for VMware

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring
● Management0/0	management	Physical				Disabled
● GigabitEthernet0/0	ISP-1	Physical	ISP1-Zone		[redacted].6.10/255.255.255.0(Static)	Enabled
● Tunnel1	VTI1	VTI	sVTI-Zone			Disabled
● Tunnel3	VTI3	VTI	VTI-SSE		169.254.0.6/30(Static)	Disabled
● GigabitEthernet0/1	ISP-2	Physical	ISP2-Zone		[redacted].7.10/255.255.255.0(Static)	Enabled
● Tunnel2	VTI2	VTI	sVTI-Zone			Disabled
● Tunnel5	VTI5	VTI	VTI-SSE		169.254.0.10/30(Static)	Disabled
● GigabitEthernet0/2	Internal-Subnet	Physical	Internal-Zone		[redacted].10.10/255.255.255.0(Static)	Disabled

Edit Physical Interface

□ Enable IP based Monitoring

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

Monitoring Type:

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

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

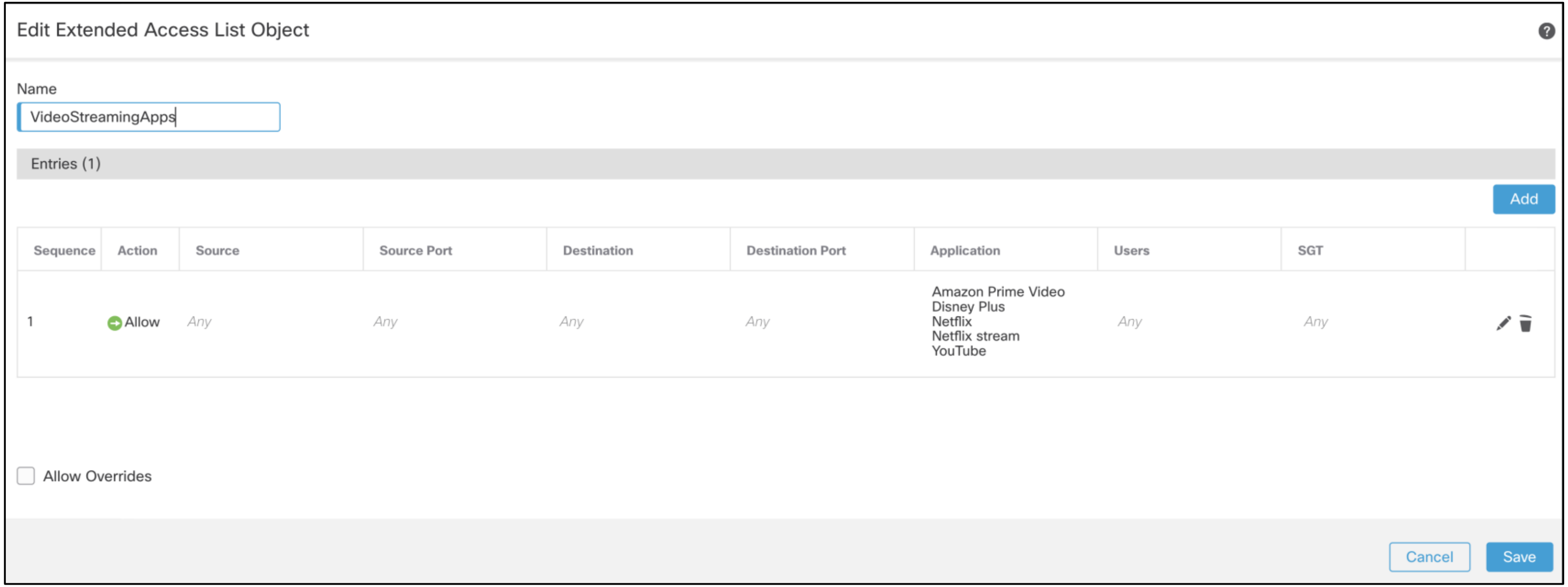
☑ Enable HTTP based Application Monitoring

