Elevating the Security in your SD-WAN

BRKENT-2708

Jeff Fanelli
Distinguished Engineer

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!

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Webex App

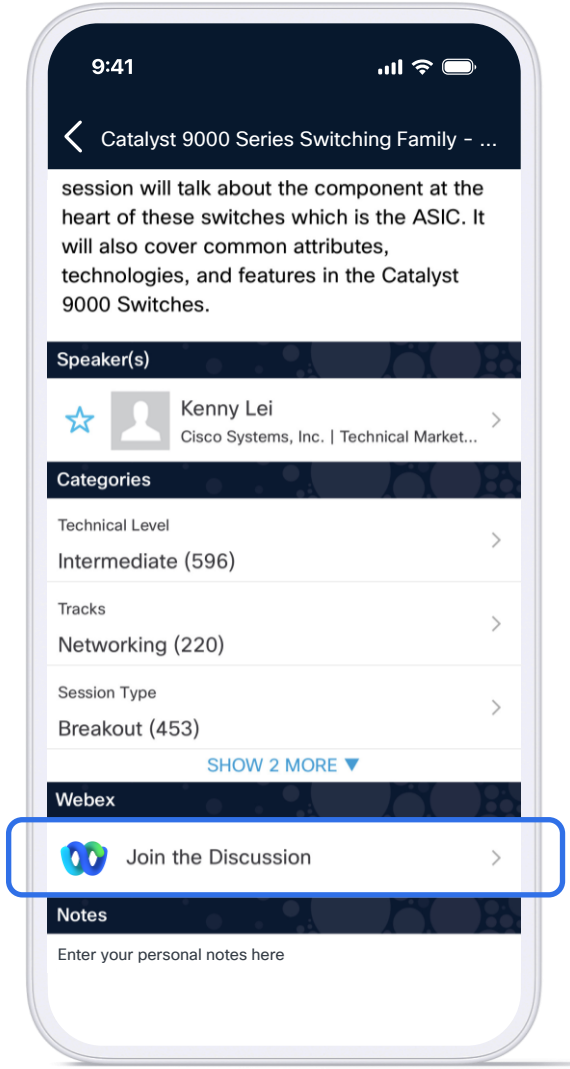
Questions?

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**

© 2025 Cisco and/or its affiliates. All rights reserved.

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

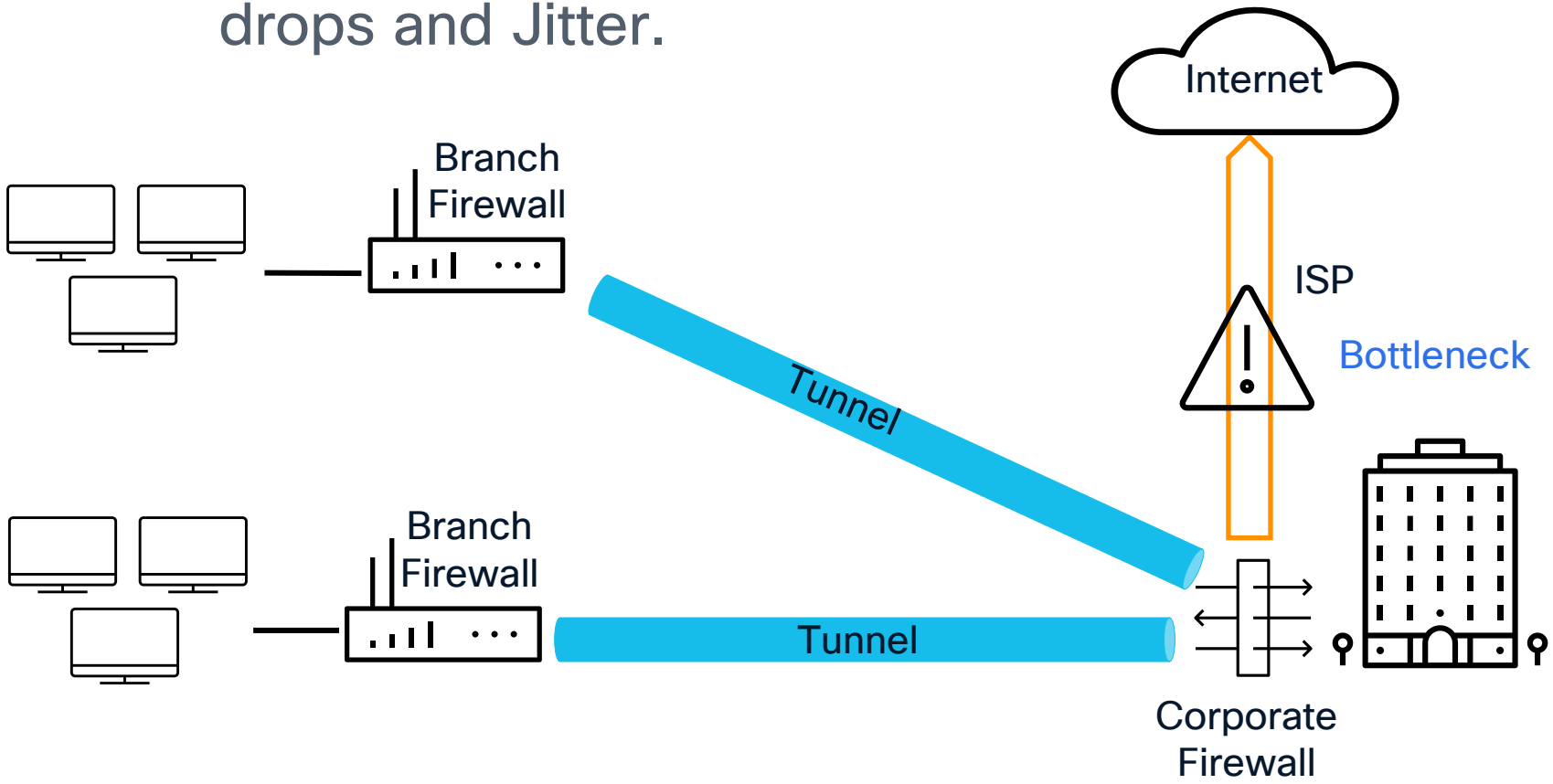
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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.



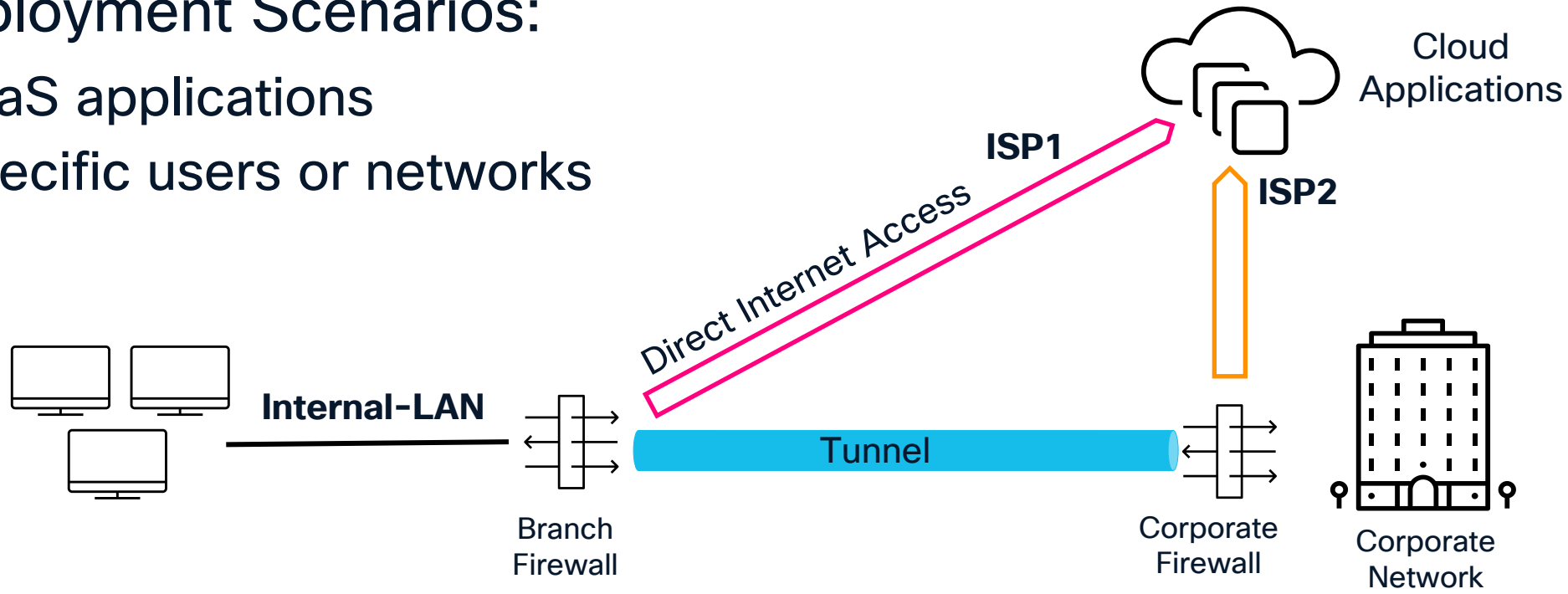
© 2025 Cisco and/or its affiliates. All rights reserved.

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

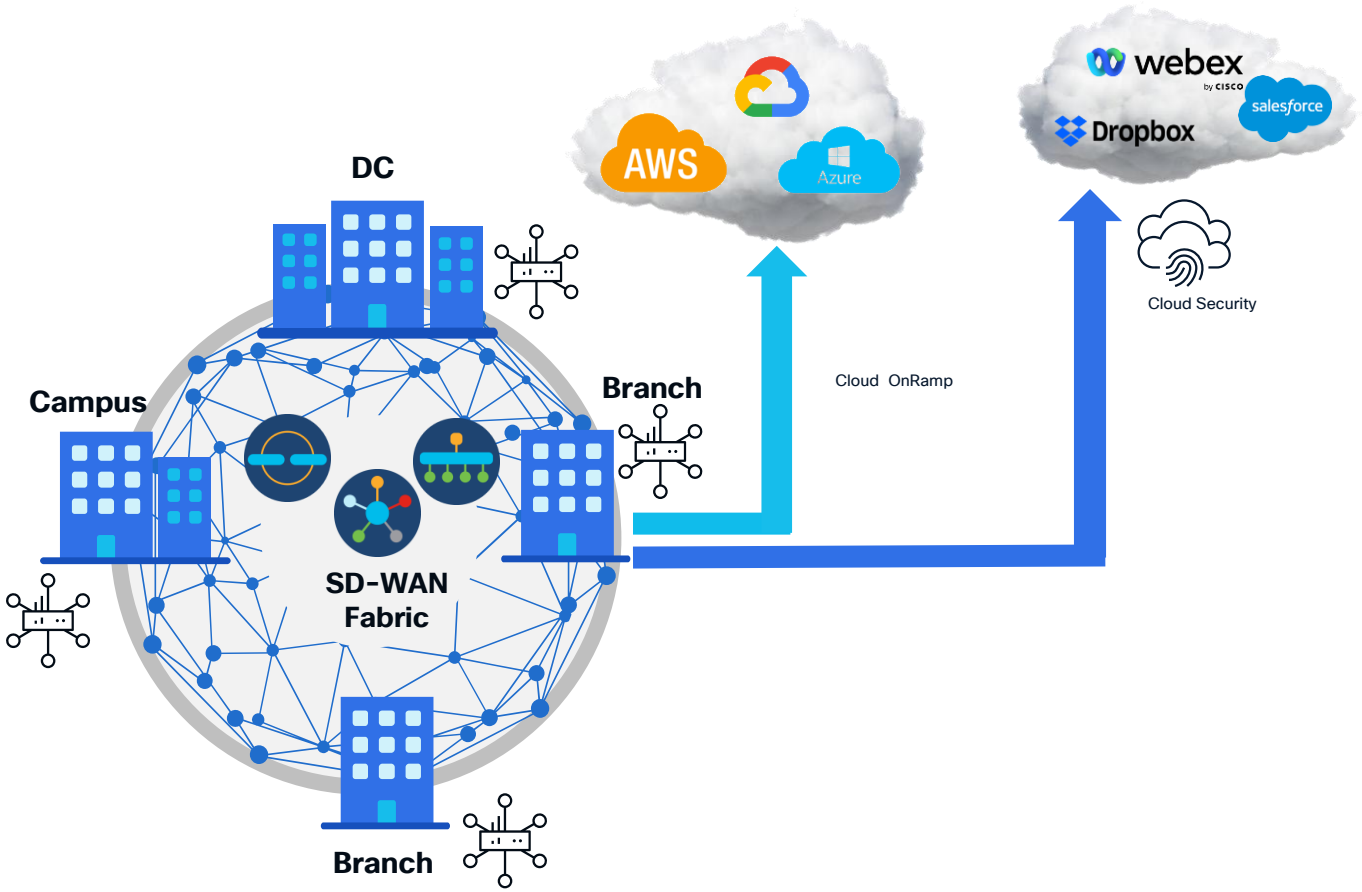


© 2025 Cisco and/or its affiliates. All rights reserved.

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.

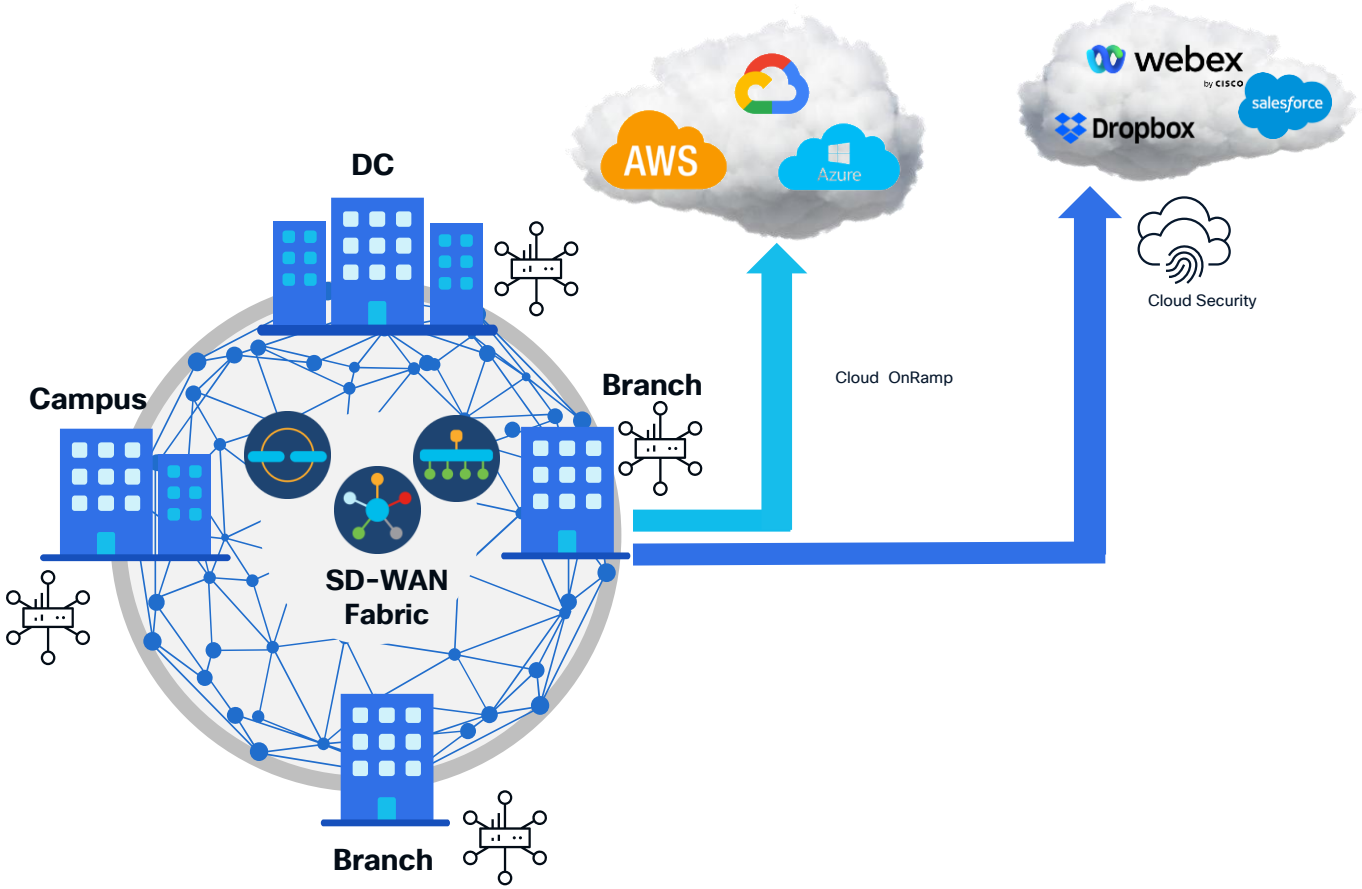


© 2025 Cisco and/or its affiliates. All rights reserved.

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

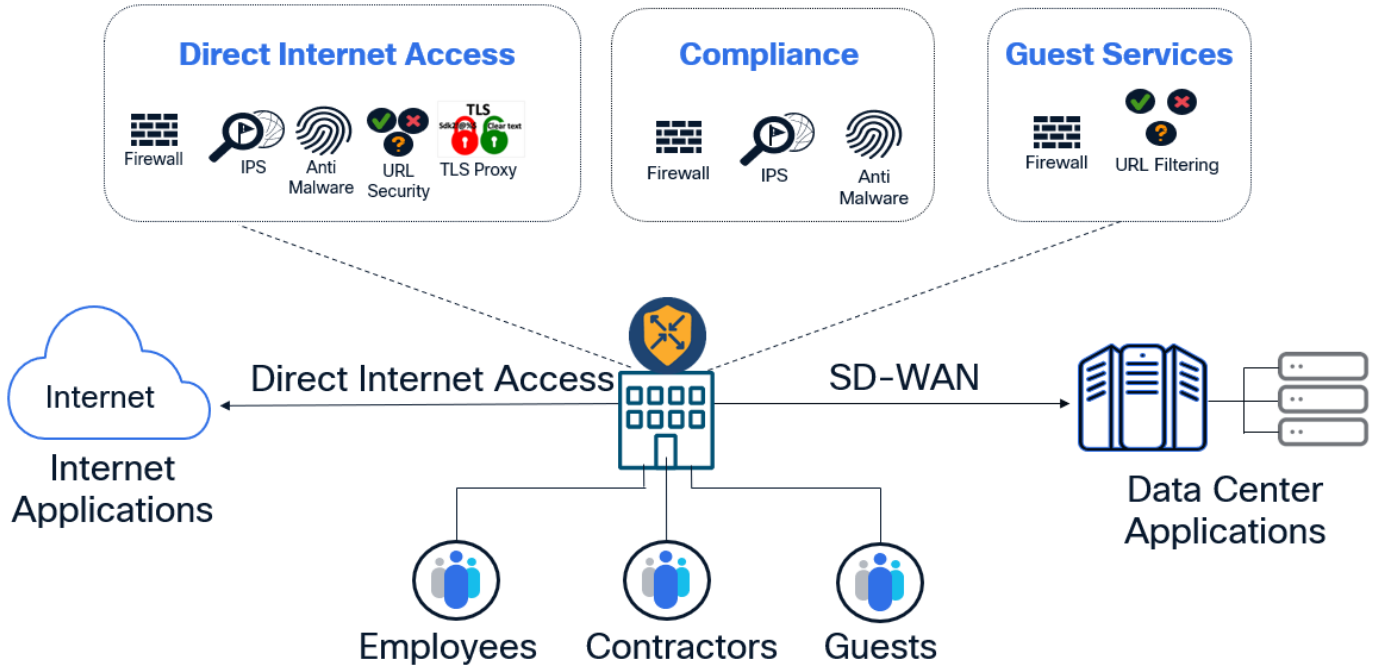


© 2025 Cisco and/or its affiliates. All rights reserved.

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.)



© 2025 Cisco and/or its affiliates. All rights reserved.

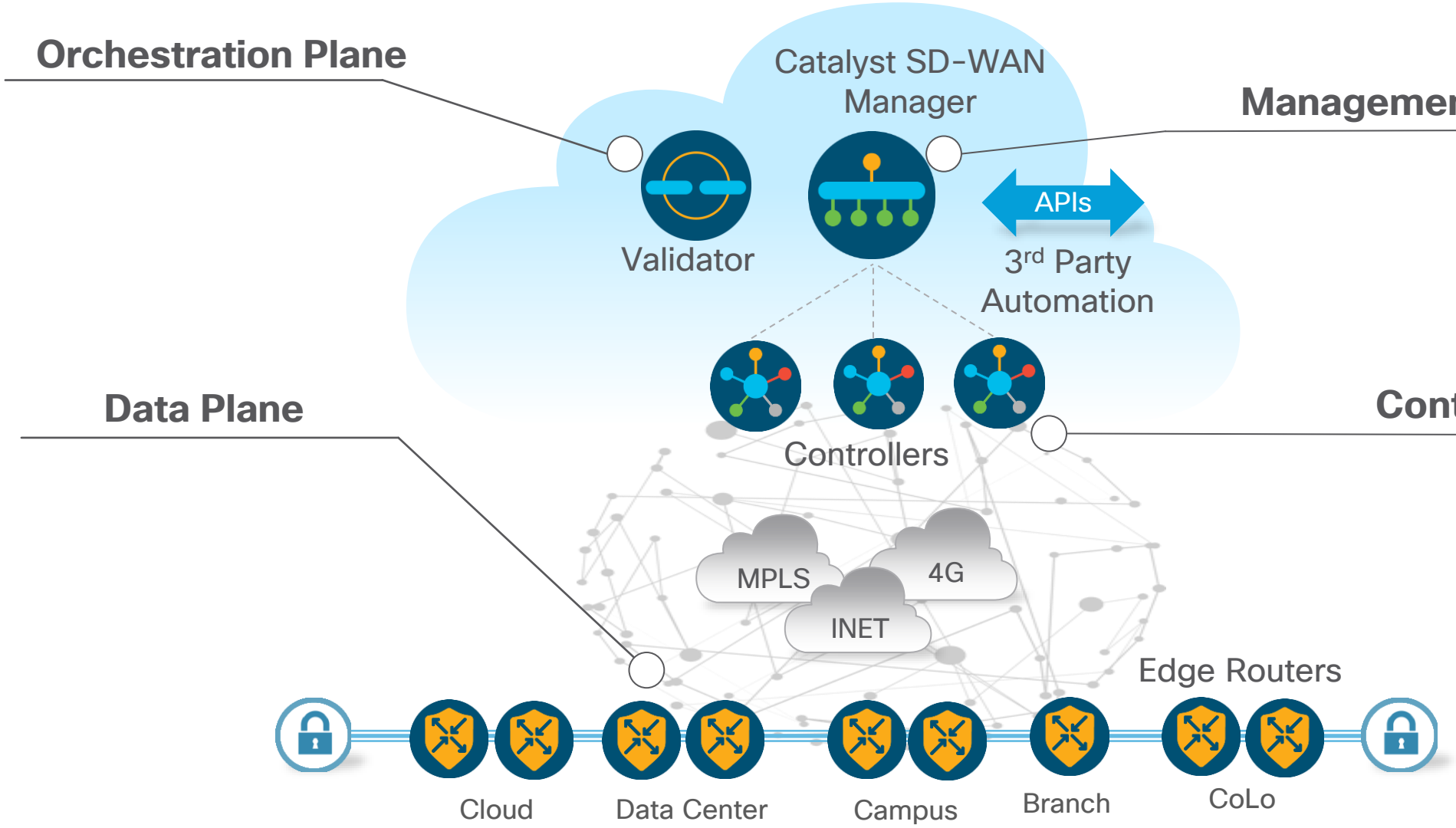
Catalyst SD-WAN
Use Cases & Capabilities

CISCO Live !

Use Case Flow

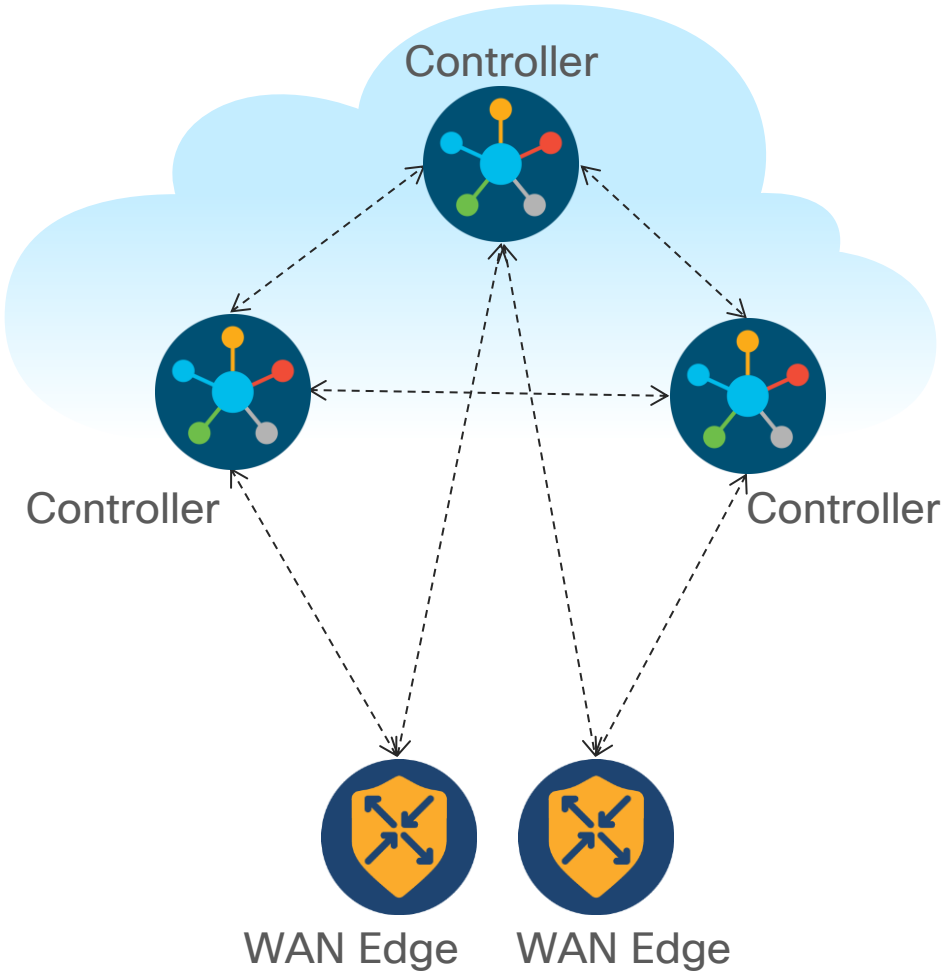
© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst SD-WAN Architecture



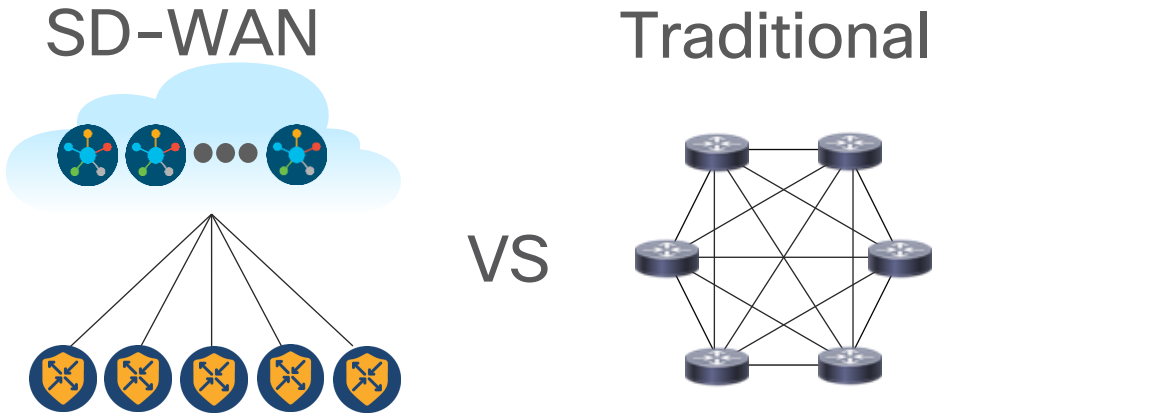
© 2025 Cisco and/or its affiliates. All rights reserved.

Overlay Management Protocol (OMP)



Note: WAN Edge routers need not connect to all Controllers

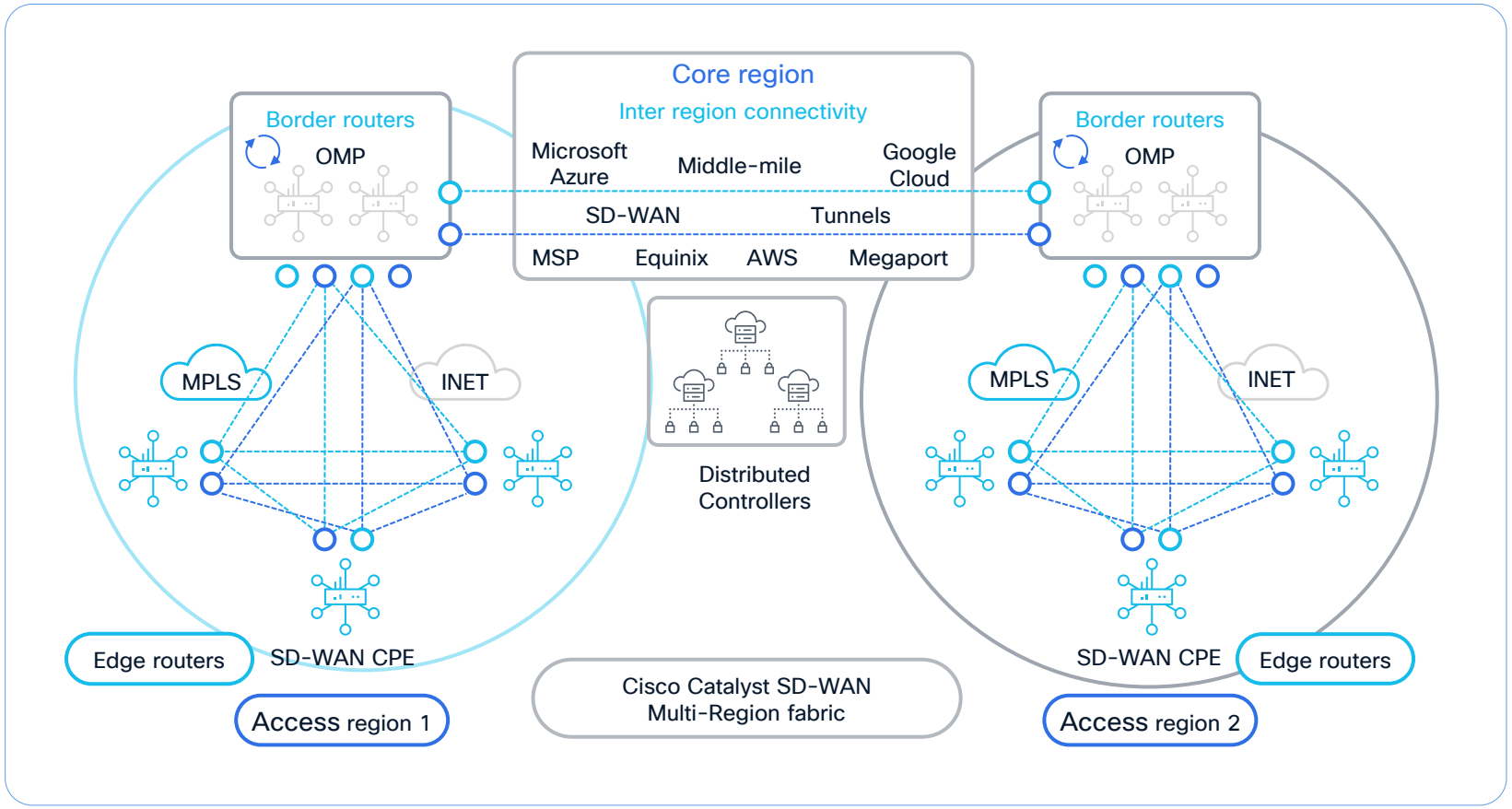
- Overlay Management Protocol (OMP)
- Runs between WAN Edge routers and Controller and between the Controllers
  - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
- Dramatically lowers control plane complexity and raises overall solution scale



© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst SD-WAN Multi-Region Fabric

SD-WAN evolved for any middle-mile topology



WAN Fabric

- 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

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Catalyst SD-WAN Security Capabilities

Overview

Fabric Security

- Encrypted Control Plane
- Encrypted Data Plane
- Enhanced Security – Pairwise keys
- HW Based Device Authentication (SUDI)

Sec-Ops Monitoring & Visibility

- Manager SecOps Dashboard
- End-to-End Monitoring & Visibility

Embedded Security

- **Firewall** Stateful ZBFW
- **Segmentation** With Multi-Topology
- **AMP** File Reputation & Sandboxing from Talos
- **IPS** Protection against complex threats (Snort)
- **URL Filtering** 82+ Web Categories
- **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

Cisco Umbrella

Third Party SSE

© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst SD-WAN Manager (UI)

Overview

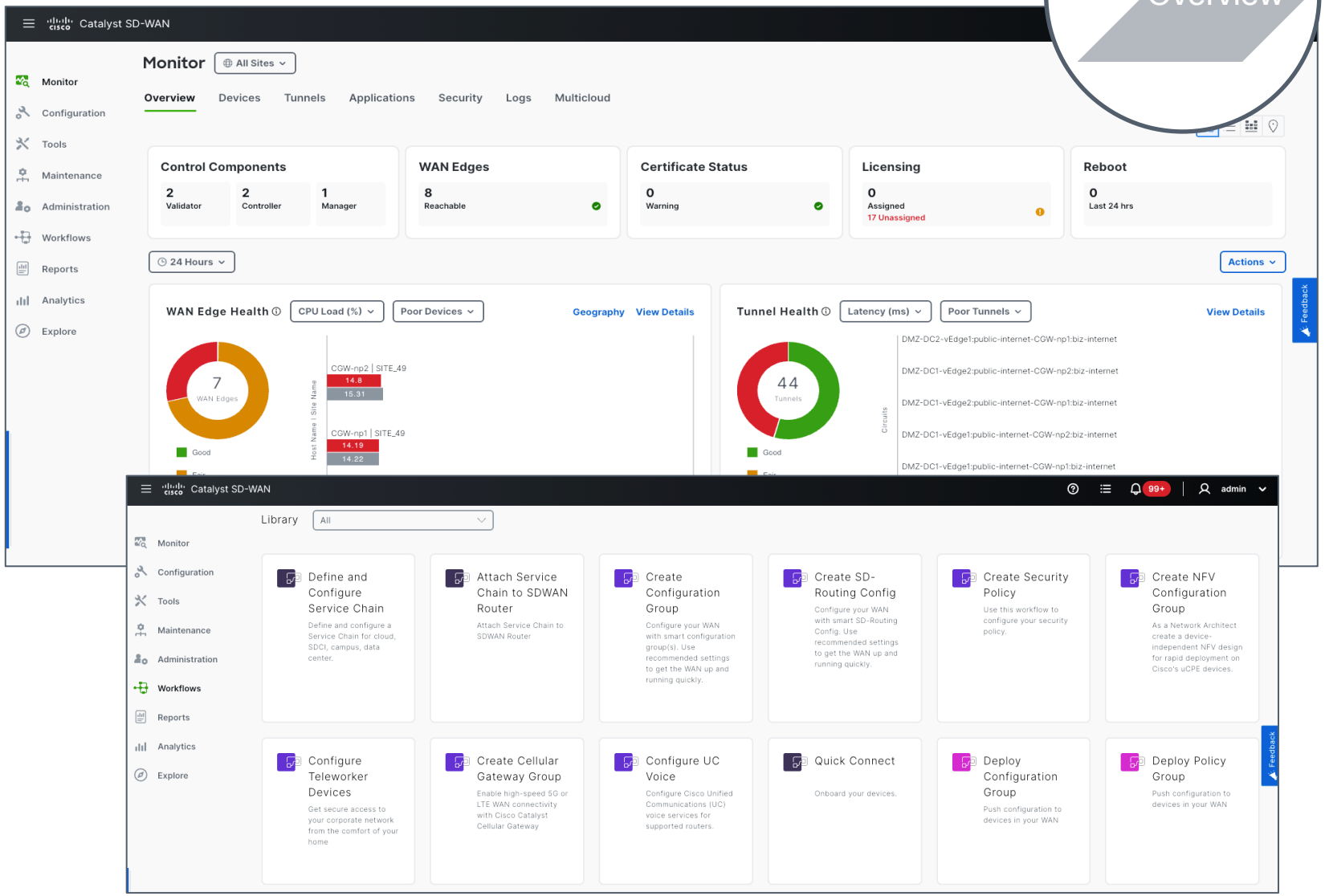
Enhanced UI

Guided Workflow

Simplified Configuration

Granular Management

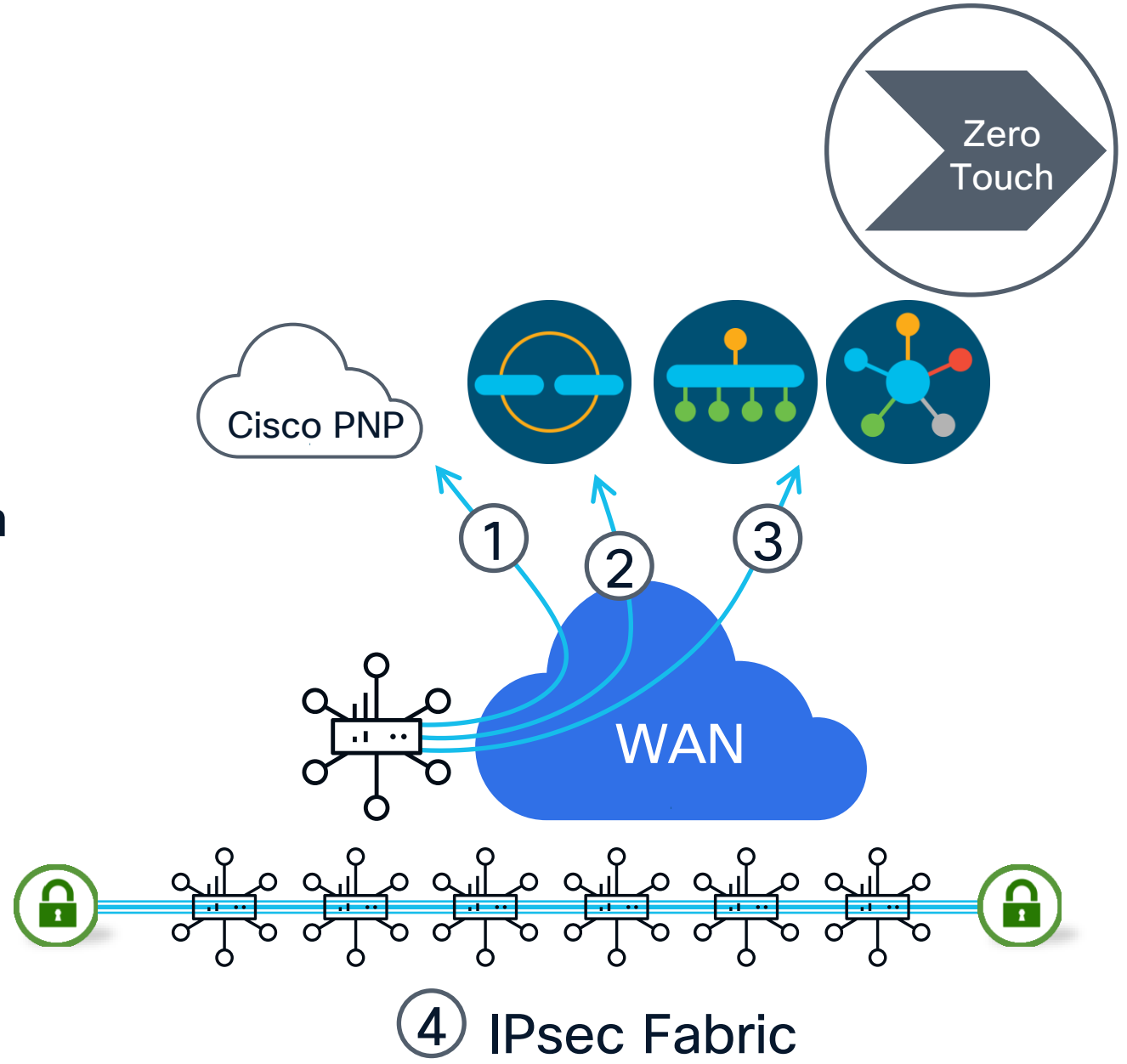
Smart Troubleshooting



© 2025 Cisco and/or its affiliates. All rights reserved.

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



© 2025 Cisco and/or its affiliates. All rights reserved.

Application Experience

App Routing

Configuration Management System

Manager - Virtualized | Scalable | Network Insights

Forward Error Correction

Packet Duplication

TCP Optimization

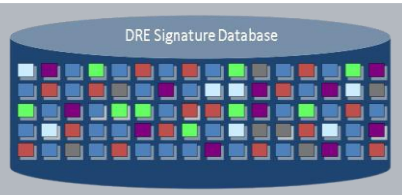
BBR2 Congestion Algorithm

Window Scaling

Large Initial Windows

Selective Acknowledgement

DRE, LZW



Byte Level Caching & Compression

Protocol Agnostic

Key building blocks

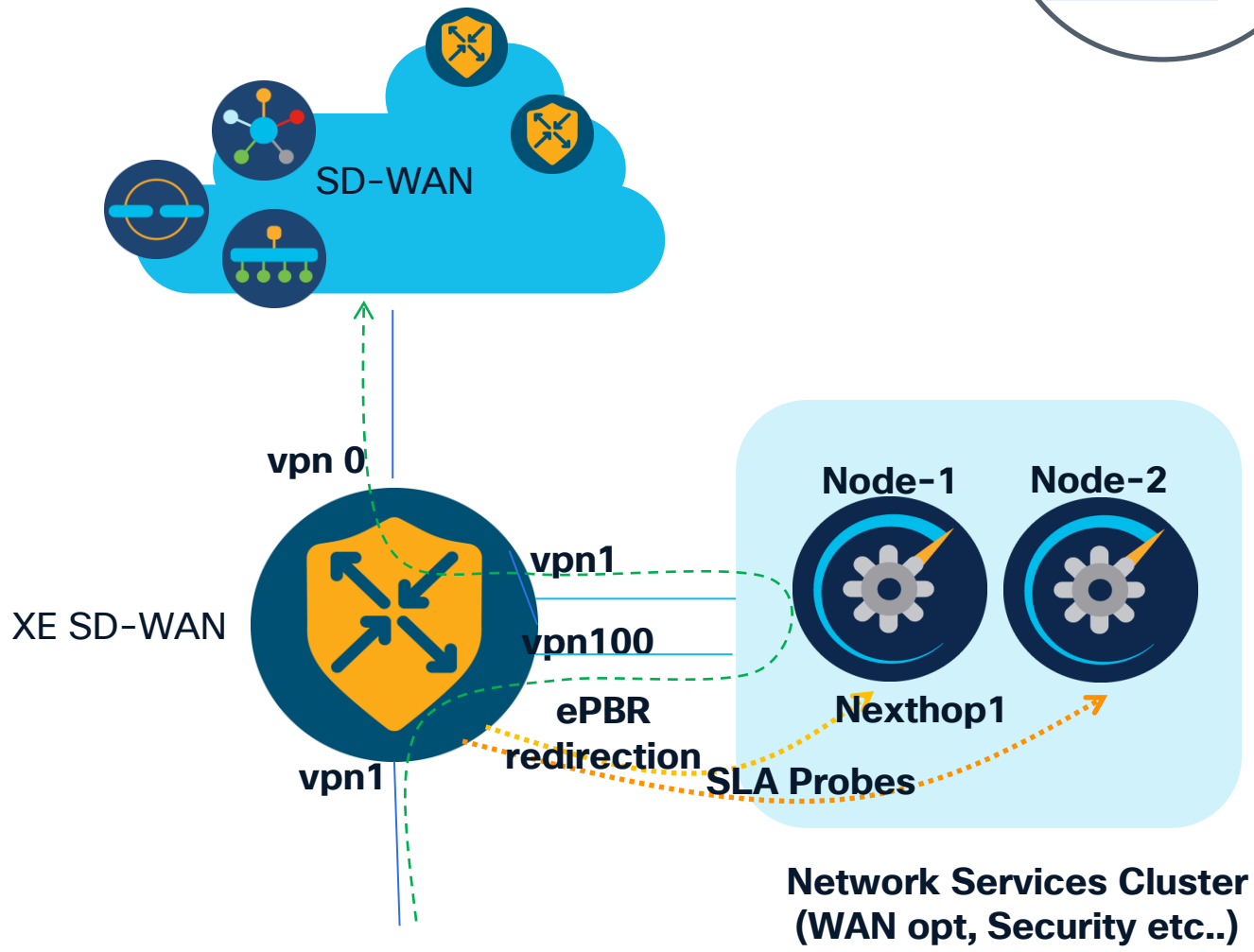
BBR - Bottleneck Bandwidth and Round-trip propagation time

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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



© 2025 Cisco and/or its affiliates. All rights reserved.

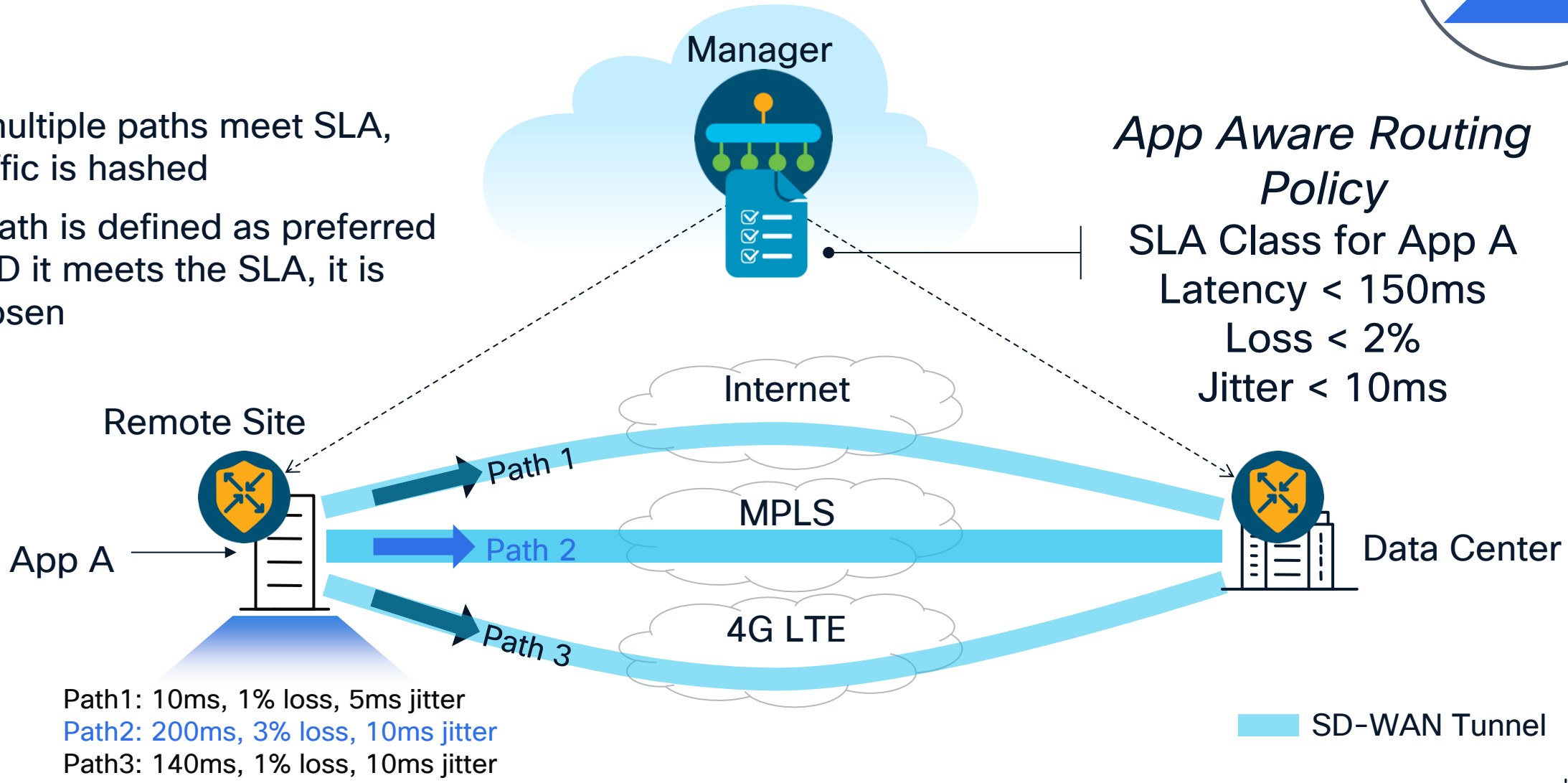
cisco

Enhanced Application-Aware Routing

Improved Application Performance Experience (from mins to sec)

App Routing

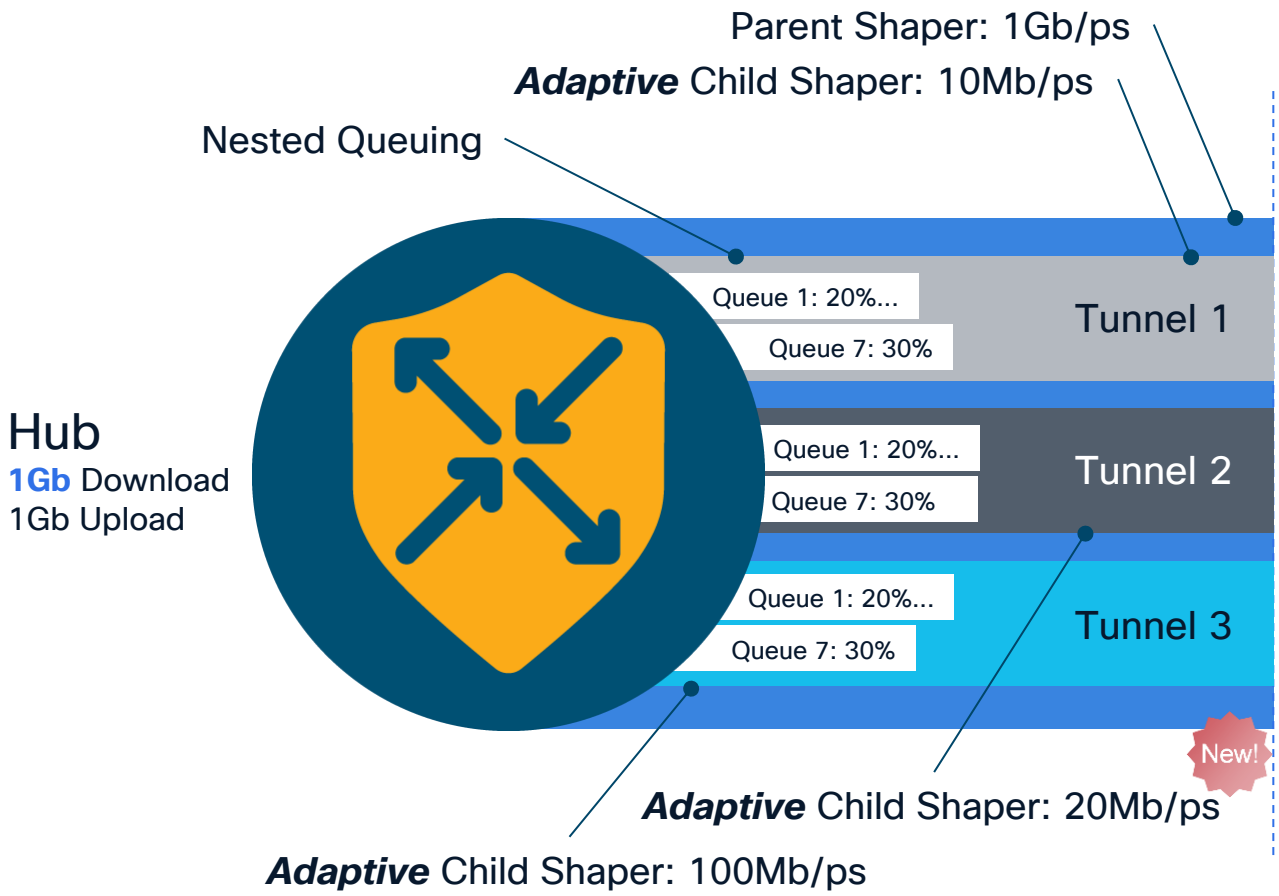
- If multiple paths meet SLA, traffic is hashed
- If path is defined as preferred AND it meets the SLA, it is chosen



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Per-Tunnel QoS with Adaptive Shaping



Hub
1Gb Download
1Gb Upload

SD-WAN Fabric

Spoke 1
10Mb Download
10Mb Upload

Spoke 2
20Mb Download
5Mb Upload

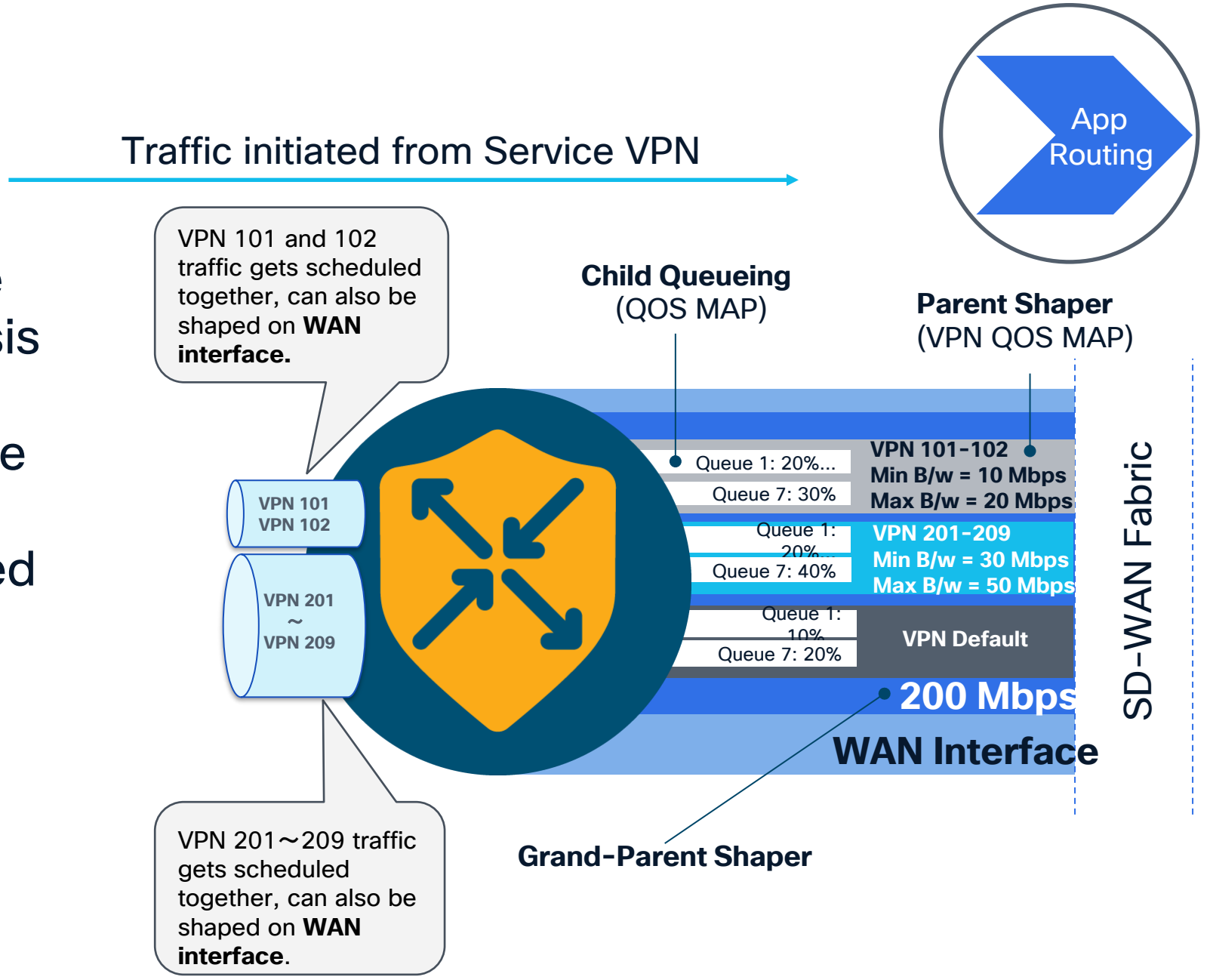
Spoke 3
100Mb Download
20Mb Upload

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

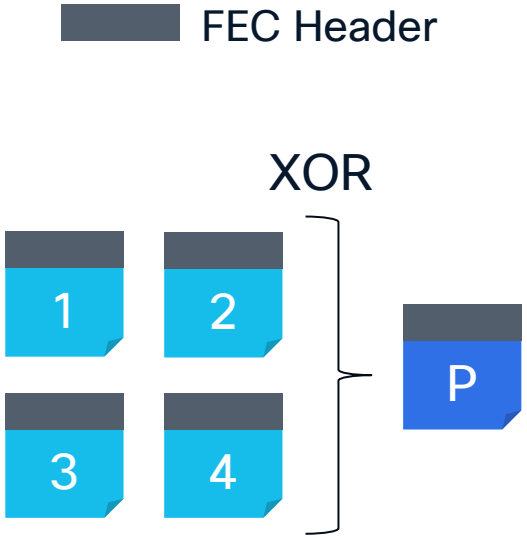
Per-VPN QOS

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



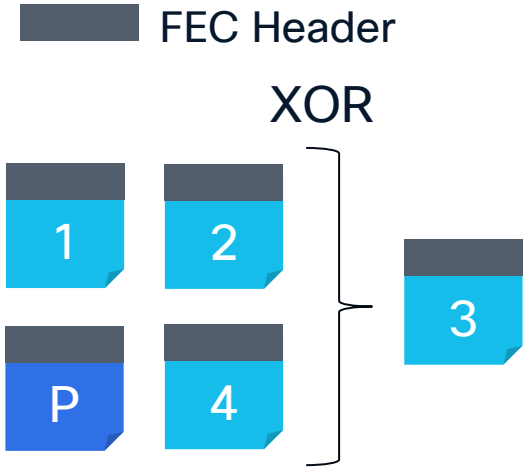
© 2025 Cisco and/or its affiliates. All rights reserved.

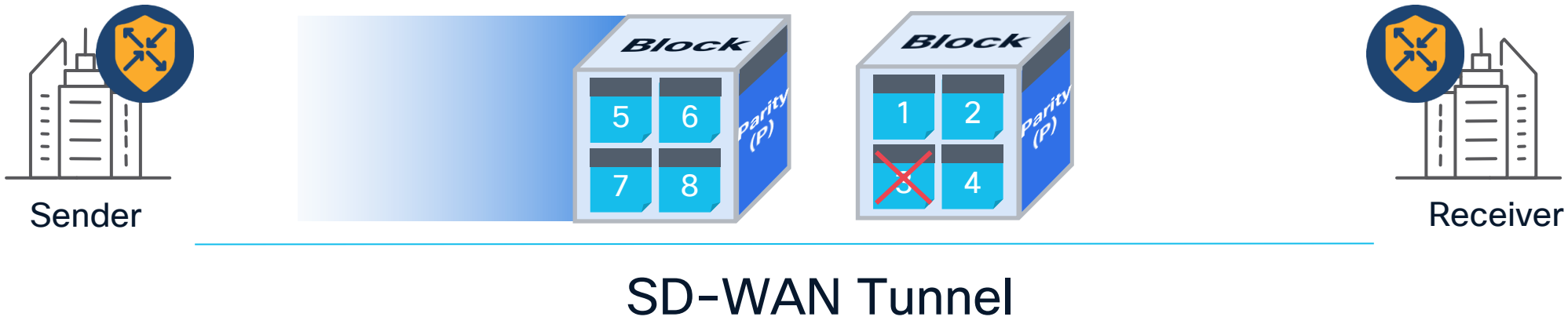
Forward Error Correction



Highlights:

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



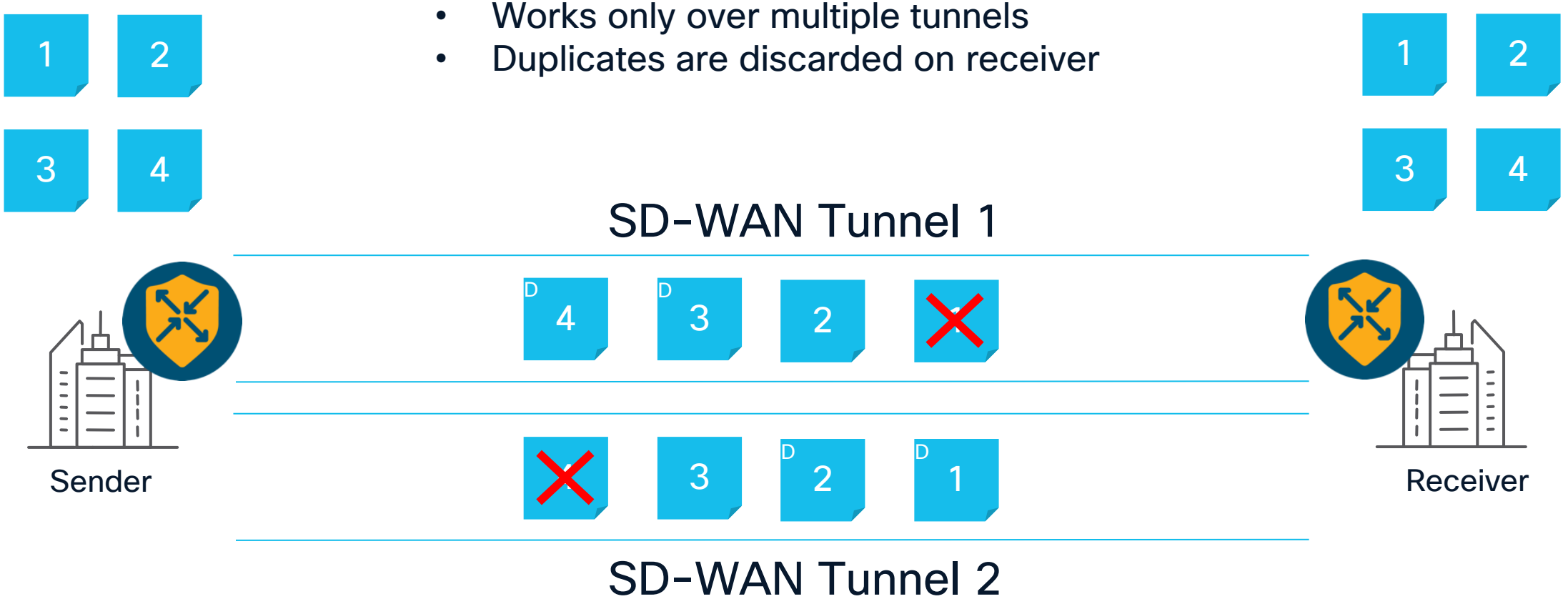


© 2025 Cisco and/or its affiliates. All rights reserved.

Packet Duplication

App Routing

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



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Native Unified Communications in SD-WAN

App Routing

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

SRST DSP Farming

Management/Control Plane

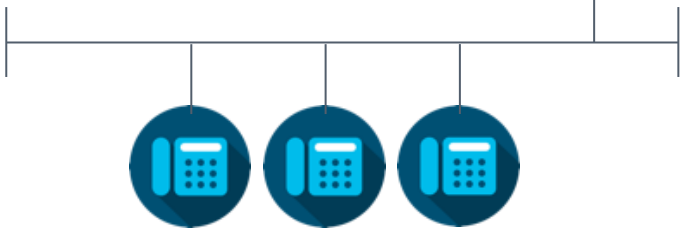
Data Plane

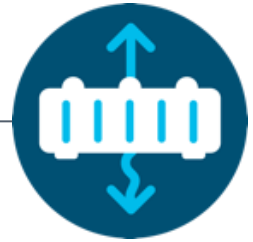
FXS, FXO, T1/PRI

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





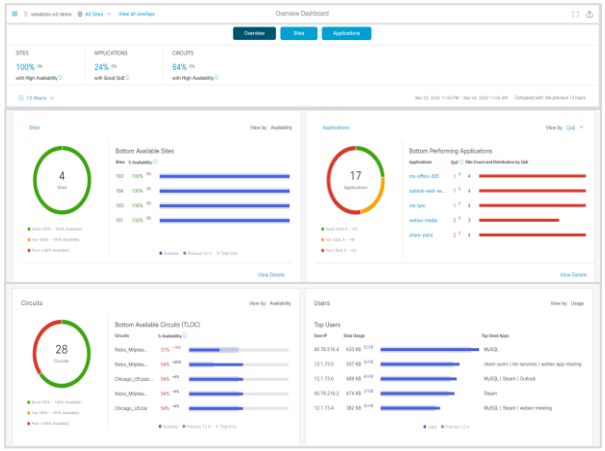
PSTN

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Underlay and Overlay visibility

Visibility into Network & App Performance



Application Experience

Scheduled Reports

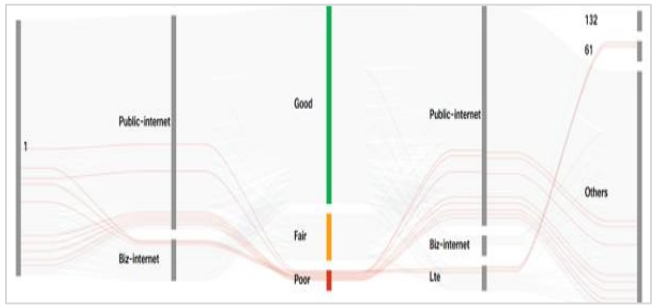
Historical Trends &

Daily/Weekly/Monthly

Aggregates

Troubleshooting w/ Extensive Traffic Analysis

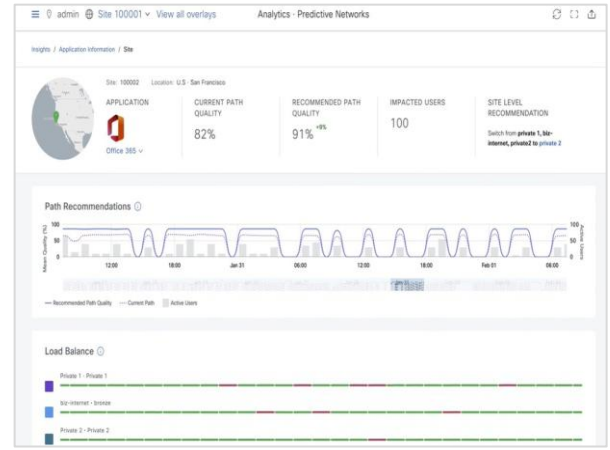
Traffic flow patterns



Underlay path tracing

App distribution across circuits

Adaptive & Predictive Networking



Predictive Path Recommendations

AIOps use-cases

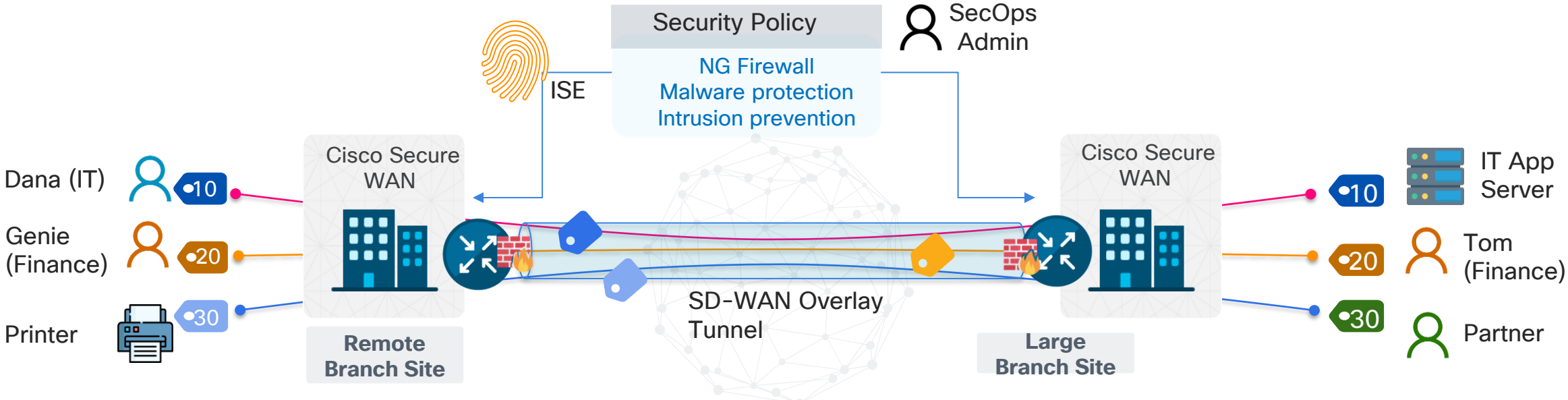
SaaS Traffic Optimization

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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

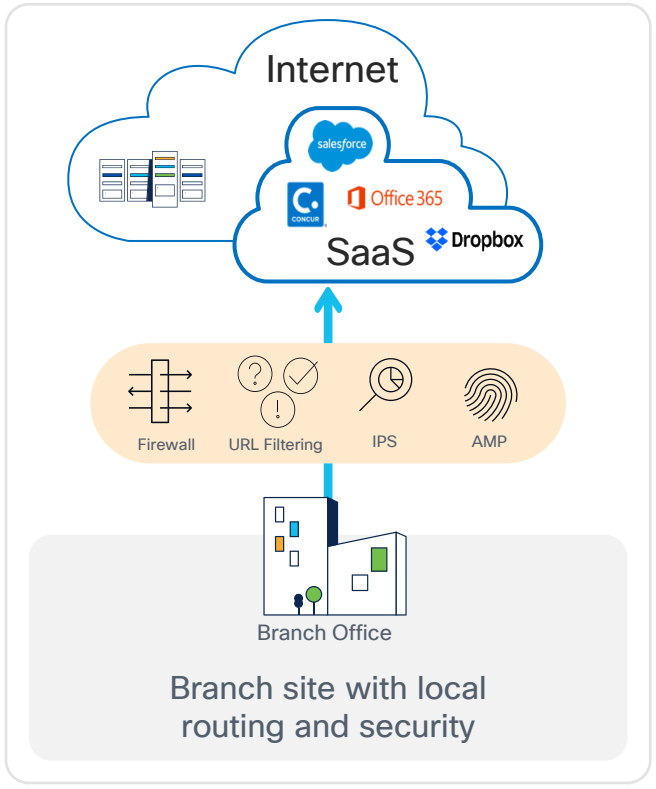


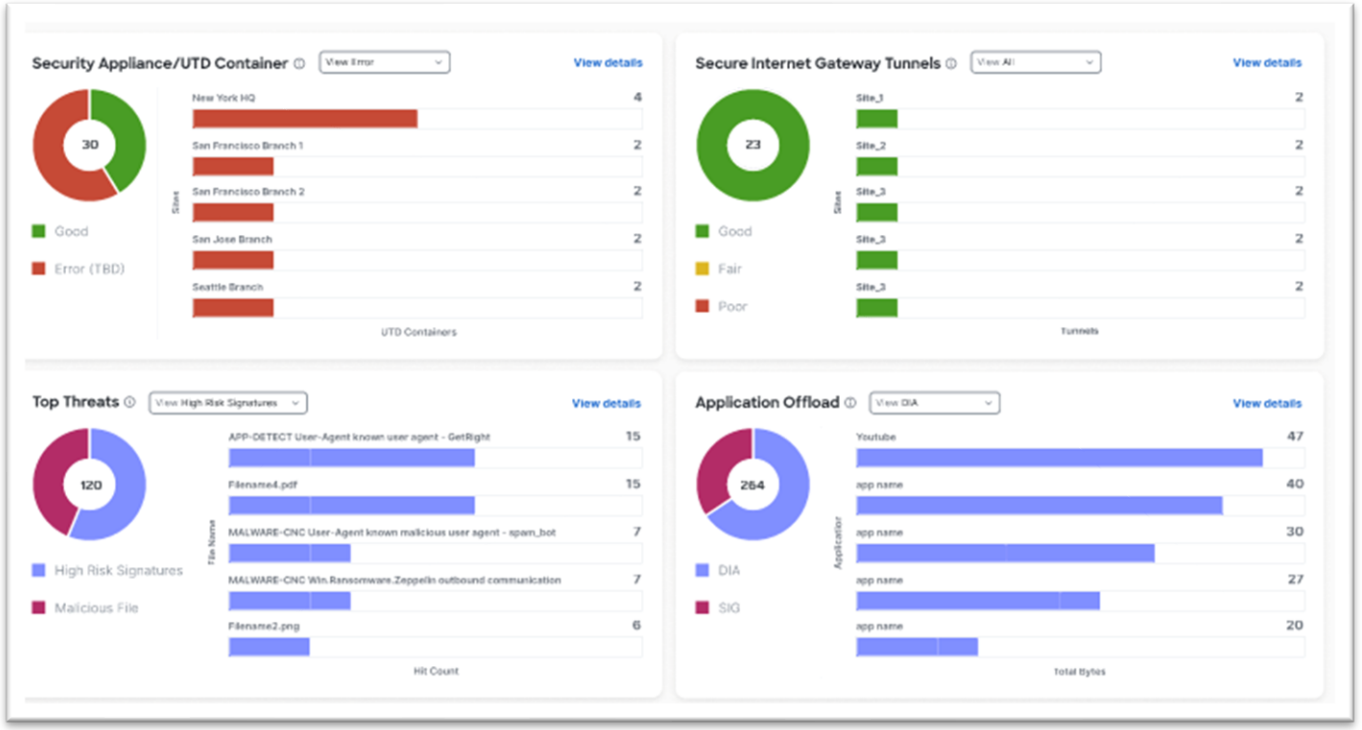
Security Policy	Source	Allow
	IT	IT (Port: 443), Printer
	Finance	Finance (Port: 443), Printer
	Partner	IT (Port: 443), Printer

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Advanced security





Next Gen Firewall

Guided Workflows

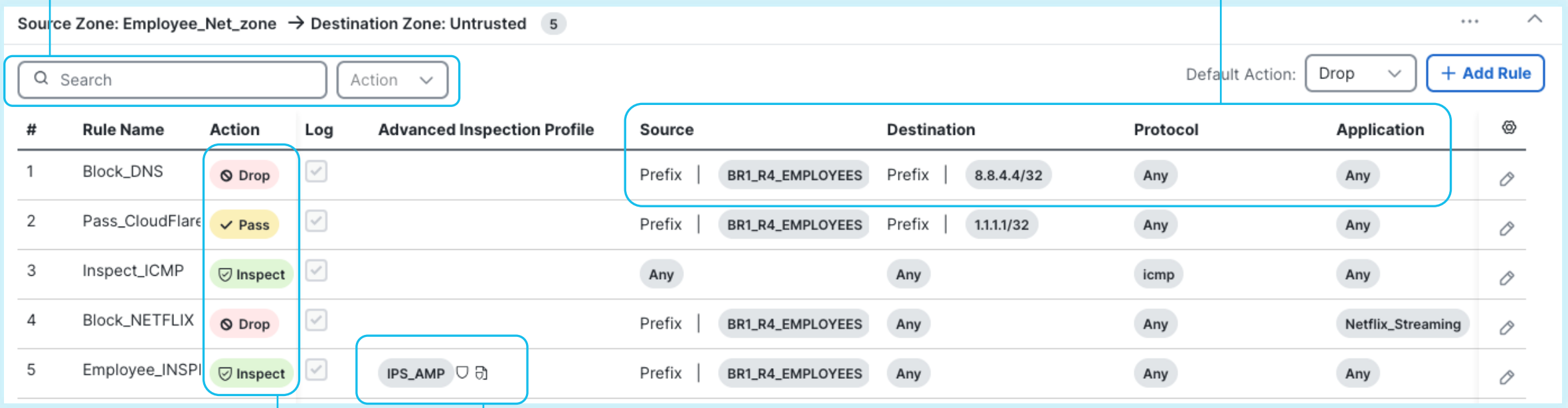
Unified Management

© 2025 Cisco and/or its affiliates. All rights reserved.

Enhanced Cisco Secure WAN NGFW Rule Table

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

Single line rule definitions



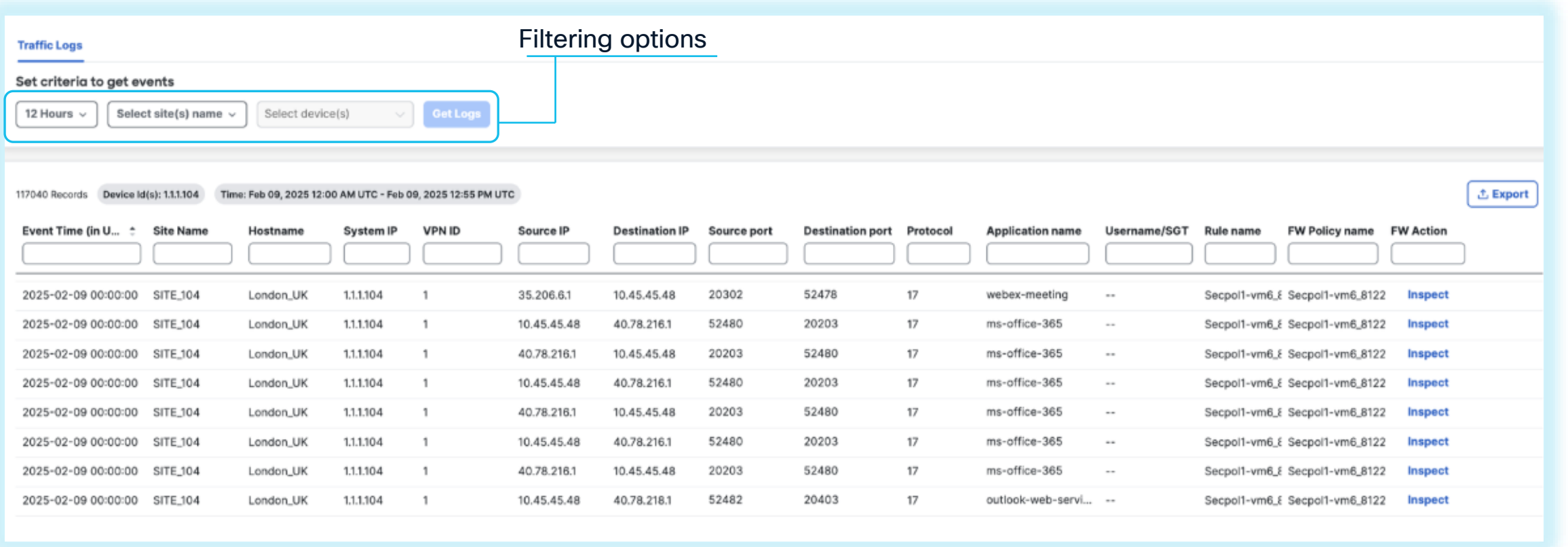
Color coded actions

Icons for security features

August 2025 Release (20.15.2) onwards

© 2025 Cisco and/or its affiliates. All rights reserved.

Detailed FW Log visualization on SD-WAN Manager



Granular Visibility

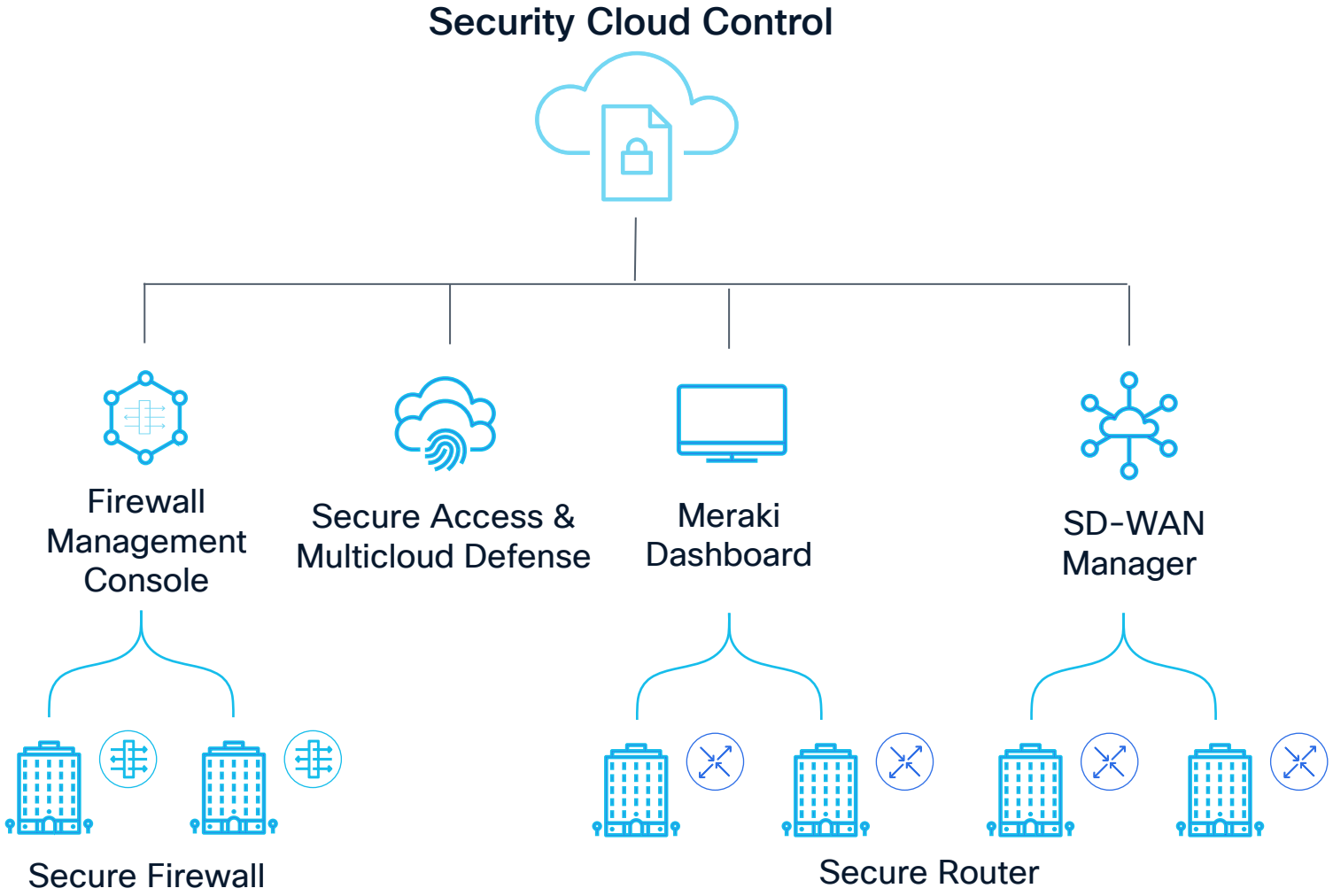
Customized Queries

Data Retention

August 2025 Release (17.18.1)

© 2025 Cisco and/or its affiliates. All rights reserved.

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)

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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)

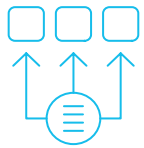
SD-WAN Analytics

Seamless Firmware Upgrades

Native Cisco SASE Integration

NBAR Deep Packet Inspection Engine

SD-WAN over cellular


IPSEC (3rd Party SSE)

Secure Remote Access

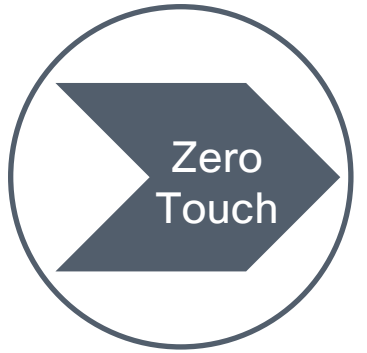
Direct Internet Access/ VPN Exclusion

Native ThousandEyes Integration

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Meraki Device-to-Cloud Connectivity

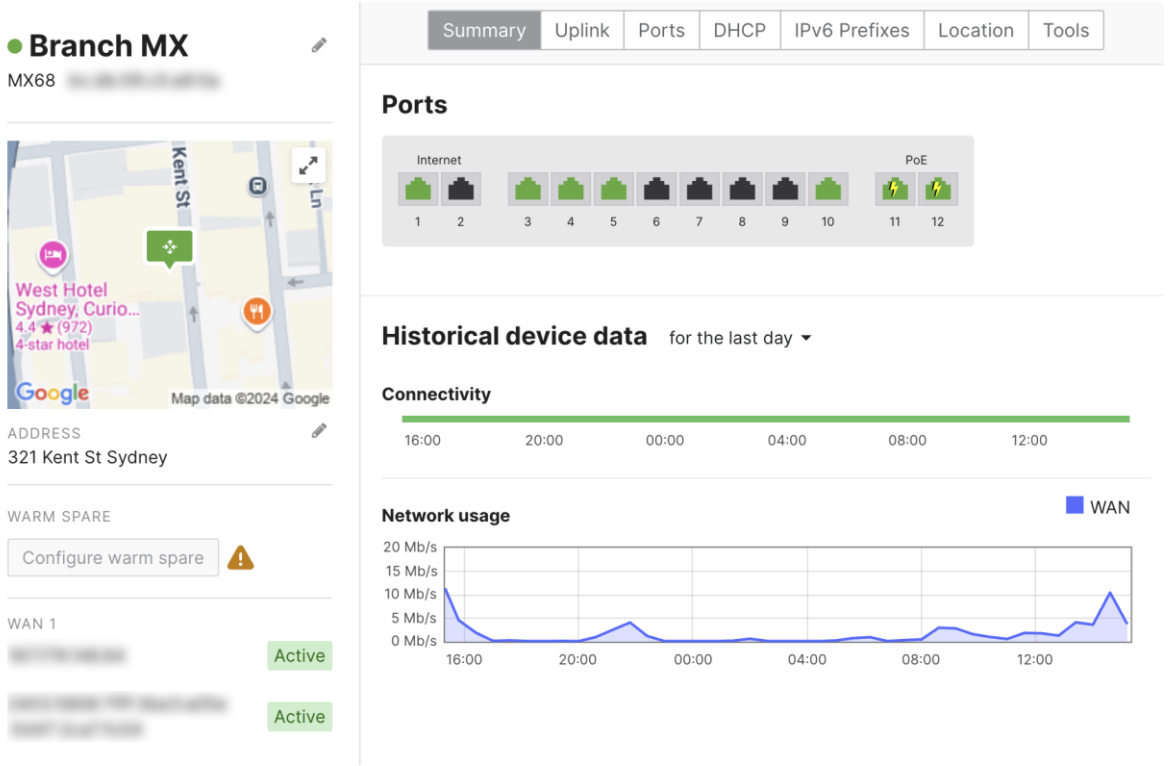


Device requests IP address

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

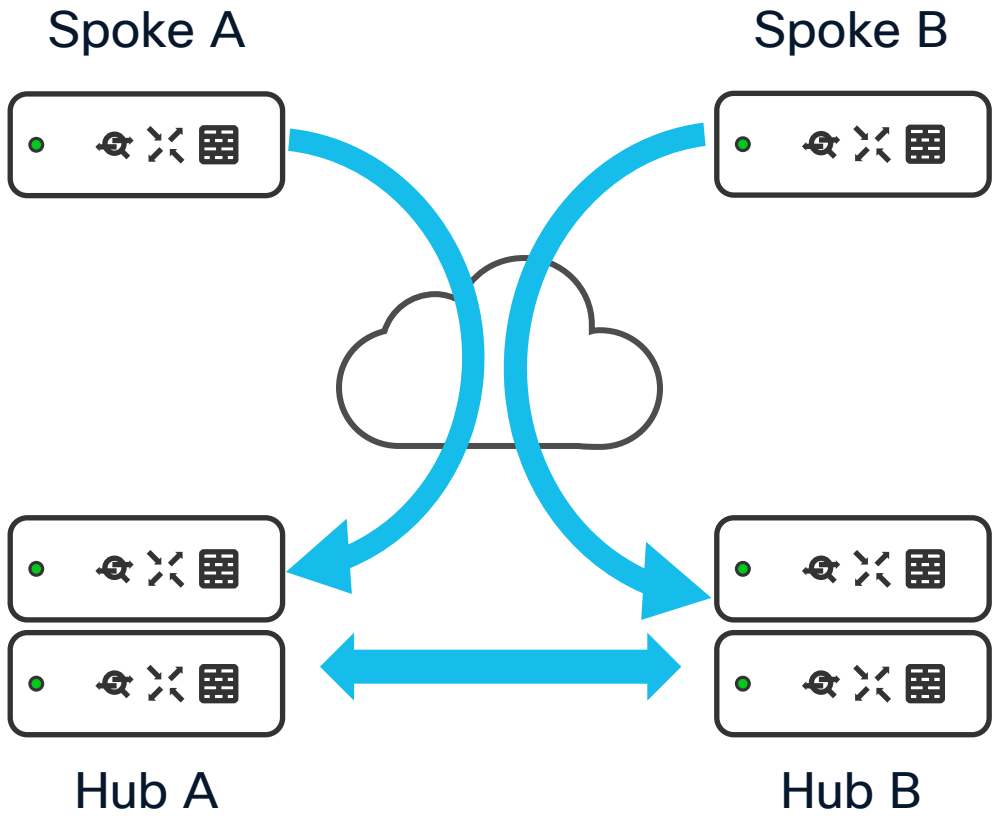
Check in complete



© 2025 Cisco and/or its affiliates. All rights reserved.

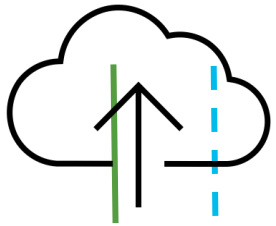
Auto VPN – Out of the box

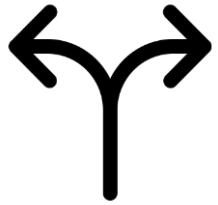
- Spokes build tunnels to hubs that they have configured
- Hubs build tunnels to all other hubs
- All MXs in an Auto VPN domain ‘learn’ about all other routes



© 2025 Cisco and/or its affiliates. All rights reserved.

IPSEC Tunnel Monitoring and Redundancy

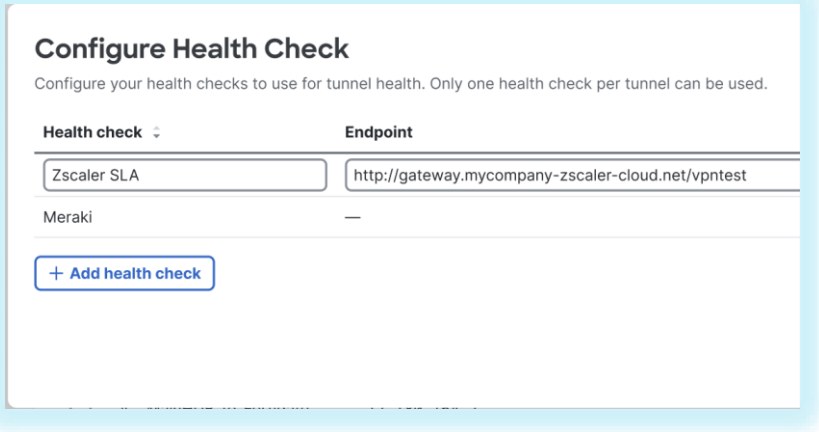


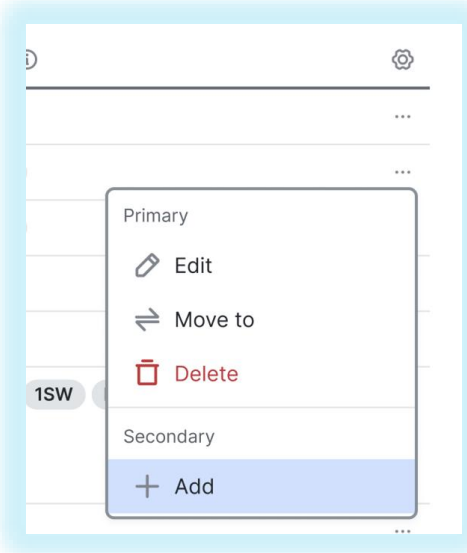


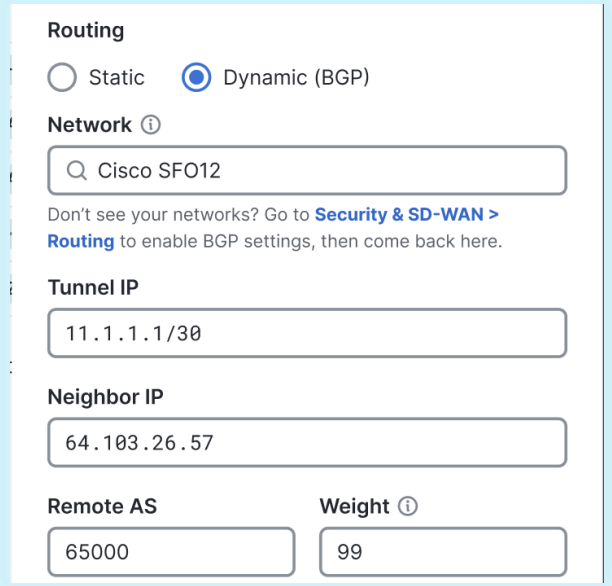
Tunnel monitoring

Active/Backup tunnels

BGP routing over IPsec

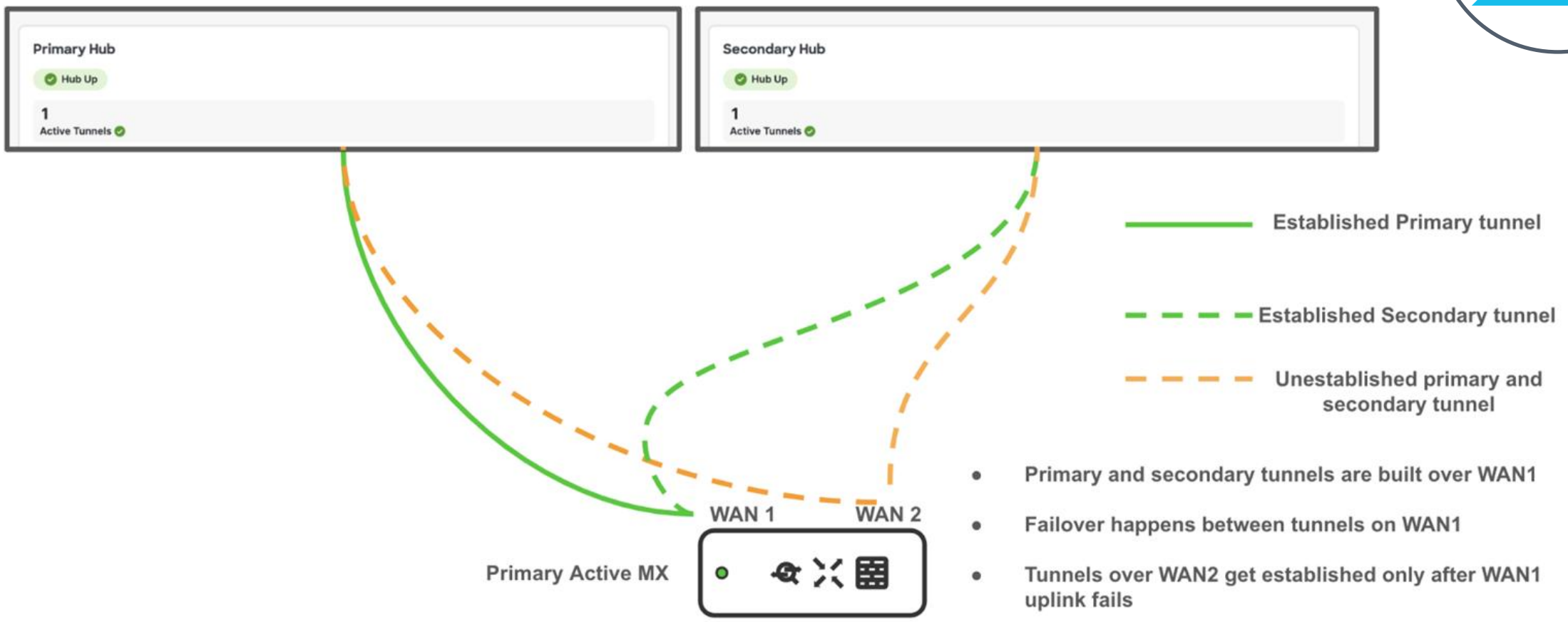






© 2025 Cisco and/or its affiliates. All rights reserved.

IPSEC Tunnel Monitoring and Redundancy



Available with MX 19.1 Firmware Release

© 2025 Cisco and/or its affiliates. All rights reserved.

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

Per peer VPN logs

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

Accurate tunnel status reporting

Available with MX 19.1 Firmware Release

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

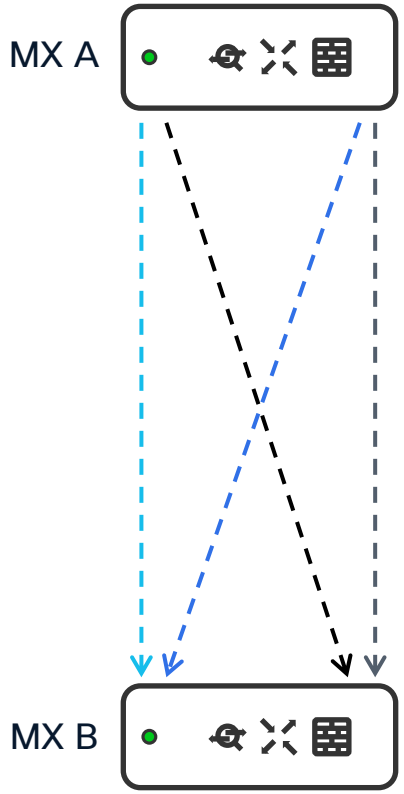
Probing

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



© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Performance Classes

Uplink Selection

Preferred Uplink: WAN 1

Fail over if: Poor performance

Performance class: VoIP

VoIP ✓

Traffic filters

All VoIP & video conferencing ✖ Add +

Policy

Preferred uplink: Best for 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

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

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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

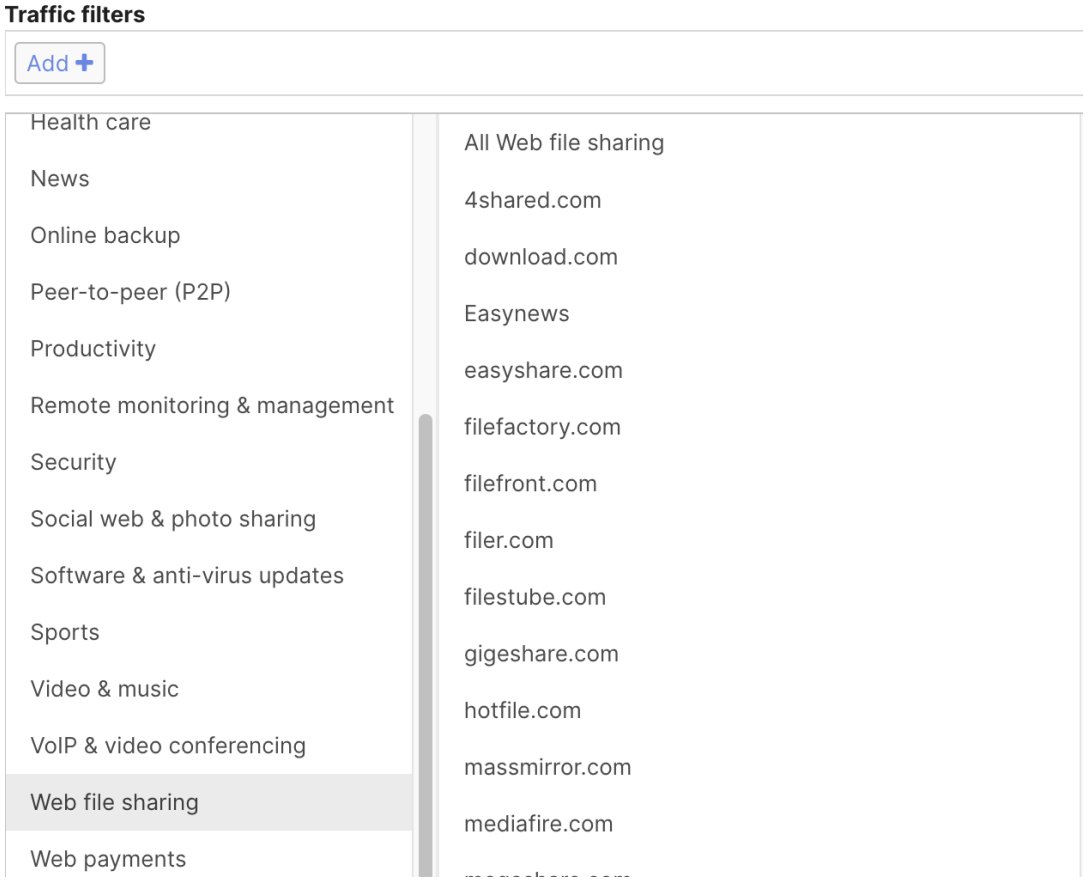
Create a new custom performance class...

© 2025 Cisco and/or its affiliates. All rights reserved.

Application

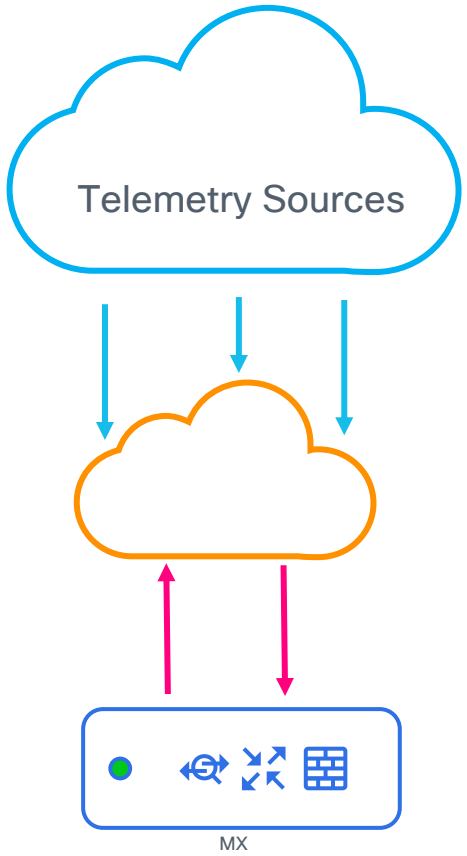
Policy applied either via custom expressions (CIDR / Hostname) or Traffic Analysis engine NBAR2

NBAR2 supports 1500 applications



© 2025 Cisco and/or its affiliates. All rights reserved.

SD-AVC Integration for NBAR



IP Feeds

Domain Feeds

Cloud Feeds

Dynamic Feeds

Custom Regex Feeds

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
- Zscalar
- CASI Umbrella Top 1 Million
- AWS
- Azure
- GCP
- SSL Crawler
- WHOIS
- rDNS
- Internet registry DB

© 2025 Cisco and/or its affiliates. All rights reserved.

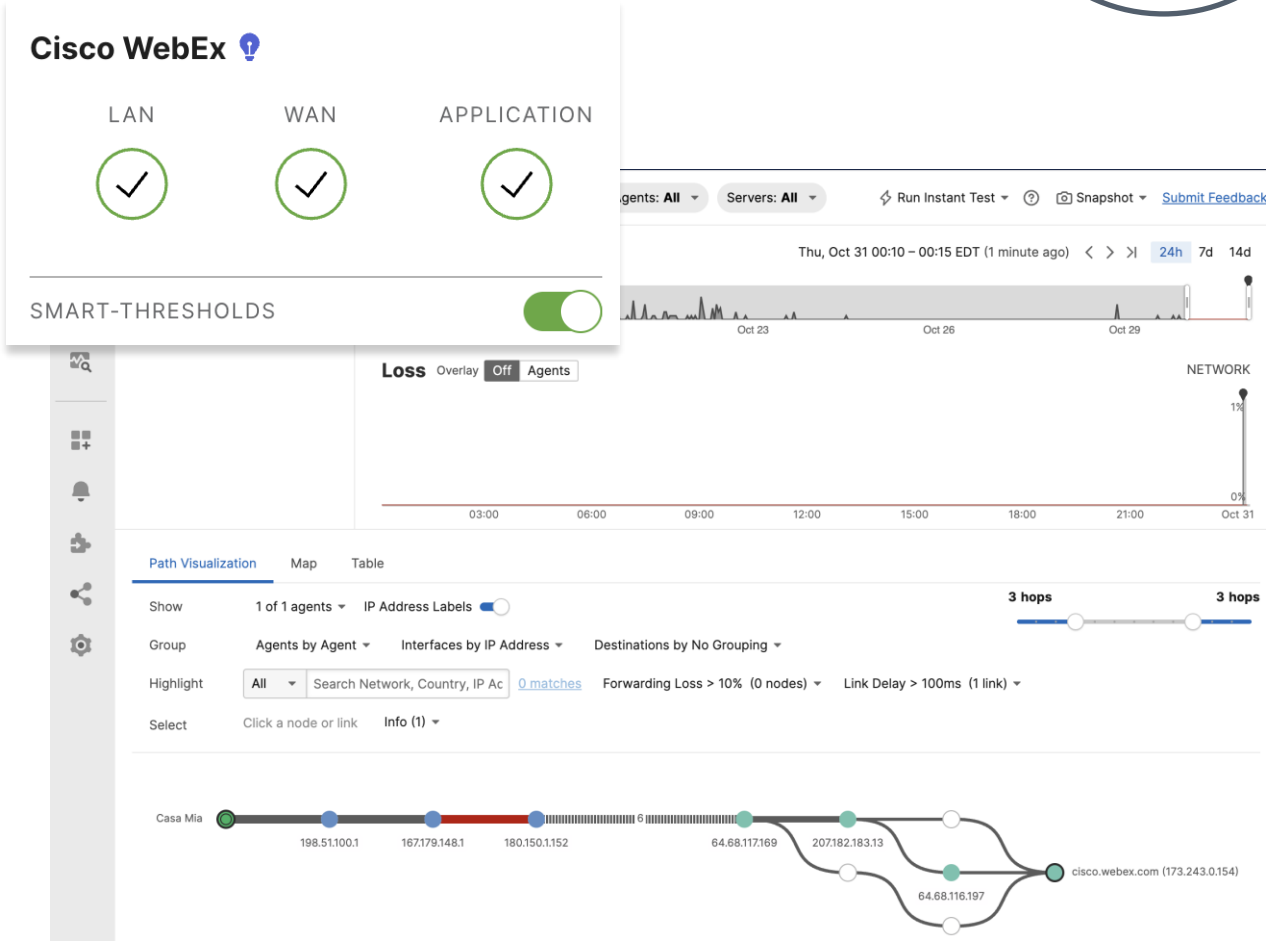
cisco

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.



© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Meraki Security Dashboard & Event Details

Cisco Meraki

NETWORK

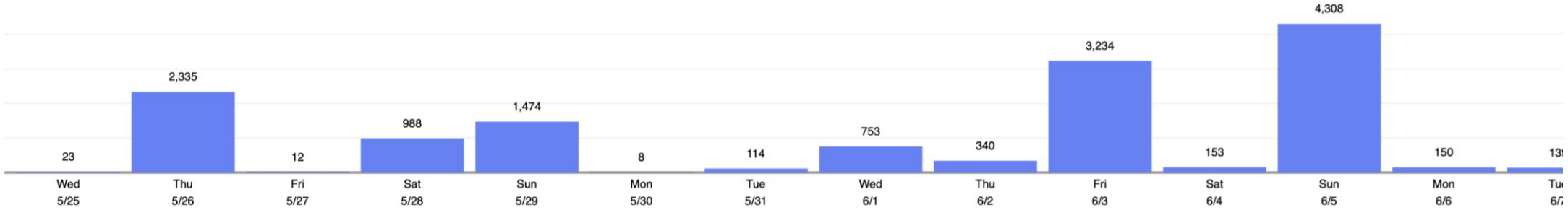
Meraki 460 Townsend - SFO22

- 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

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

Top sources of threats

MX Summary | MX Events

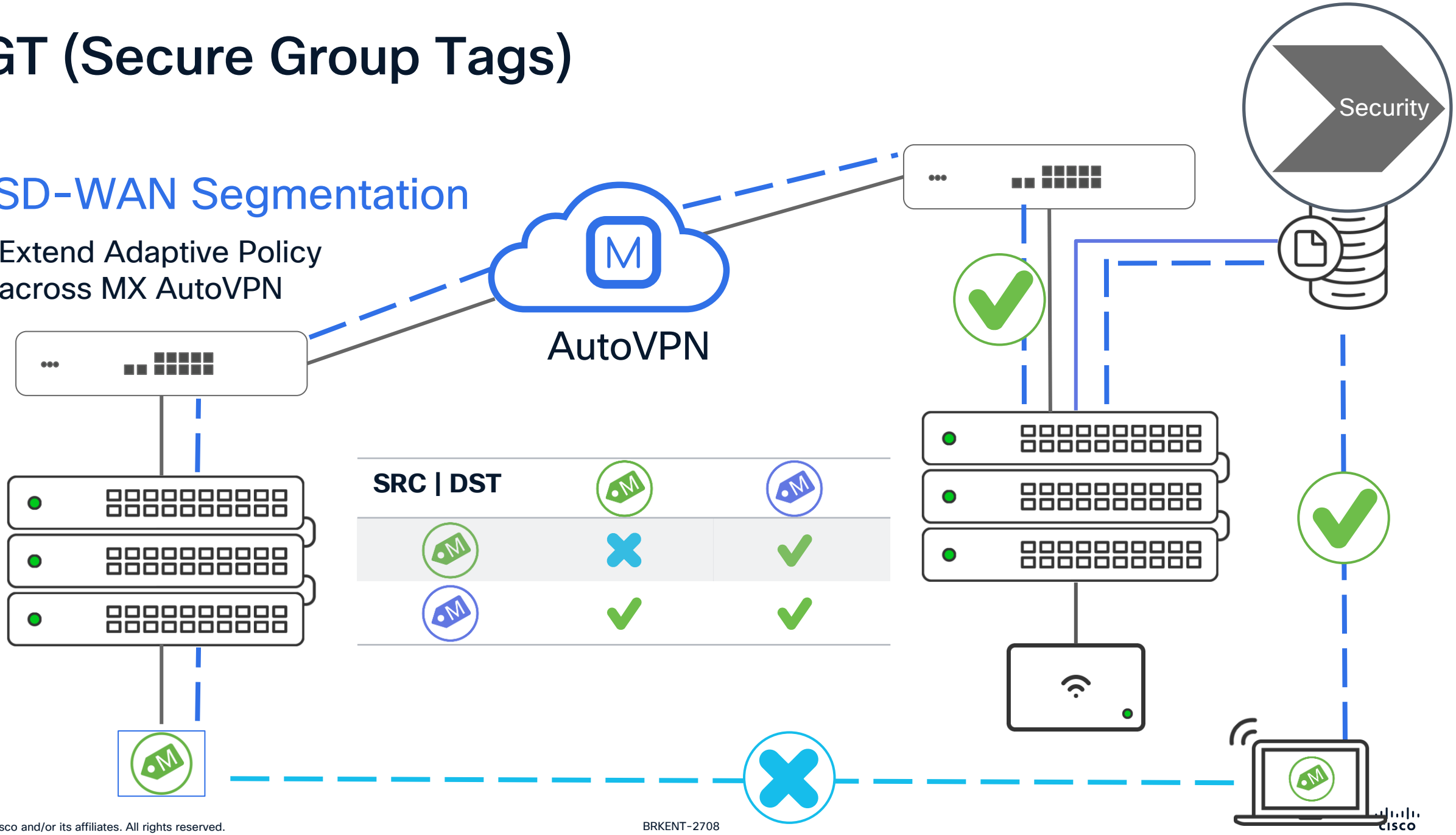
Time	Type	Source	Network	Destination	Disposition	Action	Details
Jun 8 17:00:37	IDS Alert	s3-website.ca-central-1.amazonaws.com 52.95.147.1:80	Z - San Francisco - Lab and Guest	pa-int-wan-1-mx-98188810a5f7 Meraki Network OS		Allowed	POLICY-OTHER cryptomining javascript client detected

© 2025 Cisco and/or its affiliates. All rights reserved.

SGT (Secure Group Tags)

SD-WAN Segmentation

- Extend Adaptive Policy across MX AutoVPN



© 2025 Cisco and/or its affiliates. All rights reserved.

Meraki MX Threat & Security Policies

Meraki

ORGANIZATION

Meraki - GSSO Demo

NETWORK

Meraki Demo HQ

- Network-wide
- Security & SD-WAN
- Switch
- Insight

Threat protection

Advanced Malware Protection (AMP)

Mode: Enabled

Allow list URLs: There are no URLs on the Allow list.
Add a URL to the Allow list

Allow list files: There are no files on the Allow list.
Add a file to the Allow list

Threat Grid

Mode: Enabled

Rate limit: Disabled

Intrusion detection and prevention

Mode: Prevention

Ruleset: Connectivity

Allow list rules: There are no IDS rules on the Allow list.
Add an IDS rule to Allow list

Umbrella protection

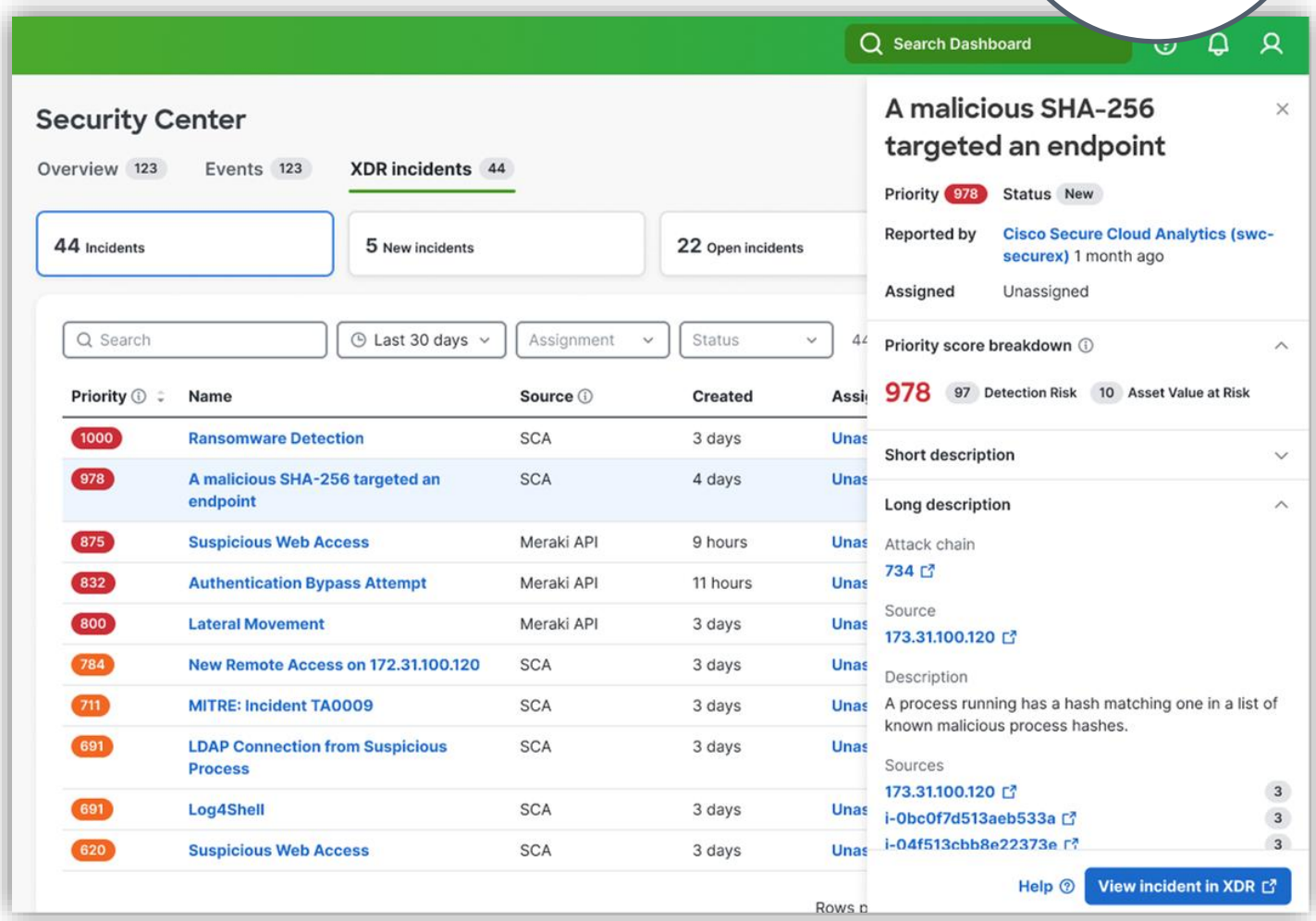
DNS layer protection (Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

© 2025 Cisco and/or its affiliates. All rights reserved.

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



© 2025 Cisco and/or its affiliates. All rights reserved.

Meraki SD-WAN Secure Edge Solution

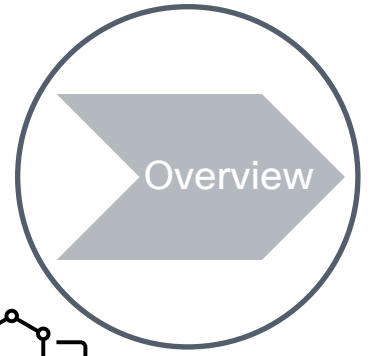
- ✓Rapid deployment at scale & simplicity across all policies
- ✓Unified management platform for all branch functions
- ✓NGFW & Snort-based security features on-box

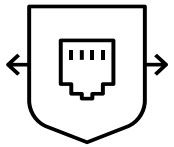
© 2025 Cisco and/or its affiliates. All rights reserved.

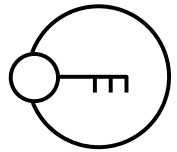
Firewall Threat Defense Use Cases & Capabilities

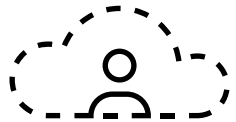
cisco Live !

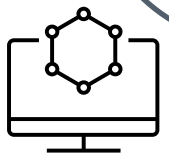
Branch Deployments with Secure Firewall











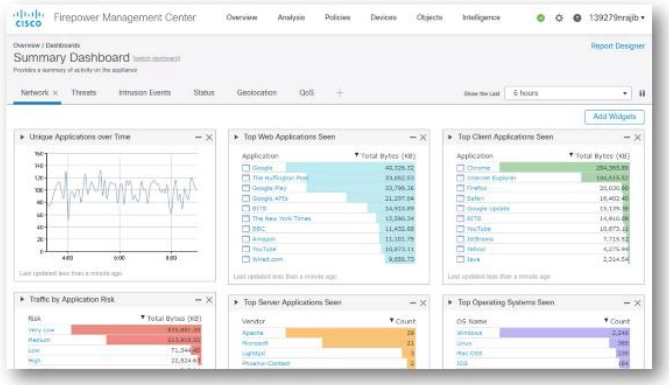
Secure Elastic Connectivity	WAN Optimization	Increased Usable Bandwidth	Direct Internet Access for Public cloud	Simplified Management
VT–based Hub & Spoke VPN	Dual ISP configuration	Increased support for load-balancing across multiple ISPs	SaaS Application detection (Fist Packet using AVC)	Data Interface Management
BGP, EIGRP, OSPF over VTI	Active-Standby Backup VTI tunnel configuration with SLA monitoring	ECMP Support for VTI	DNS Snooping using trusted DNS Servers	SASE: Umbrella Auto-Tunnel deployment
DVTI support DHCP	Optimal Path Selection based on interface Monitoring	Application based load balancing using Policy Based Routing (PBR)	PBR using Application as matching criteria	DVTI Hub and Spoke topology simplification

© 2025 Cisco and/or its affiliates. All rights reserved.

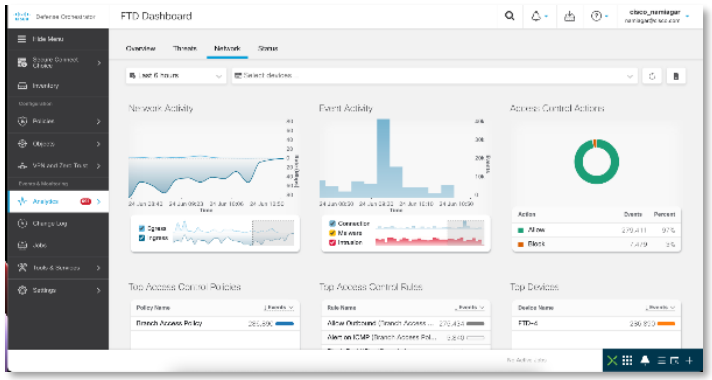
cisco

Managing Secure Firewall

Firewall Management Center

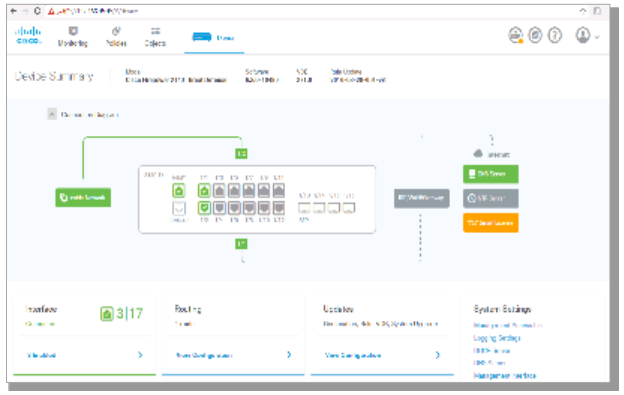


On-premises manager



Cloud-delivered via Security Cloud Control

Firewall Device Manager

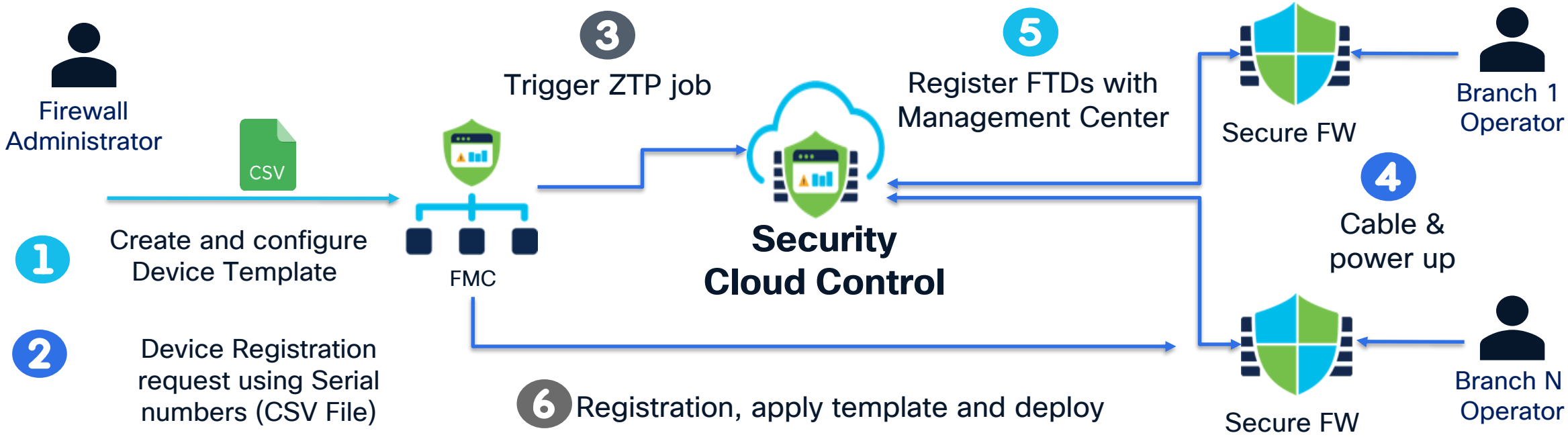


On-box manager

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Zero Touch Provisioning



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

© 2025 Cisco and/or its affiliates. All rights reserved.

IPsec Virtual Tunnel Interface

- Provides a virtual routable 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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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 addres[redacted]3.18.9.20
          Destination IP addres[redacted]3.18.7.10
          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

© 2025 Cisco and/or its affiliates. All rights reserved.

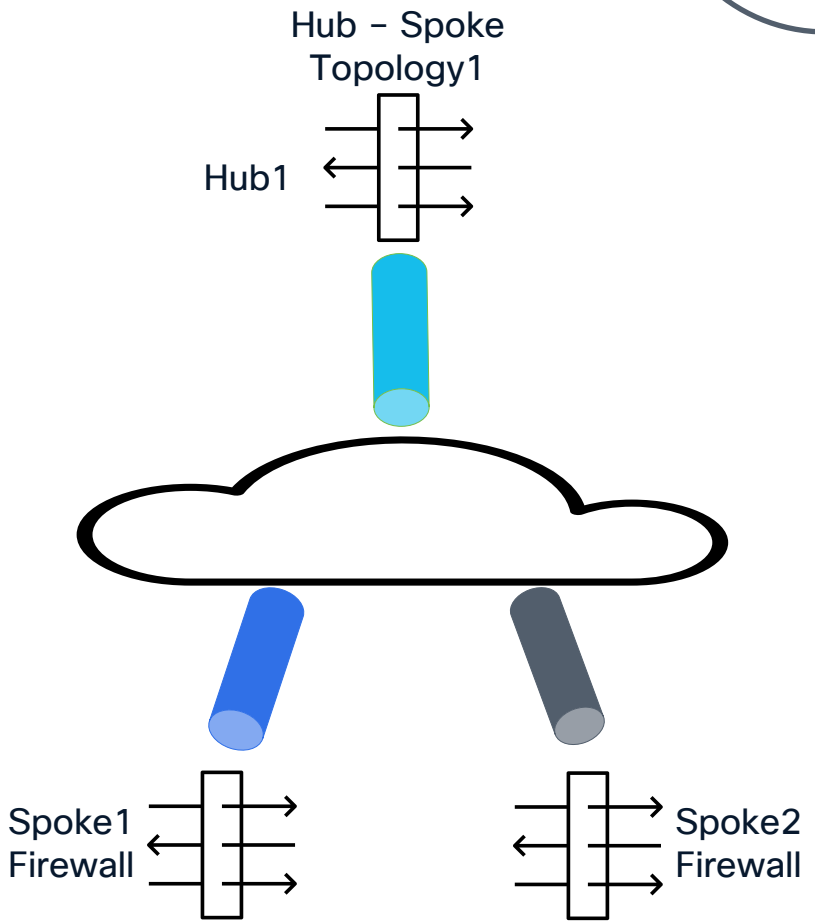
Branch to Hub Communication

Why Dynamic Virtual Tunnel Interface (DVTI) ?

High-scale, route-based VPN deployments

No additional Hub configuration while adding new spokes

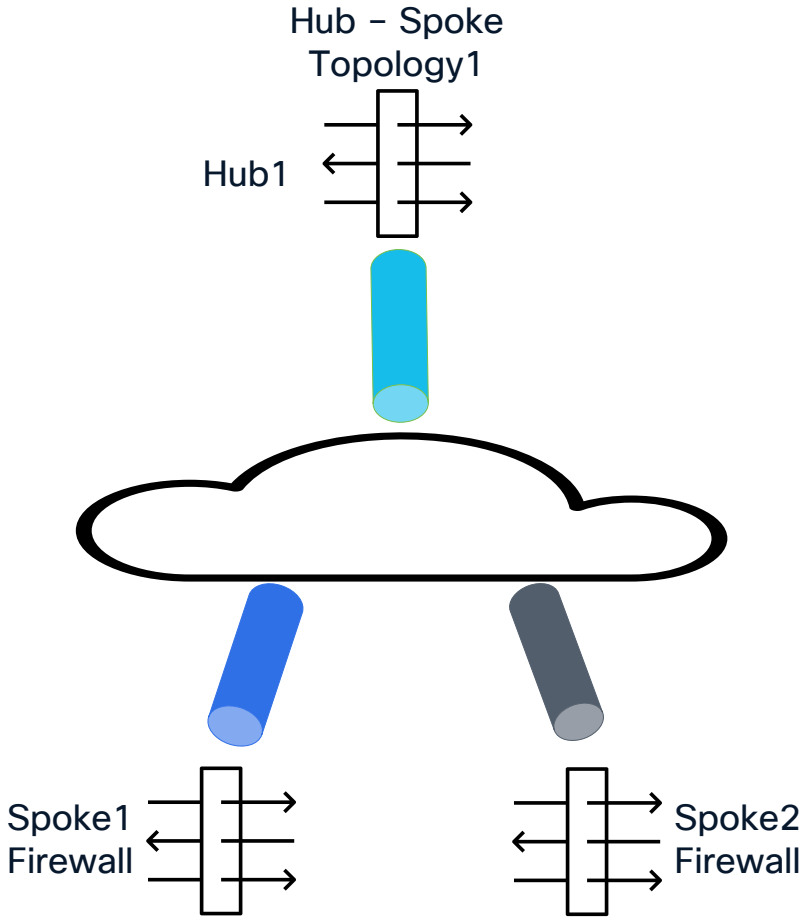
No configuration change on Hub when the spoke's DHCP IP address changes



© 2025 Cisco and/or its affiliates. All rights reserved.

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:

Point to Point | Hub and Spoke | Full Mesh

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

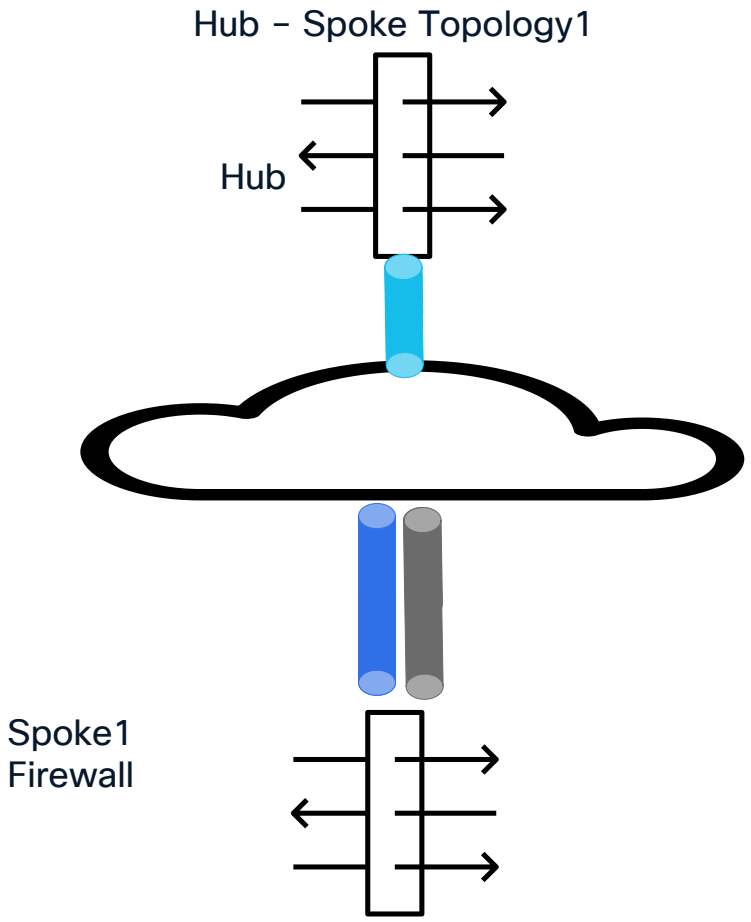
Spoke Nodes:

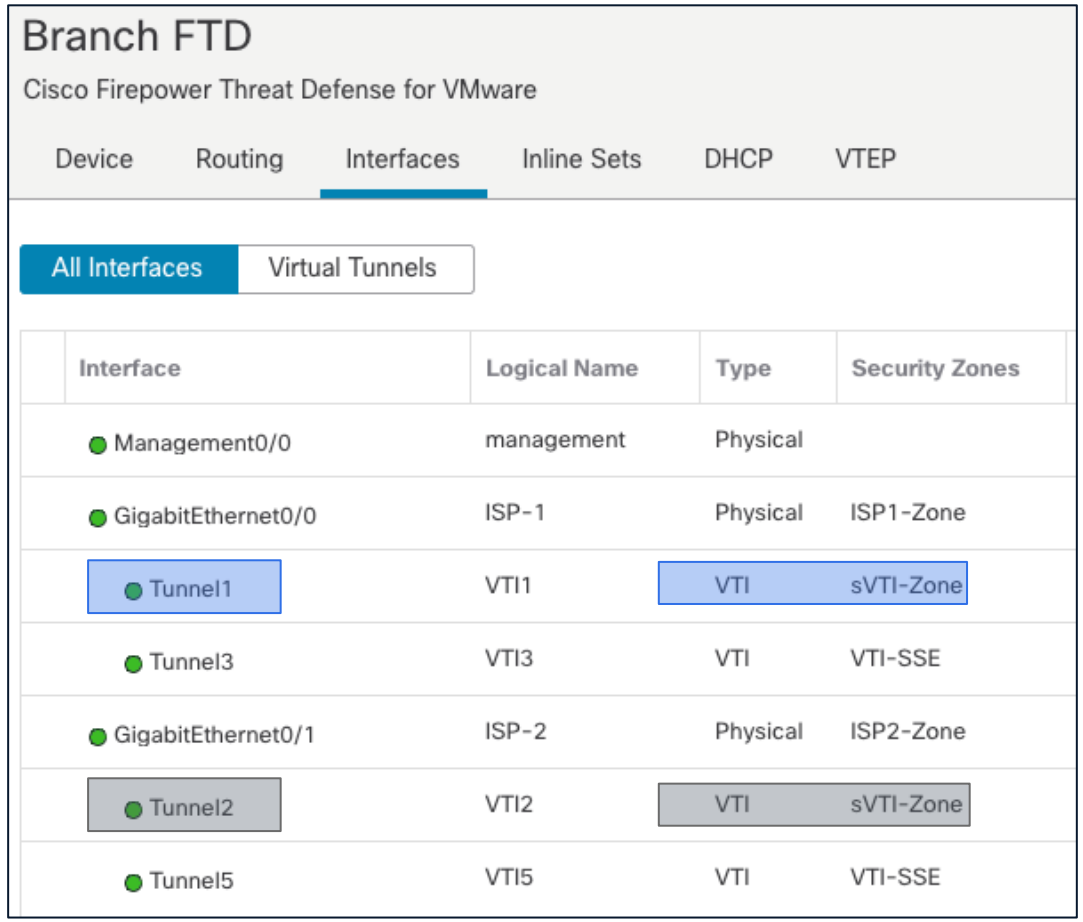
Device Name	VPN Interface	Traffic Match Criteria
FTD Branch FTD	VTI1 (169.254.255.2)	Routing Policy

© 2025 Cisco and/or its affiliates. All rights reserved.

Single Hub Topology

Spoke with Dual WAN

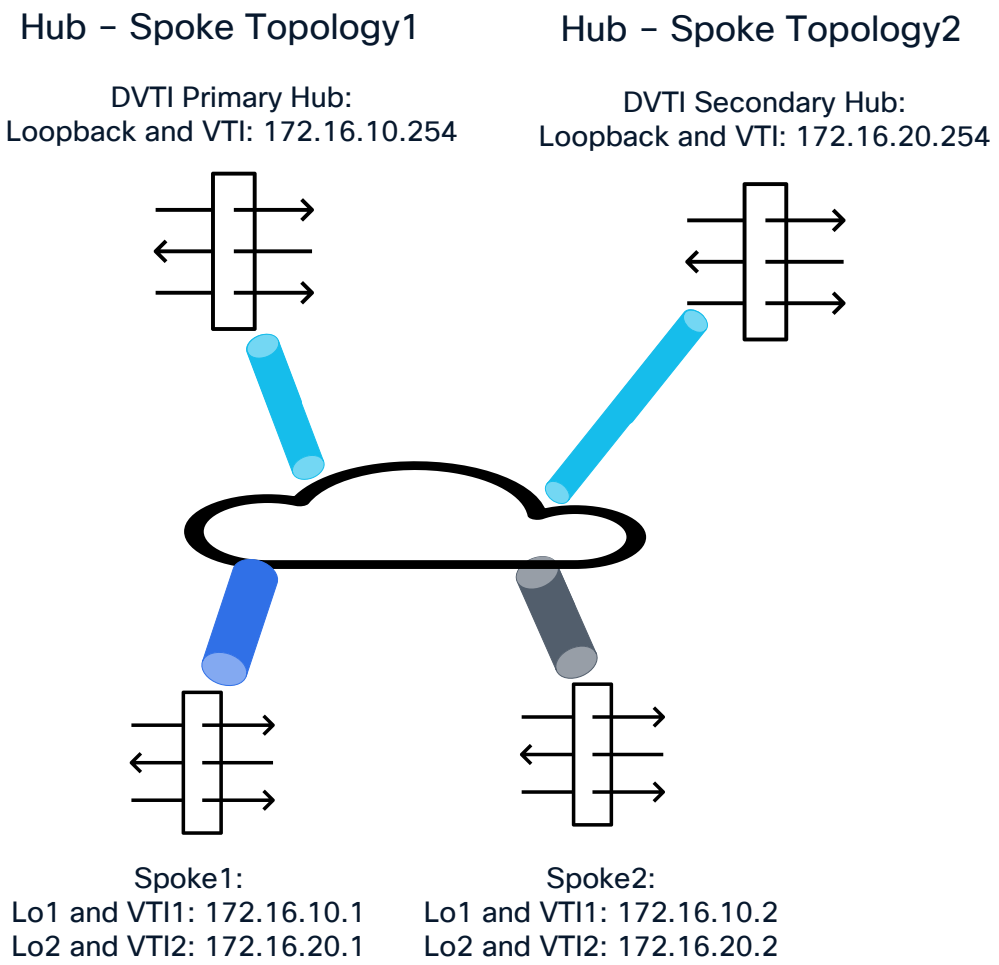




© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Dual Hub Topology

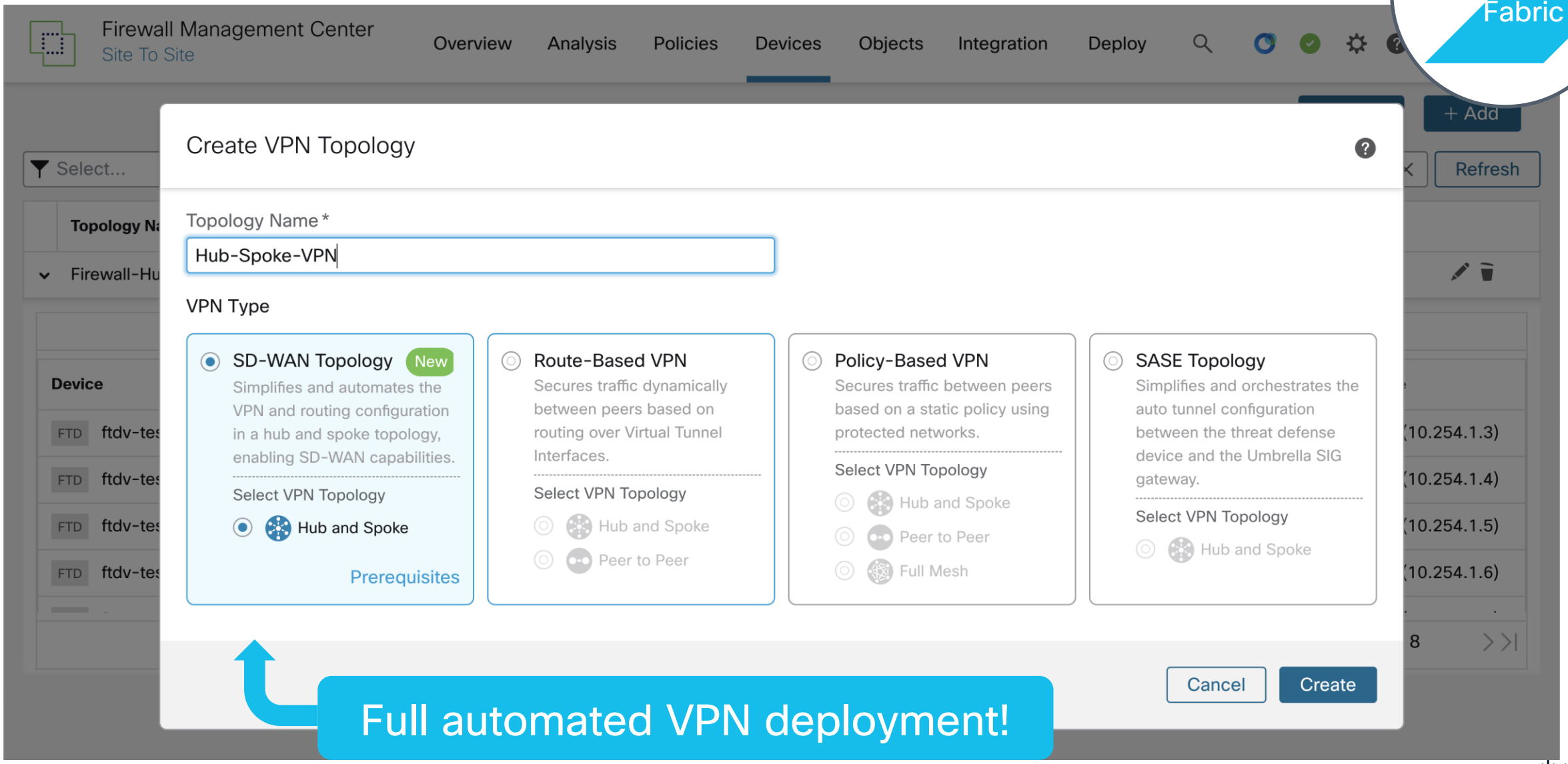


WAN Fabric

- 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)

© 2025 Cisco and/or its affiliates. All rights reserved.

Secure Firewall 7.6 Topology Wizard



© 2025 Cisco and/or its affiliates. All rights reserved.

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!

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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** Edit

Device	DVTI	Gateway IP Address	Spoke Tunnel IP Address Pool
ftdv-test-11	outside_dynamic_vti_1	64.100.14.211	DVTI-IP-Pool
ftdv-test-12	outside_dynamic_vti_1	64.100.14.212	DVTI-IP-Pool-2

2 **Spokes** Edit

Device	VPN Interface	Local Tunnel (IKE) Identity
ftdv-test-13	outside	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

3 **Authentication Settings** Edit

Authentication Pre-shared Automatic Key Pre-shared Key Length 24

4 **SD-WAN Settings** Edit

BGP enabled true Autonomous System Number 65100

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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

VTI

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

- [x] Enable BGP on the VPN overlay topology

Autonomous System Number*

65100

Community tag for local routes*

2112

- [x] Redistribute Connected Interfaces

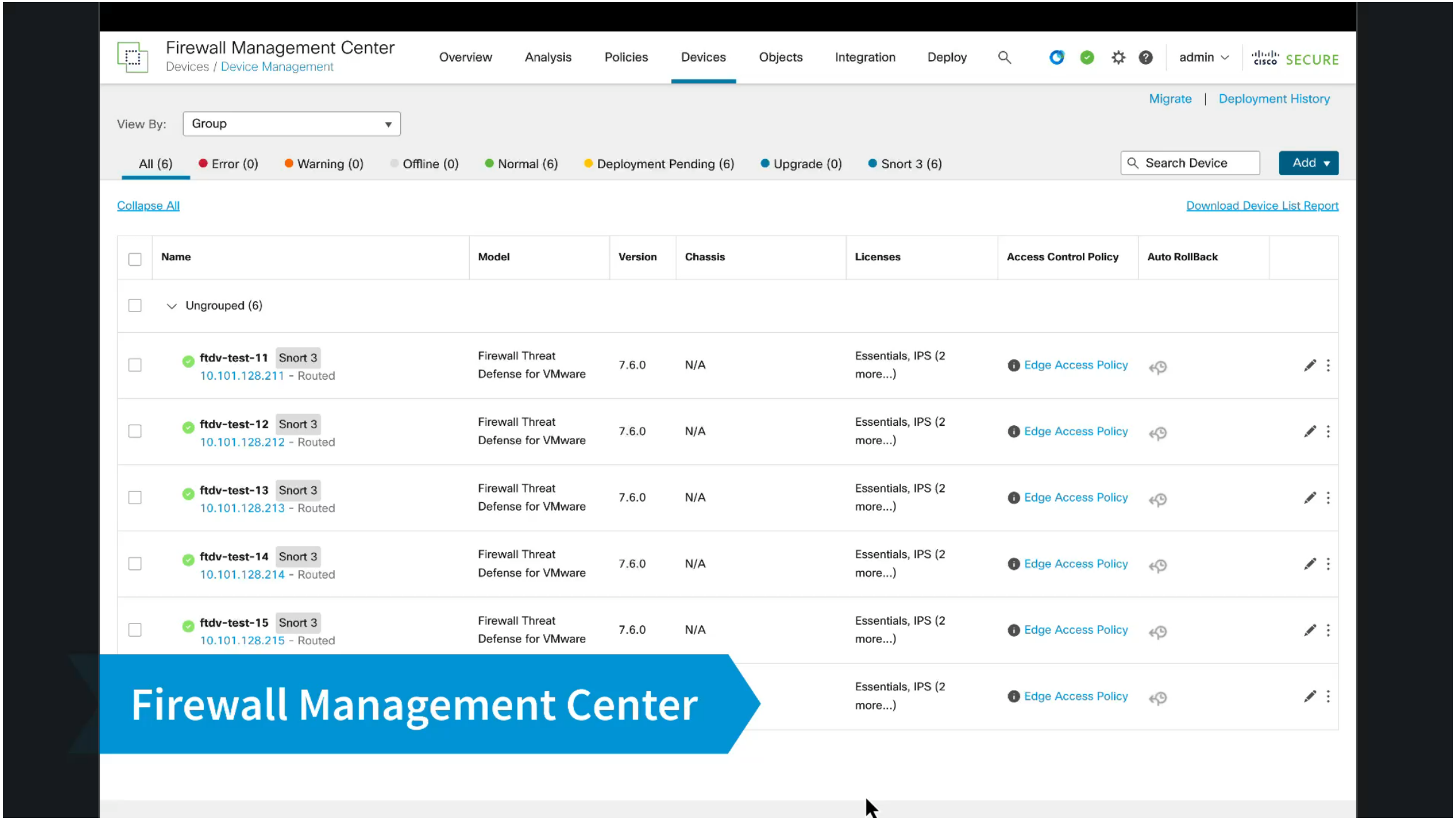
inside-interfaces

- [ ] Secondary Hub is in different Autonomous System
- [x] Enable Multiple Paths for BGP

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

© 2025 Cisco and/or its affiliates. All rights reserved.

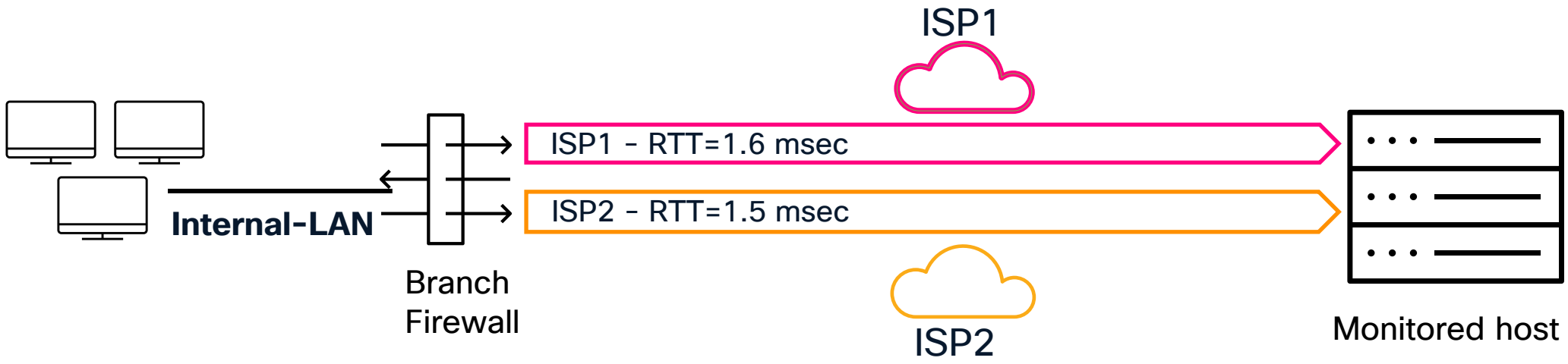
cisco



© 2025 Cisco and/or its affiliates. All rights reserved.

Policy Based Routing

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

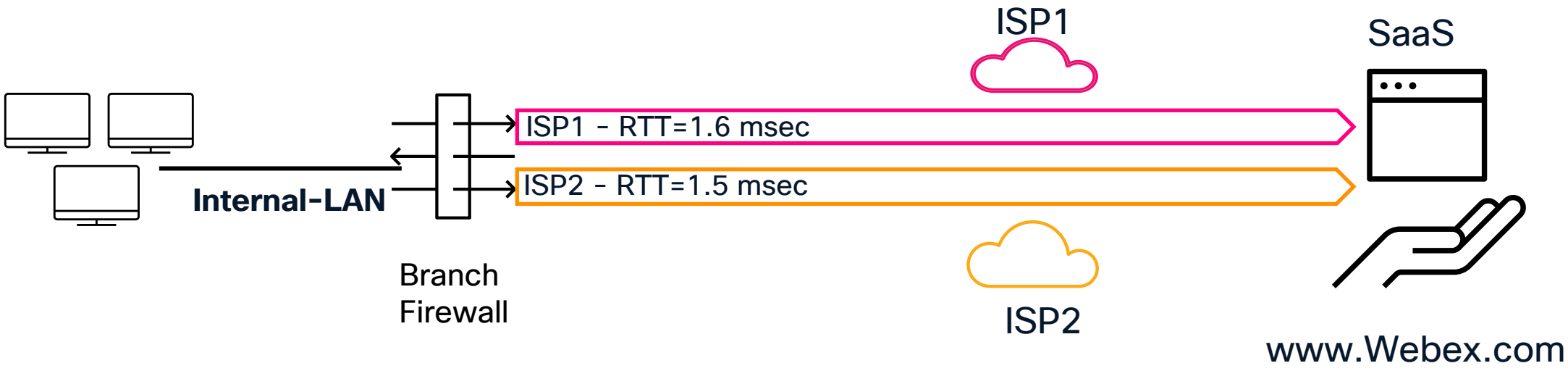


These metrics are collected dynamically using ICMP/HTTP Probe messages

© 2025 Cisco and/or its affiliates. All rights reserved.

HTTP Path Monitoring

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

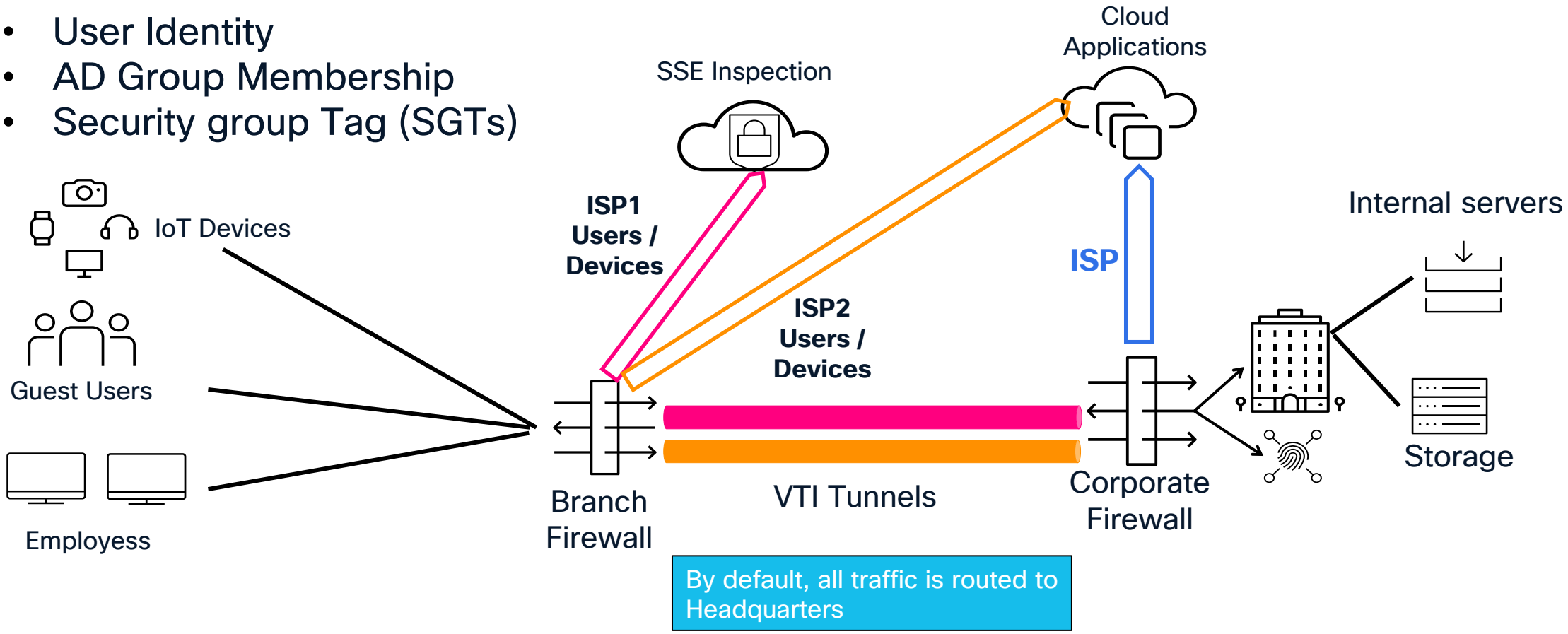


© 2025 Cisco and/or its affiliates. All rights reserved.

PBR with User Identity and SGT

Additional attributes can be leveraged in the PBR policy:

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



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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

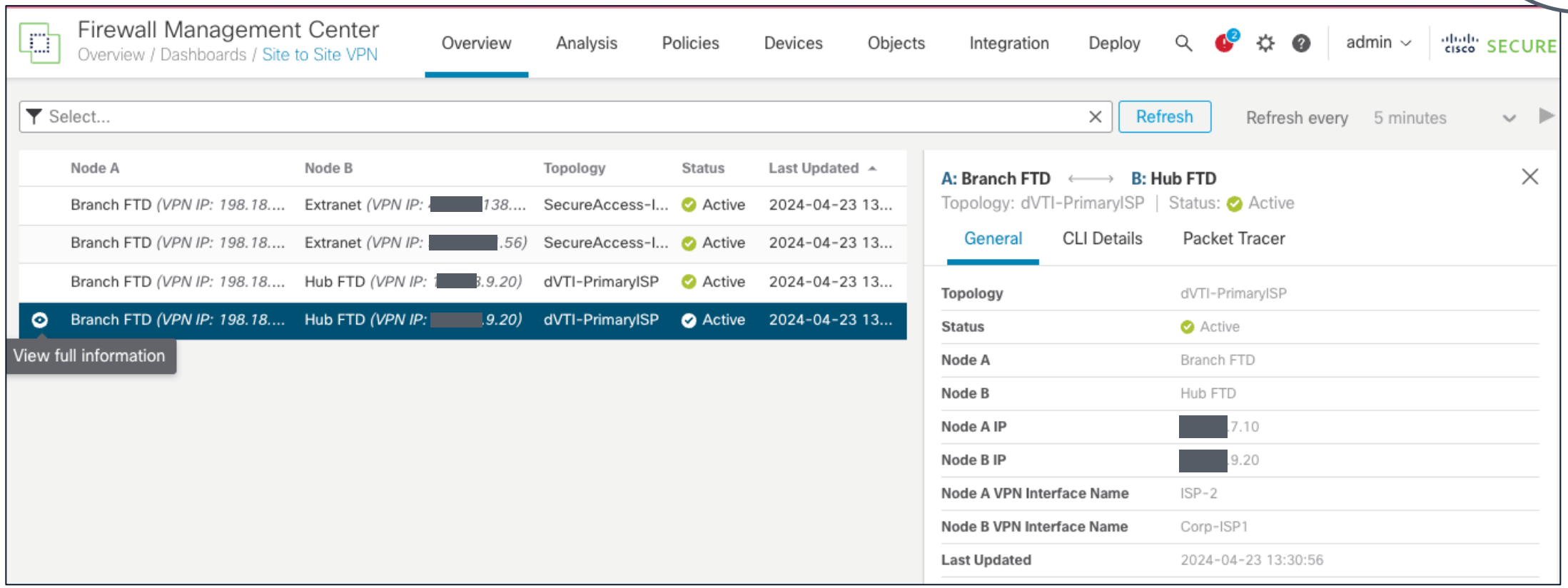
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Site to Site VPN Dashboard

WAN Fabric

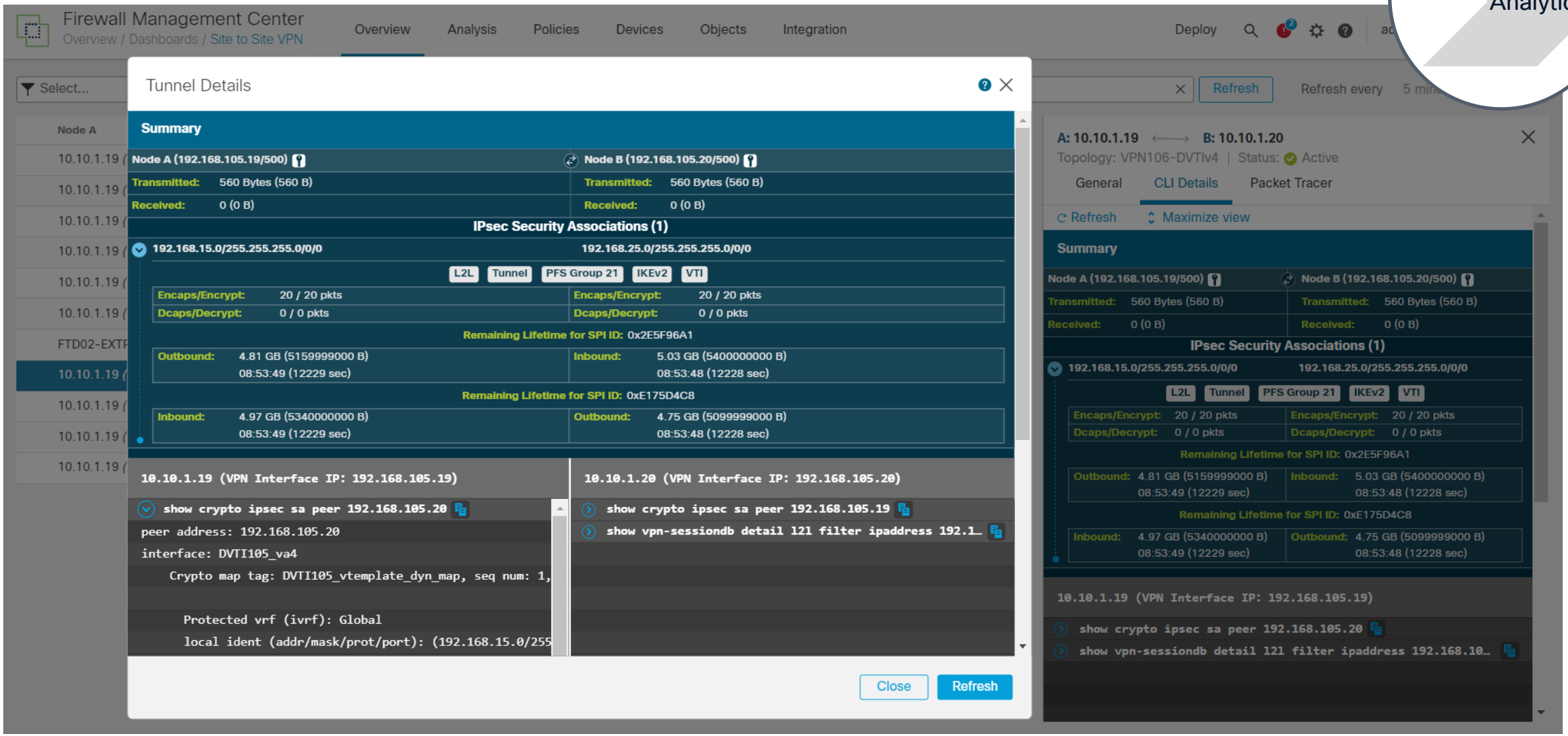
Overview



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Site to Site Monitoring (7.4+)

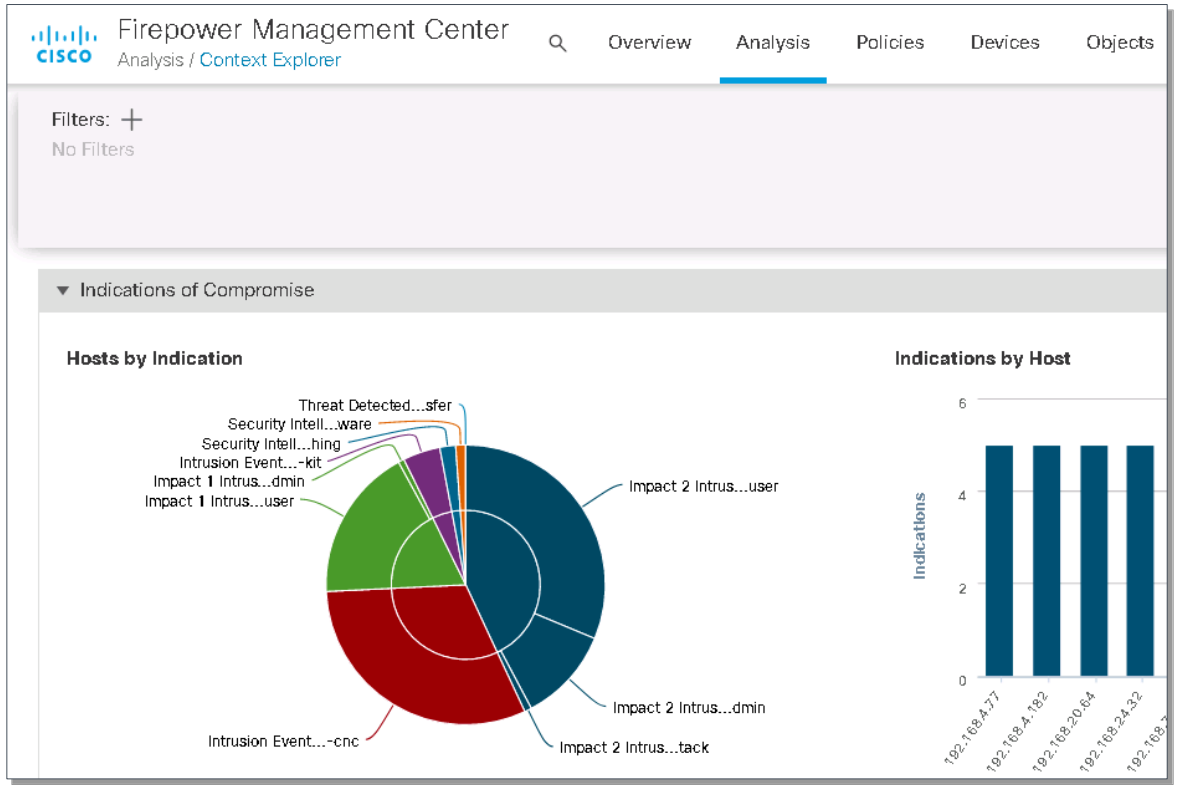


© 2025 Cisco and/or its affiliates. All rights reserved.

Best-in-class Branch Security

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

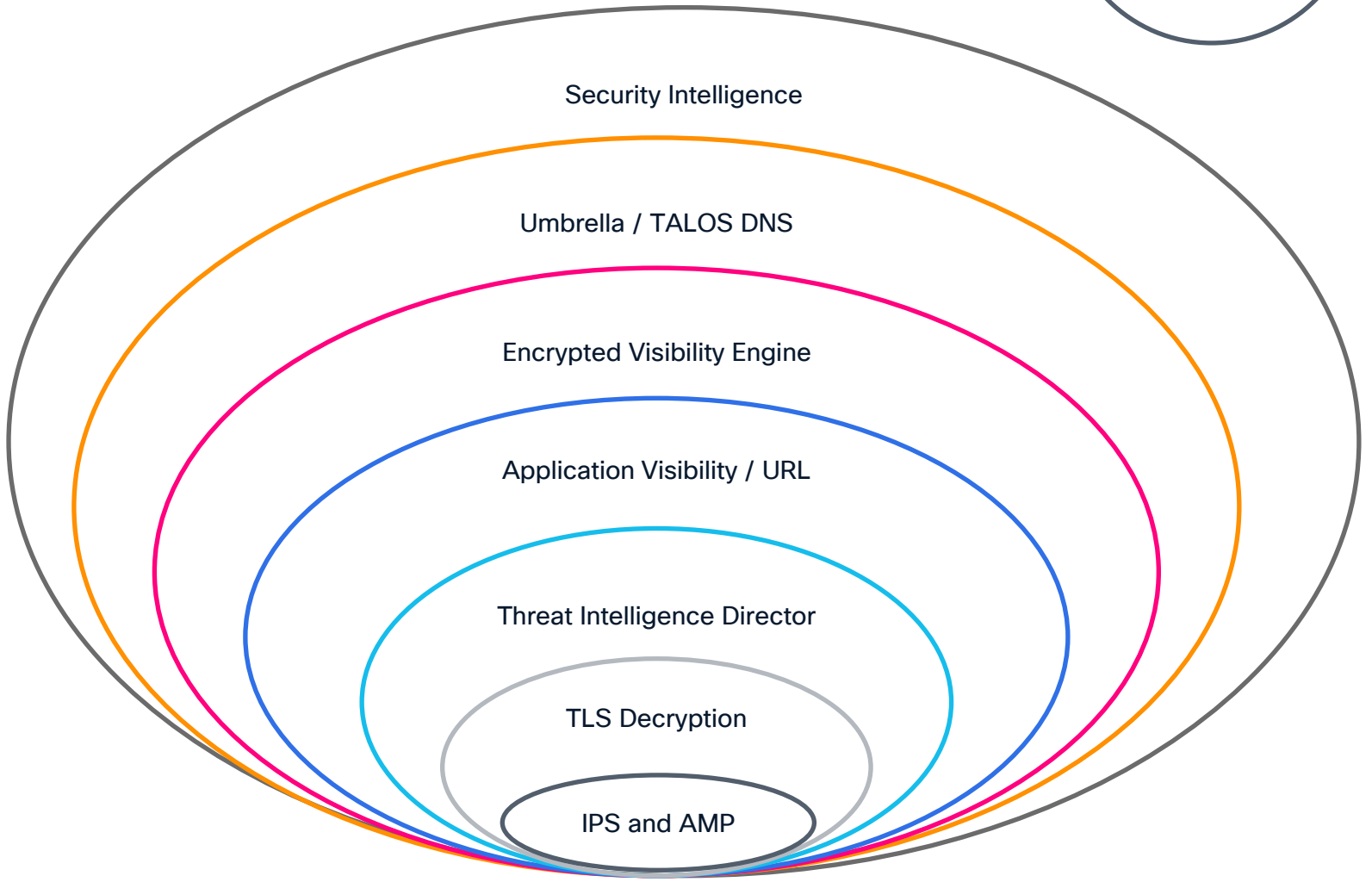
- NGFW / Intrusion Prevention
- Integrated TLS Visibility & Decryption
- VPN & Zero Trust Access Security
- Threat Intelligence Director
- Malware Analysis with Retrospection
- QUIC Fingerprinting
- Encrypted Visibility Engine



© 2025 Cisco and/or its affiliates. All rights reserved.

Layered Security built upon Snort ML

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



© 2025 Cisco and/or its affiliates. All rights reserved.

Firewall Threat Defense SD-WAN Solution

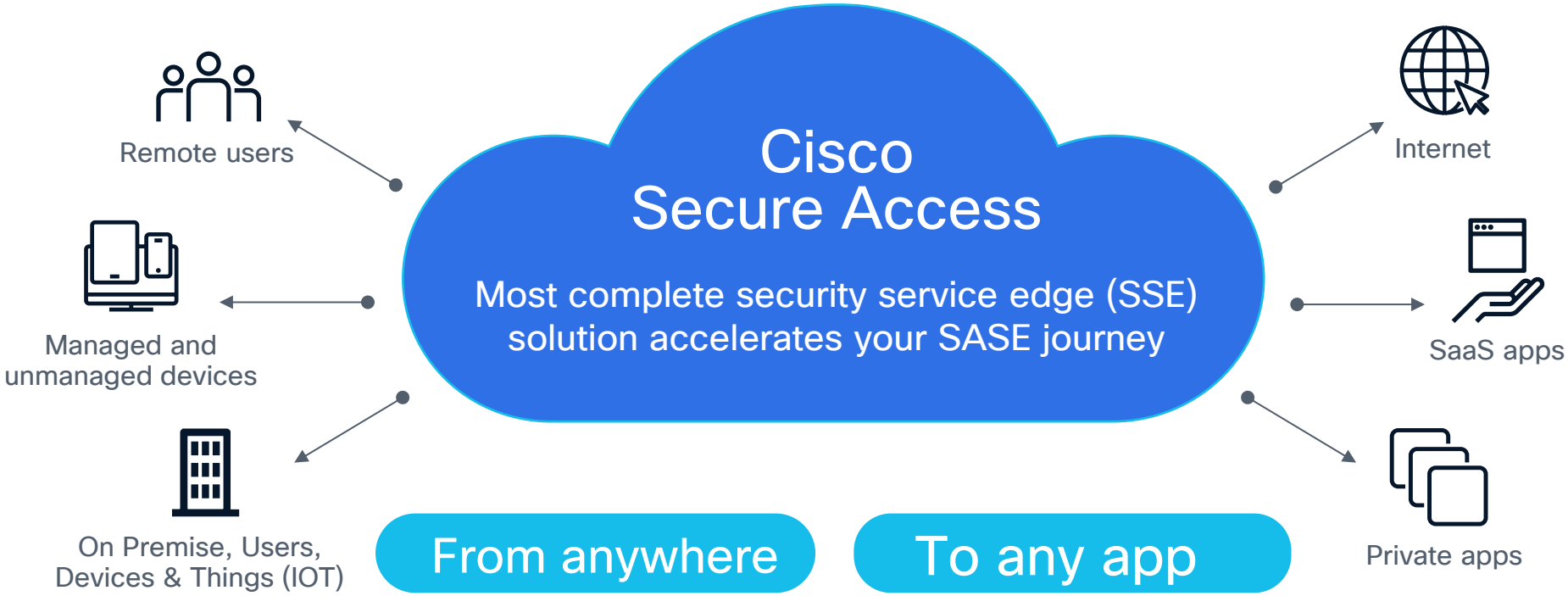
- ✓Powerful cloud or on-prem management of all capabilities
- ✓Customizable VPN and routing capabilities up to 1000 sites
- ✓Best in class edge security capabilities, especially for encrypted traffic

© 2025 Cisco and/or its affiliates. All rights reserved.

Security Service Edge (SSE)
Featuring Cisco Secure Access

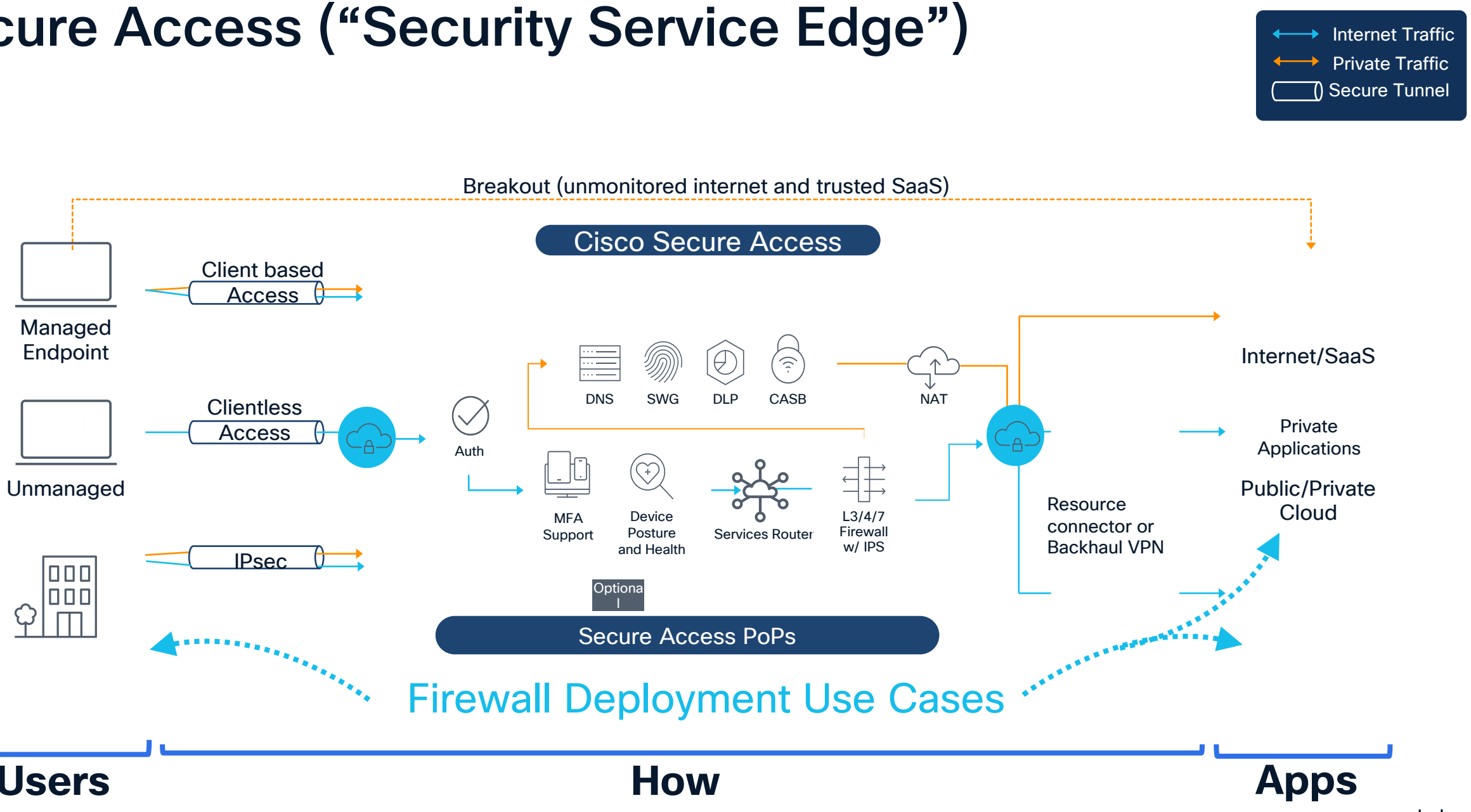
Cisco Secure Access

Converged cloud security grounded in zero trust



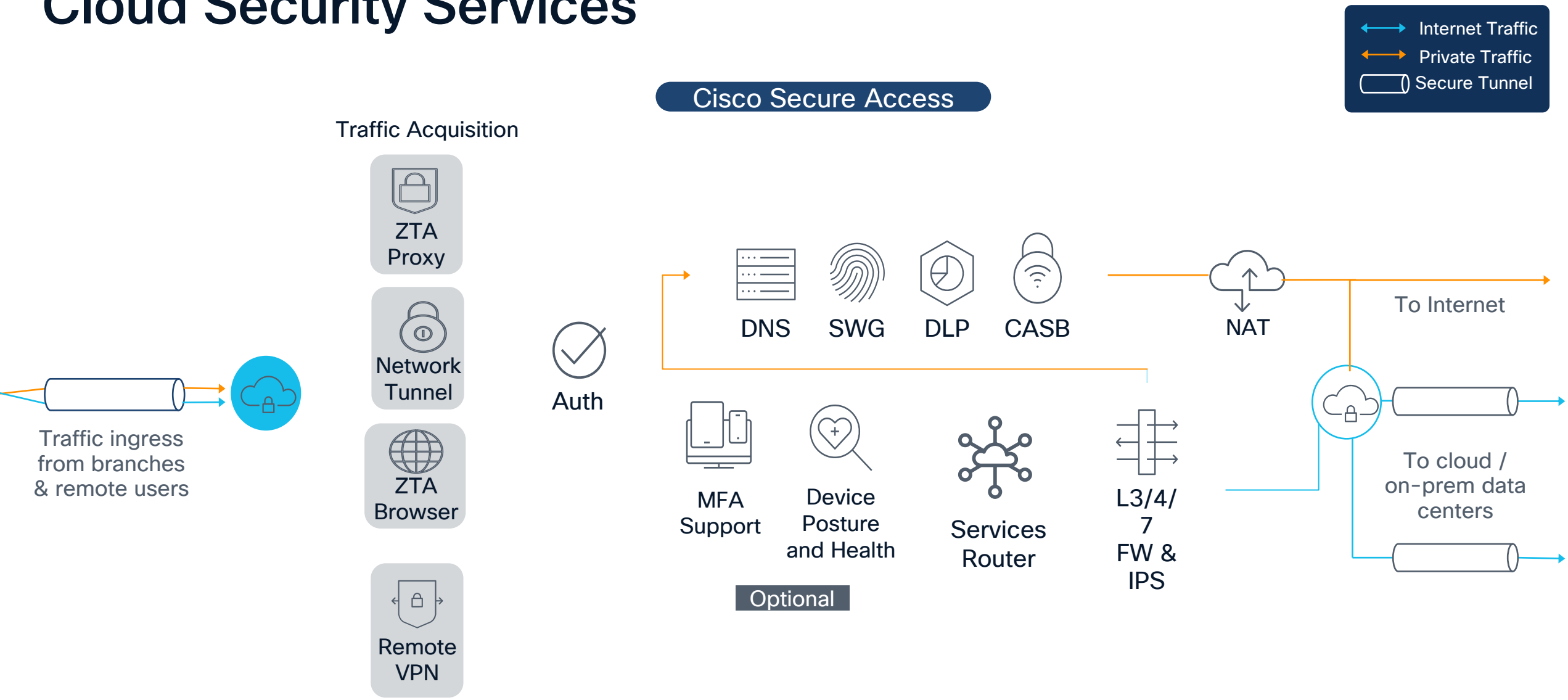
© 2025 Cisco and/or its affiliates. All rights reserved.

Secure Access (“Security Service Edge”)



© 2025 Cisco and/or its affiliates. All rights reserved.

Cloud Security Services

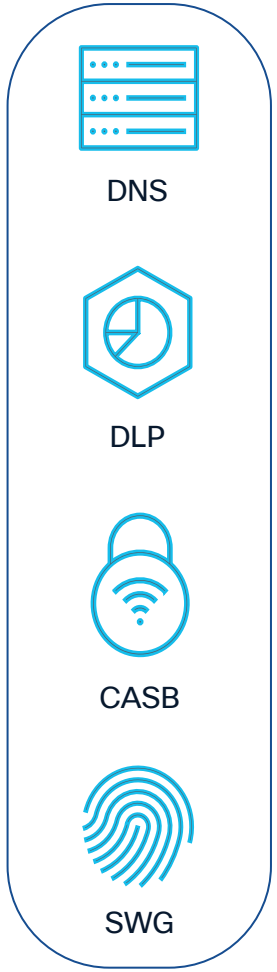


© 2025 Cisco and/or its affiliates. All rights reserved.

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.



Private application access:

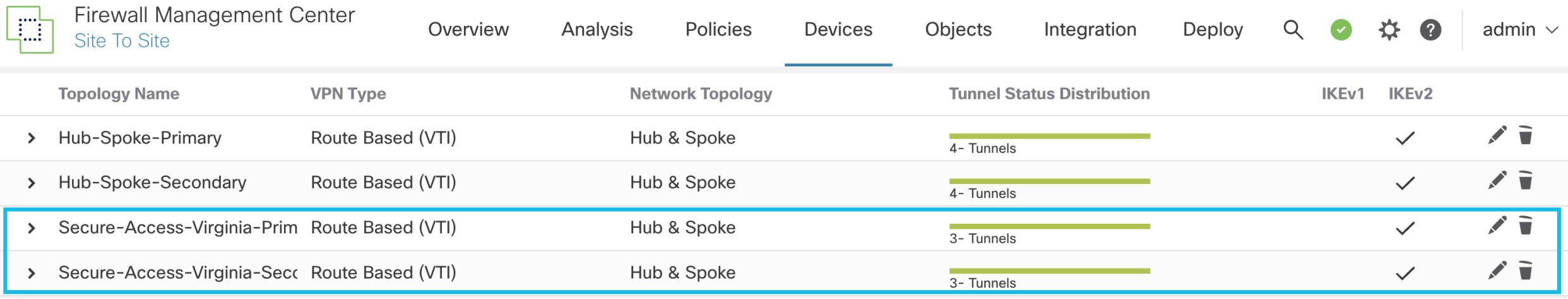
- Connectivity to private apps protected by Secure Access
- Connectivity for private applications behind branch firewall
- Connectivity to cloud delivered RAVPN as a service subnets

© 2025 Cisco and/or its affiliates. All rights reserved.

SSE Integration

with Firewall Threat Defense

Secure Access Branch Tunnels



- 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Access Routing Configuration

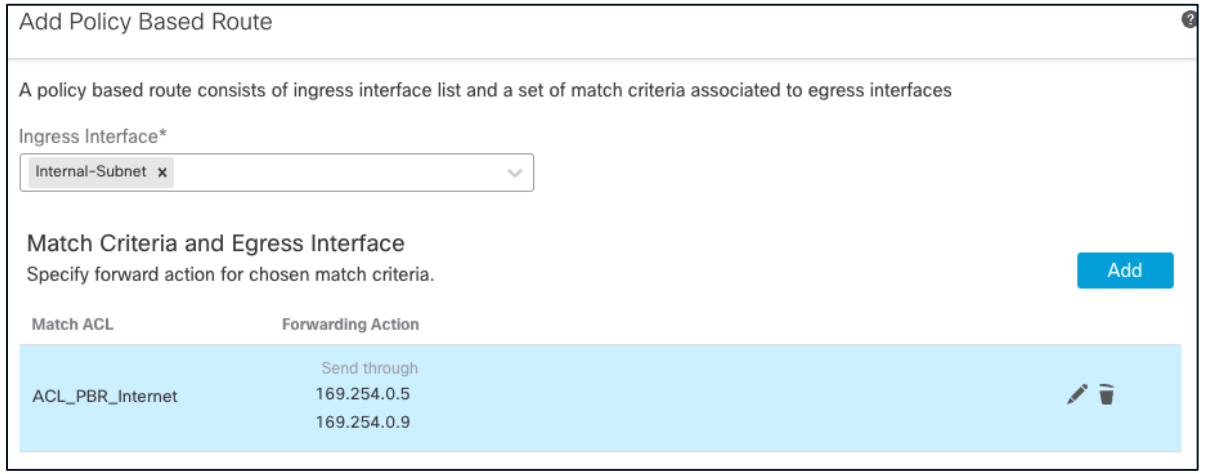
BGP or Static routing

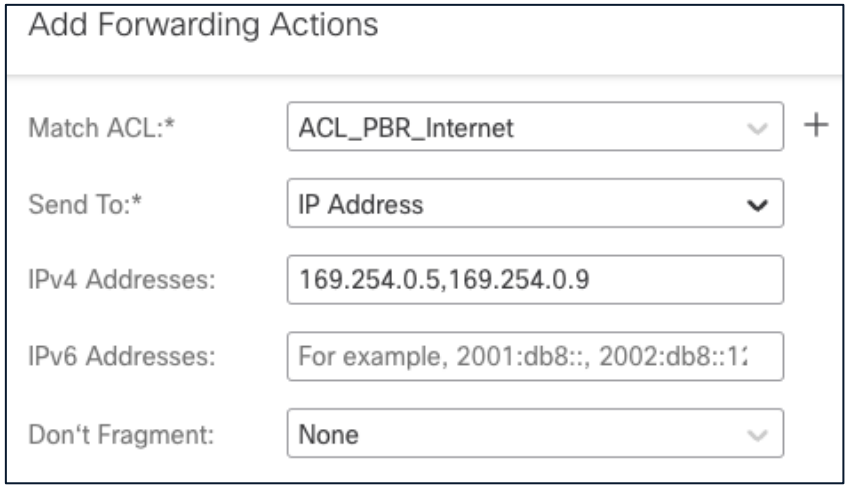
Static Route considerations:

- 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





© 2025 Cisco and/or its affiliates. All rights reserved.

FTD Branch with Secure Access

Routes from Secure Access:

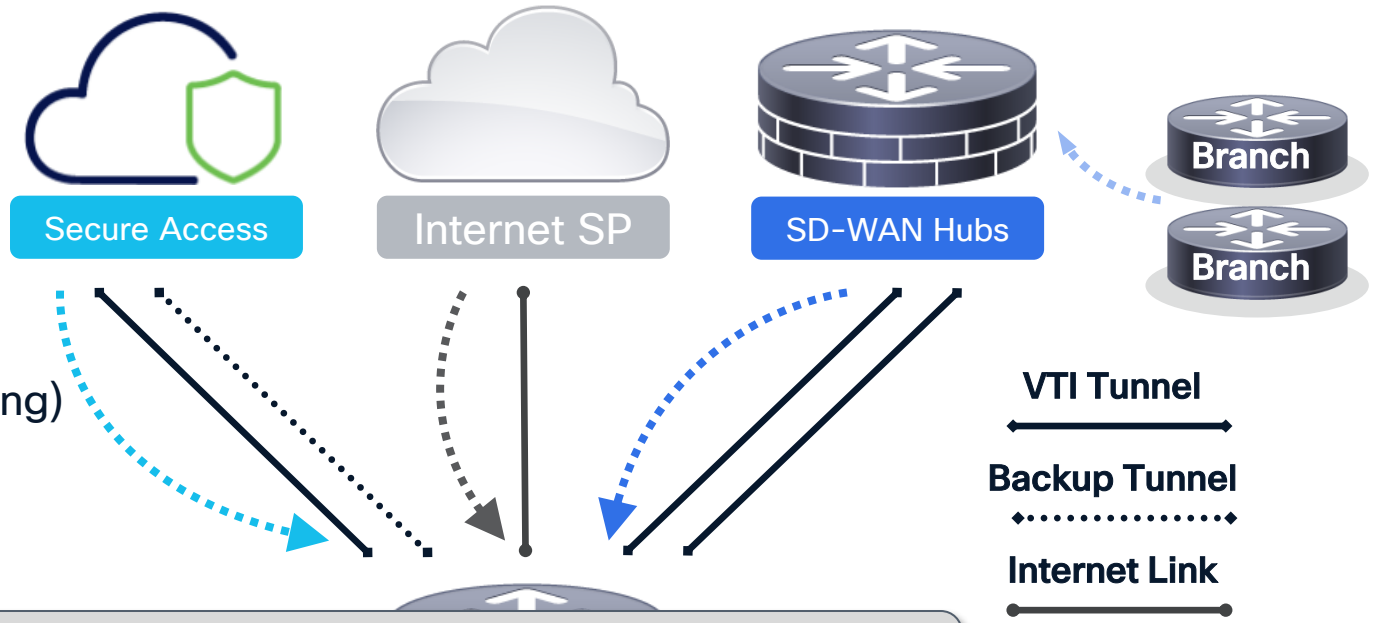
- Default Route* (Optional)
- RAVPN Subnets, Zero Trust enabled applications, Proxy Infrastructure

Static routes to ISP:

- Secure Access DC VPN Endpoint IPs (prevent flapping)

Routes from SD-WAN Hubs:

- SD-WAN HQ, branches, and data centers

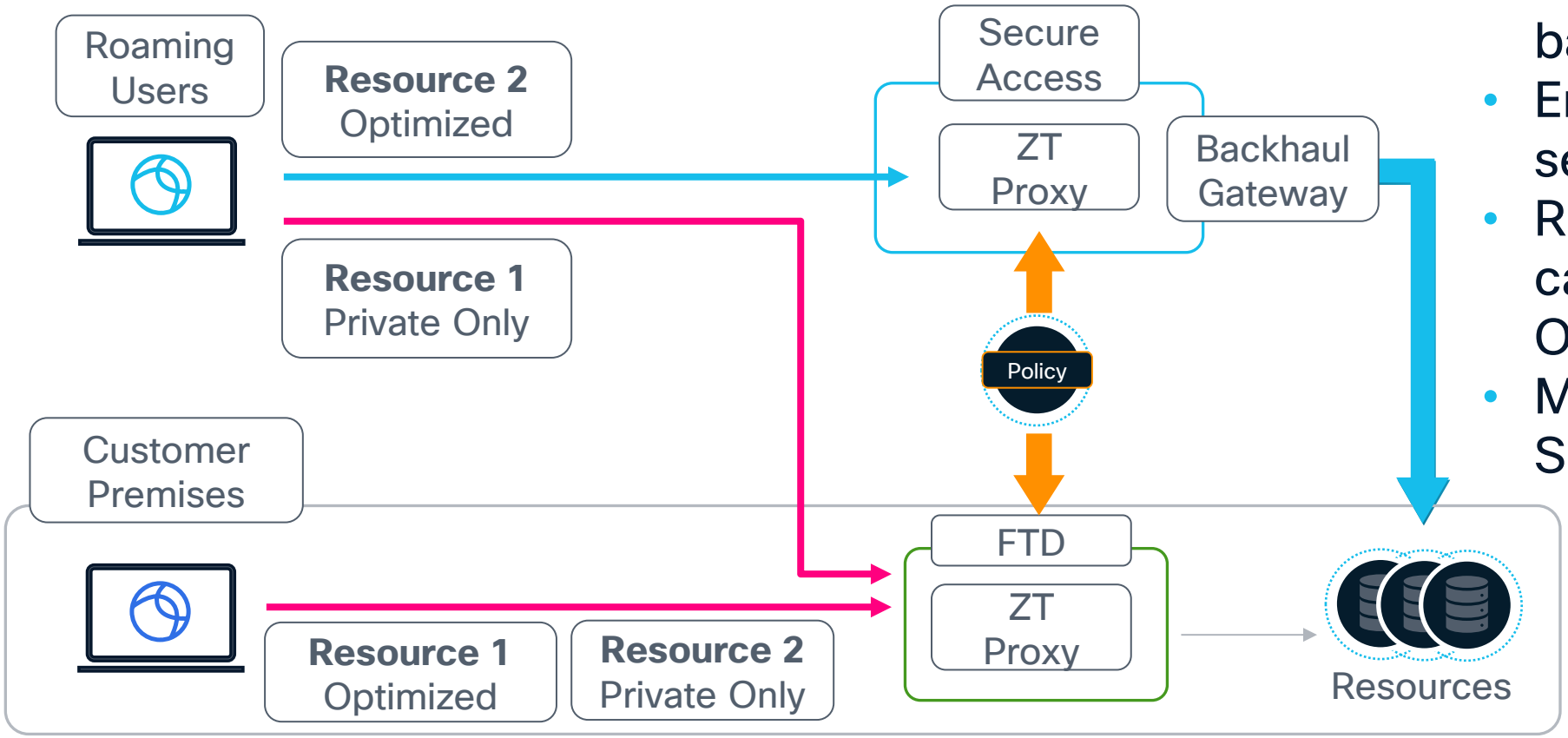



```
FTD-Spoke# show route
B* 0.0.0.0 0.0.0.0 [20/0] via 169.254.0.5
B  100.73.x.0 255.255.240.0 [20/0] via 169.254.0.5

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
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Hybrid Private Access with Secure Firewall

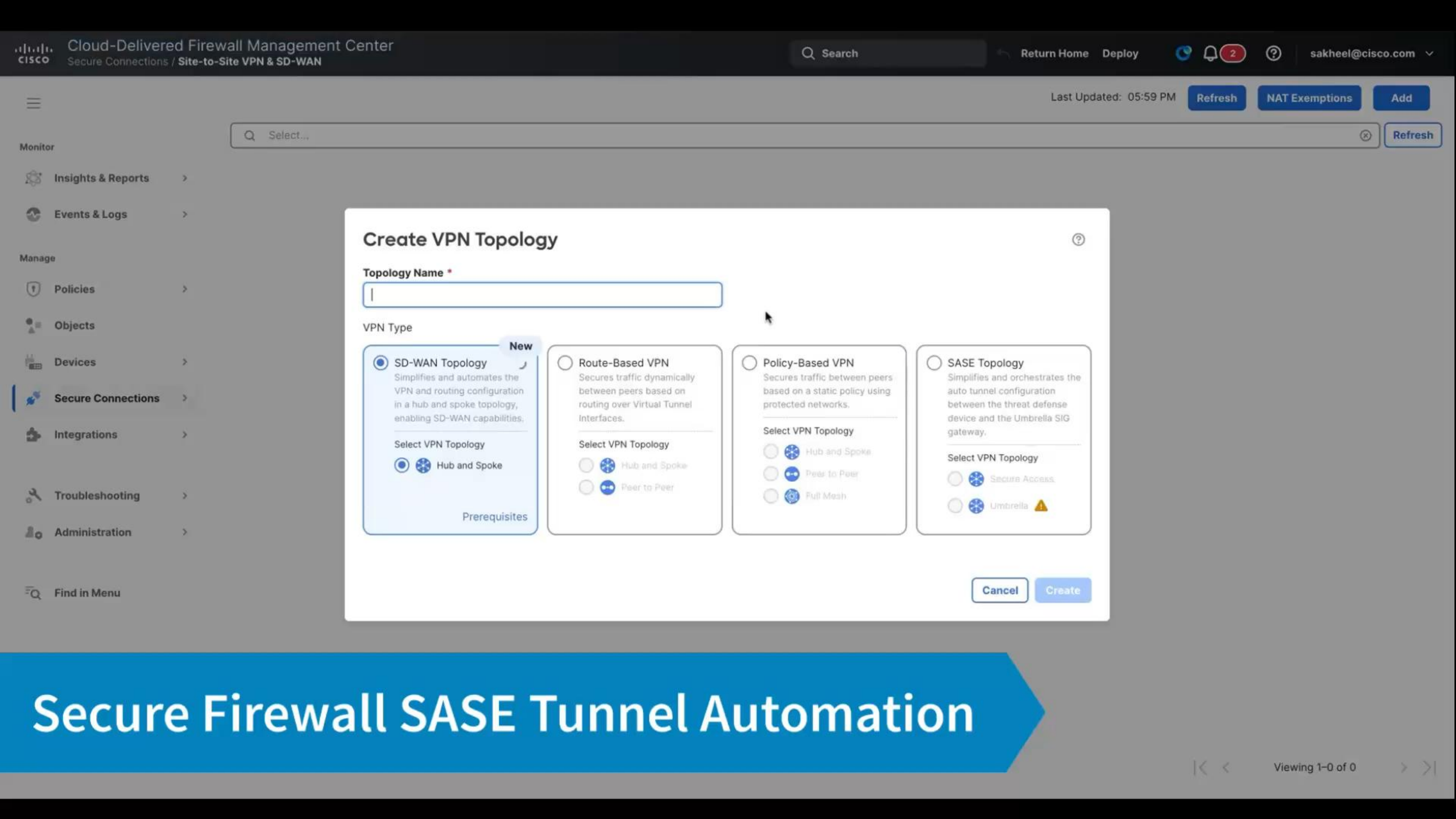
Single Policy, Distributed Enforcement (Overview)



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

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

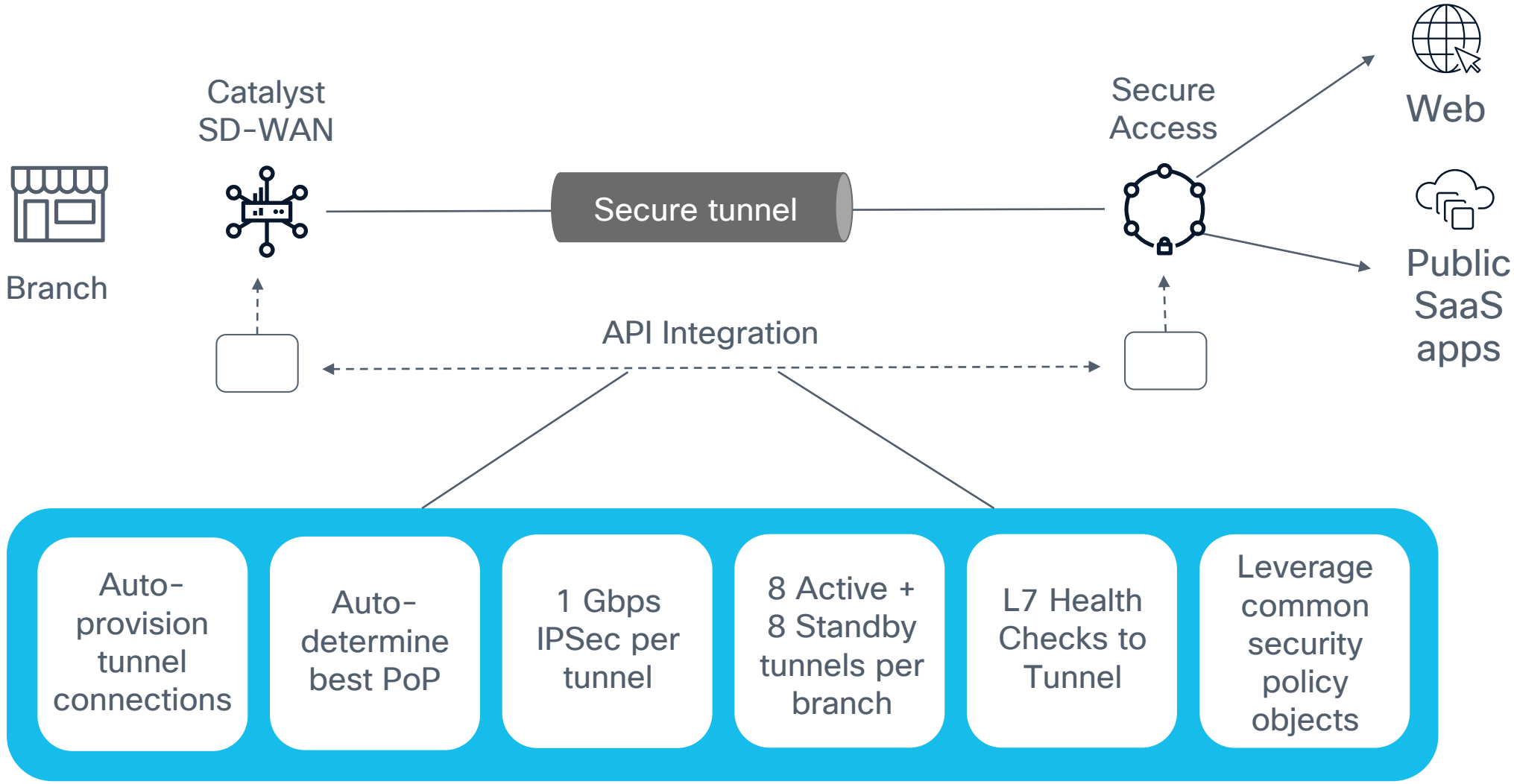


Secure Firewall SASE Tunnel Automation

SSE Integration

with Catalyst SD-WAN

Secure Access + Catalyst SD-WAN

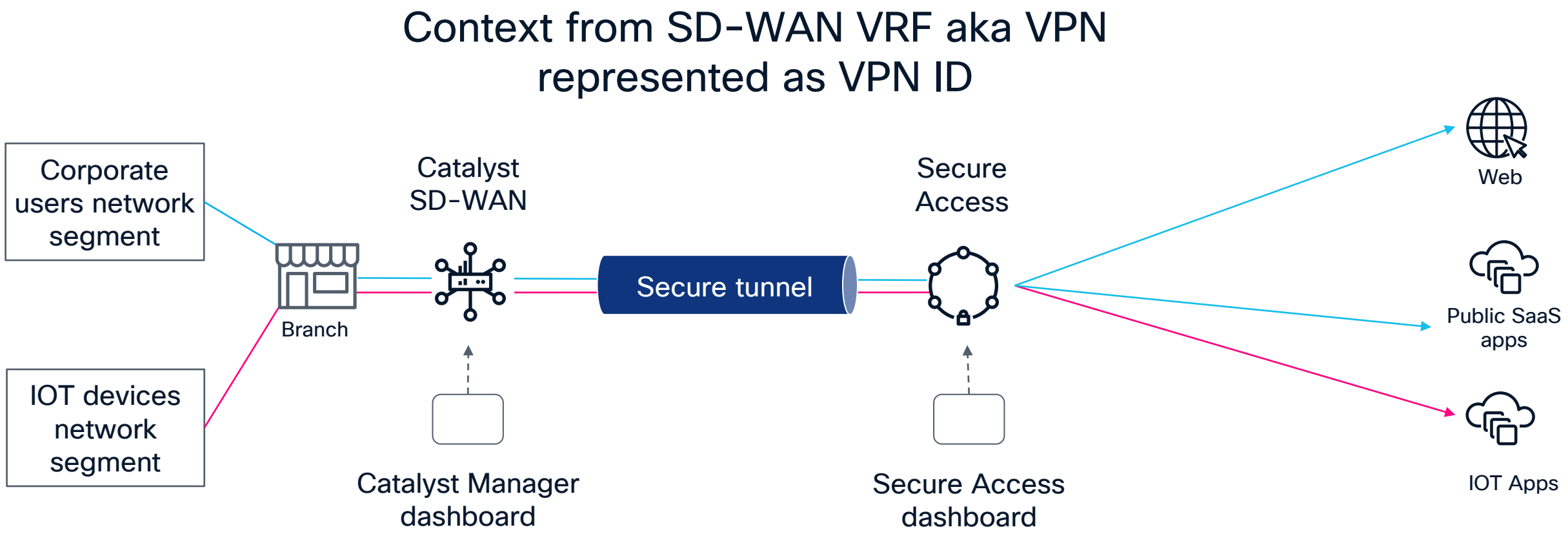


Better Together – Simplified SASE Implementation

© 2025 Cisco and/or its affiliates. All rights reserved.

Secure Access + Catalyst SD-WAN

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

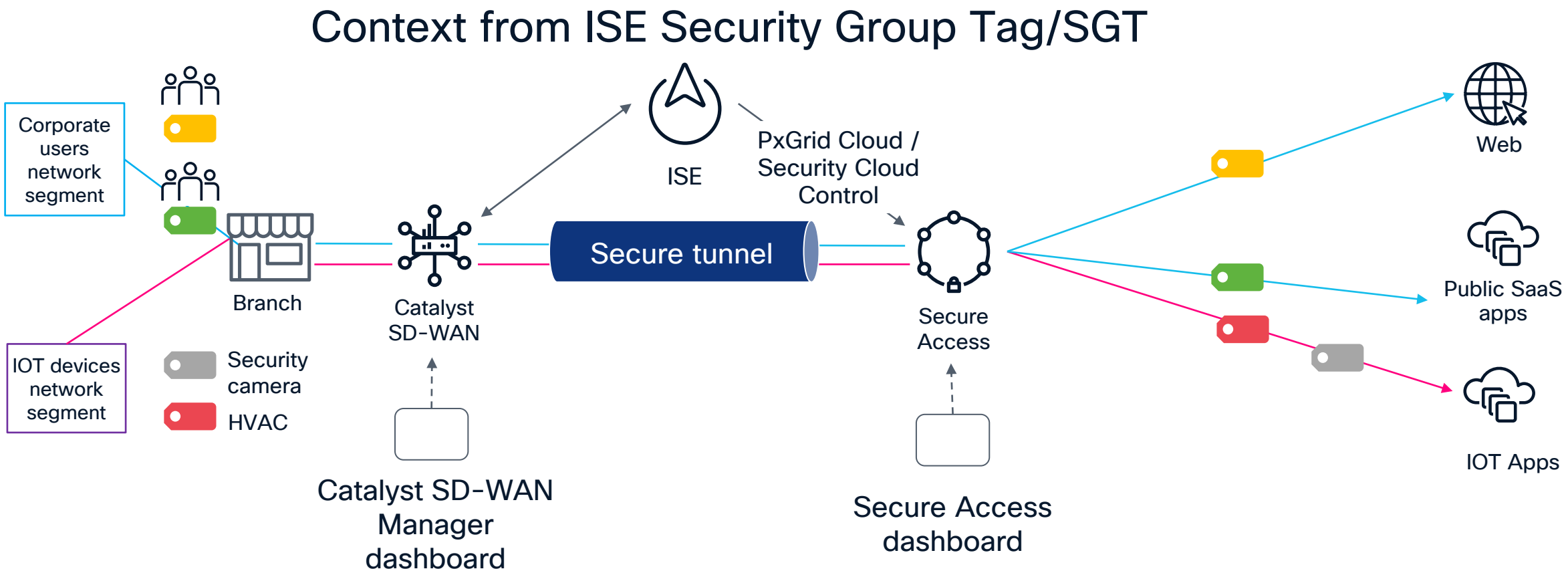


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

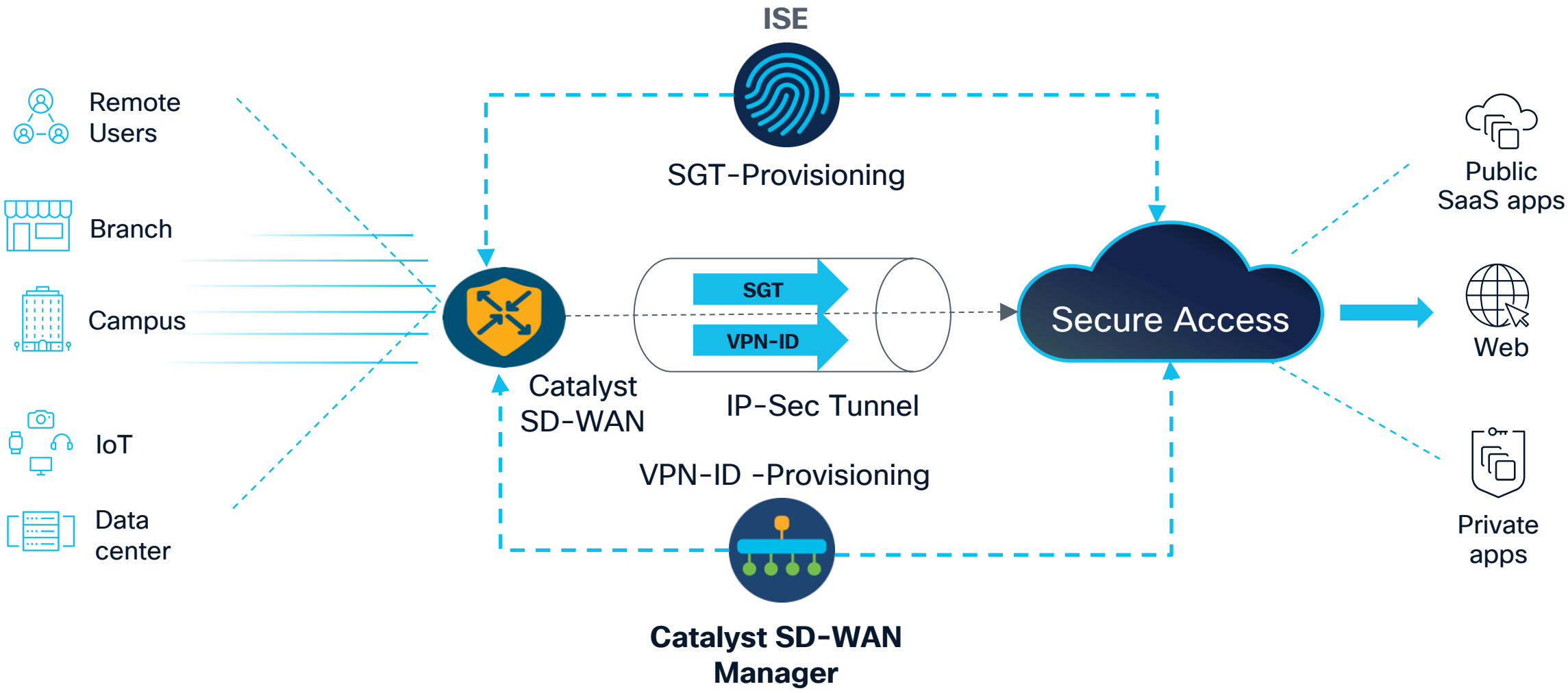
Secure Access + Catalyst SD-WAN

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

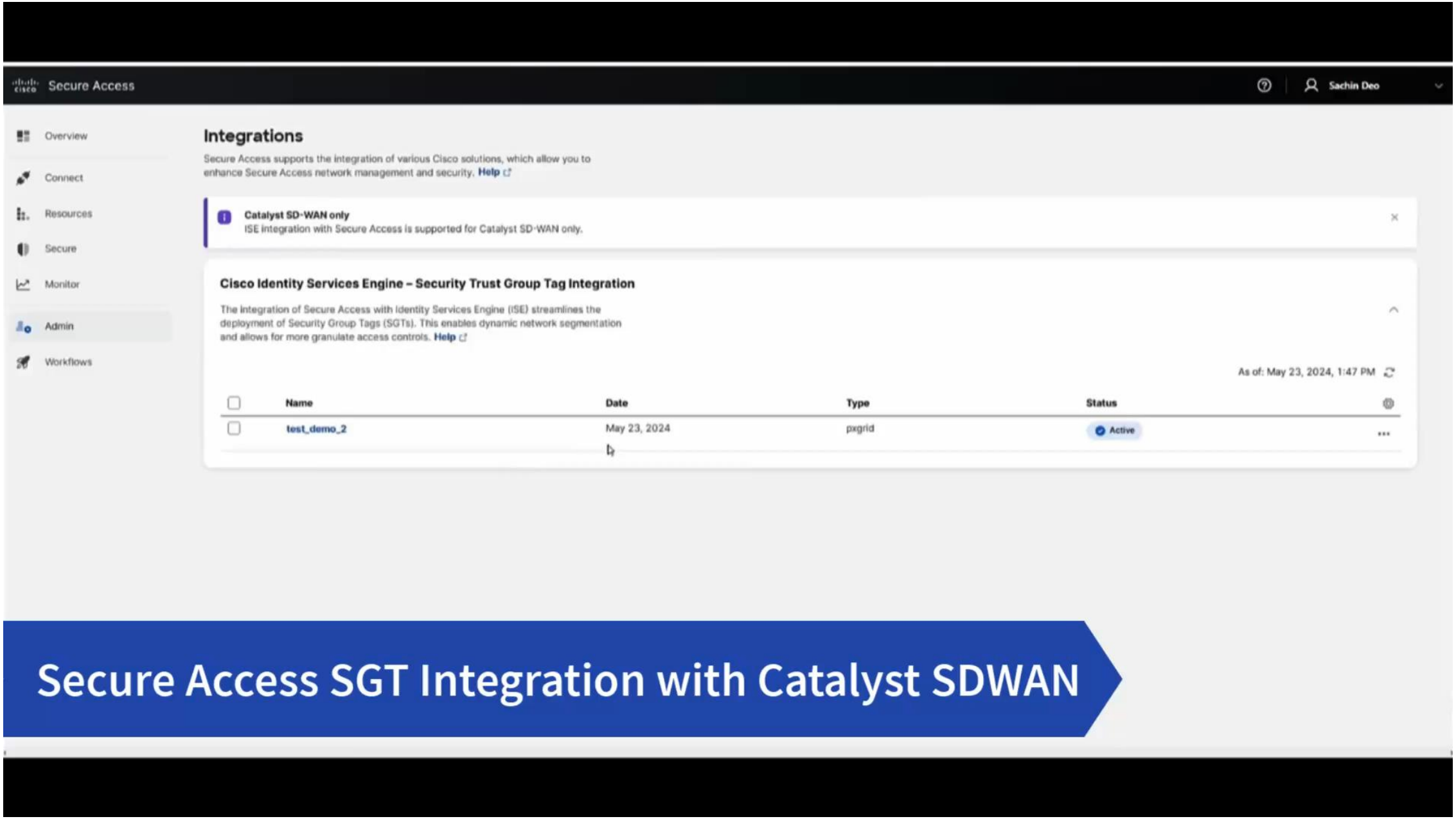


© 2025 Cisco and/or its affiliates. All rights reserved.

Macro and Micro Segmentation Based Policy



© 2025 Cisco and/or its affiliates. All rights reserved.



Secure Access SGT Integration with Catalyst SDWAN

© 2025 Cisco and/or its affiliates. All rights reserved.

SSE Integration

with Meraki MX

cisco Live !

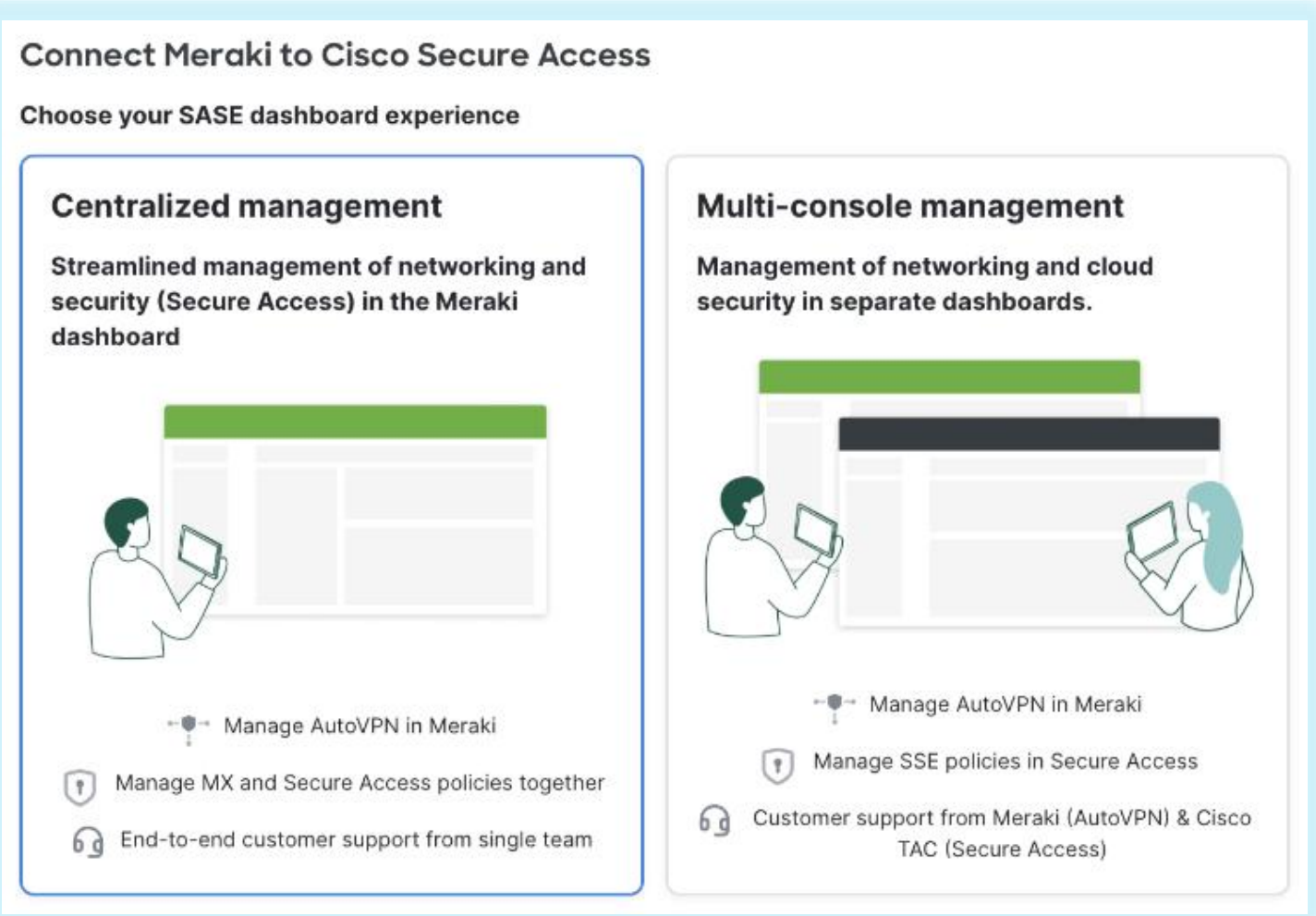
Zero Friction: One SSE, Cisco Secure Access

Cisco Secure Connect

Meraki + Umbrella,
Secure Access (ZTNA only)

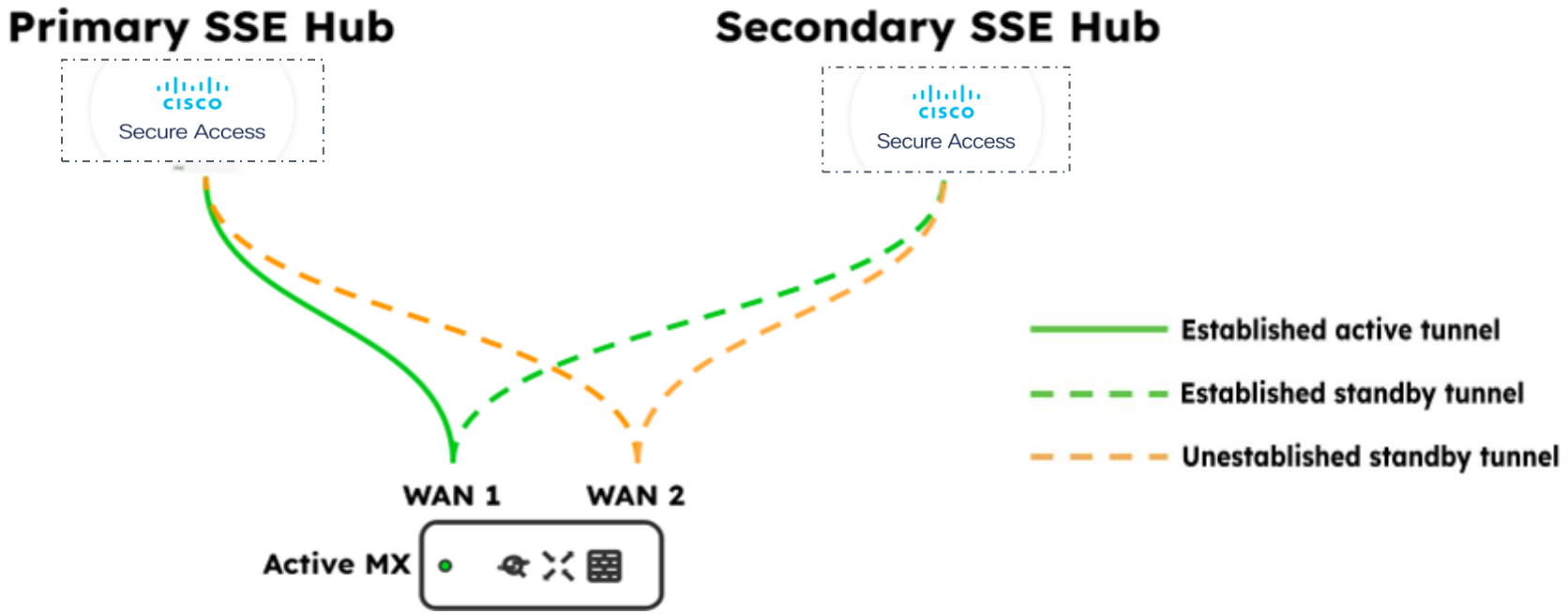
Cisco Secure Access

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



© 2025 Cisco and/or its affiliates. All rights reserved.

Secure Access (IPSEC VPN Redundancy)



Secure Internet Access with redundancy

Active & Backup tunnels

Secure Internet & Private Access with redundancy

BGP over IPsec*

** pending BGP multihop support in Secure Access*

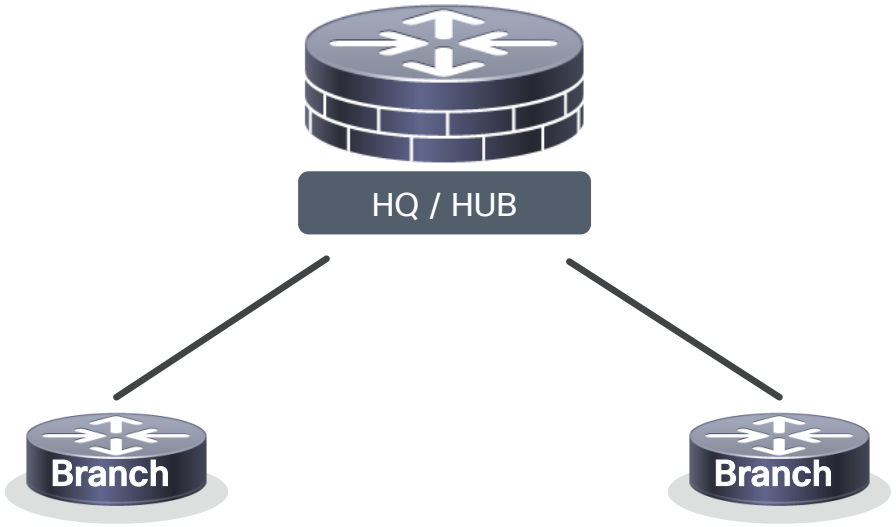
Available with MX 19.1 Firmware Release

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco’s secure & scalable SD-WAN solutions

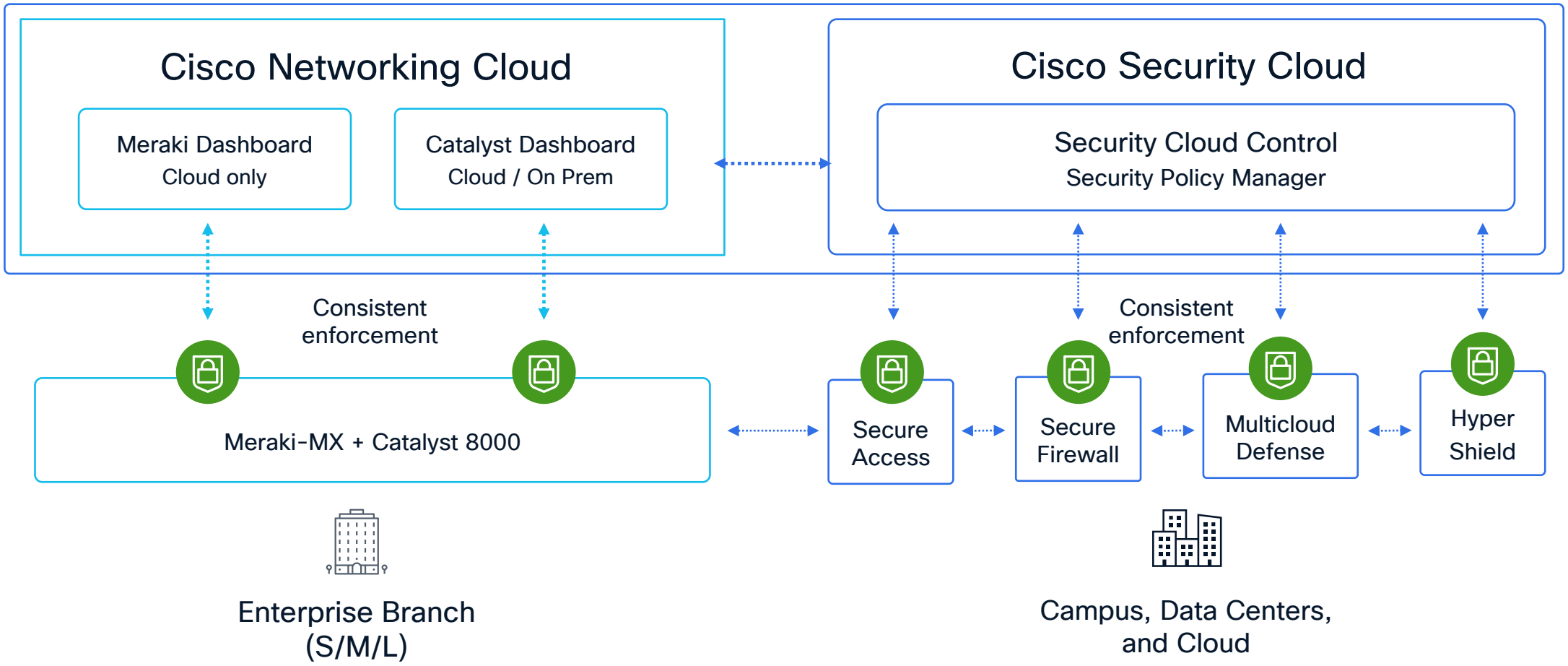
All Cisco SD-WAN Platforms offer:

- 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!



© 2025 Cisco and/or its affiliates. All rights reserved.

Unified Secure SD-WAN experience



© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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!

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Complete your session evaluations

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

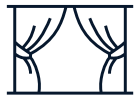
Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

CISCO