



- Expert Verified, Online, **Free**.

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: BC

Community vote distribution

BC (100%)

  **VitalIntegrators** 8 months, 3 weeks ago

Selected Answer: BC

agreed

upvoted 1 times

  **rnunes1110** 1 year, 3 months ago

Selected Answer: BC

Correct: B and C

upvoted 1 times

  **azjimpang** 2 years, 1 month ago

1 Cloud license has expired

2 the number of HW devices exceeds the number of cloud licenses

upvoted 3 times

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.

Correct Answer: AC

Community vote distribution

AC (100%)

🗳️ **VitalIntegrators** 8 months, 3 weeks ago

Selected Answer: AC

agreed

upvoted 1 times

🗳️ **rnunes1110** 1 year, 3 months ago

Selected Answer: AC

Correct: A and C

upvoted 1 times

🗳️ **liliap** 1 year, 6 months ago

Selected Answer: AC

A,C .

upvoted 2 times

🗳️ **azjlpang** 2 years, 1 month ago

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.

upvoted 3 times

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](#)

Refer to the exhibit. 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

Community vote distribution

B (100%)

🗳️ **rnunes1110** 3 months, 1 week ago

Selected Answer: B

Correct: B

upvoted 1 times

🗳️ **liliap** 6 months, 2 weeks ago

Selected Answer: B

B .

upvoted 1 times

🗳️ **Wooker** 1 year, 1 month ago

Selected Answer: B

should be B

upvoted 2 times

🗳️ **dustexam123** 1 year, 1 month ago

Nah Bro. it's B: 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.

upvoted 4 times

🗳️ **a0435** 1 year, 1 month ago

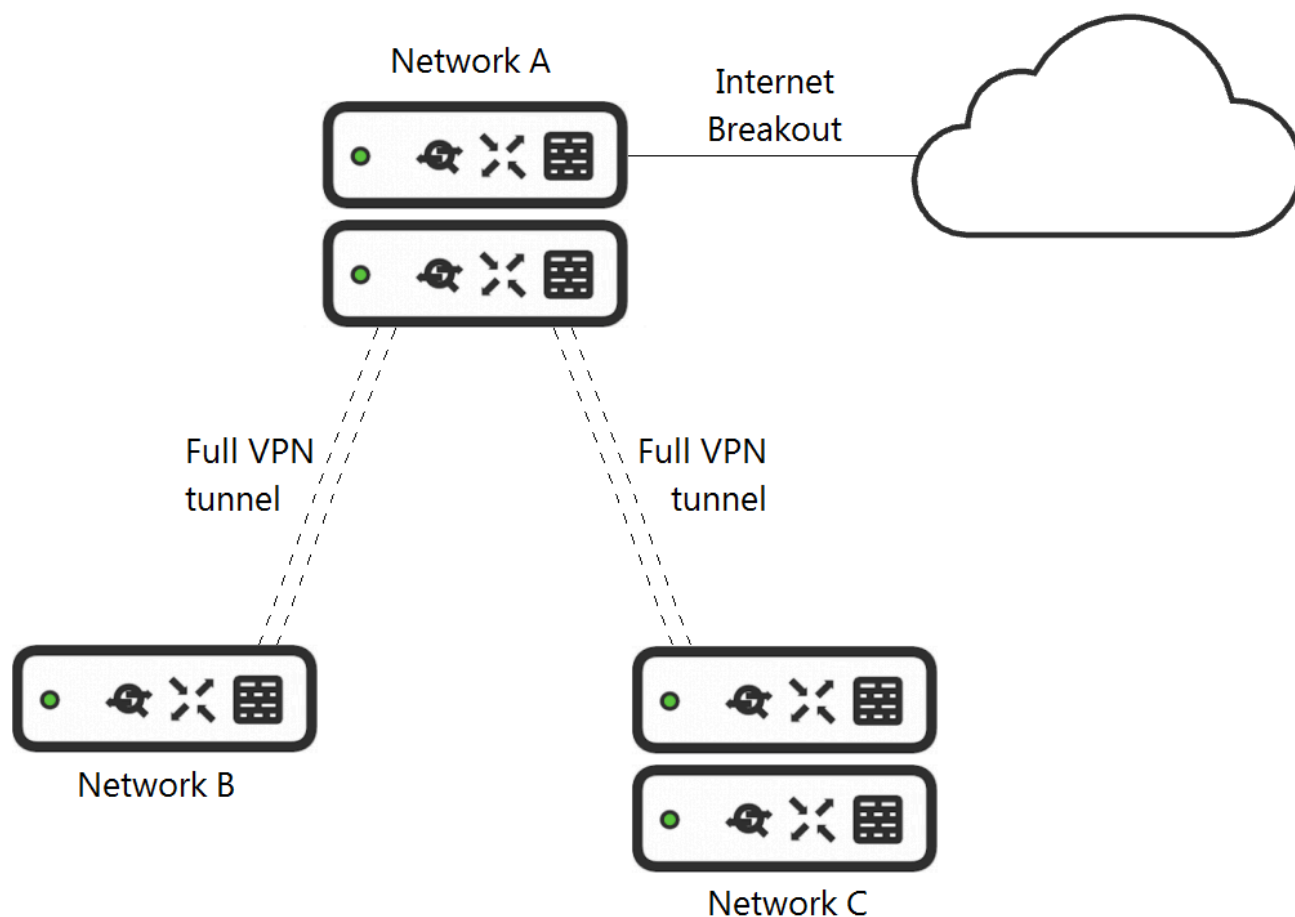
D- All APs stop functioning in 30 days

upvoted 1 times

🗳️ **El_Matador_EOD** 6 months ago

It's B

upvoted 1 times



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.

Correct Answer: B

Community vote distribution

B (100%)

Ironman_2022 Highly Voted 1 year, 3 months ago

Selected Answer: B

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.

upvoted 9 times

rnunes1110 Most Recent 3 months, 2 weeks ago

Selected Answer: B

Correct: B

'cause all other answer is related to Network A (HUB) won't gather data for remote sites (as Ironman_2022 said)

upvoted 1 times



azjimpang 1 year, 1 month ago

Selected Answer: B

Licensing Guidelines

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.

upvoted 1 times

  **JerryKamb** 1 year, 3 months ago

This would suggest just one per network, so B would be my answer.

upvoted 3 times

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

Community vote distribution

A (100%)

🗨️ **rnunes1110** 3 months, 2 weeks ago

Selected Answer: A

Answer: A

No discussion !

upvoted 2 times

🗨️ **Nick1721** 5 months, 1 week ago

Selected Answer: A

No local server

upvoted 1 times

🗨️ **AGNote3** 1 year ago

Selected Answer: A

Should be A there is no local server

upvoted 1 times

🗨️ **haluk** 1 year ago

Selected Answer: A

should be A

upvoted 1 times

🗨️ **Wooker** 1 year, 1 month ago

Selected Answer: A

should be A

upvoted 1 times

🗨️ **azjlpang** 1 year, 1 month ago

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

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

Correct Answer: AB

Community vote distribution

AB (100%)

🗨️ 👤 **Adrian1988** 3 months, 1 week ago

Selected Answer: AB

Organization Permission Types:

None: User will not have organization-wide access. Use this option if you want the user to have network only permissions.

Read-only: User able to access most aspects of network and organization-wide settings, but unable to make any changes.
Read-Only admins can perform switch port cycles and cable tests

Full: User has full administrative access to all networks and organization-wide settings. This is the highest level of access available.
upvoted 2 times

🗨️ 👤 **rnunes1110** 9 months ago

Selected Answer: AB

Answer: A and B
upvoted 1 times

🗨️ 👤 **azjlpang** 1 year, 7 months ago

Selected Answer: AB

ab
upvoted 2 times

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: A

Community vote distribution

A (100%)

🗳️ **sattori** 3 months, 1 week ago

Selected Answer: A

This is the SAML process flow:

Auth0 = Identity Provider (could be any identity management platform)

Meraki Dashboard = Service Provider

1. The user tries to log in to Meraki Dashboard from a browser.
2. Dashboard responds by generating a SAML request.
3. The browser redirects the user to an SSO URL, Auth0
4. Auth0 parses the SAML request and authenticates the user. This could be with username and password or even social login. If the user is already authenticated on Auth0, this step will be skipped. Once the user is authenticated, Auth0 generates a SAML response.
5. Auth0 returns the encoded SAML response to the browser.
6. The browser sends the SAML response to Dashboard for verification.
7. If the verification is successful, the user will be logged in to Dashboard and granted access to the resources that they are authorized to view/modify.

upvoted 1 times

🗳️ **robby77** 3 months, 1 week ago

Selected Answer: A

https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Configuring_SAML_Single_Sign-on_for_Dashboard?_gl=1%2Abodebf%2A_ga%2ANjk3MjkwOTY5LjE3MDY1NjlyNjE.%2A_ga_DG2DVWGCW%2AMTczMjk3MDg0NS4zLjEuMTczMjk3NzI2Ni4wLjAuMA..

upvoted 1 times

🗳️ **rnunes1110** 1 year, 3 months ago

Selected Answer: A

Correct: A

upvoted 1 times

🗳️ **kobaba** 1 year, 9 months ago

Selected Answer: A

Since information by meraki does not mention about type of SAML in sequence, I checked general doc in "<https://developer.okta.com/docs/concepts/saml/#planning-for-saml>".

It says [A SAML Request, also known as an authentication request, is generated by the Service Provider to "request" an authentication.]

upvoted 1 times

🗳️ **LordHammer** 2 years, 1 month ago

A based on the following documents under SP-initiate SAML

upvoted 2 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗨️ **sattori** 3 months, 1 week ago

Selected Answer: B

I agree with B, but SD-WAN is technology not feature
upvoted 1 times

🗨️ **rnunes1110** 1 year, 3 months ago

Selected Answer: B

Correct: B
upvoted 2 times

🗨️ **Jean226** 1 year, 9 months ago

Selected Answer: B

B is correct
upvoted 2 times

🗨️ **tliz** 2 years, 1 month ago

Selected Answer: B

I believe its B
upvoted 3 times

🗨️ **Consrico** 2 years, 2 months ago

Agree ..it is B
Major benefits:

Supports SD-WAN. So if you have dual connected sites, either for load balancing or failover, SD-WAN will automatically select the best path. You can also use performance classes to optimise specific types of traffic.

upvoted 4 times

🗨️ **Ironman_2022** 2 years, 3 months ago

Selected Answer: B

The vMX appliance can only be deployed as one arm-concentrator thus not a next gen firewall as cannot utilise the features.
upvoted 4 times

DRAG DROP -

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

- 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:

- 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

- Client traffic to the internet has the source IP rewritten to match the WAN IP of the appliance
- VLANs cannot be configured
- This mode is the default mode of operation
- This mode is generally also the default gateway for devices on the LAN



Passthrough mode

- The MX appliance acts as a layer 2 bridge
- DHCP services can be configured on the MX appliance
- This mode is not recommended at the network perimeter
- No address translation is provided



azjimpang Highly Voted 7 months, 4 weeks ago



Routed Mode
 This mode is default mode of operation
 DHCP services can be configured on the MX appliance
 This mode is generally also the default GW for devices on the LAN
 Client traffic to the internet has the source UP rewritten to match the WAN IP of the appliance
 Pass-through Mode



The MX appliance acts as a Layer 2 Bridge
VLANs cannot be configured
This mode is not recommended at the network perimeter
No address translation is provided
upvoted 11 times



  **DRHoppo** Highly Voted 10 months, 2 weeks ago
Router mode DHCP services can be configured
Passthrough mode VLANS cannot be configured

reference:
https://documentation.meraki.com/MX/Networks_and_Routing/Passthrough_Mode_on_the_MX_Security_Appliance_and_Z-series_Teleworker_Gateway
upvoted 9 times

  **JZeeP** Most Recent 1 month, 1 week ago
It seems to me that the solution to the question shown is not entirely correct; it says that VLANs cannot be configured in routed mode and it says that DHCP can be configured in Passthrough. I think those two answers are reversed. I'm right isn't it?
upvoted 1 times

  **hughes3845phillips** 1 month, 2 weeks ago
Routed Mode:
Default mode of operation: As stated in Meraki documentation, the MX appliance operates in Routed Mode by default.
DHCP services can be configured: In Routed Mode, the MX appliance can provide DHCP functionality for devices on the LAN.
Default gateway for devices on the LAN: In Routed Mode, the MX acts as the gateway for all devices in the LAN.
Source IP rewritten to match the WAN IP: This is NAT behavior, which is typical in Routed Mode.
Passthrough Mode:
Acts as a layer 2 bridge: In this mode, the MX passes traffic without performing routing or NAT, effectively acting as a transparent device.
VLANs cannot be configured: This is consistent with Meraki documentation—Passthrough Mode disables advanced routing features such as VLANs.
Not recommended at the network perimeter: Since Passthrough Mode offers no NAT or routing, it is unsuitable for edge deployments.
No address translation is provided: Passthrough Mode avoids NAT and operates purely as a bridge.
upvoted 1 times

  **JerryKamb** 9 months ago
Agree with DRHoppo
NO DHCP or VLANs in Passthrough, but BOTH in Routed mode.
upvoted 2 times

  **Netmanb2k** 9 months, 3 weeks ago
Refer to Question #12 to confirm that Passthrough cant configure DHCP so
Router mode DHCP services can be configured
Passthrough mode VLANS cannot be configured
upvoted 2 times

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

Community vote distribution

A (100%)

🗨️ **sattori** 3 months ago

Selected Answer: A

Ignore my previous comment, the correct answer is A as question talking about distributed Layer 3 roaming feature. I don't know why moderators keep deleting my comments.

upvoted 1 times

🗨️ **sattori** 3 months, 1 week ago

Selected Answer: B

When we talking about MX, the MX is required as mobility concentrator. We don't need concentrator when we establishing communication between AP.

upvoted 1 times

🗨️ **rnunes1110** 1 year, 4 months ago

I'm pretty sure that the answer is A:

Distributed Layer 3 Roaming

Distributed layer 3 roaming is very scalable because the access points are establishing connections with each other without the need for a concentrator. The target access point will look up in the shared user database and contact the anchor access point. This communication does not traverse the Meraki Cloud and is a proprietary protocol for secure access point to access point communication. UDP port 9358 is used for this communication between the APs.

https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/Wireless_Layer_3_Roaming_Best_Practices

upvoted 2 times

🗨️ **azjimpang** 2 years, 1 month ago

Selected Answer: A

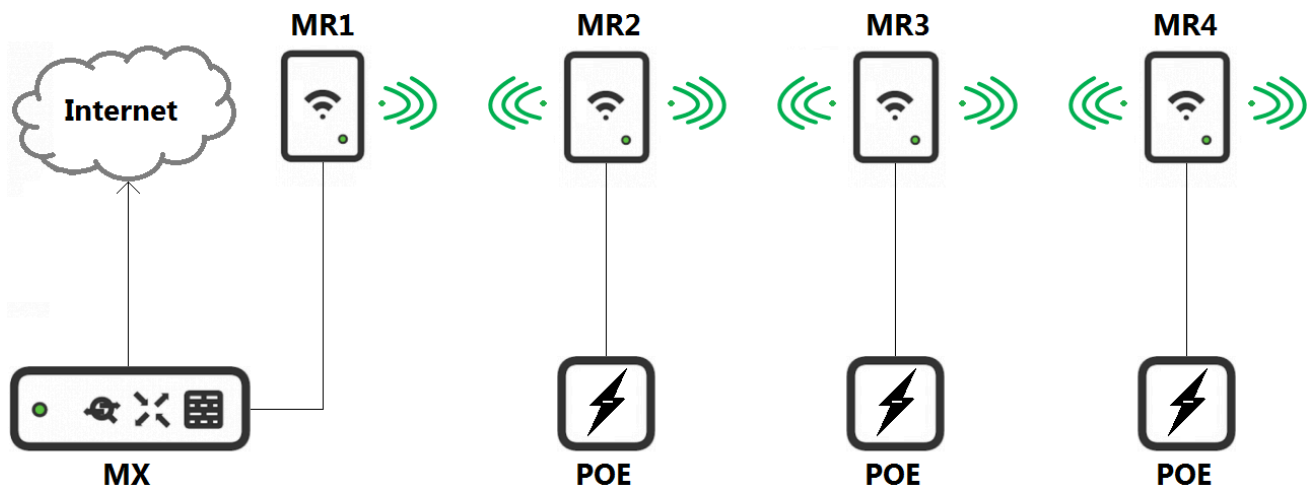
Distributed layer 3 roaming maintains layer 3 connections for end devices as they roam across layer 3 boundaries without a concentrator.

upvoted 4 times

🗨️ **bango** 2 years, 1 month ago

https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/Wireless_Layer_3_Roaming_Best_Practices

upvoted 2 times



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

Community vote distribution

C (100%)

loopback0 Highly Voted 1 year, 4 months ago

Correct: C

As a general wireless networking rule, each wireless hop in a mesh network reduces the throughput of the link in half. As a result, wireless mesh networking may not be the most viable solution for environments that are required to support high-bandwidth or latency-intolerant applications. Meraki recommends limiting the amount of wireless hops to one (1) unless more are absolutely necessary to serve additional wireless clients.

upvoted 7 times

rnunes1110 Most Recent 3 months, 1 week ago

Selected Answer: C

Correct:

upvoted 1 times

rnunes1110 3 months, 1 week ago

Correct: C

upvoted 1 times

ajay4961 5 months, 1 week ago

Selected Answer: C

Kindly follow the below document and section "Maximizing Throughput".

https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Wireless_Throughput_Calculations_and_Limitations

upvoted 4 times

rnunes1110 4 months ago

Adding comment:

Maximizing Throughput

Meraki recommends that the end user is located no more than 3 hops away from the gateway. Each hop will reduce the bandwidth by 50%. For example, a 6 Mbps connection to a gateway will reduce to 3 Mbps at the second hop and 1.5 Mbps at the third hop.

upvoted 1 times

Jean226 10 months, 1 week ago

Selected Answer: C

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.

https://documentation.meraki.com/MR/Deployment_Guides/Mesh_Deployment_Guide

upvoted 3 times

🗨️ 👤 **azjimpang** 1 year, 1 month ago

Selected Answer: C

Maximum mesh hops

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.

https://documentation.meraki.com/MR/Deployment_Guides/Mesh_Deployment_Guide

upvoted 4 times

🗨️ 👤 **JerryKamb** 1 year, 3 months ago

https://documentation.meraki.com/MR/Deployment_Guides/Mesh_Deployment_Guide

Answer is C

upvoted 3 times

🗨️ 👤 **Netmanb2k** 1 year, 3 months ago

Agree C

https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Extending_the_LAN_with_a_Wireless_Mesh_Link

upvoted 3 times

🗨️ 👤 **adoua** 1 year, 3 months ago

Agree for C

upvoted 2 times

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: AB

Community vote distribution

AB (55%)

BE (30%)

AE (15%)

🗳️ **ilcarletto** 3 weeks, 2 days ago

B and E

Passthrough mode supports only Intrusion Detection and NOT Prevention. A is not correct

upvoted 2 times

🗳️ **yottabyte_** 1 month, 2 weeks ago

Selected Answer: AB

A & B

In Passthrough Mode, since the Meraki device is not actively performing routing functions or managing network traffic in the same way, High Availability is NOT SUPPORTED.

upvoted 1 times

🗳️ **sattori** 3 months, 1 week ago

Selected Answer: BE

High availability can be in both mode:

Routed mode

Passthrough or VPN Concentrator mode.

upvoted 1 times

🗳️ **MPIAZZAL** 4 months, 3 weeks ago

Selected Answer: AE

IPS + HA

upvoted 1 times

🗳️ **Gilgamesh_SHA** 7 months, 1 week ago

Selected Answer: AB

The answer is A & B.

upvoted 1 times

🗳️ **5448108** 7 months, 1 week ago

AB

You can enable intrusion prevention by setting the Mode drop-down to Prevention under Security & SD-WAN > Configure > Threat protection > Intrusion detection. It will be blocked by best effort if it is detected as malicious based on the detection ruleset specified above.

The Protected Network section is used to control the IP addresses or subnets of the systems protected. Entries should be separated by commas or blank space. It will protect only the subnets listed.

Note: The Protected Network section is only available for Security Appliances in Passthrough mode.

https://documentation.meraki.com/MX/Content_Filtering_and_Threat_Protection/Threat_Protection#:~:text=The%20MX's%20Intrusion%20Detection%20a

upvoted 2 times

🗳️ **jzzmth** 7 months, 4 weeks ago

Selected Answer: AE

Guys, I have this exact scenario in production right now and the answer is AE. We have two MX250s in passthrough mode for Intrusion

PREVENTION and they are setup in HA. While they can technically do site-to-site VPN, but if they did, they would be considered CONCENTRATORS

and not as pass-thru devices as per all Meraki official documentation as well as the description in the dashboard itself - thus AE is the most correct answer.

upvoted 1 times

🗨️ **AnyParka0B** 10 months ago

Selected Answer: AB

A,B

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

upvoted 2 times

🗨️ **XalaGyan** 1 year, 1 month ago

Selected Answer: BE

i have configured it for production and know that both B and E are possible. two VMX in HA and both in concentrator mode.

Answers BE

upvoted 2 times

🗨️ **nyashac** 1 year, 2 months ago

Selected Answer: AB

When in passthrough mode, the MX is best used for in-line:

Layer 3/7 firewall rules, traffic shaping, and analysis

Network asset discovery and reporting

Intrusion detection

Security and content filtering

Client and site-to-site VPN

upvoted 2 times

🗨️ **rnunes1110** 1 year, 3 months ago

Selected Answer: AB

Correct: A and B

upvoted 2 times

🗨️ **fredbarron010** 1 year, 4 months ago

<https://originalcerts.org/> Pass CCNA,CCNP,ITIL,Prince2,CITRIX,JUNIPER,AZURE,IBM,HP exams Pay After Results

upvoted 1 times

🗨️ **rnunes1110** 1 year, 4 months ago

A and B

upvoted 1 times

🗨️ **CaptainPirate** 1 year, 7 months ago

Intrusion prevention Yes

Site-to-site VPN Yes

Secondary uplinks No

DHCP No

High availability No

upvoted 2 times

🗨️ **Jean226** 1 year, 9 months ago

Selected Answer: BE

BE are correct

upvoted 2 times

🗨️ **zylike** 1 year, 10 months ago

Selected Answer: BE

The question was, which features ARE supported (not which are NOT), so: B and E

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

upvoted 2 times

🗨️ **CaptainPirate** 1 year, 7 months ago

champ according to the link you shared,the answer is A and B

Configuration Differences

There are a number of differences in configuration between Routed and passthrough modes on the MX:

Secondary uplinks cannot be used for Internet connectivity. Thus Security & SD-WAN > Configure > SD-WAN & traffic shaping > Uplink configuration only has the option for limiting bandwidth on WAN 1.

Site-to-site VPN can only operate in split-tunnel mode when configured as a hub. Traffic bound to VPN subnets must be directed to the MX.

DHCP is no longer available. DHCP requests will simply pass through the MX.

Cellular uplink is no longer available.

VLANs cannot be configured. The MX/Z1 will act as a bridge between the Internet and LAN ports.

upvoted 2 times

  **blahblah2** 1 year, 11 months ago

Selected Answer: AE

intrusion detection, it cannot do prevention so A and E

upvoted 1 times

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: AB

Community vote distribution

AB (83%)

UB (17%)

 **loopback0** Highly Voted 1 year, 10 months ago

Correct: A,B

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

upvoted 10 times

 **clrf26** Most Recent 3 months ago

Selected Answer: AB

Auto VPN registries Ports: UDP 9350-9381

Ports used for IPsec tunneling: Destination UDP port range 32768-61000

[https://documentation.meraki.com/MX/Site-to-site_VPN/Meraki_Auto_VPN_-_Configuration_and_Troubleshooting#:~:text=Ports%20used%20for%20IPsec%20tunneling%3A%20Source%20UDP%20port,%26%20SD-](https://documentation.meraki.com/MX/Site-to-site_VPN/Meraki_Auto_VPN_-_Configuration_and_Troubleshooting#:~:text=Ports%20used%20for%20IPsec%20tunneling%3A%20Source%20UDP%20port,%26%20SD-WAN%20%3E%20Monitor%20%3E%20VPN%20status%20page.)

[WAN%20%3E%20Monitor%20%3E%20VPN%20status%20page.](https://documentation.meraki.com/MX/Site-to-site_VPN/Meraki_Auto_VPN_-_Configuration_and_Troubleshooting#:~:text=Ports%20used%20for%20IPsec%20tunneling%3A%20Source%20UDP%20port,%26%20SD-WAN%20%3E%20Monitor%20%3E%20VPN%20status%20page.)

upvoted 2 times

 **Adrian1988** 3 months, 1 week ago

Any devices sitting upstream of a WAN Appliance will need the following destinations whitelisted so the WAN Appliance can communicate with the Auto VPN registries:

Port:

UDP 9350-9381

Ports used for IPsec tunneling:

Source UDP port range 32768-61000

Destination UDP port range 32768-61000

A-B

upvoted 1 times

 **rnunes1110** 10 months, 1 week ago

Selected Answer: AB

Correct: A & B

upvoted 1 times

🗨️ 👤 **Jean226** 1 year, 4 months ago

Pour contacter le registre VPN :

Plage de ports UDP source 32768-61000

Plage de ports UDP de destination 9350-9381

Pour le tunneling IPsec :

Plage de ports UDP source 32768-61000

Plage de ports UDP de destination 32768-61000

upvoted 1 times

🗨️ 👤 **azjimpang** 1 year, 7 months ago

Selected Answer: AB

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

upvoted 2 times

🗨️ 👤 **JerryKamb** 1 year, 9 months ago

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

Correct A B

upvoted 2 times

🗨️ 👤 **Netmanb2k** 1 year, 9 months ago

Should BE A&B

[https://documentation.meraki.com/MX/Site-to-](https://documentation.meraki.com/MX/Site-to-site_VPAutomatic_NAT_Traversal_for_Auto_VPN_Tunneling_between_Cisco_Meraki_Peers#:~:text=The%20peer%20connection%20process%20is,registry%20)

[site_VPAutomatic_NAT_Traversal_for_Auto_VPN_Tunneling_between_Cisco_Meraki_Peers#:~:text=The%20peer%20connection%20process%20is,registry%20](https://documentation.meraki.com/MX/Site-to-site_VPAutomatic_NAT_Traversal_for_Auto_VPN_Tunneling_between_Cisco_Meraki_Peers#:~:text=The%20peer%20connection%20process%20is,registry%20)

upvoted 4 times

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

Community vote distribution

B (100%)

 **loopback0** Highly Voted 1 year, 10 months ago

Correct: B


https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/High_Density_Wi-Fi_Deployments

upvoted 11 times

 **DRHoppo** Highly Voted 1 year, 10 months ago

agree with B: The math(s) are 70% of 1000 = 700/25 = 28, and 30% of 1000 = 300/25 = 12. use the greater number out the two calculations, therefore 28

upvoted 6 times

 **Jeff8989** 1 year, 7 months ago

This is not correct.

Number of Access Points = Max (Number of Access Points based on throughput, Number of Access Points based on client count).

upvoted 1 times


 **clrf26** Most Recent 3 months ago

Selected Answer: B

#APs = (Concurrent 5GHz clients) / 25

28 = (70% of 1000) / 25

upvoted 2 times

 **rnunes1110** 9 months, 3 weeks ago

Selected Answer: B


Correct: B

upvoted 1 times

 **Knightime14** 1 year ago

It's easier for me to remember that each AP can handle 25 concurrent 5GHz connections. I know it's essentially the same thing as the formula, it's just easier for me to remember.

upvoted 5 times

 **txami** 1 year, 7 months ago

Selected Answer: B

Agree with all, this calculation appears in


https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/High_Density_Wi-Fi_Deployments

upvoted 3 times

 **dustexam123** 1 year, 7 months ago

What if the question stated 100 users instead of 1000. What would the answer be then?

upvoted 1 times

 **Nathan_** 1 year, 5 months ago

That would be 3 as the formula is as followed


#APs = (Concurrent 5GHz clients) / 25

So that means

$$(70\% \text{ of } 100) / 25 = 2.8$$

and you need to round up so that means 3

upvoted 2 times

🗉  **rocketpluto** 1 year, 7 months ago

Correct answer is B - they are asking for client count and not the number of APs based on application. If they noted based on application then it would be aggregate app throughput/device throughput=number of APs. Depending on assumptions that could be C.

upvoted 1 times

🗉  **azjimpang** 1 year, 7 months ago

$$\#APs = (\text{concurrent 5 GHz clients}) / 25$$

$$= (70\% \times 1000) / 25$$

$$= 28$$

upvoted 2 times

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

Correct Answer: D

Community vote distribution

D (100%)

 **Ironman_2022** Highly Voted 2 years, 3 months ago

Selected Answer: D

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 practice for corporate-owned devices, 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%2C
upvoted 9 times

 **sattori** Most Recent 3 months, 1 week ago

Selected Answer: D

For school-owned iOS devices, it is highly recommended that administrators use Apple School Manager and Device Enrollment Program (DEP) whenever possible. These programs allow an administrator to enforce mandatory device supervision, customize device setup, and automate enrollment into Systems Manager in bulk. This means administrators can pre-configure devices online even before they arrive on site, and these devices will enroll in SM out of the box during the setup assistant, without having to first physically configure the devices.

https://documentation.meraki.com/SM/Deployment_Guides/Education_Deployment_Guide_and_Best_Practices
upvoted 1 times

 **Adrian1988** 9 months, 2 weeks ago

Correct:D

The best practice Systems Manager enrollment method when deploying corporate-owned iOS devices is typically using the "DEP (Device Enrollment Program)" or the "Automated Enrollment" method.

upvoted 1 times

 **rnunes1110** 1 year, 4 months ago

Selected Answer: D

Correct: D

upvoted 1 times

 **AGNote3** 2 years ago

Selected Answer: D

Apple Configurator 2.5 uses DEP: 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.

upvoted 2 times

 **LordHammer** 2 years, 1 month ago

per your documentation link DEP is part of APPLE configurator 2.5 or later. Also DEP is part of apple program? so why is it not APPLE Configurator 2.5?

Apple Configurator 2.5+ Automatic Enrollment

Automatic Enrollment through Apple Configurator only works on iOS devices that are in Apple's Device Enrollment Program (DEP), and allows you to pre-provision wireless settings on devices to seamlessly enroll during the device's setup assistant. Please be sure to add your Apple DEP account to Meraki Systems Manager before beginning this process, and ensure your devices are visible in Systems Manager > Manage > DEP.

upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (100%)

tliz Highly Voted 1 year, 1 month ago

Selected Answer: D

$$[(2-1)*(2*2)] + [50*2*1]$$

$$[(1)*(4)] + [100]$$

104

Auto VPN deployment (L1=2)
with two NAT-mode hubs (H=2)
with dual uplink connections (L=2) and
50 remote sites (S=50)
with a single uplink connection (L2=1)
upvoted 7 times

rnunes1110 Most Recent 4 months ago

Selected Answer: D

Correct: D

upvoted 1 times

bango 1 year, 2 months ago

agree with rsirica

Hub and Spoke - Hub Tunnel Count

$$[(H-1)*(L1*L1)] + [S*L1*L2]$$

Auto VPN deployment (L1=2) with two NAT-mode hubs (H=2) with dual uplink connections (L=2) and 50 remote sites (S=50) with a single uplink connection (L2=1)

upvoted 3 times

rsirica 1 year, 3 months ago

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

upvoted 3 times

rsirica 1 year, 3 months ago

Answer is 104

upvoted 4 times


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.

Correct Answer: C

Community vote distribution

C (100%)

 **hemmo1998** Highly Voted 2 years, 2 months ago


Selected Answer: C

Both the MS and MX support Warm Spare.
upvoted 6 times

 **sattori** Most Recent 3 months, 1 week ago

Selected Answer: C

Since answer A says only MX which is wrong, MS also supports warm spare (high availability) but with some limitations. For example MS390 and C9300-M series switches currently do not support MS Warm Spare (VRRP) functionality. MS Series switches can only be configured in pairs from the same family when using VRRP/Warm Spare. Integration with other vendors or platforms is currently not supported. MS250 can only be paired with another MS250.
upvoted 1 times

 **Adrian1988** 9 months, 2 weeks ago

Correct: C

Device Level Redundancy: Cisco Meraki devices, such as switches, security appliances, and wireless access points, often support high availability features within the same device category. For example:

Switch Stacking: Meraki switches can be stacked to create a single logical switch with redundant links between switches, providing resilience against switch failures.

Warm Spare (HA): Certain Meraki security appliances support a high availability (HA) configuration where a standby unit takes over in case the primary unit fails. This ensures continuous operation and minimal downtime.

AP Redundancy: Meraki wireless access points can be configured with redundancy, where nearby access points can provide coverage if one access point fails.
upvoted 1 times


 **Kiprotich** 1 year, 1 month ago

Meraki MS320 and MS420 switches supports Virtual Router Redundancy Protocol (VRRP) for warm spare failover. It brings high availability to mission critical MS products through Virtual Router Redundancy Protocol (VRRP), ensuring that if a VRRP-enabled Meraki switch goes offline, a backup MS will immediately take over its gateway responsibilities.
upvoted 1 times

 **rnunes1110** 1 year, 3 months ago

Selected Answer: C

Correct: C
upvoted 1 times

 **txami** 2 years, 1 month ago

Agree, C is correct:
[https://documentation.meraki.com/MS/Layer_3_Switching/MS_Warm_Spare_\(VRRP\)_Overview](https://documentation.meraki.com/MS/Layer_3_Switching/MS_Warm_Spare_(VRRP)_Overview)
upvoted 4 times

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

Community vote distribution

C (100%)

 **rnunes1110** 4 months ago

Selected Answer: C

Answer is C

Enabling SM Sentry Enrollment

When enabled on a given SSID for a Cisco Meraki wireless AP, Sentry facilitates the secure and rapid onboarding and deployment of SM to mobile devices. Sentry enrollment is supported on Android, iOS, macOS, and Windows devices and enables employee self-service for securing BYOD devices.

If the device is not enrolled in an existing SM network, the user is prompted with a click to accept message that will enroll the device into the SM network as well as provide any configuration profiles and required apps previously configured.


SM Sentry enrollment can be enabled on any MR network via the Splash page section of the Wireless > Configure > Access control page
upvoted 1 times

 **LordHammer** 1 year ago

https://documentation.meraki.com/SM/Deployment_Guides/Systems_Manager_Sentry_Overview

yeah C ...wired is there but not supporting certain devices yet

upvoted 1 times

 **exlstde** 1 year, 1 month ago

Selected Answer: C

C

https://documentation.meraki.com/MR/MR_Splash_Page/Systems_Manager_Sentry_Enrollment

upvoted 3 times

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

Community vote distribution

C (100%)

🗳️ **loopback0** Highly Voted 2 years, 4 months ago

Correct: C

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

upvoted 9 times

🗳️ **alfonsocav1982** Highly Voted 2 years, 4 months ago

Selected Answer: C

Correct: C

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.

upvoted 5 times

🗳️ **sattori** Most Recent 3 months ago

Selected Answer: C

Actually stateful firewall database is supported in both mode (Routed mode and Passthrough Mode) but DHCP association database is supported only in Routed mode. Anyways the question says in High Availability pair which is DHCP association make sense.

upvoted 1 times

🗳️ **sattori** 3 months, 1 week ago

Selected Answer: C

The question should contains in which mode, if Routed Mode then DHCP association database, if Passthrough Mode then stateful firewall database. Poor question.

upvoted 1 times

🗳️ **AnyParka0B** 10 months ago

Selected Answer: C

MX appliances do not use spanning-tree.

upvoted 1 times

🗳️ **rnunes1110** 1 year, 4 months ago

Selected Answer: C

Correct: C

agree with the guys!

upvoted 1 times

🗳️ **donAdriano** 2 years, 2 months ago

C

The MXs in a routed mode high-availability pair exchange DHCP state information over the LAN on UDP port 3483. This prevents a DHCP IP address from being handed out to a client after a failover if it has already been assigned to another client prior to the failover.

upvoted 4 times

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: AB

Community vote distribution

AB (100%)

🗨️ **sattori** 3 months, 1 week ago

Selected Answer: AB

If an unauthenticated client has full network access and they are not whitelisted, check the following:

1. Is the "allow non_HTTP access prior to sign-on" setting enabled under Wireless > Configure > Access control > Captive portal strength? This setting permits full network access, with the exception of HTTP (TCP Port 80), prior to authentication. If you do not want clients to access network resources outside of the Walled Garden without being authenticated or whitelisted, the Captive Portal Strength should be set to "Block all access prior to sign-on".
2. If Controller disconnection behavior is set to "Open" and the Splash URL/Cloud controller is unreachable, the client will be allowed full access until the Splash URL becomes available. Set this to "Restricted" to block network access until the URL is available.

upvoted 1 times

🗨️ **rnunes1110** 1 year, 3 months ago

Selected Answer: AB

Correct: A and B

If we have to choose one, I'll go with A and B

upvoted 1 times

🗨️ **rnunes1110** 1 year, 4 months ago

I think we are missing an answer, for me, for the unauthenticated user to have full network access you should put your network in the WALLED GARDEN, this option does this.

upvoted 1 times

🗨️ **goyeyemi** 1 year, 10 months ago

connection disconnection behavior and captive portal strength

upvoted 2 times

🗨️ **18HandsOfLohan** 2 years ago

Selected Answer: AB

AB is correct.

Refer: https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Splash_Page

upvoted 3 times

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.

Correct Answer: DE

Community vote distribution

DE (88%)


13%

 **azjlpang** Highly Voted 2 years, 1 month ago

Selected Answer: DE

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
upvoted 5 times

 **sattori** Most Recent 3 months, 1 week ago

Selected Answer: DE

A Cisco Meraki AP accomplishes containment by sending deauthentication packets with the spoofed MAC address of the rogue access point (the BSSID of the rogue wireless network). The deauthentication packets force any clients that are connected to the rogue access point to disconnect. If a client attempts to connect to the rogue network, they will be immediately forced off by the Air Marshal.

upvoted 1 times

 **rnunes1110** 1 year, 3 months ago

Selected Answer: DE

D and E

upvoted 2 times

 **rnunes1110** 1 year, 4 months ago

Selected Answer: AD

I think the question is "malicious" 'cause is not saying that the user is connected in the rogue SSID, is saying that the Air Marshall has identified this rogue SSID, so for me the answer is: A & D

upvoted 1 times

 **rnunes1110** 1 year, 3 months ago

I'd like to change my Answer to D and E, I agree with @azjlpang

upvoted 2 times

 **azjlpang** 2 years, 1 month ago

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
upvoted 1 times

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

Custom performance classes	Name	Maximum latency (ms)	Maximum jitter (ms)	Maximum loss (%)	Actions
	Conf	200	50	5	×
	Create a new custom performance class				

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

Community vote distribution

B (50%) A (50%)

Idsj Highly Voted 1 year, 10 months ago

Selected Answer: B

Trick question, WebEx traffic goes over Internet flow not VPN. Custom settings don't apply. B upvoted 5 times

CiscoExam 1 year, 9 months ago

But it's not running a split tunnel for WebEx.
upvoted 2 times

sattori Most Recent 3 months, 1 week ago

Selected Answer: A

Look at Uplink Selection Policy and Traffic Filters (Webex).
upvoted 1 times

jznmth 7 months ago

Selected Answer: B

"B", because SD-WAN policies ONLY apply to VPN traffic.

upvoted 1 times

🗨️ **John_Walker** 1 year, 8 months ago

Selected Answer: A

Answer is A

upvoted 2 times

🗨️ **CiscoExam** 1 year, 9 months ago

It says full tunnel with the peer. So, webex IS expected to flow over SD-WAN / VPN. It's A.

upvoted 3 times

🗨️ **MN23** 2 years, 1 month ago

Selected Answer: A

it is A

upvoted 1 times

🗨️ **MN23** 2 years, 1 month ago

I agree it is A

read this article under "VPN Traffic and Custom Performance Classes"

https://documentation.meraki.com/MX/Firewall_and_Traffic_Shaping/MX_Load_Balancing_and_Flow_Preferences#Internet_Traffic
point 4 "WAN 1/WAN 2 - Traffic will use this uplink until the Fail over if condition is met:"

upvoted 2 times

🗨️ **JerryKamb** 2 years, 3 months ago

Selected Answer: A

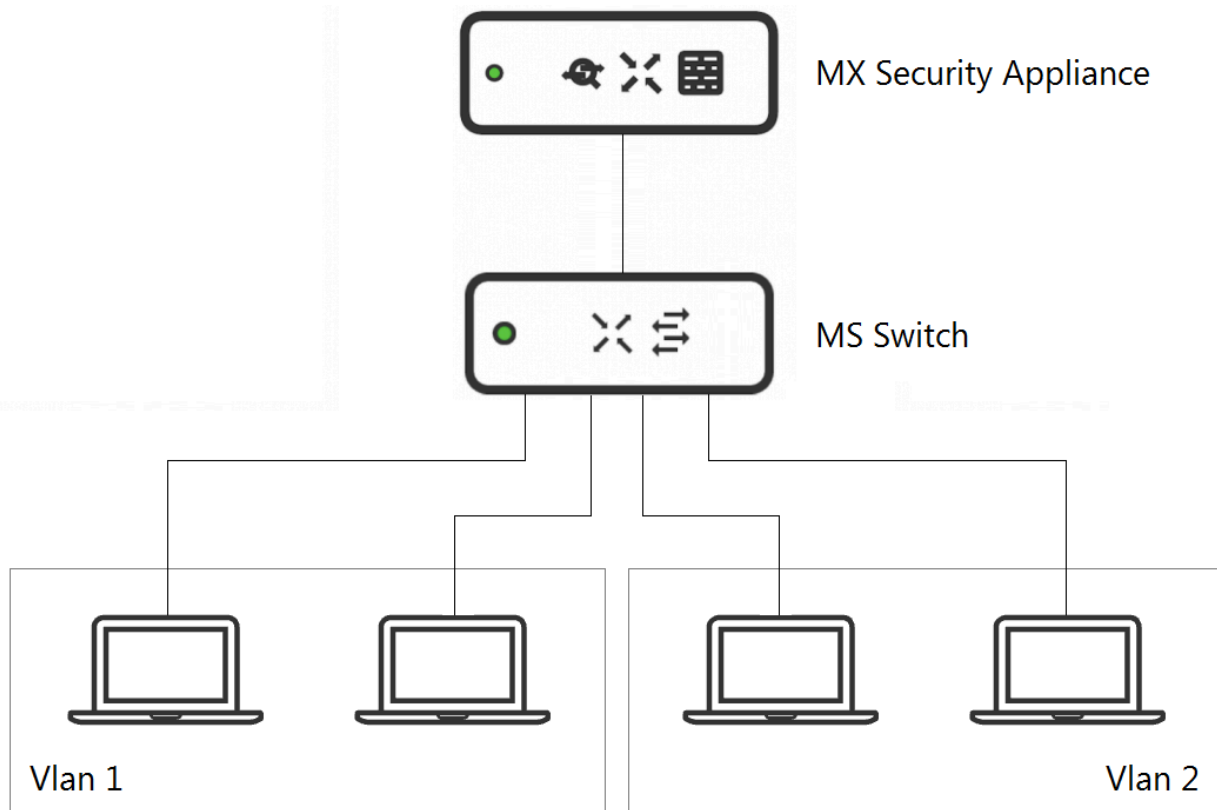
I agree with "A" also. But would like to see documentation on this.

upvoted 3 times

🗨️ **yuskehcl** 2 years, 3 months ago

It's A, It' would prefer WAN 2 over the default uplink

upvoted 4 times



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.

Correct Answer: A

Community vote distribution

A (100%)

DRHoppo Highly Voted 1 year, 10 months ago

Answer A: Intrusion Detection and Prevention

Intrusion detection feeds all packets flowing between the LAN and internet interfaces, and in between VLANs through the SNORT® intrusion detection engine, and logs the generated alerts to the Security Report. You can export these alerts via Syslog.

reference:

https://documentation.meraki.com/MX/Content_Filtering_and_Threat_Protection/Threat_Protection

upvoted 10 times

WickedShammy Most Recent 6 months, 2 weeks ago

A is the correct answer. From this:

https://documentation.meraki.com/MX/Content_Filtering_and_Threat_Protection/Threat_Protection#Intrusion_Detection_and_Prevention

Intrusion Detection and Prevention

In both IDS and IPS modes the following is inspected:

all traffic between LAN and Internet (this is both modes, IPS/IDS)

all traffic between VLANS (this is both modes, IPS/IDS)

In both IDS and IPS modes the following is not inspected:

INTRA-VLAN traffic (where Client 1 and Client 2 are both in the same VLAN)

upvoted 1 times

  **rnunes1110** 9 months, 3 weeks ago

Selected Answer: A

Correct: A

upvoted 1 times

  **CaptainPirate** 1 year ago

A IS THE CORRECT ANSWER

upvoted 1 times

  **18HandsOfLohan** 1 year, 6 months ago

Selected Answer: A

Answer A (as only IDS/IPS applies to inter-vlan routing, AMP 'only' inspects HTTP traffic)

upvoted 2 times

Meraki

NETWORK

EMEAR-TRAINER-DEMO

Network-wide

Security & SD-WAN

Switch

Wireless

Cameras

Insight

Organization

SD-WAN & traffic shaping

Uplink configuration

WAN 1 [details](#)

WAN 2 [details](#)

Cellular [details](#)

Uplink statistics	Test connectivity to	Description	Default	Actions
	8.8.8.8	Google	<input checked="" type="radio"/>	×

[Add a destination](#)

List update interval [simple](#)

Cellular

Uplink selection

Global preferences

Primary uplink

Load balancing Enabled Disabled

Flow preferences

Internet traffic There are no uplink preferences for Internet traffic configured on this network.

[Add a preference](#)

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: CE

Community vote distribution

CE (100%)

runes1110 4 months ago

Selected Answer: CE

C and E for sure:

The MX can be configured 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. The load distribution is based on the WAN 1 and WAN 2 throughput configured under Uplink configuration, such that the uplink with more throughput will distribute more flows.

In the example below, WAN 1 is configured to pass 50Mb/s, and WAN 2 is configured to pass 10Mb/s. Since the download speed ratio is 5/1, for every five flows sent over WAN 1, a single flow will be sent over WAN 2:

Refer: https://documentation.meraki.com/MX/Firewall_and_Traffic_Shaping/MX_Load_Balancing_and_

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

Community vote distribution

A (100%)

 **7e5b855** 3 months ago

Selected Answer: A

I agree with azjImpang
upvoted 1 times

 **rnunes1110** 1 year, 4 months ago

Selected Answer: A

Answer: A
upvoted 1 times

 **azjImpang** 2 years, 1 month ago

Selected Answer: A

Fast Lane

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

upvoted 2 times

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

Community vote distribution

A (100%)

🗨️ **Adrian1988** 3 months, 1 week ago

Selected Answer: A

When using OSPF (Open Shortest Path First) on a Cisco Meraki MX (Security Appliance), the authentication protocol commonly used for securing OSPF neighbor relationships is OSPF MD5 authentication. This protocol ensures that OSPF packets exchanged between OSPF-enabled routers are authenticated using MD5 (Message Digest Algorithm 5), thereby preventing unauthorized access or tampering of OSPF routing information.

upvoted 1 times

🗨️ **rnunes1110** 9 months, 3 weeks ago

Selected Answer: A

Answer is A, for sure !

upvoted 1 times

🗨️ **azjimpang** 1 year, 7 months ago

Selected Answer: A

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

upvoted 2 times

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

Community vote distribution

D (100%)

🗨️ **sattori** 3 months, 1 week ago

Selected Answer: D

Band steering detects clients capable of 5 GHz operation and steers them to that frequency, leaving the more crowded 2.4 GHz band available for legacy clients, which helps improve the end-user experience. When band steering is enabled on an SSID, APs will stop advertising that SSID in 2.4 GHz beacons.

upvoted 1 times

🗨️ **rnunes1110** 1 year, 3 months ago

Selected Answer: D

I'm not sure, but by exclusion, I vote for E

upvoted 1 times

🗨️ **rnunes1110** 1 year, 3 months ago

D I mean

upvoted 1 times

🗨️ **azjimpang** 2 years, 1 month ago

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

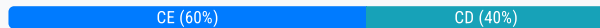
upvoted 3 times

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: CE

Community vote distribution



7e5b855 3 months ago

Selected Answer: CE

Maximum retention limit is a only set the maximum period of time that the camera will store video. Note that the actual retention depends on the configuration.

upvoted 1 times

sattori 3 months, 1 week ago

Selected Answer: CD

The answer C is pretty obvious. Some users may want to limit how much footage their cameras can retain (for example, to meet regulatory requirements). To address this, maximum retention limits can be enabled. Footage will be recorded and deleted in the same way as before, on a first-in-first-out basis, until the maximum retention time is reached. So answer is D.

upvoted 1 times

jzmmth 7 months ago

Selected Answer: CE

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

A - Is not an option available to us

B - Is not an option available to us

C - Yes this will work because by default the MV records continuously

D - This option is available to us, but would have the opposite effect as it discards footage older than the specified threshold

E - Yes this will work because again by default the MV records continuously

upvoted 2 times

murdockhd 1 year ago

Must be CE because enabling the retention limit doesn't improve the retention.

upvoted 1 times

rnunes1110 1 year, 3 months ago

Selected Answer: CE

Answer: C and E

upvoted 2 times

alejandro12 1 year, 3 months ago

Selected Answer: CD

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

upvoted 2 times

tliz 2 years, 1 month ago

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.

upvoted 3 times

tliz 2 years, 1 month ago

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

Motion-based retention covers this requirement and improves the video retention capabilities of the camera
upvoted 2 times

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

Community vote distribution

C (100%)

 **pruebawork92** Highly Voted 2 years, 3 months ago

I think is C

"nce an MX Security Appliance network has been bound to a template, some options can still be configured normally through the dashboard. Any local configuration changes made directly on the MX network will override the template configuration."

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.](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.)


upvoted 7 times

 **sattori** Most Recent 3 months, 1 week ago

Selected Answer: D

Once a template has been created, networks that are bound to it will utilize its configuration as a base. Any changes made to the template will then be pushed out to all bound networks. When binding an existing network to a template, its current configuration will be lost and it will begin using the template configuration.

upvoted 2 times

 **yottabyte_** 1 month, 1 week ago

Agree with this

upvoted 1 times

 **Adrian1988** 9 months, 1 week ago

Selected Answer: C

Once a WAN Appliance network has been bound to a template, some options can still be configured normally through the dashboard. Any local configuration changes made directly on the WAN Appliance network will override the template configuration.

upvoted 2 times

 **WickedShammy** 1 year ago

Answer is C

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](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)

Once a WAN Appliance network has been bound to a template, some options can still be configured normally through the dashboard. Any local configuration changes made directly on the WAN Appliance network will override the template configuration.

upvoted 1 times


 **rnunes1110** 1 year, 4 months ago

Selected Answer: C

I'm pretty sure that is C

I always argue with the guys in my team that does configs directly in a network that is bound in a Template, and the config is applied !

upvoted 2 times

 **Gbgreat** 1 year, 4 months ago

It is a A. The change was done to the MX network not the local device.

upvoted 1 times

🗨️ 👤 **CaptainPirate** 1 year, 7 months ago

its obviously C

upvoted 1 times

🗨️ 👤 **18HandsOfLohan** 2 years ago

Selected Answer: C

C should be correct.

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](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)

upvoted 2 times

🗨️ 👤 **Ironman_2022** 2 years, 3 months ago

Answer C, the local change overrides template config, and subsequent changes on template will not override the local changes.

upvoted 2 times

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.

switch management IP	Cloned
switch name	
port name	
interface type	Not Cloned
STP bridge property	

Correct Answer:

switch management IP	Cloned
switch name	
port name	
interface type	Not Cloned
STP bridge property	

Jeff8989 Highly Voted 2 years ago

Cloned:

Port name

Interface type

STP bridge priority

Not cloned:

Switch name

Switch management IP

upvoted 8 times

MPIAZZAL Most Recent 5 months ago

need to change the "Correct Answer image":

Not cloned:

Switch name

Switch management IP

upvoted 2 times

🗉 👤 **Kiprotich** 1 year ago

The following settings will be cloned from the source switch to the destination switch:

Port Name

Port Tags

Interface state

Spanning tree

STP guard / BPDU guard

PoE

Link

Port schedules (access only)

Interface Type

Adaptive Policy Group

Adaptive Policy Peer SGT Configuration

Access policy (access only)

(ignored if the source access policy doesn't exist in the destination network)

MAC whitelist (access only)

Whitelisted MACs (access only)

Sticky MAC whitelist (access only)

Whitelist size limit (access only)

Native VLAN (trunk only)

Allowed VLANs (trunk only)

VLAN (access only)

Voice VLAN (access only)

switch-level configurations that will not be cloned as part of this process:

Management IP

Switch Name

Any Layer 3 Settings (such as: interfaces, DHCP, multicast, OSPF)

Any of these configs that need to be cloned will have to be copied and input manually after the cloning process.

upvoted 2 times

🗉 👤 **Naphat** 1 year, 3 months ago

Cloned:

STP bridge priority

Port mirroring

Port level

- Port name

- Interface type

Not cloned:

Switch name

Switch management IP

upvoted 2 times

🗉 👤 **rnunes1110** 1 year, 3 months ago

Cloned:

port name

Interface Type

STP bridge property

Not Cloned:

switch management IP

switch name

Please take into consideration that there are some switch-level configurations that will not be cloned as part of this process:

Management IP

Switch Name

Any Layer 3 Settings (such as: interfaces, DHCP, multicast, OSPF)

Any of these configs that need to be cloned will have to be copied and input manually after the cloning process.

Ref.: https://documentation.meraki.com/MS/Other_Topics/Switch_Cloning

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.akamaitech nologies.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.akamaitech nologies.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.akamaitech nologies.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.akamaitech nologies.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

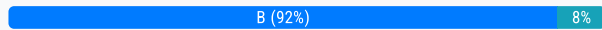
Actions Rule details
Inspect picklist
Show this signature only

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

Community vote distribution



azjimpang Highly Voted 1 year, 1 month ago

Selected Answer: B

Intrusion Prevention

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

upvoted 7 times

rnunes1110 Most Recent 4 months ago

Selected Answer: B

Answer: B

There's no option to "blocking", despite the log is showing block. The options are:

- Disabled
- Detection
- Prevention

I'm pretty sure, I accessed one of our MX to check!

upvoted 3 times

CaptainPirate 7 months ago

Key word:Blocked

upvoted 1 times

ST1996 1 year, 1 month ago

Selected Answer: B

Answer is B IPS since an action has been taken (DROP)

upvoted 1 times

ST1996 1 year, 1 month ago

Selected Answer: C

This is a Prevention since an action has been taken (DROP)

upvoted 1 times

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

Correct Answer:

enroll

create profile

create profile

add settings profile

add settings profile


enroll

define tags

define tags

apply profile

apply profile

 **IAZZUS** 8 months, 2 weeks ago

Enroll

Define tags

Create profile

Add Settings

Apply profile

upvoted 4 times

 **clrf26** 9 months ago

Enroll

Tags

Create Profile

Add Settings

Apply

upvoted 2 times

 **Petermajernik** 10 months ago

Enroll>Tags>Create Profile>Add Settings>Apply

upvoted 4 times

 **AnyParka0B** 10 months ago

Create profile
Define tags
Add settings profile
Apply profile
Enroll
upvoted 2 times

🗨️ 👤 **CaptainPirate** 1 year, 7 months ago
<https://meraki.cisco.com/blog/2014/10/automation-the-key-to-scaling/>
upvoted 1 times

🗨️ 👤 **Jean226** 1 year, 9 months ago
Enroll > Create profile > add settings profil> define tags > apply profile
upvoted 1 times

🗨️ 👤 **cdipman2** 1 year, 11 months ago
enroll>create profile> add settings profile > define tags >apply profile
upvoted 3 times

🗨️ 👤 **iuheioughfoier** 1 year, 10 months ago
Are you sure? I'm still fuzzy on the order the article recommends, let alone whether the create/apply profile part is about enrollment profile or settings.

https://documentation.meraki.com/SM/Deployment_Guides/Enterprise_Deployment_Guide_and_Best_Practices
upvoted 1 times


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.

Correct Answer: A

Community vote distribution

A (100%)


 **Netmanb2k** Highly Voted 2 years, 3 months ago

i think its A

By default, iOS apps provisioned through Systems Manager that are found in the App Store will self-update 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

upvoted 9 times

 **Netmanb2k** Highly Voted 2 years, 3 months ago

Selected Answer: A

i think its A

By default, iOS apps provisioned through Systems Manager that are found in the App Store will self-update 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

upvoted 5 times

 **sattori** Most Recent 3 months, 1 week ago

Selected Answer: A

Since the question does not mention what kind of app talking about I pick answer A. Custom iOS apps and custom B2B (business-to-business) apps can not be updated automatically and require a manual update push from the dashboard. Three types of manually updating:

Option 1 - Update app on all devices

Option 2 - Update app on individual device

Option 3 - Update all apps on all devices

However by default, iOS apps provisioned through Systems Manager that are found in the App Store will self-update if automatic updates have been enabled in the dashboard and device settings.

upvoted 1 times

 **rnunes1110** 1 year, 3 months ago

Selected Answer: A

Correct: A

upvoted 1 times

 **donAdriano** 2 years, 2 months ago

A

Automatic Updates

By default, iOS apps provisioned through Systems Manager that are found in the App Store will self-update if automatic updates has been turned on in the Settings.

upvoted 2 times

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

Community vote distribution

C (100%)

 **Ironman_2022**  2 years, 3 months ago

Selected Answer: C

there is no where to set a preserved setting, has to be a syslog server for 'complete' historical preservation.

upvoted 9 times

 **rnunes1110** 1 year, 3 months ago

I agree (and the Meraki's log is terrible, btw)


upvoted 1 times

 **sattori**  3 months, 1 week ago

Selected Answer: C

if a complete historical log is necessary, implementing a syslog server is recommended to maintain logs as long as needed.

upvoted 1 times

 **Adrian1988** 9 months, 2 weeks ago

Answer: C

The Cisco Meraki best practice method that preserves complete historical network event logs is to configure Syslog Export to an external syslog server.

By configuring Syslog Export to an external syslog server, you ensure that all network event logs generated by Cisco Meraki devices, such as MX Security Appliances, MS Switches, and MR Wireless Access Points, are securely transmitted and stored on an external syslog server.

upvoted 1 times

 **Kiprotich** 1 year ago

best practice method for preserving complete historical network event logs is to implement a syslog server. This will allow you to maintain logs for as long as needed.

Can be done via Network-wide > Monitor > Event log.

Answer: C

upvoted 1 times

 **Cmontet** 1 year, 1 month ago

The correct answer is C

upvoted 1 times

 **rnunes1110** 1 year, 3 months ago

Selected Answer: C

Answer: C


upvoted 1 times

 **Wooker** 2 years, 1 month ago

Selected Answer: C

should be C



upvoted 1 times

 **txami** 2 years, 1 month ago

Selected Answer: C

No preserving setting, you need an external syslog server for 30 days older messages.

upvoted 1 times

  **dostarr** 2 years, 3 months ago

C. Syslog server boyz.

https://documentation.meraki.com/General_Administration/Monitoring_and_Reporting/Viewing_Old_Event_Logs

upvoted 2 times

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

Community vote distribution

D (100%)

🗨️ **sattori** 3 months, 1 week ago

Selected Answer: D

Nothing wrong with question it is indeed Syslog versus SNMP, because only Syslog supports Device Flows SNMP and API/Webhooks don't, and vice versa SNMP and API/Webhooks support Client Connectivity but Syslog does not.

upvoted 1 times

🗨️ **WickedShammy** 1 year ago

Actually it is none of the above based on this document at the bottom. Only Device flows is in the Syslog. SNMP offers Client Connectivity, Proactive Alerts, Automation, and Organization-wide Information Gathering, but does not offer device flows.

https://documentation.meraki.com/General_Administration/Monitoring_and_Reporting/Meraki_Device_Reporting_-_Syslog%2C_SNMP%2C_and_API
upvoted 1 times

🗨️ **Kiprotich** 1 year ago

Syslog is implemented to meet the design requirement of gathering information such as flows and client connectivity

upvoted 1 times

🗨️ **M0nkk3y** 1 year, 1 month ago

Answer: C

Syslog allows Organization-wide information gathering but SNMP don't.

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

By other hand, Syslog allow client connectivity but not device flows which is for SNMP method, that's why I think answer D is incorrect.

upvoted 3 times

🗨️ **rnunes1110** 1 year, 3 months ago

Selected Answer: D

Answer: D

But I think the question should be "Which design requirement is met by implementing syslog AND (not versus) SNMP ?"

upvoted 1 times

🗨️ **tliz** 2 years, 1 month ago

Selected Answer: D

See Choosing a Reporting Method section

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

upvoted 4 times

WAN Health For the last 2 hours

Uplink Status	Network Name	Uplink Type	ISP	Availability	Total Usage	Average Throughput	Loss	Average Latency	Jitter
Ready	Meraki Sydney – appliance	WAN 1	unknown		↓ 4.03 GB, ↑ 1.39 GB	↓ 4.44 Mb/s, ↑ 1.55 Mb/s	0.00%	4.33 ms	0.05 ms
Active	Meraki Sydney – appliance	WAN 2	anticklockwise.net.au		↓ 23.18 GB, ↑ 14.85 GB	↓ 25.00 Mb/s, ↑ 15.39 Mb/s	0.00%	0.79 ms	0.06 ms

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

Correct Answer: C

Community vote distribution

C (67%)

A (33%)

Ironman_2022 Highly Voted 2 years, 3 months ago

Correct this should be C

https://documentation.meraki.com/MI/MI_WAN_Health#:~:text=Current%20loss%20and%20latency%20statistics,address%20is%20set%20to%208.8.8
upvoted 7 times

7e5b855 Most Recent 3 months ago

Selected Answer: C

SD-WAN & traffic shaping --> Uplink statistics is used to generate Wan Health.

Reports to which ping destination uplink statistics are reporting. Set the network default ping destination on the Traffic Shaping page.
upvoted 1 times

sattori 3 months, 1 week ago

Selected Answer: A

Answer C indicates Uplink statistics but exhibit indicates WAN Health Dashboard which is part of MI (Meraki Insight)
upvoted 1 times

rnunes1110 1 year, 3 months ago

Selected Answer: C

Answer: C
upvoted 2 times

18HandsOfLohan 2 years ago

Selected Answer: C

I'll go with C too!
upvoted 1 times

18HandsOfLohan 2 years ago

Definitely C!

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.
upvoted 2 times

LordHammer 2 years ago

A is correct even look at the link says meraki insights wan health