cisco live!

Let's go



## Route Based VPNs With Secure Firewall

Jeff Fanelli, Principal Architect @jefanell



BRKSEC-3058

# Agenda

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



### About Me

Jeff Fanelli

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





## VPN Technology Overview





### Underlay & Overlay





### Underlay & Overlay







#### BRKSEC-3058 © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public 10

### 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 ciscol23 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

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

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



# VPN Tunnel Interfaces



## **Tunnel Interface**



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



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

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

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



# Secure Firewall VPN Design



### New ASA and FTD capabilities

- These features are in ASA and FTD code right NOW:
- Static VTI Tunnels
- BGP routing support
- Per-peer IKEv2 custom identity attributes

Configs shown will be ASA CLI. (identical to FTD deployed configuration) New in the ASA 9.19 / FTD 7.3

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

### Example Design Requirements and Assumptions

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

### Single / Double Hub & Spoke design using VTI Hubs can be IOS, ASA 9.19+ or FTD 7.3+

For Secure Firewall Hubs:

- Use separate VPN topology configuration for each VPN Hub
- Backup hub can be configured for each topology

cisco ile

- 1024 maximum spokes per hub
- Routing protocol required



### Let's talk about BGP!

Border Gateway Protocol

Highly recommended! BRKENT-1179 Border Gateway Protocol Fundamentals



Gustavo Sibaja

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

### Single / Double Hub & Spoke design using VTI Hubs can be IOS, ASA 9.19+ or FTD 7.3+



cisco / ile

### Spoke ASA config - Pre ASA 9.19.1 / FTD 7.3



### Spoke ASA config - ASA 9.19.1+ / FTD 7.3+



### Spoke config using Loopback - ASA 9.19.1+ / FTD 7.3+



cisco

## Hub ASA / FTD configuration

interface Loopback101
nameif lo101
ip address 172.16.10.1 255.255.255

interface Virtual-Template101 type tunnel
nameif dVTI101
ip unnumbered lo101
tunnel source interface outside
tunnel mode ipsec ipv4
tunnel protection ipsec profile IPSEC PROFILE

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..

tunnel-group spoke1 type ipsec-121 tunnel-group spoke1 ipsec-attributes virtual-template 101 ikev2 remote-authentication pre-shared-key \*\*\*\* ikev2 local-authentication pre-shared-key \*\*\*\*\* ikev2 route set interface

cisco / ille

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

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 172.16.10.3 activate 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)

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

| <b>ftd</b><br>Cisc | tdv-a.infosec-pros.com              |           |            |                 |           |          |          |                    |           |          |          | Save       | Cancel  |
|--------------------|-------------------------------------|-----------|------------|-----------------|-----------|----------|----------|--------------------|-----------|----------|----------|------------|---------|
| D                  | evice                               | Routing   | Interfaces | Inline Sets     | DHCP      | VTEP     |          |                    |           |          |          |            |         |
|                    |                                     |           |            |                 |           |          |          | Q Search by name   |           | Syn      | c Device | Add Inter  | faces 🔻 |
|                    | Interface                           | 9         |            | Logical Name    |           | Туре     | Security | MAC Address (Activ | IP Addre  | ess      | Path M   | Virtual Ro |         |
|                    | ODiagn                              | iostic0/0 |            | diagnostic      |           | Physical |          |                    |           |          | Disabled | Global     |         |
|                    | GigabitEthernet0/0 (Manager Access) |           | outside    |                 | Physical  |          |          | 38.                | 81/255.25 | Disabled | Global   |            |         |
|                    | Virtual-Template1                   |           |            | diagnostic_dyna | mic_vti_1 | VTI      | vti-zone |                    |           |          | Disabled | Global     | / 1     |

- 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)

| <b>ftc</b><br>Cis | ftdv-b.infosec-pros.com     s       Cisco Firepower Threat Defense for VMware     s |                |                  |              |          |          |          |                    |              |             |            | Cancel   |
|-------------------|---|----------------|------------------|--------------|----------|----------|----------|--------------------|--------------|-------------|------------|----------|
| I                 | Device  | Routing        | Interfaces       | Inline Sets  | DHCP     | VTEP     |          |                    |              |             |            |          |
|                   |   |                |                  |              |          |          |          | Q Search by name   |              | Sync Device | Add Inte   | rfaces 🔻 |
|                   | Interface   | е              |                  | Logical Name |          | Туре     | Security | MAC Address (Activ | IP Address   | Path M      | Virtual Ro |          |
|                   | Diagr   | nostic0/0      |                  | diagnostic   |          | Physical |          |                    |              | Disabled    | Global     |          |
|                   | Gigab   | oitEthernet0/0 | (Manager Access) | outside      |          | Physical |          |                    | 38. 82/255.2 | 25 Disabled | Global     | <i>.</i> |
|                   | Virtual-Template1   |                | diagnostic_dyna  | amic_vti_1   | VTI      | vti-zone |          |                    | Disabled     | Global      | / 1        |          |
|                   | Loopback1   |                | loopback1        |              | Loopback |          |          | 2.2.2.1/32(Static) | Disabled     | Global      |            |          |

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

cisco /

### Hub Virtual-Template Interface Config

#### General

#### Tunnel Type

Static • Dynamic

#### Stat

#### Name:\*

diagnostic\_dynamic\_vti\_1

#### 🗹 Enabled

#### Description:

| Security Zone: |   |
|----------------|---|
| vti-zone       | • |

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

|                              |   | 0           |   |
|------------------------------|---|-------------|---|
| Template ID:*                |   |             |   |
| 1                            |   | (1 - 10413) |   |
| Tunnel Source:               |   |             |   |
| GigabitEthernet0/0 (outside) | • | 3881        | ▼ |
|                              |   |             |   |

#### **IPsec Tunnel Details**

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

#### IPsec Tunnel Mode:\*

| ● IPv4 ○ IPv6                     |  |     |  |  |  |  |  |  |  |
|-----------------------------------|--|-----|--|--|--|--|--|--|--|
| IP Address:*                      |  |     |  |  |  |  |  |  |  |
| Configure IP                      | <valid address="" ipv4="">/<mask></mask></valid> | 0   |  |  |  |  |  |  |  |
| Borrow IP (IP unnumbered)         | Loopback1 (loopback1)                            | • + |  |  |  |  |  |  |  |
|                                   |  |     |  |  |  |  |  |  |  |
| VPN Topology Usage                |  |     |  |  |  |  |  |  |  |
| Hub-Spoke-Primary (Tunnel Destina | tion IP - 3883, 38                               |     |  |  |  |  |  |  |  |



## Site to Site VPN Topology with DVTI

|        | Defense Orchestrato        | or Analysis       | Policies Devi | ices Objects    | Integration   | SReturn Ho      | me Deploy         | ର 💕         | ¢ ()   | ) jefanell@ci | sco.com ▼ |
|--------|----------------------------|-------------------|---------------|-----------------|---------------|-----------------|-------------------|-------------|--------|---------------|-----------|
|        |                            |                   |               |                 | Last Updated: | 04:11 PM        | Refresh +         | Site to Sit | e VPN  | + SASE To     | opology   |
| T Sele | ect                        |                   |               |                 |               |                 |                   |             |        | ×             | Refresh   |
| 1      | Гopology Name              | VPN Type          |               | Network Topolog | Ŋ             | Tunnel Sta      | tus Distribution  |             | IKE    | Ev1 IKEv2     |           |
| ~      | Hub-Spoke-Primary          | Route Based (VTI) |               | Hub & Spoke     |               | 2- Tunnels      |                   |             |        | ~             | / 1       |
|        |                            | Hub               |               |                 |               |                 | Spo               | oke         |        |               |           |
| Devi   | ce VPN                     | I Interface       | VTI Interface |                 | Devic         | e               | VPN Interfa       | ace         | VT     | I Interface   |           |
| FTD    | ftdv-a.infosec-pros.c outs | side (38          | diagnostic_dy | (1.1.1.1)       | FTD           | ftdv-c.infosec- | pros.c outside (3 | 38. 83      | 3) dia | agnostic_sta  | (1.1.1.2) |
| FTD    | ftdv-a.infosec-pros.c outs | side (38          | diagnostic_dy | (1.1.1.1)       | FTD           | ftdv-d.infosec- | pros.c outside (3 | 38. 84      | 4) dia | agnostic_sta  | (1.1.1.3) |

