

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font.

CISCO *Live!*

The text "Let's go" in a large, dark blue, sans-serif font, positioned to the left of a bright, multi-colored sunburst graphic that radiates from the right side of the image.

Let's go

#CiscoLiveAPJC



The bridge to possible

A Common Policy for Network Agility and Security

The Unified Meraki Approach

Alex Burger - Principal Technical Marketing Engineer
@aaburger85 | CCIEw 45253 | CWNE 249
BRKMER-2234

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

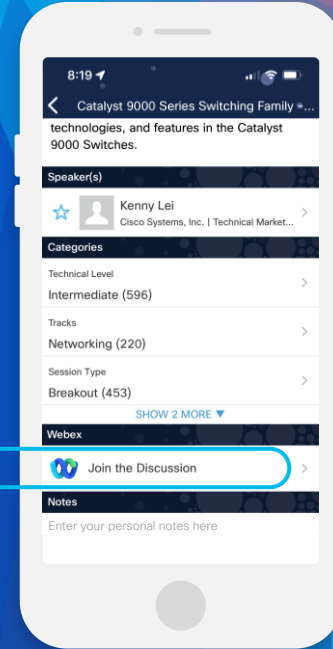
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKMER-2234>

Alex Burger

Worked in the industry for 15+ years as a:

- WiSP Deployment and Support Engineer
- Implementation Engineer for a partner
- Meraki SE
- Product Architect in Product Management
- Senior TME on Meraki Switching
- Principal TME covering Meraki NX products
- CCIE Wireless #45253 | CWNE #249
- Enjoyer of Single Malts and Scotch
- Avid runner and snowboarder
- Enjoys torturing self with home automation
- Dabbler in 3D Printing
- Sometimes a blogger: [WirelesslyWIRED](#)



CISCO *Live!*



Me



Also
Me



Not
Me



Yup,
me

Agenda

- How Meraki provides a common policy framework
- Policy Definition and Management
- Product support review
 - MX/Z
 - MS
 - MR
- Integrations across Cisco

Dashboard Structure

Dashboard Organization

Org Admins

Template Networks

Org-Wide Features

Org-Wide Settings

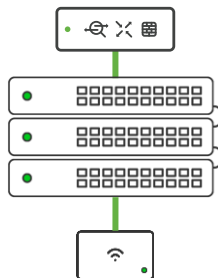
Network A

MR/MS/MX/MV/MT/SM Home

Per-Network Configs

Telemetry and Visibility

Network Level Admins



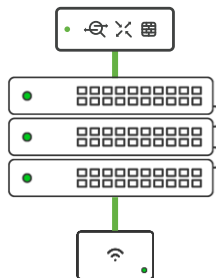
Network B

MR/MS/MX/MV/MT/SM Home

Per-Network Configs

Telemetry and Visibility

Network Level Admins



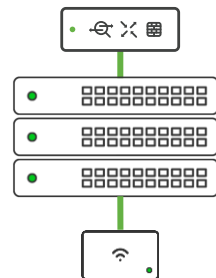
Network C

MR/MS/MX/MV/MT/SM Home

Per-Network Configs

Telemetry and Visibility

Network Level Admins



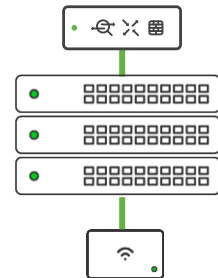
Network D

MR/MS/MX/MV/MT/SM Home

Per-Network Configs

Telemetry and Visibility

Network Level Admins



Before we jump in...

A common policy framework should help



minimize exposure in
an organization



provide multi-tenancy
in a secure way



maintain compliance
and pass security
audits



quarantine malicious
or compromised
devices



implement a zero-
trust framework

Common Policy

Adaptive Policy



Organization-Wide intent-based policy



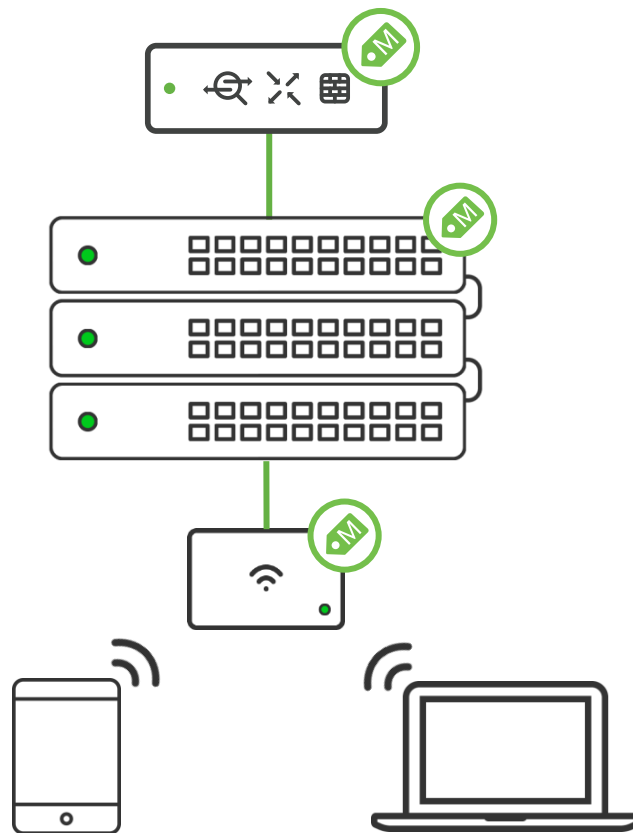
Utilizing inline Security Group Tags (SGTs)



Context shared over the data-plane



IP and topology agnostic security providing consistent policy for wired and wireless access



Group Assignment Techniques

Static Assignment

MS
Switchport
IP/Subnet to SGT
VLAN to SGT **

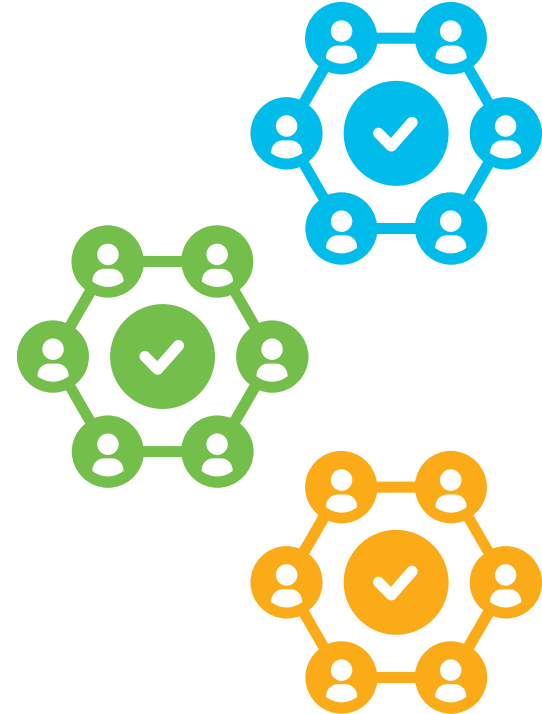
MR
SSID to SGT
Group Policy + SGT**

MX
Port/VLAN to SGT
Group Policy + SGT**

Dynamic Assignment

RADIUS assignment
attribute based classification
Examples:
Profile
Posture
Location
Credentials/Credential Types
AD Group/s
Supported on MS/MR today
Coming to MX in later release

Foundation for Zero-Trust



SGT via any RADIUS server

An SGT is just a RADIUS av-pair that is sent to the network device in the Access-Accept message

The SGT AV-Pair is:

```
cisco-av-pair:cts:security-group-tag={SGT value in HEX}-{revision number}
```

Must be hex of
SGT decimal value

Can be as simple as
00

Configuration interface showing a RADIUS client setup. The client is named "TestClient" and is associated with the "iPSK Default" group. The configuration includes a checkmark icon, the group name "iPSK Default", a computer icon, the text "Radius: Called-Station-ID CONTAINS Tornado-AP_PSK", a dropdown menu showing "DefaultPSK4Clients", and a plus sign icon.

Result

Class CACS:adcd880600000000386d43c6:ww-ise/374370439/1664

cisco-av-pair cts:security-group-tag=0fa0-00

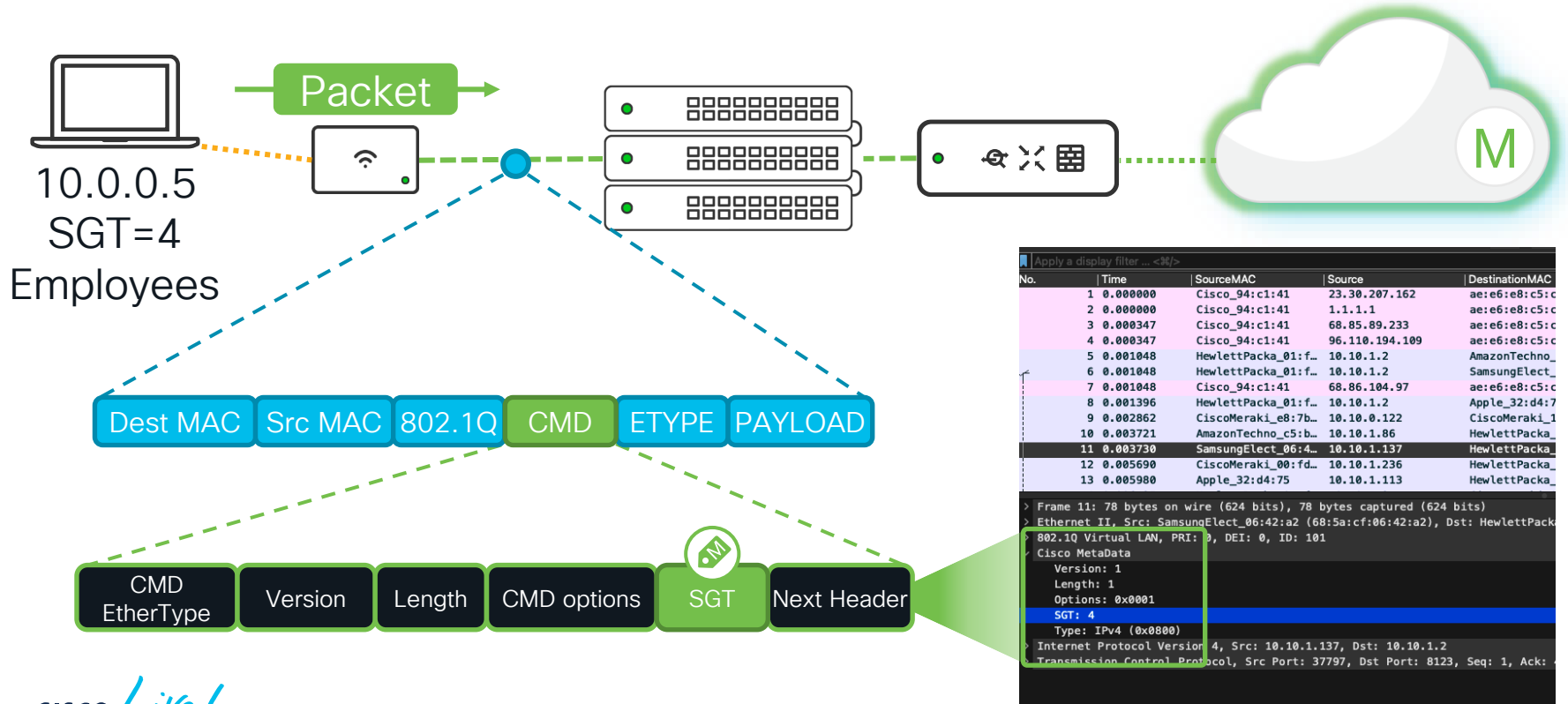
= 4000

MS-MPPE-Send-Key ****

MS-MPPE-Recv-Key ****

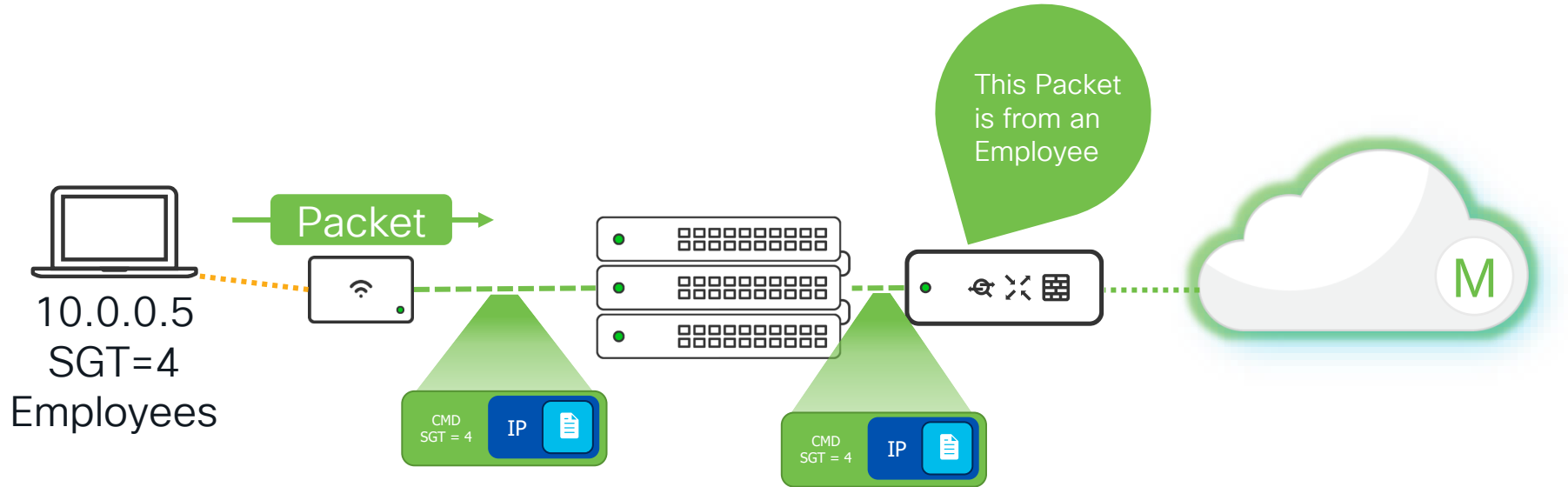
LicenseTypes Base license consumed

What are SGTs?

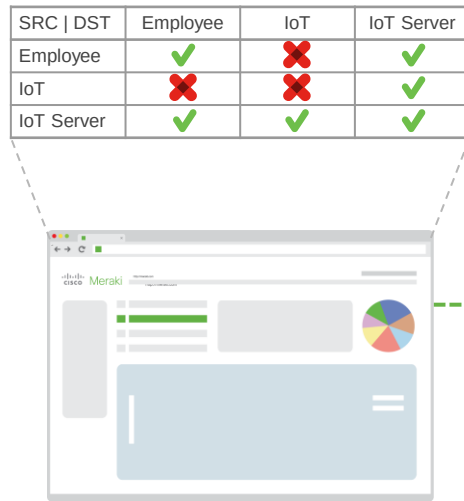
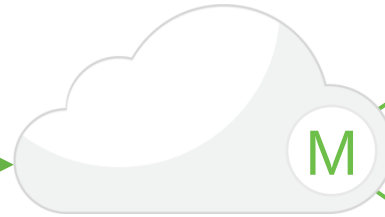


Scalable Identity and Context

Sharing information over the dataplane, in every packet



One Consistent Policy Across Networks



Policy & Groups are configured in dashboard and pushed to Adaptive Policy nodes like any other Meraki configuration change

API First!

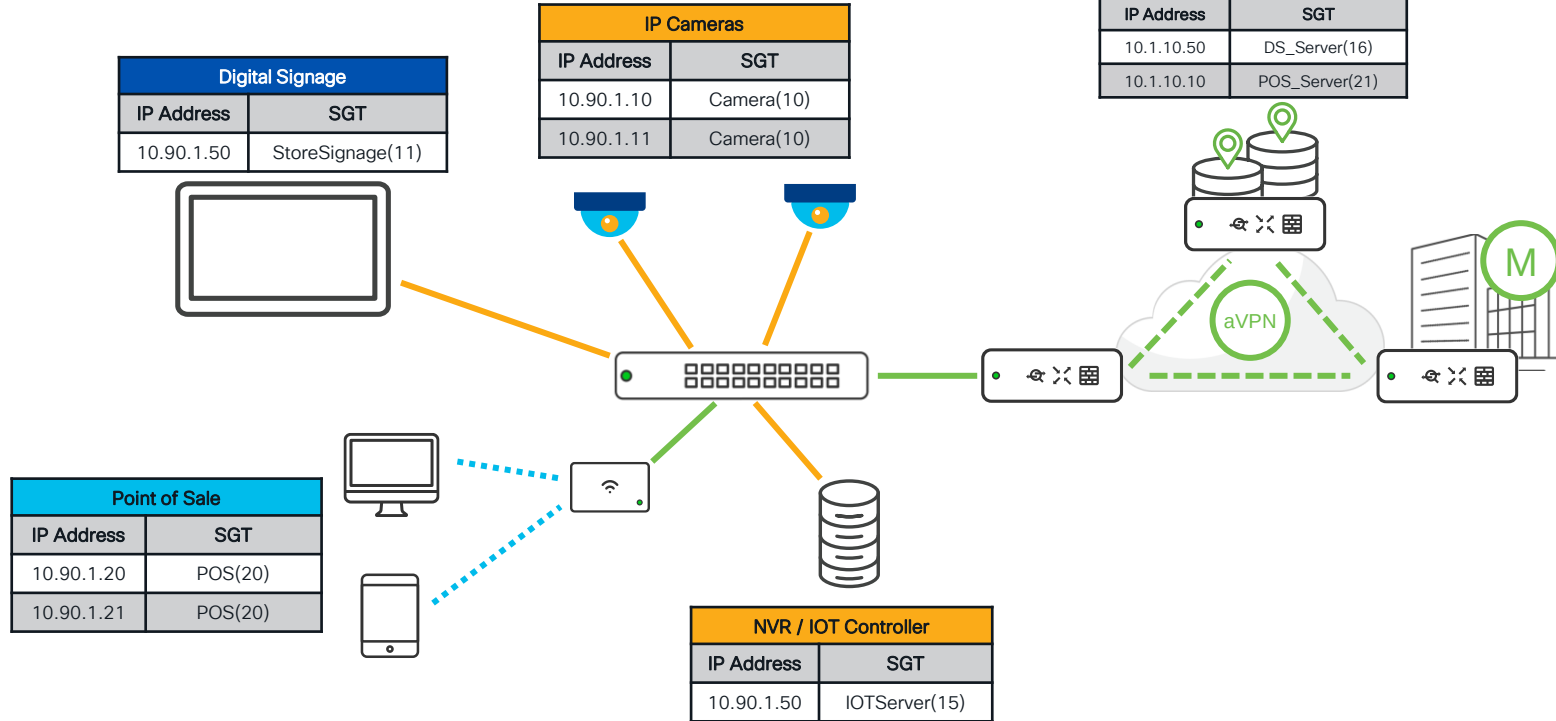
SRC DST	Employee	IoT	IoT Server
Employee	✓	✗	✓
IoT	✗	✗	✓
IoT Server	✓	✓	✓

adaptivePolicy/
__ groups
__ acls
__ bindings
__ settings

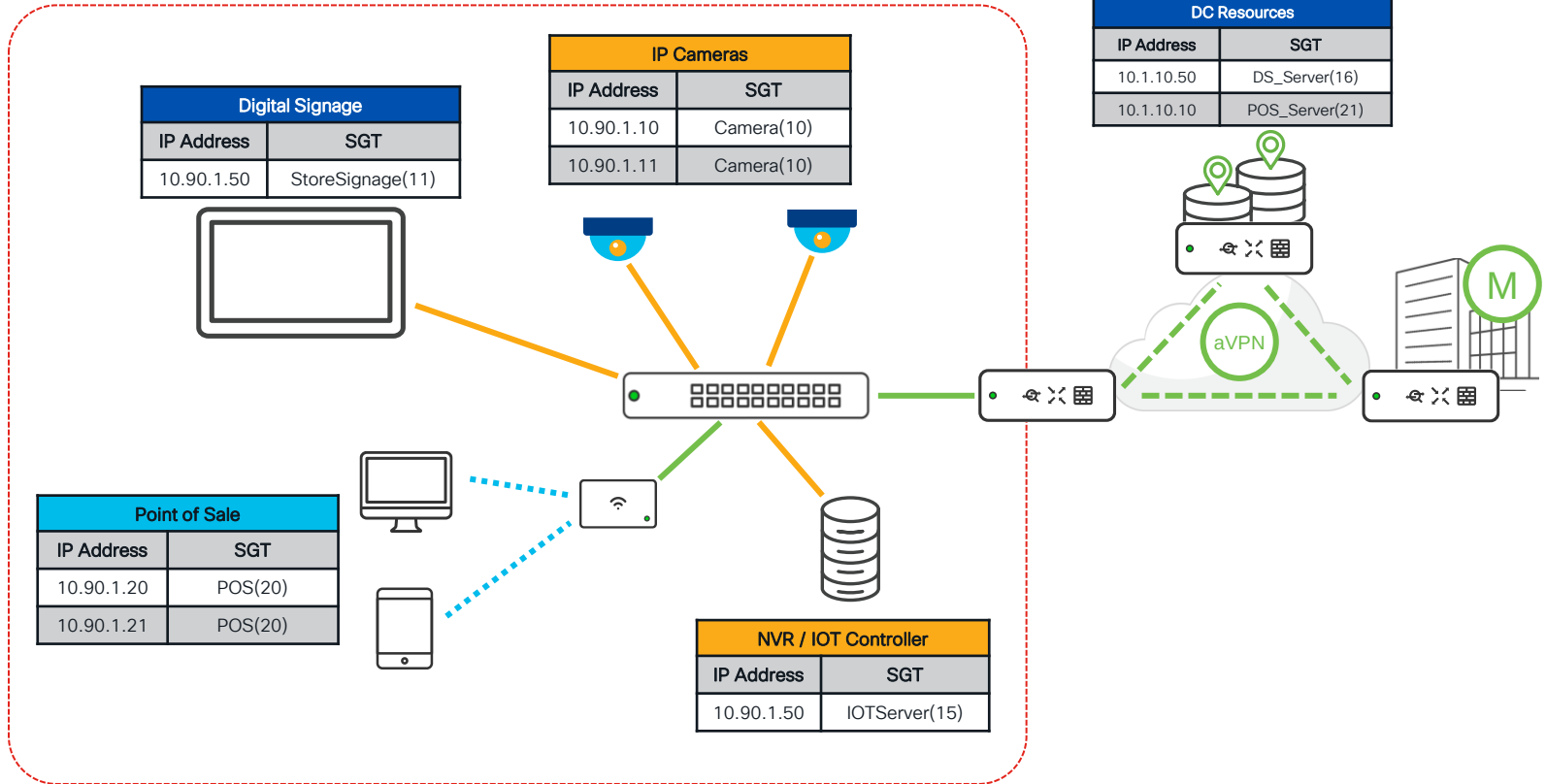


Policy Definition and Management

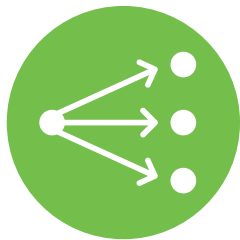
A Single Retail Location



Scope of Policy

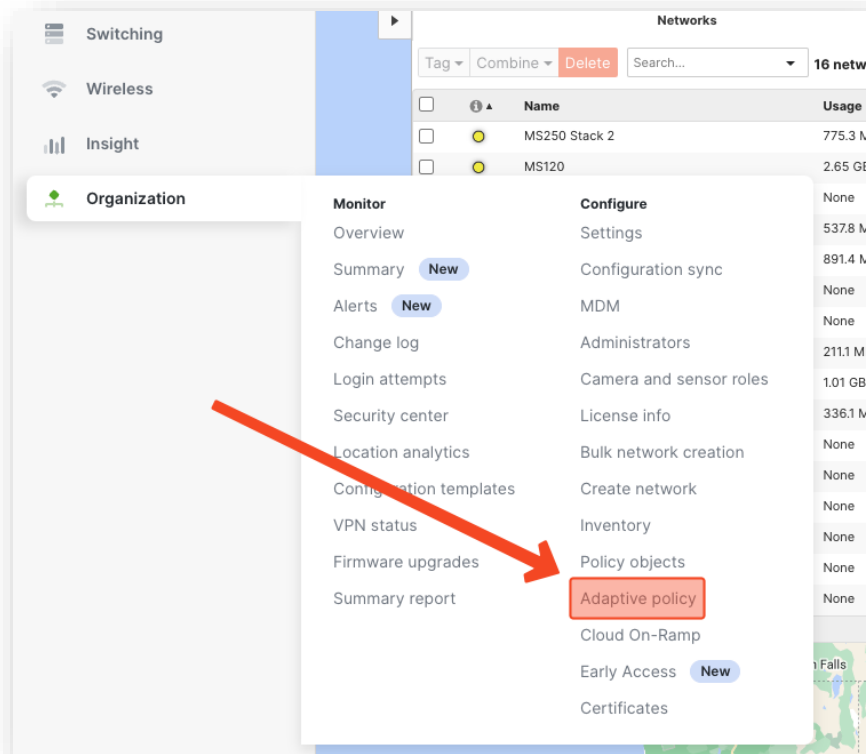


Adaptive Policy – Org Level Functions



Create Adaptive Policy

- Groups (SGTs)
- CustomACLs (SGACLs)
- Policies
- Network Enablement



Creating Adaptive Policy Groups (SGTs)

Define groups based on classifications of endpoints where policy will be shared

Example Groups:

- Employee-Compliant
- Employee-NonCompliant
- IOT
- Web-Server
- Network-Services
- Guest
- Employee-BYOD
- PCI-Server
- PCI-Endpoint

Adaptive policy

Policies Groups Custom ACLs Networks

Search... 16 groups **Add group** Edit Delete

☐	Name	SGT Value	Description	Policy Objects

Created by Meraki, the

Add adaptive policy group

Name: SomeGroupName

SGT Value ⓘ: 1010

Description: A useful description of this group

Policy Object Binding ⓘ:

Review changes

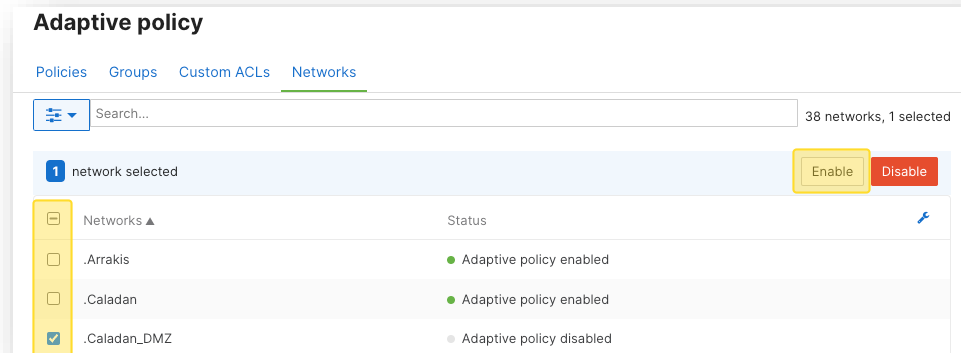
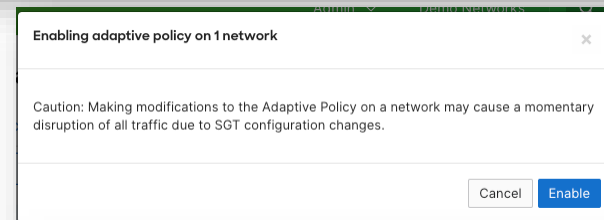
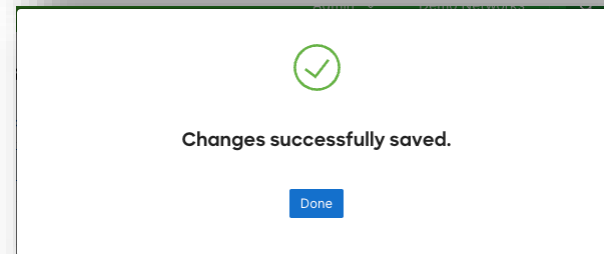
Enabling Adaptive Policy on a Meraki Network

Adaptive Policy is enabled on a per-network basis via **Organization > Adaptive policy > Networks**

Validation requirements:

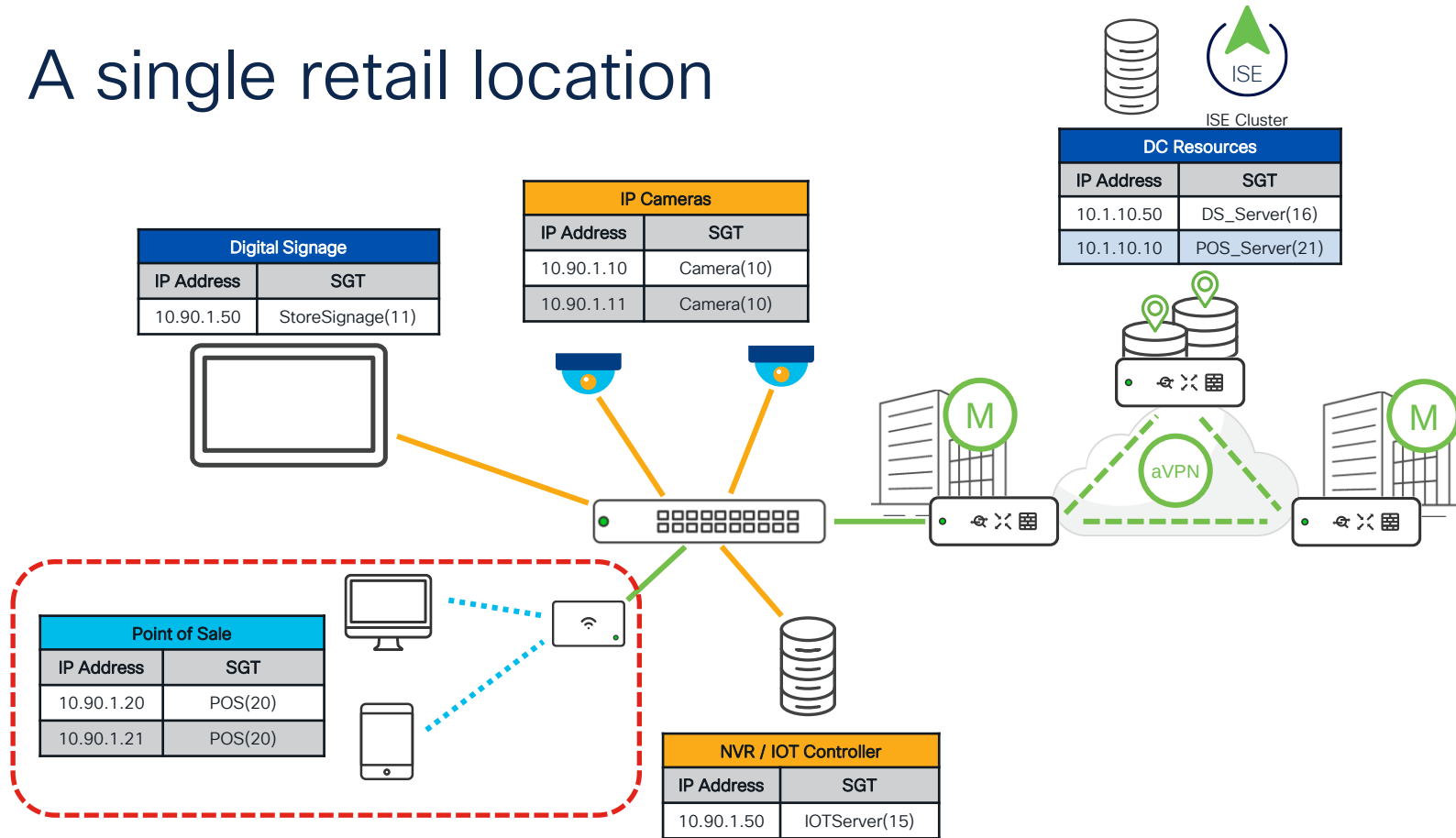
Hardware is supported and on req min firmware
MS390/MS130**/9300 is Advanced licensed
MR is Advanced licensed
MX is at least Advanced Security licensed

***Support coming in a later release for MS130 X/R*



Creating Groups and Enabling Networks Demo

A single retail location



SGT Assignment by SSID

SSID default/fallback SGT assignment

Support

- SSIDs in bridge-mode and NAT mode
- Default tag if RADIUS assignment is not performed
- Can be overridden with a RADIUS based SGT assignment

Use cases

- Single Use SSIDs (like guest)
- iPSK w/RADIUS fallback
- 802.1X fallback assignment
- MAC Auth fallback assignment

VLAN tagging ⓘ

VLAN ID

#	Access point tags	VLAN ID
	Default	<input type="text" value="101"/>

[+ Add VLAN ID](#)

Assign group policies by device type

Adaptive policy group

Bridge mode and NAT mode only

SGT Assignment by RADIUS

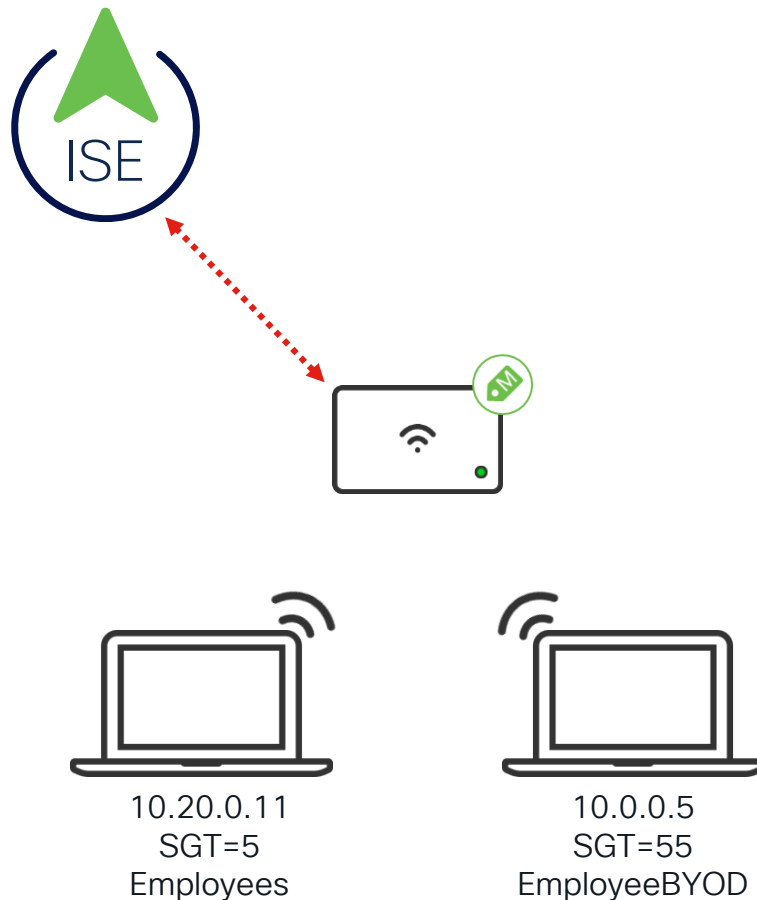
Per-Session Assignment of SGTs

Support

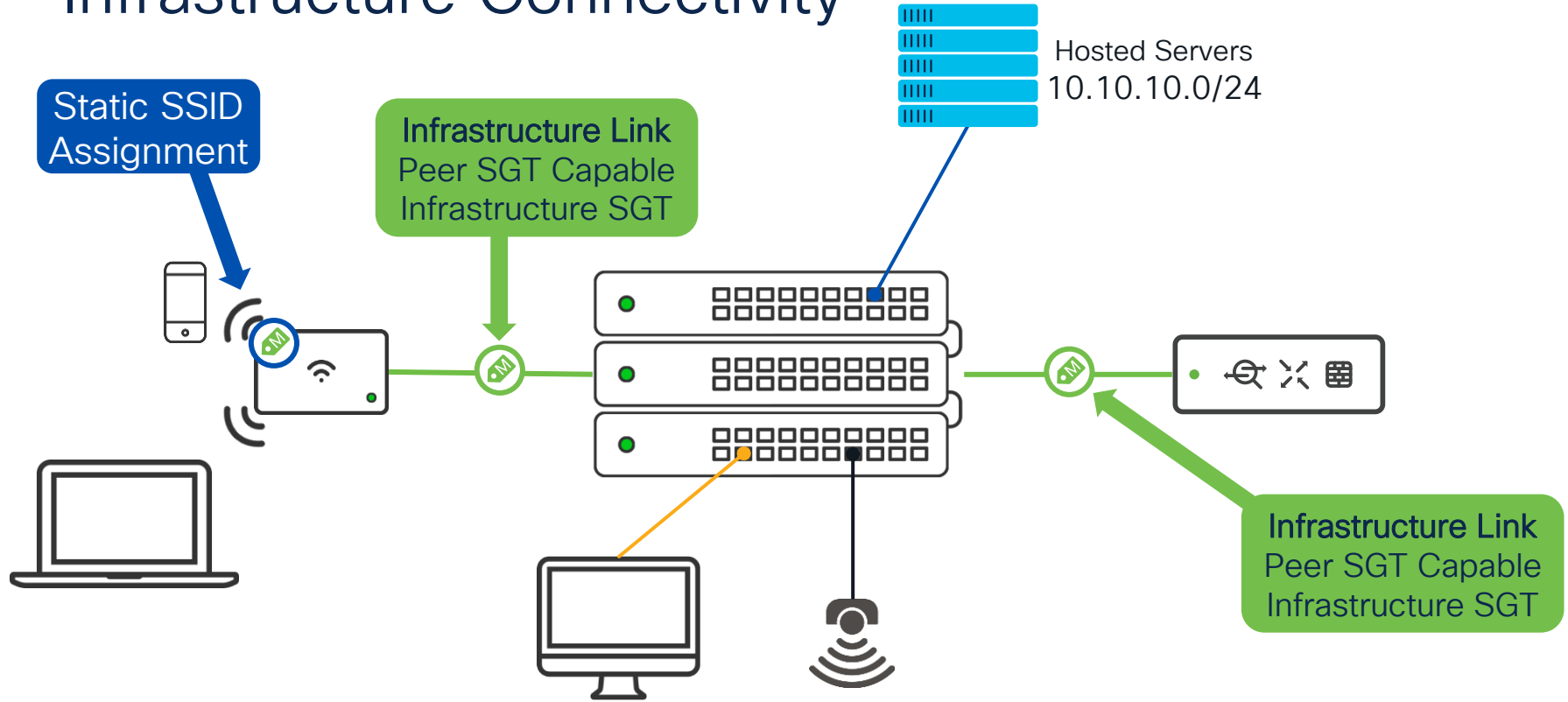
- SSIDs in bridge-mode and NAT mode
- Fallback to SSID's SGT if RADIUS does not send SGT

Use cases

- WPA2/3 Enterprise Wireless Deployments
- iPSK w/RADIUS
- Central Web-Auth (MAC Auth – URL Redirect)
- Open Auth w/ MAC Auth

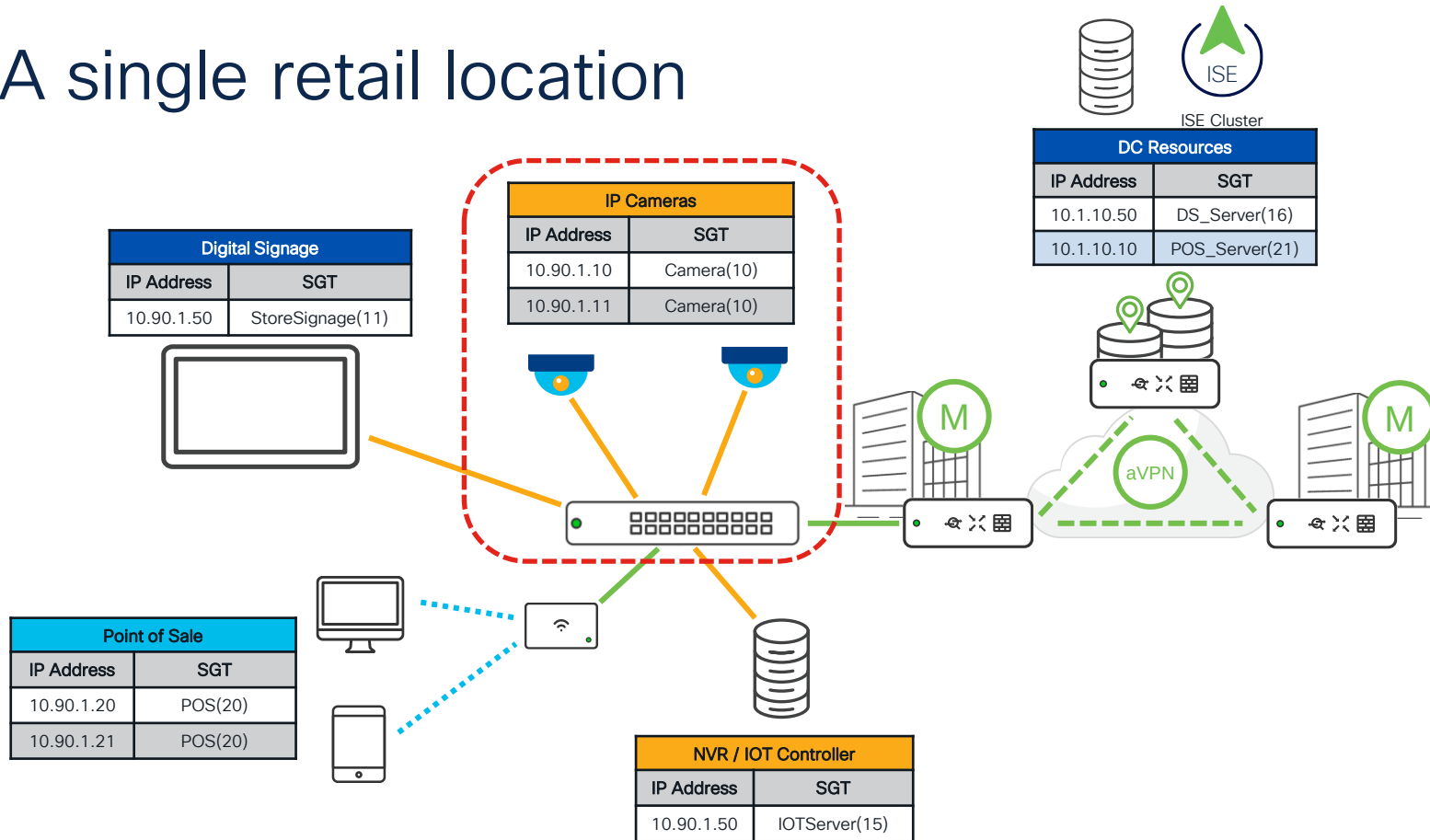


Infrastructure Connectivity



Infrastructure Links and Wireless Classification Demo

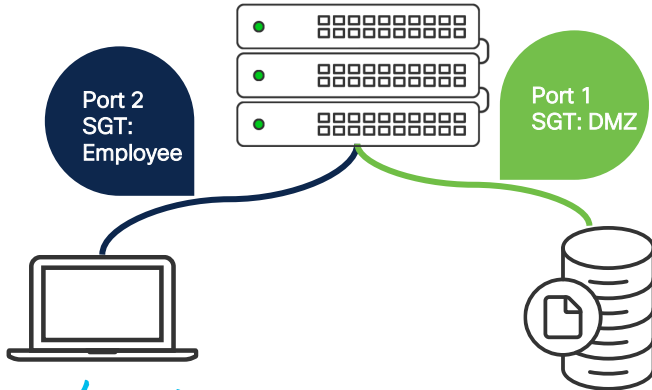
A single retail location



MS/CS Static Port to SGT Assignment

Static SGT classification based on physical port

- Supported on Access and Trunk ports
- Classifies all devices and traffic behind the port with the configured SGT



Update 1 port

Trunk **Access**

Access policy ⓘ Open

VLAN 2000

Voice VLAN 2

RSTP **Enabled** Disabled

STP guard Disabled

Port isolation Enabled **Disabled**

Trusted DAI Enabled **Disabled**

UDLD **Alert only** Enforce

Alerts will be generated if UDLD detects an error, but the port will not be shut down.

