ICM-MXSA-CT -Installing and Configuring Meraki MX Security Appliances

Following completion of this course, students will understand, Install, Configure, Monitor, and Troubleshoot the following:

- Navigate and configure the dashboard
- Add MX/MR/MS/MV devices to the Dashboard
- Understand and Configure Configuration Templates
- Understand and Configure Group Policies
- Manage/Configure/Integrate Users and Radius Policies
- Configure, Monitor, and Troubleshoot MX Firewalls
- Troubleshoot devices and Connectivity
-

he primary audience for this course is as follows:

- IT Staff and Managers
- Network and systems personnel and engineers
- Small to mid-sized organizations that require fundamental knowledge on networking terms/concepts and configuration guidance for Meraki equipmen
- This also includes organizations looking to implement remote sites, provide a guest wireless solution, and collect user analytics

Course Overview

Module 1: Introduction to Meraki

- The Meraki Mission
- Cisco Meraki: Bringing the Cloud to Enterprise Networks
- Cloud-Managed Networking Architecture
- Benefits of a Cloud-Based Solution
- The Meraki Full Stack: New and Unique Value Proposition
- Meraki Deployment – How it works
- Why Customers Choose Meraki
- Meraki MS Switches Overview
- Meraki MX Security Appliances Overview
- Meraki SD-WAN Overview
- Meraki MR Wireless Access Points Overview
- Cisco Meraki Systems Manager Overview
- Cisco Meraki MV Vision Security Cameras Overview
- Meraki API Overview
- Meraki Licensing
- Enterprise Support
- Cisco Meraki Documentation

Module 2: Cloud Management with the Meraki Dashboard

- The Cisco Meraki Dashboard
- Dashboard: Organizational Structure
- Out-of-band Cloud Management
- Loss of Connectivity to the Cisco Meraki Cloud
- Meraki Dashboard Logins
- Create Dashboard Accounts and Organization
- MSP Logins – Manage Multiple Organizations
- Modify an Organization
- View Organizations Health
- Meraki Dashboard Best Practices
- Dashboard Search
- Meraki Help
- Organizational Wide Settings
    - Configure
        - Configuring Organizational Wide Settings
        - Using Configuration Sync to View and Copy Settings
        - Administrators
        - Configuring and Monitoring Licensing
        - Creating Bulk Networks
        - Creating and Managing Networks (sites)
        - Managing the Meraki Inventory
    - Monitor
        - Overview
        - Monitoring the Change log
        - Monitoring Login Attempts
        - Monitoring the Security Center
        - Using Location Analytics
        - Monitoring VPN Status
        - Scheduling and Managing Firmware
        - Using the Summary Report
    - Create and Manage Configuration Templates
        - Understand Configuration Templates
        - VLAN Templates
        - Attach Network to Configuration Templates

- Network Wide Settings
    - Configure
        - Configuring Network Wide General Settings
            - Traffic Analysis
            - Location and Scanning
            - Configuring CloudShark for Capturing Traffic
            - Manage the Local Status Page
            - Manage Syslog, SNMP, Location, and NetFlow Services

    - Managing Network Admins and Guest Ambassadors
    - Managing Network Users
    - Managing Port Management Privileges
    - Configuring Group Policies
    - Adding Devices to the Network
  - Monitoring Networks
    - Monitoring Clients
    - Monitoring Traffic Analytics
    - Displaying and Exploring the Meraki Topology
    - Performing Packet Captures
    - Using the event Log to Perform Troubleshooting

Module 3: Meraki MX Security

- Benefits of a Cloud Managed Solution
- Threat Management Solution
- Advanced Security Licenses
- Reliable, Cost Effective Connectivity with Meraki SD-WAN
- Site-to-Site VPN (Auto VPN)
- High Availability and Path Redundancy
- Application-Aware Intelligent Path Control
- Traffic Monitoring and Analytics
- Integrating Active Directory
- Cisco Meraki MX Models and Features
  - MX 64/65/84/100/200/250/400/600 Models
  - Virtual MX for Amazon Web Services & Microsoft Azure
  - Teleworker Z1/Z3

- Configuring the Local Status Page
- Adding Appliance to Network
- Device Configuration
- Configuring the Warm Spare Feature
- Device Tags & Notes

- Configuring Addressing & VLANs
  - Pass-Through or VPN Concentrator Mode vs NAT Mode
  - Creating VLANs
  - Creating Layer 3 Interfaces
  - Creating Static Routes
  - Using Dynamic Routing Protocols
    - OSPF and BGP
- DHCP Server Configuration and Options

- Meraki Firewall Configuration
    - Firewall Basics
    - Layer 3 vs Layer 7 Firewall
    - Firewall Outbound Rules
    - Cellular Firewall Failover Rules
    - Security Appliance Services
    - Layer 7 Firewall Rules

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

    - Geo-IP Based Firewalling
    - Nat Configuration
    - Bonjour Forwarding

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

- One Arm VPN Concentrator Configuration
    - OSPF Configuration
    - BGP Configuratio

- Meraki Client VPN
    - Enable Client VPN
    - Configure Client VPN
    - Client VPN Authentication Methods
    - VPN Clients

- Meraki Active Directory Integration
    - Active Directory Authentication
    - Active Directory integration with Group Policy

- Meraki Access Control
    - Radius (2)
    - Facebook
    - Third Party (Google)

- Meraki Splash Page Configuration
- Configuring Access Policies
- Teleworker VPN / L3 Roaming

LABS

Lab 1: Configuring the Organization

- Configure Organizational Settings
- Add All Devices to Organization
- Create Networks
- Manage Network-Wide Settings
- Create group Policies
- Manage Firmware Upgrades
- Create Templates
- Manage VLAN Templates
- Bind Templates to Networks

Lab 2: Configuring MX Appliances and Z3 Teleworker Devices

- Configure MX Appliance and Configure Z3 Appliance
    - Setup VLANs and Layer 3 Interfaces
    - Setup a VPN Concentrator
    - Setup and Manage DHCP Settings
    - Configure Layer 3 Firewall Settings
    - Configure Layer 7 Firewall Settings
    - Configure Content Filtering
    - Configure Traffic Shaping
    - Configure SDWAN Feature and traffic Distribution
    - Configure Site-to-site VPN
    - Configure Client VPN
    - Integrate Active Directory with Group Policy Settings
    - Create Traffic Shaping Policies
    - Configure Access control with Radius and ISE
    - Create and Configure Splash Pages

- MX Appliances and Z3 Verification and Troubleshooting
    - Verify and Trouble Shoot Appliance Status
    - Verify and Trouble Shoot Site to Site VPN
    - Verify and Trouble Shoot Firewall Settings
    - Check the Routing Table
    - Use the Tools
    - Trouble shooting with Packet Capture