cisco Connect

GO BEYOND

#CiscoConnect

Campus Zero-Trust:

Transformez votre réseau pour le rendre plus programmable, sécurisé et modulaire (CI)

Thomas Matzeu, Technical Solutions Architect
tmatzeu@cisco.com
Sébastien Fernandez, Technical Solutions Architect
sebastfe@cisco.com

Track 3 - Session 2

Agenda

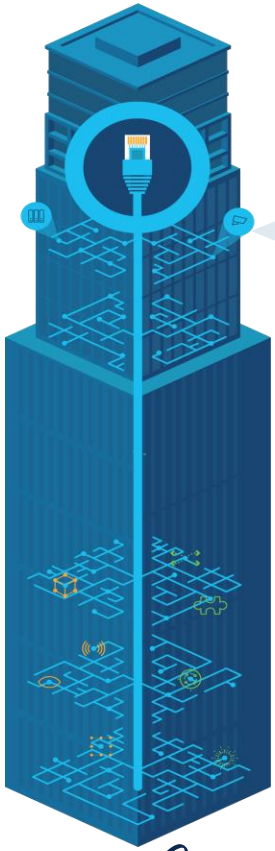
- Challenges & Limitations of Traditional LANs Campus
- Fabric IP & Fabric SDA
- Native Zero-Trust
- Conclusion

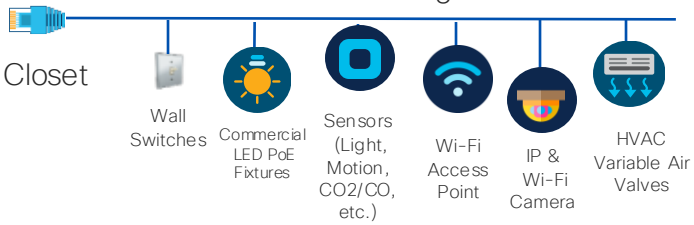
Agenda

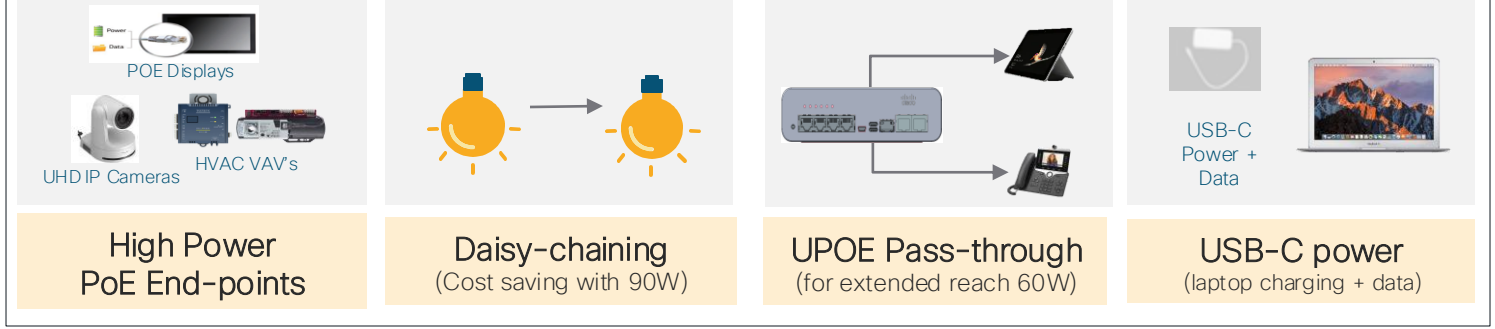
- Challenges & Limitations of Traditional LANs Campus
- Fabric IP & Fabric SDA
- Native Zero-Trust
- Conclusion

Challenges & Limitations of Traditional LANs Campus

90W UPOE+ Standard driving new IT/OT Use Cases

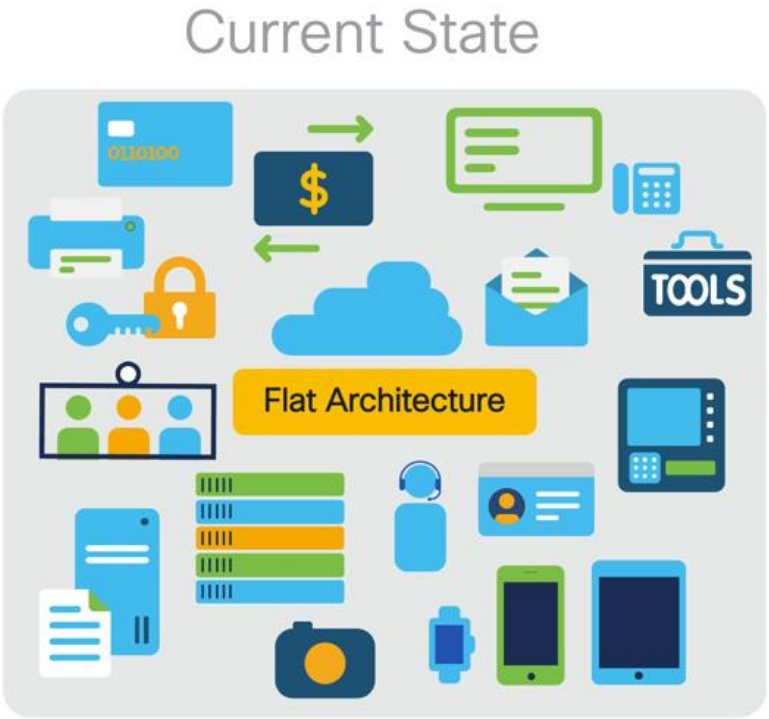






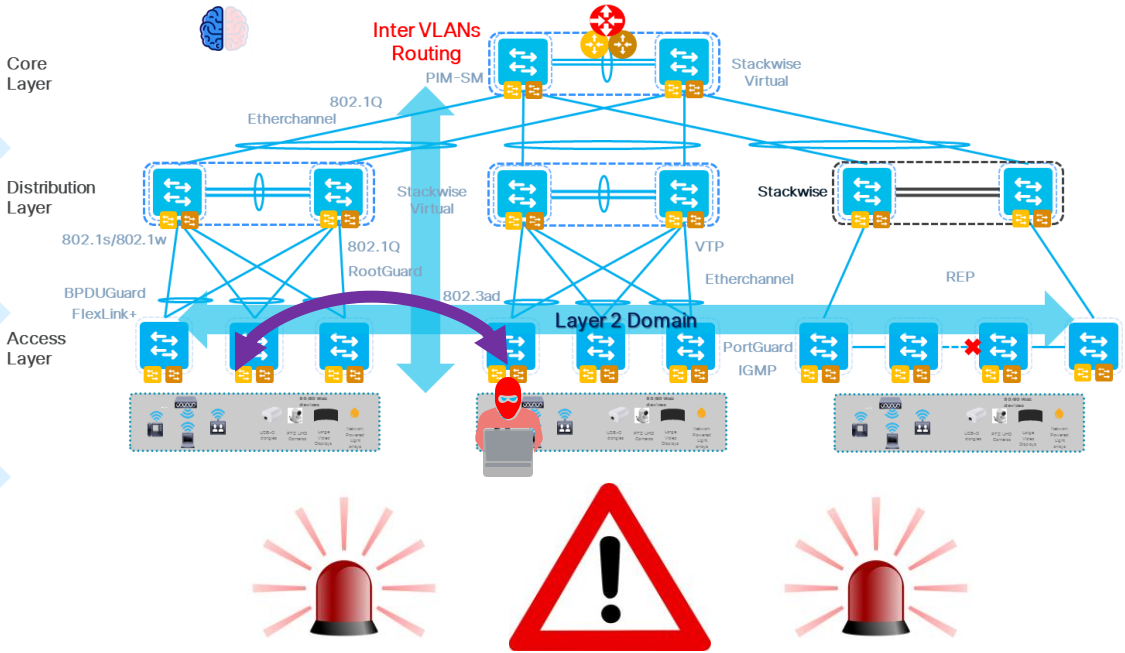
Challenges & Limitations of Traditional LANs Campus

Transition from Flat Network to Zero Trust Segmentation



Challenges & Limitations of Traditional LANs Campus

- Urbanization & Mobility
- High Availability & Reliability
- Programmability & Agility
- Security & Zero-Trust



