ガイドブック

シンプル設計のセキュリティ機能

目次

概要

IT　管理者は、ネットワーキング機器を設置し、常に最新に保つだけでなく、クライアントからアプリケーションまですべてを管理するという難しい仕事を担っています。さらに、セキュリティにも配慮する必要があります。従業員、ゲスト、請負業者などの非常に多くのタイプのユーザと、様々なタイプのデバイス（企業所有のラップトップ、従業員所有のスマートフォン、IoT　デバイス）がネットワークにアクセスしようとするため、IT 管理者は、ネットワーク、デバイス、ユーザアクセス、セキュリティを管理する拡張性に優れた方法を必要としています。

その結果、IT　チームは複数のベンダーを試して異なるダッシュボードを使用し、手動で統合し、ネットワークを保護するために複数の製品を利用することになります。実際に、25 % を超える企業が 1 ～ 20 社のベンダーを利用してネットワークを保護しようとしています。[1] この多数の異なるソリューションにより、セキュリティ環境はシンプルになるどころか複雑化しています。結局のところ、IT　管理者は諦めて基本的なファイアウォールを導入することになります。IT 管理者はネットワークのすべてのレイヤに作用するセキュリティ態勢を実装することの重要性を理解してはいるものの、通常は、これらのソリューションの実装に必要な人手と時間が不足しています。悪意のある攻撃者は、このような脆弱性を利用します。サイバーセキュリティ攻撃の 43% 以上が、IT チームが少人数の SMB [2]を標的とし、これらの攻撃の 74% 以上が、不十分なネットワークアクセスとセキュリティのポリシーを悪用しています。[3]

そこで、Meraki の出番です。単一のダッシュボードにより、ネットワーク全体を管理するだけでなく、高度なセキュリティおよびアクセスポリシーを適用できるようになりました。クラウドベースの Meraki ダッシュボードにより、すべての製品にパッチが適用され、常に最新の状態に保たれます。また、Meraki はオープンなアーキテクチャを採用しているため、拡張可能な API によってシスコのセキュリティポートフォリオとさらに統合できます。

1 シスコ 2018 年次サイバーセキュリティ レポート
2 シスコ 2018 年次サイバーセキュリティ レポート
3 シスコ 2018 年次サイバーセキュリティ レポート

ハードウェアの更新

概要

MS390 は、Cisco UADP 2.0 ASIC の性能と Meraki ダッシュボードのシンプルさを組み合わせて、ネットワーク内の様々なユーザとデバイスをマイクロセグメント化します。この製品を使用することで強力なセキュリティおよびアクセスポリシーを適用できるため、お客様のビジネスをデータ漏洩の危機から守ることができます。モジュラ型アップリンク、電源装置、およびカスタム設計の ASIC を備えた MS390 は、Meraki ポートフォリオにおける最も強力なアクセススイッチであり、IT 管理者は多くの問題を解決できます。

お知らせ

MS390 は Meraki シリーズの中で最も強力なアクセススイッチであり、クラウド管理の IT のシンプルさと、専用設計のシスコ シリコンの性能を兼ね備えています。従来のスイッチング機能に加えて、MS390 では解読が難しい個々の IP アドレスではなく、マイクロセグメント化されたユーザグループに基づいて高度なセキュリティおよびアクセスポリシーを有効にできます。その他の主要な機能は以下のとおりです。

- お客様は、専用設計の UADP 2.0 ASIC を使用して、最も厳格なサービス品質要件を満たすことができます。
- 先行機種（MS350）の 3 倍のスループットを提供し、ホットスワップ可能なモジュラ型アップリンクを搭載した 48 ポートのフル mGig SKU を特徴としています。
- 物理的なスタッキングの改善によって遅延が 1 秒未満に短縮されるため、スイッチに障害が発生した際により高速なスタックコンバージェンスが可能です。これは、エンタープライズ環境では非常に重要です。
- 使用可能なすべての電源装置をプールし、追加の電源の冗長化ソースとする StackPower を搭載しています。

キーポイント

MS390 シリーズのスイッチの UADP 2.0 ASIC により、インテントベースのネットワークをあらゆる場所で簡単に提供できます。お客様はユーザの場所ではなくユーザのタイプに基づいてマイクロセグメント化し、高度なアクセスおよびセキュリティポリシーを適用できます。MS390 の機能が豊富なハードウェアは、これまでになくシンプルな Meraki ダッシュボードによりスタック管理が容易になり、効率的に電力を管理できます。

ソフトウェアおよび機能の更新

適応型ポリシー

概要

企業が成長し、新しいデバイス、ユーザ、アプリケーションが追加されると、ネットワーク内の IP アドレスの収集をやり直すという従来の方法は非常に困難な作業となります。これに加えて、IP アドレスからはユーザ、デバイス、アプリケーションの情報は得られません。適応型ポリシーは、スイッチハードウェアのリソースとキャパシティを消費することなく、各通信回線の使用者、内容、時間を IP アドレスに追加することで、セキュリティを強化することを目的としています。

お知らせ

適応型ポリシーは、ユーザ、デバイス、アプリケーションの目的に基づいて追加のセキュリティレイヤを提供するために構築された、MS390 のソフトウェア機能です。この機能は、クライアント、ユーザアプリケーション、デバイスの目的に基づいて、ビジネス環境に合わせて自動的に調整されるネットワークポリシーを実装します。

キーポイント

適応型ポリシーは、効果的なセキュリティ、運用コストの削減、強力な自動化、可視性の向上、ハードウェアの効率性の向上、ビジネスの生産性の向上を実現することで、今日のネットワークの問題を解決します。

SecureConnect

概要

ネットワーキング ハードウェアは潜在的な脅威に晒されています。SecureConnect は、スイッチポートを保護し、デバイス設定を自動化する最もシンプルで効果的な方法です。わずか数回のクリックでこのレベルのセキュリティを実現できるベンダーは他にありません。

お知らせ

SecureConnect は、MS210 以降のすべての MS モデル、すべての 802.11 ac および 802.11 ax MR モデルで使用できるソフトウェア機能です。SecureConnect は、MS がポートに接続されている MR が同じ組織に属していることを検出して確認できるようにし、接続された MR に設定を自動的にプッシュします。

キーポイント

SecureConnect は、信頼性の高いセキュリティ、拡張可能な自動化、生産性の向上をお客様に提供し、潜在的な設定エラーを排除します。これは Meraki ライセンスモデルの利点であり、お客様にふさわしい未来のソフトウェア機能を提供する Meraki クラウドの性能を証明しています。Meraki は、製品間機能によってセキュリティのニーズに応え続けています。そのため、Meraki に投資したお客様は継続して Meraki の利点を得ることができます。

Trusted Access

概要

誰がどのようなタイプのデバイスで、いつ接続しようとしているのかを把握することは、IT 管理の現実とはかけ離れています。Meraki Trusted Access はユーザとデバイスに対する可視性を提供し、セキュアなネットワークアクセスをシームレスに実現します。

お知らせ

Meraki Trusted Access は、組織が企業資産と個人デバイス間のセキュアなネットワーク接続を確立できるようにするソフトウェア機能です。MDM エージェント/プロファイルのインストールは必要ありません。Trusted Access には MR と SM を有効にする必要があります。iOS、macOS、および Android デバイスで使用できます。

キーポイント

Meraki Trusted Access は、高度なセキュリティと組み合わせた柔軟に認証方式をお客様に提供します。ユーザエクスペリエンスを向上し、ユーザとデバイスを可視化できます。また、デバイスのオンボーディングとセキュリティポリシーの適用を自動化することもできます。さらに、Meraki Trusted Access により、API を使用したカスタム統合が可能になります。

Trustworthy Systems

概要

Cisco Meraki は、Trustworthy Systemsをサポートするハードウェアフルスタック（MR アクセスポイント、MS スイッチ、MX SD WAN セキュリティアプライアンス）によって、市場における差別化要因となっています。

お知らせ

Trustworthy Systems は、ハードウェアプラットフォームで実行されているコードが信頼でき、変更されておらず、意図した通りに動作していることを保証するシスコの一連のソリューションです。イメージ署名、セキュアブース、シスコのトラストアンカーモジュールなどの技術が含まれています。ハードウェアレベルの信頼の基点、一意のデバイス ID、スタートアップ時のすべてのレベルのソフトウェアの検証などの多層的なアプローチは、システムに対する信頼の連鎖を確立します。現在、すべての Cisco Meraki ハードウェア製品が Trustworthy Systems をサポートしています。

キーポイント

シスコの Trustworthy Systems は、偽造製品やサイバー攻撃などの脅威を防ぐために、ハードウェア製品にセキュリティと信頼を確立します。フルスタックの Meraki は、Trustworthy Systems のネットワーク インフラストラクチャによる信頼性の高いエンタープライズ ソリューションです。

Umbrella + MR ライセンス

概要

Cisco Umbrella の DNS セキュリティソリューションの力と Meraki ダッシュボードのシンプルさを組み合わせることで、お客様のネットワークを保護できるようになりました。新しい MR の Advanced および Upgrade ライセンスは、ネットワーク内の DNS レイヤで、Meraki で定義されたポリシーを自動的に有効にします。新しいライセンスにより、お客様は Meraki ダッシュボードから、ブロックされた DNS イベントに対する可視性を得ることができます。IT 管理者は Umbrella と MR アクセスポイントを手動で統合する必要がなくなり、セキュリティ展開を複数のサイトに数分で拡張できるようになりました。

お知らせ

Meraki は、Meraki ダッシュボードのセキュリティセンターを使用してブロックされた DNS イベントの詳細な可視性をお客様に提供する新しいライセンスをリリースします。また、お客様は手動で統合することなく、事前定義されたポリシーを導入できます。Meraki ダッシュボードにセキュリティセンターを追加することで、お客様は DNS レベルでワイヤレスネットワークの監視、保護、トラブルシューティングが可能になります。新しいお客様は、Advanced ライセンス SKU を購入してこれらのジョイント機能にアクセスできます。また、既存のワイヤレスのお客様は Upgrade ライセンス SKU を購入して、Meraki ネットワークで Umbrella による DNS セキュリティを有効にできます。

キーポイント

Umbrella と MR を組み合わせた新しいライセンスは、比類のないシンプルさと一元化を提供します。お客様は、ハードウェアまたは仮想マシンを追加せずに、クラウド経由ですべての Meraki AP に DNS レイヤセキュリティを展開できます。また Meraki は、事前定義されたポリシーを取得して導入し、大部分のインターネットの脅威からユーザを保護するための API エンドポイントを作成しました。IT 管理者は、複数のネットワークで DNS レイヤセキュリティを大規模に展開し、シンプルでセキュアなデジタルワークプレースを構築できるようになりました。

MX と Cisco Defense Orchestrator（CDO）の API 統合

概要

Cisco Defense Orchestrator（CDO）はクラウドベースの管理ソリューションです。シスコのセキュリティ製品全体のセキュリティポリシーと設定を簡単に管理でき、Meraki MX もこれに加わりました。

お知らせ

CDO で Meraki MX がサポートされました。いずれのシスコのセキュリティ製品でも、組織全体でポリシーを整合することで、セキュリティを強化します。これにより、複数のシスコセキュリティ製品にかけたセキュリティポリシーの管理が簡素化され、不整合やギャップが生じなくなります。Meraki MX を含むシスコのセキュリティ製品を組み合わせたお客様は、CDO を使用して、組織内のすべての場所でポリシーの統一、維持、更新を行うことで価値を見出すことができます。

キーポイント

CDO は、ハイブリッドのシスコと Meraki インフラストラクチャ全体のセキュリティ管理を統合する強力なソリューションです。

Identity Pre-Shared Key (iPSK)

概要

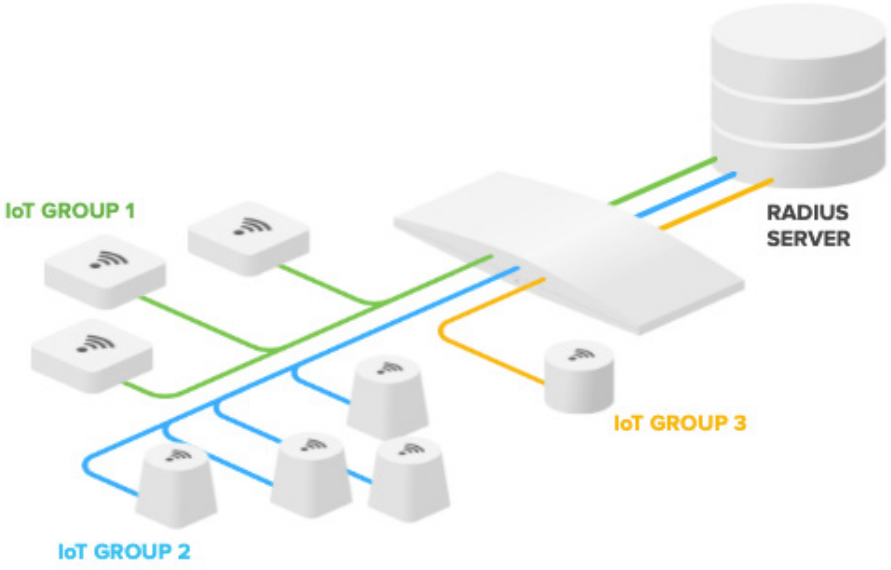
IoTデバイスの増加と共に、ネットワーク管理者はワイヤレスネットワークに接続されるデバイスが指数関数的に増えてきている現状を管理する必要があります。これらのデバイスのすべてが 802.1 X 認証をサポートしているわけではないため、認証は困難になります。
現在は WPA-PSK が使用されていますが、不正なユーザにキーが共有される可能性があります。IPSK (Identity 事前共有キー) により、
ワイヤレスネットワークの保護が大幅に簡素化されます。

お知らせ

iPSK は、ワイヤレスデバイスをより安全に認証する新しい MR 機能です。これは、WPA-PSK などの以前の方法です。これには、802.1X. や追加の認証は必要ありません。各デバイスからSSIDに接続するために必要な単一の共有キーを使う代わりに、デバイスのMACアドレスに紐づいているユニークなPSKがRADIUSサーバーによって認証される仕組みです。この機能は、PSKをベースに 一つのSSIDの中に異なるグループポリシーを割り当てることができます。例えば、PSK “Meraki123”を使用しているデバイスは自動的にグループポリシー1が割り当てられ、 PSK “Meraki456”を使用しているデバイスはグループポリシー2が割り当てられるという具合です。

キーポイント

この機能により、組織は複数の SSID を作成せずにネットワークを保護できます。これにより、ワイヤレスのパフォーマンスが損なわれる可能性があります。デジタル変革を受けている組織にセキュリティを追加します。



ファイアウォール オブジェクト グループ

概要

ファイアウォールオブジェクト グループを使用すると、テレフォニー、プリンタなどのネットワークエンティティを IP アドレスまたはサブネットにマッピングできます。これらのネットワークオブジェクトは、MX のファイアウォールルールを簡素化するためにグループ化できます。

お知らせ

ファイアウォールオブジェクトグループは、複数のファイアウォールルールを作成して管理するプロセスを簡素化する新しい MX 機能です。

キーポイント

これにより、ファイアウォールルールの作成と管理がかつてないほど簡単になりました。この新しい
プロセスにより、MX のパフォーマンスが向上し、その結果、ネットワーク管理の簡素化が向上します。

cisco Meraki