
cisco Live!
Let's go

The bridge to possible

Route Based VPNs With Secure Firewall

Jeff Fanelli, Principal Architect
@jefanell

Agenda

- IPSec VPN Solutions & Tunnel Interfaces overview
- Scalable FTD Hub & Spoke WAN Design
- SASE / Security Service Edge integration
- SDWAN Policy Based Routing
- Monitoring & Troubleshooting

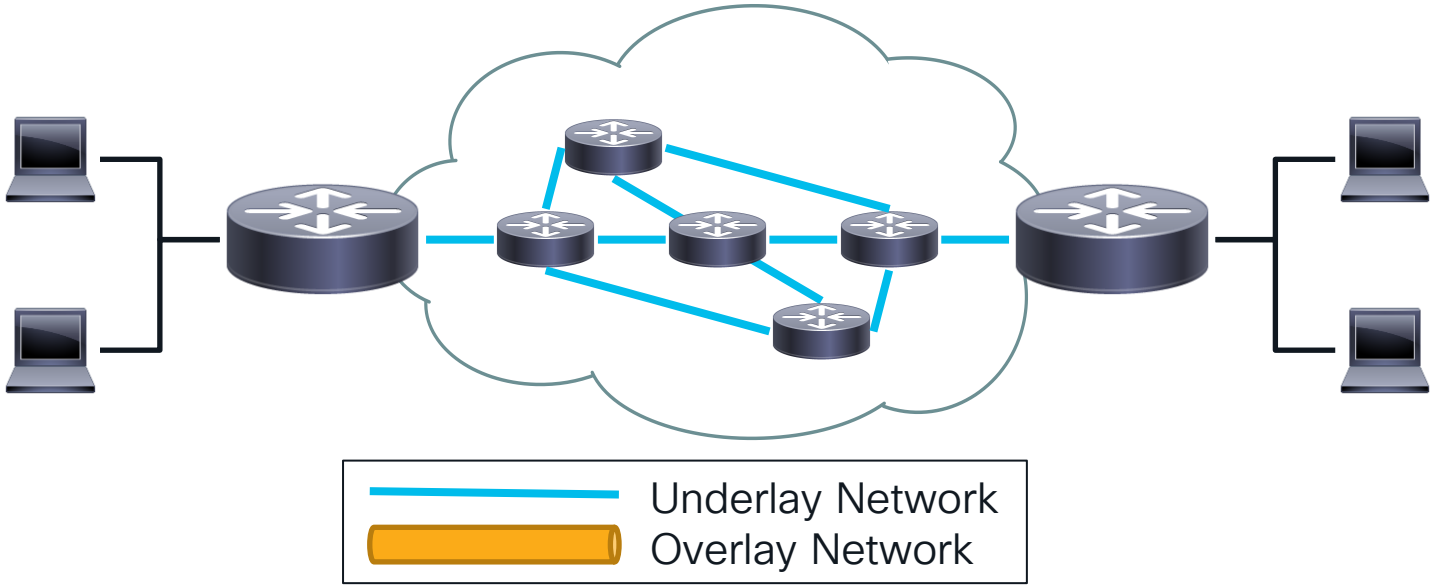
About Me

Jeff Fanelli

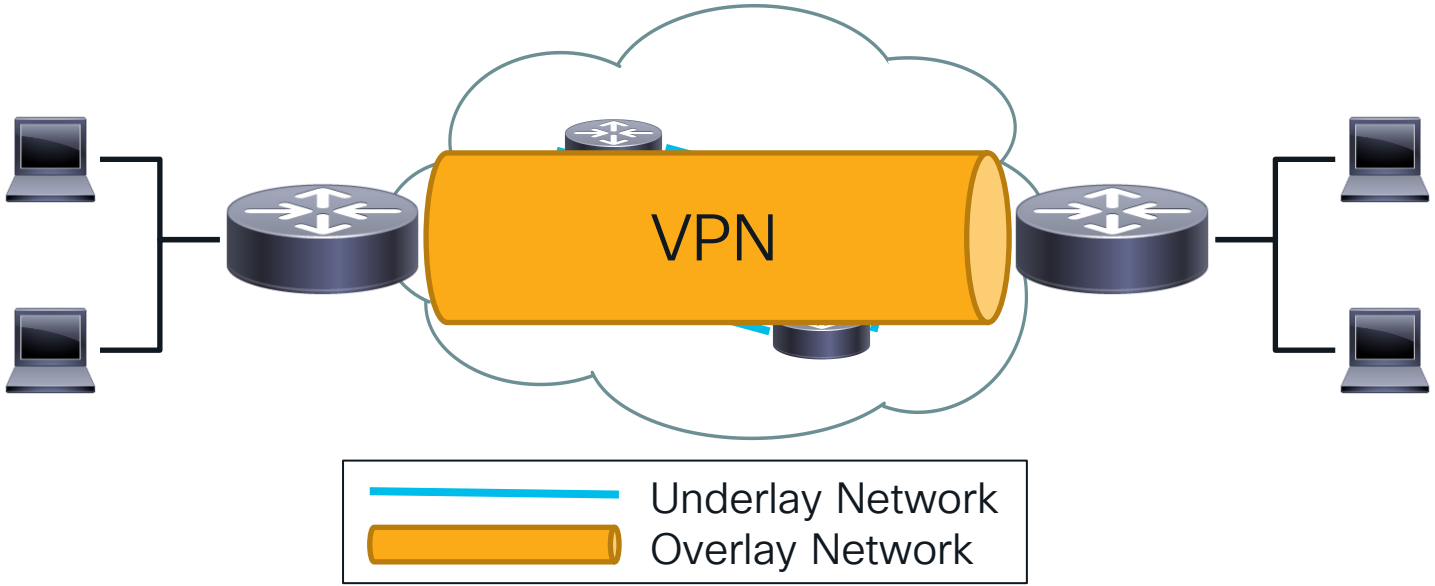
- jefanell@cisco.com
- Principal Architect
- 18 years @ Cisco
- 40+ CiscoLive! Presenter
- Husband + father
- Instrument rated pilot
- Wiener dog servant

VPN Technology Overview

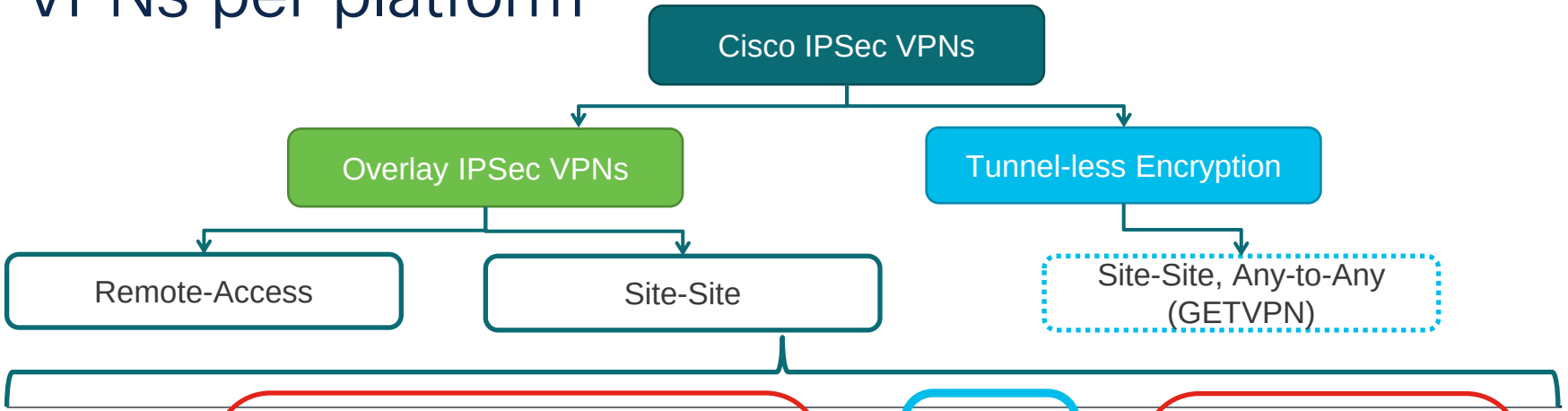
Underlay & Overlay



Underlay & Overlay



VPNs per platform



	Crypto Map	GRE over IPSec w/ Crypto Map	EZVPN	VTI	DMVPN	FlexVPN
IOS/IOS-XE	Yes	Yes	Yes	Yes	Yes	Yes
ASA	Yes	No	Yes	Yes	No	No**
FTD	Yes	No	Yes	Yes	No	No**

Not recommended

Session Focus!

IOS Only

** Limited integration is possible

Crypto Map

Reference

- First implementation of IPSec VPNs used on Cisco devices.
- Traffic to be encrypted is defined by an ACL (crypto ACL).
- Configuration nightmare:
  - Mismatched ACLs
  - ACL update requirements.

```
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set TS
 match address 110
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 crypto map outside_map
```

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2

crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set TS esp-aes esp-sha-hmac
 mode tunnel
!
access-list 110 permit ip 10.20.10.0/24 10.10.10.0/24
access-list 110 permit ip 10.20.10.0/24 10.10.20.0/24
access-list 110 permit ip 10.20.10.0/24 10.10.30.0/24
```

Dynamic Crypto Map

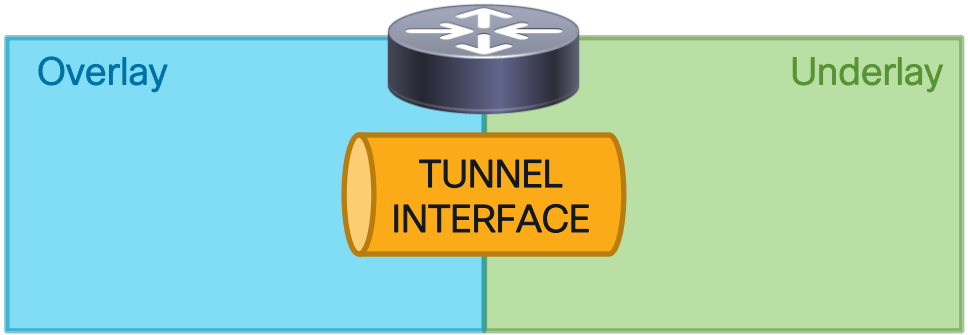
Reference

- Dynamically accepts remote (initiating) peer's IP address.
- Any proposed traffic selector will be accepted from authenticate peer.
- The DVTI technology replaces dynamic crypto maps as a dynamic hub-and-spoke method for establishing tunnels.

```
crypto ipsec transform-set TS esp-aes esp-sha-hmac
 mode tunnel
!
crypto dynamic-map dynamic_map 10
 set transform-set TS
 reverse-route
!
crypto map outside_map 10 ipsec-isakmp dynamic dynamic_map
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 crypto map outside_map
```

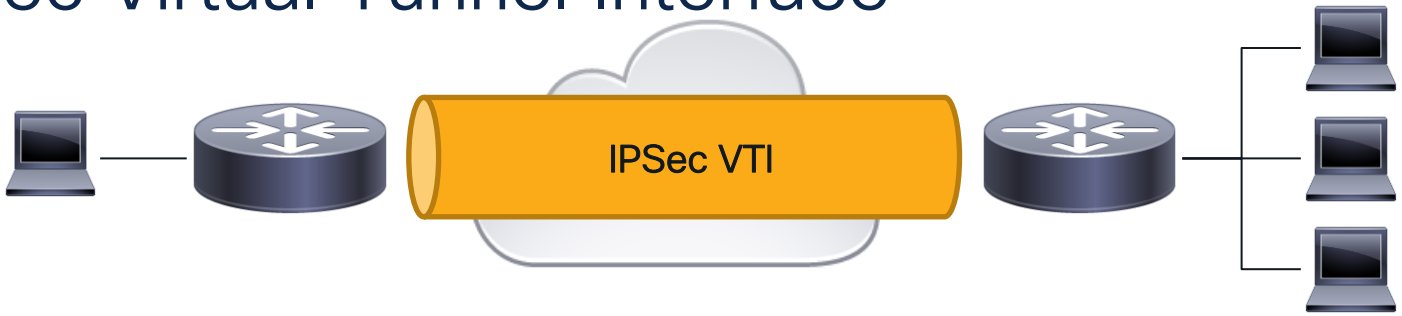
VPN Tunnel Interfaces

Tunnel Interface



- Tunnel Interface interconnects underlay and overlay network.
- Supports various encapsulation types – GRE IPv4/IPv6, Native IPSec IPv4/IPv6
- Main building block for IOS IPSec VPNs – mGRE (DMVPN), Static/Dynamic (FlexVPN) and now ASA / FTD

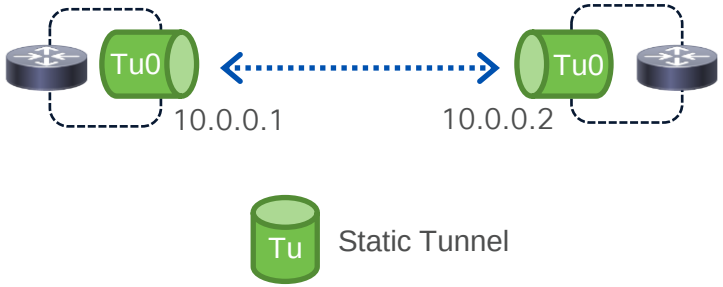
IPSec Virtual Tunnel Interface



- Provides a virtual routable interface for terminating IPsec tunnels.
- Simplifies the configuration of IPsec for protection of remote links
- Supports multicast and simplifies network management (IOS only).
- The VTI tunnel is always up (does not need “interesting traffic”)

IPSec Tunnel Interface Types – Static

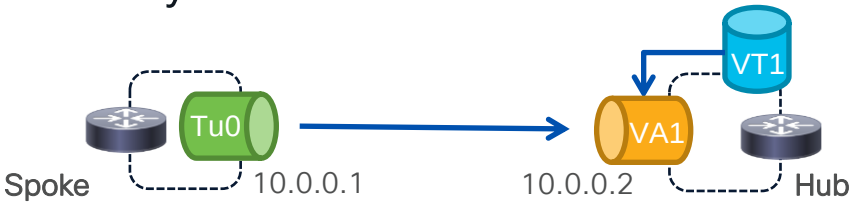
- Static Tunnel Interface

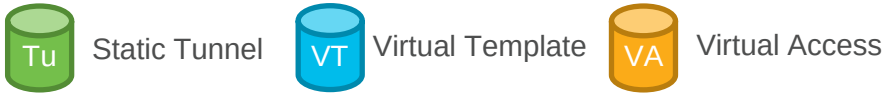



```
interface Tunnel1
 nameif tunnel-to-dc (ASA/FTD only)
 ip unnumbered Loopback1 (ASA 9.19+ FTD 7.3+)
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.2
 tunnel protection ipsec profile default
```

IPSec Tunnel Interface Types – Dynamic

- Dynamic Tunnel Interface





Dynamic Tunnel Interfaces (DVTI) are introduced in ASA 9.19 and FTD 7.3

```
interface Virtual-Template1 type tunnel
 nameif tunnel-to-dc (ASA/FTD only)
 ip unnumbered Loopback1 (ASA 9.19+ FTD 7.3+)
 tunnel source GigabitEthernet2
 tunnel protection ipsec profile default
```

```
interface Virtual-Access1
 ip unnumbered Loopback1
 tunnel source GigabitEthernet2
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile default
 no tunnel protection ipsec initiate
```

Secure Firewall VPN Design

New ASA and FTD capabilities

These features are in ASA and FTD code right NOW:

- Static VTI Tunnels
- BGP routing support
- Per-peer IKEv2 custom identity attributes

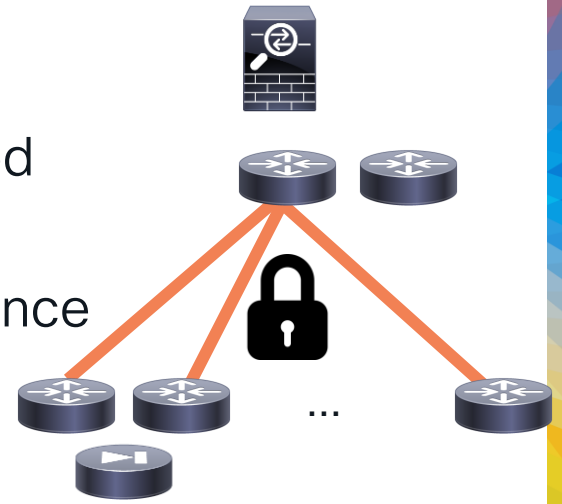
Configs shown will be ASA CLI. (identical to FTD deployed configuration)

New in the ASA 9.19 / FTD 7.3

- Loopback interfaces
- IKEv2 config-exchange for peer interface sharing over tunnel (simplifies BGP peering)
- Dynamic VTI support on ASA/FTD for VPN “hub”. Can also use IOS for VPN hub now.

Example Design Requirements and Assumptions

- Scaled Deployment / hub-and-spoke topology
- Provide security using cryptographically protected tunnels.
- Headend redundancy with 15 seconds convergence
- Branches can include ASA / FTD

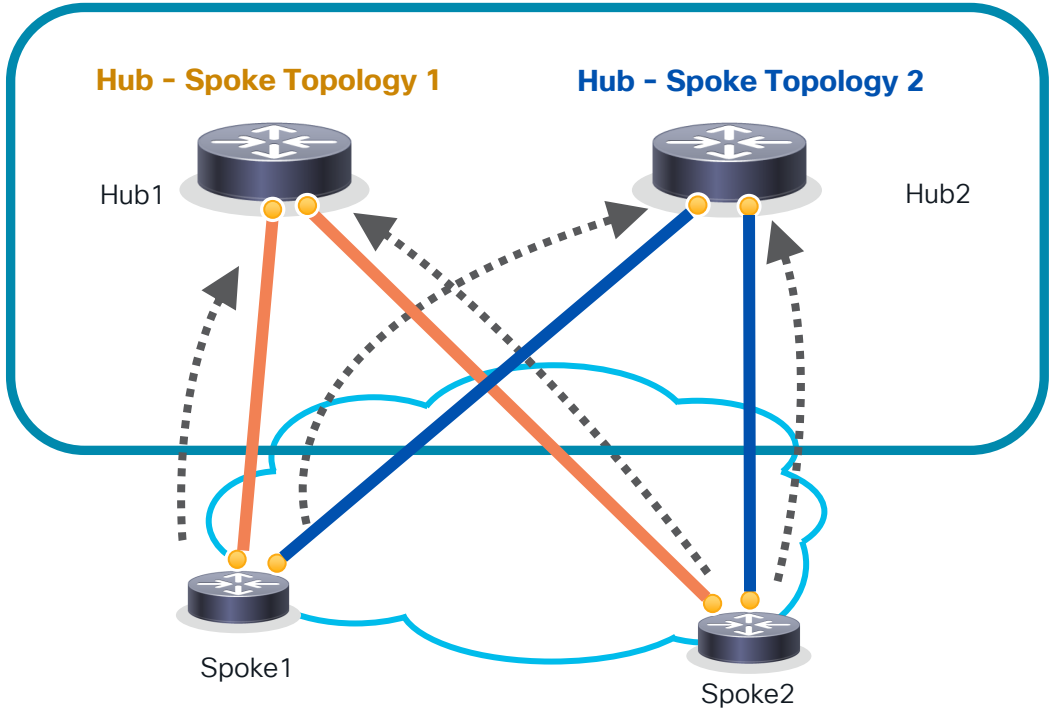


Single / Double Hub & Spoke design using VTI

Hubs can be IOS, ASA 9.19+ or FTD 7.3+

For Secure Firewall Hubs:

- Use separate VPN topology configuration for each VPN Hub
- Backup hub can be configured for each topology
- 1024 maximum spokes per hub
- Routing protocol required



Let's talk about BGP!

Highly recommended!
BRKENT-1179
Border Gateway Protocol Fundamentals

Gustavo Sibaja

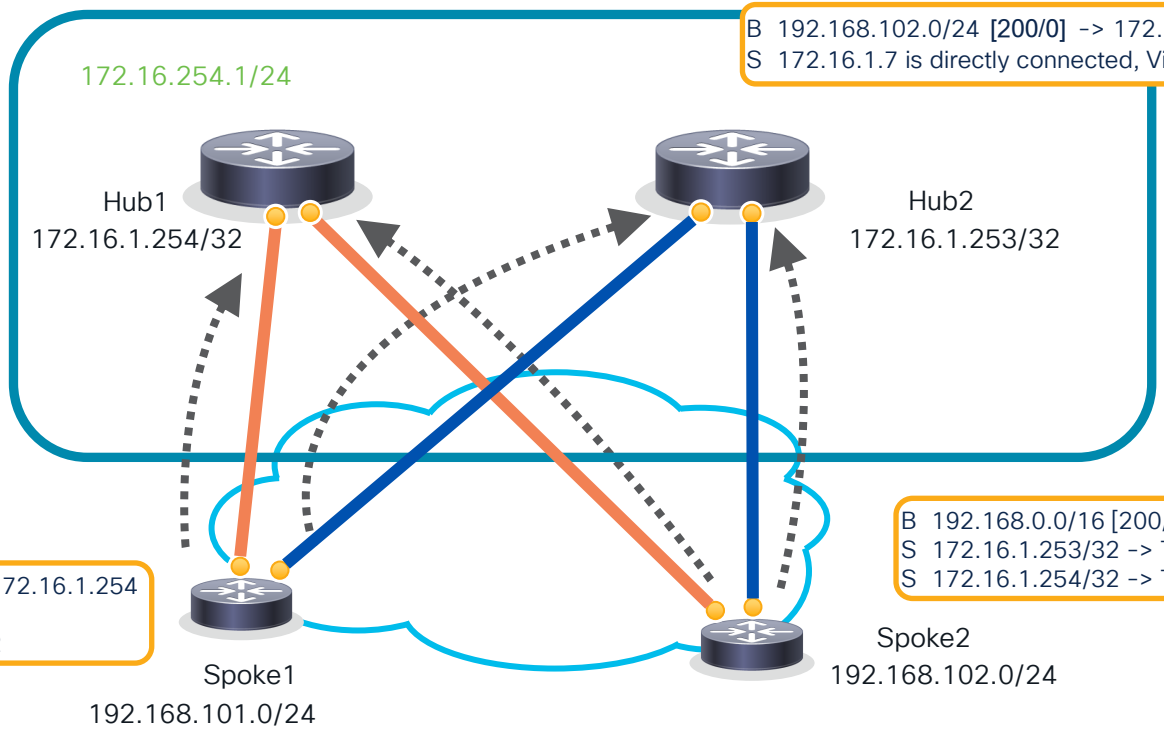
- Border Gateway Protocol
  - Large scale, robust and stable routing protocol designed to operate between autonomous systems
  - Based on TCP, listens on port 179
  - Fundamentally a distance vector protocol
  - Does not have the concept of a simple metric
  - Instead, uses multiple characteristics called attributes
  - Allows for strong control over advertised routes and their attributes
  - Assumes that the routing inside the autonomous system is already fully taken care of by an IGP (EIGRP, OSPF, IS-IS)

Single / Double Hub & Spoke design using VTI

Hubs can be IOS, ASA 9.19+ or FTD 7.3+

```
interface Virtual-Access1
 ip unnumbered Loopback0
tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile default
 no tunnel protection ipsec initiate
```

(only Hub 1 config shown)




```
B  192.168.102.0/24 [200/0] -> 172.16.1.7
S  172.16.1.7 is directly connected, Virtual-Access1
```

```
B  192.168.0.0/16 [200/0] -> 172.16.1.254
S  172.16.1.254/32 -> Tunnel1
S  172.16.1.253/32 -> Tunnel2
```

```
B  192.168.0.0/16 [200/0] -> 172.16.1.253
S  172.16.1.253/32 -> Tunnel1
S  172.16.1.254/32 -> Tunnel2
```

Spoke ASA config – Pre ASA 9.19.1 / FTD 7.3

```
hostname Spoke2
domain-name Spoke2
!
crypto isakmp identity hostname
!
```

IKE Identity

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha384
 group 19
 prf sha384
crypto ikev2 enable outside
!
crypto ipsec ikev2 ipsec-proposal IPSEC_PROP
 protocol esp encryption aes
 protocol esp integrity sha-1
!
crypto ipsec profile VTI
 set ikev2 ipsec-proposal IPSEC_PROP
!
```

IKEv2 and IPSec algorithms

pre-shared-keys

```
tunnel-group 10.0.0.253 type ipsec-l2l
tunnel-group 10.0.0.253 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
tunnel-group 10.0.0.254 type ipsec-l2l
tunnel-group 10.0.0.254 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

```
interface Tunnel1
 nameif VTI
 ip address 172.16.1.5 255.255.255.254
 tunnel source interface outside
 tunnel destination 10.0.0.253
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
!
```

Primary Tunnel

```
interface Tunnel2
 nameif VTI2
 ip address 172.16.1.7 255.255.255.254
 tunnel source interface outside
 tunnel destination 10.0.0.254
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
!
```

Secondary Tunnel

```
route VTI 172.16.1.253 255.255.255.255 172.16.1.253 1
route VTI2 172.16.1.254 255.255.255.255 172.16.1.254 1
!
router bgp 65000
 timers bgp 5 15 0
 address-family ipv4 unicast
  neighbor 172.16.1.253 remote-as 65000
  neighbor 172.16.1.253 activate
  neighbor 172.16.1.254 remote-as 65000
  neighbor 172.16.1.254 activate
  redistribute connected
```

Instead of IKEv2 routing

Spoke ASA config – ASA 9.19.1+ / FTD 7.3+

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha384
 group 19
 prf sha384
crypto ikev2 enable outside
!
crypto ipsec ikev2 ipsec-proposal IPSEC_PROP
 protocol esp encryption aes
 protocol esp integrity sha-1
!
crypto ipsec profile VTI
 set ikev2 ipsec-proposal IPSEC_PROP
!
tunnel-group 10.0.0.253 type ipsec-l2l
tunnel-group 10.0.0.253 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
 ikev2 route set interface
!
tunnel-group 10.0.0.254 type ipsec-l2l
tunnel-group 10.0.0.254 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
 ikev2 route set interface
```

No change to IKE identity, IKEv2, IPSec algorithms

IKEv2 Route learning

```
interface Tunnel1
 nameif VTI
 ip address 172.16.1.5 255.255.255.254
 tunnel source interface outside
 tunnel destination 10.0.0.253
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
!
interface Tunnel2
 nameif VTI2
 ip address 172.16.1.7 255.255.255.254
 tunnel source interface outside
 tunnel destination 10.0.0.254
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
!
~~route VTI 172.16.1.253 255.255.255.255 172.16.1.253 1~~
~~route VTI2 172.16.1.254 255.255.255.255 172.16.1.254 1~~
!
router bgp 65000
 timers bgp 5 15 0
 address-family ipv4 unicast
  neighbor 172.16.1.253 remote-as
  neighbor 172.16.1.253 activate
  neighbor 172.16.1.254 remote-as 65000
  neighbor 172.16.1.254 activate
  redistribute connected
```

Primary Tunnel

Secondary Tunnel

Static VTI routes no longer needed with IKE2 route learning

Spoke config using Loopback – ASA 9.19.1+ / FTD 7.3+

Loopback support including /32 masks

"ip unnumbered" support on tunnel interfaces

```
interface Loopback1
 nameif loop1
 ip address 172.16.1.5 255.255.255.255
!
interface Loopback2
 nameif loop2
 ip address 172.16.1.7 255.255.255.255
!
tunnel-group 10.0.0.253 type ipsec-l2l
tunnel-group 10.0.0.253 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
 ikev2 route set interface
!
tunnel-group 10.0.0.254 type ipsec-l2l
tunnel-group 10.0.0.254 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
 ikev2 route set interface
```

IKEv2 Route learning

Primary Tunnel

```
interface Tunnel1
 nameif VTI
 ip unnumbered loop1
 tunnel source interface outside
 tunnel destination 10.0.0.253
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
!
```

Secondary Tunnel

```
interface Tunnel2
 nameif VTI2
 ip unnumbered loop2
 tunnel source interface outside
 tunnel destination 10.0.0.254
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
!
router bgp 65000
 timers bgp 5 15 0
 address-family ipv4 unicast
  neighbor 172.16.1.253 remote-as 65000
  neighbor 172.16.1.253 activate
  neighbor 172.16.1.254 remote-as 65000
  neighbor 172.16.1.254 activate
  redistribute connected
```

Hub ASA / FTD configuration

```
interface Loopback101
 nameif lo101
 ip address 172.16.10.1 255.255.255.255
!
interface Virtual-Template101 type tunnel
 nameif dVTI101
 ip unnumbered lo101
 tunnel source interface outside
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC_PROFILE
```

New loopback support supporting /32 mask and Virtual-Template (DVTI) support for “hub” support on ASA/FTD

```
crypto ipsec ikev2 ipsec-proposal AES-256
 protocol esp encryption aes-256
 protocol esp integrity sha-256
crypto ipsec profile IPSEC_PROFILE
 set ikev2 ipsec-proposal AES-256
 set ikev2 local-identity address!
```

Crypto proposals must match..

```
router bgp 65000
 bgp log-neighbor-changes
 timers bgp 5 15 0 !
 address-family ipv4
  redistribute connected
  neighbor 172.16.10.2 remote-as 65000
  neighbor 172.16.10.2 activate
  neighbor 172.16.10.3 remote-as 65000
  neighbor 172.16.10.3 activate
  no auto-summary
  no synchronization exit-address-family
```

iBGP configuration requires neighbor entry for every ASA/FTD/IOS peer (no peer-group support)

```
tunnel-group spoke1 type ipsec-l2l
tunnel-group spoke1 ipsec-attributes
 virtual-template 101
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
 ikev2 route set interface
```

Peer spoke tunnel-group peer name should match what peer is providing via IKEv2 identity

”route set interface” enables hub to learn spoke interface IP via IKEv2 config exchange* (new)

Spoke router configuration – IOS Example

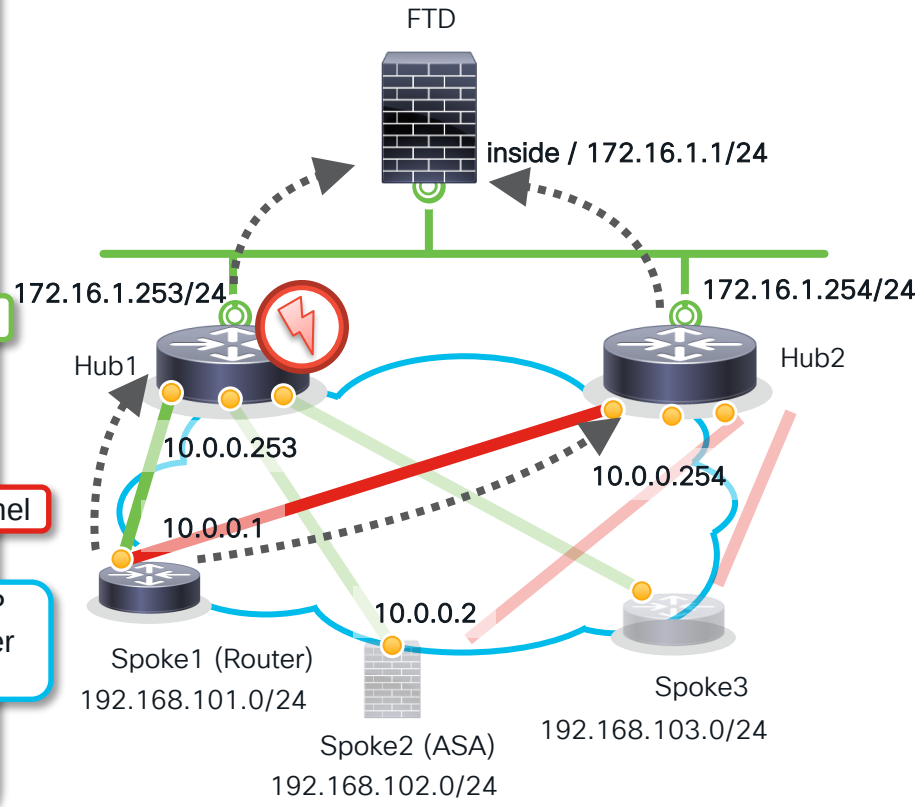
Reference

```
crypto ikev2 profile default
 match identity remote fqdn domain hub
 identity local fqdn Spoke1.router
 authentication local pre-share key <PSK>
 authentication remote pre-share key <PSK>
 aaa authorization group psk list FlexVPN default local
!
interface Tunnel101
 ip unnumbered Loopback101
 tunnel source GigabitEthernet2
 tunnel destination 10.0.0.253
 tunnel protection ipsec profile default
!
interface Tunnel102
 ip unnumbered Loopback101
 tunnel source GigabitEthernet2
 tunnel destination 10.0.0.254
 tunnel protection ipsec profile default
!
router bgp 65000
 timers bgp 5 15
 neighbor 172.16.1.253 remote-as 65000
 neighbor 172.16.1.254 remote-as 65000
!
address-family ipv4
 network 192.168.101.0 mask 255.255.255.0
(…)
```

Primary Tunnel

Secondary Tunnel

Reduced BGP timers for faster convergence



Considerations for different VPN spoke types

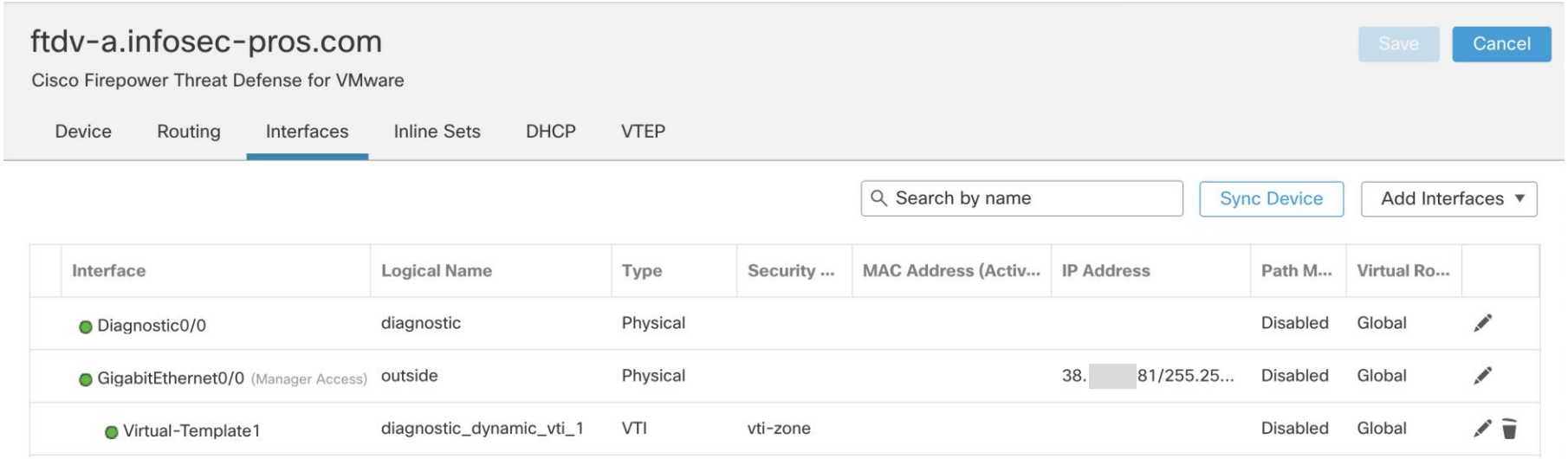
Firewall Management Center will always configure the most specific spoke configuration:

- Static IP address configuration spokes will have spoke specific crypto peer settings configured on hub (with or without NAT IP configured)
- DHCP configured peers will be configured to connect to ”L2L” default tunnel-group
- FMC will redeploy all spokes on any spoke add / change (will be addressed in 7.5). No outage on spoke redeploy.

Secure Firewall VPN Design

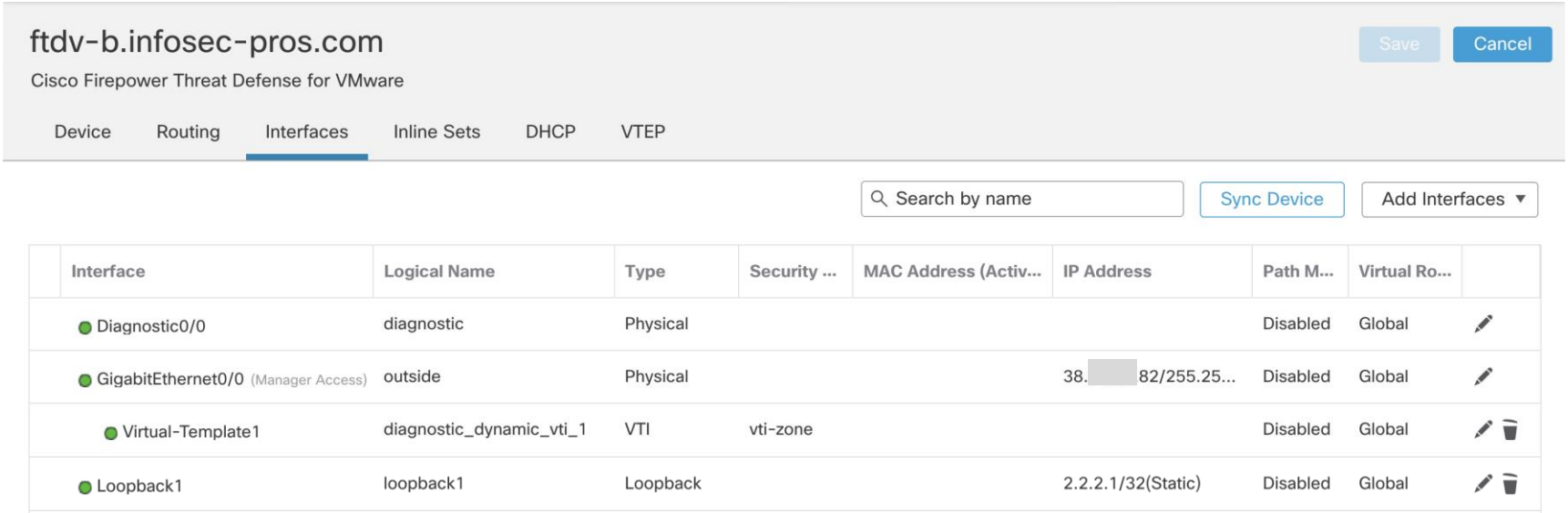
Firewall Management Center GUI

Hub Device Interface Configuration



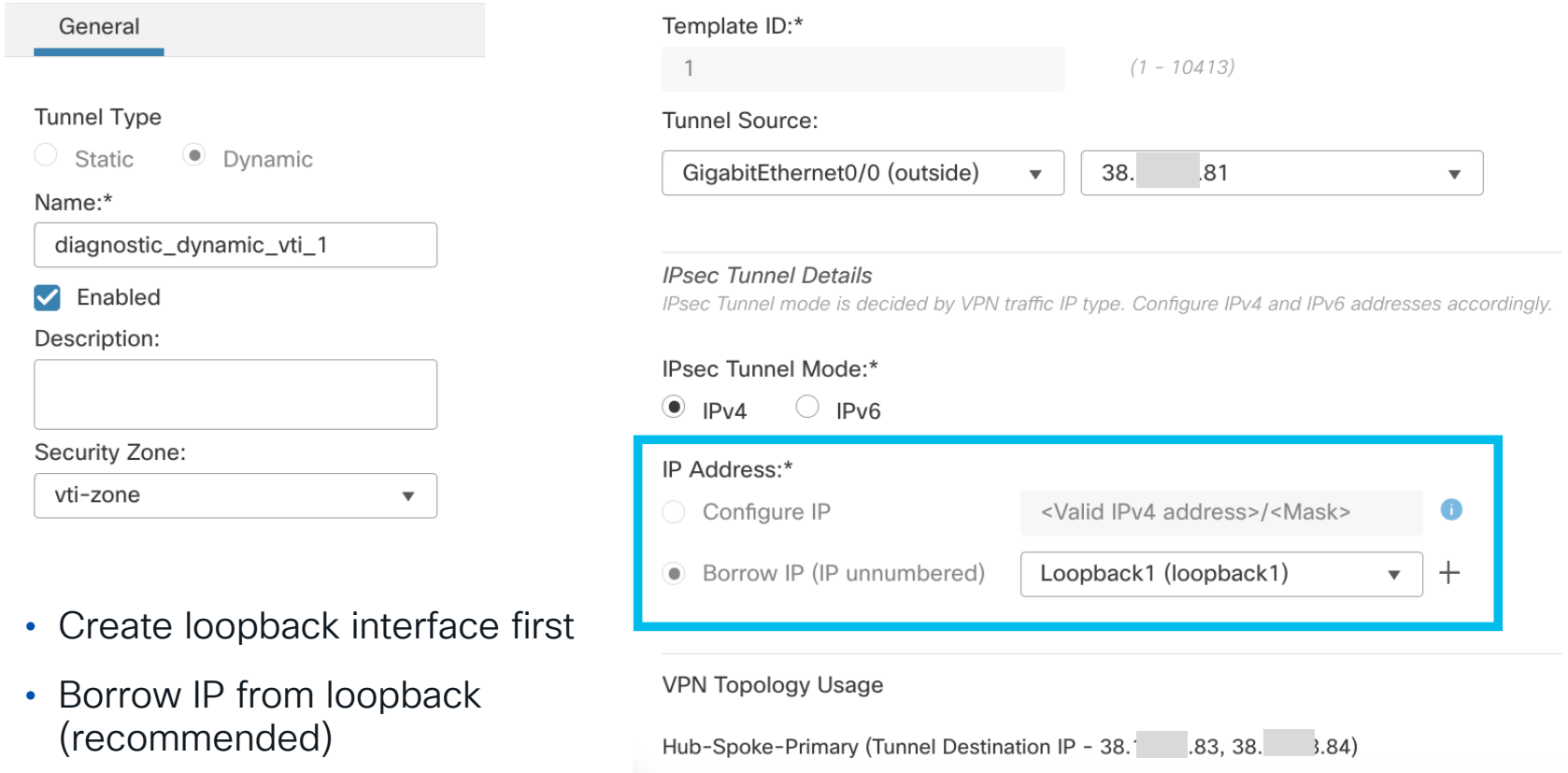
- Hub configuration “Virtual Template” interface is created by VPN Topology configuration
- Virtual Template interface can ”borrow” loopback address (recommended)
- Virtual Template interface is used to create ephemeral VTI interfaces as spokes connect

Spoke Config (with borrowed IP from loopback)



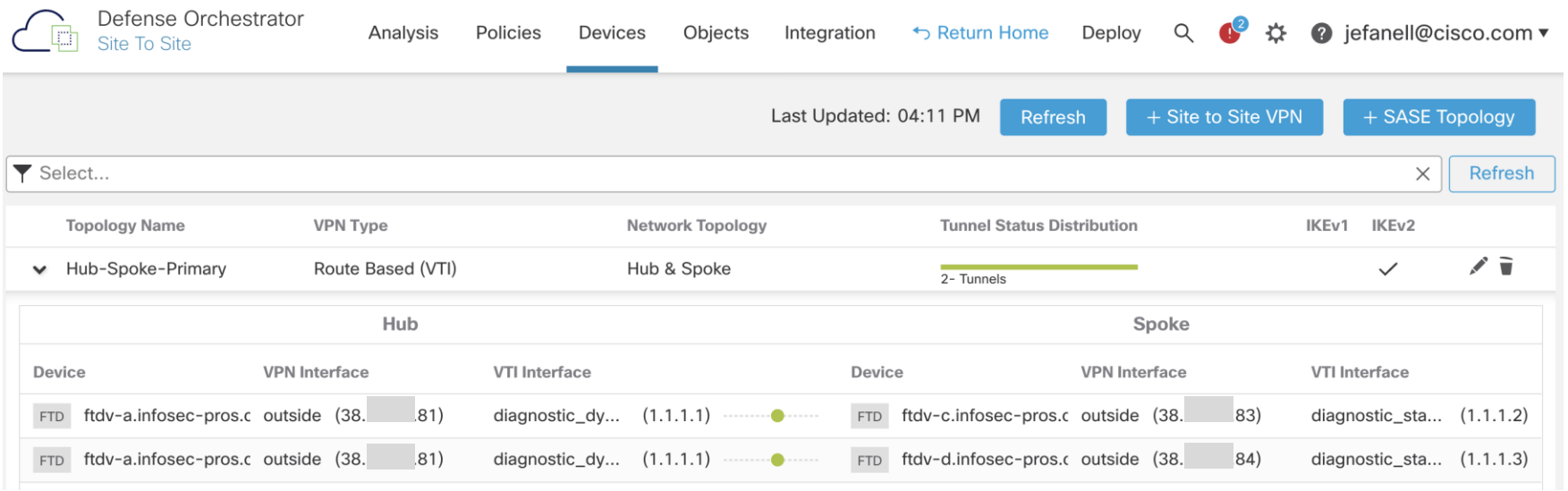
- Create loopback interface first
- SVTI interface configuration for VPN topology can “borrow” this IP address (recommended, requires 7.3)

Hub Virtual-Template Interface Config



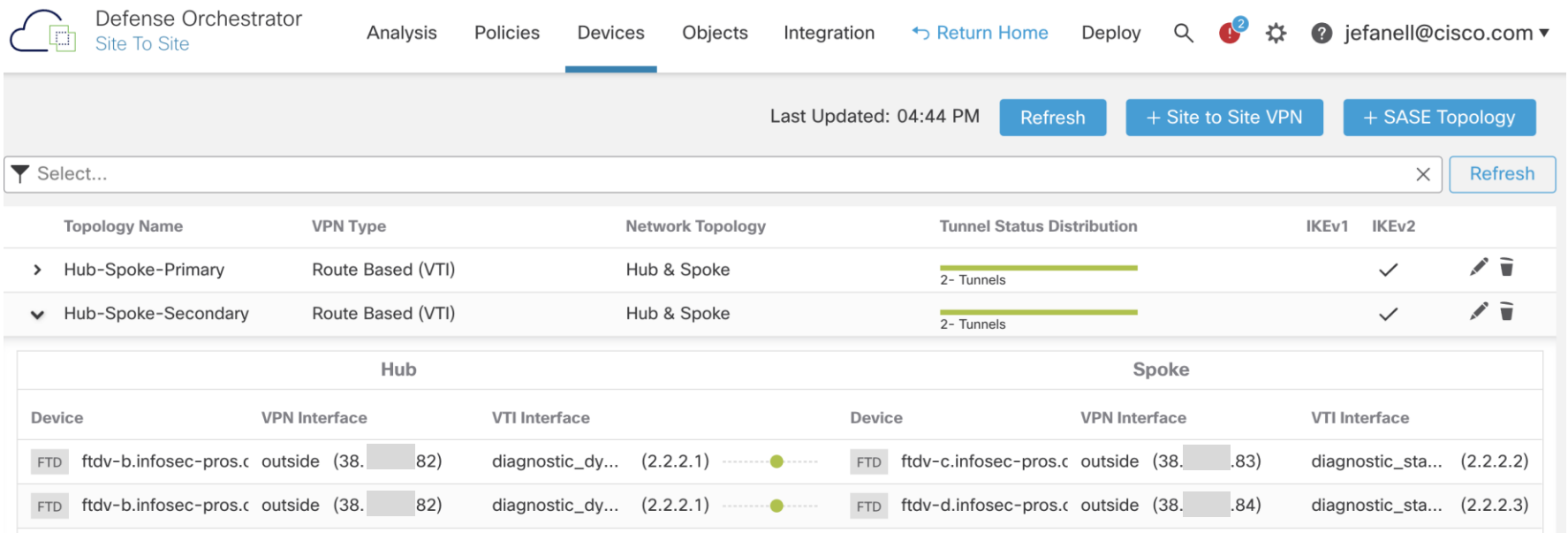
- Create loopback interface first
- Borrow IP from loopback (recommended)

Site to Site VPN Topology with DVTI



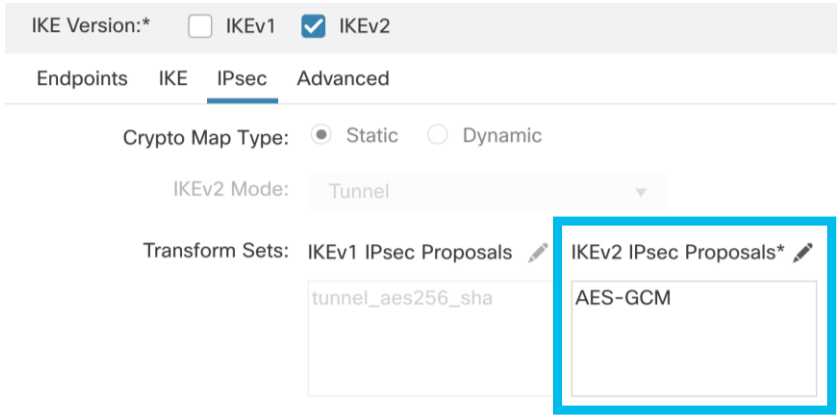
- Unmanaged / external firewalls can be referenced in topologies
- Routing protocol required on member devices to share routes
- Hub and spoke VTI interface routes shared via IKE protocol

Site to Site VPN Dual Topologies



- Same spokes in two separate hub topologies
- eBGP Routing protocol used to prioritize path selection (not shown)

Site to Site VPN Topology




```
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-gcm-256 aes-gcm-192 aes-gcm
 protocol esp integrity null
crypto ipsec profile FMC_IPSEC_PROFILE_1
 set ikev2 ipsec-proposal CSM_IP_1
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
 revocation-check crl none
crypto ikev2 policy 10
 encryption aes-gcm-256 aes-gcm-192 aes-gcm
 integrity null
 group 21 20 19 16 15 14
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
crypto ikev2 enable outside
```

- Default settings for IKEv2 are recommended
- Deployed CLI config viewable from Devices -> Threat Defense CLI
- Use these same settings on ASA platforms for mixed deployments

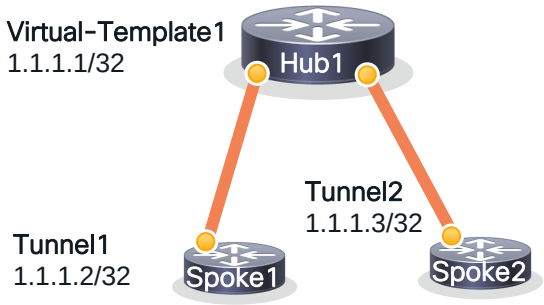
Hub routing table example

Device: ftdv-a.infosec-pros.com

Command: show Parameter: route

Output

```
S*      0.0.0.0 0.0.0.0 [1/0] via 38.    .1, outside
C       1.1.1.1 255.255.255.255 is directly connected, loopback1
V       1.1.1.2 255.255.255.255
          connected by VPN (advertised), diagnostic_dynamic_vti_1_va10
V       1.1.1.3 255.255.255.255
          connected by VPN (advertised), diagnostic_dynamic_vti_1_va9
C       38.     .0 255.255.255.0 is directly connected, outside
L       38.     .81 255.255.255.255 is directly connected, outside
V       192.168.58.0 255.255.255.0
          connected by VPN (advertised), diagnostic_dynamic_vti_1_va10
V       192.168.59.0 255.255.255.0
          connected by VPN (advertised), diagnostic_dynamic_vti_1_va9
```



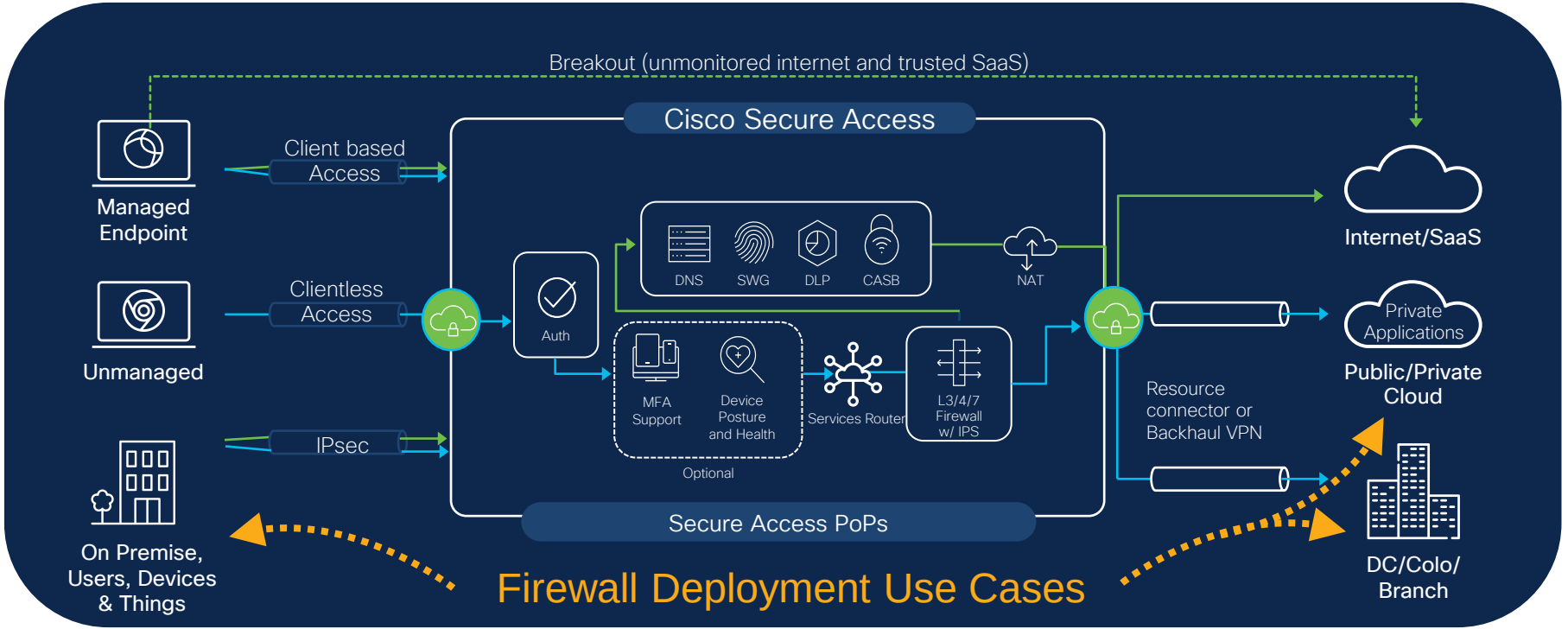
- "V" routes shared by IKEv2 (only VTI interface routes)
- Can "ping" between VTI interfaces for testing
- Branch routes should be shared via routing protocol (BGP etc)

Security Service Edge deployments

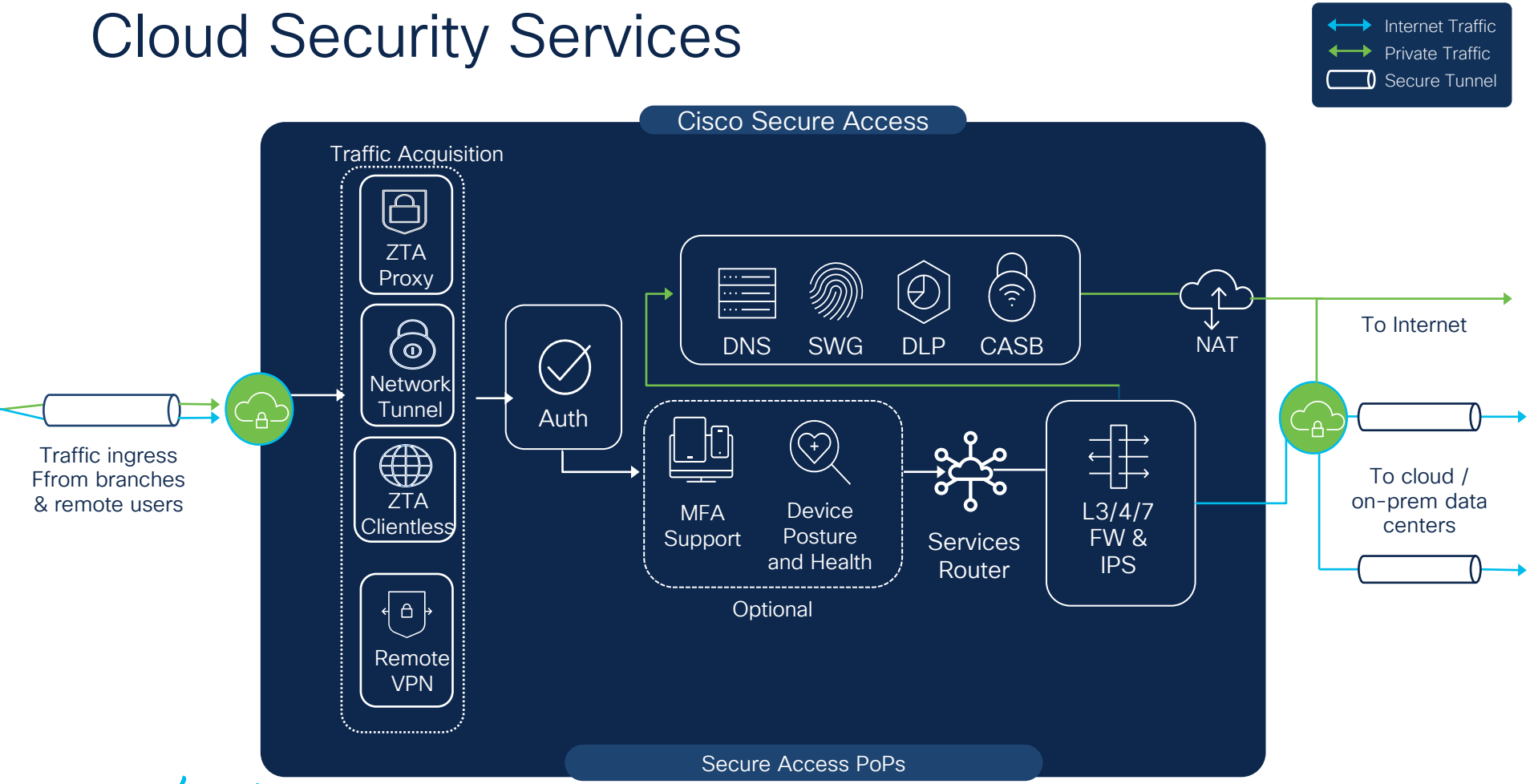
Featuring Cisco Secure Access

cisco Live!

Secure Access (“Security Service Edge”)



Cloud Security Services



Why connect your branches to Secure Access?

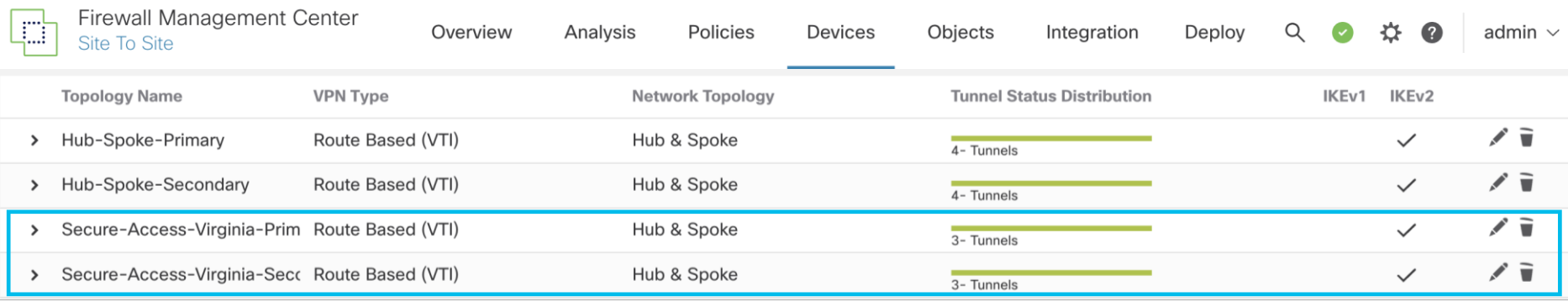
Internet Security capabilities:

- 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



- Use Hub & Spoke VTI Tunnel topology for simplicity (not required)
- Dual topologies allow for redundant tunnels to backup DC
- BGP or static routing to Secure Access data centers

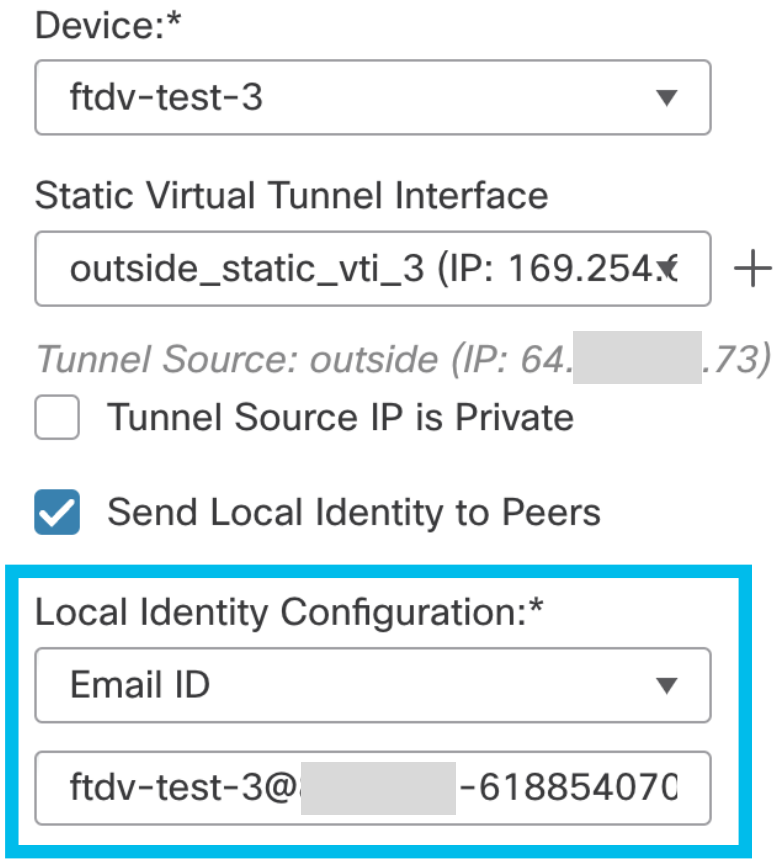
Branch Configuration for Secure Access tunnels

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:

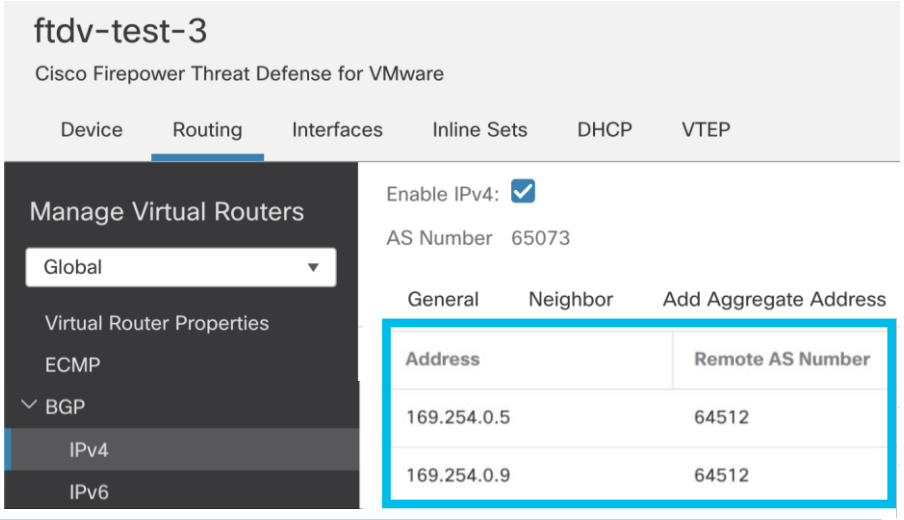
- Use “Email ID” for tunnel identity
- Default IKEv2 and IPSec settings
- If using Hub & Spoke topology, all branches use same pre-shared key



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




```
> 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:

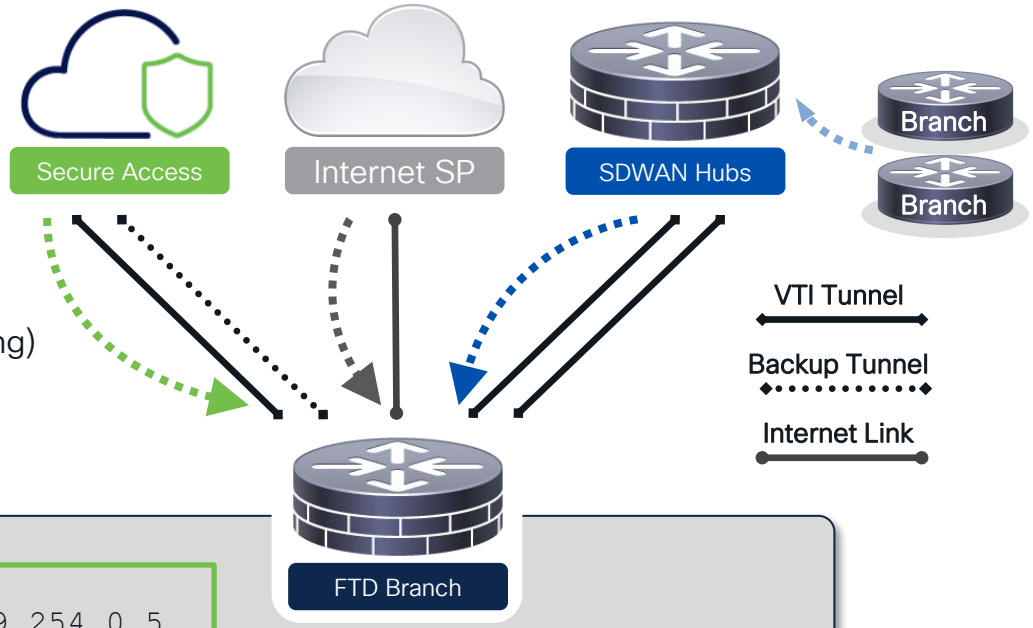
- Default Route* (Optional)
- RAVPN Subnets, Zero Trust enabled applications, Proxy Infrastructure

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
```

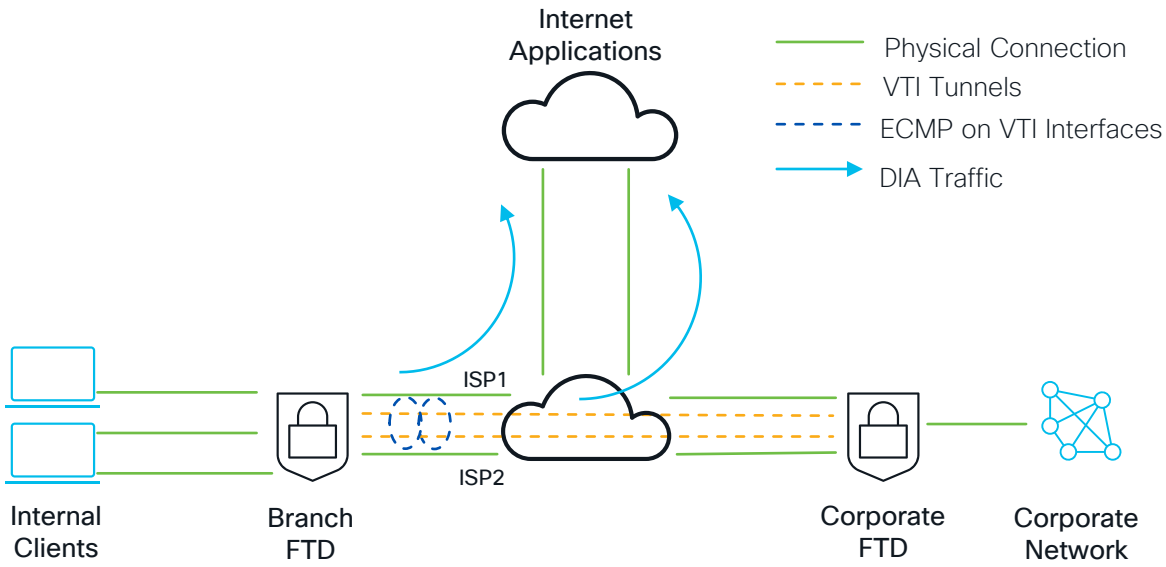
Firewall SDWAN

Policy Based Routing

Secure Firewall SD-WAN

WAN Connect and Remote Branch Management

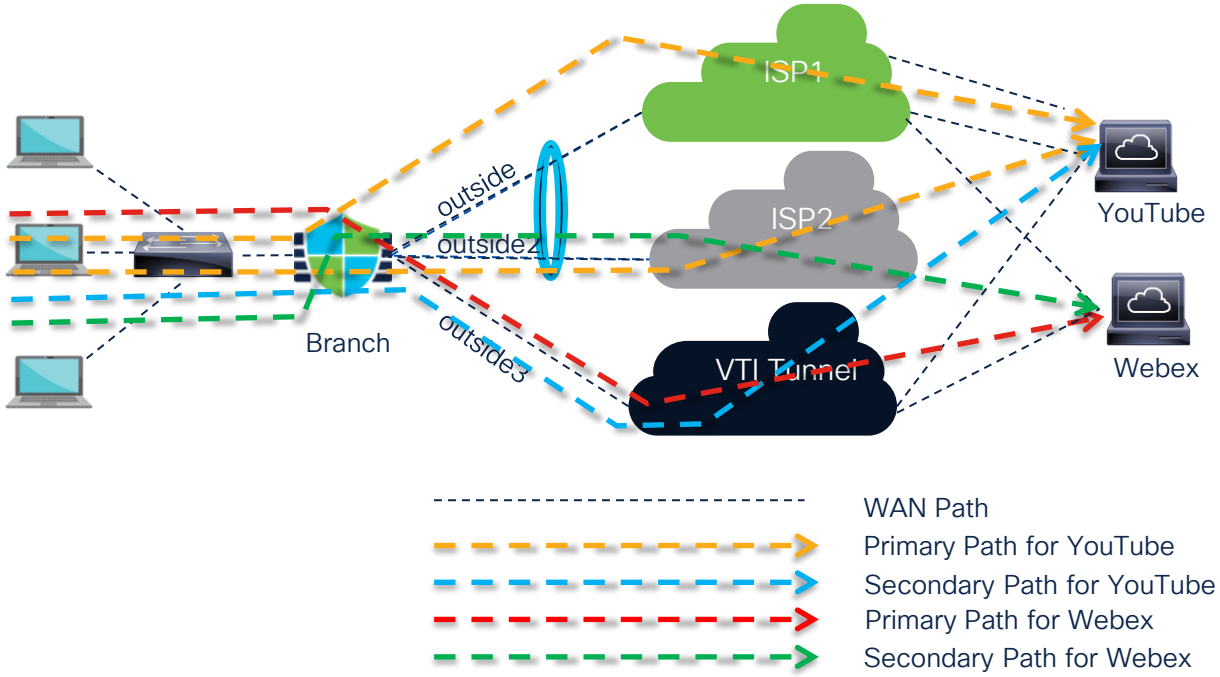
- Data Interface Management
- Intelligent Traffic Routing with Path Monitoring
- WAN PBR Path Monitoring
- Direct Internet Access
- Hub and Spoke DVTI
- Loopback Interface
- Auto-configuration rollback
- Low-touch Provisioning
- User Identity and SGT-based routing (in 7.4.1)



Intelligent Routing with Path Monitoring

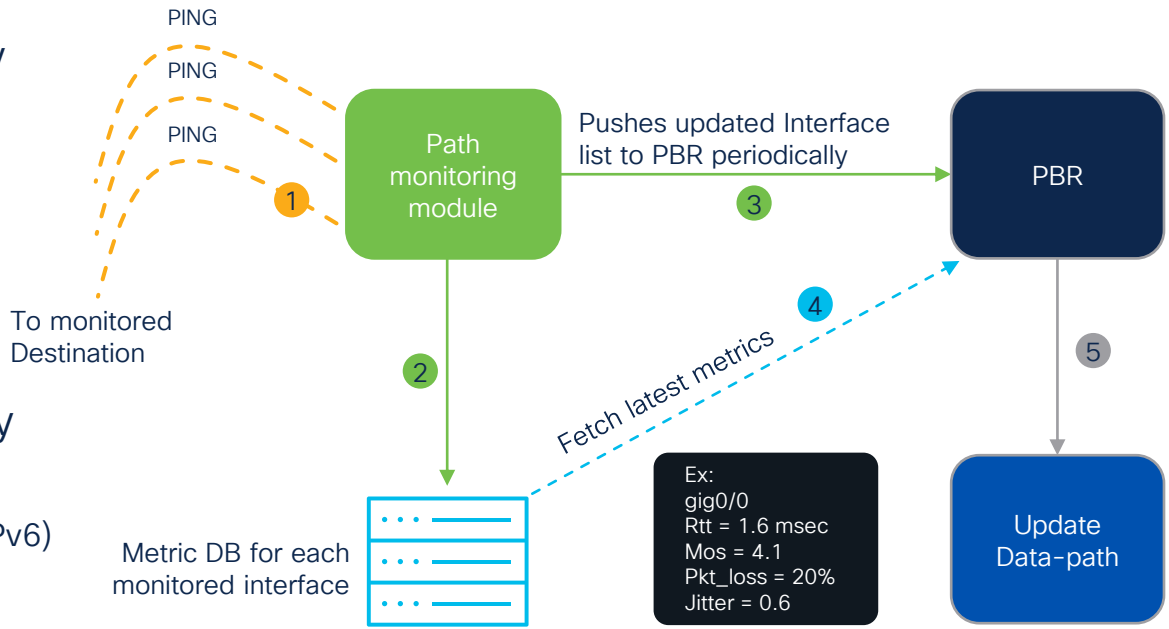
Per application-based traffic out direct Internet links or VTI tunnels

- Intelligent application routing
- Dynamic path selection using real time metrics
- Best egress path guaranteed
- Continuous monitoring of link health and network
- Egress interface selection based on multiple attributes



WAN PBR Path Monitoring

- PBR path monitoring steers traffic based on dynamically monitored interface metrics
  - Round Trip Time (RTT)
  - Jitter
  - Packet Loss
  - Mean Opinion Score (MOS)
- Interface sends a ping every 30 seconds
  - Next-hop (Auto, Auto IPv4, Auto IPv6)
  - An explicit user configured IP address (Peer-IPv4, Peer-IPv6)



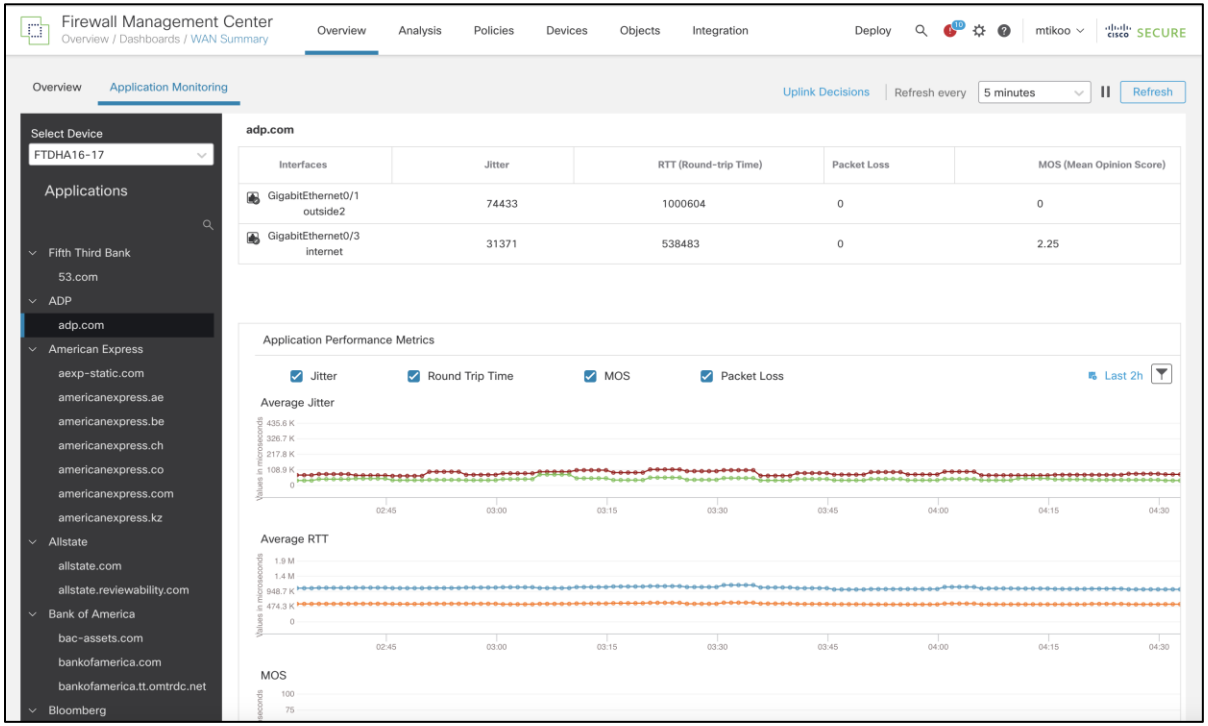
Monitoring & Troubleshooting

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

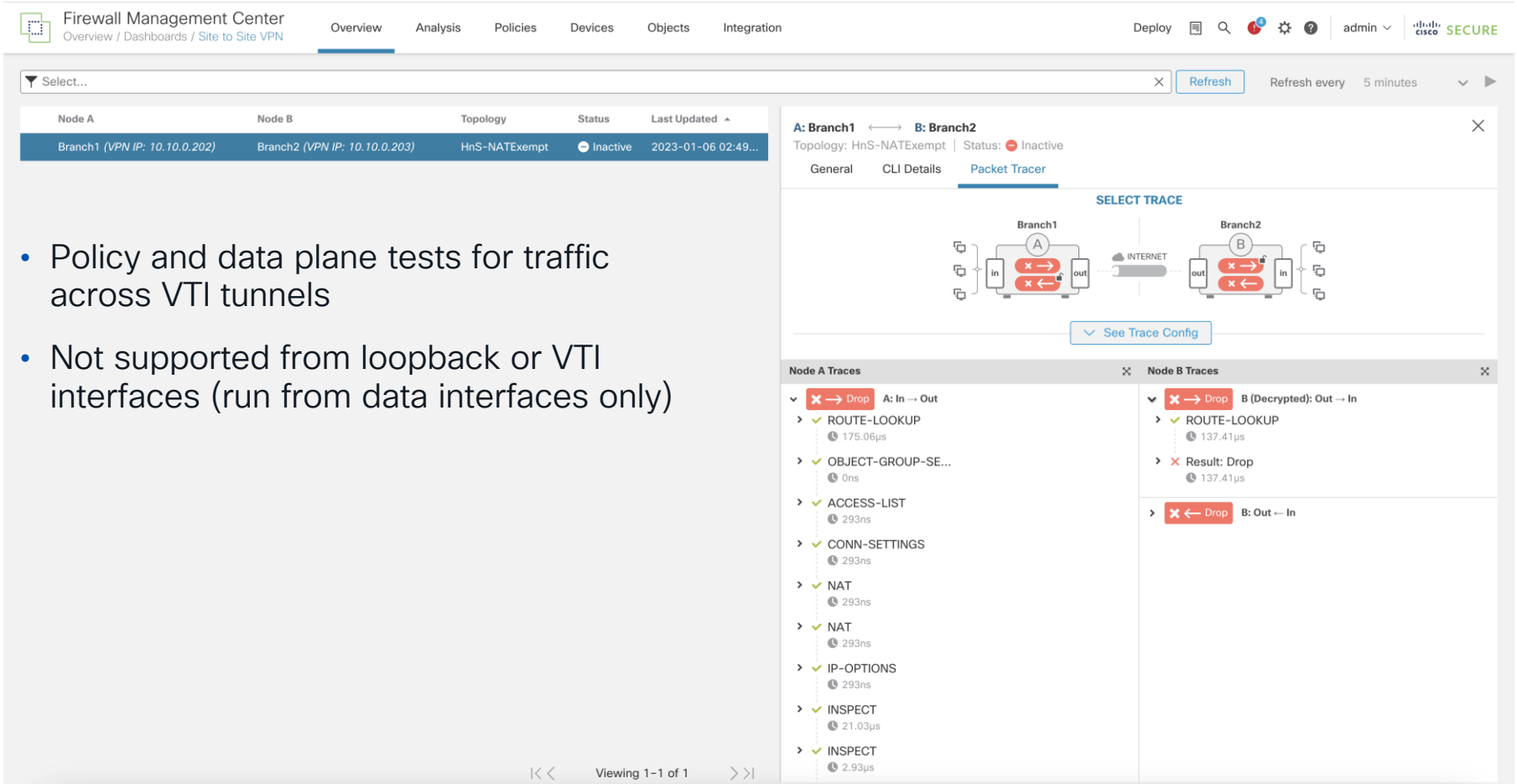
Detailed View in Health Monitoring

Enhanced WAN Application Monitoring



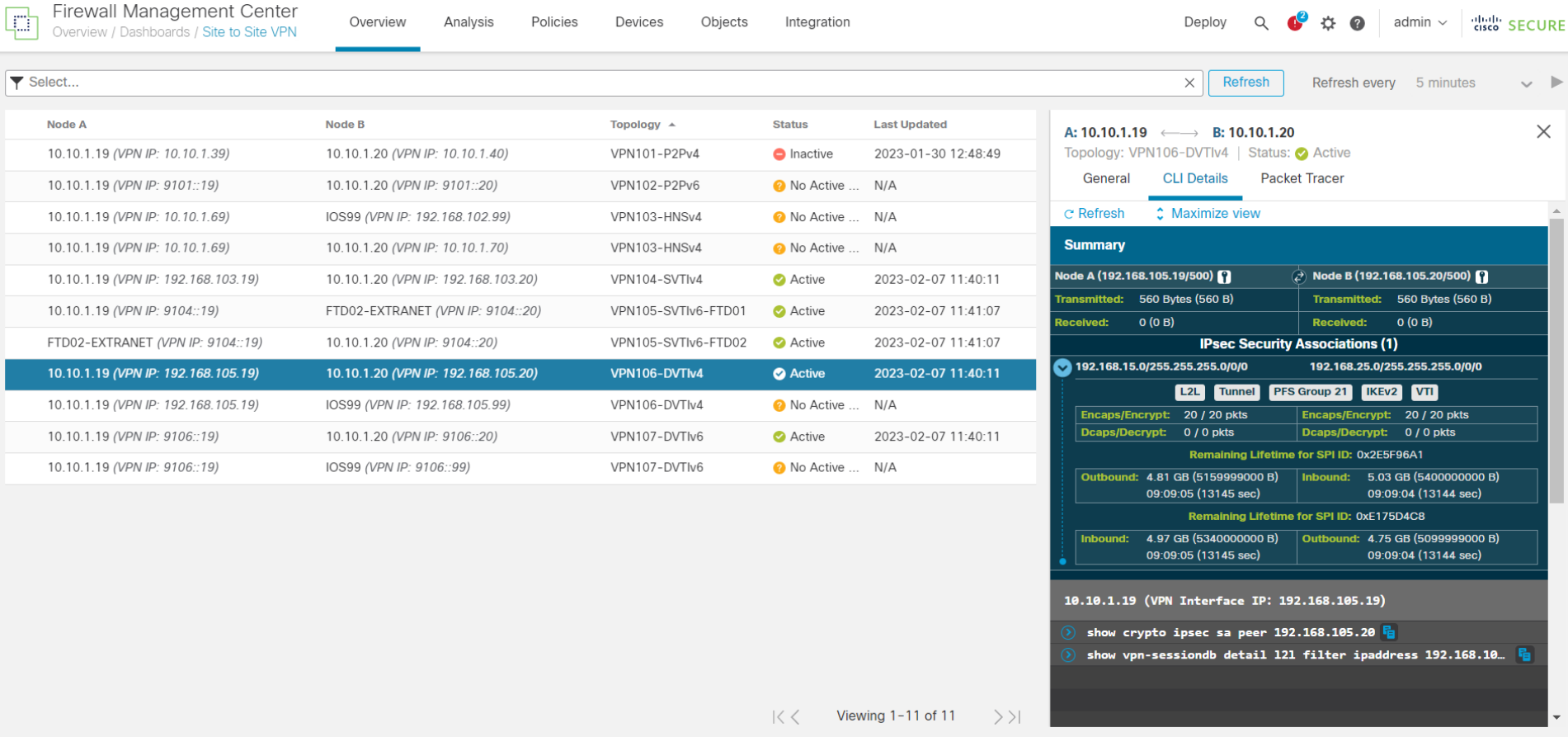
- Easily monitor all interfaces where Policy-Based Routing is enabled
- Detailed application performance metrics for Jitter, Round Trip Time, MOS and Packet Loss

VPN Packet Tracer in 7.3

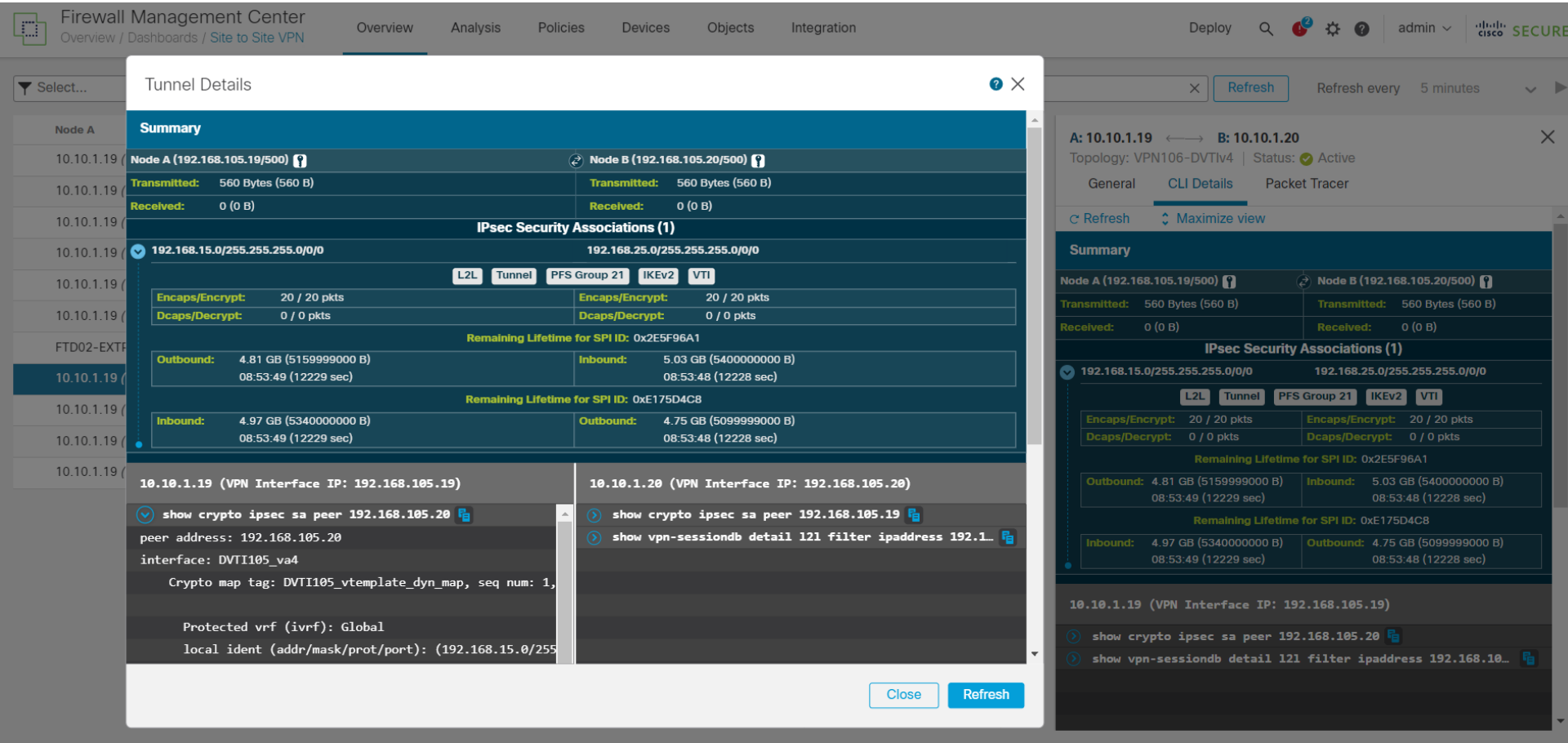


- Policy and data plane tests for traffic across VTI tunnels
- Not supported from loopback or VTI interfaces (run from data interfaces only)

Site to Site Monitoring in 7.4



Site to Site Monitoring in 7.4



CLI configuration to onboard FTDv

Allows management on outside interface for cdFMC connectivity

Reference

```
> 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.[redacted].83
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 38.[redacted].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

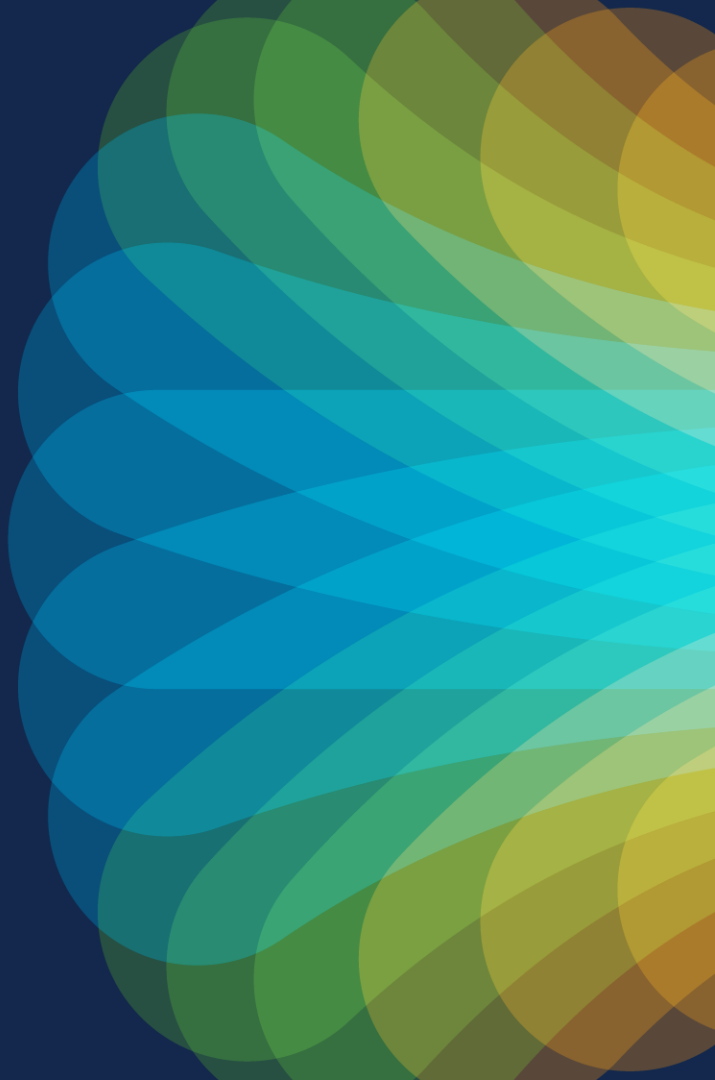
Secure Firewall Threat Defense / ASA

Scalable hub and spoke VPNs for up to 1,000 sites!

- Use VTI interfaces for all VPN tunnels including Cloud IaaS & SASE / SSE deployments!
- Use to ASA 9.19 or FTD 7.3+ for DVTI HUB support!
- Must use routing protocol for DVTI hub spoke topologies
- Policy Based Routing on FTD to prioritize Internet links or tunnels to optimize security and end user experience!
- BGP recommended for Hub & Spoke VPN deployments, SASE / SSE integrations and more!

The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go