Number: 500-220
Passing Score: 800
Time Limit: 120
File Version: 7.0

Exam Code: 500-220

Exam Name: Engineering Cisco Meraki Solutions

Exam A

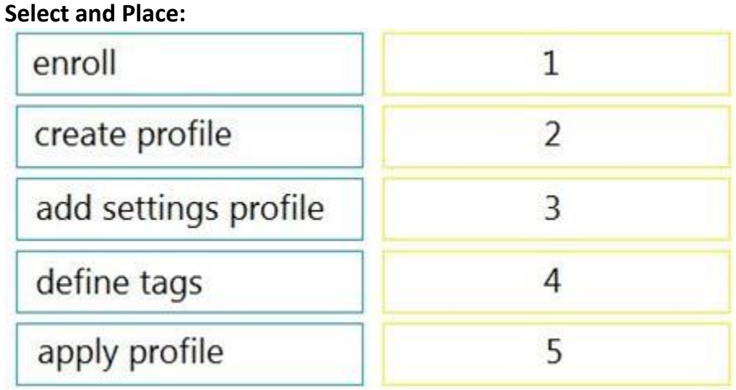
QUESTION 1
Which two primary metrics does Meraki Insight use to calculate the Application Performance Score? (Choose two.)

A. Maximum Jitter
B. Total Bandwidth Usage
C. Maximum Latency
D. Per-flow Goodput
E. Application Response Time

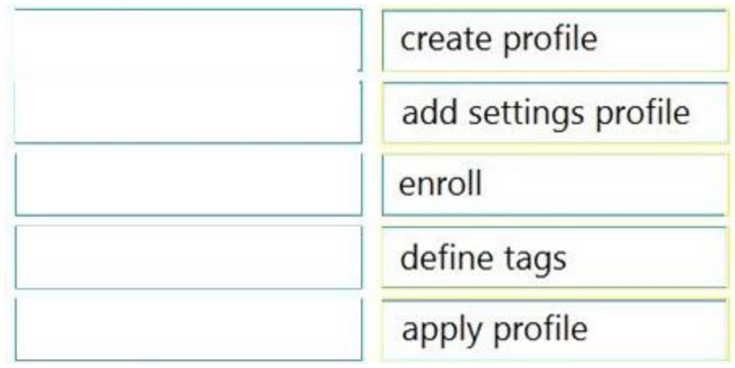
Correct Answer: D, E
Section:

QUESTION 2
DRAG DROP
Drag and drop the steps from the left into the sequence on the right to manage device control, according to Cisco Meraki best practice.

Select and Place:



Correct Answer:



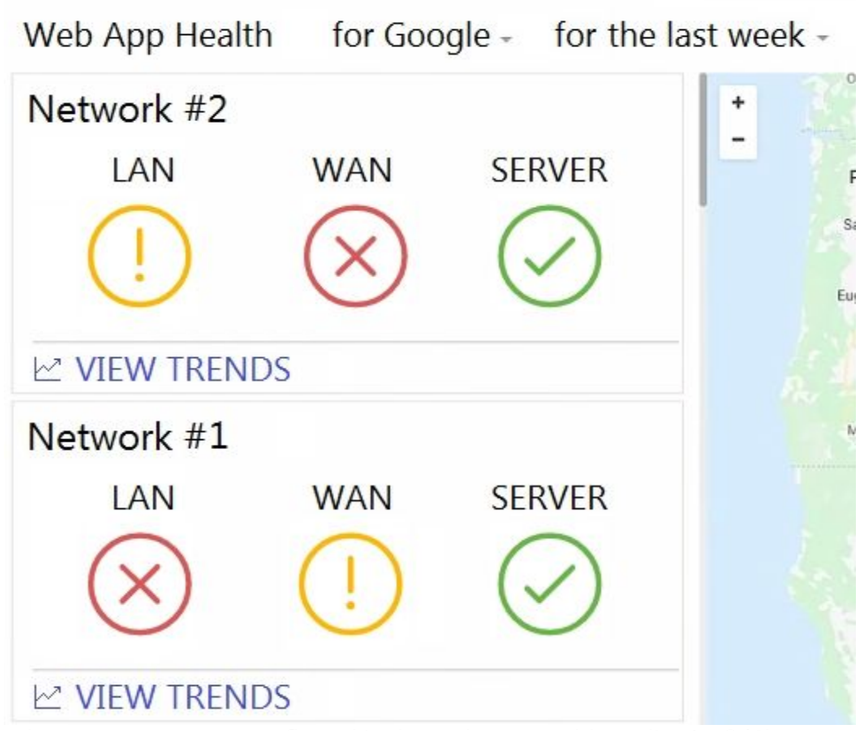
Section:
Explanation:

QUESTION 3
What is a feature of distributed Layer 3 roaming?

A. An MX Security Appliance is not required as a concentrator.
B. An MX Security Appliance is required as a concentrator.
C. All wireless client traffic can be split-tunneled.
D. All wireless client traffic is tunneled.

Correct Answer: A
Section:
Explanation:
https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/Wireless_Layer_3_Roaming_Best_Practices
This is a feature of distributed Layer 3 roaming, which maintains layer 3 connections for end devices as they roam across layer 3 boundaries without a concentrator1.The first access point that a device connects to will become the anchor access point1.

QUESTION 4
Refer to the exhibit.



What are two outcomes reflected in the Web App Health application? (Choose two.)

A. Users on both networks may be experiencing issues when attempting to reach Google.
B. Network #1 could not load Google because of a remote server issue.
C. Network #2 had better application performance than Network #1.
D. Network #2 could not load Google because of a local client misconfiguration.
E. Neither network recorded any server-side performance issues.

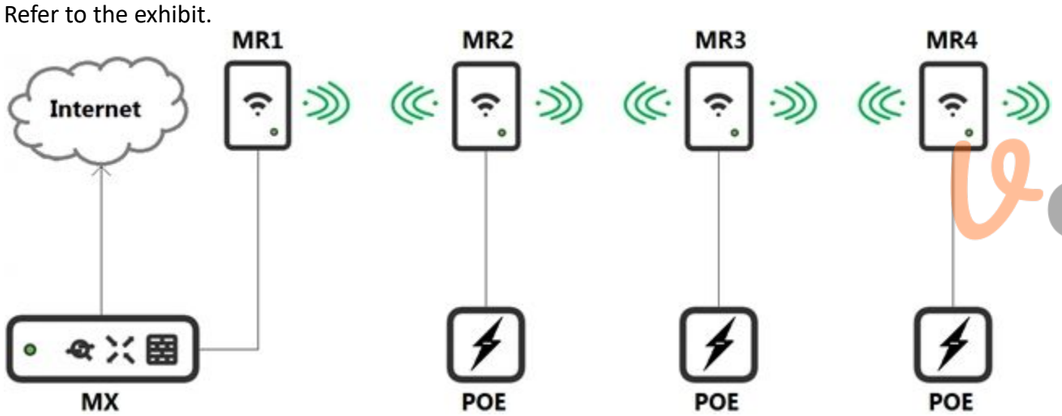
Correct Answer: A, E
Section:

QUESTION 5
What are two organization permission types? (Choose two.)

