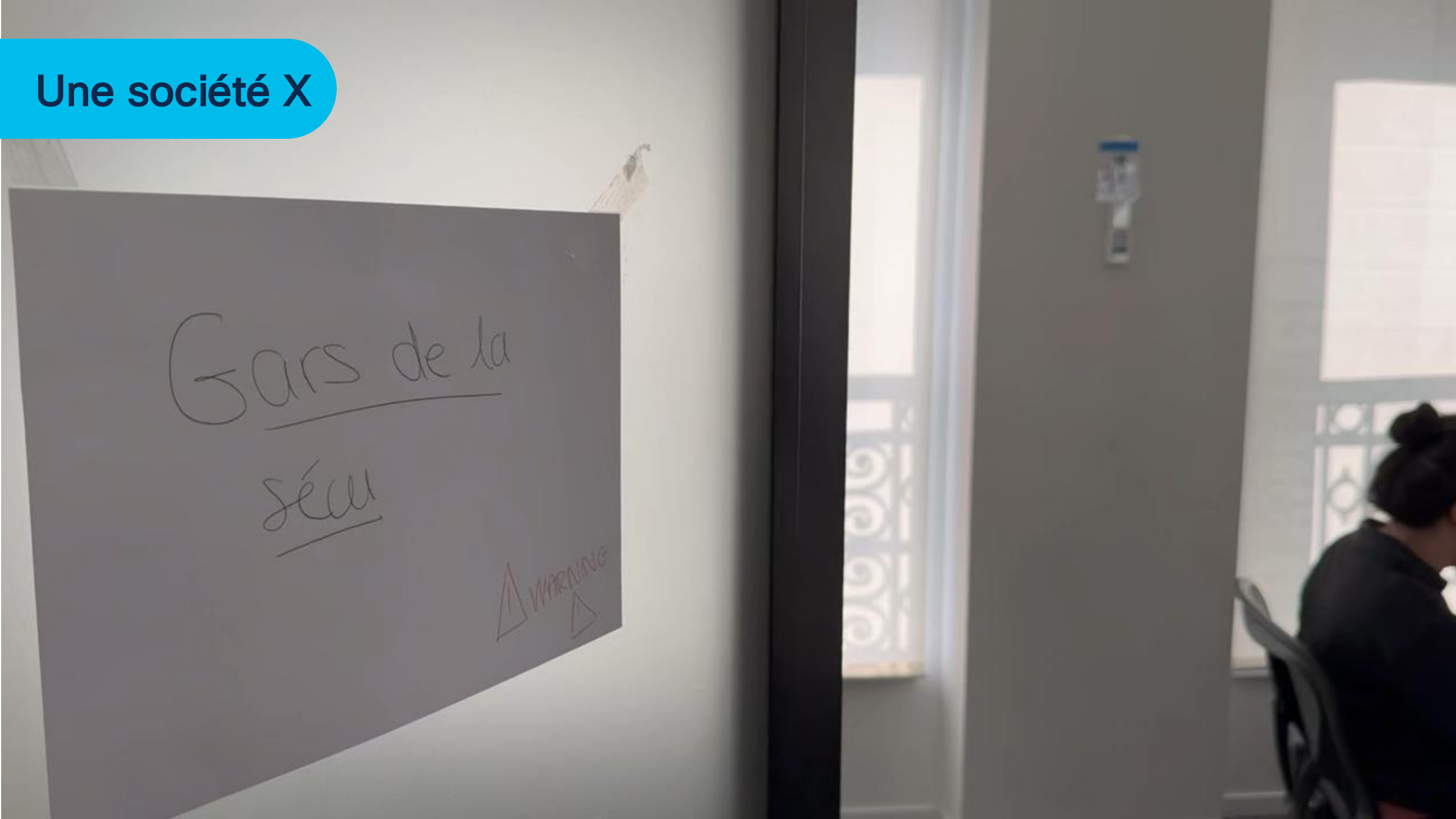
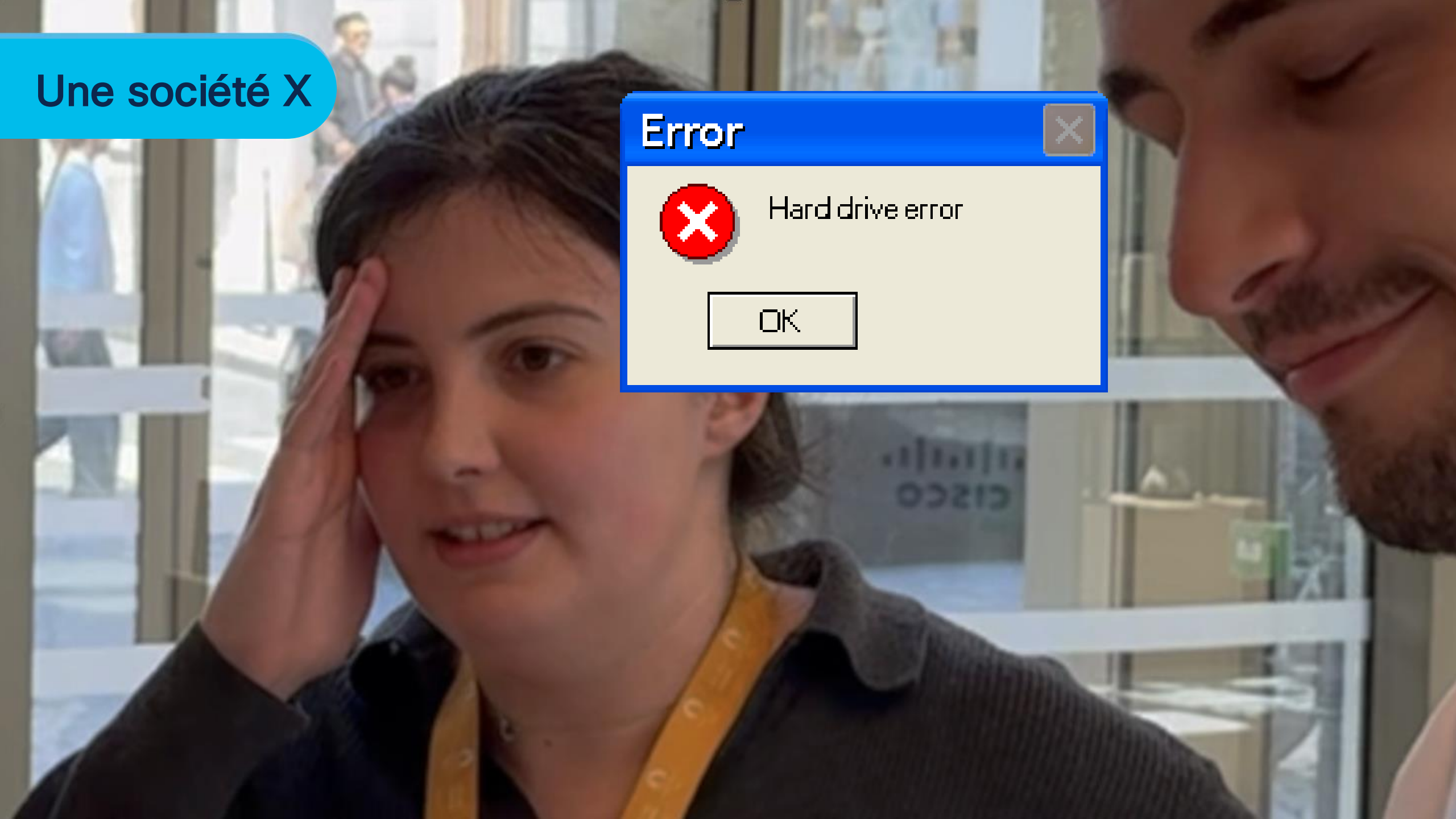
Common Policy

Simplifiez le deploiement de votre politique de segmentation de bout en bout

Marion VAILLER, Solutions Engineer
Xavier VALETTE, Solutions Engineer

Une société X



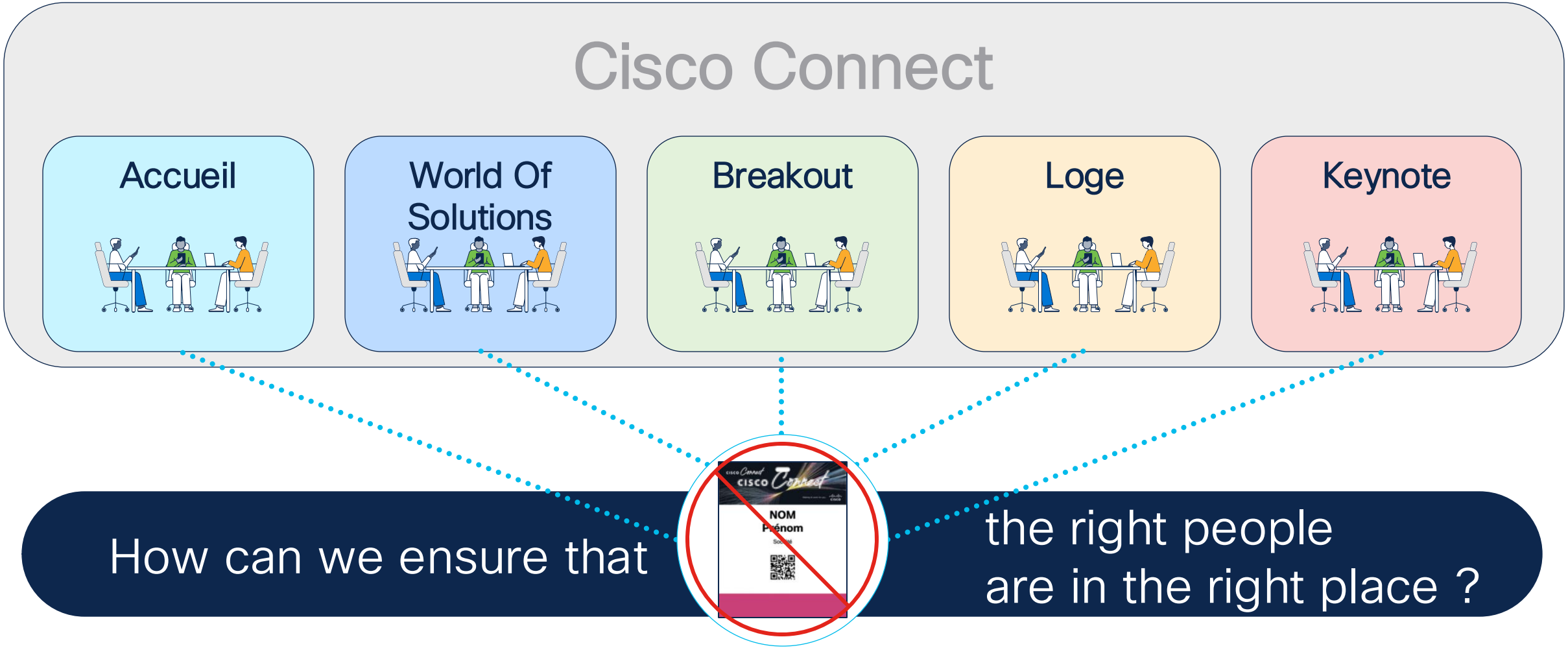

Une société X
Error
Hard drive error
OK

Common Policy

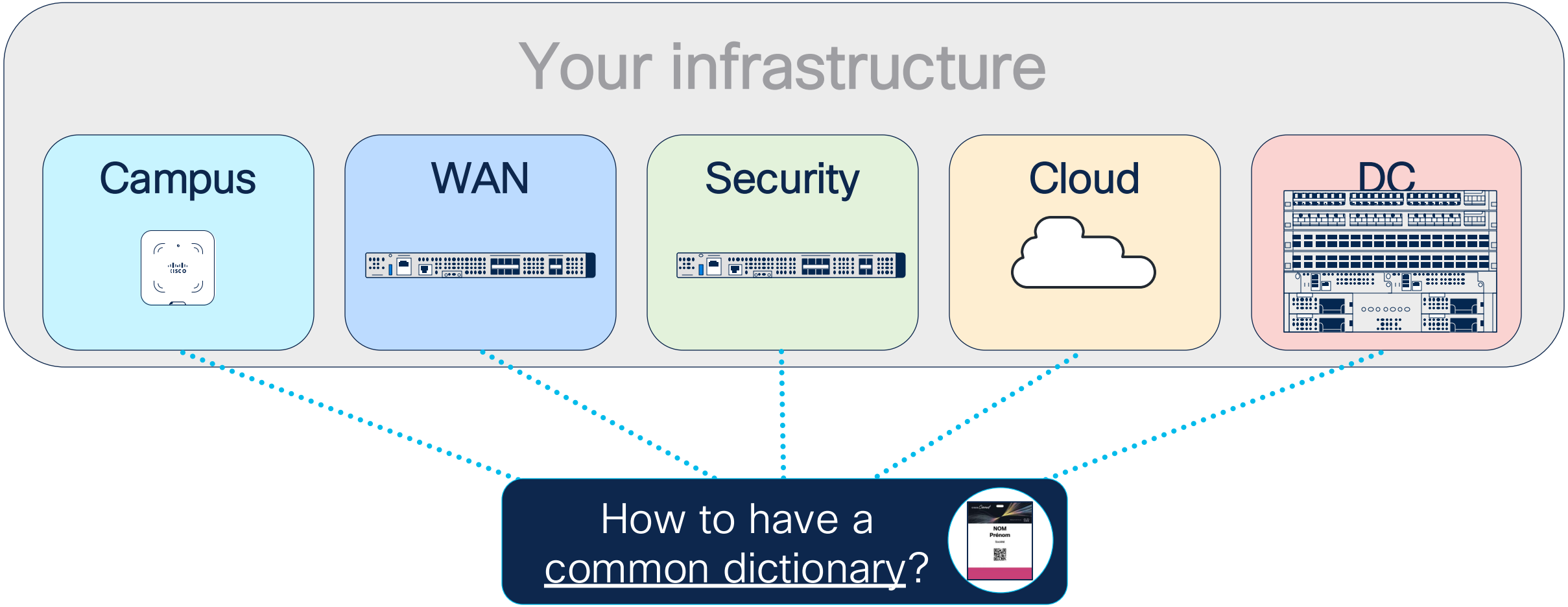
Simplifiez le deploiement de votre politique de segmentation de bout en bout

Marion VAILLER, Solutions Engineer
Xavier VALETTE, Solutions Engineer

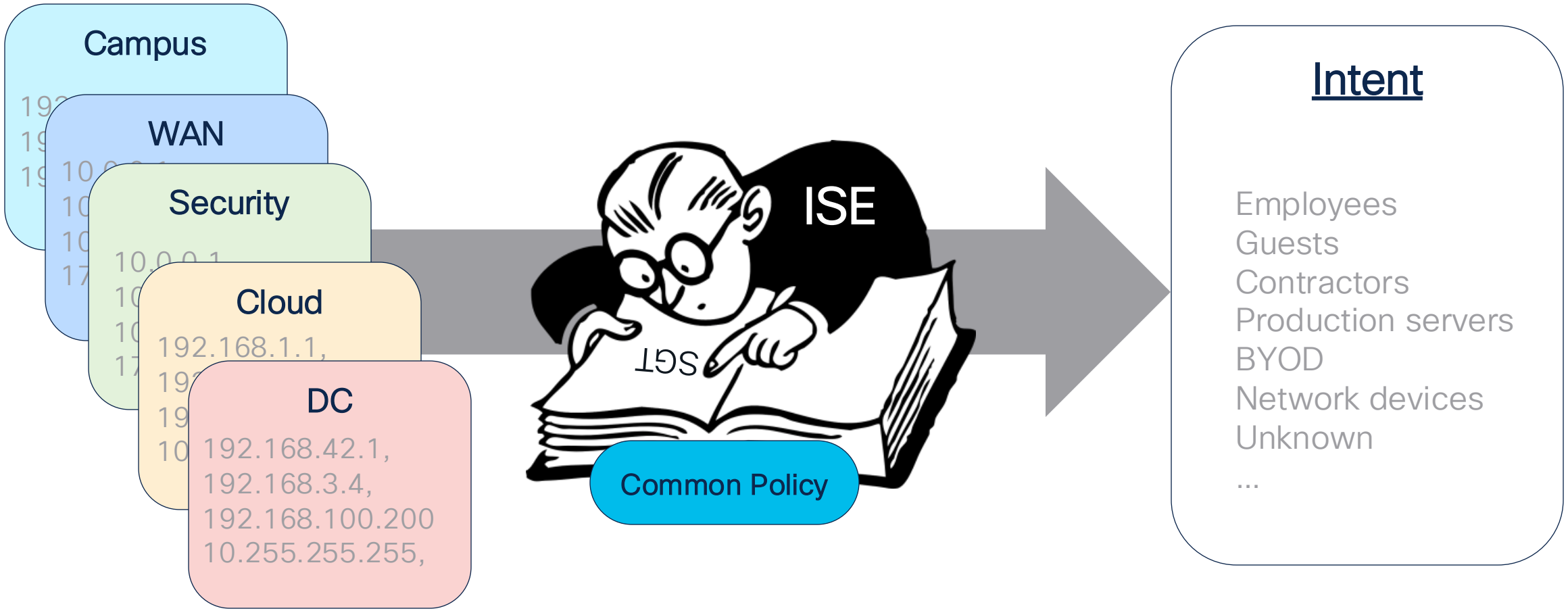
Pouvez-vous imaginer... un Cisco Connect sans badges ?



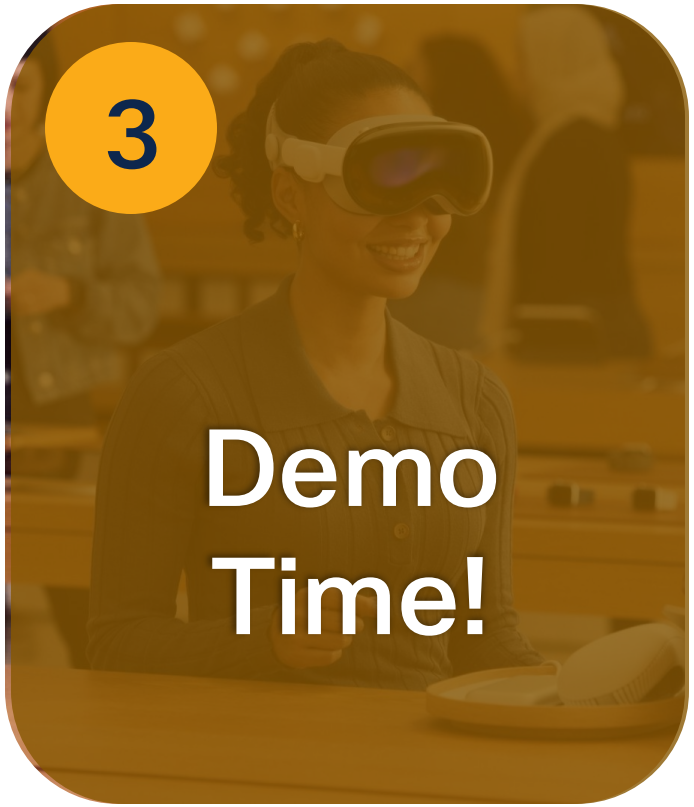
Mêmes principes pour votre infrastructure



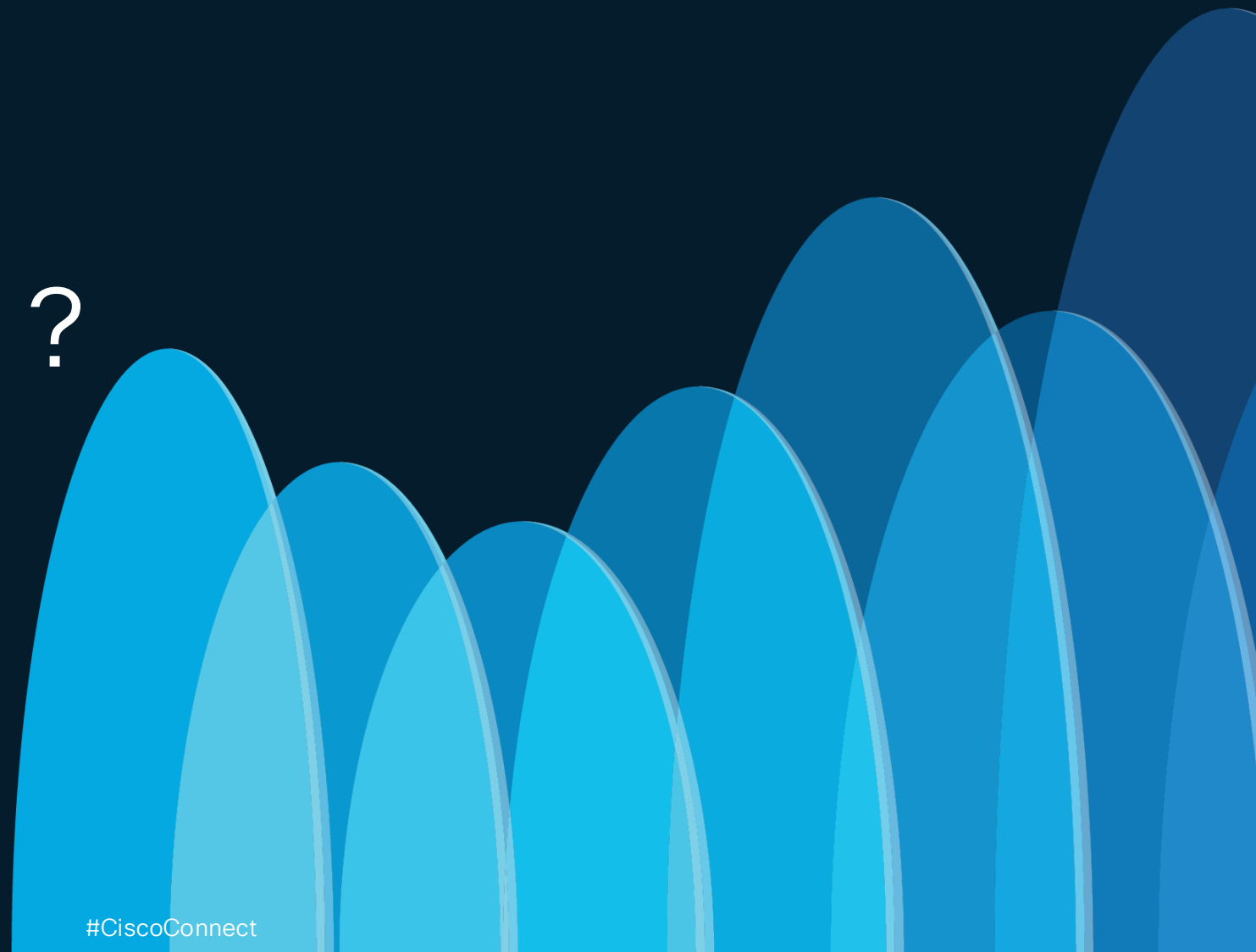
Transformez votre Securité avec Common Policy



Agenda



Qu’est-ce que Common Policy ?



cisco Connect

Common Policy is SGTs across Domains

SGTs and Domains are explained on next slides

ISE

Common Policy is a feature from ISE

Common Policy uses SGTs to build a common dictionary to implement security policies

API

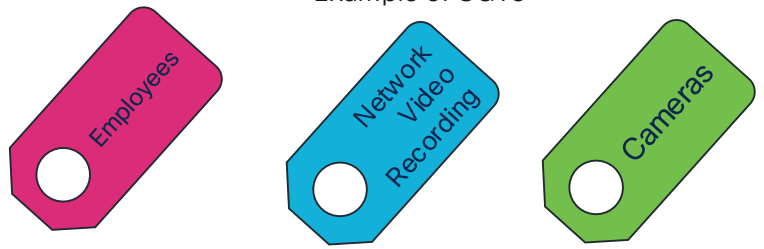
Common Policy uses API to extend SGTs across Domains

Les SGTs sont les badges Cisco Connect pour les assets

Badges identify **people**

SGT identify **assets**

*Example of SGTs



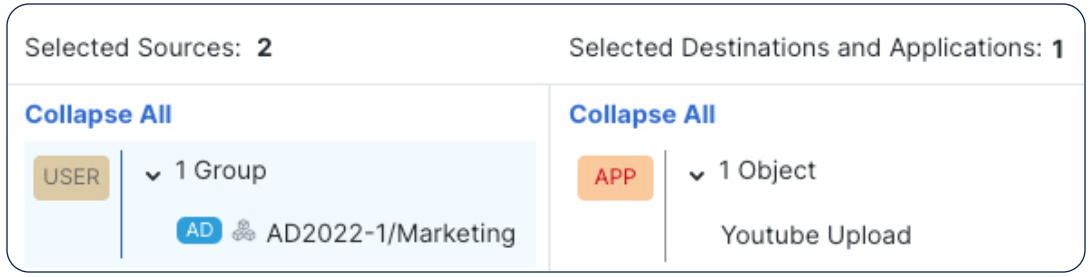
*Example of assets

Security Group Tags (SGTs) are the identities in TrustSec architecture

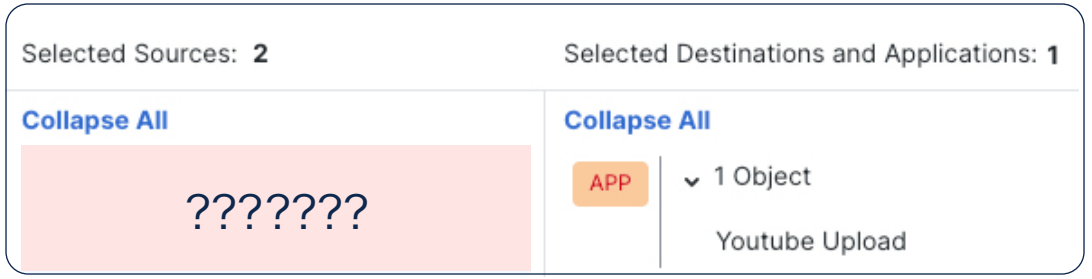
Les SGTs sont les identités communes de vos assets

"I can already filter by identity with a Firepower, why should I use a SGT?"

What about **non-managed assets**?



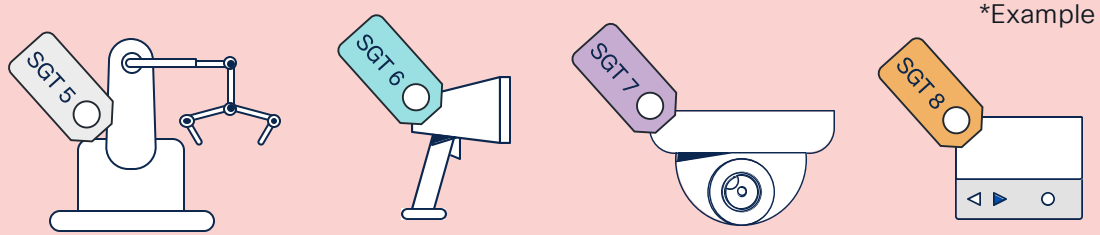
Firepower screenshot



*Example of teams

Marketing | Sales | Developers | IT

*Example of assets



Industrial machines | Barcode readers | Cameras | Sensors

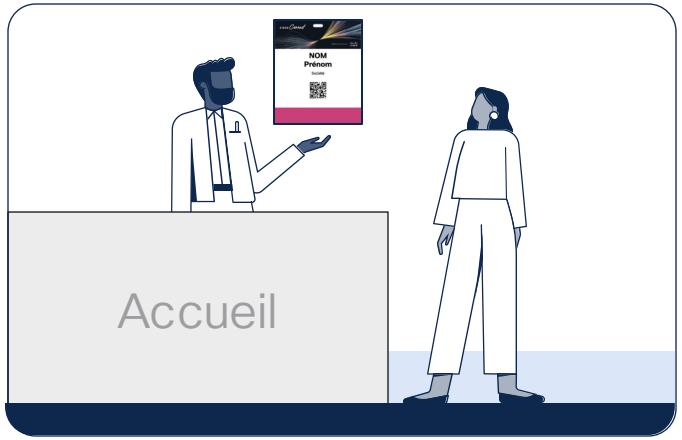
Managed assets

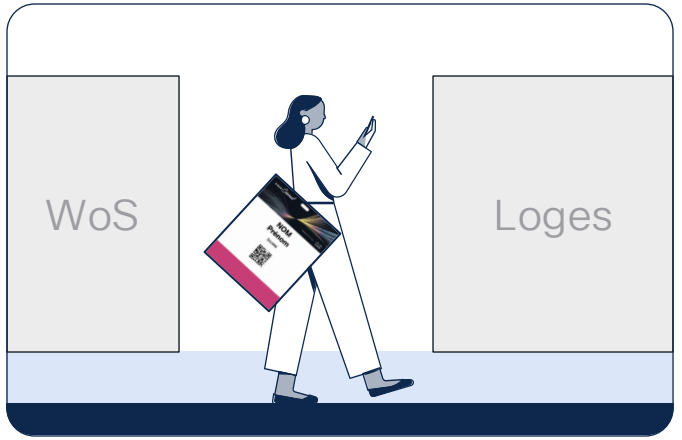
Unmanaged assets

Deploy des SGTs dans votre infrastructure via TrustSec

TrustSec s'appuie sur 3 principes clés : Classification, Propagation, Enforcement

Cisco Connect



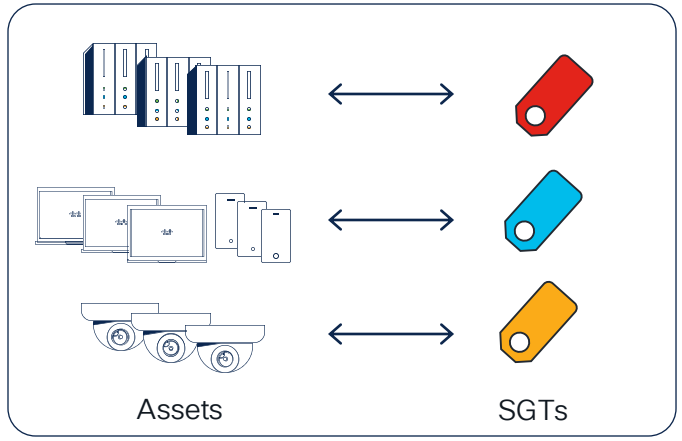


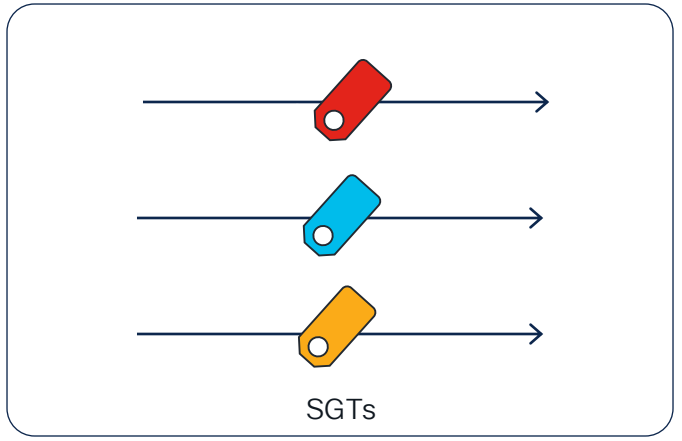
1 Classification

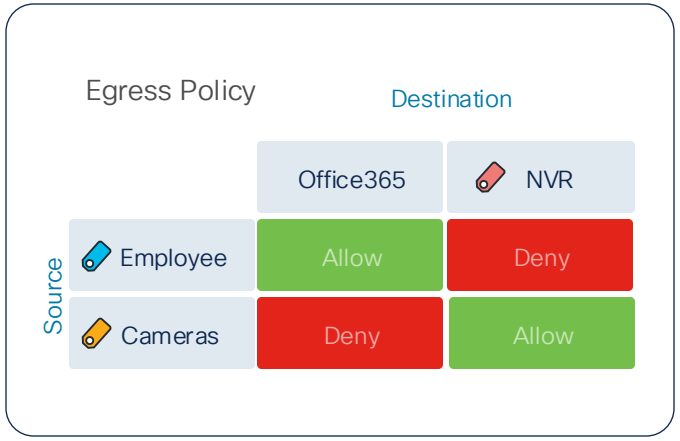
2 Propagation

3 Enforcement

Infrastructure







TrustSec s’appuie sur 3 principes clés

For your reference : examples of Classification, Propagation, Enforcement

Infrastructure

1 Classification

Dynamic assignment via RADIUS
Wired & Wireless 802.1X

Static SSID assignment
Guest Users

Static switch port assignment
Wired IOT Sensors / Fixed Devices

Static Prefix to SGT Mapping
Last resort to map traffic to an SGT

Profiling
Endpoint analytics

2 Propagation

Data plane (inline)
SGT carried inline in the data traffic. Methods include, SGT over Ethernet, MACSec, IPSec, VxLAN, DMVPN, AutoVPN, SD-WAN Tunnel
…

Control plane
IP-to-SGT data shared over control protocol. No SGT in the data plane. Methods include, IP-to-SGT exchange over SXP, pxGrid, …

3 Enforcement

SGACL
Permit all, Deny all, Custom Policy / ACL

NGFW
Stateful firewall

Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration

Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec Servers

Concretely, where are SGTs defined?

Security Groups

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 Total 21

Edit | Add | Import | Export | Trash | Push | Verify Deploy | All

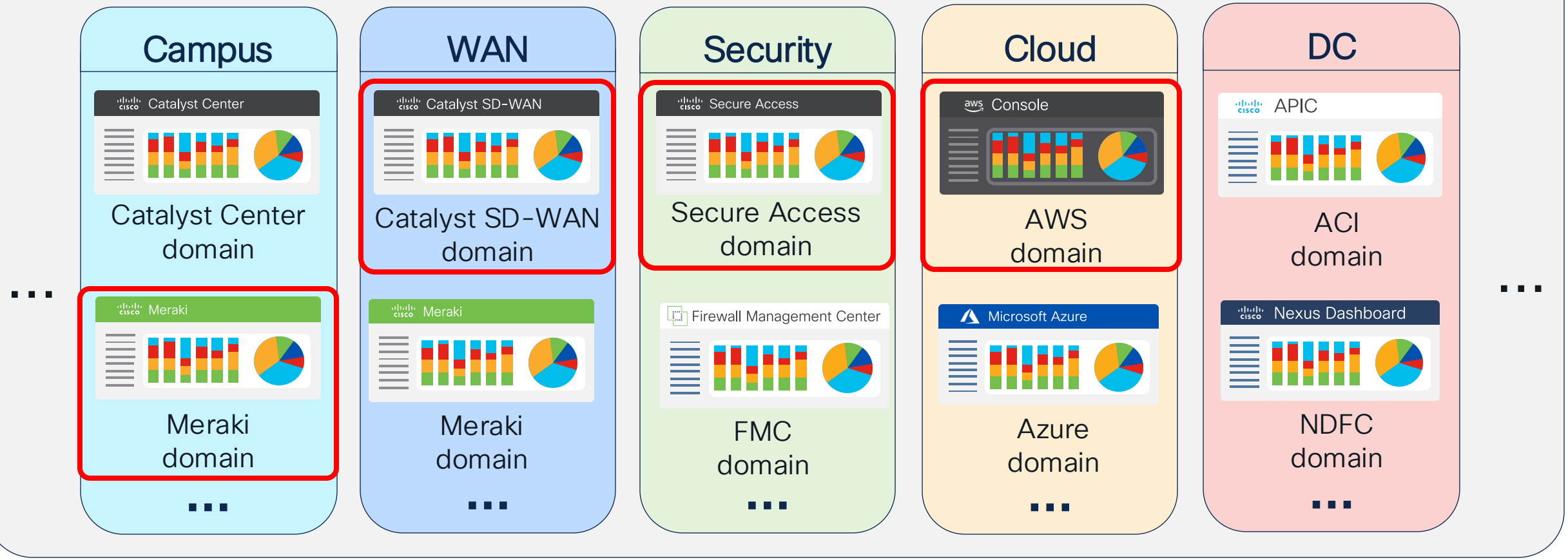
Spoiler : it is here

Icon	Name	SGT (Dec / Hex)	Description	Learned from	IP Mapping
	APP_A_SERVER	20/0014			0
	APP_B_SERVER	21/0015			0
	Auditors	9/0009	Auditor Security Group		0
	BYOD	15/000F	BYOD Security Group		0
	Cameras	42/002A			0
	Contractors	5/0005	Contractor Security Group		0
	Developers	8/0008	Developer Security Group		0
	Development_Servers	12/000C	Development Servers Security Group		0
	Employee	30/001E			0
	Employees	4/0004	Employee Security Group		0
	Guests	6/0006	Guest Security Group		0
	Network_Services	3/0003	Network Services Security Group		0
	PCI_Servers	14/000E	PCI Servers Security Group		0
	Point_of_Sale_Systems	10/000A	Point of Sale Security Group		0

Domains are defined by a manager/controller

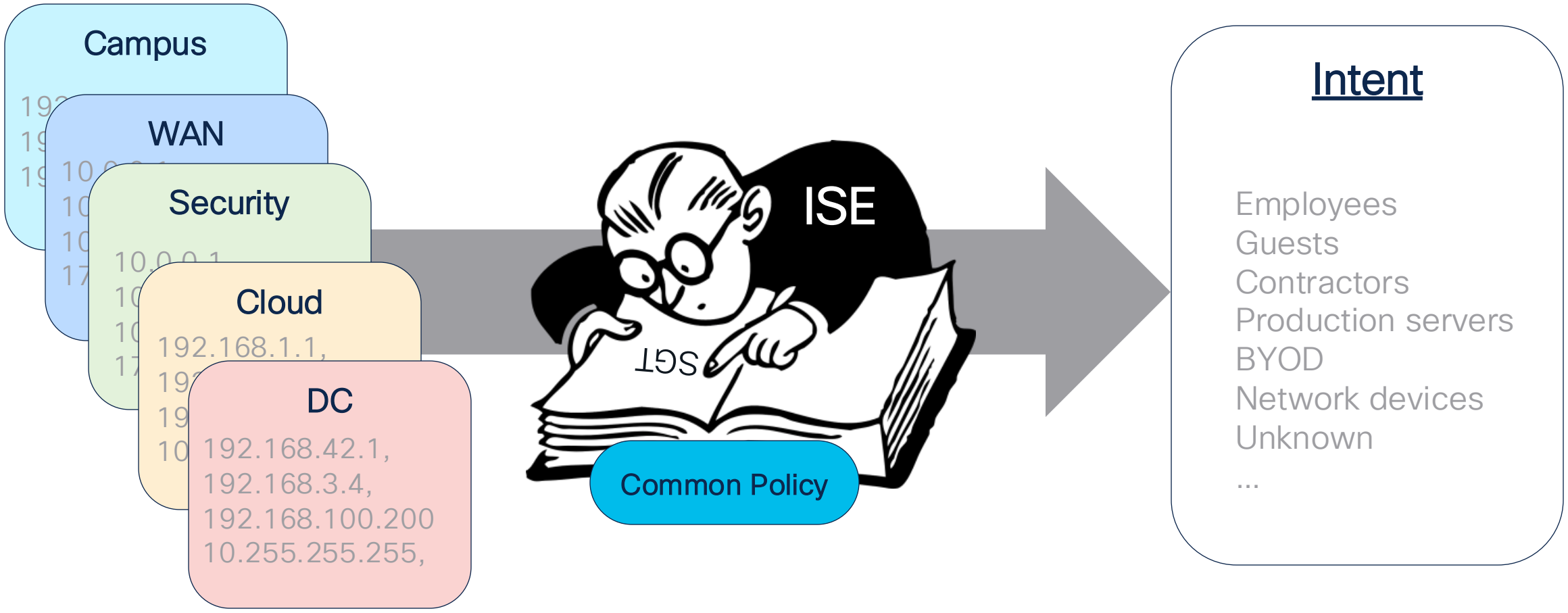
1 Domain
=
1 Controller

Your infrastructure = Multi-domains = Cross Architecture



Demoed in this session

Transformez votre Securité avec Common Policy



Quiz Time!

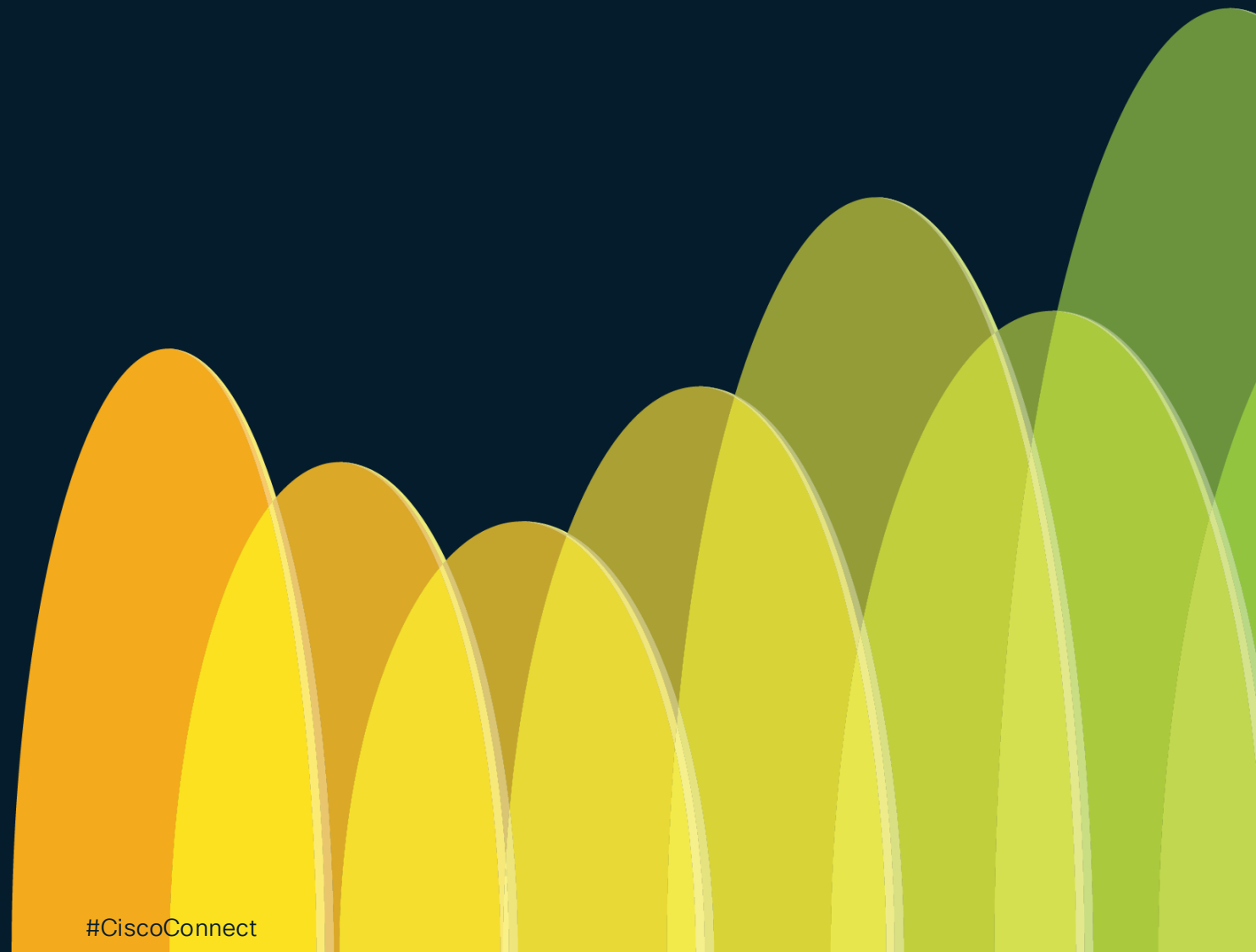
Qu'est-ce que Common Policy ?

Qu'est-ce que les Security Group Tags (SGTs) et les badges Cisco Connect ont en commun ?

Quelle fonctionnalité essentielle est ce que Identity Services Engine (ISE) peut fournir ?

Quelles sont les 3 étapes clés de TrustSec ?

Demo Time!



Deux demos = 2 cas d’usage réels

Secure Internet access

1

chatgpt.com

INET

User

Secure Cloud access

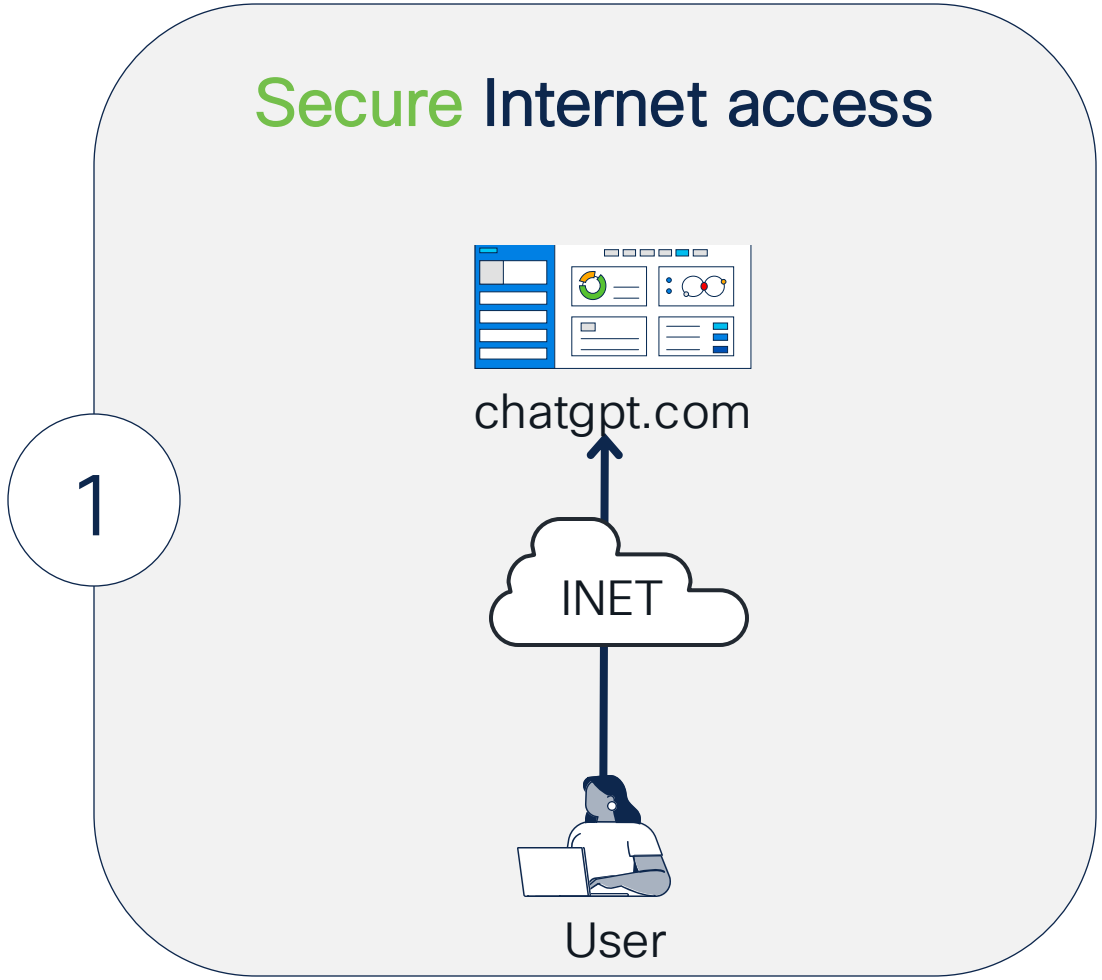
2

Custom application

aws

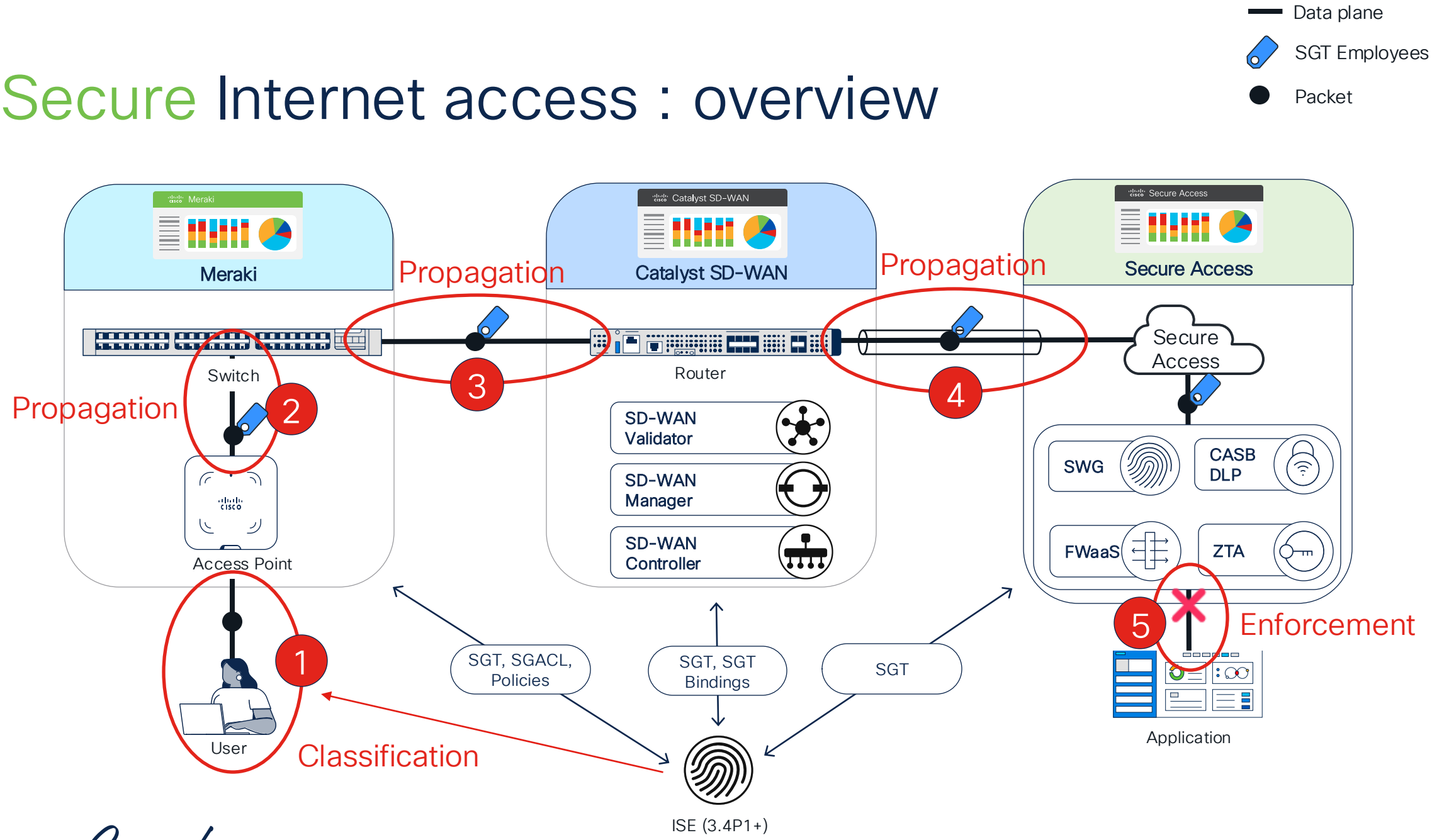
Camera

Un utilisateur accède à une application SaaS



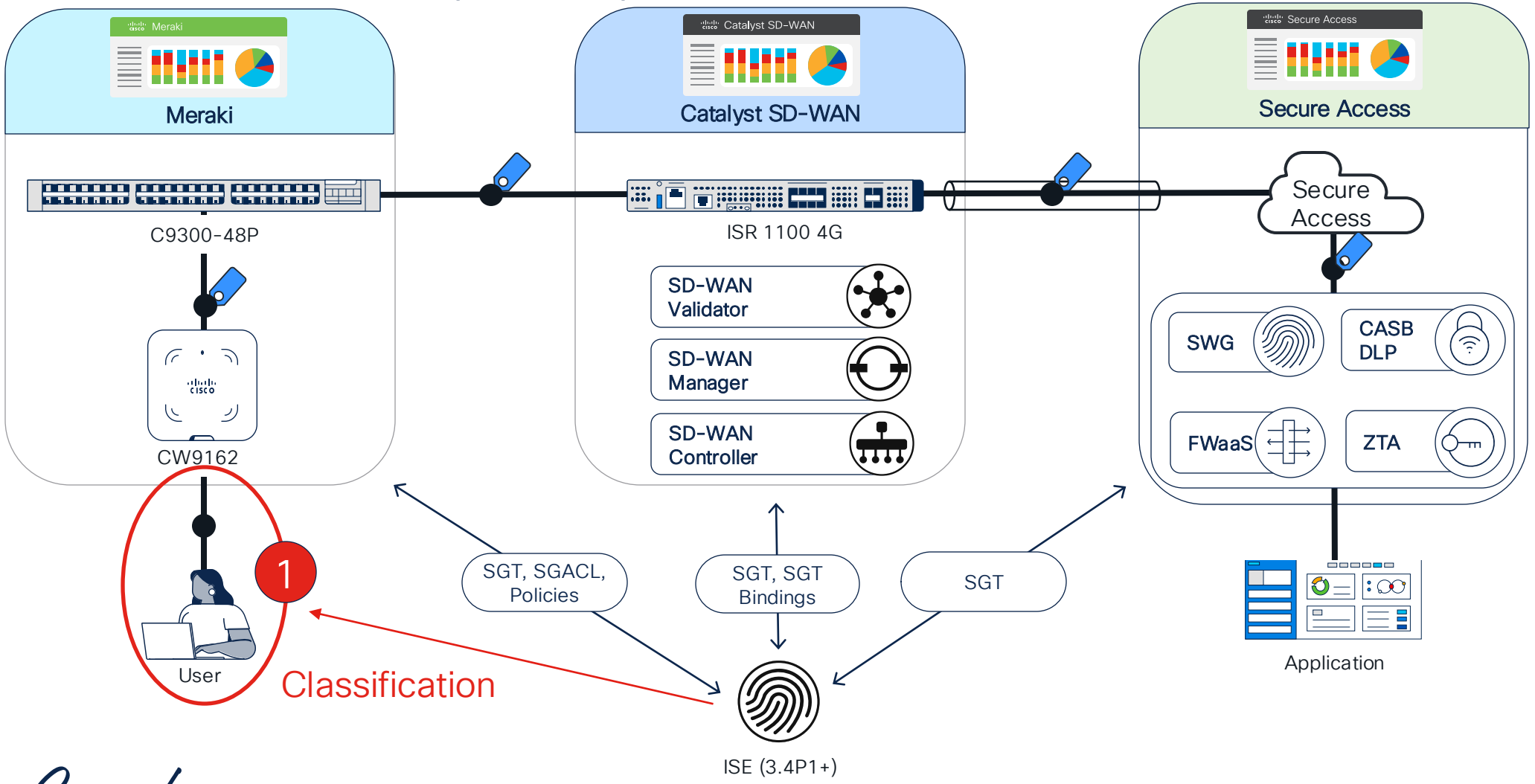
1. Classification of user via RADIUS
2. Propagation from AP to switch
3. Propagation switch to router
4. Propagation from router to Secure Access
5. Enforcement on Secure Access

Secure Internet access : overview



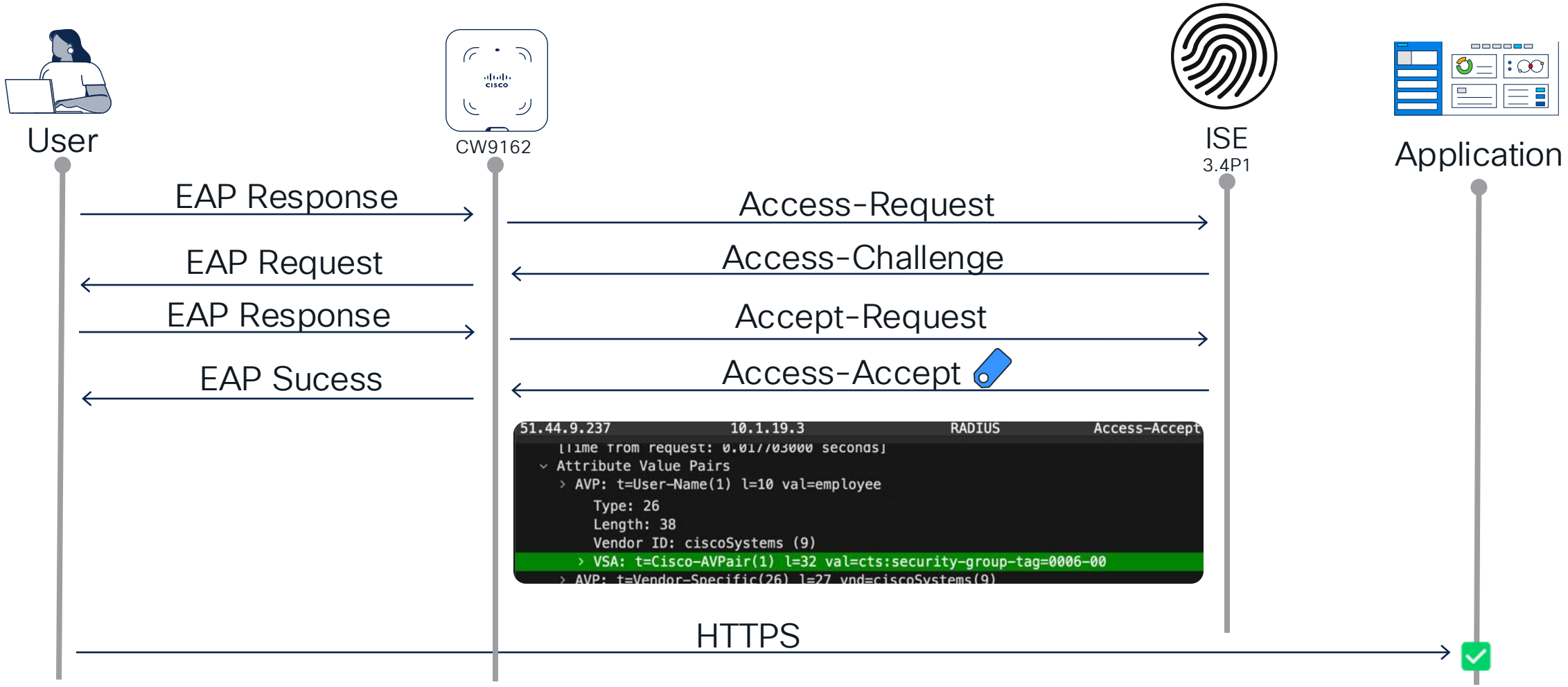
Secure Internet access

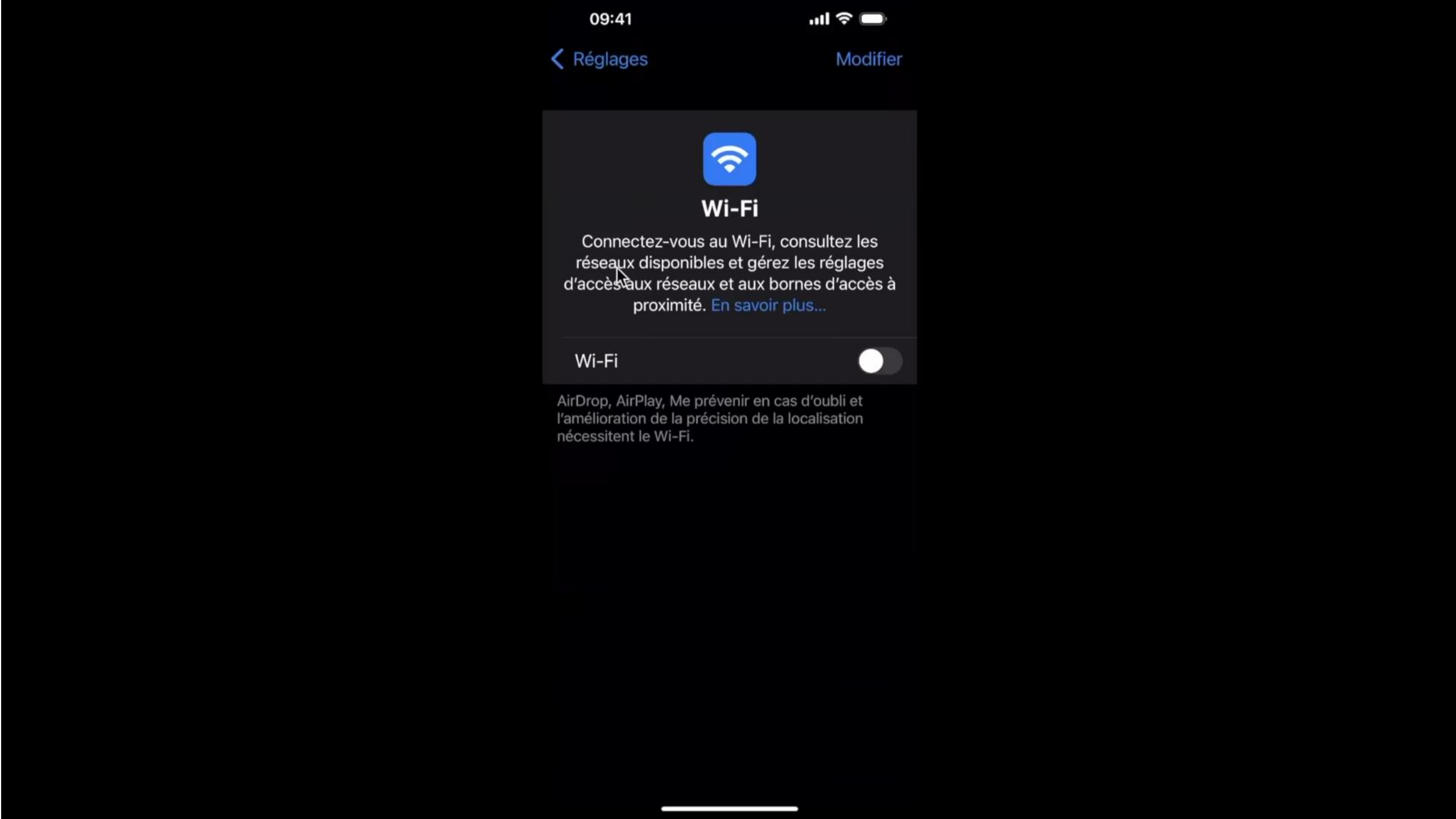
1. Classification via ISE (802.1X)

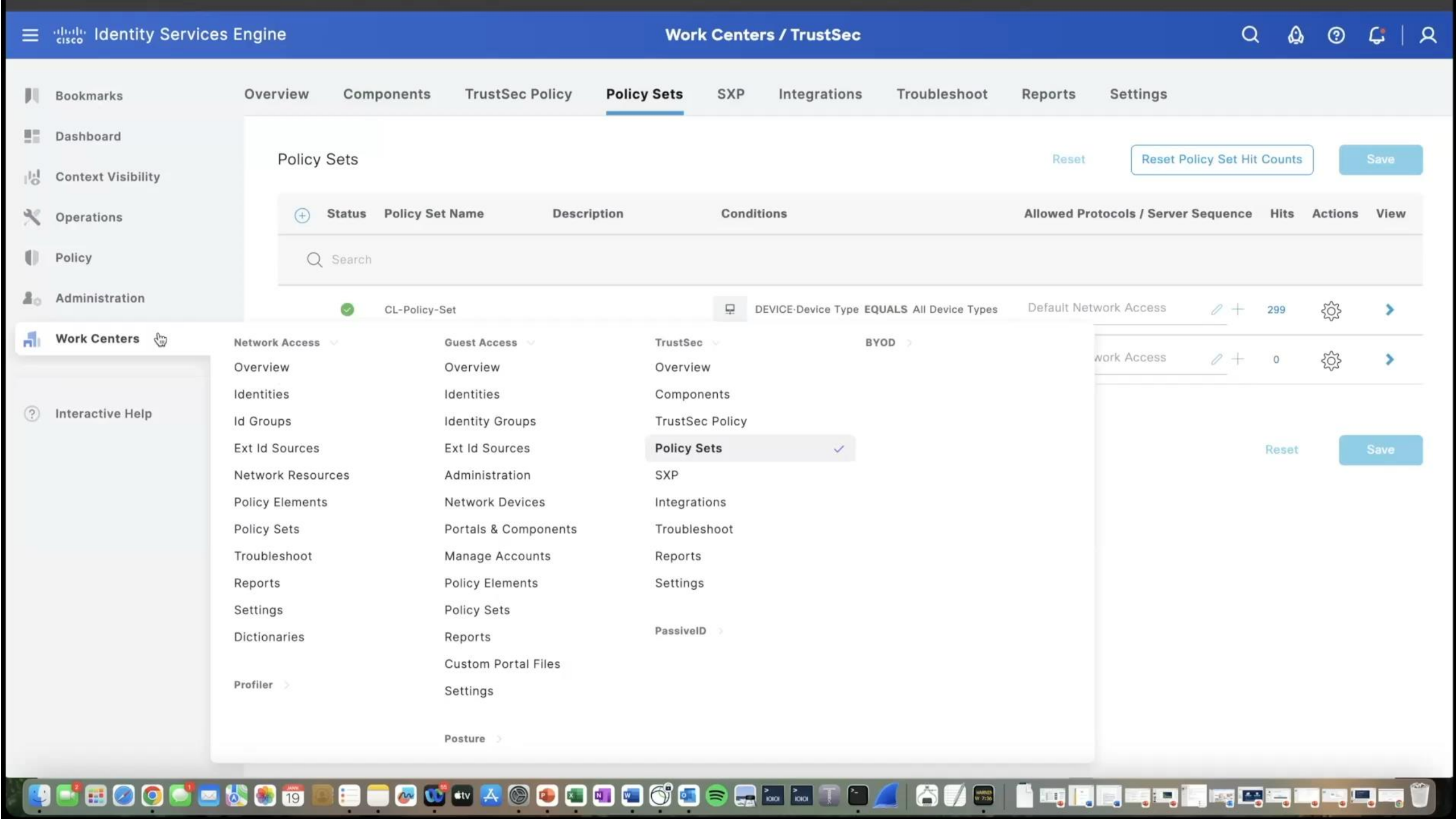


1. Classification via ISE (802.1X)

= Employees (SGT : 4)

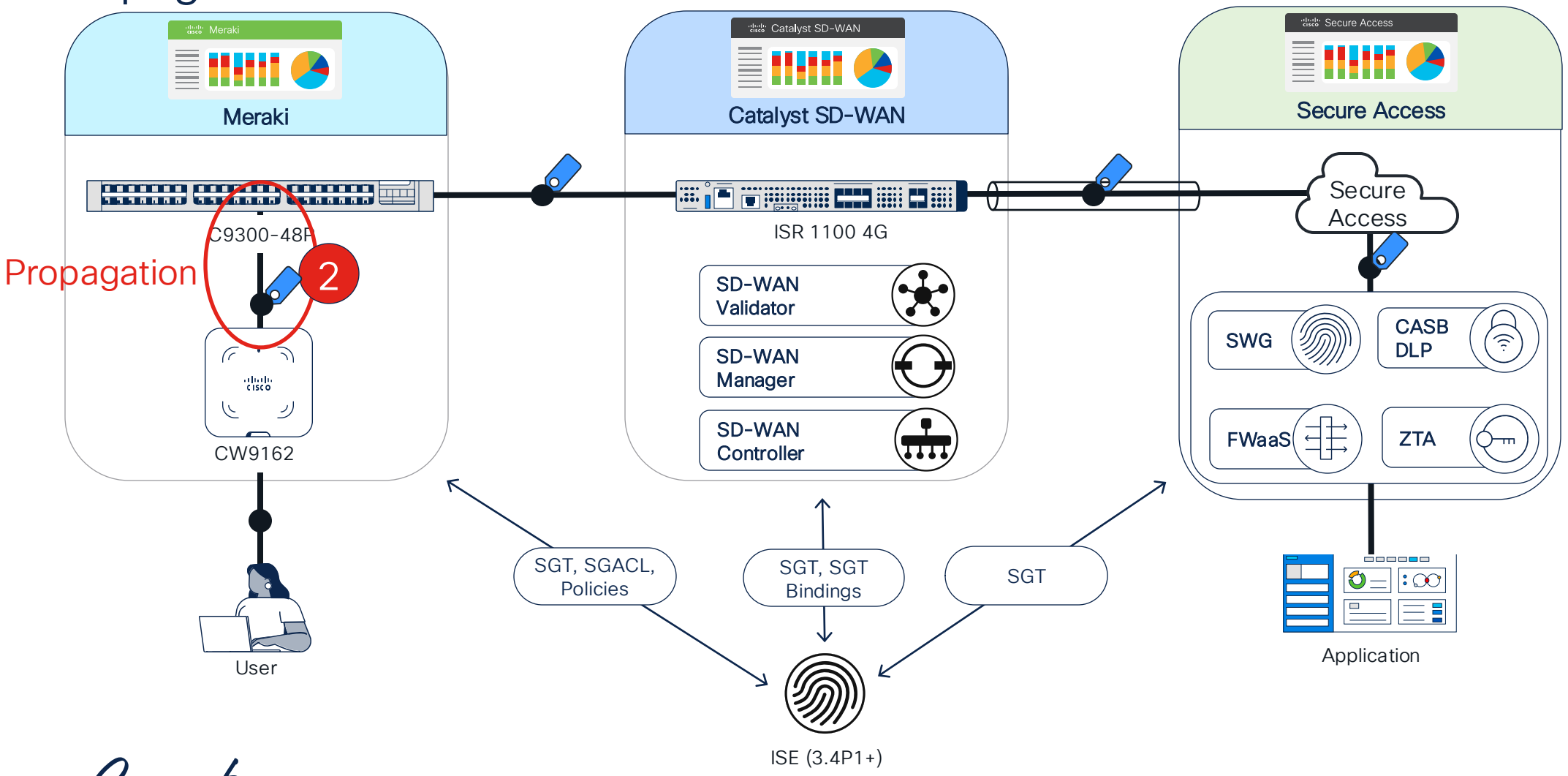



09:41
Réglages
Modifier
Wi-Fi
Connectez-vous au Wi-Fi, consultez les réseaux disponibles et gérez les réglages d'accès aux réseaux et aux bornes d'accès à proximité. En savoir plus...
Wi-Fi
AirDrop, AirPlay, Me prévenir en cas d'oubli et l'amélioration de la précision de la localisation nécessitent le Wi-Fi.


Identity Services Engine
Work Centers / TrustSec
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Overview
Components
TrustSec Policy
Policy Sets
SXP
Integrations
Troubleshoot
Reports
Settings
Policy Sets
Reset
Reset Policy Set Hit Counts
Save
Status
Policy Set Name
Description
Conditions
Allowed Protocols / Server Sequence
Hits
Actions
View
Search
CL-Policy-Set
DEVICE·Device Type EQUALS All Device Types
Default Network Access
299
0
Reset
Save
Network Access
Overview
Identities
Id Groups
Ext Id Sources
Network Resources
Policy Elements
Policy Sets
Troubleshoot
Reports
Settings
Dictionaries
Profiler
Guest Access
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Posture
TrustSec
Overview
Components
TrustSec Policy
Policy Sets
SXP
Integrations
Troubleshoot
Reports
Settings
PassiveID
BYOD

Secure Internet access

2. Propagation de l'AP au switch



2. Propagation de l’AP au switch

= Employees (SGT : 4)

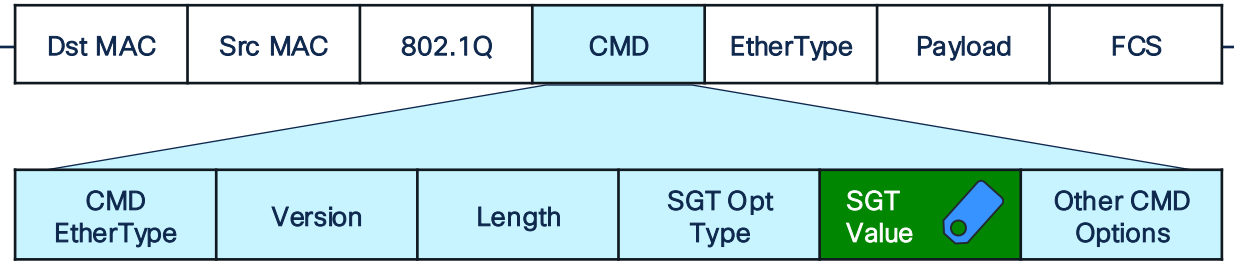
Access point	Event type	Details
CW9162I	Adaptive Policy state change	state: enabled, configured: true, uplink_sgt_support: true

CW9162

Peer SGT capable: Enabled | Disabled

Adaptive policy group: 2: Infrastructure

C9300-48U




```
10.1.19.7                142.250.186.46              TCP
> Frame 10495: 74 bytes on wire (592 bits), 74 bytes captured
> Ethernet II, Src: ba:2d:b9:74:c2:e6 (ba:2d:b9:74:c2:e6), Ds
v Cisco MetaData
    Version: 1
    Length: 1
    Options: 0x0001
    SGT: 4
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.1.19.7, Dst: 142.250.1
> Transmission Control Protocol, Src Port: 62780, Dst Port: 4
```

Global Overview

Organization
VALETTE

Network
FR92130 - Issy

Secure Connect
Network-wide
Assurance New
Security & SD-WAN
Switching
Wireless
Insight
Organization

Find in Menu

New in Dashboard: *Building Better Alerting Experiences: An Overview of Enhanced Alert Features and 3 other features.* Read more.

Switches

Last day

+ Add a switch

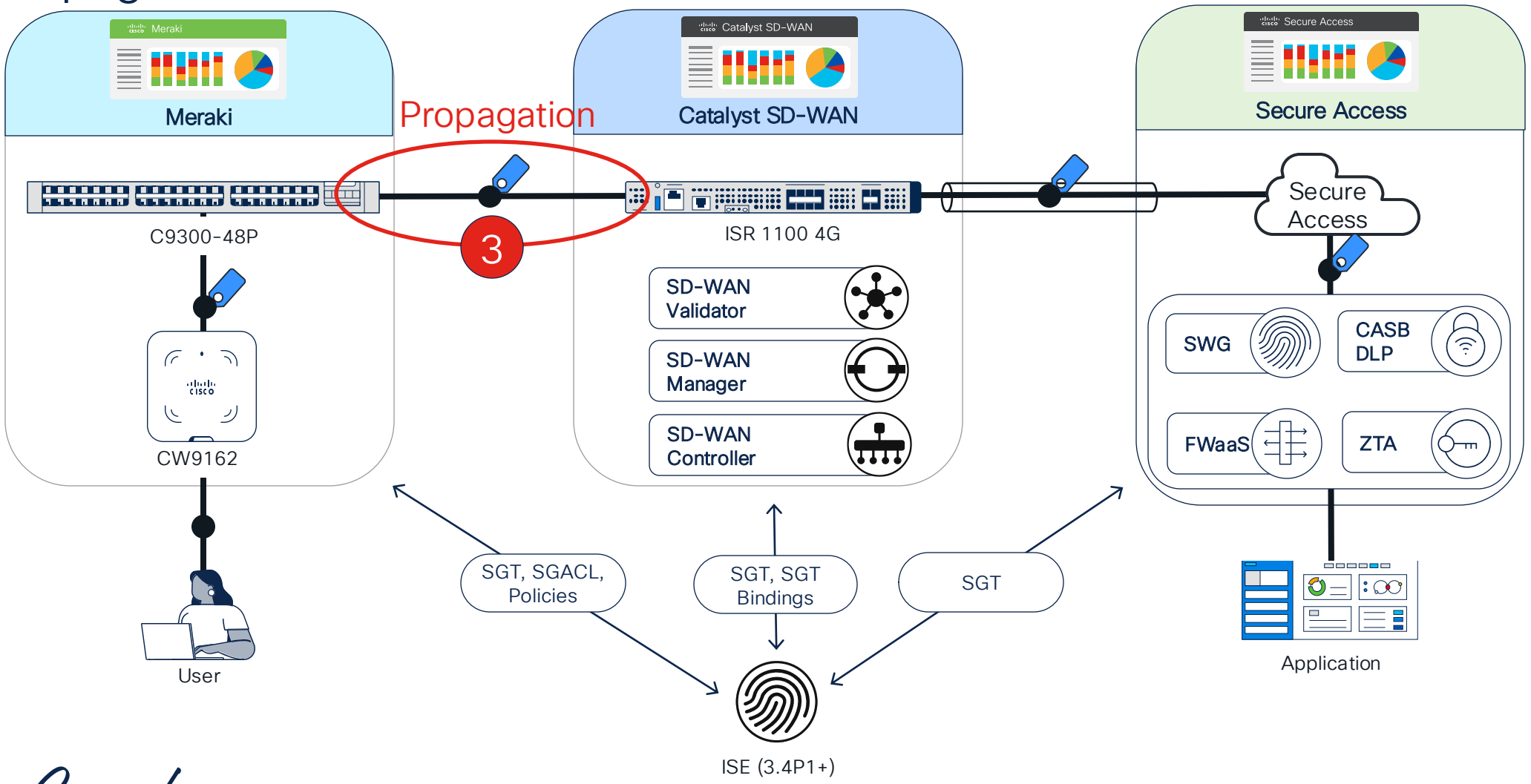
0 Offline	0 Alerting	1 Online	0 Dormant

Search | Status | Tags | Device type | 1 result | Download

Status	Name	MAC address	Connectivity (UTC-8)	Serial number	Local IP
✓	CL25-SW	e8:eb:34:a4:75:00		Q5TG-EQW2-ZA7W	10.1.19.6

Secure Internet access

3. Propagation du switch au routeur



3. Propagation du switch au routeur

= Employees (SGT : 4)

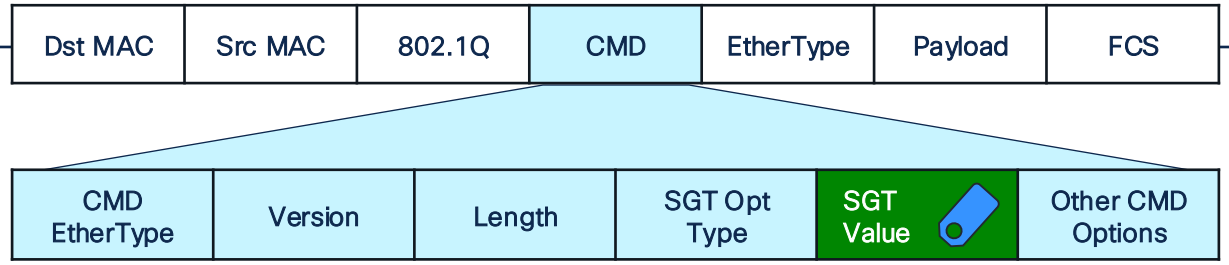
Peer SGT capable: Enabled | Disabled

Adaptive policy group: 2: Infrastructure

C9300-48U

```
interface GigabitEthernet0/0/1
 vrf forwarding 10
 cts manual
 policy static sgt 2 trusted
```

ISR 1100 4G




```
10.1.19.7                142.250.186.46              TCP
> Frame 10495: 74 bytes on wire (592 bits), 74 bytes captured
> Ethernet II, Src: ba:2d:b9:74:c2:e6 (ba:2d:b9:74:c2:e6), Ds
v Cisco MetaData
    Version: 1
    Length: 1
    Options: 0x0001
    SGT: 4
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.1.19.7, Dst: 142.250.1
> Transmission Control Protocol, Src Port: 62780, Dst Port: 4
```

The network is out of compliance due to licensing, please click here for more actions.

Monitor
Configuration
Analytics
Workflows
Tools
Reports
Maintenance
Administration
Explore

Select Device

CL25-router | 7.7.7.28 Site Name 27001 Device Model: ISR 1100 4G (Cisco OS)

AppQoE DRE Optimization
Connection Events
WAN Throughput
Flows
Top Talkers

WAN
TLOC
Tunnel
Managed Cellular Activation - eSIM

SECURITY MONITORING
Firewall
Intrusion Prevention
URL Filtering
Advanced Malware Protection
TLS/SSL Decryption
Umbrella DNS Re-direct

Control Connections
System Status
Events
ACL Logs
Troubleshooting
Real Time

Device Options: System Information

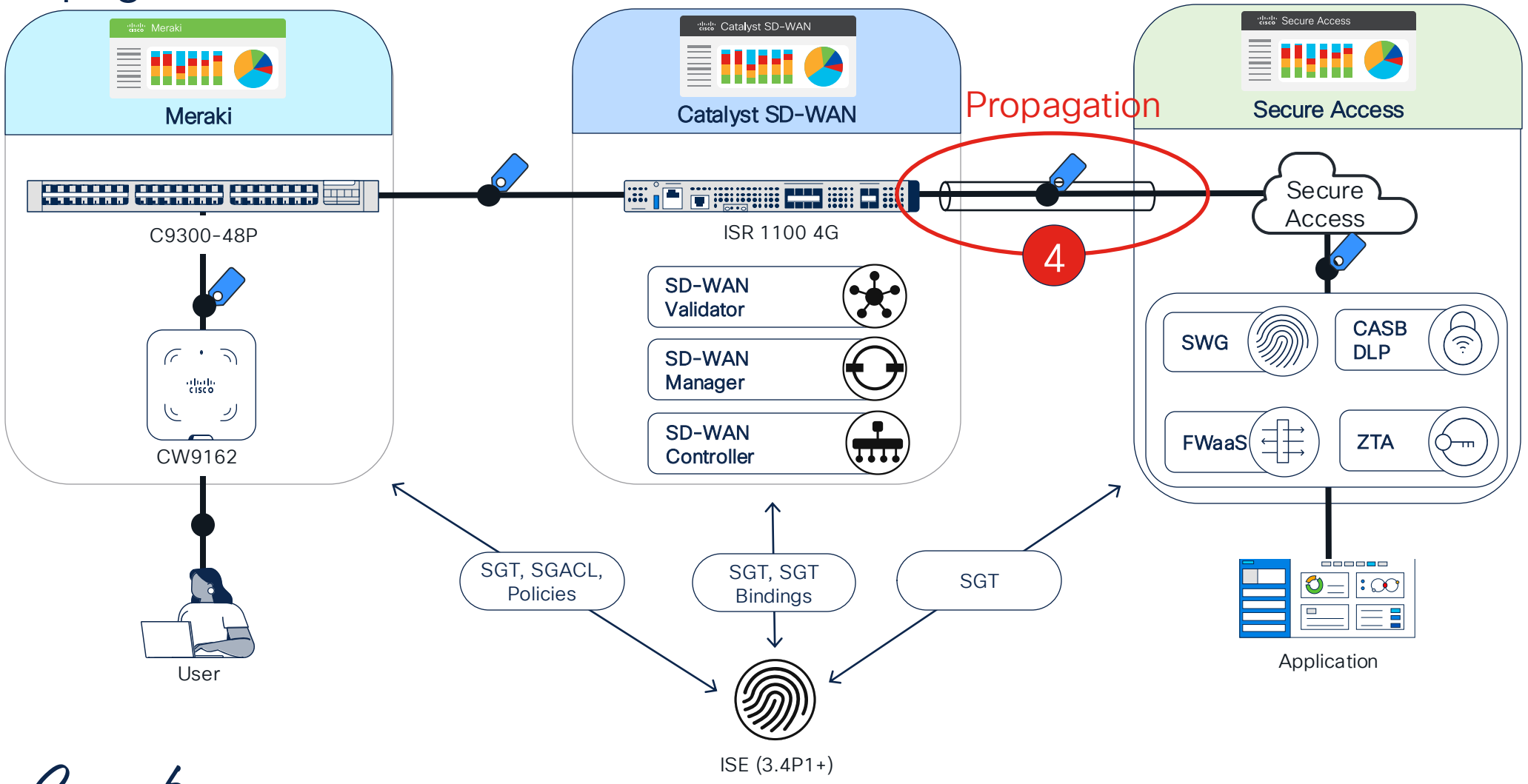
Search

Total Rows: 10

Property	Value
Hostname	CL25-router
Last Updated	19 Jan 2025 7:12:40 PM CET
Latitude	37.666684
Longitude	-122.777023
Personality	WAN Edge
Site ID	27001
Timezone	UTC +0000
Vbond	vbond-1692376.viptela.net

Secure Internet access

4. Propagation du routeur à Secure Access



4. Propagation du routeur au SSE

= Employees (SGT : 4)

ISR1100-4G-FGL2347L52J	Tunnel16000001	IPSEC	active	Cisco Secure Access
ISR1100-4G-FGL2347L52J	Tunnel16000002	IPSEC	backup	Cisco Secure Access

ISR 1100 4G

ISR1100-4G-FGL2347L52J

Review and edit this network tunnel group. Details for each IPsec tunnel added

Summary

Connected

Region Europe (Germany) Routing Type NAT / Outbound Only

Device Type Catalyst SDWAN

Secure Access

CLEUR25

SSE Provider

Cisco SSE Zscaler

Context Sharing

VPN SGT

```
CL25-router#show platform packet-trace packet 0
Packet: 0           CBUG ID: 0
Summary
  Input     : GigabitEthernet0/0/1
  Output    : GigabitEthernet0/0/0
  State     : FWD
  Timestamp
    Start   : 56785409528447 ns (01/22/2025 22:12:11.122782 UTC)
    Stop    : 56785409699943 ns (01/22/2025 22:12:11.122954 UTC)
Path Trace
  Feature: IPV4(Output)
    Input       : GigabitEthernet0/0/1
    Output      : Tunnel16000001
    Source      : 10.1.19.4
    Destination : 8.8.8.8
    Protocol    : 1 (ICMP)
  Feature: IPSec
    Result    : IPSEC_RESULT_SA
    Action    : ENCRYPT
    SA Handle : 28
    Peer Addr : 8.8.8.8
    Local Addr: 10.1.19.4
  Feature: SDWAN SSE Metadata
    Next protocol: 1
    SGT          : 0
    Source VPN   : 10
```

Monitor
Configuration
Analytics
Workflows
Tools
Reports
Maintenance
Administration
Explore

The network is out of compliance due to licensing, please click here for more actions.

Configuration Groups

SD-WAN

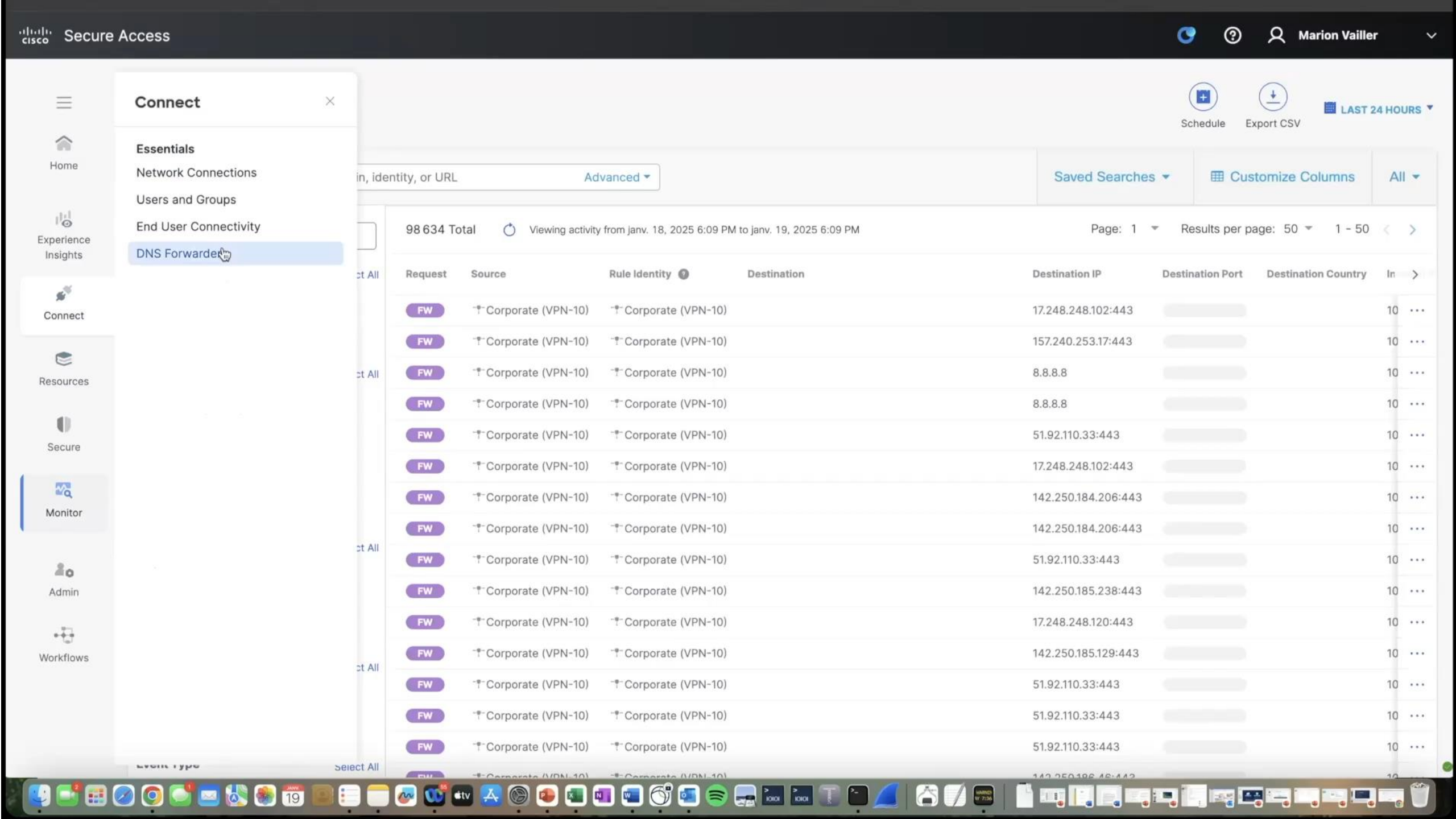
Configuration Groups 20 | System Profile 39 | Transport & Management Profile 40 | Policy Profile 1 | Service Profile 38 | CLI Add-on Profile 18 | UC Voice Profile 1 | Other Profile 3

Search | Last Updated | Status | Create Configuration Group | Export | Import

As of: Jan 23, 2025 01:17 PM

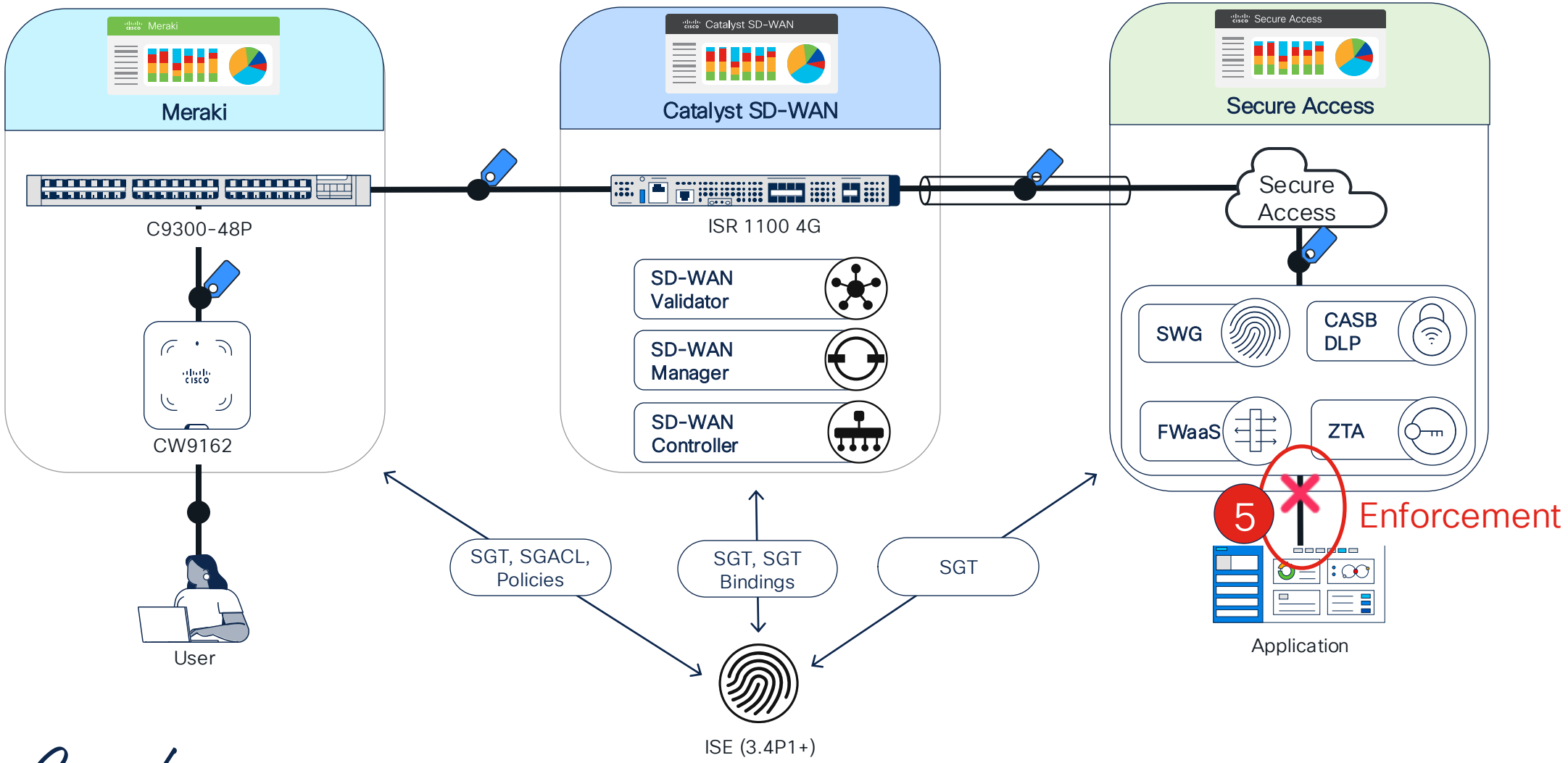
Name	Type	Profile	Provisioning Status (In Sync Devices / Associated Devices)	Origin	Updated By	Last Updated On	Actions
lab-fimoreir-home	Single Router	6	1 / 1	user	fimoreir	Jan 23, 2025, 12:50:35 PM	
CPOC-London-Large	Single Router	4	1 / 1	user	fomuya	Jan 23, 2025, 11:40:18 AM	
CPOC-London-Devices	Single Router	4	2 / 2	user	fomuya	Jan 23, 2025, 11:37:38 AM	
fomuya-cpoc	Single Router	4	0 / 0	user	fomuya	Jan 23, 2025, 11:37:38 AM	
Bydgoszcz-makrupin-Home	Single Router	4	1 / 1	user	makrupin	Jan 23, 2025, 11:23:15 AM	
ISB_Sdwan_4451	Single Router	2	0 / 1	user	fimoreir	Jan 22, 2025, 8:04:49 PM	
nboursie_home	Single Router	4	1 / 1	user	fimoreir	Jan 22, 2025, 8:01:20 PM	

Rows per page 10 | 1 | 2 | Go to: 1 / 2


Secure Access
Marion Vailler
Connect
Essentials
Network Connections
Users and Groups
End User Connectivity
DNS Forwarder
Home
Experience Insights
Connect
Resources
Secure
Monitor
Admin
Workflows
Schedule
Export CSV
LAST 24 HOURS
Advanced
Saved Searches
Customize Columns
All
98 634 Total
Viewing activity from janv. 18, 2025 6:09 PM to janv. 19, 2025 6:09 PM
Page: 1
Results per page: 50
1 - 50
Request
Source
Rule Identity
Destination
Destination IP
Destination Port
Destination Country
FW
Corporate (VPN-10)
17.248.248.102:443
157.240.253.17:443
8.8.8.8
51.92.110.33:443
142.250.184.206:443
142.250.185.238:443
17.248.248.120:443
142.250.185.129:443

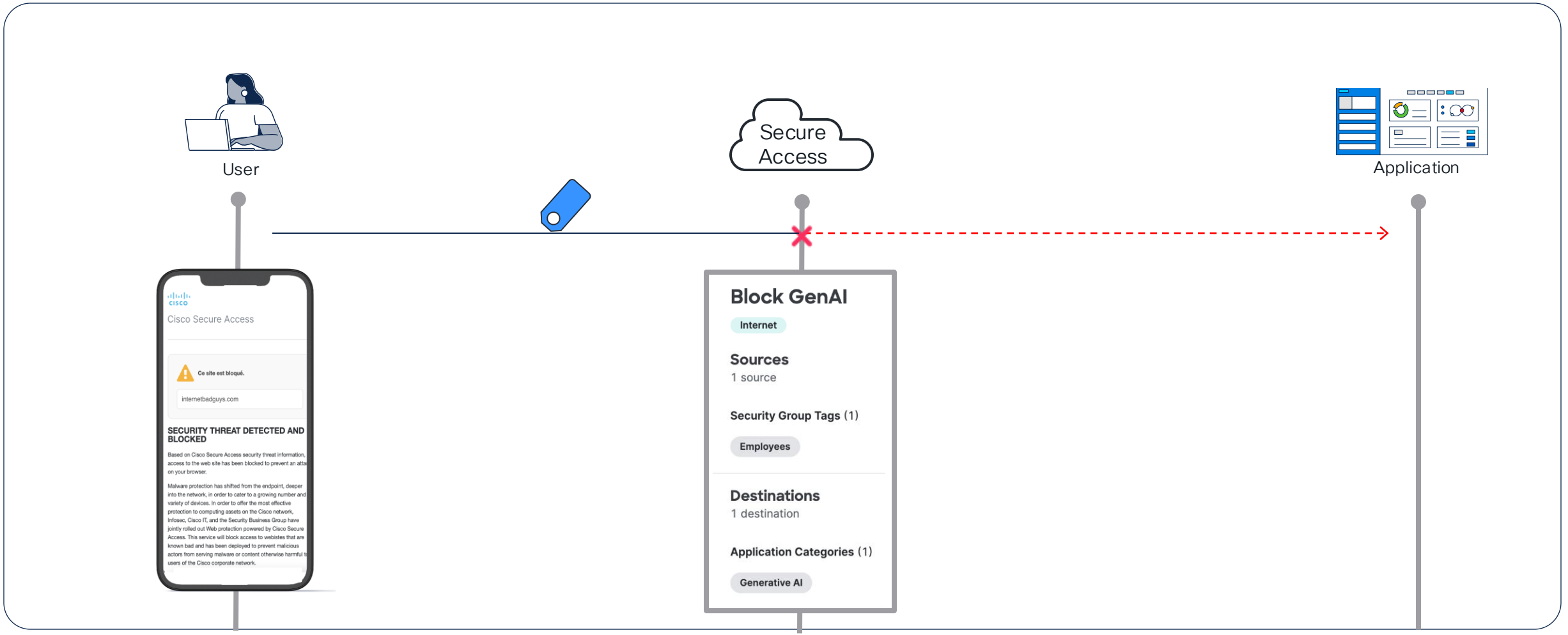
Secure Internet access

5. Enforcement sur Secure Access



5. Enforcement sur Secure Access

= Employees (SGT : 4)



Home
Experience Insights
Connect
Resources
Secure
Monitor
Admin
Workflows

Security Group Tags

Security Group Tags (SGT) specify the privileges of a traffic source within a trusted network. When you enable an Identity Services Engine integration, SGTs become available for use in access rules. Help

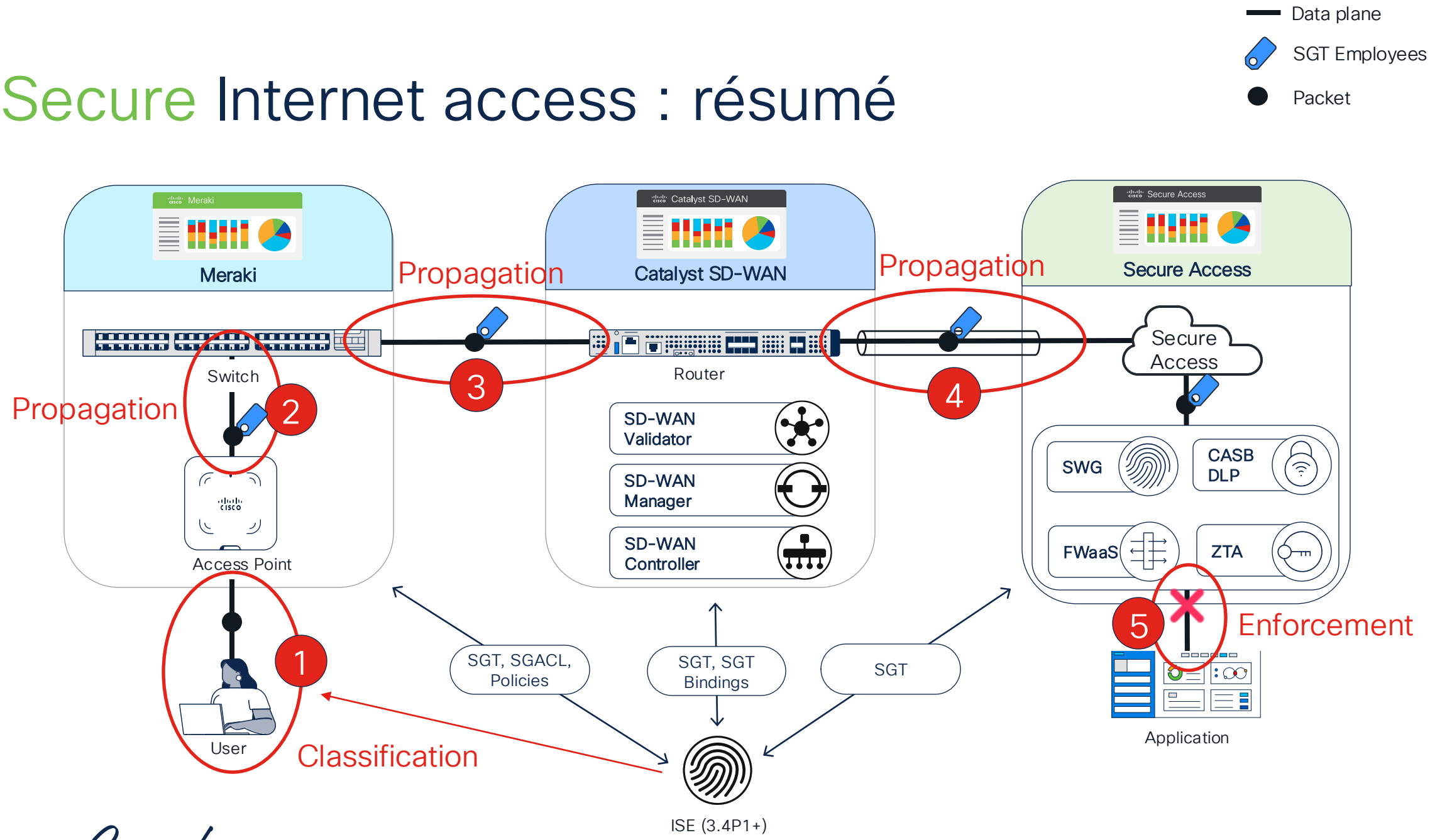
Search

18 total

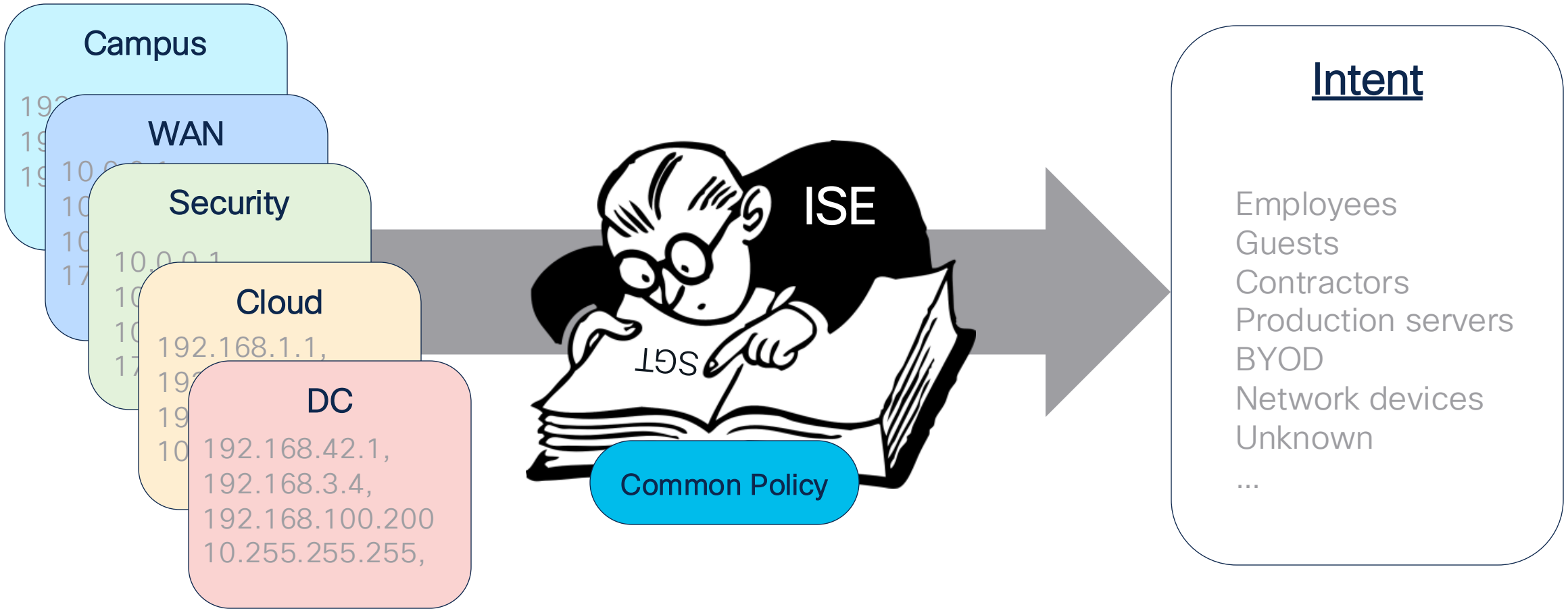
As of: Jan 19, 2025, 07:31 PM

Name	Tag
ANY	65535
Auditors	9
BYOD	15
Contractors	5
Developers	8
Development_Servers	12
Employees	4
Guests	6
Network_Services	3
PCI_Servers	14

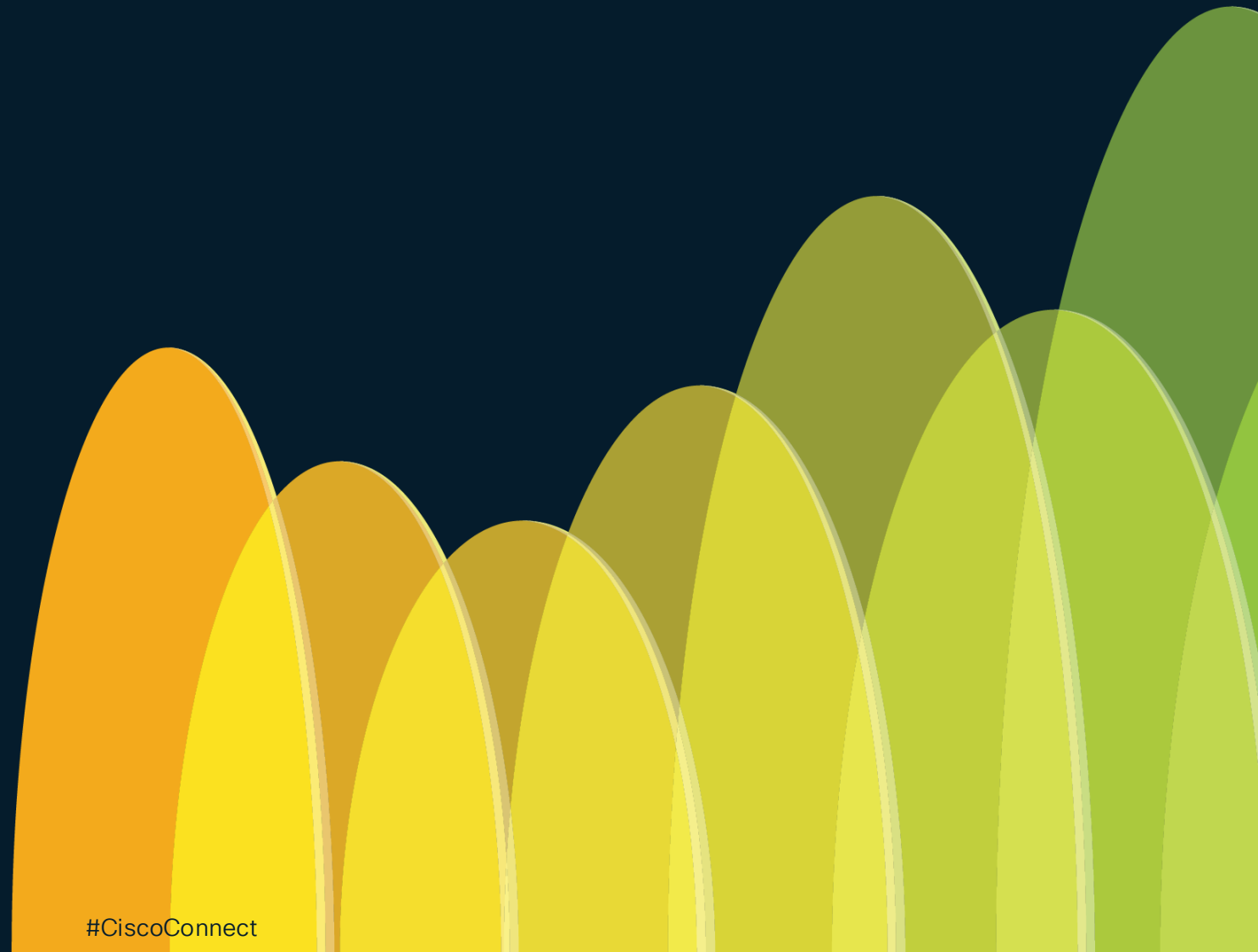
Secure Internet access : résumé



Transformez votre Securité avec Common Policy



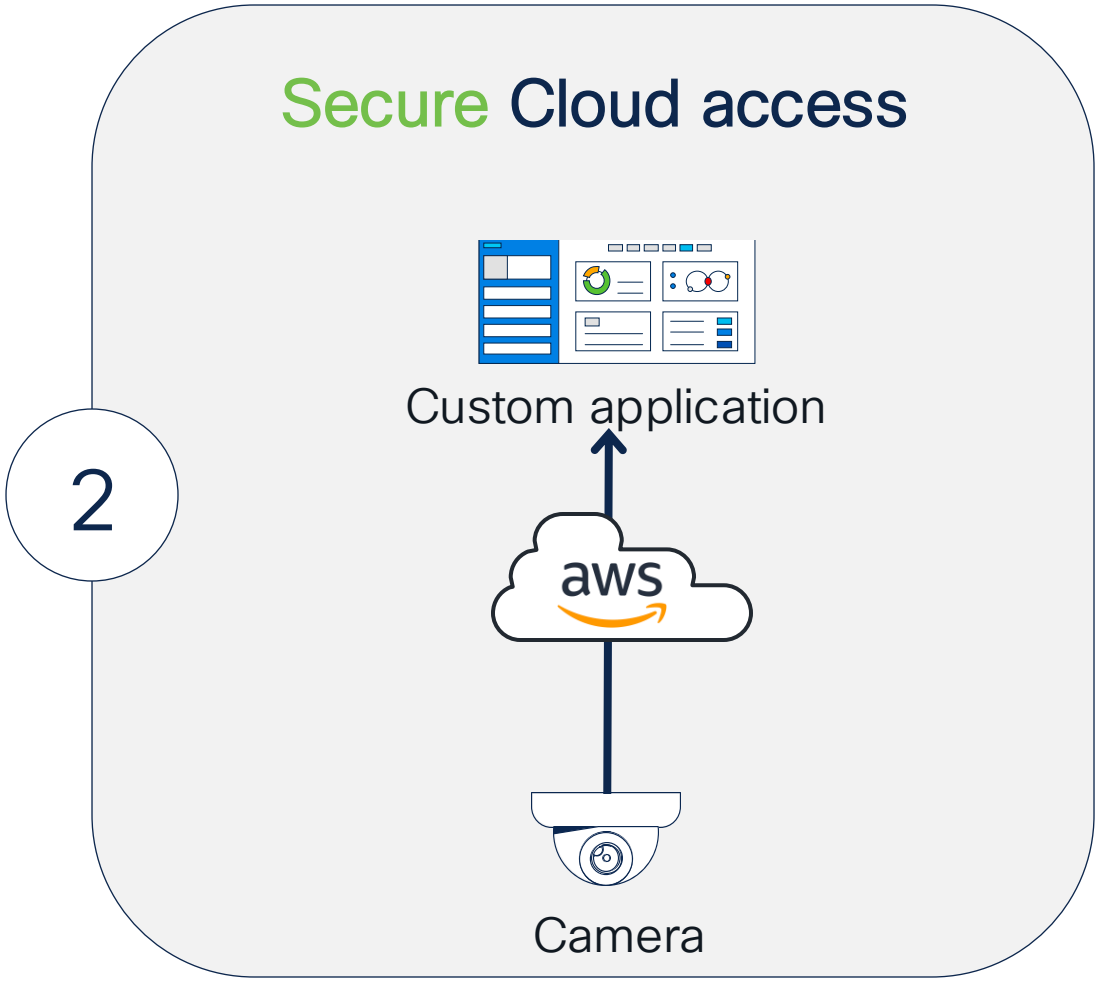
Second Demo Time !



*Already covered in Demo 1

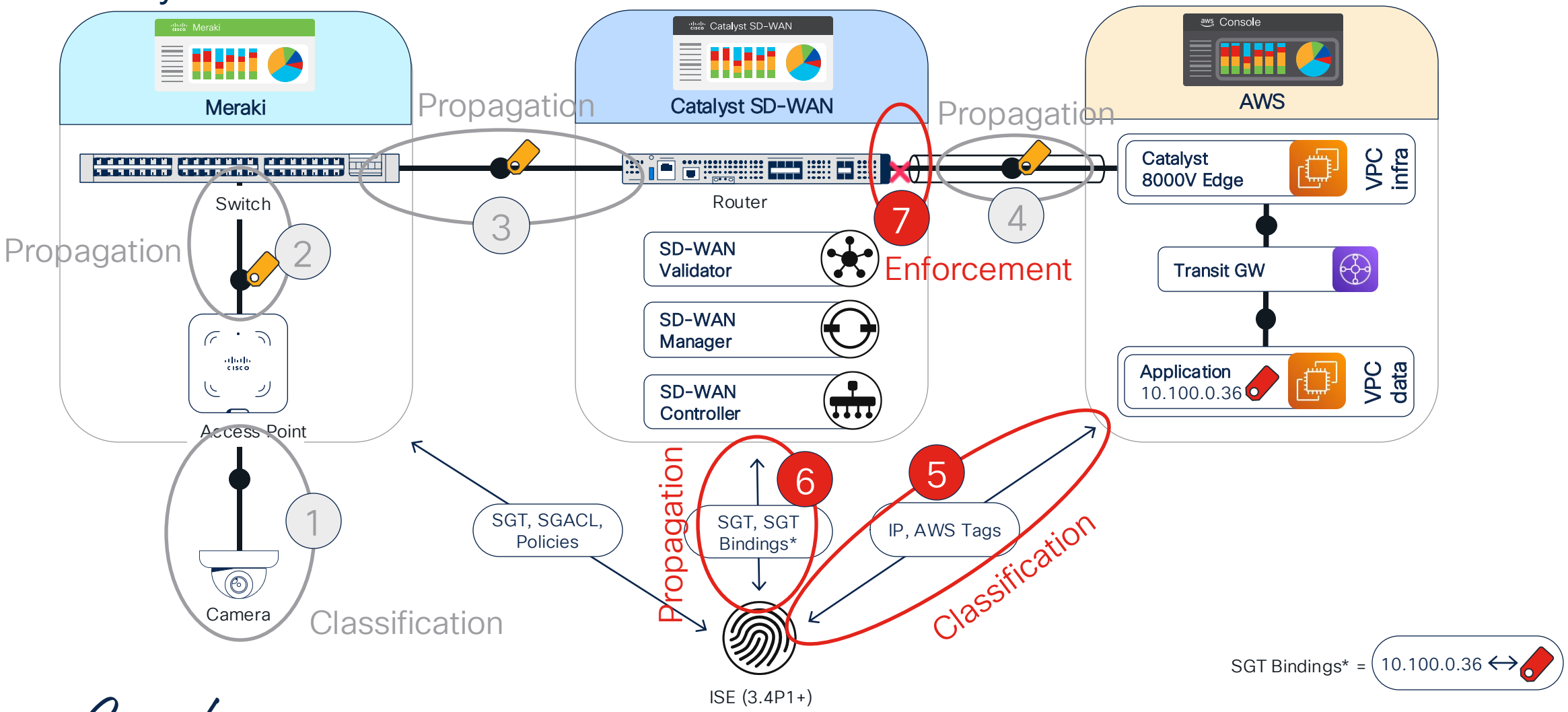
A camera needs to access to an AWS application

1. Classification of asset via profiling*
2. Propagation from AP to switch*
3. Propagation switch to router*
4. Propagation in SD-WAN Fabric*
5. Classification of EC2 via APIs
6. Propagation of EC2 classification
7. Enforcement via NGFW on SD-WAN Edge



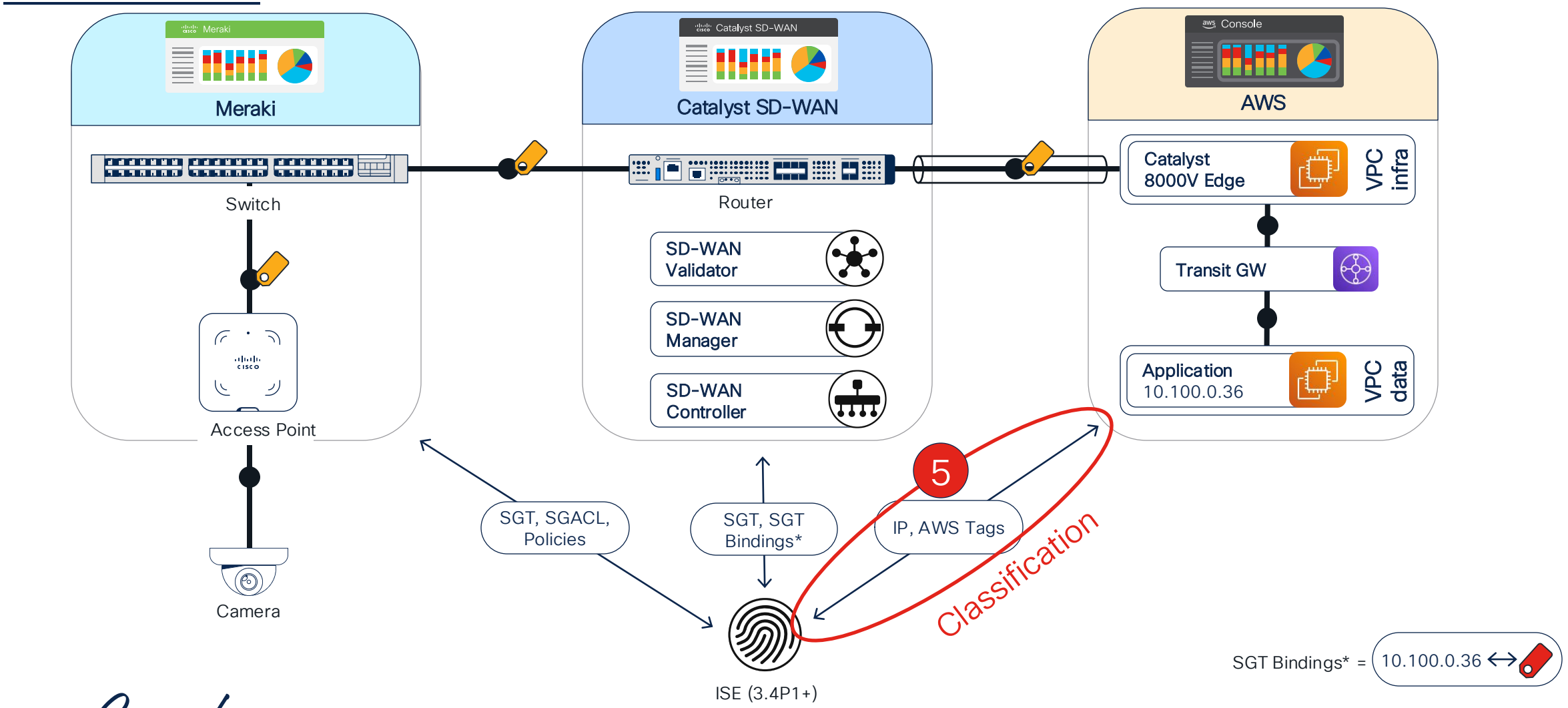
Secure Cloud access

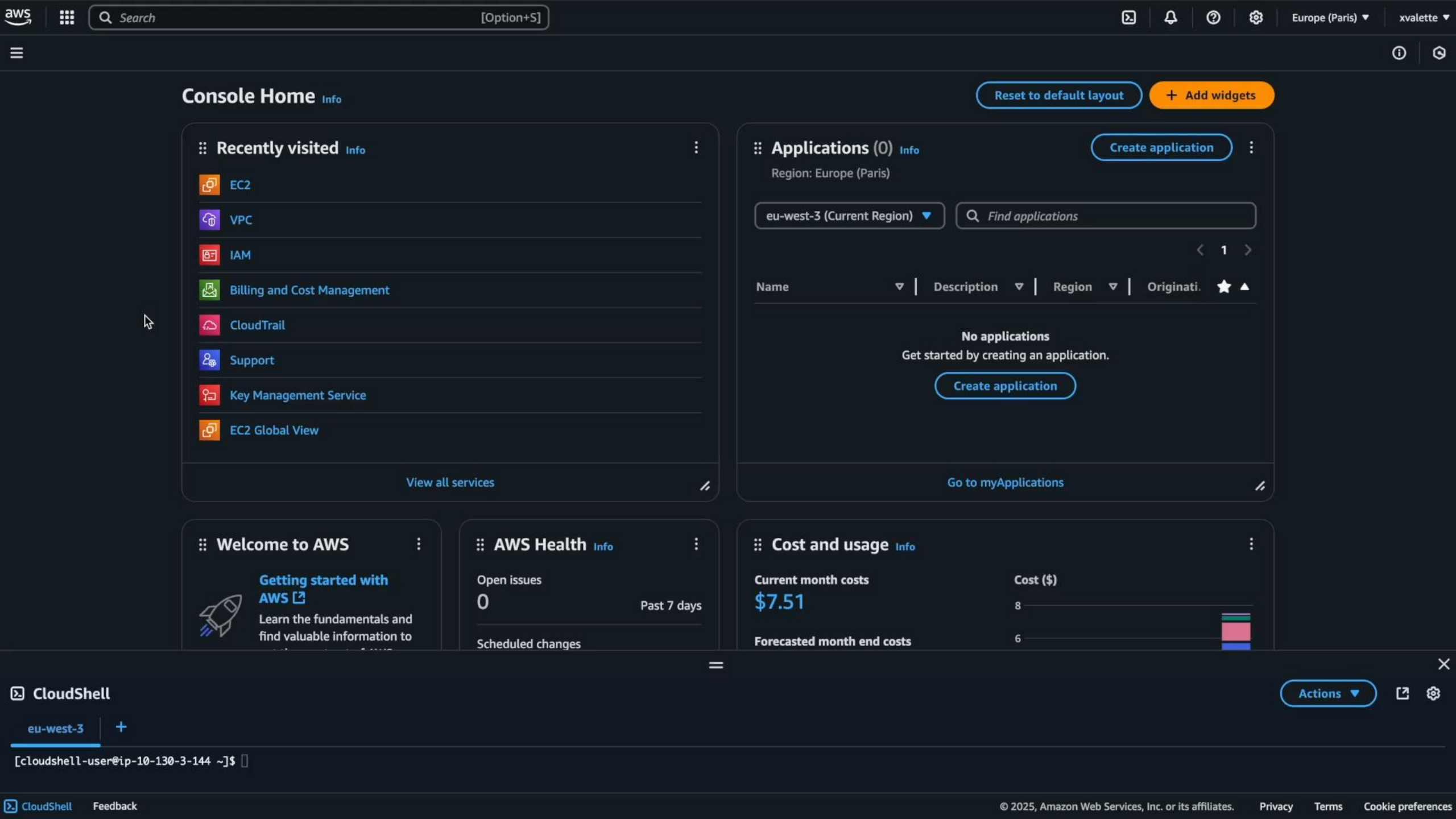
Summary



Secure Cloud access

Classification of EC2 via API




Search
[Option+S]
Europe (Paris)
xvalette
Console Home Info
Reset to default layout
Add widgets
Recently visited Info
EC2
VPC
IAM
Billing and Cost Management
CloudTrail
Support
Key Management Service
EC2 Global View
View all services
Applications (0) Info
Create application
Region: Europe (Paris)
eu-west-3 (Current Region)
Find applications
1
Name
Description
Region
Originati.
No applications
Get started by creating an application.
Create application
Go to myApplications
Welcome to AWS
Getting started with AWS
Learn the fundamentals and find valuable information to
AWS Health Info
Open issues
0
Past 7 days
Scheduled changes
Cost and usage Info
Current month costs
$7.51
Forecasted month end costs
Cost ($)
8
6
CloudShell
Actions
eu-west-3
[cloudshell-user@ip-10-130-3-144 ~]$
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

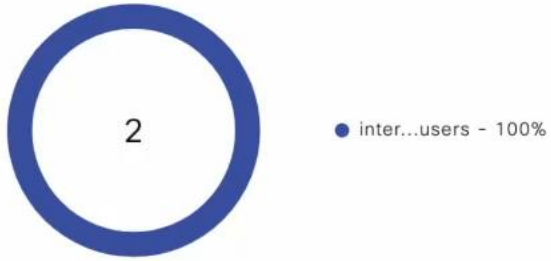
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help

Summary | Endpoints | Guests | Vulnerability | Threat | Manage

Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior	Authenticated Guests
3	1	0	0	0

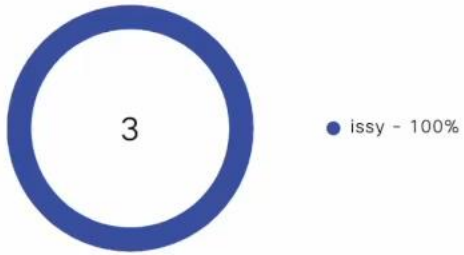
AUTHENTICATIONS

Identity Store | Identity Group | Network Device | Failure Reason



NETWORK DEVICES

Device Name | Type | Location



ENDPOINTS

Profile | Logical Profile

BYOD ENDPOINTS

Type | Profile

No data available.

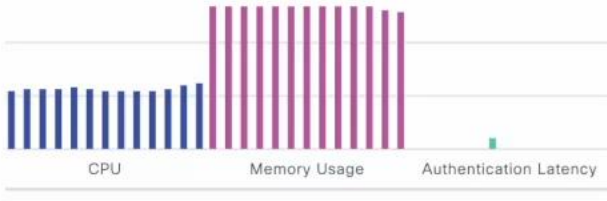
ALARMS

Severity	Name	Occu...	Last Occurr
	Name		
	DNS Resolution Failure	2261	2 mins ago
	ISE Authentication In...	10363	2 mins ago
	Configuration Changed	1769	1 hr 21 mins

SYSTEM SUMMARY

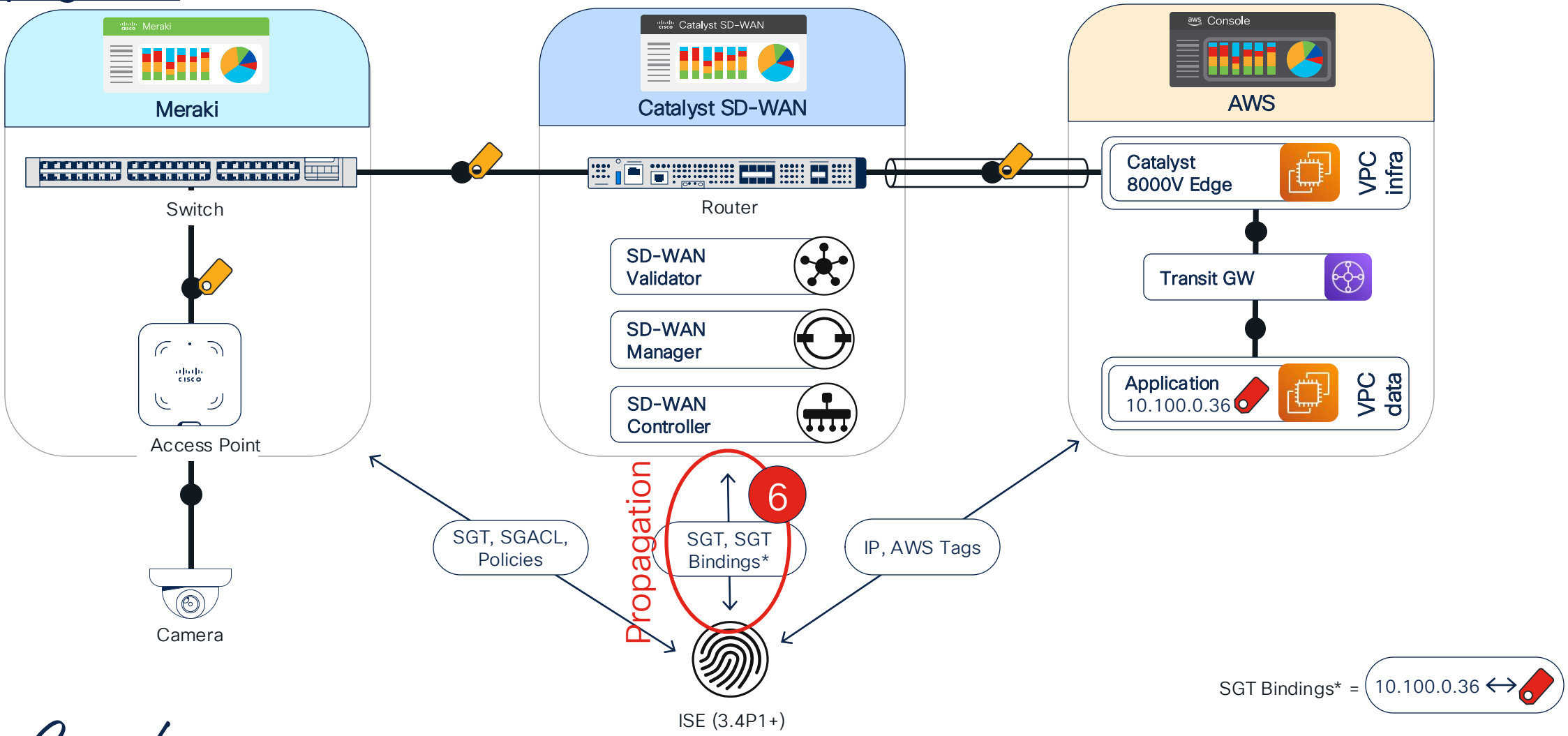
1 node(s) All 24HR

SecureWAN-ise



Secure Cloud access

Propagation of EC2 classification



Monitor
Configuration
Analytics
Workflows
Tools
Reports
Maintenance
Administration
Explore

Monitor

All Sites

Overview | Devices | Security | Multicloud | Tunnels | Logs | Energy Management | Applications | Sites | Circ

Control Components

1	1	1
Validator	Controller	Manager

WAN Edges

20	4
Reachable	Unreachable

Sites

13	6
Up	Down

Circuits

18	12
Up	Down

Certificate Status

0	0
Warning	Invalid

Licensing

2	26
Assigned	Unassigned

Reboot

4
Last 24 hrs

1 Hour

Actions

Application Experience

View Details

QoE

102
Applications

Usage (Total)

1
GB

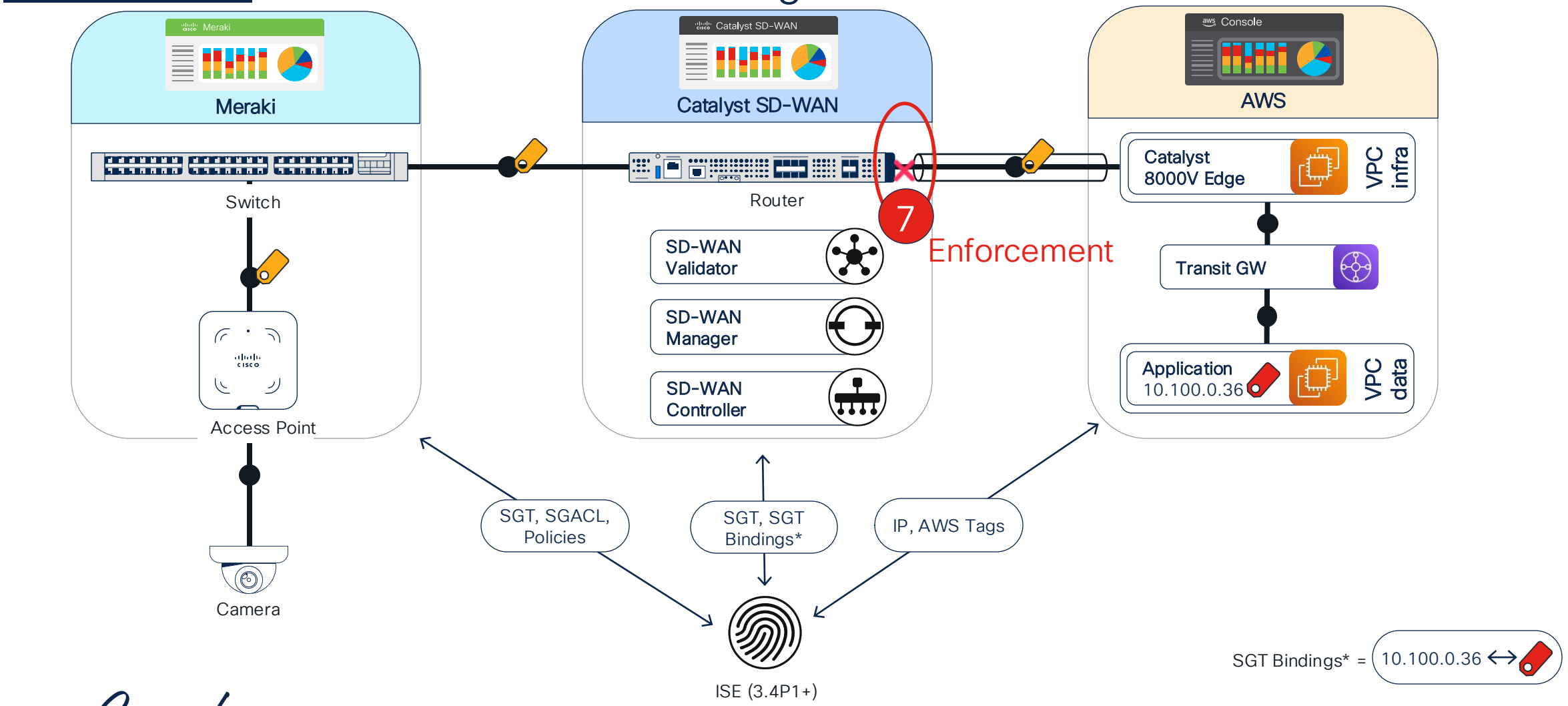
Top 20 by usage

Top 20 by usage 1 GB

0.4GB

Secure Cloud access

Enforcement via NGFW on SD-WAN Edge



Monitor
Configuration
Analytics
Workflows
Tools
Reports
Maintenance
Administration
Explore

Monitor

All Sites

Overview | Devices | Security | Multicloud | Tunnels | Logs | Energy Management | Applications | Sites | Circ

Control Components

1	1	1
Validator	Controller	Manager

WAN Edges

20	4
Reachable	Unreachable

Sites

13	6
Up	Down

Circuits

18	12
Up	Down

Certificate Status

0	0
Warning	Invalid

Licensing

2	26
Assigned	Unassigned

Reboot

4
Last 24 hrs

1 Hour

Actions

Application Experience

View Details

QoE

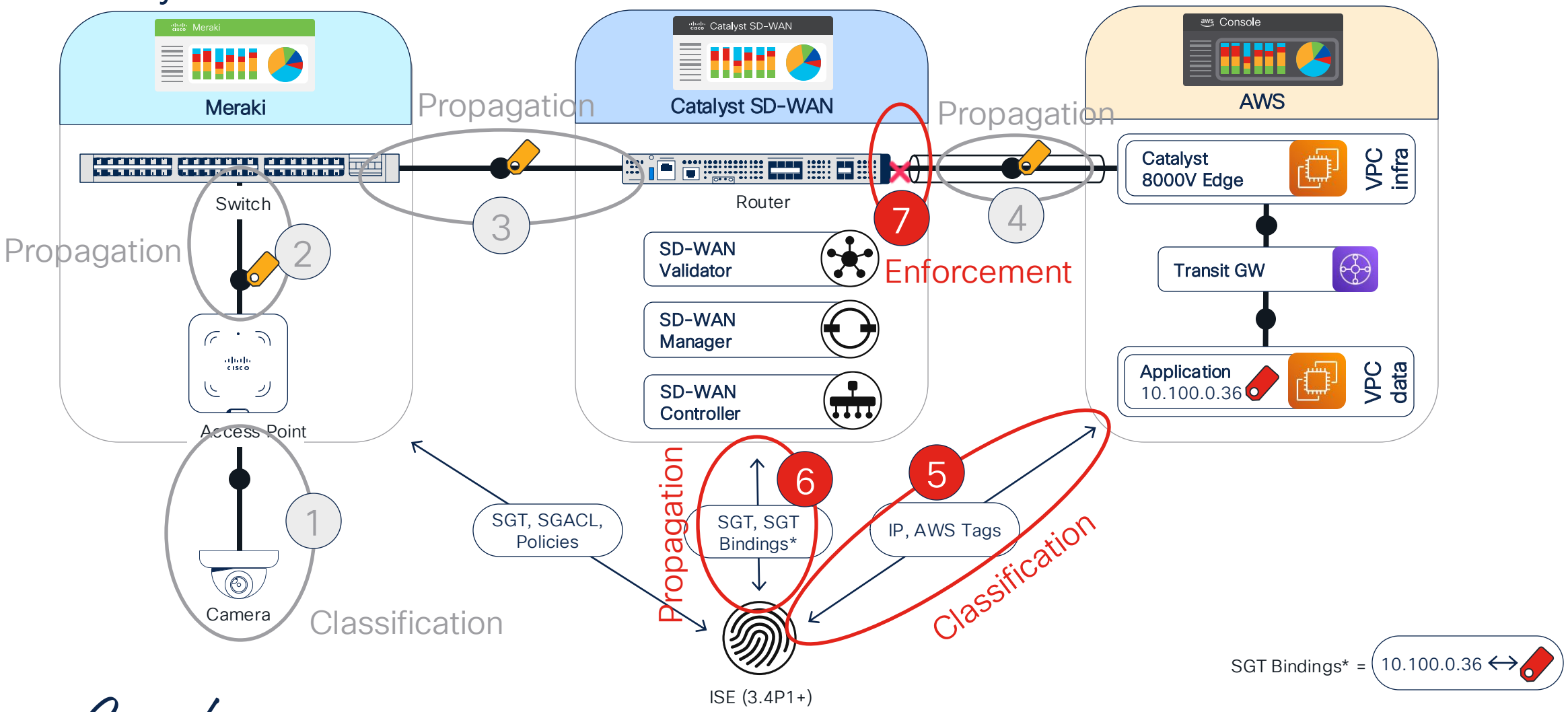
Usage (Total)

Top 20 by usage

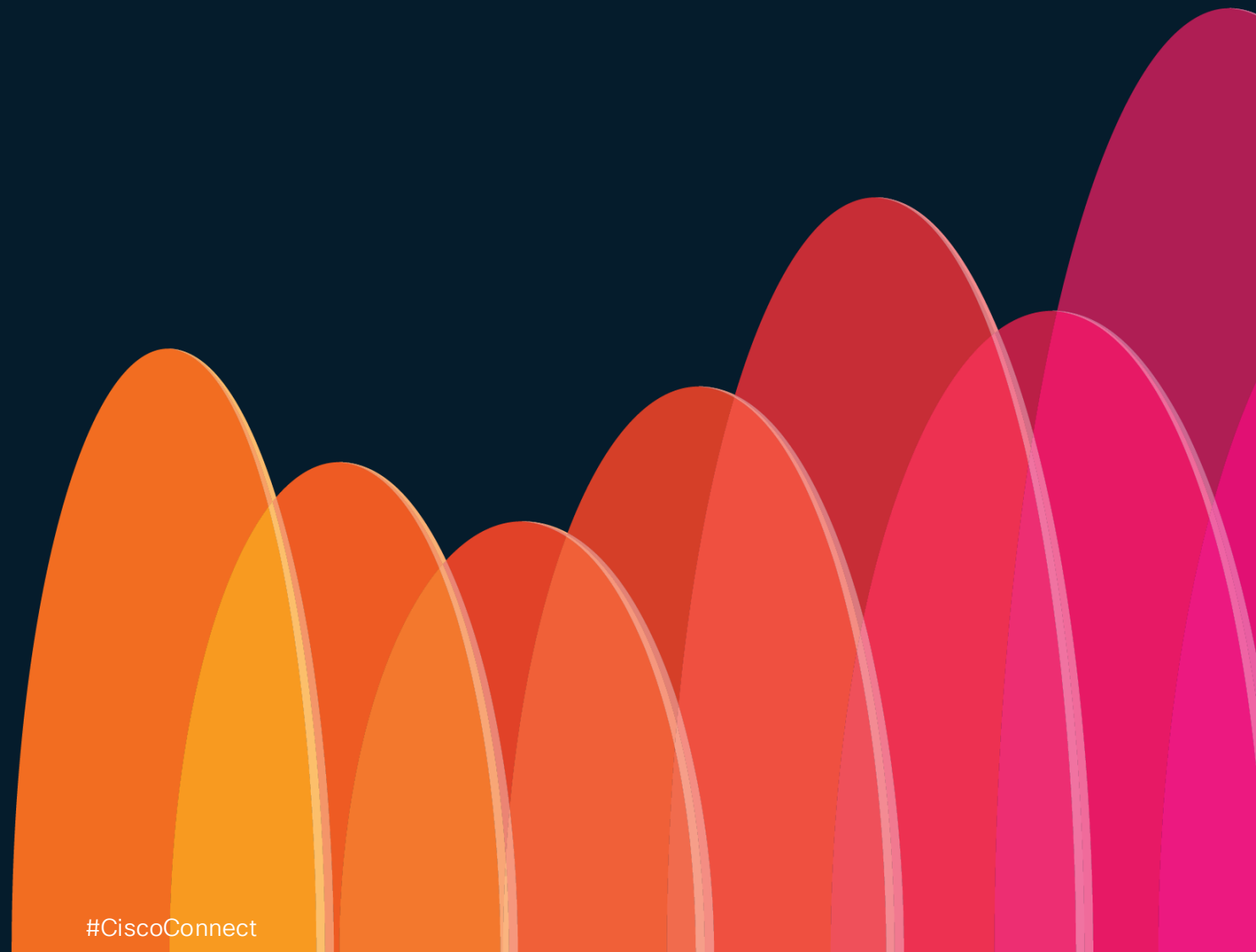
Top 20 by usage 2 GB

Secure Cloud access

Summary



Key takeaways

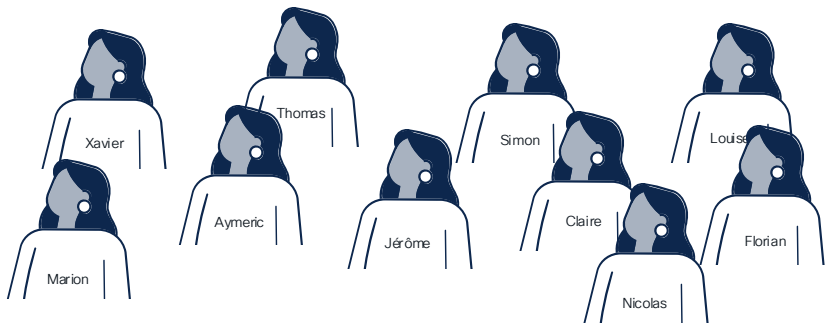


On ne peut pas imaginer un Cisco Connect sans badges

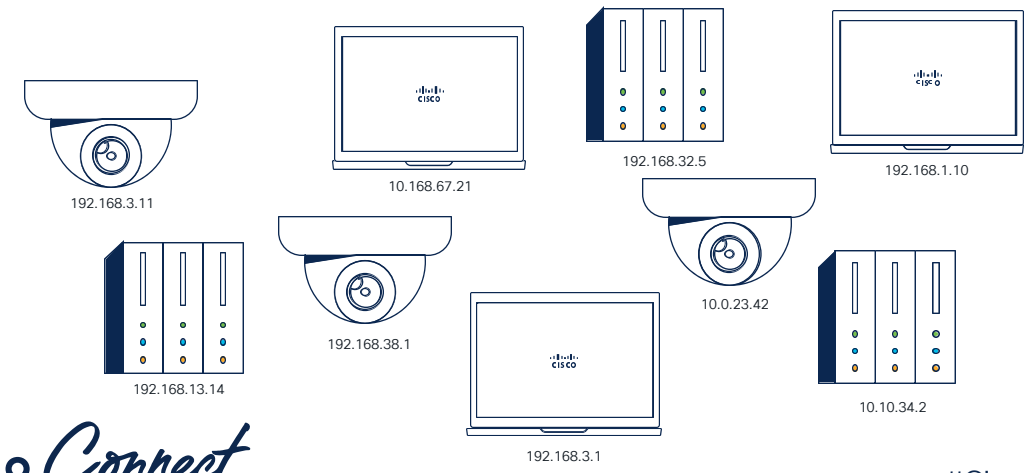
Imaginez votre infrastructure avec Common Policy

Without Common Policy

Cisco Connect



Infrastructure



With Common Policy

cisco Connect

Meet us @World of Solution Booth

Go Beyond with Cisco CX !

	Premium Support		Solution Attached Services		Lifecycle Services
	Service	Case	Service	Use Case	Example Activities
User Protection Protect users from any location, accessing applications anywhere, with frictionless zero-trust secure access	SWSS Premium	Guidance on user security software from set up assist with device trust, discovering devices and users on the network, secure access, and onboarding and configuration of Cisco Secure products in the environment with facilitation 3rd party product secure interoperability	SAS Secure Access	Securely adopt secure access-based technology to protect distributed workforce's access from any device, anywhere. Phased migration with configuration porting, intent mapping, and data plane transition	Configuration of advanced malware protection on Secure Firewall, Secure Email, and Web-Security bringing deeper visibility into network-level and network-edge threat activities. Activities include accelerating secure network access, SASE advisory
	Success Tracks Cloud and Network Security	Visibility of NGFWs HW devices across cloud and hybrid environments to ease contract management in one platform	SAS ISE	Securely adopt a zero-trust strategy by using experienced security strategy, analysis, and best practices to accelerate the safeguarding of the network along with implementation for endpoints and access ports, tuning and stabilization of ISE production environment, and evaluating implementation issues	
	Success Tracks Zero Trust	Support ISE's role in supporting zero trust capabilities via one platform to view all ISE SNS appliances	SAS Firewall	Securely adopt technology to monitor and protect your network from unauthorized access. Adopt Firewall to fully-utilize advanced capabilities including secure workload integration	


cisco
Thank you
cisco Connect
#CiscoConnect