クラウド管理型小売業界のプロファイル

2025 年 12 月 19 日

注： 小売業界（非ファブリック）におけるシスコ検証済みプロファイルについては、「Validated Profile: Retail (Non-Fabric) Vertical」を確認してください。

本書の目的と用途

このドキュメントの対象読者は、クラウド管理型のキャンパスおよびブランチネットワークを設計、展開、および運用するネットワーク設計エンジニアおよびネットワーク運用担当者です。ブランチネットワークは、シスコの一般公開されている規定型の Terraform ベースコードを使用して展開できます。

このガイドでは、企業キャンパスと、企業ネットワーク内の分散小売ストアで構成されるクラウド管理型小売ネットワークを設計および展開する方法に焦点を当てています。Day 0 および Day *n* 運用向けの Cisco Meraki ダッシュボードと Cisco Network as Code（NAC）を使用した展開、およびキャンパスネットワークとストアネットワーク両方の全体的な正常性モニタリングについて説明します。このドキュメントの内容は、同様の設計要件を持つ金融サービスなど、その他の業界のお客様にとっても参考になります。

ソリューションの概要

このドキュメントは、シスコの Cloud Managed Campus and Unified Branch アーキテクチャと、クラウド管理型インフラストラクチャと Branch as Code（BaC）の原則を活用した、包括的なクラウド管理型小売企業ネットワーク展開に関する検証の参考資料としての役割を果たします。

昨今の小売ネットワークには、さまざまな地域に分散した数百もの店舗が含まれ、それぞれに一貫性のある、セキュアで、パフォーマンスの高いネットワーク インフラストラクチャが必要です。小売業では、最高レベルのセキュリティとコンプライアンスを維持しながら、ネットワーク業務を合理化し、運用の複雑さを軽減し、展開タイムラインを短縮できる統合型の管理アプローチが要求されます。各店舗のロケーションには、支払い処理、在庫管理、顧客体験アプリケーション、およびビジネスに不可欠なオペレーションをサポートするための、信頼性の高い接続を備えた自己完結型のネットワークサービスが必要です。異なる管理システムを使用する従来のブランチ ネットワーク アプローチでは、運用上のサイロが生じ、複雑さが増し、ビジネスアジリティが制限されます。

クラウド管理型小売アーキテクチャ

昨今の小売業務では、急速に変化するビジネスニーズに対応できる、アジャイルでセキュアな、スケーラブルなネットワーク インフラストラクチャが要求されます。小売ネットワークに固有の複雑さは、数百または数千のロケーション、多様なデバイスエコシステム、厳密なコンプライアンス要件、顧客対応サービスと多岐にわたり、ネットワーク管理に対して根本的に異なるアプローチを必要とします。

Cisco Meraki のクラウド管理型プラットフォームは、従来は複数サイト展開に関連付けられていた運用の複雑さを解消し、企業レベルのセキュリティ、可視性、およびパフォーマンスを提供することで、小売ネットワークを変革します。このドキュメントでは、今日の小売組織が直面している問題に、Cisco Meraki クラウドファーストのアーキテクチャを使用して対処する方法の概要を説明します。

クラウドネイティブの管理プラットフォーム

集中的なクラウド管理は、自動デバイス検出、クラウドベースのプロビジョニング、およびテンプレート駆動型設定によるゼロタッチ展開を提供し、迅速な店舗オープンと季節ごとのロケーションの展開を可能にします。統合管理インターフェイスは、ロールベースのアクセス制御を使用して本社キャンパス、ディストリビューションセンター、ブランチストアのロケーションを一括で管理できます。自動ライフサイクル管理は、小売ネットワーク全体のファームウェアの更新、セキュリティパッチ、および設定の変更にスケジュール機能を使用して対処します。

AI 駆動のオペレーションでは、Cisco AIOps と包括的なテレメトリデータ、および ThousandEyes の統合を活用して、エンドツーエンドの可視性と実用的なインサイトを提供します。プロアクティブな問題解決では、AI 駆動分析が従来の手動ワークフローでは不可能であった迅速なインシデント解決を実現します。予測分析では、機械学習アルゴリズムを使用して、ビジネスオペレーションが影響を受ける前に、潜在的な問題を特定します。

包括的ネットワーク サービス スタック

統合セキュリティフレームワークは、データ保護と運用の継続性を優先する包括的なアプローチで小売業界固有の要件に対処します。次世代ファイアウォール統合では、ブランチ ルータ プラットフォームに直接組み込まれた侵入防御、マルウェア保護、およびコンテンツフィルタリングを統合した統合脅威管理が提供されます。この統合により、自動化されたネットワーク セグメンテーションと、決済カードのデータ保護専用に設計されたセキュリティポリシーを通じて PCI DSS への準拠が実現します。同時に、すべてのネットワークリソースのアイデンティティベースのアクセス制御と継続的な検証によるゼロトラスト ネットワーク アクセスの原則も導入できます。

高度な脅威からの保護機能は、クラウド提供型脅威インテリジェンスと自動ポリシー更新によるリアルタイムのセキュリティインテリジェンスを提供し、すべての小売店舗で最新の脅威シグニチャをすぐに利用できるように

します。AI アルゴリズムを搭載した動作分析により、異常なネットワーク動作と潜在的なセキュリティ脅威を、運用に影響を及ぼす前に検出します。セキュリティイベントが発生すると、インシデント対応の自動化によって即座に封じ込めと修復機能が提供されます。これによりビジネスの中断が最小限に抑えられ、お客様の信頼が維持されます。

SD-WAN および接続サービス

アプリケーション認識型 Meraki SD-WAN は、アプリケーション要件、リンク品質、およびビジネスポリシーに基づく自動トラフィックステアリングを使用したインテリジェントパス選択を提供します。ダイレクト インターネット アクセスは、クラウドアプリケーションのローカル インターネット ブレークアウトを可能にし、遅延が短縮され、顧客体験が向上します。アプリケーション パフォーマンスの最適化により、POS システムや在庫管理などのビジネスクリティカルな小売アプリケーション向けに、WAN の最適化と Quality of Service の優先順位付けが実現します。

接続のレジリエンスは、プライマリブロードバンドとセルラー LTE または 5G バックアップを組み合わせたマルチパス接続によってビジネスの継続性を確保し、障害時にも POS システムの接続性と店舗運用を維持します。自動フェールオーバー機能により、接続タイプ間のシームレスな移行が実現します。ダイナミックな帯域幅割り当てが、ビジネスの優先順位や時間帯の要件に基づいてトラフィックを管理し、ショッピングのピーク期間中に最適なパフォーマンスを保証します。

小売向けのインテントベース ネットワーク

必要な機能、ネットワークパフォーマンス、セキュリティルール、コンプライアンス要件などの全体的な目標を小売組織が設定すると、Cisco Meraki ダッシュボードは、これらの目標を特定のデバイス設定に自動的に変換し、すべての店舗ロケーションで常に最新の状態に保ちます。各スイッチ、アクセスポイント、およびセキュリティデバイスを個別に設定する代わりに、管理者は、決済トラフィックの分離、POS アプリケーションの優先順位付け、ブランド化されたゲスト Wi-Fi の提供などのビジネスニーズに集中できます。ダッシュボードは、数百または数千のロケーションでこれらの目標が一貫して満たされるように、バックグラウンドでネットワークを管理します。この方法により、個々のデバイスの管理から、ビジネス目標に合致する単一の統合システムとしてすべてのブランチサービスを一括で管理する方法へ移行し、小売業の IT を変革します。

小売業界固有の運用機能

Cisco Meraki ダッシュボードは、ポリシー駆動のネットワークのセグメンテーションとワンクリックの監査レポートによって、PCI DSS 準拠を自動化します。また、専用 POS セグメントが決済時のセキュリティを保証します。自動デバイス検出によるネイティブな IoT のサポートで、インベントリ管理とビジネス インテリジェンス プラットフォームを接続する包括的な API を介した、センサー、ビーコン、スマートシェルブのシームレスな統合が可能になります。MR アクセスポイント（AP）および MV カメラにより、ダッシュボードから直接、お客様の行動分析（ショッピングパターン、トラフィックフロー、および滞在時間）を確認できます。これらはすべて API 統合を介して外部システムにエクスポートできます。

運用最適化および戦略的アジリティ

Cisco Meraki ダッシュボードは、一貫したネットワークポリシーを新しいロケーションに瞬時に展開する設定テンプレートを使用して、小売業の迅速な拡張を可能にします。ゼロタッチ プロビジョニングでは、デバイスの出荷、接続、およびクラウドからの設定の自動受信により、数時間以内で店舗を稼働状態にすることができます。一元管理により、各ロケーションにネットワーク専門担当者を配置する必要がなくなり、リモートでの障害対応および診断によって現場訪問せずにほとんどの問題が解決されます。BAC は、展開前の Infrastructure-as-Code ワークフロー、バージョン管理、およびネットワーク設定の自動テストを有効にすることで、効率をさらに高めます。組み込みの変更追跡と監査ログにより、完全な可視性が提供されます。ロールベースの管理は、アクセス権限の委任による FC モデルをサポートします。

統合ブランチアーキテクチャを使用したクラウド管理型小売プロファイルは、従来のブランチネットワーキングから、ネットワーク機能をビジネス目標および運用要件と直接一致させる包括的なソフトウェア定義型小売インフラストラクチャへの進化を表しています。

Cisco Meraki クラウドダッシュボードと NAC プラクティスのこの組み合わせは、急速に変化する小売業界に合わせた、最新の小さなブランチ設計の基礎となります。

BaC の実装

BAC は DevOps NaC のアイデアを使用して、小売ブランチネットワークの管理を容易にします。各デバイスを手動で設定する代わりに、ネットワーク管理者は事前に作成された YAML テンプレートにシンプルで明確な指示を記述し、Terraform ツールを使用します。これらのテンプレートには、シスコの信頼できるベストプラクティスが含まれているため、自動的にすべてのロケーションですべてのブランチサービスを一貫して正しく設定し、管理できます。このアプローチにより、時間が短縮され、エラーが削減され、すべてのブランチが同じ高い基準に従うようになります。

このアプローチでは、Git ベースのバージョン管理、自動テスト、および CI/CD パイプラインを使用して、数日ではなく数分で新しい店舗を迅速に設定できます。さまざまなタイプの小売ビジネス間で一貫したネットワーク規格が確実になり、販売時点管理情報や在庫管理プラットフォームなどの既存の小売 IT システムとスムーズに接続できます。この自動化により、展開が迅速化し、エラーが削減され、すべての作業が効率的に連携します。このフレームワークは、小規模店舗から旗艦店まで、さまざまな小売店舗の規模に合わせてすぐに使用できるテンプレートを提供します。PCI DSS 準拠の販売時点管理（POS）ネットワーク、分析機能を備えたゲスト Wi-Fi、IoT デバイスプロファイルなど、さまざまな機能に固有の設定が含まれます。また、自動ロールバックオプションによる包括的な変更管理機能も備えています。このアプローチは、手動でのエラーが発生しやすいデバイスセットアップを自動化されたスケーラブルなサービス展開に置き換えることで、小売ネットワークの運用を変化させ、小売ネットワーク全体が最適なパフォーマンス、セキュリティ、およびコンプライアンスで稼働するようにします。

ソリューションのコンポーネント

クラウド管理型エンタープライズの基本となる 3 つの軸が存在します。シスコのプラットフォームと Cisco Meraki ダッシュボード、BaC ツールキット、および Cisco ISE です。

シスコのプラットフォームと **Cisco Meraki** ダッシュボード

Cisco Cloud Managed Enterprise では、ブランチネットワーク全体の主要なコントロールセンターとしてクラウドベースのダッシュボードを使用します。この使いやすいインターフェイスは、ネットワークコントローラのように機能し、すべての重要なデータを処理および分析します。これにより、IT チームはネットワークのあらゆる部分の正常性、パフォーマンス、およびセキュリティに関する完全なリアルタイムのインサイトを得ることができます。IT チームは、このダッシュボードから、デバイスの設定、ポリシーの適用、ユーザー体験の監視、問題の検出、および応答の自動化を実行して、ネットワークのスムーズかつ安全な稼働を維持できます。

このプラットフォームでは、この統合された管理アプローチの下に **4** つのコアサービス領域が統合されます。

Cisco Secure Routing は、従来のルーティング機能と組み込みの次世代ファイアウォール機能を単一のデバイスに統合します。さまざまなタイプのトラフィックを分離するためのネットワークのセグメンテーション、重要なアプリケーションに優先順位を付けるサービスレベル契約（SLA）に基づくポリシー、暗号化された接続用のセキュアな SD-WAN トンネル、および脅威に対する強力な保護を提供します。この統合により、ブランチオフィスやその他のロケーションに、安全かつ効率的で、適切に管理されたネットワークを作成できます。

Secure Wired Access コンポーネントは、VLAN によるネットワークのセグメンテーションを行う LAN スイッチング、ポートセキュリティ制御、および 802.1X 認証を使用して、承認されたデバイスのみがネットワークにアクセスできるようにします。

Secure Wireless Access は、従業員やゲストなどのさまざまなユーザーグループに合わせたセキュリティポリシーを使用して、個別のワイヤレスネットワークを作成する強力な認証メカニズムと複数の SSID を備えた、エンタープライズクラスの Wi-Fi 7 テクノロジーを提供します。

アプリケーションの最適化と可視化により、ビジネスに不可欠なアプリケーションがネットワーク全体で優先的に処理されます。Quality of Service（QoS）ポリシーは、音声、ビデオ、および必須のビジネスアプリケーションの一貫したパフォーマンスを保証します。ディープ パケット インスペクション（DPI）は、アプリケーションの使用パターンについての詳細な可視性を提供します。シスコと ThousandEyes の統合により、ブランチロケーションから WAN を経由してクラウドアプリケーションおよびデータセンターまで、エンドツーエンドのアプリケーション パフォーマンス モニタリングが提供されます。

これらすべてのコンポーネントが一元化されたダッシュボードを介して連携して動作するため、IT チームはデバイスの設定、ポリシーの適用、ユーザー体験の監視、異常の検出、自動応答のオーケストレーションを一元管理できます。

この統合アプローチにより、複雑な運用データが実用的なインテリジェンスに変換され、プロアクティブなネットワーク管理と迅速な問題解決が可能になり、マルチベンダーブランチ環境によく見られるフラグメンテーションが解消されます。

BaC ツールキット

BaC ツールキットにより、小売組織は実証済みの DevOps 原則と Infrastructure as Code 方法論を使用して、ネットワーク インフラストラクチャを展開して管理できるようになります。このツールキットに含まれる専用の Terraform プロバイダーは、高度なビジネスインテントを Meraki の製品ポートフォリオ全体でデバイス固有の設定に変換するためのプログラマチック インターフェイスとして機能します。検証済みの YAML テンプレートは、さまざまな店舗規模や運用要件に対応した小売業界に固有の展開パターンを提供し、POS ネットワークのセグメンテーション、ゲスト Wi-Fi 設定、IoT デバイスポリシー、およびコンプライアンス フレームワーク

に関するシスコの実証済みのベストプラクティスを組み込んでいます。このツールキットは、Git の統合によるバージョン管理されたネットワークの設定、展開前の設定を検証する自動化されたテストパイプライン、および承認プロセスと自動ロールバック機能を備えた包括的な変更管理ワークフローを有効にします。このアプローチにより、従来は数日かかっていた手動でのネットワーク展開が数分で終わるようになります。同時に、一貫性が確保され、人的エラーが削減され、何百もの小売ロケーションでの法規制遵守のための完全な監査証跡が提供されます。現在の初回リリースでは、BaC は小規模ブランチ設計をサポートしています。中規模および大規模ブランチは、次のリリースで計画されています。ブランチのセキュリティは分散型で、セキュリティは個別のブランチに対して設定されます。

Cisco ISE

ISE との統合により、すべての小売ロケーションで一元化された RADIUS 認証とポリシー適用が提供され、従業員、請負業者、ゲスト、および IoT デバイスの詳細なアクセス制御が可能になります。Cisco ISE では、ユーザーアイデンティティ、デバイスタイプ、およびロケーションのコンテキストに基づいてダイナミックなポリシー割り当てが行われ、POS 端末は自動的にセキュアな決済ネットワークに配置され、ゲストデバイスはインターネット専用セグメントに誘導されます。このプラットフォームでは、企業デバイスに対する証明書ベースの認証、従業員アクセス用の Active Directory 統合、および IoT デバイスの自動識別とポリシー割り当て用のデバイスプロファイリングがサポートされています。包括的なコンプライアンスレポート機能によって、規制要件の詳細な監査証跡が提供されます。一方、リアルタイムの脅威の封じ込めにより、侵害されたデバイスの即時のネットワーク隔離が可能になります。これにより、分散型小売環境全体で堅牢なセキュリティ態勢が保証されます。

クラウド管理型小売業界のプロファイル概要

次の表に、クラウド管理型小売業界のソリューションプロファイルの主な焦点領域を示します。

主要な展開領域	機能
企業キャンパスのグリーンフィールド展開	Cisco Meraki クラウドダッシュボードで管理する新しい企業キャンパスの立ち上げ
共通エンタープライズ サービス アクセス用データセンター接続	データセンター向けのキャンパスコアレイヤ BGP/OSPF 設定
Meraki SD-WAN 展開	企業キャンパス、データセンター、および小売店舗を接続するための Meraki SD-WAN の立ち上げ WAN の復元力
小売店舗/ブランチの展開	BaC インフラストラクチャを使用した店舗ネットワークの展開 有線およびワイヤレスのセキュリティフレームワーク Guest Access ファイアウォールポリシー
小売店舗の季節ごとの拡張性と迅速な展開	BaC を使用した新しい店舗/ブランチの展開
エンドツーエンドのアプリケーション パフォーマンス モニタリング	Thousand Eyes ブランチ/店舗の正常性ダッシュボード
組織全体のイメージ管理	ゼロタッチファームウェア管理

ハードウェアとソフトウェアの仕様

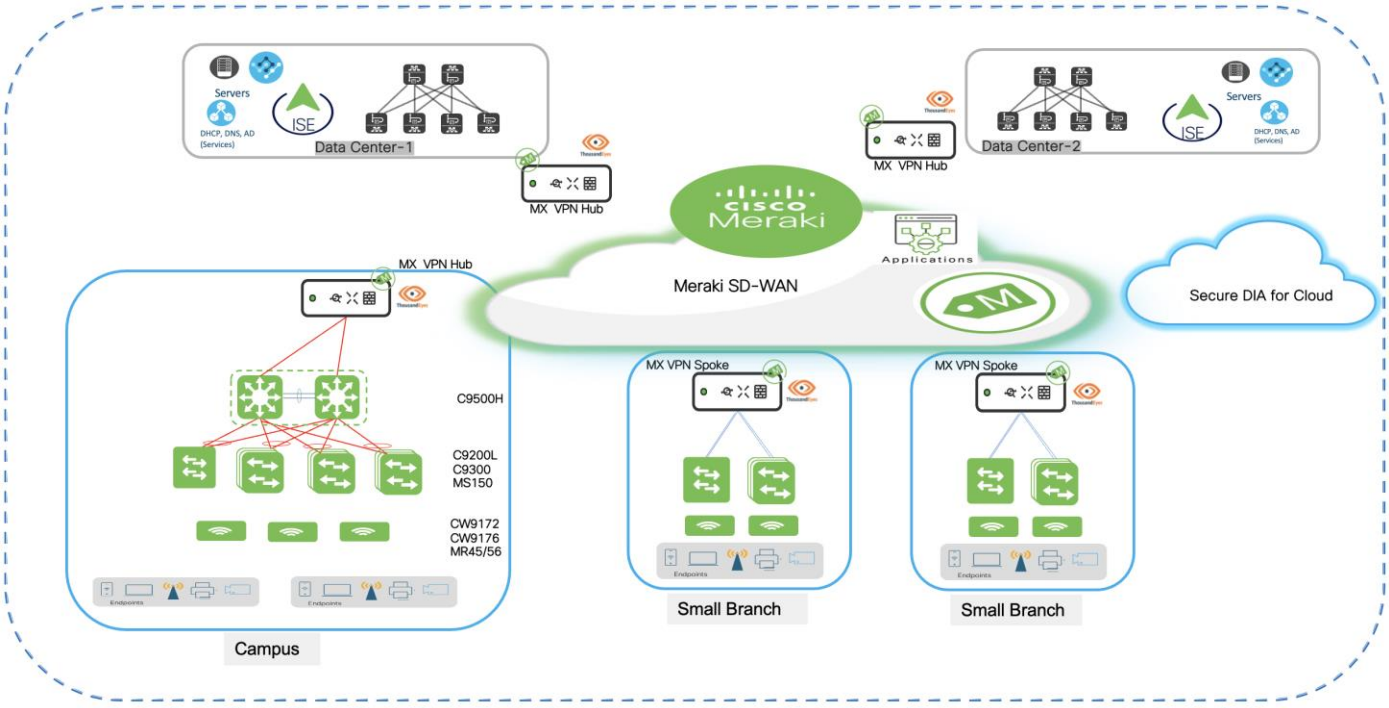
ソリューションは、次の表に示すハードウェアとソフトウェアで検証されています。

クラウド管理向けにサポートされている Catalyst の完全なリストについては、「Enable Cloud Management for Catalyst Switches with Device Configuration」を参照してください。

ロール	モデル名	ソフトウェアバージョン
クラウド管理型 Catalyst	C9500-32C、C9300-24P、C9300-48P、C9300-48T、C9300X-24Y、C9200L-24P-4G	17.18.2
Meraki MX	MX85、MX95、MX68	19.1.1
ワイヤレス アクセス ポイント	CW9172、CW9176、MR42、MR45、MR56	31.1
Meraki Vision カメラ	MV12W	
アイデンティティ管理、RADIUS サーバー	SNS-3695-K9	2.7 パッチ 7

クラウド管理型小売業ソリューショントポロジ

図 1. 企業向け小売業ソリューション トポロジ



ソリューションの使用例

主要な展開領域	機能
企業キャンパスのグリーンフィールド展開	Cisco Meraki クラウドダッシュボードで管理する新しい企業キャンパスの立ち上げ クラウド管理モードでの Catalyst スイッチのオンボーディング キャンパスでのコアレイヤ、ディストリビューション レイヤ、およびアクセスレイヤの展開 キャンパス ルーティング アーキテクチャとデザイン 冗長性とハイ アベイラビリティ
共通エンタープライズ サービス アクセス用データセンター接続	データセンター向けのキャンパスコア レイヤ BGP 設定
企業ワイヤレス展開	Cisco Meraki ダッシュボードへの AP のオンボーディング 企業本社への Wi-Fi 展開 高度な QoS とセキュリティを備えたエンタープライズグレードのワイヤレス キャプティブポータルを使用したゲストワイヤレス
Meraki SD-WAN 展開	キャンパスからブランチへの通信 本社と店舗間の AutoVPN メッシュ 高可用性と WAN の復元力：WAN アップリンクの選択と MX でのロードバランシング（ハブおよびスポーク）
小売店舗/ブランチの展開	BaC：展開ガイドライン BaC インフラストラクチャを使用したブランチ/店舗ネットワークの展開
	セキュリティフレームワーク： ゼロトラスト ネットワーク アクセスの原則 セキュアなワイヤレス接続 WPA3-Enterprise（POS は Wi-Fi を使用） 有線 POS のアクセスポリシー 脅威からの保護とコンテンツフィルタリング（AMP、IPS/IDS） POS トラフィックを保護するファイアウォールポリシー：MX での NGFW ダイレクト インターネット アクセス（ローカル インターネット ブレークアウト）/VPN 除外ルール 高可用性と WAN の復元力 SLA ベースの WAN パフォーマンスポリシー：アップリンクの選択とロードバランシング

主要な展開領域	機能
	アプリケーション モニタリングとアラート
	ゲスト Wi-Fi および顧客フットフォール分析 キャプティブポータルを使用したゲスト Wi-Fi ゲストネットワークのファイアウォールルール コンテンツフィルタリング ロケーション分析
季節ごとの拡張性と迅速なブランチ/店舗展開	BaC テンプレートを使用した新しい店舗/ブランチの展開
エンドツーエンドのアプリケーション パフォーマンス モニタリング	ネットワークパフォーマンスの可視性のためにブランチ MX に導入された ThousandEyes
組織全体のイメージ管理	企業全体のゼロタッチファームウェア管理

スケール

ソリューションのテストでは、次の表に示すスケールの数値について確認しました。

カテゴリ	値
ブランチ数	10
ブランチあたりのデバイス数	10
アクセスポイントの数	400
エンドポイントの数	4500

ソリューションの基調講演

Cisco Meraki ダッシュボード組織とデバイスインベントリの前提条件

以下のセクションで詳しく説明するキャンパスおよびブランチの展開設定に進む前に、お客様は自身の Cisco Meraki ダッシュボード組織の基本セットアップを完了し、すべてのネットワークデバイスを要求してインベントリに追加する必要があります。この前提条件は、合理化された展開エクスペリエンスを保証するもので、このクラウド管理型小売プロファイルの基盤となる一元化された管理機能が有効になります。

手順 1。 展開前の必須手順：

ステップ 1. Cisco Meraki ダッシュボード組織の作成：お客様は、小売ネットワーク インフラストラクチャ全体の中央管理プラットフォームとして機能する Cisco Meraki ダッシュボード組織アカウントを確立する必要があります。この組織は、小売企業全体のキャンパス Catalyst スイッチ、ブランチ Meraki アプライアンス、ワイヤレス AP、および関連するすべてのポリシーと設定を管理するための管理フレームワークを提供します。

ステップ 2. 企業ネットワークの作成：Cisco Meraki ダッシュボード組織内で、企業のキャンパス展開専用のネットワーク構造を作成します。[組織（Organization）] > [設定（Configure）] > [ネットワークの作成（Create Network）] の順に選択し、企業の命名規則に従って名前を付けたネットワークを確立します（「Corporate-HQ-Campus」や「Retail-Headquarters」など）。適切なネットワークタイプとして [スイッチ（Switch）] を選択し、Catalyst スイッチ管理機能を有効にします。このネットワーク構造は、すべてのキャンパス インフラストラクチャ デバイスと、その関連する設定、ポリシー、およびモニタリングデータの論理コンテナとして機能します。

ステップ 3. デバイスインベントリの要求：Catalyst 9500 コアスイッチ、Catalyst 9300 ディストリビューションおよびアクセススイッチ、MX セキュリティ アプライアンス、MS スイッチ、および MR AP を含むすべてのネットワークデバイスを、固有のシリアル番号を使用して要求し、Cisco Meraki ダッシュボードのインベントリに登録する必要があります。[組織（Organization）]、[設定（Configure）]、[インベントリ（Inventory）]の順に選択し、シリアル番号を入力するか、一括要求用の CSV ファイルをアップロードしてデバイスを追加します。この要求プロセスにより、デバイスの所有権が確立され、クラウド管理機能が有効になり、ネットワーク割り当てと設定展開のためにデバイスの準備が整います。

ステップ 4. ライセンス検証：適切な Cisco Meraki ライセンス（Enterprise、Advanced Security、SD-WAN Plus）が、要求されたすべてのデバイスに適用されていること、およびライセンスの期限日が動作要件と一致することを確認します。[組織（Organization）]、[設定（Configure）]、[ライセンス情報（License Info）] でライセンスステータスを確認し、すべてのデバイスにアクティブなサブスクリプションがあることを確認します。BaC 機能、ThousandEyes との統合、エンタープライズ セキュリティ機能といった高度な機能にアクセスするには、有効なライセンスが必要です。

ステップ 5. ネットワーク管理者アクセス：組織構造に合わせたロールベースのアクセス制御を使用して、適切な管理アカウントを確実に作成します。[組織（Organization）] > [設定（Configure）] > [管理者（Administrators）] の順に選択して、適切な権限レベルのアカウントを作成します。企業の IT チーム向けのフルアクセス権を持つ管理者、運営担当者向けの読み取り専用アクセス権、およびフランチャイズマネージャーまたは地域マネージャー向けに委任された管理者権限などがあります。

ステップ 6. ネットワークデバイスの割り当て：デバイスがインベントリに要求されたら、適切なネットワーク構成に割り当てます。キャンパス Catalyst スイッチは企業のキャンパスネットワークに割り当てますが、ブランチデバイスはそれぞれの店舗ネットワークに割り当てます。[組織（Organization）] > [インベントリ（Inventory）] の順に選択し、デバイスを選択して、[ネットワークに追加（Add to network）] 機能を使用して割り当てプロセスを完了します。

ステップ 7. Catalyst スイッチのオンボーディング：シスコの正式なオンボーディング手順に従って、Catalyst 9500 および 9300 スイッチをクラウド管理モードで Cisco Meraki ダッシュボードにオンボーディングします。このプロセスには、スイッチを従来の IOS-XE 管理からクラウド管理型動作に変換す

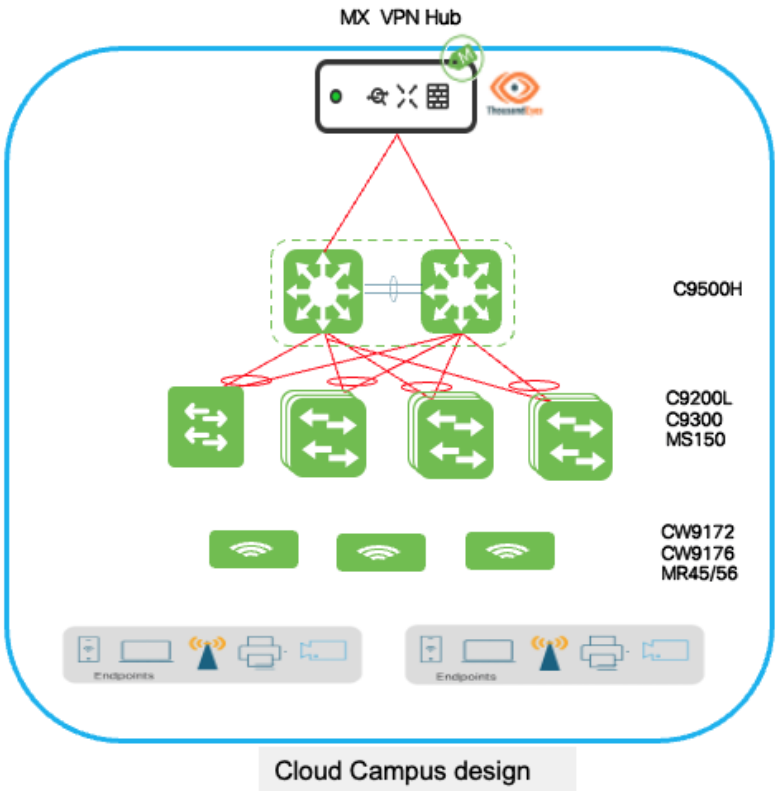
ること、Cisco Meraki クラウド インフラストラクチャとのセキュアな通信を確立すること、および企業のネットワーク構成内にデバイスを登録することが含まれます。クラウド管理型 Catalyst スイッチのオンボーディングに関する詳細な手順については、シスコの公式ドキュメント「Onboarding Cloud-Managed Catalyst switches to the Meraki Dashboard」を参照してください。オンボーディングプロセスには、最初のデバイス検出、クラウドリダイレクトの設定、セキュアな証明書の交換、クラウド管理接続の検証が含まれます。

これらの前提条件が完了したら、お客様は後続の展開セクションに進み、クラウド管理型インフラストラクチャ基盤を利用して、このシスコ検証済みプロファイルに詳しく記載されているキャンパスおよびブランチネットワークのアーキテクチャを導入できるようになります。

企業キャンパスのグリーンフィールド展開

企業キャンパスのグリーンフィールド展開では、コアまたはディストリビューションに配置された Cisco Catalyst 9500-SVL と、アクセス層に配置された Catalyst 9300/9200L スイッチを活用します。これらはすべて Cisco Meraki クラウドダッシュボードで管理され、統合された可視性を実現します。このクラウド管理型アーキテクチャは、ゼロタッチプロビジョニングを介したシームレスな Catalyst デバイスのオンボーディングによる、数百もの分散店舗の企業アプリケーション、インベントリ管理、企業サービスを含む一元化された小売業務をサポートします。企業クライアントは Active Directory と統合された 802.1X 認証を受信する一方、モバイルスキャナや保管倉庫端末などの小売業固有のデバイスは自動的にプロファイリングされて適切なネットワークセグメントに割り当てられ、ベンダーや FC パートナーのゲストアクセスには、分離されたネットワークセグメントを使用したキャプティブポータル認証が使用されます。9500-SVL コアペアは、ビジネス継続性のための分散型フォワーディングによる高可用性を提供します。一方、アクセス層は、冗長アップリンク用に EtherChannel リンク集約と StackWise スタッキングを実行し、管理を簡素化します。これにより、すべての階層でシングルポイント障害が解消されます。Cisco Meraki ダッシュボードは、一元化されたポリシー管理、リアルタイムモニタリング、および自動化されたコンプライアンスレポート機能を提供することで、さまざまなクライアントグループ間で一貫したセキュリティ態勢を維持できます。このアーキテクチャは、地域の本社から数千の店舗ロケーションを管理するエンタープライズ規模のオペレーションまで拡張でき、キャンパスをネットワーク運用、ポリシー配布、および一元化された認証の中央ハブとして配置します。一方、BaC の原則は、一貫した設定とセキュリティフレームワークをすべての店舗ロケーションに拡張します。

企業の小売キャンパス図



Catalyst スイッチのクラウド オンボーディング プロセス

Cisco Meraki ダッシュボードを介してクラウド管理型モードで動作する Cisco Catalyst 9000 シリーズ スイッチには、従来の IOS-XE 管理スイッチをクラウド管理型動作に変換する、合理化されたオンボーディングプロセスが必要です。これにより、Cisco Meraki クラウド インフラストラクチャへの安全な接続が確立され、一元化された設定とモニタリング機能が有効になります。オンボーディング ワークフローには、基本接続設定のためのスイッチへの初回コンソールアクセス、スイッチが HTTPS 経由で Cisco Meraki クラウドサービスに到達できるようにするネットワークパラメータのセットアップ、およびスイッチをローカル CLI 管理からクラウドベースのダッシュボード制御に移行させるクラウドリダイレクトのアクティブ化が含まれます。オンボーディング中、スイッチはクラウド管理ソフトウェアをダウンロードし、TLS を使用して Cisco Meraki インフラストラクチャとのセキュアな暗号化通信を確立し、ライセンスと組織の割り当てを検証し、その設定をダッシュボードで割り当て済みのネットワークと同期します。その後、後続のすべての管理操作は、直感敵に操作できる Web ベースのインターフェイスを使用して行うため、直接 CLI アクセスや複雑な設定ファイルの管理を行う必要がなくなります。

