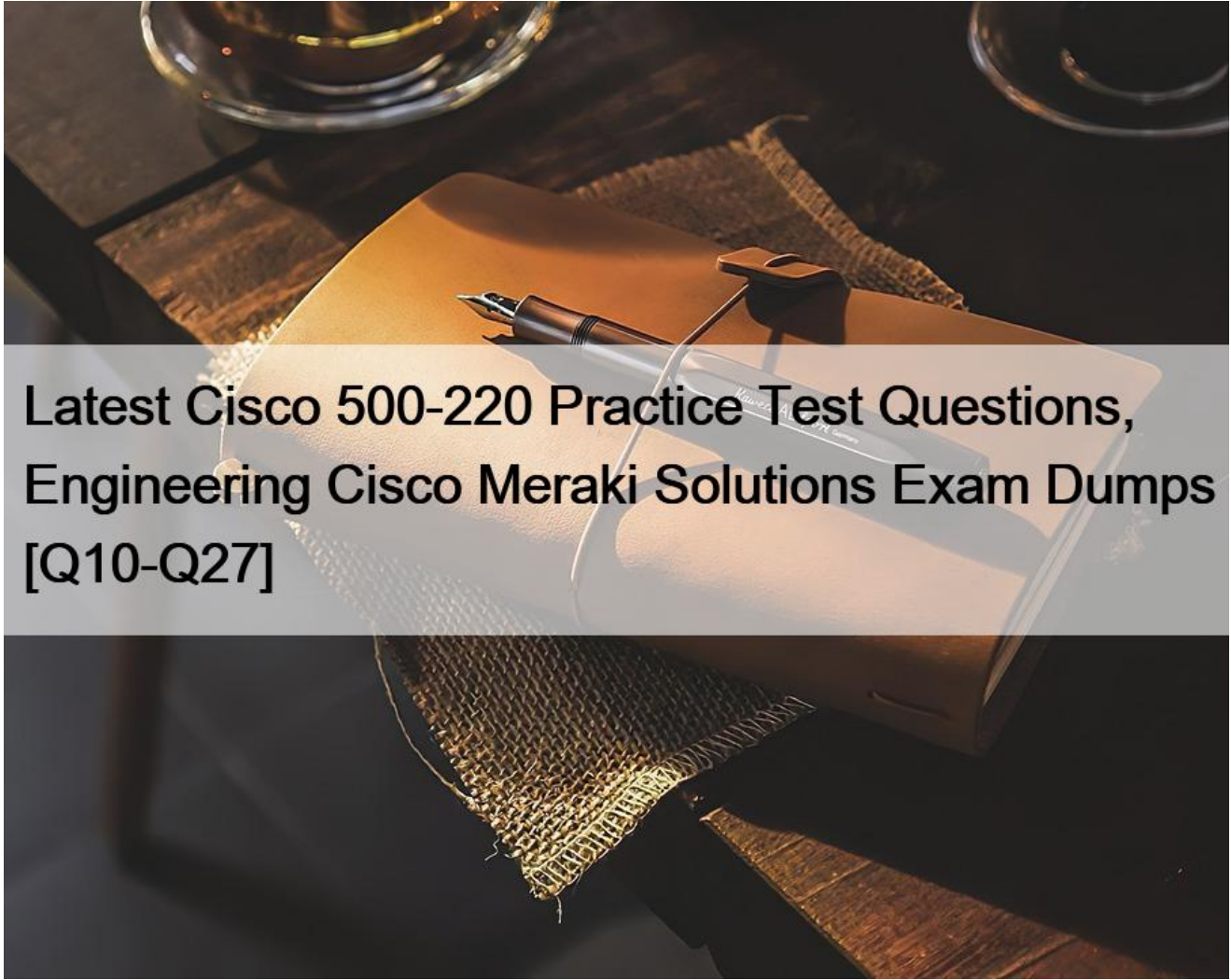


Latest Cisco 500-220 Practice Test Questions, Engineering Cisco Meraki Solutions Exam Dumps [Q10-Q27]



Latest Cisco 500-220 Practice Test Questions, Engineering Cisco Meraki Solutions Exam Dumps [Q10-Q27]

Latest Cisco 500-220 Practice Test Questions, Engineering Cisco Meraki Solutions Exam Dumps Sep-2022 Pass Cisco 500-220 Exam in First Attempt Easily NEW QUESTION 10

Refer to the exhibit.

Corp MX 1
MX450
PRIMARY

ADDRESS
PRIMARY
Current master

Live data
Ports

Internet	SFP	SFP+
2	3 5 7 9 11 13 15 17 12 14 16 18	19 21 23 25 20 22 24 26

Historical data
Connectivity
for the last day

08:00 12:00 16:00

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

- * Add a deny any/any firewall rule to the end of the firewall rules.
- * Remove the connection from Internet 1.
- * Physically disconnect all LAN ports.
- * Configure the MX appliance to Routed mode on the Addressing & VLANS page.

NEW QUESTION 11

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

- * spanning-tree state
- * time synchronization state
- * DHCP association database
- * stateful firewall database

NEW QUESTION 12

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?

- * malware protection
- * SD-WAN
- * next-generation firewall
- * intrusion prevention

NEW QUESTION 13

How is high-availability supported for Cisco Meraki devices?

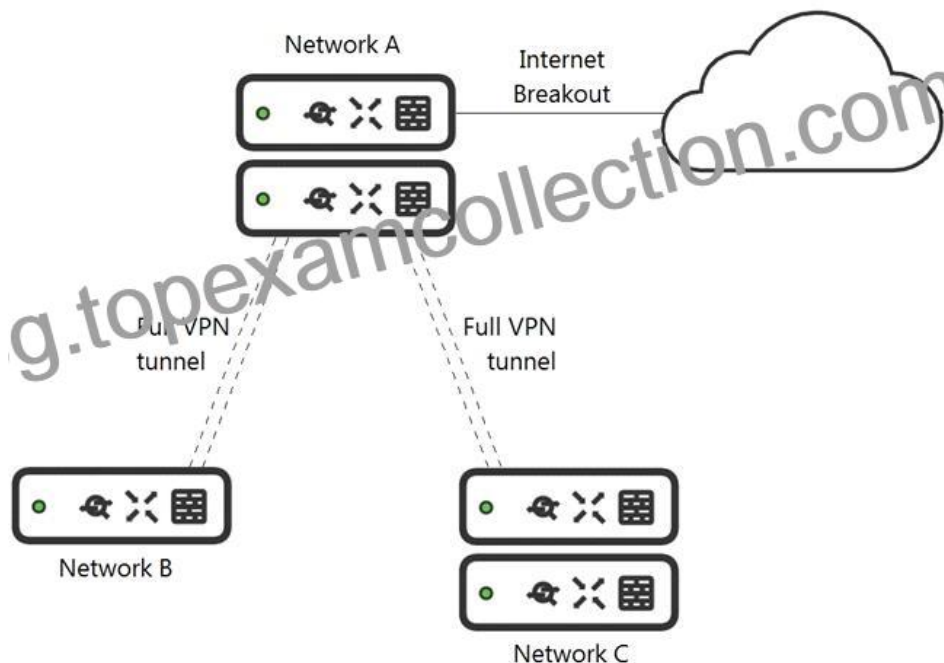
- * Only the MX Security Appliances that use VRRP support high availability.
- * An active/active high-availability pair is recommended for MX Security Appliances.
- * The MX Security Appliances and MS Series Switches that use VRRP support an active/passive high-availability pair.
- * The MX Security Appliances and MS Series Switches that use HSRP support an active/passive high-availability pair.

Reference:

[_High_Availability_Pair](#)

NEW QUESTION 14

Refer to the exhibit.



What is the minimal Cisco Meraki Insight licensing requirement?

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

NEW QUESTION 15

What is a feature of distributed Layer 3 roaming?

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

Reference:

[Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/](#)

[Wireless_Layer_3_Roaming_Best_Practices](#)

NEW QUESTION 16

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

- * MD5
- * certificate
- * plaintext
- * SHA-1

Reference:

[Using OSPF to Advertise Remote VPN Subnets](#)

NEW QUESTION 17

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

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

NEW QUESTION 18

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

- * Full
- * Read-only
- * Monitor-only
- * Write
- * Write-only

Reference:

[Managing Dashboard Administrators and Permissions](#)

NEW QUESTION 19

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?

- * 26
- * 28
- * 30
- * 32

NEW QUESTION 20

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

- * Wireless > Monitor > Access Points > AP > RF
- * Wireless > Configure > Radio Settings
- * Wireless > Monitor > Wireless Health
- * Wireless > Monitor > RF Spectrum

NEW QUESTION 21

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?

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

NEW QUESTION 22

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.)

- * Controller disconnection behavior
- * Captive Portal strength
- * Simultaneous logins
- * Firewall & traffic shaping
- * RADIUS for splash page settings

NEW QUESTION 23

Which API endpoint clones a new Organization?

- * POST /organizations/clone/{organizationId}
- * PUT /organizations/{organizationId}/clone
- * POST /organizations/{organizationId}/new
- * POST /organizations/{organizationId}/clone

NEW QUESTION 24

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

- * The Dashboard generates the SAML request.
- * The Dashboard provides user access credentials.
- * The Dashboard parses the SAML request and authenticates users.
- * The Dashboard generates the SAML response.

NEW QUESTION 25

Air Marshal has contained a malicious SSID.

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

- * Currently associated clients stay connected.
- * New clients can connect.
- * Currently associated clients are affected by restrictive traffic shaping rules.
- * New clients cannot connect.
- * Currently associated clients are disconnected.

NEW QUESTION 26

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?

- * Content filtering
- * Bridge mode
- * 802.11r
- * Dual band operating with Band Steering

NEW QUESTION 27

Refer to the exhibit.

Security Center the last 2 weeks ▾

Search events Filter ▾ 158 matching events

Summary **Events**

Time	Type	Source	Destination	Disposition	Action	Details
May 30 21:22:50	IDS Alert	Desktop [REDACTED]:10	a104-96-113-137 deploy.static.akamaitechnologies.com	Blocked	MALWARE-CNC	Win.Trojan.Cridex variant outbound connection
May 30 21:22:46	IDS Alert	Desktop [REDACTED]:10	a104-96-113-137 deploy.static.akamaitechnologies.com	Blocked	MALWARE-CNC	Win.Trojan.Cridex variant outbound connection
May 30 21:22:46	IDS Alert	Desktop [REDACTED]:10	a104-96-113-137 deploy.static.akamaitechnologies.com	Blocked	MALWARE-CNC	Win.Trojan.Cridex variant outbound connection
May 30 21:22:46	IDS Alert	Desktop [REDACTED]:10	a104-96-113-137 deploy.static.akamaitechnologies.com	Blocked	MALWARE-CNC	Win.Trojan.Cridex variant outbound connection

MALWARE-CNC Win.Trojan.Cridex variant outbound connection

Rule ID 1-31772

Whitelist On Off

Links www.virustotal.com

Actions Rule details
Inspect picklist
Show this signature only

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

- * quarantine
- * prevention
- * detection
- * blocking

Cisco 500-220 Exam Syllabus Topics:

Topic 1- Compare endpoint device and application management methods- Design dynamic path selection policies

Topic 2- Design Enterprise wireless services- Configuring MR wireless access points

Topic 3- Wireless client connectivity issues

using Dashboard- Network access control solutions
Topic 4- Alerts with Dashboard, SNMP, Syslog and Netflow in
Dashboard- Security threats using Security Center
Topic 5- Threat protection and content filtering rules- Explain access
methods to dashboard and devices
Topic 6- Troubleshooting Enterprise networks- Compare deployment workflows
Topic 7-
Device enrollment such as supervised and device owner- Interpret information from monitoring and reporting tools

Free 500-220 Exam Files Downloaded Instantly 100% Dumps & Practice Exam:

<https://www.topexamcollection.com/500-220-vce-collection.html>