Catalyst SD-WAN: Start here

Prashanth Raghavendra
Technical Marketing Engineering Technical Leader

Session ID: BRKENT-2108

Cisco Webex App

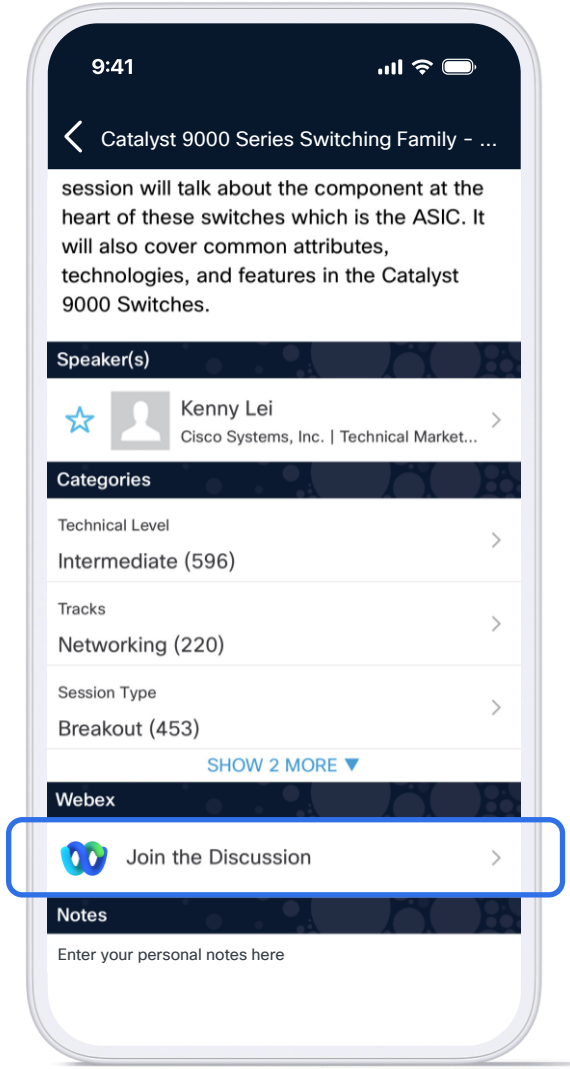
Questions?

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-2108**

Agenda

1 Why SD-WAN

2 Architecture

3 Features

4 8000 Series Secure Routers

5 Learn More

About Me

- TME Technical Leader @

  SD-WAN & Cloud Networking Team

- Focus Areas:

  User and Application experience,

  Operational simplification,

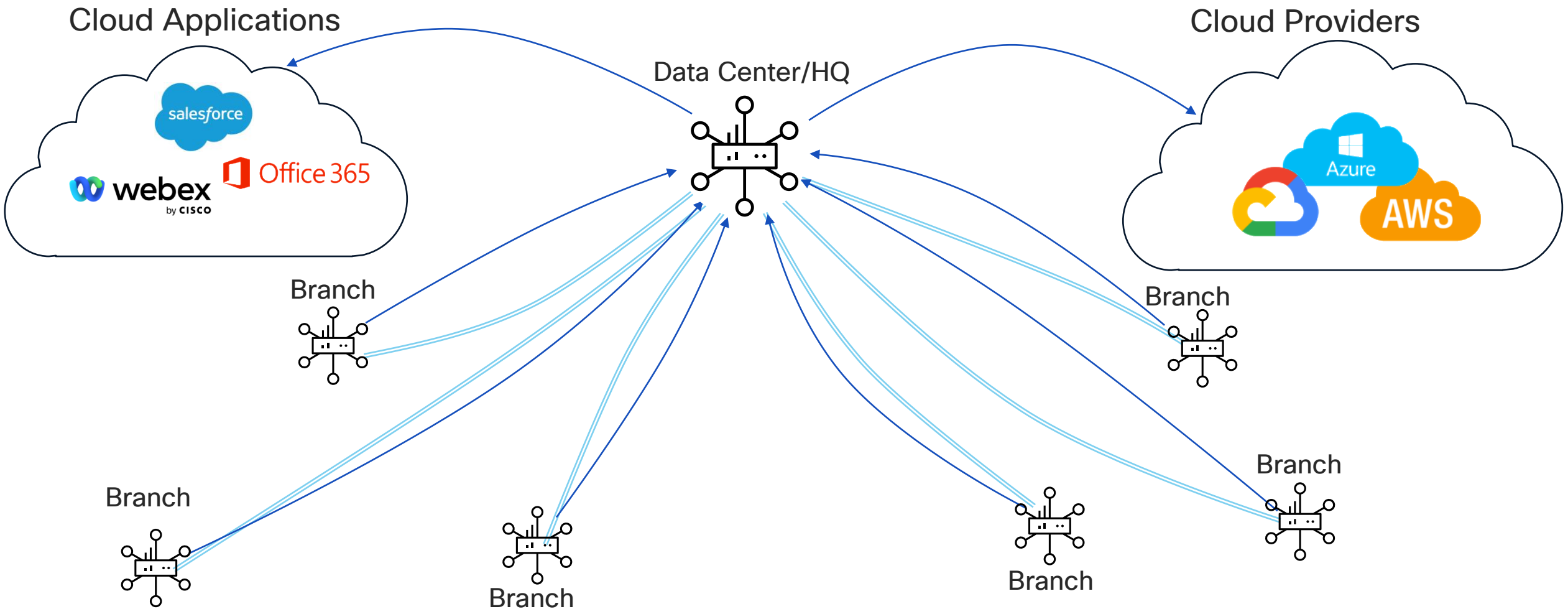
  Assurance (Analytics & AIOps)

SD-WAN – This is it.

Why SD-WAN?

The classical Hardware Based WANs

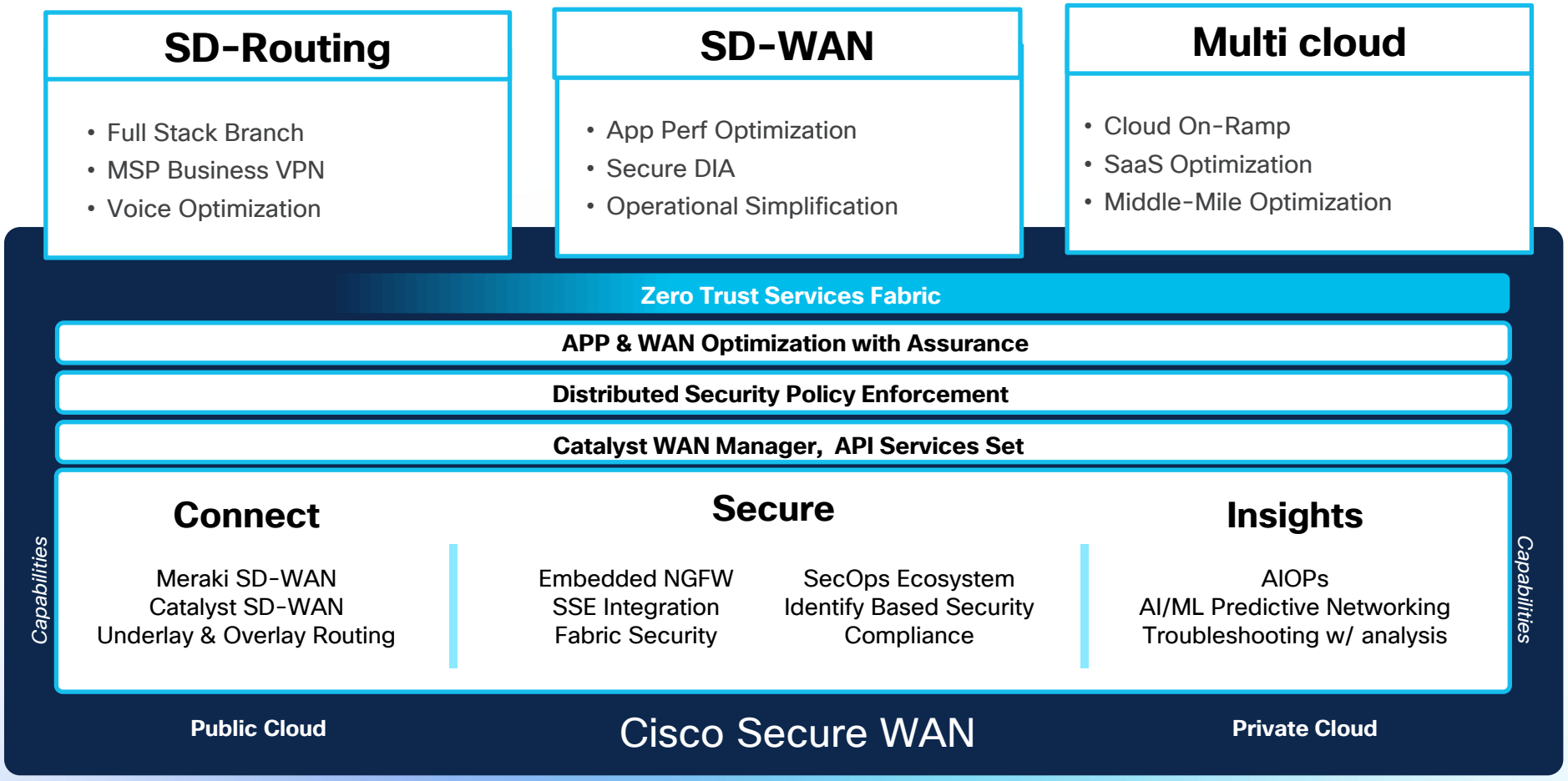
Doesn’t Keep up with the Needs of Today



cisco

Cisco SD-WAN: Software Approach

Cisco Secure WAN



Common use-cases for SD-WAN

Secure Branch connectivity

Automated, Easy, fast, visible and simplified.

Multi-Cloud Connectivity

Expand the network to any cloud provider.

Use any type of transport

Fiber, Cable, Satellite, LEO, LTE, 5G or DSL

Secure and flexible

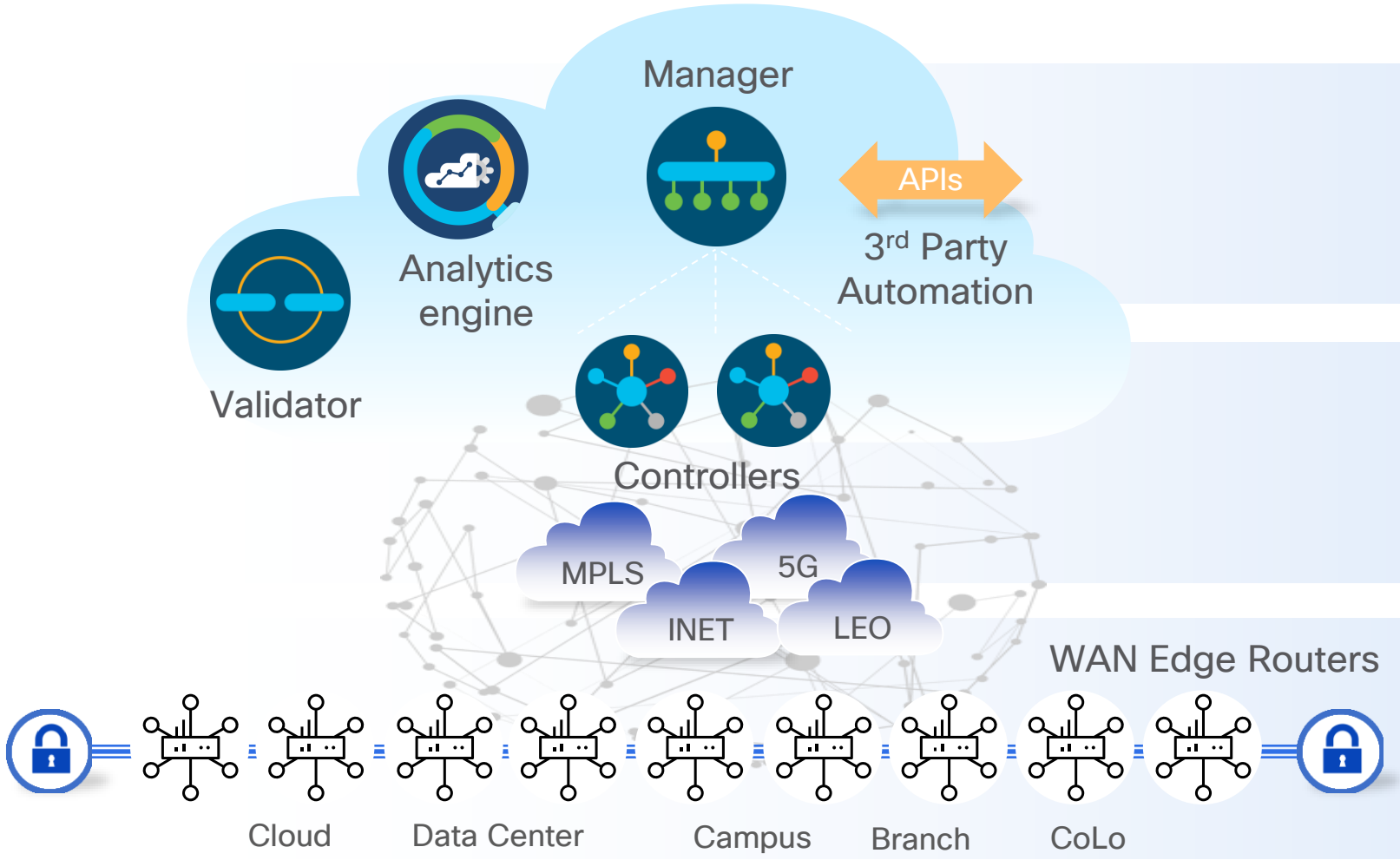
Direct Internet access, security features, SSE and scalable deployments.

Feature rich

Voice, L2VPN, WAN Optimization and much more.

Architecture

Cisco Catalyst SD-WAN Solution Overview

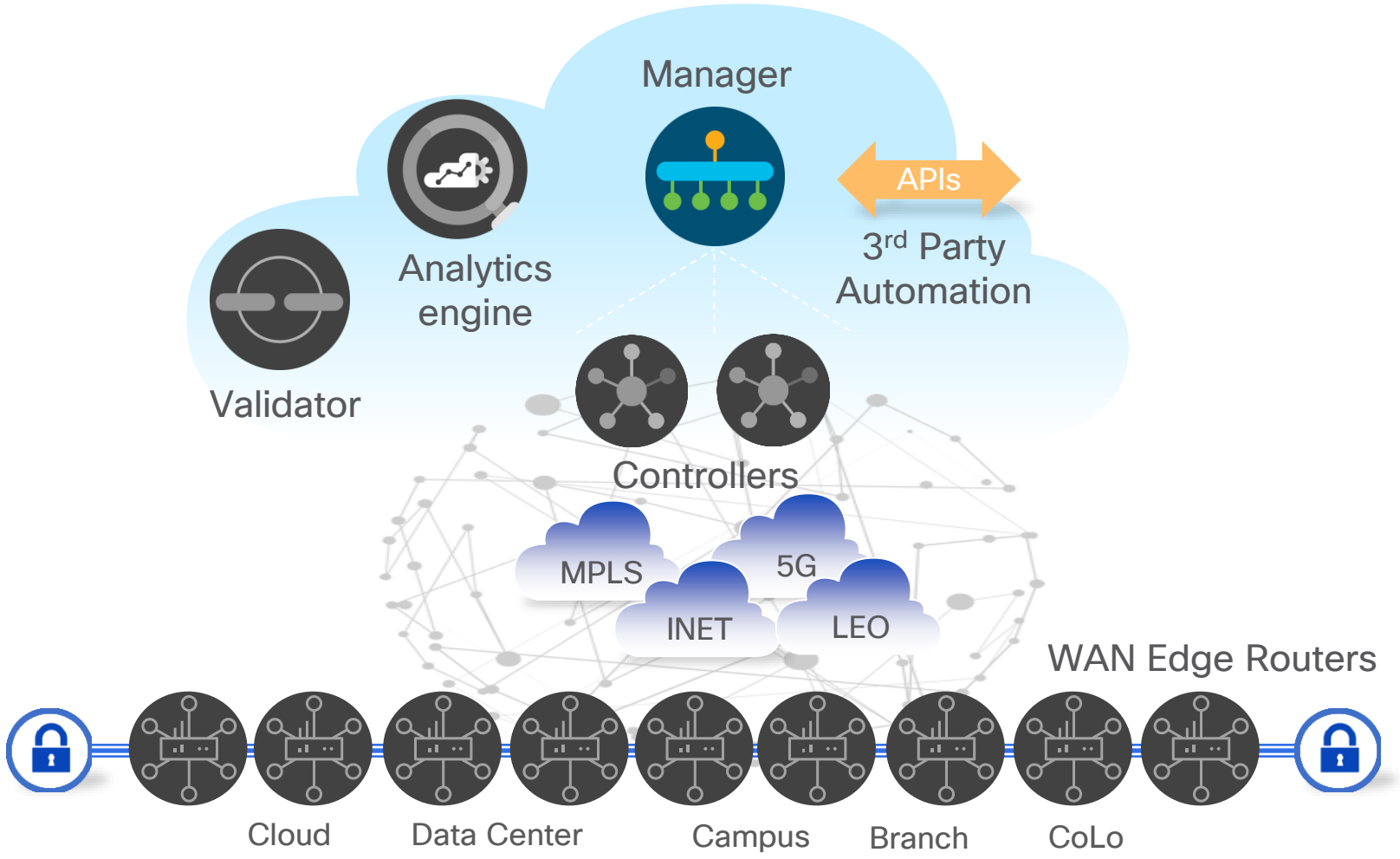


Management/ Orchestration Plane

Control Plane

Data Plane

Cisco Catalyst SD-WAN Solution Elements

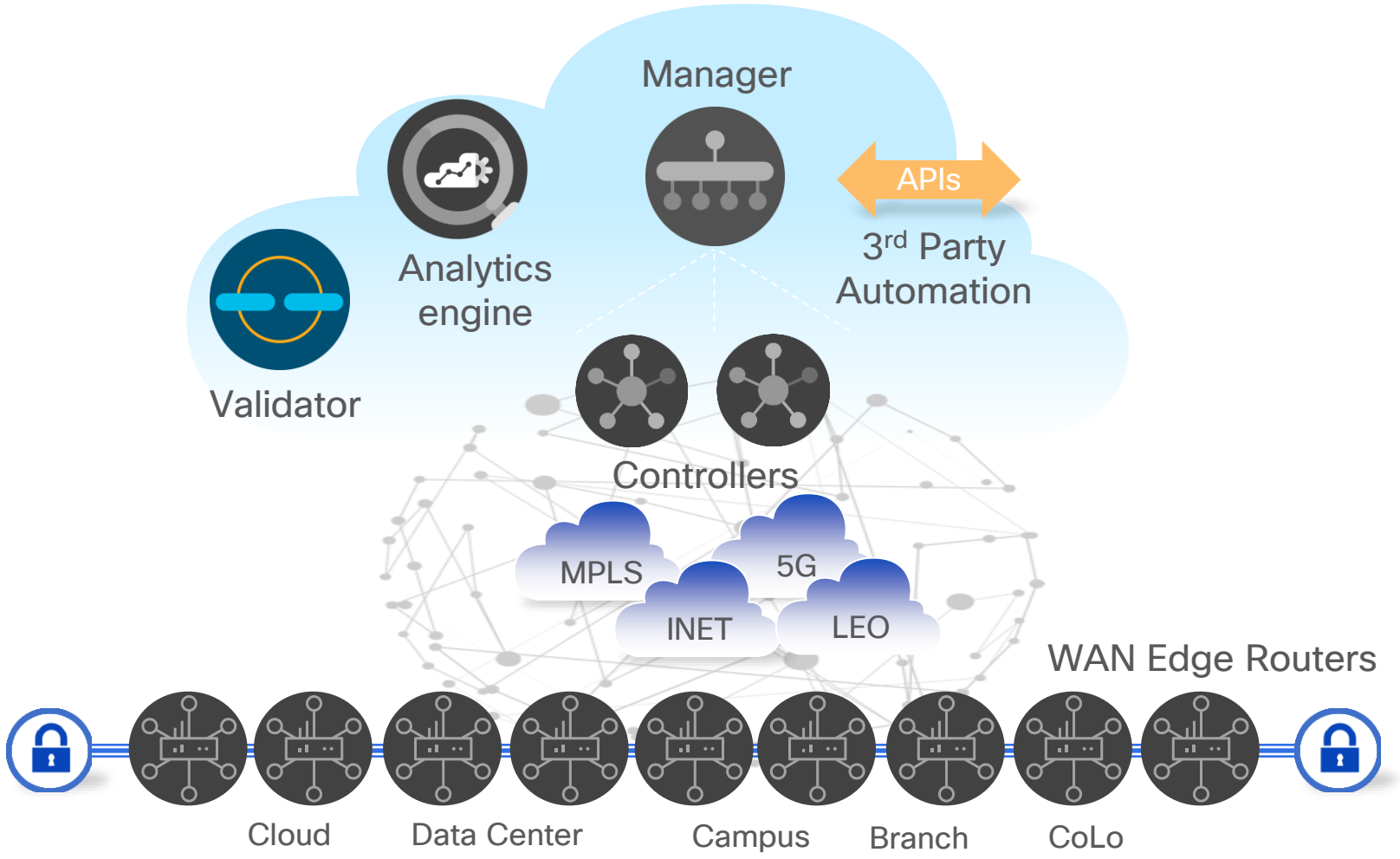


Management Plane

Cisco Catalyst SD-WAN Manager

- Single pane of glass for Day0, Day1 and Day2 operations
- Multitenant with web scale
- Centralized provisioning
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades
- GUI with RBAC
- Programmatic interfaces (REST, NETCONF)
- Highly resilient

Cisco Catalyst SD-WAN Solution Elements

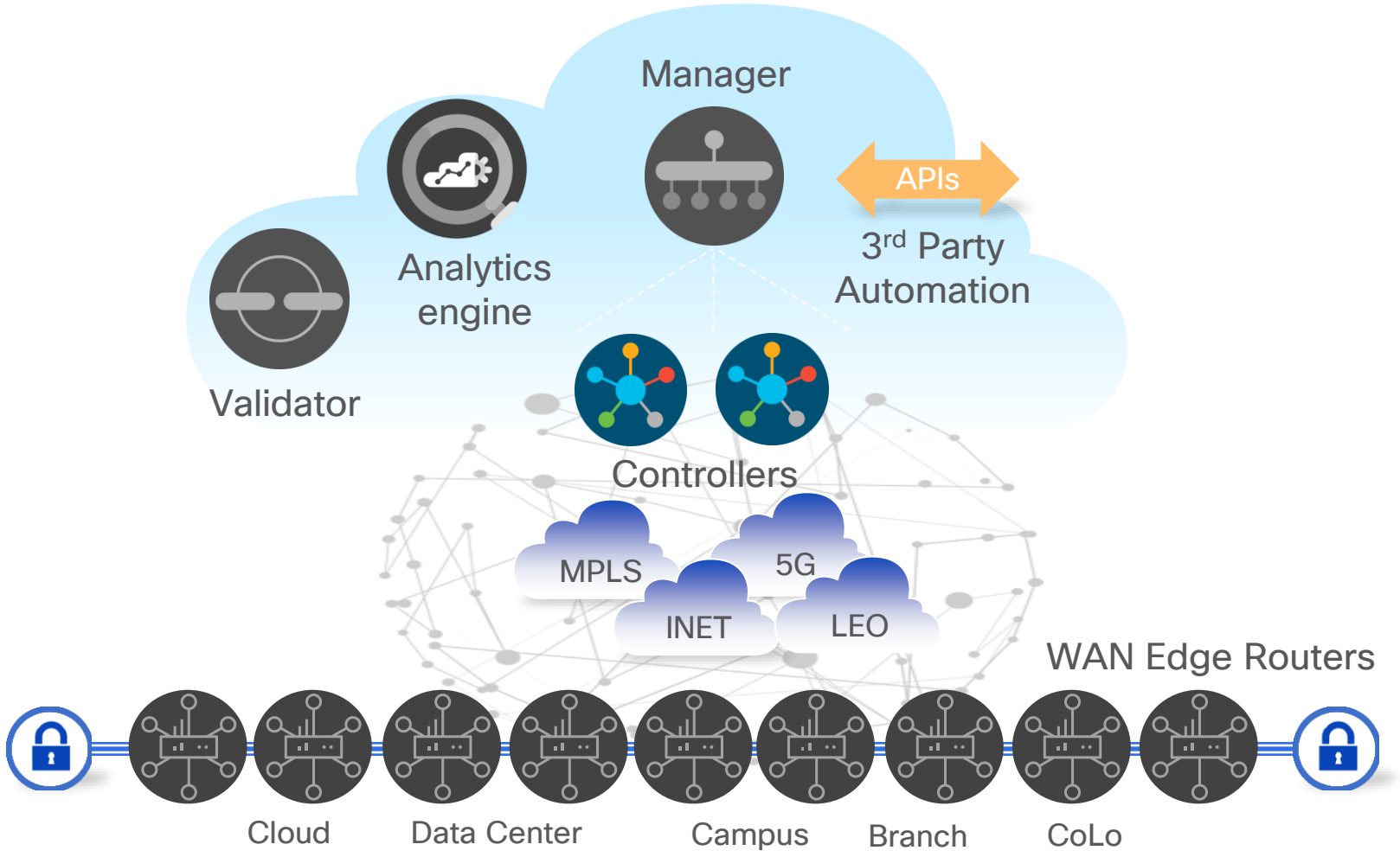


Orchestration Plane

Cisco Catalyst SD-WAN Validator

- Orchestrates control and management plane
- First point of authentication (white-list model)
- Distributes list of Controllers/ Manager to all WAN Edge routers
- Facilitates NAT traversal
- Requires public IP Address [could sit behind 1:1 NAT]
- Highly resilient

Cisco Catalyst SD-WAN Solution Elements



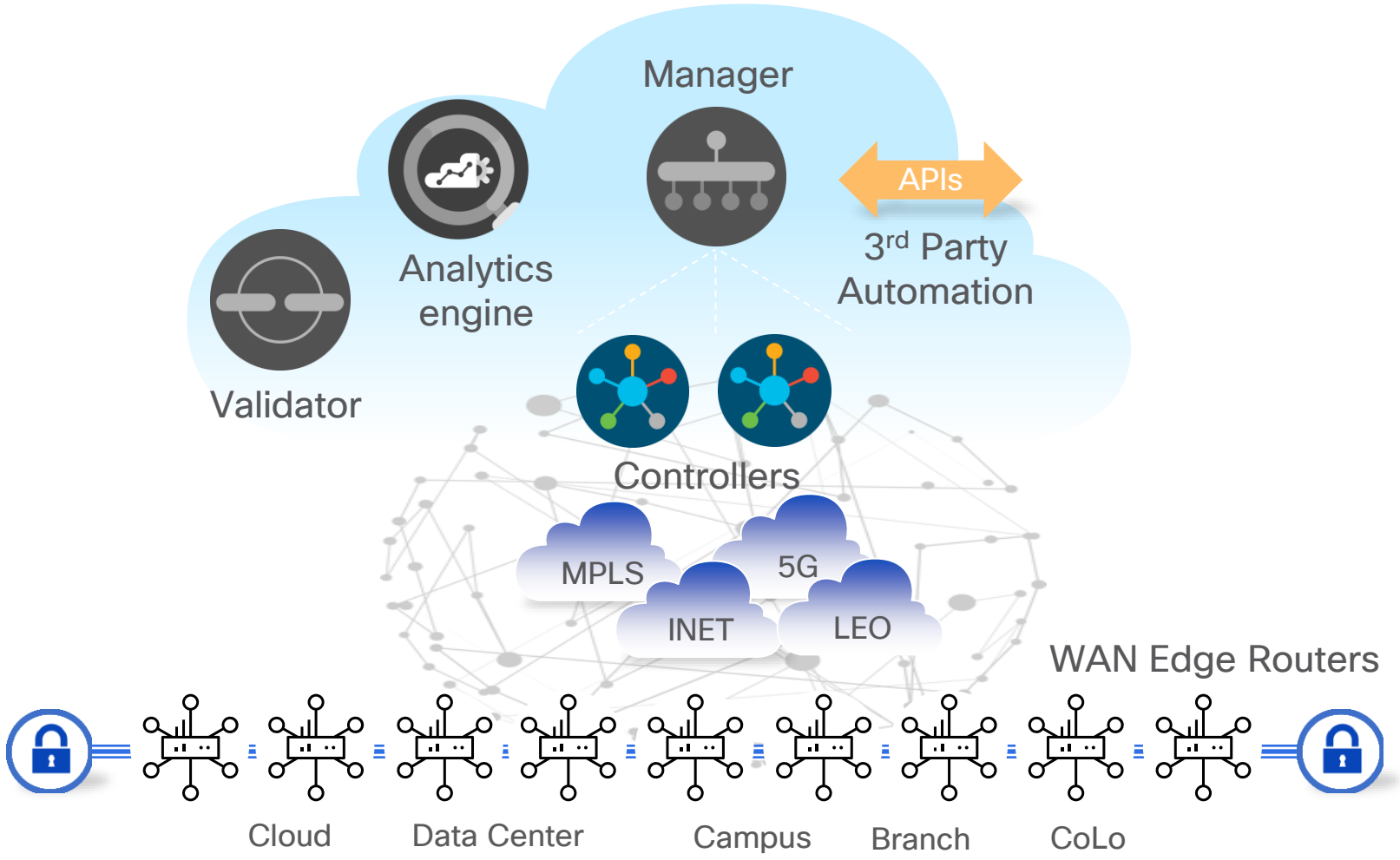
Control Plane

Cisco Catalyst
SD-WAN Controller

- Facilitates fabric discovery
- Disseminates control plane information to the WAN Edge Routers
- Distributes data plane and app-aware routing policies to the WAN Edge routers
- Implements control plane policies, such as service chaining, multi-topology and multi-hop
- Dramatically reduces control plane complexity
- Highly resilient

cisco

Cisco Catalyst SD-WAN Solution Elements



Data Plane

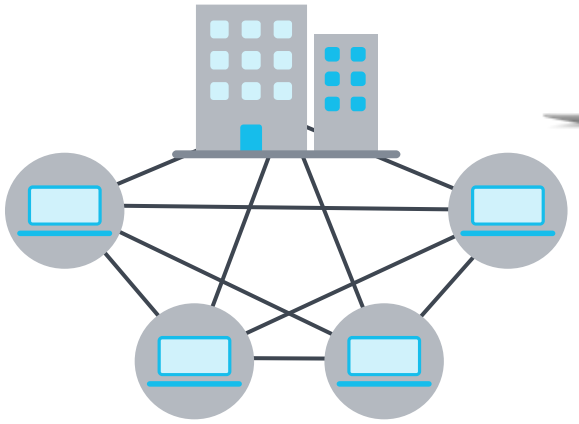
Cisco SD-WAN
WAN Edge Router

- Provides secure data plane with remote WAN Edge routers
- Establishes secure control plane with Controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP, and EIGRP
- Support Zero Touch Deployment
- Physical or Virtual form factor (100Mb, 1Gb, 10Gb,40Gb, 100Gb)

Catalyst SD-WAN Analytics

From 20.15/17.15 – SD-WAN Manager & Analytics are converged*

SD-WAN Manager



SD-WAN Fabric

Secure API

TCP/443

Flow Information
SAIE
Events
Inventory
Path Performance Metrics
...

Telemetry Repository
(Cisco Cloud)

Cloud tethered SD-WAN Manager (On-Prem or Cloud Hosted)

*Air Gap SD-WAN Manager supports monitoring capabilities local to SD-WAN Manager

Cisco Catalyst SD-WAN Fabric Deployment Models

Customer/MSP Hosted

- **Customer Private Cloud & Public Cloud**
- **MSP Private Cloud & Public Cloud**

Cisco Hosted
(AWS & Azure)

- **Standard Environment (Shared and Dedicated)**
- **Certified Environment (PCI, SOC2, ISO, C5, etc.)**
- **Gov. Cloud (FedRAMP)**

Cloud-delivered

- **Life Cycle Management of SD-WAN Fabric**
- **Agile and scalable service access**
- **Operational simplicity**
- **Rich analytics providing actionable insights**

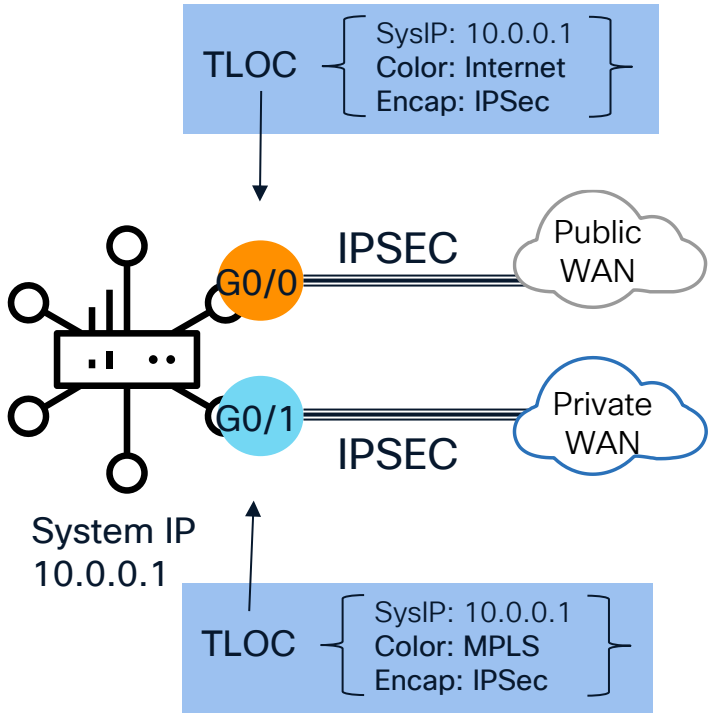
Flexible deployment models aligned to your business needs

Features

Significance of TLOC Color

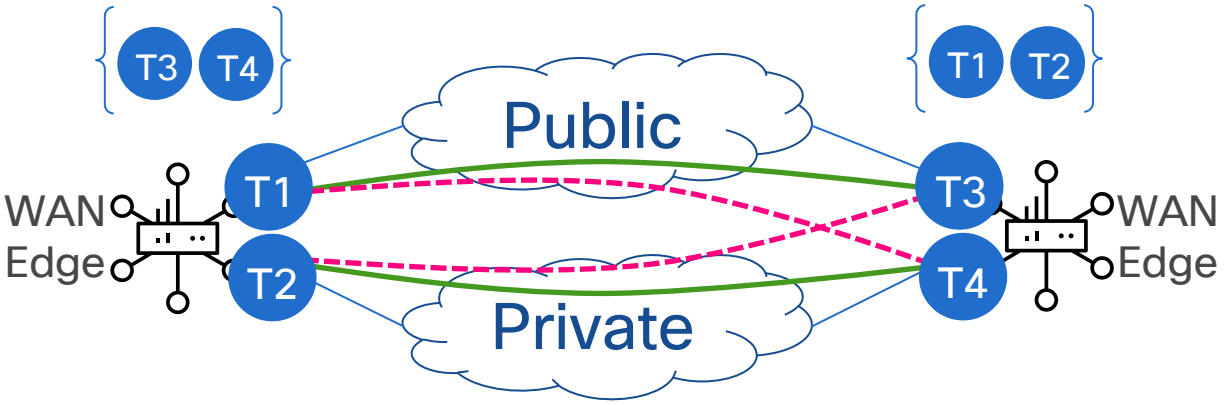
- Color is an abstraction used to identify individual WAN transport
- Policies can be created based on these
- TLOC maps to physical WAN interfaces
- "Color" dictates the use of private IP vs public IP (Dest) for Tunnel Establishment when there is NAT present

  Example:
  - If two ends have a **private** color: private IP address/port used for DTLS/TLS or IPSec
  - If endpoint has **public** color: Public IP is used for DTLS/TLS or IPSec

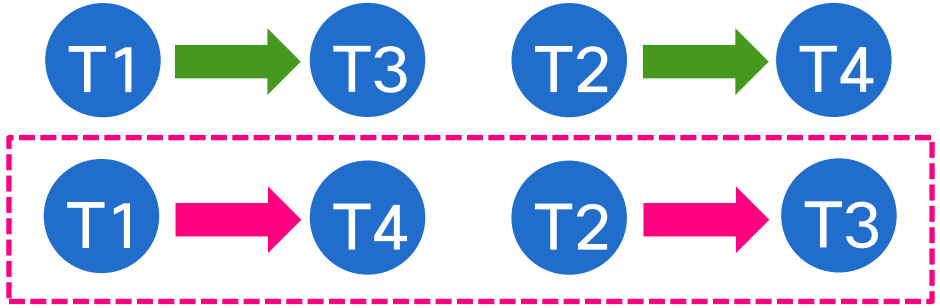


Private Colors	Public Colors
Metro-ethernet	3g
mpls	lte
private1	biz-internet
private2	public-internet
private3	blue
private4	green
private5	red
private6	gold
	silver
	bronze

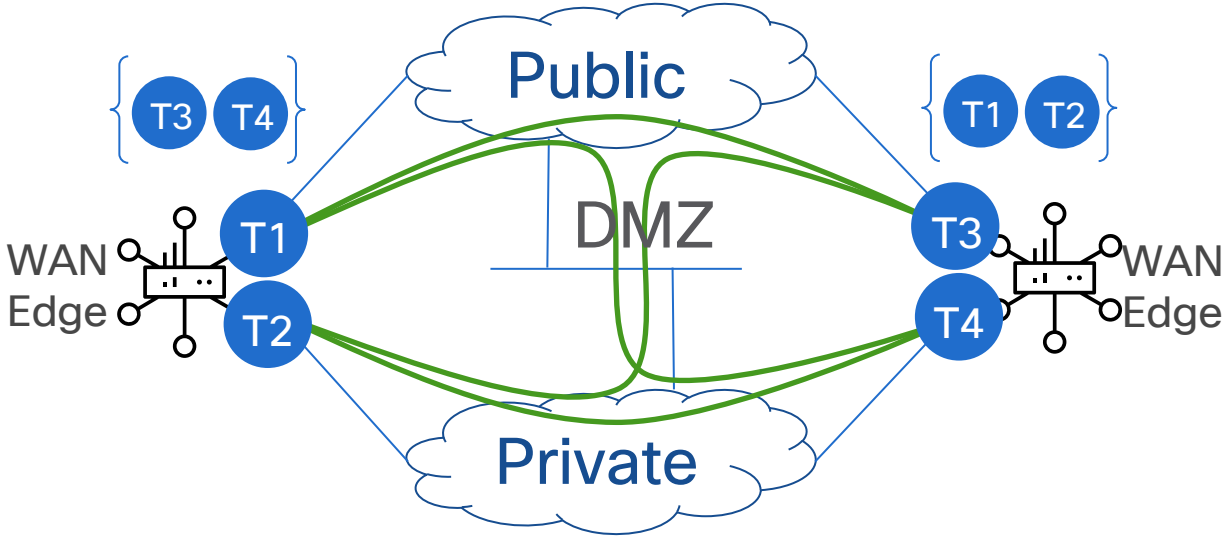
Transport Colors



T1, T3 – Public Color T2, T4 – Private Color

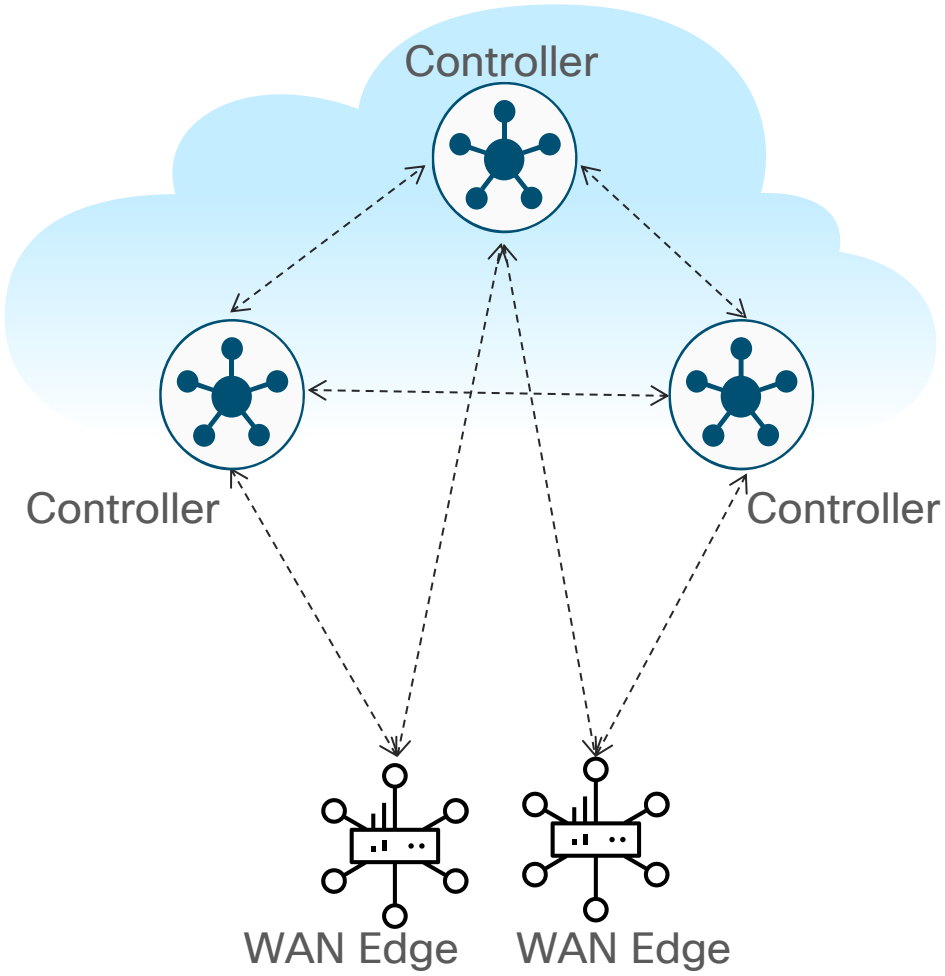


Color restrict will prevent attempt to establish IPSec tunnel to TLOCs with different color



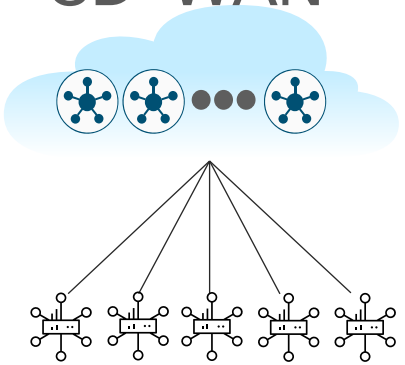
T1, T3 – Public Color T2, T4 – Private Color

Overlay Management Protocol (OMP)



- Overlay Management Protocol (OMP)
- TCP-based extensible control plane protocol
- Runs between WAN Edge routers and Controllers 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

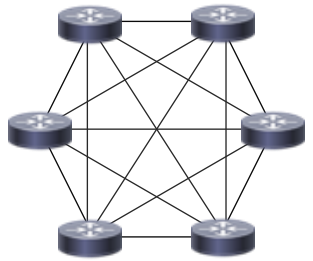
SD-WAN



O(n) Control Complexity

VS

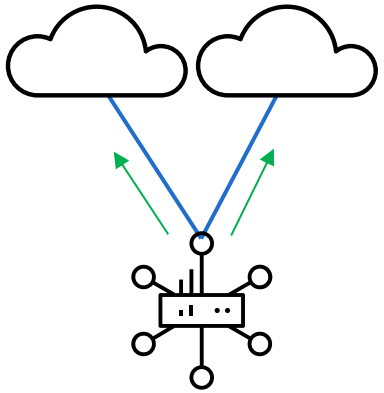
Traditional



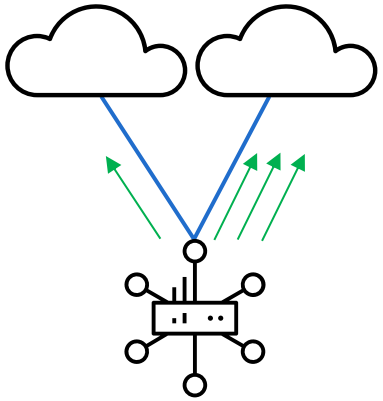
O(n^2) Control Complexity

Fabric Communication

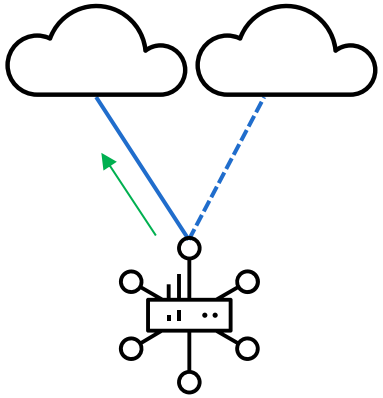
Per-Session Load-sharing
Active/Active



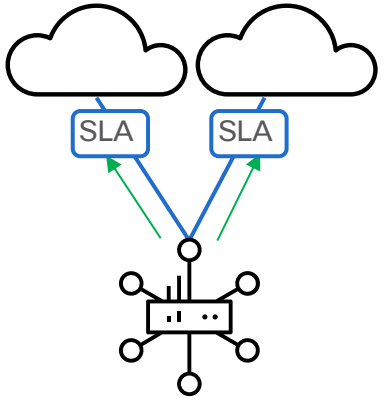
Per-Session Weighted
Active/Active



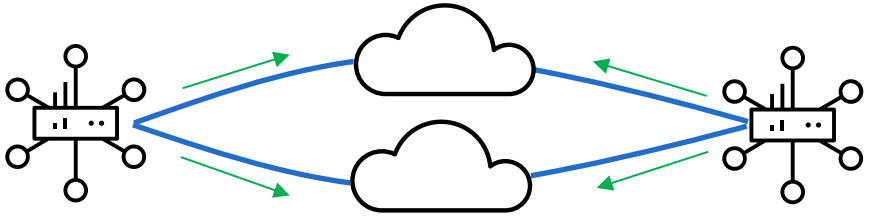
Application Pinning
Active/Standby



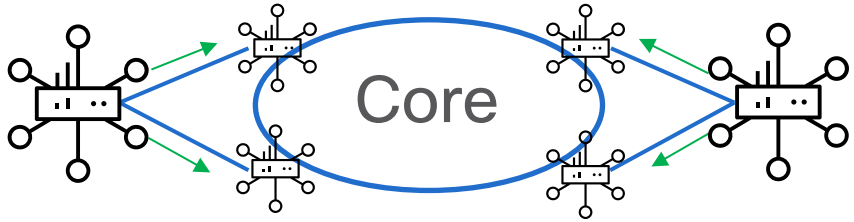
Application Aware Routing
SLA Compliant



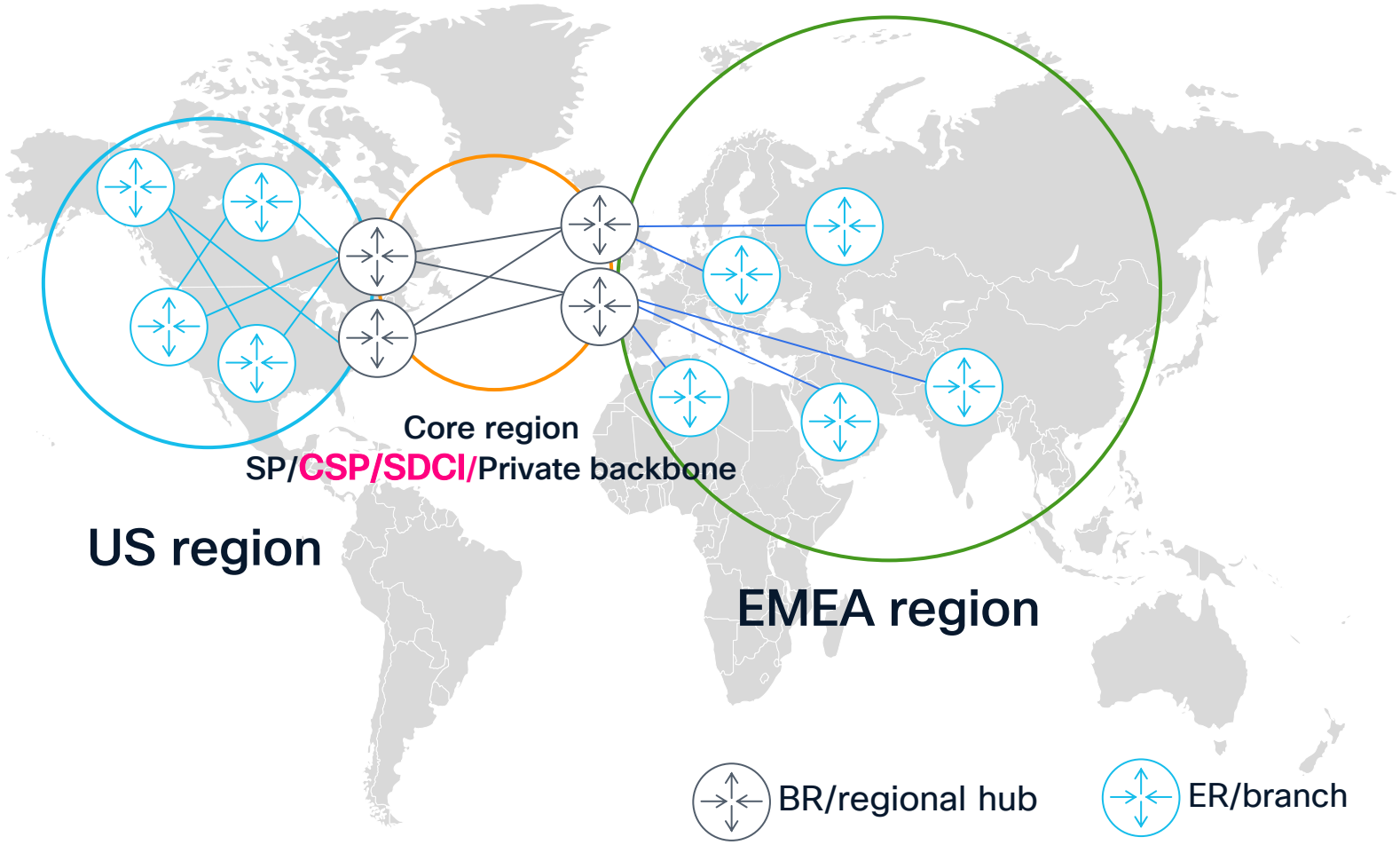
Single-hop Fabric



Multi-Region Fabric



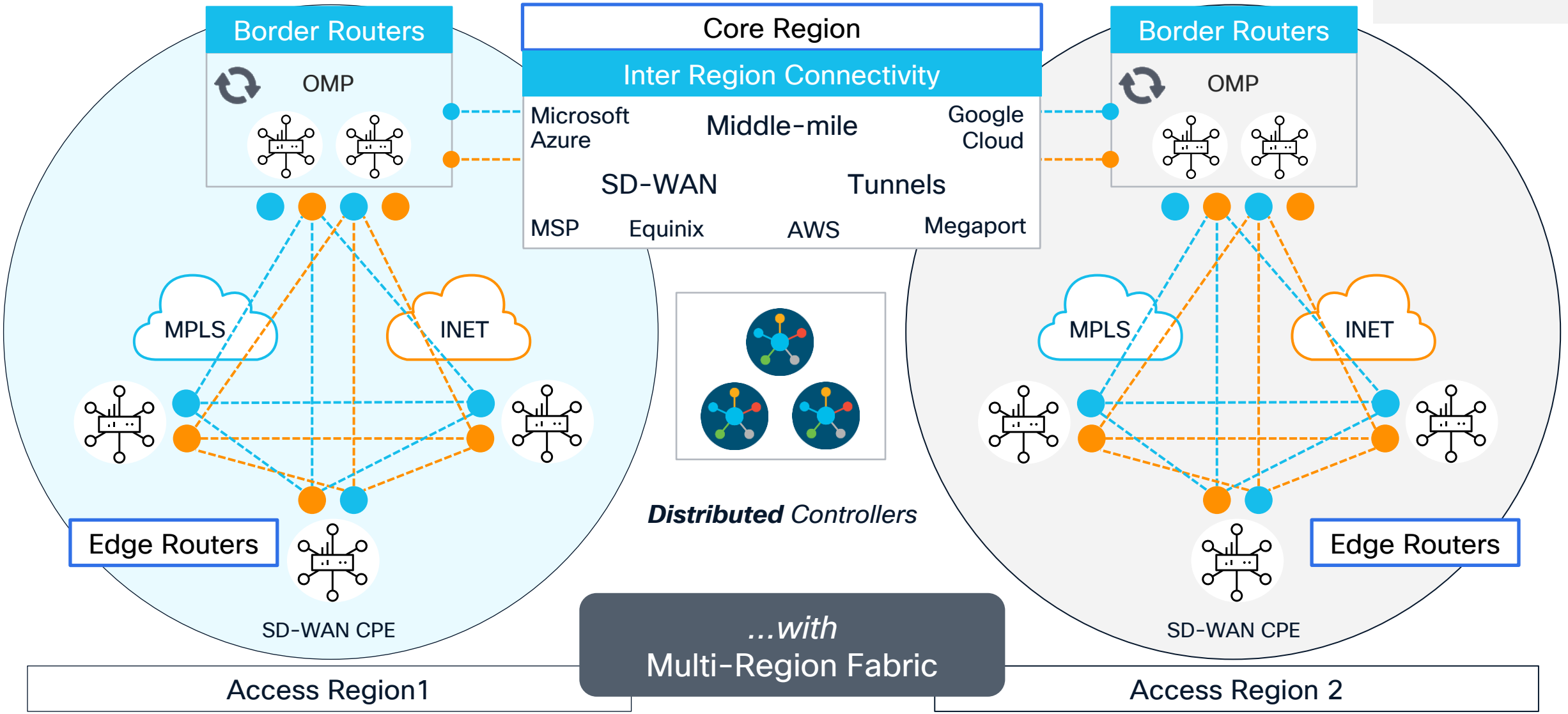
What is Multi Region Fabric (MRF)?



- Intuitive user-defined site grouping. E.g. based on geo
- Finer grouping using sub-regions
- Auto restrict overlay tunnels between regions
- Different topologies per region
- Mix access transports across regions
- Scale up control-plane per region(s)

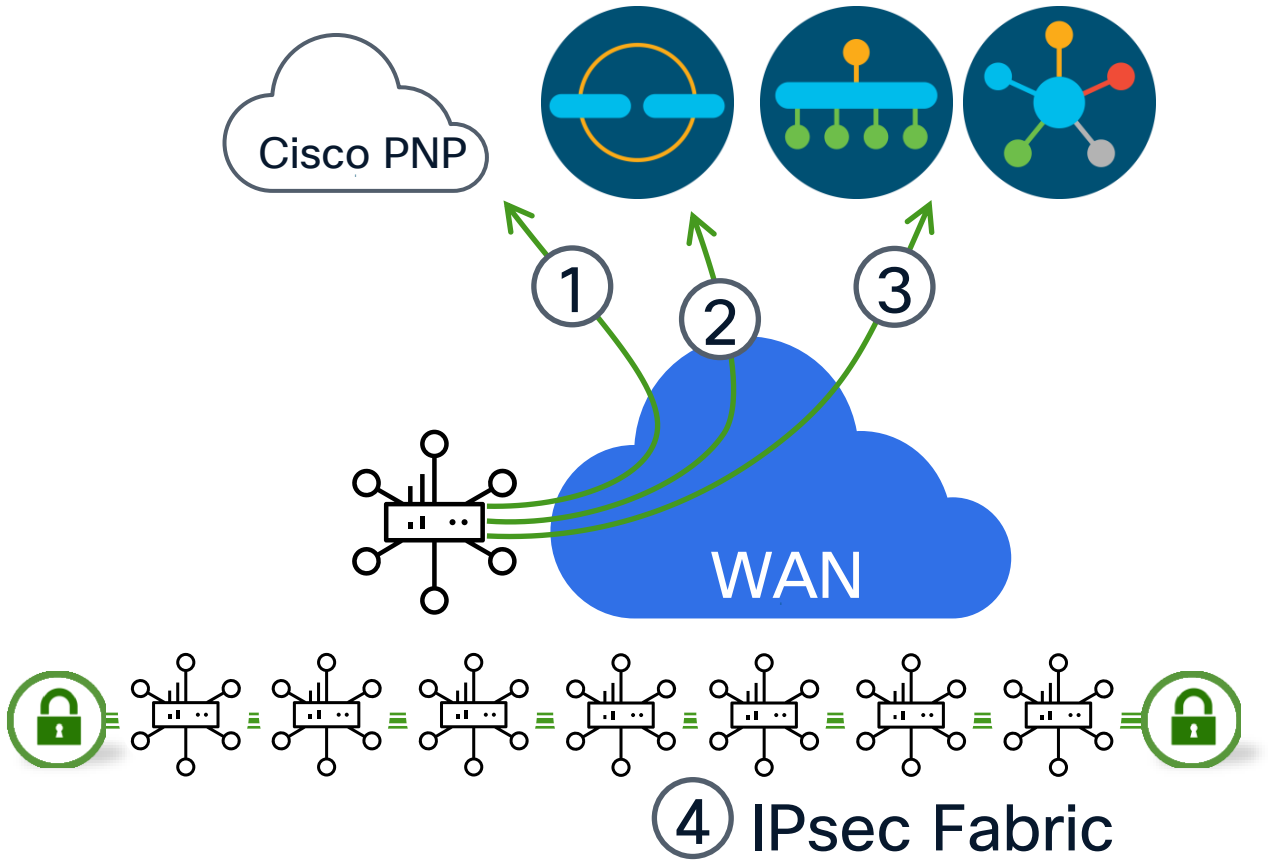
CSP = Cloud Service Provider (AWS, Azure, GCP)
SDCI = Software Defined Cloud Interconnect

The Network, with Multi-Region Fabric



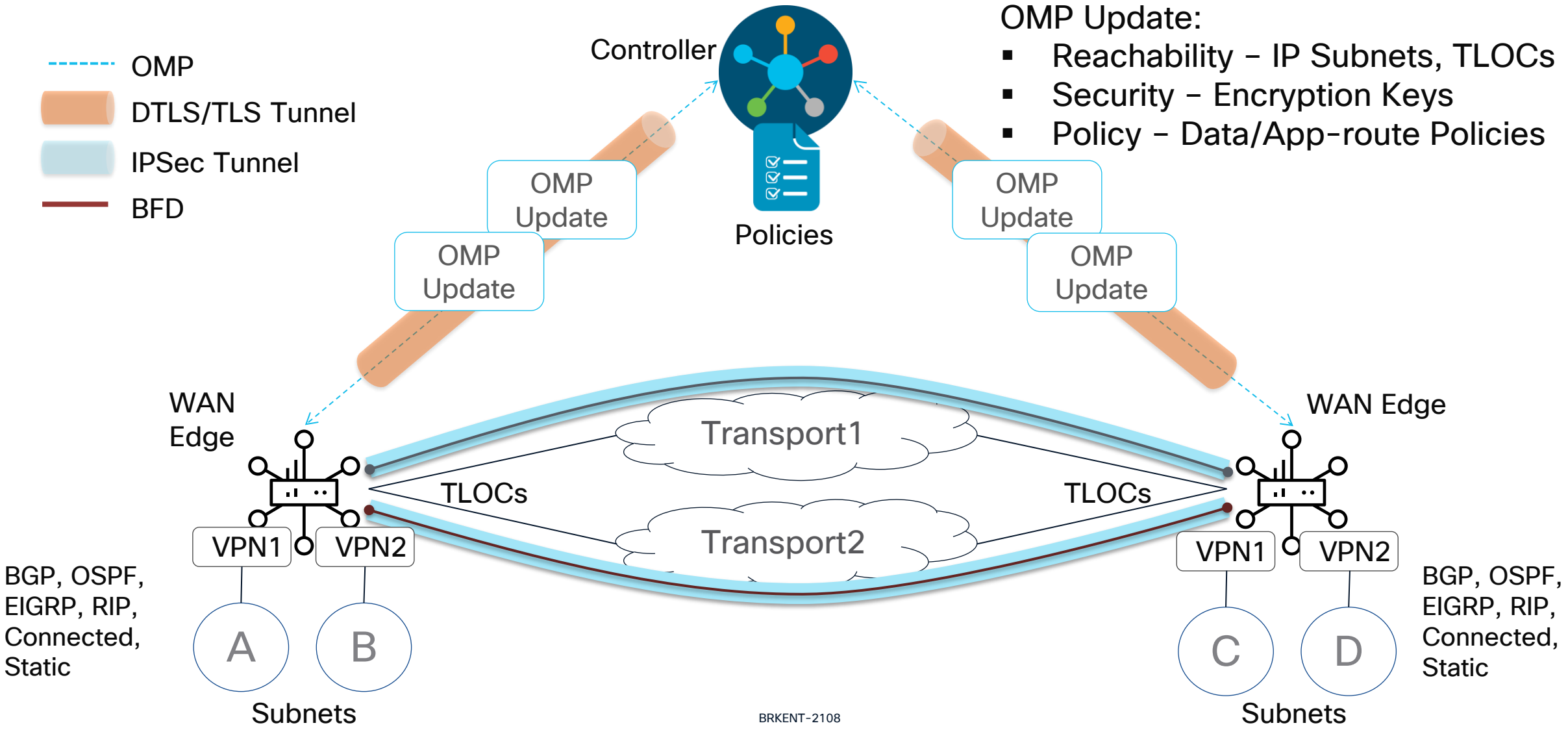
Let’s bring it up!

Automated, Zero-Touch Onboarding

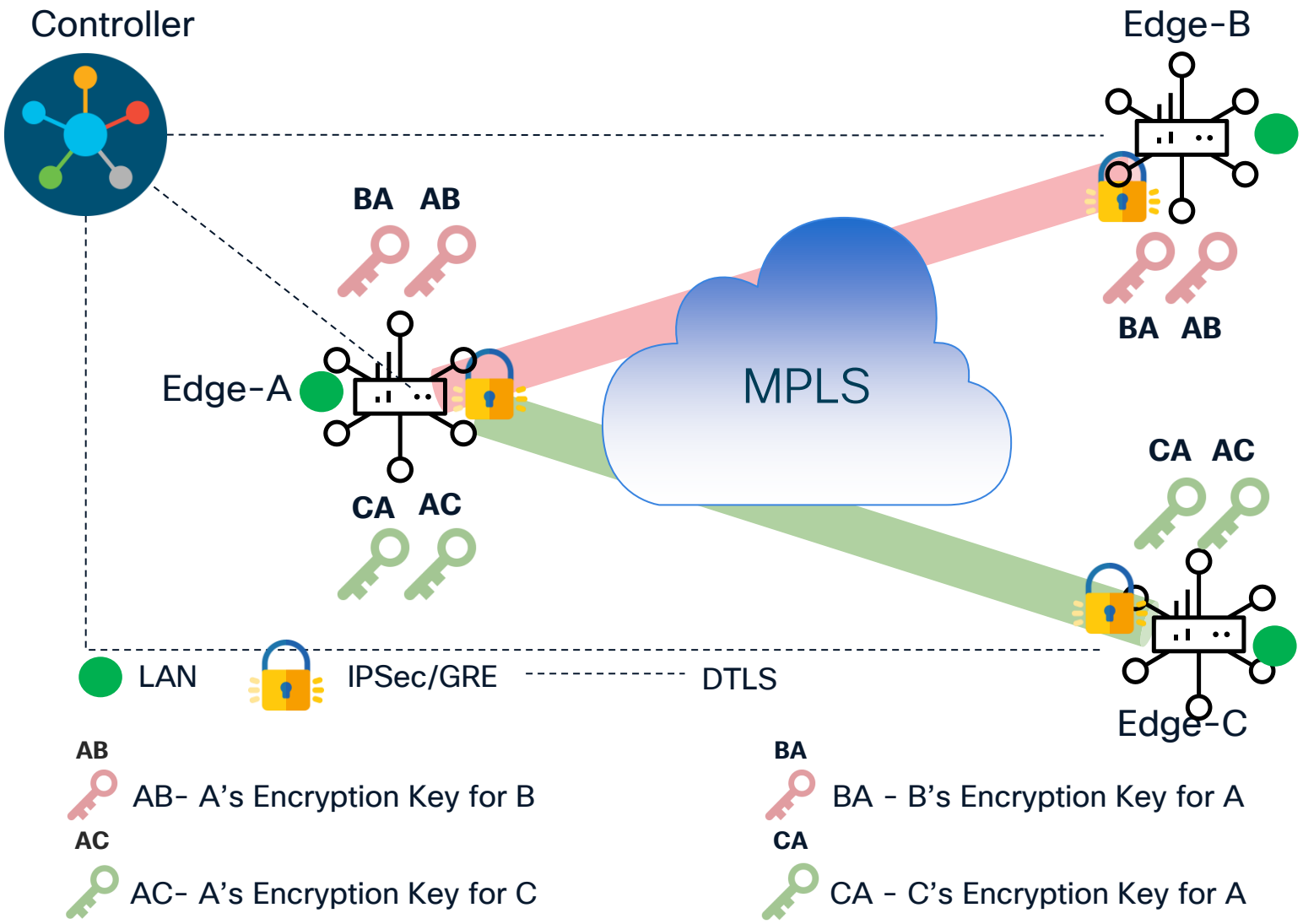


- SD-WAN Edge Router will onboard itself into the SD-WAN fabric automatically with no administrative intervention.
- Connect the SD-WAN Edge Router to a WAN transport that can provide a dynamic IP address, default-gateway and DNS information.
- If DHCP service is not available then, use the bootstrap file (on USB or Boot-flash)

Fabric Operation Walk-Through



Data Plane Privacy (Pairwise)

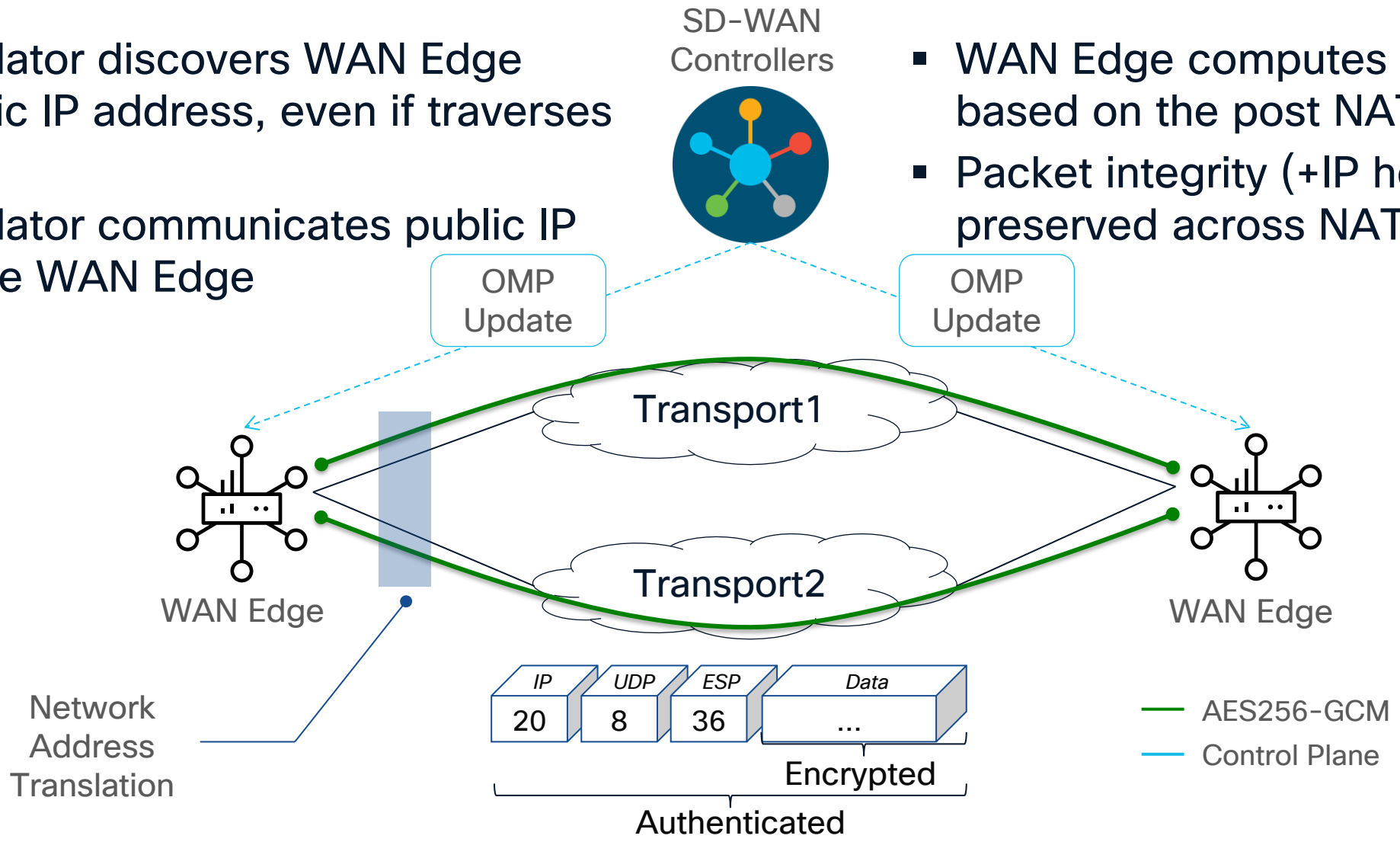


- Each WAN edge will create separate session key for each transport and for each peer
- Session keys will be advertised through Controllers using OMP
- When Edge-A needs to send traffic to Edge-B, it will use session key "AB" (B will use key "BA")

Data Plane Integrity

- Validator discovers WAN Edge public IP address, even if traverses NAT
- Validator communicates public IP to the WAN Edge

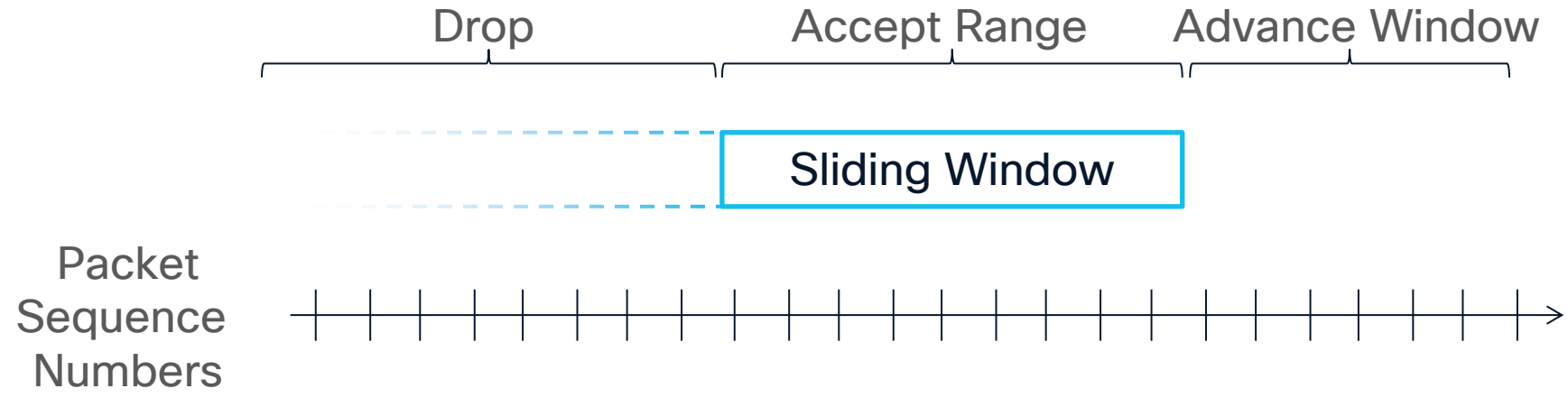
- WAN Edge computes AH value based on the post NAT public IP
- Packet integrity (+IP headers) is preserved across NAT



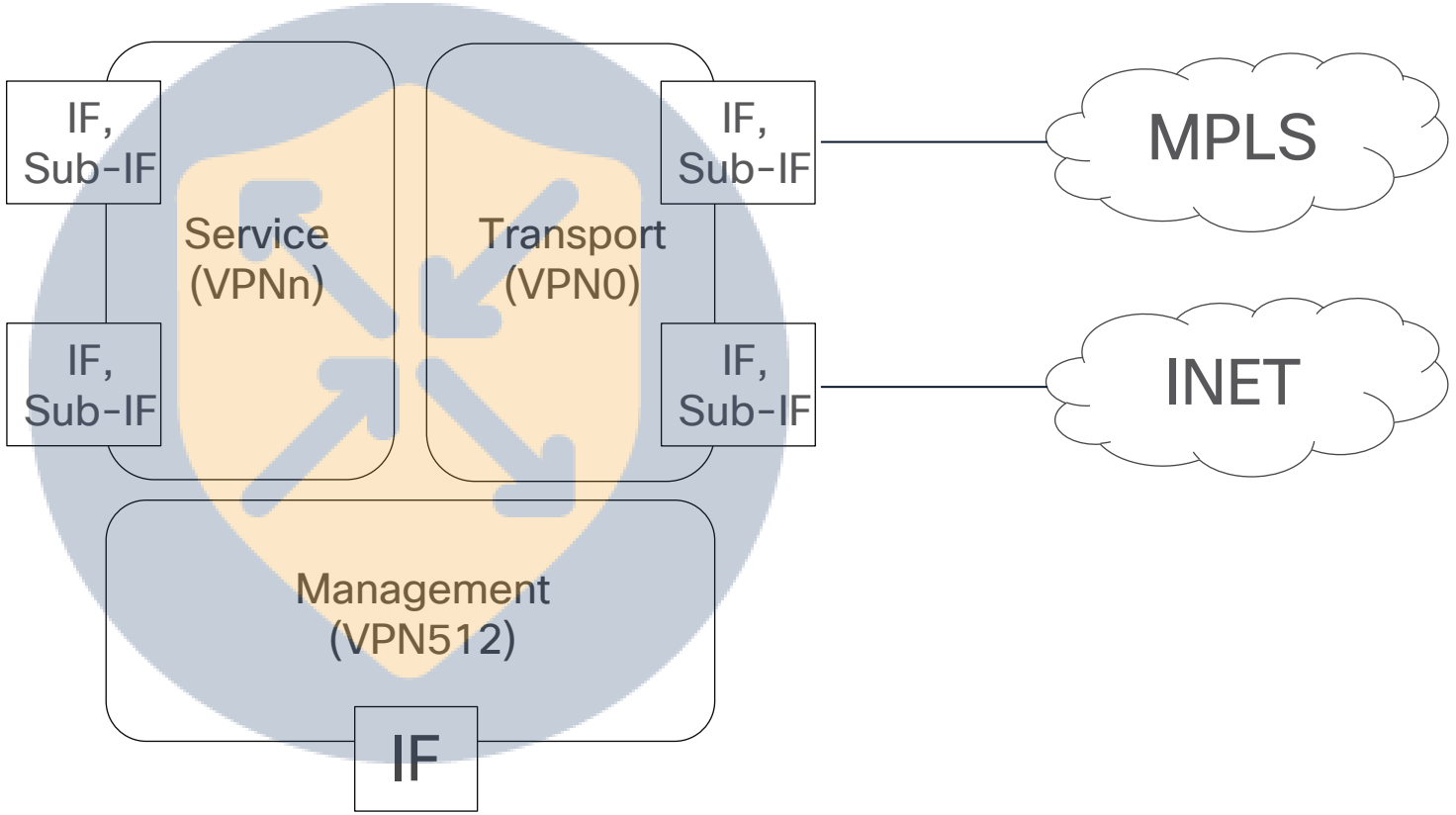
IPsec Anti-Replay Protection

FYI

- Encrypted packets are assigned sequence numbers. WAN Edge routers drop packets with duplicate sequence numbers
  - Replayed packet
- WAN Edge routers drop packets with sequence numbers lower than the minimal number of the sliding window
  - Maliciously injected packet
- Upon receipt of a packet with higher sequence number than received thus far, WAN Edge router will advance the sliding window
- Sliding window is CoS aware to prevent low priority traffic from “slowing down” high priority traffic



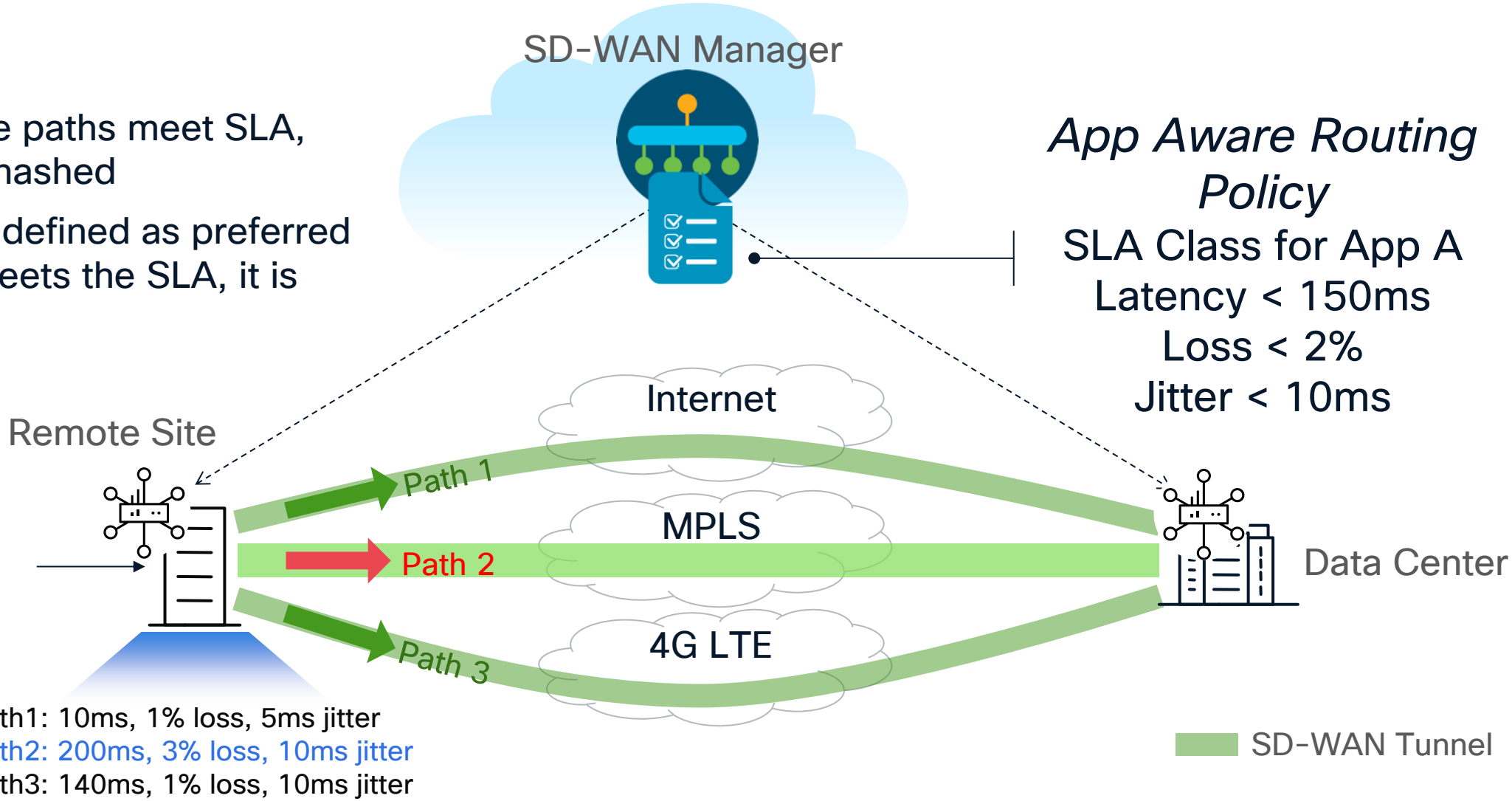
Cisco SD-WAN VPNs (VRFs)



- VPNs are isolated from each other, with each VPN has its own forwarding table
- Reachability within VPN is advertised by OMP
- VPN0 is reserved for WAN uplinks (Transport)
- VPN512 is reserved for Management interfaces
- VPNn represents user-defined LAN segments (Service)

Application Aware Routing

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

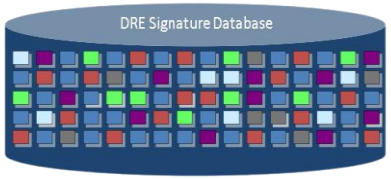


Key Building Blocks of AppQoE

Configuration Management System

SD-WAN Manager – Virtualized | Scalable | Network Insights

DRE, LZW



Byte Level Caching & Compression

Protocol Agnostic

Forward Error Correction

Packet Duplication

110 110
1011 1011
010 010
110 110
1011 1011
010 010

TCP Optimization

BBR2 Congestion Algorithm

Window Scaling

Large Initial Windows

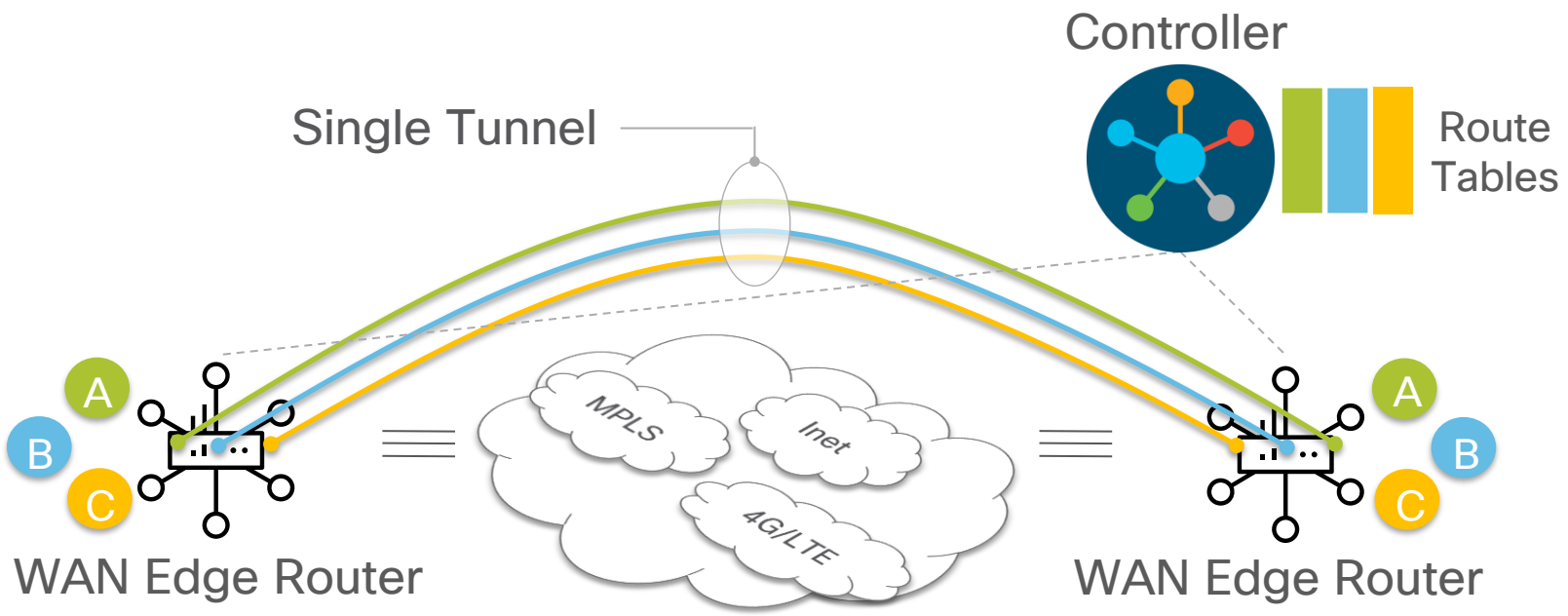
Selective Acknowledgement

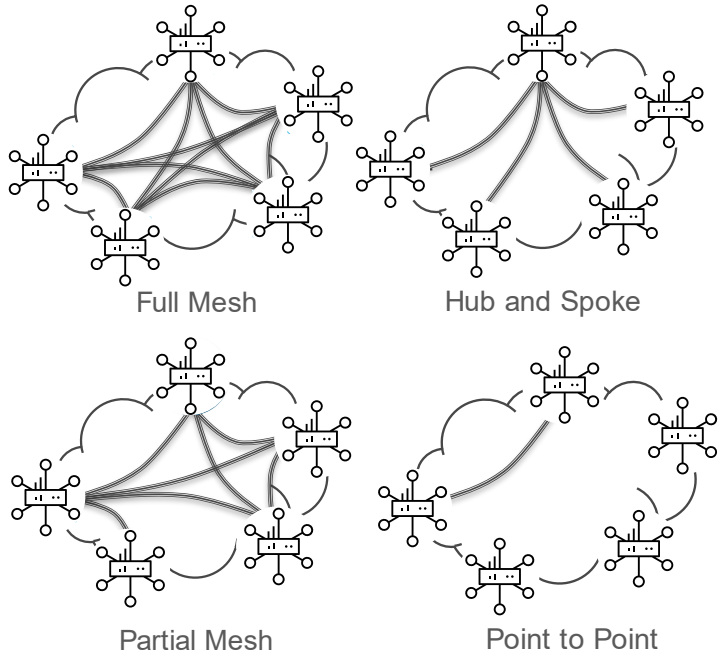
BBR – Bottleneck Bandwidth and Round-trip propagation time

cisco

Security features

End-to-End Segmentation with Multi-Topology



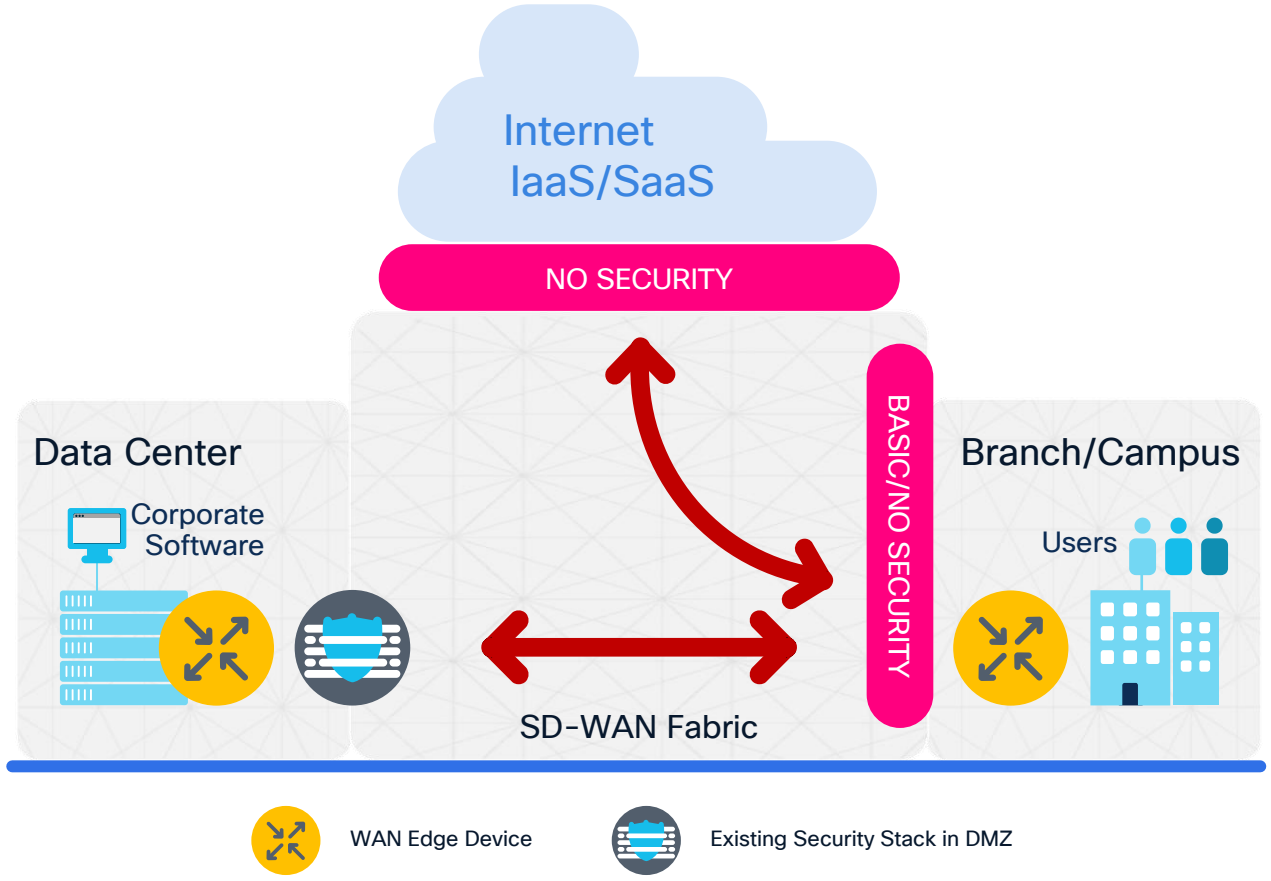


Segment connectivity across the SD-WAN fabric without reliance on underlay transport

WAN Edge routers maintain per-VPN routing table for complete control plane separation

cisco

How SD-WAN Exposes New Security Challenges



Internal & External Threats

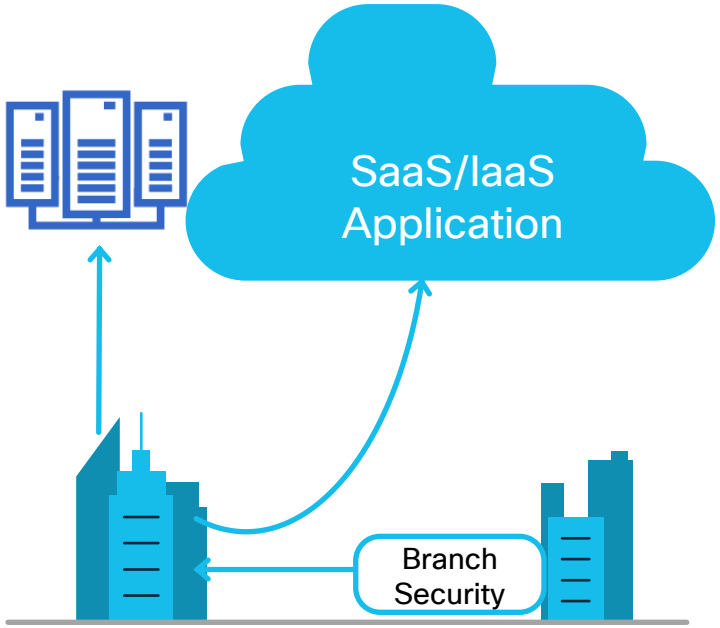
External

- Exposure to malware & phishing due to direct internet and cloud access
- Data breaches
- Guest access liability

Internal

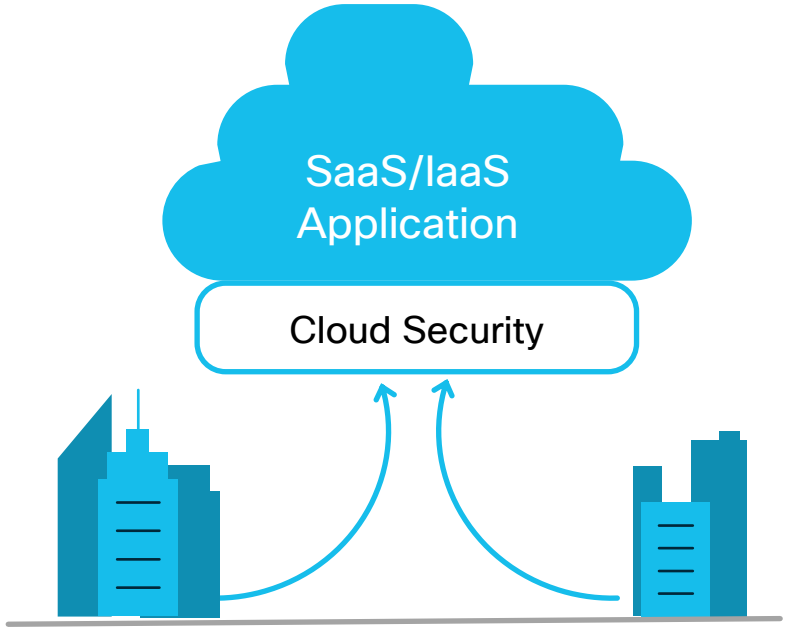
- Untrusted access (malicious insider)
- Compliance (PCI, HIPPA, GDPR)
- Lateral movements (breach propagation)

Relevant Security Models - Driving towards SASE



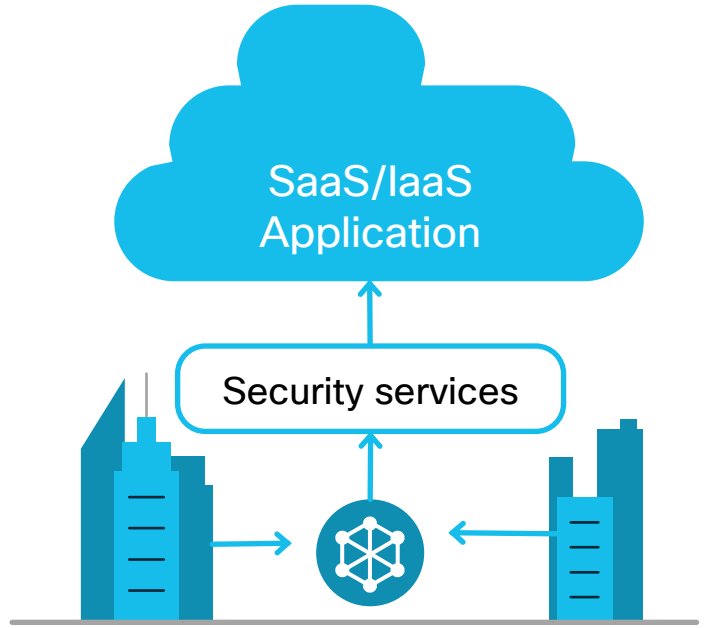
On-Prem Security

Thick branch with Routing and Security



Cisco Secure Access/SSE

Thin branch with security in the cloud



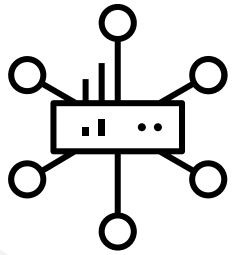
@Regional Hub

Security Services on a Regional Hub

Cisco Catalyst SD-WAN Security & SASE Solution

Consistent across on-prem and cloud

Cisco SD-WAN



> 8GB RAM

Cisco Security

Next-Generation Firewall
Layer 3 to 7 apps classified with User Identity

Intrusion Protection System
Most widely deployed IPS engine in the world

URL-Filtering
Web reputation score using 82+ web categories

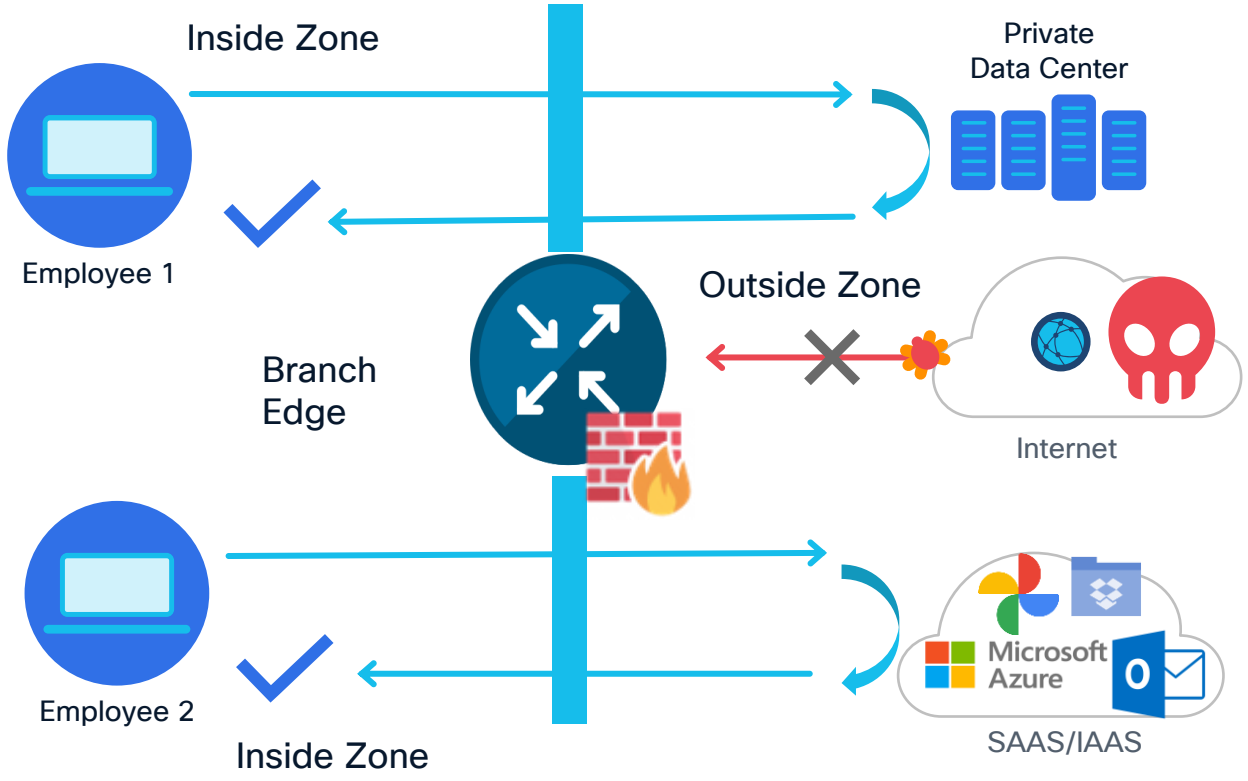
Adv. Malware Protection
With File Reputation and Sandboxing (TG)

SSL Proxy
Detect Threats in Encrypted Traffic

Cloud Security / SSE
DNS Security/Cloud FW with Cisco Secure Access

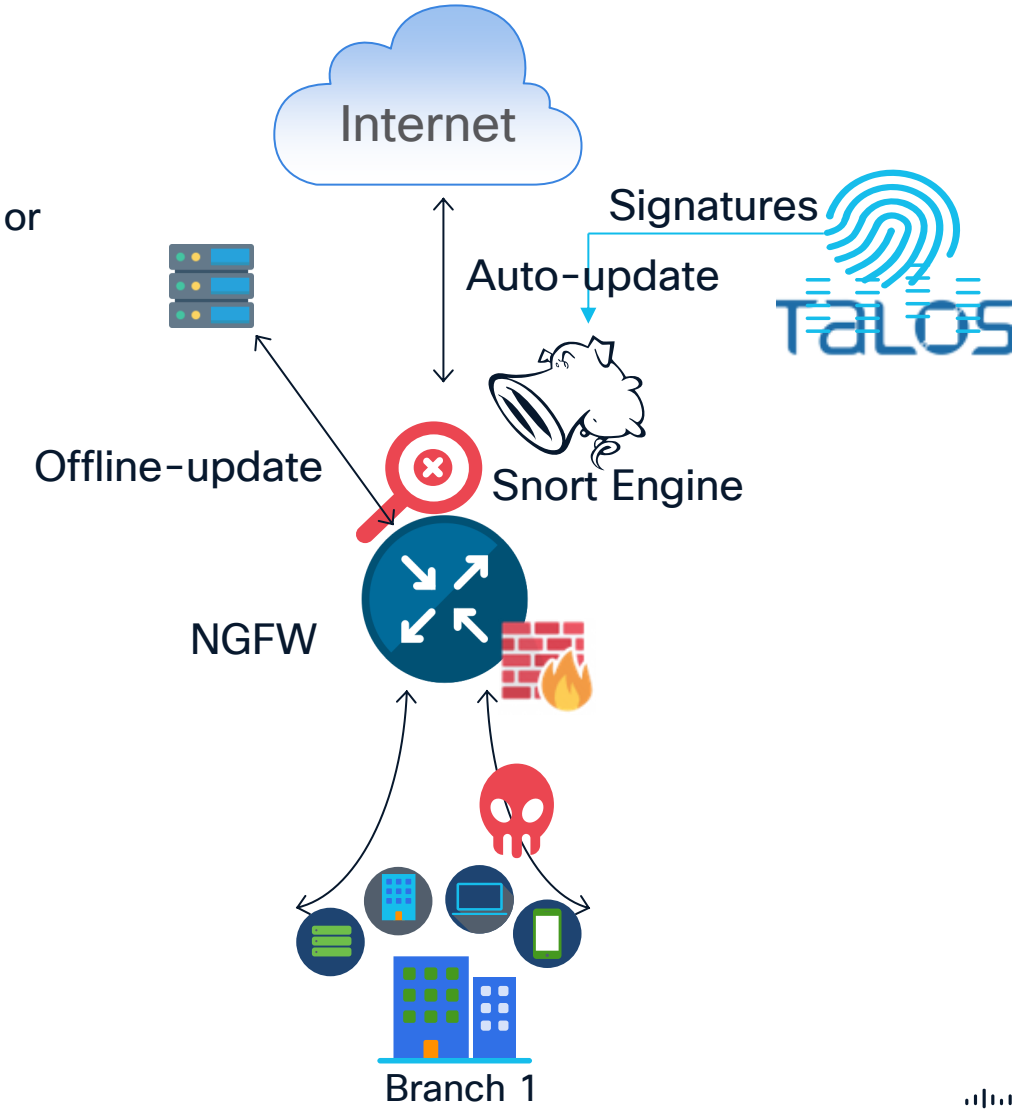
NGFW

- Stateful Firewall (TCP,UDP,ICMP)
- App-aware using NBAR2 / SDAVC (Layer 3-7 visibility), Custom-app
- VRFs / Interfaces as Zones
- Self-Zones/Default-Zones
- Policy based on IPv4/IPv6, Ports, Protocols, FQDN, GEO, SGTs, User / User-group and Applications
- HSL logging/Unified Logging (multiple collectors)
- Session re-classification, Flood attack prevention
- ALG support (FTP, TFTP, SIP etc.)
- Object-groups/Rule-sets support for scalable configs
- FW Action: Pass | Drop | Inspect along with sending for Advanced Inspection



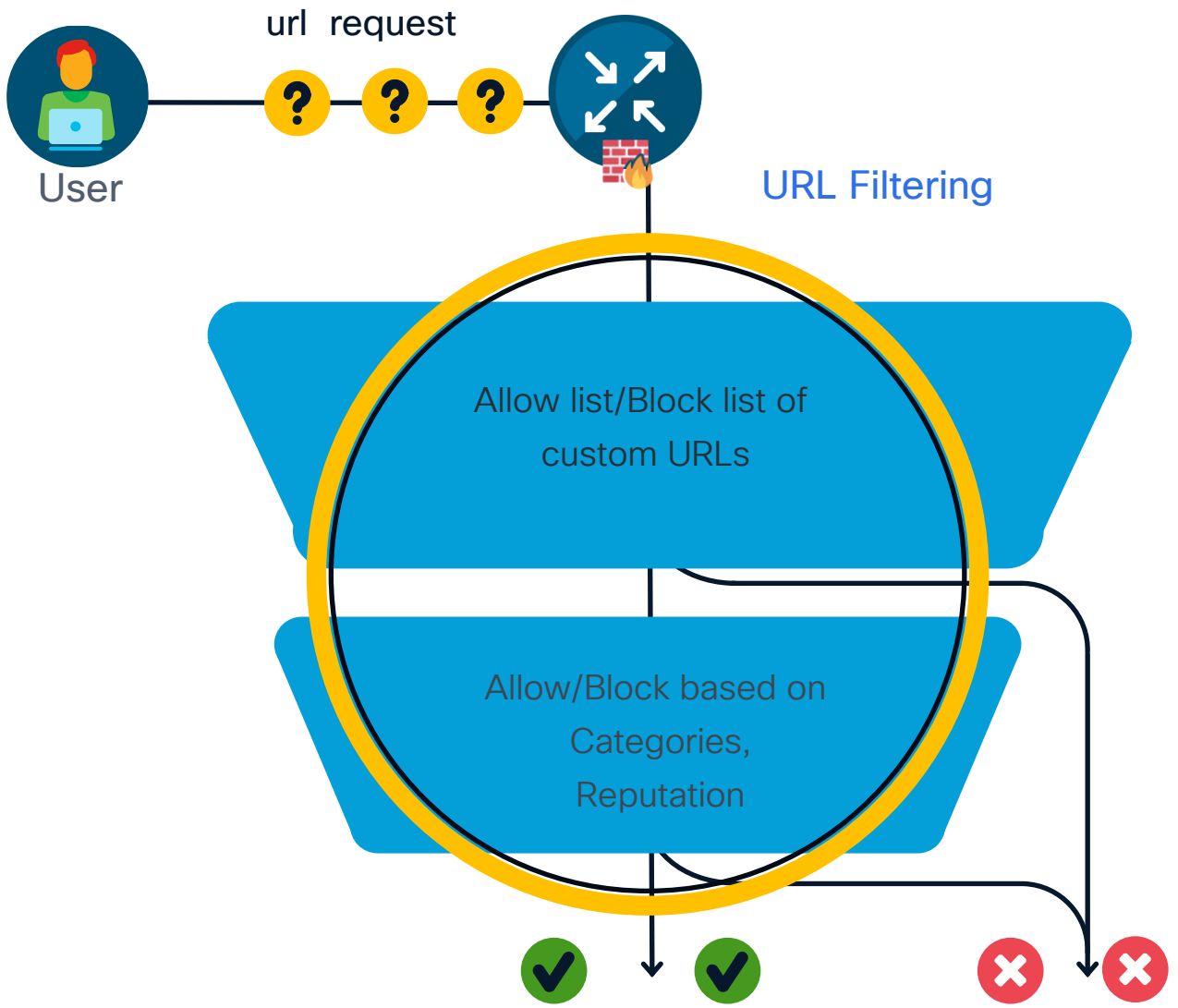
Intrusion Prevention/Detection System (IPS/IDS)

- Snort 3.0 – most widely deployed IPS engine in the world (better performance, ruleset coverage)
- IPS signatures (Talos) updated automatically by SD-WAN manager or using local-server for air-gap networks Security-levels
  - Connectivity
  - Balanced
  - Security
- Custom IPS Signature
- IPS Signature Allow list
- Notifications and Syslog



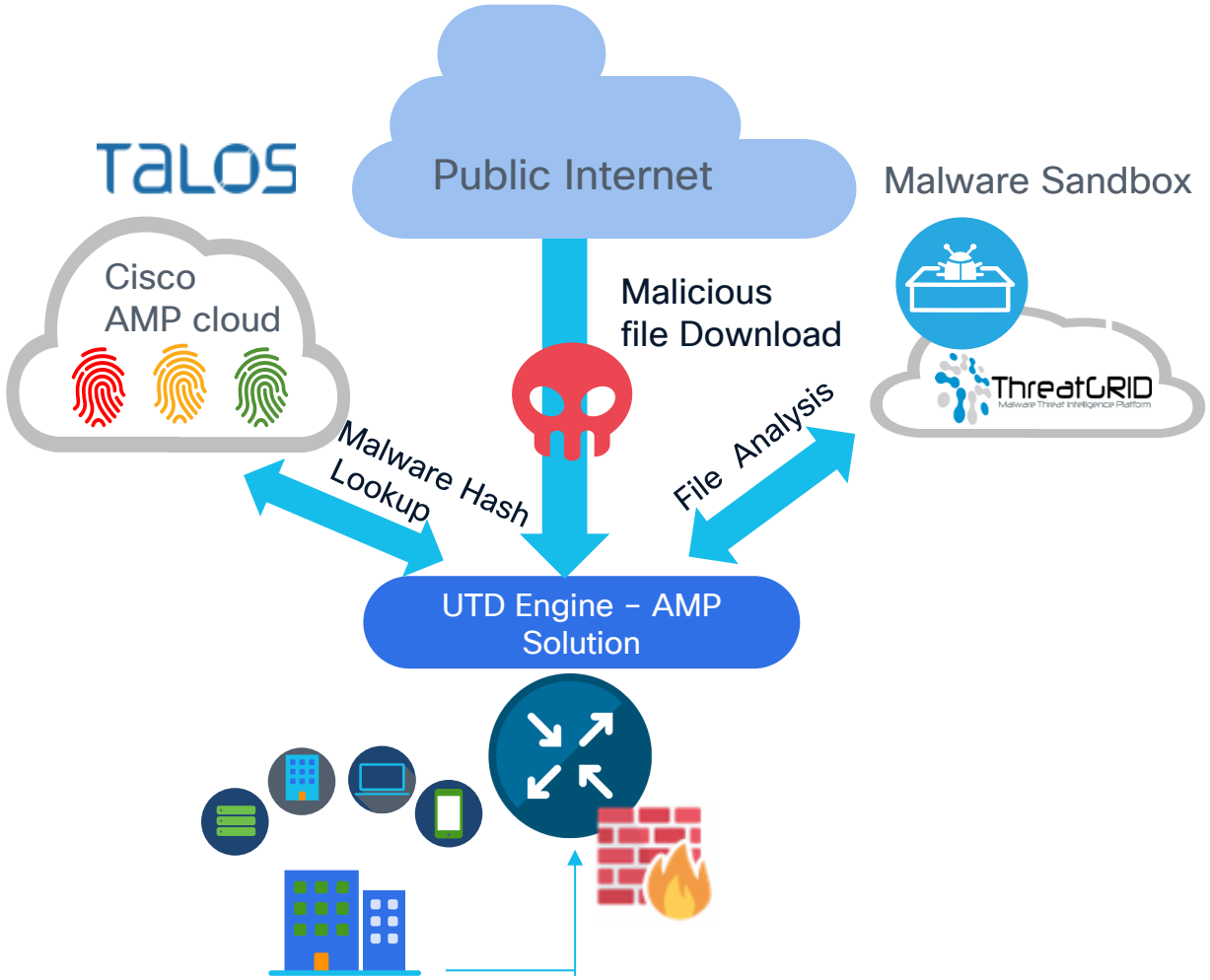
URL-Filtering

- Content filter of HTTP and HTTPs Traffic
- Utilizes Webroot Bright Cloud Web Classification and Web Reputation Service
- 82+ Web Categories and dynamic updates
- With URL-F feature enabled, order of process followed:
  - Allow lists of custom URLs
  - Block lists of custom URLs
  - Web Categories
  - Web Reputation Score
- Custom Regex based Allow and Block URL List
- Customizable End-user notifications – Block page or redirection
- Logging and Visibility



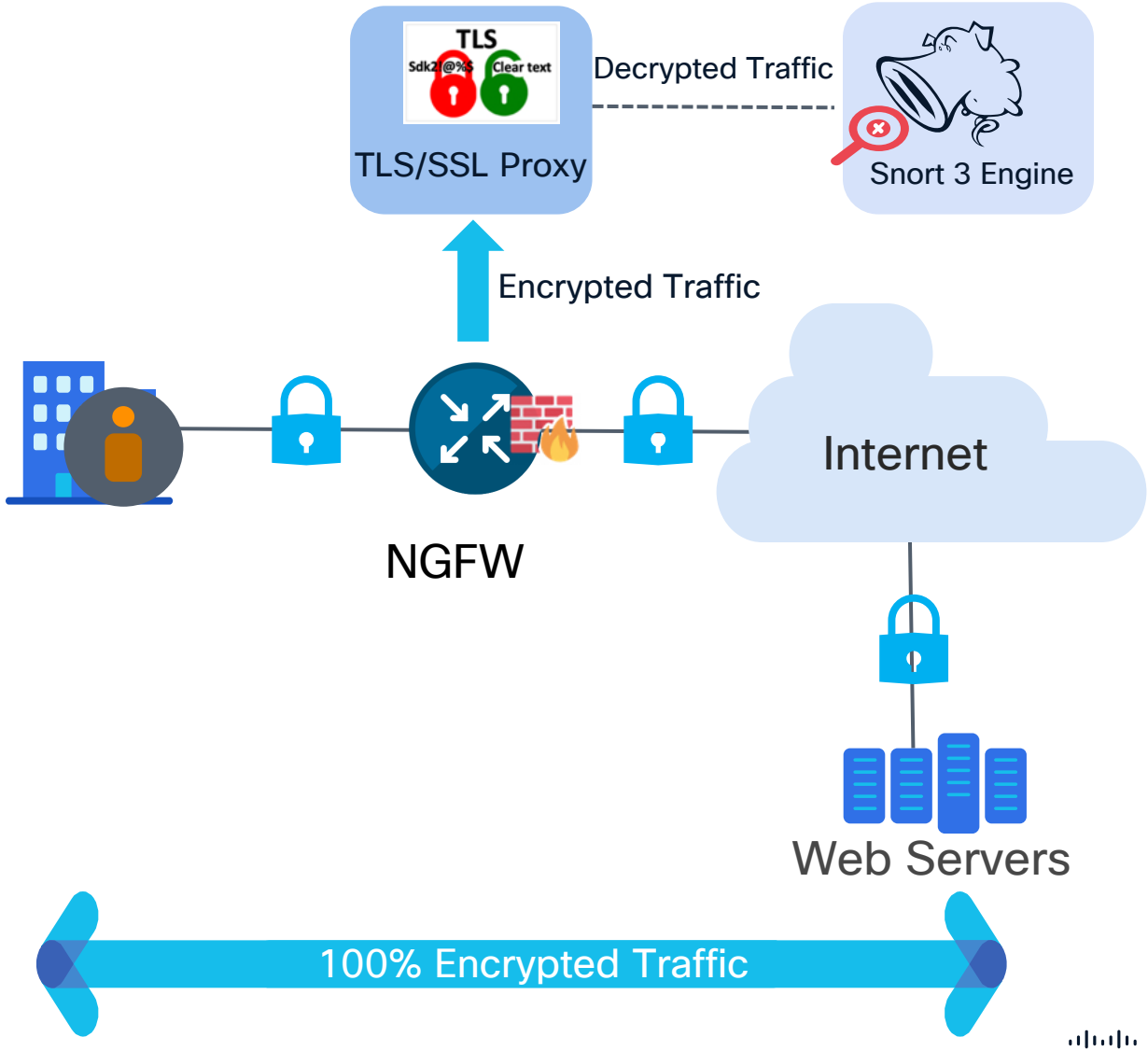
Advanced Malware Protection

- Integration with AMP Cloud
  - File Reputation
  - File Retrospection
- Integration with Threat Grid
  - File Analysis(sandboxing)
  - File Retrospection
- Customize log level



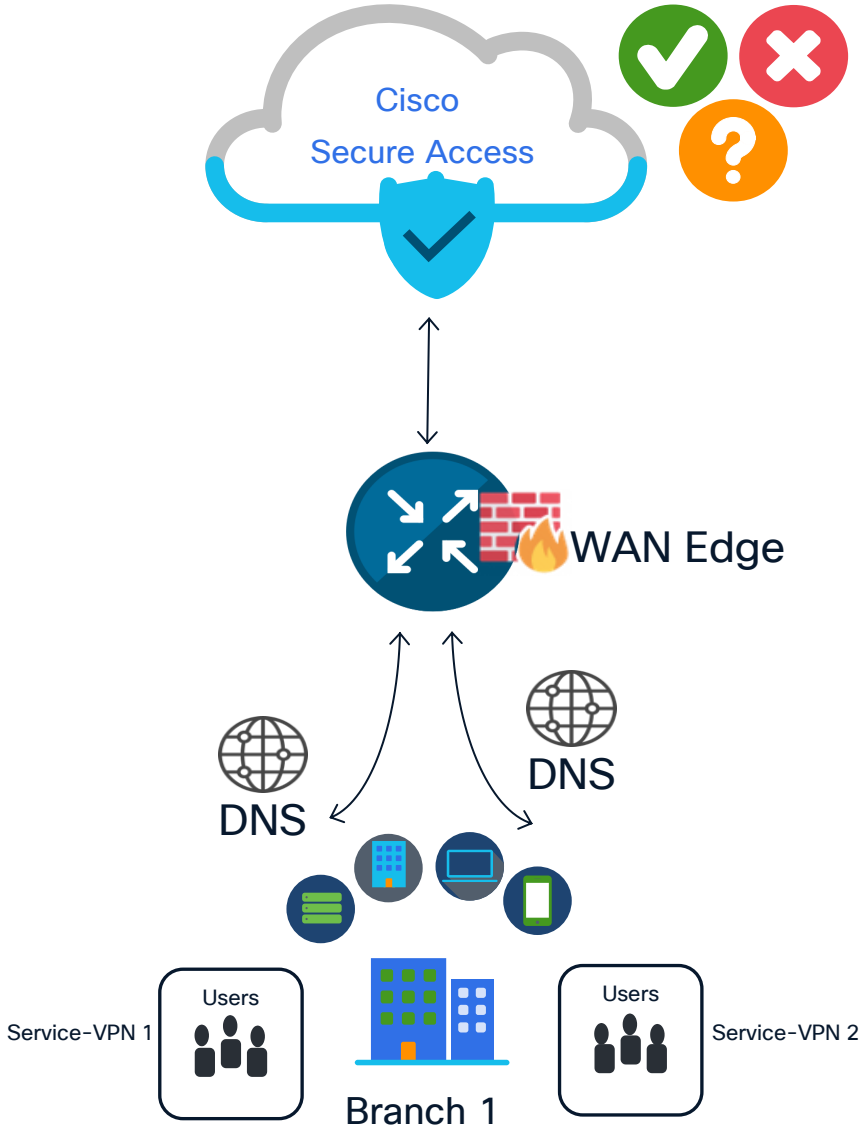
TLS/SSL Decryption

- TLS Proxy act as a Man in The Middle (MiTM)
- Proxy runs a Certificate authority
- Proxy generates Server certificates dynamically
- SD-WAN Manager can act as a Certificate Authority to automate Proxy certificates
- Policy based decryption
- URL Reputation/Categories can be excluded



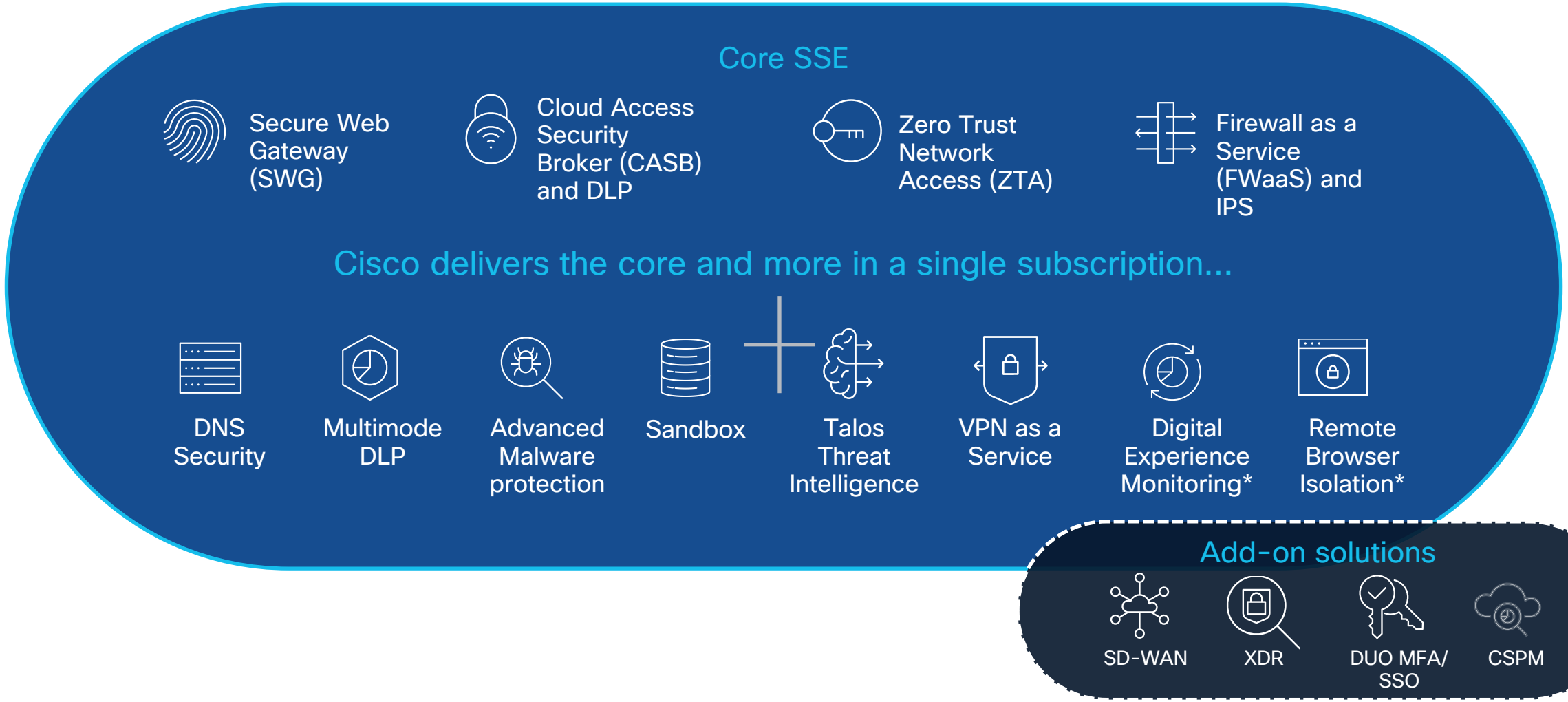
DNS Security

- Cloud-only DNS based inspection
- Automatic API Key registration
- VPN-aware policies
- Global points of presence (POP) and anycast IP for fastest response and high availability
- Block malware, phishing, and non-compliance domain requests
- Supports DNS-crypt
- Local Domain-bypass option



Cisco Secure Access

Go beyond core Secure Service Edge (SSE) to better connect and protect your business

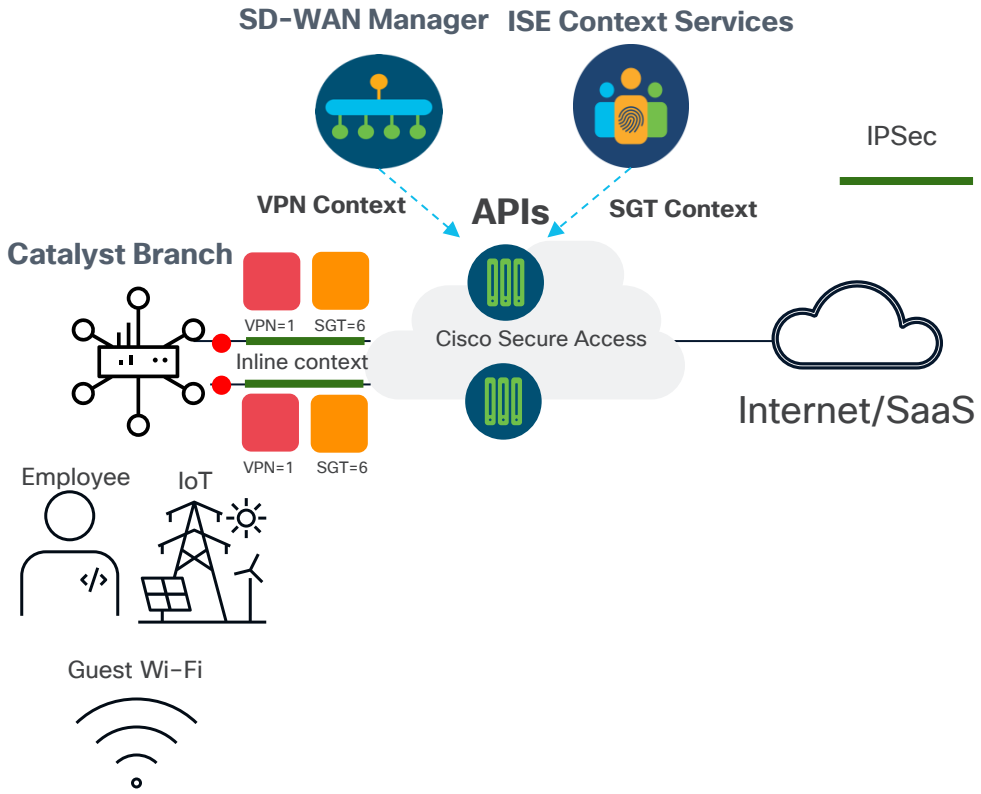


Cisco Catalyst WAN – Secure Access – Today

Use Case	Secure Internet/SAAS Access from Catalyst Branch
Catalyst Edge	• Automated connectivity with Auto/manual Region selection • Controller-Based Automation Framework • Robust Reliability with 8 Active/8 Backup Tunnels • Application Assurance and Tracking • Advanced traffic steering and monitoring • SD-Routing Support

Catalyst SD-WAN - Cisco Secure Access Context Sharing

Context-aware security is key for implementing and achieving a true zero-trust framework for an enterprise.



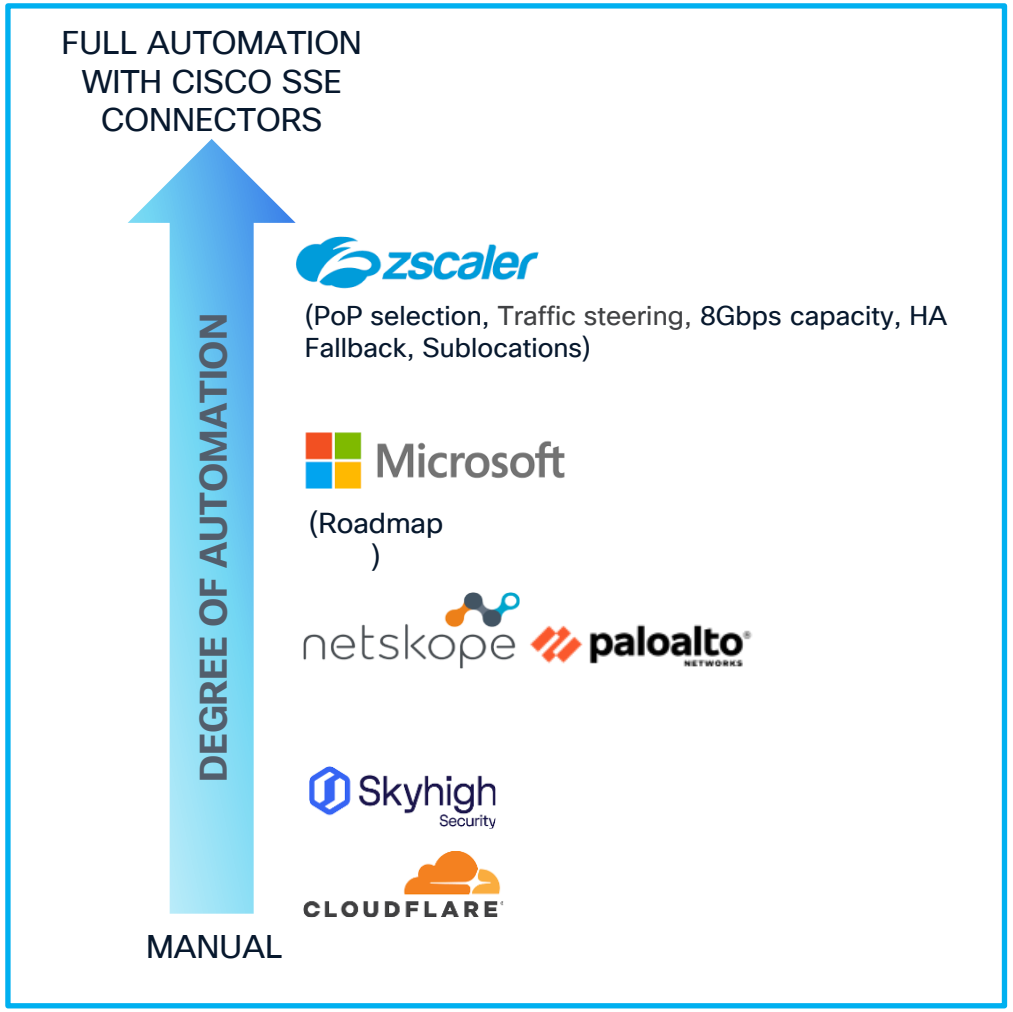
- **Catalyst SD-WAN will share enterprise context with Cisco Secure Access**
- **Part of the efforts to share end-end context across the enterprise with Cisco-on-Cisco solutions**
- **Competitive differentiator for Cisco**
- **Both Macro(VPN-ID) and Micro (SGT) segmentation support**
- **Granular but simplified security policy control on Cisco Secure Access for catalyst branches accessing internet/SAAS apps**

Employee, Guest and IOT segments behind a Catalyst Branch securely accessing Internet/SAAS with differentiated policy enforcement by Cisco Secure Access.

Multi-Vendor SSE Integrations

900+ customers love the flexibility and interoperability that Cisco SD-WAN offers

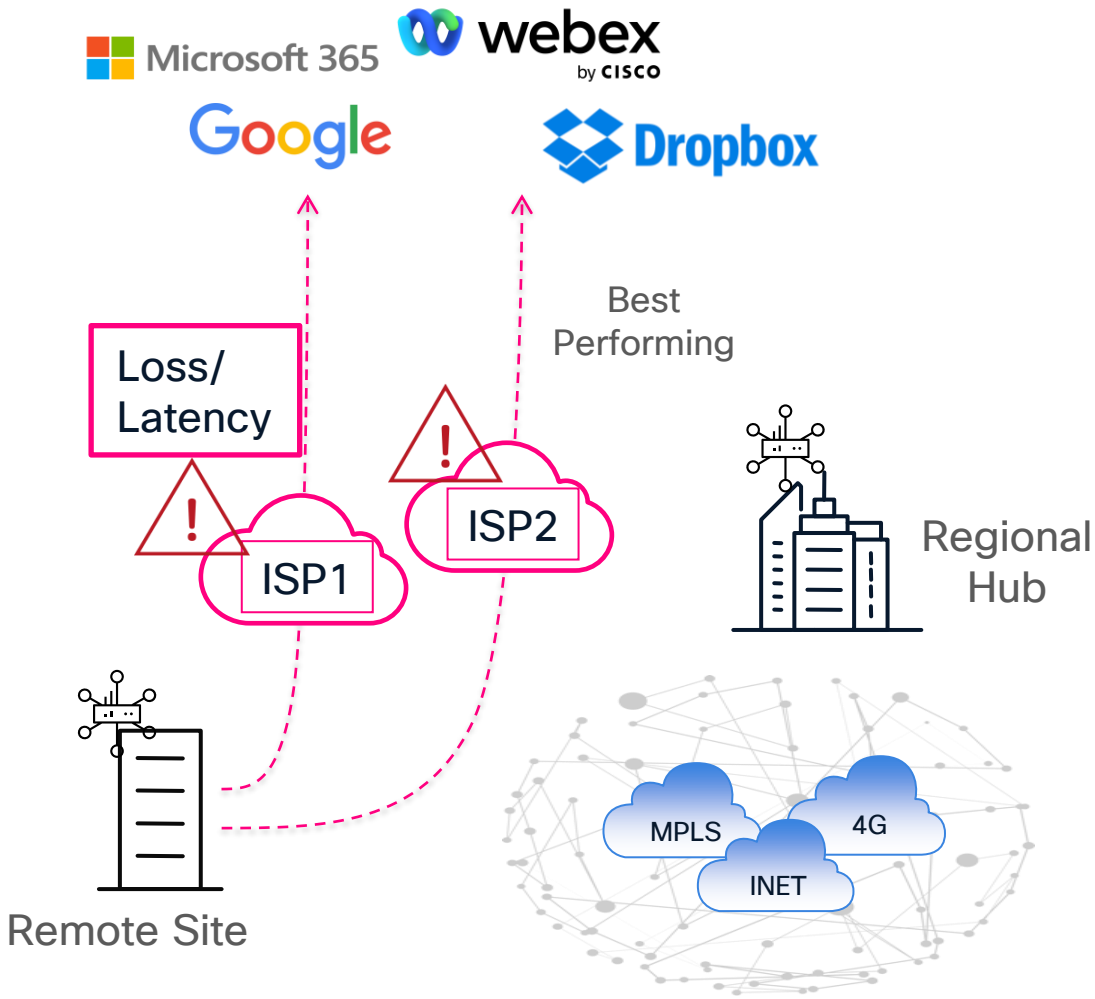
- Dashboard & API based automation
- IPSec / GRE tunnel automation and PoP selection
- Resiliency with fallback and application health check
- Granular traffic redirection
- Segmentation



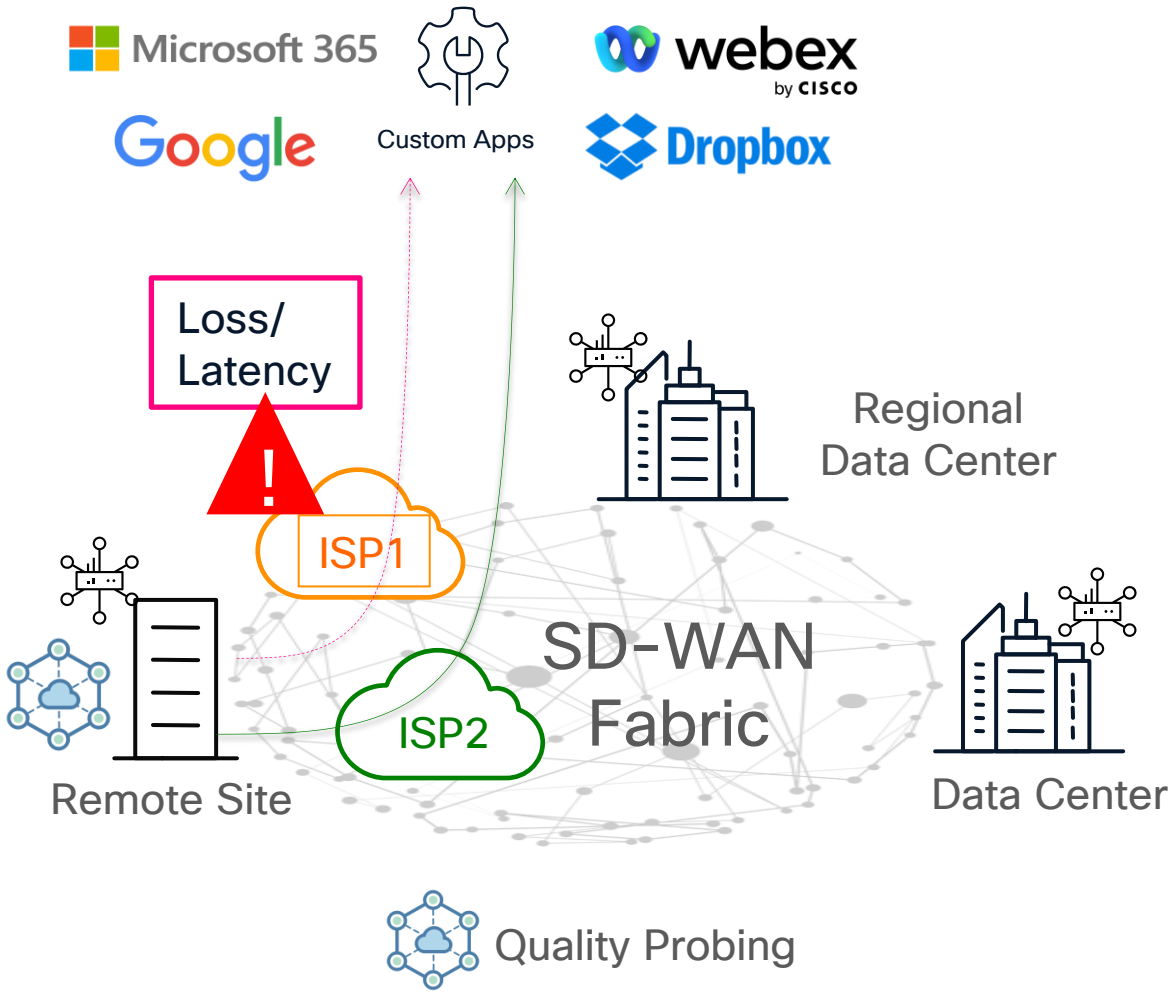
Cloud OnRamp for SaaS

SaaS Optimization Challenges

- Internet circuits performance is unreliable.
- How to get performance visibility for each available path?
- When specific path is having performance issues, How to automatically steer traffic ?

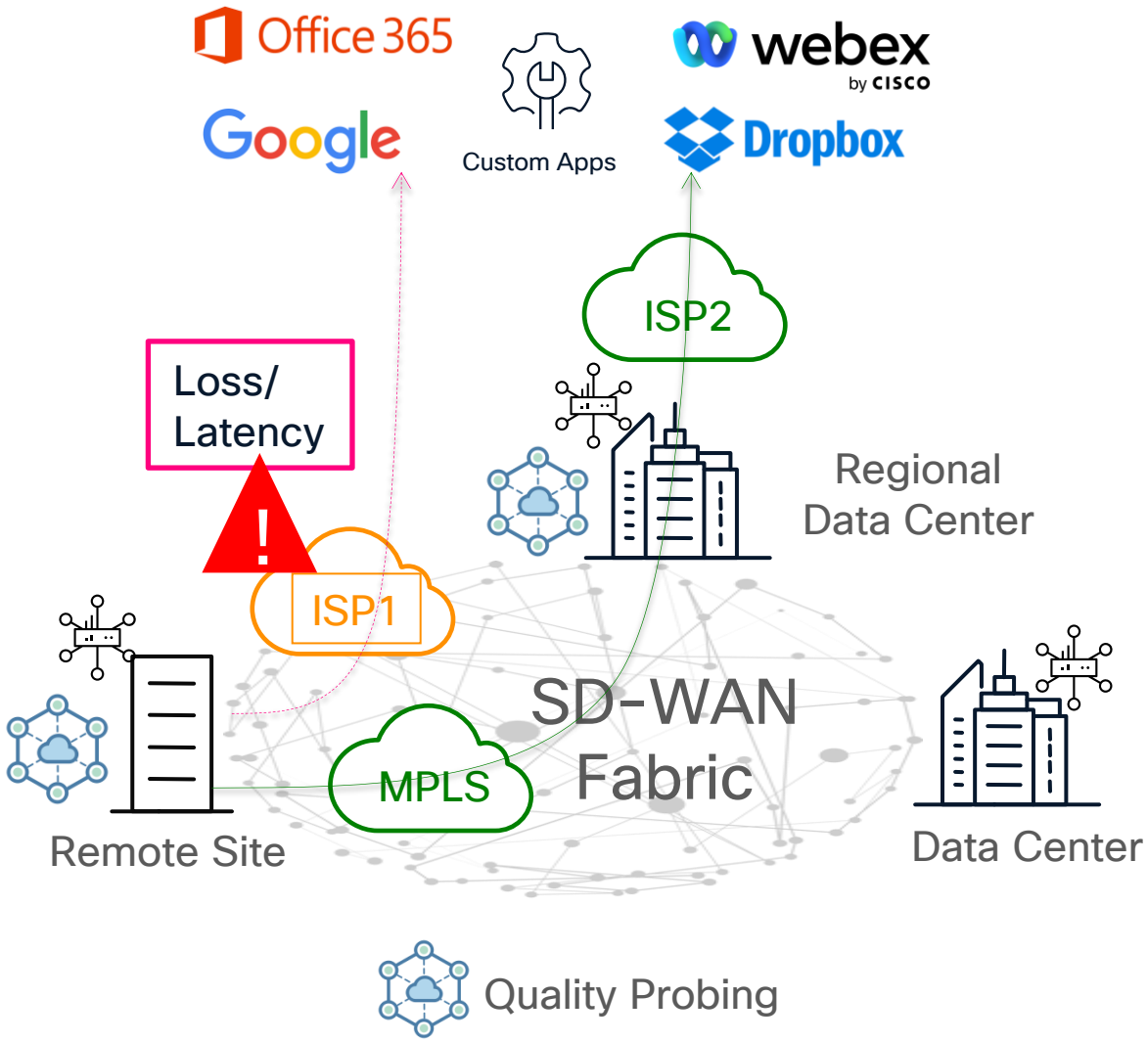


Cloud onRamp for SaaS – Internet DIA



- WAN Edge router at the remote site performs quality probing for selected SaaS applications across each local DIA exit
  - Simulates client connection using HTTP ping
- Results of quality probing are quantified as vQoE score (combination of loss and latency)
- Local DIA exit with better vQoE score is chosen to carry the traffic for the selected SaaS application
  - Initial application flow may choose sub-optimal path until DPI identification is complete and cache table is populated

Cloud onRamp for SaaS – Regional Gateway



- Wan Edge routers at the remote site and regional hub perform quality probing for selected SaaS applications across their local Internet exits
  - Simulate client connection using HTTP ping
- Results of quality probing are quantified as vQoE score (combination of loss and latency)
  - HTTP ping for local DIA and App-Route+HTTP ping for regional Internet exit
- Internet exit with better vQoE score is chosen to carry the traffic for the selected SaaS application
  - Initial application flow may choose sub-optimal path until DPI identification is complete and cache table is populated

Cloud OnRamp for MultiCloud

Use Cases

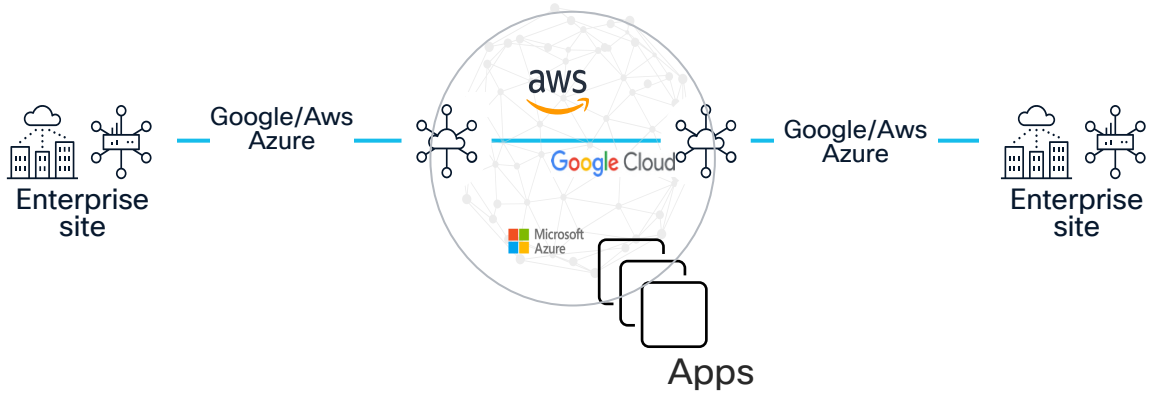
Cisco Catalyst SD-WAN offers simplified connectivity with fabric extension to cloud providers.

= Cisco SD-WAN virtual router hosted at Cloud Service Provider POP

= Cisco SD-WAN router on-premises

Enterprise Site to Cloud

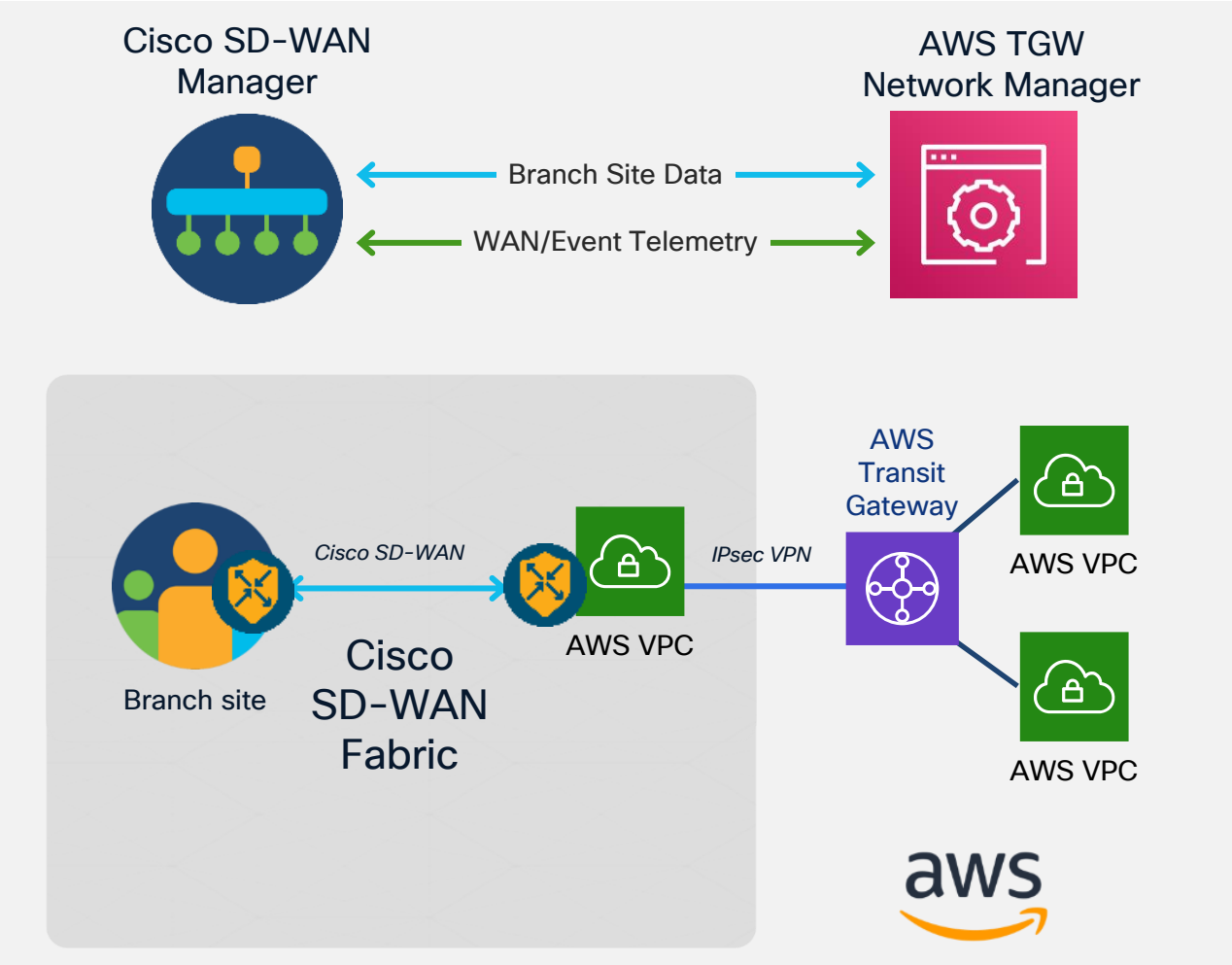
Enterprise Site to Enterprise Site



Cloud to Cloud/Inter-Cloud

It builds a programable site-to-cloud, site-to-site, region-to-region and cloud to cloud connectivity using the cloud providers' native constructs and backbone

Extending SD-WAN into Public Cloud (AWS as example)



Benefits

- Automated provisioning of SD-WAN Transit VPC and TGW, route exchange for site to cloud and site to site traffic over AWS backbone
- Full Visibility into inter-regional transit traffic and telemetry with TGW Network Manager
- Consistent Policy and Segmentation across branch and cloud for enterprise class security

Automation (CSP-generic)

FYI

Different Automation options:

- Cloud OnRamp (CoR) for Multicloud Automation built in the Manager
- Automation with 3rd party tools like Terraform and Ansible

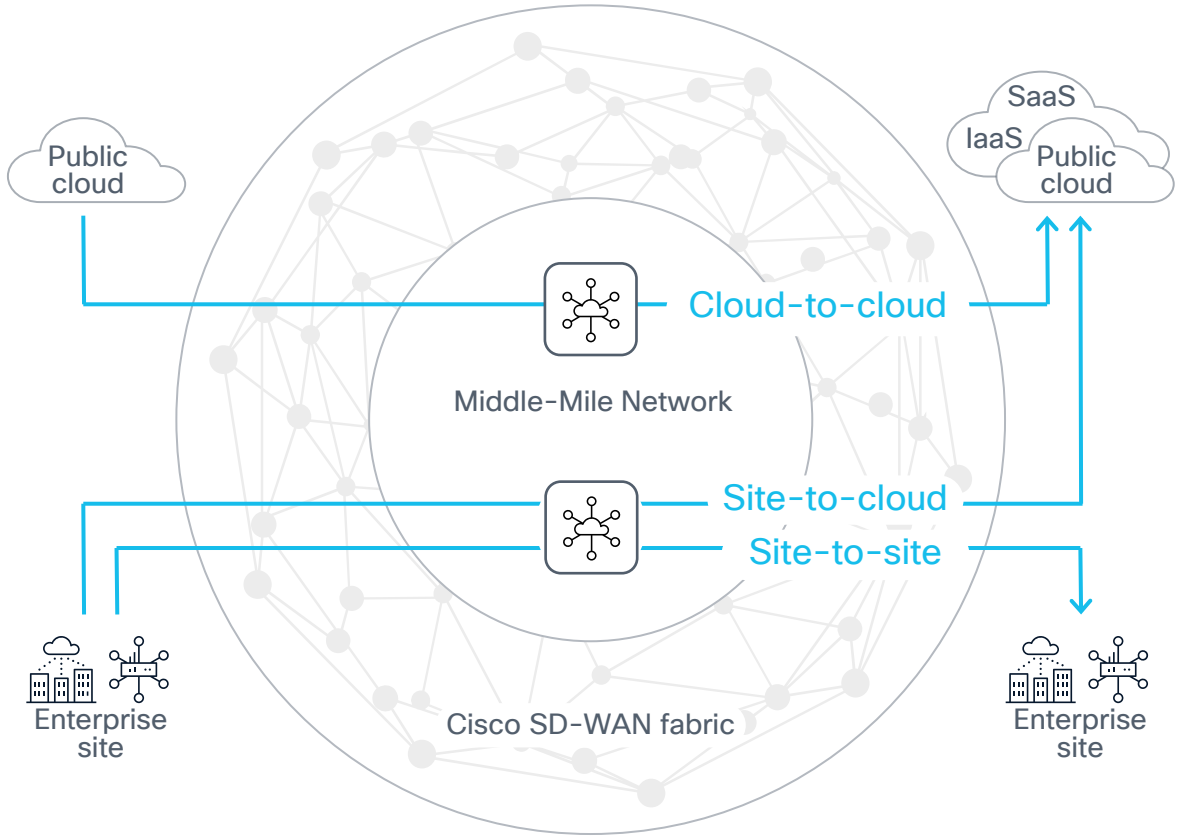
	Pros	Cons
Cloud OnRamp Automation	• Single UI in Manager for the whole workflow • Discovers host VPCs/VNETS and connects public-cloud with SD-WAN within minutes	• Not possible to add own customization for design changes i.e., virtual firewall • No built-in auto scale capabilities (yet)
Custom Automation	• Will do exactly what customer wants • Can be changed in case of any design changes	• Takes time and money to develop and test (customer, Cisco CX or Partner)

Cisco SD-WAN Middle-Mile Optimization

Megaport · EQUINIX · aws Cloud WAN · Google Cloud NCC · Microsoft Azure

= Cisco SD-WAN virtual router

= Cisco SD-WAN router on-premises



Flexibility
All or selective traffic sent based on type or app

Reliability
Reliable, high-speed connectivity between sites

Security
End-to-end encryption over middle mile global backbone

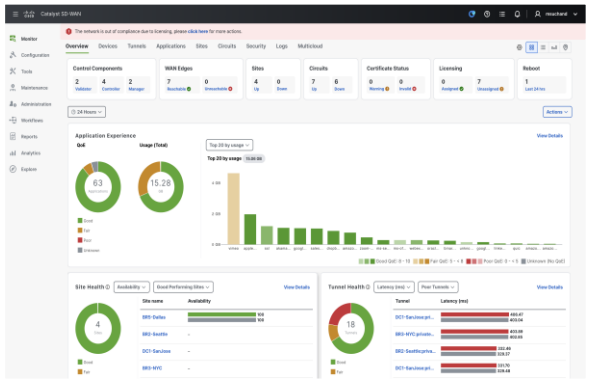
On-demand
Automated connectivity via Manager central dashboard

cisco

Assurance

Catalyst SD-WAN Analytics & Insights

Visibility into Network & App Performance



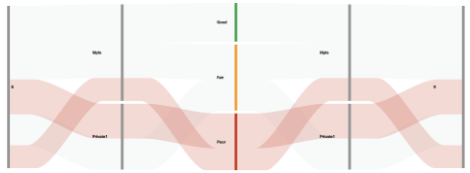
Application Experience

Scheduled Reports

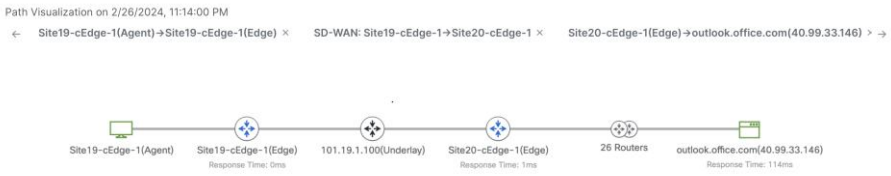
Historical Trends & Daily/Weekly/Monthly Aggregates

Troubleshooting w/ Extensive Traffic Analysis

Traffic flow patterns

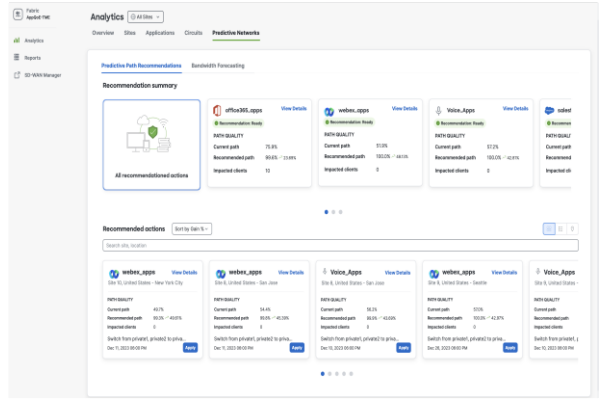


App distribution across circuits



End-to-End Path Visualization

Adaptive & Predictive Networking



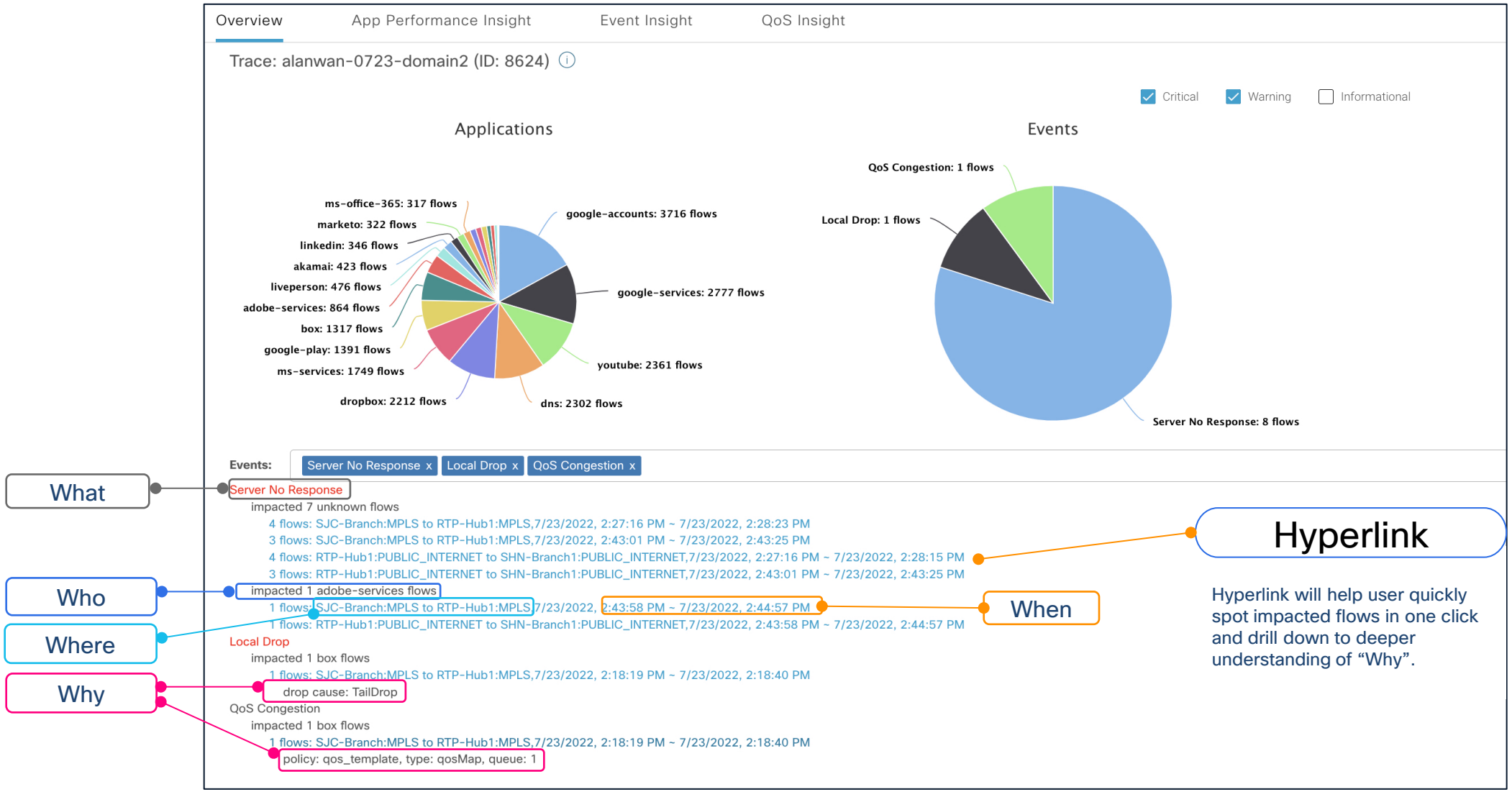
Predictive Path Recommendations

Bandwidth Forecasting

Anomaly Detection

SaaS Traffic Optimization

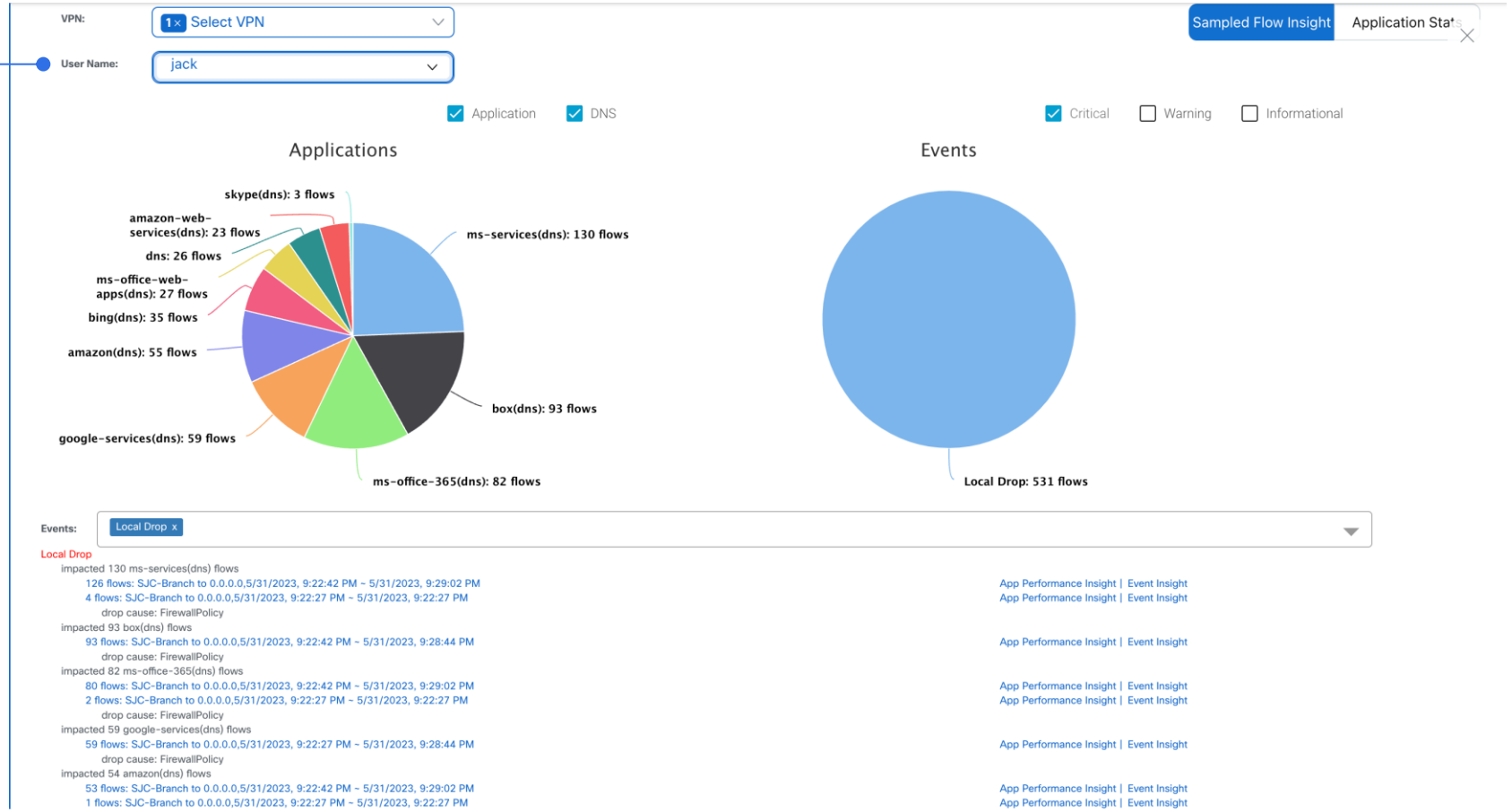
Network-Wide Path Insights (NWPI)



NWPI integration with Cisco ISE

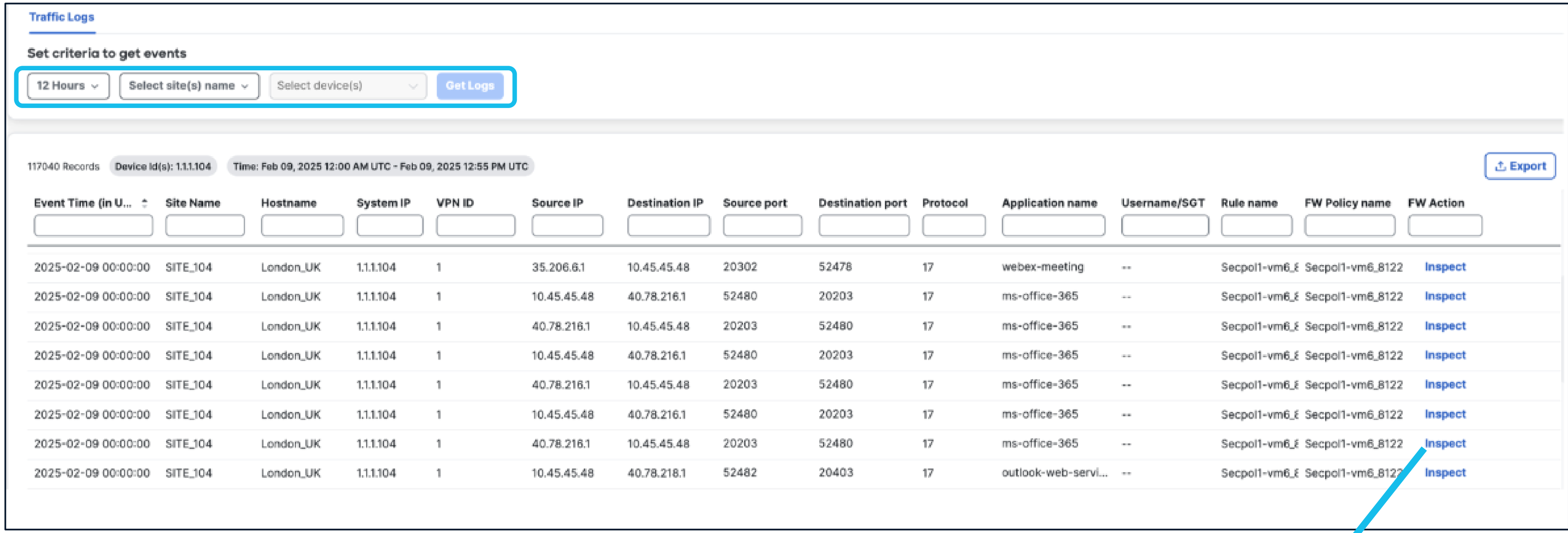
NWPI trace can be triggered for specific user and group Insight summary based on user filter.

Who

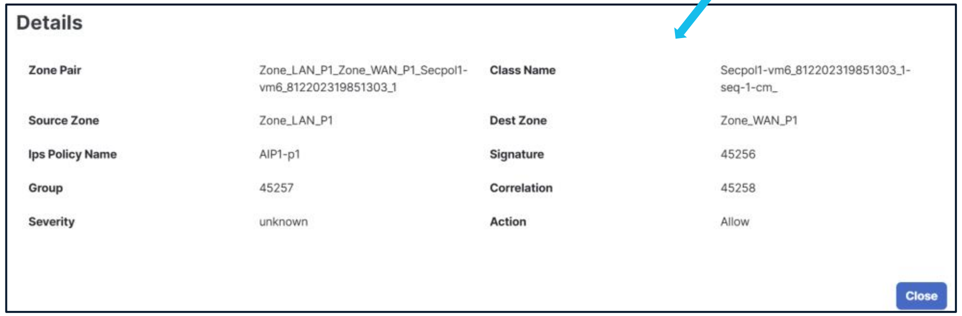


Traffic Logs

- View 5-tuple flow data for all flows across the network
- View Firewall details (FW policy name, Zone Pair, etc.)
- Run customized queries to retrieve flows information of interest



Event Time (in U...	Site Name	Hostname	System IP	VPN ID	Source IP	Destination IP	Source port	Destination port	Protocol	Application name	Username/SGT	Rule name	FW Policy name	FW Action
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	35.206.6.1	10.45.45.48	20302	52478	17	webex-meeting	--	Secpol1-vm6_ε	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	10.45.45.48	40.78.216.1	52480	20203	17	ms-office-365	--	Secpol1-vm6_ε	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	40.78.216.1	10.45.45.48	20203	52480	17	ms-office-365	--	Secpol1-vm6_ε	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	10.45.45.48	40.78.216.1	52480	20203	17	ms-office-365	--	Secpol1-vm6_ε	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	40.78.216.1	10.45.45.48	20203	52480	17	ms-office-365	--	Secpol1-vm6_ε	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	10.45.45.48	40.78.216.1	52480	20203	17	ms-office-365	--	Secpol1-vm6_ε	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	40.78.216.1	10.45.45.48	20203	52480	17	ms-office-365	--	Secpol1-vm6_ε	Secpol1-vm6_8122	Inspect
2025-02-09 00:00:00	SITE_104	London_UK	1.1.1.104	1	10.45.45.48	40.78.218.1	52482	20403	17	outlook-web-servi...	--	Secpol1-vm6_ε	Secpol1-vm6_8122	Inspect



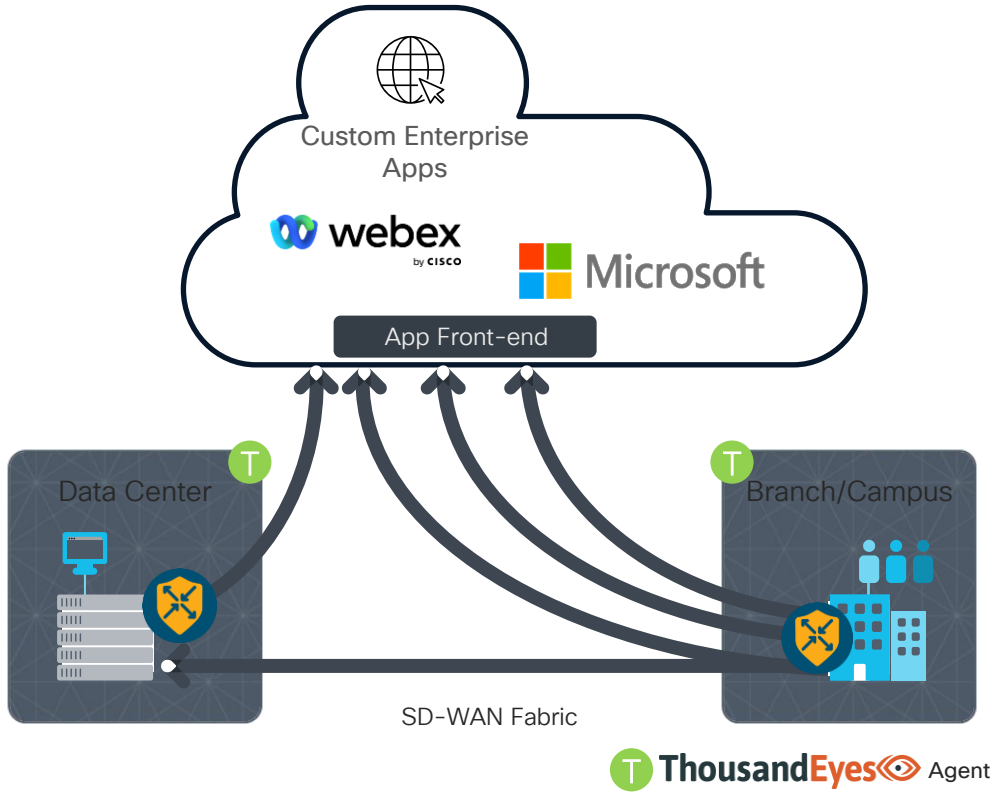
Zone Pair	Zone_LAN_P1_Zone_WAN_P1_Secpol1-vm6_812202319851303_1	Class Name	Secpol1-vm6_812202319851303_1-seq-1-cm_
Source Zone	Zone_LAN_P1	Dest Zone	Zone_WAN_P1
Ips Policy Name	AIP1-p1	Signature	45256
Group	45257	Correlation	45258
Severity	unknown	Action	Allow

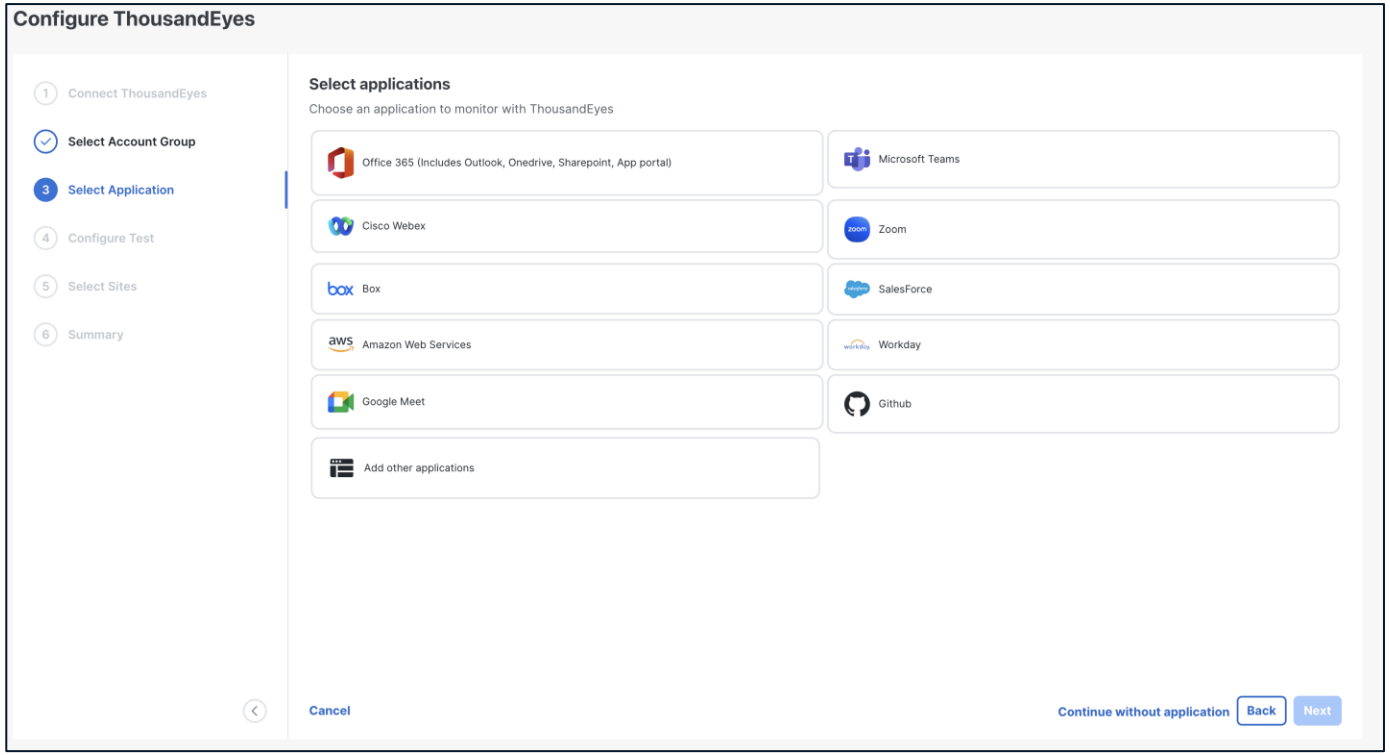
Navigation Path: From 20.18, Monitor -> Logs -> Traffic Logs

Expedite troubleshooting with detailed flow-level visibility

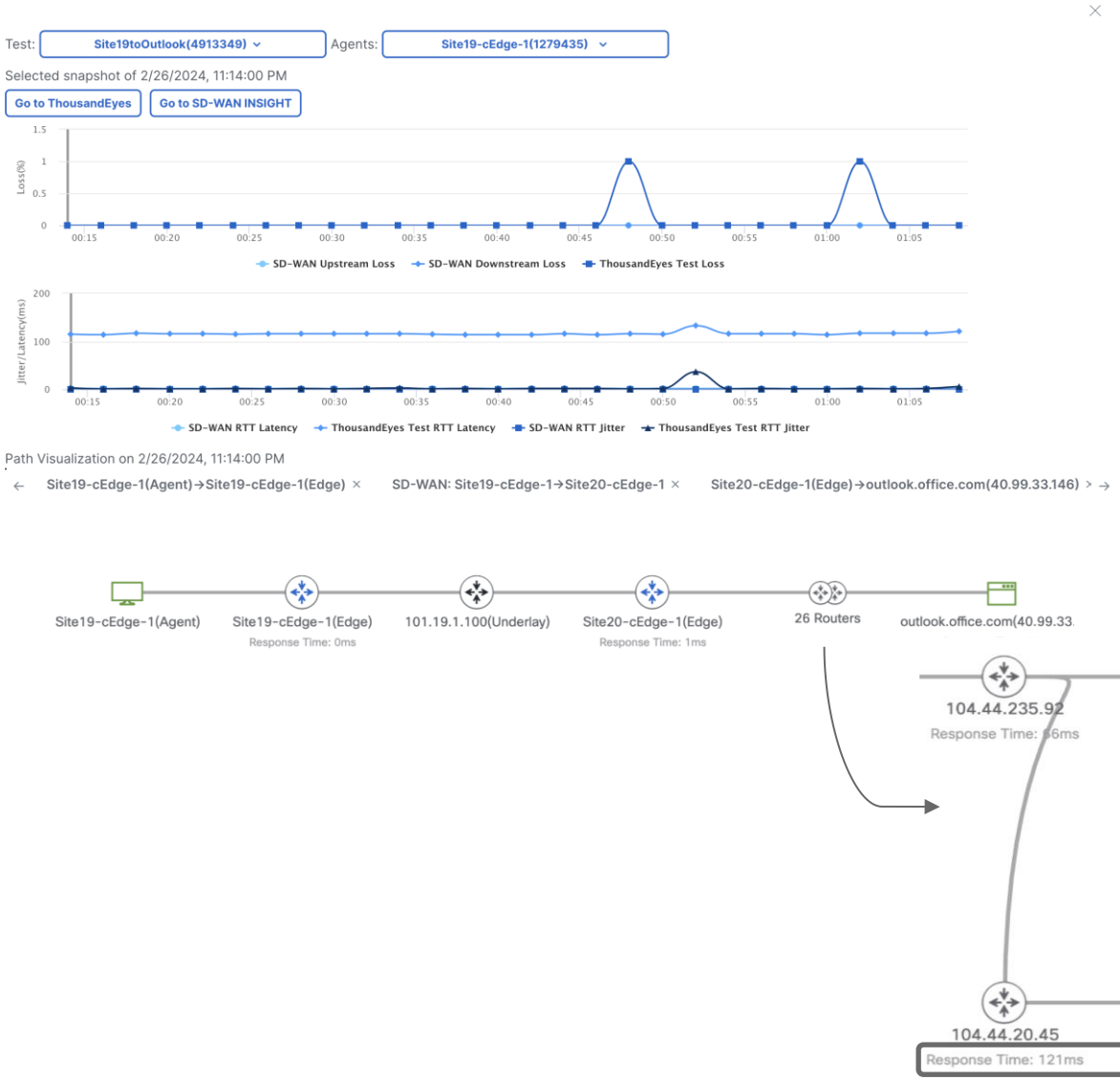
Extended Visibility with ThousandEyes

Easy Onboarding workflow to deploy ThousandEyes Agent and define Application Monitoring Tests





NWPI + ThousandEyes : Better Together



- With ThousandEyes Integration, NWPI Trace data and TE probe tests results are auto co-related.
- ThousandEyes Path Visualization provides visibility into Internet hops used when accessing the Public/SaaS apps.
- NWPI is also integrated with Underlay Measurement and Tracing Service (UMTS) to provide underlay insights corelated with TE Insights.

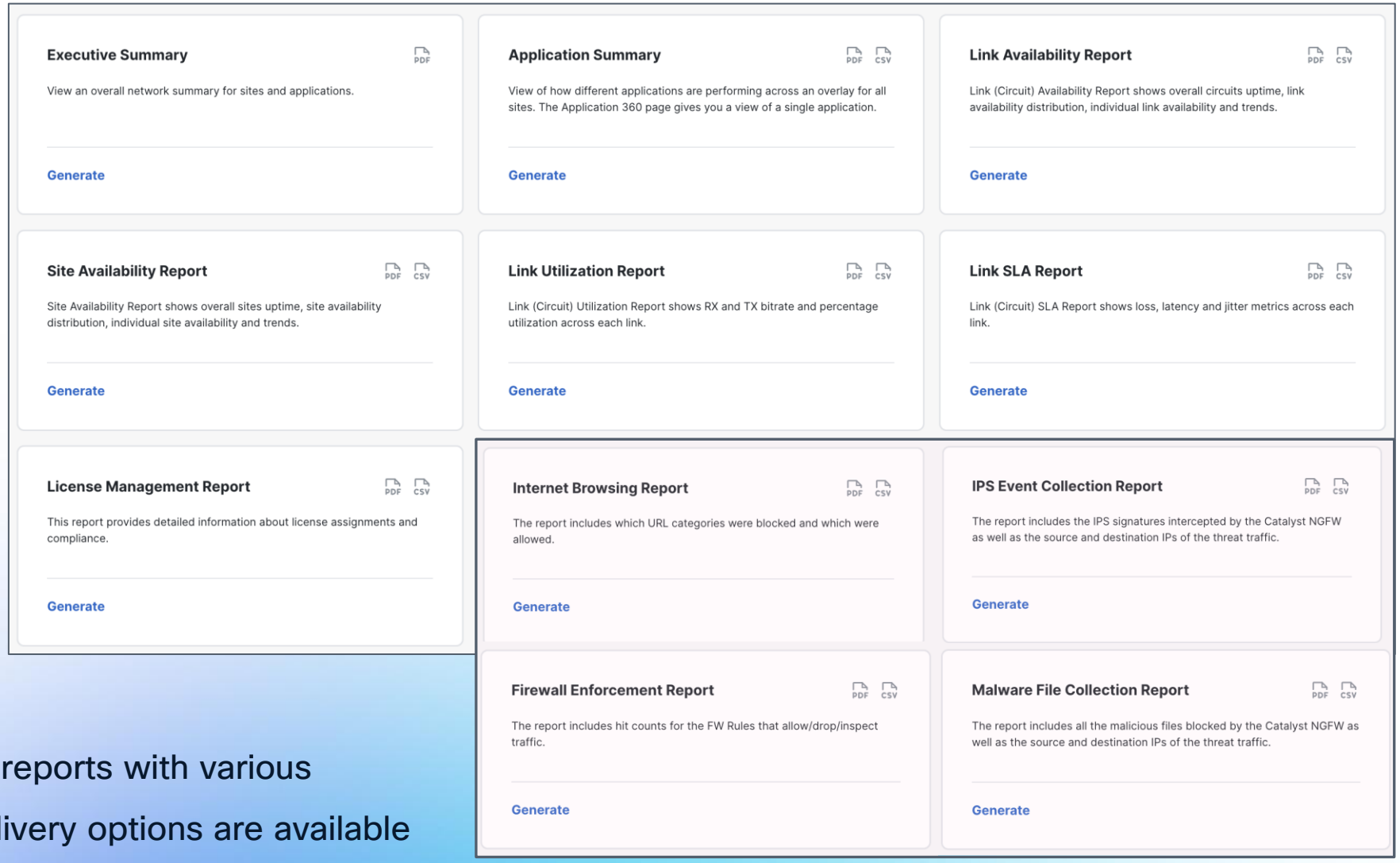
TE provides the network map where problems are occurring.

NWPI is the magnifying lens that shows why they are occurring.

Network and Security Reports

Reports can help with:

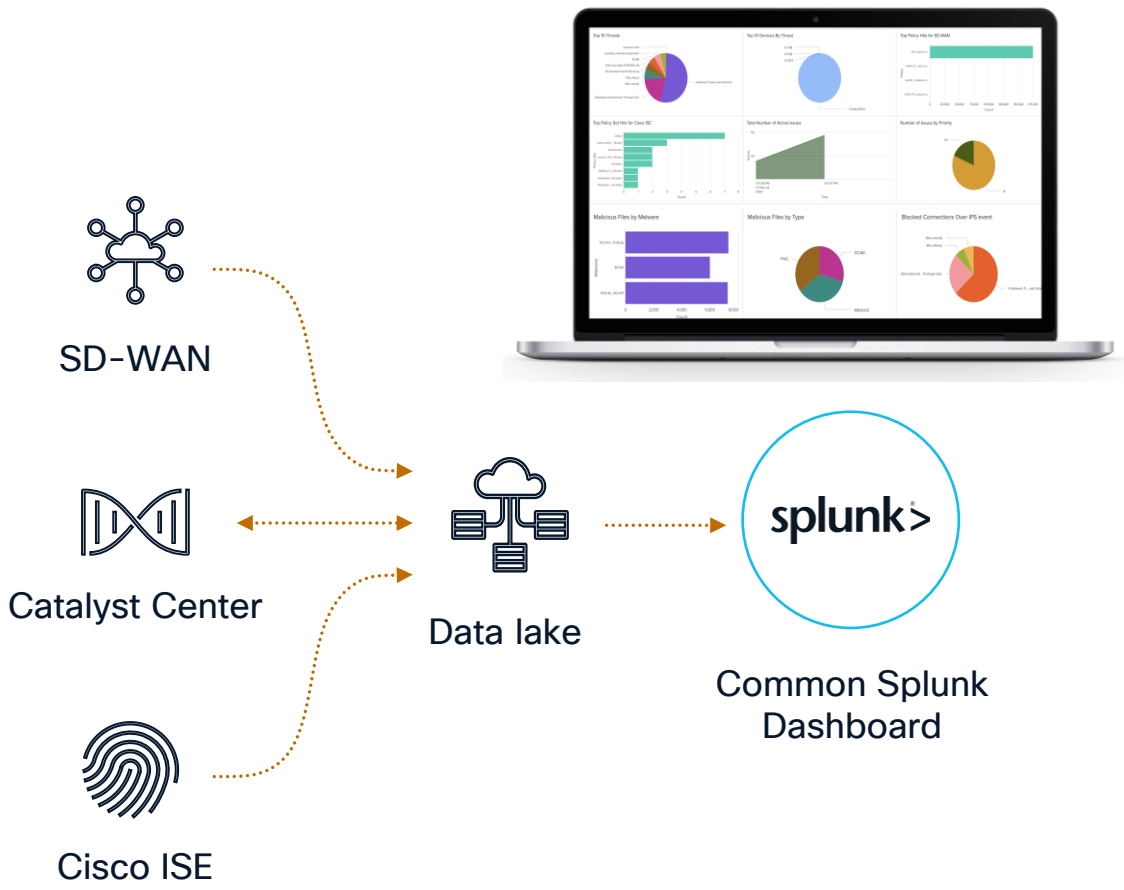
- Performance monitoring & optimization
- Capacity planning
- Compliance
- Cost management



Several Network and Security reports with various formatting, scheduling and delivery options are available

SD-WAN integration with Splunk

Cisco Enterprise Networking App for Splunk



Consolidated visibility on a common dashboard for real-time monitoring, history insights, security insights, and compliance advisory

Analytics dashboard to detect and report on anomalies based on deviation from the baseline

Playbook driven response based on certain event triggers to generate API calls back to the appropriate domain

Splunk ecosystem partner trigger notifications to 1,000+ 3rd party applications

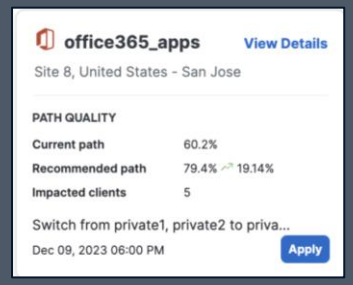
AI

AIOps: Simplifying Day-2 Operations

Optimize network and application performance to achieve higher operational efficiency

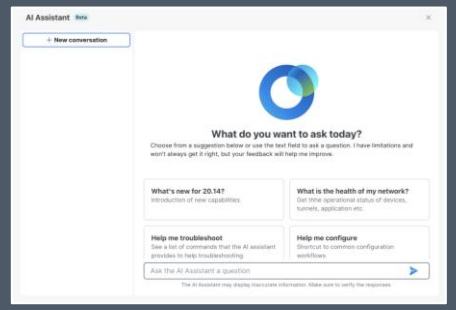
Mitigate issues before they impact. In case issues do occur, offer **root cause analysis** to **reduce MTTR**

Predictive Path Recommendations



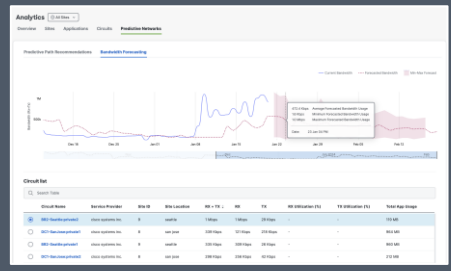
Path recommendations to Improve Application Performance

AI Assistant for Networking



Interactive LLM-based AI Assistant for Networking (Gen AI)

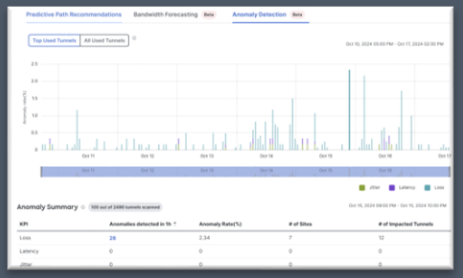
Bandwidth Forecasting



AI/ML-based forecasting

Capacity planning

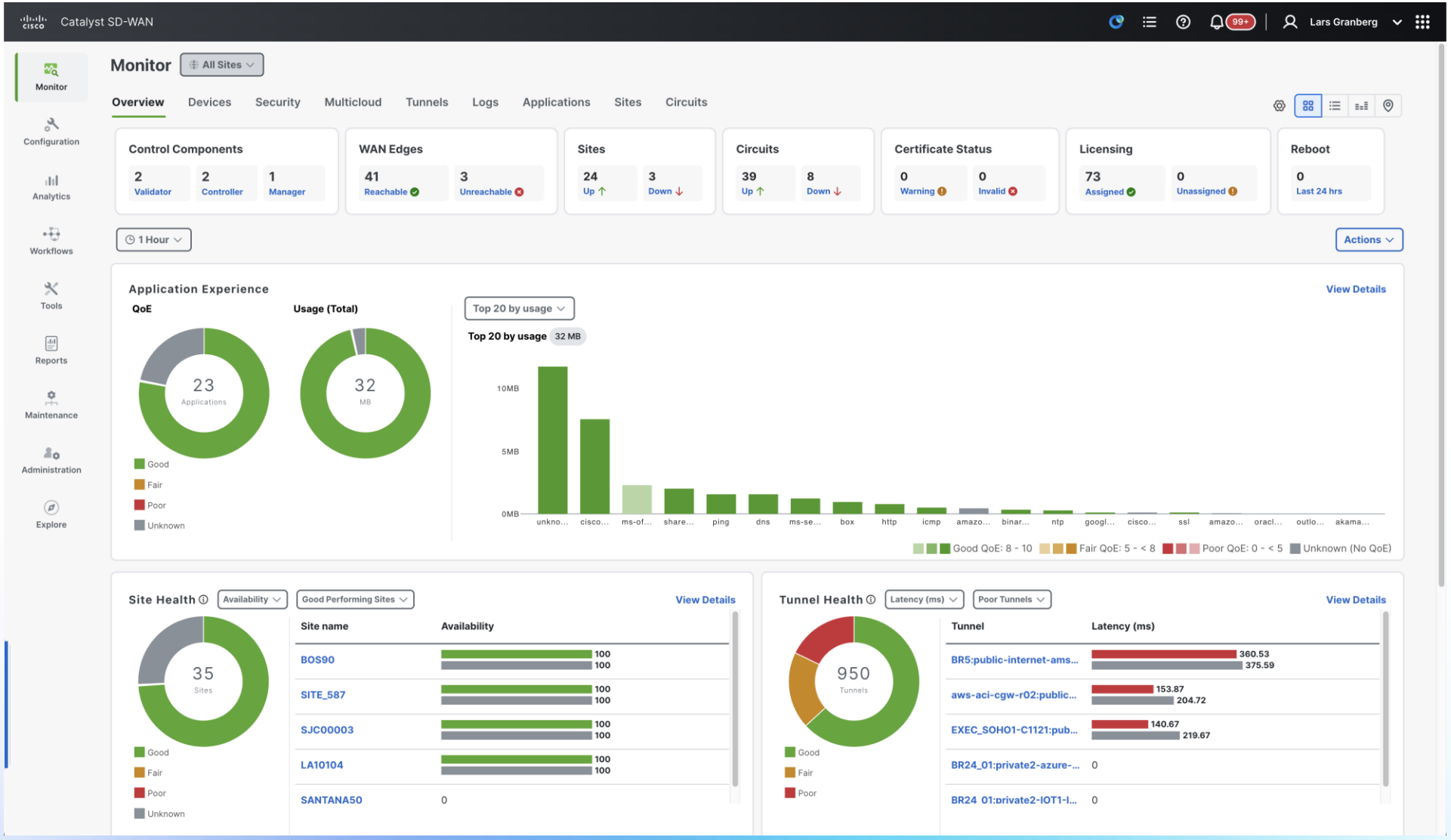
Anomaly Detection



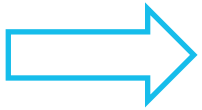
Detect Network Anomalies

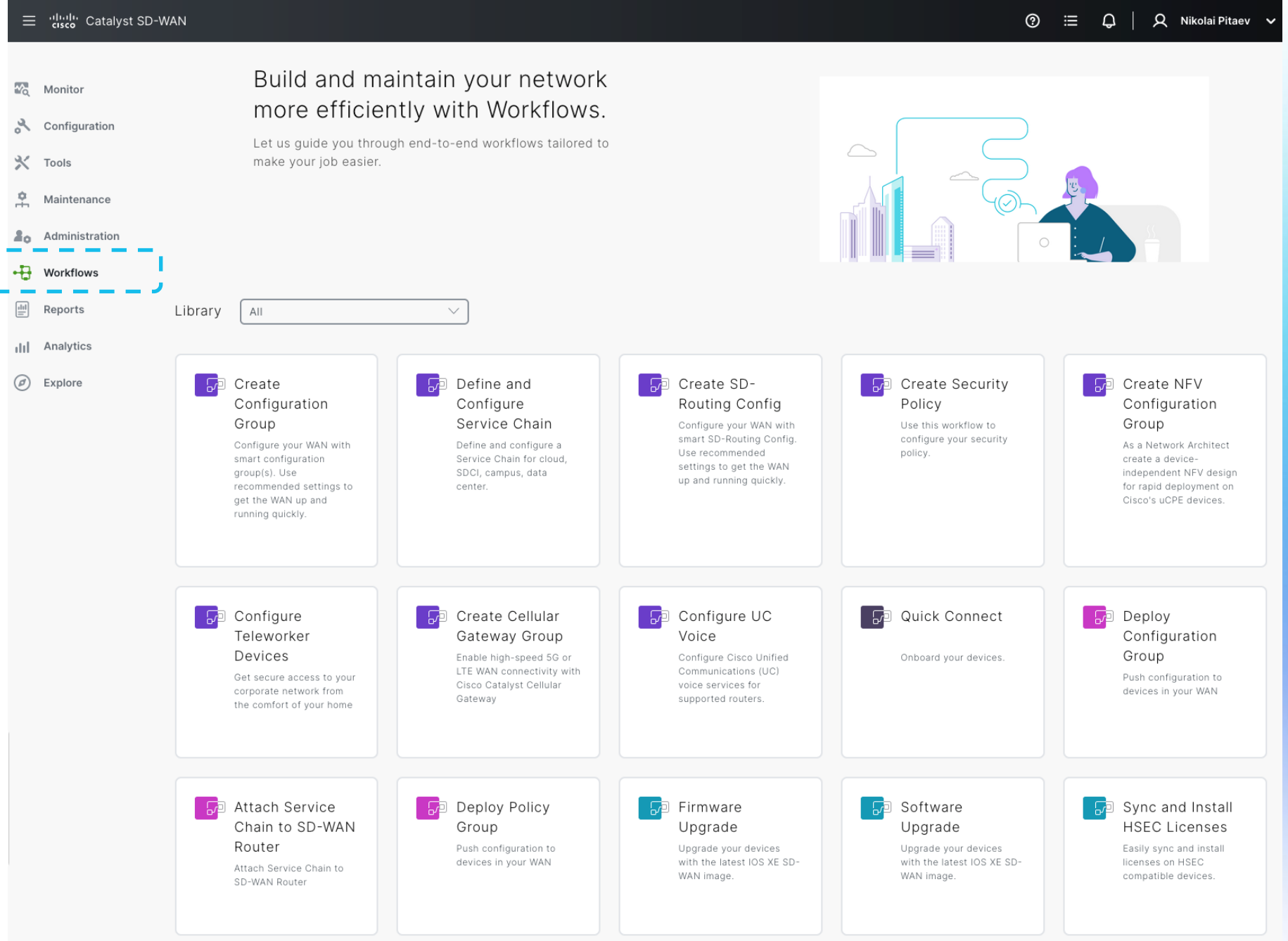
Operational

SD-WAN Manager UI



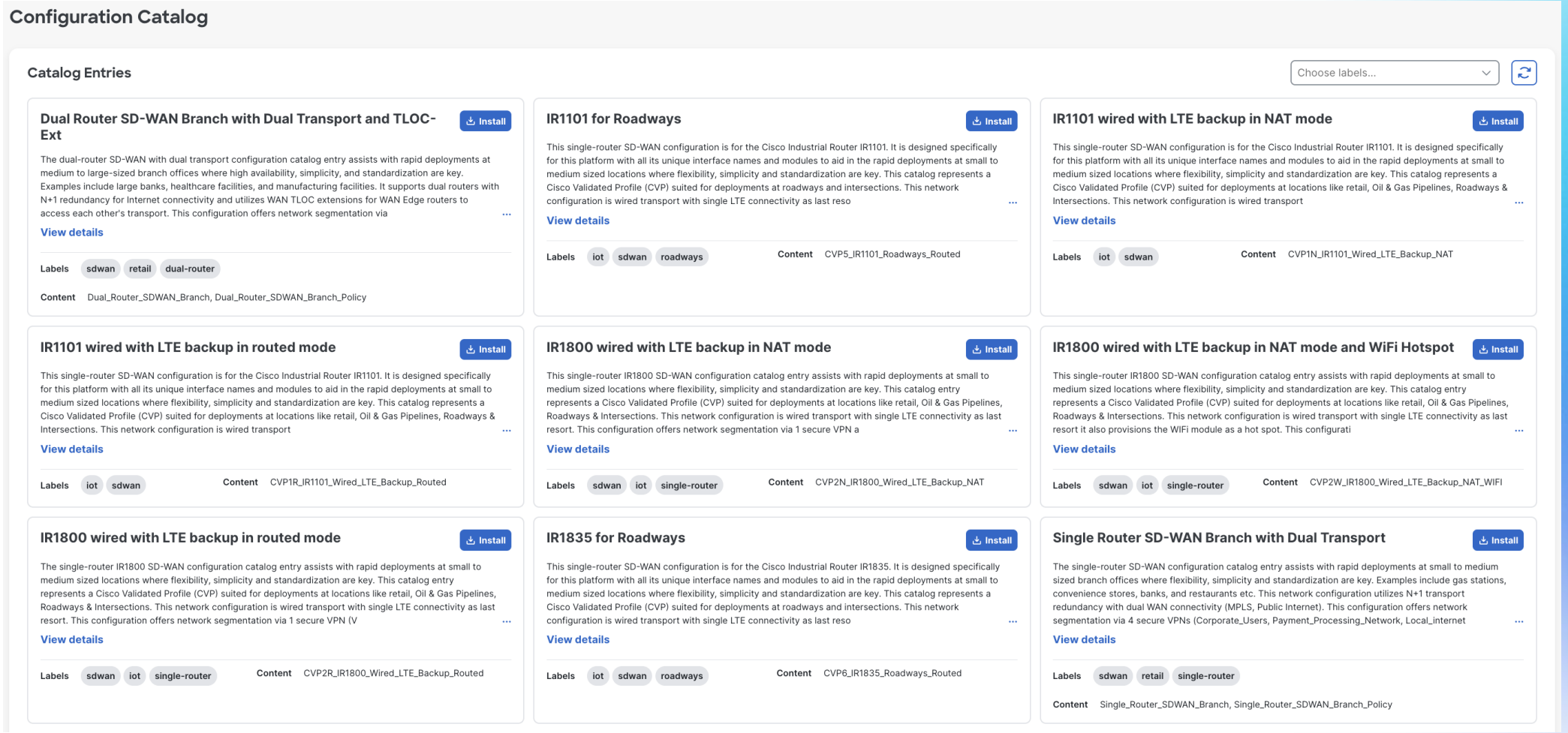
Workflows Library





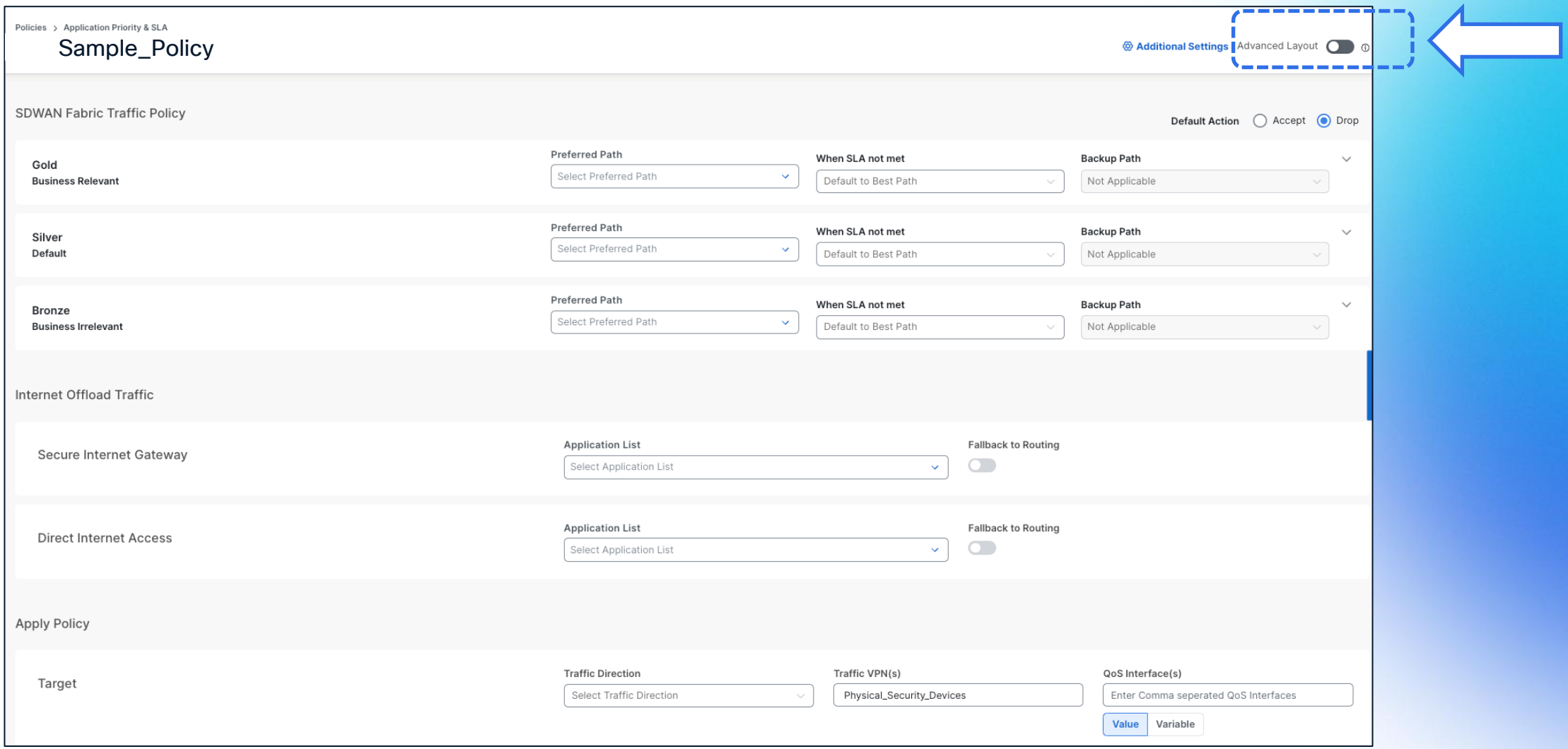
Configuration Catalog

- Cisco hosted and managed configuration
- Easy way to consume Cisco validated configuration



Policies

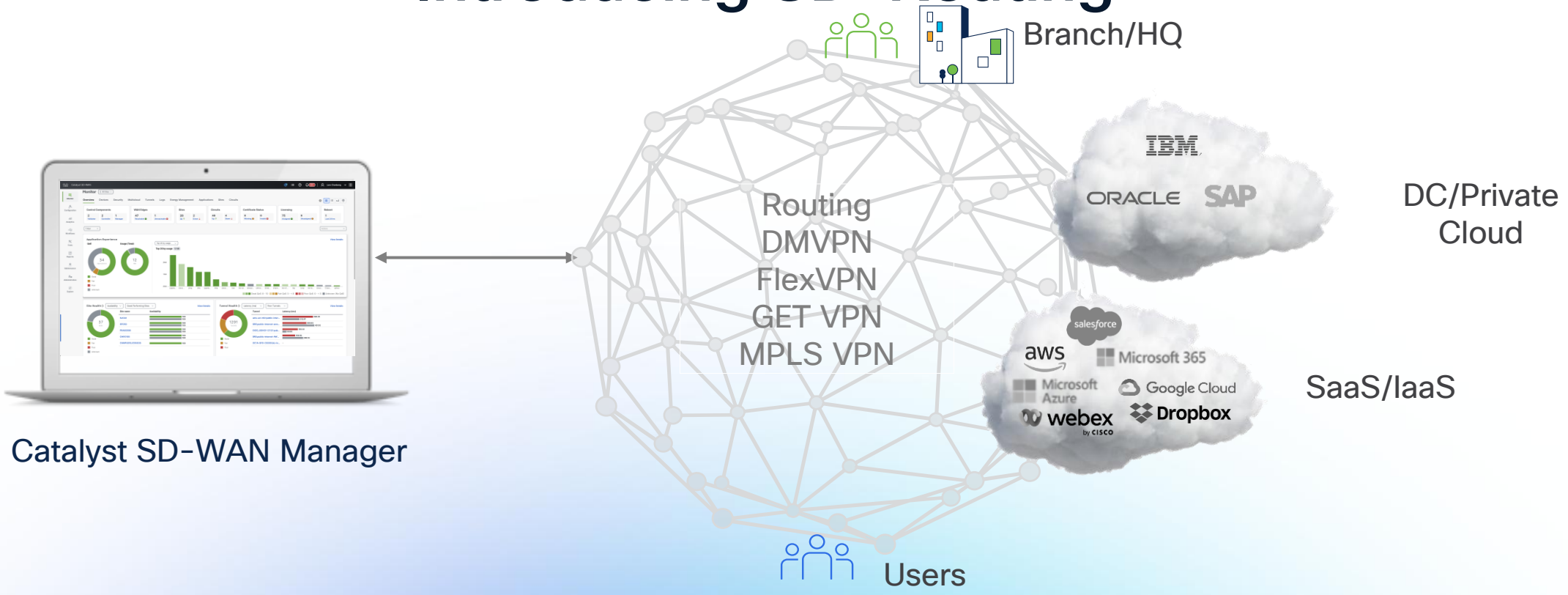
- Intent-based approach
- Easy policy creation and deployment



SD-Routing

Transform the operational experience for your routing environment

Introducing SD-Routing



Simplicity and Agility	OpEx Reduction	Future-Ready WAN	Multi-layered Security

SD-WAN vs SD-Routing

SD-WAN deployment

SD-WAN Validator

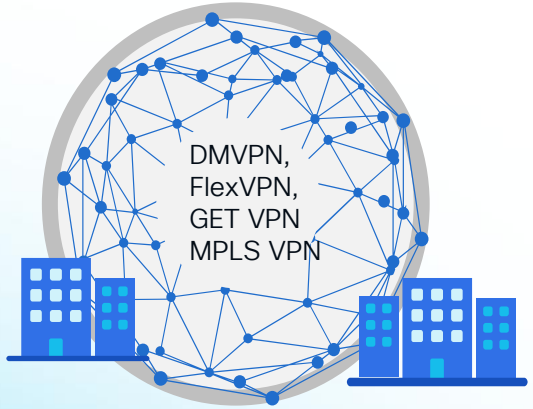
SD-WAN Manager

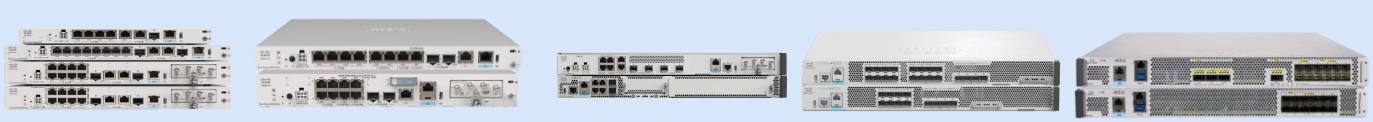
SD-WAN Controller

SD-Routing deployment

SD-WAN Validator

SD-WAN Manager





NEW: Cisco Secure Router 8000 Series

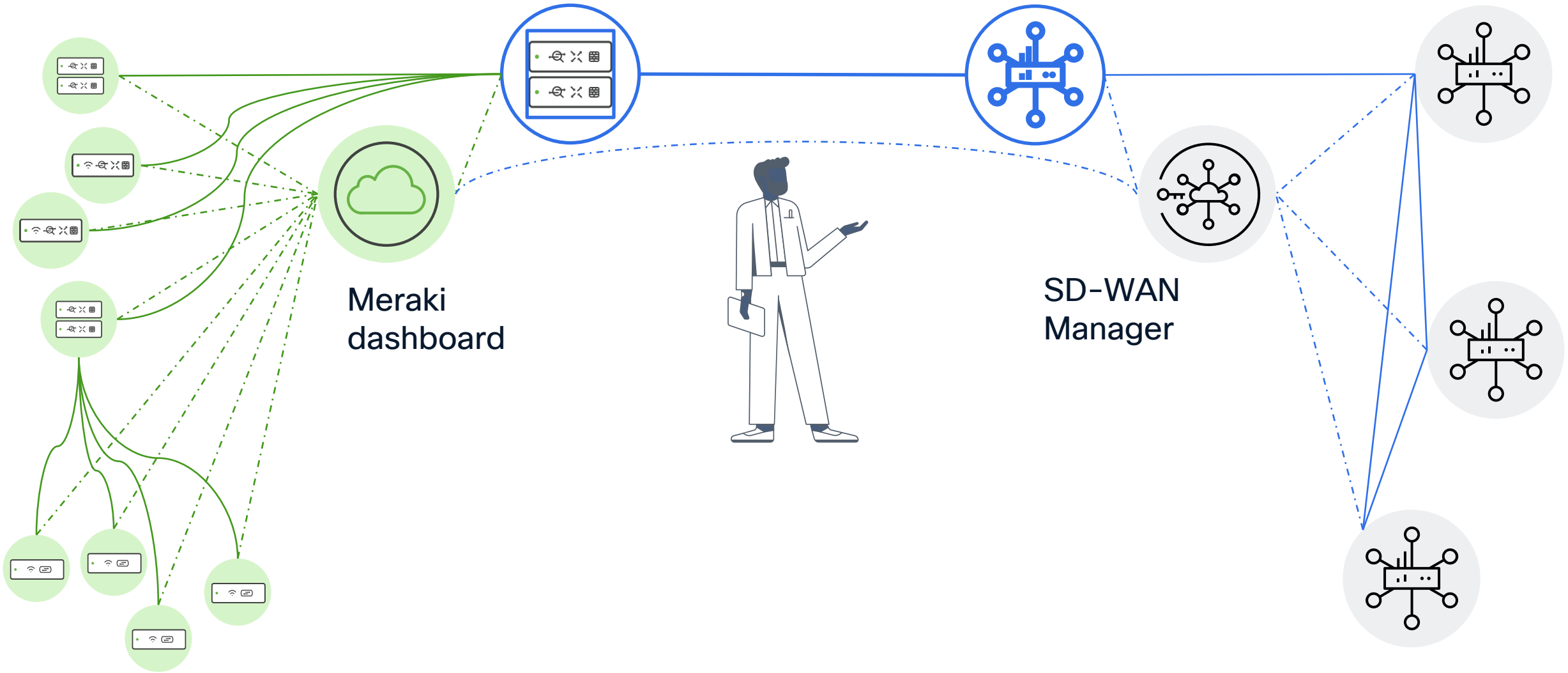
ISR 1000

Cisco Catalyst 8000 Series

Cisco IR Series

What about Meraki SD-WAN?

Joining fabrics is now a simplified experience

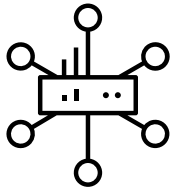


cisco

Key Takeaways

Key Takeaways

Cisco SD-WAN



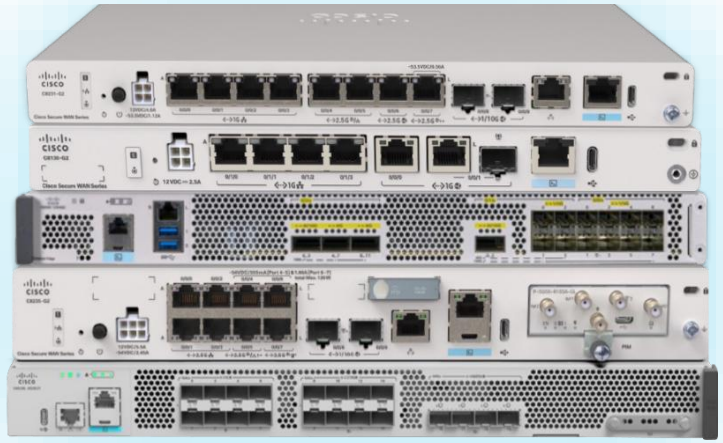
- Single pane of glass Automation
- Optimized for Cloud access
- Pervasive Security
- Predictable and actionable insights

Cisco 8000 Series Secure Routers

Introducing the industry's **most advanced router**

Cisco 8000 Series

Secure Router



- **Secure Networking Processor** – leapfrogs with 3x higher throughput
- **Advanced Security** – Post Quantum Cryptography capable, NFGW & SASE with 3x threat protection throughput
- **Assurance** – ThousandEyes Traffic Insights, GenAI troubleshooting
- **Operational Simplicity** – IOS-XE managed by Dashboard & Simplified Licensing

Routers for every size and location

Launched in JUNE 2025

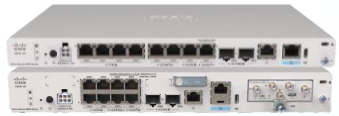
Small Branch: 8100

4 Variants

IPsec:
Up to 1.5 Gbps

SD-WAN:
Up to 1 Gbps

Threat Protection:
Up to 1 Gbps



Medium Branch: 8200

2 Variants

IPsec:
Up to 5 Gbps

SD-WAN:
Up to 4 Gbps

Threat Protection:
Up to 2.5 Gbps

Large Branch: 8300

2 Variants

IPsec:
Up to 20 Gbps

SD-WAN:
Up to 15 Gbps

Threat Protection:
Up to 7 Gbps

Campus: 8400

3 Variants

IPsec:
Up to 45 Gbps

SD-WAN:
Up to 23 Gbps

Threat Protection:
Up to 11 Gbps

Data Center: 8500

2 Variants

IPSec:
Up to 45 Gbps

SD-WAN:
Up to 23 Gbps

Route Scale up to
8M

Simplified Licensing

Cisco Networking Subscription
Cisco Routing Subscription

No More Bandwidth Tiers & HSEC !
Consistent Packages across all Platform-Class

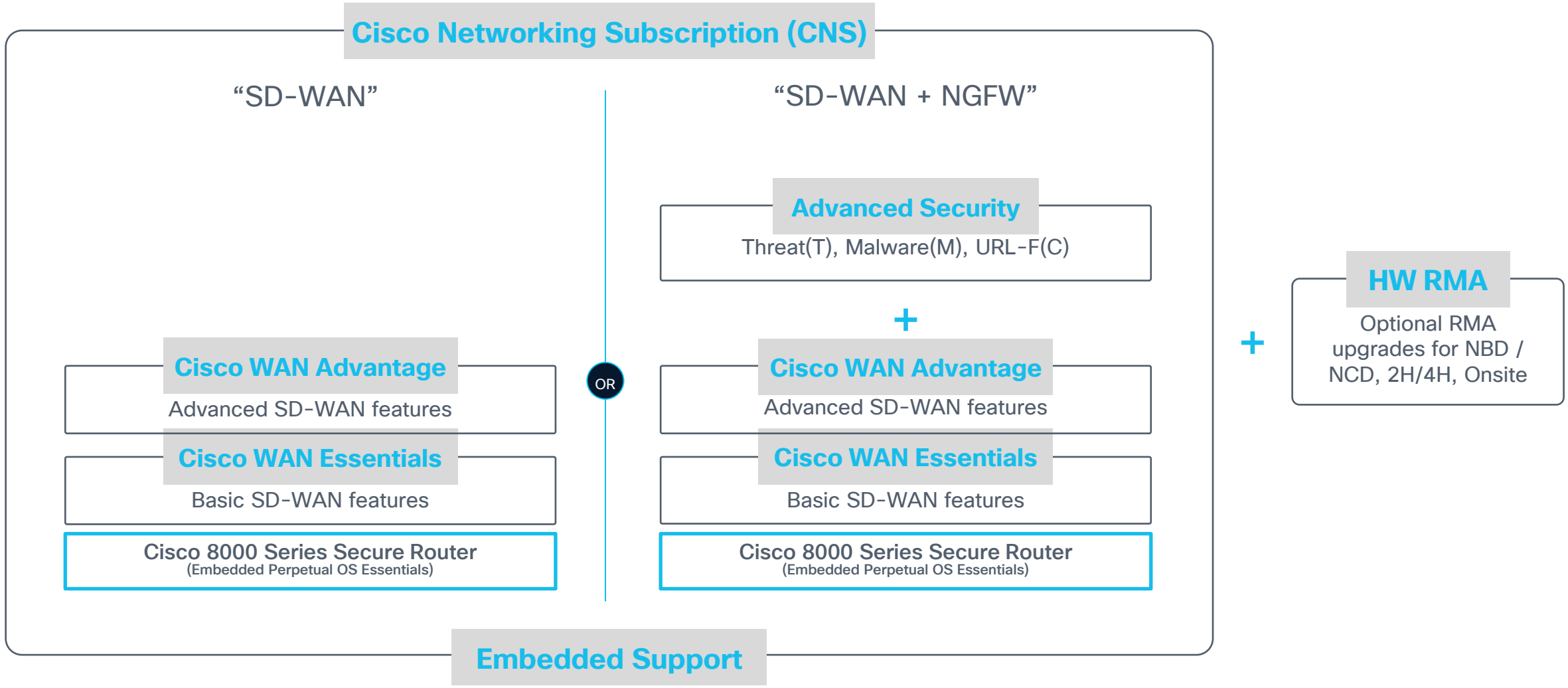
Platform-Class Specific Licenses & Pricing

Licenses co-termed to a single end-date for easy Renewals

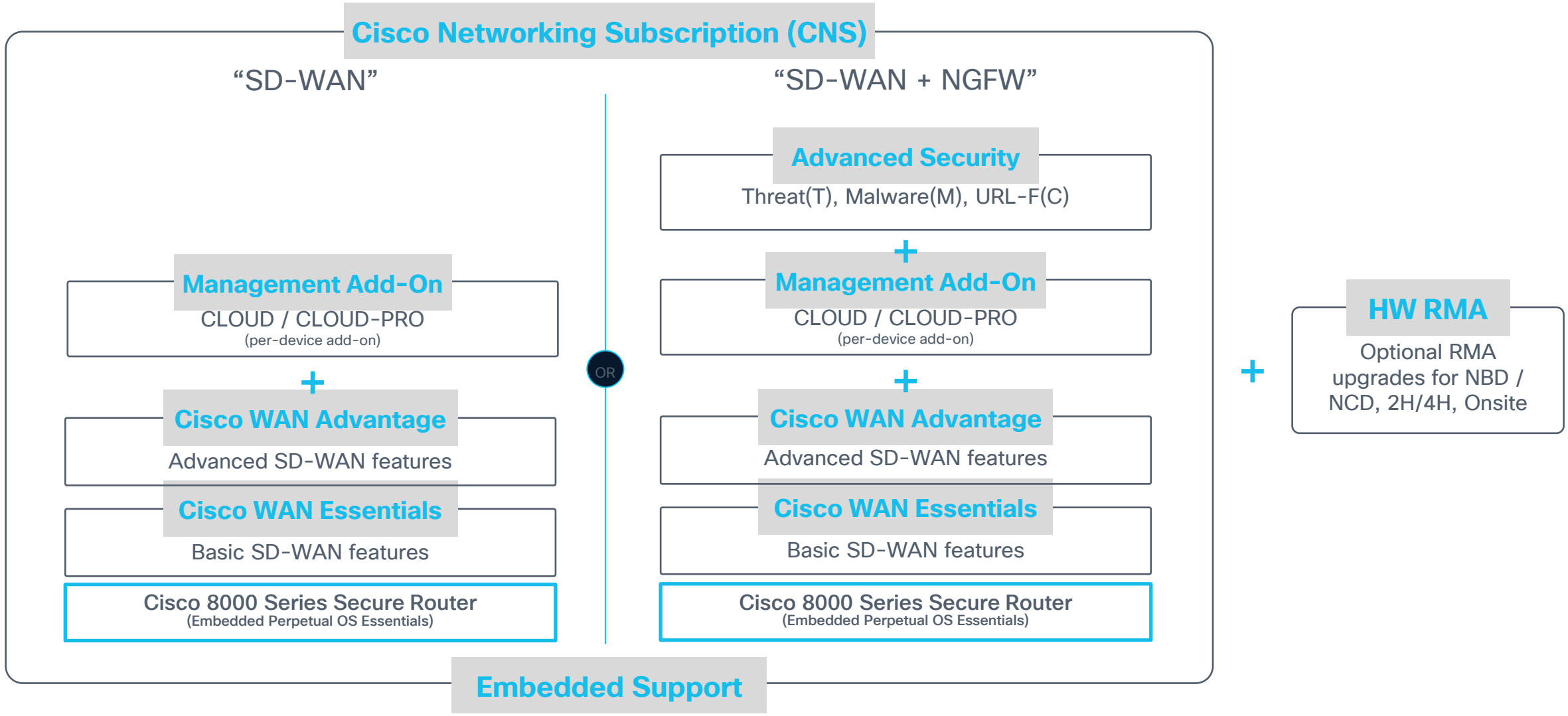
Cisco Networking Subscription and Cisco Routing Subscription
for both software and hardware, simplifying licensing and renewals

https://www.cisco.com/c/m/en_us/products/software/wan-routing-licensing-feature-matrix.html

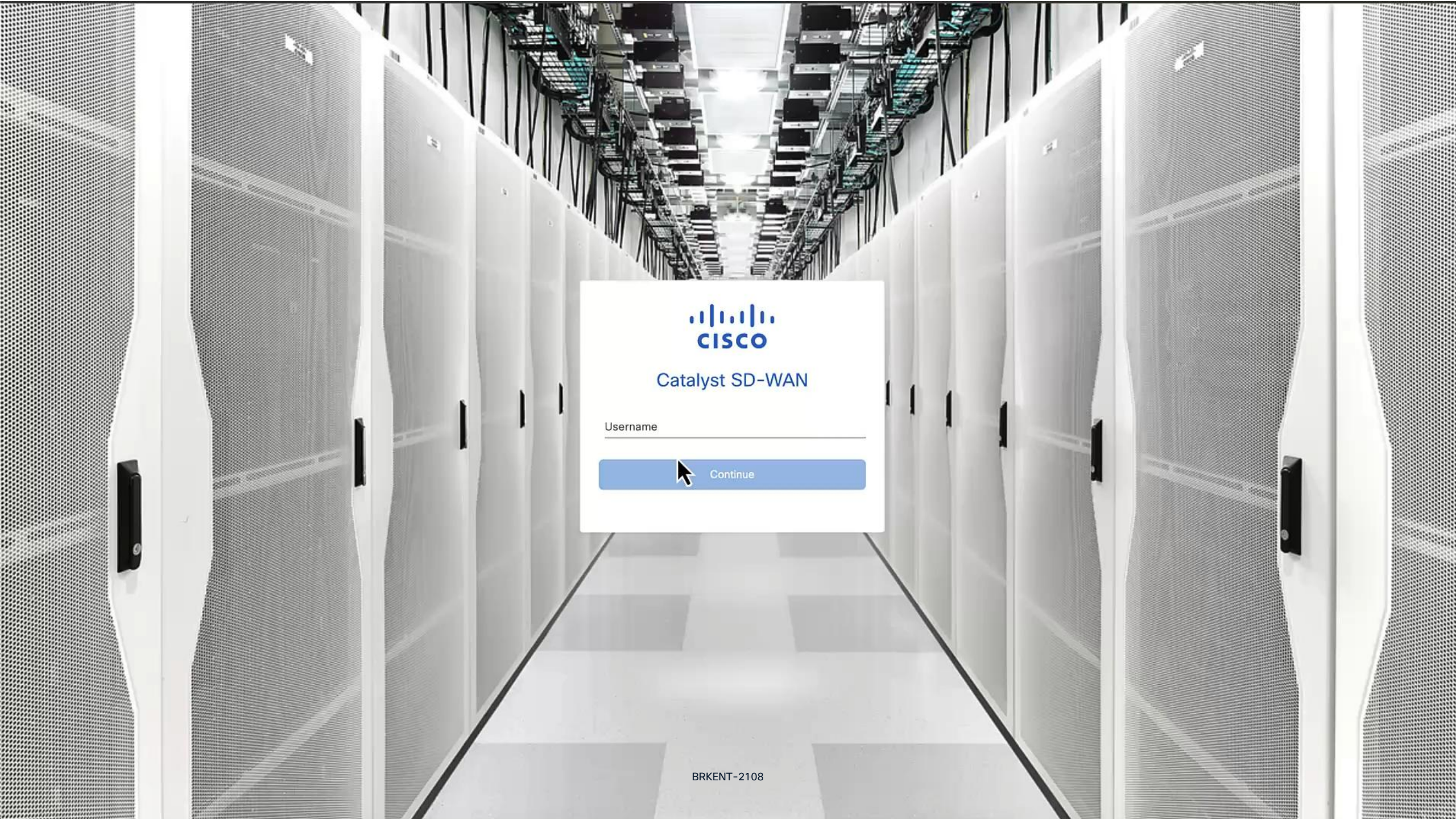
Customer hosted On-Premise/Cloud management



Cisco hosted Cloud management



Demo


Catalyst SD-WAN
Username
Continue

SD-WAN – This is it.

Complete your session evaluations

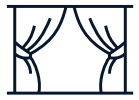
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

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

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

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

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

Thank you


CISCO