FTD デバイスの設定

インターフェイス

Cisco Defense Orchestrator（CDO）を使用して、Firepower Threat Defense（FTD）デバイスのデータインターフェイスまたは管理/診断インターフェイスを設定および編集できます。

現時点では、CDO はルーテッドインターフェイスとブリッジグループのみを設定できます。パッシブインターフェイスの設定はサポートしていません。

Firepower インターフェイス設定に関する注意事項と制約事項

Cisco Defense Orchestrator（CDO）を使用してデバイスを設定する場合、インターフェイス設定にいくつかの制限があります。次の機能のいずれかが必要な場合は、Firepower Management Center を使用してデバイスを設定する必要があります。

Firewall

- ルーテッド ファイアウォール モードのみがサポートされます。トランスペアレント ファイアウォール モードのインターフェイスは設定できません。
- スイッチポートモード用に設定されたインターフェイスをサポートするのは、Firepower 1010 の物理 デバイスだけです。詳細については、「FTD のスイッチ ポート モード インターフェイス」を参照してください。

パッシブ

- 現時点では、CDO はインターフェイステーブルのパッシブ インターフェイス モードを識別しないため、パッシブインターフェイスまたは ERSPAN インターフェイスを設定できません。パッシブインターフェイスを設定および識別するには、FDM UI を使用する必要があります。

IPS 専用モード

- インターフェイスをインライン（インラインセット内）またはインラインタップ（IPS オンリー処理用）に設定することはできません。IPS 専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティ ポリシーのみをサポートします。対照的に、ファイアウォール モードのインターフェイスでは、トラフィックが、フローの維持、IP レイヤおよび TCP レイヤの両方でのフロー状態の追跡、TCP の標準化などのファイアウォール機能の対象となります。

- また、任意で、セキュリティポリシーに従ってファイアウォールモードのトラフィックに IPS 機能を設定することもできます。

EtherChannel

CDOは、バージョン6.5以降を実行しているデバイスの読み取り、作成、および機能をサポートします。EtherChannelインターフェイスを作成するには、「Firepower Threat Defense の EtherChannel インターフェイスの追加」を参照してください。プレフィックスを作成

- 一度にアクティブにできるインターフェイスの数はデバイスモデルによって異なりますが、Firepower の物理デバイスには最大 48 の EtherChannel を設定できます。デバイス固有の制限については、「デバイス固有の制限事項」を参照してください。
- チャネルグループ内のすべてのインターフェイスは、同じメディアタイプと容量である必要があり、同じ速度とデュプレックスに設定する必要があります。メディアタイプはRJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。
- FTD EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。
- FTD は、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS vlan dot1Q tag native コマンドを使用して、隣接スイッチのネイティブ VLAN タギングを有効にすると、FTD はタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。
- すべてのFTD設定は、メンバー物理インターフェイスではなく論理EtherChannelインターフェイスを参照します。

（注） ポートチャネルとして設定されたインターフェイスは、物理インターフェイス、冗長インターフェイスのみ使用でき、サブインターフェイスのみがブリッジ グループ メンバー インターフェイスとしてサポートされます。

ブリッジ グループ

現時点では、CDOは1つのブリッジグループの設定をサポートしています。デバイスがブリッジグループをサポートしているかどうかを判断するには、「FTD設定におけるブリッジグループの互換性」で詳細を確認してください。

インターフェイスをブリッジグループに追加する際、次の点に注意してください。

- インターフェイスには名前が必要です。

- 静的に、または DHCP を介してインターフェイス用に定義された IPv4 または IPv6 アドレスは設定できません。
- BVI は、VLAN インターフェイスまたは他のルーテッドインターフェイスのいずれかをメンバーインターフェイスとして持つことができますが、1 つの BVI で両方をメンバーインターフェイスとして持つことはできません。
- BVI は、VLAN インターフェイスまたは他のルーテッドインターフェイスのいずれかをメンバーインターフェイスとして持つことができますが、1 つの BVI で両方をメンバーインターフェイスとして持つことはできません。
- インターフェイスは、Point-to-Point Protocol over Ethernet（PPPoE）にはできません。
- インターフェイスをセキュリティゾーンに関連付けることはできません（ゾーン内にある場合）。インターフェイスをブリッジグループに追加する前に、そのインターフェイスのすべての NAT ルールを削除する必要があります。
- メンバーインターフェイスは個別に有効または無効にします。そのため、未使用のインターフェイスはブリッジグループから削除することなく無効化できます。ブリッジグループ自体は常に有効になっています。
- ブリッジグループの **メンバー** になるインターフェイスを設定できます。インターフェイスの要件と作成については、「ブリッジグループの設定」を参照してください。

Point-to-Point Protocol over Ethernet

- IPv4 では、Point-to-Point Protocol over Ethernet（PPPoE）を設定できません。インターネット インターフェイスが DSL、ケーブルモデム、または ISP へのその他の接続に接続されていて、ISP が PPPoE を使用して IP アドレスを提供している場合、これらを設定するには、FDM を使用する必要があります。

VLAN

VLAN インターフェイスと VLAN メンバーを設定するには、「FTD VLAN の設定」で詳細を確認してください。スイッチポートモード用に VLAN を設定するには、「スイッチポートモード用 FTD VLAN の設定」で詳細を確認してください。

- このインターフェイスは物理的である必要があります。
- このインターフェイスは管理専用にできません。
- このインターフェイスは、BVI、サブインターフェイス、別の VLAN インターフェイス、EtherChannel など、他のタイプのインターフェイスとして関連付けることはできません。
- このインターフェイスを BVI メンバーまたは etherchannel メンバーにすることはできません。
- デバイスモデルは、さまざまな数の VLAN メンバーをサポートします。詳細については、「デバイスモデルによる VLAN メンバーの最大数」を参照してください。

（注） お使いの環境に VLAN を設定するには、「Firepower VLAN サブインターフェイスと 802.1Q トランキングの設定」で詳細を確認してください。

ネットワーク モジュール カード

任意のネットワークモジュールのインストールは、ASA 5515-X、5525-X、5545-X、5555-X、および Firepower 2100 シリーズデバイスに限定されます。

- カードはブートストラップ中（つまり、初期インストールまたは再イメージ化、ローカル/リモート管理間の切り替え時）にのみ検出されます。CDO はこれらのインターフェイスの速度とデュプレックスに正しいデフォルトを設定します。利用可能なインターフェイスの合計数を変更することなく、オプションのカードを、インターフェイスの速度/デュプレックスのオプションを変更するカードと交換する場合、交換されたインターフェイスの正しい速度/デュプレックスの値をシステムが認識できるように、デバイスを再起動します。デバイスとのコンソールセッションまたはSSHから、rebootコマンドを入力します。次に、CDO を使用して、機能の変更を含む各物理インターフェイスを編集し、有効な速度とデュプレックスのオプションを選択します。システムは元の設定を自動的に修正しないためです。すぐに変更を展開して、システムの正しい動作を確認します。

（注） カードをインターフェイスの総数が変更されたカードと交換する、または他のオブジェクトによって参照されたインターフェイスを削除すると、予期しない問題が発生することがあります。このような変更が必要な場合は、まずセキュリティゾーンのメンバーシップ、VPN接続など、削除するインターフェイスへの参照をすべて削除してください。変更を行う前にバックアップを実行することもお勧めします。

FTDv デバイスのインターフェイス

- FTDv デバイスを再初期化せずにインターフェイスを追加または削除することはできません。これらのアクションは FDM で実行する必要があります。

（注） ただし、異なる速度/デュプレックス機能を持っているインターフェイスと交換した場合、システムを再起動します（デバイスの CLI コンソールから、reboot コマンドを入力します）。これにより、システムが新しい速度/デュプレックス値を認識できるようになります。次に、CDO で機能の変更を含む各インターフェイスを編集し、有効な速度とデュプレックスのオプションを選択します。システムは元の設定を自動的に修正しないためです。すぐに変更を展開して、システムの正しい動作を確認します。

デバイスモデルによる VLAN メンバーの最大数

デバイスモデルにより、設定できる VLAN サブインターフェイスの最大数が制限されます。データ インターフェイスでのみサブインターフェイスを設定することができ、管理インターフェイスでは設定できないことに注意してください。次の表で、各デバイス モデルの制限について説明します。

モデル	VLAN サブインターフェイスの最大数
Firepower 1010	60
Firepower 1120	512
Firepower 1140、Firepower 1150	1024
Firepower 2100	1024
Cisco Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024
ASA 5508-X	50
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	100

Firepower データインターフェイス

Cisco Defense Orchestrator（CDO）は、Firepower Threat Defense（FTD）デバイスにおけるルーテッドインターフェイスとブリッジ仮想インターフェイスの設定をサポートします。

ルーテッド インターフェイス

各レイヤ3ルーテッドインターフェイス（またはサブインターフェイス）に、固有のサブネット上の IP アドレスが必要です。通常、これらのインターフェイスをスイッチ、別のルータ上のポート、または ISP/WAN ゲートウェイに接続します。

スタティックアドレスを割り当てるか、またはDHCPサーバから取得できます。ただし、DHCPサーバがデバイス上の静的に定義されたインターフェイスと同じサブネットアドレスを提供すると、システムはDHCPインターフェイスを無効にします。DHCPを使用してアドレスを取得しているインターフェイスがトラフィックの通過を停止している場合は、アドレスがデバイス上の別のインターフェイスのサブネットと重複していないかどうかを確認してください。

ルーテッドインターフェイスでは、IPv6アドレスとIPv4アドレスの両方を設定できます。IPv4と IPv6 の両方で、デフォルト ルートを設定してください。このタスクは、Firepower Device Managerを使用してFTDデバイスで実行する必要があります。デフォルトルートの設定については、『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager バージョン x.x.x 用』の「**基本 > ルーティング**」を参照してください。

ブリッジグループとブリッジ仮想インターフェイス

ブリッジ グループは、FTD デバイスがルーティングではなくブリッジするインターフェイスのグループです。ブリッジされたインターフェイスはブリッジグループに属し、すべてのインターフェイスが同じネットワーク上にあります。ブリッジグループはブリッジネットワークに IP アドレスを持つブリッジ仮想インターフェイス（BVI）によって表されます。ブリッジグループに含まれるインターフェースを「メンバー」と呼びます。

BVI に名前を付けると、ルーテッド インターフェイスと BVI の間のルーティングを実行できます。この場合、BVI はメンバー インターフェイスとルーテッド インターフェイス間のゲートウェイとして機能します。BVI に名前を指定しない場合、ブリッジ グループ メンバーのインターフェイス上のトラフィックはブリッジグループを離れることができません。通常、インターネットにメンバーインターフェイスをルーティングするため、インターフェイスに名前を付けます。

Firepower Device Manager によって管理される FTD は、1 つのブリッジグループのみをサポートします。したがって、CDO ではその 1 つのブリッジグループのみを管理でき、デバイス上に追加のブリッジグループを作成することはできません。CDO では、仮想 FTD インスタンスではなく、ハードウェアに直接インストールされた FTD 上の BVI のみを管理できます。

ブリッジグループのルーテッドモードでの使い方の1つは、外部スイッチの代わりにFirepower Threat Defense デバイスで追加のインターフェイスを使用することです。ブリッジ グループのメンバー インターフェイスにエンドポイントを直接接続できます。また、BVI と同じネットワークにより多くのエンドポイントを追加するために、スイッチを接続できます。

パッシブ インターフェイス

パッシブインターフェイスは、スイッチSPAN（スイッチドポートアナライザ）またはミラーポートを使用してネットワーク全体を流れるトラフィックをモニターします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。

現時点では、FTD のパッシブインターフェイスの管理について、CDO のサポートに制限があります。

- パッシブインターフェイスは FTD で設定する必要があります。
- CDO を使用して、ルーテッドインターフェイスをパッシブインターフェイスに変更したり、パッシブインターフェイスをルーテッドインターフェイスに変更したりすることはできません。
- CDO では、インターフェイステーブル内のパッシブインターフェイスが識別されません。

関連情報：

- Firepower インターフェイスの IPv6 アドレッシング
- Firepower インターフェイス設定に関する注意事項と制約事項
- 物理 Firepower インターフェイスの設定

管理/診断インターフェイス

管理ラベル付けされた物理ポート（または、Firepower Threat Defense Virtual の場合は Management 0/0 仮想インターフェイス）には、2 つの別個のインターフェイスが実際に関連付けられています。

- **管理仮想インターフェイス**：この IP アドレスは、システムの通信に使用されます。これはシステムがスマートライセンスに使用し、データベースの更新情報を取得するためのアドレスです。これに対して管理セッションを開くことができます（Firepower Device Manager および CLI）。**[システム設定（System Settings）]**>**[管理インターフェイス（Management Interface）]** で定義されている管理アドレスを設定する必要があります。
- **診断物理インターフェイス**：物理管理ポートは、実際には診断という名前が付けられています。外部 syslog サーバーに syslog メッセージを送信するためにこのインターフェイスを使用できます。診断物理インターフェイスの IP アドレスの設定は任意です。syslog で使用する場合にのみ、インターフェイスを設定します。このインターフェイスは、**[デバイスとサービス（Device & Services）]**>**[インターフェイス（Interfaces）]** ページに表示され、そこで設定できます。診断物理インターフェイスは管理トラフィックのみを許可し、トラフィックのスルーは許可しません。

（ハードウェア デバイス）管理/診断を設定する際、物理ポートをネットワークに接続しないことをお勧めします。代わりに、管理 IP アドレスのみを設定し、インターネットからの更新情報を得るためのゲートウェイとして、データ インターフェイスを使用するように設定します。次に、HTTPS/SSH トラフィック（デフォルトで HTTPS は有効）への内部インターフェイスを開き、内部 IP アドレスを使用して Firepower Device Manager を開きます。このタスクは、Firepower Device Manager で直接実行する必要があります。手順については、『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』の「管理アクセスリストの設定」を参照してください。

Firepower Threat Defense Virtual の推奨設定は、Management0/0 を内部インターフェイスと同じネットワークに接続し、内部インターフェイスをゲートウェイとして使用することです。診断用に別のアドレスを設定しないでください。

（注） **管理インターフェイスを編集する際の特別な手順については、**Firepower バージョン 6.4 以降の『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』を参照してください。 コンフィギュレーション ガイドを開き、**「基本」**>**「インターフェイス」**>**「管理/診断インターフェイス」**に移動します。管理インターフェイスの設定は、Firepower Device Manager で行う必要があります。

インターフェイスの設定

これは、MT ドキュメントを XML に変換するためのプレースホルダートピックですので、

準公共分野では使用しないでください。

Firepower インターフェイスの設定におけるセキュリティゾーンの使用

各インターフェイスは単一のセキュリティゾーンに割り当てることができます。ゾーンに基づいてセキュリティポリシーを適用されます。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。また、たとえば、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。

各ゾーンは、ルーテッドまたはパッシブのいずれかのモードになっています。これはインターフェイスのモードに直接関係します。ルーテッド インターフェイスとパッシブ インターフェイスは、同じモードのセキュリティ ゾーンにのみ追加できます。

ブリッジ仮想インターフェイス（BVI）は、セキュリティゾーンに追加されません。メンバーインターフェイスのみがセキュリティゾーンに追加されます。

ゾーンには診断インターフェイスや管理インターフェイスを含めません。ゾーンは、データインターフェイスにのみ適用されます。

CDO は、現在、ASA デバイスまたは FTD デバイス上の仮想トンネルインターフェイス（VTI）トンネルの管理、監視、使用をサポートしていません。VTI トンネルが設定されているデバイスを CDO にオンボーディングすることは可能ですが、VTI インターフェイスは無視されます。

セキュリティゾーンまたはスタティックルートが VTI を参照する場合、CDO は VTI 参照を除いてセキュリティゾーンとスタティックルートを読み取ります。VTI トンネルに対する CDO のサポートは近日中に提供されます。

セキュリティゾーンの詳細については、「セキュリティ ゾーン オブジェクト」を参照してください。

セキュリティゾーンへの FTD インターフェイスの割り当て

はじめる前に

セキュリティゾーンを追加する場合、インターフェイスには次の制限があります。

- インターフェイスには名前が必要です。
- このインターフェイスは管理専用にできません。このオプションは、インターフェイスの [詳細設定（Advanced）] タブから有効または無効にします。
- ブリッジ グループ インターフェイスにセキュリティゾーンを割り当てることはできません。
- スイッチポートモード用に設定したインターフェイスにセキュリティゾーンを割り当てることはできません。
- CDO は、現在、ASA デバイスまたは FTD デバイス上の仮想トンネルインターフェイス（VTI）トンネルの管理、監視、使用をサポートしていません。VTI トンネルが設定されているデバイスを CDO にオンボーディングすることは可能ですが、VTI インターフェイスは無視されます。セキュリティゾーンまたはスタティックルートが VTI を参照する場合、CDO は VTI 参照を除いてセキュリティゾーンとスタティックルートを読み取ります。VTI トンネルに対する CDO のサポートは近日中に提供されます。

Firepower インターフェイスをセキュリティゾーンに割り当てる

セキュリティゾーンを既存のインターフェイスに関連付けるには、以下の手順を実行します。

手順

ステップ 1 CDO にログインします。

ステップ 2 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 3 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 4 **FTD** デバイスをクリックし、変更する FTD を選択します。

ステップ 5 右側にある [管理（Management）] ペインで、[インターフェイス（Interfaces）] をクリックします。

ステップ 6 セキュリティゾーンを追加するインターフェイスを選択し、 [編集（Edit）] をクリックします。

ステップ 7 [セキュリティゾーン（Security Zone）] ドロップダウンメニューを使用して、このインターフェイスに関連付けるセキュリティゾーンを選択します。

（注） 必要に応じて、[新規作成（Create New）] をクリックして、このドロップダウンメニューから新しいセキュリティゾーンを作成します。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 CDO から FTD への設定変更の展開

関連情報：

- セキュリティ ゾーン オブジェクト
- Firepowerセキュリティゾーンのオブジェクトを作成または編集する
- Firepower インターフェイス設定に関する注意事項と制約事項

Firepower インターフェイス設定での Auto-MDI/MDX の使用

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレートケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX を有効にするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションが無効にされ、Auto-MDI/MDIX も無効になります。ギガビット イーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常に有効になり、無効にできません。

これらの設定は、インターフェイスの編集時に [詳細（Advanced）] タブで行います。

Firepower インターフェイス設定での MAC アドレスの使用

Media Access Control（MAC）アドレスを手動で設定してデフォルト値を上書きできます。

高可用性設定の場合は、インターフェイスのアクティブ MAC アドレスとスタンバイ MAC アドレスの両方を設定できます。アクティブユニットがフェールオーバーしてスタンバイユニットがアクティブになると、その新規アクティブユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。

アクティブおよびスタンバイの MAC アドレスは、インターフェイスを設定する際に [詳細（Advanced）] タブで指定します。

デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- **物理インターフェイス**：物理インターフェイスは Burned-In MAC Address を使用します。
- **サブインターフェイス**：物理インターフェイスのすべてのサブインターフェイスは同じ Burned-In MAC Address を使用します。サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になります。

Firepower インターフェイス設定で MTU 設定を使用する

MTU について

MTU は、Firepower Threat Defense デバイスが特定のイーサネット インターフェイスで送信可能な最大フレームペイロードサイズを指定します。MTU 値は、イーサネット ヘッダー、VLAN タギング、またはその他のオーバーヘッドを含まないフレーム サイズです。たとえば MTU を 1500 に設定した場合、想定されるフレーム サイズはヘッダーを含めて 1518 バイト、VLAN を使用する場合は 1522 バイトです。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

『Path MTU Discovery』

Firepower Threat Defense デバイスは、Path MTU Discovery（RFC 1191 の定義に従う）をサポートします。つまり、2 台のホスト間のネットワークパスに含まれるすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

MTU およびフラグメンテーション

IPv4 では、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは宛先（場合によっては中間ホップ）で組み立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6 では、通常、パケットをフラグメント化することはできません。したがって、フラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

UDP または ICMP の場合、アプリケーションではフラグメント化を避けるために MTU を考慮する必要があります。

（注） Firepower Threat Defense デバイスは、メモリに空きがある限り、設定された MTU よりも大きいフレームを受信できます。

MTU とジャンボ フレーム

MTU が大きいほど、大きいパケットを送信できます。パケットが大きいほど、ネットワークの効率が良くなる可能性があります。次のガイドラインを参照してください。

- トラフィックパスでの MTU の一致：すべての Firepower Threat Defense デバイスインターフェイスとトラフィックパスに含まれる他のデバイスインターフェイスで、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボフレームへの対応：ジャンボフレームとは、標準的な最大値 1522 バイト（レイヤ 2 ヘッダーおよび VLAN ヘッダーを含む）より大きく、9216 バイトまでのイーサネットパケットのことです。ジャンボ フレームに対応するために、9198 バイトまでの MTU を設定できます。Firepower Threat Defense Virtual の場合は最大 9000 バイトです。

（注） MTU を増やすとジャンボ フレームに割り当てるメモリが増え、他の機能（アクセス ルールなど）の最大使用量が制限される場合があります。ASA 5500-X シリーズ デバイスまたは Firepower Threat Defense Virtual で、MTU をデフォルトの 1500 より大きくする場合、システムを再起動する必要があります。ジャンボ フレームのサポートが常に有効な場合、Firepower 2100 シリーズ デバイスを再起動する必要はありません。

Firepower インターフェイスの IPv6 アドレッシング

Firepower 物理インターフェイスに、次の 2 種類のユニキャスト IPv6 アドレスを設定できます。

- [グローバル（Global）]：グローバルアドレスは、パブリックネットワークで使用可能なパブリックアドレスです。ブリッジグループの場合、各メンバーインターフェイスではなくブリッジ仮想インターフェイス（BVI）上でグローバルアドレスを設定します。次のいずれかをグローバル アドレスとして指定することはできません。
  - 内部で予約済みの IPv6 アドレス：fd00::/56 (from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - 未指定のアドレス（::/128 など）
  - ループバック アドレス（::1/128）
  - マルチキャストアドレス（ff00::/8）
  - リンクローカル アドレス（fe80::/10）
- [リンクローカル（Link-local）]：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベートアドレスです。ルータは、リンクローカルアドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決およびネイバー探索などのネットワーク検出機能に使用できます。リンクローカルアドレスがセグメントでのみ使用可能であり、インターフェイス MAC アドレスに接続されているため、各インターフェイスは独自のアドレスを持つ必要があります。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。グローバル アドレスを設定しない場合は、リンクローカルアドレスを自動的にするか、手動で設定する必要があります。

Firepower インターフェイスの設定

インターフェイス接続（物理的または仮想）のためにケーブルを接続するとき、インターフェイスを設定する必要があります。少なくとも、トラフィックを通過させることができるように、インターフェイスに名前を付けて有効化します。インターフェイスがブリッジグループのメンバーである場合、インターフェイスに名前を付けるだけで十分です。インターフェイスがブリッジ仮想インターフェイス（BVI）の場合、BVI に IP アドレスを割り当てる必要があります。単一の物理インターフェイスではなく、VLAN サブインターフェイスを特定のポートで作成する場合、通常、物理インターフェイスではなくサブインターフェイス上で IP アドレスを設定します。VLAN サブインターフェイスを使用すると、物理インターフェイスを異なる VLAN ID がタグ付けされた複数の論理インターフェイスに分割できます。

インターフェイス リストは、利用可能なインターフェイス、その名前、アドレスおよびステータスを表示します。インターフェイスの行を選択し、[操作（Actions）] ウィンドウで [編集（Edit）] をクリックして、インターフェイスの状態（オンまたはオフ）を変更したり、インターフェイスを編集したりすることができます。このリストは、設定に基づいたインターフェイス特性を示します。インターフェイスの行を展開して、サブインターフェイスまたはブリッジグループメンバーを表示します。

関連情報：

- インターフェイス
- 物理 Firepower インターフェイスの設定
- 高度な Firepower インターフェイスオプションの設定 （24 ページ）
- Firepower VLAN サブインターフェイスと 802.1Q トランキングの設定
- スイッチポートモード用 FTD VLAN の設定

物理 Firepower インターフェイスの設定

少なくとも 1 つの物理インターフェイスを有効にして使用できるようにする必要があります。通常、物理インターフェイスに名前を付けて IP アドレッシングを設定する必要がありますが、VLAN サブインターフェイスを設定する予定の場合、パッシブ モード インターフェイスを設定している場合、またはインターフェイスをブリッジグループに追加する予定の場合は、IP アドレッシングを設定しません。

（注） ブリッジグループ メンバー インターフェイスまたはパッシブインターフェイスに IP アドレスを設定することはできません。ただし、IPv6 アドレッシングとは関連がない詳細設定を変更することは可能です。

接続されたネットワークでの送信を一時的に防ぐために、インターフェイスを無効にできます。インターフェイスの設定を削除する必要はありません。現時点では、Cisco Defense Orchestrator（CDO）はルーテッドインターフェイスとブリッジグループのみを設定できます。CDO はパッシブインターフェイスを一覧表示しますが、CDO からアクティブインターフェイスとして再設定することはできません。

（注） **注**：CDO では、IPv4 の Point-to-Point Protocol over Ethernet（PPPoE）はサポートされていません。FDM でこのオプションを設定すると、CDO UI で問題が発生する可能性があります。デバイスに PPPoE を構成する必要がある場合は、FDM で適切な変更を行う必要があります。

手順

手順

ステップ 1 [デバイスとサービス（Devices & Services）] ページで、設定するインターフェイスがあるデバイスをクリックし、右側の [管理（Management）] ペインで [インターフェイス（Interfaces）] をクリックします。

ステップ 2 [インターフェイス（Interfaces ）] ページで、設定する物理インターフェイスを選択します。

ステップ 3 右側の操作ウィンドウで、[編集（Edit）] をクリックします。

ステップ 4 [論理名（Logical Name）] に物理インターフェイの論理名を入力し、任意で [説明（Description）] を入力します。サブインターフェイスを設定する場合を除き、インターフェイスには名前が必要です。

（注） 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバー オブジェクト、DHCP サーバーの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

ステップ 5 次のいずれかのオプションを選択します。

- サブインターフェースを追加する場合：

この物理インターフェイスのサブインターフェイスを設定する予定の場合、すでに設定している可能性が高いです。[保存（Save）] をクリックして、「Firepower VLAN サブインターフェイスと 802.1Q トランキングの設定」に進みます。それ以外の場合は続行します。

（注） サブインターフェイスを設定している場合でも、インターフェイスに名前を付けて、IP アドレスを指定できます。これは一般的な設定ではありませんが、必要だとわかっている場合は設定できます。

- サブインターフェイスを追加しない場合は、「物理インターフェイスの IPv4 アドレス指定」と「物理インターフェイスの IPv6 アドレス指定の設定」のいずれかまたは両方に進みます。

物理インターフェイスの IPv4 アドレス指定

警告 DHCP アドレスプールを設定して保存すると、DHCP アドレスプールがインターフェイスに設定された IP アドレスにバインドされます。DHCP アドレスプールを設定した後にインターフェイスのサブネットマスクを編集すると、FTD デバイスへの展開に失敗します。また、FDM コンソールで DHCP アドレスプールを編集し、FDM から CDO に設定を読み込むと、読み込みに失敗します。

手順

ステップ 1 [物理インターフェースの編集（Editing Physical Interface）] ダイアログで、[IPv4アドレス（IPv4 Address）] タブをクリックします。

ステップ 2 [タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [スタティック（Static）]：変わらないアドレスを割り当てる必要がある場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネットマスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。入力するアドレスがネットワーク ID またはネットワークのブロードキャストアドレスではなく、そのネットワークでまだ使用されていないことを確認してください。
  - [スタンバイIPアドレスとサブネットマスク（Standby IP Address and Subnet Mask）]：高可用性を設定し、このインターフェイスの HA をモニターリングしている場合は、同じサブネット上にスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。
  - （任意）[DHCPアドレスプール（DHCP Address Pool）]：単一の DHCP サーバーの IP アドレス、または IP アドレスの範囲を入力します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自体の IP アドレス、ブロードキャスト アドレス、またはサブネット ネットワーク アドレスを含めることはできません。プールの開始アドレスと終了アドレスをハイフンで区

切って指定します。この DHCP サーバを一時的に無効にするには、[Firepower Threat Defenseデバイス設定（Firepower Threat Defense Device Settings）] ページの [DHCPサーバー（DHCP Servers）] セクションでサーバーを編集します。DHCP サーバーの設定（387 ページ）

- [ダイナミック（Dynamic）]（DHCP）：ネットワーク上の DHCP サーバーからアドレスを取得する必要がある場合は、このオプションを選択します。必要に応じて、次のオプションを変更します。
  - [デフォルトルートを取得（Obtain Default Route）]：デフォルトルートを DHCP サーバーから取得するかどうかを指定します。通常、このオプションのチェックボックスをオンにします。
  - [ルートメトリック（Route Metric）]：DHCP サーバーからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。

（注） インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。

ステップ 3 設定が完了した場合、または次のいずれかの手順を続行する場合は、[保存（Save）] をクリックします。

- このインターフェイスに IPv4 アドレスだけでなく IPv6 アドレスも割り当てる場合は、「物理インターフェイスの IPv6 アドレス指定の設定」に進みます。
- 高度な Firepower インターフェイスオプションの設定 （24 ページ）。詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。
- インターフェイスを保存し、インターフェイスの詳細オプションの設定に進まない場合は、「物理インターフェイスの有効化」に進みます。

物理インターフェイスの IPv6 アドレス指定の設定

手順

ステップ 1 [物理インターフェースの編集（Editing Physical Interface）] ダイアログで、[IPv6アドレス（IPv6 Address）] タブをクリックします。

ステップ 2 [状態（State）]：グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[状態（State）] スライダをクリックして有効にします。

リンクローカルアドレスはインターフェイスの MAC アドレス（Modified EUI-64 形式）に基づいて生成されます。

（注） IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

ステップ 3 [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、チェックボックスをオンにします。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

RFC 4862 では、ステートレス自動設定用に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合は、FTD デバイスがルータ アドバタイズメント メッセージを送信します。メッセージを抑制して、RFC に準拠するためには、[RA を抑制（Suppress RA）] を選択します。

ステップ 4 [RAを抑制（Suppress RA）]：ルータアドバタイズメントを抑制する場合にチェックボックスをオンにします。Firepower Threat Defense デバイスをルータアドバタイズメントに参加させると、ネイバーデバイスがデフォルトのルータアドレスをダイナミックに把握できるようになります。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定できます。

Firepower Threat Defense デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージを抑制できます。

ステップ 5 [リンクローカルアドレス（Link-Local Address）]：アドレスをリンク ローカルのみとして使用する場合に入力します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

（注） リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feee:6a82。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカル アドレスによりパケットがドロップされることがあります。

ステップ 6 [スタンバイリンクローカルアドレス（Standby Link-Local Address）]：インターフェイスがデバイスの高可用性ペアに接続する場合は、このアドレスを設定します。このインターフェイスが

接続されている他の FTD のインターフェイスに設定されているリンクローカルアドレスを入力します。

ステップ 7 [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティックグローバル IPv6 アドレスとネットワークプレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、「Firepower インターフェイスの IPv6 アドレッシング」を参照してください。

ステップ 8 [スタンバイ IPアドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

ステップ 9 設定が完了した場合、または次のいずれかの手順を続行する場合は、[保存（Save）] をクリックします。

- 高度な Firepower インターフェイスオプションの設定 （24 ページ）。詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。
- インターフェイスを保存し、インターフェイスの詳細オプションの設定に進まない場合は、「物理インターフェイスの有効化」に進みます。

物理インターフェイスの有効化

手順

ステップ 1 有効化するインターフェイスを選択します。

ステップ 2 インターフェイスの論理名に関連付けられている、ウィンドウ右上の [状態（State）] スライダを青にスライドします。

ステップ 3 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Firepower VLAN サブインターフェイスと 802.1Q トランキングの設定

VLAN サブインターフェイスを使用すると、物理インターフェイスを異なる VLAN ID がタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはデバイスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。

物理インターフェイスをスイッチのトランク ポートに接続する場合は、サブインターフェイスを作成します。スイッチ トランク ポートで表示できる各 VLAN のサブインターフェイスを作成します。物理インターフェイスをスイッチのアクセス ポートに接続する場合は、サブインターフェイスを作成しても意味がありません。

（注） 必要に応じて詳細設定を変更することはできますが、ブリッジグループ メンバーインターフェイスの IP アドレスを設定することはできません。

はじめる前に

物理インターフェイス上のタグなしパケットの禁止。物理インターフェイスはタグの付いていないパケットを通過させるため、サブインターフェイスを使用する場合、通常は物理インターフェイスでトラフィックを通過させないようにします。サブインターフェイスでトラフィックを通過させるには物理的インターフェイスを有効にする必要があるため、インターフェイスに名前を付けないことでトラフィックを通過させないようにします。物理インターフェイスにタグの付いていないパケットを通過させる場合には、通常のようにインターフェイスに名前を付けることができます。

手順

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、インターフェイスを設定するデバイスをクリックします。

ステップ 4 右側の [管理（Management）] ペインで [インターフェイス（Interfaces）] をクリックします。

ステップ 5 [インターフェイス（Interfaces）] ページで、設定する物理インターフェイスを選択し、右側の操作ウィンドウで [+新しいサブインターフェイス（+ New Subinterface）] をクリックします。

[親インターフェイス（Parent Interface）] フィールドには、このサブインターフェイスを作成する対象の物理インターフェイス名が表示されます。いったん作成したサブインターフェイスの親インターフェイスは変更できません。

ステップ 6 [論理名（Logical Name）] に物理インターフェイの論理名を入力し、任意で [説明（Description）] を入力します。論理名を設定しないと、インターフェイスの残りの設定は無視されます。

（注） 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバー オブジェクト、DHCP サーバーの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

ステップ 7 VLAN ID とサブインターフェイス ID を次のように設定します。

- [VLAN ID]：VLAN ID を 1 ～ 4094 の範囲で入力します。これは、このサブインターフェイス上のパケットにタグを付けるために使用されます。
- [サブインターフェイスID（Sub-Interface ID）]：サブインターフェイス ID を 1 ～ 4294967295 の範囲の整数で入力します。許可されるサブインターフェイスの番号は、デバイスモデルによる VLAN メンバーの最大数。いったん作成したサブインターフェイスの ID は変更できません。

「サブインターフェイスの IPv4 アドレスの設定」および「サブインターフェイスの IPv6 アドレスの設定」に進みます。

サブインターフェイスの IPv4 アドレスの設定

手順

ステップ 1 [サブインターフェースの追加（Adding Subinterface）] ダイアログで、[IPv4アドレス（IPv4 Address）] タブをクリックします。

ステップ 2 [タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [スタティック（Static）]：変わらないアドレスを割り当てる必要がある場合は、このオプションを選択します。

  インターフェイスに接続されたネットワークに対するインターフェイスの **IP アドレスとサブネットマスク**を入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。入力するアドレスがネットワーク ID またはネットワークのブロードキャストアドレスではなく、そのネットワークでまだ使用されていないことを確認してください。

- [スタンバイIPアドレス（Standby IP Address）]および[サブネットマスク（Subnet Mask）]：このインターフェイスがデバイスの高可用性ペアで使用されている場合にのみ入力します。

- [ダイナミック（Dynamic）]（DHCP）：ネットワーク上の DHCP サーバーからアドレスを取得する必要がある場合は、このオプションを選択します。必要に応じて、次のオプションを変更します。

  - [デフォルトルートを取得（Obtain Default Route）]：デフォルトルートを DHCP サーバーから取得するかどうかを指定します。通常、このオプションのチェックボックスをオンにします。
  - [ルートメトリック（Route Metric）]：DHCP サーバーからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。

    「DHCP サーバーの設定」を参照してください。

（注） インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。

ステップ 3 設定が完了した場合、または次のいずれかの手順を続行する場合は、[作成（Create）] をクリックします。

- このインターフェイスに IPv4 アドレスだけでなく IPv6 アドレスも割り当てる場合は、「物理インターフェイスの IPv6 アドレス指定の設定」に進みます。
- 高度な Firepower インターフェイスオプションの設定 （24 ページ）。詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。
- サブインターフェイスを作成した場合は、「物理インターフェイスの有効化 」に進みます。

サブインターフェイスの IPv6 アドレスの設定

手順

ステップ 1 [IPv6アドレス（IPv6 Address）] タブをクリックします。

ステップ 2 **IPv6 処理の有効化**：グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[状態（State）] スライダを青にスライドします。リンクローカルアドレスはインターフェイスの MAC アドレス（Modified EUI-64 形式）に基づいて生成されます。

（注） IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

ステップ 3 [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、チェックボックスをオンにします。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバルプレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

ステップ 4 [RAを抑制（Suppress RA）]：ルータアドバタイズメントを抑制する場合にチェックボックスをオンにします。Firepower Threat Defense デバイスをルータアドバタイズメントに参加させると、ネイバーデバイスがデフォルトのルータアドレスをダイナミックに把握できるようになり

ます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定できます。

Firepower Threat Defense デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージを抑制できます。

ステップ 5 [リンクローカルアドレス（Link-Local Address）]：アドレスをリンク ローカルのみとして使用する場合に入力します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。

（注） リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feee:6a82。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカル アドレスによりパケットがドロップされることがあります。

ステップ 6 [スタンバイリンクローカルアドレス（Standby Link-Local Address）]：インターフェイスがデバイスの高可用性ペアに接続する場合は、このアドレスを設定します。

ステップ 7 [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、136 ページの「IPv6 アドレッシング」を参照してください。

ステップ 8 [スタンバイ IPアドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

ステップ 9 設定が完了した場合、または次のいずれかの手順を続行する場合は、[作成（Create）]をクリックします。

- [詳細設定（Advanced）]タブをクリックして、高度な Firepower インターフェイス オプションの設定 （24 ページ） を行います。詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。
- サブインターフェイスを作成した場合は、「物理インターフェイスの有効化」に進みます。

物理インターフェイスの有効化

手順

ステップ 1 サブインターフェースを有効にするには、サブインターフェースの論理名に関連付けられている [状態（State）] スライダを青にスライドします。

ステップ 2 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

高度な Firepower インターフェイスオプションの設定

高度なインターフェイスオプションには、ほとんどのネットワークに適合するデフォルト設定が用意されています。ネットワークの問題を解決する場合のみ設定を行います。

次の手順では、インターフェイスが定義済みであることを前提としています。インターフェイスを最初に編集または作成するときに、これらの設定を編集することもできます。

この手順と手順内のすべてのステップはオプションです。

制限事項

- Firepower 2100 シリーズ デバイス上の管理インターフェイスに MTU、デュプレックス、速度を設定することはできません。
- 名前のないインターフェイスの MTU は、1500 バイトに設定する必要があります。

手順

ステップ 1 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、インターフェイスを設定するデバイスをクリックします。

ステップ 4 右側の [管理（Management）] ペインで [インターフェイス（Interfaces）] をクリックします。

ステップ 5 [インターフェイス（Interfaces）] ページで、設定する物理インターフェイスを選択し、右側の操作ウィンドウで [編集（Edit）] をクリックします。

ステップ 6 [詳細設定（Advanced）] タブをクリックします。

ステップ 7 [HAモニタリングの有効化（Enable for HA Monitoring）] は自動的に有効になります。これが有効になっている場合、高可用性の設定でピア装置にフェールオーバーするかどうかの判断要素にインターフェイスの状態が含まれます。このオプションは、高可用性を設定しない場合は無視されます。インターフェイスの名前を設定しない場合も、無視されます。

ステップ 8 データインターフェイスを管理専用に指定する場合は、[管理専用（Management Only）] チェックボックスをオンにします。

管理専用インターフェイスはトラフィックの通過を許可しないため、データインターフェイスを [管理専用（Management Only）] インターフェイスに設定する意味はあまりありません。管理/診断インターフェイスは、常に管理専用であるため、この設定を変更することはできません。

ステップ 9 IPv6 DHCP の設定を変更します。

- [IPv6アドレス設定でDHCPを有効化する（Enable DHCP for IPv6 address configuration）]：IPv6 ルータのアドバタイズメントパケットに、管理アドレス設定フラグを設定するかどうか。このフラグは、取得されるステートレス自動設定のアドレス以外のアドレスの取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。
- [IPv6のアドレス以外の設定でDHCPを有効化する（Enable DHCP for IPv6 non-address configuration）]：IPv6 ルータのアドバタイズメントパケットに、その他のアドレス設定フラグを設定するかどうか。このフラグは、DHCPv6 から DNS サーバ アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。

ステップ 10 [DADの試行（DAD Attempts）]：インターフェイスで重複アドレス検出（DAD）を実行する頻度（0 ～ 600）。デフォルトは 1 です。ステートレス自動設定プロセスでは、DAD はアドレスがインターフェイスに割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を検証します。重複アドレスがインターフェイスのリンクローカル アドレスであれば、インターフェイス上で IPv6 パケットの処理は無効になります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。インターフェイスは、ネイバー送信要求メッセージを使用して、重複アドレス検出を実行します。重複アドレス検出（DAD）プロセスを無効にするには、この値を 0 に設定します。

ステップ 11 [MTU]（最大伝送ユニット）を目的の値に変更します。

デフォルトの MTU は 1500 バイトです。64 ～ 9198 の値を指定できます（Firepower Threat Defense Virtual の場合は最大値が 9000）。ジャンボ フレームが頻繁にやり取りされるネットワークでは、大きな値に設定します。詳細については、「Firepower インターフェイス設定で MTU 設定を使用する」を参照してください。

（注） ASA 5500-X シリーズ デバイス、ISA 3000 シリーズ デバイス、または Firepower Threat Defense Virtual で MTU を 1500 より大きい値に設定する場合は、デバイスを再起動する必要があります。CLI にログインし、reboot コマンドを使用します。ジャンボフレームのサポートが常に有効な場合、Firepower 2100 シリーズ デバイスを再起動する必要はありません。

ステップ 12 （物理インターフェイスのみ）**速度**および**デュプレックス**の設定を変更します。

デフォルトでは、インターフェイスは接続相手のインターフェイスに対し、互いに最適なデュプレックスおよび速度をネゴシエートしますが、必要に応じて、特定のデュプレックスおよび速度を強制的に適用することもできます。記載されているオプションは、インターフェイスでサポートされるもののみです。ネットワークモジュールのインターフェイスにこれらのオプションを設定する前に、「Firepower インターフェイス設定に関する注意事項と制約事項」をお読みください。

- [二重（Duplex）] : [自動（Auto）]、[ハーフ（Half）]、[フル（Full）]、または [デフォルト（Default）] を選択します。[自動（Auto）] は、インターフェイスによってサポートされる場合のみデフォルトとなります。たとえば、Firepower 2100 シリーズの SFP インターフェイスでは [自動（Auto）] を選択できません。Firepower Device Manager が設定を試行できないことを示すために [Default] を選択します。

  既存の設定は、すべてそのまま変更されません。

- [速度（Speed）] : [自動（Auto）] を選択してインターフェイスに速度をネゴシエートさせるか（これがデフォルトです）、または特定の速度：[10]、[100]、[1000]、[10000] Mbps を選択します。次の特別オプションも選択できます。

  既存の設定は、すべてそのまま変更されません。

  インターフェイスのタイプによって、選択可能なオプションが制限されます。たとえば、Firepower 2100 シリーズデバイスの SFP+ インターフェイスは 1000（1 Gbps）および 10000（10 Gpbs）のみをサポートし、SFP インターフェイスは 1000（1 Gbps）のみをサポートしますが、GigabitEthernet ポートは 10000（10 Gpbs）をサポートしません。その他のデバイス上の SPF インターフェースでは [ネゴシエートなし（No Negotiate）] が必須の場合があります。インターフェイスのサポート対象については、ハードウェアのマニュアルを参照してください。

ステップ 13 （必要に応じて、サブインターフェイスおよび高可用性装置に推奨されます。）MAC アドレスを設定します。

[MACアドレス（MAC Address）] : H.H.H 形式の Media Access Control。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は 000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

[スタンバイMACアドレス（Standby MAC Address）] : 高可用性で使用します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 14 [作成（Create）] をクリックします。

ブリッジグループの設定

ブリッジ グループは 1 つ以上のインターフェイスをグループ化する仮想インターフェイスです。インターフェイスをグループ化する主な理由は、スイッチドインターフェイスのグループを作成することにあります。そのため、ブリッジグループに含まれているインターフェイスにワークステーションやその他のエンドポイントデバイスを直接接続できます。それらは別の物理スイッチを介して接続する必要はありませんが、スイッチをブリッジ グループ メンバーに接続することもできます。

グループ メンバーには IP アドレスはありません。代わりに、すべてのメンバー インターフェイスがブリッジ仮想インターフェイス（BVI）の IP アドレスを共有します。BVI で IPv6 を有

効にすると、メンバー インターフェイスには一意のリンクローカル アドレスが自動的に割り当てられます。

通常は、メンバー インターフェイス経由で接続されているエンドポイントの IP アドレスを提供するブリッジ グループ インターフェイス（BVI）に DHCP サーバーを設定します。ただし、必要に応じて、メンバー インターフェイスに接続されているエンドポイントにスタティック アドレスを設定できます。ブリッジ グループ内のすべてのエンドポイントには、ブリッジ グループの IP アドレスと同じサブネットの IP アドレスが必要です。

（注） ISA 3000 では、デバイスは inside という名前のブリッジグループ BVI で事前に設定されており、outside インターフェイスを除くすべてのデータインターフェイスを含んでいます。そのため、デバイスにはインターネットやその他のアップストリーム ネットワークへの接続に使用される 1 つのポートが事前に設定されています。また、その他のポートはすべて有効になっていて、エンドポイントへの直接接続に使用できます。新しいサブネットで内部インターフェイスを使用する場合は、まず必要なインターフェイスを BVI から削除する必要があります。