PoE **Enabled** Disabled

Adaptive policy group 4: GeneralData

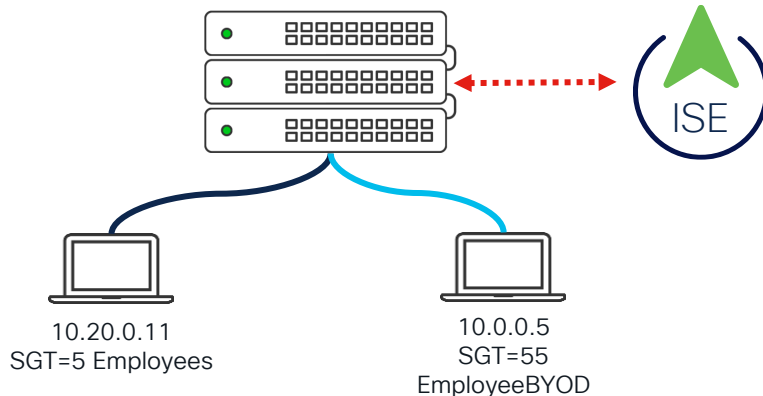
Storm control **Enabled** Disabled

Cancel Update

MS/CS RADIUS SGT Assignment

RADIUS Assignment

- Supported on Access ports
- SGT Assignment done by RADIUS and not by Static Port SGT
 - Fallback mapping done by Static Subnet to SGT or *VLAN to SGT



Update 1 port

Tags: +

Type: Trunk **Access**

Access policy ⓘ ISE_MD_Crit

VLAN 2000

Voice VLAN 2

RSTP **Enabled** Disabled

STP guard Disabled

Port isolation **Enabled** Disabled

UDLD **Alert only** Enforce

Alerts will be generated if UDLD detects an error, but the port will not be shut down.

PoE **Enabled** Disabled

Adaptive policy group ⓘ Select...

Storm control **Enabled** Disabled

Cancel Update

Switchport Classification Demo

Example Policy

Source / Destination	Unknown (0)	POS (20)	Camera (10)	Employee (4)	POS_Server (21)	IOT_Server (15)
Unknown (0)	Permit	Deny	Deny	Permit	Deny	Deny
POS (20)	Deny	Deny	Deny	Deny	Permit	Deny
Camera (10)	Deny	Deny	Deny	Deny	Deny	Permit
Employee (4)	Permit	Deny	Deny	Deny	Deny	Deny
POS_Server (21)	Deny	Permit	Deny	Deny	Permit	Deny
IOT_Server (15)	Deny	Deny	Permit	Deny	Deny	Permit

Creating Policies between SGTs

Policies are defined in a single direction of source group to destination group

- Overview of Explicit Policies Currently Defined
- Filterable by text or by the filter drop down
- Visibility into last policy update
- High level Overview of Total defined policies, groups, and ACLs

Adaptive policy

Policies Groups Custom ACLs Networks

Add a new policy

TOTAL POLICIES
121

DENY POLICIES
10 /121

ALLOW POLICIES
54 /121

GROUPS
48

ACLs
22



Search...

Add Policies

1 Policy selected

Edit

Delete

Source Group	Destination Group ▲	Permission	Policy Name	Last update
☐ Quarantine	Adaptive_Dot1x_Contractor	* Custom	Quarantine - Adaptive_Dot1x_Contractor	Jun 2, 2023 16:53
☐ IOT_Device	Adaptive_Dot1x_Contractor	✓ Allow	IOT_Device - Adaptive_Dot1x_Contractor	Aug 24, 2020 14:02
☐ Quarantine	Adaptive_Dot1x_DomainAccount	* Custom	Quarantine - Adaptive_Dot1x_DomainAccount	Jun 2, 2023 16:53
☐ IOT_Device	Adaptive_Dot1x_DomainAccount	✓ Allow	IOT_Device - Adaptive_Dot1x_DomainAccount	Aug 24, 2020 14:02
☐ Quarantine	Adaptive_Dot1x_Engineer	* Custom	Quarantine - Adaptive_Dot1x_Engineer	Jun 2, 2023 16:53

One to One or One to Many

Add Policies

Source groups

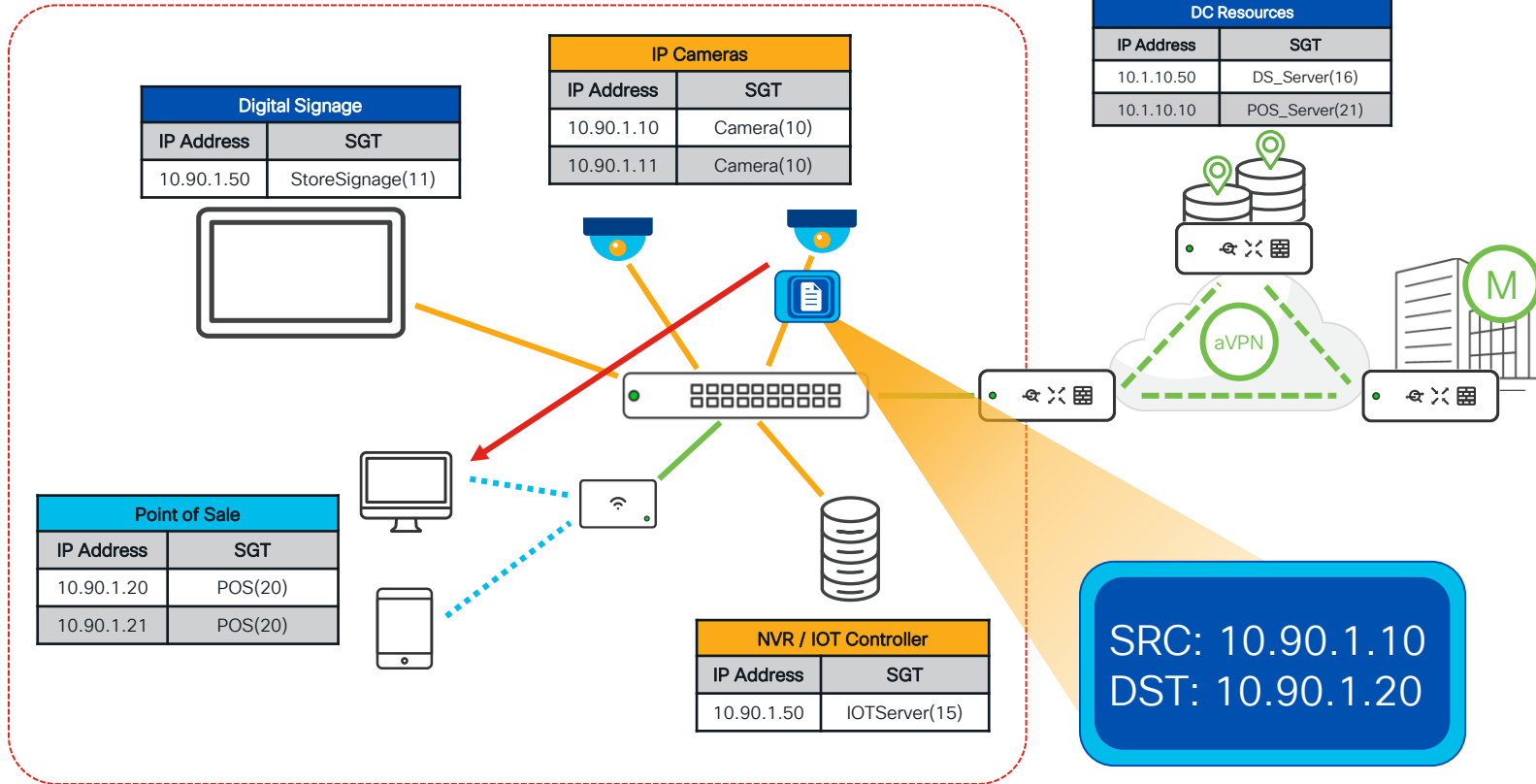
☒	Name	SGT Value ▲	Description
☒	Quarantine	563	No good

Destination groups

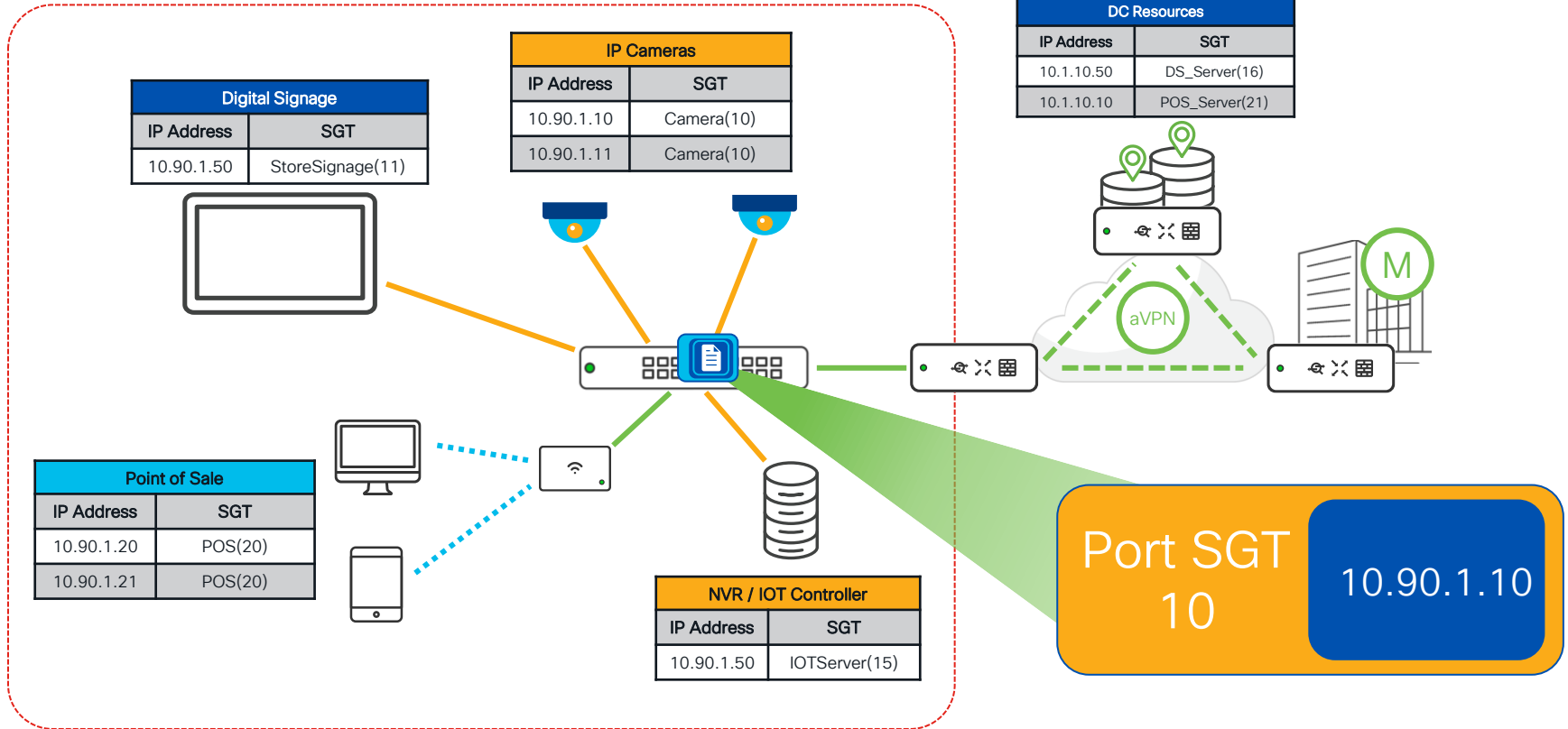
5 policies selected				☒ Allow	☒ Deny	☒ Custom	☒ Delete
☐	Name	SGT Value ▲	Description				
☐	Unknown	0	Created by Meraki, the Unknown group applies when a policy is specified for unsuccessful group classification				
☒	Infrastructure	2	Created by Meraki, the Infrastructure group is used by Meraki devices for internal and dashboard communication				
☒	GeneralData	4	Data				
☒	Media_Devices	5	Streaming and gaming devices				
☒	alex_office_tag	6	alex's office tag				
☒	alex_office_block	7	test blocking in alexs office				
☐	VoIP_Device	8	Voip Devices				
☐	Cameras	9	cameras on the network				

- Bulk editing of a single source to destination
- Bulk editing of a single source to many destinations

