

Meraki デバイスの設定

- Security Cloud Control Firewall Management でのセキュリティポリシーの管理 （1 ページ）
- Meraki テンプレート, on page 3
- 共有オブジェクト, on page 4
- オブジェクトフィルタ, on page 5
- Meraki ローカル ネットワーク オブジェクトの作成 （7 ページ）
- Meraki デバイスに関連付けられるオブジェクト, on page 12

Security Cloud Control Firewall Management でのセキュリティポリシーの管理

セキュリティポリシーは、目的の宛先へのトラフィックを許可するか、セキュリティ脅威が特定された場合にトラフィックをドロップすることを最終的な目標として、ネットワークトラフィックを検査します。Security Cloud Control を使用して、さまざまな種類のデバイスでセキュリティポリシーを設定できます。

Meraki アクセスコントロールポリシー

Meraki MX デバイスは、Security Cloud Control にオンボーディングする前に Meraki ダッシュボードによって管理されていた可能性があり、デバイスにはすでにいくつかのアウトバウンドルールが設定されている可能性があります。これらのルールは、Security Cloud Control でアクセス制御ルールとして表示されます。

これらのルールを変更し、アクセスコントロールポリシー内に追加のルールを作成できます。アクセスコントロールポリシーをカスタマイズするには、オブジェクトを作成してアタッチします。関連情報については、関連する記事のセクションを参照してください。

Note Meraki アクセスコントロールポリシーのアクションは、デフォルトで [許可（Allow）] です。このアクションを変更することはできません。

Security Cloud Control を使用して Meraki アクセス コントロール ポリシーを編集するには、次の手順を使用します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 [テンプレート（Templates）] タブをクリックします。

ステップ 4 [Meraki] タブをクリックし、アクセス コントロール ポリシーを編集する Meraki MX デバイステンプレートを選択します。

ステップ 5 [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 6 次のいずれかを実行します。

- 新しいルールを作成するには、追加ボタン（）をクリックします。
- 既存のルールを編集するには、ルールを選択し、**[アクション（Actions）]**ペインの編集ボタン（）をクリックします。編集モードに入らずに簡単なインライン編集を行うことができます。
- 不要になったルールを削除するには、ルールを選択し、[アクション（Actions）] ペインで [削除（Remove）] ボタン をクリックします。
- ポリシー内でルールを移動させるには、アクセス コントロール テーブルでルールを選択し、ルールの行の最後にある上下の矢印をクリックしてルールを移動します。

ステップ 7 [順序（Order）] フィールドで、ポリシー内のルールの位置を選択します。ネットワークトラフィックは、ルールのリストに照らして 1 から「最後」の番号までの順に評価されます。

ルールは最初の一致に基づいて適用されます。特定のトラフィック一致基準を持つルールは、同じトラフィックに適用される一般的な基準を持つポリシーよりも前に配置する必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 8 ルール名を入力します。英数字、スペース、および次の特殊文字を使用できます：+ . _ -

Note アクセス制御ルールの [名前（Name）] は Security Cloud Control のルール名として使用されます。一方、**[備考（Remark）]**フィールドは Meraki ダッシュボードのルール名として扱われます。この 2 つのフィールドは互いに依存していません。

ステップ 9 ネットワークトラフィックがルールに一致する場合に適用するアクションを選択します。

- [Block]：トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。

- [Allow]：ポリシーで侵入およびその他のインスペクション設定の対象となるトラフィックを許可します。

Note ルールアクションのみを設定または変更できます。デフォルトポリシーのアクションを Security Cloud Control から変更することはできません。

ステップ 10 次のタブ内の属性を任意に組み合わせて、トラフィック一致基準を定義します。

- **[Source]**：**[送信元（Source）]** タブをクリックして、ネットワーク（ネットワークと大陸を含む）またはネットワークトラフィック発信元ポートを追加または削除します。デフォルト値は、[任意（Any）] です。
- [Destination]：[宛先（Destination）] タブをクリックして、ネットワーク（ネットワークと大陸を含む）またはネットワークトラフィック着信ポートを追加または削除します。デフォルト値は、[任意（Any）] です。

Note 送信元および宛先のネットワークは、設定されたいずれかの VLAN サブネット内にある必要があります。または、VLAN サブネットが手動で設定されていない場合は、デフォルトの VPN サブネット内にある必要があります。無効な送信元または接続先ネットワークを含むルールの展開は失敗します。

ステップ 11 [保存（Save）] をクリックします。

ステップ 12 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Meraki テンプレート

Meraki テンプレートは、複数のサイト/ネットワークで共有できるネットワーク設定です。個々のサイトネットワークをテンプレートネットワークにバインドできます。単一のテンプレートに変更を加えると、バインドされるすべてのネットワークが自動的に更新されます。バインドされたネットワークは、Security Cloud Control のバインドされたデバイスとして表示できます。この設定は、異なる場所にある複数のネットワークに 1 つのポリシーを適用する場合に最適です。

1 つのテンプレートに対して複数のネットワークを設定する方法については、「設定テンプレートを使用した複数のネットワークの管理」を参照してください。.Cisco Meraki テンプレート、テンプレートの計画、およびセットアップの詳細については、「Meraki Templates Best Practices」を参照してください。

Cisco Meraki デバイスの管理と同じ方法で、Meraki テンプレートを管理します。最初に、Cisco Meraki ダッシュボードを使用してテンプレートを設定し、Security Cloud Control にオンボーディ

ングします。テンプレートを Security Cloud Control にオンボーディングすると、既存のルールまたは IP のグループが Security Cloud Control に読み込まれ、オブジェクトに変換されます。同期後、[セキュリティデバイス（Security Devices）] ページの [デバイスの詳細（Device Details）] ペインで、テンプレート名と関連するネットワークの数が（バインドされたデバイスとして）表示されます。テンプレートに関連付けられたポリシーとバインドされたネットワークを Security Cloud Control から管理、変更、デプロイすることも可能です。Security Cloud Control への Cisco Meraki テンプレートのオンボーディングの詳細については、「Security Cloud Control へのCisco Meraki テンプレートのオンボーディング」を参照してください。

共有オブジェクト

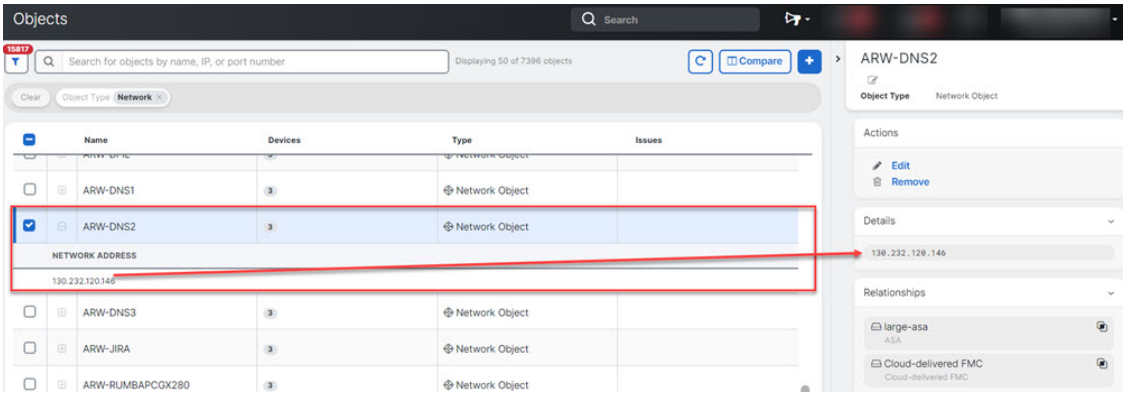
共有オブジェクトは、複数のデバイス上の同じ名前と同じ内容を持つオブジェクトです。1 つの共有オブジェクトの変更がそのオブジェクトを使用するすべてのポリシーに影響するため、共有オブジェクトはポリシーの維持に役立ちます。

共有オブジェクトはこのアイコンで識別されます。



これは、[オブジェクト（Objects）]ページに表示されます。共有オブジェクトを使用すると、1 ヵ所でオブジェクトを変更でき、その変更がそのオブジェクトを使用する他のすべてのポリシーに影響するため、ポリシーの維持が容易になります。共有オブジェクトを使用しない場合は、同じ変更が必要なすべてのポリシーを個別に変更する必要があります。

共有オブジェクトを調査する場合、Security Cloud Control ではオブジェクトの内容がオブジェクトテーブルに表示されます。共有オブジェクトの内容はまったく同じです。Security Cloud Control では、オブジェクトの要素の結合された、つまり「フラット化された」ビューが詳細ペインに表示されます。詳細ペインでは、ネットワーク要素が単純なリストにフラット化されており、名前付きオブジェクトに直接関連付けられていないことに注意してください。

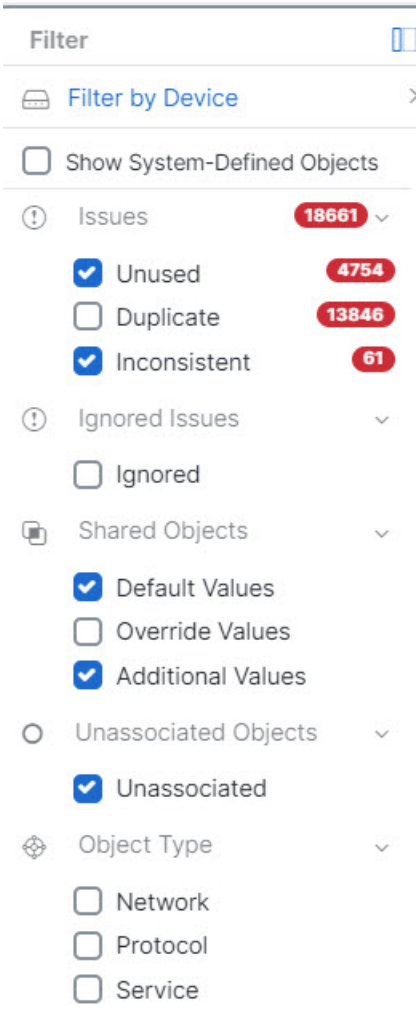


オブジェクトフィルタ

[オブジェクト（Objects）]ページのフィルタを使用して、デバイス、問題、共有状態、関連付け状態、オブジェクトタイプ、または検索値でオブジェクトを検索します。また、システム定義オブジェクトを含めたり除外したりすることもできます。

オブジェクトタイプフィルタを使用すると、ネットワークオブジェクト、ネットワークグループ、URL オブジェクト、URL グループ、サービスオブジェクト、サービスグループなどのオブジェクトタイプでフィルタリングできます。共有オブジェクトフィルタを使用すると、デフォルト値、オーバーライド値、または追加の値を持つオブジェクトをフィルタリングできます。

デバイスフィルタとオブジェクトフィルタを組み合わせて、焦点を絞った検索ストラテジーを作成できます。たとえば、次のロジックに一致するオブジェクトを検索できます。[問題（Issues）] は [未使用（Unused）] OR [不整合（Inconsistent）] であり、AND [共有オブジェクト（Shared Objects）] は [デフォルト値（Default Values）] OR [追加の値（Additional Values）] で、AND [関連付けられていないオブジェクト（Unassociated Objects）] が選択されます。



フィルタ処理するには、[オブジェクト（Objects）] タブの左側のペインで [フィルタ処理（Filter）] をクリックします。

- [デバイスでフィルタリング（Filter by Device）]：選択したデバイスで見つかったオブジェクトを表示します。
- [システム定義オブジェクトの表示（Show System-Defined Objects）]：検索およびフィルタリングの結果に事前定義されたシステムオブジェクトが含められます。システムオブジェクトは編集または削除できません。一部のデバイスには、一般的なサービス用に事前定義されたオブジェクトがあります。これらのシステムオブジェクトは既に作成されており、ルールやポリシーで使用できるので便利です。オブジェクトテーブルには多くのシステムオブジェクトが含まれる場合があります。システムオブジェクトは編集または削除できません。
- [問題（Issues）]：未使用の、重複している、または不整合なオブジェクトを表示します。複数の問題を選択した場合、選択したすべての問題カテゴリのオブジェクトが含められます。

- [無視された問題（Ignored Issues）]：管理者によって無視された問題を含むオブジェクトを表示します。
- [共有オブジェクト（Shared Objects）]：共有オブジェクトを表示します。デフォルト値、オーバーライド値、追加の値、またはこれらの組み合わせでフィルタリングできます。
- [関連付けられていないオブジェクト（Unassociated Objects）]：ルールまたはポリシーに関連付けられていないすべてのオブジェクトを表示します。
- [オブジェクトタイプ（Object Type）]：ネットワークオブジェクト、ネットワークグループ、URL オブジェクト、URL グループ、サービスオブジェクト、サービスグループなど、選択したタイプのオブジェクトを表示します。

メインフィルタ内でサブフィルタを使用して、ネットワーク、サービス、プロトコルなどのオブジェクトタイプで結果をさらに絞り込めます。複数のカテゴリでのフィルタリングは、AND 関係と組み合わされます。1 つのカテゴリ内での複数選択は、OR 関係と組み合わせることができます。

たとえば、フィルタセットで、次のロジックに一致するオブジェクトを検索できます：選択したデバイス上のオブジェクト AND 不整合オブジェクト AND ネットワークオブジェクトまたはサービスオブジェクト AND [group] を含むオブジェクト名。

Meraki ローカル ネットワーク オブジェクトの作成

ローカルの Meraki ネットワークオブジェクトは、Cisco Meraki ダッシュボードで作成する必要があります。Security Cloud Control にまだオンボードされていない Meraki デバイスがある場合、既存のローカルオブジェクトはすべてデバイスと一緒にオンボードされます。**オンボード済みの** Meraki デバイスがある場合は、Security Cloud Control でデバイスを同期して、新しい構成とローカルオブジェクトを読み取ります。

（注） Meraki ネットワークオブジェクトやネットワーク オブジェクト グループを参照するデバイス構成が Security Cloud Control UI でオンボードまたは同期されると、これらのオブジェクトは **FTD 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として表示されます。

これらのオブジェクトおよびオブジェクトグループは、Security Cloud Control では**読み取り専用**になります。

始める前に

Meraki の**オープン ベータ ネットワーク オブジェクト**を有効にしていない場合は、Cisco Meraki ダッシュボードにログインし、**組織** > **ポリシーオブジェクト** に移動して、ローカルオブジェクトとオブジェクトグループに登録してアクセスします。

手順

ステップ 1 Meraki ダッシュボードにログインし、ローカルオブジェクトまたはローカルオブジェクトグループを作成します。詳細については、『Network Objects Configuration Guide』を参照してください。

ステップ 2 Security Cloud Control にログインします。

注：Meraki デバイスを Security Cloud Control にまだオンボードしていない場合は、詳細についてSecurity Cloud Control への MX デバイスのオンボードを参照してください。デバイスをオンボーディングすると、既存のすべてのオブジェクトもオンボーディングされます。

ステップ 3 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 4 Meraki デバイスを見つけて選択し、デバイスの行が強調表示されるようにします。デバイスのステータスは [競合が検出されました] になっています。右側のペインで、[競合の確認] を選択してデバイスの構成に追加された変更を確認するか、[確認せずに承認] を選択してすべての構成変更を承認します。

Merakiネットワークオブジェクトまたはネットワークグループの作成または編集

MX デバイスは Firepower および ASA **ネットワークオブジェクト**と同じ形式を使用し、CIDR 表記で表されたホスト名、IP アドレス、またはサブネットアドレスを含めることができます。**ネットワークグループ**は、ネットワークオブジェクトと、グループに追加するその他の個々のアドレスまたはサブネットのコレクションです。ネットワークオブジェクトとネットワークグループは、アクセスルールで使用されます。Security Cloud Control を使用して、ネットワークオブジェクトとネットワークグループを作成、読み取り、更新、および削除できます。

ネットワークオブジェクトに追加できる IP アドレス

デバイス タイプ（Device Type）	[IPv4 / IPv6]	シングル アドレス	アドレス範囲	完全修飾ドメイン名	CIDR 表記法によるサブネット
MX	IPv4	対応	対応	非対応	対応

Note クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

Note クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

Meraki ネットワークオブジェクトの作成

Note クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3 をクリックしてから、**[FTD]** > **[ネットワーク（Network）]**または**[ASA]** > **[ネットワーク（Network）]** をクリックします。

ステップ 4 オブジェクト名を入力します。

ステップ 5 [ネットワークオブジェクトの作成（Create a network object）] を選択します。

ステップ 6 [値（Value）] セクションで、単一の IP アドレスまたは CIDR 表記で表されるサブネットアドレスを入力します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Meraki ネットワークグループの作成

ネットワークグループは、複数のネットワークオブジェクトまたは IP アドレスで構成されます。

ネットワークグループをネットワークオブジェクトで構成する場合は、上記の「ネットワークオブジェクトの作成」の手順を使用して、IP アドレスごとに個別のネットワークオブジェクトを作成します。

Note クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側の Security Cloud Control ナビゲーションバーで、**オブジェクト** をクリックします。

ステップ 3 をクリックしてから、**[FTD]** > **[ネットワーク（Network）]**または**[ASA]** > **[ネットワーク（Network）]** のいずれかをクリックします。

ステップ 4 オブジェクト名を入力します。

ステップ 5 [ネットワークグループの作成（Create a network group）] を選択します。

ステップ 6 [オブジェクトの追加（Add Object）] をクリックし、リストからネットワークオブジェクトを選択して、[選択（Select）] をクリックします。必要なすべてのネットワークオブジェクトを追加するまで、この操作を繰り返します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Firepower ネットワークオブジェクトまたはネットワークグループの編集

Note クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3 オブジェクトフィルタと検索フィールドを使用して、編集するオブジェクトを見つけます。

ステップ 4 編集するオブジェクトを選択します。

ステップ 5 [詳細（details）] ペインの [編集（edit）] ボタン をクリックします。

ステップ 6 前述の手順で作成したのと同じ方法で、ダイアログボックスの値を編集します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 Security Cloud Control は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。

ステップ 9 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Security Cloud Control のネットワークオブジェクトとグループの削除

クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

オブジェクトページからネットワークオブジェクトまたはグループを削除すると、クラウド提供型 Firewall Management Center の **オブジェクト** ページから重複するネットワークオブジェクトまたはグループが削除されます。その逆も同様です。

Meraki デバイスに関連付けられるオブジェクト

Meraki デバイスで使用されるオブジェクトについて

Meraki ダッシュボードは、アウトバウンドアクセス制御ルールの送信元および宛先フィールドに指定された IP アドレス、プロトコル、またはポート範囲のグループを利用します。オンボーディングすると、Security Cloud Control は、IP アドレスをネットワークオブジェクトに変換し、アプリケーションレイヤのプロトコル値をサービスオブジェクトまたはプロトコルオブジェクトに変換します。

Security Cloud Control の 1 つのルールがダッシュボードで複数のルールに変換される可能性があります。たとえば、TCP プロトコルと UDP プロトコルの両方を含む ASA プロトコルグループを Security Cloud Control の単一のアクセス制御ルールに追加すると、Security Cloud Control は 1 つの Security Cloud Control ルールをダッシュボード内の複数のルールに変換します。変換後のルールは、TCP プロトコルを含む 1 つのルールと UDP プロトコルを含む 1 つのルールになります。

Meraki ダッシュボードと Security Cloud Control はどちらも CIDR サブネット表記をサポートしていることに注意してください。レイヤ 3 スイッチインターフェイスと MX デバイスレイアウトの詳細については、Meraki ナレッジベースを参照してください。

Security Cloud Control の Meraki デバイスで使用できるオブジェクト

Security Cloud Control には、MX デバイス専用のオブジェクトはありません。代わりに、FTD、FDM および ASA オブジェクトを作成または共有し、デバイスに展開されるルールにこれらのオブジェクトを関連付けることができます。Meraki には FTD および ASA オブジェクトとの完全な互換性がないため、MX デバイスがオブジェクトを使用する方法に影響するいくつかの制限がある可能性があります。

FTD、FDM または ASA オブジェクトを MX デバイスに関連付けると、そのオブジェクトが共有されるようになることに注意してください。関連付けられたオブジェクトへの変更は、そのオブジェクトが共有されているすべてのデバイスに影響し、デバイスの設定ステータスには [未同期（Not Synced）] と表示されます。詳細については、「共有オブジェクト」を参照してください。オブジェクトに影響する付加的なオブジェクト状態については、このページの下部に表示されている「**関連記事**」セクションを参照してください。

Meraki は、IPv6 アドレスまたは FQDN を含むオブジェクトをサポートしていません。

Security Cloud Control のオブジェクト	Meraki との互換性あり
プロトコルオブジェクト	TCP、UDP、ICMP
ネットワーク オブジェクト	○

Security Cloud Control のオブジェクト	Meraki との互換性あり
ネットワーク グループ	○
サービス オブジェクト	○
ASA サービスグループ	×
FTD サービスグループ	×

Meraki クラウドのローカル ネットワーク オブジェクトおよびオブジェクトグループ

ネットワークオブジェクトとオブジェクトグループを使用すると、Merakiデバイスのファイアウォールルールを簡単に管理できます。これらは、ファイアウォールルールなどのアクセスポリシーで使用できる IP サブネットおよび FQDN のラベルとして機能します。同じ IP サブネットや FQDN を使用する複数のアクセスポリシーを変更する必要がある場合は、ネットワークオブジェクトを変更して、すべてのポリシーに反映させるだけです。現時点では、Meraki ダッシュボードを使用して、これらのオブジェクトを作成および変更する必要があります。お使いの環境でネットワークオブジェクトを使って何ができるのかについては、Meraki の『ネットワークオブジェクトのハイライト』[英語] を参照してください。

Note Meraki ネットワークオブジェクトやネットワーク オブジェクト グループを参照するデバイス設定が Security Cloud Control UI にオンボードまたは同期されると、これらのオブジェクトは **FTD ネットワークオブジェクト**として表示されます。

これらのオブジェクトおよびオブジェクトグループは、Security Cloud Control では**読み取り専用**になります。

Security Cloud Control での Meraki ルールの表示

デバイスのポリシーページからオブジェクトを表示するか、デバイスに基づいてオブジェクトページをフィルタ処理できます。ポリシーページから、アクセス制御ルールの表示、編集、および並べ替えを実行できます。Security Cloud Control は、Meraki ダッシュボードからのアウトバウンドルールをオブジェクトへのアクセス制御ルールに変換するため、Meraki ダッシュボードからのルールとプロトコルの表示が変更される場合があります。次の表は、Security Cloud Control へのデバイスのオンボーディングを完了した後のプロトコルの新しい名前を示しています。

Meraki ダッシュボードでのルールまたはプロトコルのヘッダー	Security Cloud Control でのルールまたはオブジェクトのヘッダー
ポリシー	操作
[ソースIP（Source IP）]	ネットワークオブジェクトまたはネットワークグループ

Meraki ダッシュボードでのルールまたはプロトコルのヘッダー	Security Cloud Control でのルールまたはオブジェクトのヘッダー
[宛先 IP アドレス（Destination IP）]	ネットワークオブジェクトまたはネットワークグループ
送信元ポート（Source Port）	ネットワークオブジェクトまたはネットワークグループ
[宛先ポート（Destination Port）]	ネットワークオブジェクトまたはネットワークグループ
レイヤ 3 アプリケーションプロトコル	ポート（プロトコルグループ、ポートグループ、またはサービスオブジェクト）

次の例は、Meraki ダッシュボードからのアウトバウンドルールが Security Cloud Control でどのように表示されるかを示しています。



Meraki サービスオブジェクトの作成または編集

サービスオブジェクトの概要

サービスオブジェクトは、TCP/IP プロトコルとポートを指定する再利用可能なコンポーネントです。Security Cloud Control は、これらのオブジェクトをサービスオブジェクトとして分類します。MX デバイスに展開すると、Security Cloud Control はオブジェクトをプロトコルまたはポート範囲に変換します。Security Cloud Control が Meraki プロトコルをオブジェクトとして処理する方法の詳細については、Meraki デバイスに関連付けられるオブジェクト, on page 12を参照してください。

サービスオブジェクトの作成

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3  をクリックしてから、**[FTD]** > **[サービス（Service）]** または **[ASA]** > **[サービス（Service）]** をクリックします。

ステップ 4 オブジェクト名と説明を入力します。

ステップ 5 [サービスオブジェクトの作成（Create a service object）] を選択します。

ステップ 6 [サービスタイプ（Service Type）] ボタンをクリックし、オブジェクトを作成するプロトコルを選択します。

ステップ 7 次のいずれかのアクションを実行して、プロトコルを識別する情報を入力します。

- TCP または UDP ポートの特定のポート番号を入力します。
- ICMP または ICMPv6 メッセージタイプを選択します。
- 「その他」のサービスタイプを選択した場合は、リストから TCP/IP プロトコルの 1 つを選択します。

ステップ 8 [追加（Add）] をクリックします。

ステップ 9 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

サービスグループを作成する

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3  をクリックしてから、**[FTD]** > **[サービス（Service）]** をクリックします。



Note Meraki は ASA サービスグループをサポートしていません。

ステップ 4 オブジェクト名と説明を入力します。

ステップ 5 [サービスグループの作成（Create a service group）] を選択します。

ステップ 6 [オブジェクトの追加（Add Object）] をクリックし、オブジェクトを選択して [選択（Select）] をクリックすることで既存のオブジェクトを追加します。このステップを繰り返してさらにオブジェクトを追加します。

ステップ 7 サービスオブジェクトとサービス値のサービスグループへの追加が完了したら、[追加（Add）] をクリックします。

ステップ 8 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

サービスオブジェクトまたはサービスグループの編集

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3 オブジェクトをフィルタリングして編集するオブジェクトを見つけ、オブジェクトテーブルでオブジェクトを選択します。

ステップ 4 詳細ペインで、[編集（Edit）] をクリックします。

ステップ 5 前述の手順で作成したのと同じ方法で、ダイアログボックスの値を編集します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 Security Cloud Control は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。これで、オブジェクトを Meraki ポリシーで使用する準備ができました。

ステップ 8 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Firepowerネットワークオブジェクトまたはネットワークグループの編集

Note クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、およびFTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3 オブジェクトフィルタと検索フィールドを使用して、編集するオブジェクトを見つけます。

ステップ 4 編集するオブジェクトを選択します。

ステップ 5 [詳細（details）] ペインの [編集（edit）] ボタン をクリックします。

ステップ 6 前述の手順で作成したのと同じ方法で、ダイアログボックスの値を編集します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 Security Cloud Control は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。

ステップ 9 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

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。