CISCO MERAKI SD-WAN

Advanced Policy, Security and Programmability

Version 2.4

1 Course Overview

This 3-day workshop provides hands-on training on Cisco Meraki SD-WAN implementations as well as basic and advanced security features that are available on Meraki MX devices. Deep dive into capabilities like Firewall and Traffic, Application Aware Firewall, AMP Integration, Content Filtering and Threat Protection and many other advanced features are covered as a part of this training. This course also provides hands-on training on Cisco Meraki SD-WAN programmability features.

2 Who Should Attend

This course is ideal for those who regularly deploy or manage Meraki networks and want to deepen their technical expertise and understanding of the full Meraki product suite and features. This may include professionals like:

- Field Deployment Technicians
- Network Administrators
- Pre-/Post-Sales Engineers
- Systems Engineers
- Security Engineers

3 Prerequisites

Students should meet the following prerequisites:

- Basic Networking Concepts
- Familiarity with basic Network Protocols and Applications
- Familiarity with basic Security concepts

4 Why Attend a Blue River Experts Course

Our courses are not delivered by instructors but by consulting system engineers who have vast experience regarding real life design, deployment, and troubleshooting of actual customer installations. Besides delivering courses, our engineers usually design and deploy large enterprise solutions or perform real world POVs (proof of value) and POCs (proof of concept) for large customers. We are often requested and contracted by product vendors to help customers make buying decisions based on their particular use case. This allows us to discuss real world use cases, designs, and operational situations with our students.

If you would like to get educated by experts who will explain to you the whole life cycle from day 0 to day 2 as they have comprehensive knowledge from having written numerous business requirements documents, customer requirements documents, high level design and detailed design documents and having deployed and troubleshooted many customer installations then you should choose to attend one of our courses.

5 Course Objectives

After completing this course, students will be able to:

- Understand key concepts of Cisco Meraki SD-WAN
- Implement Meraki SD-WAN Solutions
- Understand Cisco Meraki SD-WAN Security Features
- Implement Firewalls and IPS Policies
- Understand Cisco SD-WAN Programmability features
- Script APIs to automate Cisco SD-WAN vManage configurations

6 Course Details

6.1 Introduction to Meraki SD-WAN and Meraki Key Concepts

6.1.1 Meraki Centralized Dashboard

6.1.2 Meraki Key Concepts

- Meraki Concentrator Modes
- VPN Topology
- Split Tunnel and Full Tunnel
- Hub and Spoke and VPN Mesh

6.1.3 Meraki Connection Monitor

6.1.4 Data Center Redundancy (DC-DC Failover)

- Hub/DC redundancy (Disaster Recovery)
- DC Failover Architecture - Concentrator Priority

6.1.5 Warm Spare for VPN Concentrators

6.2 Meraki SD-WAN Deployment Models

6.2.1 Introduction

6.2.2 MX Deployment Considerations

- MX Deployment Considerations
- Upstream DC Switching Considerations
- Routing Considerations
- Firewall Considerations

6.2.3 Data Center Deployment

- VPN concentrator in NAT mode
- One-arm concentrator mode
- Dynamic Routing – OSPF, BGP

6.2.4 Branch Deployment

- AutoVPN at the Branch
- Hub and Spoke VPN Deployment
- Hub Priorities and Design Considerations

6.3 Meraki SD-WAN Security

6.3.1 Exploring the SD-WAN and Security Dashboard

6.3.2 Site-to-site VPN Deep Dive

- What is a VPN
- Site-to-Site Hub Configuration
  - Hub Configuration
    - Hub Configuration with an Exit Hub
  - Spoke Configuration
    - Split Tunnel vs Full Tunnel
- VPN Firewall Rules
- Monitor VPN Status

6.3.3 Client VPN Technologies

- Enable Client VPN
- Configure Client VPN
- Client VPN Authentication Methods
- VPN Clients
- Enable the AnyConnect Client VPN
- AnyConnect Client VPN Authentication Methods

6.3.4 Access Control and Splash Page

6.3.5 NAT and Port Forwarding

6.3.6 Firewall and Traffic Shaping

6.3.7 Meraki and Cisco Umbrella Integration

6.4 Firewall and Traffic Shaping Policies

6.4.1 MX Firewall Settings

- Outbound Rules
- Appliance Services
- Layer 7 Firewall Rules
- Forwarding Rules

6.4.2 IP Source Address Spoofing Protection

- Overview and Key Terms
- NAT Modes Implementation
- Supported Deployment Topologies

6.4.3 SD-WAN and Traffic Shaping

- Uplink Configurations
- Uplink Selections
- Global Bandwidth Limitations
- Traffic Shaping Rules
- Web Cache

6.5 Meraki Insight

- Web Application Health
- Alert Management for WAN Packet Loss
- Global Bandwidth Limitations
- Alert Management for WAN Utilization
- Alert Management for Uplink Latency
- Monitor WAN Health

6.6 Content Filtering and Threat Protection

6.6.1 MX and Active Directory Integrations

- Active Directory Authentication
- Active Directory integration with Group Policy

6.6.2 Content Filtering Implementations and Troubleshooting

- Adult Content Filtering
- Gaming Content Filtering
- Social Site Content Filtering

6.6.3 Cisco AMP Integrations and Threat Protection

- Threat Protection – AMP
- Threat Protection – IDS/IPS
- Threat Protection – Umbrella Protection

6.6.4 Threat Grid Integrations

6.7 Programmable API

6.7.1 Meraki Dashboard API with Postman

6.7.2 Meraki Organization and Networks Import into Postman

6.7.3 Meraki Devices into the appropriate Networks using APIs

6.7.4 Troubleshooting Meraki using APIs

- Dashboard
- Device Dashboard

7 Lab Exercises

7.1 Meraki MX Site-to-Site VPN Configuration

- Configuring VLANs
- Configuring Site-To-Site VPN (Auto VPN)
- VPN Topologies – Split Tunnel
- VPN Topologies – Full Tunnel

7.2 Meraki MX – SDWAN Configuration

- SD-WAN & Traffic Shaping
- Configuring SD-WAN
- Policies for Traffic Preferences
- SD-WAN – Global Bandwidth Limits

7.3 Configuring Meraki Insight

- Configuring Web Application Health
- Configuring Alert Management for WAN Packet loss
- Configuring Alert Management for WAN Utilization
- Configuring Alert Management for Uplink Latency
- Monitor WAN Health

7.4 Meraki Security Configurations

- Group Policy
- Layer 3 Firewall Rules
- Content Filtering
- Threat Protection

7.5 Programmability

- Instructor Demo
    - Meraki API Technologies and Tools
    - Meraki Dashboard API
    - Organization and Network import
    - Device / Network mapping
    - Troubleshooting using APIs