The bridge to possible

Extending Your Segmentation Strategy for Your Hybrid Environment

Using Cisco SASE

Ryan Shoemaker – Technical Solutions Architect
@ersatzshoe

BRKSEC-2092

cisco Live!

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2092

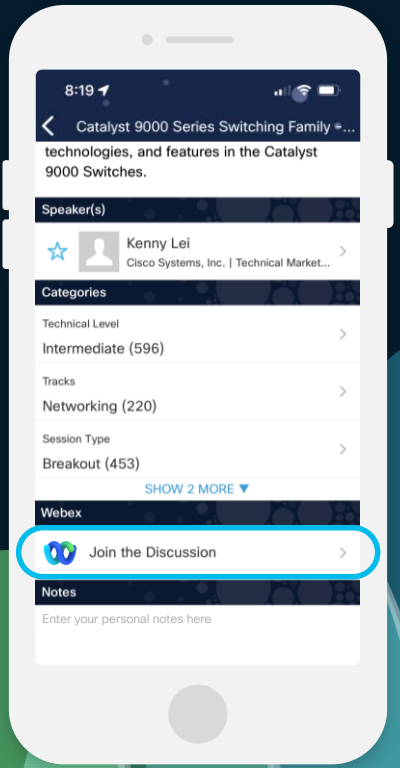
Questions?

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 7, 2024.



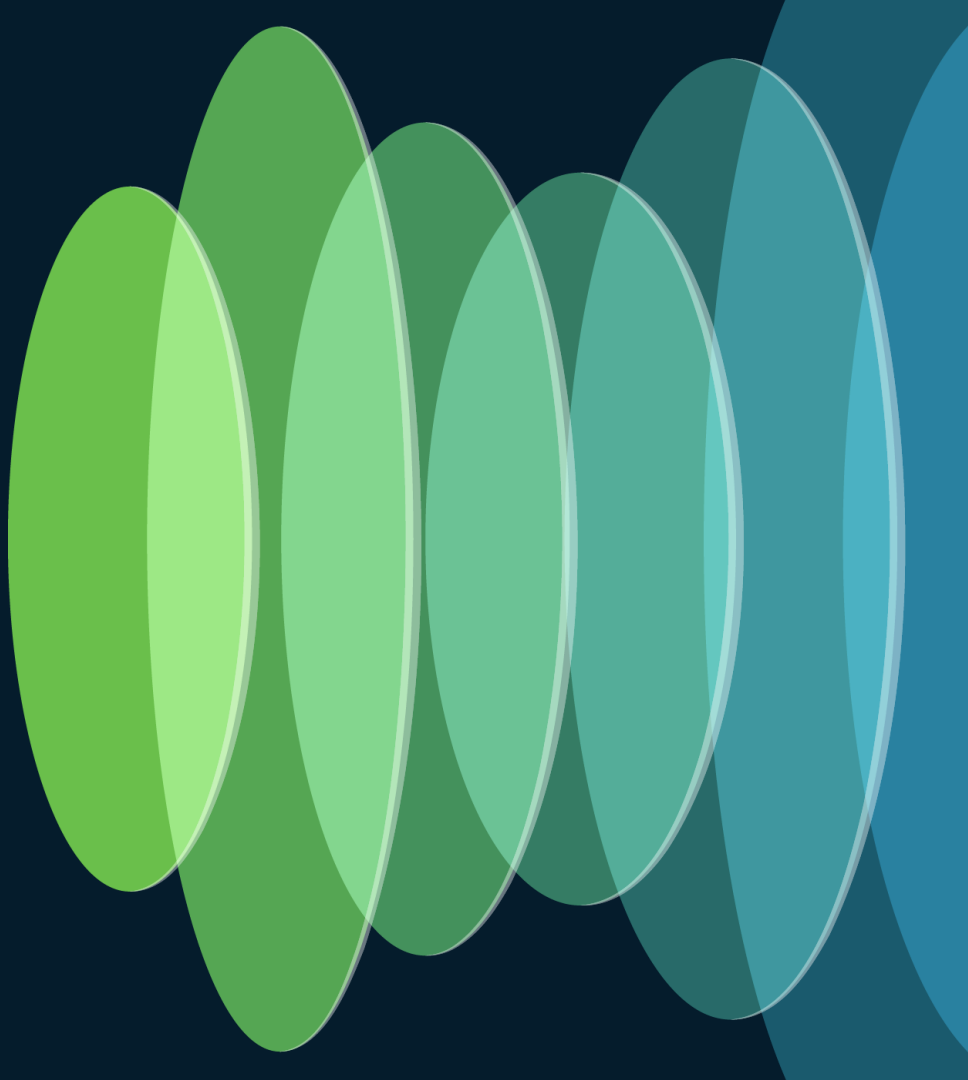
Why This Session

- Organizations have implanted network segmentation to isolate systems and services
- Permits common policies to be applied to like devices and users
- This session will cover using typical network segmentation technologies and leverage them for creating differentiated security and control for cloud-based resources
- The focus of the session is on *Catalyst SD-WAN* and *Cisco Secure Access* and attendees will leave with an understanding of how they integrate to create this differentiated security policy

Agenda

- SASE and Segmentation Overviews
- Extend Edge Segmentation for DNS
- Extend Edge Segmentation for Internet and SaaS
- Enforce Security Policies for Group Id Using SAML
- Extend Cloud Workload Segmentation in CSPs
- Conclusion

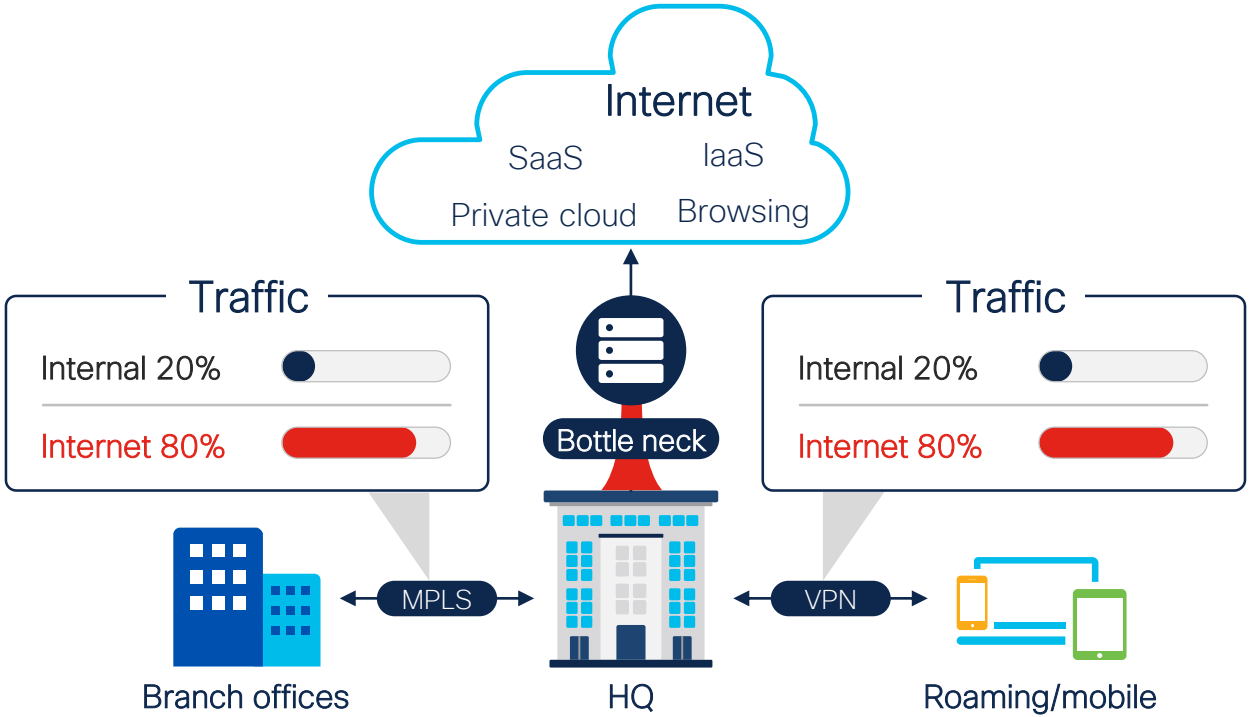
SASE Overview



Changes in the types of traffic and destinations
Have inverted the traffic model

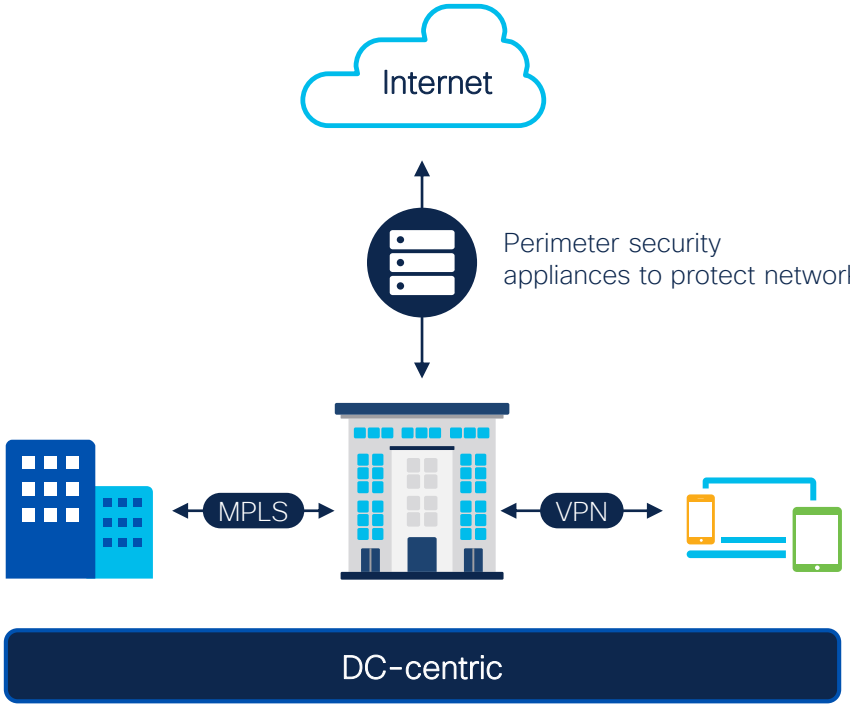
Problems

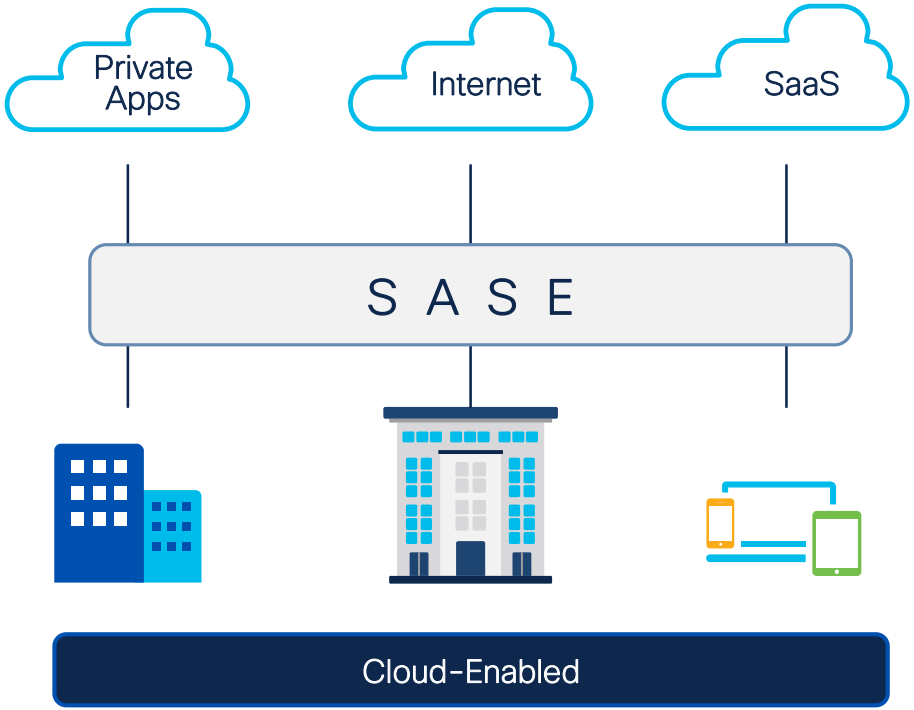
- App performance
- User experience
- Security efficacy
- # Tools/vendors
- Integrations



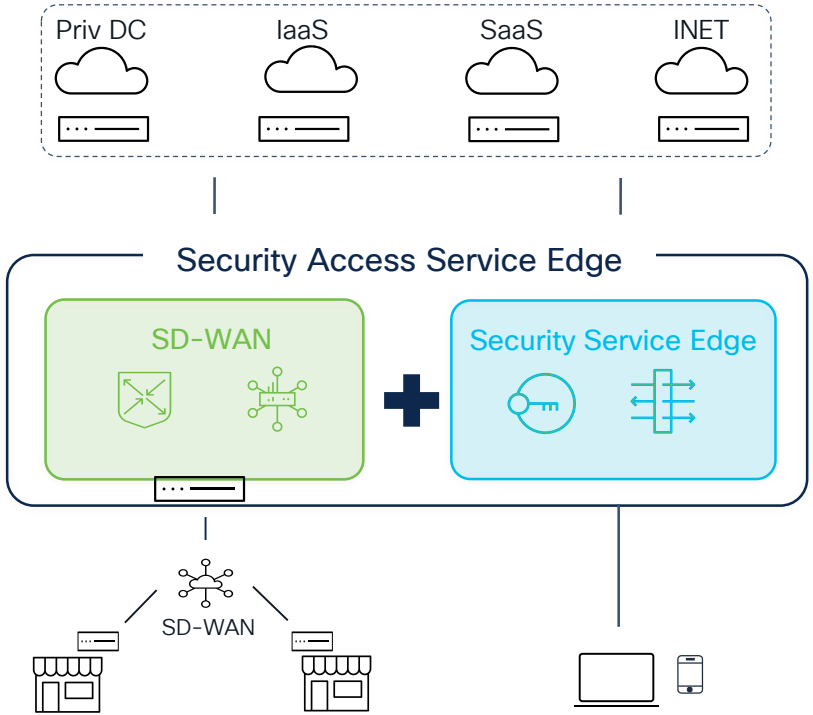
Network transformation

Transition from a DC-centric topology to one that's cloud ready

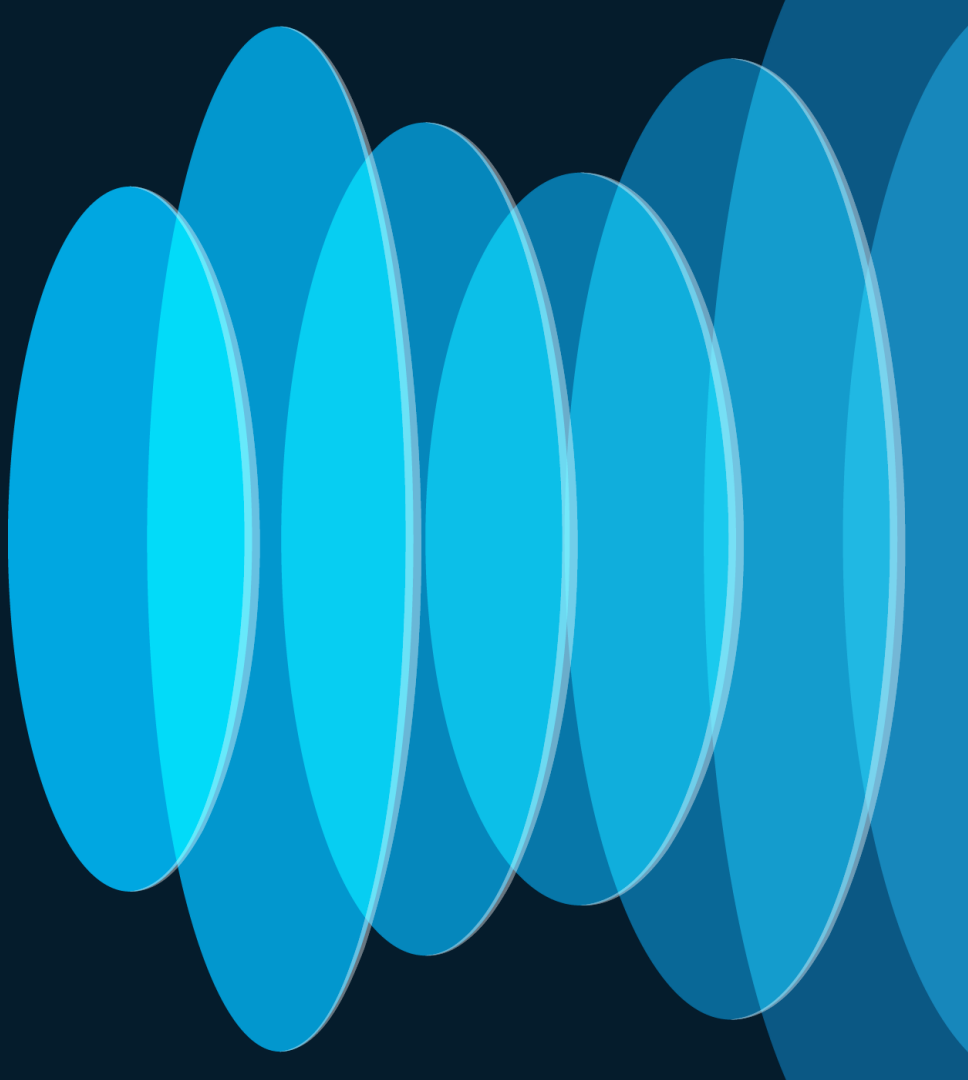




SASE – Convergence of SD-WAN and SSE



Segmentation



Some Network Segmentation Definitions

As defined by Catalyst SD-WAN

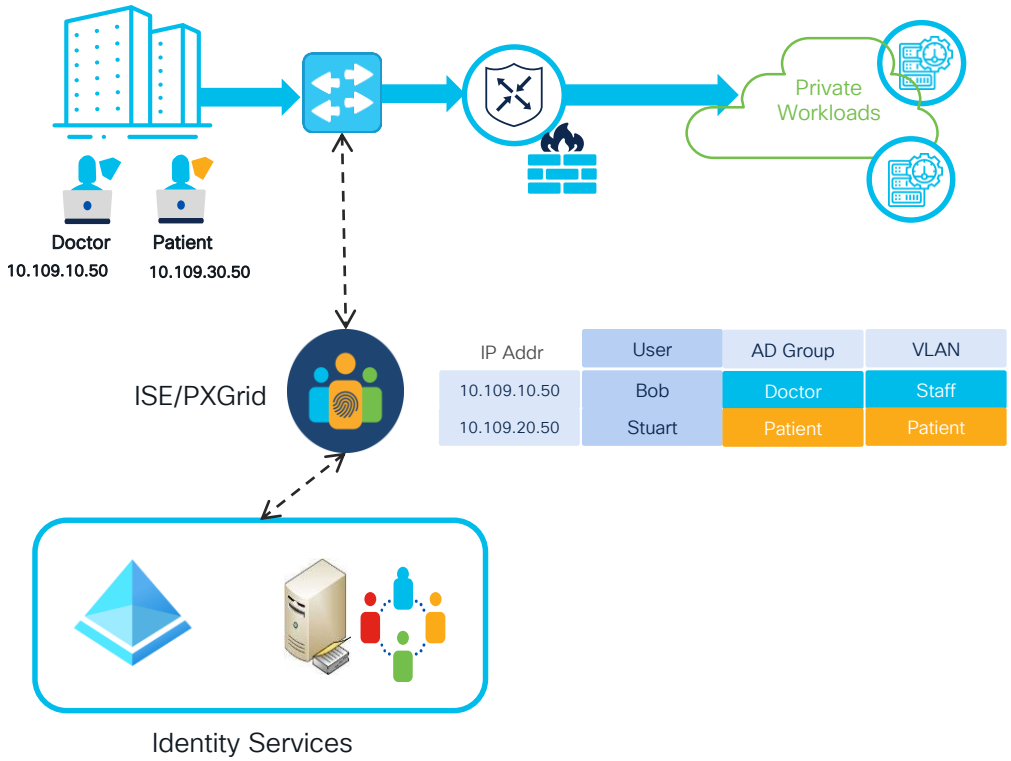
VLAN / Subnet: Separation of broadcast domains where traffic between different VLANS must traverse a router

VRF / VPN: a Separation of routing planes so that traffic in different VRFs is handled in an isolated fashion

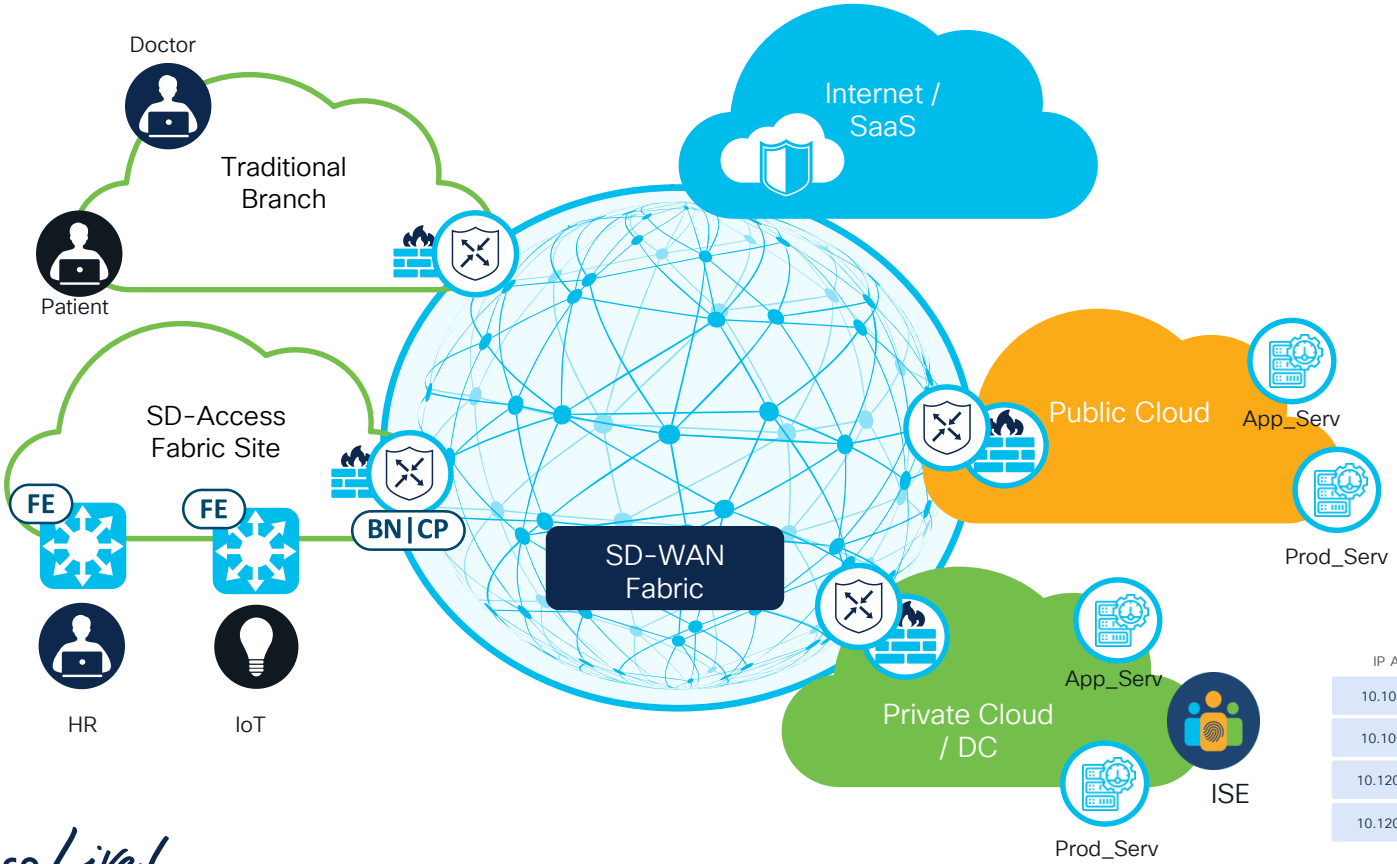
Security Group Tag (SGT): a label which identifies a group the device belongs to

User Authentication to Network Example

- Users connecting on wired or wireless infrastructure authenticate to network
- Successful auth allows ISE to register user's IP address and map it to Username, AD group, and VLAN
- Accounts for dynamic IP address changes

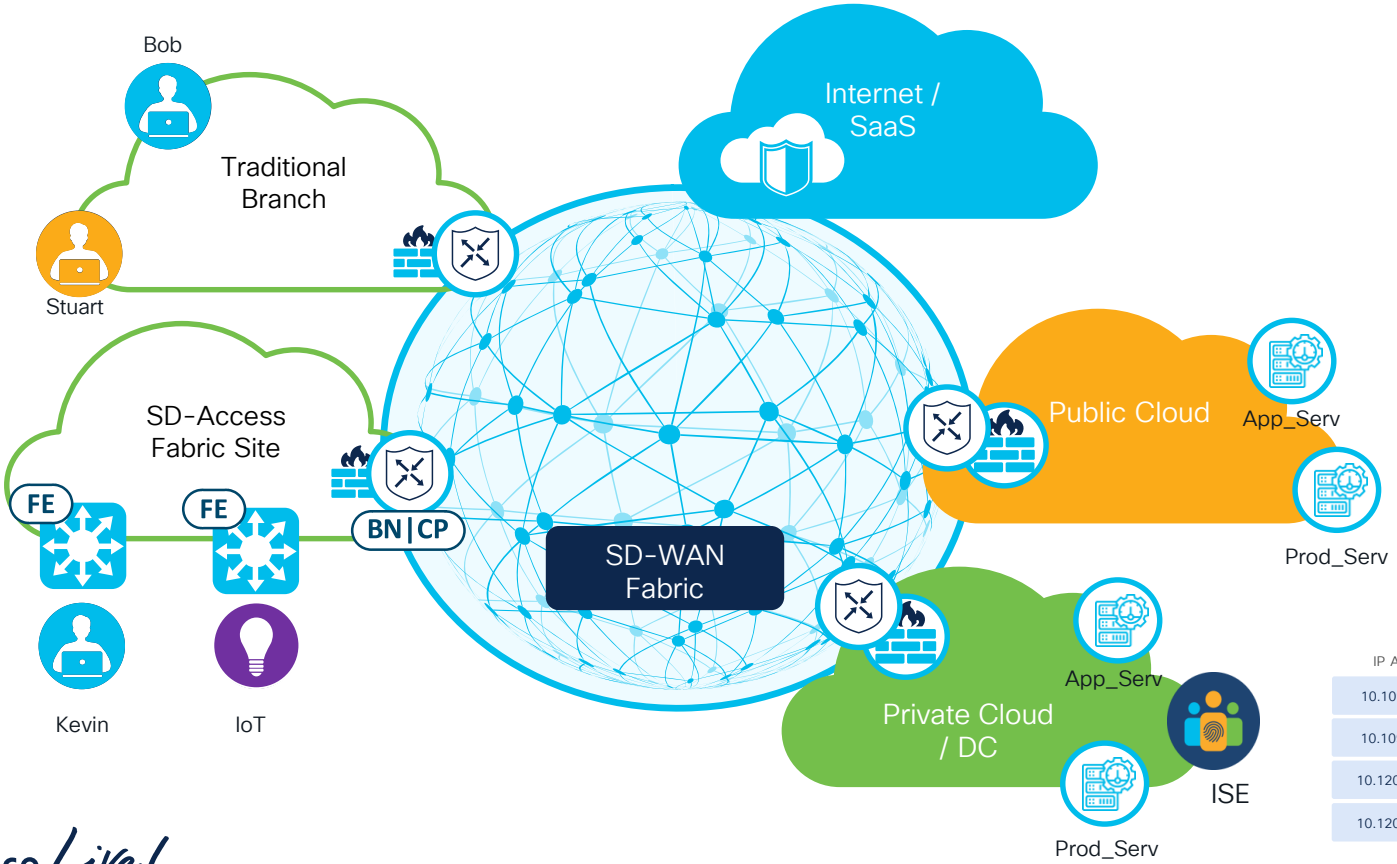


Segmenting Traffic



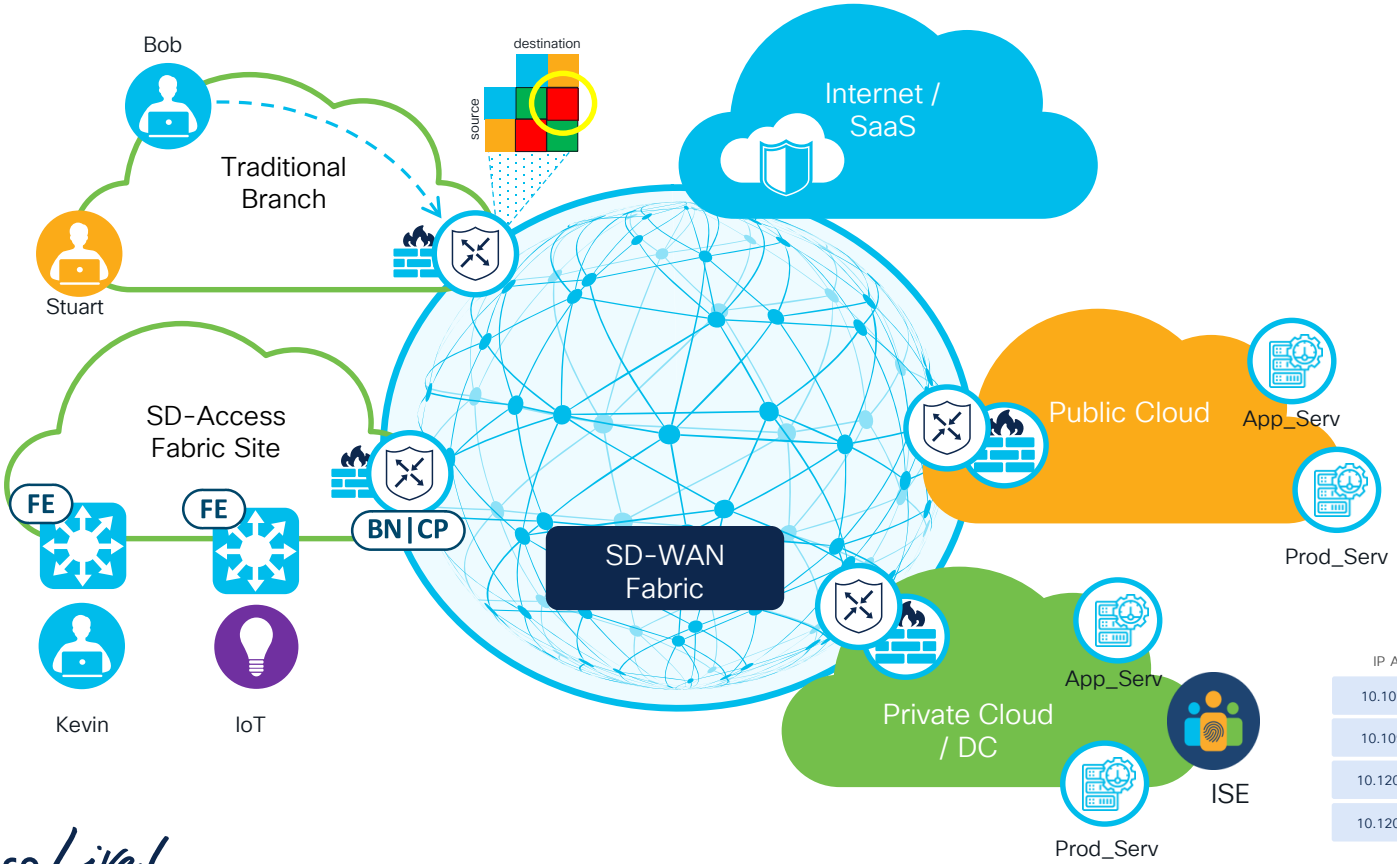
IP Addr	User/Profile	VRF/VPN
10.109.10.50	Bob	Staff
10.109.30.50	Stuart	Patient
10.120.10.101	Kevin	Staff
10.120.40.101	Light	IoT

Users / Devices Authenticate to Network



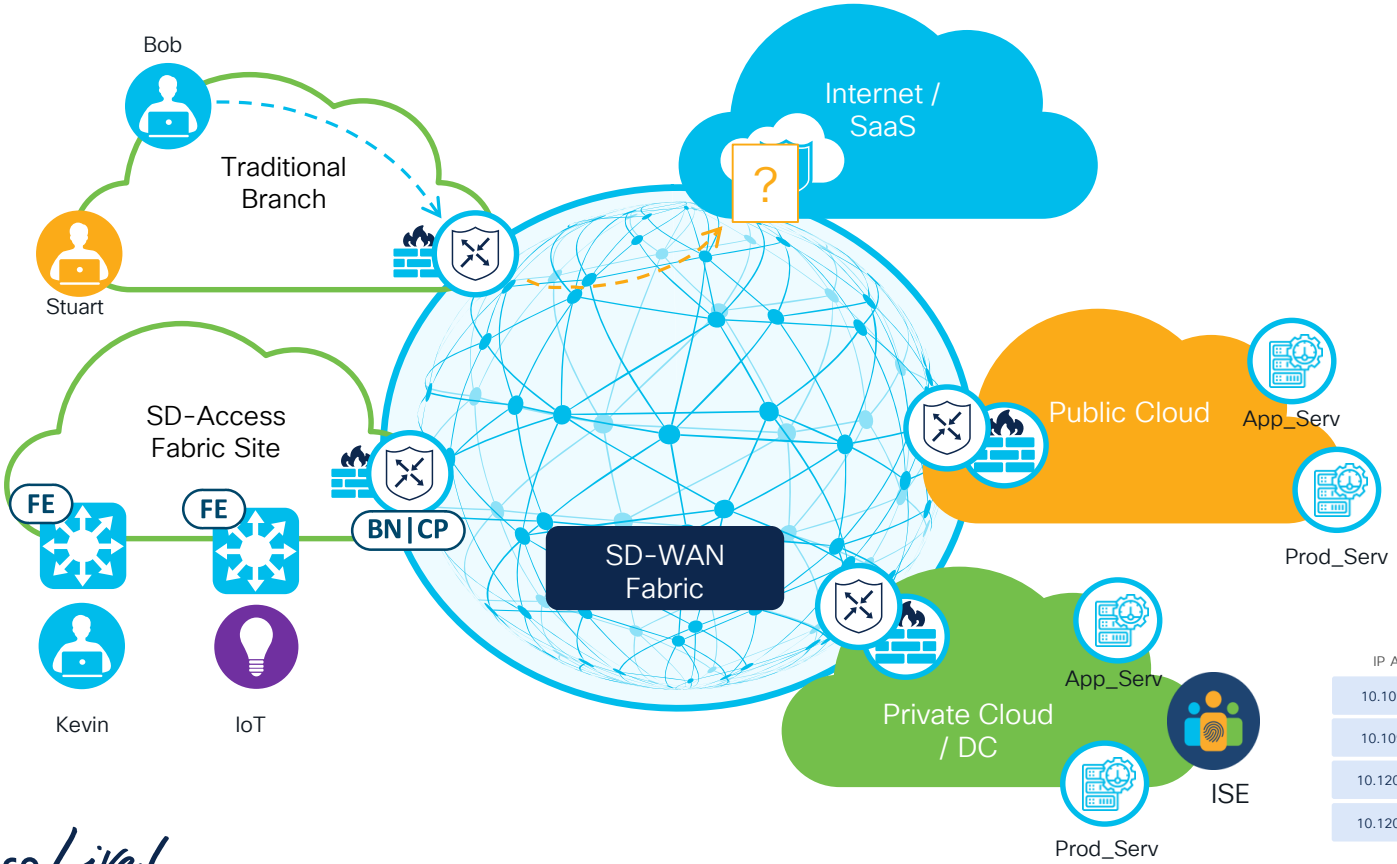
IP Addr	User/Profile	VRF/VPN
10.109.10.50	Bob	Staff
10.109.30.50	Stuart	Patient
10.120.10.101	Kevin	Staff
10.120.40.101	Light	IoT

Segmentation Prevents Dr. Bob Talking to Stuart



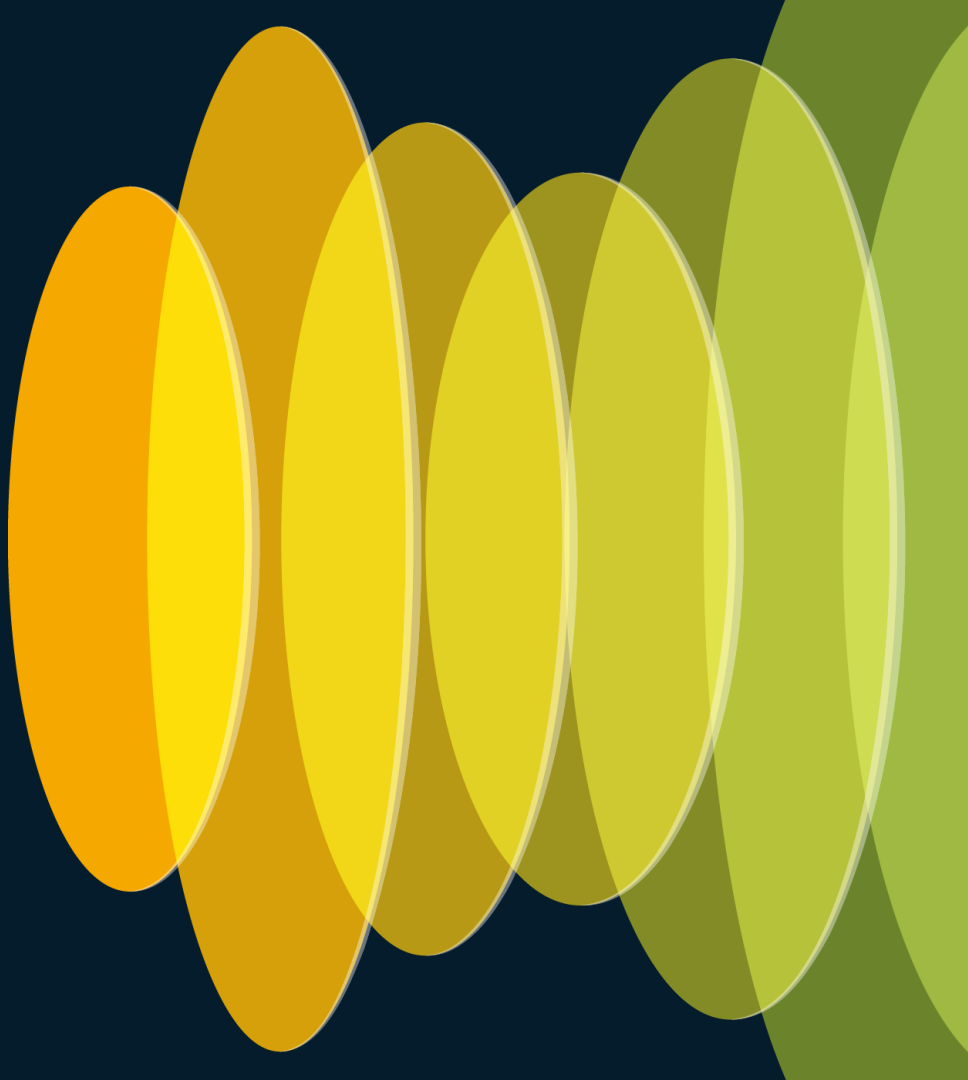
IP Addr	User/Profile	VRF/VPN
10.109.10.50	Bob	Staff
10.109.30.50	Stuart	Patient
10.120.10.101	Kevin	Staff
10.120.40.101	Light	IoT

How to Extend Segmentation Policies to Cloud?



IP Addr	User/Profile	VRF/VPN
10.109.10.50	Bob	Staff
10.109.30.50	Stuart	Patient
10.120.10.101	Kevin	Staff
10.120.40.101	Light	IoT

Extending Edge Segmentation for DNS Policies

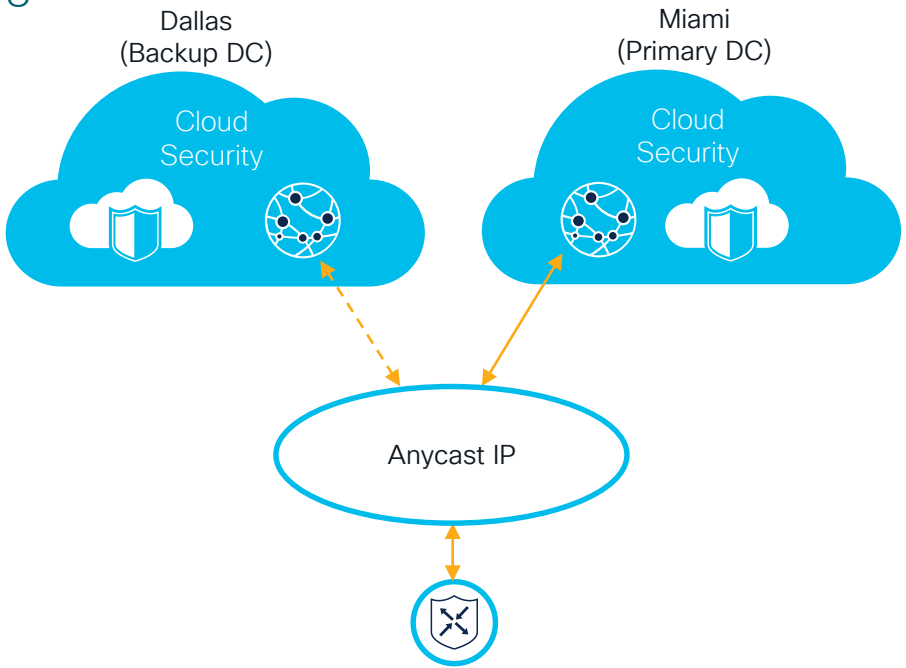


cisco Live!

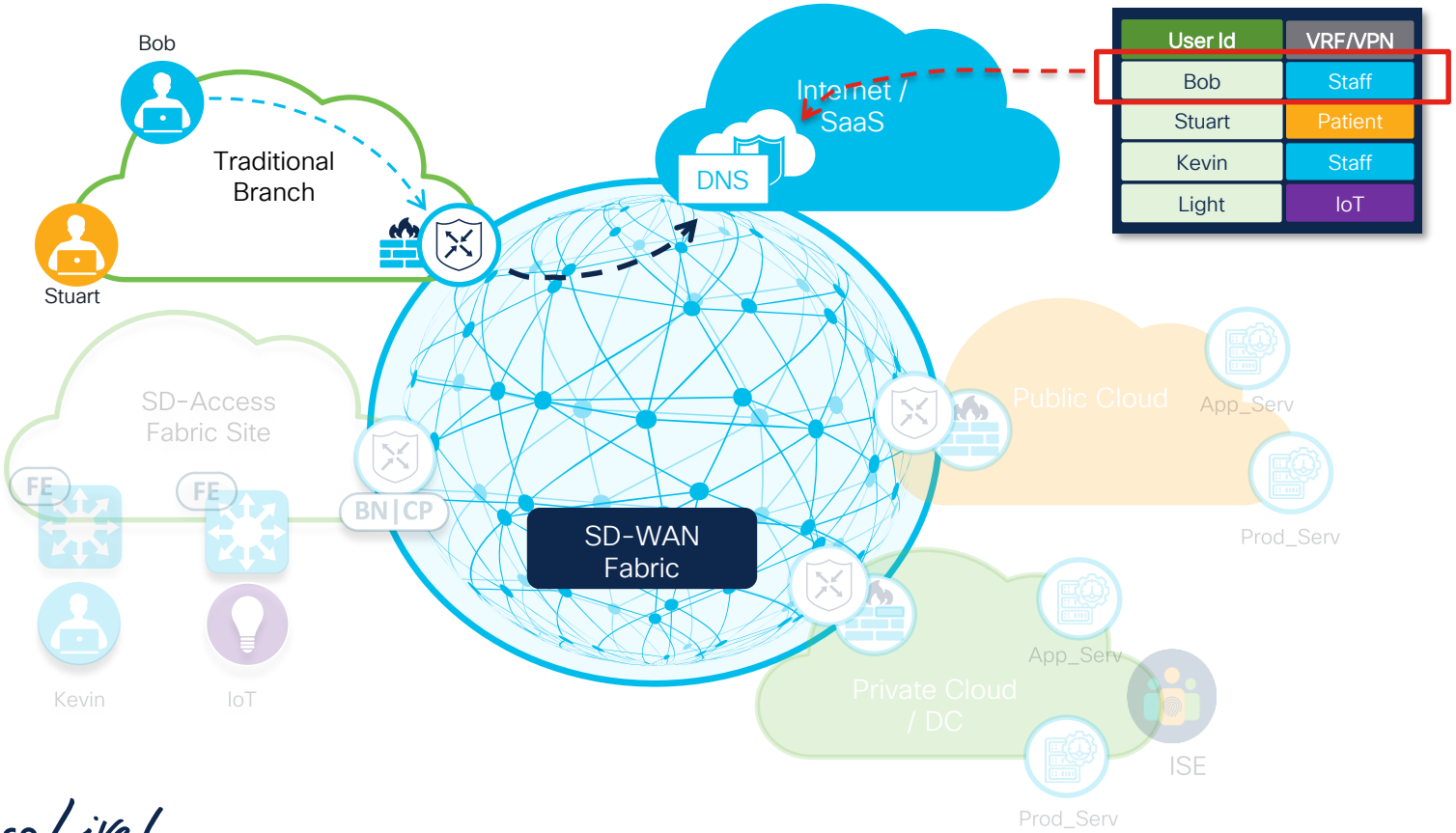
Extend Segmentation for DNS Protection

Catalyst SD-WAN and **Umbrella DNS** Integration

- Auto-Deploy DNS integration with Umbrella Network Devices API
- Anycast architecture for highly available integration – directs clients to not just closest DC but also includes awareness of load distribution
- Segmentation extension through VPN/VRF aware identity sources
- DNScrypt support for enhanced security – and necessary to share contextual data



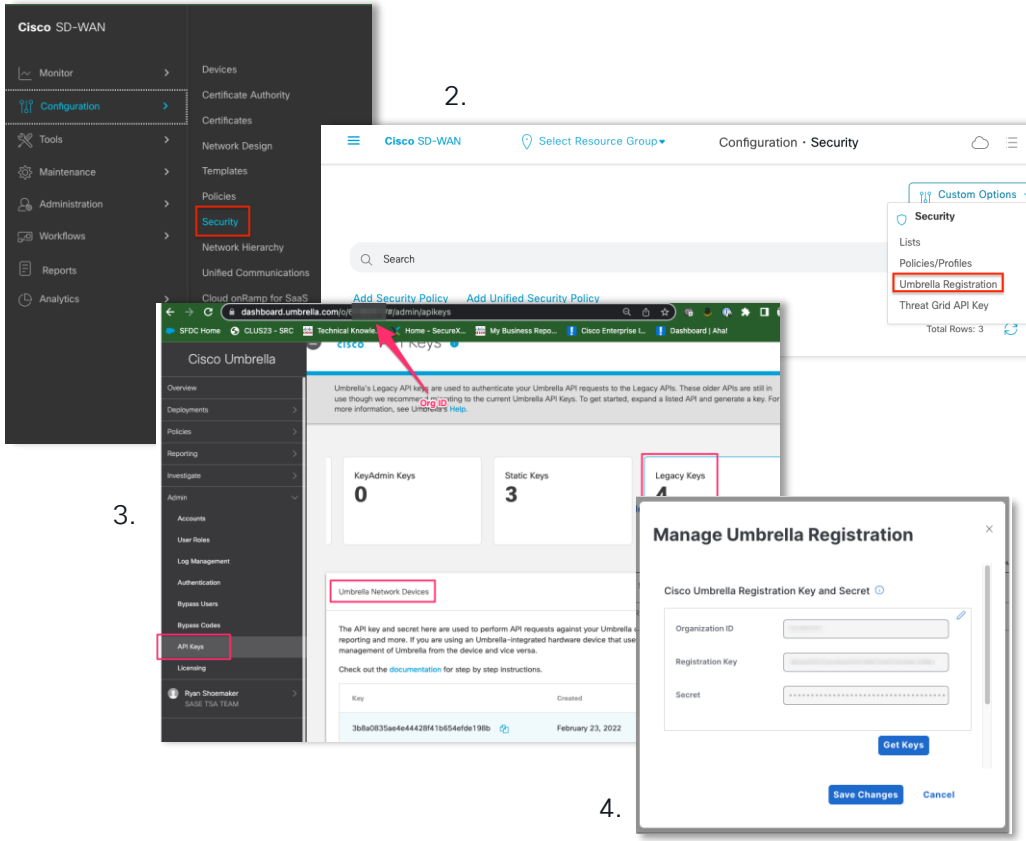
Dr. Bob Needs a Specific DNS Policy



Integrating Catalyst SD-WAN to Umbrella DNS

Reference

1. Select Configuration -> Security
2. Choose Custom Options -> Umbrella Registration
3. Add Umbrella API Keys
   - A. Created at Umbrella Dashboard: Admin -> API Keys
   - B. Use **Umbrella Network Devices** API Key (collect Key and secret)
   - C. Organization ID is located in URL of Umbrella Dashboard
4. Save Registration

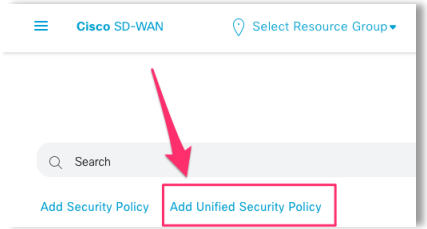


Setting DNS Redirection at the Router

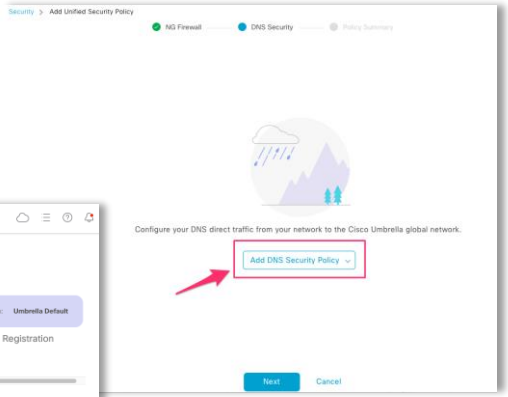
Reference

4. Add Unified Security Policy
5. Skip NG Firewall to move to DNS Security and Add DNS Security Policy
6. Complete Data for Policy
   - A. Note: Umbrella Registration Status will display green flag if registered correctly
   - **B. Choose match all VPNs or subset**
   - C. Create a domain bypass list for local domains
   - D. Under Advanced, ensure **DNSCrypt is enabled to convey source VPN info to Umbrella**
   - E. Save DNS Policy

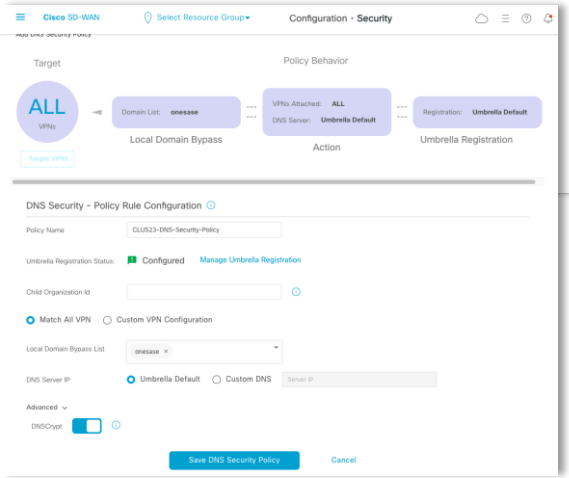
4.



5.



6.

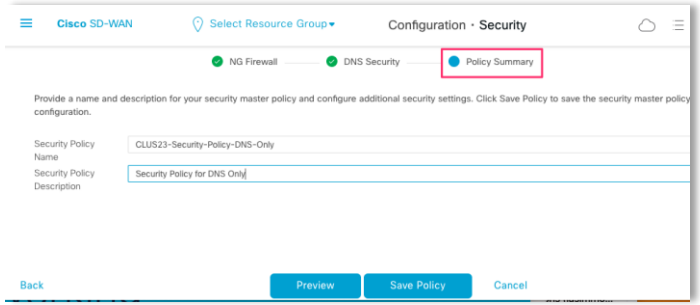


Setting DNS Redirection at the Router (cont.)

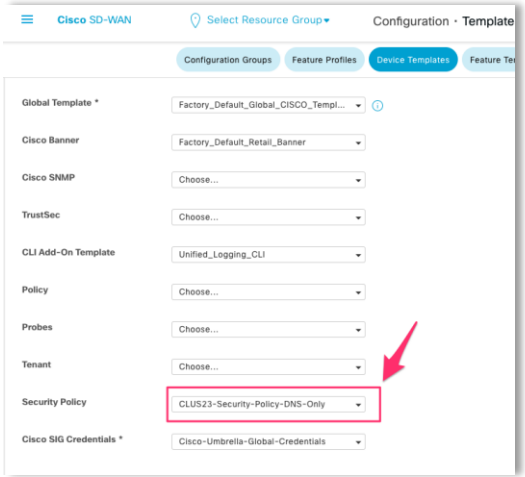
Reference

7. Name and save security policy
8. Assign policy to template
   A. either traditional template
   B. or UX2.0

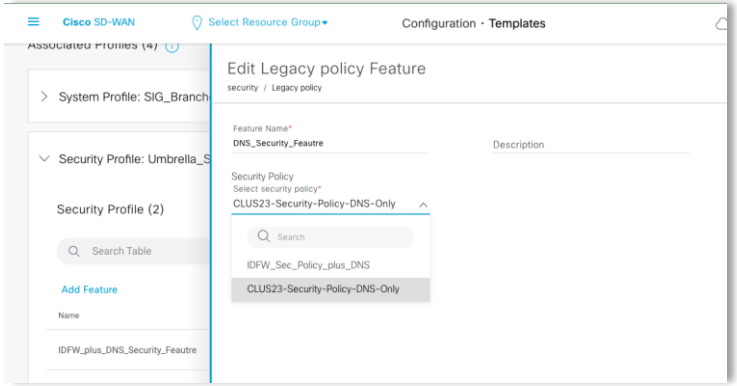
7.



8a.



8b.

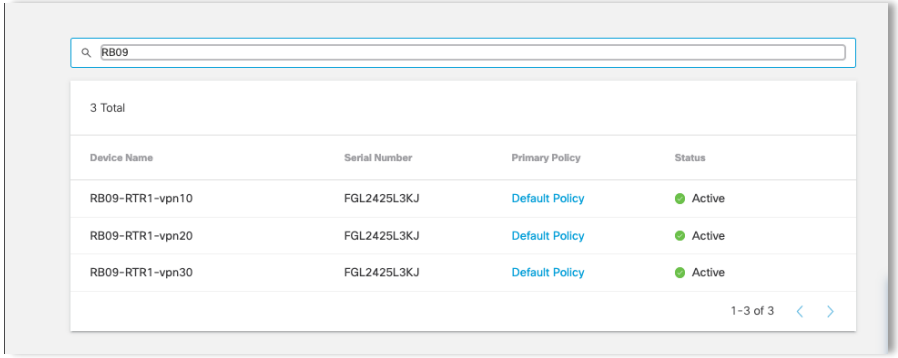


Leverage Source VRF/VPN for DNS Policy

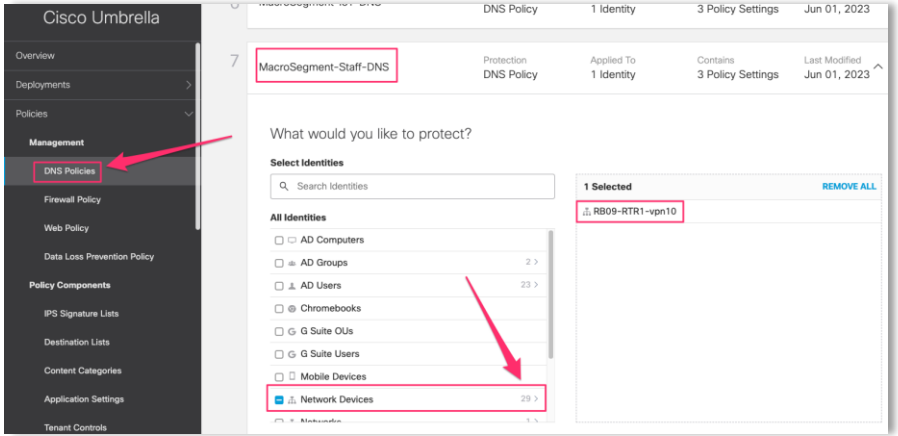
Reference

Umbrella Dashboard

In Umbrella, VPNs from branches appear automatically in: **Core Identities -> Network Devices**



Assign VPNs as Identities for DNS Policies in: **Policies -> DNS Policies -> Specific Policy -> Edit Identity**

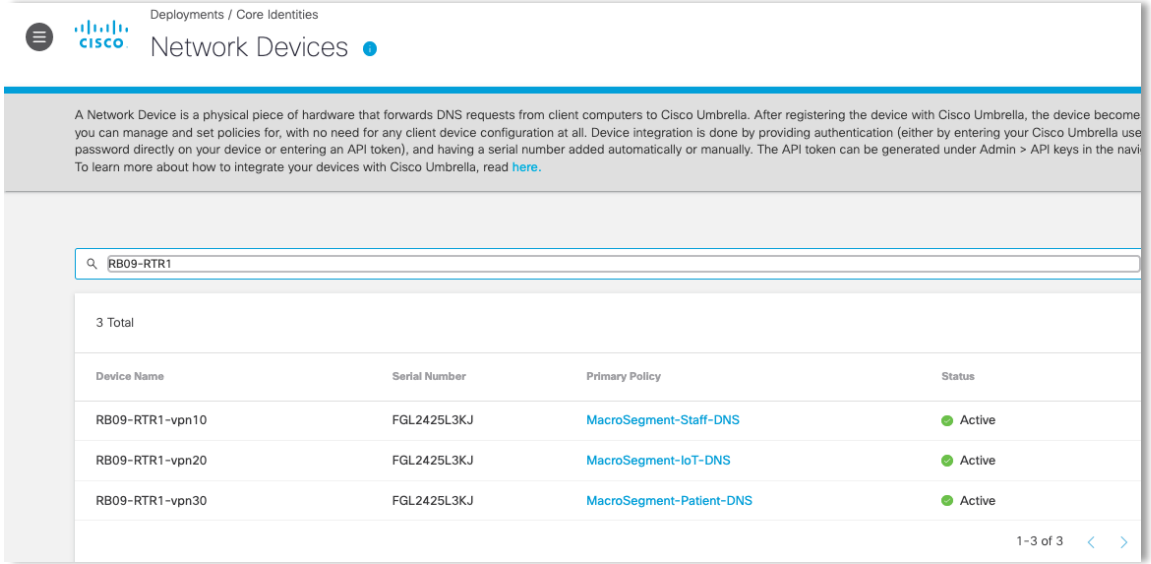


Leverage Source VRF/VPN for DNS Policy

Reference

Umbrella Dashboard

VPNs from branches now have different policy based on source VRF/VPN



DNS Policy Segmentation At Work

Policy for Staff might differ from Patient

2 Total Viewing activity from Jun 1, 2023 1:36 PM to Jun 2, 2023 1:36 PM

Results per page: 50 1 - 2

Request	Identity	Policy or Ruleset Identity	Destination	Destination IP	Internal IP	External IP	Action
DNS	RB09-RTR1-vpn30	RB09-RTR1-vpn30	www.box.com		10.109.30.101	209.122.90.235	Blocked – Public Application
DNS	RB09-RTR1-vpn10	RB09-RTR1-vpn10	www.box.com		10.109.10.103	209.122.90.235	Allowed

Category **Blocked** for Patient VRF

Event Details

Action
Blocked – Public Application

Time
Jun 2, 2023 1:36 PM

Identity
RB09-RTR1-vpn30

Policy or Ruleset Identity
RB09-RTR1-vpn30

Internal IP Address
10.109.30.101

External IP Address
209.122.90.235

Destination
www.box.com

Categories
Application Block, Online Storage and Backup, File Storage (Legacy)
Dispute Categorization

Public Application
Box Cloud Storage

Application Category
Cloud Storage

DNS Type
A

Category **Allowed** for Staff VRF

Event Details

Action
Allowed

Time
Jun 2, 2023 1:35 PM

Identity
RB09-RTR1-vpn10

Policy or Ruleset Identity
RB09-RTR1-vpn10

Internal IP Address
10.109.10.103

External IP Address
209.122.90.235

Destination
www.box.com

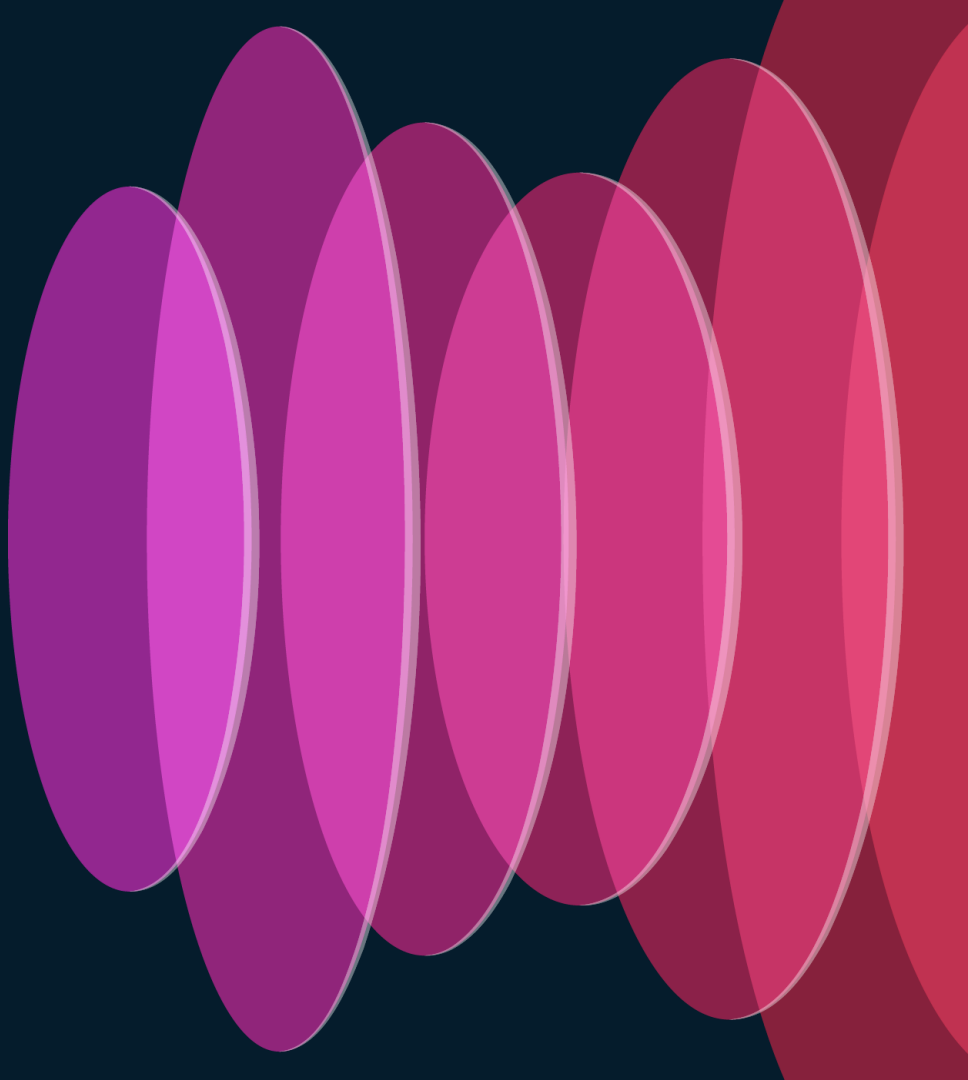
Categories
File Storage (Legacy), Online Storage and Backup
Dispute Categorization

Public Application
Box Cloud Storage

Application Category
Cloud Storage

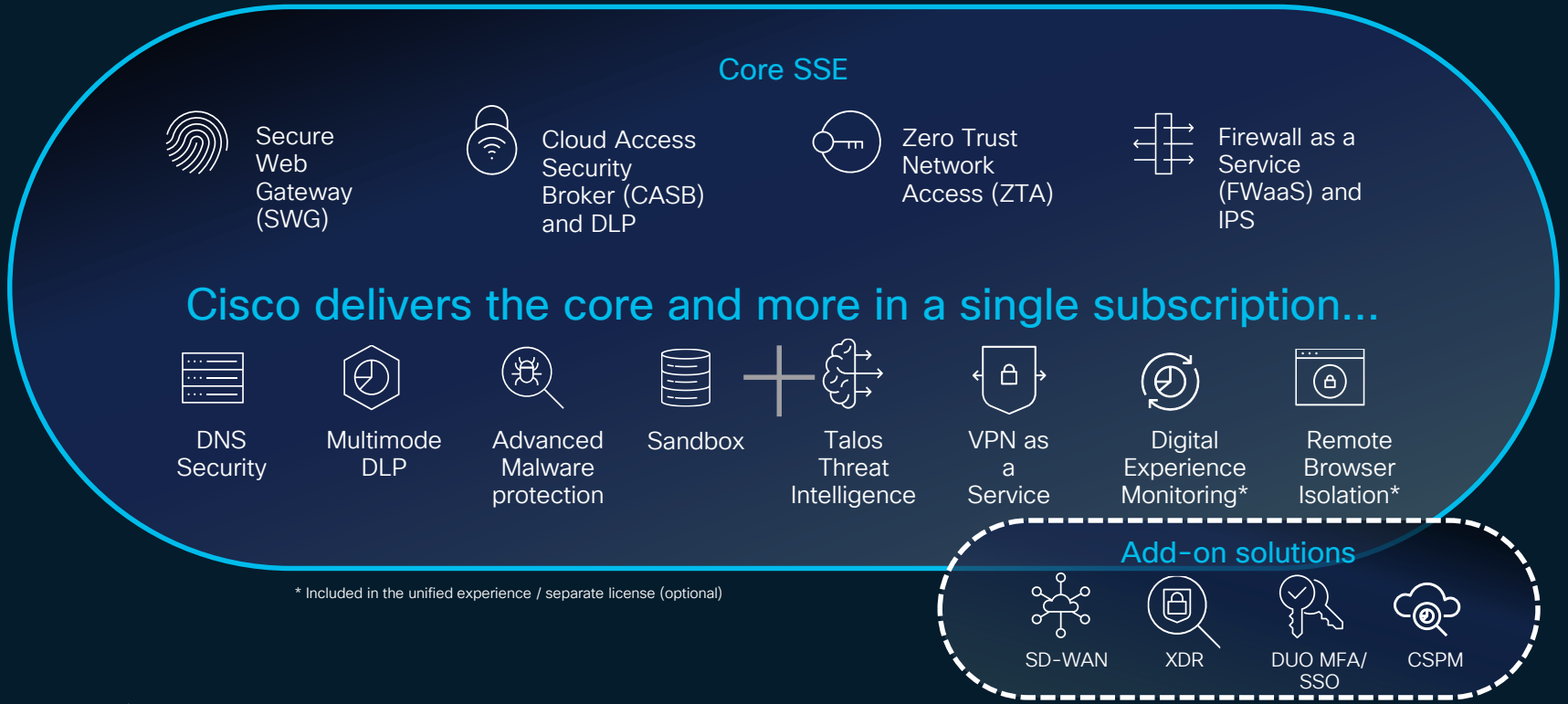
DNS Type
A

Extending Edge Segmentation for Internet and SaaS Policies



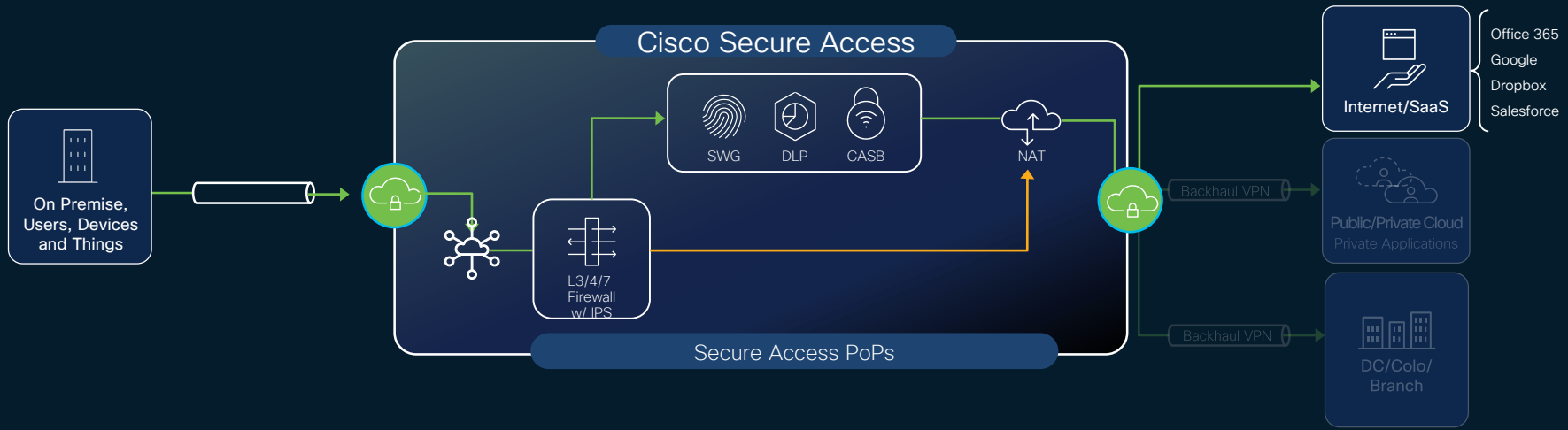
cisco Live!

Cloud Security Provided Cisco Secure Access



Secure Branch Access

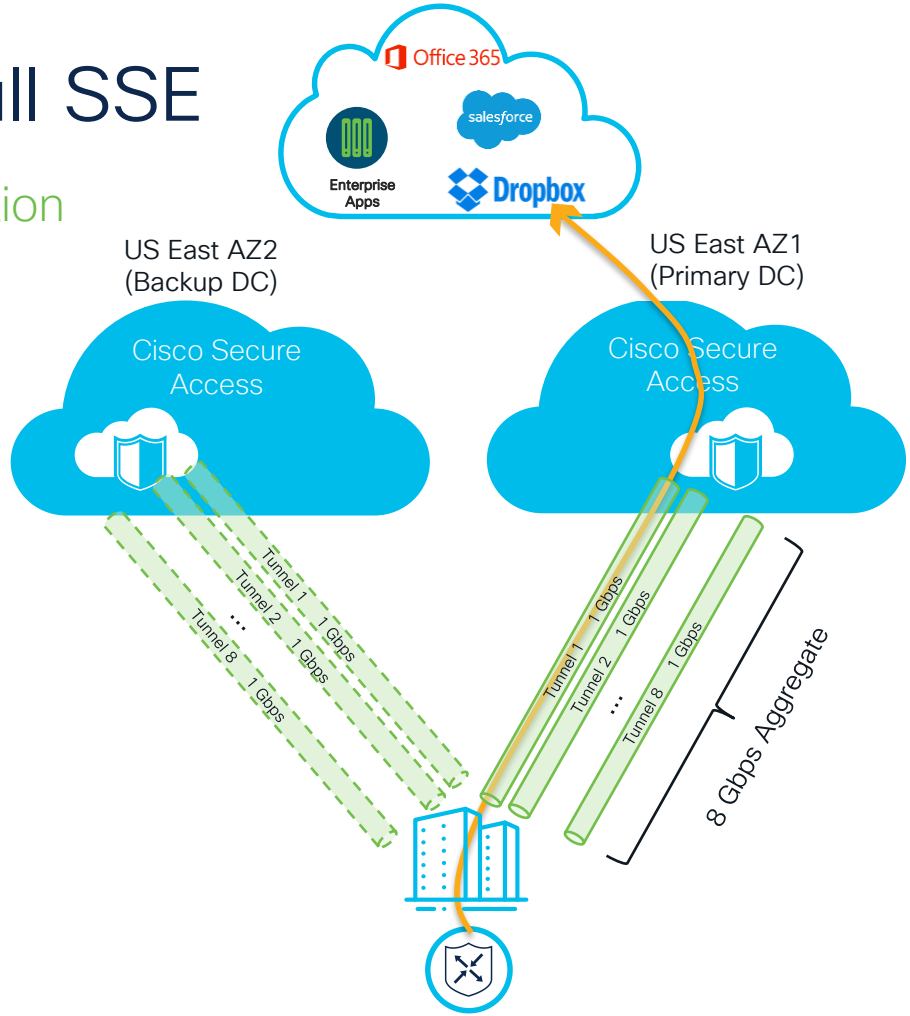
Secure Internet Access



Extend Segmentation for Full SSE

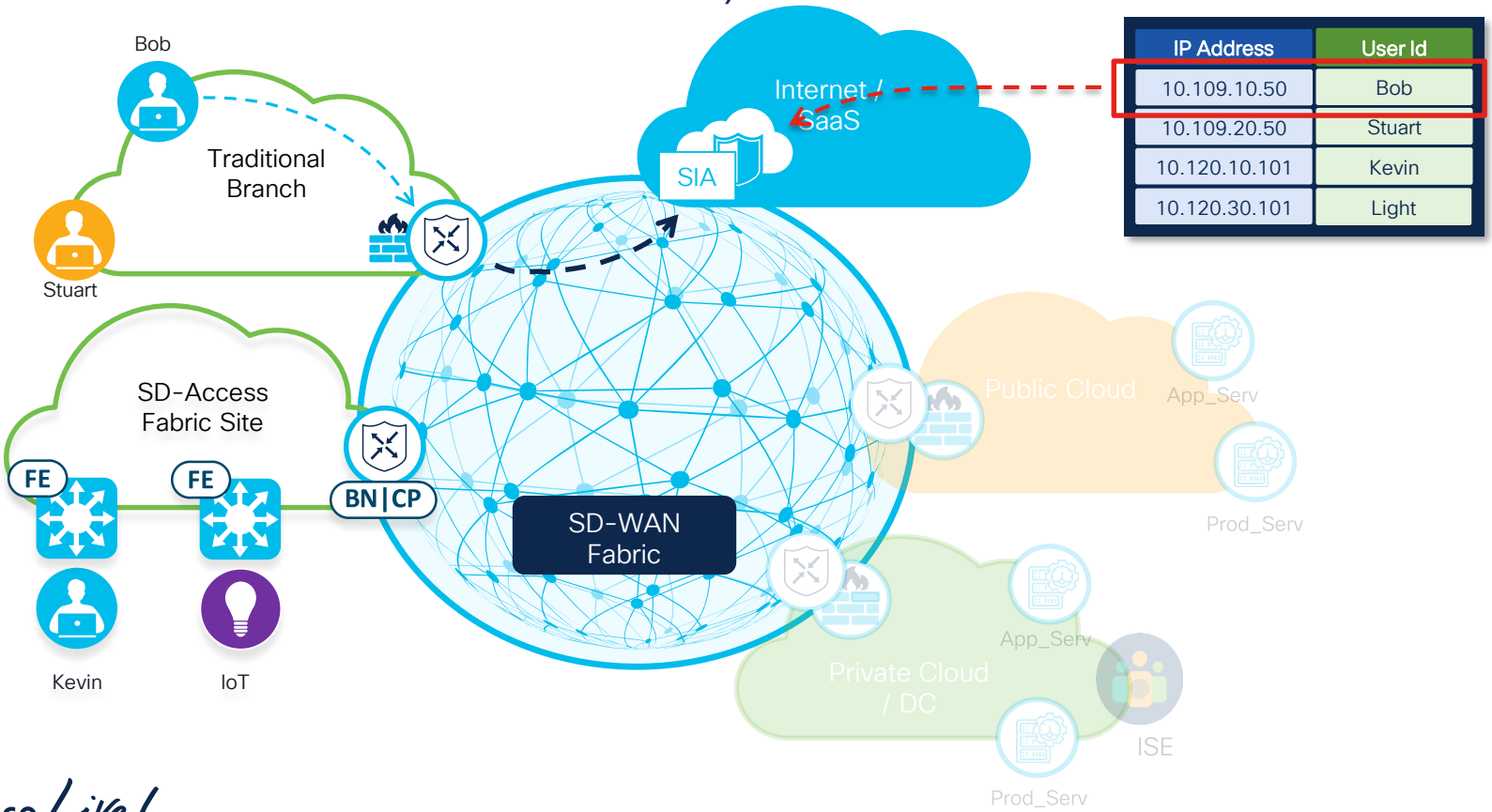
Catalyst SD-WAN & Secure Access Integration

- Auto-provision and Auto-deploy highly available tunnels with a few clicks
- Active-Active and Active/Standby design
- Support for auto or manual DC selection
- Up to 8 active and 8 standby tunnels
- ECMP or weighted load-balancing
- Throughput capacity to 8 Gbps
- Layer 7 health checks to Secure Access to monitor the health of the tunnel
- SaaS traffic optimization for Critical Apps with Layer7 health check



And Dr. Bob Needs a Specific Security Policy

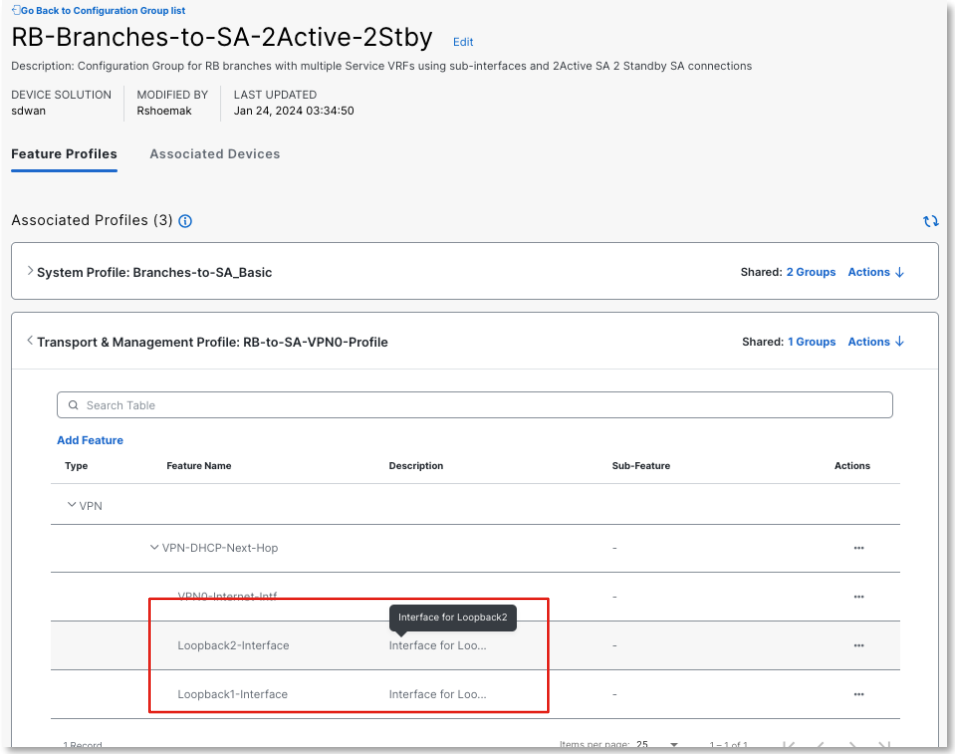
(Associated with his Network Subnet)



Catalyst SD-WAN and Secure Access Integration

Pre-requisites

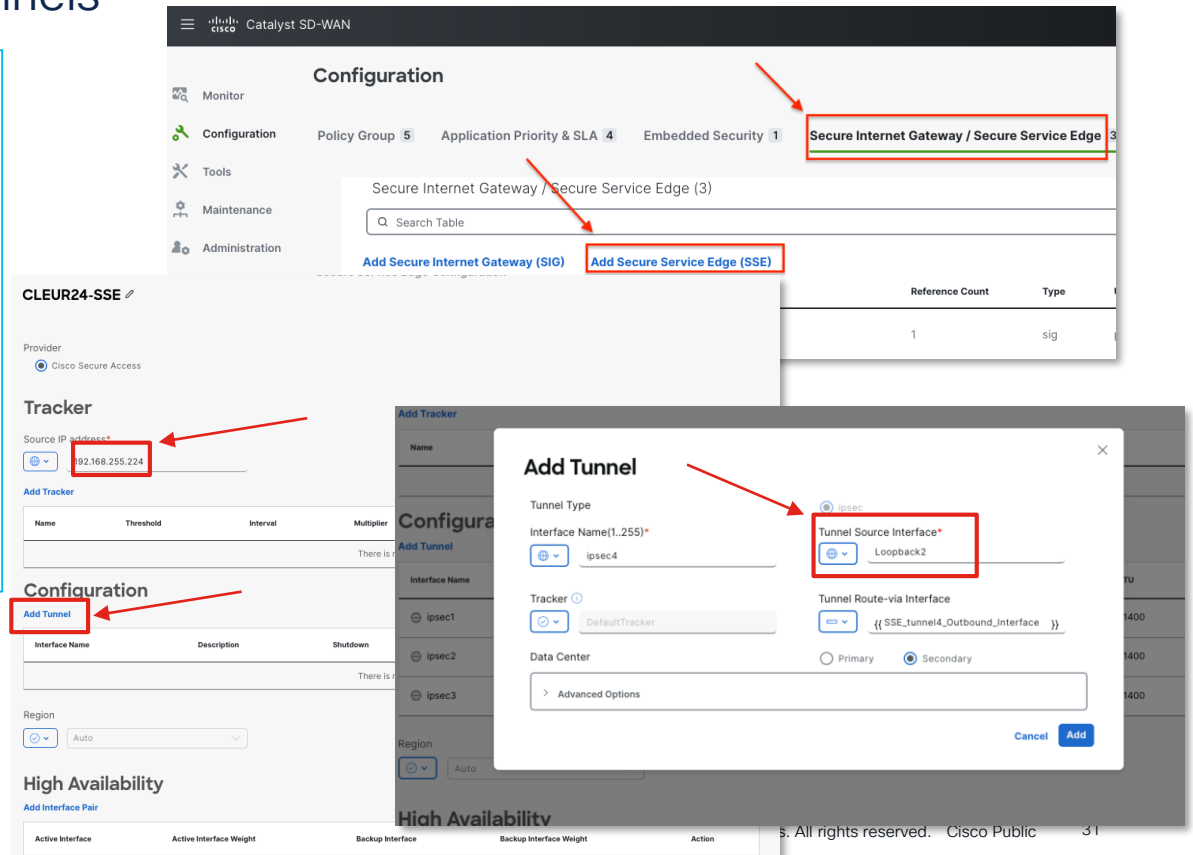
- Manager 20.13 and Edge 17.13
- Secure Access API added to Catalyst SD-WAN Manager: Administration -> Cloud Credentials -> Cloud Provider Credentials -> Cisco Secure Access
- Secure Access integration only through **Configuration Groups** and **Feature Profiles**
- “Domain Lookup” enabled in Global Feature
- DNS Server Configured on VPN0 in Catalyst Manager
- Each active tunnel requires a unique IP source address – can be physical or loopback



Catalyst SD-WAN and Secure Access Integration

Policy Groups – Adding Tunnels

- Add Secure Service Edge
- Tracker source IP address – required, any 1918 address
- Add tunnel(s) for each connection to Secure Access
- Each active/backup pair needs unique source interface - if multiple tunnels will use same physical interface, then source tunnel using Loopbacks

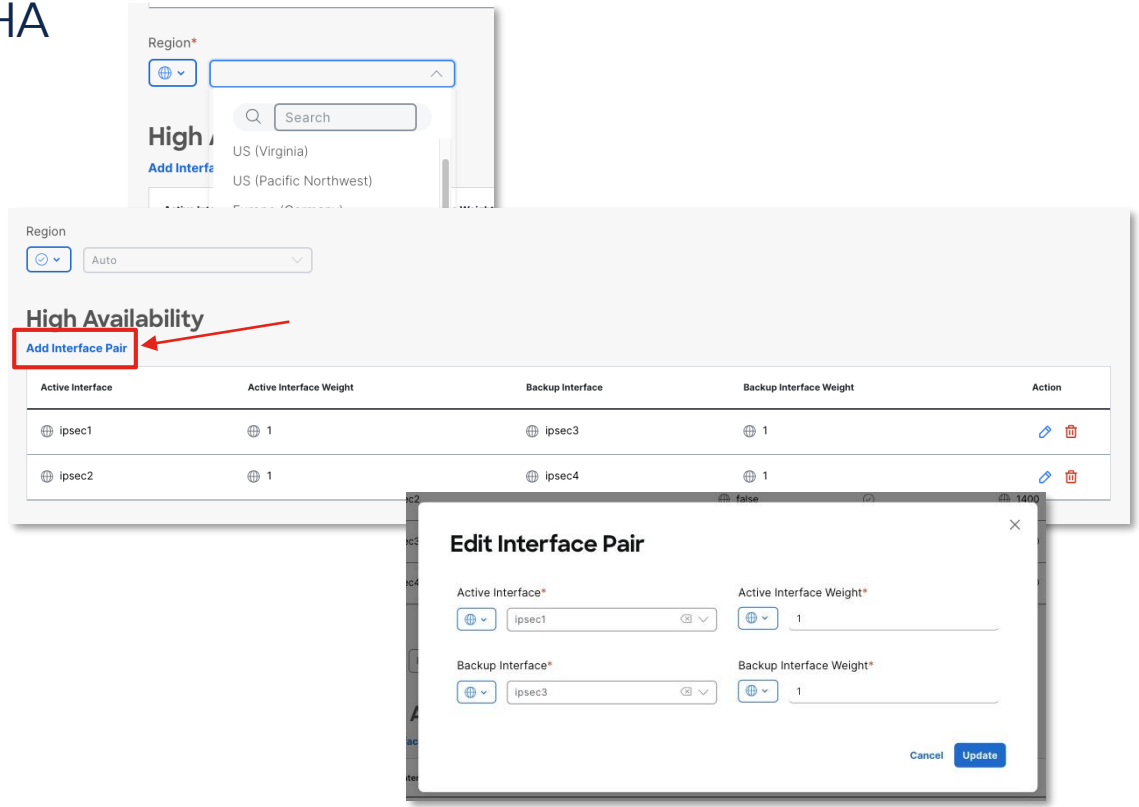


Reference

Catalyst SD-WAN and Secure Access Integration

Policy Groups – Choosing HA

- Automatically or manually choose Secure Access region
- Add Interface Pair – Up to 8 active + 8 backup tunnels allowed
- Select active and backup interfaces and weight for each – default is ECMP

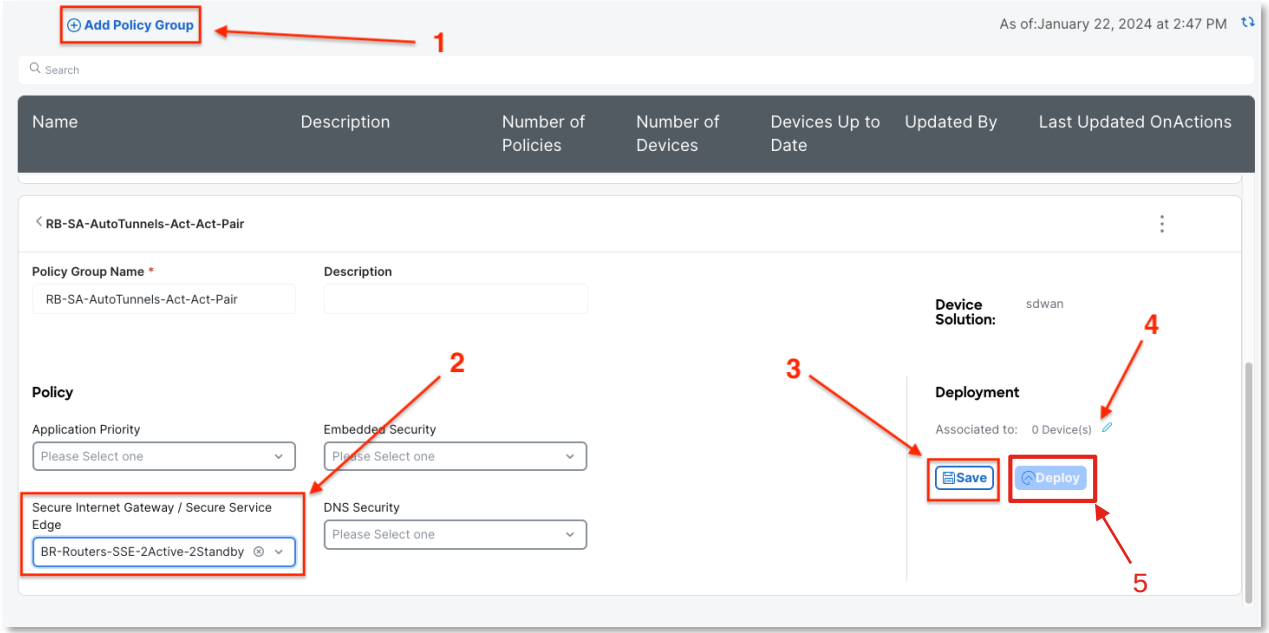


Reference

Catalyst SD-WAN and Secure Access Integration

Policy Groups – Assigning SSE

1. Add Policy Group
2. Select SSE Configuration
3. Save Policy Group
4. Associate Device(s)
5. Deploy



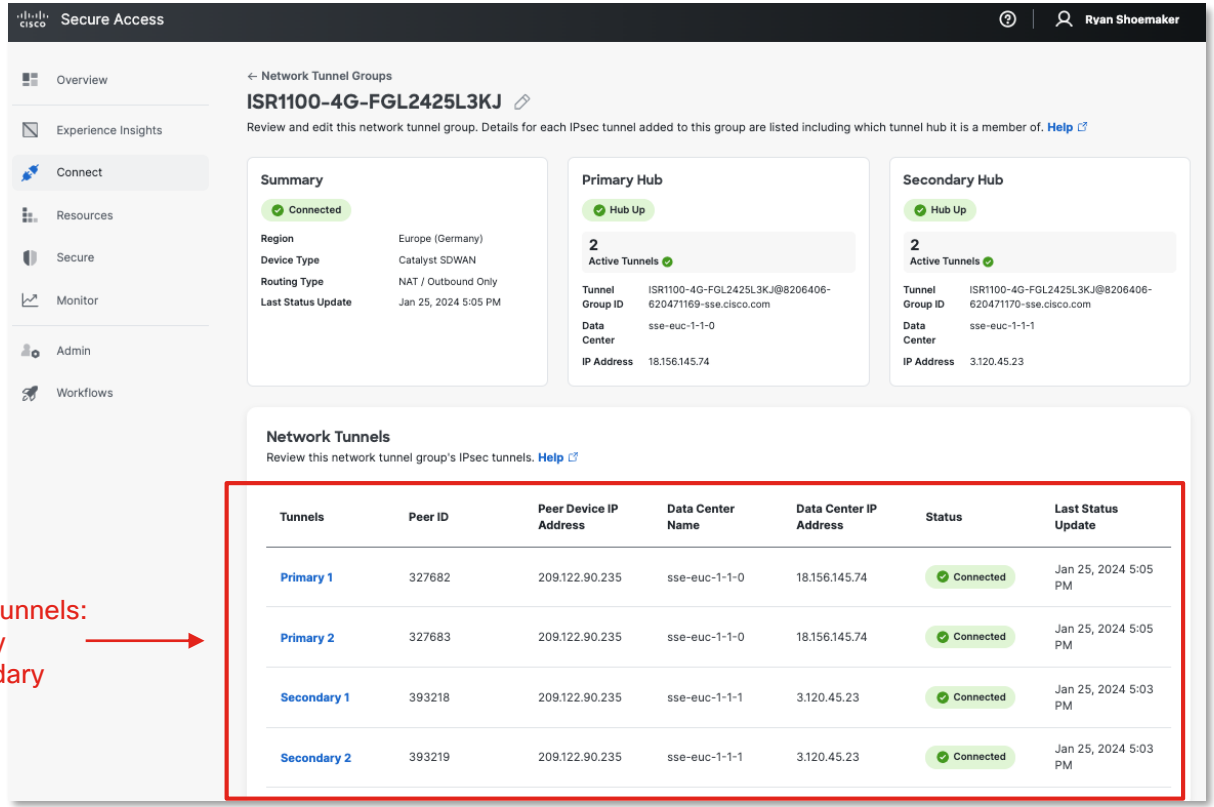
Reference

Verify Integration

Cisco Secure Access

- Tunnels Connected at Secure Access
- Leverage Network *Tunnel Group* for all tunnels from router
- Enables simplified policy rules to enforce for all traffic coming form router

4 IPSec tunnels:
2 Primary
2 Secondary



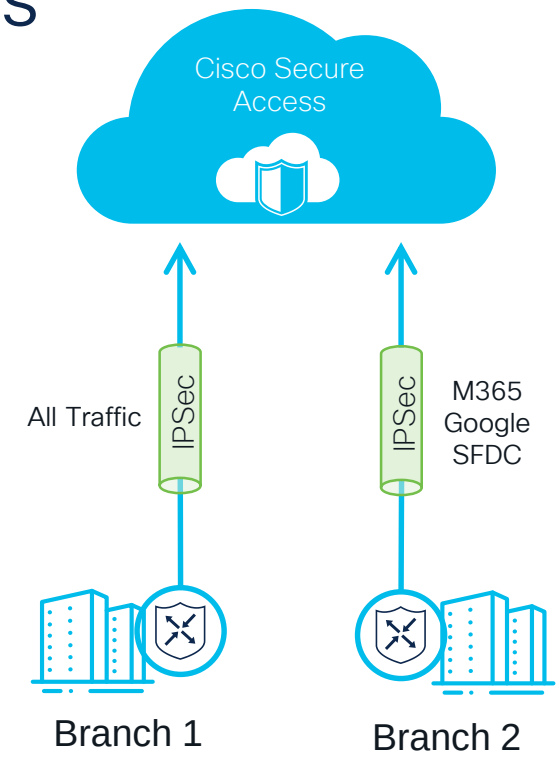
Directing Traffic to Secure Access

Option 1: Set Service Route of 0.0.0.0/0 to direct default to SSE

- Simple to set the default route pointing for all non-internal traffic to SSE
- Set per VRF

Option 2: Policy Based Routing Using Flexible Traffic Engineering

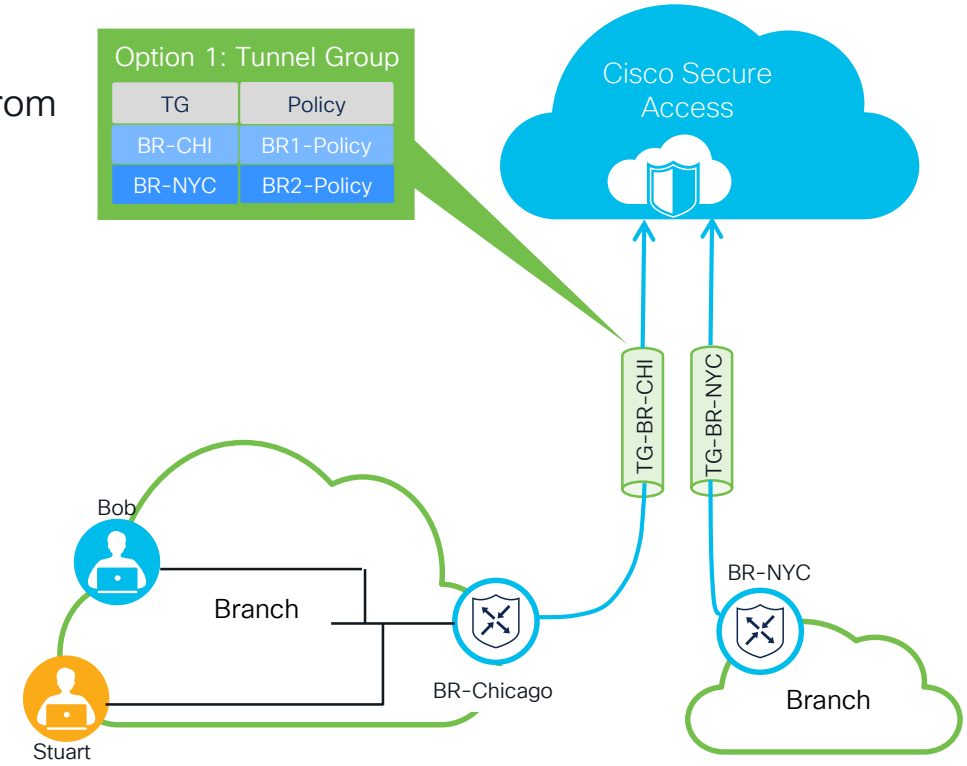
- Flexibility to select which applications send traffic to SSE
- Leverage DPI for app-classification
- Route-based redirection also possible



Setting Security Policy for Branch Users

As of SD-WAN Release 20.13 / 17.13

Option 1: Set Policy for all traffic coming from Branch via ***Tunnel Group***

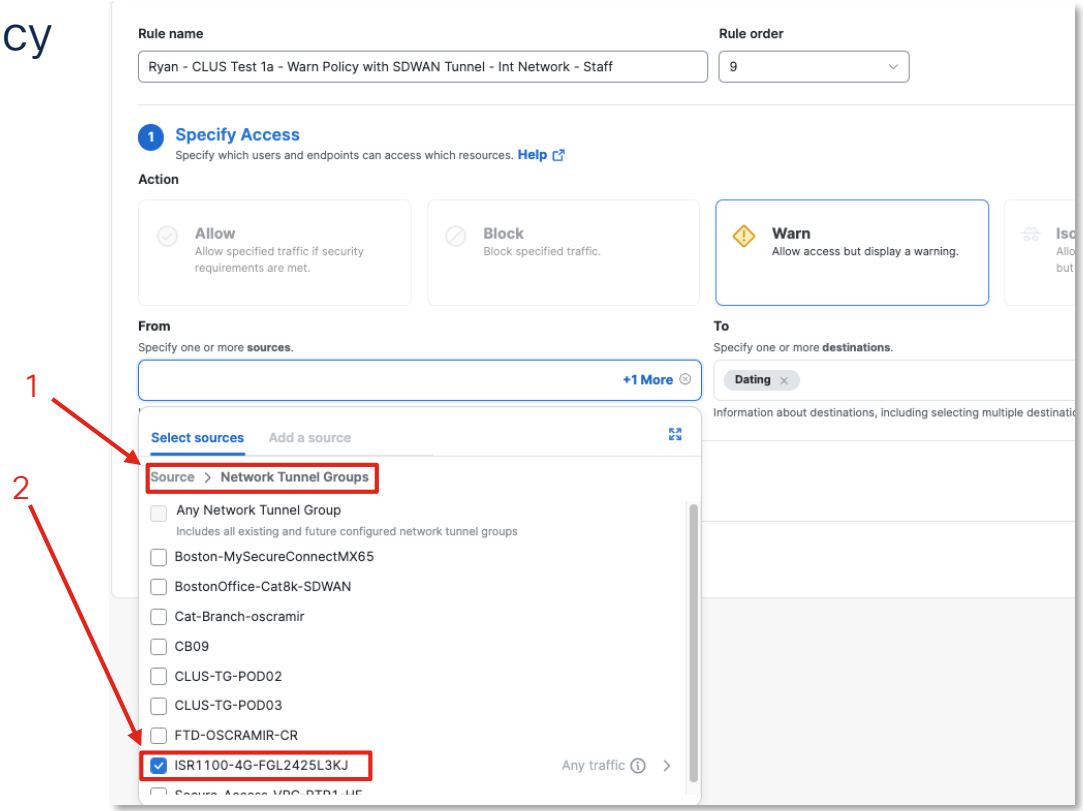


Secure Access Network Tunnel Groups

Set TG as Source of Policy

1. In Access Policy, create Rule and in From: expand Network Tunnel Groups as source.

2. Select specific Tunnel Group to apply policy to any traffic coming through the tunnel.

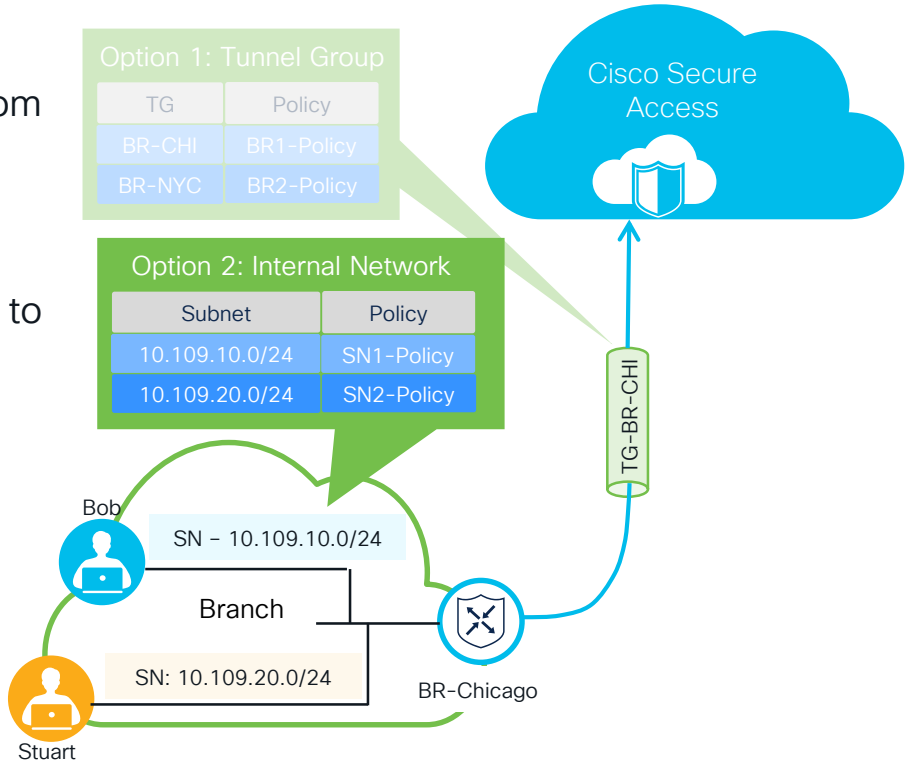


Setting Security Policy for Branch Users

As of SD-WAN Release 20.13 / 17.13

Option 1: Set Policy for all traffic coming from Branch via ***Tunnel Group***

Option 2: Create ***Internal Network*** mapping to set policy per IP subnet per TG



Secure Access Internal Networks

Reference

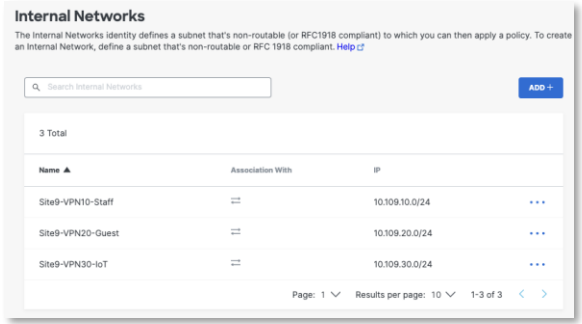
Set Subnet at Branch as Source of Policy

1. Identify specific internal networks at **Resources -> Internal Networks**. Select **Add+**

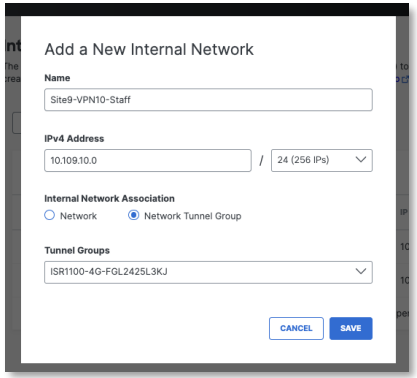
2. Map VPN subnet to source Tunnel Group by adding VPNs IP Subnet and choose the correct **Network Tunnel Group**.

3. In Access Policy, create Rule and in From: expand Network Tunnel Groups then the specific Tunnel Group as source.
4. Check box for correct internal network

1

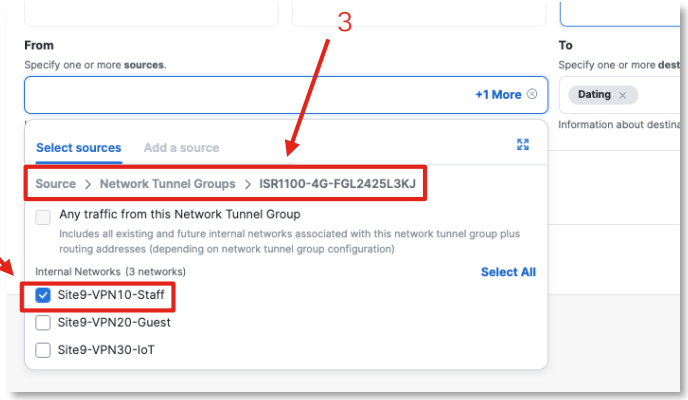


2



3

4



Web Policy Segmentation At Work

Policy for Staff might differ from Patient

Request	Source	Rule Identity	Destination	Internal IP	Action	Categories
WEB	Site9-VPN20-Guest	Site9-VPN20-Guest	https://www.box.com/	10.109.20.2	Blocked	**Online Storage and Backup,** File Storage
WEB	Site9-VPN10-Staff	Site9-VPN10-Staff	https://www.box.com/	10.109.10.2	Allowed — Warn Page Displayed	**Application Warn, Online Storage and Backup,** File Storage
WEB	Site9-VPN10-Staff	Site9-VPN10-Staff	https://www.box.com/	10.109.10.2	Allowed — Warn Page Displayed	**Application Warn, Online Storage and Backup,** File Storage

Web policy specifically applied to traffic from VPN20 coming through SD-WAN tunnel

Category **Blocked** for Patient VRF

Action
Blocked

Time
May 30, 2024 4:02 PM

Rule Name
Ryan - CLUS Test 1b - Block Policy with SDWAN Tunnel - Int Network - Staff

Source
Site9-VPN20-Guest
ISR1100-4G-FGL2425L3KJ

Rule Identity
Site9-VPN20-Guest

Internal IPv4 Address
10.109.20.2

External IP Address
-

Destination
https://www.box.com/

Hostname
www.box.com

Categories
Online Storage and Backup, File Storage
Dispute Categorization

Resource/Application
Box Cloud Storage

Application Category
Cloud Storage

Category **Warned** for Staff VRF

Action
Allowed — Accessed After Warn

Time
May 30, 2024 4:03 PM

Rule Name
Ryan - CLUS Test 1a - Warn Policy with SDWAN Tunnel - Int Network - Staff

Source
Site9-VPN10-Staff
ISR1100-4G-FGL2425L3KJ

Rule Identity
Site9-VPN10-Staff

Internal IPv4 Address
10.109.10.2

External IP Address
-

Destination
https://www.box.com/

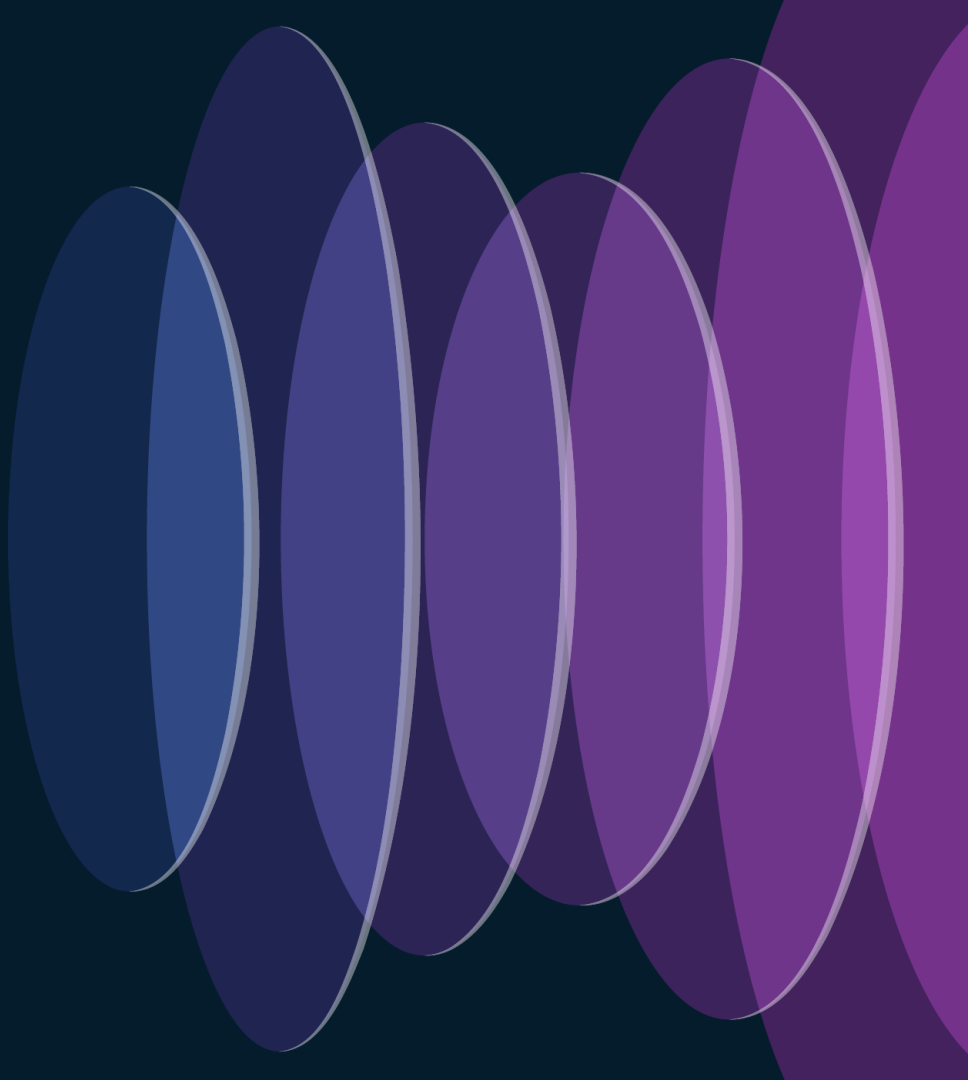
Hostname
www.box.com

Categories
Application Warn, Online Storage and Backup, File Storage
Dispute Categorization

Resource/Application
Box Cloud Storage

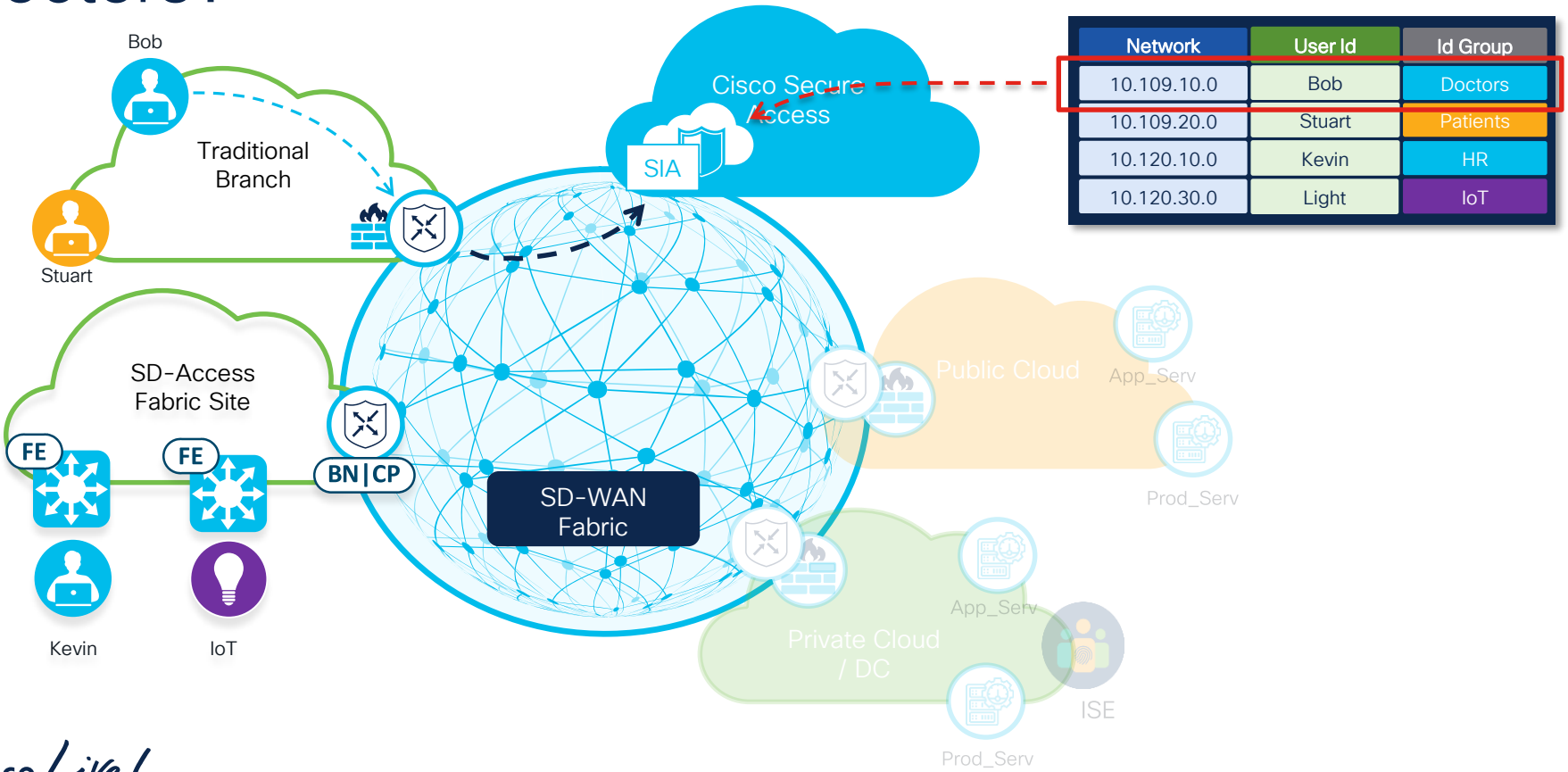
Application Category
Cloud Storage

Internet and SaaS Policy for Groups using SAML



cisco Live!

But What If Dr. Bob Needs Security Policy for Doctors?



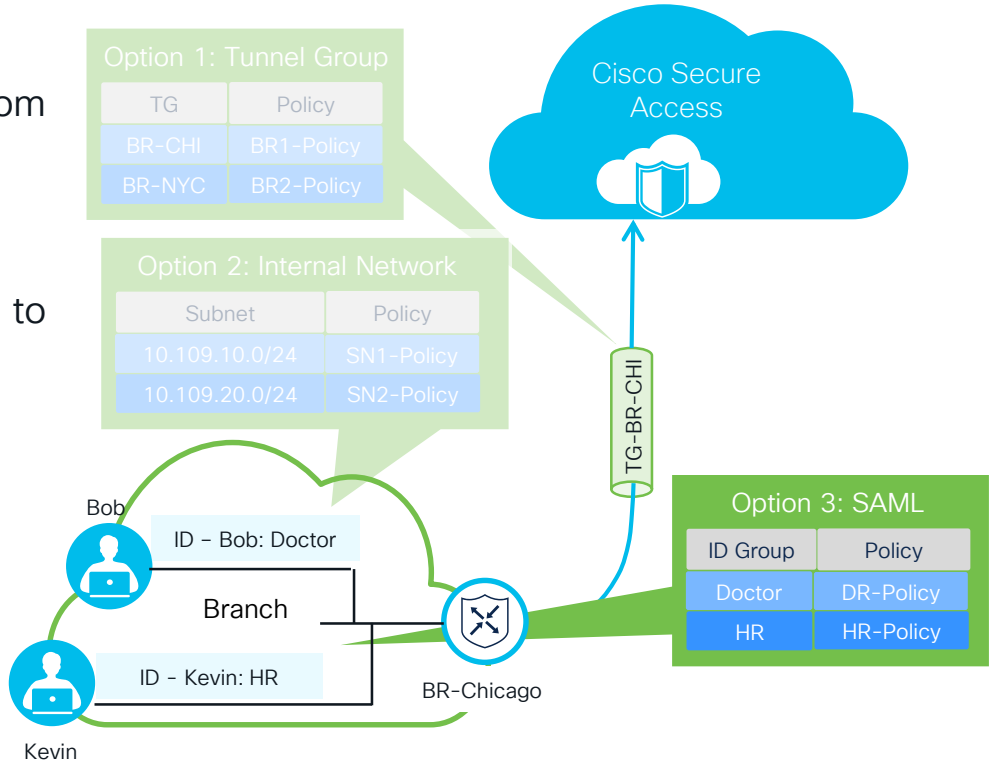
Setting Security Policy for Branch Users

As of SD-WAN Release 20.13 / 17.13

Option 1: Set Policy for all traffic coming from Branch via ***Tunnel Group***

Option 2: Create ***Internal Network*** mapping to set policy per IP subnet per TG

Option 3: Enable ***SAML*** authentication to identify ID Group to set policy per group



A Word About SAML and SCIM

SCIM (System for Cross-domain Identity Management)

- Automates the exchange of user identity information between domains
- Creates standard data structure so identity information is stored in a consistent way
- Provides a single system to manage users and groups

SAML (Security Assertion Markup Language)

- Authentication language between identity providers (IdP) and Service Providers (SP)
- Enabled Single Sign-On (SSO)
- Can be Used in Combination with MFA

ID as Policy Source from a Branch

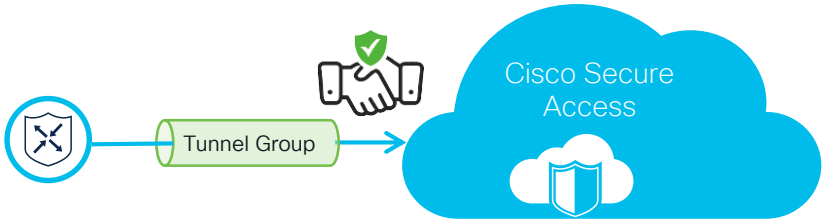
Secure Access **is not** an open proxy

So what?

It must trust the source of the request

Adding Tunnel Groups from a router creates a trusted identity

But that means policy is based on the tunnel name of Internal Network and so the same policy applies to any device connecting through that tunnel or subnet, right?



SAML

(to the rescue!!)

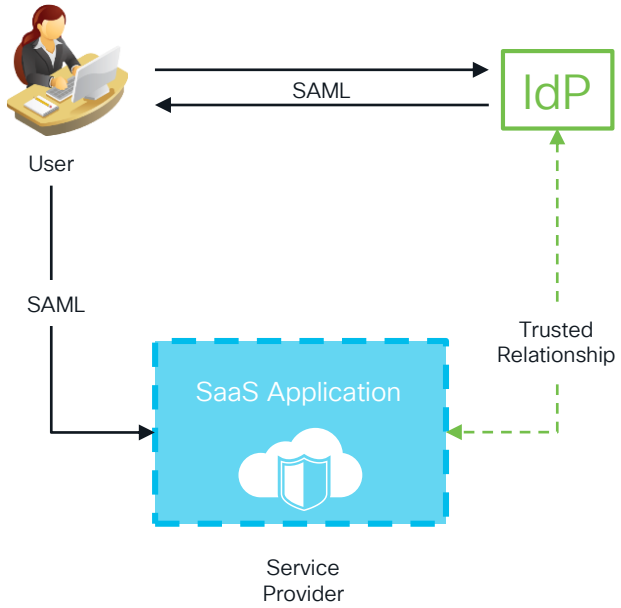
SAML at a High Level

Security Assertion Markup Language

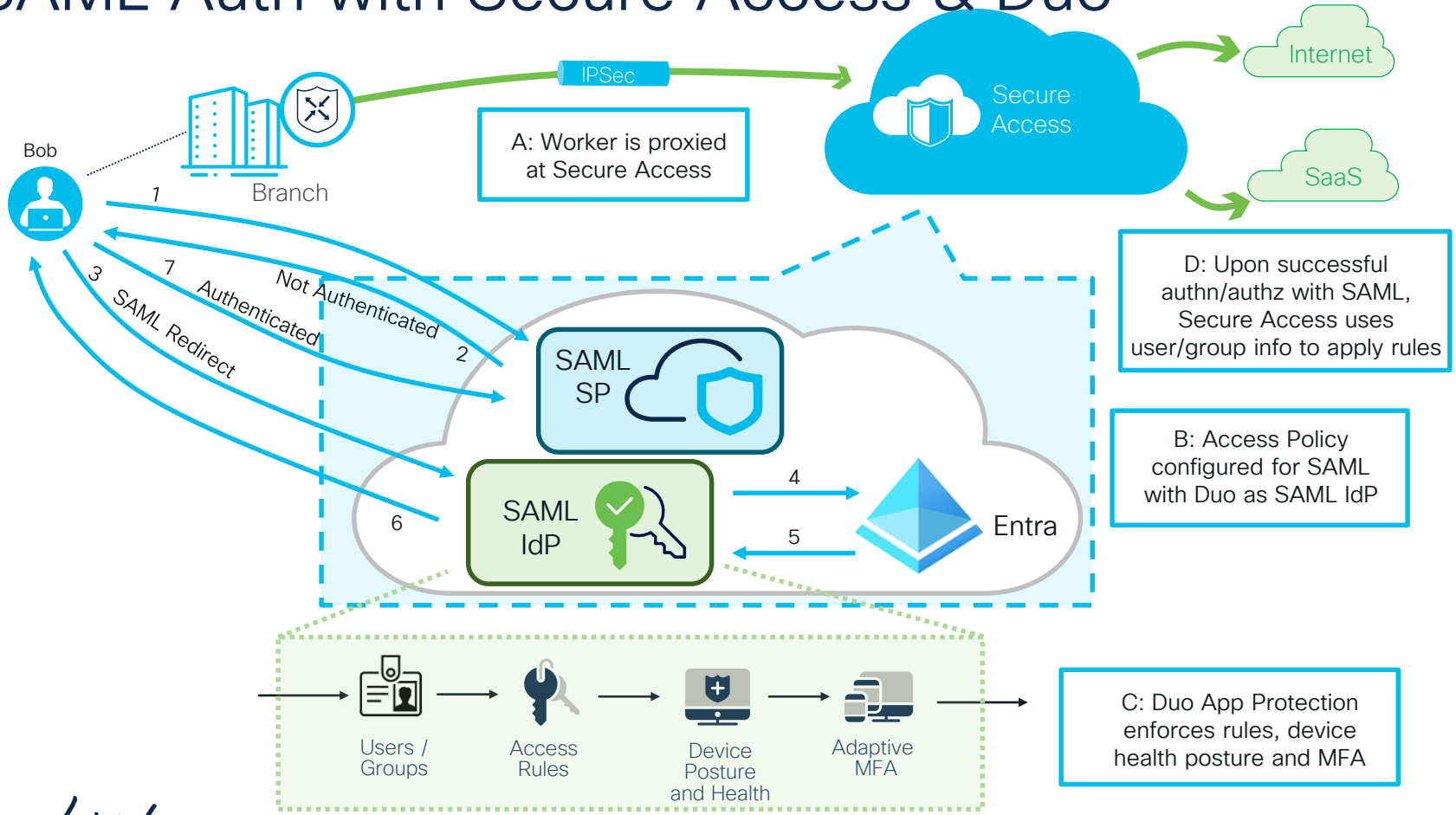
SAML is authentication mechanism used to access multiple web applications with one set of credentials (SSO)

Works by passing authentication information via HTTP redirects between a Service Provider (SP) and an Identity Provider (IdP)

Authentication information includes logins, authentication state, identifiers, or other relevant attributes



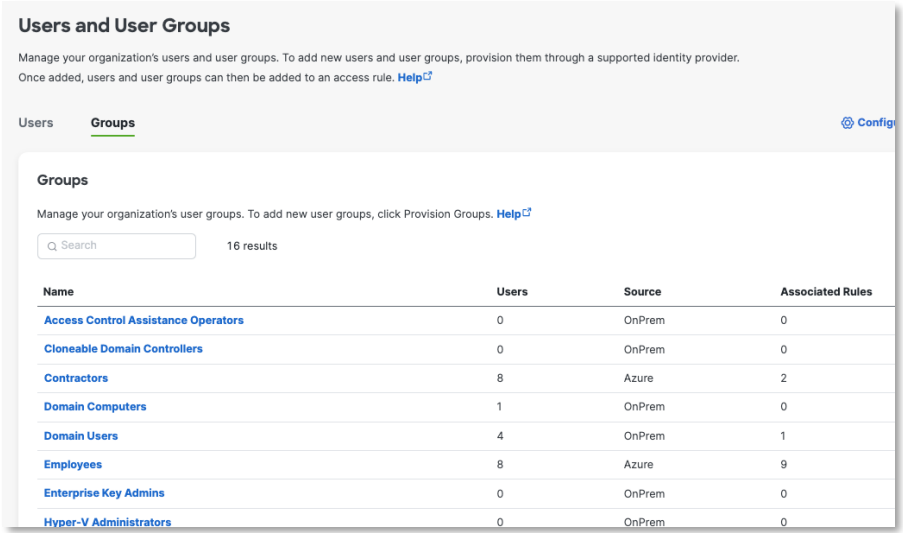
SAML Auth with Secure Access & Duo



SCIM Enables Id Services to Provide Users and Groups

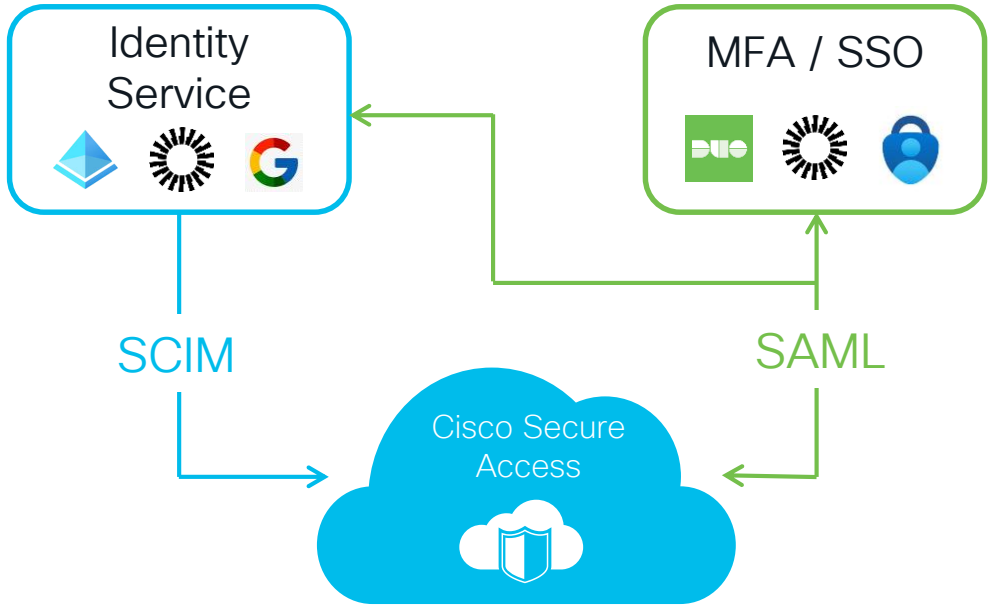
Secure Access integrates with Identity services such as Active Directory, Entra Id, G Suite, Okta, other SCIM IdP

After integration, identities become part of **Users and Groups** and can assign policy based on user or group



Using Identity for Polices with Secure Access

- SCIM provides identity info to Secure Access from Id Service to create identity-based policy
- SAML provides authentication process which can use MFA or directly to Id Service



Reference

Setting Secure Access Policy for SAML

Supports SAML 2.0 POST profiles

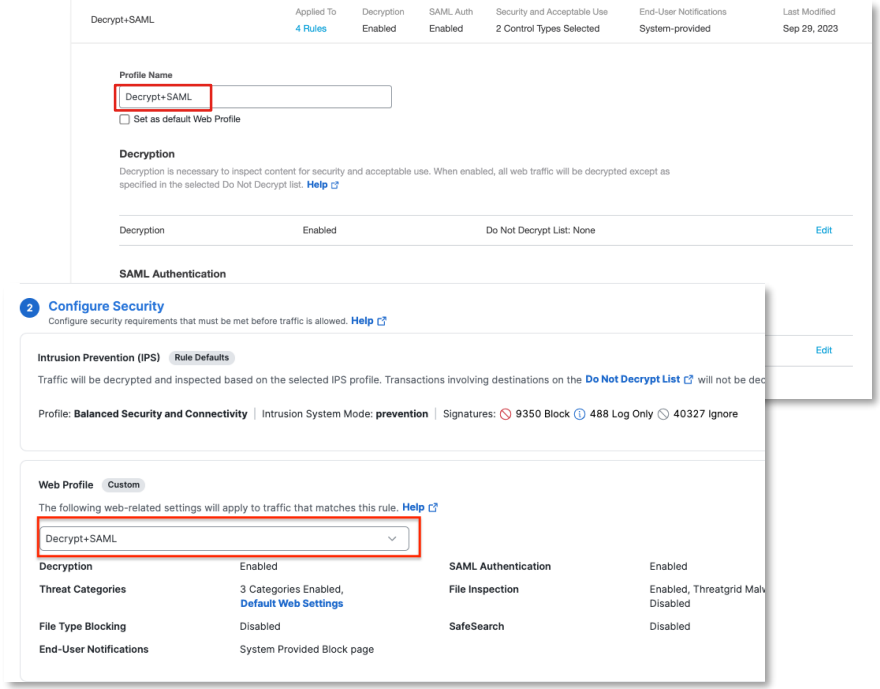
Integrate Secure Access (the SP) with an IdP
Out of scope for today, but documentation on several SAML integrations is here:
https://docs.sse.cisco.com/sse-user-guide/docs/manage-users-and-groups

Web Profile must have SAML Enabled and Decryption Enabled

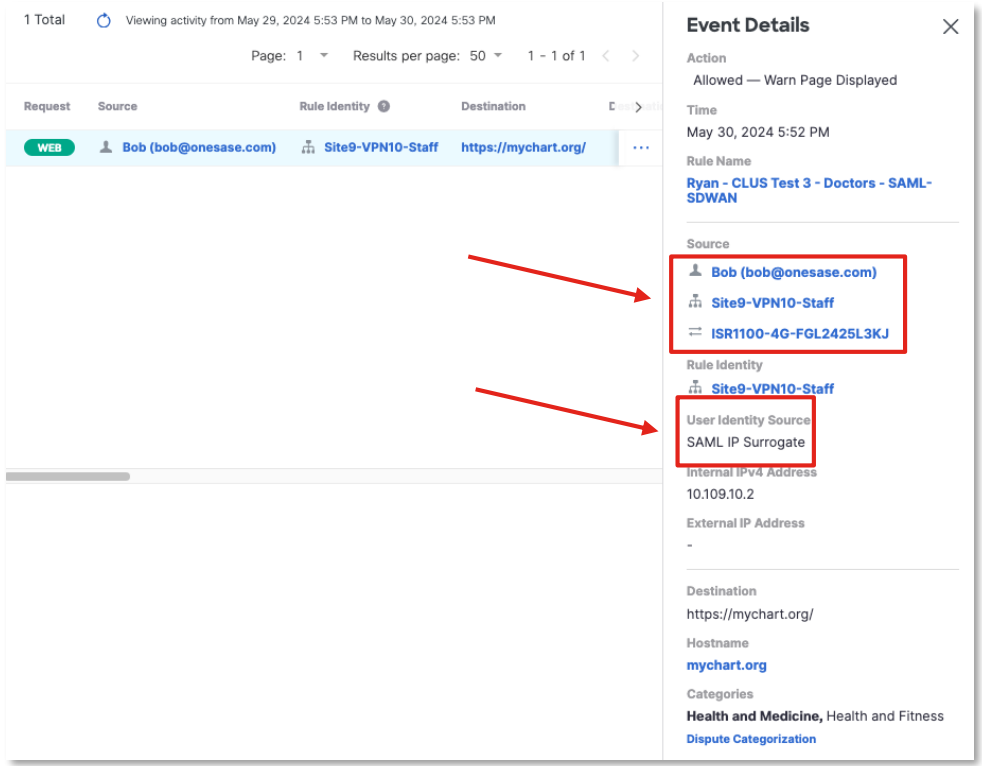
Set the Web Profile on an Access Policy that includes Network Tunnel from which user traffic arrives

After Web Policy matches on Network Tunnel, the SAML challenge will be initiated

Access Policy will be re-evaluated, but now include user and group identities

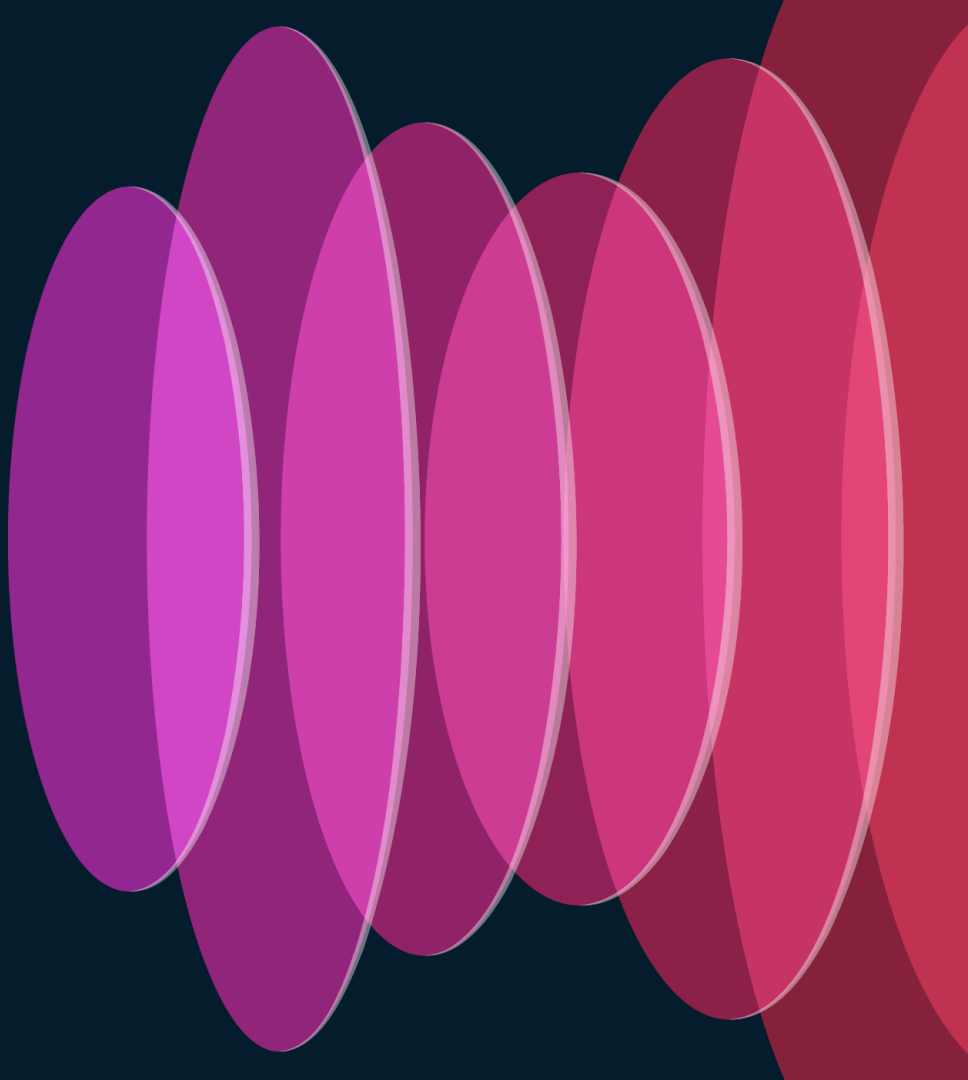


Group Specific Web Policy at Work



Web policy specifically applied to traffic from Entra group **Doctors** sourced from **VPN10-Staff** coming through SD-WAN tunnel

New Policy Source Methods

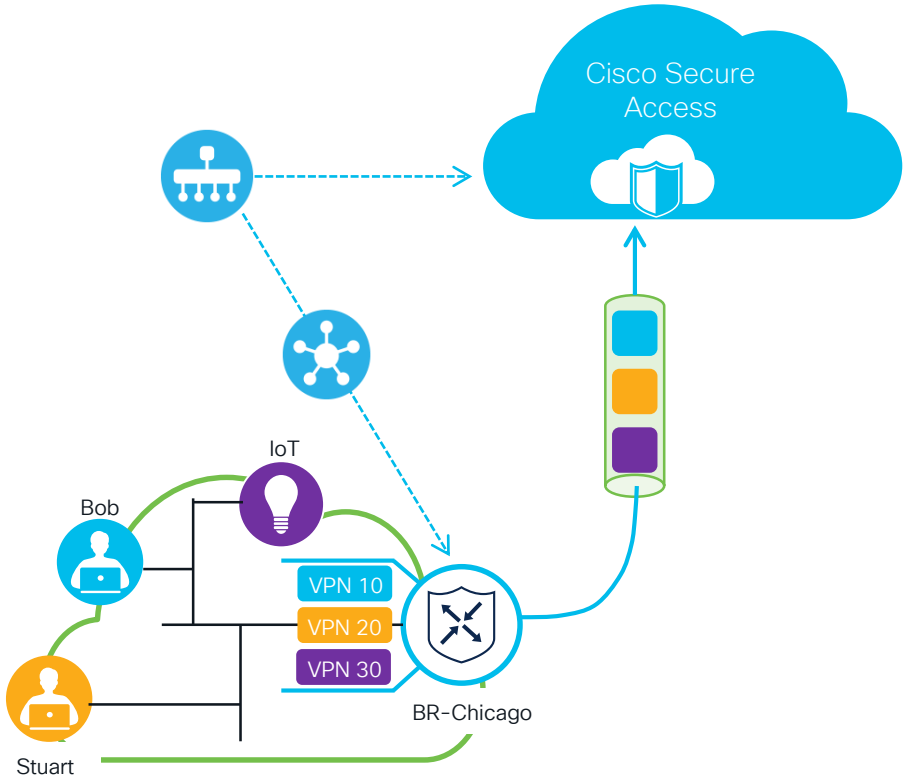


Setting Security Policy for Branch Users

Coming with SD-WAN Release 20.15 / 17.15

Extend VPN/VRF segmentation to Secure Access

- Enables differentiated internet access policies
- VPN separation at Edge Device either physical interface or sub-interface
- WAN interface propagates VPN-ID to Secure Access
- Catalyst SD-WAN Manager provides list of VPN-IDs for creating policy

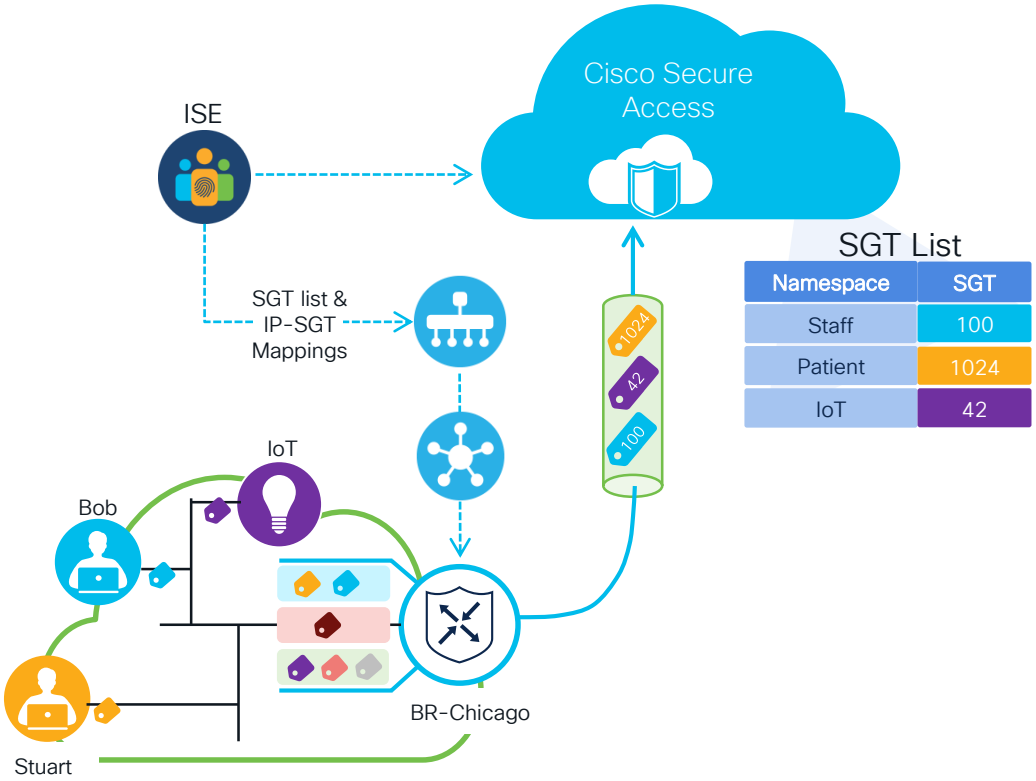


Adding Micro-Segmentation to Secure Access

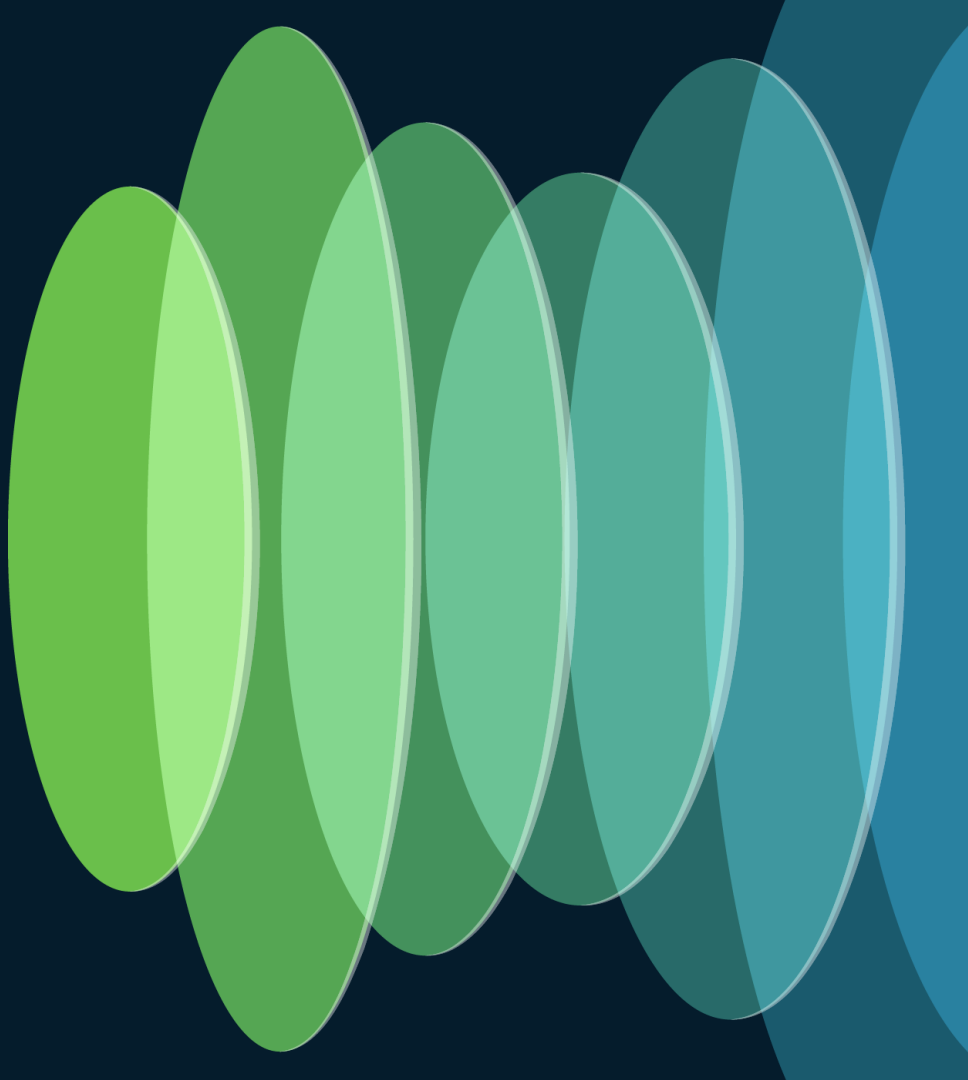
Coming with SD-WAN Release 20.15 / 17.15

Extend SGT segmentation to Secure Access

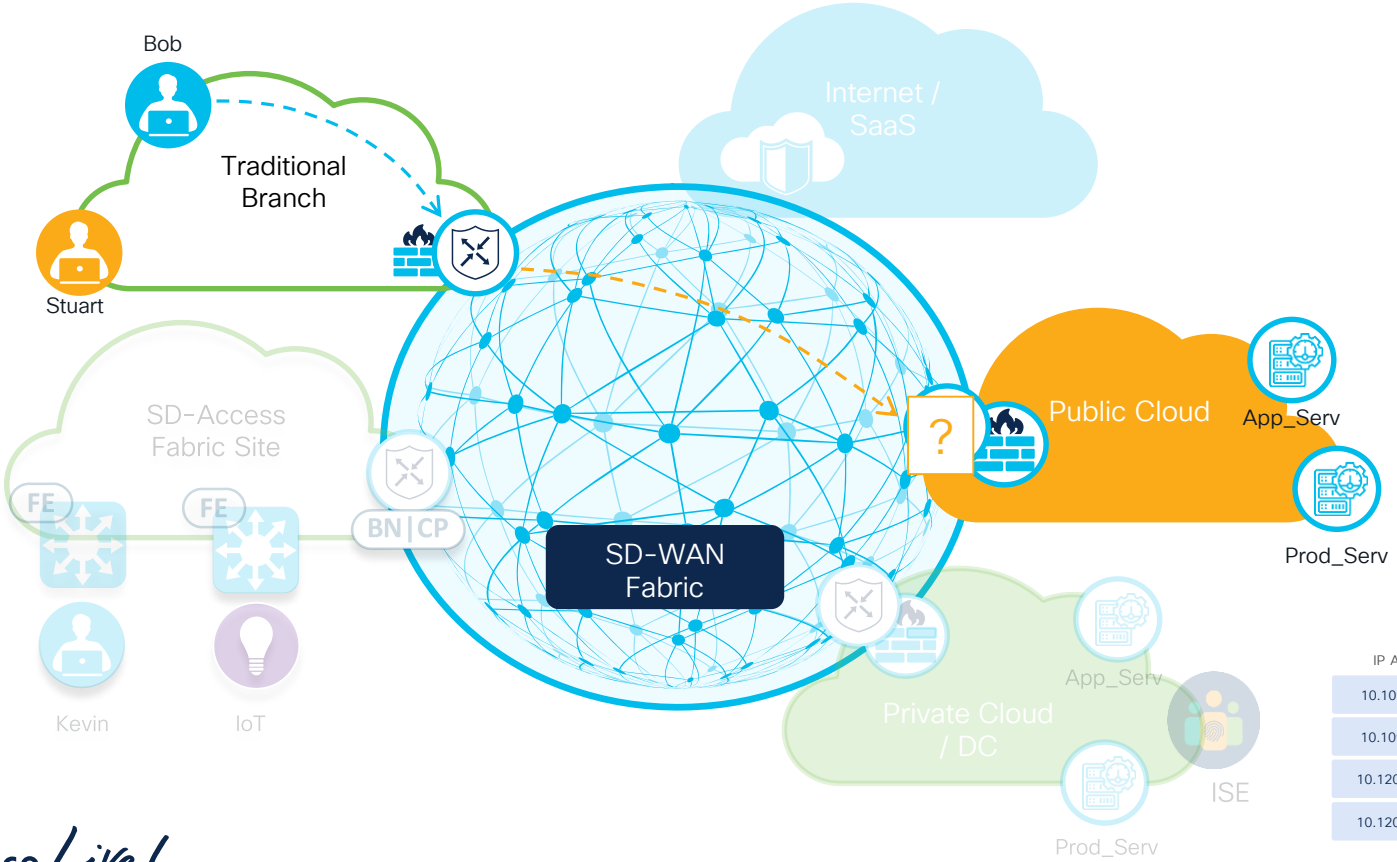
- Enables finer-grained internet access policies
- Apply separate SSE policies for VPN-ID / SGT across same IPSec tunnel
- ISE provides SGT list and mapping of IP-SGTs
- WAN interface propagates VPN-ID and SGT to Secure Access



Segment Cloud Workloads in CSPs



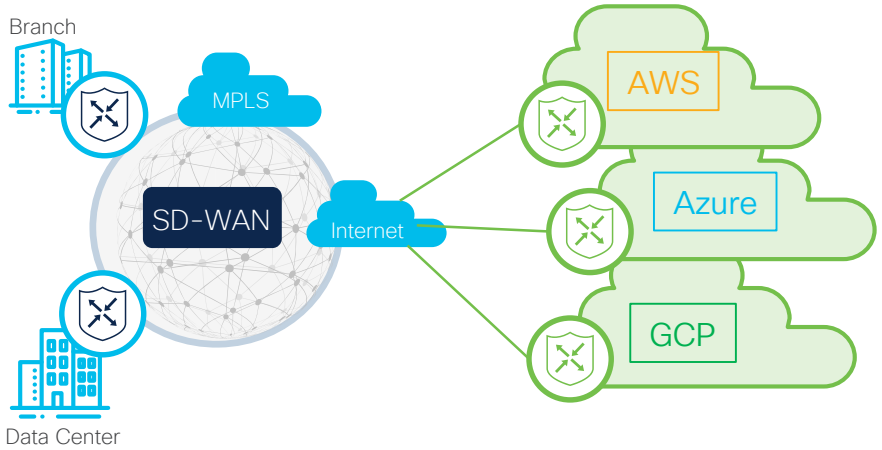
Dr. Bob Needs to Access Workload in CSP



IP Addr	User/Profile	VRF/VPN
10.109.10.50	Bob	Staff
10.109.30.50	Stuart	Patient
10.120.10.101	Kevin	Staff
10.120.40.101	Light	IoT

Automate SD-WAN Extensions into Public Clouds

Cloud OnRamp for Multicloud

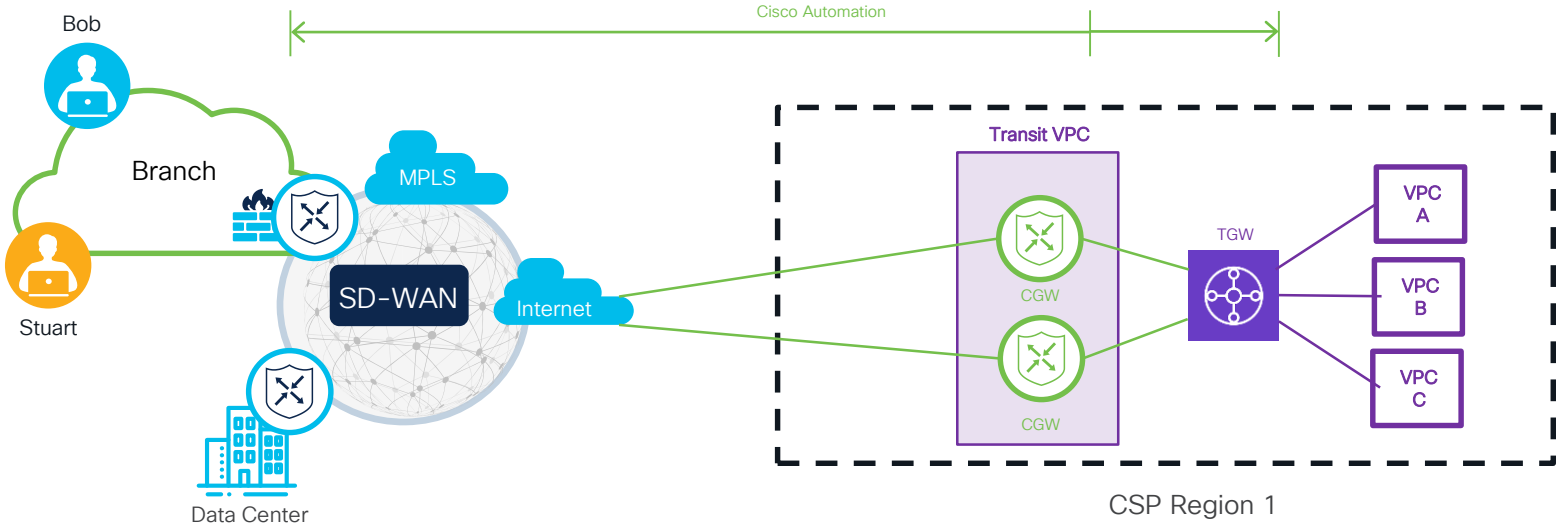


Benefits

- Automate SD-WAN fabric into CSPs
- Extend policy framework into cloud
- Unify control plane for dynamic routing
- Simplify operations with one management plane
- Enhance visibility for devices and circuits
- Integrate multiple cloud providers

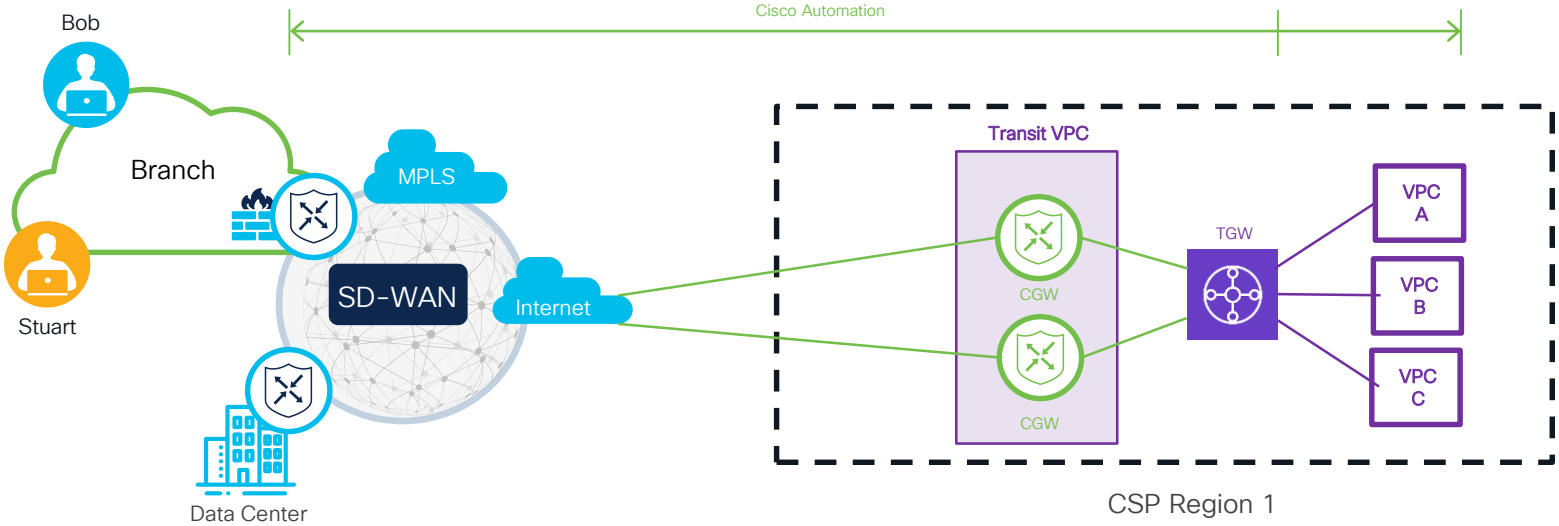
CSP Connection – Cloud GW

Automating AWS Transit GW Integration



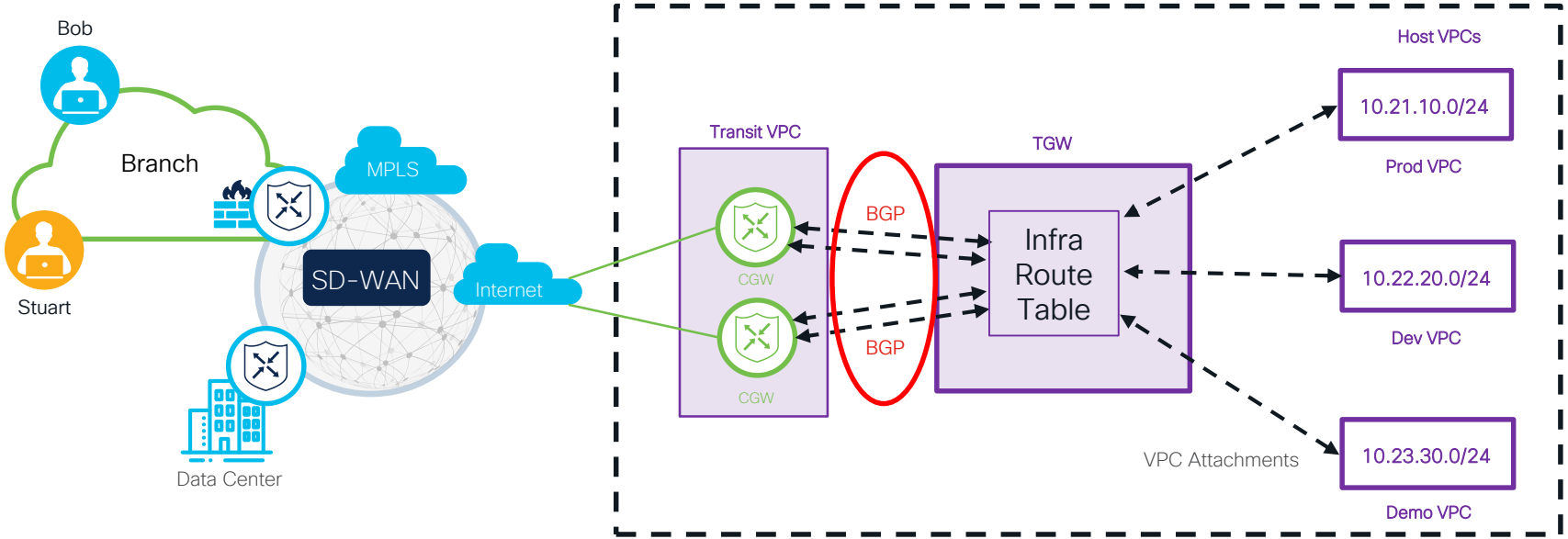
CSP Connection – Cloud GW

Automating AWS Transit GW Integration



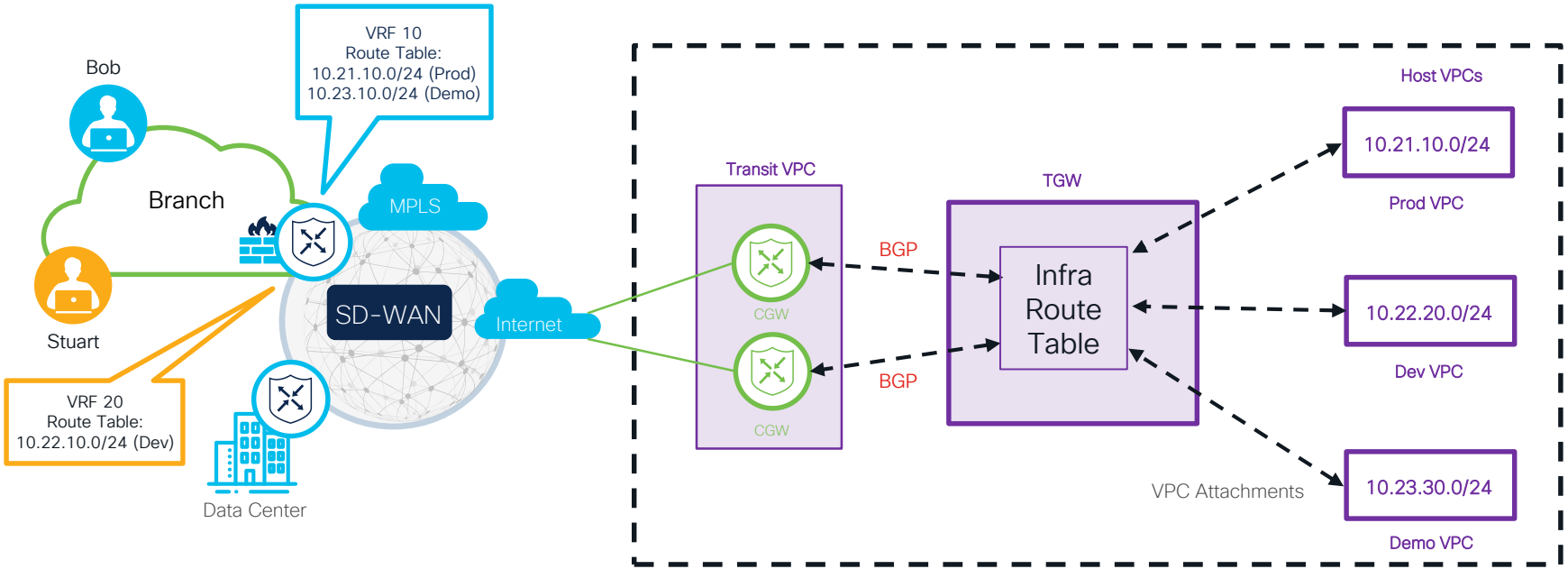
CSP Connection Example – Cloud GW

Dynamic Routing to Host VPCs



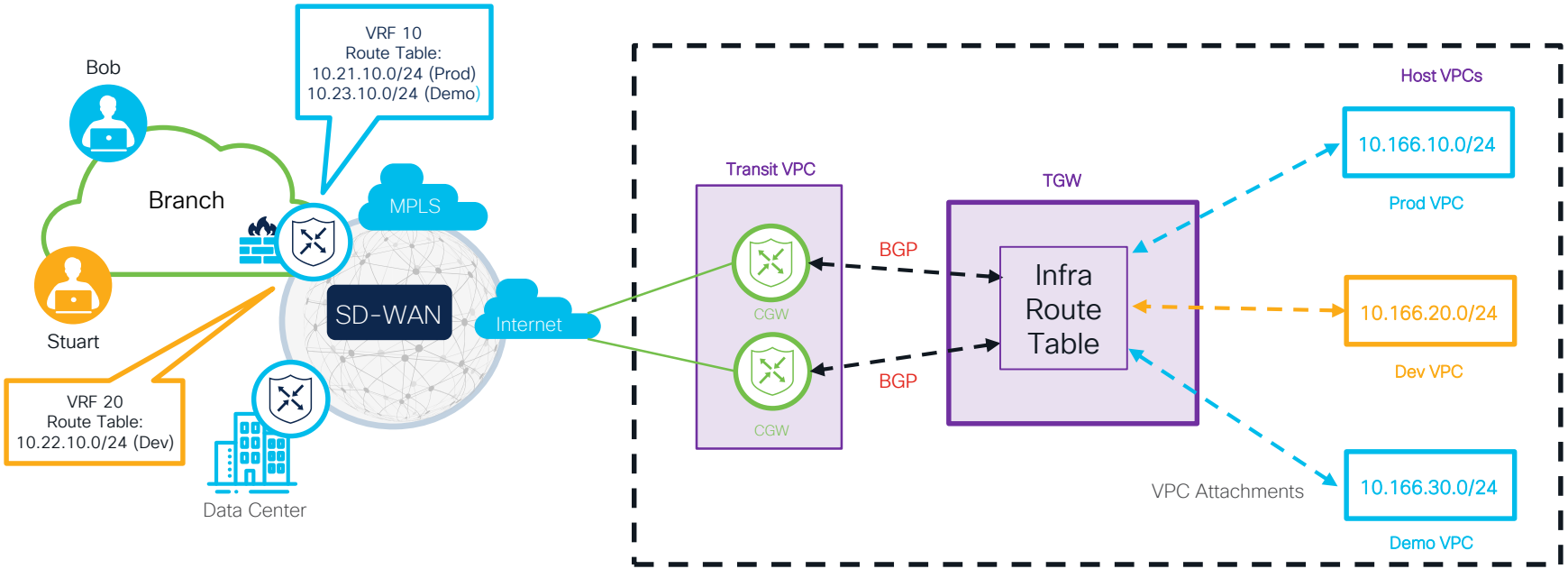
CSP Connection Example – Cloud GW

Segmenting Host VPCs to VPNs



CSP Connection Example – Cloud GW

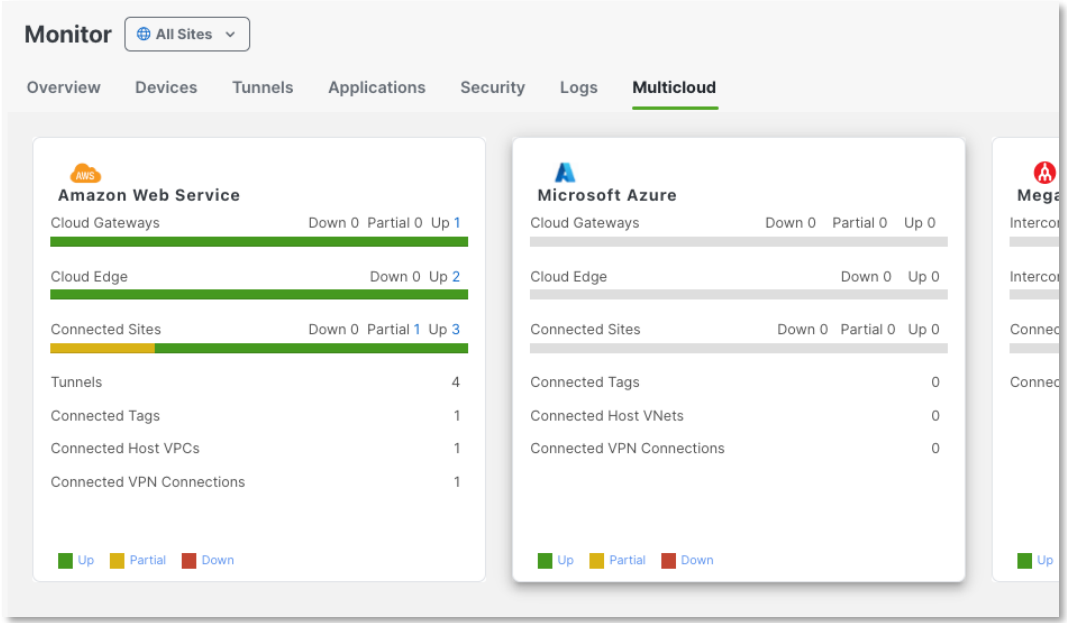
VPC Segmentation through Automation



Extend Segmentation into Cloud Service Providers (CSPs)

Cloud OnRamp for Multicloud*

1. Launch Cloud OnRamp for Multicloud
2. Complete pre-deployment steps (per CSP)
   - A. Associate cloud provider account
   - B. Complete cloud global settings
   - C. Discover host private networks
   - D. Deploy CGW staging template to Catalyst 8000v router(s)
3. Create Cloud Gateway
4. Edit Intent to automatically map VPNs to VPCs/VNETs



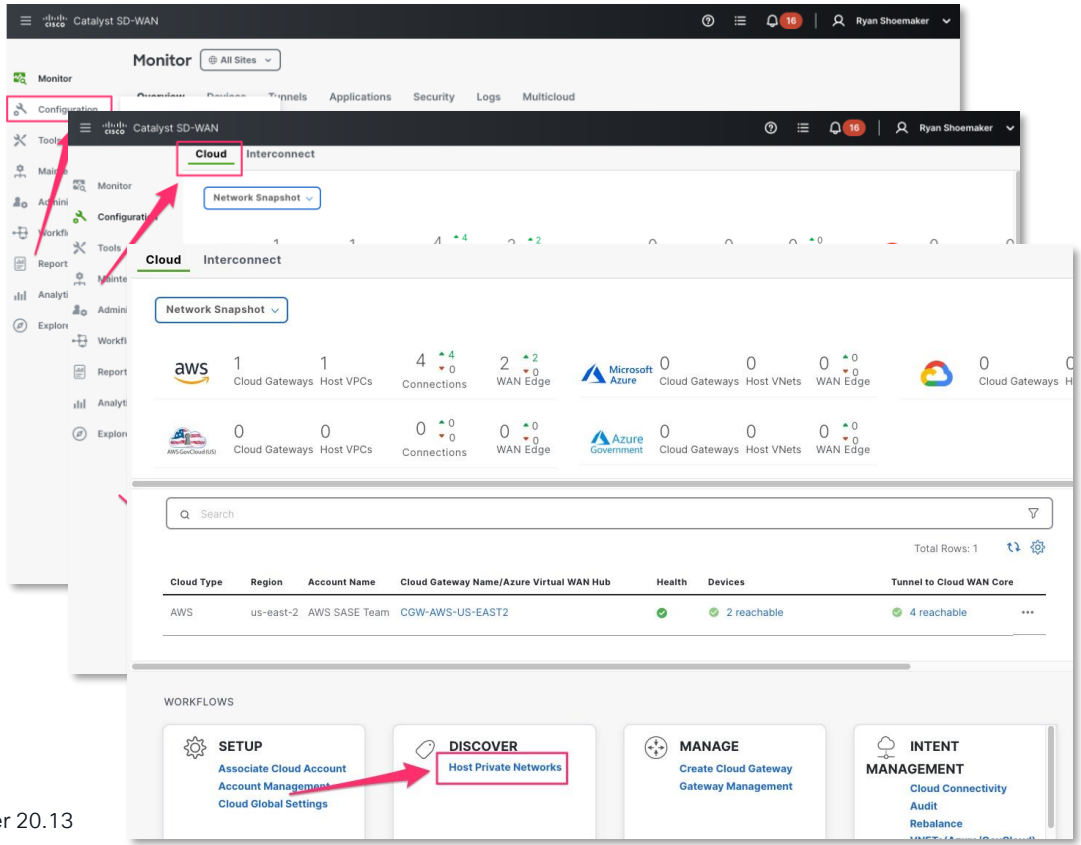
*Screenshots are of Catalyst SD-WAN Manager 20.13

Reference

Automating Cloud Extensions in SD-WAN

Cloud OnRamp for Multicloud*

1. Select Cloud OnRamp for Multicloud
2. Complete pre-deployment steps (per CSP)
   - A. Associate cloud provider account
   - B. Complete cloud global settings
   - C. Discover host private networks

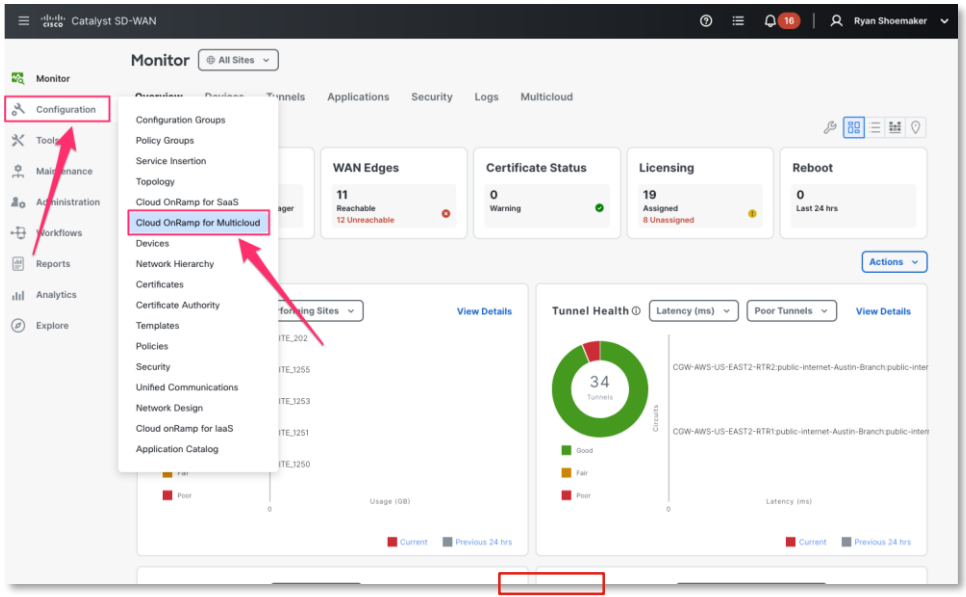


*Screenshots are of Catalyst SD-WAN Manager 20.13

Automating Cloud Extensions in SD-WAN

Cloud OnRamp for Multicloud*

1. Select Cloud OnRamp for Multicloud

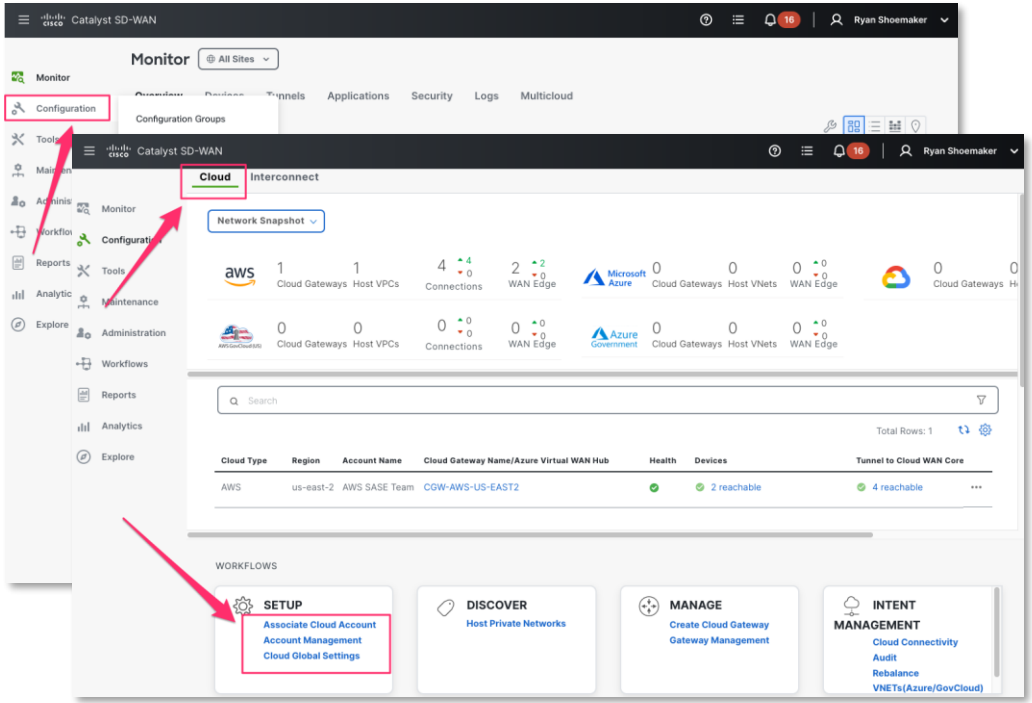


*Screenshots are of Catalyst SD-WAN Manager 20.13

Automating Cloud Extensions in SD-WAN

Cloud OnRamp for Multicloud*

1. Select Cloud OnRamp for Multicloud
2. Complete pre-deployment steps (per CSP)
   A. Associate cloud provider account
   B. Complete Cloud global settings

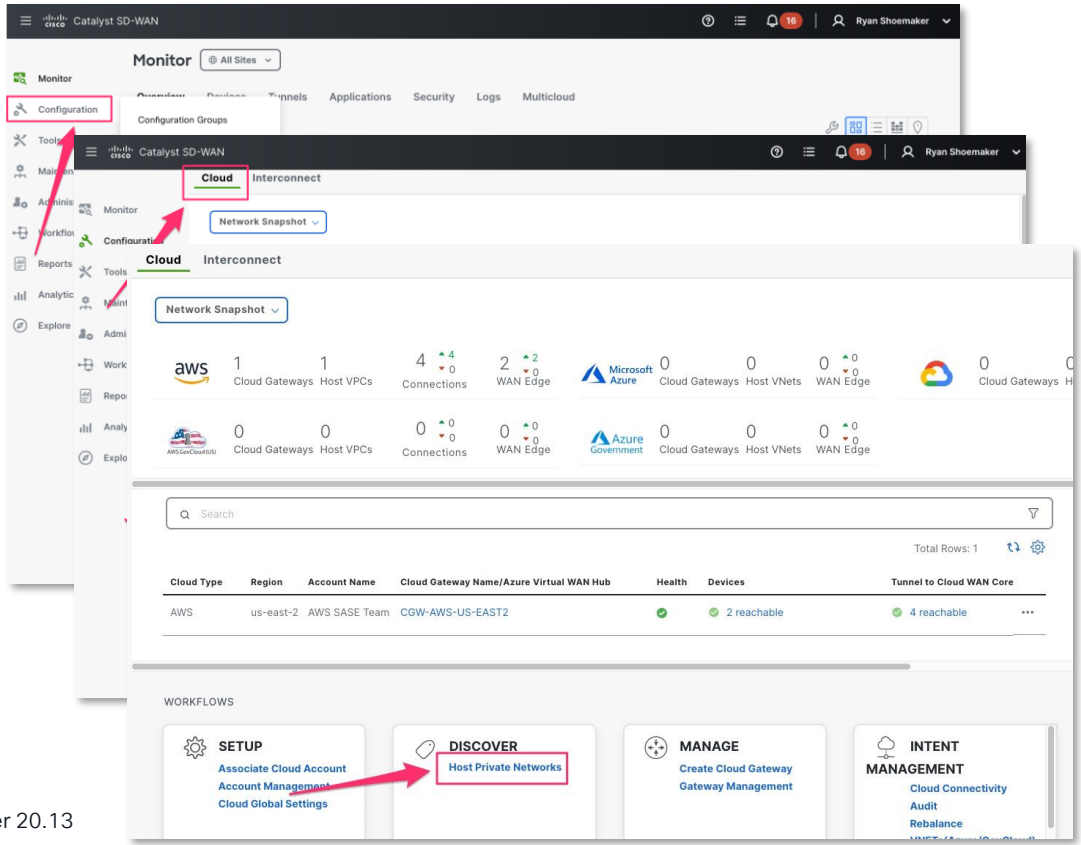


*Screenshots are of Catalyst SD-WAN Manager 20.13

Automating Cloud Extensions in SD-WAN

Cloud OnRamp for Multicloud*

1. Select Cloud OnRamp for Multicloud
2. Complete pre-deployment steps (per CSP)
   - A. Associate cloud provider account
   - B. Complete Cloud global settings
   - C. Discover host private networks



*Screenshots are of Catalyst SD-WAN Manager 20.13

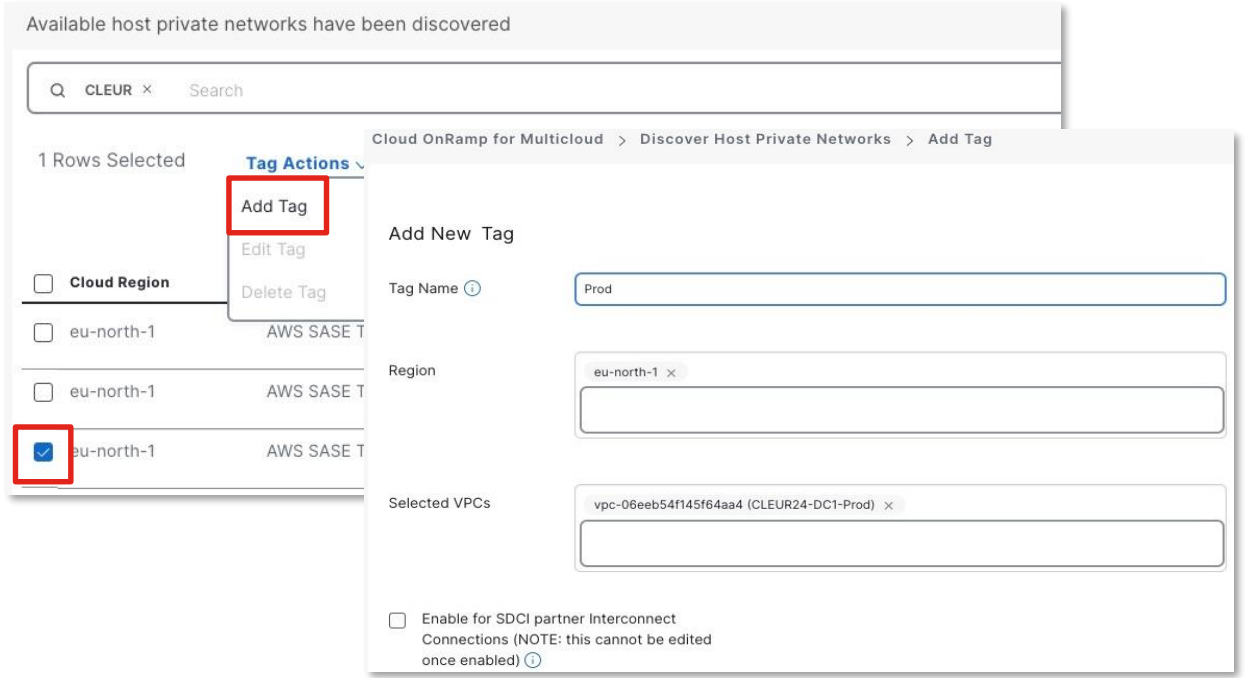
Reference

Automating Cloud Extensions in SD-WAN

Discover Host Private Networks

**Only Tagged VPCs will be available to map to SD-WAN VRFs*

1. Select VPC for Mapping
2. Add Tag
   A. Name
   B. Select Region
   C. Select VPC

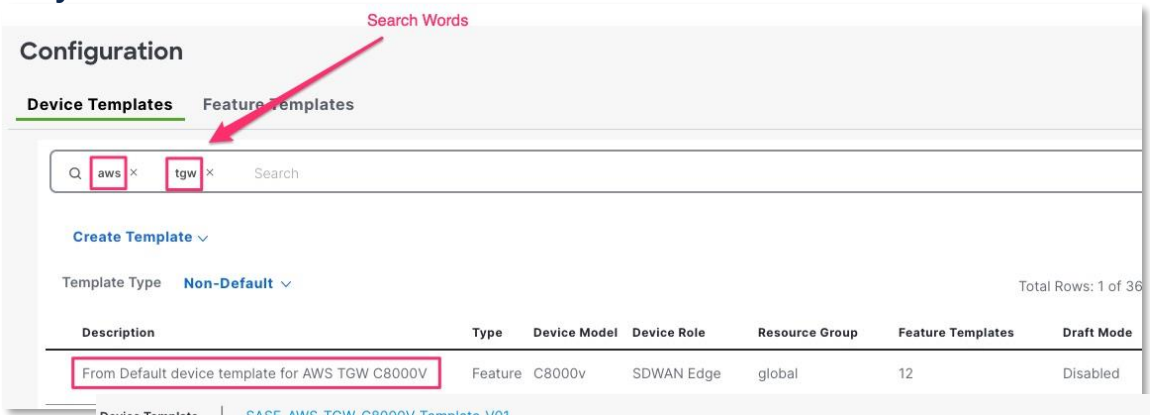


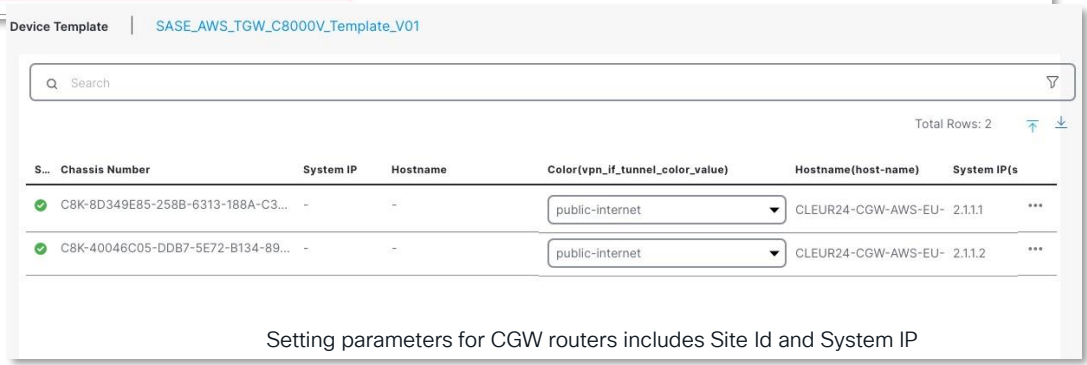
Reference

Automating Cloud Extensions in SD-WAN

Stage C8Kvs for Cloud Gateway

1. Select Cloud OnRamp for Multicloud
2. Complete pre-deployment steps (per CSP)
   - A. Associate cloud provider account
   - B. Complete Cloud global settings
   - C. Discover host private networks
   - D. Deploy CGW staging template to Catalyst 8000v router(s)





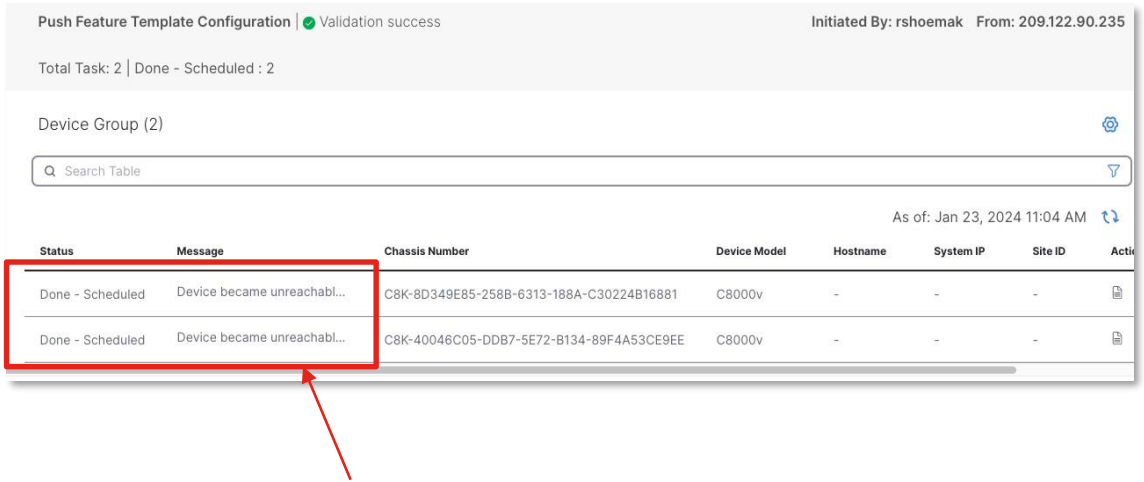
Setting parameters for CGW routers includes Site Id and System IP

Reference

Automating Cloud Extensions in SD-WAN

Stage C8Kvs for Cloud Gateway

1. Select Cloud OnRamp for Multicloud
2. Complete pre-deployment steps (per CSP)
   - A. Associate cloud provider account
   - B. Complete Cloud global settings
   - C. Discover host private networks
   - D. Deploy CGW staging template to Catalyst 8000v router(s)



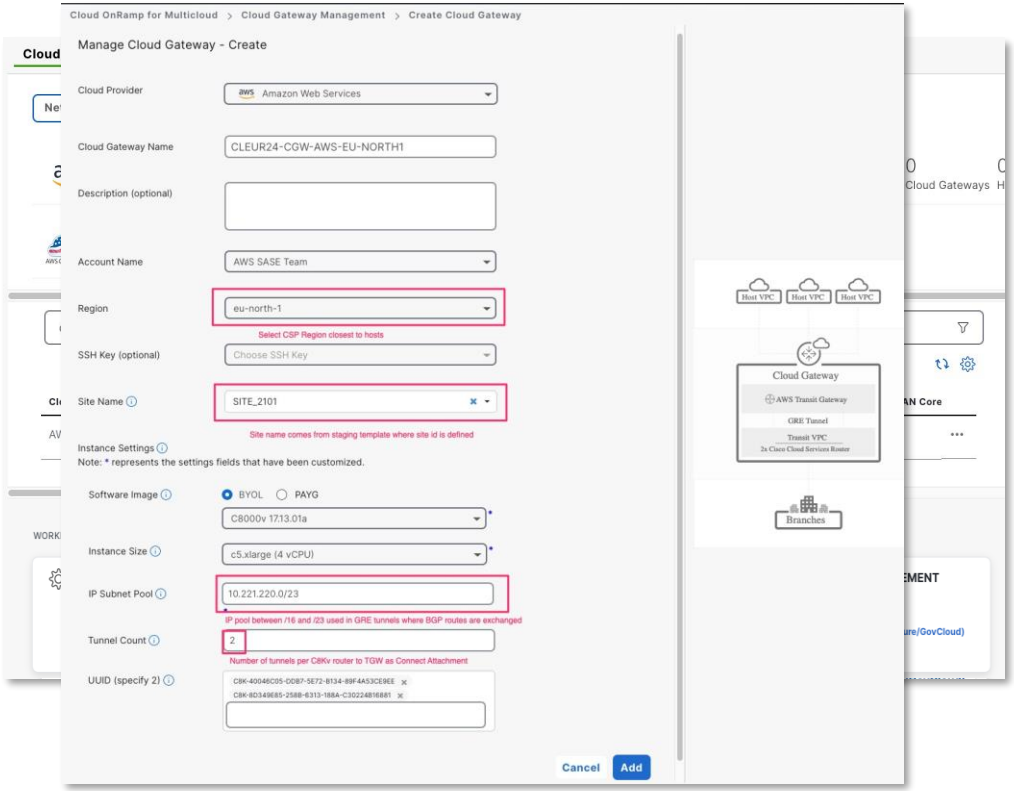
After applying staging template, device becomes unreachable

Reference

Automating Cloud Extensions in SD-WAN

Create Cloud Gateway

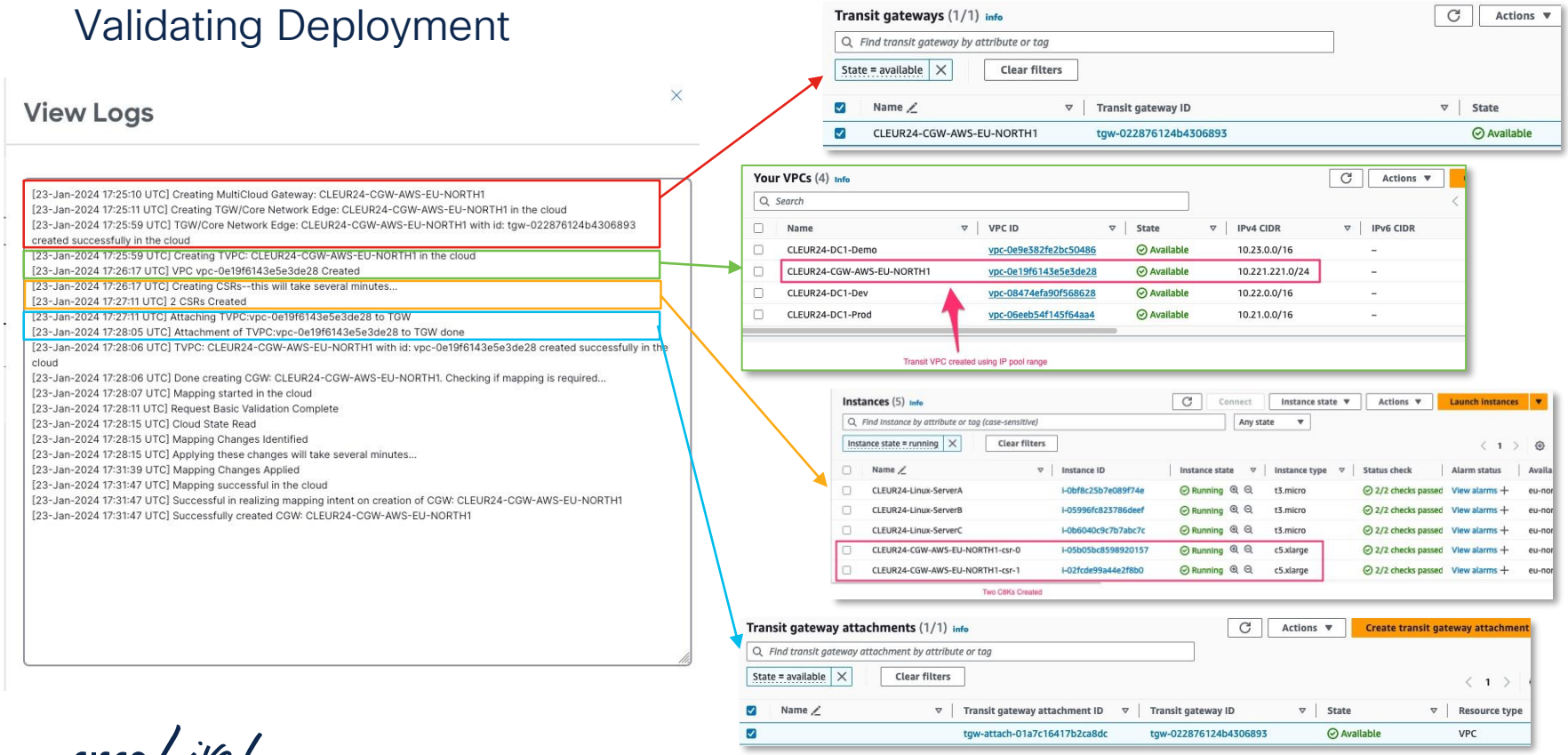
1. Select Cloud OnRamp for Multicloud
2. Complete pre-deployment steps (per CSP)
   - A. Associate cloud provider account
   - B. Complete Cloud global settings
   - C. Discover host private networks
   - D. Deploy CGW staging template to Catalyst 8000v router(s)
3. Create Cloud Gateway (creates transit hub/VPC, transit GW, deploys cloud service routers, creates GW attachment, and creates subnets)



Reference

Automating Cloud Extensions in SD-WAN

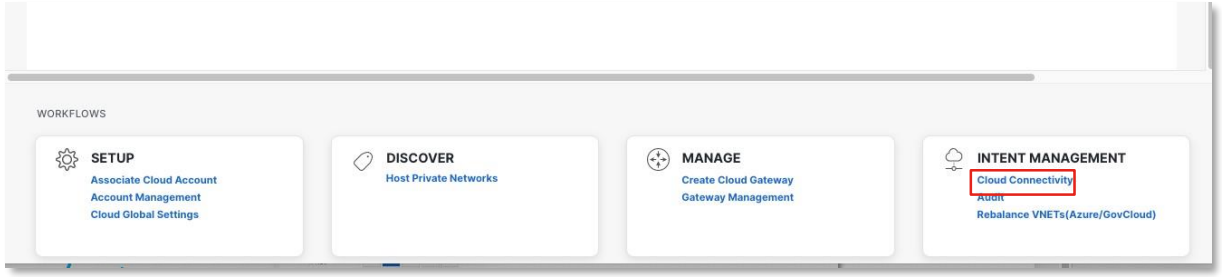
Validating Deployment

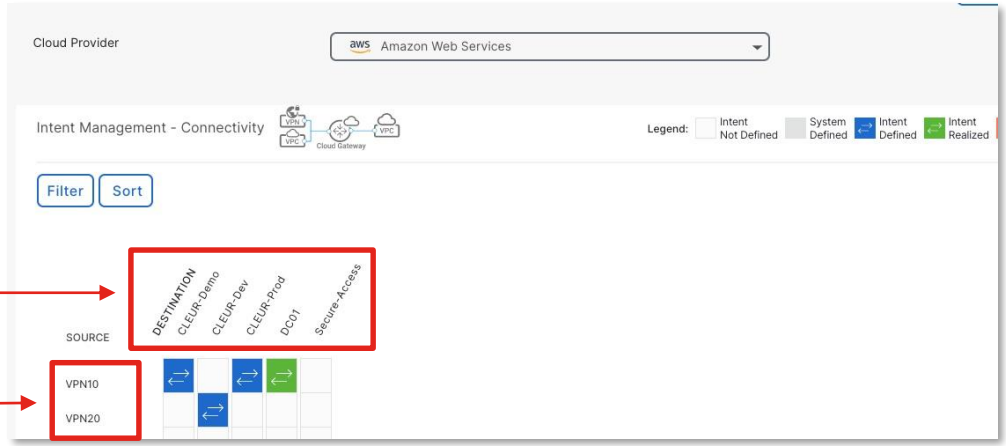


Automating Cloud Extensions in SD-WAN

Managing Intent

1. Select Cloud OnRamp for Multicloud
2. Select **Cloud Connectivity**
3. Edit Intent to automatically map VPNs to VPCs/VNETs





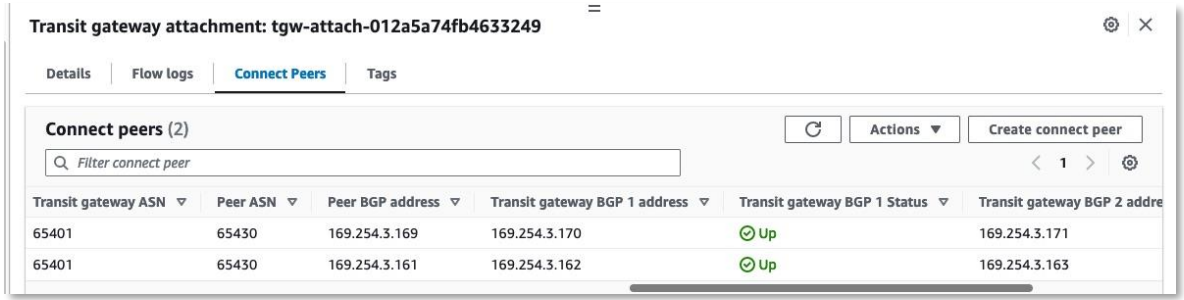
VPC

VRF/VPN

Automating Cloud Extensions in SD-WAN

Validating Intent

Mapping intent creates Connect Adjacency which established GRE tunnel between C8K router and AWS TGW and BGP adjacency(ies) is formed over this tunnel



AWS – TG Connect Attachment

```
CLEUR24-CGW-AWS-EU-NORTH1-RTR2#show ip bgp vpnv4 vrf 10 summary
BGP router identifier 10.221.221.46, local AS number 65430
BGP table version is 13, main routing table version 13
11 network entries using 2904 bytes of memory
17 path entries using 2312 bytes of memory
2 multipath network entries and 8 multipath paths
6/5 BGP path/bestpath attribute entries using 1872 bytes of memory
3 BGP AS-PATH entries using 88 bytes of memory
3 BGP extended community entries using 88 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 7264 total bytes of memory
BGP activity 12/0 prefixes, 21/0 paths, scan interval 60 secs
12 networks peaked at 20:09:20 Jan 23 2024 UTC (00:20:43.575 ago)

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
169.254.3.162   4        65401     128     133       13    0    0 00:20:43        2
169.254.3.163   4        65401     128     133       13    0    0 00:20:42        2
169.254.3.170   4        65401     127     134       13    0    0 00:20:37        2
169.254.3.171   4        65401     128     133       13    0    0 00:20:44        2
CLEUR24-CGW-AWS-EU-NORTH1-RTR2#
```

C8K – BGP summary in VRF 10

Reference

Automating Cloud Extensions in SD-WAN

Validating Intent

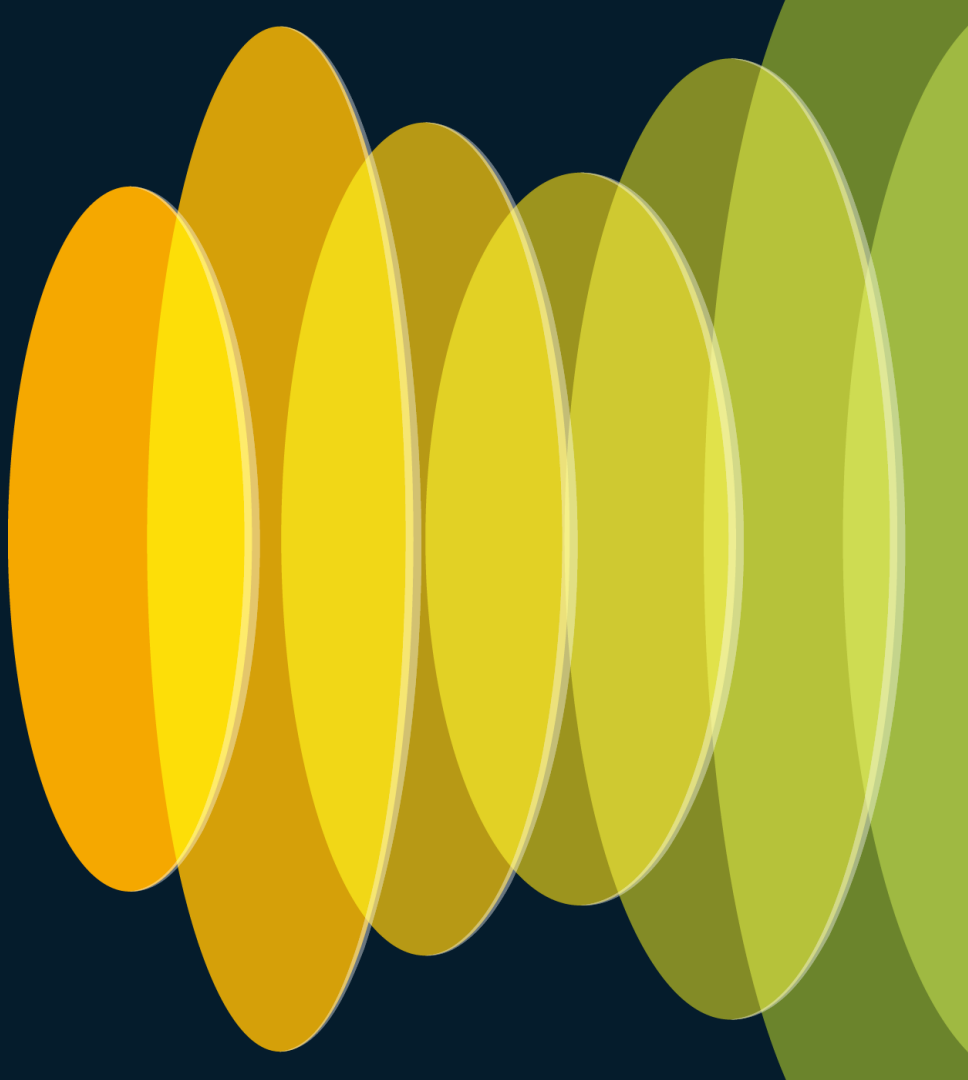
```
CLEUR24-CGW-AWS-EU-NORTH1-RTR2#show ip route vrf 10

Routing Table: 10
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/16 is subnetted, 6 subnets
m        10.10.0.0 [251/0] via 1.1.97.2, 00:24:40, Sdwan-system-intf
                   [251/0] via 1.1.97.1, 00:24:40, Sdwan-system-intf
B        10.21.0.0 [20/100] via 169.254.3.171, 00:24:26
                   [20/100] via 169.254.3.170, 00:24:26
                   [20/100] via 169.254.3.163, 00:24:26
                   [20/100] via 169.254.3.162, 00:24:26
B        10.23.0.0 [20/100] via 169.254.3.171, 00:24:26
                   [20/100] via 169.254.3.170, 00:24:26
                   [20/100] via 169.254.3.163, 00:24:26
```

C8K – VRF 10 Routing Table – Prod and Demo VPCs present

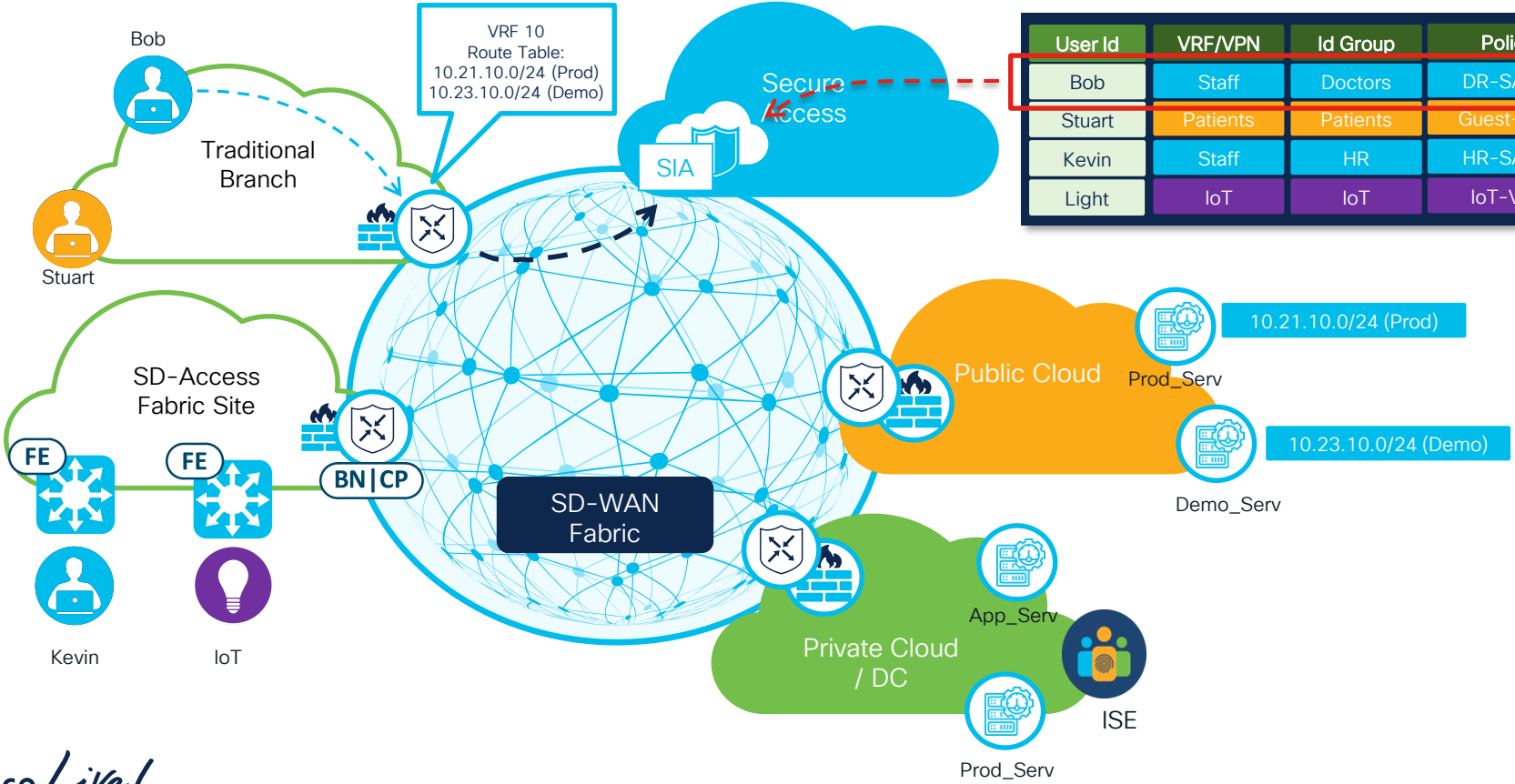
```
CLEUR24-CGW-AWS-EU-NORTH1-RTR2#show ip route vrf 20

Routing Table: 20
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/16 is subnetted, 1 subnets
B        10.22.0.0 [20/100] via 169.254.3.235, 00:25:08
                   [20/100] via 169.254.3.234, 00:25:08
                   [20/100] via 169.254.3.227, 00:25:08
                   [20/100] via 169.254.3.226, 00:25:08
```

C8K – VRF 20 Routing Table – Dev VPC present

Conclusion



Bob has an Internet/SaaS policy as a Doctor and Access to Correct VPCs in the CSP



Conclusion

- Catalyst SD-WAN to Umbrella can differentiate DNS policy based on VRF/VPN
- Catalyst SD-WAN to Secure Access can differentiate SSE policy based on
  - Source device or tunnel
  - Source subnet
  - Source ID group via SAML
  - Source VRF/VPN*
  - Source SGT*
- VPN/VRF segmentation to CSPs integrated and automated with Catalyst SD-WAN

*Coming with 20.15/17.17 SD-WAN Release

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

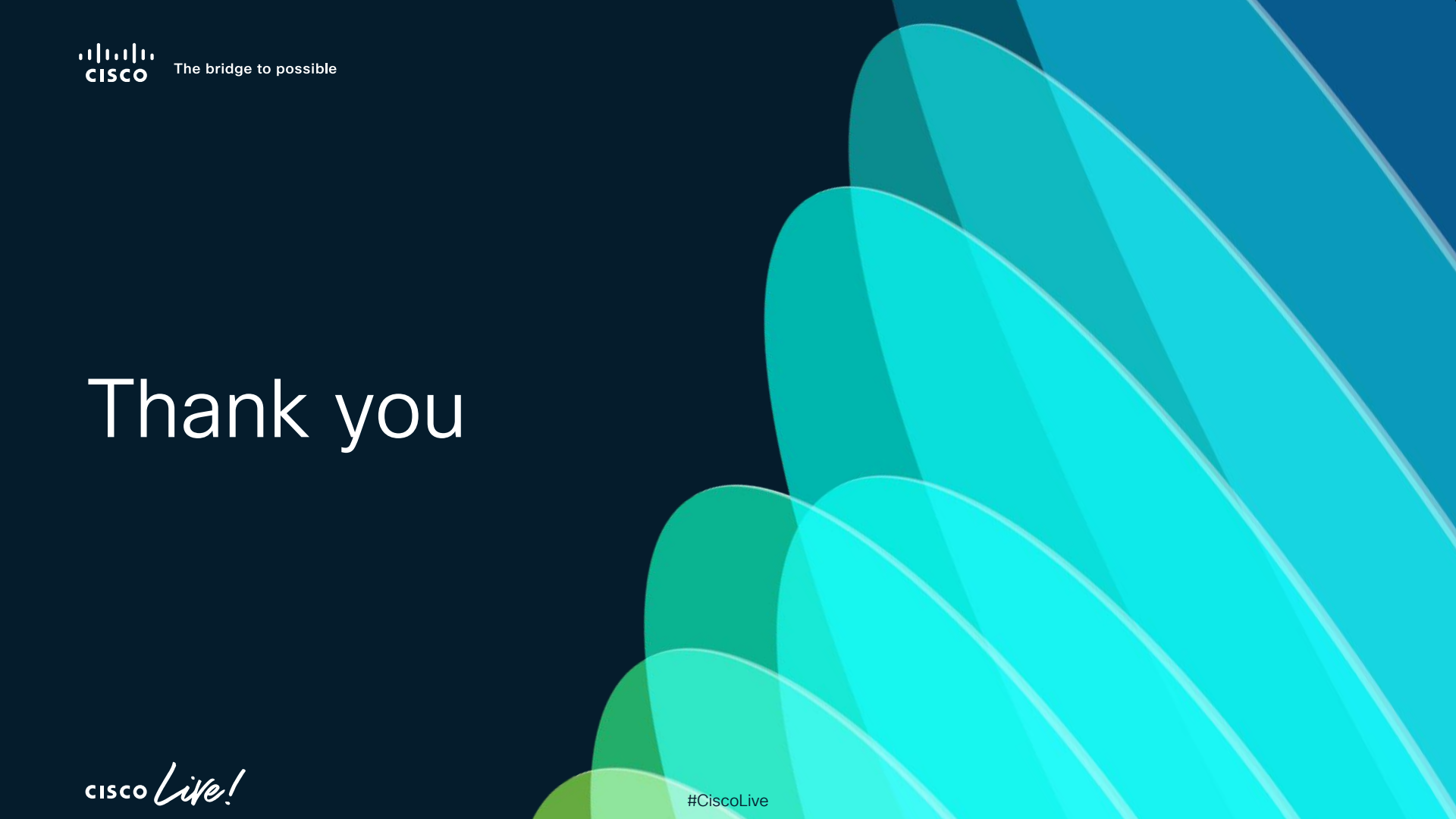
Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

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


The bridge to possible
Thank you
cisco Live!
#CiscoLive