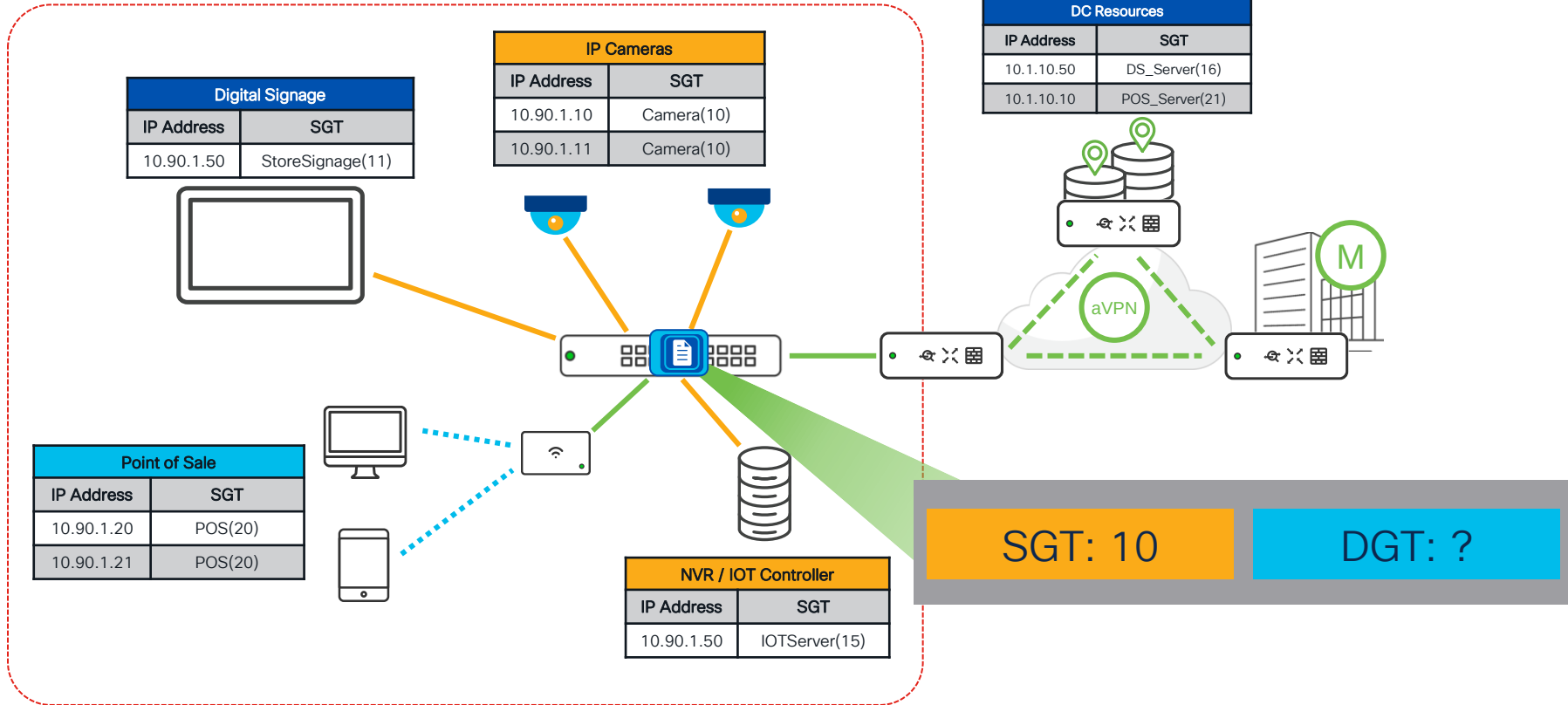
Policy Enforcement Flow



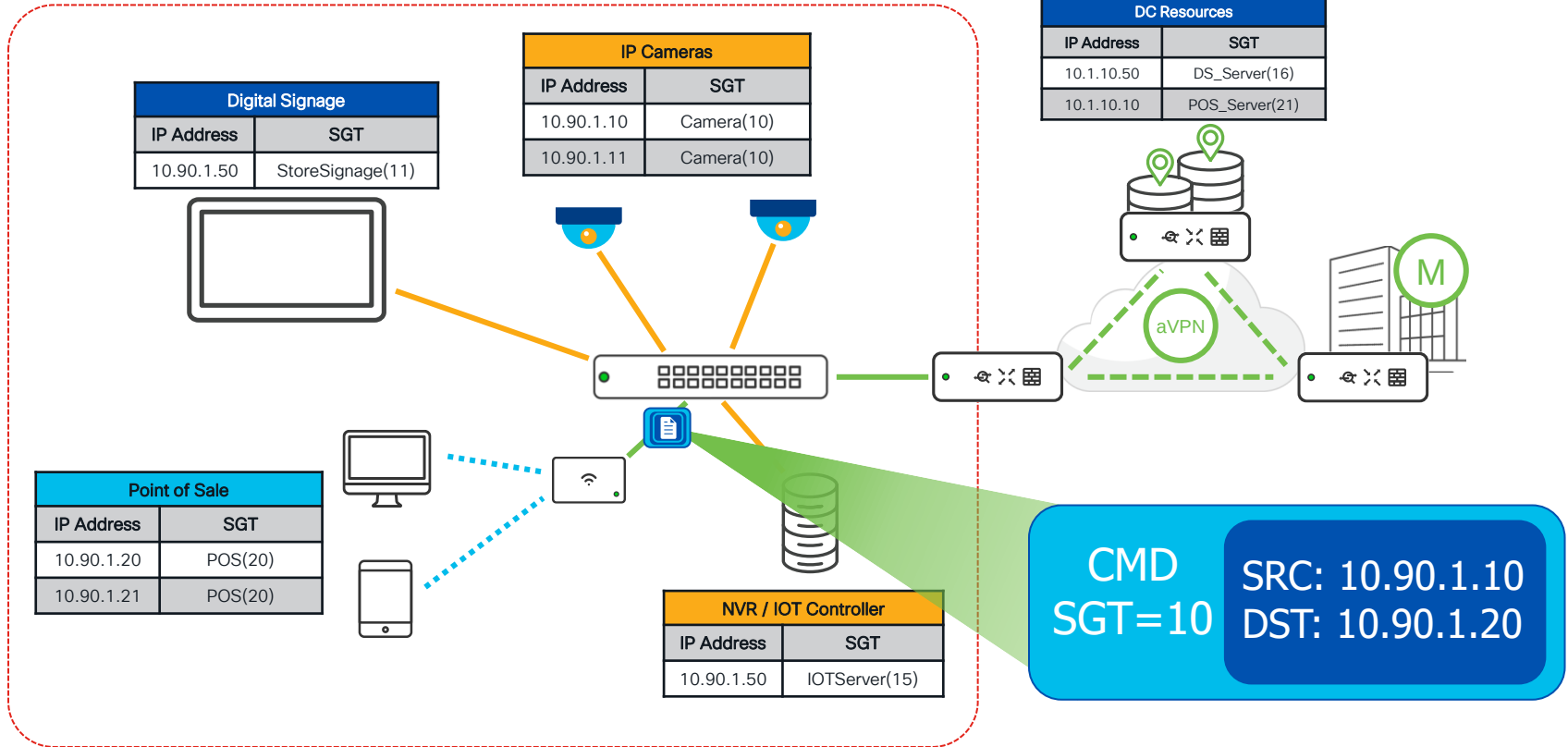
Policy Enforcement Flow



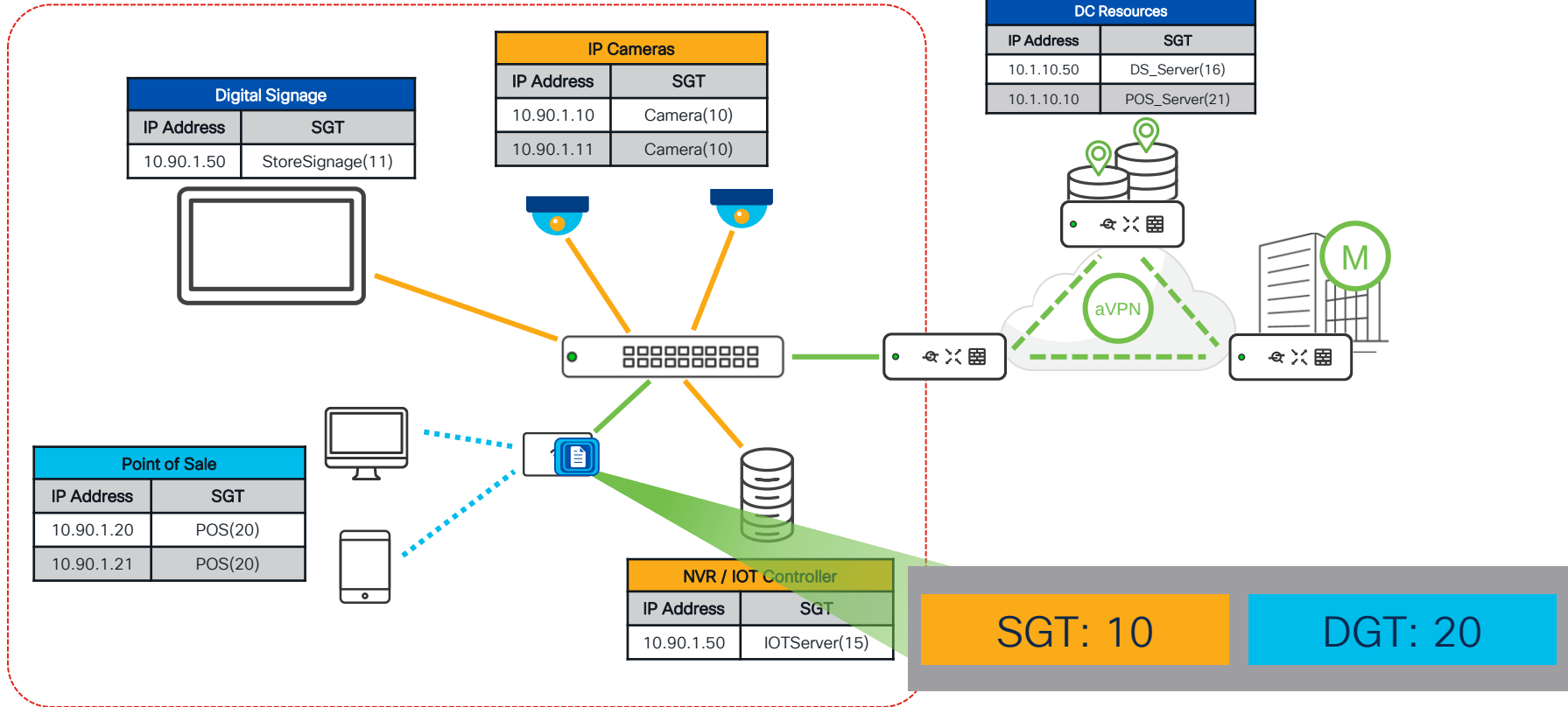
Policy Enforcement Flow



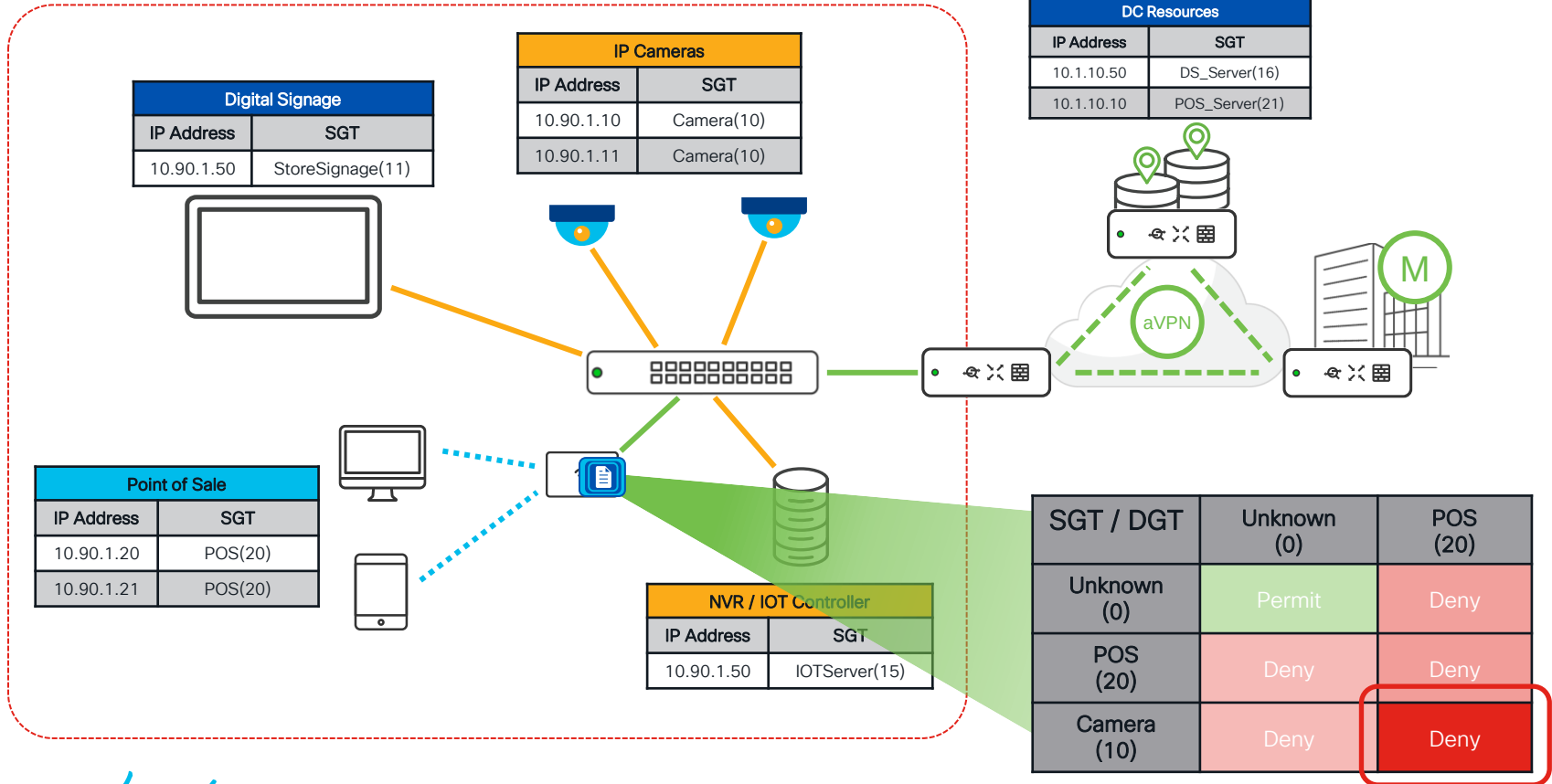
Policy Enforcement Flow



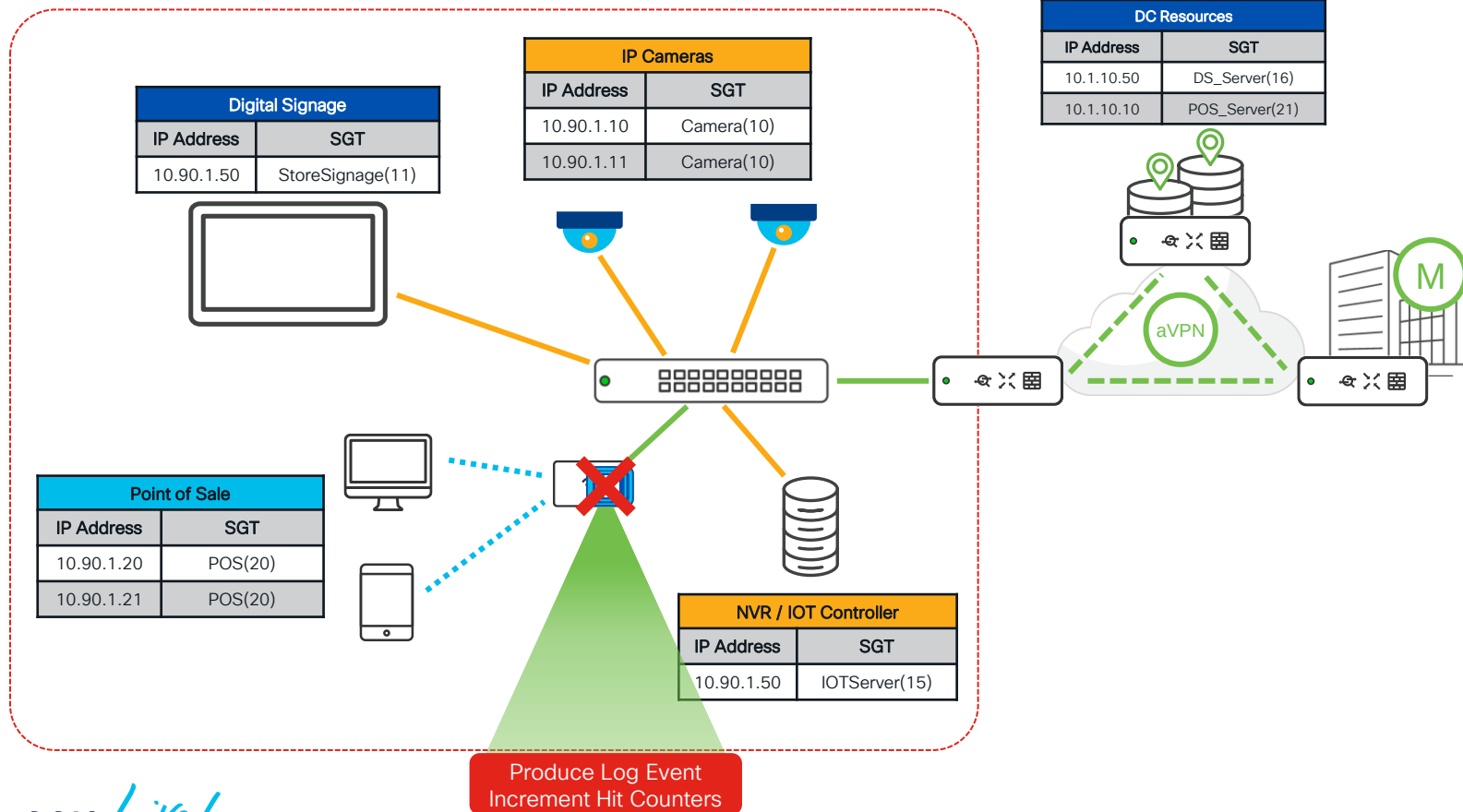
Policy Enforcement Flow



Policy Enforcement Flow

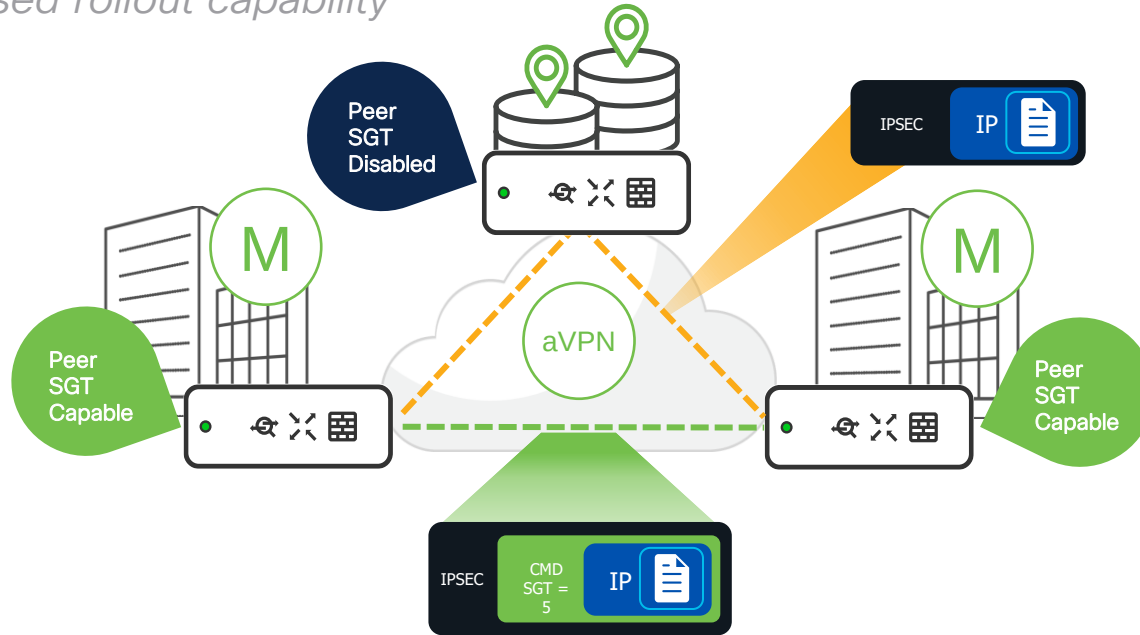


Policy Enforcement Flow



Expanding the policy scope beyond a site

A simple phased rollout capability



- Sites with Adaptive Policy enabled will propagate SGTs to like peers
- Sites without Adaptive Policy enabled will still be able to communicate with the AutoVPN topology
 - Sites enabled will strip the header to non capable peers

AutoVPN Propagation + Preservation

Enabling SGT Propagation and Preservation over AutoVPN takes 3 steps

Step 1: Configure VLAN support on MX

Step 2: Set Site-to-Site VPN to Peer SGT capable

Step 3: Convert downlink to Trunk and enable Peer SGT Capable + Infrastructure SGT (when connected to a supported switch or access point)

Step 2

Tells all VPN peers it can receive SGT encapsulated traffic

Step 3

Propagates SGTs from VPN to Port Trusts incoming tagged traffic

VPN settings

Peer SGT capable ⓘ

IPv4 VPN subnet translation ⓘ

Local networks	Name	VPN mode	Subnet	Uplink
	DMZ	<input type="button" value="Disabled"/>	10.10.0.0/24	Any
	Fabric_DMZ	<input type="button" value="Enabled"/>	10.10.255.0/28	Any

Configure MX LAN ports ✕

Enabled

Type

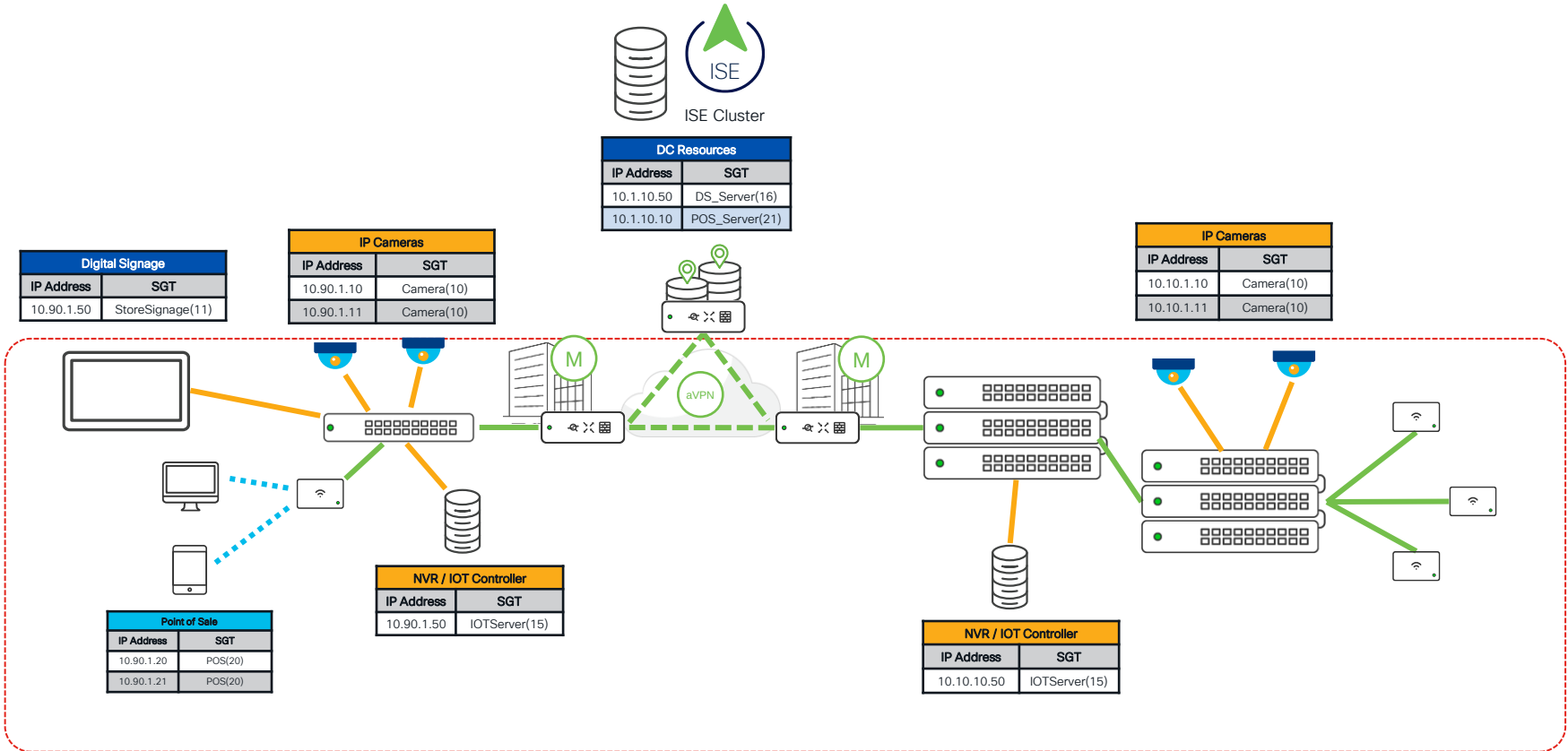
Native VLAN

Allowed VLANs

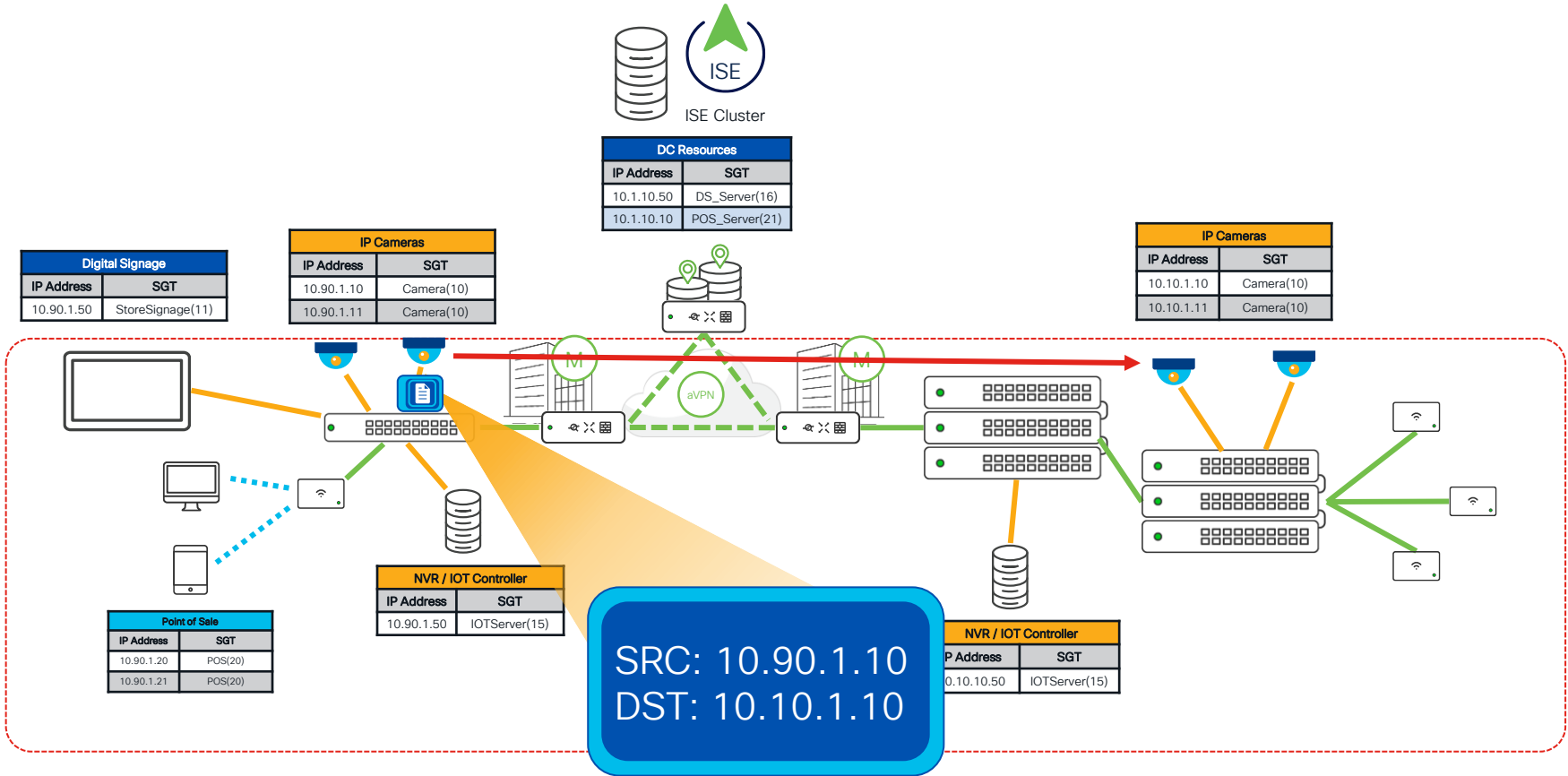
Peer SGT capable ⓘ

Adaptive policy ⓘ

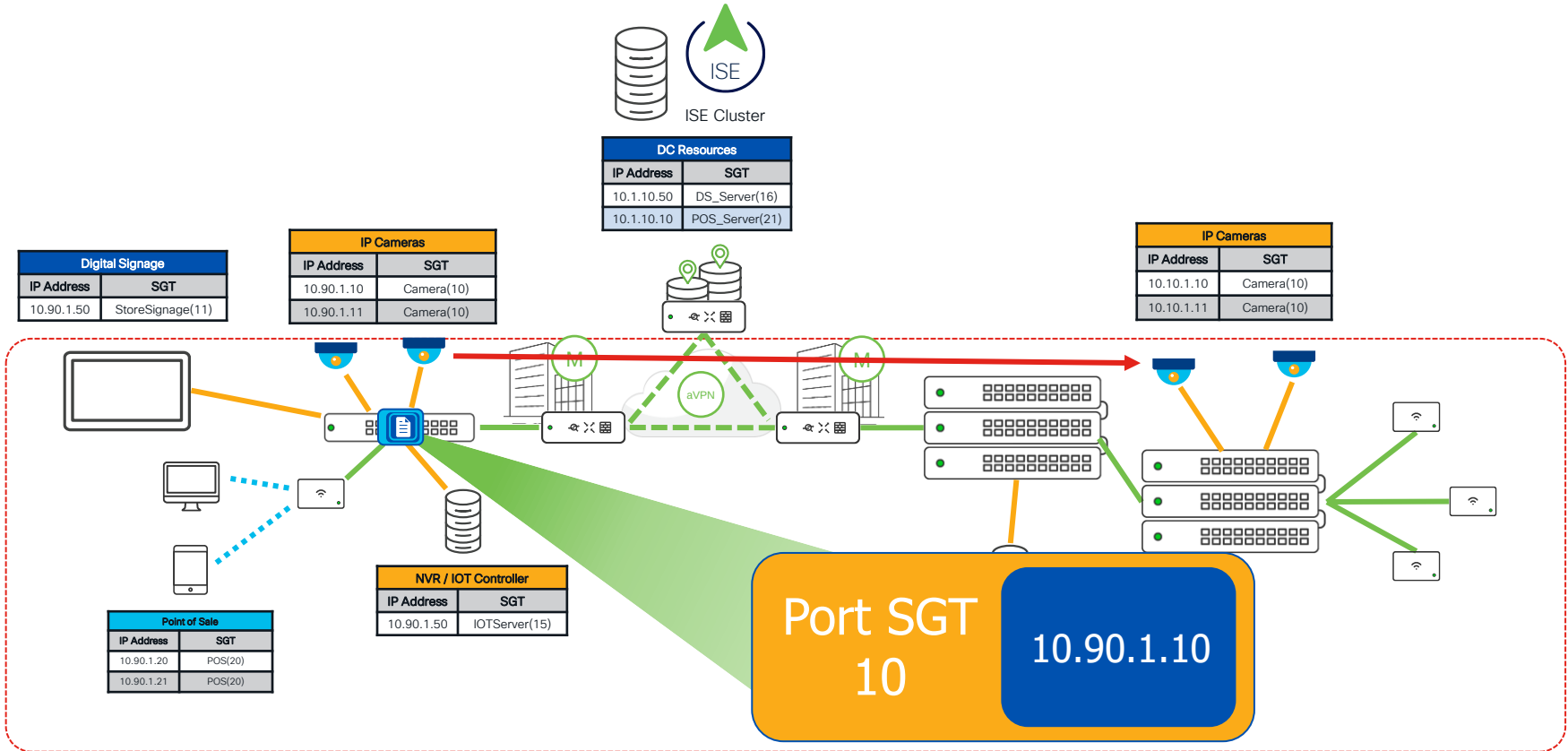
Expanding the policy scope beyond a site



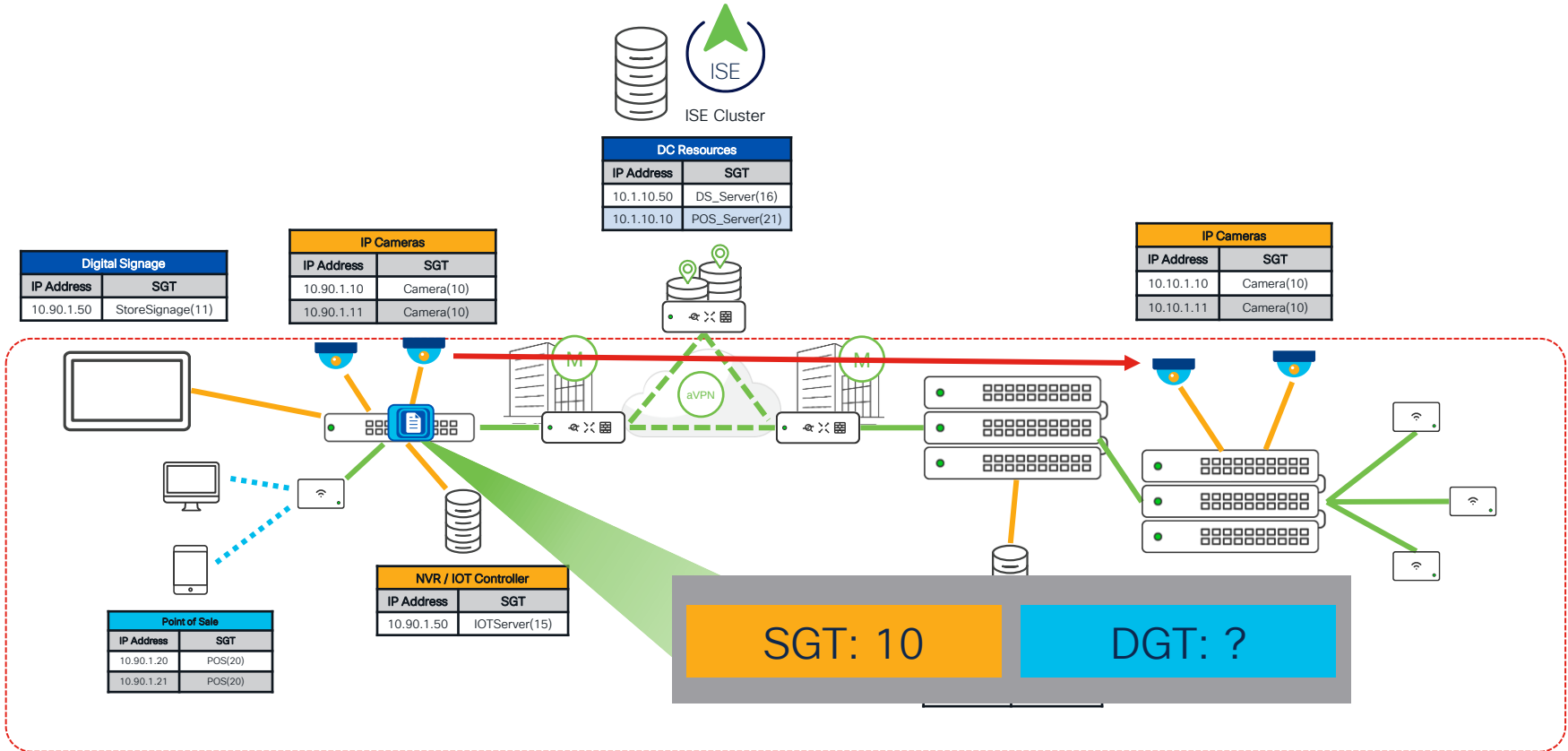
Expanding the policy scope beyond a site



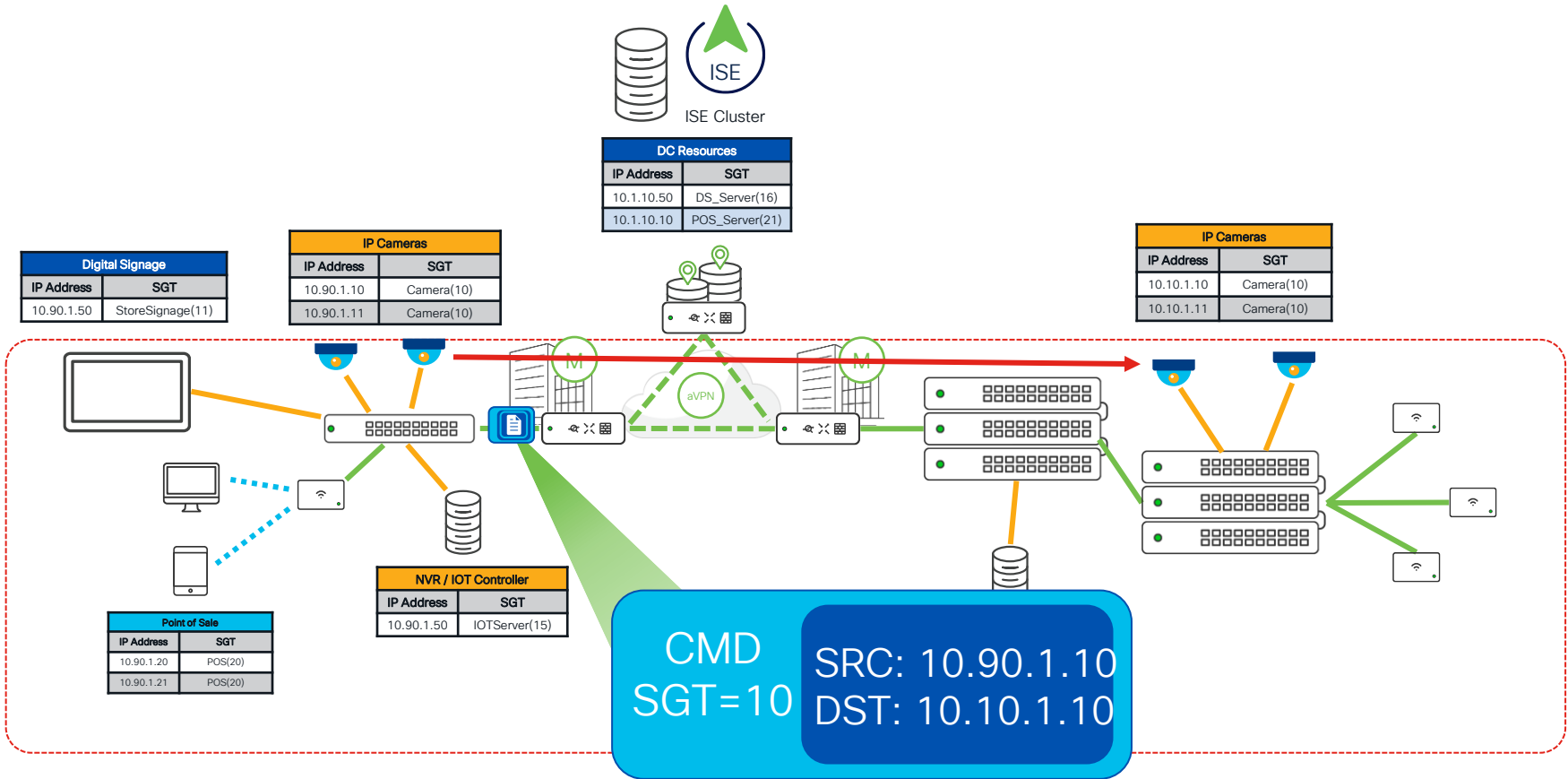
Expanding the policy scope beyond a site



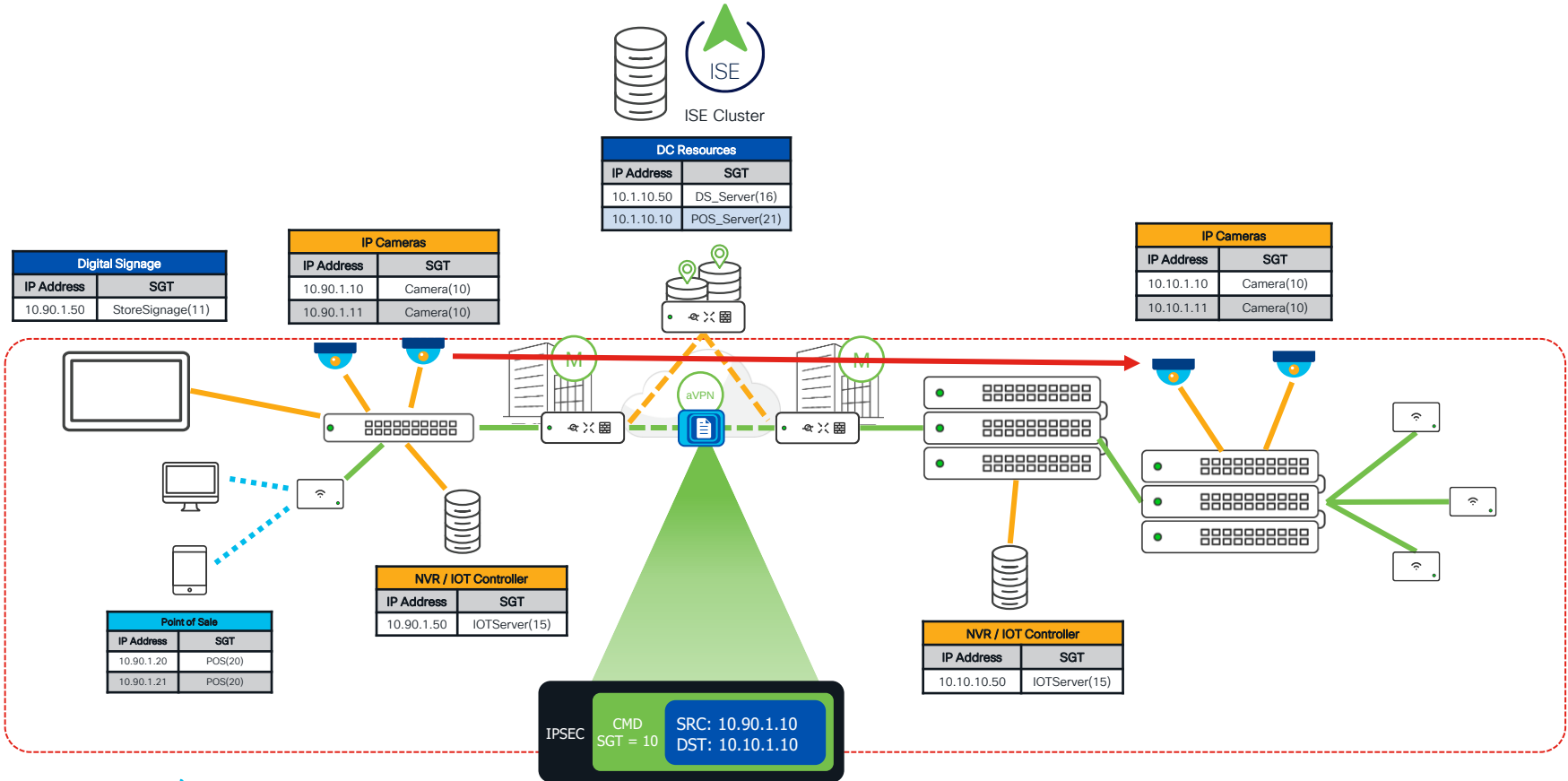
Expanding the policy scope beyond a site



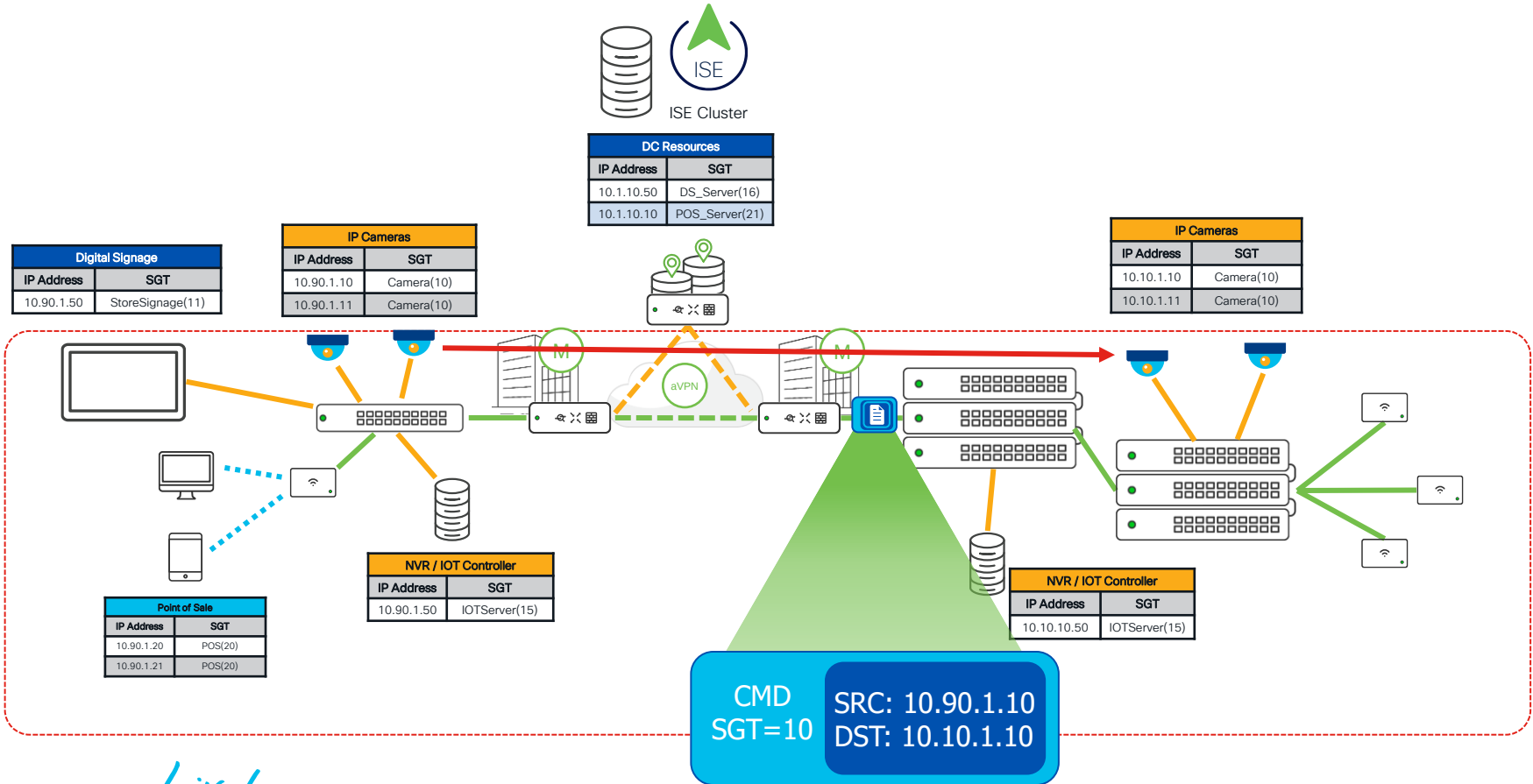
Expanding the policy scope beyond a site



