

Enhancing Network Integrity with Catalyst SD-WAN

cisco Live !

Deep Dive into End-to-End Security

Shamil Fernando
Global Technical Solutions Architect

Session ID: BRKENS-2567

Cisco Webex App

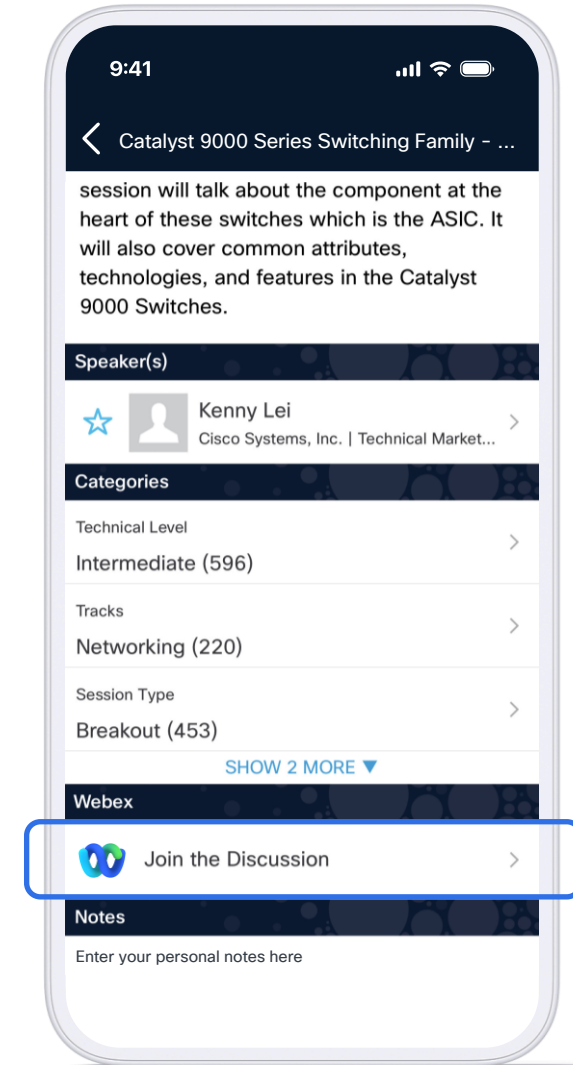
Questions?

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.

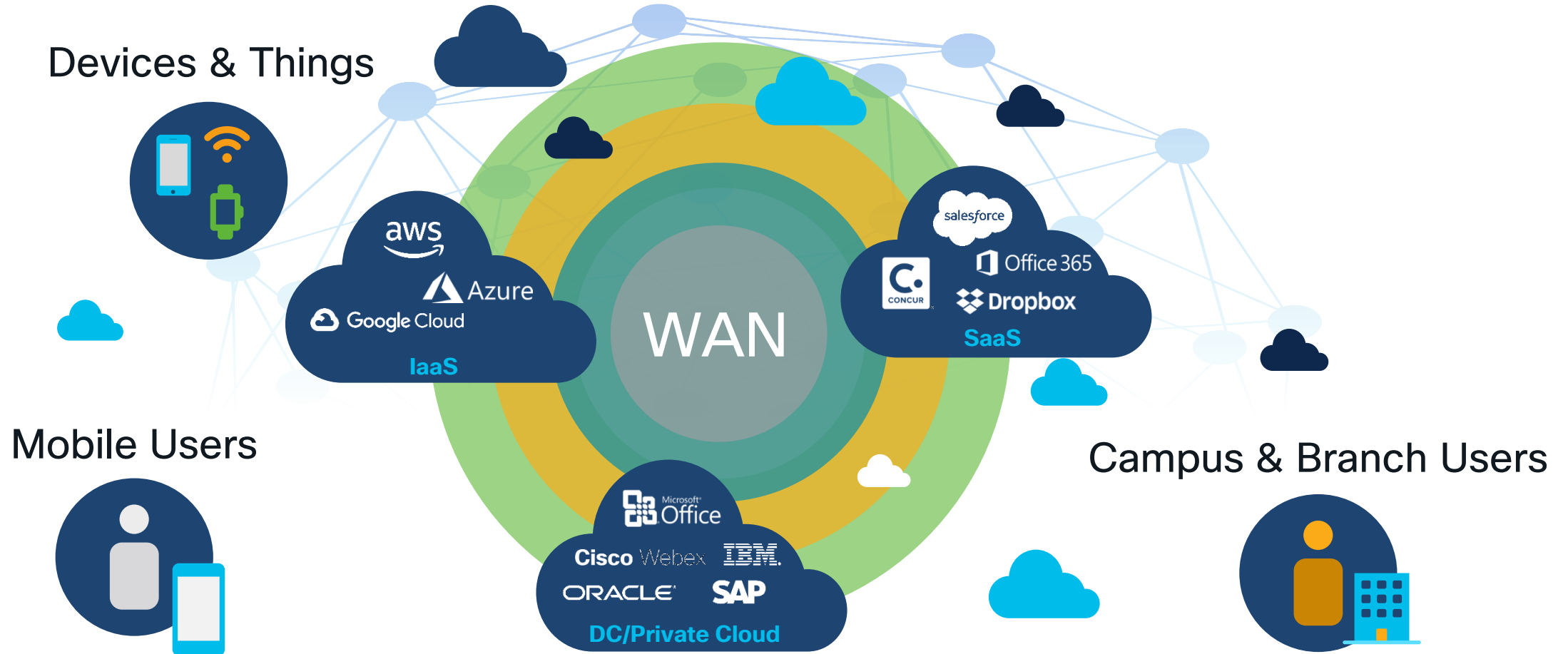


<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2567>

Agenda

- 01 Today's Application & Security
- 02 SD-WAN Architecture
- 03 Fabric Security
- 04 New Secure Router
- 05 Secure WAN Ecosystem
- 06 Common Policy
- 07 Macro & Micro Segmentation
- 08 SD-WAN + Secure Access
- 09 Cisco Security Cloud Control
- 10 Bringing It All Together

Modern Applications and the Evolution of Centralized Security Policy with SASE



SD-WAN Architecture

Orchestration Plane

- First point of authentication
- Distributes list of vSmarts/vManage to all Secure Edges
- Facilitates NAT traversal

Management Plane

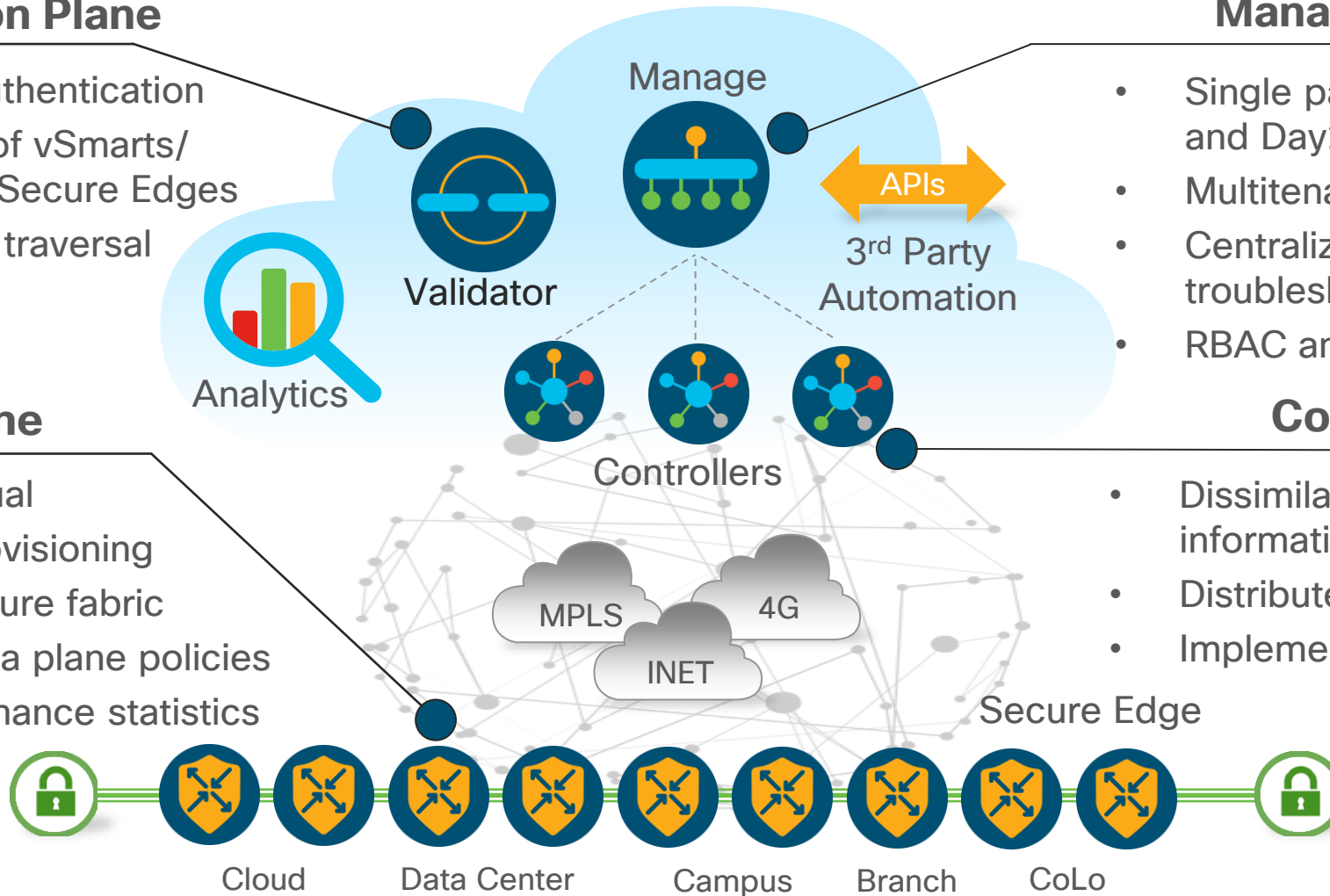
- Single pane of glass for Day0, Day1 and Day2 operations
- Multitenant or single-tenant
- Centralized provisioning, troubleshooting and monitoring
- RBAC and APIs

Data Plane

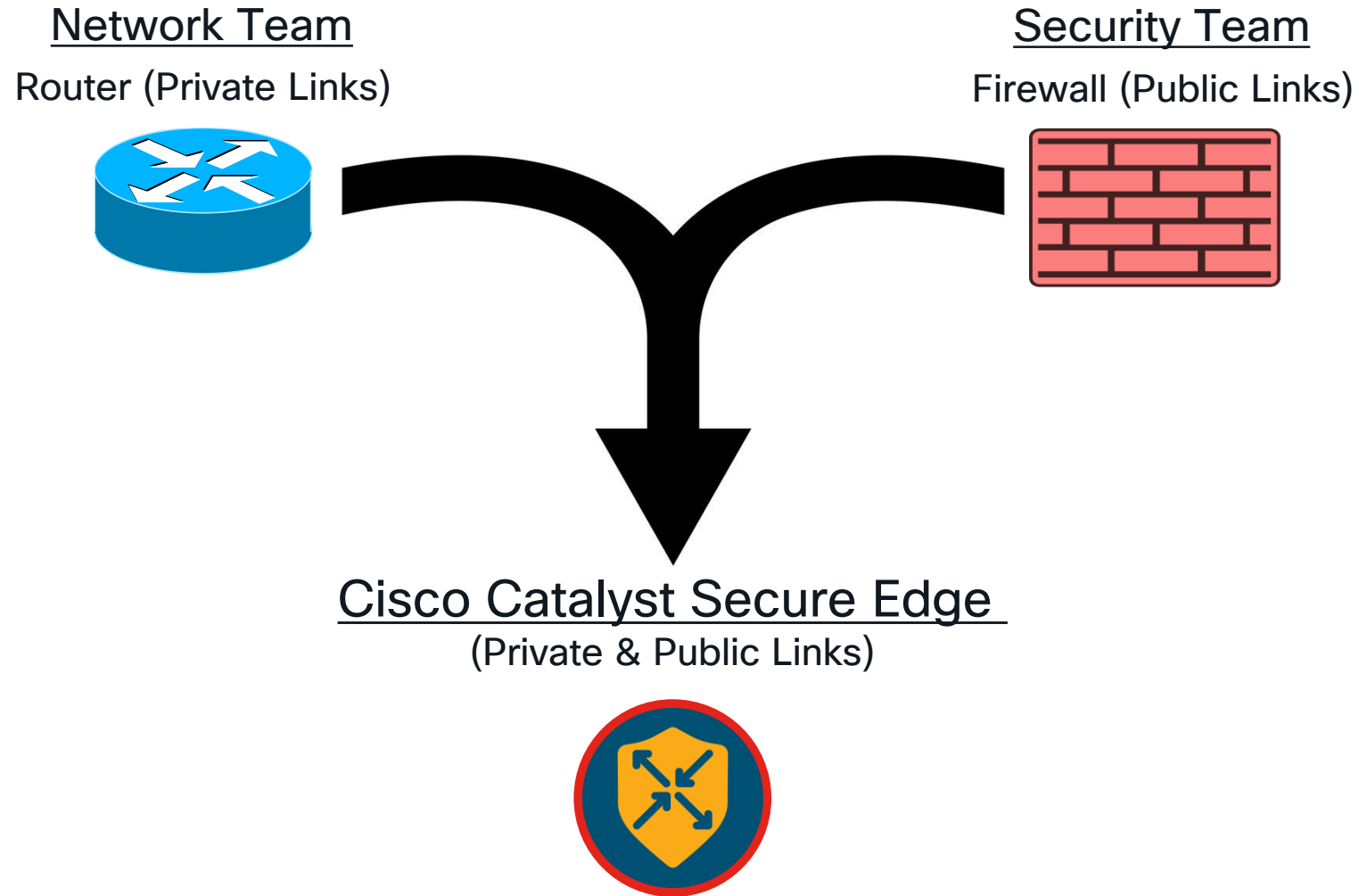
- Physical or virtual
- Zero Touch Provisioning
- Establishes secure fabric
- Implements data plane policies
- Exports performance statistics

Control Plane

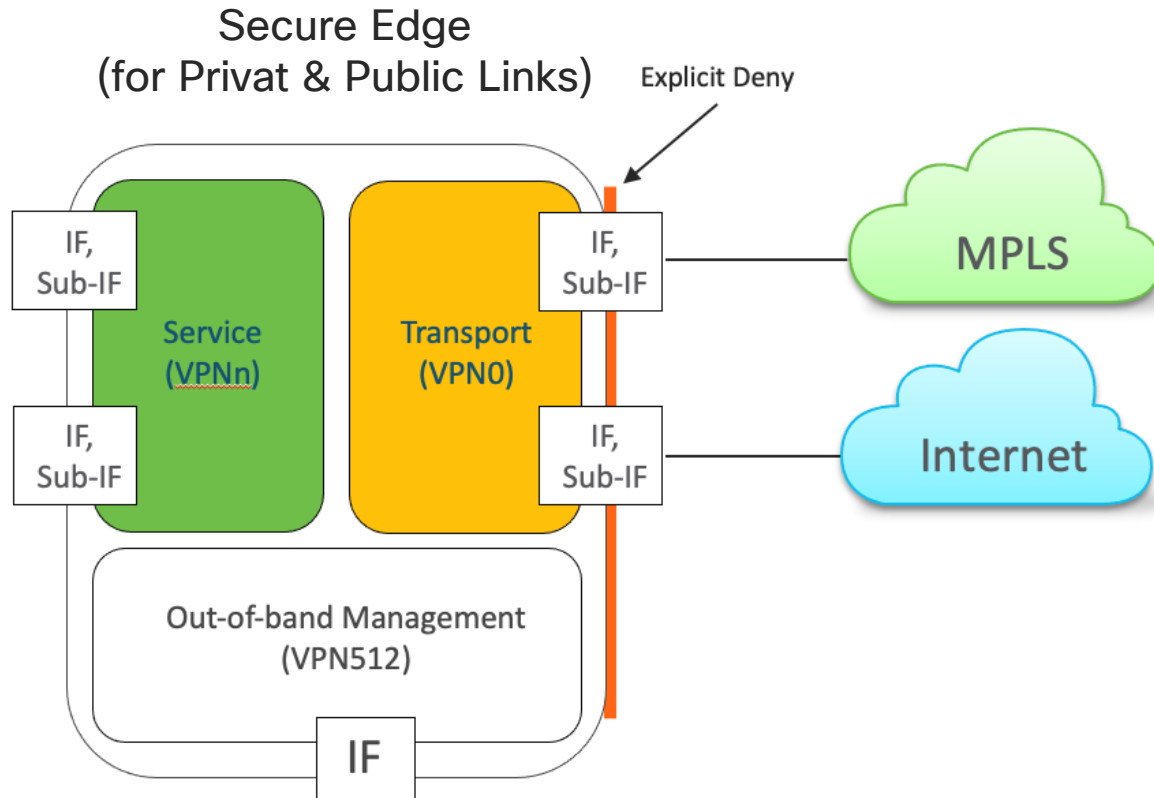
- Disseminates control plane information between Secure Edges
- Distributes data plane policies
- Implements control plane policies



Secure Edge



Secure Edge



- Explicit Deny
- Zones Based Architecture
- No Open Ports
- DDOS Mitigation
- VPNs are isolated from each other, each VPN has its own forwarding table
- Reachability within VPN is automatically advertised by the OMP

Fabric Security



Secure Edge Perimeter Protection

- Explicit Deny
- Zones Based Architecture
- No Open Ports
- DDOS Mitigation
- Trust Anchor Module (TAm)
- Secure Boot of Signed Images
- Runtime Defenses (RTD)



Onboarding & Authentication

- Devices Onboarding Process
- Zero Trust
- Certificate-based Authentication & Whitelisting
- Automate Custom Certificate Authority (CA)
- Certificate Management through SD-WAN Manager



Transport Security

- IKE less IPsec (Key exchange using a controller, high scale)
- Key - Using RNG (NIST SP 800-90A)
- Key Rotation - 24hr Default
- Anti-Replay Protection



Least Access Principle

- Segmentation (VRF) - True VRF with separate route table & different topology each VRF
- Overlay Management Protocol (OMP)

New Advanced Secure Routers

AI/ML & Assurance

AI/ML Engin

AI Troubleshooting

ThousandEyes with Traffic Insights

Secure Networking Processor

Post Quantum Security capable
with 3x higher throughput

Advanced Security

NGFW and SASE with
3x Threat protection

Cloud Management

IOS-XE managed by dashboard

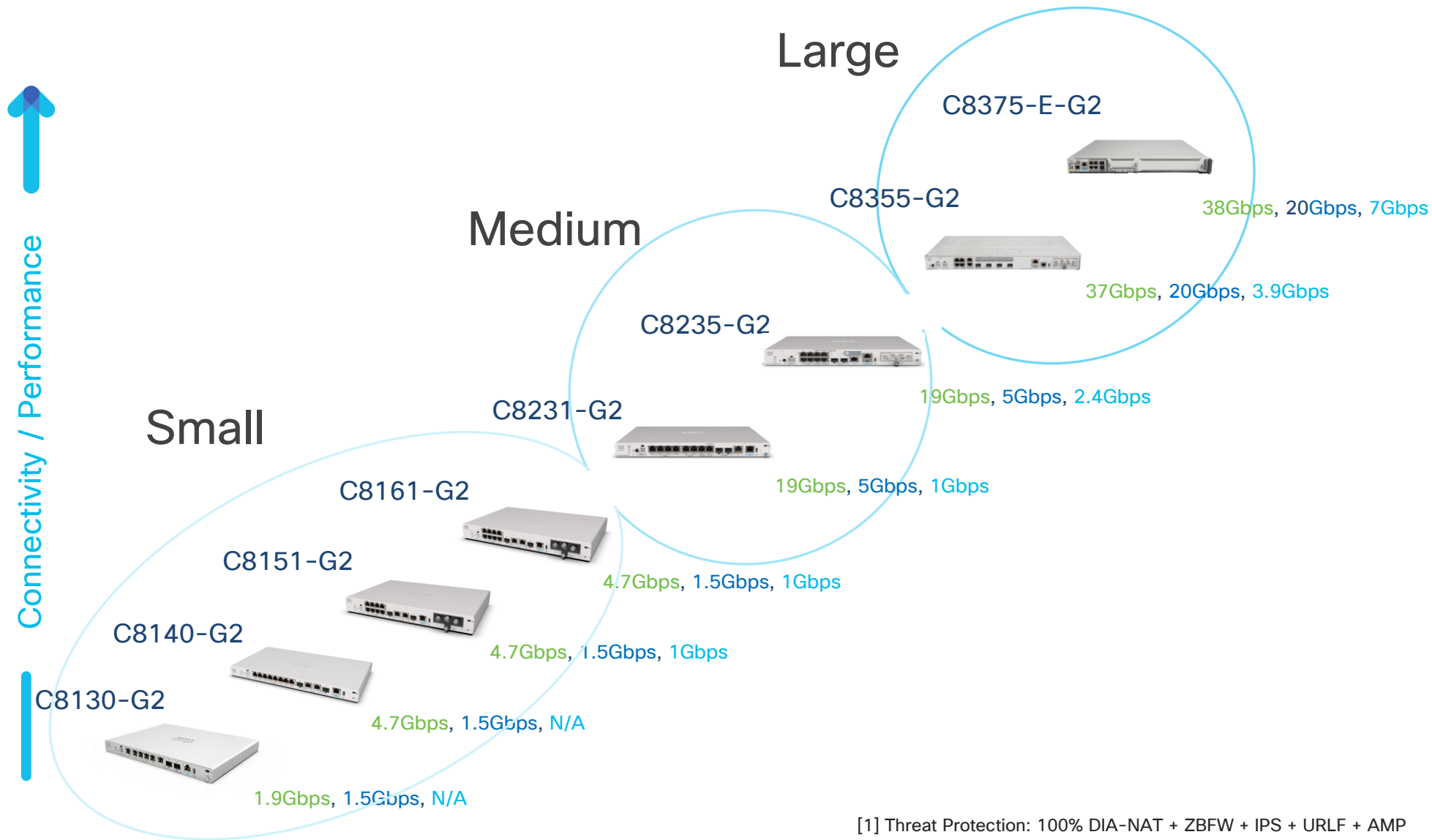
Simplified Licensing

Cisco Networking & Routing Subscriptions

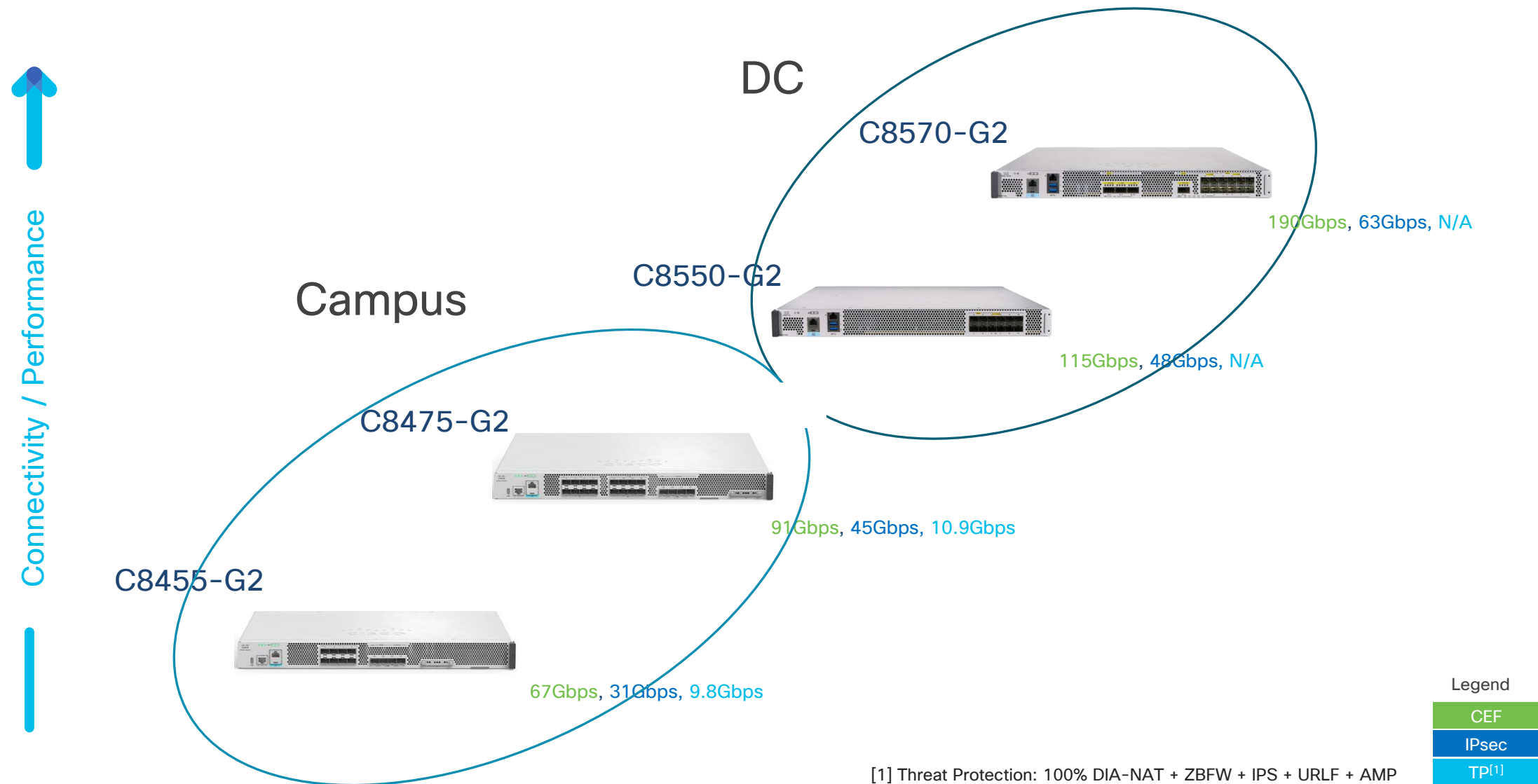


Cisco 8000 Series
Secure Routers

Branch



Data Center and Campus



Secure WAN Ecosystem



An integrated, intelligent architecture combining networking and security to deliver consistent-policy, threat-resilient connectivity at scale.

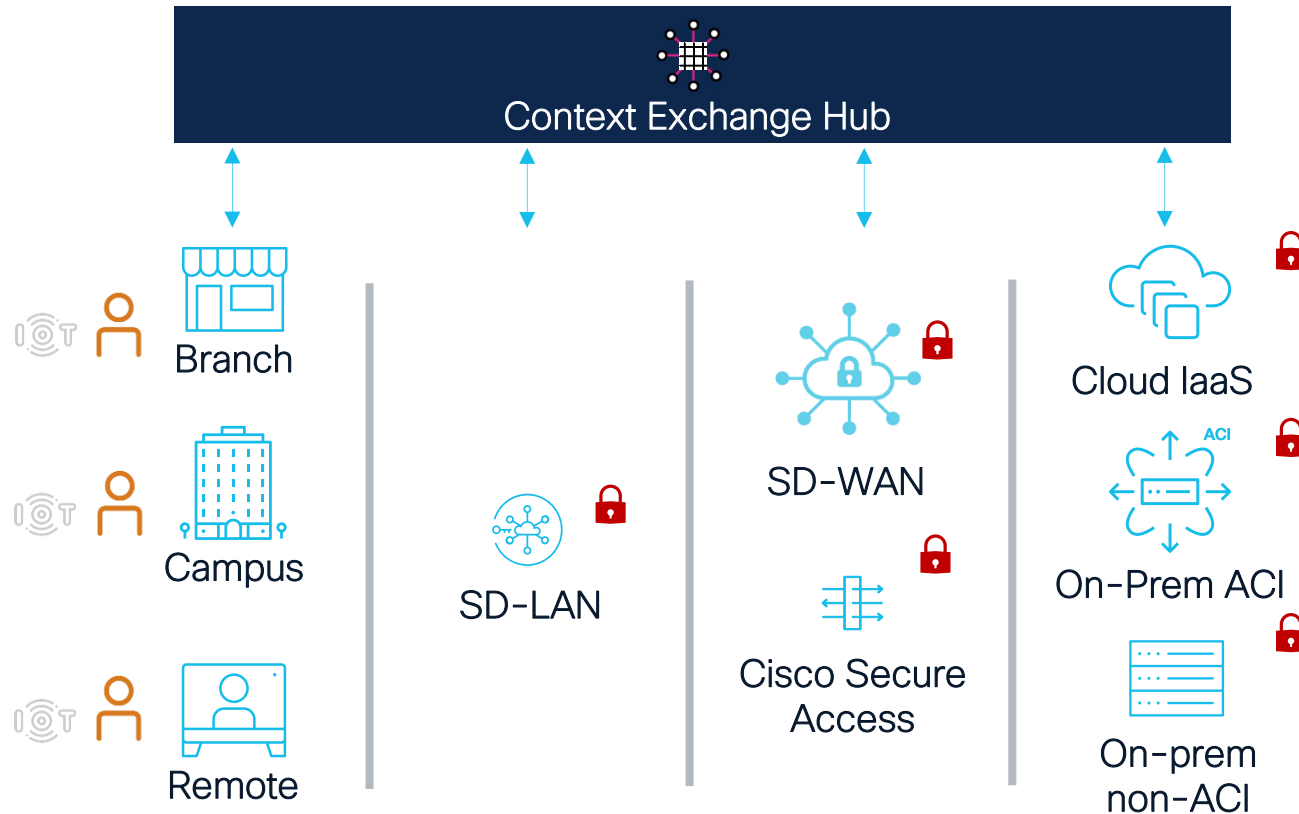
Common Policy Starts with Cisco ISE



Common Policy

Enabling context across domains

 Policy Enforcement Points:
Consistent Policies



Creates consistent access policies regardless of which domain IT chooses to enforce policy

Build context in its local domain and store it as standard security group tags (SGT)

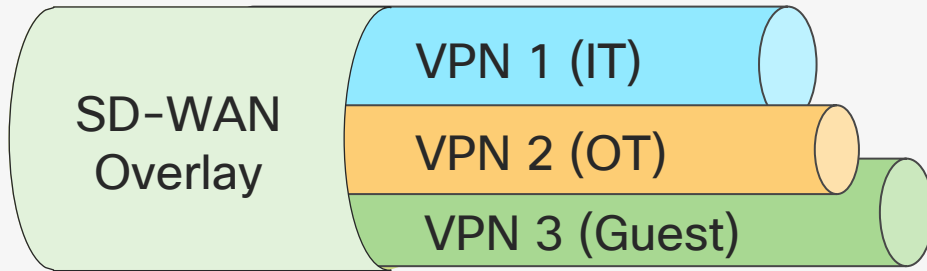
Share context everywhere, across networking and security domains

Enforce consistent SGT-based policies, enable simple and unified policy experience

Context-aware policies for on-premises app and cloud workloads for multiple enforcement points.

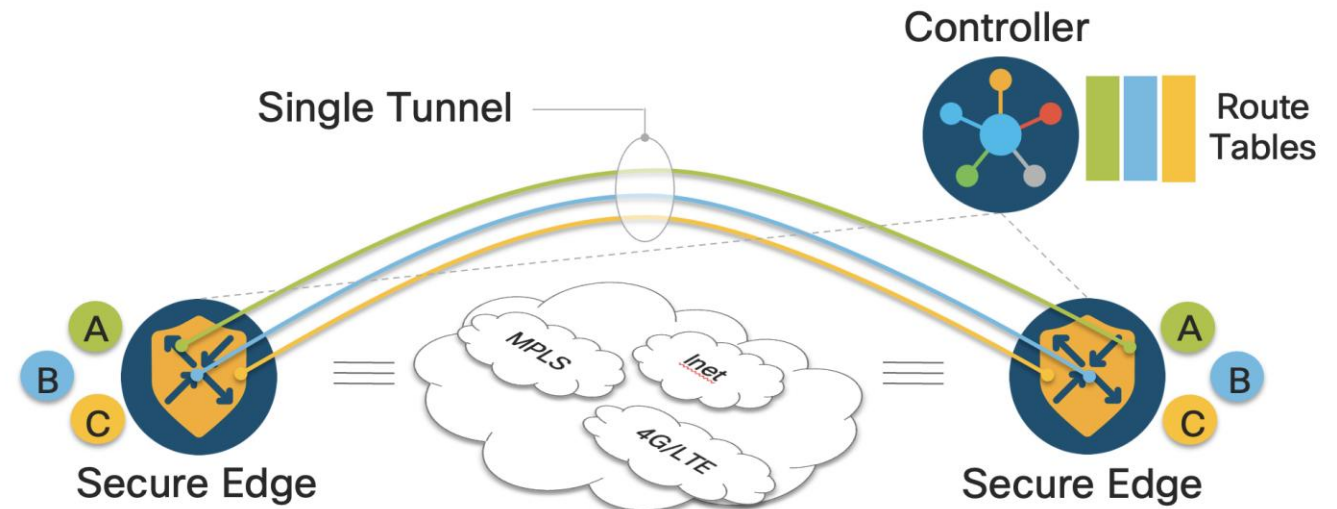
Segmentation is built into SD-WAN

Macro Segmentation

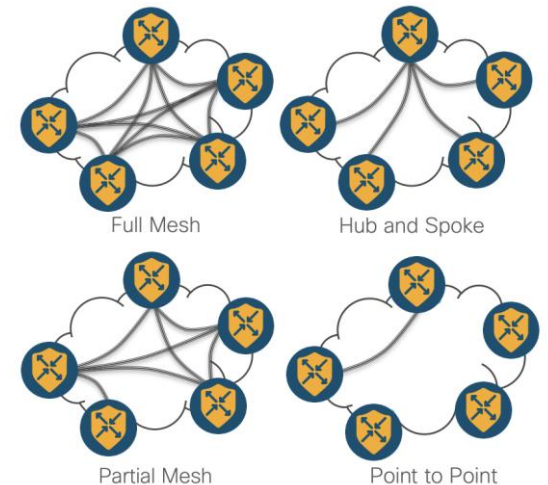


VPN Level Segmentation

- IT VPN
- OT VPN
- Guest VPN

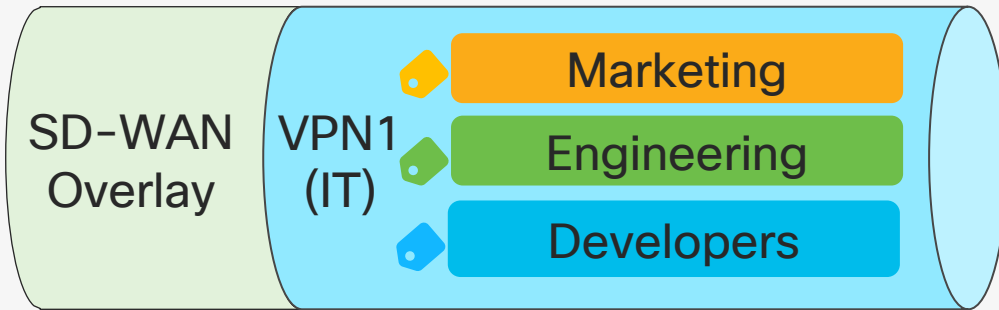


- Segment connectivity across the SD-WAN fabric without reliance on underlay transport
- Secure Edge maintain per-VPN routing table for complete control plane separation



Micro Segmentation with ISE Integration

Micro Segmentation



Group Level Segmentation

Example: IT VPN

- Marketing
- Engineering
- Developers

1 Identify the User/Device

- Cisco ISE is the Identity Provider
- ISE updates SD-WAN Manager

3a Continuously Check Posture

- ISE evaluates device Security Posture
- ISE updates SGT of device

2 Enforce Security Policy

- SD-WAN Manager is the Policy Engine
- Policy created based on Identity

3b Respond to Change in Posture

- SD-WAN Manager learns of change in security
- Security policy is automatically updated



With Catalyst SD-WAN's Micro-Segmentation powered by ISE, dynamically enforce zero-trust policies across the WAN
— so users, devices, and applications are strictly segmented based on identity and risk context.

Secure Router with Next Generation Firewall



L3 - L7 FW

Empower your network with intelligent, multi-layered traffic control and threat defense.



IPS/IDPS

Stop threats in motion with real-time intrusion prevention and detection.



AMP

Block, detect, and remediate advanced malware across your environment.



URL-F

Enable secure, productive access through intelligent web and content filtering.



TLS
Decryption

Reveal hidden risks within encrypted traffic for complete visibility and control.



Sandboxing

Detect unknown threats through advanced file analysis in Cisco Threat Grid.



Encrypted Threat Detection

Defend against encrypted threats without compromising privacy or performance.



Snort DLP*

Safeguard sensitive data and prevent exfiltration with deep content inspection.



File Control*

Enforce security and compliance by managing file transfers by type and policy.

* Future capabilities with NGFW v2 Engine

With Catalyst SD-WAN Hybrid Mesh Firewall, you get a converged security fabric that spans edge to cloud – enforcing policy consistently, detecting threats everywhere, and scaling without complexity.

SD-WAN + SSE Redefining Security for Tomorrow

Integrated SASE

SASE a-la-carte

Build-your-own SASE approach

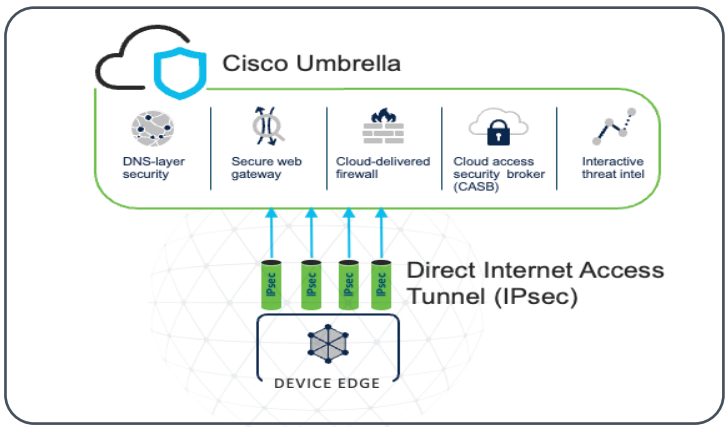
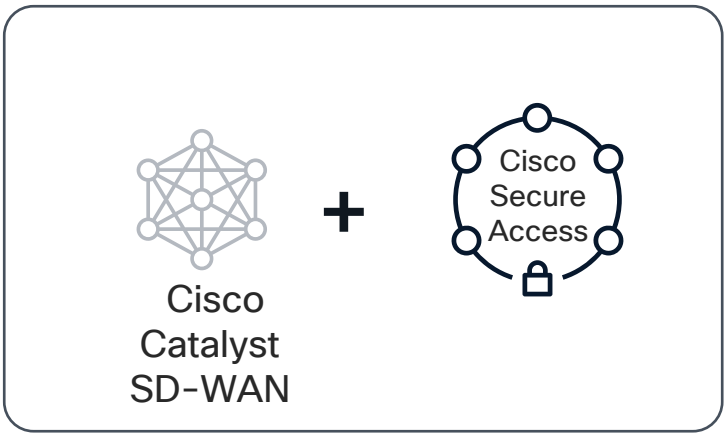


Unified SASE



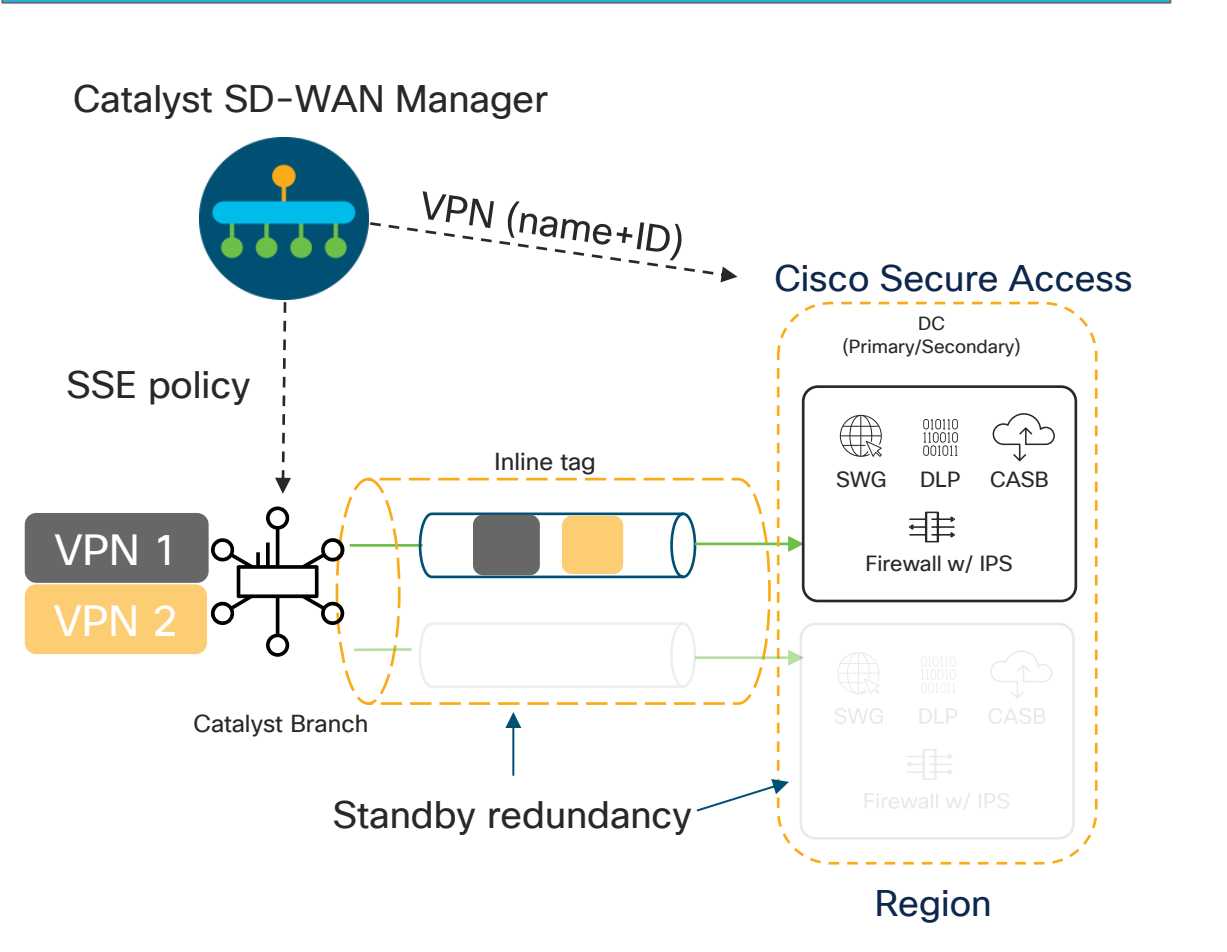
Cisco On Cisco

Cisco on Cisco - Tailored Security for Your Network's Unique Needs

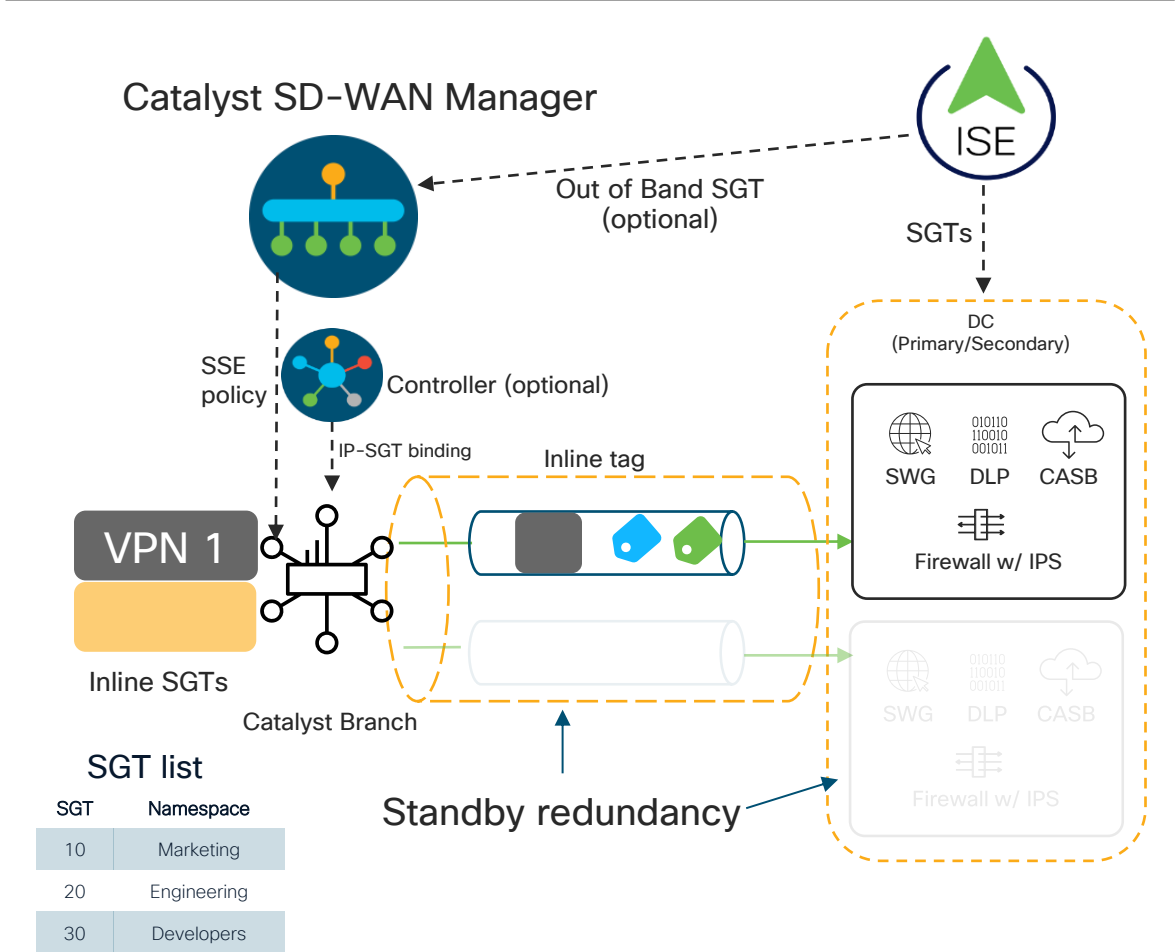


Context-Sharing: Macro / Micro (STG) Segmentation

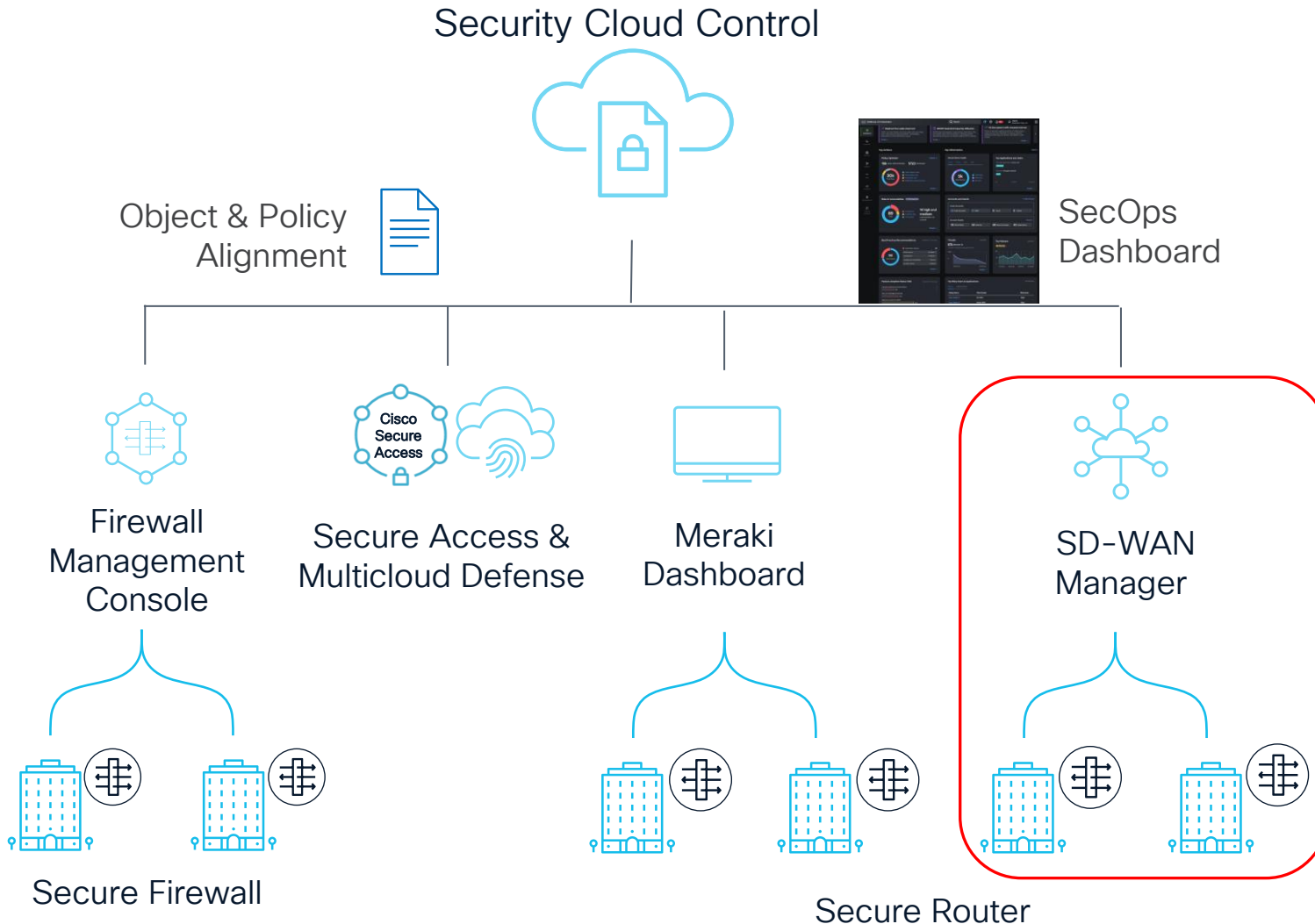
Extending VPN-id Segmentation to Cisco Secure Access



Extending Micro Segmentation (SGT) to Secure Access



Management of Secure Router NGFW using SCC



Security Object/Policy Configuration

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

Monitoring

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

Troubleshooting (Future)

- Leverage SCC tools for security troubleshooting

Management of Secure Router NGFW using SCC

Organization
anz-cpoc

Home

Products

AI Defense

Firewall

Multicloud Defense

Secure Access

Platform services

Favorites

Security Devices

Shared Objects

Platform Management

Home

Top Insights & Alerts

Best practices and recommendation

Multicloud Defense

Account Resources

Security Considerations

Organization
anz-cpoc

Platform menu

Firewall

Dashboard

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Secure Connections

Administration

Platform services

Favorites

Security Devices

Shared Objects

Platform Management

Organization
anz-cpoc

Platform menu

Firewall

Dashboard

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Secure Connections

Administration

Platform services

Favorites

Security Devices

Shared Objects

Platform Management

☐	CloudGW01 VEDGE	Online	Cisco_Cloud01	C8000v
☐	CloudGW02 VEDGE	Online	Cisco_Cloud02	C8000v
☐	DC-Edge1 VEDGE	Online	Data_Center	C8500-12X4QC
☐	DC-Edge2 VEDGE	Online	Data_Center	C8500-12X4QC
☐	IOT-Edge1 VEDGE	Unreachable	jujoubert_IoT	IR1101
☐	IOT-Edge2 VEDGE	Unreachable	datalla_IoT	IR1835
☐	LRG-Edge1 VEDGE	Online	Large_Branch	C8300-1N1S-4T2X
☐	LRG-Edge2 VEDGE	Online	Large_Branch	C8300-1N1S-4T2X
☐	MED-Edge1 VEDGE	Online	Medium_Branch	C8200L-1N-4T
☐	MED-Edge2 VEDGE	Online	Medium_Branch	C8200L-1N-4T
☐	SML-Edge1 VEDGE	Online	Small_Branch	C1111X-8P
☐	SOHO-CG1 VEDGE	Online	jujoubert_Soho	CG522-E
☐	SOHO-Edge1 VEDGE	Online	jujoubert_Soho	C1131X-8PLTEPW
☐	SOHO-Edge2 VEDGE	Online	shamilf_Soho	C1121X-8PLTEPW*
☐	SOHO-Edge4 VEDGE	Online	datalla_Soho	IR1835



Enhanced Cisco Secure Router NGFW Rule Table

Source Zone: Employee_Net_zone → Destination Zone: Untrusted 5

Search

Action

Default Action: Drop

+ Add Rule

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

Rows per page 30

< 1 > Go to: 1 / 1

Single line rule definitions

Color coded actions

Icons for security features

IPS Signature Management using SCC

- Customize rule actions
- Customize Signatures
- Package new rules
- Inherit enterprise packages
- Group overrides

Policy Groups > Objects & Profiles

Custom_SigSet

Base Policy Security

Alert 659

Disabled 28358

Drop 22282

Rewrite 0

Overridden 0

Base policy

Group overrides

Rule overrides

All Rules

Overridden rules

Local groups 3

Rule categories 9

Malware 5

Exploit Kit

Backdoor

Tools

Other

Command and Control

File 9

Intrusion prevention rules

Alert 56 Disabled 7150 Drop 4985 Rewrite 0 Overridden 0

Search

Rule Action

	GID:SID	Rule details	Rule action	Assigned groups	Set by	
>	1:20558	EXPLOIT-KIT URI request for known malicious URI /stat2...	Drop (default)	Exploit Kit	Base policy	...
>	1:20668	EXPLOIT-KIT URI request for known malicious URI - /con...	Alert	Exploit Kit	Base policy	...
>	1:20669	EXPLOIT-KIT URI request for known malicious URI - w.p...	Disable (default)	Exploit Kit	Base policy	...
>	1:21041	EXPLOIT-KIT Blackhole exploit kit URL - main.php?page=	Drop (default)	Exploit Kit	Base policy	...
>	1:21042	EXPLOIT-KIT Blackhole exploit kit post-compromise do...	Drop (default)	Exploit Kit	Base policy	...
>	1:21043	EXPLOIT-KIT Blackhole exploit kit post-compromise do...	Drop (default)	Exploit Kit	Base policy	...
>	1:21044	EXPLOIT-KIT Blackhole exploit kit landing page	Drop (default)	Exploit Kit	Base policy	...
>	1:21045	EXPLOIT-KIT Blackhole exploit kit landing page	Drop (default)	Exploit Kit	Base policy	...
>	1:21068	EXPLOIT-KIT Flashers exploit kit landing page	Drop (default)	Exploit Kit	Base policy	...

Cancel

Save

Rows per page 30

< 1 2 3 4 5 ... 407 >

Go to: 1 / 407

Pick the rule categories to edit

Edit the action of any Rule

Add comments to track changes
Duplicate any Rule to build custom signatures

Duplicate
Comment

Detailed FW Log visualization using SCC

Logs

As of: Oct 24, 2023 15:25

AlarmsEventsAudit logsACL LogsTraffic Logs

Set criteria to get events

HistoricalLive

Select device *

uw11uw12

Time period *

24 hours

Rule name

Rule name

Source IP

Source IP

Destination IP

Destination IP

Application

Application

Username/User Group

Username/User Group

SGT

SGT

Destination port

Destination port

+ Advanced

100 results

Get log

Reset

Save filter

Search

Export

Time of occurrence	Hostname	Device system IP	Source IP	Destination IP	Source port	Destination port	Protocol	Application details	Username/SGT	Rule name	FW Policy name	FW action	
Mar 15, 2024 04:52 AM	SJ Branch	1.1.1.1	192.168.20.10	151.101.195.5	65987	443	HTTP	CNN	john	Internet_Traffic	West_Coast_Policy	Inspect	...
Mar 15, 2024 04:51 AM	NY Branch	1.1.1.2	192.168.20.11	151.101.195.6	65988	444	FTP	Facebook	karl	Internet_Traffic1	East_Coast_Policy	Inspect	...
Mar 15, 2024 04:50 AM	CA Branch	1.1.1.3	192.168.20.12	151.101.195.7	65989	445	DNS	CNN	juan	Internet_Traffic2	South_Pacific_Policy	Inspect	...
Mar 15, 2024 04:30 AM	MI Branch	1.1.1.4	192.168.20.13	151.101.195.8	65990	446	HTTPS	Fox News	sara	Internet_Traffic3	Americas_Policy	Inspect	...
Mar 15, 2024 04:29 AM	DE Branch	1.1.1.5	192.168.20.14	151.101.195.9	65991	447	FTP	X	lucy	Internet_Traffic4	European_Policy	Inspect	...

Granular Visibility

- Detailed FW log visualization including NGFW functions

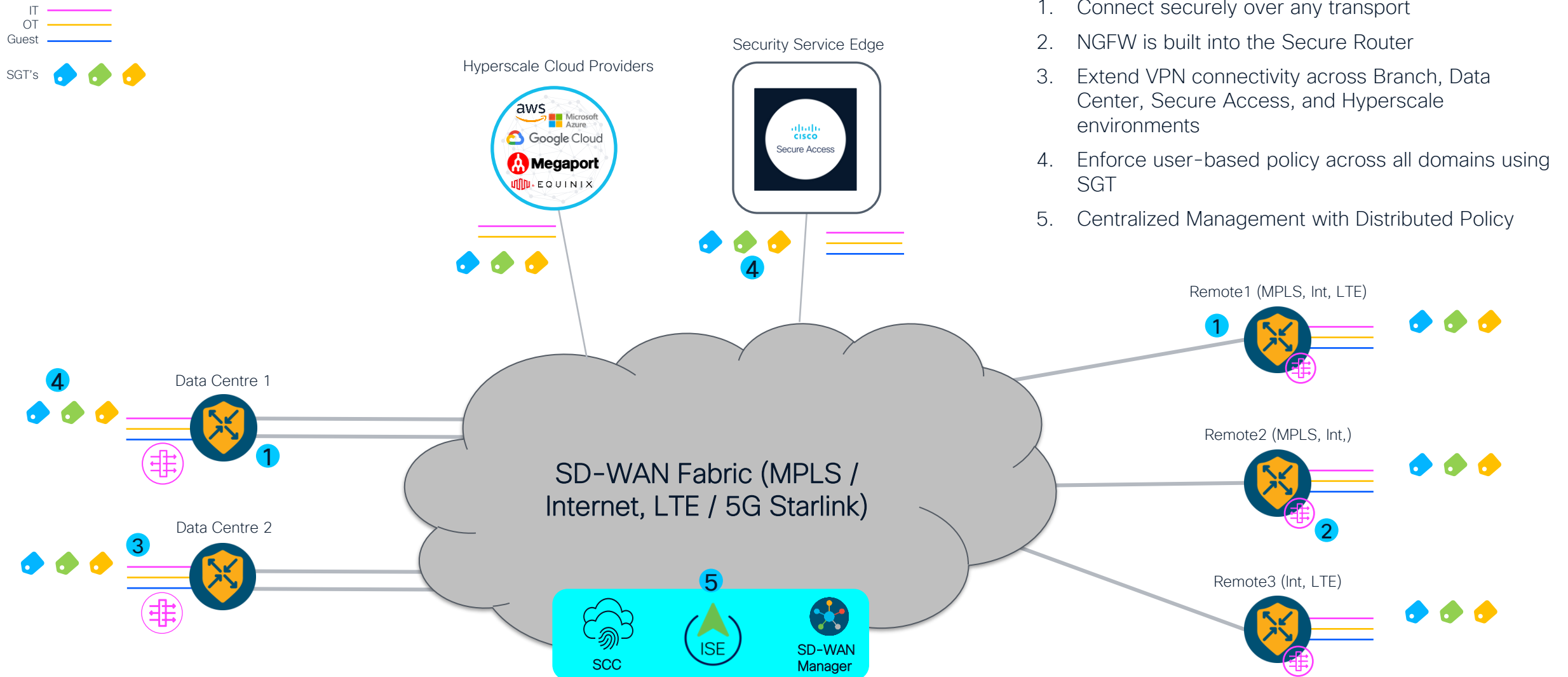
Customized Queries

- Query table provides refined log retrieval

Data Retention

- Leverage Analytics to store logs for up to 1 month

Cisco SD-WAN and SASE: Bringing It All Together



Complete your session evaluations



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



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



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



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



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

Contact me at: Insert preferred comms method

Thank you

CISCO Live !

