Exploring Security & SD-WAN with Meraki MX
Cisco Meraki Cloud Networking Series

Speaker: Tony Carmichael
Hostess: Kara Sullivan | Cisco Networking Academy
11 October 2017
Welcome to the 4th session of the Cisco Meraki Cloud Networking webinar series

- Use the Q and A panel to ask questions.
- Use the Chat panel to communicate with attendees and panelists.
- A link to a recording of the session will be sent to all registered attendees.
- Please take the feedback survey at the end of the webinar.
Cisco Meraki Cloud Networking Series

PREVIOUS SESSIONS:

• Intro to Cloud Networking using Meraki
• Exploring Meraki Cloud Switching & Wireless
• Exploring Meraki Cloud Telephony & Vision

Intro to Cybersecurity Self-Enroll Course

Introduction to Cybersecurity
Learn how to protect yourself online and in social media while discovering careers in cybersecurity.

Enroll Now

You can enroll today to learn more @ http://bit.ly/Intro2Cyber
Exploring Security and SD-WAN with Meraki MX

Simple, effective security and WAN Management
Agenda

Welcome & Introduction
Why choose Meraki?
Product demo
Product families
Careers at Meraki
Q&A
About the Cisco Meraki MX
Simplifying IT with cloud management

A complete cloud managed IT solution
Wireless, switching, security, SD-WAN, communications, EMM, and security cameras
Integrated hardware, software, and cloud services

Leader in cloud managed IT
Among Cisco’s fastest growing portfolios
Over 140,000 unique customers
Over 2 million Meraki network devices online
Benefits of a cloud managed solution

- Security
- Reliability
- Scalability
- Future-proofing
A complete connectivity and threat management solution

**Security**
- Next generation firewall
- AES encrypted VPN
- Intrusion prevention (IPS)
- Malware protection
- Geo-IP firewalling

**Networking**
- 3G / 4G failover
- Branch routing
- WAN balancing and failover
- High Availability
- Intelligent path control

**Application Control**
- Bandwidth shaping
- URL content filtering
- Quality of Service control
Why customers choose the Cisco Meraki MX

Powerful security that’s easy to implement
- Robust suite of Cisco Security technologies
- Intuitive GUI-based configuration
- Seamless updates from the cloud

Exceptional scalability
- Zero-touch provisioning with cloud brokered VPN
- Easy centralized management with built-in remote troubleshooting tools
- Multi-location configuration templates

Industry-leading visibility
- Fingerprint users, applications, devices, and threats
- Monitor one location or an entire deployment
- Unified monitoring and reporting with other Cisco Meraki technologies
Security made simple
Ironclad security

Next Generation Firewall  Application aware firewallsing

Intrusion Prevention (IPS)  Based on Cisco Snort

URL Content Filtering  With over 80 categories and over 4 billion categorized URLs

Geo-based security  Allow or block traffic by country

Malware Protection  Cisco AMP and Threat Grid

Automatic updates  Software and security updates delivered from the cloud

PCI compliance  PCI 3.2 certified cloud management backend
Backed by Cisco Talos threat intelligence

- 1.5 million malware samples / day
- 600 billion email messages / day
- 16 billion web requests / day
- Internet-wide scanning
- Telemetry
- Honeypots
- Open source communities
- Internal vulnerability discovery

- Over 250 full time threat researchers
- Millions of telemetry agents
- 4 global data centers
- Over 100 threat intelligence partners
- Over 1100 threat traps

Over 250 full time threat researchers
Millions of telemetry agents
4 global data centers
Over 100 threat intelligence partners
Over 1100 threat traps
Advanced Malware Protection for Meraki MX

Enhanced Threat Defense
Automatic protection against an ever-growing list of known malicious files, plus malware sandboxing with Threat Grid

Contextual Visibility
Security Center makes it easy to ensure you have the latest information about attacks on your network

Rapid Detection
Automatic alerting when a downloaded file is found to be malicious after the fact

Ease of Management
Enable best-in-class malware protection with just two clicks

- 220 million known malicious files
- 407 million known clean files
- 1.5 million new incoming malware samples per day
- 1.6 million devices using AMP globally
- 3.1 billion lookup requests per day
How does it work?
Connectivity and SD-WAN
Reliable, cost effective connectivity with Meraki SD-WAN

Dual uplink ports
2 uplink support on all MX models for load balancing and redundancy

LTE failover
USB modem support in all models with automatic failover

Site to site VPN
Cloud orchestrated VPN (Meraki Auto VPN) with load balancing and self-healing capabilities

Intelligent path control
Policy based routing and performance based dynamic path selection

Branch Routing
Automatic route distribution via Auto VPN
OSPF route advertisement
BGP support coming soon

High Availability
Active/passive hardware redundancy

Traffic shaping
Application bandwidth limiting and prioritization
Connections that fit your business and location needs

- **Broadband + MPLS**
  - Data Center
  - ISP A
  - Auto VPN
  - Broadband
  - MPLS
  - Branch

- **Broadband + 4G**
  - Data Center
  - ISP A
  - Auto VPN
  - Broadband
  - LTE
  - Branch

- **Dual Broadband**
  - Data Center
  - ISP A (DSL)
  - ISP C (Cable)
  - Auto VPN
  - Broadband
  - Branch
Automated site-to-site VPN (Auto VPN)

Simple
Create VPN tunnels between locations with easy point-and-click interface, or apply configuration templates to enable and configure VPN at many locations at once.

Automatic
VPN configuration generated and deployed automatically from the cloud – create a mesh or hub-and-spoke topology with only a few clicks.

Resilient
Automatically adjusts to changes in order to maintain secure connectivity during an ISP or datacenter outage, hardware failure, or IP address update.
Application-aware intelligent path control

**Dual active VPN**
Load balance your VPN traffic over your hybrid WAN

**Policy based routing**
Select the preferred path for traffic based on protocol, port, source and destination IP, or even application

**Dynamic Path Selection**
Select the best VPN tunnel for traffic automatically based on performance

The only solution to combine cutting edge SD-WAN with industry leading security technology
In-depth visibility
Traffic monitoring and analytics

- View bandwidth usage by application or by client
- Highlight an application or a client to see their portion of total network bandwidth
- See a client’s active time for specific applications
- Easily create policies to limit bandwidth for problematic users or applications
URL logging

- See complete web browsing history
- Smart search to find the specific information you need
- Active Directory integration for user identification
- See data for one location or across all locations
- Export log data for aggregation if needed
VPN health, bandwidth, and performance monitoring

- See VPN connection status between locations
- Monitor VPN bandwidth usage
- Track performance of VPN tunnels using built-in loss, latency, jitter, and MOS voice score reporting
- Live updating log of traffic flows and path decisions
- Compare historical performance to configured performance policies
Email alerts from the cloud

- Fully integrated alerting - no need for an email server
- Customizable alerting – only get emails about the things you need to know about
- Get alerts if critical network clients go offline
- Configure alerting for all Cisco Meraki devices in one simple interface
- Send alerts to network administrators or custom recipients
Demo
Customer case studies
Case study: Peet’s Coffee & Tea

Artisan coffee roaster and specialty tea retailer, founded 1966 in Berkeley, CA

193 locations, ~4,000 employees

Branches using AutoVPN for site-to-site connectivity and control

Client monitoring, traffic analytics, Live Tools give complete visibility

Centralized control via Meraki dashboard dramatically reduces IT support load
Case study: Kindred Healthcare

Largest diversified provider of post-acute care services in the United States

2000+ locations in 46 states, 75,000+ staff

Use 3G/4G uplinks to service branch locations when no broadband available

HIPAA compliant architecture

Layer 7 firewall, traffic shaping, and content filtering blocks peer-to-peer traffic and controls users and devices
MX Product Portfolio
Licensing that fits the business’ needs

**Enterprise License**
- Next Generation Firewall
- Site-to-site and client VPN
- Intelligent path control
- Link bonding and failover
- Bandwidth shaping and QoS
- Branch routing
- Web caching
- Active/Passive high availability

**Advanced Security License**
- All enterprise features, plus
  - Content filtering (with Google SafeSearch enforcement)
  - Cisco Advanced Malware Protection
  - Snort IDS/IPS
  - Threat Grid integration*
  - Geo-based firewall rules

*additional Threat Grid subscription required
MX Portfolio – Fall 2017

Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

Small
MX64
~50 users
802.11ac wireless & PoE
FW throughput: 250 Mbps

Medium Branch
MX84
~200 users
FW throughput: 500 Mbps

MX100
~500 users
FW throughput: 750 Mbps

Large Branch, Campus or Concentrator
MX250
~2,000 users
FW throughput: 4 Gbps

MX400
~2,000 users
FW throughput: 1 Gbps

New
MX450
~10,000 users
FW throughput: 6 Gbps

Virtual
vMX100 for AWS & Azure
FW throughput: 750 Mbps
VPN & SD-WAN features

New
vMX for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX100 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX250 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX400 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX450 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX600 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

All MX devices support 3G/4G

New
vMX64 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX65 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX84 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX100 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX400 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX450 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3

New
vMX600 for Teleworker
Z1
~5 users
802.11ac Wireless & PoE
FW throughput: 50-100 Mbps

Z3
The Meraki Full Stack

A complete cloud managed IT portfolio
Single pane of glass management
Technical Careers at Cisco Meraki

Sales
- Systems Engineering
- Solution Architecture

Engineering
- UX/UI
- Firmware
- Hardware

Marketing
- Product Marketing
- Webmaster

Product Management
- Product Specialist
- Product Manager
Thank you
Q&A
Intro to Cybersecurity Self-Enroll Course

Introduction to Cybersecurity
Learn how to protect yourself online and in social media while discovering careers in cybersecurity.

You can enroll today to learn more @ http://bit.ly/Intro2Cyber