Implementing and Operationalizing Meraki SD-WAN SASE

Duration: 3 Days Course Code: N1_MESASE

Overview:

This Meraki SD-WAN training is targeted to engineers and technical personnel involved in deploying, implementing, operating and optimizing Meraki SD-WAN solution, both in enterprise and Service Provider environments. This training is specially designed for implementing Meraki SD-WAN in integration with the complete feature set of Cisco Umbrella including DNS Security, Cloud Based Firewall and Secure Internet Gateway. The course walks you through how each integration works and how to design and implement it step-by-step.

Target Audience:

The primary audience for this course is as follows:
System Engineers
System Administrators
System Architects
Channel Partners

Content:

Module 1: Introduction to Meraki SD-WAN and Meraki Key Concepts

- Meraki Centralized Dashboard
- Meraki key concepts
- Meraki Concentrator Modes
- VPN Topology
- Split Tunnel and Full Tunnel
- Hub and Spoke and VPN Mesh
- Meraki Connection Monitor
- Data Center Redundancy (DC-DC Failover)
- Warm Spare for VPN Concentrators
- Deployment Models:
- Deploying vMX in the Public and Private Cloud

Module 2: Meraki SD-WAN Deployment Models

- Introduction
- Data Center Deployment
- MX Deployment Considerations
- MX Deployment Considerations
- Upstream DC Switching Considerations
- Routing Considerations
- Firewall Considerations
- Branch Deployment
- AutoVPN at the Branch
- Hub and Spoke VPN Deployment
- Hub Priorities and Design considerations
- Meraki Centralized Policies
- DIA traffic steering using Smart Path
- Implementing QoS from the dashboard
- Configuring arbitrary topologies

Module 3: Meraki SD-WAN Security

- Exploring the SD-WAN and Security Dashboard
- Site-to-site VPN Deep Dive
- Client VPN Technologies
- Access control and Splash Page
- NAT and Port Forwarding
- Firewall and Traffic Shaping
- Content Filtering and Threat Protection
- Meraki and Cisco Umbrella Integration

Module 4: Designing and Implementing DNS Security

- Pre-requisite check before integrating Umbrella with Meraki SD-WAN
- Making sure you have the correct licensing
- Platform support check
- Internet Connectivity check
- Walking through the Umbrella Dashboard
- Dashboard Overview
- DNS Policy GUI Overview
- Firewall Policy GUI Overview
- Web Policy GUI Overview
- Umbrella AD/SAML Integration Overview (optional)
- Integrating Cisco Umbrella for DNS Security
- Umbrella API Integration
- Configuring the DNS Encryption Policy
- Excluding the local domains
- Configuring the Security Policy in Meraki
- Implementing the policy at the DIA Sites

Module 5: Meraki MX and Cisco Umbrella SIG IPSEC Tunnels

- Cisco Umbrella SIG Overview
- Phase 1: IPSEC plus Cloud Security
- Licensing requirement for Phase1
- Meraki MX IPSEC integration with Cisco Umbrella
- Enhanced DNS protection with Selective Proxy
- Security Policy: URL Inspection, HTTPS Inspection, Cloud Delivered Firewall, Granular Content Filtering, Non-Web Traffic Security
- Phase 2: SIG Integration with Meraki SD-WAN
- Verification
- Checking the logs on Umbrella Dashboard

Module 6: Troubleshooting Umbrella Integration

- Troubleshooting DNS Security
- API Integration not working
- DNS for local domain failing
- No redirection to Cisco Umbrella for external domains
- Troubleshooting SIG and Firewall
- Making sure the IPSec Tunnels to Umbrella are operational
- Troubleshooting the policies for redirection
- Reviewing logs in Umbrella
- Checking Alarms and Notifications
- Checking Alarms on Meraki Dashboard
- Checking Alarms on Cisco Umbrella
- Leveraging Meraki Insights for
- Network Visibility
- Traffic Analytics using DPI
- Faster Resolution

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK