はじめに

Security Cloud Control Firewall Management（旧称 Cisco Defense Orchestrator）は、クラウドベースのプラットフォームで、Cisco のファイアウォールおよびデバイス全体でセキュリティポリシー管理を統合し、簡素化します。ポリシーの一貫性が合理化され、直感的で高度なインターフェイスが提供され、複数のデバイスマネージャ間での設定の変更が調整されます。

Security Cloud Control を使用した Meraki の管理

Meraki MX は、分散展開用に設計されたエンタープライズセキュリティおよびソフトウェア定義ワイドエリアネットワーク（SD-WAN）の次世代ファイアウォール アプライアンスです。Cisco Meraki ダッシュボードは、Cisco Meraki MX をリモートで管理します。Security Cloud Control（旧称 Cisco Defense Orchestrator）を使用して、Cisco Meraki MX デバイスのレイヤ 3 ネットワークルールを管理できます。詳細については、Cisco Meraki の次世代ファイアウォールテクノロジーおよび Cisco Meraki 製品に関する資料を参照してください。

Cisco Meraki デバイスを Security Cloud Control にオンボーディングすると、Security Cloud Control は Cisco Meraki ダッシュボードと通信してそのデバイスを管理します。Security Cloud Control は MX デバイスと直接通信しません。

Security Cloud Control は設定要求を Cisco Meraki ダッシュボードに安全に転送し、その後ダッシュボードが新しい設定をデバイスに適用します。詳細については、Security Cloud Control と Meraki の通信方法 （3 ページ）を参照してください。

Security Cloud Control は、オブジェクトとポリシーの問題を特定し、考えられる修正や代替オプションを提案することで、Cisco Meraki 環境を最適化するツールを提供します。これは、デバイスとテンプレートの両方に関連付けられたポリシーに適用されます。Security Cloud Control を使用して次のことができます。

- 1 つ以上の Meraki デバイスでポリシーを同時に管理します。
- 包括的な環境で、FTD および Cisco ASA デバイスとともに Cisco Meraki ポリシーまたはテンプレートを監視および管理します。

- Meraki テンプレートを使用して複数のネットワークを管理します。
- FTD や Cisco ASA デバイスなど、サポートされている他のプラットフォームとの互換性のあるオブジェクトを使用してアクセスルールをカスタマイズします。

Meraki MX デバイスのオンボーディング

デバイスを Security Cloud Control にオンボーディングする前に、Cisco Meraki ダッシュボードでアカウントを作成し、デバイスまたはテンプレートをダッシュボードにオンボーディングする必要があります。API トークンを生成して Security Cloud Control と通信するためには、組織が Cisco Meraki ダッシュボードにアカウントを持っている必要があります。

Cisco Meraki MX デバイスまたは Cisco Meraki テンプレートのいずれかを Security Cloud Control にオンボーディングできます。

Security Cloud Control コンソールを介して Cisco Meraki MX のログイン情報と権限を処理します。正しいログイン情報または権限がないと、Security Cloud Control は Meraki デバイスと通信できません。

詳細については、「Cisco Meraki MX ログイン情報の更新」および「Cisco Meraki API キーの生成と取得」を参照してください。

Meraki レイヤ 3 ルールと Security Cloud Control

現時点では、Security Cloud Control はレイヤ 3 ファイアウォールルールのみをサポートしています。レイヤ 3 ルールは、OSI モデルのネットワーク層でポリシーを管理することを可能にします。詳細については、「Using Layer 3 Firewall Rules」を参照してください。

Cisco Meraki ダッシュボードでレイヤ 3 アウトバウンドルールを作成できます。Security Cloud Control は、デバイスを Security Cloud Control にオンボーディングするときに、Cisco Meraki ダッシュボードで定義されたレイヤ 3 ルールを読み取ります。その後、FTD または Cisco ASA ルールを管理する場合と同様に、Security Cloud Control でこれらのルールを管理できます。詳細については、「Cisco Meraki アクセス コントロール ポリシーの管理」を参照してください。

オブジェクト

オブジェクトを使用して、新しいアクセス コントロール ポリシーを最適化できます。Cisco Meraki ダッシュボードでは、プロトコルと IP アドレスのグループまたは IP アドレス範囲を使用します。対照的に、Security Cloud Control ではさまざまなオブジェクトを使用してルールを管理します。Security Cloud Control が Cisco Meraki プロトコルをオブジェクトに移行する方法を理解するには、「Cisco Meraki デバイスに関連付けられたオブジェクト」を参照してください。次のオブジェクトを Security Cloud Control で作成して、Cisco Meraki ダッシュボードの IP グループに変換できます。

- ネットワークオブジェクトまたはオブジェクトグループ
- ネットワークサービス（ポート）オブジェクト

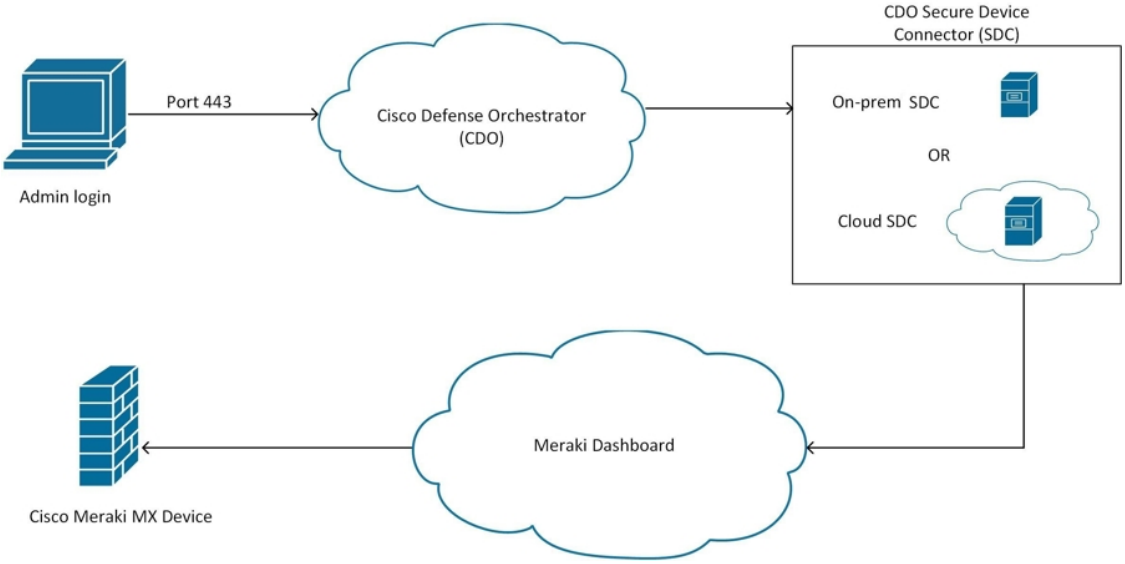
Cisco Meraki ダッシュボードでレイヤ 3 アウトバウンドルールを作成できます。Security Cloud Control は、デバイスを Security Cloud Control にオンボーディングするときに、Cisco Meraki

ダッシュボードで定義したレイヤ 3 ルールを読み取ります。その後、Security Cloud Control で FTD または ASA ルールを管理する場合と同様に、これらのルールを管理できます。Cisco Meraki アクセス コントロール ポリシーの詳細については、「Cisco Meraki アクセス コントロール ポリシーの管理」を参照してください。

Security Cloud Control と Meraki の通信方法

Security Cloud Control から Meraki デバイスへの展開

Security Cloud Control は、設定の変更を Meraki MX デバイスに直接展開しません。展開は複数のステップからなるプロセスです。次の図は、デプロイメントプロセスを示しています。



Meraki MX デバイスの Security Cloud Control で行った設定の変更は、展開を決定するまで Security Cloud Control でステージングされます。設定の変更を展開すると、Security Cloud Control から Meraki ダッシュボードに転送され、Meraki MX デバイスに実装されます。Security Cloud Control はファイアウォールポリシーを管理し、Meraki ダッシュボードはポリシーが適用されるネットワークを管理します。どちらの操作も、Cisco Meraki MX デバイスがネットワークトラフィックを管理および処理する方法に影響を与えます。

古いテナントを持つ一部のお客様は、SDC を介して Meraki MX デバイスを Security Cloud Control に接続する場合があります。そのようなお客様は、この方法を引き続き使用できます。あるいは、Meraki MX を再オンボーディングするか、接続ログイン情報を更新して SDC を削除できます。Security Cloud Control を Meraki MX に接続するために SDC は必要ありません。

Security Cloud Control と Cisco Meraki ダッシュボードの違いの 1 つは、オブジェクトの使用です。Cisco Meraki ダッシュボードで作成されたルールの場合、Security Cloud Control は Meraki の IP アドレスグループまたは IP アドレス範囲を取得し、それらをルールやデバイスポリシーに添付または関連付けできるオブジェクトに変換します。Security Cloud Control で作成されたオブジェクトを Meraki アプライアンスに展開すると、Cisco Meraki ダッシュボードはそれらのオブジェクトを IP アドレスグループまたは IP アドレス範囲に変換し直します。Security Cloud Control 内のオブジェクトは、他のデバイス プラットフォームと互換性があるため、固有かつ

汎用性の高いオブジェクトです。Security Cloud Control でオンボードされた他のデバイスがある場合、すべてのデバイスに対して単一のオブジェクトを作成できる場合があります。Meraki デバイスに関連付けられているオブジェクトの詳細については、「Meraki デバイスに関連付けられるオブジェクト」を参照してください。

関連情報

- Meraki MX の Security Cloud Control へのオンボーディング
- Meraki アクセスコントロールポリシー

Security Cloud Control Firewall Management の概要

Security Cloud Control Firewall Management （旧Cisco Defense OrchestratorまたはCDO）は、Cisco IOS や SSH などの Cisco ファイアウォールやその他のデバイス間でセキュリティポリシーを簡素化し、統合するのに役立つクラウドベースのセキュリティポリシーマネージャです。ファイアウォールとデバイスは、Security Cloud Control ダッシュボードの**[Products]** の下にリストされている **[Firewall]** から管理できます。

Security Cloud Control Firewall Management は、セキュリティポリシー内の不整合を特定し、修正するためのツールを提供することにより、セキュリティポリシーを最適化するのに役立ちます。オブジェクトとポリシーを共有できるだけでなく、設定テンプレートを作成することで、デバイス間でのポリシーの一貫性を維持できます。

Security Cloud Control Firewall Management は Cisco Adaptive Security Device Manager（ASDM）と共存するため、ASDM によって行われた設定の変更が追跡され、違いが調整されます。

さまざまなデバイスを一元的に管理できます。上級ユーザーは、従来の CLI インターフェイスに新しい機能拡張を追加して、管理の効率をさらに向上させます。

Security Cloud Control Firewall Management では、ガイド付きの「Day 0」エクスペリエンスも提供され、Threat Defense デバイスをオンプレミスまたは クラウド提供型 Firewall Management Center にすばやくオンボーディングできます。また、有効化および設定するのに役立つその他の主要な機能も紹介されています。

デバイスのオンボーディング要件

デバイスを導入準備する前に、次の前提条件を満たしてください。

- インストール構成ウィザードを完了します。
- デバイスのライセンスを取得します。

これらの前提条件を満たした後、 Security Cloud Control Firewall Management オンボーディングウィザードを使用してデバイスを導入準備します。

「デバイスとサービスの導入準備」を参照してください。

次の制約事項に注意してください。

- 組織に関連付けられている Security Cloud Control Firewall Management にデバイスを導入準備した後は、それらのデバイスを別の組織に移行できません。
- デバイスを新しい組織に移動するには、新しい組織にデバイスを再度オンボーディングする必要があります。

Security Cloud Control のサポート対象デバイスの完全なリストについては、Security Cloud Control Firewall Management でサポートされるデバイス、ソフトウェア、ハードウェア を参照してください。

シスコ オンライン プライバシー ポリシー

Cisco Systems, Inc. およびその子会社（以下総称して「シスコ」といいます）は、皆様のプライバシーを保護し、シスコの Web サイト、ならびに製品およびサービス（以下「ソリューション」）を快適にお使いいただけるよう全力を尽くします。『シスコ オンライン プライバシー ポリシー』をよく読み、シスコがユーザーの個人情報を収集、使用、共有、保護する方法を明確に理解してください。

Security Cloud Control Firewall Management ダッシュボード

Security Cloud Control Firewall Management ダッシュボードは、さまざまなカテゴリにわたって組織レベルの詳細をモニタリングおよび管理するための中央ハブです。ログインすると、セキュリティと運用の効率を最適化するための重要なインサイトとアクションを提供するカスタマイズ可能なダッシュボードにアクセスできます。

ダッシュボードをカスタマイズする

表示されるウィジェットをカスタマイズして、特定のニーズに合わせてダッシュボードをカスタマイズします。

1. **[Home]** ページで、**[Customize]** をクリックします。
2. ダッシュボードウィジェットを選択または選択解除し、ドラッグアンドドロップして希望の順序に配置します。

上位情報

このセクションでは、さまざまなテナントレベルのメトリックに関する詳細なインサイトが提供されます。有効にすると、次のウィジェットが表示できます。

- **設定状態**：デバイス上の設定と、Security Cloud Control によって維持されているデバイス上の設定との不一致を示します。この比較は、存在する可能性のある不整合や競合を特定するのに役立ちます。

  詳細については、「デバイス管理」を参照してください。

- **変更ログ管理**： 変更ログを管理して、正確な運用管理を実現できます。ウィジェットには、**完了済み**の変更ログと**保留中**の変更ログが表示されます。

  詳細については、「ログの変更」を参照してください。

- **RA VPN セッション**：リモートアクセス VPN セッションをモニターするのに役立ちます。

  詳細については、「RA VPN セッション」を参照してください。

- **全体のインベントリ**：すべてのデバイスの正常性とステータスをモニターするのに役立ちます。ウィジェットには、**[Issues]**、**[Pending Actions]**、**[Other]**、**[Online]** に分類されたデバイス、およびハードウェアサポートの最終日に近づいているデバイス、またはすでにハードウェアサポートの最終日に達しているデバイスが表示されます。

  詳細については、「すべてのデバイス」を参照してください。

- **サイト間 VPN**：サイト間 VPN 接続を管理および評価するのに役立ちます。ウィジェットには、VPN トンネルの総数と、**アクティブ**および**アイドル**の割合が表示されます。

  詳細については、「サイト間 VPN」を参照してください。

- **アカウントとアセット**：
  - マルチクラウドアカウントとリソースを効果的に追跡および管理できます。ここから Multicloud Defense Controller を起動できます。
  - **[+Add Account]** をクリックして、新しいアカウントを追加します。

  詳細については、「Multicloud Defense コントローラ」を参照してください。

- **トップリスク接続先**：アクセスが許可されている最も高リスクの接続先を特定してモニターするのに役立ちます。ウィジェットには、アプリケーションおよび URL カテゴリが一覧表示され、過去 90、60、または 30 日間のデータをフィルタ処理できます。**許可された**トラフィック（デフォルト）と**ブロックされた**トラフィックの間でフィルタ処理できます。

- **上位の侵入およびマルウェアイベント**：上位の侵入およびマルウェアイベントをモニターして対処するのに役立ちます。ウィジェットには、侵入イベントとマルウェアイベントが表示され、過去 90 日間、60 日間、および 30 日間のデータをフィルタ処理できます。**許可された**イベント（デフォルト）と**ブロックされた**イベントの間でフィルタ処理できます。

アナウンスメント

[Announcements] アイコンをクリックすると、最新の Security Cloud Control 機能と更新を確認できます。リストされている項目のいずれかについて詳細が必要な場合は、関連ドキュメントへのリンクが提供されます。

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。