PassQueen
a.k.a dumpsqueen.com

Engineering Cisco Meraki Solutions (ECMS) v2.2

Cisco 500-220

Version Demo

Total Demo Questions: 10

Total Premium Questions: 108

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Cloud Management	22
Topic 2, Design	13
Topic 3, Implementation	25
Topic 4, Monitoring, Logging, Alerting, and Troubleshooting	25
Topic 5, Security	23
Total	108

QUESTION NO: 1

Which two methods can be used to claim Meraki devices into an organization inventory? (Choose two.)

A. Serial number

B. Meraki order number

C. Device MAC address

D. Network ID

E. Management IP address

ANSWER: A B

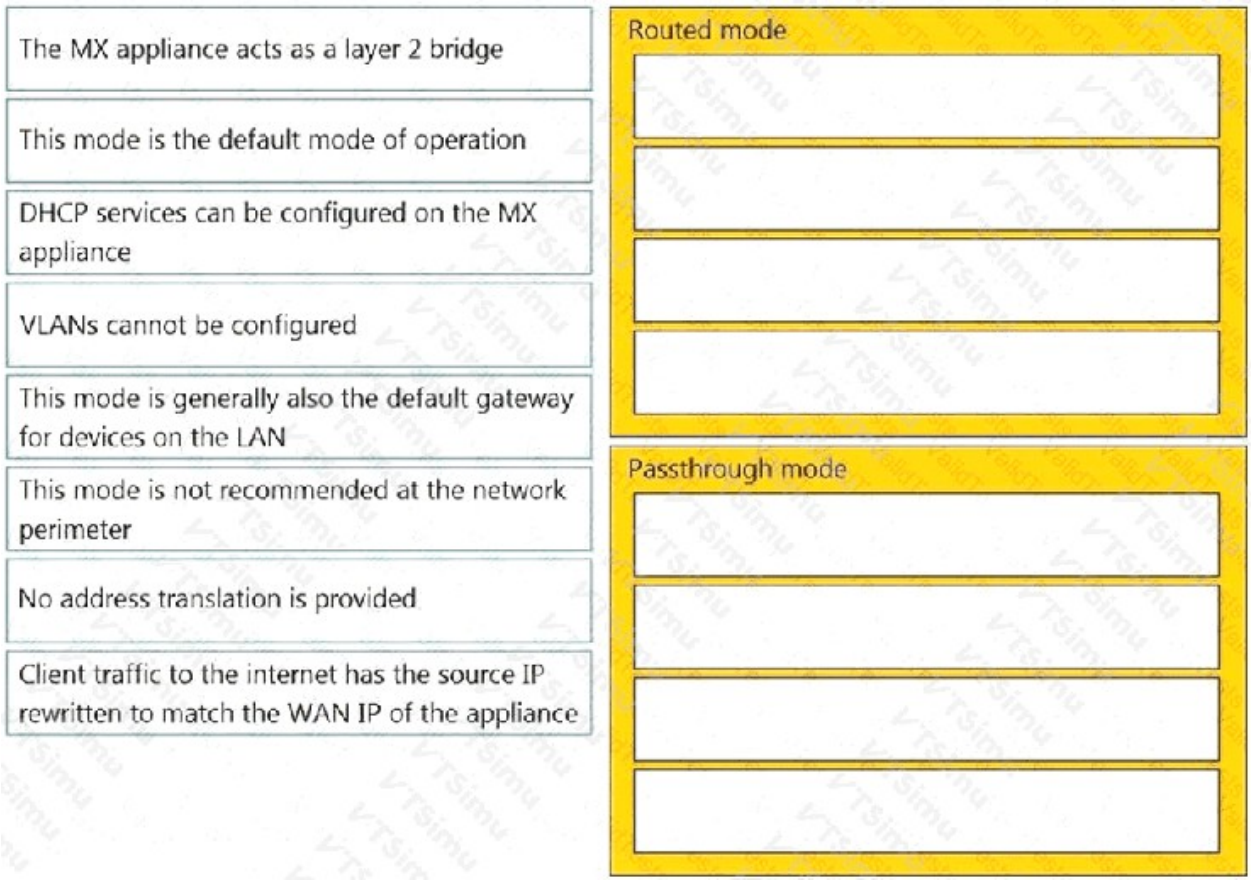
Explanation:

An administrator can claim devices by entering their **serial numbers** or by entering a valid **Meraki order number**. Claiming adds the hardware to the organization inventory, where it can then be assigned to a network and configured through Dashboard.

A device MAC address does not claim hardware into Dashboard, and a network ID identifies a Dashboard network rather than a purchased device. Devices can be claimed from the Organization inventory page or through applicable Dashboard API endpoints. See Cisco Meraki's Adding and Removing Devices from Dashboard Networks.

QUESTION NO: 2 - (DRAG DROP)

Drag and drop the descriptions from the left onto the corresponding MX operation mode on the right.



ANSWER:

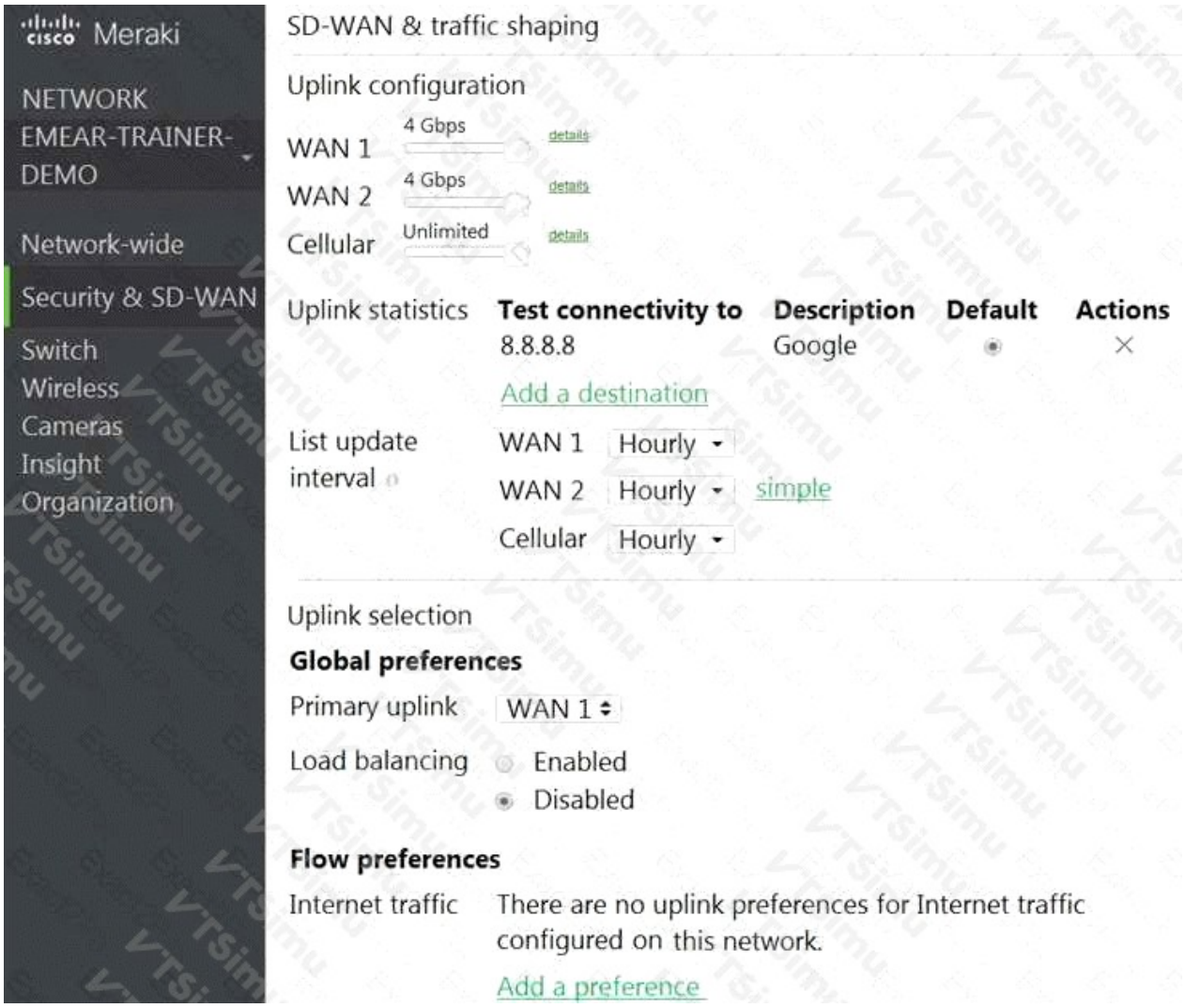
Explanation:

MX Routed mode is the normal deployment mode for a Meraki security appliance and is the default operating mode. In this design, the MX performs Layer 3 gateway functions for the local network, so it is generally configured as the default gateway used by LAN clients. Routed mode also permits the MX to provide DHCP services, allowing it to allocate addressing information and other DHCP settings to clients on configured local networks. For internet-bound traffic, the MX performs source network address translation, rewriting the client source address to the applicable WAN address of the appliance. This enables privately addressed LAN clients to access external networks through the MX WAN interface.

Passthrough mode is intended for an MX that must be inserted transparently into an existing network design. The appliance operates as a Layer 2 bridge, allowing traffic to pass through it while retaining inline security and visibility capabilities. Because it is transparent rather than acting as the routed gateway for locally configured VLANs, VLANs cannot be configured on the MX in this mode, and it does not provide address translation. This makes passthrough mode suitable for situations where another upstream device already owns routing, addressing, and NAT responsibilities. It is not generally used as the perimeter design because the MX is not taking the normal gateway and translation role expected at the internet edge. Cisco Meraki documents these mode behaviors in its MX Addressing and VLANs guide, including the routed gateway, DHCP, NAT, and passthrough bridging characteristics.

QUESTION NO: 3

Refer to the exhibit.



Which two actions are required to optimize load balancing asymmetrically with a 4:1 ratio between links? (Choose two.)

A. Change the primary uplink to " none " .

B. Add an internet traffic preference that defines the load-balancing ratio as 4:1.

C. Enable load balancing.

D. Set the speed of the cellular uplink to zero.

E. Change the assigned speeds of WAN 1 and WAN 2 so that the ratio is 4:1.

ANSWER: C E

Explanation:

Enable load balancing is required because an MX appliance uses the configured uplinks concurrently only when load balancing is enabled in the SD-WAN and traffic-shaping settings. With this feature enabled, the appliance can distribute eligible Internet-bound flows across both WAN links rather than using a single preferred uplink except during failover. Load balancing is flow based, so individual sessions remain on their selected uplink while the aggregate traffic distribution follows the configured link capacities.

Change the assigned speeds of WAN 1 and WAN 2 so that the ratio is 4:1 is also required because MX load-balancing decisions are weighted according to the configured uplink bandwidth values. The assigned speeds must therefore reflect the intended proportion. For example, configuring one WAN uplink for 100 Mbps and the other for 25 Mbps supplies a 4:1 weighting, allowing the MX to steer approximately four times as many eligible traffic flows toward the higher-capacity circuit over time. These values should represent the usable WAN bandwidth, not merely the physical interface speed, so the load-balancing behavior matches the actual capacity delivered by each provider. Cisco documents that MX load balancing uses the configured uplink bandwidth and that it must be enabled for simultaneous use of multiple WAN uplinks. See Cisco Meraki MX Load Balancing and Failover and Cisco Meraki SD-WAN and Traffic Shaping.

QUESTION NO: 4

Refer to the exhibit.



For an AP that displays this alert, which network access control method must be in use?

A. preshared key

B. WPA2-enterprise with my RADIUS server

C. splash page with my RADIUS server

D. MAC-based access control with RADIUS server

ANSWER: B

Explanation:

WPA2-enterprise with my RADIUS server is the required network access control method because the displayed alert identifies an 802.1X authentication failure. In Meraki wireless networks, WPA2-Enterprise uses 802.1X/EAP to authenticate wireless clients against a RADIUS server. The access point acts as the authenticator, relaying EAP authentication exchanges between the client (supplicant) and the configured RADIUS server (authentication server). Therefore, an alert specifically associated with 802.1X and RADIUS authentication indicates that the SSID is configured for Enterprise authentication rather than a shared-secret-only model. The RADIUS server validates the client's identity and returns the authorization result, allowing Meraki to apply the enterprise wireless security policy. Cisco Meraki's authentication documentation describes Enterprise authentication as using a RADIUS server and 802.1X-based EAP authentication, while its wireless encryption documentation identifies WPA2-Enterprise as the appropriate mode for this design. See the Meraki Encryption and Authentication Overview and Meraki RADIUS Issues documentation.

QUESTION NO: 5

What is the default frequency of SD-WAN probes sent between VPN peers in a Cisco Meraki MX SD-WAN deployment?

A. 10 milliseconds

B. 100 milliseconds

C. 1 second

D. 10 seconds

ANSWER: C

Explanation:

1 second is the default probe interval for Cisco Meraki MX SD-WAN traffic between Auto VPN peers. MX appliances continuously send synthetic VPN performance probes across available WAN paths at this cadence to measure the path characteristics that matter for real-time applications: latency, loss, and jitter. The resulting measurements populate VPN performance statistics and provide the current path-quality information used by SD-WAN policies, including performance-based uplink selection and failover decisions. A one-second interval gives the MX a sufficiently current view of tunnel health and application experience while avoiding excessive control and measurement overhead on WAN circuits. This behavior is part of Meraki's Auto VPN and SD-WAN performance-monitoring design, where an appliance evaluates available paths between VPN peers and can steer traffic according to configured performance requirements. Cisco's Meraki SD-WAN documentation describes the use of VPN performance metrics for path selection, and Cisco Live material on Meraki SD-WAN specifies the one-second probing behavior. See Cisco Meraki SD-WAN and Traffic Shaping documentation and Cisco Live: Meraki SD-WAN presentation.

QUESTION NO: 6

Which Meraki Dashboard menu section is accessed to enable Sentry enrollment on an SSID?

A. Wireless > Configure > Access Control

B. Wireless > Configure > Splash page

C. Wireless > Configure > Firewall & Traffic Shaping

D. Wireless > Configure > SSIDs

ANSWER: A

Explanation:

Wireless > Configure > Access Control is the correct menu path because Sentry enrollment is configured as part of the authentication and access-control settings for an individual Meraki MR SSID. An administrator selects the relevant SSID on the Access Control page and enables the Systems Manager Sentry enrollment capability there. This workflow connects wireless access to Meraki Systems Manager device enrollment, allowing unmanaged devices that join the SSID to be directed through enrollment before receiving the intended level of network access.

Meraki places Sentry-related wireless authentication controls alongside other SSID access policies because the feature governs how clients authenticate and become managed, rather than how the SSID is named, how its splash page is branded, or how traffic rules are applied after connection. The Access Control page is therefore the operational location used to activate and manage this enrollment behavior on the selected wireless network. Cisco Meraki's documentation for Systems Manager Sentry Enrollment describes the integration of Systems Manager enrollment with Meraki network access. The MR Access Control documentation also covers the SSID-level authentication and access settings where this configuration is administered.

QUESTION NO: 7

Which two notification delivery methods are available when configuring an alert in the Meraki Dashboard? (Choose two.)

A. Email

B. Webhook

C. Syslog server

D. Auto VPN tunnel

E. RADIUS Access-Accept message

ANSWER: A B

Explanation:

Email and **webhook** are available notification methods for Dashboard alerts. Email notifications can be delivered to designated recipients, while webhooks enable an external application or automation platform to receive alert information programmatically.

Alert conditions and available delivery options vary by Meraki product and alert type. A syslog server receives exported syslog event messages rather than Dashboard alert notifications, and an Auto VPN tunnel is not an alert-delivery method. See Cisco Meraki's Alerts and Notifications Overview.

QUESTION NO: 8

A customer requires a hub-and-spoke Auto VPN deployment with two NAT-mode hubs with dual uplink connections and 50 remote sites with a single uplink connection.

How many tunnels does each hub need to support?

A. 52

B. 54

C. 100

D. 104

ANSWER: C

Explanation:

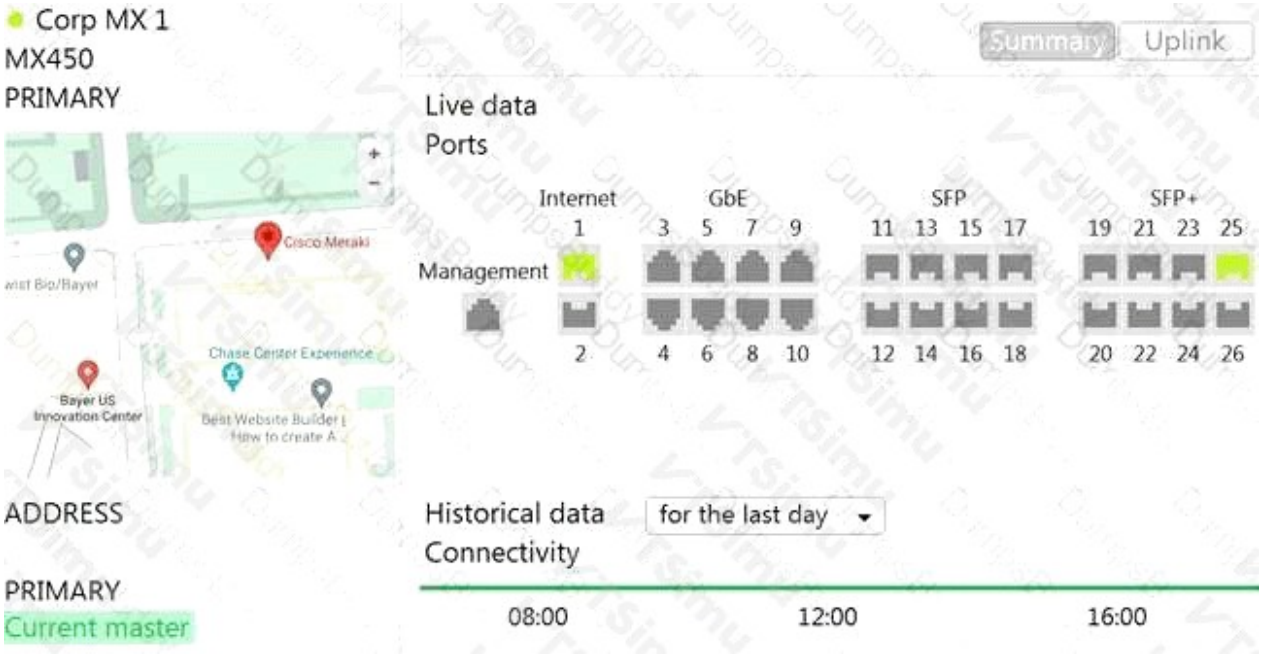
100 is correct. Each of the 50 remote sites has one active uplink and must establish Auto VPN connectivity to each active uplink on a hub. Because each hub has two uplink connections, every single-uplink spoke creates two VPN tunnels to that hub: one tunnel per hub WAN interface. The required tunnel capacity for an individual hub is therefore 50 remote sites multiplied by 2 hub uplinks, which equals 100 tunnels.

The presence of a second hub provides hub redundancy for the spoke sites, but the question asks for the capacity required *by each hub*. Thus, the calculation is performed independently for either hub using its own two WAN interfaces and all 50 spokes. NAT mode does not alter this tunnel-count calculation; Auto VPN uses the Meraki cloud to distribute peer and connectivity information and establishes the appropriate encrypted VPN paths across the available Internet-facing interfaces.

Cisco Meraki explains Auto VPN operation and hub-and-spoke topology in its Site-to-Site VPN Overview. Additional design details for redundant hub deployments are available in the VPN Concentrator Deployment Guide.

QUESTION NO: 9

Refer to the exhibit.



The VPN concentrator is experiencing issues. Which action should be taken to ensure a stable environment?

A. Add a deny any/any firewall rule to the end of the firewall rules.

B. Remove the connection from Internet 1.

C. Physically disconnect all LAN ports.

D. Configure the MX appliance to Routed mode on the Addressing & VLANS page.

ANSWER: C

Explanation:

Physically disconnect all LAN ports. An MX deployed as a one-arm VPN concentrator must connect to the upstream network only through its Internet/WAN interface. In this deployment model, VPN traffic is forwarded to and from the concentrator through that same interface; the appliance is not intended to participate in the production network through LAN interfaces. A LAN-side connection can create an unintended parallel path or Layer 2/Layer 3 topology issue, resulting in unstable routing or VPN behavior.

For a redundant concentrator pair, each MX should be configured for Passthrough or VPN Concentrator mode and connected through its respective Internet port to the same reachable network/subnet. The MX appliances must be able to communicate with one another and with the Meraki Dashboard. Removing every physical LAN-port connection restores the supported one-arm topology while retaining the WAN-side connectivity needed for Auto VPN termination and concentrator high availability. Cisco Meraki documents that one-arm concentrators are connected to the network exclusively through their Internet ports in its Auto VPN general best practices. Additional deployment guidance is available in the VPN Concentrator Deployment Guide.

QUESTION NO: 10

Which two controls can be applied to a client by using a Meraki group policy? (Choose two.)

A. Firewall rules

B. Bandwidth limits

C. Dashboard administrator permissions

D. Organization licensing term

E. Device firmware release channel

ANSWER: A B

Explanation:

Firewall rules and **bandwidth limits** can be applied through a Meraki group policy. Group policies allow administrators to apply differentiated controls to selected clients without creating a separate network-wide configuration. For example, a policy can limit guest-client throughput and restrict access to internal destinations.

Group policies can be assigned manually, through RADIUS attributes, or by other supported assignment methods depending on the product and deployment. The policy is enforced when the client is identified as a member of that group. Cisco Meraki documents available group-policy controls in the Creating and Applying Group Policies guide.