

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Meraki SD-WAN

Designs, Approaches, and What's New

Anthony Belcastro
Technical Marketing Engineer - MXIG
BRKENS-1560



#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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-1560>





Agenda

- Introduction
- Site Connectivity
- Routing & Policy
- Integrations & Security
- Conclusion

Cisco Merakian for over 7 years

Look after routing and IPv6 on the platform

Played the role of partner, end customer before coming to Meraki



Anthony Belcastro

Technical Marketing Engineer

Meraki Device-to-Cloud Connectivity

Site Connectivity

- Device requests IP address
- Check in starts
 - FIPS 140 compliant connection over TCP 443 to the cloud controller
 - All data is continually duplicated between two separate cloud controllers
 - Initial WAN tests
 - Live tools populate
 - Download configuration
 - User traffic passes
 - Firmware & lists update
- Check in complete

Branch MX
MX68



ADDRESS
321 Kent St Sydney

WARM SPARE
[Configure warm spare](#)

WAN 1
[Configure WAN 1](#) **Active**

FIRMWARE
Up to date
Current version: MX 18.211.2
[Open source licenses](#)

CONFIG
Up to date



Auto VPN - Out of the box

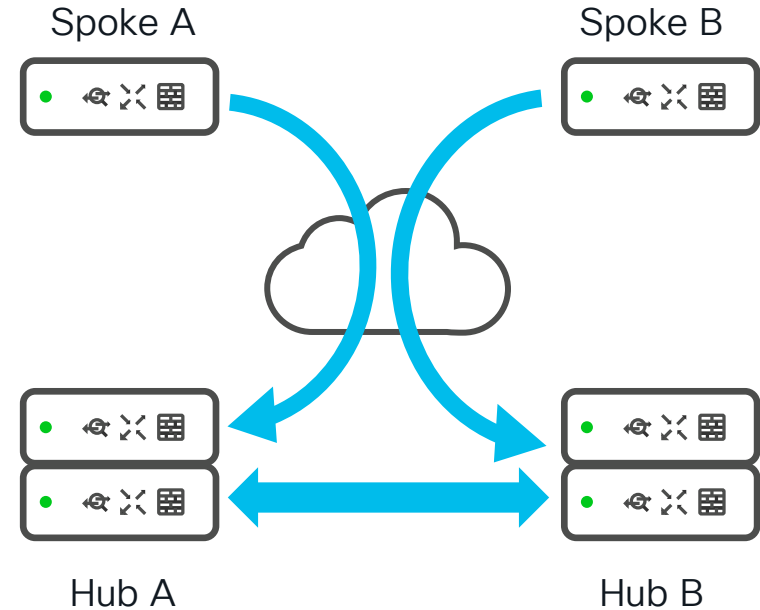
Site Connectivity

Spokes build tunnels to hubs that they have configured

Hubs build tunnels to spokes who have them configured as hubs

Hubs build tunnels to all other hubs

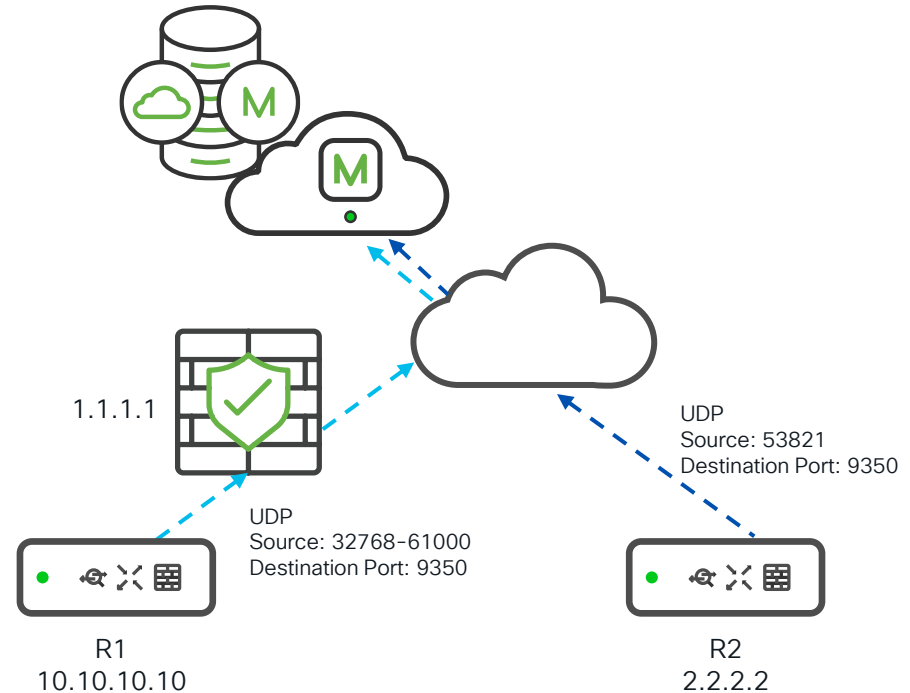
All MXs in an Auto VPN domain 'learn' about all routes included into the Auto VPN via dashboard unless additional controls are applied.



VPN Registry

Site Connectivity

R1& R2 makes a UDP connection
outbound on port 9350 to the VPN
registry

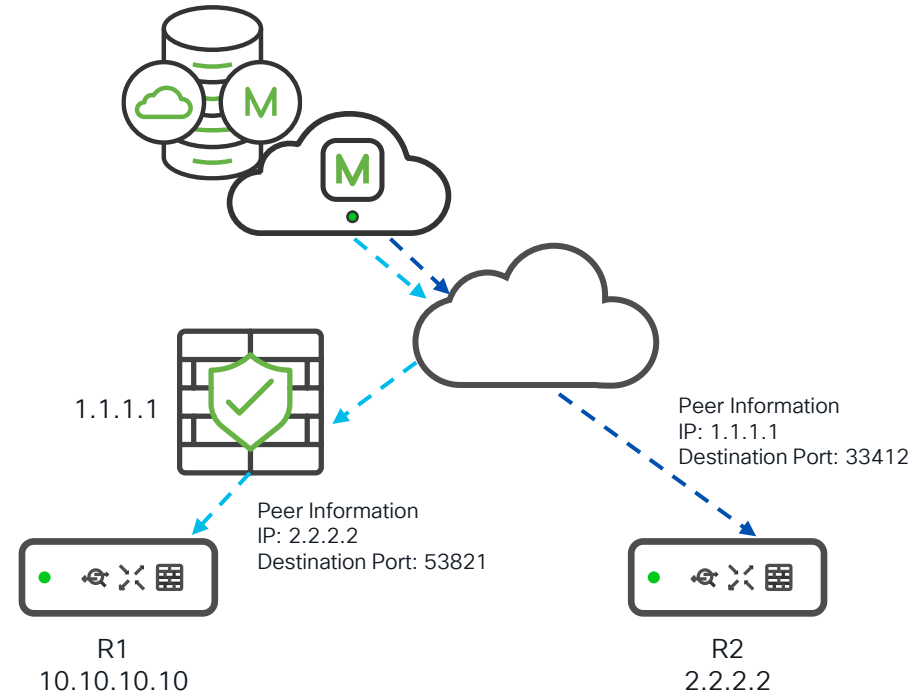


VPN Registry

Site Connectivity

VPN registry instructs R1 to connect to R2 at IP Address 2.2.2.2 and port 53821

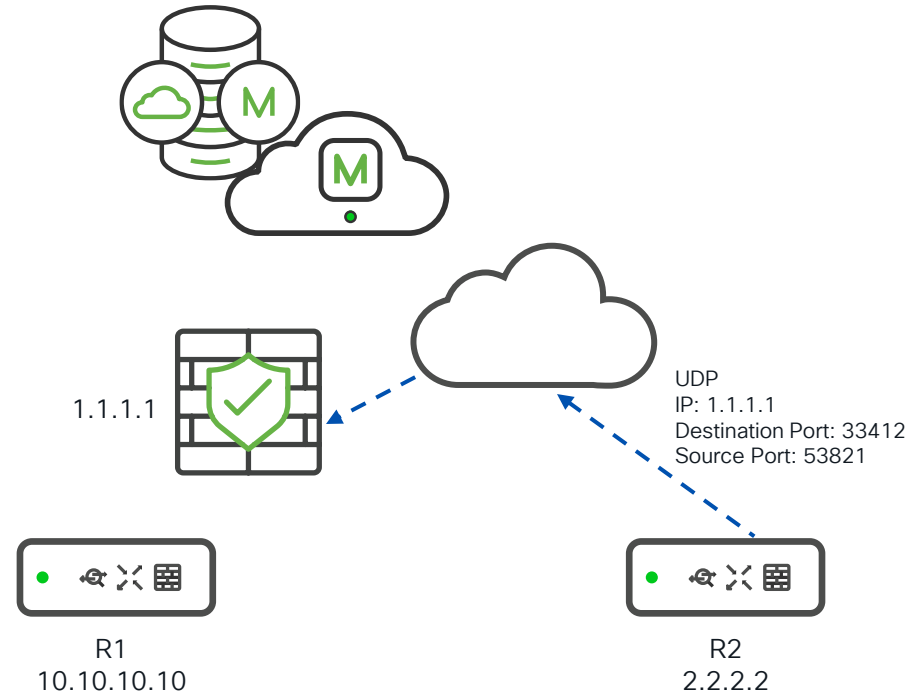
VPN registry instructs R2 to connect to R1 at IP Address 1.1.1.1 and port 33412



AutoVPN Convergence

Site Connectivity

R2 makes the connection to R1 but
is blocked by upstream firewall



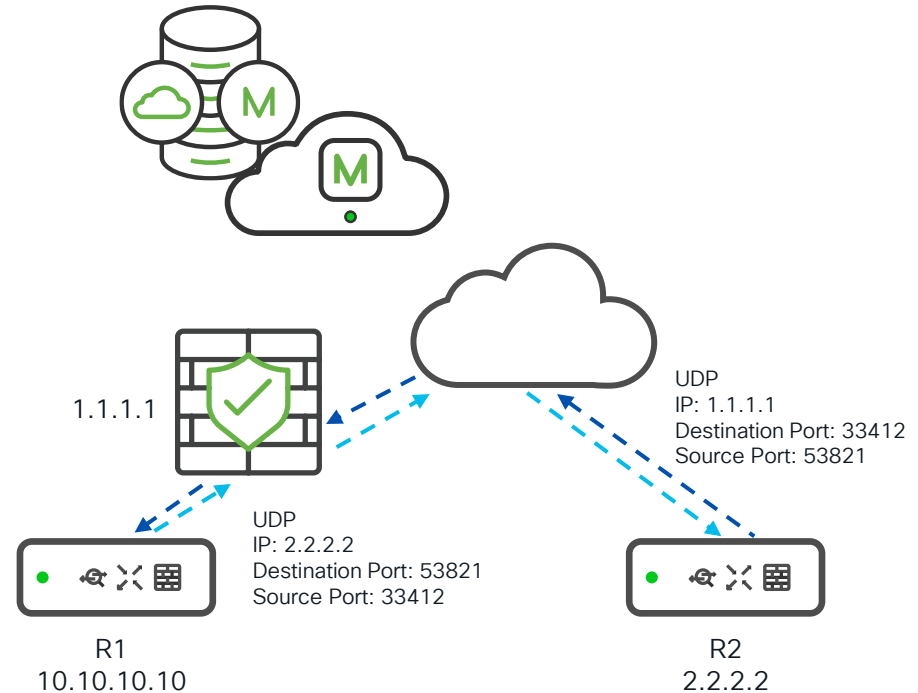
AutoVPN Convergence

Site Connectivity

R1 makes connection to R2
creating a NAT entry upstream

R1 and R2 now have a bidirectional
session

If firewalling is strict upstream,
you can manually specify the port used
for AutoVPN.



Alternative Connectivity Options

Site Connectivity

Cellular

Integrated Cellular

- Supported on MX67C & MX68CW
- Active Cellular Option - Cellular interface takes over WAN2

MG

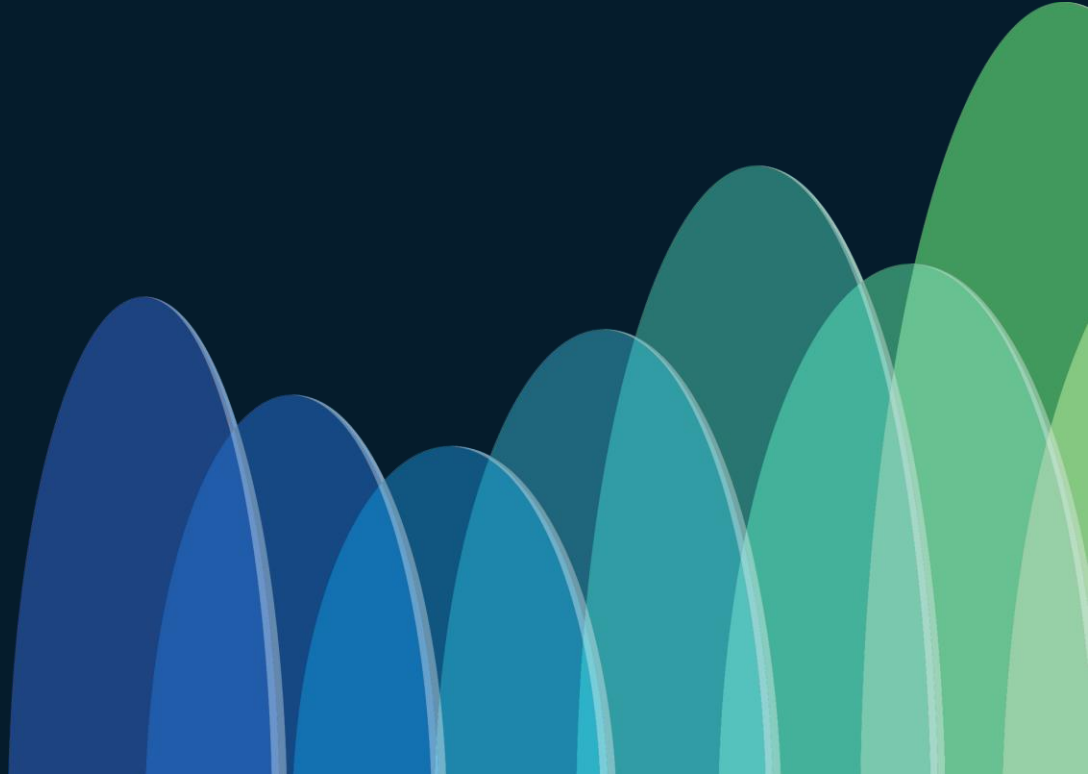
- MG52 - 5G SA Enabled
- IP67 rated
- Internal + External antennas

LEO & Starlink Services

- 18,000+ MX/Z nodes and counting
- 64% of those nodes using Starlink as their only connection



SD-WAN Routing & Policy



Probing

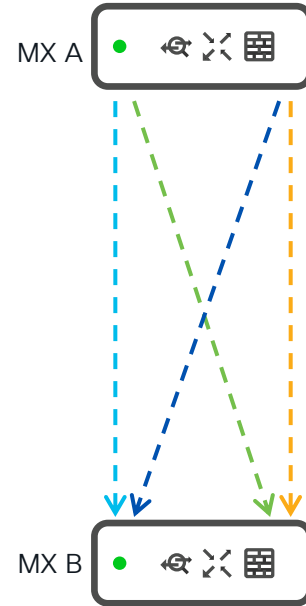
Measuring Performance

Probes are unidirectionally sent over all available transport paths

- MX-A W1 -> MX-B W1
- MX-A W2 -> MX-B W1
- MX-A W1 -> MX-B W2
- MX-A W2 -> MX-B W2

Probes are UDP frames follow Auto VPN transport path for more accurate path sampling

Probe data is <100 bytes, typically 87 bytes of data plus standard 8 byte UDP header



Calculating MOS

Measuring Performance

1 second probing

Under 2500 Auto VPN nodes

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



10 second probing

Over 2500 Auto VPN nodes

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



Performance Classes

Policy

Uplink Selection

Preferred Uplink

WAN 1

Fail over if:

Poor performance

Performance class:

VoIP

VoIP

Default

“Ensure connection is up”

- Also known as connection monitor failover
- If loss >60%, failover to an alternative transport network

Match Performance Class

“Ensure connection is good enough”

- Used when flows are to be 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

Traffic filters

All VoIP & video conferencing

Add +

Policy

Preferred uplink: Best for VoIP

Dynamic Selection

“Ensure we are using the best path”

- 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

Custom Performance Classes

Policy

Custom combination of latency, jitter and loss

Generally mapped to application or service level

Custom performance
classes

Name	Maximum latency (ms)	Maximum jitter (ms)	Maximum loss (%)	Actions
Bronze	200	50	8	×
Silver	150	50	5	×
Gold	100	40	3	×
Platinum	50	20	1	×
0356	60	30	1	×

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

Maximum of 6 configurable in the dashboard

Application Policy

Policy applied either via custom expressions (CIDR / Hostname) or Traffic Analysis engine NBAR2

Uplink selection policy

Traffic filters

Office 365 ✕ Add +

Policy

Preferred uplink: WAN 2 ▼

Fail over if: Poor performance ▼

Performance class: 0356 ▼

Uplink selection policy

Traffic filters

Office 365 ✕ Add +

Policy

Preferred uplink: Load balance ▼

On uplinks that meet performance class: VoIP ▼

Traffic filters

Add +

Health care	All Web file sharing
News	4shared.com
Online backup	download.com
Peer-to-peer (P2P)	Easynews
Productivity	easysshare.com
Remote monitoring & management	filefactory.com
Security	filefront.com
Social web & photo sharing	filer.com
Software & anti-virus updates	filetube.com
Sports	gigeshare.com
Video & music	hotfile.com
VoIP & video conferencing	massmirror.com
Web file sharing	mediafire.com
Web payments	...

Bringing it all together

Policy

Policy will be applied top down,
with a failback to your global
preference.

The same process applies to SD-
Internet traffic.

1 SD-WAN policies

VPN traffic

Uplink selection policy	Traffic filters	Actions
Prefer WAN 2. Fail over if poor performance for VoIP.	All Databases & cloud services	 
Use the uplink that's best for VoIP traffic.	WebEx	 
Add a preference		

2 Uplink selection

Global preferences

Primary uplink WAN 1

WAN failover and
fallback behavior  Graceful

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 or if the primary uplink fails.

VPN Exclusions

Policy

Allow applications to egress DIA at the site.

Applications scoped via NBAR engine or Protocol / CIDR mapping.

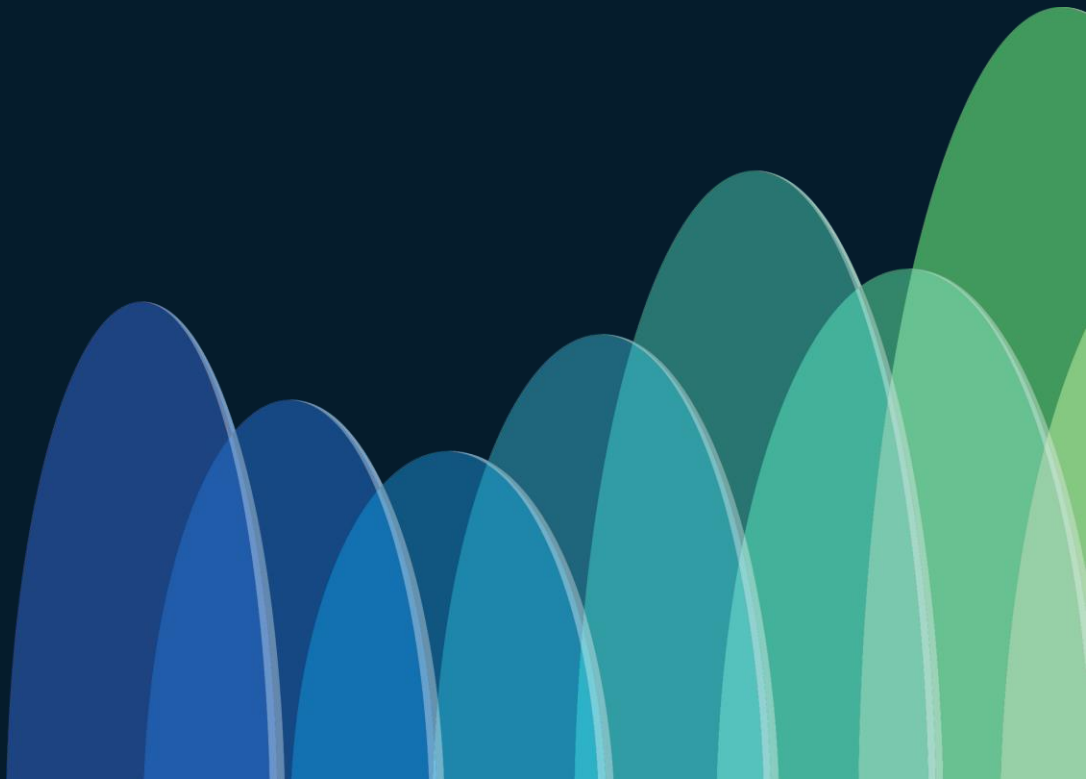
API ready

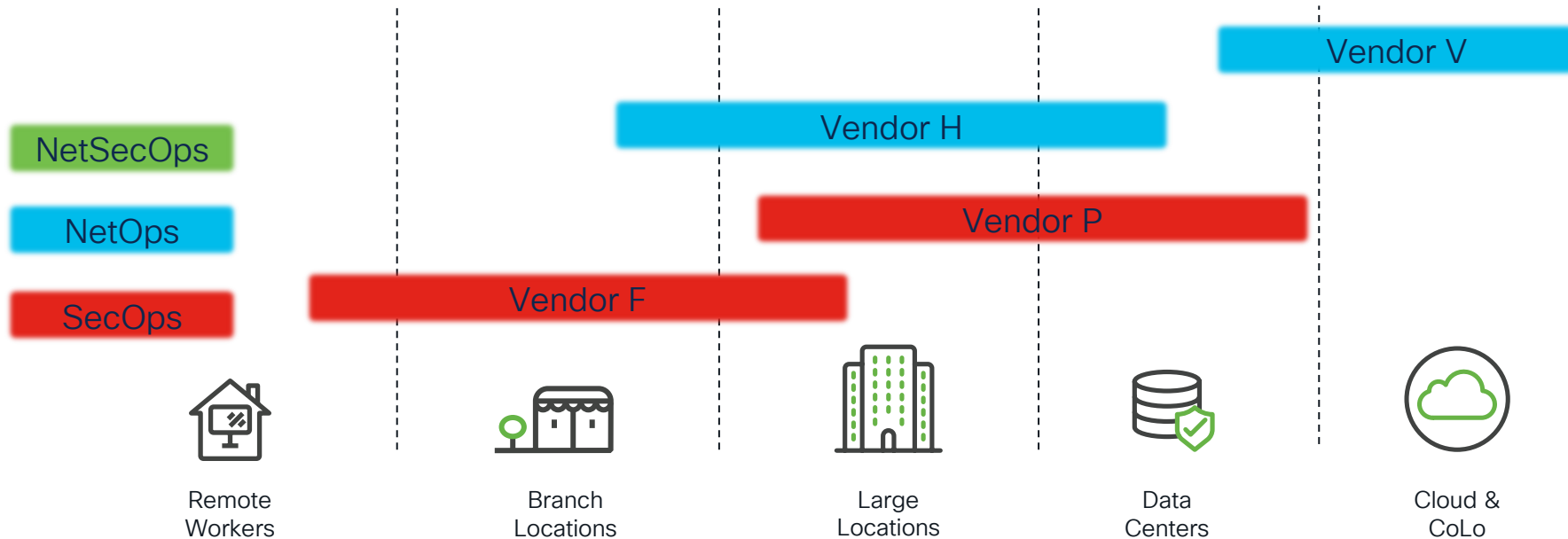
Local internet breakout

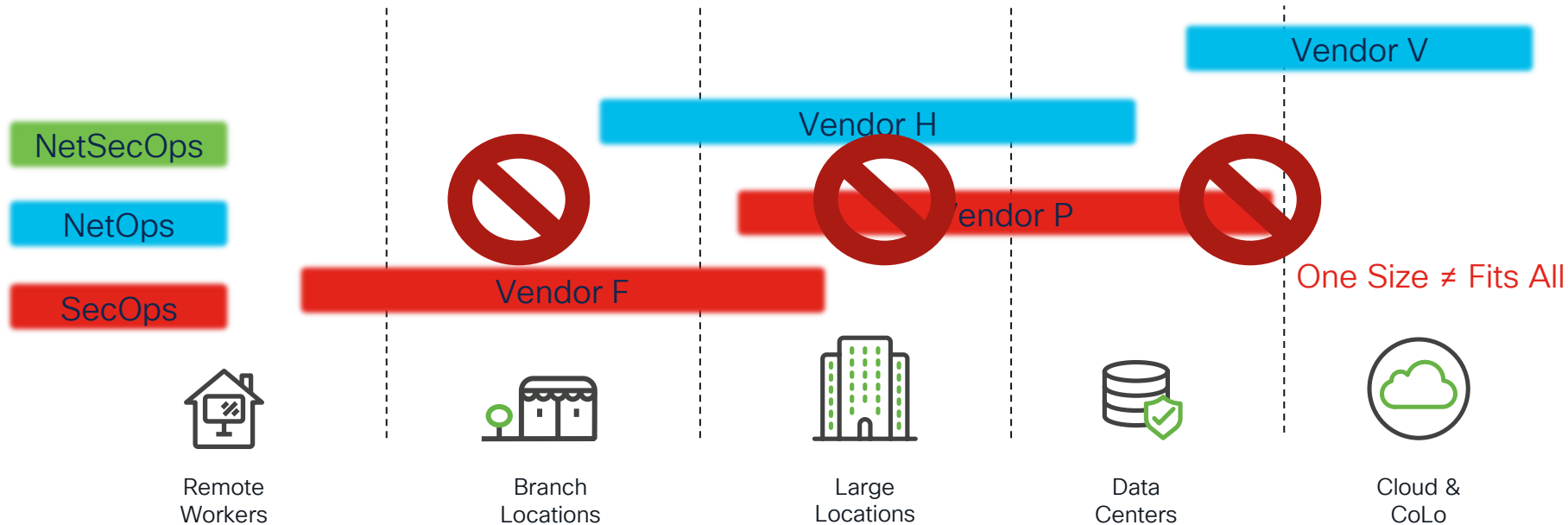
VPN exclusion rules

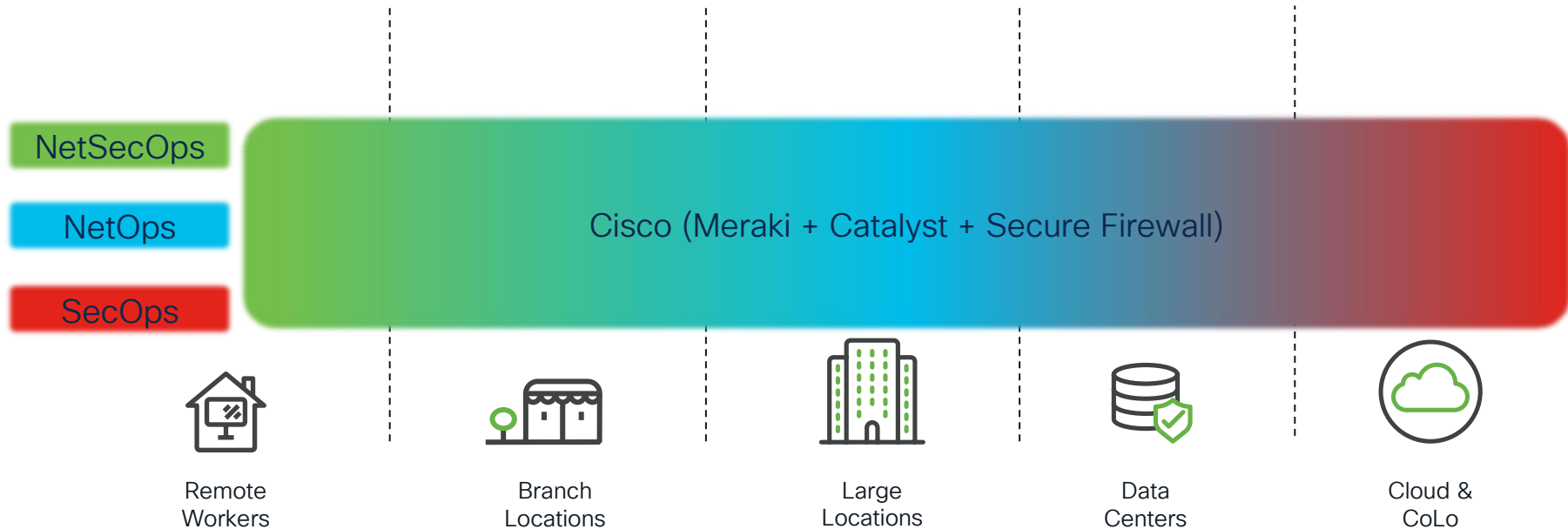
Office 365 Suite ✕		Salesforce ✕		Webex ✕		Add +	
Custom expressions				Custom expressions			
Major applications				Protocol			

SD-WAN Security & Integrations









Meraki and Catalyst SD-WAN Interconnect

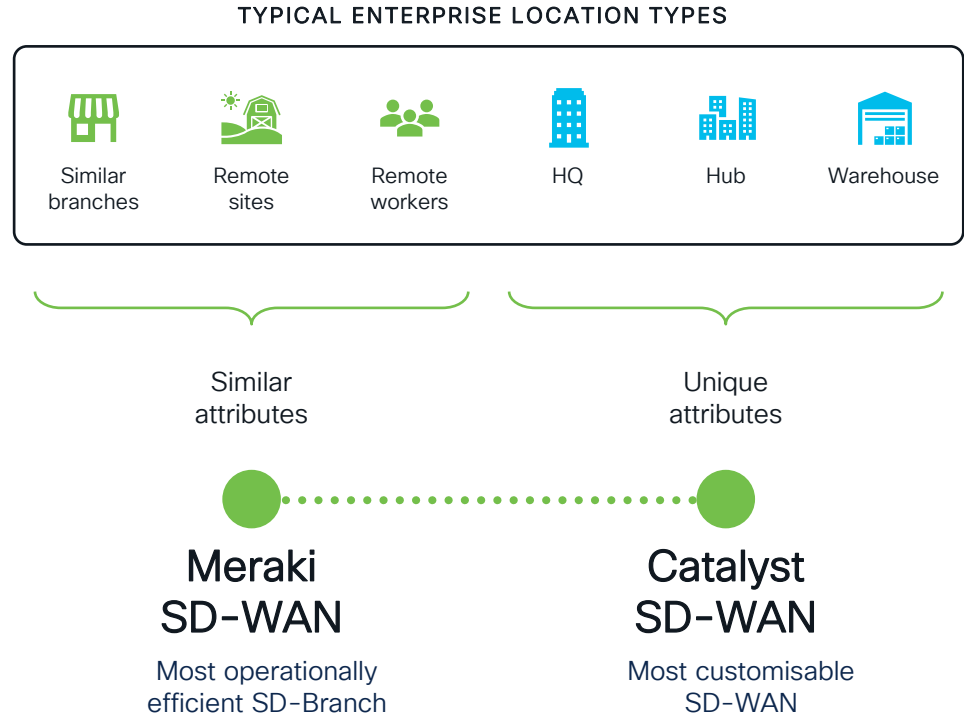
Choose the best fit for every location and streamline management

Fully automated workflow – initiated from the Meraki Dashboard

Bond VPN Fabrics at a collocated site

Available early next year

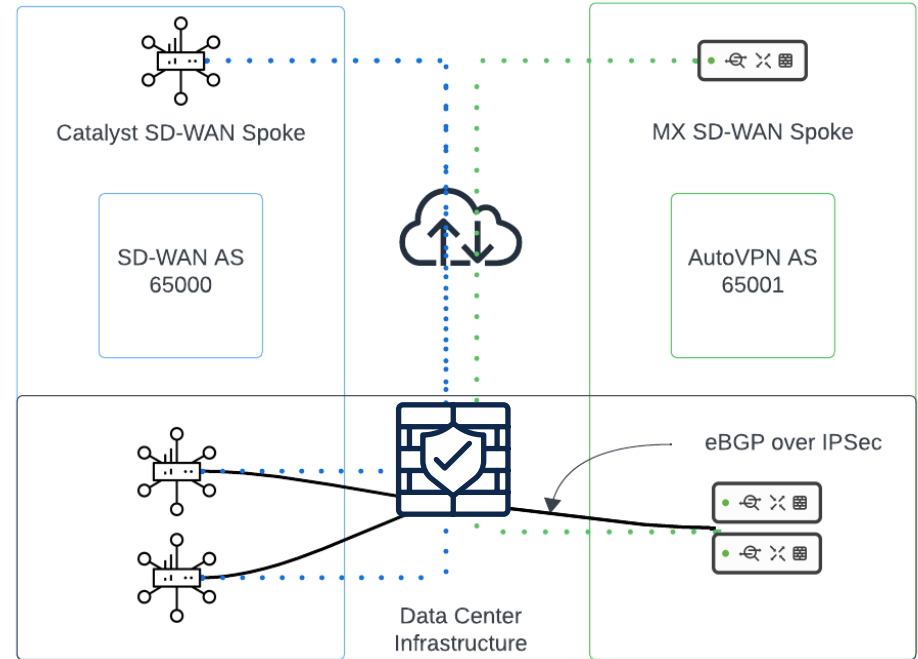
CISCO *Live!*



Design

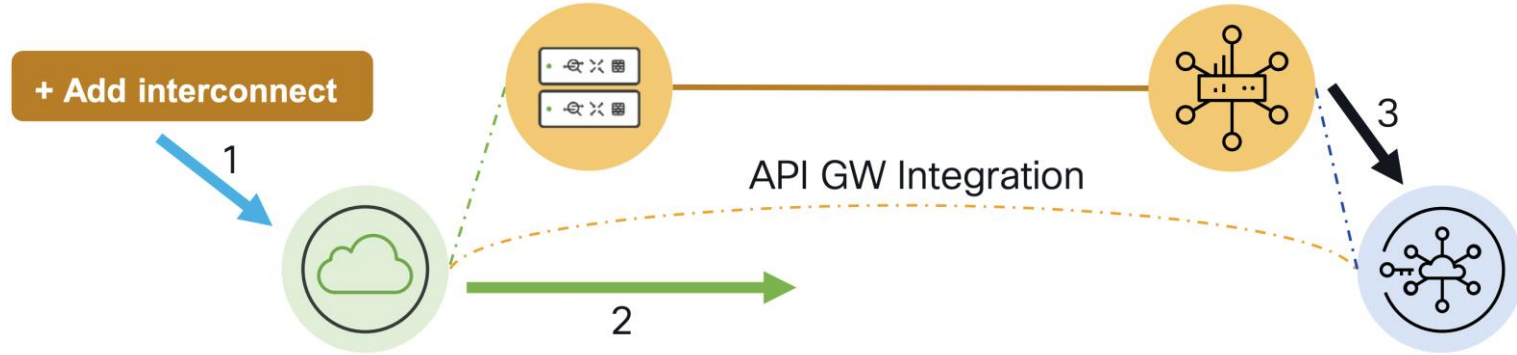
Meraki and Catalyst SD-WAN Interconnect

- Forms up to 2x IPsec tunnels
- eBGP leveraged for route distribution between AutoVPN and SD-WAN VPN Fabrics
- Enabling eBGP on a network will make all MXs participate in iBGP
- Fully redundant at device and protocol levels



Configuration

Meraki and Catalyst SD-WAN Interconnect



1. User adds integration in Meraki dashboard
2. API Requests for Realtime Configuration & Monitoring
3. Real time updates are sent between nodes and clouds

Configuration

Meraki and Catalyst SD-WAN Interconnect

1. Create the interconnect
2. Scope Interconnect
 - Site/Configuration Group
 - VPN
 - Interface
 - ASN
3. Review & Accept Changes

The screenshot shows the 'Add Interconnect' configuration page in the Cisco Meraki dashboard. The page is titled 'Interconnects' and 'Add Interconnect'. It has two steps: '1. Configure interconnect' (active) and '2. Summary'. The 'Configure interconnect' step includes a description: 'Route a VPN from Marketing-Demo to Meraki. Select the Catalyst site and segment, and a Meraki network to configure all necessary tunnels.' The form fields are: 'Name' (Denver Interconnect, 64 character limit), 'Catalyst Site' (DENT0023), 'VPN' (Corporate_Users), 'Ethernet Interface' (VPN0 - Internet), and 'Catalyst BGP ASN' (61002). On the right, the 'Meraki' section shows 'Network' (COLO1 - DEN), 'VPN' (All VPN-enabled subnets), and 'Devices' (DEN SD-WAN Secondary, DEN-Primary MX). A 'Next' button is at the bottom right.

← Interconnects
Add Interconnect

1 Configure interconnect
2 Summary

Configure interconnect
Route a VPN from **Marketing-Demo** to Meraki. Select the Catalyst site and segment, and a Meraki network to configure all necessary tunnels.

Name
Denver Interconnect
64 character limit

Catalyst
Site
DENT0023
VPN
Corporate_Users
Ethernet Interface
VPN0 - Internet
Catalyst BGP ASN
61002

Meraki
Network
COLO1 - DEN
VPN
All VPN-enabled subnets
Devices
DEN SD-WAN Secondary DEN-Primary MX

Cancel Next

Configuration

Meraki and Catalyst SD-WAN Interconnect

Meraki

- Create IPsec Tunnels
- Add BGP Neighbours
- Apply Policy
 - Primary routes
 - AS Path, Weight 20
 - Secondary Routes
 - AS Path Prepended x2, Weight 10

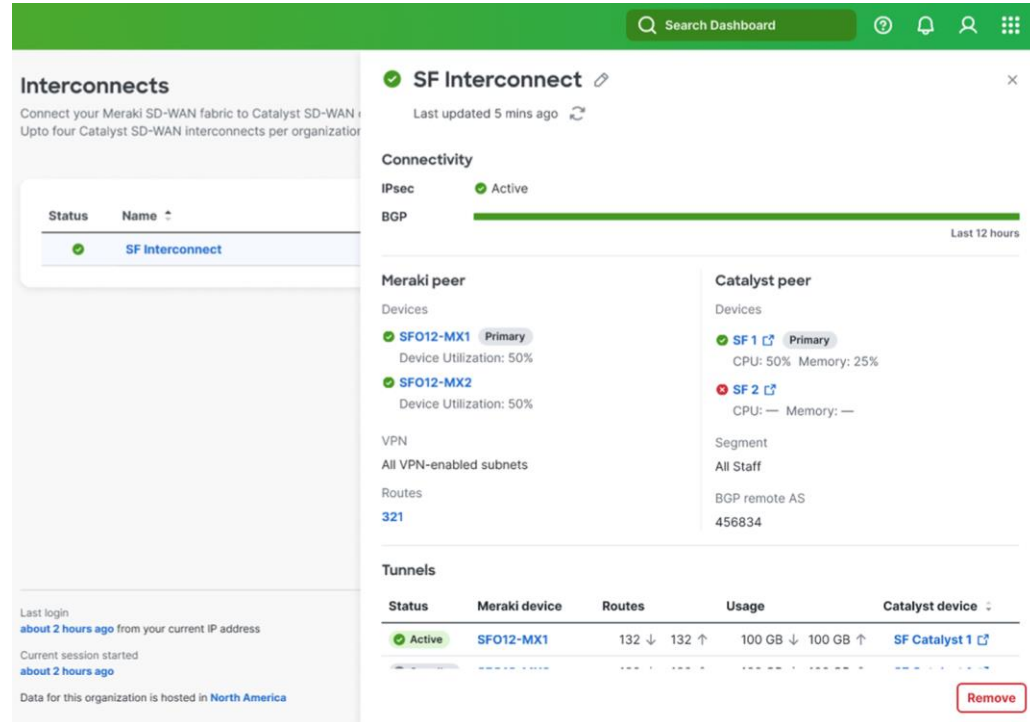
Catalyst

- Create Service VPN Tunnels
- Add BGP Neighbours
- Apply Policy
 - Redistribute OMP, Connected, propagate-
aspath
 - OMP
 - AS_Path -> OMP Preference enabled

Interconnect Monitoring

Meraki and Catalyst SD-WAN Interconnect

- Interconnect Health
- eBGP Router statistics
- IPsec VPN statistics
- Device health statistics
- Deep linking into the Catalyst SDWAN Manager



BGP Monitoring

Meraki and Catalyst SD-WAN Interconnect

Dynamic Protocol Status Page

- BGP Neighbour state
- Learned route count
- Historical State

Route Table

- Live information
- BGP information via tooltip
- Filtering
- IPv6 Support

The screenshot displays two pages from the Cisco Meraki management interface. The top page, 'Dynamic Protocol Status', shows the status of BGP peers. It has two summary boxes: 'IBGP peers 7 total' with 7 'Alerting' status, and 'eBGP peers 2 total' with 1 'Alerting' status. Below these is a table titled 'BGP Peers' with columns for Peer status, Peer, AS number, Peer type, # Routes, and Status changes. The table shows two entries: one 'Established' peer (10.0.0.2/32, AS 65476, eBGP, 25 routes) and one 'Idle' peer (10.0.0.6/32, AS 65477, eBGP, 0 routes). The bottom page, 'Route table', shows a table of routes. A tooltip is visible for the route 10.10.10.0/24, showing details like Type (Internal BGP), Name (Internal), IP Version (4), Subnet (10.10.10.0/24), Protocol (IBGP), AS Path, Origin (I), Local Pref (100), Next Hop (MEL), and Connectivity (green bar).

Dynamic Protocol Status Last 2 hours

IBGP peers 7 total
7 Alerting

eBGP peers 2 total
1 Alerting

BGP Peers

Search Peer status eBGP 2 matching results

Peer status	Peer	AS number	Peer type	# Routes	Status changes
Established	10.0.0.2/32	65476	eBGP	25	
Idle	10.0.0.6/32	65477	eBGP	0	

Rows per page 10 < 1 >

Route table Rebuild

Routes updated as of Today at 8:25 PM.

IP VERSION SUBNET/PREFIX NAME VLAN NEXT HOP DESTINATION TYPE REPORTED

All Search by subnet/prefix Search by name Search by VLAN ID Search by network Search by destination Internal BGP Current

Stat	Version	Subnet	Name	VLAN	Next hop	Destination	Type
10		10.10.10.0/24	Internal	—	MEL	MEL	Internal BGP

10

Type Internal BGP
Name Internal
IP Version 4
Subnet 10.10.10.0/24
Protocol IBGP
AS Path
Origin I
Local Pref 100
Next Hop MEL
Connectivity

BGP over IPsec

IPsec Improvements

- Locally significant attributes
 - Weight
- Remote Peer significant attributes
 - AS Path Prepend
 - MED

Edit VPN Peer

Routing

☐ Static

☒ Dynamic (BGP)

Network ⓘ

BGP over IPsec is only supported on networks with firmware version 19.1 and higher

IPsec subnet

IPsec subnet must use a /30 subnet mask

BGP source IP

BGP source IP must fall within the same /30 subnet range

BGP neighbor IP

BGP neighbor IP must fall within the same /30 subnet range

Remote AS

Weight (optional) ⓘ

Path prepending (optional) ⓘ

Enter a space-separated list for each AS

MED (optional) ⓘ

Multihop

sec

Hold timer

sec

Secondary Tunnels

IPsec Improvements

Operates in an Active / Standby configuration

Three click provisioning

FQDN support

Primary

 Edit primary peer

 Move to

 Delete primary peer

Secondary

 Add secondary peer

Add Secondary VPN Peer ×

[Inherit primary peer configurations](#) ⓘ

Private subnets ⓘ

192.168.0.0/24

Availability ⓘ

All Networks

Tunnel monitoring

Health check

MyApplication ⓘ ▾

Failover directly to internet ⓘ

☐ Enable failover

IPsec Monitoring

IPsec Improvements

Event Logging

Per peer IPsec negotiation logging

VPN Status Page

IKE Status

- Red – IKE Phase 1 down & phase 2 down
- Amber – IKE Phase 1 up & phase 2 down
- Green – IKE Phase 1 up & phase 2 up

Time (PDT) ▼	Client	Category	Event type	Details
Apr 7 16:56:19		Non-Meraki VPN	Non-Meraki VPN negotiation	msg: <remote-peer-2 1301> c
Apr 7 16:56:19		Non-Meraki VPN	Non-Meraki VPN negotiation	msg: <remote-peer-2 1301> c
Apr 7 16:56:19		Non-Meraki VPN	Non-Meraki VPN negotiation	msg: <remote-peer-2 1302> c
Apr 7 16:56:19		Non-Meraki VPN	Non-Meraki VPN negotiation	msg: <remote-peer-2 1302> I

1 site-to-site peer

4 exported subnets

2 Non-Meraki peers

Status ▲	Name	Public IP	Subnets	+
	MySSE	1.1.1.1	10.10.10.0/24	
	MySSE Secondary	1.1.1.2	10.10.10.0/24	
2 total				

Tunnel Monitoring & Failover

IPsec Improvements

- HTTP probes track layer 3 and layer 7 connectivity
- Probes sent every 10 seconds
- Failover in the event of tunnel down or health check probe fail
 - Up - 1xx, 2xx or 3xx status code to GET request
 - Down - ICMP unreachable, TCP reset, HTTP 4xx/5xx code or timed out after 10 seconds.

Non-Meraki VPN peers ⓘ

36 results [Configure health check](#) [+ Add peer](#)

☐	#	Name	Public IP or Hostname	Local ID	Availability ⓘ	ⓘ
--------------------------	---	------	-----------------------	----------	----------------	---

Configure health checks

Configure your health checks to use for tunnel health. Health check will use this IP for probing when the MX is in passthrough mode. Only one health check per tunnel can be used.

[+ Add health check](#)

Health check	Endpoint	
<input type="text" value="MyApplication"/>	<input type="text" value="http://my.app"/>	Cancel Done

Rows per page [<](#) [1](#) [>](#)

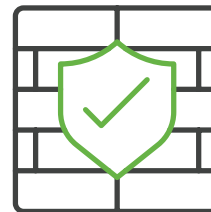
[Cancel](#) [Done](#)



2.1M+
MX and Z Devices Online



16+ Trillion
Flows secured per month



25B+
Security threats blocked per month



75M+
Endpoints securely connected
every day



400,000+
Remote access VPN users
connected per day



2B+
MX API calls per month for
high scale automation

Advanced Security on MX

Security

Next Gen Firewall



IDS/IPS

Content Filtering

Advanced Malware Protection
(AMP)

Cisco Secure Malware Analytics
(Threat Grid)

DNS Layer Protection
(Cisco Umbrella)



Advanced Security now on vMX

Secure east-west - site to site traffic

Secure north-south - internet bound traffic.



TALOS

Enterprise Firewall

IDS / IPS

Content Filtering

Adv. Malware Protection (AMP)

SNOC

Security & Network Operations Center

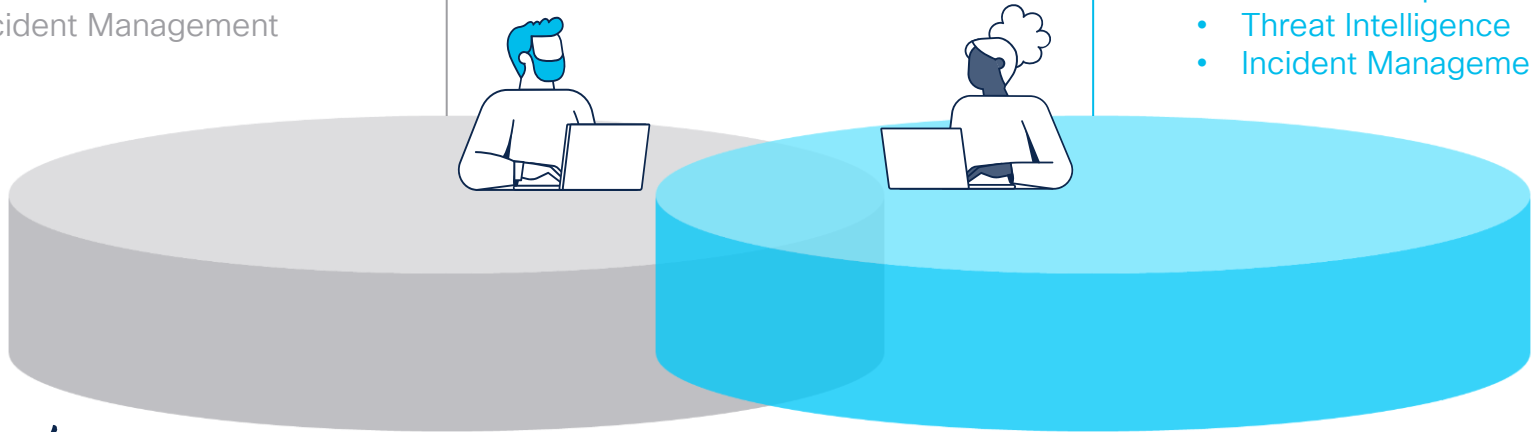
Real-time monitoring, response and reporting of Network & Security Events

