You make **possible**

Infrastructure as Code – 2002

Hardening Your Meraki Network with Code (and APIs)

Shiyue (Shay) Cheng, Solutions Architect @ Cisco Meraki

DEVNET-2434

Barcelona | January 27-31, 2020

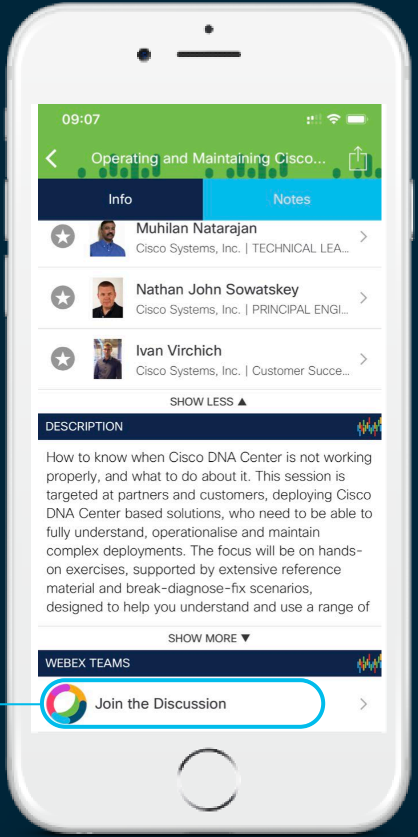
Cisco Webex Teams

Questions?

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

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



09:07

Operating and Maintaining Cisco...

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

WEBEX TEAMS

cisco Live!

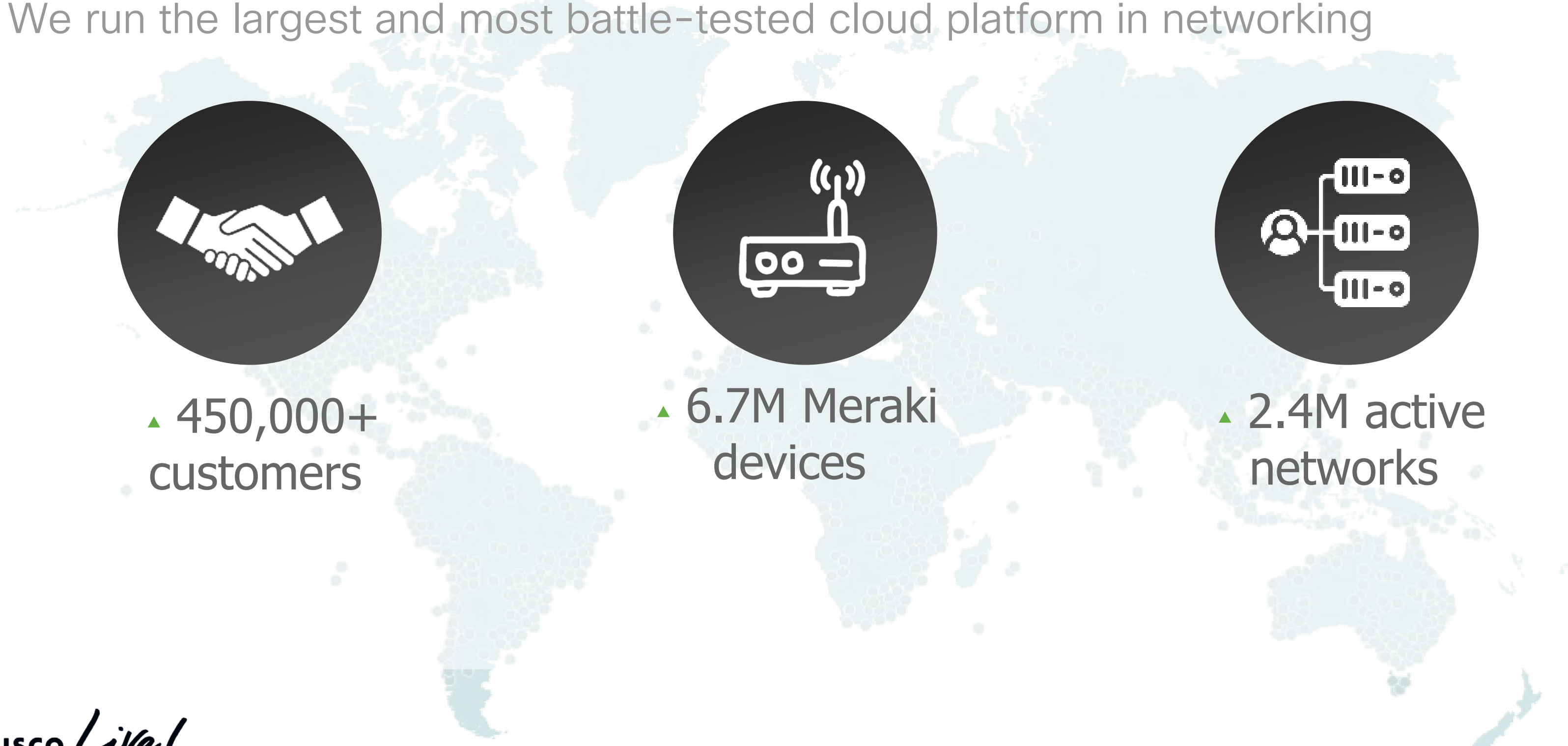
Agenda

- Meraki Security API Overview
- VLAN Management
- Content Filtering
- Firewalls
  - Firewalled Services
  - MX L7 Firewall Rules
  - MX L3 Firewall Rules
  - MR L3 Firewall Rules
- Group Policy
- Switchport Management
- Webhook Alerts & Demo
- Action Batches & Demo

The Meraki Platform

Meraki Cloud Platform

- We run the largest and most battle-tested cloud platform in networking

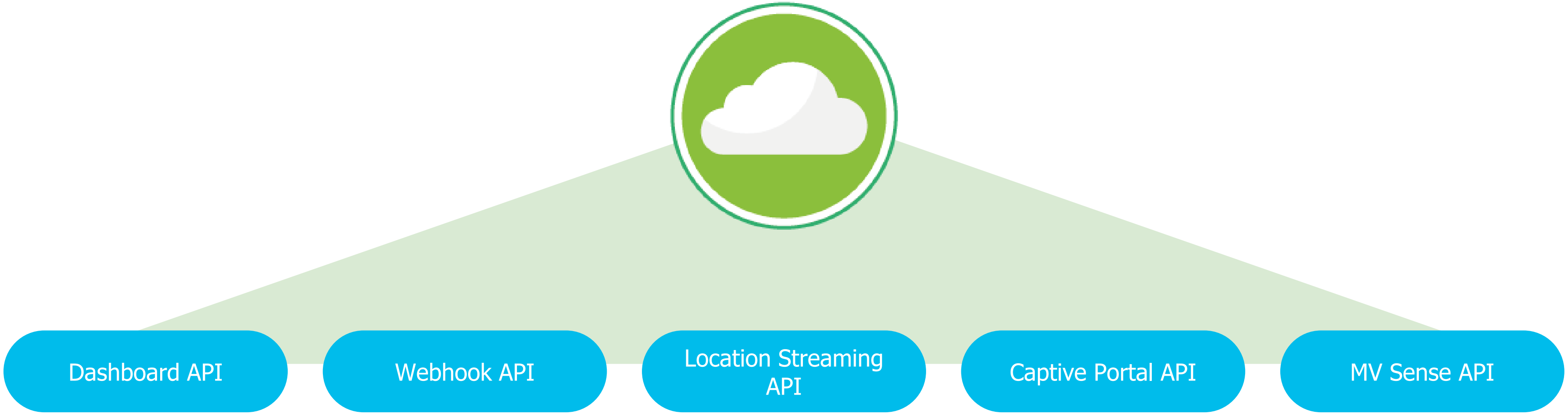


▲ 450,000+ customers

▲ 6.7M Meraki devices

▲ 2.4M active networks

Meraki API Services



Dashboard API

- Programmability
- Automation
- Monitoring
- Reporting
- Data Insights

Webhook API

- Event stream
- Automation trigger

Location Streaming API

- Wayfinding
- Asset tracking
- Location & footfall analytics

Captive Portal API

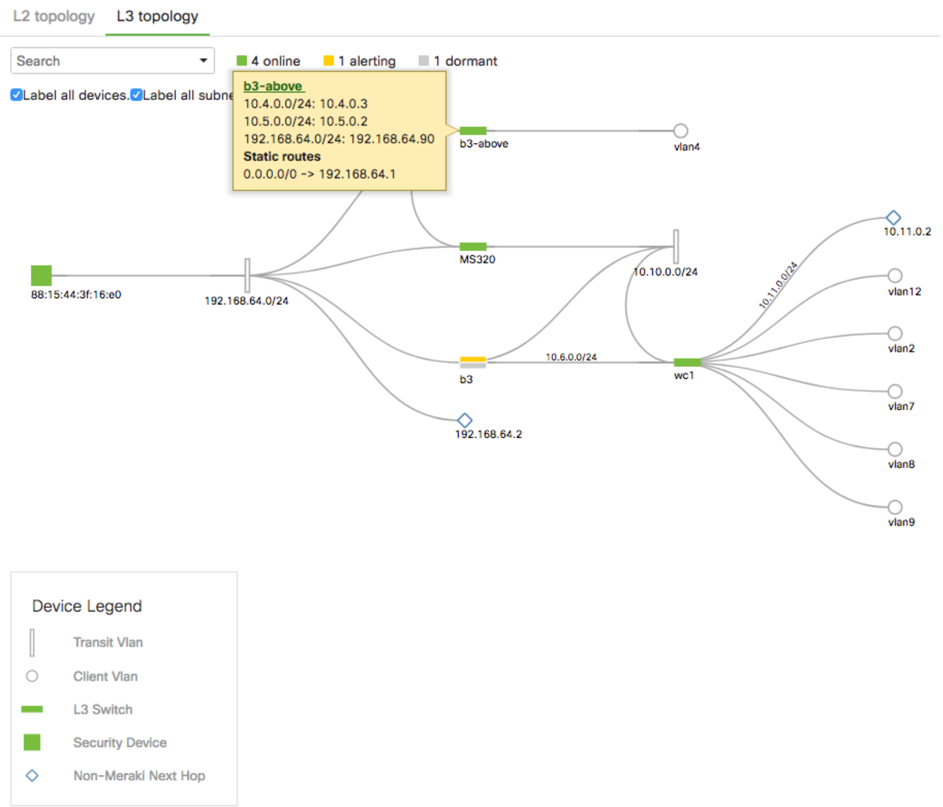
- Guest Wi-Fi experiences
- Secure Onboarding

MV Sense API

- Real-time (4Hz) data stream
- Historical time-series via REST
- Current snapshot

VLANS – **POST** /networks/{networkId}/vlans

- Traffic Shaping
- Network Segmentation
- Client Isolation
- DMZs



L2 topology | L3 topology

Search

🟩 4 online 🟨 1 alerting ▨ 1 dormant

☑ Label all devices. ☑ Label all subne

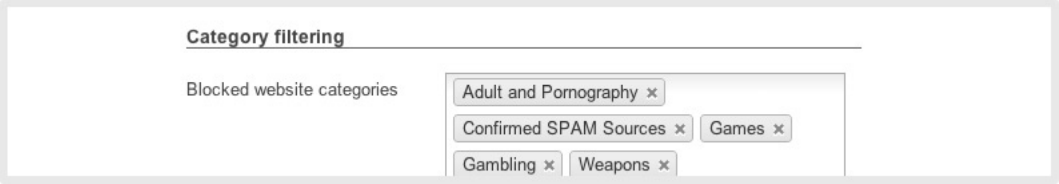
b3-above
10.4.0.0/24: 10.4.0.3
10.5.0.0/24: 10.5.0.2
192.168.64.0/24: 192.168.64.90
Static routes
0.0.0.0/0 -> 192.168.64.1

Device Legend

▯	Transit Vlan
○	Client Vlan
▬	L3 Switch
🟩	Security Device
◇	Non-Meraki Next Hop

Content Filtering - **PUT** /networks/**{networkId}**/contentFiltering

- Blocked website categories
- URL category list size
- Web search filtering
- Block encrypted search
- Restricted YouTube content
- Blocked URL patterns
- Whitelisted URL patterns

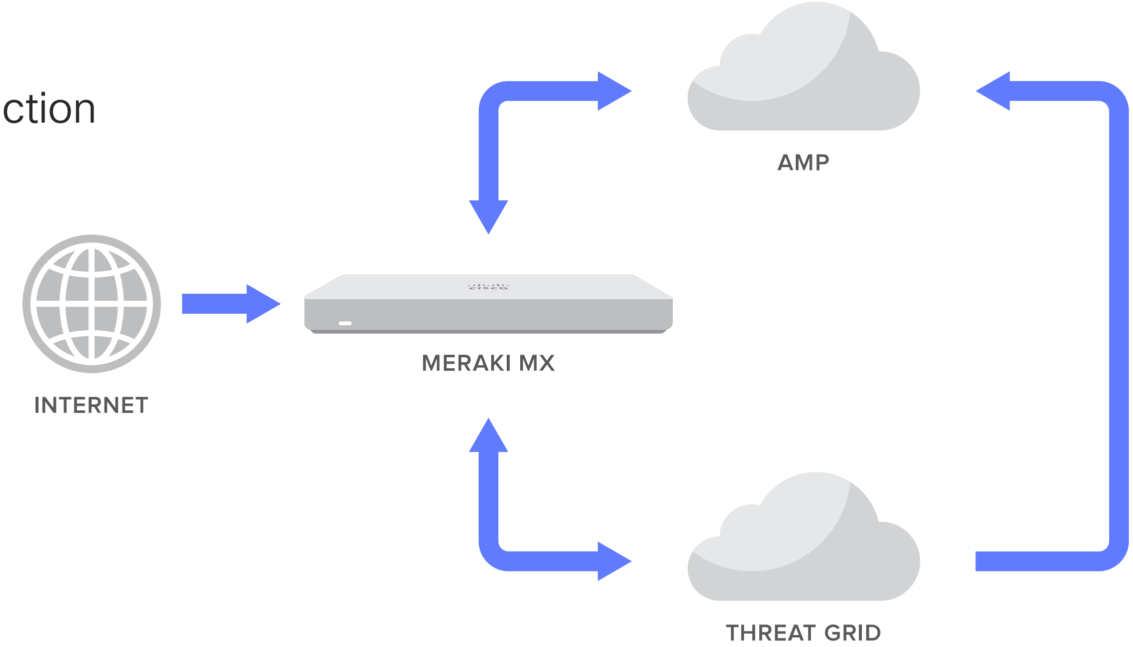


Category filtering

Blocked website categories: Adult and Pornography ×, Confirmed SPAM Sources ×, Games ×, Gambling ×, Weapons ×

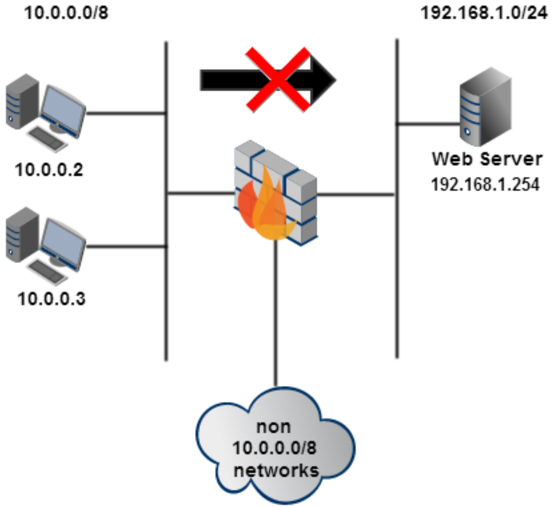
Network Malware Settings - **PUT** /networks/{networkId}/security/malwareSettings

- Real-time Malware blocking
- Retrospective Malware Detection
- Threat Grid



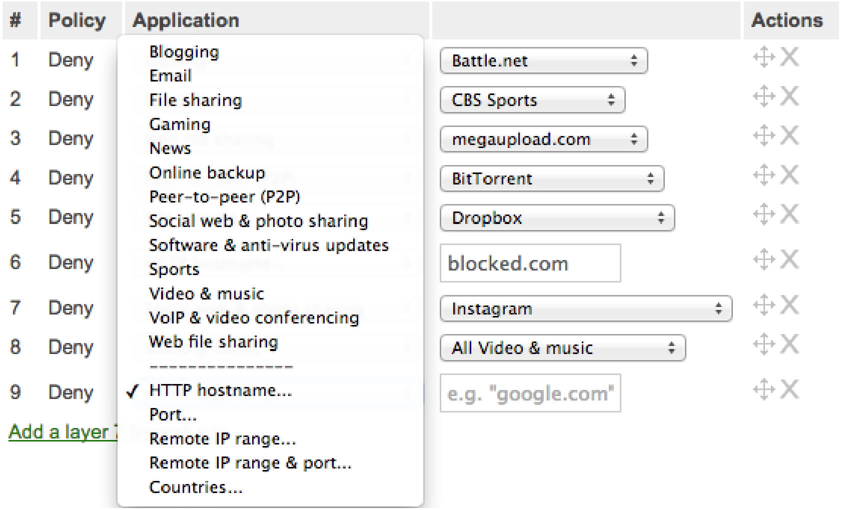
Firewalled Services - **PUT**
/networks/**{networkId}**/firewalledServices/**{service}**

- ICMP Ping: reply to inbound ICMP ping requests coming from the specified address(es). Web (local status & configuration): Use this setting to allov or disable access to the local management page SNMP: Use this setting to allow SNMP polling of the appliance from the WAN. Supported values for the remote IPs field are the same as for ICMP Ping.



MX L7 Firewall Rules - **PUT** /networks/**{networkId}**/l7FirewallRules

- Block specific web-based services,
  - Websites or types of websites
  - No specific IP address or port ranges
- Block by Category

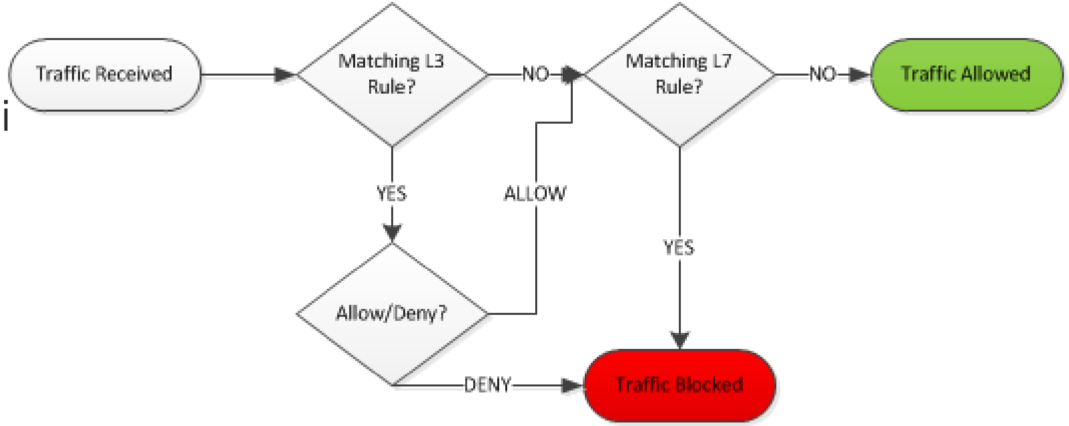


#	Policy	Application		Actions
1	Deny		Battle.net	✥ ✕
2	Deny		CBS Sports	✥ ✕
3	Deny		megaupload.com	✥ ✕
4	Deny		BitTorrent	✥ ✕
5	Deny		Dropbox	✥ ✕
6	Deny		blocked.com	✥ ✕
7	Deny		Instagram	✥ ✕
8	Deny		All Video & music	✥ ✕
9	Deny	✓ HTTP hostname...	e.g. "google.com"	✥ ✕

Add a layer 7

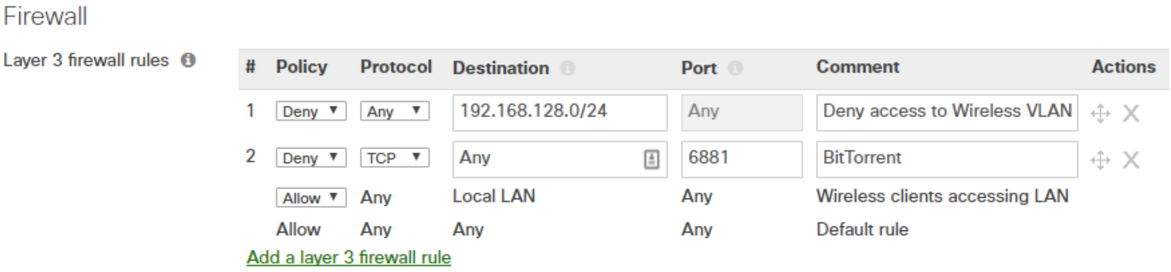
MX L3 Firewall Rules - **PUT** /networks/**{networkId}**/l3FirewallRules

- Evaluated for every request
- Top to Bottom
- First rule that matches is appli
- Default if no match



MR L3 Firewall Rules - **PUT**
/networks/**{networkId}**/ssids/**{number}**/l3FirewallRules

- Evaluated for every request
- Top to Bottom
- First rule that matches is ap
- Default if no match



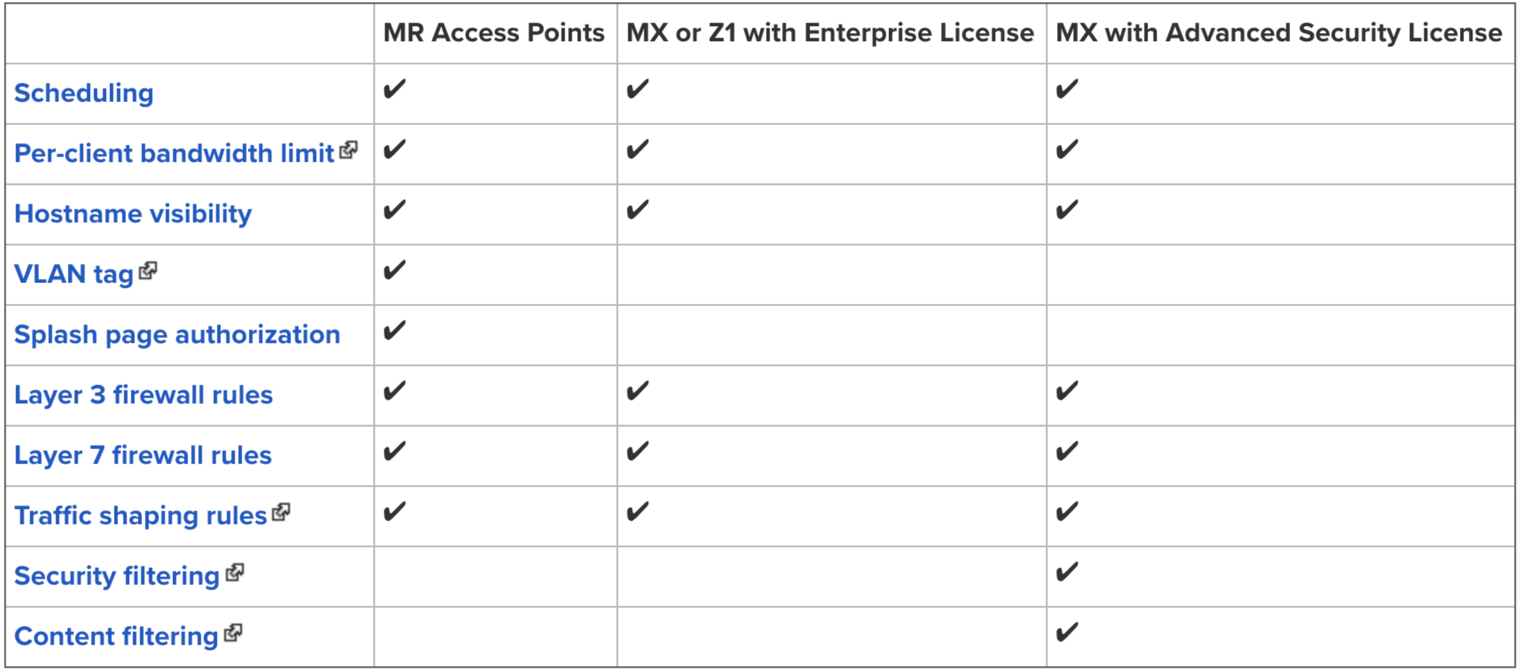
Firewall

Layer 3 firewall rules

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny ▼	Any ▼	192.168.128.0/24	Any	Deny access to Wireless VLAN	✥ ✕
2	Deny ▼	TCP ▼	Any	6881	BitTorrent	✥ ✕
	Allow ▼	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

Add a layer 3 firewall rule

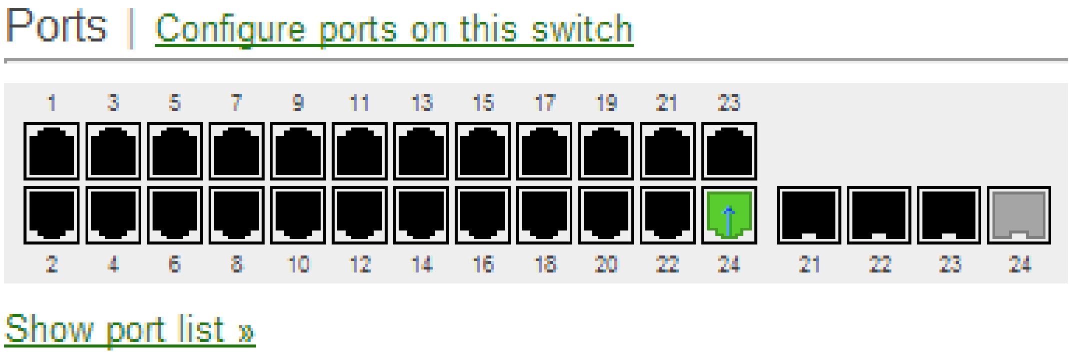
Group Policies - **POST** /networks/**{networkId}**/groupPolicies



	MR Access Points	MX or Z1 with Enterprise License	MX with Advanced Security License
Scheduling	✔	✔	✔
Per-client bandwidth limit	✔	✔	✔
Hostname visibility	✔	✔	✔
VLAN tag	✔		
Splash page authorization	✔		
Layer 3 firewall rules	✔	✔	✔
Layer 7 firewall rules	✔	✔	✔
Traffic shaping rules	✔	✔	✔
Security filtering			✔
Content filtering			✔

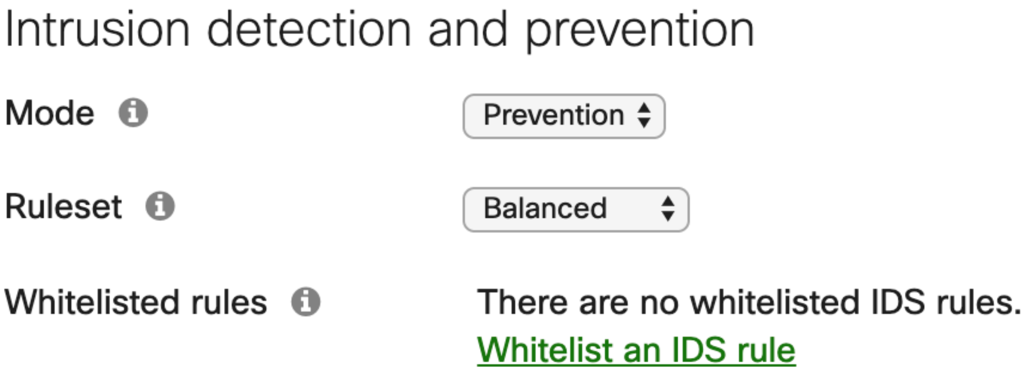
Switchport Management - **PUT** /devices/**{serial}**/switchPorts/**{number}**

- Enable/Disable
- Isolation
- VLAN management



Intrusion Protection - **PUT** /networks/**{networkId}**/security/intrusionSettings

- Connectivity
- Balanced
  - Malware-CNC
  - Blacklist
  - SQL Injection
  - Exploit-kit
- Security:
  - Malware-CNC
  - Blacklist
  - SQL Injection
  - Exploit-kit
  - App Detect



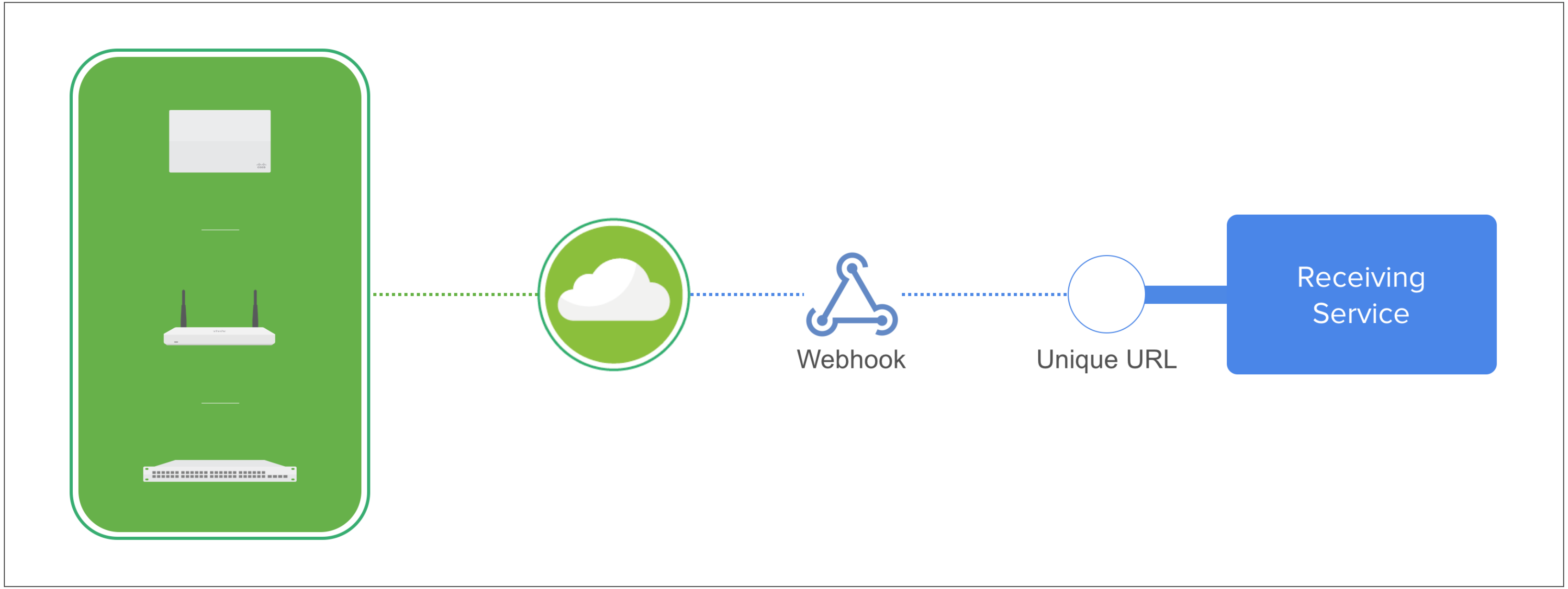
Intrusion detection and prevention

Mode: Prevention

Ruleset: Balanced

Whitelisted rules: There are no whitelisted IDS rules. Whitelist an IDS rule

Webhook Alerts



Action Batches

Submit batch configuration changes

High efficiency (1 request vs 100)

Support for synchronous and asynchronous actions

Supported resources include

Devices

Switch ports

VLANs

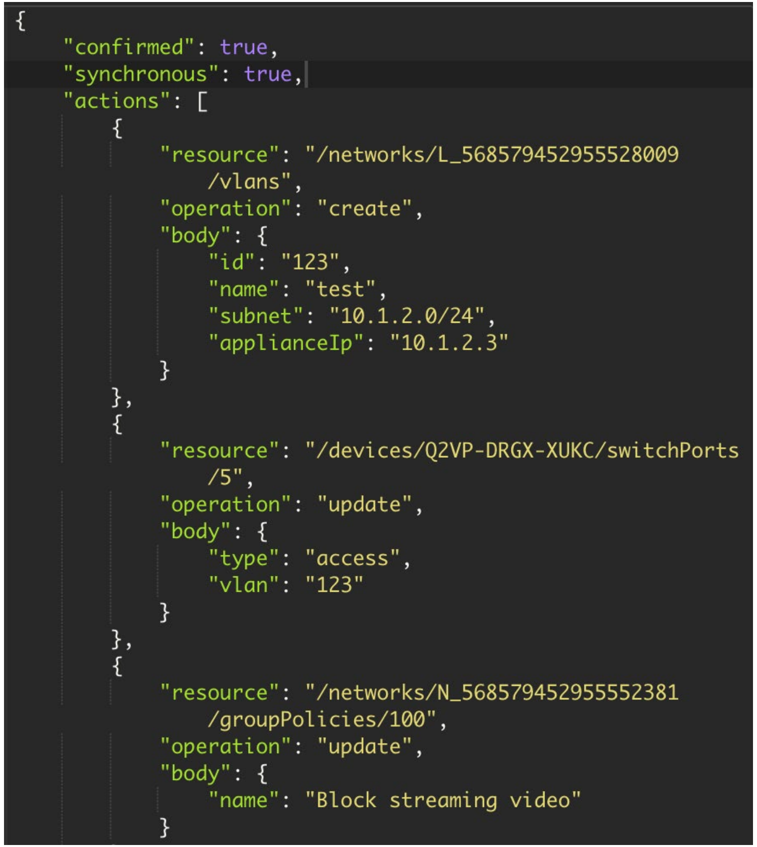
RF profiles

Traffic shaping

Group policies

Networks

SSIDs & more



```
{
    "confirmed": true,
    "synchronous": true,
    "actions": [
        {
            "resource": "/networks/L_568579452955528009
                /vlans",
            "operation": "create",
            "body": {
                "id": "123",
                "name": "test",
                "subnet": "10.1.2.0/24",
                "applianceIp": "10.1.2.3"
            }
        },
        {
            "resource": "/devices/Q2VP-DRGX-XUKC/switchPorts
                /5",
            "operation": "update",
            "body": {
                "type": "access",
                "vlan": "123"
            }
        },
        {
            "resource": "/networks/N_568579452955552381
                /groupPolicies/100",
            "operation": "update",
            "body": {
                "name": "Block streaming video"
            }
```

Demo

Learn more about the new DevNet Certifications and how you can prepare now!

	Associate Level	Specialist Level	Professional Level	Expert Level
Engineering	CISCO CERTIFIED CCNA	CISCO CERTIFIED SPECIALIST	CISCO CERTIFIED CCNP	CISCO CERTIFIED CCIE
Software	CISCO CERTIFIED DEVNET Associate	CISCO CERTIFIED DEVNET SPECIALIST	CISCO CERTIFIED DEVNET Professional	CISCO CERTIFIED DEVNET Expert Future Offering

Start Here | Upcoming Cisco DevNet Certifications

Start at **Meet DevNet**

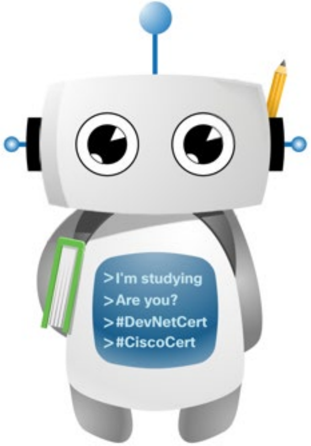
DEVNET-2864: Getting ready for Cisco DevNet Certifications
Offered daily at 9am, 1pm & 4pm at Meet DevNet

Attend a **brownbag session**

DEVNET-4099: DevNet Certifications: Bringing software practices & software skills to networking
Offered daily 12:15-12:45 in the DevNet Zone Theater

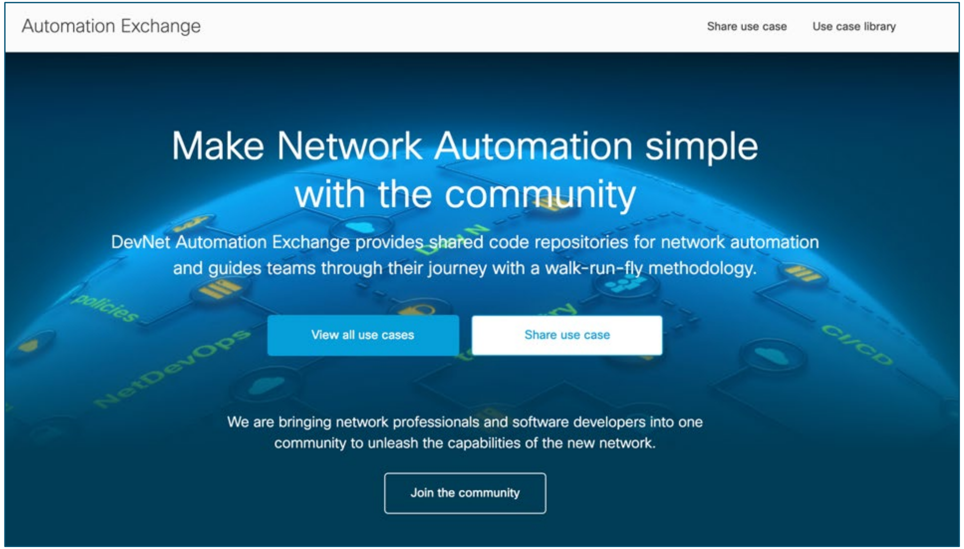
Visit the **Learning@Cisco** booth

Scan this code to **sign up** for the latest updates or go to http://cs.co/20eur02



Find shared code repositories of use cases for network automation & more

Don't miss our 5 Automate Infrastructure demos in the DevNet Zone!



Automation Exchange

Make Network Automation simple with the community

DevNet Automation Exchange provides shared code repositories for network automation and guides teams through their journey with a walk-run-fly methodology.

We are bringing network professionals and software developers into one community to unleash the capabilities of the new network.

Scan this code or go to the URL to **learn more**

http://cs.co/20eur01

Start at **Meet DevNet**

DEVNET-3010 [a-j] Learn how to make Network Automation Simple with the Community

Offered Monday 2pm & 5pm, Tuesday & Wednesday 10am, 2pm & 5pm, and Thursday 10am & 5pm at Meet DevNet

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

Demos in the
Cisco Showcase

Walk-In Labs

Meet the Engineer
1:1 meetings

Related sessions

Thank you

You make **possible**