The bridge to possible

Route Based VPNs

With Secure Firewall

Jeff Fanelli, Principal Architect
@jefanell

cisco Live!

BRKSEC-3058

Agenda

- IPSec VPN Solutions Overview
- VPN Tunnel Interfaces and types
- Scalable VPN with FTD Integration Deployment Example
- IPSec VPN Best Practices
- Conclusion

About Me

Jeff Fanelli

- jefanell@cisco.com
- Principal Architect
- 17 years @ Cisco
- 35+ CiscoLive! Presenter
- Husband + father
- Private pilot
- Slave to three wiener dogs

Cisco Webex App

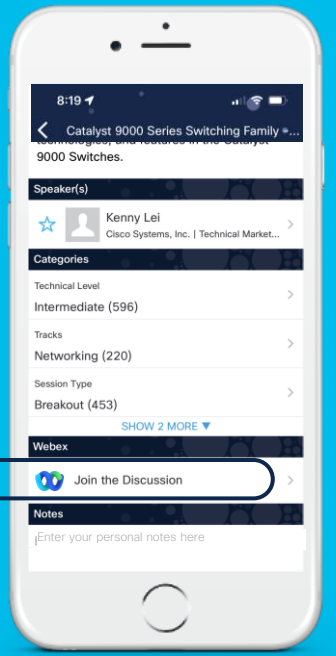
Questions?

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 until February 24, 2023.

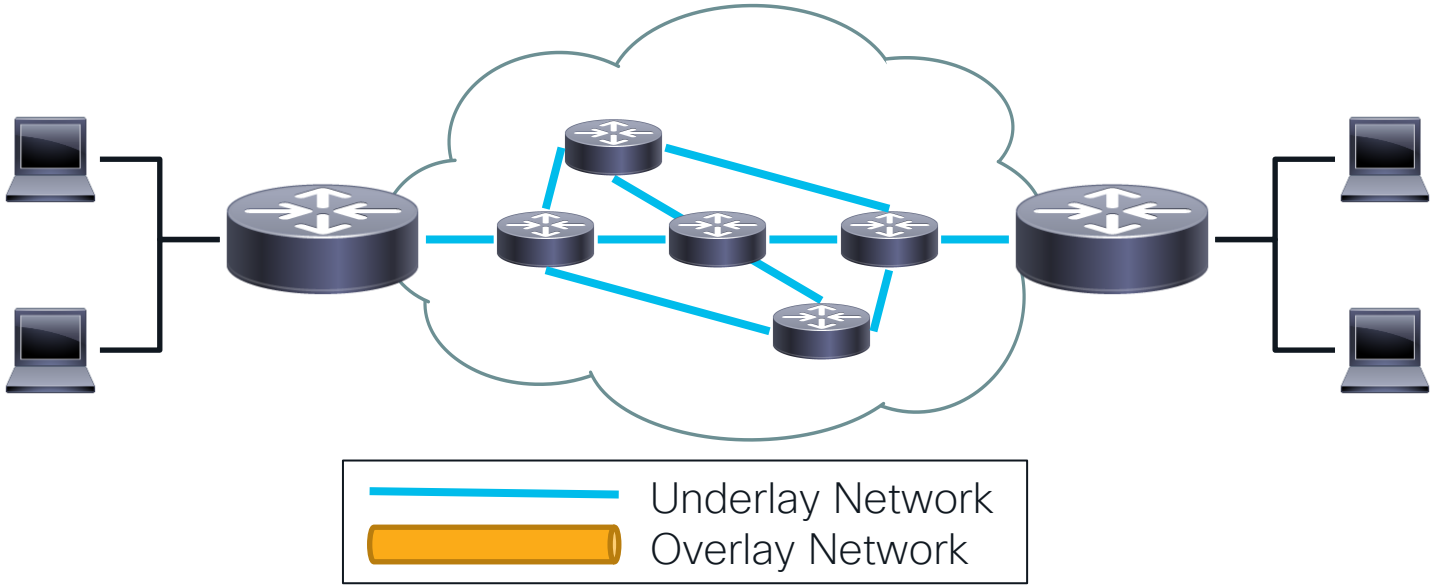


Platform names and abbreviations

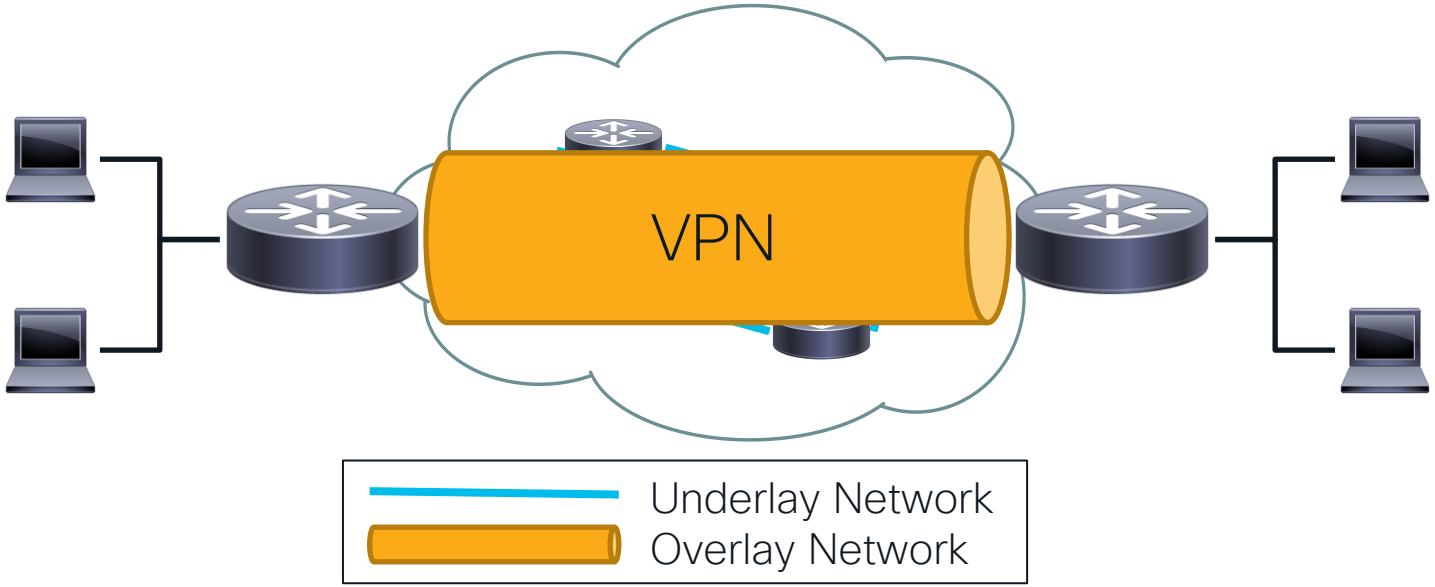
- Cisco Secure Firewall – Product line name
- Cisco Secure Firewall ASA
  - Adaptive Security Appliance “ASA” (software platform)
- Cisco Secure Firewall Threat Defense
  - Firepower Threat Defense “FTD” (software platform)
- Catalyst 8000 Edge – Product line name
  - Internet Operating System “IOS” (or IOS-XE) (software platform)