Challenges & Limitations of Traditional LANs Campus

Urbanization & Mobility

High Availability & Reliability

Programmability & Agility

Security & Zero-Trust

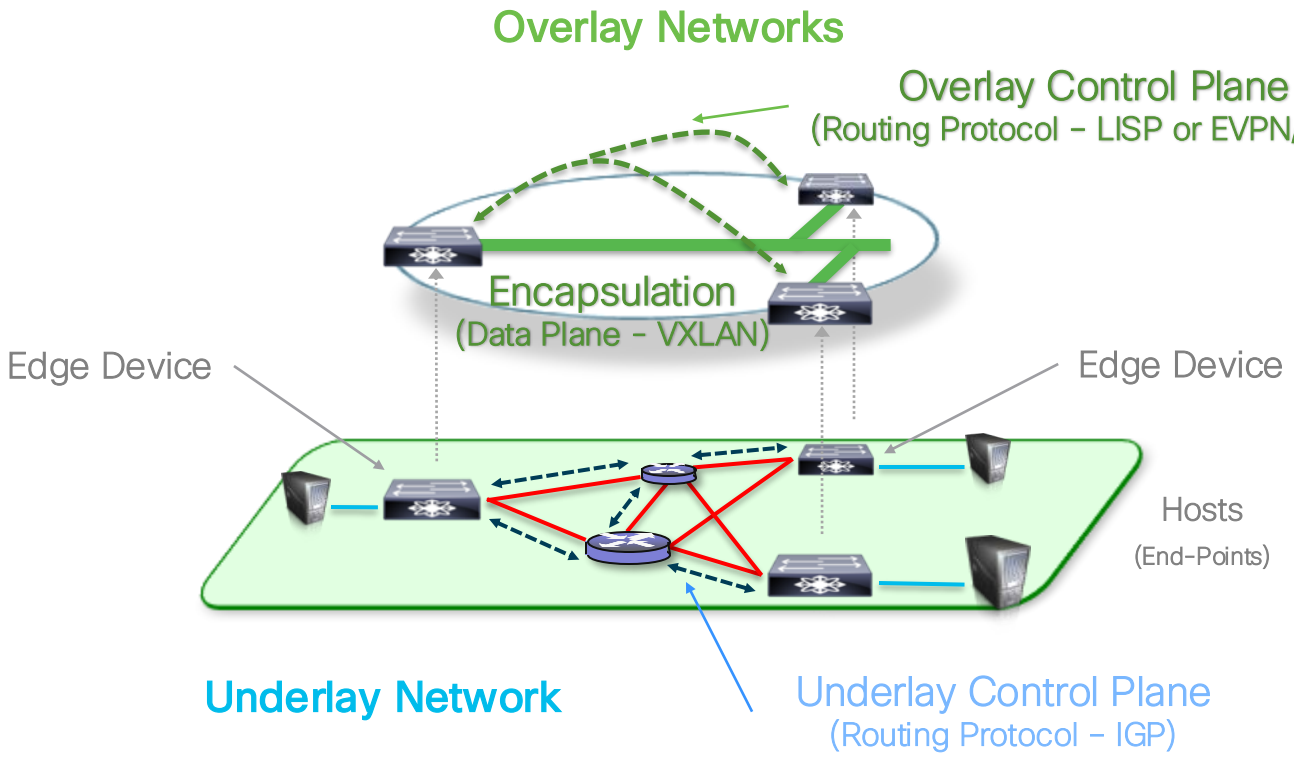
Needs for Level 2 Services without the constraints and difficulties induced by Level 2 Architectures

Agenda

- Challenges & Limitations of Traditional LANs Campus
- Fabric IP & Fabric SDA
- Native Zero-Trust
- Conclusion

Fabric IP – The Fundamentals

Level 3 Architecture: Robustness, Resilience, Programmability, “Scale-out” Model…



Robustness

Resilience

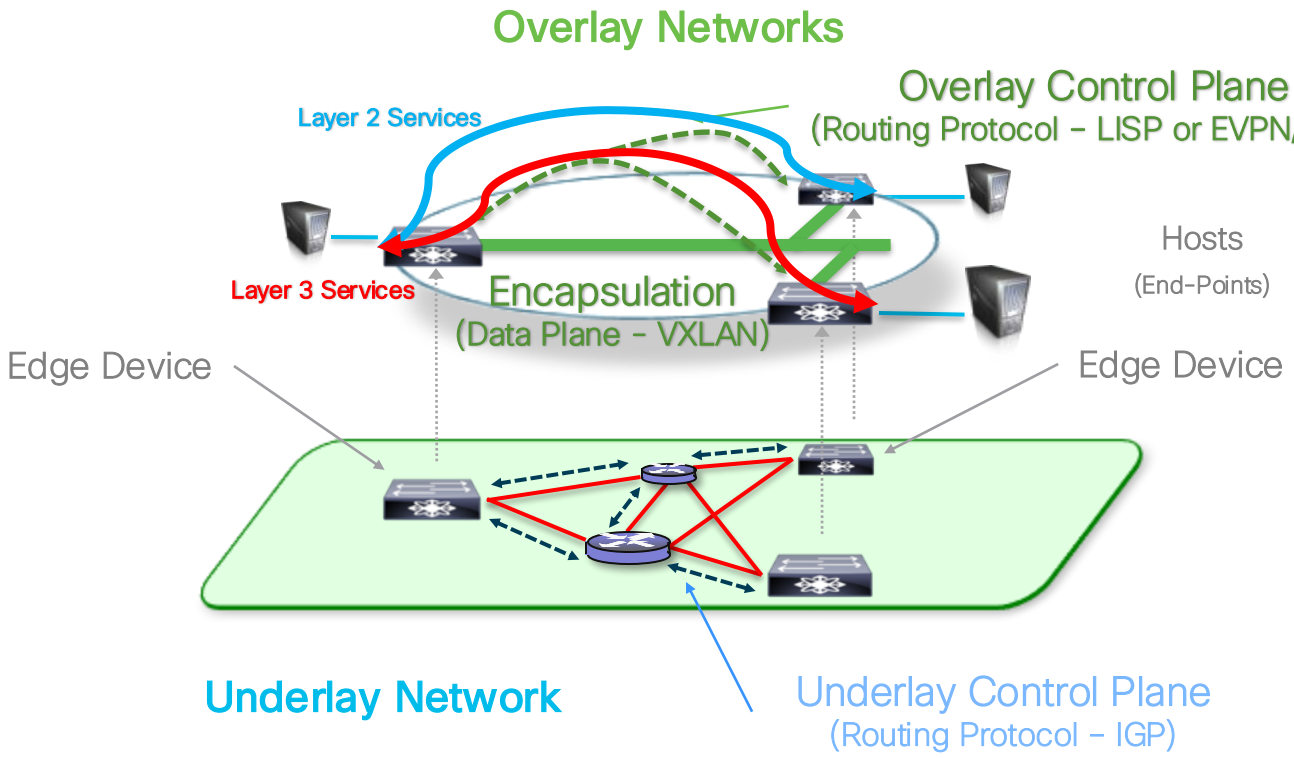
Programmability

“Scale-out” Model

Value ➔ Access

Fabric IP – The Fundamentals

Level 3 Architecture: Robustness, Resilience, Programmability, “Scale-out” Model…



Robustness

Resilience

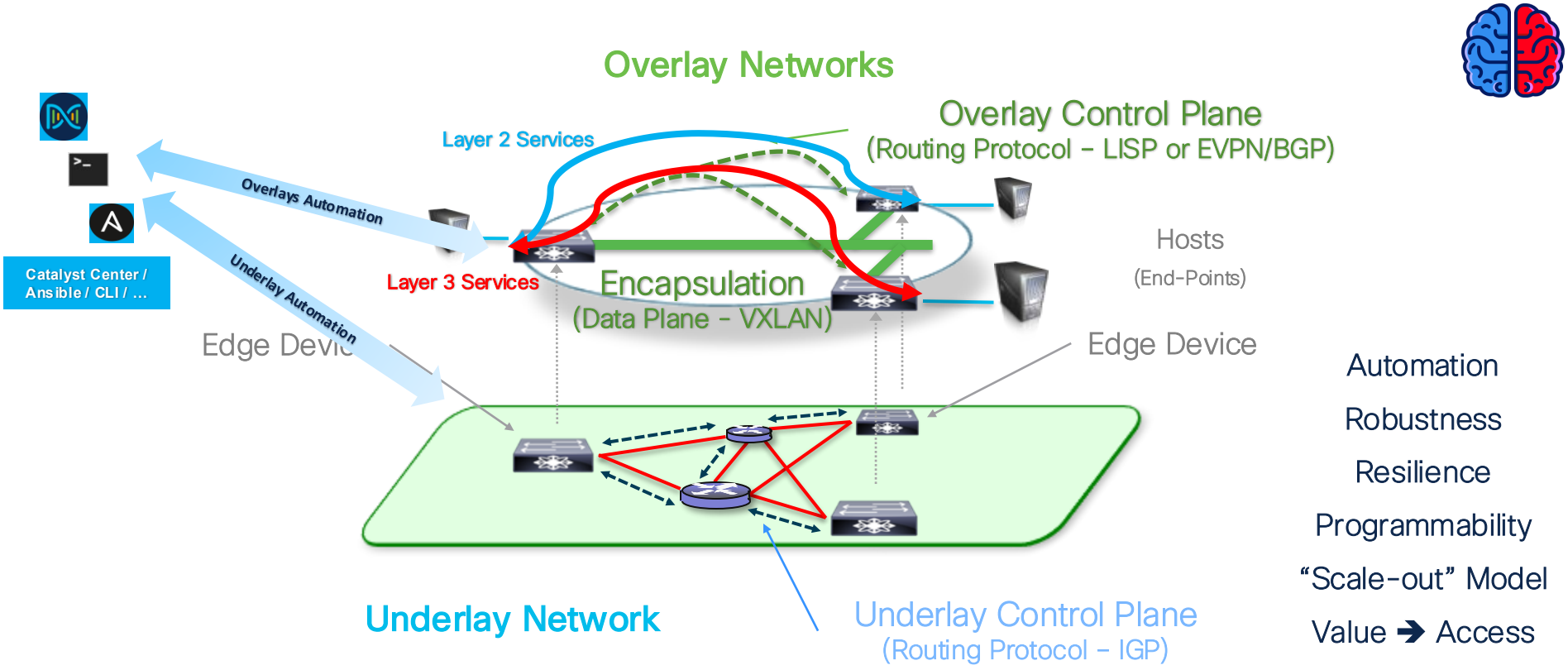
Programmability

“Scale-out” Model

Value ➔ Access

Fabric IP – The Fundamentals

Level 3 Architecture: Robustness, Resilience, Programmability, “Scale-out” Model…



Automation

Robustness

Resilience

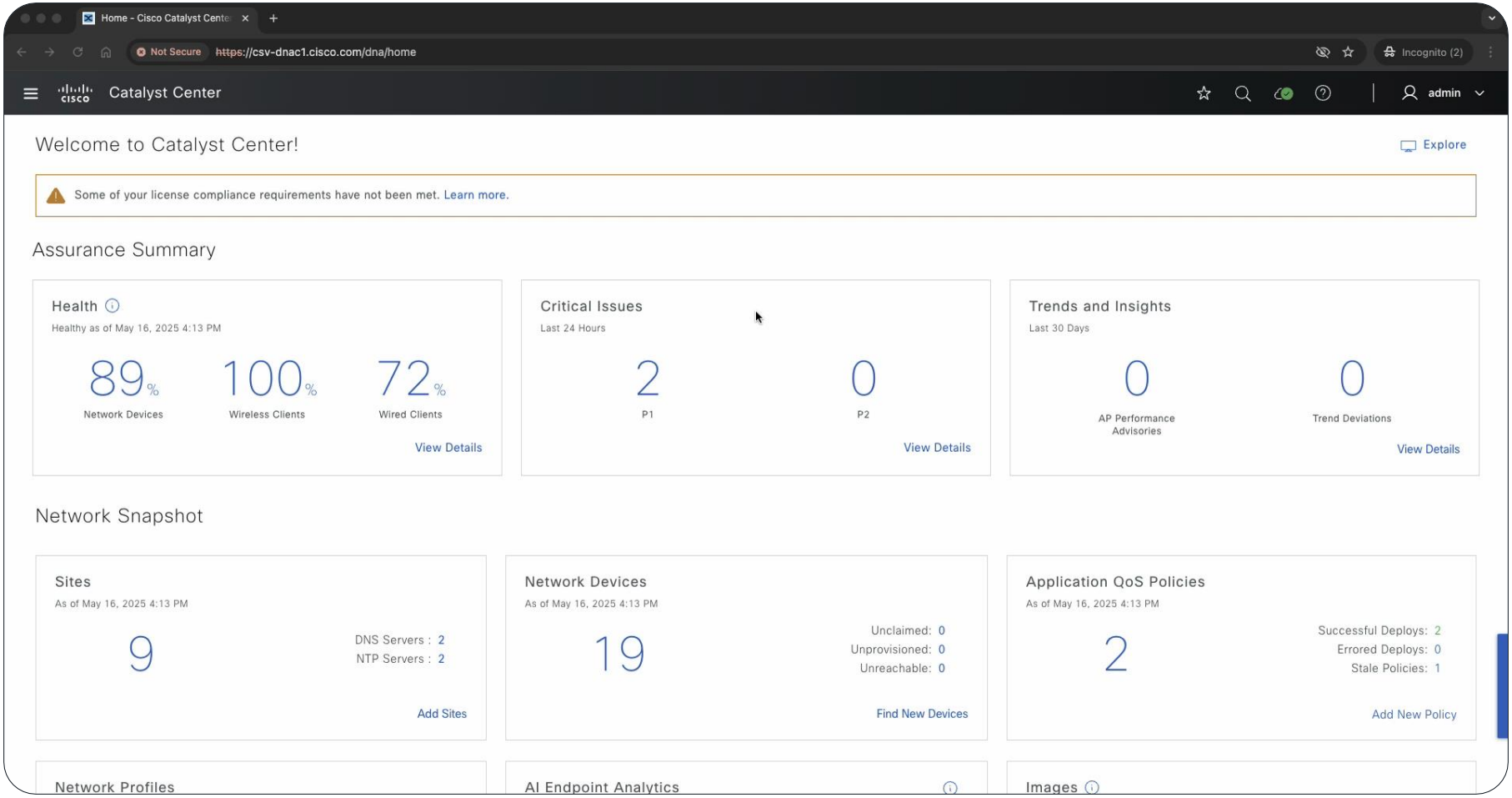
Programmability

“Scale-out” Model

Value ➔ Access

Demo / Video 1

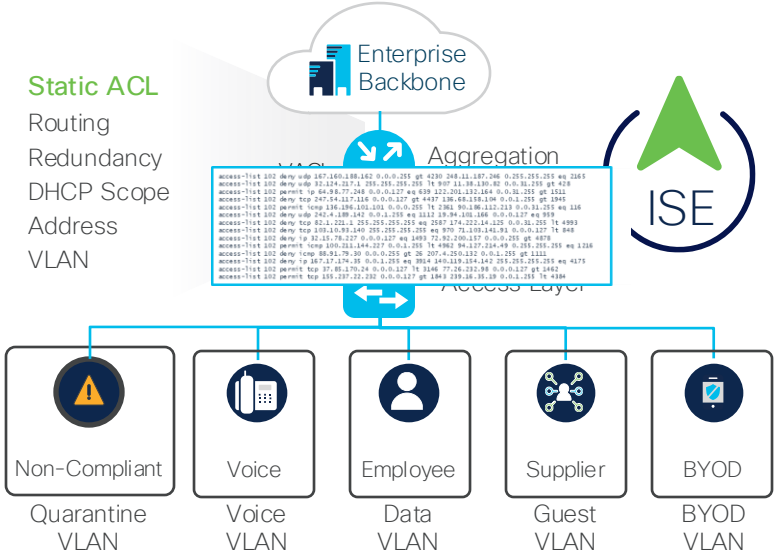
Video showing how to automate
an Edge Node in a Fabric (NetOps) ...



TrustSec

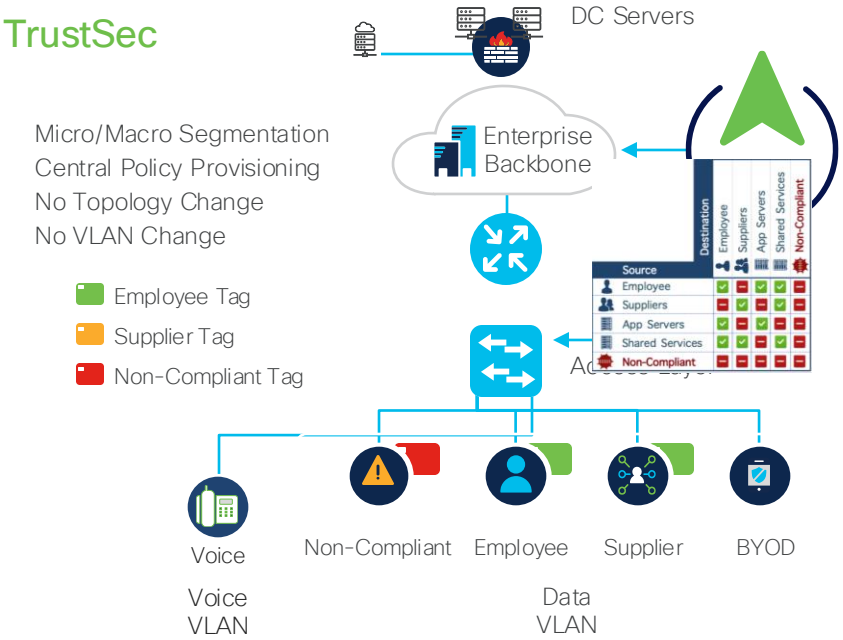
Group Based Policy Simplifies Segmentation

Traditional Segmentation



Security Policy based on Topology
High cost and complex maintenance

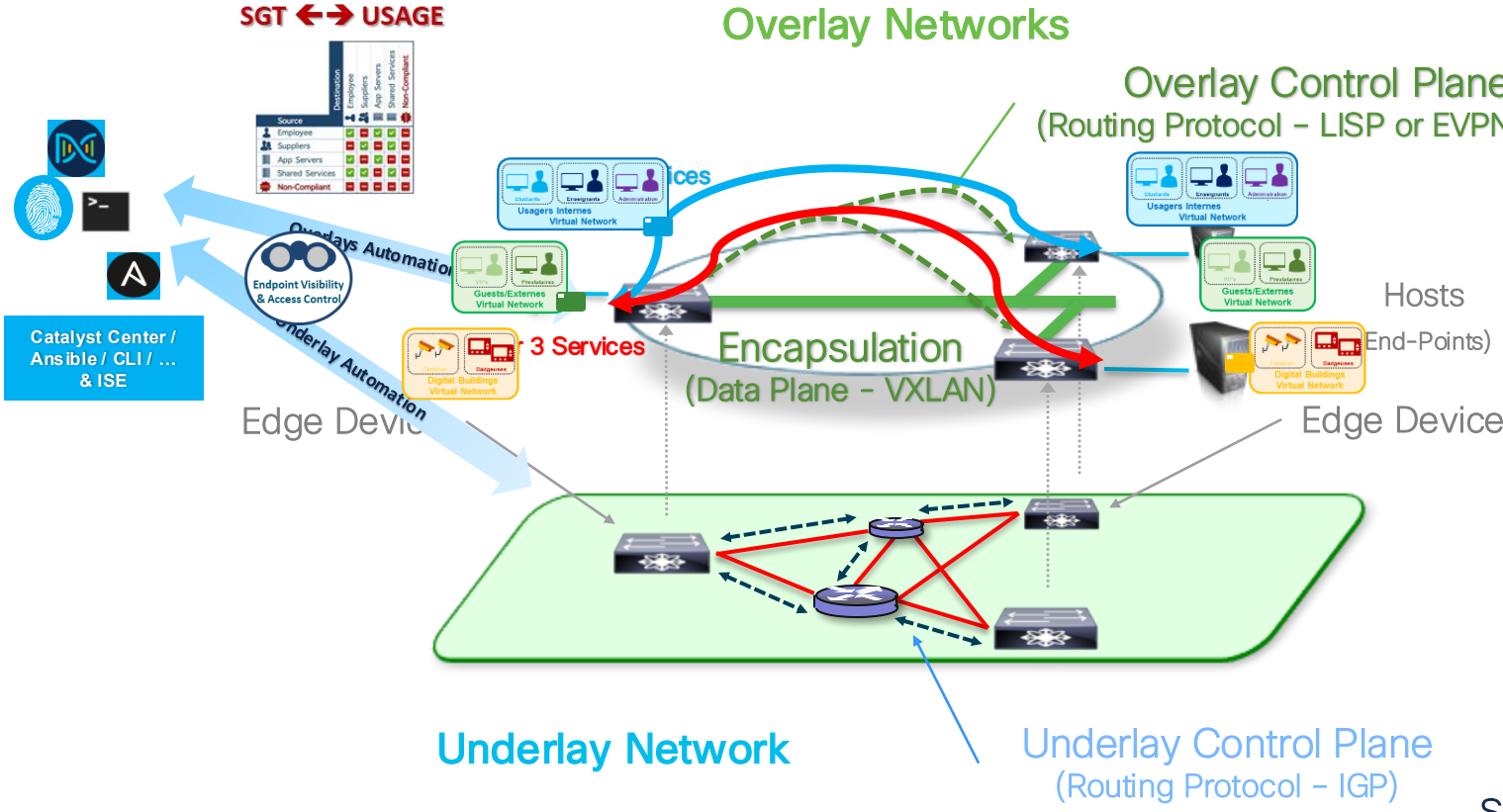
TrustSec



Use existing topology and automate
security policy to reduce OpEx

SD-Access: IP Fabric + Automated Security Services

"Security Plane": Access Control + Macro & Micro Segmentation…



Automation

Access Control

Macro & Micro Segmentation

VXLAN: Transport of Segmentation

Identity-based Segmentation & Mobility

SD-Access: 2 technological offers

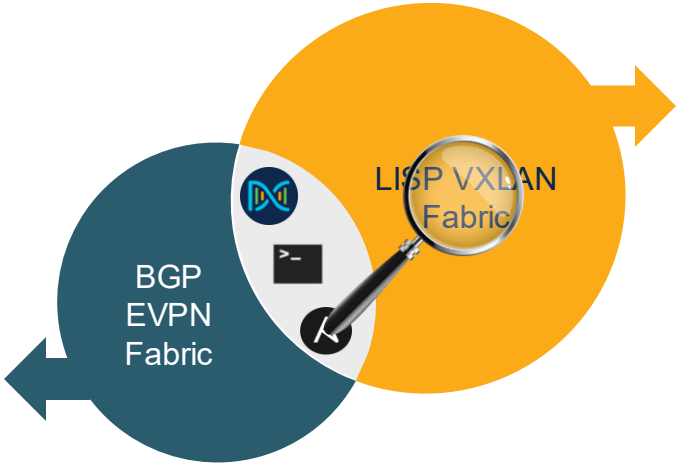
Flexibility in Fabric options according to Customer needs

CUSTOMER PROFILE:
"Network Centric"
Go with *Fabric IP with BGP EVPN*

One Fabric Technology (Campus & DC)
Operational ease with a single familiar protocol

Multi-vendor interoperability
Vendor-agnostic solution with unique Cisco differentiators

Segmentation
Zero-Trust Architecture with Micro and Macro Segmentation with customizable Overlay Network Types and Topologies.



CUSTOMER PROFILE:
"Identity Centric"
Lead with *Fabric IP with LISP*

Network Simplification
Lightweight, extensible, massive scale with rapid convergence. Single overlay for wired/wireless

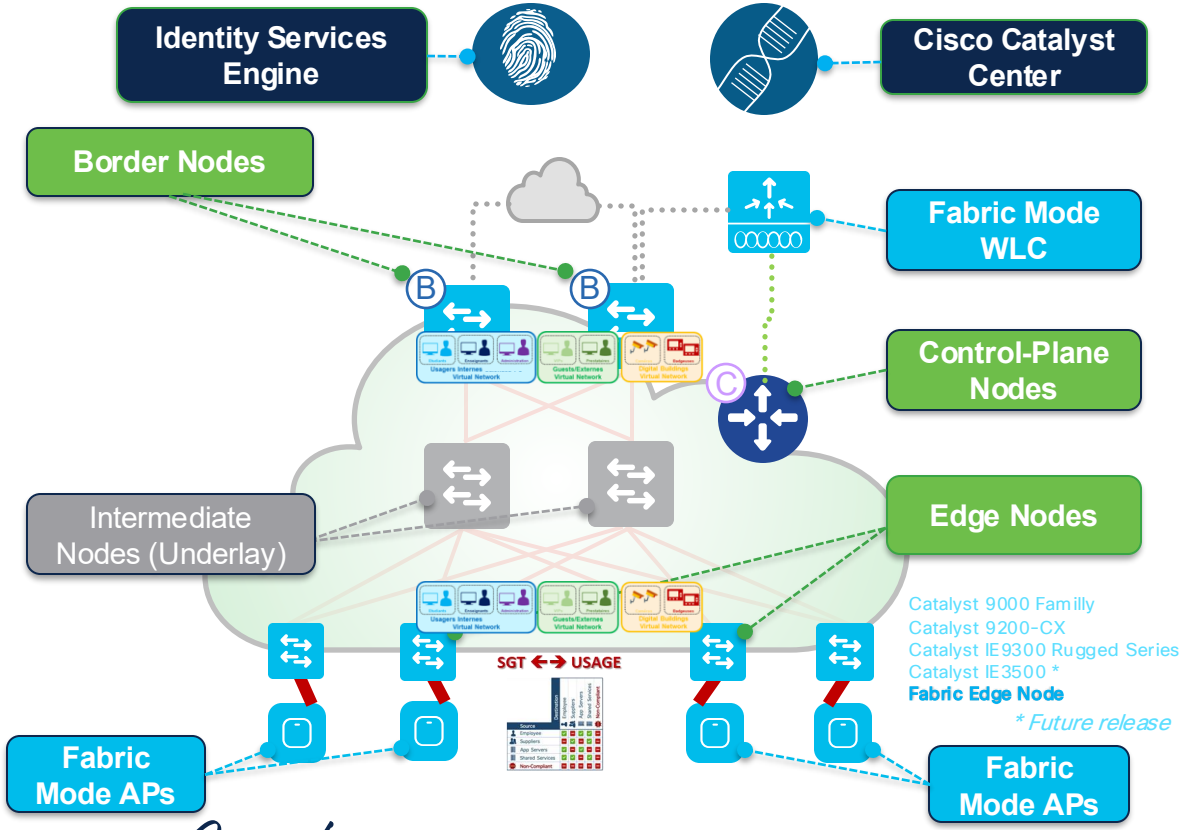
Mobility First Requirement
Fabric Integrated Wireless, L2 Mobility, Enhanced wireless performance

Segmentation
Zero-Trust Architecture with Unified Wired + Wireless Policy

One Infrastructure | Single Data plane | Consistent Zero-Trust Experience

Fabric IP – SDA-LISP

Roles & Terminologies



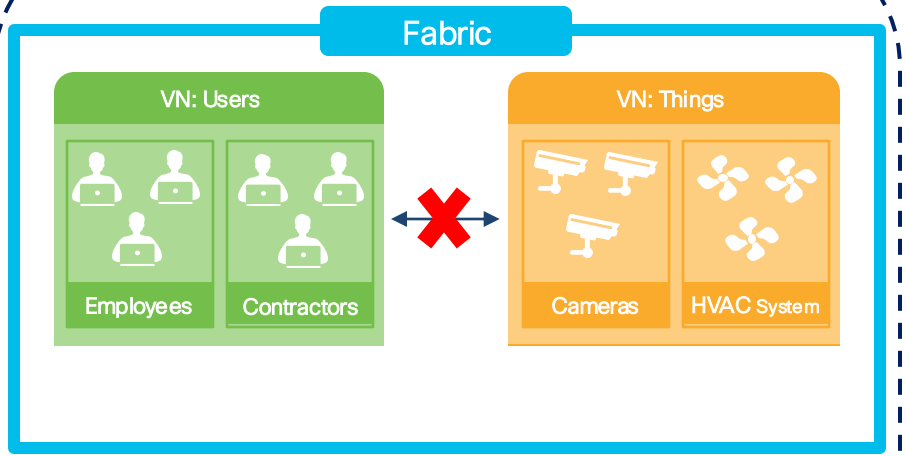
Fabric SDA-LISP - Compatibility Matrix
https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/catalyst_center_compatibility_matrix/index.html

- **Cisco Catalyst Center** – Automation appliance for fabric automation, policy and assurance
- **ISE – Identity Service Engine** – advanced AAA solution, implements segmentation using trustsec
- **Control-Plane Nodes** – Map System that manages Endpoint ID to Device relationships. Can be collocated with Border Node
- **Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Fabric Wireless Controller** – Wireless Controller (WLC) that is fabric-enabled
- **Fabric Mode APs** – Access Points that are fabric-enabled.

Fabric IP – SDA-LISP

Policy Segmentation Strategy

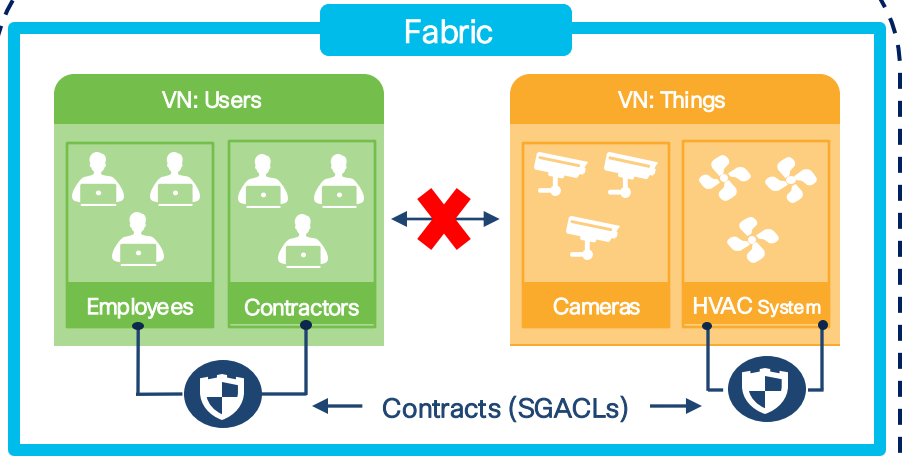
Macro Segmentation



Virtual Network (VN)

- VN = VRF = LISP Instance ID
- Complete Isolation between VN's
- Default Policy: No communication

Micro Segmentation

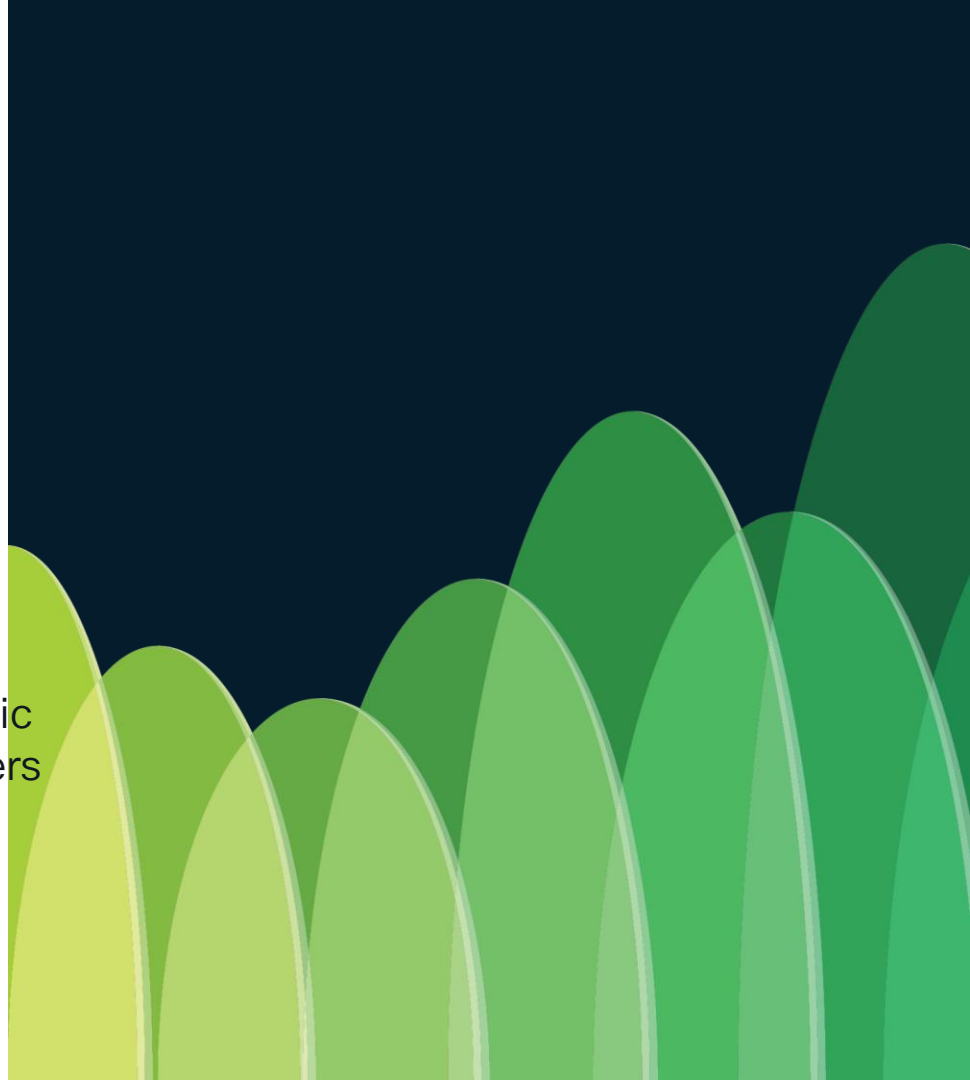


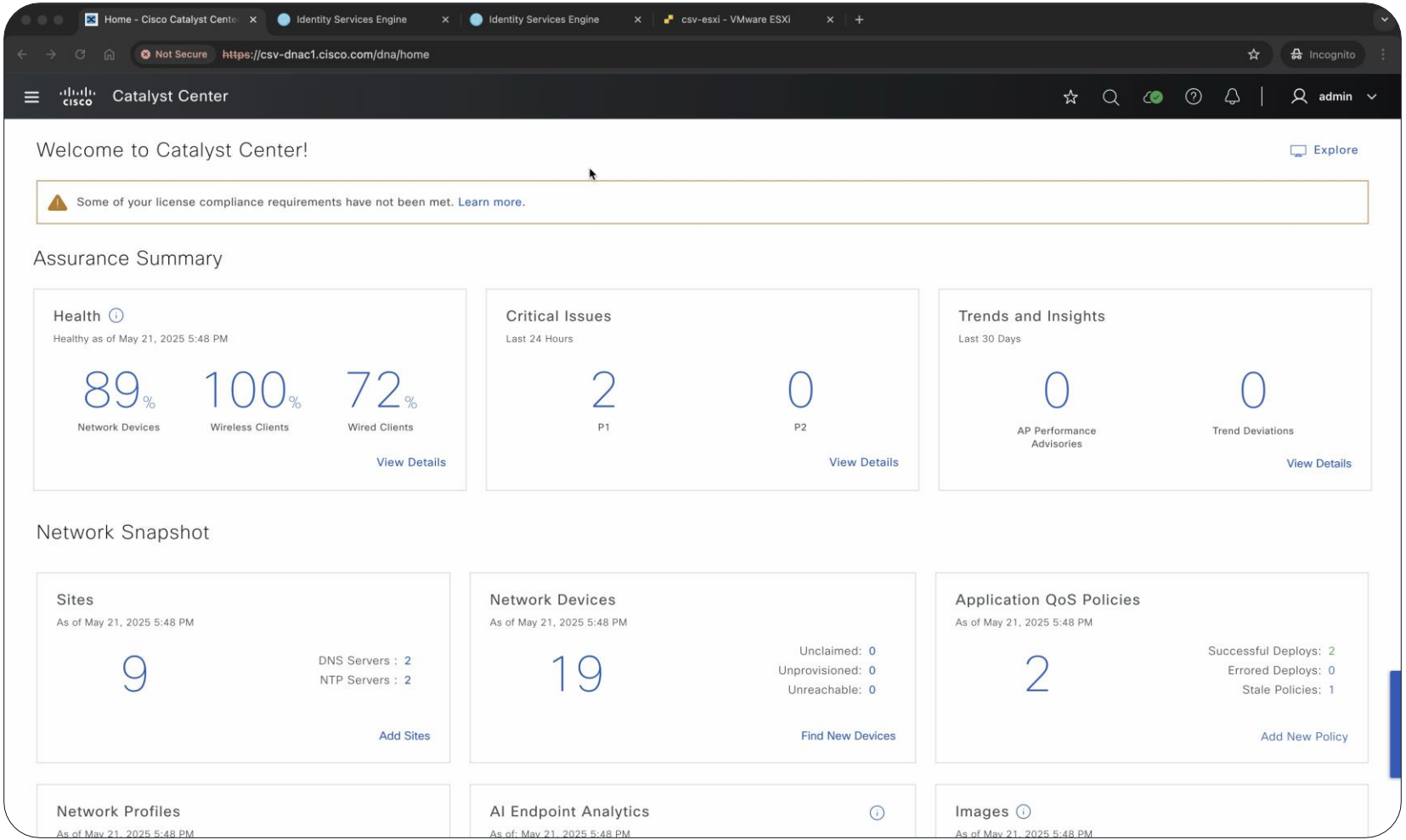
Security Group Tag (SGT)

- Location Independent Policy
- Simple Permit/Deny/Contracts
- Default Policy: Permit/Deny

Demo / Video 2

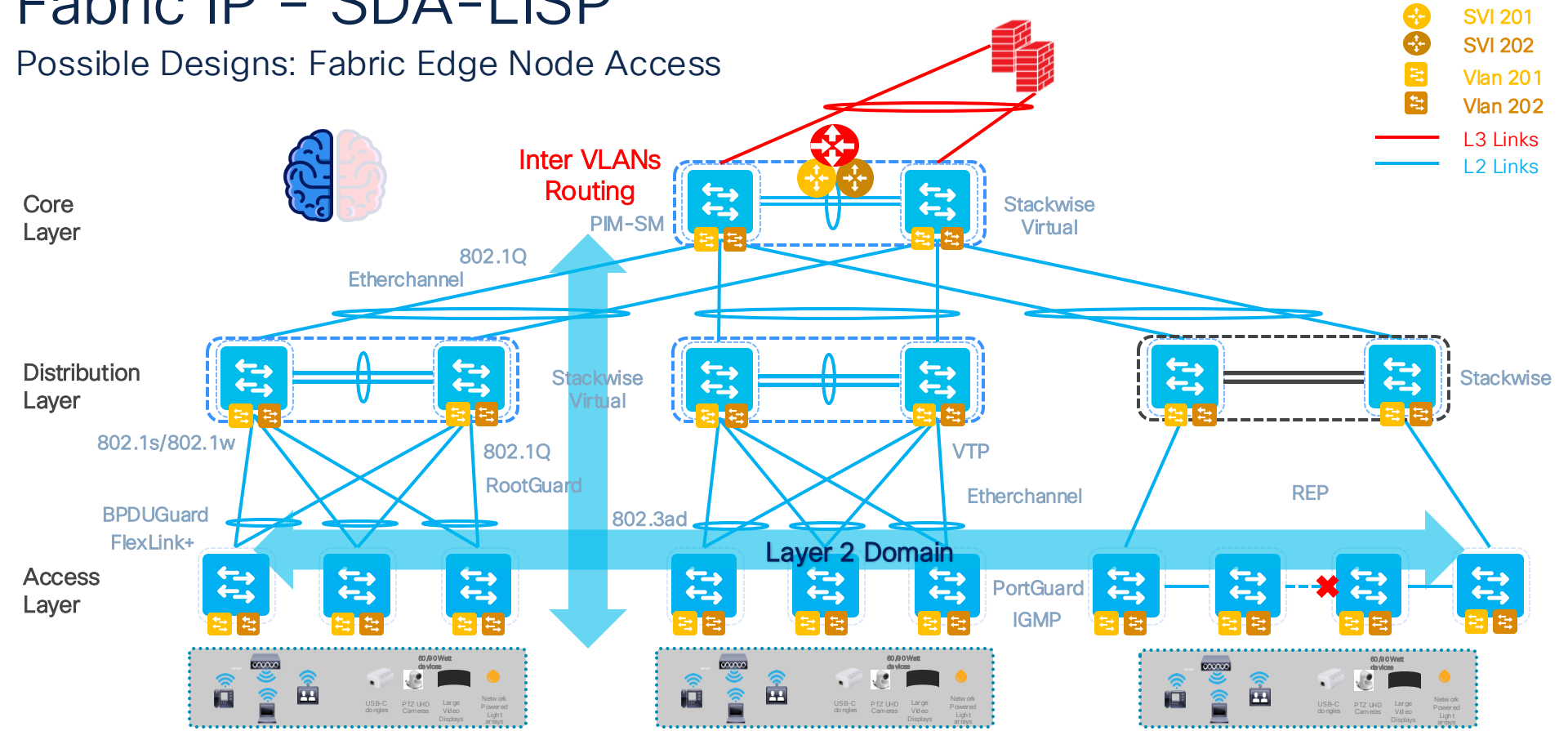
Video showing how to apply an Identity Centric Policy Model (SGT) between multiple end users (SecOps) ...





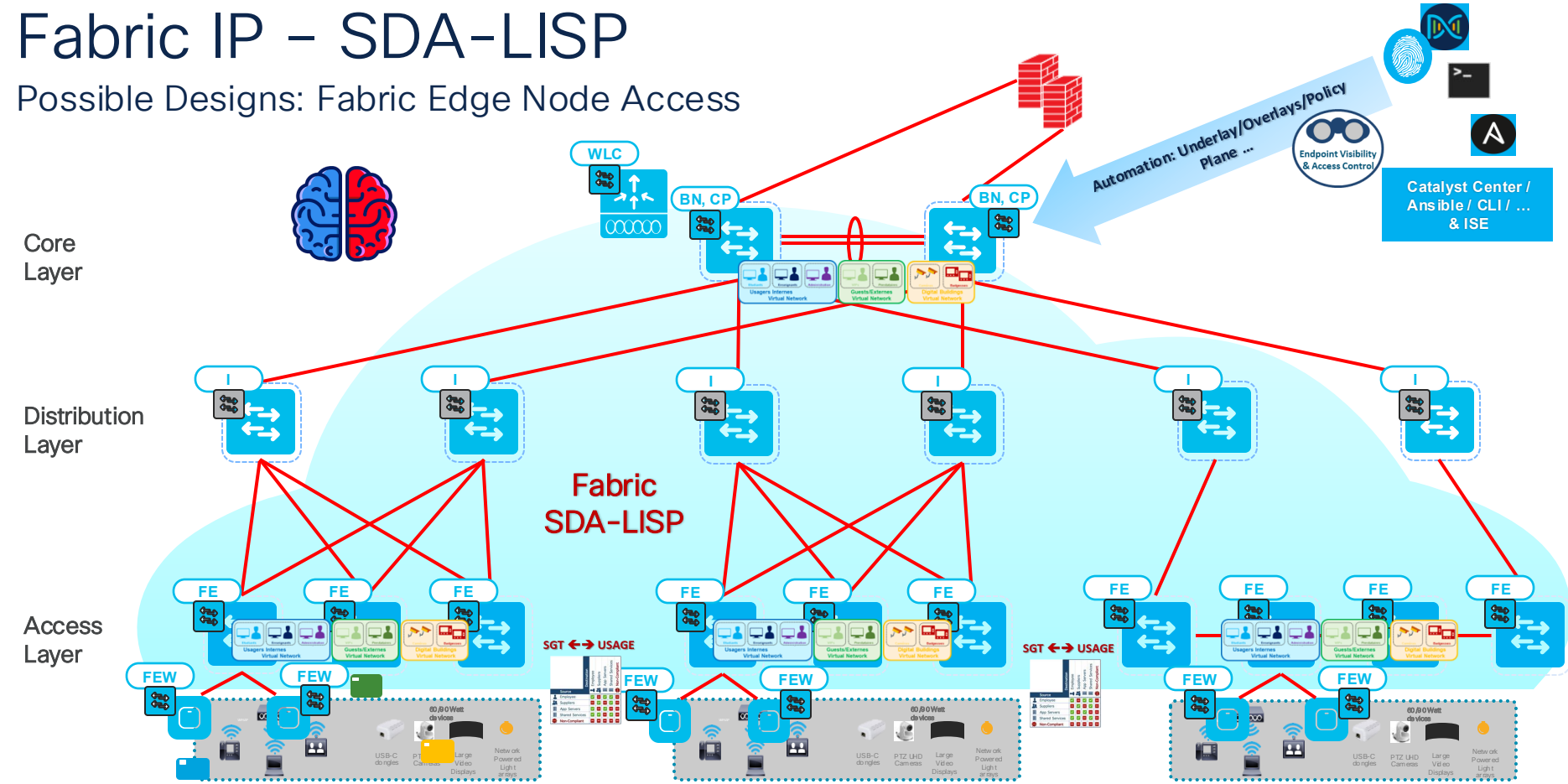
Fabric IP – SDA-LISP

Possible Designs: Fabric Edge Node Access



Fabric IP – SDA-LISP

Possible Designs: Fabric Edge Node Access



Fabric SDA

In summary…

Core Layer

Distribution Layer

Access Layer

Fabric SDA

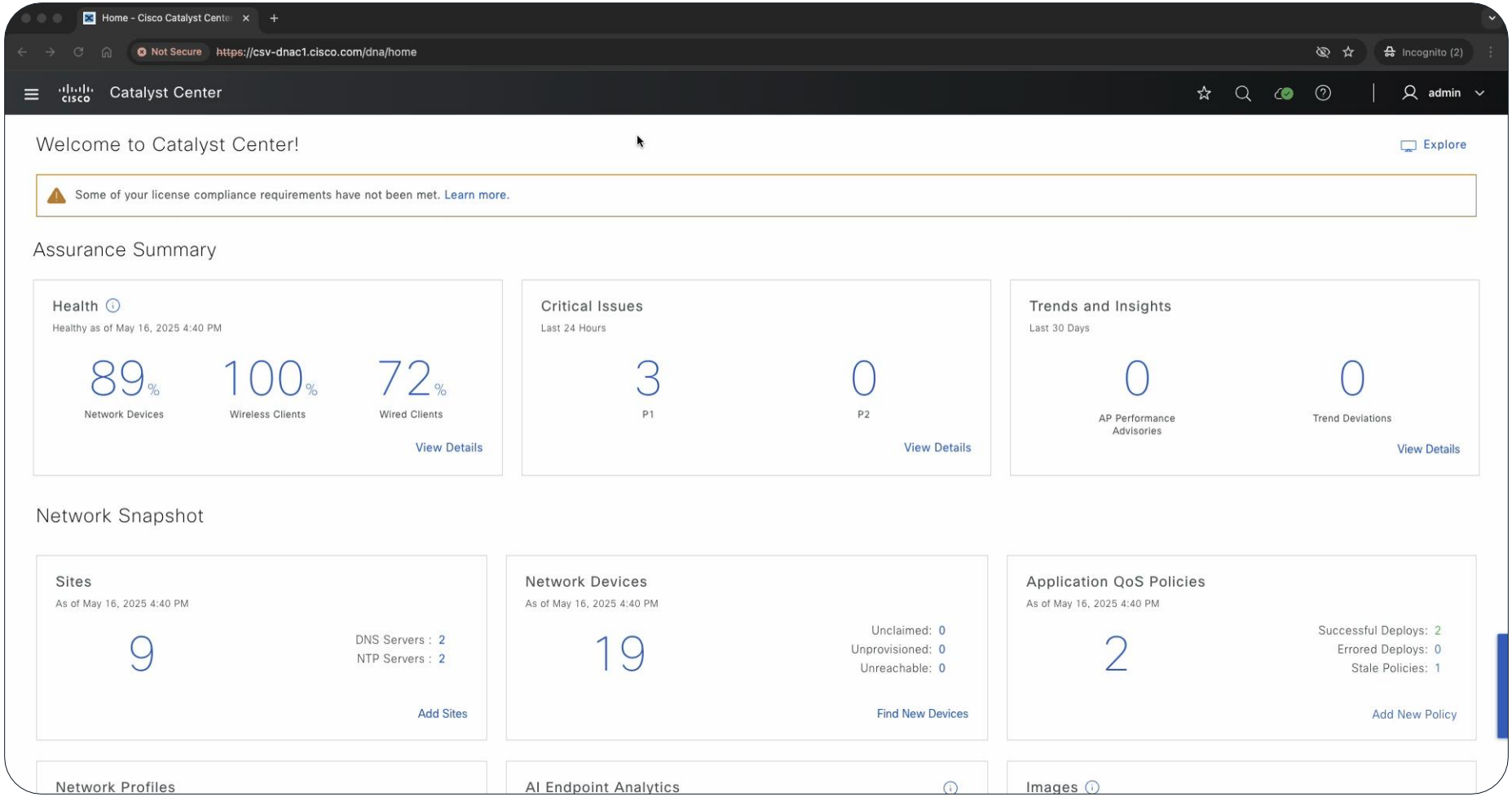
Control Plane (LISP / EVPN)

Data Plane : VXLAN

Policy Plane : Virtual Network & Security Group Tag

Demo / Video 3

Video showing how Assurance (AIOps) helps keep a Fabric SDA healthy



Agenda

- Challenges & Limitations of Traditional LANs Campus
- Fabric IP & Fabric SDA
- Native Zero-Trust
- Conclusion

Zero-Trust Evolution

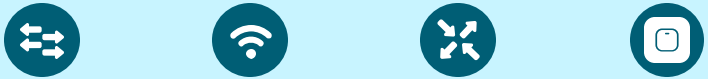
LAN Campus ➔ Fabric SD-Access

Three pillars of Workplace Zero Trust Security

Cisco Catalyst Center & Meraki dashboard

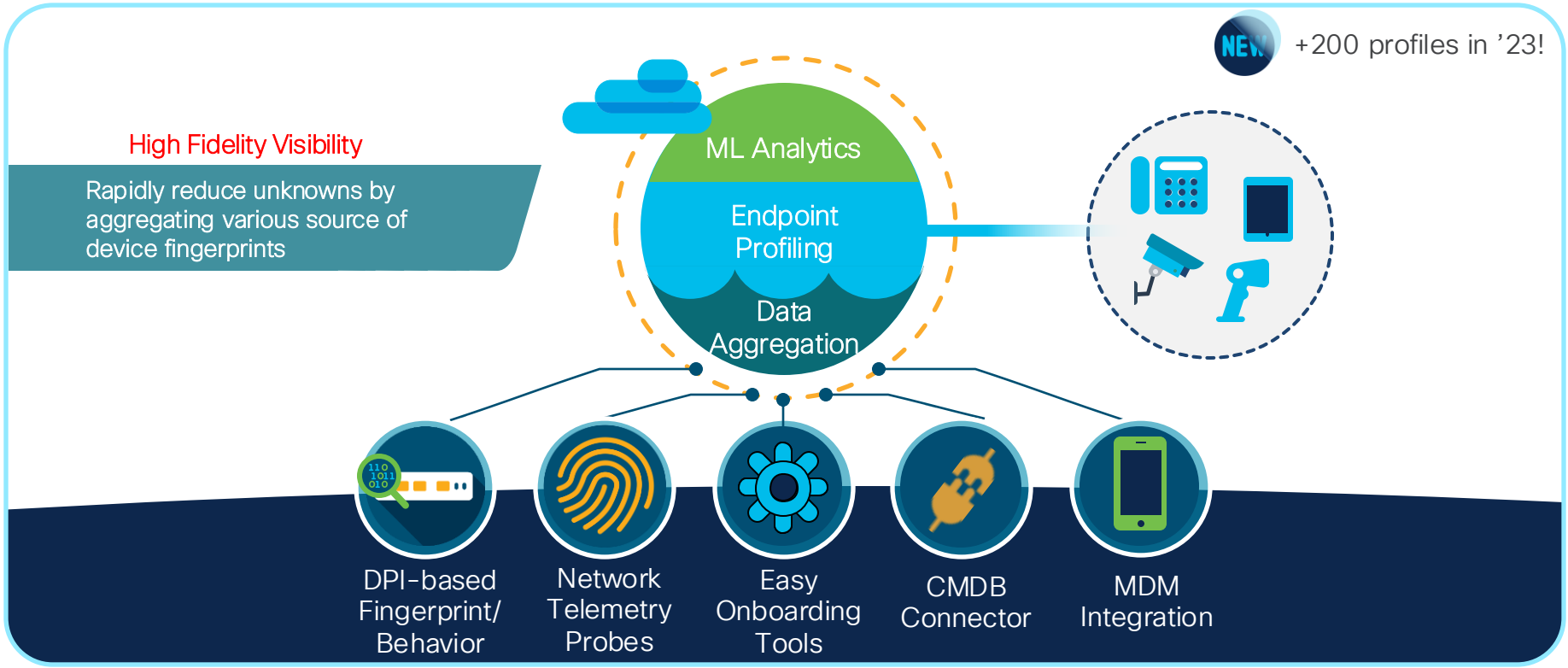
Cisco ISE

Enabled on Cisco Catalyst 9000 Infrastructure (Classical Ethernet or SD-Access)



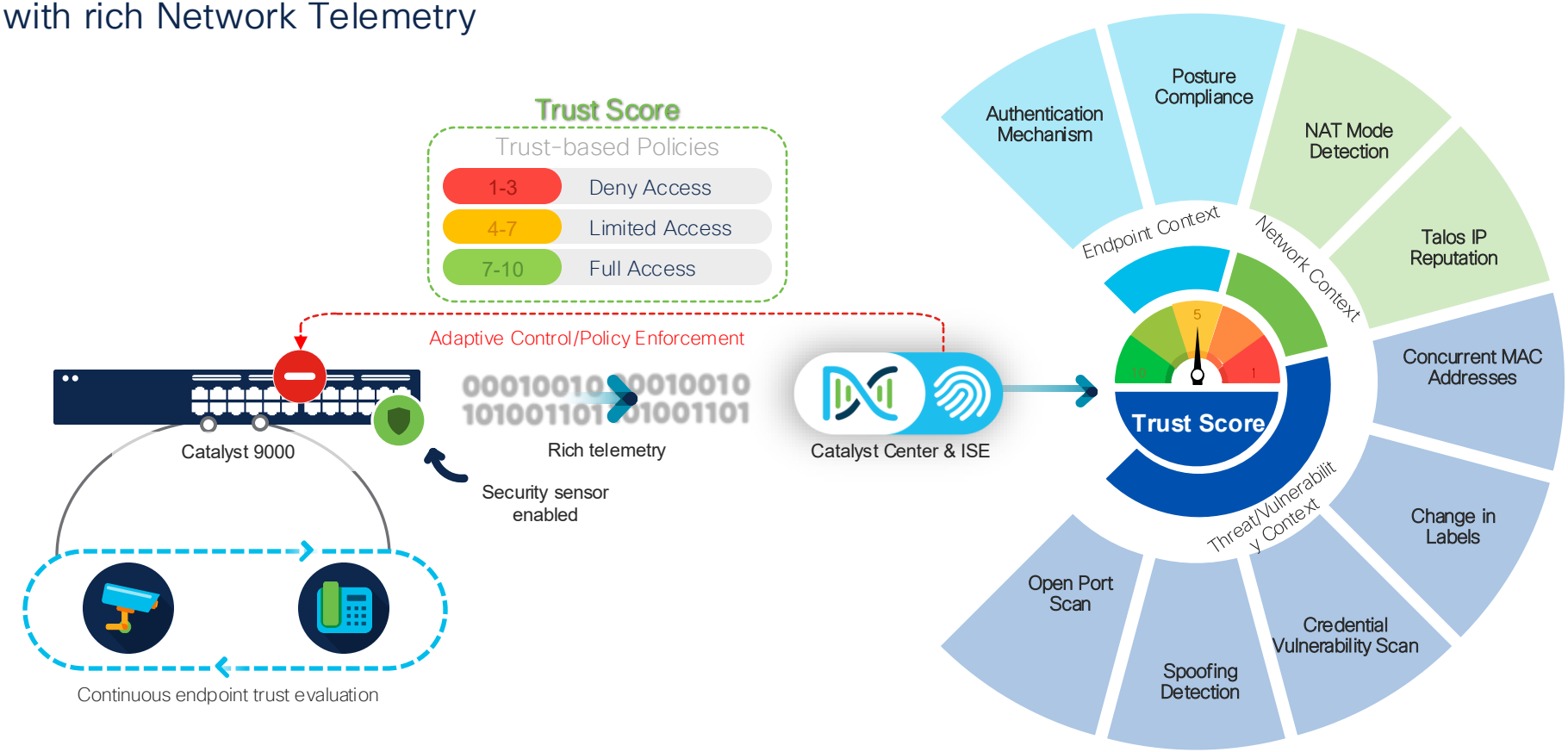
Endpoint Analytics (EA)

on Access Infrastructure



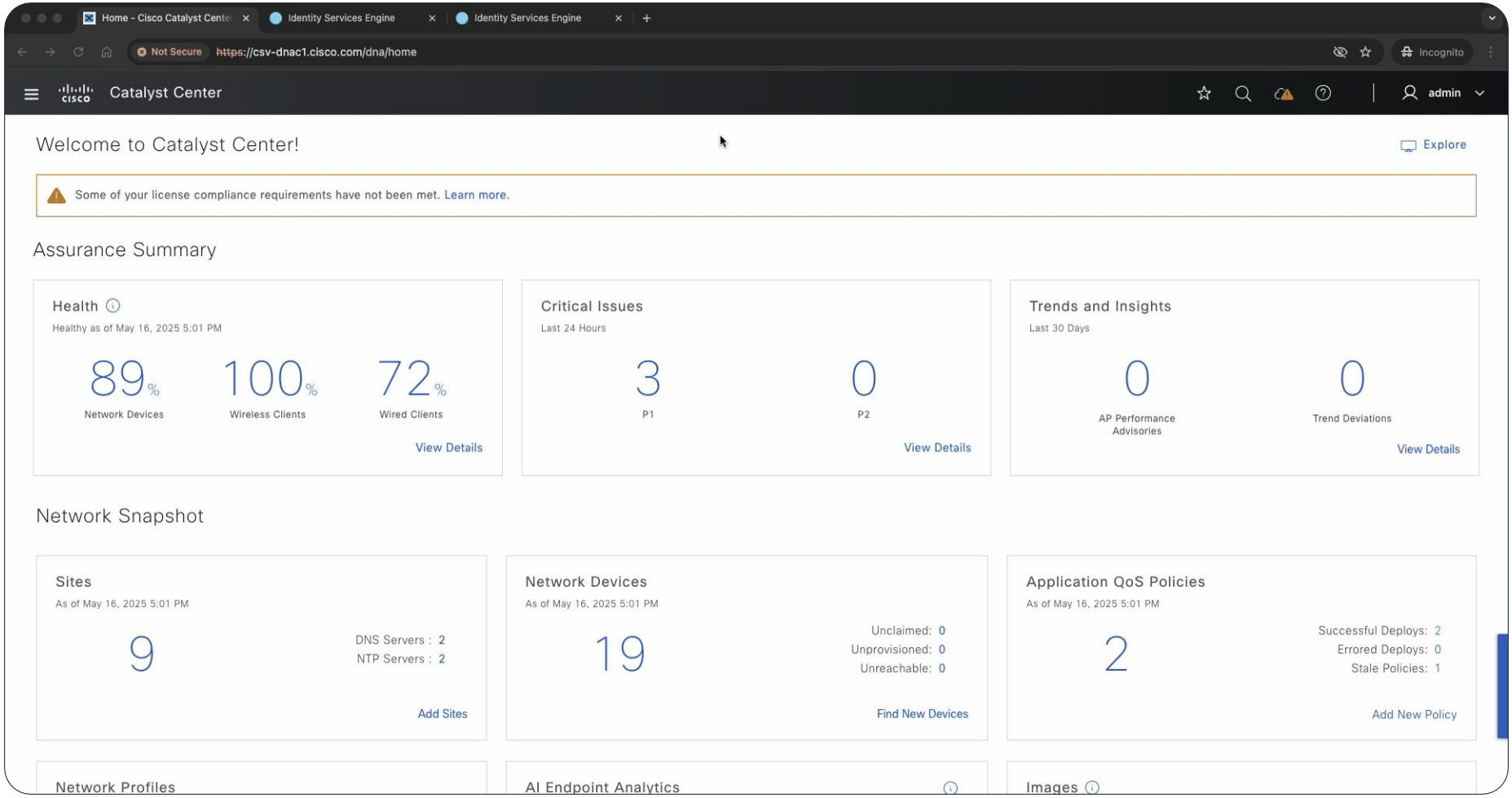
Continuously Assess Trust

with rich Network Telemetry



Demo / Video 4

Video showing EndPoint Analytics and Trust Score (SecOps) …



Agenda

- Challenges & Limitations of Traditional LANs Campus
- Fabric IP & Fabric SDA
- Native Zero-Trust
- Conclusion

Key Takeaways

Access Layer ➔ The Key Point of Transformation

mGig, UPoE/UPoE+, diversity of EndPoints (laptops, smartphones, sensors, IoT, …)

Urbanization, Resilience & Security of the LAN Campus are Major Challenges

“Traditional” Architectures work but have Limitations!!!

Fabric IP / SD-Access

Automation, Robustness, High Availability, Elasticity to adapt to all issues related to urbanization

Single Connectivity Service for Wired & Wireless End-Points

Zero-Trust Native

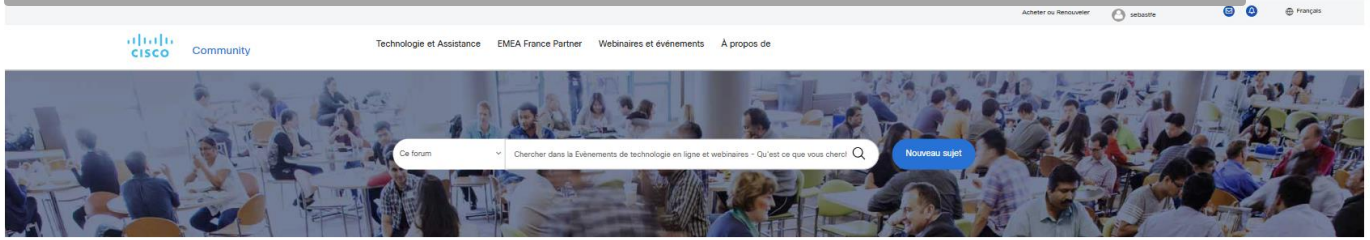
Fabric IP / SD-Access is part of the Customer’s Roadmap

Currently Fabric IP & Fabric SDA are IaaS Solutions

Roadmap to offer a SaaS Solution for Fabric IP & Fabric SDA

Key Takeaways

17.06 Création en Direct d'une Fabric SD-Access : Démonstration et Étapes Clés - Cisco Community



Cisco Community > Communauté Cisco > Évènements de technologie > Évènements de technologie en ligne et webinaires
> 17.06 Création en Direct d'une Fabric SD-Access : Démonstration et Étapes Clés

S'abonner | Options

17.06 Création en Direct d'une Fabric SD-Access : Démonstration et Étapes Clés

Publié le 13-02-2025 09:16 PM par citeambot | Mis à jour le 04-03-2025 12:40 AM

Mardi 17 juin 2025 à 15h00 (heure de Paris) / 9h00 (heure de Montréal)

Évènement Community Live

Création en Direct d'une Fabric SD-Access : Démonstration et Étapes Clés

Ce webinaire sera présenté par Jérôme Durand.

Vous trouvez SD-Access complexe ? Vous vous demandez par où commencer ? Participez à notre webinaire entièrement dédié aux démonstrations, dans lequel nous vous guiderons à travers chaque étape pour créer une Fabric SD-Access avec l'ensemble de ses services.

Horaires

- 9h00 Montréal, Toronto
- 15h00 Paris, Bruxelles
- 14h00 Tunis, Alger
- 13h00 Conakry, Dakar
- 13h00 Lomé, Abidjan
- 16h00 Antananarivo

Agenda

- (en attente)

* Cet événement est gratuit et ouvert à tous les publics, y compris les partenaires commerciaux, les ingénieurs réseau et télécommunications, les étudiants et les clients de Cisco.

Webinaire en français

Création en Direct d'une Fabric SD-Access : Démonstration et Étapes Clés

Mardi 17 juin 2025. Événement en français !

Début : mar., juin 17, 2025 06:00 AM PDT
Finit : mar., juin 17, 2025 07:30 AM PDT

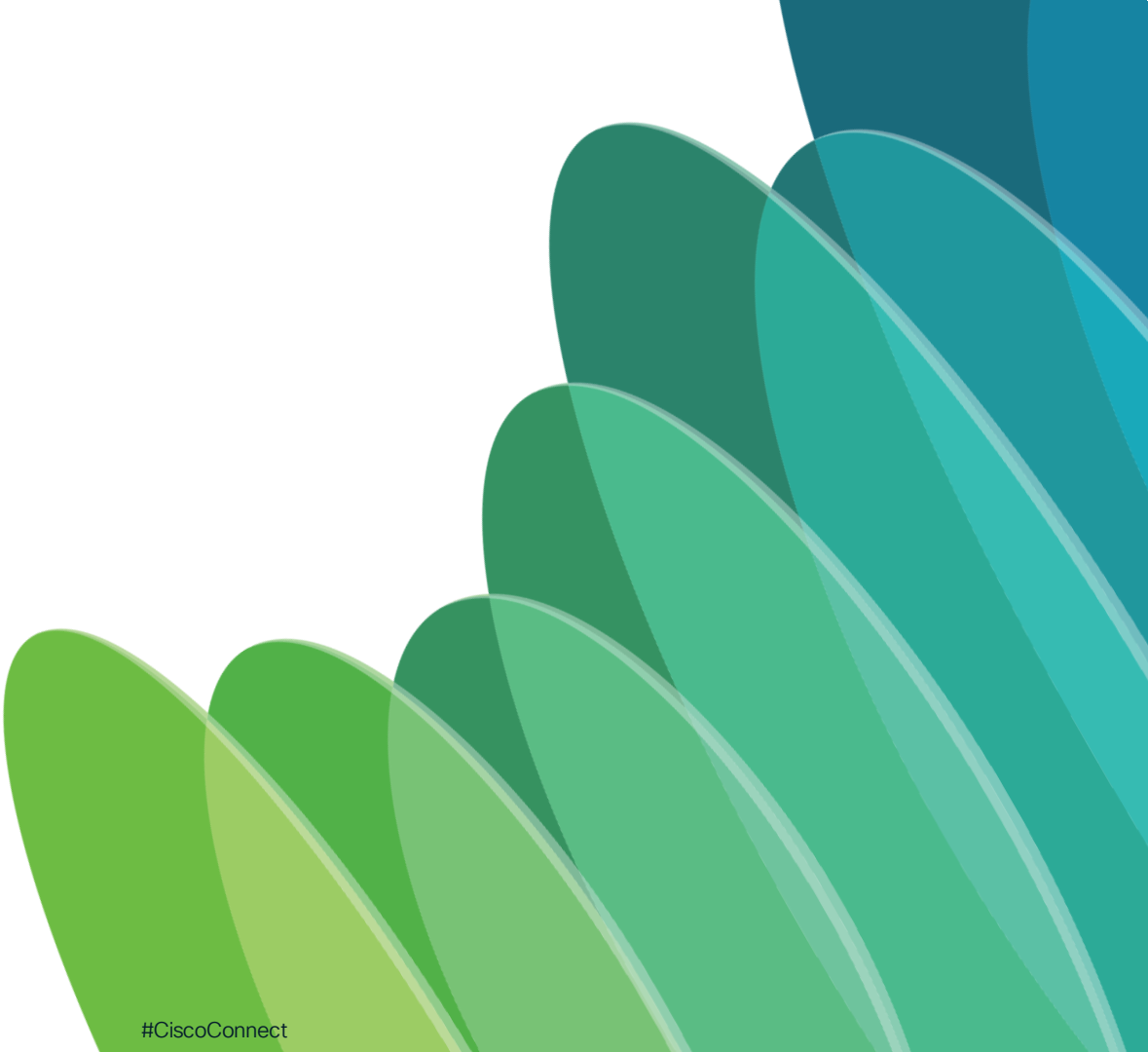
Étiquettes (3)

Community Live | Commutation | Routage

Go Beyond with Cisco CX !

Meet us @World of Solutions Booth

	Premium Support		Solution Attached Services		Lifecycle Services
	Service	**Case**	**Service**	**Use Case**	**Example Activities**
Secure Campus and Branch Networking Get secure networking with real-time performance data, smart recommendations, and closed-loop automation	Success Tracks Campus Network	Access to digital insights on campus network operations, risks, and devices with quick remediation options (switching, routing, and wireless).	SAS Campus Networking *	Implement and adopt Catalyst (Switching, Wireless, Routing, Cisco Spaces) along with Catalyst Center to ensure consistency of network services through regular device image management and deployment plus software recommendations	Utilize automation capabilities across facets of the network including DNA-C with SVS and Services-as-Code to dynamically adjust network configurations based on real-time demand and usage patterns, and AIA (automated incident and assurance) for automated fault detection.
			SAS Future-Proofed Workplaces Outcomes Program Management	Aligning networking products to business goals via analysis of current IT network capabilities and ongoing single program management for Cisco technology and third-party integrations	
			ThousandEyes Implementation Services	ThousandEyes implementation via onboarding programs with training and advice tailored to specific business outcomes	
	Success Tracks WAN	Insights to improve, optimize, and secure SD-WAN whether the use case is Secure Automated WAN, Secure Direct Internet Access, or WAN Digital Transformation on ramping for customers migrating from a non-controller environment	SAS Meraki	Get assistance with planning and executing a migration from on-premises to cloud through site surveys and migrations deployment planning, execution, and validation. Along with ISE integration into Meraki wireless.	



Thank you

cisco Connect

#CiscoConnect

cisco Connect

GO BEYOND

#CiscoConnect