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

Applications
Amazon Prime Video
Disney Plus
Netflix
Netflix stream
YouTube

Extended Access-List Configuration

- Objects > Object Management > Access-List > Extended



Edit Extended Access List Object

Name

VideoStreamingApps

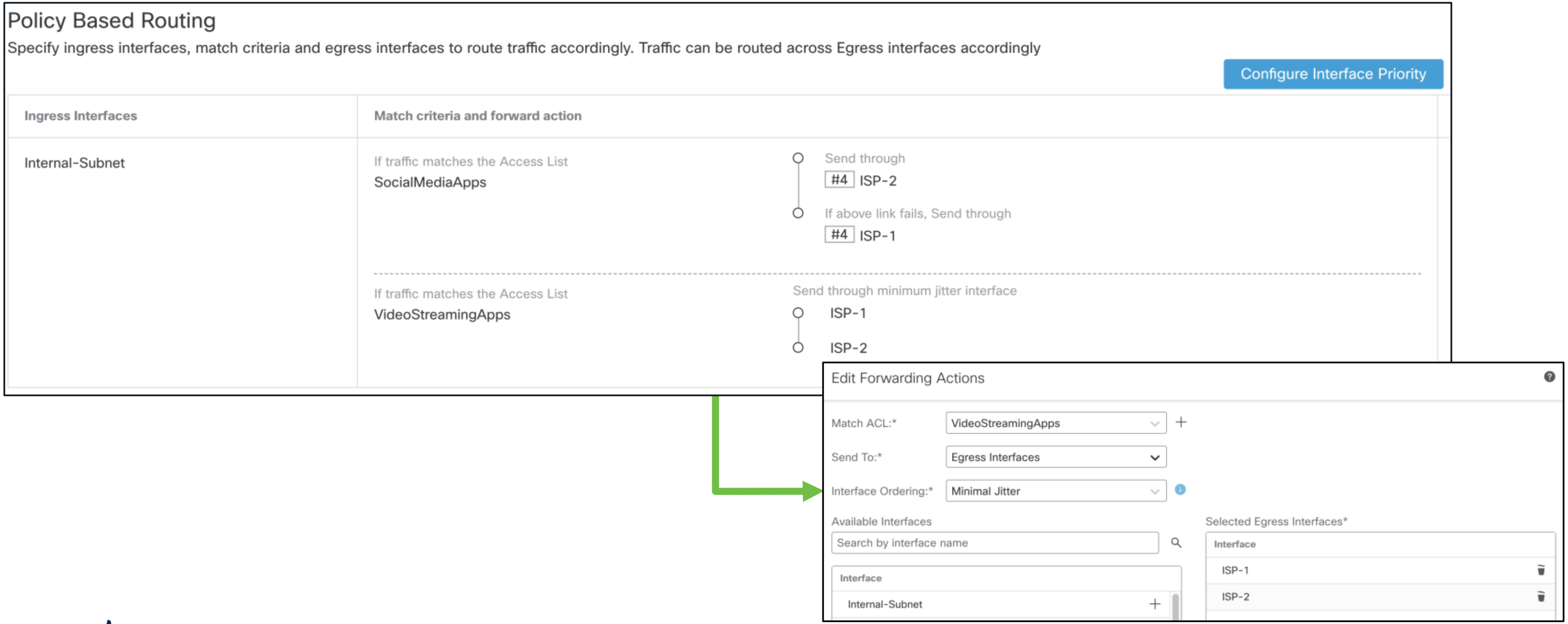
Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	Any	Any	Any	Any	Amazon Prime Video Disney Plus Netflix Netflix stream YouTube	Any	Any	

□ Allow Overrides

Policy Based Routing

- Devices > Routing > Policy Based Routing



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

Ingress Interfaces	Match criteria and forward action	
Internal-Subnet	If traffic matches the Access List SocialMediaApps	○ Send through #4 ISP-2 ○ If above link fails, Send through #4 ISP-1
	If traffic matches the Access List VideoStreamingApps	Send through minimum jitter interface ○ ISP-1 ○ ISP-2

