Free Questions for 500-220 by dumpssheet

Shared by Mcmahon on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is a feature of distributed Layer 3 roaming?

Options:

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 2

Question Type: DragDrop

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	1
create profile	2
add settings profile	3
define tags	4
apply profile	5

Answer:

Question 3

Question Type: MultipleChoice

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

Options:

A- Maximum Jitter

B- Total Bandwidth Usage

C- Maximum Latency

D- Per-flow Goodput

E- Application Response Time

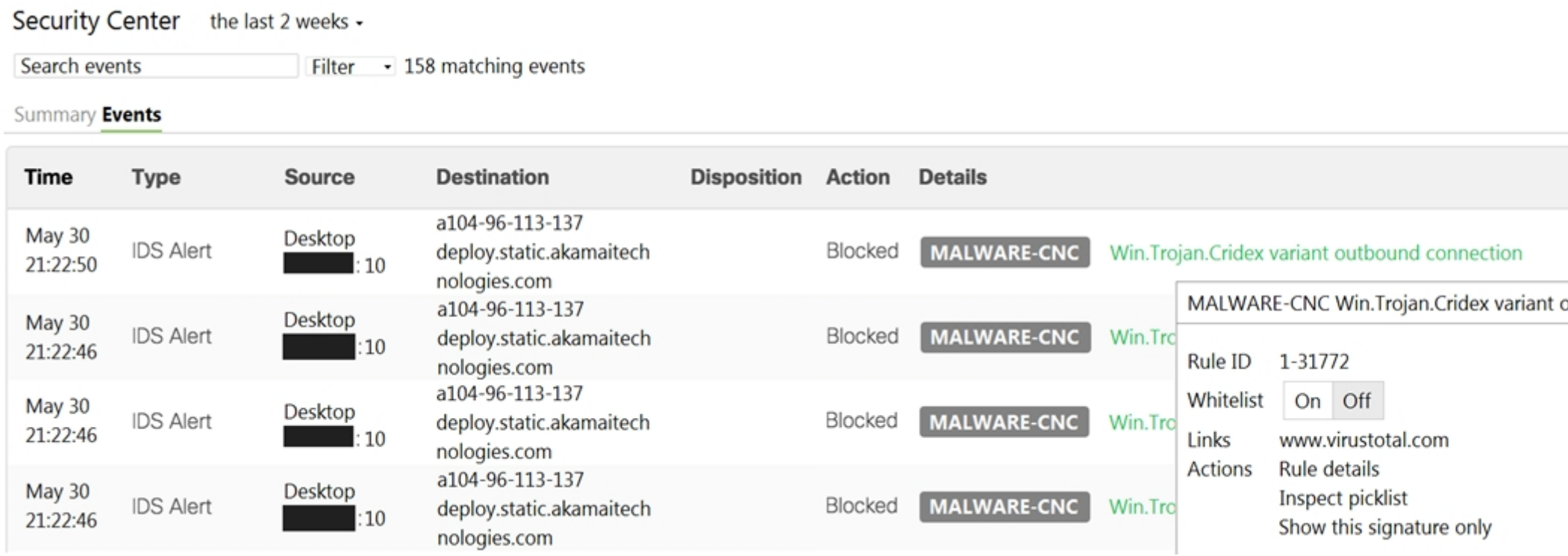
Answer:

D, E

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit.



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

Options:

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_Protection

Question 5

Question Type: MultipleChoice

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

Options:

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 6

Question Type: MultipleChoice

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)	×

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?

Options:

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:

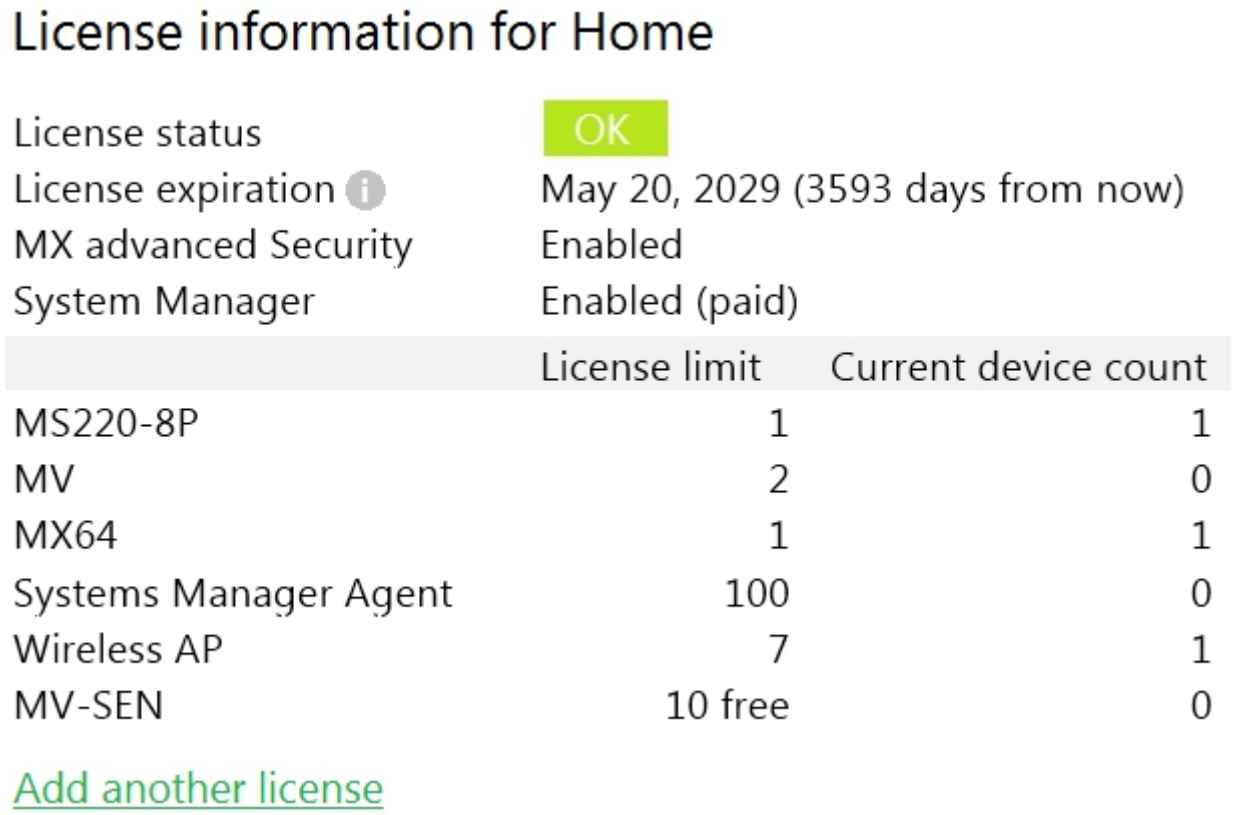
The performance probe is a small payload (approximately 100 bytes) of UDP data sent over all established VPN tunnels every 1 second. MX appliances track the rate of successful responses and the time that elapses before receiving a response. This data allows the MX to determine the packet loss, latency, 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 7

Question Type: MultipleChoice

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?

Options:

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

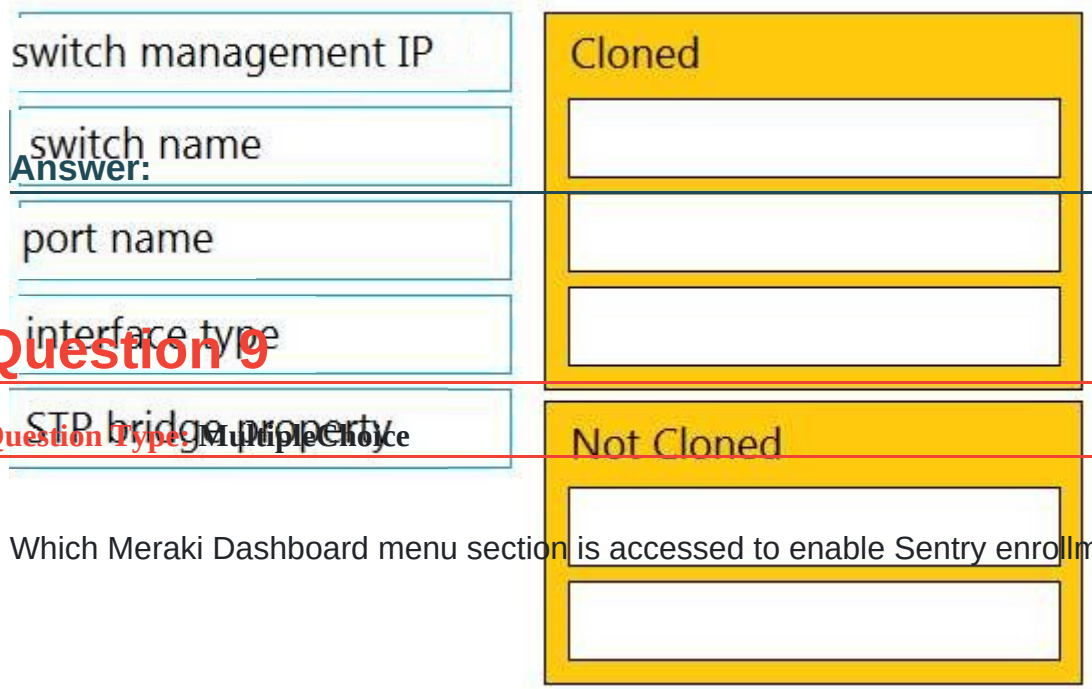
Explanation:

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 8

Question Type: DragDrop

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:

Question 9

Question Type: MultipleChoice

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

Options:

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 10

Question Type: MultipleChoice

Refer to the exhibit.

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

Options:

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 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.