- 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

|      | Defense Orchestrat     Site To Site | tor Analysis      | Policies Devi | ces Objects      | Integration   | ✤ Return Home       | Deploy Q         | <b>6</b> 🎸  | iefanell@cis   | sco.com ▼ |
|------|-------------------------------------|-------------------|---------------|------------------|---------------|---------------------|------------------|-------------|----------------|-----------|
|      |                                     |                   |               |                  | Last Updated: | 04:44 PM Ref        | resh + Site      | to Site VPN | + SASE To      | opology   |
| T Se | elect                               |                   |               |                  |               |                     |                  |             | ×              | Refresh   |
|      | Topology Name                       | VPN Type          |               | Network Topology | У             | Tunnel Status I     | Distribution     |             | IKEv1 IKEv2    |           |
| >    | Hub-Spoke-Primary                   | Route Based (VTI) |               | Hub & Spoke      |               | 2- Tunnels          |                  |             | $\checkmark$   | 1         |
| ~    | Hub-Spoke-Secondary                 | Route Based (VTI) |               | Hub & Spoke      |               | 2- Tunnels          |                  |             | $\checkmark$   | / 1       |
|      |                                     | Hub               |               |                  |               |                     | Spoke            |             |                |           |
| De   | vice VP                             | PN Interface      | VTI Interface |                  | Devic         | ce                  | VPN Interface    |             | VTI Interface  |           |
| FT   | p ftdv-b.infosec-pros.c ou          | itside (38. 82)   | diagnostic_dy | . (2.2.2.1)      | FTD           | ftdv-c.infosec-pros | s.c outside (38. | .83)        | diagnostic_sta | (2.2.2.2) |
| FT   | p ftdv-b.infosec-pros.c ou          | itside (38. 82)   | diagnostic_dy | . (2.2.2.1)      | FTD           | ftdv-d.infosec-pros | s.c outside (38. | .84)        | diagnostic_sta | (2.2.2.3) |

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

cisco ile

### Site to Site VPN Topology

| IKE Version:* IKEv1 | KEv2                    |                                     |
|---------------------|-------------------------|-------------------------------------|
| Endpoints IKE IPsec | Advanced                |                                     |
| Crypto Map Type:    | Static      Dynamic     |                                     |
| IKEv2 Mode:         | Tunnel                  | v                                   |
|                     |                         |                                     |
| Transform Sets:     | IKEv1 IPsec Proposals 💉 | IKEv2 IPsec Proposals* 🖋            |
| Transform Sets:     | IKEv1 IPsec Proposals 💉 | IKEv2 IPsec Proposals* 🖋<br>AES-GCM |
| Transform Sets:     | IKEv1 IPsec Proposals 🖋 | IKEv2 IPsec Proposals* 🖋<br>AES-GCM |

```
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

cisco ile

### Hub routing table example





- "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) BRKSEC-3058

## Security Service Edge deployments

Featuring Cisco Secure Access





### Secure Access ("Security Service Edge")





### **Cloud Security Services**

←→ Internet Traffic Private Traffic Secure Tunnel



BRKSEC-3058 © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public 42

### Why connect your branches to Secure Access?

Internet Security capabilities:

- Umbrella DNS protection
- DLP & CASB controls
- Web Application controls
- Microsoft & Google Tenant Controls
- Cloud malware protection, sandboxing, decryption.



Private application access:

- Connectivity to private apps protected by Secure Access
- Connectivity for private applications behind branch firewall
- Connectivity to cloud delivered RAVPN as a service subnets



### Secure Access Branch Tunnels

|   | Firewall Management C<br>Site To Site | Center      | Overview | Analysis | Policies     | Devices | Objects    | Integration       | Deploy | Q | 0     | ¢ ()         | admin $\vee$ |
|---|---------------------------------------|-------------|----------|----------|--------------|---------|------------|-------------------|--------|---|-------|--------------|--------------|
|   | Topology Name                         | VPN Type    |          | Netw     | ork Topology |         | Tunnel St  | atus Distribution |        |   | IKEv1 | IKEv2        |              |
| > | Hub-Spoke-Primary                     | Route Based | (VTI)    | Hub      | & Spoke      |         | 4- Tunnels |                   |        |   |       | $\checkmark$ | 1            |
| > | Hub-Spoke-Secondary                   | Route Based | (VTI)    | Hub      | & Spoke      |         | 4- Tunnels |                   |        |   |       | $\checkmark$ | 1            |
| > | Secure-Access-Virginia-Prim           | Route Based | (VTI)    | Hub      | & Spoke      |         | 3- Tunnels |                   |        |   |       | $\checkmark$ | 1            |
| > | Secure-Access-Virginia-Seco           | Route Based | (VTI)    | Hub      | & Spoke      |         | 3- Tunnels |                   |        |   |       | $\checkmark$ | 1            |

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

### Branch Configuration for Secure Access tunnels

Tunnel addressing best practices:

- No need for loopback interfaces
- Use these IP tunnel addresses
  - 169.254.0.6/30 for Primary
  - 169.254.0.10/30 for Secondary

IPSec best practices:

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

Device:\* ftdv-test-3 ▼ Static Virtual Tunnel Interface outside\_static\_vti\_3 (IP: 169.254.€ +.73) Tunnel Source: outside (IP: 64. Tunnel Source IP is Private Send Local Identity to Peers Local Identity Configuration:\* Email ID ftdv-test-3@ -618854070



### Branch Configuration for Secure Access tunnels

> BG Pa

BGP Peering to Secure Access:

- Remote AS 64512
- Unique AS for each branch
- Use BGP Route Maps to restrict inbound / outbound route advertisements
- FTD static default route should use metric of 254 if BGP default from Secure Access is desired
- Backup tunnel from Secure Access will use AS prepend to ensure primary tunnel preference



#### ftdv-test-3

Cisco Firepower Threat Defense for VMware

| Device   | Routing           | Interfaces         | Inline Sets         | DHCP              | VTEP             |             |  |  |  |  |  |
|--|-------------------|--------------------|---------------------|-------------------|------------------|-------------|--|--|--|--|--|
| Manage V<br>Global   | irtual Route      | ers                | nable IPv4: 🗹       | 5073              |                  |             |  |  |  |  |  |
| Virtual Pout   | er Droperties     |                    | General             | Neighbor          | Add Aggreg       | ate Address |  |  |  |  |  |
| ECMP   | er Properties     |                    | Address             |                   | Remote A         | \S Number   |  |  |  |  |  |
| ✓ BGP  |                   |                    | 169.254.0.5         |                   | 64512            |             |  |  |  |  |  |
| IPv4<br>IPv6   |                   |                    | 169.254.0.9         |                   | 64512            |             |  |  |  |  |  |
| show bgp 0.0.0.0<br>P routing table entry for 0.0.0.0/0, version 530<br>Ths: (2 available, best #2, table default)<br>Advertised to update-groups: |                   |                    |                     |                   |                  |             |  |  |  |  |  |
| 64512 64512<br>169.254.0.<br>Origin J  | 9 from<br>GP, loc | 169.254<br>calpref | 4.0.9 (1<br>100, va | 69.254<br>lid, ex | .0.9)<br>kternal |             |  |  |  |  |  |
| 169.254.0.   | 5 from            | 169.254            | 1.0.5 (1            | 69.254.           | .0.5)            | best        |  |  |  |  |  |

### FTD Branch with Secure Access



## Firewall SDWAN

### Policy Based Routing





### Secure Firewall SD-WAN

WAN Connect and Remote Branch Management

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





## Intelligent Routing with Path Monitoring

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

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





WAN Path Primary Path for YouTube Secondary Path for YouTube Primary Path for Webex Secondary Path for Webex

### WAN PBR Path Monitoring

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





# Monitoring & Troubleshooting





## WAN Summary Dashboard (7.4)

#### Application bandwidth consumption data

- 2 WAN interfaces status
- VPN interfaces status
- WAN interfaces throughput
- 5 Inventory of Devices part of WAN topology
- 6 Overall SDWAN Health

Detailed View in Health Monitoring





### **Enhanced WAN Application Monitoring**

| Firewall Management O<br>Overview / Dashboards / WAN St | Center<br>Ummary Overview      | Analysis Polie | cies Devi               | ces Objects  | Integration         | Deploy Q 🧃                              | 🏴 🌣 🕜 🦷 mtiko | o ~ dialla SECURE   |
|---|--------------------------------|----------------|-------------------------|--------------|---------------------|---|---------------|---------------------|
| Overview Application Monitoring                         | _                              |                |                         |              | Uplink              | Decisions Refresh eve                   | ery 5 minutes | V II Refresh        |
| Select Device   | adp.com                        |                |                         |              |                     |   |               |                     |
| FTDHA16-17 V  | Interfaces                     | Jit            | tter                    | RT           | T (Round-trip Time) | Packet Loss                             | MOS           | Mean Opinion Score) |
| Applications  | GigabitEthernet0/1<br>outside2 | 74             | 4433                    | 10           | 000604              | 0                                       | 0             |                     |
| ⊂.<br>✓ Fifth Third Bank                                | GigabitEthernet0/3<br>internet | 3              | 1371                    | 53           | 88483               | 0                                       | 2.25          |                     |
| 53.com  |                                |                |                         |              |                     |   |               |                     |
| ✓ ADP   |                                |                |                         |              |                     |   |               |                     |
| adp.com   | Application Performan          | nce Metrics    |                         |              |                     |   |               |                     |
| <ul> <li>American Express</li> </ul>                    |                                |                |                         |              |                     |   |               |                     |
| aexp-static.com   | Jitter                         | Round Trip T   | ïme                     | MOS          | Packet Loss         |   |               | s Last 2h           |
| americanexpress.ae                                      | Average Jitter                 |                |                         |              |                     |   |               |                     |
| americanexpress.be                                      | 9 435.6 K                      |                |                         |              |                     |   |               |                     |
| americanexpress.ch                                      | 8 326.7 K                      |                |                         |              |                     |   |               |                     |
| americanexpress.co                                      | 108.9 K                        |                |                         | •••••••••••• |                     | ******                                  |               |                     |
| americanexpress.com                                     | Oatuee                         |                |                         |              |                     |   |               |                     |
| americanexpress.kz                                      |                                | 02:45 03       | 3:00                    | 03:15        | 03:30               | 03:45 04:00                             | 04:15         | 04:30               |
| ✓ Allstate  | Average RTT                    |                |                         |              |                     |   |               |                     |
| allstate.com  | 50 1.9 M                       |                |                         |              |                     |   |               |                     |
| allstate.reviewability.com                              | 948.7 K                        |                | • • • • • • • • • • •   |              | ******              | +++++++++++++++++++++++++++++++++++++++ |               |                     |
| <ul> <li>Bank of America</li> </ul>                     | E 474.3 K                      |                | • • • • • • • • • • • • |              | ******              |   |               | ••••••              |
| hac-assate com  | Value                          |                |                         |              |                     |   |               |                     |
| bankafamarian anm                                       |                                | 02:45 03       | 3:00                    | 03:15        | 03:30               | 03:45 04:00                             | 04:15         | 04:30               |
| bankolamerica.com                                       | MOS                            |                |                         |              |                     |   |               |                     |
| bankofamerica.tt.omtrdc.net                             | 9 100                          |                |                         |              |                     |   |               |                     |
| <ul> <li>Bloomberg</li> </ul>                           | 8 75                           |                |                         |              |                     |   |               |                     |

 Easily monitor all interfaces where Policy-Based Routing is enabled

 Detailed application performance metrics for Jitter, Round Trip Time, MOS and Packet Loss



### VPN Packet Tracer in 7.3

| Ę | Firewall Management C<br>Overview / Dashboards / Site to Si | enter Overview Analy          | ysis Policies | Devices  | Objects Integrati | Deploy 🗏 Q 🚱 🌣 🕼 admin 🗸 👘                         | SECURE |
|---|---|-------------------------------|---------------|----------|-------------------|--|--------|
| Ţ | Select  |                               |               |          |                   | X Refresh every 5 minutes                          | ~ ►    |
|   | Node A  | Node B                        | Topology      | Status   | Last Updated 🔺    | A: Branch1 $\longleftrightarrow$ B: Branch2        | ×      |
|   | Branch1 (VPN IP: 10.10.0.202)                               | Branch2 (VPN IP: 10.10.0.203) | HnS-NATExempt | Inactive | 2023-01-06 02:49  | Topology: HnS-NATExempt   Status: Control Inactive |        |
|   |   |                               |               |          |                   | General CLI Details Packet Tracer                  |        |

Viewing 1-1 of 1

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

|  | X Refresh Refresh every 5 minutes V                |
|--|--|
| A: Branch1   | ×  |
| Topology: HnS-NATExempt   Status: Oliverative Constraints          | ive  |
| General CLI Details Packet Tracer                                  | _  |
|  | SELECT TRACE                                       |
|  |  |
|  | ✓ See Trace Config                                 |
| Node A Traces  | X Node B Traces                                    |
| → Drop A: In → Out   | ✓ $X \longrightarrow Drop$ B (Decrypted): Out → In |
| > V ROUTE-LOOKUP   | ROUTE-LOOKUP<br>137 41us                           |
| > V OBJECT-GROUP-SE  | > × Result: Drop                                   |
| 🔇 Ons  | <b>()</b> 137.41µs                                 |
| >  | > 🗙 ← Drop B: Out ← In                             |
| <ul> <li>CONN-SETTINGS</li> <li>293ns</li> </ul>                   |  |
| > < NAT<br>() 293ns  |  |
| <ul> <li>VAT</li> <li>Q 293ns</li> </ul>                           |  |
| <ul> <li>V IP-OPTIONS</li> <li>Q 293ns</li> </ul>                  |  |
| <ul> <li>V INSPECT</li> <li>              21.03µs      </li> </ul> |  |
|  |  |

### Site to Site Monitoring in 7.4

|             | Firewall Management Center<br>Overview / Dashboards / Site to Site VPN | Overview Analysis Policies          | s Devices Objects   | Integration |                     | Deploy Q 🥵 🌣 🕢 admin 🗸 端 SECU  |
|-------------|--|-------------------------------------|---------------------|-------------|---------------------|--|
| <b>▼</b> Se | elect  |                                     |                     |             |                     | × Refresh Refresh every 5 minutes V  |
|             | Node A   | Node B                              | Topology 🔺          | Status      | Last Updated        | A: 10.10.1.19 ↔ B: 10.10.1.20 ×  |
|             | 10.10.1.19 (VPN IP: 10.10.1.39)  | 10.10.1.20 (VPN IP: 10.10.1.40)     | VPN101-P2Pv4        | Inactive    | 2023-01-30 12:48:49 | Topology: VPN106-DVTIv4   Status: 🤣 Active   |
|             | 10.10.1.19 (VPN IP: 9101::19)  | 10.10.1.20 (VPN IP: 9101::20)       | VPN102-P2Pv6        | ON Active   | N/A                 | General CLI Details Packet Tracer  |
|             | 10.10.1.19 (VPN IP: 10.10.1.69)  | IOS99 (VPN IP: 192.168.102.99)      | VPN103-HNSv4        | 8 No Active | N/A                 | C Refresh C Maximize view  |
|             | 10.10.1.19 (VPN IP: 10.10.1.69)  | 10.10.1.20 (VPN IP: 10.10.1.70)     | VPN103-HNSv4        | ON Active   | N/A                 | Summary  |
|             | 10.10.1.19 (VPN IP: 192.168.103.19)                                    | 10.10.1.20 (VPN IP: 192.168.103.20) | VPN104-SVTIv4       | Active      | 2023-02-07 11:40:11 | Node A (192.168.105.19/500) 👔 🔗 Node B (192.168.105.20/500) 👔  |
|             | 10.10.1.19 (VPN IP: 9104::19)  | FTD02-EXTRANET (VPN IP: 9104::20)   | VPN105-SVTIv6-FTD01 | Active      | 2023-02-07 11:41:07 | Transmitted:     560 Bytes (560 B)         Transmitted:     560 Bytes (560 B)  |
|             | FTD02-EXTRANET (VPN IP: 9104::19)                                      | 10.10.1.20 (VPN IP: 9104::20)       | VPN105-SVTIv6-FTD02 | Active      | 2023-02-07 11:41:07 | Received: 0 (0 B) Received: 0 (0 B)  IPsec Security Associations (1)   |
|             | 10.10.1.19 (VPN IP: 192.168.105.19)                                    | 10.10.1.20 (VPN IP: 192.168.105.20) | VPN106-DVTIv4       | Active      | 2023-02-07 11:40:11 | V 192.168.15.0/255.255.255.0/0/0   |
|             | 10 10 1 19 (VPN IP: 192 168 105 19)                                    | IOS99 (V/DN ID: 192 168 105 99)     | VPN106-DVTbv4       | No Active   | N/A                 | L2L Tunnel PFS Group 21 IKEv2 VTI  |
|             | 10.10.11.15 (VPNVPP. 152.100.105.15)                                   | 100000 (111111-102.100.100.000)     | V111100 DV1114      |             | N/A                 | Encaps/Encrypt:         20 / 20 pkts         Encaps/Encrypt:         20 / 20 pkts           Deans/Decrypt:         0 / 0 pkts         Deans/Decrypt:         0 / 0 pkts  |
|             | 10.10.1.19 (VPN IP: 9106::19)  | 10.10.1.20 (VPN IP: 9106::20)       | VPN107-DVTIv6       | Active      | 2023-02-07 11:40:11 | Remaining Lifetime for SPI ID: 0x2F5F96A1  |
|             | 10.10.1.19 (VPN IP: 9106::19)  | IOS99 (VPN IP: 9106::99)            | VPN107-DVTIv6       | O No Active | N/A                 | Outbound:         4.81 GB (5159999000 B)         Inbound:         5.03 GB (5400000000 B)         09:09:05 (13145 sec)         09:09:04 (13144 sec)         00:00:00:00:00:00:00:00:00:00:00:00:00:  |
|             |  |                                     |                     |             |                     | Remaining Lifetime for SPI ID: 0xE175D4C8  |
|             |  |                                     |                     |             |                     | Inbound:         4.97 GB (534000000 B)         Outbound:         4.75 GB (5099999000 B)         O9:09:09:05 (13145 sec)         09:09:04 (13144 sec)         O9:09:04 (13144 sec)         O9:04 (13144 sec)         O9:04 (13144 sec) |
|             |  |                                     |                     |             |                     | 10.10.1.19 (VPN Interface IP: 192.168.105.19)  |
|             |  |                                     |                     |             |                     | 📀 show crypto ipsec sa peer 192.168.105.20 🖥   |
|             |  |                                     |                     |             |                     | 📀 show vpn-sessiondb detail 121 filter ipaddress 192.168.10 🎦  |
|             |  |                                     |                     |             |                     |  |
|             |  |                                     |                     |             |                     |  |

### Site to Site Monitoring in 7.4

| <b>Firewa</b><br>Overview | all Managem                            | ent Center<br>Site to Site VPN | view Analysis       | Policies          | Devices         | Objects          | Integration         |               |     |                  | Deploy Q                                     | 🗳 🌣 🕜 🛛 admir                       | ~ ahaha<br>cisco | SECURE |
|---------------------------|--|--------------------------------|---------------------|-------------------|-----------------|------------------|---------------------|---------------|-----|------------------|--|-------------------------------------|------------------|--------|
| ▼ Select                  | Tunnel De                              | etails                         |                     |                   |                 |                  |                     | 0 ×           |     |                  | × Refresh                                    | Refresh every 5                     |                  | ~ ►    |
| Node A                    | Summary                                |                                |                     |                   |                 |                  |                     |               | î I | A: 10.10.1.19    | ←→ B: 10.10.1.2                              | 0                                   |                  | ×      |
| 10.10.1.1                 | 9 ( Node A (192.16                     | 8.105.19/500) 💡                |                     | 🤌 Nor             | de B (192.168.1 | 05.20/500) 💡     |                     |               |     | Topology: VPN    | I106-DVTIv4   Status                         | : 📀 Active                          |                  |        |
| 10 10 1 1                 | Transmitted:                           | 560 Bytes (560 B)              |                     | Tra               | nsmitted: 56    | 0 Bytes (560 B)  |                     |               |     | General          | CLI Details Pack                             | et Tracer                           |                  |        |
| 10.10.1.1                 | Received:                              | 0 (0 В)                        |                     | Rec               | ceived: 0       | (0 B)            |                     |               |     | e Defeech        | A Manimira view                              |                                     |                  |        |
| 10.10.1.1                 | 9 (                                    |                                | IPsec S             | Security Assoc    | ciations (1)    |                  |                     |               |     | C Refresh        |  |                                     |                  | Ē      |
| 10.10.1.1                 | 9 ( 😪 192.168.15.                      | 0/255.255.255.0/0/0            |                     | 192               | .168.25.0/255.2 | 255.255.0/0/0    |                     |               |     | Summary          |  |                                     |                  |        |
| 10 10 1 1                 | a (                                    |                                | L2L Tunr            | nel PFS Group     | 21 IKEv2        | VTI              |                     |               | No  | ode A (192.168.1 | 105.19/500) 😭                                | Node B (192.168.105.                | 20/500) 😭        |        |
|                           | Encaps/Enc                             | crypt: 20 / 20 pkts            |                     | Encaj             | ps/Encrypt:     | 20 / 20 pkts     |                     |               | Tr  |                  | 0 Bytes (560 B)                              | Transmitted: 560 B                  | /tes (560 B)     |        |
| 10.10.1.1                 | ) ( Dcaps/Dec                          | rypt: 0 / 0 pkts               |                     | Dcap              | s/Decrypt:      | 0 / 0 pkts       |                     |               | Re  | ceived: 0 (      | ов)  | Received: 0 (0 B                    |                  |        |
| FTD02-EX                  | TE                                     |                                | Remaining           | g Lifetime for SP | 11D: 0x2E5F96   | A1               |                     |               |     |                  | IPsec Security                               | Associations (1)                    |                  |        |
|                           | Outbound:                              | 4.81 GB (5159999000 B)         |                     | Inbou             | ind: 5.03       | GB (540000000    | ) В)                |               |     | 102 168 15 0/2   | 255 255 255 0/0/0                            | 102 168 25 0/255 255                | 255 0/0/0        |        |
| 10.10.1.1                 | ין ∟                                   | 08:53:49 (12229 sec)           |                     |                   | 08:5            | 3:48 (12228 sec) |                     |               | Ĭ   |                  |  |                                     | •                |        |
| 10.10.1.1                 | 9 (                                    |                                | Remaining           | g Lifetime for SP | 1 ID: 0xE175D4  | C8               |                     |               |     |                  | L2L Tunnel PF                                | S Group 21 IKEV2 VI                 |                  |        |
|                           | Inbound:                               | 4.97 GB (5340000000 B)         |                     | Outb              | ound: 4.75      | GB (5099999000   | ) B)                |               |     |                  | /pt: 20 / 20 pkts                            | Encaps/Encrypt: 20 /                | 20 pkts          |        |
| 10.10.1.1                 | ــــــــــــــــــــــــــــــــــــــ | 08:53:49 (12229 sec)           |                     |                   | 08:5            | 3:48 (12228 sec) |                     |               |     |                  | pt: 0 / 0 pkts                               | Dcaps/Decrypt: 0/0                  |                  |        |
| 10.10.1.1                 | 9 (                                    |                                |                     |                   |                 |                  |                     |               |     |                  | Remaining Lifetim                            | e for SPI ID: 0x2E5F96A1            |                  |        |
|                           | 10.10.1.19                             | (VPN Interface IP: 192.1       | 68.105.19)          | 10.               | .10.1.20 (VF    | N Interface ]    | IP: 192.168.105.20) |               |     |                  | .81 GB (5159999000 B)<br>8:53:49 (12229 sec) | Inbound: 5.03 GB (54<br>08:53:48 (1 |                  |        |
|                           | Show cry                               | /pto ipsec sa peer 192.16      | 8.105.20 🔓          | <u>^</u> (>)      | show crypto     | ipsec sa pee     | er 192.168.105.19   | <b>.</b>      |     |                  |  | e for SPI ID: 0xE175D4C8            |                  |        |
|                           | peer addres                            | s: 192.168.105.20              |                     | $\bigcirc$        | show vpn-se     | ssiondb detai    | il 121 filter ipadd | ress 192.1… 🔓 |     |                  |  |                                     |                  |        |
|                           | interface:                             | DVTI105_va4                    |                     |                   |                 |                  |                     |               |     |                  | 8:53:49 (12229 sec)                          | 08:53:48 (1                         | 2228 sec)        |        |
|                           | Crypto                                 | map tag: DVTI105_vtempla       | ite_dyn_map, seq nu | ım: 1,            |                 |                  |                     |               |     |                  |  |                                     |                  |        |
|                           |  |                                |                     |                   |                 |                  |                     |               | -   | 10.10.1.19 (\    | VPN Interface IP: 1                          |                                     |                  |        |
|                           | Prote                                  | ected vrf (ivrf): Global       |                     |                   |                 |                  |                     |               | 0   | > show crypt     | to ipsec sa peer 19                          | 2.168.105.20 🖷                      |                  |        |
|                           | local                                  | l ident (addr/mask/prot/p      | oort): (192.168.15. | .0/255            |                 |                  |                     |               | -   | > show vpn-      | sessiondb detail 12                          | l filter ipaddress 1                | 92.168.10        | - 6    |
|                           |  |                                |                     |                   |                 |                  |                     | Defeat        |     |                  |  |                                     |                  |        |

## CLI configuration to onboard FTDv



Allows management on outside interface for cdFMC connectivity

| > 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: 3883  |
| Netmask/IPv6 Prefix: 255.255.255.0   |
| Default Gateway: 38.   |
| Configuration done with option to allow FMC access from any network, if you wish<br>to change the FMC access network use the 'client' option in the command 'config<br>ure network management-data-interface'. |

- Physical firewalls offer "Low Touch Provisioning" based on serial # to cdFMC
- Virtual firewalls offer CLI provisioning.
- "configure network management-data-interface" to manage firewall on outside interface

### Secure Firewall Threat Defense / ASA

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

- Use VTI interfaces for all VPN tunnels including Cloud IaaS & SASE / SSE deployments!
- Use to ASA 9.19 or FTD 7.3+ for DVTI HUB support!
- Must use routing protocol for DVTI hub spoke topologies

- Policy Based Routing on FTD to prioritize Internet links or tunnels to optimize security and end user experience!
- BGP recommended for Hub & Spoke VPN deployments, SASE / SSE integrations and more!







# Thank you





cisco live!

Let's go