A. Full
B. Read-only
C. Monitor-only
D. Write
E. Write-only

Correct Answer: A, B
Section:
Explanation:
Managing_Dashboard_Administrators_and_Permissions

QUESTION 6
Refer to the exhibit.



Which design recommendation should be considered?

A. A 25-percent throughput loss occurs for every hop. Cisco Meraki best practice recommends a 1-hop maximum.
B. A 25-percent throughput loss occurs for every hop. Cisco Meraki best practice recommends a 2-hop maximum.
C. A 50-percent throughput loss occurs for every hop. Cisco Meraki best practice recommends a 1-hop maximum.
D. A 50-percent throughput loss occurs for every hop. Cisco Meraki best practice recommends a 2-hop maximum.

Correct Answer: C
Section:
Explanation:
https://documentation.meraki.com/MR/Deployment_Guides/Mesh_Deployment_Guide
There will be a throughput reduction (~50% reduction) with each ''hop'' in a mesh. It is recommended that a mesh network be designed for no more than one mesh hop from the gateway to client device.

QUESTION 7
Which requirement is needed to implement Fast Lane on Cisco Meraki APs?

A. wireless profile installed on an Apple iOS device

B. wireless profile installed on a Cisco iOS access point
C. adaptive 802.11r disabled
D. traffic shaping rule tagging traffic with a DSCP value of 46 to Apple.com

Correct Answer: A
Section:
Explanation:
Meraki MR Access Points, in combination with a wireless profile installed on the iOS device, will enable the Fast Lane technologies. The fastest way to install a wireless profile on an iOS device is via Meraki EMM.
https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Wireless_QoS_and_Fast_Lane
Wireless_QoS_and_Fast_Lane

QUESTION 8
Which type of authentication protocol is used when using OSPF on an MX appliance?

A. MD5
B. certificate
C. plaintext
D. SHA-1

Correct Answer: A
Section:
Explanation:
Using_OSPF_to_Advertise_Remote_VPN_Subnets

QUESTION 9
When wireless SSIDs are configured in Dashboard, which setting on the Access Control page affects the ability of a 2.4 GHz only client device from associating to the WLAN for the first time?

A. Content filtering
B. Bridge mode
C. 802.11r
D. Dual band operating with Band Steering

Correct Answer: D
Section:
Explanation:
When band steering is enabled on an SSID, APs will stop advertising that SSID in 2.4GHz beacons. Since 2.4GHz-only clients that rely on a passive scan will not ''see'' that SSID in beacons, they might not be able to join this SSID unless they do an active scan or have been pre-configured with the SSID name and security settings (for example, a pre-shared key). https://documentation.meraki.com/MR/Radio_Settings/Band_Steering

QUESTION 10
Which two actions can extend the video retention of a Cisco Meraki MV Smart Camera? (Choose two.)

A. enabling audio compression
B. installing an SSD memory extension
C. enabling motion-based retention
D. enabling maximum retention limit
E. configuring a recording schedule

Correct Answer: C, E
Section:
Explanation:
https://documentation.meraki.com/MV/Advanced_Configuration/Scheduled_Recording
By default, the Meraki security camera's will record continuously 24/7. In some situations, certain times of day are not allowed to be recorded. Scheduled recording covers this requirement as well as improve the video retention capabilities of the camera.

QUESTION 11
How does a Meraki device behave if cloud connectivity is temporarily lost?

A. The offline device continues to run with its last known configuration until cloud connectivity is restored.
B. The offline device reboots every 5 minutes until connection is restored.
C. The offline device stops passing traffic.
D. The offline device tries to form a connection with a local backup sever.

Correct Answer: A
Section:
Explanation:
What happens if a network loses connectivity to the Meraki cloud?
Because of Meraki's out of band architecture, most end users are not affected if Meraki wireless APs, switches, or security appliances cannot communicate with Meraki's cloud services (e.g., because of a temporary WAN failure):
* Users can access the local network (printers, file shares, etc.)
* If WAN connectivity is available, users can access the Internet
* Network policies (firewall rules, QoS, etc.) continue to be enforced
* Users can authenticate via 802.1X/RADIUS and can roam wirelessly between access points
* Users can initiate and renew DHCP leases
* Established VPN tunnels continue to operate
* Local configuration tools are available (e.g., device IP configuration
https://meraki.cisco.com/lib/pdf/meraki_datasheet_cloud_management.pdf

QUESTION 12
Where should a network admin navigate to investigate wireless mesh information between Meraki APs?

A. Wireless > Monitor > Access Points > AP > RF
B. Wireless > Configure > Radio Settings
C. Wireless > Monitor > Wireless Health
D. Wireless > Monitor > RF Spectrum

Correct Answer: A
Section:
Explanation:
See Monitoring Mesh section Mesh monitoring tools are located at the bottom of every AP detail page, which can be accessed by navigating to Wireless > Monitor > Access Points, then clicking on an Access Point.
https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Wireless_Mesh_Networking

QUESTION 13
What are two ways peers interact with ports that Auto VPN uses? (Choose two.)

A. For IPsec tunneling, peers use high UDP ports within the 32768 to 61000 range.

B. Peers contact the VPN registry at UDP port 9350.
C. For IPsec tunneling, peers use high TCP ports within the 32768 to 61000 range.
D. Peers contact the VPN registry at TCP port 9350.
E. For IPsec tunneling, peers use UDP ports 500 and 4500.

Correct Answer: A, B
Section:
Explanation:
Ports used to contact the VPN registry:
- Source UDP port range 32768-61000
- Destination UDP port 9350 or UDP port 9351
Ports used for IPsec tunneling:
- Source UDP port range 32768-61000
- Destination UDP port range 32768-61000
https://documentation.meraki.com/MX/Site-to-site_VPN/Meraki_Auto_VPN_-_Configuration_and_Troubleshooting_Configuration_and_Troubleshooting

QUESTION 14
What occurs when a configuration change is made to an MX network that is bound to a configuration template?

A. The configuration change in the bound network is combined with the template configuration inside the template.
B. The more restrictive configuration is preferred.
C. The configuration change in the bound network overrides the template configuration.
D. The template configuration overrides the configuration change in the bound network.

Correct Answer: C
Section:
Explanation:
https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MX_Security_and_SD-WAN/MX_Templates_Best_Practices#:~:text=policy%2C%20choose%20Save-,Local%20Overrides,will%20override%20the%20template%20configuration.

QUESTION 15
One thousand concurrent users stream video to their laptops. A 30/70 split between 2.4 GHz and 5 GHz is used.
Based on client count, how many APs (rounded to the nearest whole number) are needed?

A. 26
B. 28
C. 30
D. 32

Correct Answer: B
Section:
Explanation:
https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/High_Density_Wi-Fi_Deployments

QUESTION 16
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

Correct Answer: B
Section:
Explanation:
This is because the alert mentions 802.1X failure, which is a network access control method that is used with WPA2-enterprise and RADIUS servers1.
This question is related to the topic ofWireless Access Points Quick Startin the Cisco Meraki documentation. You can find more information about this topic in theWireless Access Points Quick Startarticle or theUsing the Cisco Meraki Device Local Status Pagepage.

QUESTION 17
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

Correct Answer: A
Section:
Explanation:
SM Sentry enrollment can be enabled on any MR network via the Splash page section of the Wireless > Configure > Access control page.
https://documentation.meraki.com/MR/MR_Splash_Page/Systems_Manager_Sentry_Enrollment

QUESTION 18
DRAG DROP
Drag and drop the descriptions from the left onto the corresponding MX operation mode on the right.

Select and Place:

The MX appliance acts as a layer 2 bridge

This mode is the default mode of operation

DHCP services can be configured on the MX appliance

VLANs cannot be configured

This mode is generally also the default gateway for devices on the LAN

This mode is not recommended at the network perimeter

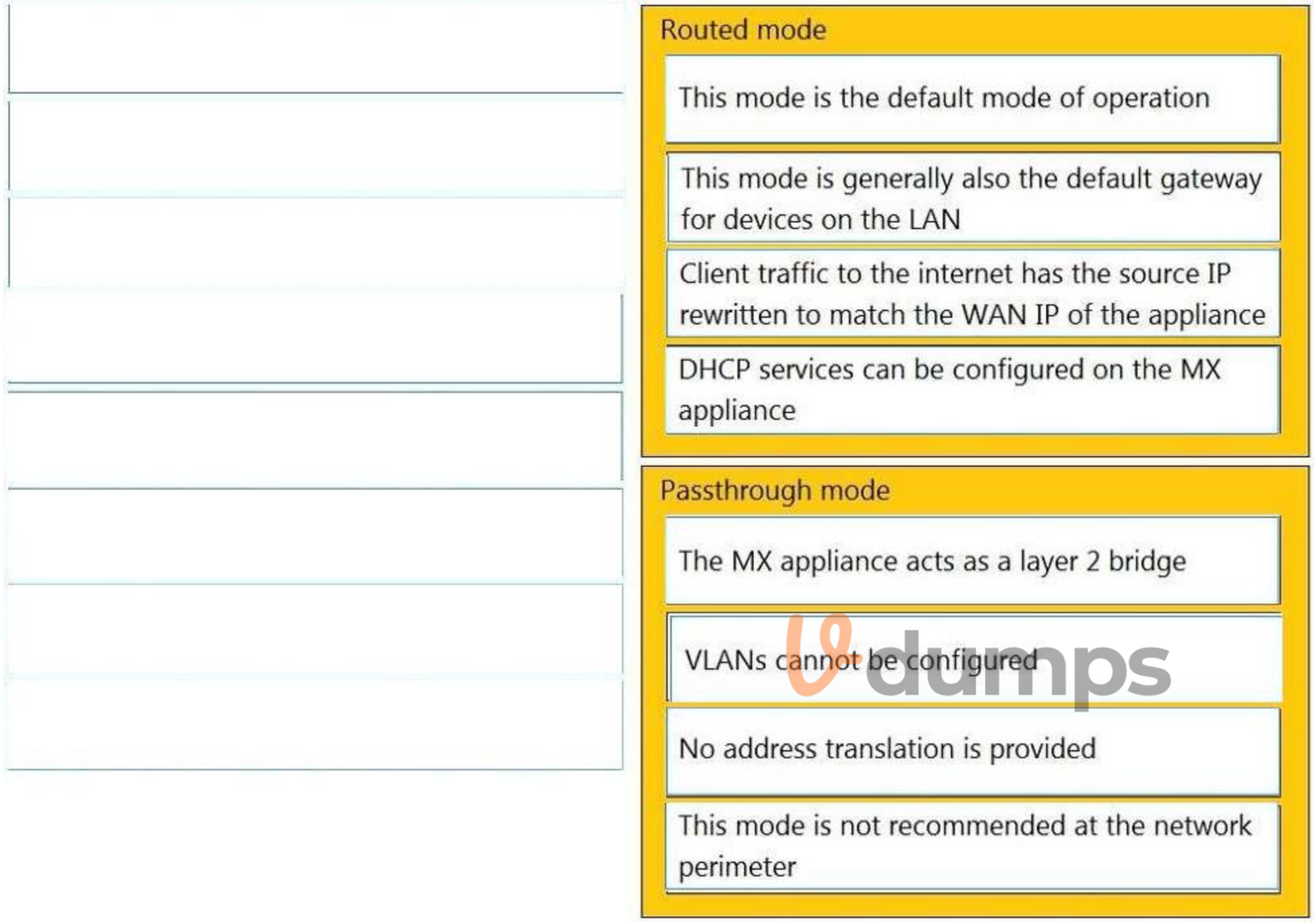
No address translation is provided

Client traffic to the internet has the source IP rewritten to match the WAN IP of the appliance

Routed mode

Passthrough mode

Correct Answer:



Section:
Explanation:

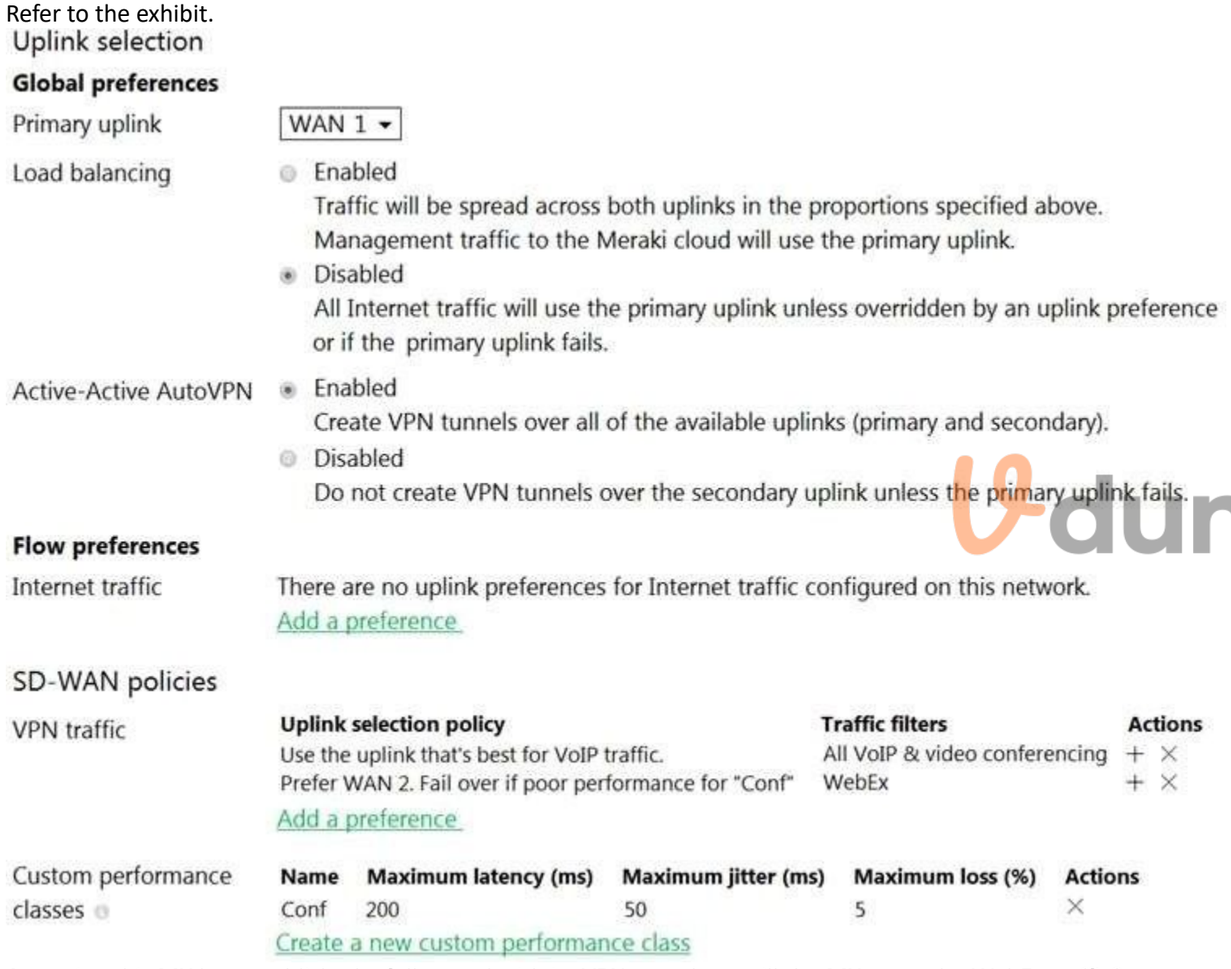
QUESTION 19
When an SSID is configured with Sign-On Splash page enabled, which two settings must be configured for unauthenticated clients to have full network access and not be allow listed? (Choose two.)

A. Controller disconnection behavior
B. Captive Portal strength
C. Simultaneous logins
D. Firewall & traffic shaping
E. RADIUS for splash page settings

Correct Answer: A, B
Section:

Explanation:
To clarify, when an SSID is configured with Sign-On Splash page enabled, the two settings that must be configured for unauthenticated clients to have full network access and not be allow listed are:
Controller disconnection behavior: This setting determines how the clients are treated when the Meraki cloud controller is unreachable. The options areRestrictedorUnrestricted. The former option blocks all traffic from unauthenticated clients until the controller is reachable again.The latter option allows unauthenticated clients to access the network without signing on until the controller is reachable again1.
Captive Portal strength: This setting determines how often the clients are redirected to the splash page for authentication. The options areBlock all access until sign-on is completeorAllow non-HTTP traffic prior to sign-on. The latter option allows unauthenticated clients to access other protocols such as DNS, DHCP, ICMP, etc., but blocks HTTP and HTTPS traffic until they sign on.This option is recommended for compatibility with devices that do not support web-based authentication1.

QUESTION 20
Refer to the exhibit.



Assuming this MX has established a full tunnel with its VPN peer, how will the MX route the WebEx traffic?

A. WebEx traffic will prefer WAN 2 as long as it meets the thresholds in the ''Conf'' performance class.
B. WebEx traffic will prefer WAN 1 as it is the primary uplink.
C. WebEx traffic will prefer WAN 2 as long as it is up.
D. WebEx traffic will be load-balanced between both active WAN links.

Correct Answer: A
Section:
Explanation:

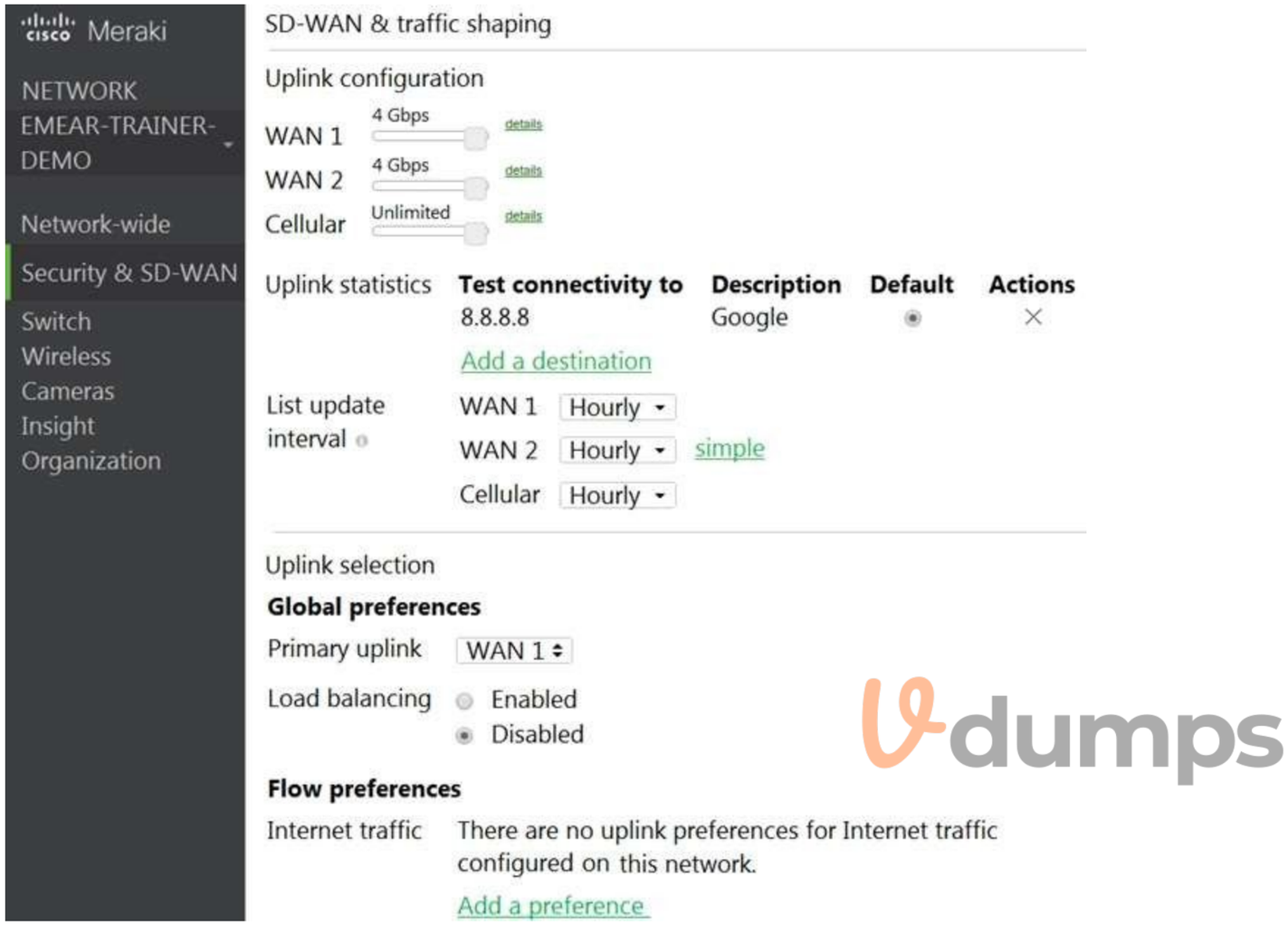
Assuming this MX has established a full tunnel with its VPN peer, the MX will route the WebEx traffic based on the SD-WAN policy configured in the exhibit. The SD-WAN policy has two performance classes:ConfandDefault.TheConfperformance class matches the traffic with destination port 9000, which is used by WebEx for VoIP and video RTP3. TheConfperformance class has a preferred uplink of WAN 2 and a failover uplink of WAN 1. It also has thresholds for latency, jitter, and loss that determine when to switch from the preferred uplink to the failover uplink. Therefore, the WebEx traffic will prefer WAN 2 as long as it meets the thresholds in theConfperformance class. If WAN 2 exceeds the thresholds or goes down, the WebEx traffic will switch to WAN 1 as the failover uplink.

QUESTION 21
For which two reasons can an organization become ''Out of License''? (Choose two.)

A. licenses that are in the wrong network
B. more hardware devices than device licenses
C. expired device license
D. licenses that do not match the serial numbers in the organization
E. MR licenses that do not match the MR models in the organization

Correct Answer: B, C
Section:
Explanation:
More hardware devices than device licenses: An organization needs to have enough device licenses to cover all the hardware devices in its network. A device license is consumed by each device that is added to the network.If the number of devices exceeds the number of licenses, the organization will be out of license and will lose access to some features and support until it purchases more licenses or removes some devices4.
Expired device license: A device license has an expiration date that depends on the license term purchased by the organization. If a device license expires, it will no longer be valid and will not count towards the license limit.The organization will need to renew the expired license or purchase a new one to avoid being out of license4.

QUESTION 22
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.

Correct Answer: C, E
Section:
Explanation:
To clarify, to optimize load balancing asymmetrically with a 4:1 ratio between links, two actions that are required are:
Enable load balancing: This option allows the MX to use both of its uplinks for load balancing.When load balancing is enabled under Security & SD-WAN > Configure > SD-WAN & Traffic shaping, traffic flows will be distributed between the two uplinks proportional to the WAN 1 and WAN 2 bandwidths specified under Uplink configuration1.
Change the assigned speeds of WAN 1 and WAN 2 so that the ratio is 4:1: The assigned speed of a WAN link is a value that indicates the bandwidth available on that link.By changing the assigned speeds of WAN 1 and WAN 2 so that they reflect the desired load-balancing ratio, the administrator can ensure that the MX uses both links efficiently and proportionally1. For example, if WAN 1 has a bandwidth of 100 Mbps and WAN 2 has a bandwidth of 25 Mbps, then setting their assigned speeds to 100 Mbps and 25 Mbps respectively will achieve a 4:1 load-balancing ratio.

QUESTION 23
Which Cisco Meraki best practice method preserves complete historical network event logs?

A. Configuring the preserved event number to maximize logging.
B. Configuring the preserved event period to unlimited.
C. Configuring a syslog server for the network.
D. Configuring Dashboard logging to preserve only certain event types.

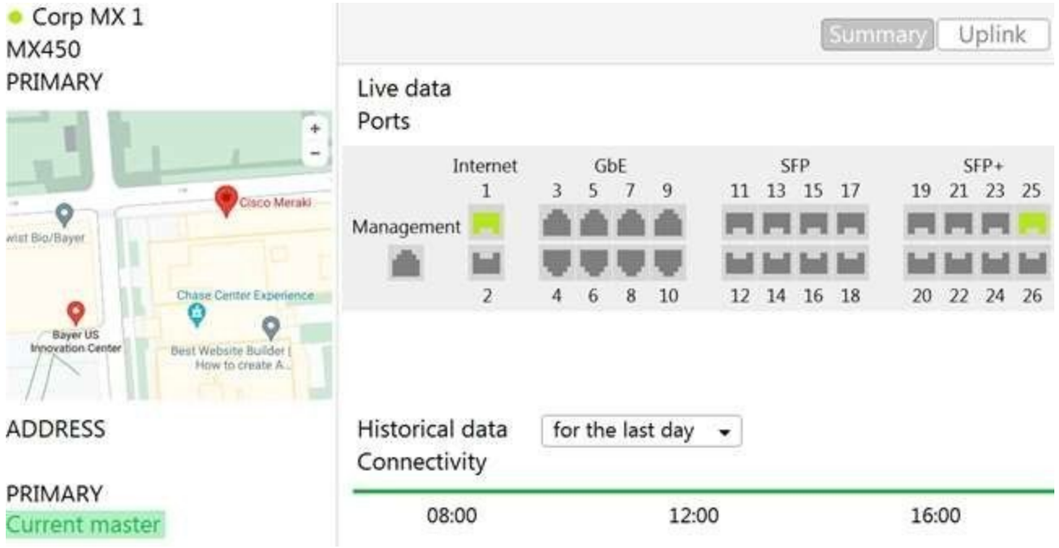
Correct Answer: C
Section:
Explanation:
Configuring a syslog server for the network is the Cisco Meraki best practice method to preserve complete historical network event logs.A syslog server can be configured to store messages for reporting purposes from MX Security Appliances, MR Access Points, and MS switches1.The syslog server can collect various types of events, such as VPN connectivity, uplink connectivity, DHCP leases, firewall rules, IDS alerts, and security events2. The syslog server can also help with troubleshooting and monitoring the network performance and security.

QUESTION 24
Which design requirement is met by implementing syslog versus SNMP?

A. when automation capabilities are needed
B. when proactive alerts for critical events must be generated
C. when organization-wide information must be collected
D. when information such as flows and client connectivity must be gathered

Correct Answer: D
Section:
Explanation:
Implementing syslog versus SNMP can meet the design requirement of gathering information such as flows and client connectivity. Syslog can collect and report various types of events, such as VPN connectivity, uplink connectivity, DHCP leases, firewall rules, IDS alerts, and security events. Syslog can also provide detailed information about the flows and client connectivity on the network devices, such as source and destination IP addresses, ports, protocols, bytes transferred, etc. SNMP, on the other hand, can collect and report various statistics and information about the network devices, such as CPU utilization, interface status, memory usage, etc. However, SNMP does not provide as much information about the flows and client connectivity as syslog does.
Meraki_Device_Reporting_-_Syslog%2C_SNMP%2C_and_API

QUESTION 25
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.

Correct Answer: C
Section:
Explanation:
Before deploying MXs as one-arm VPN concentrators, place them into Passthrough or VPN Concentrator mode on the Addressing and VLANs page. In one-armed VPN concentrator mode, the units in the pair are connected to the network 'only' via their respective 'Internet' ports. Make sure they are NOT connected directly via their LAN ports. Each MX must be within the same IP subnet and able to communicate with each other, as well as with the Meraki dashboard. Only VPN traffic is routed to the MX, and both ingress and egress packets are sent through the same interface.
https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MX_Security_and_SD-WAN/Meraki_Auto_VPN_General_Best_Practices

QUESTION 26
Refer to the exhibit.

Route table

SUBNET: Search by subnet | NAME: Search by name | TYPE: All | SORT BY: Priority

Subnet	Name	Type	Next hop
10.115.32.0/28	Store 1532 – appliance: MGMT	Meraki VPN: VLAN	Peer: Store 1532 – appliance
10.116.32.0/28	Store 1532 – appliance: DATA	Meraki VPN: VLAN	Peer: Store 1532 – appliance
192.39.2.28/32	External	BGP	10.128.124.62
192.168.70.8/29	MSP NOC	IPSec Peer	4.99.111.99
192.168.70.0/29	MSP NOC	IPSec Peer	4.100.99.100
192.39.228.0/24	External	BGP	10.128.124.62
192.168.0.0/16	External	BGP	10.128.124.62

A packet arrives on the VPN concentrator with source IP 10.168.70.3 and destined for IP 10.116.32.4.
What is the next hop for the packet, based on this concentrator routing table?

A. The concentrator gateway (10.128.124.62) is the next hop.
B. Not enough detail is available to determine the next hop.
C. The packet is stopped.
D. The Auto VPN peer ''Store 1532 -- appliance'' is the next hop.

Correct Answer: D
Section:
Explanation:
This can be determined by looking at the concentrator routing table and finding the entry for the destination IP 10.116.32.4. The next hop for this entry is the Auto VPN peer ''Store 1532 -- appliance''.
This question is related to the topic ofImplementing Dynamic Routing Protocolsin the Engineering Cisco Meraki Solutions (ECMS) official training documentation. You can find more information about this topic in theECMS v2.2 Course Overviewor theECMS1 v2.1 Course Overview.

QUESTION 27
Company iPads are enrolled in Systems Manager without supervision, and profiles are pushed through Systems Manager.
Which outcome occurs when a user attempts to remove the ''Meraki Management'' profile on an iPad?

A. The ''Meraki Management'' profile cannot be removed.
B. The ''Meraki Management'' profile is removed and then pushed automatically by Systems Manager.
C. The ''Meraki Management'' profile is removed. All the profiles that Systems Manager pushed are also removed.
D. The ''Meraki Management'' profile is removed. All the profiles Systems Manager pushed remain.

Correct Answer: C
Section:
Explanation:
On the device, navigate to Settings > General > Device Management
Select Meraki Management, and select Remove to delete the management profile and any managed configuration profiles installed via SM

QUESTION 28
Which two features and functions are supported when using an MX appliance in Passthrough mode? (Choose two.)

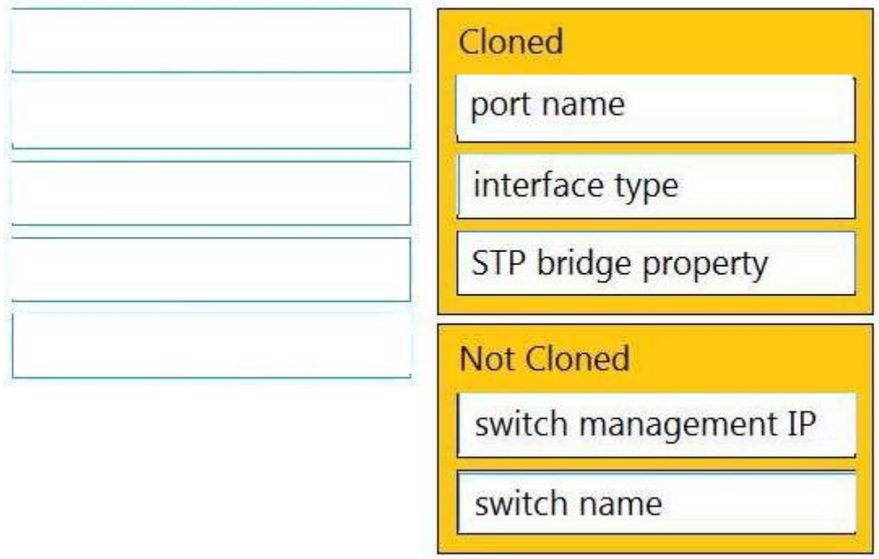
A. intrusion prevention
B. site-to-site VPN
C. secondary uplinks
D. DHCP
E. high availability

Correct Answer: A, B
Section:
Explanation:
These are the two features and functions that are supported when using an MX appliance in Passthrough mode. According to the [MX Addressing and VLANs] article, Passthrough mode allows the MX appliance to act as a layer 2 bridge, passing traffic between its LAN and WAN ports without performing any routing or address translation. However, some features such as intrusion prevention and site-to-site VPN are still available in this mode.
Passthrough_Mode_on_the_MX_Security_Appliance_and_Z-series_Teleworker_Gateway

QUESTION 29
DRAG DROP
Drag and drop the settings from the left into the boxes on the right to indicate if the setting will be cloned or not cloned using the Cisco Meraki MS switch cloning feature.

Select and Place:

Correct Answer:



Section:
Explanation:

QUESTION 30
Refer to the exhibit.

License information for Home

License status	OK
License expiration	May 20, 2029 (3593 days from now)
MX advanced Security	Enabled
System Manager	Enabled (paid)

	License limit	Current device count
MS220-8P	1	1
MV	2	0
MX64	1	1
Systems Manager Agent	100	0
Wireless AP	7	1
MV-SEN	10 free	0

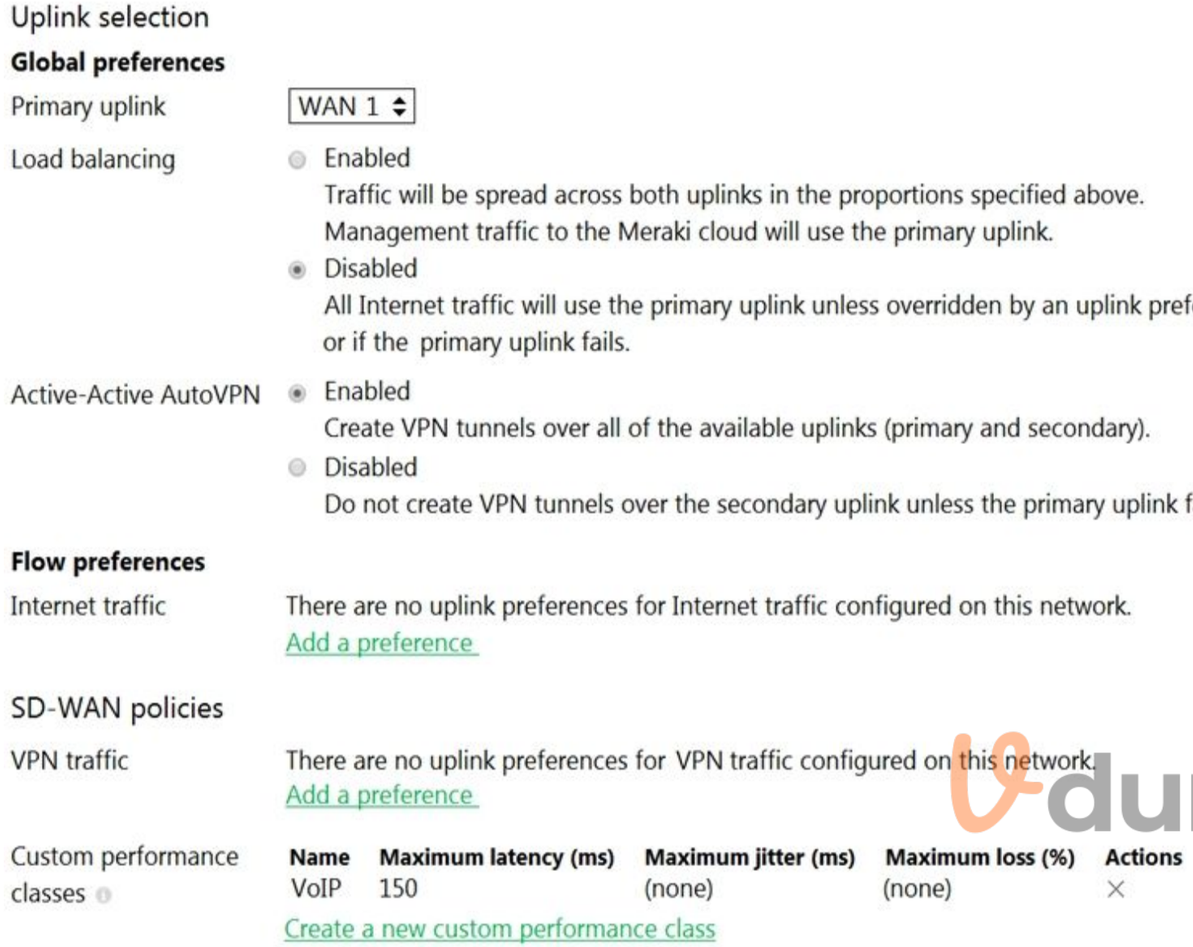
Add another license

This Dashboard organization uses Co-Termination licensing model.
What happens when an additional seven APs are claimed on this network without adding licenses?

A. All APs immediately stop functioning.
B. All network devices stop functioning in 30 days.
C. One AP Immediately stops functioning.
D. All APs stop functioning in 30 days.

Correct Answer: B
Section:
Explanation:
The number of devices in an organization can not exceed the license limits. If this occurs, the organization will enter a 30-day grace period, during which the organization must be brought back into compliance, otherwise it will be shut down until proper licensing is applied to the organization. https://documentation.meraki.com/General_Administration/Licensing/Meraki_Co-Termination_Licensing_Overview

QUESTION 31
Refer to the exhibit.



What does the MX Security Appliance send to determine whether VPN traffic exceeds the configured latency threshold in the VoIP custom performance class?

A. 1000-byte TCP probes every second, through VPN tunnels that are established over the primary WAN link.
B. 100-byte UDP probes every second, through VPN tunnels that are established over every WAN link.
C. 100-byte UDP probes every second, through VPN tunnels that are established over the primary WAN link.
D. 1000-byte TCP probes every second, through VPN tunnels that are established over every WAN link.

Correct Answer: B
Section:
Explanation:
The performance probe is a small payload (approximately 100 bytes) of UDP data sent over all established VPN tunnels every 1 second. MX appliances track the rate of successful responses and the time that elapses before receiving a response. This data allows the MX to determine the packet loss, latency, and jitter over each VPN tunnel in order to make the necessary performance-based decisions.
https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MX_Security_and_SD-WAN/Meraki_SD-WAN#Performance_Probes

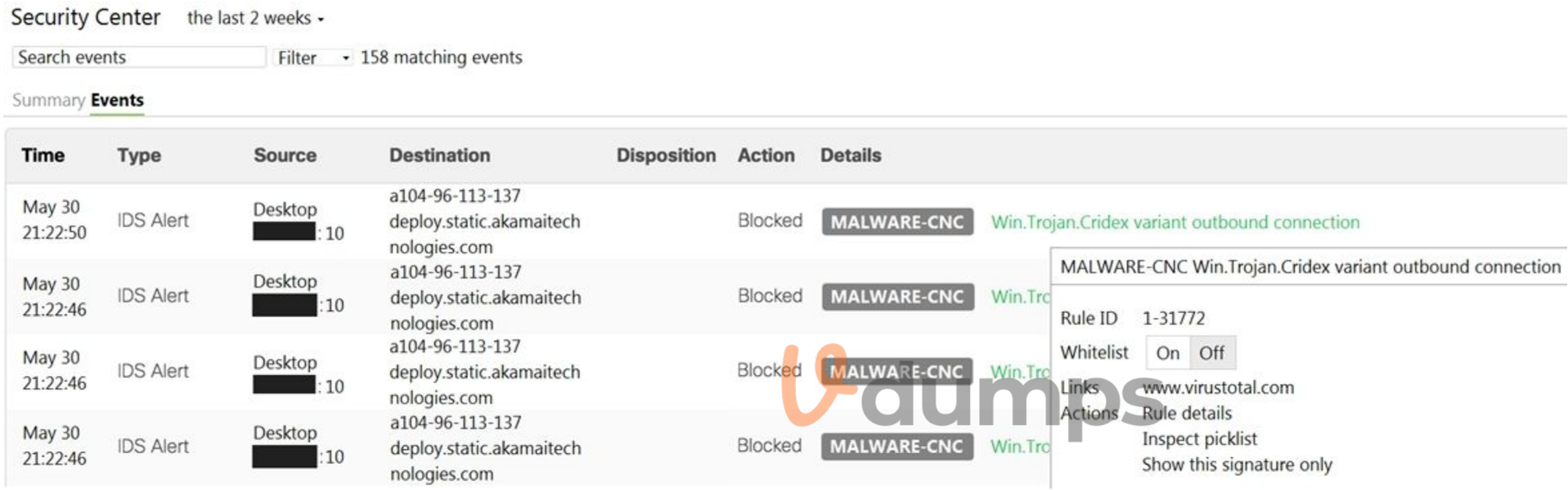
QUESTION 32
What is the role of the Meraki Dashboard as the service provider when using SAML for single sign-on to the Dashboard?

A. The Dashboard generates the SAML request.
B. The Dashboard provides user access credentials.

C. The Dashboard parses the SAML request and authenticates users.
D. The Dashboard generates the SAML response.

Correct Answer: C
Section:
Explanation:
https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Configuring_SAML_Single_Sign-on_for_Dashboard

QUESTION 33
Refer to the exhibit.



Which IDS/IPS mode is the MX Security Appliance configured for?

A. quarantine
B. prevention
C. detection
D. blocking

Correct Answer: B
Section:
Explanation:
You can enable intrusion prevention by setting the Mode drop-down to Prevention under Security & SD-WAN > Configure > Threat protection > Intrusion detection and prevention. Traffic will be automatically blocked by best effort if it is detected as malicious based on the detection ruleset specified above. https://documentation.meraki.com/MX/Content_Filtering_and_Threat_Protection/Threat_Protection

QUESTION 34
What are two roles of the network and device tags in a Dashboard? (Choose two.)

A. Tags enable administrators to configure a combination of network and device specific tags to create summary reports filtered for specific devices across multiple networks.
B. Network tags can be used to assign networks to separate Auto VPN domains in an Organization with many networks.
C. Network tags can be used to simplify the assignment of network-level permissions in an Organization with many networks.
D. Device tags can be used to simplify the assignment of device-level permissions in an Organization with many administrators.

E. Device tags can be assigned to MR APs to influence the gateway selection for repeaters in a mesh wireless network.

Correct Answer: A, C
Section:
Explanation:
See Permissions by Network Tag section To simplify the assignment of network-level permissions in an organization with many networks, permissions can be granted to users for a given network tag.
https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Managing_Dashboard_Administrators_and_Permissions
The Organization > Configure > Manage Tags page allows Administrators to configure a combination of Network and Device specific tags to create Summary Reports filtered for specific devices across multiple networks.
https://documentation.meraki.com/General_Administration/Organizations_and_Networks/Organization_Menu/Manage_Tags

QUESTION 35
Refer to the exhibit.

Outbound rules

#	Policy	Protocol	Source	Src port	Destination	Dst port	Comment	Logging	Hits	Actions
	Allow	Any	Any	Any	Any	Any	Default rule	Enabled	2	

Add a rule

Which outcome occurs when logging is set to Enabled?

A. Outbound flows are sent to a configured syslog server if a syslog sender is configured for flows.
B. The hits counter within this section is now enabled.
C. This firewall rule is now enabled.
D. Inbound flows are sent to a configured syslog server if a syslog server configured for flows.

Correct Answer: A
Section:
Explanation:
'Inbound and outbound flows will generate a syslog message showing the source and destination along with port numbers and the firewall rule that they matched. For inbound rules, 1=deny and 0=allow.'
https://documentation.meraki.com/General_Administration/Monitoring_and_Reporting/Syslog_Server_Overview_and_Configuration

QUESTION 36
A Cisco Meraki MX security appliance is trying to route a packet to the destination IP address of 172.18.24.12. Which routes contained in its routing table does it select?

A. Auto VPN route 172.18.0.0/16
B. static route 172.16.0.0/12
C. non-Meraki VPN route 172.18.24.0/24
D. directly connected 172.18.16.0/20

Correct Answer: C
Section:
Explanation:
Route Priority
Each type of route configured on the MX has a specific priority in comparison with other types of routes. The priority is as follows:
Directly Connected
Client VPN
Static Routes
AutoVPN Routes
Non-Meraki VPN Peers
BGP learned Routes

NAT*
https://documentation.meraki.com/MX/Networks_and_Routing/MX_Routing_Behavior

QUESTION 37
A Cisco Meraki MV camera is monitoring an office and its field of vision currently captures work desks and employee computer screens. However, recording employee computer screens is prohibited by local regulation. Which feature in Dashboard can be used to preserve the current position of the camera while also meeting regulation requirements?

A. zone exclusion
B. privacy window
C. area or interest
D. sensor crop
E. restricted mode

Correct Answer: B
Section:
Explanation:
https://documentation.meraki.com/MV/Initial_Configuration/Privacy_Windows

QUESTION 38
Which Cisco Meraki product must be deployed in addition to Systems Manager so that Systems Manager Sentry enrollment can be used?

A. MS Switch
B. Meraki Insight
C. MR Access Point
D. MV Smart Camera

Correct Answer: C
Section:
Explanation:
https://documentation.meraki.com/MR/MR_Splash_Page/Systems_Manager_Sentry_Enrollment

QUESTION 39
Which information do the MXs in a High Availability pair share?

A. spanning-tree state
B. time synchronization state
C. DHCP association database
D. stateful firewall database

Correct Answer: C
Section:
Explanation:
DHCP Synchronization To prevent a scenario in which an IP address is assigned by the primary via DHCP and then that same address is assigned to another client by the secondary after a failover, the DHCP lease table is synchronized regularly between the primary and secondary over UDP port 3483. https://documentation.meraki.com/MX/Deployment_Guides/MX_Warm_Spare_-_High_Availability_Pair

QUESTION 40

Which VLAN is used to source pings across the site-to-site VPN when using the MX Live tools?

A. highest VLAN ID that is configured and set to NO to use VPN
B. lowest VLAN ID that is configured and set to YES to use VPN
C. highest VLAN ID that is configured and set to YES to use VPN
D. lowest VLAN ID configured and set to NO to use VPN

Correct Answer: C
Section:
Explanation:
See Behavior - Firmware MX 15.11 or Lower section For MXs running firmware MX15.11 or below, the source IP that MX uses while pinging a destination is the MX IP of highest VLAN ID. If the destination is across a VPN, the MX uses the MX IP of highest VLAN ID participating in VPN. For MXs running firmware MX 15.12+, additional ping options have been added to the live tool. The ping tool now has a drop down to select the source IP address for pinging destinations from the MX. https://documentation.meraki.com/General_Administration/Tools_and_Troubleshooting/Using_the_Ping_Live_Tool

QUESTION 41
A new application needs to be pushed to all iOS devices. Some devices report ''NotNow'' in the event log and do not install the application.
What does the ''NotNow'' event indicate?

A. The application requires the most recent iOS version.
B. The device is locked with a passcode.
C. The device cannot connect to Apple servers.
D. The device cannot connect to Cisco Meraki servers.

Correct Answer: B
Section:
Explanation:
The error message ''NotNow'' is seen in the Event Log on an iOS device's details page when an action cannot be performed because the device is locked with a passcode. These actions include pushing managed apps, installing profiles, and other actions. When this occurs the device will attempt to re-connect with the MDM server as soon as the device is unlocked in order to retry the action.
https://documentation.meraki.com/SM/Monitoring_and_Reporting/Status_of_%22NotNow%22_in_Systems_Manager_Event_Log