cisco Live!

ALL IN

The bridge to possible

Route Based VPNs

With Secure Firewall

Jeff Fanelli, Principal Architect
@jefanell

BRKSEC-3058

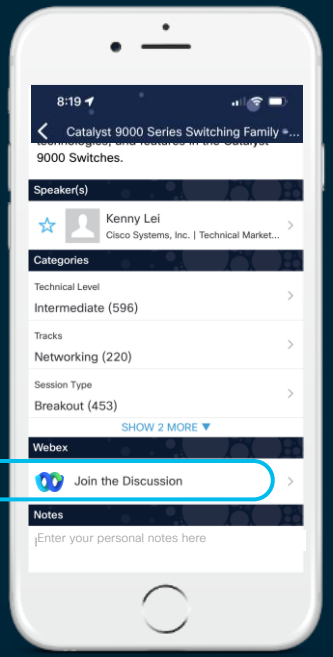
Cisco Webex App

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



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-3058

Webex spaces will be moderated by the speaker until June 17, 2022.

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

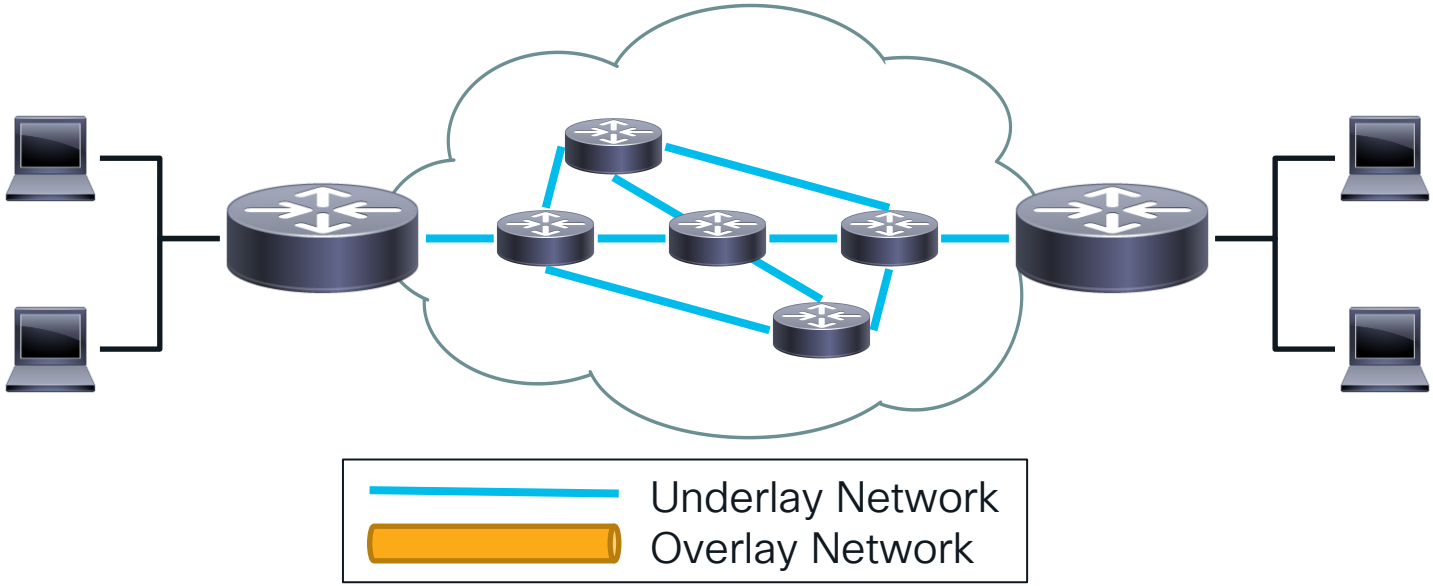
- jefanell@cisco.com
- Principal Architect
- 16 years @ Cisco
- 30+ CiscoLive! Presenter
- Husband + father
- Private pilot
- Slave to three wiener dogs

Platform names and abbreviations

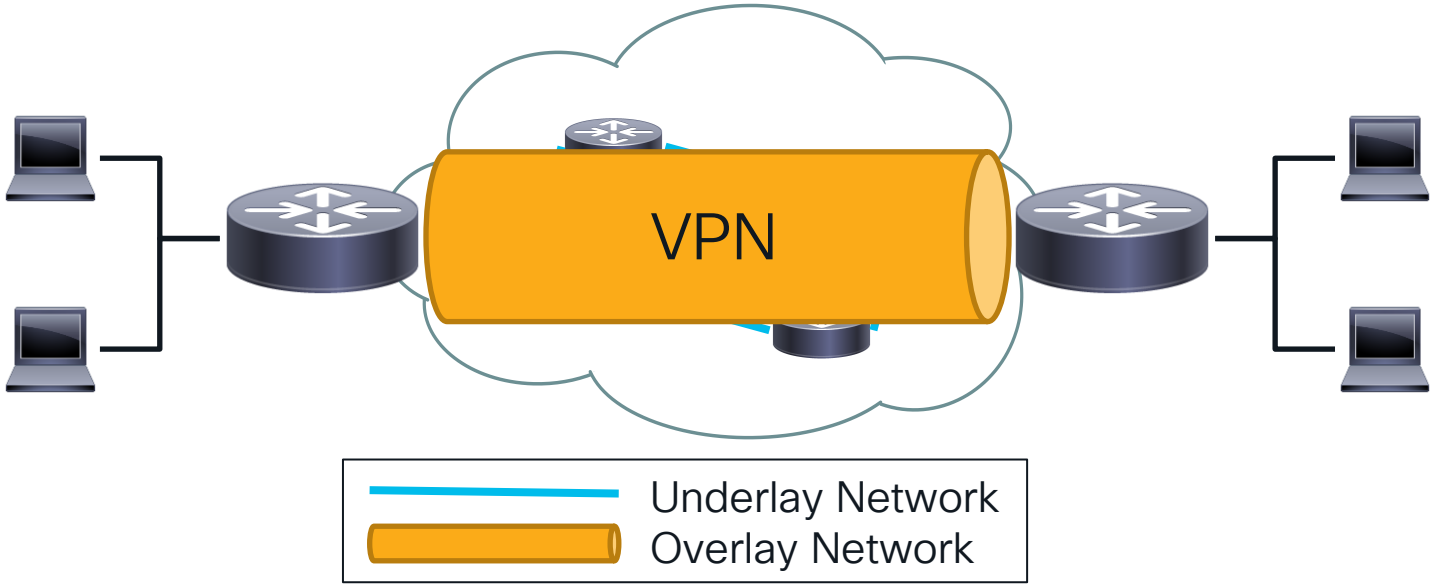
- Cisco Secure Firewall – Product line name
- Cisco Secure Firewall ASA
  - Adaptive Security Appliance “ASA” (software platform)
- Cisco Secure Firewall Threat Defense
  - Firepower Threat Defense “FTD” (software platform)
- Catalyst 8000 Edge – Product line name
  - Internet Operating System “IOS”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

VPN Technology Overview

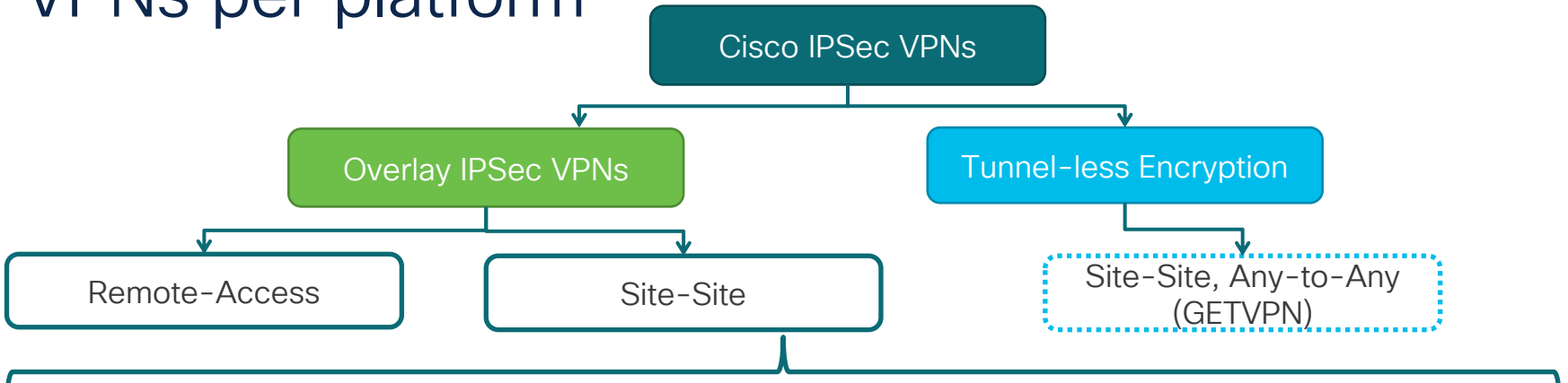
Underlay & Overlay



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

Reference

Crypto Map

- 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
```

Reference

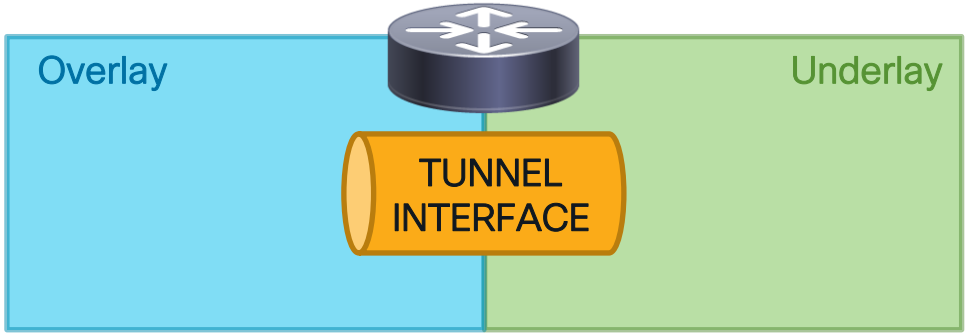
Dynamic Crypto Map

- 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
```

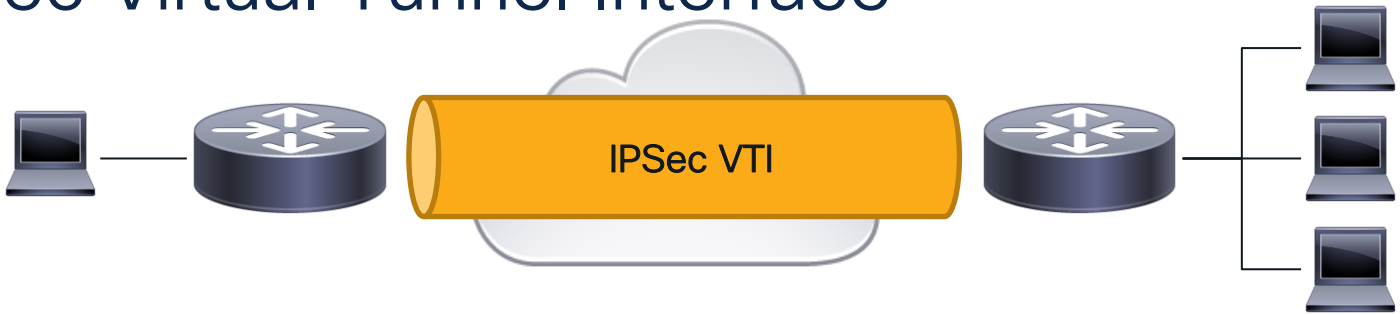
VPN Tunnel Interfaces

Tunnel Interface



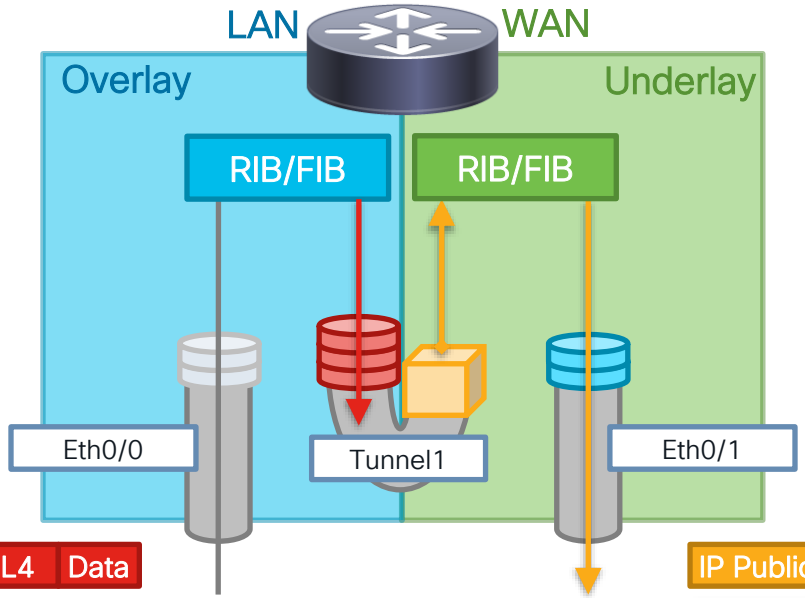
- Tunnel Interface interconnects underlay and overlay network.
- Supports various encapsulation types – GRE IPv4/IPv6, Native IPSec IPv4/IPv6
- Main building block for IOS IPSec VPNs – mGRE (DMVPN), Static/Dynamic (FlexVPN) also supported on ASA / FTD

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”)

IOS Tunnel Interface – Packet Flow




```
interface Tunnel <>
 vrf forwarding blue
 ip address <>
 tunnel mode gre ipv6
 tunnel source <>
 tunnel vrf green
 tunnel destination <>
```

- vrf forwarding blue → Overlay VRF (IVRF)
- ip address <> → Overlay IP address
- tunnel mode gre ipv6 → Tunnel encap type
- tunnel source <> → Underlay src IP address
- tunnel vrf green → Underlay VRF (FVRF)
- tunnel destination <> → Underlay dst IP address

IP Private | L4 | Data

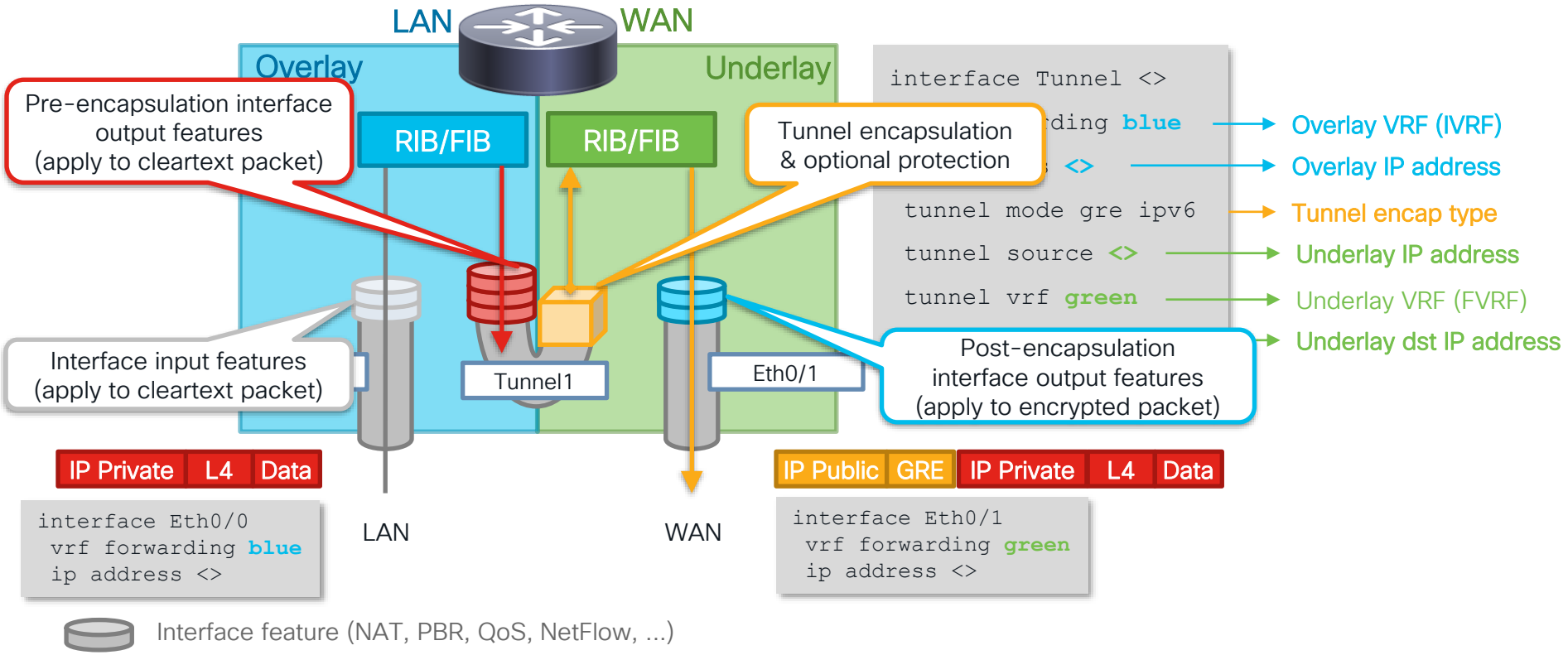
```
interface Eth0/0
 vrf forwarding blue
 ip address <>
```

IP Public | GRE | IP Private | L4 | Data

```
interface Eth0/1
 vrf forwarding green
 ip address <>
```

Interface feature (NAT, PBR, QoS, NetFlow, ...)

IOS Tunnel Interface – Packet Flow



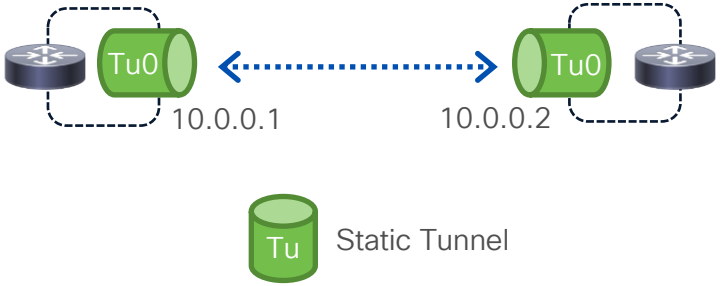
Reference

Virtual Interface Types

	GRE over IPSec	IPsec Native	CLI
Dynamic	Virtual-Template Virtual-Access Dynamic GRE/IPSec	Virtual-Template Virtual-Access DVTI DVTI Multi-SA	`interface Tunnel <>`
Static	Tunnel interface Static GRE/IPSec	Tunnel Interface SVTI SVTI Multi-SA	`interface Virtual-Template <>`

IPSec Tunnel Interface Types - Static

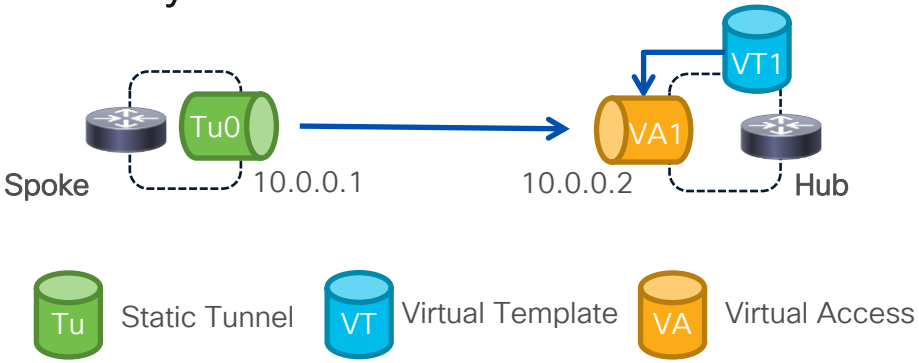
- Static Tunnel Interface




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

IPSec Tunnel Interface Types - Dynamic

- Dynamic Tunnel Interface



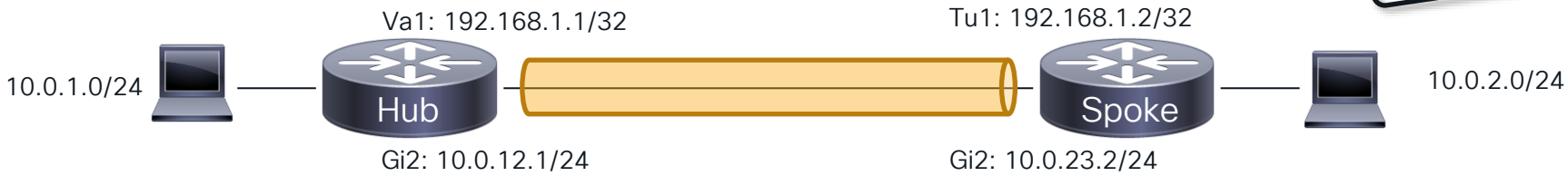
Dynamic Tunnel Interfaces (DVTI) are introduced in ASA 9.19 and FTD 7.3

```
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

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
```

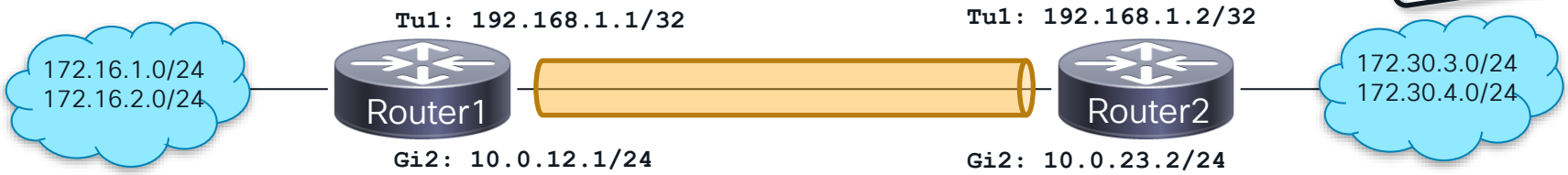
Reference

IKEv2 Multi-SA Static VTI

- 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

New ASA and FTD Features ahead!

These features are in ASA and FTD code right NOW:

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

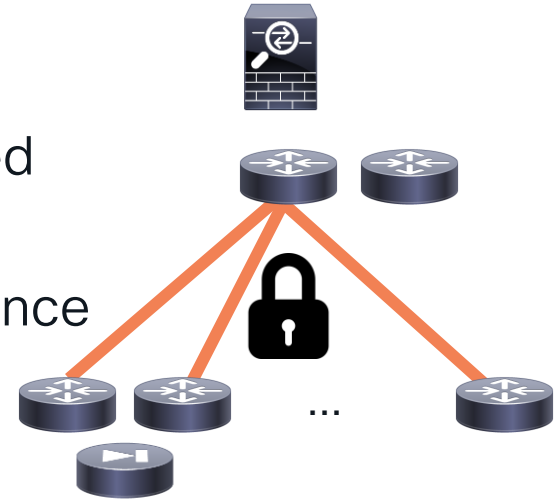
Configs shown will be ASA CLI. (identical to FTD deployed configuration)

These capabilities are coming in the ASA 9.19 / FTD 7.3 release:

- 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.

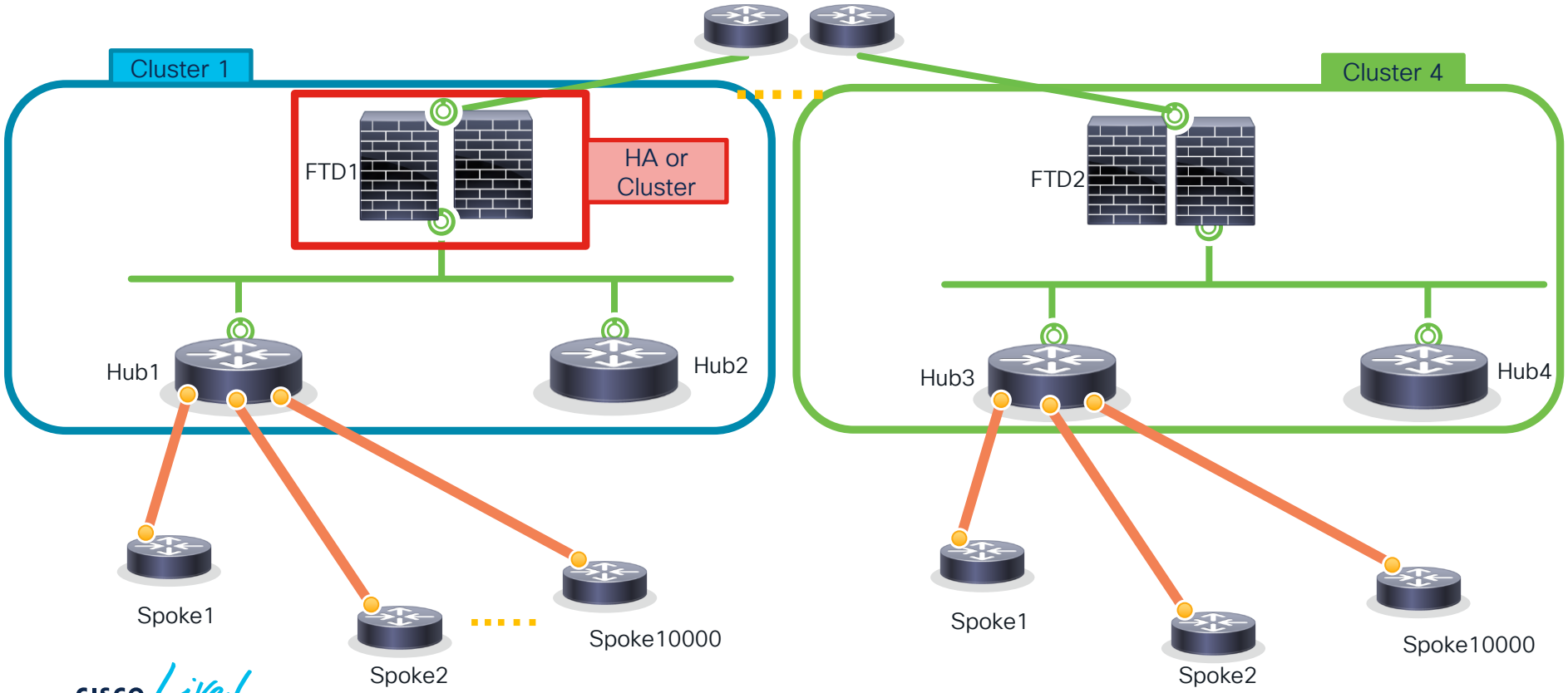
Example Design Requirements and Assumptions

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



High Level Design – Topology

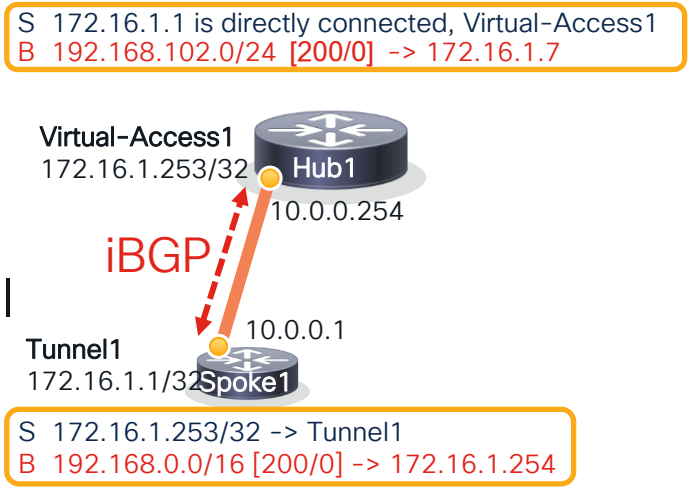
Hub-and-spoke + Large Scale



BGP routing considerations

Headend redundancy with 15 seconds convergence

- Two tunnels primary and secondary.
- Decrease BGP timers for fast convergence.
- For the BGP neighborship we need IKEv2 routing to exchange the addresses that will be used for peering.
- BGP listen range on Hub.
- Route reflector between Hubs.
- Summary advertised to spokes.

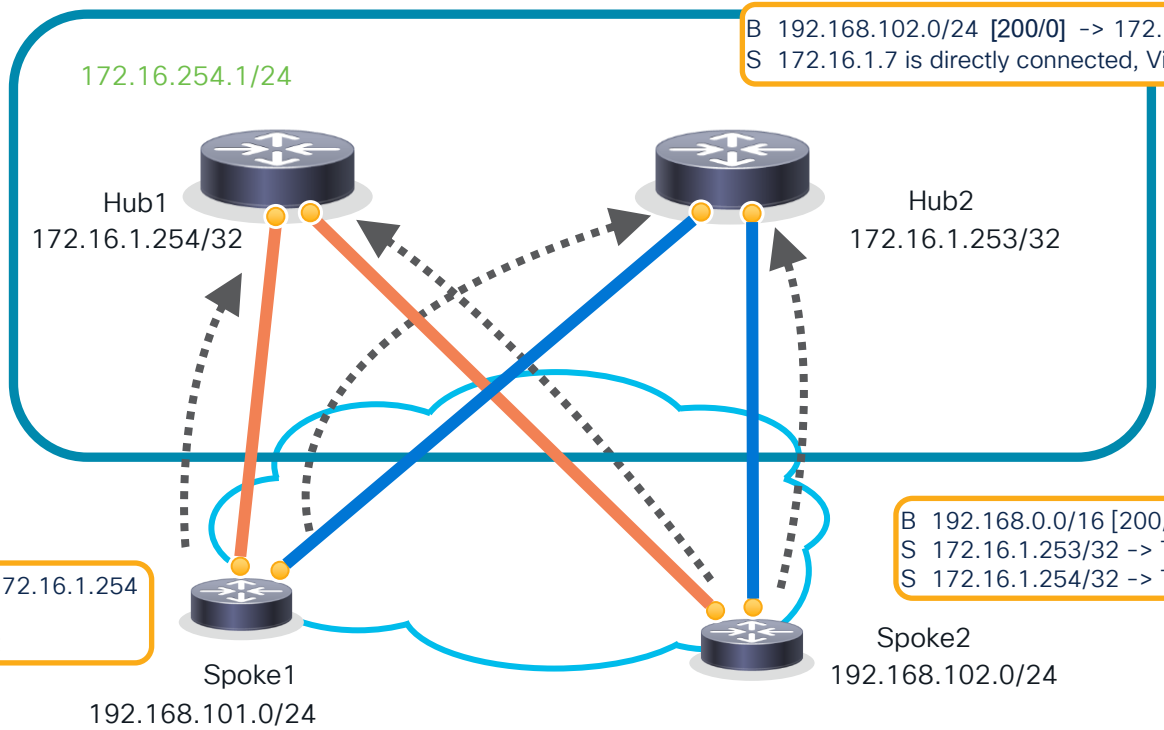


Single / Double Hub & Spoke design using VTI

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)



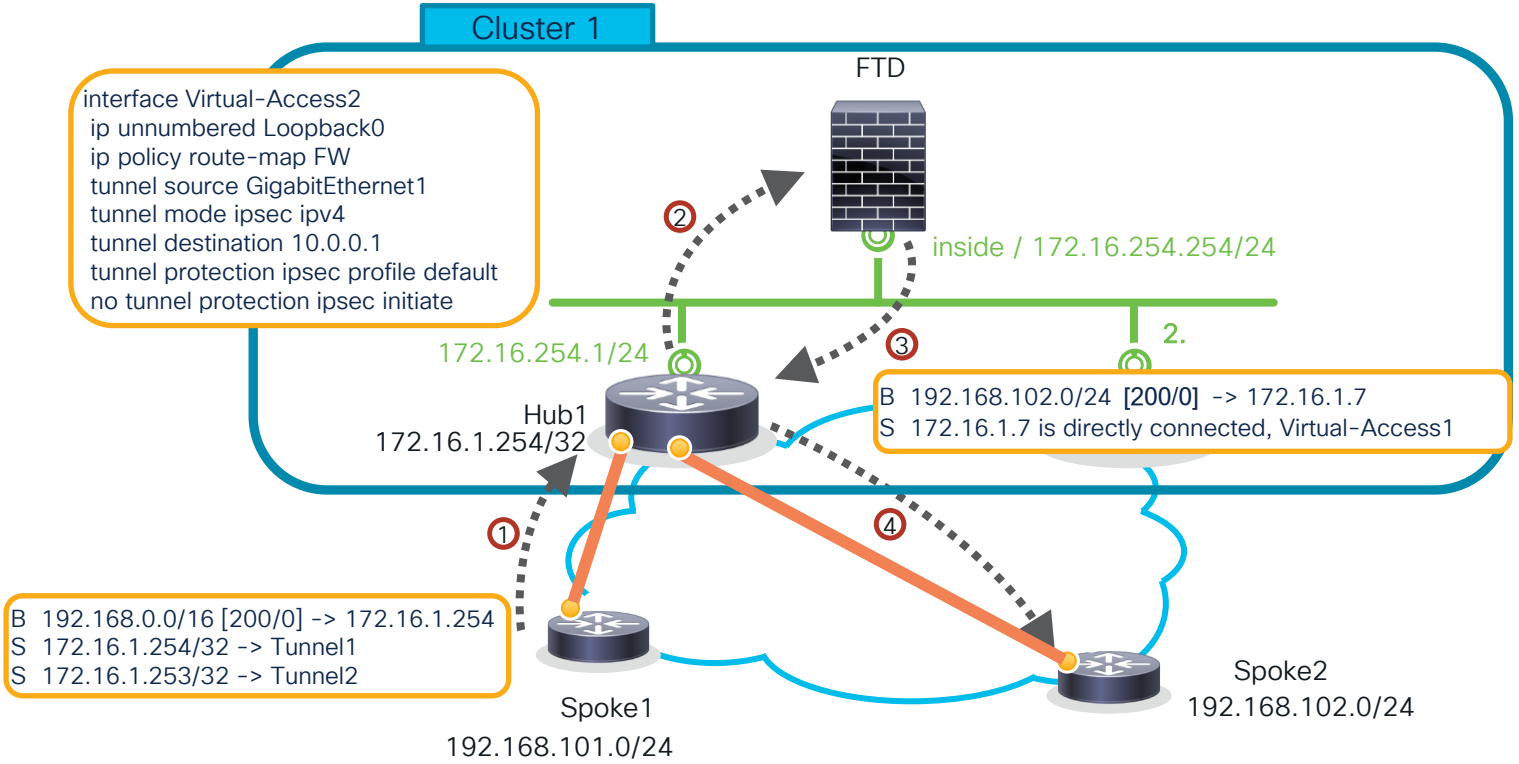

```
B   192.168.102.0/24  [200/0]  -> 172.16.1.7
S   172.16.1.7 is directly connected, Virtual-Access1
```

```
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
```

FTD Routed mode on a stick

IPS inspection for the spoke-to-spoke traffic using FTD



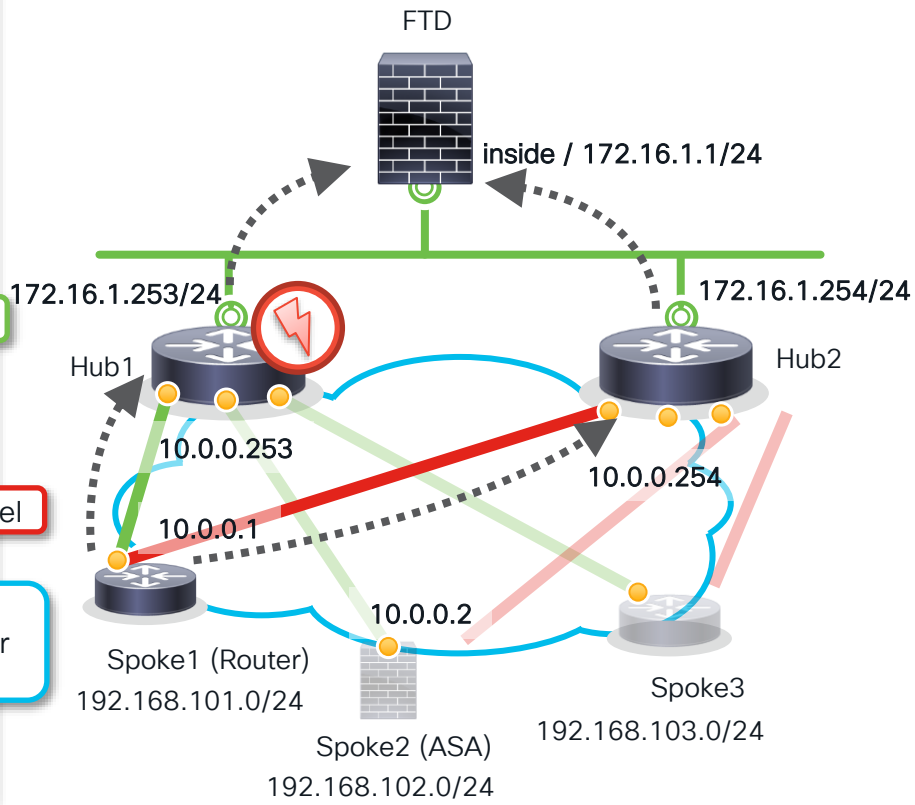
Spoke router configuration – IOS Example

```
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



Spoke ASA config – Pre ASA 9.19.1 / FTD 7.3

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

IKE Identity

IKEv2 and IPSec algorithms

pre-shared-keys

```
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 65000
  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

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 ASA config – 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
!
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
```

Secondary Tunnel

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
```

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

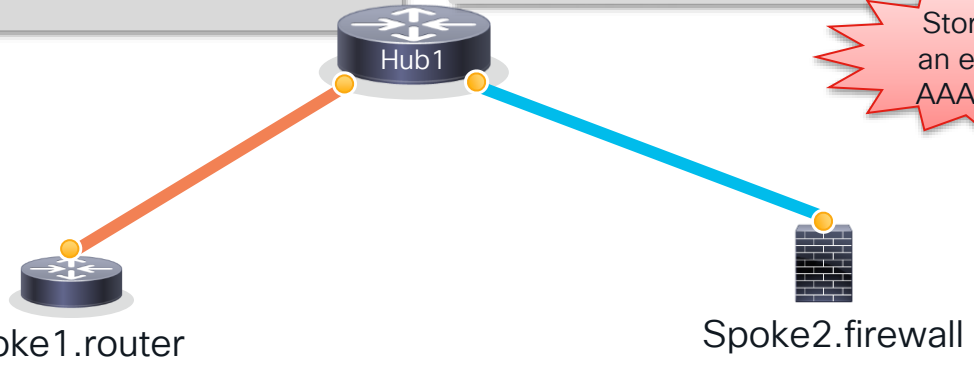
```
crypto ikev2 authorization policy router
 route set interface
```

```
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



* VTI for FTD on 6.7 roadmap

Hub router configuration – with PBR

```
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

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)

Interface and routing verification

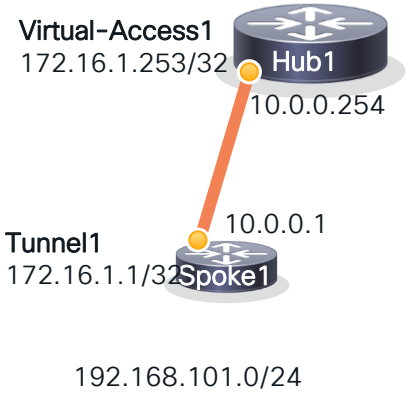
```
Hub1# show derived-config interface Virtual-Access 1
Building configuration...

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
```



Conclusions!

DO's for ASA/FTD VPNs:

- Use VTI interfaces as default choice for all site-to-site tunnels (including Cloud IaaS)
- Static or (BGP) routing protocol for VTI tunnel route peering
- Upgrade to ASA 9.19 or FTD 7.3 for DVTI HUB support! (IOS can be used today).

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.

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

CISCO SECURE

Security Reference Architecture

TALOS — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt: Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) | **ZERO TRUST**

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- ISE TrustSec
- Cisco DNA Center
- Secure Web Appliance

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

- Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

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

Thank you

cisco Live!

ALL IN