Edit Forwarding Actions

Match ACL:* VideoStreamingApps

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter

Available Interfaces

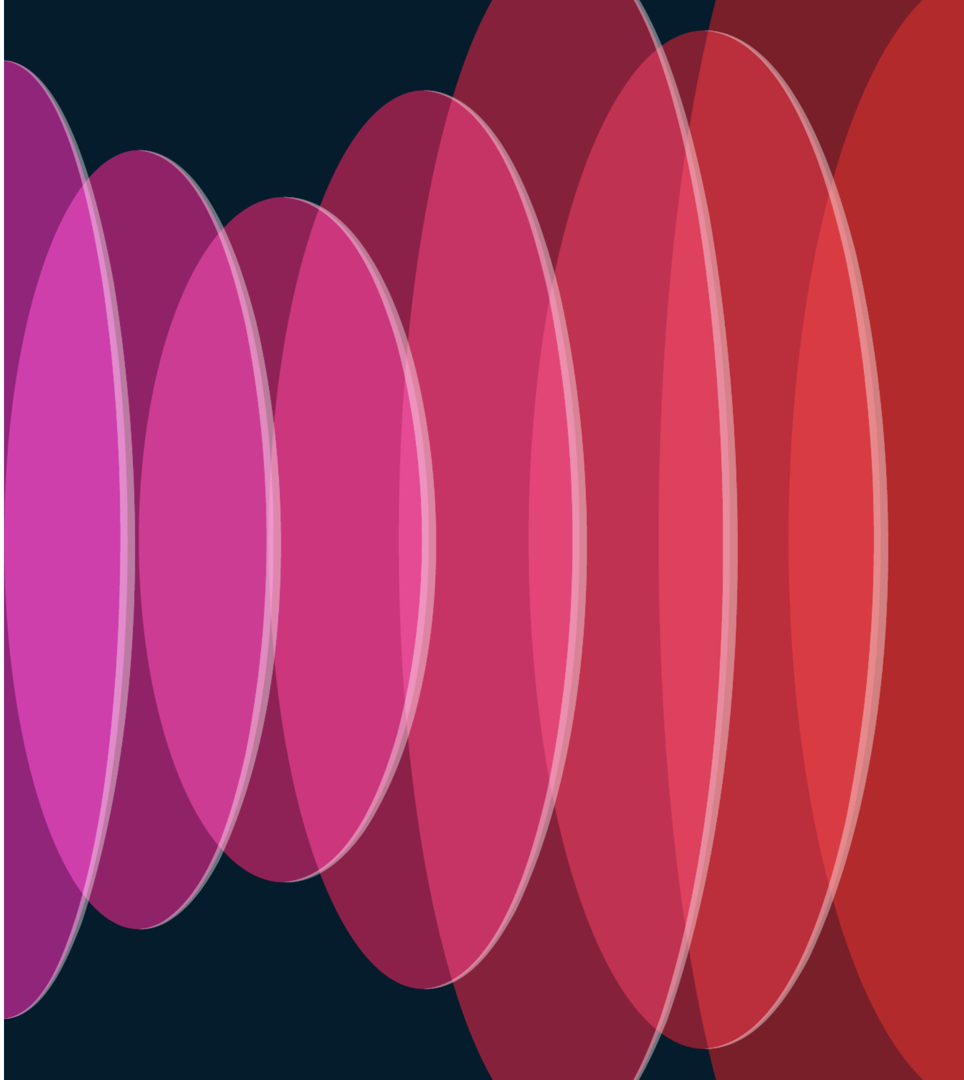
Search by interface name

Interface
Internal-Subnet

Selected Egress Interfaces*

Interface
ISP-1
ISP-2

Verification and Troubleshooting



Verification Commands

Route-Map configuration:

To show the route-map configuration:

```
Branch-FTD# show running-config route-map

route-map FMC_GENERATED_PBR_1712953355572 permit 5
 match ip address SocialMediaApps
 set interface ISP-2 ISP-1
route-map FMC_GENERATED_PBR_1712953355572 permit 10
 match ip address VideoStreamingApps
 set adaptive-interface jitter ISP-1 ISP-2
```

To show the access lists associated with the PBR:

```
Branch-FTD# show runn access-list SocialMediaApps
access-list SocialMediaApps extended permit ip any object-group-network-service FMC_NSG_47244673306

Branch-FTD# show runn access-list VideoStreamingApps
access-list VideoStreamingApps extended permit ip any object-group-network-service FMC_NSG_47244673325
```

CLI Troubleshooting

TEST 2

In a production environment, debugs may generate a substantial volume of messages. It is advisable to use debug commands exclusively for troubleshooting specific issues and during times of low network traffic. Disable debugging once the troubleshooting is completed.

- Client machine navigates to a Video Streaming Application
- PBR rule applied to Video Streaming Application traffic

```
pbr: policy based route lookup called for [redacted].10.5/56423 to [redacted].189.238/443
proto 6 sub_proto 0 received on interface Internal-Subnet,
pbr: First matching rule from ACL(4)
pbr: route map FMC_GENERATED_PBR_1712953355572, sequence 10, permit; proceed with policy
routing
pbr: Ingress ifc Internal-Subnet, PBR adaptive traffic forward for dest [redacted].189.238,
egress-ifc ISP-2 nh [redacted].7.2
pbr: policy based routing applied; egress_ifc = ISP-2 : next_hop = [redacted].7.2
```

Verification Commands

TEST 2

To show Interface metrics:

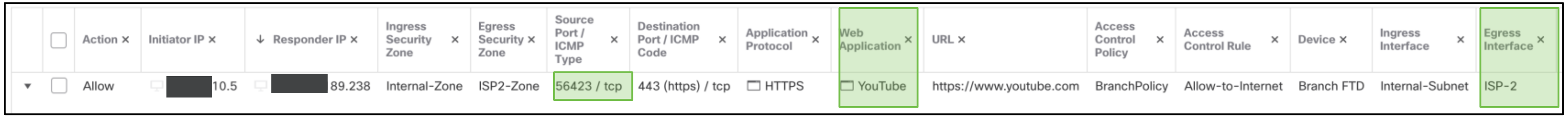
```
firepower# show path-monitoring
Interface: ISP1 (GigabitEthernet0/0)
Remote NSG: FMC_NSG_47244673325
 Network Service: YouTube
    Domain name: youtube.com
    Remote peer reachable: Yes
    RTT average: 27333 microsecond(s)
    Jitter: 12625 microsecond(s)
    Packet loss: 0%
    MOS: 4.37
    Last updated: 6 second(s) ago

Network Service: YouTube
    Domain name: googlevideo.com
    Remote peer reachable: Yes
    RTT average: 82812 microsecond(s)
    Jitter: 713 microsecond(s)
    Packet loss: 0%
    MOS: 4.35
    Last updated: 26 second(s) ago
```

```
Interface: ISP2 (GigabitEthernet0/1)
Remote NSG: FMC_NSG_47244673325
 Network Service: YouTube
    Domain name: youtube.com
    Remote peer reachable: Yes
    RTT average: 24006 microsecond(s)
    Jitter: 570 microsecond(s)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 6 second(s) ago

 Network Service: YouTube
    Domain name: googlevideo.com
    Remote peer reachable: Yes
    RTT average: 82770 microsecond(s)
    Jitter: 756 microsecond(s)
    Packet loss: 0%
    MOS: 4.35
    Last updated: 26 second(s) ago
```

FMC Troubleshooting

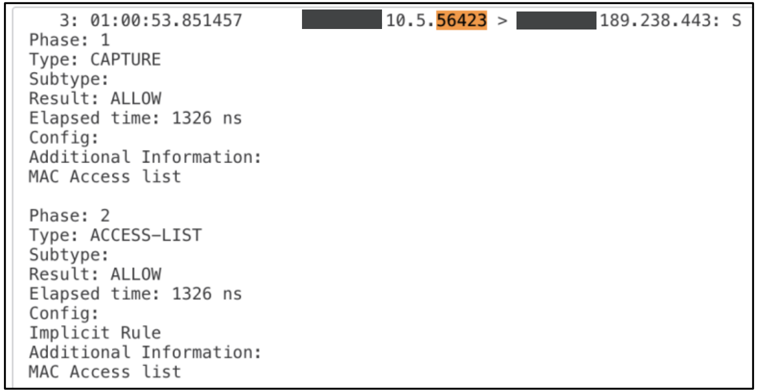
TEST 2

Connection Events:

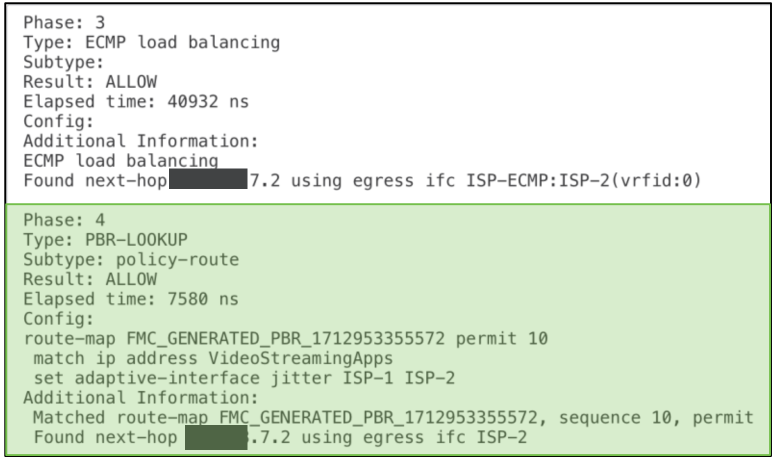


	☐	Action ×	Initiator IP ×	↓ Responder IP ×	Ingress Security Zone ×	Egress Security Zone ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	Application Protocol ×	Web Application ×	URL ×	Access Control Policy ×	Access Control Rule ×	Device ×	Ingress Interface ×	Egress Interface ×
▾	☐	Allow	[redacted]10.5	[redacted]89.238	Internal-Zone	ISP2-Zone	56423 / tcp	443 (https) / tcp	HTTPS	YouTube	https://www.youtube.com	BranchPolicy	Allow-to-Internet	Branch FTD	Internal-Subnet	ISP-2

Packet Captures:



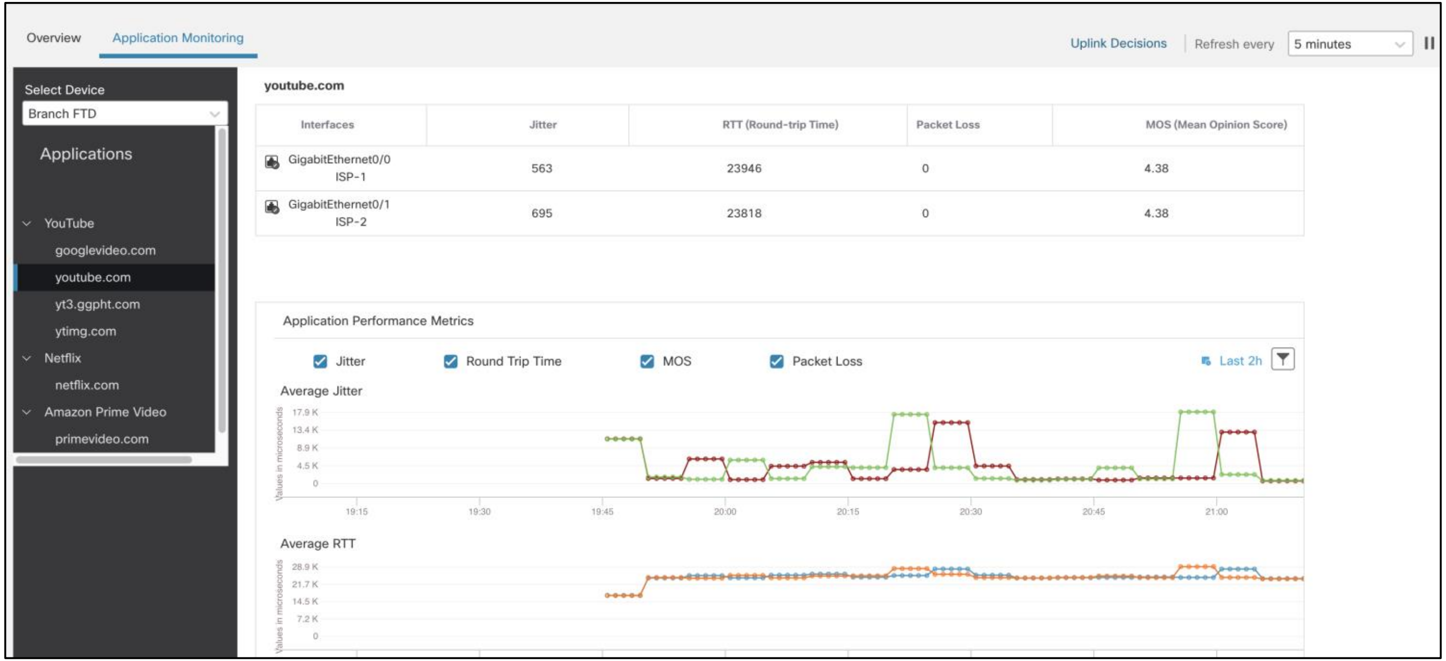
```
   3: 01:00:53.851457       [redacted]10.5.56423 > [redacted]189.238.443: S
 Phase: 1
 Type: CAPTURE
 Subtype:
 Result: ALLOW
 Elapsed time: 1326 ns
 Config:
 Additional Information:
 MAC Access list

 Phase: 2
 Type: ACCESS-LIST
 Subtype:
 Result: ALLOW
 Elapsed time: 1326 ns
 Config:
 Implicit Rule
 Additional Information:
 MAC Access list
```



```
Phase: 3
Type: ECMP load balancing
Subtype:
Result: ALLOW
Elapsed time: 40932 ns
Config:
Additional Information:
ECMP load balancing
Found next-hop [redacted]7.2 using egress ifc ISP-ECMP:ISP-2(vrfid:0)

Phase: 4
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 7580 ns
Config:
route-map FMC_GENERATED_PBR_1712953355572 permit 10
 match ip address VideoStreamingApps
 set adaptive-interface jitter ISP-1 ISP-2
Additional Information:
 Matched route-map FMC_GENERATED_PBR_1712953355572, sequence 10, permit
 Found next-hop [redacted].7.2 using egress ifc ISP-2
```

SD-WAN Summary Dashboard

Application Monitoring:



youtube.com

Interfaces	Jitter	RTT (Round-trip Time)	Packet Loss	MOS (Mean Opinion Score)
GigabitEthernet0/0 ISP-1	563	23946	0	4.38
GigabitEthernet0/1 ISP-2	695	23818	0	4.38

Conclusion

Some SDWAN Capabilities can be leveraged in the Secure Firewall to simplify branch deployments, optimize network performance, and ensure better user application experience while keeping the network secure.

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

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

Continue your education

- Visit the Cisco Showcase for related demos

- Book your one-on-one Meet the Engineer meeting

- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

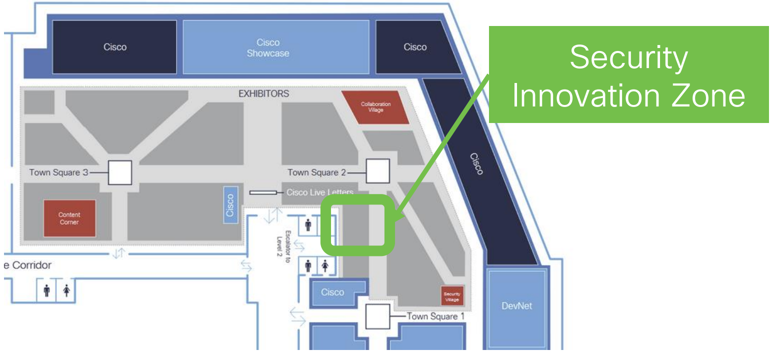
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Continue your education

- Hear Tom Gillis at the Security Deep Dive Keynote KDDSEC-1000!

  Securing User to Application and Everything in Between
  Wednesday, June 5 | 1 – 2pm

- Visit us at the Security Innovation Zone (#4435) for demos and workshops



The bridge to possible

Thank you