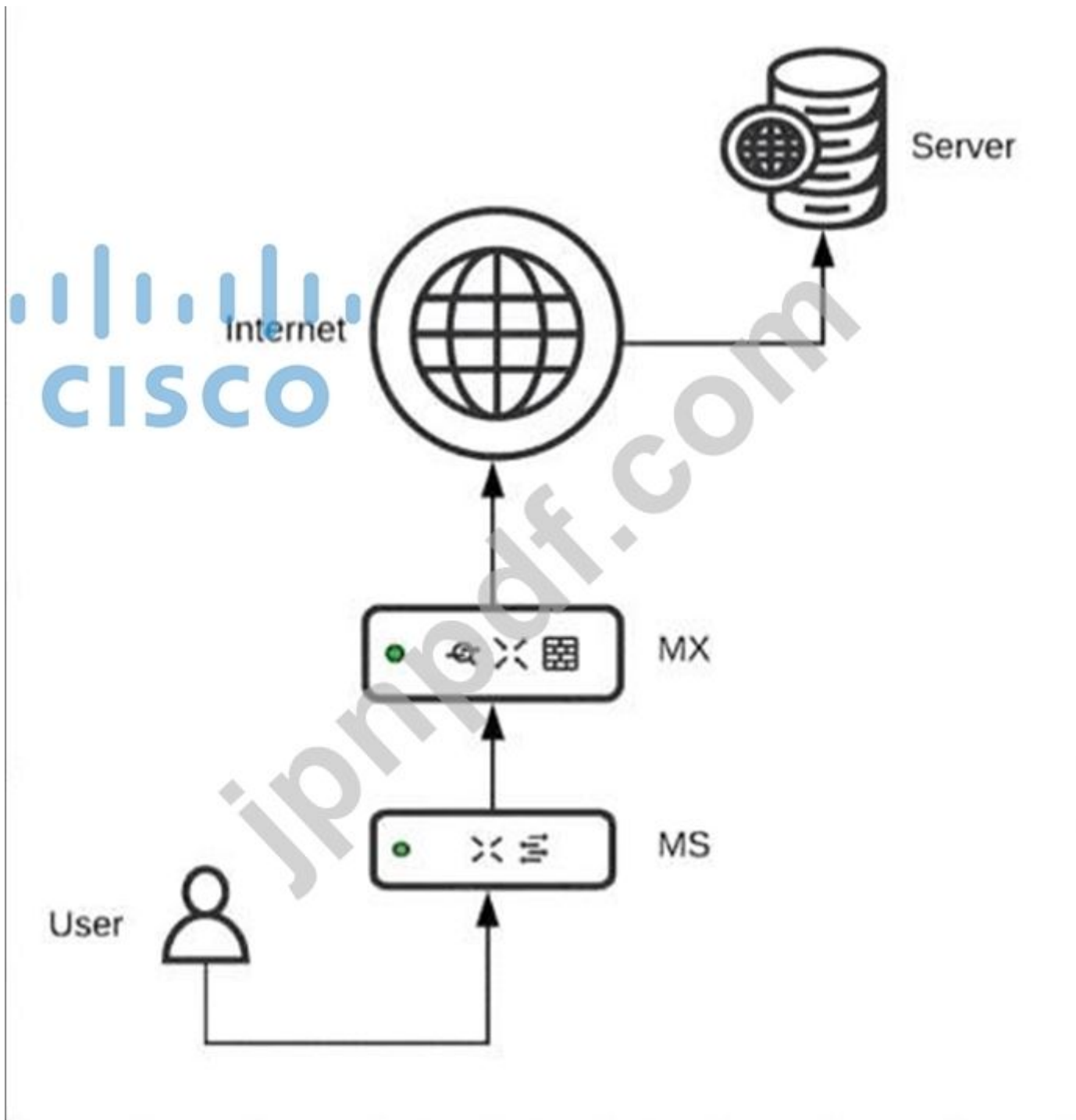


Cisco.500-220.v2024-02-12.q42

試験コード:	500-220
試験名称:	Engineering Cisco Meraki Solutions
認定資格:	Cisco
無料問題数:	42
バージョン:	v2024-02-12
アクセス数:	277
ページビュー数:	420
https://www.jpnpdf.com/Cisco.500-220.v2024-02-12.q42-mondaishu.html	

最新問題: 1

展示を参照してください。



ユーザが Cisco Meraki Insight を使用してアクセスしているカスタム アプリケーションを正常に監視するには、どの 2 つの設定が必要ですか? (2つお選びください)

- A. カスタム アプリケーションは任意のポートで TLS を使用します。
- B. カスタム アプリケーションはポート 8080 で HTTP を使用します。
- C. カスタム アプリケーションは TCP 443 で HTTPS を使用します。
- D. カスタム アプリケーションは SMB/CIFS を使用します。
- E. カスタム アプリケーションはポート 8080 で HTTPS を使用します。

Answer: B,C (メッセージを残す)

説明

https://documentation.meraki.com/MI/MI_Web_App_Health/Overview#:~:text=On%20this%20page%2C%20yo

最新問題: 2

ネットワーク管理者は、Meraki AP 間のワイヤレス メッシュ情報を調査するにはどこに移動すればよいですか？

- A. ワイヤレス > モニター > ワイヤレスの状態
- B. ワイヤレス > モニター > RF スペクトル
- C. ワイヤレス > 設定 > 無線設定
- D. ワイヤレス > モニター > アクセス ポイント > AP > RF

Answer: D ([メッセージを残す](#))

最新問題: 3

Systems Manager Sentry 登録を使用できるようにするには、Systems Manager に加えてどの Cisco Meraki 製品を導入する必要がありますか？

- A. MS スイッチ
- B. Meraki インサイト
- C. MR アクセス ポイント
- D. MV スマート カメラ

Answer: C ([メッセージを残す](#))

説明

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

最新問題: 4

Cisco Meraki のベスト プラクティスに従って、左側のステップを右側のシーケンスにドラッグ アンド ドロップしてデバイス制御を管理します。

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

Answer:

enroll	create profile
create profile	add settings profile
add settings profile	enroll
define tags	define tags
apply profile	apply profile

説明

create profile
add settings profile
enroll
define tags
apply profile

中程度の信頼度で自動的に生成されるテーブルの説明

最新問題: 5

サインオン スプラッシュ ページを有効にして SSID を構成する場合、認証されていないクライアントが完全なネットワーク アクセスを持ち、許可リストに登録されないようにするために構成する必要がある 2 つの設定はどれですか? (2つお選びください。)

- A. スプラッシュ ページ設定の RADIUS
- B. ファイアウォールとトラフィック シェーピング
- C. キャプティブ ポータルの強度
- D. 同時ログイン
- E. コントローラーの切断動作

Answer: C,E ([メッセージを残す](#))

説明

明確にするために、サインオン スプラッシュ ページを有効にして SSID を構成する場合、認証されていないクライアントが完全なネットワーク アクセスを持ち、許可リストに登録されないように構成する必要がある 2 つの設定は次のとおりです。

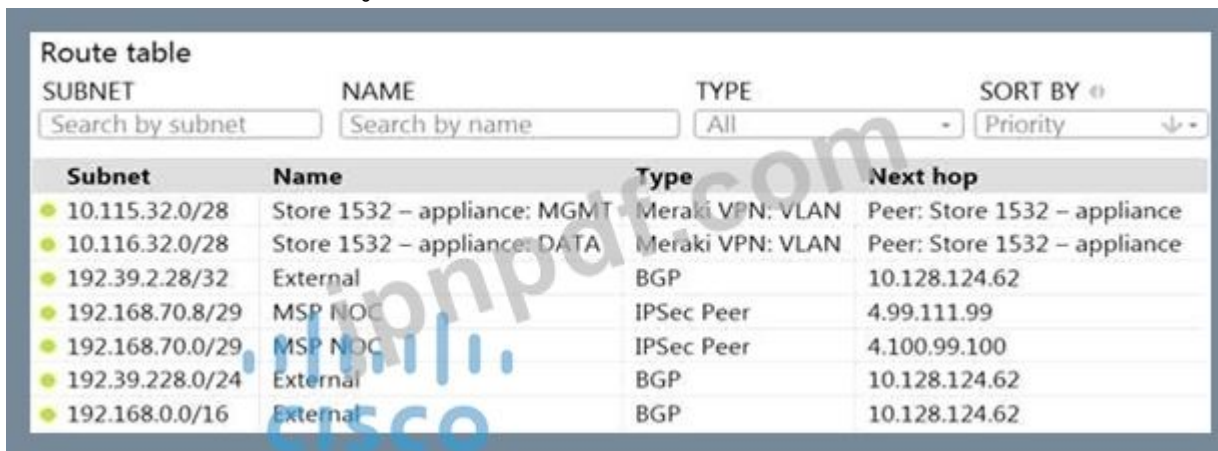
コントローラーの切断動作: この設定は、Meraki クラウド コントローラーに到達できない場合にクライアントがどのように処理されるかを決定します。オプションは「制限付き」または「無制限」です。前者のオプションは、コントローラーが再び到達可能になるまで、認証されていないクライアントからのすべてのトラフィックをブ

ロックします。後者のオプションでは、コントローラが再び到達可能になるまで、認証されていないクライアントがサインオンせずにネットワークにアクセスできます1。

キャプティブ ポータルの強度: この設定は、クライアントが認証のためにスプラッシュ ページにリダイレクトされる頻度を決定します。オプションは、サインオンが完了するまですべてのアクセスをブロックするか、サインオン前に非 HTTP トラフィックを許可するです。後者のオプションでは、認証されていないクライアントは DNS、DHCP、ICMP などの他のプロトコルにアクセスできますが、サインオンするまで HTTP および HTTPS トラフィックはブロックされます。このオプションは、Web ベースの認証をサポートしていないデバイスとの互換性のために推奨されます1。

最新問題: 6

展示を参照してください。



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

送信元 IP 10.168.70.3、宛先 IP 10.116.32.4 のパケットが VPN コンセントレータに到着します。このコンセントレータ ルーティング テーブルに基づくパケットのネクスト ホップは何ですか？

- A. コンセントレータ ゲートウェイ (10.128.124.62) がネクスト ホップです。
- B. パケットは停止されています。
- C. 次のホップを決定するのに十分な詳細がありません。
- D. Auto VPN ピア 「ストア 1532 - アプライアンス」はネクスト ホップです。

Answer: C ([メッセージを残す](#))

最新問題: 7

構成テンプレートにバインドされている MX ネットワークに構成変更が行われるとどうなりますか？

- A. バインドされたネットワークの構成変更は、テンプレート内のテンプレート構成と結合されます。
- B. より制限的な構成が優先されます。
- C. バインドされたネットワークの構成変更により、テンプレート構成がオーバーライドされます。
- D. テンプレート設定は、バインドされたネットワーク内の設定変更をオーバーライドします。

Answer: (解答を表示する)

参照 :

構成テンプレートを使用した複数のネットワークの管理

最新問題: 8

ピアが Auto VPN が使用するポートと対話する 2 つの方法は何ですか? (2つお選びください。)

- A. IPsec トンネリングの場合、ピアは 32768 ~ 61000 の範囲内の上位 UDP ポートを使用します。
- B. ピアは UDP ポート 9350 で VPN レジストリに接続します。
- C. IPsec トンネリングの場合、ピアは 32768 ~ 61000 の範囲内の上位 TCP ポートを使用します。
- D. ピアは TCP ポート 9350 で VPN レジストリに接続します。
- E. IPsec トンネリングの場合、ピアは UDP ポート 500 および 4500 を使用します。

Answer: B,C ([メッセージを残す](#))

参照 :

[_構成と_トラブルシューティング](#)

最新問題: 9

新しいアプリケーションはすべての iOS デバイスにプッシュする必要があります。一部のデバイスでは、イベント ログに NotNow」が報告され、アプリケーションがインストールされません。

NotNow」イベントは何を示していますか?

- A. アプリケーションには最新の iOS バージョンが必要です。
- B. デバイスはパスコードでロックされています。
- C. デバイスは Apple サーバーに接続できません。
- D. デバイスは Cisco Meraki サーバーに接続できません。

Answer: ([解答を表示する](#))

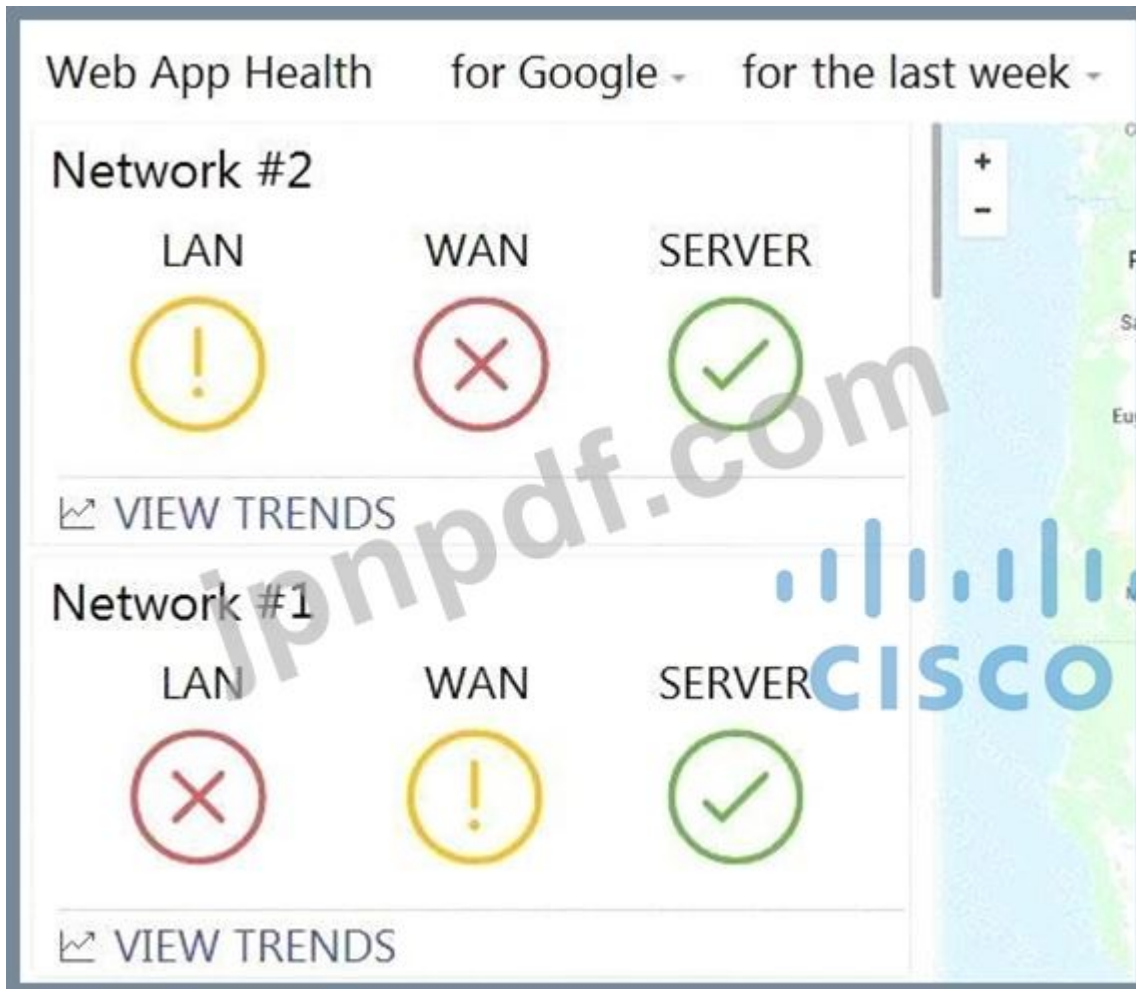
説明

デバイスがパスコードでロックされているためにアクションを実行できない場合、iOS デバイスの詳細ページのイベント ログにエラー メッセージ NotNow」が表示されます。これらのアクションには、管理対象アプリのプッシュ、プロファイルのインストール、その他のアクションが含まれます。この問題が発生すると、デバイスはロックが解除されるとすぐに、アクションを再試行するために MDM サーバーへの再接続を試みます。

https://documentation.meraki.com/SM/Monitoring_and_Reporting/Status_of_%22NotNow%22_in_Systems_Ma

最新問題: 10

展示を参照してください。



Web App Health アプリケーションに反映される 2 つの結果は何ですか? (2つお選びください。)

- A. ローカルクライアントの構成ミスのため、ネットワーク #2 は Google を読み込むことができませんでした。
- B. ネットワーク #2 はネットワーク #1 よりもアプリケーションのパフォーマンスが優れていました。
- C. 両方のネットワーク上のユーザーが Google にアクセスしようとする可能性があります。
- D. どちらのネットワークもサーバー側のパフォーマンスの問題を記録しませんでした。
- E. リモートサーバーの問題のため、ネットワーク #1 は Google をロードできませんでした。

Answer: C,D (メッセージを残す)

最新問題: 11

Apple Mac および Windows PC でのみ使用でき、iOS または Android モバイル デバイスでは使用できない 2 つの Systems Manager Live ツールはどれですか? (2つお選びください。)

- A. OS アップデート
- B. 通知を送信する
- C. 選択的ワイプ
- D. スクリーンショット
- E. リモート デスクトップ

Answer: D,E (メッセージを残す)

説明

https://documentation.meraki.com/SM/Monitoring_and_Reporting/MDM_Commands_in_Systems_Manager_Live_Tools の選択的ワイピングは MacOS のみに適用されます。ここにはWindowsラップトップもあります

最新問題: 12



展示を参照してください。WAN 2 と比較して、WAN 1 経由でルーティングされるインターネット宛のフローの比率はどれくらいですか？

- A. すべてのフローが 5:1 の比率で交互に行われます。
- B. すべてのフローが 2:1 の比率で交互に行われます。
- C. すべてのフローは WAN 1:1 の比率を介して一致します。
- D. すべてのフローは WAN1 経由で出力されます。

Answer: ([解答を表示する](#))

説明

https://documentation.meraki.com/MX/Firewall_and_Traffic_Shaping/MX_Load_Balancing_and_Flow_Prefere

最新問題: 13

Cisco Meraki AP に Fast Lane を実装するにはどの要件が必要ですか？

- A. Apple iOS デバイスにインストールされているワイヤレス プロファイル
- B. Cisco iOS アクセス ポイントにインストールされているワイヤレス プロファイル
- C. アダプティブ 802.11r が無効になっています
- D. DSCP 値 46 のトラフィックを Apple.com にタグ付けするトラフィック シェーピング ルール

Answer: A ([メッセージを残す](#))

参照 :

無線 QoS および高速レーン

最新問題: 14

左側の設定を、右側の Cisco Meraki MR アクセス ポイントにグループ ポリシーを適用する利用可能な方法または利用できない方法にドラッグ アンド ドロップします。

The screenshot shows a configuration interface with two columns. The left column contains six light blue boxes with the following text from top to bottom: "By Sentry Policy", "By Radius Attribute", "By VLAN", "By Device Type", "By Active Directory Group", and "By Client". The right column is divided into two yellow boxes. The top box is titled "Available Options" and contains four empty rectangular slots. The bottom box is titled "Non-Available Options" and contains two empty rectangular slots. A large "CISCO" watermark is visible across the center of the image.

Answer:

The screenshot shows the same configuration interface as above, but with the correct assignments. The left column boxes are now outlined with a dashed green border. The "Available Options" box contains four light blue boxes with the text: "By Sentry Policy", "By Radius Attribute", "By Device Type", and "By Client". The "Non-Available Options" box contains two light blue boxes with the text: "By VLAN" and "By Active Directory Group". A large "CISCO" watermark is visible across the center of the image.

説明

コンピュータ画面のスクリーンショット 自動生成された説明



jnpdf.com

Available Options

- By Sentry Policy
- By Radius Attribute
- By Device Type
- By Client

Non-Available Options

- By VLAN
- By Active Directory Group

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

最新問題: 15

展示を参照してください。

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

送信元 IP 10.168.70.3、宛先 IP 10.116.32.4 のパケットが VPN コンセントレータに到着します。このコンセントレータ ルーティング テーブルに基づくパケットのネクスト ホップは何ですか？

- A. コンセントレータ ゲートウェイ (10.128.124.62) がネクスト ホップです。
- B. 次のホップを決定するのに十分な詳細がありません。
- C. パケットは停止されています。
- D. Auto VPN ピア 「ストア 1532 - アプライアンス」はネクスト ホップです。

Answer: D (メッセージを残す)

説明

これは、コンセントレータのルーティング テーブルを調べ、宛先 IP のエントリを見つけることで判断できます。

10.116.32.4。このエントリのネクスト ホップは、「自動 VPN ピア 「ストア 1532 - アプライアンス」」です。

この質問は、エンジニアリング Cisco Meraki Solutions (ECMS) 公式トレーニング ドキュメントのダイナミックルーティング プロトコルの実装のトピックに関連しています。このトピックの詳細については、「ECMS v2.2 コースの概要」または「ECMS1 v2.1 コースの概要」を参照してください。

最新問題: 16

展示を参照してください。

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

Use the uplink that's best for VoIP traffic.

Prefer WAN 2. Fail over if poor performance for "Conf"

[Add a preference](#)

Traffic filters

All VoIP & video conferencing

WebEx

Actions

+ ×

+ ×

Custom performance

Name	Maximum latency (ms)	Maximum jitter (ms)	Maximum loss (%)	Actions
------	----------------------	---------------------	------------------	---------

Conf	200	50	5	×
------	-----	----	---	---

[Create a new custom performance class](#)

この MX が VPN ピアとの完全なトンネルを確立していると仮定すると、MX は WebEx トラフィックをどのようにルーティングしますか？

- A. WebEx トラフィックは、両方のアクティブな WAN リンク間で負荷分散されます。
- B. WebEx トラフィックは、「Conf」パフォーマンス クラスのしきい値を満たしている限り、WAN 2 を優先します。
- C. WebEx トラフィックは、プライマリ アップリンクである WAN 1 を優先します。
- D. WebEx トラフィックは、稼働している限り WAN 2 を優先します。

Answer: C ([メッセージを残す](#))

有効な 500-220 問題集は GoShiken.com が提供された合格しやすい 500-220 試験問題集！ GoShiken.com が最新の 500-220 試験問題集を提供しています。GoShiken.com 500-220 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 500-220 問題集をゲットする人はこちら：

<https://www.goshiken.com/Cisco/500-220-mondaishu.html> (7430%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 17

展示を参照してください。

The screenshot shows the 'Uplink selection' configuration page. Under 'Global preferences', 'Primary uplink' is set to 'WAN 1'. 'Load balancing' is set to 'Enabled', with a note that management traffic to the Meraki cloud will use the primary uplink. 'Active-Active AutoVPN' is also set to 'Enabled', with a note that VPN tunnels will be created over all available uplinks. Under 'Flow preferences', 'Internet traffic' and 'VPN traffic' both have no uplink preferences configured. At the bottom, there is a table for 'Custom performance classes' with one entry for 'VoIP'.

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

MX セキュリティ アプライアンスは、VPN トラフィックが VoIP カスタム パフォーマンス クラスで設定された遅延しきい値を超えているかどうかを判断するために何を送信しますか？

- A. プライマリ WAN リンク上に確立された VPN トンネルを通じて、毎秒 1000 バイトの TCP プローブが行われます。
- B. すべての WAN リンク上に確立された VPN トンネルを介して、毎秒 100 バイトの UDP プローブが行われます。
- C. プライマリ WAN リンク上に確立された VPN トンネルを介して、毎秒 100 バイトの UDP プローブを実行します。

D. すべての WAN リンク上に確立された VPN トンネルを通じて、毎秒 1000 バイトの TCP プロブが行われます。

Answer: B (メッセージを残す)

説明

パフォーマンス プロブは、確立されたすべての VPN トンネルを介して 1 秒ごとに送信される UDP データの小さなペイロード (約 100 バイト) です。MX アプライアンスは、成功した応答の割合と、応答を受信するまでの経過時間を追跡します。このデータにより、MX は各 VPN トンネル上のパケット損失、遅延、ジッターを判断し、パフォーマンスに基づいて必要な決定を下すことができます。

https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best

最新問題: 18

Cisco Meraki MV カメラはオフィスを監視しており、その視野には現在、ワークデスクと従業員のコンピュータ画面がキャプチャされています。ただし、従業員のコンピュータ画面を録画することは地域の規制により禁止されています。

ダッシュボードのどの機能を使用すれば、規制要件を満たしながらカメラの現在位置を保存できますか？

- A. 制限モード
- B. エリアまたは興味
- C. センサークロップ
- D. ゾーンの除外
- E. プライバシー ウィンドウ

Answer: A (メッセージを残す)

最新問題: 19

左側の設定を右側のボックスにドラッグアンドドロップし、Cisco Meraki MS スイッチのクローン作成機能を使用して設定を複製するかどうかを指定します。

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

Answer:

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

説明

Cisco Meraki MS スイッチの複製機能を使用して複製される設定は次のとおりです。

ポート名

インターフェースの種類

STPブリッジのプロパティ

Cisco Meraki MS スイッチのクローン作成機能を使用してクローンが作成されない設定は次のとおりです。

スイッチ管理IP

スイッチ名

最新問題: 20

App Store にある Systems Manager を通じてプロビジョニングされた iOS アプリの自動更新が必要な場合、どの構成手順が必要ですか？

- A. 構成手順は必要ありません。自動更新はデフォルトの動作です。
- B. Meraki インストール済みプロファイルで iOS デバイスの自動更新を設定します。
- C. 自動更新を有効にするセキュリティ ポリシーを作成します。
- D. 自動更新を有効にしてプロファイルを作成し、iOS デバイ스에適用します。

Answer: (解答を表示する)

説明

デフォルトでは、設定で自動更新がオンになっている場合、App Store にあるシステム マネージャーを通じてプロビジョニングされた iOS アプリは自動更新されます。カスタム iOS アプリの場合、または更新を手動でプッシュダウンするには、次の手順を確認してください。

https://documentation.meraki.com/SM/Apps_and_Software/Updating_Managed_iOS_Apps

最新問題: 21

展示を参照してください。

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

損失と平均レイテンシの統計は何に基づいていますか？

- A. [セキュリティと SD-WAN > SD-WAN とトラフィック シェーピング] ページで構成された接続テスト IP アドレスで MX アプライアンスが受信する応答
- B. [インサイト] > [Web アプリの健全性] ページの接続テスト ホスト名で MX アプライアンスが受信する応答
- C. [ヘルプ] > [ファイアウォール情報] ページの接続テスト IP アドレスで MX アプライアンスが受信する応答
- D. [セキュリティと SD-WAN > ファイアウォール] ページの接続テスト IP アドレスで MX アプライアンスが受信する応答

Answer: D (メッセージを残す)

最新問題: 22

MX アプライアンスをパススルー モードで使用する場合にサポートされる 2 つの機能はどれですか？ (2つお選びください。)

- A. 侵入防止
- B. サイト間 VPN
- C. セカンダリ アップリンク
- D. DHCP

E. 高可用性

Answer: A,B ([メッセージを残す](#))

説明

これらは、MX アプライアンスをパススルー モードで使用する場合にサポートされる 2 つの機能です。
[MX アドレッシングと VLAN] の記事によると、パススルー モードを使用すると、MX アプライアンスがレイヤー 2 ブリッジとして機能し、ルーティングやアドレス変換を実行せずに LAN ポートと WAN ポートの間でトラフィックを渡すことができます。ただし、侵入防止やサイト間 VPN などの一部の機能は、このモードでも引き続き使用できます。

最新問題: 23

[展示を参照してください。](#)

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

このダッシュボード組織は、共同終了ライセンス モデルを使用します。
ライセンスを追加せずに、このネットワーク上でさらに 7 つの AP を要求するとどうなりますか？

- A. 1 つの AP がただちに機能を停止します。
- B. すべての AP が直ちに機能を停止します。
- C. すべてのネットワーク デバイスは 30 日後に機能を停止します。
- D. すべての AP は 30 日後に機能を停止します。

Answer: ([解答を表示する](#))

最新問題: 24

Cisco Meraki デバイスの高可用性はどのようにサポートされていますか？

- A. VRRP を使用する MX セキュリティ アプライアンスのみが高可用性をサポートします。
- B. MX セキュリティ アプライアンスにはアクティブ/アクティブ高可用性ペアが推奨されます。

C. VRRP を使用する MX セキュリティ アプライアンスおよび MS シリーズ スイッチは、アクティブ/パッシブ 高可用性ペアをサポートします。

D. HSRP を使用する MX セキュリティ アプライアンスおよび MS シリーズ スイッチは、アクティブ/パッシブ の高可用性ペアをサポートします。

Answer: A (メッセージを残す)

参照 :

高可用性 ペア

最新問題: 25

左側の説明を右側の対応する MX 動作モードにドラッグ アンド ドロップします。

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

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

This mode is the default mode of operation

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

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

DHCP services can be configured on the MX appliance

Passthrough mode

The MX appliance acts as a layer 2 bridge

VLANs cannot be configured

No address translation is provided

This mode is not recommended at the network perimeter

CISCO

説明

ルーテッドモード:

このモードはデフォルトの動作モードです

このモードは通常、LAN 上のデバイスのデフォルト ゲートウェイでもあります。

インターネットへのクライアント トラフィックでは、アプライアンスの WAN IP に一致するようにソース IP が書き換えられます。DHCP サービスは、MX アプライアンスのパススルー モードで設定できます。

MX アプライアンスはレイヤー 2 ブリッジとして機能します。

VLANは設定できません

アドレス変換は提供されません

このモードはネットワーク境界では推奨されません

この質問は、Cisco Meraki ドキュメントの MX アドレッシングと VLAN のトピックに関連しています。このトピックの詳細については、「MX アドレッシングと VLAN」の記事または「一般的な MX ベスト プラクティス」ページを参照してください。

最新問題: 26

Cisco Meraki API で使用できるリクエストの 3 つの動詞はどれですか? 3つお選びください。)

- A. 設定
- B. 置く
- C. パッチ
- D. 追加

E. POST

F. 取得

Answer: B,E,F (メッセージを残す)

説明

API の動詞は、通常の REST 規則に従います。

GET は、識別子が指定されているかどうかに応じて、リソースの値またはリソースのリストを返します。

POST は新しいリソースを追加します

PUT はリソースを更新します

DELETE はリソースを削除します

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

最新問題: 27

展示を参照してください。



どの設計推奨事項を考慮する必要がありますか？

A. ホップごとに 50% のスループット損失が発生します。Cisco Meraki のベスト プラクティスでは、最大 2 ホップが推奨されています。

B. ホップごとに 50% のスループット損失が発生します。Cisco Meraki のベスト プラクティスでは、最大 1 ホップが推奨されています。

C. ホップごとに 25% のスループット損失が発生します。Cisco Meraki のベスト プラクティスでは、最大 1 ホップが推奨されています。

D. ホップごとに 25% のスループット損失が発生します。Cisco Meraki のベスト プラクティスでは、最大 2 ホップが推奨されています。

Answer: C (メッセージを残す)

最新問題: 28

会社の iPad は監視なしで Systems Manager に登録され、プロファイルは Systems Manager を通じてプッシュされます。

ユーザーが iPad で「Meraki Management」プロファイルを削除しようとする、どのような結果が発生しますか？

- A. Meraki Management」プロファイルが削除されます。Systems Manager がプッシュしたすべてのプロファイルも削除されます。
- B. Meraki Management」プロファイルが削除されます。Systems Manager がプッシュしたすべてのプロファイルが残ります。
- C. Meraki Management」プロファイルは削除できません。
- D. Meraki Management」プロファイルは削除され、Systems Manager によって自動的にプッシュされます。

Answer: ([解答を表示する](#))

最新問題: 29

クラウド接続が一時的に失われた場合、Meraki デバイスはどのように動作しますか？

- A. オフライン デバイスは、クラウド接続が復元されるまで、最後に知られた構成で動作し続けます。
- B. オフライン デバイスはローカル バックアップ サーバーとの接続を確立しようとします。
- C. オフライン デバイスは、接続が復元されるまで 5 分ごとに再起動します。
- D. オフライン デバイスはトラフィックの通過を停止します。

Answer: B ([メッセージを残す](#))

最新問題: 30

Cisco Meraki API で使用できるリクエストの 3 つの動詞はどれですか？ (3つお選びください。)

- A. 設定
- B. 置く
- C. パッチ
- D. 追加
- E. POST
- F. 取得

Answer: ([解答を表示する](#))

参照 :

Cisco_Meraki_Dashboard_API

最新問題: 31

Cisco Meraki MV スマート カメラのビデオ保存期間を延長できる 2 つのアクションはどれですか？ (2つお選びください。)

- A. オーディオ圧縮を有効にする
- B. SSD メモリ拡張機能のインストール
- C. モーションベースの保持を有効にする
- D. 最大保持制限を有効にする
- E. 録画スケジュールの構成

Answer: C,E ([メッセージを残す](#))

説明

https://documentation.meraki.com/MV/Advanced_Configuration/Scheduled_Recording デフォルトでは、Meraki セキュリティ カメラは 24 時間 365 日継続的に録画します。状況によっては、一日の特定の時間帯を記録する

ことが許可されない場合があります。スケジュールされた録画は、この要件を満たし、カメラのビデオ保持機能を向上させます。

有効な **500-220** 問題集は GoShiken.com が提供された合格しやすい 500-220 試験問題集！ GoShiken.com が最新の **500-220** 試験問題集を提供しています。GoShiken.com 500-220 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 500-220 問題集をゲットする人はこちら：
<https://www.goshiken.com/Cisco/500-220-mondaishu.html> (**7430%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 32

MX Live ツールを使用する場合、サイト間 VPN 経由で ping を送信するためにどの VLAN が使用されますか？

- A. VPN を使用するために構成され、NO に設定されている最大の VLAN ID
- B. VPN を使用するために構成され、YES に設定されている最小の VLAN ID
- C. VPN を使用するために構成され、YES に設定されている最大の VLAN ID
- D. VPN を使用するために構成され、NO に設定された最小の VLAN ID

Answer: C (メッセージを残す)

説明

動作 - ファームウェア MX 15.11 以前」セクションを参照してください。ファームウェア MX15.11 以下を実行している MX の場合、MX が宛先に ping を送信するときに使用する送信元 IP は、最も高い VLAN ID の MX IP です。宛先が VPN を介している場合、MX は VPN に参加している最大の VLAN ID の MX IP を使用します。ファームウェア MX 15.12+ を実行している MX の場合、追加の ping オプションがライブ ツールに追加されました。ping ツールには、MX から宛先に ping を送信するための送信元 IP アドレスを選択するためのドロップダウンが追加されました。

https://documentation.meraki.com/General_Administration/Tools_and_Troubleshooting/Using_the_Ping_Live_T

最新問題: 33

展示を参照してください。

SD-WAN & traffic shaping

Uplink configuration

WAN 1 4 Gbps [details](#)

WAN 2 4 Gbps [details](#)

Cellular Unlimited [details](#)

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

[Add a destination](#)

List update interval

WAN 1 Hourly ▾

WAN 2 Hourly ▾ [simple](#)

Cellular Hourly ▾

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](#)

リンク間の比率を 4:1 にして非対称にロード バランシングを最適化するために必要な 2 つのアクションはどれですか？

(2つお選びください。)

- A. プライマリ アップリンクを「なし」に変更します。
- B. 負荷分散比を 4:1 として定義するインターネット トラフィック設定を追加します。
- C. 負荷分散を有効にします。
- D. 携帯電話のアップリンクの速度をゼロに設定します。
- E. WAN 1 と WAN 2 の割り当て速度を 4:1 になるように変更します。

Answer: C,E (メッセージを残す)

説明

明確にするために、リンク間の比率を 4:1 にして非対称にロード バランシングを最適化するには、次の 2 つのアクションが必要です。

負荷分散を有効にする: このオプションを使用すると、MX が負荷分散に両方のアップリンクを使用できるようになります。[セキュリティと SD-WAN] > [設定] > [SD-WAN とトラフィック シェーピング] でロード バラン

シングが有効になっている場合、トラフィック フローは、アップリンク設定で指定された WAN 1 および WAN 2 の帯域幅に比例して 2 つのアップリンク間で分散されます¹。

比率が 4:1 になるように、WAN 1 と WAN 2 の割り当て速度を変更します。WAN リンクの割り当て速度は、そのリンクで利用可能な帯域幅を示す値です。WAN 1 と WAN 2 に割り当てられた速度を変更して、目的のロード バランシング率を反映することで、管理者は MX が両方のリンクを効率的かつ比例的に使用できるようにすることができます¹。たとえば、WAN 1 の帯域幅が 100 Mbps、WAN 2 の帯域幅が 25 Mbps の場合、割り当てられた速度を次のように設定します。

100 Mbps と 25 Mbps では、それぞれ 4:1 の負荷分散比が達成されます。

最新問題: 34

管理プロファイルをターゲットにして System Manager クライアントに適用する 2 つの方法は何ですか? (2つ お選びください。)

- A. Wi-Fi タグを使用する
- B. スコープを定義することにより
- C. シリアル番号の範囲を定義することによって
- D. デバイスタグを使用する
- E. 動的 IP タグを使用する

Answer: ([解答を表示する](#))

説明

正解は B と D です。[System Manager: Getting Started] の記事によれば、これらは、System Manager クライアントを対象にして管理プロファイルを適用する 2 つの方法です。記事では次のように説明されています。

スコープの定義: この方法では、ネットワーク、タグ、または所有者に基づいてデバイスをターゲットにすることができます。プロファイルの範囲は、[システム マネージャー] > [管理] > [設定] ページ、または [システム マネージャー] > [モニター] > [概要] ページから定義できます。

デバイス タグの使用: この方法では、OS、モデル、場所、ユーザーなどの属性に基づいてデバイスをターゲットにすることができます。デバイス タグを使用すると、共通の特性を共有するデバイスの動的なグループを作成できます。デバイス タグは、[システム マネージャ] > [モニタ] > [デバイス] ページ、または [システム マネージャ] > [管理] > [タグ] ページから適用できます。

最新問題: 35

展示を参照してください。

The screenshot shows the Cisco Security Center interface. At the top, it says 'Security Center the last 2 weeks' and '159 matching events'. Below this is a table of events with columns for Time, Type, Source, Destination, Disposition, Action, and Details. The events listed are all 'IDS Alert' type, occurring on May 30 at 21:22:50, 21:22:46, 21:22:46, and 21:22:46. The source is 'Desktop' and the destination is 'a104-96-113-137 deploy.static.akamaitech nologies.com'. The disposition is 'Blocked' and the action is 'MALWARE-CNC'. The details for the first event are 'Win.Trojan.Cridex variant outbound connection'. A detailed view of the first event is shown on the right, including the Rule ID (1-31772), Whitelist status (On/Off), Links (www.vinustotal.com), and Actions (Rule details, Inspect picklist, Show this signature only).

MX セキュリティ アプライアンスはどの IDS/IPS モードに設定されていますか?

- A. 隔離
- B. 予防
- C. 検出
- D. ブロック

Answer: B (メッセージを残す)

説明

侵入防御を有効にするには、[セキュリティと SD-WAN] で [モード] ドロップダウンを [防御] に設定します。
> [設定] > [脅威からの保護] > [侵入の検出と防御]。上記で指定された検出ルールセットに基づいてトラフィックが悪意のあるものとして検出された場合、トラフィックはベスト エフォートによって自動的にブロックされます。

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

最新問題: 36

左側の設定を、右側の OS システムまたはそれをサポートするシステムにドラッグ アンド ドロップします。設定は複数回使用できます。

The interface shows a list of settings on the left and two target OS systems on the right. The settings are: Kiosk mode, Backpack, Single App mode, Wallpaper, Cisco Security Connector, and Active Sync. The OS systems are IOS and Android. Each OS system has three empty slots for dropping the settings.

Answer:



説明

iOS:

キオスクモード

シングルアプリモード

壁紙

シスコ セキュリティ コネクタ

アクティブシンク

アンドロイド:

キオスクモード

バックパック

壁紙

アクティブシンク

この質問は、Cisco Meraki ドキュメントのトピックに関連しています。

このトピックの詳細については、[System Manager: Getting Started] の記事または [システムマネージャー概要] ページ。

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

最新問題: 37

企業所有の iOS デバイスを展開する際のベスト プラクティスの Systems Manager 登録方法は何ですか？

A. マニュアル

B. Apple コンフィギュレータ

C. セントリーの登録

D. DEP

Answer: D (メッセージを残す)

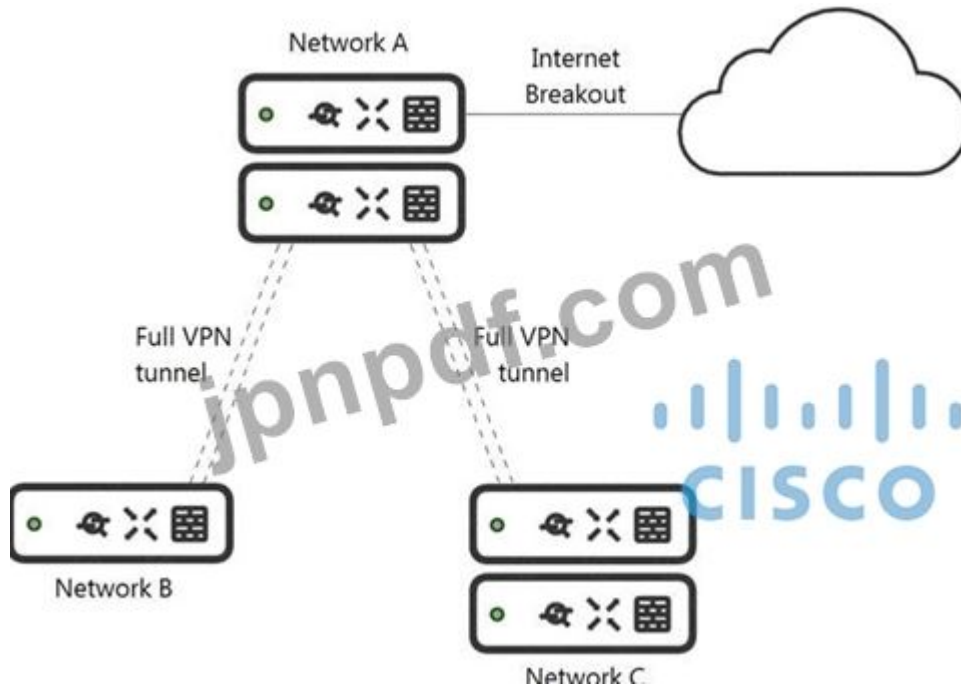
説明

Apple の Device Enrollment Program (DEP) を使用している iOS デバイスは、出荷時設定にリセットしていつでも無線で監視および登録できます。DEP は、デバイスを組織が永久に所有および管理するように強制する最良の方法であり、展開前に DEP 設定を適切に割り当てることです。

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

最新問題: 38

展示を参照してください。



Cisco Meraki Insight の最小ライセンス要件は何ですか？

- A. ネットワーク B で Web App Health を可視化するには、ネットワーク A で単一の Meraki Insight ライセンスを設定する必要があります。
- B. ネットワーク B で Web App Health を可視化するには、ネットワーク B で単一の Meraki Insight ライセンスを設定する必要があります。
- C. ネットワーク B で Web App Health を可視化するには、単一の Meraki Insight ライセンスをネットワーク A で構成し、単一のライセンスをネットワーク B で構成する必要があります。
- D. ネットワーク B で Web App Health を可視化するには、ネットワーク A で 2 つの Meraki Insight ライセンスを構成する必要があります。
- E. ネットワーク B で Web App Health を可視化するには、ネットワーク A で 2 つの Meraki Insight ライセンスを設定し、ネットワーク B で 1 つのライセンスを設定する必要があります。

Answer: B (メッセージを残す)

説明

スポーク サイトクライアントからのトラフィック統計のみが必要な場合は、ハブ サイトがリモート サイトのデータを収集しないため、スポーク ネットワーク上の分析情報を有効にするだけで済みます。

<https://community.meraki.com/t5/Wireless-LAN/Meraki-Insight-Licensing/mp/152684> ライセンスは、Meraki Insight 機能が必要なネットワークにのみ必要です。ネットワークに単一の MX ペアがあるか HA ペアがあるかに関係なく、ネットワークごとに 1 つのライセンスが必要です。ライセンスはネットワーク間で移動できますが、古いネットワークの履歴データは失われます。

https://meraki.cisco.com/lib/pdf/meraki_datasheet_mi.pdf

最新問題: 39

会社の iPad は監視なしで Systems Manager に登録され、プロファイルは Systems Manager を通じてプッシュされます。

ユーザーが iPad で「Meraki Management」プロファイルを削除しようとする、どのような結果が発生しますか？

- A. Meraki Management」プロファイルは削除できません。
- B. Meraki Management」プロファイルは削除され、Systems Manager によって自動的にプッシュされます。
- C. Meraki Management」プロファイルが削除されます。Systems Manager がプッシュしたすべてのプロファイルも削除されます。
- D. Meraki Management」プロファイルが削除されます。Systems Manager がプッシュしたすべてのプロファイルが残ります。

Answer: ([解答を表示する](#))

説明

デバイス上で、[設定] > [一般] > [デバイス管理] に移動します。

[Meraki Management] を選択し、[削除] を選択して管理プロファイルと SM 経由でインストールされた管理対象構成プロファイルを削除します。

最新問題: 40

Cisco Meraki MX セキュリティ アプライアンスの WAN 接続が混雑しており、MX アプライアンスは LAN ポートから WAN ポートに向かうトラフィックをバッファリングしています。高優先度、通常優先度、および低優先度のキュー バッファがすべていっぱいです。他のキューと比較して、通常のトラフィックのどの割合が転送されますか？

- A. 4/10 パケット
- B. 2/7 パケット
- C. 2/10 パケット
- D. 5/15 パケット

Answer: B ([メッセージを残す](#))

説明

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

最新問題: 41

左側の説明を右側の権限タイプにドラッグ アンド ドロップします。

An administrator can access most aspects of a network but no changes can be made.



An administrator can only view a subset of the Monitor section in Dashboard and no changes can be made.



An administrator has access to view all aspects of a network and can make any changes to it.



An administrator can only view the list of Meraki authentication users, add users, update existing users, and authorize/deauthorize users on an SSID or client VPN.



Answer:

An administrator can access most aspects of a network but no changes can be made.

An administrator has access to view all aspects of a network and can make any changes to it.

An administrator can only view a subset of the Monitor section in Dashboard and no changes can be made.

An administrator can only view the list of Meraki authentication users, add users, update existing users, and authorize/deauthorize users on an SSID or client VPN.

An administrator has access to view all aspects of a network and can make any changes to it.



An administrator can only view the list of Meraki authentication users, add users, update existing users, and authorize/deauthorize users on an SSID or client VPN.

An administrator can only view a subset of the Monitor section in Dashboard and no changes can be made.

An administrator has access to view all aspects of a network and can make any changes to it.

An administrator can only view the list of Meraki authentication users, add users, update existing users, and authorize/deauthorize users on an SSID or client VPN.

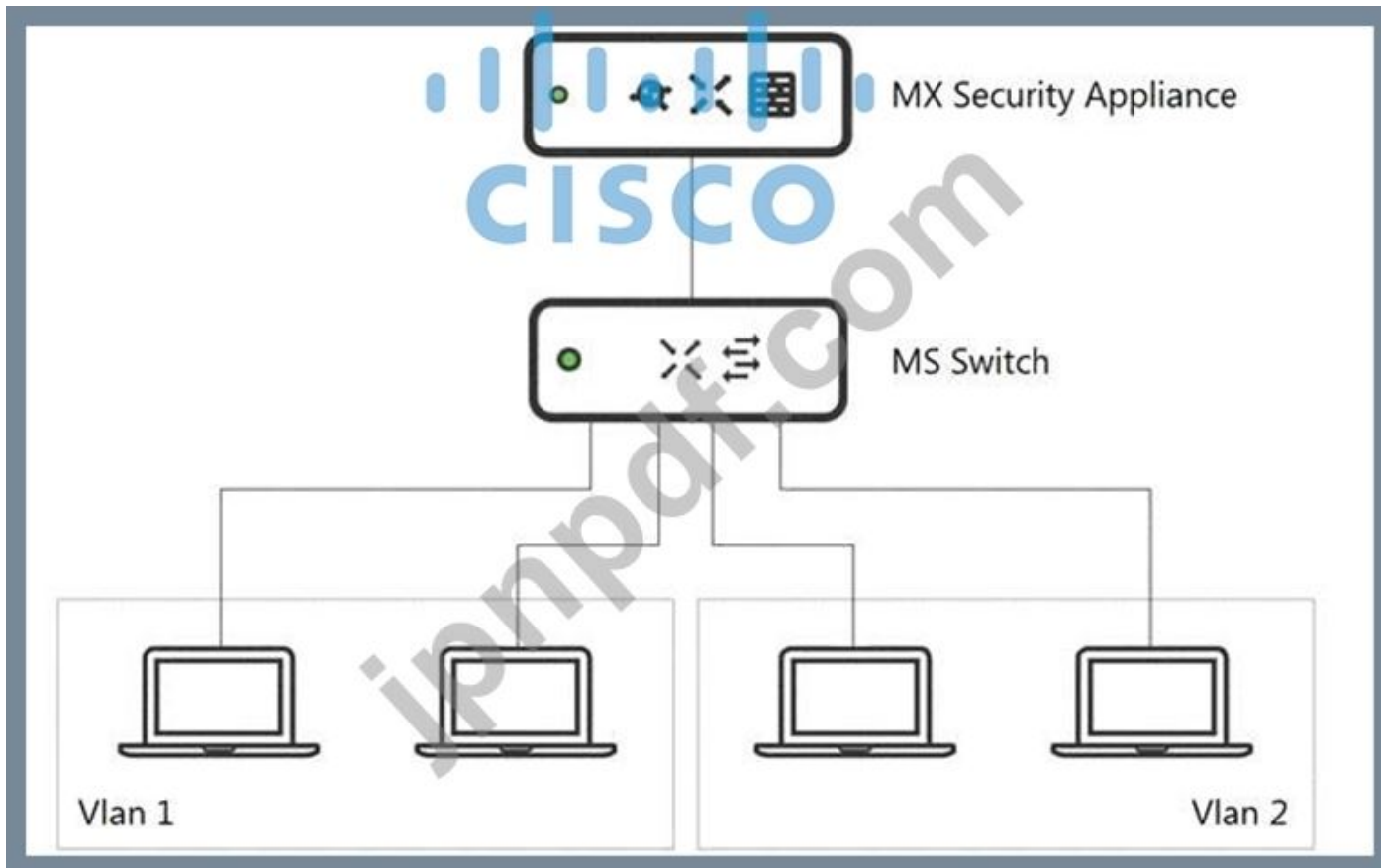
An administrator can access most aspects of a network but no changes can be made.



An administrator can only view a subset of the Monitor section in Dashboard and no changes can be made.

最新問題: 42

展示を参照してください。



MS シリーズ スイッチで VLAN 間ルーティングを実行するのではなく、MX セキュリティ アプライアンスで VLAN 間ルーティングを実装する利点は何ですか？

- A. MX アプライアンスは、VLAN 間のトラフィックに対してコンテンツ フィルタリングを実行します。
- B. MX アプライアンスは、VLAN 間トラフィックのデータ暗号化を実行します。
- C. MX アプライアンスは、VLAN 間トラフィックに対して IDS/IPS を実行します。
- D. MX アプライアンスは VLAN 間トラフィックに対して AMP を実行します。

Answer: B ([メッセージを残す](#))

Valid 500-220 Dumps shared by GoShiken.com for Helping Passing 500-220 Exam! GoShiken.com now offer the **newest 500-220 exam dumps**, the GoShiken.com 500-220 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com 500-220 dumps with Test Engine here: <https://www.goshiken.com/Cisco/500-220-mondaishu.html> (74 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)