
TURN
IT
UP
cisco Live!
#CiscoLive

The bridge to possible

Connect and Secure with Meraki

Rob Watt – CCIE: Security #19459
Product Manager, Cisco Meraki

BRKMER-2020

Agenda

- Introduction
- What is Zero Trust?
- Secure Infrastructure with Meraki SecureConnect
- Intent based Security with Meraki Adaptive Policy
- IP Access Controls using Meraki MS Group Policy ACLs
- Conclusion

Introduction

A little bit about me?

- Expat Canadian!
- Will work for motorcycles
- Happy Husky owner!
- CCIE:Sec #19459
- Cisco for 7 Years
- PM in Cisco Meraki on MS Switching
- Prior Meraki CSE in Global Enterprise
- Way way back… Post/Pre-sales Engineer w/ partners

Cisco's Implementation of Zero Trust

We establish trust by verifying:

- ✓ User & device identity
- ✓ Device posture & vulnerabilities
- ✓ Any workloads
- ✓ App/service trust
- ✓ Any indicators of compromise

We enforce least privilege access to:

- ✓ Applications
- ✓ Network resources
- ✓ Workload communications
- ✓ All workload users/admins

We continuously verify:

- ✓ Original tenets used to establish trust are still true
- ✓ Traffic is not threat traffic
- ✓ Any risky, anomalous and malicious behavior
- ✓ If compromised, then the trust level is changed

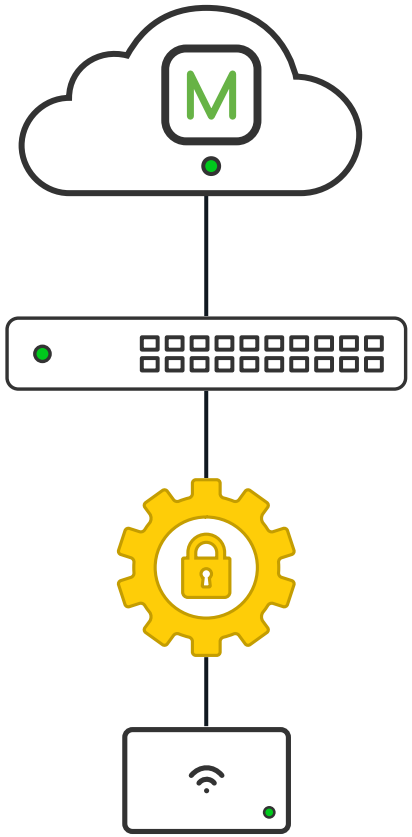
Zero Trust with SecureConnect

cisco Live!

Meraki SecureConnect

Automated secure on-boarding of MR APs

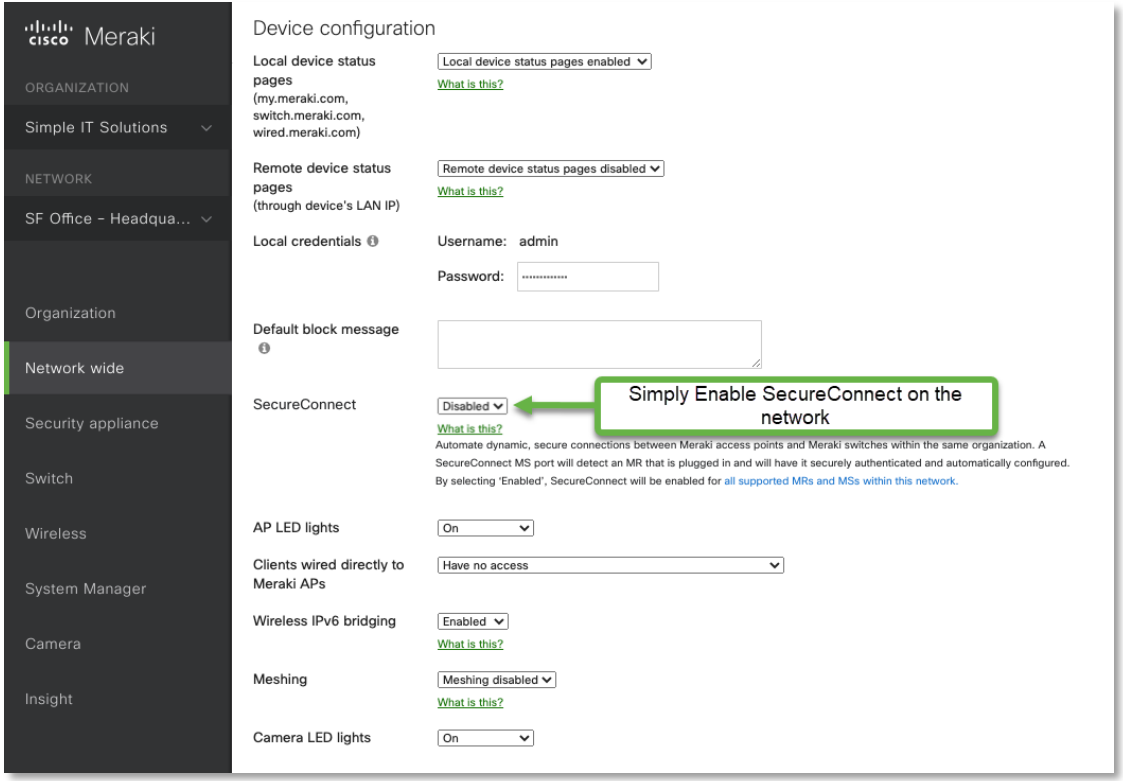
- Automated securing of Access Point switchports
- Maintains infrastructure security with a focus on simplicity
- Consistent configuration of AP ports
- Certificate based verification of AP identity



https://documentation.meraki.com/MS/Access_Control/SecureConnect

Supported on MS210/225/250/350/355/425/450 and 802.11ac wave 2 / Wi-Fi 6 (802.11ax) MR access points

Setting up SecureConnect



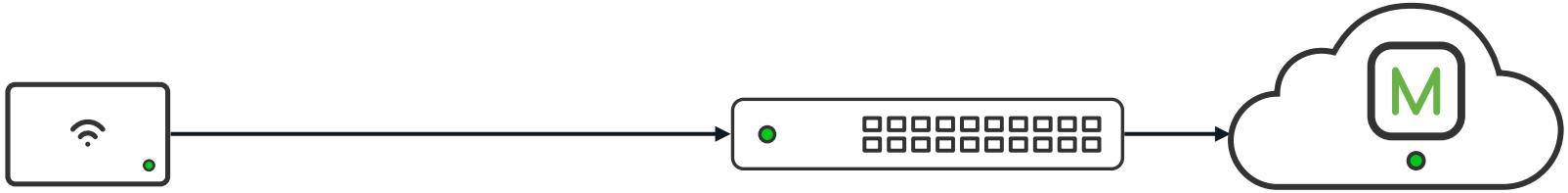
How Does it Work?

Step 1 – Plug in an MR Access Point to an MS Switch

MR physically
connected to MS

How Does it Work?

Step 2 – Temporary Access for MR to Meraki Cloud

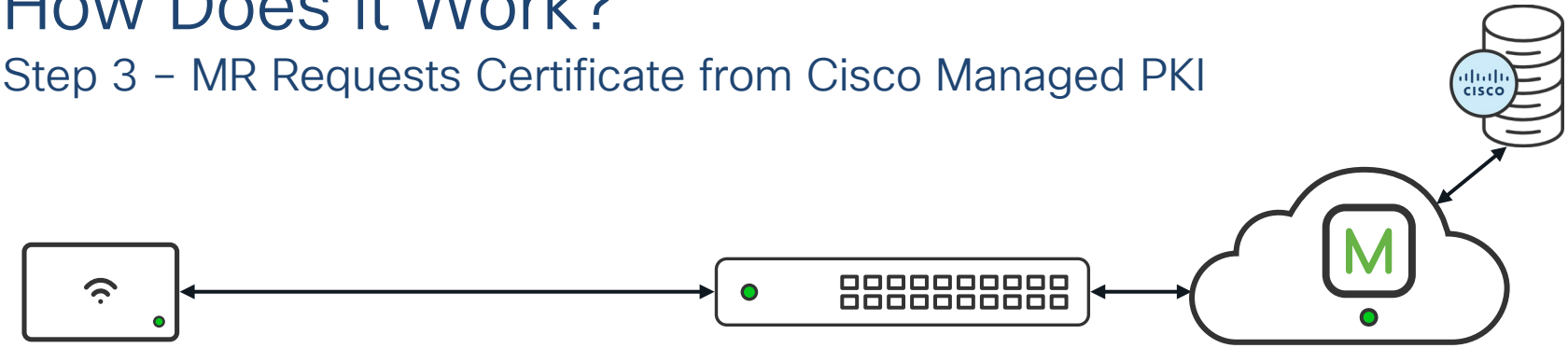


MR physically connected to MS

MS permits Meraki dashboard connection for MR

How Does it Work?

Step 3 – MR Requests Certificate from Cisco Managed PKI



MR physically connected to MS

MS permits Meraki dashboard connection for MR

MR requests certificate from Cisco PKI

SecureConnect Packet Capture

Initial Meraki Dashboard Connection – Management Traffic Only

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x4b6933f6
10.39.0.1	10.39.0.115	DHCP	342	DHCP Offer - Transaction ID 0x4b6933f6
0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0x4b6933f6
10.39.0.1	10.39.0.115	DHCP	342	DHCP ACK - Transaction ID 0x4b6933f6
0.0.0.0	255.255.255.255	DHCP	346	DHCP Release - Transaction ID 0x5f117916
0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x4b6933f7
10.39.0.1	10.39.0.115	DHCP	342	DHCP Offer - Transaction ID 0x4b6933f7
0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0x4b6933f7
10.39.0.1	10.39.0.115	DHCP	342	DHCP ACK - Transaction ID 0x4b6933f7
10.39.0.115	10.39.0.1	DNS	78	Standard query 0x5d24 A mtunnel.meraki.com
10.39.0.115	10.39.0.1	DNS	78	Standard query 0x4223 AAAA mtunnel.meraki.com
10.39.0.1	10.39.0.115	DNS	115	Standard query response 0x5d24 A mtunnel.meraki.com CNAME
10.39.0.115	10.39.0.1	DNS	79	Standard query 0xe4b7 A mtunnel3.meraki.com
10.39.0.115	10.39.0.1	DNS	79	Standard query 0xac9c AAAA mtunnel3.meraki.com
10.39.0.1	10.39.0.115	DNS	116	Standard query response 0xe4b7 A mtunnel3.meraki.com CNAME
10.39.0.115	10.39.0.1	DNS	78	Standard query 0x3382 AAAA mtunnel.meraki.com
10.39.0.1	10.39.0.115	DNS	109	Standard query response 0x3382 AAAA mtunnel.meraki.com CNA
10.39.0.115	209.206.48.214	UDP	146	44546 → 7351 Len=104
10.39.0.115	209.206.52.14	UDP	146	44798 → 7351 Len=104
209.206.52.14	10.39.0.115	UDP	88	7351 → 44798 Len=46
209.206.48.214	10.39.0.115	UDP	88	7351 → 44546 Len=46
209.206.48.214	10.39.0.115	UDP	166	7351 → 44546 Len=124
10.39.0.115	209.206.48.214	UDP	173	44546 → 7351 Len=131
209.206.48.214	10.39.0.115	UDP	158	7351 → 44546 Len=116
209.206.48.214	10.39.0.115	UDP	164	7351 → 44546 Len=122
10.39.0.115	209.206.48.214	UDP	165	44546 → 7351 Len=123
10.39.0.115	209.206.48.214	UDP	530	44546 → 7351 Len=488
209.206.48.214	10.39.0.115	UDP	158	7351 → 44546 Len=116

MR obtains IP on Management VLAN

Performs lookup to connect to Meraki Cloud

Normal dashboard communication (config/firmware download + Cisco PKI enrollment over management connection)

How Does it Work?

Step 4 – MR Initiates EAPOL using new certificate

MR physically connected to MS

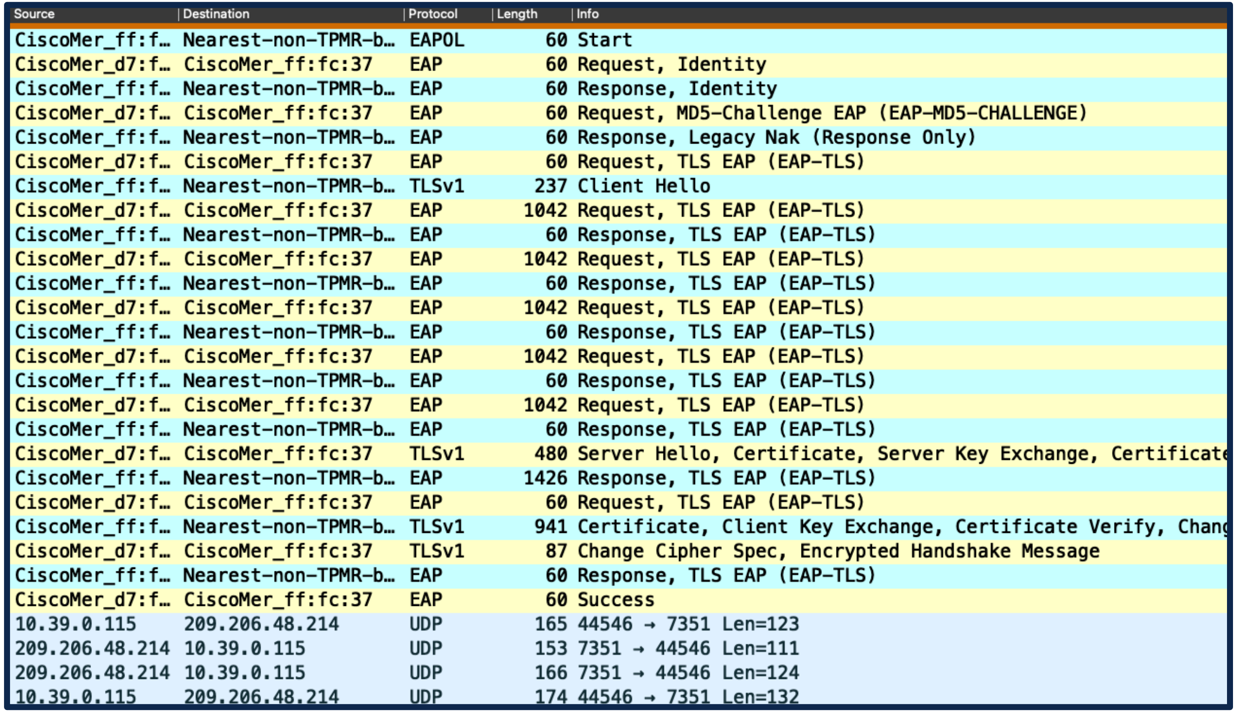
MS permits Meraki dashboard connection for MR

MR requests certificate from Cisco PKI

MR authenticates with acquired certificate

SecureConnect Packet Capture

SecureConnect Authentication via EAP-TLS



```
Source          Destination         Protocol  Length  Info
CiscoMer_ff:f…  Nearest-non-TPMR-b… EAPOL         60 Start
CiscoMer_d7:f…  CiscoMer_ff:fc:37   EAP           60 Request, Identity
CiscoMer_ff:f…  Nearest-non-TPMR-b… EAP           60 Response, Identity
CiscoMer_d7:f…  CiscoMer_ff:fc:37   EAP           60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
CiscoMer_ff:f…  Nearest-non-TPMR-b… EAP           60 Response, Legacy Nak (Response Only)
CiscoMer_d7:f…  CiscoMer_ff:fc:37   EAP           60 Request, TLS EAP (EAP-TLS)
CiscoMer_ff:f…  Nearest-non-TPMR-b… TLSv1        237 Client Hello
CiscoMer_d7:f…  CiscoMer_ff:fc:37   EAP         1042 Request, TLS EAP (EAP-TLS)
CiscoMer_ff:f…  Nearest-non-TPMR-b… EAP           60 Response, TLS EAP (EAP-TLS)
CiscoMer_d7:f…  CiscoMer_ff:fc:37   EAP         1042 Request, TLS EAP (EAP-TLS)
CiscoMer_ff:f…  Nearest-non-TPMR-b… EAP           60 Response, TLS EAP (EAP-TLS)
CiscoMer_d7:f…  CiscoMer_ff:fc:37   EAP         1042 Request, TLS EAP (EAP-TLS)
CiscoMer_ff:f…  Nearest-non-TPMR-b… EAP           60 Response, TLS EAP (EAP-TLS)
CiscoMer_d7:f…  CiscoMer_ff:fc:37   EAP         1042 Request, TLS EAP (EAP-TLS)
CiscoMer_ff:f…  Nearest-non-TPMR-b… EAP           60 Response, TLS EAP (EAP-TLS)
CiscoMer_d7:f…  CiscoMer_ff:fc:37   EAP         1042 Request, TLS EAP (EAP-TLS)
CiscoMer_ff:f…  Nearest-non-TPMR-b… EAP           60 Response, TLS EAP (EAP-TLS)
CiscoMer_d7:f…  CiscoMer_ff:fc:37   TLSv1        480 Server Hello, Certificate, Server Key Exchange, Certificate
CiscoMer_ff:f…  Nearest-non-TPMR-b… EAP         1426 Response, TLS EAP (EAP-TLS)
CiscoMer_d7:f…  CiscoMer_ff:fc:37   EAP           60 Request, TLS EAP (EAP-TLS)
CiscoMer_ff:f…  Nearest-non-TPMR-b… TLSv1        941 Certificate, Client Key Exchange, Certificate Verify, Chang
CiscoMer_d7:f…  CiscoMer_ff:fc:37   TLSv1         87 Change Cipher Spec, Encrypted Handshake Message
CiscoMer_ff:f…  Nearest-non-TPMR-b… EAP           60 Response, TLS EAP (EAP-TLS)
CiscoMer_d7:f…  CiscoMer_ff:fc:37   EAP           60 Success
10.39.0.115     209.206.48.214      UDP          165 44546 → 7351 Len=123
209.206.48.214  10.39.0.115         UDP          153 7351 → 44546 Len=111
209.206.48.214  10.39.0.115         UDP          166 7351 → 44546 Len=124
10.39.0.115     209.206.48.214      UDP          174 44546 → 7351 Len=132
```

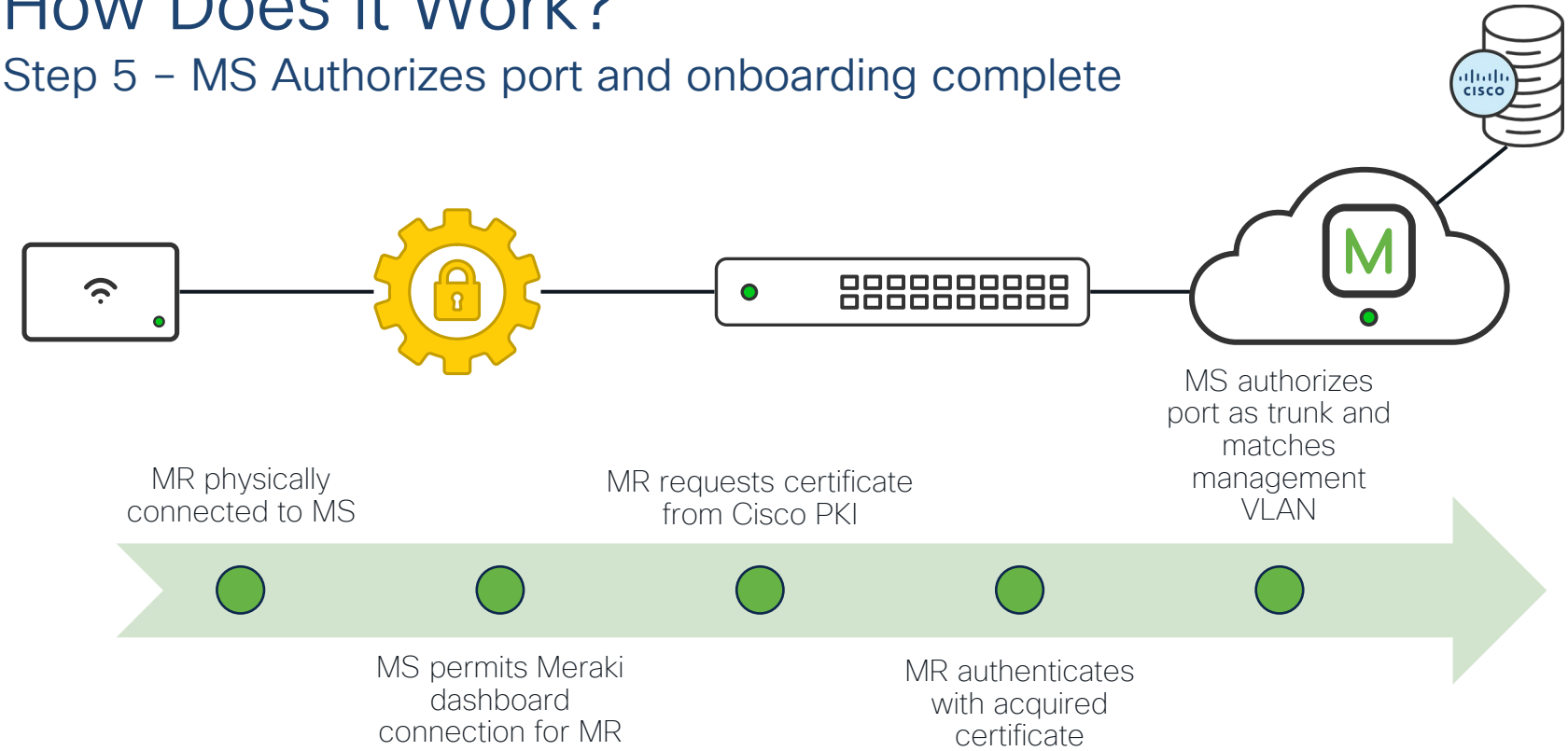
MR initiates EAPOL Start once client cert received

EAP-TLS Authentication Exchange

Cloud management traffic continues

How Does it Work?

Step 5 – MS Authorizes port and onboarding complete



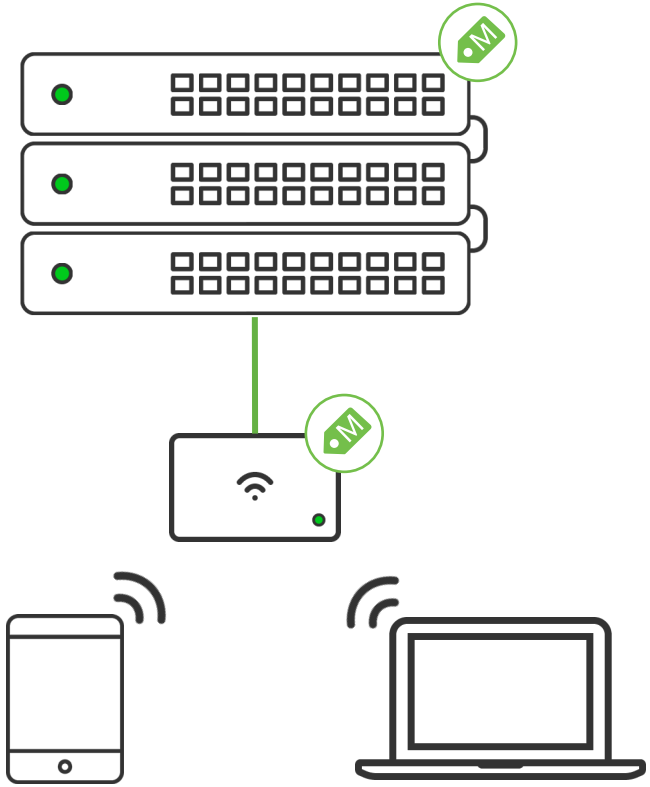
SecureConnect Demo

Building Zero Trust with Meraki Adaptive Policy

cisco Live!

Adaptive Policy

- Intent-based policy leveraging inline Security Group Tags as identity
- One consistent policy across networks
- Micro-segmentation enforcement



What do I need to enable Adaptive Policy?

MS390

MS Advanced License

802.11ax/ac**

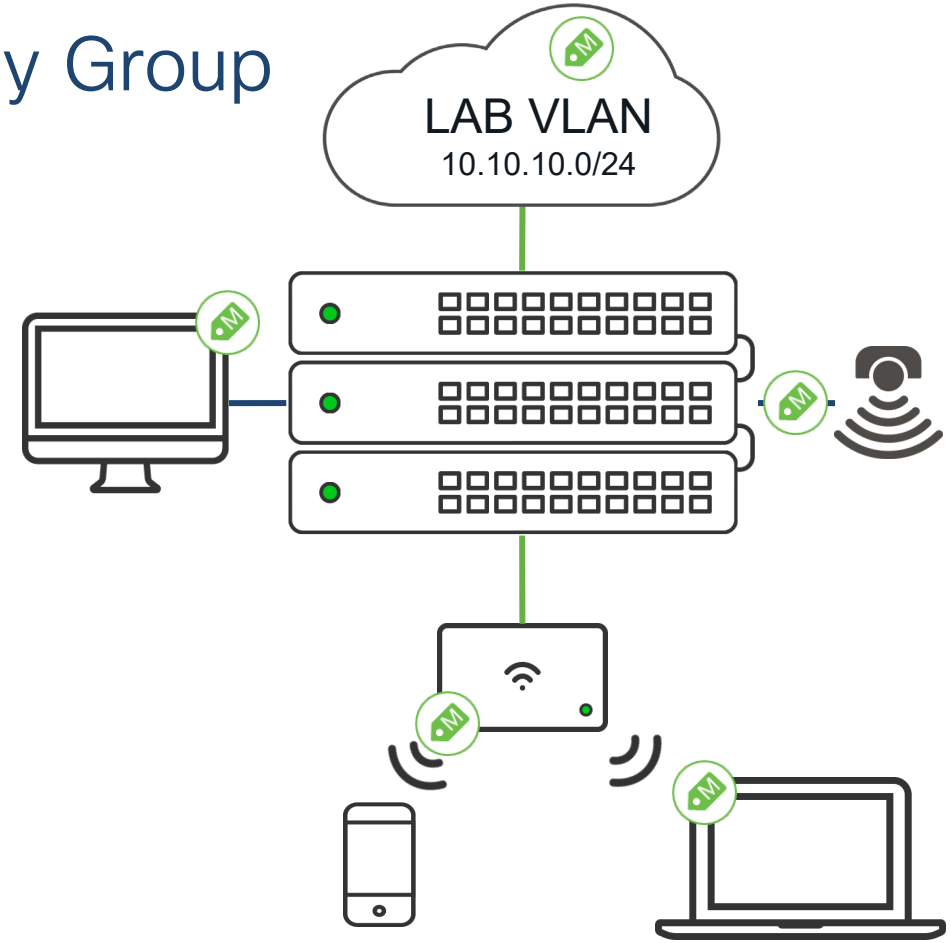
MR Advanced License

** wave 2 only

Assigning Adaptive Policy Group

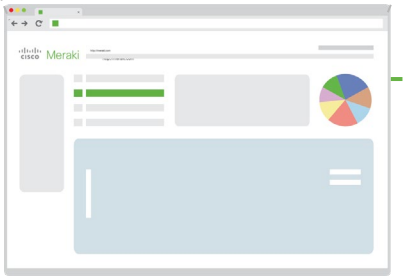
Groups/tags can be applied in a number of ways:

- Statically assigned to a switch port
- Static assignment per SSID
- Dynamic assignment via RADIUS
- Static Prefix to SGT Mapping



One Consistent Policy Across All Sites

SRC | DST	Employee	IoT	IoT Server
Employee	✔	✘	✔
IoT	✘	✘	✔
IoT Server	✔	✔	✔



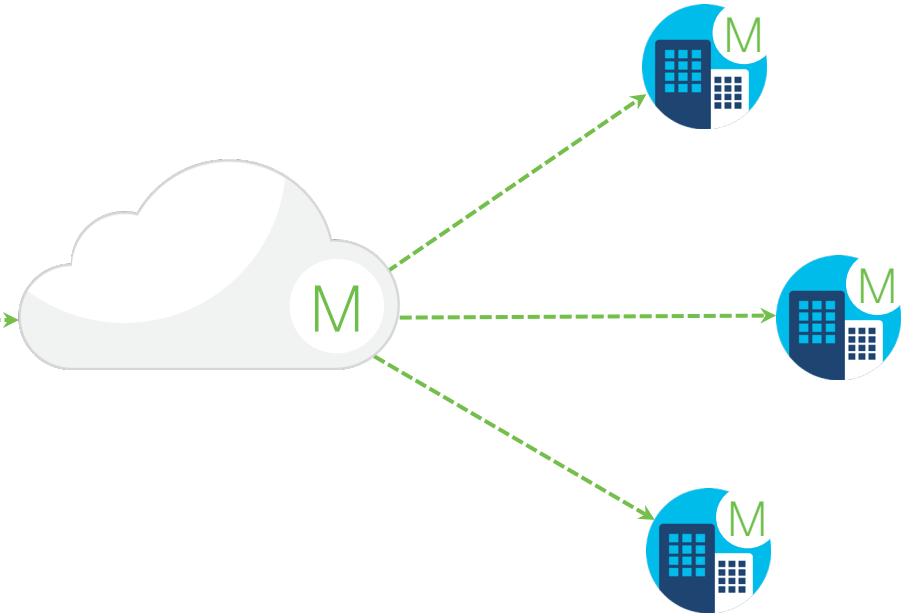
Policy & Groups are configured in dashboard and pushed to Adaptive Policy nodes like any other Meraki configuration change

API First Development!

All settings available via Meraki dashboard APIs

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

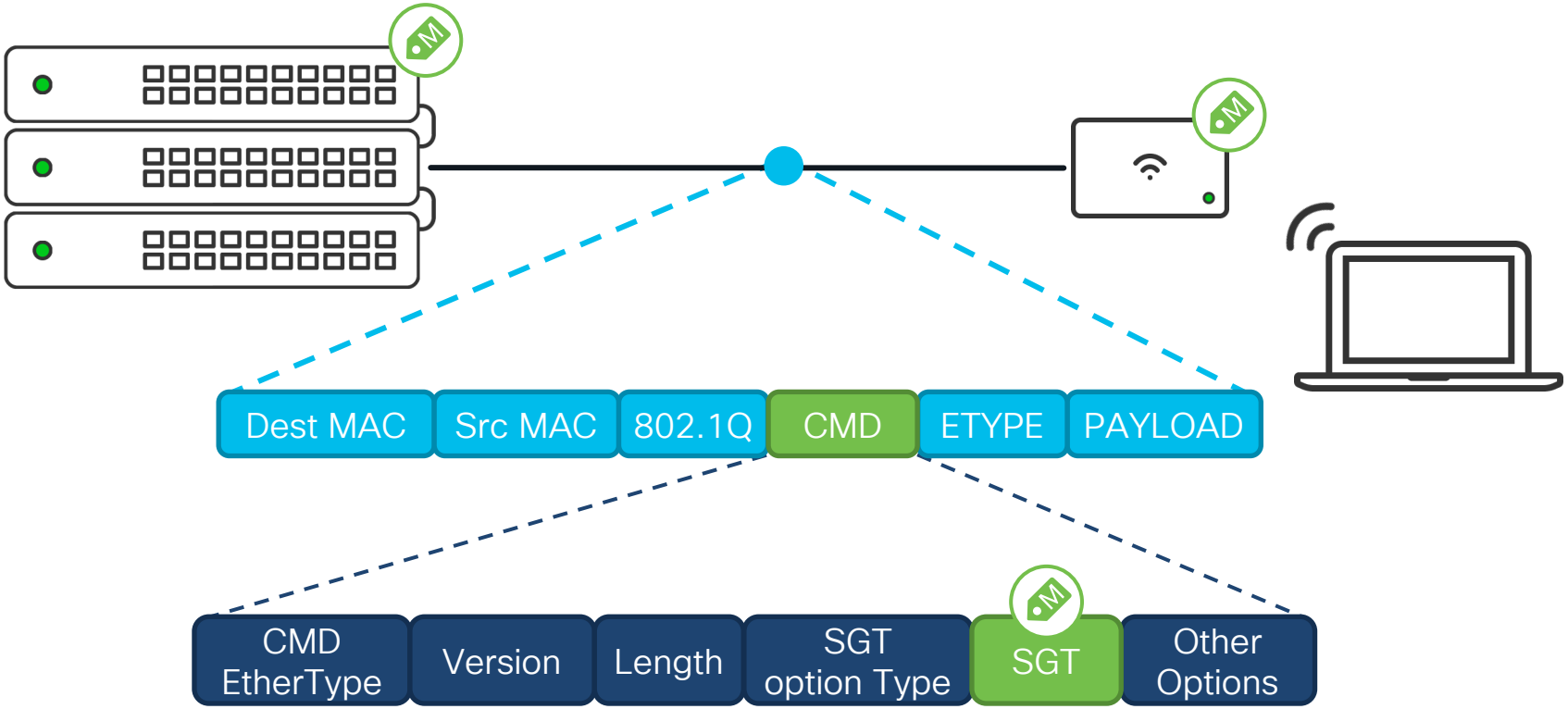
```
adaptivePolicy/
|__ groups
|__ acls
|__ bindings
|__ settings
```



Adaptive Policy Technical Details

cisco Live!

What are SGTs?



SGT Packet Capture

Apply a display filter ...<⌘/>

No.	Time	VLAN	Source	Destination	Protocol	Port	Length	Info
	8.914741	1011	10.1.1.109	209.206.52.14	UDP	7351	185	45951 → 7351 Len=131
	8.957899	1011	209.206.52.14	10.1.1.109	UDP	45951	170	7351 → 45951 Len=116
	8.958062	1011	209.206.52.14	10.1.1.109	UDP	45951	214	7351 → 45951 Len=160
	8.958813	1011	10.1.1.109	209.206.52.14	UDP	7351	177	45951 → 7351 Len=123
	8.965981	1011	10.1.1.109	209.206.52.14	UDP	7351	1325	45951 → 7351 Len=1271
	8.966280	1011	10.1.1.109	209.206.52.14	UDP	7351	1325	45951 → 7351 Len=1271
	8.966583	1011	10.1.1.109	209.206.52.14	UDP	7351	1325	45951 → 7351 Len=1271

```
> Frame 15: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
> Ethernet II, Src: CiscoMer_8a:65:41 (e0:cb:bc:8a:65:41), Dst: Cisco_03:15:ea (00:2f:5c:03:15:ea)
v 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1011
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0011 1111 0011 = ID: 1011
    Type: CiscoMetaData (0x8909)
v Cisco MetaData
    Version: 1
    Length: 1
    Options: 0x0001
    SGT: 2
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.1.1.109, Dst: 209.206.52.14
> User Datagram Protocol, Src Port: 45951, Dst Port: 7351
> Data (123 bytes)
```

Cisco MetaData
SGT=2

SGT Order of Application

Static Tag Applied to Port/SSID

Tag Received via RADIUS

192.0.2.0/24

Policy Object to Tag Mapping

MS Port Configuration and Behavior

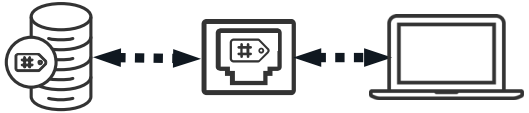
Peer SGT Capable

- Trust received tags/send tagged frames on trunk ports
- Untagged frames tagged have port Group applied
- Used when connecting MS to Adaptive Policy capable MS/MR

Static Tag Assigned

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

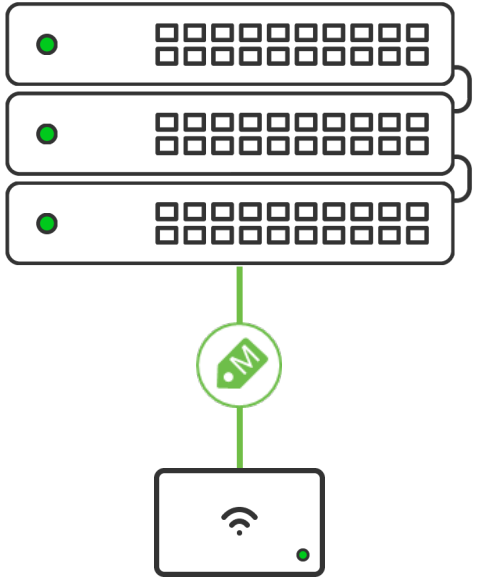
802.1x Assigned



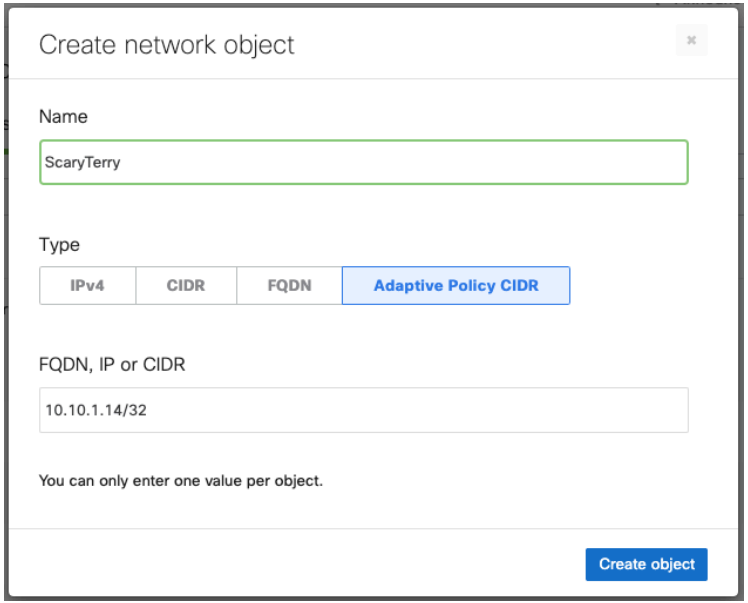
- Per-Session assignment based on RADIUS response
- Static fallback performed through Prefix to SGT map

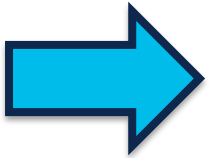
Connecting MR to Adaptive Policy MS

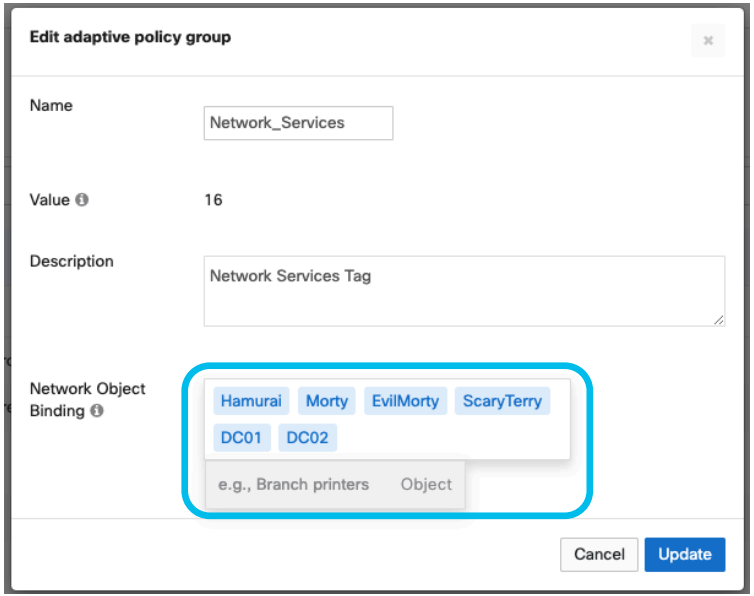
- Meraki Simple!
- No MR configuration needed
- MR recognizes inbound CMD frames
- Automatically switches to CMD encapsulation
- Applies infrastructure SGT to management traffic



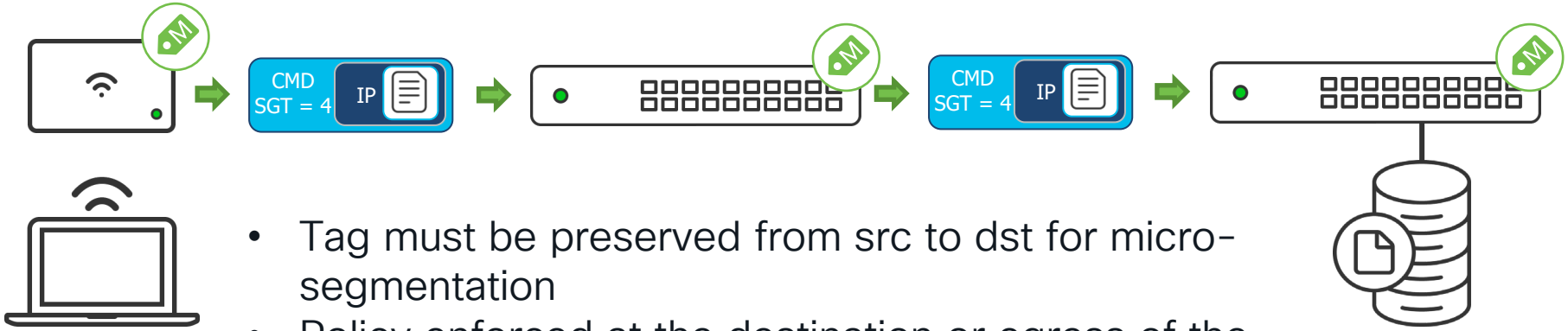
Using Policy Objects to map IP to SGT





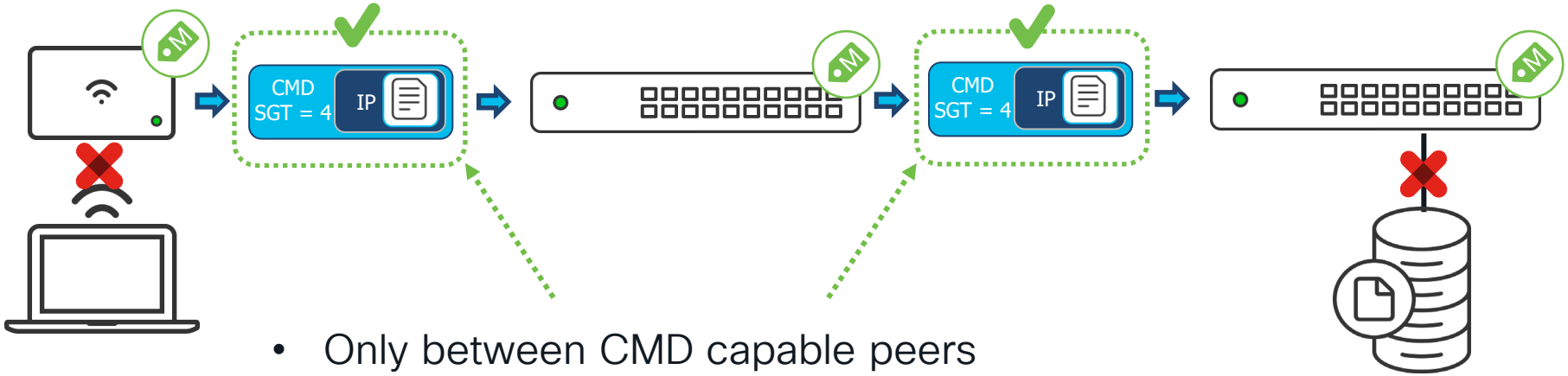


Tag Application and Preservation



- Tag must be preserved from src to dst for micro-segmentation
- Policy enforced at the destination or egress of the Adaptive Policy Domain

So where do we see tags?



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

SGT via RADIUS

Assign SGT values using the AV Pair:
cisco-av-pair:cts:security-group-tag = {SGT value in HEX}-{revision number}

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
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

Adaptive Policy Scaling

- Maximum of 60 tags
- Maximum 10 custom ACLs per **tag <> tag** relationship
- Maximum 16 ACE **entries** per custom ACL
- Endpoint scale is based on network/platform hardware and not on SGT/ACL

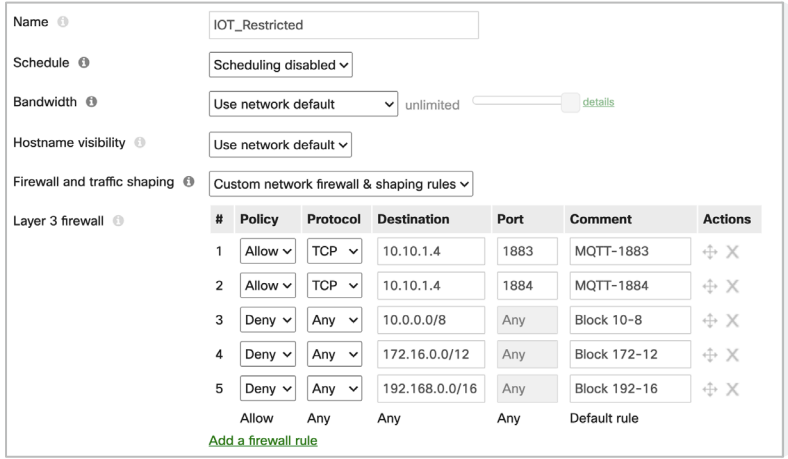
Adaptive Policy Demo

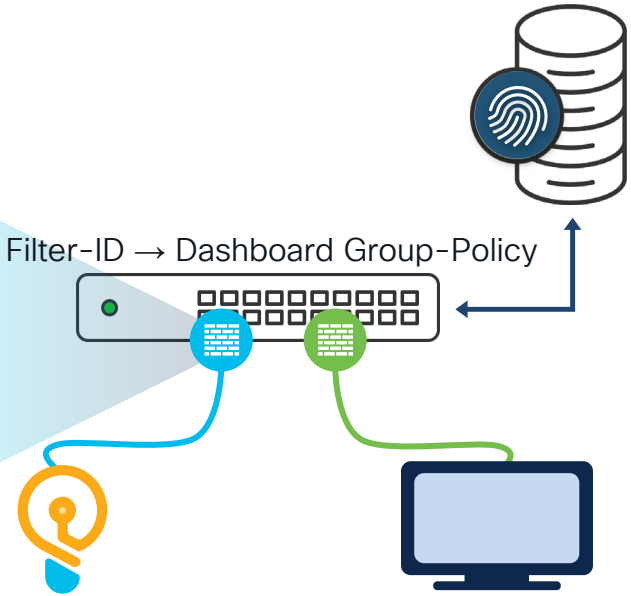
Group Policy ACLs

Group Policy ACL

Granular Wired Permissions

- Per-session 802.1X inbound ACL
- dACL-like functionality
- ACL orchestration via Dashboard
- On-the-fly ACL update (no CoA required)

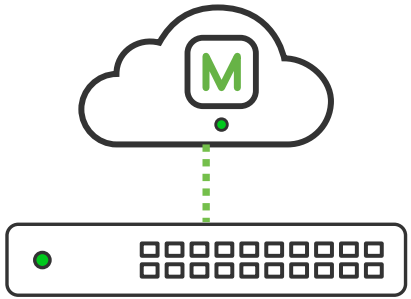




Supported on MS210/225/250/350/355/425/450

How Does it Work?

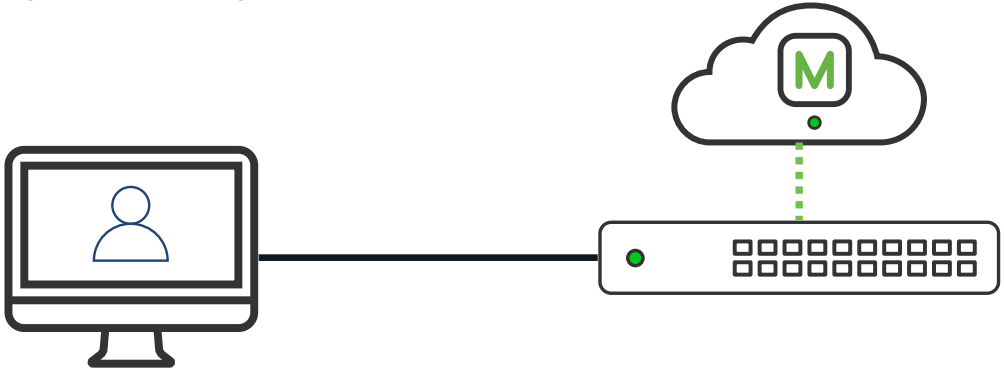
Step 1 - GP ACL downloaded



MS Receives GP ACL as config from dashboard

How Does it Work?

Step 2 – Endpoint connected

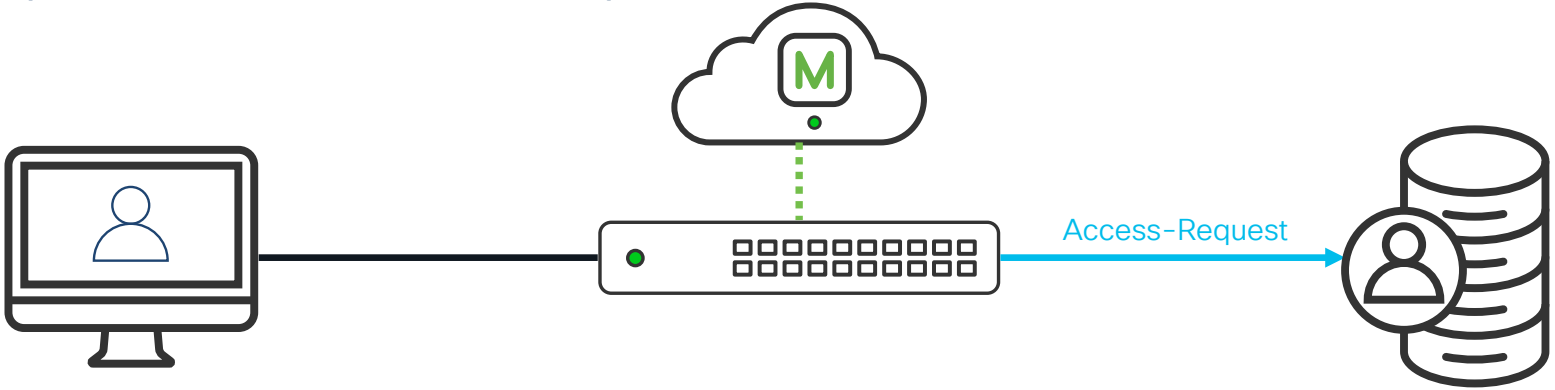


MS Receives GP ACL as config from dashboard

Endpoint connects to network

How Does it Work?

Step 3 – RADIUS Access-Request



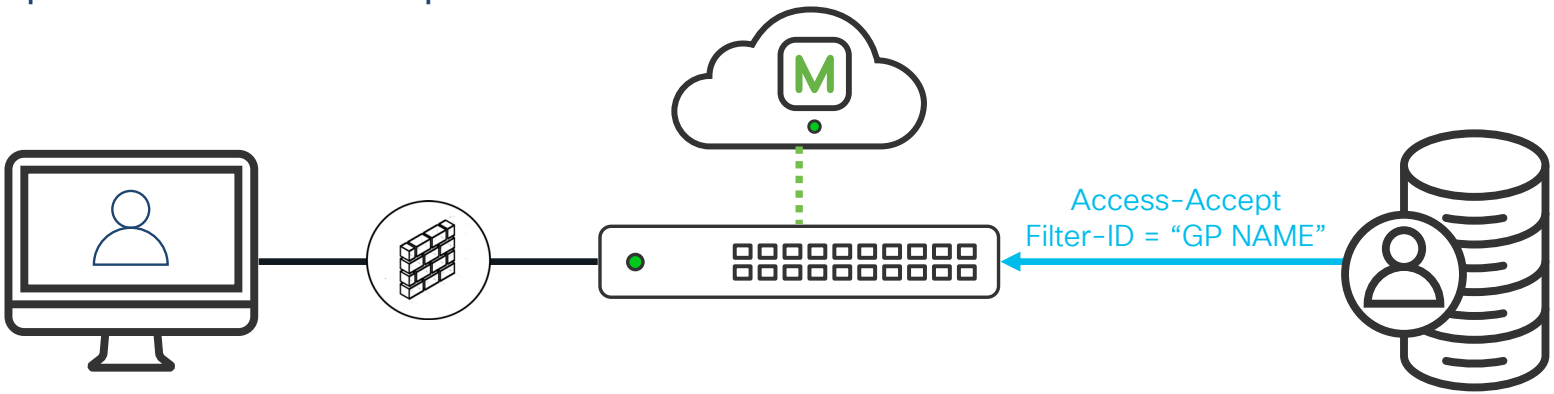
MS Receives GP ACL as config from dashboard

Endpoint connects to network

MS Sends RADIUS Access-Request

How Does it Work?

Step 4 – RADIUS Responds



MS Receives GP ACL as config from dashboard

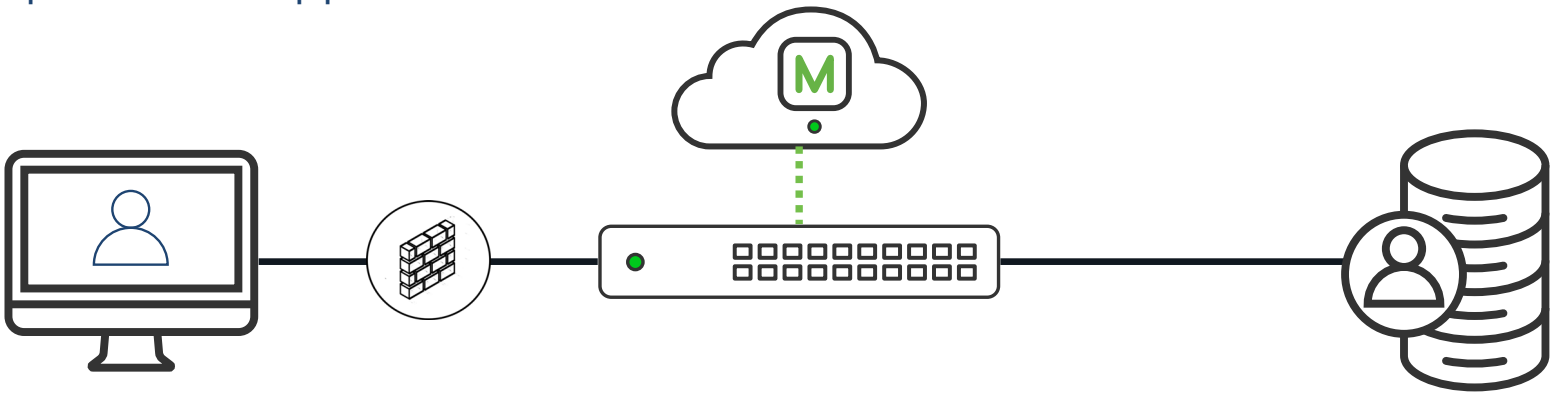
Endpoint connects to network

MS Sends RADIUS Access-Request

Server Responds with Access-Accept & Filter-ID AV-Pair

How Does it Work?

Step 6 – ACL Applied



MS Receives GP ACL as config from dashboard

Endpoint connects to network

MS Sends RADIUS Access-Request

Server Responds with Access-Accept & Filter-ID AV-Pair

MS Applies GP ACL to IP traffic

ACL Entry Re-use

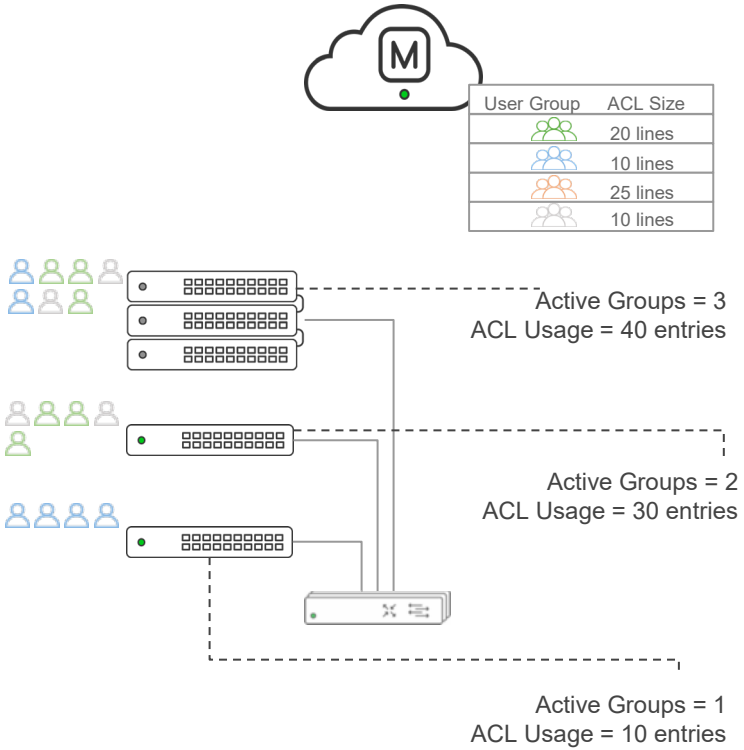
- Up to 20 active groups
- Maximum 600 active ACL entries per switch
- Group is active if there is an authenticated client with that policy applied
- ACL entry utilization does not increase with increase in number of clients using same group

$1_{\text{client}} \times 1_{\text{group}} \times 10_{\text{rules}} = 10_{\text{hardware ACL entries}}$

$2_{\text{clients}} \times 1_{\text{group}} \times 10_{\text{rules}} = 10_{\text{hardware ACL entries}}$

$2000_{\text{clients}} \times 1_{\text{group}} \times 10_{\text{rules}} = 10_{\text{hardware ACL entries}}$

But 2000 MAC addresses with ACL applied!



Group Policy ACLs Demo

Conclusion

Use Meraki as a building block to Zero Trust

- The latest Meraki Policy solutions enable building a Zero Trust workplace
- SecureConnect brings the concept of Zero Trust to infrastructure devices
- Adaptive Policy leverages mature security technologies to deliver a scalable, simple to deploy, LAN infrastructure

Continue your education

- Demos in the Cisco campus
- Meet the engineer 1:1 meetings
- Walk-in labs
- Related sessions

Thank you


TURN
IT
UP
cisco Live!
#CiscoLive