Troubleshooting SD-WAN IPsec SIG Tunnels

Tushar Jagtap
Technical Consulting Engineer

Alain Perez
Technical Consulting Engineer

Session ID: TACENT-2027

CISCO CERTIFIED CCNP ENTERPRISE

CISCO CERTIFIED SPECIALIST

Agenda

01 Secure Internet GW Overview

02 Prerequisites

03 Configuration

04 Verification

05 Monitoring

06 Troubleshooting Scenarios

07 Q & A

Overview

Acronyms Used

SIG - Secure Internet Gateway

DIA - Direct Internet Access

NTP – Network Time Protocol

NAT – Network address Translation

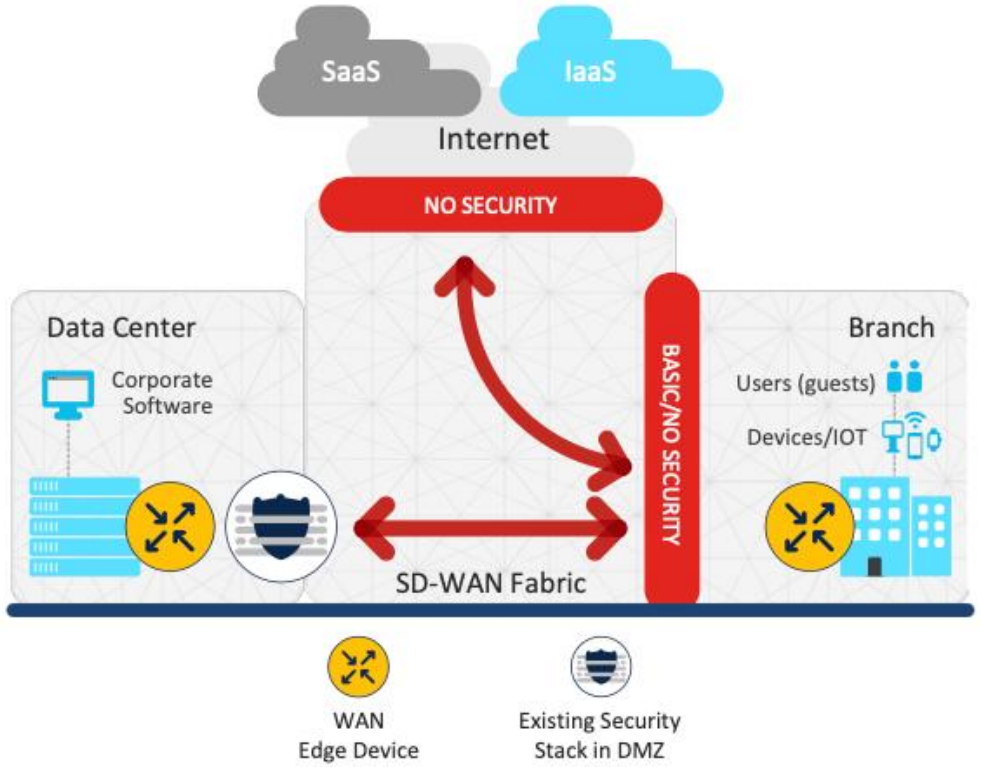
FTM – Forwarding table Manager

FSM - Finite State Machine

PCI - Payment Card Industry

HIPAA - Health Insurance Portability and Accountability Act

Overview



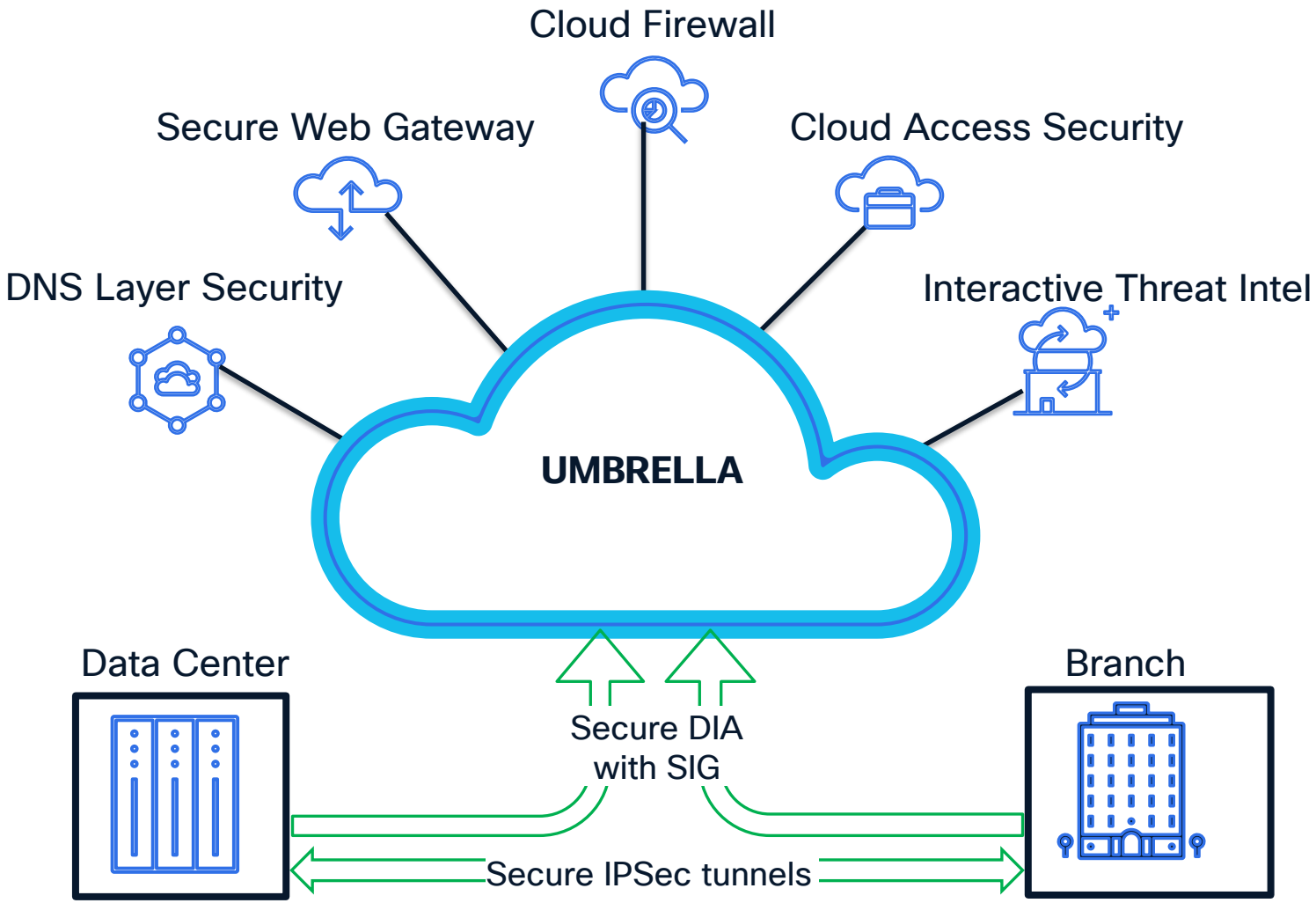
External Threats

- Exposure to malware & phishing due to direct internet and cloud access
- Data breaches
- Guest access liability

Internal Threats

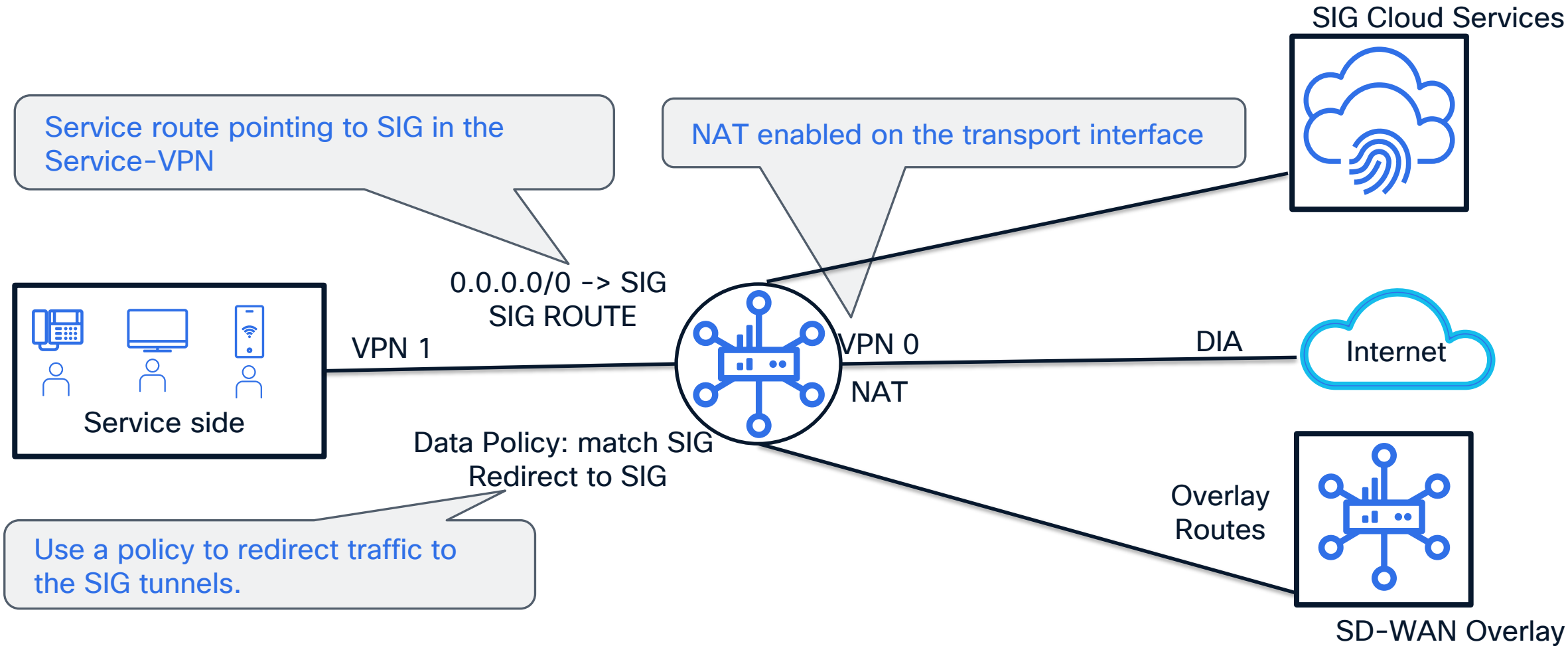
- Untrusted access (malicious insider)
- Compliance (PCI, HIPAA)
- Lateral movements (breach propagation)

Cisco SD-WAN SIG Tunnel Security Features



Prerequisites

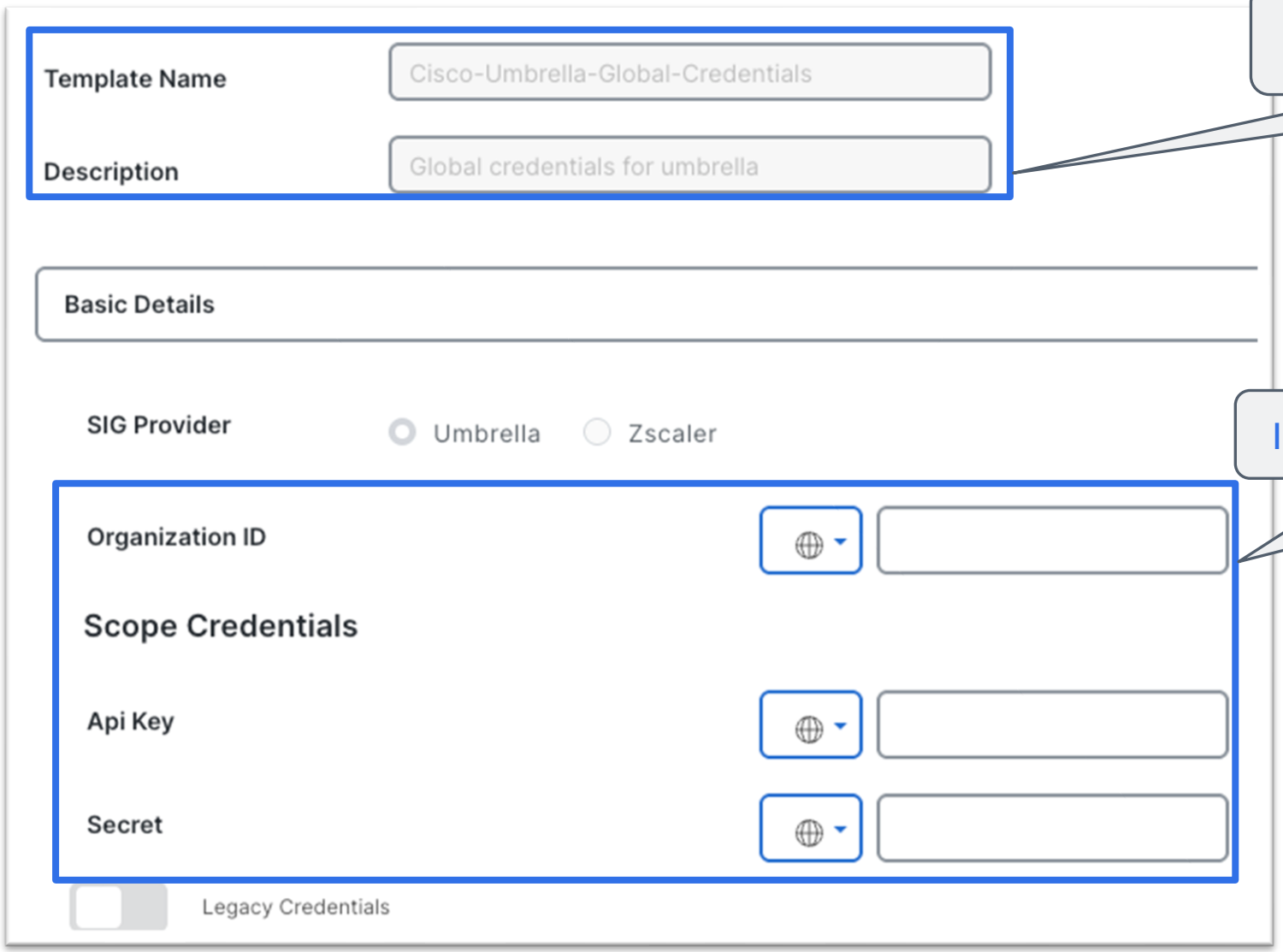
Prerequisites



Configuration via GUI

Configuration via GUI

Configuration → Template → SIG Credential

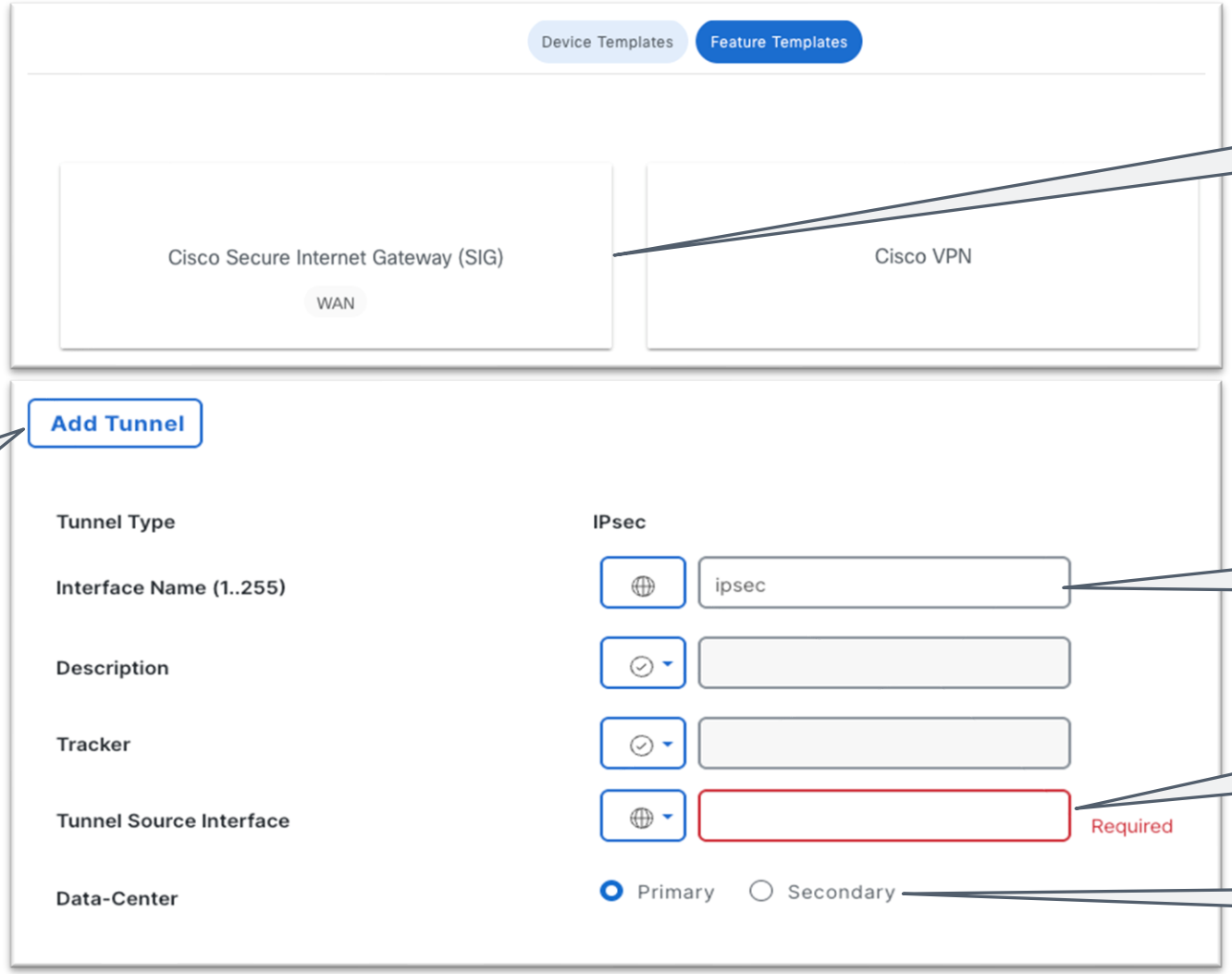


Provide Template name and description

Input organization ID, registration & secret

Configuration via GUI

Configuration → Feature Template → Cisco Secure Internet Gateway



Select Cisco “SIG” Template

Add Tunnel

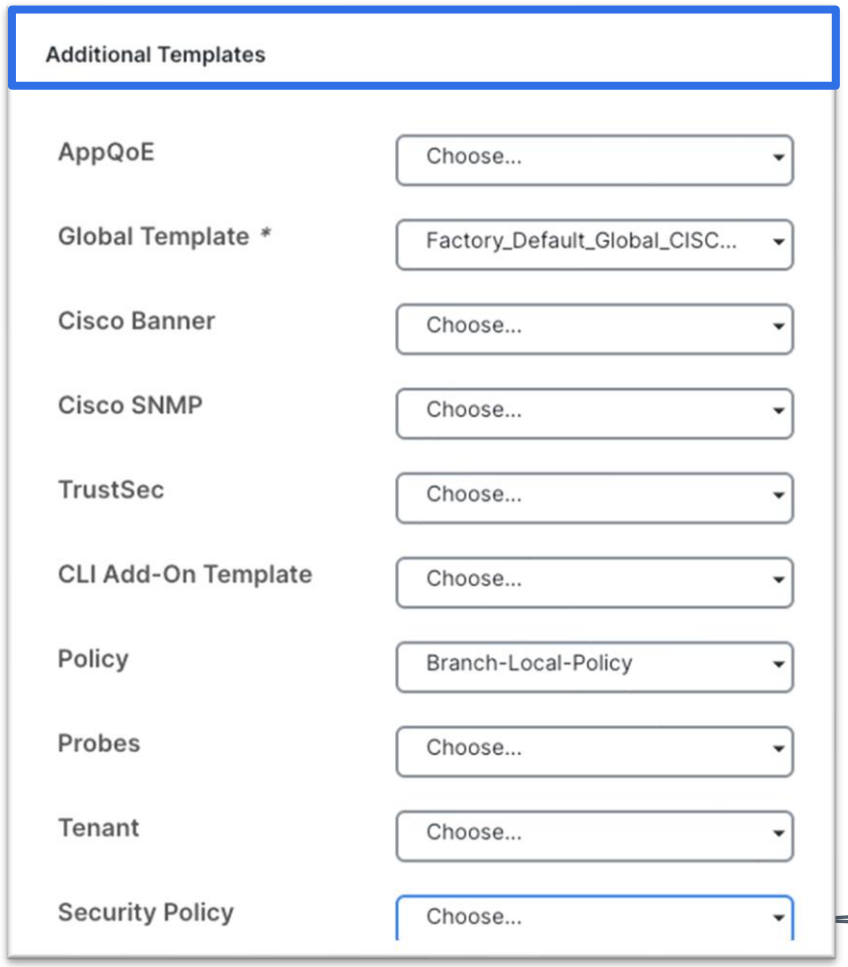
Input interface name

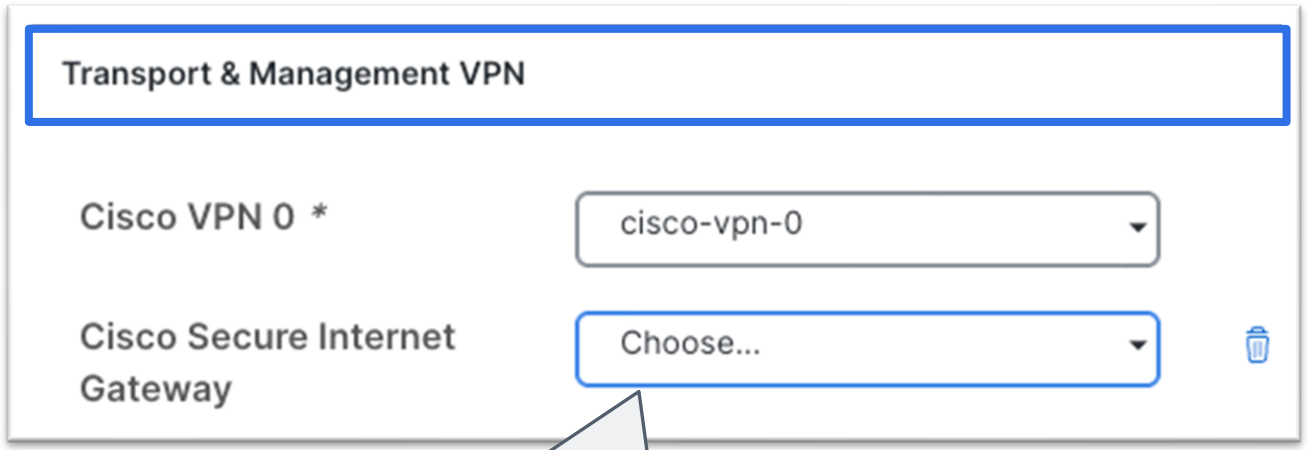
Input source interface

Select DC Role

Configuration via GUI

Configuration → Template → Device Template



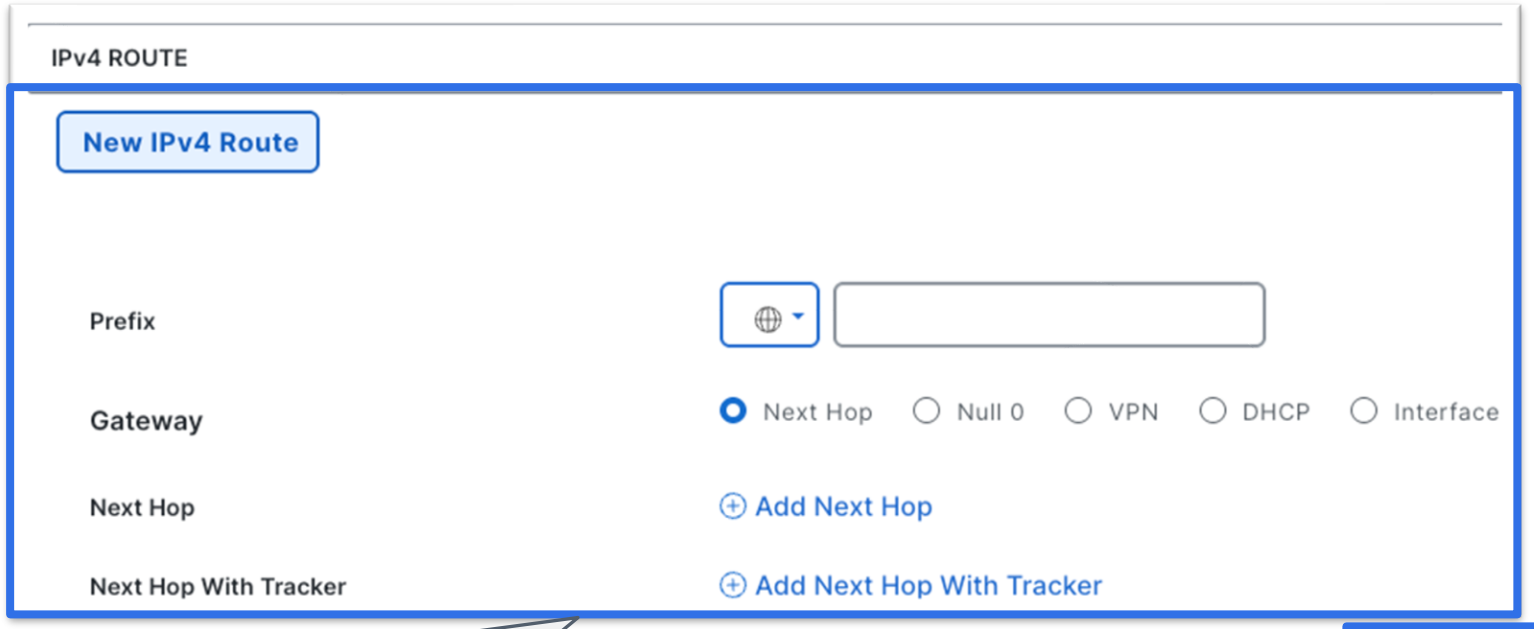


Add previously created SIG feature template.

Add previously created SIG credential template.

Configuration via GUI

Configuration → Template → Device Template



In Service VPN template, Navigate to section Service Route and add a 0.0.0.0 with SIG Service Route.

Other way to redirect traffic to SIG tunnels is by using a data policy and under action set SIG.
In this example

```
vSmart# show running-config policy
Policy
  data-policy _VPN10_sig-default
    vpn-list VPN10
       sequence 1
          match
                source-data-prefix-
list Default
             !
             action accept
                sig
```

Configuration CLI Preview

SIG CLI Config Preview

SIG credential config

SIG Credential config

```
Show sdwan run | sec secure-internet-gateway
secure-internet-gateway
 umbrella org-id 8XXX5
 umbrella api-key 3XXXXXXXXX4
 umbrella api-secret "$8XXXXXXXXX=="
```

SIG service global config

SIG global config
- Here we can we have 2 tunnels, 1 active and 1 backup

```
Show sdwan run | sec service sig
service sig vrf global
  ha-pairs
   interface-pair Tunnel100001 active-interface-weight 1 Tunnel100021 backup-interface-weight 1
```

SIG source loopback interface

Interface loopback config
-The Private IP address used should be unique

```
 interface Loopback65528
no shutdown
vrf forwarding 65528
ip address 192.168.10.10 255.255.255.255
```

SIG Configuration CLI

MTU 1400 TAC Tip

SIG tunnel config

Tunnel preference and source interface

```
interface Tunnel100001
  tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc source-interface
GigabitEthernet2
interface Tunnel100021
  tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference secondary-dc source-interface
GigabitEthernet3
```

```
interface Tunnel100001
 description Transport1
 no shutdown
 ip unnumbered       GigabitEthernet2
 no ip clear-dont-fragment
 ip mtu              1400
 tunnel source GigabitEthernet2
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec1-ipsec-profile
 tunnel vrf multiplexing
 tunnel route-via GigabitEthernet2 mandatory
```

```
interface Tunnel100021
 description Transport2
 no shutdown
 ip unnumbered       GigabitEthernet3
 no ip clear-dont-fragment
 ip mtu              1400
 tunnel source GigabitEthernet3
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec21-ipsec-profile
 tunnel vrf multiplexing
 tunnel route-via GigabitEthernet3 mandatory
```

Tunnel destination is set to dynamic in auto mode

SIG Configuration CLI

SIG tunnel IKEv2 settings

```
crypto ikev2 policy policy1-global
 proposal p1-global

crypto ikev2 profile if-ipsec1-ikev2-profile
 no config-exchange request
 dpd 10 3 on-demand
 dynamic
 lifetime 14400

crypto ikev2 profile if-ipsec21-ikev2-profile
 no config-exchange request
 dpd 10 3 on-demand
 dynamic
 lifetime 14400

crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 group 14 15 16 19 20 21
 integrity sha1 sha256 sha384 sha512
```

IKEv2 parameters
The DPD (keepalive) encryptions & integrity type accepted.

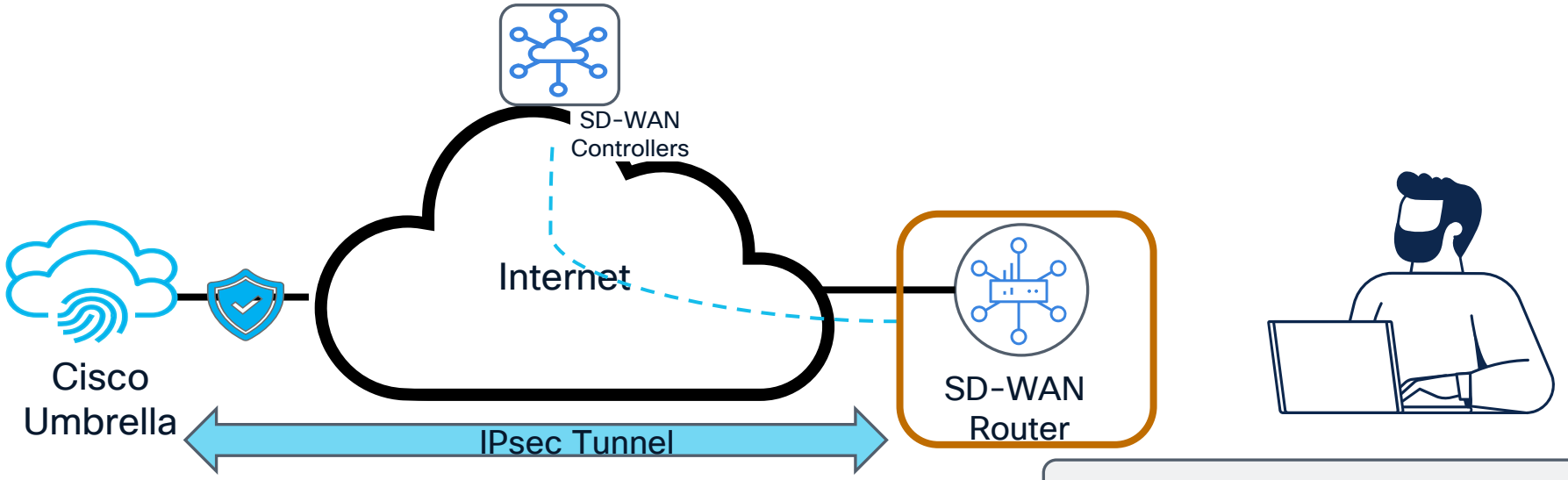
SIG tunnel IPSec settings

```
crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256
 mode tunnel
crypto ipsec transform-set if-ipsec21-ikev2-transform esp-gcm 256
 mode tunnel

crypto ipsec profile if-ipsec1-ipsec-profile
 set ikev2-profile if-ipsec1-ikev2-profile
 set transform-set if-ipsec1-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512

 set ikev2-profile if-ipsec21-ikev2-profile
 set transform-set if-ipsec21-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
```

IPsec parameters
- IKEv2 profile, Encryptions

Verification

Verify Tunnel Creation from the CLI Edge Device



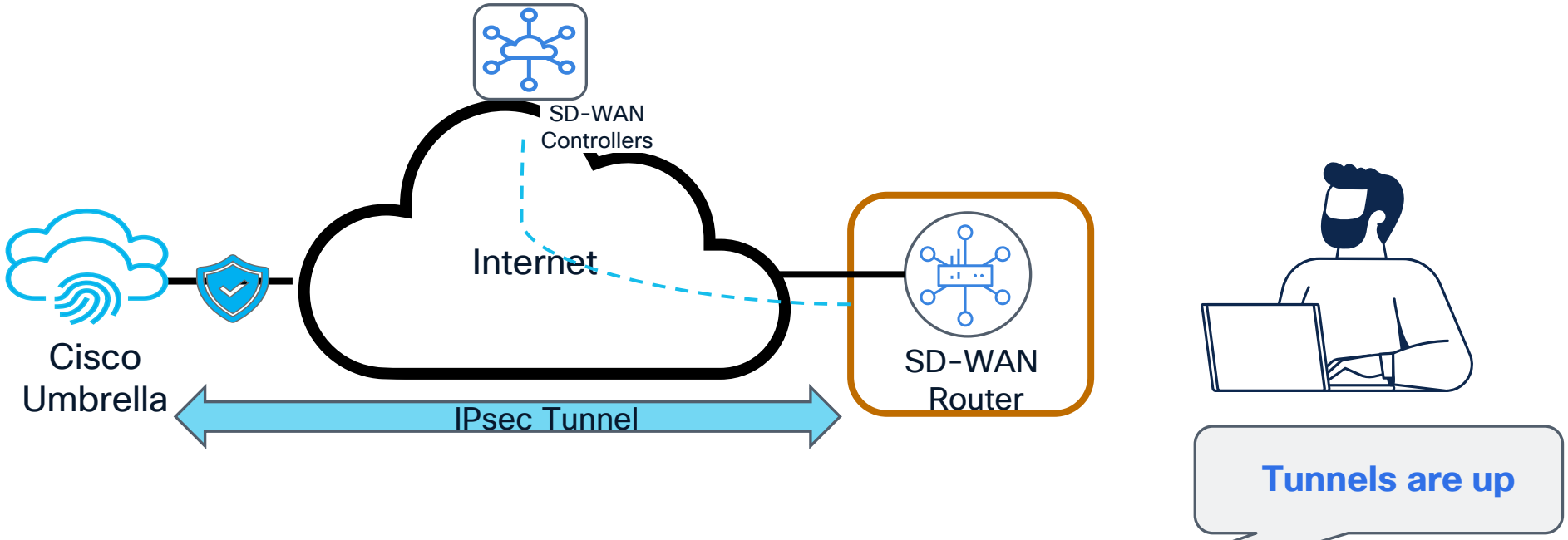
HTTP 200 = Successful API call

 # show sdwan secure-internet-gateway umbrella tunnels

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	650765613	SITE87617586GSYS10x1x0x50ITunnel100001	st-tun-create-notif	200	create-tunnel
Tunnel100021	650765614	SITE87617586GSYS10x1x0x50ITunnel100021	st-tun-create-notif	200	create-tunnel

Successful Request

Verify Tunnel Status from the CLI Edge Device

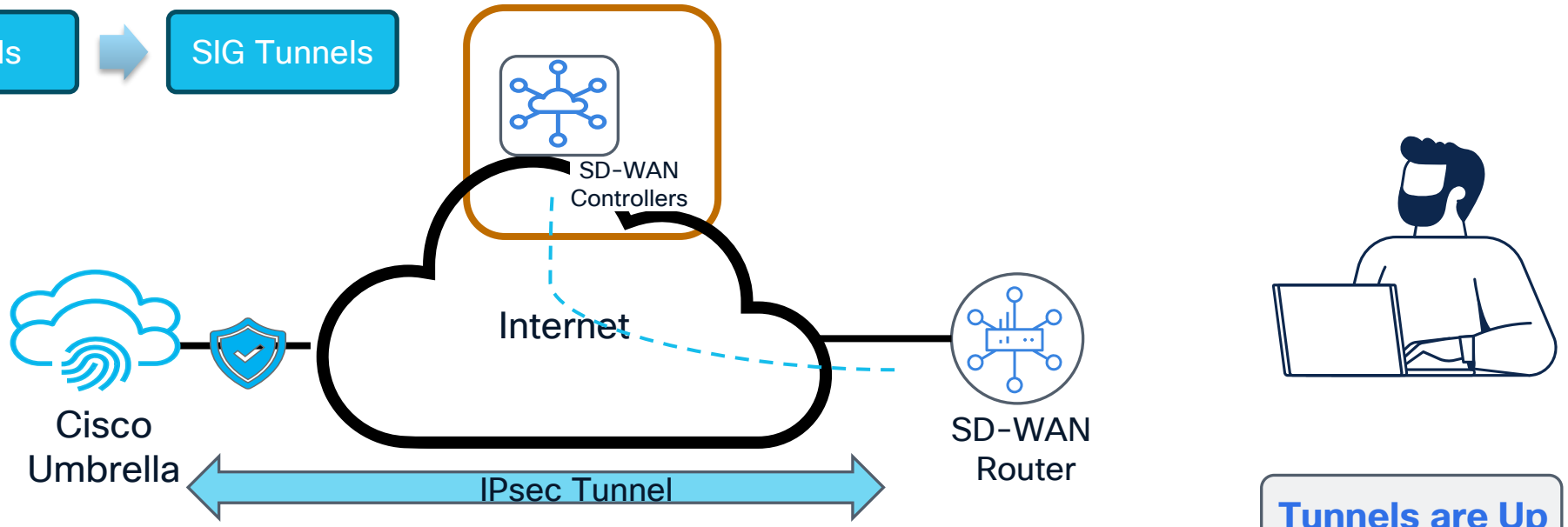


 # show sdwan secure-internet-gateway tunnels

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	HA PAIR	DEVICE STATE	SIG STATE	TRACKER STATE	SITE ID	DESTINATION DC	PROVIDER	TUNNEL TYPE
Tunnel100001	650765613	SITE87617586GSYS10x1x0x50ITunnel100001	Active	Up	UP	Enabled	87617586	Equinix Los Angeles	Umbrella	IPsec
Tunnel100021	650765614	SITE87617586GSYS10x1x0x50ITunnel100021	Backup	Up	UP	Enabled	87617586	Equinix Santa Clara	Umbrella	IPsec

Verify Tunnel Status Using SD-WAN vManage GUI

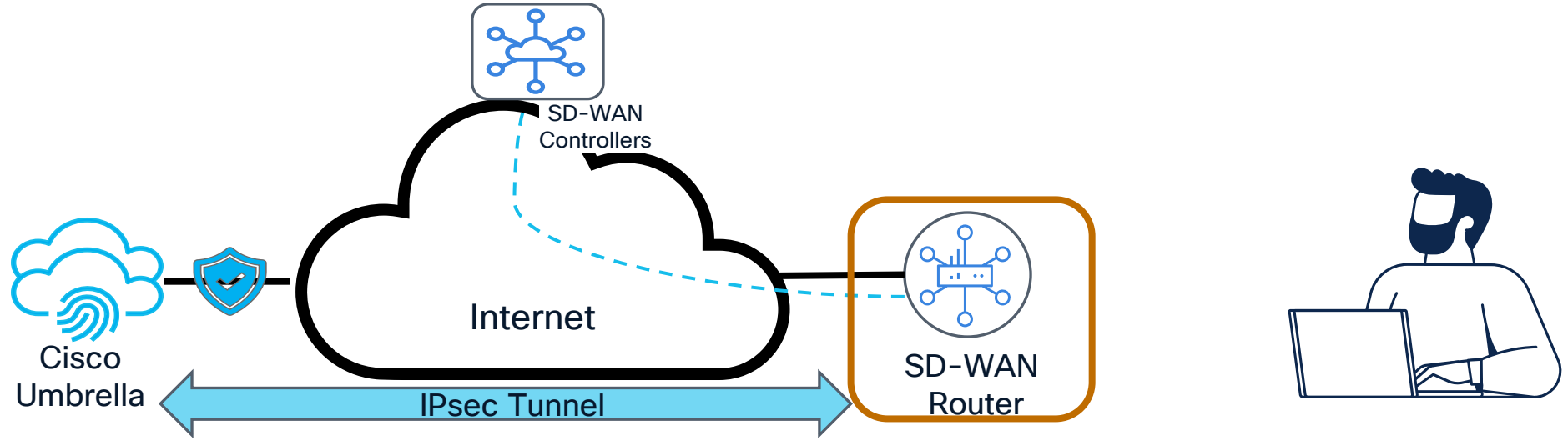
Monitor → Tunnels → SIG Tunnels



Tunnels are Up

Host Name	Site Name	Tunnel ID	Transport Type	Tunnel Name	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)	Events
cEdge_DC1_West_R01	SITE_87617586	650891107	IPsec	SITE87617586SYS10x1x0x50IFTunnel100001	Active	Umbrella	Equinix Los Angeles	Up	UP	18
cEdge_DC1_West_R01	SITE_87617586	650891108	IPsec	SITE87617586SYS10x1x0x50IFTunnel100002	Active	Umbrella	Equinix Santa Clara	Up	UP	18
cEdge_DC1_West_R01	SITE_87617586	650891109	IPsec	SITE87617586SYS10x1x0x50IFTunnel100011	Backup	Umbrella	Equinix Los Angeles	Up	UP	18
cEdge_DC1_West_R01	SITE_87617586	650891110	IPsec	SITE87617586SYS10x1x0x50IFTunnel100021	Backup	Umbrella	Equinix Santa Clara	Up	UP	18

Route Validation CLI Edge Device




```
Router# show ip route vrf 65528
Routing Table: 65528
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

n*Nd  0.0.0.0/0 [6/0], 2d00h, Null0
      10.0.0.0/32 is subnetted, 1 subnets
S        10.0.0.1 [2/65535], Tunnel100001
                  [2/65535], Tunnel100002
```

NAT route is automatically created in this VRF to send the traffic to VPN-0

Static route added for tunnels

```
Router# show ip route vrf 1
Routing Table: 1
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
 S*    0.0.0.0/0 [2/65535], Tunnel100001
                 [2/65535], Tunnel100002
```

Auto-Tracker Status CLI Edge Device

Probes are initiated from VRF 65530

TAC Tip

Endpoint Tracker Config

Endpoint Tracker Configured

Router# show endpoint-tracker records

Record Name	Endpoint	EndPoint Type	Threshold (ms)	Multiplier	Interval (s)	Tracker-Type
#SIGL7#AUTO#TRACKER	http://service.sig.umbrella.com	API_URL	1000	2	30	interface

Verify the Endpoint Tracker Status

Router# show endpoint-tracker

Interface	Record Name	Status	RTT (ms)	Probe ID	Next Hop
Tunnel100001	#SIGL7#AUTO#TRACKER	Up	27	158	None

Tracker is up and tied to ip SLA

IP sla status

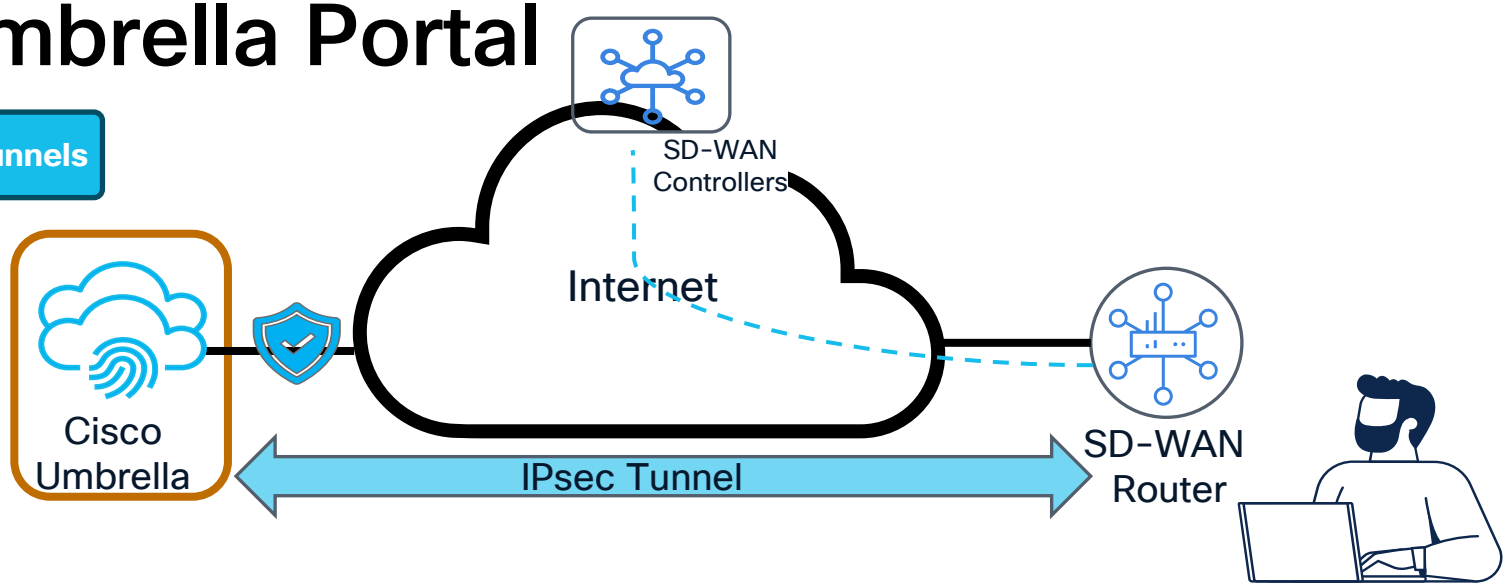
Router# show ip sla summary

ID	Type	Destination	RTT (ms)	Return Code	Last Run
134	http	146.112.255.40	66	OK	26 sec ago

IP SLA status is ok

Verify SIG Tunnel from Umbrella Portal

From Side Pane → Deployments → Network Tunnels



Active Tunnels For The Site

Search Site ID

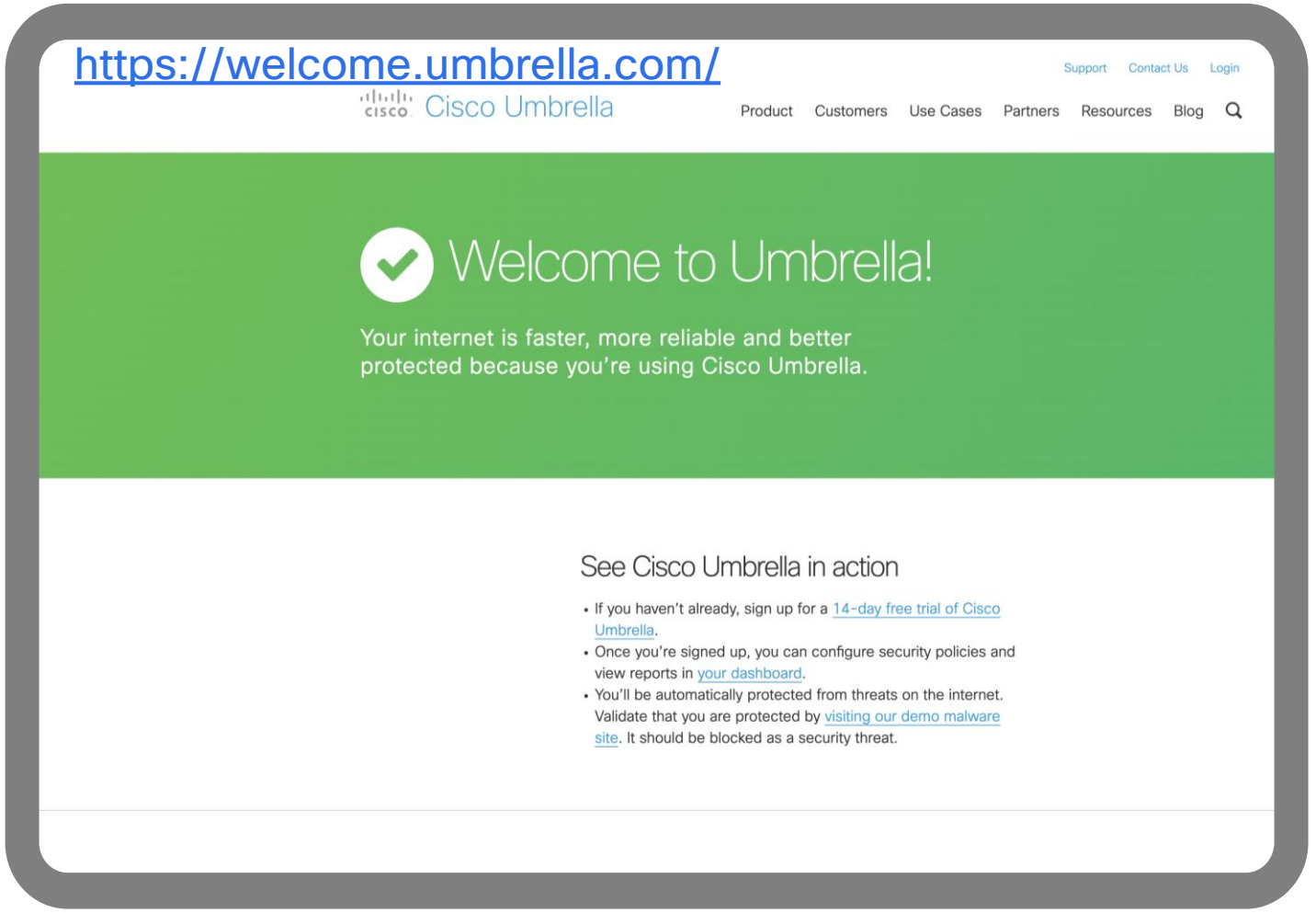
Tunnels Are Active

Active Tunnels	Inactive Tunnels	Unestablished Tunnels	Unknown Tunnel Status	Data Center Locations
4	0	0	0	2

FILTERS | SITE8761 | CLEAR

Tunnel Name	Site	Data Center Location	Device Public IP	Tunnel Status	Last Status Update
SITE87617586SYS10x... Secure Internet Access	Default Site	Los Angeles, California - US	44.225.52.105	Active	Apr 28, 2025 - 2:36 PM
SITE87617586SYS10x... Secure Internet Access	Default Site	Santa Clara, CA - US	44.225.52.105	Active	Apr 28, 2025 - 2:36 PM

Congratulations! Your Tunnels are Up

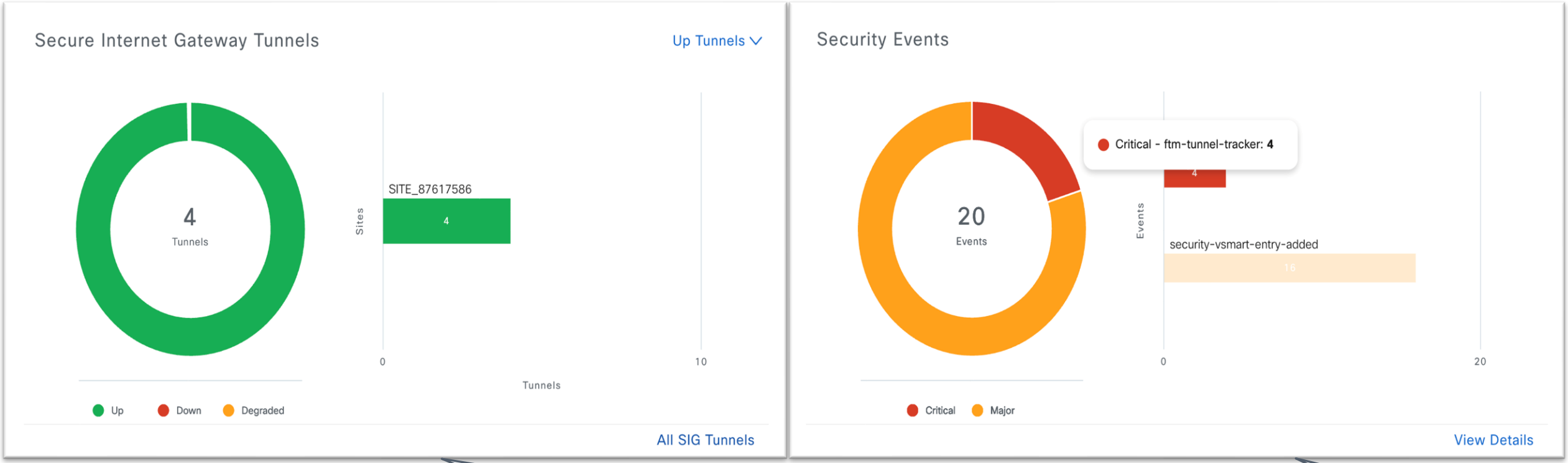


Client Machine

Monitoring

SD-WAN vManage GUI

Monitor → Security → SIG Tunnels

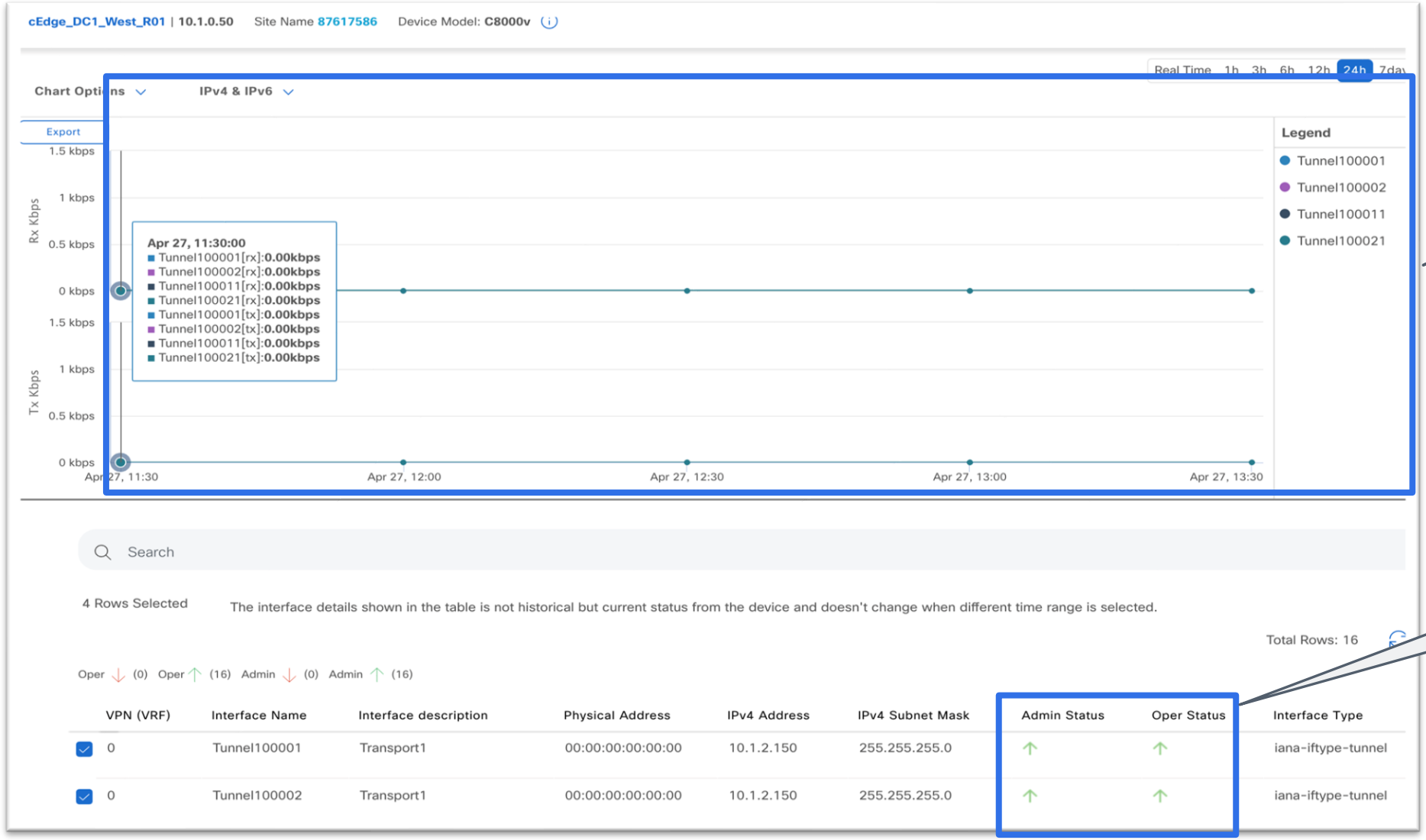


Shows UP, Down & Degraded state

Granular Details for Tunnels

SD-WAN vManage GUI

Monitor → Devices → Interface

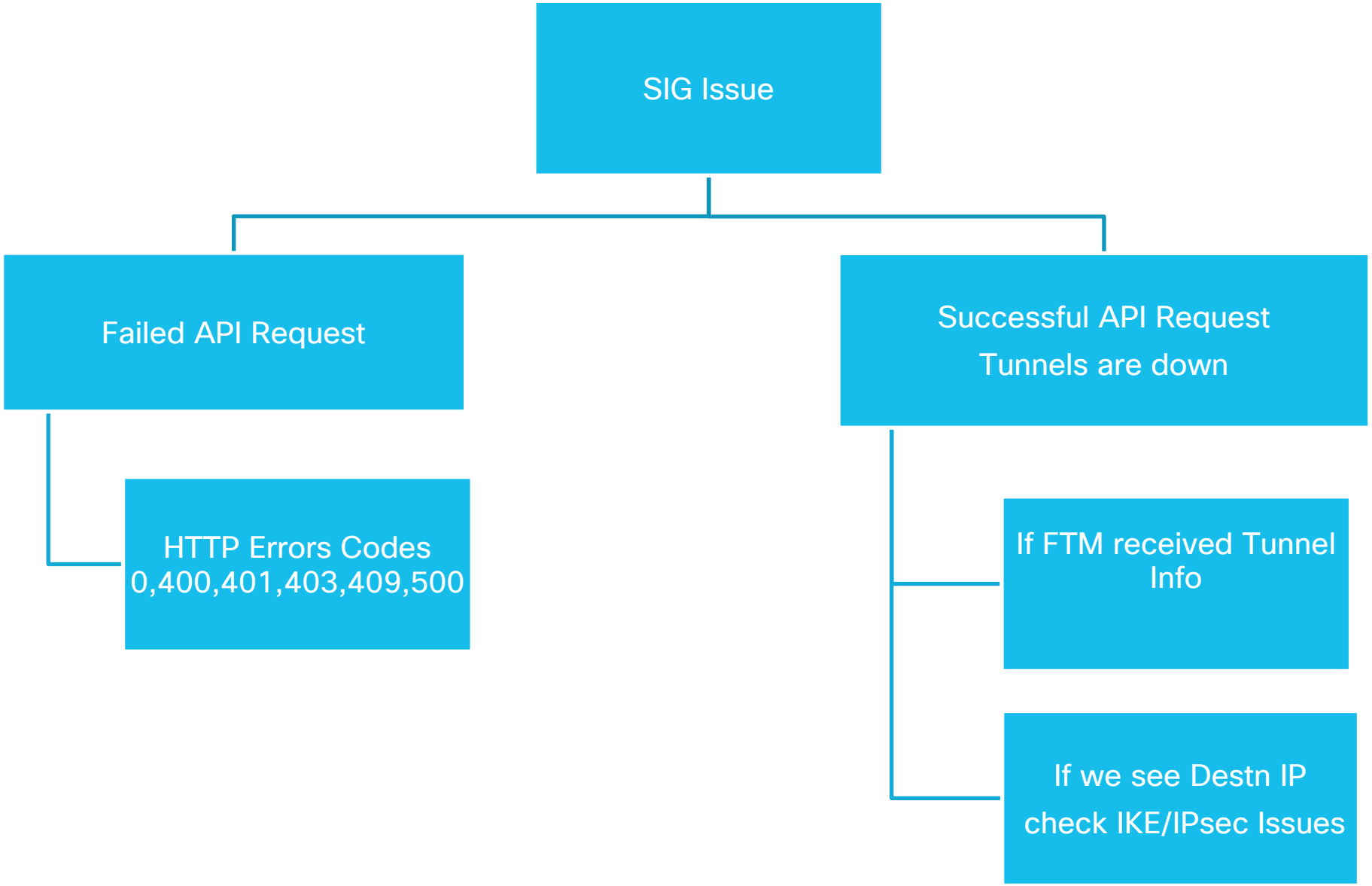


Traffic over Tunnel

Tunnel Status

Troubleshooting

High Level Troubleshooting Workflow



Cheat Sheet

TAC Tip

Show Commands

- Show sdwan secure-internet-gateway tunnels
- Show sdwan secure-internet-gateway umbrella tunnels

SIG-Specific Debug

- Debug platform software sdwan sig
- Debug platform software sdwan ftm sig
- Debug platform software sdwan tracker
- Debug platform software sdwan ftm rtm-events

To show the logs for above enabled logs

- show sdwan ftm log-error
- show logging process ftmd_R0 internal start last 5 minutes
- show logging process ftm internal | i sig
- show Logging | I sig

Tracker Debug

- Debug platform software sdwan ftm sig
- Debug ip sla events
- Debug ip sla errors
- Debug ip sla trace

IKE / IPSEC Debug

- Debug crypto ikev2
- Debug crypto ikev2 packet
- Debug crypto ikev2 internal
- Debug crypto ipsec
- Debug crypto ipsec error

To show the logs for above enabled logs

- show crypto ike sessions
- show crypto ikev2 sa [detail]
- show crypto session detail
- show logging | sec include ikev2

SIG Debugs for newer release

- Debug platform software sdwan ftm rtm-events
- Debug platform software sdwan ftm fnf
- show sdwan ftm log-show error
- show logging process ftm internal | i sig
- show Logging | I sig

HTTP Response Codes and Recommended Actions

HTTP Error Codes

Status Code	Description	Recommended Action
0	Missing network config	Configure DIA, DNS, and NTP
400	Bad request. Corrupted Syntax .	Validate and correct the umbrella parameters
401	Unauthorized token.	Reconfigure or update the token.
404	Resource not found. ORG-ID mismatch.	Update correct ORG-ID in the template.
409	Device conflict or tunnel names not unique.	Ensure tunnel names are unique.
500	Internal server error.	Check with Umbrella Administrator.

Scenario 1: HTTP 0
SIG Tunnels configured via vManage are down due to failed API requests

Failure Analysis

Tunnels in up/down state

Router# show ip int brief | i Tunnel100

Tunnel100001	10.1.2.150	YES TFTP	up	Down
Tunnel100002	10.1.2.150	YES TFTP	up	Down

Failed API Request

Router# show sdwan secure-internet-gateway umbrella tunnels

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	650765613	SITE87617586GSYS10x1x0x50ITunnel100001	st-tun-create-req	0	invalid

 # show sdwan secure-internet-gateway tunnels

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	HA PAIR	DEVICE STATE	SIG STATE	TRACKER STATE	SITE ID	DESTINATION DATA CENTER PROVIDER	TUNNEL TYPE
Tunnel100001	0	SITE87617586SYS10x1x0x50IFTunnel100001	Active	-	-	Enabled	87617586	Umbrella	IPsec

Tunnel state is blank

Scenario 1: HTTP 0
SIG Tunnels configured via vManage are down due to failed API requests

Analyzing the Logs

Enable SIG debugs

Router # show sdwan ftm log-error

```
==========================================================================
[Idx]  Time          <Log message>  (Shown last entry first)
==========================================================================
[278]   23:16:33:793   HTTP request failed with response-code = 0 will retry(retryCnt=4)
```

HTTP 0
Missing Basic configuration
DIA, DNS and NTP Config.

Scenario 2: HTTP 400
SIG Tunnels configured via vManage are down due to failed API requests

Failure Analysis

Failed API Request

Router# show sdwan secure-internet-gateway umbrella tunnels

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	650765613	SITE87617586GSYS10x1x0x50lTunnel100001	st-tun-add-rest-failed	400	invalid

Analyzing the Logs

Enable SIG debugs

Router# show sdwan ftm log-error

```
============================================================
[Idx]        Time          <Log message>  (Shown last entry first)
============================================================
[169]  21:32:46:812  REST call failed for if=Tunnel100001
[168]  21:32:46:812  HTTP request failed with response-code = 400 , response-msg={"message":"INVALID_INPUT_ARGUMEN"}.
```

HTTP 400 – Bad Request:
The server rejects the request due to a client-side error, such as malformed syntax, invalid message structure, or suspicious routing.

Scenario 3: HTTP 401
SIG Tunnels configured via vManage are down due to failed API requests

Failure Analysis

Failed API Request

Router# show sdwan secure-internet-gateway umbrella tunnels

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	650765613	SITE87617586GSYS10x1x0x50lTunnel100001	st-tun-add-rest-failed	401	invalid

Analyzing the Logs

Enable SIG debugs

Router# show sdwan ftm log-error

```
==========================================================================
[Idx]        Time            <Log message>  (Shown last entry first)
==========================================================================
[190]  21:32:46:812  REST call failed for if=Tunnel100001
[189]  21:32:46:812  HTTP request failed with response-code = 401, response-msg={"message":"Unauthorized"}
```

HTTP 401
Unauthorized Request.
Authentication failure; missing or invalid credentials

Scenario 4: HTTP 404
SIG Tunnels configured via vManage are down due to failed API requests

Failure Analysis

Failed API Request

Router# show sdwan secure-internet-gateway umbrella tunnels

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	650765613	SITE87617586GSYS10x1x0x50ITunnel100001	st-tun-add-rest-failed	404	invalid

Analyzing the Logs

Enable SIG debugs

Router# show sdwan ftm log-error

```
==========================================================================
[Idx]        Time            <Log message>  (Shown last entry first)
==========================================================================
[190] 1:44:43:942   REST call failed for if=Tunnel100001
[189] 1:44:43:942   HTTP req failed with response-code =404, response-msg={"msg":"no Route Matched with those values"}
```

HTTP 404:
Resource not found
ORG-ID mismatch – update the correct ORG-ID in the feature template

Scenario 5: HTTP 409
SIG Tunnels configured via vManage are down due to failed API requests

Failure Analysis

Failed API Request

Router# show sdwan secure-internet-gateway umbrella tunnels

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	650765613	SITE87617586GSYS10x1x0x50ITunnel100001	st-init	409	invalid

Analyzing the Logs

Enable SIG debugs

Router# show sdwan ftm log-error

```
==============================================================
[Idx]        Time            <Log message>  (Shown last entry first)
==============================================================
[572] 14:51:35:692  REST call failed for if=Tunnel100001
[571] 14:51:35:692  HTTP request failed with response-code=409, response-msg={"error":"Tunnel Name must be unique."}
```

HTTP 409
Conflict of Resource
Umbrella detects duplicate tunnels. Delete the duplicate entry on Umbrella and trigger tunnel rebuild from the router.

Scenario 6: HTTP 200
API call for SIG Tunnels succeeded, but tunnels remain down

Failure Analysis

Router# show ip int brief | i Tunnel100

Tunnel100001	10.1.2.150	YES TFTP	up	Down
Tunnel100002	10.1.2.150	YES TFTP	up	Down

Tunnels in up/down state

Successful API Request

Router# show sdwan secure-internet-gateway umbrella tunnels

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	650765613	SITE87617586GSYS10x1x0x50ITunnel100001	st-tun-create-notif	200	create-tunnel

Router# show sdwan secure-internet-gateway tunnels

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	HA PAIR	DEVICE STATE	SIG STATE	TRACKER STATE	SITE ID	DESTINATION DATA CENTER PROVIDER	TUNNEL TYPE
Tunnel100001	0	SITE87617586SYS10x1x0x50IFTunnel100001	Active	Down	-	Enabled	87617586	Umbrella	IPsec

Tunnel state is Down

Scenario 6: HTTP 200
API call for SIG Tunnels succeeded, but tunnels remain down

Analyzing the Logs

Enable SIG debugs

Router# show logging process ftm internal | inc sig

{ftmd_R0-0}{255}: [sig] [19352]: (debug): FSM moving **(prevSate=st-init)** st-tun-cfg-create->[**evt-send-create-req**]->st-tun-create-req

{ftmd_R0-0}{255}: [sig] [19352]: (debug):**Prep url for Umbrella**

{ftmd_R0-0}{255}: [sig] [19352]: (debug):**Sess=23 prepared URL=https://management.api.umbrella.com/v1/organizations/8xxxx5/tunnels**

{ftmd_R0-0}{255}: [sig] [19352]: (debug):**Sess=23 prepared j-son object={"name":"SITE87617586SYS10x1x0x50IFTunnel100001", "deviceType":"Viptela cEdge","resourceAttributes":{ "viptela:siteId":"87617586","viptela:deviceId":"C8K-xx-x-2x339"} }**

{ftmd_R0-0}{255}: [sig] [19352]: (debug): **Sess=23 prepared AUTH=Basic MzU2M2RmYTQxZjdmNGU5M2JmMmVjNznJiN=**

{ftmd_R0-0}{255}: [sig] [19352]: (debug): **Sending request request over GigabitEthernet2**

API call sent via GigabitEthernet 2 interface

{ftmd_R0-0}{255}: [sig] [19352]: (debug): Internal VRF 65528 exists

{ftmd_R0-0}{255}: [sig] [19352]: (debug): **Switched to namespace vrf.65528**

{ftmd_R0-0}{255}: [sig] [19352]: (debug): Successfully sent ADD_BY_NAME http-request for sess=23

{ftmd_R0-0}{255}: [sig] [19352]: (debug): Request state change INIT -> TRYING for sess 23

{ftmd_R0-0}{255}: [sig] [19352]:(debug):**SIG received HTTP responce for p_sess=0x0ba0(sess=23)with res-code=200 res-code-line=OK**

{ftmd_R0-0}{255}: [sig] [19352]: (debug): **Received response for sess: 23, http_res_code: 200, http_res: OK**

{ftmd_R0-0}{255}: [sig] [19352]: (debug): REST success for Auto tunnel add by name Tunnel100001

HTTP 200 OK response received

{ftmd_R0-0}{255}: [sig] [19352]: (debug): **Sending notification (Tunnel creation in SIG successful)**

{ftmd_R0-0}{255}: [sig] [19352]: (debug): **FSM moving (prevSate=st-tun-cfg-create) st-tun-create-req->[evt-send-create-notif]->st-tun-create-notif**

{ftmd_R0-0}{255}: [sig] [19352]: (debug): IF Name : SITE87617586SYS10x1x0x50IFTunnel100001

{ftmd_R0-0}{255}: [sig] [19352]: (debug): Request state change TRYING -> **SUCCESS for sess 23**

Scenario 6: HTTP 200
API call for SIG Tunnels succeeded, but tunnels remain down

Enable IPSEC debugs

Router# show interfaces Tunnel100001 | inc destination
Tunnel source 10.1.2.150 (GigabitEthernet2), destination 146.112.67.8

If Tunnel has valid destination IP
API call info is sent by Forwarding Traffic Manager process(FTM) to IOS

Router# show logging | inc OUTBOUND
(key eng. msg.) OUTBOUND local= 10.1.2.150:500, remote= 146.112.67.8:500

IKE packets are being Sent

Router# show logging | inc INBOUND
(key eng. msg.) INBOUND local= 10.1.2.150:500, remote= 146.112.67.8:500

IKE packets are being Received

In IKE failure cases ISP/connectivity/FW can trigger issue with building IPSec tunnel.

To further debug IPSEC issues, the following article can be used as a reference IKE Debug

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with Detailed sessions

LTRENT-2117 Implementing Catalyst SD-WAN Branch On-Prem and SASE Security

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

Contact us at: tusjagta@cisco.com , aperezre@cisco.com

Q&A

Thank you