

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC





# Securing Cloud Managed Networks

Delivering Zero Trust with Meraki and Cisco Security Technologies

Ryan Pascoe - Solutions Engineer

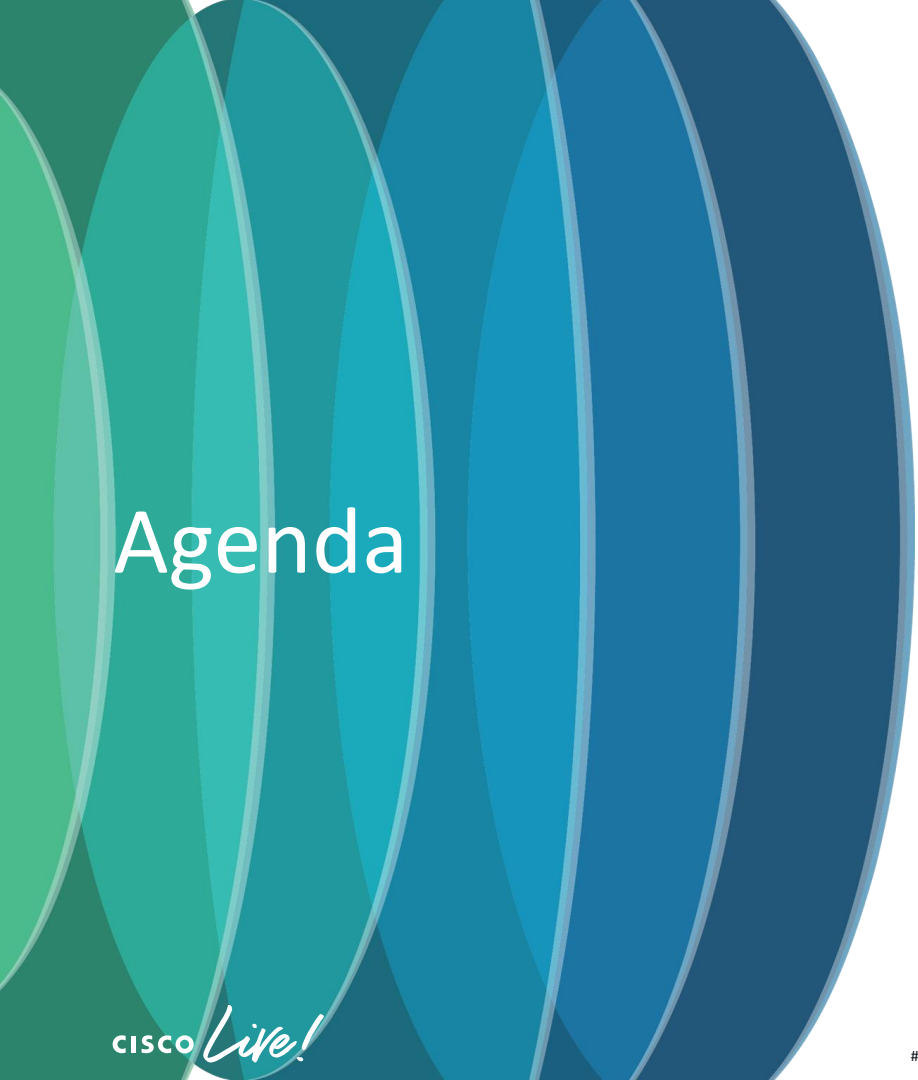
Alex Burger – Principal TME

BRKSEC-2597

CISCO *Live!*

#CiscoLiveAPJC

# Why are we here?



# Agenda

- Understanding what we are trying to protect against
- Discuss a vision for simplified network segmentation
- Roadmap, other tools and integrations

# Cisco Webex App

## Questions?

Use Cisco Webex App to chat with the speaker after the session

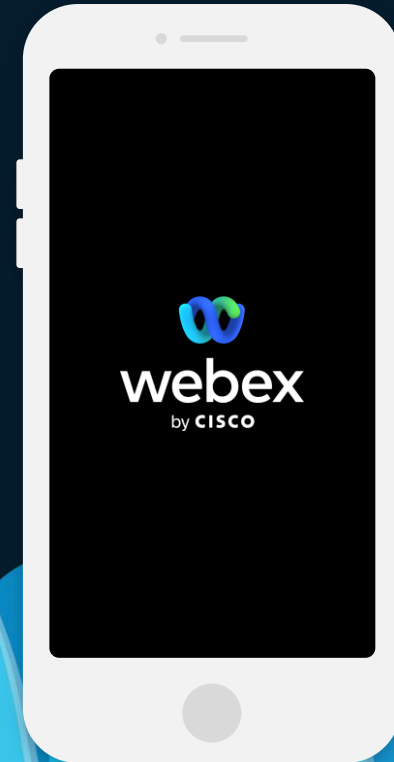
## How

- 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

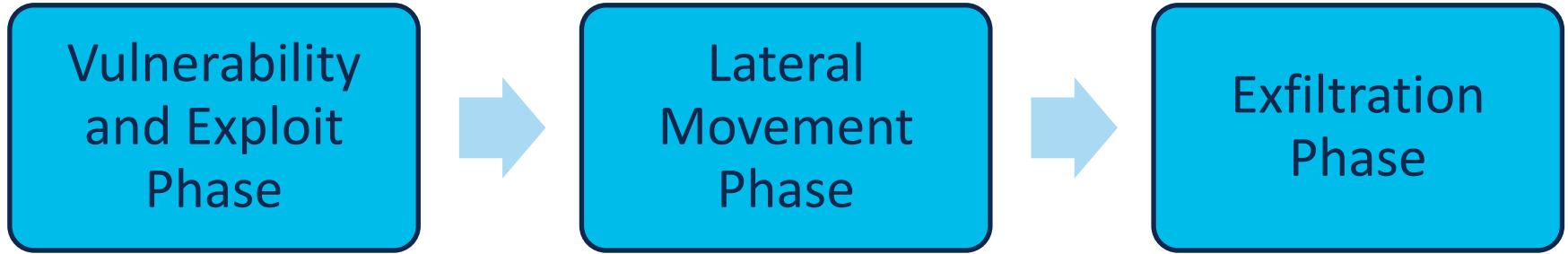
Webex spaces will be moderated by the speaker until November 15, 2024.



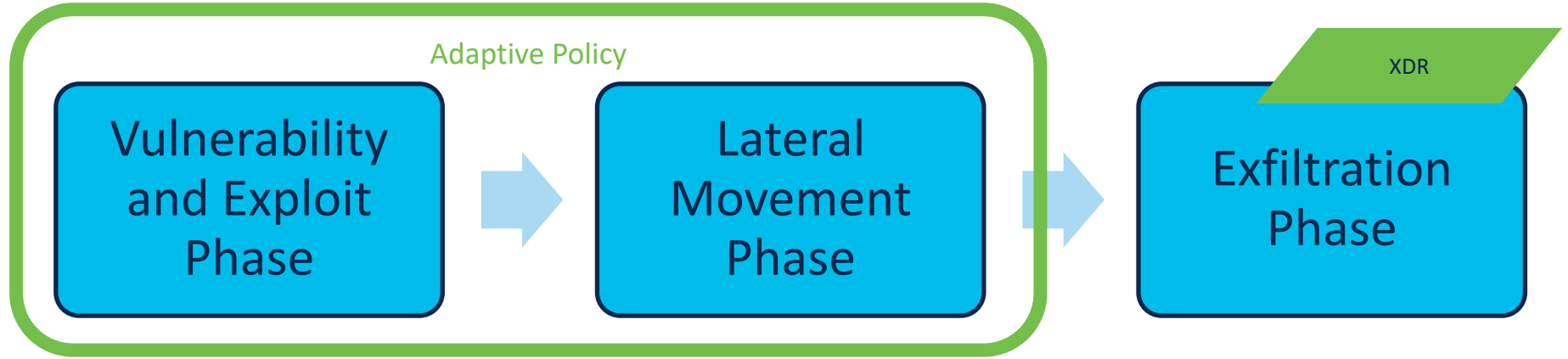
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2597>



# Break the lifecycle



# Break the lifecycle

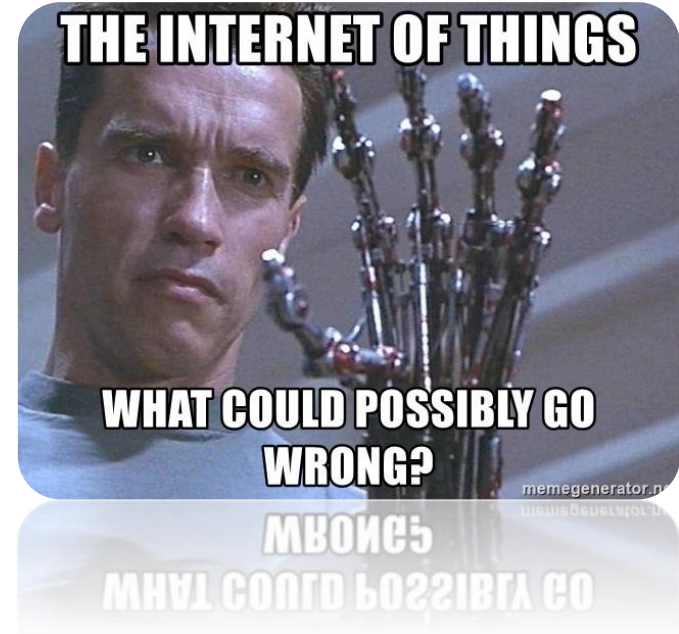


# Exploit the Vulnerabilities



More and more IoT devices

Less and less secure



# Accountability and Executive Pressure

- Cyber security legislative reforms engagement
  - Secure-by-design standards for Internet of Things devices
  - Mandatory reporting
  - Critical infrastructure protections



**Australian Government**  
**Department of Home Affairs**

# There are a lot of opinions on Zero Trust

## A Guide to **Embracing a Zero Trust Security Model in Government**

A security strategy for a safer  
and more resilient digital world

Forrester Report Prepared For Teresa Jimenez With Cisco Systems, Inc.

TRENDS REPORT

## **Decoding Zero Trust**

TRENDS REPORT

## **The Definition Of Modern Zero Trust**

Forrester Report Copy Prepared Exclusively For Rebecca Young With Cisco Systems, Inc. Distribution and reproduction are prohibited.

BEST PRACTICE REPORT

## **An Architect's Guide To Zero Trust Edge**

**Predicts 2024: Zero Trust Journey to Maturity**

# Zero Trust Network Access

*The principle of least privilege*



As the perimeter dissolves and data moves outside enterprise walls



Assume you have already been compromised you simply don't know it yet.



Ensure continuous and adaptive authorization

# Why are traditional approaches not working?

- ACL's

- Difficult to translate to security intent
- Do not scale well – more sites/control points the worse it gets
- Difficult to keep up to date

IP ACL:

```
Deny IP 192.168.255.0/24 to 192.168.0.0/16
```

```
Deny IP 192.168.255.0/24 to 172.16.0.0/12
```

```
Deny IP 192.168.255.0/24 to 10.0.0.0/8
```

```
Permit IP 192.168.255.0/24 to Any
```

```
Permit IP 192.168.1.0/24 to 192.168.50.0/24
```

```
Deny IP Any
```

IP ACL:

```
Deny IP 192.168.255.0/24 to 192.168.0.0/16
```

```
Deny IP 192.168.255.0/24 to 172.16.0.0/12
```

```
Deny IP 192.168.255.0/24 to 10.0.0.0/8
```

```
Permit IP 192.168.255.0/24 to Any
```

```
Permit IP 192.168.1.0/24 to 192.168.50.0/24
```

```
Deny IP Any
```

IP ACL:

```
Deny IP 192.168.255.0/24 to 192.168.0.0/16
```

```
Deny IP 192.168.255.0/24 to 172.16.0.0/12
```

```
Deny IP 192.168.255.0/24 to 10.0.0.0/8
```

```
Permit IP 192.168.255.0/24 to Any
```

```
Permit IP 192.168.1.0/24 to 192.168.50.0/24
```

```
Deny IP Any
```

# Why are traditional approaches not working?

- VRF's –
  - Excellent broad segmentation approach
  - Doesn't scale well VRF per use case
  - Inevitable inter-vrf leaks and
  - Skills to manage config complexity



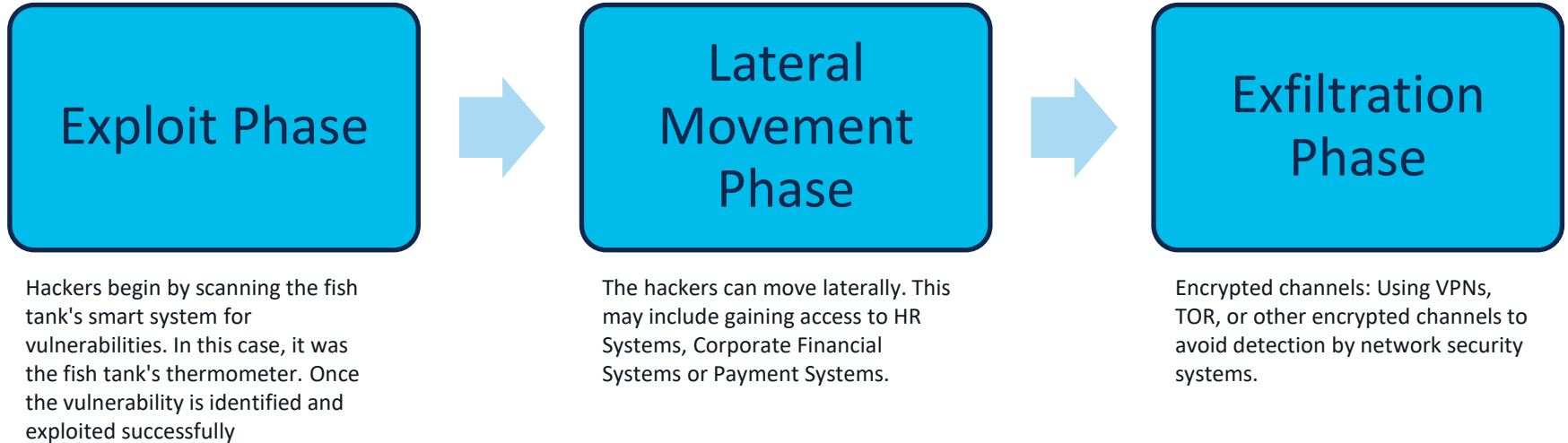
*Everybody gets a VRF*

# Why are traditional approaches not working?

- Perimeter FW
  - Great when the threats are on the other side
  - The more we have the more difficult they can be to manage
  - Often suboptimal traffic flows required



# Real world example



*security = complexity*

*security = complexity*

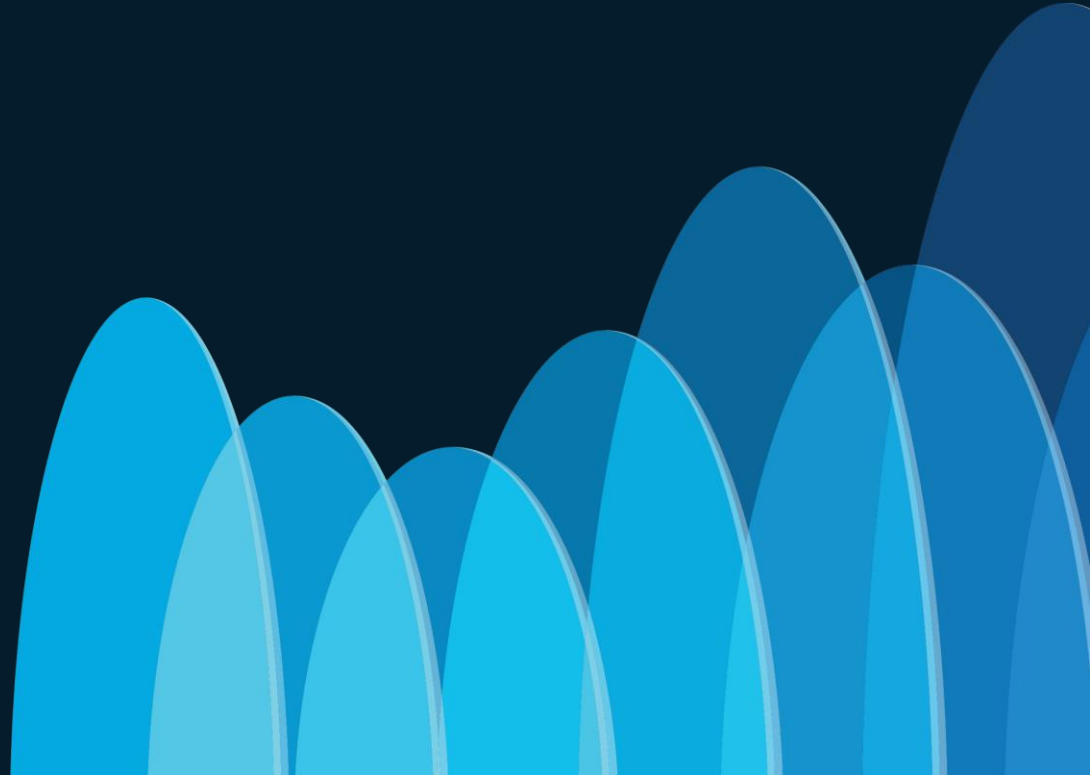
# Alex Burger

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](https://www.wirelesslywired.com)



# Adaptive Policy



# Adaptive Policy



Organization-Wide intent-based policy



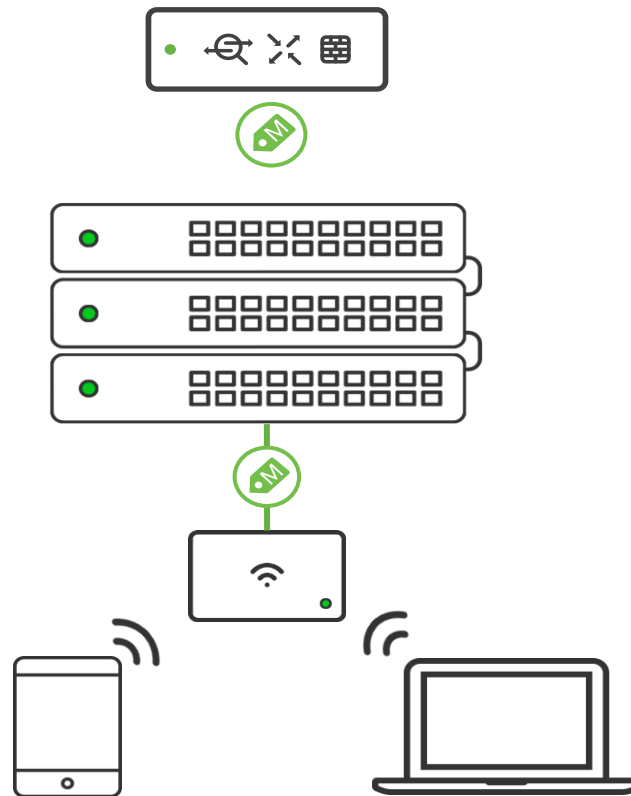
Utilizing inline Security Group Tags (SGTs)



Context shared over the data-plane

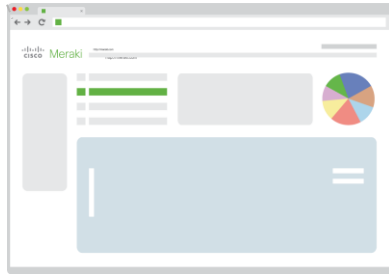
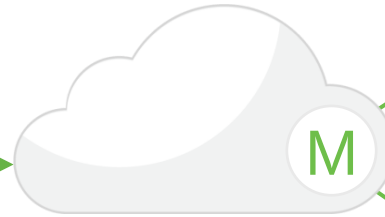


IP and topology agnostic security providing consistent policy for wired and wireless access



# One Consistent Policy Across Networks

| SRC   DST  | Employee | IoT | IoT Server |
|------------|----------|-----|------------|
| Employee   | ✓        | ✗   | ✓          |
| IoT        | ✗        | ✗   | ✓          |
| IoT Server | ✓        | ✓   | ✓          |

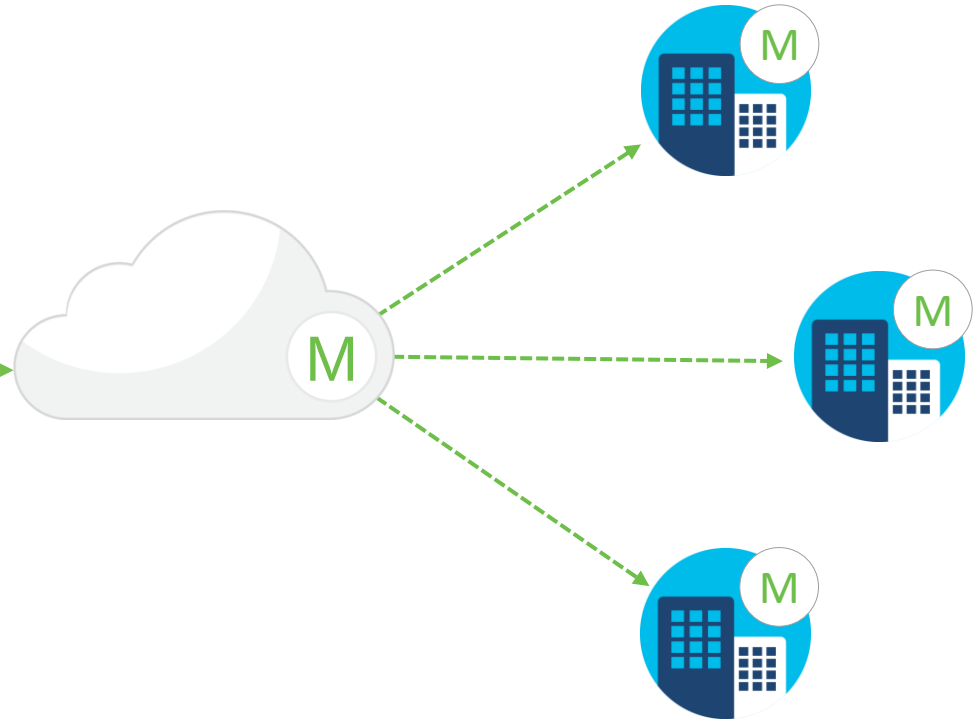


Policy & Groups are configured in dashboard and pushed to Adaptive Policy nodes like any other Meraki configuration change

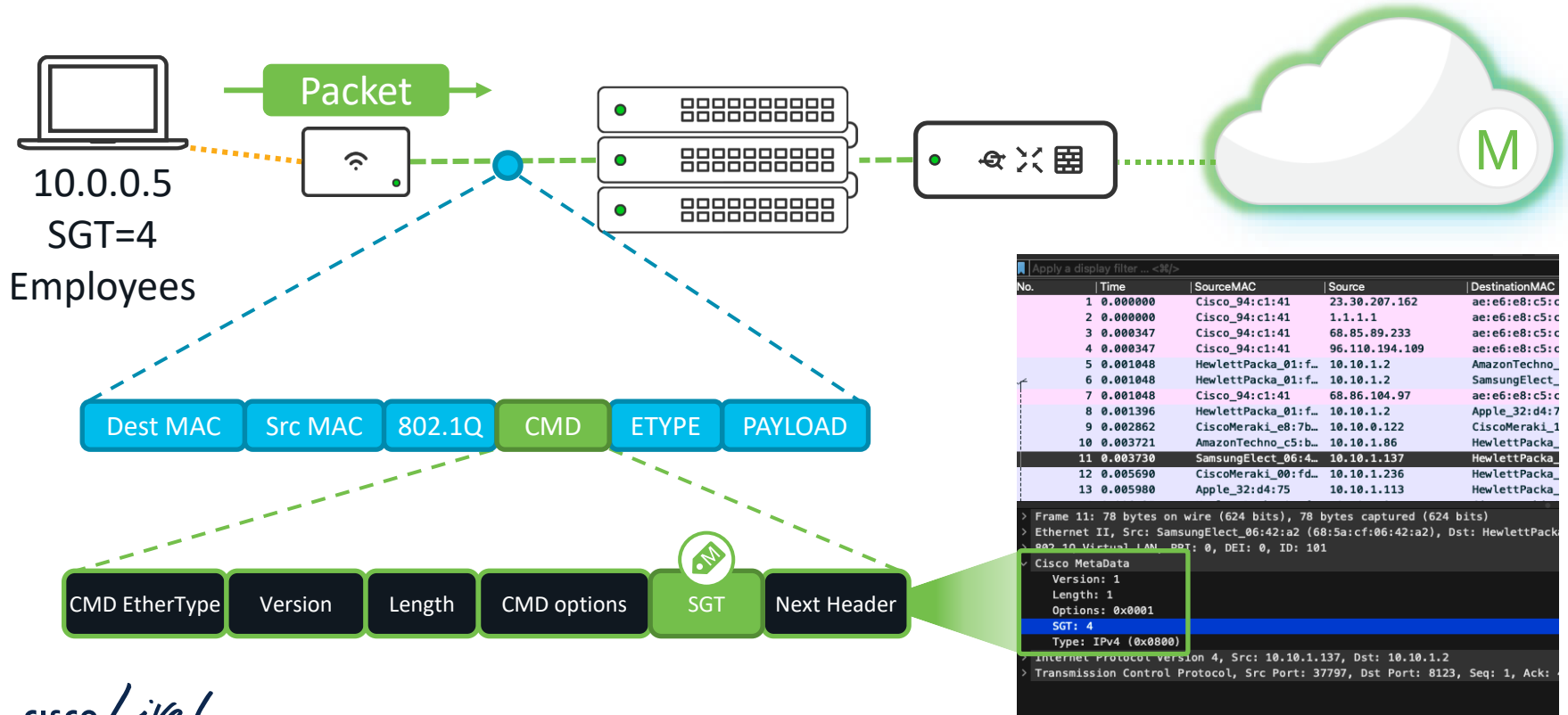
# API First!

| SRC   DST  | Employee | IoT | IoT Server |
|------------|----------|-----|------------|
| Employee   | ✓        | ✗   | ✓          |
| IoT        | ✗        | ✗   | ✓          |
| IoT Server | ✓        | ✓   | ✓          |

```
adaptivePolicy/  
  __ groups  
  __ acls  
  __ bindings  
  __ settings
```

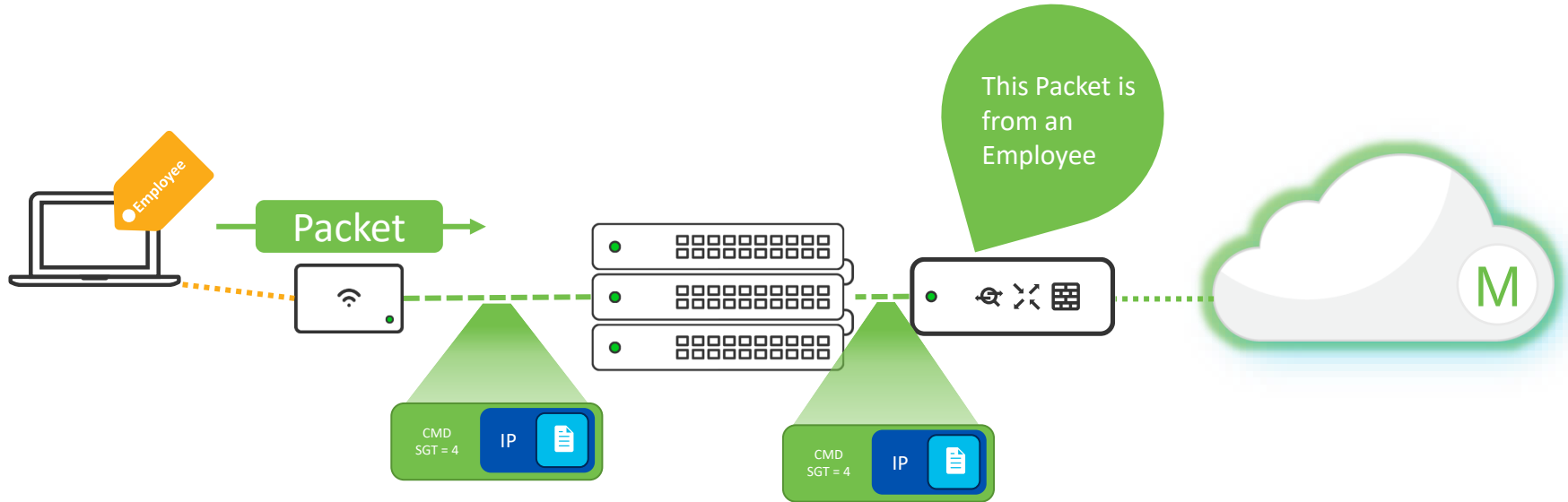


# What are SGTs?



# Scalable Identity and Context

*Sharing information over the dataplane, in every packet*



**CISCO** *Live!*



# 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

✓ iPSK Default Radius: Called-Station-ID CONTAINS Tornado-AP\_PSK × DefaultPSK4Clients + TestClient × +

## 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

# Large scale customer use case

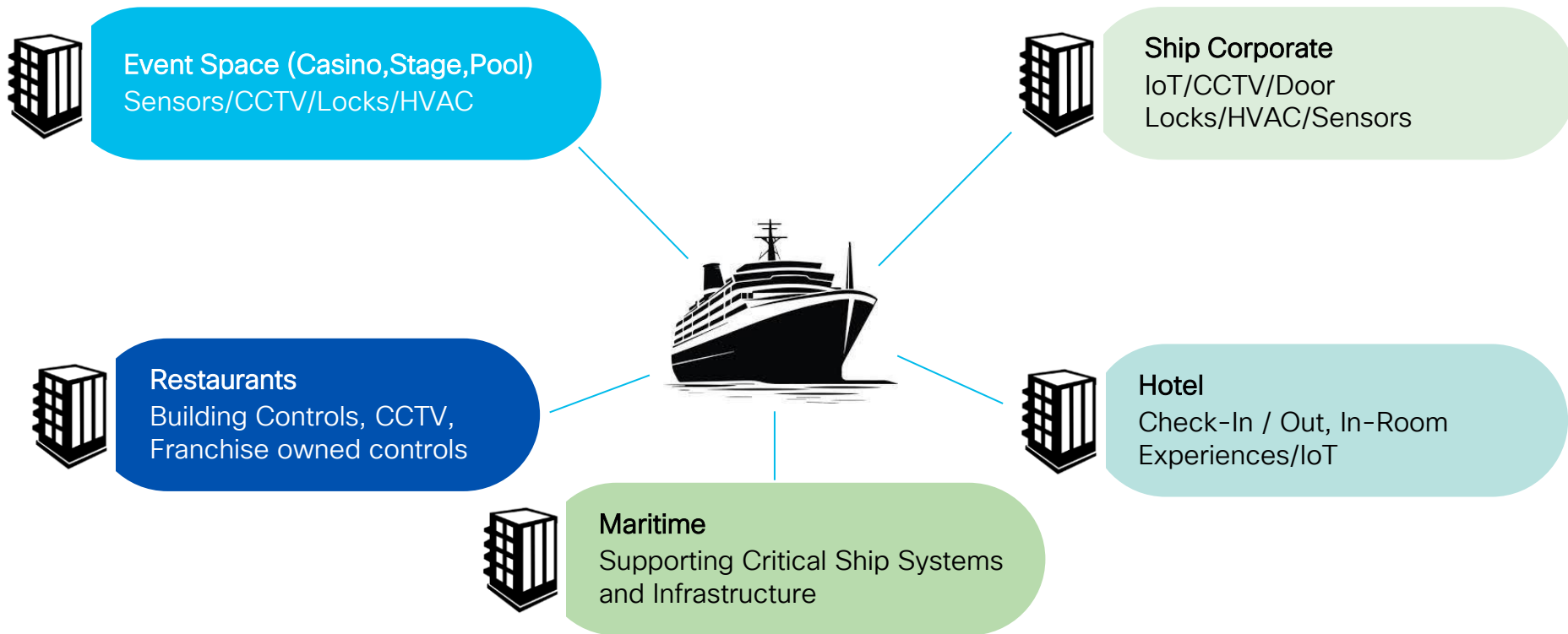
# Securing a Floating City



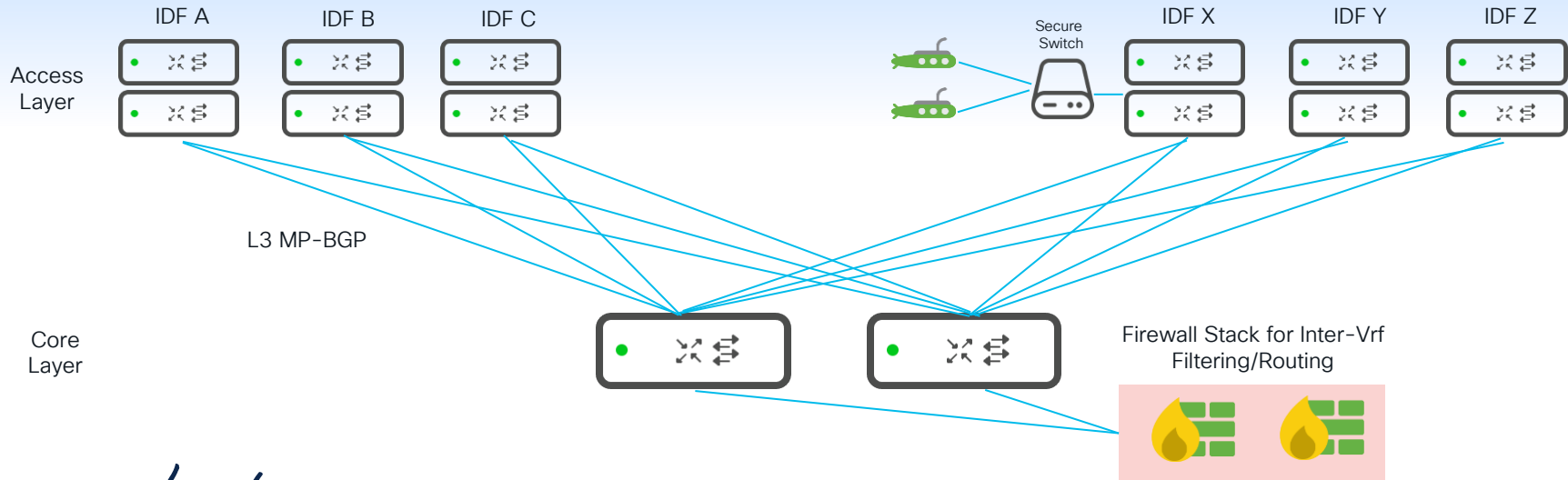
- Hospitality - Floating Hotel with Full In Room Controls
- Financial - Casino
- Marine Ops - Bridge, Maritime PLCs
- Physical Security (IPTV, Door Locks, etc)
- IoT/OT - Room controls, HVAC, Environment Sensors

# What is a Cruise Ship?

Many Smart Buildings in one Smart City



# The OLD way – Everyone Gets a Vrf



# The New solution – Adaptive Policy

Cloud Monitored Catalyst + Catalyst Meraki Managed 9Ks + ISE



Reduce to 3-5 VRFs for macro segmentation (traffic engineering)

- PCI
- Guest/Public Facing
- Ship side
- Vendor

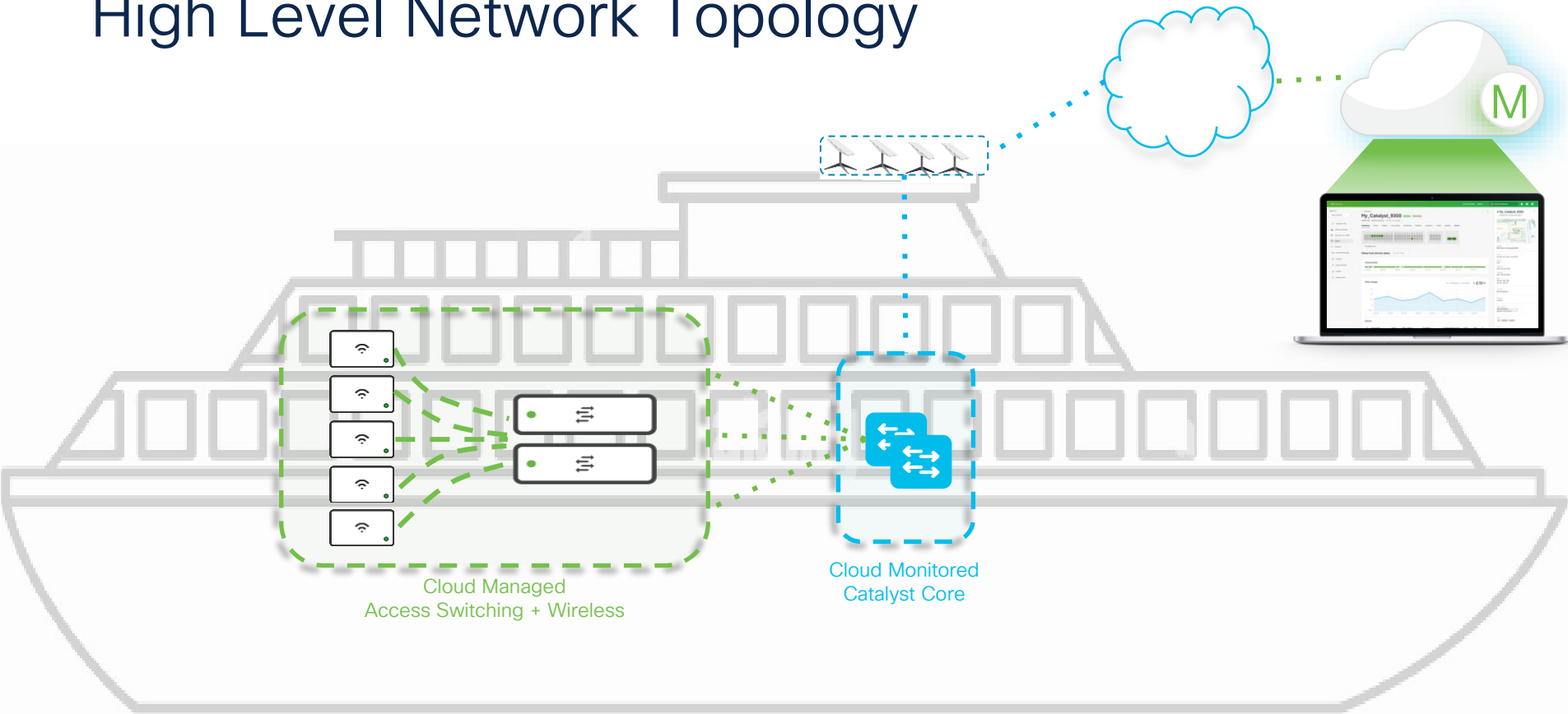
Adaptive Policy for Micro Segmentation within the VRFs

- Example Ship Side VRF: HVAC Controls SGT , IP cameras SGT, Door Locks

Adaptive Policy for Segmentation within the same SGT

- Example: Maritime Controls, Employee Ship Side machines

# High Level Network Topology



# Adaptive Policy Logical – 40+ VRFs reduced to 6

## Ship VRF

CCTV – SGT



Crew – SGT



Policies:

SGT to SGT are deny with Logging

Within the same SGT Anti-Malware ACL applied to SOME SGTs (Example: Employees)

## Maritime VRF

Marine OPS – SGT



Policies:

SGT to SGT is DENY with logging

Within same SGT is DENY with logging

## PCI VRF

PCI – SGT



POS – SGT



Policies:

SGT to SGT are deny with Logging

Within the same SGT Anti-Malware ACL applied to SOME SGTs (Example: Employees) – Logging Enabled

# Adaptive Policy Logical - Continued

## Vendor VRF



Policies:

SGT to SGT are deny with Logging

Within the same SGT Anti-Malware ACL applied to SOME SGTs (Example: Employees)

## Guest VRF



Policies:

Tunneled to DMZ for internet Only

## In-Room IOT VRF



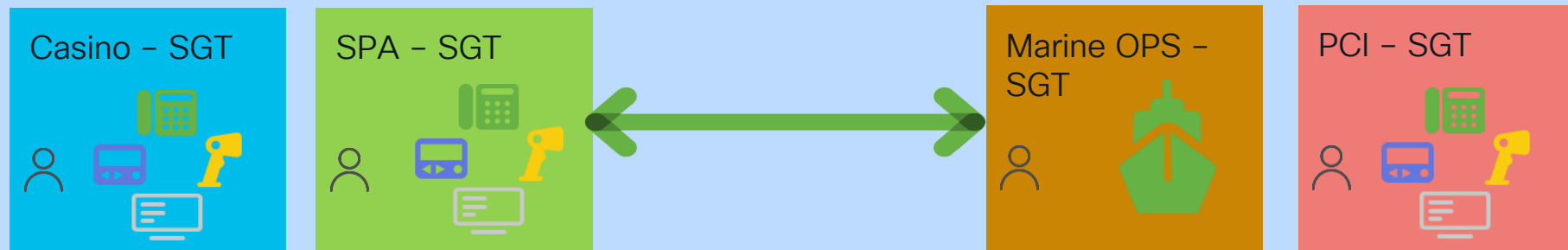
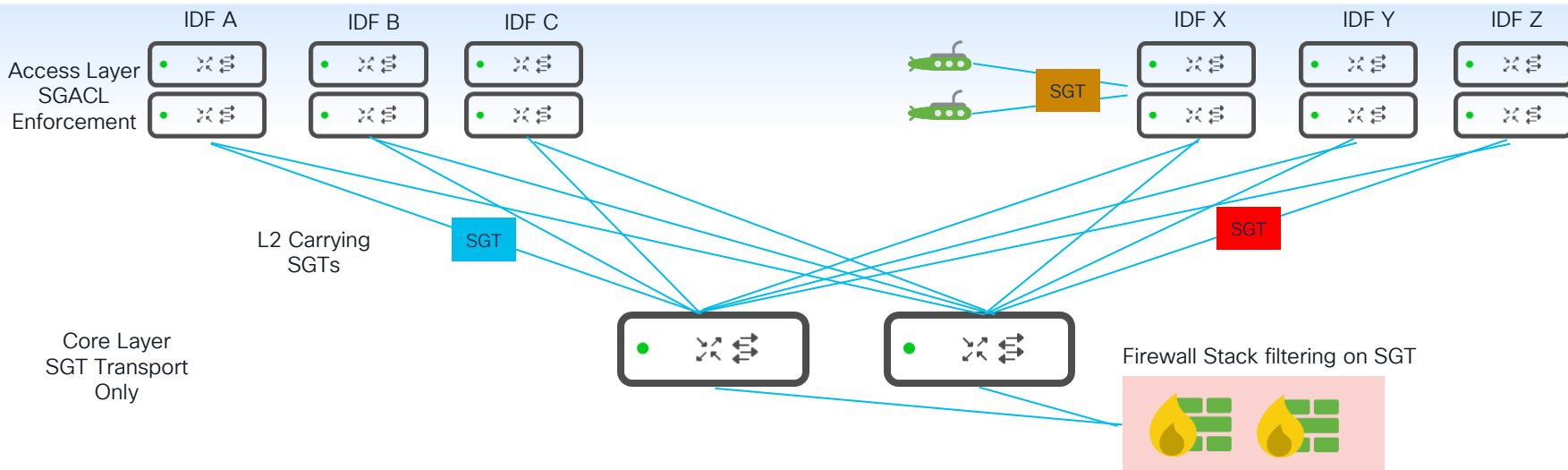
Policies:

Wifi to other SGTs - DENY with logging

SGT to SGT Room controls - Permit

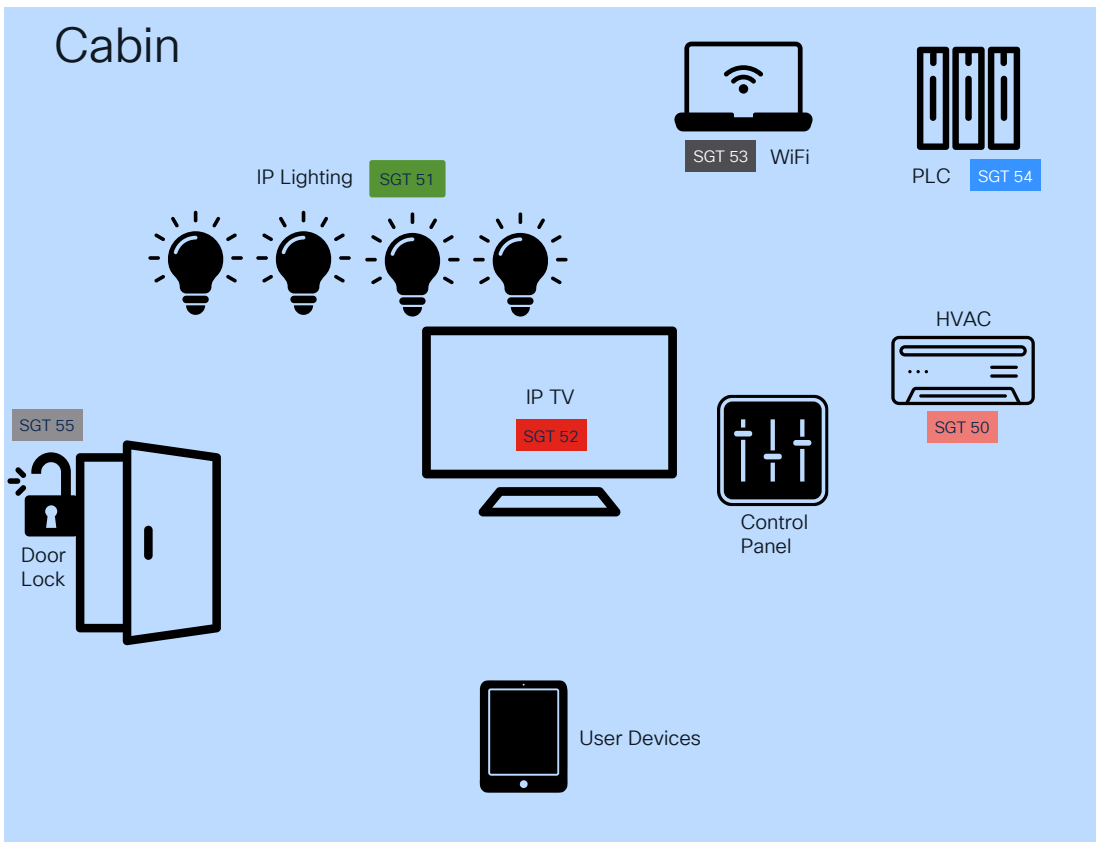
Within the same SGT - PERMIT

# Adaptive Policy Topology



# IoT Cabin Control Example

## Cabin



## In Cabin User Controls

- Users can control everything about their cabin from anywhere on the ship
- Each Room has its own dedicated Wall Plate AP
- HVAC, Door Lock, IPTV, Control Panel and IP Lighting are all connected to the Cabin PLC

Cabin Control devices are profiled by ISE and assigned the appropriate SGT for the device. Any device NOT profiled as a Cabin Automation Device is DENIED Access from ISE

Cabin Automation controls can only talk to Cabin automation controls and Cabin control servers in the Datacenter

Users are denied direct access to Cabin automation Controls

# Example Policies

Policies

Groups

Custom ACLs

Networks

TOTAL POLICIES

13

DENY POLICIES

0 /13

ALLOW POLICIES

0 /13

GROUPS

10

ACLs

1

Search...

Add Policies

| <input type="checkbox"/> | Source Group | Destination Group | Permission | Policy Name               | Last update        |
|--------------------------|--------------|-------------------|------------|---------------------------|--------------------|
| <input type="checkbox"/> | MarineOps    | PCI               | * Custom   | MarineOps - PCI           | Mar 13, 2024 10:50 |
| <input type="checkbox"/> | MarineOps    | Ship Side         | * Custom   | MarineOps - Ship Side     |                    |
| <input type="checkbox"/> | MarineOps    | Guest             | * Custom   | MarineOps - Guest         |                    |
| <input type="checkbox"/> | MarineOps    | Arcade            | * Custom   | MarineOps - Arcade        |                    |
| <input type="checkbox"/> | MarineOps    | Spa               | * Custom   | MarineOps - Spa           |                    |
| <input type="checkbox"/> | MarineOps    | Game Services     | * Custom   | MarineOps - Game Services |                    |
| <input type="checkbox"/> | Arcade       | PCI               | * Custom   | Arcade - PCI              |                    |
| <input type="checkbox"/> | Arcade       | Ship Side         | * Custom   | Arcade - Ship Side        |                    |
| <input type="checkbox"/> | Arcade       | Guest             | * Custom   | Arcade - Guest            |                    |
| <input type="checkbox"/> | Arcade       | Spa               | * Custom   | Arcade - Spa              |                    |

☐ RoomPLC

RoomLighting

☐ RoomPLC

RoomHVAC

☐ RoomPLC

RoomWiFi

☐ RoomPLC

RoomIPTV

☐ RoomPLC

RoomPLCPanel

☐ RoomPLC

PCI

☐ RoomPLC

Ship Side

☐ RoomPLC

Arcade

☐ RoomPLC

Spa

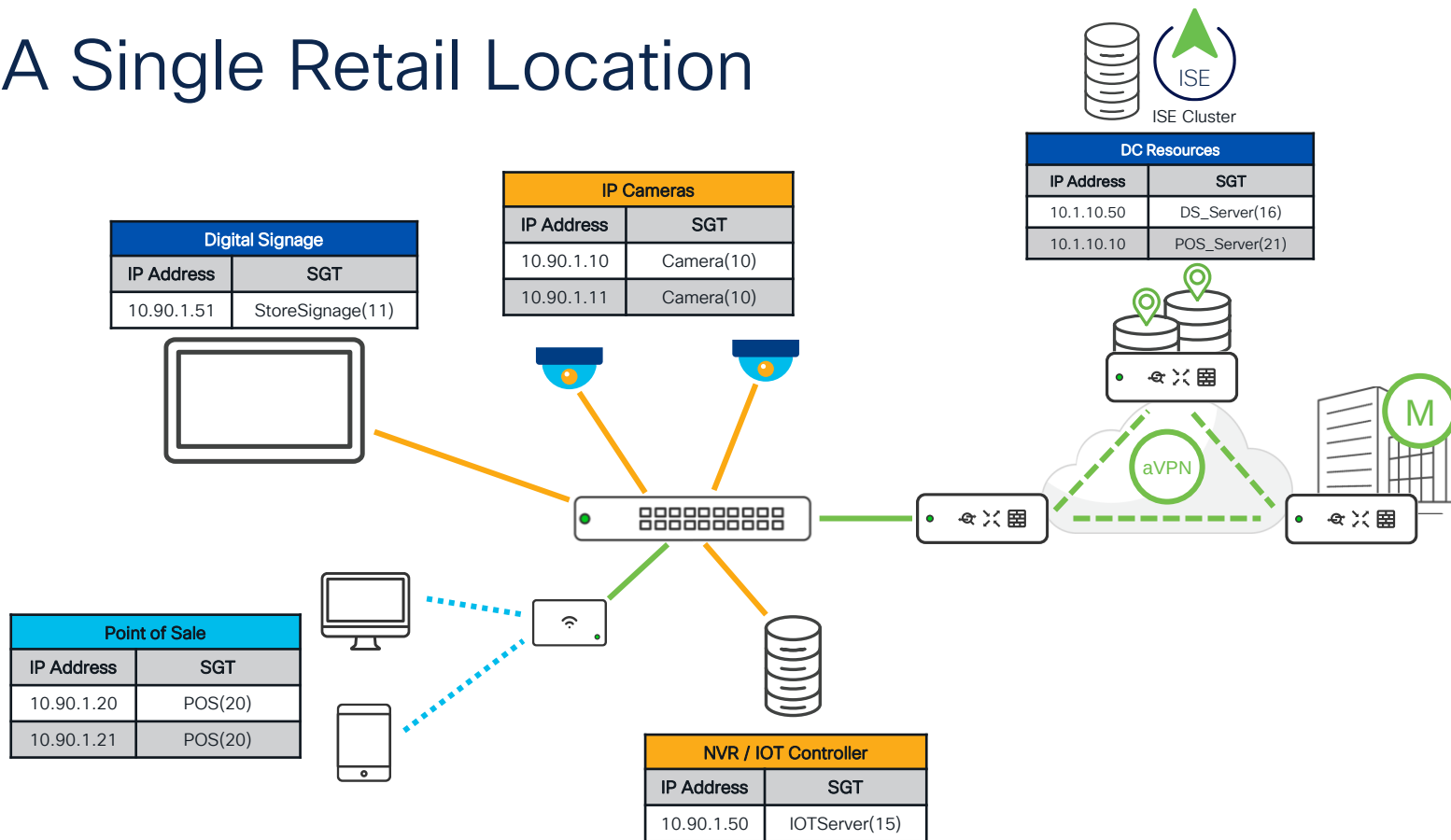
|                          |         |               |          |                         |                    |
|--------------------------|---------|---------------|----------|-------------------------|--------------------|
| <input type="checkbox"/> | RoomPLC | RoomLighting  | ✓ Allow  | RoomPLC - RoomLighting  | Mar 13, 2024 10:50 |
| <input type="checkbox"/> | RoomPLC | RoomHVAC      | ✓ Allow  | RoomPLC - RoomHVAC      | Mar 13, 2024 10:50 |
| <input type="checkbox"/> | RoomPLC | RoomWiFi      | ✓ Allow  | RoomPLC - RoomWiFi      | Mar 13, 2024 10:50 |
| <input type="checkbox"/> | RoomPLC | RoomIPTV      | ✓ Allow  | RoomPLC - RoomIPTV      | Mar 13, 2024 10:50 |
| <input type="checkbox"/> | RoomPLC | RoomPLCPanel  | ✓ Allow  | RoomPLC - RoomPLCPanel  | Mar 13, 2024 10:50 |
| <input type="checkbox"/> | RoomPLC | PCI           | * Custom | RoomPLC - PCI           | Mar 13, 2024 10:53 |
| <input type="checkbox"/> | RoomPLC | Ship Side     | * Custom | RoomPLC - Ship Side     | Mar 13, 2024 10:53 |
| <input type="checkbox"/> | RoomPLC | Arcade        | * Custom | RoomPLC - Arcade        | Mar 13, 2024 10:53 |
| <input type="checkbox"/> | RoomPLC | Spa           | * Custom | RoomPLC - Spa           | Mar 13, 2024 10:53 |
| <input type="checkbox"/> | RoomPLC | Game Services | * Custom | RoomPLC - Game Services | Mar 13, 2024 10:53 |
| <input type="checkbox"/> | RoomPLC | MarineOps     | * Custom | RoomPLC - MarineOps     | Mar 13, 2024 10:53 |
| <input type="checkbox"/> | RoomPLC | BridgeOps     | * Custom | RoomPLC - BridgeOps     | Mar 13, 2024 10:53 |
| <input type="checkbox"/> | RoomPLC | RoomPLC       | * Custom | RoomPLC - RoomPLC       | Mar 13, 2024 10:53 |
| <input type="checkbox"/> | RoomPLC | Guest         | ✓ Allow  | RoomPLC - Guest         | Mar 13, 2024 10:53 |

# Example ACLs

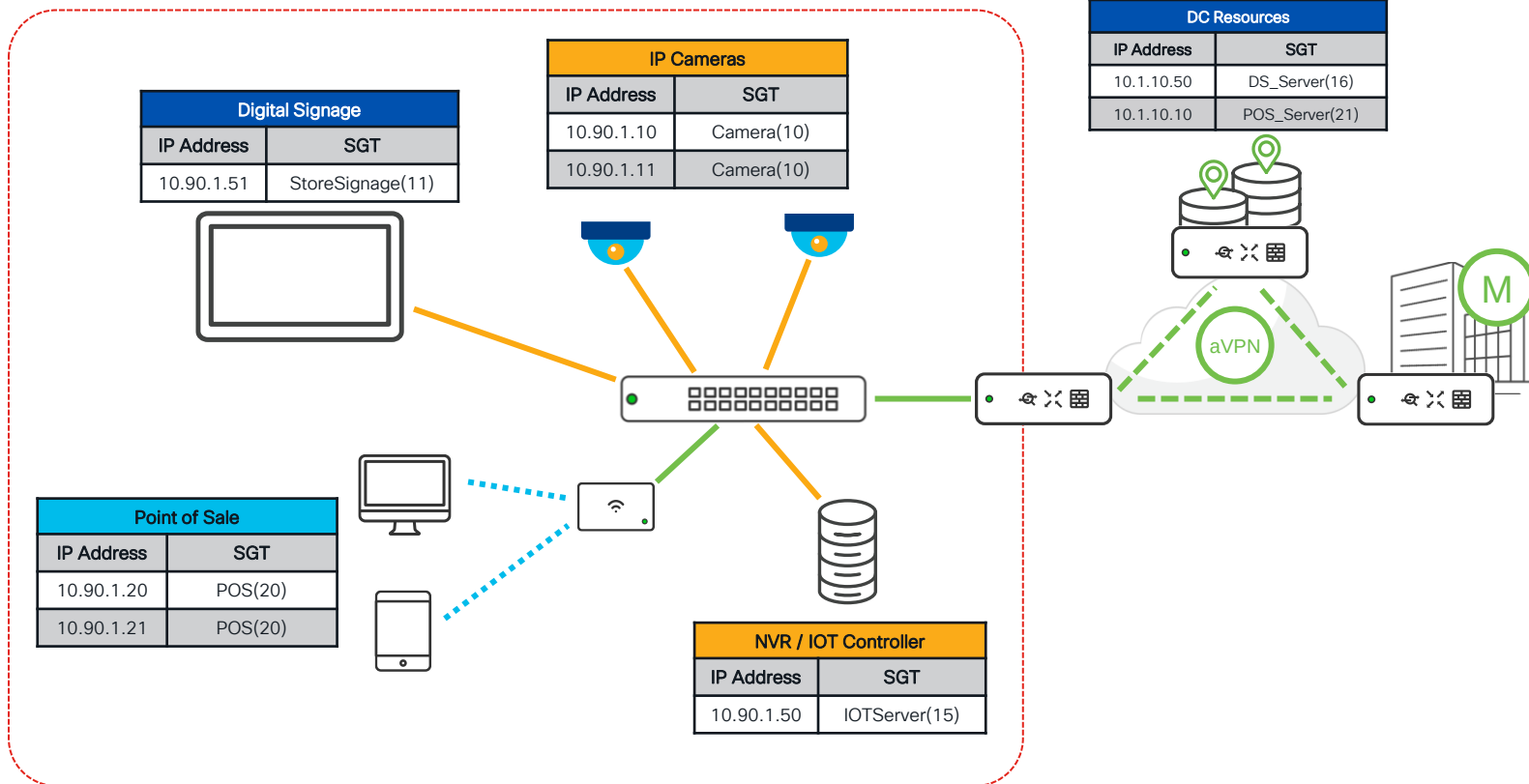
|  | Name         | Description          | IP Version | Rules                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------|--------------|----------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/>                                                        | Deny_IP_Log  | Deny IP with logging | any        | deny any   src: any, dst: any   tcp established: Disabled   log: Enabled                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <input checked="" type="checkbox"/>                                             | Anti_Malware |                      | any        | deny icmp   src: any, dst: any   tcp established: Disabled   log: Disabled<br>deny udp   src: any, dst: 53   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 3389   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 1433   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 1521   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 445   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 137   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 138   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 139   tcp established: Disabled   log: Enabled<br>deny udp   src: any, dst: 161   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 23   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 80   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 443   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 22   tcp established: Disabled   log: Enabled<br>deny tcp   src: any, dst: 123   tcp established: Disabled   log: Enabled<br>allow any   src: any, dst: any   tcp established: Disabled   log: Disabled |

# How does it work?

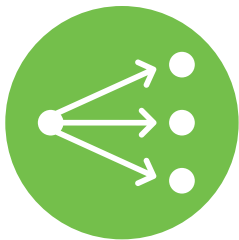
# A Single Retail Location



# Scope of Policy

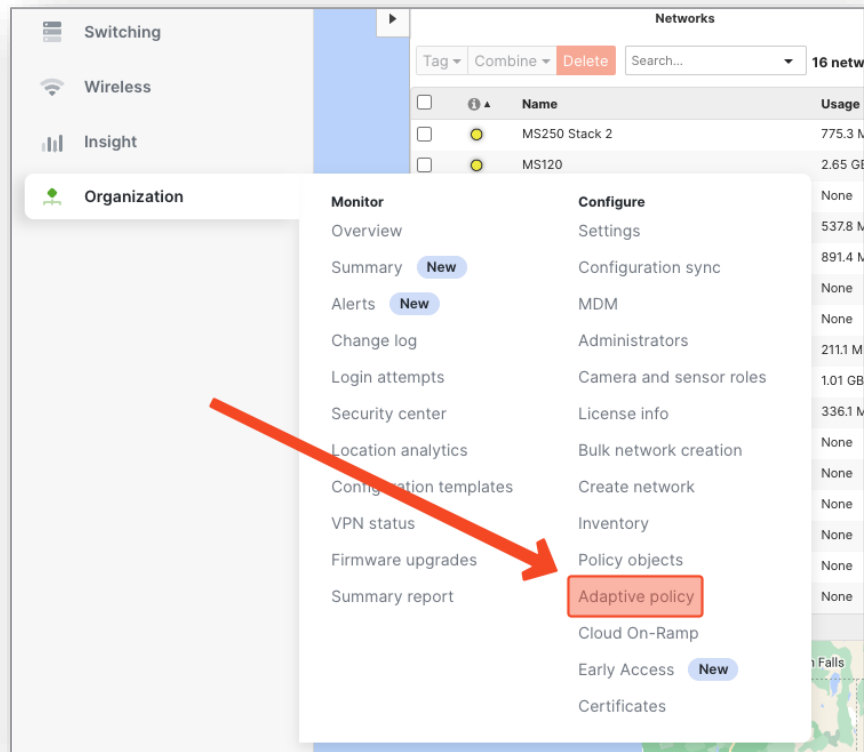


# Adaptive Policy – Org Level Functions



## 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

**CISCO** *Live!*

**Adaptive policy**

Policies Groups Custom ACLs Networks

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

| <input type="checkbox"/> | Name | SGT Value | Description | Policy Objects |
|--------------------------|------|-----------|-------------|----------------|
|--------------------------|------|-----------|-------------|----------------|

**Add adaptive policy group** ✕

Name

SGT Value ⓘ

Description

Policy Object Binding ⓘ

**Review changes**

# Enabling Adaptive Policy on a Meraki Network

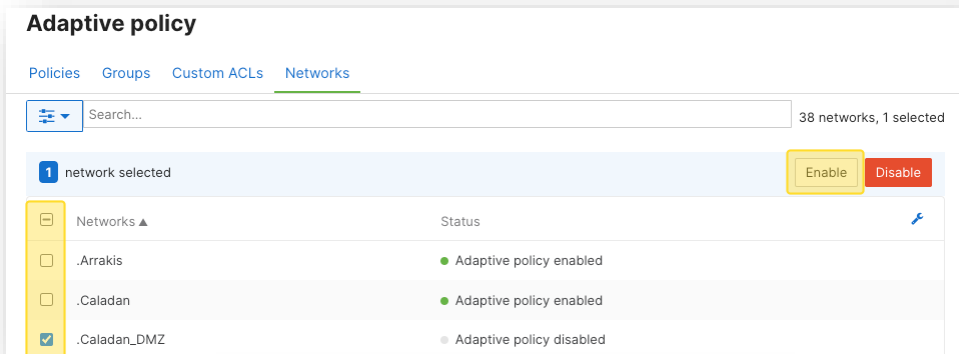
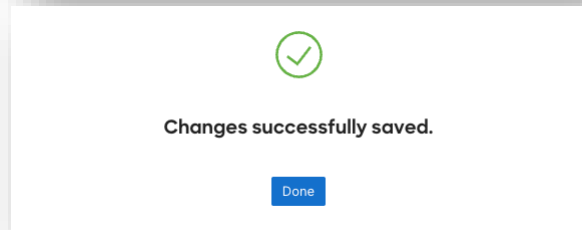
Adaptive Policy is enabled on a per-network basis via  
**Organization > Adaptive policy > Networks**

## 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 in MS17 for MS130 X/R*

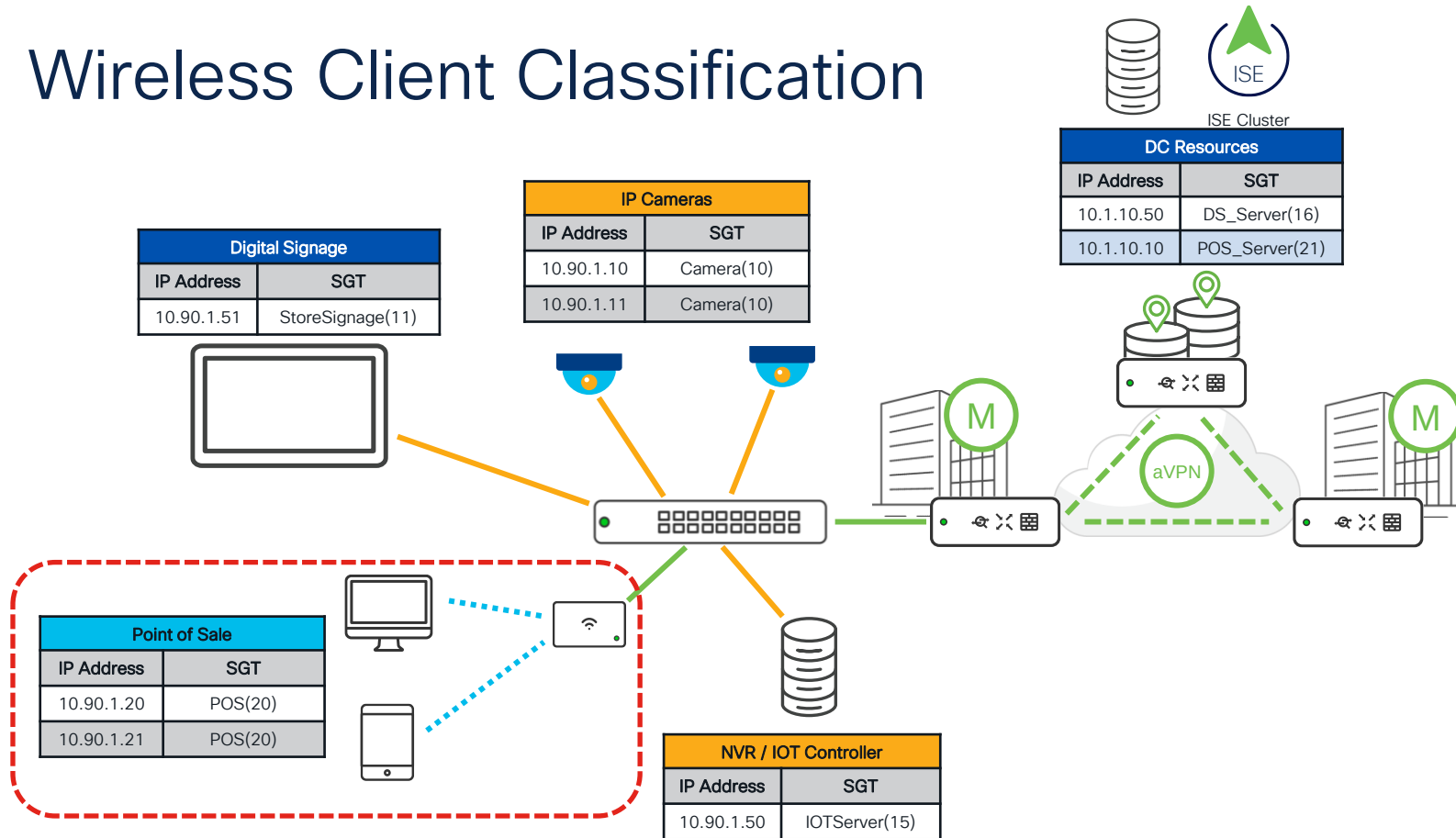
**CISCO** *Live!*



# Classifying Wireless Clients



# Wireless Client Classification



# 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

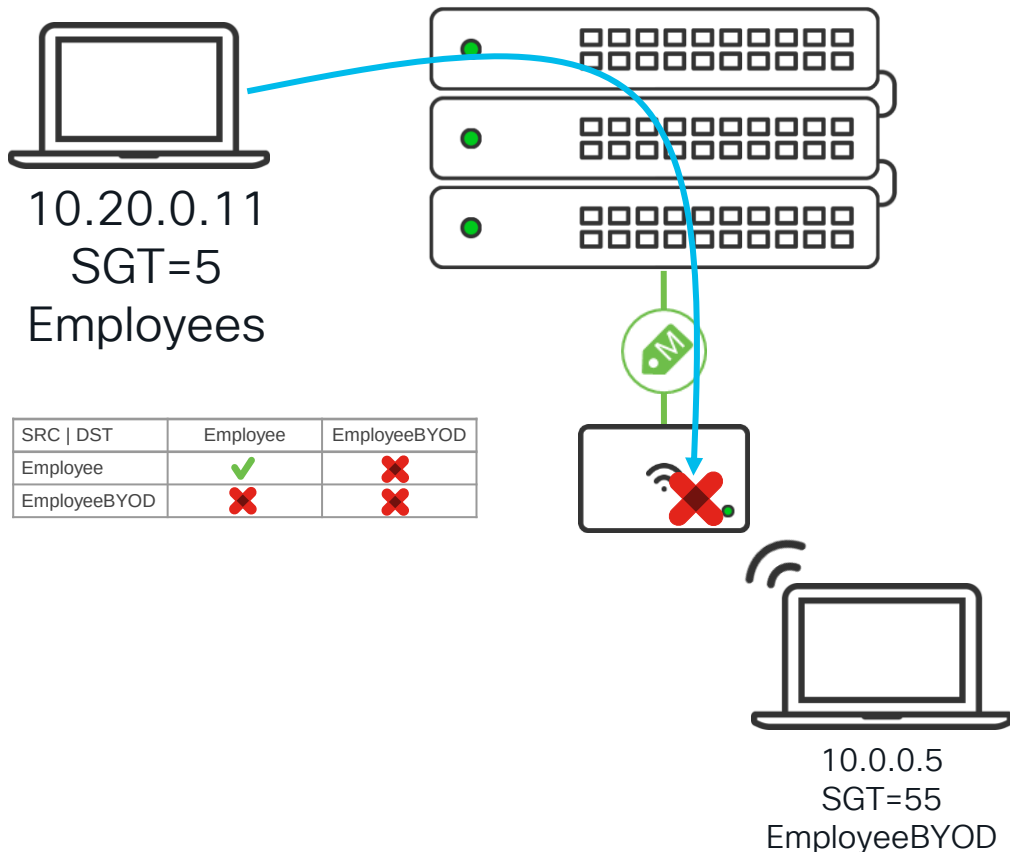


# Propagation and Enforcement

## MR Policy Handling

### Support

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



# SGT Assignment through Meraki Group Policy

Beta - R31

SGT assignment through  
Dashboard's group policy  
constructs

Applicable to:

MR

Example Uses:

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

## Group Policy + SGT

Group policies

Name: WPN\_Group\_1

Schedule:

Bandwidth:  unlimited

Hostname visibility:

Adaptive Policy Group:  (highlighted with a red box)

Firewall and traffic shaping:

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](#)

## iPSK

Add Identity PSK

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

Name:

Passphrase:

Group Policy:  (highlighted with a red box)

## Dashboard

Policy:   15 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                    |

# 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

The screenshot displays a configuration page for SGT assignment. It includes several settings:

- RADIUS guest VLAN**: A dropdown menu set to "Disabled".
- Bonjour forwarding**: A toggle switch with "Enabled" and "Disabled" buttons. The "Disabled" button is highlighted in blue.
- VLAN tagging**: A dropdown menu set to "Disabled".
- Assign group policies by device type**: A toggle switch with "Enabled" and "Disabled" buttons. The "Disabled" button is highlighted in blue.
- Adaptive policy group**: A dropdown menu set to "20: POS". This section is highlighted with a red border.

# SGT Assignment by RADIUS

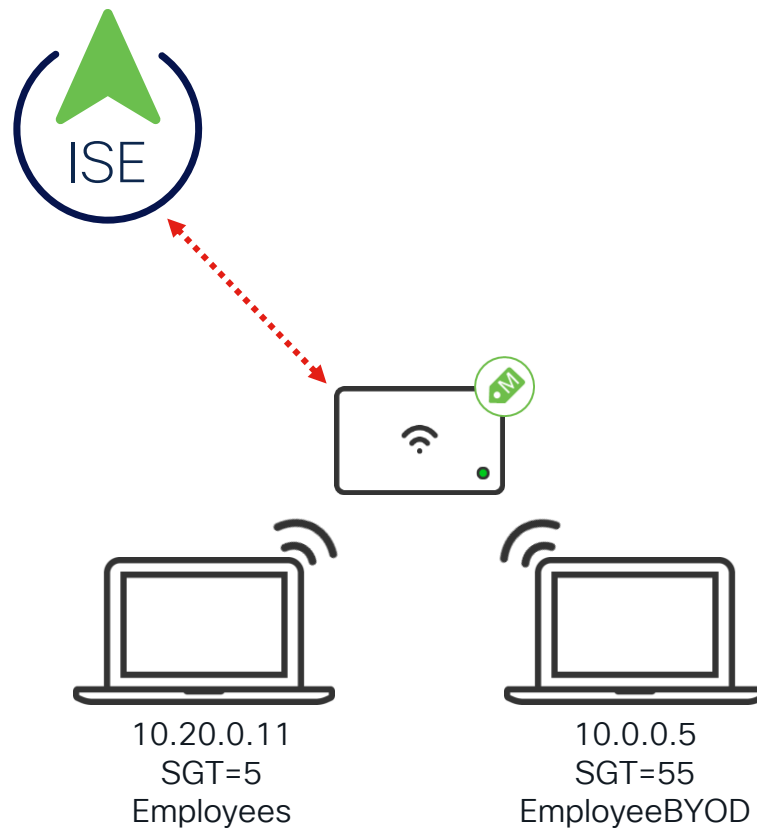
## Per-Session Assignment of SGTs

### Support

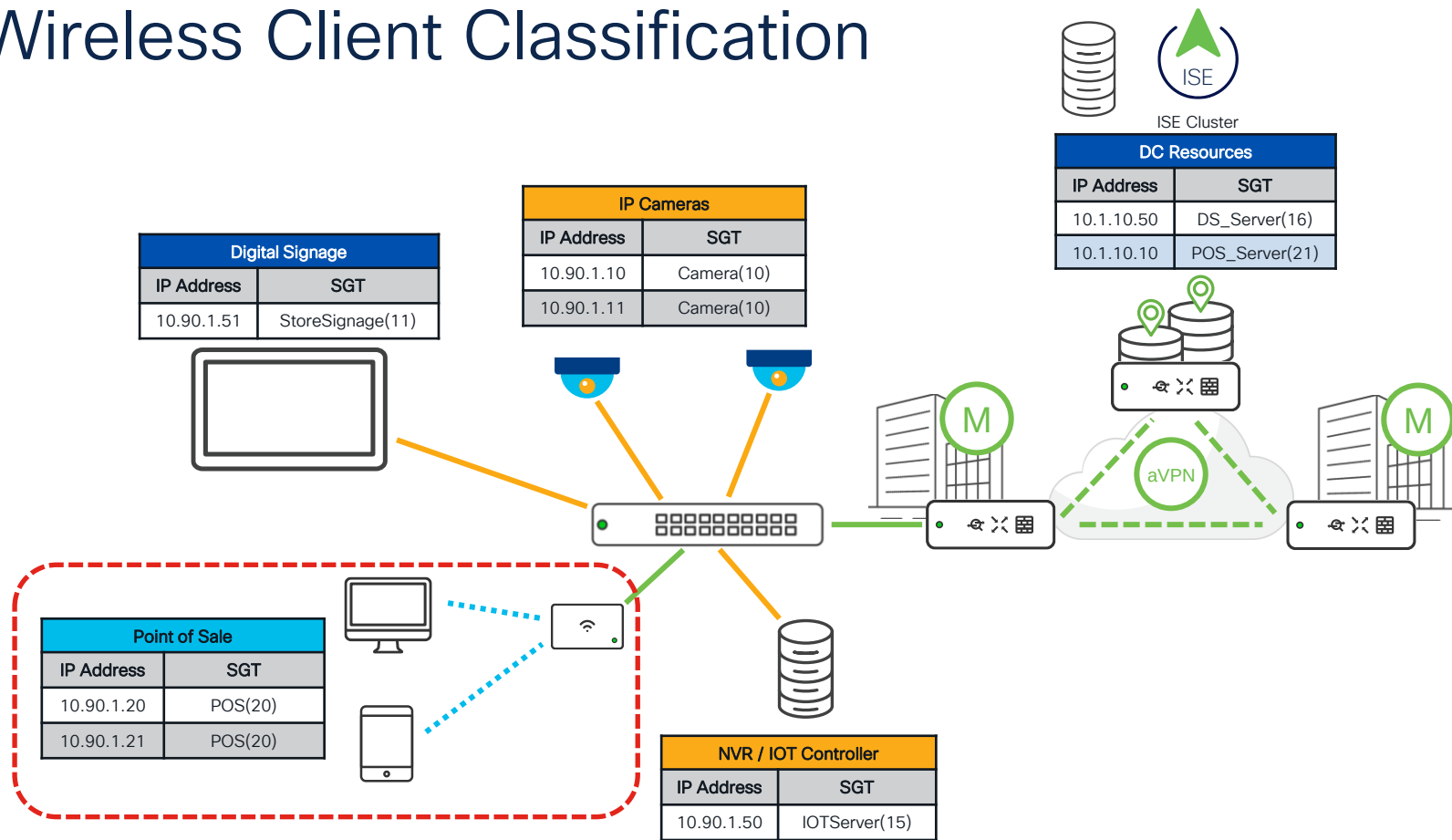
- SSIDs in bridge-mode and NAT mode
- Fallback to SSID's SGT if RADIUS does not send SGT

### Use cases

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



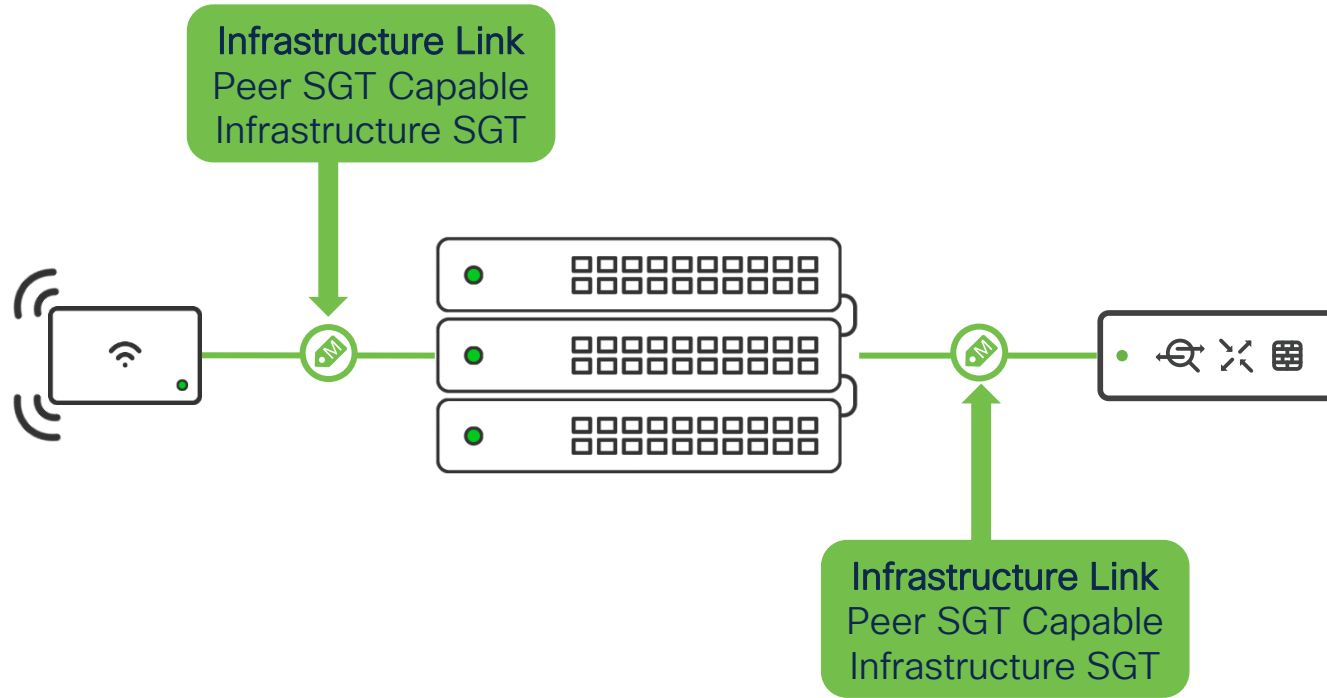
# Wireless Client Classification



# Infrastructure Link Configuration

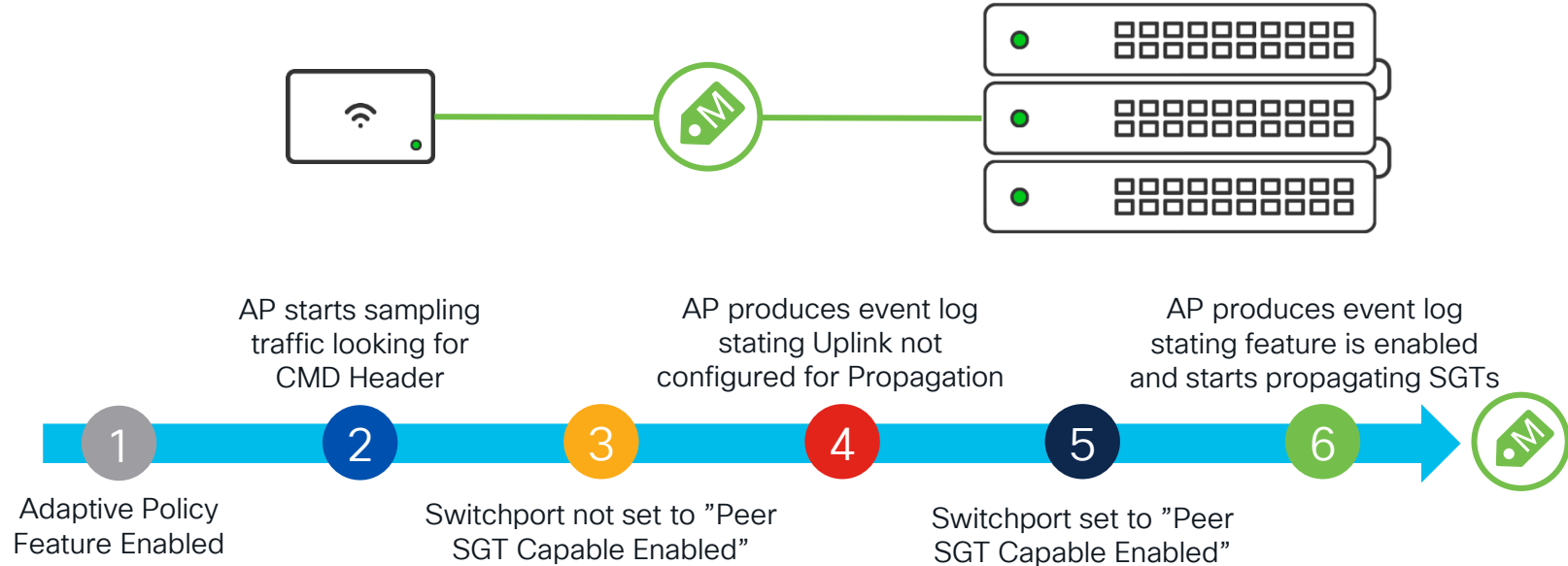


# Infrastructure Connectivity

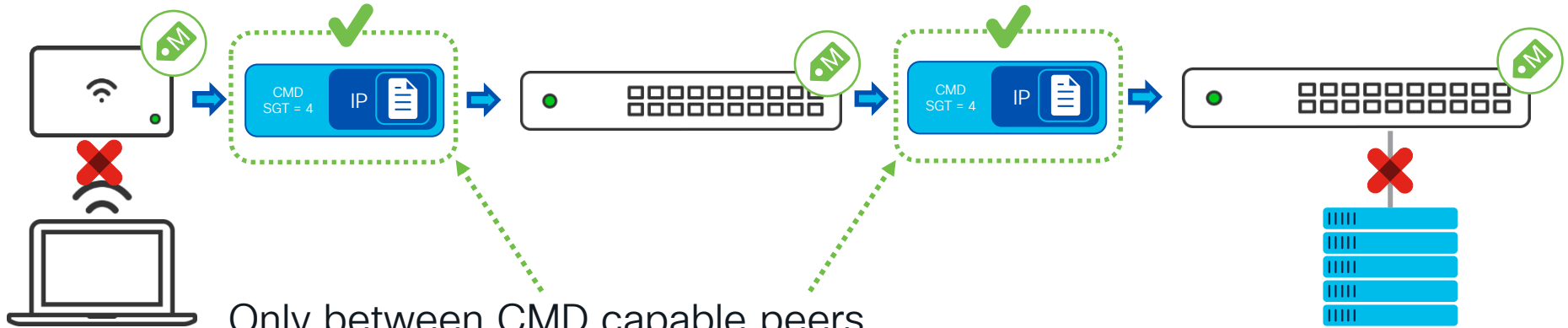


# MR/CW Adaptive Policy Enablement

*How not to strand an AP in the field*



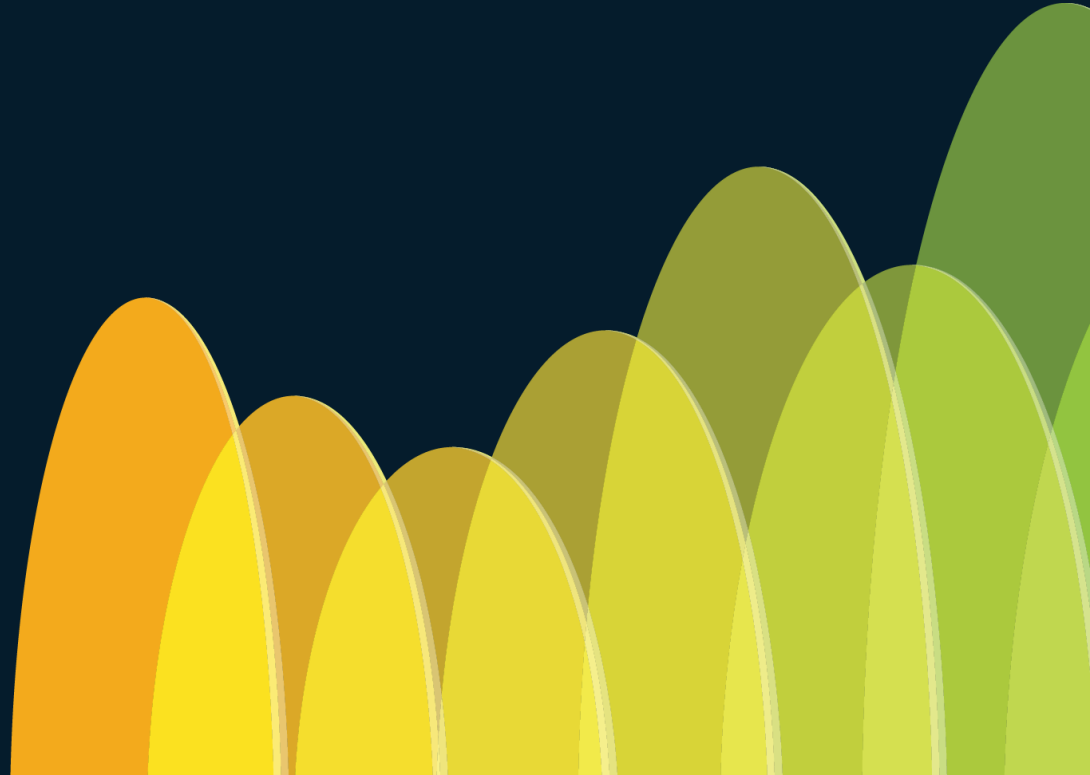
## So where do we see tags?



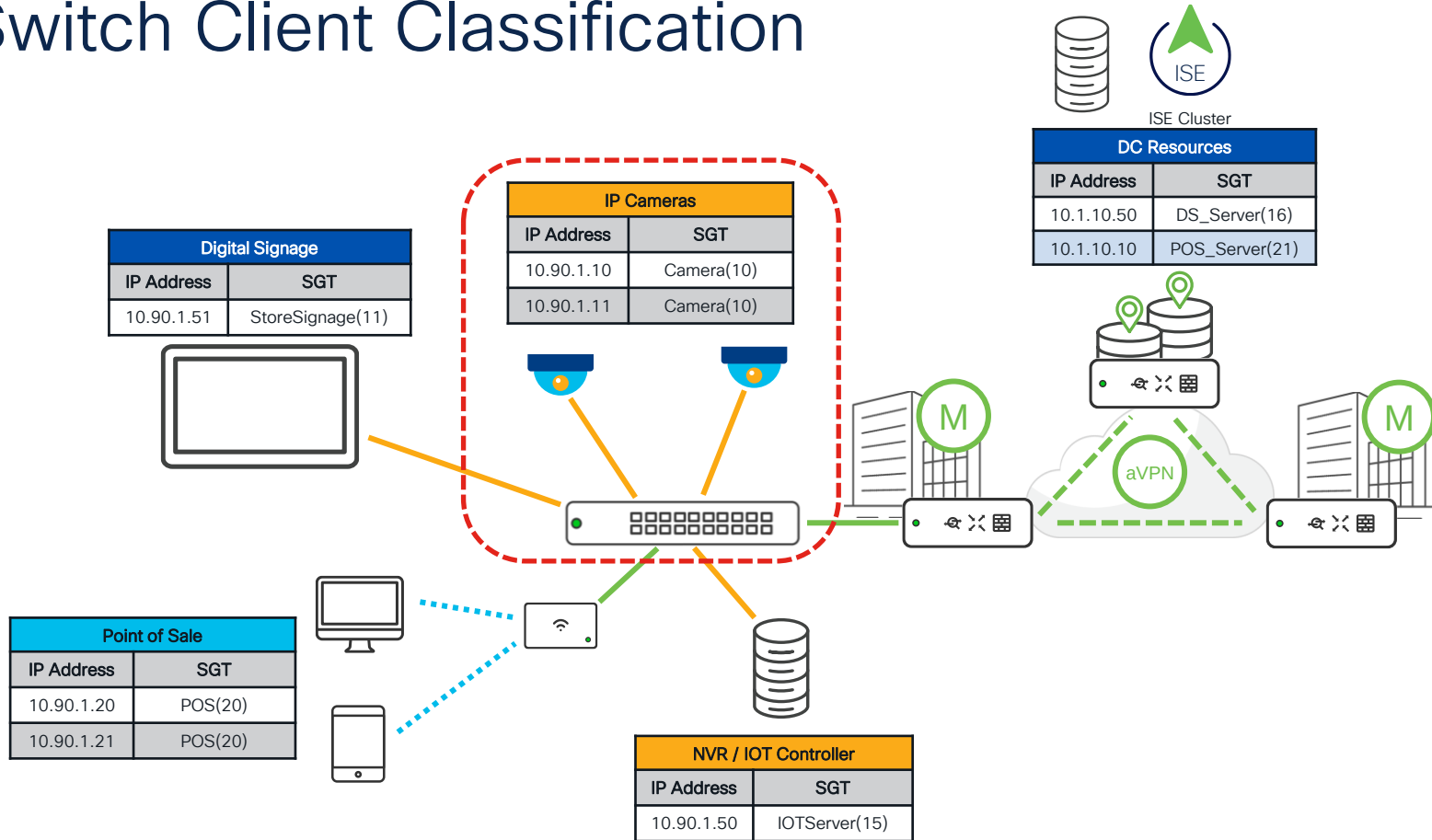
Only between CMD capable peers

Client Ports have no knowledge of SGTs or the encapsulation

# Configuring Switching Classification



# Switch Client Classification



# 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



# Adaptive Policy from Access Switching to Aggregation/Core

## Fiber aggregation



C9300X-12Y/24Y



C9300-24S/48S

## Access



MS130X/R

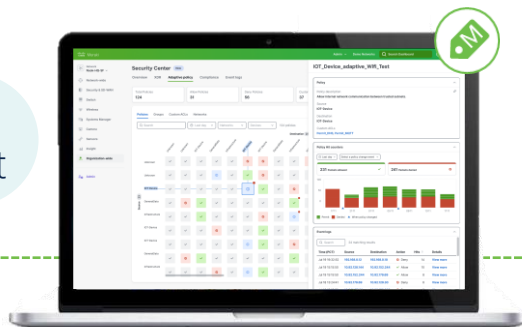


MS390



Catalyst 9K-M

ONE dashboard  
ANY environment



Rugged



MS130R

Compact



MS130X

Rack Mount



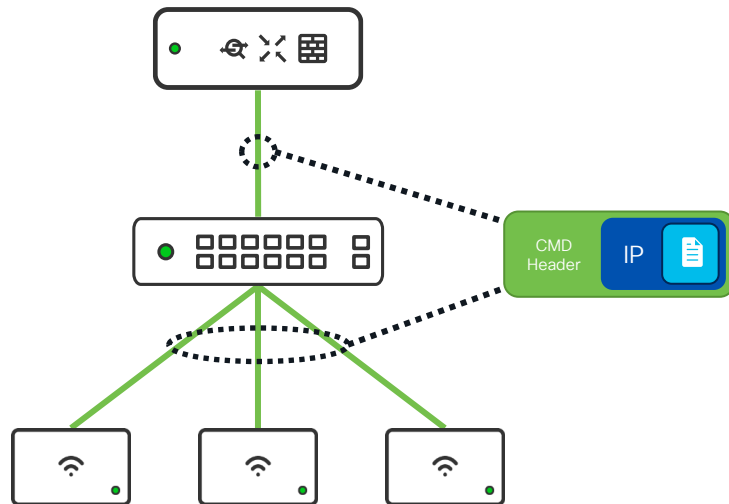
Most Demanding



Catalyst Meraki  
9300/X

Extending **adaptive policy** to **more** platforms

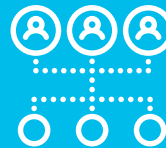
# MS130X/R SGT Interoperability and Scaling



Standard CMD Support  
interoperable with any inline  
SGT capable network device



60x SGTs



400x Directly  
Classified Endpoints

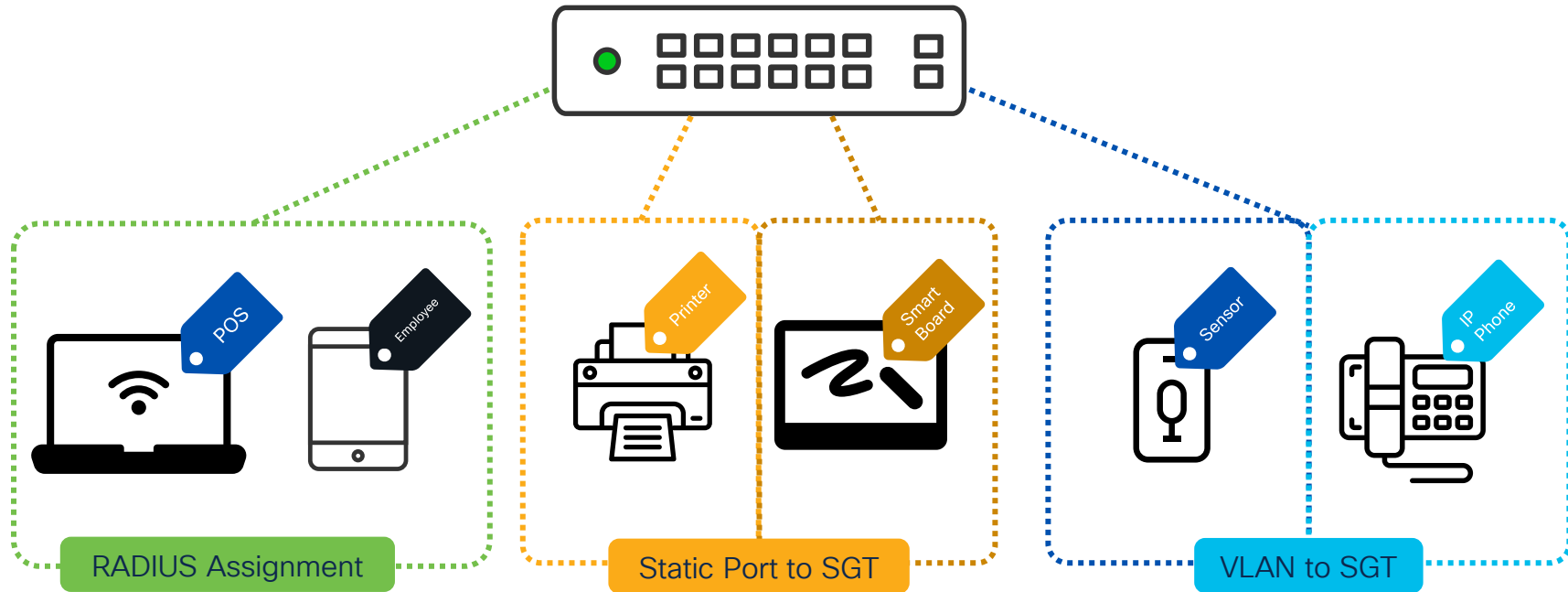


3600x Policies  
1000x Unique ACEs



100x VLAN to SGT  
Per VLAN Profile

# MS130X/R Adaptive Policy SGT Classification



# 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 and other SGT capable platforms

## 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

# 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

# VLAN to SGT (MS/CS)

### Edit profile

Profile name

Iname

Default

#### VLAN name

[+ Add Named VLAN](#)

| # | VLAN name   | VLAN ID                          | Adaptive policy group                          | Actions |
|---|-------------|----------------------------------|------------------------------------------------|---------|
| 1 | GUEST       | <input type="text" value="110"/> | <input type="text" value="666 : Guest"/>       |         |
| 2 | Data        | <input type="text" value="1"/>   | <input type="text" value="100 : Employees"/>   |         |
| 3 | Voice       | <input type="text" value="2"/>   | <input type="text" value="50 : VoIP"/>         |         |
| 4 | Contractors | <input type="text" value="3"/>   | <input type="text" value="200 : Contractors"/> |         |
| 5 | IOT         | <input type="text" value="4"/>   | <input type="text" value="10 : IOT"/>          |         |

#### Group name

[+ Add VLAN Group](#)

| #                     | Group Name | VLAN list | Actions |
|-----------------------|------------|-----------|---------|
| <div> No record</div> |            |           |         |

## 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 not found

# SGT Assignment Order of Operation



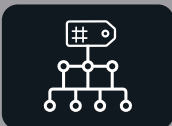
RADIUS SGT Assignment



Port SGT Assignment



IP / Subnet SGT Assignment

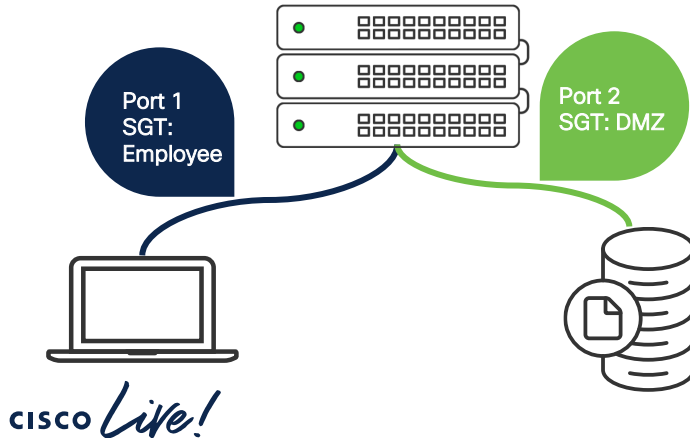


VLAN SGT Assignment

# 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

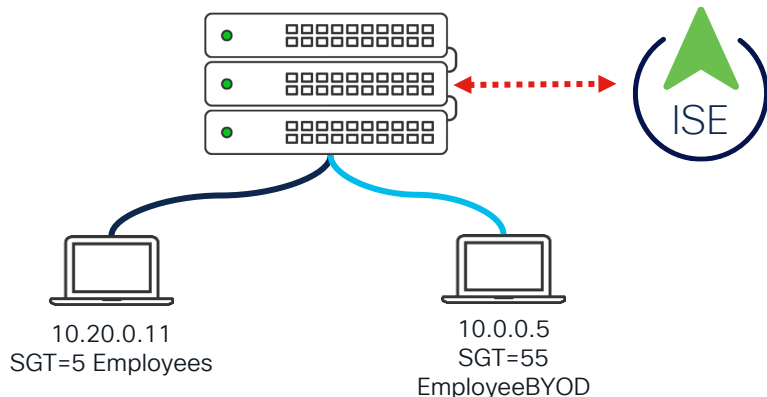
Storm control Enabled Disabled

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.

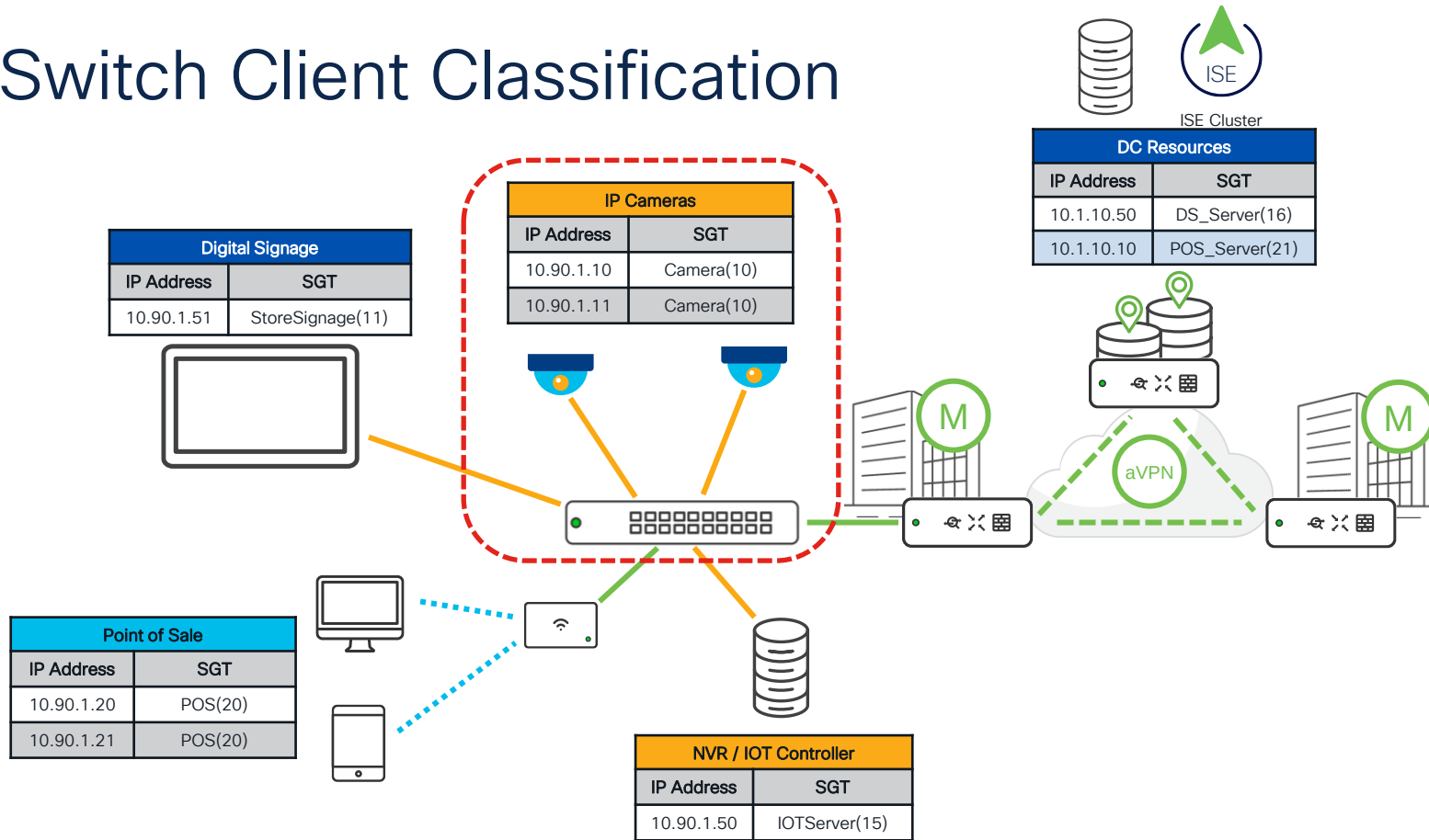
PoE: **Enabled** Disabled

Adaptive policy group ⓘ: Select...

Storm control: **Enabled** Disabled

Cancel Update

# Switch Client Classification



# Simple Policy Definition



# 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 341 DENY POLICIES 221/341 ALLOW POLICIES 99/341 GROUPS 20 ACLS 4

Search... Add Policies

| <input type="checkbox"/> | Source Group   | Destination Group | Permission | Policy Name                   | Last update ▲      |
|--------------------------|----------------|-------------------|------------|-------------------------------|--------------------|
| <input type="checkbox"/> | Unknown        | AlexOffice        | ✓ Allow    | Unknown - AlexOffice          | Feb 14, 2024 15:13 |
| <input type="checkbox"/> | Infrastructure | AlexOffice        | ✓ Allow    | Infrastructure - AlexOffice   | Feb 14, 2024 15:15 |
| <input type="checkbox"/> | AlexOffice     | Unknown           | ✓ Allow    | AlexOffice - Unknown          | Feb 20, 2024 16:41 |
| <input type="checkbox"/> | AlexOffice     | Infrastructure    | ✓ Allow    | AlexOffice - Infrastructure   | Feb 20, 2024 16:41 |
| <input type="checkbox"/> | OT Device      | Network Services  | ✗ Deny     | OT Device - Network Services  | May 22, 2024 18:46 |
| <input type="checkbox"/> | OT Device      | Domain Controller | ✗ Deny     | OT Device - Domain Controller | May 22, 2024 18:46 |

# One to One or One to Many

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

## Adaptive policy

POLICIES

### Add Policies

#### Source groups

IOT

| <input checked="" type="checkbox"/> | Name ▾     | SGT Value | Description         |
|-------------------------------------|------------|-----------|---------------------|
| <input checked="" type="checkbox"/> | IOT Server | 15        | IOT and NVR Servers |

#### Destination groups

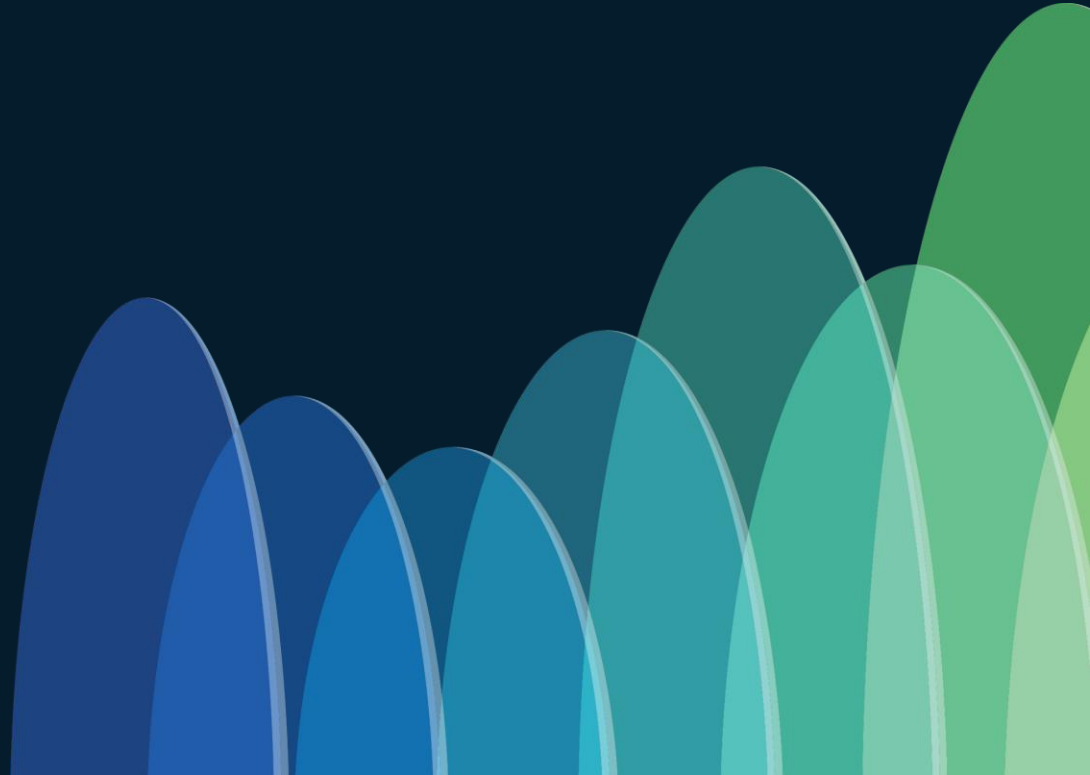
Search...

0 policies selected

☒ Allow ☒ Deny ☒ Custom

| <input type="checkbox"/> | Name          | SGT Value | Description                                                             |
|--------------------------|---------------|-----------|-------------------------------------------------------------------------|
| <input type="checkbox"/> | AlexOffice    | 6         | Alex's Office devices                                                   |
| <input type="checkbox"/> | Employees     | 100       | Users with Corporate Managed Devices                                    |
| <input type="checkbox"/> | Contractors   | 200       | Temporary Contractor Access                                             |
| <input type="checkbox"/> | Guest         | 666       | Guest Users                                                             |
| <input type="checkbox"/> | VoIP          | 50        | Voice Over IP                                                           |
| <input type="checkbox"/> | POS           | 20        | Point of Sale Devices                                                   |
| <input type="checkbox"/> | POS Server    | 21        | Point of Sale Server                                                    |
| <input type="checkbox"/> | OT Controller | 23        | PLC Controllers                                                         |
| <input type="checkbox"/> | Quarantine    | 563       | Complete Quarantine                                                     |
| <input type="checkbox"/> | Remediation   | 564       | Devices that need to be remediated before getting access to the network |

# MX and AutoVPN enablement



# MX/Z Supported Models and Firmware

[MX/Z Documentation and Support](#)

## 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 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

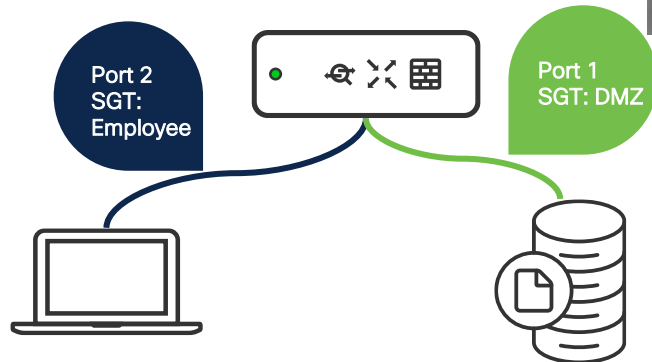
Enabled: Enabled

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 for traffic ingress on a port where:

- There is no SGT configuration defined on the port

Supported in MX18.2+

### Modify VLAN

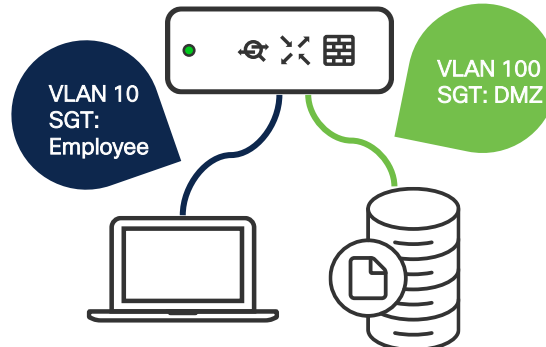
VLAN name  
DMZ

VLAN ID  
100

Group policy  
None

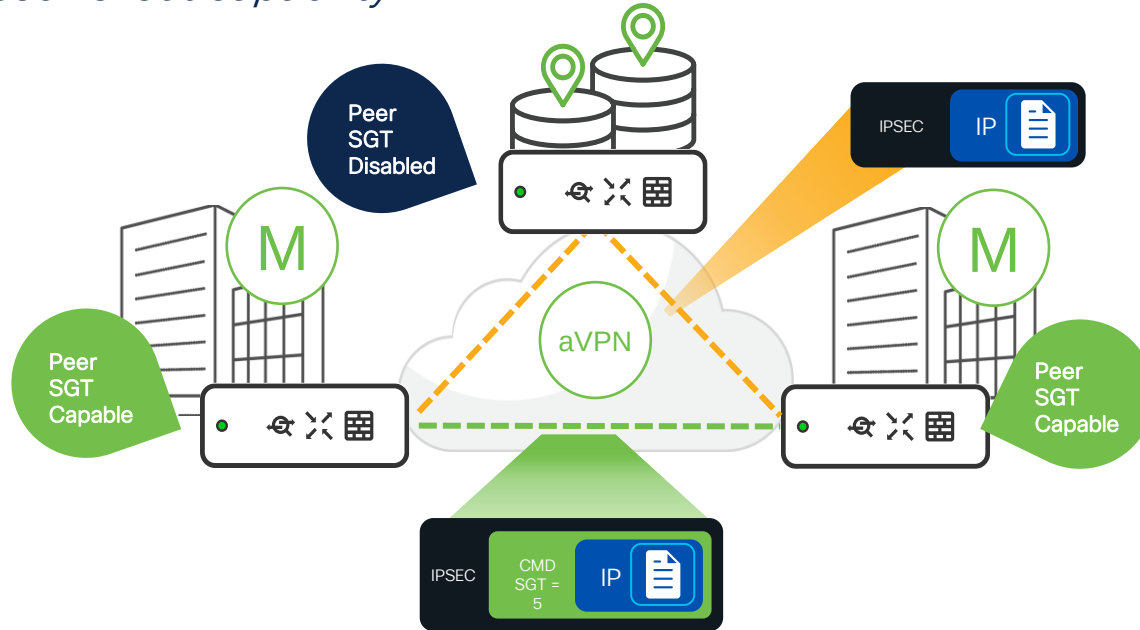
Adaptive policy group  
999: DMZ\_Clients

Next



# 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

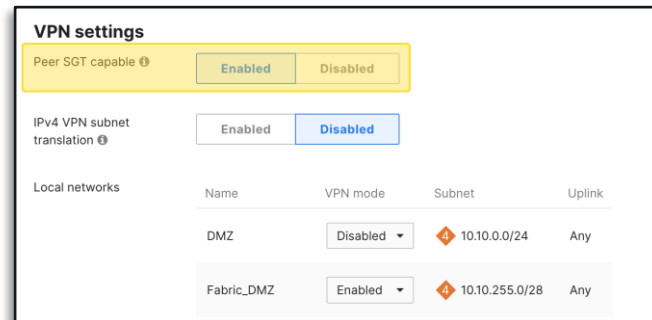
**Step 3:** Convert downlink to Trunk and enable Peer SGT Capable + Infrastructure SGT (when connected to a supported switch or access point)

Step 2

Tells all VPN peers it can receive SGT encapsulated traffic

Step 3

Propagates SGTs from VPN to Port Trusts incoming tagged traffic

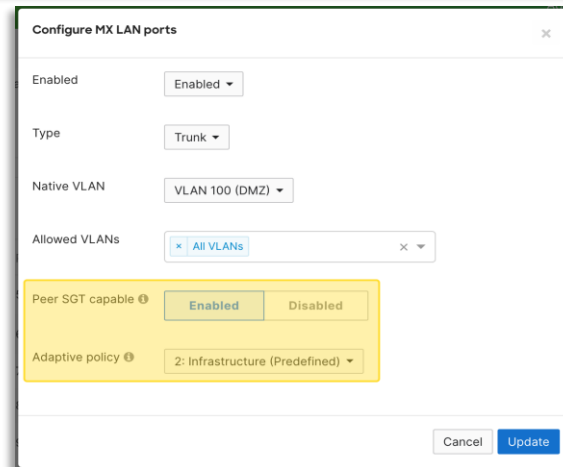


**VPN settings**

Peer SGT capable ⓘ Enabled Disabled

IPv4 VPN subnet translation ⓘ Enabled Disabled

| Local networks | Name       | VPN mode              | Subnet         | Uplink |
|----------------|------------|-----------------------|----------------|--------|
|                | DMZ        | <span>Disabled</span> | 10.10.0.0/24   | Any    |
|                | Fabric_DMZ | <span>Enabled</span>  | 10.10.255.0/28 | Any    |



**Configure MX LAN ports**

Enabled Enabled

Type Trunk

Native VLAN VLAN 100 (DMZ)

Allowed VLANs All VLANs

Peer SGT capable ⓘ Enabled Disabled

Adaptive policy ⓘ 2: Infrastructure (Predefined)

Cancel Update

# Integrations across the Cisco portfolio

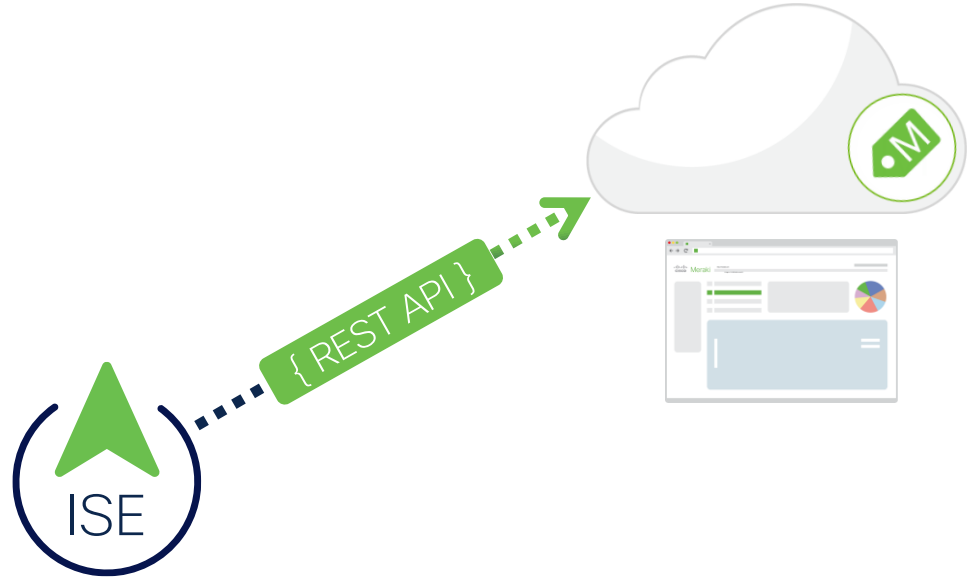


# Native Policy Syncing to Dashboard in ISE 3.2 P1

Using Dashboard APIs

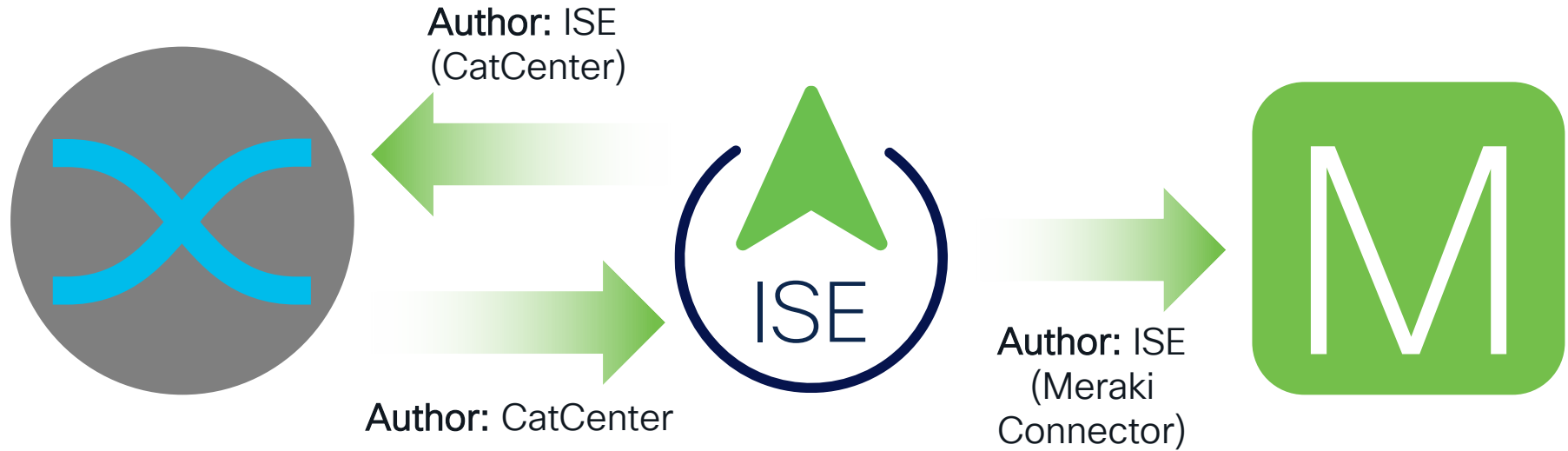
Pushed directly from ISE

Single Source of Truth



| SRC   DST  | Employee | IoT | IoT Server |
|------------|----------|-----|------------|
| Employee   | ✓        | ✗   | ✗          |
| IoT        | ✗        | ✗   | ✓          |
| IoT Server | ✗        | ✓   | ✓          |

# Catalyst Center $\Leftrightarrow$ ISE $\Rightarrow$ Meraki

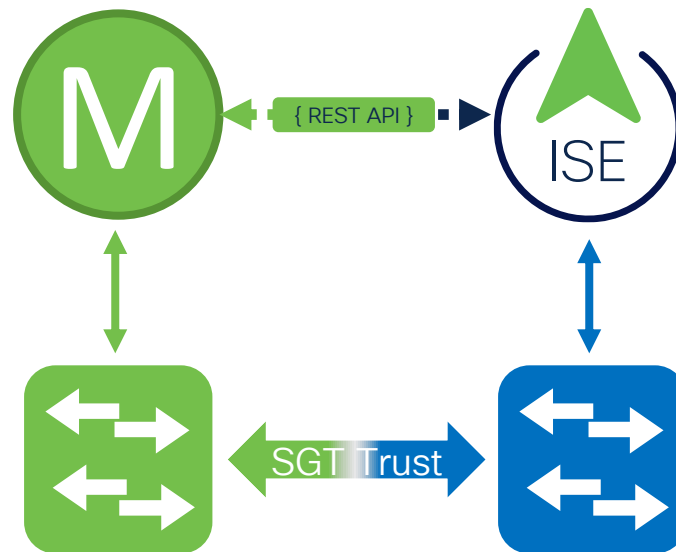


# Adaptive Policy and TrustSec

Native Rest API syncing between Dashboard and ISE

Tag trust at the data-plane interconnect

Context and policy shared between architectures



# Adaptive Policy & Secure Network Analytics

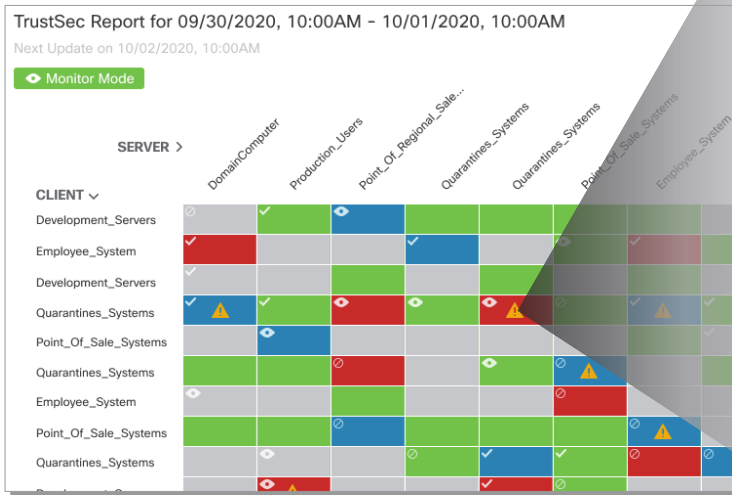
*Informed policy creation and validation*



Global flow visibility  
and context



Group based policy  
and traffic flow



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

# Meraki NetFlow Exporters



| Product Line | Protocol Support                              |
|--------------|-----------------------------------------------|
| MX/Z         | NetFlow v9                                    |
| MS390/C9K-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 | <input checked="" type="checkbox"/>        |
| ETA collector port          | 9996                                       |

*Requires Advanced Licensing*

**CISCO** *Live!*

# C9300-M/MS390 NetFlow v10 (IPFIX) & ETA



NetFlow / IPFIX



| Match          | Collect                                                                   |  |  |
|----------------|---------------------------------------------------------------------------|--|--|
| Application    | Security Group Tag                                                        |  |  |
| SRC/DST IP     | Connection Client Location (IP, Port, Direction, VLAN, Observation Point) |  |  |
| SRC Interface  | Connection Client Counters (Bytes, Packets, Timestamps, TCP flags)        |  |  |
| SRC / DST Port | Connection State (Server, Source Port, Dest Port, Initiator)              |  |  |
| Protocol       | Encrypted Traffic Analytics                                               |  |  |
|                | Initial Data Packet                                                       |  |  |
|                | Sequence of Packets Lengths and Times                                     |  |  |
|                | Byte Distribution                                                         |  |  |

# MS390 with SNA & ISE



Telemetry provided by MS390/9300-M to SNA



Flexible outcomes: Policy Violation



Trigger CoA via ISE

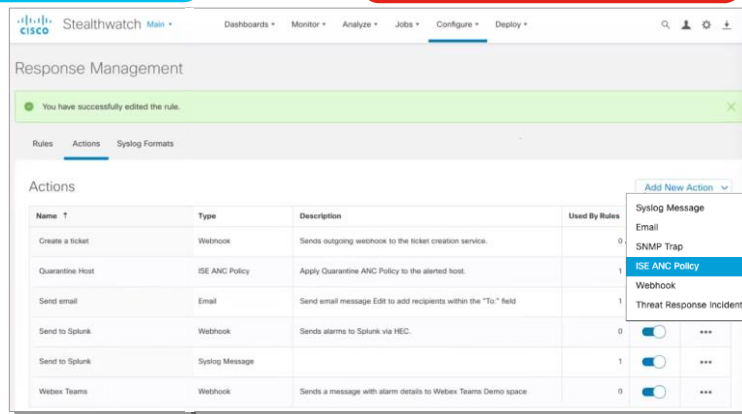


NetFlow & ETA

RADIUS CoA



ISE PxGrid ANC



# Adaptive Policy and ASA/Firepower

**Add Rule**

Name: Block HR to Accounting ☒ Enabled

Insert: below rule 1

Action: Block

Time Range: None

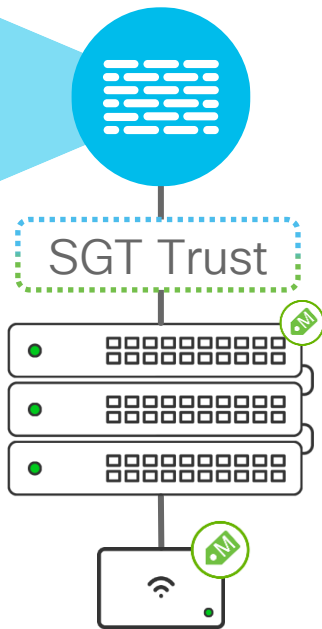
Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Metadata: Search by name or value, Security Group Tag, Acct, ANY, HR

Selected Source Metadata (1): HR

Selected Dest Metadata (1): Acct

Buttons: Cancel, Add

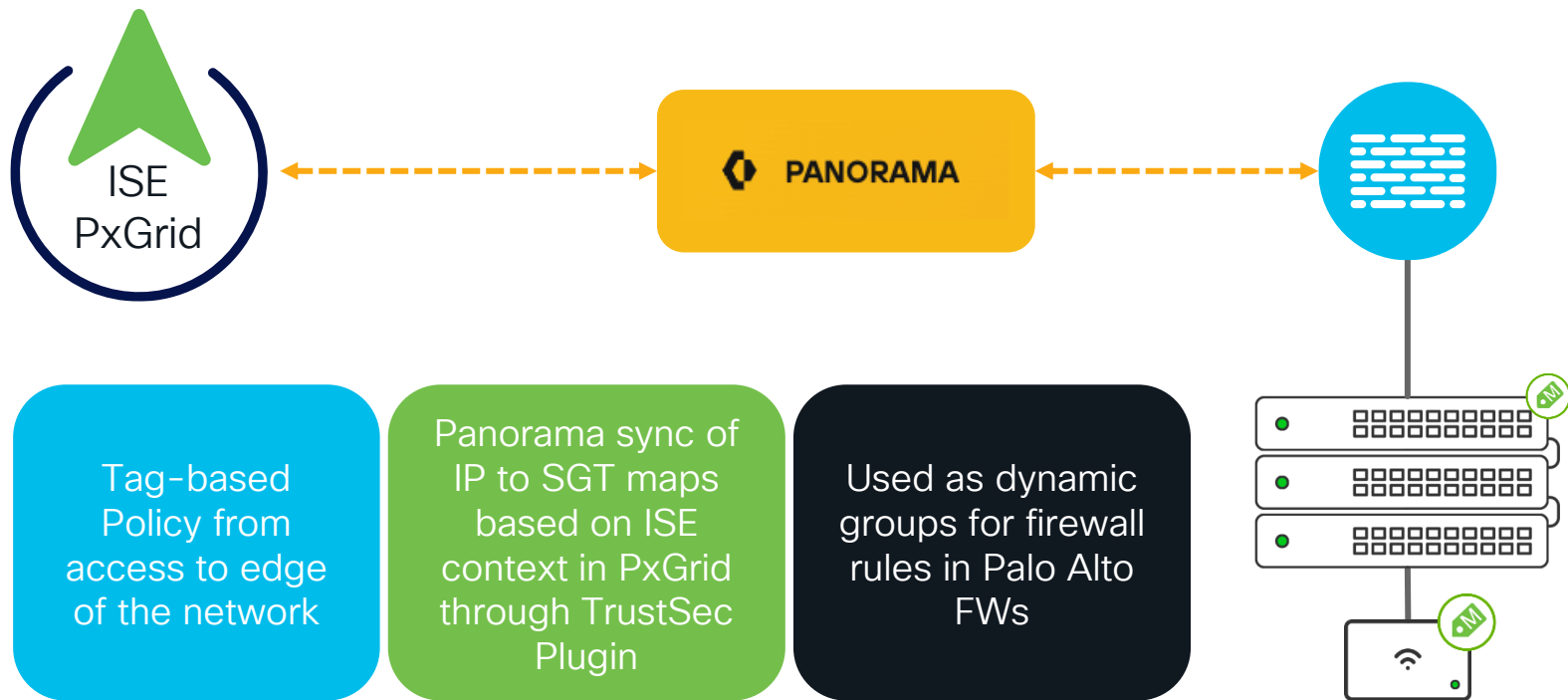


Tag-based  
Policy from  
access to edge  
of the network

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

Rules based on  
data-plane  
context sharing  
via SGTs

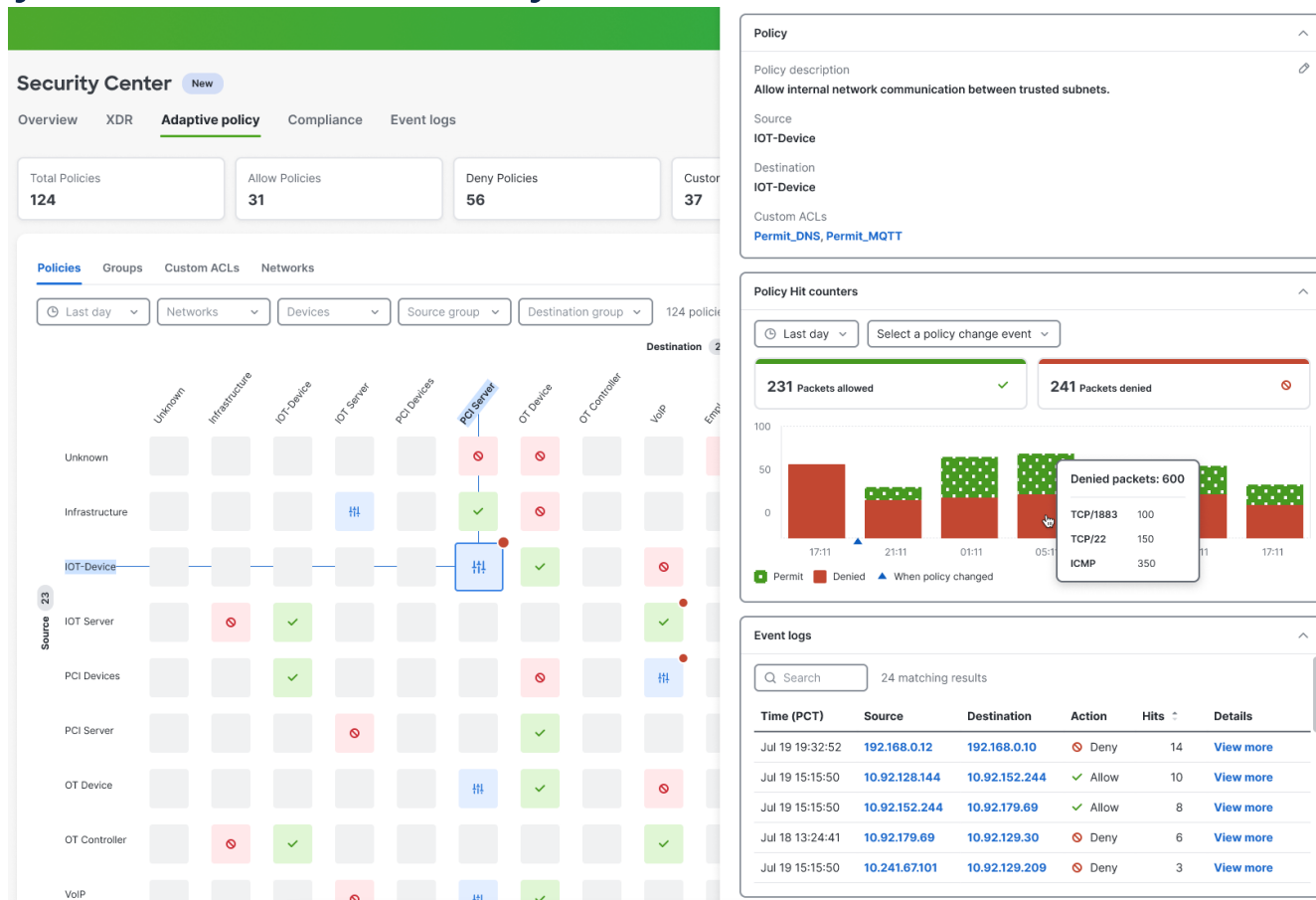
# Adaptive Policy and Palo Alto Panorama



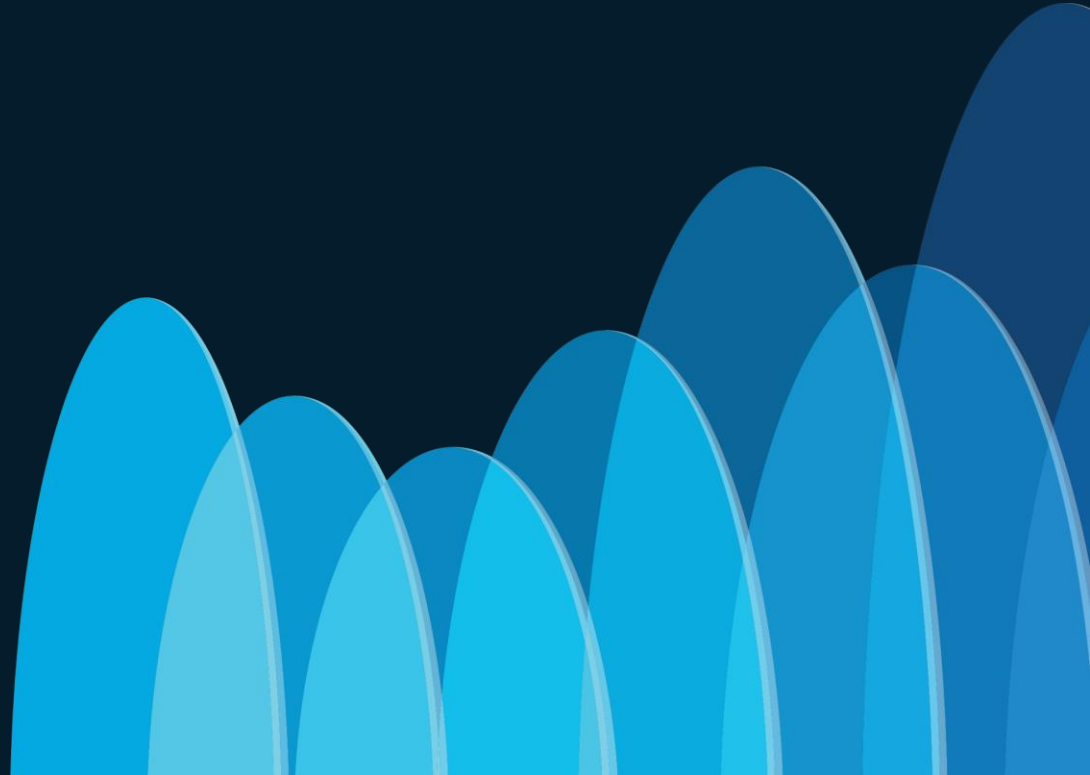
# Adaptive Policy Matrix and Policy Visualisation

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



# Conclusion



# Keynote Deep Dives

**Wednesday**  
**10:30am – 11:30am**



Experiences Amplified:  
How AI Can Fuel Better Employee and Customer Experiences

**Level 1**  
**Room 106**



Smart, Secure, Seamless:  
Transforming Experiences with Next-Generation Networking

**Level 2**  
**Room 204**



Harness a Bold New Era:  
Transform Data Centre and Service Provider Connectivity

**Level 2**  
**Room 203**



Securing User to Application and Everything in Between

**Level 2**  
**Melbourne Room 2**



Unlocking Digital Resilience through Unified Observability

**The HUB**  
**Centre Stage**

# Complete Your Session Evaluations



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

---



Complete your surveys in the **Cisco Live mobile 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 DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



# Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC