

# Securing Enterprise Networks with Cisco Meraki



# Securing Enterprise Networks with Cisco Meraki

---

Ryan Chaney, CCIE No. 16666

Simerjit Singh, CCIE No. 38710

# Securing Enterprise Networks with Cisco Meraki

## Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Contents

Introduction

Chapter 1 Merakis History

Roofnet

Start-up

Acquisition by Cisco

The Meraki Museum

Summary

Notes

Further Reading

Chapter 2 Security Frameworks and Industry Best Practices

The Cybersecurity Imperative

Adopting Industry Best Practice

Industry Standards

Security as a Team Sport

Key Themes Across Security Standards

Continuous Improvement

# **Table of Contents**

Comparison of Common Security Standards and Framework Requirements

Summary

Further Reading

## **Chapter 3 Meraki Dashboard and Trust**

Meraki Dashboard

Out-of-Band Management

Meraki Dashboard Hierarchy

Trust

Privacy

Data Retention Policy

Data Security

Data Center Resiliency

Compliance with Information Standards, Regulations, and Industry Best Practices

Hardware Trust Model

Supply Chain Security

Secure Boot

Secure Device Onboarding

Software Trust Model

Cloud Shared Responsibility Model

Summary

Notes

Further Reading

## **Chapter 4 Role-Based Access Control (RBAC)**

Meraki Dashboards Administration Hierarchy

Administrator Access Levels for Dashboard Organizations and Networks

Assigning Permissions Using Network Tags

# **Table of Contents**

Port-Level Permissions

Role-Based Access Control for Camera-Only Administrators

Role-Based Access Control for Sensor-Only Administrators

Role-Based Access Control Using Systems Manager Limited Access  
Roles

Summary

Further Reading

## **Chapter 5 Securing Administrator Access to Meraki Dashboard**

### **Securing Administrative Access to Meraki Dashboard**

Meraki Dashboard Local Administrator Access Controls

Creating Meraki Dashboard Local Administrator Accounts

Password Age

Password Reuse

Password Complexity

Account Lockout After Invalid Login Attempts

Idle Timeout

IP Whitelisting

Multifactor Authentication (MFA)

### **Configuring SAML Single Sign-On (SSO) for Dashboard**

The Use Cases for Single Sign-On

SAML Single Sign-On Login Flow

SAML Single Sign-On Design

Configuring Meraki SAML SSO Using Cisco Duo and Microsoft Entra ID

Prerequisites

Adding SP-Initiated SAML SSO

Verifying SAML SSO Access to Meraki Dashboard with Cisco Duo and Microsoft  
Entra (Including Duo Inline Enrollment)

### **Implementing Additional Access Controls Using Cisco Duo and**

# **Table of Contents**

## Microsoft Entra ID

- Password Policies

- Password Age

- Password Reuse

- Password Complexity

- Account Lockout After Invalid Login Attempts

- Security Policies

- IP Whitelisting

- Restricting Concurrent Logins

- Automatically Disabling Inactive Accounts

- Automatically Disabling Accounts After a Predetermined Period of Time Unless Revalidated

- Automatically Disabling Temporary Accounts

- Summary

- Further Reading

## Chapter 6 Security Operations

- Centralized Logging Capabilities

- Login Attempts

- Change Log

- Event Log

- Creating API Keys

- Finding Your Organization ID

- Exporting Logs

- Exporting Logs to Splunk

- Syslog

- Exporting Flow Data

- NetFlow, IPFIX, and Encrypted Traffic Analytics

- Syslog Flows

- Compliance Reporting with AlgoSec

# **Table of Contents**

Prerequisites

Integrating AlgoSec with Meraki Dashboard for Compliance Reporting

## **Monitoring and Incident Response**

Security Center

Alerts

External Alerting

Webhooks

SNMP Traps

## **External Polling**

Meraki Dashboard API

SNMP

## **Automated Incident Response with ServiceNow**

## **Security Management**

Inventory

Hardware

Software

Configuration

Client Devices

Topology

## **Summary**

Notes

Further Reading

## **Chapter 7 User Authentication**

Configuring Meraki Cloud Authentication

Configuring SAML with Cisco Duo and Microsoft Entra

Confirming Functionality of SAML Configuration Using AnyConnect VPN

Configuring RADIUS Using Cisco ISE, Cisco Duo, and Microsoft Active Directory

# **Table of Contents**

Prerequisites

Configuring Users and Groups in Microsoft Active Directory

Configuring Group(s) in Active Directory

Configuring User(s) in Active Directory

Configuring Cisco Identity Services Engine (ISE)

Adding Network Access Devices (NADs) to Cisco ISE

RADIUS Configuration for Wired and Wireless 802.1X

Configuring Organization-Wide RADIUS in Meraki Dashboard

Creating a Policy Set for Wired and Wireless 802.1X in Cisco ISE

Configuring an Authentication Policy in Cisco ISE

Configuring an Authorization Policy in Cisco ISE

Confirming Functionality of RADIUS Authentication on Wireless

Confirming Functionality of RADIUS Authentication for Wired 802.1X

RADIUS Configuration for AnyConnect VPN with Duo MFA

Configuring Duo Authentication Proxy

Configuring AD Sync in Duo Admin Panel

Encrypting Passwords in Duo Authentication Proxy

Enrolling Users with Cisco Duo

Configuring Cisco Duo as an External RADIUS Server in Cisco ISE

Creating the Policy Set for AnyConnect VPN in Cisco ISE

## **Meraki Dashboard Using Active Directory Authentication for AnyConnect VPN**

Prerequisites

Configuring Active Directory Authentication

Confirming Functionality of Active Directory Configuration

Summary

Further Reading

## **Chapter 8 Wired and Wireless LAN Security**

Access Control Lists and Firewalls



# **Table of Contents**

Access Control Lists (Meraki MS)

Meraki MR Firewall

Layer 3 Firewall

Layer 7 Firewall (Including NBAR Content Filtering)

## **Ethernet Port Security Features (Meraki MS)**

MAC Allow Lists

Sticky MAC Allow Lists

Port Isolation

SecurePort

Dynamic ARP Inspection

Rogue DHCP Server Detection (Meraki MS)

Hardening Meraki MR and MS Devices (Local Status Page)

## **Zero Trust (Wired and Wireless Dot1x)**

802.1X with Protected EAP (PEAP) on Wired and Wireless Networks

Configuring Wireless 802.1X with Protected EAP (PEAP)

Configuring Wired 802.1X with Protected EAP (PEAP)

Configuring 802.1X Using EAP-TLS on Wired and Wireless Networks

Configuring the Identity Source Sequence in Cisco ISE

Configuring the Policy Set in Cisco ISE

Generating a Client Certificate Using Cisco ISE

Exporting the Cisco ISE Certificate Authority Certificate

Testing Wireless 802.1X with EAP-TLS

Testing Wired 802.1X with EAP-TLS

## **Sentry-Based 802.1X with EAP-TLS on Wired and Wireless Networks**

Sentry Wi-Fi

Sentry LAN

Configuring MAC Authentication Bypass (MAB)

Configuring an Endpoint Identity Group in Cisco ISE

Creating a Policy Set in Cisco ISE for MAC Authentication Bypass

# **Table of Contents**

Configuring Wireless MAC Authentication Bypass in Meraki Dashboard

Configuring Wired MAC Authentication Bypass in Meraki Dashboard

## **Group Policies**

Creating a Group Policy

Applying Group Policies

Applying Group Policies to a Client Manually

Applying Group Policies Using a Sentry Policy

Applying Group Policies Using RADIUS Attributes and Cisco ISE

## **Adaptive Policy and Security Group Tags (SGTs)**

Enabling Adaptive Policy

Configuring Security Group Tag Propagation

Enabling SGT Propagation on Meraki MS Switches

Enabling SGT Propagation on Meraki MX Security Appliances

Creating Security Group Tags

Creating Adaptive Policy Groups in Meraki Dashboard

Creating Security Group Tags in Cisco ISE

Assigning Security Group Tags

Statically Assigning Security Group Tags to SSIDs

Statically Assigning Security Group Tags to Switch Ports

Assigning Security Group Tags Using Cisco ISE

Creating an Adaptive Policy

Testing Adaptive Policy

Client Laptop

POS Terminal

POS Server

Testing

## **Wireless Security**

## **Summary**

## **Notes**

# **Table of Contents**

Further Reading

## **Chapter 9 Meraki MX and WAN Security**

Meraki MX Introduction

Site-to-Site VPN (Auto VPN)

Site-to-Site VPN with Non-Meraki Devices

ThousandEyes

Remote-Access VPN

Client VPN

Sentry VPN

AnyConnect VPN

Confirming Functionality of AnyConnect VPN Access

Restricting Client VPN Traffic

Virtual MX (vMX)

Sizing a Virtual MX

Understanding Feature Parity with Meraki MX

Deploying Virtual MX in Amazon Web Services (AWS)

Creating a New vMX Network in Meraki Dashboard

Configuring the Default VPC in AWS

Deploying vMX in AWS

Viewing the New vMX in Meraki Dashboard

Summary

Notes

Further Reading

## **Chapter 10 Securing User Traffic**

Comparison of Meraki's Native Security Capabilities and Cisco

Secure Connect

Native Meraki MX Capabilities

Layer 3 Firewall

# Table of Contents

- Layer 7 Firewall
- Geo-IP Firewall
- Enabling Detailed Traffic Analysis
- Configuring Geo-IP Firewall
- Content Filtering
- URL Filtering
- Category Blocking with Cisco Talos Intelligence
- Threat Protection
- Advanced Malware Protection (AMP)
- Intrusion Detection and Prevention (IDS/IPS)

## Cisco Secure Connect

- Setting Up Secure Connect
- Initial Setup and Integration with Cisco Umbrella
- Adding Meraki SD-WAN Sites to Secure Connect
- Configuring DHCP to Assign Umbrellas DNS Servers
- Installing Umbrellas Root CA Certificate on Clients
- Enabling Intelligent Proxy and SSL Decryption in Cisco Umbrella
- DNS Security
- Cloud Firewall
- Layer 3/4 Firewall
- Application Blocking
- Intrusion Detection and Prevention (IDS/IPS)
- Secure Web Gateway (SWG)
- URL Filtering (Destination Lists)
- Content Filtering (Content Categories)
- File Inspection and Advanced Sandboxing
- File Type Control
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)

## Summary

# **Table of Contents**

Notes

Further Reading

## **Chapter 11 Securing End-User Devices**

Integrating with Vender Mobile Device Enrollment Programs

Enrolling Devices with Systems Manager

Checking Compliance with Security Policy (Systems Manager Policies)

Creating a Systems Manager Profile

Configuring End-User Devices for Network Connectivity

    Certificate Settings Payload

    Wi-Fi Settings Payload

    VPN Settings Payload

Applying Security Policy to Devices (Systems Manager Profiles)

    Passcode Policy (Includes Screen Lock)

    Disk Encryption

    Preventing the Installation of Banned Apps

Deploying Applications to Devices

Pushing Operating System Updates to Devices

Summary

Notes

Further Reading

## **Chapter 12 Physical Security**

Meraki MV Security Cameras

    Privacy

    Monitoring Video

    Motion Alerts

    Motion Search

Sensor Sight (Meraki Smart Camera and Sensor Integration)

# **Table of Contents**

Summary

Further Reading

Appendix A Comparison of Common Security Standards and  
Framework Requirements

Index