
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Segmentation Simplified

A Case Study of Meraki Adaptive Policy and Cisco TrustSec

Lee Sudduth, Customer Delivery Architect
Praveen Poojary, Customer Delivery Architect

BRKXAR-2005

Cisco Webex App

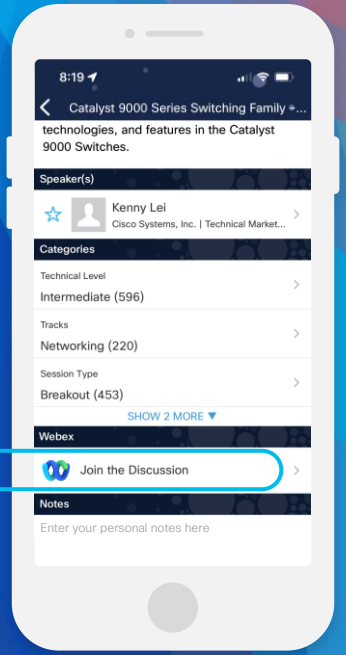
Questions?

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 June 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKXAR-2005

About Us

Praveen Poojary

Customer Delivery Architect

12 Years in Cisco

#3xCCIE

#CCDE

Lee Sudduth

Customer Delivery Architect

23 Years in Cisco

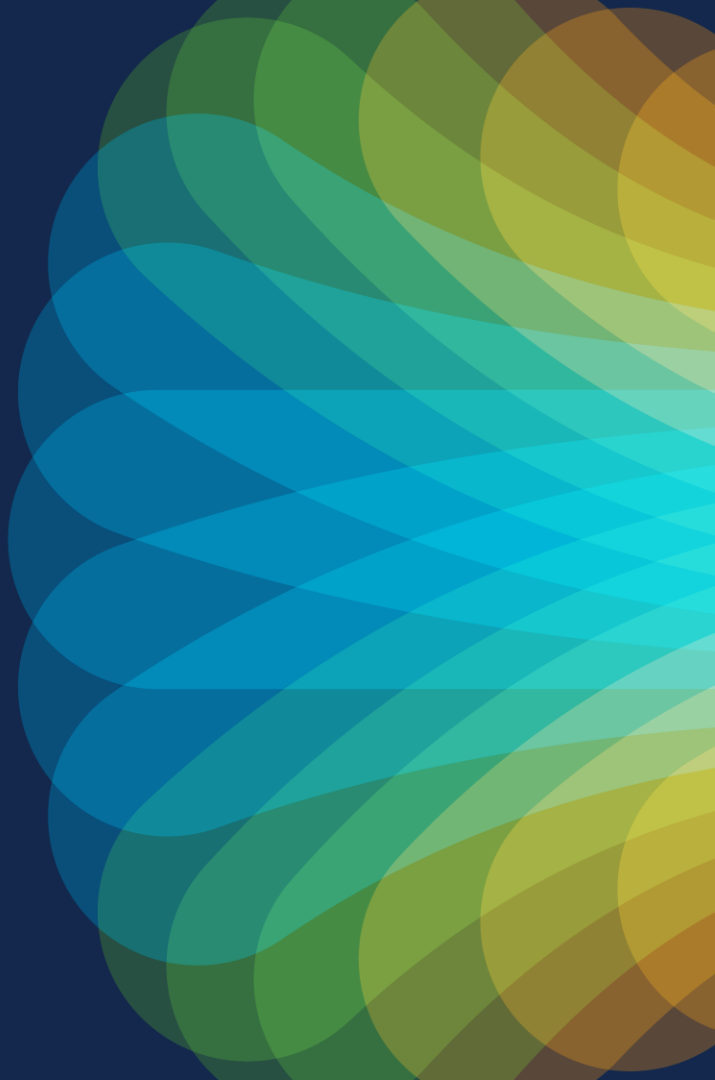
#CCIE

#CCDE

Agenda

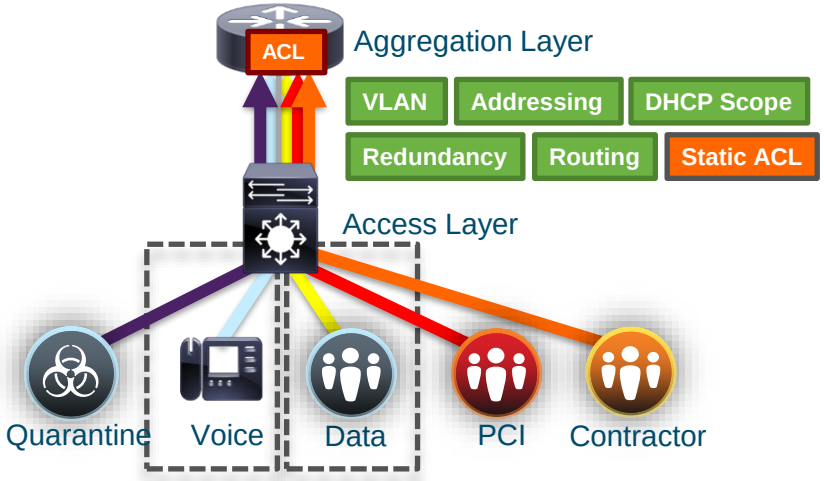
- Technology Overview
  - Scalable Group Tag
  - Adaptive Policy
- Case Study
  - Design Considerations and Best Practices
- Conclusion

Technology Overview



Traditional Segmentation

Design needs to be replicated for floors, buildings, offices, and other facilities. Cost could be extremely high

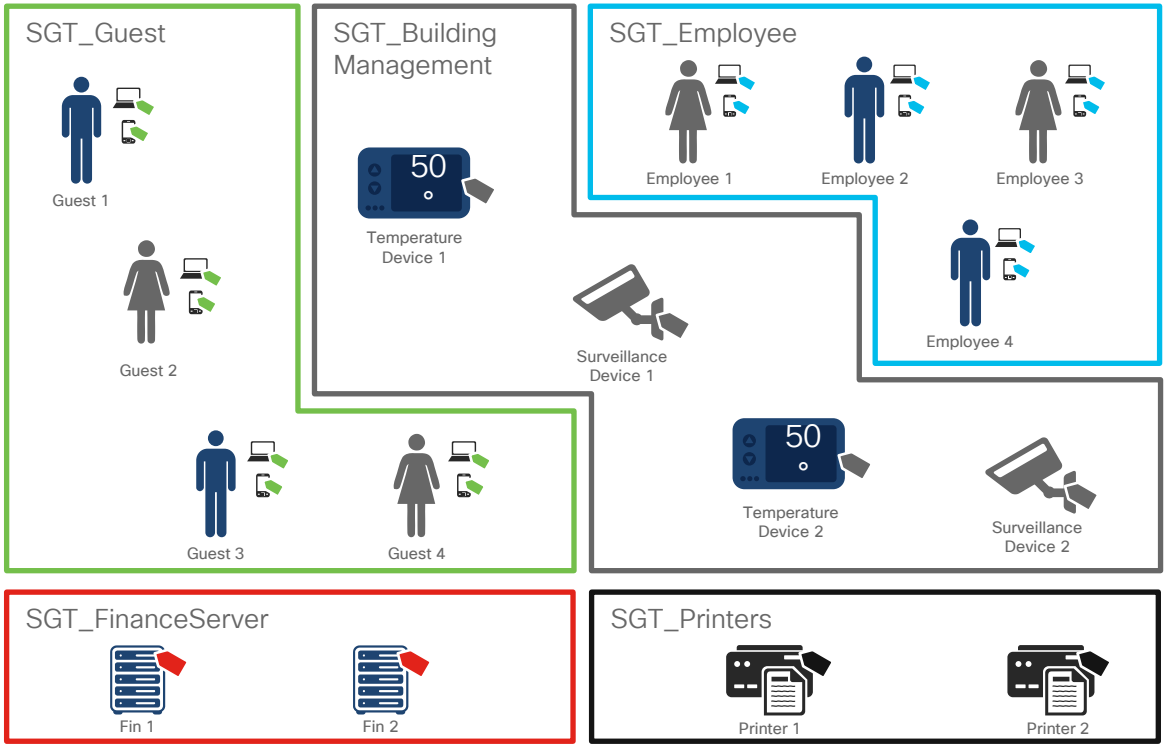


Simple Segmentation with 2 VLANs

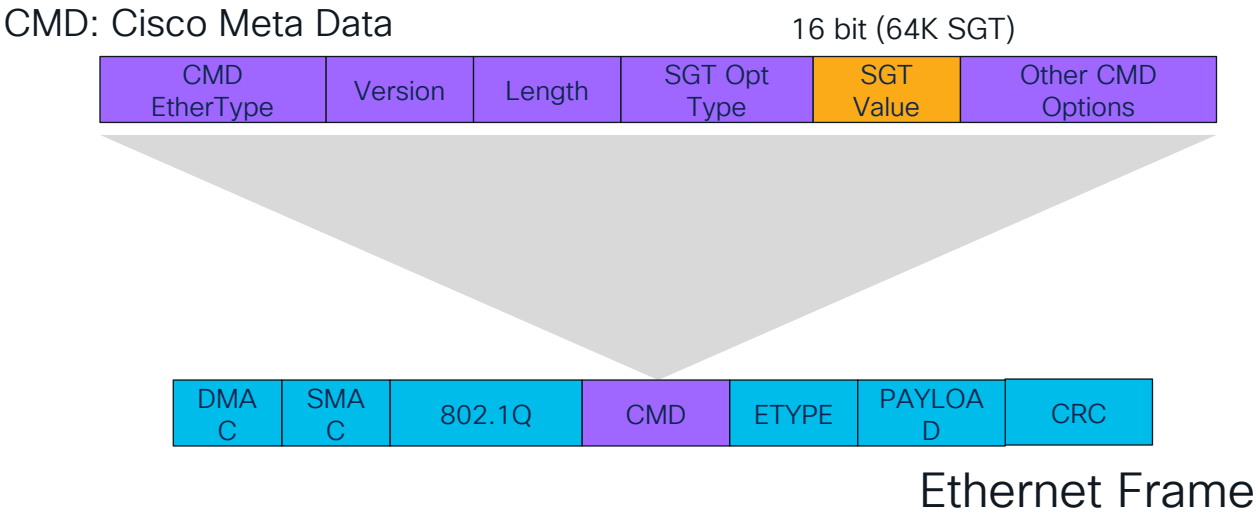
More Policies using more VLANs

User Segmentation for Effective Policy Enforcement

- Implement business-based groupings to ensure consistent policy and access regardless of network topology.
- Utilize attributes like user role, location, and device type to define group assignments and access control.



What are Scalable Group Tag's(SGT)?

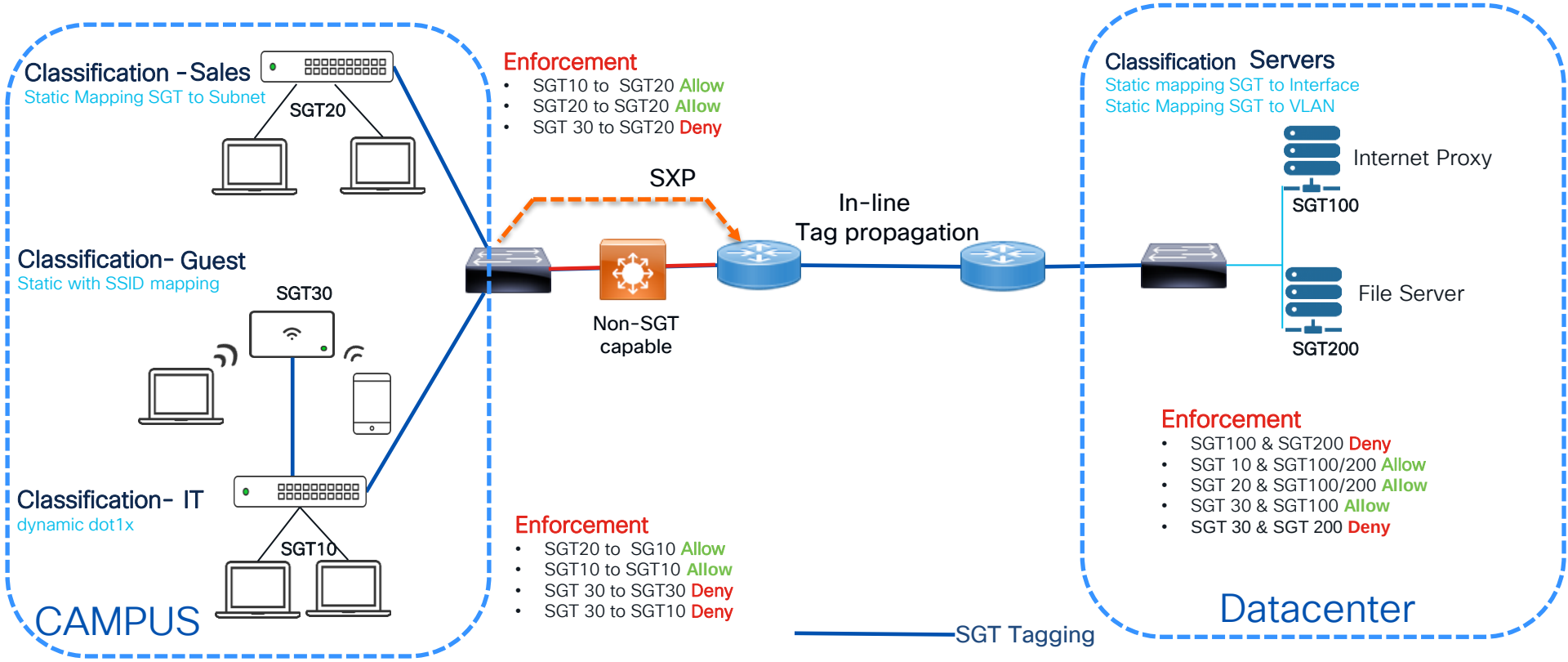


CMD Packet Structure

```
> Frame 310: 1325 bytes on wire (10600 bits), 1325 bytes captured (10600 bits)
> Ethernet II, Src: CiscoMer_75:65:00 (38:84:79:75:65:00), Dst: Cisco_9c:44:bf (70:b3:17:9c:44:bf)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1
v Cisco MetaData
    Version: 1
    Length: 1
    Options: 0x0001
    SGT: 2
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src:                 Dst: 209.206.51.215
> User Datagram Protocol, Src Port: 40152, Dst Port: 7351
> Data (1271 bytes)
```

MS390 Cat9k

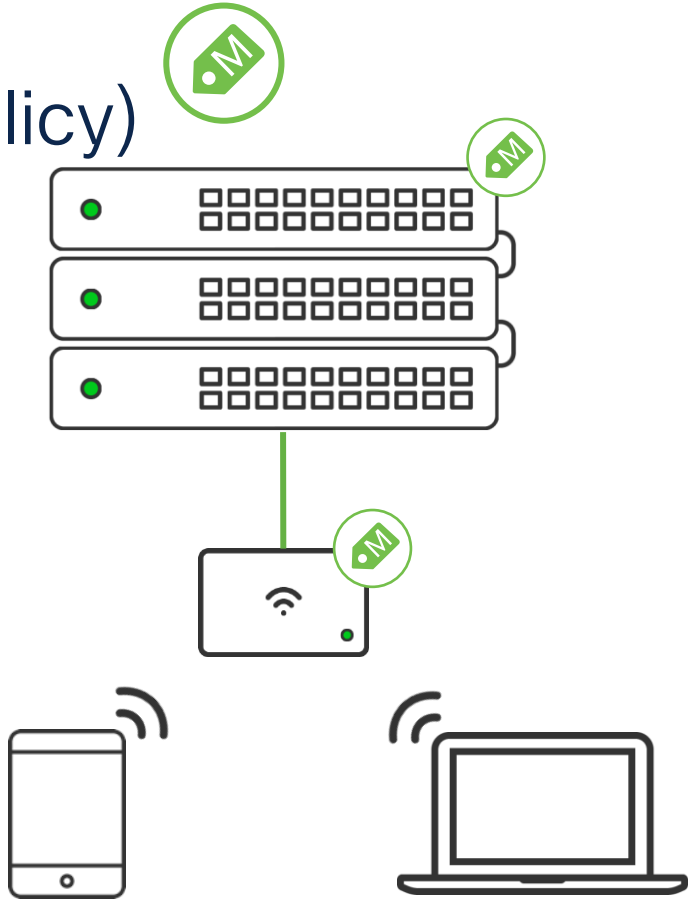
Secure Network Infrastructure with TrustSec



Meraki Adaptive Policy

TrustSec in Meraki (Adaptive Policy)

- Identity and policy based on tags
- Uses inline SGTs
- Org-wide policy based on intent, not IP
- Provides micro-segmentation within VLANs
- Flexible tag assignment



Supported platforms:

- **MR:** all Wifi5 wave 2, Wifi6, and Wifi6E MR and CW access points
- **MS390**: Switching platform
- **MX/Z3+:** all models capable of running MX18+ firmware

Flexible Tag Assignment

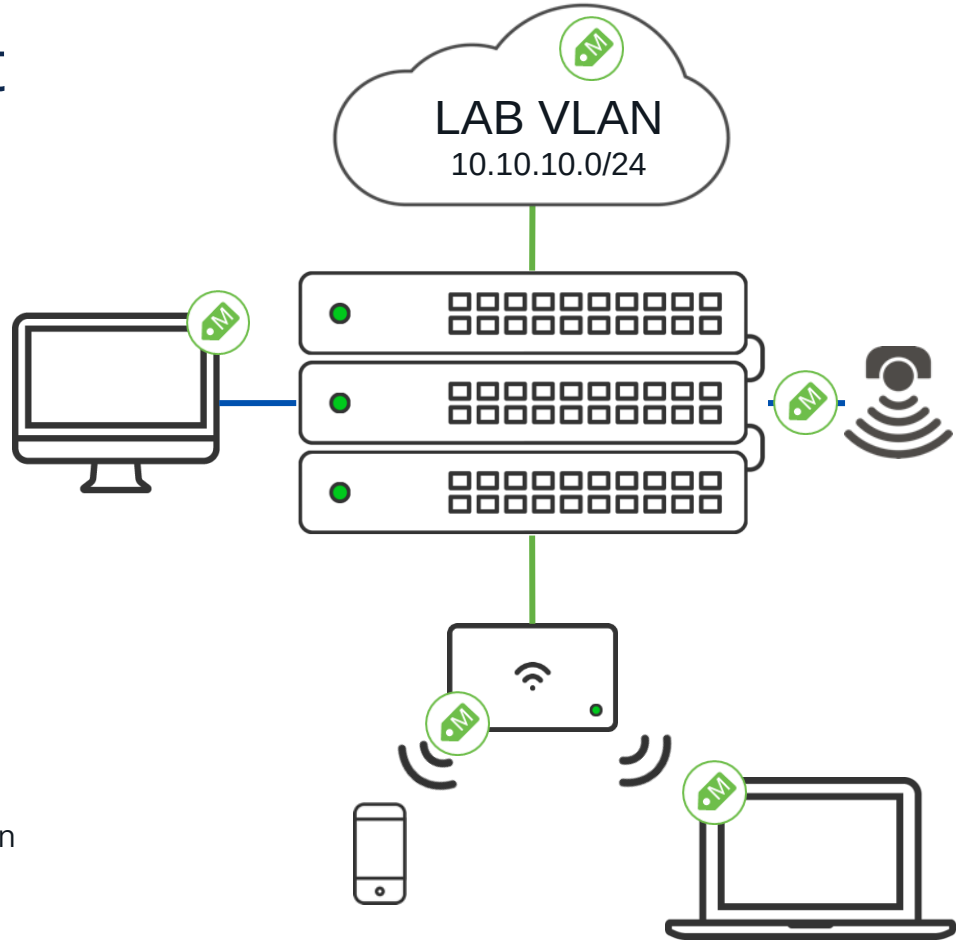
Tags can be applied in many different ways:

Statically assigned to a switch port
- Wired IOT Sensors

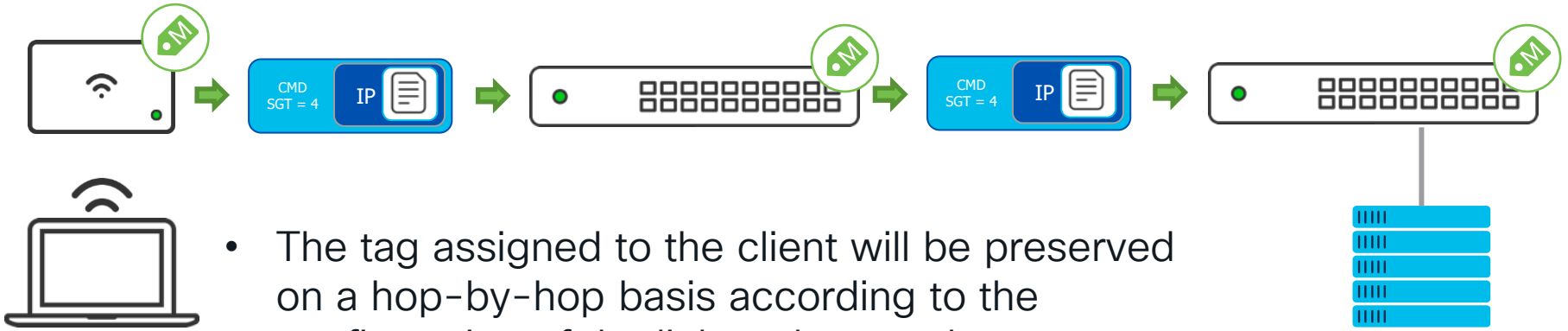
Static assignment per SSID
- Guest Users

Dynamic assignment via RADIUS
- Wired & Wireless 802.1x

Static IP to SGT Mapping
- Last resort to map traffic to an SGT
- Uses network objects as source for mapping
- Available w/ network object public beta – coming soon

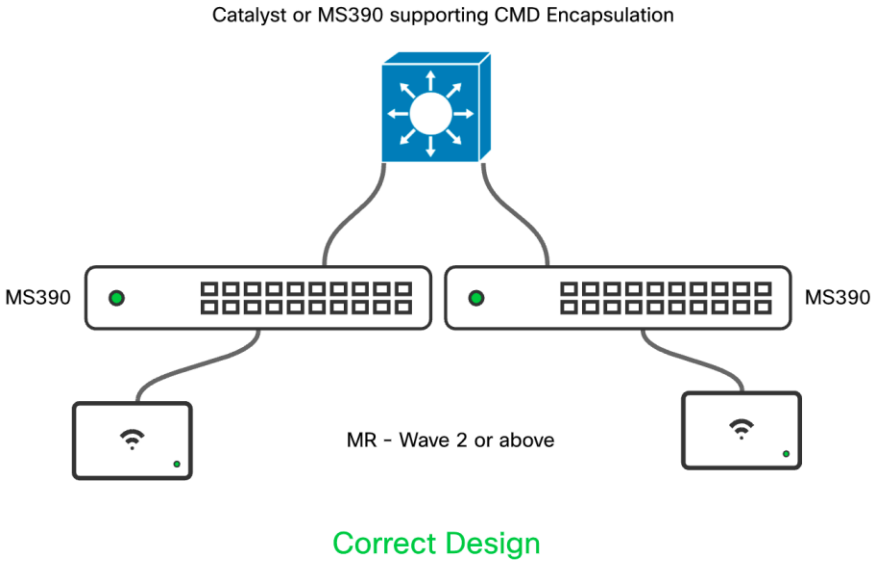


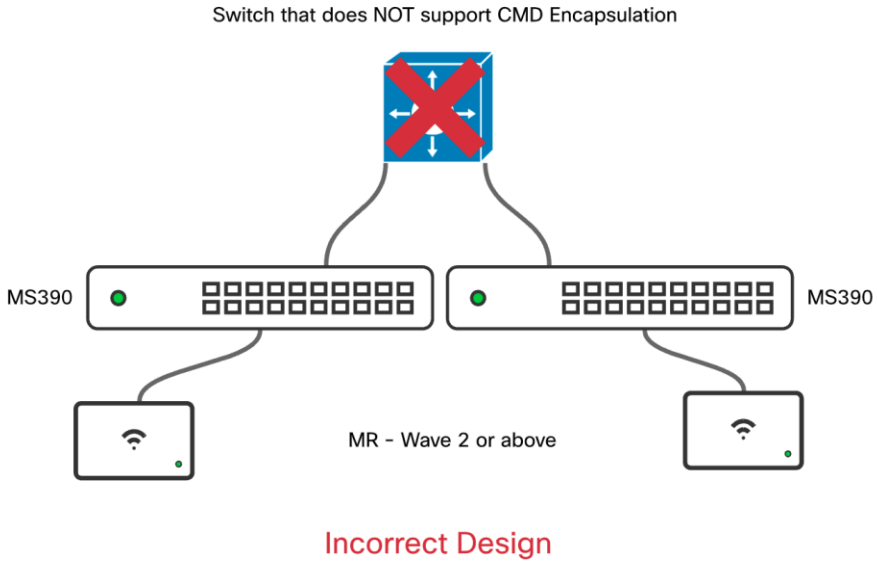
Tag Application and Preservation



- The tag assigned to the client will be preserved on a hop-by-hop basis according to the configuration of the link to the next hop
- Entire path must support inline SGTs
- The tag can be seen on the network device, not on the sending/receiving client

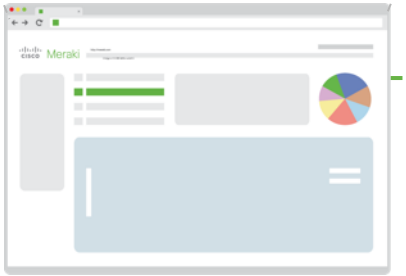
Co-working of Meraki with other Cisco Devices





One Consistent Policy Across All Sites

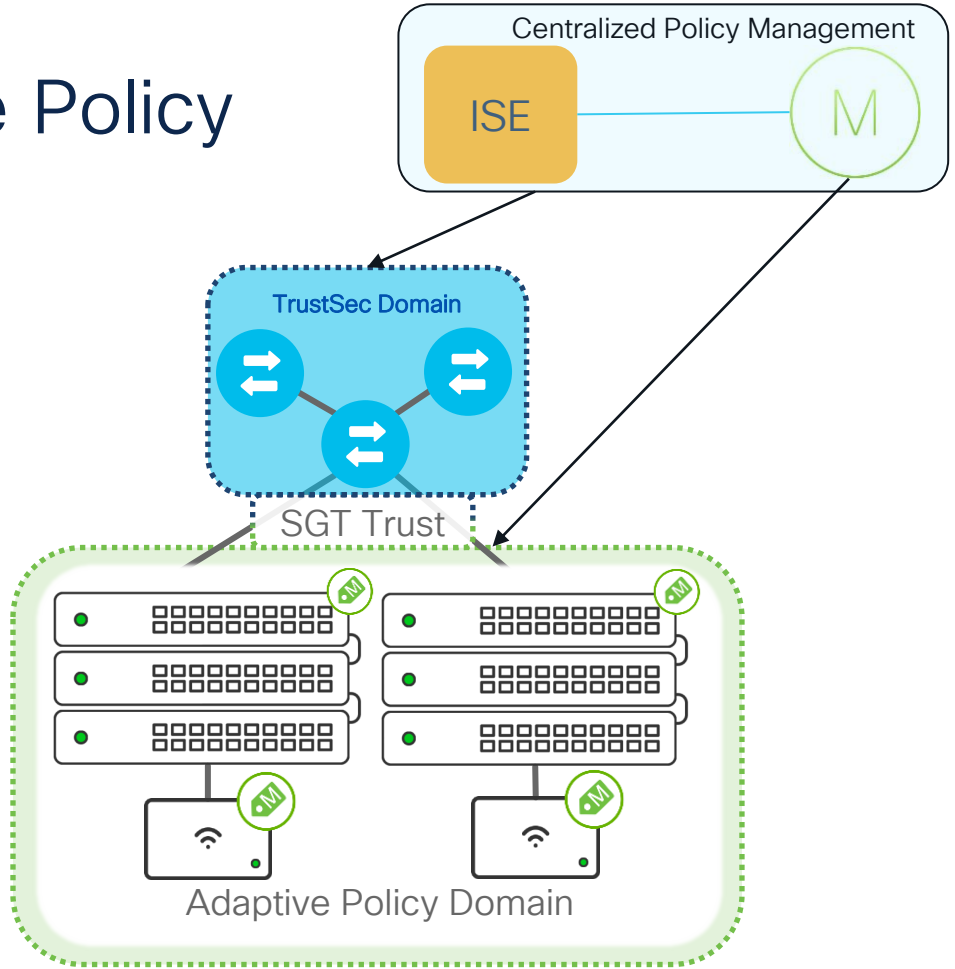
SRC | DST	Employee	IoT	IoT Server
Employee	✔	✘	✔
IoT	✘	✘	✔
IoT Server	✔	✔	✔



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

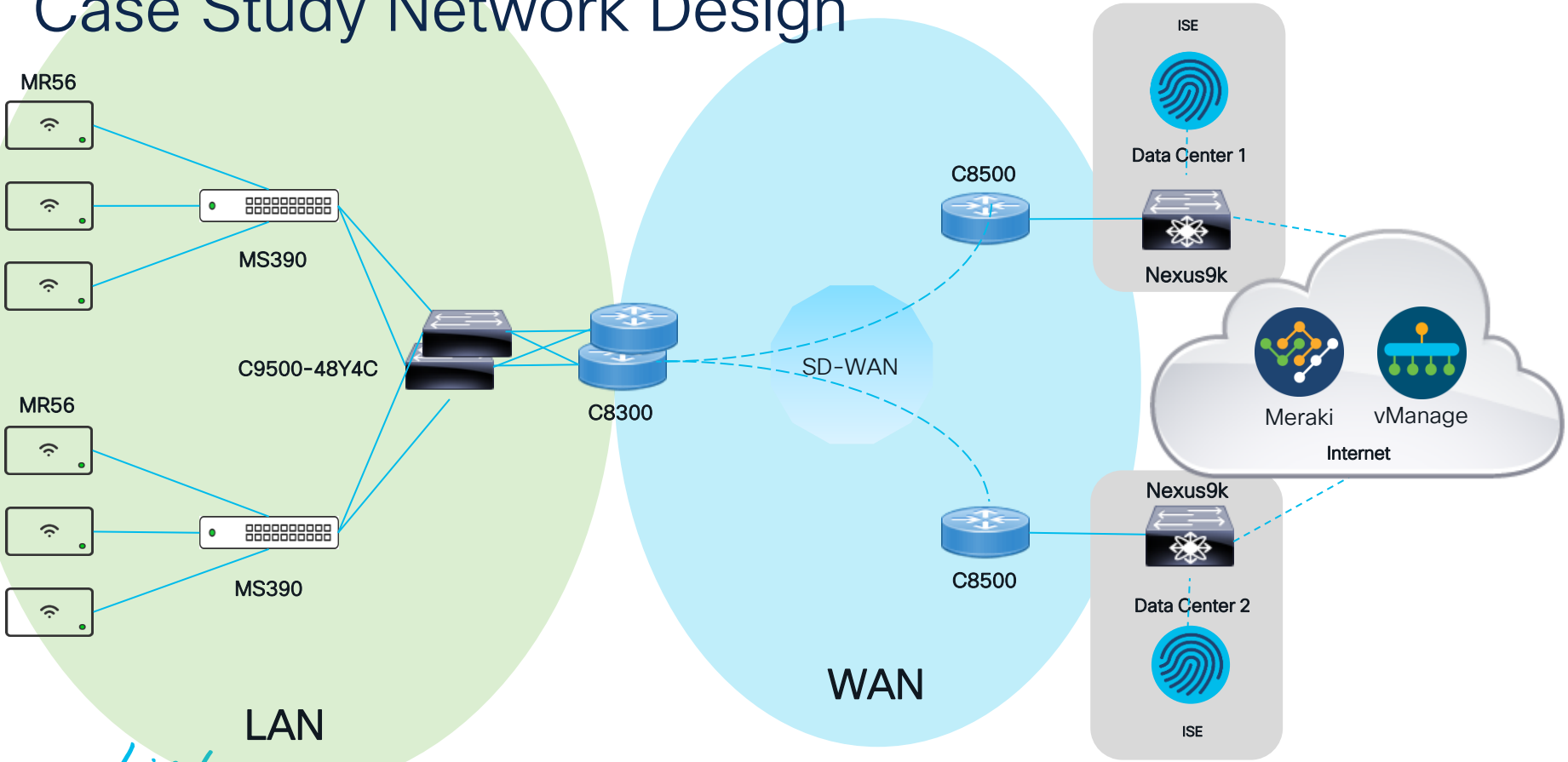
TrustSec and Adaptive Policy

- ISE as the central policy source
- ISE3.2 P1 and later got native capability to integrate with Meraki Dashboard using API
- Tag & Policy propagation from ISE to Meraki Dashboard
- Use external container for bi-directional policy sync *(Optional)*

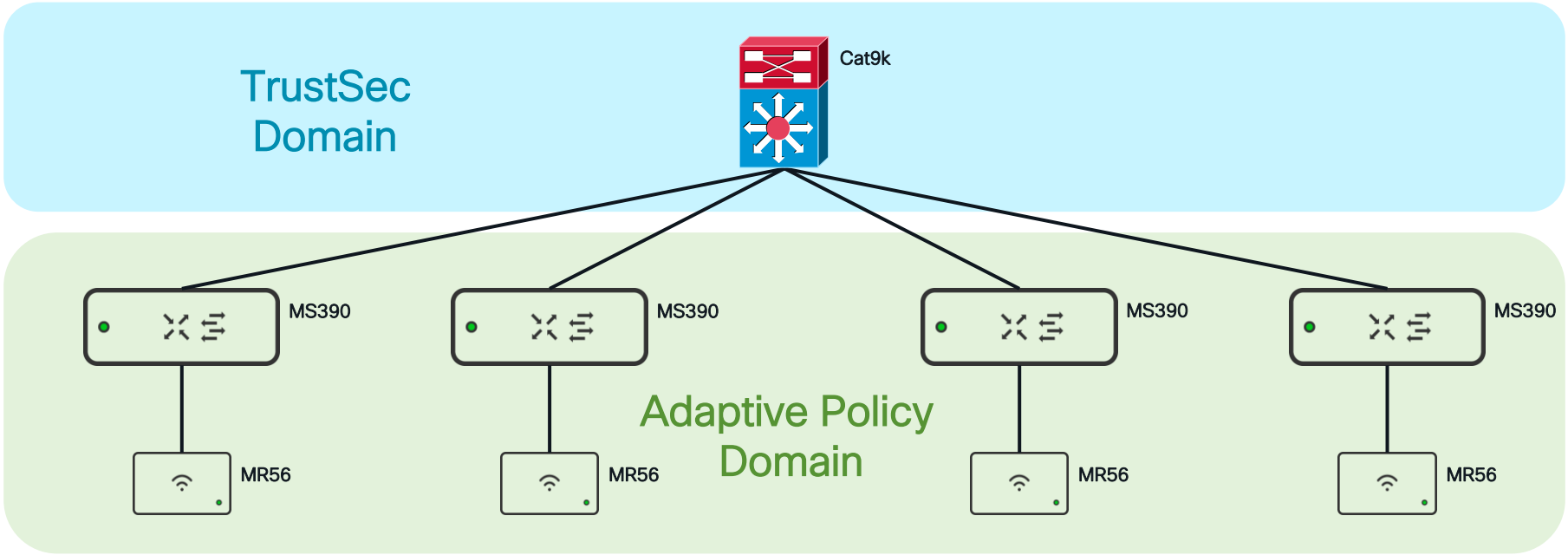


Case Study

Case Study Network Design



Meraki Access / Catalyst Core
Core: Propagate and Enforce



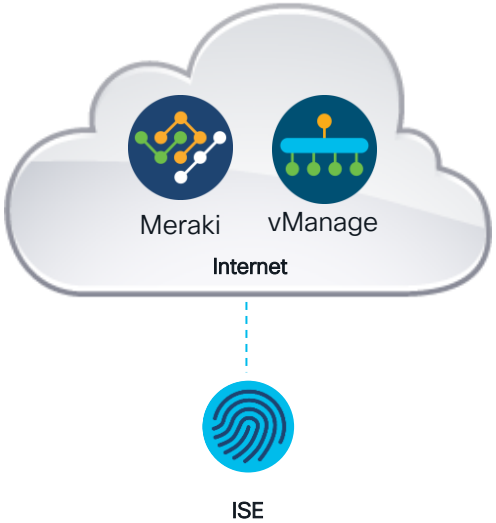
Case Study Orchestration Design

Meraki Dashboard
- Wireless Access

Meraki Dashboard
- Wired Access
- Cat9k Core Switches

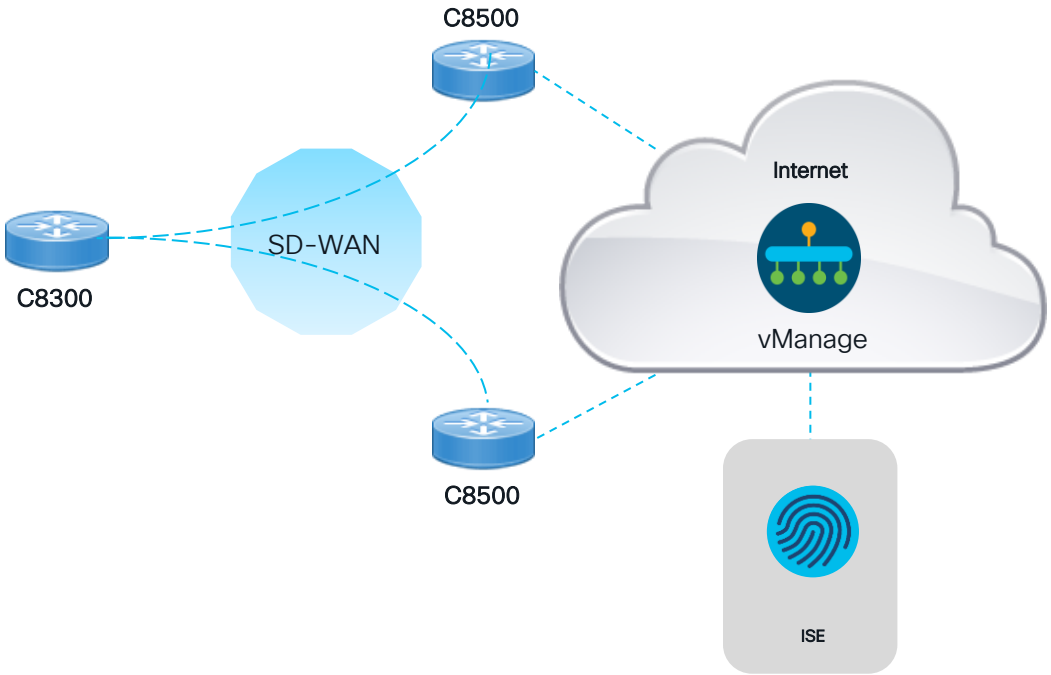
vManage
- SD-WAN

ISE/ Meraki Dashboard
- Adaptive Policy



SD-WAN Overlay Design

- C8300 cEdge Router
- C8500 cEdge Router
- Routing to Data Center via C8500
- TrustSec Security Policy



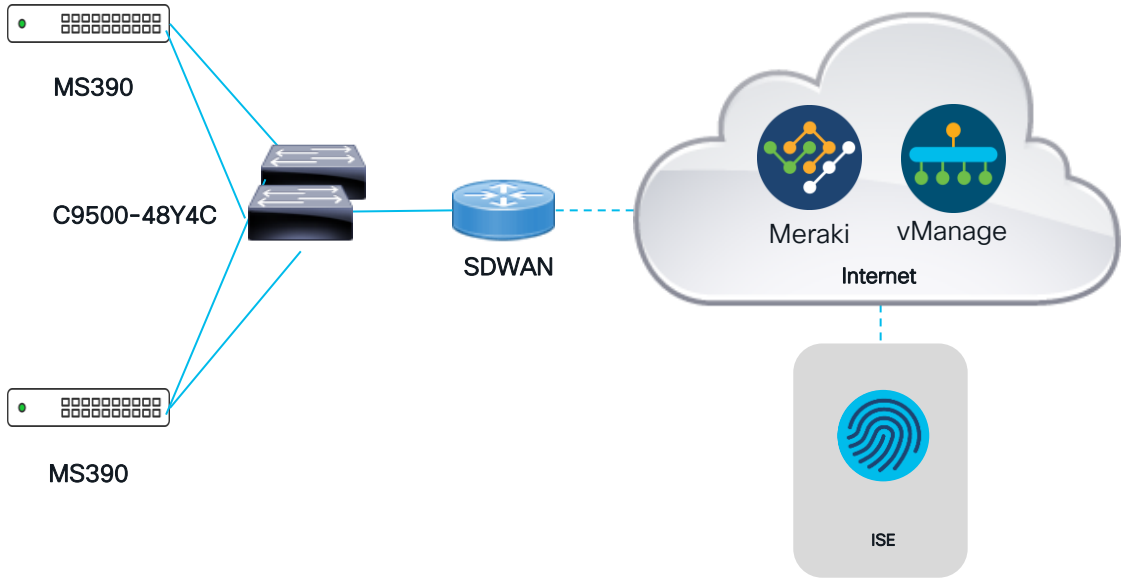
Catalyst 9500 LAN Routing and Switching Core

Catalyst 9500-48Y4C
- Stackwise Virtual

Layer 2
- VLAN Segmentation
- SGT Propagation

Layer 3
- IP Segmentation
- Local Routing
- WAN Routing

Security Policy
- TrustSec



Meraki LAN Access

- MR56 Wireless Access
- MS390 Wired Access

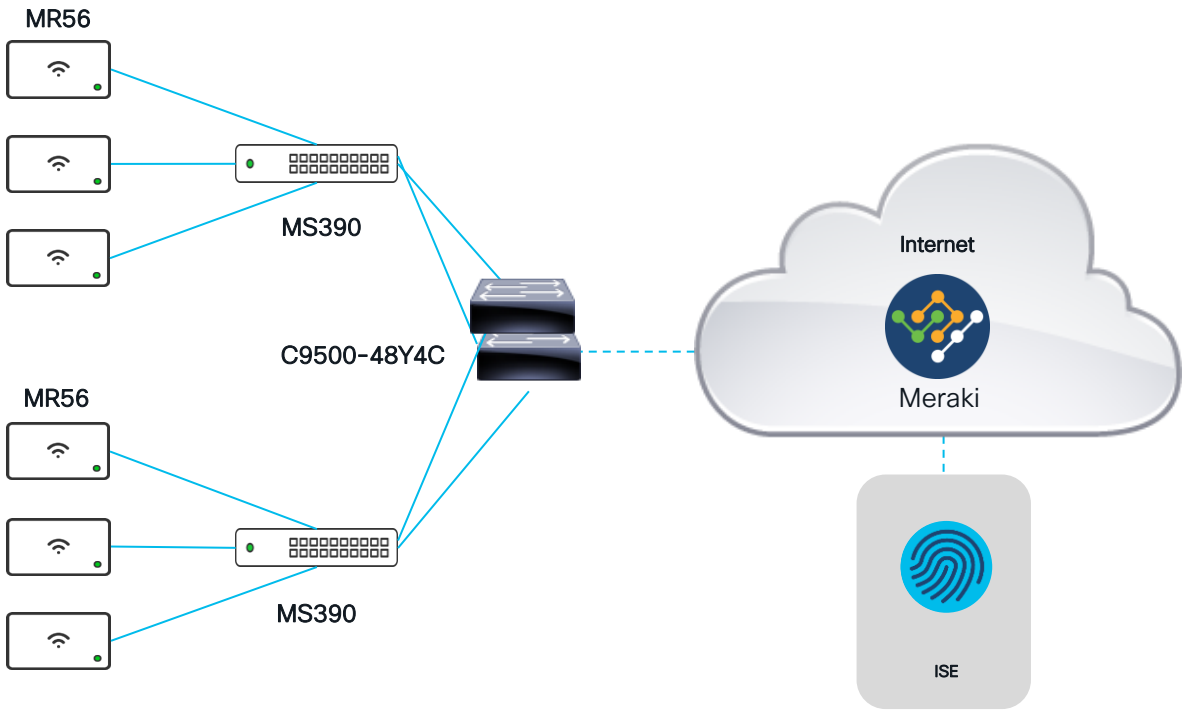
- Security Policy

Statically assigned to a switch port

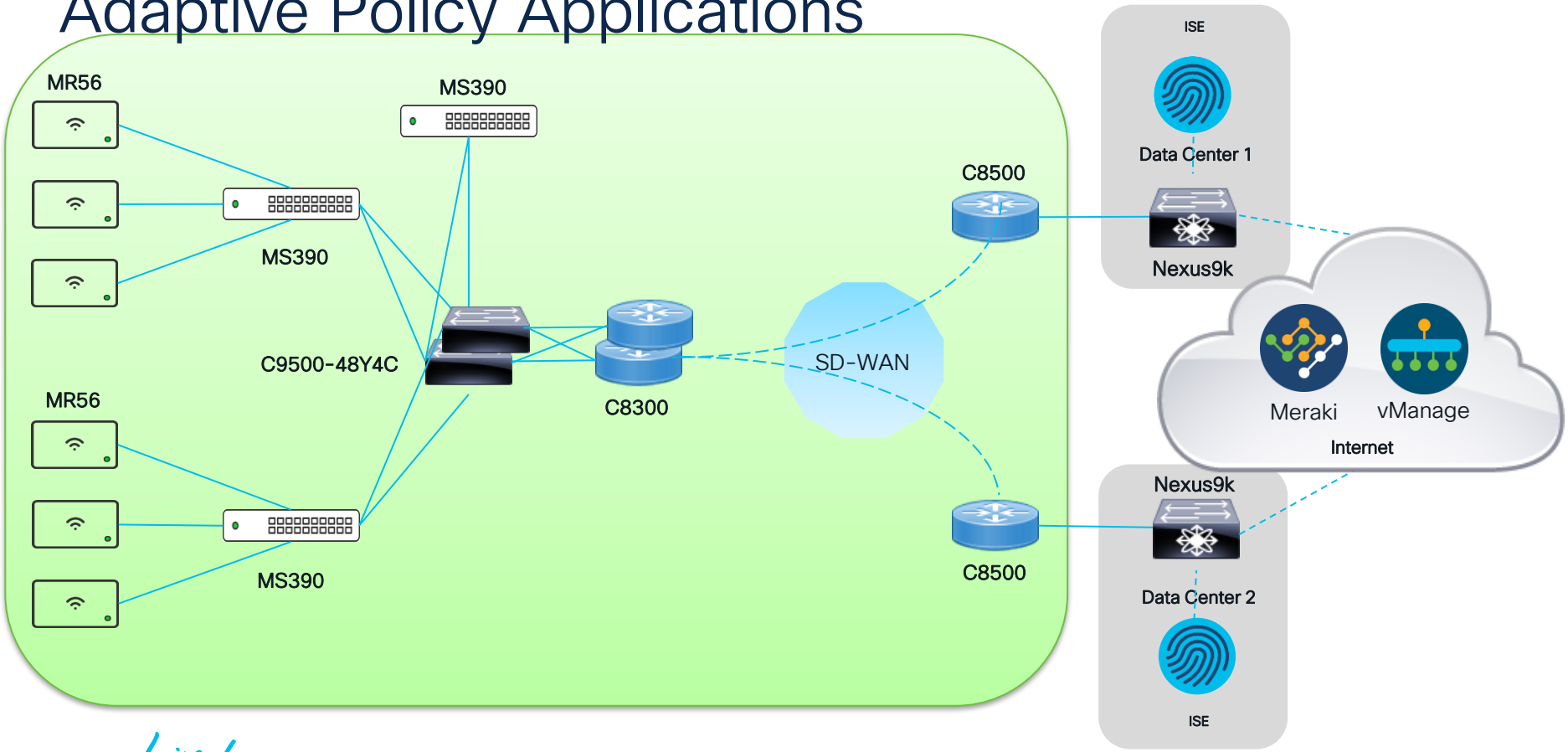
Static assignment per SSID

Dynamic assignment via RADIUS
Wired & Wireless 802.1x

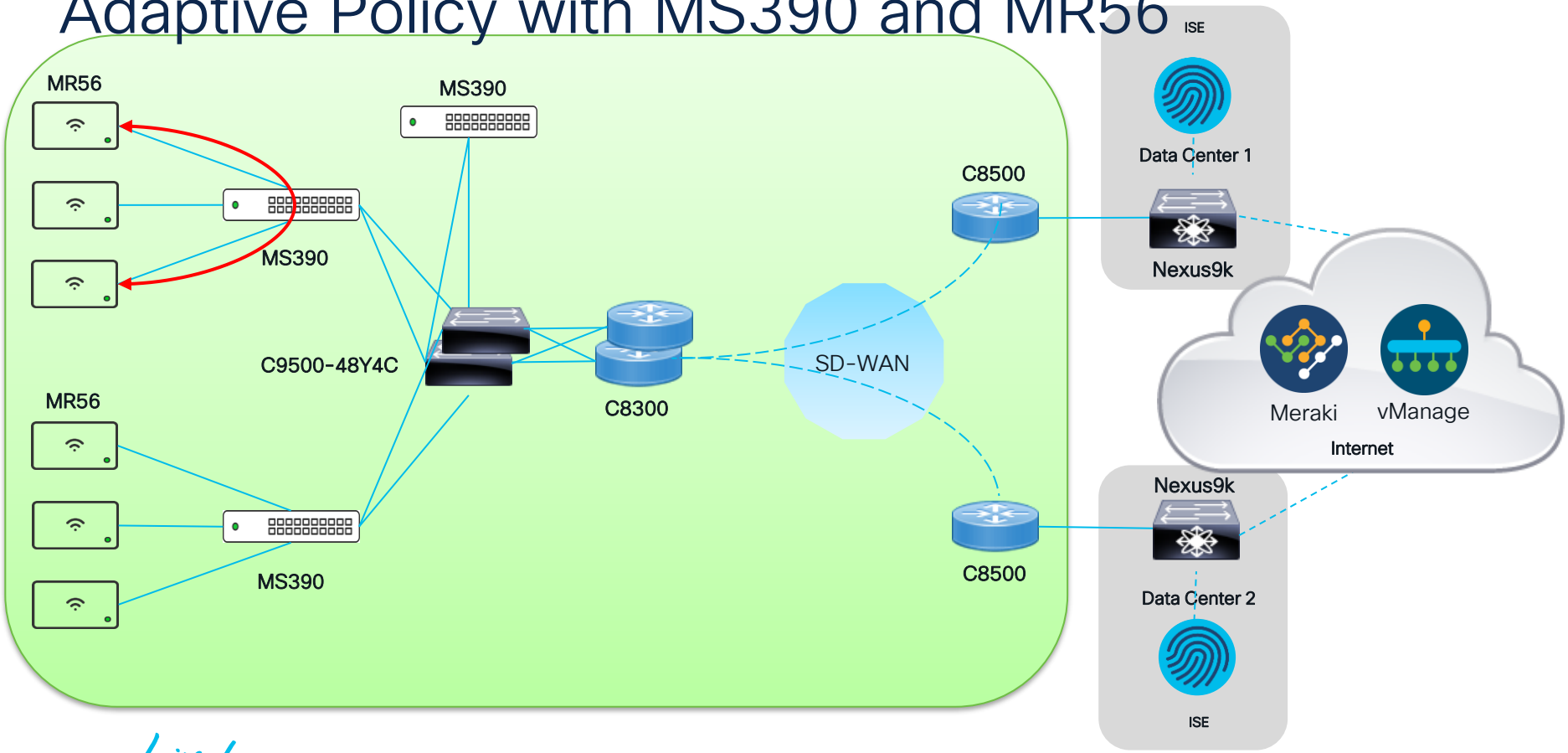
Static IP to SGT Mapping
Uses network objects



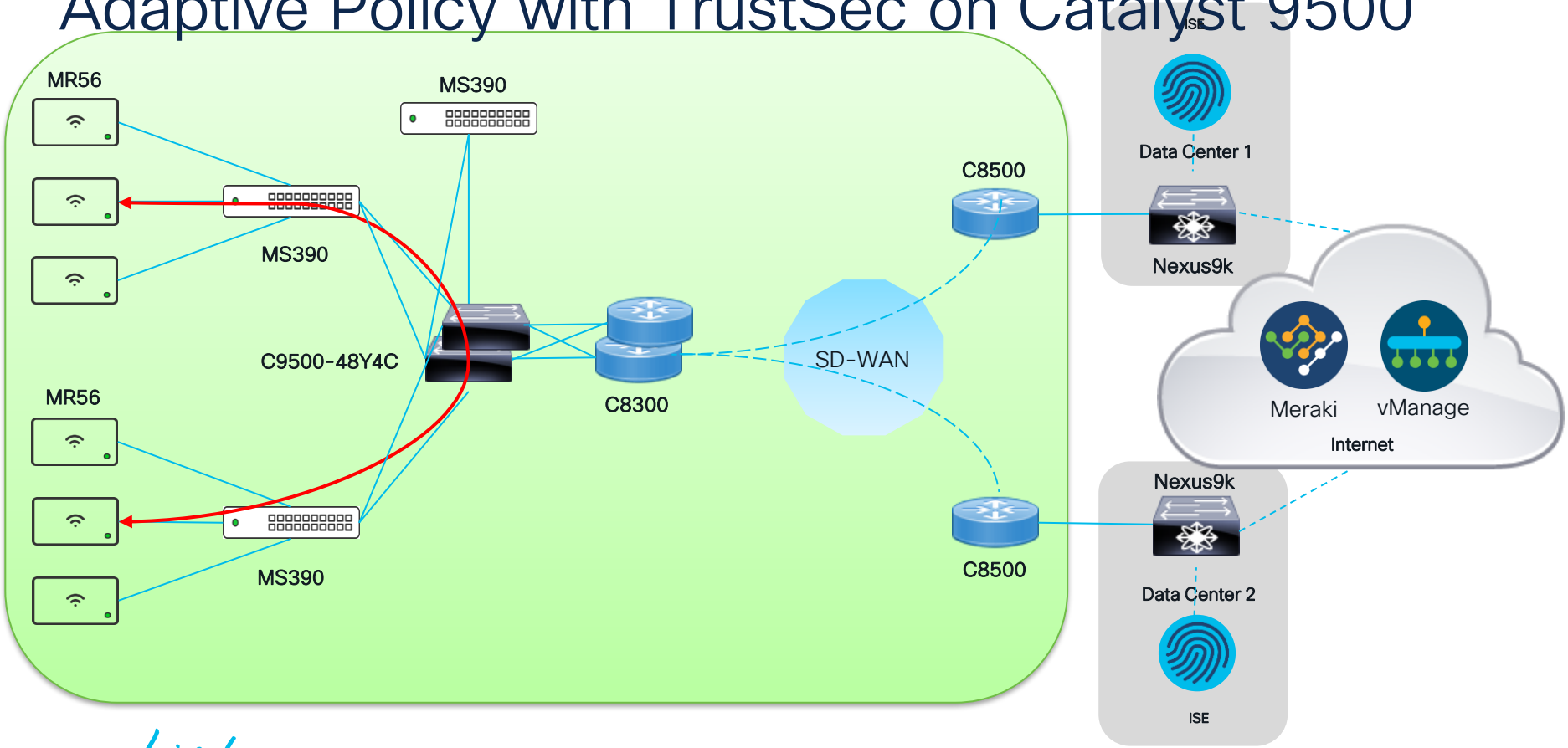
Adaptive Policy Applications



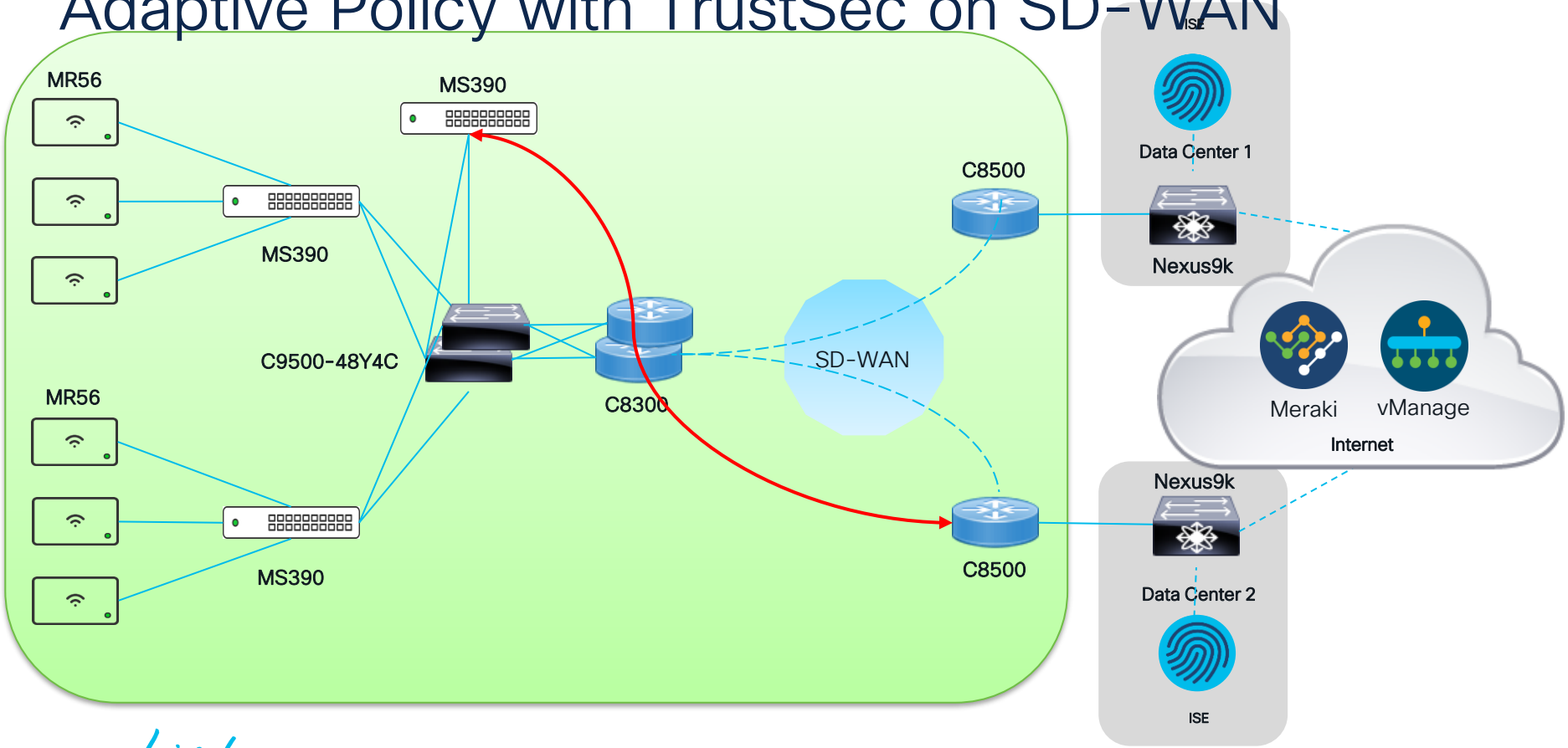
Adaptive Policy with MS390 and MR56



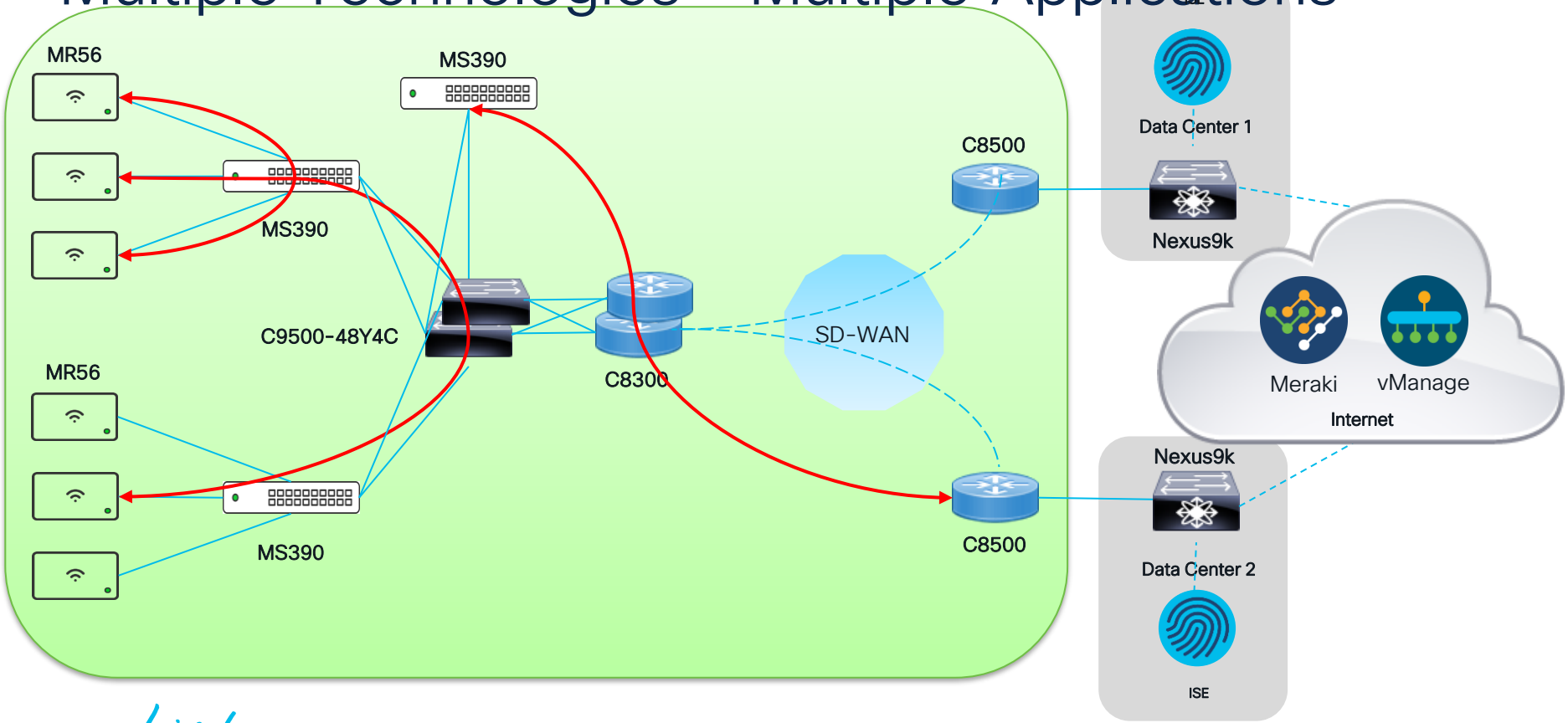
Adaptive Policy with TrustSec on Catalyst 9500



Adaptive Policy with TrustSec on SD-WAN



Multiple Technologies--Multiple Applications

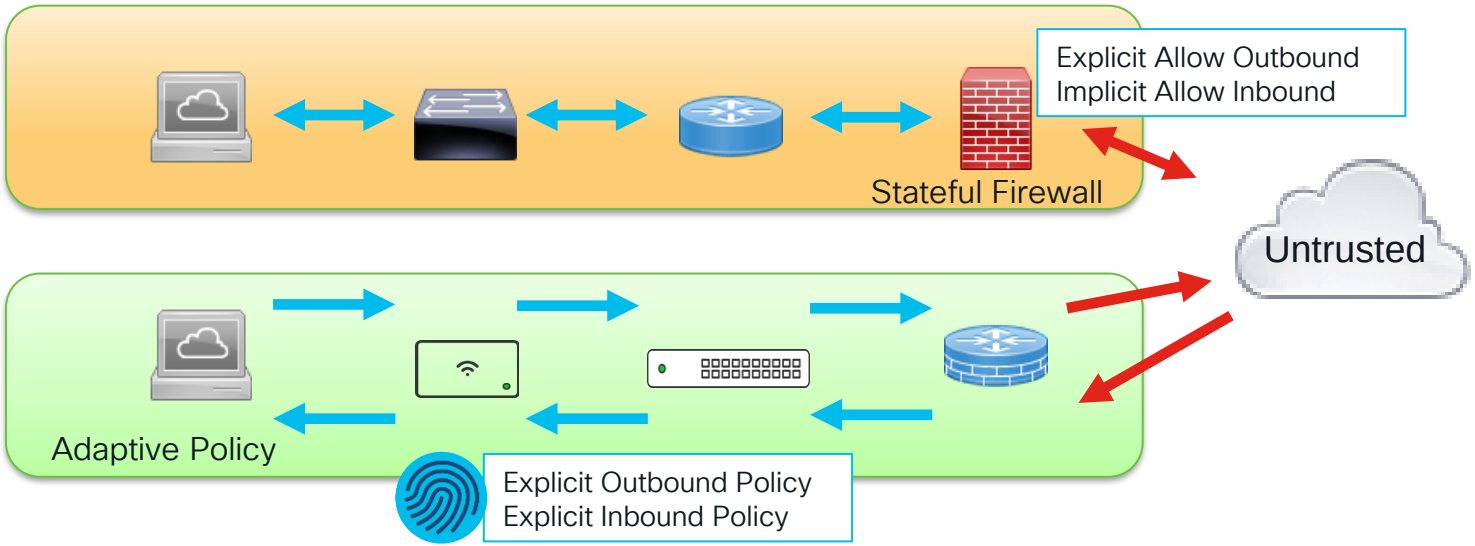


Design Considerations and Best Practices

Security Policy Design Considerations

Stateful Firewall: Stateful security model with point policy

Adaptive Policy: Stateless security model with central policy



Best Practices for Scalability

- Security Policy is a Matrix
- Policies increase exponentially
- Use the minimum SGTs required to achieve goals

Forward Policy

Reverse Policy

SGT	10	20	30	40	50	60	70
10	✓	✗	✓	✓	✓	✓	✓
20	✗	✓	✗	✗	✗	✗	✗
30	✓	✗	✓	✓	✓	✓	✓
40	✓	✗	✓	✗	✓	✓	✓
50	✓	✗	✓	✓	✓	✓	✓
60	✓	✗	✓	✓	✓	✓	✓
70	✓	✗	✓	✓	✓	✓	✓

Conclusion

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

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

The bridge to possible

Thank you

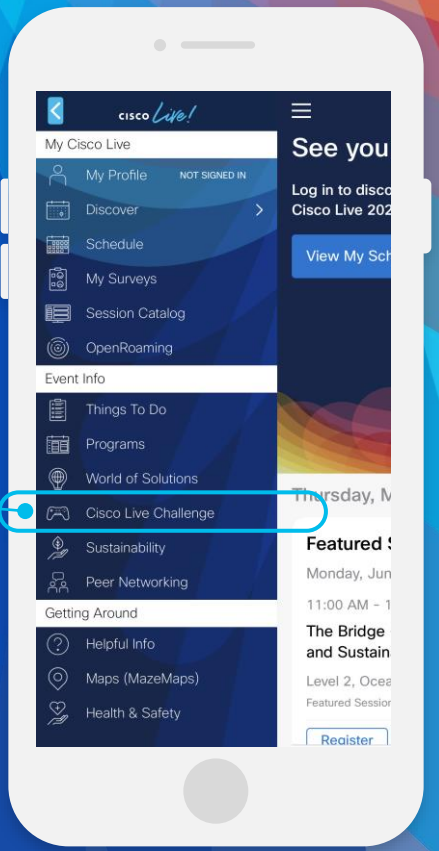
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:




cisco Live!
Let's go
#CiscoLive