www.atmicnetworks.com

ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

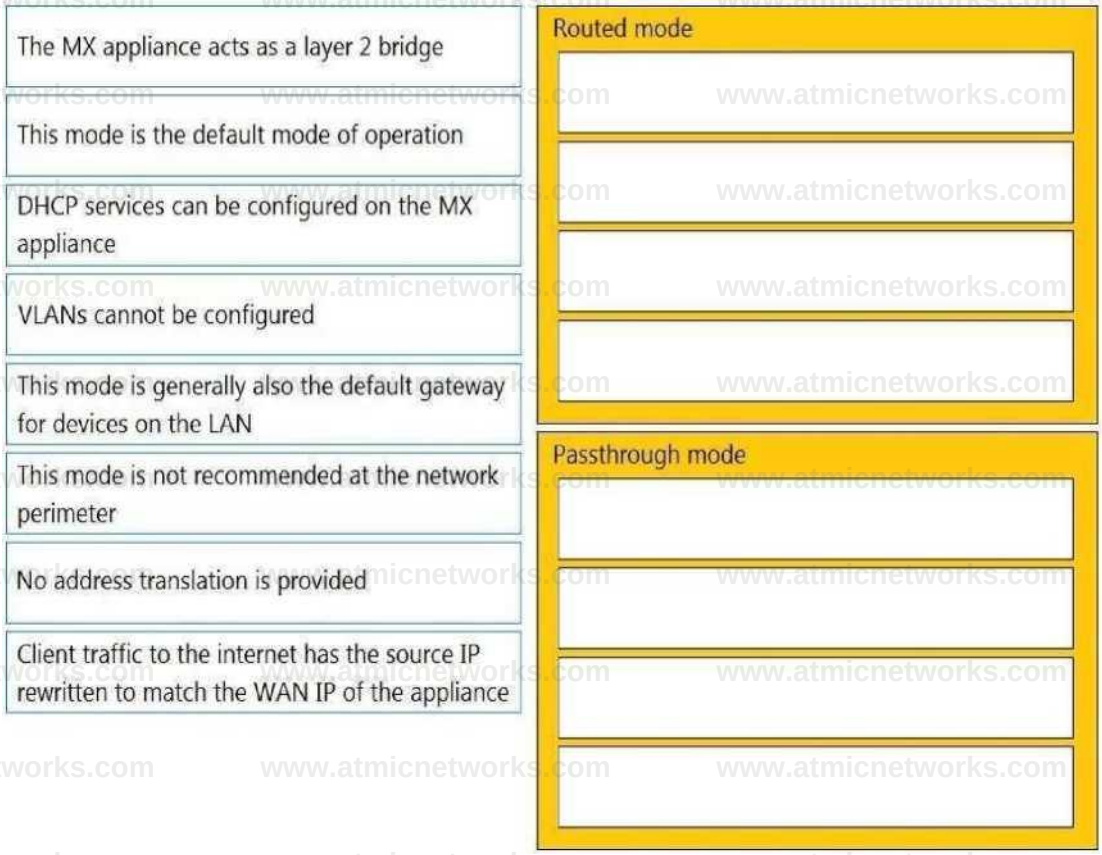
www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

DRAG DROP

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



Answer:

Explanation:

Routed Mode:
This mode is the default mode of operation

This mode is generally also the default gateway for devices on the LAN
Client traffic to the internet has the source IP rewritten to match the WAN IP of the appliance
DHCP services can be configured on the MX appliance
Passthrough Mode:
The MX appliance acts as a layer 2 bridge
VLANs cannot be configured
No address translation is provided
This mode is not recommended at the network perimeter
This question is related to the topic of MX Addressing and VLANs in the Cisco Meraki documentation.
You can find more information about this topic in the MX Addressing and VLANs article or the General MX Best Practices page.

Question: 2

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

Answer: AB

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 are Restricted or Unrestricted. 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 are Block all access until sign-on is complete or Allow 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.

Reference: https://documentation.meraki.com/MR/Access_Control

Question: 3

Refer to the exhibit.

www.atmicnetworks.com

Uplink selection

Global preferences

Primary uplink: WAN 1 r l

Load balancing:

- Enabled
  Traffic will be spread across both uplinks in the proportions specified above.
  Management traffic to the Meraki cloud will use the primary uplink.
- Disabled
  All Internet traffic will use the primary uplink unless overridden by an uplink preference or if the primary uplink fails.

Active-Active AutoVPN:

- Enabled
  Create VPN tunnels over all of the available uplinks (primary and secondary).
- Disabled
  Do not create VPN tunnels over the secondary uplink unless the primary uplink fails.

Flow preferences

Internet traffic: There are no uplink preferences for Internet traffic configured on this network. Add a preference

SD-WAN policies

VPN traffic

Uplink selection policy	Traffic filters	Actions
Use the uplink that's best for VoIP traffic	All VoIP & video conferencing	+ X
Prefer WAN 2. Fail over if poor performance for "Conf"	WebEx	+ X
Add a preference		

Custom performance classes

Name	Maximum latency (ms)	Maximum jitter (ms)	Maximum loss (%)	Actions
Conf	200	50	5	X

Create a new custom performance class

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.

Answer: A

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: Conf and Default. The Conf performance class matches the traffic with destination port 9000, which is used by WebEx for VoIP and video RTP3. The Conf performance 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 the Conf performance class. If WAN 2 exceeds the thresholds or goes down, the WebEx traffic will switch to WAN 1 as the failover uplink.

Question: 4

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

www.atmicnetworks.com

Answer: BC

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.

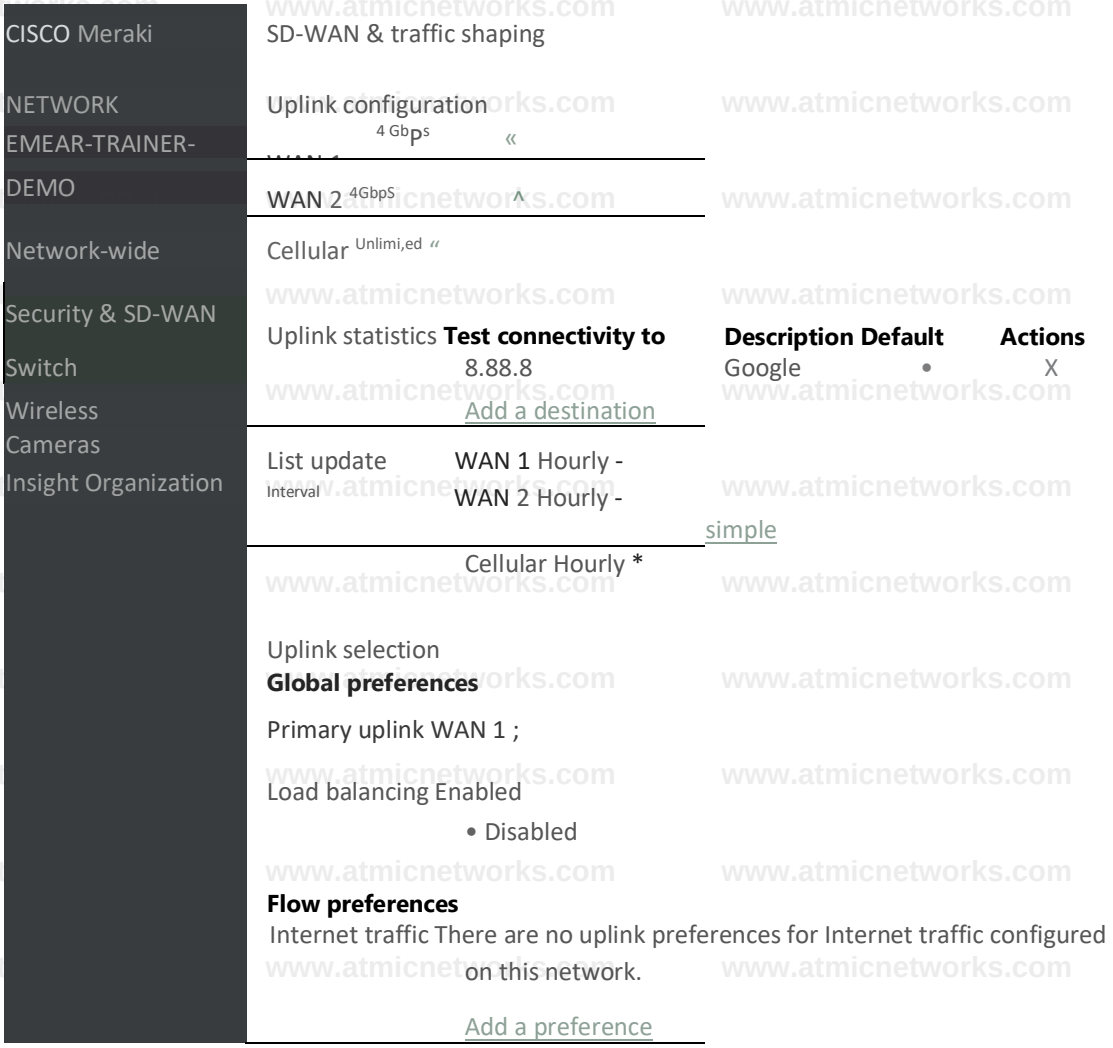
Expired device license: A device license has an expiration date that depends on the license term purchased by the organization. If a device license expires, it will no longer be valid and will not count towards the license limit. The organization will need to renew the expired license or purchase a new one to avoid being out of license4.

Reference:

https://documentation.meraki.com/General_Administration/Licensing/Meraki_Licensing_FAQs

Question: 5

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: CE

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: 6

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.

Answer: C

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: 7

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

Answer: D

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.

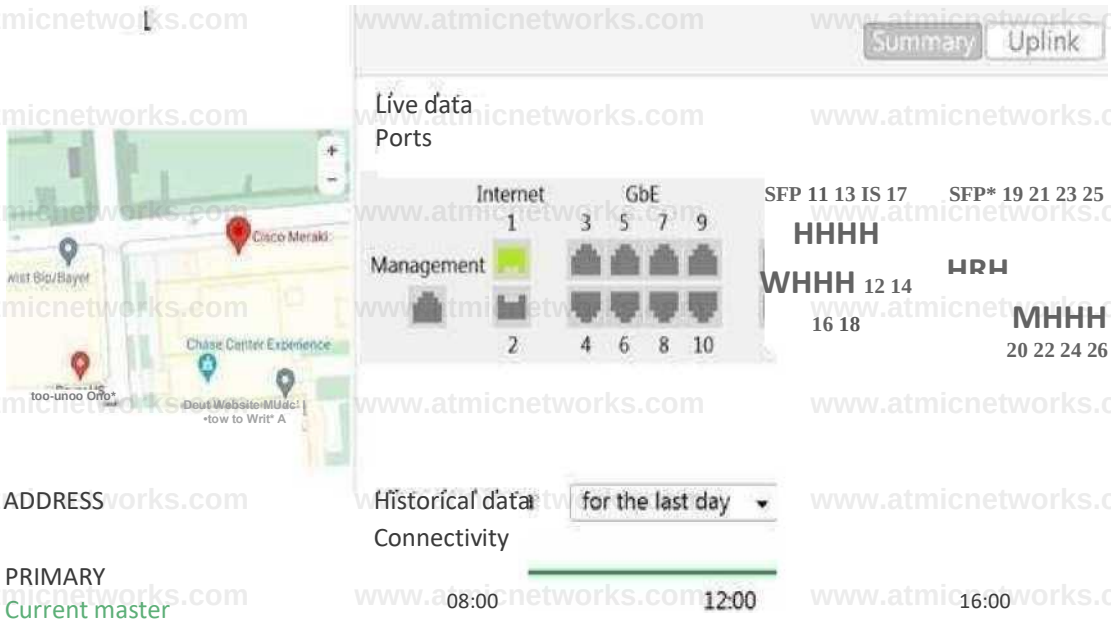
Reference:

https://documentation.meraki.com/General_Administration/Monitoring_and_Reporting/ Meraki_Device_Reporting_-_Syslog%2C_SNMP%2C_and_API

Question: 8

Refer to the exhibit.

Corp MX 1



PRIMARY
Current master

MX450
PRIMARY

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:

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: 9

Refer to the exhibit.

Route table

SUBNET NAME TYPE SORT BY ♦>

| Search by subnet | | Search by name) [All ~| | Priority j

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.

Answer: D

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 of Implementing Dynamic Routing Protocols in the Engineering Cisco Meraki Solutions (ECMS) official training documentation. You can find more information about this topic in the ECMS v2.2 Course Overview or the ECMS1 v2.1 Course Overview.

Question: 10

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.

Answer: C

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: 11

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

Answer: AB

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.

Reference: https://documentation.meraki.com/MX/Networks_and_Routing/Passthrough_Mode_on_the_MX_Security_Appliance_and_Z-series_Teleworker_Gateway

Question: 12

Refer to the exhibit.

What are the Loss and Average Latency statistics based on?

A. responses that the MX appliance receives on the connectivity-testing hostnames on the Insight > Web App Health page
B. responses that the MX appliance receives on the connectivity-testing IP addresses on the Security & SD- WAN > Firewall page
C. responses that the MX appliance receives on the connectivity-testing IP address that is configured on the Security & SD-WAN > SD-WAN & Traffic Shaping page
D. responses that the MX appliance receives on the connectivity-testing IP addresses on the Help > Firewall info page

Answer: C

Explanation:
Quote from referred documentation-Link: Loss and latency will be determined over the configured IP address under Security and SD-WAN > SD-WAN and Traffic Shaping > Uplink Statistics. If no IP is configured, these values will be measured against 8.8.8.8 by default. On the WAN Health page, all the configured IP address statistics can be reviewed by changing the destination under the "Ping Destination" column.
https://documentation.meraki.com/MI/MI_WAN_Health#:~:text=Current%20loss%20and%20latency%20statistics,address%20is%20set%20to%208.8.

Question: 13

In an organization that uses the Co-Termination licensing model, which two operations enable licenses to be applied? (Choose two.)

A. Renew the Dashboard license.
B. License a network.
C. License more devices.
D. Call Meraki support.

E. Wait for the devices to auto-renew.

Answer: A, C

Explanation:

There are two operations in which a license can be applied, License more devices or Renew my dashboard license. This article will compare both operations and describe their behaviors.
https://documentation.meraki.com/General_Administration/Licensing/Meraki_Licensing_-_License_More_Devices_vs_Renewal
These are the two operations that enable licenses to be applied in an organization that uses the CoTermination licensing model.
According to the Meraki Co-Termination Licensing Overview, there are two ways to add licenses to an organization:
Renewing the Dashboard license: This option allows you to extend the co-termination date of your organization by purchasing new licenses for the same or longer term as your existing licenses. You can renew your Dashboard license from the Organization > Configure > License Info page or from the Meraki Dashboard homepage.
Licensing more devices: This option allows you to add new devices to your organization by purchasing new licenses for them. You can license more devices from the Organization > Inventory page or from the Meraki Dashboard homepage.

Question: 14

Which two Systems Manager Live tools are available only for Apple Macs and Windows PCs and cannot be used on iOS or Android mobile devices? (Choose two.)

A. OS updates
B. Send notification
C. Selective wipe
D. Screenshot
E. Remote Desktop

Answer: DE

Explanation:

https://documentation.meraki.com/SM/Monitoring_and_Reporting/MDM_Commands_in_Systems_Manager - Under Live Tools
Selective Wiping is only for MacOS. Here we have Windows Laptop as well
Reference: https://documentation.meraki.com/SM/Other_Topics/Systems_Manager_FAQ

Question: 15

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.

Answer: AB

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

Reference: https://documentation.meraki.com/MX/Site-to-site_VPN/Meraki_Auto_VPN_-_Configuration_and_Troubleshooting

Question: 16

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.

Answer: C

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: 17

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

Answer: B

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: 18

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:

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 of Wireless Access Points Quick Start in the Cisco Meraki documentation. You can find more information about this topic in the Wireless Access Points Quick Start article or the Using the Cisco Meraki Device Local Status Page page.

Question: 19

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

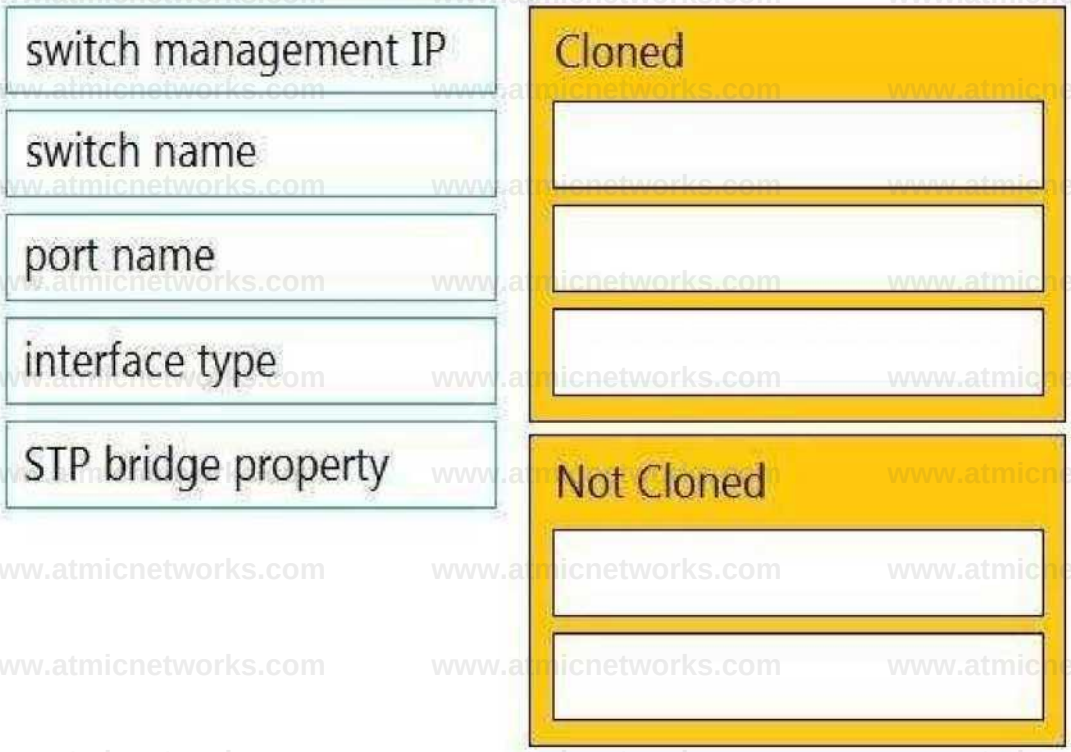
Explanation:

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: 20

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.



Answer:

Explanation:

The settings that will be cloned using the Cisco Meraki MS switch cloning feature are: port name interface type STP bridge property

The settings that will not be cloned using the Cisco Meraki MS switch cloning feature are: switch management IP switch name

Question: 21

Refer to the exhibit.

License information for Home

License status	1211	
License expiration MX	May 20, 2029 (3593 days from now)	
advanced Security System	Enabled	
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.

Answer: B

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: 22

Refer to the exhibit.

Uplink selection

Global preferences

Primary uplink: WAN 1

Load balancing:
- Enabled
  Traffic will be spread across both uplinks in the proportions specified above.
  Management traffic to the Meraki cloud will use the primary uplink.
- Disabled
  All Internet traffic will use the primary uplink unless overridden by an uplink preference or if the primary uplink fails.

Active-Active AutoVPN:
- Enabled
  Create VPN tunnels over all of the available uplinks (primary and secondary).
- Disabled
  Do not create VPN tunnels over the secondary uplink unless the primary uplink fails.

Flow preferences

Internet traffic: There are no uplink preferences for Internet traffic configured on this network. Add a preference

SD-WAN policies

VPN traffic: There are no uplink preferences for VPN traffic configured on this network. Add a preference

Custom performance classes:

Name	Maximum latency (ms)	Maximum jitter (ms)	Maximum loss (%)	Actions
VoIP	150	(none)	(none)	X

Create a new custom performance class

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.

Answer: B

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: 23

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.

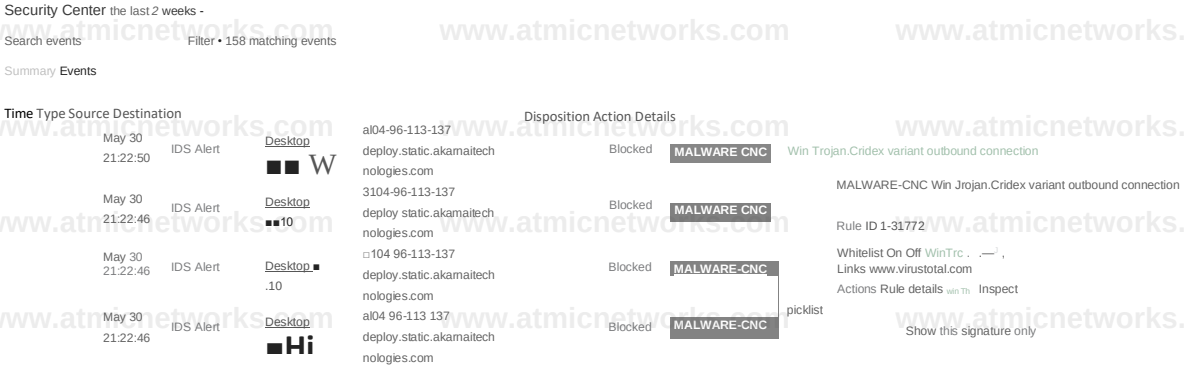
Answer: C

Explanation:

https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Configuring_SAML_Single_Sign-on_for_Dashboard

Question: 24

Refer to the exhibit.



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

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

Answer: B

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_Protectio n

Question: 25

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

Answer: DE

Explanation:

Reference: https://cloudcontrolled.uk/wp-content/uploads/2018/08/MerakiInsight.pdf (04)

Question: 26

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.

enroll	
create profile	2
add settings profile	3
define tags	4
apply profile	5

Answer:

Explanation:

Question: 27

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.

Answer: A

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: 28

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.

Answer: AE

Explanation:

Question: 29

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

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

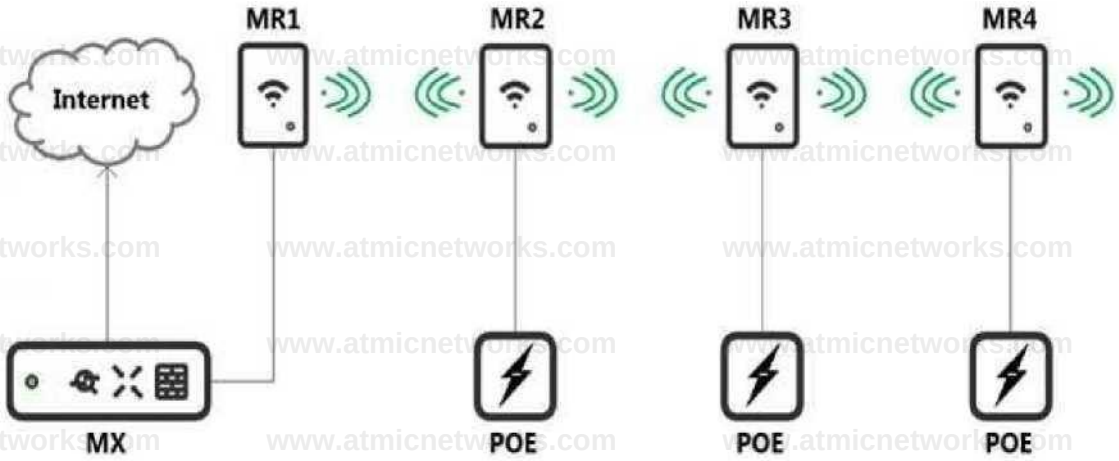
Answer: AB

Explanation:

Reference:
https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Managing_Dashboard_Administrators_and_Permissions

Question: 30

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.

Answer: C

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: 31

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.

Answer: AC

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: 32

Refer to the exhibit.

Outbound rules

#	Policy	Protocol	Source	Src port	Destination	Dst port	Comment	Logging	Hits	Actions
	Allow	Any	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.

Answer: A

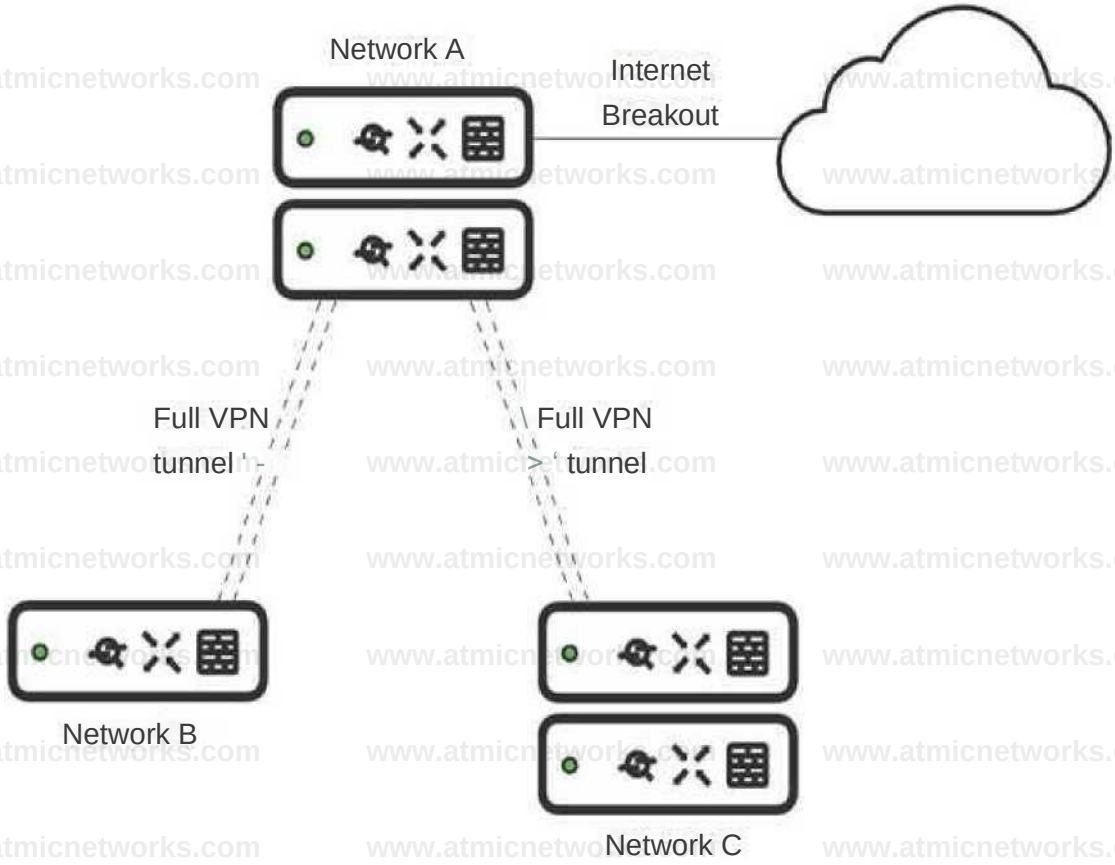
Explanation:

"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: 33

Refer to the exhibit.



What is the minimal Cisco Meraki Insight licensing requirement?

A. A single Meraki Insight license must be configured on network A to gain Web App Health visibility on network B.

B. A single Meraki Insight license must be configured on network B to gain Web App Health visibility on network B.

C. A single Meraki Insight license must be configured on network A, and a single license must be configured on network B, to gain Web App Health visibility on network B.

D. Two Meraki Insight licenses must be configured on network A to gain Web App Health visibility on network B.

E. Two Meraki Insight licenses must be configured on network A and a single license must be configured on network B, to gain Web App Health visibility on network B.

Answer: B

Explanation:

If you only need traffic statistics from your spoke site clients then you only need to enable insight on the spoke network as the hub site will not gather data for remote sites.

https://community.meraki.com/t5/Wireless-LAN/Meraki-Insight-Licensing/m-p/152684

A license is only required for those networks where Meraki Insight functionality is desired. One license is required per network, regardless of whether that network has a single MX or HA pair. Licenses can be moved between networks, but historical data for the old network will be lost. https://meraki.cisco.com/lib/pdf/meraki_datasheet_mi.pdf

Question: 34

Air Marshal has contained a malicious SSID.

What are two effects on connectivity? (Choose two.)

A. Currently associated clients stay connected.
B. New clients can connect.
C. Currently associated clients are affected by restrictive traffic shaping rules.
D. New clients cannot connect.
E. Currently associated clients are disconnected.

Answer: DE

Explanation:

When a rogue access point is contained, clients will be unable to connect to the rogue AP.
Additionally, any currently associated clients will lose their connection to the rogue AP.
https://documentation.meraki.com/MR/Monitoring_and_Reporting/Air_Marshal

Question: 35

What is the best practice Systems Manager enrollment method when deploying corporate-owned iOS devices?

A. manual
B. Apple Configurator
C. Sentry enrollment
D. DEP

Answer: D

Explanation:

iOS devices that are using Apple's Device Enrollment Program (DEP) can be supervised and enrolled over-the-air anytime they are factory reset. DEP is the best way to permanently force your devices to be owned and managed by your organization, and it is important to assign your DEP settings properly before deployment.
https://documentation.meraki.com/SM/Device_Enrollment/Enrolling_and_Supervising_iOS_Devices_using_Apple_Configurator_2.5_or_Later#:~:text=DEP%20is%20the%20best%20way,DEP%20settings%20properly%20before%20deployment.

Question: 36

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: D

Explanation:

https://documentation.meraki.com/Architectures_and_Best_Practices/Auto_VPN_Hub_Deployment_Recommendations

This is the number of tunnels that each hub needs to support in 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. This can be calculated by using the formula for the hub tunnel count in a hub-and- spoke topology1:

Hub Tunnel Count = (H x (H - 1) / 2 x L1) + (H x S x L1 x L2)

Where H is the number of hubs, S is the number of spokes, L1 is the number of uplinks for the hubs, and L2 is the number of uplinks for the spokes. In this case, H = 2, S = 50, L1 = 2, and L2 = 1.

Therefore,

Hub Tunnel Count = (2 x (2 - 1) / 2 x 2) + (2 x 50 x 2 x 1) Hub Tunnel Count = (2 x 1 / 2 x 2) + (200 x 2)

Hub Tunnel Count = (2 / 2 x 2) + (400) Hub Tunnel Count = (1 x 2) + (400) Hub Tunnel Count = 2 + 400 Hub Tunnel Count = 402

This question is related to the topic of Auto VPN Hub Deployment Recommendations in the Cisco Meraki documentation. You can find more information about this topic in the Auto VPN Hub Deployment Recommendations article or the Meraki Auto VPN General Best Practices page.

Question: 37

Which order is accurate for a firmware upgrade on MX appliances in a high-availability configuration?

A. starts on the secondary MX appliance and then occurs on the primary MX appliance

B. starts on both MX appliances at the same time and then reboots both appliances after traffic on the primary MX appliance ceases

C. starts on both MX appliances at the same time and then immediately reboots both appliances

D. starts on the primary MX appliance and then occurs on the secondary MX appliance

Answer: D

Explanation:

Reference: https://community.meraki.com/t5/Security-SD-WAN/Firmware-Update-to-HA-unit/td- p/47865

Question: 38

How is high-availability supported for Cisco Meraki devices?

A. Only the MX Security Appliances that use VRRP support high availability.

B. An active/active high-availability pair is recommended for MX Security Appliances.

C. The MX Security Appliances and MS Series Switches that use VRRP support an active/passive high-availability pair.

D. The MX Security Appliances and MS Series Switches that use HSRP support an active/passive high- availability pair.

Answer: C

Explanation:

https://documentation.meraki.com/MS/Layer_3_Switching/MS_Warm_Spare_(VRRP)_Overview

Question: 39

Which three verbs of request are available in the Cisco Meraki API? (Choose three.)

A. SET

B. PUT
C. PATCH
D. ADD
E. POST
F. GET

Answer: BEF

Explanation:

Verbs in the API follow the usual REST conventions:

GET returns the value of a resource or a list of resources, depending on whether an identifier is specified.
POST adds a new resource
PUT updates a resource
DELETE removes a resource

https://documentation.meraki.com/General_Administration/Other_Topics/Cisco_Meraki_Dashboard_API

Question: 40

A customer wants to use Microsoft Azure to host corporate application servers.

Which feature does the customer get by using a vMX appliance rather than connecting directly to Azure by VPN?

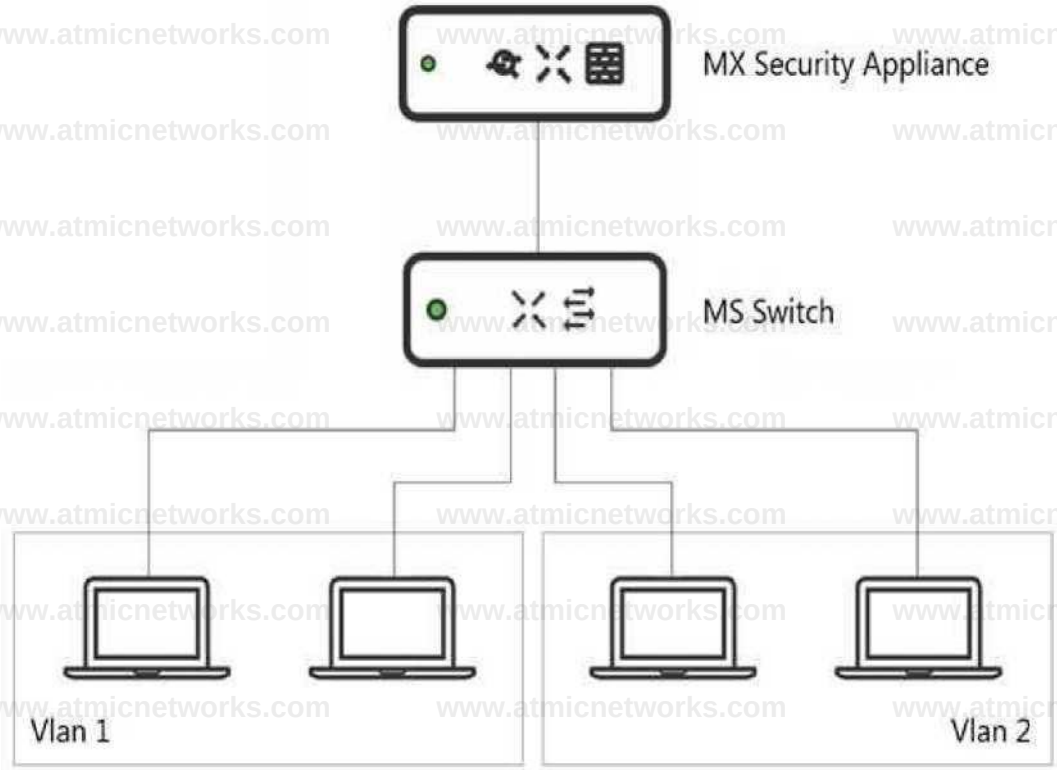
A. malware protection
B. SD-WAN
C. next-generation firewall
D. intrusion prevention

Answer: B

Explanation:
https://documentation.meraki.com/MX/MX_Installation_Guides/vMX_Setup_Guide_for_Microsoft_Azure

Question: 41

Refer to the exhibit.



What is an advantage of implementing inter-VLAN routing on an MX Security Appliance rather than performing inter-VLAN routing on an MS Series Switch?

A. The MX appliance performs IDS/IPS for inter-VLAN traffic.
B. The MX appliance performs AMP for inter-VLAN traffic.
C. The MX appliance performs data encryption for inter-VLAN traffic.
D. The MX appliance performs content filtering for inter-VLAN traffic.

Answer: C

Explanation:

Question: 42

Which API endpoint clones a new Organization?

A. POST /organizations/clone/{organizationId}
B. PUT /organizations/{organizationId}/clone
C. POST /organizations/{organizationId}/new
D. POST /organizations/{organizationId}/clone

Answer: D

Explanation:
https://developer.cisco.com/meraki/api-v1/#!clone-organization

Question: 43

What happens to an unsupervised iOS device when the "Meraki management" profile is removed?

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

Answer: B

Explanation:

Question: 44

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

Answer: A

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

Reference: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/ Wireless_QoS_and_Fast_Lane

Question: 45

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

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

Answer: A

Explanation:

Reference: https://documentation.meraki.com/MX/Site-to-site_VPN/ Using_OSPF_to_Advertise_Remote_VPN_Subnets

Question: 46

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

Answer: D

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: 47

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

Answer: CE

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.

Reference: https://documentation.meraki.com/MV/Initial_Configuration/Video_Retention

Question: 48

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.

Answer: A

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: 49

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

Answer: A

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: 50

Refer to the exhibit.

During a Meraki AP deployment, the default SSID that the exhibit shows is broadcast. What causes this behavior?

A. An AP does not have a wired connection to the network.
B. An AP cannot connect to the default gateway.
C. An AP has never connected to the Meraki Cloud Controller.
D. An AP has Site Survey mode enabled.

Answer: C

Explanation:

If a Meraki Access Point does not have a configuration from the Meraki Cloud Controller it will instead broadcast a default SSID of "Meraki-Scanning."

vs
<SSID_name>-scanning
Cause: Similar to 'bad-gateway', an AP is unable to connect to its default gateway.

https://documentation.meraki.com/MR/Other_Topics/Troubleshooting_local_connection_issues_using_default_SSID_on_MR_Access_Points
This is because the AP is broadcasting the default SSID "meraki-scanning" which is only broadcast when the AP has never connected to the Meraki Cloud Controller1.
This question is related to the topic of Wireless Access Points Quick Start in the Cisco Meraki documentation. You can find more information about this topic in the Wireless Access Points Quick Start article or the Using the Cisco Meraki Device Local Status Page page.

Question: 51

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

Answer: B

Explanation:
https://documentation.meraki.com/MV/Initial_Configuration/Privacy_Windows

Question: 52

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

Answer: C

Explanation:

https://documentation.meraki.com/MR/MR_Splash_Page/Systems_Manager_Sentry_Enrollment
Reference: https://meraki.cisco.com/blog/tag/systems-manager/page/4/

Question: 53

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

Answer: C

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: 54

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

Answer: C

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: 55

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.

Answer: B

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 reconnect 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

Reference: https://community.meraki.com/t5/Mobile-Device-Management/Check-NotNow-Status/td-p/3887

Question: 56

Which information is used to calculate whether a WAN link has high usage?

A. data under Security & SD WAN > Appliance Status > Uplink > Live Data
B. total historical throughput of an uplink
C. total number of devices that are actively passing traffic
D. value under Security & SD WAN > SD WAN & Traffic Shaping > Uplink Configuration

Answer: D

Explanation:

Which information is used to calculate whether a WAN link has high usage not how to view (To accurately identify high utilization, users must set the ISP-provided bandwidth limits under Security and SD-WAN > SD-WAN and Traffic Shaping > Uplink Configuration for each uplink. If the bandwidth usage is higher than 80% of the defined limit, it will mark that uplink as High Usage.)
https://documentation.meraki.com/MI/MI_WAN_Health#:~:text=To%20accurately%20identify%20high%20utilization,that%20uplink%20as%20High%20Usage.

Question: 57

Which configuration step is necessary when automatic updating is required of iOS apps provisioned through Systems Manager that are found in the App Store?

A. No configuration step is necessary; automatic updating is the default behavior.
B. Configure automatic updating of iOS devices in the Meraki installed profile.
C. Create a security policy that enables automatic updates.
D. Create a profile with automatic update enabled and apply it to iOS devices.

Answer: A

Explanation:

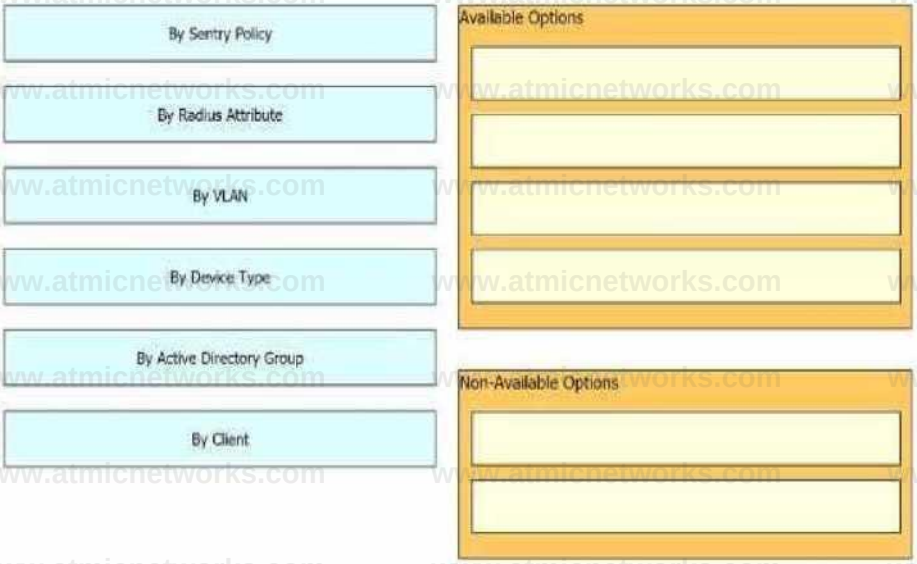
By default, iOS apps provisioned through Systems Manager that are found in the App Store will selfupdate if automatic updates has been turned on in the Settings. For custom iOS apps, or to manually push down updates, check the following steps.
https://documentation.meraki.com/SM/Apps_and_Software/Updating_Managed_iOS_Apps

Question: 58

DRAG DROP

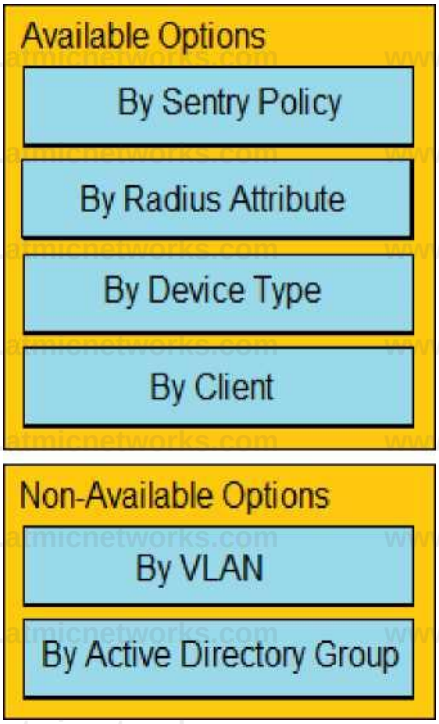
Drag and drop the settings from the left onto the available or non-available methods of applying a group policy to a Cisco Meraki MR access point on the right.

www.atmicnetworks.com



Answer:

Explanation:



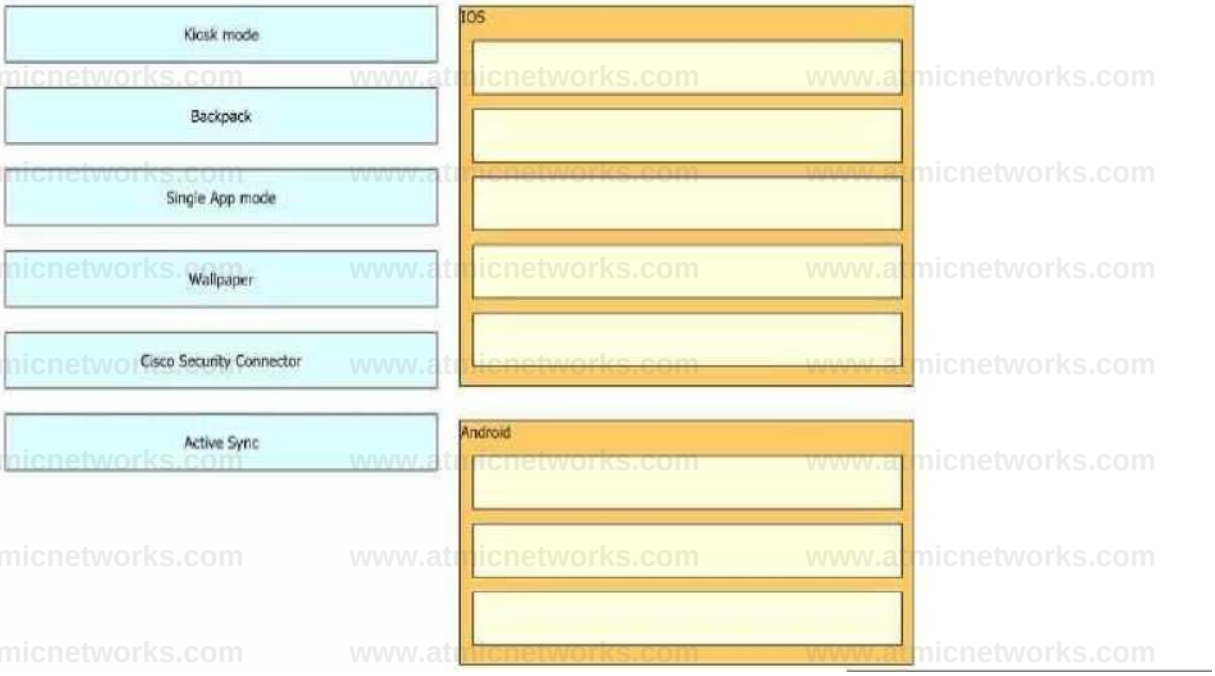
https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Creating_and_Applying_Group_Policies

Question: 59

DRAG DROP

Drag and drop the settings from the left onto the OS system or systems that support it on the right

Settings can be used more than once.



Answer:

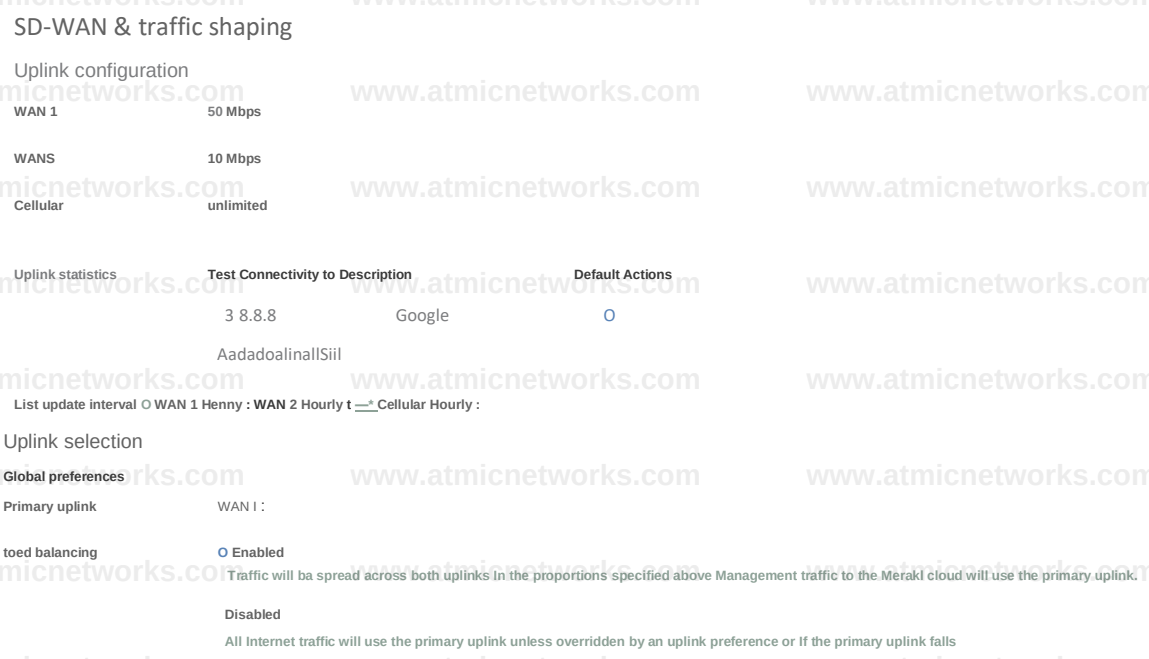
Explanation:

IOS:
Kiosk mode
Single App mode
Wallpaper
Cisco Security Connector
Active Sync
Android:
Kiosk mode
Backpack
Wallpaper
Active Sync
This question is related to the topic of System Manager: Getting Started in the Cisco Meraki documentation. You can find more information about this topic in the [System Manager: Getting Started] article or the [System Manager Overview] page.

https://documentation.meraki.com/SM/Profiles_and_Settings/Configuration_Settings_Payloads

Question: 60

Refer to the exhibit.



Refer to the exhibit. What Is the ratio of internet-bound flows that route via WAN 1 compared with WAN 2?

A. All flows alternate in a 5:1 ratio.
B. All flows alternate in a 2:1 ratio.
C. All flows agrees via WAN 1:1 ratio.
D. All flows egress via WAN1.

Answer: C

Explanation:

https://documentation.meraki.com/MX/Firewall_and_Traffic_Shaping/MX_Load_Balancing_and_Flow_Preferences#Load_Balancing

Question: 61

An organization requires that BYOD devices be enrolled in Systems Manager before they gain access to the network. Part of the enrollment includes pushing out the corporate SSID preshared key, corporate email settings, and some business-sensitive PDFs. When a user leaves the organization, which Systems Manager feature allows the removal of only the MDM-delivered content from the user's device?

A. Erase Device
B. Clear Pushed Data
C. Unenroll Device
D. Selective Wipe

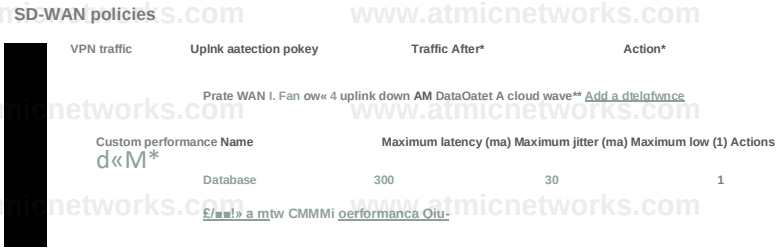
Answer: D

Explanation:

https://documentation.meraki.com/SM/Monitoring_and_Reporting/Selective_Wipe_and_Device_Quarantine_in_Systems_Manager

Question: 62

Refer to the exhibit.



Which condition or conditions will cause the "All Databases & cloud services" SD-WAN traffic to be routed via a VPN2 tunnel on WAN2?

A. WAN1 tunnel latency is 20 ms or less, irrespective of WAN2 tunnel performance.

B. WAN1 tunnel latency is 20 ms or more, and WAN2 tunnel meets the configured performance criteria.
C. WAN1 tunnel latency is 20 ms or less, and WAN2 tunnel meets the configured performance criteria.
D. WAN1 tunnel latency is 20 ms or more, irrespective of WAN2 tunnel performance.

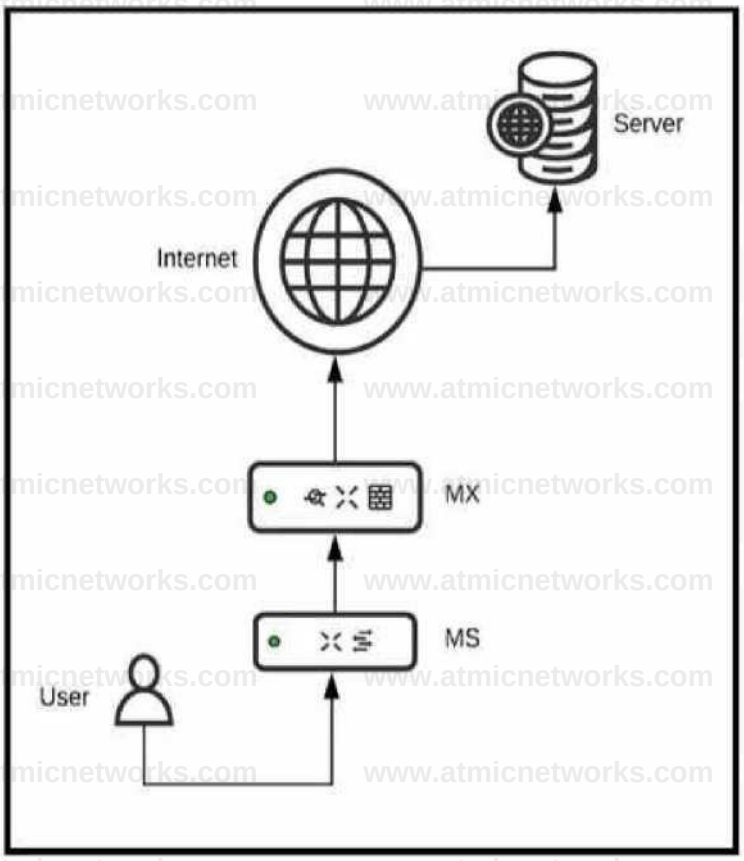
Answer: B

Explanation:

This is because the SD-WAN policy for "All Databases & cloud services" has the following settings: Uplink selection policy: Prefer WAN1, Fail over if down
Traffic filters: Custom performance classes
Custom performance classes: Database
Database performance criteria: Maximum latency 200 ms, Maximum jitter 20 ms, Maximum loss 1% This means that the SD-WAN traffic will be routed via WAN1 by default, unless WAN1 is down or fails to meet the database performance criteria. In that case, the traffic will be routed via WAN2, if WAN2 meets the database performance criteria. Therefore, the condition that will cause the traffic to be routed via WAN2 is when WAN1 tunnel latency is 20 ms or more (which exceeds the maximum jitter of 20 ms), and WAN2 tunnel meets the configured performance criteria (maximum latency 200 ms, maximum jitter 20 ms, maximum loss 1%).

Question: 63

Refer to the exhibit.



Which two configurations are needed to successfully monitor custom applications that a user is accessing using Cisco Meraki Insight? (Choose two)

A. The custom application uses TLS on any ports.
B. The custom application uses HTTP on port 8080.
C. The custom application uses HTTPS on TCP 443.
D. The custom application uses SMB/CIFS.
E. The custom application uses HTTPS on port 8080.

Answer: BC

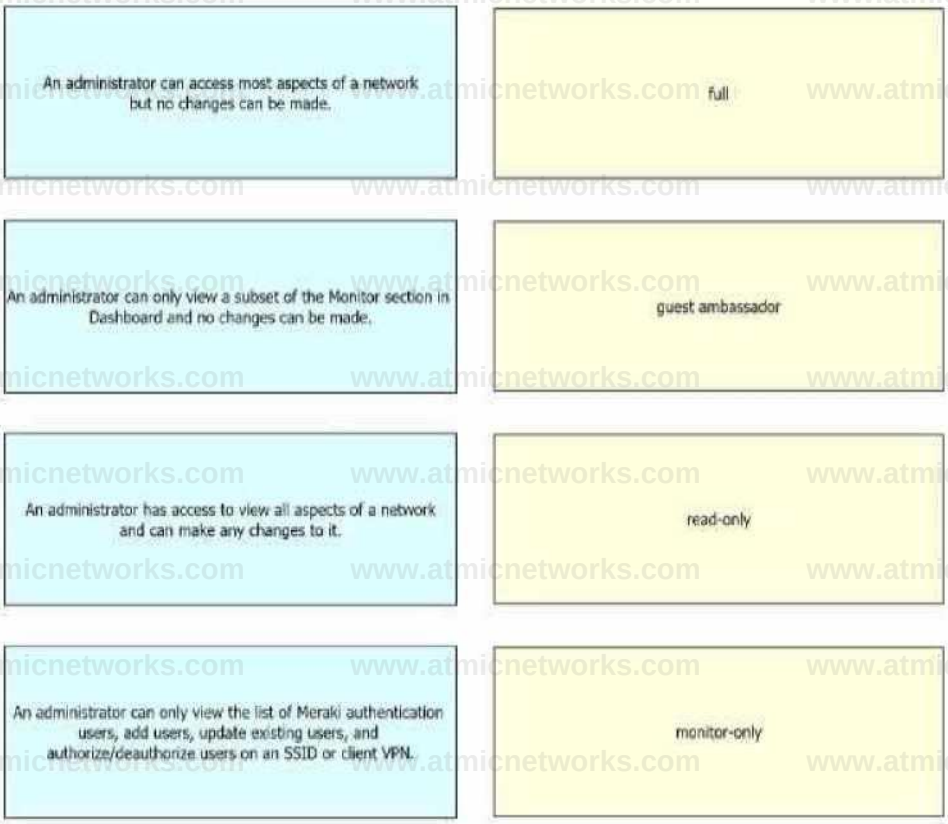
Explanation:

https://documentation.meraki.com/MI/MI_Web_App_Health/Overview#:~:text=On%20this%20page%2C%20you%20can,that%20ports%20cannot%20be%20specified.

Question: 64

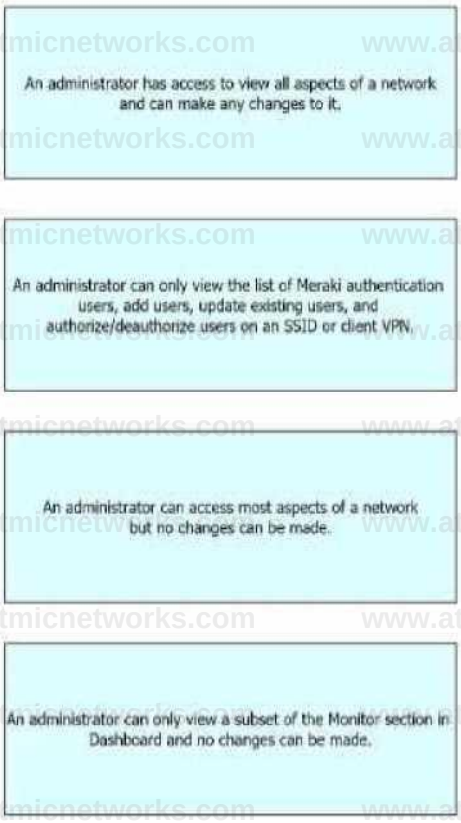
DRAG DROP

Drag and drop the descriptions from the left onto the permission types on the right.



Answer:

Explanation:



Question: 65

What are two methods of targeting and applying management profiles to System Manager clients? (Choose two.)

A. by using Wi-Fi tags
B. by defining the scope
C. by defining a range of serial numbers
D. by using device tags
E. by using dynamic IP tags

Answer: B, D

Explanation:

The correct answer is B and D. These are the two methods of targeting and applying management profiles to System Manager clients, according to the [System Manager: Getting Started] article. The article explains that: Defining the scope: This method allows you to target devices based on their network, tag, or owner. You can define the scope of a profile from the Systems Manager > Manage > Settings page or from the Systems Manager > Monitor > Overview page.
Using device tags: This method allows you to target devices based on their attributes, such as OS, model, location, or user. You can use device tags to create dynamic groups of devices that share common characteristics. You can apply device tags from the Systems Manager > Monitor > Devices page or from the Systems Manager > Manage > Tags page.

Question: 66

There will be 100 concurrent users streaming video to their laptops. A 30/70 split between 2.4 Ghz and 5 Ghz will be used. Roughly how many APs (rounded to the nearest whole number) are needed based on client count?

A. 2
B. 3
C. 4
D. 5

Answer: C

Explanation:

This is the approximate number of APs that are needed based on client count, assuming that each AP can support up to 25 concurrent video streaming users. This can be calculated by using the formula: Number of APs = (Number of Users x Percentage of Users on a Band) / Number of Users per AP on that Band
Where Number of Users is 100, Percentage of Users on 2.4 Ghz is 30%, Percentage of Users on 5 Ghz is 70%, Number of Users per AP on 2.4 Ghz is 15, and Number of Users per AP on 5 Ghz is 30. Therefore, Number of APs = (100 x 0.3 / 15) + (100 x 0.7 / 30) Number of APs = (3.33) + (2.33) Number of APs =

5.66

Rounding to the nearest whole number, the number of APs is 4.

This question is related to the topic of Wireless Capacity Planning in the Cisco Meraki documentation. You can find more information about this topic in the [Wireless Capacity Planning] article or the [Best Practice Design - MR Wireless] page.

Question: 67

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:

https://www.ciscolive.com/c/dam/r/ciscolive/latam/docs/2019/pdf/BRKCRS-1579.pdf

Question: 68

The WAN connection of a Cisco Meraki MX security appliance is congested, and the MX appliance is buffering the traffic from LAN ports going to the WAN ports. High, normal, and low priority queue buffers are all full. Which proportion of the normal traffic is forwarded compared to the other queues?

A. 4/10 packets
B. 2/7 packets
C. 2/10 packets
D. 5/15 packets

Answer: B

Explanation:

https://documentation.meraki.com/MX/Firewall_and_Traffic_Shaping/SD-WAN_and_Traffic_Shaping

Question: 69

Which enrollment method must be used when containerization is required on BYOD Android devices managed by Systems Manager?

A. Android Enterprise utilizing a Work Profile
B. Systems Manager network ID
C. Android Business utilizing a BYOD Profile
D. Systems Manager container ID

Answer: A

Explanation:

https://documentation.meraki.com/SM/Device_Enrollment/Containerization_with_Systems_Manager

Question: 70

What is out of scope when considering the Best practices for high-density wireless designs?

A. maximum beamforming
B. band selection
C. minimum bitrate
D. number of SSIDs

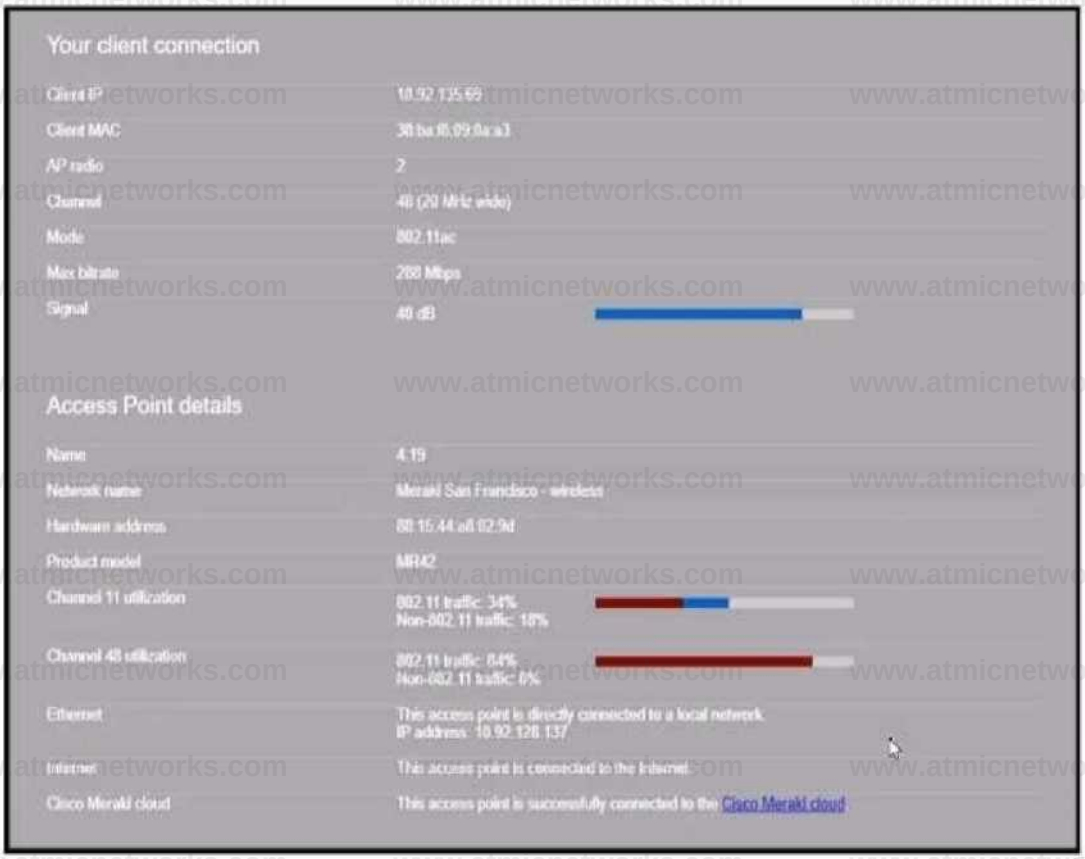
Answer: A

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: 71

Refer to the exhibit.



Why does the end user complain of poor wireless performance?

A. Channel 48 utilization is at 84 percent.
B. Non-802.11 traffic of 18 percent indicates poor AP placement.
C. The client is connected to the secondary radio of the AP instead of the primary radio
D. The client is using a 20 MHz channel width to connect.

Answer: A

Explanation:

Question: 72

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

Answer: C

Explanation:

www.atmicnetworks.com

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