Engineering Cisco Meraki Solutions v1.0 (500-220)

Exam Description: The Engineering Cisco Meraki Solutions v1.0 (ECMS 500-220) is a 90-minute exam associated with the Cisco Meraki Solutions Specialist. This exam tests a candidate's knowledge and skills to engineer Meraki solutions including cloud management, design, implementing, monitoring, and troubleshooting. The courses, Engineering Cisco Meraki Solutions Part 1 and Part 2, help candidates to prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

15% 1.0 Cisco Meraki Cloud Management

- 1.1 Explain Cisco Meraki cloud architecture
- 1.2 Explain access methods to dashboard and devices
- 1.3 Explain organizational structure, segmentation and permissions
- 1.4 Explain licensing, co-termination, and renewals
- 1.5 Compare deployment workflows

30% 2.0 Design

- 2.1 Design scalable Meraki Auto VPN architectures
- 2.2 Explain deployment consideration for the vMX
- 2.3 Design dynamic path selection policies
- 2.4 Design stable, secure, and scalable routing deployments
- 2.5 Design Enterprise network services
  - 2.5a Redundant networks and high availability
  - 2.5b QOS strategy for voice and video
  - 2.5c Applying security at layer 2
  - 2.5d Firewall and IPS rules on MX and MR
  - 2.5e Network access control solutions
- 2.6 Design Enterprise wireless services
  - 2.6a High density wireless deployments
  - 2.6b MR wireless networks for Enterprise
  - 2.6c MR wireless networks for guest access
- 2.7 Compare endpoint device and application management methods
  - 2.7a Device enrollment such as supervised and device owner
  - 2.7b Application deployment

25% **3.0 Implementation**

- 3.1 Configuring MX security appliances
  - 3.1a SVI, dynamic routing and static routes
  - 3.1b Auto VPN
  - 3.1c Traffic shaping and SD-WAN
  - 3.1d Threat protection and content filtering rules
  - 3.1e Access policies and 802.1x
- 3.2 Configuring MS switches
  - 3.2a SVI, dynamic routing and static routes
  - 3.2b QoS using Meraki switching networks
  - 3.2c Access policies and 802.1x
  - 3.2d Replicate a switch configuration
- 3.3 Configuring MR wireless access points
  - 3.3a SSIDs for Enterprise and BYOD deployments
  - 3.3b Traffic shaping
  - 3.3c RF profiles
  - 3.3d Air Marshal
- 3.4 Configuring SM endpoint management
  - 3.4a Management profiles
  - 3.4b Security policies
  - 3.4c Sentry for Meraki managed deployments
- 3.5 Configuring MV security cameras
  - 3.5a Camera video and alerting
  - 3.5b Retention settings
- 3.6 Configuring MI application assurance
  - 3.6a Standard applications
  - 3.6b Application thresholds

30% **4.0 Monitoring and Troubleshooting**

- 4.1 Interpret information from monitoring and reporting tools
  - 4.1a Alerts with Dashboard, SNMP, Syslog and Netflow in Dashboard
  - 4.1b Logging and reporting in Dashboard
- 4.2 Describe how to use the dashboard API to monitor and maintain networks
- 4.3 Explain firmware upgrades

4.4 Troubleshooting Enterprise networks

- 4.4a Layer 2 technologies using Dashboard
- 4.4b Layer 3 technologies using Dashboard
- 4.4c Wireless client connectivity issues using Dashboard
- 4.4d Device local status pages
- 4.4e Security threats using Security Center
- 4.4f Application performance issues using Meraki Insight