

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

# Cisco Meraki SD-WAN

Powerful Networking, Made Easy

Steve Harrison, Director Technical Marketing  
BRKMER-2215

CISCO *Live!*

#CiscoLiveAPJC

# Cisco Webex App

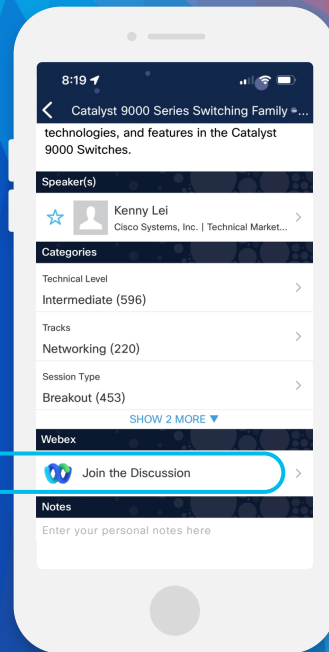
## Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKMER-2215>

# Agenda

- Background
- AutoVPN
- SD-WAN & SD-Internet
- Scaling
- What else?
- Conclusion

# Introduction



Steve Harrison  
Director  
Technical Marketing

- Runs technical PM for SD-WAN & Cellular GW
  - Don't actually do 'marketing'
    - 20+ years' experience
- Specialised in Meraki SD-WAN for 8 years
  - Retired basketball player
  - Gaming nerd

# Background

# Inception & History

It was 2015...



- The industry was a wash with SDN
- SD-WAN had only just been coined as a term
- Cisco published the 200+ page IWAN CVD
- Todd Nightingale has recently become Meraki GM
- Meraki started the 'Meraki IWAN' project
- First/pilot customer for Meraki IWAN was DaVita\*
- Deal closed in early 2016
- Was one of the first 8 figure Meraki deals
- Meraki were not allowed to use PfR terminology
- Solution was L3/4 only

# Fast Forward to Today

NORDSTROM

Ladbrokes



vitalant.



LC Waikiki

Walgreens Boots Alliance



World Acceptance Corporation

L'ORÉAL



ROSSMANN



metro



CISCO Live!

# AutoVPN

# AutoVPN Specification & Operation

## Specification

- Tunnel derived through the use of dashboard 'service' VPN Registry
- Secret used to derive authentication and encryption keys of all VPN tunnels via IKE & DH process
- Both the encryption and authentication keys are re-derived based on either the packet-based lifetime or time-based lifetime expiring

|                       |                |
|-----------------------|----------------|
| Authentication (HMAC) | SHA-256, SHA-1 |
| Encryption            | AES-128-CTR    |
| Diffie-Hellman        | 15 (modp3072)  |

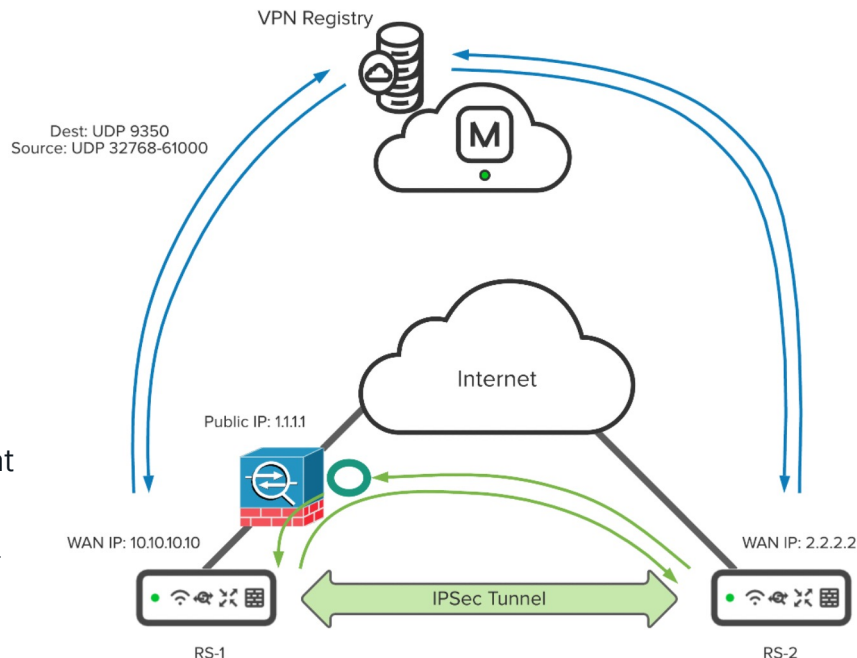
## Operation

- Hubs build tunnels to all other hubs and spokes who have them configured as hubs
- Spokes build tunnels to hubs that they have configured
- All MXs in an AutoVPN domain 'learn' about all routes tagged into the AutoVPN from dashboard
- \*Unless additional controls are applied
  - No hub-to-hub removes hub based routes
  - No spoke-to-spoke removes spoke based routes

# VPN Registry Example

| Device | WAN IP / Port   | Received IP / Port |
|--------|-----------------|--------------------|
| RS-1   | 1.1.1.1 / 35000 | 1.1.1.1 / 35000    |
| RS-2   | 2.2.2.2 / 40000 | 2.2.2.2 / 40000    |

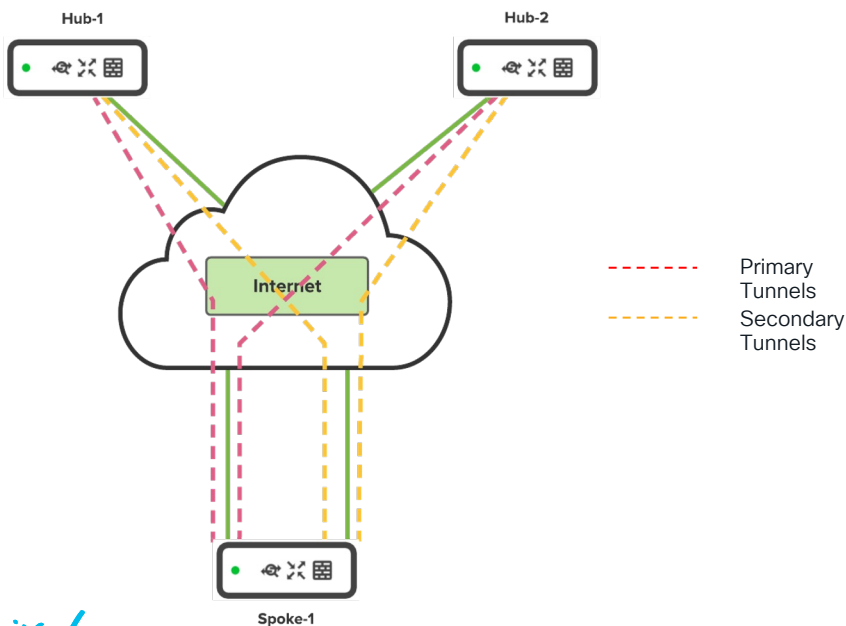
- RS-1 punches to VPN Registry
  - RS-2 learns how to reach RS-1
- RS-2 punches to VPN Registry
  - RS-1 learns how to reach RS-2
- RS-2 attempts to connect to RS-1, connection drop at edge firewall
- RS-1 attempts to connect to RS-2, creating new NAT entry for path to RS-2
- RS-1 & RS-2 establish bidirectional session



# Active-Active AutoVPN

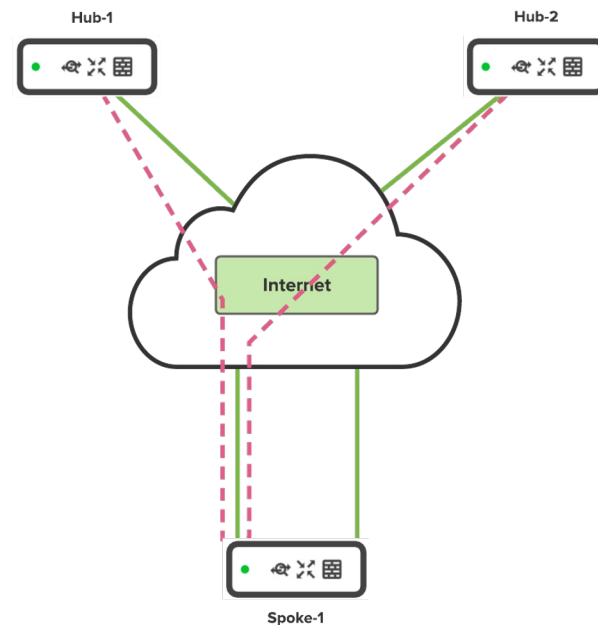
Active-Active AutoVPN

- ☒ Enabled  
Create VPN tunnels over all of the available uplinks (primary and secondary).
- ☐ Disabled  
Do not create VPN tunnels over the secondary uplink unless the primary uplink fails.

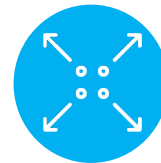


Active-Active AutoVPN

- ☒ Enabled  
Create VPN tunnels over all of the available uplinks (primary and secondary).
- ☐ Disabled  
Do not create VPN tunnels over the secondary uplink unless the primary uplink fails.



# Topologies



## Hub & Spoke

## Full Mesh

## Geo Hub & Spoke

## Hierarchical H&S

- Hubs are typically VPN concentrators
- Includes inline hub operation
- Scalable
- Requires large number of numbers for massive customers

- All devices are hubs
- Hubs can be routed or concentrator
- Exit hubs are possible
- Least scalable

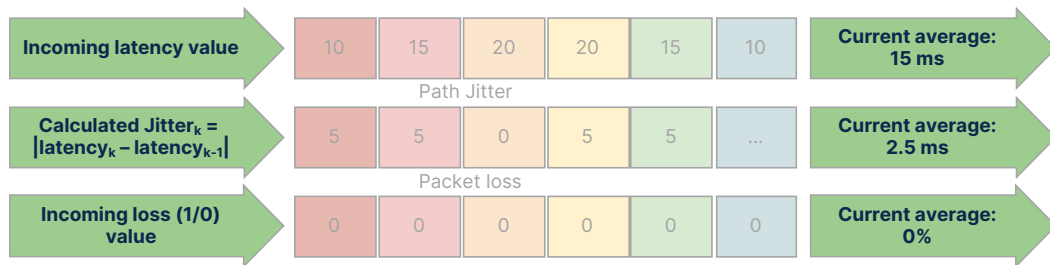
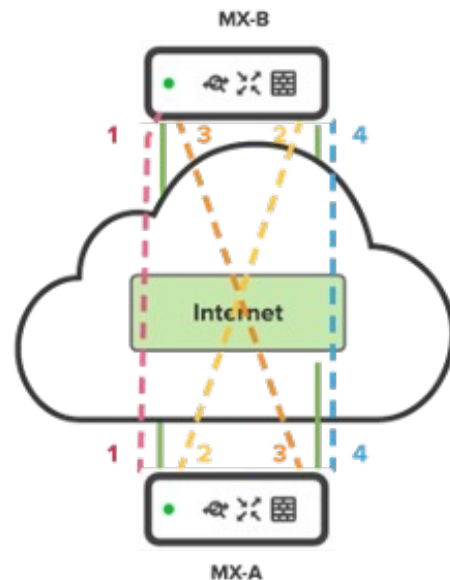
- Builds on H&S
- Includes geo and trans-geo hubs
- Regional routing
- Most scalable
- Used in largest customers

- Breaks hub full mesh
- Creates hierarchical traffic flow
- Prevents spoke to spoke comms via AutoVPN
- Used in segmentation use cases

# SD-WAN

# Measuring Performance (Probing)

- Probes are sent over all available transport paths
- MX-A W1 -> MX-B W1, MX-A W1 -> MX-B W2, MX-A W2 -> MX-B W1, MX-A W2 -> MX-B W2
- Probes are unidirectional, MX-A measures all paths to MX-B and MX-B does the same
- Probing interval is 1 second or 10 seconds by default
- 1 sec for under 2500 AutoVPN nodes, 10 sec for over 2500 AutoVPN nodes
- at least 1 probe per interval
- Latency is intentionally added to probes, to ensure non-uniformity



# Probe Packet Format

- Probes use UDP for transport
- Matches AutoVPN transport for more accurate path sampling
- Probe data is <100 bytes, typically 87 bytes of data plus standard 8-byte UDP header
- MXs are synchronised with shard NTP source
- Data payload is a timestamp
- Latency variable is known on both sides (can be disabled)
- Differences are used to calculate performance

```
> Frame 97: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits)
> Ethernet II, Src: CiscoMer_3c:d4:50 (a8:46:9d:3c:d4:50), Dst: AVMAudio_21:a3:24 (74:42:7f:21:a3:24)
> PPP-over-Ethernet Session
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 217.155.75.120, Dst: 155.190.33.17
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 115
  Identification: 0x38aa (14506)
> Flags: 0x00
  Fragment Offset: 0
  Time to Live: 250
  Protocol: UDP (17)
  Header Checksum: 0xa5ec [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 217.155.75.120
  Destination Address: 155.190.33.17
> User Datagram Protocol, Src Port: 60105, Dst Port: 38598
  Source Port: 60105
  Destination Port: 38598
  Length: 95
  Checksum: 0x3070 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 2]
> [Timestamps]
  UDP payload (87 bytes)
> Data (87 bytes)
  Data: 100186a73802324f0a203036376339306466666239353837373232316134653364336632666365663834300112203235613665303233636566383239646136633061636564316262616462633334380018c3c8b4fc9028
  [Length: 87]
```

## Probe Data - very small delta

```
100186a73802324f0a203036376339306466666239353837373232316134653364336632666365663834300112203235613665303233636566383239646136633061636564316262616462633334380018c3c8b4fc9028
100186a73802324f0a203036376339306466666239353837373232316134653364336632666365663834300112203235613665303233636566383239646136633061636564316262616462633334380018c5bacbfcc9028
```

# Performance Calculations

- Timestamp from return packets are used to calculate the round-trip time (RTT)
- Average RTT divided by 2 is the latency
- Variation in RTT (divided by 2) is the jitter
- Any lost probes are used to calculate the loss
- Latency, jitter and loss yield an R value which we then convert to MOS

$$MOS = \frac{\sum_{n=1}^N R_n}{N}$$



## 1 second probing

- Latency, Jitter, Loss & MOS are the average of the last 30 seconds of data, i.e., at least 30 probes



## 10 second probing

- Latency, Jitter, Loss & MOS are the average of the last 30 seconds of data, i.e., at least 3 probes

# Policies – Performance Classes (built in)

VPN traffic

There are no uplink preferences for VPN traffic  
[Add a preference](#)

Custom performance classes

[Create a new custom performance class...](#)

## Traffic filters

All VoIP & video conferencing ✕ Add +

## Policy

Preferred uplink: WAN 1 ⌵

Fail over if: Poor performance ⌵

Performance class: VoIP ⌵

## Traffic filters

All VoIP & video conferencing ✕ Add +

## Policy

Preferred uplink: Best for VoIP ⌵

## Default (60% Loss)

- Also known as connection monitor failover
- If loss >60% we will failover to an alternative transport network
- If alternative is also >60% we do not failover

## VoIP (3.5 MOS)

- Used when flows are associated with a preferred uplink
- Will use preferred uplink if MOS for paths is >3.5 MOS
- Will not use alternative path even if MOS for path is higher

## Best for VoIP (Best MOS)

- Flows are routed via the best performing path for MOS
- If the calculated MOS for a given path becomes better, it will be immediately preferred

# Policies – Custom Performance Classes

- Custom combination of latency, jitter and loss
- Application specific
- Performance criteria
- Service Level Agreement or Service Level Target mapping
- Managed Service Provider based

Overlay  
SD-WAN



Internet  
SD-WAN

Custom performance  
classes

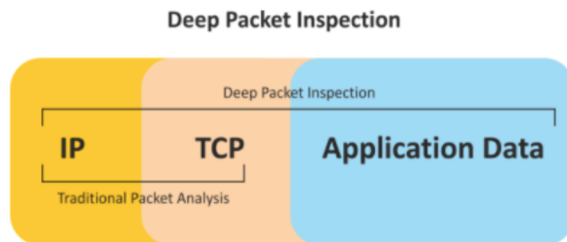
| Name     | Maximum latency (ms) | Maximum jitter (ms) | Maximum loss (%) | Actions |
|----------|----------------------|---------------------|------------------|---------|
| O365     | 200                  | 50                  | 5                | ×       |
| ICA      | (none)               | (none)              | 2                | ×       |
| Platinum | 150                  | 20                  | 1                | ×       |
| Gold     | 250                  | 40                  | 3                | ×       |
| Silver   | 250                  | 50                  | 5                | ×       |
| Bronze   | 500                  | 50                  | 10               | ×       |

[Create a new custom performance class...](#)

**\*\*Only 6 Total\*\***  
**\*\*Configurable\*\***

# Policies – Traffic Analysis (NBAR2)

| Traffic filters                |                                   |
|--------------------------------|-----------------------------------|
| <a href="#">Add +</a>          |                                   |
| Custom expressions             | All File sharing                  |
| Advertising                    | Apple file sharing                |
| Blogging                       | Box                               |
| Business management            | Dropbox                           |
| Databases & cloud services     | File Transfer [Default Data]      |
| Email                          | Financial Information eXchange    |
| File sharing                   | ftp protocol control over TLS/SSL |
| Gaming                         | Globus GridFTP                    |
| Health care                    | Google Talk File Transfer         |
| News                           | Grid FTP                          |
| Online backup                  | Hangouts File Transfer            |
| Peer-to-peer (P2P)             | Mega                              |
| Productivity                   | Microsoft OneDrive                |
| Remote monitoring & management | Microsoft-DS                      |



## Current Solution

- Overlay SDWAN
- SD-Internet (underlay)
- VPN Exclusion
- SaaS Tracking (Insight)

Plus – NGFW, Full Stack  
Traffic Analytics



**1500 Apps**

supported with NBAR

# Policies – Custom Expressions

**Source Specific**

**Custom expressions**

Protocol:

Source:  Src port:

Destination:  Dst port:

**Custom expressions**

Protocol:

Source:

Destination:

**Custom expressions**

Protocol:

Source:  Src port:

Destination:  Dst port:

Alternative

**Custom expressions**

Protocol:

Source:  Src port:

Destination:  Dst port:

## URL Destination

**Custom expressions**

Protocol:

Source:  Src port:

Destination:  Dst port:

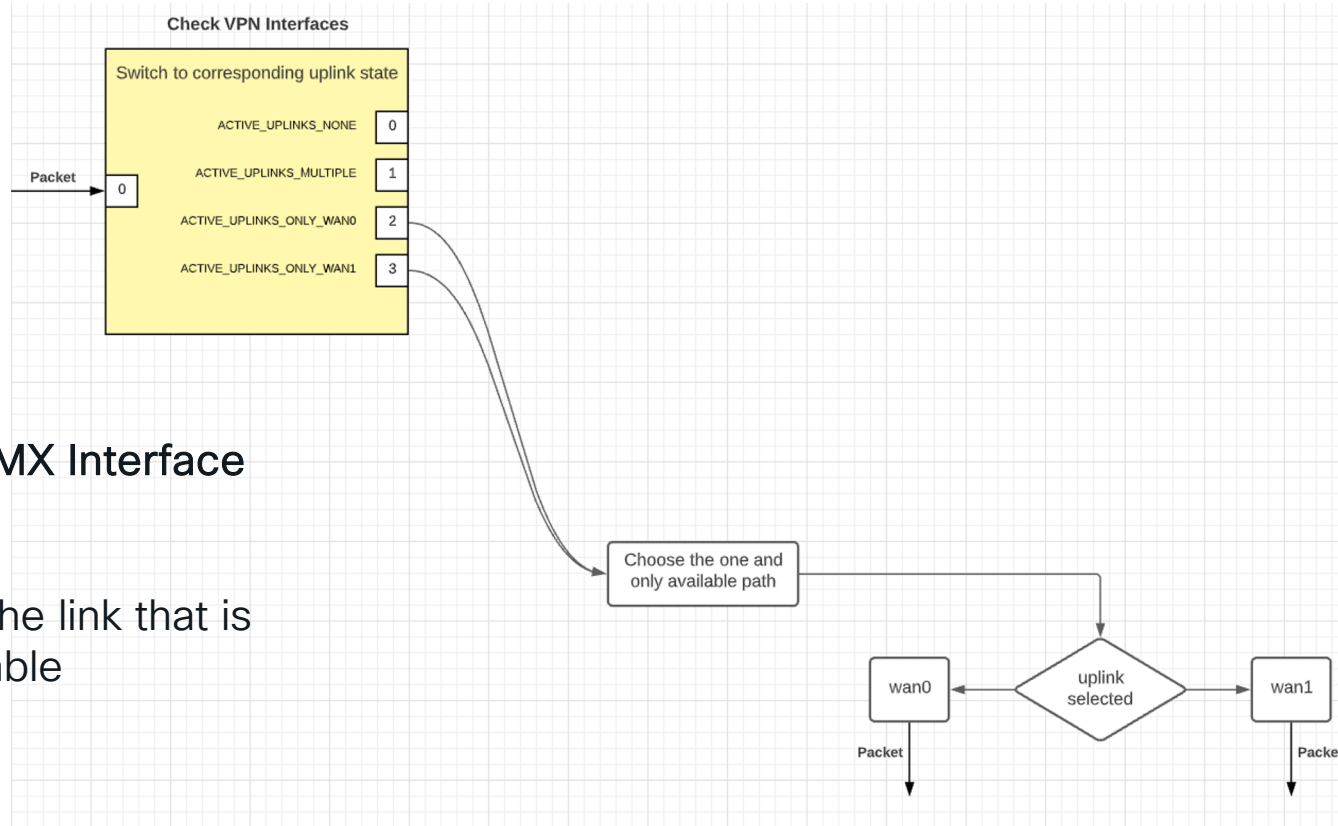
Alternative

# Policies – Side Note on Hostnames





# Policies – Interface Logic



## Default MX Interface Logic

- Use the link that is available

# Policies – DPS/PfR – Performance Only



**Uplink selection policy**✕

**Traffic filters**

Office 365 ✕

Add +

**Policy**

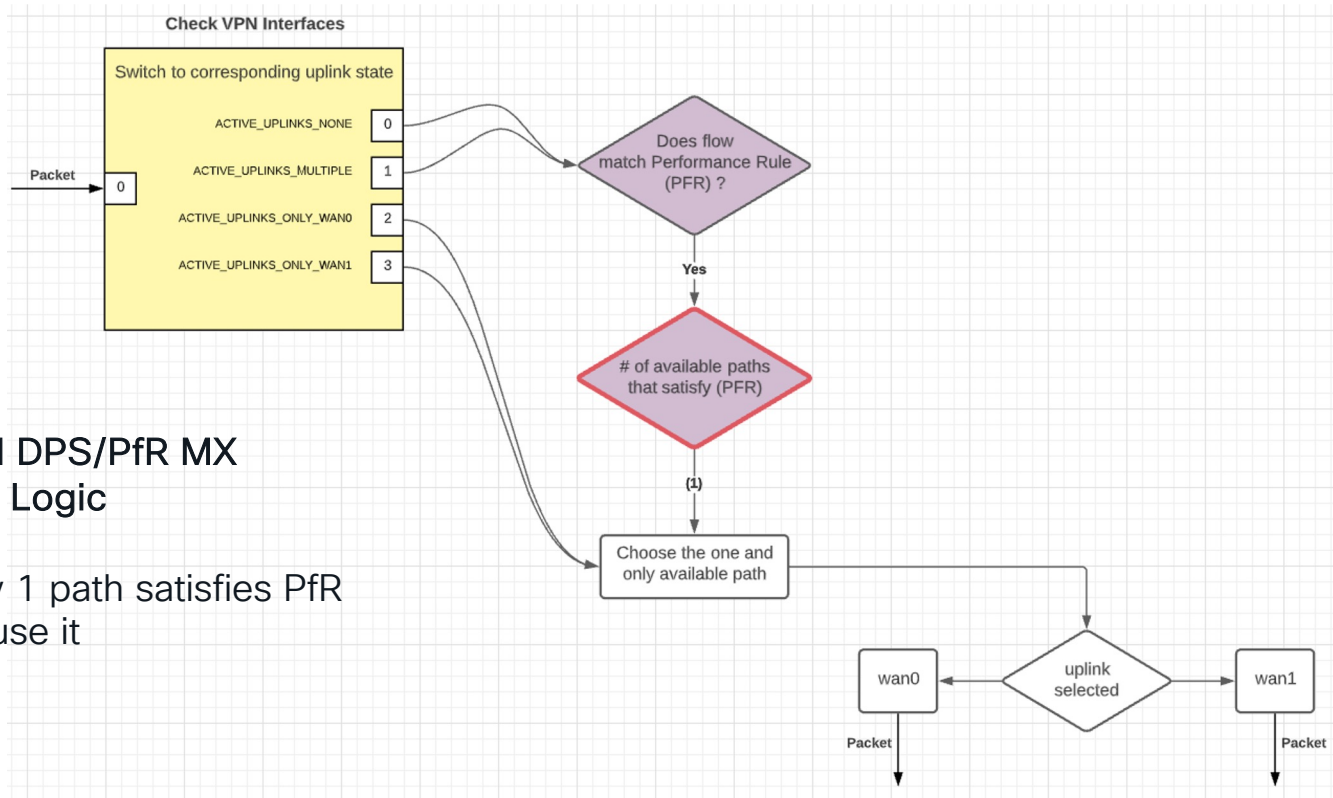
Preferred uplink: 

Best for VoIP ↕

Save



# Policies – DPS/PfR – Performance Only



## SD-WAN DPS/PfR MX Interface Logic

- If only 1 path satisfies PfR then use it

# Policies – DPS/PfR – With PBR



## Uplink selection policy



### Traffic filters

Office 365



Add +

### Policy

Preferred uplink:

WAN 1



Fail over if:

Poor performance



Performance class:

