Secure!

Cisco SDWAN Use Cases & Best Practices

Jeff Fanelli - Distinguished Solutions Engineer
@jefanell

BRKSEC-2708

cisco Live!

Session Abstract

- In this session, we will explore Cisco's robust secure SDWAN 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 SDWAN offerings!

Agenda

- Introduction & SD-WAN Basics
- Use cases based on platform benefits:
  - Catalyst SDWAN
  - Meraki MX
  - Firewall Threat Defense
- SSE / SASE integration
- Summary

Webex App

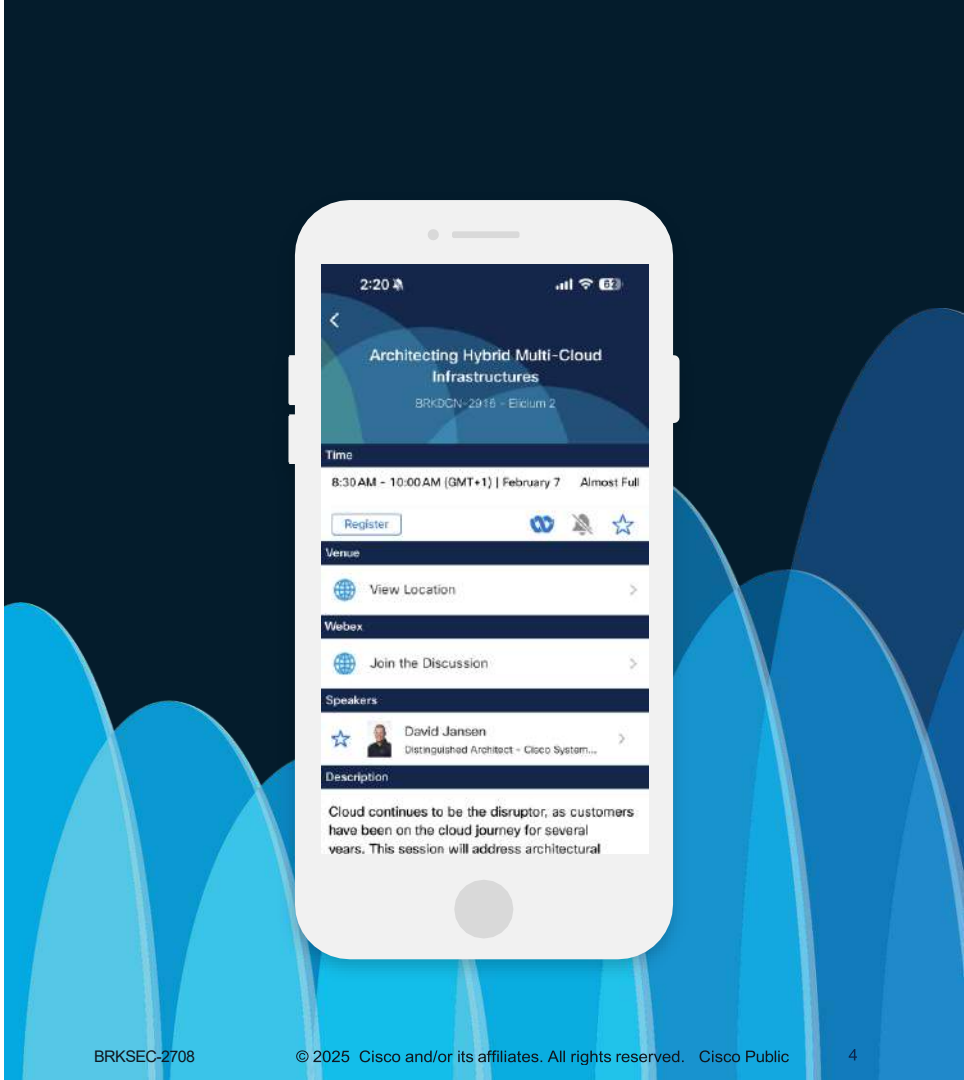
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.



About Me

Jeff Fanelli

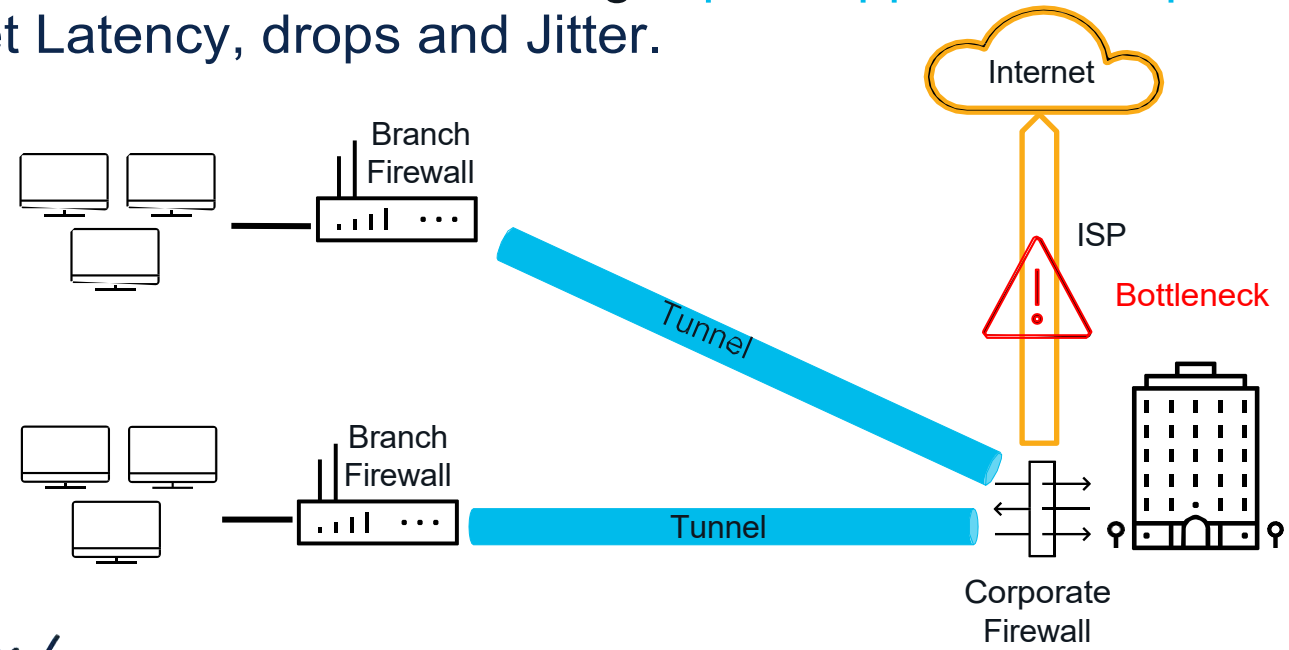
- jefanell@cisco.com
- Distinguished Solutions Engineer
- 19 years @ Cisco
- 40+ Cisco Live Presenter
- Husband + father
- Instrument rated pilot
- Sausage dog servant

SD-WAN Basics

cisco Live!

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.

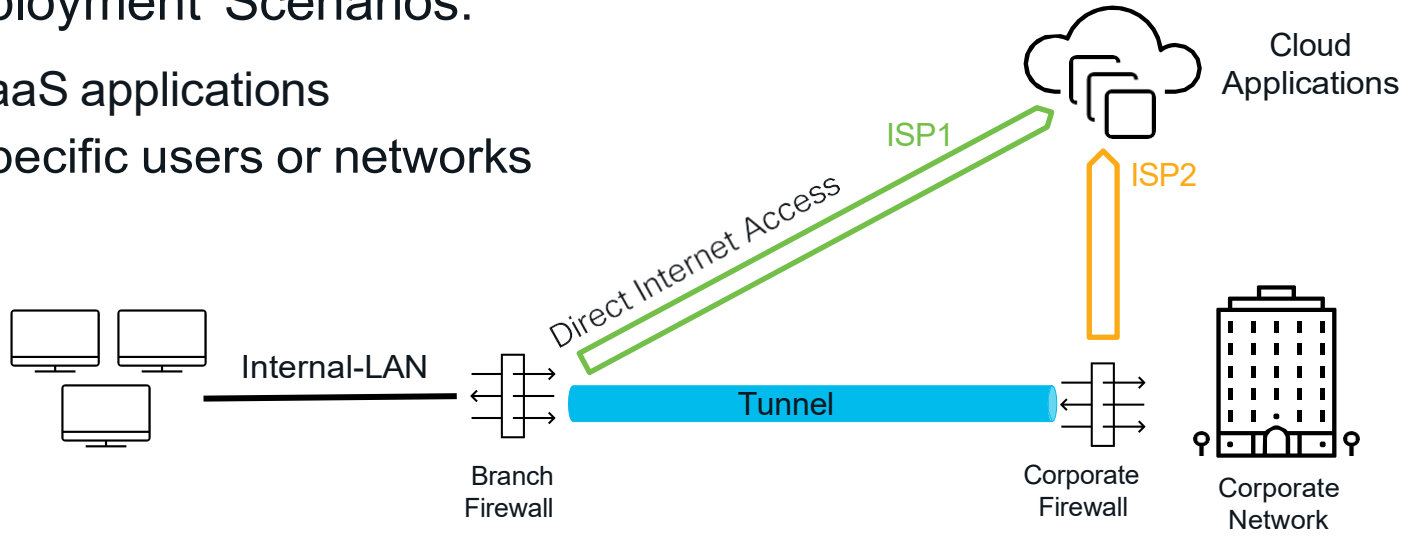


Direct Internet Access (DIA)

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

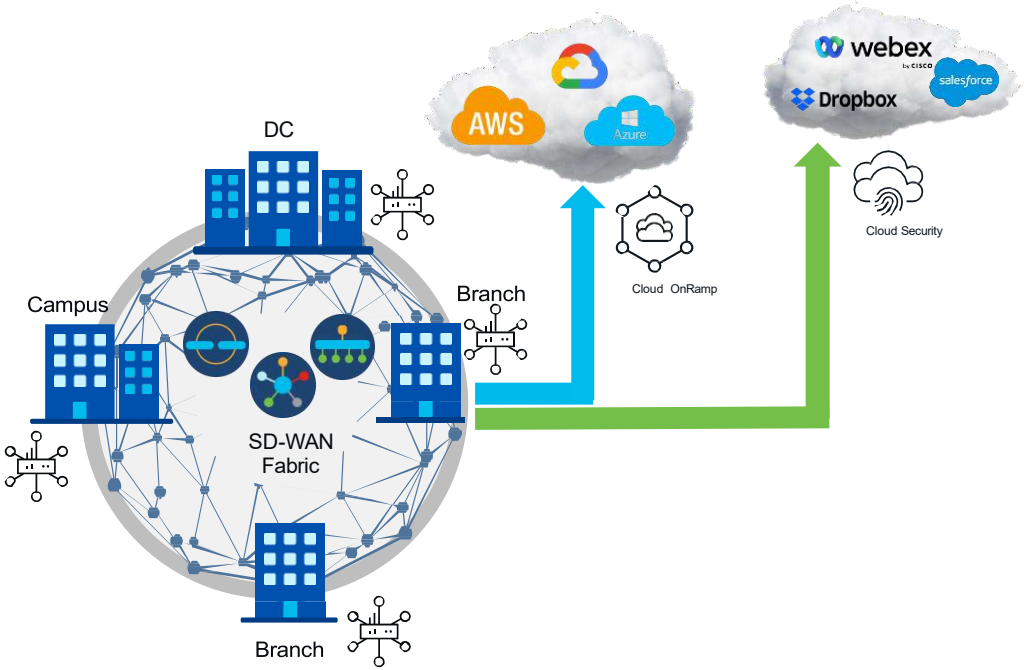
Deployment Scenarios:

- SaaS applications
- Specific users or networks



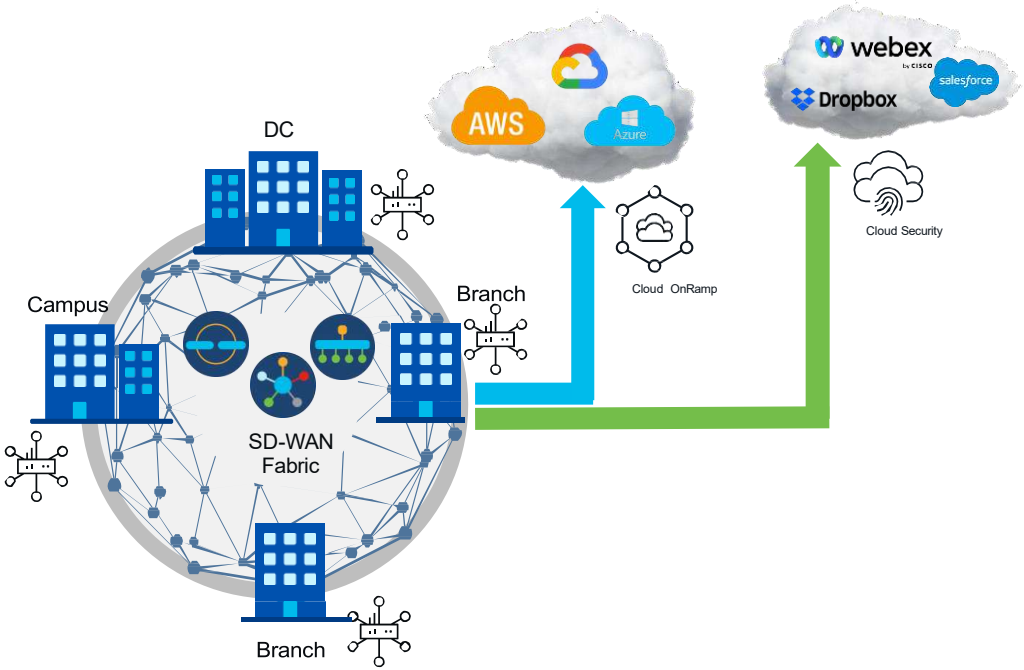
Software-Defined Wide Area Network

- 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.

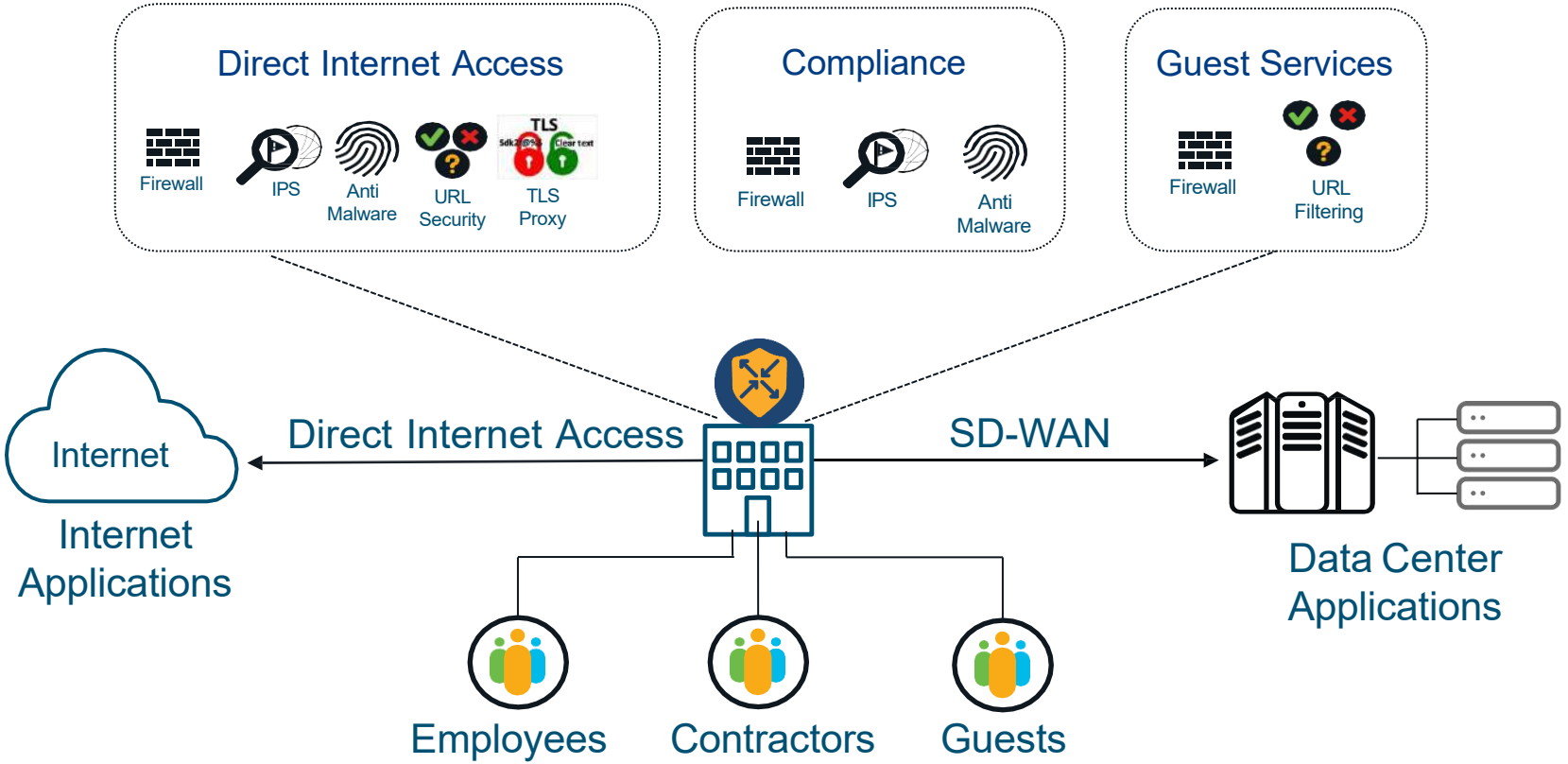


What Software-Defined Internet?

- 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



SD-WAN Security Use Cases

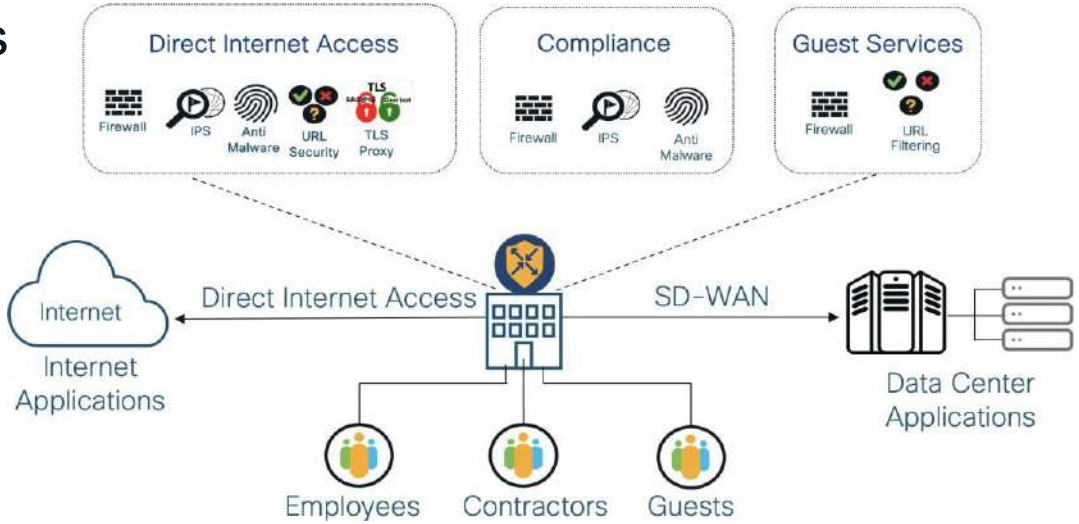


Why Secure SD-WAN?

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

Examples:

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



Catalyst SDWAN Use Cases & Capabilities

SD-WAN Secure Edge Solution Overview

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 (splunk> LiveAction)

Embedded Security

- Firewall Stateful ZBFW
- **Segmentation** With Multi-Topology
- AMP File Reputation & Sandboxing from Talos
- Snort
- IPS Protection against complex threats
- 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

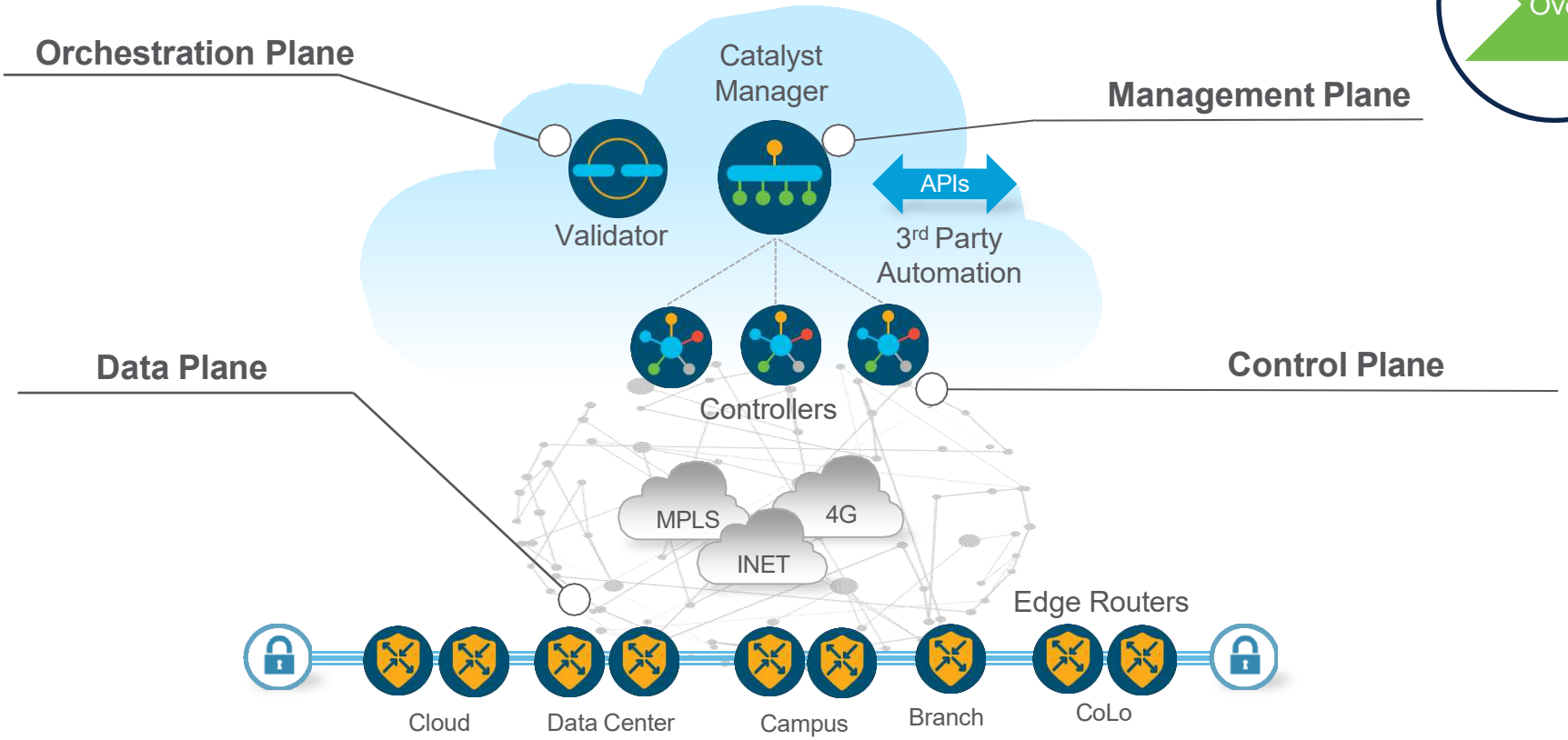
Cisco Secure Access

Cisco Umbrella

Third Party SSE

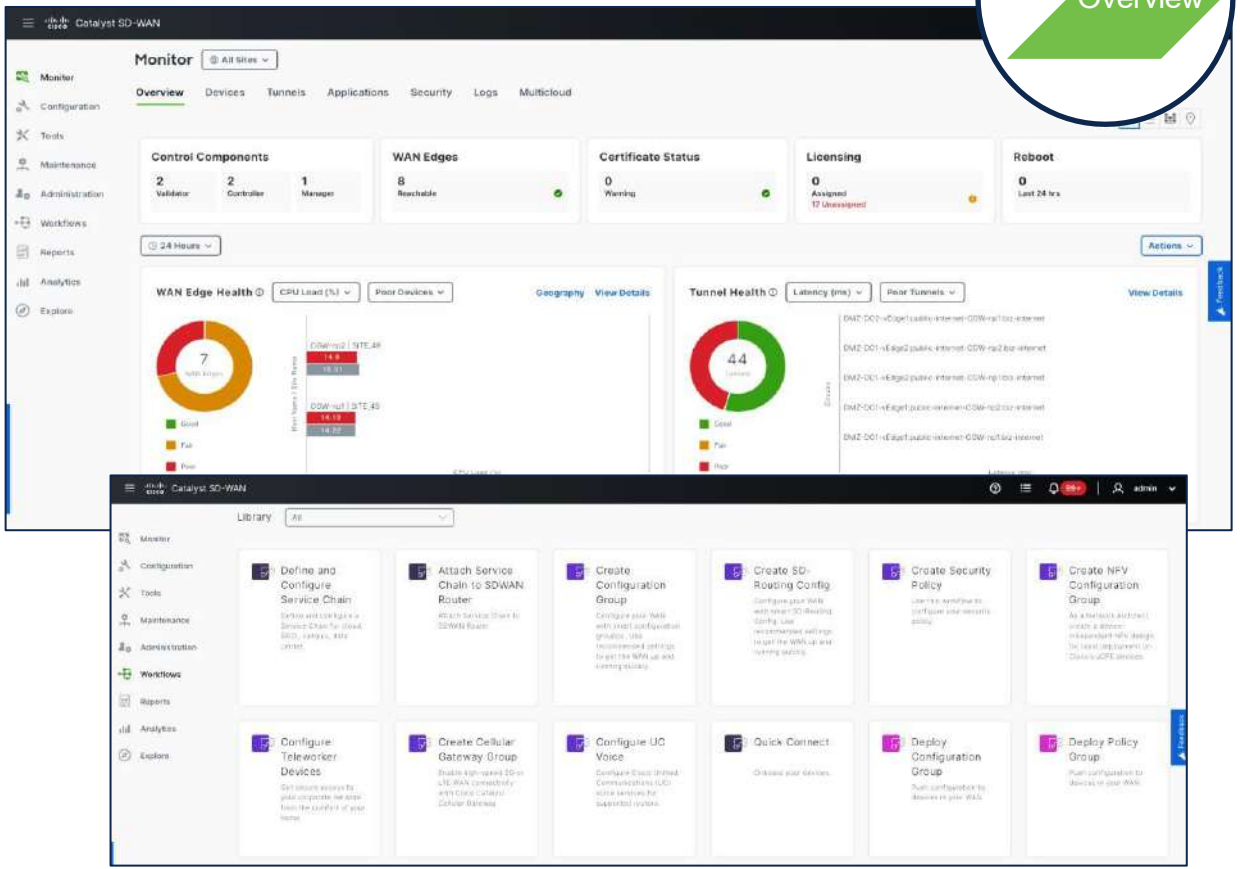
Cisco Catalyst SD-WAN Architecture

Overview



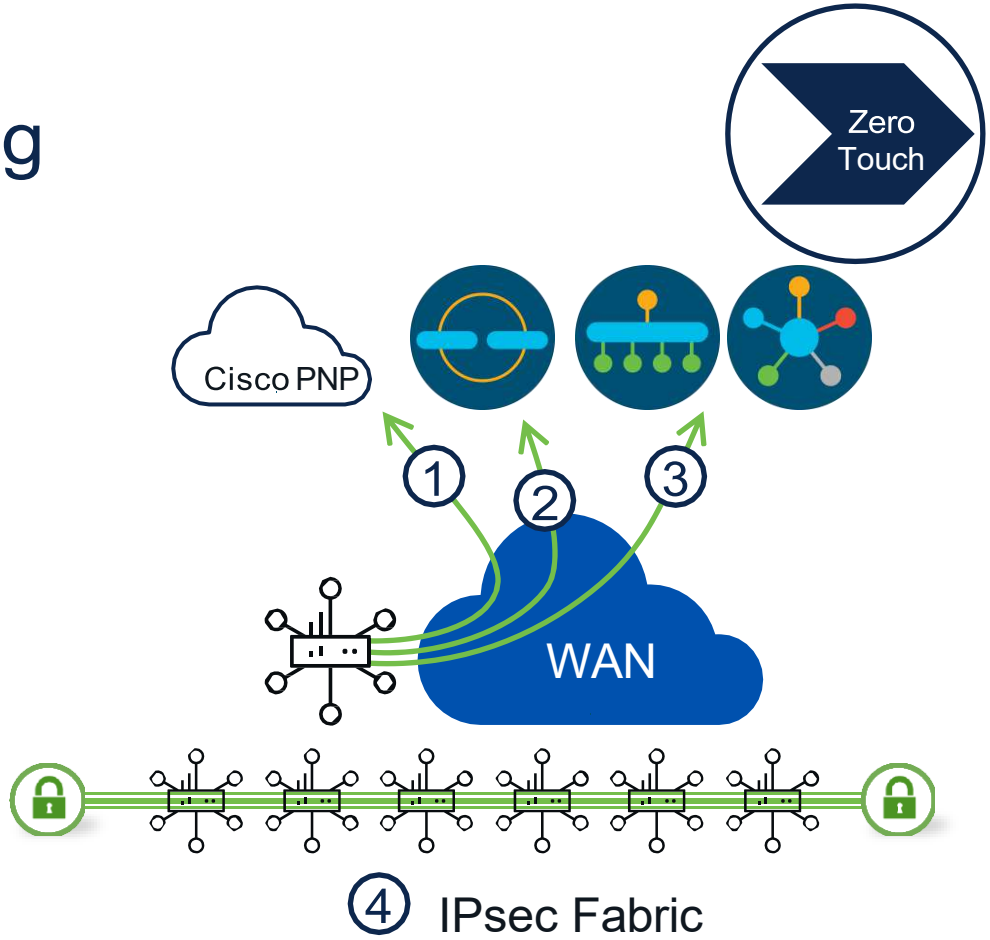
SD-WAN Manager (UI)

- Enhanced UI
- Guided Workflow
- Simplified Configuration
- Granular Management
- Smart Troubleshooting



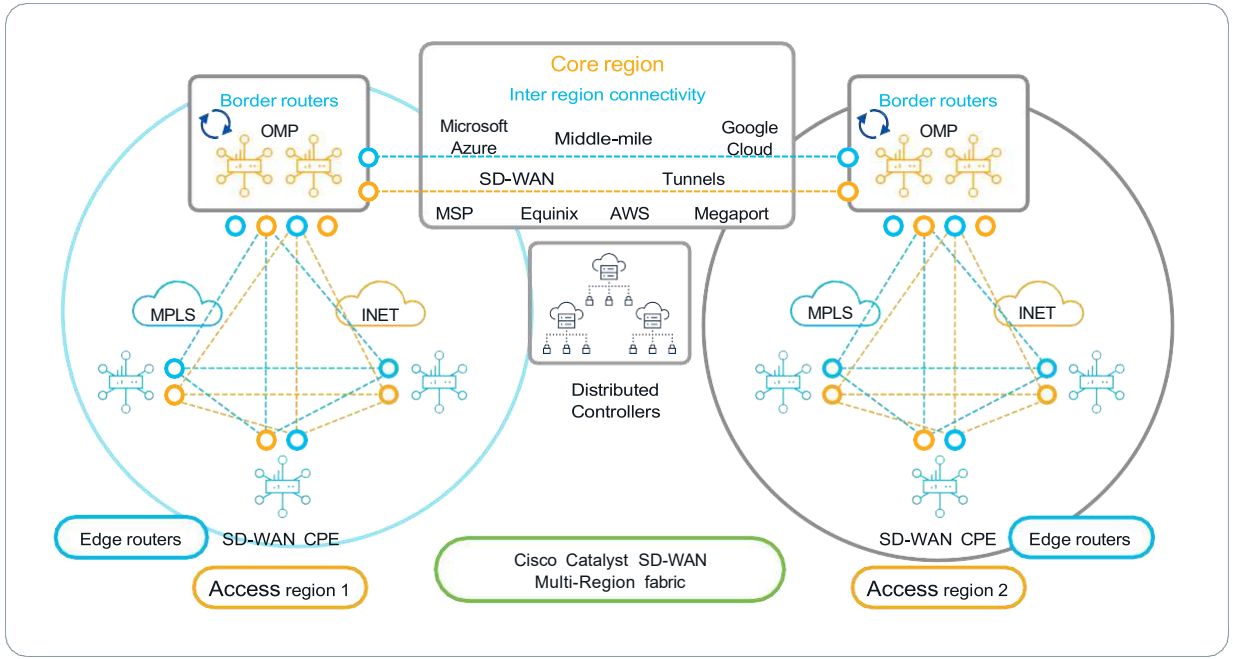
Zero-Touch Provisioning

- 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



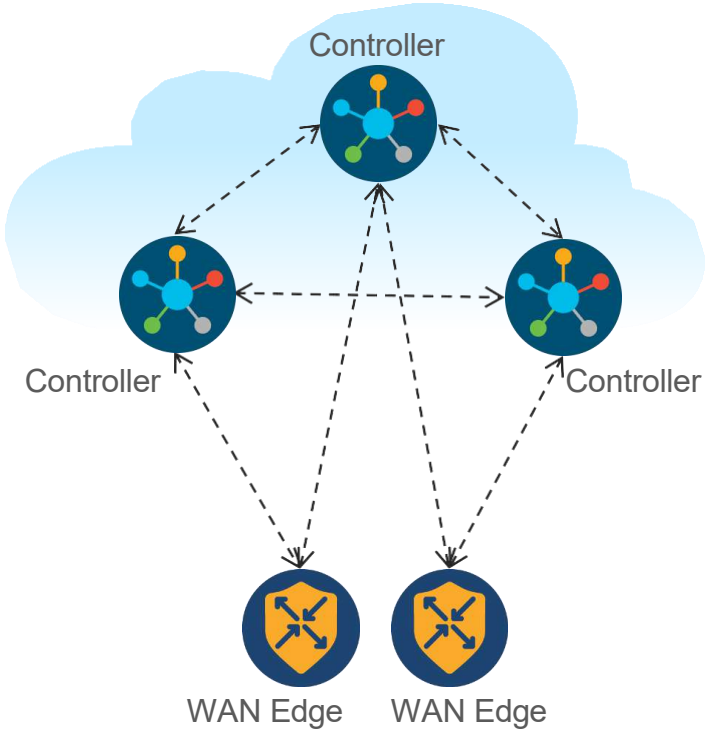
Cisco Catalyst SD-WAN Multi-Region Fabric

SD-WAN evolved for any middle-mile topology



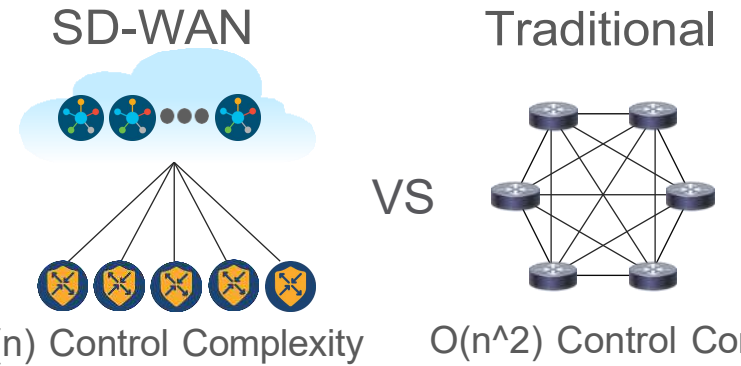
- Eliminate lengthy global network policies
- Automatic hop-by-hop inter-region routing
- Scalable design
- Simpler redundancy planning
- Flexible architecture to cater to dynamic network needs
- Operationally easier to deploy and manage

Overlay Management Protocol (OMP)

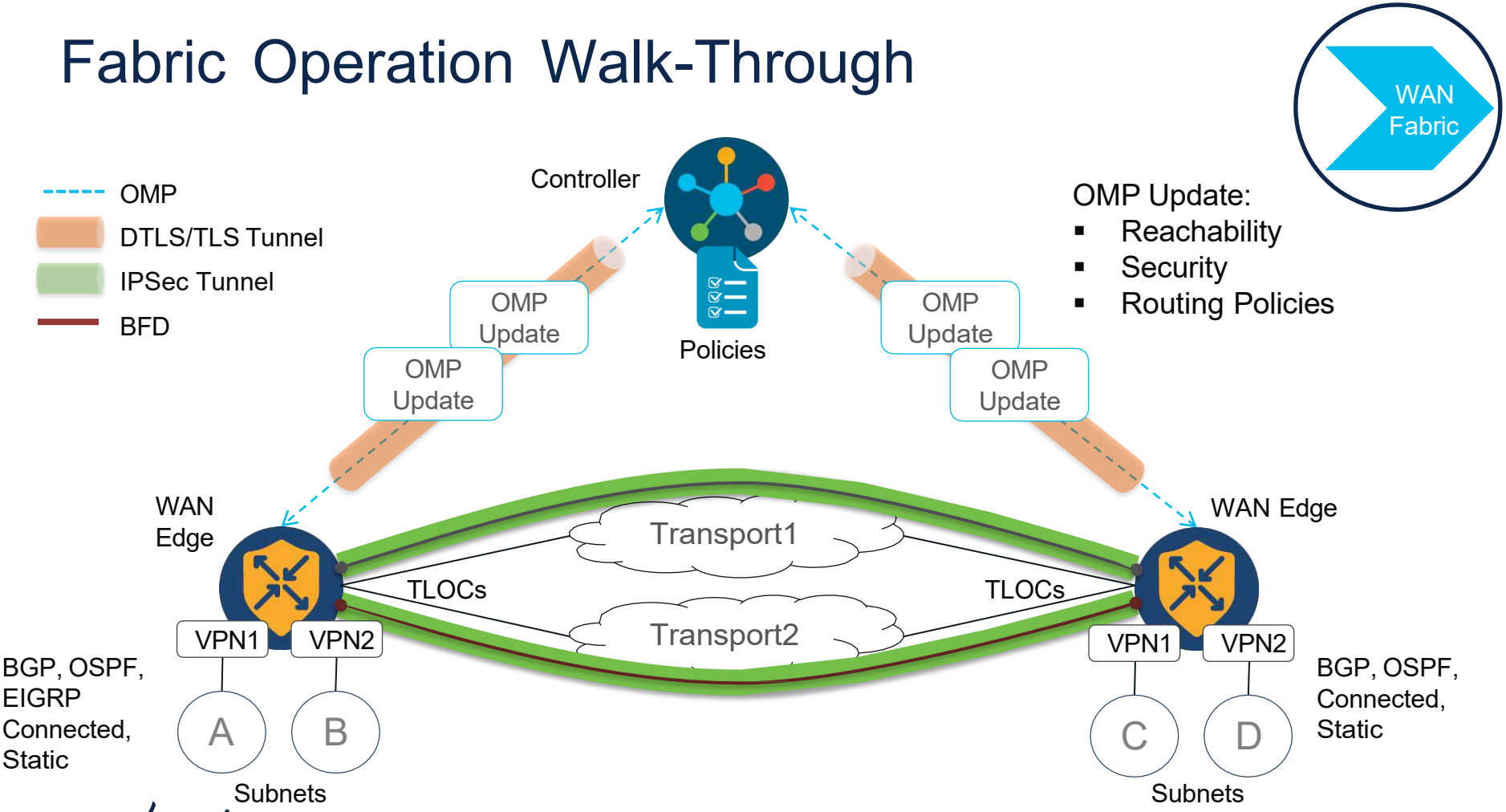


Note: WAN Edge routers need not connect to all Controllers

- 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



Fabric Operation Walk-Through

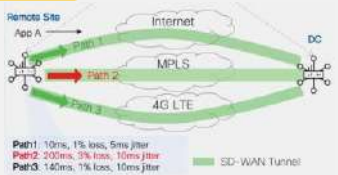


Application Experience

App Routing

Application Aware routing

- Detects brownout conditions in overlay path.
- SLA based traffic steering
- Automatic failover to secondary path if primary path fails.

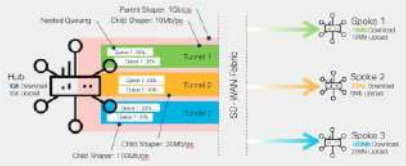


Packet Duplication

- Send duplicate packets over alternate path
- Mitigate packet loss for critical voice or video traffic
- Enhances Application quality of experience

Quality of Service (QOS)

- Manage and avoid network congestion
- Guaranteed Bandwidth
- Traffic queueing and shapin
- Prioritize critical application traffic over other traffic.



TCP optimization

- BBR2 Congestion control algorithm
- Window scaling
- Large Initial windows
- Selective acknowledgement
- Helps in reducing latency and increase throughput

Forward Error Correction

- Protects against packet loss
- Protocol agnostic (TCP/UDP)
- Enhances Application quality of experience

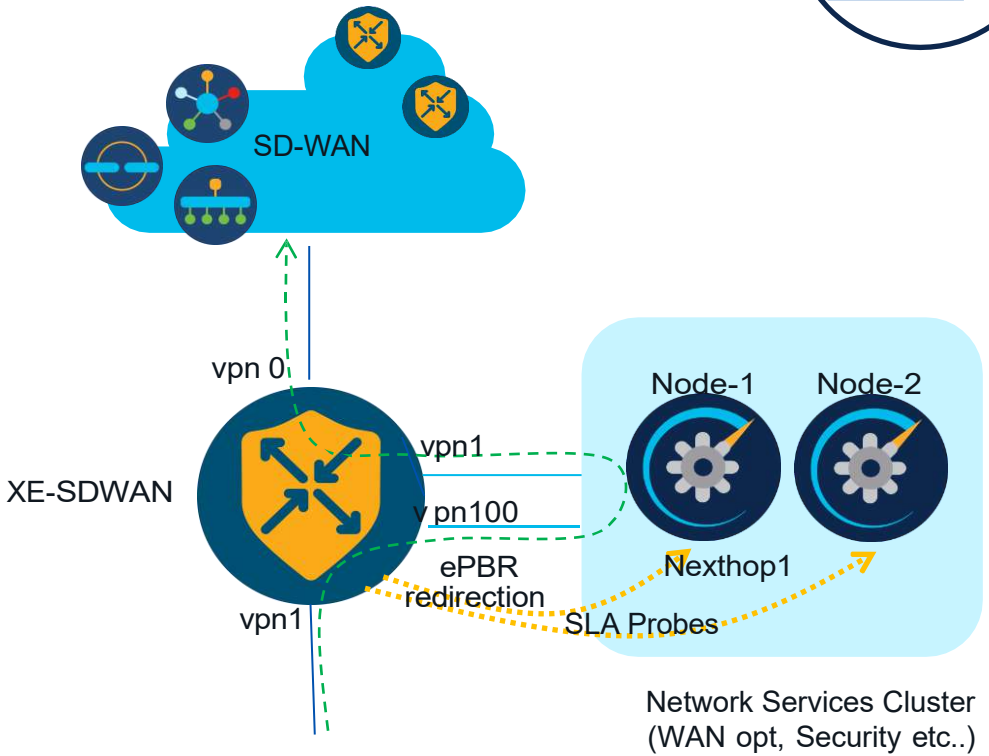
DRE, LZW

- Traffic optimization techniques
- Byte level caching & Data compression
- Protocol agnostic

Enhanced Policy Based Routing

App Routing

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



Application Experience

Key building blocks

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

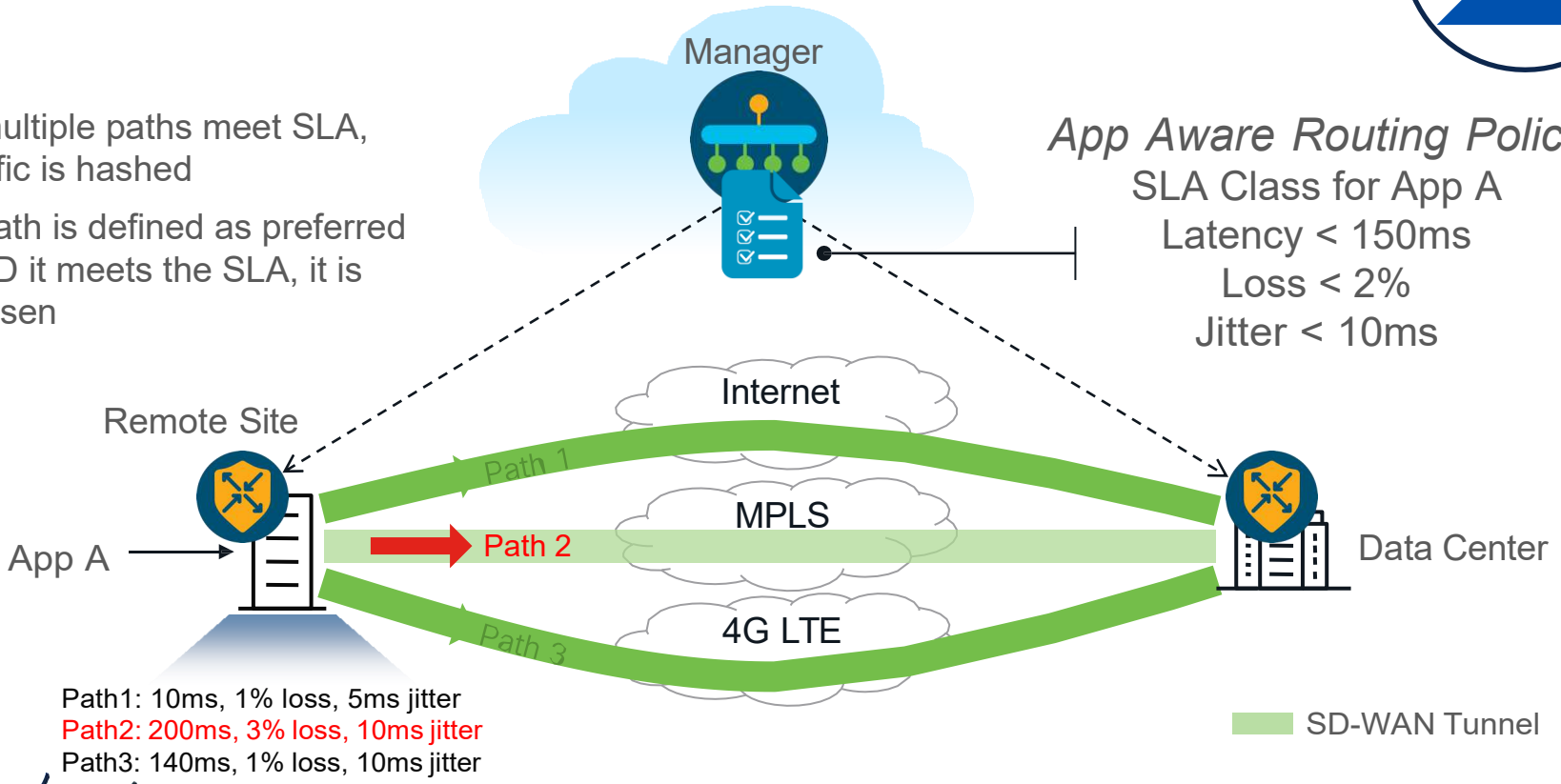
BBR – Bottleneck Bandwidth and Round-trip propagation time

Enhanced Application-Aware Routing

Improved Application Performance Experience (from mins to sec)

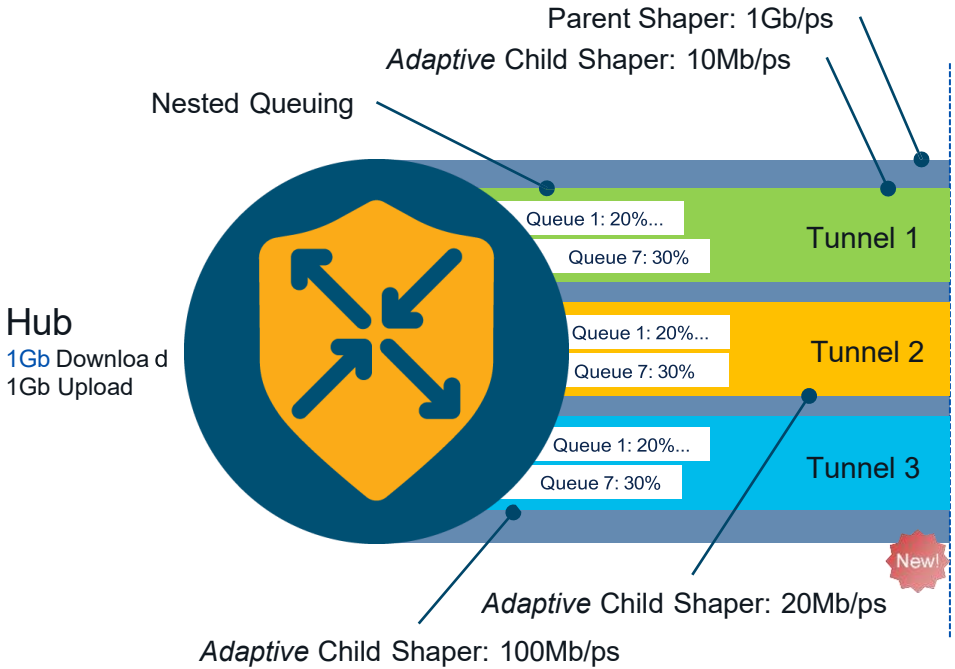
App Routing

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



Per-Tunnel QoS with Adaptive Shaping

App Routing



SD-WAN Fabric

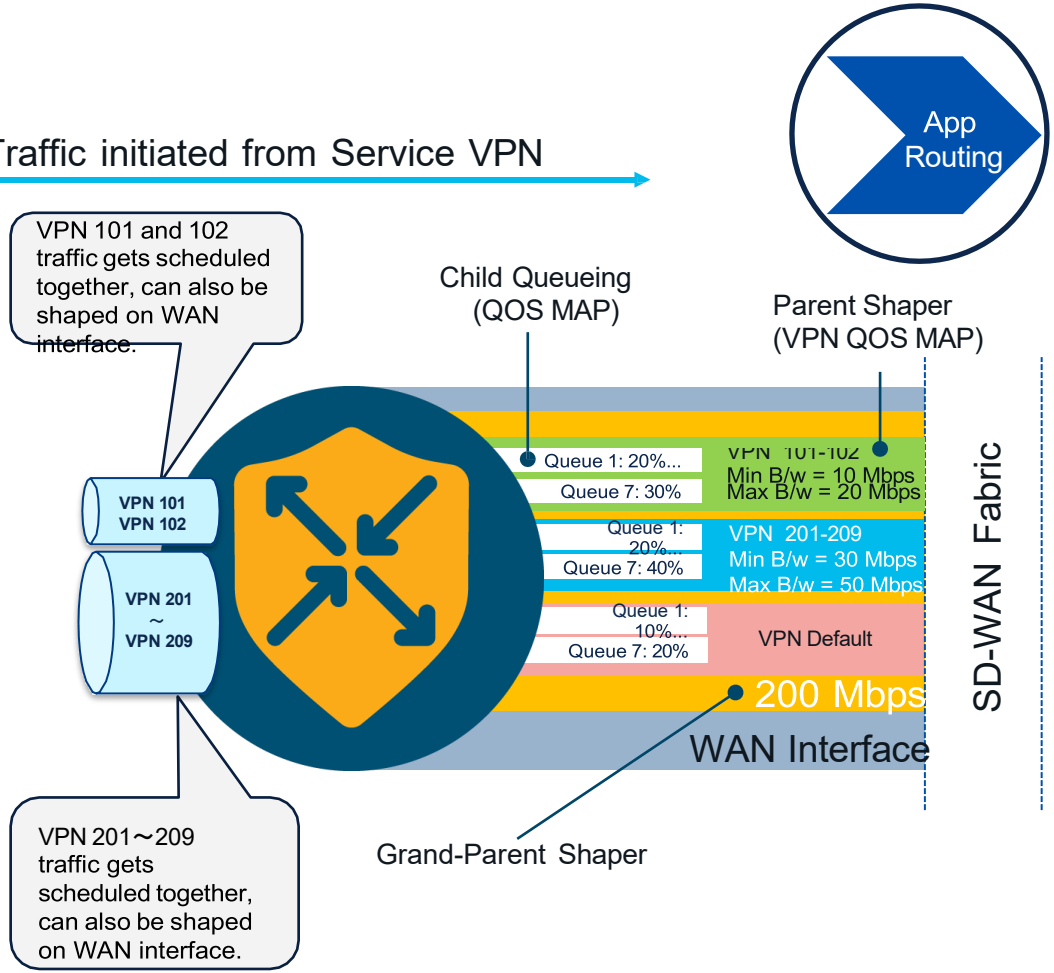
Spoke 1
10Mb Download
10Mb Upload

Spoke 2
20Mb Download
5Mb Upload

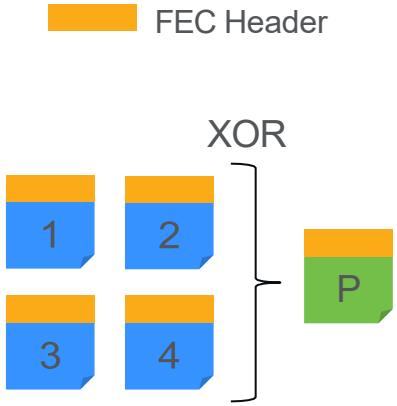
Spoke 3
100Mb Download
20Mb Upload

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

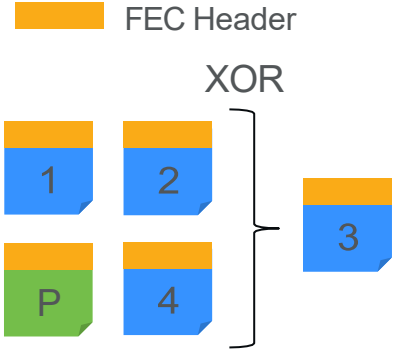


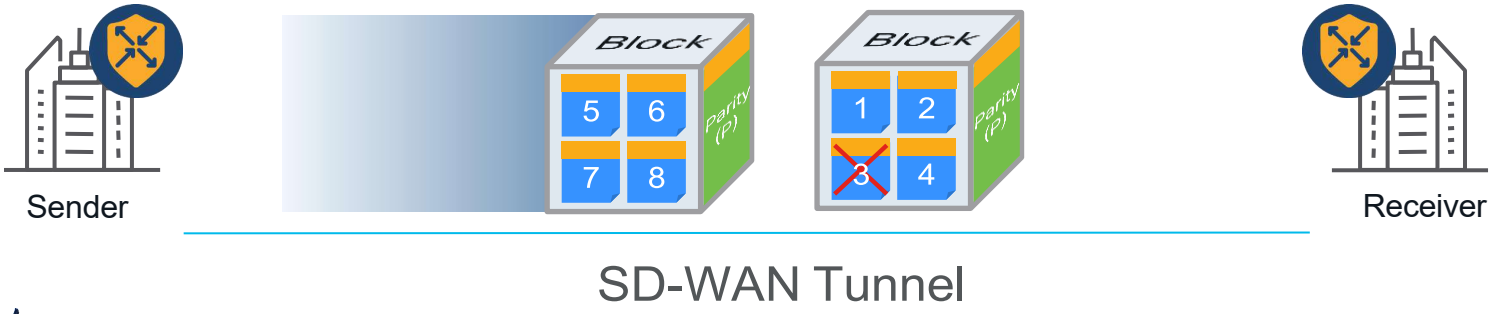
Forward Error Correction



Highlights:

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

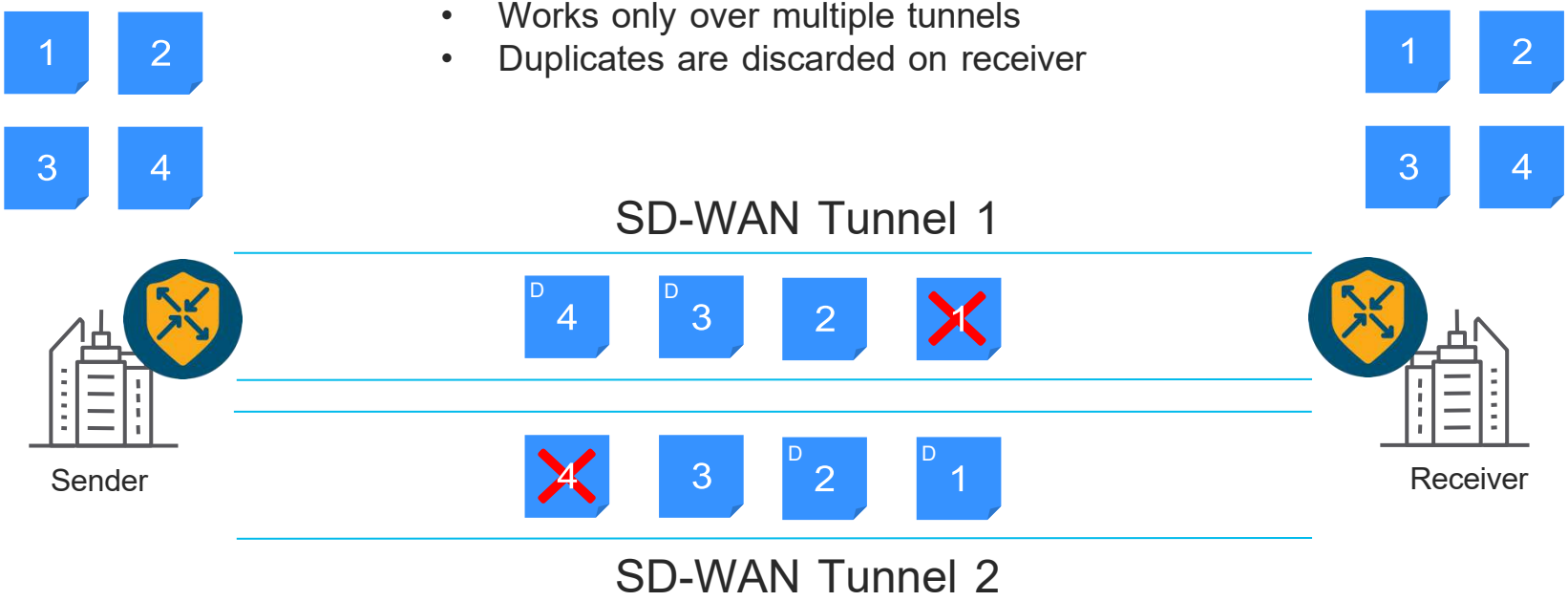




Packet Duplication

App Routing

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



Native Unified Communications in SD-WAN

App Routing

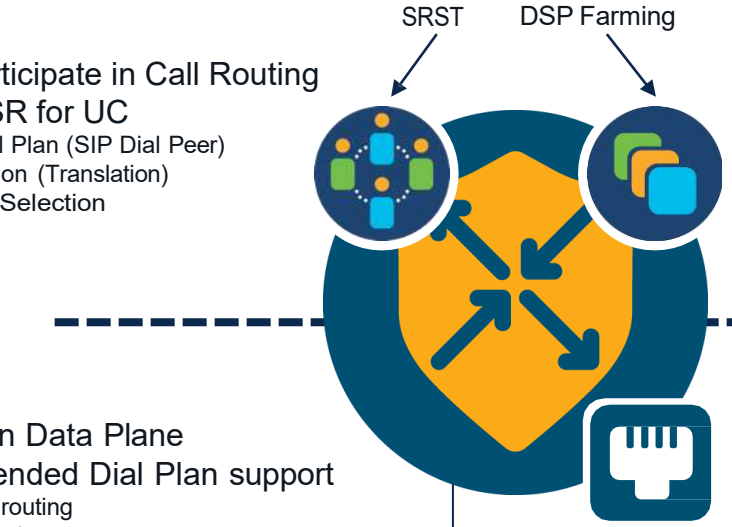
Manager/Controller

Does not participate in Call Routing
Provisions ISR for UC
- Distributed Dial Plan (SIP Dial Peer)
- Call Manipulation (Translation)
- Media/Codec Selection
- SRST

Call Control

Participates in Data Plane
Provides extended Dial Plan support
- Enterprise call routing
- Media Termination
- SIP only (CUBE is not currently supported)

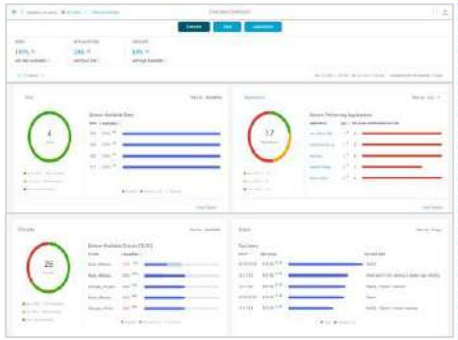
Does not invoke configuration change



Predictive Analytics & Underlay and Overlay visibility

Analytics

Visibility into Network & App Performance



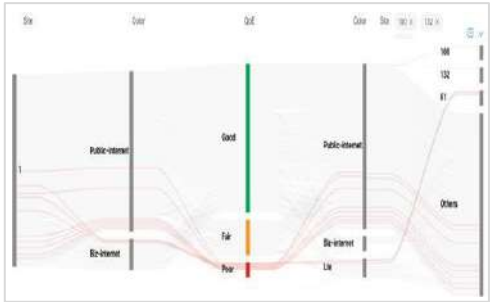
Application Experience

Scheduled Reports

Historical Trends & Daily/Weekly/Monthly Aggregates

Troubleshooting w/ Extensive Traffic Analysis

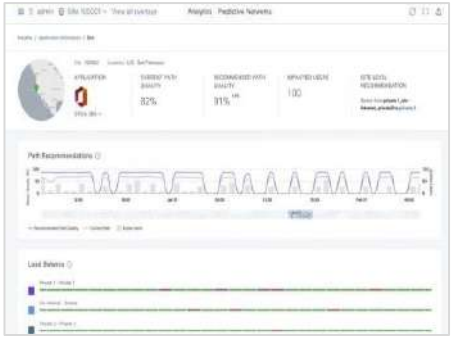
Traffic flow patterns



Underlay path tracing

App distribution across circuits

Adaptive & Predictive Networking



Predictive Path Recommendations

AIOps use-cases

SaaS Traffic Optimization

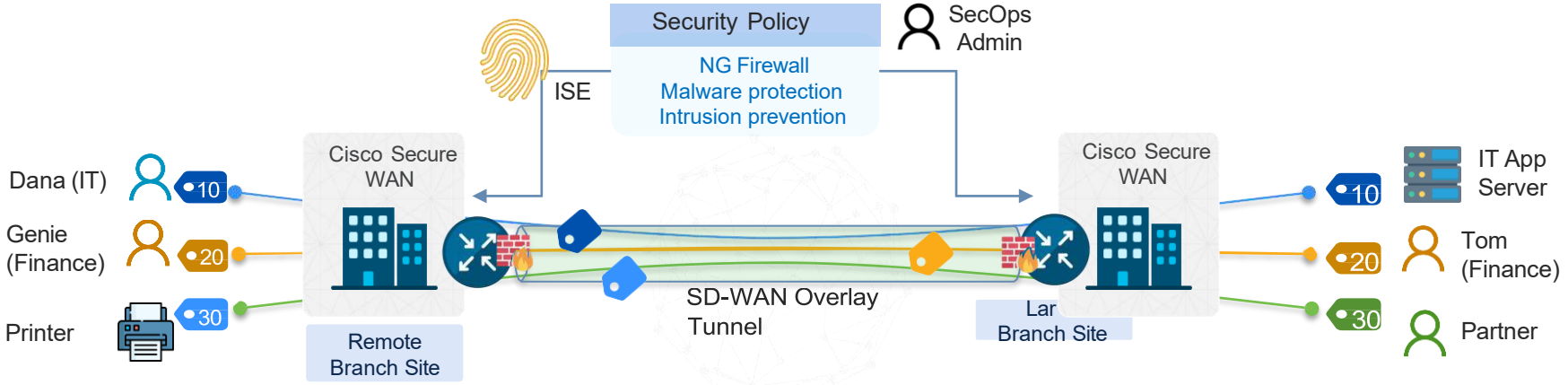
SD-WAN Analytics

Network Performance	Visibility into network KPIs – loss, latency, jitters, and bandwidth consumption across WAN
Application Insights	Multi-layer insights correlating application behavior (QoE) with the underlying network conditions
Granular Statistics	Site-level, VPN-level, and Device-level statistics; Top Talkers, Top Flows
Improved experience	Refreshed GUI for easy navigation; Secure login with multi-factor authentication (MFA)

Improved overall network visibility and insights

Secure Segmentation

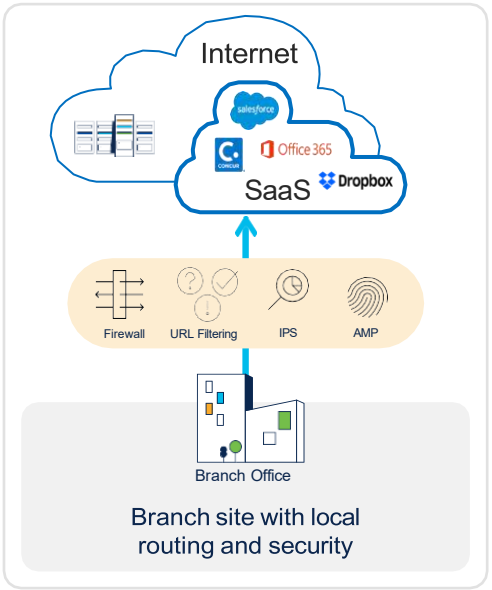
- Identity Firewall provides security policy for segmenting at the macro and micro level
- Macro segmentation at the VLAN/VRF level
- Context-aware policies with User/User-group or SGT to control policy within a VRF / VPN

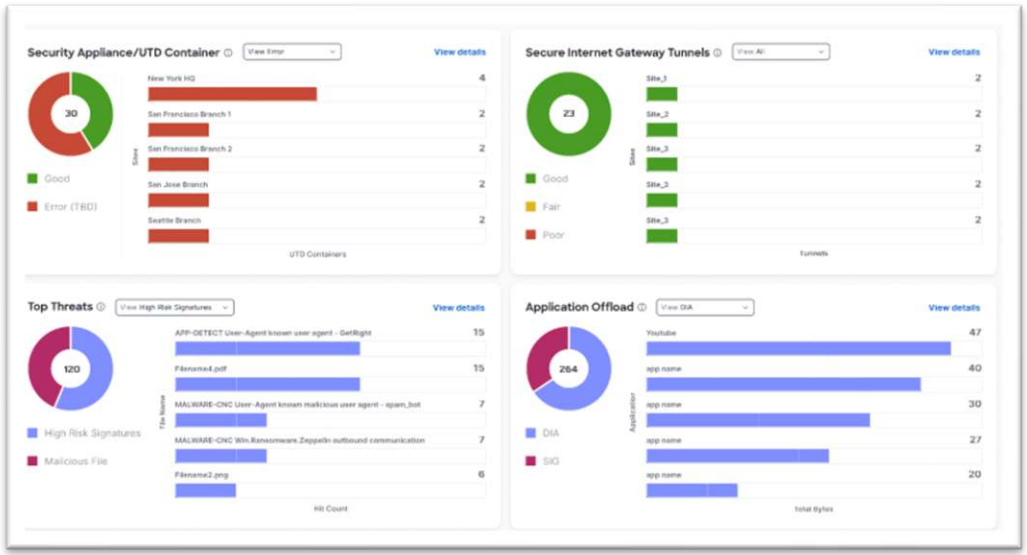


Source	Allow
IT	IT (Port: 443), Printer
Finance	Finance (Port: 443), Printer
Partner	IT (Port: 443), Printer

Security Policy

Advanced security





Next Gen Firewall

Guided Workflows

Unified Management

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 SDWAN Use Cases & Capabilities

Meraki MX Secure SDWAN Platform

Overview

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


Auto VPN


Intelligent Routing


Quality of Service (QoS)

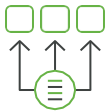

SD-WAN Analytics


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

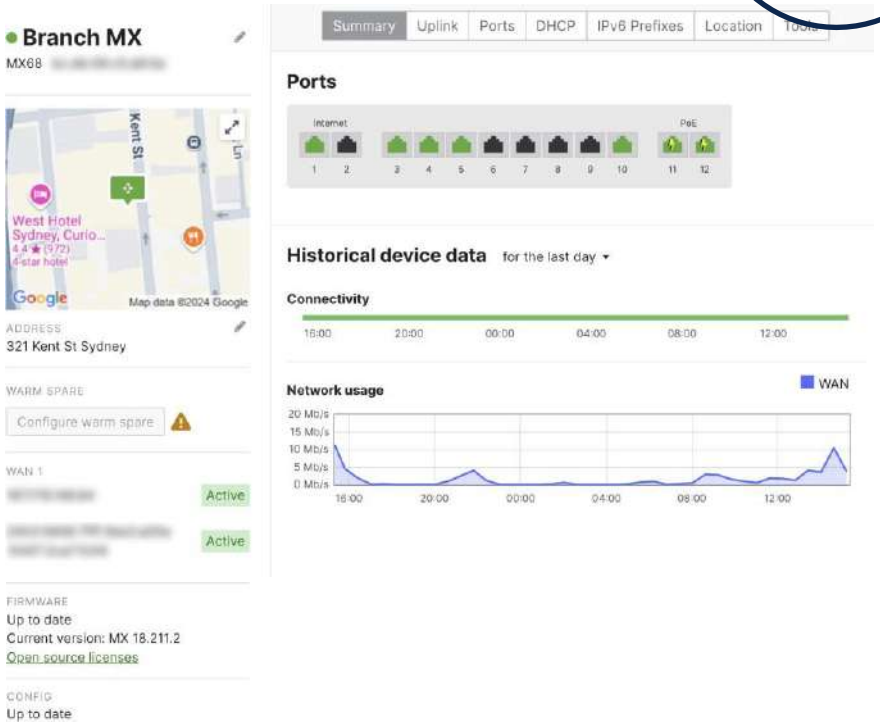

Native ThousandEyes Integration

Meraki Device-to-Cloud Connectivity

Site Connectivity

Zero Touch

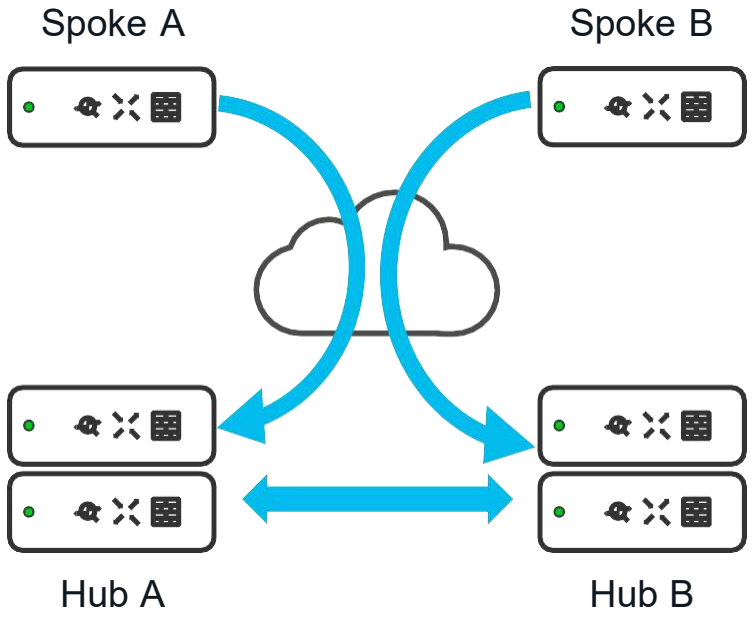
- Device requests IP address
- Check in starts
  - Initial WAN tests
  - FIPS 140 compliant connection over TLS to the cloud controller
  - All data is continually duplicated between two separate cloud controllers
  - Device serial # matched to Meraki Org
  - Download configuration
- Check in complete



Auto VPN – Out of the box

Site Connectivity

- 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



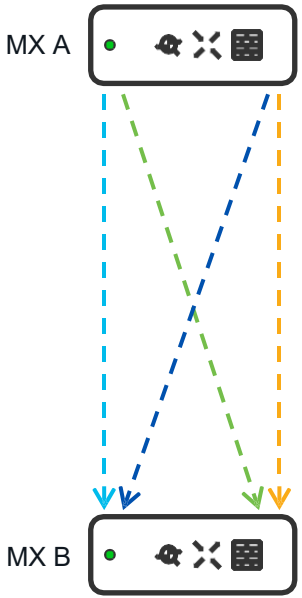
Probing

Measuring Performance

- 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 MOS

Measuring Performance

App Routing

1 second probing

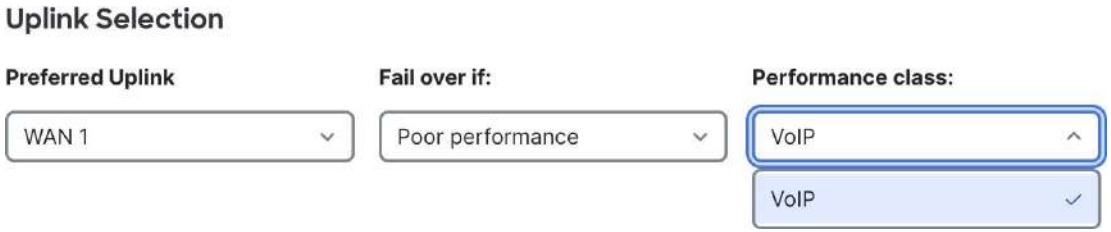
Latency, Jitter, Loss & MOS are the average of the last 30 seconds of data – at least 30 probes

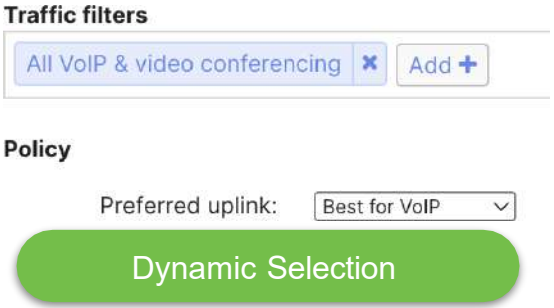
10 second probing

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

Performance Classes

Policy





Default

"Ensure connection is up"

- Also known as connection monitor failover
- If loss >60%, failover to an alternative transport network

Match Performance Class

"Ensure connection is good enough"

- Used when flows are to be associated with a preferred uplink
- Will use 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

Custom Performance Classes

Policy

- Custom combination of latency, jitter and loss
- Mapped to application or service level
- Maximum of 6 configurable

Custom performance classes

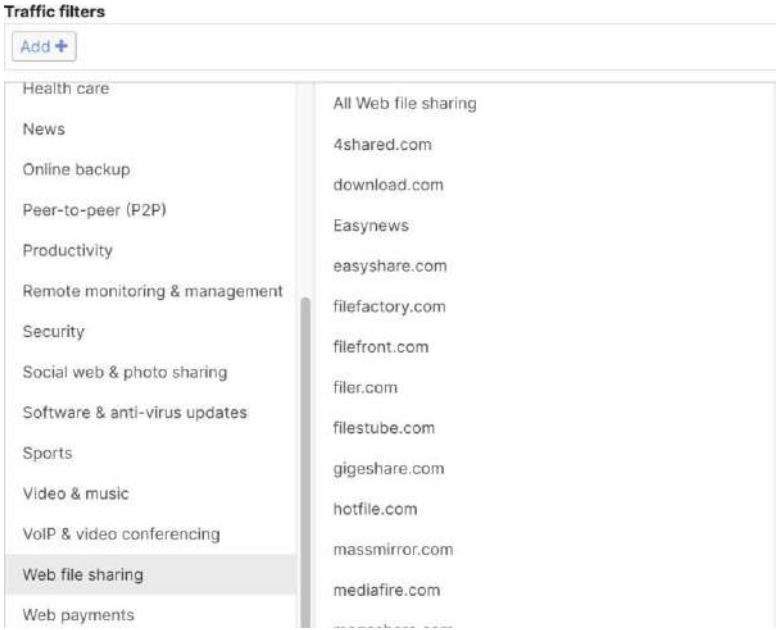
Name	Maximum latency (ms)	Maximum jitter (ms)	Maximum loss (%)	Actions
Bronze	200	50	8	✕
Silver	150	50	5	✕
Gold	100	40	3	✕
Platinum	50	20	1	✕
0356	60	30	1	✕

Create a new custom performance class...

Application
Policy

App Routing

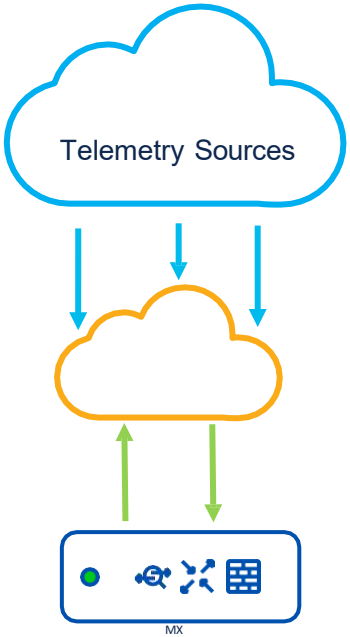
- Policy applied either via custom expressions (CIDR / Hostname) or Traffic Analysis engine NBAR2
- NBAR2 supports 1500 applications



SD-AVC Integration for NBAR

Security

App Routing



IP Feeds

Domain Feeds

Cloud Feeds

Dynamic Feeds

Custom Regex Feeds

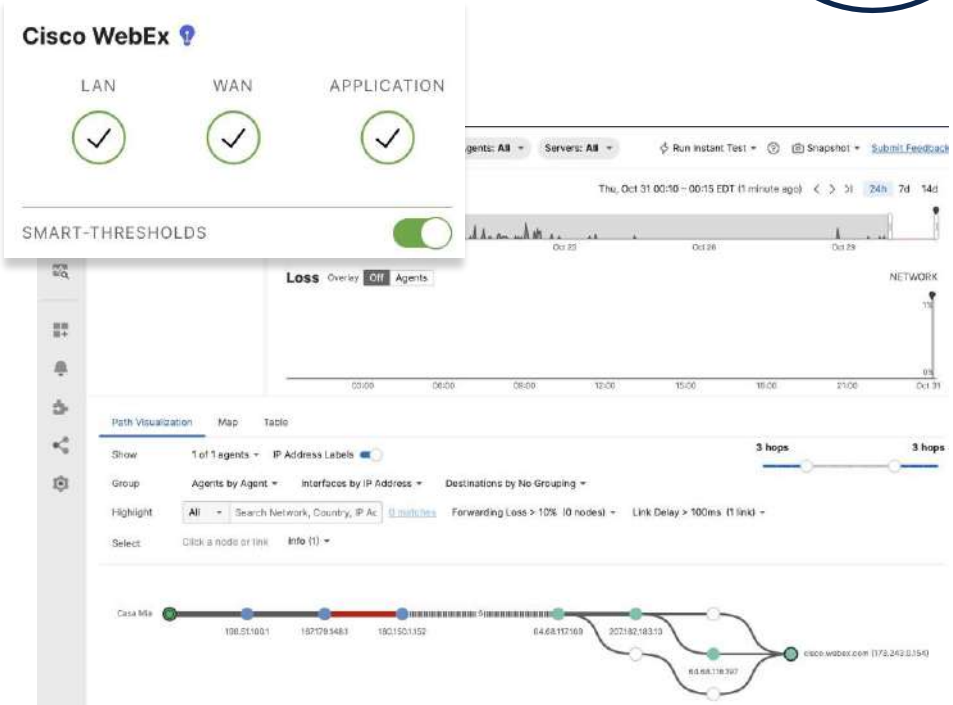
Up to 90%+ first packet classification with additional telemetry sources!

- 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

Thousand Eyes enriched Web App Health

Monitoring & Troubleshooting

- 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

Security

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

TLS Decryption

Stateful Firewall, Routing, NAT

Intrusion Prevention

Malware Protection & Sandboxing

URL Filtering & Categorization

Application Layer Detection

High Availability

VPN

Talos Intelligence

Geography based FW rules

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

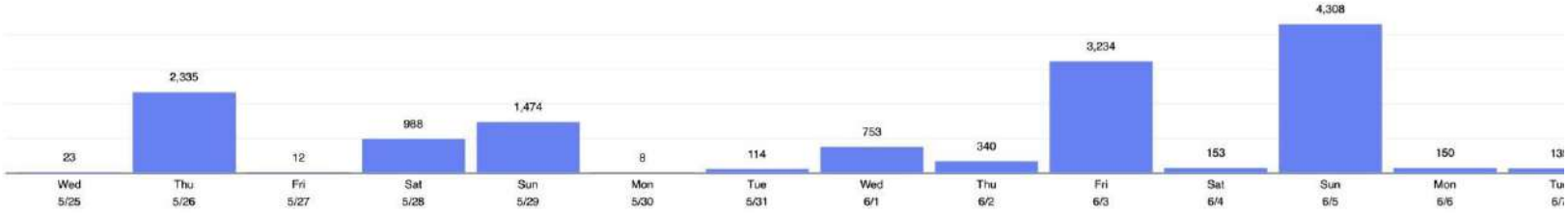
Insight

Organization

Search events | Filter | 14125 matching events | All times are in UTC

MX Summary | MX Events

Events over time



Most affected networks

Network	Events
Meraki San Francisco SFO12	5377
Meraki London - Finsbury LON11	4377
Meraki Sydney S	
Z - San Francisc	
Z - Cloud Interco	

Top sources of threats

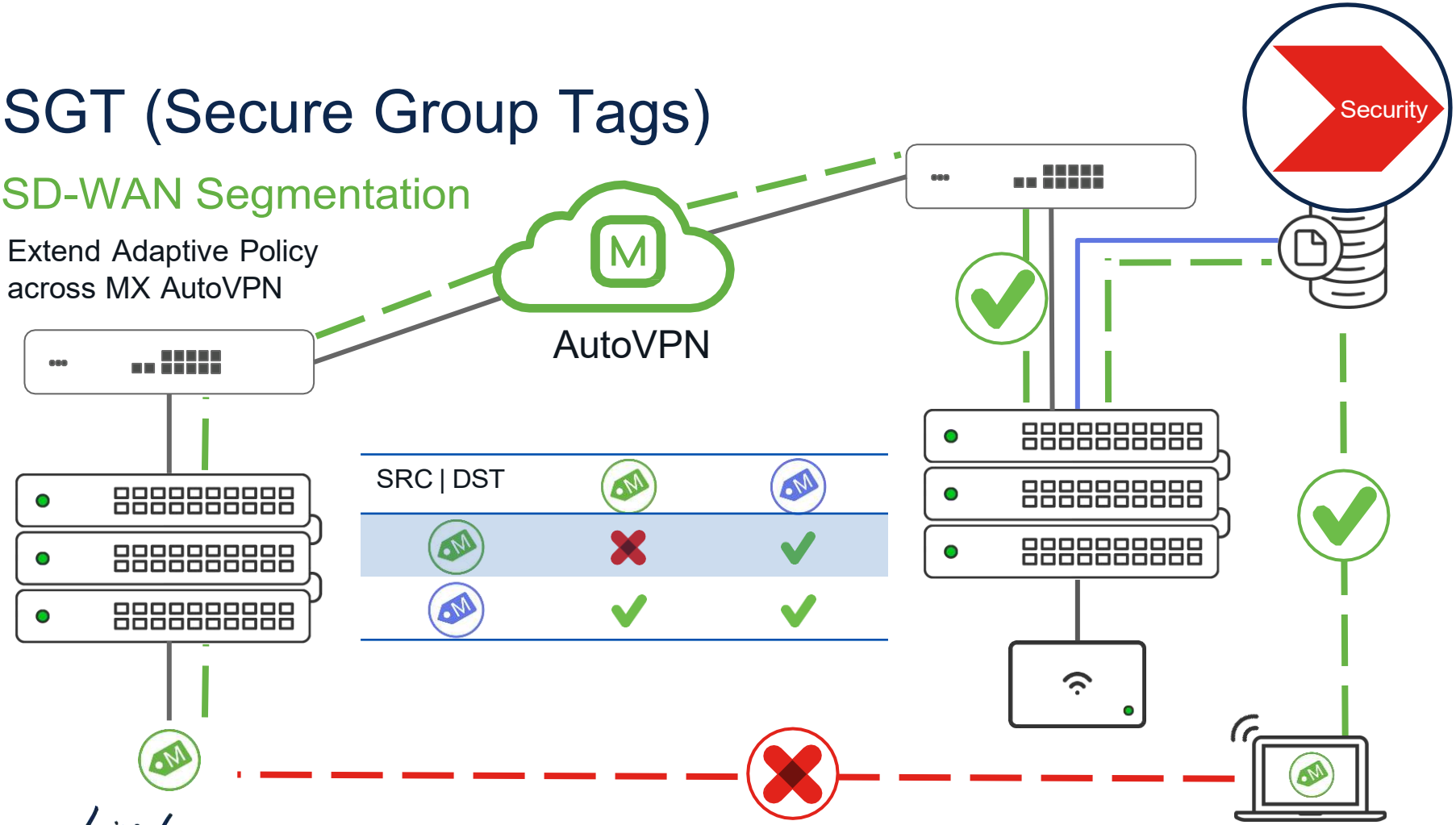
MX Summary | MX Events

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

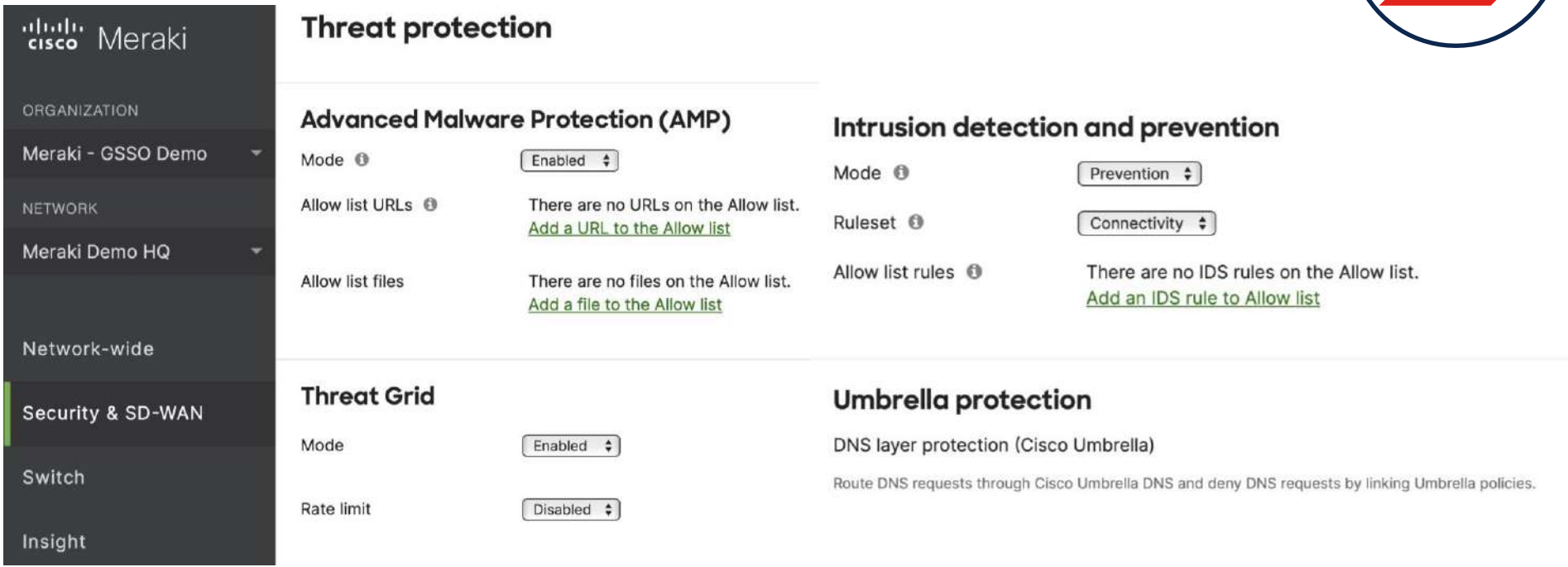
SGT (Secure Group Tags)

SD-WAN Segmentation

- Extend Adaptive Policy across MX AutoVPN



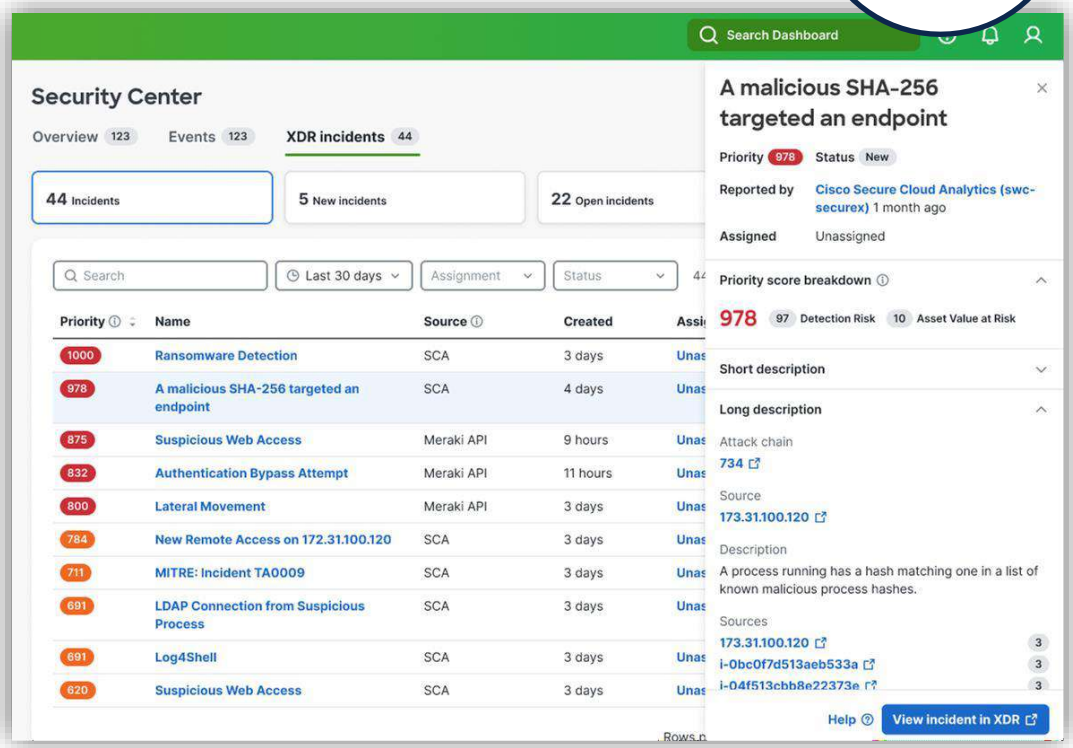
Meraki MX Threat & Security Policies



XDR Integration

Security

- Contextual Threat and Behavioural Analytics using Netflow data
- XDR uses AI/ML to analyse network data and detect malicious behaviour or early indicators of compromise
- Button-click integration to send telemetry from all your MX devices to XDR.
- Meraki is the sensor



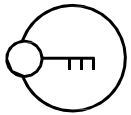
Meraki SD-WAN Secure Edge Solution

- ✓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

Overview

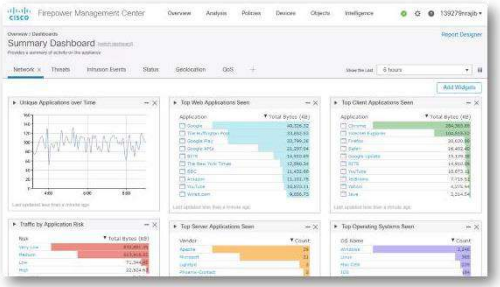

Secure Elastic Connectivity	WAN Optimization	Increased Usable Bandwidth	Direct Internet Access for Public cloud	Simplified Management
VT—based Hub & Spoke VPN	Dual ISP configuration	Increased support for load-balancing across multiple ISPs	SaaS Application detection (Fist Packet using AVC)	Data Interface 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

Managing Secure Firewall

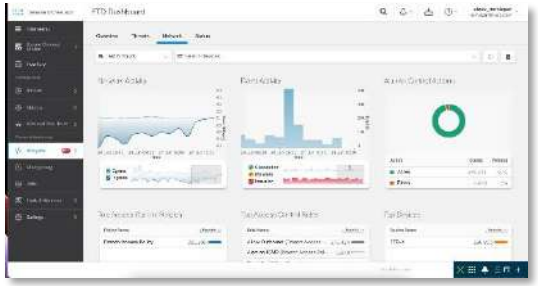
Flexibility of cloud or on-premises options

Overview

Firewall Management Center

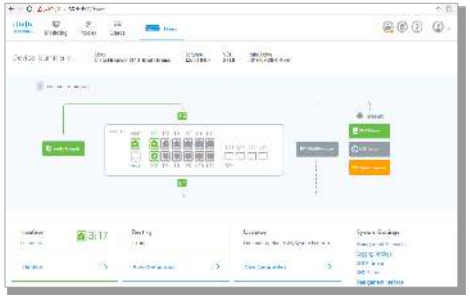


On-premises manager



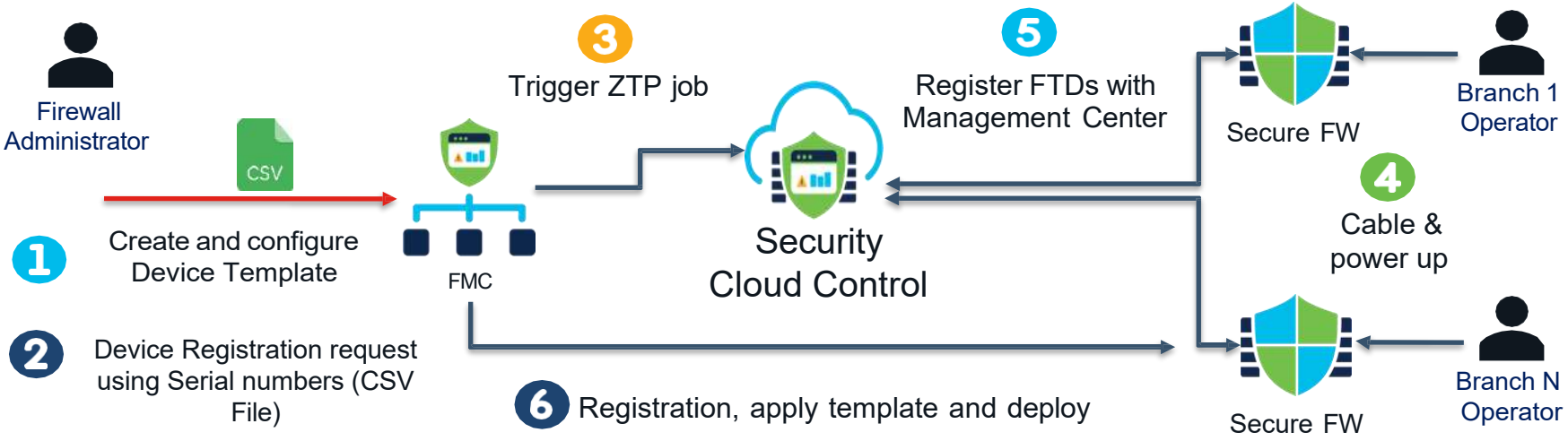
Cloud-delivered via Security Cloud Control

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 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

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: [redacted].9.20
       Destination IP address: [redacted].7.10
       Vaccess cloned from template 101
       Mode: ipsec ipv4     IPsec profile: FMC_IPSEC_PROFILE_2
       IPsec MTU Overhead : 55
```

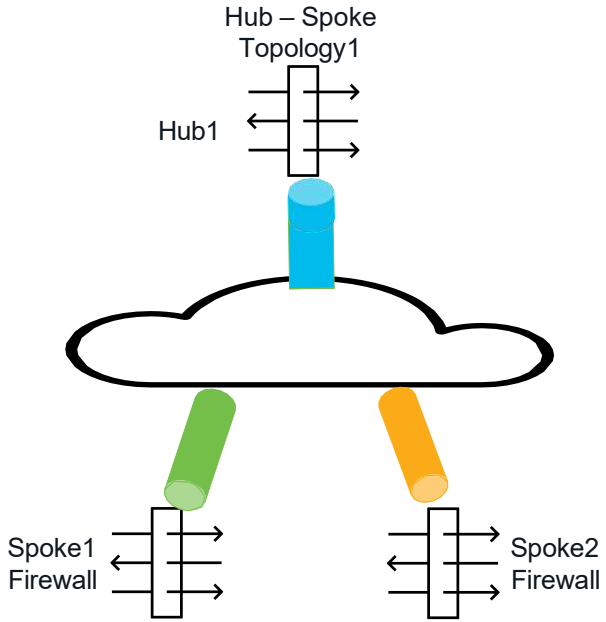
- Dynamic Virtual Tunnel Interfaces are introduced in FTD 7.3
- DVTI uses a virtual template for dynamic instantiation and management
- VPN Sessions using DVTIs only support IKEv2

Branch to Hub Communication

Why Dynamic Virtual Tunnel Interface (DVTI) ?

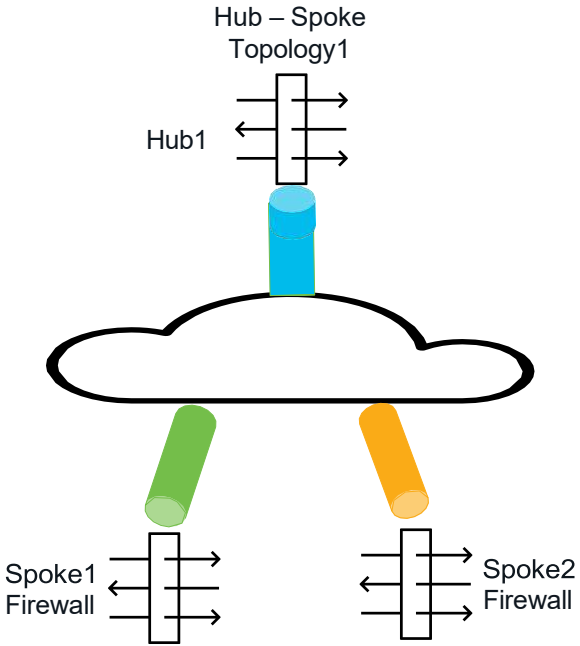
WAN Fabric

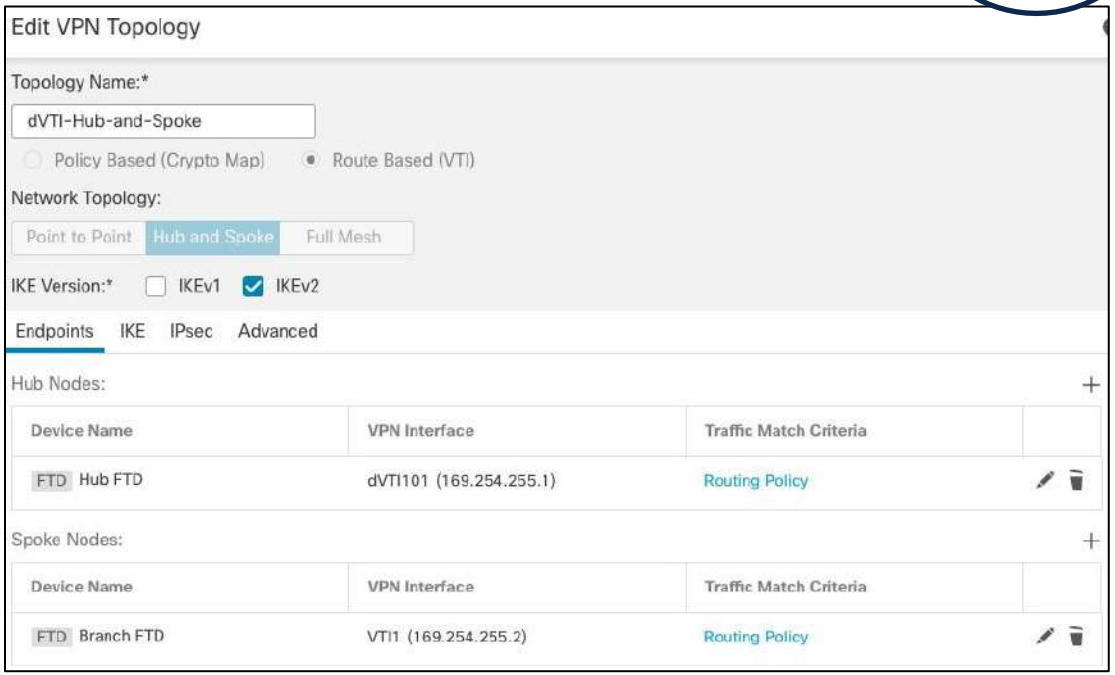
- High-scale, route-based VPN deployments
- No additional Hub configuration while adding new spokes
- No configuration change on Hub when the spoke's DHCP IP address changes



Hub and Spoke design using DVTI + SVTI

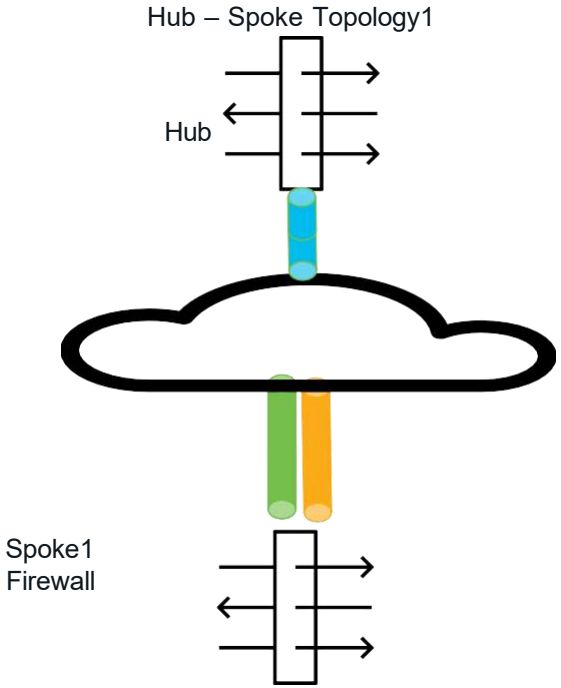
Single Hub Topology





Single Hub Topology

Spoke with Dual WAN



Branch FTD

Cisco Firepower Threat Defense for VMware

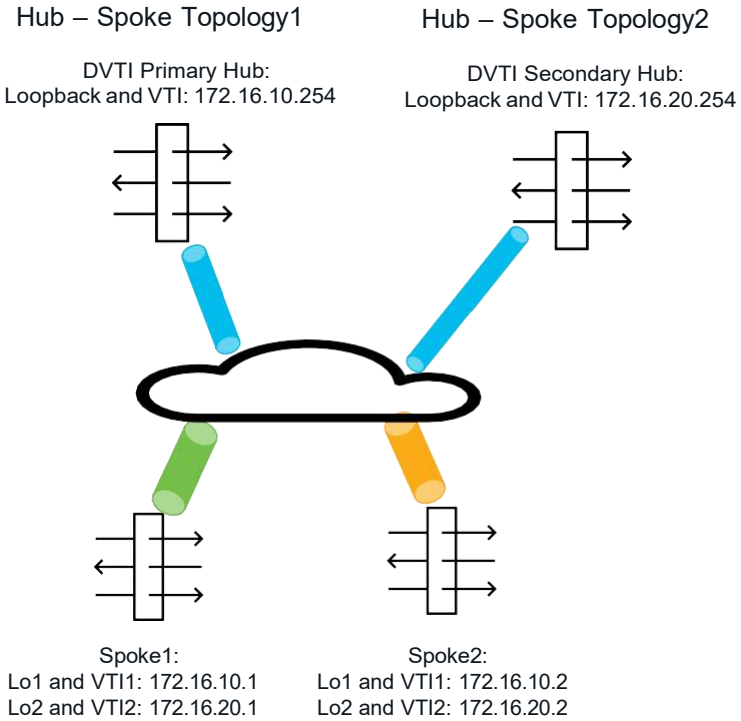
Device | Routing | Interfaces | Inline Sets | DHCP | VTEP

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

WAN Fabric

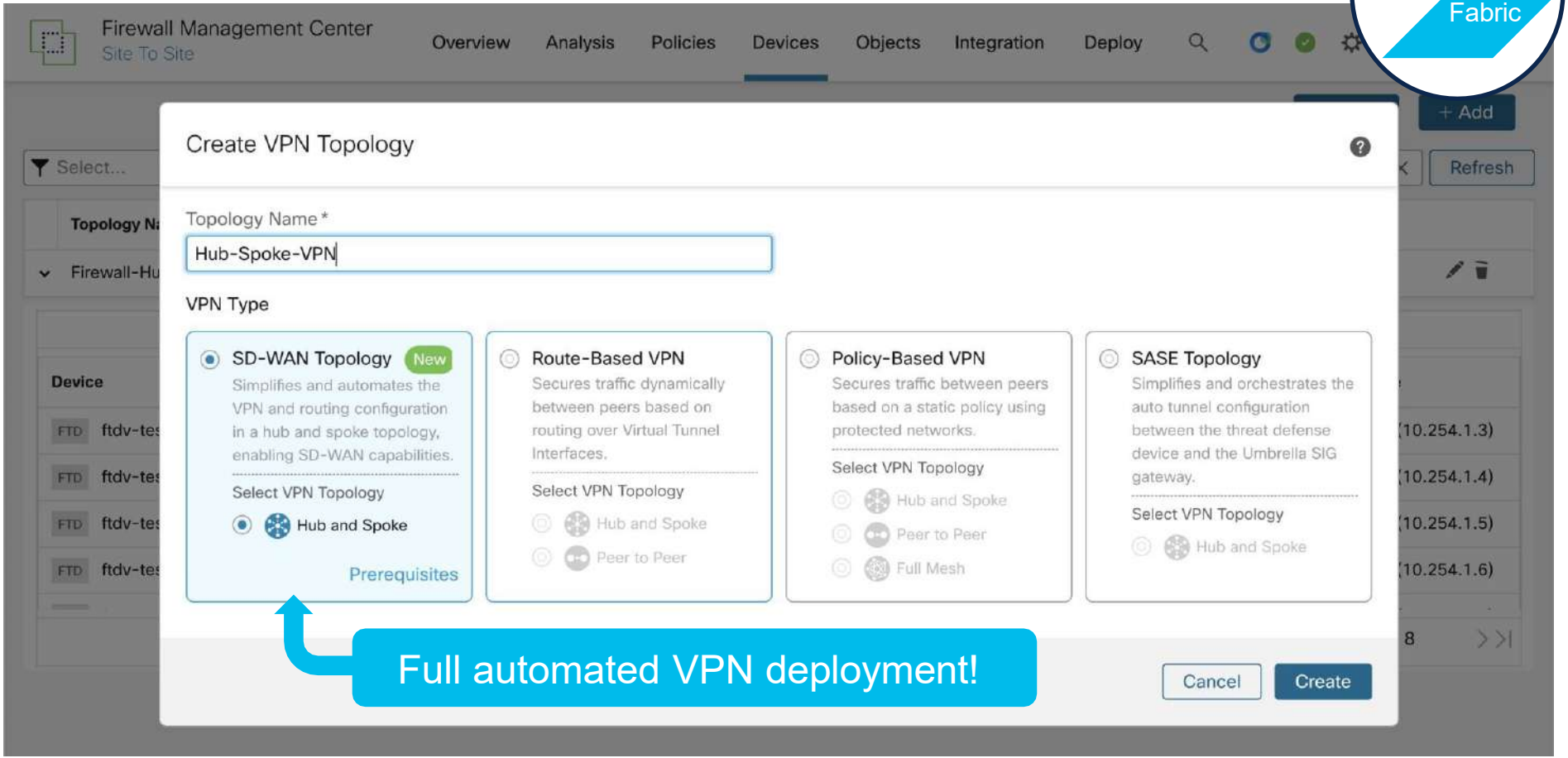
Dual Hub Topology



- 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

VPN Fabric



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 SDWAN 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** 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**

Secure Firewall 7.6 Topology Wizard

4 **SD-WAN Settings**

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

Enable BGP on the VPN overlay topology

Autonomous System Number*

65100

Community tag for local routes*

2112

Redistribute Connected Interfaces

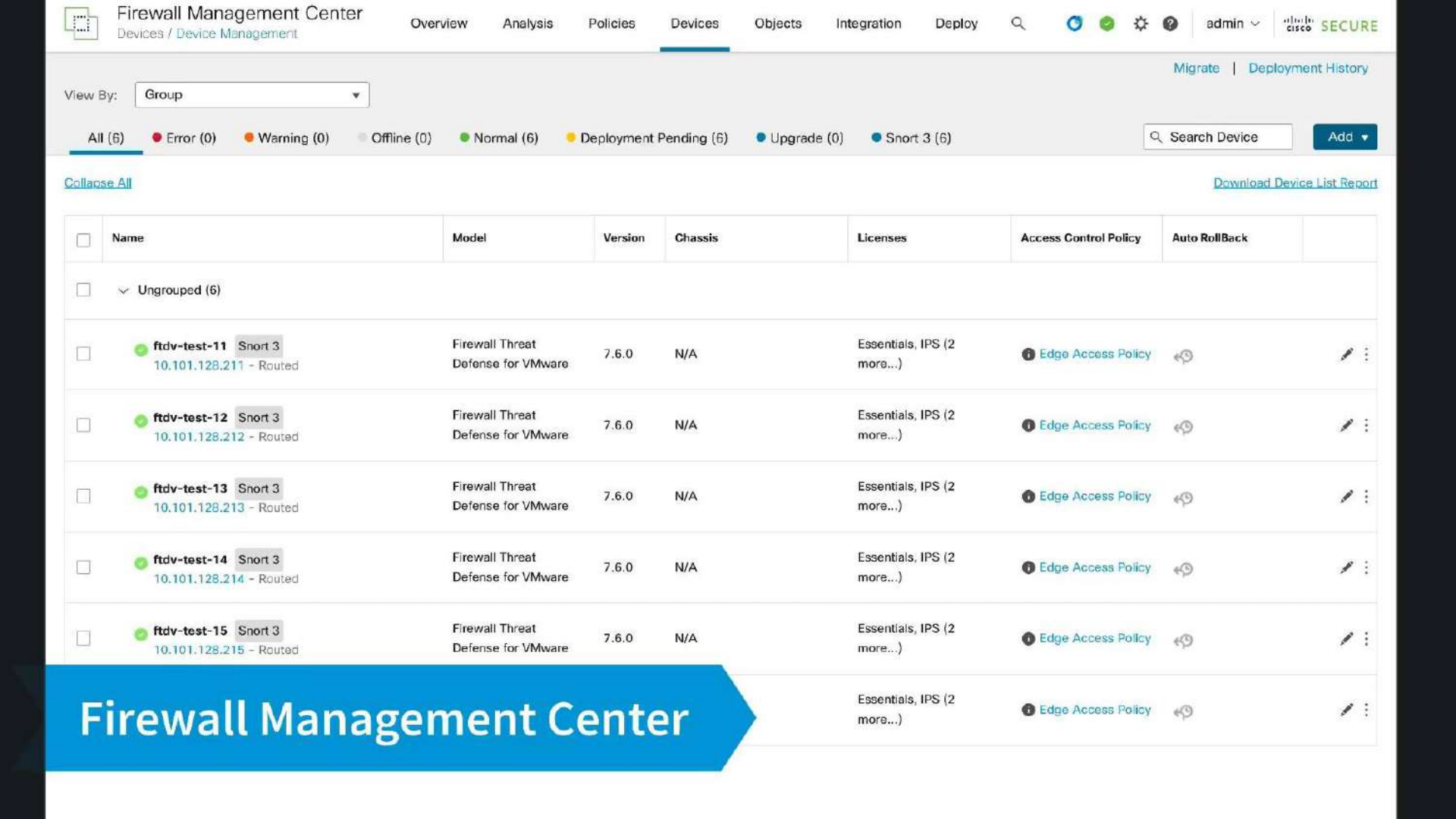
inside-interfaces

Secondary Hub is in different Autonomous System

Enable Multiple Paths for BGP

Allows multiple BGP routes to be used at the same time to reach the same destination. Enables BGP to load-balance traffic across multiple links.

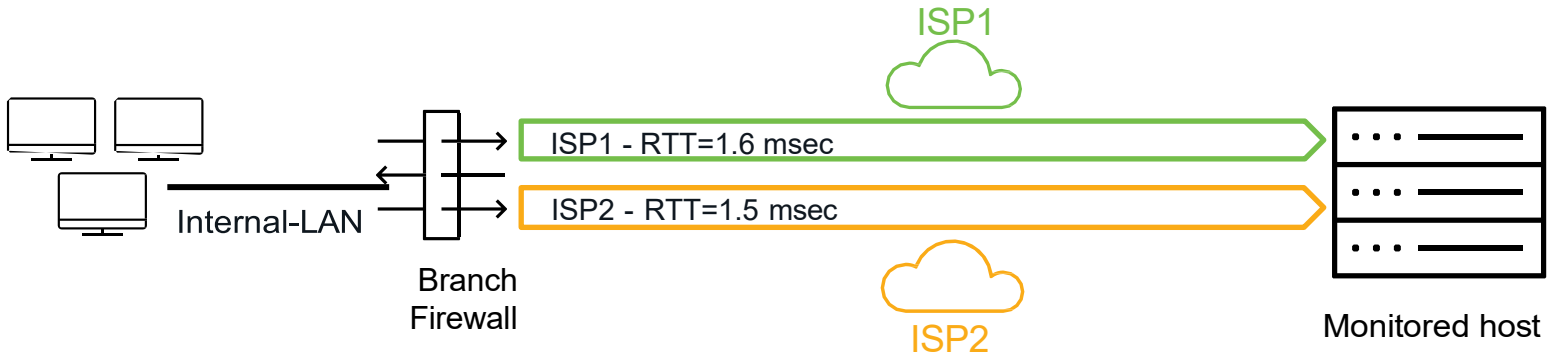
- Automated iBGP configuration
- Auto-distribution of connected routes
- Community TAG support to tag routes


Firewall Management Center
Devices / Device Management
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Migrate | Deployment History
View By: Group
All (6)
Error (0)
Warning (0)
Offline (0)
Normal (6)
Deployment Pending (6)
Upgrade (0)
Snort 3 (6)
Search Device
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

App Routing

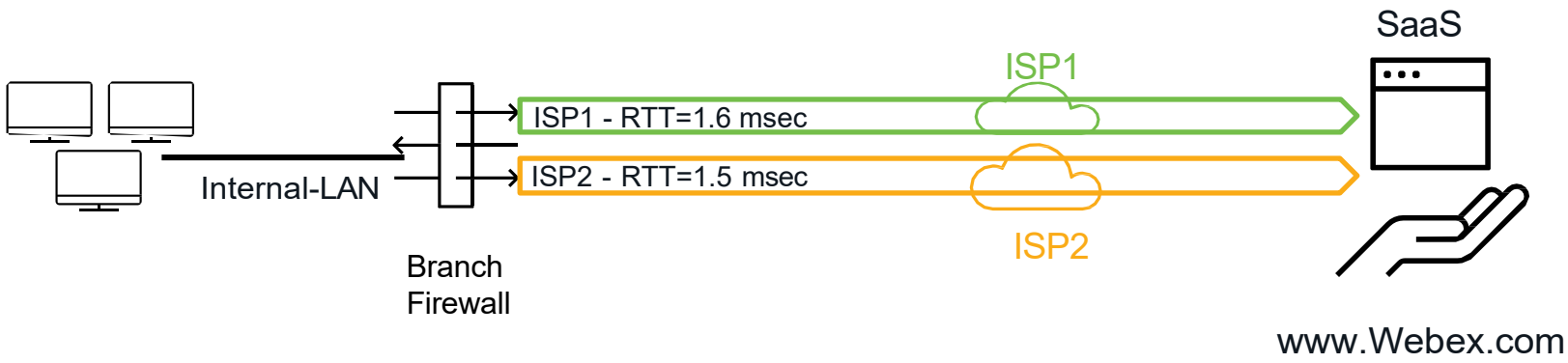
- PBR with Path Monitoring steers traffic based on dynamically monitored interface statistics such as RTT, Jitter, MOS and packet loss
  - These metrics are collected dynamically using ICMP/HTTP Probe messages



HTTP Path Monitoring

App Routing

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

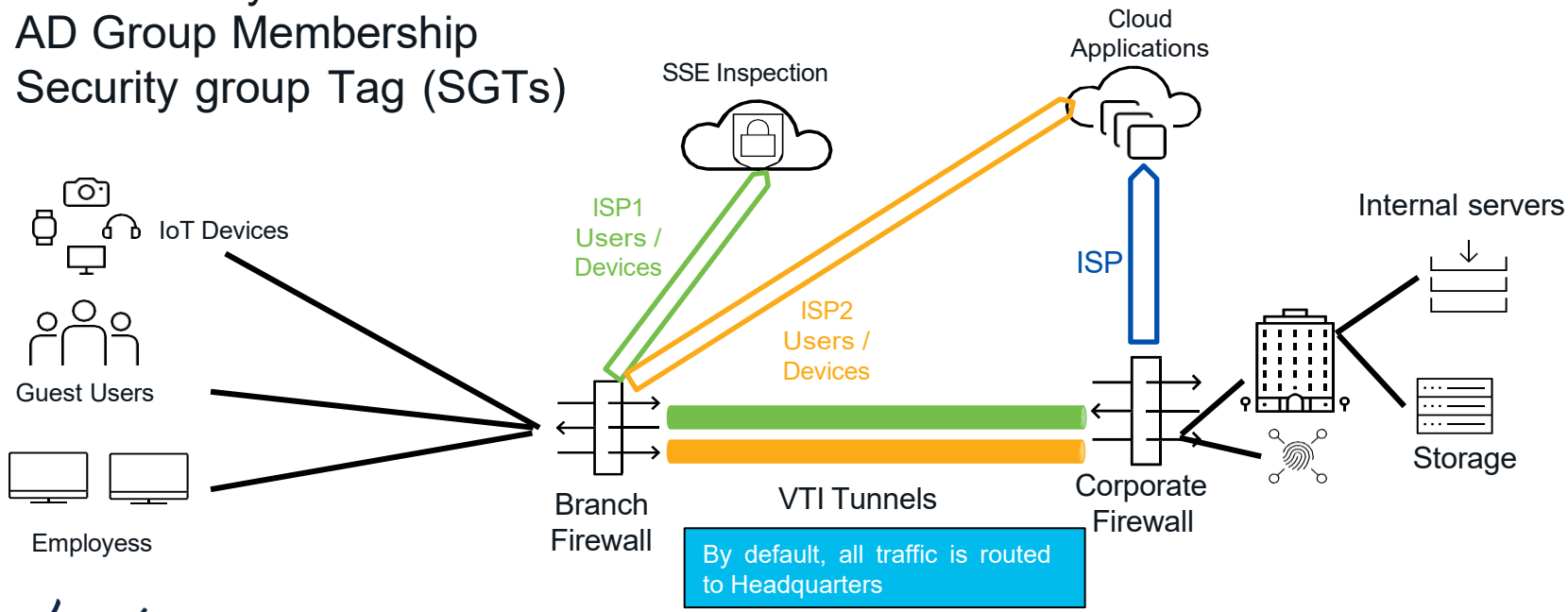


PBR with User Identity and SGT

App Routing

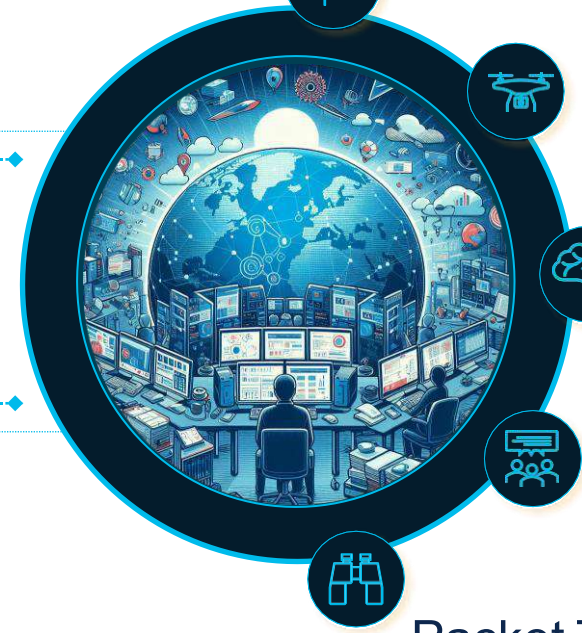
Additional attributes can be leveraged in the PBR policy:

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



S2S VPN – Monitoring & Insights

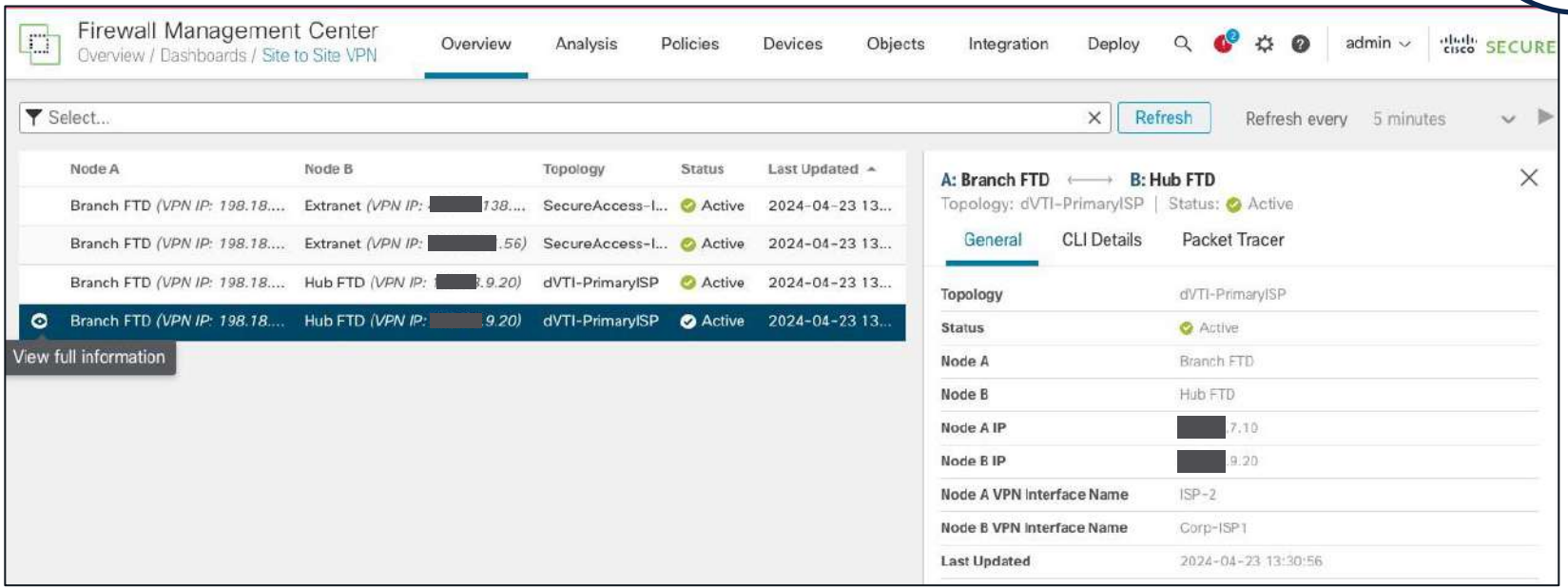
Site to Site VPN Monitoring



- Monitor VPN Tunnel Status
- Unified Event Viewer to analyze VPN Traffic flow
- Identify Suspicious activity
- Optimize Bandwidth allocation
- Packet Tracer for troubleshooting

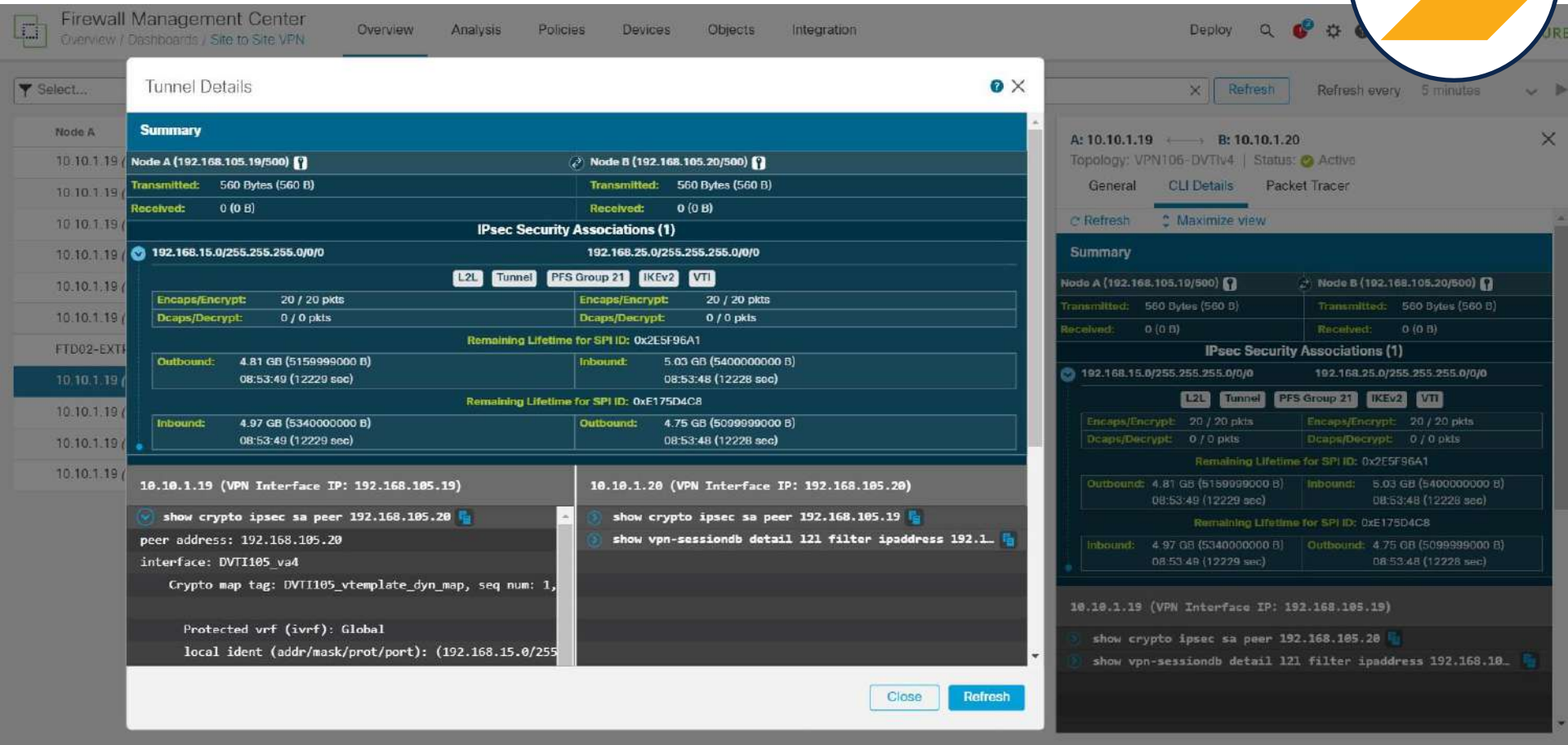
Site to Site VPN Dashboard

Overview



Site to Site Monitoring (7.4+)

Analytics

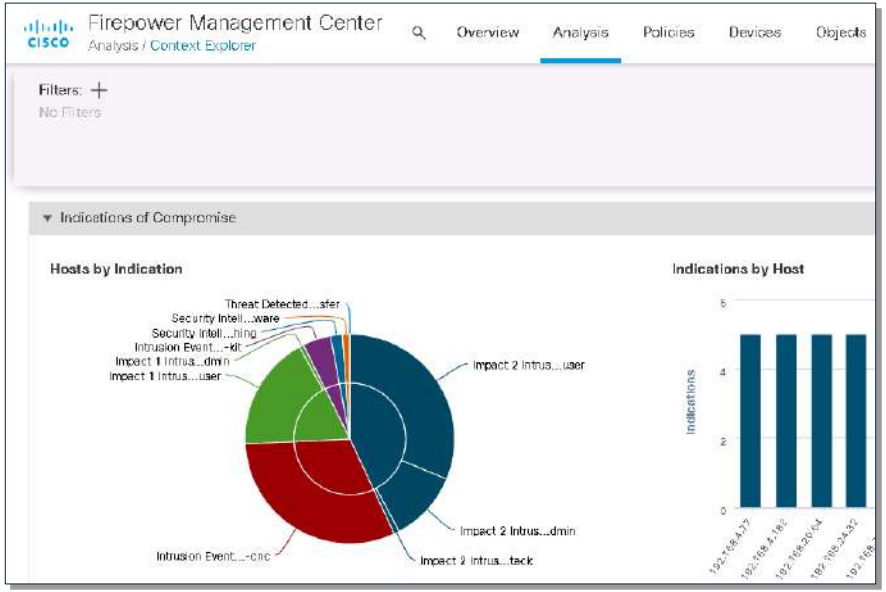


Best-in-class Branch Security

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

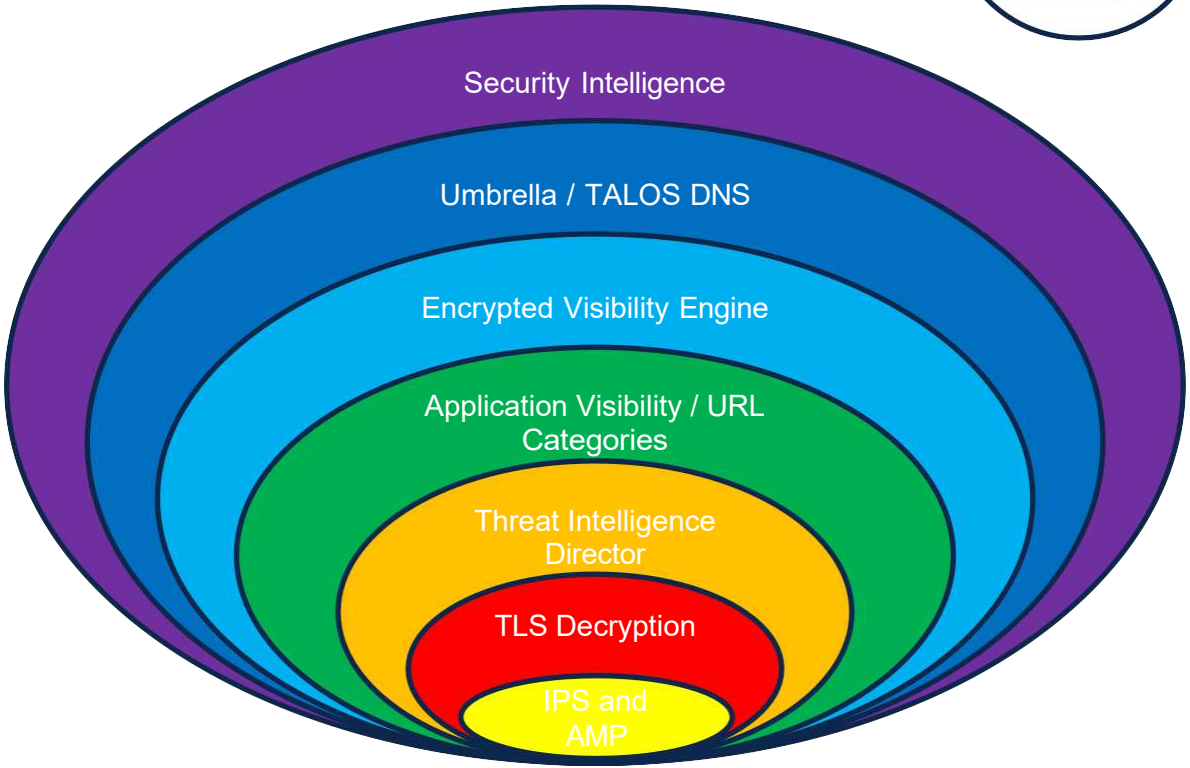
Security

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



Encrypted Visibility Engine
ML-Powered Snort IPS

- EVE is a new player in the security features team
- Sifts out malware threats with minimal effort
- EVE reduce pressure on more resource-heavy functions
- It brings the best value when used as yet another layer of protection



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)

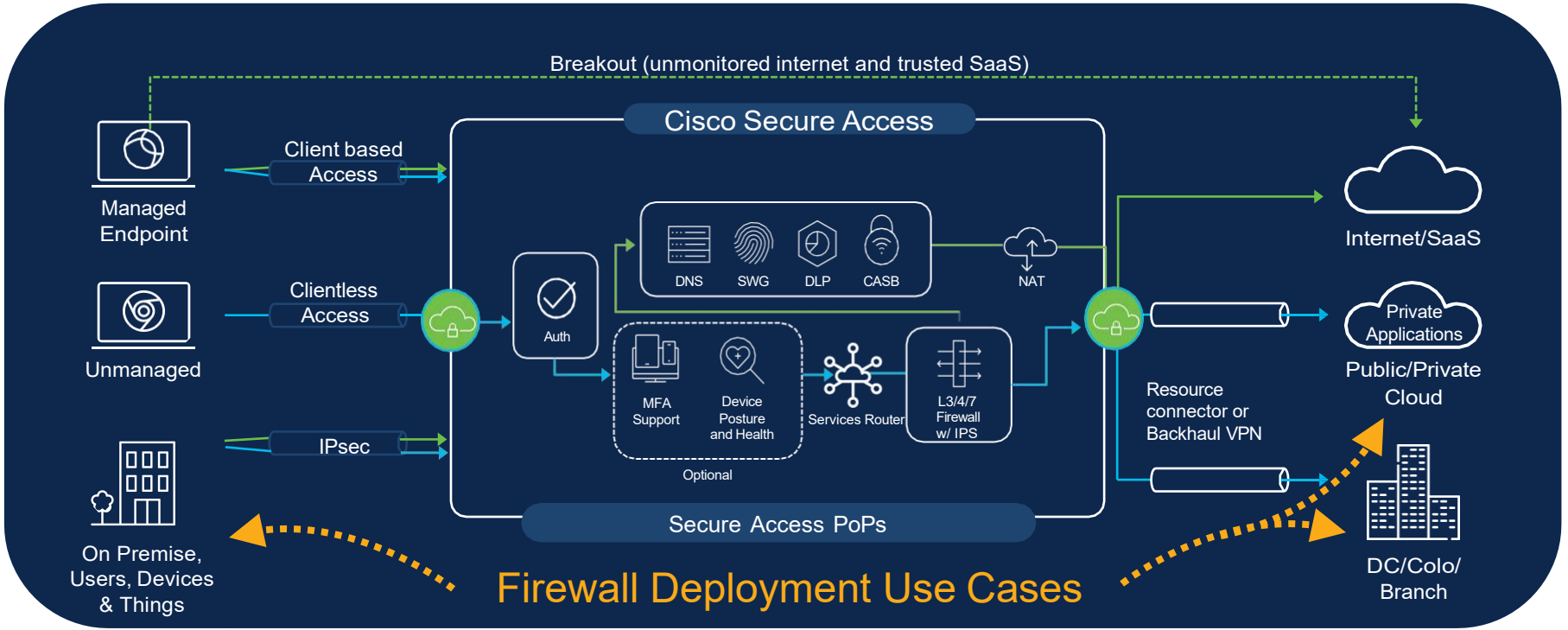
Featuring Cisco Secure Access

cisco Live!

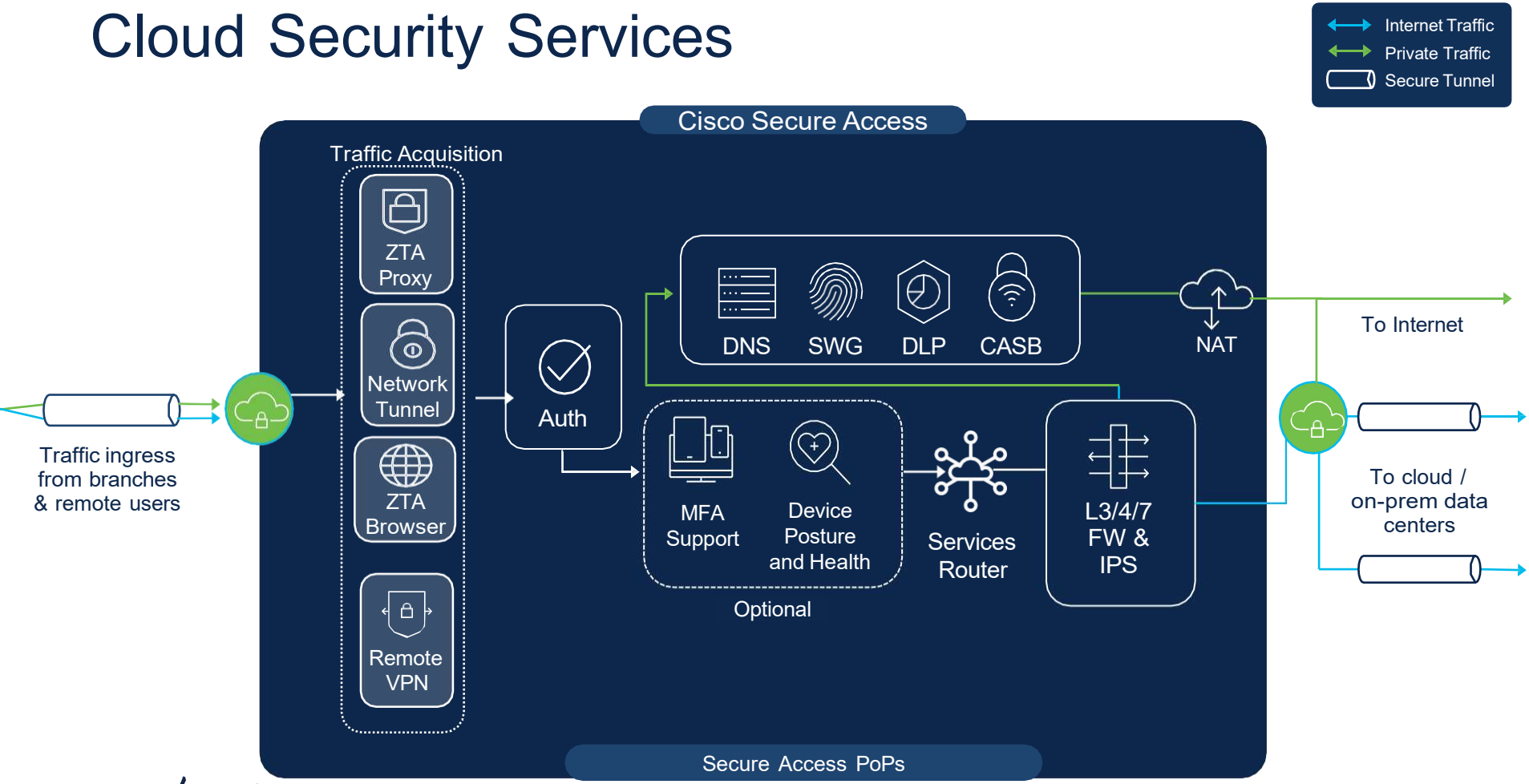
Cisco Secure Access

Converged cloud security grounded in zero trust

Secure Access (“Security Service Edge”)



Cloud Security Services



Why connect your branches to Secure Access?

Internet Security capabilities:

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

Private application access:

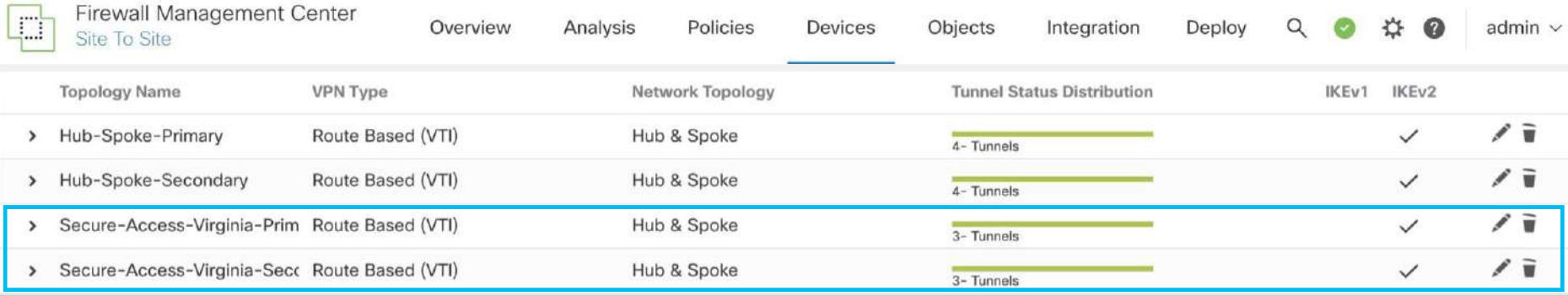
- Connectivity to private apps protected by Secure Access
- Connectivity for private applications behind branch firewall
- Connectivity to cloud delivered RAVPN as a service subnets

SSE Integration

with Firewall Threat Defense

cisco Live!

Secure Access Branch Tunnels



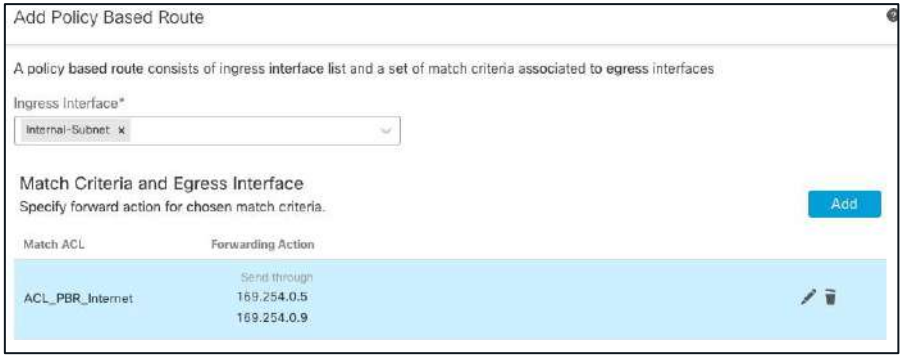
- Use dedicated Hub & Spoke VTI Tunnel topologies for simplicity
- Dual topologies for redundant tunnels to backup DC
- eBGP or static routing to Secure Access data centers
  - Can assign “branch networks” to tunnel on Cloud Side if using static routing.

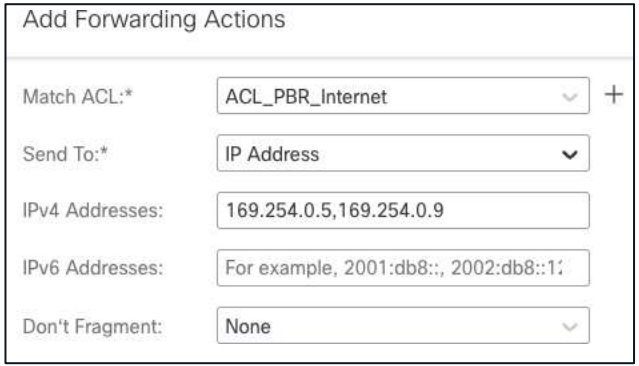
Cisco Secure Access

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





FTD Branch with Secure Access

Routes from Secure Access:

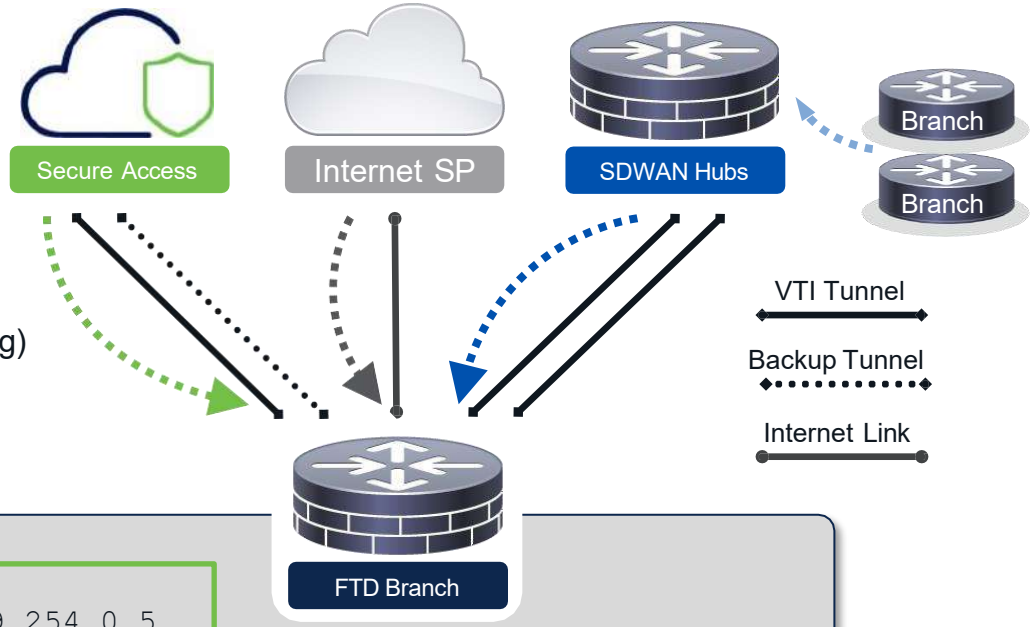
- Default Route* (Optional)
- RAVPN Subnets, Zero Trust enabled applications, Proxy Infrastructure

Static routes to ISP:

- Secure Access DC VPN Endpoint IPs (prevent flapping)

Routes from SDWAN Hubs:

- SDWAN HQ, branches, and data centers



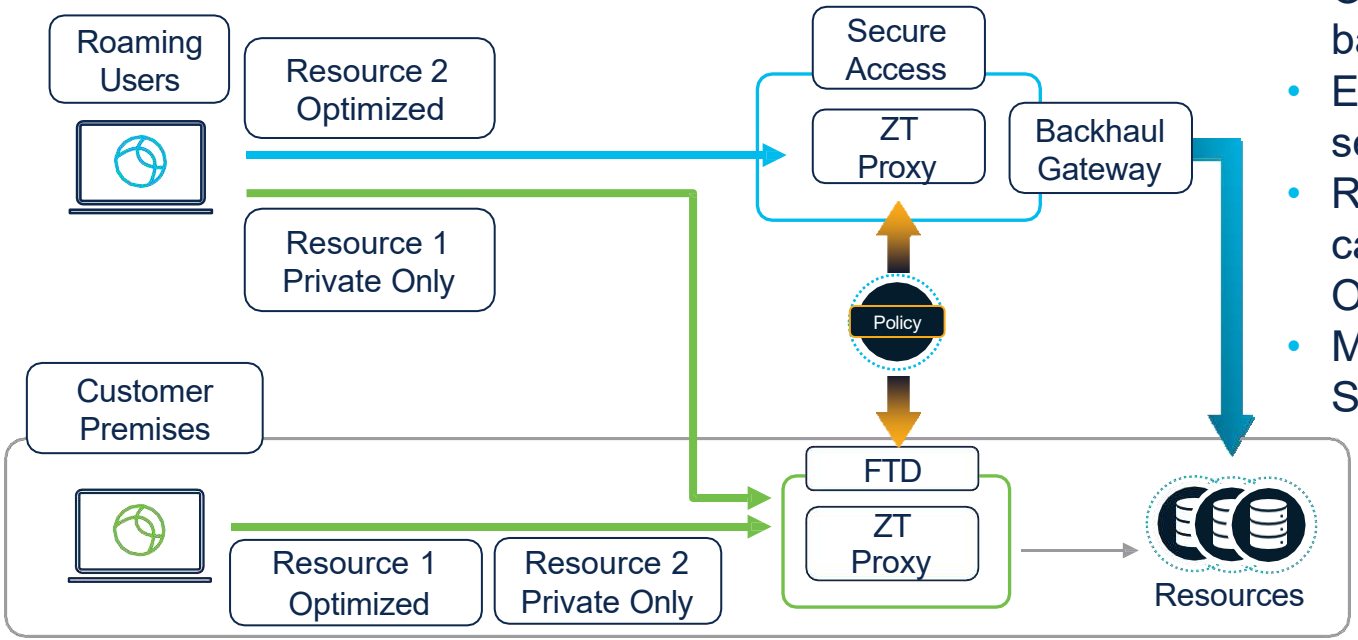

```
FTD-Spoke# show route
B* 0.0.0.0 0.0.0.0 [20/0] via 169.254.0.5
B  100.73.x.0 255.255.240.0 [20/0] via 169.254.0.5

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
```

Cool stuff coming soon! - Universal ZTNA

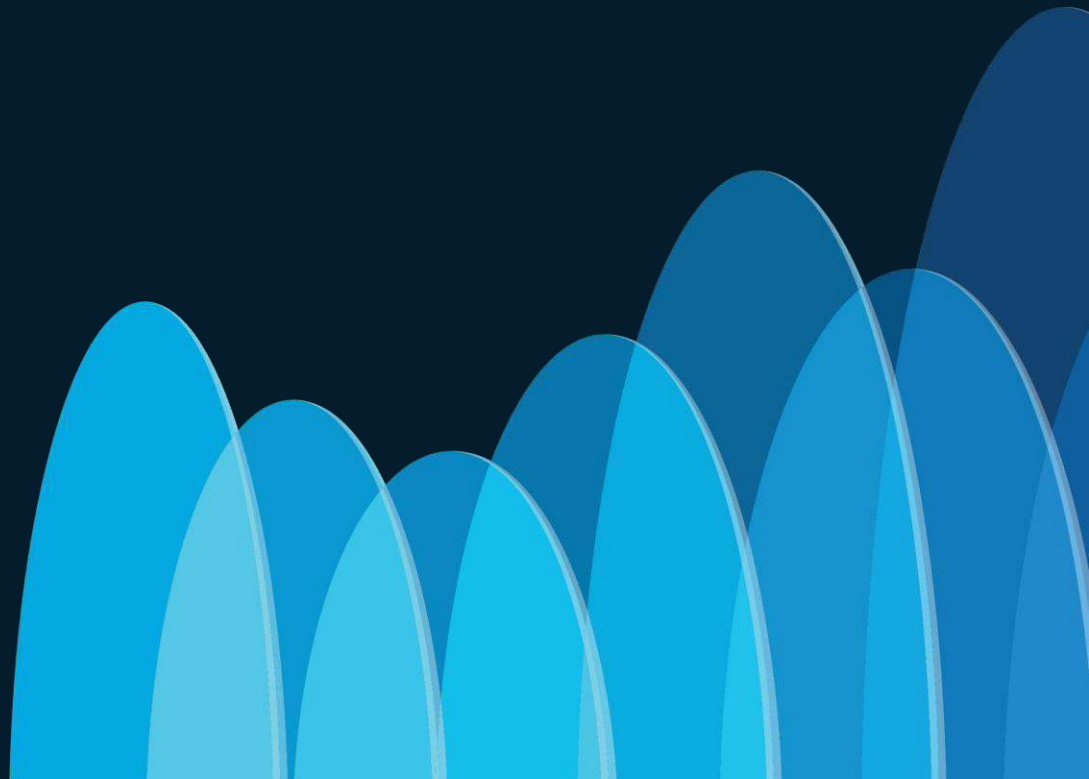
Single Policy, Distributed Enforcement (Overview)



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

SSE Integration

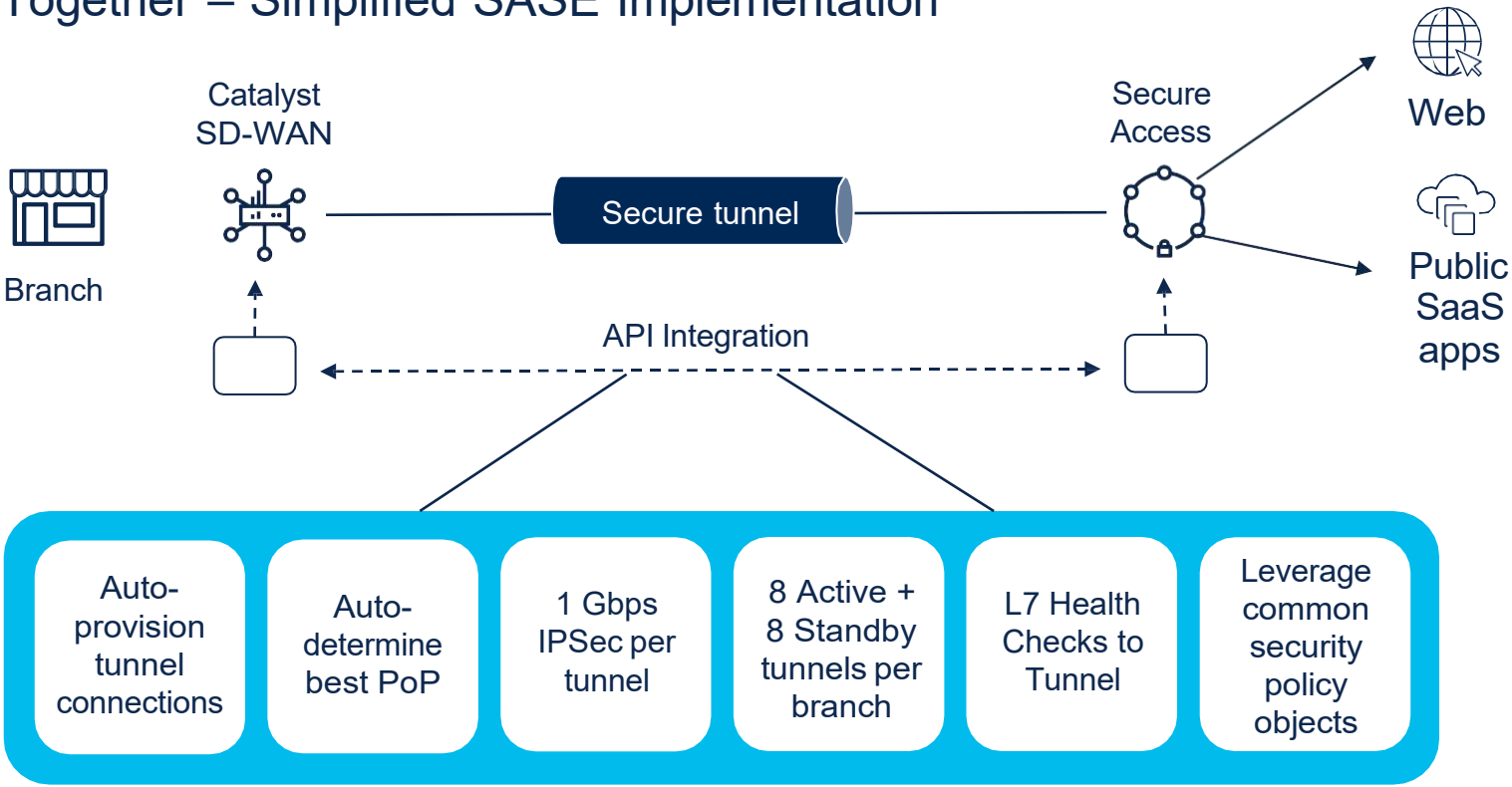
with Catalyst SDWAN



cisco Live!

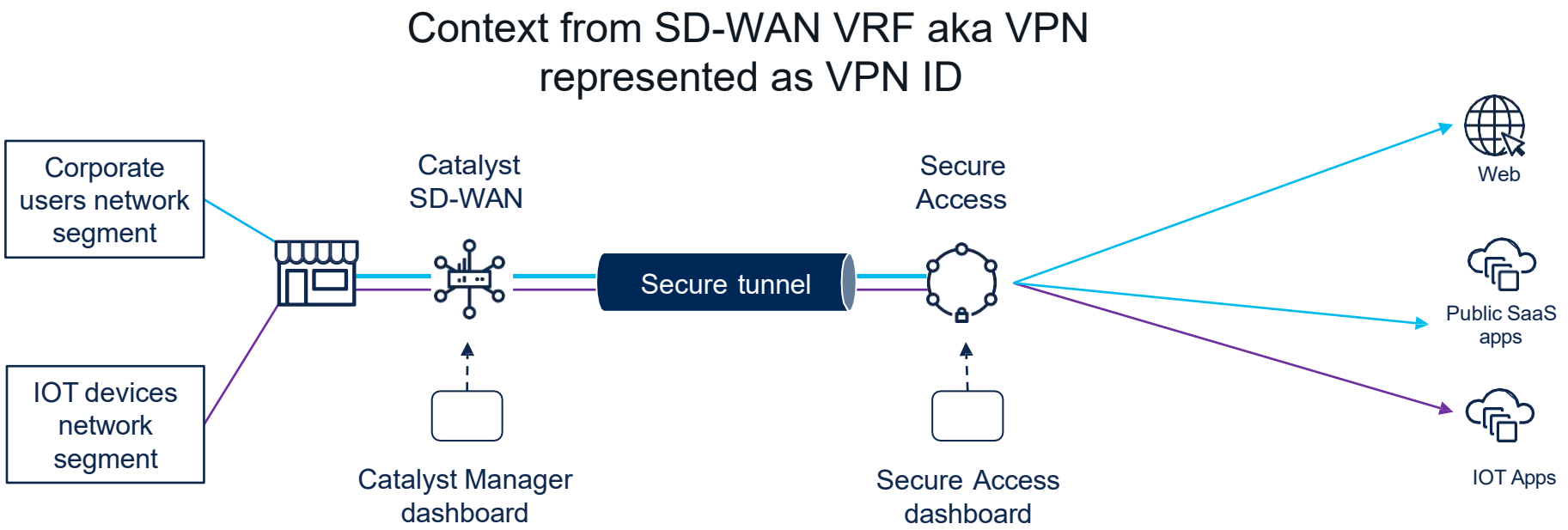
Secure Access + Catalyst SD-WAN

Better Together – Simplified SASE Implementation



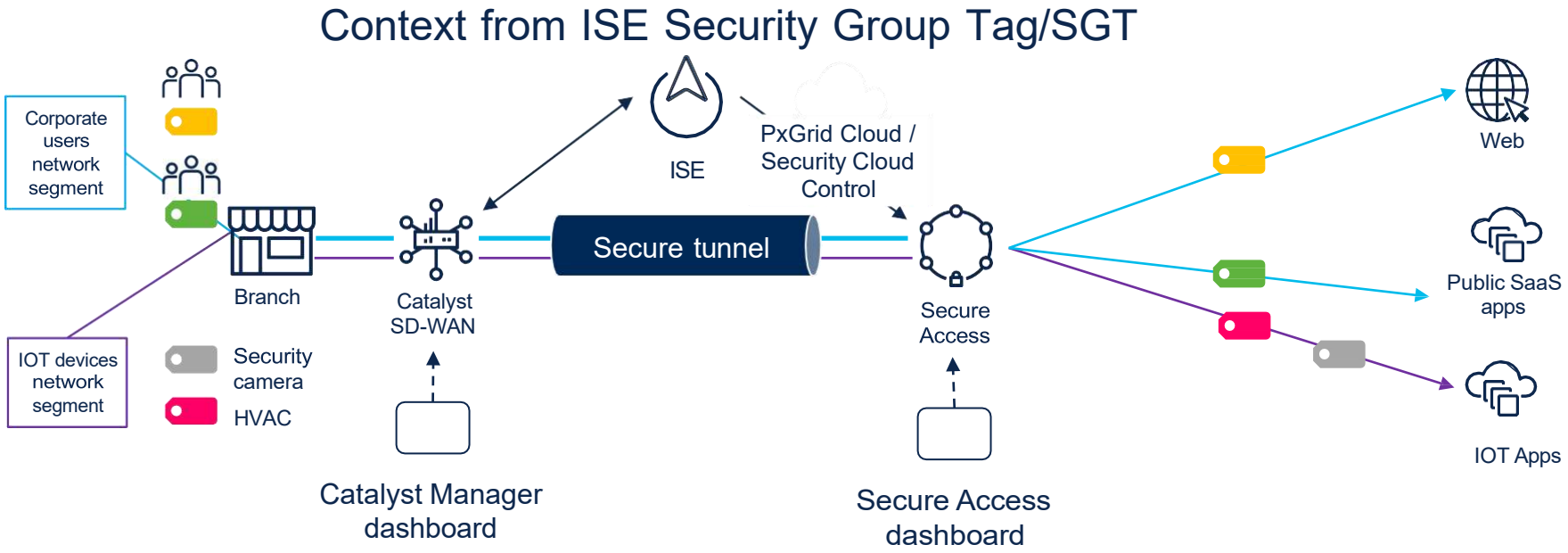
Secure Access + Catalyst SD-WAN

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

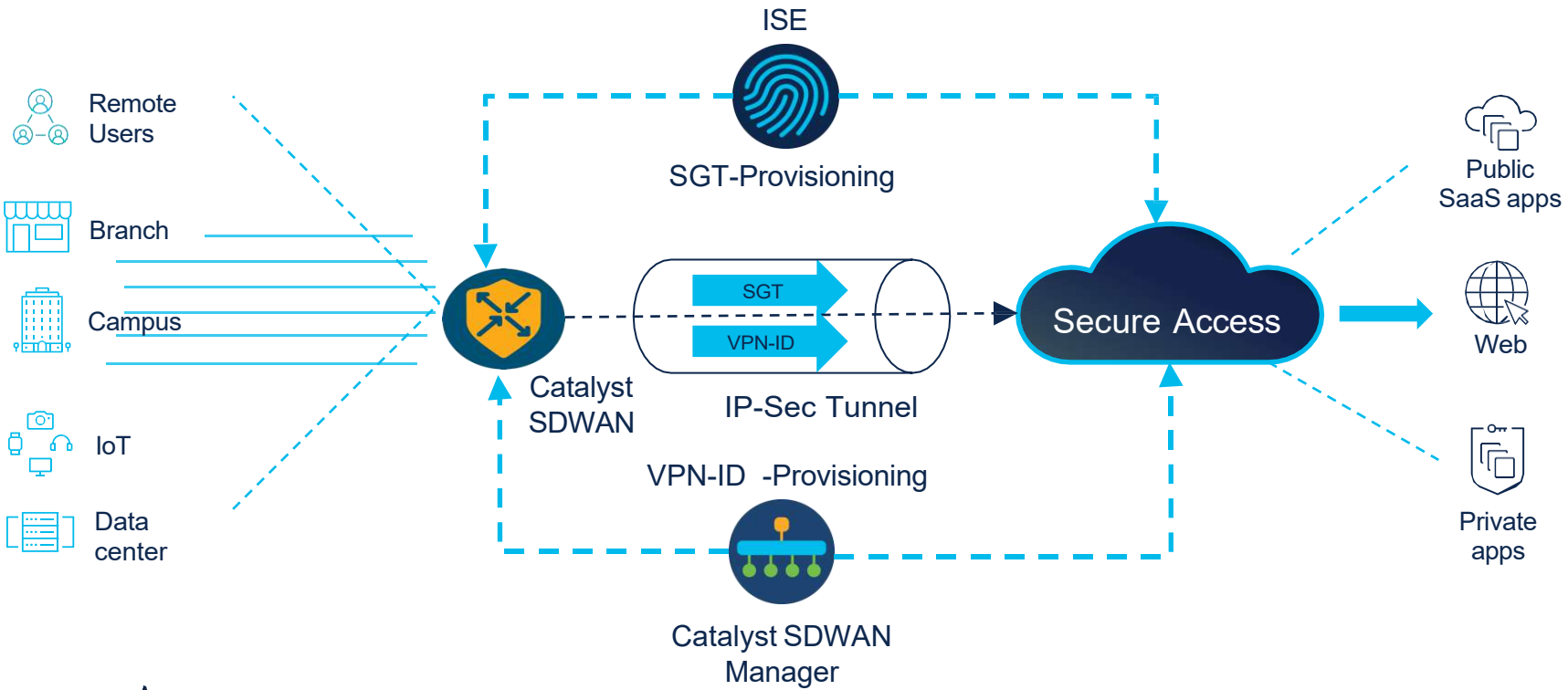


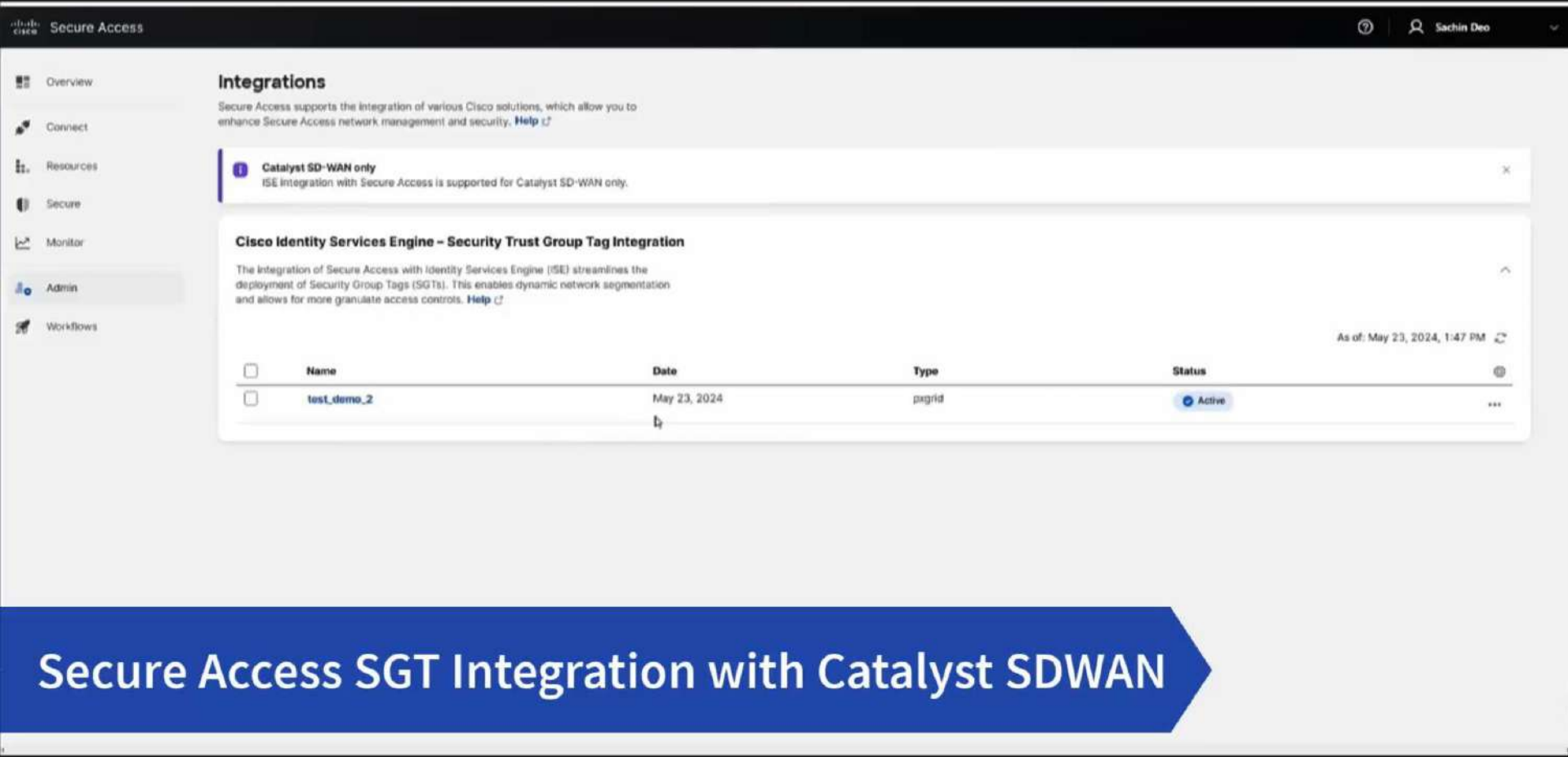
Secure Access + Catalyst SD-WAN

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



Macro and Micro Segmentation Based Policy





Secure Access SGT Integration with Catalyst SDWAN

SSE Integration with Meraki MX

cisco Live!

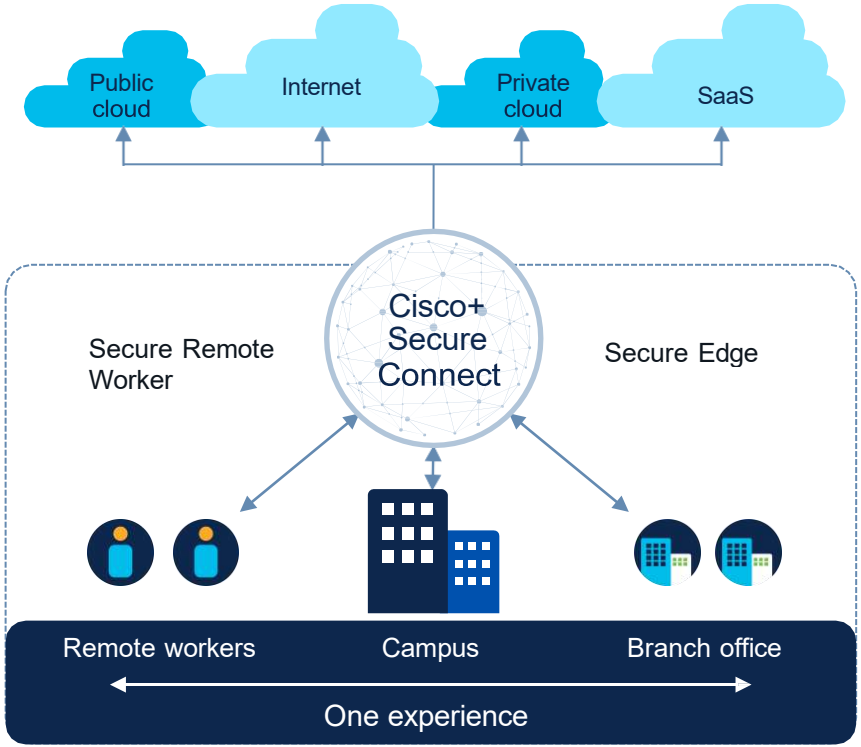
Secure Connect Overview

Secure Internet Access
Provide safe access to the internet and cloud applications from any location and block malicious activity and threats

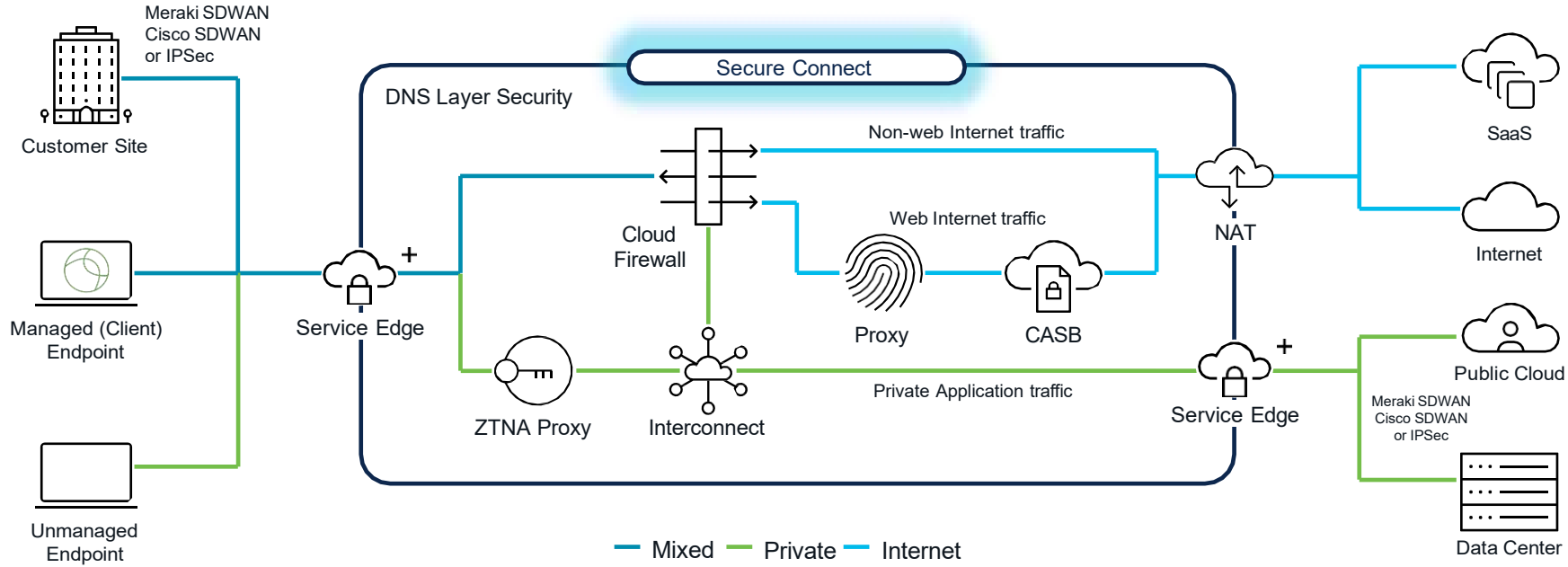
Secure Private Access
Define policy to control branch workers access to private apps behind data center, private or public cloud, or branches.

Secure Remote Access
Connect remote IdP workers to cloud fabric for secure internet access. Enable unmanaged devices to access private apps in browser.

Site Interconnect
Interconnect sites, branch users, and apps with integration of Meraki Secure SD-WAN, IPSec VPN support and direct SaaS/IaaS Peering.



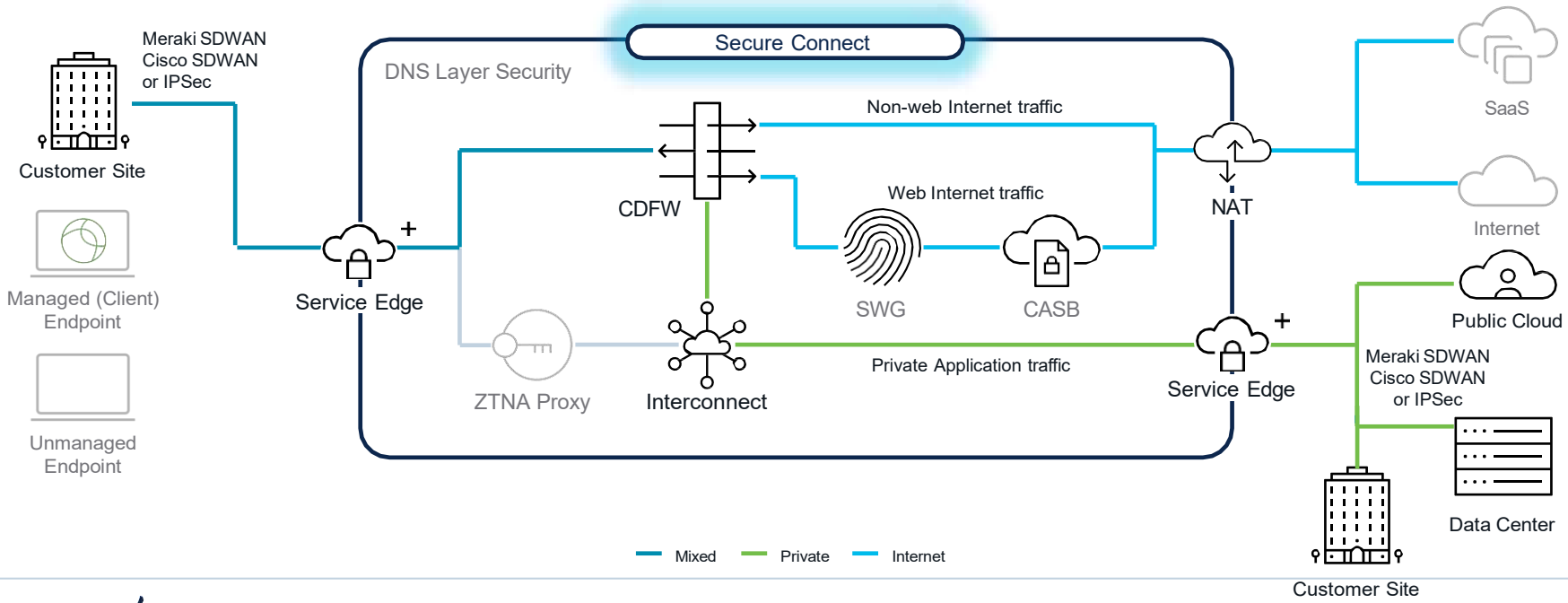
Secure Connect Architecture



Interconnect Everything **Security Everywhere**

Secure Branch Traffic

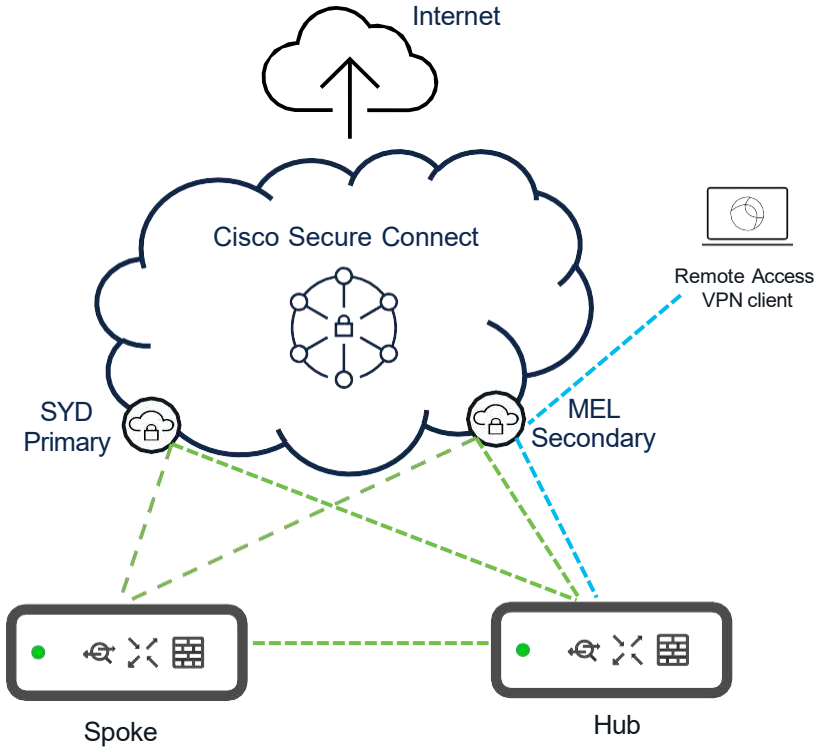
Site Interconnect
Secure Internet Access
Secure Private Access



Secure Connect - Hybrid Hub Design

Security

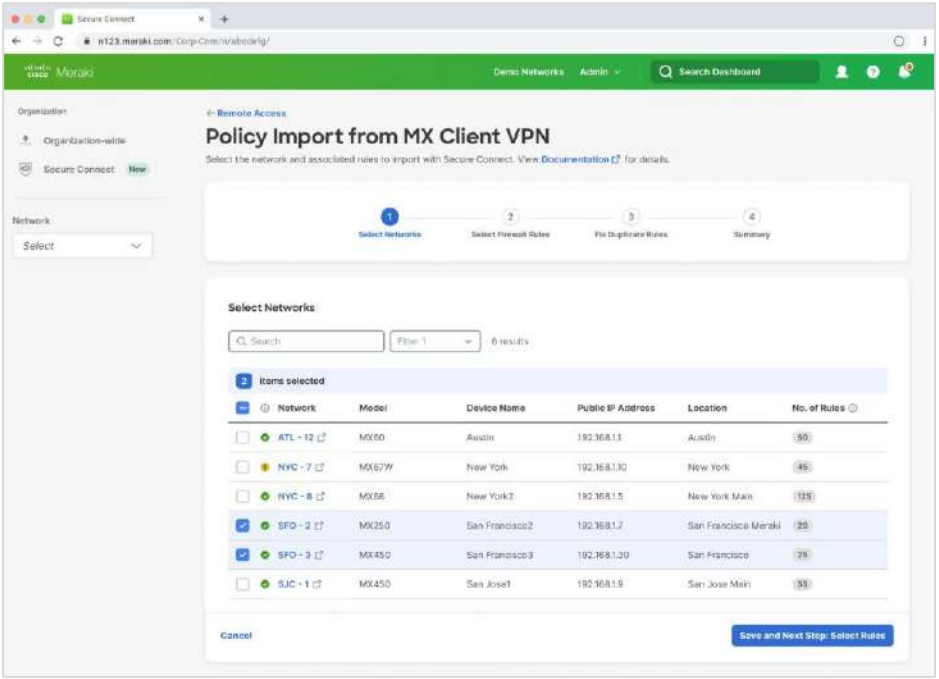
- Supports Meraki Hub & Spoke East / West
- More specific (branch) routes are advertised, other traffic default routed to Secure Connect
- Optimizes Secure Connect fabric consumption

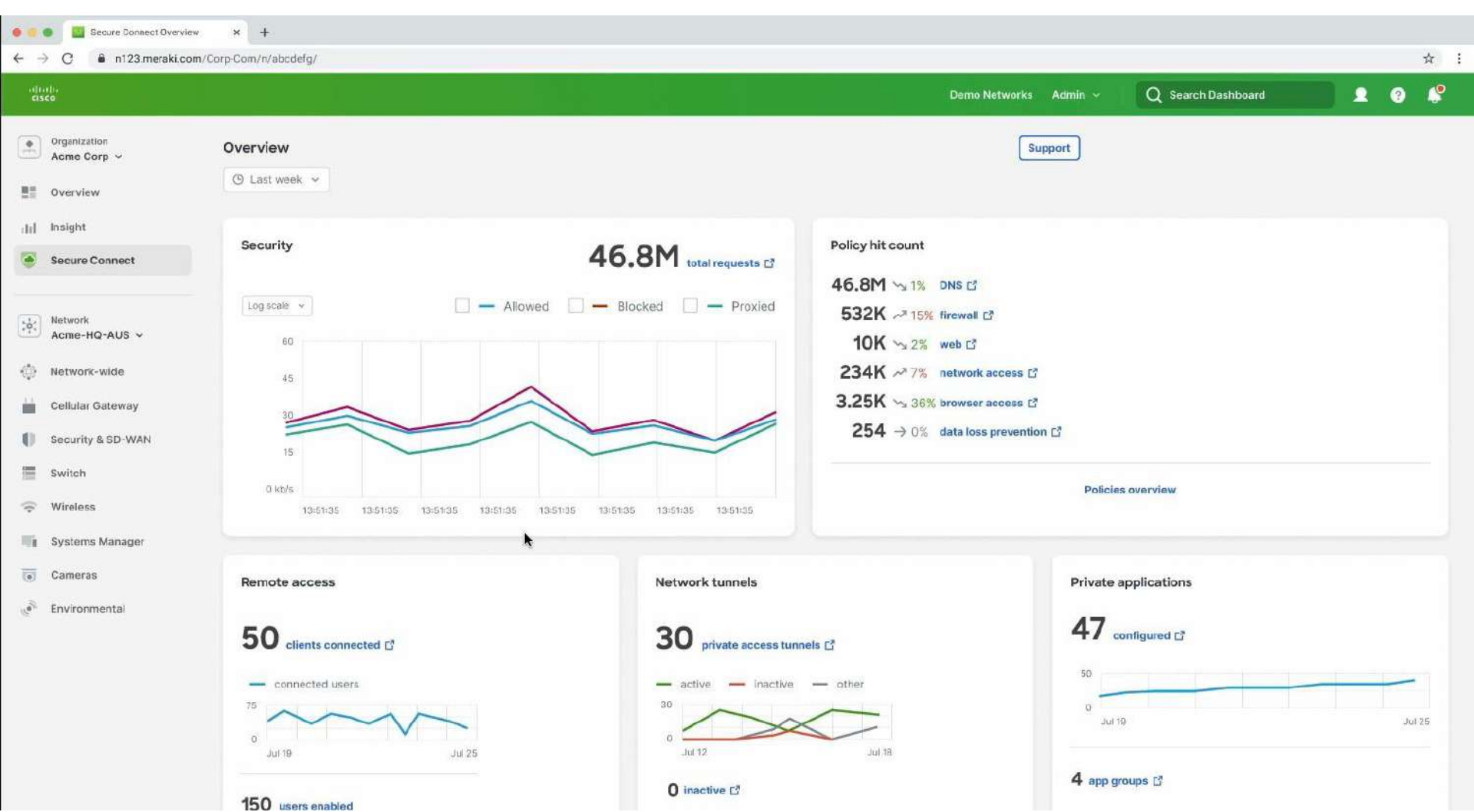


Policy Import

Policy Import allows administrator to import existing Meraki firewall policies into Secure Connect.

- Reduce cloud transition time by bulk import of rules
- Streamline remote access to internet rules by removing duplicated rules
- Find unused rules prior to make informed import decisions



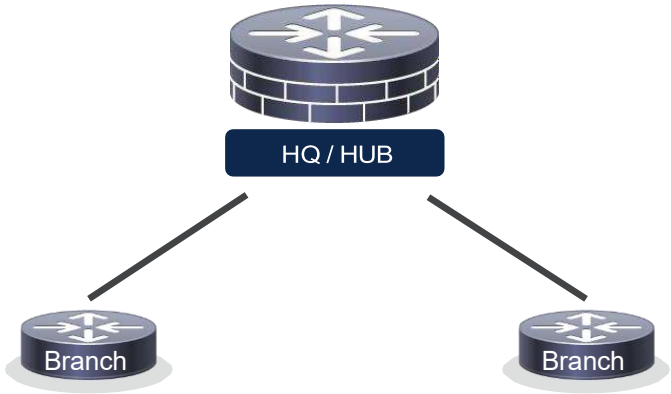

Secure Connect Overview
n123.meraki.com/Corp-Com/n/abcdefg/
Demo Networks
Admin
Search Dashboard
Organization
Acme Corp
Overview
Insight
Secure Connect
Network
Acme-HQ-AUS
Network-wide
Cellular Gateway
Security & SD-WAN
Switch
Wireless
Systems Manager
Cameras
Environmental
Overview
Last week
Support
Security
46.8M total requests
Log scale
Allowed
Blocked
Proxied
60
45
30
15
0 kb/s
13:51:35
Policy hit count
46.8M ↘ 1% DNS
532K ↗ 15% firewall
10K ↘ 2% web
234K ↗ 7% network access
3.25K ↘ 36% browser access
254 → 0% data loss prevention
Policies overview
Remote access
50 clients connected
connected users
75
0
Jul 19
Jul 25
150 users enabled
Network tunnels
30 private access tunnels
active
inactive
other
30
0
Jul 12
Jul 18
0 inactive
Private applications
47 configured
50
0
Jul 19
Jul 25
4 app groups

Cisco's secure & scalable SD-WAN solutions

All Cisco SD-WAN Platforms offer:

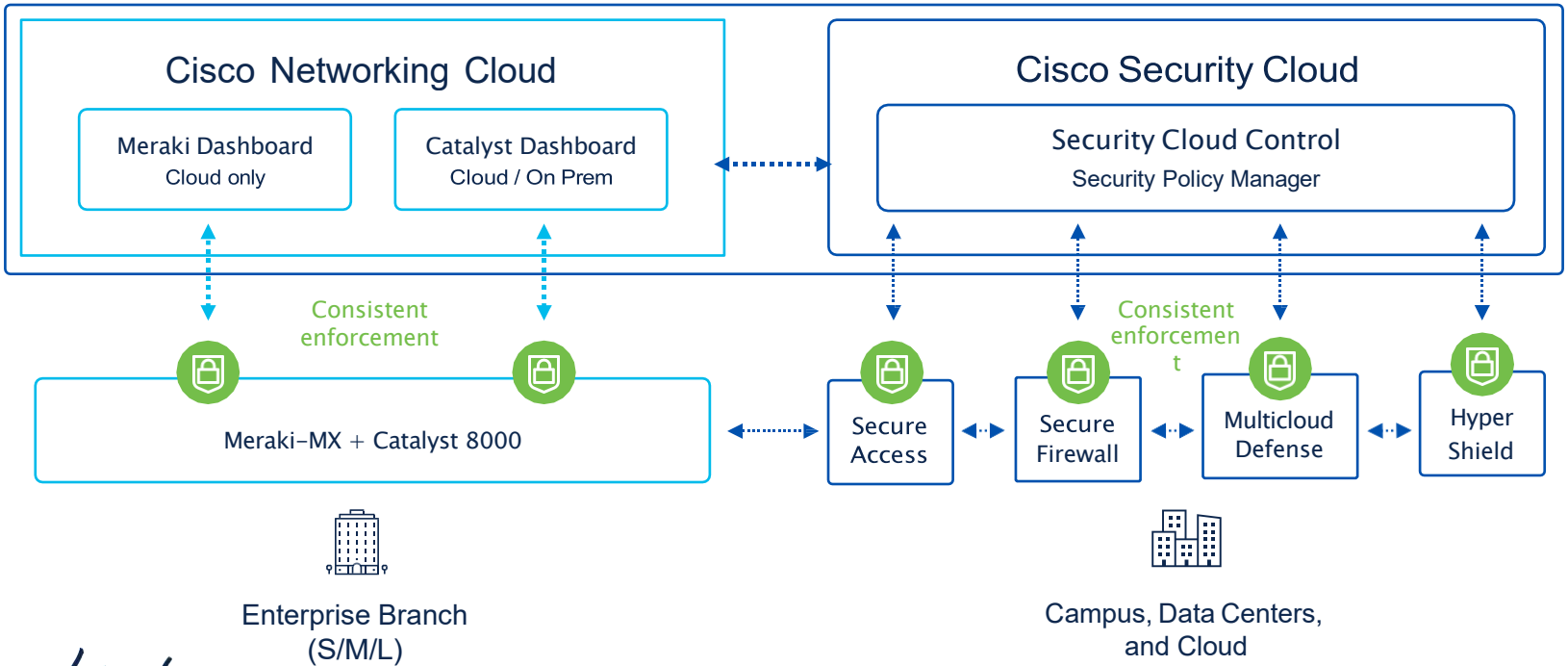
- Scalable (1000+) hub & spoke node designs
- Application Policy Based Routing
- Robust on-box branch security capabilities
- SASE / SSE integration with Secure Access / Secure Connect (Meraki)

Each platform architecture offers unique differentiation for use case specific benefits!



Unified Secure WAN experience

Centralized security policy with consistent enforcement at WAN Edge



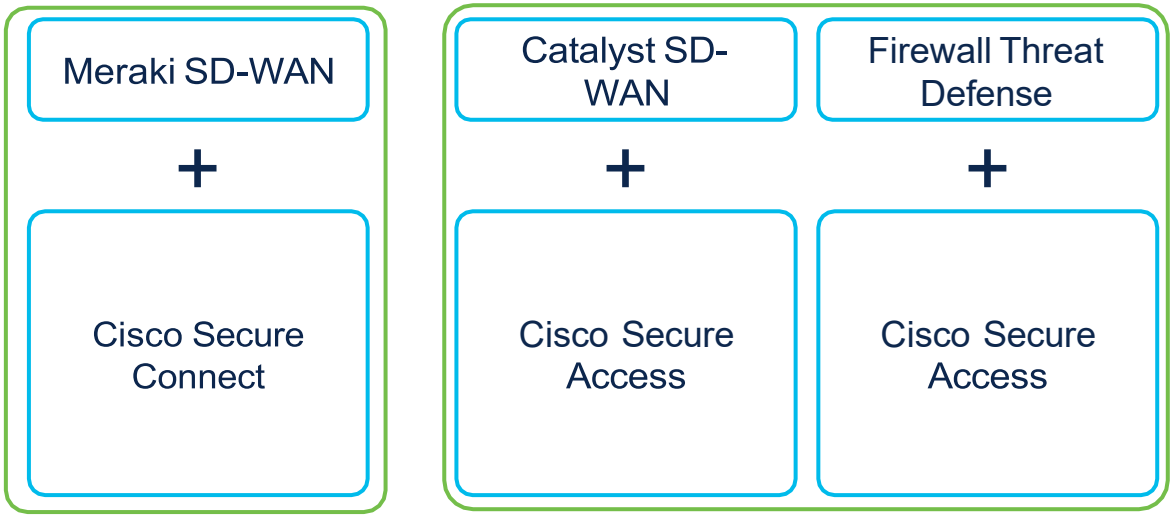
Cisco SASE: Powerful, flexible, and intelligent for

Cisco SASE

Powerful, flexible, and intelligent

Unified SASE

One dashboard, unified policies



Multi-Vendor SASE options

Open, validated integrations

Common architecture and components
Shared by Secure Access & Secure Connect

SDWAN 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	SDWAN 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!

Webex App

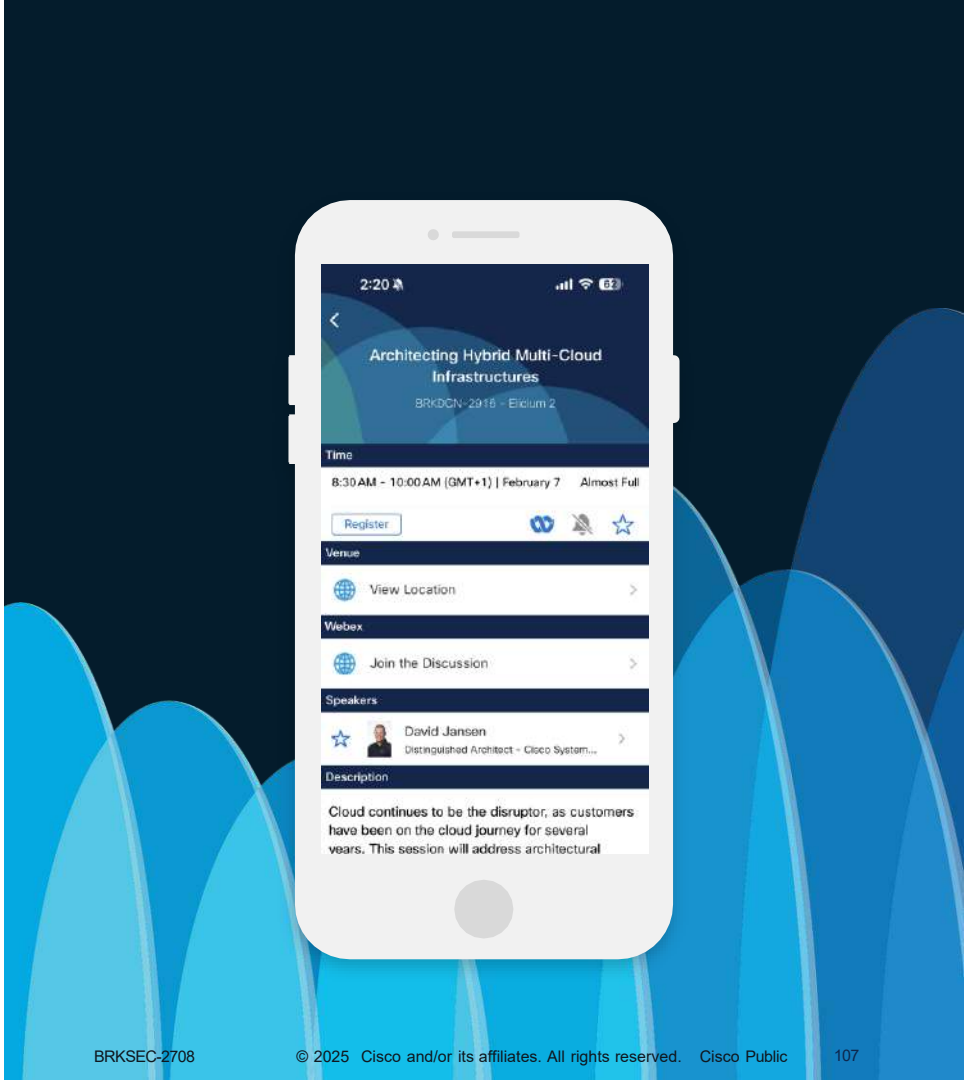
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.



Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.


cisco
Thank you
cisco Live!

cisco Live!

enquiries@aritofafrica.com, support@aritofafrica.com

www.aritofafrica.com