You make **possible**

cisco

Designing IPSec VPNs with Firepower Threat Defense integration for Scale and High Availability

cisco Live!

Barcelona | January 27-31, 2020

Abstract

This session covers the design and deployment aspects of integrating IPSec VPNs with Firepower Threat Defense (FTD) services. VPN (FlexVPN/DMVPN) and FTD deployment options will be reviewed with high availability and scalability in mind. The second part contains a detailed walk through of an example deployment which will help to understand the configuration and packet flow between different setup components. Proper understating of how each of the components of the deployment work is a key for successful design and operation. This session is aimed at Network Specialists and Architects involved in designing, managing and troubleshooting security solutions. This is NOT an introductory session; attendees should have existing knowledge of FlexVPN/DMVPN and FTD capabilities.

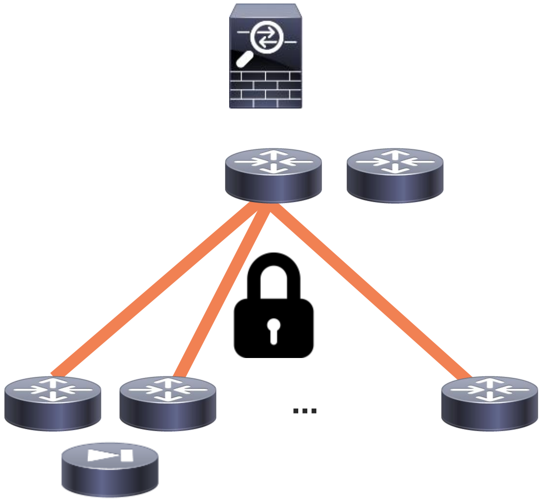
For your reference

- There are slides in your PDF that will not be presented.
- They are valuable, but included only “For your reference”.

Reference

Example Design Requitements

- Large Scale Deployment - 40000 locations
- Hub-and-spoke topology
- Provide security using cryptographically protected tunnels.
- Headend redundancy with 15 seconds convergence
- Mix of ASA and IOS routers on branch locations
- IPS inspection for the spoke-to-spoke traffic using FTD



Session Objectives

- Large scale IPSec VPN deployments, i.e. deployments exceeding single platform limits.
- VPN Design Selection.
- Understand challenges of inserting a security appliance into a VPN topology (Firewall, IPS)

Agenda

- IPSec VPN Solutions Overview
- IPSec VPN High Availability and Scalability
- Selecting a VPN Design
- FTD Deployment and Interface Modes
- FTD Resiliency and Scalability
- Scalable VPN with FTD Integration Deployment Example
- IPSec VPN Best Practices
- Conclusion

IPSec VPN Solutions Overview

IPSec VPN High Availability and Scalability

Selecting a VPN Design

FTD Deployment and Interface Modes

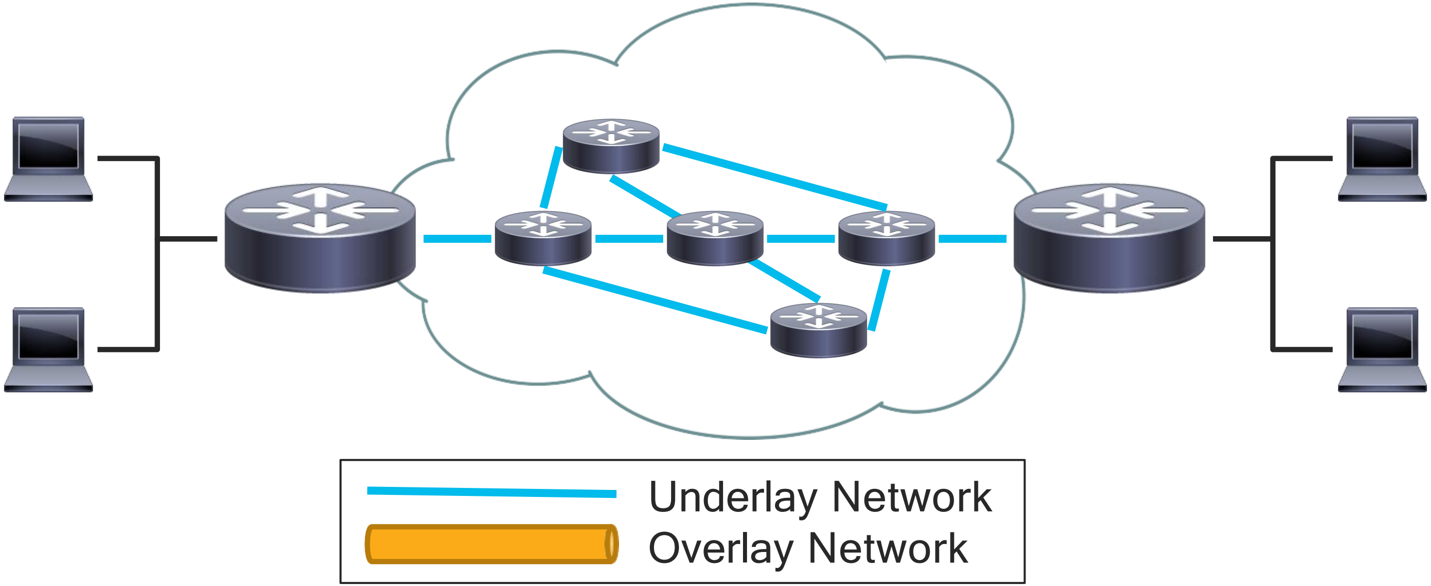
FTD Resiliency and Scalability

Scalable VPN with FTD Integration Deployment Example

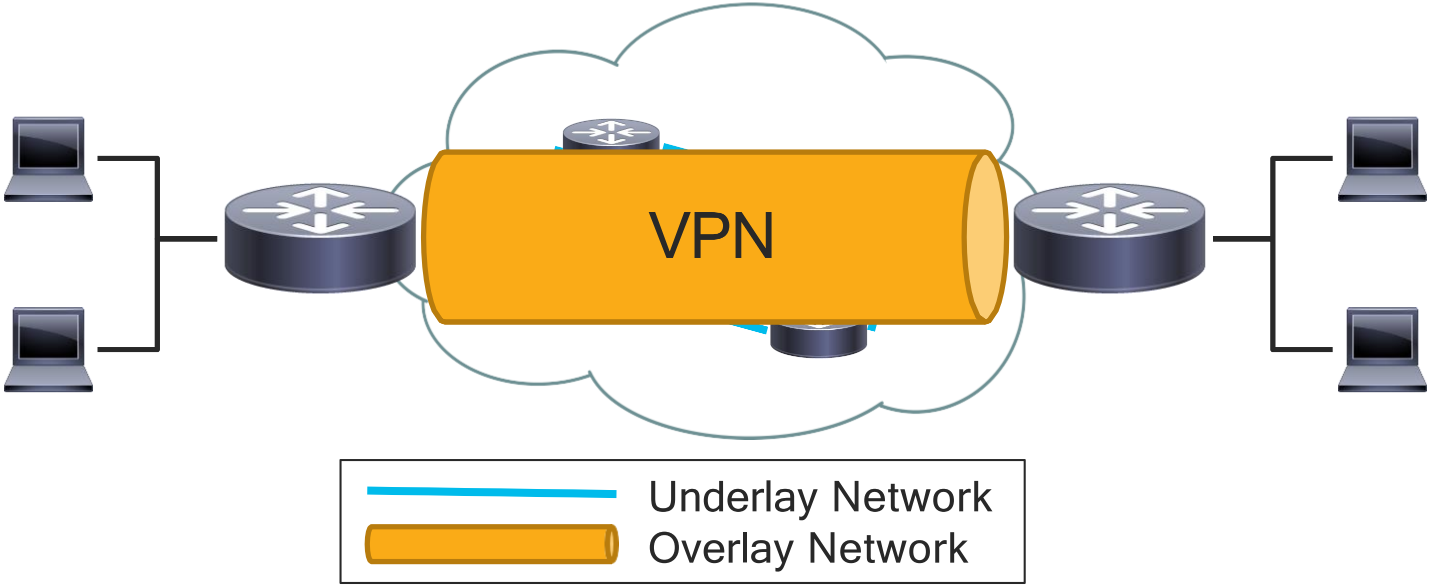
IPSec VPN Best Practices

Conclusion

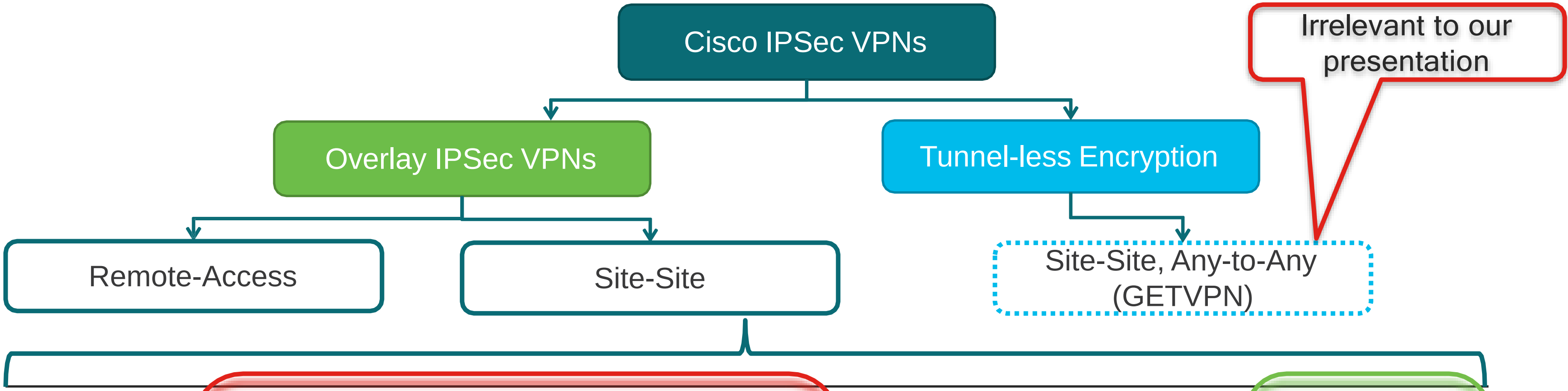
Underlay & Overlay



Underlay & Overlay



IPSec 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 (Crypto Map, GRE over IPSec w/ Crypto Map, EZVPN)

All in One (FlexVPN)

* On FTD 6.7 roadmap

** Limited integration is possible

What about SD-WAN?

Crypto Map

Reference

- Crypto Map was the first implementation of IPSec VPNs used on Cisco devices.
- Aligned to the IPsec protocol, were traffic that is about to be encrypted is defined by an ACL (crypto ACL).
- Configuration nightmare:
  - Mismatched/not mirrored ACL entries.
  - ACL must be updated every time new networks are added.

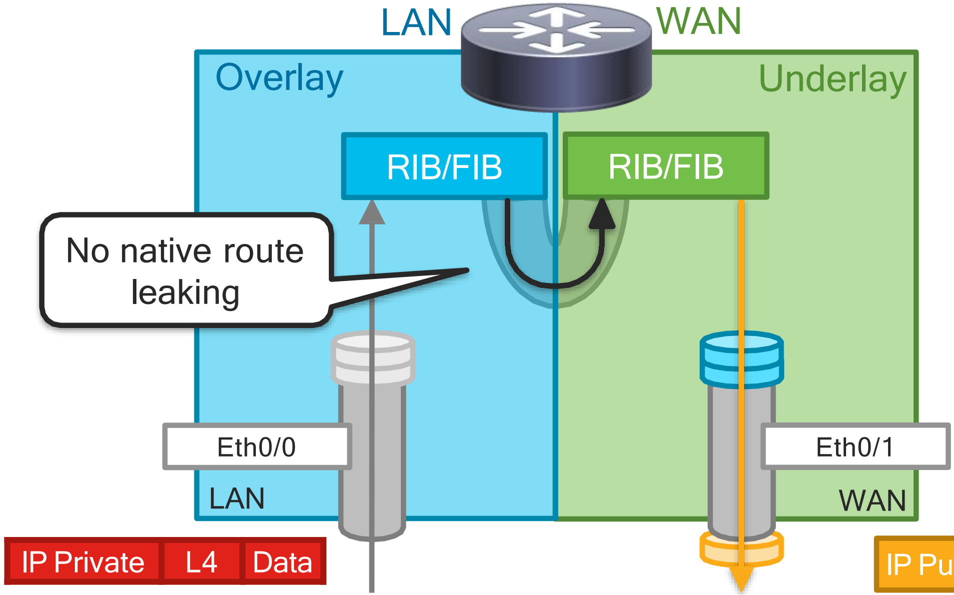
```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2

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
```

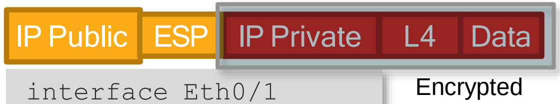
```
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set TS
 match address 110
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 crypto map outside_map
```

Crypto Map - Packet Flow

Reference




```
crypto keyring internet-keyring vrf green
 pre-shared-key address 10.1.1.2 key cisco123
!
crypto isakmp profile cust1-ike-prof
   vrf blue
   keyring internet-keyring
   match identity address 172.16.1.1 green
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
```




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

```
interface Eth0/1
 vrf forwarding green
 ip address <>
 ip nat outside
 crypto map CMAP
```

Need to know the order of operations

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

cisco Live!

Dynamic Crypto Map

Reference

- Dynamic Crypto Map dynamically accepts remote (initiating) peer's IP address.
- By default, any proposed traffic selector will be accepted from an authenticate peer.
- By design requires more TCAM space (IOS-XE).
- The DVTI technology replaces dynamic crypto maps as a dynamic hub-and-spoke method for establishing tunnels.

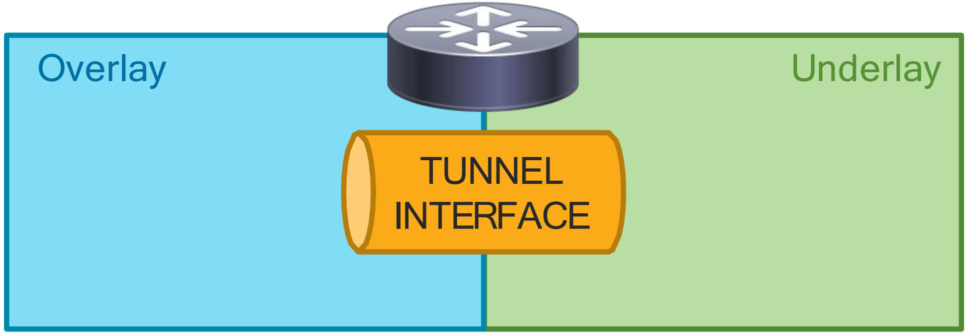
Crypto Map Summary

Reference

- Crypto Map is a legacy VPN solution with many limitations:
  - Does not support multicast.
  - A crypto map and VTI using the same physical interface is not supported.
  - It is not supported on port-channel interface (IOS-XE).
  - Multi-VRF limitations; fvrf=vrf1 and ivrf=global not supported.
  - Limited HA capabilities (IOS-XE does not support stateful IPSec failover).
  - IOS-XE architecture has scaling limitations for dynamic crypto map.
- IOS-XE IKEv2 multi-SA SVTI replaces Static Crypto Map
- IOS-XE IKEv2 multi-SA DVTI replaces Dynamic Crypto Map
- VTI on ASA 9.7.1+
- VTI on FTD – on 6.6 roadmap

Tunnel Interface

Tunnel Interface

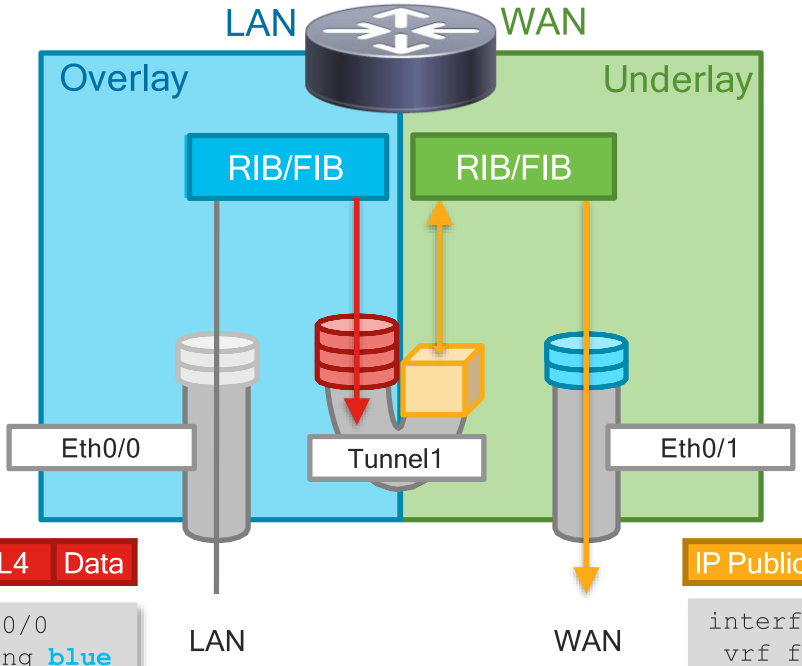


- Tunnel Interface interconnects underlay and overlay network.
- Supports various encapsulation types - GRE IPv4/IPv6, Native IPSec IPv4/IPv6
- Main building block for IOS IPSec VPNs - mGRE (DMVPN), Static/Dynamic (FlexVPN)

IPSec Virtual Tunnel Interface

- IPsec Virtual Tunnel Interface (VTI) provides a virtual routable interface for terminating IPsec tunnels and an easy way to define protection between sites to form an overlay network.
- Simplifies the configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing.
- The VTI tunnel is always up.

IOS Tunnel Interface - Packet Flow



IP Private | L4 | Data

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

IP Public | GRE | IP Private | L4 | Data

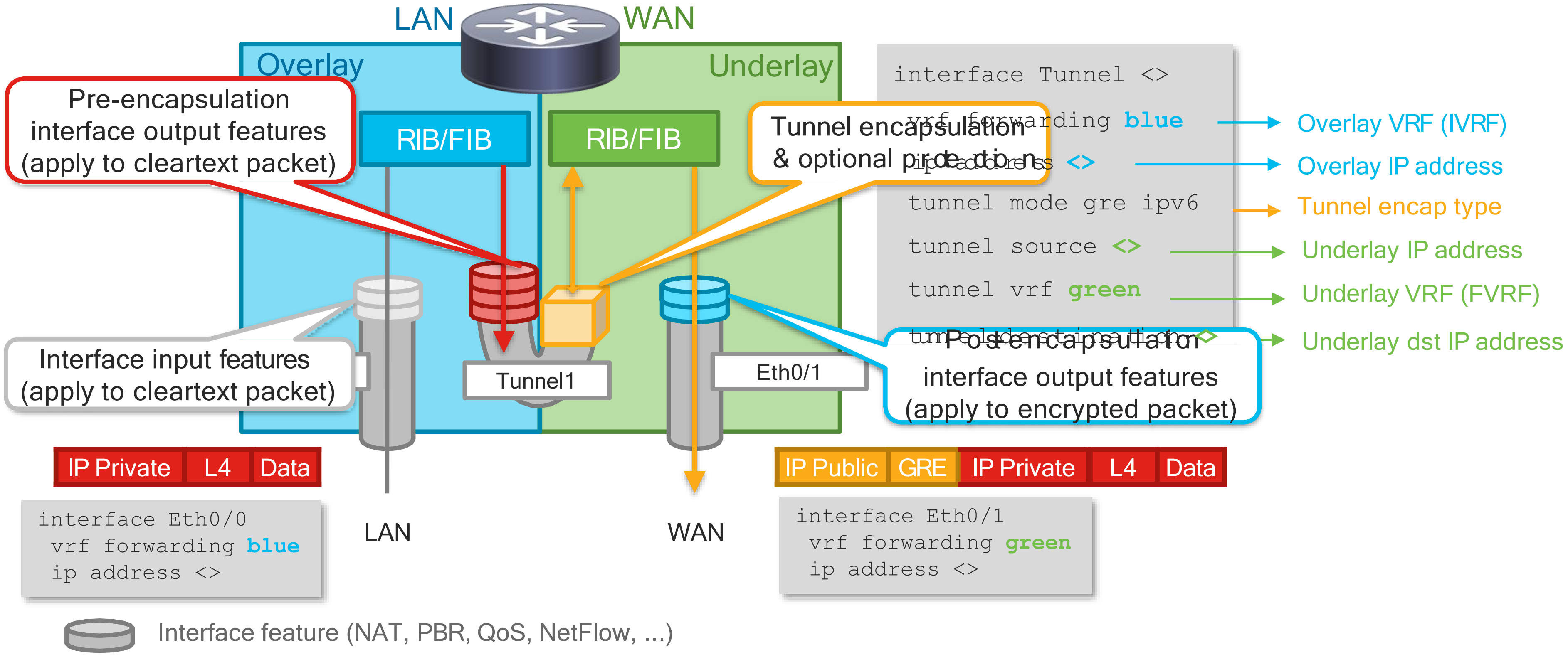
```
interface Eth0/1
 vrf forwarding green
 ip address <>
```

```
interface 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

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

IOS Tunnel Interface - Packet Flow



cisco Live!

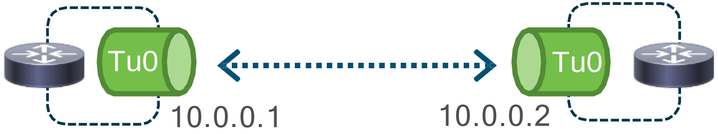
Virtual Interface Types

Reference

	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

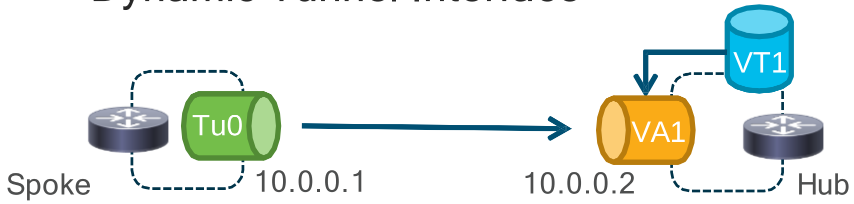



```
interface Tunnel1
 ip  unnumbered  Loopback1
 tunnel source GigabitEthernet2
 tunnel mode gre ipv4
 tunnel destination 10.0.0.2
 tunnel protection ipsec profile default
```

Static Tunnel

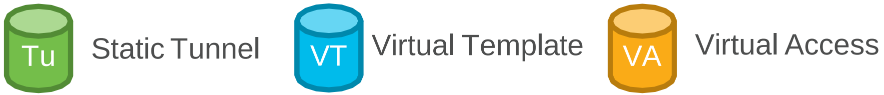
IPSec Tunnel Interface Types - Dynamic

Dynamic Tunnel Interface



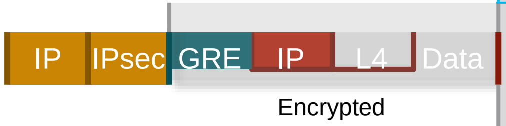

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel source GigabitEthernet2
 tunnel protection ipsec profile default
```

```
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
```



IOS Tunnel interface types - with GRE

Tunnel Type	Encapsulation	Configuration	Use Cases

Static GRE/IPSec *		`interface Tunnel <id>`
		`tunnel mode gre {ip | ipv6}`
		`tunnel protection ipsec profile default`
			• p2p GRE
			• p2p GRE over IPSec
			• FlexVPN Spoke w/ shortcuts

Dynamic GRE/IPSec		`interface Virtual-Template <id> type tunnel`
		`tunnel mode gre {ip | ipv6}`
		`tunnel protection ipsec profile default`
			• FlexVPN Hub
			• FlexVPN Spoke w/ shortcuts
			FlexVPN

mGRE over IPSec*		`interface Tunnel <id>`
		`tunnel mode gre multipoint [ipv6]`
		`tunnel protection ipsec profile default`
			• DMVPN
			DMVPN

- Enables tunneling of non-IP protocols (e.g. MPLS, NHRP)
- Required for dynamic mesh scenarios
- *"tunnel mode gre ip"* is the default on static and dynamic tunnel interfaces

* IPSec protection is optional

IOS Tunnel interface types - without GRE

Tunnel Type	Encapsulation	Configuration	Use Cases

Native IPsec (SVTI)	IP | IPsec | IP | L4 | Data (Encrypted: IP | L4 | Data)	`interface Tunnel <id>`
		`tunnel mode ipsec {ipv4 | ipv6}`
		`tunnel protection ipsec profile default`
			• p2p IPSec
			• FlexVPN Spoke w/o shortcuts
			• FlexVPN inter-Hub

Native IPsec (DVTI)		`interface Virtual-Template <id> type tunnel`
		`tunnel mode ipsec {ipv4 | ipv6}`
		`tunnel protection ipsec profile default`
			• FlexVPN Hub w/o shortcuts
			FlexVPN

Native IPsec Multi-SA SVTI	16. 12.1	`interface tunnel <id>`
		`tunnel mode ipsec <ipv4|ipv6>`
		`tunnel protection ipsec profile default`
		`tunnel protection ipsec policy ipv4 ACL`
			• Static Crypto Map replacement for 3rd party peers

Native IPsec Multi-SA DVTI	15.2(1)T+	`interface Virtual-Template <id> type tunnel`
		`tunnel mode ipsec {ipv4 | ipv6}`
		`tunnel protection ipsec profile default`
			• Dynamic Crypto Map replacement for 3rd party peers

FlexVPN
Crypto Map compatibility

- Less overhead - no GRE
- Multi-SA support
- Mixed Mode - IPv4 over IPv6 (`tunnel mode ipsec ipv4 v6-overlay`) or vice versa

cisco Live!

Traffic Permitted by Protection Type

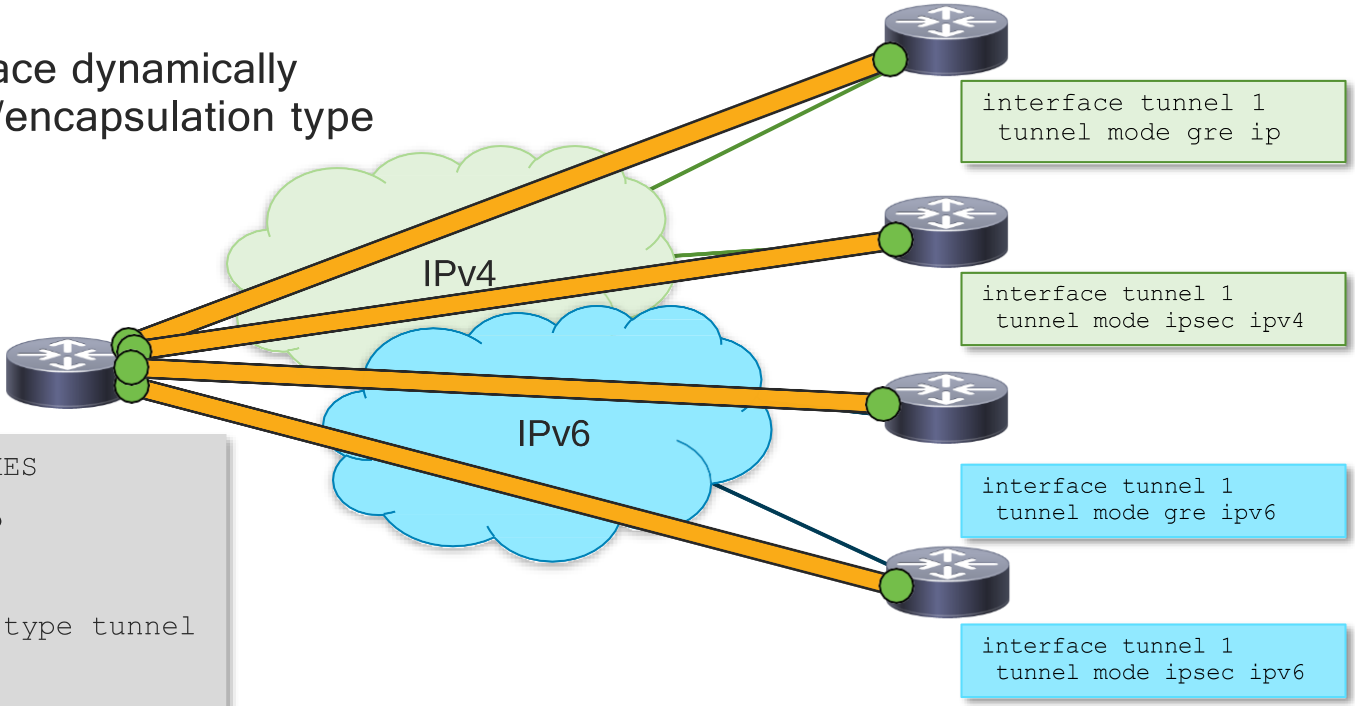
	IPv4 only	IPv6 only	IPv4 & IPv6 (Dual Stack)	IP Multicast	Non-IP
Crypto Map	Yes	Yes	No	No	No
Native IPsec IPv4 Tunnel (SVTI/DVTI)	Yes	Yes	No	Yes	No
Native IPsec IPv6 Tunnel (SVTI/DVTI)	Yes	Yes	No	Yes	No
GRE over IPSec*	Yes	Yes	Yes	Yes	Yes

Recommended

* With Static and Dynamic Tunnel

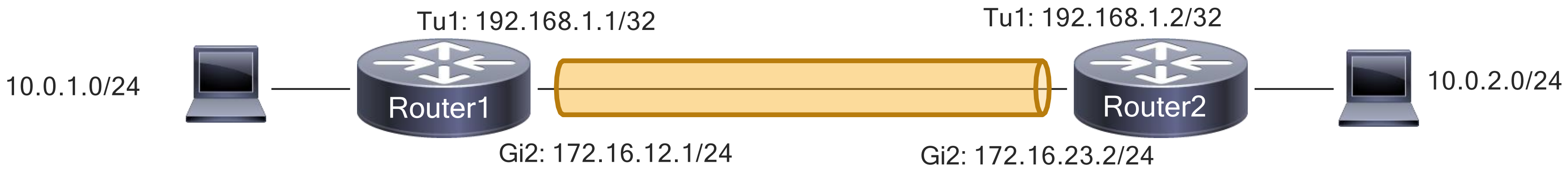
FlexVPN - Mode Auto to Rule Them All

- Automatic transport and encapsulation protocol detection
- Virtual-Access interface dynamically adjusted to transport/encapsulation type




```
crypto ikev2 profile ALL-SPOKES
 virtual-template 1 mode auto
!
interface virtual-template 1 type tunnel
 tunnel mode gre ip
```


FlexVPN Configuration Example



Router1

Smart Defaults

```
crypto ikev2 authorization policy default
 route set remote ipv4 10.0.1.0 255.255.255.0
!
crypto ikev2 profile default
 match identity remote address 172.16.23.2
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list flex default local
!
interface Tunnel1
 ip unnumbered Loopback1
 tunnel source GigabitEthernet2
 tunnel destination 172.16.23.2
 tunnel protection ipsec profile default
```

IKEv2 Routing – pushing a static route to a remote peer

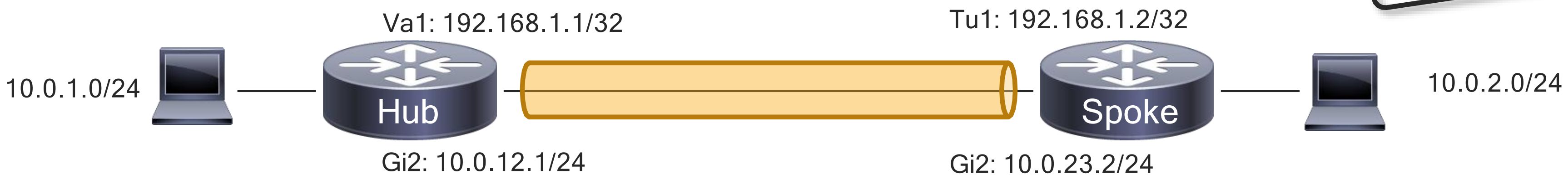
IKEv2 Profile - repository of nonnegotiable parameters of the IKE SA

Tunnel Interface defining tunnel endpoints, encapsulation and IPSec protection

BRKSEC-3054 - IOS FlexVPN Remote Access, IoT and Site-to-Site advanced Crypto VPN Designs
Thursday, January 30 | 11:00 AM - 01:00 PM

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
```

IKEv2 Multi-SA Static VTI

Reference

IOS XE 16.12.1

- 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.
- 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
```

IKEv2 Multi-SA Dynamic VTI

Reference

15.2(1)T+

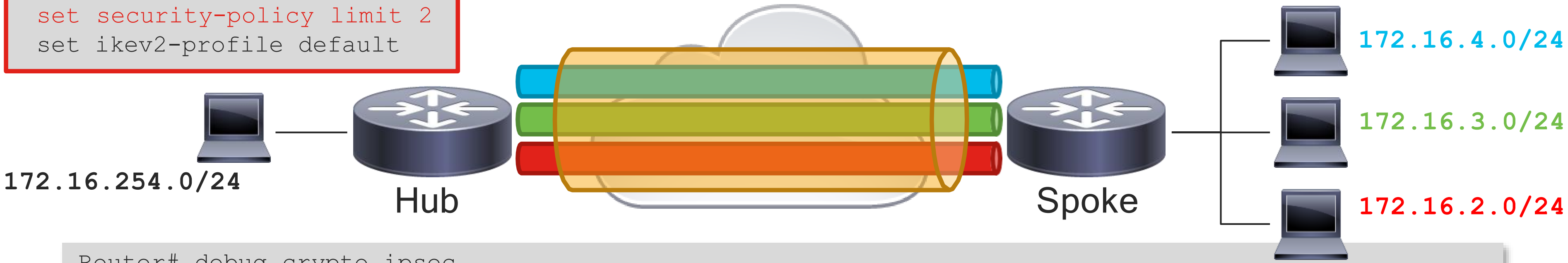
- IKEv2 DVTI supports multiple IPsec SAs proposed by the initiator - Multi-SA DVTI
- Multi-SA DVTI is interoperable with third-party devices that implement only crypto maps.
- DVTI allow per peer features to be applied on a dedicated interface.

Multi-SA DVTI - security-policy limit

Reference

```
Hub# show crypto session detail
  IPSEC FLOW: permit ip 172.16.254.0/255.255.255.0 172.16.4.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4607999/3353
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4607999/3353
  IPSEC FLOW: permit ip 172.16.254.0/255.255.255.0 172.16.3.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4607999/3342
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4607999/3342
```

```
crypto ipsec profile default
 set security-policy limit 2
 set ikev2-profile default
```




```
Router# debug crypto ipsec
(…)
*Nov 28 12:12:40.609: IPSEC(vti_multi_sa): Maximum SA limit has reached. Dropping the connection
```

IKEv2 Multi-SA DVTI - Configuration

Reference

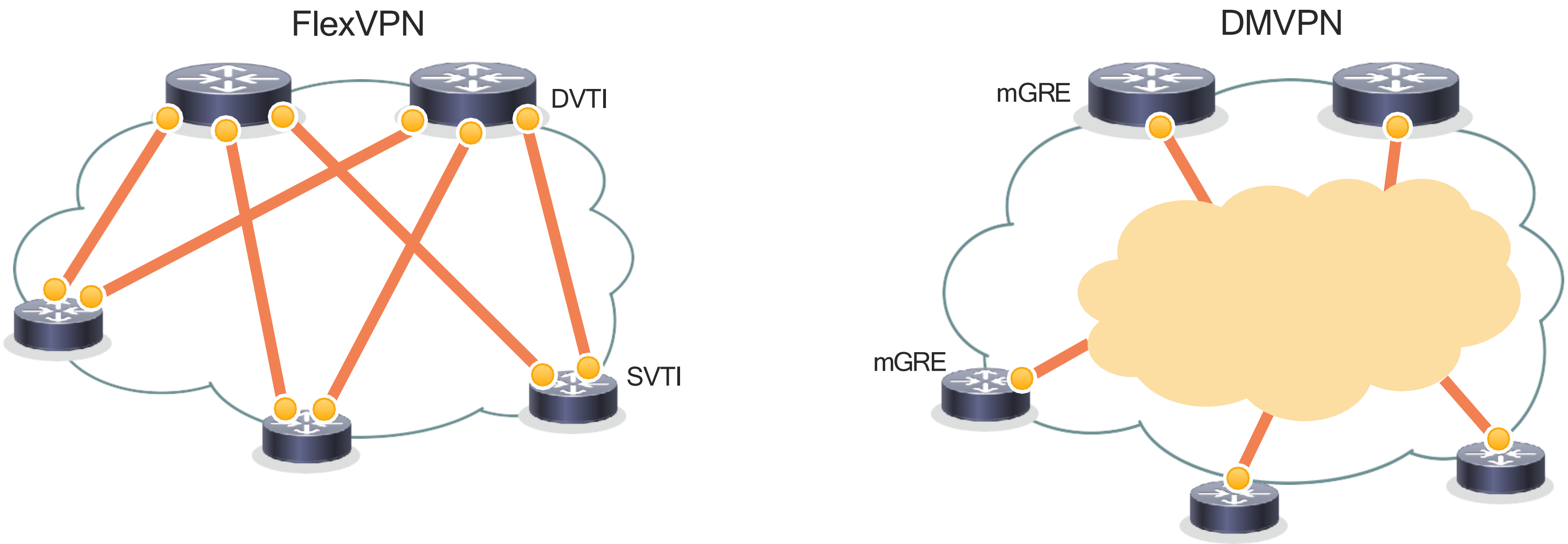
Hub - IKEv2 Multi-SA DVTI

Spoke - IKEv2 Crypto Map

```
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 default default
!
access-list 100 permit ip 10.0.12.0/24 10.0.0.0/16
access-list 100 permit ip 10.0.13.0/24 10.0.0.0/16
access-list 100 permit ip 10.0.14.0/24 10.0.0.0/16
!
crypto map CMAP 10 ipsec-isakmp
 set peer 10.0.0.1
 set ikev2-profile default
 match address 100
!
interface GigabitEthernet2
 ip address 172.16.1.1 255.255.255.0
 crypto map CMAP
```

FlexVPN and DMVPN comparison

Reference



- DMVPN uses mGRE interface while FlexVPN is using p2p tunnels - SVTI or DVTI.
- In DMVPN crypto is optional, FlexVPN is tied to crypto configuration and requires IKEv2.
- If direct spoke-to-spoke is not needed, GRE encapsulation can be omitted for FlexVPN.

FlexVPN and DMVPN comparison

Reference

- Compatibility with any IKEv2-based third-party VPN vendors
- IKEv2 routing – very light solution fit for IoT
- Point-to-point tunnel interfaces instead of mGRE
- Granular per tunnel configuration of QoS, ZBF, VRF, etc. (AAA server)
- Simplified use of NHRP – no NHS registration
- One way of configuring NHRP compared to 3 phases in DMVPN

Demo - FlexVPN

IPSec VPN Solutions Overview

IPSec VPN High Availability and Scalability

Selecting a VPN Design

FTD Deployment and Interface Modes

FTD Resiliency and Scalability

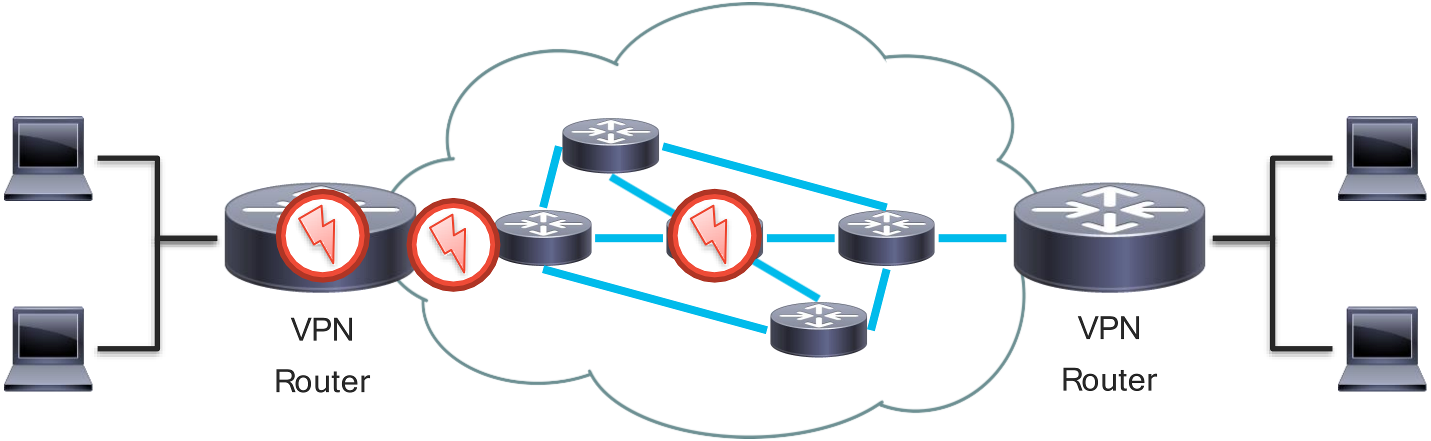
Scalable VPN with FTD Integration Deployment Example

IPSec VPN Best Practices

Conclusion

Designing Fault-Tolerant IPSec VPNs

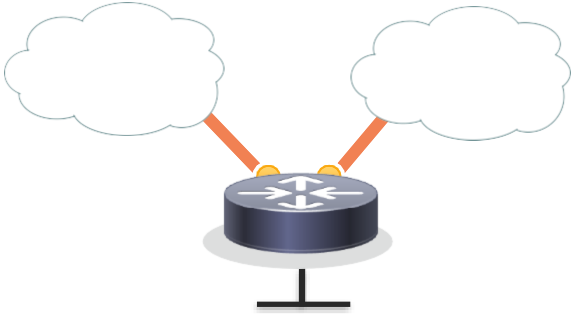
- The design depends on what faults the VPN needs to be able to withstand.
- From the fault-tolerance perspective, the design can be broken down into:
  - Transport Network - connectivity between IPSec Gateways
  - Access Link - link/device that connects the IPSec gateway to the Transport Network
  - IPSec Gateway



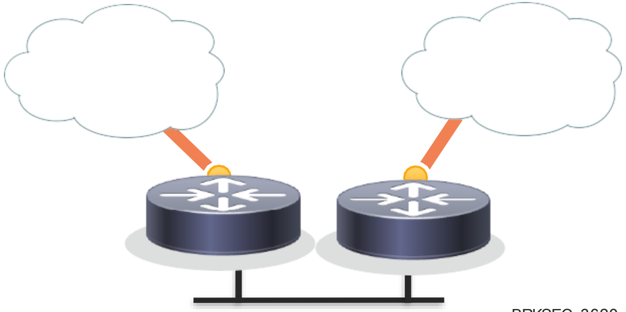
Branch Location Design

- Single-Router, Single-Link

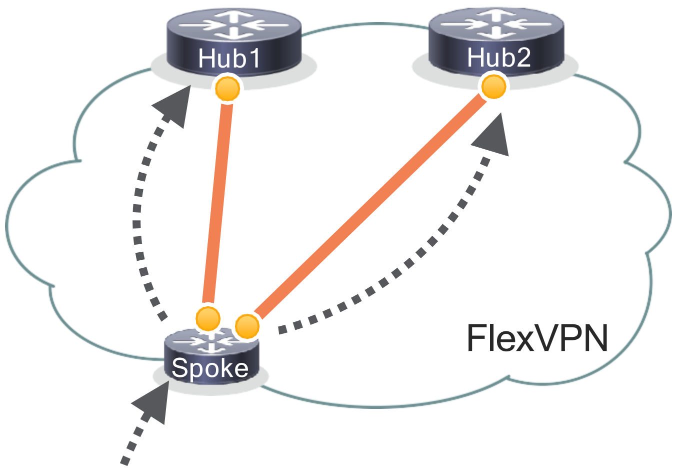
- Single-Router, Dual-Link



- Dual-Router, Dual-Link

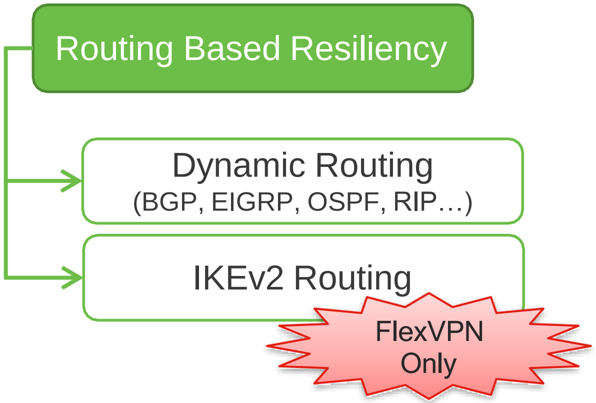


FlexVPN Hub Redundancy - active-active




```
interface Tunnel1
 (…)
 tunnel destination <hub1-nbma-ip>

interface Tunnel2
 (…)
 tunnel destination <hub2-nbma-ip>
```



In case of link/hub failure, dynamic routing protocol timers or IKEv2 DPD timers determine the convergence time

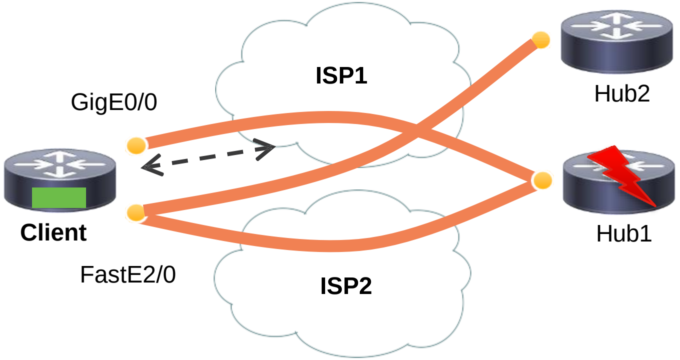
Tunnel Origin/Destination Dynamic Modification

FlexVPN Only

Tunnel Origin/Destination

- **Tunnel Peer Selection**
  - Backup Peer List
  - Static or Downloadable
  - Peer State Tracking
  - Peer re-activation
  - Backup Groups
  - Load-Balancing
- **Tunnel Source Selection**
  - Tunnel Pivoting

```
crypto ikev2 client flexvpn <name>
 client connect tunnel 1
 peer 1 <address> track 10 up
 peer 2 <address> track 10 down
 source 1 <primary interface> track 100
 source 2 <cellular interface> track 200
!
interface Tunnel1
 (…)
 tunnel source dynamic
 tunnel destination dynamic
```

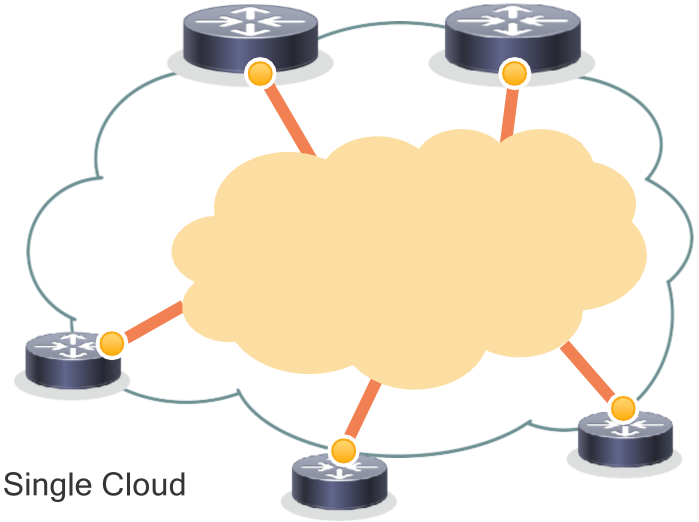


Reference

DMVPN Hub Redundancy

Reference

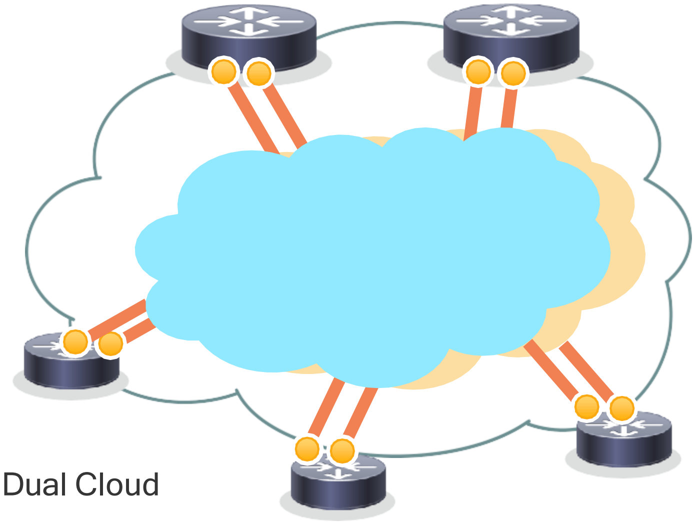
DMVPN



Dual hub - Single Cloud

```
interface Tunnel1
 (…)
 ip nhrp nhs <hub-tunnel> nbma <hub1-nbma-ip> multicast
 ip nhrp nhs <hub-tunnel> nbma <hub2-nbma-ip> multicast
```

DMVPN



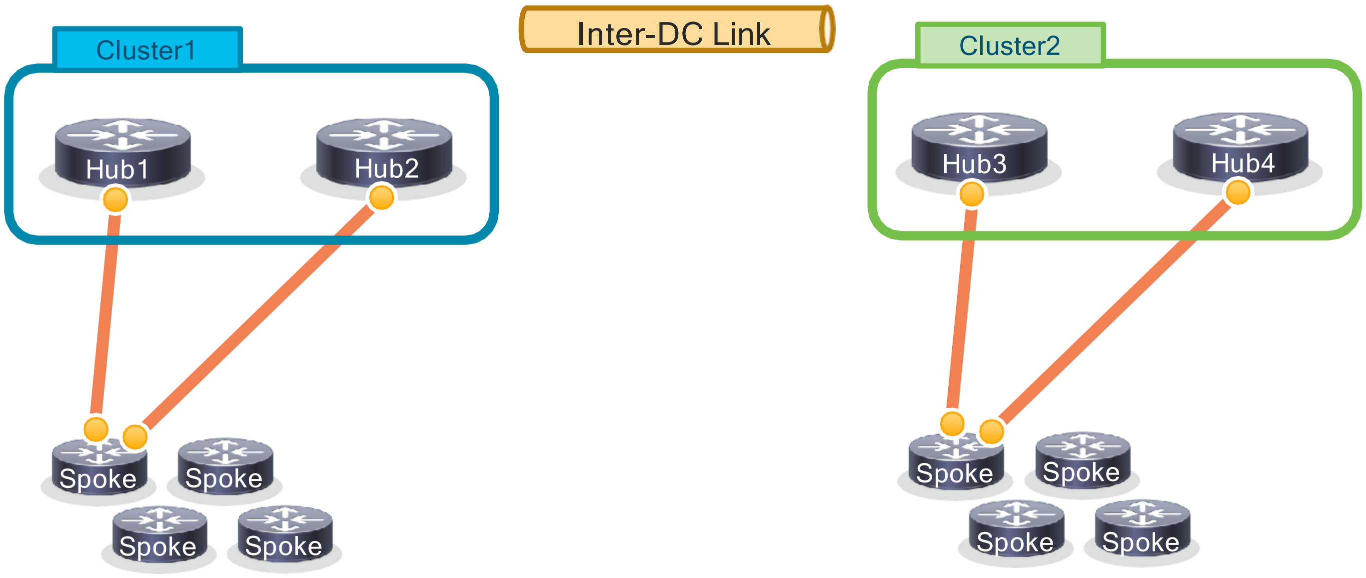
Dual hub - Dual Cloud

```
interface Tunnel1
 (…)
 ip nhrp nhs <hub-tunnel> nbma <hub1-nbma-ip> multicast

interface Tunnel2
 (…)
 ip nhrp nhs <hub-tunnel> nbma <hub2-nbma-ip> multicast
```

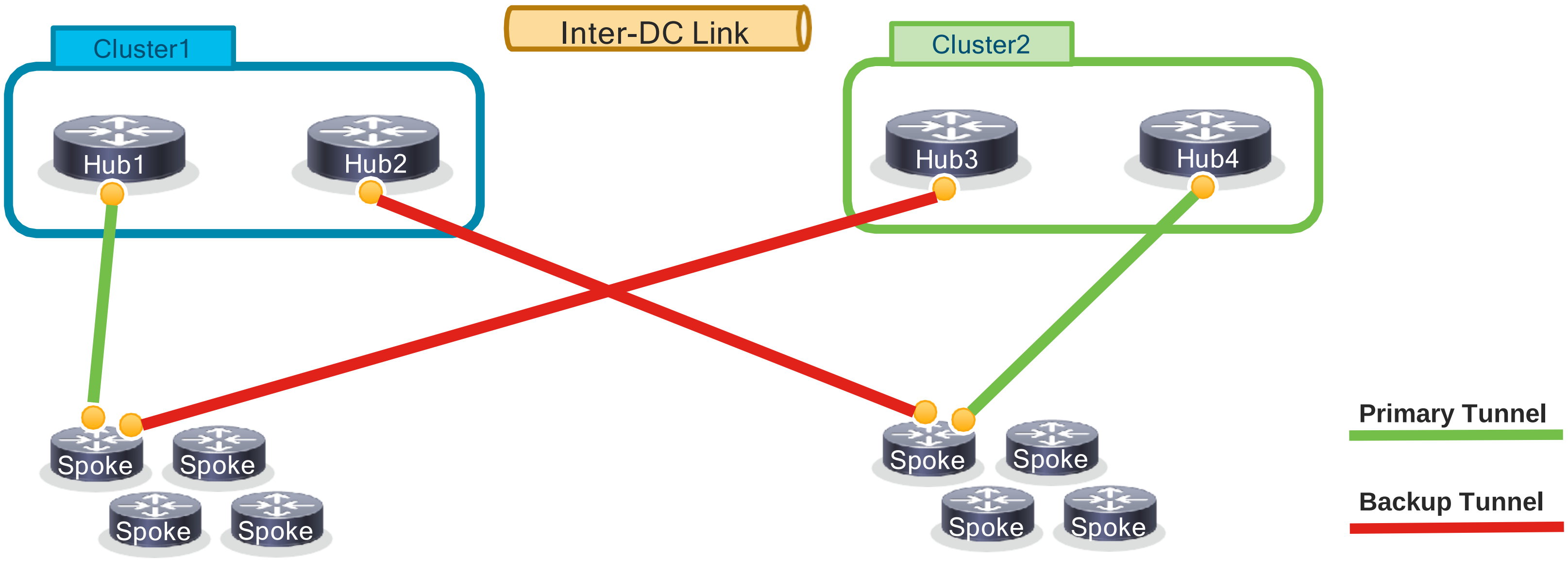
Scaling beyond the limits of one hub router
Static assignment active/standby cluster

- Multiple clusters for scale
- 1+1 redundancy



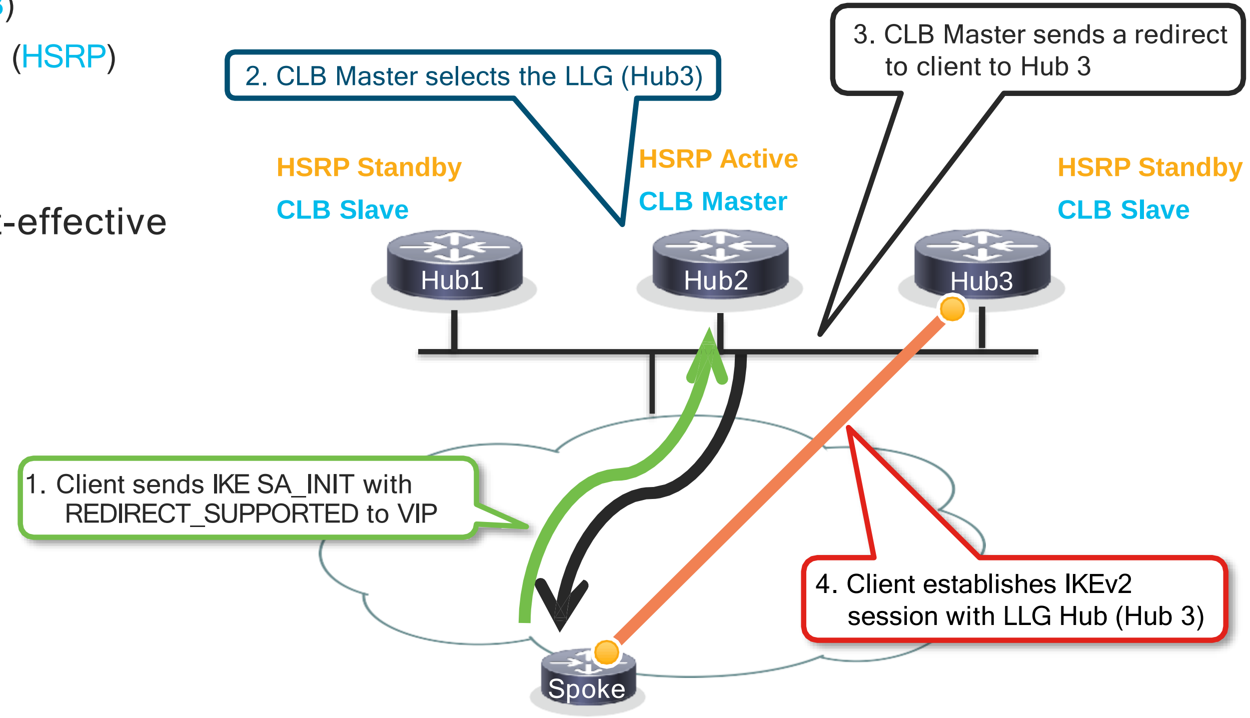
Scaling beyond the limits of one hub router
Static assignment active/standby cluster

- Multiple clusters for scale
- 1+1 redundancy



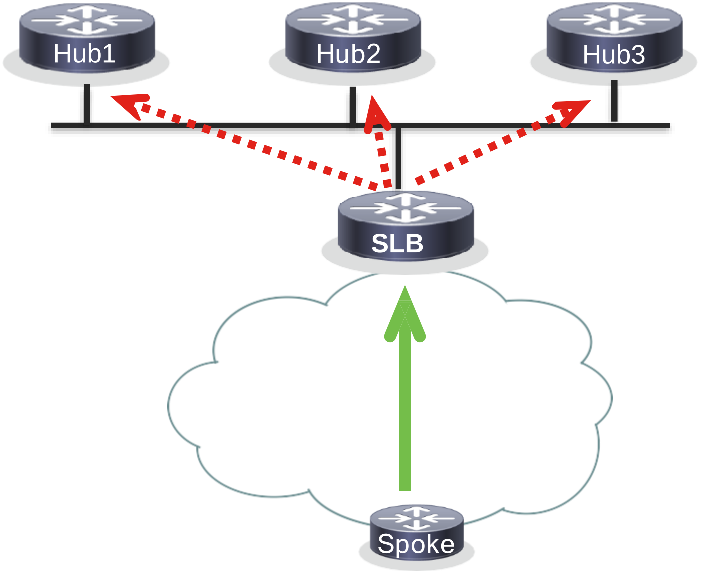
Scaling beyond the limits of one hub router
IKEv2 Load Balancer

- IKEv2 Load Balancer Components:
  - Cluster Load Balancing (CLB)
  - Hot Standby Router Protocol (HSRP)
  - IKEv2 Redirect
- N+1 redundancy (N<5)
- Easy to configure and cost-effective

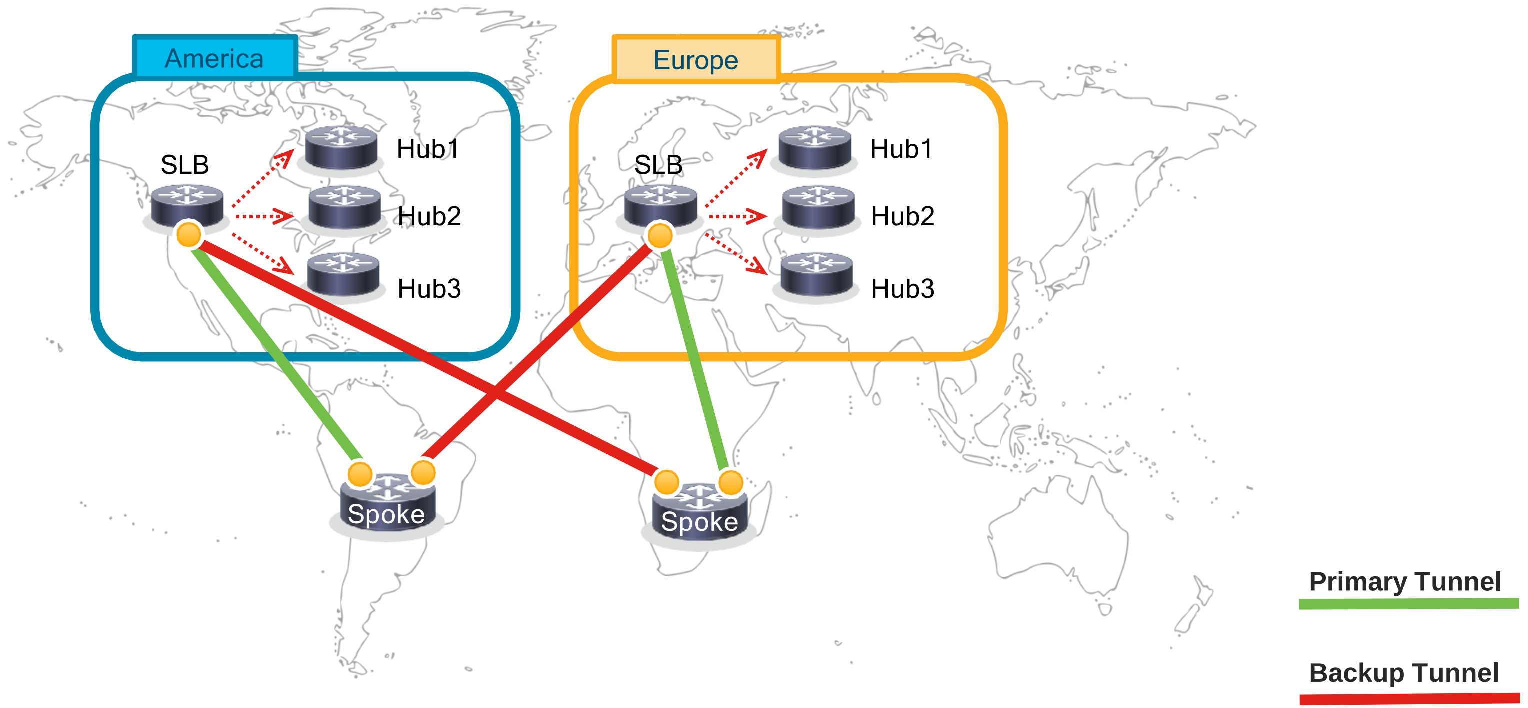


Scaling beyond the limits of one hub router
Server Load Balancing

- SLB (Server Load Balancing)
- N+1 redundancy with N >> 5
- SLB options:
  - Nexus (Intelligent Traffic Director)
  - F5 SLB
  - A10 Thunder SLB
- Today, we have designs in 100K+ (250K known), tested with 1M.



Bringing it all together - Geo LB + SLB



Selecting a VPN Design

- Large or small number of branch offices?
  - Small Scale -> Static Tunnels
  - Large Scale -> Dynamic Tunnels on Hub + Clustering, DNS Balancing, IKEv2 Load Balancer, SLB
- What level of high availability is required?
- Is direct spoke-to-spoke required?
- What protocols will be transported?
  - Non-IP -> GRE required
  - Dual stack -> GRE required
- 3rd party support?
  - Crypto Map -> FlexVPN (Multi-SA SVTI/DVTI)
- DMVPN or FlexVPN?

IPSec VPN Solutions Overview

IPSec VPN High Availability and Scalability

Selecting a VPN Design

FTD Deployment and Interface Modes

FTD Resiliency and Scalability

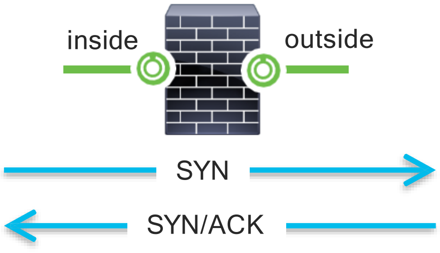
Scalable VPN with FTD Integration Deployment Example

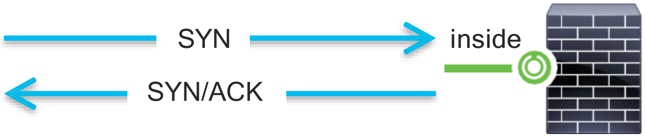
IPSec VPN Best Practices

Conclusion

Firewall - Asymmetric Traffic Challenge

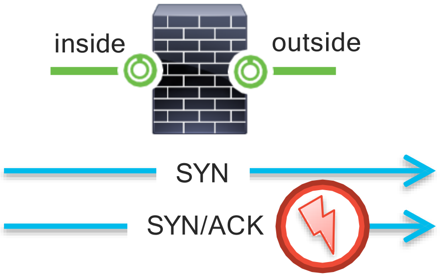
- Symmetric flow example:

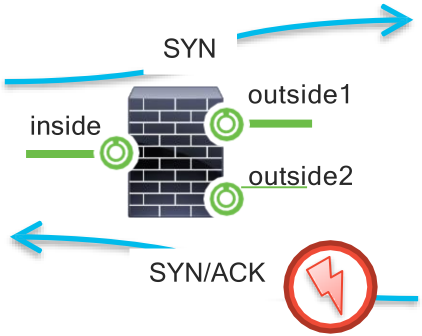




same-security-traffic is not applicable on FTD. Traffic is allowed for both inter- and intra-interface

- Asymmetric flow examples:



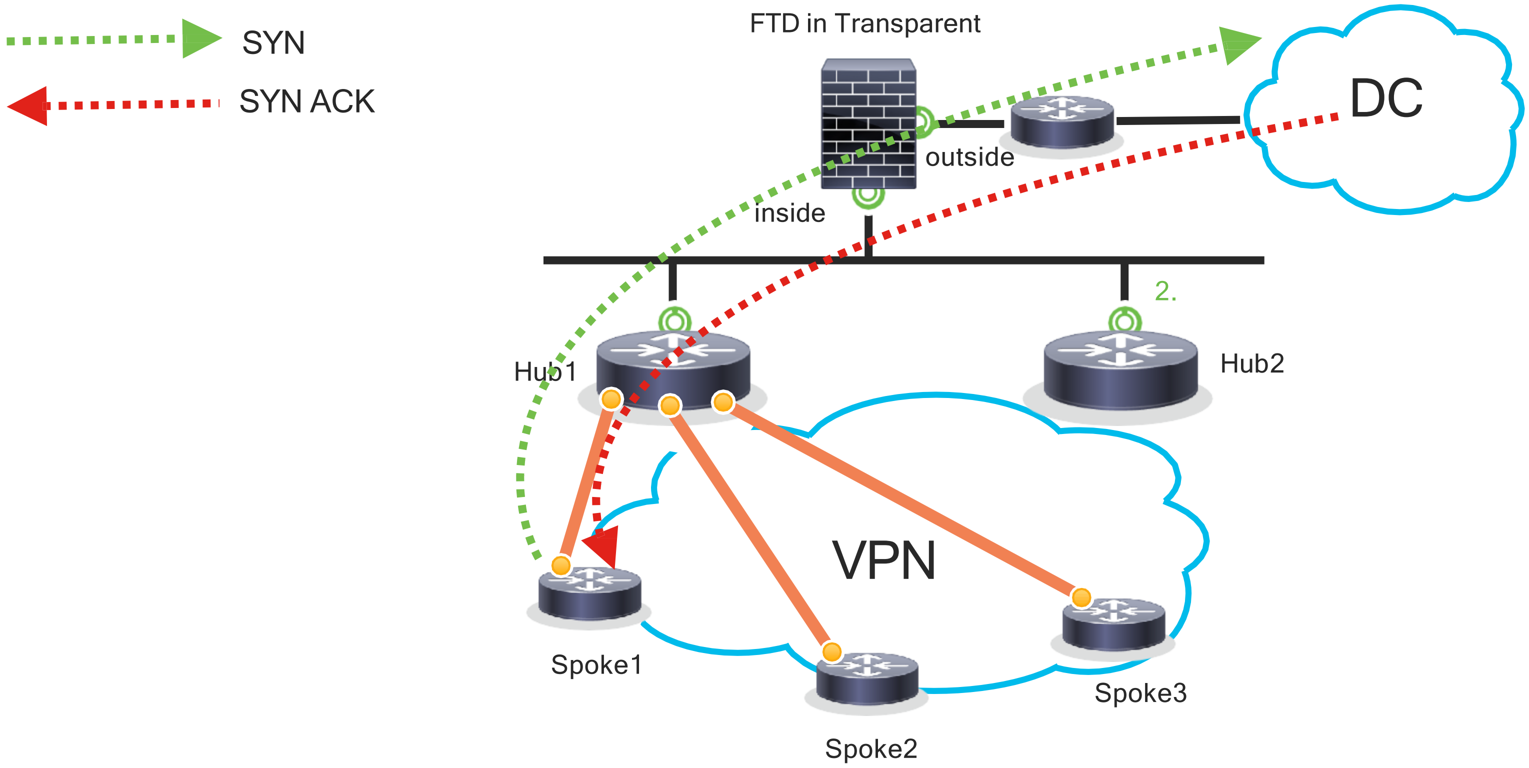


With IPS-Only asymmetry is not a problem. We just need to reassemble the packet.

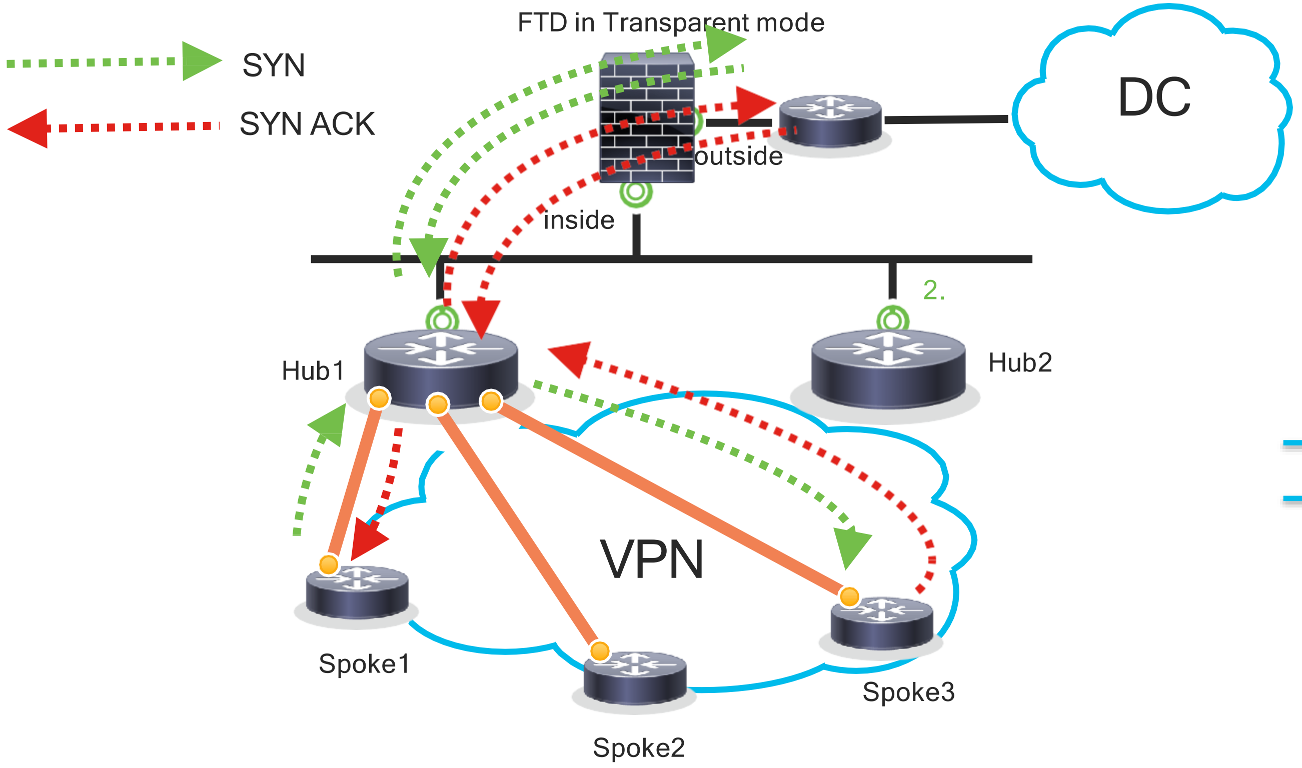
FTD Deployment and Interface Modes

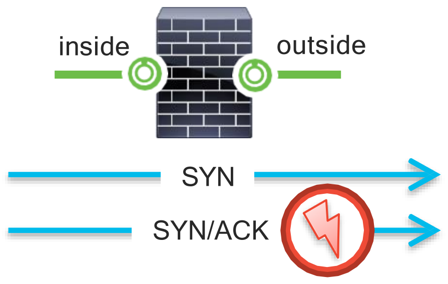
	FTD Interface Mode	FTD Deployment Mode (inherited from ASA)	Description	Real traffic can be dropped?
ASA	Routed	Routed	Full ASA and Snort checks	Yes
	Switched	Routed or Transparent	Full ASA and Snort checks	Yes
FirePower	Inline Set	Routed or Transparent	Partial ASA and full Snort checks	Yes
	Inline Set with Tap	Routed or Transparent	Partial ASA and full Snort checks	No
	Passive	Routed or Transparent	Partial ASA and full Snort checks	No
	Passive (ERSPAN)	Routed	Partial ASA and full Snort checks	No

Symmetric VPN flow - Spoke to DC

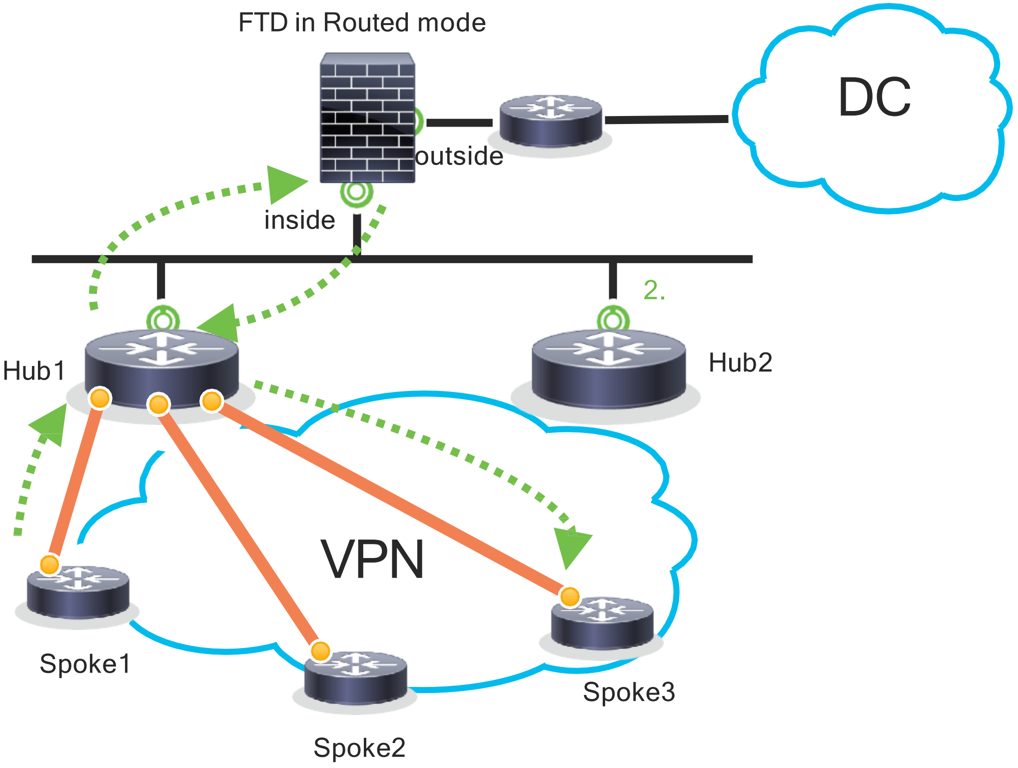


Asymmetric VPN traffic flow example?





FTD on a stick

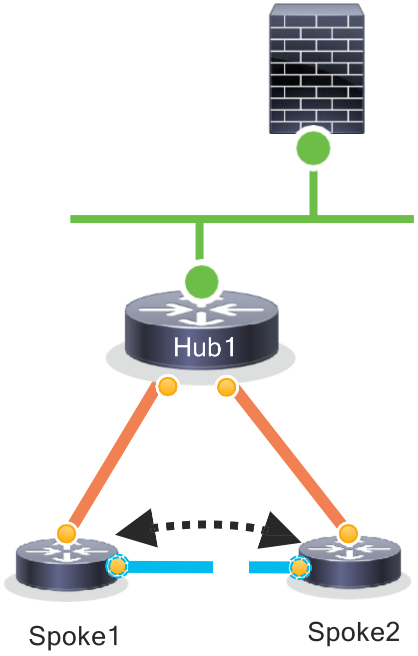


Protecting direct spoke-spoke traffic

Option 1 - spoke being an FTD/ASA

Option 2 - spoke being an IOS router:

- IOS Firewall
  - ZBF
  - Application Aware ZBF (XE16.9.1)
- Snort IPS*
- URL Filtering*
- Cisco Umbrella
- ETA (Encrypted Traffic Analytics)



* Available only on selected platforms

IPSec VPN Solutions Overview

IPSec VPN High Availability and Scalability

IPSec VPN Best Practices

Selecting a VPN Design

FTD Deployment and Interface Modes

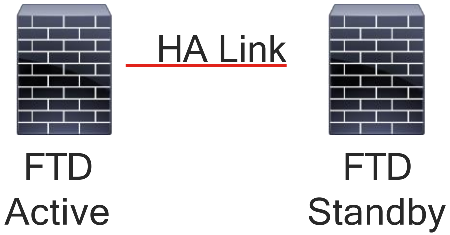
FTD Resiliency and Scalability

Scalable VPN with FTD Integration Deployment Example

Conclusion

High Availability for Firepower Threat Defense

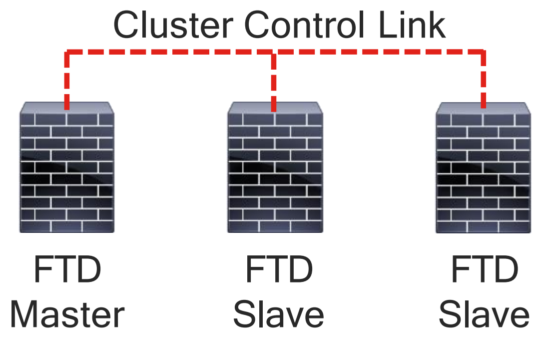
- FTD High Availability (failover), requires:
  - two identical FTD devices
  - dedicated failover link and, optionally, a state link
- FTD supports Active/Standby stateful failover
- Supports all NGFW/NGIPS interface modes
- Provides redundancy but not scalability



Clustering for the Firepower Threat Defense

- Grouping of multiple FTD units together as a single logical device.
- Supported only on the Firepower 9300 and the Firepower 4100 series.
- Provides increased throughput and redundancy of multiple devices.
- All packets for a flow are redirected to connection Owner.

Firepower NGFW Clustering Deep Dive - BRKSEC-3032
Friday, January 31 | 11:30 AM - 01:30 PM



IPSec VPN Solutions Overview

IPSec VPN High Availability and Scalability

Selecting a VPN Design

FTD Deployment and Interface Modes

FTD Resiliency and Scalability

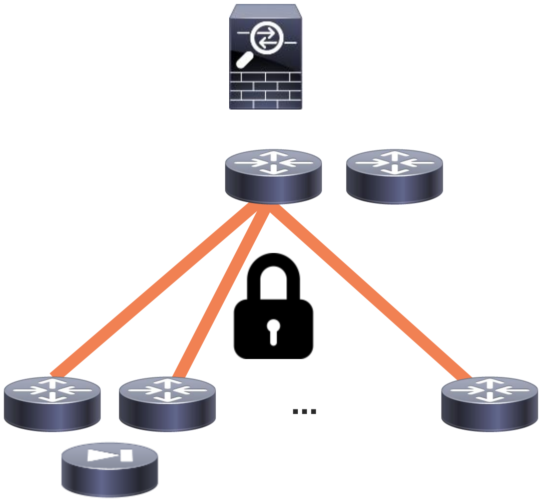
Scalable VPN with FTD Integration Deployment Example

IPSec VPN Best Practices

Conclusion

Example Design Requirements and Assumptions

- Large Scale Deployment - 40000 locations
- Hub-and-spoke topology
- Provide security using cryptographically protected tunnels.
- Headend redundancy with 15 seconds convergence
- Mix of ASA and IOS routers on branch locations
- IPS inspection for the spoke-to-spoke traffic using FTD

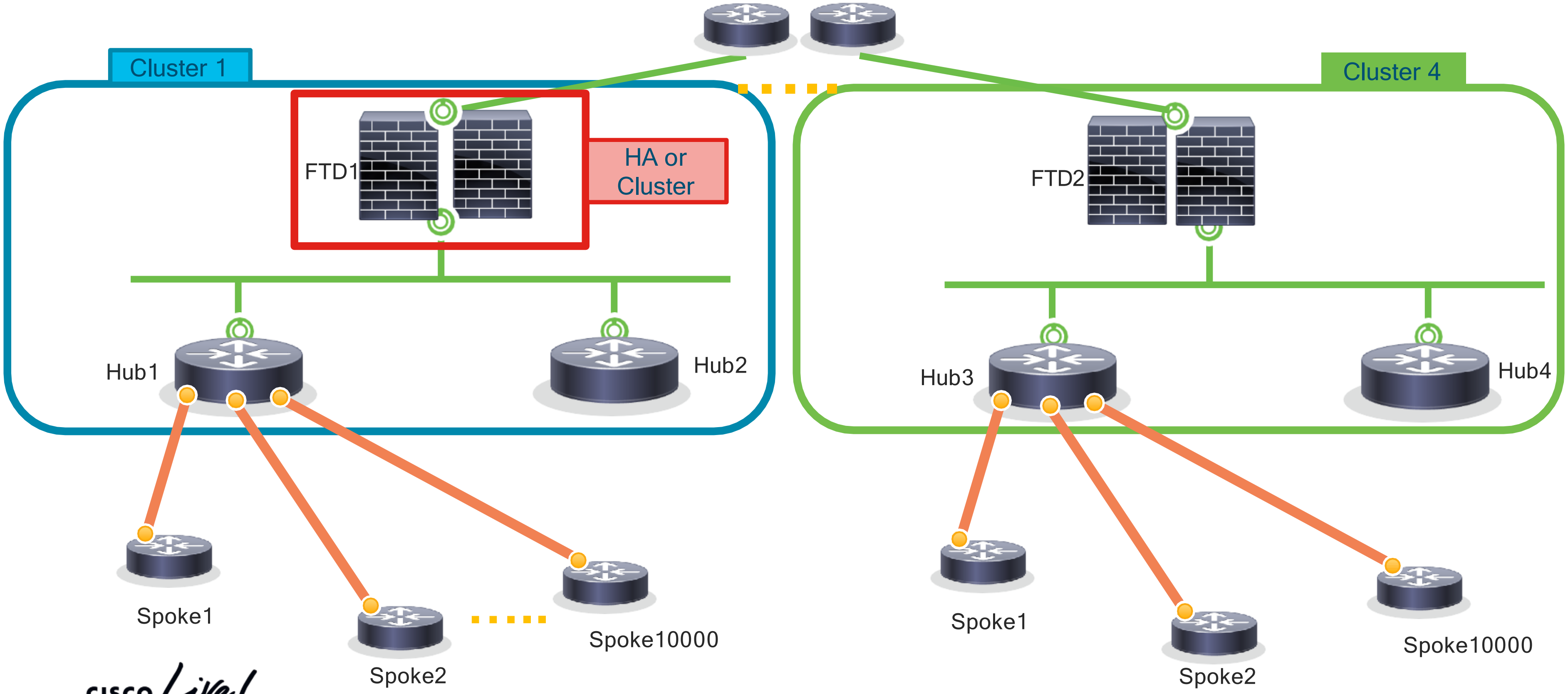


Proposed Solution

- FlexVPN Hub-and-Spoke topology
- HA and scalability using active/standby clusters with BGP
- PBR to redirect spoke-spoke traffic to FTD on a stick

High Level Design - Topology

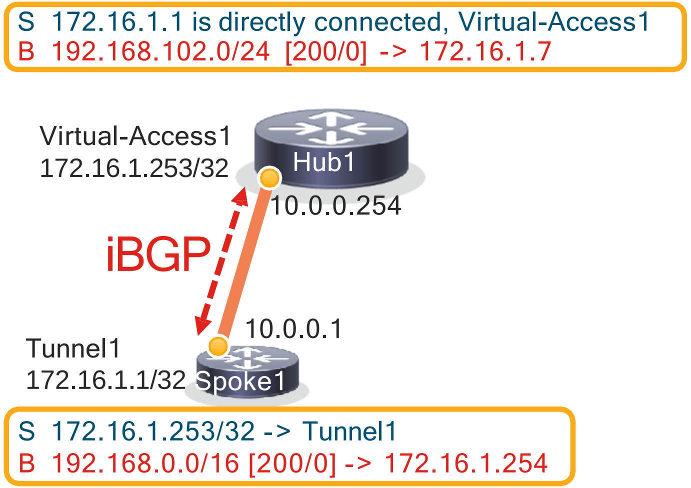
Hub-and-spoke + Large Scale



BGP routing considerations

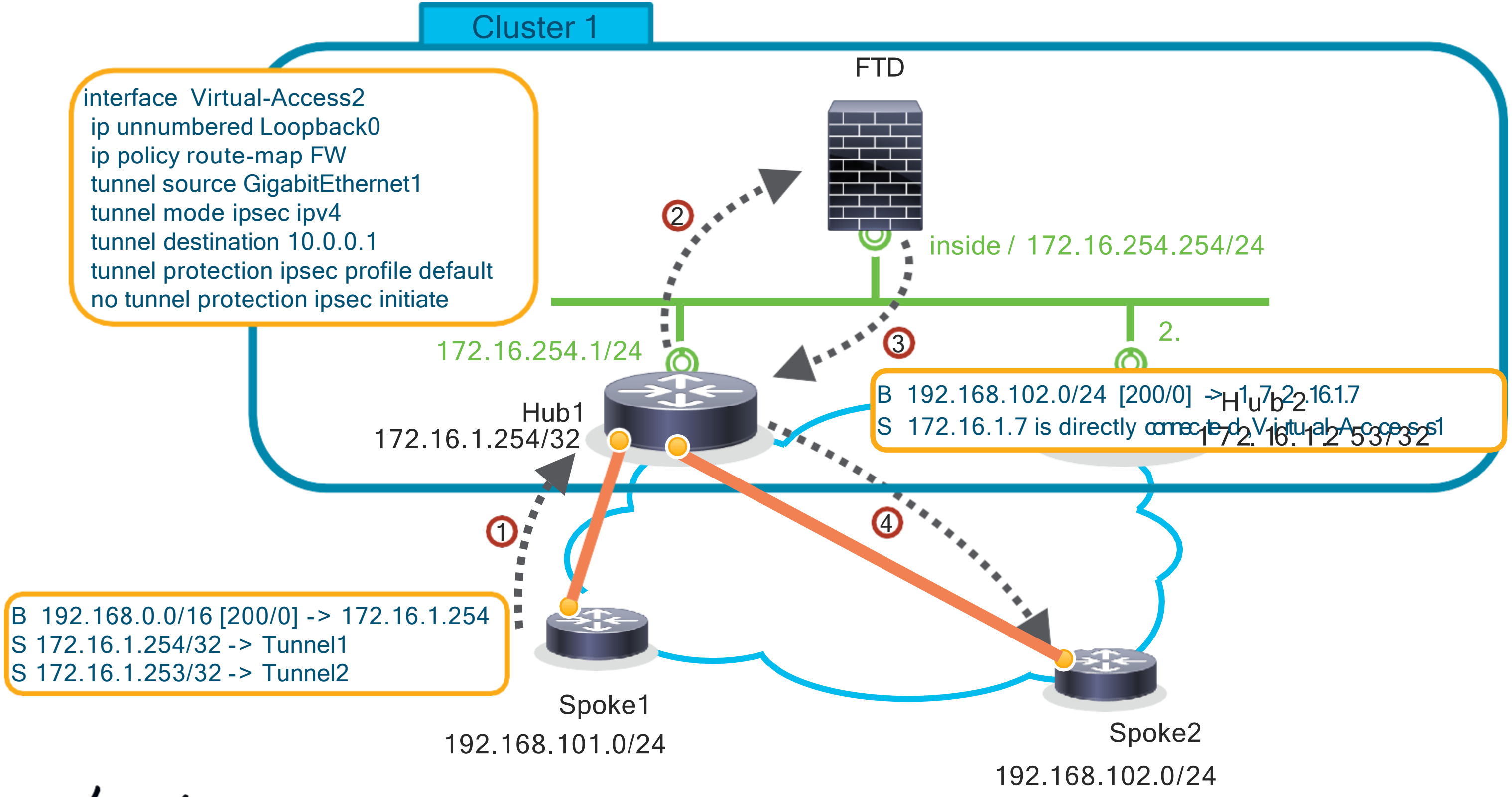
Headend redundancy with 15 seconds convergence

- 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.



FTD Routed mode on a stick

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



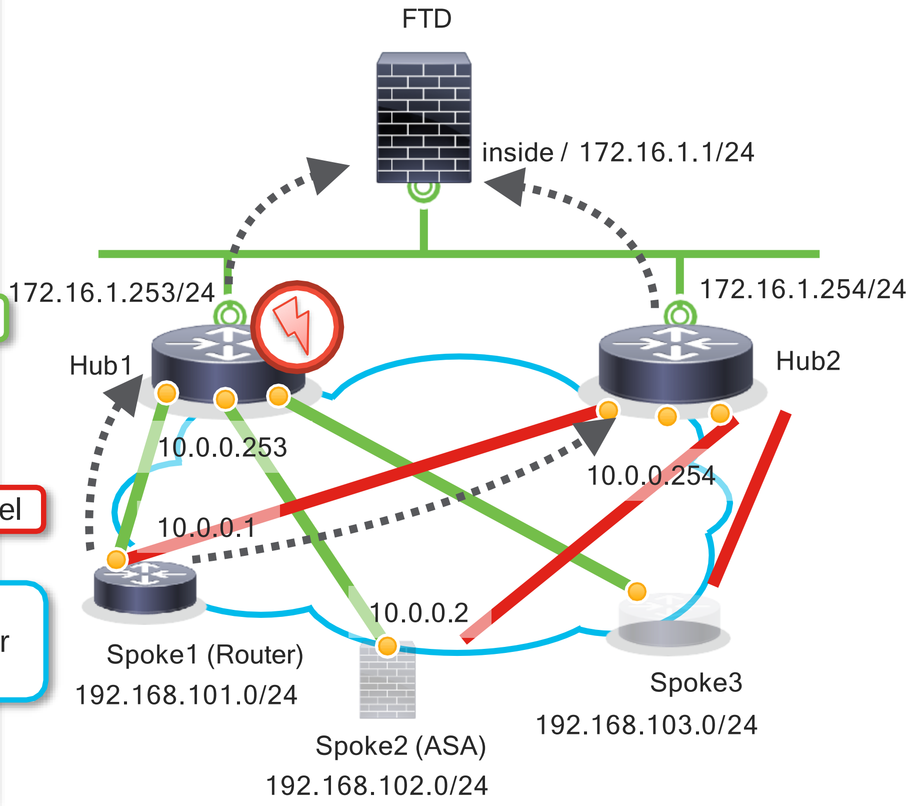
Spoke router configuration - IOS Example

```
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 router configuration - ASA Example

```
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

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
```

Required only if we want to terminate ASA/FTD* because they do not support IKEv2 config exhange

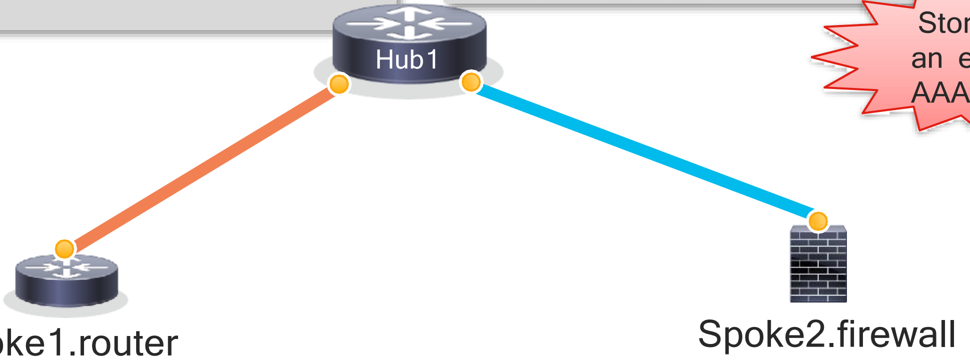
```
crypto ikev2 name-mangler extract-domain
 fqdn domain
```

```
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



* 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
```

PBR

Separate IKEv2 profiles for routers and firewalls

```
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
```

iBGP with listen range

Interface and routing verification

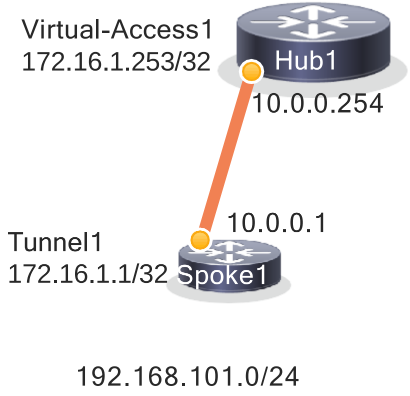
```
Hub1# show derived-config interface Virtual-Access 1
Building configuration...

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

```
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
```



IPSec VPN Solutions Overview

IPSec VPN High Availability and Scalability

Selecting a VPN Design

FTD Deployment Modes Overview

FTD Resiliency and Scalability

Scalable VPN with FTD Integration Deployment Example

IPSec VPN Best Practices

Conclusion

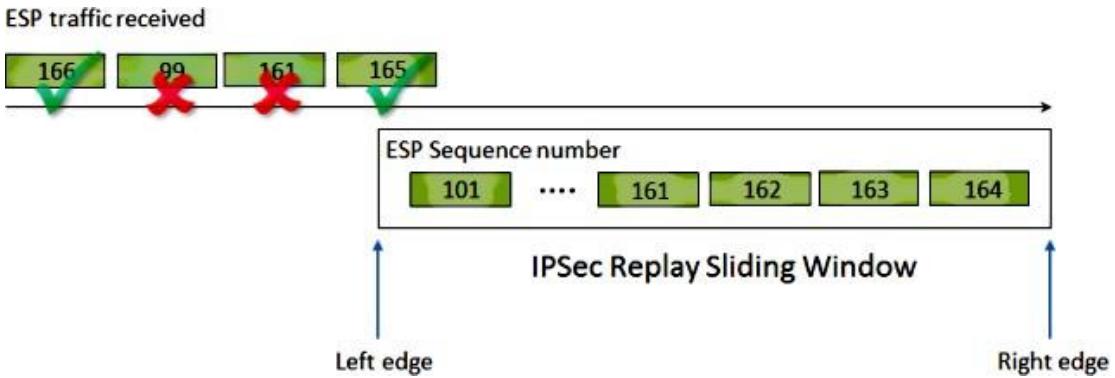
IPSec Security Association Lifetime

- The IPSec SA rekey can be triggered from two angles:
  - From a time-based perspective (lifetime in seconds of the SAs). Default value - 3600s.
  - From a traffic volume perspective (lifetime in kilobytes of data processed by the SAs). Default value ~ 4GB.
- Block Ciphers become unsafe with more than $2^{n/2}$ blocks of message encrypted.
- 3DES is broken
- With AES encryption algorithms, the volume-based re-key is justified only if more than 2^{64} blocks of 16 bytes are encrypted = 256 exabytes of data.

```
crypto ipsec profile IPsec-Profile
 set security-association lifetime kilobytes disable
```

Recommended

IPSec Anti-Replay Window Size Tuning



- When QoS is used, packets from different traffic classes can be queued and delivered out of order by a large number, bigger than anti-replay window size.
- There are a couple of possibilities to address this issue:
  - Increase the IPsec anti-replay window size (default is 64 packets).

```
crypto ipsec security-association replay window-size 1024
```

  - Disable the anti-replay protection mechanism.

```
crypto ipsec security-association replay disable
```

  - IPSec Anti-Replay Checking with Multiple Sequence Number Spaces

cisco Live!

IPSec Anti-Replay Checking with Multiple Sequence Number Spaces

CSR 16.6.1
ISR4k 16.7.1
ASR1k 16.8.1

- IPSec Anti-Replay multi-SNS is enabled with:

```
crypto ipsec security-association multi-sn
```

- The feature must be configured on both ends.
- The tunnel interface needs to be flapped.
- First 4 bits from SPI number are used to map DSCP to SNS

esp.sequence == 11

No.	Time	Source	Destination	ID	Protocol	Length	ESP Sequence	Info
1	2018-04-25 10:31:46.626797	10.0.0.1	10.0.0.2	0x0414 (1044)	ESP	182	11	ESP (SPI=0xb80acc20)
2	2018-04-25 10:31:46.627595	10.0.0.2	10.0.0.1	0x040b (1035)	ESP	182	11	ESP (SPI=0xb27210f5)
11	2018-04-25 10:31:51.252574	10.0.0.1	10.0.0.2	0x0419 (1049)	ESP	182	11	ESP (SPI=0x180acc20)
12	2018-04-25 10:31:51.253142	10.0.0.2	10.0.0.1	0x0410 (1040)	ESP	182	11	ESP (SPI=0x127210f5)

- Different SPI values even though this is the same SA.

0xb80acc20

0x180acc20

Call Admission Control for IKE

- For IKEv1 the default number of in-negotiation IKE connections is unlimited.

```
Router(config)# crypto call admission limit ike in-negotiation-sa 40
```

- For IKEv2 the default setting is 40.

```
Router(config)# crypto ikev2 limit max-in-negotiation-sa 40
```

- For large scale consider starting at 100 at reduce/increase based on results.

IPsec & Fragmentation

- The goal is to avoid post-encrypt fragmentation by controlling pre-encrypt fragmentation
- Incorrect MTU/MSS settings lead to problems with performance and packet drop.
- Proper MTU/MSS tuning helps achieve best performance and to avoid fragmentation.
- IPSec Overhead Calculator Tool https://cway.cisco.com/tools/ipsec-overhead-calc/

```
interface Tunnel1
 ip mtu 1400
 tcp adjust-mss 1360
```

Recommended settings covering majority of scenarios

IPSec Overhead Calculator Tool

ORIGINAL PACKET INFORMATION

Original IP Packet size (bytes) 100

TUNNEL SETTINGS

GRE over IPSec

IPSEC TRANSPORT SETTINGS

IP Version ⦿ IPv4 ○ IPv6

NAT-Traversal (IPSec over UDP port 4500)

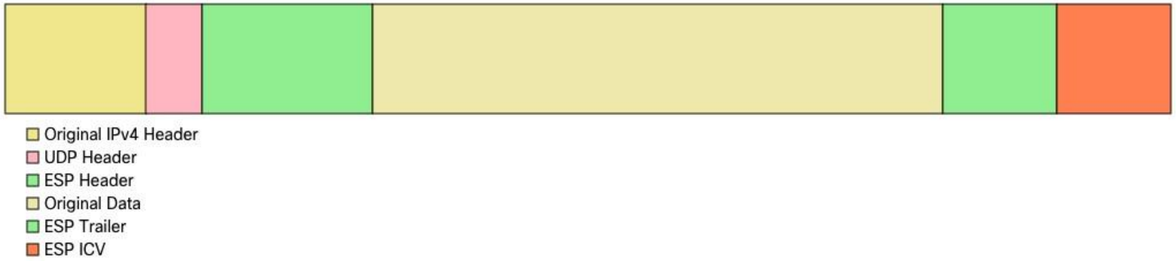
IPSEC TRANSFORM SETTINGS

Tunnel Mode ○ Tunnel ⦿ Transport

ESP Encryption ESP-AES-128/192/256 ESP Integrity ESP-SHA-256-HMAC

AH Integrity none

PACKET FORMAT



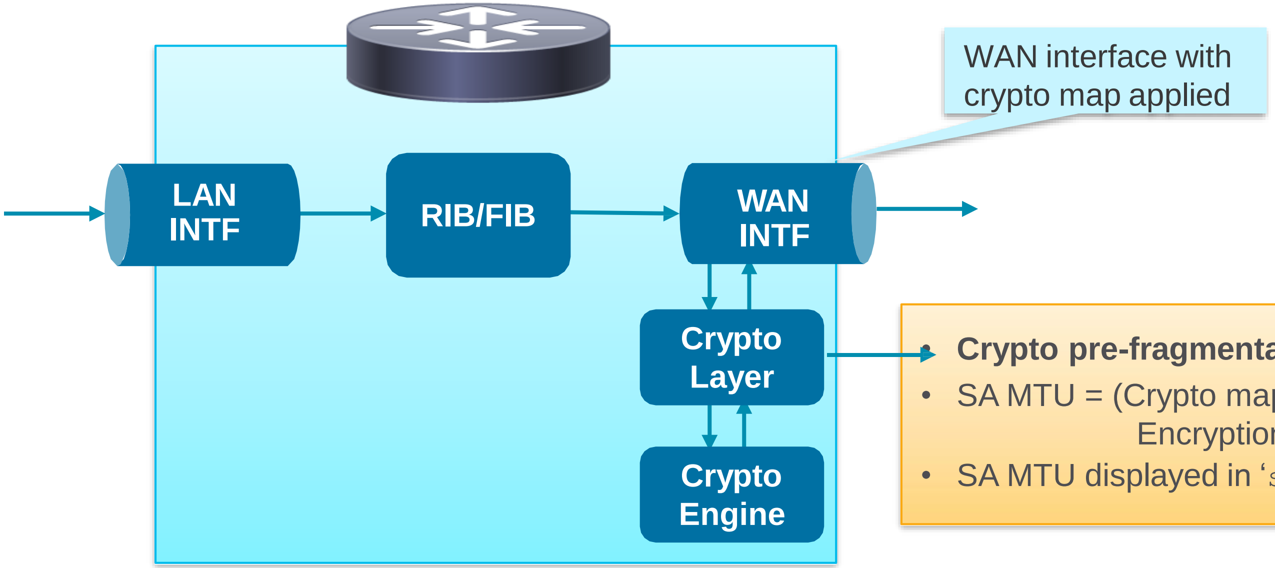
PACKET DETAILS

Field	Bytes
Original IPv4 Header	20
UDP Header (NAT-T)	8
SPI (ESP Header)	4
Sequence (ESP Header)	4
ESP-AES (IV)	16
Original Data Payload	80
ESP Pad (ESP-AES)	14
Pad length (ESP Trailer)	1
Next Header (ESP Trailer)	1
ESP-SHA-256-HMAC ICV (ESP Trailer)	16
Total IPSec Packet Size	**164**

IPsec & Fragmentation - Crypto Map

Reference

Fragmentation with Crypto maps (Crypto pre-fragmentation)

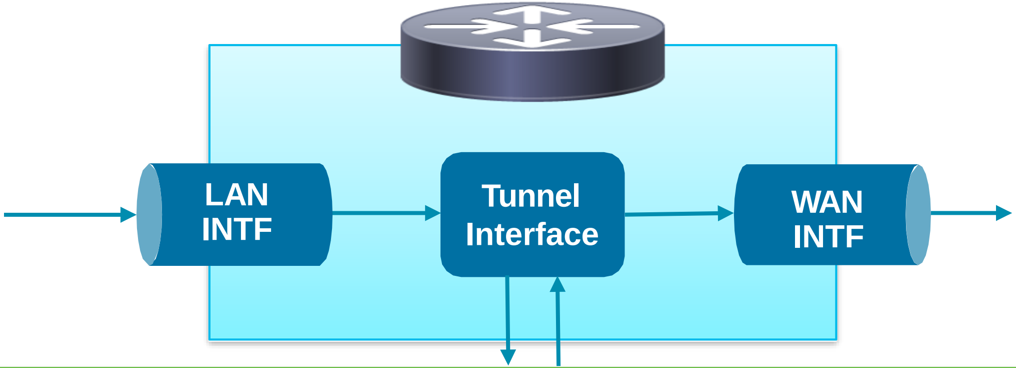


- **Crypto pre-fragmentation based on SA-MTU**
- SA MTU = (Crypto map interface IP MTU – Encryption Overhead)
- SA MTU displayed in '`show crypto ipsec sa`'

IPsec & Fragmentation - Tunnel Protection

Reference

Fragmentation with Tunnel protection



- **Pre-encap fragmentation based on Tunnel IP MTU**
- Tunnel IP MTU
  - Configured using 'ip mtu <>' on tunnel interface
  - If not configured,

    (Tunnel egress interface IP MTU –

    Tunnel encap overhead - Encryption Overhead)
- Tunnel IP MTU displayed in '`show ip interface tunnel <>`'
- **Crypto pre-fragmentation & SA MTU are not relevant for tunnel protection**

```
interface Tunnel <>
 ip address <>
 ip mtu <>
```

QoS Considerations - VPN Hub

- Implementing quality of service (QoS) on the FlexVPN Hub is often necessary, because Spoke's inbound physical bandwidth can become congested.
- The Hub has a much faster connection that does not become congested as fast as the Spoke connection (that is, the Hub can overrun the Spoke).

Step 1 - configure shaping policy on physical interface

Step 2 - configure per-spoke QoS policies which will get applied to virtual-access interfaces

QoS Considerations - VPN Spoke

- QoS on FlexVPN Spoke is setup to shape/police outbound traffic to ensure that the spoke doesn't overrun its own outbound bandwidth.
- This is an aggregate (across all tunnels) policy that is applied to the outbound physical interface on the spoke.

Step 1 - configure physical interface QoS policy on FlexVPN Spoke

IPSec VPN Solutions Overview

IPSec VPN High Availability and Scalability

Selecting a VPN Design

FTD Deployment Modes Overview

FTD Resiliency and Scalability

Scalable VPN with FTD Integration Deployment Example

IPSec VPN Best Practices

Conclusion

Conclusion

- Many VPN Solutions; asses the design requirements before selecting the best option.
- Evaluate failure scenarios and acceptable convergence time.
- Understand the packet flow to properly insert a security appliance (Firewall, IPS).
- Keep it simple.
- Follow the IPSec VPN best practices to achieve best performance and avoid problems.

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on 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 Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**