Network Operations Center

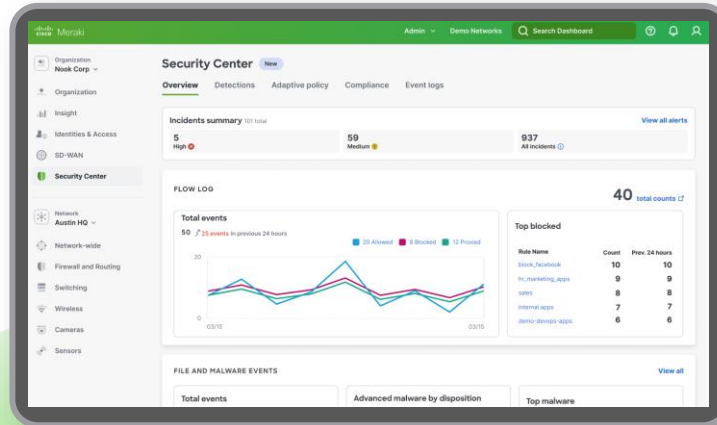
- Network Visibility
- Network Configuration
- Minimise Downtime
- Incident Management

Security Operations Center

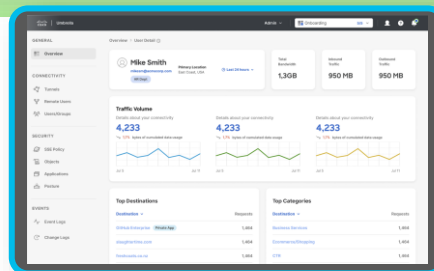
- Threat Monitoring & Detection
- Incident Response
- Threat Intelligence
- Incident Management



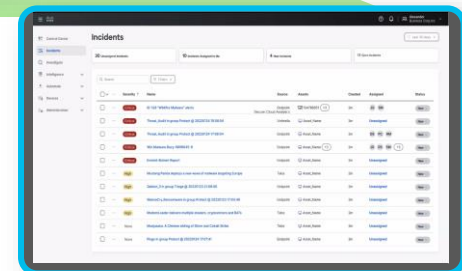
Enabling the SNOOC



ThousandEyes



Umbrella/Secure Access



XDR

XDR Integration

Security

Contextual Threat and Behavioural Analytics using Netflow data

XDR uses AI/ML to analyse network data and detect malicious behaviour or early indicators of compromise

Button-click integration to send telemetry from all your MX devices to XDR.

Contextually aware incidents are brought into the Meraki dashboard, can triage from here.

The screenshot displays the Cisco Meraki Security Center interface. At the top, there's a green header with a search bar and user icons. Below the header, the 'Security Center' section is active, showing a summary of incidents: 44 total, 5 new, and 22 open. A table lists various incidents with columns for Priority, Name, Source, Created, and Assignment. The incident 'A malicious SHA-256 targeted an endpoint' is highlighted. A detailed view of this incident is shown on the right, including its priority score breakdown (978 total, 97 Detection Risk, 10 Asset Value at Risk), short and long descriptions, attack chain, source IP (173.31.100.120), and a list of matching malicious process hashes. A 'View incident in XDR' button is visible at the bottom right of the incident details.

Priority	Name	Source	Created	Assignment
1000	Ransomware Detection	SCA	3 days	Unassigned
978	A malicious SHA-256 targeted an endpoint	SCA	4 days	Unassigned
875	Suspicious Web Access	Meraki API	9 hours	Unassigned
832	Authentication Bypass Attempt	Meraki API	11 hours	Unassigned
800	Lateral Movement	Meraki API	3 days	Unassigned
784	New Remote Access on 172.31.100.120	SCA	3 days	Unassigned
711	MITRE: Incident TA0009	SCA	3 days	Unassigned
691	LDAP Connection from Suspicious Process	SCA	3 days	Unassigned
691	Log4Shell	SCA	3 days	Unassigned
620	Suspicious Web Access	SCA	3 days	Unassigned

XDR Configuration

Security

1. Authenticate
2. Scope Networks
3. Deploy

Networks

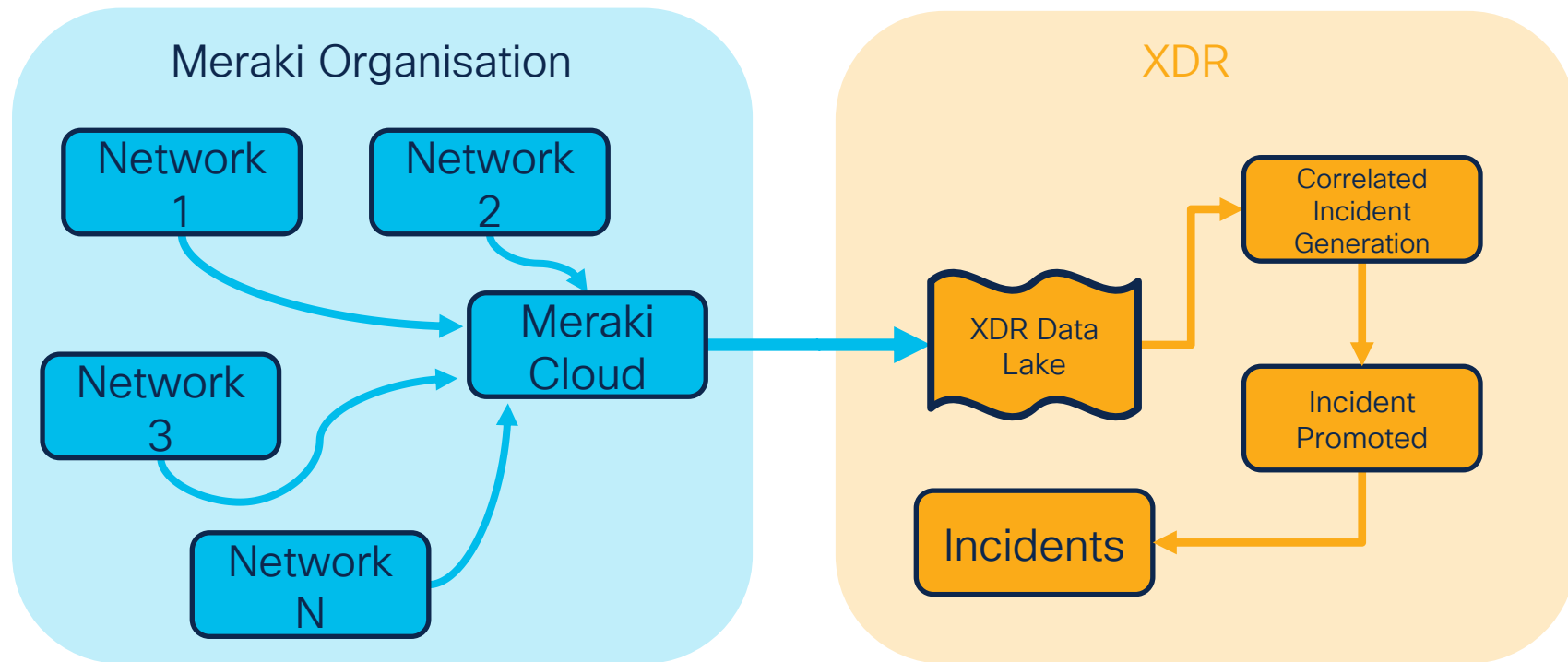
Filters 3 networks Disable Enable

☐	Network	XDR status	Tags	XDR eligibility	Model	Firmware	License compliant
☐	Site 1	✓ Enabled		✓ Eligible	MX68	MX 19.1.4	✓ Compliant

Rows per page < >

XDR Packet flow

Security



Secure Connect – Hybrid Hub Design

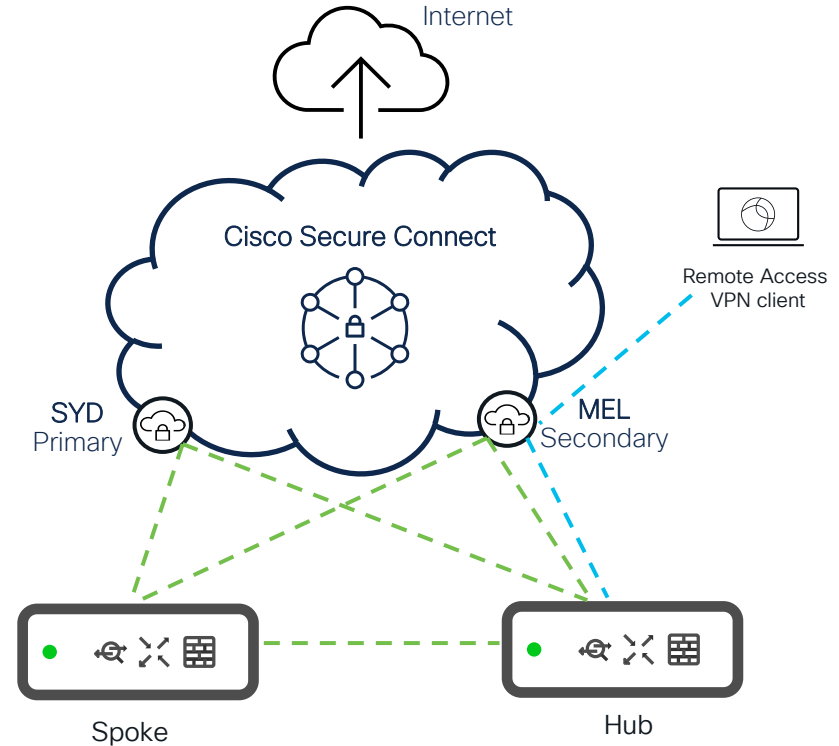
Security

Everything peers with Secure Connect cloud

Supports Meraki Hub & Spoke East / West

More specific routes are advertised, other traffic default routed to Secure Connect

Optimises Secure Connect fabric consumption



Secure Connect – Configuration

Security

1. Authenticate
2. Scope networks
3. Select region
4. Deploy

Automatic peering with predefined primary and secondary DC pairs

Failover handled by the Meraki SD-WAN fabric

The screenshot displays the 'Sites' configuration page in the Cisco Meraki dashboard. The page title is 'Sites' with a sub-header 'Last 2 hours'. Below the title is a search bar. The main content is a table listing sites with columns for Site name, Region / Cloud Hub, Site Features, and Connectivity. The 'Los Angeles hub 144' is highlighted in blue. To the right of the table, there is a sidebar with details for the 'Los Angeles hub 144', including MX devices, local networks, remote routes, and security events.

Site name	Region / Cloud Hub	Site Features	Connectivity
☐ Perth branch 105 - appliance	Australia-1 Region	Meraki network Spoke	<div></div>
☐ Raleigh apps 107	US Northeast Region	Meraki network Spoke	<div></div>
☐ Montreal branch 131	Canada-1 Region	Meraki network Spoke	<div></div>
☐ Paris branch 132	Europe-2 Region	Meraki network Spoke	<div></div>
☐ Tokyo branch 103	Asia-1 Region	Meraki network Spoke	<div></div>
☐ Los Angeles hub 144	US West Region	Meraki network Hub	<div></div>
☐ _San Francisco branch 104 - appliance	US West Region	Meraki network Spoke	<div></div>
☐ Dallas branch 106	US Central Region	Meraki network Spoke	<div></div>
☐ San Francisco Lab	US West Region	Meraki network Spoke	<div></div>

Los Angeles hub 144

MX devices

Device	Model
08:f1:b3:db:22:4e	MX75-HW

[Full details in Meraki Appliance Status ->](#)

Local networks

Local networks announced to Secure Connect

10.144.0.0/24

[Enable or disable Meraki network subnets ->](#)

Remote routes

Route settings for this Meraki Hub in relation to Secure Connect

Default Route: [Disabled](#)

Region

The Secure Connect region where traffic enters and exits. Regions can be changed per tunnel

US West Healthy

Security Events

Security events in the last 2 hours

Total: 0

[View DNS and CDFW events in Umbrella <](#)

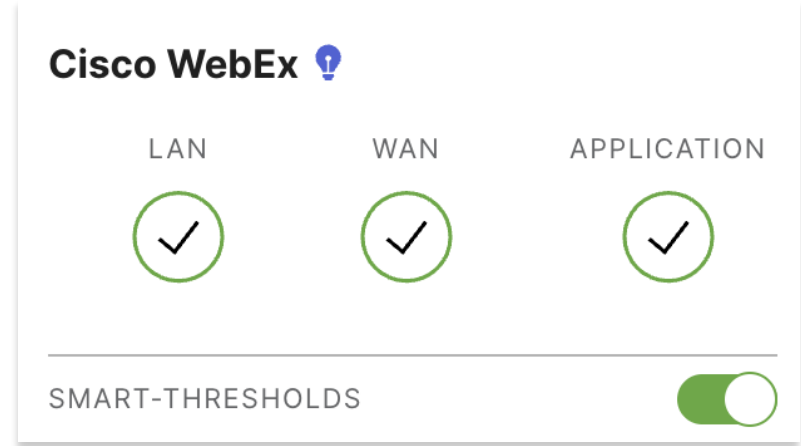
Thousand Eyes enriched Web App Health

Monitoring & Troubleshooting

End-to-end visibility from branch to cloud

Clear demarcation points between LAN / WAN / Transit & Applications

Automatically configured synthetic testing with smart thresholding.



Thousand Eyes enriched Web App Health

Monitoring & Troubleshooting

Configuration is clicks

- Authenticate
- Select Apps
- Confirm sub domains
- Scope networks
- Go!

Monitor Critical Applications for SD-WAN [Configuration Guide](#)

✓ Connect ThousandEyes
ThousandEyes authorized

2 Select application

3 Configure monitoring

4 Select networks

5 Summary

Select application

Choose an application to monitor with enhanced application monitoring.

 Office 365 Suite

 Office 365 Sharepoint

 Cisco WebEx

 Zoom

 Box

 Salesforce

 Amazon Web Services

 Add a custom application

Don't want to set up an application right now?

Continue without an application

Cancel

Back Next

Thousand Eyes enriched Web App Health

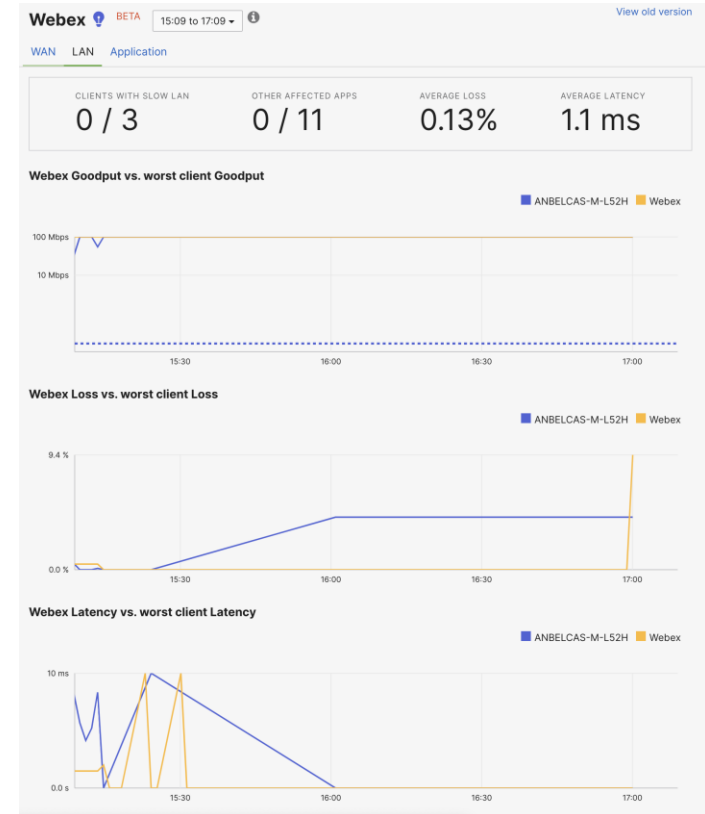
Monitoring & Troubleshooting

WAN

- Application goodput vs uplink
- Application loss vs uplink
- Application latency vs uplink
- Server specific loss / latency
- Uplink specific loss latency

LAN

- Application goodput vs worst client
- Application loss vs worst client
- Application latency vs worst client
- Client Loss / Latency

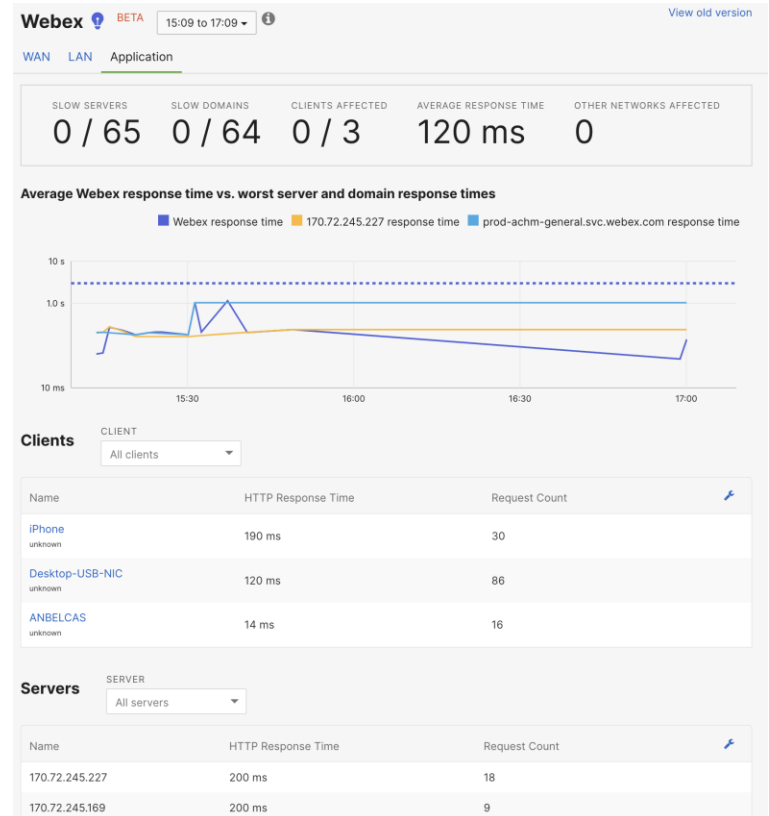


Thousand Eyes enriched Web App Health

Monitoring & Troubleshooting

Application - Response time tracking

- Client
- Server
- Domain

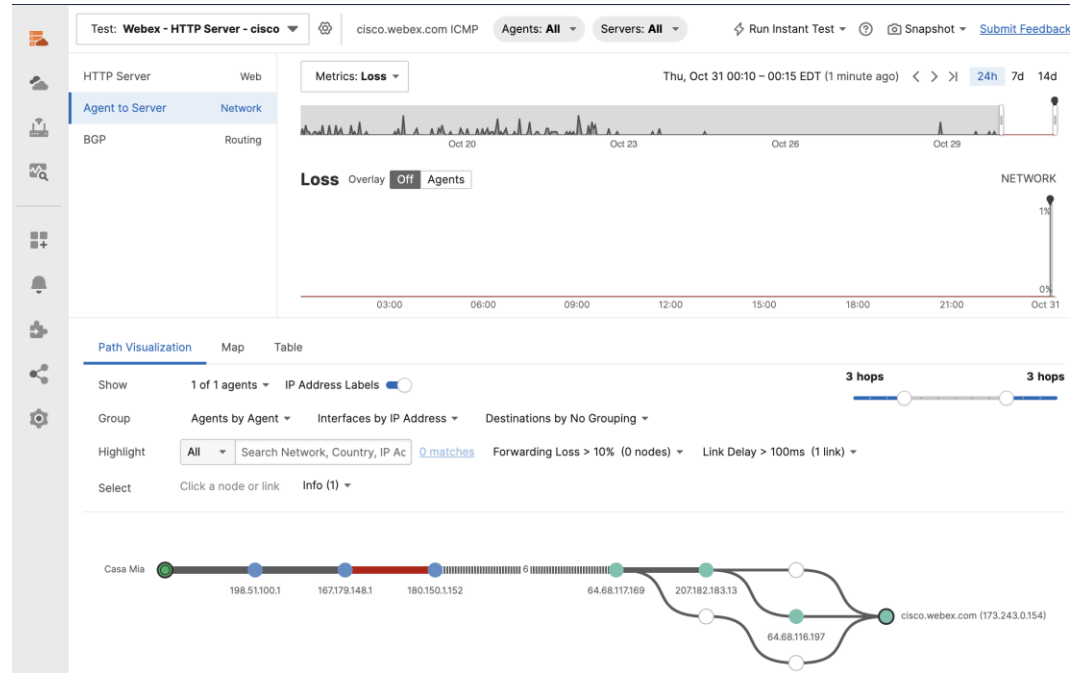


Thousand Eyes enriched Web App Health

Monitoring & Troubleshooting

Still not enough?

Contextual deep handoff



Hitless Updates

Security

Updates to core services are pushed and digested independent of firmware

For new threats, TALOS have a 3.5 average hour time to detect versus the industry average of over 100 days.

Uplink configuration

List update interval ⓘ

WAN 1 Hourly ▾

WAN 2 Hourly ▾ [simple](#)

Cellular Weekly ▾

Event log for security appliances ▾

Client:

Before: (AEDT)

Event type include:

Event type ignore:

[Reset filters](#)

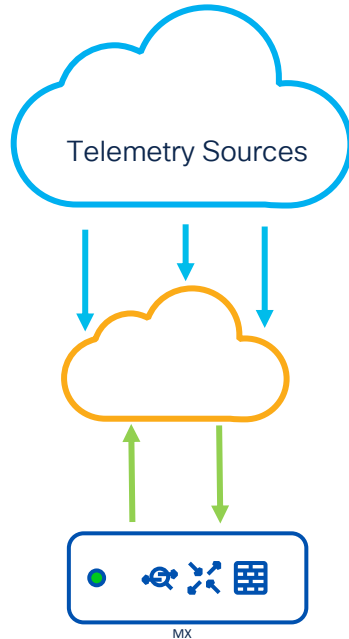
Download as ▾

[« newer](#) [older »](#)

Time (AEDT) ▾	Client	Category	Event type	Details
Oct 30 21:13:50		Intrusion Detection	Intrusion detection rules update	snort_rules_version: 20241028-1735
Oct 25 20:54:29		Intrusion Detection	Intrusion detection rules update	snort_rules_version: 20241023-2032
Oct 23 22:01:44		Intrusion Detection	Intrusion detection rules update	snort_rules_version: 20241021-2004
Oct 21 11:05:32		Intrusion Detection	Intrusion detection rules update	snort_rules_version: 20241016-1834
Oct 18 21:23:37		Intrusion Detection	Intrusion detection rules update	snort_rules_version: 20241016-1834
Oct 18 15:16:20		Intrusion Detection	Intrusion detection rules update	snort_rules_version: 20241014-1855
Oct 18 11:17:34		Intrusion Detection	Intrusion detection rules update	snort_rules_version: 20241014-1855

SD-AVC Integration for NBAR

Security



IP Feeds

Domain Feeds

Cloud Feeds

Dynamic Feeds

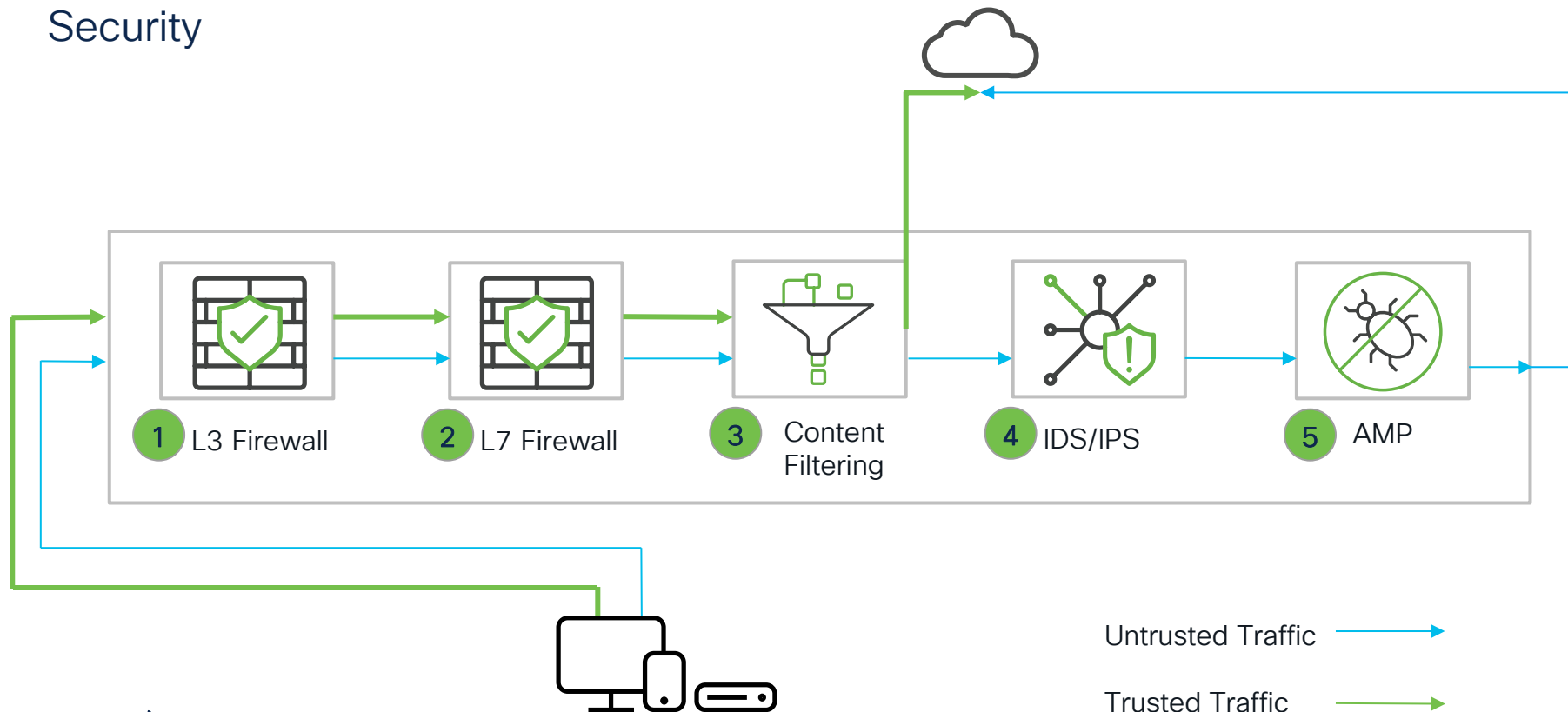
Custom Regex Feeds

Up to 90%+ first packet classification with additional telemetry sources!

- Amazon Chime
- Atlassian
- Box
- Cisco Meraki
- Code42
- Crashplan
- Dropbox
- Github
- Google Meet
- HubSpot
- Intuit
- Microsoft Intune
- MS Office 365
- RingCentral
- Salesforce
- SAP
- ServiceNow
- SugarCRM
- Telegram
- Webex
- Whatsapp
- Workday
- Zoho
- Zoom
- Zscaler
- CASI Umbrella Top 1 Million
- AWS
- Azure
- GCP
- SSL Crawler
- WHOIS
- rDNS
- Internet registry DB

Trusted Traffic Exclusions (TTE)

Security



Trusted Traffic Exclusions (TTE)

Security

- Each later of security function has a computation cost associated with it
- Each packet needs to be inspected
- For traffic that is not important we can skip the security checks and egress the WAN
- Top applications / Subnet support

Trusted Traffic Exclusions

To increase network performance, select traffic categories and IP addresses or subnets to bypass when AMP or IDS/IPS is enabled.

Trusted Applications ⓘ

☒ Streaming & entertainment Amazon Video, Google Services, Hulu, Netflix, Pandora Radio, PL... View all	☒ Software updates Adobe Updates, Apple Updates, Google Updates, Microsoft Upd... View all
☒ Collaboration Cisco Collaboration, MS Teams, RTP, SCCP, SIP, Skinny Call Con... View all	☒ Online storage Box, Dropbox, Google Workspace, Microsoft OneDrive, iCloud View all
☒ Business critical applications AWS, Atlassian, Azure, Concur, Google Workspace, Jira, LogMeI... View all	

Trusted IP Addresses/Subnets ⓘ

Address	Comments
<input type="text" value="10.0.0.0/24"/>	<input type="text" value="Lab"/>
+ Add IP address	

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand 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



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC