cisco Live!

Let's go

The bridge to possible

Connecting Datacenters and Branch Offices to the Cisco SASE Platform

Fernando Ferrari – SSE Incubation TSA

BRKSEC-3022

Cisco Webex App

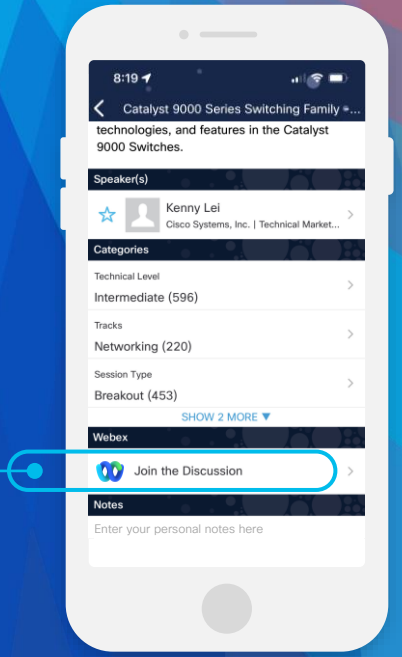
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.

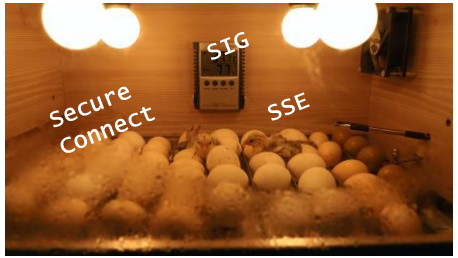


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-3022

Fernando? Never heard about!

Technical Solutions Architect – SSE
feferrar@cisco.com

Part of SSE Incubation team



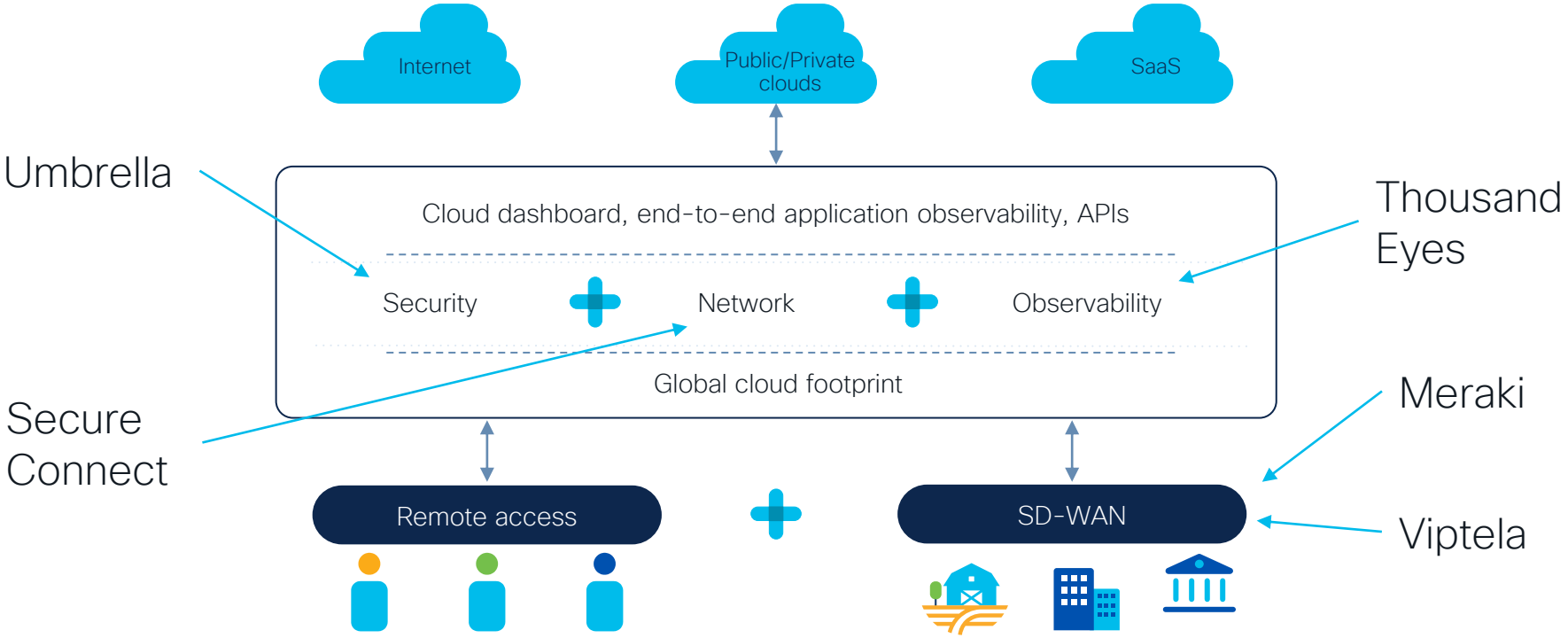
LinkedIn

Agenda

- What is Cisco SASE Platform?
- Cloud side IPSec implementation
  - Secure internet gateway vs private access tunnels
  - Datacenter failover and tunnel high availability
- Automations
  - Tunnel API
  - ASA
  - Firepower
  - Viptela
  - Meraki

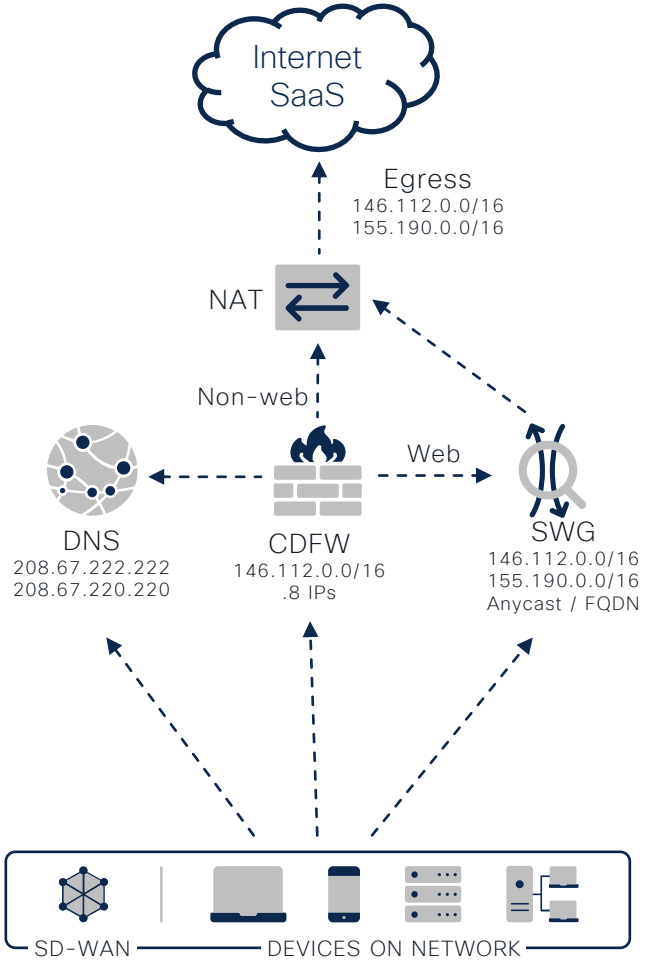
What is Cisco SASE Platform?

