cisco Meraki

MX サイジング ガイド

2018 年 9 月

この技術資料では、実際の導入、業界標準のベンチマーク、詳細な機能説明に基づき、適切な Cisco Meraki セキュリティ アプライアンスを選択するためのガイドラインを示します。

概要

Cisco Meraki MX セキュリティ アプライアンスは、統合脅威管理（UTM）製品です。
UTM 製品は、展開が容易な統合フォーム ファクタで複数のセキュリティ機能を提供します。
MX に導入可能なセキュリティ機能は複数あるため、デバイスのパフォーマンスは使用例によって異なります。正しい MX の選択は、使用例と展開の特性によって異なります。

この技術ガイドでは、次のような内容をご説明いたします。

- 必要な MX モデルはどのように決定するのか。
- どの機能を有効にする必要があるのか。
- MX モデルと競合製品にはどのような違いがあるのか。

正しいハードウェアの選択

Cisco Meraki MX 製品では、8 種類の製品ファミリが用意されています。以下の図では、各製品ファミリで利用できる MX ハードウェア特性の概要を示しています。

	MX64（W）	MX65（W）	MX67(W/C)	MX68(W/CW)	MX84	MX100	MX250	MX450
								
デュアル WAN リンク	✓	✓	✓	✓	✓	✓	✓	✓
3G/4G フェールオーバー	✓	✓	✓	✓	✓	✓	✓	✓
利用可能な組み込み LTE モデムのモデル			✓	✓				
利用可能な組み込みワイヤレス	✓	✓	✓	✓				
利用可能な組み込み PoE + モデル		✓		✓				
ハード ドライブ					1 TB	1 TB	128 GB（SSD）	128 GB（SSD）
ファイバ接続					SFP	SFP	SFP、SFP+	SFP、SFP+
デュアル電源							✓	✓
フォーム ファクタ	デスクトップ	デスクトップ	デスクトップ	デスクトップ	1U	1U	1U	1U

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

ネットワークのパフォーマンス ベンチマーク

業界標準のベンチマークは、MX セキュリティ アプライアンスと他のベンダーのファイアウォールを比較するために役立ちます。このテストでは、理想的なトラフィック パターンを持つネットワーク条件を想定しています。特定の機能の最大スループットを測定するときは、他のすべての機能を無効にしています。実稼働ネットワークにおける実際の結果は異なります。

	MX64/65 シリーズ	MX67/68 シリーズ	MX84	MX100	MX250	MX450
すべてのセキュリティ機能を有効にした状態での最大スループット	200 Mbps	300 Mbps	320 Mbps	650 Mbps	2 Gbps	4 Gbps
パススルー モードでのステートフル（L3）ファイアウォールの最大スループット	250 Mbps	450 Mbps	500 Mbps	750 Mbps	4 Gbps	6 Gbps
NAT モードでのステートフル（L3）ファイアウォールの最大スループット	200 Mbps	450 Mbps	500 Mbps	750 Mbps	4 Gbps	6 Gbps
最大 VPN スループット	100 Mbps	200 Mbps	250 Mbps	500 Mbps	1 Gbps	2 Gbps
最大同時 VPN トンネル [1] （サイト間またはクライアント VPN）	50	50	100	250	3,000	5,000
最大同時 VPN トンネル [2] （サイト間またはクライアント VPN）	50	50	100	250	1,000	1,500
最大 AMP スループット	250 Mbps	300 Mbps	500 Mbps	750 Mbps	2 Gbps	4 Gbps
最大 IDS スループット	200 Mbps	300 Mbps	320 Mbps	650 Mbps	2 Gbps	4 Gbps

MX 用の SD-WAN 機能セットには、使用可能なすべてのアップリンクでピア間に VPN トンネルを作成し、使用可能な WAN 帯域幅を最も効率的に使用できるようにするための、アクティブ-アクティブ VPN が含まれています。そのため、2 つのピア間の接続には、各サイトの MX アップリンクの数に応じて、最大 4 つのトンネルが含まれます。VPN のサイジングに関する決定を行うときには、このことを考慮する必要があります。

[1] 最大同時 VPN トンネル数は、VPN トンネル経由のクライアント トラフィック送信がないシナリオでのラボ テスト に基づいています。

[2] 推奨の VPN トンネル数は、VPN トンネル経由のクライアント トラフィック送信がないシナリオでのラボ テスト に基づいています。

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

機能、利点、パフォーマンスへの影響

UTM 製品には、さまざまなセキュリティ機能とネットワーク機能があります。パフォーマンスを不必要に低下させずにセキュリティ上の利点を最大限得るためには、これらの機能の利点とトレードオフを理解することが重要です。

	メリット	パフォーマンスへの影響	推奨事項
マルウェア防御	Cisco AMP クラウドから取得した判定結果に基づいて、HTTP ベースのファイル ダウンロードをブロック	高	ゲスト VLAN を無効にし、ファイアウォール ルールを使用してその VLAN を隔離することを検討してください。ホスト デバイス上で AMP for Endpoints などの完全なマルウェア クライアントを実行する場合は、無効化も検討します。
IDS/IPS	疑わしいネットワーク トラフィックに対するアラートの発行/疑わしいネットワーク トラフィックの阻止	高	低帯域幅ネットワークでは、VPN 経由で IDS/IPS syslog データを送信しないことを検討してください。
VPN	ロケーション間の、安全で暗号化されたトラフィック	中	スプリット トンネル VPN を使用し、エッジにセキュリティ サービスを展開します。
Web キャッシング	ローカル キャッシュによる Web コンテンツへのアクセスの高速化	中	重いマルチメディア コンテンツに頻繁に繰り返しアクセスする低帯域幅ネットワークに適しています。高帯域幅ネットワークには推奨されません。YouTube は Web キャッシングをサポートしていないことに注意してください。
コンテンツ フィルタリング（トップ サイト）	ローカルにダウンロードされたデータベースを使用したカテゴリ ベースの URL フィルタリング	低	範囲よりも速度を優先する場合は、このオプションを選択します。
コンテンツ フィルタリング（フル リスト）	Brightcloud.com でホストされている全データベースを使用したカテゴリ ベースの URL フィルタリング	中	範囲とセキュリティを 100% 優先する場合は、このオプションを選択します。最初は Web ブラウジングが若干遅くなりますが、URL カテゴリがキャッシュされるにつれて改善されます。
Web セーフ サーチ	Google/Bing のセーフ サーチ オプションの有効化	低	有効にするには、「暗号化された検索を無効にする」オプションと並行して導入する必要があります。
暗号化された検索のブロッキング	https（ポート 443）経由の Google または Bing の検索を無効化し、Web セーフ サーチを適用可能にする	低	有効にするには、「Web セーフ サーチ」と並行して導入する必要があります。DNS 設定を変更する必要があります。変更しないと、Google Apps も中断されます。詳細については、Meraki ナレッジ ベースを確認してください。

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

推奨クライアントデバイス数

MX セキュリティ アプライアンスの下に展開できるクライアント デバイス数にハード リミットはありませんが、このドキュメントではすべてのテストを次の表に示すクライアント数で実行しています。このクライアント数を超えると、このガイドに記載されているサイジング データとは異なるパフォーマンスになる場合があります。

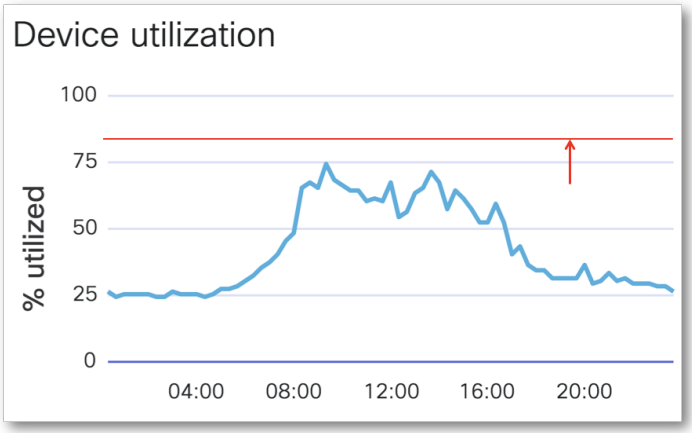
推奨クライアント デバイス数

	MX64/65 シリーズ	MX67/68 シリーズ	MX84	MX100	MX250	MX450
推奨クライアント デバイス数	50	50	200	500	2,000	10,000

ダッシュボードに組み込まれた MX デバイスの使用率レポート

このガイドでは、特定の機能が有効になった特定の MX モデルの予想使用率と負荷レベルに関する情報を、ユーザに伝えることを目的とします。ただし、デバイス上の負荷を正確に予測するには、求める条件の下で、指定された環境でテストする必要があります。使用時の固有のトラフィックの組み合わせや機能など、実際のパフォーマンスに影響する個々のネットワークの変数が数多くあります。

MX デバイスの使用率によって、時間の経過に伴うデバイスの負荷をよりよく把握できます。また、使用率のレベルを評価し、上位デバイスへのアップグレードと負荷の削減のどちらが必要かを決定するためにも使用できます。MX デバイスが通常の動作中*に、使用率が常に 85 % を超えている場合は、スループットが高いモデルへのアップグレードまたはデバイスごとの負荷の削減を考慮すべきです。MX デバイスの使用率のツールは API 経由で利用可能です。また、サマリー レポートのページに表示されるグラフとしても利用できます。



MX デバイスの使用率の計算

Meraki ダッシュボードに報告されたデバイス使用率のデータは、1 分間にわたって測定された負荷の平均に基づいています。負荷の値は 1 から 100 までの数値で返されます。値が低いほど負荷が低いことを示し、値が高いほどワークロードが大きいことを示します。現在、デバイスの使用率の値は、そのトラフィック負荷と同様、MX の CPU 使用率に基づいて算出されています。

負荷を平均化しているため、瞬間的な負荷の急増が発生しても使用率のメトリックに表れない可能性があります。たとえば、85 % 未満で常に表示されるデバイスの負荷には、瞬間的な負荷の急増が発生している可能性があります。こうした瞬間的な負荷の急増によって、デバイスの転送キャパシティを超えて受信したパケットが欠落する可能性があります。

** 必要な機能はすべて有効になっていて、予想された数のクライアントが接続し、予想された組み合わせのトラフィックがデバイスを通過している。*

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

まとめ

各ネットワークには固有のトラフィック パターンがありますが、このガイドでは、ご使用の環境に適した Cisco Meraki MX 製品を選択するために役立つ、いくつかの一般的なシナリオを紹介しています。ファイアウォールの選択時に、将来の成長を考慮して十分に余裕を持った計画を検討してください（現在 550 人のユーザがいる場合は 1000 人のユーザをサポートする MX を選択するなど）。これにより、追加のセキュリティ機能とネットワーク機能が利用可能になったときも、引き続きその機能を活用できます。また、ISP の速度が前年比で増加していることを考慮すると、長期にわたって十分なサービスを提供するファイアウォールを選択することが重要です。

当資料は、米国で発表された英語資料の抄訳です。

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com