オンボーディングの前提条件と手順の詳細

包括的なステップバイステップのオンボーディングガイドは、シスコの公式ドキュメント「Onboarding Cloud-Managed Catalyst switches to the Meraki Dashboard」を参照してください。このドキュメントでは、コンソール接続の要件とデフォルトのクレデンシャルアクセスを含む最初のスイッチの準備、管理 VLAN のセットアップと IP アドレス割り当て方法（DHCP または静的）を指定するネットワーク接続の設定、スイッチが必要な Cisco Meraki クラウドエンドポイント（meraki.com、*.cisco.com）に到達できるようにするインターネット接続の検証、運用制御をダッシュボードに移行させる enable cloud-managed コマンドによるクラウド管理モードのアクティブ化、シリアル番号または注文番号を使用して物理スイッチを組織のインベントリに関連付ける要求手順、および、クラウド登録の成功を妨げる可能性のある接続障害、証明書検証の問題、またはライセンスの問題などのよくあるオンボーディング課題に対処するトラブルシューティング ガイダンスについて詳しく説明しています。

リテールキャンパス環境に複数の Catalyst スイッチを展開する組織は、展開アクティビティを開始する前にオンボーディング ドキュメント一式を確認し、コア層、ディストリビューション層、およびアクセス層全体への大規模なロールアウトに進む前に、IT 担当者がプロセスフロー、必要なネットワークの前提条件、および検証手順を理解できるようにする必要があります。

オンボーディング後の設定および管理接続

Catalyst スイッチがクラウド オンボーディング プロセスを完了し、Cisco Meraki ダッシュボードでネットワークに正常に追加されると、スイッチはファームウェア同期プロセスを自動的に開始し、組織レベルで設定された最新の安定したファームウェアバージョンにアップグレードします。これにより、手動介入なしで展開内のすべてのスイッチでの一貫性が確保されます。初回接続の確立時に、スイッチはアップストリーム ネットワーク デバイスで使用可能な VLAN から DHCP を介して動的に管理 IP アドレスを取得するため、管理者が特定の管理ネットワークパラメータを設定する前であっても、即時のクラウド通信とダッシュボードの登録が可能になります。このブートストラップ接続により、スイッチが Cisco Meraki クラウドサービスに到達し、設定がダウンロードされ、ダッシュボードでオンラインデバイスとして表示されます。これにより、スイッチを遠隔地に直接出荷し、技術者以外の担当者が電源を投入し、自動的にプロビジョニングできる真のゼロタッチ展開が可能になります。オンサイトでの IT 専門スタッフや手動での設定は不要であり、最終的なネットワーク アーキテクチャがまだ完全に実装されていない展開フェーズ中にも運用の柔軟性を提供します。クラウド接続と初期登録が成功したことを確認したら、ネットワークに専用管理 VLAN を設定します。

手順 2。 ネットワークに専用管理 VLAN を設定するには、次の手順を実行します。

ステップ 1. [スイッチ（Switch）] > [設定（Configure）] > [スイッチ設定（Switch Settings）] > [管理 VLAN（Management VLAN）] の順に選択します。

ステップ 2. ネットワーク管理用に指名された VLAN ID を指定します。

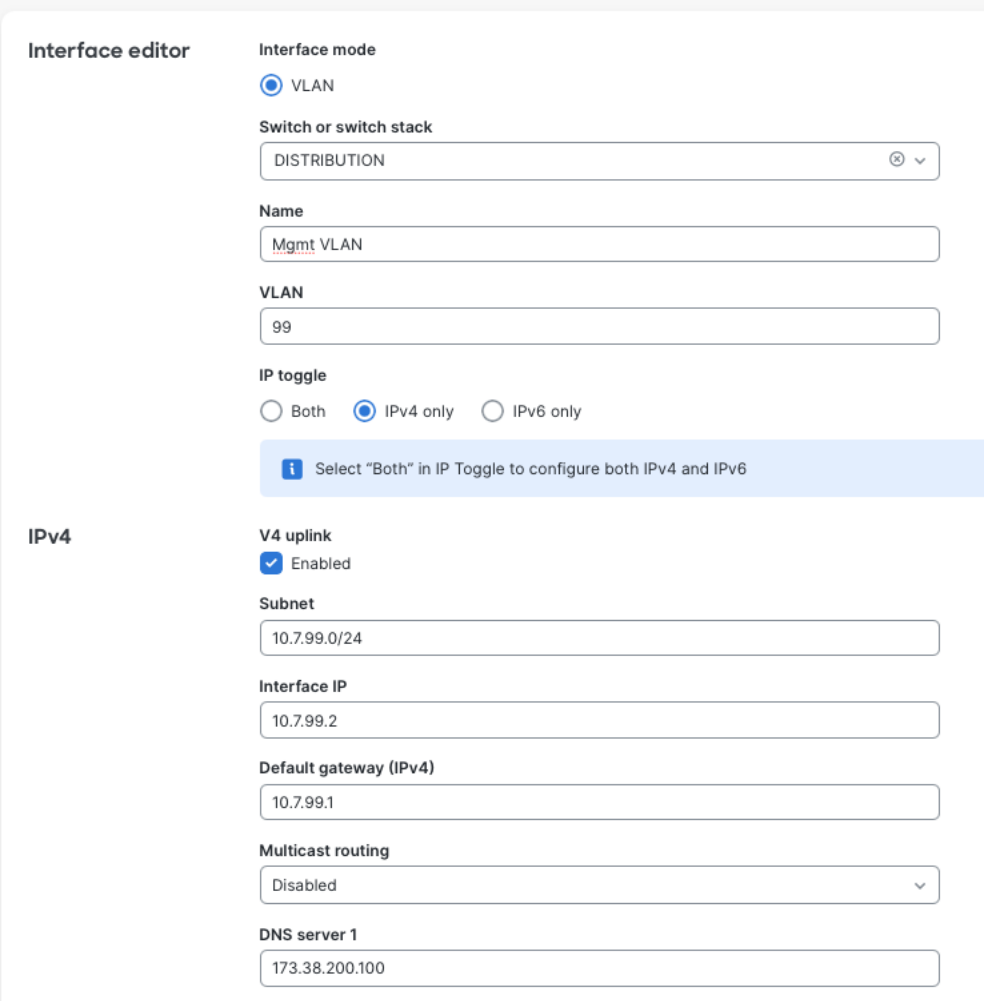
ネットワークの管理 VLAN を設定すると、そのネットワーク内のすべてのスイッチは、現在の DHCP 割り当て IP アドレスを自動的に放棄し、定義した管理 VLAN から新しい IP アドレスを要求します。この変更により、管理接続が、ネットワーク インフラストラクチャの管理、モニタリング、およびアクセスに使用される特定の標準的なネットワークセグメントに移動されます。これにより、管理トラフィックを分離して整理しておくことができます。

ステップ 3. （オプション）モニタリングシステム、ドキュメント要件、または組織 IP アドレス管理ポリシーをサポートするために、管理インターフェイスに静的 IP アドレス指定が必要な環境では、[スイッチ（Switch）]、[スイッチの詳細（Switch Details ）]、[スイッチの選択（Select Switch）]、[管理インターフェイス（Management Interface）] でスイッチごとに静的管理 IP アドレスを設定します。

ステップ 4. （オプション）DHCP から静的アドレス指定に移行する場合は、[スイッチング（Switching）] > [ルーティング＆DHCP（Routing & DHCP）] を使用して、指定された管理 VLAN 内に管理 IP サブネットを作成します。

1. 管理接続用のサブネット範囲、デフォルトゲートウェイ、および DNS サーバーを定義します。
2. 管理 VLAN 設定で [アップリンク（Uplink）] 設定を有効にし、Cisco Meraki クラウド インフラストラクチャを含む外部ネットワークに到達できる VLAN として指定します。

この静的 IP 設定はスイッチごとに適用されるため、一部のスイッチでは簡素化された管理のために DHCP を使用し、重要なインフラストラクチャスイッチ（コア層およびディストリビューション層）では静的アドレス指定を使用する混在環境が可能になります。静的アドレス指定は、正確なドキュメント化と、一貫した接続とレポート機能を実現するために予測可能で変化しない管理 IP アドレスを必要とするエンタープライズ ネットワーク管理システム、SNMP モニタリング プラットフォーム、および syslog サーバーとの統合のために必要です。



Catalyst 9500 StackWise Virtual をコアに展開する

コア層展開では、Cisco Catalyst 9500 シリーズ スイッチは StackWise Virtual Link（SVL）設定で導入され、小売本社のキャンパスネットワークに復元力のあるルーティング、VLAN 間サービス、および集約機能を提供する高可用性インフラストラクチャが作成されます。大規模なキャンパス展開では、9500-SVL ペアは、ディストリビューション ブロック、データセンター接続、および WAN エッジサービス間の高速転送を提供する専用コア層として機能しますが、小規模または中規模のキャンパスでは、9500-SVL をコラプストコア/ディストリビューション層として展開する場合があります。これは単一の冗長スイッチペア内で両方の階層機能を結合して、エンタープライズクラスの機能を維持しながら、インフラストラクチャの複雑さとコストを削減できます。

StackWise Virtual テクノロジーは、物理的に離れている 2 つの Catalyst 9500 シャーシを、統合管理、アクティブ-アクティブ転送、および 1 秒未満のフェールオーバー機能を使用して単一の論理スイッチに仮想化することで、シングルポイント障害をなくし、運用管理を簡素化します。SVL の実装では、ペアリングされたシャーシ間でデュアル 100G SVL 接続を使用して広帯域幅のシャーシ間通信を提供し、シームレスなトラフィック転送と設定の同期を保証します。ディストリビューション層とアクセス層は、SVL ペアを単一の論理アップストリーム デバイスとして扱うマルチシャーシ EtherChannel（MEC）設定を介して接続し、シャーシまたはリンク障害発生時の再コンバージェンス遅延なしで、アクティブ-アクティブ トラフィック分散と自動フェールオーバーを有効にします。

手順 3。 Catalyst 9500 クラウドをオンボーディングするには、次の手順を実行します。

注： オンボーディングでは、Catalyst 9300 シリーズと同じプロビジョニング ワークフローに従います。

ステップ 1. オンボーディングとクラウド登録が成功したら、Cisco Meraki ダッシュボード内で [スイッチング（Switching）] > [スイッチスタック（Switch Stacks）] > [スタックの追加（Add a Stack）] の順に選択します。

SVL 作成ウィザードでは、SVL リンクインターフェイスの割り当てやデュアルアクティブ検出（DAD）プロトコルリンクなどの重要な設定パラメータの入力が要求されます。

注： SVL および DAD ポートの選択は、適切な冗長性を確保するために、両方の物理スイッチで等しく一致する必要があります。

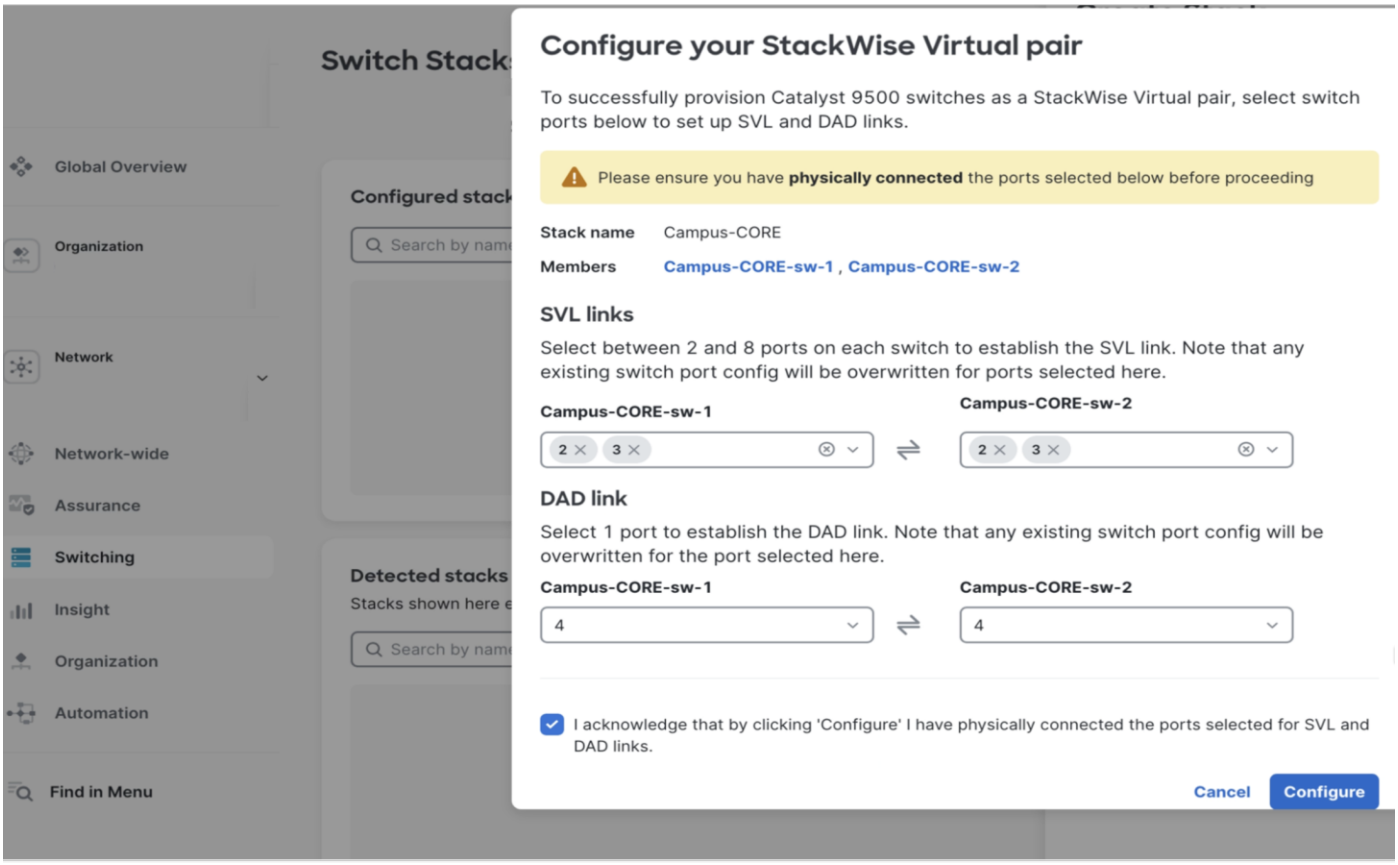
ステップ 2. スタック用に指定されている両方の Catalyst 9500 スイッチを選択します。

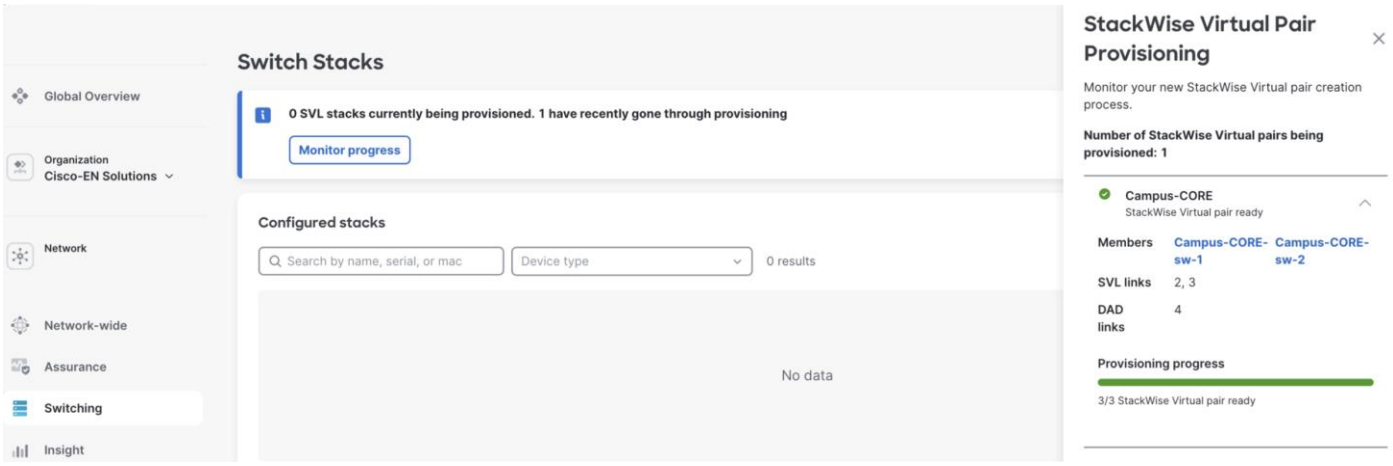
ステップ 3. SVL メンバー優先順位を指定します。

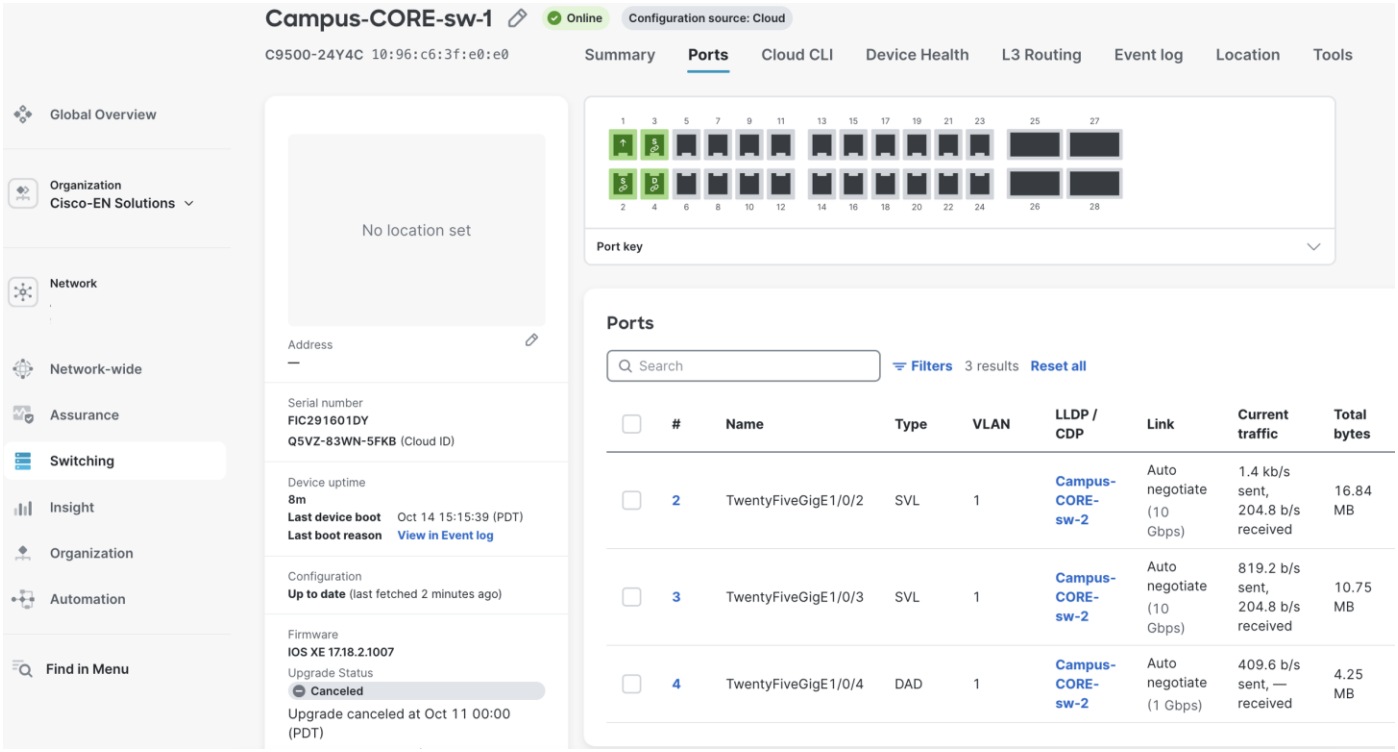
ステップ 4. 対応する物理インターフェイスを設定します。

ワークフローが完了すると、両方のスイッチが自動的に同期リブートを開始し、SVL ドメインと、アクティブロールおよびスタンバイロールを確立します。リアルタイムの SVL 生成の進行状況は、[スイッチスタック（Switch Stacks）] ページで監視でき、スタックメンバーのステータス、同期状態、およびリンクの正常性が表示されます。

稼働状態になると、統合 SVL ペアは、ポートの複合容量、自動フェールオーバー機能、および Cisco Meraki ダッシュボードを介した一元管理機能を備えた単一の論理スイッチエンティティとして表示されます。







9300 および 9200L スタック構成アクセス層の展開

アクセス層は、エンドユーザーデバイス、プリンタ、IP 電話、ワイヤレス AP、および IoT インフラストラクチャにエンタープライズレベルの接続を提供する Cisco Catalyst 9300 シリーズ スイッチを使用しており、最新の小売キャンパス環境に必要なパフォーマンス、セキュリティ、および管理機能を提供します。コストが重要な展開や、管理オフィス、会議室、バックオフィス業務などの低密度エリアでは、Cisco Catalyst 9200L シリーズは、PoE+ サポート、固定アップリンク設定、および完全な Meraki ダッシュボード統合といった経済的な代替を提供します。

アクセス層設定では、コアの 9500-SVL ペアに向けてマルチシャーシ EtherChannel（MEC）が実装され、許可された VLAN をリンク全体でトランキングしてレイヤ 2 の冗長性と帯域幅の集約を提供し、レイヤ 3 ルーティングにはダイナミック ルート アドバタイズメントと最適なパスの選択のためにディストリビューション層とコア層の間で OSPF が設定され、ルーテッド SVI（スイッチド仮想インターフェイス）の設定は Cisco Meraki ダッシュボードから直接管理されるため、VLAN および IP アドレス指定の一元管理が可能になります。

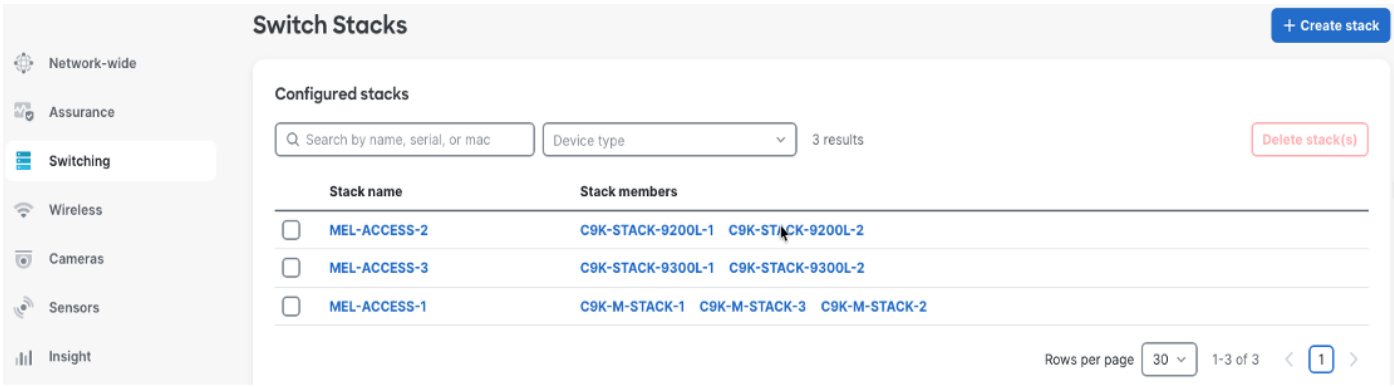
アクセス層スイッチは、スイッチの背面パネルにあるスタックポート間で専用のスタックケーブルを使用して、StackWise または StackWise-480 設定で物理的に接続され、オンボーディングプロセスが開始される前に、レジリエンスの高いマルチシャーシシステムを構築します。前のセクションで説明した標準のクラウド オンボーディング手順に従って、物理スタックにある個々のスイッチの電源が投入され、Cisco Meraki クラウド インフラストラクチャに接続され、一意のシリアル番号を使用してダッシュボードに登録されます。Cisco Meraki ダッシュボードは、スイッチ間のスタッキングプロトコルの交換を介して物理的なスタッキングトポロジを自動的に検出し、手動の設定や CLI コマンドを必要とせずに論理スタック構成をインテリジェントに形成してスタッキング機能を有効にします。

手順 4。 新しく形成されたスタックを、すべてのメンバースイッチが表示された単一の管理可能なエンティティとして表示するには、次の手順を実行します。

ステップ 1. [スイッチ（Switch）] > [スイッチスタック（Switch Stacks）] の順に選択します。

ステップ 2. スタックロール（マスター/メンバー）を特定し、スタック帯域幅集約を表示します。

ステップ 3. 統合設定管理を有効にします。この場合、スタックに適用された設定は、すべてのメンバースイッチに自動的に伝達され、マルチシャーシシステム全体で一貫した動作が保証されます。



ステップ 4. アクセスポート設定は、Cisco Meraki ダッシュボードの集中型スイッチポート設定インターフェイスを介して、すべてのスイッチに一貫したポリシーを導入します。

ステップ 5. VLAN 割り当て、PoE パラメータ、セキュリティポリシー、およびサービス品質パラメータなどの同一の設定を使用した複数ポートの同時設定を有効にします。

マルチポート編集機能により、ネットワーク管理者は、単一または複数のスイッチ間で数十～数百のポートを選択し、標準化された設定を一括で適用できます。これにより、展開時間が大幅に短縮され、キャンパス インフラストラクチャ全体での設定の不整合がなくなります。

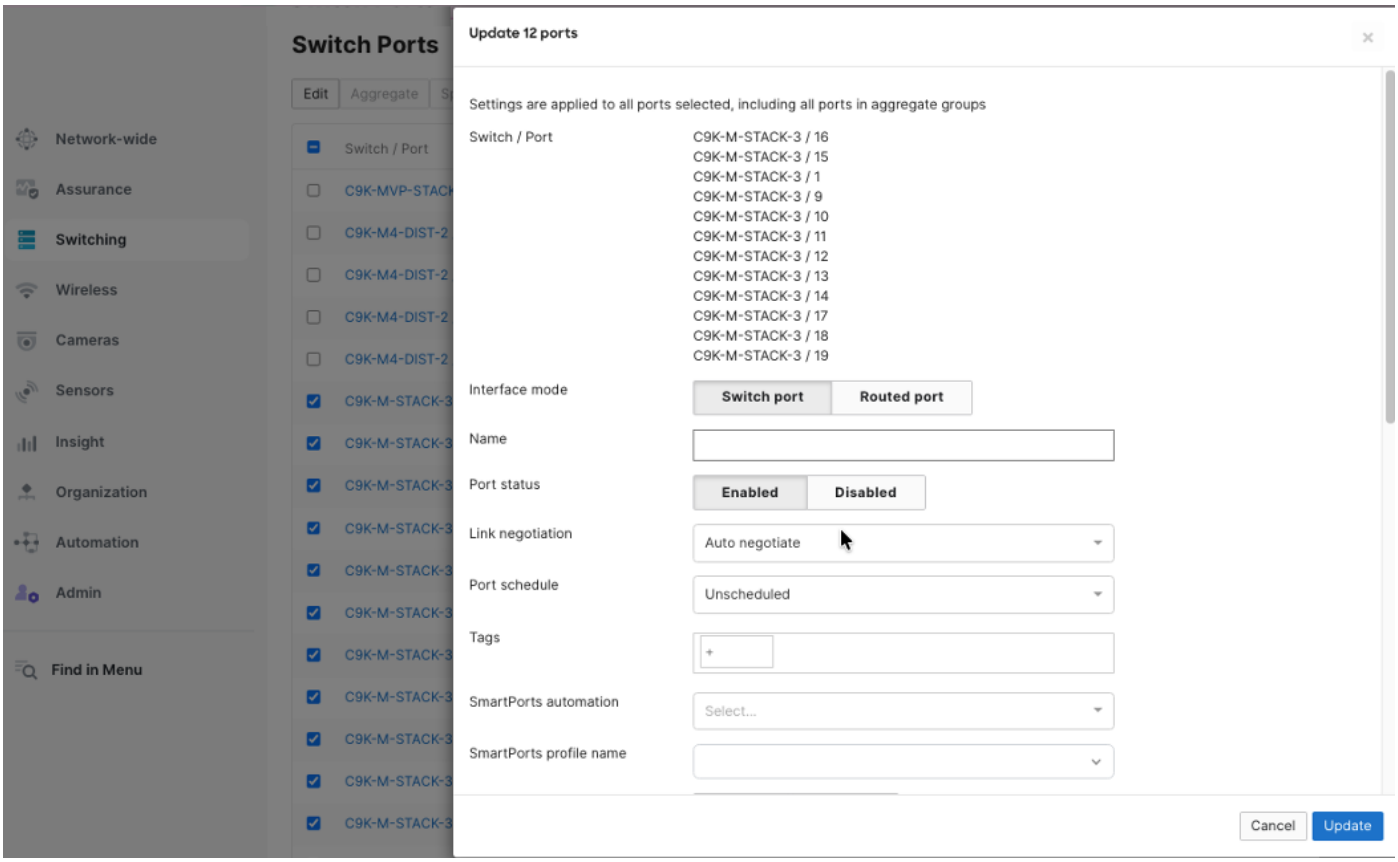
手順 5。 複数のスイッチポートをまとめて設定するには、次の手順を実行します。

ステップ 1. ダッシュボードで、[スイッチ（Switch）] > [スイッチポート（Switch Ports）] の順に選択します。

ステップ 2. 個々のスイッチポートまたはポートのグループにアクセスポリシーを割り当てます。

これらのポリシーには、VLAN メンバーシップ、認証ルール、通信シェーピング、セキュリティ制御などの設定が含まれています。

複数のポートに同じアクセスポリシーを適用すると、ポートがキャンパスのどこにあるかに関係なく、それらのポートに接続されているデバイスは同じネットワーク設定を受信します。



ネットワーク アクセス ポリシーを設定する場合は、デバイスタイプによってセキュリティおよび運用上のニーズがあることに注意してください。次に例を示します。

- **従業員ワークステーション**：802.1X 認証を使用し、企業 VLAN に接続します。
- **IP 電話**：Power over Ethernet（PoE）および QoS 設定を使用して音声 VLAN に割り当てます。
- **ワイヤレス AP**：複数の SSID をサポートするには、トランクポートを使用します。
- **プリンタ**：インターネットアクセスが制限された専用プリンタ VLAN に配置します。
- **IP カメラ**：拡張 PoE（PoE++）を使用して別のセキュリティ VLAN に割り当てます。

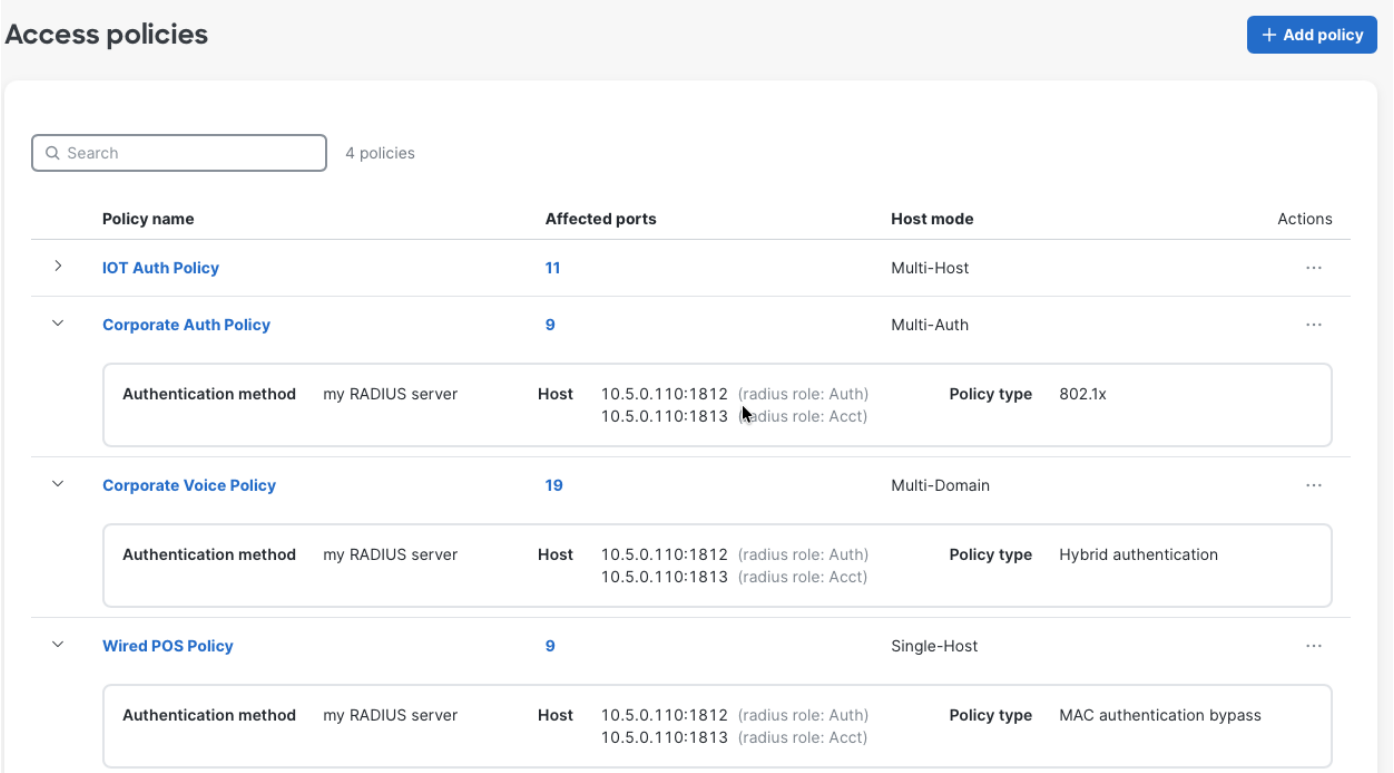
このアプローチにより、各デバイスタイプに適切なネットワーク設定とセキュリティが適用されます。

手順 6。 有線デバイスのアクセスポリシーを作成するには、次の手順を実行します。

ステップ 1. [スイッチ（Switch）] > [アクセスポリシー（Access Policies）] の順に移動します。

ポリシーは、許可およびアカウンティングに集中型エンタープライズ Cisco ISE を使用するように設定できます。

ステップ 2. 音声およびデータドメインには 802.1x、MAB またはハイブリッド認証を設定します。クリティカル/失敗/ゲスト VLAN および Radius キャッシングの詳細なオプションを使用できます。



ネットワーク VLAN プロファイルと名前付き VLAN でネットワーク管理を簡素化

Cisco Meraki ダッシュボードは、名前付き VLAN と VLAN プロファイルを統合し、Cisco ISE との統合により、分散型小売キャンパス インフラストラクチャにアイデンティティベースのダイナミックなネットワーク セグメンテーションを提供します。名前付き VLAN では、数値である VLAN 識別子が「Corporate-Employees」、「POS-Systems」、「Guest-Wi-Fi」などビジネスに関連するわかりやすいラベルに置き換えられます。これにより、設定が自動的に文書化され、管理者のエラーが削減されます。VLAN プロファイルでは、管理者が同じネットワーク内の異なるスイッチグループに対して異なる VLAN 設定を定義できるグループ化メカニズムが有効になります。これにより、建物 A のスイッチは「Corporate-Employees」を VLAN 10 にマッピングし、建物 B のスイッチは同じ名前を VLAN 40 にマッピングできます。各プロファイルには、共通の名前付き VLAN へのロケーション固有の VLAN ID の割り当てが含まれます。

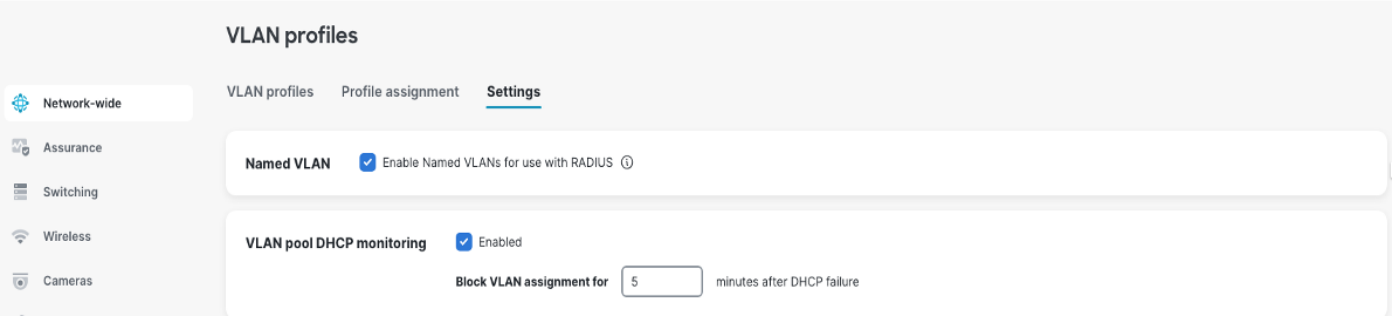
802.1X 認証中に、Cisco ISE はユーザーのログイン情報を検証し、許可フェーズで VLAN 名（「Corporate-Employees」など）を RADIUS 属性として返します。認証スイッチはこの VLAN 名を受信し、割り当てられた VLAN プロファイルを参照して、そのロケーションに対応する VLAN ID を決定します。建物 A のスイッチは「Corporate-Employees」を VLAN 10 にマッピングし、建物 B のスイッチは同じ VLAN 名を VLAN 40 にマッピングします。これにより、分散型キャンパス インフラストラクチャ全体でロケーション固有の VLAN 番号付けスキームに対応しながら、一元化された ISE 設定による一貫したポリシーの適用が実現します。このアーキテクチャにより、ISE 管理者はサイト固有の VLAN ID を認識することなく、ビジネスにとって意味のある VLAN 名を使用して認証ポリシーを定義できます（「Corporate-Employees VLAN に従業員を割り当てる」）。一方、ネットワーク管理者は建物、フロア、またはアドレス指定スキーム、レガシー インフラストラクチャの制約、または組織の環境設定に基づく機能エリアに従って、異なる VLAN 番号を柔軟に使用できます。これらはすべて Cisco Meraki ダッシュボードの統合インターフェイスを介して管理され、小売本社のキャンパス全体で一元化された設定管理と一貫したポリシーの適用が可能になります。

手順 7。 VLAN プロファイルを作成するには、次の手順を実行します。

ステップ 1. [ネットワーク全体（Network-wide）] > [VLAN プロファイル（VLAN Profiles）] の順に選択します。

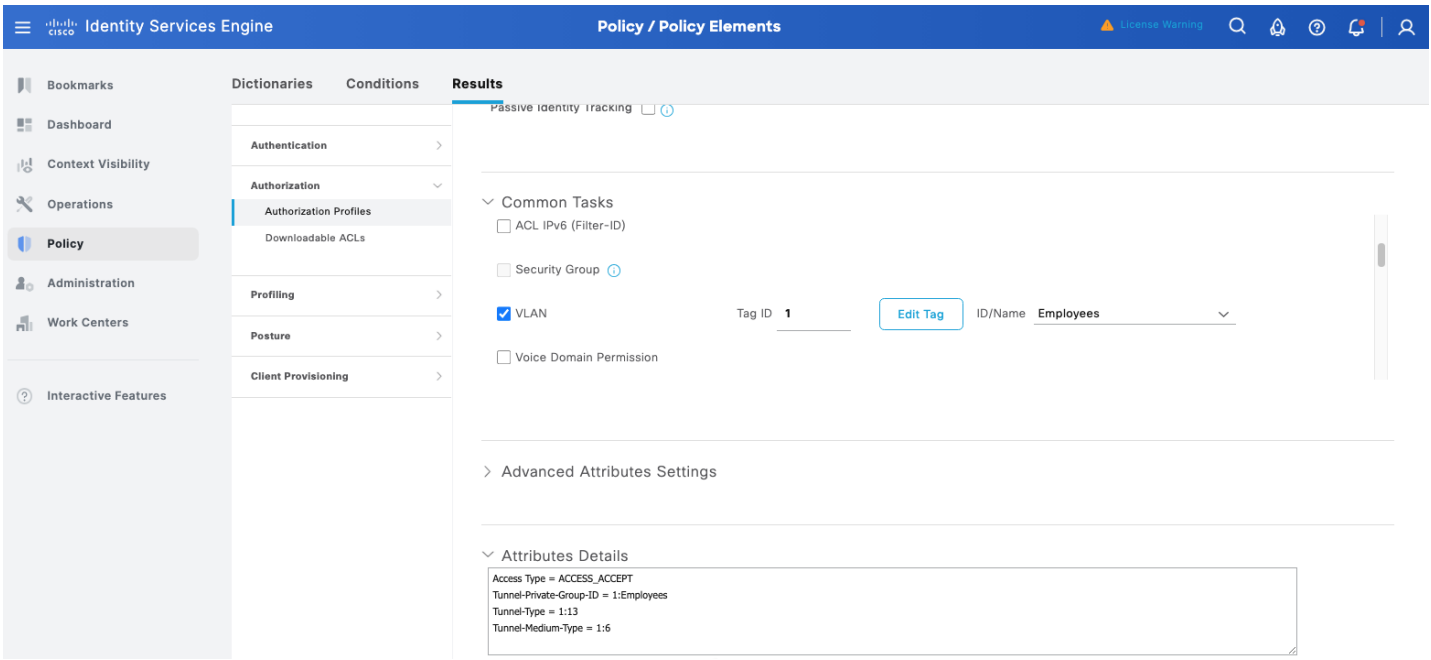
ステップ 2. アクセススイッチをそれぞれのプロファイルに割り当てます。

ステップ 3. この機能を Cisco ISE 認証で使用するには、[RADIUS で使用する名前付き VLAN を有効化（Enable Named VLANs for use with RADIUS）] オプションを有効にします。

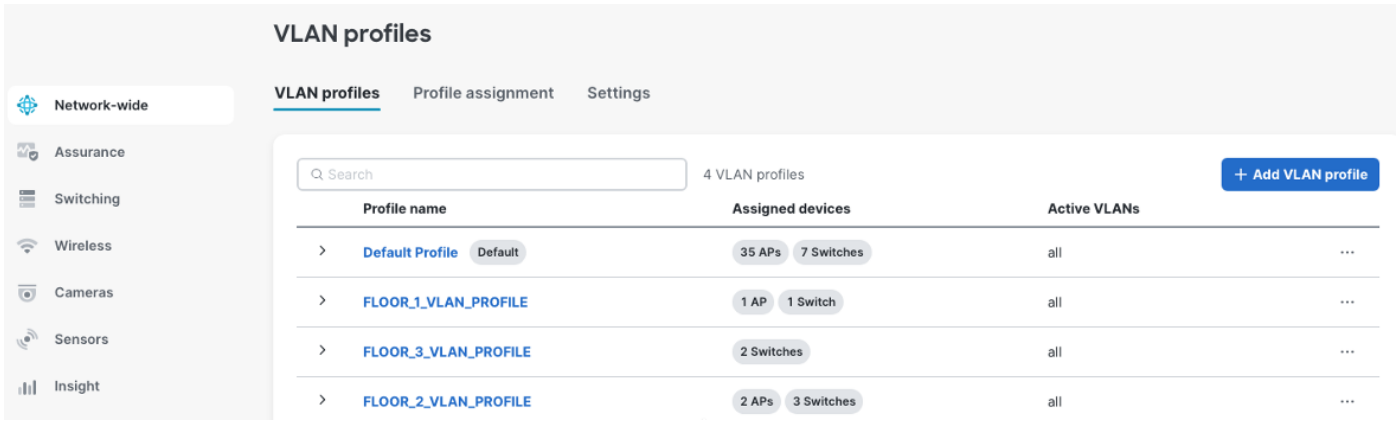


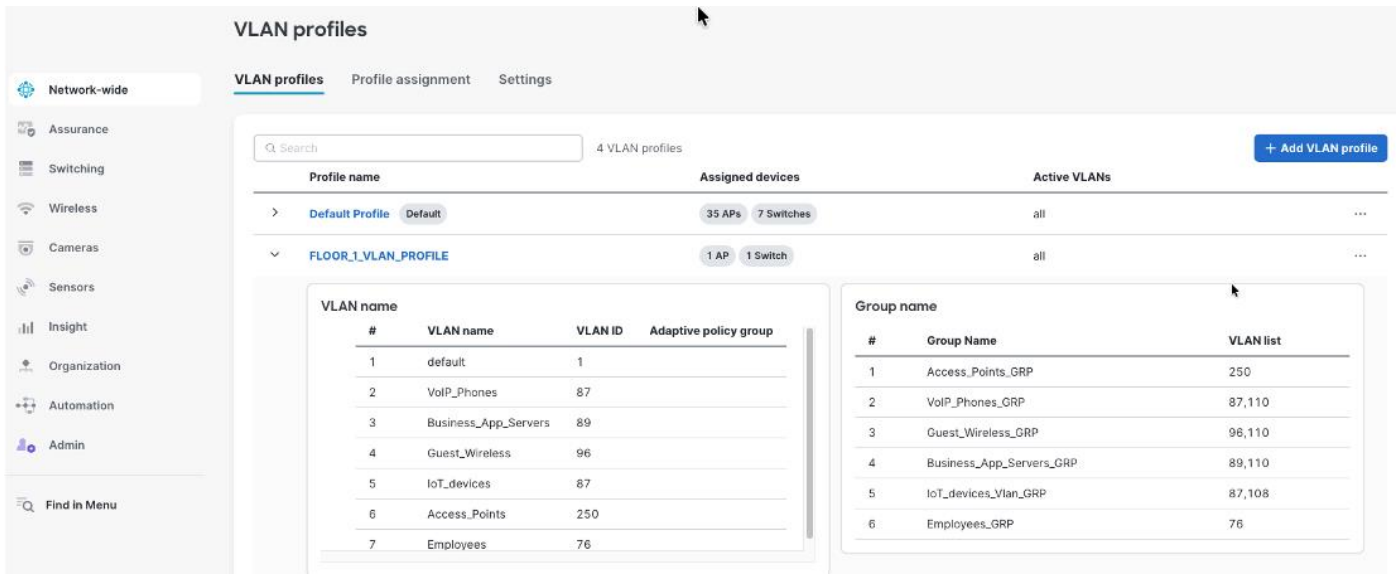
Cisco ISE の場合、VLAN 名をパラメータとして使用して認証ポリシーを定義する必要があります。

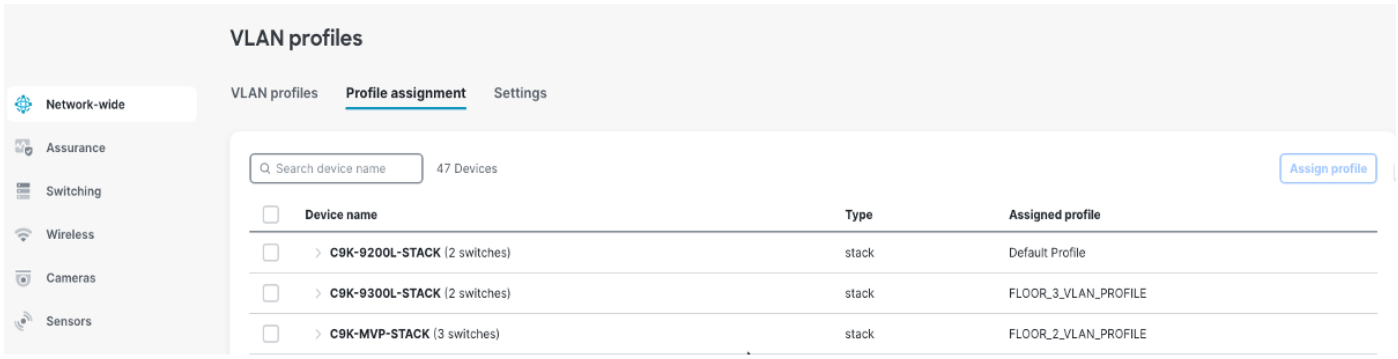
ステップ 4. [Cisco ISE] > [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）] > [プロファイル名（Profile name）] > [共通タスク（Common Tasks）] > [VLAN 名（VLAN name）] の順に選択します。次のイメージ例を参照してください。



ステップ 5. 引き続き Cisco Meraki ダッシュボードで VLAN プロファイルを定義し、アクセス スイッチをそれぞれのプロファイルに割り当てます。次のイメージ例を参照してください。







キャンパス ルーティング アーキテクチャとデザイン

クラウド管理型 Catalyst スイッチ向け Cisco Meraki ダッシュボード ソフトウェア リリースでは、キャンパスの規模、複雑さ、および運用要件に合わせた柔軟なルーティング アーキテクチャがサポートされており、小売組織が特定のインフラストラクチャのニーズや拡張性の目標に合わせた設計を導入できるようになります。

統合アーキテクチャを導入する小売環境では、Cisco Catalyst 9500 スイッチを使用したコラプストコア/ディストリビューション層を使用することで、単一の高性能スイッチペア内の両方の階層機能が結合され、すべてのキャンパス VLAN がコラプストコア上で直接設定されます。リテールサブネット SVI は、セキュリティ検査、トラフィックフローの最適化、およびルーティング制御に関する設計要件に応じて、Catalyst 9500 コアスイッ

チまたは Cisco Meraki MX アプライアンスのいずれかに柔軟に配置できます。Catalyst 9500 スイッチは、WAN 接続およびルート学習のために、ローカル Meraki MX セキュリティアプライアンス（Meraki SD-WAN ハブモードで展開）を使用して、BGP ピアリングを確立します。これらの小売サブネットは、小売キャンパス MX ハブとデータセンター MX ハブ（同じく Meraki SD-WAN ハブモードで展開）間の iBGP ピアリングを介してデータセンターにアドバタイズされます。この一元化されたアーキテクチャは、小売キャンパス インフラストラクチャ全体にデフォルト ゲートウェイ サービスと VLAN 間ルーティングを提供すると同時に、Meraki SD-WAN ファブリックの iBGP メッシュを介したハブロケーション間のダイナミックルーティングとフルネットワークの到達可能性を有効にします。

アクセス層のスイッチはレイヤ 2 モードで動作し、ディストリビューション層またはコア層への VLAN トランキングとエンドユーザーデバイス向けのアクセスポート接続を提供します。これにより、ルーティング インテリジェンスが上位のネットワーク階層に集中すると同時に、アクセス層の設定と運用が簡素化されます。

Cisco Meraki ダッシュボードを使用した Catalyst 9500 での BGP 設定

Catalyst 9500-SVL コアスイッチは、Meraki MX への BGP ピアリングセッションを確立します。これは、CLI アクセスや従来の IOS-XE コマンドライン設定を必要とせずに、Cisco Meraki ダッシュボードのスイッチング インターフェイスを介して完全に設定および管理されます。管理者は、Cisco Meraki ダッシュボードの BGP 設定インターフェイスで、データセンター フュージョン スイッチの IP アドレス、リモート AS 番号、およびセキュアなピアリングセッション用の認証ログイン情報を指定して、BGP ネイバー関係を定義します。ダッシュボード インターフェイスは、自動的にネイバー設定を検証し、ネットワークに変更をコミットする前に、AS 番号の不一致、到達不能なネイバーアドレス、認証パラメータの欠落などの一般的なエラーを検出します。

BGP パラメータの設定は、Cisco Meraki ダッシュボードのキャンパスネットワークのスイッチング設定セクションから行います。AS 番号、ネイバー関係、およびルートアドバタイズメントは設定が必要です。このクラウド管理型アプローチにより、設定シンタックスエラーがなくなり、BGP パラメータの組み込みの検証機能が提供され、キャンパス コア インフラストラクチャ全体にルーティング変更を迅速に展開できます。

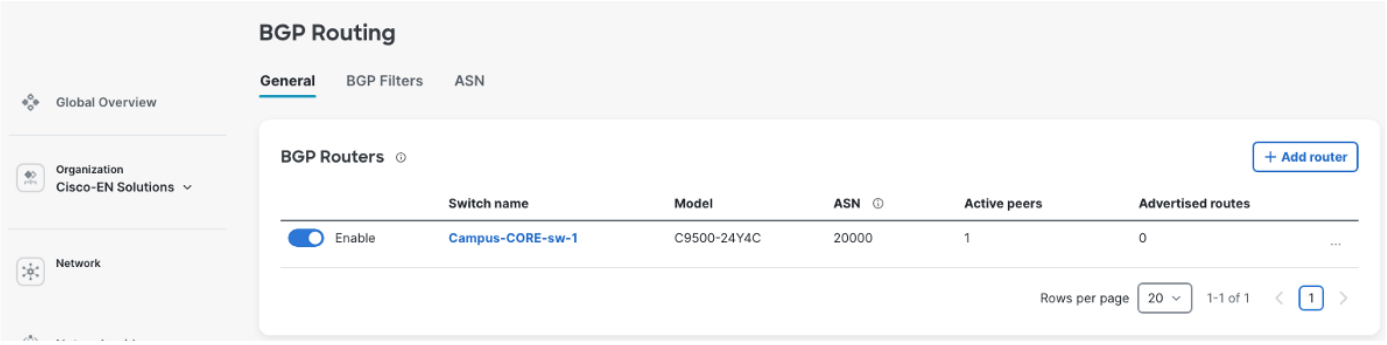
手順 8。 キャンパスの ASN を作成するには、次の手順を実行します。

ステップ 1. キャンパスコアで SVL が正常に作成されたら、[スイッチング（Switching）] > [BGP ルーティング（BGP routing）] の順に選択します。

ステップ 2. BGP ルータを追加します。

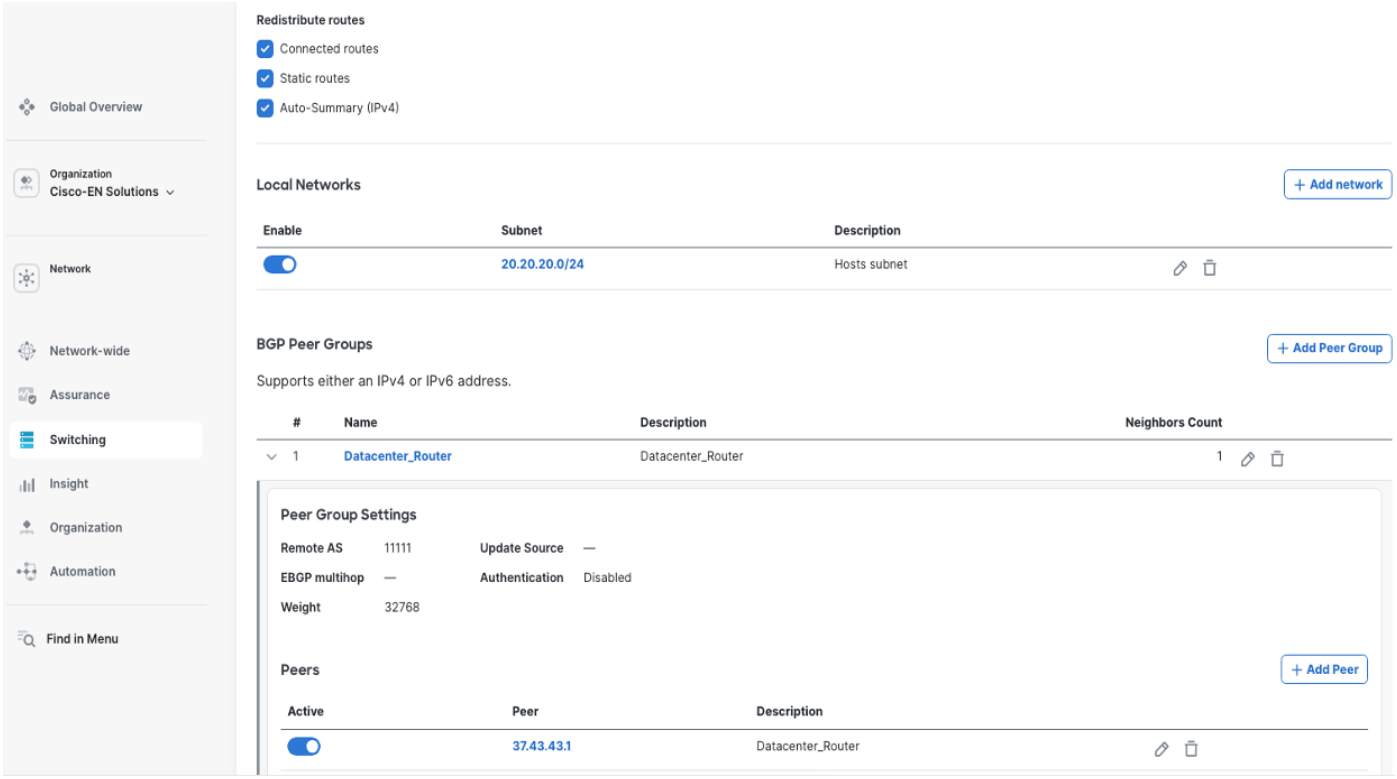
ステップ 3. スイッチを選択します。

ステップ 4. ルータ ID を設定します。



ステップ 5. ルートの再配布、ローカル ネットワーク アドバタイズメント、BGP ピアグループなどの追加機能を設定するには、作成された BGP ルータをクリックします。

最初に BGP ピアグループが作成され、次に BGP ピアがこの構成内で定義されます。



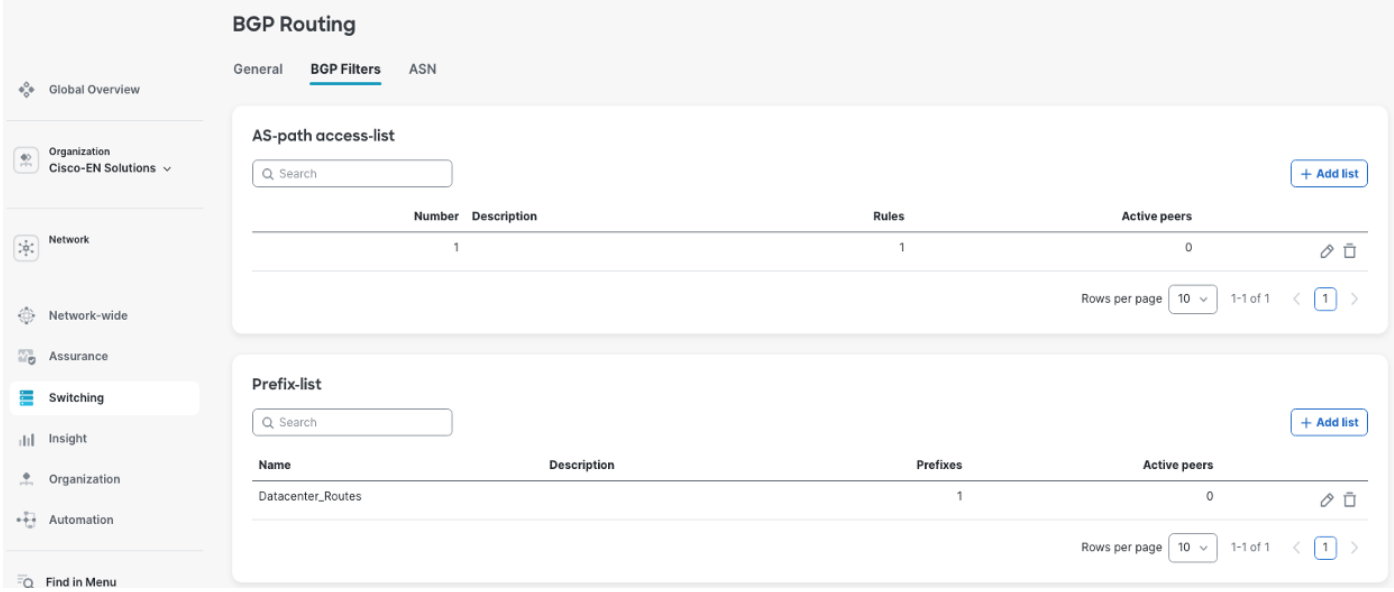
ルートアドバタイズメントおよび BGP 機能

BGP スイッチング機能

Catalyst スイッチ用 Cisco Meraki ダッシュボードの BGP 実装では、データセンター インフラストラクチャへのキャンパス ネットワーク プレフィックスのルートアドバタイズメントと、キャンパスコアに戻るデータセンター サービス ネットワークのルート受信がサポートされます。BGP プレフィックスリストとルートフィルタによって、BGP ネイバーにアドバタイズされる、または BGP ネイバーから受け入れられるルートが制御され、ルーティングループや不正なルートインジェクションが防止されます。プレフィックスリストでは、許可または拒否される特定の IP アドレス範囲が定義されます。これに対し、ルートマップでは、AS パス、コミュニティタグ、ルートメトリックを含む追加のフィルタリング基準が適用されます。このメカニズムにより、正当な承認されたルートのみがネットワークを伝播するため、設定不備、ルートハイジャック、および意図しないトラフィックのリダイレクトから保護されます。同時に、キャンパスからデータセンターへの BGP ピアリングセッション全体で、ルーティングポリシーの適用に関する詳細な制御が維持されます。

手順 9。 AS パスアクセスリストおよびプレフィックスリストを作成するには、次の手順を実行します。

[スイッチング（Switching）] > [BGP ルーティング（BGP Routing）] > [BGP フィルタ（BGP Filters）] の順に選択します。



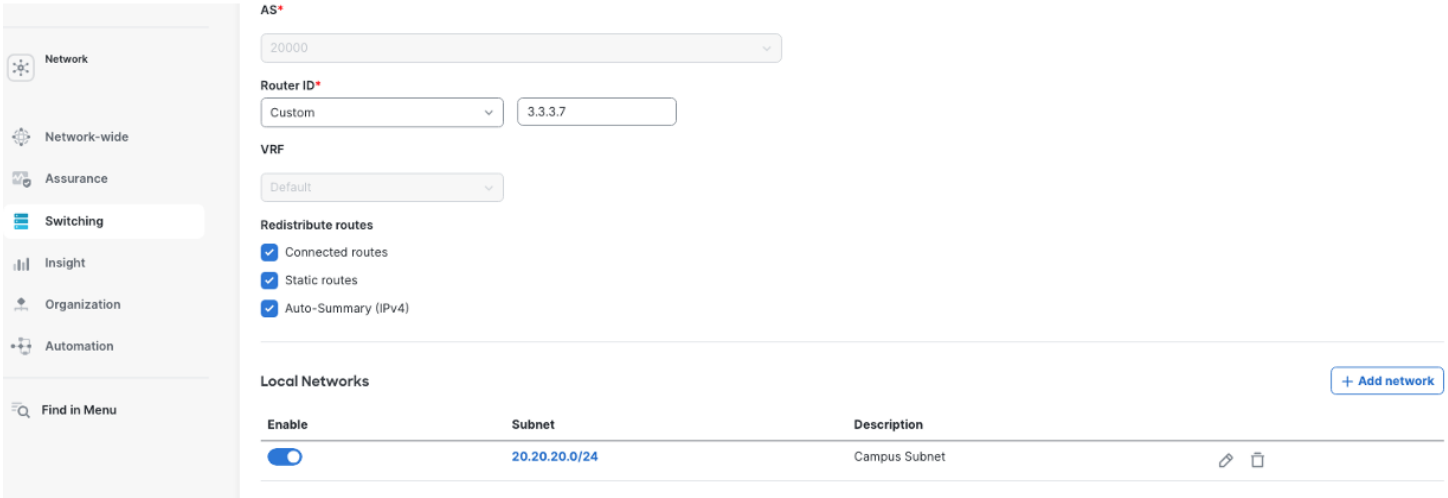
これらのフィルタは、[スイッチング（Switching）] > [BGP ルーティング（BGP Routing）] > [一般（General] > [BGP ルータ（BGP Routers）] > [BGP ピアグループ（BGP Peer Groups）] > [ピアグループ設定（Peer Group Settings）] で BGP ピアグループにアタッチされます。

ネットワーク アドバタイズメントの設定

ダッシュボードを使用して、キャンパスネットワークのネットワーク アドバタイズメントを設定できます。BGP を使用してデータセンターと共有するローカルサブネット（従業員ネットワーク、ゲスト Wi-Fi、管理ネットワークなど）を選択する必要があります。BGP セットアップでは、直接接続されたネットワーク、静的ルート、および結合されたネットワーク範囲をアドバタイズできます。このアプローチにより、セキュリティとネットワークの分離を維持しながら、データセンターがアクセスできるキャンパスリソースを柔軟に制御できます。

手順 10。アドバタイズされるローカルサブネットを設定するには、次の手順を実行します。

[スイッチング（Switching）] > [BGP ルーティング（BGP Routing）] > [BGP ルータ（BGP Router）] の順に選択します。



SD-WAN ハブモードで展開されたキャンパス Meraki MX は、Catalyst 9500 コラプストコアスイッチと eBGP または iBGP ピアリングを確立して、ダイナミックルート交換を有効にします。9500 SVI と Meraki MX 間でピアリングが成功すると、キャンパスルート（9500 で定義された SVI）が、BGP によって学習された Meraki

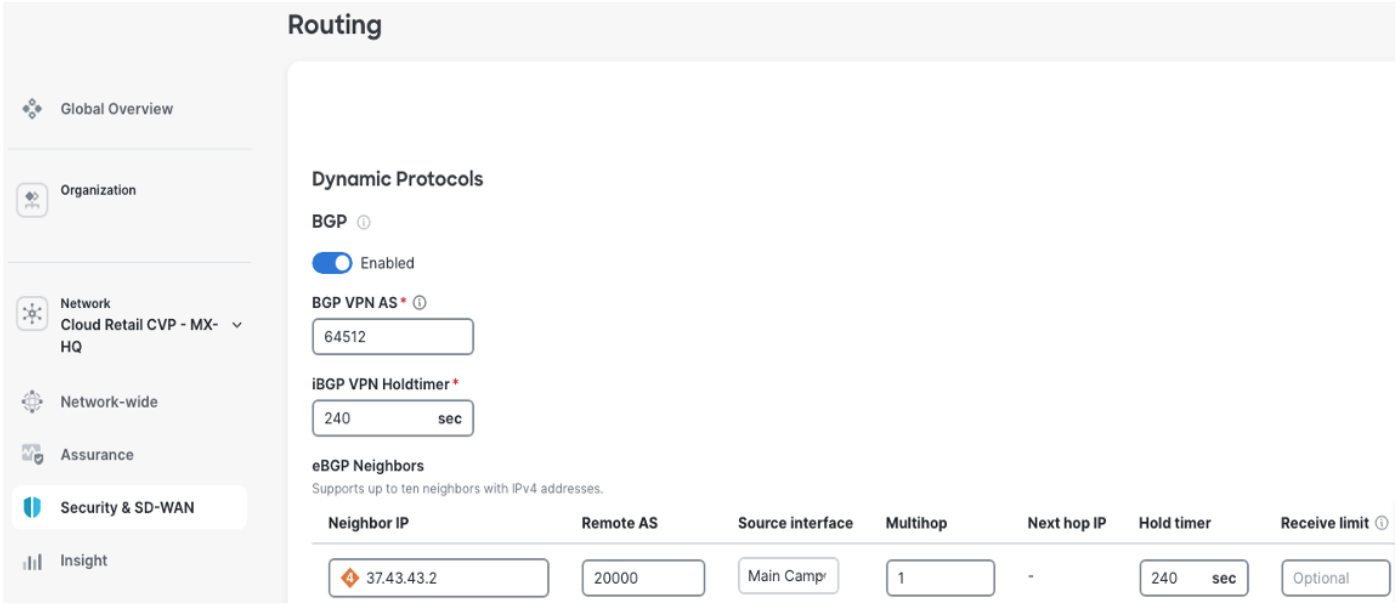
MX ルーティングテーブルに表示されます。同様に、データセンタールートは 9500 ルーティングテーブルに表示されます。このとき、これらのルートは、Meraki AutoVPN オーバーレイを介した iBGP を通じて、データセンター Meraki MX（同じく SD-WAN ハブモードで展開）からキャンパス Meraki MX によって学習され、その後、BGP ピアリングを介して 9500 に自動的に再配布されます。

Meraki MX BGP 実装の詳細な設定ガイダンスについては、Meraki の公式ドキュメント「Border Gateway Protocol (BGP)」を参照してください。

手順 11。 9500 コアへのキャンパス MX BGP ネイバーシップを設定するには、次の手順を実行します。

ステップ 1. [セキュリティおよび SD-WAN（Security & SD-WAN）] > [設定（Configure）] > [ルーティング（Routing）] の順に選択します。

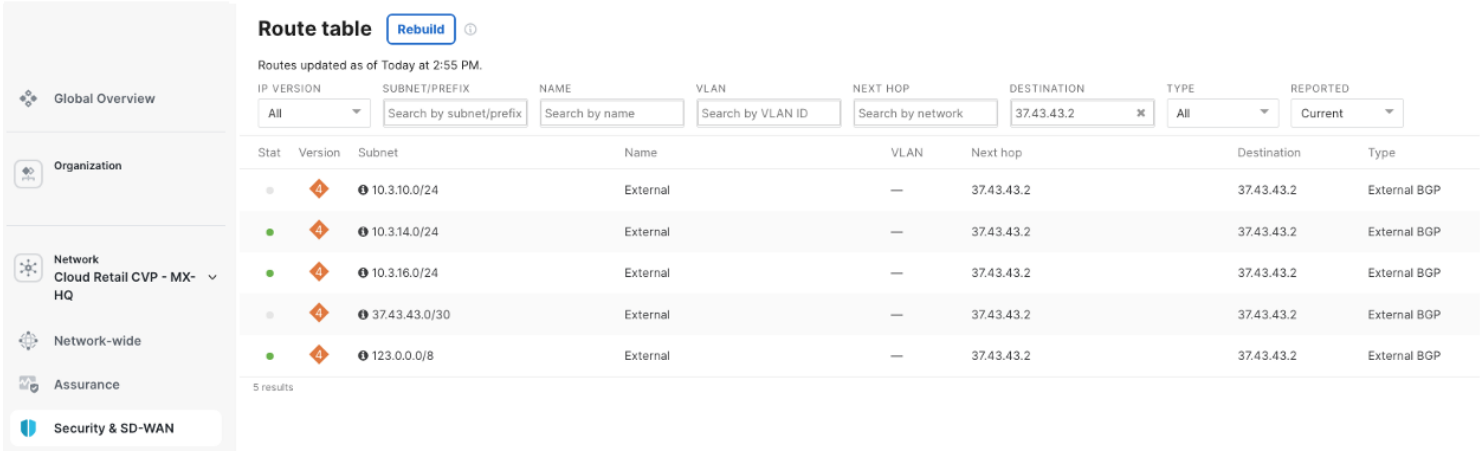
ステップ 2. iBGP を使用する場合は、MX ルーティング側で [トランジットを許可（Allow transit）] を選択して、データセンタールートを MX から 9500 に送信できるようにします。



手順 12。 キャンパス MX ルーティングテーブルを確認するには、次の手順を実行します。

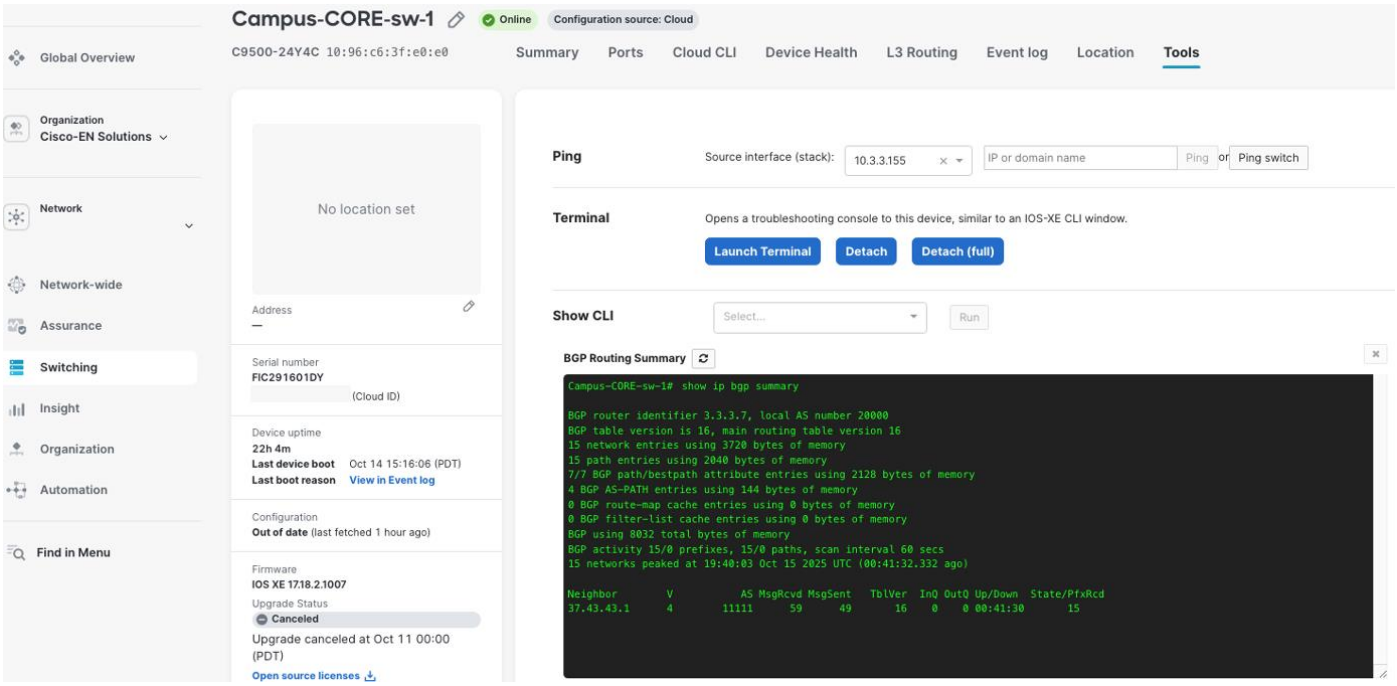
ステップ 1. [セキュリティおよび SD-WAN（Security & SD-WAN）] > [モニター（Monitor）] > [ルートテーブル（Route table）] の順に選択します。

ステップ 2. 9500 コア BGP ネイバーシップから受信したキャンパスルートを表示します。



Cisco 9500 スイッチでは、Cisco Meraki ダッシュボードの「端末ツール」を使用して、BGP 接続、ネイバー状態、ルートアドバタイズメント、およびネットワーク コンバージェンス イベントのステータスを確認できます。このツールでは、コマンドラインにアクセスして **show ip bgp summary**、`show ip bgp neighbors`、および `show ip route bgp` などのコマンドを実行できるため、これらの詳細情報をリアルタイムで確認できます。ダッシュボード インターフェイスから直接 BGP をモニターしてトラブルシュートするのに便利です。

「CLI の表示」ツールでも、この例に示すような BGP 状態に関する情報が提供されます。



冗長性とハイアベイラビリティ

ディストリビューション層およびアクセス層の設計に複数の冗長性メカニズムを導入することで、小売本社の事業の継続性が確保されます。

リンク レベルの冗長性

すべてのアップリンクで EtherChannel（LACP）設定を使用することで、帯域幅集約と自動フェールオーバー機能の両方が提供され、障害発生時にトラフィックが残りのリンクに自動的に再配布されます。

デバイス レベルの冗長性

ディストリビューション層の StackWise Virtual ペアとアクセス層の StackWise スタックにより、シングルポイント障害が解消され、デバイス障害が検出されてから数秒以内に自動フェールオーバーが発生します。

パス レベルの冗長性

デュアルホーム アクセス スイッチは、両方のディストリビューション スイッチへの接続を維持するため、ディストリビューション スイッチのメンテナンス中または障害発生中にも継続的な動作が保証されます。

電源の冗長性

ディストリビューション スイッチは、別の電気回路に接続されたデュアル電源モジュールを使用するため、電源の障害や電気回路の障害から保護されます。

共通エンタープライズ サービス アクセス用データセンター接続

小売キャンパスコア層では、Meraki SD-WAN を介して、企業のデータセンター インフラストラクチャへの高性能でレジリエンスの高い接続が確立されます。小売アーキテクチャには、階層型ハブアンドハブトポロジ、データセンター MX VPN ハブ、およびキャンパス MX VPN ハブが実装されます。

データセンター MX ハブは、中央集約ポイントとして機能し、ISE と統合して一元化された 802.1X 認証とネットワーク アクセス コントロールを提供すると同時に、DHCP、DNS、Active Directory などのコア企業サービス、およびインベントリ管理や支払い処理システムなどのビジネスに不可欠なアプリケーションをホストします。

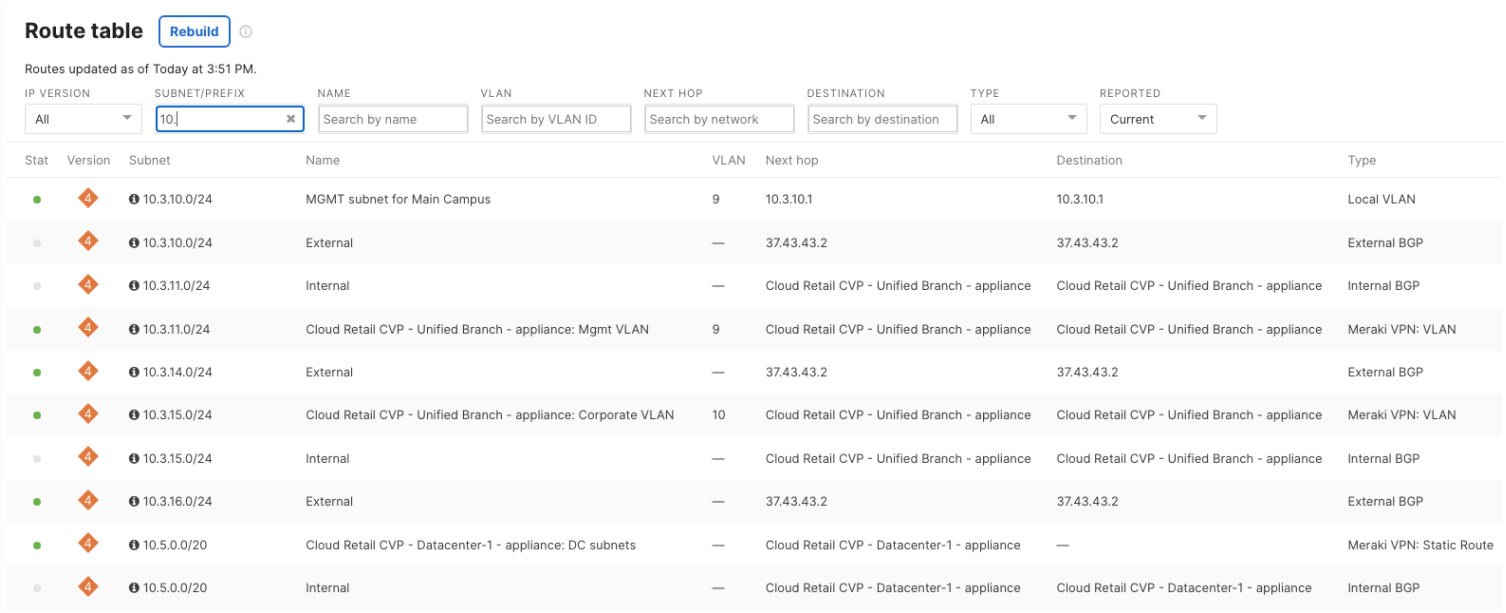
キャンパス MX ハブは、ローカル キャンパス スイッチングとワイヤレス インフラストラクチャを集約し、データセンターハブと小売店舗ブランチの両方への AutoVPN 接続を確立します。

SD-WAN アーキテクチャが提供するインテリジェント トラフィック ルーティングでは、ISE 認証および内部アプリケーション用の重要な企業トラフィックが AutoVPN トンネルを通過してデータセンターハブに向かう一方、SaaS およびインターネットバウンド トラフィックはローカルブレークアウトを使用するか、最適なパフォーマンスを確保するためにキャンパスハブを通ってルーティングされます。これについては、「Meraki SD-WAN 展開」セクションで詳しく説明しています。

手順 13。 キャンパス MX ルーティングテーブルを確認するには、次の手順を実行します。

ステップ 1. キャンパスネットワークのダッシュボードで、[セキュリティおよび SD-WAN（Security & SD-WAN）] > [モニター（Monitor）] > [ルートテーブル（Route table）] の順に選択します。

ステップ 2. 9500 コア eBGP ネイバーシップから受信したキャンパスルート、DC MX ハブから（iBGP を介して）受信したデータセンタールート、およびスポーク MX から受信した小売ブランチルートを確認します。



企業ワイヤレス展開

小売本社のワイヤレス インフラストラクチャは、企業の従業員、経営陣、会議施設、およびキャンパス環境全体をサポートするエンタープライズクラスの接続を提供します。この展開では、高度なセキュリティ、QoS、および一元化された認証機能を備えた Wi-Fi 7 テクノロジーを活用することで、Cisco Meraki プラットフォームの簡素化されたクラウド管理という利点を維持しながら、ビジネスに不可欠なワイヤレスアプリケーションに優れたパフォーマンスとユーザー体験を提供します。

Cisco Meraki ダッシュボードへの AP のオンボーディング

初回デバイス登録

Meraki MR AP は、クラウド管理接続を確立し、展開用のデバイスを準備する合理化された要求プロセスによって、Cisco Meraki ダッシュボードにオンボーディングされます。

手順 14。 Meraki MR AP をオンボーディングするには、次の手順を実行します。

ステップ 1. [組織（Organization）] > [設定（Configure）] > [インベントリ（Inventory）] ページに移動します。

ステップ 2. 個別に、または CSV の一括アップロードを使用して、アクセスポイントのシリアル番号を追加します。

ステップ 3. デバイスを組織に関連付けます。

ステップ 4. デバイスをネットワーク割り当て可能な状態にします。

ステップ 5. 所有権を確立し、クラウド管理機能を有効にするため、ダッシュボードを使用して、各 AP の一意のシリアル番号と要求コード（デバイスラベルに印刷されています）を入力します。

組織のインベントリに要求されると、AP は初期セットアップ中に作成された企業のキャンパスネットワーク構造に割り当てられます。

ステップ 6. [組織（Organization）] > [インベントリ（Inventory）] に移動します。

ステップ 7. 適切なキャンパスネットワークにデバイスを割り当てるには、要求された AP を選択して、[ネットワークに追加（Add to network）] を選択します。

この割り当てにより、AP がキャンパス スイッチング インフラストラクチャ、VLAN 設定、および本社運営用に定義されたワイヤレスポリシーにリンクされ、ワイヤレス展開全体で一貫した動作と一元化された管理が保証されます。

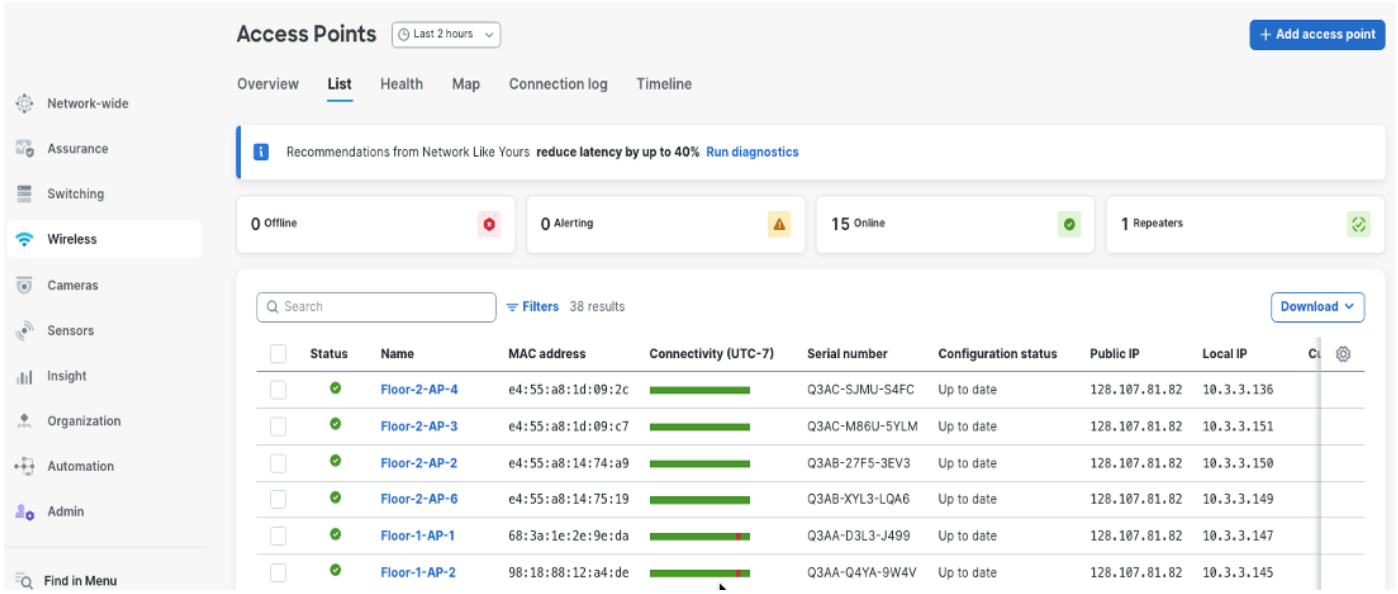
同じ AP で複数の SSID をブロードキャストする場合、AP を接続するスイッチポートの設定が異なります。

複数の SSID の場合、スイッチポートはトランクモードとする必要があります。トランクポートのネイティブ VLAN は、AP が管理 IP アドレスを取得する VLAN です。トランクポート上の [許可された VLAN（Allowed VLAN）] は、SSID が使用する VLAN に対応します。

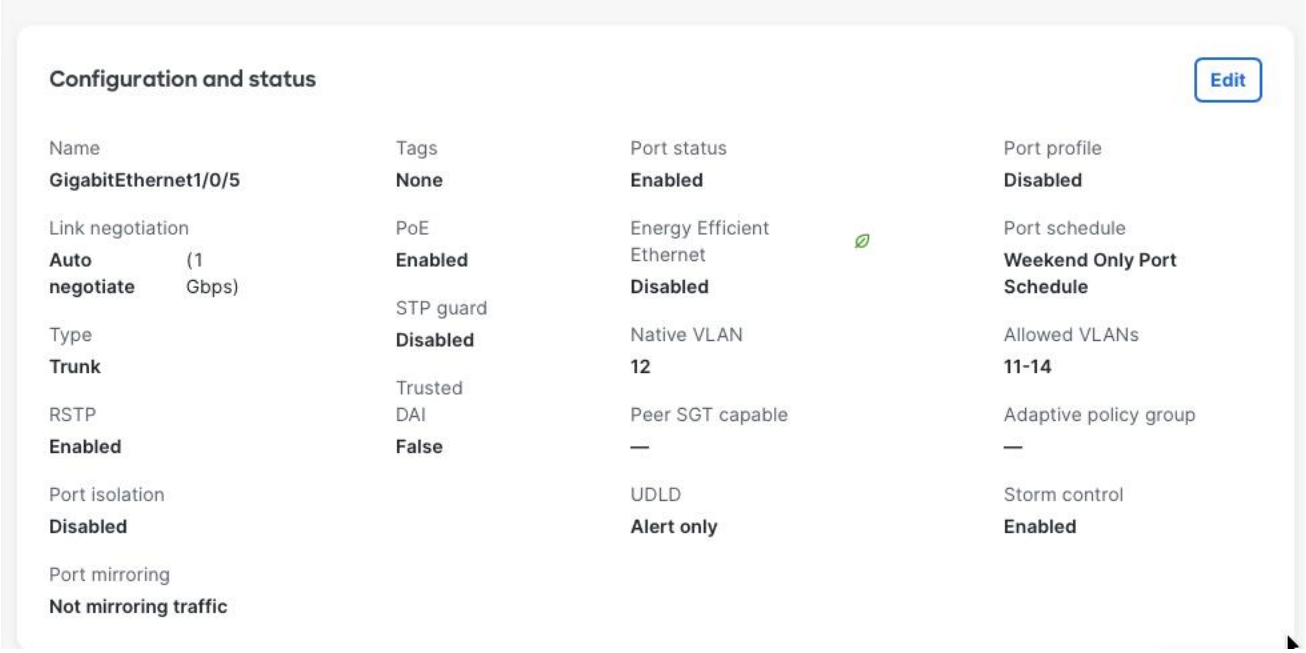
ゼロタッチプロビジョニングの場合、ネットワーク割り当て AP は、ネットワークに接続され電源が投入されると、Cisco Meraki クラウド インフラストラクチャから自動的に設定をダウンロードします。ダッシュボード インターフェイスには、クラウドに接続されたデバイスを示すリアルタイムのオンボーディングステータスが表示されます。

ステップ 8. 必要に応じてファームウェアの更新をダウンロードし、動作ステータスに移行します。

ステップ 9. [ネットワーク全体（Network-wide）] > [モニター（Monitor）] > [アクセスポイント（Access Points）] でデバイスのステータス、ファームウェアバージョン、および接続の正常性を表示して、ゼロタッチプロビジョニングをモニターできます。



ステップ 10. すべての AP が適切にオンボーディングされていて、ワイヤレスサービス展開の準備ができていることを確認します。



企業本社への Wi-Fi 展開

小売本社のワイヤレス インフラストラクチャは、キャンパス環境全体で企業の従業員、経営陣、会議施設、および業務エリアをサポートするエンタープライズクラスの接続を提供し、ビジネスに不可欠なワイヤレス アプリケーションに優れたパフォーマンスとユーザー体験を提供すると同時に、Cisco Meraki プラットフォームを介したクラウド管理の簡素化を維持します。

企業およびゲスト Wi-Fi の導入

企業 SSID は、802.1X/RADIUS 認証を使用して WPA3-Enterprise を実装し、本社のインフラストラクチャから一元化された DHCP を使用してクライアントを企業 VLAN（VLAN 11）に割り当て、フル ネットワーク リソース アクセスを提供し、ビジネストラフィックを優先するアプリケーションベースの QoS を適用します。ゲスト SSID は、キャプティブポータル認証を使用し、MR AP によって直接提供される DHCP サービスを使用し

てローカルブリッジモードで動作し、インターネット専用アクセスを使用してクライアントをゲスト VLAN（VLAN 13）に隔離し、帯域幅制限（クライアントあたり 5 Mbps）を導入し、クライアント間通信をブロックします。これにより、完全なネットワークのセグメンテーションと企業リソースからのセキュリティ隔離が保証されます。

後続のセクションでは、企業用とゲスト用の両方に向けた Wi-Fi のさまざまな側面について説明します。

セキュリティに関する考慮事項

企業ワイヤレスネットワークとゲスト ワイヤレス ネットワークには、異なる使用パターンを反映した異なるセキュリティアーキテクチャが必要です。企業の SSID は通常、WPA2-Enterprise または WPA3-Enterprise を導入して、組織のデバイスおよびユーザーに強力な認証と暗号化を提供します。WPA2-Enterprise は、AES-CCMP 暗号化による 802.1X 認証を使用しており、後方互換性を必要とするレガシーデバイスをサポートするために今でも広範に展開されています。WPA3-Enterprise では、802.1X/EAP 認証が引き続き使用されますが、必須の保護管理フレーム（PMF）、暗号化アルゴリズムの強化、および AES-GCMP-256 および SHA-384 を使用した 192 ビットのセキュリティモードのサポートによってセキュリティを強化しています。EAP-TLS などの証明書ベースの EAP 方式とペアリングすると、WPA3-Enterprise は前方秘匿性を提供し、ログイン情報の侵害に対する対策を強化できます。組織は、WPA2 と WPA3 対応クライアントの両方をサポートするために、WPA2/WPA3 混合構成または移行構成を展開することができます。これにより、さまざまな企業のエンドポイントユーザー間で互換性を維持しながら、段階的なモダナイゼーションが可能になります。

802.1X 認証

企業 SSID では dot1x が使用されます。これは、ユーザーまたはデバイスがネットワークにアクセスする前にログイン情報を提供する必要があり、そのログイン情報が中央の RADIUS サーバーに対してチェックされることを意味します。

手順 15。 802.1X 認証を設定するには、次の手順を実行します。

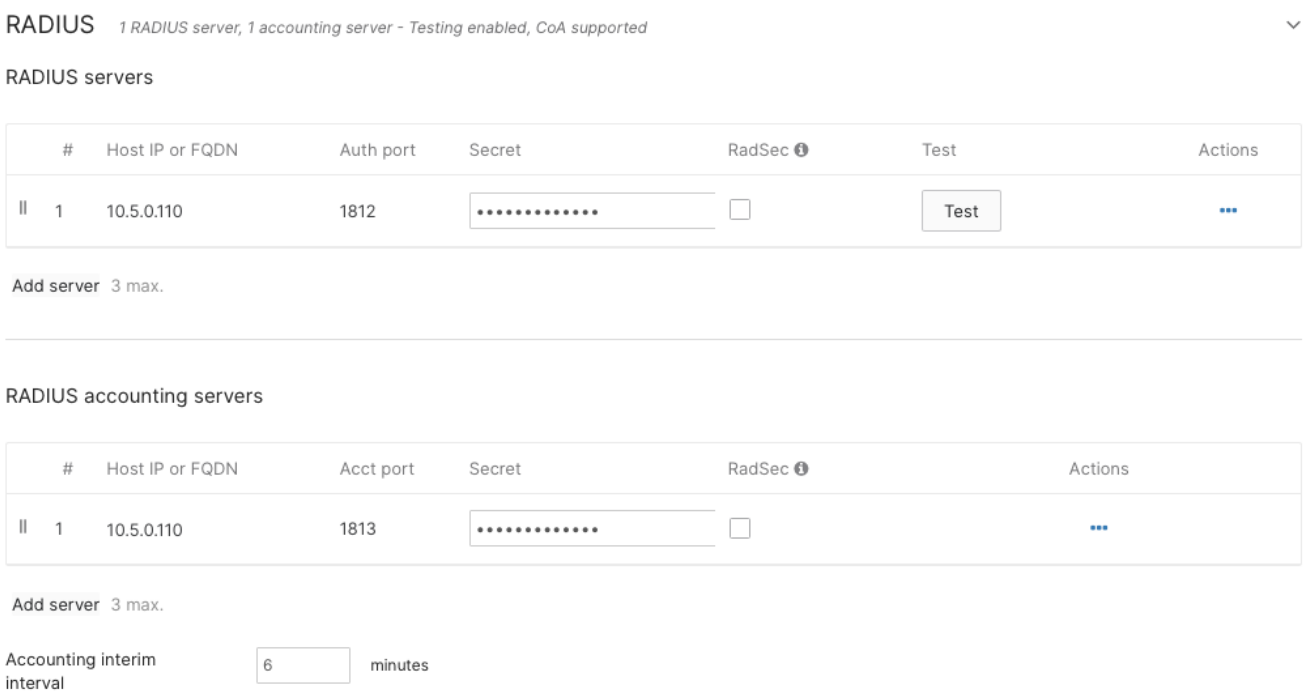
ステップ 1. ダッシュボードで [ワイヤレス（Wireless）] > [設定（Configure）] > [アクセス制御（Access Control）] ページに移動します。

ステップ 2. [セキュリティ（Security）] 設定で、[マイ RADIUS サーバーを使用する企業（Enterprise with my RADIUS server）] を選択します。

ステップ 3. このページの [RADIUS] セクションに RADIUS サーバーの詳細を追加するか、組織レベルで設定します。セットアップに応じて、Meraki 認証または外部 RADIUS サーバーを使用できます。

ステップ 4. 小売本社の場合は、Cisco ISE サーバーの IP アドレスを入力し、セキュア通信用に共有秘密を設定して、認証ポート（通常は認証用に UDP 1812、アカウンティング用に UDP 1813）を指定します。

このセットアップにより、承認されたユーザーまたはデバイスのみが企業の Wi-Fi ネットワークに参加できます。



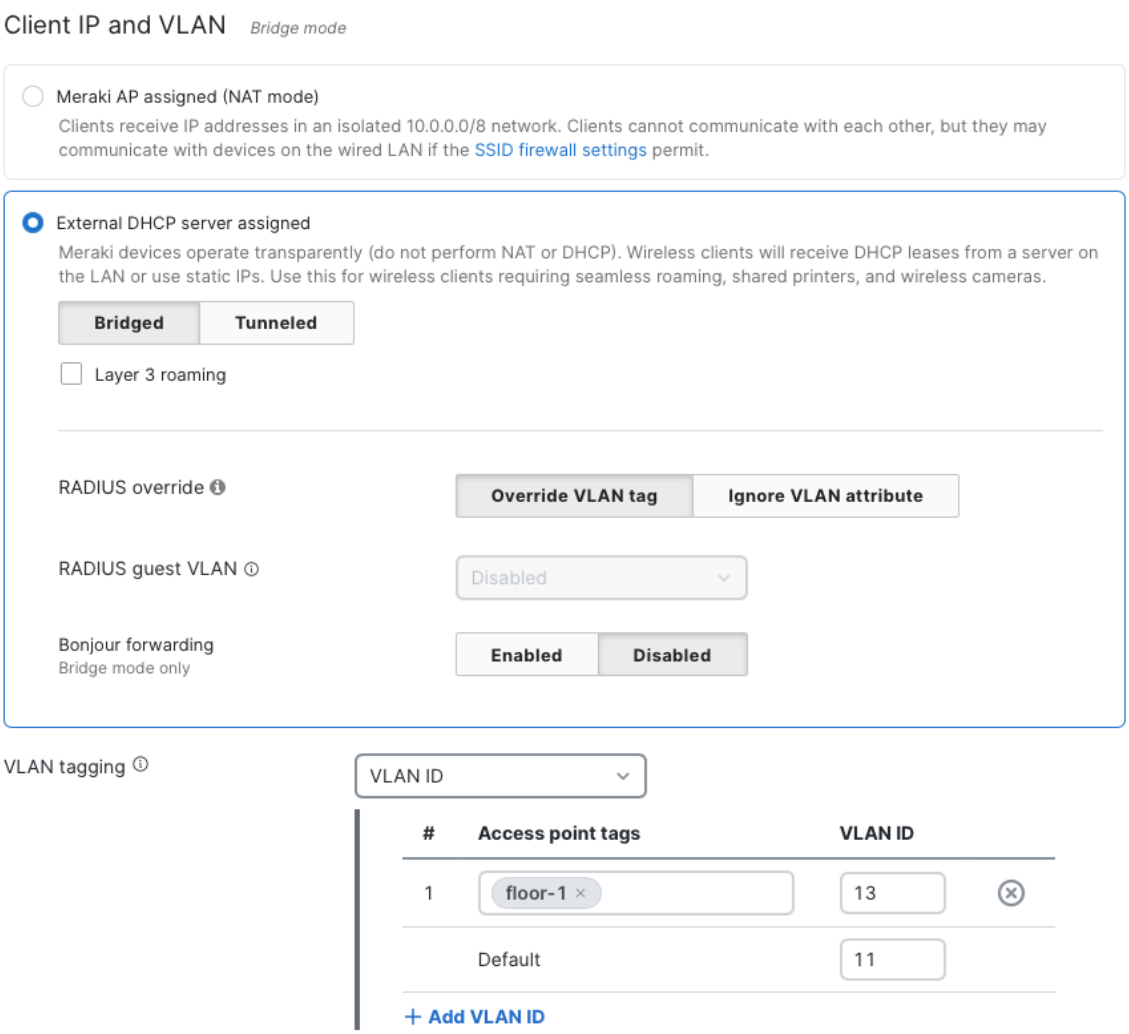
クライアント DHCP とネットワークの割り当て

VLAN 割り当て

ネットワークのセグメンテーションとポリシーが正しく機能するようにするには、VLAN タギングを使用するように企業の SSID を設定する必要があります。[クライアント IP および VLAN（Client IP and VLAN）] 設定で、この SSID のワイヤレスクライアントを企業のネットワーク VLAN（VLAN 10）に割り当てます。

企業のワイヤレスクライアントの場合は、外部 DHCP サーバーを使用するオプションを選択します。これは、ワイヤレスデバイスが AP またはワイヤレスコントローラ上のローカル DHCP サービスからではなく、キャンパスコアまたはデータセンターの中央 DHCP サーバーから IP アドレスを取得することを意味します。

アクセスポイントタグに基づいて特定の VLAN を割り当てる場合は、[ワイヤレス（Wireless）] > [設定（Configure）] > [アクセス制御（Access Control）] の [VLAN タギング（VLAN tagging）] セクションを使用することもできます。このセットアップは、異なる AP で同じ SSID をブロードキャストする必要があるが、異なるサブネットから IP アドレスを取得するためにクライアントを異なる AP グループに接続したい場合に役立ちます。VLAN ID は有線クライアントとワイヤレスクライアント間で同じであるため、ワイヤレスユーザーはアクセス層スイッチを介して接続された有線企業ユーザーと同じネットワークアクセスおよびセキュリティポリシーを受信できます。この設定は、RADIUS 属性によるダイナミック VLAN 割り当てをサポートし、ユーザーまたはグループ固有の VLAN 配置を可能にします。これにより、経営陣ユーザーをネットワーク権限が強化された個別の VLAN に割り当て、標準の従業員は一般的な企業 VLAN に接続することができます。



ゲスト SSID はオープン認証を使用するため、ユーザーはパスワードなしで接続できます。ただし、アクセスする前に、キャプティブポータルを経由してサービス利用条件に同意する必要があります。この方法はセキュリティと利便性を両立させます。アカウンタビリティのために基本的なユーザー情報は収集しますが、ゲスト、訪問者、または請負業者がアカウントを持ったり、複雑なログイン手順を実行したりする必要はありません。

ゲストネットワーク IP アドレスには、Meraki AP による割り当て（NAT モード）またはローカル MX DHCP を使用できます。

ファイアウォールおよび通信シェーピング

企業ネットワーク

本社リソース、データ センター アプリケーション、およびインターネット接続先への企業 VLAN（VLAN 11）アクセスを許可するレイヤ 3 ファイアウォールルールを導入します。ビジネスに不可欠なアプリケーションを優先するアプリケーション認識型トラフィックシェーピングを使用して、VoIP とビデオ会議には最も高い優先順位を置き、コラボレーションツールや Web ブラウジングには中程度の優先順位、一括ダウンロードには低い優先順位を置くことで、時間的制約のある企業の通信に最適なパフォーマンスを提供します。アプリケーションごとの帯域幅保証と DSCP マーキングを設定し、キャンパス インフラストラクチャ全体でエンドツーエンドの QoS を維持します。

ゲスト ネットワーク

ゲスト VLAN（VLAN 13）上のデバイスのみがインターネットにアクセスできるように、厳密なファイアウォールルールを設定します。会社のリソース、内部ネットワーク、およびその他の VLAN へのすべてのアクセスをブロックして、信頼できないデバイスから組織のデータを保護します。

各ゲストのインターネット速度を、ダウンロードの場合は 5 Mbps、アップロードの場合は 2 Mbps に制限します。これにより、特定のゲストが過剰な帯域幅を使用することがなくなります。また、ピアツーピアのファイル共有、VPN 接続をブロックし、ストリーミングサービスの優先順位を下げます。これにより、ビジネスニーズに対応するための十分な帯域幅を確保しながら、ゲストが Web を参照したり、電子メールをチェックしたりできるようになります。

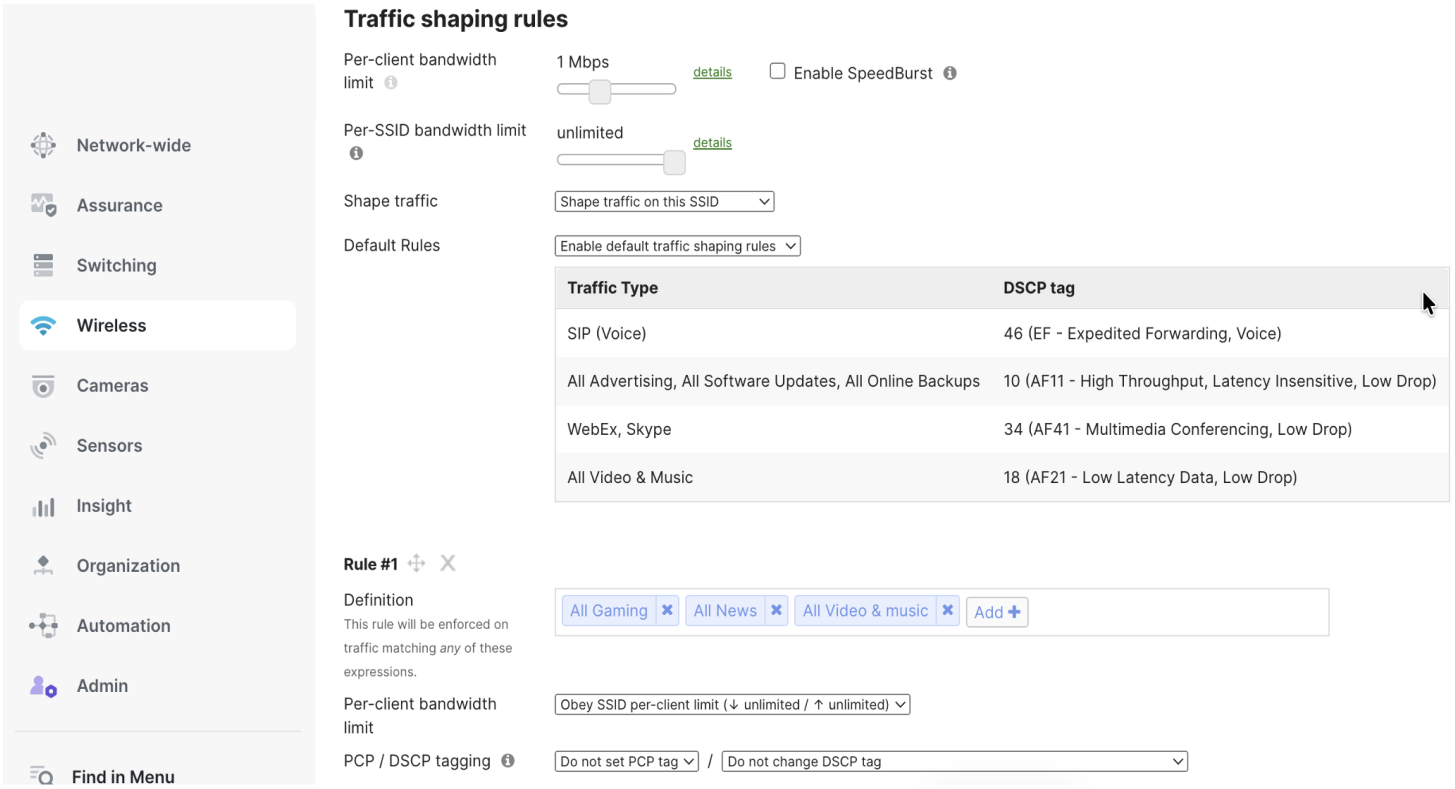
設定するには、[ワイヤレス（Wireless）] > [ファイアウォールおよび通信シェーピング（Firewall & Traffic Shaping）] の順に選択し、保護する SSID を選択して、レイヤ 3 およびレイヤ 7 のファイアウォールルールを追加します。

ファイアウォールルールは、説明にあるとおり SSID レベルで適用するか、または、[セキュリティおよび SD-WAN（Security & SD-WAN）] > [設定（Configure）] > [ファイアウォール（Firewall）] の順に選択し、[レイヤ 3（Layer 3）] > [アウトバウンドルール（Outbound rules）] でルールを追加することで、MX 次世代ファイアウォールに適用できます。

クライアントごとの帯域幅の制限

ユーザーごとの帯域幅制限を設定して、特定のユーザーがワイヤレスネットワークの容量を使い切ることがないようにします。これにより、すべての従業員がネットワークを公正に共有できます。たとえば、各デバイスを、ダウンロードの場合は最大 100 Mbps、アップロードの場合は 50 Mbps に設定できます。これはほとんどの作業タスクで十分ですが、バックアップ、大容量ファイルのダウンロード、ストリーミングなどによって同じエリア内の他のユーザーのネットワークに遅延が発生するのを防ぎます。

これらの制限は、[ワイヤレス（Wireless）]、[ファイアウォールおよび通信シェーピング（Firewall & Traffic Shaping）]、[クライアントごとの帯域幅制限（Per-client bandwidth limit）] の順に選択して設定できます。ネットワークを使用する人数と、キャンパスのさまざまな部分にある各アクセスポイントのキャパシティに基づいて、制限を調整できます。



認証後のワイヤレスクライアントは企業 SSID に配置されます。クライアントは、[ネットワーク全体（Network-wide）] > [クライアント（Clients）] で確認できます。

Meraki SD-WAN 展開

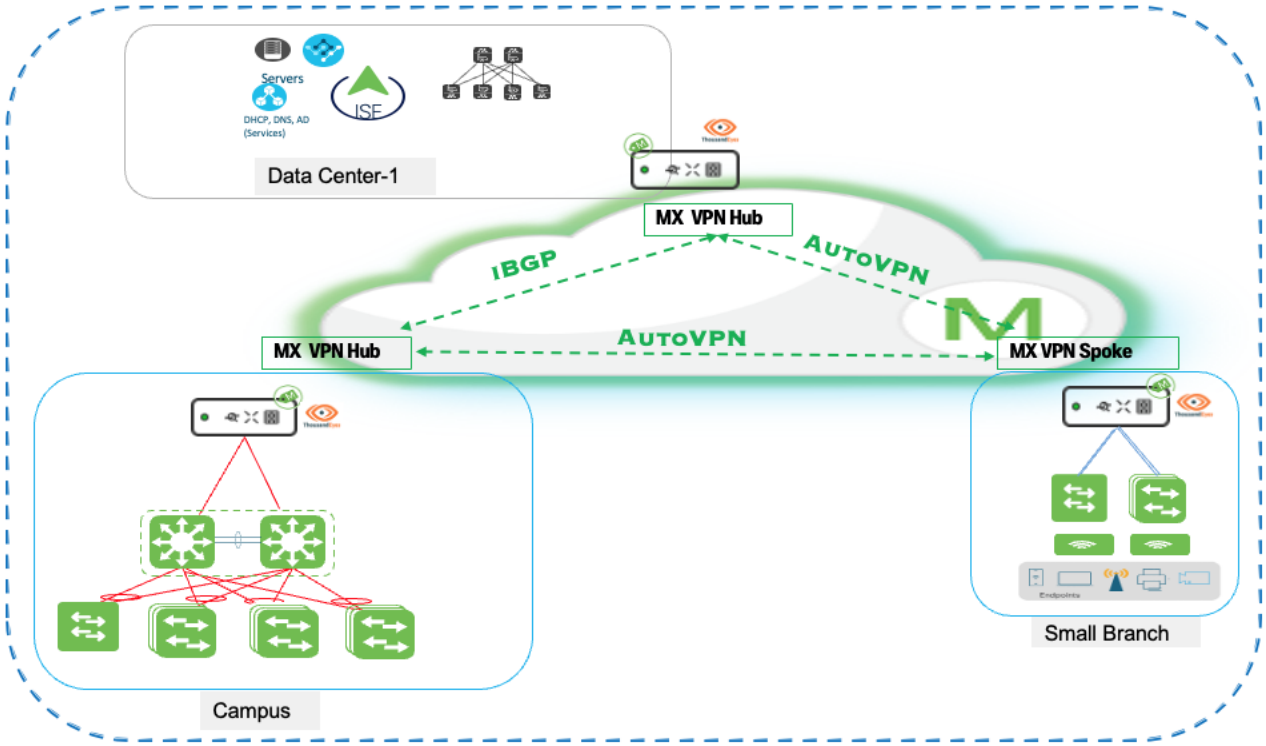
小売ネットワーク インフラストラクチャでは、Meraki SD-WAN の機能を利用して、企業本社キャンパスと小売企業全体の分散した店舗ロケーションの間に、セキュアでパフォーマンスの高い接続を確立します。この SD-WAN アーキテクチャは、インテリジェントパスの選択、アプリケーション認識型ルーティング、および自動フェールオーバー機能を導入し、POS、インベントリ管理、企業コミュニケーション、および一元化されたビジネスサービスなどのミッションクリティカルな小売アプリケーションの事業継続性を保証します。

キャンパスからデータセンターへの通信

小売キャンパスコア層では、Meraki SD-WAN を介して、企業のデータセンター インフラストラクチャへの高性能でレジリエンスの高い接続が確立されます。小売アーキテクチャでは、データセンターの MX VPN ハブ、キャンパス MX VPN ハブ、および MX VPN スポークとしての分散ブランチという 3 つの階層が含まれる階層型ハブアンドスポーク トポロジを実装します。データセンターハブは、中央集約ポイントとして機能し、ISE と統合して一元化された 802.1X 認証とネットワーク アクセス コントロールを提供すると同時に、DHCP、DNS、Active Directory などのコア企業サービス、およびインベントリ管理や支払い処理システムなどのビジネスに不可欠なアプリケーションをホストします。

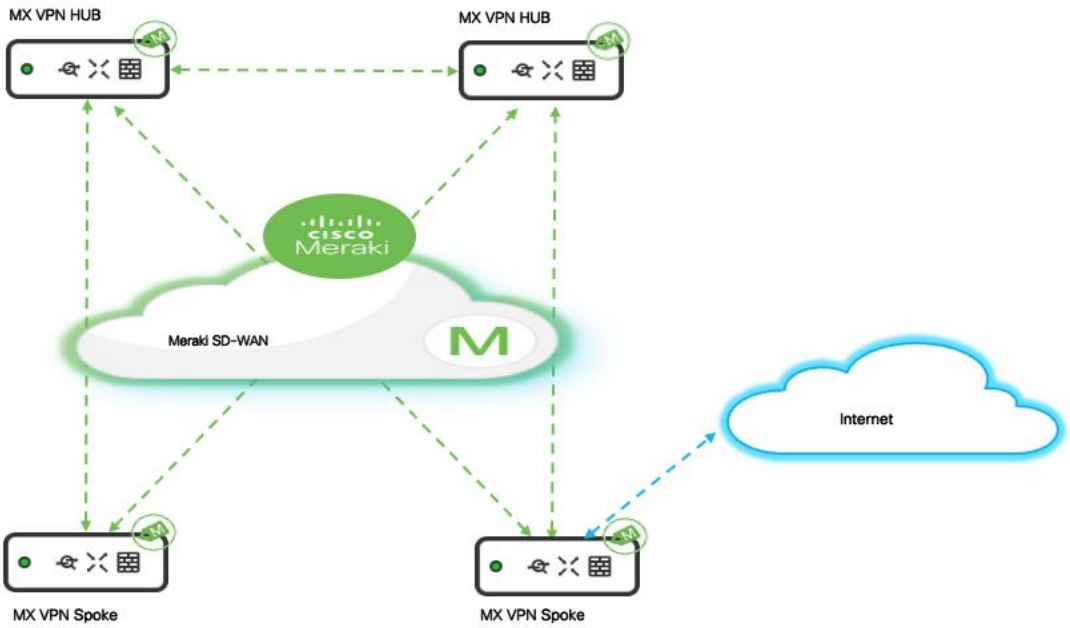
キャンパス MX ハブは、ローカル キャンパス スイッチングとワイヤレス インフラストラクチャを集約し、データセンターハブと小売店舗ブランチの両方への AutoVPN 接続を確立します。ブランチロケーションでは、AutoVPN トンネルを確立するように設定された MX スポークアプライアンスが両方のハブロケーションに展開され、レジリエンスの高いマルチハブトポロジが作成されます。この設計により、ブランチスポークは、クラウド接続とインターネット接続用の最適化されたパスを維持しながら、企業サービスや認証用のデータセンターリソースにアクセスできます。この 3 階層のハブアンドスポーク設計により、データセンターでのコアサービスの一元化された制御が提供されると共に、キャンパスハブおよび分散スポークアーキテクチャによる地理的な冗長性とアプリケーションのパフォーマンス最適化が提供されます。

2 つの MX アプライアンスの両方をハブモードに設定すると、ハブ間の AutoVPN ピアリングが確立され、ルーティング情報が双方向で自動的に交換されます。各ハブは、ローカルに設定されたサブネットと集約されたスポークルートをピアハブにアドバタイズすることで、トポロジ全体で完全な到達可能性を実現します。データセンターハブはキャンパスサブネットを学習し、キャンパスハブはデータセンターサブネットを学習し、両方のハブが完全なルートテーブルをそれぞれのスポークサイトに伝播します。このハブ間ルート交換により、手動によるルート再配布や静的ルート設定なしで、シームレスなルーティングドメインが作成されます。AutoVPN は、手動設定なしで、ルーティング情報をデータセンターハブ、キャンパスハブ、およびブランチスポーク間で自動的に交換します。各 MX は、ローカルに設定されたサブネットを接続されたハブにアドバタイズし、ハブはこれらのルートを参加しているすべてのスポークに伝播します。ブランチのスポークがデータセンターとキャンパスのネットワークを動的に学習し、AutoVPN メッシュを介して最適なパスを確立します。このゼロ設定のルート配布により、新しいブランチの展開時やトポロジ全体にネットワークの変更が発生したときに、自動接続が確保されます。



キャンパスからブランチへの通信

AutoVPN メッシュアーキテクチャ：Meraki SD-WAN は、本社とすべての店舗ロケーション間に AutoVPN メッシュ接続を確立し、小売ネットワーク全体で暗号化された通信を自動的に形成および維持するセキュアな IPsec VPN トンネルを作成します。キャンパス本社とデータセンターは、SD-WAN トポロジ内のハブとして機能し、MX セキュリティアプライアンスがネットワークエッジに展開されるため、VPN の集約、トラフィックの集約、および一元化されたポリシーの適用が可能になります。店舗ロケーションはスポークとして機能し、ローカル MX アプライアンスが本社ハブに戻る VPN トンネルを確立します。これにより、ゲスト Wi-Fi およびクラウド アプリケーション アクセス用のローカル インターネット ブレークアウト機能を維持しながら、ブランチから本社のトラフィックフローのセキュアな通信が可能になります。



ハブアンドスポークトポロジ

AutoVPN 展開では、大部分のトラフィックが店舗間の通信ではなく、個々の店舗と中央本社の間で流れる小売オペレーションに最適化された、ハブアンドスポークトポロジを使用します。

企業のキャンパス MX アプライアンスは、Cisco Meraki ダッシュボードで設定されます。

手順 16。 VPN コンセントレータとして設定するには、次の手順を実行します。

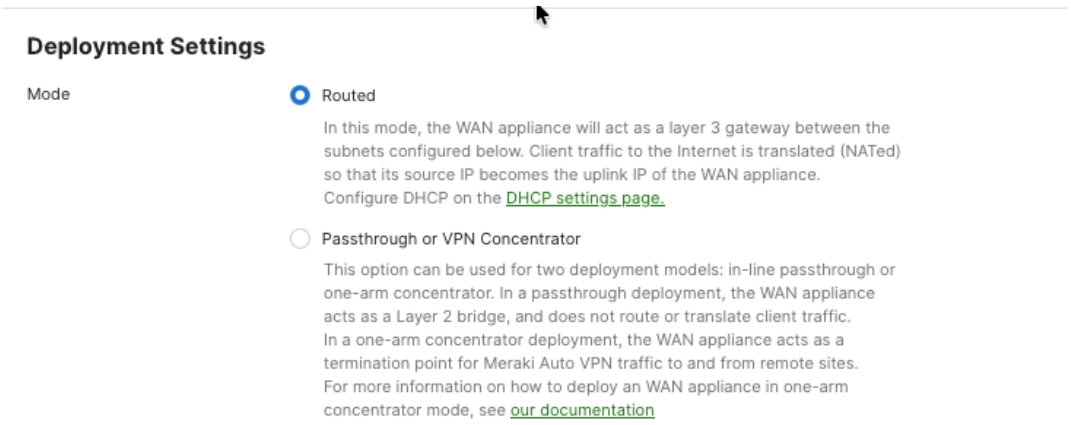
ステップ 1. [セキュリティおよび SD-WAN（Security & SD-WAN）] > [サイト間 VPN（Site-to-site VPN）] の順に選択します。

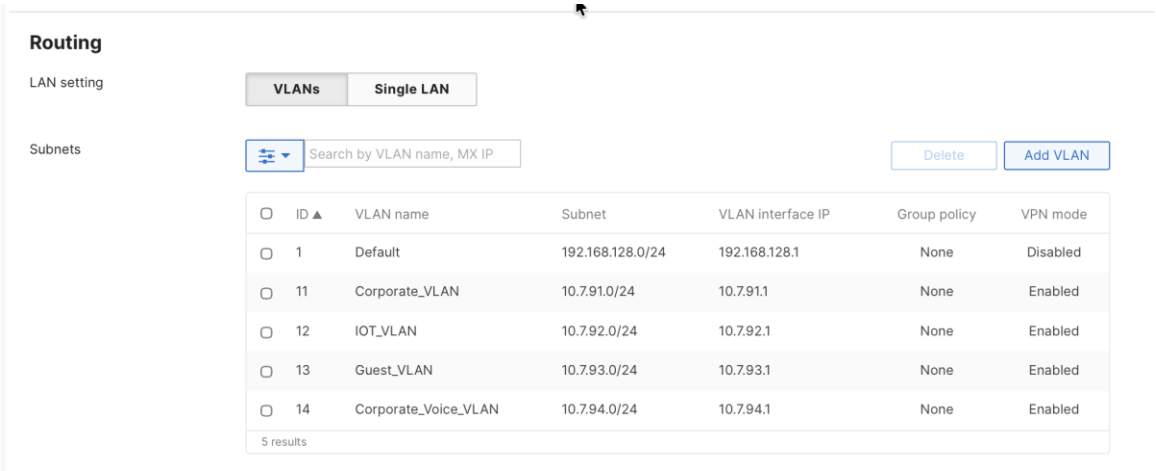
ステップ 2. ハブモードを有効にすると、これらのデバイスは数百のブランチロケーションからの VPN 接続を同時に受け入れることができます。

ブランチストアの MX アプライアンスはスポークモードで設定され、本社はハブ接続先として指定されます。この設定により、暗号化されたトンネルが自動的に確立され、VPN コンセントレータに登録されて、一元化管理とトラフィック転送が自動的に確立されます。ブランチ MX は、AutoVPN を介してブランチサブネットをアドバタイズする「ルーテッド展開」モードで設定されます。これが、企業キャンパスおよびデータセンターへの VPN トンネルを形成します。

手順 17。 MX 展開モードを選択し、AutoVPN へとアドバタイズする必要があるサブネットを選択するには、次の手順を実行します。

[セキュリティおよび SD-WAN（Security & SD-WAN）] > [アドレッシングおよび VLAN（Addressing & VLAN）] の順に選択します。





トンネルの自動確立

Cisco Meraki AutoVPN は、サイト間 VPN 展開で従来必要とされていた手動での IPsec 設定、事前共有キー配布、および複雑なルーティングプロトコルのセットアップを不要にすることで、サイト間 VPN 展開を簡素化しますが、管理者は引き続き Cisco Meraki ダッシュボードを使用して VPN トポロジを設定する必要があります。

手順 18。 ハブアンドスポークの関係を定義するには、次の手順を実行します。

ステップ 1. 各ネットワーク内で [セキュリティおよび SD-WAN（Security & SD-WAN）] > [サイト間 VPN（Site-to-site VPN）] の順に選択して、VPN ロールを設定します。

ステップ 2. [ハブ（Hub）] モードを選択して本社の MX アプライアンスを VPN ハブとして指定し、複数のブランチロケーションからの着信 VPN 接続を受け入れられるようにします。

店舗ロケーションの MX アプライアンスは、VPN スポークとして設定されます。

ステップ 3. [スポーク（Spoke）] モードを選択し、スポークがトンネルを確立するハブを、使用可能なハブリストから選択します。

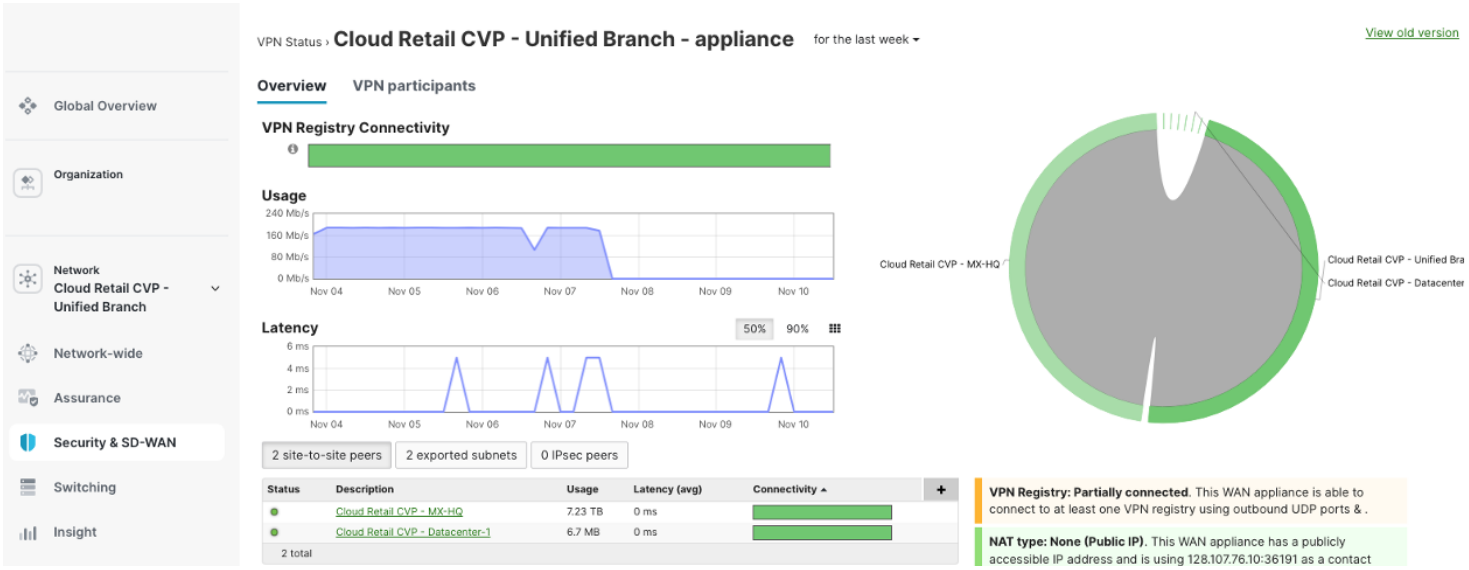
ダッシュボードを使用して VPN トポロジを定義した後で、ブランチ MX アプライアンスの電源をオンにしてインターネット接続を確立すると、トンネルが自動的に確立されます。スポークは、Cisco Meraki クラウドインフラストラクチャを介して指定されたハブを自動的に検出し、クラウド管理キーマテリアルを使用して暗号化されたトンネルの確立を開始し、定義されたルーティングとセキュリティポリシーに従ってトラフィックの転送を開始します。管理者は、IPsec パラメータの手動設定、事前共有キーの交換、各サイトでのトンネルネゴシエーションの問題をトラブルシュートする必要がありません。

このクラウドでオーケストレーションされた VPN プロビジョニングにより、従来の VPN ソリューションに比べて展開の複雑さが大幅に軽減され、管理者が複雑な IPsec 設定を実行する代わりに、ダッシュボードを介して VPN ロールとハブの選択を設定するだけで簡単にカスタマイズできます。ビジネス要件でロケーション固有の VPN アーキテクチャが必要な場合は、トンネル動作、フェールオーバーポリシー、およびサイトごとのトラフィックルーティングをカスタマイズする柔軟性が引き続き維持されます。

手順 19。 AutoVPN で MX のロールを設定するには、次の手順を実行します。

ステップ 1. [セキュリティおよび SD-WAN（Security & SD-WAN）] > [サイト間 VPN（Site-to-site VPN）] の順に選択します。

ステップ 2. [セキュリティおよび SD-WAN（Security & SD-WAN）] > [アドレッシングと VLAN（Addressing & VLANs）] > [VPN ステータスおよびルートテーブル（VPN Status and Route Table）] の順に選択して、サイトの AutoVPN とルーティングテーブルを表示します。



MX トンネルのスケーリングのガイドラインについては、「MX Sizing Guide and Principles」を参照してください。

トラフィックのルーティングと最適化

AutoVPN は、スマート トラフィック ルーティングを使用して、どのネットワークトラフィックがセキュア VPN トンネルを通ってメインオフィス（本社）に向かうか、およびどのトラフィックが各ブランチロケーションでローカルインターネット接続を使用するかを決定します。

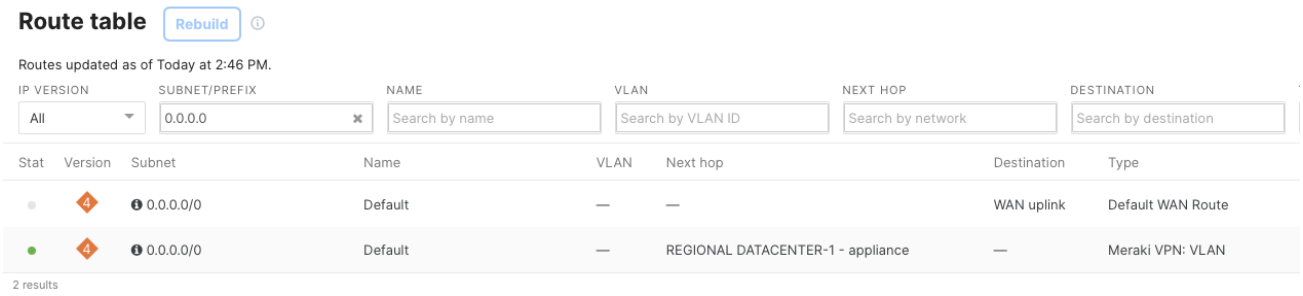
- 本社でホストされている企業アプリケーション、中央データベース、およびサービスのトラフィックは、VPN トンネル経由で自動的に送信されます。これにより、データの安全性が維持され、企業ポリシーに確実に準拠できます。
- ゲスト Wi-Fi、パブリッククラウドサービス、SaaS アプリケーションなど、インターネット向けのトラフィックは、ブランチオフィスでローカルインターネット接続を使用できます。これにより、メインネットワーク（WAN）を通過するデータ量が削減され、アプリケーションがクラウドプロバイダーに近いため、アプリケーションの実行速度が向上します。

デフォルトでは、本社が共有している企業ネットワークのリストに一致しないブランチオフィスのトラフィックはすべて、インターネットに直接ルーティングされます。これは、ブランチデバイス（スポーク MX）に設定されているデフォルトルート（0.0.0.0/0）が原因です。

ブランチが、デフォルトですべてのトラフィックが本社に送信される「フルトンネル」モードでセットアップされている場合は、VPN 除外ルールを作成する必要があります。これらのルールでは、VPN トンネルの代わりにローカルインターネット接続を使用するトラフィックタイプを指定します。

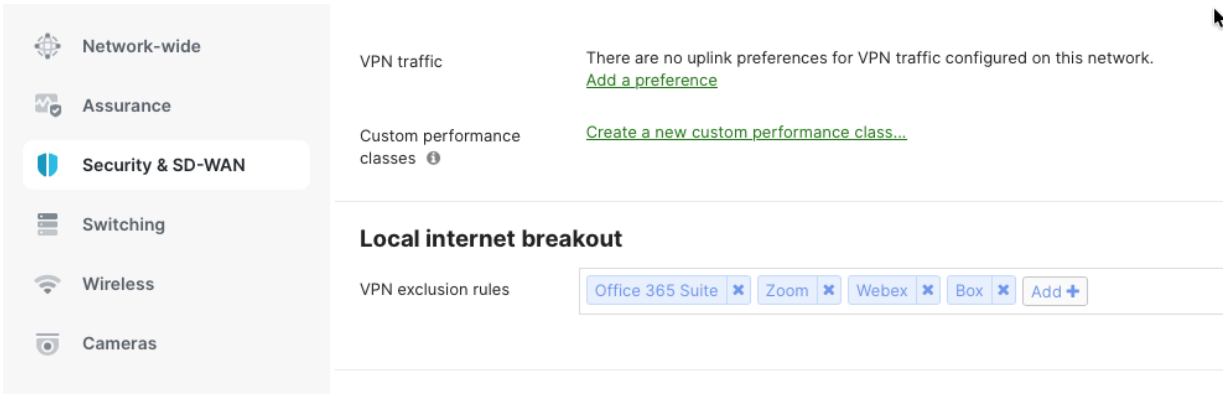
手順 20。 サイトの IPv4 デフォルトルートオプションを選択するには、次の手順を実行します。

[セキュリティおよび SD-WAN（Security & SD-WAN）] > [サイト間 VPN（Site-to-site VPN）] の順に選択します。



手順 21。 サイトのローカル インターネット ブレークアウトおよび VPN 除外ルールを定義するには、次の手順を実行します。

[セキュリティおよび SD-WAN（Security & SD-WAN）] > [SD-WAN および通信シェーピング（SD-WAN & Traffic Shaping）]の順に選択します。

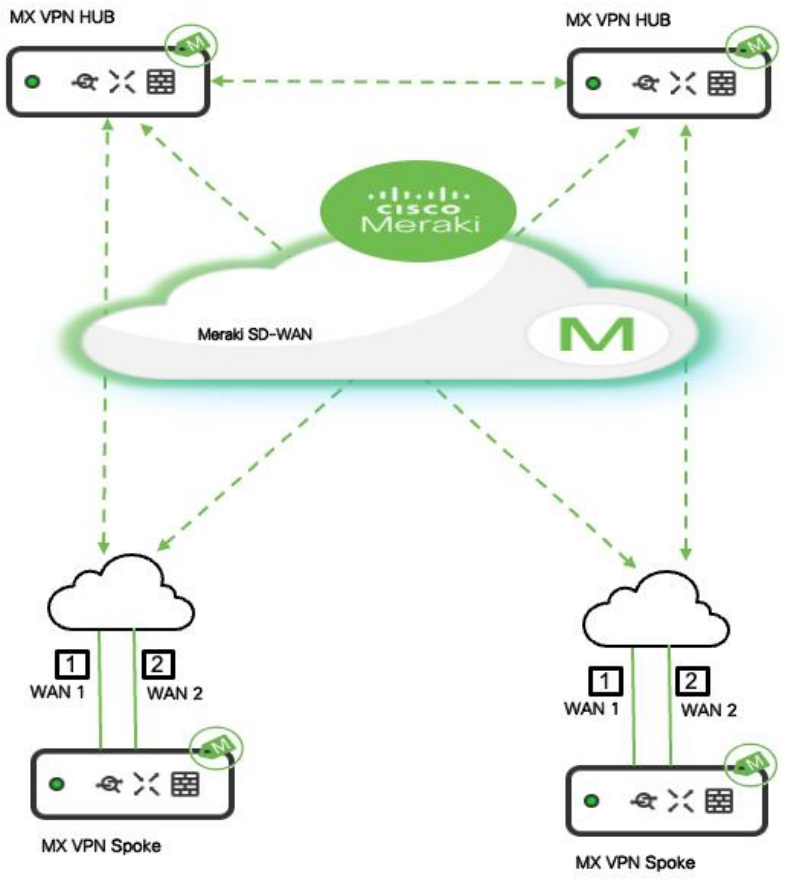


高可用性と WAN の復元力

WAN の高可用性

本社（ハブ）と店舗（スポーク）の両方にある Meraki MX セキュリティアプライアンスは、スマートな WAN アップリンクの選択とロードバランシングを使用して、ネットワークのスムーズな稼働を保証します。メイン接続で障害が発生したり、速度が低下した場合は、別のインターネット接続に自動的に切り替わります。MX アプライアンスは、プライマリおよびバックアップブロードバンド接続（ケーブルまたは光ファイバなど）を含む複数の WAN アップリンクをサポートしているため、メインのインターネット接続に問題がある場合でもビジネスを維持できます。

さらに、追加のバックアップ用にウォームスペアユニットを使用して、MX アプライアンスを高可用性モードでセットアップできます。両方の MX デバイスがウォームスペアモードで展開され、それぞれに 2 つの WAN 接続（WAN1 および WAN2）がある場合、サイトのインターネット接続の冗長性は 4 層となります。



アップリンク選択ポリシー

Meraki MX を使用すると、管理者は、さまざまな種類のトラフィックまたはアプリケーションが使用するインターネット接続（WAN リンク）を選択できます。これはポリシーベースのアップリンクの選択によって行われ、ビジネスニーズを一致させ、コストを制御するのに役立ちます。

Cisco Meraki ダッシュボードでアップリンク選択ポリシーを設定するには、[セキュリティおよび SD-WAN（Security & SD-WAN）] > [通信シェーピング（Traffic Shaping）] の順に選択します。ここでは、販売時点情報（POS）トランザクションや Voice over IP（VoIP）通話などの重要なビジネストラフィックが、常にメインの高速インターネット接続を使用するようにするルールを作成できます。大容量ファイルの転送、ソフトウェア

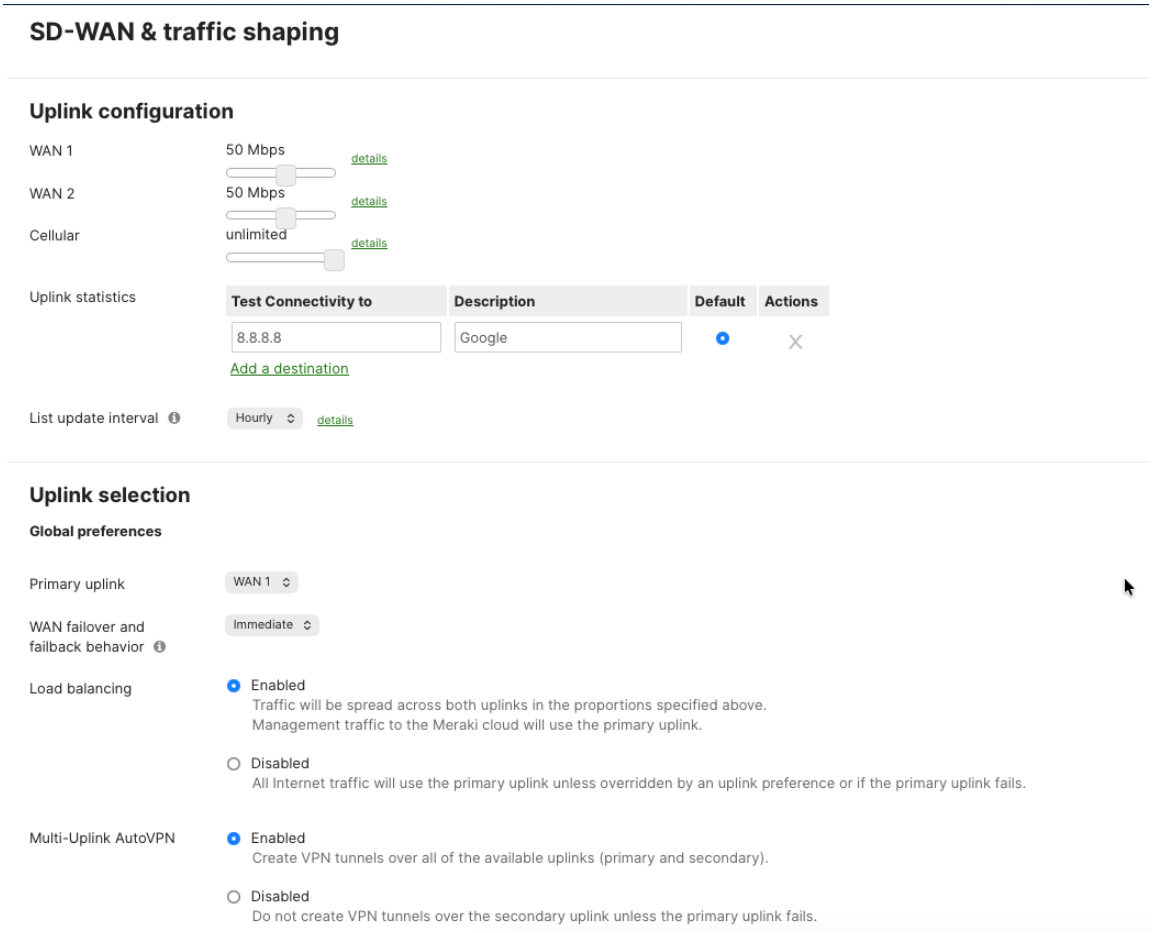
の更新、バックアップなど、重要度が低いトラフィックは、バックアップ接続またはセカンダリ接続を介して送信できます。

このセットアップにより、重要なビジネスアプリケーションでは最も高速で信頼性の高い接続が取得され、重要でないタスクはバックアップリンクが使用されます。利用可能な総帯域幅をより効率的に使用し、従量課金制接続のコストを管理し、重要なビジネストラフィックが常に優先順位付けされるようにします。

また、「アクティブ-アクティブ」なロードバランシング用にシステムを設定することもできます。これは、両方のインターネット接続が同時に使用され、VPN トラフィックなどのデータフローが分割されることを意味します。この方法では、使用可能なすべての帯域幅が使用され、通常の運用中に接続が未使用のままになることはありません。

手順 22。アップリンクの選択と設定を定義するには、次の手順を実行します。

[セキュリティおよび SD-WAN（Security & SD-WAN）] > [SD-WAN および通信シェーピング（SD-WAN & Traffic Shaping）]の順に選択します。



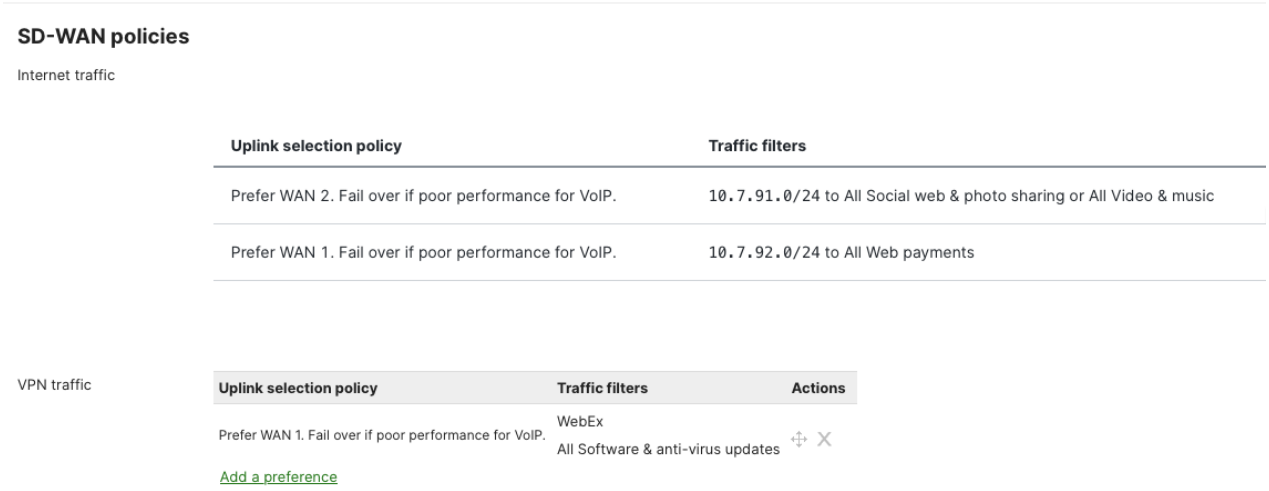
パフォーマンスベースのロードバランシング

MX プラットフォームは、遅延、ジッター、パケット損失、および使用可能な帯域幅などの WAN アップリンクの評価指標を継続的に監視し、最適なアプリケーション パフォーマンスを維持するためにトラフィック分散を動的に調整します。プライマリアップリンクでパフォーマンス低下が検出された場合（ピーク時の遅延の増加や輻輳を示すパケット損失など）。MX は、手動の介入なしで、アプリケーションのパフォーマンスを維持する代替アップリンクにトラフィックを自動的に移行させます。このアクティブなパフォーマンス モニタリングは継

続的に運用され、品質低下を秒単位で検出するため、ビジネスオペレーションやカスタマーエクスペリエンスに影響を与える可能性のある WAN の状態の変化に迅速に対応できます。

手順 23。ポリシーを定義するには、次の手順を実行します。

[セキュリティおよび SD-WAN（Security & SD-WAN）] > [SD-WAN および通信シェーピング（SD-WAN & Traffic Shaping）]の順に選択します。



ThousandEyes を使用した WAN の正常性モニタリング

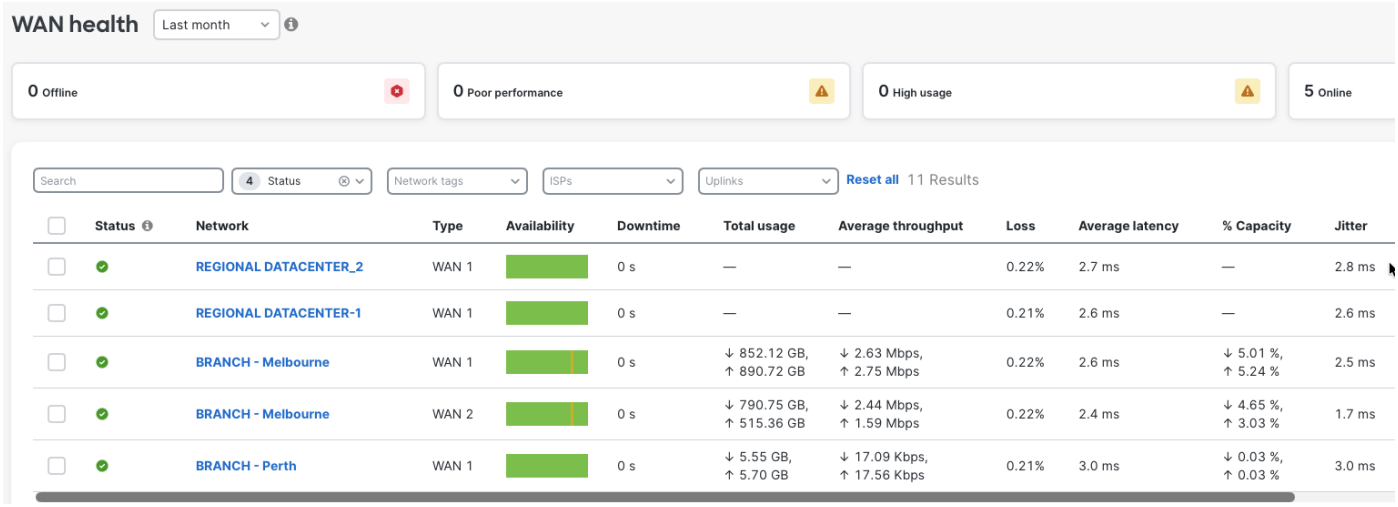
Cisco Meraki ダッシュボードを Cisco ThousandEyes と統合することで、ブランチエッジを超えたエンドツーエンドの WAN の可視性が提供されます。MX アプライアンスに展開された ThousandEyes エージェントは、インターネットおよびマルチクラウド環境全体でアプリケーションのパフォーマンス、パスの可視化、および ISP の正常性を継続的にモニターします。合成テストで、重要な SaaS アプリケーションへの接続を検証します。一方、ホップバイホップのパスの分析は、ネットワーク、ISP、またはアプリケーション プロバイダー インフラストラクチャを問わずパフォーマンス低下が発生している場所を特定することで、より迅速な障害対応とプロアクティブな解決を可能にします。

手順 24。ThousandEyes を組織に統合するには、次の手順を実行します。

[インサイト（Insights）] > [設定（Configure）] > [アクティブアプリケーションモニタリング（Active Application Monitoring）] の順に選択します。

手順 25。ネットワークの WAN の正常性を確認するには、次の手順を実行します。

[インサイト（Insights）] > [WAN の正常性（WAN Health）] の順に選択します。



小売店舗とブランチの展開

小売店舗とブランチ展開では、BaC インフラストラクチャを使用して、数百ものロケーションでネットワークを一貫して迅速にセットアップできます。Terraform プロバイダーと事前テスト済み YAML テンプレートを使用することで、手動セットアップが不要な自動設定によって新しい店舗を数時間以内に稼働状態とすることができます。

セキュリティフレームワークは、ゼロトラストの原則に従います。ワイヤレス POS デバイスには WPA3-Enterprise を使用し、有線 POS システムには 802.1X 認証を使用します。Meraki MX アプライアンスは、PCI DSS 要件を満たすために、AMP、IPS/IDS、および次世代ファイアウォール機能を含む、高度な脅威からの保護を提供します。

ファイアウォールポリシーは、承認された決済ゲートウェイへの接続のみを許可する個別の安全なネットワークセグメントでの決済処理を維持することで、POS トラフィックを保護します。ダイレクト インターネット アクセス ポリシーにより、ゲスト Wi-Fi およびクラウドアプリケーションはローカルインターネット接続を使用できます。これにより、 WAN の使用率が削減され、スマート VPN 除外ルールによってパフォーマンスが向上します。

ゲスト Wi-Fi は、カスタム キャプティブ ポータルおよび分離されたネットワークセグメントを使用して設定されるため、会社のリソースへのアクセスが防止されます。帯域幅管理により POS システムが優先され、ファイアウォールルールによりゲストユーザーはインターネット専用アクセスに制限され、ゲストデバイス間の通信はブロックされます。

アプリケーション モニタリング ツールは、POS のパフォーマンス、決済ゲートウェイ接続、およびネットワーク全体の正常性に関するリアルタイムのインサイトを提供します。自動アラートは、緊急に対処する必要がある接続の問題、セキュリティイベント、またはパフォーマンスの問題を迅速に通知します。

Meraki Location Analytics は、訪問者のカウント、滞在時間、再訪問者の追跡、ヒートマップ、エンゲージメントメトリックなどの顧客訪問分析を提供します。これは、GDPR および CCPA に準拠し続けながら、人員配置や商品の配置を決定するのに役立ちます。

まとめると、このブランチ展開アプローチにより、自動化されたセットアップ、強力なセキュリティ、スマートなトラフィック管理、価値のあるビジネス分析がもたらされます。これらはすべて Cisco Meraki ダッシュボードを介して一元管理され、一貫したポリシーの適用、障害対応の容易さ、および小売ネットワークの統合ビューがもたらされます。

BaC ツールキットの導入

BaC では、Infrastructure as Code（IaC）の原則を使用してブランチネットワークの展開を自動化します。手動セットアップを廃止し、自動化された管理しやすいプロビジョニングに置き換えます。これにより、小売ビジネスはシスコの実証済みの設計および自動化ツールを使用して、多くの店舗ロケーションでネットワークを迅速かつ一貫して展開、管理、拡張できます。

このアプローチでは、ネットワークチームは、ルーティング、セキュリティ、ワイヤレスおよび有線インフラストラクチャに関するシスコのベストプラクティスを含む事前テスト済みの構成テンプレートを使用してブランチサービスを定義します。これにより、一貫性のある標準化されたネットワークが作成されますが、小規模な店舗から大きな主要店舗まで、さまざまな規模の店舗やレイアウトにも引き続き柔軟に対応できます。

BaC ツールキットには、全体的なネットワーク計画と特定のデバイス設定間のリンクとして機能する、専用の Terraform プロバイダーが含まれています。組み込みの API 接続を使用して、ビジネスニーズを詳しいデバイス設定に自動的に変換します。ルーティング、セキュリティ、ワイヤレス、およびスイッチングに関する最適化された設定を含む、すぐに使用できる YAML テンプレートのライブラリもあります。

小売業者は、さまざまなタイプの店舗（小規模店舗、標準店舗、スーパーストア、フラグシップなど）用に設計されたテンプレートだけでなく、POS ネットワーク分離、顧客 Wi-Fi、および IoT デバイスのセットアップ用の機能的なテンプレーもを使用できます。これにより店舗オープンが迅速化され、新しいネットワーク インフラストラクチャは数分で実稼働の準備が整います。すべての設定は Git リポジトリで追跡および管理されます。

この方法では、展開前のチェックによって設定ミスが防止され、問題が発生した場合の即時の復元が可能になり、監査用に完全な記録が生成されるため、手動作業が大幅に削減されます。DevOps を使用するチームは IaC 機能と CI/CD パイプラインを利用して、テスト、承認、およびビジネスニーズへの迅速な対応を実行できます。

BaC は、ソフトウェア エンジニアリング プラクティスを企業のネットワーキングにもたらし、ネットワーク インフラストラクチャを戦略的ビジネス資産にする一方、フランチャイズのカスタマイズや、POS やインベントリ管理などの主要な小売システムとの統合も引き続き可能です。

小売展開で BaC を使用するには、Terraform が必要です。これは設定ファイルを実際の Meraki デバイス設定に変換するプロセスを自動化するツールです。シスコでは、検証済みの Terraform 設定、さまざまな店舗タイプの YAML テンプレート、および小売向けのセキュリティおよびコンプライアンスに準拠した展開パターンを含む、詳細な BaC Git リポジトリを用意しています。これは、シスコの公式 Branch as Code リポジトリで確認できます。Terraform のインストール、環境設定、および展開の準備に関する詳しい説明は、このドキュメントの「参考資料」セクションにあります。YAML 設定テンプレートの詳細については、「Network as Code: Overview」を参照してください。

BaC リポジトリのセットアップ

「テクニカルリファレンス」の説明に従って Terraform のインストールと環境設定が終了したら、次のステップとして、Meraki 展開に必要なすべてのプロバイダーコード、モジュール、および事前検証済みの YAML 設定テンプレートを含む BaC リポジトリを取得します。シスコは Network-as-Code（NaC）Meraki リポジトリを維持管理しています。このリポジトリには、Terraform プロバイダーモジュール、ブランチ展開テンプレート、および自動化された店舗ネットワーク プロビジョニングの基盤となる小売固有の設定例が含まれています。

手順 26。 BaC リポジトリを複製するには、次の手順を実行します。

ステップ 1. Terraform がインストールされているローカルマシンまたは仮想マシンにリポジトリを複製するには、次のコマンドを実行します。

```
bash
git clone https://wwwin-github.cisco.com/netascode/nac-meraki.git

cd nac-meraki
```

ステップ 2. リポジトリを複製したら、main.tf ファイルで正しい Terraform プロバイダーが定義されていることを確認します。リポジトリには、以下を参照している事前設定済みのプロバイダー定義が含まれています。

`Terraform Cisco Meraki Network-as-Code モジュール：nac-meraki`

`Meraki プロバイダー：CiscoDevNet/meraki`

ステップ 3. main.tf ファイルを確認して、これらのプロバイダーが正しく指定されていて、Terraform のインストールバージョンと互換性があることを確認します。リポジトリ構造には、テンプレート、モジュール、および設定例のディレクトリが含まれており、これらを特定の小売展開要件に合わせてカスタマイズします。

ステップ 4. Meraki HUB/データセンターネットワークは、BaC フレームワークの外部で手動で作成されます。次のコマンドシンタックスを使用して、これらのネットワークを Terraform 状態ファイルにインポートする必要があります。

```
terraform import
'module.meraki.meraki_network.network["ORG_NAME/NETWORK_NAME"]'<ORG_ID>,<NETWORK_ID>
```

Cisco Meraki ダッシュボードの組織の API キーを環境変数として設定します。これにより、Terraform は、自動化された Infrastructure-as-Code 展開および管理ワークフローのために Meraki 組織と認証および通信できるようになります。

リポジトリが正常に複製され、プロバイダーが検証されたら、中小規模および大規模店舗のフォーマットのスタート地点として、提供されたテンプレートを活用して、小売店舗の展開要件に合わせてブランチ YAML 設定ファイルの作成およびカスタマイズを続けることができます。

BaC ツールキットを使用した店舗ネットワークの展開

前述の説明に従って BAC ツールキットを設定し、Terraform を設定したら、Cisco Meraki ダッシュボードで基本的なネットワーク インフラストラクチャを設定して、ブランチ展開プロセスを開始します。この基盤が整ったら、BaC テンプレートを使用して、店舗全体の構成を自動的に設定できます。

BAC ファイル構造では、/data ディレクトリに、ネットワークとその設定を定義するすべての YAML ファイルが含まれます。提供されたテンプレートを使用して変数値を入力することでブランチや設定を作成できます。または、必要に応じて独自の YAML ファイルを作成できます。

注： このドキュメントの以降のセクションはすべて、YAML 設定の例と、ダッシュボードでの対応する結果を示します。

手順 27。ブランチを展開するには、次の手順を実行します。

ステップ 1. ネットワークデバイスのクラウド ID が組織に要求され、ネットワークに追加されましたか?

このサンプル YAML ファイルでは、デバイスを組織に対して要求し、ネットワークを作成し、デバイスをブランチネットワークに追加します。

```
organizations:
  - name: Next_Gen_Retail
    inventory:
      serials:
        - Q3LA-X6VB-FXVV
        - Q5UA-VE6K-VRJD
        - Q5BB-XY4E-M4NT
        - Q5TA-T45N-TQS9
        - Q5TA-VD2Q-EQSP
        - Q2GV-P8YL-J8K3
        - Q4GV-9K82-SPTX
        - Q5TA-UKHK-A5EY
```

```
networks:
  - name: BRANCH - Melbourne
    product_types:
      - appliance
      - camera
      - switch
      - wireless
      - cellularGateway
      - sensor
    devices:
      - name: BRANCH-Mel-MX
        serial: Q3LA-X6VB-FXVV
      - name: BRANCH-Mel-MX-spare
        serial: Q3LA-6TBL-A36E
      - name: DISTRIBUTION
        serial: Q5TA-UKHK-A5EY
      - name: MEL01-STACK-1-2
        serial: Q5TA-T45N-TQS9
      - name: MEL01-STACK-1-1
        serial: Q5TA-VD2Q-EQSP
      - name: MEL01-MS150-ACCESS
        serial: Q4GV-9K82-SPTX
      - name: MEL01-Floor-1-AP-1
        serial: Q5BB-XY4E-M4NT
        tags:
          - floor-1
      - name: MEL01-Floor-1-CAM-1
        serial: Q2GV-P8YL-J8K3
    switch_stacks:
      - name: Mel-Floor-1-STACK-1
        devices:
          - MEL01-STACK-1-1
          - MEL01-STACK-1-2
    time_zone: America/Los_Angeles
    notes: This is Unfied Branch site Melbourne
    tags:
      - branch_office
    settings:
      local_status_page_enabled: true
      remote_status_page: true
      secure_port: false
      local_status_page_authentication:
        enabled: true
      named_vlans: true
    snmp:
      access: "users"
      users:
```

ステップ 2. POS デバイス、VoIP 電話、AP などの割り当てを使用して、アクセススイッチポートを設定します。

注： デフォルトでは、スイッチがクラウドによって管理される場合、すべてのスイッチポートがトランクモードに設定されます。セキュリティ上の理由により、未使用のすべてのポートをアクセスモードに設定し、無効にすることが重要です。

```
- name: MEL01-ACCESS-2
  switch:
    ports:
    - port_ids: "1-10" #VOIP Phones
      name: VoIP Phones
      enabled: true
      type: access
      vlan: 1
      voice_vlan: 14
      access_policy_name: Corporate Voice Policy
      access_policy_type: "Custom access policy"
      port_schedule_name: "Weekend Only Port Schedule"
    - port_ids: "11-20" #PoS Wired
      name: PoS Wired
      enabled: true
      type: access
      vlan: 1
      access_policy_name: Wired POS Policy
      access_policy_type: "Custom access policy"
      port_schedule_name: "Weekend Only Port Schedule"
    - port_ids: "21-30" #Access Points
      name: Access Points
      enabled: true
      type: trunk
      vlan: 11
      port_schedule_name: "Weekend Only Port Schedule"
    - port_ids: "30-45"   # Default all unused ports and disable
      name: Defaulted Ports
      enabled: false
      type: access
      vlan: 1
      port_schedule_name: "Weekend Only Port Schedule"
```

ステップ 3. アップストリーム MX デバイスで、すべてのエンドデバイスとユーザーをオンボーディングするためのブランチ ユーザー ネットワークを作成します。

注： MX アプライアンスで作成されたクライアントサブネットは、それ自体が DHCP サーバーとして動作することも、企業全体の集中型 DHCP サーバーに DHCP 要求をリレーすることもできます。

```yaml
networks:
  - name: BRANCH - Melbourne
    appliance:
      vlans:
        - vlan_id: 11
          name: "Corporate_VLAN"
          subnet: "10.7.91.0/24"
          appliance_ip: "10.7.91.1"
          dhcp_handling: "Run a DHCP server"
          dhcp_lease_time: "1 day"
          dhcp_boot_options: false
          dns_nameservers: "173.38.200.100"
          mandatory_dhcp: true
        - vlan_id: 12
          name: "POS_VLAN"
          subnet: "10.7.92.0/24"
          appliance_ip: "10.7.92.1"
          dhcp_handling: "Run a DHCP server"
          # dhcp_lease_time: "1 day"
          # dhcp_boot_options: false
          # dns_nameservers: "173.38.200.100"
          mandatory_dhcp: true
        - vlan_id: 13
          name: "Guest_VLAN"
          subnet: "10.7.93.0/24"
          appliance_ip: "10.7.93.1"
          dhcp_handling: "Run a DHCP server"
          dhcp_lease_time: "1 day"
          dhcp_boot_options: false
          dns_nameservers: "173.38.200.100"
          mandatory_dhcp: true
```

デバイス要求、ネットワーク作成、VLAN プロビジョニングを含め、ネットワーク インフラストラクチャが BaC を介して正常に展開されたら、小売店舗ネットワークで、エンドユーザーの接続と運用機能を有効にするクライアントデバイスのオンボーディング設定を行う準備が整います。

ネットワークの一般的な VLAN セグメンテーションは、データと音声用の企業 VLAN、IoT、およびゲストのセグメンテーションで構成されます。前述の展開手順により確立されたネットワークの基礎には、POS システム（VLAN 12 - 10.7.92.0/24）、従業員デバイス（VLAN 11 - 10.7.91.0/24）、ゲスト（VLAN 13 - 10.7.93.0/24）、および IoT インフラストラクチャ（VLAN 14 - 10.7.94.0/24）のサブネットが設定され、セキュアなポリシー駆動型クライアントアクセスに必要なセグメント化されたネットワーク アーキテクチャを作成します。これらの基盤ネットワークセグメントが適切な IP アドレス指定、DHCP サービスで運用できるようになりましたので、次に、小売固有のクライアントデバイスがデバイスタイプ、ユーザーアイデンティティ、およびビジネス要件に基づいて適切なネットワークリソースに接続、認証、およびアクセスできるようにする認証メカニズム、アクセスポリシー、およびサービス設定の導入に焦点を移します。

小売店舗のセキュリティフレームワーク

ゼロトラスト ネットワーク アクセスの原則

小売店舗におけるゼロトラスト ネットワーク アクセスの原則では、ネットワークの場所に関係なく、すべてのデバイス、ユーザー、およびアプリケーションの要求が継続的に認証および承認される「決して信頼せず、常に確かめる」セキュリティモデルが導入されます。このアプローチでは、POS システム、ゲストネットワーク、および IoT デバイスが細かいアクセス制御によって隔離されたゾーンにセグメント化されることで、決済データの保護と PCI DSS への準拠が保証され、セキュリティ侵害が発生したときの侵入拡大の動きが防止されます。

有線およびワイヤレス用 POS のセキュアな接続

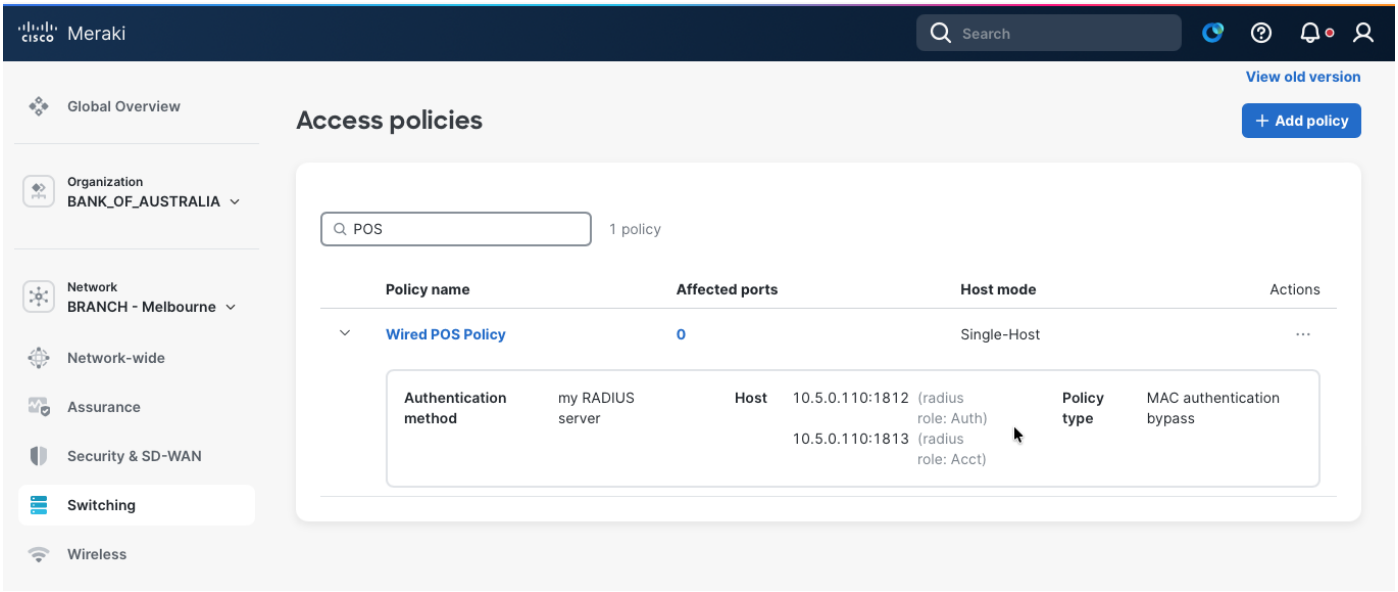
POS システムには、PCI DSS 準拠を維持し、決済用カードのデータを保護するために、厳密なアクセス制御とセキュリティ設定が必要です。有線 POS デバイスの場合、Cisco Meraki ダッシュボードで専用スイッチポートアクセス ポリシーを設定します。これには、[スイッチ（Switch）] > [スイッチポート（Switchports）] の順に選択し、802.1X 認証が有効になっているポートにポリシーを割り当て、ネットワークアクセスを許可する前にデバイス証明書またはユーザーログイン情報の中央 RADIUS サーバーに対する検証を要求します。ポートごとの MAC アドレス数を制限するポートセキュリティを有効にし、不正な DHCP サーバーを防ぐ DHCP スヌーピングを設定し、POS トランザクショントラフィックに優先順位を付ける通信シェーピングポリシーを適用して、ピーク期間中に最適なパフォーマンスを得ることができます。

モバイル決済端末やハンドヘルド インベントリ スキャナを含むワイヤレス POS デバイスの場合、パッシブな盗聴から保護する強化された暗号化と個別のデータ暗号化を提供する WPA3-Enterprise セキュリティで設定された専用 SSID（「POS-Secure」など）を作成します。干渉を減らし、スループットを向上させるために、RADIUS 検証、専用 POS ネットワーク VLAN への VLAN 割り当て、および 5 GHz への接続を優先するバンドステアリングを必要とする 802.1X 認証を使用して、[ワイヤレス（Wireless）] > [SSID] から SSID を設定します。高速ローミング（802.11r）を有効にしてモバイル POS デバイスが店舗内を移動するときのシームレスなハンドオフを実現し、最小ビットレート設定（12 Mbps）を設定してトランザクション処理時間や顧客体験に影響を与える可能性のある低パフォーマンスの接続を防止します。

この設定で有線 POS デバイスをオンボーディングするための YAML ファイルの例を次に示します。

```yaml
meraki:
  domains:
    - name: EMEA
      organizations:
        - name: BANK_OF_AUSTRALIA
          - name: Wired POS Policy
            access_policy_type: MAC authentication bypass
            dot1x_control_direction: both
            guest_port_bouncing: false
            host_mode: Single-Host
            radius:
              critical_auth:
                suspend_port_bounce: false
            radius_accounting: true
            radius_accounting_servers:
              - host: 10.5.0.110
                port: 1813
                secret: SecretKey123
            radius_coa_support: true
            radius_group_attribute: ''
            radius_servers:
              - host: 10.5.0.110
                port: 1812
                secret: SecretKey123
            radius_testing: true
            url_redirect_walled_garden: false
            voice_vlan_clients: false
```

この YAML を 'terraform apply' を使用して Terraform で実行すると、Cisco Meraki ダッシュボードに次のアクセスポリシーが作成されます。

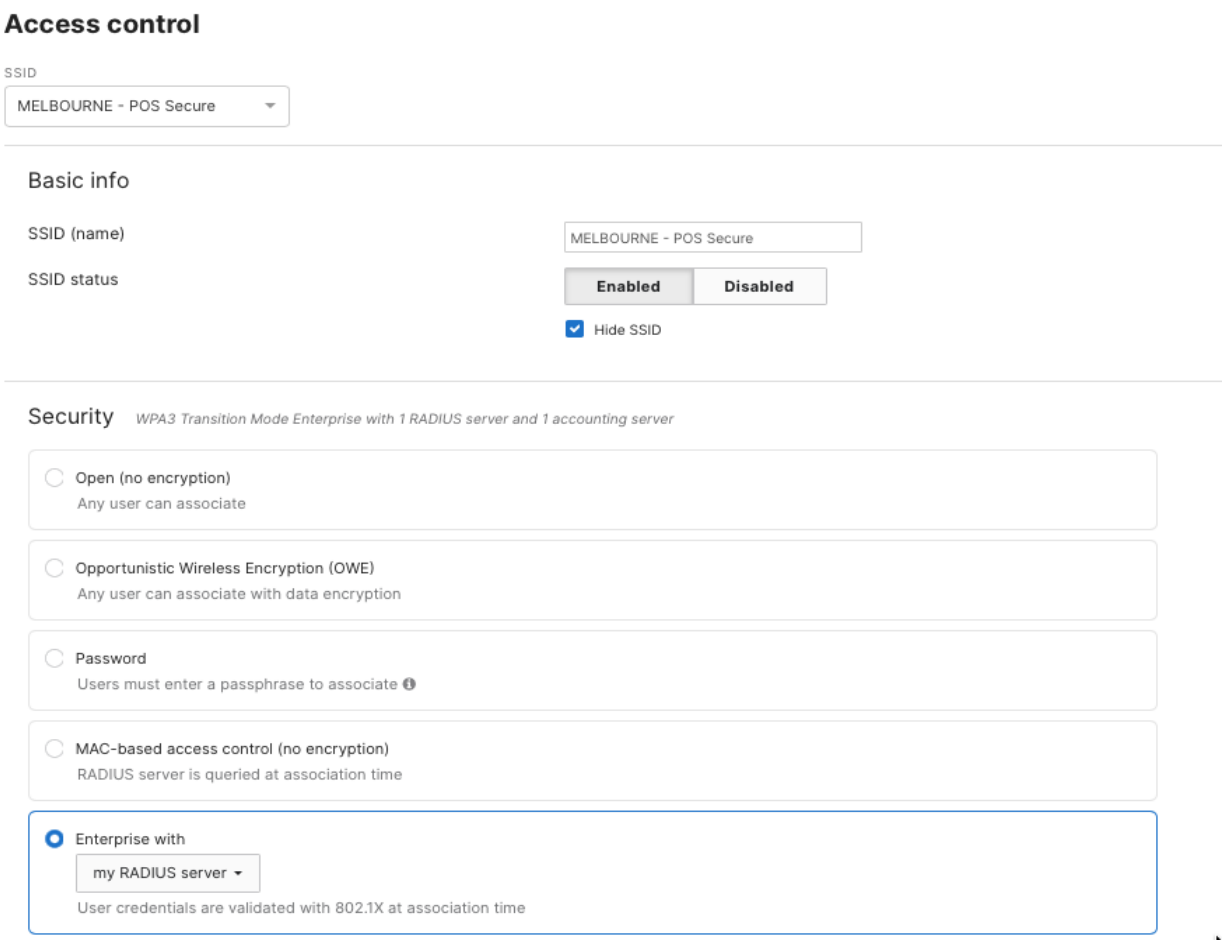


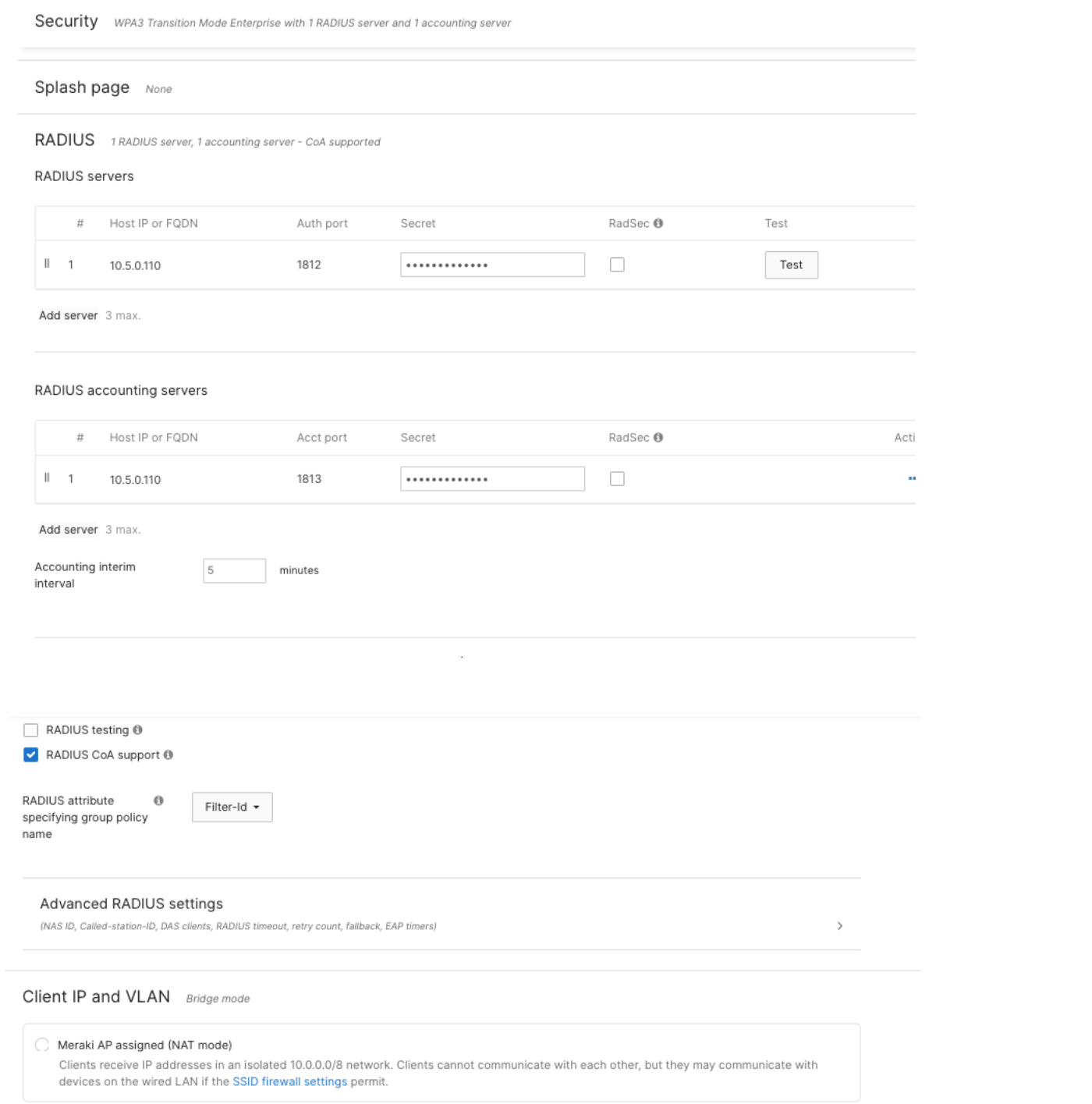
この設定でワイヤレス POS デバイスをオンボーディングするための YAML ファイルの例を次に示します。

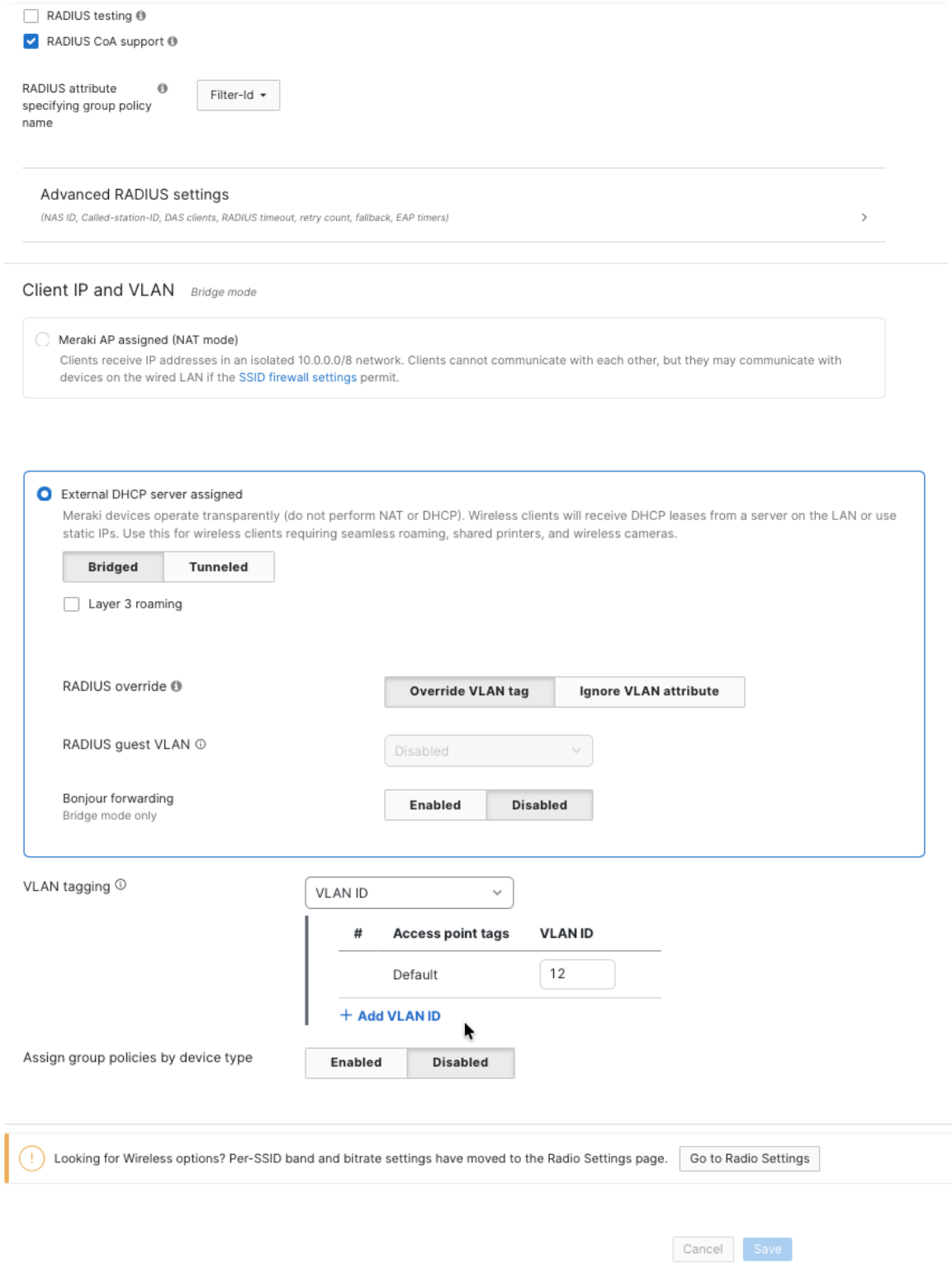
```yaml
# POS Devices SSID - Secure onboarding for point-of-sale systems
- name: "MELBOURNE - POS Secure"
  ssid_number: "3"
  auth_mode: 8021x-radius
  available_on_all_aps: true
  default_vlan_id: 20
  encryption_mode: wpa-eap
  ip_assignment_mode: Bridge mode
  lan_isolation: true
  mandatory_dhcp: true
  use_vlan_tagging: true
  splash_page: None
  enabled: true
  visible: false  # Hidden SSID for security
  wpa_encryption_mode: "WPA3 Transition Mode"
  dot11w:
    enabled: true      # Allow unsupported clients
    required: false    # Don't reject older POS devices
  radius:
    proxy: false
    testing: false
    server_timeout: 3
    server_attempts_limit: 2
    coa: true
    fallback: false
    override: true
    accounting: true
    accounting_interim_interval: 300
    attribute_for_group_policies: Filter-Id
    servers:
      - host: 10.5.0.110
        secret: "!env radius_secret"
        port: 1812
        radsec: false
    accounting_servers:
      - host: 10.5.0.110
        port: 1813
        secret: "!env radius_secret"
        radsec: false
  # No bandwidth limits for POS traffic
  per_client_bandwidth_limit_down: 0  # Unlimited
  per_client_bandwidth_limit_up: 0    # Unlimited
  per_ssid_bandwidth_limit_down: 0    # Unlimited
  per_ssid_bandwidth_limit_up: 0      # Unlimited
  # High priority for POS transactions
  traffic_shaping_rules:
```

```
  rules:
    - definitions:
      - type: applicationCategory
        value: meraki:layer7/category/5   # Payment processing
      - type: applicationCategory
        value: meraki:layer7/category/17  # Database
      per_client_bandwidth_limits:
        settings: ignore  # No limits for POS traffic
      dscp_tag_value: 46  # Expedited Forwarding (highest priority)
# POS operates 24/7 - no scheduling restrictions
schedules:
  enabled: false
```

この YAML を 'terraform apply' を使用して Terraform で実行すると、Cisco Meraki ダッシュボードに次の SSID が作成されます。







同様の設定は、従業員のオンボーディング、IoT デバイスのオンボーディング、IP 電話などに対して、有線およびワイヤレスで使用できます。

脅威からの保護とコンテンツフィルタリング

小売店舗での Meraki MX セキュリティアプライアンスには、Cisco Advanced Malware Protection（AMP）、侵入防御システム（IPS）、侵入検知システム（IDS）などの組み込みの脅威からの保護機能が用意されており、決済システムやビジネスオペレーションをサイバー脅威から保護できます。

手順 28。 脅威からの保護を設定するには、次の手順を実行します。

ステップ 1. ダッシュボードで、[セキュリティおよび SD-WAN（Security & SD-WAN）] > [脅威からの保護（Threat Protection）] の順に選択します。

ステップ 2. [AMP] をオンにしてファイルをリアルタイムでスキャンし、後で検出される可能性のある脅威を捕捉します。

ステップ 3. バランス型ルールセットを使用する防御モードで [IPS/IDS] を有効にし、エクスプロイトの試行と有害なトラフィックを自動的にブロックします。

手順 29。 コンテンツフィルタリングを設定するには、次の手順を実現します。

ステップ 1. [セキュリティおよび SD-WAN（Security & SD-WAN）] > [コンテンツフィルタリング（Content Filtering）]の順に選択します。

ステップ 2. 重要なビジネスアプリケーションへのアクセスを許可しながら、成人向けコンテンツ、違法サイト、ピアツーピアファイル共有などの不要なカテゴリをブロックします。

ステップ 3. 競合他社のサイトなどの特定の Web サイトをカスタム URL リストに追加してブロックします。

これらの設定は、すべての店舗ロケーションの安全性を維持し、事業運営をサポートし、規制への準拠を維持するのに役立ちます。

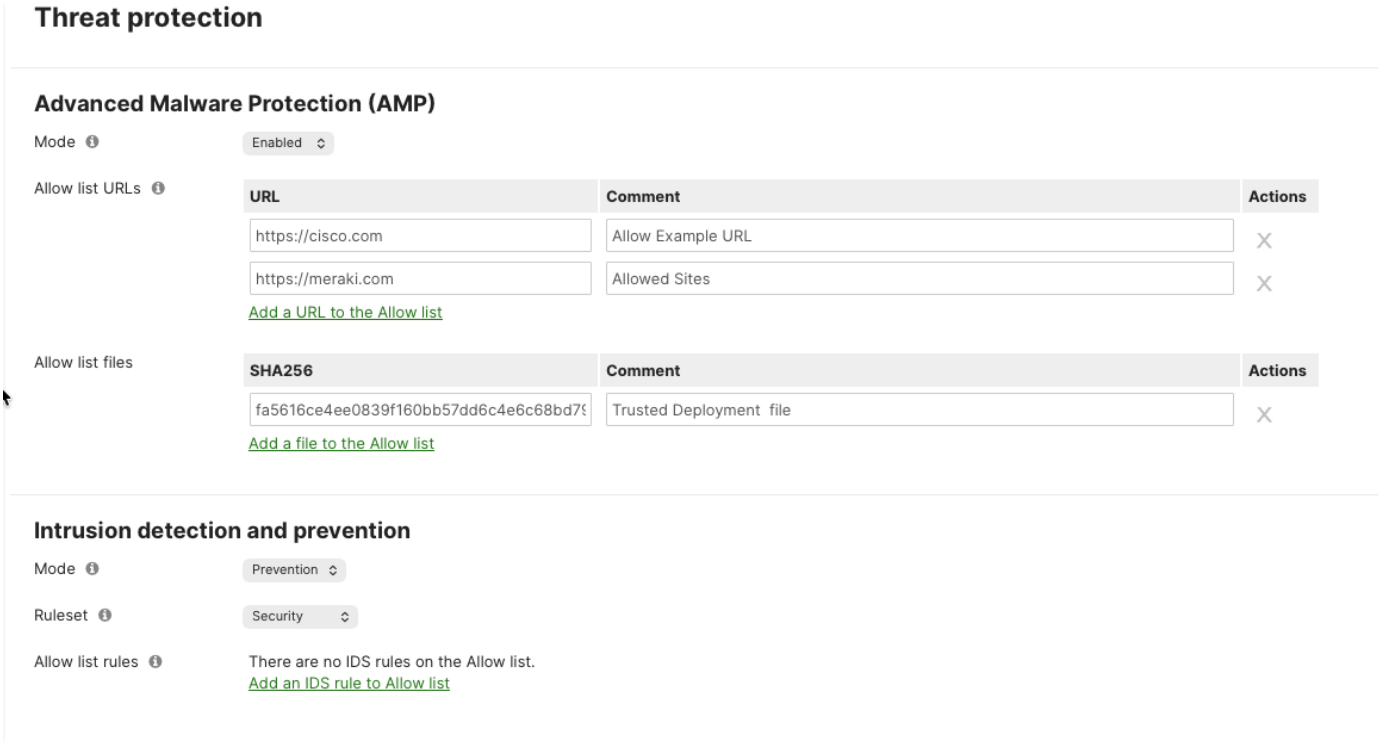
コンテンツフィルタリングを使用して AMP および IPS/IDS を有効にするための YAML ファイルの例を次に示します。

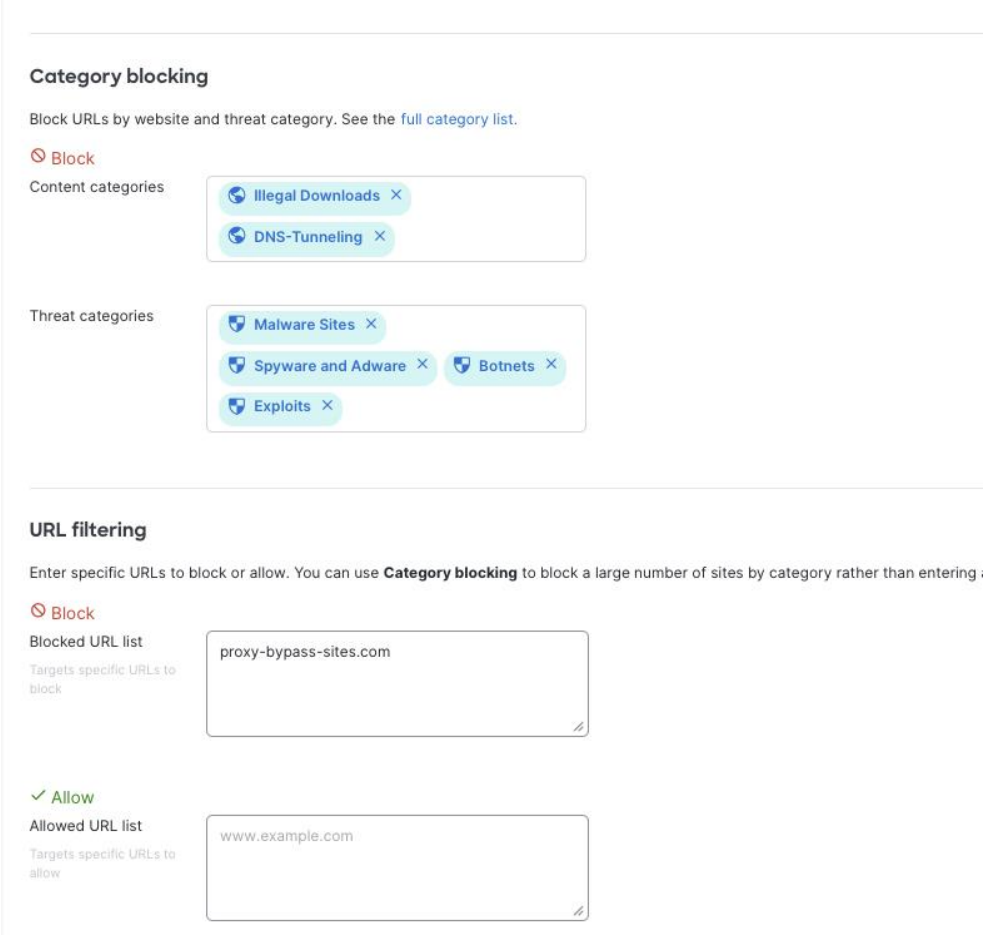
```
    - name: BRANCH - Melbourne
      appliance:
        security_malware:
          mode: "enabled"
          allowed_urls:
            - url: "https://cisco.com"
              comment: "Allow Example URL"
            - url: "https://meraki.com"
              comment: "Allowed Sites"
          allowed_files:
            - sha256: "fa5616ce4ee0839f160bb57dd6c4e6c68bd79894418c85963e972c71bdfdf
              comment: "Trusted Deployment  file"
        security_intrusion:
          mode: "prevention"  # or "prevention or detection"
          ids_rulesets: "security"  # or "security", "performance", "balanced"

```

```yaml
- name: BRANCH - Melbourne
  appliance:
    content_filtering:
      # allowed_url_patterns:
      #   - "www.cisco.com"
      #   - "*.meraki.com"
      blocked_url_patterns:
        - "proxy-bypass-sites.com"
      blocked_url_categories:
        - "meraki:contentFiltering/category/C122"
        - "meraki:contentFiltering/category/C84"
        - "meraki:contentFiltering/category/T01"
        - "meraki:contentFiltering/category/T02"
        - "meraki:contentFiltering/category/T04"
        - "meraki:contentFiltering/category/T06"
      url_category_list_size: fullList
```

この YAML を 'terraform apply' を使用して Terraform で実行すると、Cisco Meraki ダッシュボードに次が作成されます。





MX での NGFW 向けの POS トラフィックを保護するファイアウォール ポリシー

POS システムは機密性の高い決済カードデータを処理するため、小売ネットワークにおける最も重大なセキュリティ上の懸念事項となります。PCI DSS への厳密な準拠とデータ侵害からの保護を必要とし、データ侵害が発生した場合は重大な金銭的ペナルティ、評判の低下、およびお客様からの信頼の損失につながる可能性があります。Meraki MX セキュリティアプライアンスに実装された包括的なファイアウォールポリシーは、必要不可欠な決済処理通信のみを許可し、幾重もの防御レイヤで POS システムを不正アクセスから隔離します。

POS ネットワーク セグメンテーションの基盤

セキュリティアーキテクチャは、隔離されたサブネット（例：10.10.10.0/24）を使用して VLAN X にすべての POS デバイスを配置する専用 VLAN 割り当てから始まり、従業員ネットワーク、ゲスト Wi-Fi、IoT デバイス、およびバックオフィスシステムから完全なレイヤ 2 およびレイヤ 3 の分離を作成します。このセグメンテーションにより、Meraki MX アプライアンスでのステートフル ファイアウォール インスペクションによって適用されるセキュリティ境界が確立され、VLAN 境界を超えるすべての通信には、明示的なファイアウォールルールの承認が必要になります。MX アプライアンスは、アプリケーションの認識、侵入防御、および高度なマルウェア保護を提供する統合された次世代ファイアウォール機能を備えた適用ポイントとして機能し、特に小売決済システムをターゲットとした高度な攻撃から POS 環境を保護します。

Cisco Meraki ダッシュボードでのファイアウォールルールの実装

手順 30。 ファイアウォールルールを設定するには、次の手順を実行します。

ステップ 1. 店舗ネットワークのダッシュボードで、[セキュリティおよび SD-WAN（Security & SD-WAN）] > [ファイアウォール（Firewall）] の順に選択します。

ステップ 2. ここでは、POS トラフィックを保護するためのレイヤ 3 ファイアウォールルールを作成および管理できます。

ステップ 3. Cisco Meraki ダッシュボードでは、ファイアウォールルールの追加、配置、編集が簡単で、適用前にルールにエラーがないかチェックされます。

ステップ 4. ファイアウォールルールは上から下の順に適用されます。トラフィックに一致する最初のルールが使用されるため、ルールの順序は非常に重要です。

ステップ 5. 最も具体的で厳密なルールを最初に配置し、その後により広範囲なルールを配置します。

ステップ 6. 一部下には、具体的に許可されていないその他すべてのトラフィックをブロックする最後のルールを追加します。これにより、承認されたトラフィックのみが許可され、その他の試行がブロックされてセキュリティモニタリング用にログに記録されます。

レイヤ 3 ファイアウォールルールの設定

手順 31。 レイヤ 3 ファイアウォールルールを設定するには、次の手順を実行します。

ステップ 1. ダッシュボードで、[セキュリティおよび SD-WAN（Security & SD-WAN）] > [ファイアウォール（Firewall）] > [レイヤ 3 ファイアウォールルール（Layer 3 Firewall Rules）] の順に選択します。ここでは既存のルールのリストが表示されます。

ステップ 2. [ルールの追加（Add a rule）] をクリックして、新しいファイアウォールポリシーを作成します。

ステップ 3. 各ルールについて、次のように設定します。

- [アクション（Action）]：トラフィックの許可または拒否を選択します
- [プロトコル（Protocol）]：プロトコル（TCP や UDP など）を指定します
- [送信元（Source）]：送信元ネットワークまたは IP アドレスを設定します
- [宛先（Destination）]：宛先ネットワークまたは IP アドレスを設定します
- [ポート（Port）]：関連するポート番号を入力します
- （オプション）[ロギング（Logging）]：必要に応じてロギングを有効にします
- （オプション）[スケジューリング（Scheduling）]：必要に応じて、タイムスケジュールを設定します

ステップ 4. POS システムに関連するすべてのルールのロギングが有効になっていることを確認します。これにより、PCI DSS 準拠のために必要な詳細な記録が保持されます。

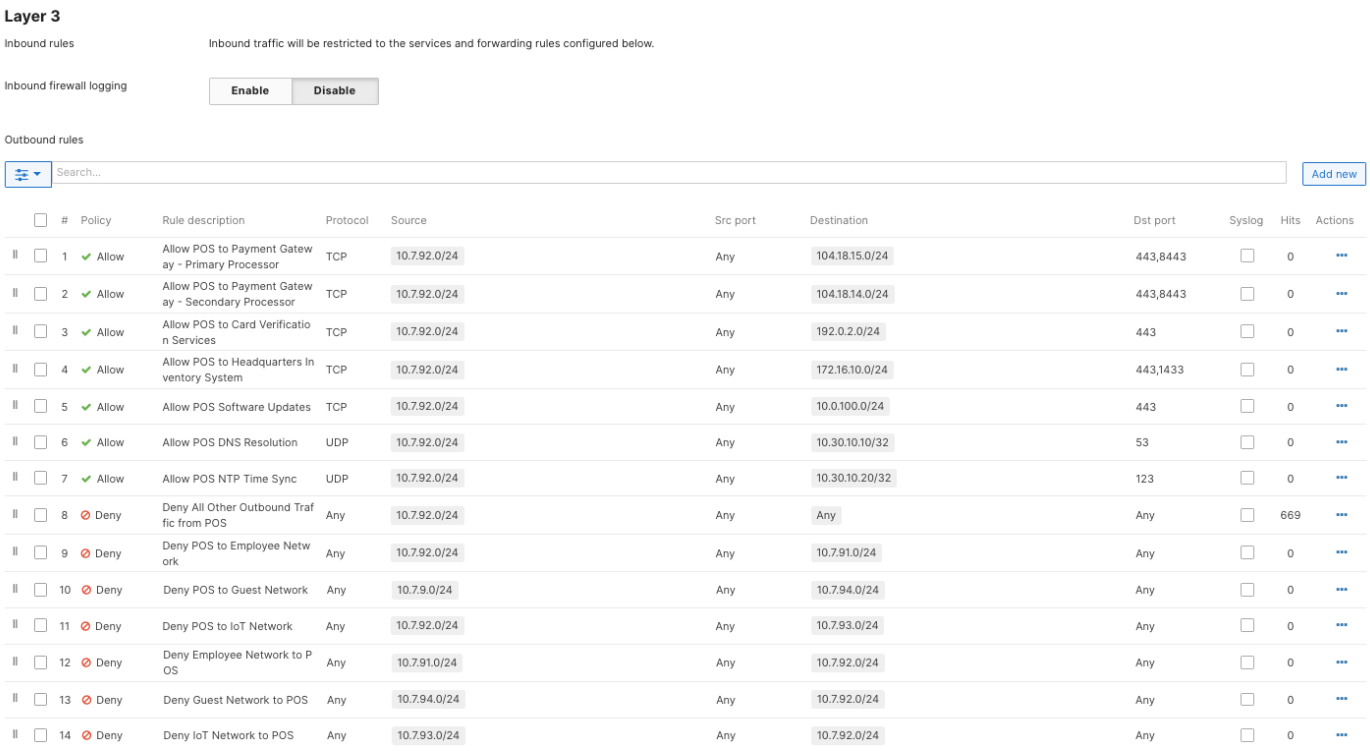
ステップ 5. ログは自動的に Cisco Meraki クラウドに送信され、分析や今後の参照用に保存されることで調査や監査の要件をサポートします。

次に、MX での POS トラフィックのレイヤ 3 ファイアウォールルールの YAML ファイルの例を示します。

```yaml
appliance:
  firewall:
    firewalled_services: …
    l3_firewall_rules:
      rules:
        # POS Outbound Traffic Rules (VLAN 92 - POS Network)
        - comment: "Allow POS to Payment Gateway - Primary Processor"
          policy: allow
          protocol: tcp
          source_port: Any
          source_cidr: "10.7.92.0/24"
          destination_port: "443,8443"
          destination_cidr: "104.18.15.0/24"  # Replace with actual payment gateway IPs
        - comment: "Allow POS to Payment Gateway - Secondary Processor"
          policy: allow
          protocol: tcp
          source_port: Any
          source_cidr: "10.7.92.0/24"
          destination_port: "443,8443"
          destination_cidr: "104.18.14.0/24"  # Replace with actual backup gateway IPs
        - comment: "Allow POS to Card Verification Services"
          policy: allow
          protocol: tcp
          source_port: Any
          source_cidr: "10.7.92.0/24"
          destination_port: "443"
          destination_cidr: "192.0.2.0/24"  # Replace with card verification service IPs
        - comment: "Allow POS to Headquarters Inventory System"
          policy: allow
          protocol: tcp
          source_port: Any
          source_cidr: "10.7.92.0/24"
          destination_port: "443,1433"
          destination_cidr: "172.16.10.0/24"  # HQ inventory subnet via VPN
        - comment: "Allow POS Software Updates"
          policy: allow
          protocol: tcp
          source_port: Any
          source_cidr: "10.7.92.0/24"
          destination_port: "443"
          destination_cidr: "10.0.100.0/24"  # Replace with POS vendor update servers
        - comment: "Allow POS DNS Resolution"
          policy: allow
          protocol: udp
          source_port: Any
          source_cidr: "10.7.92.0/24"
          destination_port: "53"
          destination_cidr: "10.30.10.10/32"  # Corporate DNS server
        - comment: "Allow POS NTP Time Sync"
          policy: allow
          protocol: udp
          source_port: Any
          source_cidr: "10.7.92.0/24"
          destination_port: "123"
          destination_cidr: "10.30.10.20/32"  # Corporate NTP server
        - comment: "Deny All Other Outbound Traffic from POS"
          policy: deny
          protocol: any
          source_port: Any
          source_cidr: "10.7.92.0/24"
          destination_port: Any
          destination_cidr: Any
        # Inter-VLAN Traffic Rules (POS Network Isolation)
        - comment: "Deny POS to Employee Network"
          policy: deny
          protocol: any
          source_port: Any
          source_cidr: "10.7.92.0/24"
          destination_port: Any
          destination_cidr: "10.7.91.0/24"  # Employee/Back-office Network
```

```yaml
- comment: "Deny POS to IoT Network"
  policy: deny
  protocol: any
  source_port: Any
  source_cidr: "10.7.92.0/24"
  destination_port: Any
  destination_cidr: "10.7.93.0/24"  # IoT Devices Network
- comment: "Deny Employee Network to POS"
  policy: deny
  protocol: any
  source_port: Any
  source_cidr: "10.7.91.0/24"
  destination_port: Any
  destination_cidr: "10.7.92.0/24"
- comment: "Deny Guest Network to POS"
  policy: deny
  protocol: any
  source_port: Any
  source_cidr: "10.7.94.0/24"
  destination_port: Any
  destination_cidr: "10.7.92.0/24"
- comment: "Deny IoT Network to POS"
  policy: deny
  protocol: any
  source_port: Any
  source_cidr: "10.7.93.0/24"
  destination_port: Any
  destination_cidr: "10.7.92.0/24"
```

この YAML を 'terraform apply' を使用して Terraform で実行すると、Cisco Meraki ダッシュボードにこの例が作成されます。



Layer 3

Inbound rules — Inbound traffic will be restricted to the services and forwarding rules configured below.

Inbound firewall logging — Enable | Disable

Outbound rules

Search... | Add new

#	Policy	Rule description	Protocol	Source	Src port	Destination	Dst port	Syslog	Hits	Actions
1	Allow	Allow POS to Payment Gateway - Primary Processor	TCP	10.7.92.0/24	Any	104.18.15.0/24	443,8443		0	
2	Allow	Allow POS to Payment Gateway - Secondary Processor	TCP	10.7.92.0/24	Any	104.18.14.0/24	443,8443		0	
3	Allow	Allow POS to Card Verification Services	TCP	10.7.92.0/24	Any	192.0.2.0/24	443		0	
4	Allow	Allow POS to Headquarters Inventory System	TCP	10.7.92.0/24	Any	172.16.10.0/24	443,1433		0	
5	Allow	Allow POS Software Updates	TCP	10.7.92.0/24	Any	10.0.100.0/24	443		0	
6	Allow	Allow POS DNS Resolution	UDP	10.7.92.0/24	Any	10.30.10.10/32	53		0	
7	Allow	Allow POS NTP Time Sync	UDP	10.7.92.0/24	Any	10.30.10.20/32	123		0	
8	Deny	Deny All Other Outbound Traffic from POS	Any	10.7.92.0/24	Any	Any	Any		669	
9	Deny	Deny POS to Employee Network	Any	10.7.92.0/24	Any	10.7.91.0/24	Any		0	
10	Deny	Deny POS to Guest Network	Any	10.7.9.0/24	Any	10.7.94.0/24	Any		0	
11	Deny	Deny POS to IoT Network	Any	10.7.92.0/24	Any	10.7.93.0/24	Any		0	
12	Deny	Deny Employee Network to POS	Any	10.7.91.0/24	Any	10.7.92.0/24	Any		0	
13	Deny	Deny Guest Network to POS	Any	10.7.94.0/24	Any	10.7.92.0/24	Any		0	
14	Deny	Deny IoT Network to POS	Any	10.7.93.0/24	Any	10.7.92.0/24	Any		0	

ダイレクト インターネット アクセスおよび VPN 除外ルール

ダイレクト インターネット アクセス（DIA）は、ローカル インターネット ブレークアウトとも呼ばれ、特定のアプリケーションやサービスが、VPN トンネル経由で企業本社にルーティングするのではなく、ブランチロケーションから直接インターネットにアクセスする戦略的トラフィック管理アプローチです。このアーキテクチャでは、ネットワークパフォーマンスを最適化し、WAN 帯域幅の消費を削減し、クラウドベースのアプリ

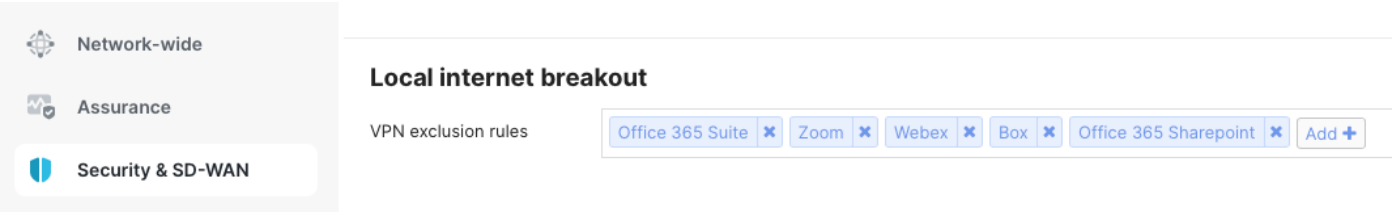
ケーションのユーザー体験を向上させます。一方で、各店舗では Meraki MX セキュリティアプライアンスによるセキュリティ管理と一元化されたポリシーの適用を維持します。

スプリットトンネル アーキテクチャにより、Office 365、ビデオ会議プラットフォーム、および SaaS ビジネスツールなどのクラウドアプリケーションは、近隣のクラウドデータセンターへの最適なルーティングを利用できます。一方で、企業のトラフィックは VPN トンネルを通過して本社に安全に流れ続けます。これにより、セキュリティ要件やコンプライアンス上の義務と、パフォーマンスの最適化とのバランスをとることができます。Office 365、Salesforce、Google Workspace、およびコラボレーション プラットフォームを含むクラウド SaaS アプリケーションでは、ローカルブレークアウトから大きなメリットが得られます。デフォルトでは、HUB によってアドバタイズされた企業サブネットのいずれにも一致しないすべてのブランチトラフィックは、ブランチスポーク MX の 0.0.0.0/0 ルートを使用してインターネットにルーティングされます。スポークが HUB MX からデフォルトルートを受信するフルトンネルモードのシナリオでは、ローカル DIA を通過する必要があるトラフィックの種類を記述する VPN 除外ルールを定義する必要があります。

ブランチでの MX の VPN 除外ルールを設定する YAML ファイルの例を次に示します。

```yaml
appliance:
  traffic_shaping:
    vpn_exclusions:
      major_applications:
        - "meraki:vpnExclusions/application/1"
        - "meraki:vpnExclusions/application/10"
        - "meraki:vpnExclusions/application/6"
        - "meraki:vpnExclusions/application/11"
        - "meraki:vpnExclusions/application/2"
```

この YAML を 'terraform apply' を使用して Terraform で実行すると、Cisco Meraki ダッシュボードにこの例が作成されます。



アプリケーション モニタリングおよびネットワークアラート

Cisco Meraki ダッシュボードでのトラフィック分析

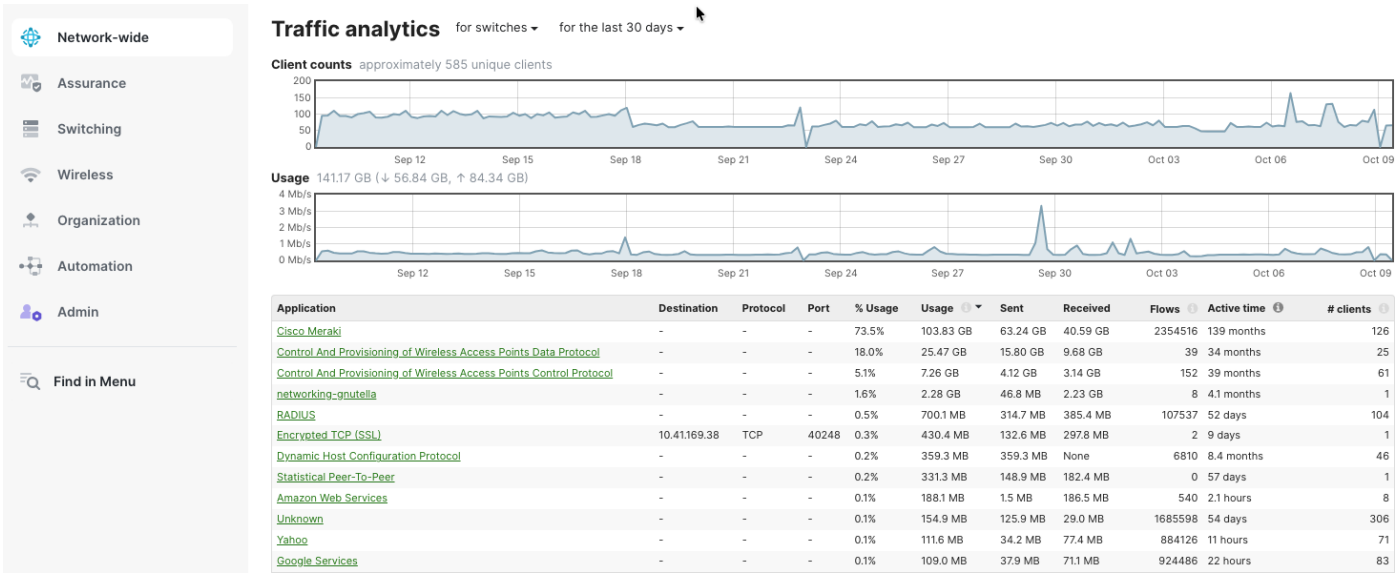
Cisco Meraki ダッシュボードでは、組み込みのトラフィック分析を使用して、すべての小売ロケーションで詳細なアプリケーションの可視性とパフォーマンスのモニタリングを提供します。Cisco Catalyst 9000 スイッチは、Network-Based Application Recognition（NBAR）を使用して、ディープ パケット インスペクション（DPI）と動作分析によって 1,400 を超えるアプリケーションを自動的に特定および分類します。これにより、ネットワークを使用しているアプリケーションを正確に確認でき、インテリジェントな Quality of Service（QoS）、セキュリティ制御、および帯域幅管理の設定に役立ちます。

NBAR を使用すると、ネットワークは POS システムやインベントリ管理などの重要なビジネスアプリケーションを優先順位付けし、重要性の低いトラフィックや娯楽用トラフィックを制限でき、そのすべてが手動でのプロトコルのセットアップなしで行えます。

手順 32。トラフィック分析を使用するには、次の手順を実行します。

ステップ 1. [ネットワーク全体（Network-wide）] > [設定（Configure）] > [トラフィック分析（Traffic Analysis）] に移動して、この機能をオンにします。

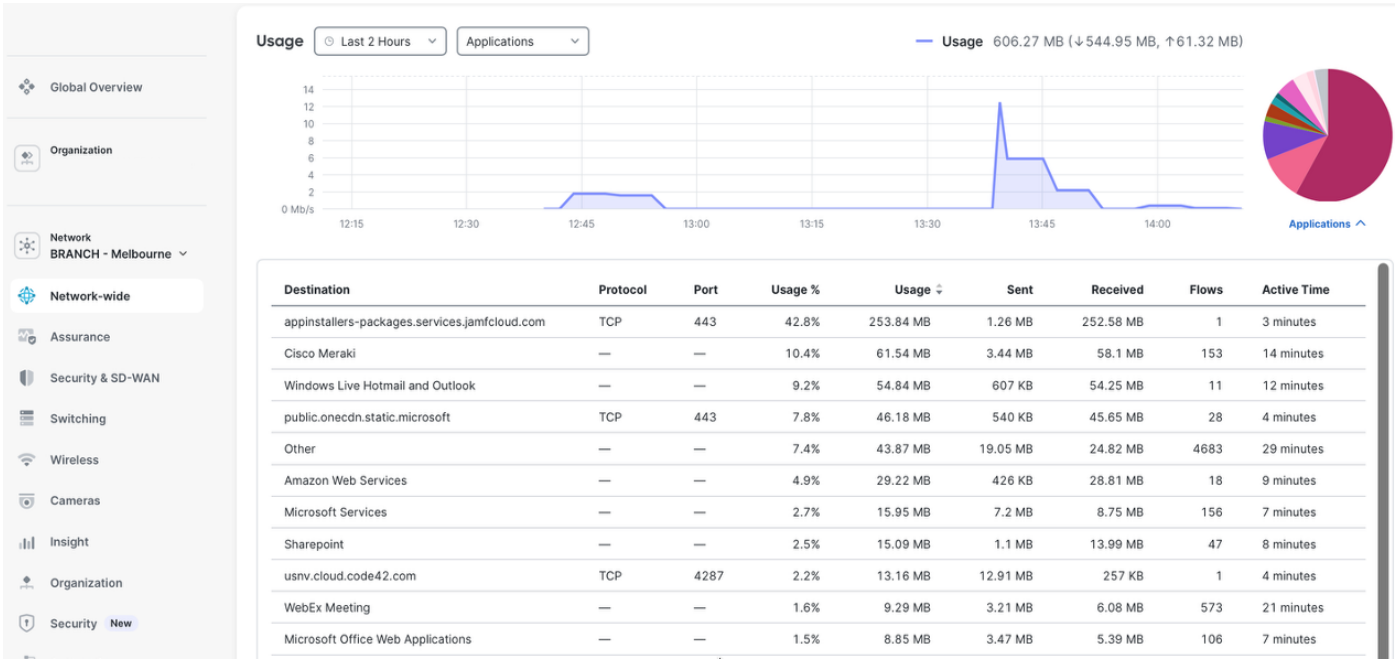
ステップ 2. ネットワーク全体の分析を表示するには、[ネットワーク全体（Network-wide）] > [モニター（Monitor）] > [トラフィック分析（Traffic Analysis）] に移動します。



手順 33。個々のデバイスの分析を確認するには、次の手順を実行します。

ステップ 1. [ネットワーク全体（Network-wide）] > [クライアント（Clients）] の順に選択します。

ステップ 2. 任意のクライアントを選択して、そのデバイスの詳細なアプリケーション使用状況を確認します。



ネットワークアラート

Cisco Meraki ダッシュボードでは、電子メール、SMS、またはウェブフックを使用して通知を送信するなど、ネットワーク全体を対象にカスタマイズ可能なアラートを設定できます。デバイス接続の問題、帯域幅の高使用

率、設定変更、セキュリティインシデント、VPN ステータス、アプリケーション パフォーマンスの低下などに関するアラートを設定できます。

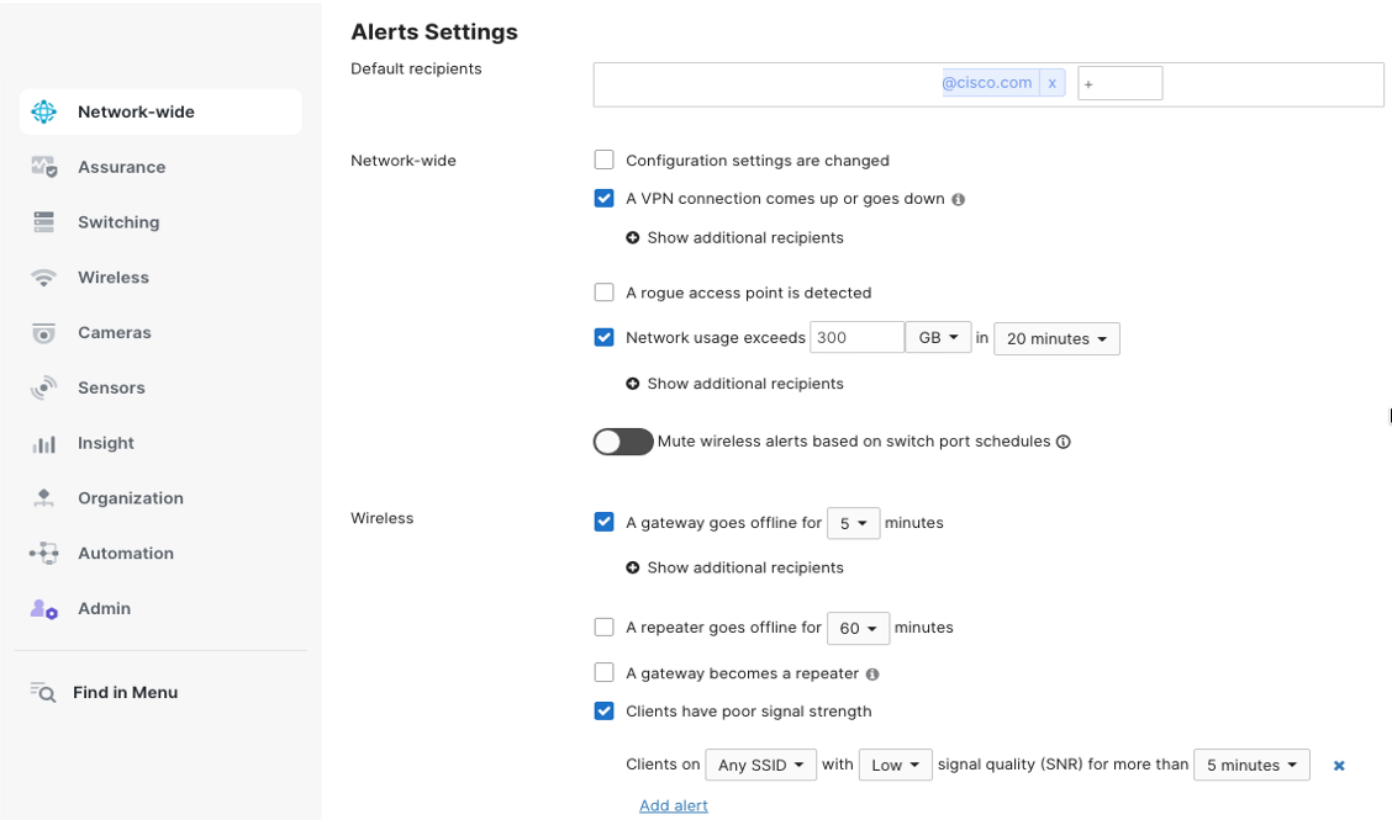
これらのリアルタイム通知により、IT チームは事業運営が影響を受ける前に問題に迅速に対処できます。また、監査や規則遵守のために使用できるアラート履歴も保持します。

適切なチームが自身にとって重要な通知のみを受信するようにロールベースのアラートを設定することで、不要なアラートが減り、すべての小売ロケーションでインシデントをより迅速に解決できます。

手順 34。 アラートを設定するには、次の手順を実行します。

ステップ 1. ダッシュボードで、[ネットワーク全体（Network-wide）] > [設定（Configure）] > [アラート（Alerts）] に移動します。

ステップ 2. 有効にするアラートタイプと通知方法を選択します。



顧客訪問分析

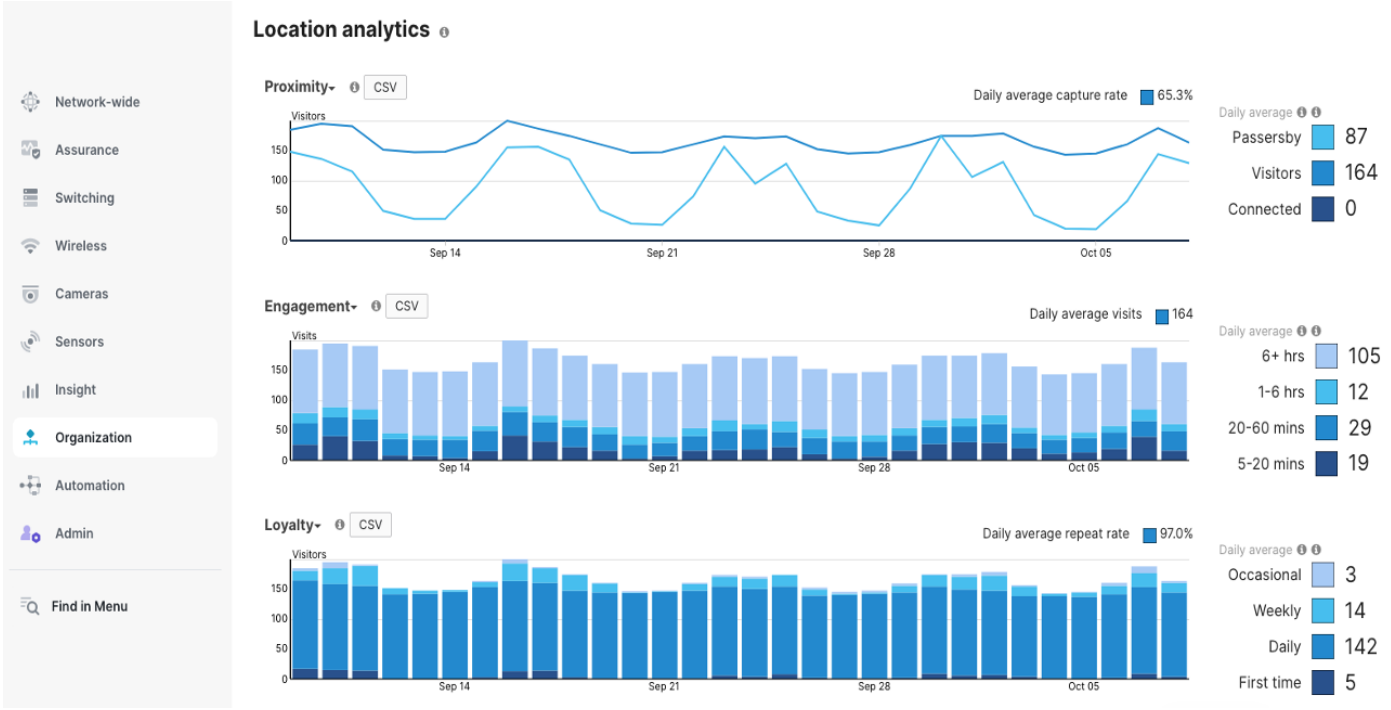
Cisco Meraki ダッシュボードの位置分析は、アクセスポイントのプレゼンス検出とエンゲージメント トラッキングを利用して、Wi-Fi インフラストラクチャをカスタマー インテリジェンス プラットフォームに変換します。MR AP は、範囲内の Wi-Fi 対応デバイスを継続的に検出し、デバイス接続を必要とせずに、訪問者数、滞在時間、再訪問パターン、および歩行者の流れをキャプチャします。管理者は、フロアプラン内にカスタムゾーン（入口エリア、部門、チェックアウトレーン）を設定して、移動パターンや人気のある店舗セクションを分析します。リアルタイムダッシュボードには、現在の混雑状況、ピークトラフィック期間、および訪問者の属性が表示されます。一方で、履歴レポートは、日、週、または月ごとの傾向を示します。キャプティブポータルと統合すると、Wi-Fi ログインを介して顧客の電子メールアドレスと顧客層がキャプチャされ、識別可能な訪問者データにより分析が強化されます。API エクスポートにより、CRM プラットフォーム、マーケティング自動化システム、ビジネス インテリジェンス ツールとのシームレスな統合が可能になり、実用的な小売インサイトを得ることができます。

位置分析と Meraki の連携方法の詳細については、「Location Analytics」を参照してください。

手順 35。 組織のデータを表示するには、次の手順を実行します。

ステップ 1. [ネットワーク全体（Network-wide）] > [設定（Configure）] > [一般（General）] > [ロケーションとスキャン（Location and scanning）] > [分析（Analytics）] の順に選択します。[組織（Organization）] > [ロケーション分析（Location Analytics）] の順に選択します。

ステップ 2. 機能を有効にします。



季節ごとの拡張性と迅速なブランチまたは店舗展開

BaC は、シスコが提供する再利用可能な YAML テンプレートを使用して、小売展開を変革します。テンプレートは、VLAN、ファイアウォールルール、SSID、および AutoVPN 関係などの完全なネットワーク設定を宣言型コードとしてカプセル化します。エンジニアは、サイト名や IP アドレス指定などのロケーション固有のパラメータを含む変数ファイルを変更することで展開をカスタマイズできますが、コアポリシーは変わりません。Terraform はこれらのテンプレートを処理し、手動設定なしで完全に運用可能なブランチを作成します。バージョン管理により、組織の規範を維持しながら、テンプレートの進化、ロールバック機能、およびカスタマイズが可能になります。テンプレートベースの展開により、数百の店舗間で一貫性が確保され、変数によるロケーション固有のカスタマイズもサポートされます。CI/CD 統合によって展開前に設定が検証されるため、エラーが防止され、必要に応じて迅速なロールバックが可能になります。これにより、数週間かかっていた展開サイクルが、店舗での同日アクティベーションに変換されます。

季節限定のポップアップストアやブラックフライデーの拡張では、デバイスを箱から出してそのまま小売ロケーションで展開できます。従業員はケーブル電源とアップリンク接続を使用するだけです。デバイスのシリアル番号を含む BaC テンプレートが Terraform を介して実行されると、デバイスが組織に自動的に要求され、新しく作成されたネットワークに割り当てられ、Cisco Meraki ダッシュボードクラウドからすべての設定がプッシュされます。物理的に接続してから数分以内に、スイッチ、AP、およびセキュリティアプライアンスがポリシーをダウンロードして完全に動作するようになります。これにより、ブランチの展開が、事前ステージングや手動でのダッシュボードの操作なしで、真のプラグアンドプレイのプロビジョニングに変わります。

（組織に合わせて変数値をカスタマイズした）テンプレートを参照して新しいネットワークを作成することにより、新しいブランチまたは店舗を簡単に展開できます。テンプレートはデータフォルダにあります。

手順 36。テンプレートを使用して新しいネットワークを展開するには、次の手順を実行します。

ステップ 1. 組織用にいくつかの変数をエクスポートすることから始めます。

ステップ 2. export MERAKI_API_KEY=cd18a3df66d236xxxxxxxxx738326

ステップ 3. export v3_auth_pass=Lablab123-Lablab123-

ステップ 4. export v3_priv_pass=Lablab123-Lablab123-

ステップ 5. export local_status_page_password=Lablab123-Lablab123-

ステップ 6. export snmp_passphrase=Lablab123-Lablab123-

ステップ 7. export domain=EMEA

ステップ 8. export org_name=RETAIL_AUSTRALIA

ステップ 9. ネットワーク変数は `data/pods_variables.yaml` にあります。要件に応じて各値を変更します。

ステップ 10. 完了したら、新しいブランチを作成するために、`terraform plan` と `terraform apply` を実行します。

この合理化された BaC ワークフローにより、反復可能なバージョン管理された運用によって季節ごとの拡張やポップアップストアの迅速な展開が可能になります。ブラックフライデーやホリデーシーズンなどの繁忙期に、一貫した設定で多数の一時的なロケーションを同時展開し、シーズン後にそれらをデコミッションすることができます。従来は数週間かかっていた手作業が、ダイナミックに変化する小売事業の需要に完全に一致する、自動化されたスケーラブルなインフラストラクチャのプロビジョニングに変わります。

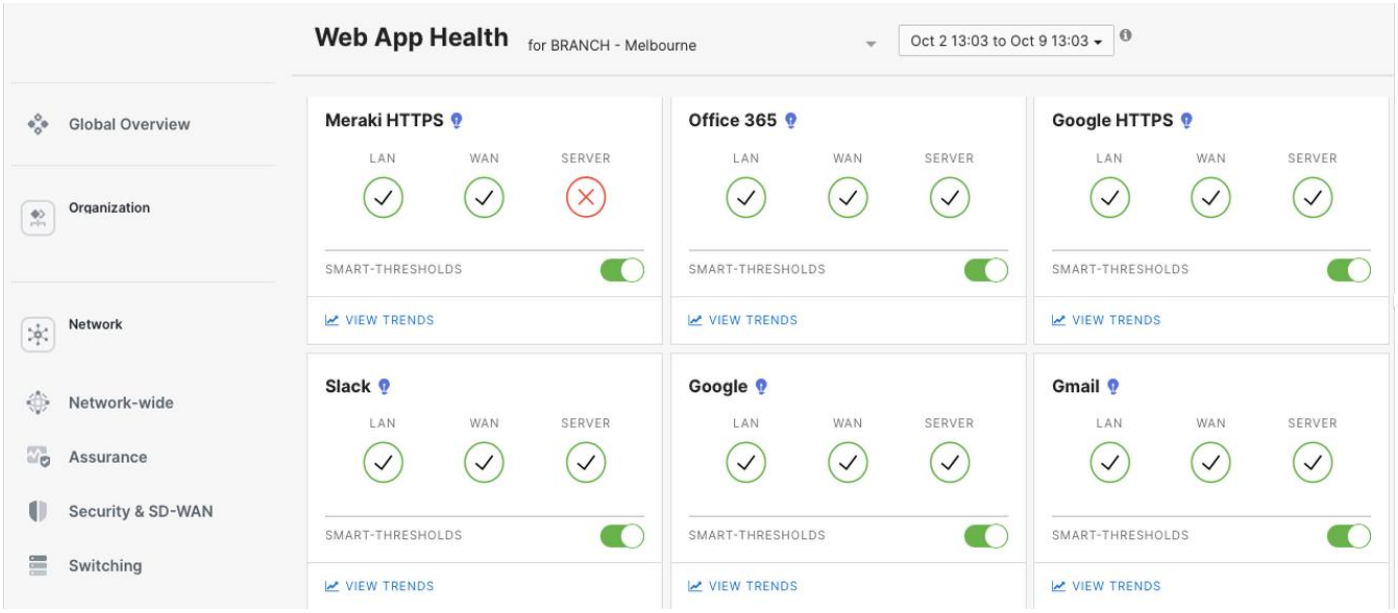
エンドツーエンドのアプリケーション パフォーマンス モニタリング

ThousandEyes を使用した Web アプリケーションの正常性モニタリング

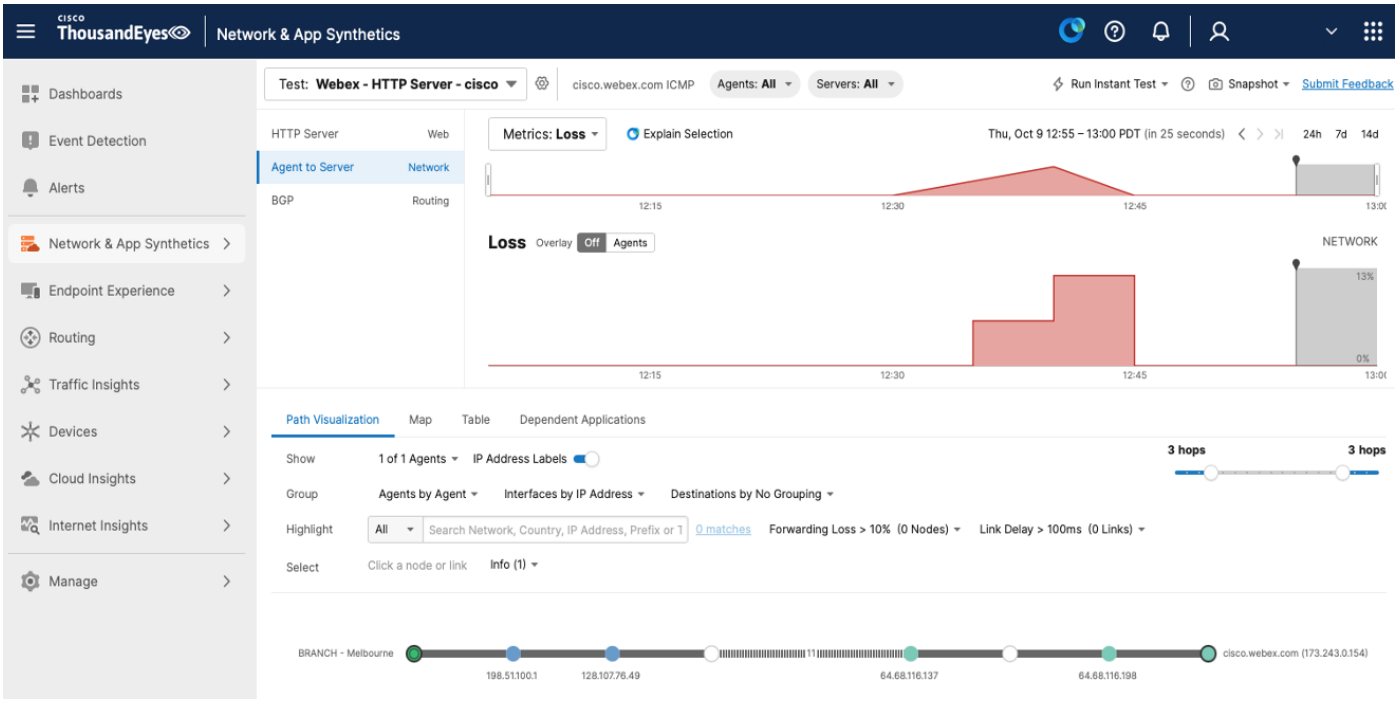
Cisco Meraki ダッシュボードを Cisco ThousandEyes と統合することで、ブランチエッジを超えたエンドツーエンドの WAN の可視性が提供されます。MX アプライアンスに展開された ThousandEyes エージェントは、インターネットおよびマルチクラウド環境全体でアプリケーションのパフォーマンス、パスの可視化、および ISP の正常性を継続的にモニターします。合成テストで、重要な SaaS アプリケーションへの接続を検証します。一方、ホップバイホップのパスの分析は、ネットワーク、ISP、またはアプリケーション プロバイダー インフラストラクチャを問わずパフォーマンス低下が発生している場所を特定することで、より迅速な障害対応とプロアクティブな解決を可能にします。

ThousandEyes を組織に統合するには、[インサイト（Insights）] > [設定（Configure）] > [アクティブアプリケーションモニタリング（Active Application Monitoring）] の順に選択します。

ネットワークのアプリケーションの正常性を確認するには、[インサイト（Insights）] > [Web アプリケーションの正常性（Web App Health）] の順に選択します。



Web アプリケーションの詳細な正常性モニタリングは、特定のアプリケーション エンドポイントを対象として、ThousandEyes ダッシュボード内で HTTP サーバーテストまたはページロードテストを設定することで実現できます。たとえば、Cisco Webex モニタリングでは、管理者はユーザーのログインワークフローをシミュレートする模擬トランザクションテストを展開し、API 応答時間を測定し、SSL 証明書の正常性を検証し、DNS 解決パフォーマンスを追跡します。Meraki MX アプライアンスまたはクラウドの監視ポイントに展開された ThousandEyes エージェントは、設定可能な間隔でこれらのテストを実行し、可用性、応答時間、スループット、パスの可視化などのメトリックをキャプチャします。ThousandEyes ダッシュボードには、ネットワーク パスのパフォーマンス、BGP ルーティングの変更、アプリケーション層のメトリックが示される多層的なビューがあり、チームはホップバイホップ遅延分析とパケット損失の相関関係を使用して、WAN の問題、ISP の問題、Webex インフラストラクチャの劣化を区別することができます。



組織全体のイメージ管理

Cisco Meraki ダッシュボードは、クラウドでオーケストレーションされた自動更新ワークフローを介して、小売企業全体でファームウェアを一元管理します。管理者は、設定可能なメンテナンス期間を使用して、組織全体またはネットワークごとのファームウェアのアップグレードをスケジュールし、非ピーク時のビジネスの中断を最小限に抑えます。企業全体に配布する前にパイロットストアで更新をテストする段階的な展開が可能で、障害検出時の自動ロールバックも含まれます。ダッシュボードには、すべてのデバイスのファームウェア適合性ステータスがリアルタイムで表示され、更新が必要な旧式のスイッチ、AP、セキュリティアプライアンスが強調表示されます。ゼロタッチ自動化により手動介入が不要：デバイスは Meraki クラウドサーバーからファームウェアを自動的にダウンロードし、スケジュールされた期間にインストールし、完了ステータスをレポートします。バージョン固定により、特定のデバイスモデルがテスト済みのファームウェアビルドを維持することができると同時に、アップグレード遅延オプションによって重要なロケーションを制御できます。一元化された可視性によって、アップグレードの進行状況、成功率、および注意が必要な失敗が表示されます。これにより、ファームウェア管理は、複雑で時間のかかるプロセスから、何千もの小売エンドポイントでリスクを軽減できる自動化された運用に変わります。

手順 37。 Cisco Meraki ダッシュボードでファームウェアのアップグレードを管理するには、次の手順を実行します。

ステップ 1. [組織（Organization）] > [ファームウェアのアップグレード（Firmware upgrades）] に移動して、すべてのネットワークと使用可能なファームウェアバージョンを確認します。

ステップ 2. アップグレードするネットワークを、一度に 1 つまたはグループ単位で選択します。

ステップ 3. 使用するファームウェアバージョン（通常は「推奨」バージョン）を選択し、ビジネスに適したメンテナンス期間にアップグレードをスケジュールします。

ステップ 4. より安全に展開するには、最初にいくつかのパイロットストアをアップグレードし、問題がないか確認してから、残りのサイトをアップグレードします。

ステップ 5. スイッチのアップグレードを段階的に管理するには、[スイッチング（Switching）] > [段階的アップグレード（Staged Upgrades）] の順に選択します。スイッチをバケットにグループ化し、アップグレードする順序を設定できます。

ステップ 6. デバイスを特定のファームウェアバージョンに維持するには、必要に応じて自動アップグレードとバージョン固定を設定します。

ステップ 7. リアルタイムで更新されるアップグレードの進行状況を確認し、イベントログをチェックしてアップグレードが成功したことを確認し、問題が発生した場合はロールバックオプションを使用します。

ステップ 8. 電子メールまたは SMS アラートを設定して、アップグレードの進行状況または失敗について通知を受けます。

テクニカルリファレンス

- Onboarding Cloud-Managed Catalyst switches to the Meraki Dashboard
- Cisco Unified Branch Solution Brief
- MX Sizing Guide and Principles

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。