Cisco SASE Architecture

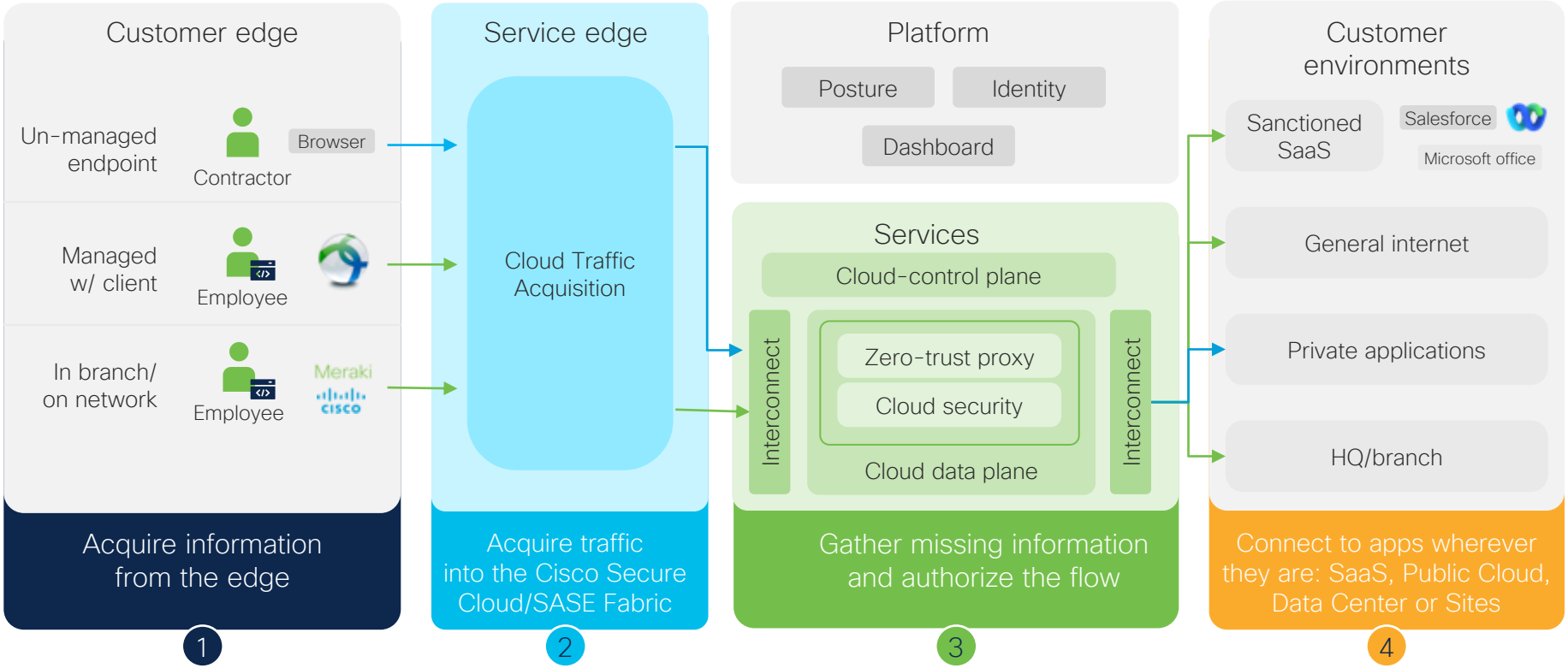


Umbrella Architecture

- DNS
  - Block/allow or Intelligent proxy
  - Very efficient for threat protection
- CDFW
  - L3/L4/L7 and IDS/IPS (Snort)
- SWG
  - Full proxy, decryption, DLP, RBI, file control and analysis, sandboxing, tenant control ……



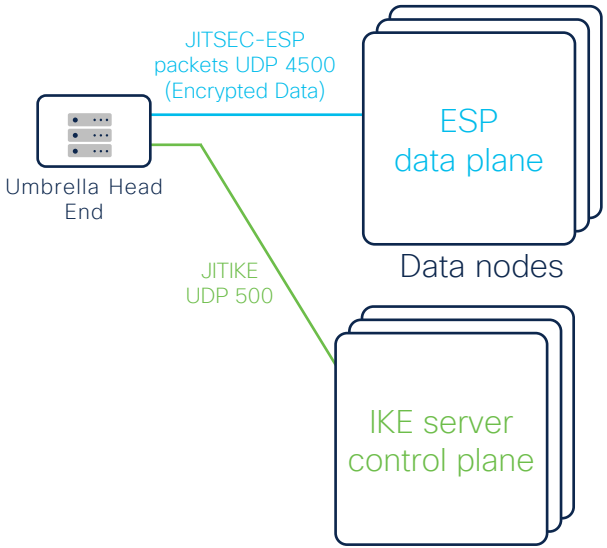
Secure Connect Architecture



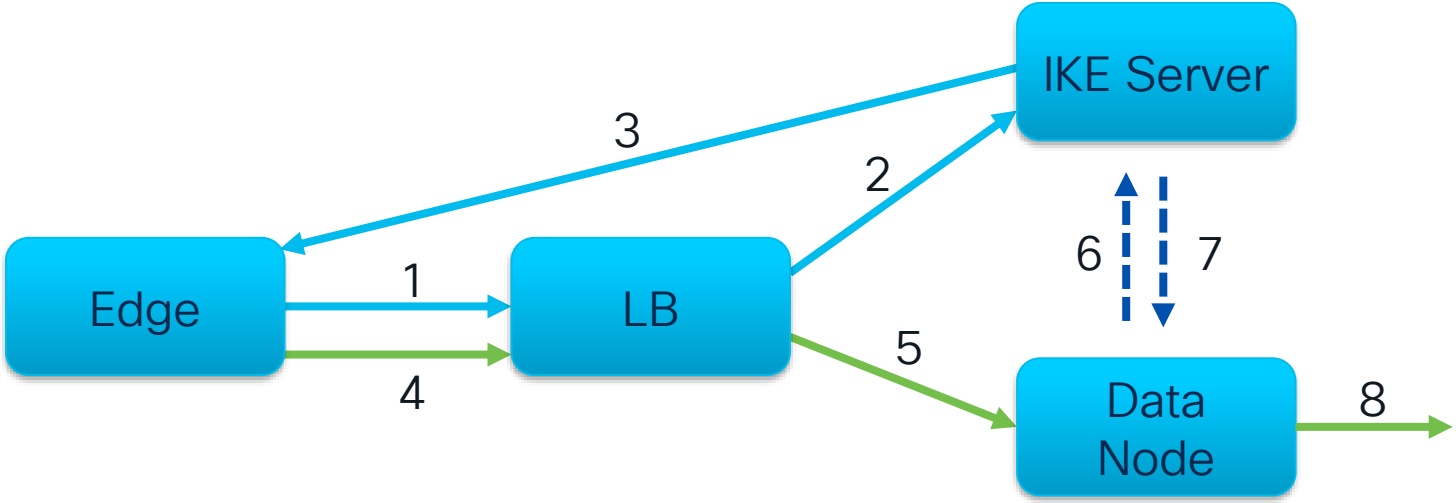
Cloud Side IPSec Implementation

Just-in-Time IKE and IPSec

- Just in time IKE / SEC – seamless same DC failover
- Tunnel should always be initiated from customer side
- 250Mbps per tunnel – ECMP for higher throughput



Just-in-Time IKE and IPSec



IKE

ESP over UDP (NAT-T)

Multiple Tunnels NATing

IKEv2 RFC-5996

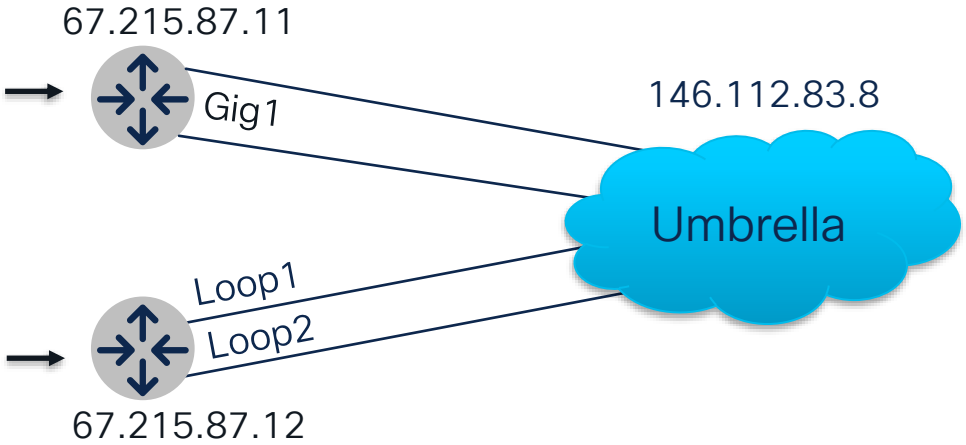
> Port 4500 is reserved for UDP-encapsulated ESP and IKE. An IPsec endpoint that discovers a NAT between it and its correspondent (as described below) MUST send all subsequent traffic from port 4500, which NATs should not treat specially (as they might with port 500).

> It is a common practice of NATs to translate TCP and UDP port numbers as well as addresses and use the port numbers of inbound packets to decide which internal node should get a given packet. For this reason, even though IKE packets MUST be sent to and from UDP port 500 or 4500, they MUST be accepted coming from any port and responses MUST be sent to the port from whence they came. This is because the ports may be modified as the packets pass through NATs. Similarly, IP addresses of the IKE endpoints are generally not included in the IKE payloads because the payloads are cryptographically protected and could not be transparently modified by NATs.

T1: 67.215.87.11:**4500** <-> 146.112.83.8:**4500**
T2: 67.215.87.11:**4500** <-> 146.112.83.8:**4500**

NAT loopback subnet to Gig1 overload (PAT)

T1: 67.215.87.12:**1111** <-> 146.112.83.8:**4500**
T2: 67.215.87.12:**2222** <-> 146.112.83.8:**4500**



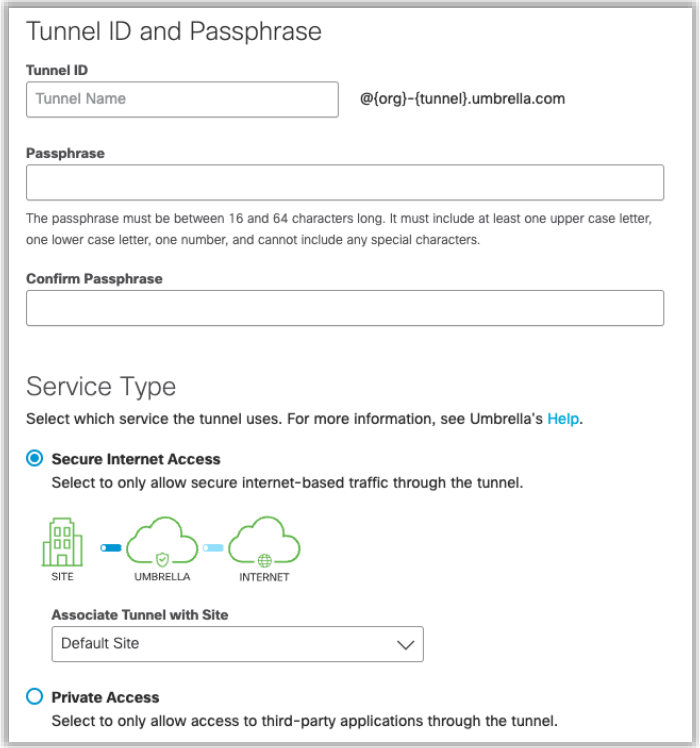
Ciphers

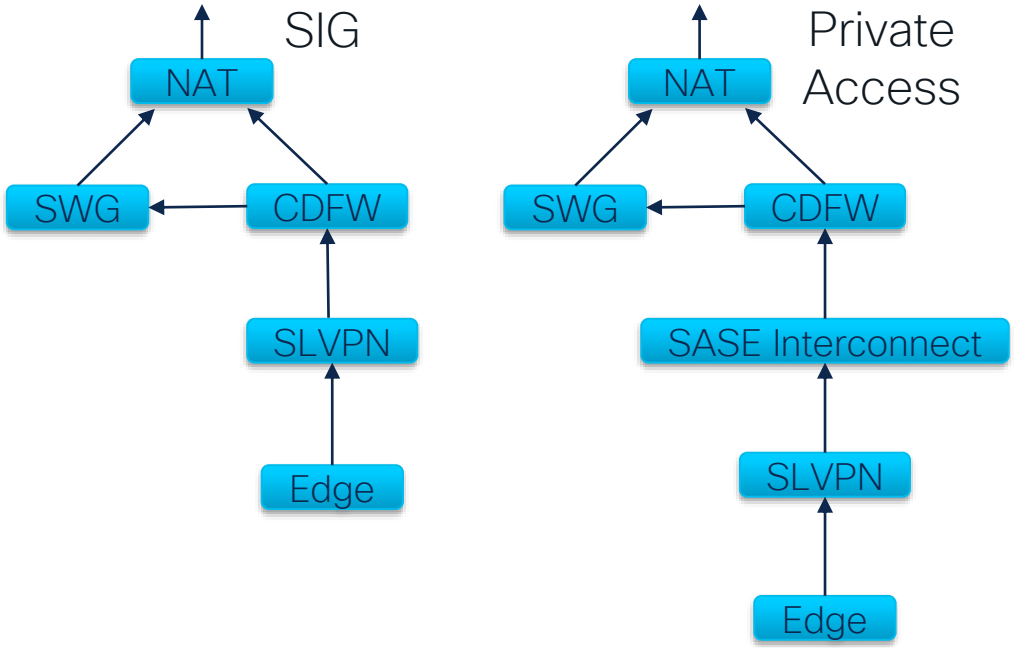
Always prefer GCM over CBC

Components	IKEv2	ESP
Encryption	AES-256 (GCM)	AES-256 (GCM)
Hashing	SHA256	SHA1
Diffie-Hellman (DH) Group	19, 20	N/A
Authentication	Pre-Shared Key (PSK)	N/A
Perfect Forward Secrecy	N/A	Disabled
IKE Fragmentation	Enabled	N/A

https://docs.umbrella.com/umbrella-user-guide/docs/supported-ipsec-parameters

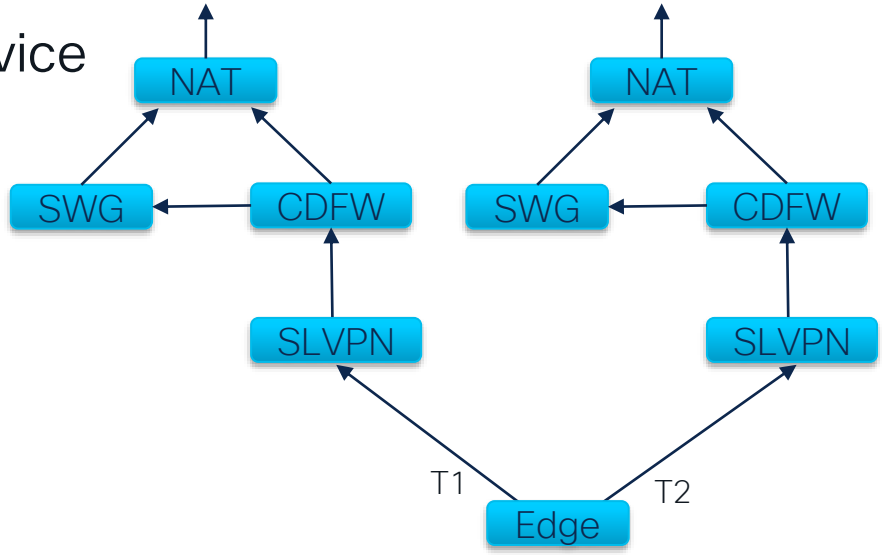
Secure Internet Access vs Private Access





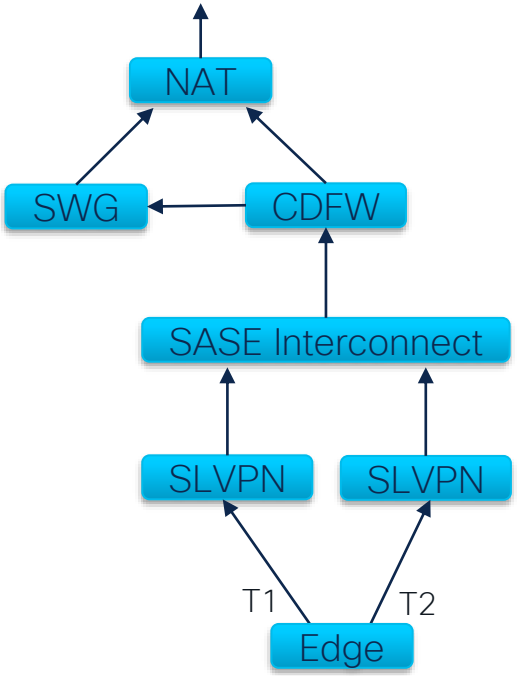
Secure Internet Access – Service Chain

- Internet traffic only
- Each tunnel is part of a unique service chain
- Overlapping IPs supported
- ECMP to the same DC only
- Path selection should be based on source and destination IP/port



Private Access Tunnel – Service Chain

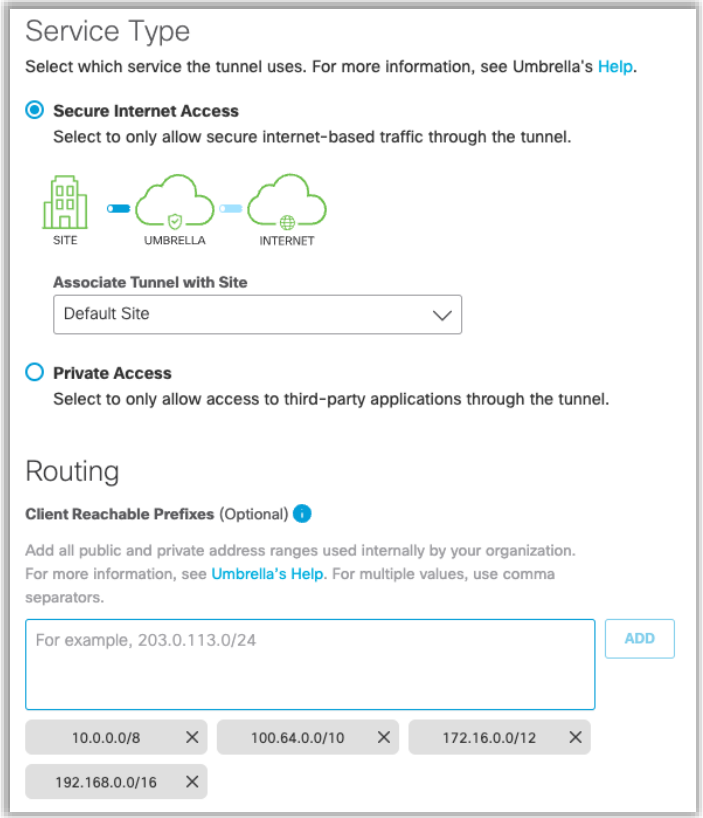
- Private access and internet traffic
- Overlapping IPs only to the same DC for higher throughput (ECMP)
- Up to 10 ECMP tunnels (cloud side limit)
- For firewall add all tunnels to the same security zone



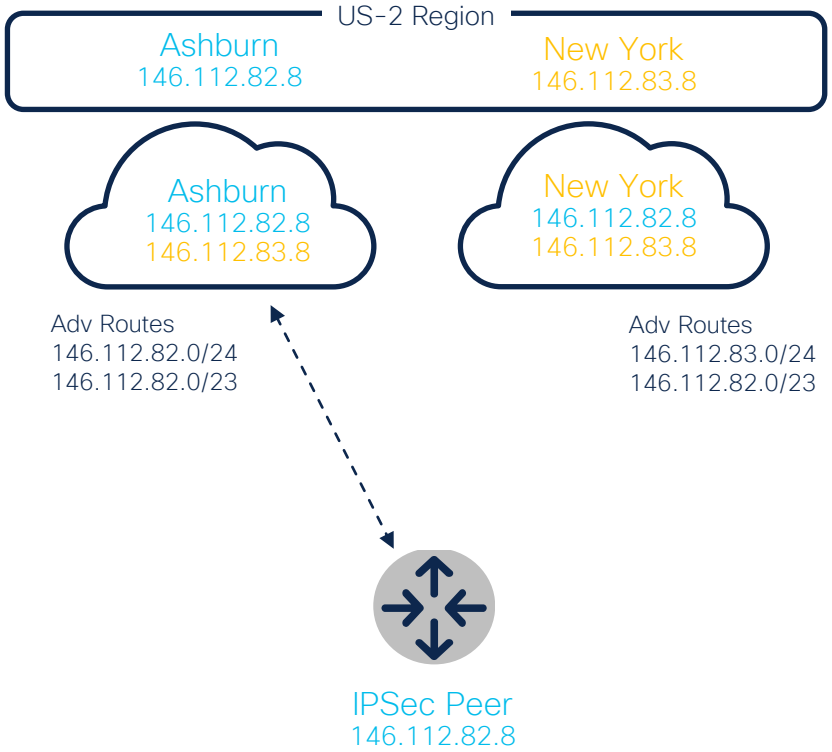
Default Routing Settings

- SIG Tunnels:
  - RFC 1918 (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16) and CGNAT (100.64.0.0/10) added by default

- Private Access Tunnels:
  - No default subnets added
  - Should be specific



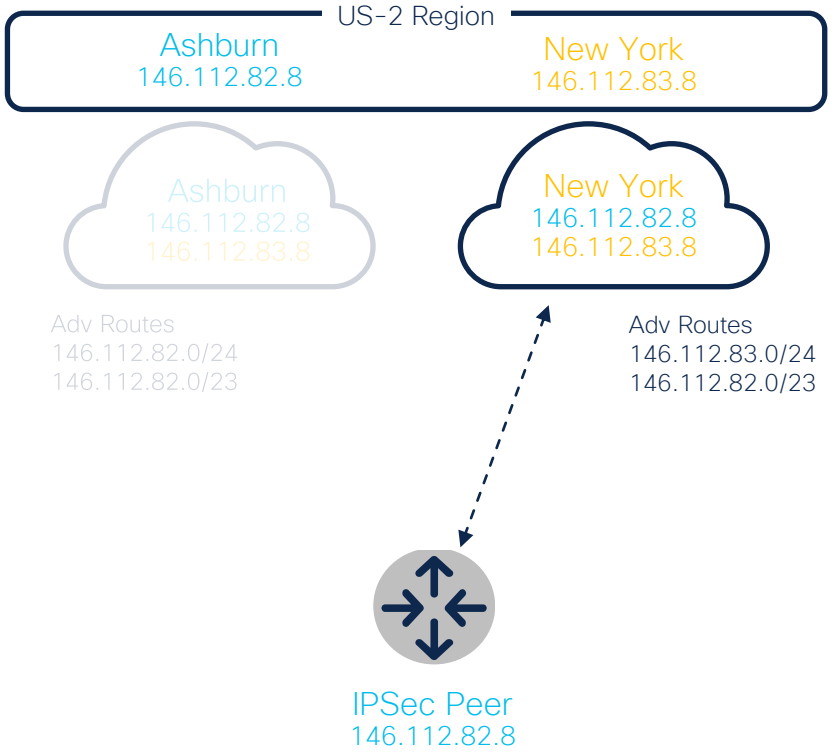
Cloud Side Tunnel Failover



Routing table

146.112.82.0/24 -> ASH
146.112.83.0/24 -> NYC
146.112.82.0/23 -> ASH or NYC

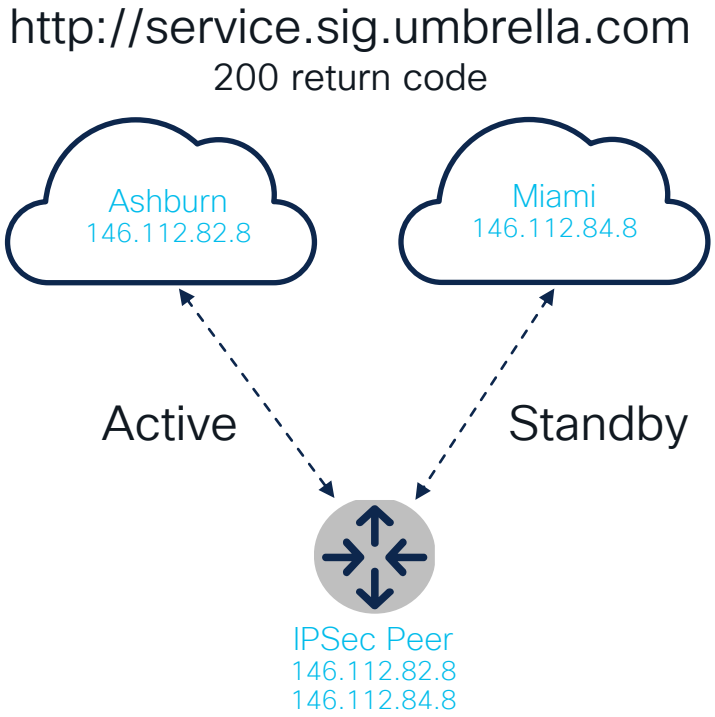
Cloud Side Tunnel Failover

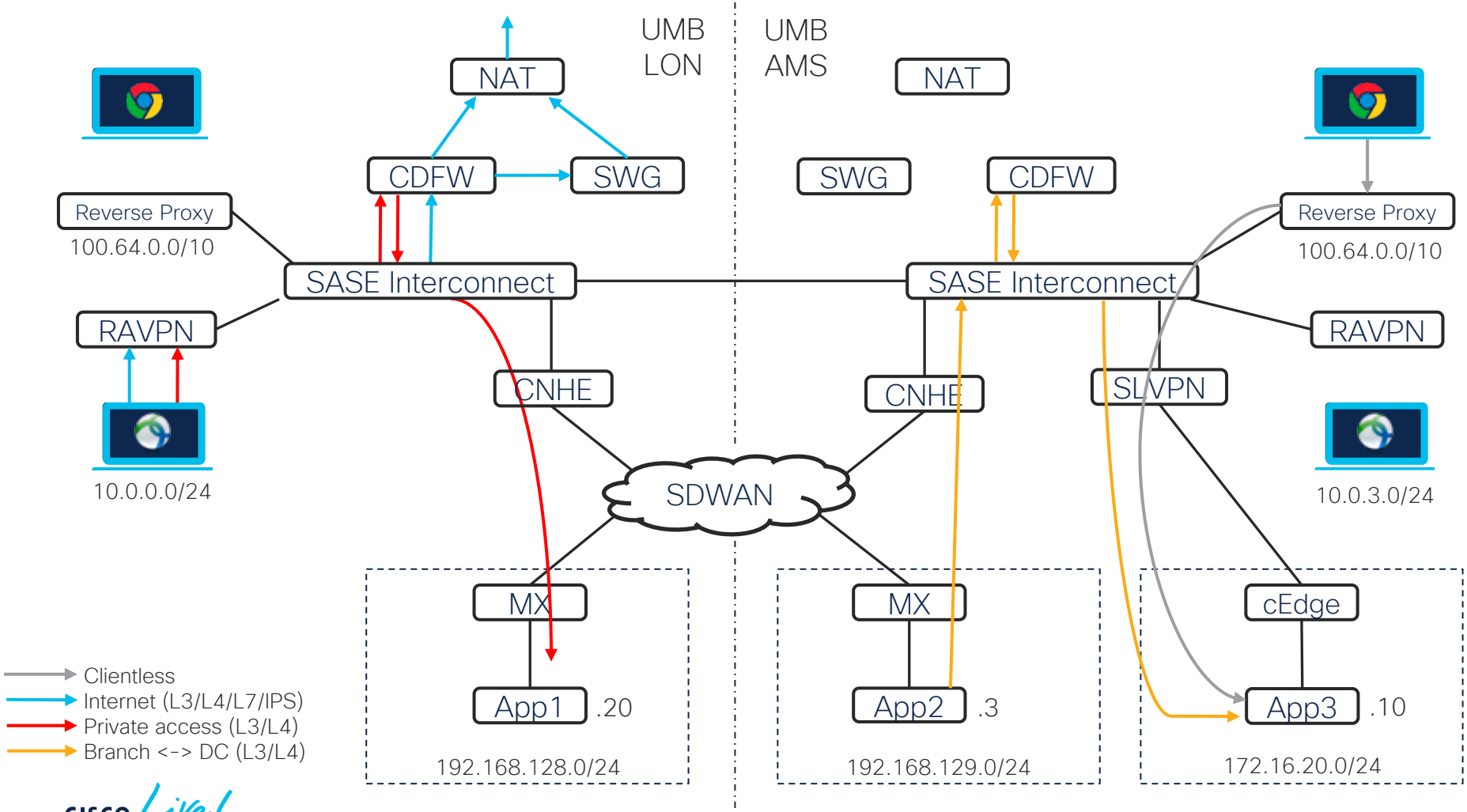


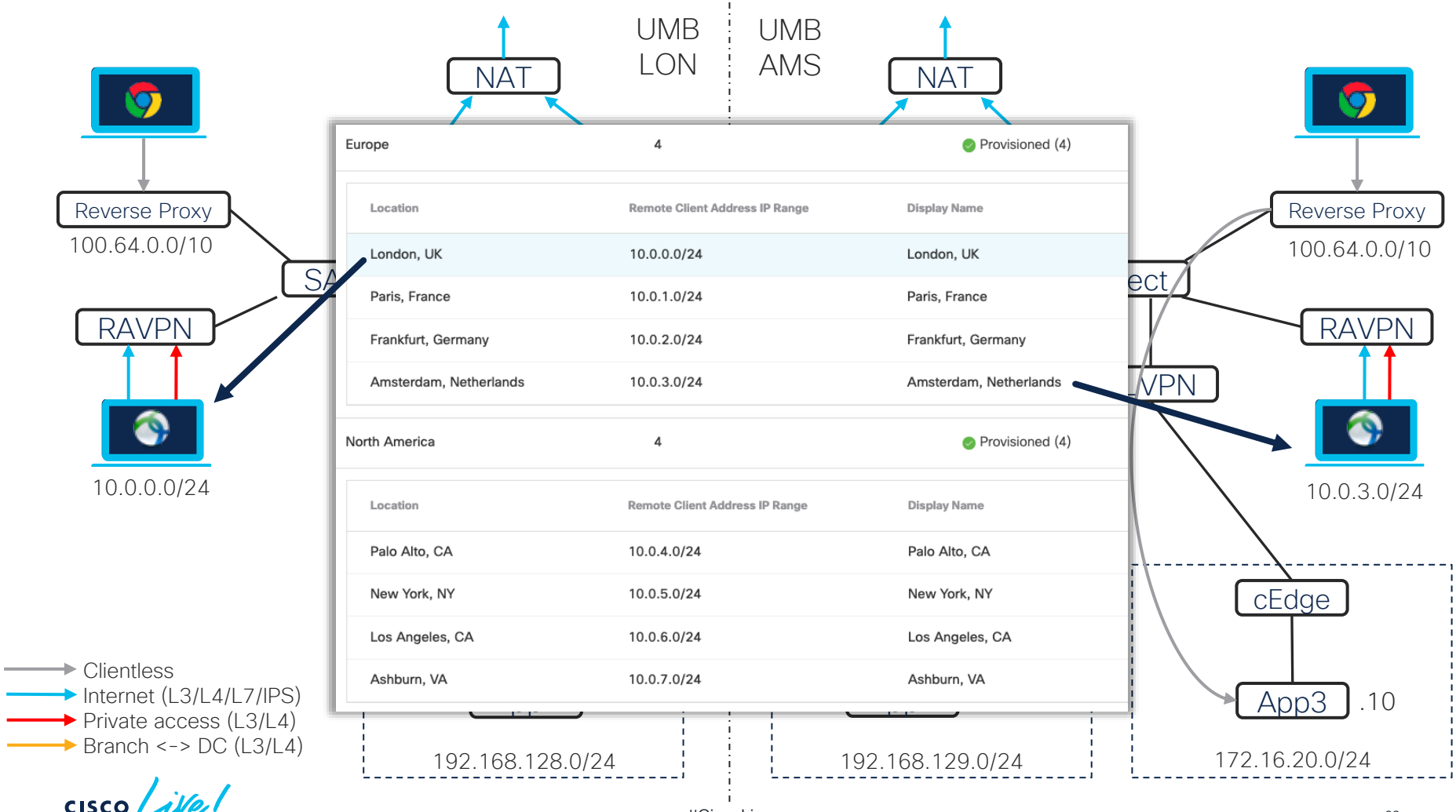
Routing table

146.112.82.0/24 -> ~~ASH~~
146.112.83.0/24 -> NYC
146.112.82.0/23 -> ~~ASH~~ or NYC

Customer Side Tunnel Failover

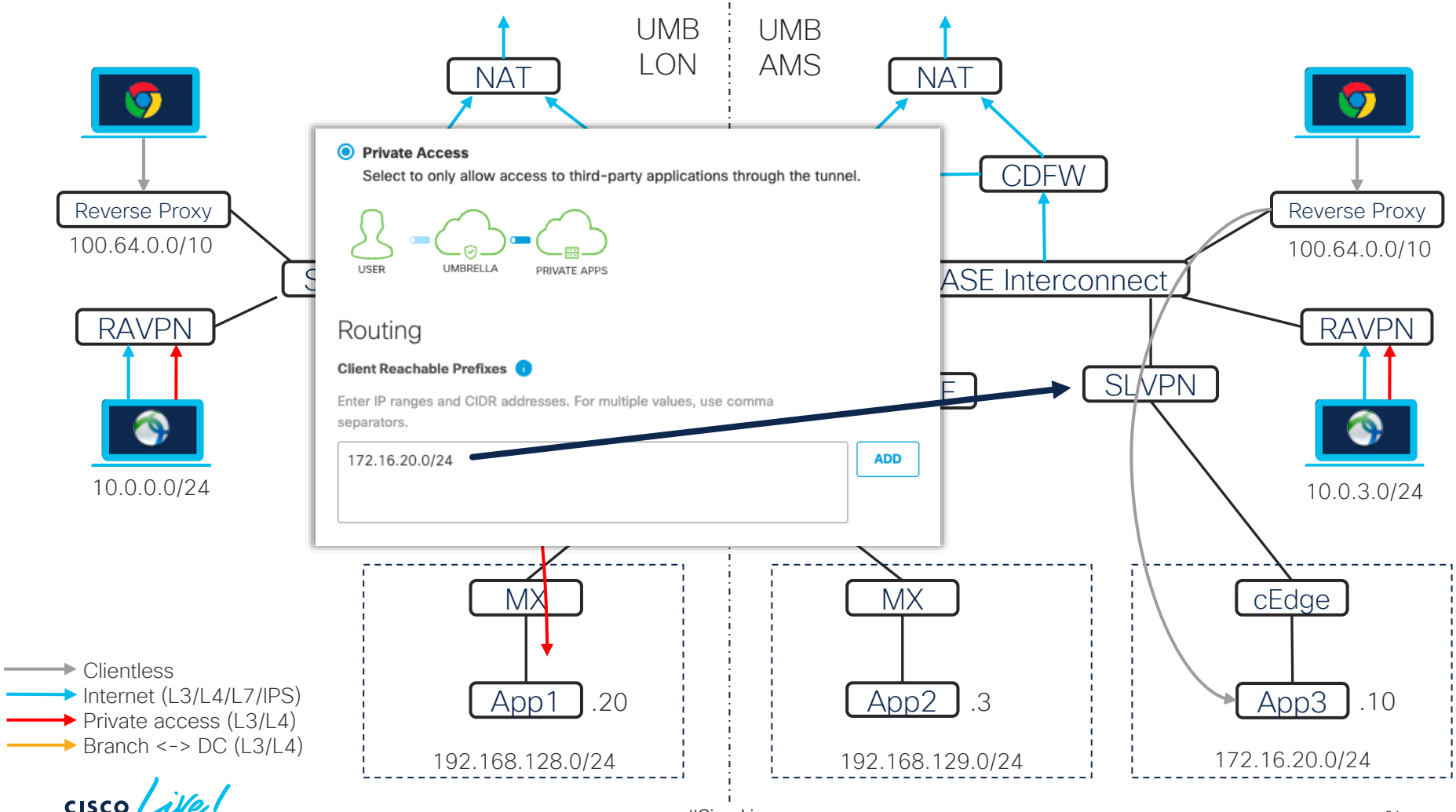






Europe	4	Provisioned (4)
Location	**Remote Client Address IP Range**	**Display Name**
London, UK	10.0.0.0/24	London, UK
Paris, France	10.0.1.0/24	Paris, France
Frankfurt, Germany	10.0.2.0/24	Frankfurt, Germany
Amsterdam, Netherlands	10.0.3.0/24	Amsterdam, Netherlands

North America	4	Provisioned (4)
Location	**Remote Client Address IP Range**	**Display Name**
Palo Alto, CA	10.0.4.0/24	Palo Alto, CA
New York, NY	10.0.5.0/24	New York, NY
Los Angeles, CA	10.0.6.0/24	Los Angeles, CA
Ashburn, VA	10.0.7.0/24	Ashburn, VA



Automations

What we trying to avoid with automations

Add A New Tunnel

Tunnel Name

LAB-FTD

Device Type

FTD

Tunnel ID and Passphrase

Tunnel ID Format

Email IP Address

Tunnel ID

lab-ftd-01 @{org

Passphrase

The passphrase must be between 16 and 64 characters lor
letter, one lower case letter, one number, and cannot includ

Confirm Passphrase

Passphrases match

Tunnel ID and Passphrase Confirmed

Copy your Tunnel ID and Passphrase to your device.

Tunnel ID: lab-ftd-01@7955832-604851841-umbrella.com

Passphrase: Cisco12345Cisco12345

DONE

Service Type

Select which service the tunnel uses. For more information, see Umbrella's Help.

Secure Internet Access

Select to only allow secure internet-based traffic through the tunnel.

INTERNET

s to third-party applications through the tunnel.

ss ranges used internally by your organization.
ella's Help. For multiple values, use comma

ADD

What we trying to avoid with automations

```
!
vrf definition INET
!
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1
 description *** INSIDE ***
 ip address 172.16.20.1 255.255.255.0
!
interface GigabitEthernet2
 description *** OUTSIDE ***
 vrf forwarding INET
 ip address XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX
!
ip route vrf INET 0.0.0.0 0.0.0.0 XXX.XXX.XXX.XXX
!
```

```
!
ip access-list extended TRAFFIC_TO_UMB
 permit ip 172.16.10.0 0.0.0.255 any
 permit ip 172.16.20.0 0.0.0.255 any
!
route-map ROUTE_TO_UMB permit 10
 match ip address TRAFFIC_TO_UMB
 set interface Tunnel1
!
interface GigabitEthernet1
 ip policy route-map ROUTE_TO_UMB
!
```

```
!
crypto ikev2 proposal default
 encryption aes-cbc-256
 integrity sha1
 group 14
!
crypto ikev2 profile UMB_IKE_PROFILE_T1
 match fvrf INET
 match identity remote address 146.112.0.0 255.255.0.0
 identity local email lab-ftd-01@7955832-604851841-umbrella.com
 authentication remote pre-share key Cisco12345Cisco12345
 authentication local pre-share key Cisco12345Cisco12345
 dpd 10 2 periodic
!
crypto ikev2 nat keepalive 20
crypto ikev2 fragmentation mtu 1300
!
crypto ipsec transform-set UMB_IPSEC_TRANSFORM_SET esp-gcm 256
 mode tunnel
!
crypto ipsec profile UMB_IPSEC_PROFILE_T1
 set transform-set UMB_IPSEC_TRANSFORM_SET
 set ikev2-profile UMB_IKE_PROFILE_T1
!
interface Tunnel1
 ip unnumbered GigabitEthernet2
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 146.112.97.8
 tunnel vrf INET
 tunnel protection ipsec profile UMB_IPSEC_PROFILE_T1
!
```

Umbrella Open APIs

Before	After
API keys are predefined in terms of what they can access	Tailored access controls for API Keys
A different authentication method is needed depending on the API being used	Unified Authentication: one method of authentication for Management, Network Devices and Reporting APIs
An org can only have 1 API key per type	Create multiple API keys and-Give them meaningful names
API keys are static	You can set expiration dates for your API Keys

Legacy API

Full access to the scope

API Keys
2

KeyAdmin Keys
0

Static Keys
3

Legacy Keys
4

Umbrella Network Devices — Keys 1

Legacy Network Devices — Keys 1

Umbrella Reporting — Keys 1

Umbrella Management — Keys 1

The API Key and secret pair enable you to manage the deployment for your different organizations. This includes the management of networks, roaming clients and other core-identity types.

Check out the documentation for step by step instructions.

Key	Created		
e7a9c9ca8ade4e75a8d14c82235c68c7	April 17, 2023	REFRESH	DELETE

Open API

What can access

For how long can access

Add Tunnel

Created By
feferrar@cisco.com

Last Modified
Apr 17, 2023

Last Used
Apr 17, 2023

Key Expiration
Never expires

API Key Name

Add Tunnel

Created on: Apr 17, 2023

Key Scope
Select the appropriate access scopes to define what this API key can do.

- [ ] Admin 3 >
- [ ] Auth 1 >
- [-] Deployments 11 >
- [ ] Policies 4 >
- [ ] Reports 5 >

1 selected REMOVE ALL

Scope	
Deployments / Tunnels	Read / Write

Expiry Date

- (•) Never expire
- ( ) Expire on: Jul 15 2023

Copy the API key and secret and use them to authenticate API requests. This secret is only displayed once. Click Refresh to generate a new key and secret.
For more information, see Umbrella's Help.

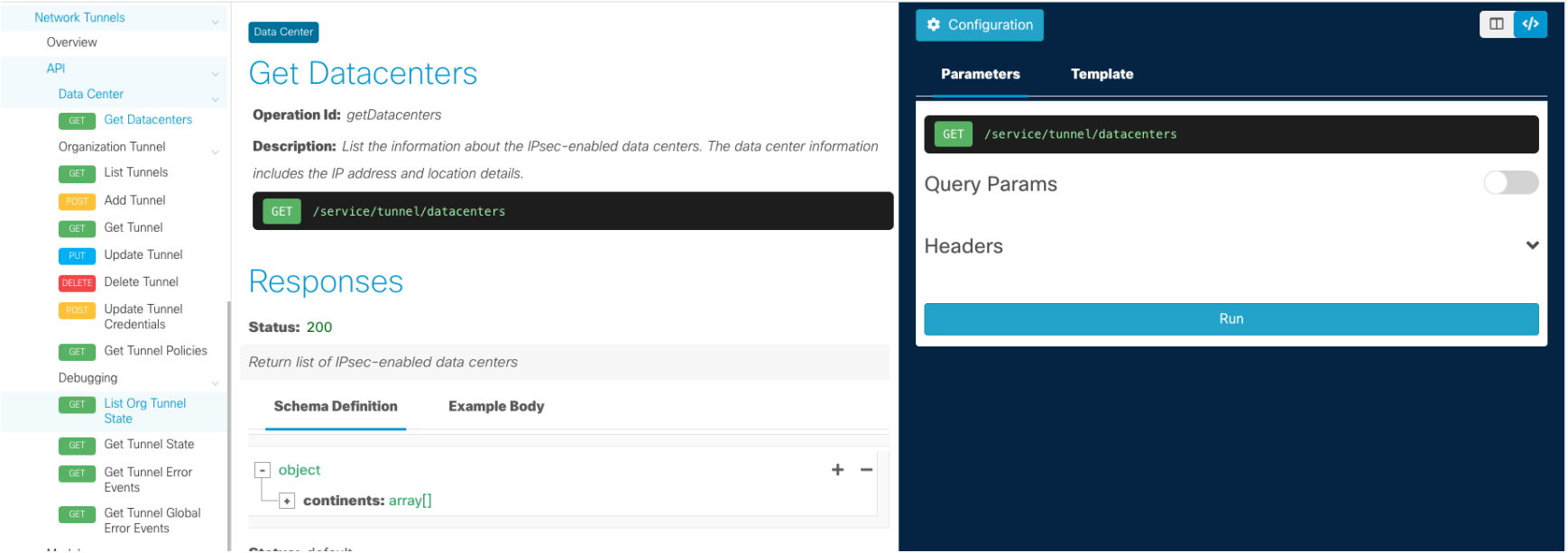
API Key
b7d969b86f9942e6b1e1e88708ecf076

Key Secret
######

REFRESH KEY

Access level

API Documentation



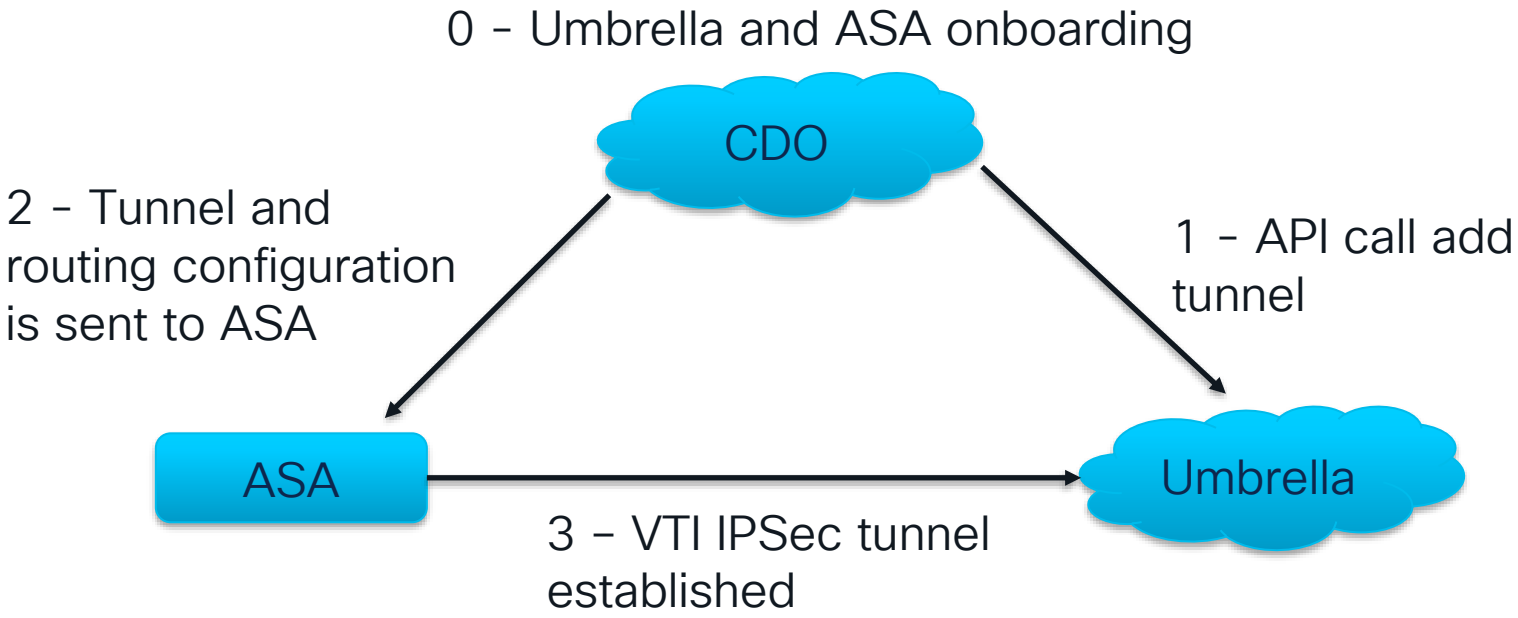
https://developer.cisco.com/docs/cloud-security/

API DEMO

ASA

- Cisco ASA automation is achieved via Cisco Defense Orchestrator
- Both Umbrella and ASA should be onboarded to CDO
- CDO uses Umbrella new API model
- During tunnel configuration CDO will do an API call to Umbrella and create the tunnel
- Running configuration is sent to ASA in the end of the SASE tunnel configuration wizard

ASA Automation Flow

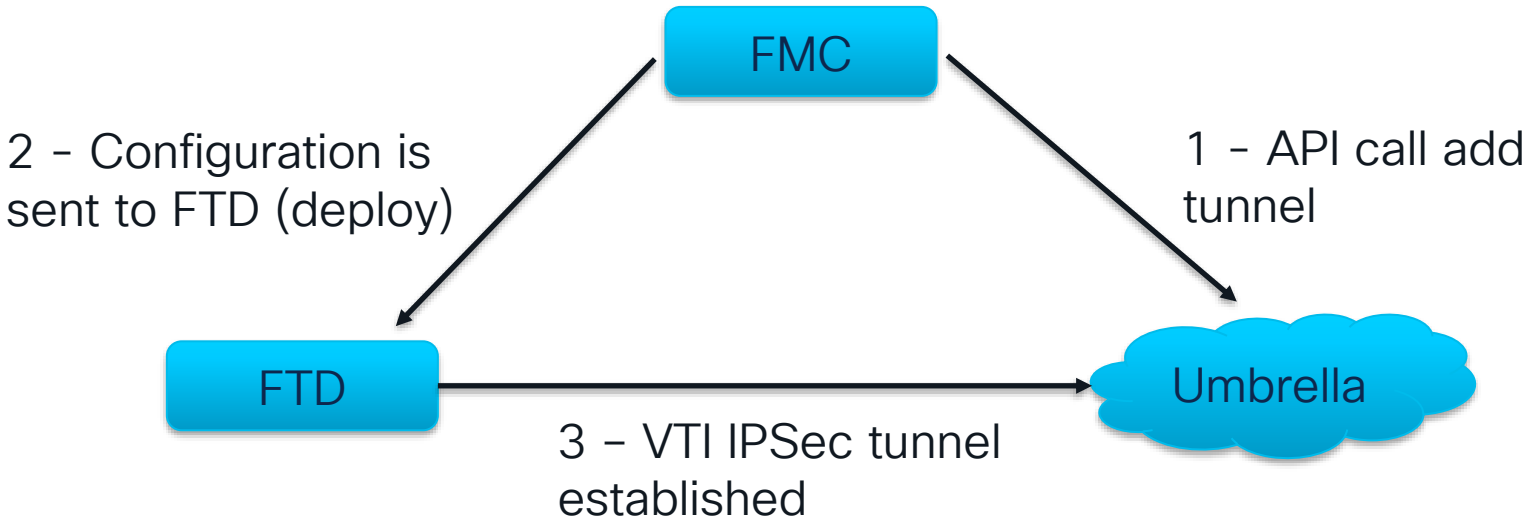


ASA DEMO

Firepower

- Legacy API key
- Firewall Management Center does the API call to Umbrella and create the tunnel
- Multiple tunnels on multiple devices can be added in a single configuration flow
- Configuration is then deployed to the edge firewalls

Firepower Automation Flow

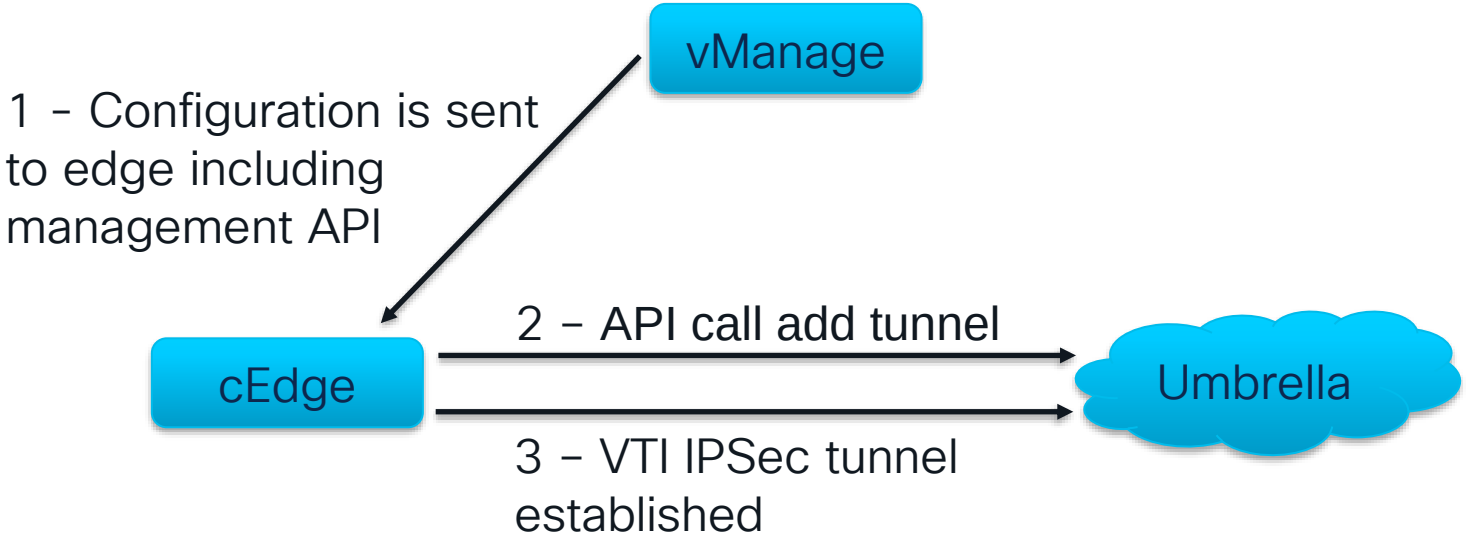


FIREPOWER DEMO

Viptela

- Legacy API key
- Two feature templates required, SIG Credentials and SIG Tunnels
- Management API key is sent to the edge device and the edge device is the one doing to API call to Umbrella to create the tunnel
- Layer 7 health check is part of SIG template, only need to provide source IP
- RMK: NAT should be enabled in the outside interface and edge device should be able to resolve DNS

Firepower Automation Flow

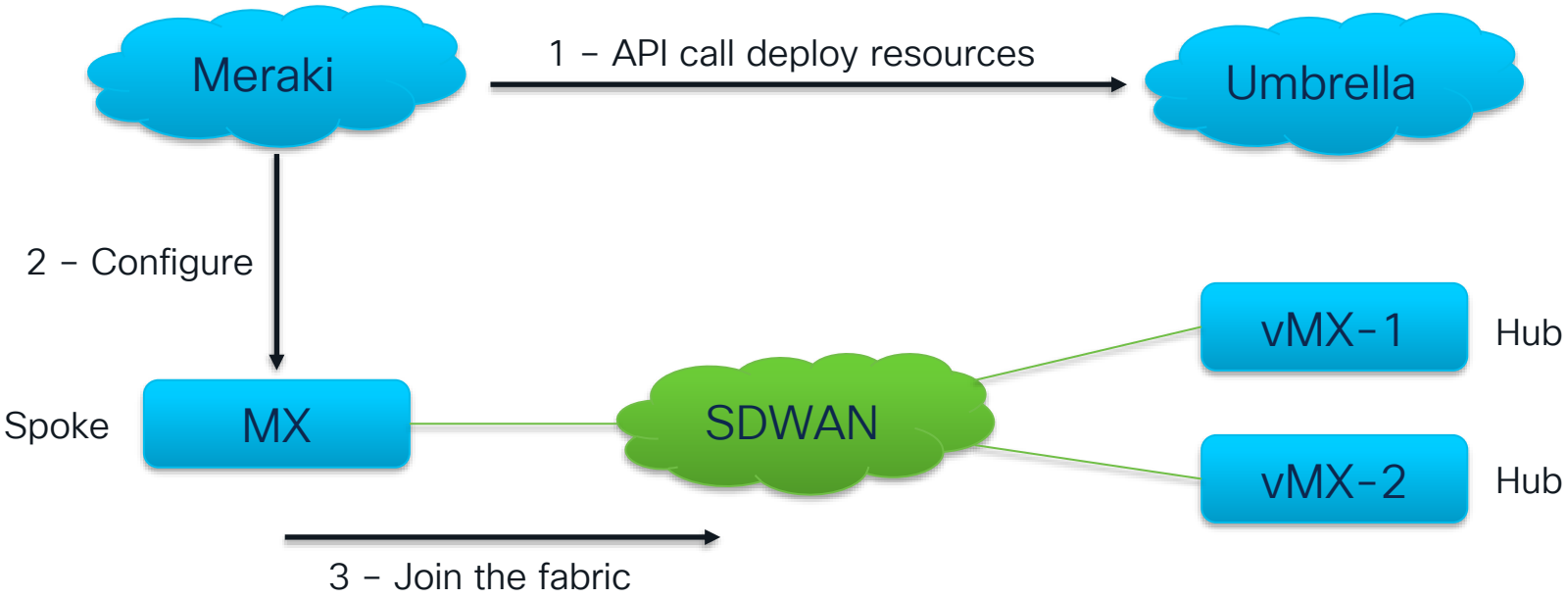


VIPTELA DEMO

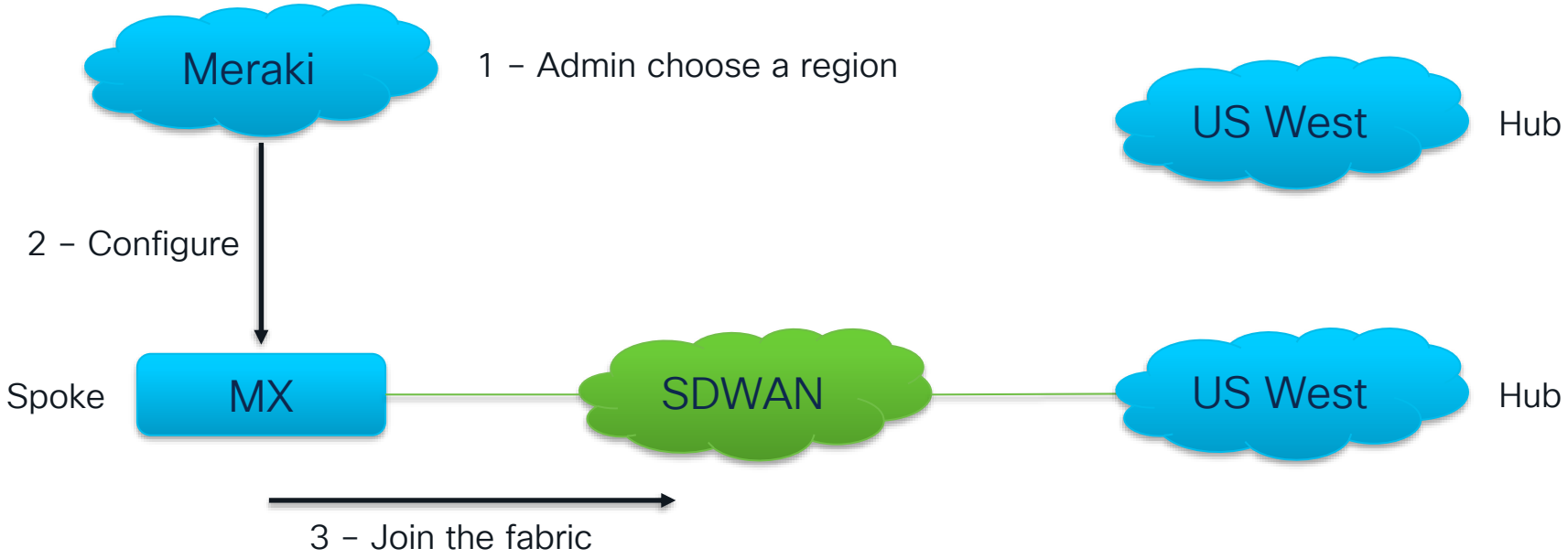
Meraki

- Legacy management API
- Umbrella/Secure Connect becomes part of the Meraki SDWAN fabric
- Management key is used to deploy the resources instead of adding IPSec tunnels

Meraki with SIG Automation Flow



Secure Connect Automation Flow



RMK: Region is a pair of datacenters

SECURE CONNECT DEMO

Key Takeaways

- If building your own automation use the new API model
- Plan before implement, routing traffic over the IPSec tunnels can have unexpected results
- Use the documentation

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

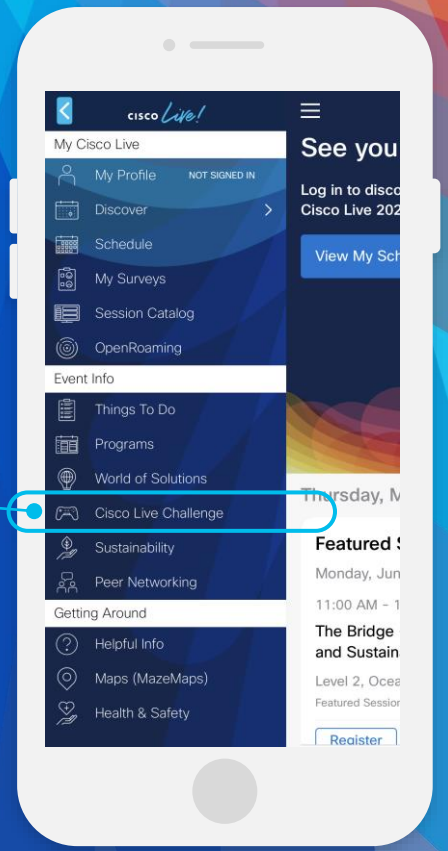
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

Let's go