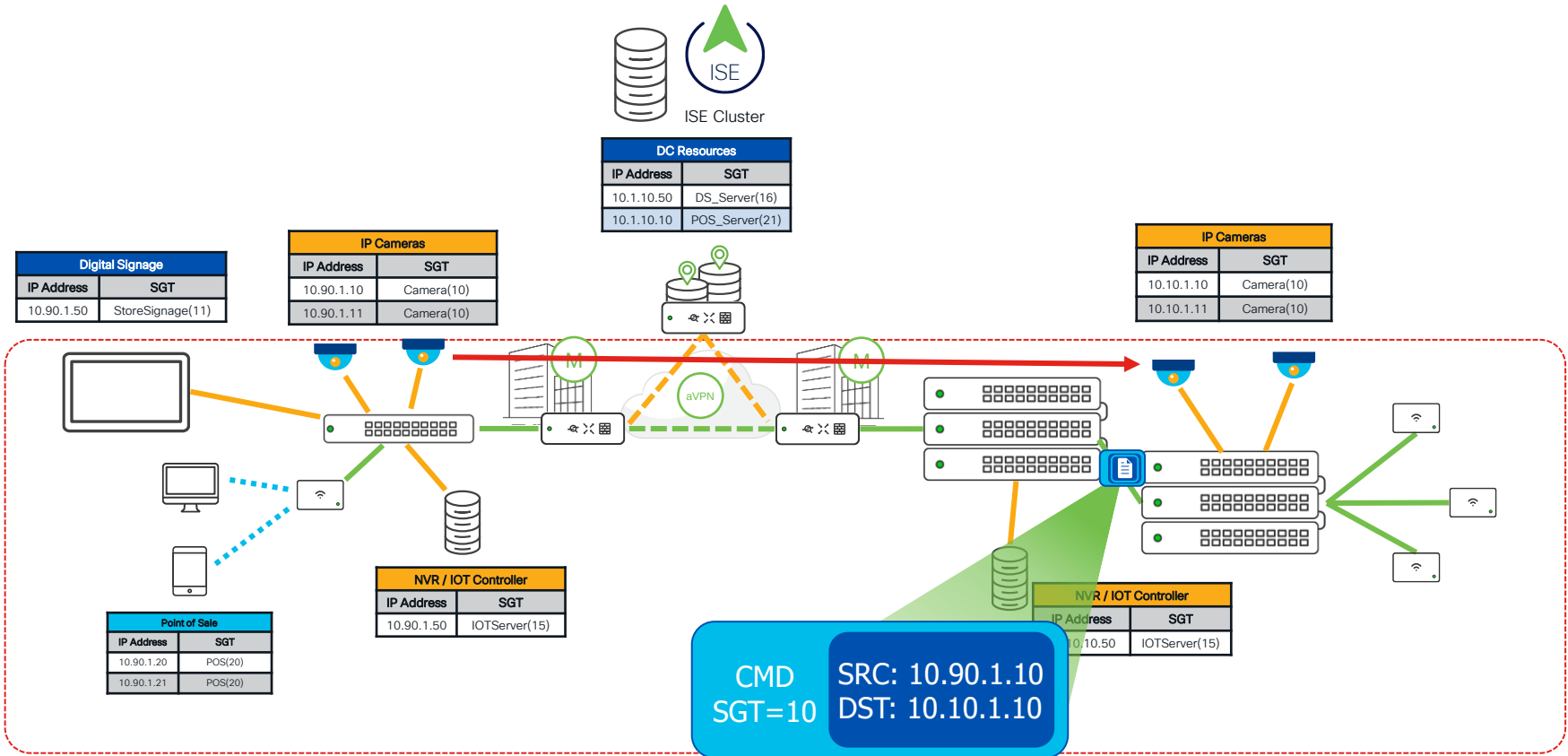
Expanding the policy scope beyond a site



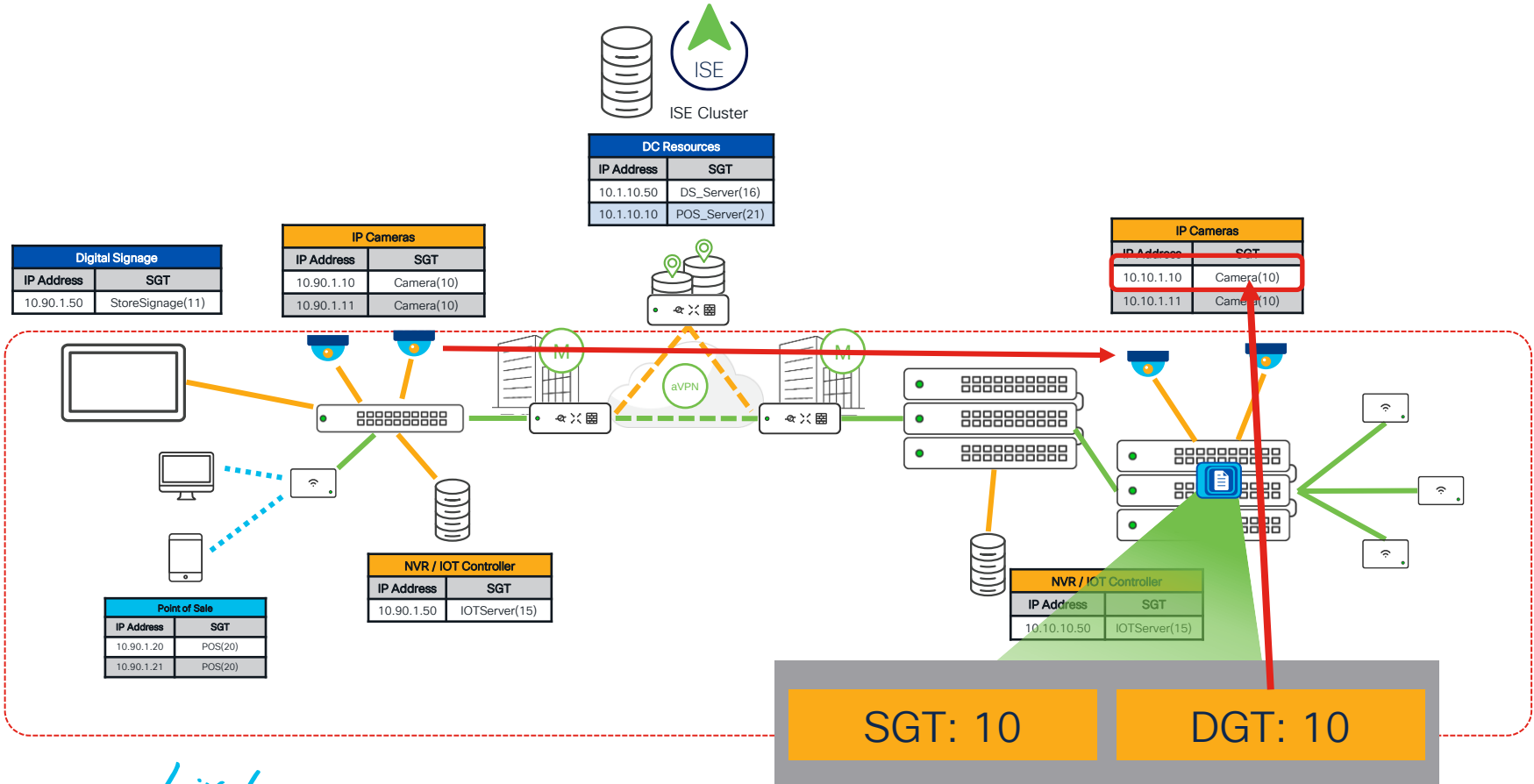
Expanding the policy scope beyond a site



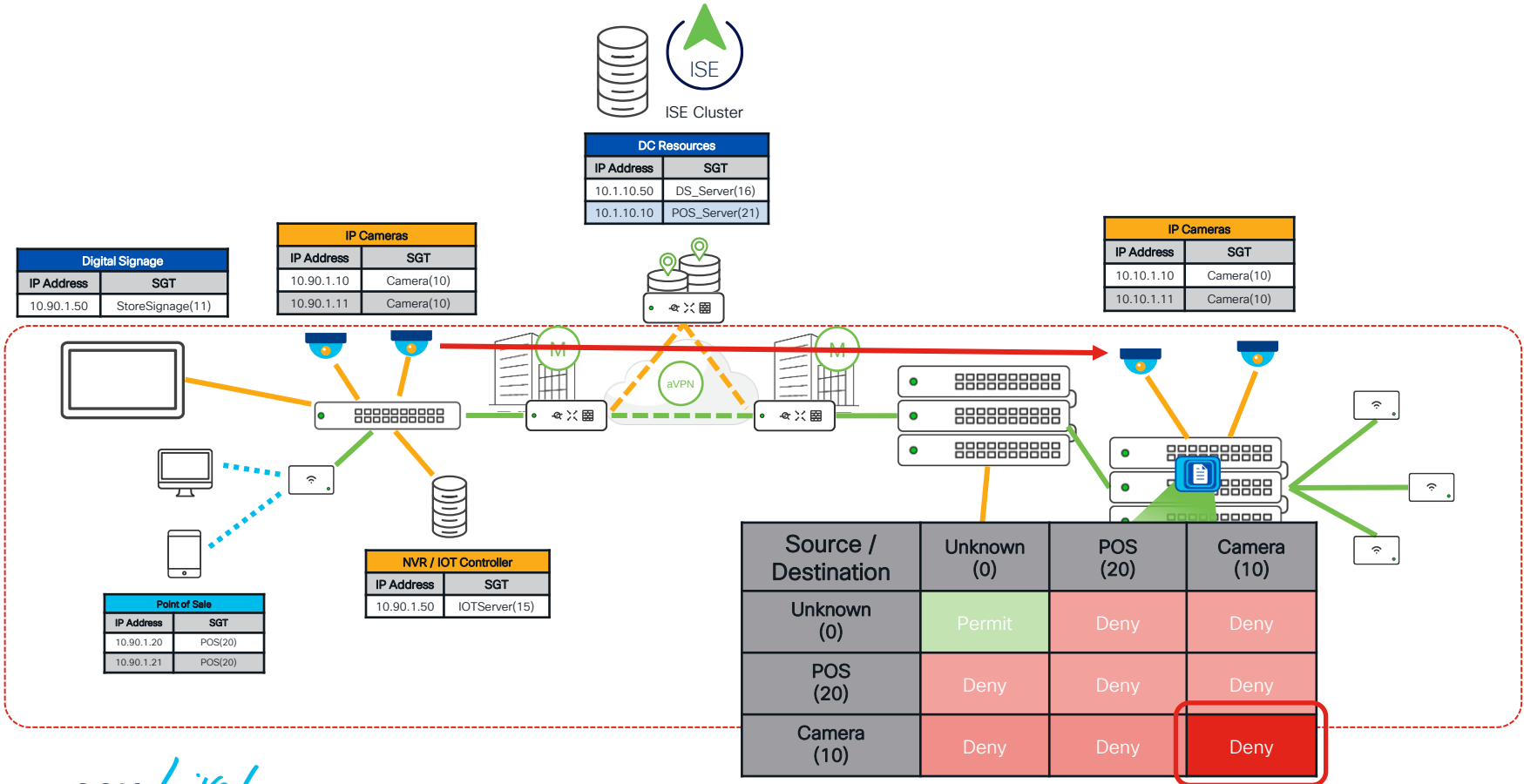
Expanding the policy scope beyond a site



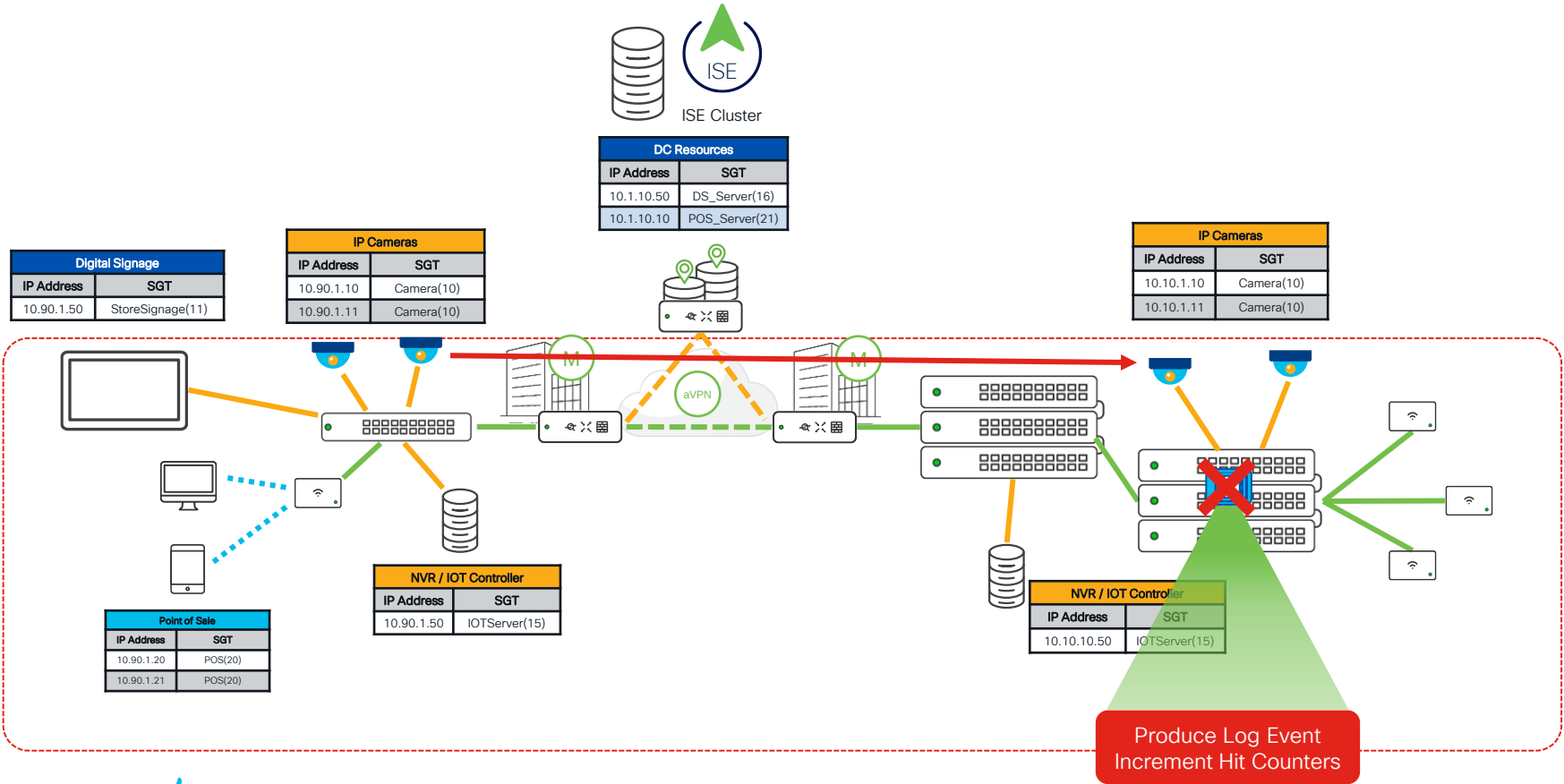
Expanding the policy scope beyond a site



Expanding the policy scope beyond a site



Expanding the policy scope beyond a site



Policy is a constantly evolving definition

Source / Destination	Unknown (0)	POS (20)	Camera (10)	IOT_Device (11)	DigitalSignage(12)	Employee (4)	POS_Server (21)	IOT_Server (15)	DS_Server (16)
Unknown (0)	Permit	Deny	Deny	Deny	Deny	Permit	Deny	Deny	Deny
POS (20)	Deny	Deny	Deny	Deny	Deny	Deny	Permit	Deny	Deny
Camera (10)	Deny	Deny	Deny	Deny	Deny	Deny	Deny	Permit	Deny
IOT_Device (11)	Deny	Deny	Deny	Deny	Deny	Deny	Deny	Permit	Deny
DigitalSignage (12)	Deny	Deny	Deny	Deny	Deny	Deny	Deny	Deny	Permit
Employee (4)	Permit	Deny	Deny	Deny	Deny	Deny	Deny	Deny	Deny
POS_Server (21)	Deny	Custom	Deny	Deny	Deny	Deny	Custom	Deny	Deny
IOT_Server (15)	Deny	Deny	Custom	Custom	Deny	Deny	Deny	Custom	Deny
DS_Server (16)	Deny	Deny	Deny	Deny	Permit	Deny	Deny	Deny	Permit

Custom ACLs (SGACLs)

An ACL that restricts and permits specific services/ranges of ports in a single direction

Functionality:

Allow / Deny
TCP/UDP/ICMP src and dst matching
TCP Established match*
Logging on hits*

Limited to 16 Entries per ACL

**Initially supported on MS390/9300-M*

The screenshot displays the 'Adaptive policy' configuration page in the Cisco Adaptive Policy Manager. The 'Custom ACLs' tab is selected, showing a list of ACLs with columns for Name, Description, IP Version, and Rules. A red box highlights the 'Add Custom ACL' button in the top right corner. Below this, the 'Add adaptive policy ACL' dialog is open, showing the configuration for a new ACL named 'No_SSH_HTTP'. The dialog includes fields for Name, Description, IP Version (set to 'Any'), and a table for Rules. The table has columns for #, Policy, Protocol, Source port, Destination port, Log, TCP Established, and Action. Two rules are listed: Rule 1 (Deny, TCP, Any, 22) and Rule 2 (Deny, TCP, Any, 80). Both rules have 'Log' and 'TCP Established' checkboxes checked. The 'Add ACL Rule' button is at the bottom of the table. The 'Cancel' and 'Create' buttons are at the bottom right of the dialog.

Adaptive policy

Policies Groups **Custom ACLs** Networks

Search... **Add Custom ACL** 21 ACLs

	Name	Description	IP Version	Rules
☐				

Add adaptive policy ACL

Name: No_SSH_HTTP

Description:

IP Version: ☒ Any ☐ IPv4 ☐ IPv6

#	Policy	Protocol	Source port	Destination port	Log	TCP Established	Action
1	Deny	TCP	Any	22	☒	☐	Cancel Done
2	Deny	TCP	Any	80	☒	☐	Cancel Done

Add ACL Rule

Cancel Create

Custom ACL Logging

Set the ACL to initiate a log event when hit, aggregated and sent on an interval

Functionality:

Logging is performed and collected over an interval and sent via Syslog (if configured) and propagated to dashboard as an event log

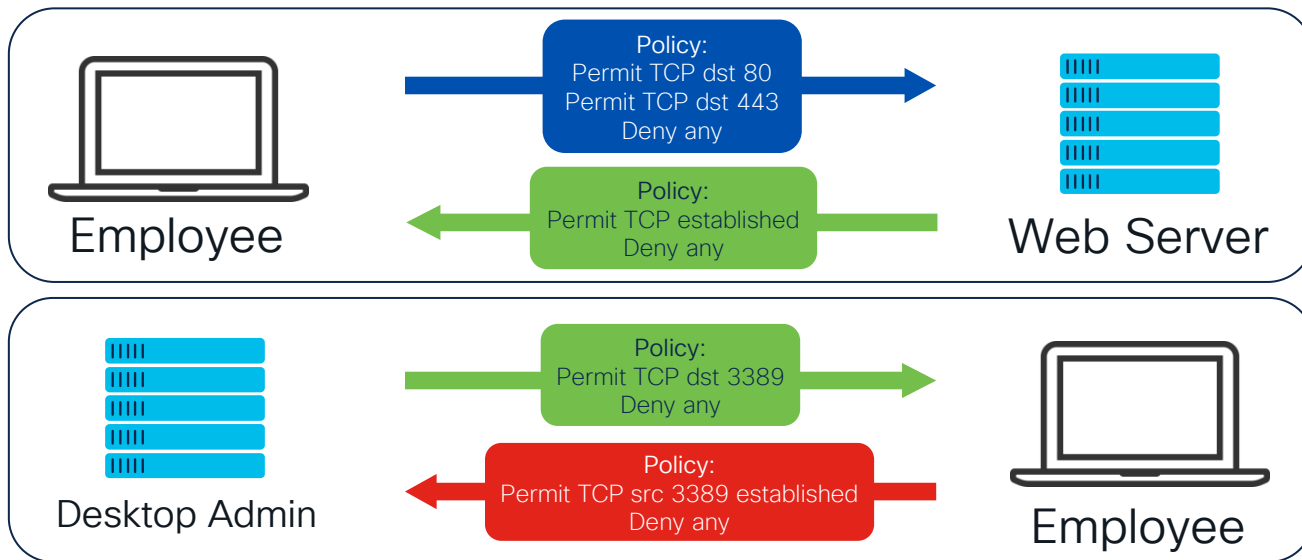
Configurable on ACE Permits and Denies as a method of capturing more detailed information on policy instantiation

#	Policy	Protocol	Source port	Destination port	Log	TCP Established		
1	Deny	TCP	Any	22	☒	☐	Cancel	Done
2	Deny	TCP	Any	80	☒	☐	Cancel	Done

Example log content:

Sep 28 15:37:46		Adaptive Policy ACL Log		port: 16, acl: Deny_IP_Log, action: Deny hide	
				protocol	icmp
				src-ip	10.39.0.102
				src-port	8
				dest-ip	10.39.0.164
				dest-port	0
				sgt	22
				dgt	21
				hits	1

TCP Established Usage in Custom ACLs



#	Policy	Protocol	Source port	Destination port	Log	TCP Established
1	✓ Allow	TCP	3389	Any	✓	✓

Part of switching CS17 release – coming to MR in MR31

Scaling Considerations



60x SGTs



3600 Policies



113 ACEs Per Policy



8000 IP to SGT Maps



**Limited by standard hardware endpoint scaling e.g. CAM tables*

Dashboard Troubleshooting Tools

Client SGT Visibility

Network-Wide Clients and Details

☐	Status ▾	Description	Adaptive Policy Group	Last seen	Usage
☐	📶	PBL-ODA6500	10: IOT_Device	Oct 5 10:22	764.6 KB
☐	📶	Korvo	4: GeneralData	Oct 5 10:22	3.48 GB
☐	📶	d4:ad:fc:93:75:64	10: IOT_Device	Oct 5 10:21	10.0 MB
☐	📶	Samsung-Refrigerator	4: GeneralData	Oct 5 10:21	1.1 MB
☐	📶	CastTV	4: GeneralData	Oct 5 10:22	53.0 MB

MS Port Live Details

Status

Connectivity 

Usage 19.6 MB (9.9 MB sent, 9.7 MB received)

Traffic 8.8 Kbps (4.0 Kbps sent, 4.8 Kbps received)

PoE usage Not drawing power

Current clients 2

Description	IP address	VLAN	MAC address	Traffic	Adaptive Policy Group	Tools
win11-template1	192.168.60.74	11	00:0c:29:28:3d:3f	65 bps (65 bps sent, - received)	7	Ping
DESKTOP-99BMF20	192.168.60.77	11	00:0c:29:48:3a:34	-	8	Ping

MR Live Client Association List

Current clients 7

Description	IP address	VLAN	MAC address	Usage	Associated for	SSID	Channel	Current channel width	Signal strength	Adaptive Policy Group	Port	Tools
MyQ-456	10.10.1.119	101	64:52:99:c8:f9:b9	1.9 MB	2 days	tsunami	6	20	 58 dB	10	—	Ping
SenseEnergyMonitor	10.10.1.50	101	70:74:14:80:37:b7	345.7 MB	2 days	tsunami	6	20	 49 dB	10	—	Ping
MyQ-450	10.10.1.160	101	64:52:99:c8:f9:b0	1.2 MB	1 day	tsunami	6	20	 58 dB	10	—	Ping

3 results per page

Troubleshooting Tools – Hit Counters

Adaptive Policy Counters

Run

AdP Hit Counters

Filter by:

Source SGT

7

Source SGT	Destination SGT	IPv4 Allow	IPv4 Deny	IPv6 Allow	IPv6 Deny
7	7	0	83	0	83
7	14	0	0	0	0
7	18	0	93	0	93

Live tool capture of hits between SGTs

Switch local data updated every 30 seconds

Hits are captured between groups when policy is explicitly defined (Allow/Deny/CustomACL)

MS/CS Support for CS16 GA

MR/CW Support for MR31 GA

Troubleshooting Tools – ACL Logging

Event log for switches ▾

Switch: Client: Before: (EDT)

Event type include: Event type ignore:

[Reset filters](#)

Download as ▾ [« newer](#) [older »](#)

Time (EDT) ▾	Switch	Switch port	Client	Category	Event type	Details
Oct 5 00:22:43	Aurora-SW1	Port 1		Adaptive Policy	Adaptive Policy ACL Log	port: 1, acl: Deny_IP_Log, action: Deny « hide protocol icmp src-ip 172.16.41.11 src-port 8 dest-ip 192.168.60.74 dest-port 0 sgt 7 dgt 7 hits 61

Interval Log Reporting on ACE Processing

Switch Collects hits over interval and reports via Syslog + Dashboard Event Log
Logs are only collected on ACEs with logging enabled

MS/CS Support for CS16 GA

MR/CW Support for MR31 GA

MX/Z Deployment and Best Practices

MX/Z Supported Models and Firmware

Models:

MX64/65/100*

MX67/68/75/85/95/105/250/450

Z3/Z4

Not supported on:

MX84

MX18.1+

NAT mode AutoVPN
Support

MX18.2+

VPNc WAN propagation
VLAN/Port SGT
Inter-VLAN Preservation

**MX19+

Enforcement and further
classification support

Licensing:

MX Advanced Licensing / SD-WAN



**only supported for AutoVPN transport in NAT mode*

*** subject to change based on release timelines for MX/Z*

[MX/Z Documentation and Support](#)

MX/Z Port to SGT classification

Static SGT classification based on physical port

- Supported on Access and Trunk ports
- Classifies all devices and traffic behind the port with the configured SGT

Support starting in MX18.2+

Configure MX LAN ports

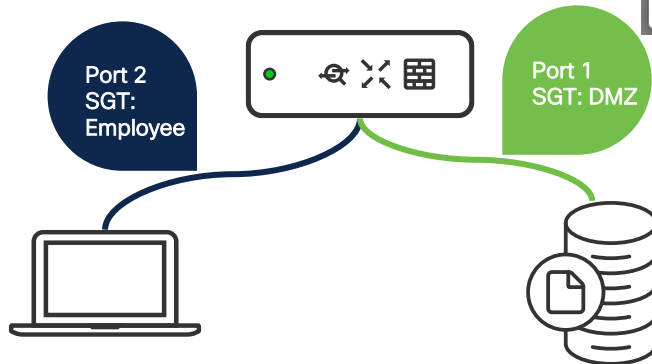
Enabled Enabled ▾

Type Access ▾

VLAN VLAN 100 (DMZ) ▾

Adaptive policy ⓘ 999: DMZ_Clients ▾

Cancel Update



MX/Z VLAN to SGT classification

Static SGT classification based on physical port

Utilized on traffic ingressing a port where:

- There is no SGT configuration defined on the port whether static or Infrastructure (Peer SGT Capable)

Support starting in MX18.2+

Modify VLAN

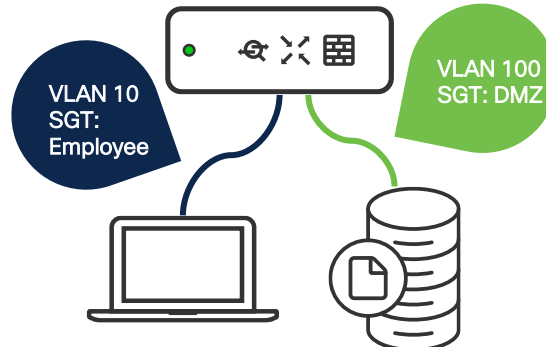
VLAN name
DMZ

VLAN ID
100

Group policy
None

Adaptive policy group
999: DMZ_Clients

Next



MS/CS Deployment and Best Practices

MS/CS Supported Models and Firmware

Models:

MS390 – All Models
C9300-M – All Models

Coming Soon:

MS130 X/R models

MS14

Initial Introduction
Port to SGT
Subnet to SGT
RADIUS assignment

CS16

Policy Hit Counters
ACL Logging

CS17

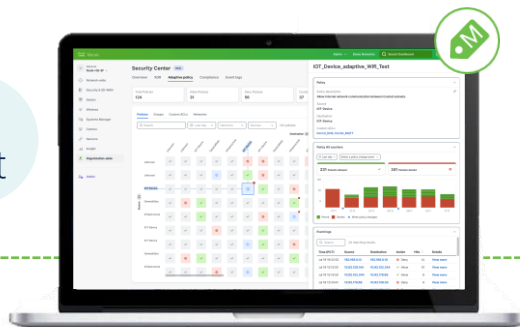
TCP Established

Licensing:

MS/CS Advanced Licensing



ONE dashboard
ANY environment



Rugged



MS130R

Compact



MS130X

Rack Mount



Most Demanding



Catalyst Meraki
9300/X

Extending **adaptive policy** to **more** platforms
No longer limited to a single MS platform

MS130X/R support coming in a future firmware release

Adaptive Policy from Access Switching to Aggregation/Core

Fiber aggregation



C9300X-12Y/24Y



C9300-24S/48S

Access



MS130X/R



MS390

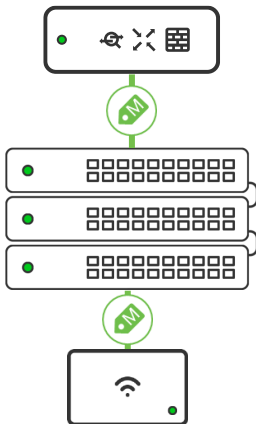


Catalyst Meraki 9300/X

MS/CS SGT Propagation

Infrastructure Propagation

- Supported on Trunk ports
- Propagates SGTs
 - Of directly assigned endpoints
 - From other SGT capable devices



Update 1 port

Type: **Trunk** Access

Native VLAN: 1

Allowed VLANs: 1-5,300-320,400-420

RSTP: **Enabled** Disabled

STP guard: Disabled

Port isolation: Enabled **Disabled**

Trusted DAI: Enabled **Disabled**

UDLD: **Alert only** Enforce

Alerts will be generated if UDLD detects an error, but the port will not be shut down.

PoE: **Enabled** Disabled

Peer SGT capable: **Enabled** Disabled

Adaptive policy group: 2: Infrastructure

Storm control: **Enabled** Disabled

Cancel Update

MS Port Configuration and Behavior

Peer SGT Capable



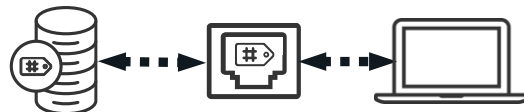
- Trust received tags/send tagged frames on **trunk** ports
- Used when connecting MS to Adaptive Policy capable MS/MR/MX

Static Tag Assignment



- Incoming traffic tagged with configured Adaptive Policy Group
- Only available on Open/MAC Allow-List ports

802.1x Assignment



- Per-Session assignment based on RADIUS response
- Static fallback performed through Prefix to SGT map or VLAN to SGT map*

**coming as part of the CS17 release*

Creating Static IP to SGT Maps

Define IP segment/s that are outside of the purview of the AdP Domain where an applicable SGT can be shared. Also called last resort classification and can be attached as an IP to SGT map

Example Segments:

- Fallback mapping
- AWS instances
- DMZ network
- Servers behind a VM environment

Create network object

Name

ScaryTerry

Type

IPv4 CIDR FQDN Adaptive Policy CIDR

FQDN, IP or CIDR

10.10.1.14/32

You can only enter one value per object.

Create object



Edit adaptive policy group

Name

Network_Services

Value

16

Description

Network Services Tag

Network Object Binding

Hamurai Morty EvilMorty ScaryTerry DC01 DC02

e.g., Branch printers Object

Cancel Update

Specifications:

- Associate a subnet to 1x SGT
- Support for any CIDR notated IP space
- Closest match wins

SGT Assignment Order of Operation



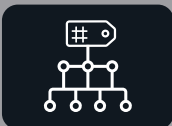
RADIUS SGT Assignment



Port SGT Assignment



IP / Subnet SGT Assignment



VLAN SGT Assignment**

MR Deployment and Best Practices

Supported Models and Firmware

Models:

Wifi5 Wave 2 (all models)
Wifi6/E MR + CW (all models)

MR27+

SSID - SGT
RADIUS based SGT
Propagation & enforcement

MR31

Group Policy + SGT
Policy Hit Counters
ACL Logging
TCP Established Matching

Licensing:

MR Advanced Licensing



[MR Adaptive Policy Documentation](#)

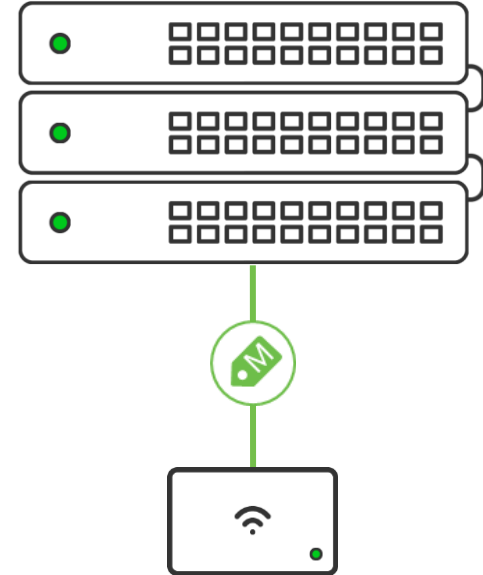
MR Adaptive Policy Enablement

Automatically tags all traffic with an SGT including management and control traffic

MR identifies CMD encapsulated traffic from MS and switches on SGT tagging (Peer SGT capable)

If no CMD encapsulation observed – Disable tagging and produce event

Provides a fail-safe for upstream SGT support

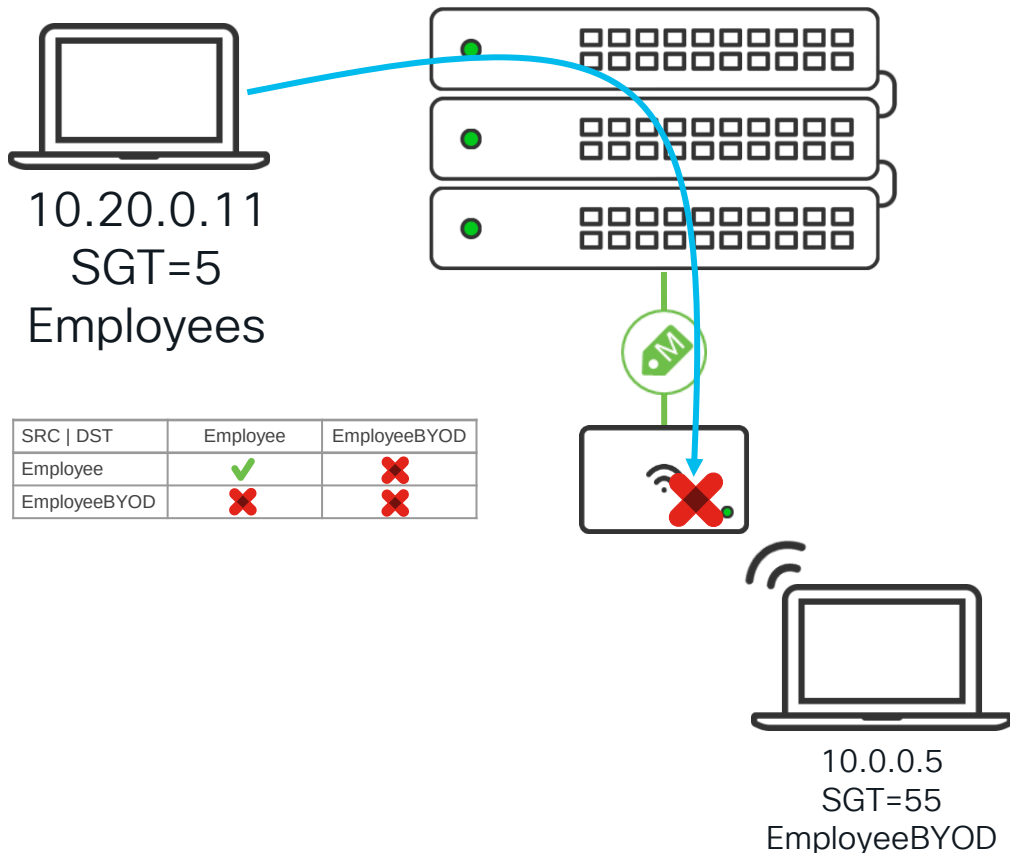


Propagation and Enforcement

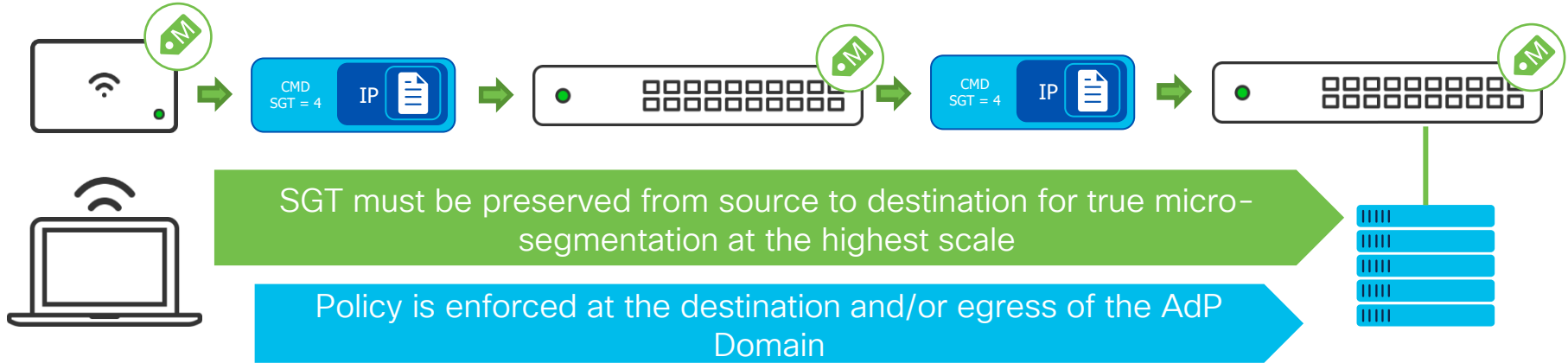
MR Policy Handling

Support

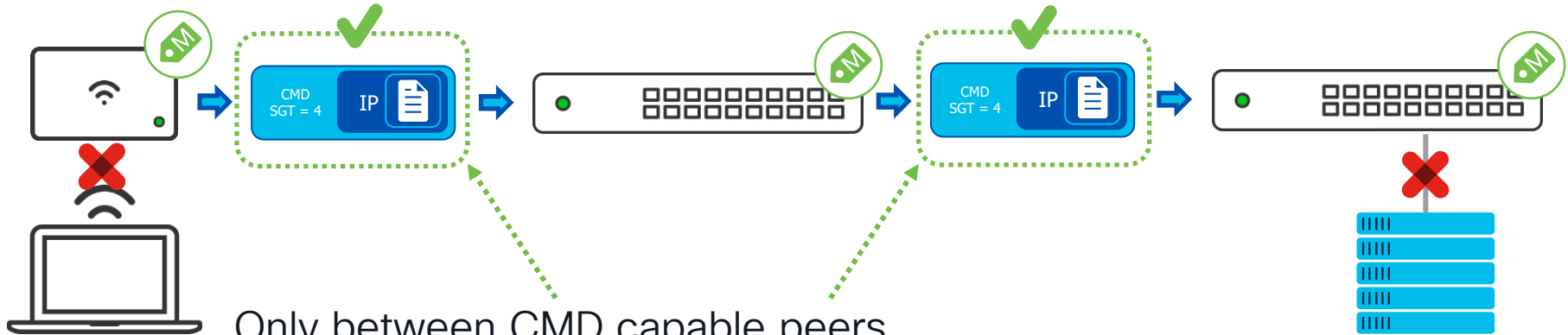
- MR enforces policy at egress (traffic to wireless client)
- MR Propagates SGTs from wireless clients to upstream network appliance



Tag Application and Preservation

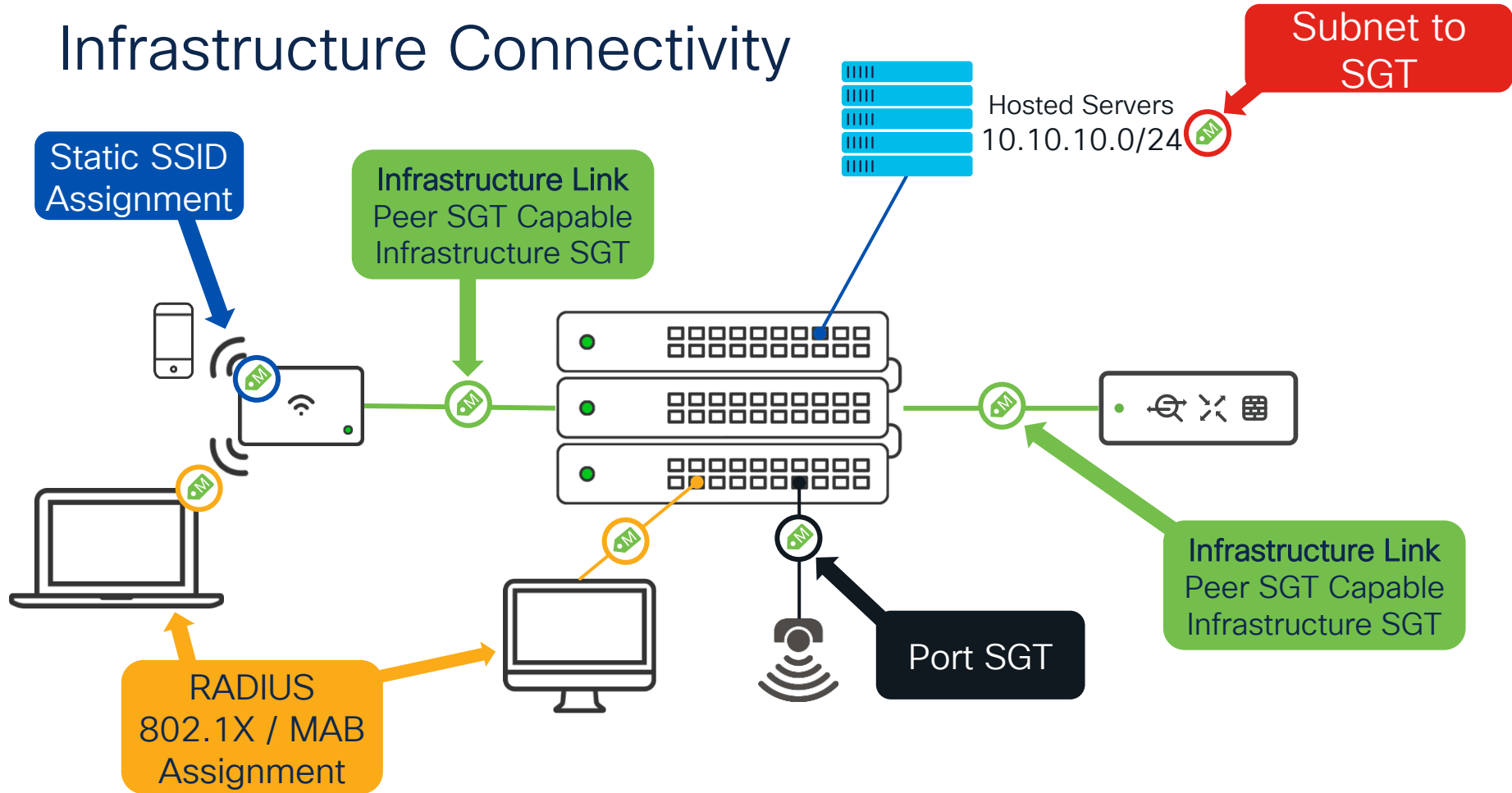


So where do we see tags?



Only between CMD capable peers
Client Ports have no knowledge of SGTs or the encapsulation

Infrastructure Connectivity



What's Next for Adaptive Policy

Adaptive Policy Matrix and Policy Visualization

Coming Soon

Finally.



Organization-Wide
Multi-network
filtering
Device-level filtering

- Policy Management
- Activity Indicators
- Policy Visualization
- Historical Hit Counters
- Historical ACL Logging
- Policy change filtering for validation pre<>post change

CISCO *Live!*

Security Center

Overview Events Integrations **Adaptive Policy**

Total Policies: 124 | Allow Policies: 31 | Deny Policies: 56 | Custom Policies: 37

Policies Groups Custom ACLs Networks

Search: [] Last day [v] Networks [v] Devices [v] 124 policies

	Unknown	Unknown	IOT-Device	GeneralData	Infrastructure	IOT-Device	IOT-Device	GeneralData	Infrastructure
Unknown	✓	✓	✓	✓	✓	✗	✗	✓	✓
Unknown	✓	✓	✓	①	✓	✓	✗	✓	✓
IOT-Device	✓	✓	✓	✓	✓	①	✓	✓	✗
GeneralData	✓	✗	✓	✓	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓	✗	✓	①	✓
IOT-Device	✓	✓	✓	✗	✓	✓	✓	✓	✓
IOT-Device	✓	✓	✓	✓	①	✓	✓	✗	✓
GeneralData	✓	✗	✓	✓	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✗	✓	①	✓	✓	✓

IOT_Device_adaptive_Wifi_Test

Policy

Policy description: Allow internal network communication between trusted subnets.

Source: IOT-Device

Destination: IOT-Device

Custom ACLs: Permit_DNS, Permit_MQTT

Policy Hit counters

Last day [v] Select a policy change event [v]

231 Packets allowed ✓ | 241 Packets denied ✗

Bar chart showing hit counts over time (17:11, 21:11, 01:11, 05:11, 09:11, 13:11, 17:11). Legend: Permit (green), Denied (red), When policy changed (blue triangle).

Event logs

Search: [] 24 matching results

Time (PCT)	Source	Destination	Action	Hits	Details
Jul 19 19:32:52	192.168.0.12	192.168.0.10	✗ Deny	14	View more
Jul 19 15:15:50	10.92.128.144	10.92.152.244	✓ Allow	10	View more
Jul 19 15:15:50	10.92.152.244	10.92.179.69	✓ Allow	8	View more
Jul 18 13:24:41	10.92.179.69	10.92.129.30	✗ Deny	6	View more
Jul 19 15:15:50	10.241.67.101	10.92.129.209	✗ Deny	3	View more

Last login: about 2 hours ago from your current IP address
Current session started: about 2 hours ago

[Cancel](#) [Save](#)

Static Per-Network VLAN to SGT (MS/CS)

Coming Soon

Not final design

VLAN profiles

1 You are modifying the default profile.

Edit profile

Profile name
Default

Iname
Default

VLAN name + Add Named VLAN

#	VLAN name	VLAN ID	AdP Group	Actions
1	WORKSTATION	101	4: Emj	
2	VOICE	102	12: VC	
3	IOTDEVICES	103	10: IO	

Save profile changes Cancel

Group name + Add VLAN group

#	Group name	VLAN list	Actions
1	WORKSTATIONS	400-401	
2	Guest	150-155	
3	EmployeeWireless	110-120	

Using Network VLAN Profiles

- Map an SGT to a VLAN
- Support for multiple profiles

Used as a fallback when static IP to SGT or more specific match is found

Adaptive Policy Assignment through Meraki Group Policy

SGT assignment through Dashboard's group policy constructs

Applicable to:

MR
MX**

MS uses RADIUS/Port/IP/VLAN

Example Uses:

- iPSK w/o RADIUS psk-based SGT
- Single RADIUS attribute for group policy assignment + SGT
- AnyConnect VPN SGT assignment
- Static API/Dashboard assignment

** subject to change based on release timelines for MX/Z

Group Policy

Group policies > **WPN_Group_1**

Name: WPN_Group_1

Schedule: Scheduling disabled

Bandwidth: Use network default unlimited

Hostname visibility: Use network default

Adaptive Policy Group: Select Adaptive Policy Group

Firewall and traffic shaping: Use network firewall & shaping rules

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment
	Allow	Any	Any	Any	Default rule

[Add a firewall rule](#)

Layer 7 firewall

There are no rules defined for this group.

[Add a layer 7 firewall rule](#)

Dashboard

Policy > Forget status: online 10 clients in 30

Apply policy to 1 selected client

☐ Normal
☐ Allow list (no bandwidth limits or splash page)
☐ Block list (no access allowed)
☒ Group policy

Employee

Usage	Client type, OS
1.9 MB	Cisco wireless access po
6.5 MB	Debian-based Linux
66.8 MB	Other
130.1 MB	Other
298.2 MB	Other
262.5 MB	Other
67.8 MB	Other
323.9 MB	Other
5.8 MB	Other
15.1 MB	Other
377.0 MB	Other
1.3 MB	Other
36.1 MB	Other
4.4 MB	Other
987.4 MB	Other

iPSK

Add Identity PSK

Note: You may not edit or view passphrase after Identity PSK has been created

Name: Guest

Passphrase:

Group Policy: Guests

Cancel Add

AnyConnect**

Dynamic Client Routing: ☒ Disable Dynamic Split Tunneling

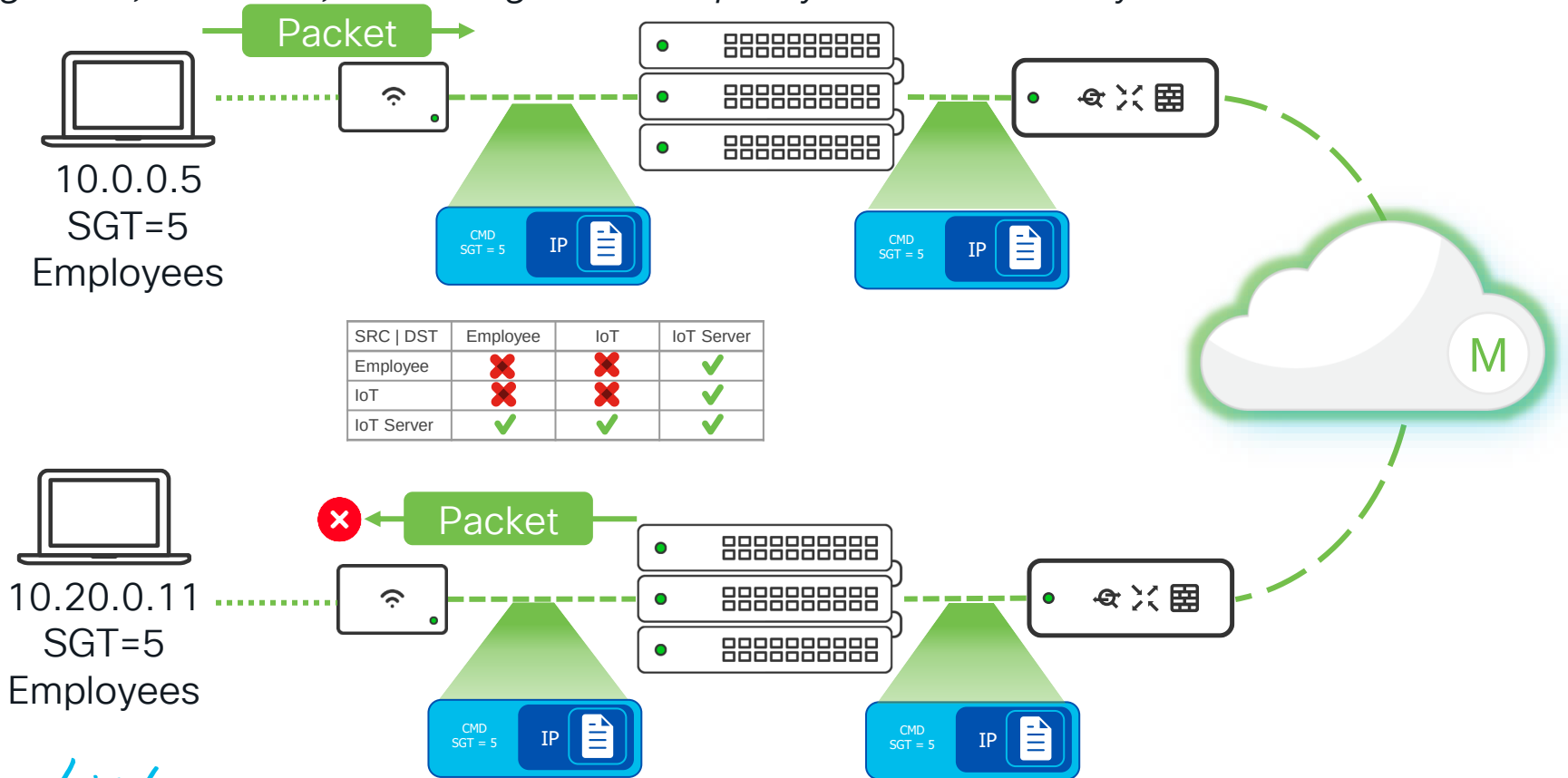
☐ Send all traffic except traffic going to these hostnames
☐ Only send traffic going to these destinations

Session Timeout: None

Default Group Policy: Guests

Foundation for Meraki Zero Trust

Org-Wide, full-stack, micro-segmentation policy based on Identity



Common Policy and Integrations in Cisco

Native Policy Syncing to Dashboard in ISE 3.2 P1

Using Dashboard APIs

Pushed directly from ISE

Single Source of Truth



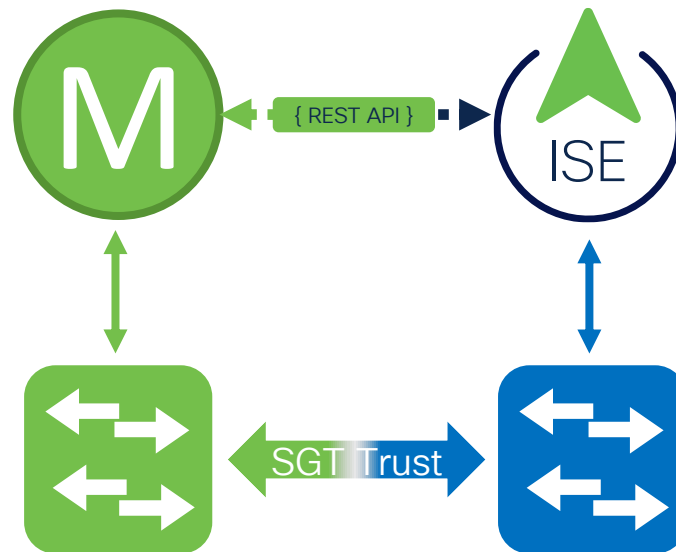
SRC DST	Employee	IoT	IoT Server
Employee	✓	✗	✗
IoT	✗	✗	✓
IoT Server	✗	✓	✓

Adaptive Policy and TrustSec

Native Rest API syncing between Dashboard and ISE

Tag trust at the data-plane interconnect

Context and policy shared between architectures



Adaptive Policy and ASA/Firepower

Add Rule

Name: Block HR to Accounting ☒ Enabled

Action: Block

Time Range: None

Insert: below rule 1

Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Metadata: Search by name or value, Security Group Tag, Add to Source, Add to Destination, Acct, ANY, HR

Selected Source Metadata (1): HR

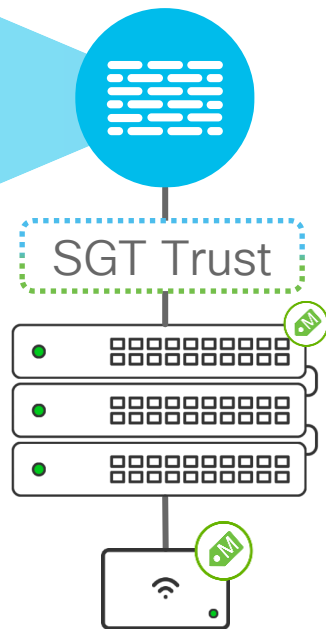
Selected Dest Metadata (1): Acct

Cancel Add

Tag-based Policy
from access to
edge of the network

Ability to statically
create tags in FMC
or dynamically via
Cisco Identity
Services Engine

Rules based on
data-plane context
sharing via SGTs



Meraki NetFlow Exporters



Product Line	Protocol Support
MX/Z3+	NetFlow v9
MS390/C9300-M	IPFIX (NetFlow v10) Enriched with AVC and ETA

NetFlow & Encrypted Traffic Analytics

AVC NetFlow*

IPv4 and v6 records built for
Cisco Secure Analytics

All East-West Traffic***

capturing flows on every client
facing port on all supported
switches in the network

Encrypted Traffic Analytics**

for in-depth analysis of traffic
without MiTM decryption

Adaptive Policy**

Export of Source Security Group
Tags (SGTs)



NetFlow traffic reporting	Enabled: send netflow traffic statistics ▼
NetFlow collector IP	10.10.0.45
NetFlow collector port	2055
Encrypted Traffic Analytics	☒
ETA collector port	9996

Requires Advanced Licensing

* should work with any standard up-to-date collector

** When integrated with Cisco Secure Network and/or Cloud Analytics (XDR)

*** Uplink port flow collection excludes AVC + SGT data

Adaptive Policy & Secure Network Analytics

Informed policy creation and validation



Global flow visibility and context



Group based policy and traffic flow tracking



Up to 90 Days of Historical data

Cell Details

TRAFFIC INFORMATION



Traffic Volume:
Start: ...
End: ...

PROTOCOLS

▲ ICMP (11KB) ...
TCP (2.5GB) ...
▲ UDP (0.6MB) ...

PORTS

22/SSH (320MB) ...
80/HTTP (100MB) ...
▲ 443/HTTPS (2GB) ...
▲ 54180 (52MB) ...

[View Flows](#)
[View Offending Traffic Flows](#)

ISE DATA

ISE Policy
Enabled ✓

SECURITY GROUP ACLS

Name: DevProdCommunication
IP Version: IP Agnostic
ACEs: Deny IP
permit tcp eq 80
permit tcp eq 22

MS390 with SNA & ISE



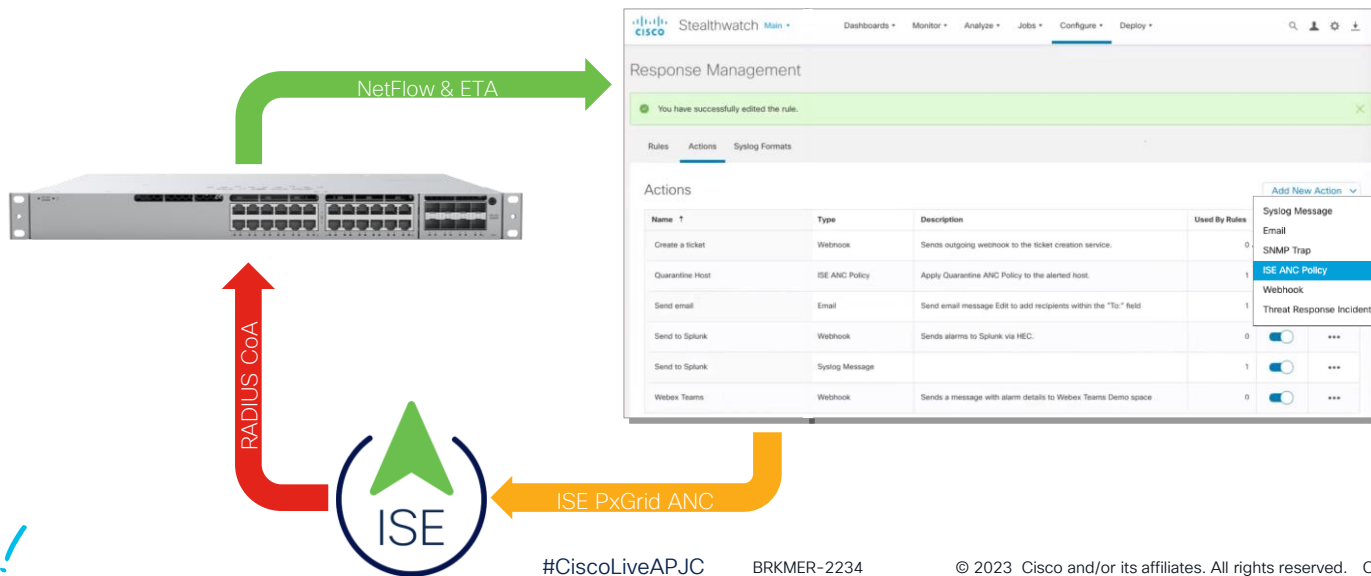
Telemetry provided by MS390/9300-M to SNA



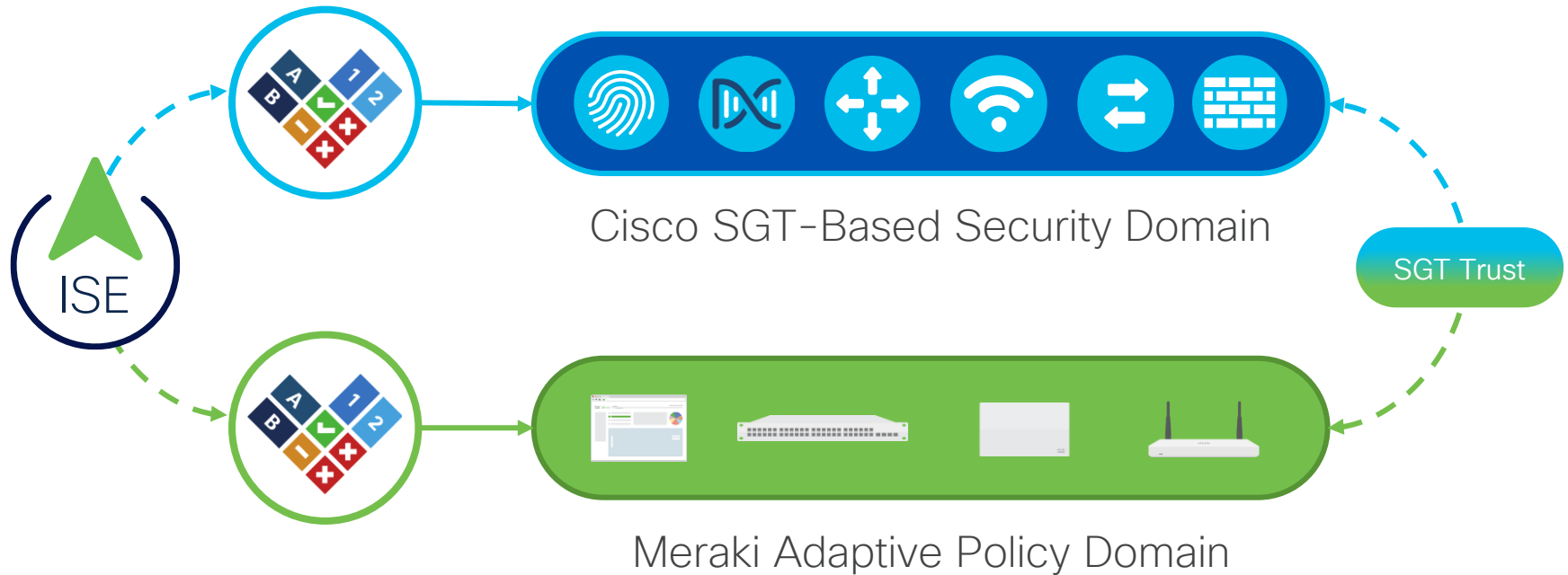
Flexible outcomes: Policy Violation



Trigger CoA via ISE



A true multi-domain zero-trust framework



CISCO *Live!*

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC