

Elevating the Security in your SD-WAN

BRKENT-2708

Jeff Fanelli
Distinguished Engineer

CISCO Live !

Session Abstract

In this session, we will explore Cisco's robust secure SD-WAN capabilities in the Catalyst, Meraki MX and Secure Firewall branch platforms. The most common deployment use cases of each will be covered, in an effort to guide customers to the perfect capabilities matched for their environment.

This session will not be an exhaustive deep dive into all the features of our SD-WAN offerings!

Cisco Webex App

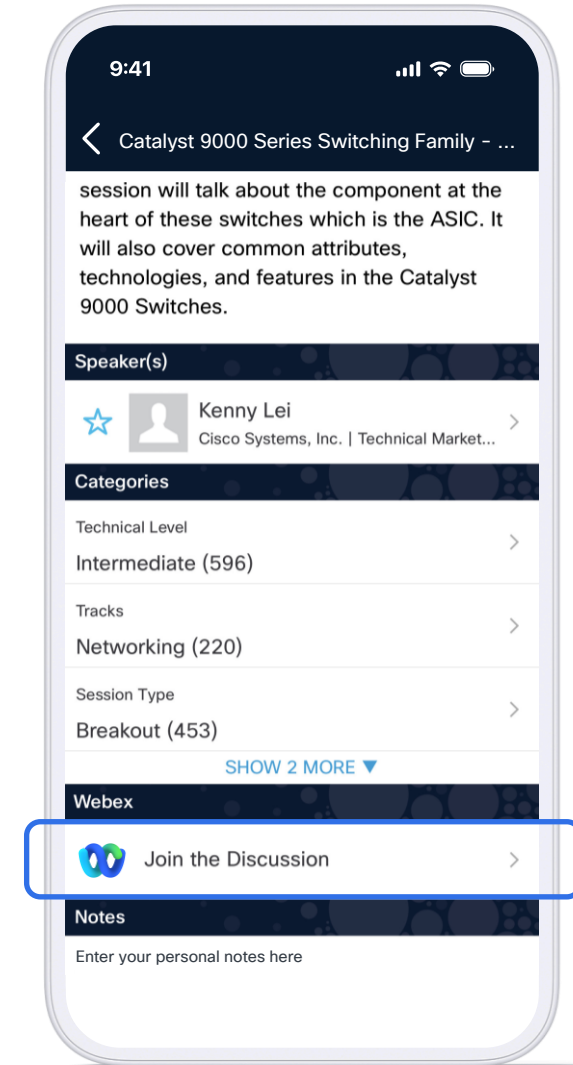
Questions?

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 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2708>

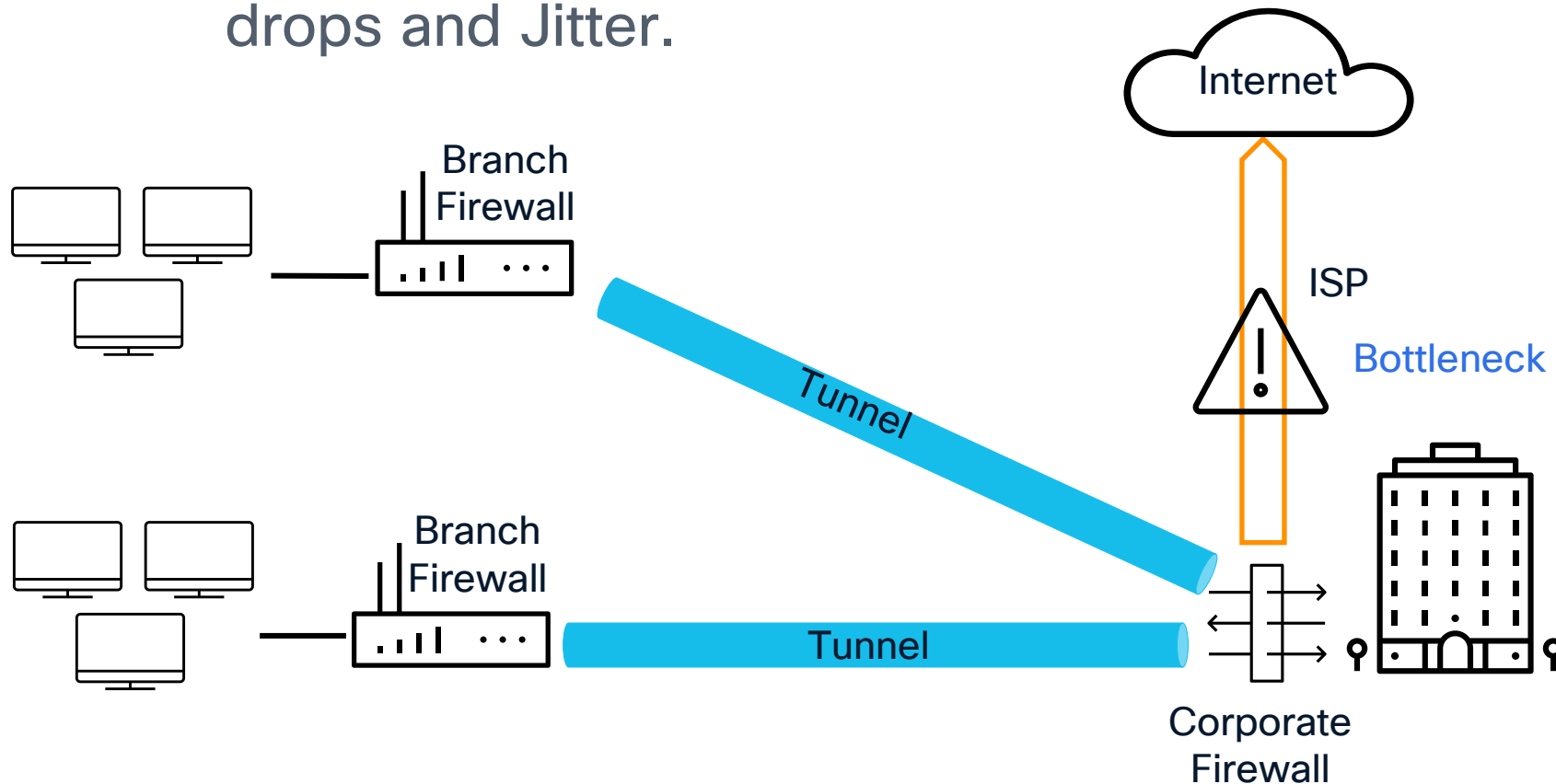
Agenda

- 01 SD-WAN Basics
- 02 Platform use cases:
- 03 Catalyst SD-WAN
- 04 Meraki MX
- 05 Firewall Threat Defense
- 06 SSE / SASE integration
- 07 Summary

SD-WAN Basics

Traditional WAN Architecture

Traditional WAN topology backhauls **all internet traffic** to the enterprise Data center, resulting in **poor application experience**, Packet Latency, drops and Jitter.

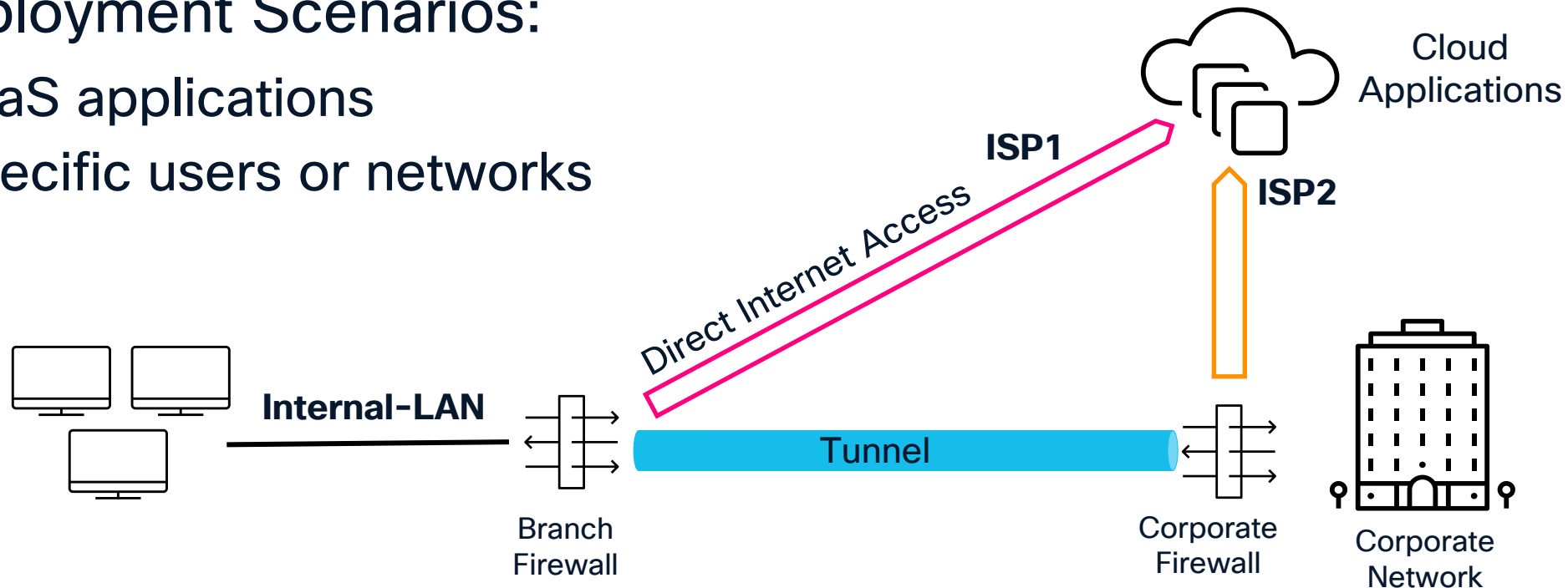


Direct Internet Access (DIA)

Routing traffic directly out to the internet rather than backhaul to central site

Deployment Scenarios:

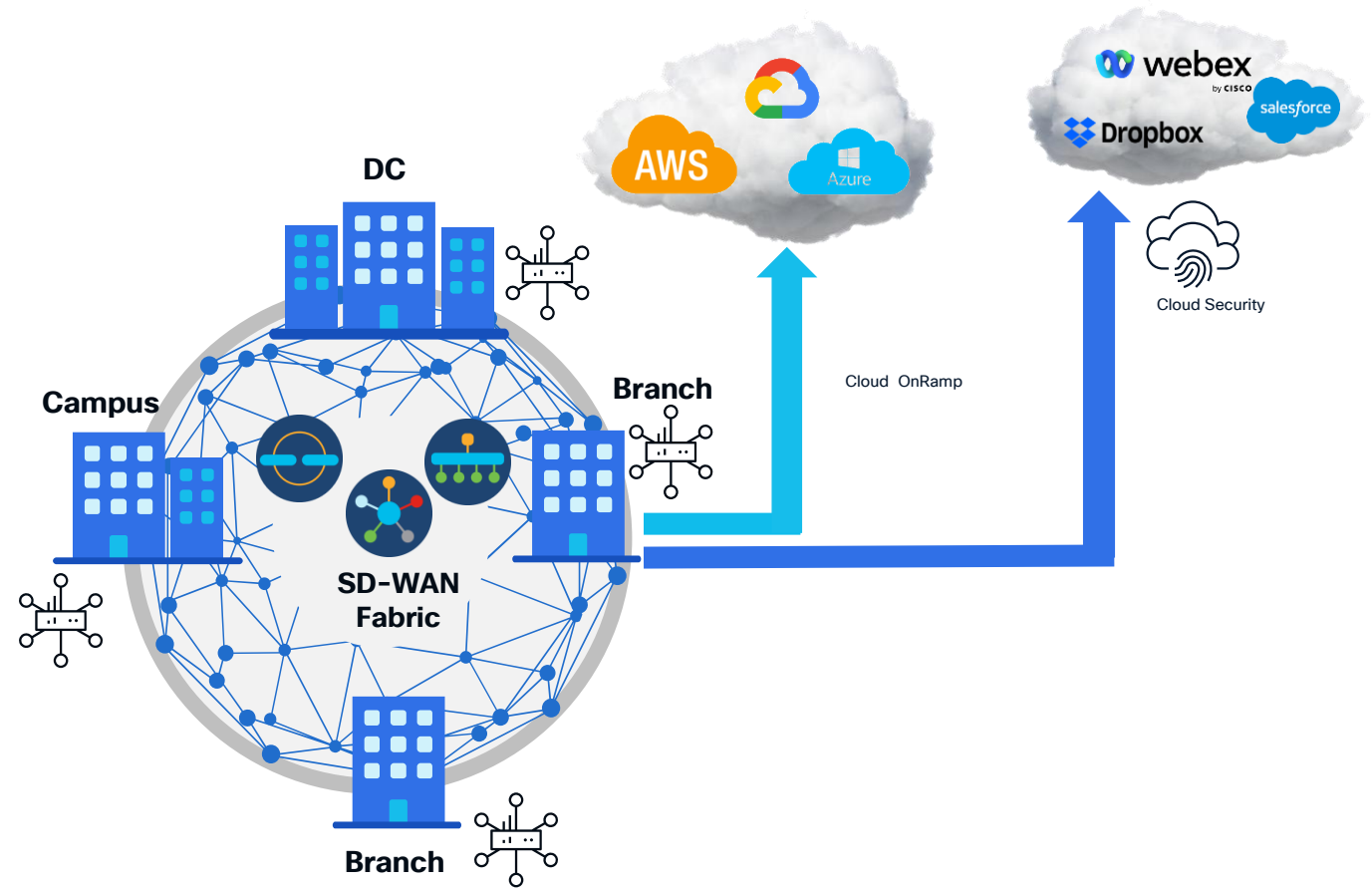
- SaaS applications
- Specific users or networks



Software-Defined Wide Area Network

Offers centralized control of network devices, **dynamic management** of network traffic and (VPN) tunnels.

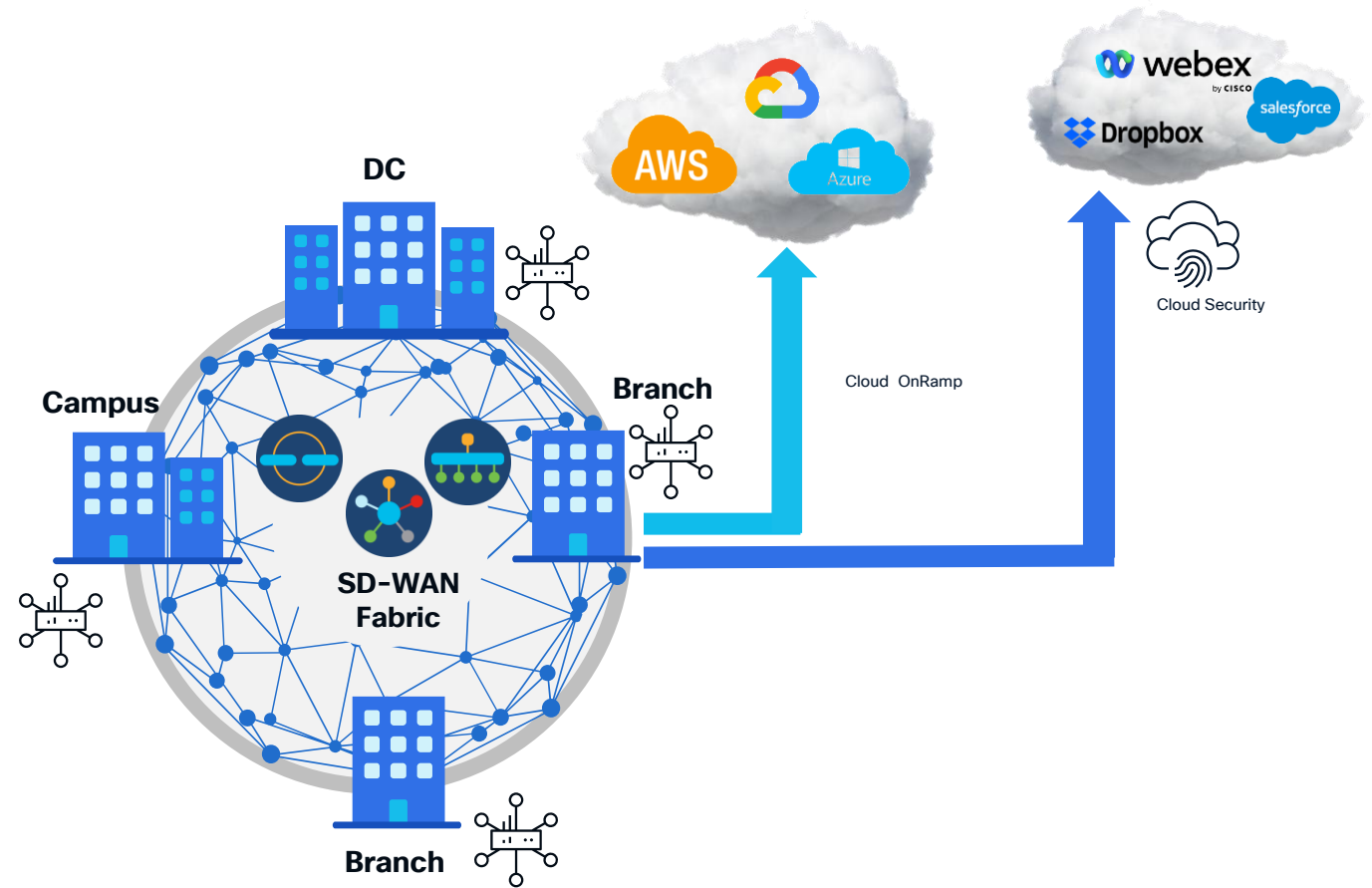
Software defined control of routing based on application performance and other metrics.



What Software-Defined Internet?

Policy based automation to optimize the use of multiple Internet connections.
Can include:

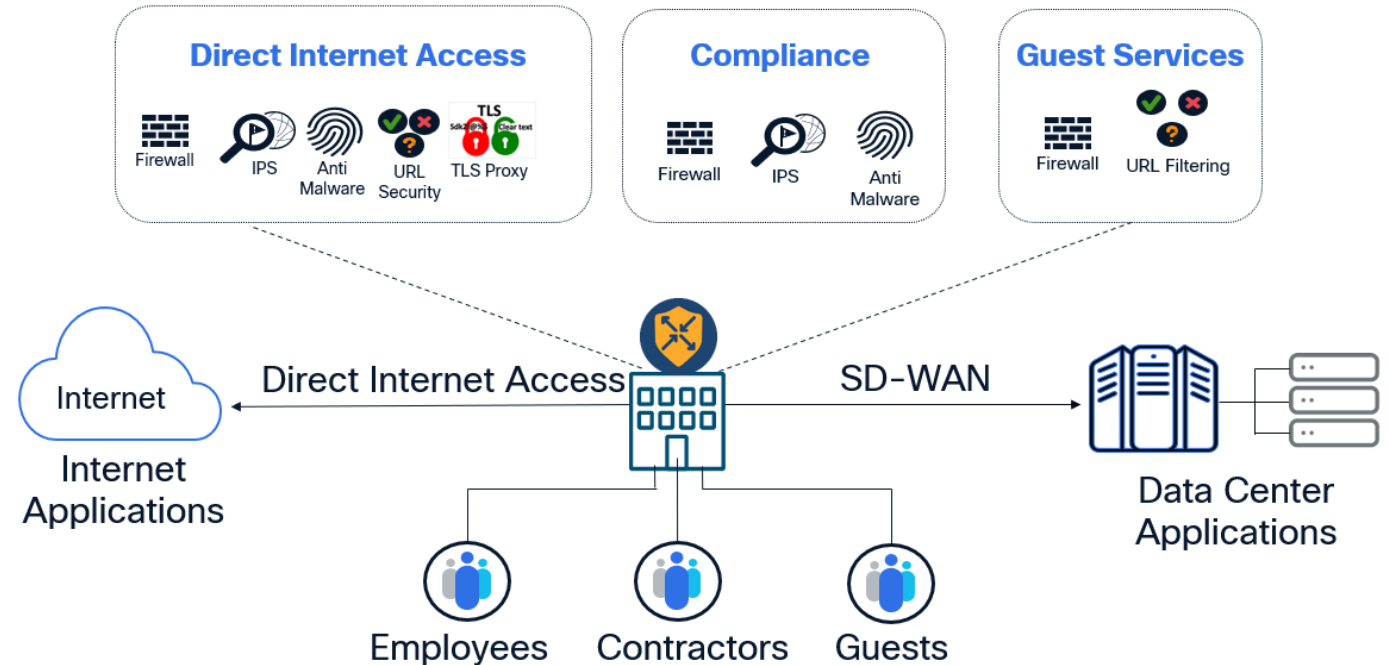
- Bandwidth aggregation
- Auto path failover during congestion or loss
- Prioritization of critical traffic over high(er) quality links



Why Secure SD-WAN?

Enforce security policies as close to users / clients as possible.

- Identity-based NGFW for least privileged access
- DNS inspection & URL filtering
- Threat inspection (IPS, decryption etc.)

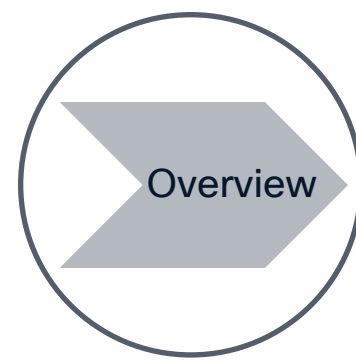
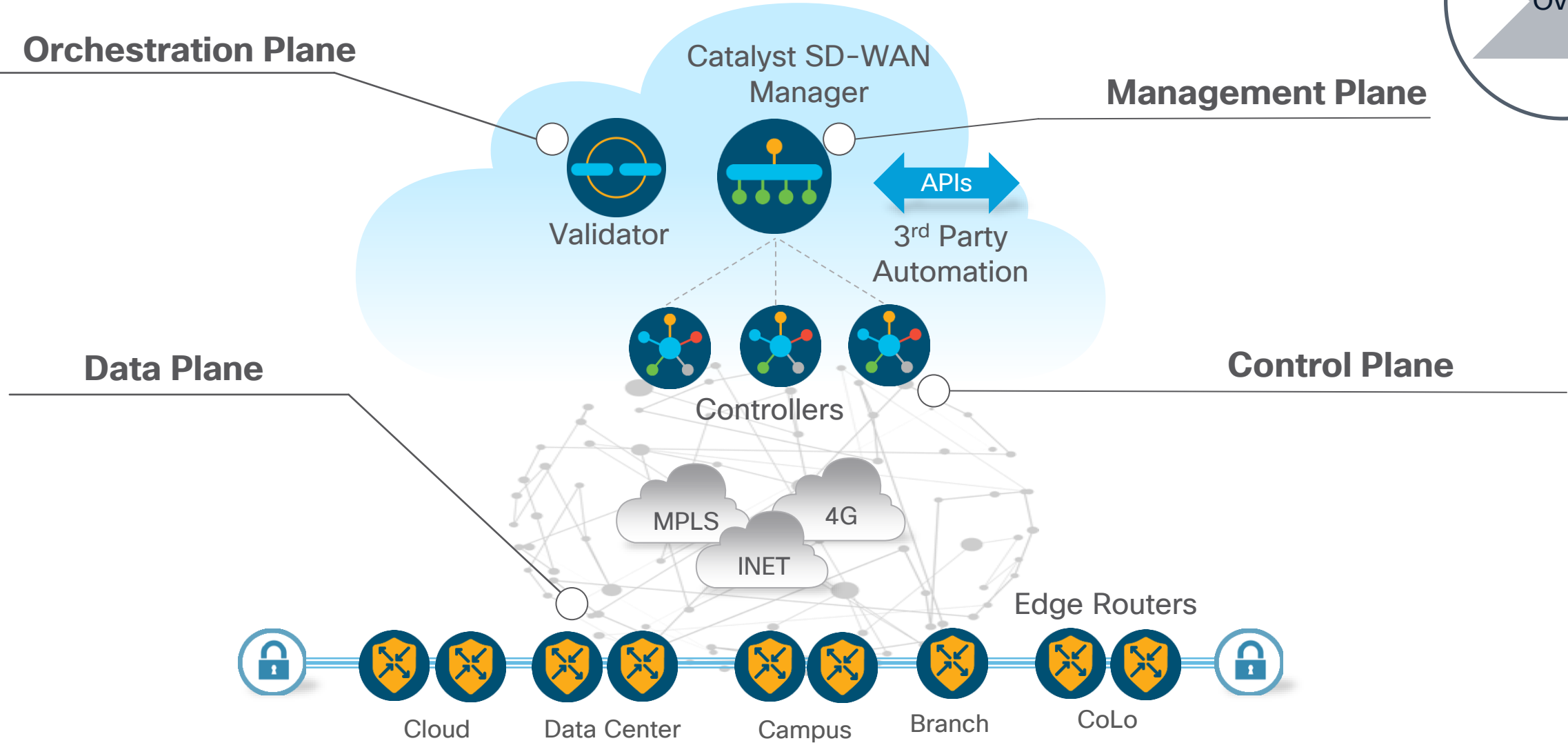


Catalyst SD-WAN Use Cases & Capabilities

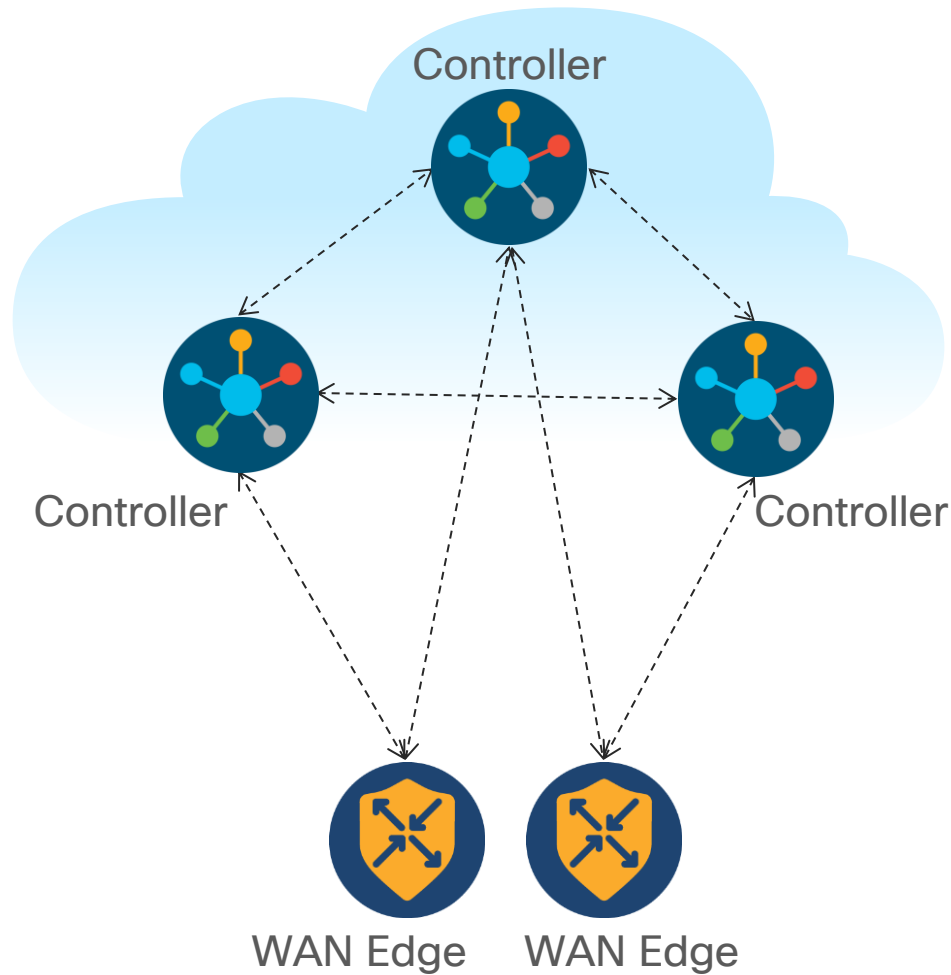
Use Case Flow



Catalyst SD-WAN Architecture

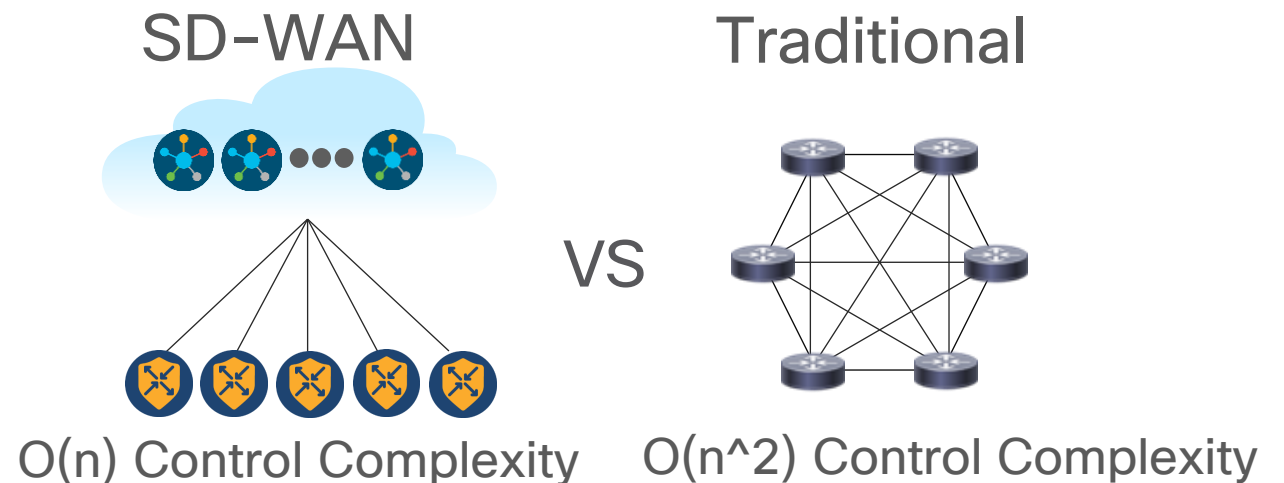


Overlay Management Protocol (OMP)



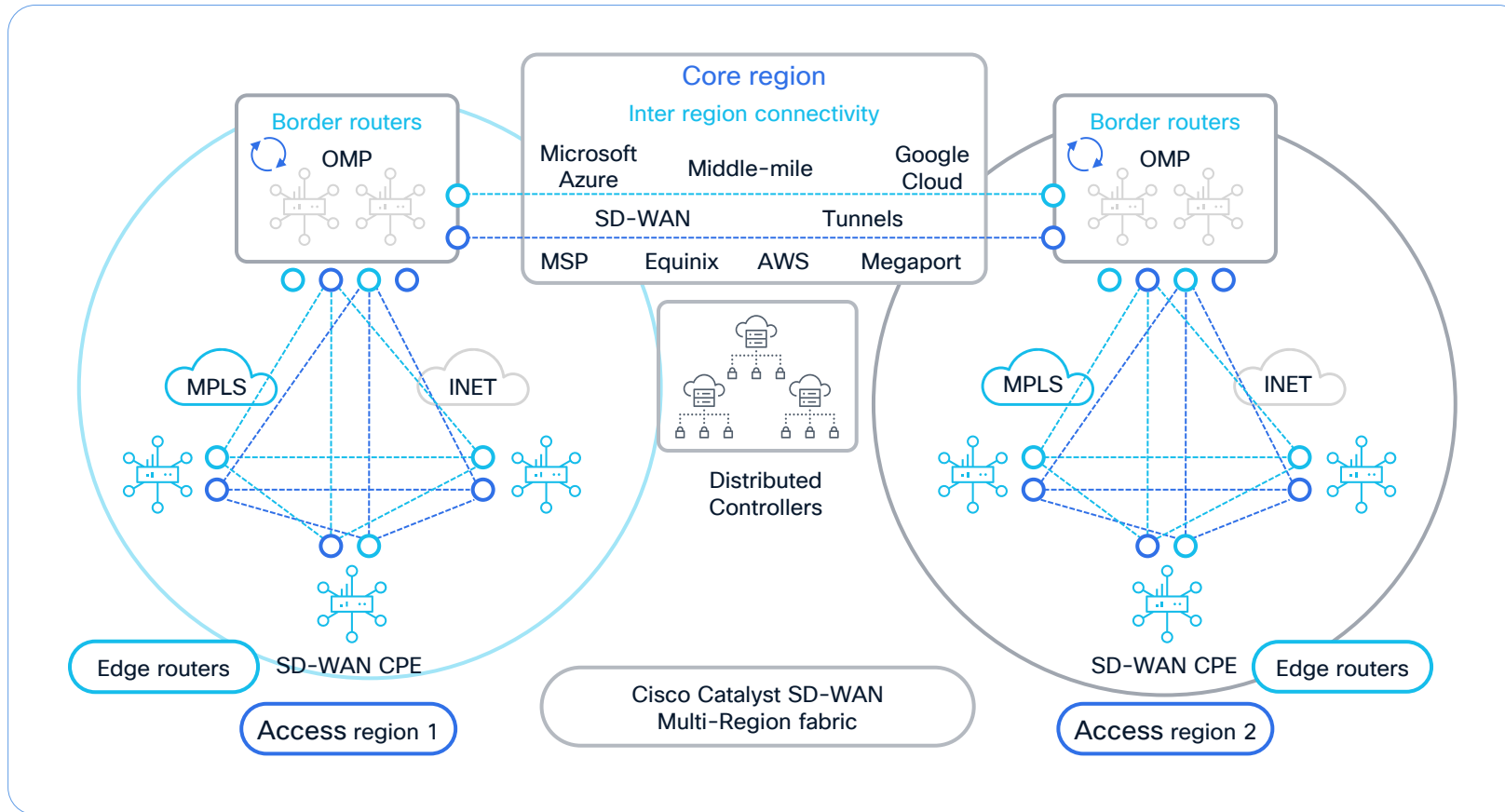
Note: WAN Edge routers need not connect to all Controllers

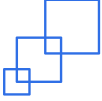
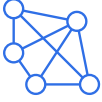
- Overlay Management Protocol (OMP)
- Runs between WAN Edge routers and Controller and between the Controllers
 - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
- Dramatically lowers control plane complexity and raises overall solution scale



Catalyst SD-WAN Multi-Region Fabric

SD-WAN evolved for any middle-mile topology

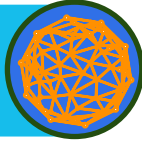


-  Eliminate lengthy global network policies
-  Automatic hop-by-hop inter-region routing
-  Scalable design
-  Simpler redundancy planning
-  Flexible architecture to cater to dynamic network needs
-  Operationally easier to deploy and manage

Catalyst SD-WAN Security Capabilities



Fabric Security



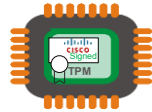
Encrypted
Control Plane



Encrypted
Data Plane



Enhanced
Security -
Pairwise keys



HW Based Device
Authentication
(SUDI)

Sec-Ops Monitoring & Visibility



Manager SecOps
Dashboard

splunk>

LiveAction

End-to-End Monitoring
& Visibility

Embedded Security



Firewall
Stateful
ZBFW



AMP
File Reputation &
Sandboxing from
Talos



URL Filtering
82+ Web Categories



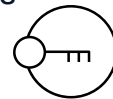
Segmentation
With Multi-
Topology



IPS
Protection
against
complex threats



**Unified Policy &
Logging**



Zero Trust

Cloud Security



DNS security



IPsec/GRE Tunnel
Connection



Simplified
Configuration



Traffic Steering
Policies



Traffic Load
Balancing
(ECMP)



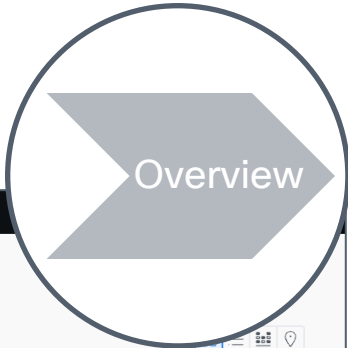
Layer-7 Health
Check

Cisco Secure Access



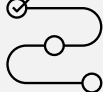
Third Party SSE

Catalyst SD-WAN Manager (UI)





Enhanced UI



Guided Workflow



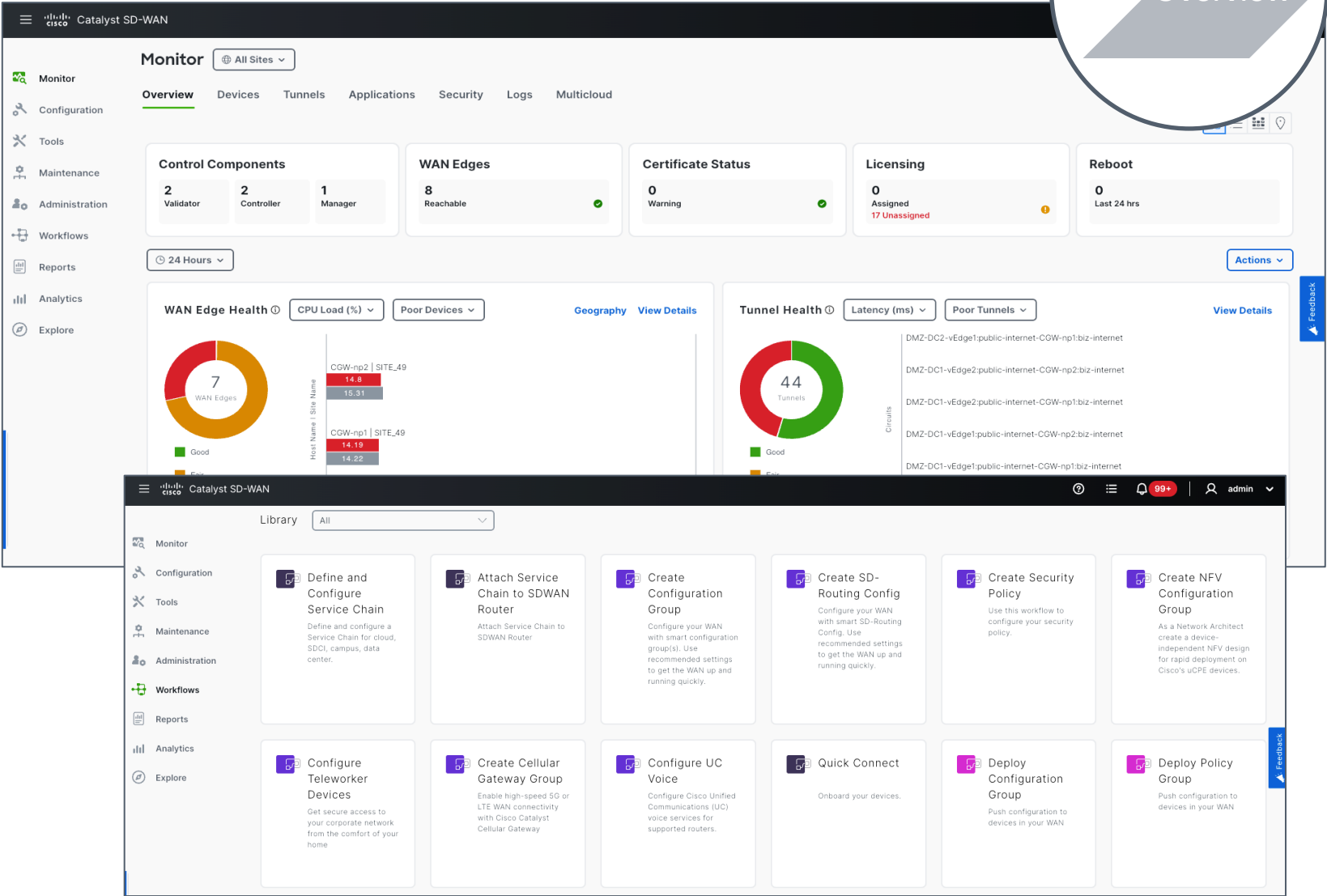
Simplified Configuration



Granular Management

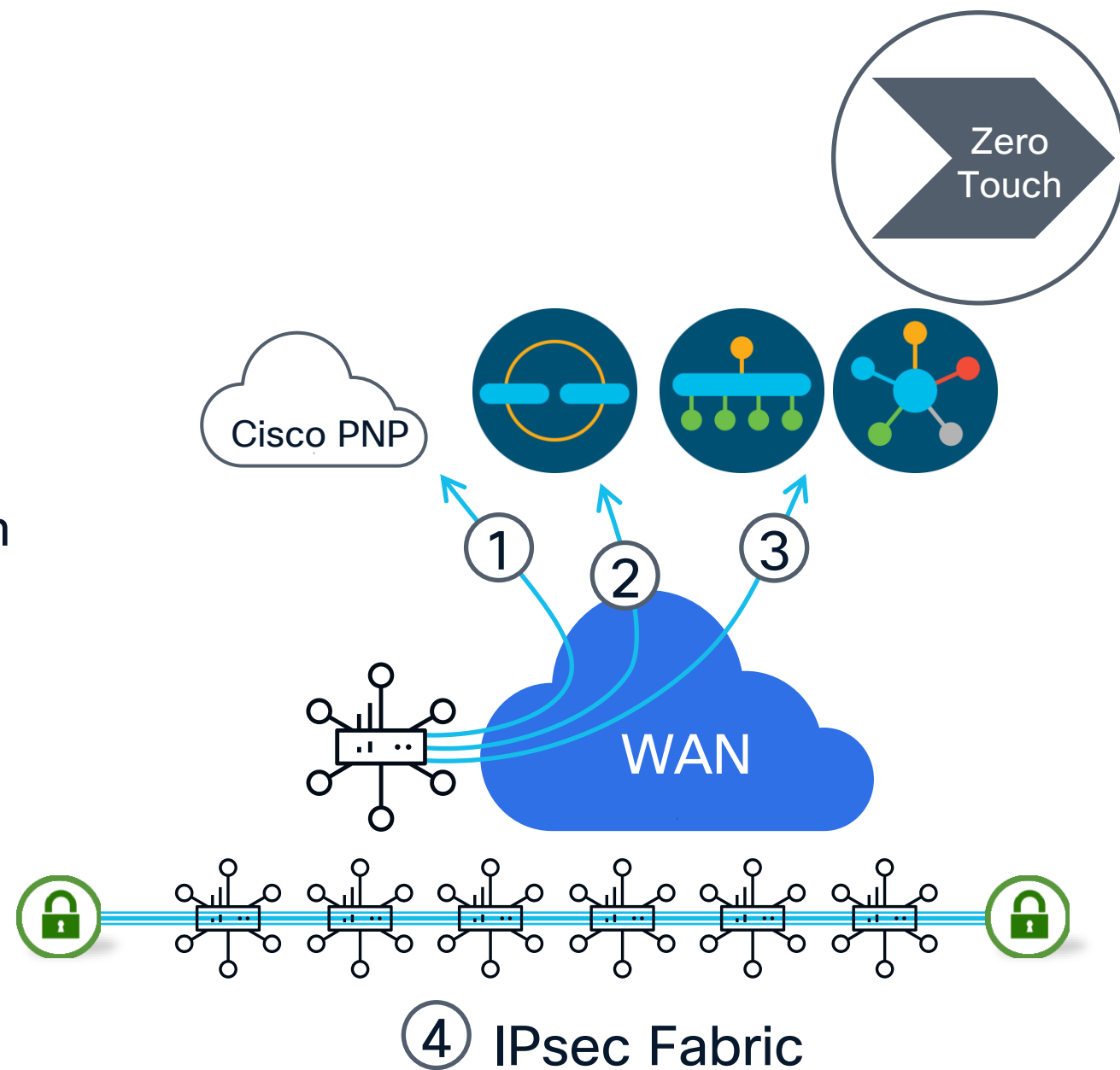


Smart Troubleshooting



Zero-Touch Provisioning

- Onboard the SD-WAN device to join SD-WAN fabric automatically.
- Use DHCP IP and DNS information from ISP to reach the PNP server .
- Ensures establishment of secure connection to controllers during the onboarding process.
- Policy can apply static IP addresses



Application Experience



Configuration Management System

Manager – Virtualized | Scalable | Network Insights

Forward Error Correction

Packet Duplication

```
110 110
1011 1011
010 010

110 110
1011 1011
010 010
```

TCP Optimization

BBR2 Congestion Algorithm

Window Scaling

Large Initial Windows

Selective Acknowledgement

DRE, LZW

Byte Level Caching & Compression

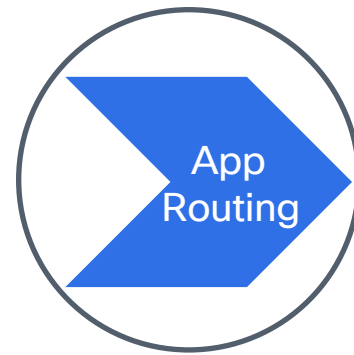
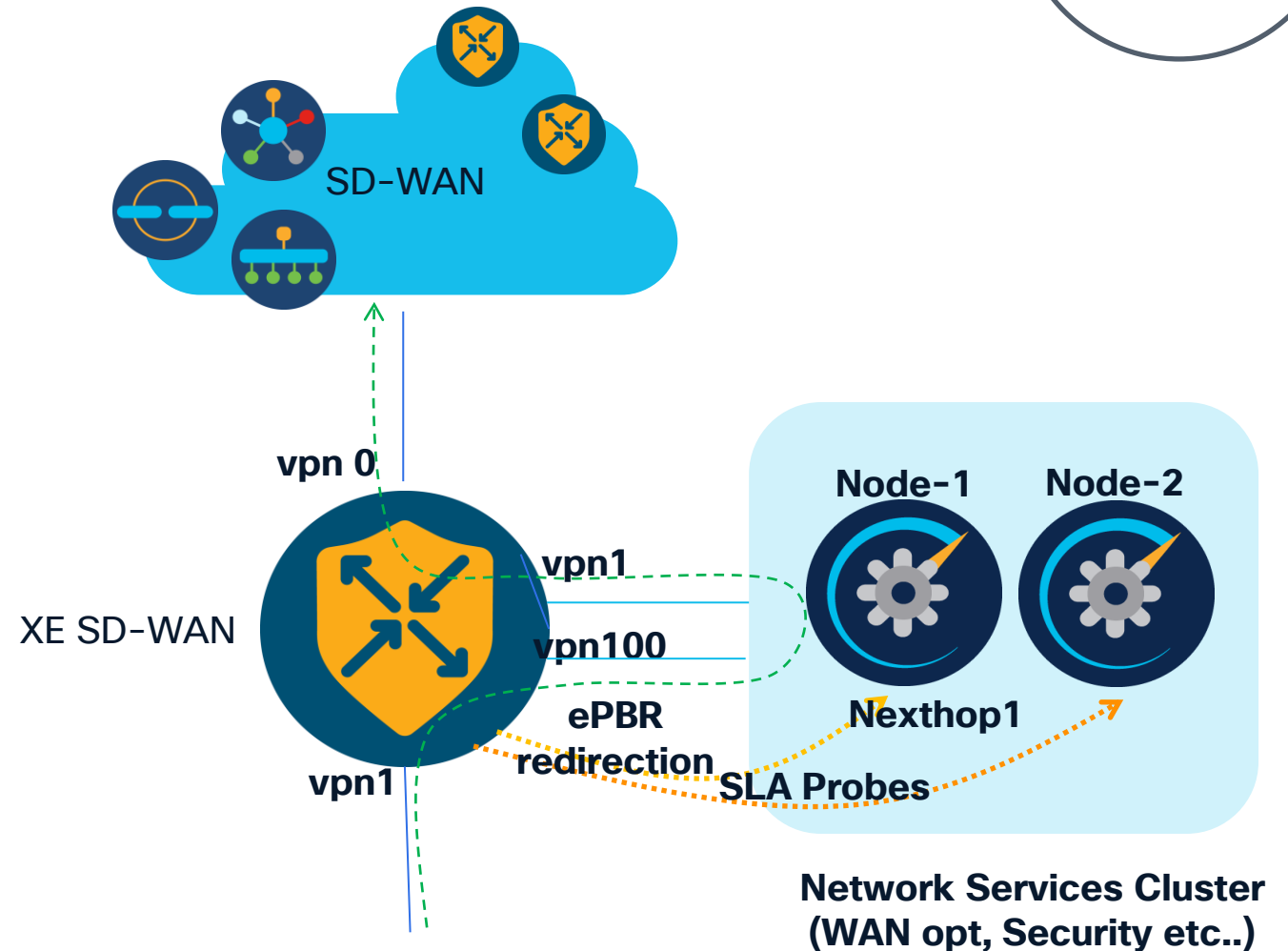
Protocol Agnostic

Key building blocks

BBR – Bottleneck Bandwidth and Round-trip propagation time

Service Insertion (Application Aware Routing)

- Classify traffic based on Prefix, SGT, Apps
- Configure SLA probe (optional)
- Set next hop in policy map
- Apply policy map on incoming interface

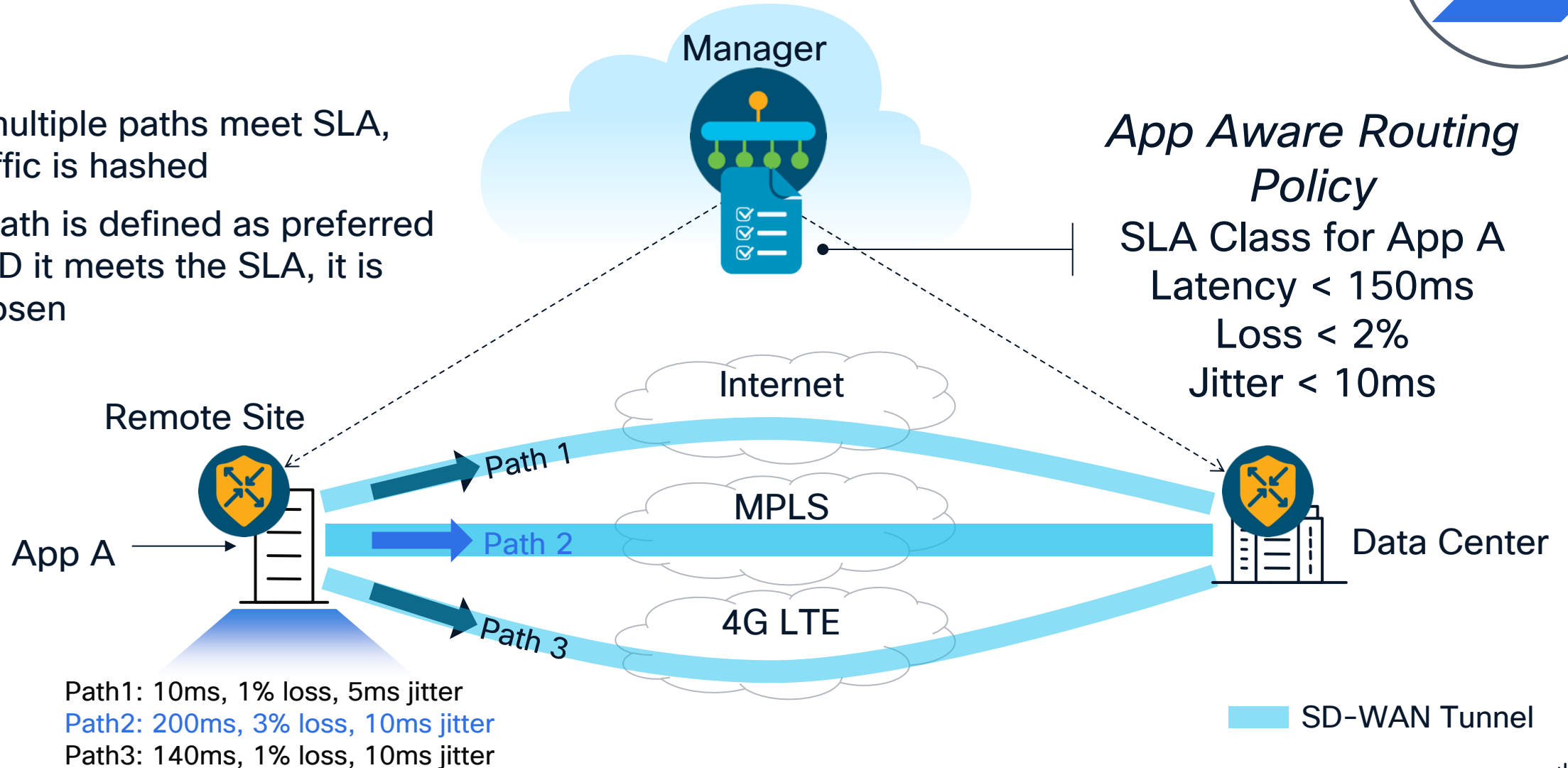


Enhanced Application-Aware Routing

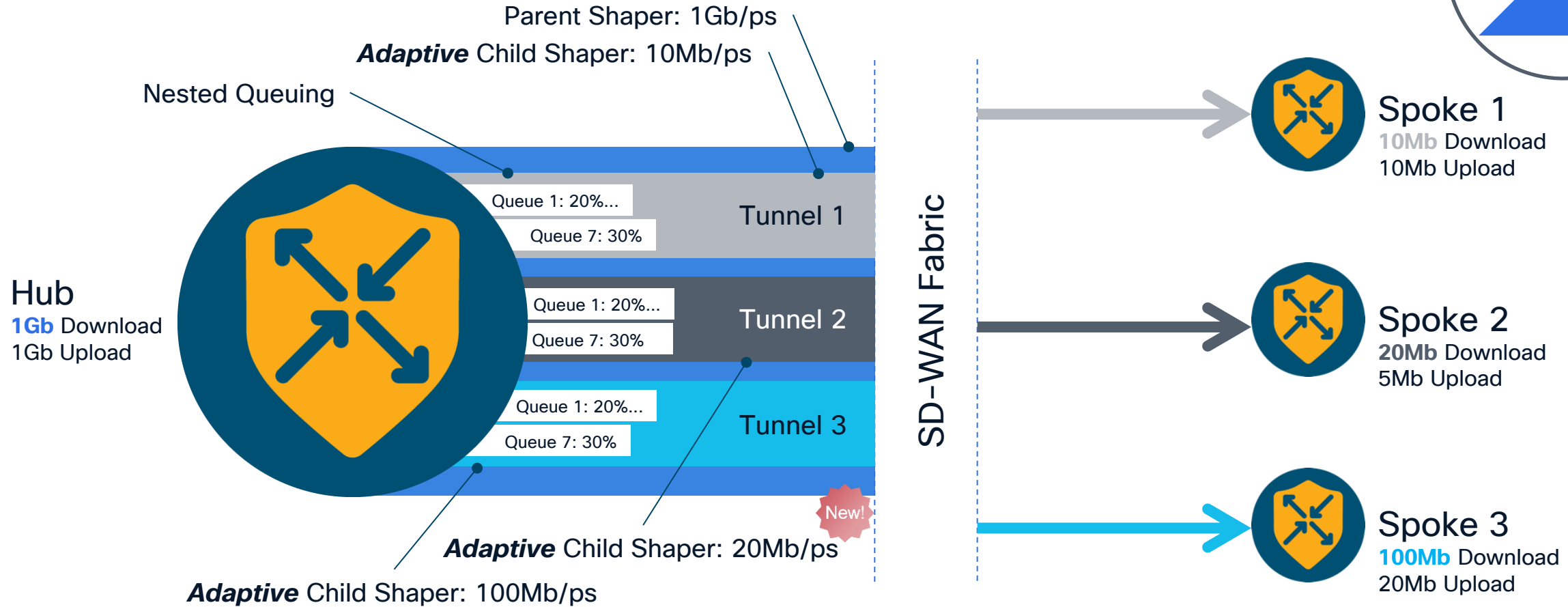
Improved Application Performance Experience (from mins to sec)



- If multiple paths meet SLA, traffic is hashed
- If path is defined as preferred AND it meets the SLA, it is chosen



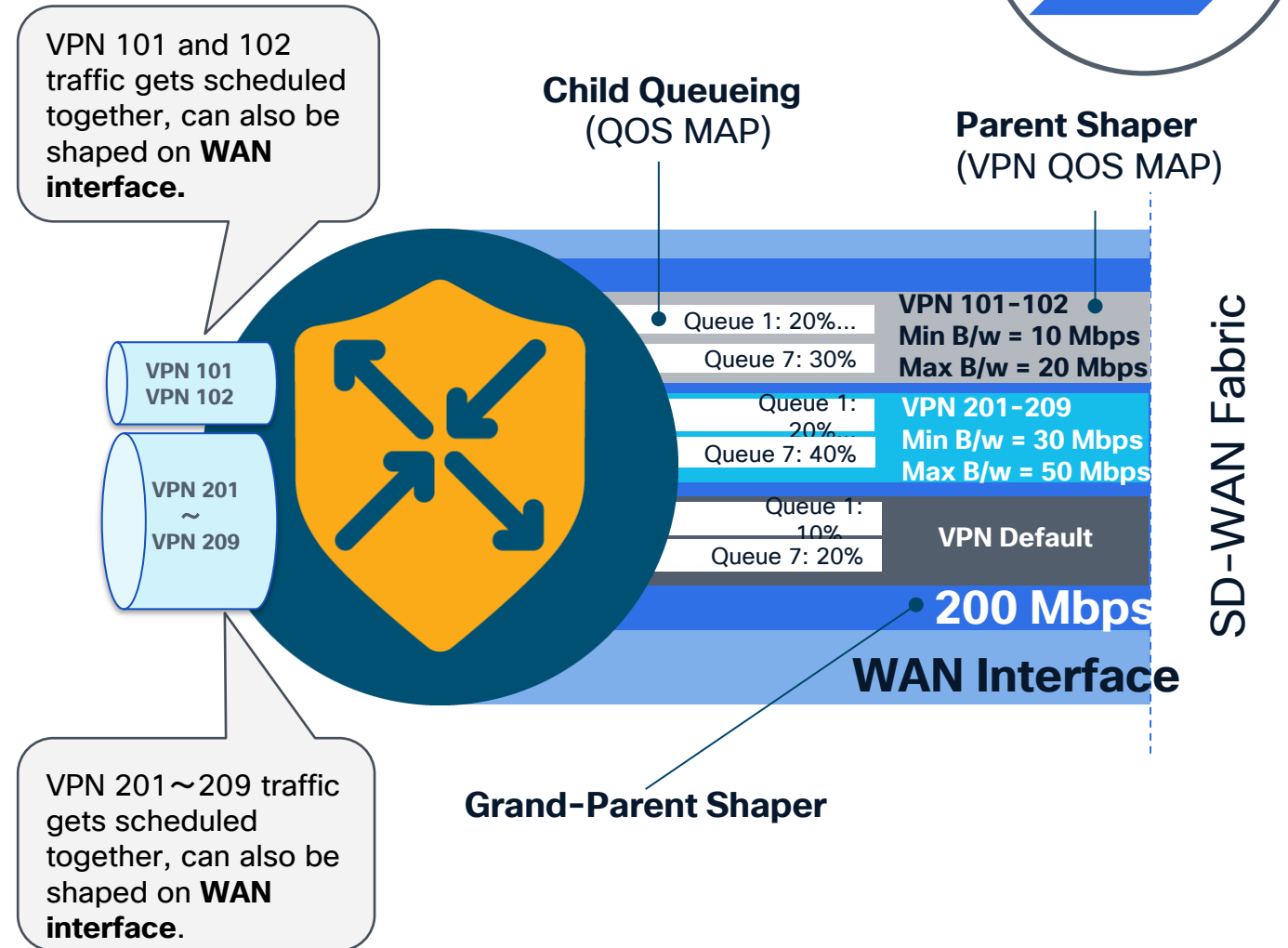
Per-Tunnel QoS with Adaptive Shaping



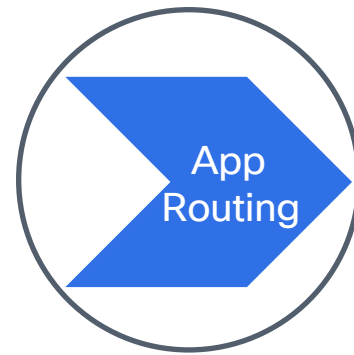
Per-VPN QoS

Traffic throughput can be differentiated per-VPN basis
A greedy VPN can't hog WAN's resource and starve other VPNs.
QoS policy could be applied per-VPN

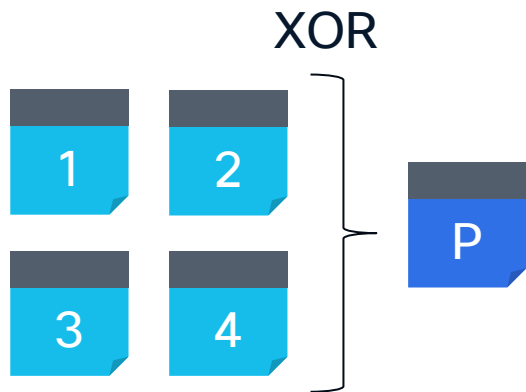
Traffic initiated from Service VPN



Forward Error Correction



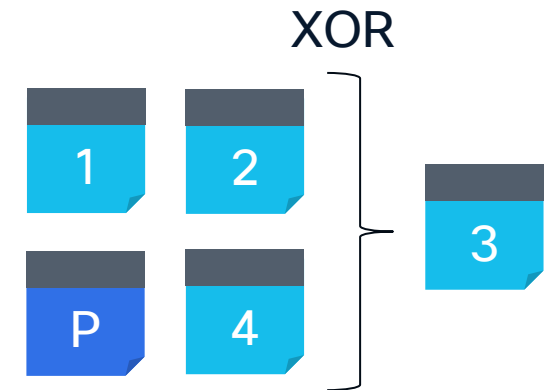
 FEC Header



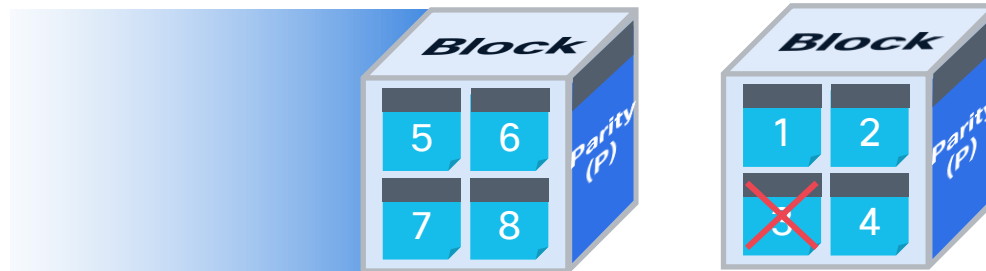
Highlights:

- Mitigates packet loss for critical applications
- Protocol agnostic (TCP/UDP)
- Dynamically invoked
- Operates per-tunnel

 FEC Header



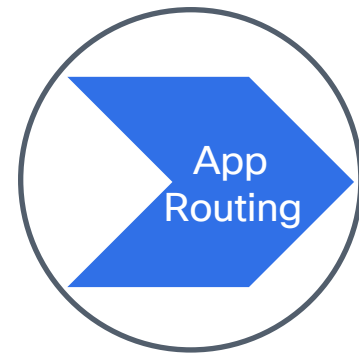
Sender



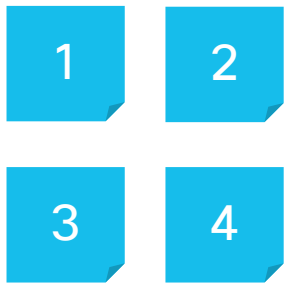
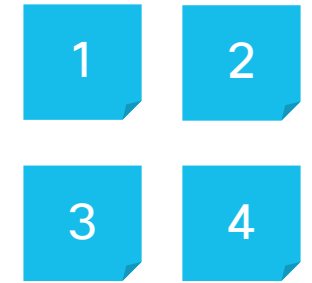
Receiver

SD-WAN Tunnel

Packet Duplication



- Mitigates packet loss for critical applications
- Protocol agnostic (TCP/UDP)
- Works only over multiple tunnels
- Duplicates are discarded on receiver



SD-WAN Tunnel 1



SD-WAN Tunnel 2

Native Unified Communications in SD-WAN



Manager/Controller



Does not participate in Call Routing

Provisions ISR for UC

- Distributed Dial Plan (SIP Dial Peer)
- Call Manipulation (Translation)
- Media/Codec Selection
- SRST

Participates in Data Plane

Provides extended Dial Plan support

- Enterprise call routing
- Media Termination
- SIP only (CUBE is not currently supported)

Does not invoke configuration change

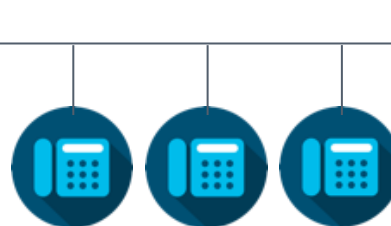
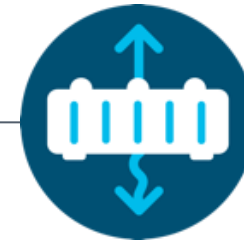
Call Control



Management/Control Plane

Data Plane

FXS, FXO, T1/PRI

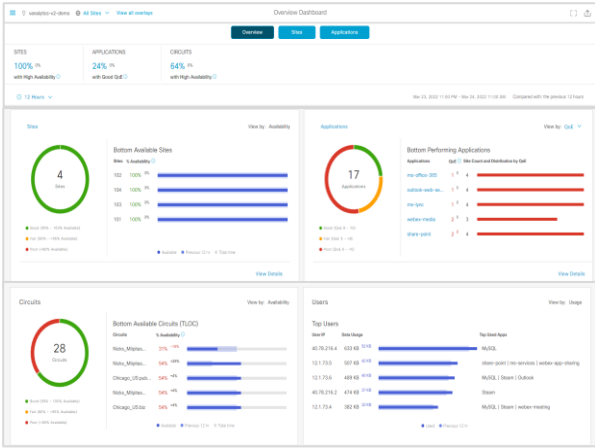


PSTN

Underlay and Overlay visibility



Visibility into Network & App Performance

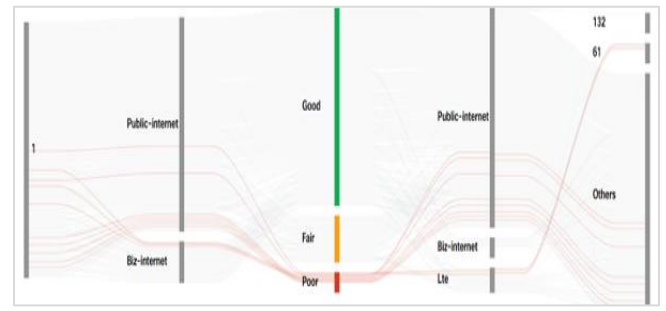


Application Experience
Scheduled Reports
Historical Trends &
Daily/Weekly/Monthly
Aggregates



Troubleshooting w/ Extensive Traffic Analysis

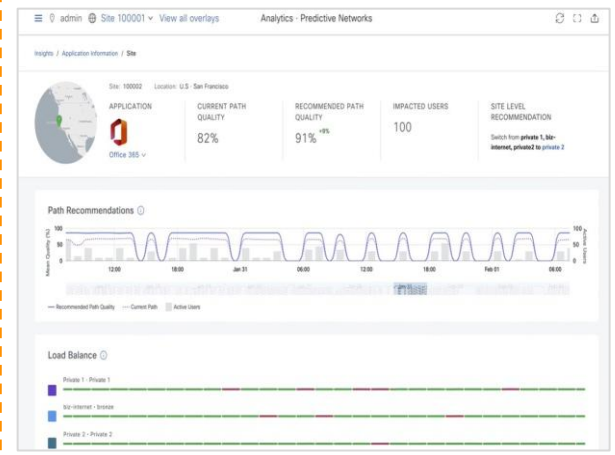
Traffic flow patterns



Underlay path tracing

App distribution across circuits

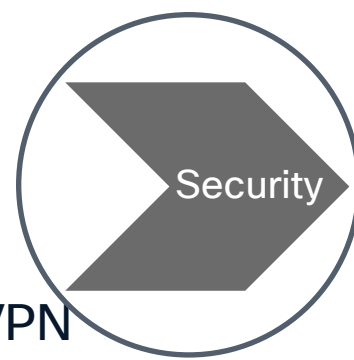
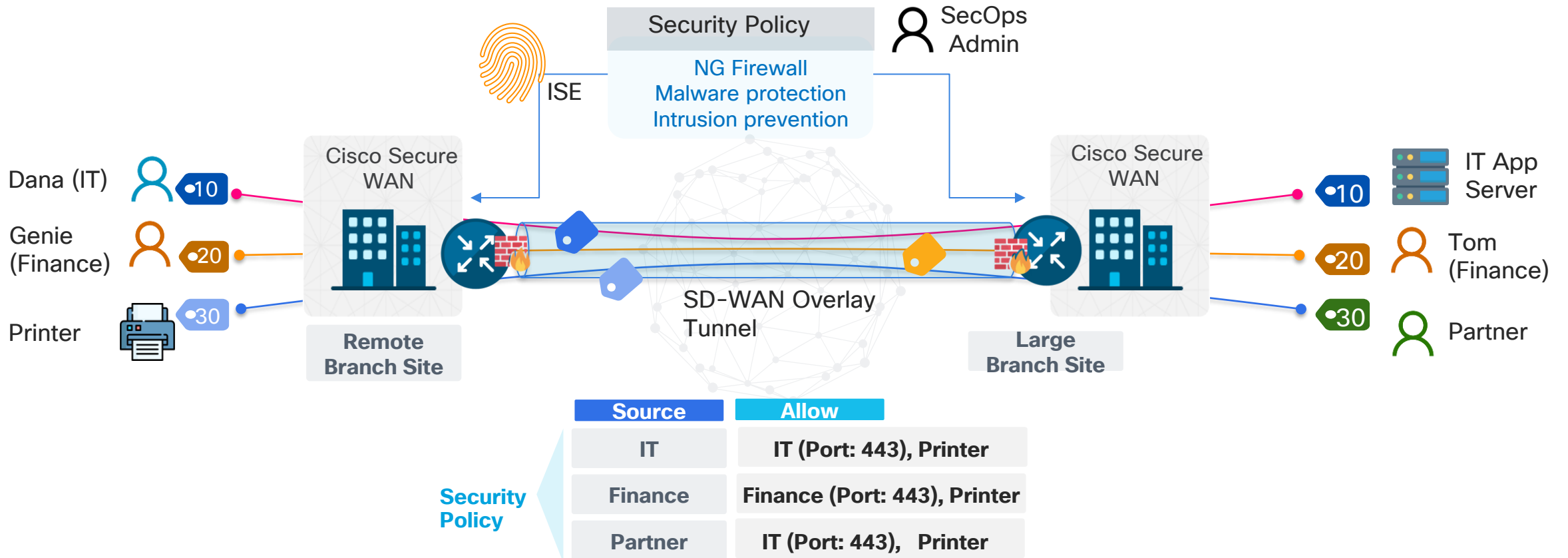
Adaptive & Predictive Networking



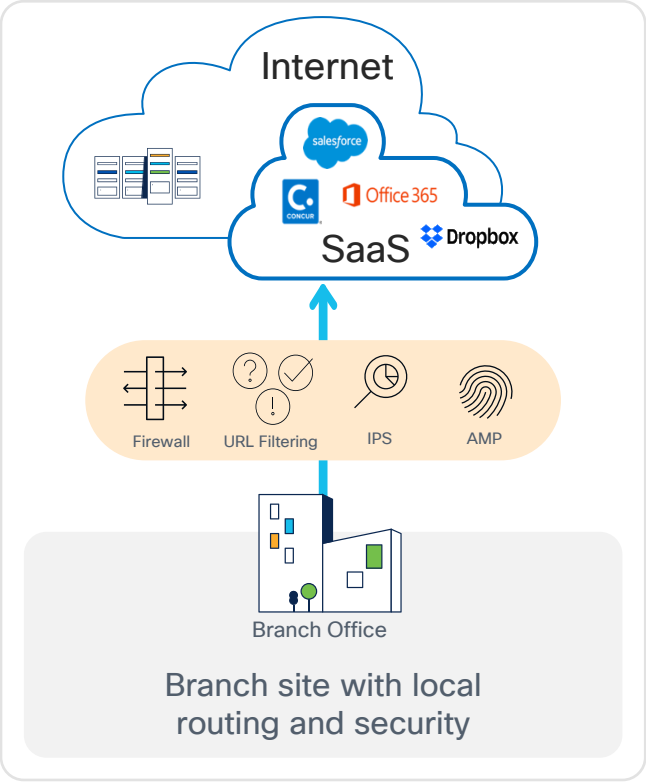
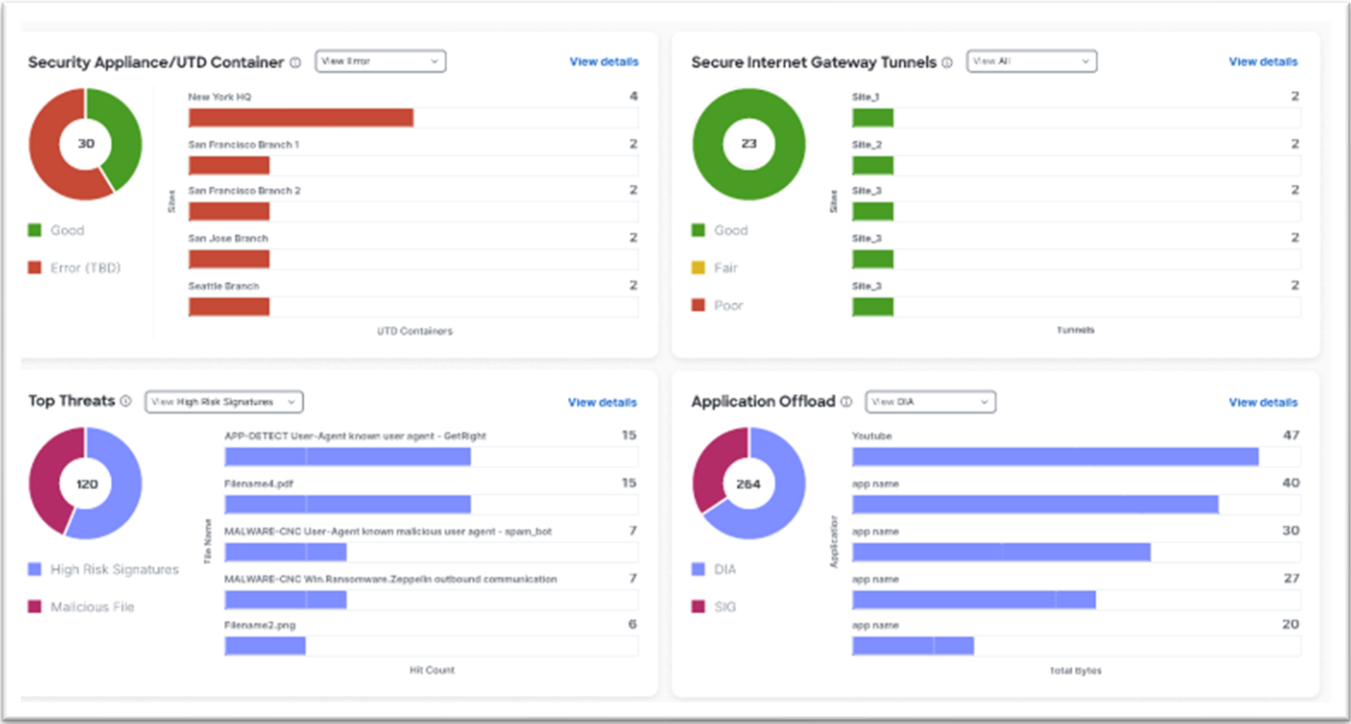
Predictive Path Recommendations
AIOps use-cases
SaaS Traffic Optimization

Secure Segmentation

- Macro segmentation at the VLAN/VRF level
- Context-aware policies with User/User-group or SGT to control policy within a VRF / VPN



Advanced security



- Next Gen Firewall
- Guided Workflows
- Unified Management

Enhanced Cisco Secure WAN NGFW Rule Table

Updated toolbar for granular search (IP, prefix, app, action)

Single line rule definitions

Source Zone: Employee_Net_zone → Destination Zone: Untrusted 5

Q Search

Action ▾

Default Action: Drop ▾ [+ Add Rule](#)

#	Rule Name	Action	Log	Advanced Inspection Profile	Source	Destination	Protocol	Application	
1	Block_DNS	Drop	✓		Prefix BR1_R4_EMPLOYEES	Prefix 8.8.4.4/32	Any	Any	
2	Pass_CloudFlare	Pass	✓		Prefix BR1_R4_EMPLOYEES	Prefix 1.1.1.1/32	Any	Any	
3	Inspect_ICMP	Inspect	✓		Any	Any	icmp	Any	
4	Block_NETFLIX	Drop	✓		Prefix BR1_R4_EMPLOYEES	Any	Any	Netflix_Streaming	
5	Employee_INSPI	Inspect	✓	IPS_AMP	Prefix BR1_R4_EMPLOYEES	Any	Any	Any	

Color coded actions

Icons for security features

August 2025 Release (20.15.2) onwards

Detailed FW Log visualization on SD-WAN Manager

Traffic Logs

Filtering options

Set criteria to get events

12 Hours

Select site(s) name

Select device(s)

Get Logs

117040 Records

Device Id(s): 1.1.1.104

Time: Feb 09, 2025 12:00 AM UTC - Feb 09, 2025 12:55 PM UTC

Export

Event Time (in U...	Site Name	Hostname	System IP	VPN ID	Source IP	Destination IP	Source port	Destination port	Protocol	Application name	Username/SGT	Rule name	FW Policy name	FW Action
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	35.206.6.1	10.45.45.48	20302	52478	17	webex-meeting	--	Secpol1-vm6_8	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	10.45.45.48	40.78.216.1	52480	20203	17	ms-office-365	--	Secpol1-vm6_8	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	40.78.216.1	10.45.45.48	20203	52480	17	ms-office-365	--	Secpol1-vm6_8	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	10.45.45.48	40.78.216.1	52480	20203	17	ms-office-365	--	Secpol1-vm6_8	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	40.78.216.1	10.45.45.48	20203	52480	17	ms-office-365	--	Secpol1-vm6_8	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	10.45.45.48	40.78.216.1	52480	20203	17	ms-office-365	--	Secpol1-vm6_8	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	40.78.216.1	10.45.45.48	20203	52480	17	ms-office-365	--	Secpol1-vm6_8	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	10.45.45.48	40.78.216.1	52482	20403	17	outlook-web-servi...	--	Secpol1-vm6_8	Secpol1-vm6_8122	Inspect

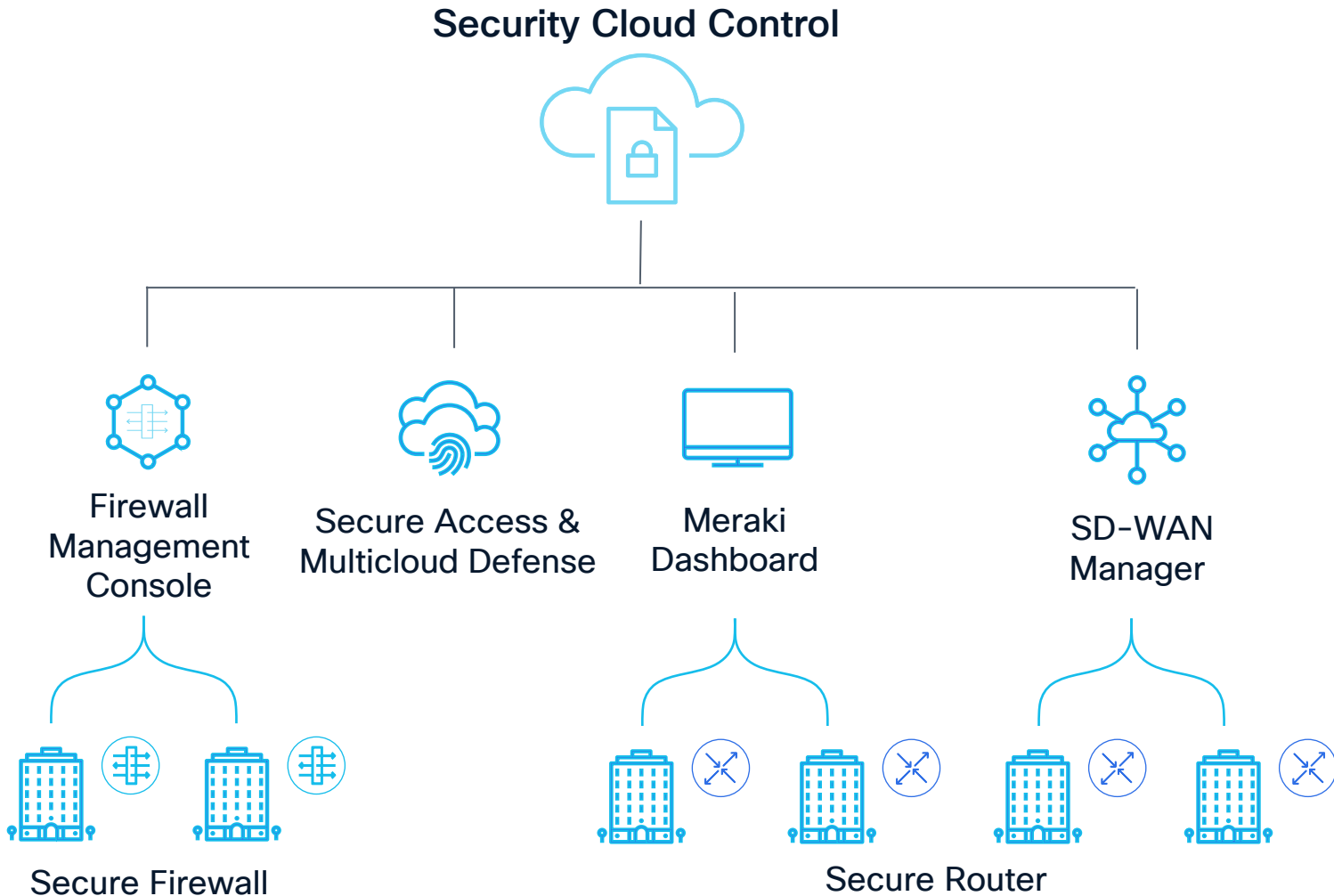
Granular Visibility

Customized Queries

Data Retention

August 2025 Release (17.18.1)

Management of Secure Router NGFW using SCC



Security Object/Policy Configuration

- Create security objects for Secure Router NGFW stack
- Push security policies to different security solutions using single orchestrator

Monitoring

- Common logging repository via SAL (Security Analytics and Logging)

Troubleshooting (Future)

- Leverage SCC tools for security troubleshooting

August 2025 Release (17.18.1)

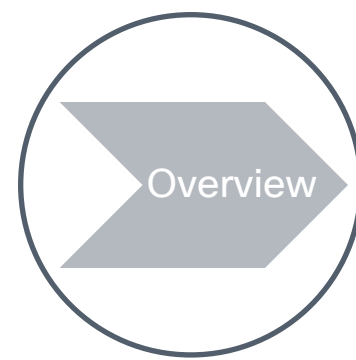
Catalyst SD-WAN Secure Edge Solution

- ✓ Best in class application routing and path resiliency ideal for collaboration
- ✓ Powerful segmentation capabilities from branch across WAN
- ✓ NGFW & Snort-based security features on-box



Meraki SD-WAN Use Cases & Capabilities

Meraki MX Secure SD-WAN Platform



Meraki Dashboard: configuration, updates and analytics
in a single pane of glass



Auto VPN



Intelligent
Routing



Quality of
Service (QoS)



SD-WAN
Analytics



Seamless
Firmware
Upgrades



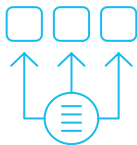
Native Cisco
SASE Integration



NBAR Deep
Packet
Inspection
Engine



SD-WAN over
cellular



IPSEC
(3rd Party SSE)



Secure Remote
Access

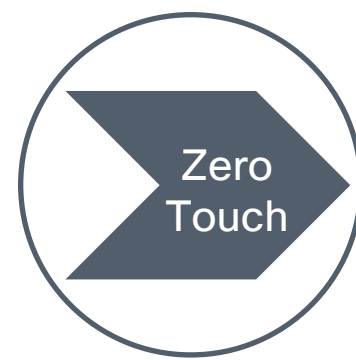


Direct Internet
Access/ VPN
Exclusion



Native
ThousandEyes
Integration

Meraki Device-to-Cloud Connectivity



Device requests IP address Check in starts

Initial WAN tests

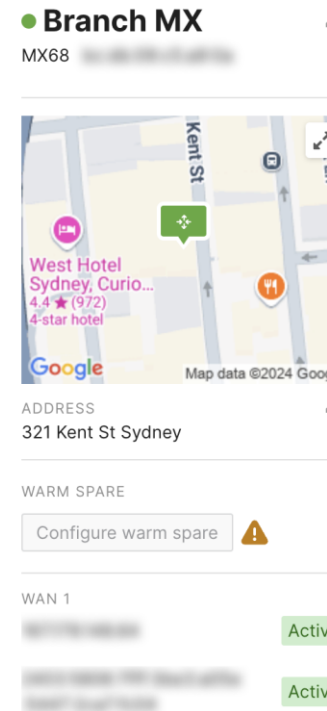
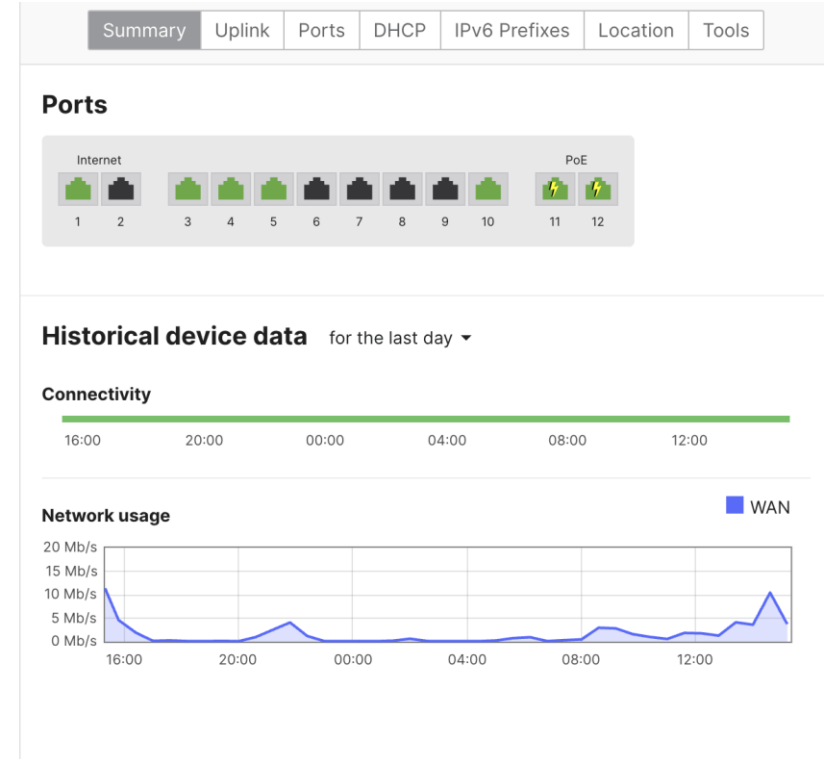
FIPS 140 compliant connection over TLS to
the cloud controller

All data is continually duplicated between
two separate cloud controllers

Device serial # matched to Meraki Org

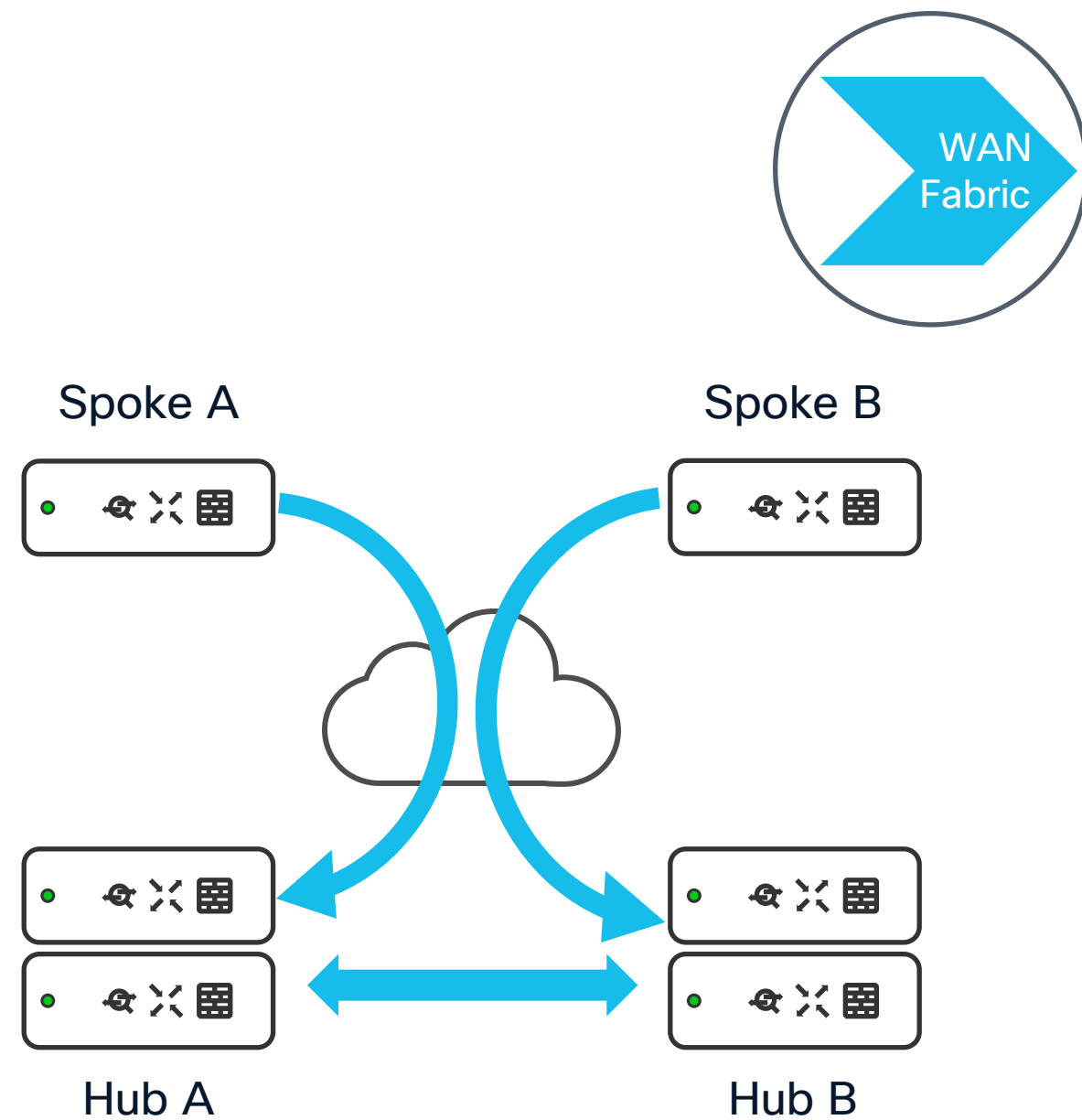
Download configuration

Check in complete

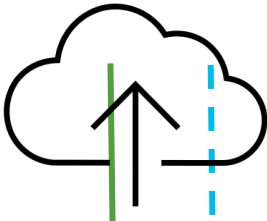
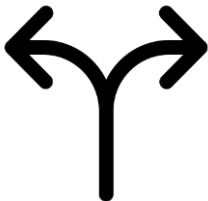


Auto VPN - Out of the box

- Spokes build tunnels to hubs that they have configured
- Hubs build tunnels to all other hubs
- All MXs in an Auto VPN domain 'learn' about all other routes



IPSEC Tunnel Monitoring and Redundancy



Tunnel monitoring

Active/Backup tunnels

BGP routing over IPsec

Configure Health Check

Configure your health checks to use for tunnel health. Only one health check per tunnel can be used.

Health check	Endpoint
Zscaler SLA	http://gateway.mycompany-zscaler-cloud.net/vptest
Meraki	—

+ Add health check

1SW

Primary

Edit

Move to

Delete

Secondary

+ Add

Routing

☐ Static ☒ Dynamic (BGP)

Network

Cisco SFO12

Don't see your networks? Go to [Security & SD-WAN > Routing](#) to enable BGP settings, then come back here.

Tunnel IP

11.1.1.1/30

Neighbor IP

64.103.26.57

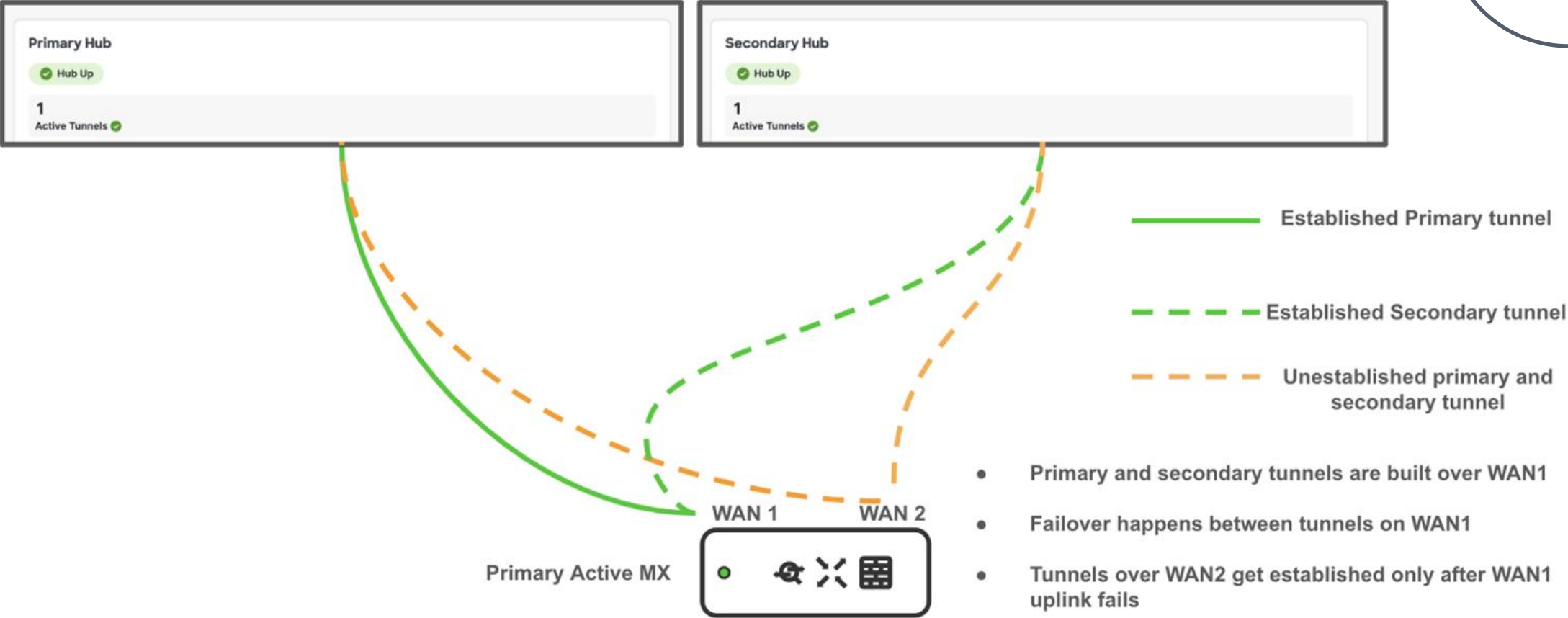
Remote AS

65000

Weight

99

IPSEC Tunnel Monitoring and Redundancy



Available with MX 19.1 Firmware Release

IPSEC Tunnel Reporting and Logging



Reference configured IPsec peer name in
Event log for easy correlation



Time (PDT) ▼	Client	Category	Event type	Details
Apr 7 16:56:19		Non-Meraki VPN	Non-Meraki VPN negotiation	msg: <remote-peer-2 1301> c
Apr 7 16:56:19		Non-Meraki VPN	Non-Meraki VPN negotiation	msg: <remote-peer-2 1301> c
Apr 7 16:56:19		Non-Meraki VPN	Non-Meraki VPN negotiation	msg: <remote-peer-2 1302> (
Apr 7 16:56:19		Non-Meraki VPN	Non-Meraki VPN negotiation	msg: <remote-peer-2 1302> I

Red
Amber
Green

1 site-to-site peer	2 exported subnets	1 Non-Meraki peer
Status ▲	Name	Public IP
	MicrosoftSSE	168.62.8.77
1 total		

Per peer VPN logs

Accurate tunnel status reporting

Available with MX 19.1 Firmware Release

Probing



Probes are unidirectionally sent over all available transport paths

MX-A W1 -> MX-B W1

MX-A W1 -> MX-B W2

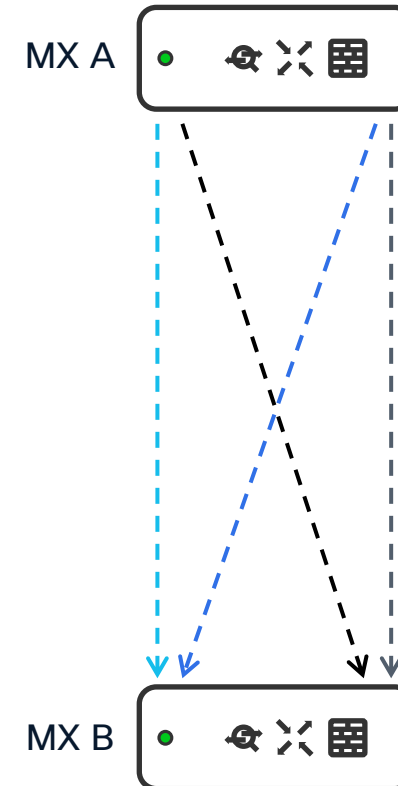
MX-A W2 -> MX-B W1

MX-A W2 -> MX-B W2

Probing interval is

1 second for under 2500 Auto VPN nodes

10 sec for over 2500 Auto VPN nodes



Calculating Performance



1 second probing

Latency, Jitter, Loss & MOS are the average of the last 30 seconds of data - at least 30 probes

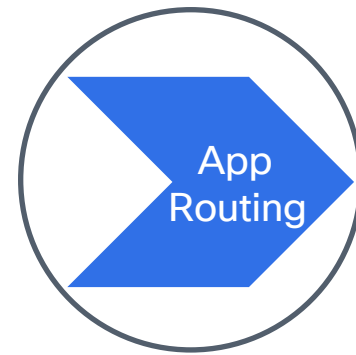


10 second probing

Latency, Jitter, Loss & MOS are the average of the last 30 seconds of data - at least 3 probes



Performance Classes



Uplink Selection

Preferred Uplink

WAN 1 ▾

Fail over if:

Poor performance ▾

Performance class:

VoIP ^
VoIP ✓

Default

“Ensure connection is up”

- Connection monitor failover
- If loss >60%, failover to an alternative transport network

Match Performance Class

“Ensure connection is good enough”

- App uses preferred uplink if MOS for paths is >3.5 MOS
- Will not use alternative path even if MOS for path is higher

Traffic filters

All VoIP & video conferencing ✕ Add +

Policy

Preferred uplink: Best for VoIP ▾

Dynamic Selection

“Ensure we are using the best path”

- Flows are routed via the best performing path for MOS
- If the calculated MOS for a given path becomes better, it will be immediately preferred

Custom Performance Classes



Custom combination of latency, jitter and loss

Mapped to application or service level

Maximum of 6 configurable

Custom performance
classes

Name	Maximum latency (ms)	Maximum jitter (ms)	Maximum loss (%)	Actions
Bronze	200	50	8	X
Silver	150	50	5	X
Gold	100	40	3	X
Platinum	50	20	1	X
0356	60	30	1	X

[Create a new custom performance class...](#)

Application

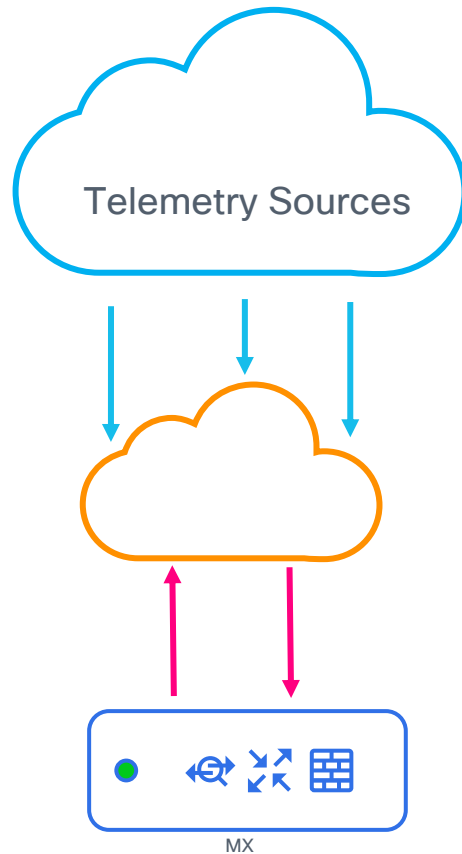


Policy applied either via custom expressions (CIDR / Hostname) or Traffic Analysis engine
NBAR2

NBAR2 supports 1500 applications

Traffic filters	
Add +	
Health care	All Web file sharing
News	4shared.com
Online backup	download.com
Peer-to-peer (P2P)	Easynews
Productivity	easysshare.com
Remote monitoring & management	filefactory.com
Security	filefront.com
Social web & photo sharing	filer.com
Software & anti-virus updates	filestube.com
Sports	gigeshare.com
Video & music	hotfile.com
VoIP & video conferencing	massmirror.com
Web file sharing	mediafire.com
Web payments	

SD-AVC Integration for NBAR



Up to 90%+ first packet classification with additional telemetry sources!

- Amazon Chime
- Atlassian
- Box
- Cisco Meraki
- Code42
- Crashplan
- Dropbox
- Github
- Google Meet
- HubSpot
- Intuit
- Microsoft Intune
- MS Office 365
- RingCentral
- SalesForce
- SAP
- ServiceNow
- SugarCRM
- Telegram
- Webex
- Whatsapp
- Workday
- Zoho
- Zoom
- Zscaler
- CASI Umbrella Top 1 Million
- AWS
- Azure
- GCP
- SSL Crawler
- WHOIS
- rDNS
- Internet registry DB

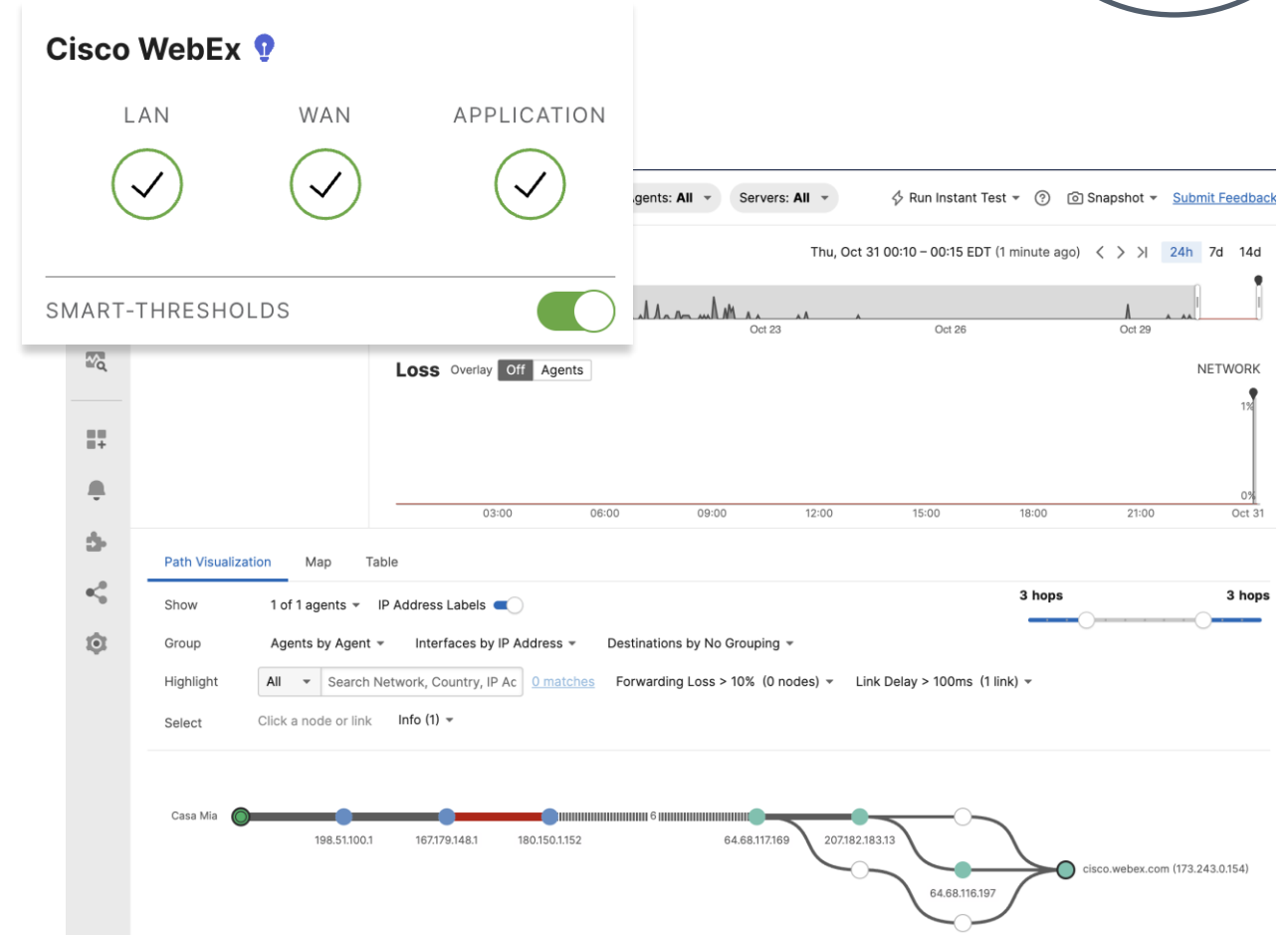
Thousand Eyes enriched Web App Health



End-to-end visibility from branch to cloud

Clear demarcation points between LAN / WAN / Transit & Applications

Automatically configured synthetic testing with smart thresholding.



Comprehensive Firewall Capabilities



Meraki Dashboard: Security policy control, events, analytics and integrations



Stateful Firewall,
Routing, NAT



Intrusion
Prevention



Malware
Protection &
Sandboxing



URL Filtering &
Categorization



Talos
Intelligence



Geography
based FW rules



Application
Layer Detection



High Availability



VPN



TLS Decryption



Identity &
Attribute Based
Access Control



Live tools for
troubleshooting

Meraki Security Dashboard & Event Details



Cisco Meraki

NETWORK

Meraki 460 Townsend - SFO22

Network-wide

Security & SD-WAN

Switch

Wireless

Insight

Organization

Search events

Filter

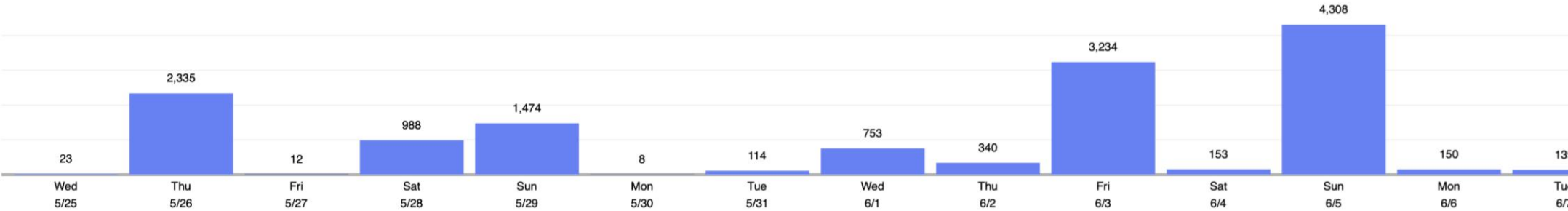
14125 matching events

All times are in UTC

MX Summary

MX Events

Events over time



Most affected networks

Top sources of threats

Network	Events
Meraki San Francisco	
Meraki London - F	
Meraki Sydney SY	
Z - San Francisco	
Z - Cloud Intercon	

MX Summary

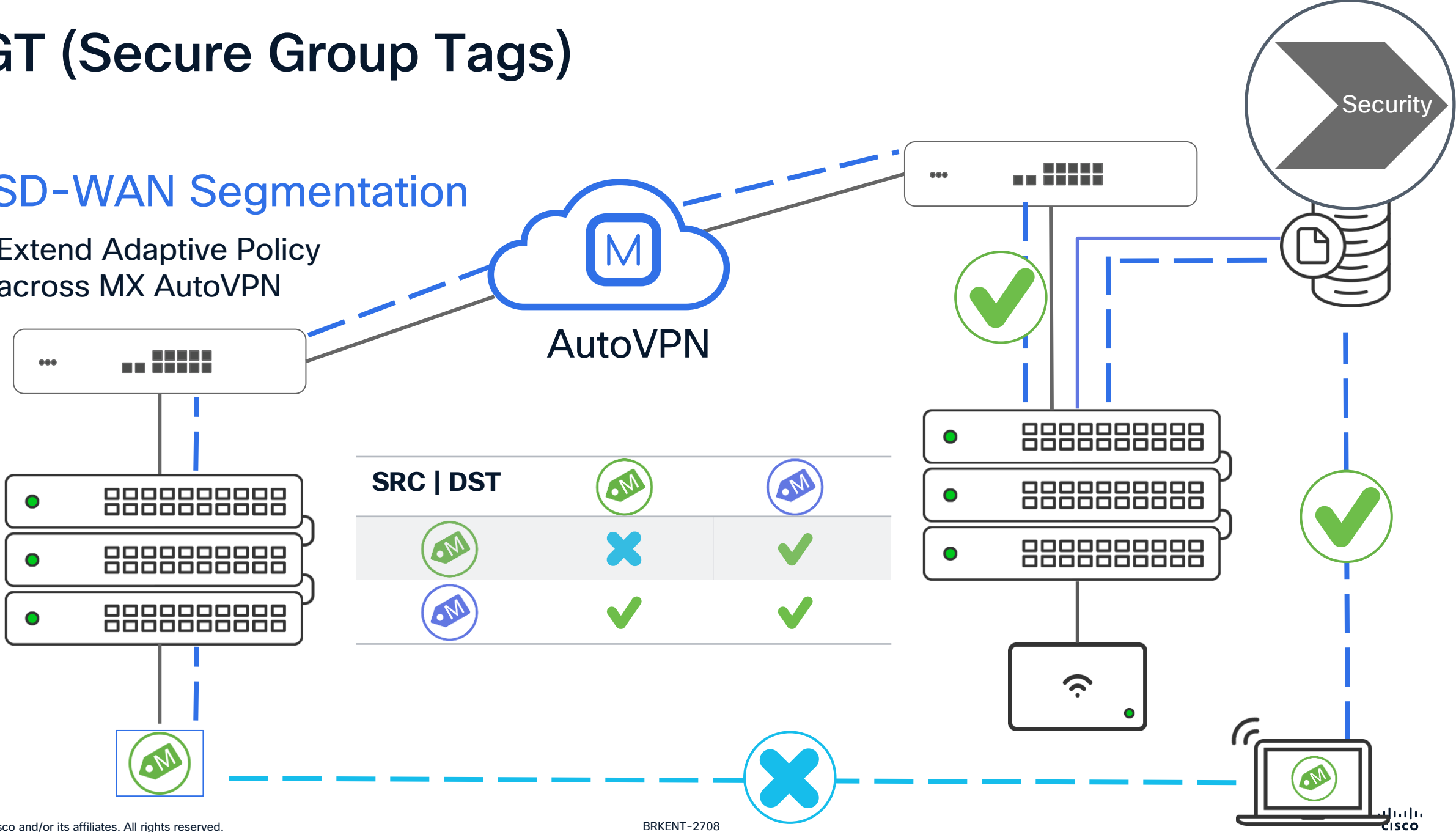
MX Events

Time	Type	Source	Network	Destination	Disposition	Action	Details
Jun 8 17:00:37	IDS Alert	s3-website.ca-central-1.amazonaws.com 52.95.147.1:80	Z - San Francisco - Lab and Guest	pa-int-wan-1-mx-98188810a5f7 Meraki Network OS		Allowed	<div>POLICY-OTHER</div> cryptomining javascript client detected

SGT (Secure Group Tags)

SD-WAN Segmentation

- Extend Adaptive Policy across MX AutoVPN





XDR Integration



- Meraki MX is the sensor
- Contextual Threat and Behavioral Analytics using NetFlow
- XDR uses AI/ML to analyze network data and detect malicious behavior or early indicators of compromise
- Button-click integration to send telemetry from all your MX devices to XDR

Security Center

Overview 123 Events 123 **XDR incidents 44**

44 Incidents 5 New incidents 22 Open incidents

Search Last 30 days Assignment Status

Priority	Name	Source	Created	Assigned
1000	Ransomware Detection	SCA	3 days	Unassigned
978	A malicious SHA-256 targeted an endpoint	SCA	4 days	Unassigned
875	Suspicious Web Access	Meraki API	9 hours	Unassigned
832	Authentication Bypass Attempt	Meraki API	11 hours	Unassigned
800	Lateral Movement	Meraki API	3 days	Unassigned
784	New Remote Access on 172.31.100.120	SCA	3 days	Unassigned
711	MITRE: Incident TA0009	SCA	3 days	Unassigned
691	LDAP Connection from Suspicious Process	SCA	3 days	Unassigned
691	Log4Shell	SCA	3 days	Unassigned
620	Suspicious Web Access	SCA	3 days	Unassigned

A malicious SHA-256 targeted an endpoint

Priority 978 Status New

Reported by Cisco Secure Cloud Analytics (swc-securex) 1 month ago

Assigned Unassigned

Priority score breakdown 978 97 Detection Risk 10 Asset Value at Risk

Short description

Long description

Attack chain 734

Source 173.31.100.120

Description A process running has a hash matching one in a list of known malicious process hashes.

Sources 173.31.100.120 i-0bc0f7d513aeb533a i-04f513cbb8e22373e

Help View incident in XDR

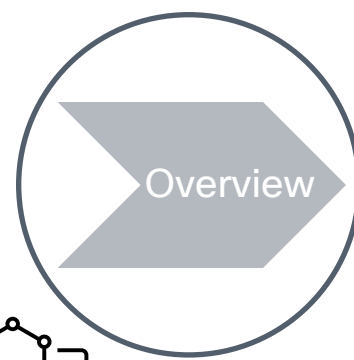
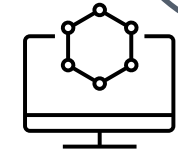
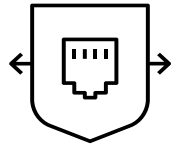
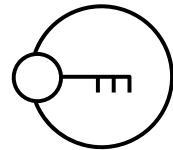
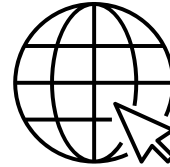
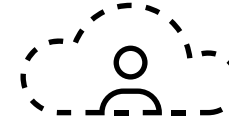
Meraki SD-WAN Secure Edge Solution

- ✓ Rapid deployment at scale & simplicity across all policies
- ✓ Unified management platform for all branch functions
- ✓ NGFW & Snort-based security features on-box



Firewall Threat Defense Use Cases & Capabilities

Branch Deployments with Secure Firewall



Secure Elastic Connectivity

VT-based Hub & Spoke VPN

BGP, EIGRP, OSPF over VTI

DVTI support DHCP

WAN Optimization

Dual ISP configuration

Active-Standby Backup VTI tunnel configuration with SLA monitoring

Optimal Path Selection based on interface Monitoring

Increased Usable Bandwidth

Increased support for load-balancing across multiple ISPs

ECMP Support for VTI

Application based load balancing using Policy Based Routing (PBR)

Direct Internet Access for Public cloud

SaaS Application detection (Fist Packet using AVC)

DNS Snooping using trusted DNS Servers

PBR using Application as matching criteria

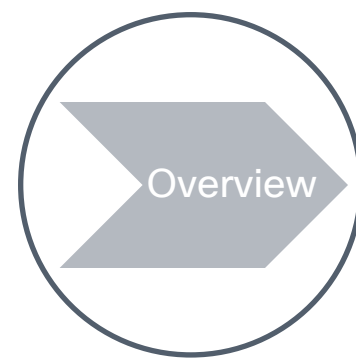
Simplified Management

Data Interface Management

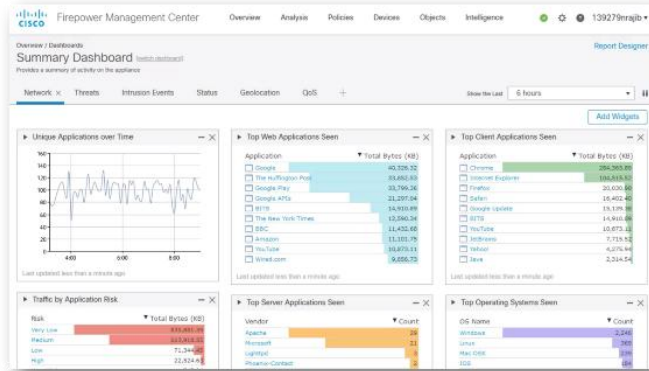
SASE: Umbrella Auto-Tunnel deployment

DVTI Hub and Spoke topology simplification

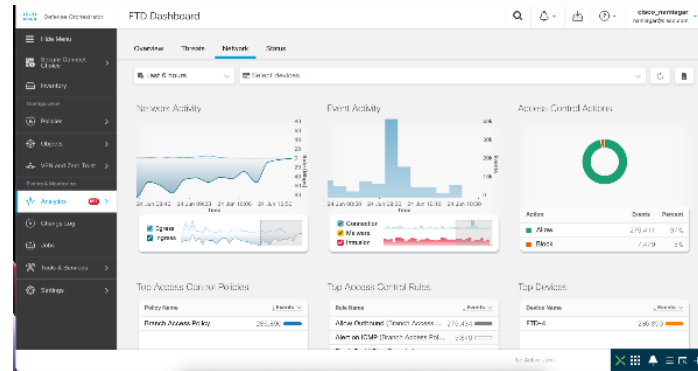
Managing Secure Firewall



Firewall Management Center

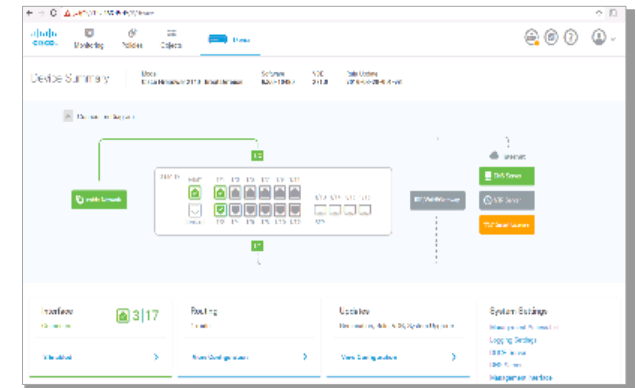


On-premises manager



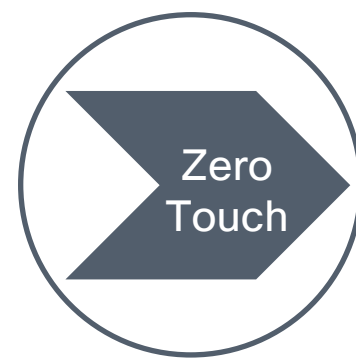
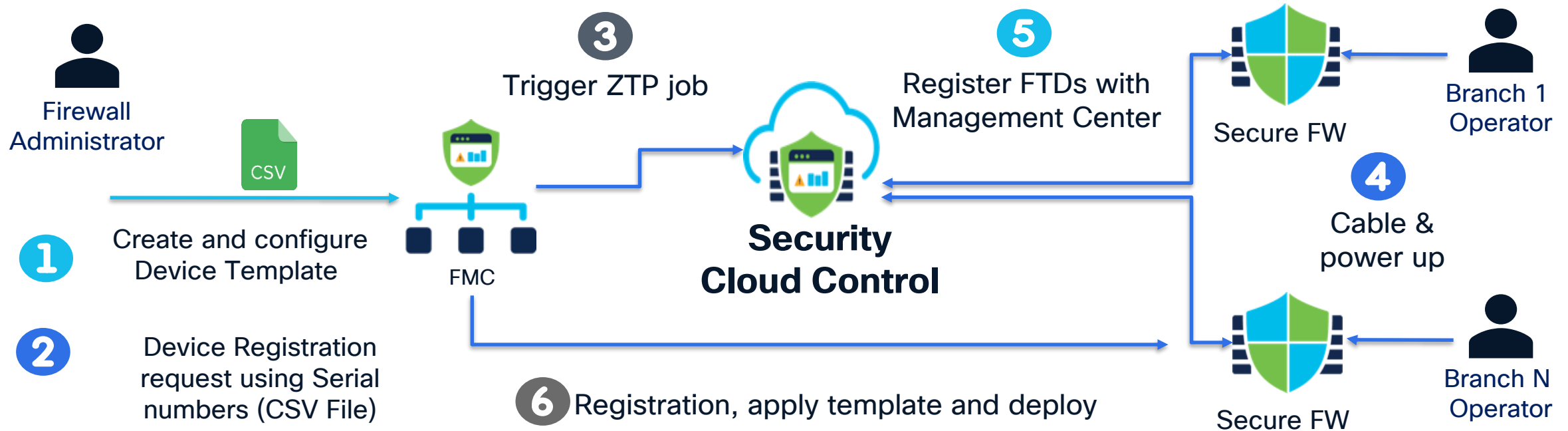
Cloud-delivered via
Security Cloud Control

Firewall Device Manager



On-box manager

Zero Touch Provisioning



ZTP of firewalls to either on-prem Firewall Management Center or Security Cloud Control using device templates

IPsec Virtual Tunnel Interface



- Provides a virtual **routeable interface** for terminating IPsec tunnels
- **Simplifies the configuration** of IPsec for protection of remote links
- The **VTI tunnel is always up** (does not need “interesting traffic”)
- No multicast support on ASA / FTD over VTI

IPSec Tunnel Interface Types



Static Virtual Tunnel Interface (SVTI)



```
Interface tunnel1
nameif tunnel-to-dc
ip unnumbered loopback1
tunnel source GigabitEthernet1
tunnel destination 10.0.0.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile default
```

Static Virtual Tunnel Interfaces (VTI) are introduced in **FTD 6.7**

Static VTI is supported in HA and Multi-Instance

VTI are not supported in clustering

IPSec Tunnel Interface Types

Dynamic Virtual Tunnel Interface (DVTI)



```
interface Virtual-Template101 type tunnel
 nameif dVTI101
 ip unnumbered Lo10
 tunnel source interface Corp-ISP1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_2
```

```
> show interface Virtual-Access 1
Interface Virtual-Access1 "dVTI101_va3", is up, line protocol is up
Hardware is Virtual Access  MAC address N/A, MTU 1445
IP address 169.254.255.1, subnet mask 255.255.255.255
Vaccess Interface Information:
Source IP address 10.18.9.20
Destination IP address 10.18.7.10
Vaccess cloned from template 101
Mode: ipsec ipv4    IPsec profile: FMC_IPSEC_PROFILE_2
IPsec MTU Overhead : 55
```

- Dynamic Virtual Tunnel Interfaces are introduced in **FTD 7.3**
- DVTI uses a virtual template for dynamic instantiation and management
- VPN Sessions using DVTIs only support IKEv2

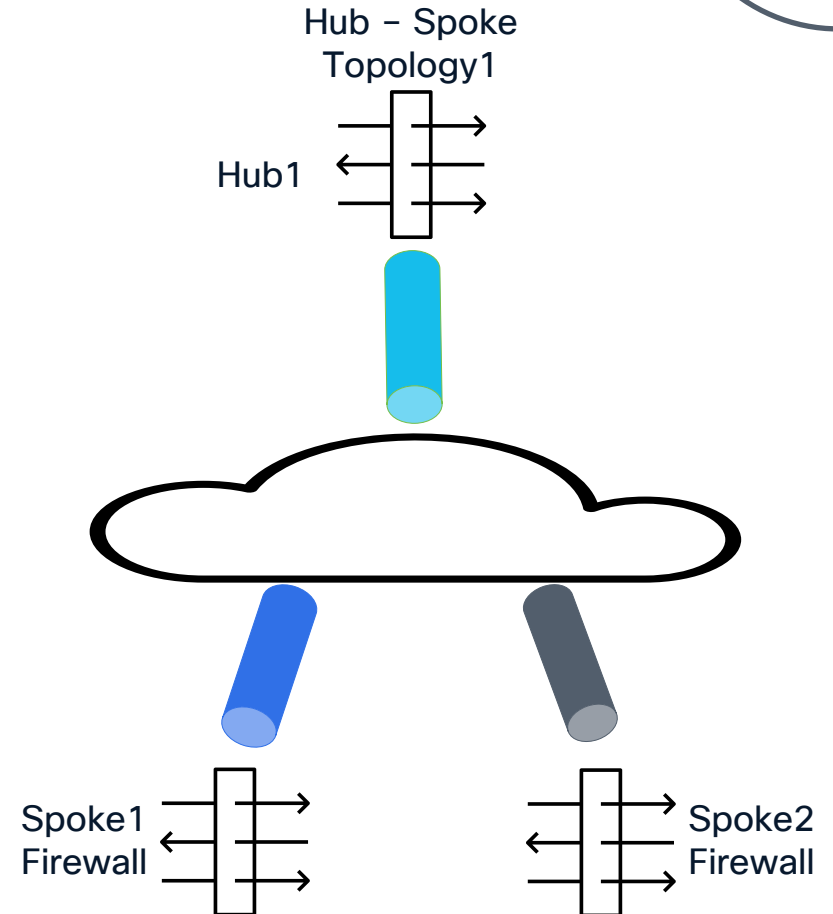
Branch to Hub Communication

Why Dynamic Virtual Tunnel Interface (DVTI) ?

High-scale, route-based VPN
deployments

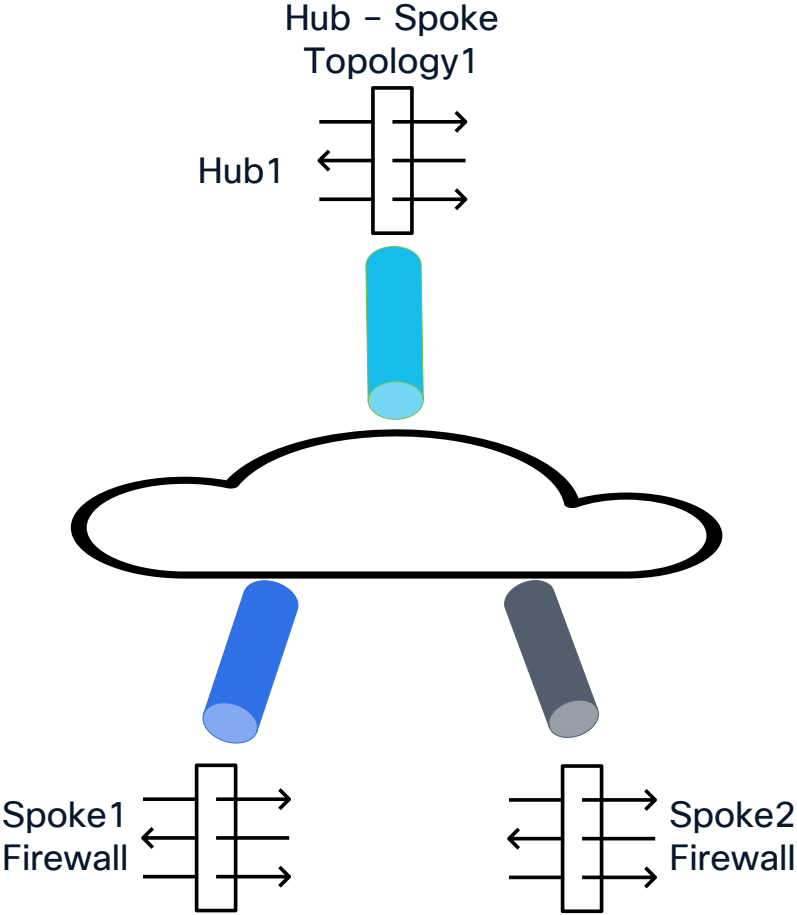
No additional Hub configuration while
adding new spokes

No configuration change on Hub when the
spoke's DHCP IP address changes



Hub and Spoke design using DVTI + SVTI

Single Hub Topology



Edit VPN Topology

Topology Name:
dVTI-Hub-and-Spoke

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Hub Nodes:

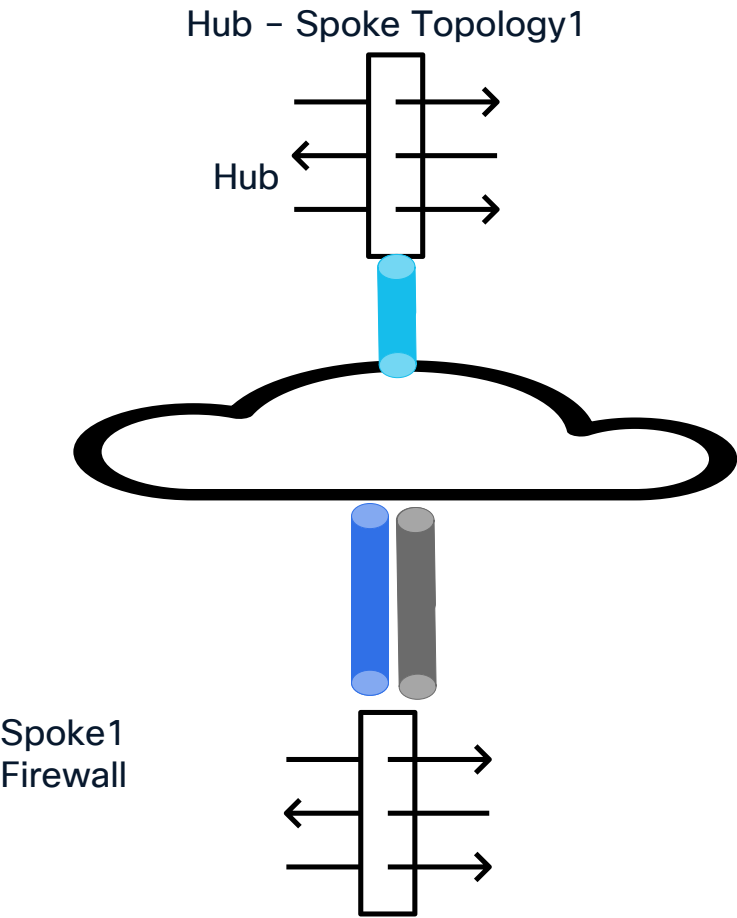
Device Name	VPN Interface	Traffic Match Criteria	
FTD Hub FTD	dVTI101 (169.254.255.1)	Routing Policy	

Spoke Nodes:

Device Name	VPN Interface	Traffic Match Criteria	
FTD Branch FTD	VTI1 (169.254.255.2)	Routing Policy	

Single Hub Topology

Spoke with Dual WAN



Branch FTD

Cisco Firepower Threat Defense for VMware

Device

Routing

Interfaces

Inline Sets

DHCP

VTEP

All Interfaces

Virtual Tunnels

Interface	Logical Name	Type	Security Zones
 Management0/0	management	Physical	
 GigabitEthernet0/0	ISP-1	Physical	ISP1-Zone
 Tunnel1	VTI1	VTI	sVTI-Zone
 Tunnel3	VTI3	VTI	VTI-SSE
 GigabitEthernet0/1	ISP-2	Physical	ISP2-Zone
 Tunnel2	VTI2	VTI	sVTI-Zone
 Tunnel5	VTI5	VTI	VTI-SSE

Dual Hub Topology

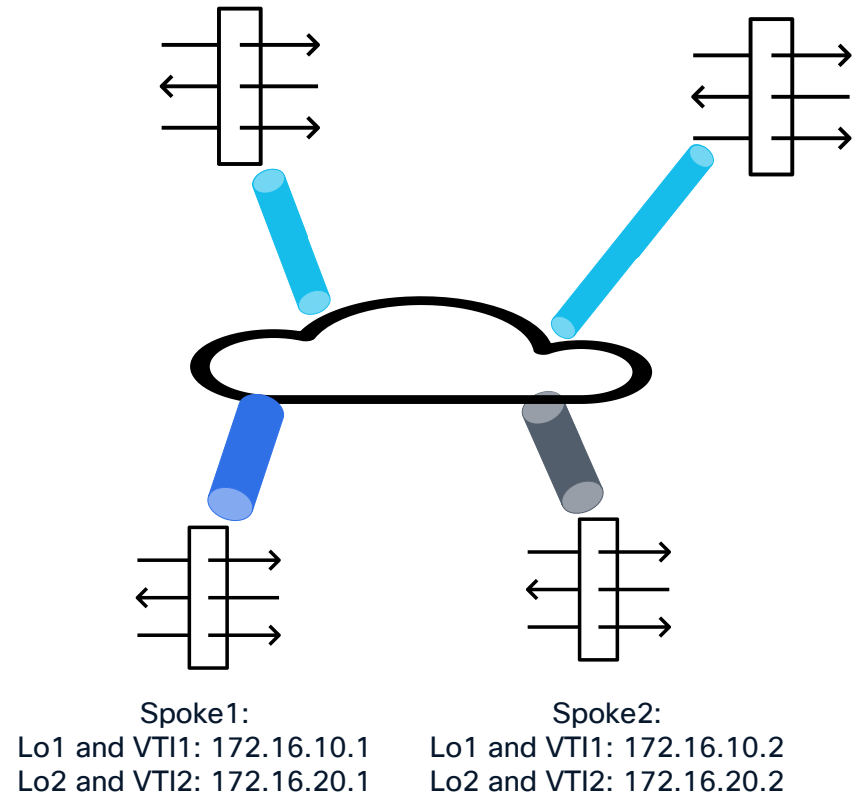


Hub – Spoke Topology1

DVTI Primary Hub:
Loopback and VTI: 172.16.10.254

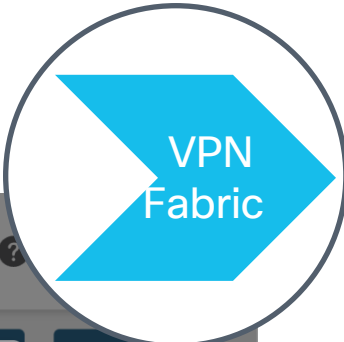
Hub – Spoke Topology2

DVTI Secondary Hub:
Loopback and VTI: 172.16.20.254



- VPN Topology can have multiple hubs for a set of spokes
 - With one hub as the Backup Hub
- Use a separate VPN topology configuration for each Hub
- Each spoke will have 2 VPN tunnels, one per Hub
- Dynamic routing protocol required
 - (BGP recommended)

Secure Firewall 7.6 Topology Wizard



Firewall Management Center
Site To Site

OverviewAnalysisPoliciesDevicesObjectsIntegrationDeploy

Search icons

+ Add

Refresh

Select...

Topology Name
Firewall-Hu

Device
FTD ftdv-tes
FTD ftdv-tes
FTD ftdv-tes
FTD ftdv-tes

Create VPN Topology ?

Topology Name *
Hub-Spoke-VPN

VPN Type

☒ SD-WAN Topology New
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.
Select VPN Topology
☒ Hub and Spoke
Prerequisites

☐ Route-Based VPN
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.
Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer

☐ Policy-Based VPN
Secures traffic between peers based on a static policy using protected networks.
Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer
☐ Full Mesh

☐ SASE Topology
Simplifies and orchestrates the auto tunnel configuration between the threat defense device and the Umbrella SIG gateway.
Select VPN Topology
☐ Hub and Spoke

Cancel Create

Full automated VPN deployment!

Why did we create this new wizard?



Pre-7.6 VPN deployment requirements:

- **Manual & unique** BGP configuration per spoke
- **Manual assignment** of spoke VTI interface IP address (and you have to keep track of these!)
- Easy but several steps for each spoke = time consuming

Starting with 7.6 SD-WAN Topology **automatically** configures:

- VTI interface pool to auto-assign VTI interfaces of all spokes
- BGP configuration for all spokes using same BGP AS (iBGP)
- Fast and easy!

Secure Firewall 7.6 Topology Wizard



Firewall-Hub-Spoke

Hub and Spoke Route-Based (VTI) VPN Topology

Wizard configuration can be edited anytime to add more sites, make changes etc.

1

Hubs 

Device

ftdv-test-11

DVTI

outside_dynamic_vti_1

Gateway IP Address

64.100.14.211

Spoke Tunnel IP Address Pool

DVTI-IP-Pool

ftdv-test-12

outside_dynamic_vti_1

64.100.14.212

DVTI-IP-Pool-2

Edit

2

Spokes 

Device

ftdv-test-13

VPN Interface

outside

Local Tunnel (IKE) Identity

Key ID: Firewall-Hub-Spoke_ftdv-test-13

ftdv-test-14

outside

Key ID: Firewall-Hub-Spoke_ftdv-test-14

ftdv-test-15

outside

Key ID: Firewall-Hub-Spoke_ftdv-test-15

ftdv-test-16

outside

Key ID: Firewall-Hub-Spoke_ftdv-test-16

Edit

3

Authentication Settings 

Authentication

Pre-shared Automatic Key

Pre-shared Key Length

24

Edit

4

SD-WAN Settings

BGP enabled

true

Autonomous System Number

65100

Edit

Secure Firewall 7.6 Topology Wizard



Spoke Tunnel Interface Auto Generation

Static Virtual Tunnel Interfaces (SVTIs) are auto generated on each spoke using the spoke's VPN interface as tunnel source to establish a VPN to the DVTI on each of the hubs.

Spoke Tunnel Interface Security Zone i

VTI x v

+

Overlay Routing Configuration

BGP can be enabled on the VPN overlay topology for seamless VPN connectivity from the spokes to the hub, and for spoke-to-spoke connectivity via the hub. [View more](#)

☒ Enable BGP on the VPN overlay topology

Autonomous System Number * i

65100

Community tag for local routes * i

2112

☒ Redistribute Connected Interfaces i

inside-interfaces x v

+

☐ Secondary Hub is in different Autonomous System i

☒ Enable Multiple Paths for BGP

- Automated iBGP configuration
- Auto-distribution of connected routes
- Community TAG support to tag routes



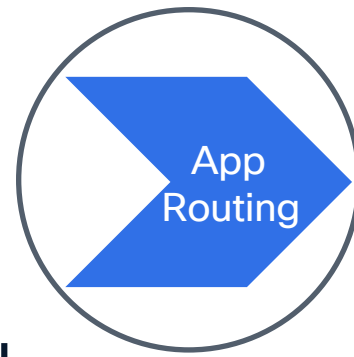
View By: Group

[All \(6\)](#)[Error \(0\)](#)[Warning \(0\)](#)[Offline \(0\)](#)[Normal \(6\)](#)[Deployment Pending \(6\)](#)[Upgrade \(0\)](#)[Snort 3 \(6\)](#)[Add](#)[Collapse All](#)[Download Device List Report](#)

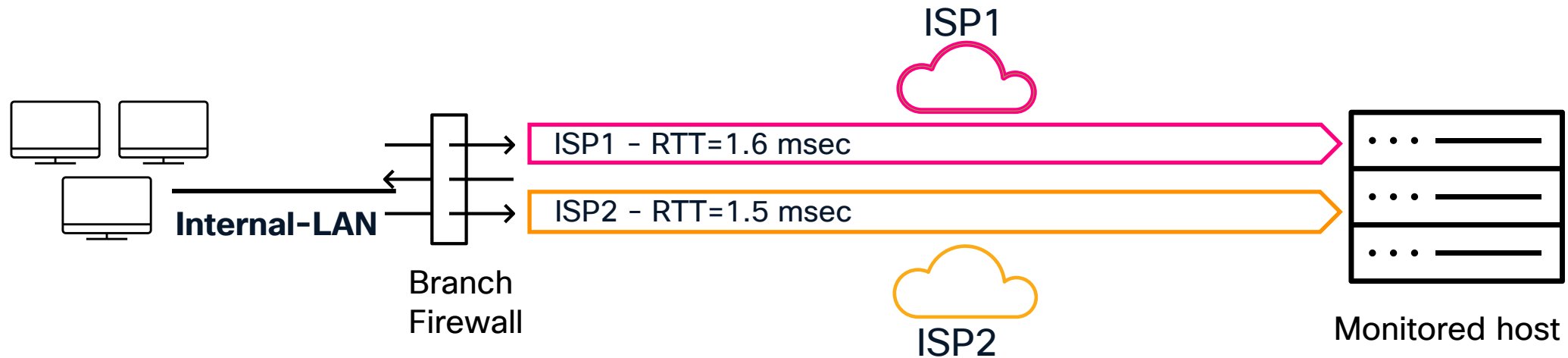
☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
☐	▼ Ungrouped (6)							
☐	ftdv-test-11 Snort 3 10.101.128.211 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	Edge Access Policy		
☐	ftdv-test-12 Snort 3 10.101.128.212 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	Edge Access Policy		
☐	ftdv-test-13 Snort 3 10.101.128.213 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	Edge Access Policy		
☐	ftdv-test-14 Snort 3 10.101.128.214 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	Edge Access Policy		
☐	ftdv-test-15 Snort 3 10.101.128.215 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	Edge Access Policy		
					Essentials, IPS (2 more...)	Edge Access Policy		

Firewall Management Center

Policy Based Routing

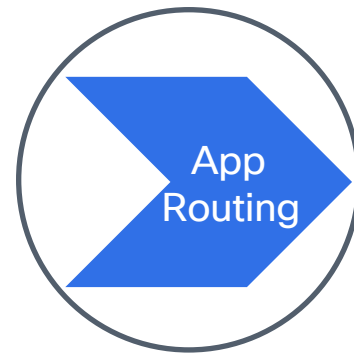


PBR with Path Monitoring steers traffic based on dynamically monitored interface statistics such as **RTT, Jitter, MOS and packet loss**

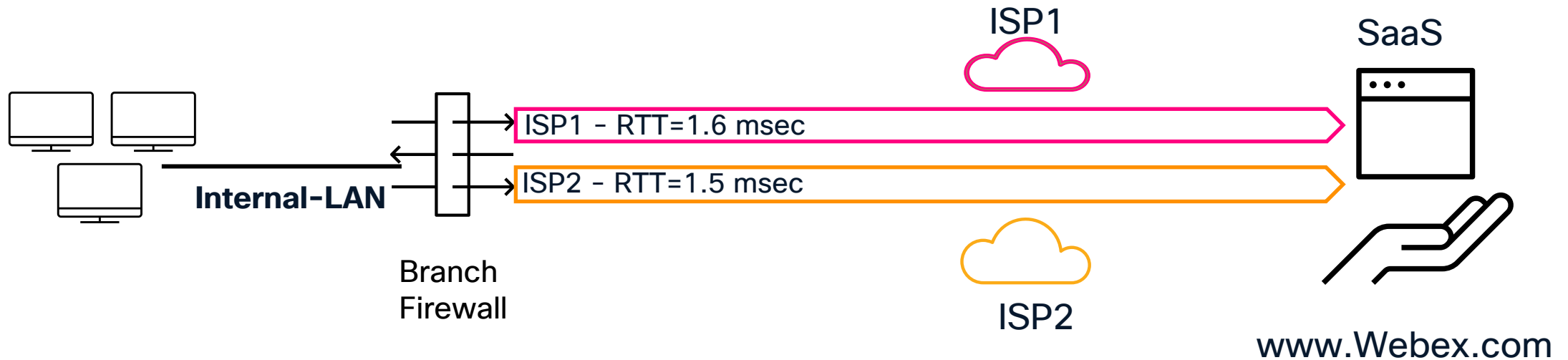


These metrics are collected dynamically using ICMP/HTTP Probe messages

HTTP Path Monitoring



HTTP probes are sent to measure path metrics for selected applications across all egress interfaces configured for path monitoring.

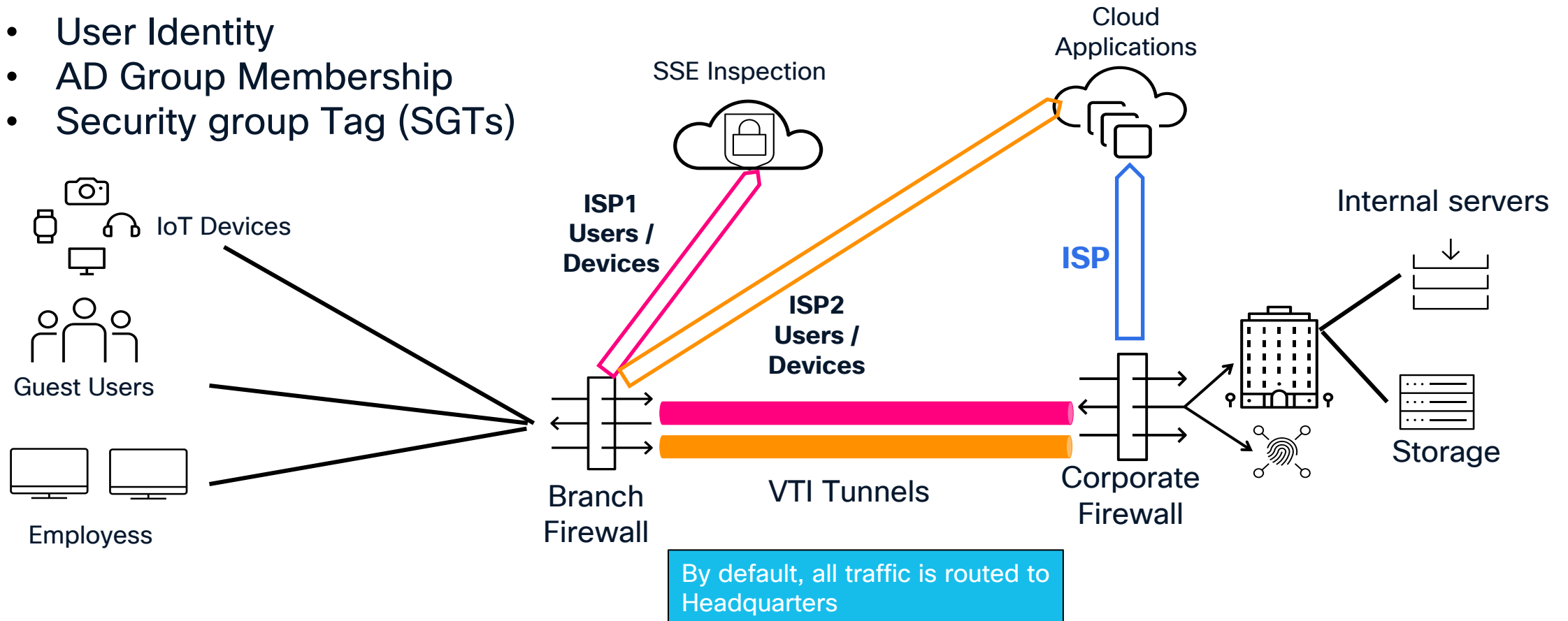


PBR with User Identity and SGT



Additional attributes can be leveraged in the PBR policy:

- User Identity
- AD Group Membership
- Security group Tag (SGTs)



S2S VPN – Monitoring & Insights



Site to Site
VPN Monitoring



Monitor VPN Tunnel Status

Unified Event Viewer to analyze VPN
Traffic flow

Identify Suspicious activity

Optimize Bandwidth allocation

Packet Tracer for troubleshooting

Firewall Management Center

Overview / Dashboards / Site to Site VPN

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

SECURE

Select...

Refresh

Refresh every 5 minutes

Node A	Node B	Topology	Status	Last Updated
Branch FTD (VPN IP: 198.18.1.1)	Extranet (VPN IP: 198.18.1.2)	SecureAccess-ISP	Active	2024-04-23 13:30:56
Branch FTD (VPN IP: 198.18.1.1)	Extranet (VPN IP: 198.18.1.56)	SecureAccess-ISP	Active	2024-04-23 13:30:56
Branch FTD (VPN IP: 198.18.1.1)	Hub FTD (VPN IP: 198.18.1.9.20)	dVTI-PrimaryISP	Active	2024-04-23 13:30:56
Branch FTD (VPN IP: 198.18.1.1)	Hub FTD (VPN IP: 198.18.1.9.20)	dVTI-PrimaryISP	Active	2024-04-23 13:30:56

View full information

A: Branch FTD ↔ B: Hub FTD

Topology: dVTI-PrimaryISP | Status: Active

General CLI Details Packet Tracer

Topology	dVTI-PrimaryISP
Status	Active
Node A	Branch FTD
Node B	Hub FTD
Node A IP	198.18.1.1
Node B IP	198.18.1.9.20
Node A VPN Interface Name	ISP-2
Node B VPN Interface Name	Corp-ISP1
Last Updated	2024-04-23 13:30:56

Site to Site Monitoring (7.4+)



Firewall Management Center
Overview / Dashboards / Site to Site VPN

OverviewAnalysisPoliciesDevicesObjectsIntegration

Select...

Node A

10.10.1.19 (VPN Interface IP: 192.168.105.19)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

FTD02-EXT

10.10.1.19 (VPN Interface IP: 192.168.105.19)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

Tunnel Details

Summary

Node A (192.168.105.19/500)Node B (192.168.105.20/500)

Transmitted: 560 Bytes (560 B)Received: 0 (0 B)

Transmitted: 560 Bytes (560 B)Received: 0 (0 B)

IPsec Security Associations (1)

192.168.15.0/255.255.255.0/0192.168.25.0/255.255.255.0/0

L2LTunnelPFS Group 21IKEv2VTI

Encaps/Encrypt: 20 / 20 pktsDcaps/Decrypt: 0 / 0 pkts

Encaps/Encrypt: 20 / 20 pktsDcaps/Decrypt: 0 / 0 pkts

Remaining Lifetime for SPI ID: 0xE5F96A1

Outbound: 4.81 GB (5159999000 B) 08:53:49 (12229 sec)

Inbound: 5.03 GB (5400000000 B) 08:53:48 (12228 sec)

Remaining Lifetime for SPI ID: 0xE175D4C8

Inbound: 4.97 GB (5340000000 B) 08:53:49 (12229 sec)

Outbound: 4.75 GB (5099999000 B) 08:53:48 (12228 sec)

10.10.1.19 (VPN Interface IP: 192.168.105.19)10.10.1.20 (VPN Interface IP: 192.168.105.20)

show crypto ipsec sa peer 192.168.105.20

peer address: 192.168.105.20

interface: DVTI105_va4

Crypto map tag: DVTI105_vtemplate_dyn_map, seq num: 1,

Protected vrf (ivrf): Global

local ident (addr/mask/prot/port): (192.168.15.0/255

show crypto ipsec sa peer 192.168.105.19

show vpn-sessiondb detail 121 filter ipaddress 192.1

CloseRefresh

Deploy

Refresh

Refresh every 5 min

A: 10.10.1.19 ↔ B: 10.10.1.20

Topology: VPN106-DVTIv4 | Status: Active

GeneralCLI DetailsPacket Tracer

RefreshMaximize view

Summary

Node A (192.168.105.19/500)Node B (192.168.105.20/500)

Transmitted: 560 Bytes (560 B)Received: 0 (0 B)

Transmitted: 560 Bytes (560 B)Received: 0 (0 B)

IPsec Security Associations (1)

192.168.15.0/255.255.255.0/0192.168.25.0/255.255.255.0/0

L2LTunnelPFS Group 21IKEv2VTI

Encaps/Encrypt: 20 / 20 pktsDcaps/Decrypt: 0 / 0 pkts

Encaps/Encrypt: 20 / 20 pktsDcaps/Decrypt: 0 / 0 pkts

Remaining Lifetime for SPI ID: 0xE5F96A1

Outbound: 4.81 GB (5159999000 B) 08:53:49 (12229 sec)

Inbound: 5.03 GB (5400000000 B) 08:53:48 (12228 sec)

Remaining Lifetime for SPI ID: 0xE175D4C8

Inbound: 4.97 GB (5340000000 B) 08:53:49 (12229 sec)

Outbound: 4.75 GB (5099999000 B) 08:53:48 (12228 sec)

10.10.1.19 (VPN Interface IP: 192.168.105.19)

show crypto ipsec sa peer 192.168.105.20

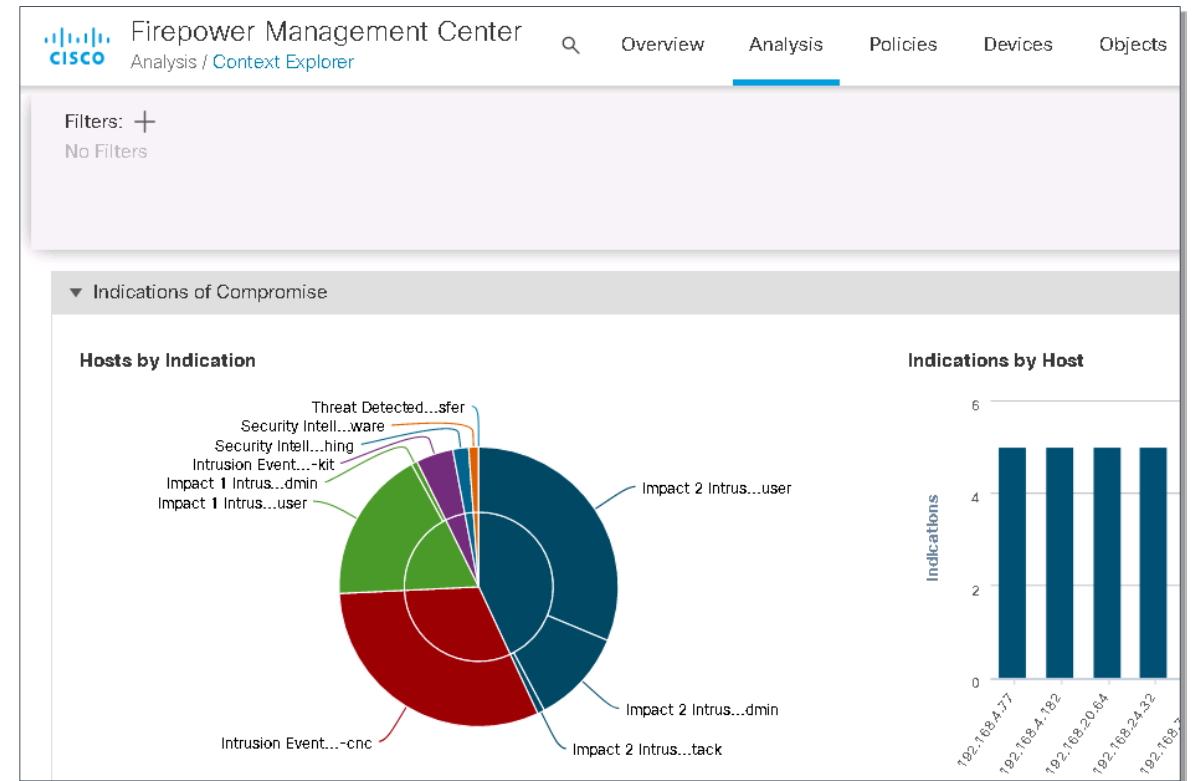
show vpn-sessiondb detail 121 filter ipaddress 192.168.10

Best-in-class Branch Security

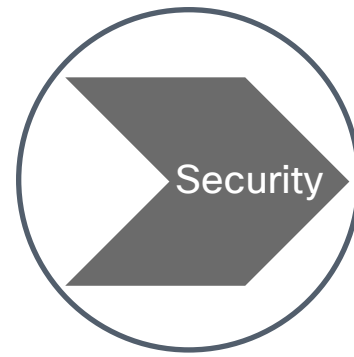
Delivers nearly 100% efficacy on blocking malicious flows and network threats



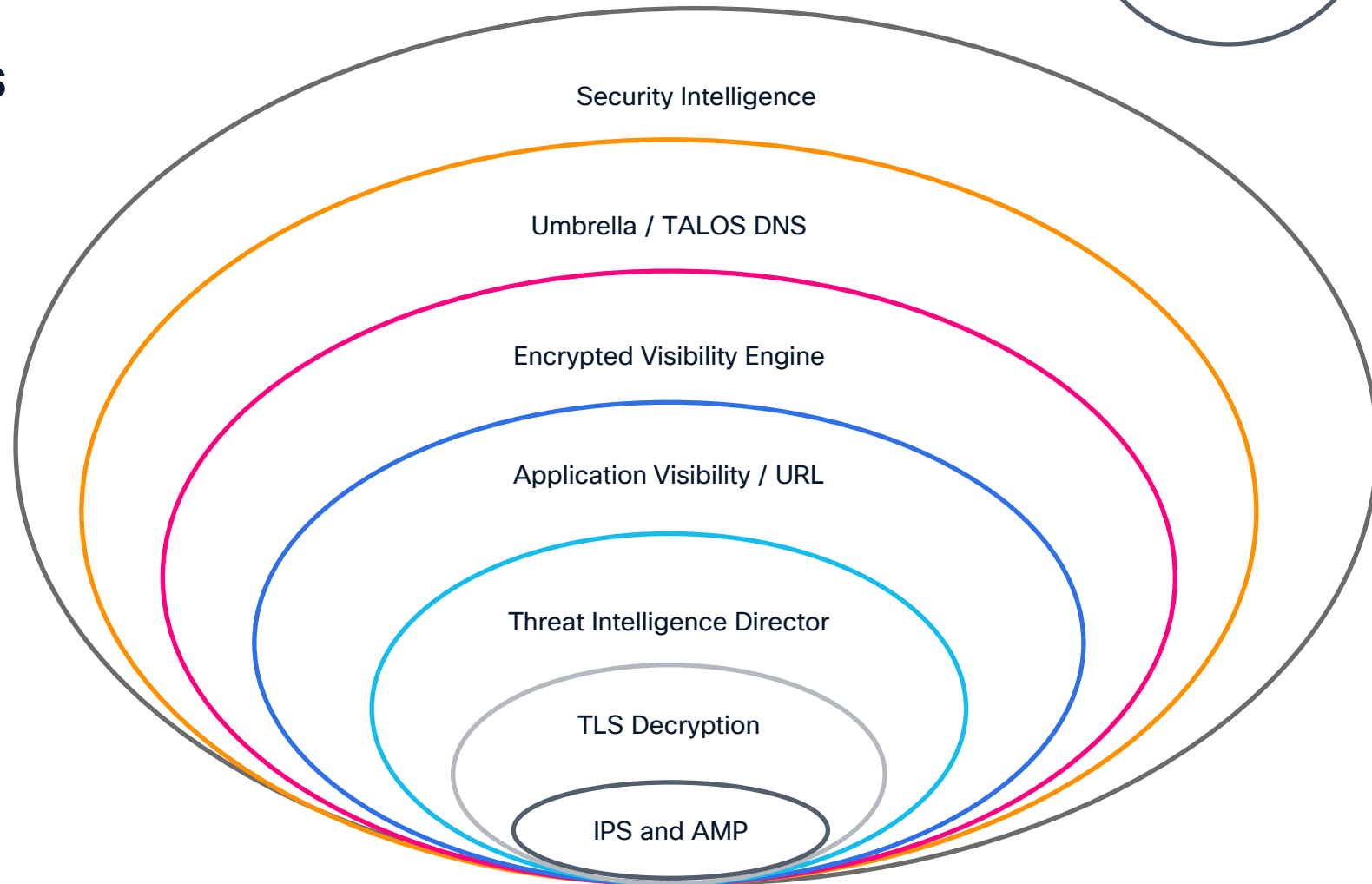
- NGFW / Intrusion Prevention
- Integrated TLS Visibility & Decryption
- VPN & Zero Trust Access Security
- Threat Intelligence Director
- Malware Analysis with Retrospection
- QUIC Fingerprinting
- Encrypted Visibility Engine



Layered Security built upon Snort ML



- Security intelligence feeds
- Umbrella / Talos DNS feeds
- Encrypted Visibility Engine
- Application Visibility
- URL Categories
- URL Categories
- Threat Intelligence Director
(3rd party STIX/TAXII)
- TLS Decryption
- IPS and AMP



Firewall Threat Defense SD-WAN Solution

- ✓ Powerful cloud or on-prem management of all capabilities
- ✓ Customizable VPN and routing capabilities up to 1000 sites
- ✓ Best in class edge security capabilities, especially for encrypted traffic



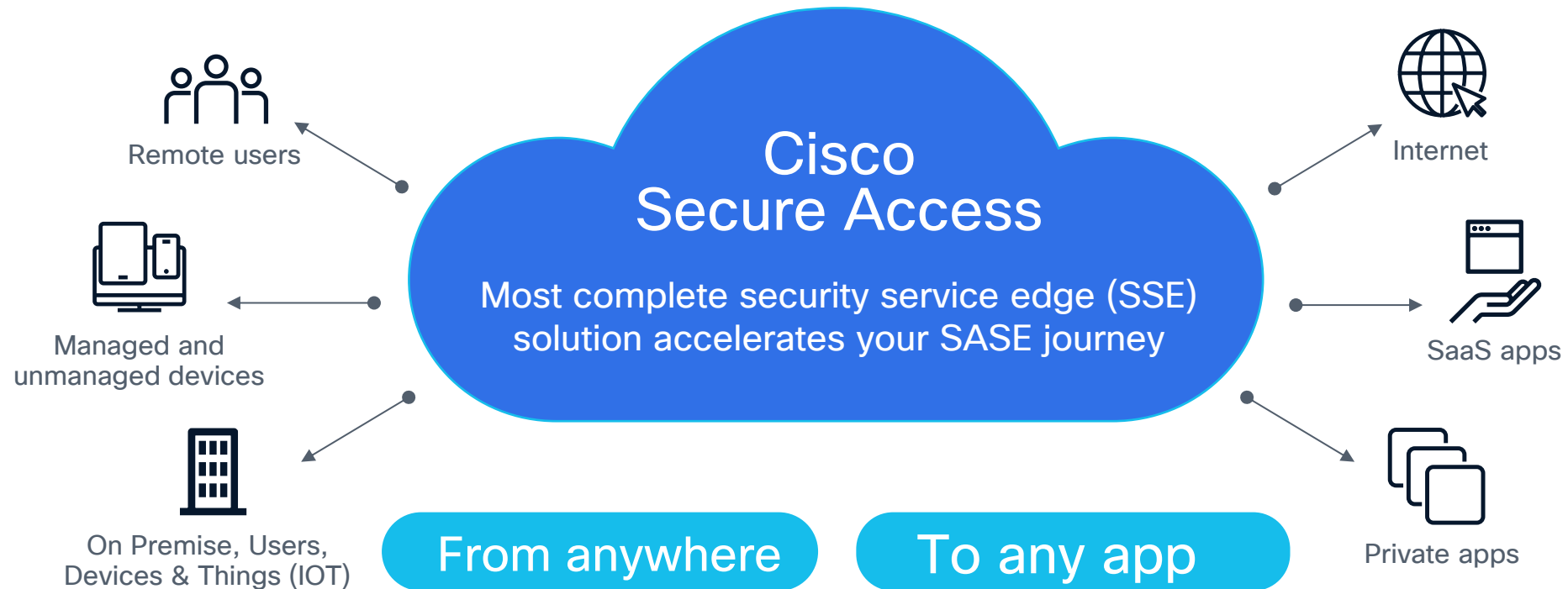


Security Service Edge (SSE)

Featuring Cisco Secure Access

Cisco Secure Access

Converged cloud security grounded in zero trust



Secure Access (“Security Service Edge”)

↔

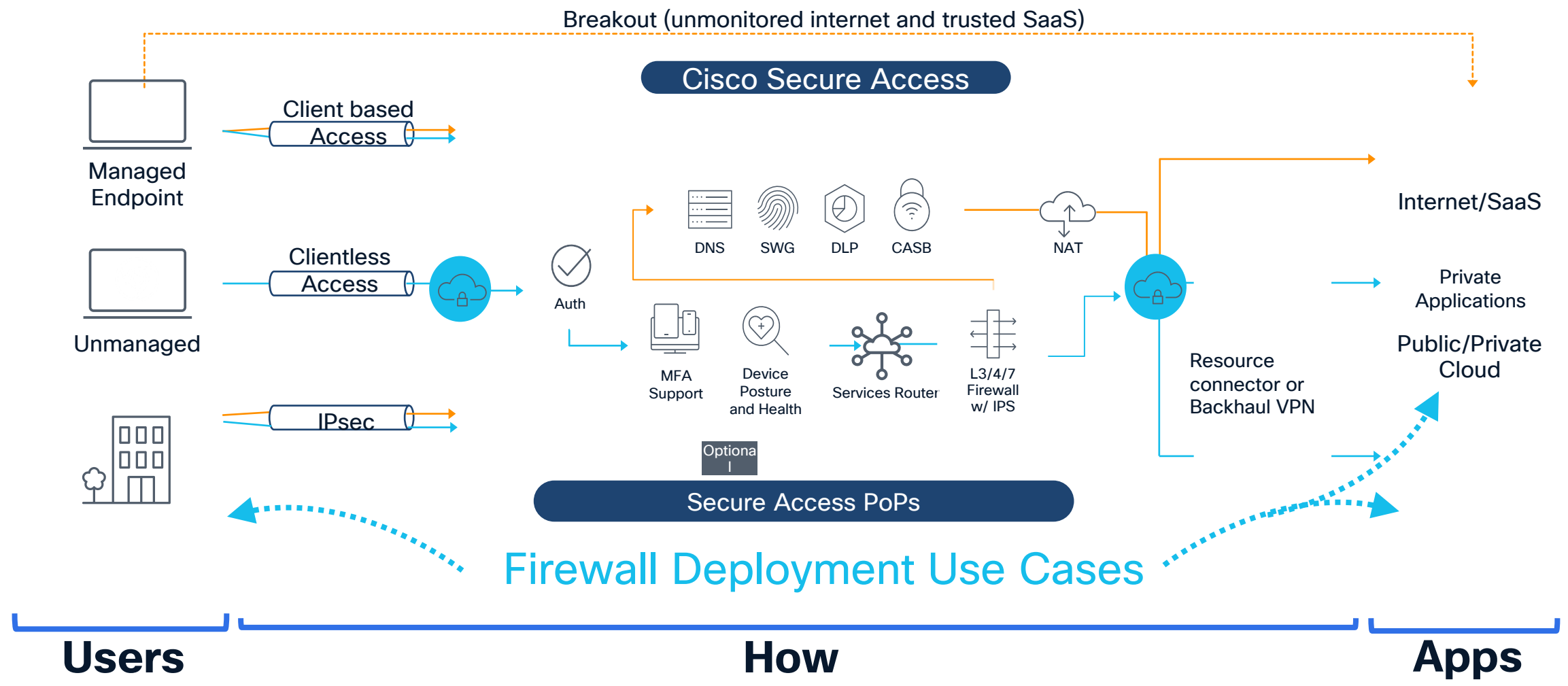
 Internet Traffic

→

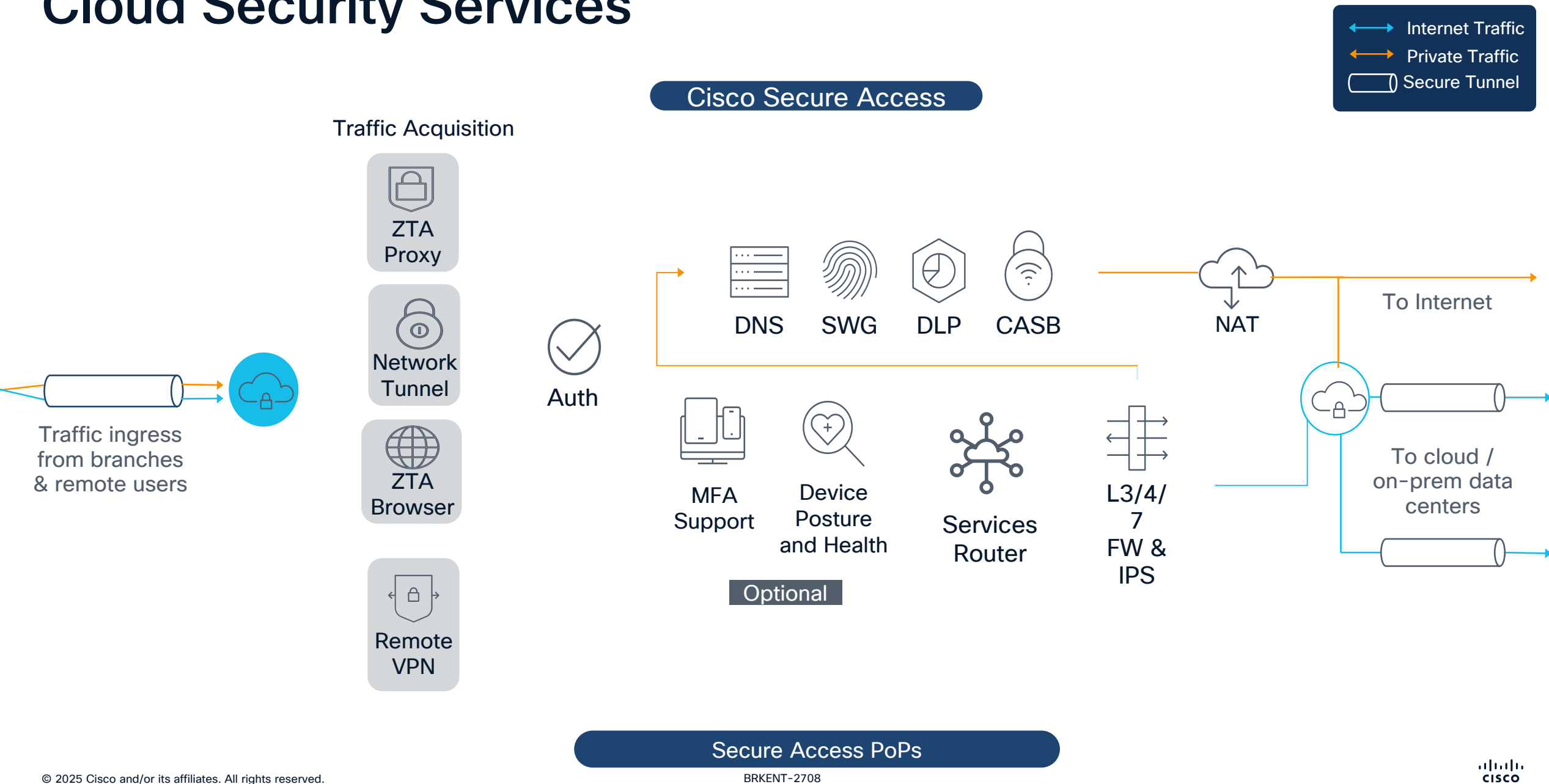
 Private Traffic

⬭

 Secure Tunnel



Cloud Security Services



Why connect your branches to Secure Access?

Internet Security:

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



DNS



DLP



CASB



SWG

Private application access:

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

SSE Integration

with Firewall Threat Defense

Secure Access Branch Tunnels

Firewall Management Center
Site To Site

OverviewAnalysisPoliciesDevicesObjectsIntegrationDeploy

admin

- Use dedicated Hub & Spoke VTI Tunnel topologies for simplicity
- Dual topologies for redundant tunnels to backup DC
- eBGP or static routing to Secure Access data centers
 - Can assign “branch networks” to tunnel on Cloud Side if using static routing.

Cisco Secure Access Routing Configuration

BGP or Static routing

Static Route considerations:

Set Next Hop as any IP address from within the VTI subnet

BGP Routing considerations:

Unique AS for each branch (eBGP)

Can not use iBGP based SD-WAN Topology Wizard!

Use Route Maps to restrict inbound / outbound route advertisements

Add Policy Based Route

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

Internal-Subnet x

Match Criteria and Egress Interface
Specify forward action for chosen match criteria.

Add

Match ACL	Forwarding Action
ACL_PBR_Internet	Send through 169.254.0.5 169.254.0.9

Add Forwarding Actions

Match ACL:* ACL_PBR_Internet +

Send To:* IP Address

IPv4 Addresses: 169.254.0.5,169.254.0.9

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

FTD Branch with Secure Access

Routes from Secure Access:

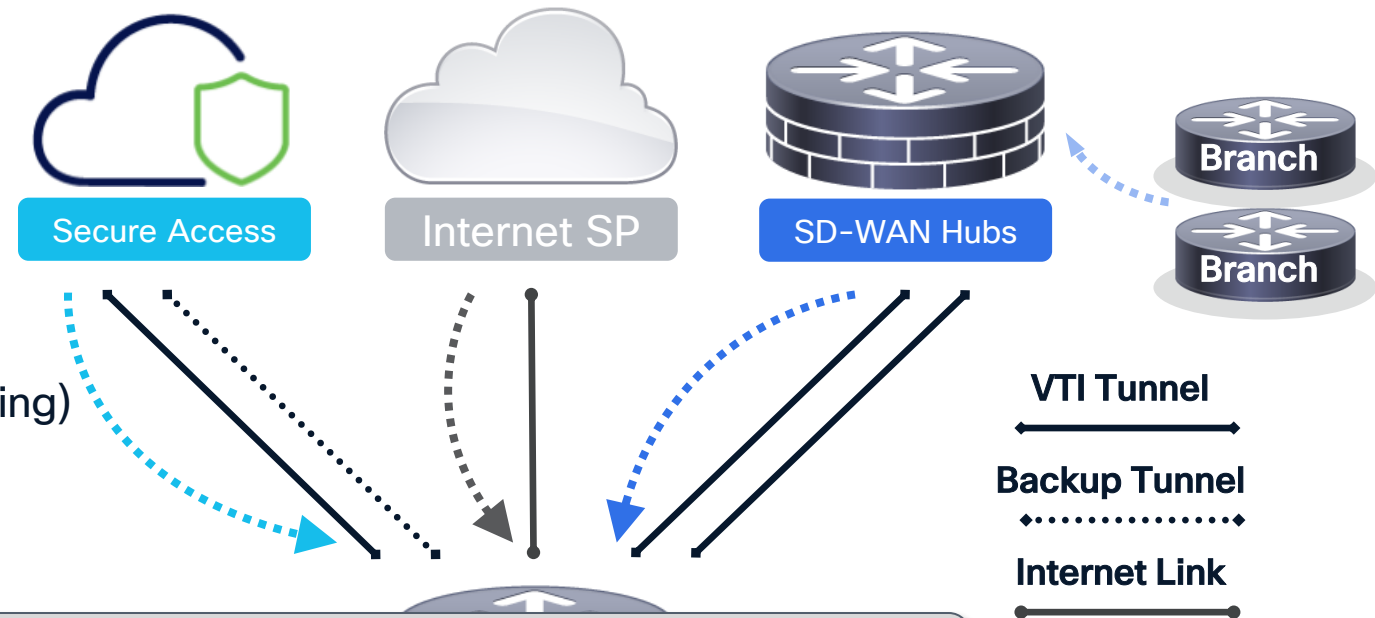
- Default Route* (Optional)
- RAVPN Subnets, Zero Trust enabled applications, Proxy Infrastructure

Static routes to ISP:

- Secure Access DC VPN Endpoint IPs (prevent flapping)

Routes from SD-WAN Hubs:

- SD-WAN HQ, branches, and data centers



```
FTD-Spoke# show route
```

```
B* 0.0.0.0 0.0.0.0 [20/0] via 169.254.0.5
```

```
B 100.73.x.0 255.255.240.0 [20/0] via 169.254.0.5
```

```
S 35.171.x.188 255.255.255.255 [1/0] via 64.x.14.254, outside
```

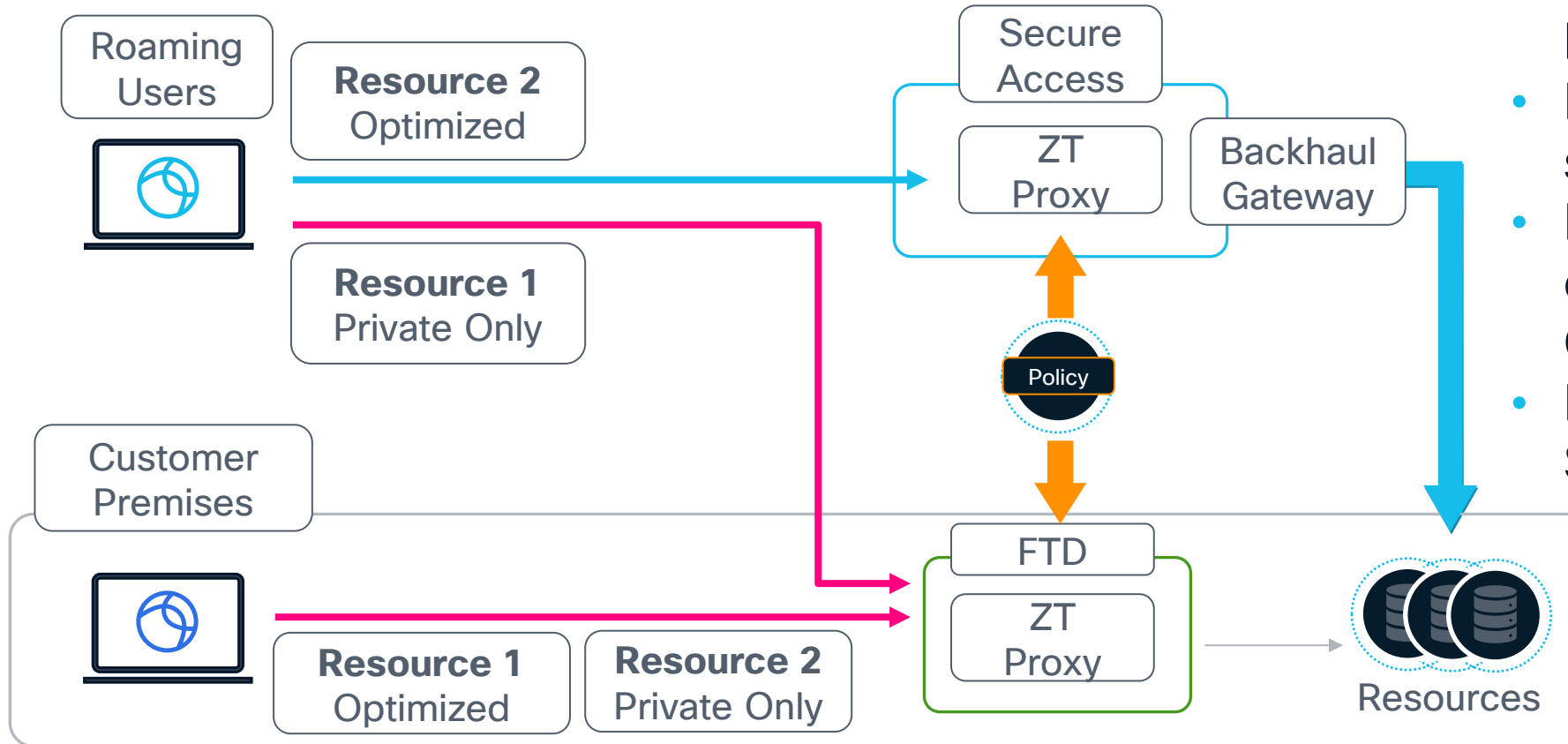
```
S 217.195.x.188 255.255.255.255 [1/0] via 64.x.14.254, outside
```

```
V 1.0.1.1 255.255.255.255 connected by VPN (advertised), outside_static_vti_1
```

```
V 1.0.2.1 255.255.255.255 connected by VPN (advertised), outside_static_vti_2
```

Hybrid Private Access with Secure Firewall

Single Policy, Distributed Enforcement (Overview)



- Optimal connectivity based on user location
- Enterprise privacy for sensitive resources
- Resiliency in case of catastrophic Cloud Outage (Future)
- Managed through Security Cloud Control

Firewall Threat Defense

③

New

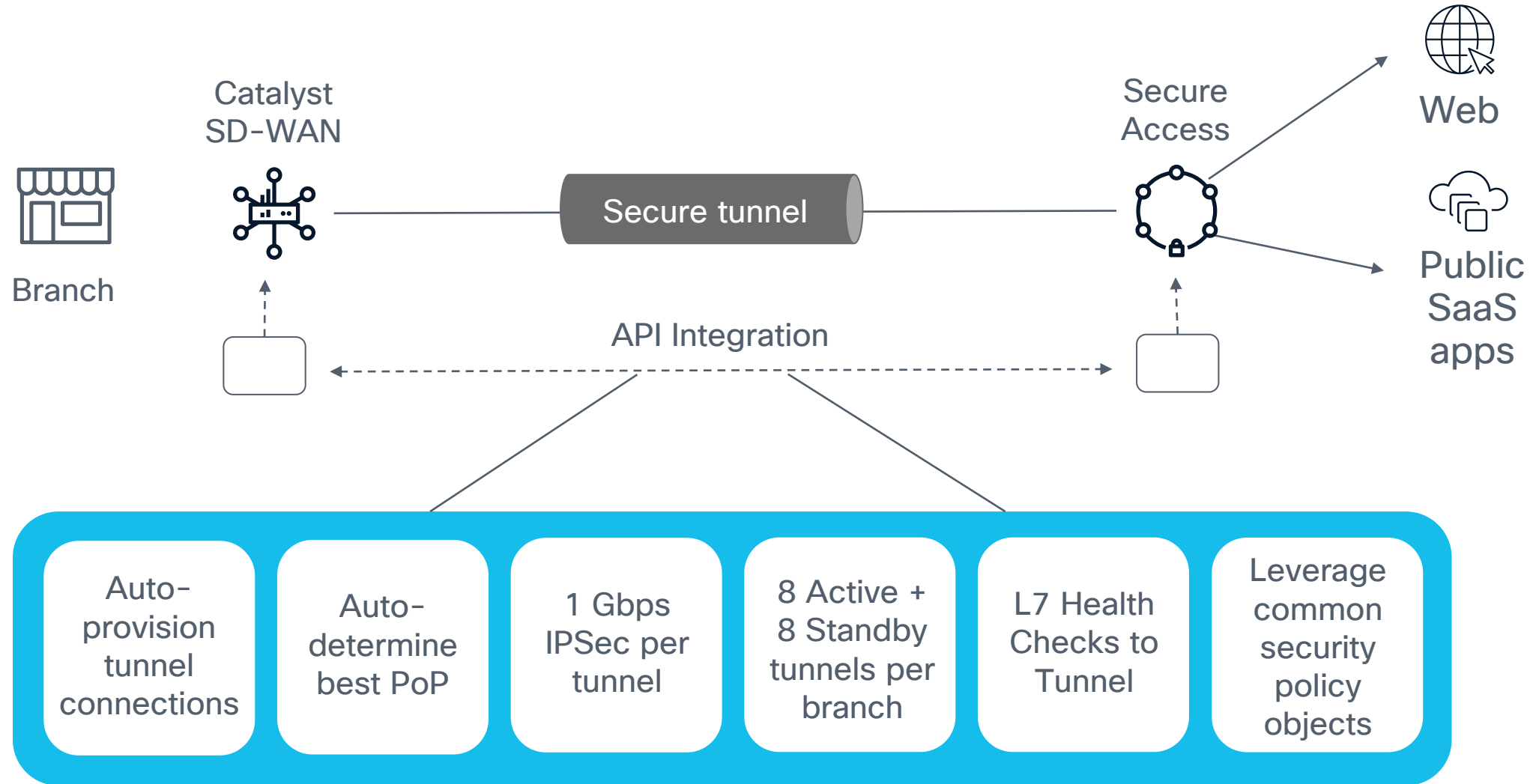
9

Prerequisites

☐ ☒ Peer to Peer☒ Full Mesh

SSE Integration with Catalyst SD-WAN

Secure Access + Catalyst SD-WAN

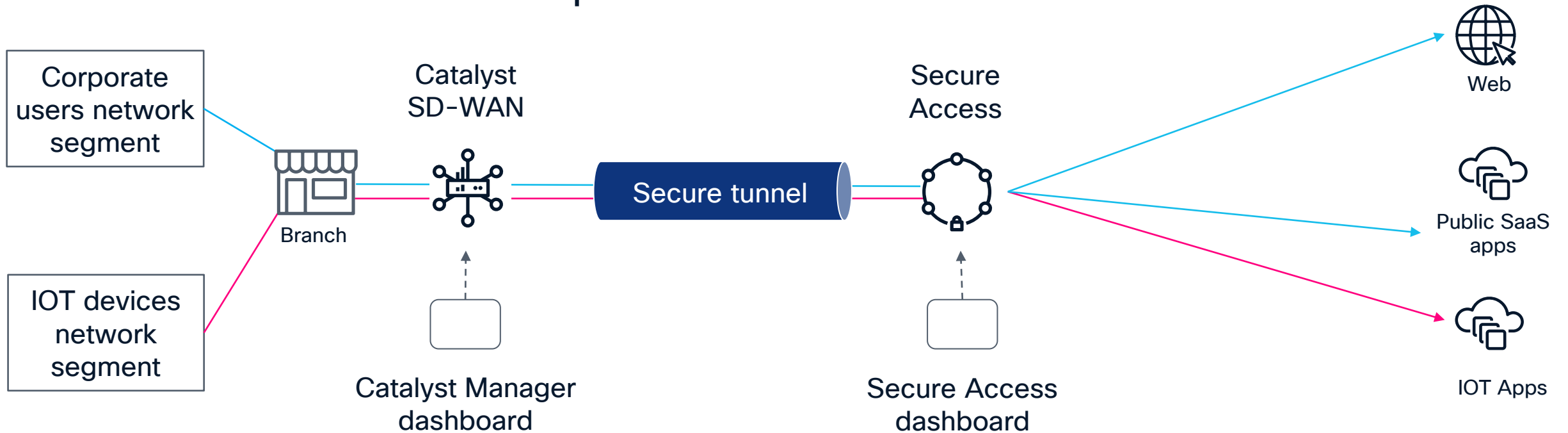


Better Together – Simplified SASE Implementation

Secure Access + Catalyst SD-WAN

Secure Internet Access (SIA), for branch networks, “coarse grain” segmentation

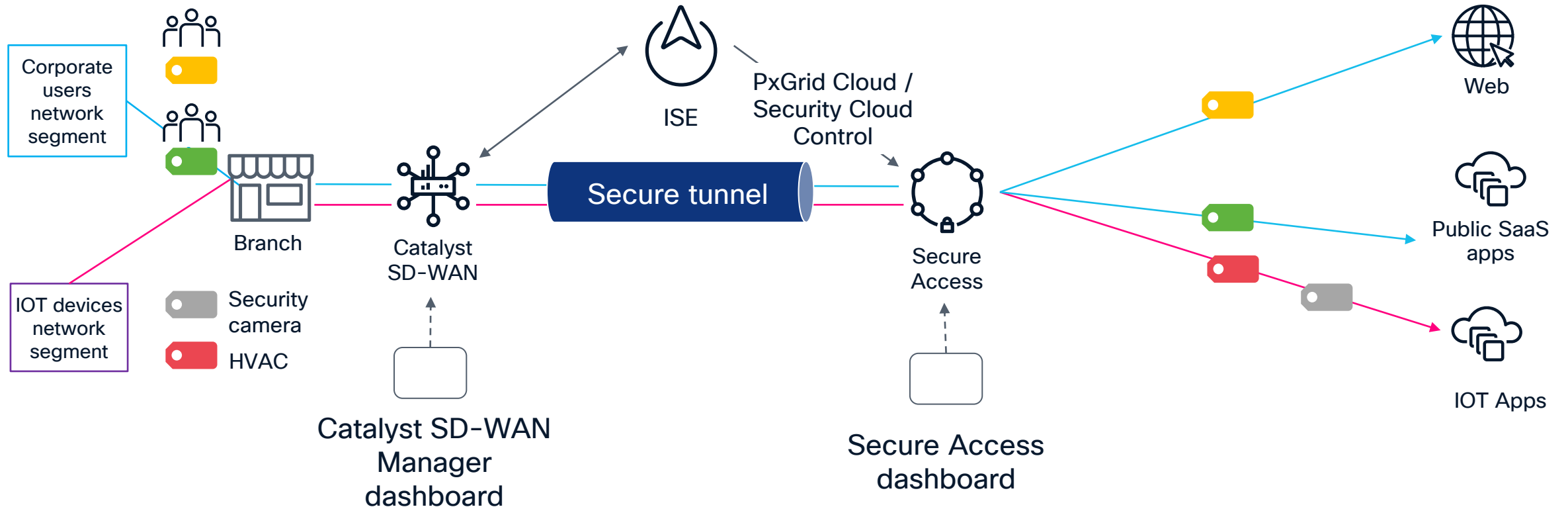
Context from SD-WAN VRF aka VPN
represented as VPN ID



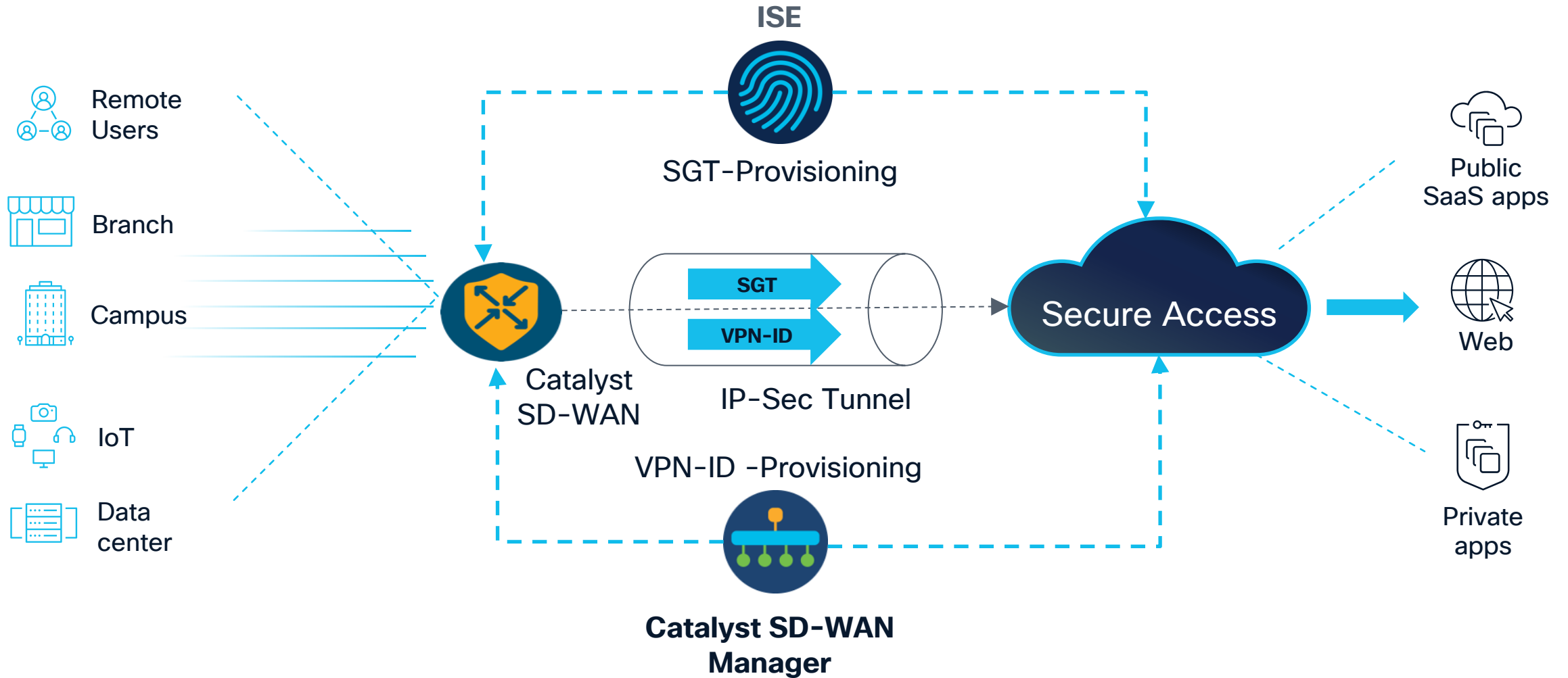
Secure Access + Catalyst SD-WAN

Secure Internet Access (SIA), for branch networks, “fine grain” segmentation

Context from ISE Security Group Tag/SGT



Macro and Micro Segmentation Based Policy



Overview

Connect

Resources

Secure

Monitor

Admin

Workflows

Integrations

Secure Access supports the integration of various Cisco solutions, which allow you to enhance Secure Access network management and security. [Help](#)

Catalyst SD-WAN only
ISE integration with Secure Access is supported for Catalyst SD-WAN only.

Cisco Identity Services Engine – Security Trust Group Tag Integration

The integration of Secure Access with Identity Services Engine (ISE) streamlines the deployment of Security Group Tags (SGTs). This enables dynamic network segmentation and allows for more granulate access controls. [Help](#)

As of: May 23, 2024, 1:47 PM

☐	Name	Date	Type	Status	
☐	test_demo_2	May 23, 2024	pxgrid	Active	...

Secure Access SGT Integration with Catalyst SDWAN

SSE Integration with Meraki MX

Zero Friction: One SSE, Cisco Secure Access

Cisco Secure Connect

Meraki + Umbrella,
Secure Access (ZTNA only)



Cisco Secure Access

Meraki + Secure Access
(full suite of Cisco SSE capabilities)

Connect Meraki to Cisco Secure Access

Choose your SASE dashboard experience

Centralized management

Streamlined management of networking and security (Secure Access) in the Meraki dashboard



Manage AutoVPN in Meraki

Manage MX and Secure Access policies together

End-to-end customer support from single team

Multi-console management

Management of networking and cloud security in separate dashboards.

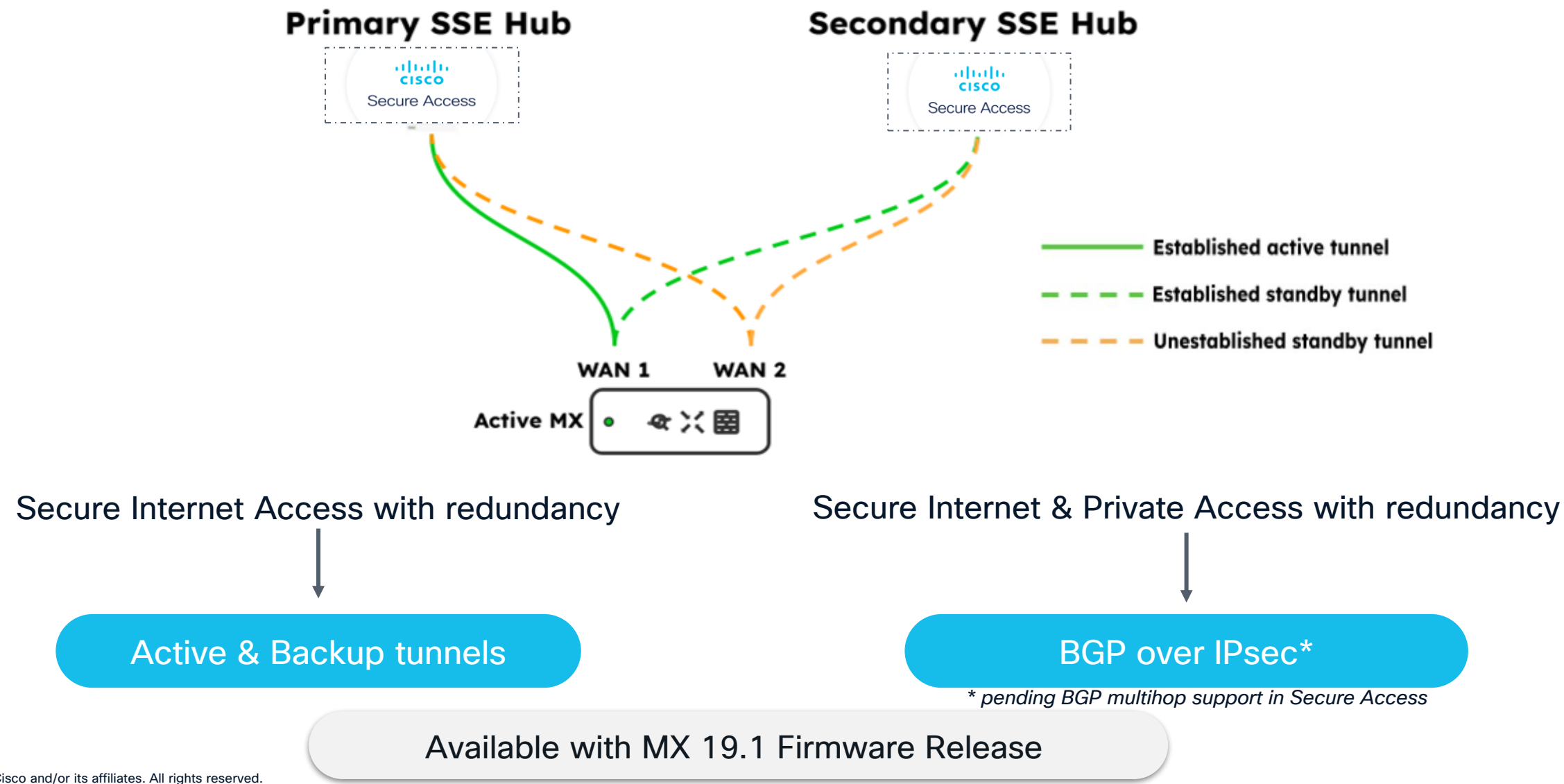


Manage AutoVPN in Meraki

Manage SSE policies in Secure Access

Customer support from Meraki (AutoVPN) & Cisco TAC (Secure Access)

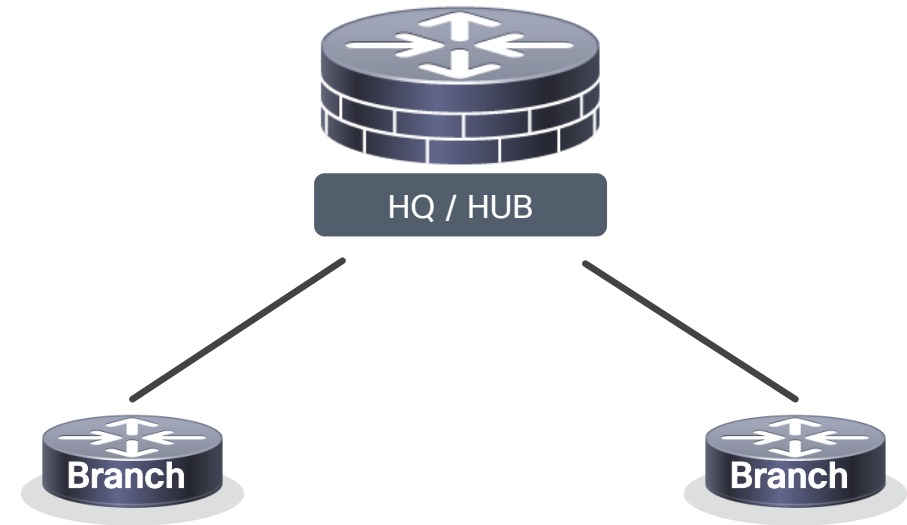
Secure Access (IPSEC VPN Redundancy)



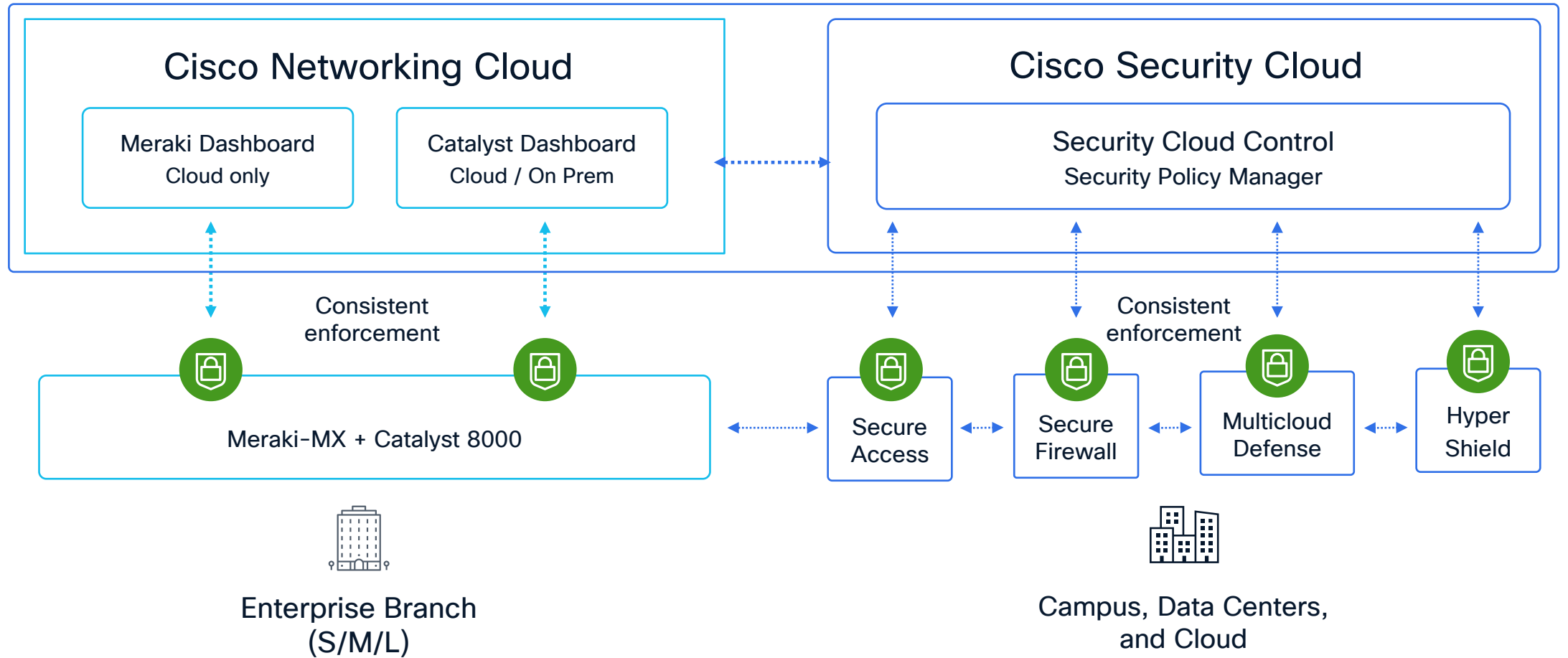
Cisco's secure & scalable SD-WAN solutions

All Cisco SD-WAN Platforms offer:

- Scalable (1000+) hub & spoke node designs
- Application Policy Based Routing
- Robust on-box branch security capabilities
- SASE / SSE integration with Secure Access / Secure Connect
- Each platform architecture offers unique differentiation for use case specific benefits!



Unified Secure SD-WAN experience



SD-WAN Capability High-level comparison

	Scalable Hub & Spoke VPN	App based Policy Routing	Path Optimization & Redundancy	Forward Error Correction	Packet Duplication	Per tunnel & Per VPN QoS	Zero Touch Provisioning	SD-WAN Analytics	Overlay / tunnel segmentation
Catalyst 8k	✓	✓	✓	✓	✓	✓	✓	✓	✓
Meraki MX	✓	✓	✓	✗	✗	✗	✓	✓	✗
Secure Firewall	✓	✓	✓	✗	✗	✗	✓	✓	✓

 * These capabilities primarily beneficial for on-prem / branch to branch VoIP

Security Capability High-level comparison

	L7 App based Firewall policies	User & TrustSec firewall policies	Snort IPS Security	Advanced Malware Protection	Cloud based file sandbox analysis	Encrypted Traffic Visibility	TLS / QUIC decryption	Cloud Event Logging	Splunk integrations
Catalyst 8k	✓	✓	✓	✓	✓	✗	✓	✓	✓
Meraki MX	✓	✓	✓	✓	✓	✗	✓	✓	✓
Secure Firewall	✓	✓	✓	✓	✓	✓	✓	✓	✓

Firewall Threat Defense has advanced encrypted traffic visibility & QUIC decryption!

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



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

Contact me at: Insert preferred comms method

Thank you

CISCO Live !