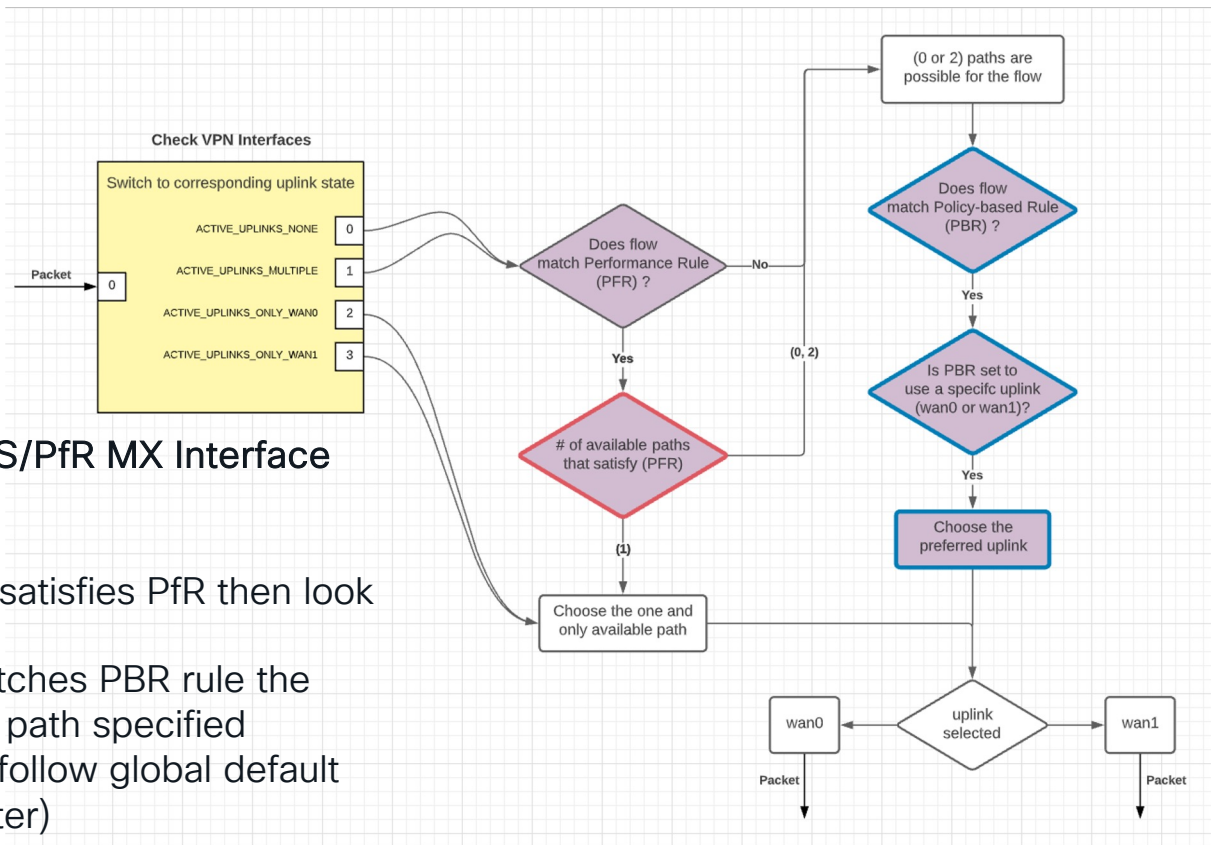
o365



Save



# Policies – DPS/PfR – With PBR



## SD-WAN DPS/PfR MX Interface Logic

- If 2 paths satisfies PfR then look at PBR
- If flow matches PBR rule the follow the path specified
- If no PBR follow global default (shown later)

# Policies – PBR



## Uplink selection policy



### Traffic filters

Facebook



Add +

### Policy

Preferred uplink:

WAN 2



Fail over if:

Uplink down



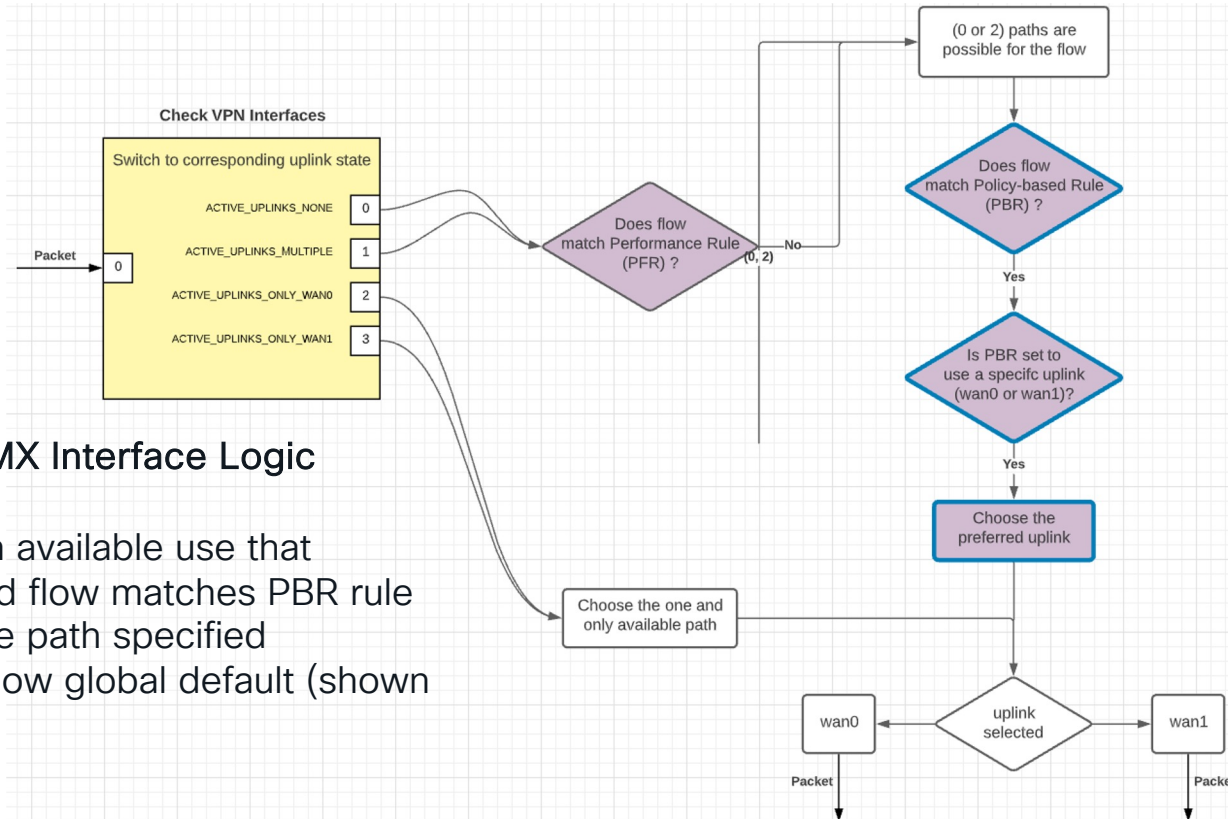
Save

# Policies - PBR



## SD-WAN PBR MX Interface Logic

- If only 1 path available use that
- If 2 paths and flow matches PBR rule the follow the path specified
- If no PBR follow global default (shown later)



# Policies – Global Preference



## Uplink selection policy

Traffic filters

All News × Add +

Policy

Preferred uplink: Global preference ↕

Uplink selection

Global preferences

Primary uplink: WAN 2 ⓘ

Load balancing

☒ Enabled

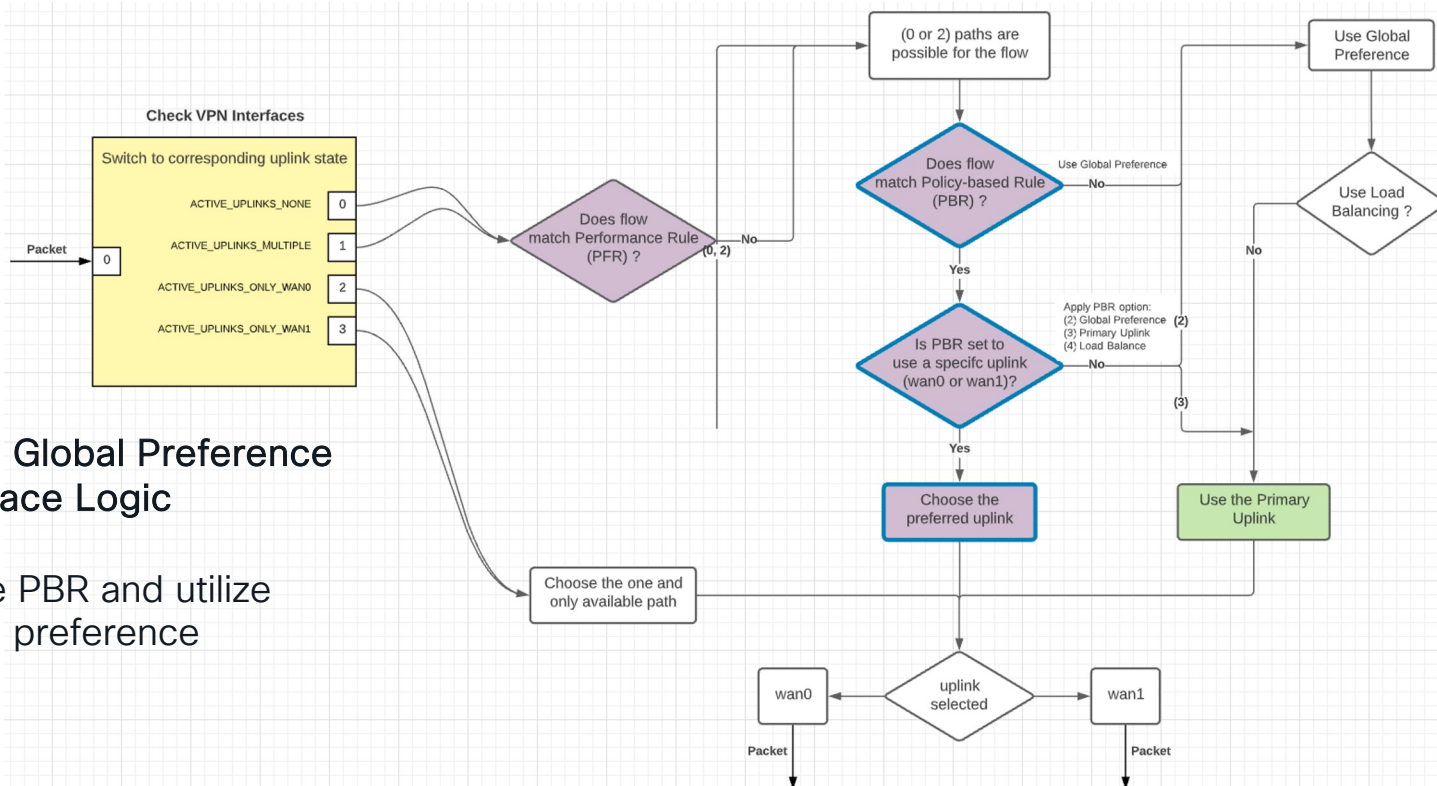
Traffic will be spread across both uplinks in the proportions specified above. Management traffic to the Meraki cloud will use the primary uplink.

☐ Disabled

All Internet traffic will use the primary uplink unless overridden by an uplink preference.

Save

# Policies – Global Preference



## SD-WAN Global Preference MX Interface Logic

- Ignore PBR and utilize global preference

# Policies – Performance Based Load Balance



## Uplink selection policy



### Traffic filters

Office 365



Add

### Policy

Preferred uplink:

Load balance



On uplinks that meet  
performance class:

o365



### Uplink selection

#### Global preferences

Primary uplink

WAN 2

Load balancing

☒ Enabled

Traffic will be spread across both uplinks in the proportions specified above.  
Management traffic to the Meraki cloud will use the primary uplink.

☐ Disabled

All Internet traffic will use the primary uplink unless overridden by an uplink preference.

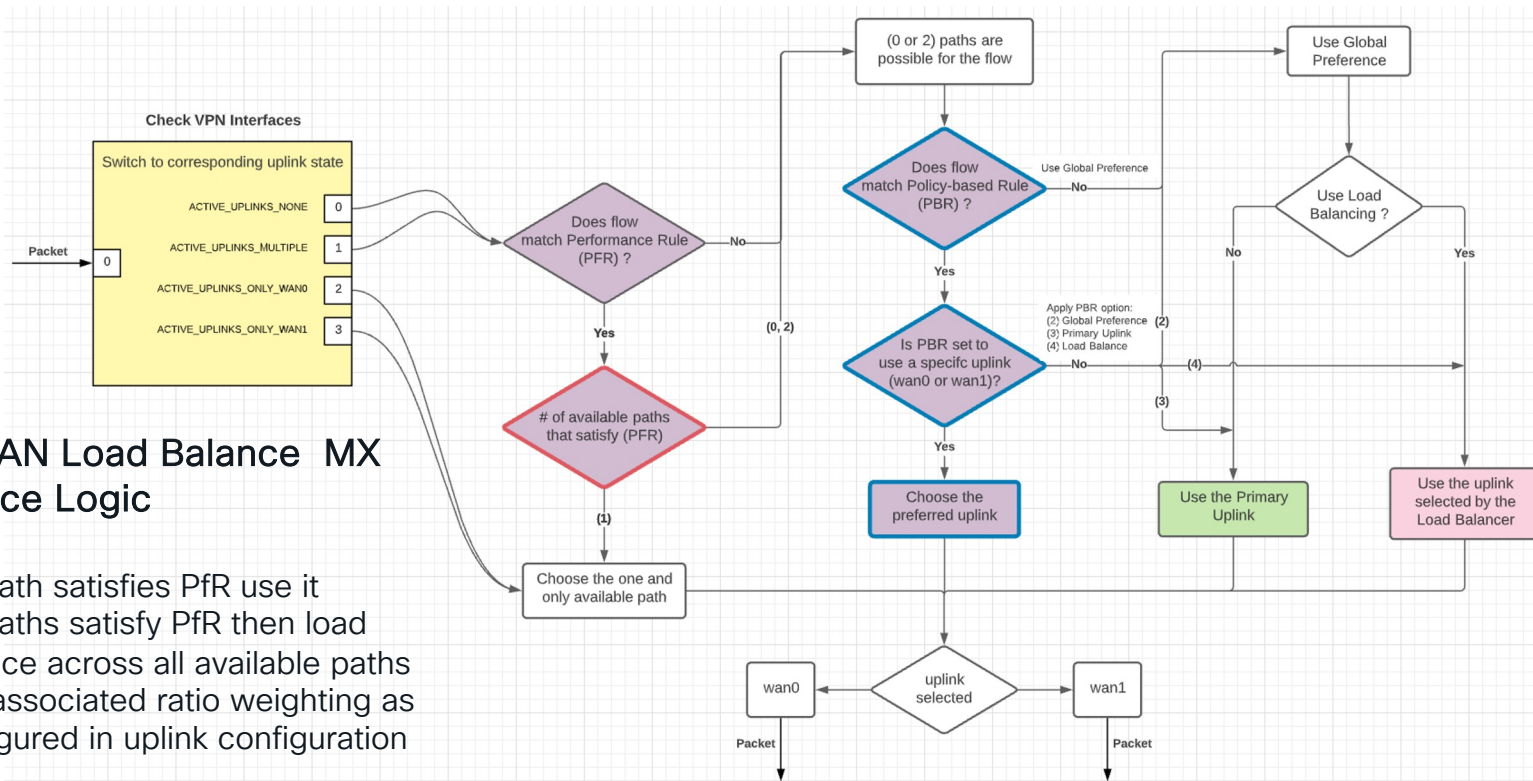
Save

# Policies – Performance Based Load Balance

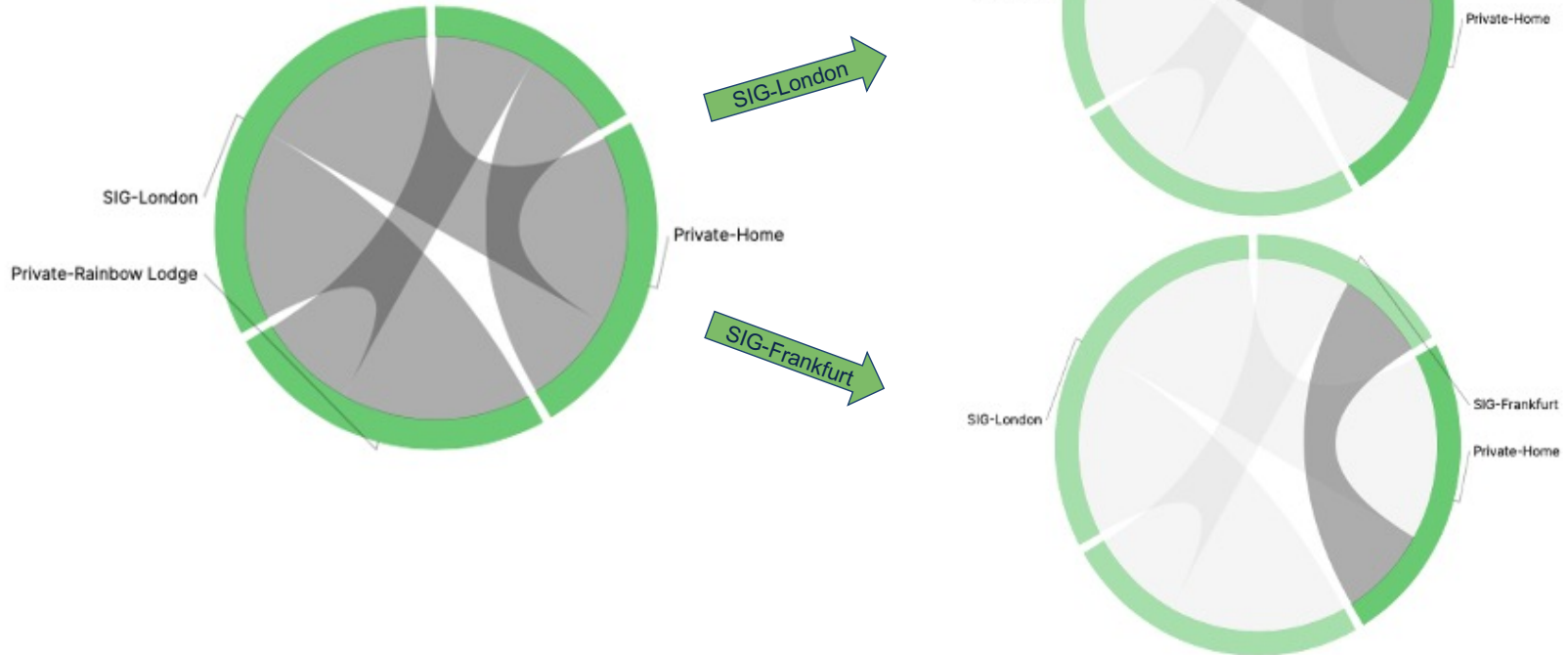


## SD-WAN Load Balance MX Interface Logic

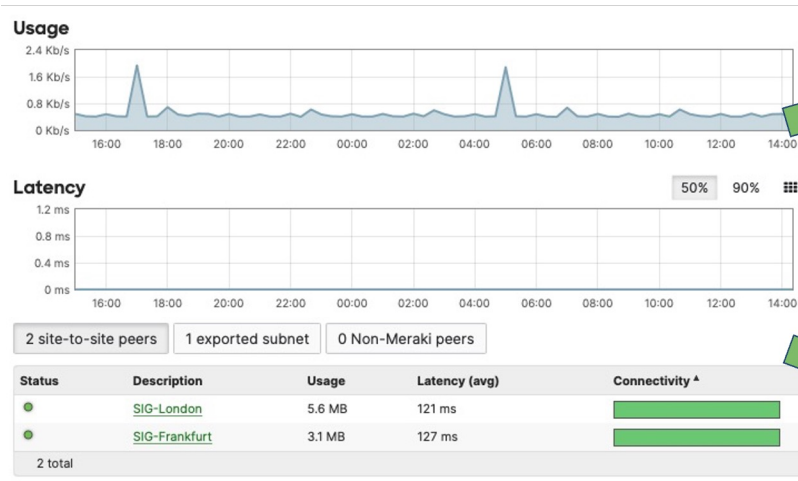
- If 1 path satisfies PfR use it
- If 2 paths satisfy PfR then load balance across all available paths
- Use associated ratio weighting as configured in uplink configuration



# Reporting – The Funky Pie Chart



# Reporting – AutoVPN Peers



SIG-London

SIG-Frankfurt



# Reporting – IWAN (Yes! IWAN)

## IWAN Page

- Custom view of 2-hour, day, week or month
- Shows measured latency, jitter and loss with calculated MOS

Local MX  
Umbrella Connector-Los Angeles

### Custom performance classes

| Name               | Latency (ms) | Jitter (ms) | Loss (%) |
|--------------------|--------------|-------------|----------|
| Umbrella Connector | 100          | 20          | 2        |

### VPN flow preferences

Load balance on uplinks that are suitable for "Umbrella Connector", any from any:any to any:any

Modify VPN flow preferences on the [traffic shaping page](#)



Local MX

Umbrella Connector-Los Angeles

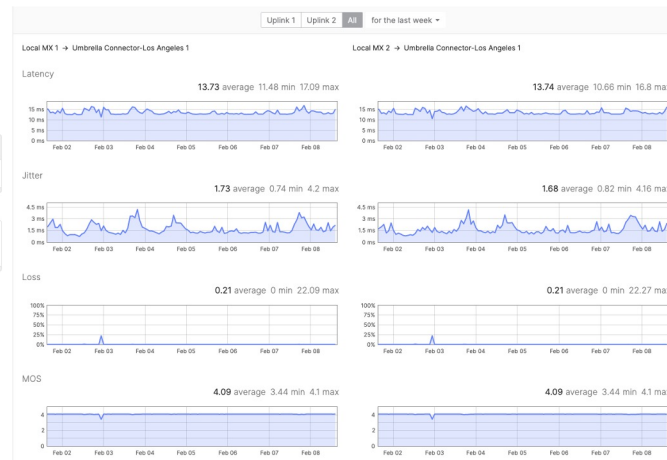
### Custom performance classes

| Name               | Latency (ms) | Jitter (ms) | Loss (%) |
|--------------------|--------------|-------------|----------|
| Umbrella Connector | 100          | 20          | 2        |

### VPN flow preferences

Load balance on uplinks that are suitable for "Umbrella Connector", any from any:any to any:any

Modify VPN flow preferences on the [traffic shaping page](#)



## Highlight Perf Class for compliance

- Allows for historical view of actual performance versus required performance
- Allows for historical inference of flow routing over SD-WAN fabric

# Reporting – Uplink Decisions

## Uplink decisions

| Peer                           | Protocol | Source            | Destination         | Uplink decision | Reason        | Policy                                                             | Last seen ▼ |
|--------------------------------|----------|-------------------|---------------------|-----------------|---------------|--------------------------------------------------------------------|-------------|
| San Francisco - appliance      | TCP      | 172.21.30.1:179   | 172.16.11:46918     | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | TCP      | 172.21.30.1:179   | 6.12.198.192:57337  | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | UDP      | 172.211.7:48808   | 209.206.53.173:7351 | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | TCP      | 172.21.30.1:34382 | 52.206.206.244:443  | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | TCP      | 172.21.10.6:48390 | 175.0.61.158:60870  | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | UDP      | 172.211.6:41707   | 209.206.48.17:7351  | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | UDP      | 172.211.6:45636   | 209.206.53.173:7351 | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | ICMP     | 172.211.6:31936   | 8.8.8.8:0           | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | ICMP     | 172.211.7:10855   | 8.8.8.8:0           | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | UDP      | 172.211.7:46382   | 209.206.48.17:7351  | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Palo Alto   | TCP      | 172.21.30.1:179   | 6.12.139.25:55114   | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | UDP      | 172.21.30.1:5557  | 13.229.110.108:2055 | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | UDP      | 172.211.4:41685   | 209.206.48.17:7351  | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | UDP      | 172.211.4:46715   | 209.206.53.173:7351 | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | ICMP     | 172.211.4:2989    | 8.8.8.8:0           | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| Umbrella Connector-Los Angeles | TCP      | 172.21.10.6:53282 | 146.112.61.106:80   | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| San Francisco - appliance      | TCP      | 172.21.30.1:179   | 172.16.11:45212     | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |

## Uplink decisions

| Peer                      | Protocol | Source          | Destination     | Uplink decision | Reason        | Policy                                                             | Last seen ▼ |
|---------------------------|----------|-----------------|-----------------|-----------------|---------------|--------------------------------------------------------------------|-------------|
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:39988 | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:46918 | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:13       |
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:45212 | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:12       |
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:44951 | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:10       |
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:35165 | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:08       |
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:59733 | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:07       |
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:39653 | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:05       |
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:40240 | WAN 1           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:03       |
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:39401 | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:02       |
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:45284 | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 09:00       |
| San Francisco - appliance | TCP      | 172.21.30.1:179 | 172.16.11:35907 | WAN 2           | Load balanced | Load balance on uplinks that are suitable for "Umbrella Connector" | 08:58       |

## Searchable for troubleshooting

- Source or destination IP address
- Peer or protocol too

## Real-time flow behavior of SD-WAN fabric

- All flow details (protocol, source, destination)
- Path followed => Uplink, reason and policy

# SD-WAN over Cellular



## What about integrated cellular MX?

- SD-WAN over (integrated) cellular
- Cellular interface takes over WAN2
- MX16 feature
- Supports MX67C & MX68CW

## Best SD-WAN over Cellular Solution = MG

- Allows for optimal placement
- External mounting
- Negligible loss over cable
- Integrated and external antenna options
- Multi-vendor (not just MX) solution

### Uplink configuration

Cellular active uplink ☒ Enabled [ⓘ](#)

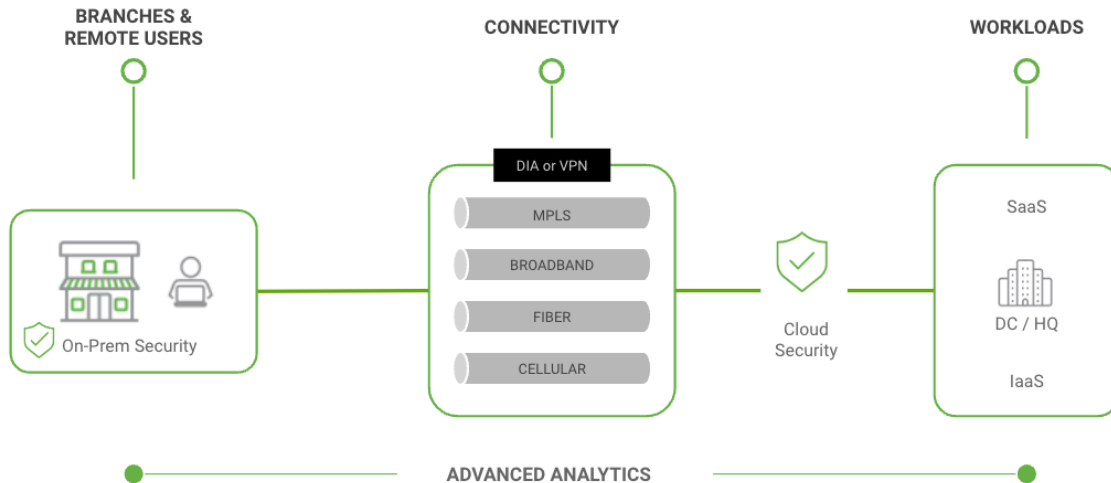
|          |           |                         |
|----------|-----------|-------------------------|
| WAN 1    | 600 Mbps  | <a href="#">details</a> |
| WAN 2    | 600 Mbps  | <a href="#">details</a> |
| Cellular | unlimited | <a href="#">details</a> |



# SD-Internet

# What is SD-Internet anyway?

- SD-Internet does SaaS what SD-WAN does to traditional apps
- More companies are moving to SaaS
- Optimises the underlay
- Ensures optimal quality of experience
- Eliminates the risk of SaaS adoption



# Network Config – Uplink Configuration

## Uplink configuration

Cellular active uplink Disabled

WAN 1  
down (Mb/s)  [simple](#)  
up (Mb/s)

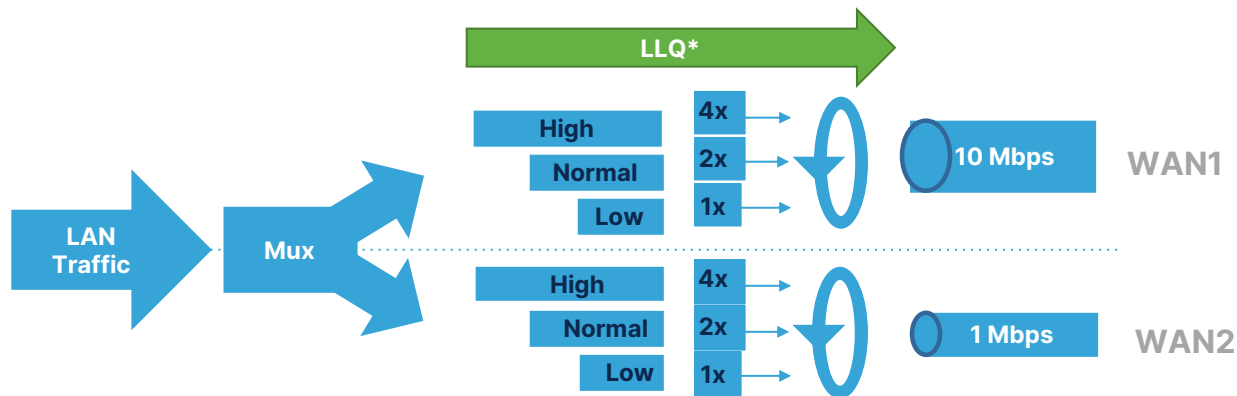
WAN 2  
down (Mb/s)  [simple](#)  
up (Mb/s)

Cellular  
unlimited [details](#)

## SD-WAN builds on network config

- Bandwidth (CIDR) config results in best possible performance
- All queues are FIFO based
- 3 Weighted Round Robin (WRR) queues
- High:Normal:Low are 4:2:1 ratioed
- LLQ rides over the top

Proper CIDR  
Configuration  
Vital



# Network Config – Uplink Selection

## Uplink selection

### Global preferences

Primary uplink

WAN 1

Load balancing

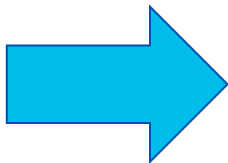
☒ Enabled

Traffic will be spread across both uplinks in the proportions specified a Management traffic to the Meraki cloud will use the primary uplink.

☐ Disabled

All Internet traffic will use the primary uplink unless overridden by an up

Results in 'Load  
Balance' policies not  
being possible



## Uplink Selection

- Network default configuration
- SD-WAN policies selectively deviate from this
- If policies are not matching flows, underlay routing will follow this configuration
- Very simple but often used incorrectly

## Uplink selection

### Global preferences

Primary uplink

WAN 1

Load balancing

☐ Enabled

Traffic will be spread across both uplinks in the proportions specified Management traffic to the Meraki cloud will use the primary uplink.

☒ Disabled

All Internet traffic will use the primary uplink unless overridden by a

# Network Config – Uplink Statistics

## Uplink statistics

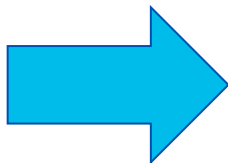
| Test Connectivity to | Description     | Default                          | Actions |
|----------------------|-----------------|----------------------------------|---------|
| 8.8.8.8              | Google          | <input type="radio"/>            | ×       |
| 208.67.220.220       | 2nd ODNS        | <input type="radio"/>            | ×       |
| 208.67.222.222       | OpenDNS Primary | <input checked="" type="radio"/> | ×       |

[Add a destination](#)

## Uplink Statistics

- ICMP based
- Used in connection monitor
- Provides per transport latency, loss and jitter data
- Data is also used for SD-Internet probing

Uplink statistics  
used for live  
reporting



### Historical device data for the last day ▾

Connectivity to 208.67.222.222 ⓘ

#### Latency



#### Loss



# Performance Calculations (SD-Internet)

- Exactly the same as SD-WAN (overlay) performance calculations with the following differences:
  - ICMP based as opposed to UDP
  - All transport classified by single (pinger) location
  - Probes sent over all transport networks
  - Ping is always 1/sec and never changes

$$MOS = \frac{\sum_{n=1}^N R_n}{N}$$



1 second probing

- Latency, Jitter, Loss & MOS are the average of the last 30 seconds of data, i.e., at least 30 probes



Loss & MOS are the average of the last 30 seconds of data, i.e., at least 30 probes

# SaaS Optimization – VPN Exclusions

## Applications Based

- NBAR based with up to 1500 apps
- Uses NBAR2 DPI engine

## SD-WAN Plus Only

### Traffic filters

Add +

|                                |                                   |
|--------------------------------|-----------------------------------|
| Custom expressions             | All File sharing                  |
| Advertising                    | Apple file sharing                |
| Blogging                       | Box                               |
| Business management            | Dropbox                           |
| Databases & cloud services     | File Transfer (Default Data)      |
| Email                          | Financial Information eXchange    |
| File sharing                   | ftp protocol control over TLS/SSL |
| Gaming                         | Globus GridFTP                    |
| Health care                    | Google Talk File Transfer         |
| News                           | Grid FTP                          |
| Online backup                  | Hangouts File Transfer            |
| Peer-to-peer (P2P)             | Mega                              |
| Productivity                   | Microsoft OneDrive                |
| Remote monitoring & management | Microsoft-DS                      |



**1500 Apps**

supported with NBAR

## Custom Expression

- Allows for custom L3/4 rule creation only

### Local internet breakout

VPN exclusion rules

Office 365 Suite x Webex x Salesforce x Office 365 Sharepoint x Layer 3 Any to 82.163.125.250/32 x

Add +

### Global bandwidth

Per-client limit

### Traffic shaping rule

Default Rules

Custom expressions

Major applications **BETA**

Custom expressions

Protocol  
TCP

Destination ⓘ  
Enter a CIDR/hostname  
Any

Dst port ⓘ  
443

IP: 17.0.0.0/8

Add

All Advertising, All Software Updates, All Online Backups 10 (AF11 - High Throughput, Latency Insensitive, Low Drop)

# SaaS Optimization – Traffic Analytics & CPCs

\*\*\*SD-WAN Plus for SaaS\*\*\*



## Traffic Analytics

- Used NBAR2 engine

## Custom Performance Classes

Custom performance  
classes

- 6 configurable, shared with SD-WAN overlay
- Logically distinct in code
- Allows for future breakout

| Name     | Maximum latency (ms) | Maximum jitter (ms) | Maximum loss (%) | Actions |
|----------|----------------------|---------------------|------------------|---------|
| O365     | 200                  | 50                  | 5                | X       |
| ICA      | (none)               | (none)              | 2                | X       |
| Platinum | 150                  | 20                  | 1                | X       |
| Gold     | 250                  | 40                  | 3                | X       |
| Silver   | 250                  | 50                  | 5                | X       |
| Bronze   | 500                  | 50                  | 10               | X       |

[Create a new custom performance class...](#)

# SaaS Optimization – Policies

## \*\*\*SD-WAN Plus for SaaS\*\*\*

CIDR ⓘ  
Any

Port ⓘ  
Any

### Destination

☐ Application Categories ☐ Major Applications ☒ Custom

CIDR ⓘ  
Any

Port ⓘ  
Any

### Destination

☒ Application Categories ☐ Major Applications ☐ Custom

|                                             |   |                                                            |
|---------------------------------------------|---|------------------------------------------------------------|
| <input checked="" type="checkbox"/> Email   | > | <input type="checkbox"/> Gmail                             |
| <input type="checkbox"/> Blogging           | > | <input type="checkbox"/> Yahoo Mail                        |
| <input type="checkbox"/> File sharing       | > | <input type="checkbox"/> Rackspace Hosted Exchange         |
| <input type="checkbox"/> News               | > | <input type="checkbox"/> Hotmail                           |
| <input type="checkbox"/> Sports             | > | <input type="checkbox"/> Windows Live Hotmail and Outlook  |
| <input type="checkbox"/> Gaming             | > | <input type="checkbox"/> Web based email                   |
| <input type="checkbox"/> Online backup      | > | <input type="checkbox"/> Host-based email (POP3/IMAP/SMTP) |
| <input type="checkbox"/> Peer-to-peer (P2P) | > |                                                            |

### Different UI per policy type

- Red section for custom L3/4 expressions
- Blue section for NBAR2 or Major L7 applications

# SaaS Optimization – Policy Options

PfR for  
configured 'SD-  
Int' perf class

\*\*\*SD-WAN Plus for SaaS\*\*\*

## Destination

☒ Application Categories ☐ Major Applications ☐ Custom

WebEx X

|                                                               |   |                                                              |
|---------------------------------------------------------------|---|--------------------------------------------------------------|
| <input type="checkbox"/> Social web & photo sharing           | > | <input type="checkbox"/> Skype                               |
| <input type="checkbox"/> Software & anti-virus updates        | > | <input type="checkbox"/> SIP (Voice)                         |
| <input type="checkbox"/> Video & music                        | > | <input type="checkbox"/> Vocera                              |
| <input checked="" type="checkbox"/> VoIP & video conferencing | > | <input type="checkbox"/> SCCP (Skinny Call Control Protocol) |
| <input type="checkbox"/> Web file sharing                     | > | <input checked="" type="checkbox"/> WebEx                    |
| <input type="checkbox"/> Security                             | > | <input type="checkbox"/> Dropcam                             |
| <input type="checkbox"/> Productivity                         | > |                                                              |
| <input type="checkbox"/> Remote monitoring & management       | > |                                                              |
| <input type="checkbox"/> Business management                  | > |                                                              |

## Policy

Preferred Uplink

Best for VoIP v

PfR for built-in  
'Best for VoIP'  
CPC

Cancel Save

## Destination

☒ Application Categories ☐ Major Applications ☐ Custom

Office 365 X

|                                                         |   |                                                |
|---------------------------------------------------------|---|------------------------------------------------|
| <input type="checkbox"/> Video & music                  | > | <input checked="" type="checkbox"/> Office 365 |
| <input type="checkbox"/> VoIP & video conferencing      | > | <input type="checkbox"/> Windows Live Office   |
| <input type="checkbox"/> Web file sharing               | > | <input type="checkbox"/> Adobe Creative Cloud  |
| <input type="checkbox"/> Security                       | > | <input type="checkbox"/> Symphony.NET          |
| <input checked="" type="checkbox"/> Productivity        | > | <input type="checkbox"/> Sharepoint            |
| <input type="checkbox"/> Remote monitoring & management | > | <input type="checkbox"/> Slack                 |
| <input type="checkbox"/> Business management            | > |                                                |
| <input type="checkbox"/> Health care                    | > |                                                |

## Policy

Preferred Uplink

WAN 1 v

Fail over if:

Poor performance v

Performance class:

SD-Int v

Cancel Save

# SaaS Optimization – Policy Options (cont)

## \*\*\*SD-WAN Plus for SaaS\*\*\*

Load Balance for  
configured 'SD-Int'  
perf class

### Destination

☒ Application Categories ☐ Major Applications ☐ Custom

Facebook X

|                                                                |   |                                              |
|----------------------------------------------------------------|---|----------------------------------------------|
| <input type="checkbox"/> Online backup                         | > | <input type="checkbox"/> Picasa              |
| <input type="checkbox"/> Peer-to-peer (P2P)                    | > | <input type="checkbox"/> MySpace             |
| <input checked="" type="checkbox"/> Social web & photo sharing | > | <input type="checkbox"/> Flickr              |
| <input type="checkbox"/> Software & anti-virus updates         | > | <input type="checkbox"/> smugmug             |
| <input type="checkbox"/> Video & music                         | > | <input checked="" type="checkbox"/> Facebook |
| <input type="checkbox"/> VoIP & video conferencing             | > | <input type="checkbox"/> Twitter             |
| <input type="checkbox"/> Web file sharing                      | > | <input type="checkbox"/> img.ly              |
| <input type="checkbox"/> Security                              | > | <input type="checkbox"/> Instagram           |
| <input type="checkbox"/> Productivity                          | > |                                              |

### Policy

Preferred Uplink

WAN 2 v

Fail over if:

Uplink Down v

PBR to  
WAN2

Cancel

Save

### Destination

☒ Application Categories ☐ Major Applications ☐ Custom

Citrix ICA X Remote desktop X

|                                                                    |   |                                                    |
|--------------------------------------------------------------------|---|----------------------------------------------------|
| <input type="checkbox"/> VoIP & video conferencing                 | > | <input type="checkbox"/> Citrix Online             |
| <input type="checkbox"/> Web file sharing                          | > | <input checked="" type="checkbox"/> Citrix ICA     |
| <input type="checkbox"/> Security                                  | > | <input checked="" type="checkbox"/> Remote desktop |
| <input type="checkbox"/> Productivity                              | > | <input type="checkbox"/> MyRMM                     |
| <input checked="" type="checkbox"/> Remote monitoring & management | > | <input type="checkbox"/> Marconet                  |
| <input type="checkbox"/> Business management                       | > | <input type="checkbox"/> auvik                     |
| <input type="checkbox"/> Health care                               | > |                                                    |
| <input type="checkbox"/> Web payments                              | > |                                                    |

### Policy

Preferred Uplink

Load Balance v

On uplinks that meet performance class:

SD-Int v

Cancel

Save

# SaaS Optimization – Policy Options (cont)

## \*\*\*SD-WAN Plus for SaaS\*\*\*

### Destination

☒ Application Categories ☐ Major Applications ☐ Custom

Citrix ICA X Remote desktop X

|                                                                    |   |                                                    |
|--------------------------------------------------------------------|---|----------------------------------------------------|
| <input type="checkbox"/> VoIP & video conferencing                 | > | <input type="checkbox"/> Citrix Online             |
| <input type="checkbox"/> Web file sharing                          | > | <input checked="" type="checkbox"/> Citrix ICA     |
| <input type="checkbox"/> Security                                  | > | <input checked="" type="checkbox"/> Remote desktop |
| <input type="checkbox"/> Productivity                              | > | <input type="checkbox"/> MyRMM                     |
| <input checked="" type="checkbox"/> Remote monitoring & management | > | <input type="checkbox"/> Marconet                  |
| <input type="checkbox"/> Business management                       | > | <input type="checkbox"/> auvik                     |
| <input type="checkbox"/> Health care                               | > |                                                    |
| <input type="checkbox"/> Web payments                              | > |                                                    |

### Policy

#### Preferred Uplink

Global Preference v

Cancel

Save

### Destination

☐ Application Categories ☐ Major Applications ☒ Custom

#### CIDR ⓘ

17.0.0.0/8

#### Port ⓘ

Any

### Policy

#### Preferred Uplink

WAN 1 v

#### Fail over if:

Poor performance v

#### Performance class:

SD-Int v

Cancel

Save

Follow the  
Global  
Preference

Custom Expression PfR for  
configured 'SD-Int' perf  
class

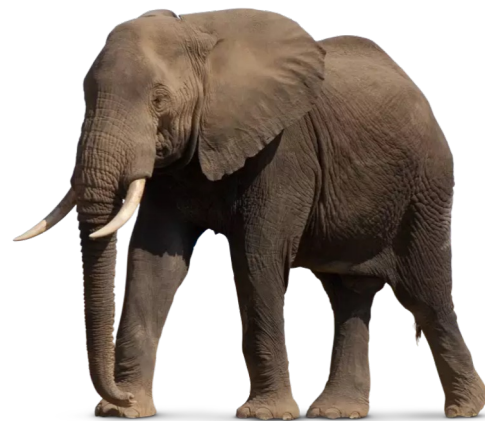
# Scaling

# Scaling – Tunnel Count

## Problem Statement

- Current largest physical MX support max recommend tunnel count of 1500
- Full mesh node crosses this with 751 nodes
- Even a 2 hub H&S hub node crosses this with 749 spoke nodes

\*\*\*Large customers will need a design\*\*\*



## Hub & Spoke

$$\left( \frac{H(H-1)}{2} \right) \times L_1 + (S \times N) \times L_2$$

$$(H-1) \times L_1 + S \times L_2$$

$$N \times L_2$$

Where:

H is the number of hubs  
L<sub>1</sub> is the number of links a hub has  
S is the number of spokes  
N is the number of hubs configured per spoke

L<sub>2</sub> is the number of links per spoke

## Full Mesh

$$\frac{N(N-1)}{2} \times L_1$$

$$(N-1) \times L_1$$

Where:

N is the number of hubs  
L<sub>1</sub> is the number of links a hub has

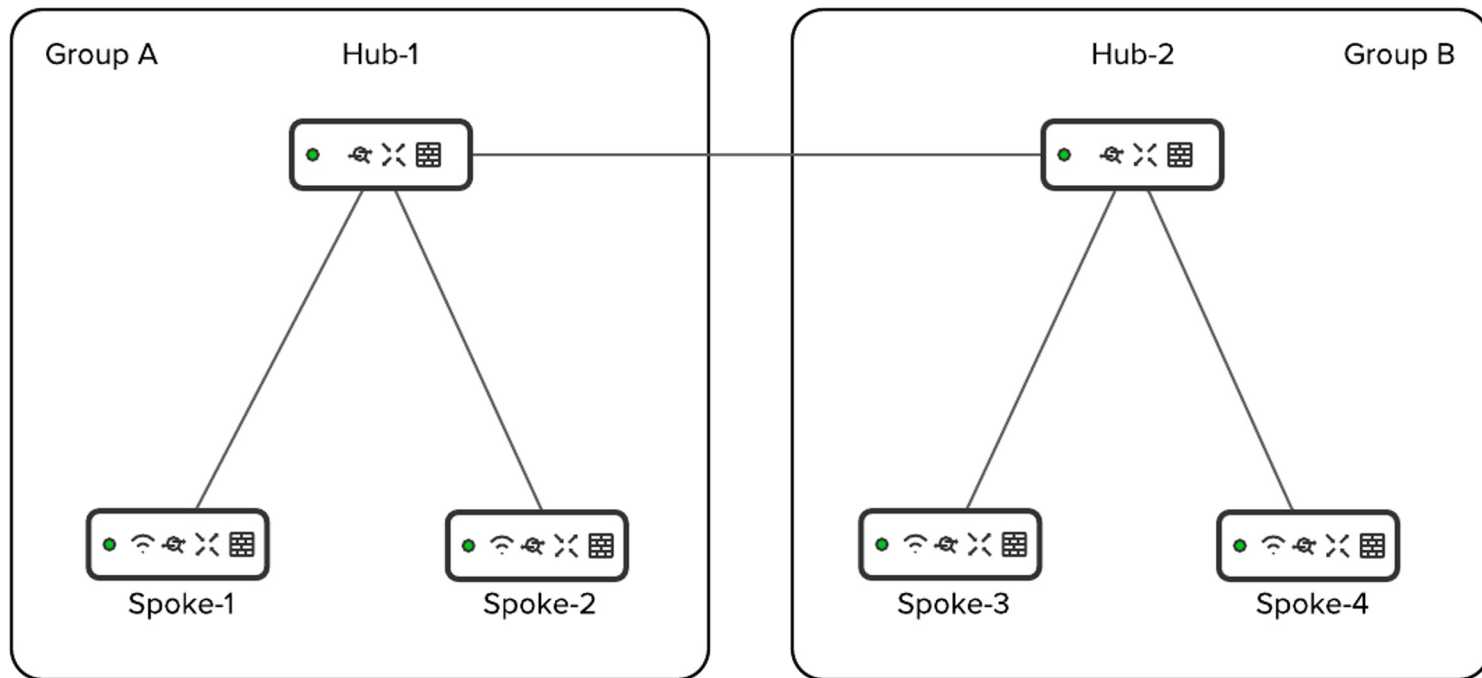
# Scaling – Group Scaling

## Solution:

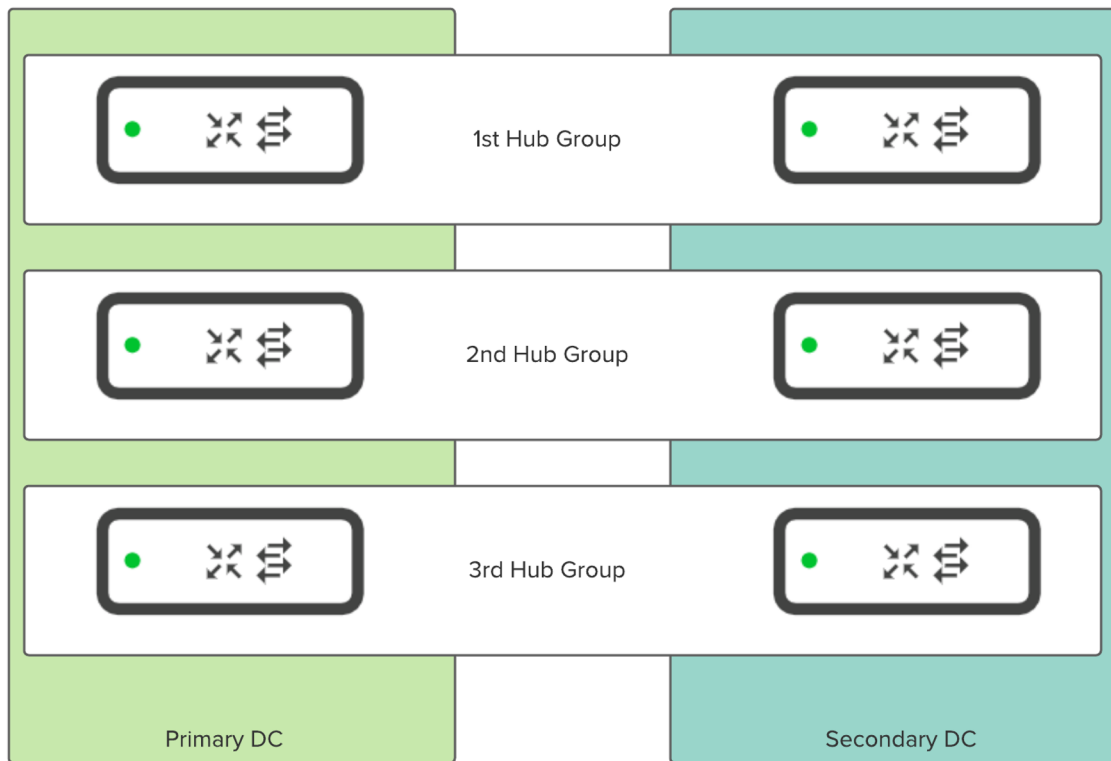
- Create multiple spoke groups associated with a HA pair of MXs

## Problems:

- HA failover is slow
- Requires underlay to re-establish
- SD-WAN failover not possible



# Scaling – Horizontal Scaling (N+N)



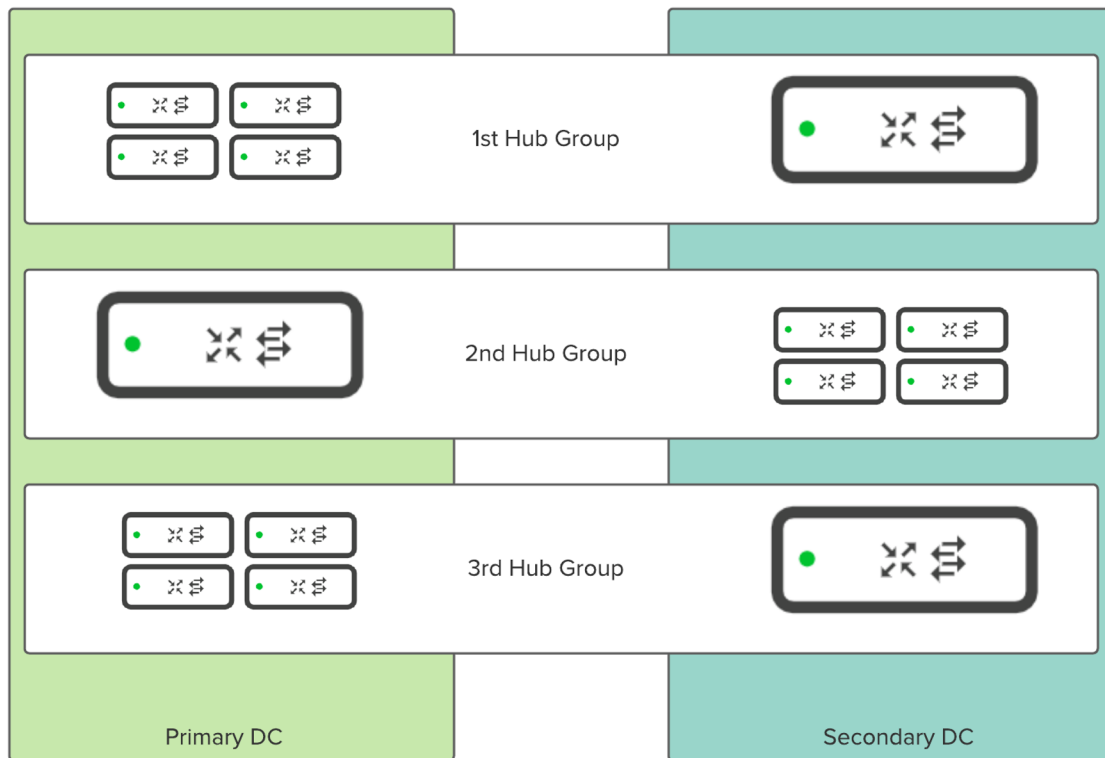
## Solution:

- For each hub group both MXs are active
- All spokes form active tunnels to each MX
- SD-WAN failover and hubs can be geo-diverse, no SPOF
- 'Best' solution

## Problems:

- Increased tunnel count on spokes and other hubs
- Additional license cost
- Most expensive solution

# Scaling – Horizontal Scaling (N+1)



## Solution:

- A 'backup hub' is shared amongst a hub group
- Spokes tunnel to 1 hub from group and backup hub
- Most scalable solution

## Problems:

- Increased tunnel count on spokes and other hubs
- Additional license cost

# Scaling – Templates & APIs

## Templates

- Good feature coverage
- Required to yield specific control
- Local override for some but not all features
- Best scale
- Affects speed of change

## API

- Lagging feature coverage
- Designer maintains control
- If there's an API you can control it
- Requires external platform or specific skill set to scale
- Only limited by calls/second

Largest

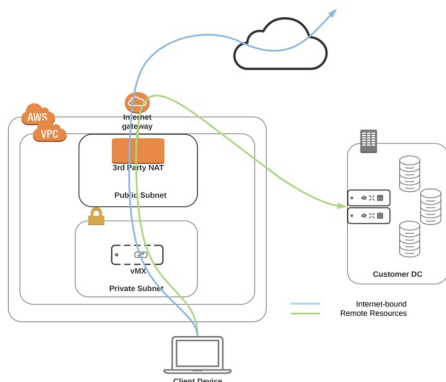
Terraform

Fastest

# What's new?

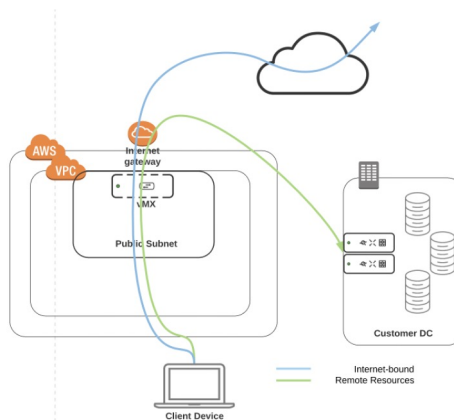
# NAT Mode vMX

Connect



## PROBLEM

More and more customers are moving workloads to the cloud and require internet bound traffic to go via the vMX. This causes additional complexity on the cloud as a NAT device needs to be placed upstream of the vMX.



## SOLUTION

NAT Mode vMX will simplify cloud deployments. Customers **no longer need to rely on 3rd party solutions** where NAT is required. It also simplifies routing on the cloud and allows customers to easily configure and manage core networking features via the Meraki dashboard.

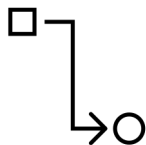


## COMPATIBILITY

**Platform:** All vMX SKUs (vMX-S/M/L)

**Licensing:** ENT

# Non-Meraki VPN peering with FQDN



## PROBLEM

VPN peering to an IP address inherently creates a single point of failure, thus creating a need for additional configuration and complexity.



## SOLUTION

Non-Meraki peering with FQDN allows for MXs to build Non-Meraki VPN tunnels to the FQDN of a peer, **eliminating the single point of failure** whilst concurrently allowing for regional load balancing via anycast DNS resolution.



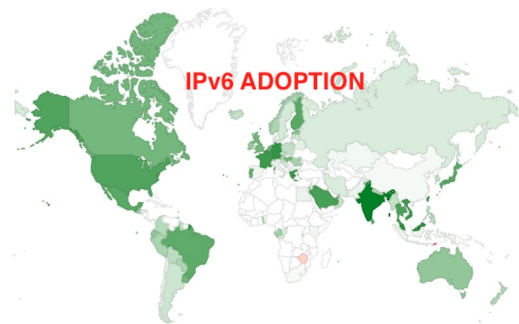
## COMPATIBILITY

**Platform:** Z3, Z3C, Z4, Z4C, MX64, MX64W, MX65, MX65W, MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX450

**Licensing:** ENT, ADV, SDWAN+

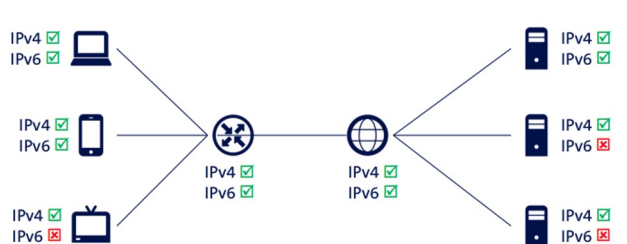
# IPv6 Phase 2

Connect



## PROBLEM

Lack of public IPv4 addresses and continued global IPv6 growth with increased IPv6 regulations are limiting next-gen services.



## SOLUTION

Phase 1 was focused on connectivity and Phase 2 **focused on scalability** with the introductions such as AMP, TG, OSPF, EBGp, and many more.

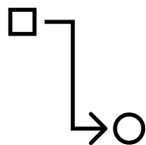


## COMPATIBILITY

**Platform:** Z3, Z3C, Z4, Z4C, MX64, MX64W, MX65, MX65W, MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX450

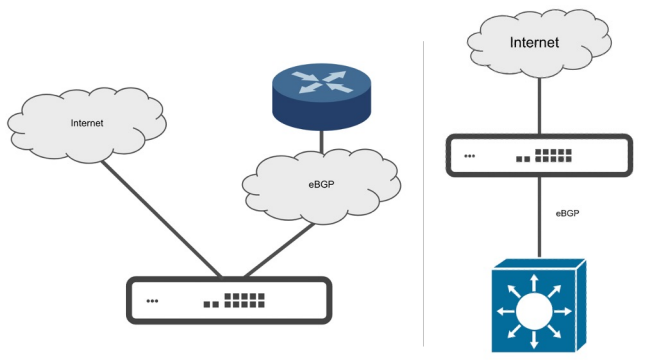
**Licensing:** ENT, ADV, SDWAN+

# Routed Mode eBGP



## PROBLEM

Customers are limited in datacentre design and ease of transition to overlay networking due current BGP versatility.



## SOLUTION

Allow for eBGP on the WAN with authentication.

Allow for eBGP LAN for edge MX

New visibility added to see status of BGP sessions.

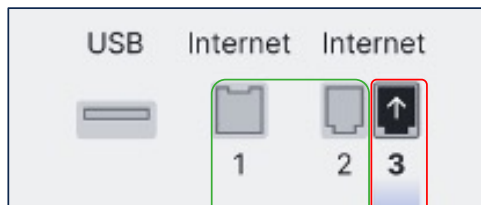


## COMPATIBILITY

**Platform:** Z4, Z4C, MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX85, MX95, MX105, MX250, MX450

**Licensing:** ENT, ADV, SDWAN+

# Multi-WAN (2+1)

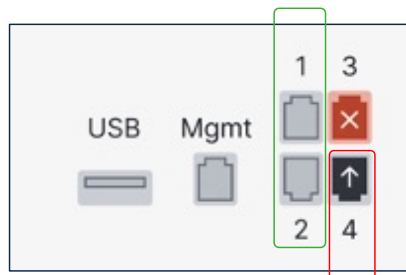


2 Active WAN uplinks

1 Backup WAN uplink

## PROBLEM

Customers want to more than 2 transport connections to provide extra resilience through redundancy



1 Backup WAN uplink  
(port 4 is PoE capable to power MG)

## SOLUTION

Starting with 2+1 all MXs that support >2 physical WAN interfaces will be able to failover to a tertiary WAN connection in the event of the failure of the primary and secondary connections.



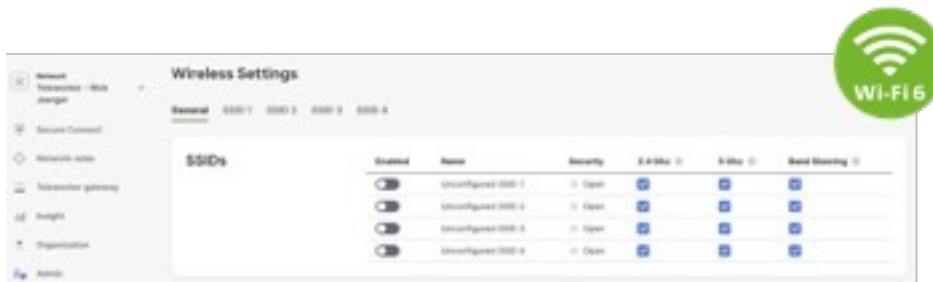
## COMPATIBILITY

**Platform:** MX75, MX85, MX95, MX105

**Licensing:** ENT, ADV, SDWAN+

# Wi-Fi 6

Connect



## PROBLEM

Customers who deploy teleworker gateways in challenging and contended Wi-Fi environments often struggle to provide a good wireless experience.

Also, making changes to a fleet of integrated Wi-Fi teleworker appliances is challenging

## SOLUTION

Starting with the Z4 and the Z4C Meraki teleworker gateways now have Wi-Fi 6 and all of the high-density benefits, such as OFDMA.

In addition to this the Wi-Fi settings page has been updated and API endpoints have been added for greater manageability

## COMPATIBILITY

**Platform:** Z4, Z4C

**Licensing:** ENT, ADV Teleworker



# Advanced Teleworker

Connect

## Advanced security

- One-click Cisco Advanced Malware Protection (AMP)
- Protection for unknown files with ThreatGrid
- Cisco Talos content filtering
- Built-in UI integration for Cisco Umbrella cloud security

## PROBLEM

With more and more SaaS applications requiring direct (underlay) routing, the utility of a device that solely extends the office network into a employee's home office is limited.

## Advanced analytics with ML

- Automatically applied Smart Thresholds to identify true app degradation
- At-a-glance performance of apps across the LAN, home uplink, and app server
- Instant root-cause analysis of degradation with intelligent recommendations
- Status of all remote worker uplinks in one view, including cellular

## SOLUTION

Starting with the Z4 and the Z4C Meraki teleworker gateways can now be configured with an advanced license.

This allows customers to see the QoE of SaaS applications with ML powered advanced analytics from remote locations whilst also securing them with Cisco Talos backed technology.



## COMPATIBILITY

**Platform:** Z4, Z4C

**Licensing:** ENT, ADV Teleworker

# vMX-L in Azure and vMX-XL in AWS



## PROBLEM

More and more customers moving workloads to the cloud, requiring higher throughputs and greater scale.



## SOLUTION

vMX-L supported across all Azure regions with support of up to 1-Gbps VPN throughput.

Highly scalable vMX with up to 10 Gbps VPN throughput from a single instance.

Highly cost effective by using optimized compute instances with up to 8 vCPUs.



## COMPATIBILITY

**Platform:** vMX-L, vMX-XL

**Licensing:** ENT

# Cloud OnRamp (AWS)

Connect



## PROBLEM

Customers are moving to one or more clouds, but managing multiple environments is complex, requiring:

- Nuanced processes
- Differing user experiences
- Varying configurations

| Status                   | Instance name                           | Provider | vMX type | Instance type | Instance ID | Region            |
|--------------------------|-----------------------------------------|----------|----------|---------------|-------------|-------------------|
| <input type="checkbox"/> | vMX AWS US East (N. Virginia) Primary   | AWS      | vMX-L    | c5.large      |             | US East (N. Virg) |
| <input type="checkbox"/> | vMX AWS US East (N. Virginia) Secondary | AWS      | vMX-S    | c5.small      |             | US East (N. Virg) |

## SOLUTION

Deploy and manage your vMX via the Meraki dashboard.

- Unified and automated cloud management
- Expand network connectivity
- Consistent user experience



## COMPATIBILITY

**Platform:** vMX-S/M/L

**Licensing:** ENT

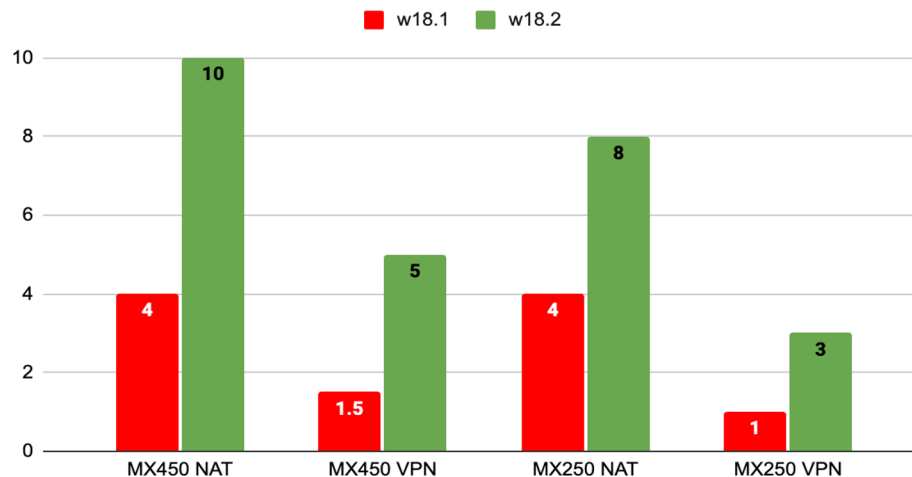
# Performance Boost



Up to 3x

Performance  
Enhancement for  
MX75, MX250 &  
MX450

*Performance Optimized Firmware Throughput (EMIX)*



Platform: MX250, MX450

Licensing: ENT, ADV, SDW+

# Adaptive Policy

Supported = SGT preservation, propagation, and assignment

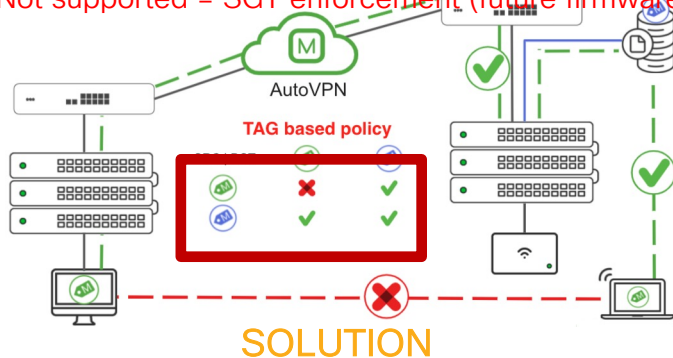
Not supported = SGT enforcement (future firmware)

| #  | Policy | Protocol | Source IP                      | Src port | Destination IP          | Dst port | Comment                 | Logging  | Hits | Action |
|----|--------|----------|--------------------------------|----------|-------------------------|----------|-------------------------|----------|------|--------|
| 1  | [deny] | TCP      | 192.168.200.101/255.255        | Any      | 192.168.0.1/4/23        | 443      | DMZ - HTTPS             | Disabled | 0    | Deny   |
| 2  | [deny] | TCP      | 192.168.200.101/255.255        | Any      | 192.168.0.1/4/23        | Any      | DMZ - HTTP              | Disabled | 0    | Deny   |
| 3  | [deny] | TCP      | 192.168.200.101/255.255        | Any      | 192.168.0.1/4/23        | Any      | DMZ - IPsec             | Disabled | 0    | Deny   |
| 4  | [deny] | TCP      | 192.168.200.101/255.255        | Any      | 192.168.0.1/4/23        | Any      | DMZ - All Other         | Disabled | 0    | Deny   |
| 5  | [deny] | TCP      | Any                            | Any      | 192.168.200.101/255.255 | 443      | ADPS                    | Disabled | 0    | Deny   |
| 6  | [deny] | TCP      | 192.168.0.0/16, 192.168.0.0/16 | Any      | Any                     | Any      | Default Allow           | Disabled | 0/23 | Deny   |
| 7  | [deny] | TCP      | 192.168.0.0/16                 | Any      | 172.16.16.0/24          | Any      | PLC Network Query       | Disabled | 0    | Deny   |
| 8  | [deny] | TCP      | 172.16.16.0/23                 | Any      | Any                     | 443,80   | Client Traffic          | Disabled | 2031 | Deny   |
| 9  | [deny] | TCP      | 172.16.16.0/23                 | Any      | 192.168.0.0/16          | Any      | Client Guard Inter View | Disabled | 205  | Deny   |
| 10 | [deny] | TCP      | 192.168.0.0/16                 | Any      | 172.16.16.0/23          | Any      | Client Guard Inter View | Disabled | 0    | Deny   |
| 11 | [deny] | TCP      | 192.168.0.0/16                 | Any      | 172.16.16.0/23          | Any      | Client Guard CSMP       | Disabled | 1889 | Deny   |
| 12 | [deny] | TCP      | 172.16.16.0/24                 | Any      | 192.168.0.0/16          | Any      | Client Guard CSMP       | Disabled | 0    | Deny   |
| 13 | [deny] | TCP      | 172.16.16.0/24                 | Any      | 192.168.0.0/16          | Any      | Client Guard CSMP       | Disabled | 0    | Deny   |
| 14 | [deny] | TCP      | Any                            | Any      | Any                     | Any      | Default Deny            | Disabled | 1824 | Deny   |
|    | Allow  | Any      | Any                            | Any      | Any                     | Any      | Default Allow           | Disabled | 0/23 | Allow  |

## PROBLEM

Traditional segmentation is based on subnets, VLANs and ACL rules.

