



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!*

#CiscoLive

Cisco Webex App

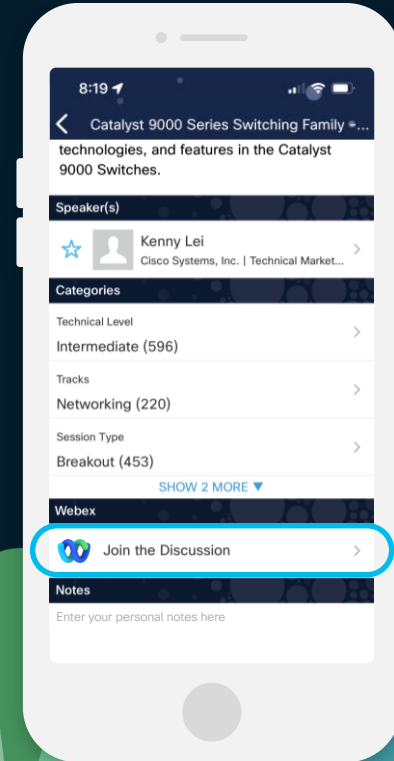
Questions?

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 7, 2024.



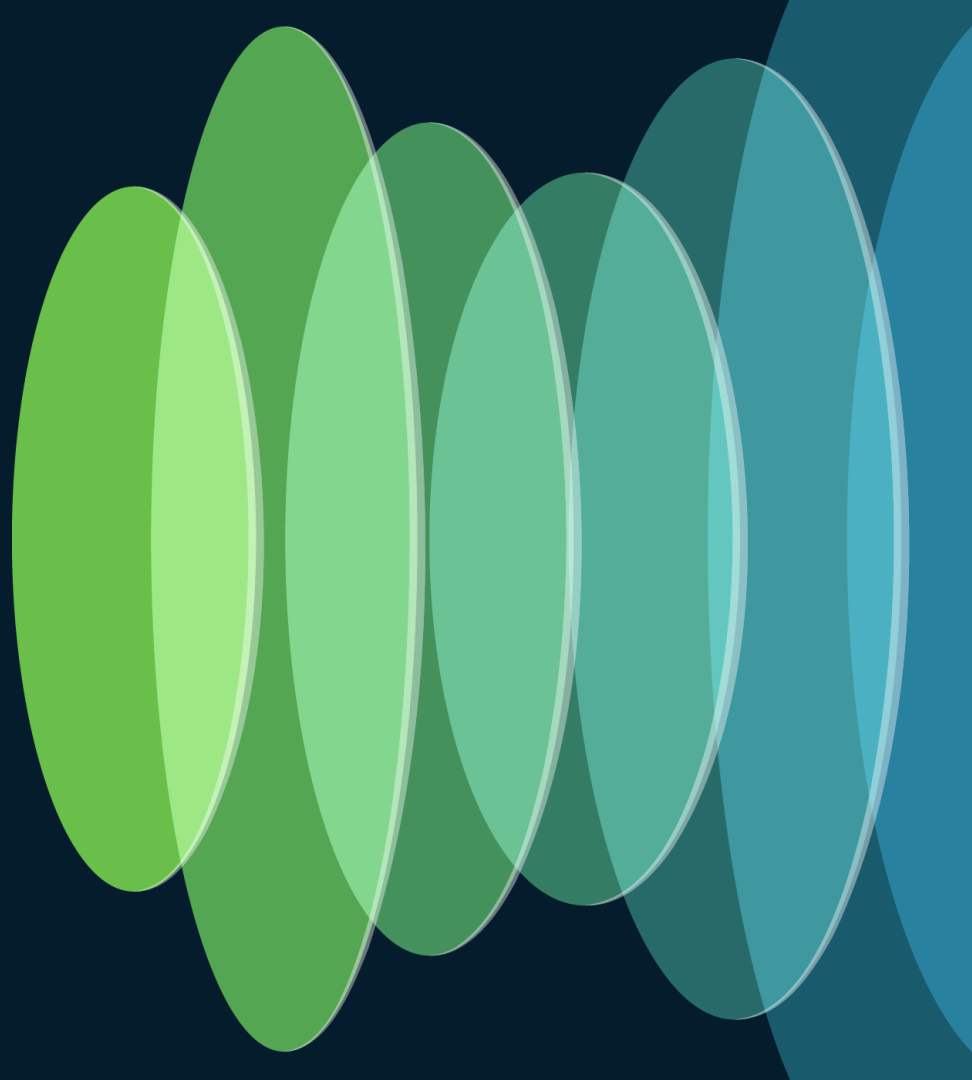
Why This Session

- 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

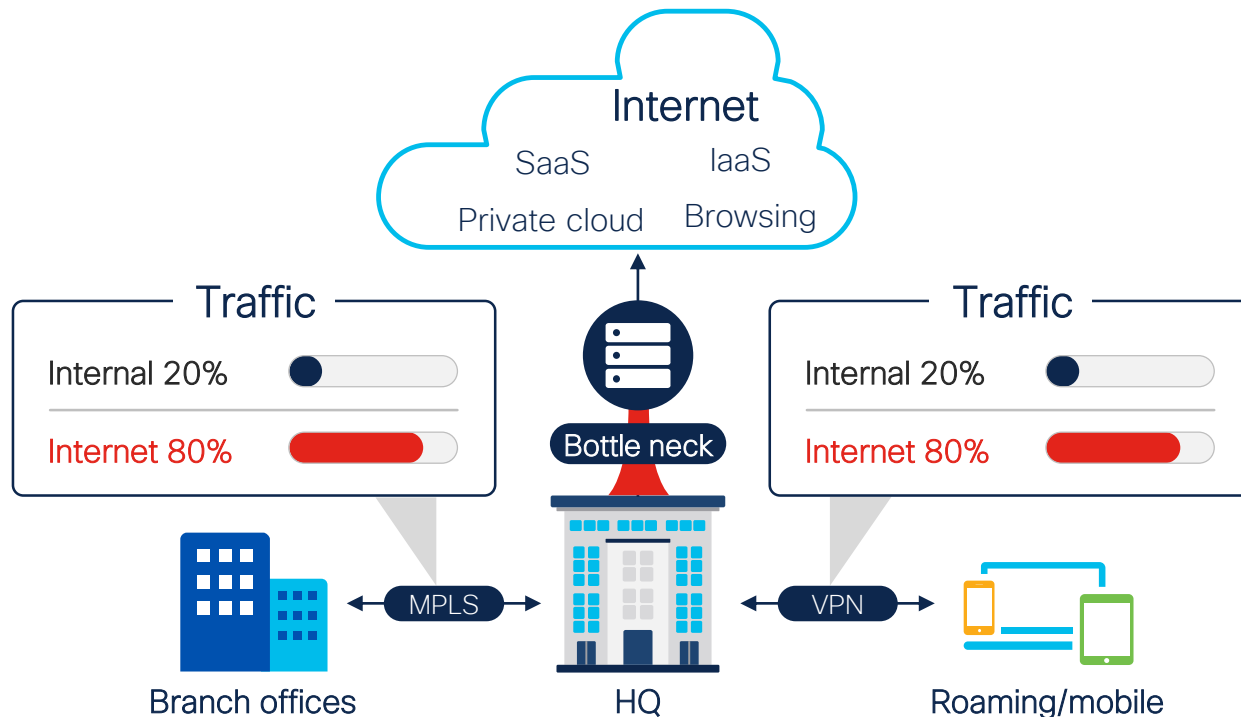


Changes in the types of traffic and destinations

Have inverted the traffic model

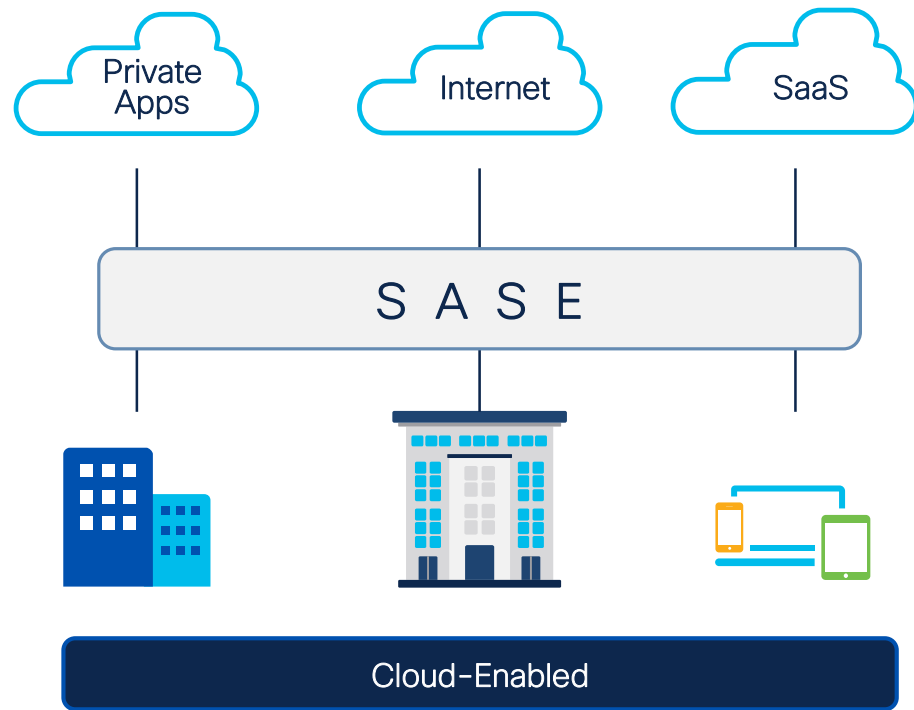
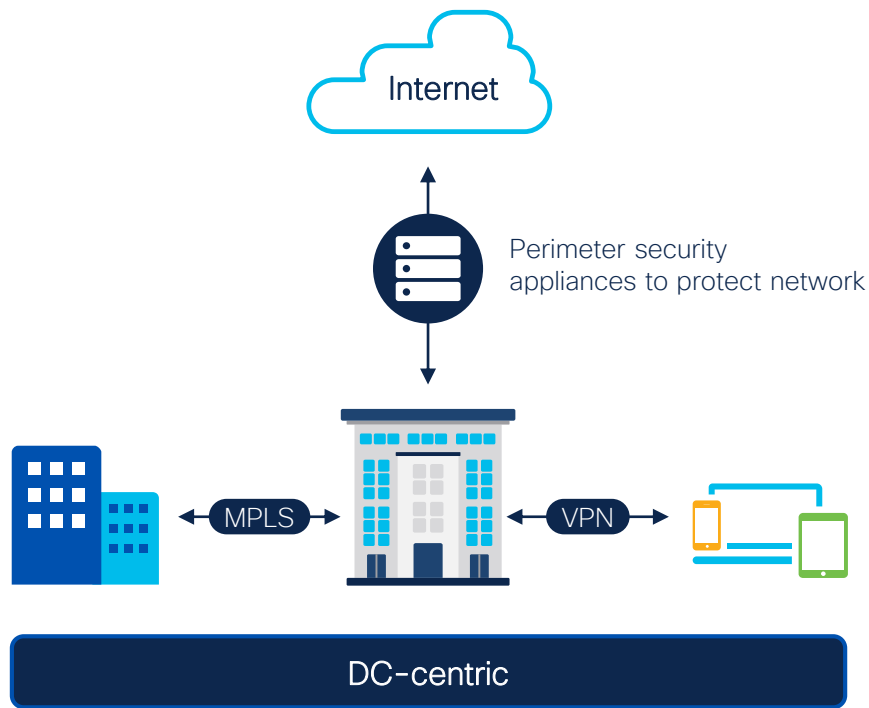
Problems

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

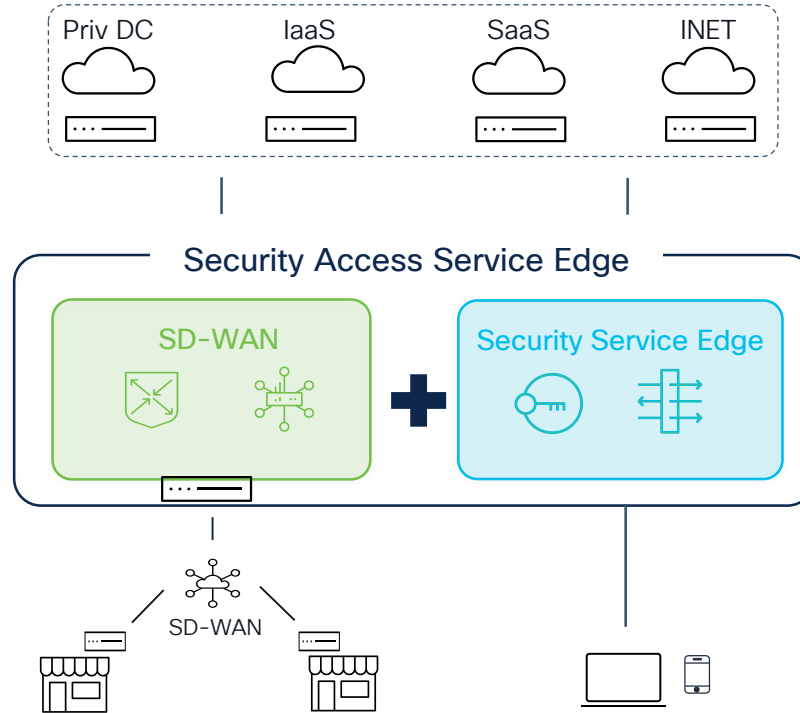


Network transformation

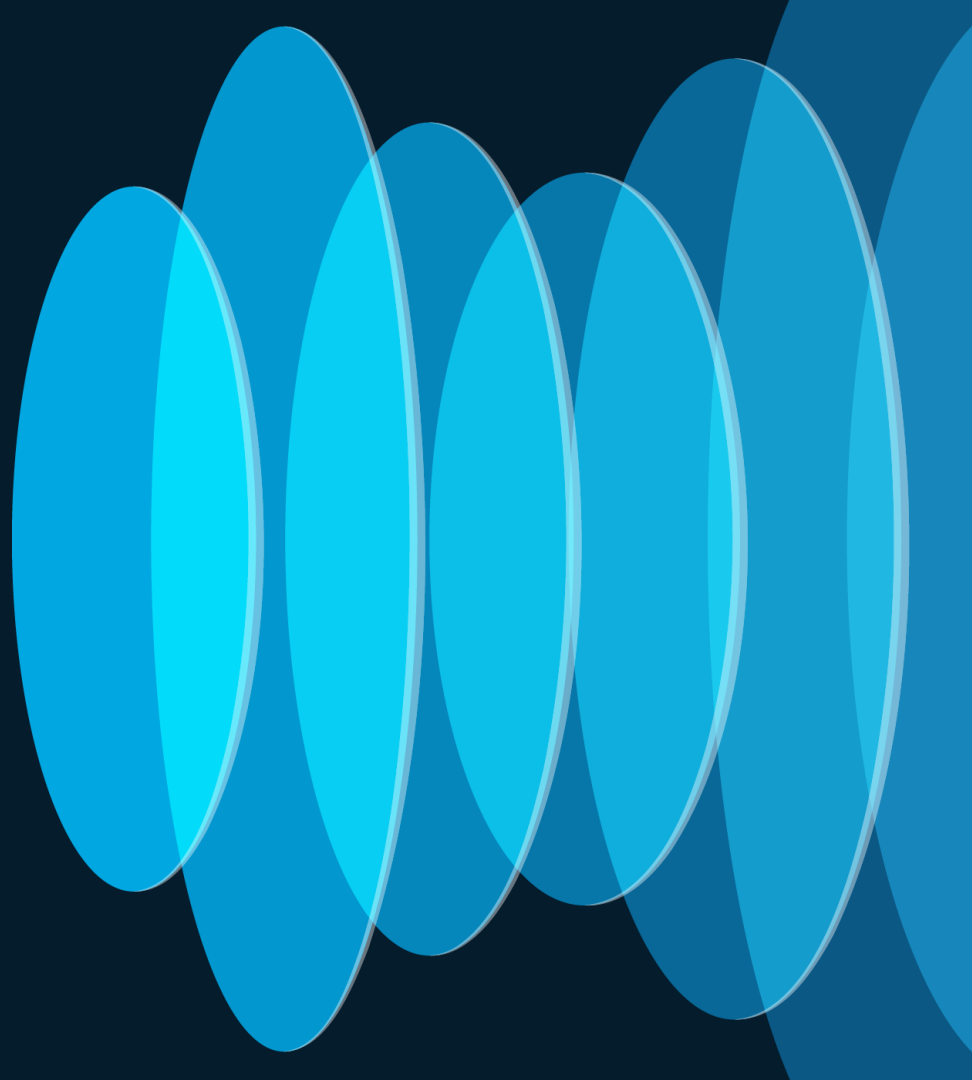
Transition from a DC-centric topology to one that's cloud ready



SASE – Convergence of SD-WAN and SSE



Segmentation



Some Network Segmentation Definitions

As defined by Catalyst SD-WAN

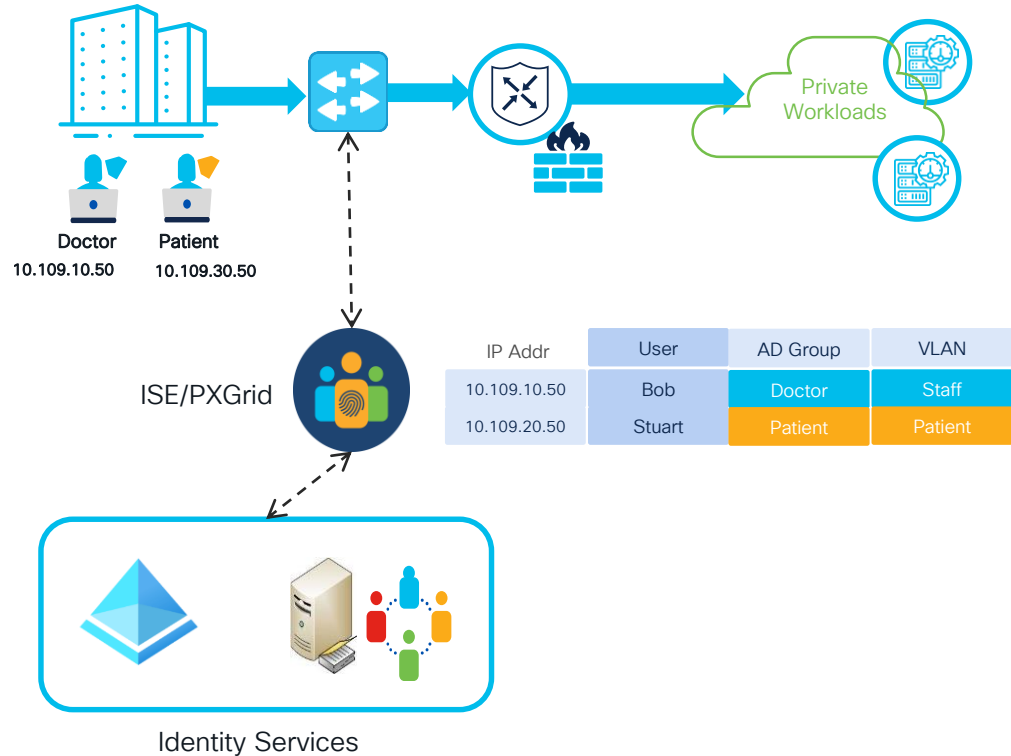
VLAN / Subnet: Separation of broadcast domains where traffic between different VLANS must traverse a router

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

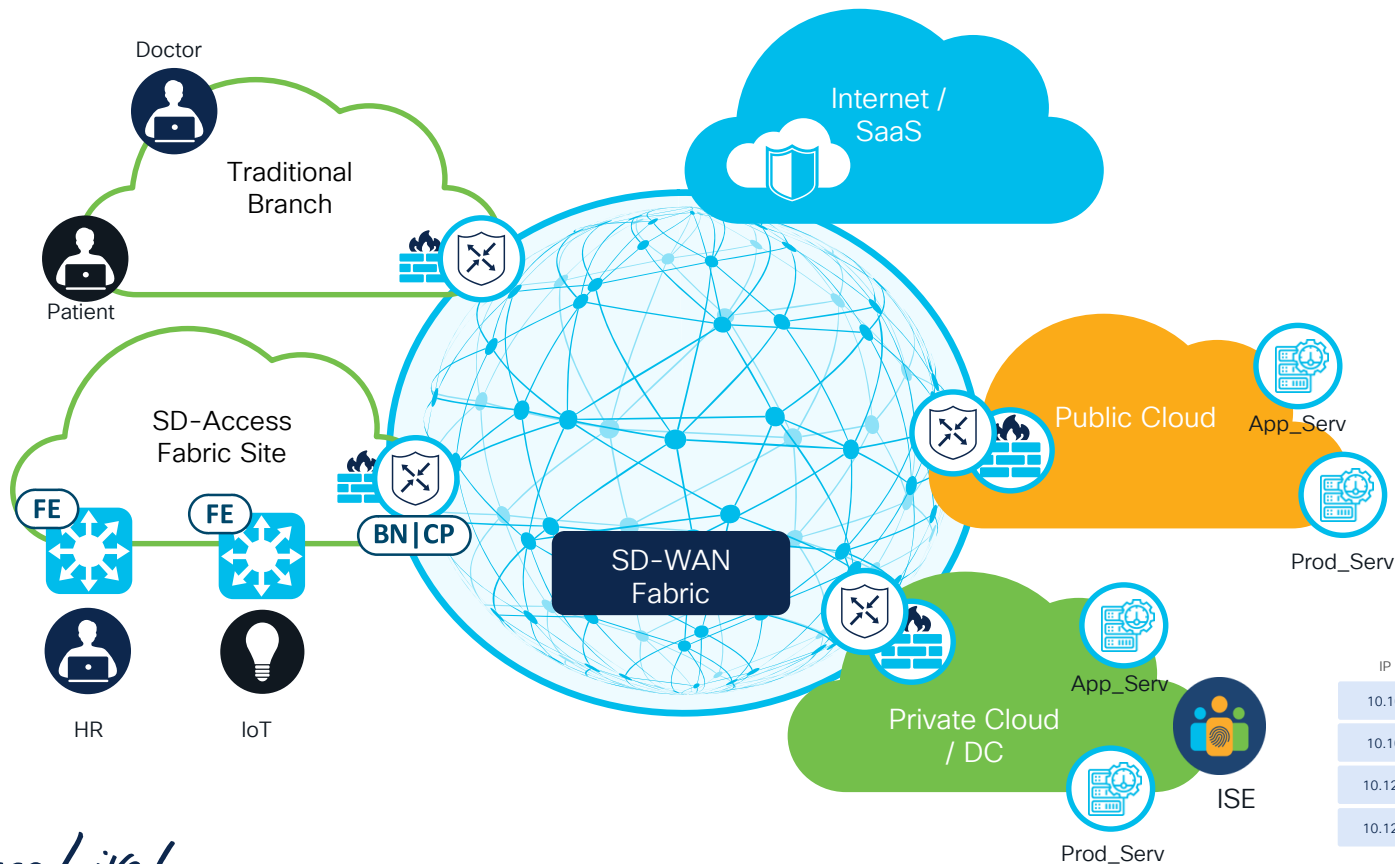
Security Group Tag (SGT): a label which identifies a group the device belongs to

User Authentication to Network Example

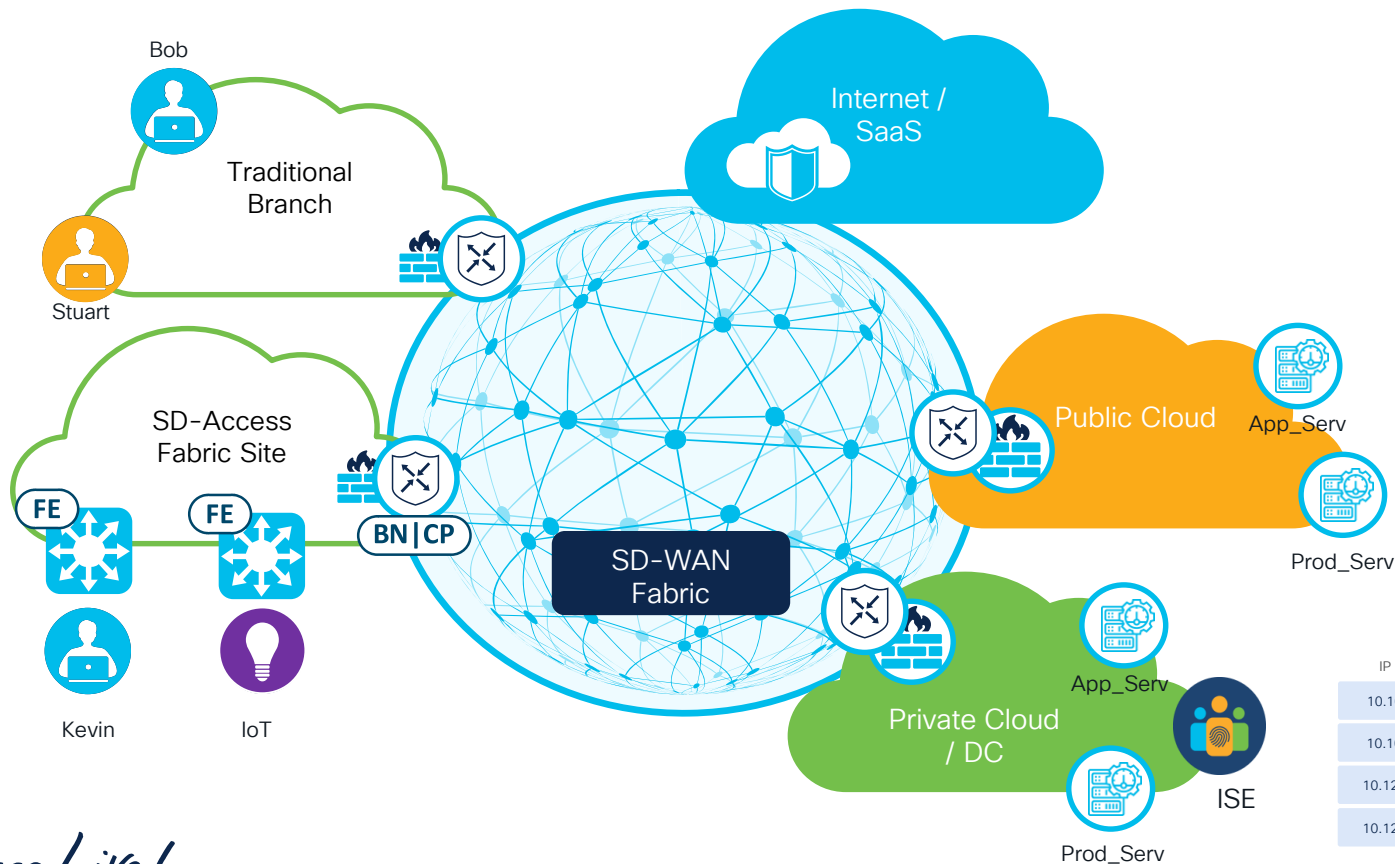
- ▶ Users connecting on wired or wireless infrastructure authenticate to network
- ▶ Successful auth allows ISE to register user's IP address and map it to Username, AD group, and VLAN
- ▶ Accounts for dynamic IP address changes



Segmenting Traffic

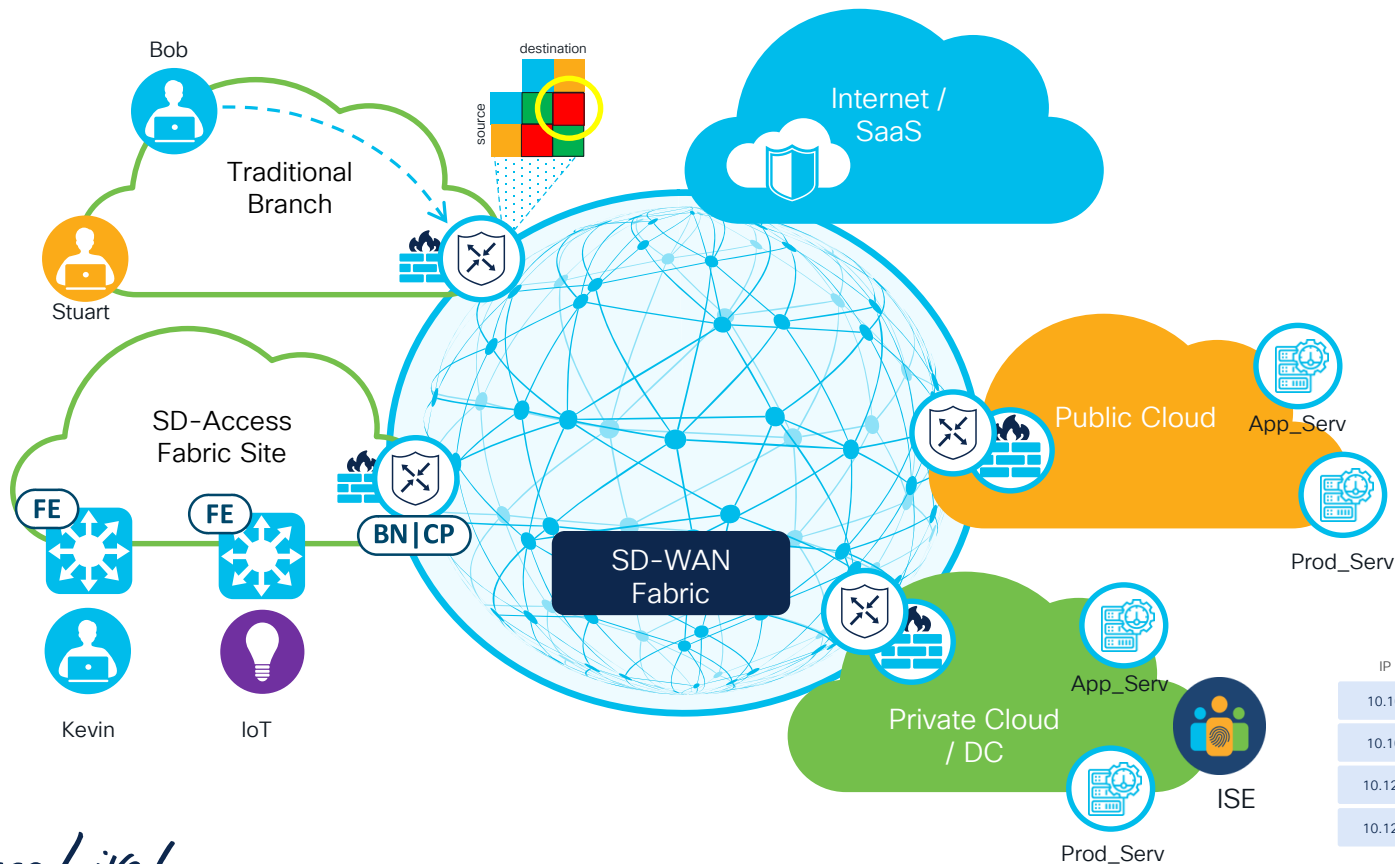


Users / Devices Authenticate to Network



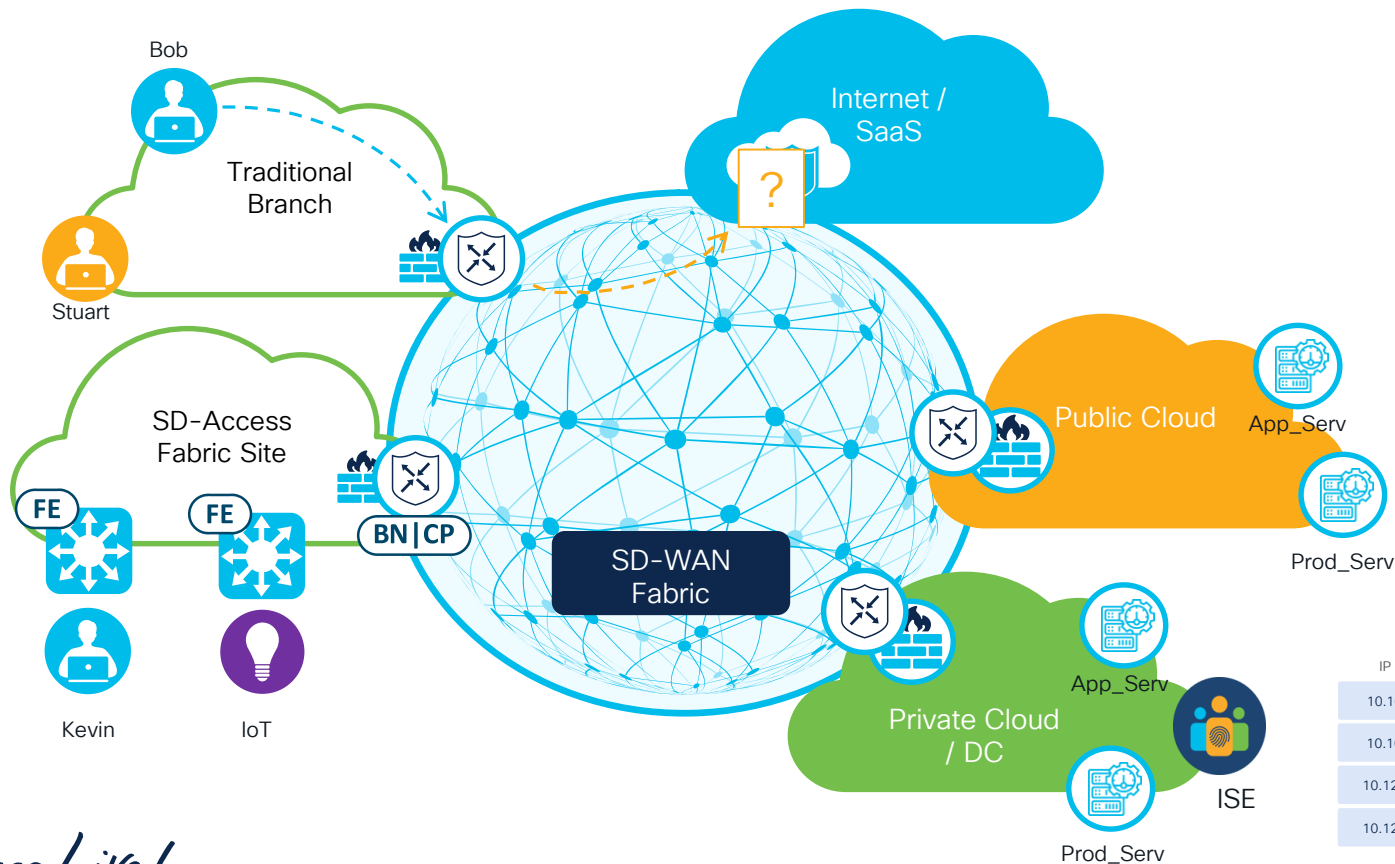
IP Addr	User/Profile	VRF/VPN
10.109.10.50	Bob	Staff
10.109.30.50	Stuart	Patient
10.120.10.101	Kevin	Staff
10.120.40.101	Light	IoT

Segmentation Prevents Dr. Bob Talking to Stuart



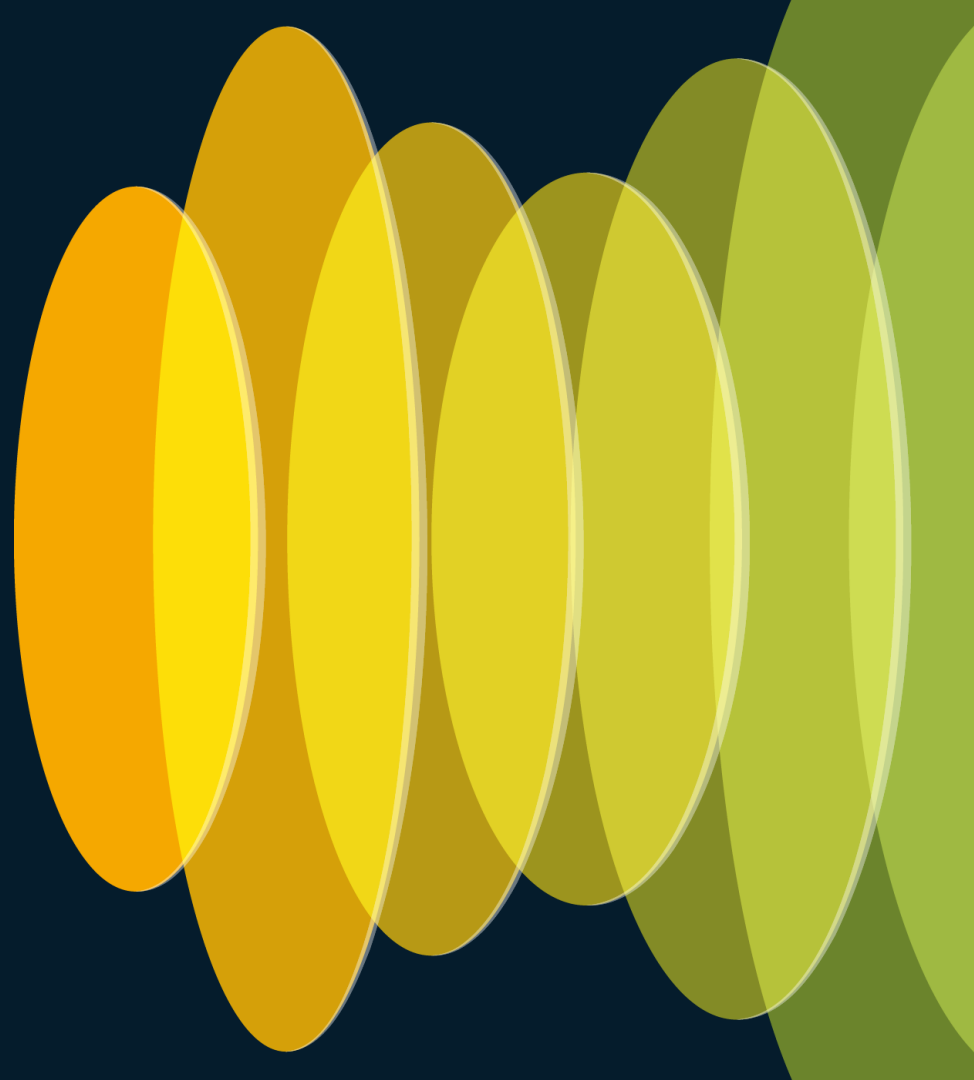
IP Addr	User/Profile	VRF/VPN
10.109.10.50	Bob	Staff
10.109.30.50	Stuart	Patient
10.120.10.101	Kevin	Staff
10.120.40.101	Light	IoT

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

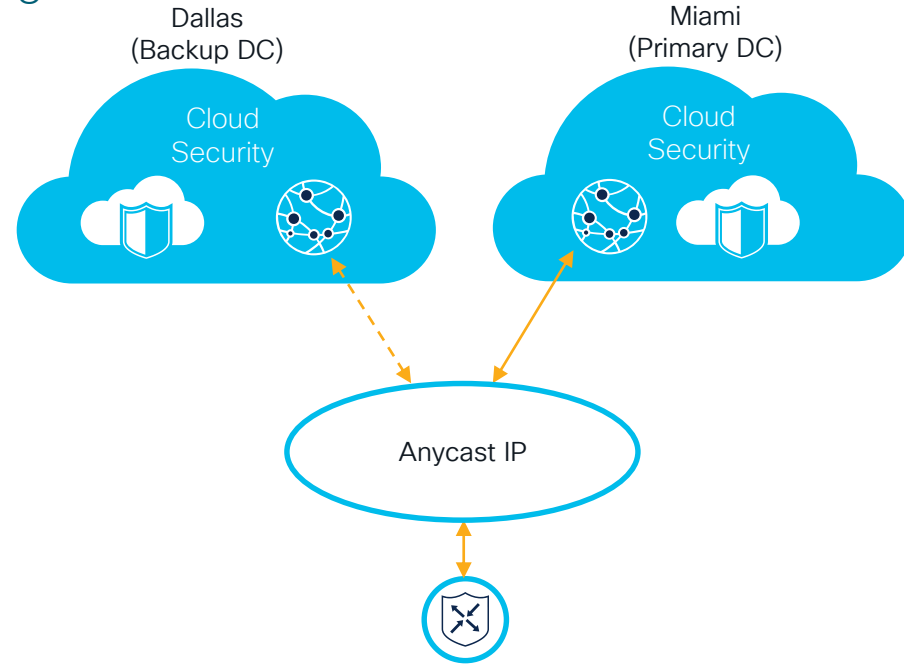
Extending Edge Segmentation for DNS Policies



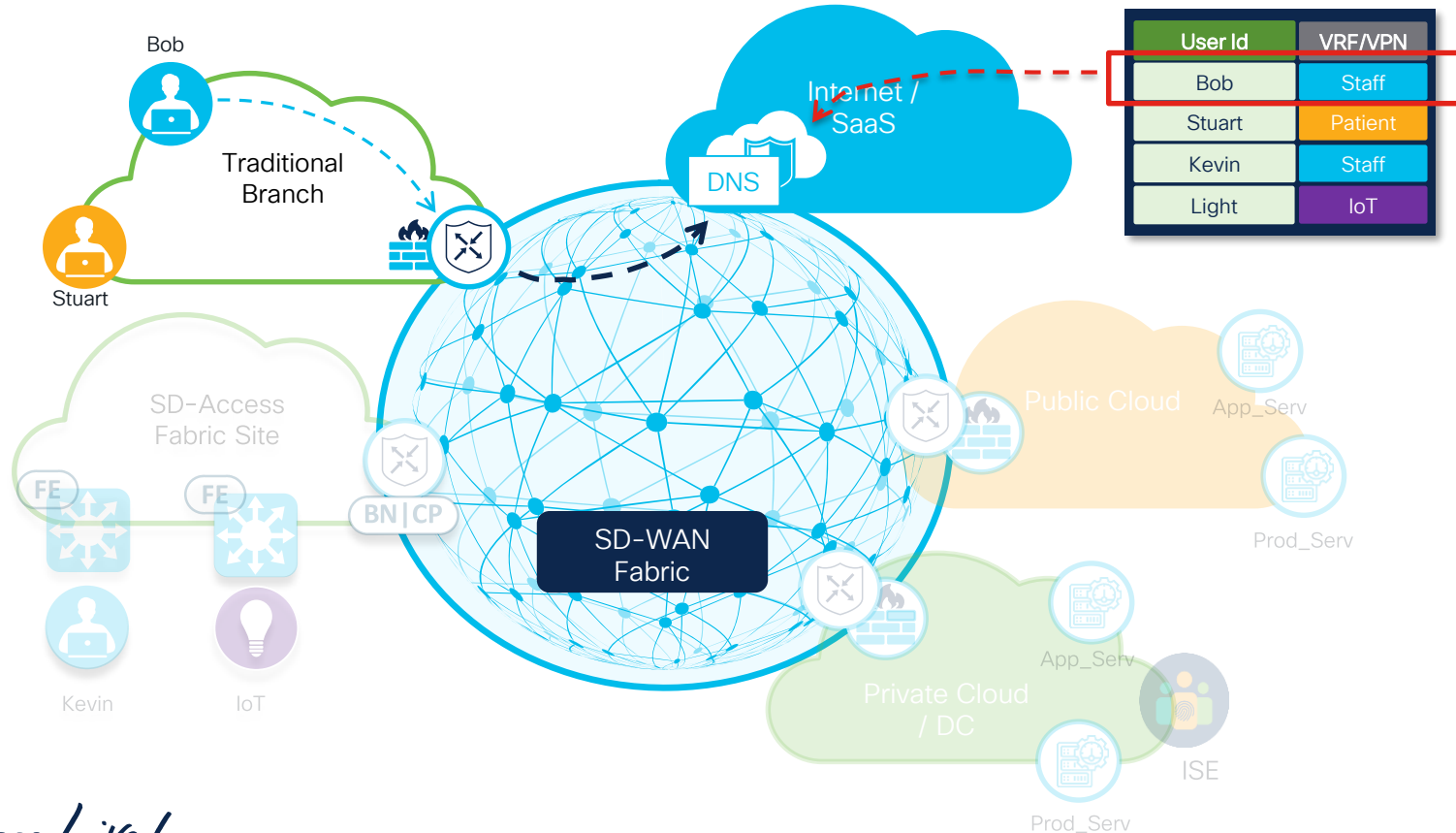
Extend Segmentation for DNS Protection

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



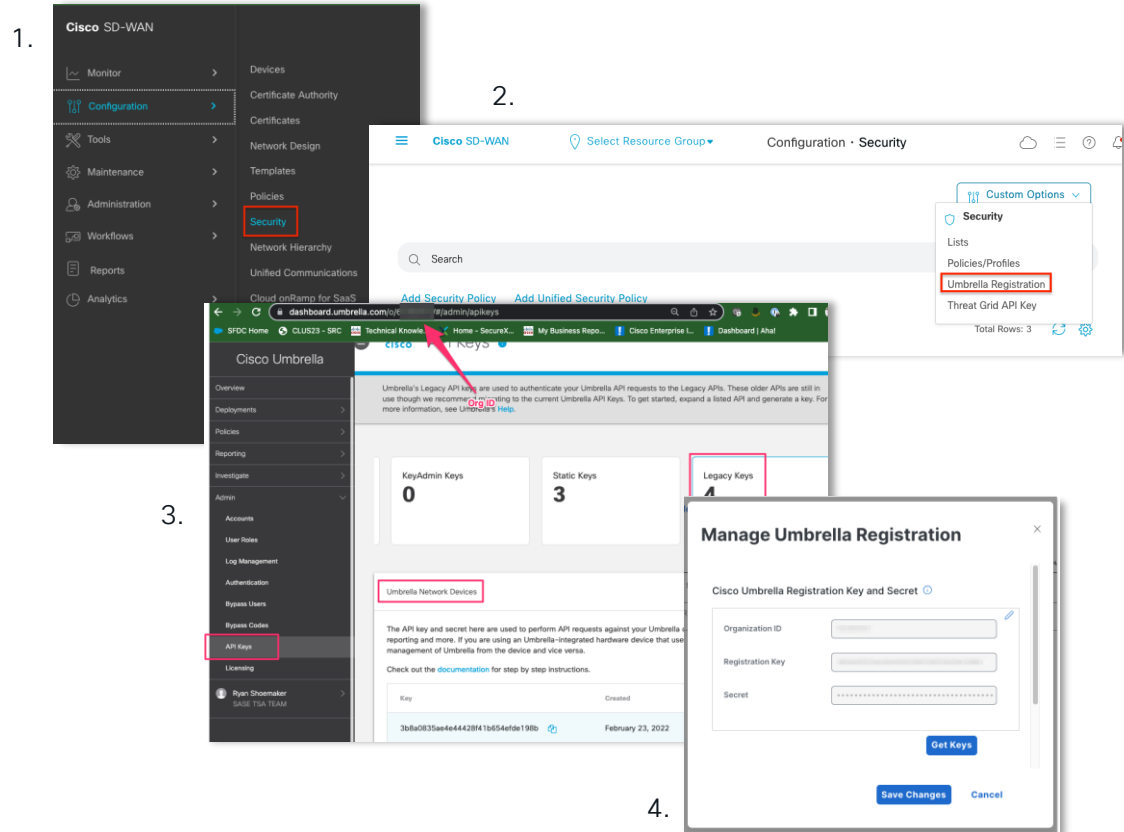
Dr. Bob Needs a Specific DNS Policy



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

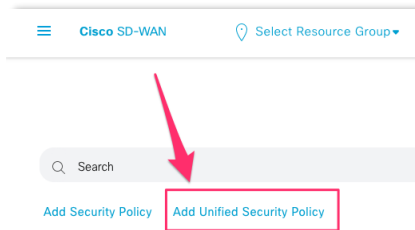


Setting DNS Redirection at the Router

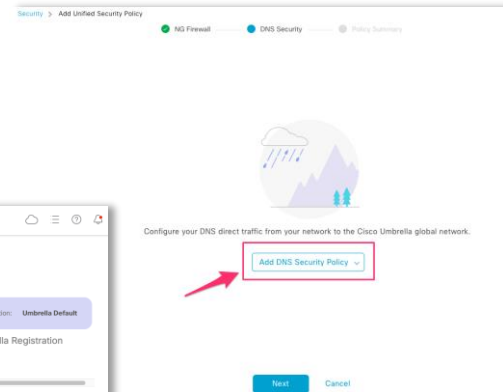
Reference

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

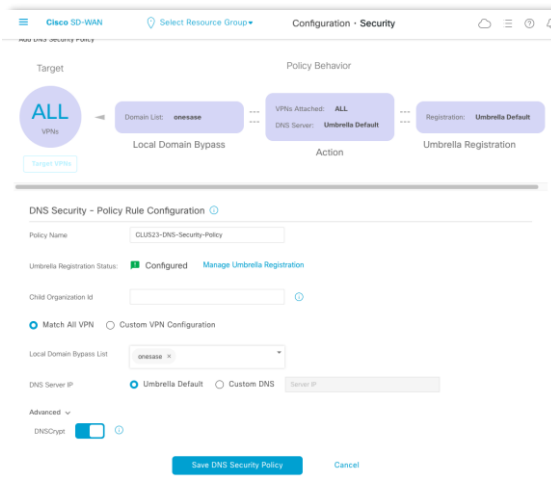
4.



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.

Cisco SD-WAN Configuration · Security

NG Firewall DNS Security Policy Summary

Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name: CLUS23-Security-Policy-DNS-Only

Security Policy Description: Security Policy for DNS Only

Back Preview Save Policy Cancel

8a.

Cisco SD-WAN Configuration · Template

Configuration Groups Feature Profiles Device Templates Feature Templates

Global Template * Factory_Default_Global_CISCO_Templ...

Cisco Banner Factory_Default_Retail_Banner

Cisco SNMP Choose...

TrustSec Choose...

CLI Add-On Template Unified_Logging_CLI

Policy Choose...

Probes Choose...

Tenant Choose...

Security Policy CLUS23-Security-Policy-DNS-Only

Cisco SIG Credentials * Cisco-Umbrella-Global-Credentials

8b.

Cisco SD-WAN Configuration · Templates

Associated Profiles (4)

System Profile: SIG_Branch

Security Profile: Umbrella_S

Search Table

Add Feature

Name IDFW_plus_DNS_Security_Feature

Edit Legacy policy Feature

security / Legacy policy

Feature Name * DNS_Security_Feature

Description

Security Policy Select security policy * CLUS23-Security-Policy-DNS-Only

IDFW_Sec_Policy_plus_DNS

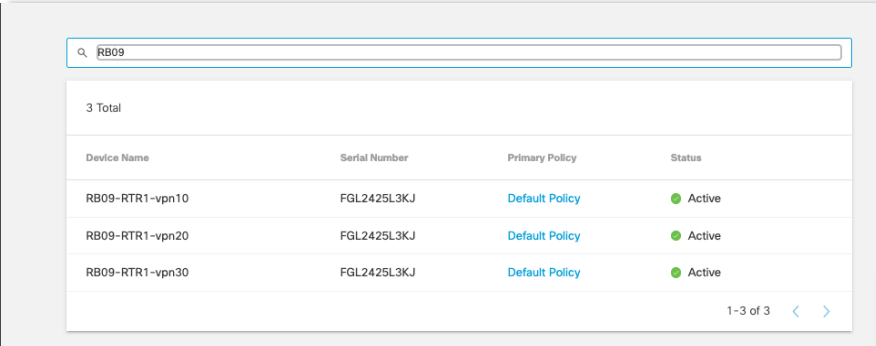
CLUS23-Security-Policy-DNS-Only

Leverage Source VRF/VPN for DNS Policy

Reference

Umbrella Dashboard

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



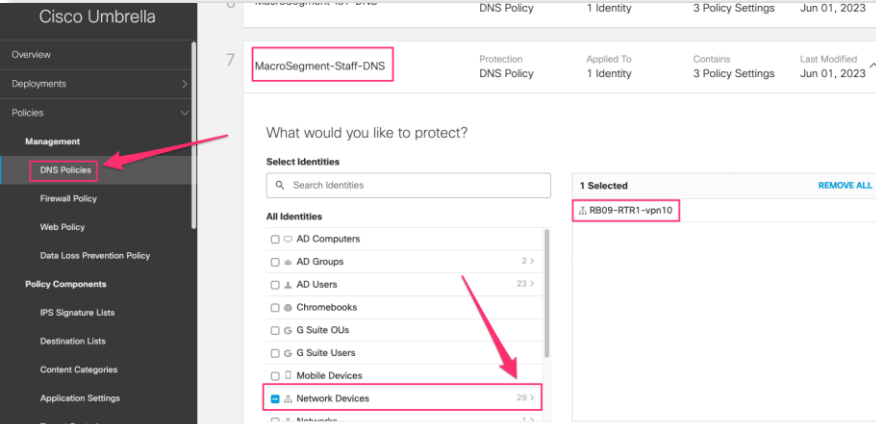
Search: RB09

3 Total

Device Name	Serial Number	Primary Policy	Status
RB09-RTR1-vpn10	FGL2425L3KJ	Default Policy	Active
RB09-RTR1-vpn20	FGL2425L3KJ	Default Policy	Active
RB09-RTR1-vpn30	FGL2425L3KJ	Default Policy	Active

1-3 of 3

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



Cisco Umbrella

Overview
Deployments
Policies
Management
Firewall Policy
Web Policy
Data Loss Prevention Policy
Policy Components
IPS Signature Lists
Destination Lists
Content Categories
Application Settings
Tenant Controls

DNS Policy

MacroSegment-Staff-DNS

Protection: DNS Policy

Applied To: 1 Identity

Contains: 3 Policy Settings

Last Modified: Jun 01, 2023

What would you like to protect?

Select Identities

Search Identities

1 Selected

REMOVE ALL

RB09-RTR1-vpn10

All Identities

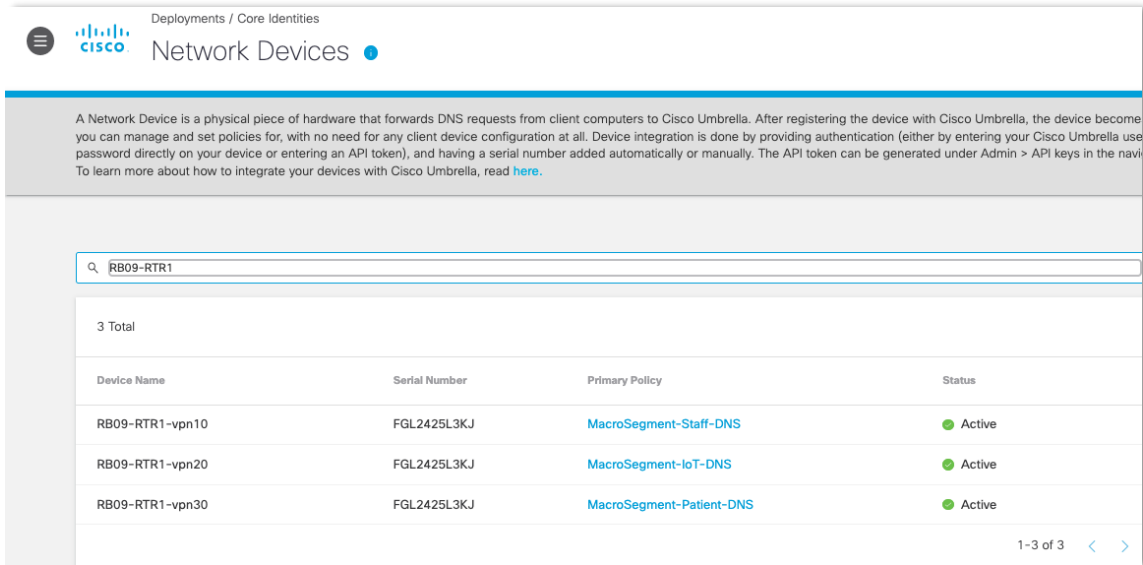
- ☐ AD Computers
- ☐ AD Groups
- ☐ AD Users
- ☐ Chromebooks
- ☐ G Suite OUs
- ☐ G Suite Users
- ☐ Mobile Devices
- ☒ Network Devices

Leverage Source VRF/VPN for DNS Policy

Reference

Umbrella Dashboard

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



The screenshot shows the Cisco Umbrella Network Devices dashboard. At the top, there's a navigation bar with the Cisco logo and the text "Deployments / Core Identities" and "Network Devices". Below this, a descriptive paragraph explains that a Network Device is a physical piece of hardware that forwards DNS requests from client computers to Cisco Umbrella. It mentions that after registering the device, it becomes manageable and policies can be set without client configuration. It also notes that device integration is done by providing authentication (either by entering your Cisco Umbrella user password directly on your device or entering an API token), and having a serial number added automatically or manually. The API token can be generated under Admin > API keys in the navigation menu. To learn more about how to integrate your devices with Cisco Umbrella, it refers to a link labeled "here".

Below the text, there's a search bar with the text "RB09-RTR1". Below the search bar, it says "3 Total". Below that, there's a table with the following columns: Device Name, Serial Number, Primary Policy, and Status.

Device Name	Serial Number	Primary Policy	Status
RB09-RTR1-vpn10	FGL2425L3KJ	MacroSegment-Staff-DNS	Active
RB09-RTR1-vpn20	FGL2425L3KJ	MacroSegment-IoT-DNS	Active
RB09-RTR1-vpn30	FGL2425L3KJ	MacroSegment-Patient-DNS	Active

At the bottom right of the table, it says "1-3 of 3" with navigation arrows.

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 1:36 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

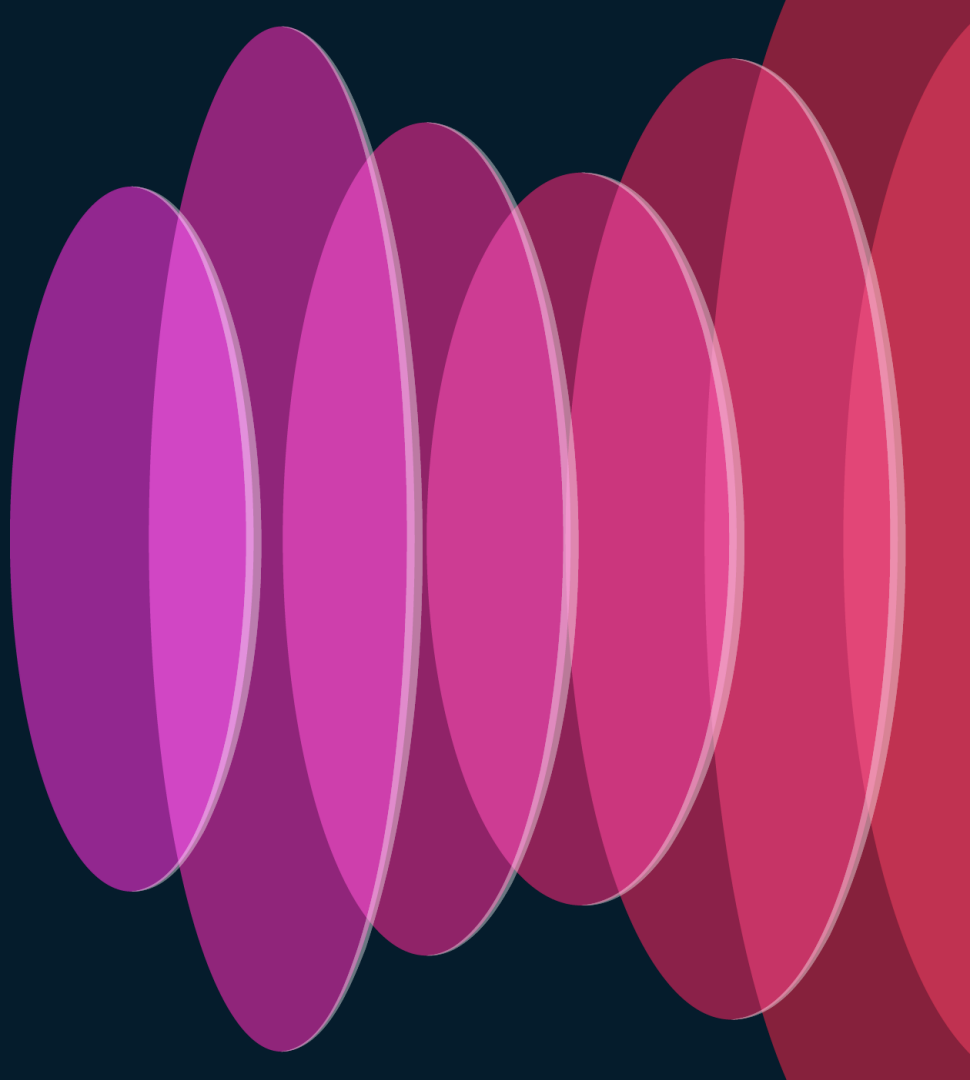
Application Category

Cloud Storage

DNS Type

A

Extending Edge Segmentation for Internet and SaaS Policies



Cloud Security Provided Cisco Secure Access

Core SSE



Secure Web Gateway (SWG)



Cloud Access Security Broker (CASB) and DLP



Zero Trust Network Access (ZTA)



Firewall as a Service (FWaaS) and IPS

Cisco delivers the core and more in a single subscription...



DNS Security



Multimode DLP



Advanced Malware protection



Sandbox



Talos Threat Intelligence



VPN as a Service



Digital Experience Monitoring*



Remote Browser Isolation*

* Included in the unified experience / separate license (optional)

Add-on solutions



SD-WAN



XDR



DUO MFA/SSO

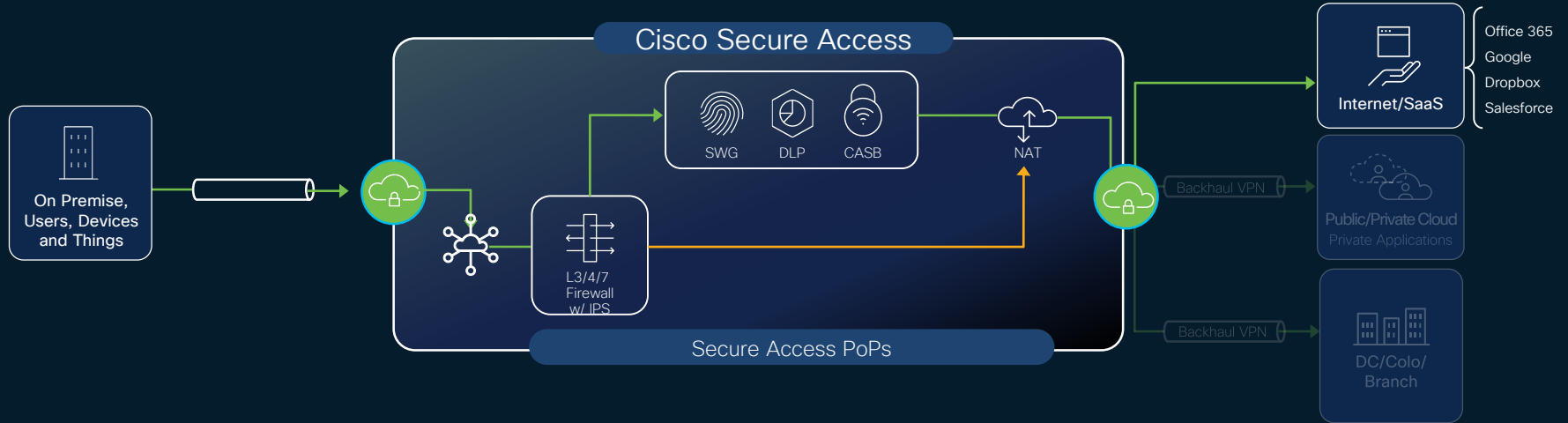


CSPM

Secure Branch Access

Secure Internet Access

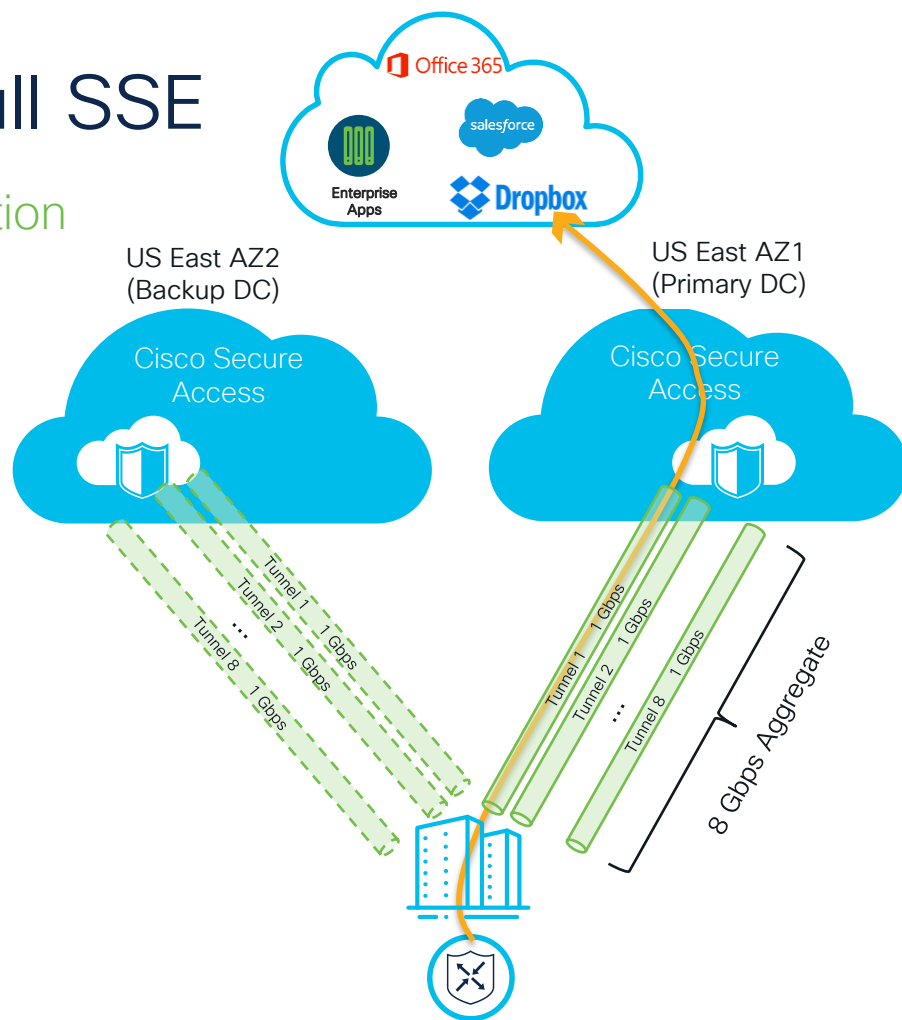
- ↔ Internet Traffic
- Non Web Traffic
- Secure Tunnel



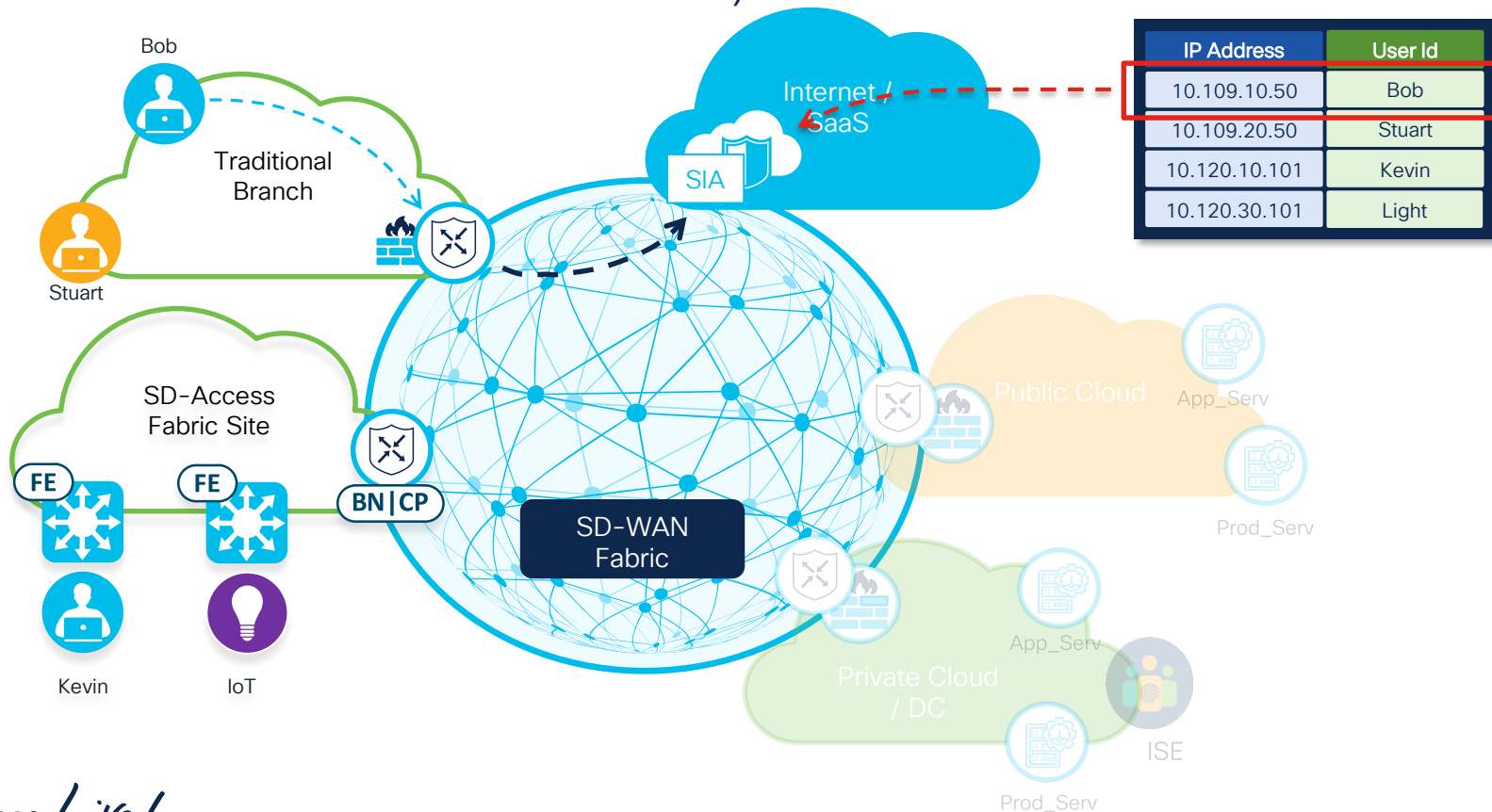
Extend Segmentation for Full SSE

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

The screenshot displays the Cisco Catalyst SD-WAN Manager interface for a configuration group named "RB-Branches-to-SA-2Stby". The description states: "Configuration Group for RB branches with multiple Service VRFs using sub-interfaces and 2Active SA 2 Standby SA connections".

Key details visible:

- Device Solution:** sdwan
- Modified By:** Rshoemak
- Last Updated:** Jan 24, 2024 03:34:50

The interface shows two tabs: "Feature Profiles" (selected) and "Associated Devices". Under "Associated Profiles (3)", the "System Profile: Branches-to-SA_Basic" is listed.

The "Transport & Management Profile: RB-to-SA-VPN0-Profile" is expanded, showing a table of features. A red box highlights the "Loopback2-Interface" and "Loopback1-Interface" entries, which are sub-features of the "VPN0-Internet-Intf" feature. A tooltip for "Loopback2-Interface" reads "Interface for Loopback2".

Type	Feature Name	Description	Sub-Feature	Actions
VPN	VPN-DHCP-Next-Hop		-	...
	VPN0-Internet-Intf		-	...
	Loopback2-Interface	Interface for Loo...	-	...
	Loopback1-Interface	Interface for Loo...	-	...

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

The image displays three overlapping screenshots from the Cisco Catalyst SD-WAN configuration interface, illustrating the process of adding a tunnel to a policy group.

Top Screenshot (Configuration Page): Shows the 'Configuration' tab with a breadcrumb trail: 'Secure Internet Gateway / Secure Service Edge'. A red box highlights the 'Secure Internet Gateway / Secure Service Edge' link. Below it, a table lists the configuration items, with 'Add Secure Service Edge (SSE)' highlighted by a red box and an arrow.

Middle Screenshot (CLEUR24-SSE Configuration): Shows the configuration for the 'CLEUR24-SSE' provider. The 'Tracker' section has a red box around the 'Source IP address' field, which contains '192.168.255.224'. A red arrow points to this field.

Bottom Screenshot (Add Tunnel Dialog): Shows the 'Add Tunnel' dialog box. The 'Tunnel Type' is set to 'ipsec4'. The 'Interface Name' is 'ipsec4'. The 'Tracker' is 'DefaultTracker'. The 'Tunnel Source Interface' is set to 'Loopback2', highlighted by a red box and an arrow. The 'Tunnel Route-via Interface' is set to '{{ SSE_tunnel4_Outbound_Interface }}'. The 'Data Center' is set to 'Secondary'. The 'Add' button is visible at the bottom right.

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

Region*
Auto

High Availability

Add Interface Pair

Active Interface	Active Interface Weight	Backup Interface	Backup Interface Weight	Action
ipsec1	1	ipsec3	1	Edit Delete
ipsec2	1	ipsec4	1	Edit Delete

Edit Interface Pair

Active Interface*
ipsec1

Active Interface Weight*
1

Backup Interface*
ipsec3

Backup Interface Weight*
1

Cancel Update

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

The screenshot displays the Catalyst SD-WAN configuration interface. At the top right, it shows the date and time: "As of: January 22, 2024 at 2:47 PM". Below this is a search bar. The main content area is a table with columns: Name, Description, Number of Policies, Number of Devices, Devices Up to Date, Updated By, and Last Updated On. Below the table is a form for adding a new policy group. The form has a header "RB-SA-AutoTunnels-Act-Act-Pair" and a "Policy Group Name" field with the value "RB-SA-AutoTunnels-Act-Act-Pair". The "Description" field is empty. The "Policy" section has a dropdown menu for "Application Priority" with the value "Please Select one". The "Embedder Security" dropdown menu has the value "Please Select one". The "Secure Internet Gateway / Secure Service Edge" dropdown menu has the value "BR-Routers-SSE-2Active-2Standby". The "DNS Security" dropdown menu has the value "Please Select one". The "Device Solution" section shows "sdwan". The "Deployment" section shows "Associated to: 0 Device(s)". At the bottom right, there are two buttons: "Save" and "Deploy".

Annotations:

- 1. Points to the "Add Policy Group" button at the top left.
- 2. Points to the "Secure Internet Gateway / Secure Service Edge" dropdown menu.
- 3. Points to the "Save" button.
- 4. Points to the "Deploy" button.
- 5. Points to the "Deploy" button.

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 from router

4 IPsec tunnels:
2 Primary
2 Secondary

Secure Access

← Network Tunnel Groups

ISR1100-4G-FGL2425L3KJ

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of. [Help](#)

Summary

Connected

Region: Europe (Germany)
Device Type: Catalyst SDWAN
Routing Type: NAT / Outbound Only
Last Status Update: Jan 25, 2024 5:05 PM

Primary Hub

Hub Up

2 Active Tunnels

Tunnel Group ID: ISR1100-4G-FGL2425L3KJ@8206406-620471169-sse.cisco.com
Data Center: sse-euc-1-1-0
IP Address: 18.156.145.74

Secondary Hub

Hub Up

2 Active Tunnels

Tunnel Group ID: ISR1100-4G-FGL2425L3KJ@8206406-620471170-sse.cisco.com
Data Center: sse-euc-1-1-1
IP Address: 3.120.45.23

Network Tunnels

Review this network tunnel group's IPsec tunnels. [Help](#)

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Primary 1	327682	209.122.90.235	sse-euc-1-1-0	18.156.145.74	Connected	Jan 25, 2024 5:05 PM
Primary 2	327683	209.122.90.235	sse-euc-1-1-0	18.156.145.74	Connected	Jan 25, 2024 5:05 PM
Secondary 1	393218	209.122.90.235	sse-euc-1-1-1	3.120.45.23	Connected	Jan 25, 2024 5:03 PM
Secondary 2	393219	209.122.90.235	sse-euc-1-1-1	3.120.45.23	Connected	Jan 25, 2024 5:03 PM

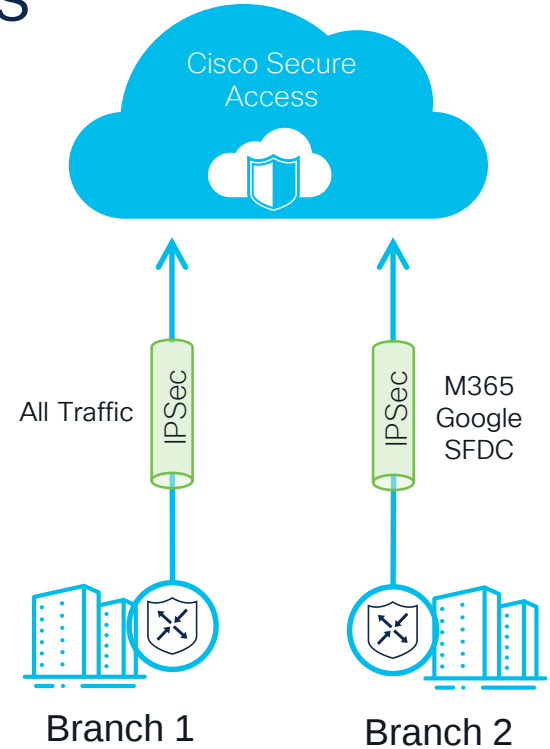
Directing Traffic to Secure Access

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

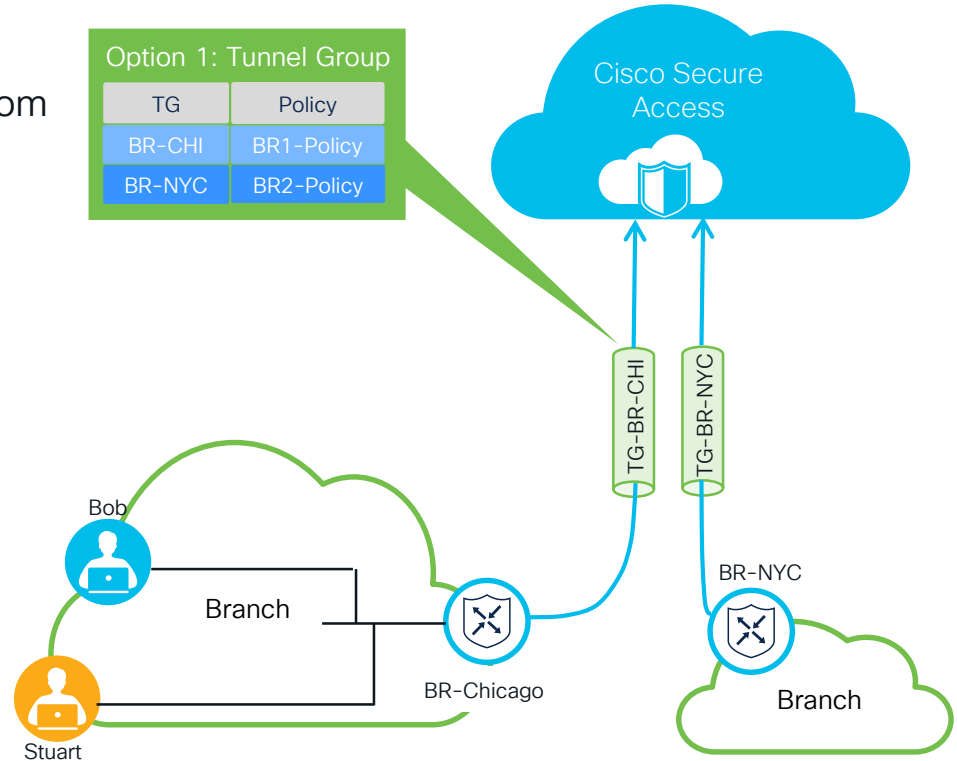
- Flexibility to select which applications send traffic to SSE
- Leverage DPI for app-classification
- Route-based redirection also possible



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.

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

Rule order: 9

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action

☒ **Allow**
Allow specified traffic if security requirements are met.

☐ **Block**
Block specified traffic.

☐ **Warn**
Allow access but display a warning.

From
Specify one or more sources.

[+1 More](#)

To
Specify one or more destinations.

[x](#)

Information about destinations, including selecting multiple destinations

Select sources [Add a source](#)

Source > Network Tunnel Groups

- ☐ Any Network Tunnel Group
Includes all existing and future configured network tunnel groups
- ☐ Boston-MySecureConnectMX65
- ☐ BostonOffice-Cat8k-SDWAN
- ☐ Cat-Branch-oscrimir
- ☐ CB09
- ☐ CLUS-TG-POD02
- ☐ CLUS-TG-POD03
- ☐ FTD-OSCRAMIR-CR
- ☒ **ISR1100-4G-FGL2425L3KJ**
- ☐ Secure Access VDO-PTD1-UE

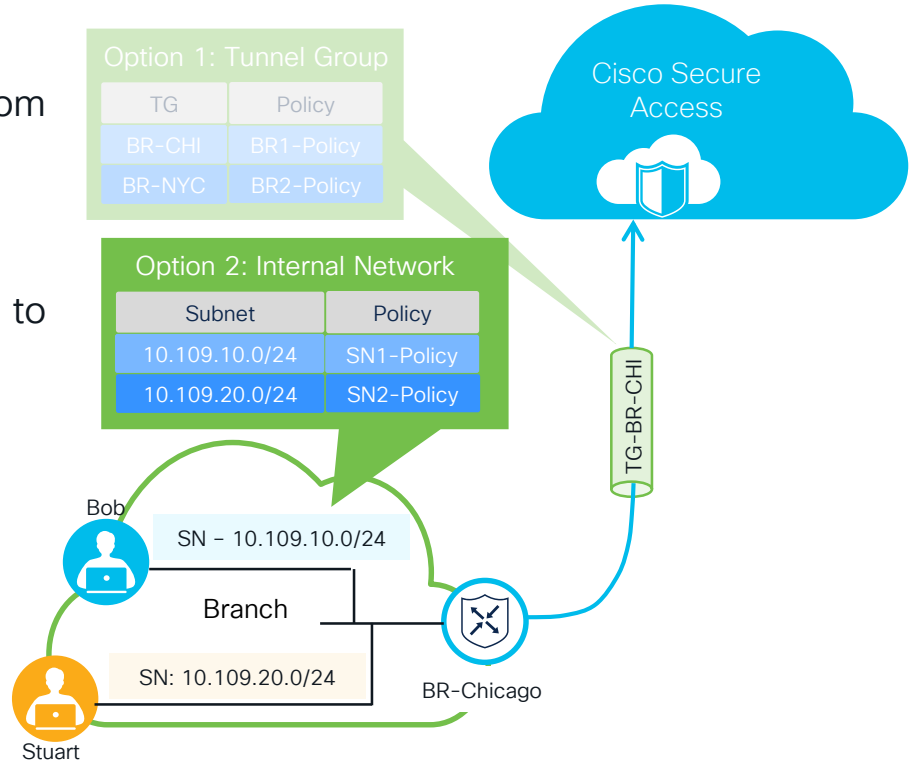
Any traffic ⓘ >

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

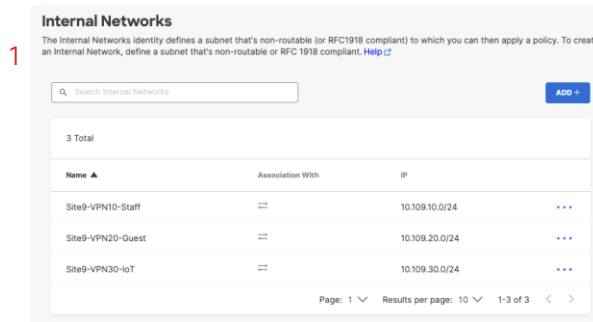


Secure Access Internal Networks

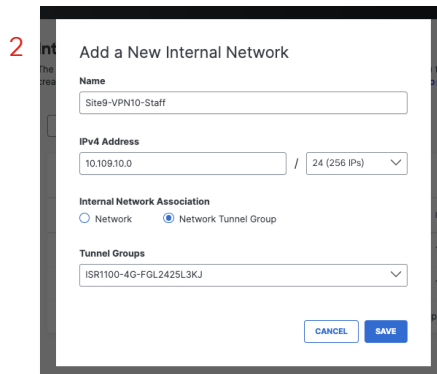
Reference

Set Subnet at Branch as Source of Policy

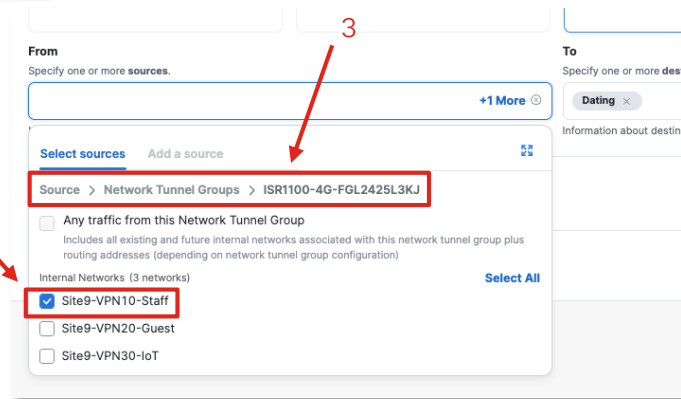
1. Identify specific internal networks at **Resources -> Internal Networks**. Select **Add+**



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



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

Category **Blocked**
for Patient VRF

Category **Warned**
for Staff 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

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

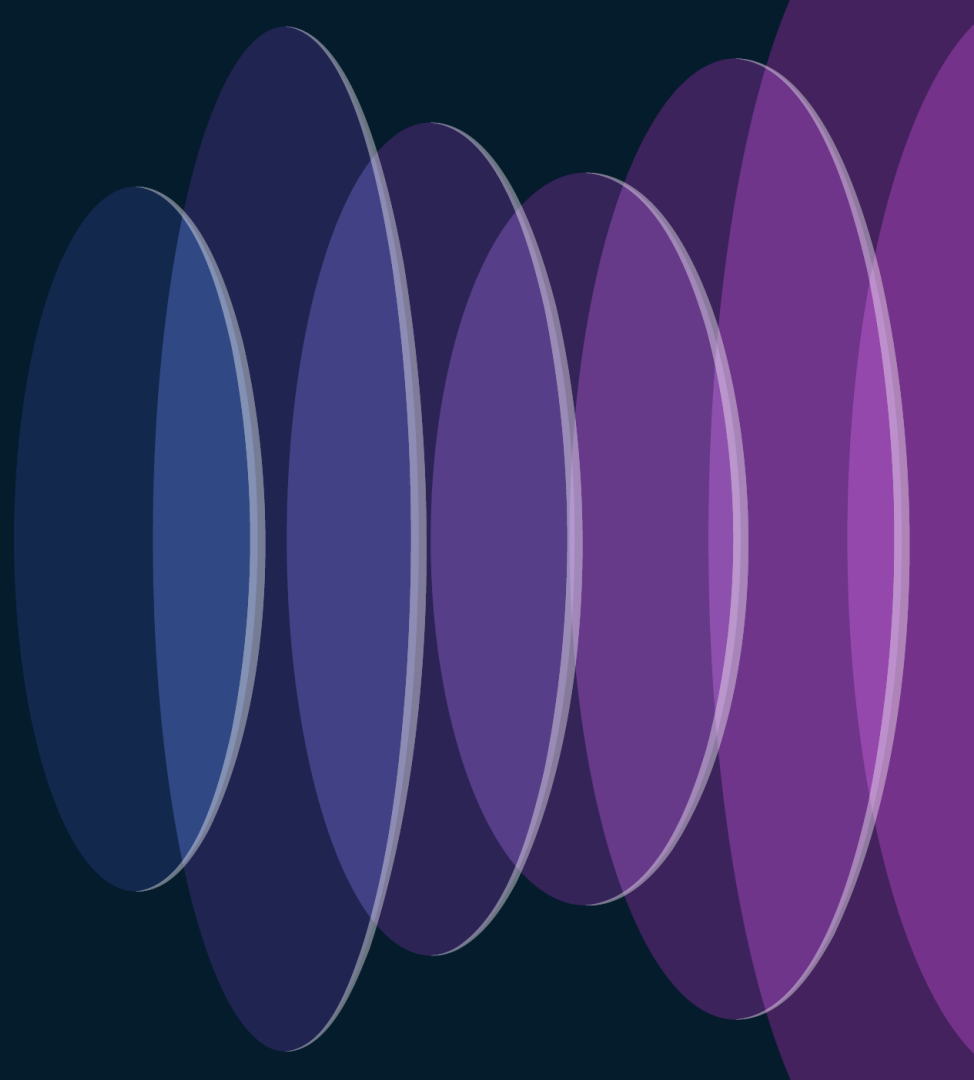
Categories
Application Warn, Online Storage and Backup, File Storage
Dispute Categorization

Resource/Application
Box Cloud Storage

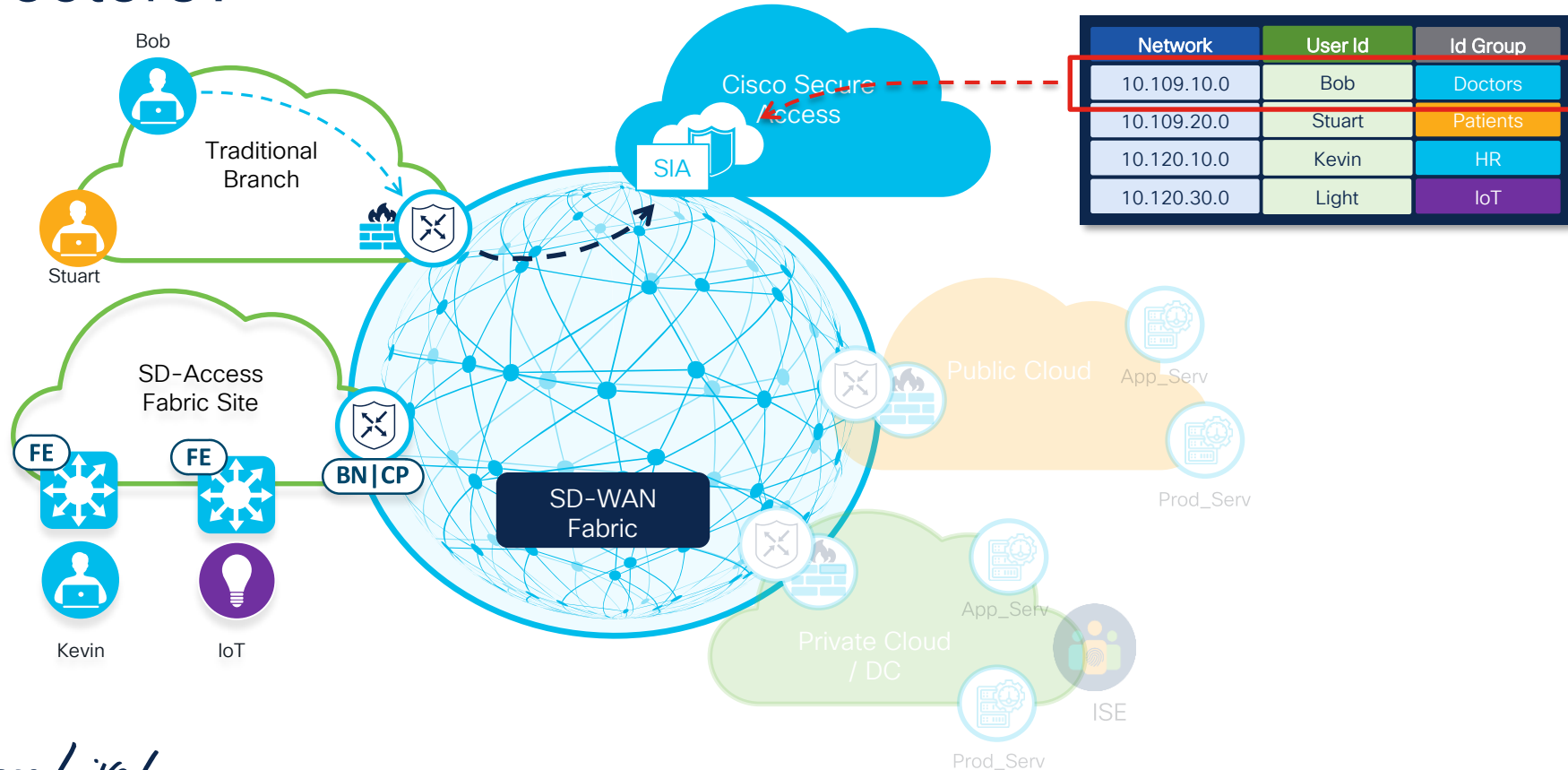
Application Category
Cloud Storage

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

Internet and SaaS Policy for Groups using SAML



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



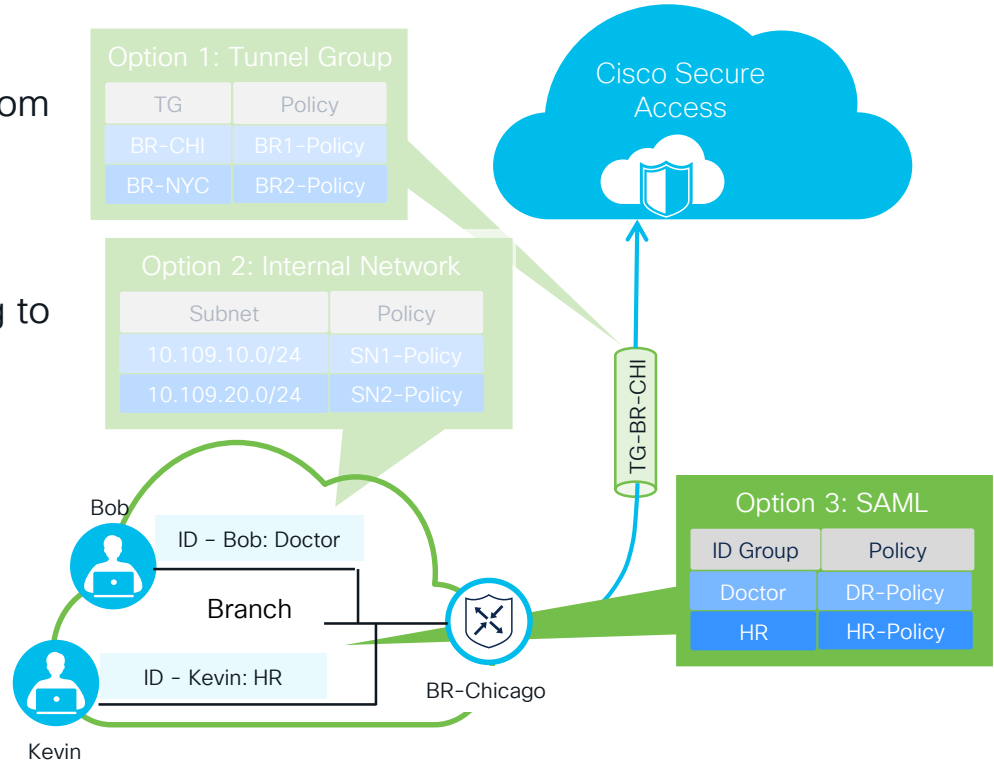
Setting Security Policy for Branch Users

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

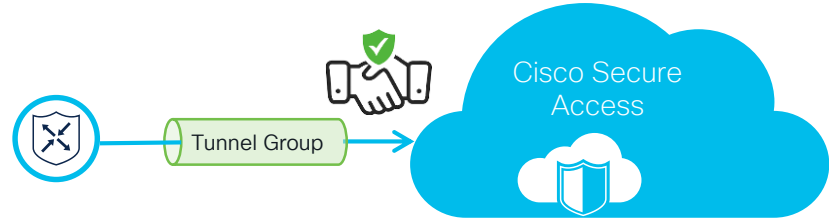
Secure Access is **not** an open proxy

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!!)

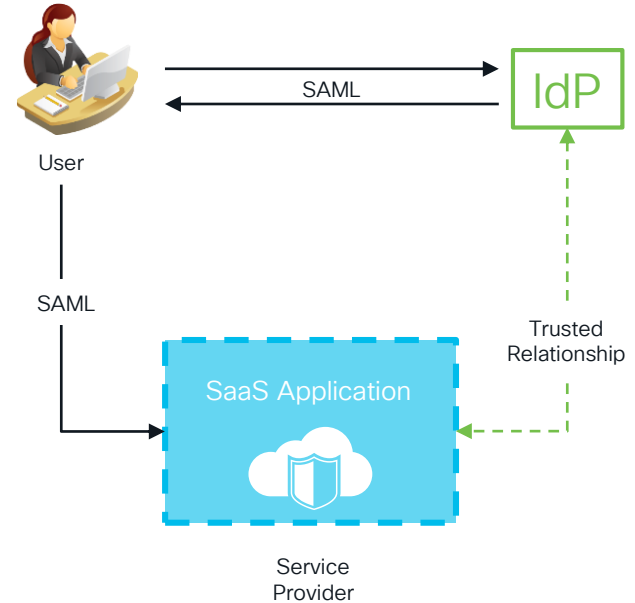
SAML at a High Level

Security Assertion Markup Language

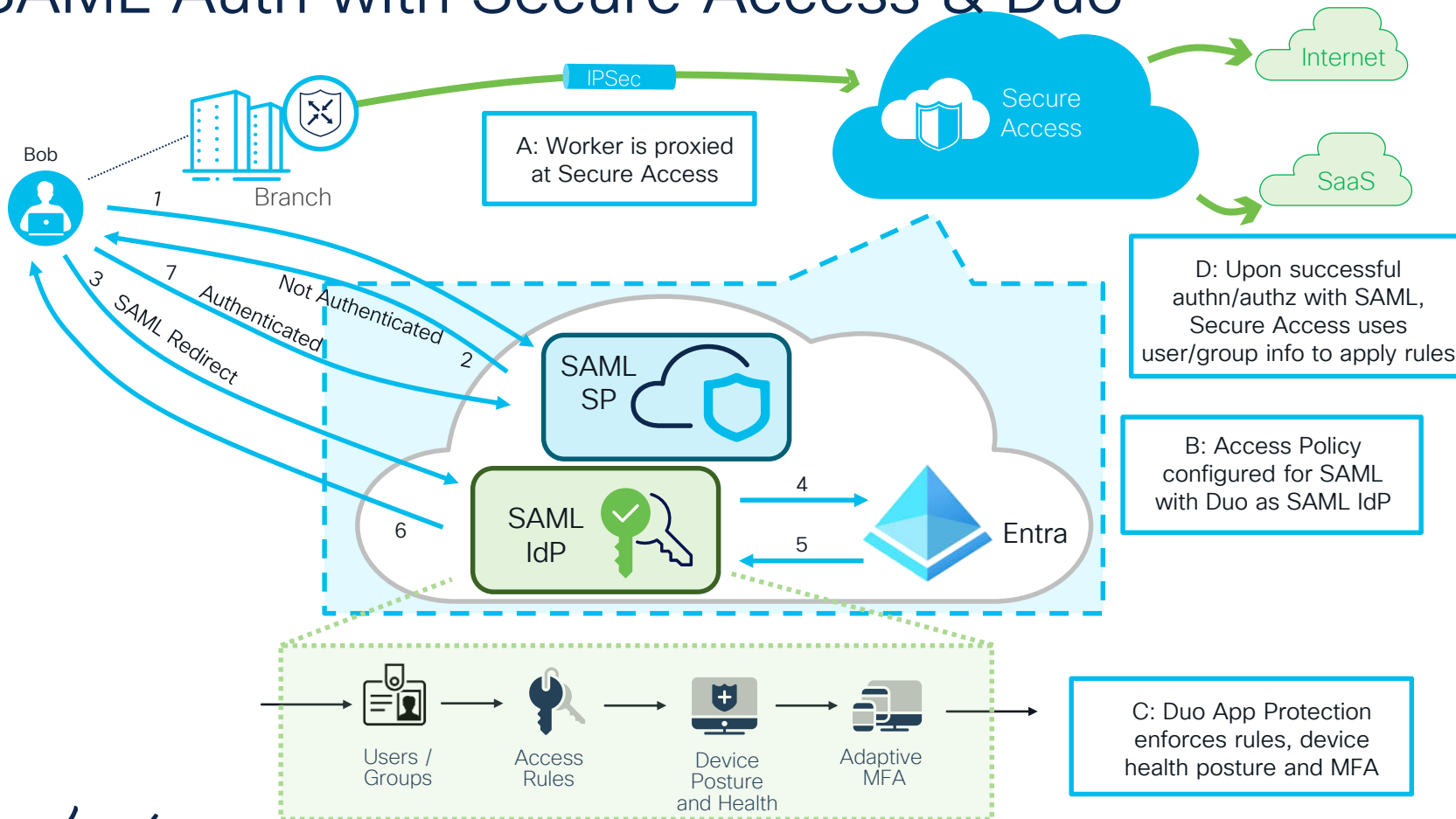
SAML is authentication mechanism used to access multiple web applications with one set of credentials (SSO)

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

Users and User Groups

Manage your organization's users and user groups. To add new users and user groups, provision them through a supported identity provider. Once added, users and user groups can then be added to an access rule. [Help](#)

Users

Groups

[Config](#)

Groups

Manage your organization's user groups. To add new user groups, click Provision Groups. [Help](#)

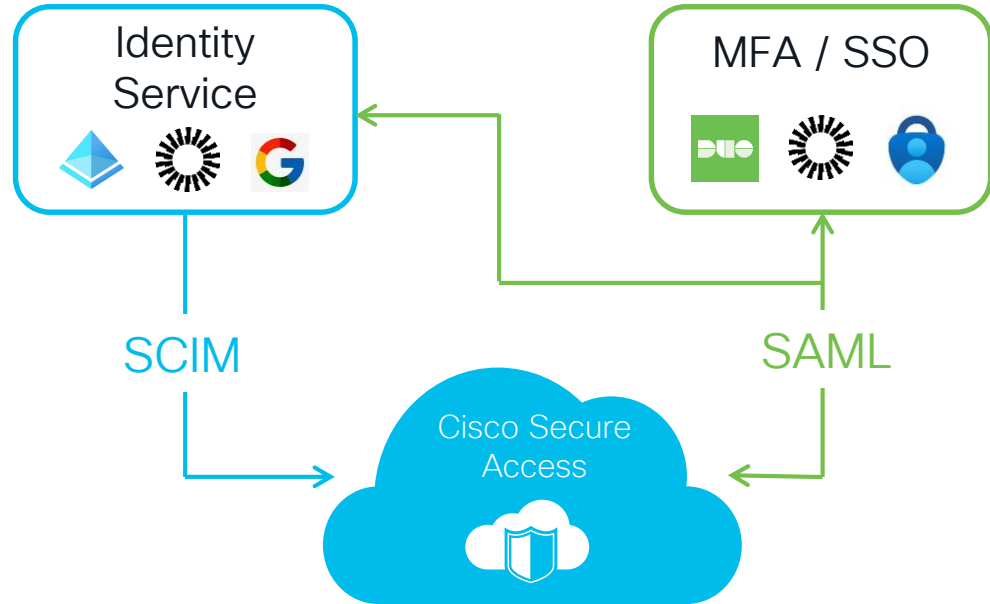
Q Search

16 results

Name	Users	Source	Associated Rules
Access Control Assistance Operators	0	OnPrem	0
Cloneable Domain Controllers	0	OnPrem	0
Contractors	8	Azure	2
Domain Computers	1	OnPrem	0
Domain Users	4	OnPrem	1
Employees	8	Azure	9
Enterprise Key Admins	0	OnPrem	0
Hyper-V Administrators	0	OnPrem	0

Using Identity for Policies 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



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

The screenshot displays the configuration interface for a Secure Access policy. At the top, a summary bar shows: 'Decrypt+SAML' (Applied To: 4 Rules), 'Decryption' (Enabled), 'SAML, Auth' (Enabled), 'Security and Acceptable Use' (2 Control Types Selected), 'End-User Notifications' (System-provided), and 'Last Modified' (Sep 29, 2023).

The main configuration area is divided into sections:

- Profile Name:** A dropdown menu is set to 'Decrypt+SAML' (highlighted with a red box). Below it is a checkbox for 'Set as default Web Profile'.
- Decryption:** A text block explaining that decryption is necessary for security and acceptable use. Below this, a table shows 'Decryption' is 'Enabled' and 'Do Not Decrypt List' is 'None'. An 'Edit' link is present.
- SAML Authentication:** A section header.
- 4 Configure Security:** A sub-section header with a 'Help' link. Below it, a text block states: 'Traffic will be decrypted and inspected based on the selected IPS profile. Transactions involving destinations on the Do Not Decrypt List will not be decrypted.' Below this, a status bar shows: 'Profile: Balanced Security and Connectivity | Intrusion System Mode: prevention | Signatures: 9350 Block, 488 Log Only, 40327 Ignore'.
- Web Profile Custom:** A section header. Below it, a text block states: 'The following web-related settings will apply to traffic that matches this rule. Help'. Below this, a dropdown menu is set to 'Decrypt+SAML' (highlighted with a red box). Below the dropdown, a table lists settings:

Decryption	Enabled	SAML Authentication	Enabled
Threat Categories	3 Categories Enabled, Default Web Settings	File Inspection	Enabled, Threatgrid Malware
File Type Blocking	Disabled	SafeSearch	Disabled
End-User Notifications	System Provided Block page		

Group Specific Web Policy at Work

The screenshot displays the Cisco Duo Web Policy interface. At the top, it shows '1 Total' and a time range filter for 'Viewing activity from May 29, 2024 5:53 PM to May 30, 2024 5:53 PM'. Below this is a table with columns: Request, Source, Rule Identity, and Destination. A single event is listed with the following details:

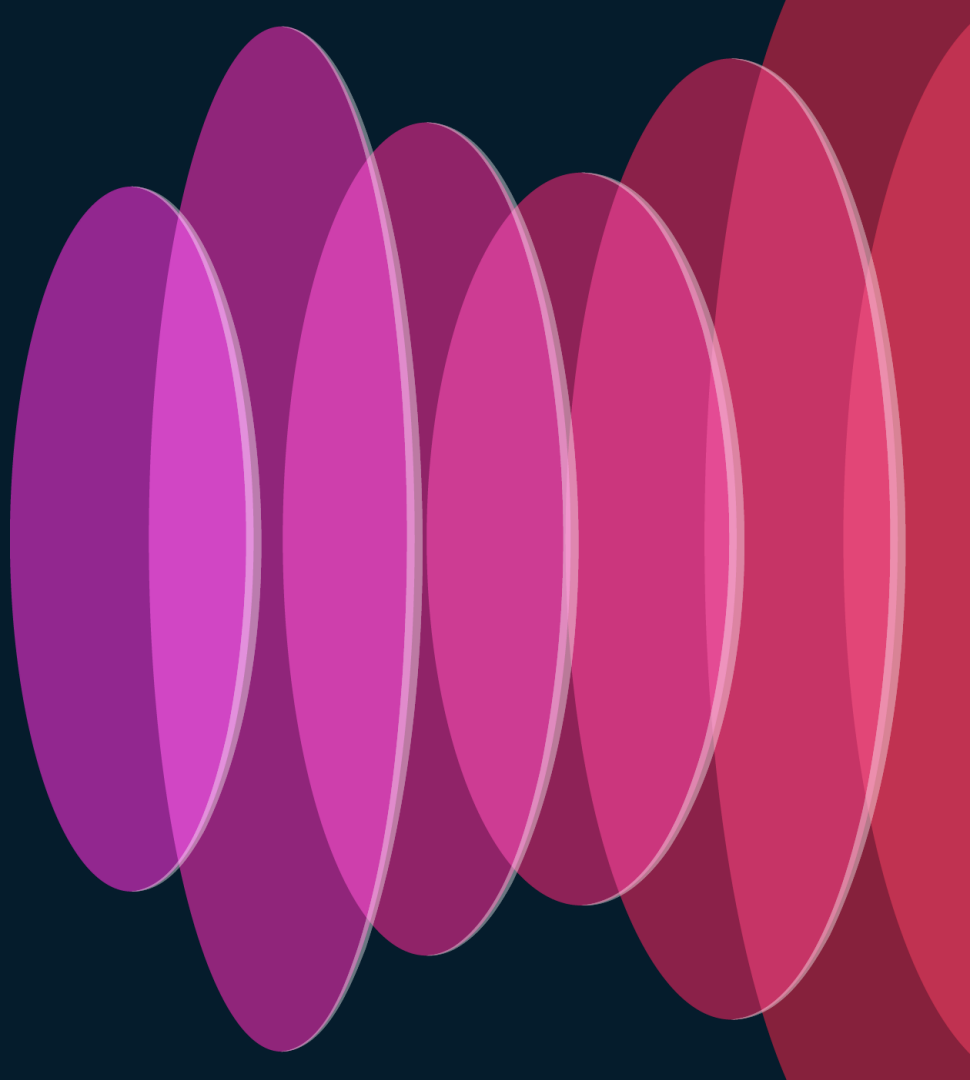
Request	Source	Rule Identity	Destination
WEB	Bob (bob@onesase.com)	Site9-VPN10-Staff	https://mychart.org/

Two red arrows point from the 'Source' and 'Rule Identity' columns of the table to the 'Event Details' panel on the right. The 'Event Details' panel shows the following information:

- Action:** Allowed — Warn Page Displayed
- Time:** May 30, 2024 5:52 PM
- Rule Name:** Ryan - CLUS Test 3 - Doctors - SAML-SDWAN
- Source:**
 - Bob (bob@onesase.com)
 - Site9-VPN10-Staff
 - ISR1100-4G-FGL2425L3KJ
- Rule Identity:** Site9-VPN10-Staff
- User Identity Source:** SAML IP Surrogate
- Internal IPv4 Address:** 10.109.10.2
- External IP Address:** -
- Destination:** https://mychart.org/
- Hostname:** mychart.org
- Categories:** Health and Medicine, Health and Fitness; Dispute Categorization

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

New Policy Source Methods

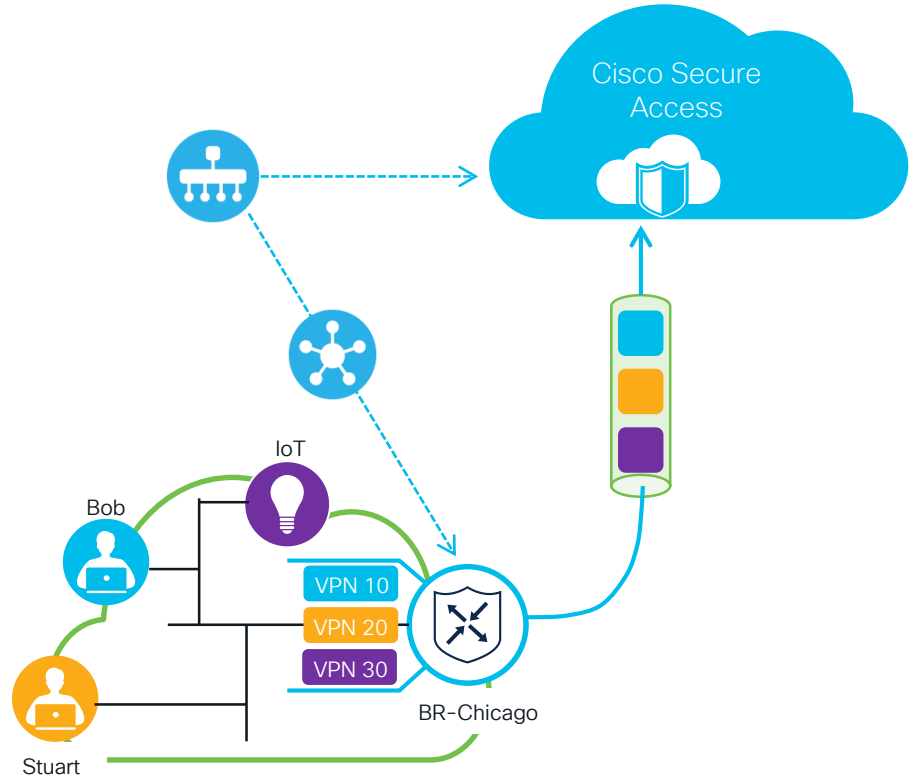


Setting Security Policy for Branch Users

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

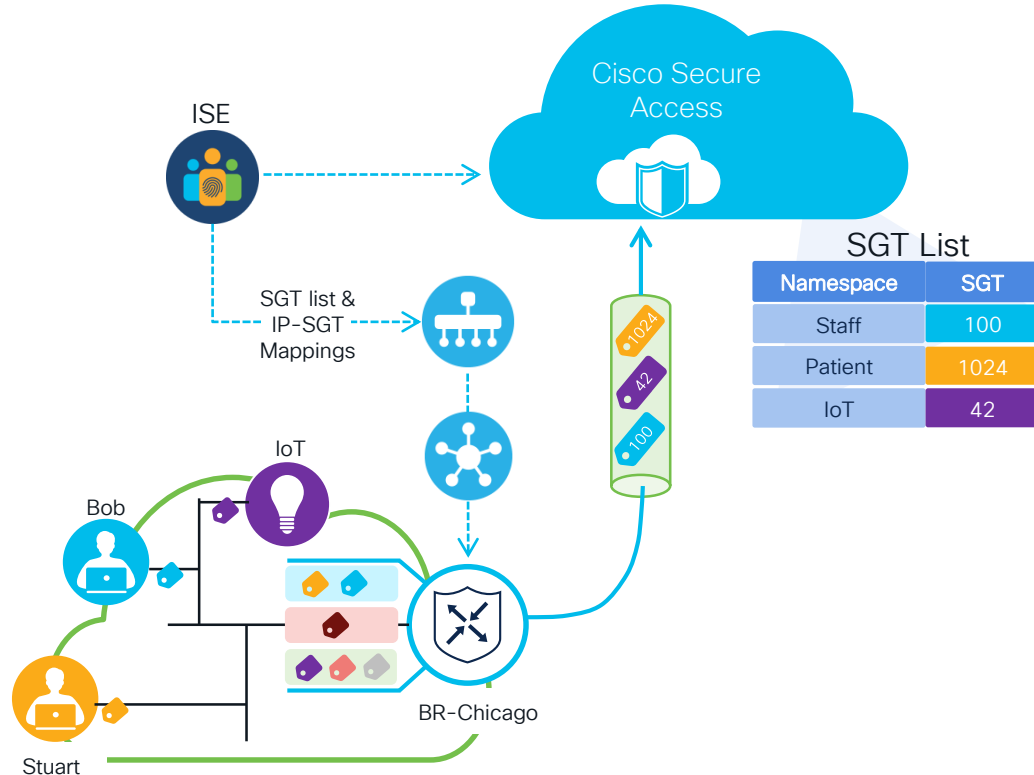


Adding Micro-Segmentation to Secure Access

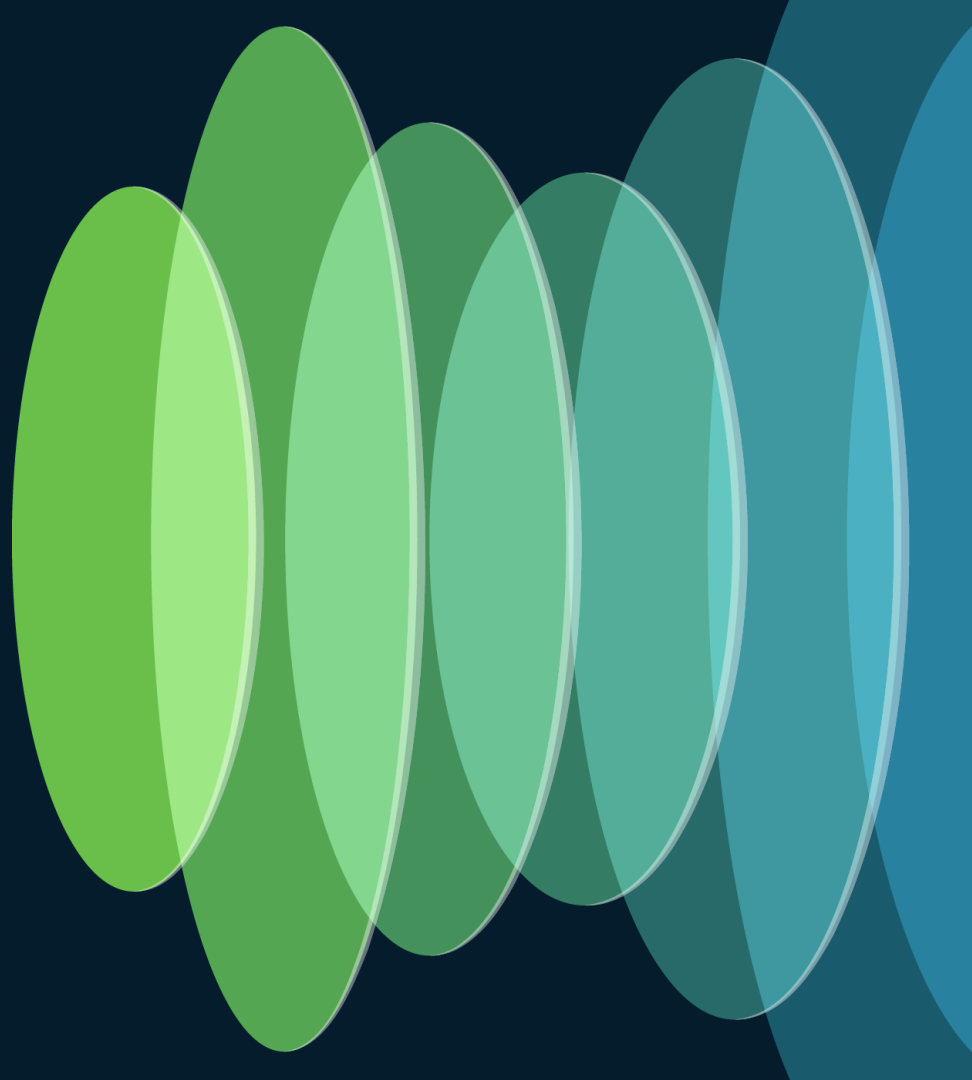
Coming with SD-WAN Release 20.15 / 17.15

Extend SGT segmentation to Secure Access

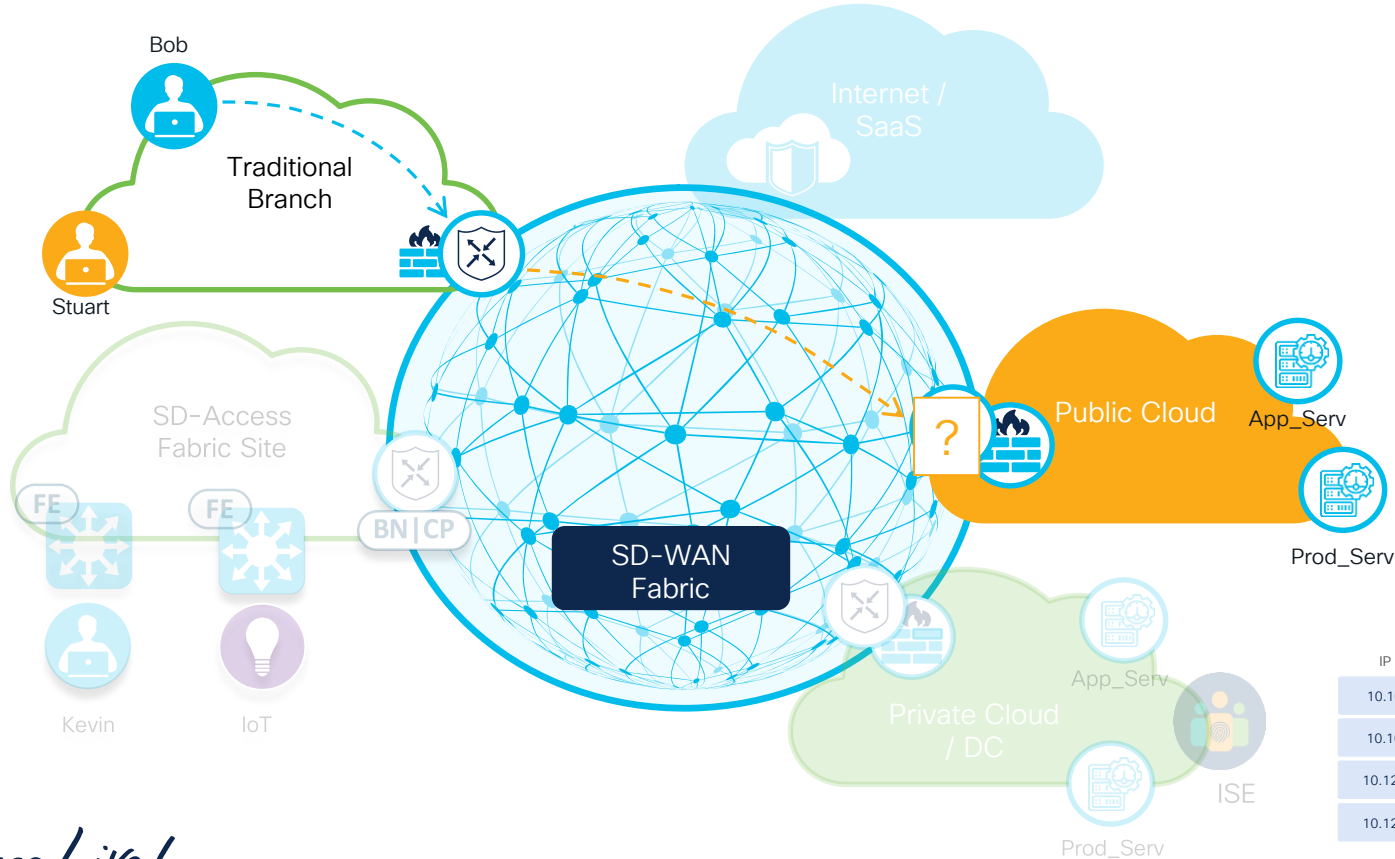
- Enables finer-grained internet access policies
- Apply separate SSE policies for VPN-ID / SGT across same IPSec tunnel
- ISE provides SGT list and mapping of IP-SGTs
- WAN interface propagates VPN-ID and SGT to Secure Access



Segment Cloud Workloads in CSPs



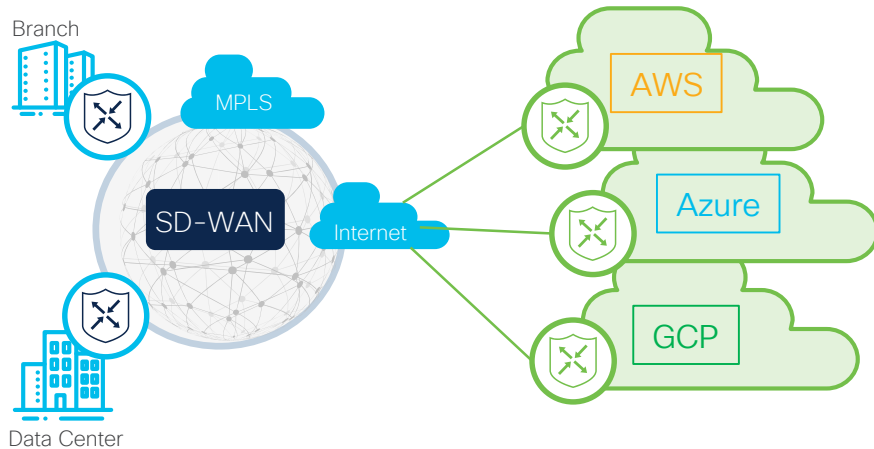
Dr. Bob Needs to Access Workload in CSP



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

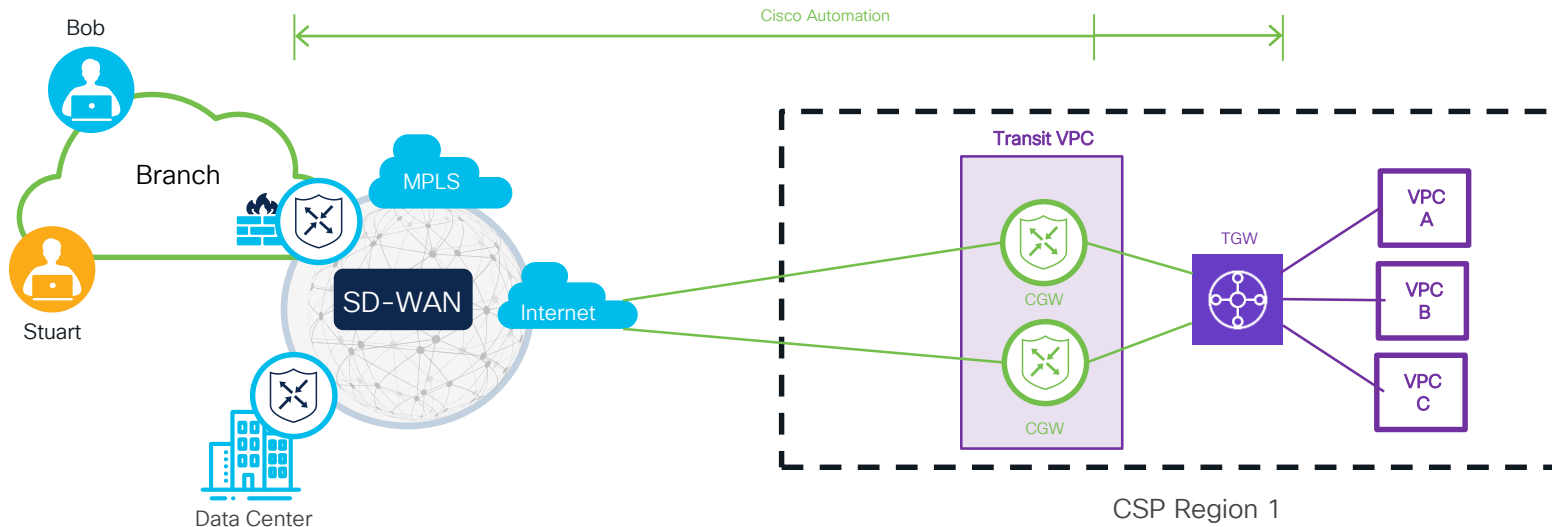
Simplify operations with one management plane

Enhance visibility for devices and circuits

Integrate multiple cloud providers

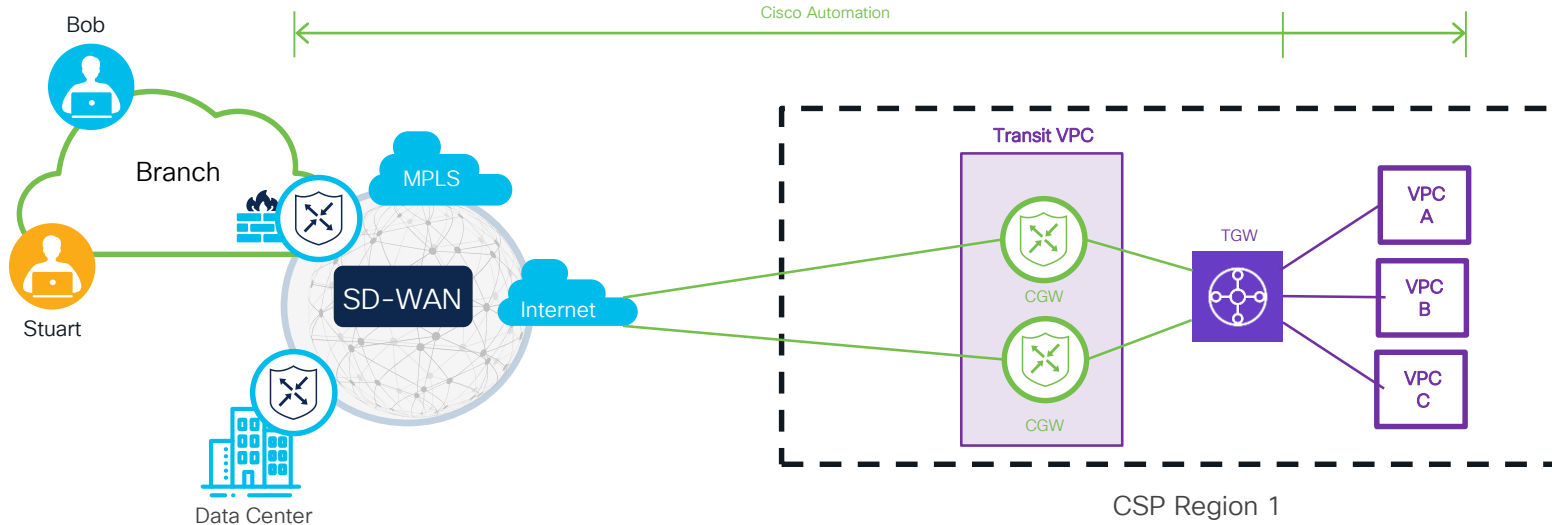
CSP Connection – Cloud GW

Automating AWS Transit GW Integration



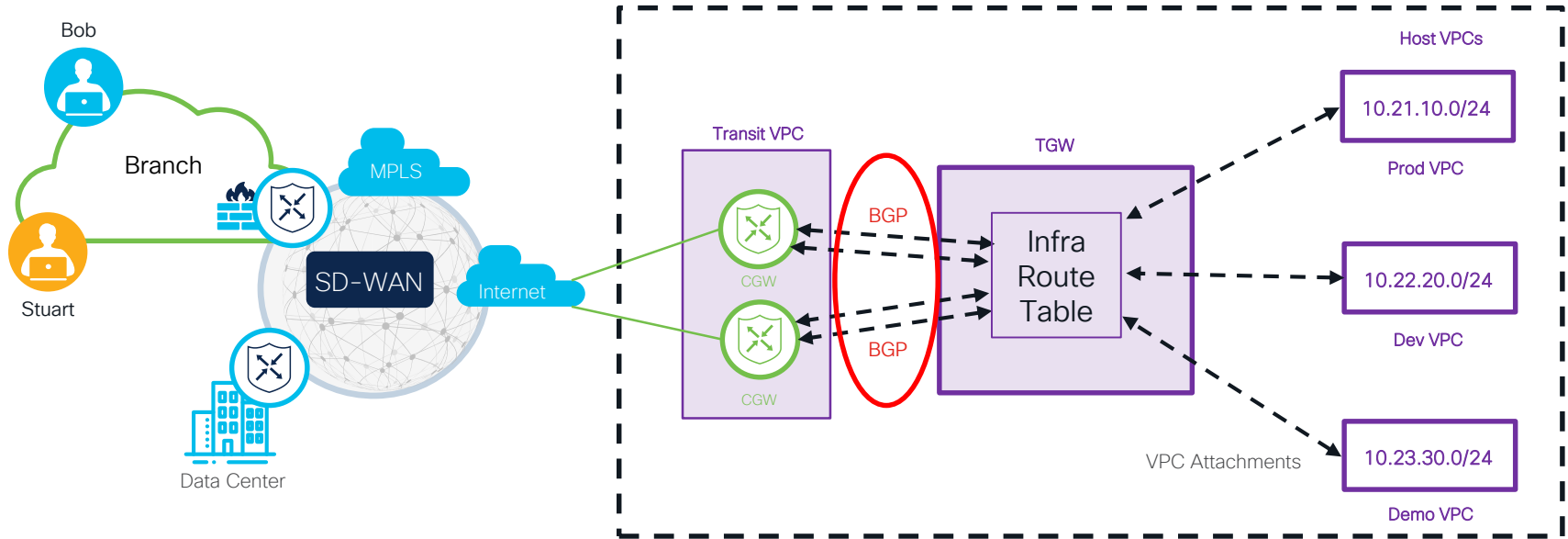
CSP Connection – Cloud GW

Automating AWS Transit GW Integration



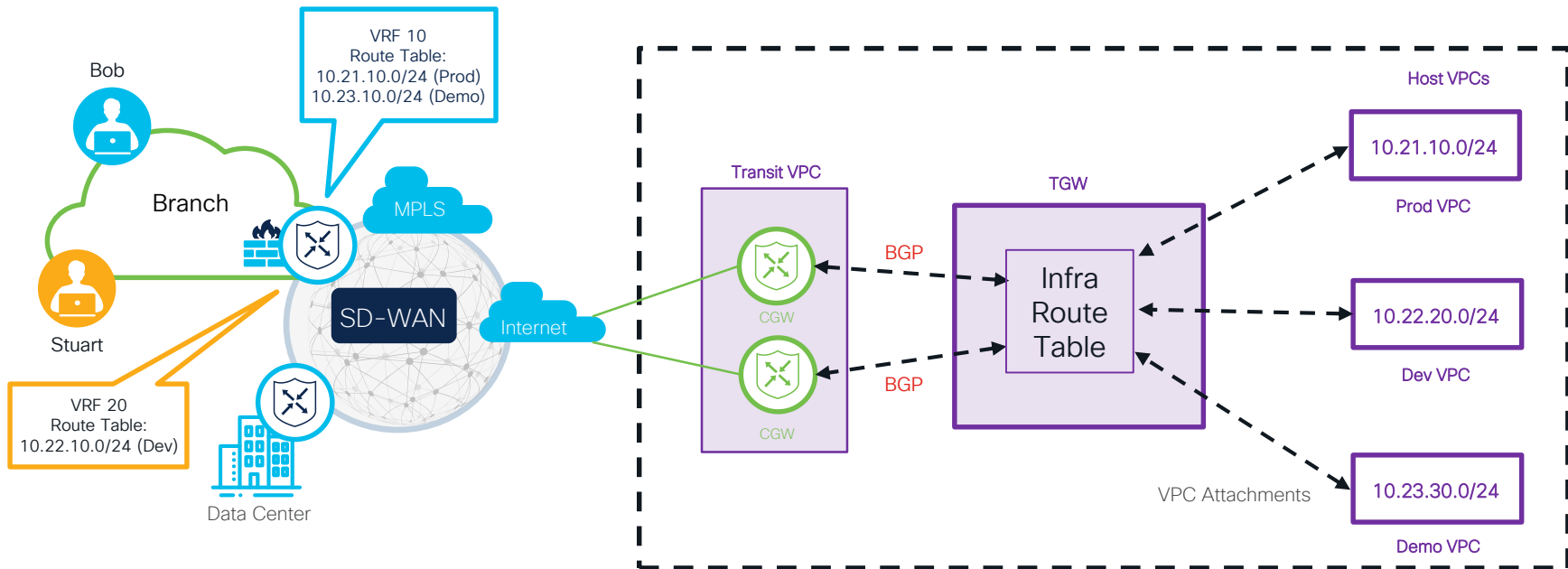
CSP Connection Example – Cloud GW

Dynamic Routing to Host VPCs



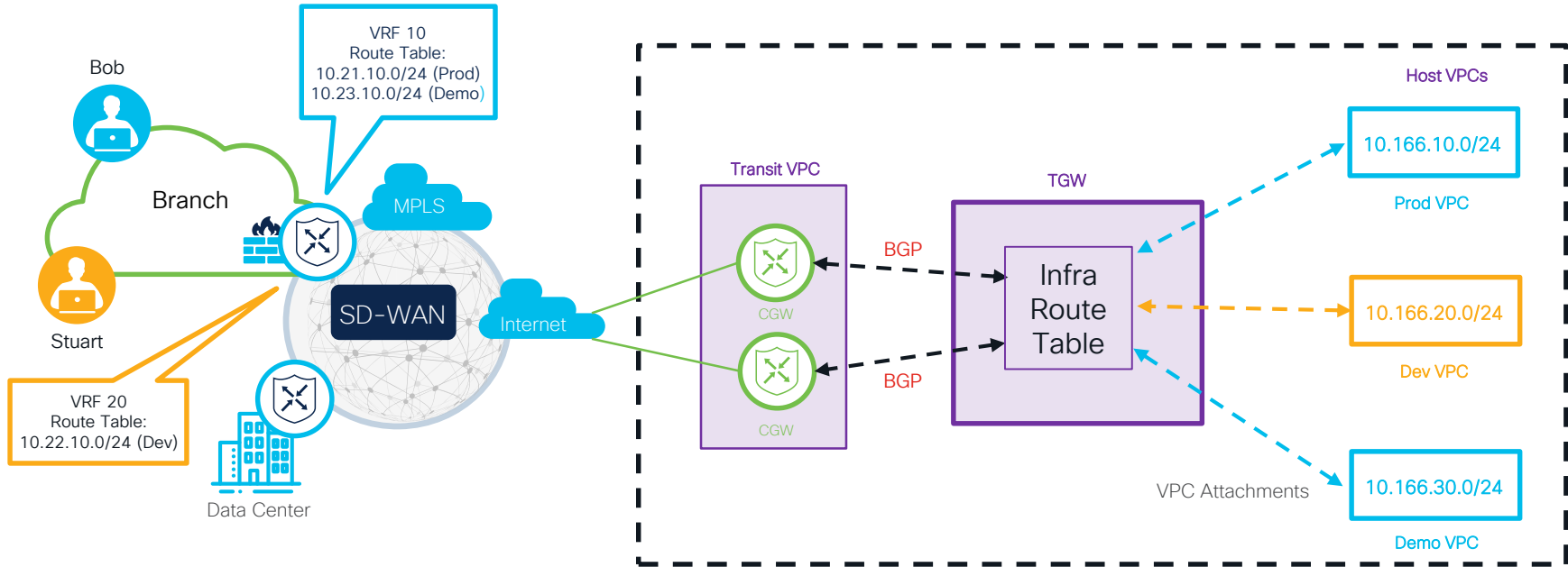
CSP Connection Example – Cloud GW

Segmenting Host VPCs to VPNs



CSP Connection Example – Cloud GW

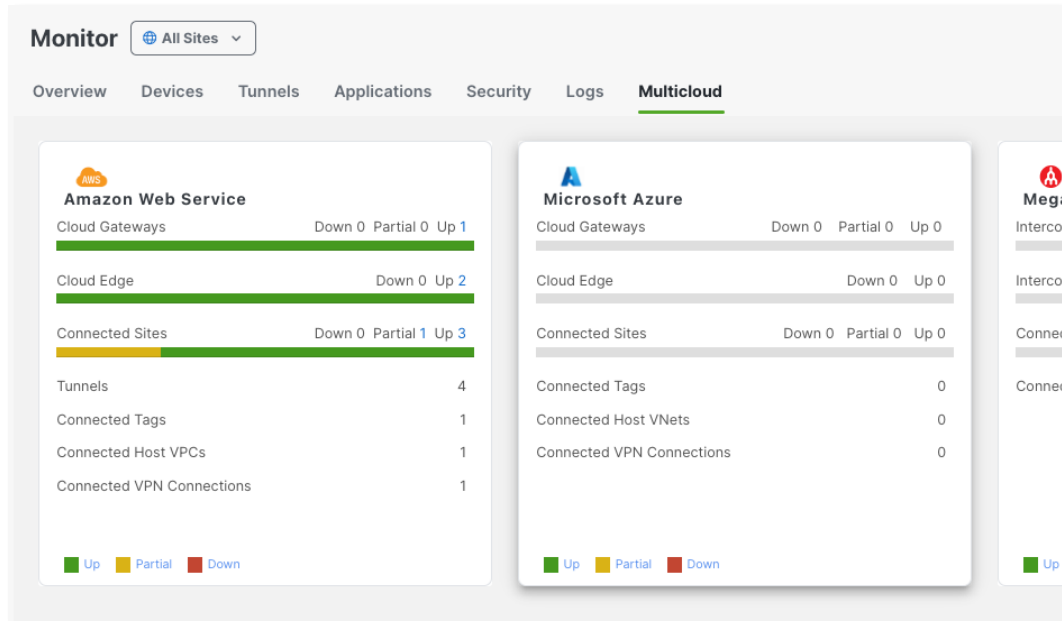
VPC Segmentation through Automation



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



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

The image displays three overlapping screenshots of the Catalyst SD-WAN Manager interface, illustrating the steps for configuring Cloud OnRamp for Multicloud.

Top Screenshot: Shows the 'Monitor' tab with a sidebar menu. The 'Cloud' option is highlighted with a red box and a red arrow pointing to it.

Middle Screenshot: Shows the 'Cloud' tab with a 'Network Snapshot' dropdown menu. The 'Cloud' option is highlighted with a red box and a red arrow pointing to it.

Bottom Screenshot: Shows the 'WORKFLOWS' section. The 'DISCOVER' workflow is highlighted with a red box and a red arrow pointing to it. The 'DISCOVER' workflow includes the step 'Host Private Networks'.

Table Data:

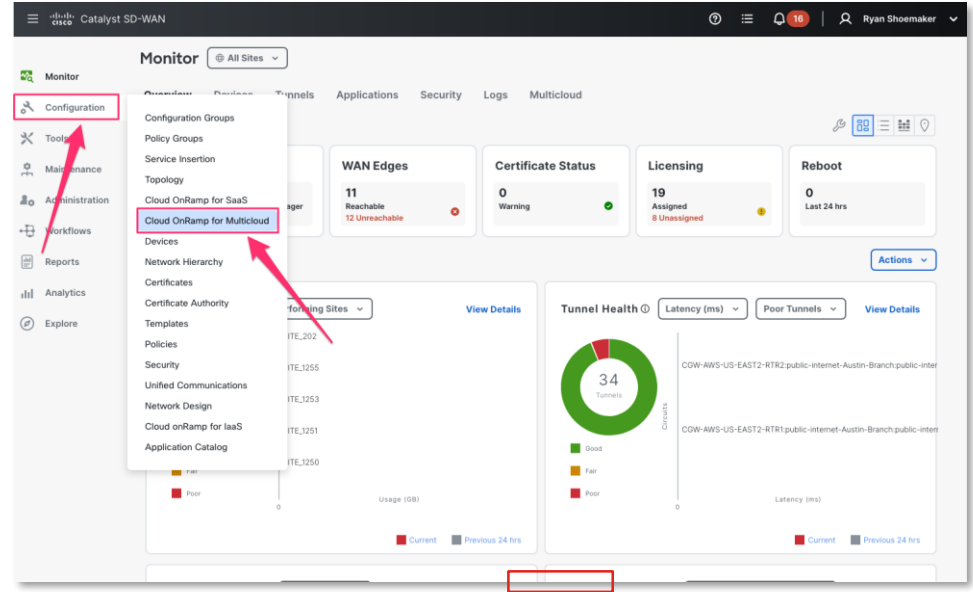
Cloud Type	Region	Account Name	Cloud Gateway Name/Azure Virtual WAN Hub	Health	Devices	Tunnel to Cloud WAN Core
AWS	us-east-2	AWS SASE Team	CGW-AWS-US-EAST2	✓	✓ 2 reachable	✓ 4 reachable

*Screenshots are of Catalyst SD-WAN Manager 20.13

Automating Cloud Extensions in SD-WAN

Cloud OnRamp for Multicloud*

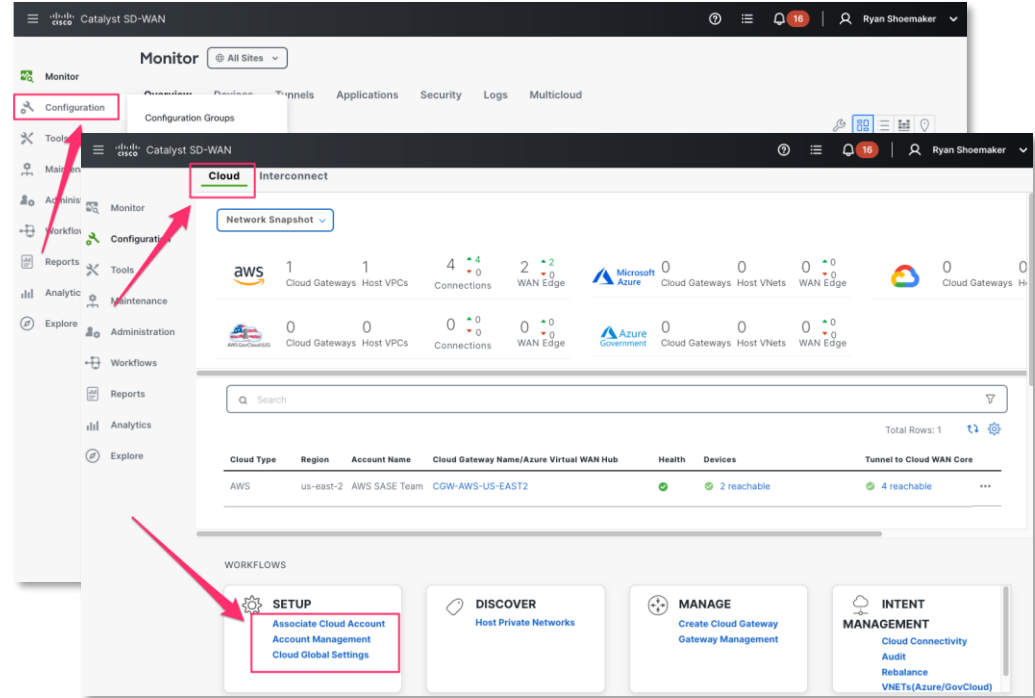
1. Select Cloud OnRamp for Multicloud



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

The image displays three overlapping screenshots of the Catalyst SD-WAN Manager interface, illustrating the steps to configure Cloud OnRamp for Multicloud. Red boxes and arrows highlight the navigation path: from the 'Configuration' menu to the 'Cloud' tab, then to the 'Discover' workflow.

Configuration Groups

Cloud Interconnect

Network Snapshot

Cloud Interconnect

Network Snapshot

Cloud Type	Region	Account Name	Cloud Gateway Name/Azure Virtual WAN Hub	Health	Devices	Tunnel to Cloud WAN Core
AWS	us-east-2	AWS SASE Team	CGW-AWS-US-EAST2	✓	✓ 2 reachable	✓ 4 reachable

WORKFLOWS

- SETUP**
Associate Cloud Account
Account Management
Cloud Global Settings
- DISCOVER**
Host Private Networks
- MANAGE**
Create Cloud Gateway
Gateway Management
- INTENT MANAGEMENT**
Cloud Connectivity
Audit
Rebalance

*Screenshots are of Catalyst SD-WAN Manager 20.13

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

Available host private networks have been discovered

Q CLEUR X Search

1 Rows Selected

Tag Actions

- Add Tag
- Edit Tag
- Delete Tag

☐	Cloud Region	
☐	eu-north-1	AWS SASE T
☐	eu-north-1	AWS SASE T
☒	eu-north-1	AWS SASE T

Add New Tag

Tag Name

Region

Selected VPCs

☐ Enable for SDCI partner Interconnect Connections (NOTE: this cannot be edited once enabled)

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)

Search Words

Configuration

Device Templates Feature Templates

Q **aws** x **tgw** x Search

Create Template ▾

Template Type **Non-Default** ▾ Total Rows: 1 of 36

Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode
From Default device template for AWS TGW C8000V	Feature	C8000v	SDWAN Edge	global	12	Disabled

Device Template | [SASE_AWS_TGW_C8000V_Template_V01](#)

Q Search ▾ Total Rows: 2

S...	Chassis Number	System IP	Hostname	Color(vpn_if_tunnel_color_value)	Hostname(hostname)	System IP(s)
✓	C8K-8D349E85-258B-6313-188A-C3...	-	-	public-internet	CLEUR24-CGW-AWS-EU-	2.1.1.1 ***
✓	C8K-40046C05-DDB7-5E72-B134-89...	-	-	public-internet	CLEUR24-CGW-AWS-EU-	2.1.1.2 ***

Setting parameters for CGW routers includes Site Id and System IP

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)

Push Feature Template Configuration | Validation success Initiated By: rshoemak From: 209.122.90.235

Total Task: 2 | Done - Scheduled : 2

Device Group (2)

Q Search Table

As of: Jan 23, 2024 11:04 AM

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	Action
Done - Scheduled	Device became unreachable...	C8K-8D349E85-258B-6313-188A-C30224B16881	C8000v	-	-	-	📄
Done - Scheduled	Device became unreachable...	C8K-40046C05-DOB7-5E72-B134-89F4A53CE9EE	C8000v	-	-	-	📄

After applying staging template, device becomes unreachable

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)

Cloud OnRamp for Multicloud > Cloud Gateway Management > Create Cloud Gateway

Manage Cloud Gateway - Create

Cloud

Cloud Provider:

Cloud Gateway Name:

Description (optional):

Account Name:

Region:

SSH Key (optional):

Site Name:

Note: * represents the settings fields that have been customized.

Instance Settings

Software Image: ☒ ☐

Instance Size:

IP Subnet Pool:

Tunnel Count:

UUID (specify 2):

Cancel Add

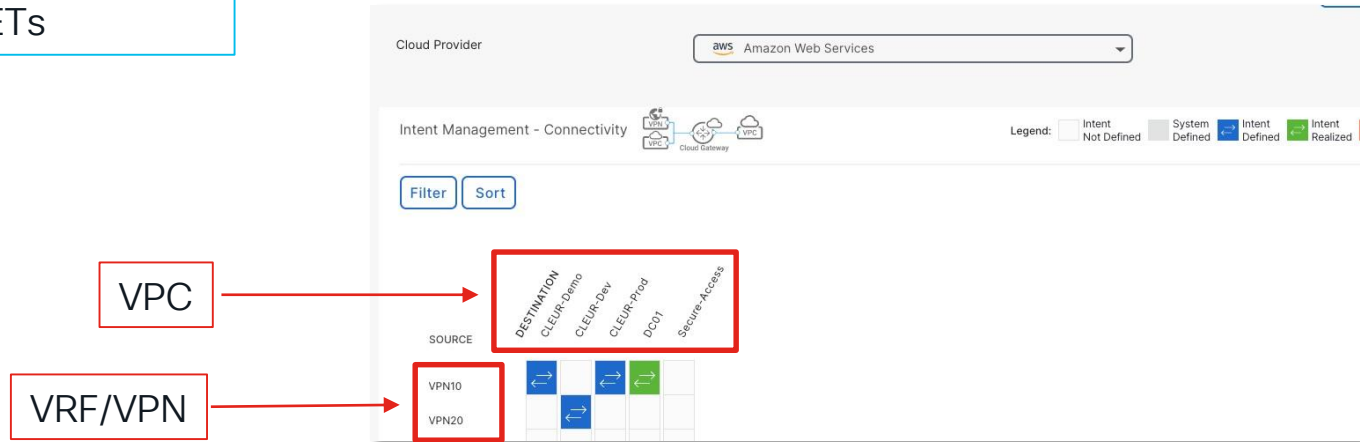
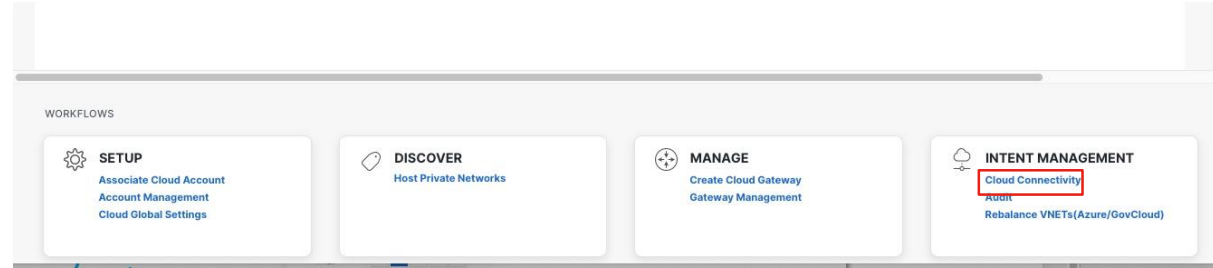
Diagram illustrating the Cloud Gateway architecture:

- Host VPC
- Cloud Gateway
- AWS Transit Gateway
- GRE Tunnel
- Transit VPC
- In Cloud Services Router
- Branches

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



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

Transit gateway attachment: tgw-attach-012a5a74fb4633249

Details

Flow logs

Connect Peers

Tags

Connect peers (2)

Filter connect peer

1

Actions

Create connect peer

Transit gateway ASN	Peer ASN	Peer BGP address	Transit gateway BGP 1 address	Transit gateway BGP 1 Status	Transit gateway BGP 2 address
65401	65430	169.254.3.169	169.254.3.170	Up	169.254.3.171
65401	65430	169.254.3.161	169.254.3.162	Up	169.254.3.163

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

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
    10.10.0.0 [251/0] via 1.1.97.2, 00:24:40, Sdwan-system-intf
    10.10.0.0 [251/0] via 1.1.97.1, 00:24:40, Sdwan-system-intf
    10.21.0.0 [20/100] via 169.254.3.171, 00:24:26
    10.21.0.0 [20/100] via 169.254.3.170, 00:24:26
    10.21.0.0 [20/100] via 169.254.3.163, 00:24:26
    10.21.0.0 [20/100] via 169.254.3.162, 00:24:26
    10.23.0.0 [20/100] via 169.254.3.171, 00:24:26
    10.23.0.0 [20/100] via 169.254.3.170, 00:24:26
    10.23.0.0 [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

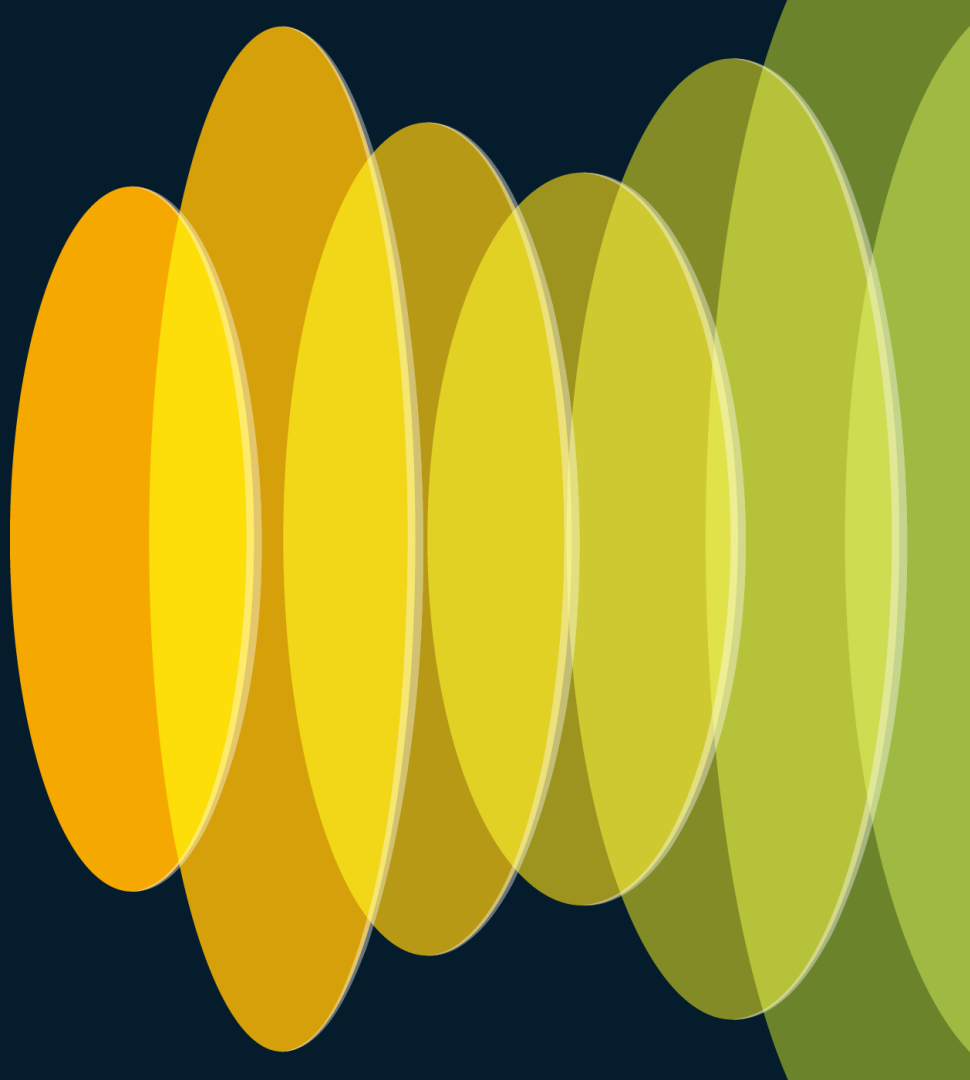
Routing Table: 20
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       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

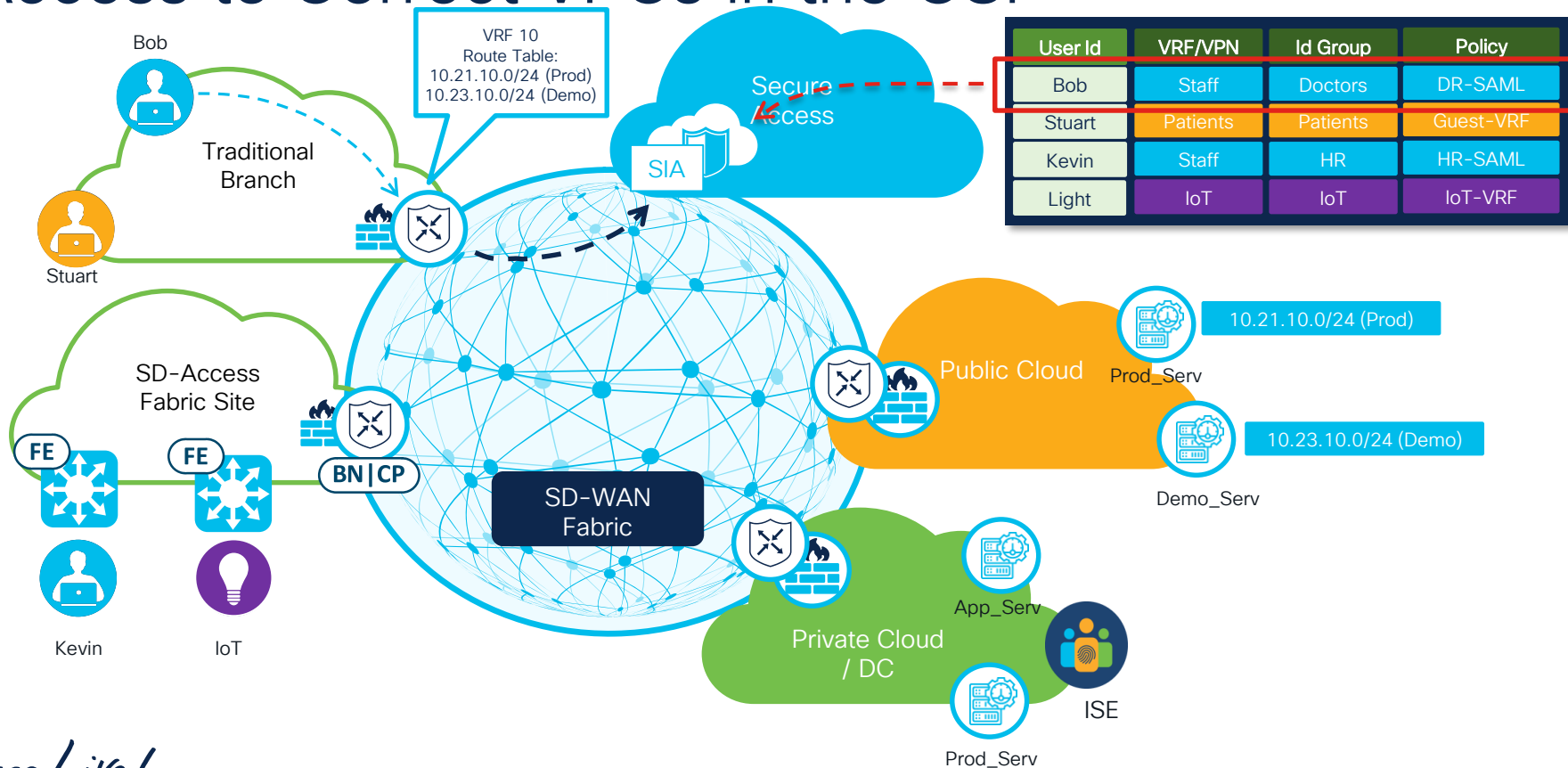
10.0.0.0/16 is subnetted, 1 subnets
    10.22.0.0 [20/100] via 169.254.3.235, 00:25:08
    10.22.0.0 [20/100] via 169.254.3.234, 00:25:08
    10.22.0.0 [20/100] via 169.254.3.227, 00:25:08
    10.22.0.0 [20/100] via 169.254.3.226, 00:25:08
```

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