Let’s go

The bridge to possible

Harnessing Identity-Based Firewalling on the Meraki MX

Powered by the Meraki Full Stack

Chris Weber, Product Manager – Meraki MX Security
Linkedin: christopherwweber/

An analogy for Full Stack Identity-Based Security

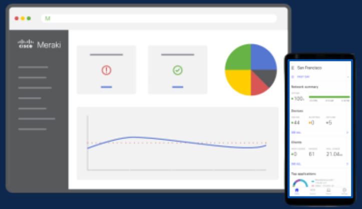
Company X
Company Y
Company Z
TEAMBUILDING
WELCOME
Restricted Space
Restricted Space
Main Entrance

Agenda

- What are Group Policies?
- Full Stack Identity with 802.1x
- Full Stack Identity with Adaptive Policy
- Sentry Policies with Systems Manager
- Passive Identity with Active Directory
- Zero Trust with Secure Connect

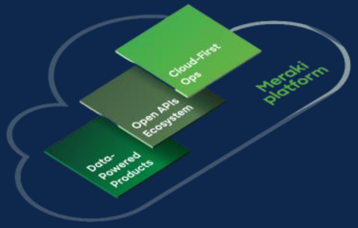
Cisco’s Meraki platform for the secure cloud managed branch

3x
larger than competitors



MERAKI DASHBOARD

Built-in solutions



API

Tailored solutions

CUSTOM BUILT

developer.cisco.com/meraki

TECH PARTNERS

meraki.com/marketplace

Wireless

Switching

Mobile Device Management

Firewall and SD-WAN

Cellular Gateways

Smart Cameras

IoT Sensors

ACCESS & ENDPOINT

SECURITY AND IOT

15 years of helping customers and partners deliver exceptional secure network experiences

700K+
Customers

99.99%
Cloud SLA

5+
MILLION
Customer networks

15+
MILLION
Meraki devices online

190+
Countries in network

8+
BILLION
External API monthly calls

2+
MILLION
Firewalls Deployed

8+
TRILLION
Flows secured per week

25+
BILLION
Threats Blocked per Month

400+
THOUSAND
Secure Client Users Per Day

40+
THOUSAND
SD-WAN Customers

Born in the cloud, growing daily, and
trusted everywhere

Full Stack Identity-Based Security

What are Group Policies?

Foundation For Full-Stack identity-based Security Policies

Open Question

“Groups”

Forms of network segmentation + groups of users

(e.g. VLANs, subnets, SSIDs, SM tags, AD, SGT)

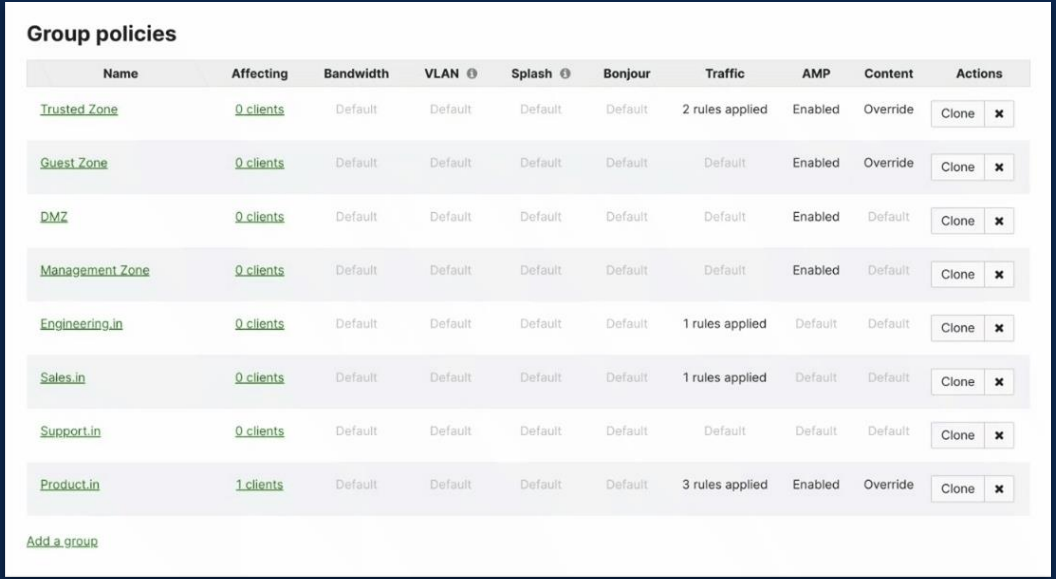
“Policies”

Rules that will actively or passively affect network traffic or end client functionality

(e.g. firewall, content filtering, AMP, SSL Decrypt, QoS, MDM)

Group Policies

Foundation to identity-based Security Policy Enforcement Across Meraki



Group policies

Name	Affecting	Bandwidth	VLAN	Splash	Bonjour	Traffic	AMP	Content	Actions
Trusted Zone	0 clients	Default	Default	Default	Default	2 rules applied	Enabled	Override	Clone ✖
Guest Zone	0 clients	Default	Default	Default	Default	Default	Enabled	Override	Clone ✖
DMZ	0 clients	Default	Default	Default	Default	Default	Enabled	Default	Clone ✖
Management Zone	0 clients	Default	Default	Default	Default	Default	Enabled	Default	Clone ✖
Engineering.in	0 clients	Default	Default	Default	Default	1 rules applied	Default	Default	Clone ✖
Sales.in	0 clients	Default	Default	Default	Default	1 rules applied	Default	Default	Clone ✖
Support.in	0 clients	Default	Default	Default	Default	Default	Default	Default	Clone ✖
Product.in	1 clients	Default	Default	Default	Default	3 rules applied	Enabled	Override	Clone ✖

Add a group

Security Policies

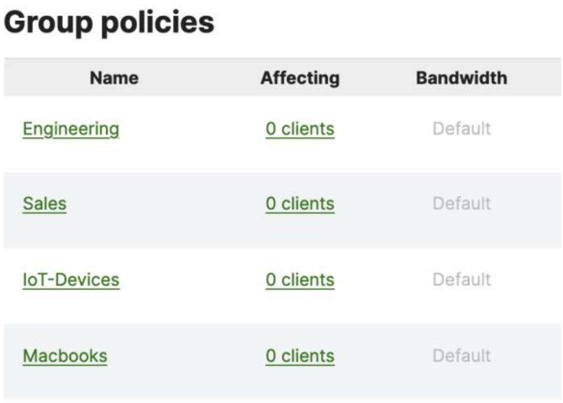
- Distributed L3 Firewall (MX/MS/MR)
- Distributed L7 Firewall (MX/MR)
- Umbrella DNS Security (MX/MR)
- Threat Protection Policies (MX):
  - AMP
  - Talos Content Filtering (content & threat categories)
  - URL Filtering
  - YouTube Filtering
  - Web Search Filtering
  - HTTPS Decryption

Network Policies

- VLAN Assignment (MR)
- QoS/Traffic Shaping (MX/MR)

Best Practices for using Group Policies

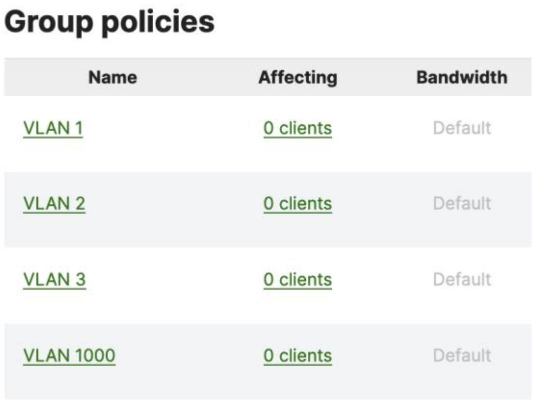
User and Device Policies



Group policies

Name	Affecting	Bandwidth
Engineering	0 clients	Default
Sales	0 clients	Default
IoT-Devices	0 clients	Default
Macbooks	0 clients	Default

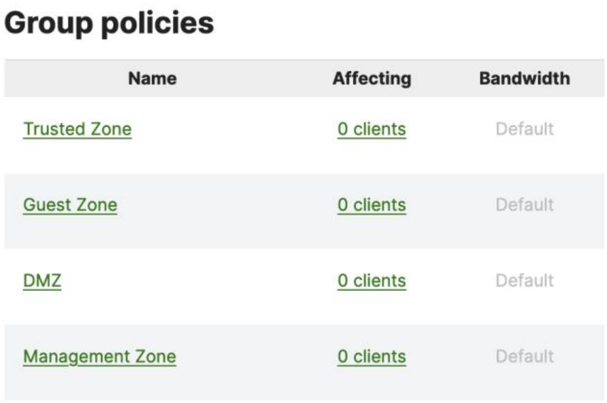
Per-VLAN Policies



Group policies

Name	Affecting	Bandwidth
VLAN 1	0 clients	Default
VLAN 2	0 clients	Default
VLAN 3	0 clients	Default
VLAN 1000	0 clients	Default

Zones-Based Policies



Group policies

Name	Affecting	Bandwidth
Trusted Zone	0 clients	Default
Guest Zone	0 clients	Default
DMZ	0 clients	Default
Management Zone	0 clients	Default

Applying Firewall & Security Policies Based on Identity

Leverage active and passive auth across the full stack to apply MX security policies based on user or role

Static Policy Assignment

Active Directory Policies

802.1x (MR/MS) with policy map sync

SM (MDM) Sentry Policies

AnyConnect or Secure Client VPN with 802.1x

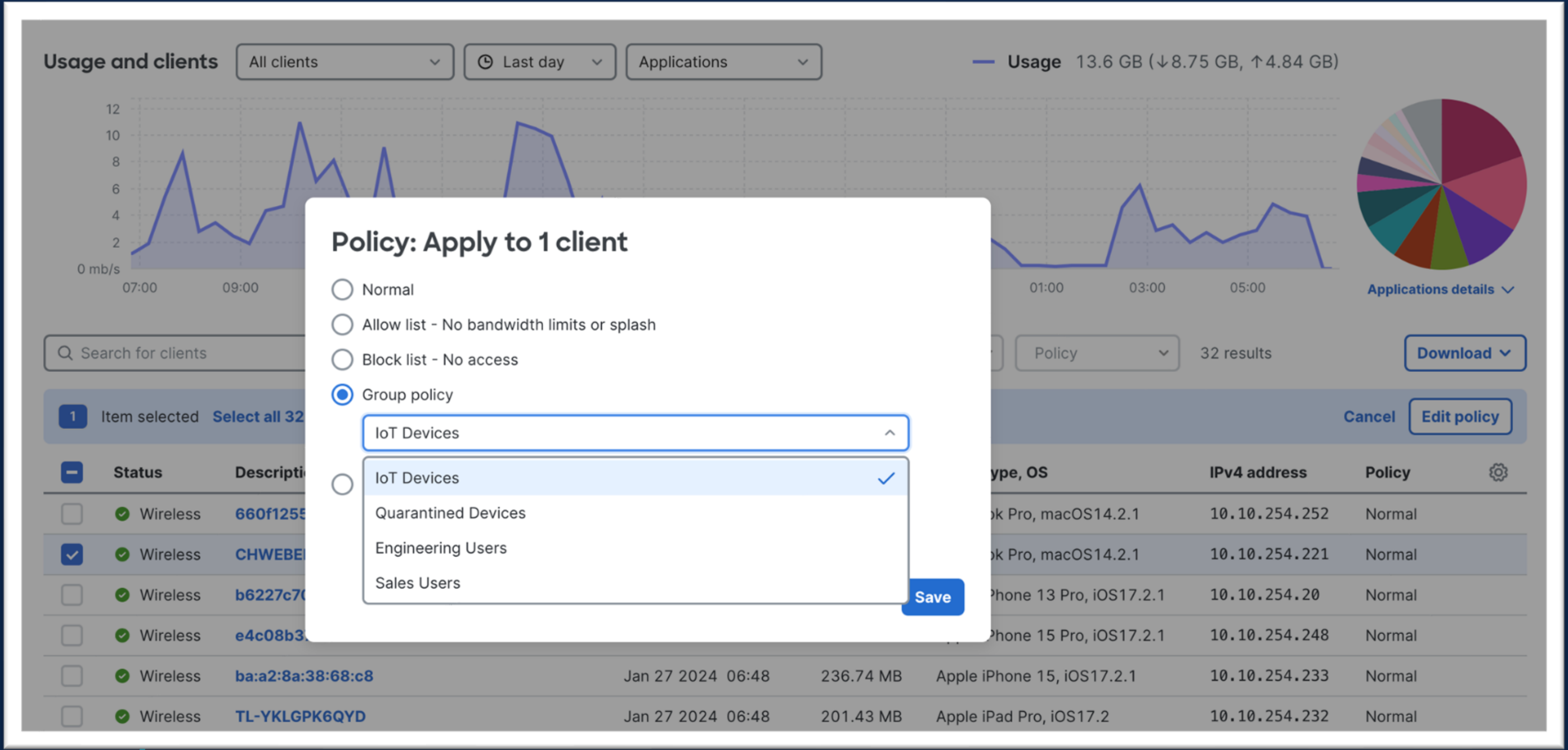
ZTNA Policies with Secure Connect

Adaptive Policy (SGT)

MX 802.1x (Port and wifi) GP Assignment

Static Group Policy Device Assignment

Useful when devices don't have a user behind them or can't do 802.1x (ex. IoT devices)



Policy: Apply to 1 client

○ Normal

○ Allow list - No bandwidth limits or splash

○ Block list - No access

● Group policy

IoT Devices

- IoT Devices ✓
- Quarantined Devices
- Engineering Users
- Sales Users

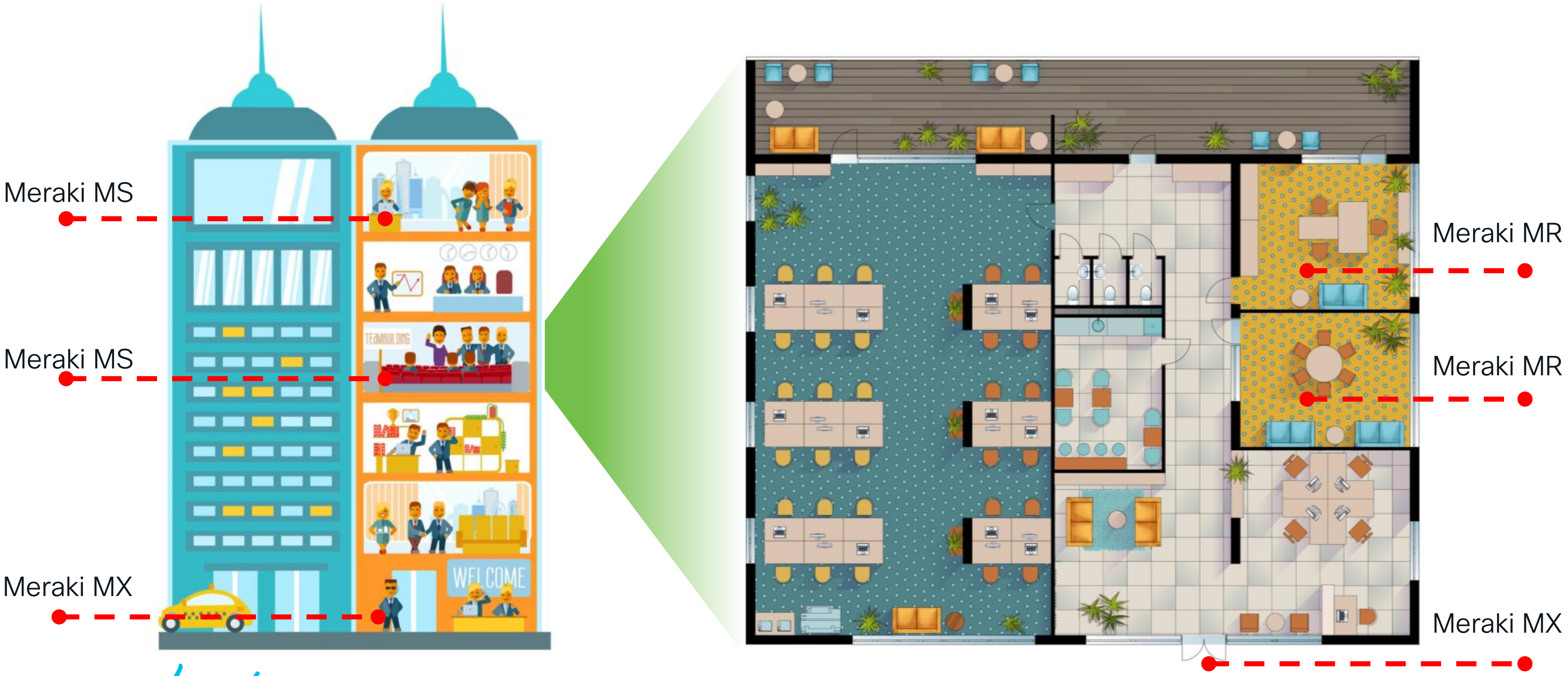
○

Save

☐	Status	Descripti			ype, OS	IPv4 address	Policy
☐	✓ Wireless	660f1255			ok Pro, macOS14.2.1	10.10.254.252	Normal
☑	✓ Wireless	CHWEBE			ok Pro, macOS14.2.1	10.10.254.221	Normal
☐	✓ Wireless	b6227c7			Phone 13 Pro, iOS17.2.1	10.10.254.20	Normal
☐	✓ Wireless	e4c08b3			Phone 15 Pro, iOS17.2.1	10.10.254.248	Normal
☐	✓ Wireless	ba:a2:8a:38:68:c8	Jan 27 2024 06:48	236.74 MB	Apple iPhone 15, iOS17.2.1	10.10.254.233	Normal
☐	✓ Wireless	TL-YKLGPK6QYD	Jan 27 2024 06:48	201.43 MB	Apple iPad Pro, iOS17.2	10.10.254.232	Normal

Identity-based Security with Full-Stack NAC (802.1x)

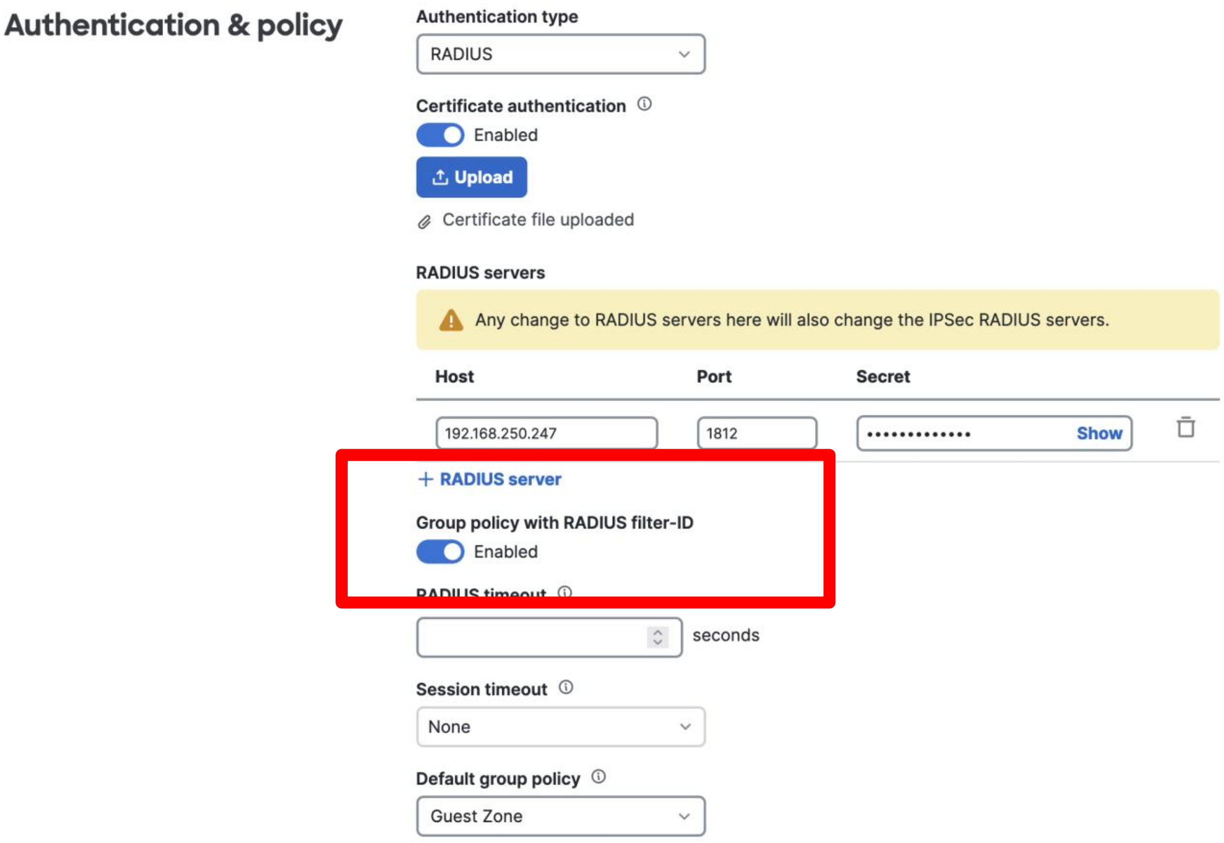
An analogy for Full Stack Identity-Based Security



cisco Meraki

How it Works

MX Firewall & Secure Client (formerly AnyConnect) RADIUS with Group Policy Assignment



Authentication & policy

Authentication type: RADIUS

Certificate authentication: Enabled

Certificate file uploaded

RADIUS servers

⚠ Any change to RADIUS servers here will also change the IPSec RADIUS servers.

Host	Port	Secret
192.168.250.247	1812	•••••••••••••• Show

Group policy with RADIUS filter-ID: Enabled

RADIUS timeout: seconds

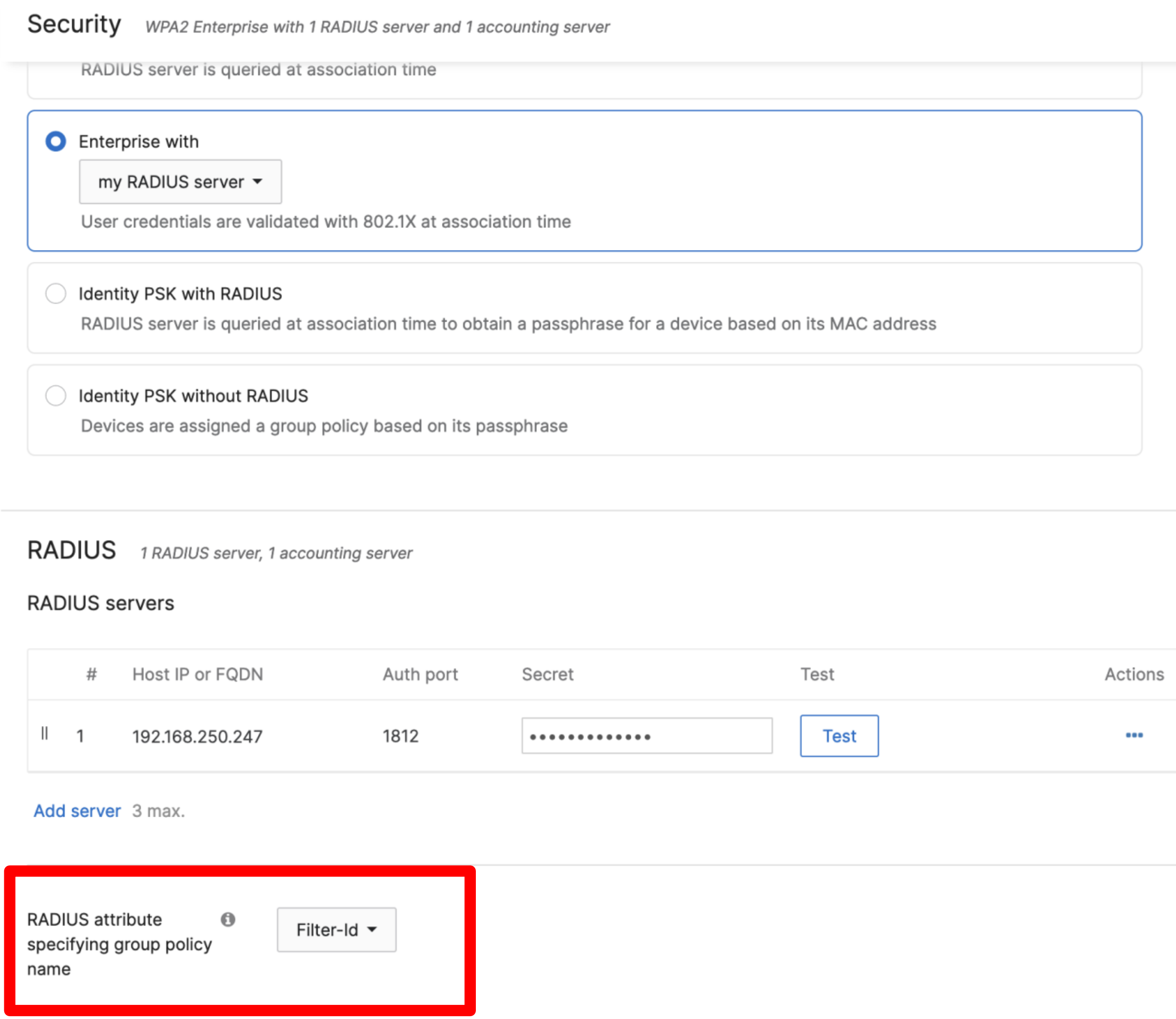
Session timeout: None

Default group policy: Guest Zone

cisco Live!

How it Works

Wireless SSID RADIUS with Group Policy Assignment



Security *WPA2 Enterprise with 1 RADIUS server and 1 accounting server*

RADIUS server is queried at association time

● Enterprise with

my RADIUS server ▾

User credentials are validated with 802.1X at association time

○ Identity PSK with RADIUS

RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

○ Identity PSK without RADIUS

Devices are assigned a group policy based on its passphrase

RADIUS *1 RADIUS server, 1 accounting server*

RADIUS servers

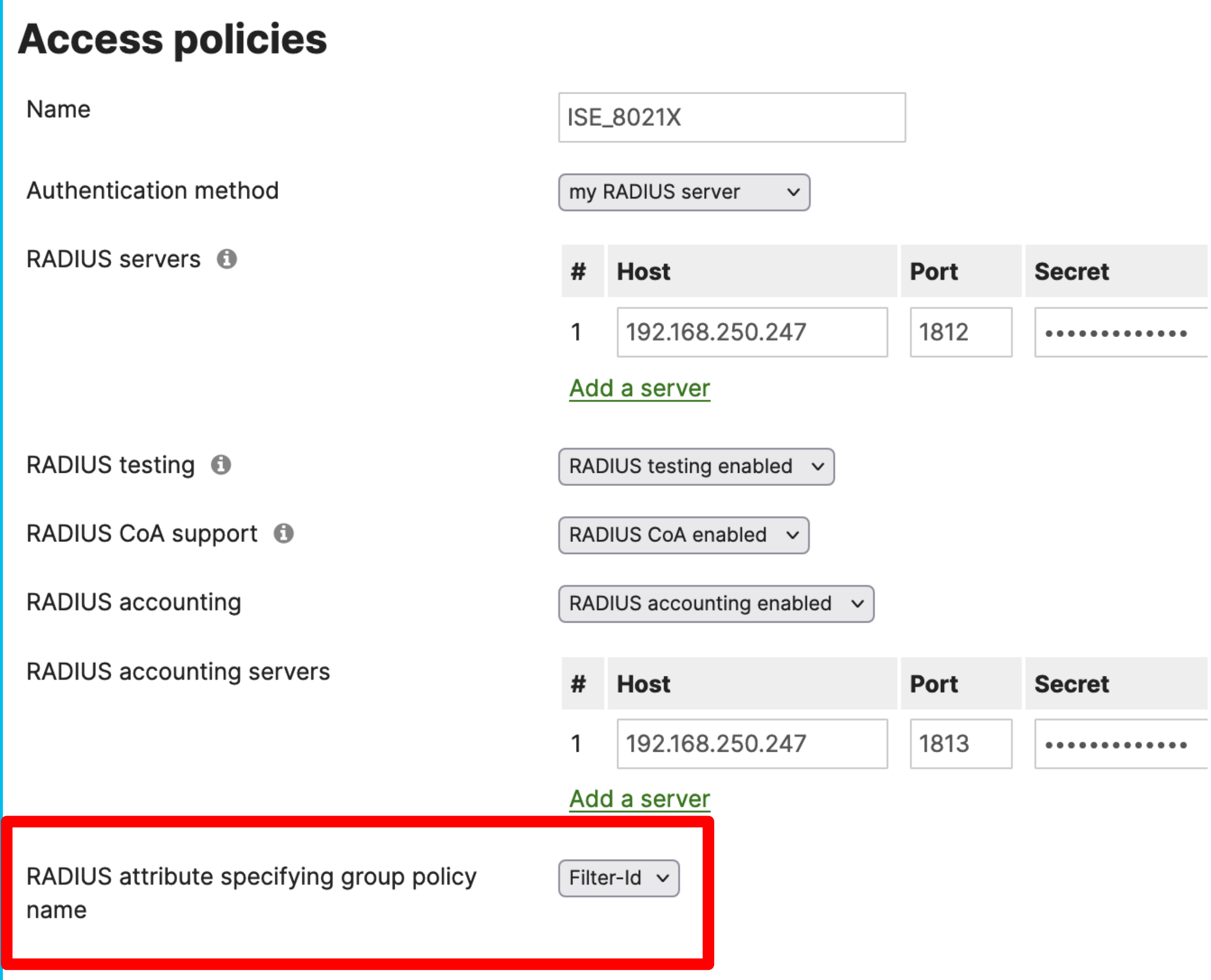
#	Host IP or FQDN	Auth port	Secret	Test	Actions
1	192.168.250.247	1812	•••••••••••••	Test	•••

Add server 3 max.

RADIUS attribute specifying group policy name: Filter-Id ▾

How it Works

Switchport RADIUS with Group Policy Assignment



Access policies

Name: ISE_8021X

Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret
1	192.168.250.247	1812	•••••••••••••

Add a server

RADIUS testing: RADIUS testing enabled

RADIUS CoA support: RADIUS CoA enabled

RADIUS accounting: RADIUS accounting enabled

RADIUS accounting servers

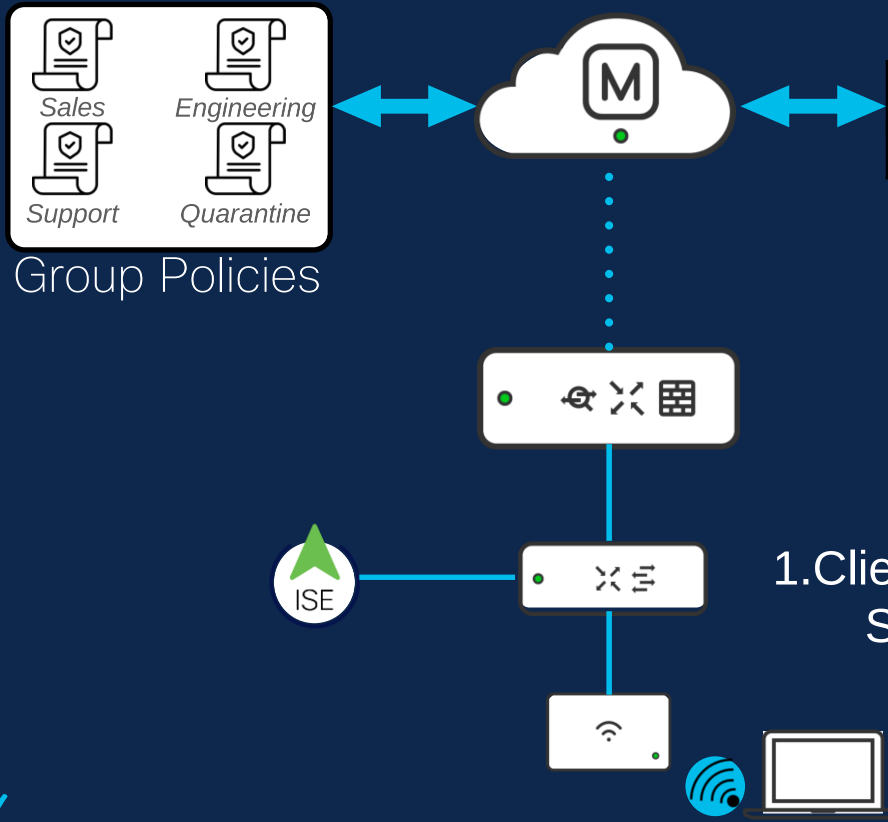
#	Host	Port	Secret
1	192.168.250.247	1813	•••••••••••••

Add a server

RADIUS attribute specifying group policy name: Filter-Id

Identity-Based Security Policy with Meraki MX

Active/Passive Identity with Meraki Full Stack and Group Policies



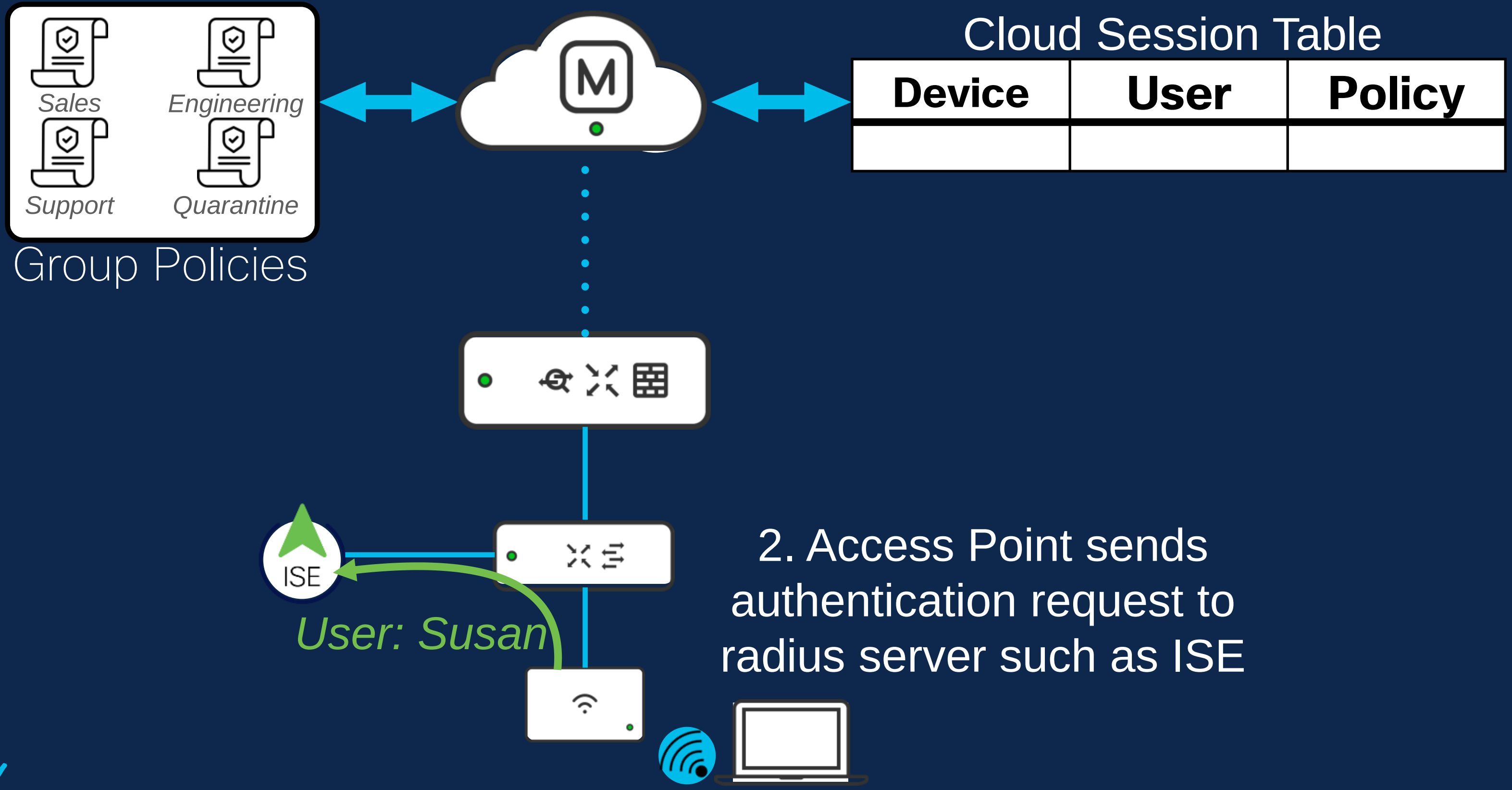
Cloud Session Table

Device	User	Policy

1.Client authenticates to network on SSID configured for RADIUS

Identity-Based Security Policy with Meraki MX

Active/Passive Identity with Meraki Full Stack and Group Policies



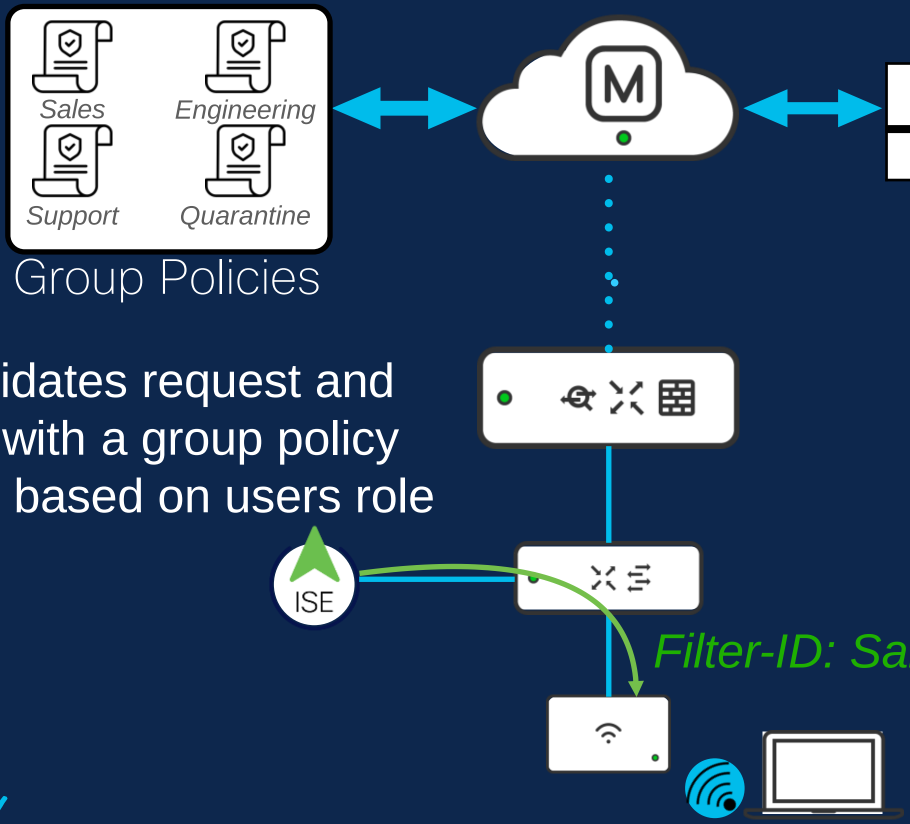
Cloud Session Table

Device	User	Policy

2. Access Point sends authentication request to radius server such as ISE

Identity-Based Security Policy with Meraki MX

Active/Passive Identity with Meraki Full Stack and Group Policies



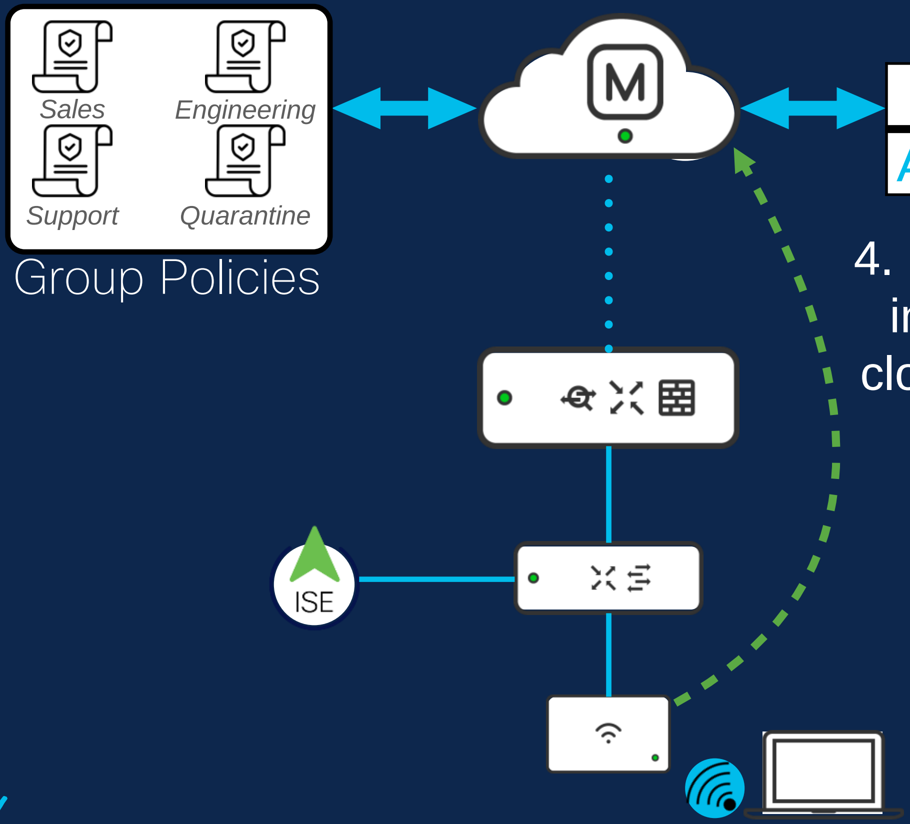
Cloud Session Table

Device	User	Policy

3. ISE validates request and responds with a group policy assignment based on users role

Identity-Based Security Policy with Meraki MX

Active/Passive Identity with Meraki Full Stack and Group Policies



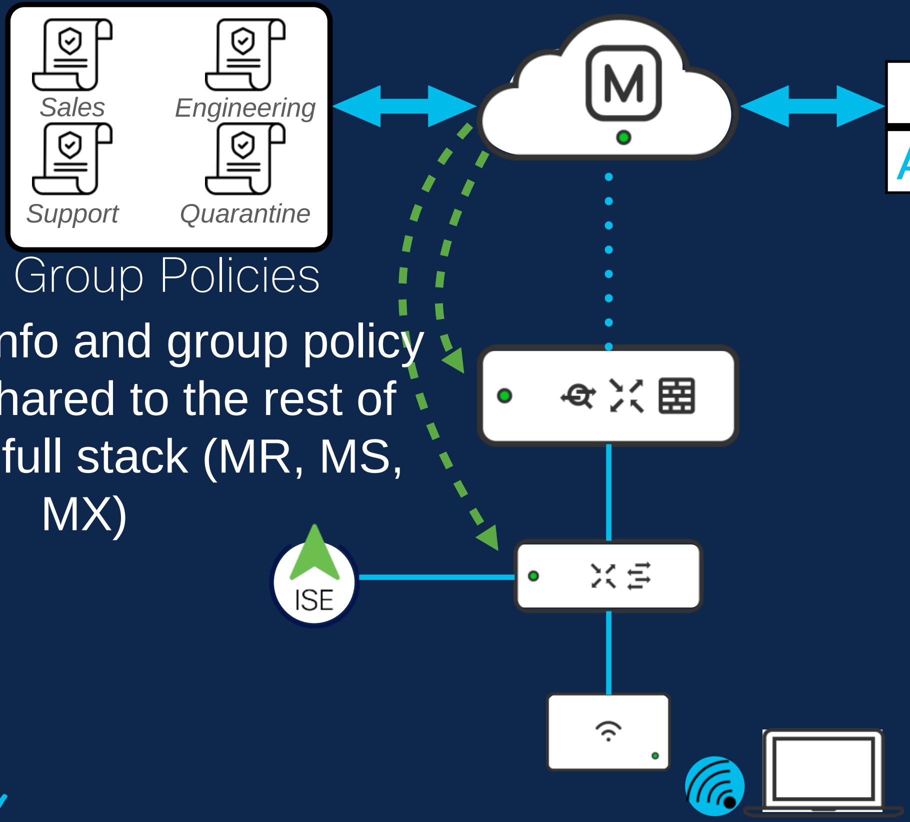
Cloud Session Table

Device	User	Policy
AA:BB:CC	Susan	Sales

4. Device, user and authentication information shared with Meraki cloud and added to cloud session table

Identity-Based Security Policy with Meraki MX

Active/Passive Identity with Meraki Full Stack and Group Policies



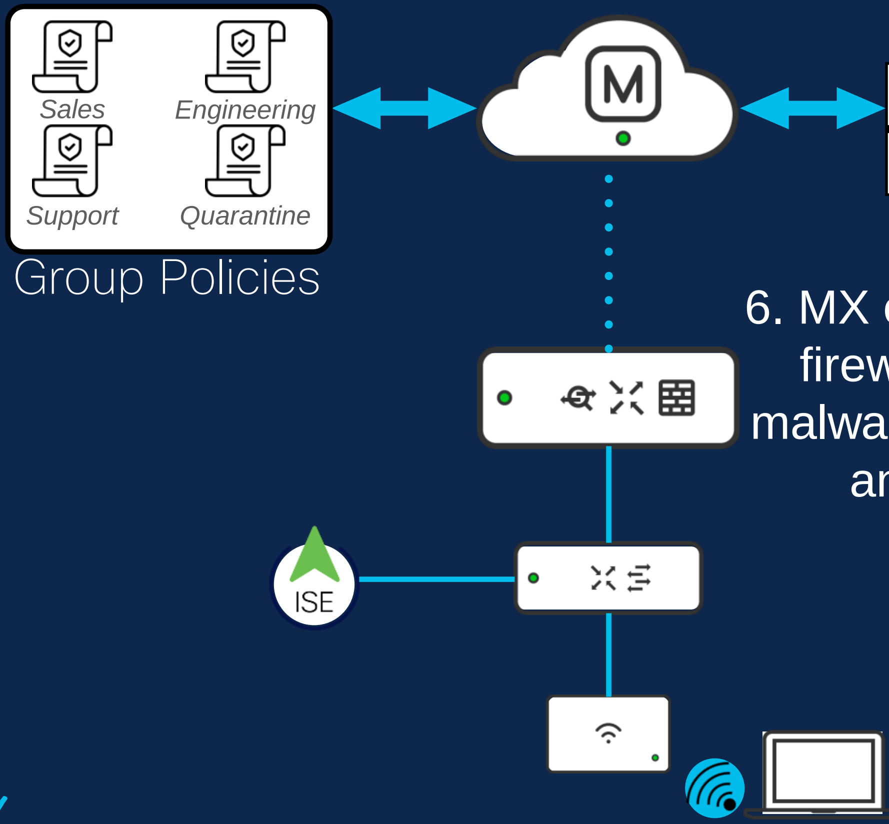
Cloud Session Table

Device	User	Policy
AA:BB:CC	Susan	Sales

5. Session info and group policy mapping shared to the rest of the Meraki full stack (MR, MS, MX)

Identity-Based Security Policy with Meraki MX

Active/Passive Identity with Meraki Full Stack and Group Policies

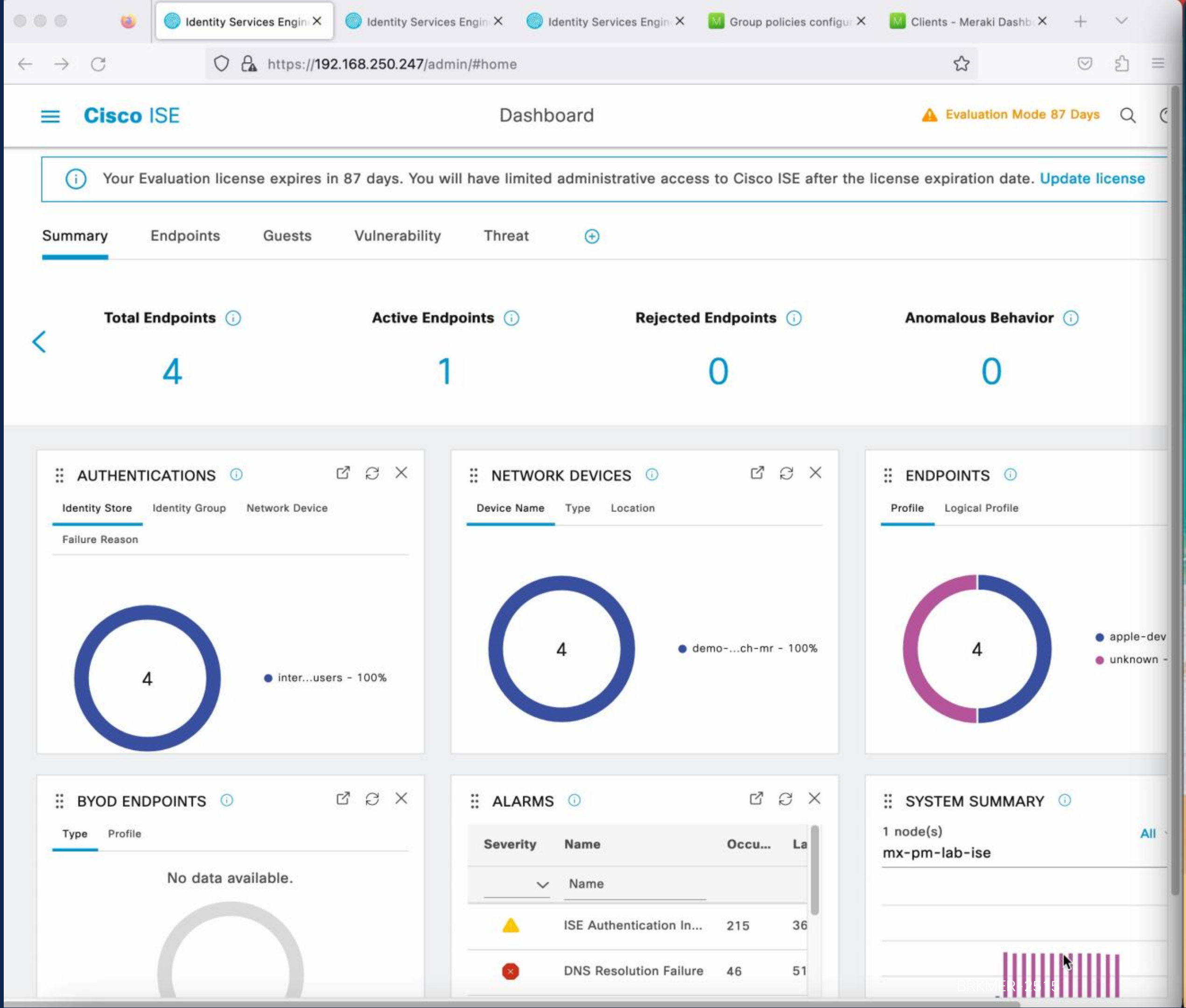


Cloud Session Table

Device	User	Policy
AA:BB:CC	Susan	Sales

6. MX enforces group policy including firewall rules, URL filtering rules, malware protection, SSL decrypt and any QoS specific to the role

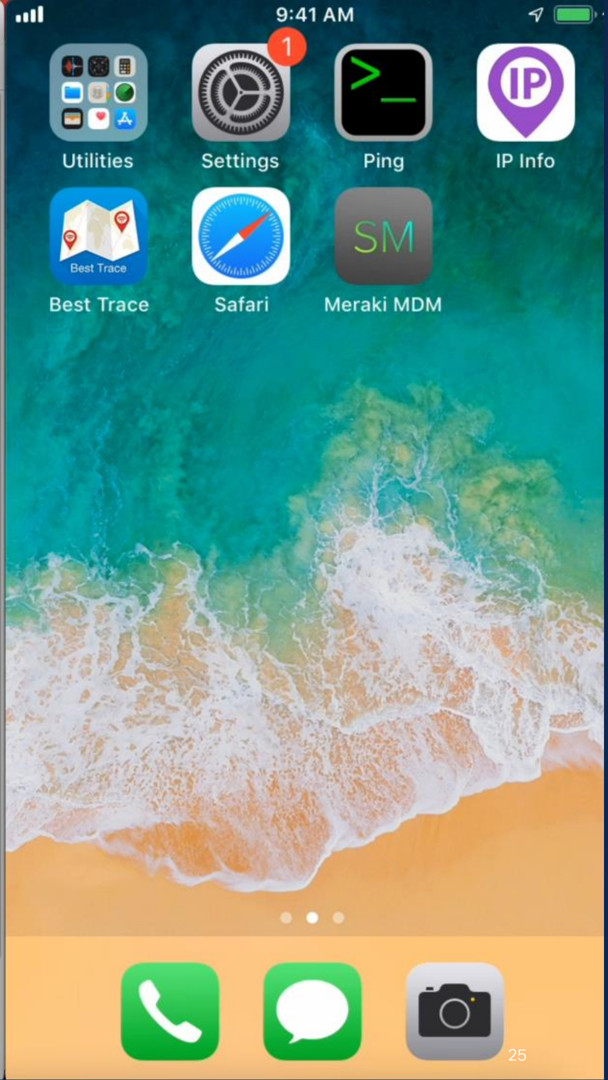
Demo



Your Evaluation license expires in 87 days. You will have limited administrative access to Cisco ISE after the license expiration date. Update license

Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior
4	1	0	0

Severity	Name	Occu...	La
	Name		
⚠	ISE Authentication In...	215	36
✕	DNS Resolution Failure	46	51



Identity-Based Security with Adaptive Policy (SGT)

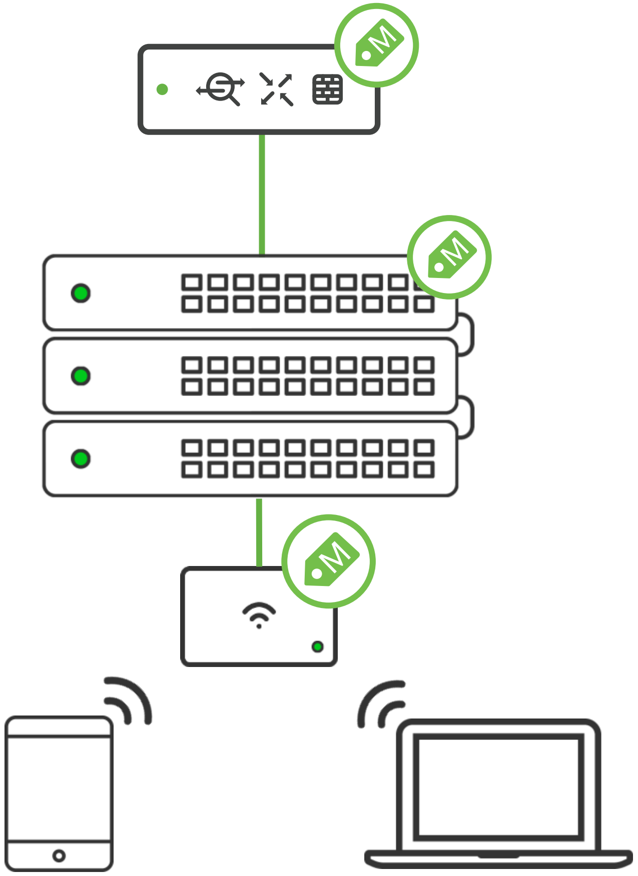
Adaptive Policy

Micro-Segmentation and Context with Security Group Tags

Organization-Wide intent-based policy

Utilizing inline **Security Group Tags** (SGTs)

Context shared over the data-plane providing identical policy for wired and wireless access



Flexible Group Assignment

Static port assignment

(MX/MS/MR)

Fixed wired devices without a supplicant

Static SSID assignment

*(*MX/MS/MR)*

Single-use SSIDs like guest

Dynamic via RADIUS

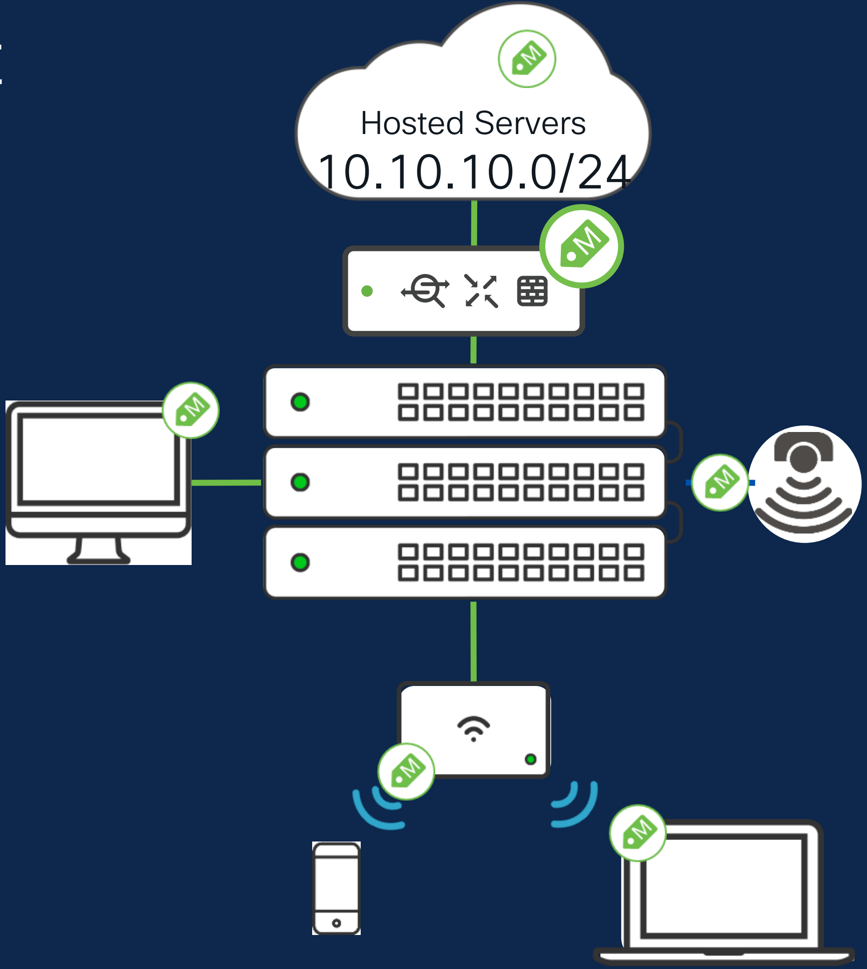
*(*MX/MS/MR)*

Wired and Wireless MAB/802.1X & iPSK w/RADIUS

IP Prefix to SGT Map

*(*MX/MS/MR)*

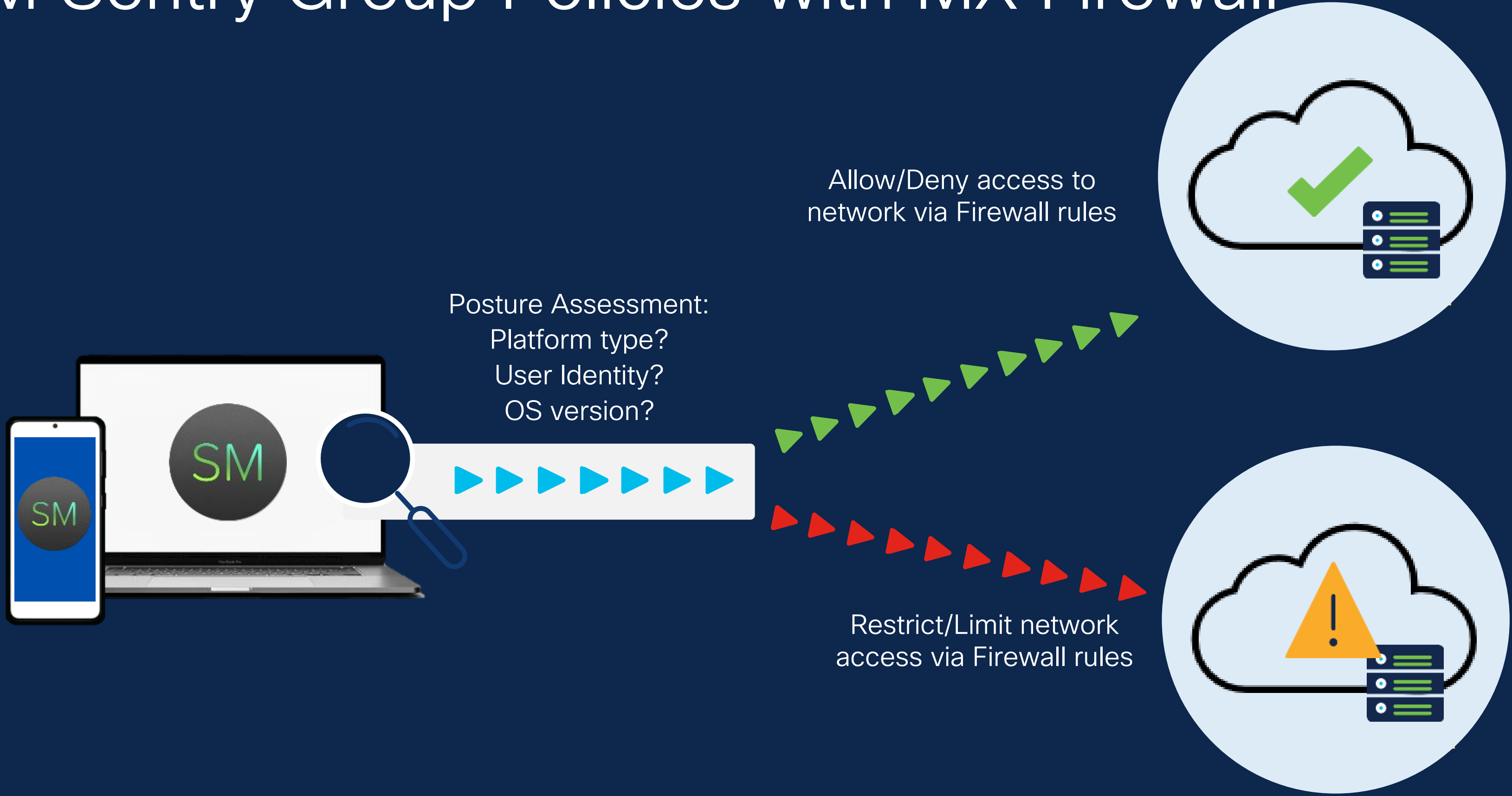
Last resort traffic match based on IP/Subnet



**MX Coming*

Identity-Based Security with Systems Manager Sentry Group Policies

SM Sentry Group Policies with MX Firewall



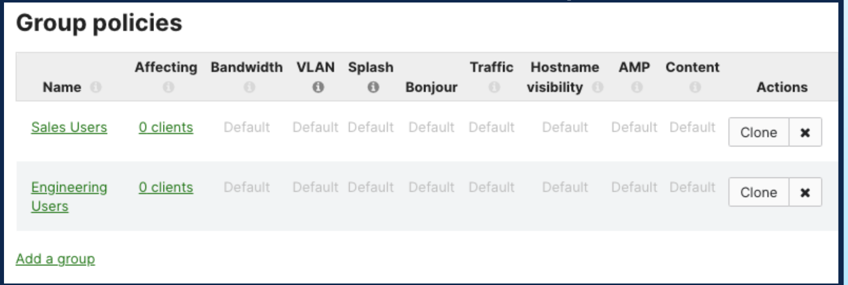
Posture Assessment:
Platform type?
User Identity?
OS version?

Allow/Deny access to network via Firewall rules

Restrict/Limit network access via Firewall rules

New Combined Group and Sentry Policies View

Network-Wide > Group Policies

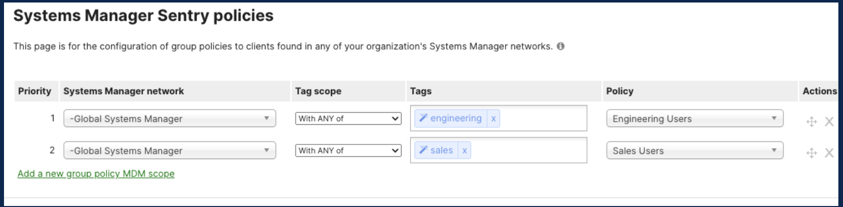


Group policies

Name	Affecting	Bandwidth	VLAN	Splash	Bonjour	Traffic	Hostname visibility	AMP	Content	Actions
Sales Users	0 clients	Default	Default	Default	Default	Default	Default	Default	Default	Clone ✖
Engineering Users	0 clients	Default	Default	Default	Default	Default	Default	Default	Default	Clone ✖

Add a group

Network-Wide > Sentry Policies



Systems Manager Sentry policies

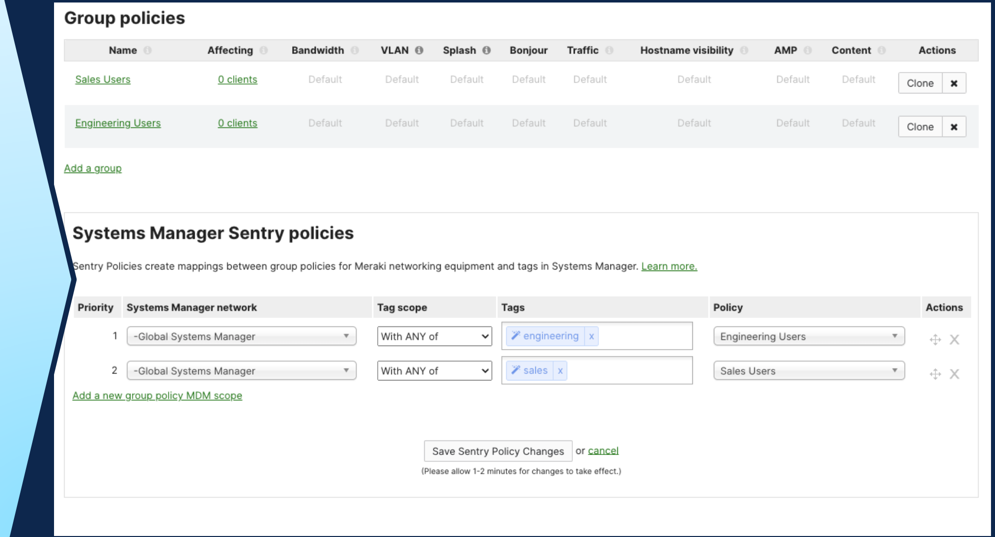
This page is for the configuration of group policies to clients found in any of your organization's Systems Manager networks.

Priority	Systems Manager network	Tag scope	Tags	Policy	Actions
1	-Global Systems Manager	With ANY of	engineering x	Engineering Users	✕
2	-Global Systems Manager	With ANY of	sales x	Sales Users	✕

Add a new group policy MDM scope

The Standalone *Network-Wide > Sentry Policies* page was deprecated on February 1, 2024

Network-Wide > Group Policies



Group policies

Name	Affecting	Bandwidth	VLAN	Splash	Bonjour	Traffic	Hostname visibility	AMP	Content	Actions
Sales Users	0 clients	Default	Default	Default	Default	Default	Default	Default	Default	Clone ✖
Engineering Users	0 clients	Default	Default	Default	Default	Default	Default	Default	Default	Clone ✖

Add a group

Systems Manager Sentry policies

Sentry Policies create mappings between group policies for Meraki networking equipment and tags in Systems Manager. Learn more.

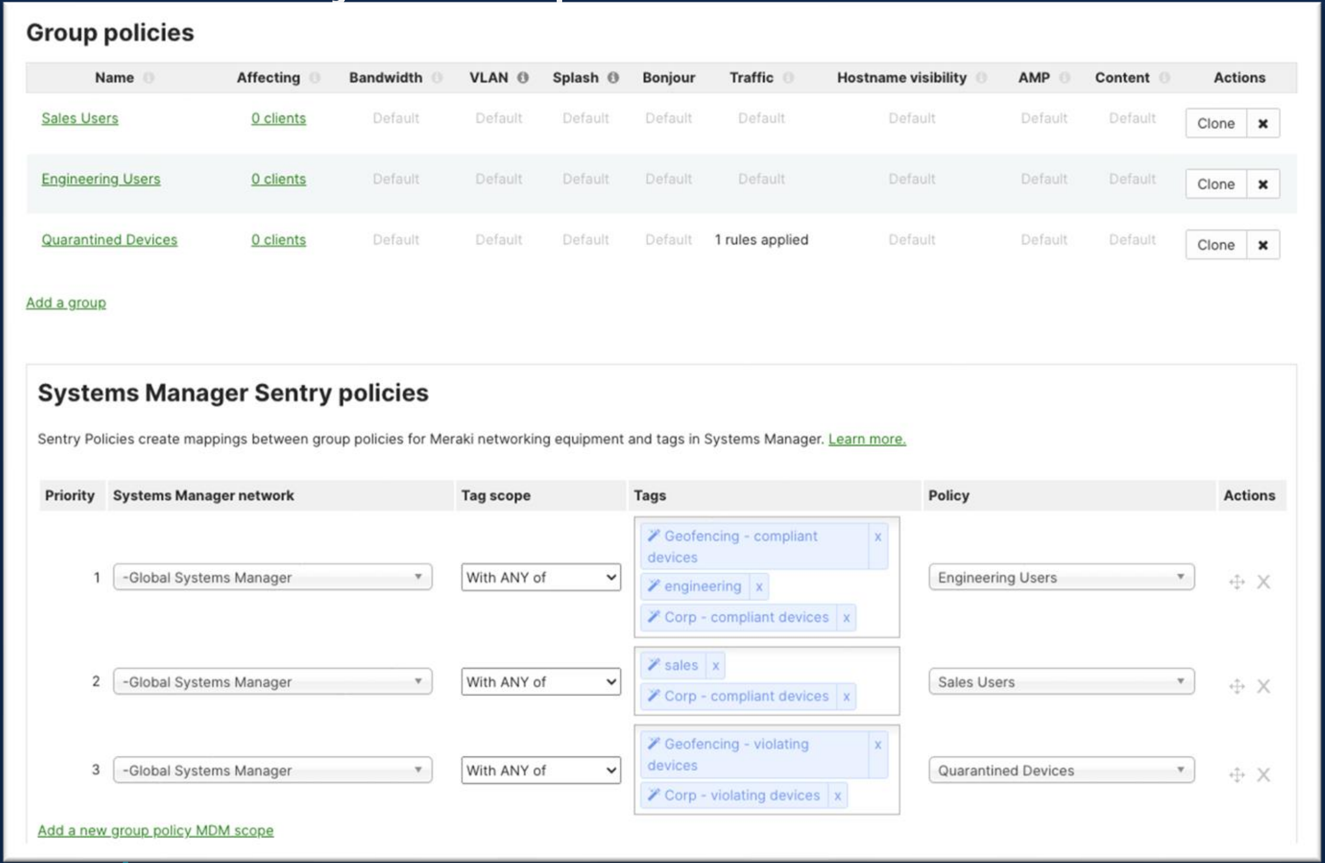
Priority	Systems Manager network	Tag scope	Tags	Policy	Actions
1	-Global Systems Manager	With ANY of	engineering x	Engineering Users	✕
2	-Global Systems Manager	With ANY of	sales x	Sales Users	✕

Add a new group policy MDM scope

Save Sentry Policy Changes or cancel

(Please allow 1-2 minutes for changes to take effect.)

SM Sentry Group Policies with MX Firewall



Group policies

Name	Affecting	Bandwidth	VLAN	Splash	Bonjour	Traffic	Hostname visibility	AMP	Content	Actions
Sales Users	0 clients	Default	Default	Default	Default	Default	Default	Default	Default	Clone ✖
Engineering Users	0 clients	Default	Default	Default	Default	Default	Default	Default	Default	Clone ✖
Quarantined Devices	0 clients	Default	Default	Default	Default	1 rules applied	Default	Default	Default	Clone ✖

Add a group

Systems Manager Sentry policies

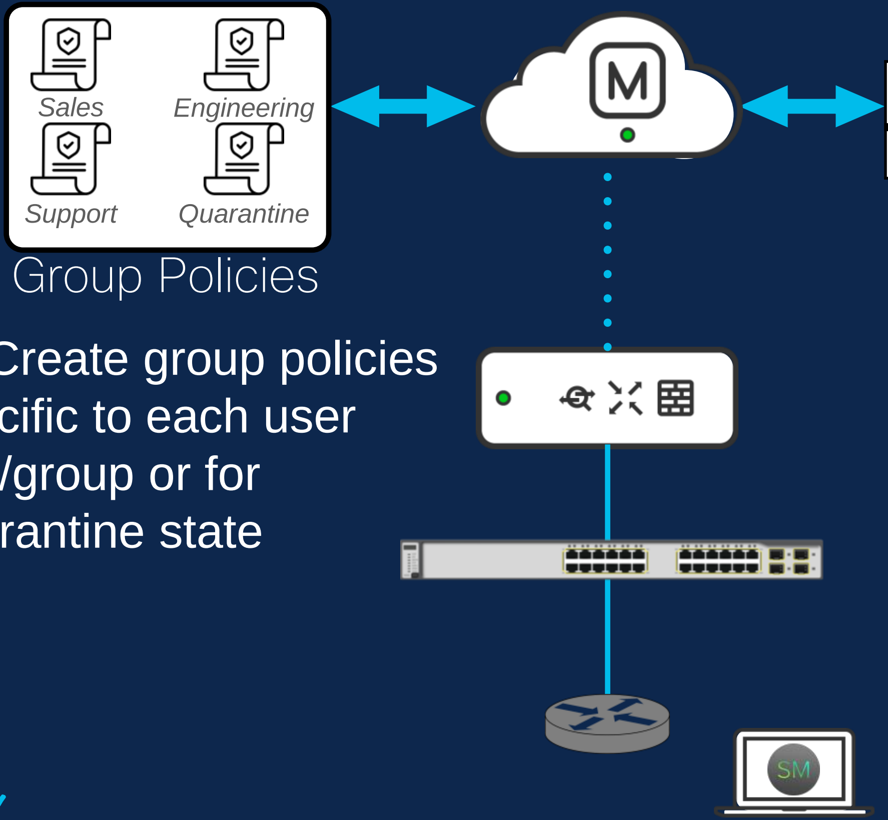
Sentry Policies create mappings between group policies for Meraki networking equipment and tags in Systems Manager. Learn more.

Priority	Systems Manager network	Tag scope	Tags	Policy	Actions
1	-Global Systems Manager	With ANY of	Geofencing - compliant devices engineering Corp - compliant devices	Engineering Users	✕
2	-Global Systems Manager	With ANY of	sales Corp - compliant devices	Sales Users	✕
3	-Global Systems Manager	With ANY of	Geofencing - violating devices Corp - violating devices	Quarantined Devices	✕

Add a new group policy MDM scope

Identity-Based Security Policy with Meraki MX

Posture-based security with Meraki Systems Manager and Sentry Policies



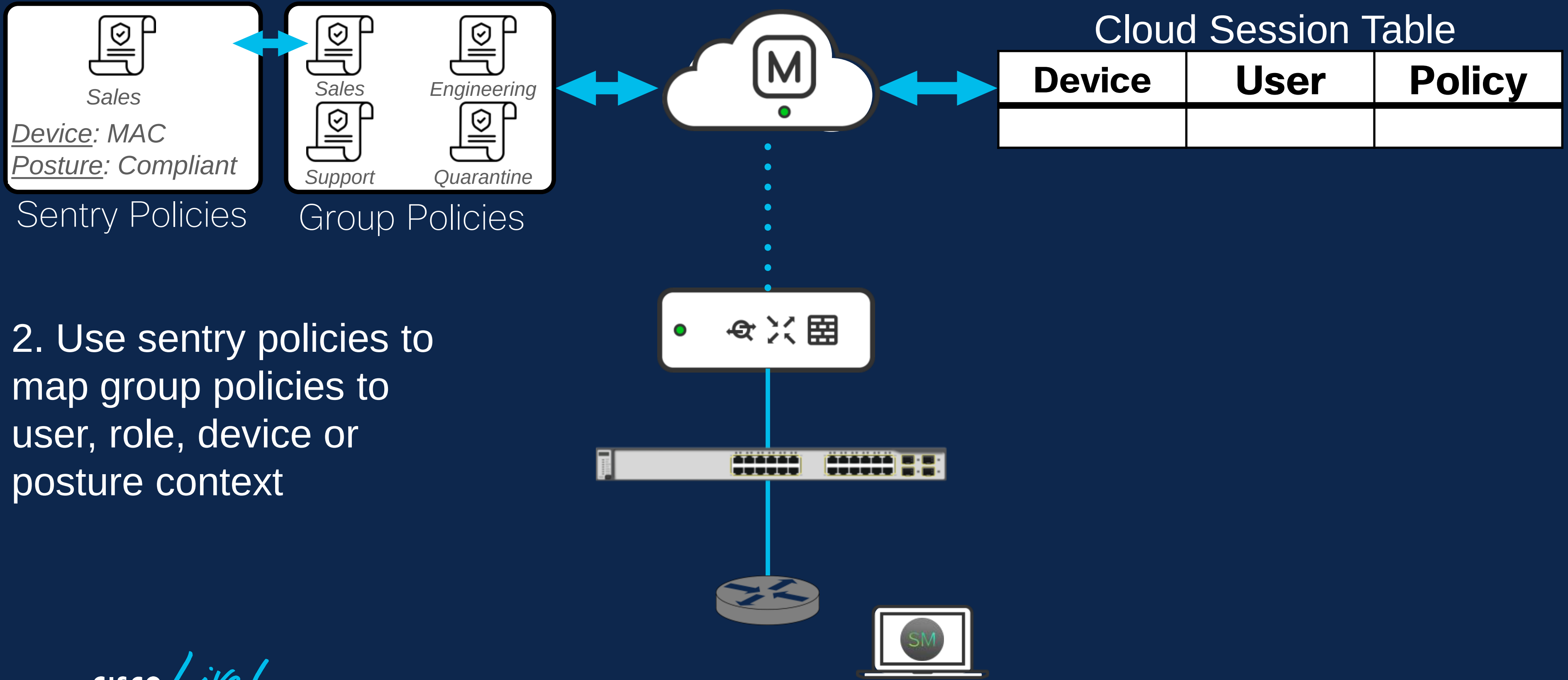
Cloud Session Table

Device	User	Policy

1. Create group policies specific to each user role/group or for quarantine state

Identity-Based Security Policy with Meraki MX

Posture-based security with Meraki Systems Manager and Sentry Policies



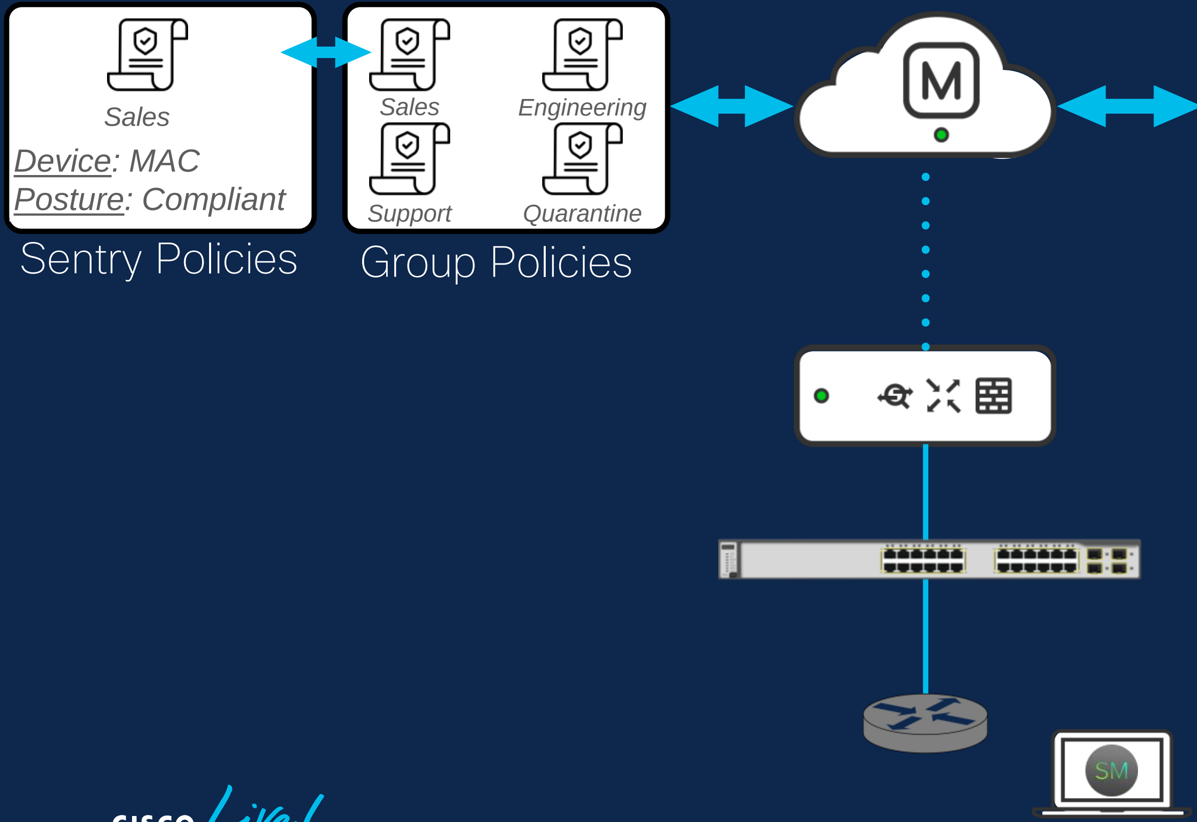
Cloud Session Table

Device	User	Policy

2. Use sentry policies to map group policies to user, role, device or posture context

Identity-Based Security Policy with Meraki MX

Posture-based security with Meraki Systems Manager and Sentry Policies



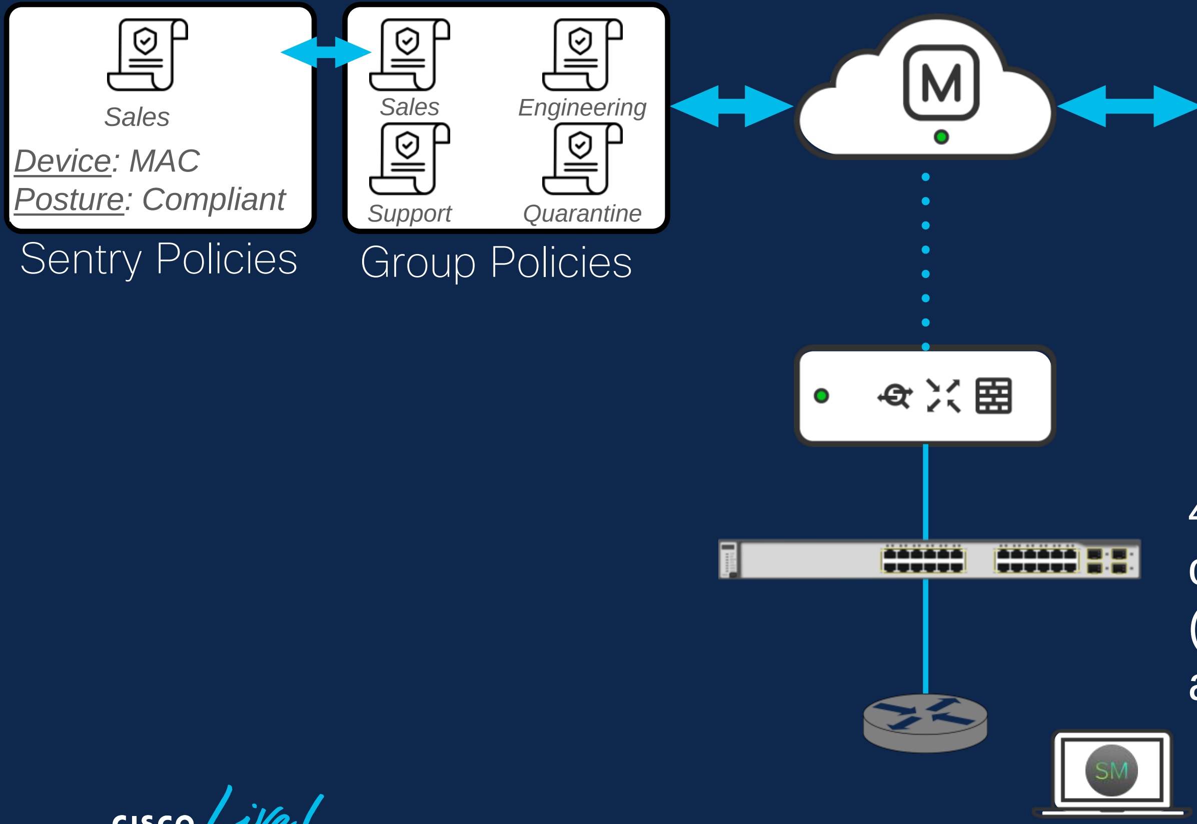
Cloud Session Table

Device	User	Policy

3. Endpoint enrolled in Meraki MDM. SM client installed

Identity-Based Security Policy with Meraki MX

Posture-based security with Meraki Systems Manager and Sentry Policies



Cloud Session Table

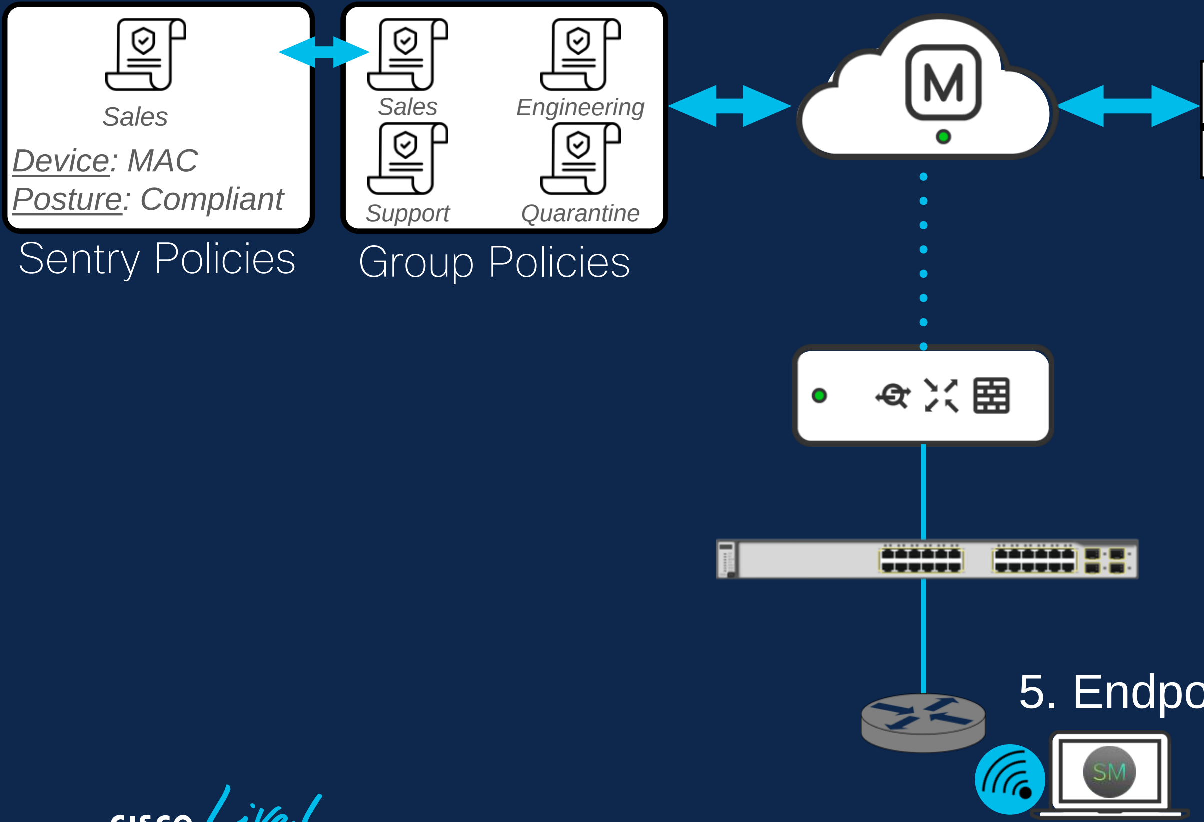
Device	User	Policy

4. Enrolled device assigned an owner in Meraki dashboard (from Azure AD, OIDC, Meraki auth, etc)

Device: Susan's-Laptop
Device Type: MAC
Security Posture: Compliant
Role: Sales

Identity-Based Security Policy with Meraki MX

Posture-based security with Meraki Systems Manager and Sentry Policies



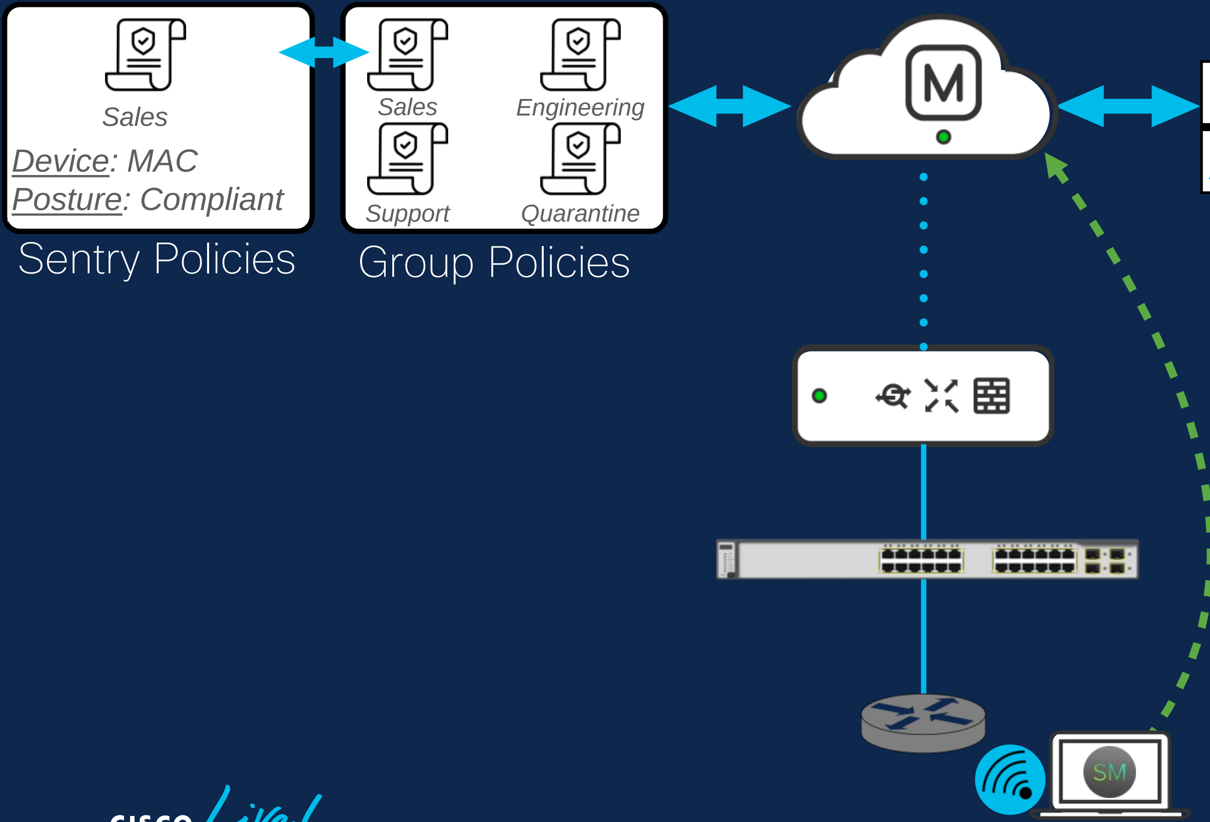
Cloud Session Table

Device	User	Policy

5. Endpoint connects to network

Identity-Based Security Policy with Meraki MX

Posture-based security with Meraki Systems Manager and Sentry Policies



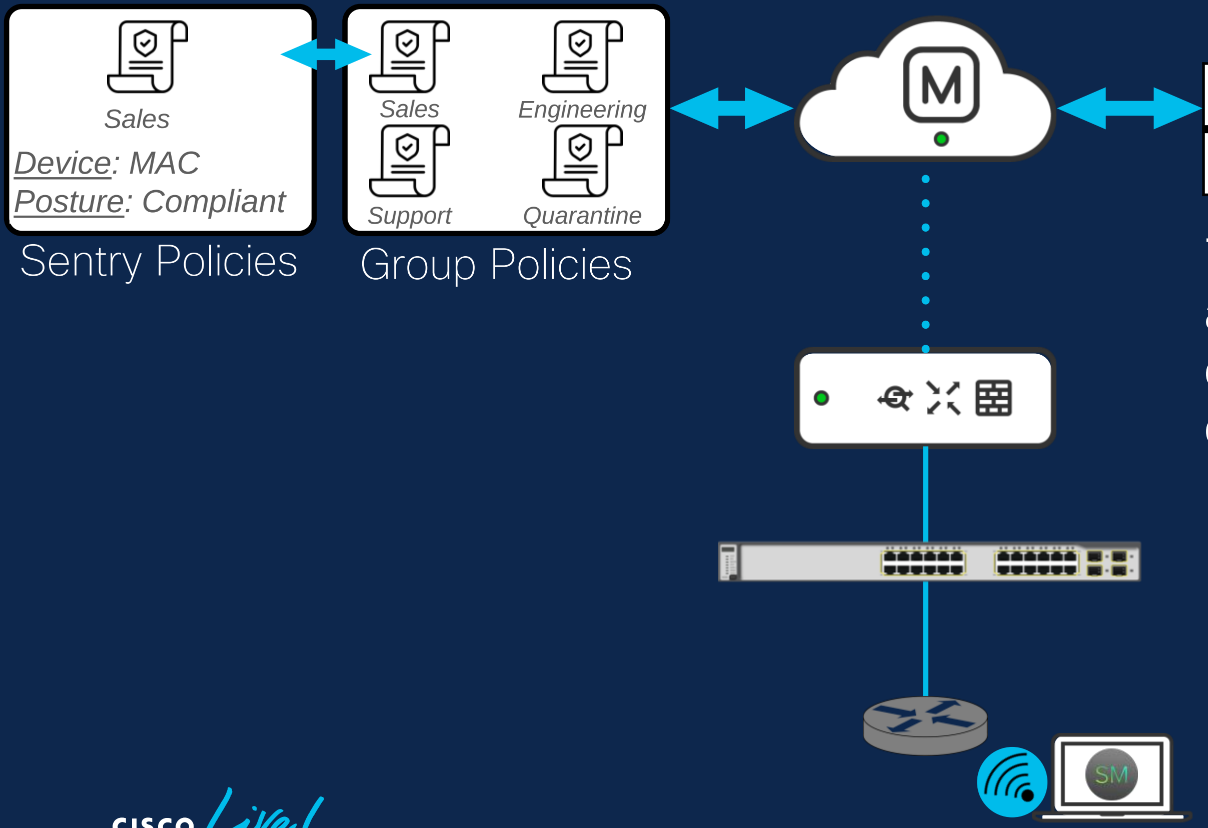
Cloud Session Table

Device	Posture	Policy
AA:BB:CC	Compliant	

6. SM shares IP/MAC and device posture information with Meraki cloud *(even if wireless or switch network is non-Meraki)*

Identity-Based Security Policy with Meraki MX

Posture-based security with Meraki Systems Manager and Sentry Policies



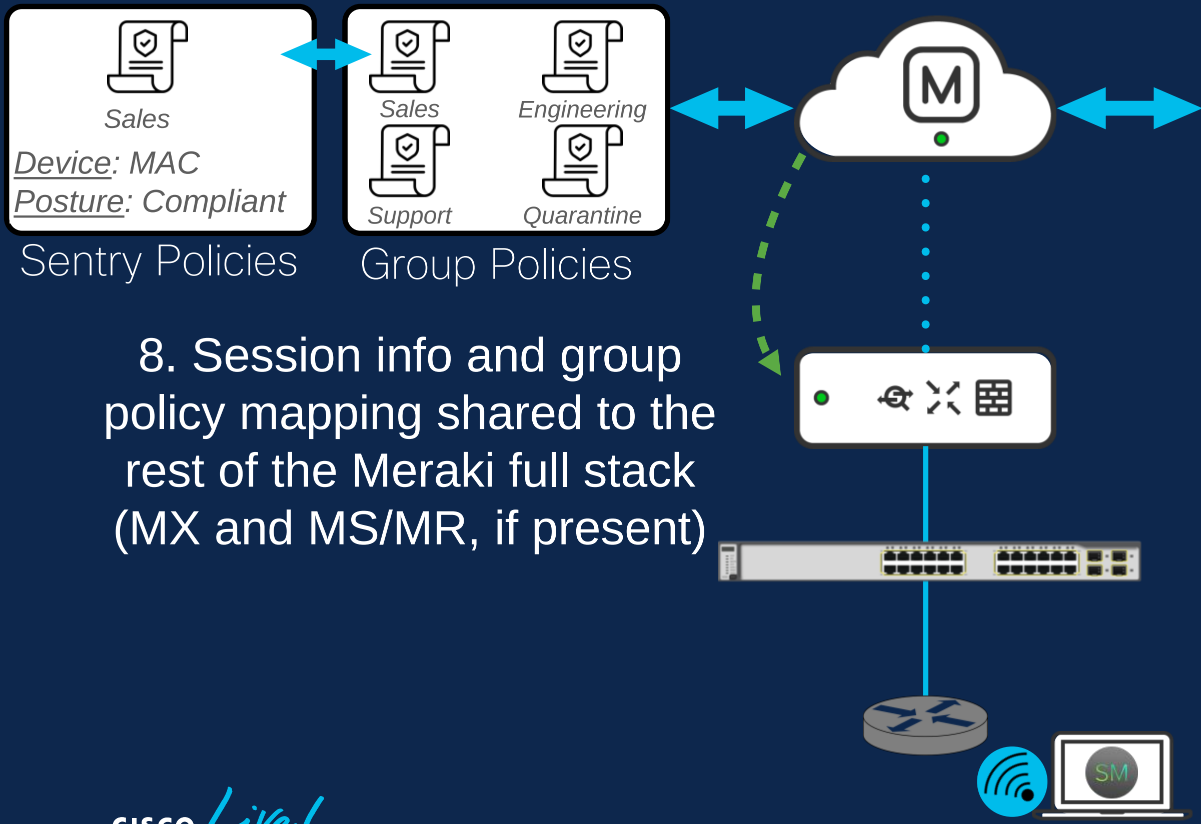
Cloud Session Table

Device	Posture	Policy
AA:BB:CC	Compliant	Sales

7. Group policy automatically applied to device based on owner, endpoint and posture context

Identity-Based Security Policy with Meraki MX

Posture-based security with Meraki Systems Manager and Sentry Policies



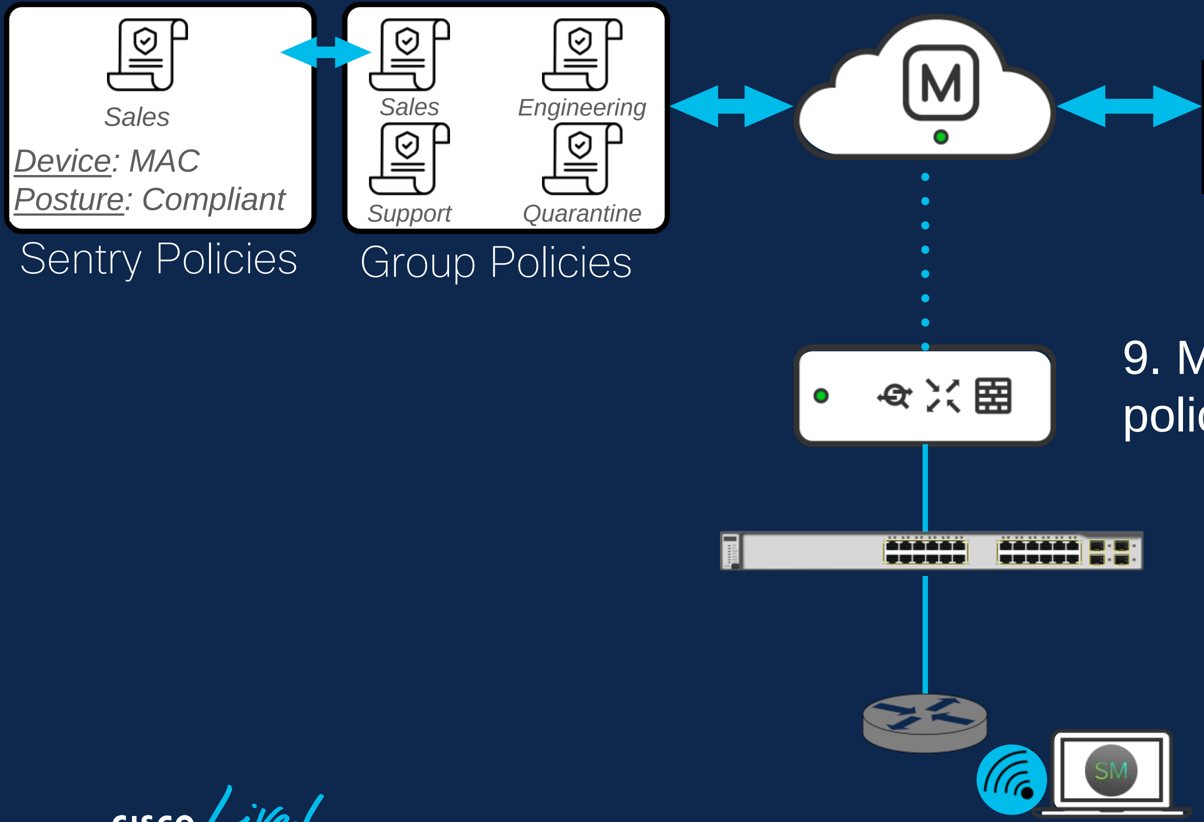
8. Session info and group policy mapping shared to the rest of the Meraki full stack (MX and MS/MR, if present)

Cloud Session Table

Device	Posture	Policy
AA:BB:CC	Compliant	Sales

Identity-Based Security Policy with Meraki MX

Posture-based security with Meraki Systems Manager and Sentry Policies



Cloud Session Table

Device	Posture	Policy
AA:BB:CC	Compliant	Sales

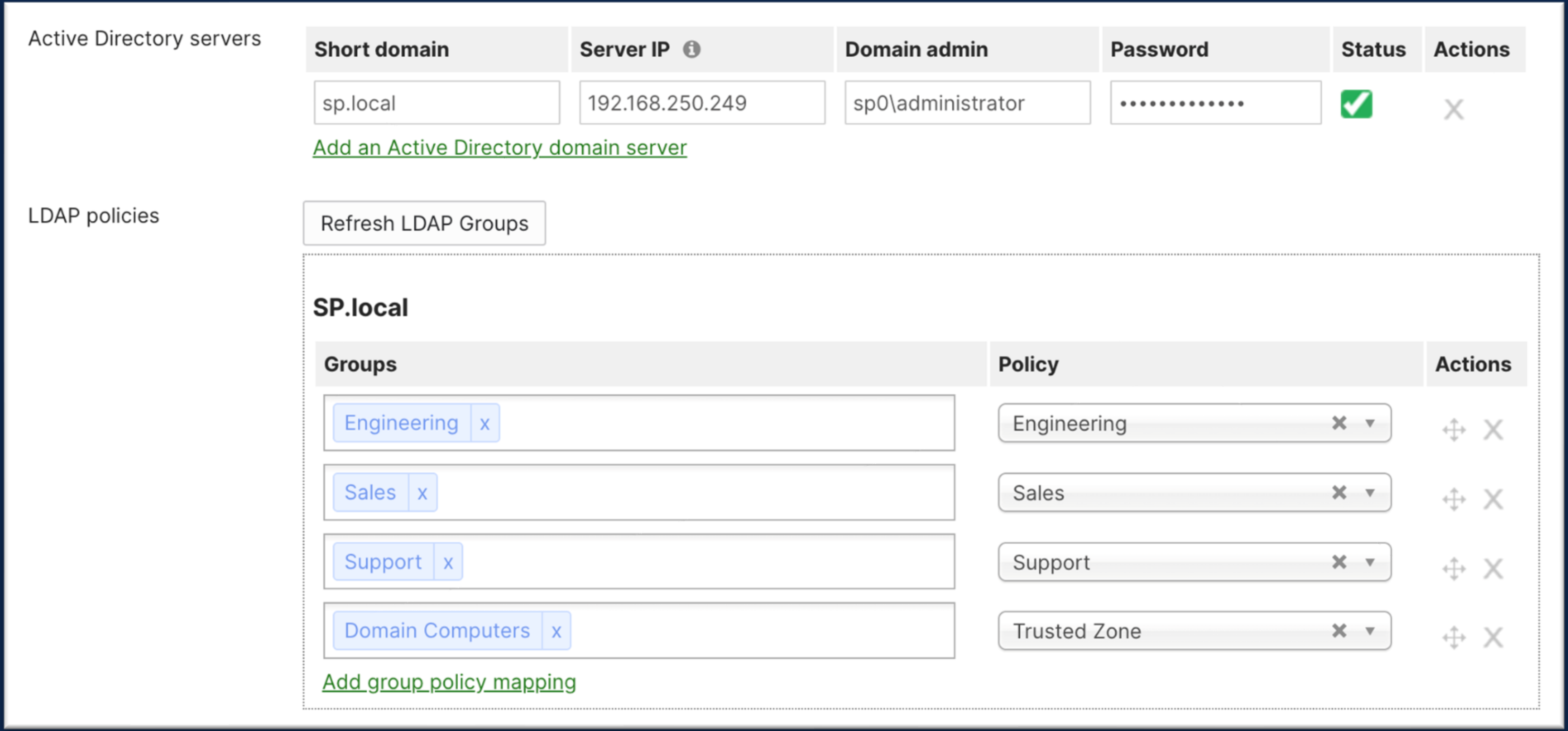
9. MX enforces group policy for endpoint

Identity-based Security with Active Directory Integration

Open Question

Mapping Active Directory Groups to Meraki Group Policies

Automatically apply group policies based on user’s AD group membership



Active Directory servers

Short domain	Server IP	Domain admin	Password	Status	Actions
sp.local	192.168.250.249	sp0\administrator	•••••••••••••	✓	X

Add an Active Directory domain server

LDAP policies

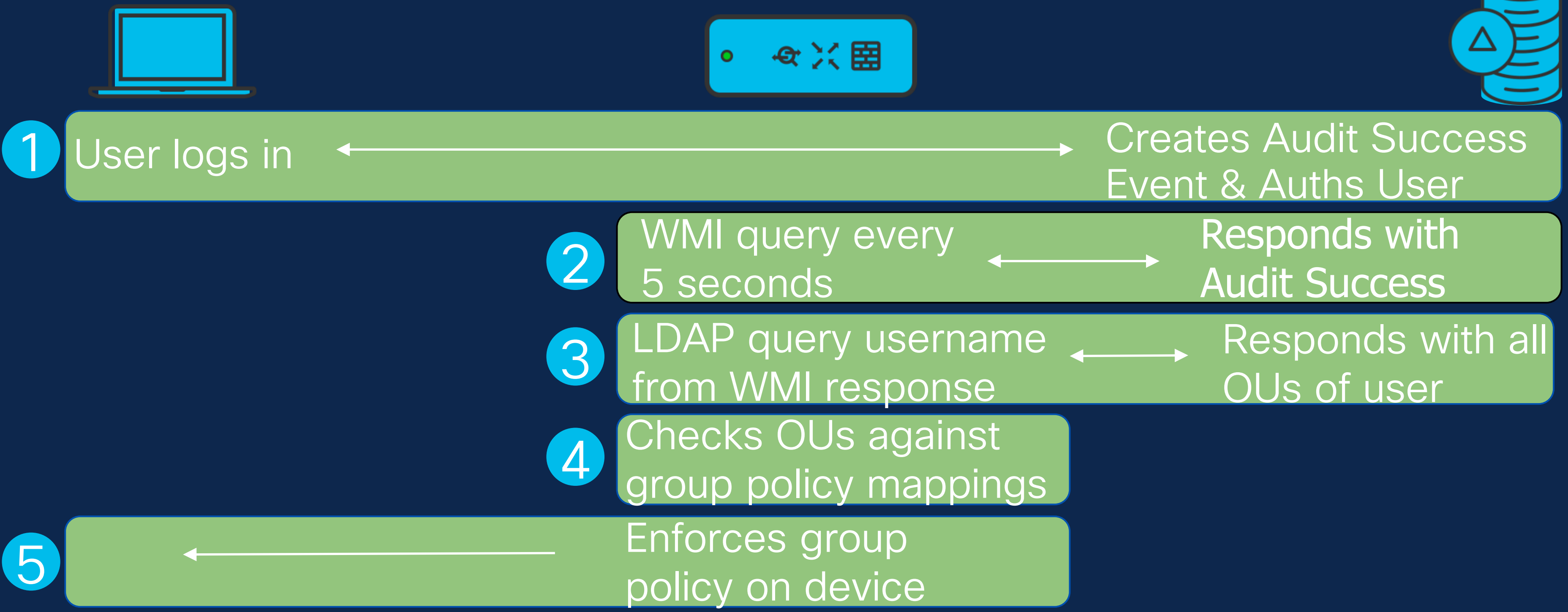
Refresh LDAP Groups

SP.local

Groups	Policy	Actions
Engineering x	Engineering	✥ X
Sales x	Sales	✥ X
Support x	Support	✥ X
Domain Computers x	Trusted Zone	✥ X

Add group policy mapping

MX Active Directory Traffic Flow



1 User logs in — Creates Audit Success Event & Auths User

2 WMI query every 5 seconds — Responds with Audit Success

3 LDAP query username from WMI response — Responds with all OUs of user

4 Checks OUs against group policy mappings

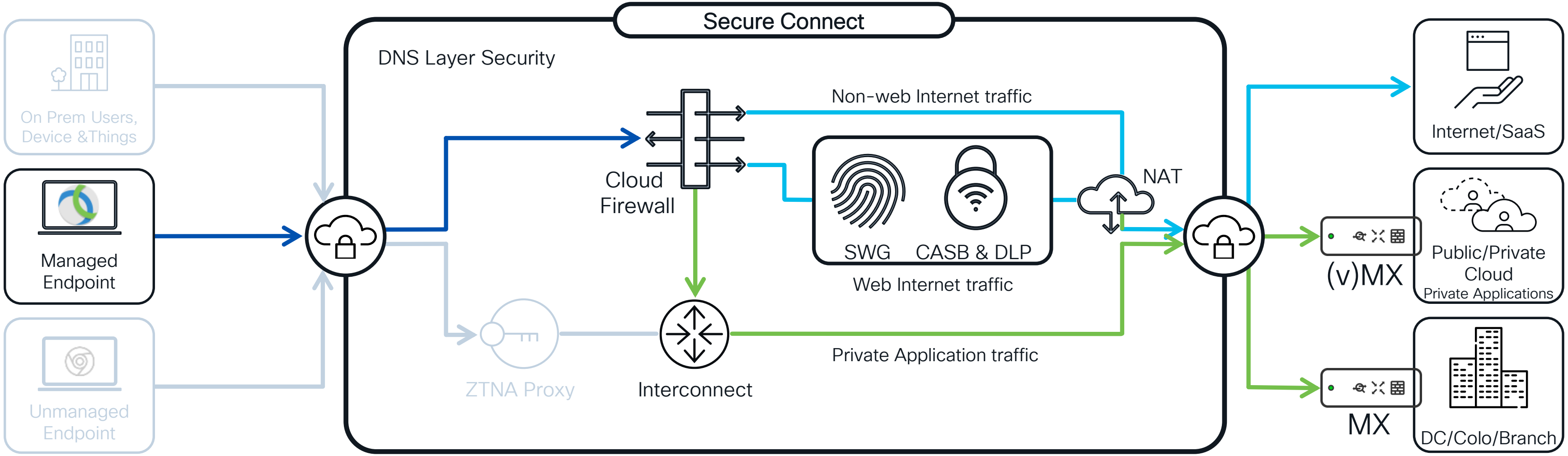
5 Enforces group policy on device

Zero Trust Remote Access with Secure Connect

Open Question

Secure Internet Access

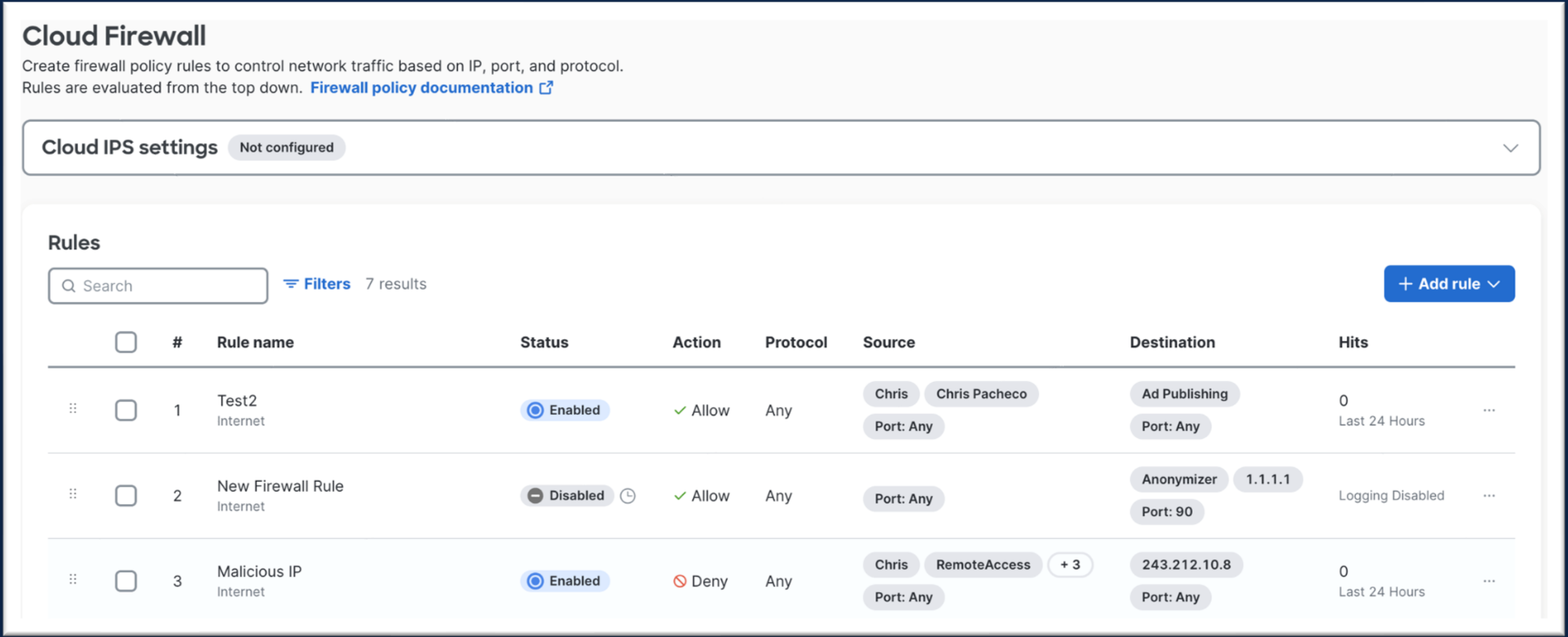
For Remote Users with Secure Client (formerly AnyConnect)



Mixed Private Internet

Secure Internet Access

For Remote Users with Secure Client (formerly AnyConnect)



Cloud Firewall

Create firewall policy rules to control network traffic based on IP, port, and protocol.
Rules are evaluated from the top down. **Firewall policy documentation**

Cloud IPS settings Not configured

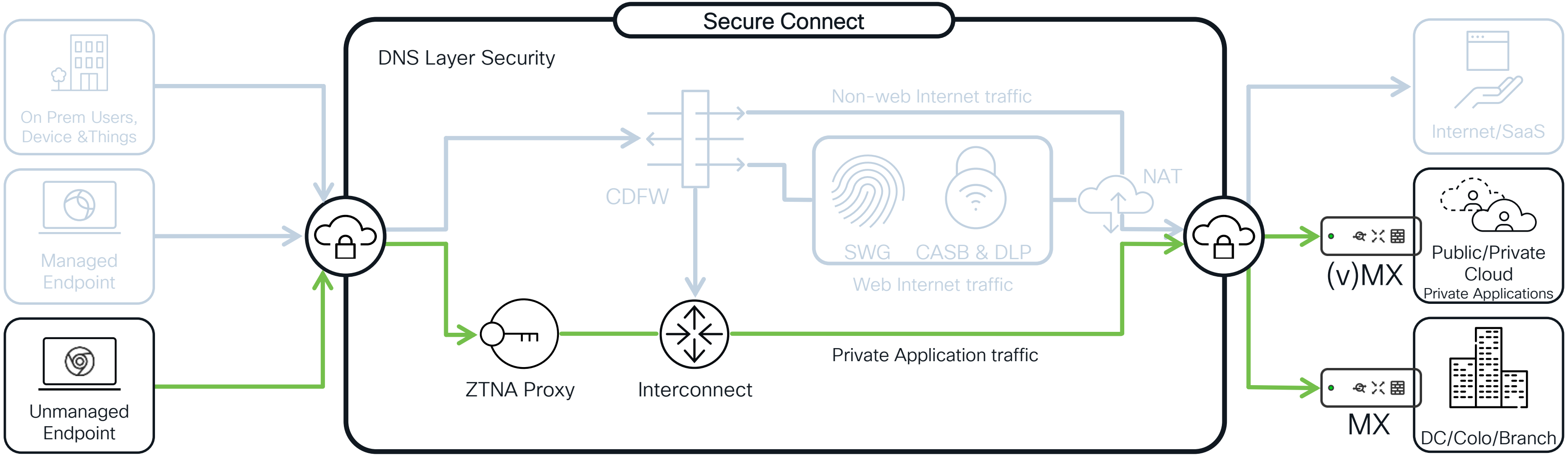
Rules

Search | Filters | 7 results | + Add rule

□	#	Rule name	Status	Action	Protocol	Source	Destination	Hits
□	1	Test2 Internet	Enabled	✓ Allow	Any	Chris Chris Pacheco Port: Any	Ad Publishing Port: Any	0 Last 24 Hours
□	2	New Firewall Rule Internet	Disabled	✓ Allow	Any	Port: Any	Anonymizer 1.1.1.1 Port: 90	Logging Disabled
□	3	Malicious IP Internet	Enabled	Deny	Any	Chris RemoteAccess + 3 Port: Any	243.212.10.8 Port: Any	0 Last 24 Hours

Secure Private Access

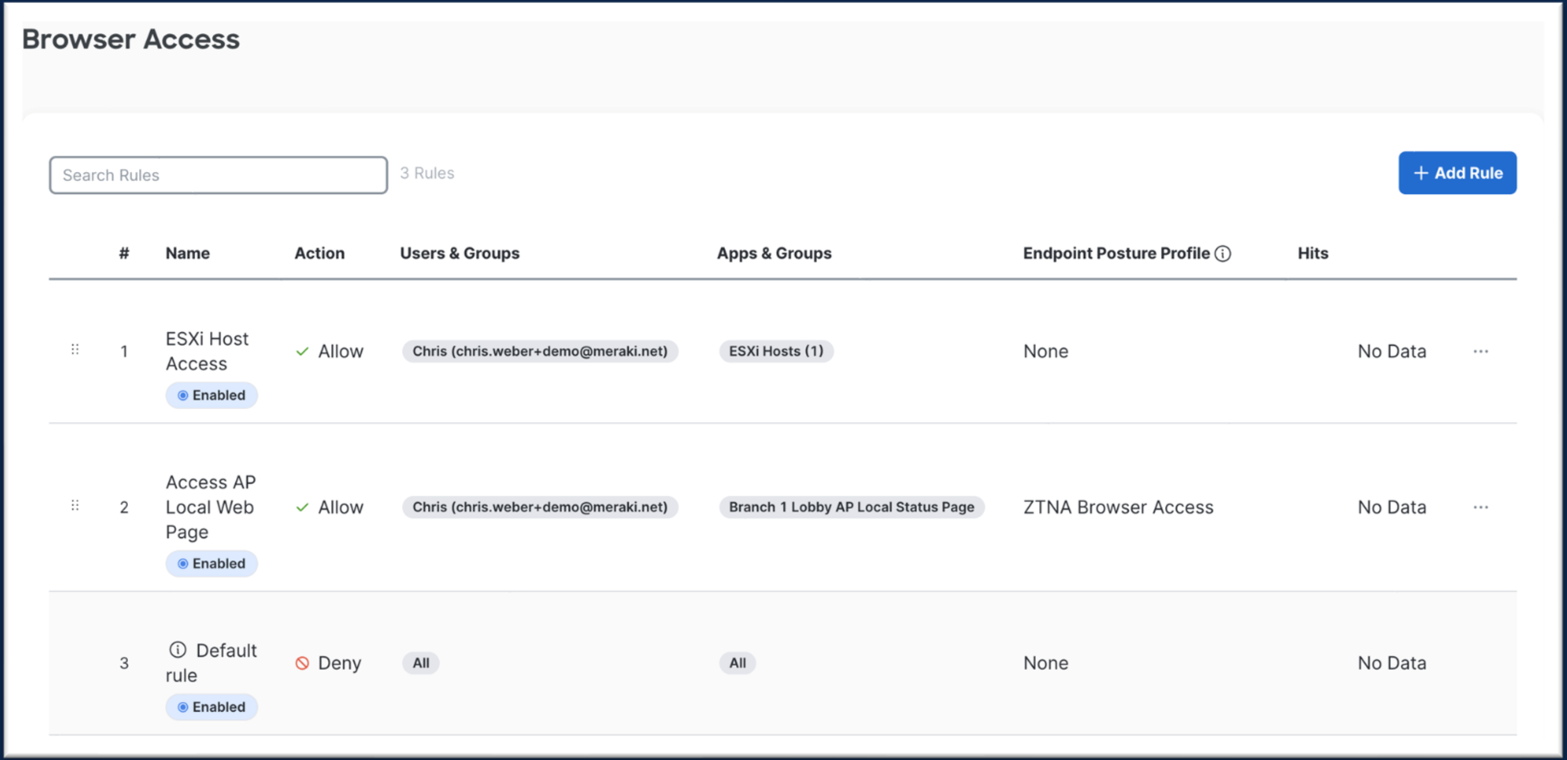
For Remote Users with no client installed (browser-based remote access)



▬ Mixed ▬ Private ▬ Internet

Secure Private Access

For Remote Users with no client installed (browser-based remote access)



Browser Access

Search Rules

3 Rules

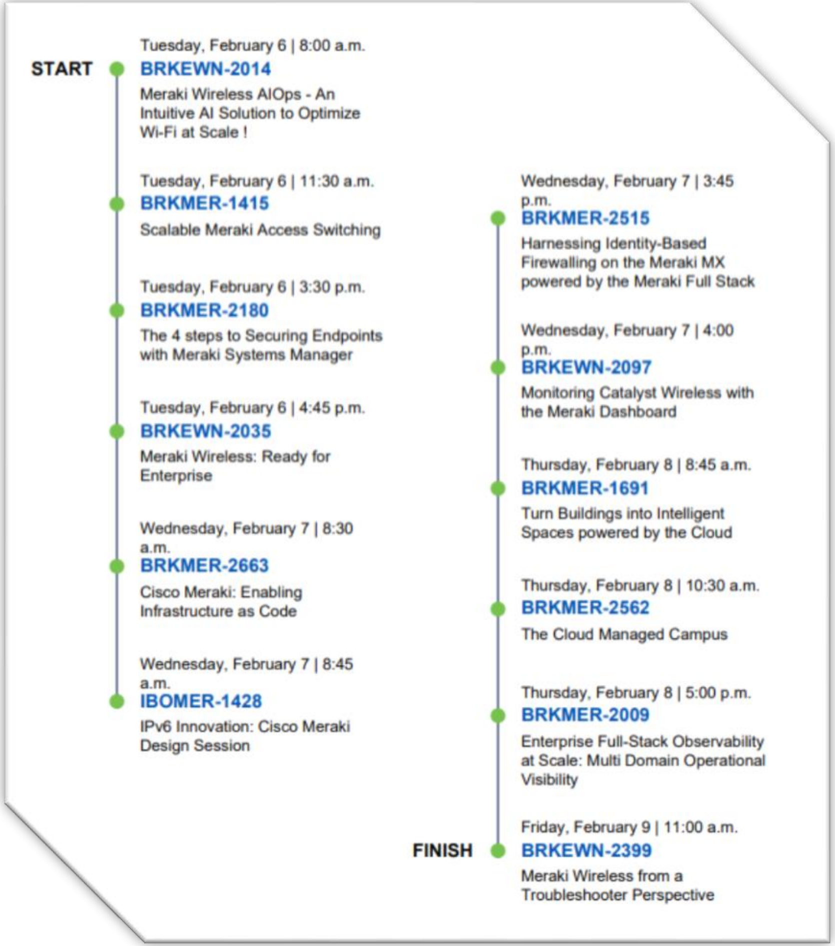
+ Add Rule

#	Name	Action	Users & Groups	Apps & Groups	Endpoint Posture Profile ⓘ	Hits
1	ESXi Host Access ● Enabled	✓ Allow	Chris (chris.weber+demo@meraki.net)	ESXi Hosts (1)	None	No Data
2	Access AP Local Web Page ● Enabled	✓ Allow	Chris (chris.weber+demo@meraki.net)	Branch 1 Lobby AP Local Status Page	ZTNA Browser Access	No Data
3	ⓘ Default rule ● Enabled	⃠ Deny	All	All	None	No Data

Cisco Meraki Learning Map

Expand your horizons and see what Cisco's cloud management platform can do for your business. The Meraki Learning map includes content that spans many topics ranging from programmability to cybersecurity.

Remember, there are also Lab and DevNet Sessions, Capture the Flag activities, and Meraki demos throughout the World of Solutions show floor.



START

Tuesday, February 6 | 8:00 a.m.
BRKEWN-2014
Meraki Wireless AIOps - An Intuitive AI Solution to Optimize Wi-Fi at Scale !

Tuesday, February 6 | 11:30 a.m.
BRKMER-1415
Scalable Meraki Access Switching

Tuesday, February 6 | 3:30 p.m.
BRKMER-2180
The 4 steps to Securing Endpoints with Meraki Systems Manager

Tuesday, February 6 | 4:45 p.m.
BRKEWN-2035
Meraki Wireless: Ready for Enterprise

Wednesday, February 7 | 8:30 a.m.
BRKMER-2663
Cisco Meraki: Enabling Infrastructure as Code

Wednesday, February 7 | 8:45 a.m.
IBOMER-1428
IPv6 Innovation: Cisco Meraki Design Session

Wednesday, February 7 | 3:45 p.m.
BRKMER-2515
Harnessing Identity-Based Firewalling on the Meraki MX powered by the Meraki Full Stack

Wednesday, February 7 | 4:00 p.m.
BRKEWN-2097
Monitoring Catalyst Wireless with the Meraki Dashboard

Thursday, February 8 | 8:45 a.m.
BRKMER-1691
Turn Buildings into Intelligent Spaces powered by the Cloud

Thursday, February 8 | 10:30 a.m.
BRKMER-2562
The Cloud Managed Campus

Thursday, February 8 | 5:00 p.m.
BRKMER-2009
Enterprise Full-Stack Observability at Scale: Multi Domain Operational Visibility

FINISH

Friday, February 9 | 11:00 a.m.
BRKEWN-2399
Meraki Wireless from a Troubleshooter Perspective

Engage with us:
Become a Cisco Meraki Insider

Join
the community

Complete
challenges

Receive
rewards

The bridge to possible

Thank you

cisco Live!

Let’s go