The rule sets are limited to the network which it resides in and is not meant to be globally scalable.



## SOLUTION

Cisco's solution to this challenging problem is Cisco TrustSec (CTS). Each group is **assigned to a Security Group Tag (SGT)** and all user traffic associated with the group inherits the tag and its associated enforcement policy.

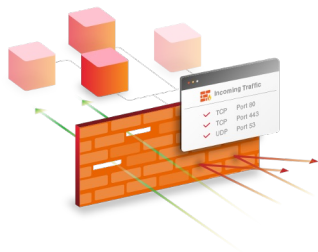


## COMPATIBILITY

**Platform:** Z3, Z3C, Z4, Z4C, MX64, MX64W, MX65, MX65W, MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX450,

**Licensing:** ENT, ADV, SDWAN+

# Firewall Logging Live Tool



## PROBLEM

Limited visibility and monitoring options into real-time FW decision-making make it harder for network admin to test policy configurations or FW rulesets, as well as troubleshoot active issues in the network.

Firewall Log

Client: Client filter (fuzzy) IP Address: Source or Destination (comm, Port) 15600 Allowed ☒ Blocked ☒ Start

Firewall log (78 entries) Download

Filter by: Firewall name

| Verdict | Time            | Source IP   | Source Port | Destination IP  | Destination Port | Protocol | Client                     | Firewall |
|---------|-----------------|-------------|-------------|-----------------|------------------|----------|----------------------------|----------|
| ✗       | May 16 15:51:55 | 192.168.0.4 | 48886       | 239.255.255.250 | 15600            | UDP      | rb0(nat/inet0/from_inet_fi |          |
| ✗       | May 16 15:51:58 | 192.168.0.4 | 54278       | 192.168.0.255   | 15600            | UDP      | rb0(nat/inet0/from_inet_fi |          |
| ✗       | May 16 15:52:01 | 192.168.0.4 | 48698       | 239.255.255.250 | 15600            | UDP      | rb0(nat/inet0/from_inet_fi |          |
| ✗       | May 16 15:52:04 | 192.168.0.4 | 59016       | 192.168.0.255   | 15600            | UDP      | rb0(nat/inet0/from_inet_fi |          |
| ✗       | May 16 15:52:07 | 192.168.0.4 | 35771       | 239.255.255.250 | 15600            | UDP      | rb0(nat/inet0/from_inet_fi |          |
| ✗       | May 16 15:52:10 | 192.168.0.4 | 47751       | 192.168.0.255   | 15600            | UDP      | rb0(nat/inet0/from_inet_fi |          |
| ✗       | May 16 15:52:13 | 192.168.0.4 | 50685       | 239.255.255.250 | 15600            | UDP      | rb0(nat/inet0/from_inet_fi |          |
| ✗       | May 16 15:52:16 | 192.168.0.4 | 55501       | 192.168.0.255   | 15600            | UDP      | rb0(nat/inet0/from_inet_fi |          |
| ✗       | May 16 15:52:19 | 192.168.0.4 | 58795       | 239.255.255.250 | 15600            | UDP      | rb0(nat/inet0/from_inet_fi |          |
| ✗       | May 16 15:52:22 | 192.168.0.4 | 33963       | 192.168.0.255   | 15600            | UDP      | rb0(nat/inet0/from_inet_fi |          |

10 Results per page

## SOLUTION

The live firewall log will allow network administrators to troubleshoot or test their firewall policies, rulesets and FW decision-making in real-time. Users will be able to monitor traffic events for L3/L7 FW, cellular failover, site-to-site VPN and group policies.

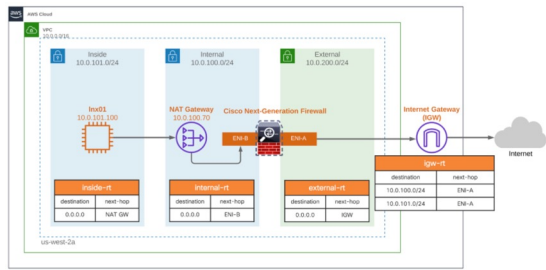


## COMPATIBILITY

**Platform:** Z4, Z4C, Z3, Z3C, MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX85, MX95, MX105, MX250, MX450, vMX-S/M/L

**Licensing:** ENT, ADV, SDWAN+

# Advanced Security vMX



## PROBLEM

Customers transitioning to the cloud have a common ask to secure both east-west flows within a given cloud (between subnets) as well as north-south traffic from workloads to the internet.



## SOLUTION

Advanced security features on the vMX enable users to secure their cloud environments.

Powered by  
**TALOS**



## COMPATIBILITY

**Platform:** vMX-S/M/L

**Licensing:** ADV

# Policy Object

Security

| #  | Policy | Protocol | Source IP        | Src port | Destination IP | Dst port         | Comment | Logging      | Hit     | Actions |
|----|--------|----------|------------------|----------|----------------|------------------|---------|--------------|---------|---------|
| 1  | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 443     | DNAT - HTTP  | Enabled | 5       |
| 2  | Allow  | HTTP     | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 80      | DNAT - HTTP  | Enabled | 0       |
| 3  | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 8080    | DNAT - HTTP  | Enabled | 0       |
| 4  | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 8080    | DNAT - HTTP  | Enabled | 1       |
| 5  | Allow  | TCP      | Any              |          | Any            | 192.168.0.104/32 | 443     | ADPS         | Enabled | 3       |
| 6  | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 8080    | Default rule | Enabled | 0       |
| 7  | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 8080    | Default rule | Enabled | 0       |
| 8  | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 8080    | Default rule | Enabled | 0       |
| 9  | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 8080    | Default rule | Enabled | 0       |
| 10 | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 8080    | Default rule | Enabled | 0       |
| 11 | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 8080    | Default rule | Enabled | 0       |
| 12 | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 8080    | Default rule | Enabled | 0       |
| 13 | Allow  | TCP      | 192.168.0.104/32 |          | Any            | 192.168.0.104/32 | 8080    | Default rule | Enabled | 0       |
| 14 | Allow  | TCP      | Any              |          | Any            | Any              | Any     | Default rule | Enabled | 0       |

**Policy Objects** BETA

Groups All objects

Search...

| # | Group name      | Contains            | Outbound rules |
|---|-----------------|---------------------|----------------|
| 1 | Virtual Machine | VM Out VM In        | 0              |
| 2 | Meraki MDs      | Firewall MDCS WSA   | 0              |
| 3 | Kids Devices    | Residence MSA       | 0              |
| 4 | Proxies         | Server HP OfficeJet | 0              |
| 5 | Servers         | Server Oracle VM    | 0              |
| 6 | Meraki APs      | AP Garage M57C      | 0              |
| 7 | Meraki Switches | Switch Kitchen M122 | 0              |

| # | Policy | Rule description     | Protocol | Source         | Src port | Destination | Dst port | Logging | Hit | Actions |
|---|--------|----------------------|----------|----------------|----------|-------------|----------|---------|-----|---------|
| 1 | Allow  | Allow Entertainment  | Any      | Server Desktop | Any      | Any         | Any      | 0       | 0   | ...     |
| 2 | Allow  | Allow Meraki Devices | Any      | Meraki APs     | Any      | Any         | Any      | 0       | 24  | ...     |
| 3 | Allow  | Allow Data Devices   | Any      | Client Desktop | Any      | Any         | Any      | 0       | 1   | ...     |
| 4 | Allow  | Allow Servers        | Any      | Server Desktop | Any      | Any         | Any      | 0       | 3   | ...     |
| 5 | Allow  | Allow Infrastructure | Any      | Server Desktop | Any      | Any         | Any      | 0       | 6   | ...     |
| 6 | Deny   | Deny IP Power        | Any      | IP Power       | Any      | Any         | Any      | 0       | 33  | ...     |
| 7 | Allow  | Default rule         | Any      | Any            | Any      | Any         | Any      | 0       | 0   | ...     |



## PROBLEM

Enterprise customers have complex firewalling needs, with traditional ACL based rules this can lead to very large rulesets that are difficult to visualise and troubleshoot

## SOLUTION

With policy objects customers can re-use clients and groupings of clients in multiple networks **resulting in policy consistency**, much smaller rulesets and easier troubleshooting

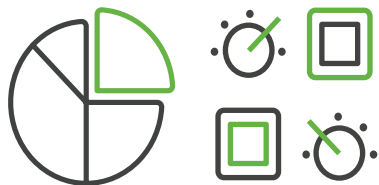
## COMPATIBILITY

**Platform:** Z3, Z3C, Z4, Z4C, MX64, MX64W, MX65, MX65W, MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX450

**Licensing:** ENT, ADV, SDWAN+

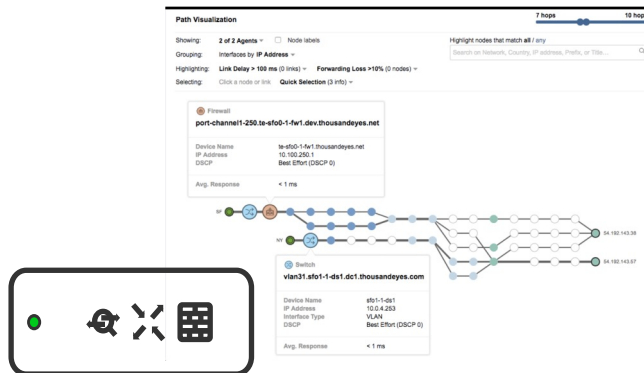
# ThousandEyes Agent

Automate



## PROBLEM

MI & SD-WAN analytics provide great near real-time data for organizations to leverage, however sometimes customers need to directly visualize the data path for optimal performance



## SOLUTION

ThousandEyes agents running directly on the MX give customers the ability to **view the application or overlay path and its hop-by-hop performance** for the best data to inform SD-WAN routing decisions



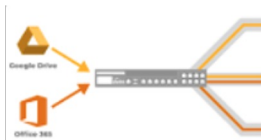
## COMPATIBILITY

**Platform:** MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX85, MX95, MX105, MX250, MX450

**Licensing:** SEC\*, SDWAN+

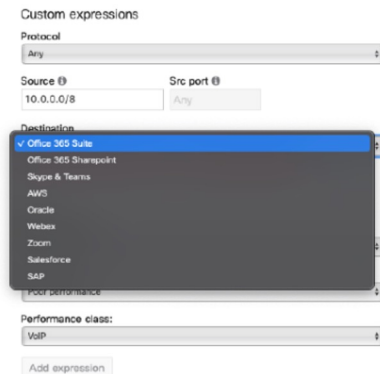
\*=Limited capability

# Non-Meraki VPN Exclusions



## PROBLEM

Many customer tunnel all internet bound traffic to an SSE platform for consistent application of security policies and application visibility, this does affect the quality of trusted SaaS applications.



## SOLUTION

Customers can now **exclude trusted SaaS applications from NMVPN tunnels** to 3rd party SSE platforms.

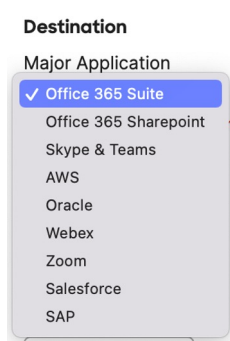


## COMPATIBILITY

**Platform:** Z4, Z4C, MX64, MX64W, MX65, MX65W, MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX450

**Licensing (L3):** ENT, ADV, SDWAN+  
**Licensing (L7/App):** SDWAN+/ADV Teleworker

# SD-Internet powered by NBAR2



## PROBLEM

Previously SD-Internet was Limited Applications (10 Apps)



**1500 Apps**

supported with NBAR

## SOLUTION

Leveraging NBAR for Steering traffic to SaaS or public cloud-based applications over the best performing WAN connection at the time the traffic is forwarded

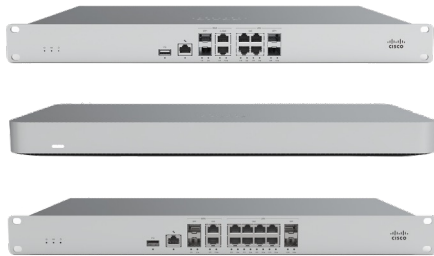


## COMPATIBILITY

**Platform:** MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX85, MX95, MX105, MX250, MX450

**Licensing:** SDWAN+

# Platform Story



## MX/Z SECURITY AND SD-WAN

Protect and securely  
connect what matters  
most, regardless of  
location



## MG WIRELESS WAN

Extend your network to  
anywhere with a cellular  
connection



## VIRTUAL MX (vMX)

Seamlessly extend  
your SD-WAN fabric  
to public or private  
cloud environments

# Engage with us: Become a Cisco Meraki Insider



Join  
the community



Complete  
challenges



Receive  
rewards



# Did you know?

You can have a  
one-on-one session with  
a technical expert!

Visit Meet the Expert in The HUB  
to meet, greet, whiteboard & gain  
insights about your unique questions  
with the best of the best.



## Meet the Expert Opening Hours:

|                  |                         |
|------------------|-------------------------|
| <b>Tuesday</b>   | <b>3:00pm – 7:00pm</b>  |
| <b>Wednesday</b> | <b>11:15am – 7:00pm</b> |
| <b>Thursday</b>  | <b>9:30am – 4:00pm</b>  |
| <b>Friday</b>    | <b>10:30am – 1:30pm</b> |

# Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



# Continue your education



- Visit the Cisco Showcase 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)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background is a vibrant, abstract graphic featuring a rainbow color palette. On the left, there are horizontal, wavy bands of color transitioning from red at the top to blue at the bottom. On the right, a bright white light source emits a series of sharp, triangular rays of color in a radial pattern, also using the rainbow spectrum. The overall effect is energetic and celebratory.

cisco *Live!*

Let's go

#CiscoLiveAPJC