VPN Technology Overview

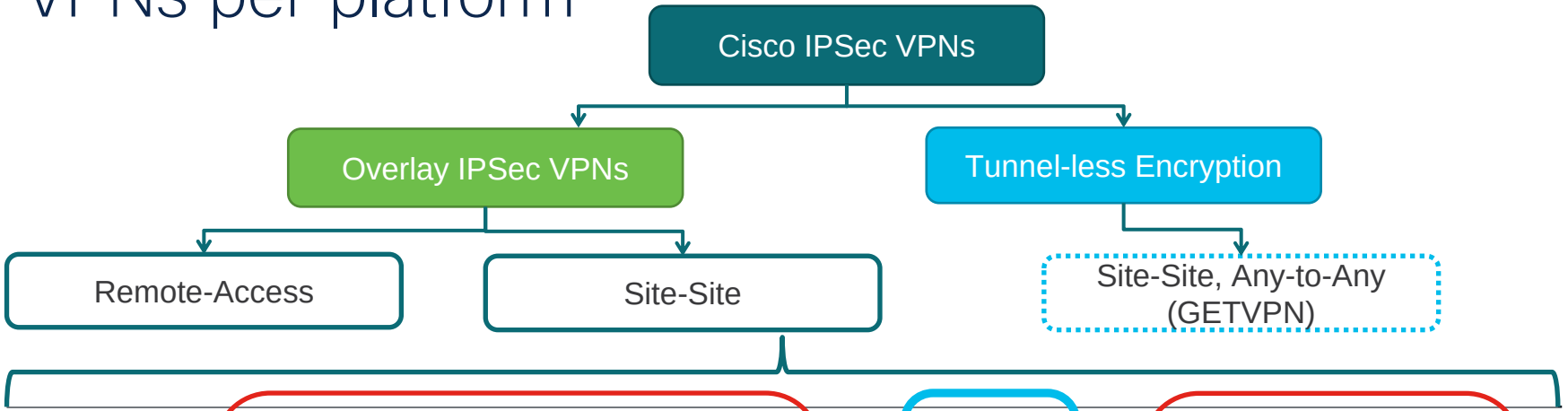
Underlay & Overlay



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

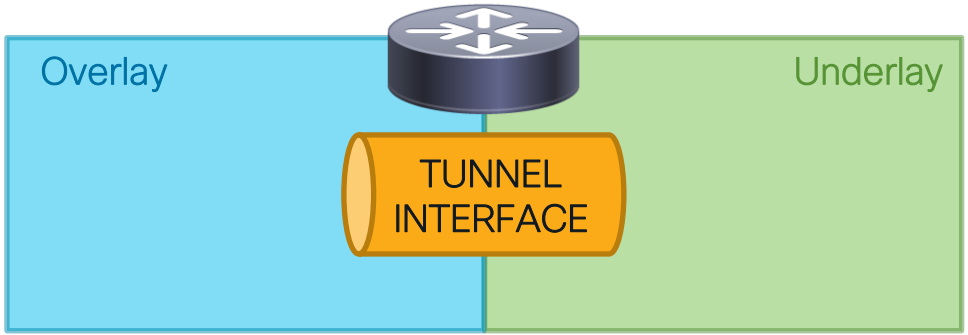
Reference

- 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
```

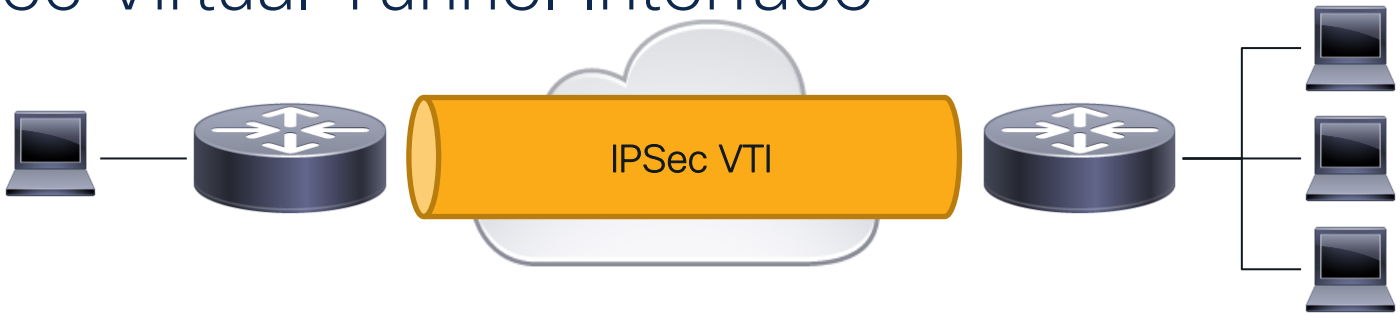
VPN Tunnel Interfaces

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) also supported on ASA / FTD

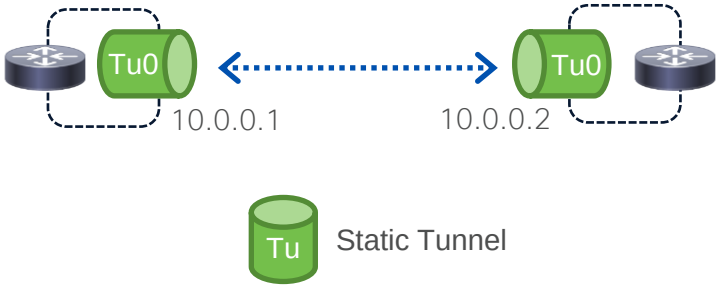
IPSec Virtual Tunnel Interface



- 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

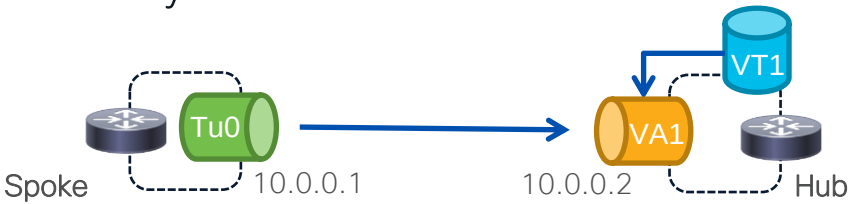
- Static Tunnel Interface

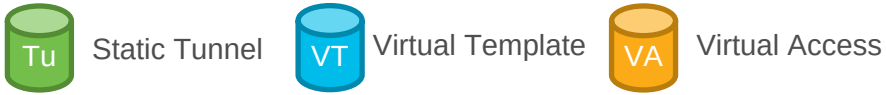



```
interface Tunnel1
 nameif tunnel-to-dc (ASA/FTD only)
 ip unnumbered Loopback1 (ASA 9.19+ FTD 7.3+)
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.2
 tunnel protection ipsec profile default
```

IPSec Tunnel Interface Types - Dynamic

- Dynamic Tunnel Interface





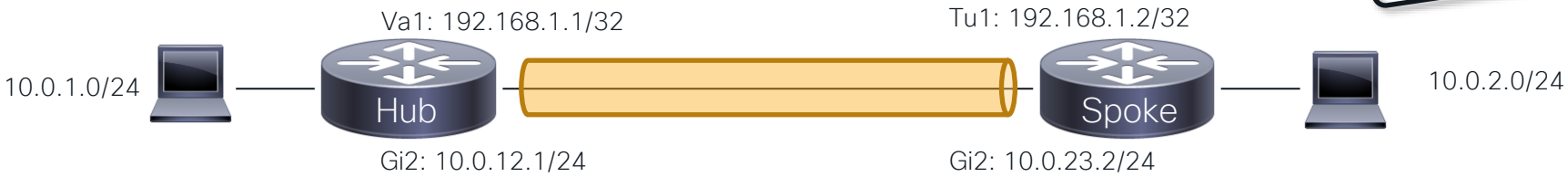
Dynamic Tunnel Interfaces (DVTI) are introduced in ASA 9.19 and FTD 7.3

```
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
```

IKEv2 Dynamic VTI – Configuration (IOS)

Reference



Hub

```
crypto ikev2 authorization policy default
 route set remote ipv4 10.0.0.0 255.0.0.0
!
crypto ikev2 profile default
 match identity remote any
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list flex default local
 virtual-template 1
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 ip ospf 1 area 1
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

Spoke

```
crypto ikev2 authorization policy default
 route set remote ipv4 10.0.2.0 255.255.255.0
!
crypto ikev2 profile default
 match identity remote address 10.0.12.1
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list flex default local
!
interface Tunnel1
 ip address 192.168.1.2 255.255.255.255
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 10.0.12.1
 tunnel protection ipsec profile default
!
interface GigabitEthernet2
 ip address 10.0.23.2 255.255.255.0
```

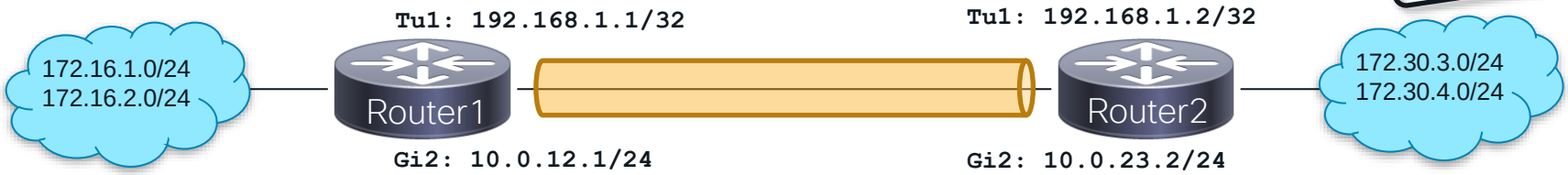
IKEv2 Multi-SA Static VTI

Reference

- By default, the traffic selector for an SVTI is set to ‘any any’.
- From Cisco IOS XE 16.12.1 we can define and associate an ACL with an SVTI.
- Supported in ASA 9.19+ and FTD 7.3+
- IPSec SAs are created for each non-any-any traffic selector, and thus, multiple SAs are attached to an SVTI.

IKEv2 Multi-SA SVTI - Configuration

Reference



Router1

```
crypto ikev2 profile default
 match identity remote 10.0.23.2
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
aaa authorization group psk list flex default local
!
crypto ipsec profile default
 reverse-route
!
ip access-list extended SVTI_ACL
 permit ip 172.16.1.0 0.0.0.255 172.30.3.0 0.0.0.255
 permit ip 172.16.2.0 0.0.0.255 172.30.4.0 0.0.0.255
!
interface Tunnel1
 ip address 192.168.1.1 255.255.255.252
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 10.0.23.2
 tunnel protection ipsec policy ipv4 SVTI_ACL
 tunnel protection ipsec profile default
```

Router2

```
crypto ikev2 profile default
 match identity remote 10.0.12.1
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list flex default local
!
crypto ipsec profile default
 reverse-route
!
ip access-list extended SVTI_ACL
 permit ip 172.30.3.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 172.30.4.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface Tunnel1
 ip address 192.168.1.2 255.255.255.252
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 10.0.12.1
 tunnel protection ipsec policy ipv4 SVTI_ACL
 tunnel protection ipsec profile default
```

Secure Firewall VPN Design

cisco Live!

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

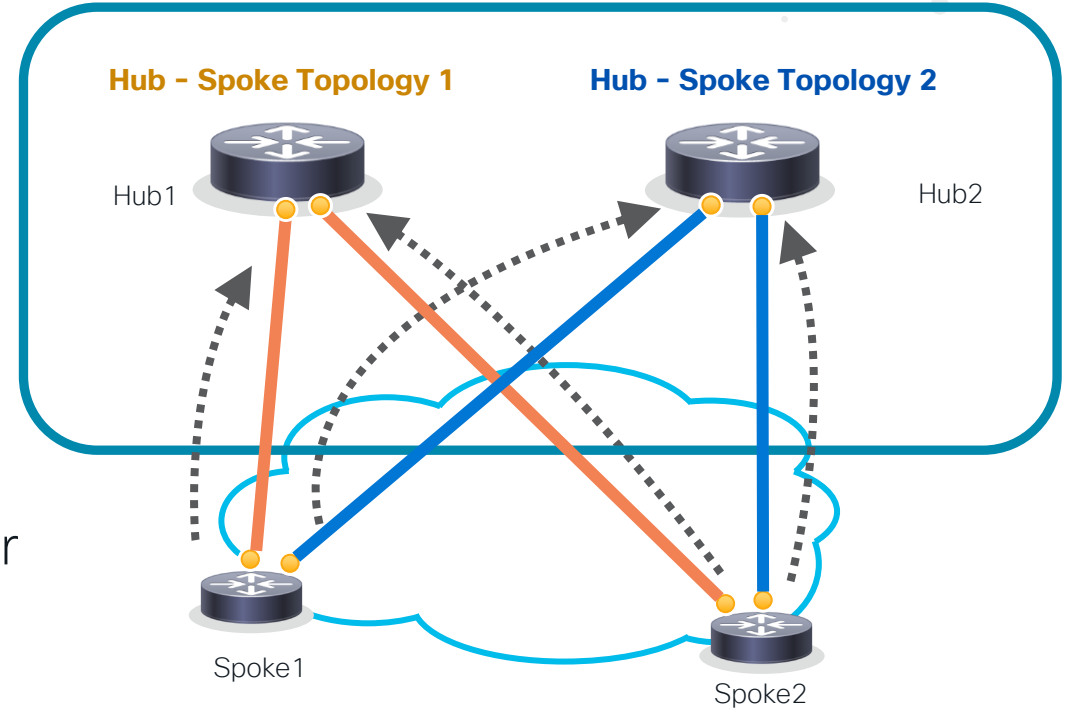
- Scaled Deployment / hub-and-spoke topology
- Provide security using cryptographically protected tunnels.
- Headend redundancy with 15 seconds convergence
- Branches can include ASA / FTD

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

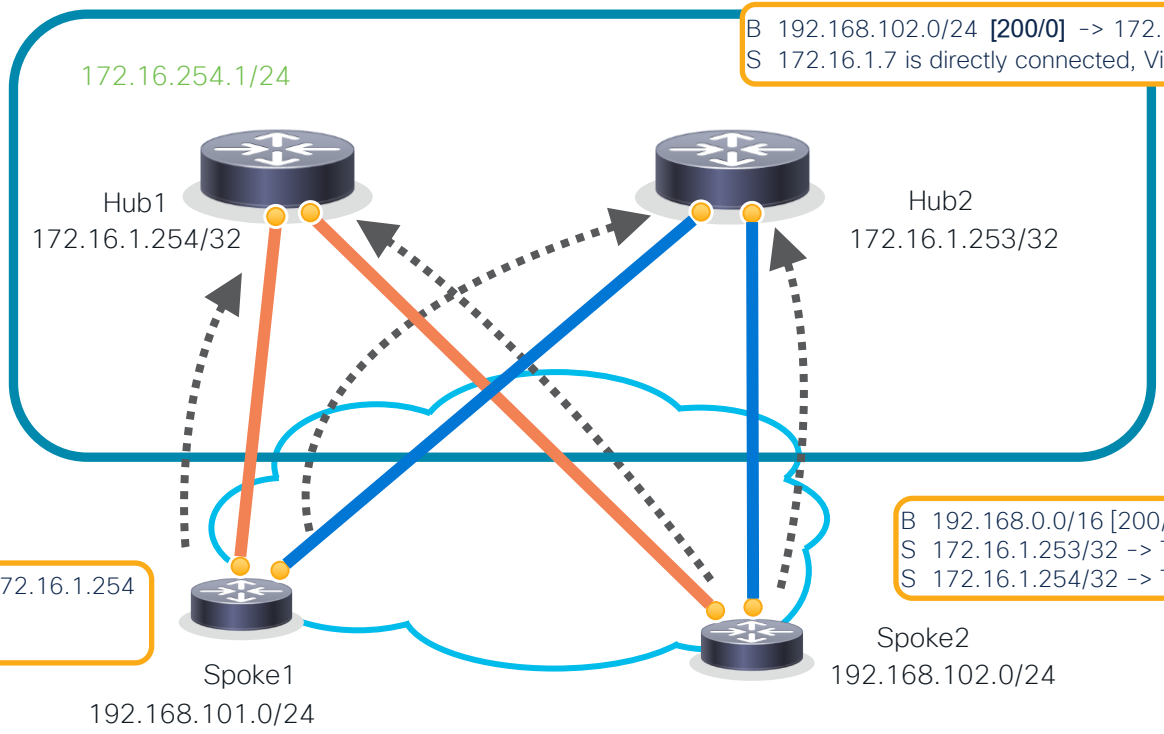


Single / Double Hub & Spoke design using VTI

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
```

Spoke router configuration – IOS Example

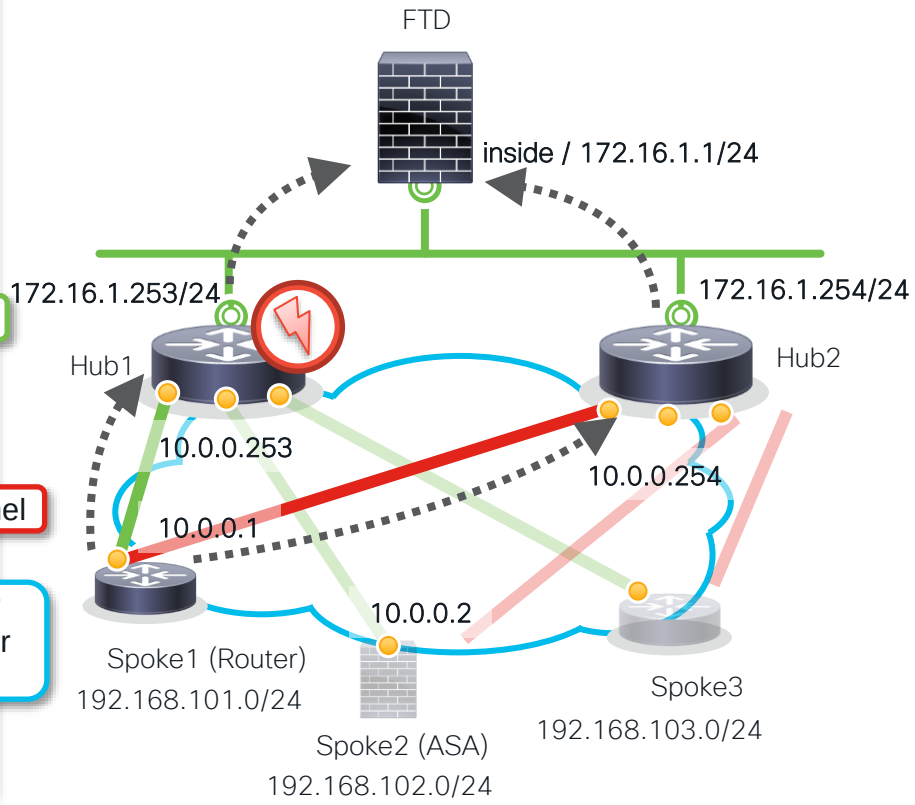
Reference

```
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



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)

Considerations for different VPN spoke types

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

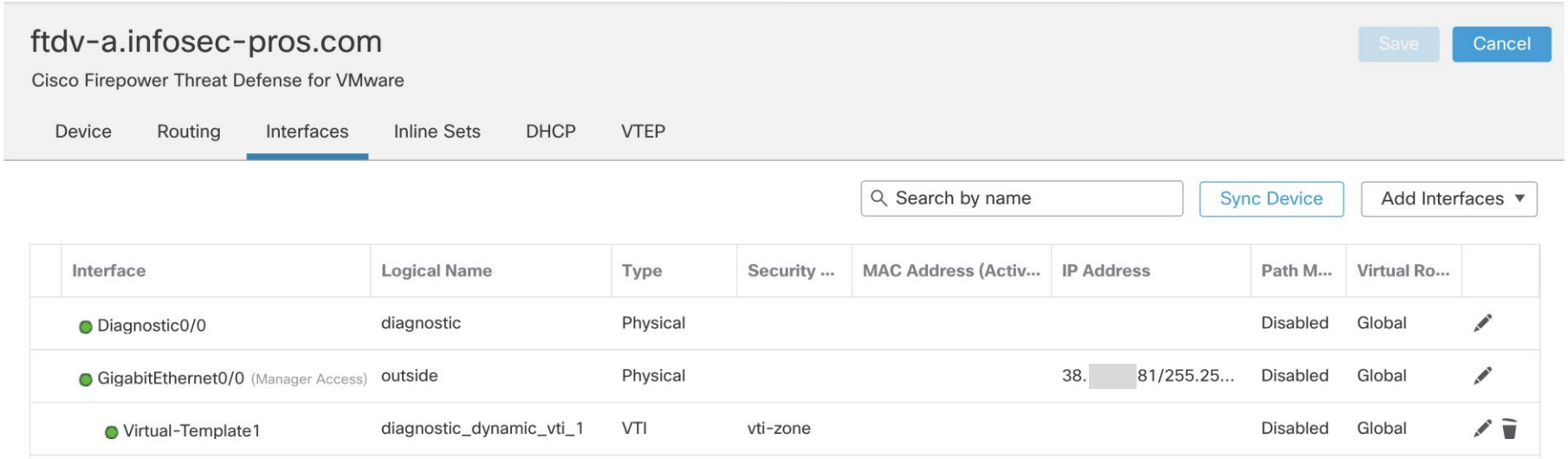
- Static IP address configuration spokes will have spoke specific crypto peer settings configured on hub (with or without NAT IP configured)
- DHCP configured peers will be configured to connect to ”L2L” default tunnel-group
- FMC will redeploy all spokes on any spoke add / change (will be addressed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

Secure Firewall VPN Design

Firewall Management Center GUI

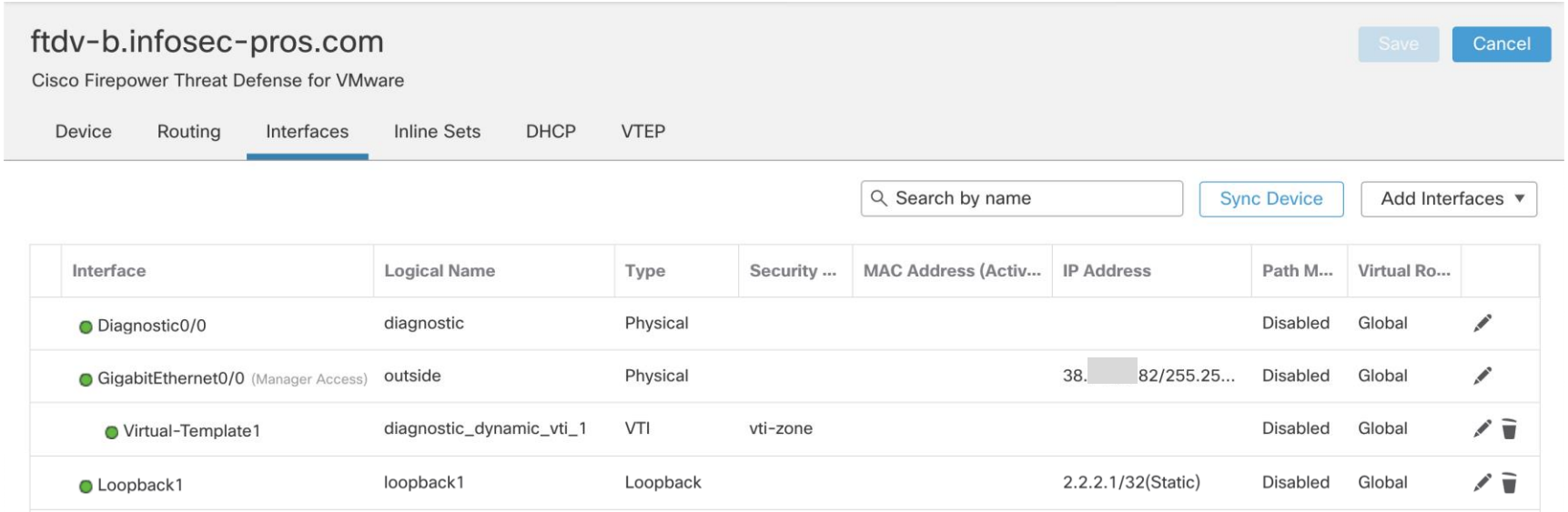
cisco Live!

Hub Device Interface Configuration



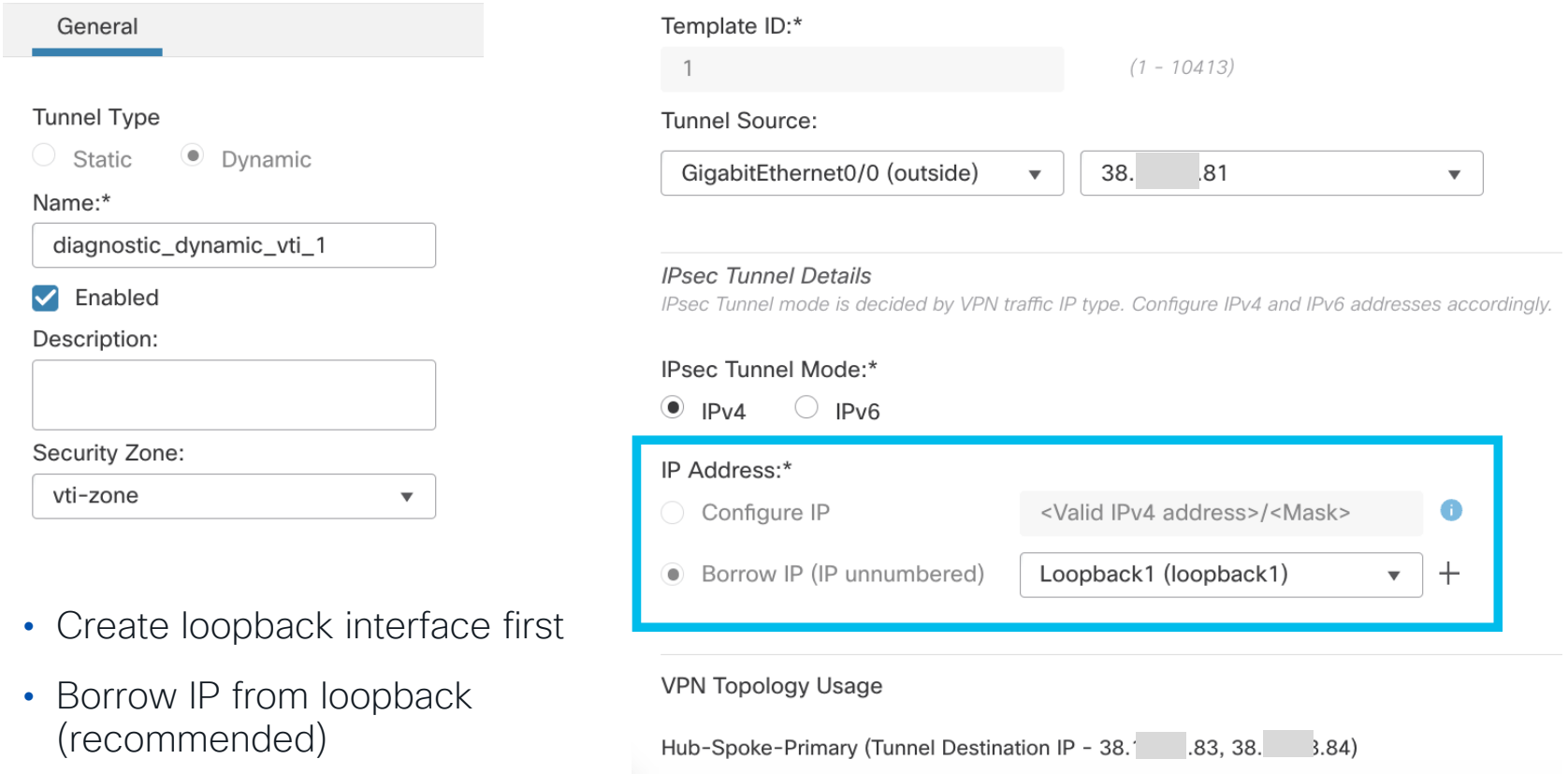
- Hub configuration “Virtual Template” interface is created by VPN Topology configuration
- Virtual Template interface can ”borrow” loopback address (recommended)
- Virtual Template interface is used to create ephemeral VTI interfaces as spokes connect

Spoke Config (with borrowed IP from loopback)



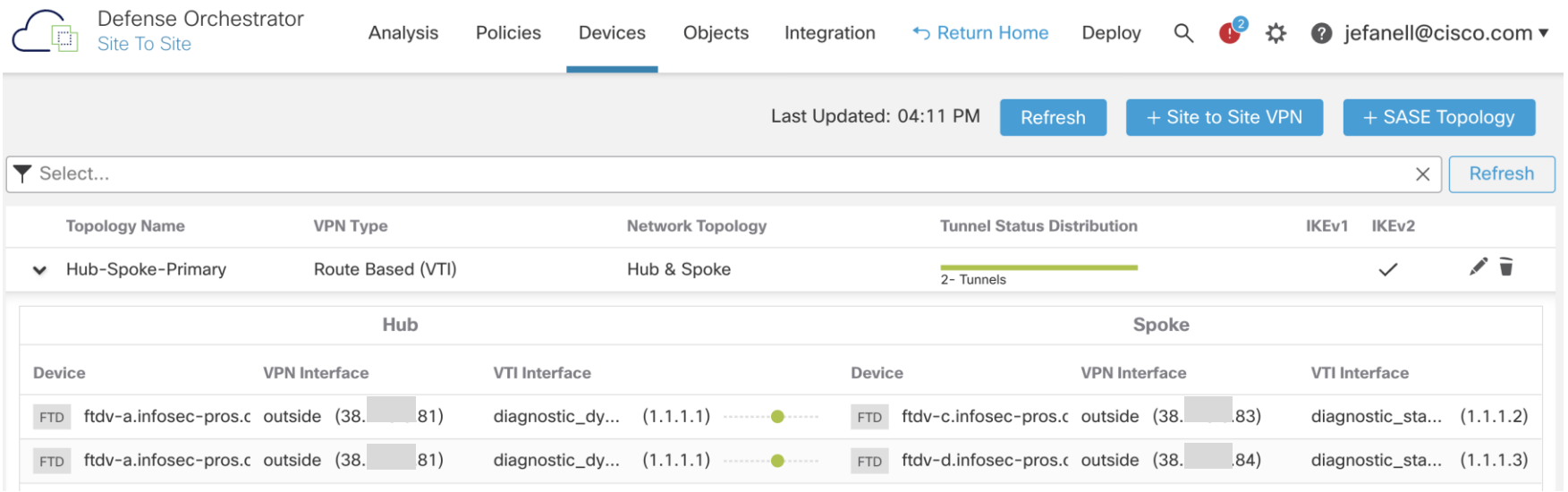
- Create loopback interface first
- SVTI interface configuration for VPN topology can “borrow” this IP address (recommended, requires 7.3)

Hub Virtual-Template Interface Config



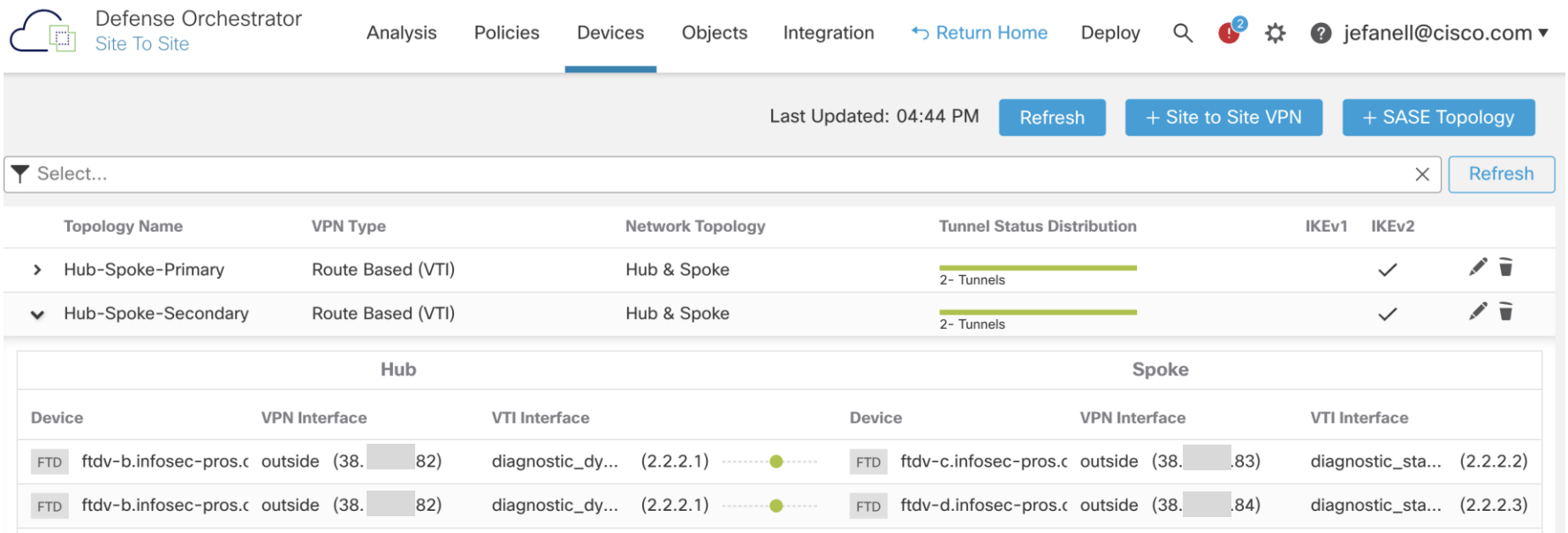
- Create loopback interface first
- Borrow IP from loopback (recommended)

Site to Site VPN Topology with DVTI



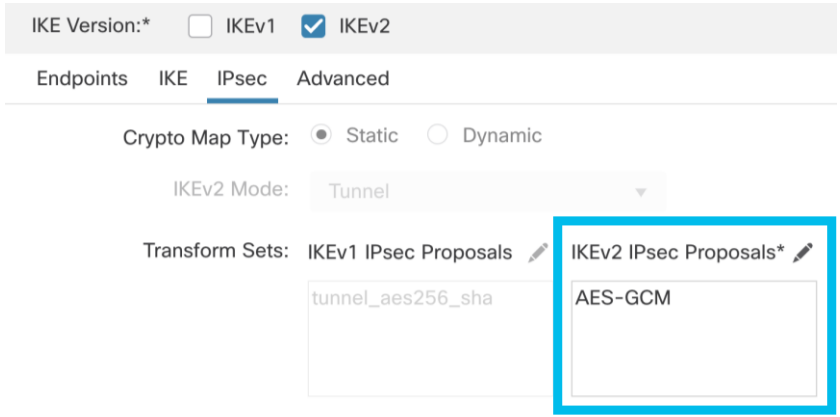
- Unmanaged / external firewalls can be referenced in topologies
- Routing protocol required on member devices to share routes
- Hub and spoke VTI interface routes shared via IKE protocol

Site to Site VPN Dual Topologies



- Same spokes in two separate hub topologies
- 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

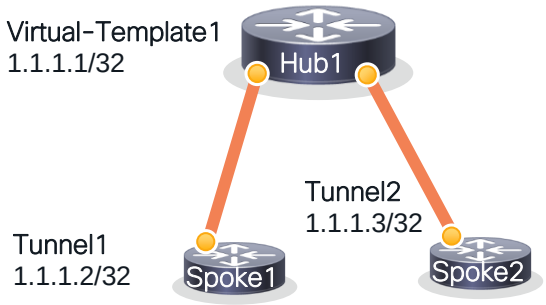
Hub routing table example

Device: ftdv-a.infosec-pros.com

Command: show Parameter: route

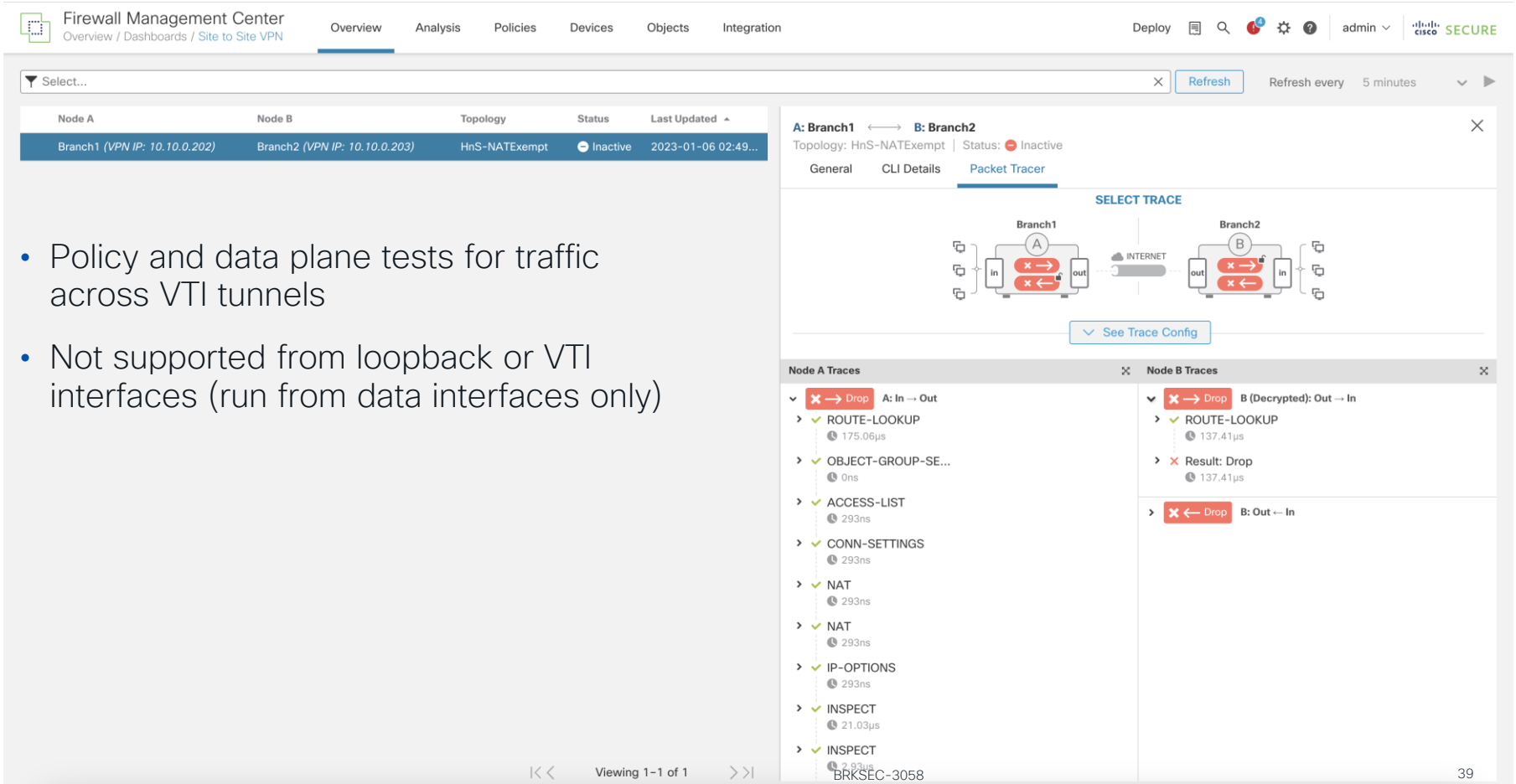
Output

```
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       38.1      .0 255.255.255.0 is directly connected, outside
L       38.1      .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
```



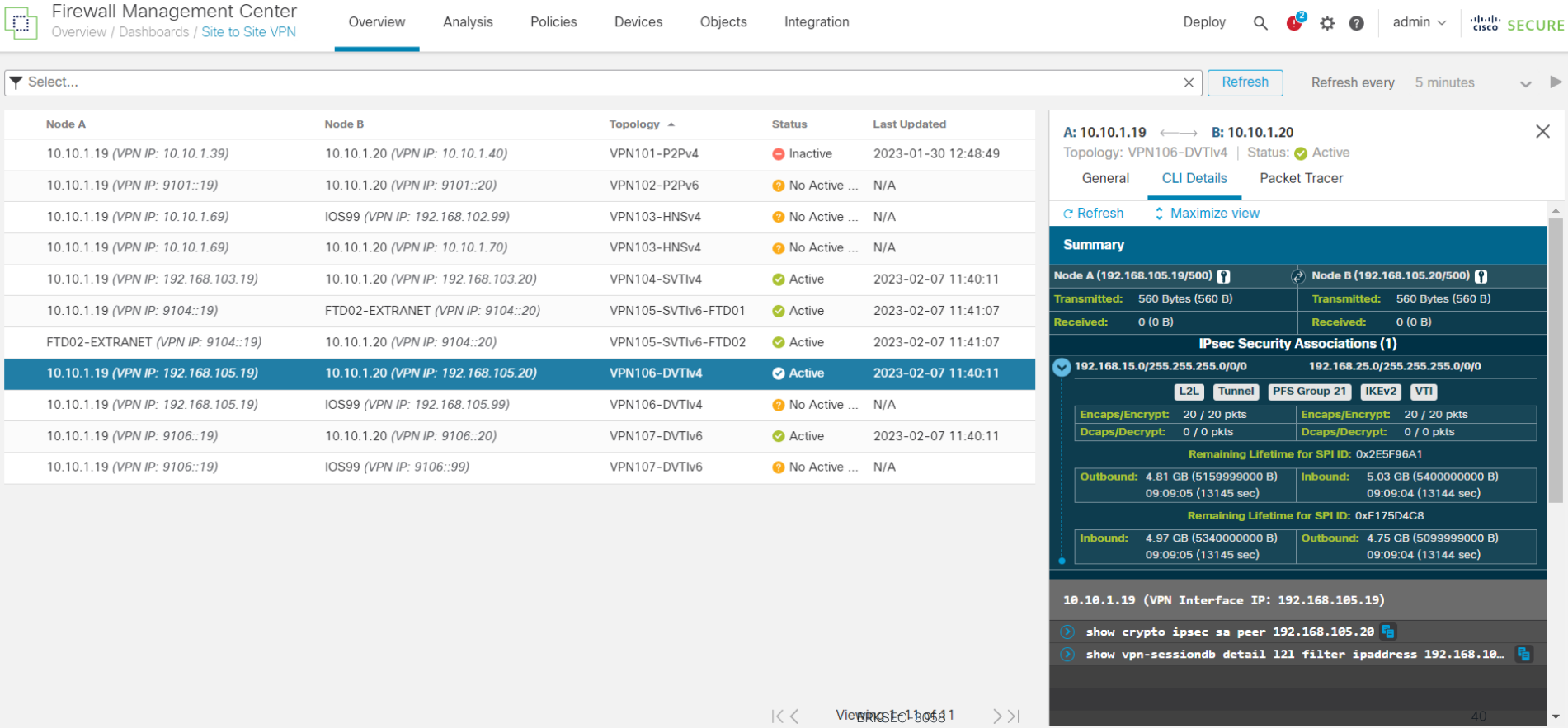
- "V" routes shared by IKEv2 (only VTI interface routes)
- Can "ping" between VTI interfaces for testing
- Branch routes should be shared via routing protocol (BGP etc)

VPN Packet Tracer in 7.3

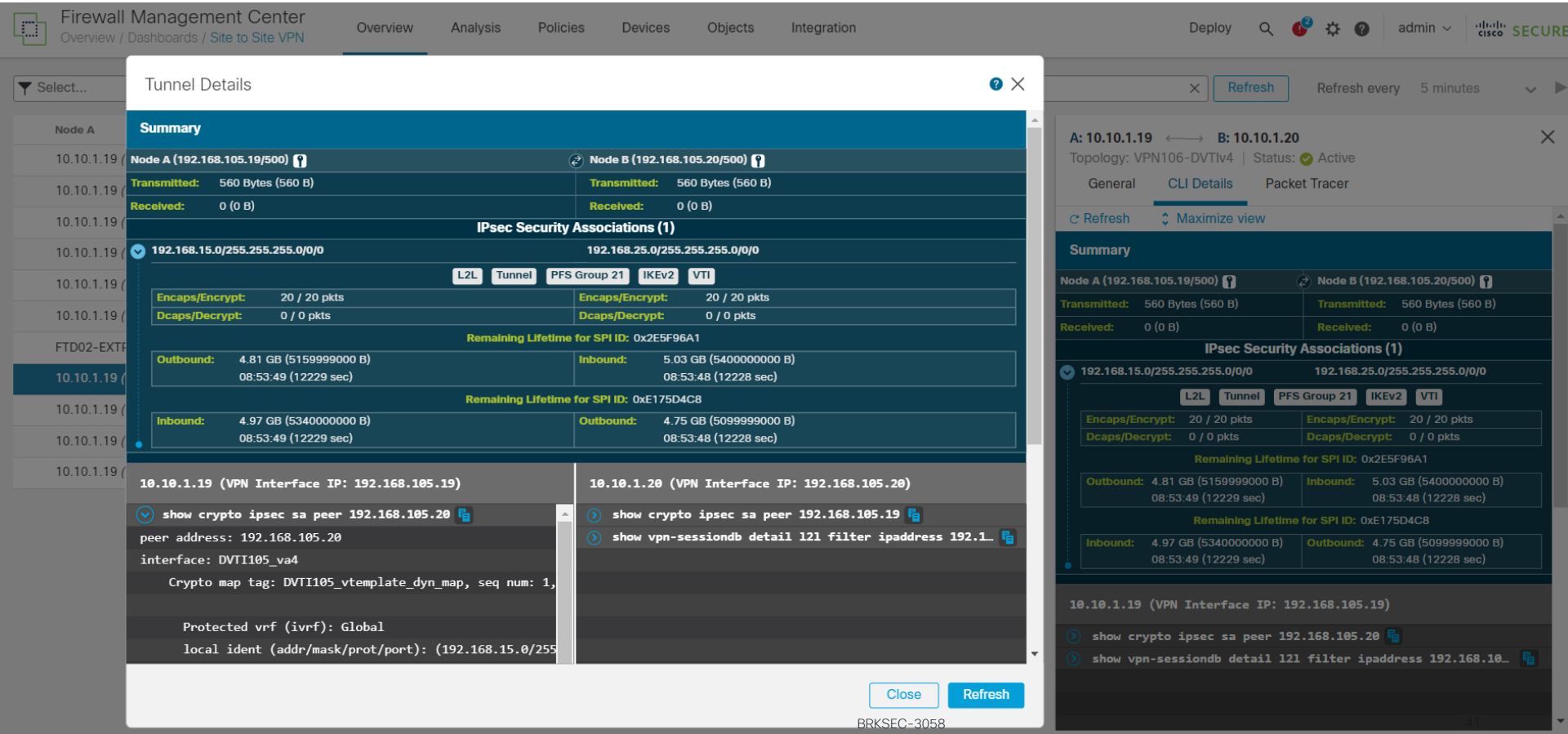


- Policy and data plane tests for traffic across VTI tunnels
- Not supported from loopback or VTI interfaces (run from data interfaces only)

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!

DO's for ASA/FTD VPNs:

- Use VTI interfaces for all site-to-site tunnels (including Cloud IaaS)
- Use to ASA 9.19 or FTD 7.3+ for DVTI HUB support!
- Must use routing protocol for DVTI hub spoke topologies
- SVTI-SVTI tunnels can be statically routed

DON'Ts for ASA/FTD VPNs:

- Don't forget to lock down tunnel interface(s) with Access Control List (ASA) or Access Control Policy (FTD)
- Don't forget to lock down IPSec Profiles for peers with complex, unique passwords and / or additional unique IKE identifiers.

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

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

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

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


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN

Hub's IKEv2 profile selection

```
crypto ikev2 profile router
 match identity remote fqdn domain router
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list FlexVPN name-mangler extract-domain
 virtual-template 1 mode auto
```

```
crypto ikev2 profile firewall
 match identity remote fqdn domain firewall
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list FlexVPN name-mangler extract-host
 virtual-template 1 mode auto
 no config-exchange request
```

Reference

```
crypto ikev2 name-mangler extract-domain
 fqdn domain
```

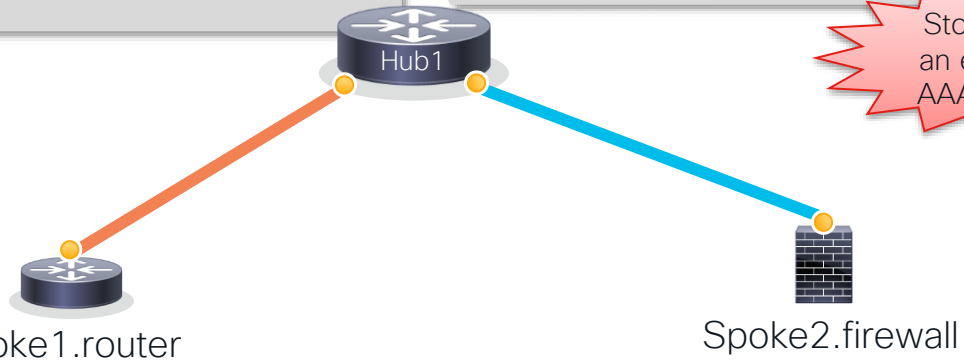
```
crypto ikev2 authorization policy router
 route set interface
```

```
crypto ikev2 name-mangler extract-host
 fqdn hostname
```

```
crypto ikev2 authorization policy Spoke2
 route set local ipv4 172.16.1.5
255.255.255.255
```

Store it on an external AAA server

Required only if we want to terminate ASA/FTD versions pre 9.19/7.3 because they do not support IKEv2 config exchange



cisco Live!

* VTI for FTD on 6.7 roadmap

Hub router configuration – with PBR

Reference

```
aaa new-model
aaa authorization network FlexVPN local
!
access-list 123 permit ip 192.168.0.0 0.0.255.255 any
!
route-map FW permit 10
  match ip address 123
  set ip next-hop 172.16.254.254
!
crypto ikev2 profile router
 match identity remote fqdn domain router
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list FlexVPN name-mangler
extract-domain
 virtual-template 1 mode auto
!
crypto ikev2 profile firewall
 match identity remote fqdn domain firewall
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list FlexVPN name-mangler
extract-domain
 virtual-template 1 mode auto
 no config-exchange request
```

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 ip policy route-map FW
 tunnel protection ipsec profile default
!
router bgp 65000
 bgp listen range 172.16.1.0/24 peer-group Flex
 bgp listen limit 10000
 timers bgp 5 15
 neighbor Flex peer-group
 neighbor Flex remote-as 65000
 !
 address-family ipv4
  redistribute connected
  neighbor Flex activate
  neighbor Flex route-reflector-client
  neighbor Flex next-hop-self all
 exit-address-family
```

PBR

Separate IKEv2 profiles for routers and firewalls

iBGP with listen range

Interface and routing verification (IOS Only!)

Reference

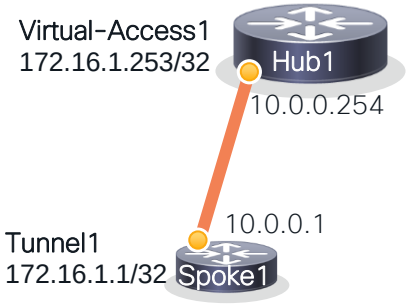
```
Hub1# show derived-config interface Virtual-Access 1
Building configuration...

Derived configuration : 197 bytes
!
interface Virtual-Access1
 ip unnumbered Loopback1
 ip policy route-map FW
 tunnel source GigabitEthernet2
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile default
 no tunnel protection ipsec initiate
```

Derived from the Virtual-Template (show command not available on ASA/FTD)

```
Hub1# show ip route
S        172.16.1.1/32 is directly connected, Virtual-Access1
B        192.168.101.0/24 [200/0] via 172.16.1.1, 00:25:06
```

```
Spoke1# show ip route
S        172.16.1.254/32 is directly connected, Tunnel1
S        172.16.1.253/32 is directly connected, Tunnel2
B     192.168.0.0/16 [200/0] via 172.16.1.254, 00:07:27
```



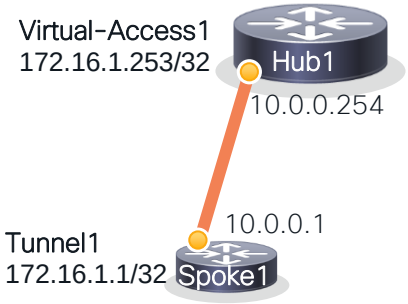
Interface and routing verification

Reference

```
Hub1# show derived-config interface Virtual-Access 1
Building configuration...

Derived configuration : 197 bytes
!
interface Virtual-Access1
 ip unnumbered Loopback1
 ip policy route-map FW
 tunnel source GigabitEthernet2
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile default
 no tunnel protection ipsec initiate
```

Derived from the Virtual-Template (show command not available on ASA/FTD)




```
Hub1# show ip route
S        172.16.1.1/32 is directly connected, Virtual-Access1
B        192.168.101.0/24 [200/0] via 172.16.1.1, 00:25:06
```

```
Spoke1# show ip route
S        172.16.1.254/32 is directly connected, Tunnel1
S        172.16.1.253/32 is directly connected, Tunnel2
B     192.168.0.0/16 [200/0] via 172.16.1.254, 00:07:27
```

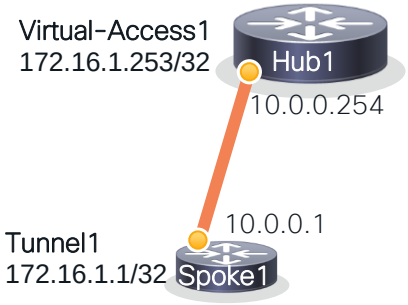
Interface and routing verification

Reference

```
Hub1# show derived-config interface Virtual-Access 1
Building configuration...

Derived configuration : 197 bytes
!
interface Virtual-Access1
 ip unnumbered Loopback1
 ip policy route-map FW
 tunnel source GigabitEthernet2
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile default
 no tunnel protection ipsec initiate
```

Derived from the Virtual-Template (show command not available on ASA/FTD)



192.168.101.0/24

```
Hub1# show ip route
S        172.16.1.1/32 is directly connected, Virtual-Access1
B        192.168.101.0/24 [200/0] via 172.16.1.1, 00:25:06
```

```
Spoke1# show ip route
S        172.16.1.254/32 is directly connected, Tunnel1
S        172.16.1.253/32 is directly connected, Tunnel2
B     192.168.0.0/16 [200/0] via 172.16.1.254, 00:07:27
```

Interface and routing verification

Reference

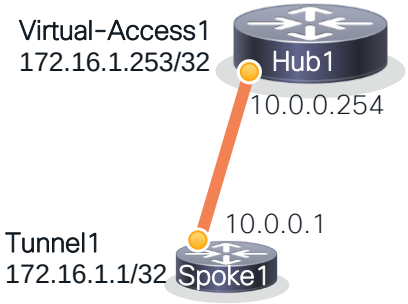
```
Hub1# show derived-config interface Virtual-Access 1
Building configuration...

Interface Virtual-Access1 "diagnostic_dynamic_vti_1_va9", is
up, line protocol is up
  Hardware is Virtual Access  MAC address N/A,
     IP address 1.1.1.1, subnet mask 255.255
  Vaccess Interface Information:
     Source IP address: 38.146.3.81
     Vaccess cloned from template 1
     Mode: ipsec ipv4    IPsec profile: FMC_IPS
     IPsec MTU Overhead : 55
```

Derived from the Virtual-Template (show command not available on ASA/FTD)

```
Hub1# show ip route
S        172.16.1.1/32 is directly connected, Virtual-Access1
B        192.168.101.0/24 [200/0] via 172.16.1.1, 00:25:06
```

```
Spoke1# show ip route
S        172.16.1.254/32 is directly connected, Tunnel1
S        172.16.1.253/32 is directly connected, Tunnel2
B     192.168.0.0/16 [200/0] via 172.16.1.254, 00:07:27
```




CISCO Live!
ALL IN