Firepower Device Manager によって管理される FTD は、1 つのブリッジグループのみをサポートします。したがって、CDO ではその 1 つのブリッジグループのみを管理でき、デバイス上に追加のブリッジグループを作成することはできません。

CDO でブリッジグループを作成した後、設定が FTD に展開されるまで、ブリッジグループ ID はわかりません。FTD によって BVI1 などのブリッジグループ ID が割り当てられます。インターフェイスが削除され、新しいブリッジグループが作成されると、新しいブリッジグループには、BVI2 などの増分された番号が割り当てられます。

はじめる前に

ブリッジグループの**メンバー**になるインターフェイスを設定します。具体的には、各**メンバー**インターフェイスは、次の要件を満たしている必要があります。

- インターフェイスには名前が必要です。
- インターフェイスは**管理専用**として設定できません。
- インターフェイスはパッシブモードで設定できません。
- インターフェイスを EtherChannel インターフェイスまたは EtherChannel サブインターフェイスにすることはできません。
- 静的に、または DHCP を介してインターフェイス用に定義された IPv4 または IPv6 アドレスは設定できません。現在使用しているインターフェイスからアドレスを削除する必要がある場合、そのインターフェイスのその他の設定（アドレスを持つインターフェイスに依存するスタティック ルート、DHCP サーバー、NAT ルールなど）も削除する必要がある場合があります。IP アドレスを持つインターフェイスをブリッジグループに追加しようとすると、CDO は警告を表示します。インターフェイスをブリッジグループに追加し続けると、CDO はインターフェイス設定から IP アドレスを削除します。

- BVI は、VLAN インターフェイスまたは他のルーテッドインターフェイスのいずれかをメンバーインターフェイスとして持つことができますが、1 つの BVI で両方をメンバーインターフェイスとして持つことはできません。
- インターフェイスは、Point-to-Point Protocol over Ethernet（PPPoE）にはできません。
- インターフェイスをセキュリティゾーンに関連付けることはできません（ゾーン内にある場合）。インターフェイスをブリッジグループに追加する前に、そのインターフェイスのすべての NAT ルールを削除する必要があります。
- メンバーインターフェイスは個別に有効または無効にします。そのため、未使用のインターフェイスはブリッジグループから削除することなく無効化できます。ブリッジグループ自体は常に有効になっています。
- ブリッジグループではクラスタリングがサポートされません。

（注） ブリッジグループは、ルーテッドモードの Firepower 2100 デバイス、またはブリッジされた ixgbevf インターフェイスを備えた VMware ではサポートされていません。

ブリッジ グループ インターフェイス名の設定とブリッジグループメンバーの選択

この手順では、ブリッジグループインターフェイス（BVI）に名前を付け、ブリッジグループに追加するインターフェイスを選択します。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、ブリッジグループを作成するデバイスを選択します。

ステップ 4 次のいずれかを実行します。

- BVI ブリッジグループを選択し、操作ウィンドウで [編集（Edit）] をクリックします。
- プラスボタン をクリックして、ブリッジ グループ インターフェイスを選択します。

（注） 作成および設定できるのは 1 つのブリッジグループのみです。ブリッジ グループをすでに定義している場合は、新しいグループ作成するのではなく、そのグループを編集する必要があります。新しいブリッジ グループを作成する必要がある場合は、まず既存のブリッジ グループを削除する必要があります。

ステップ 5 次を設定します。

- [論理名（Logical Name）]：ブリッジグループに名前を付ける必要があります。最大 48 文字です。英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定は無視されます。

（注） 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバー オブジェクト、DHCP サーバーの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

- （任意）[説明（Description）]：説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ 6 [ブリッジグループメンバー（Bridge Group Members）] タブをクリックします。1 つのブリッジグループに最大 64 個のインターフェイスまたはサブインターフェイスを追加できます。

- インターフェイスを確認して、ブリッジグループに追加します。
- ブリッジグループから削除するインターフェイスのチェックボックスをオフにします。

ステップ 7 [保存（Save）] をクリックします。

BVI に名前とメンバーインターフェイスが追加されました。次のタスクに進み、ブリッジ グループインターフェイスを設定します。メンバーインターフェイス自体に対して次のタスクを実行していません。

- IPv4 アドレスを BVI に割り当てる場合は、BVI の IPv4 アドレスの設定。
- IPv6 アドレスを BVI に割り当てる場合は、BVI の IPv6 アドレスの設定。
- ブリッジ グループ インターフェイスに高度なインターフェイス オプションの設定。

BVI の IPv4 アドレスの設定

手順

ステップ 1 ブリッジグループを作成するデバイスを選択します。

ステップ 2 インターフェイスのリストで [BVI] を選択し、操作ウィンドウで [編集（Edit）] をクリックします。

ステップ 3 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

ステップ 4 [タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [スタティック（Static）]：変わらないアドレスを割り当てる必要がある場合は、このオプションを選択します。ブリッジ グループの IP アドレスとサブネット マスクを入力します。接続されているエンドポイントはすべて、このネットワーク上に存在することになり

ます。ブリッジグループが事前設定されたモデルでは、デフォルトのBVIの「内部」ネットワークは 192.168.1.1/24（つまり 255.255.255.0）です。このアドレスがネットワーク上ですでに使用されていないことを確認します。

高可用性を設定し、このインターフェイスのHAをモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

（注） インターフェイスに対して設定されているDHCPサーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCPサーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。「DHCPサーバーの設定」を参照してください。

- [ダイナミック（Dynamic）]（DHCP）：ネットワーク上のDHCPサーバーからアドレスを取得する必要がある場合は、このオプションを選択します。これはブリッジグループの一般的なオプションではありませんが、必要に応じて設定できます。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
  - [ルートメトリック（Route Metric）]：DHCP サーバーからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
  - [デフォルトルートを取得（Obtain Default Route）]：チェックボックスをオンにすると、デフォルトルートがDHCPサーバーから取得されます。通常は、デフォルトのこのオプションを選択します。

ステップ 5 次の手順のいずれかに進みます。

- IPv4 アドレスを BVI に割り当てる場合は、「BVI の IPv6 アドレスの設定」を行います。
- インターフェイスの詳細オプションを設定します。
- [保存（Save）] をクリックして、Firepower デバイスに変更を展開します。詳細については、「CDO から FTD への設定変更の展開」を参照してください。

BVI の IPv6 アドレスの設定

手順

ステップ 1 [IPv6アドレス（IPv6 Address）] タブをクリックして、BVI の IPv6 アドレスを設定します。

ステップ 2 IPv6 アドレスの次の項目を設定します。

ステップ 3 **IPv6 処理の有効化**：グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[状態（State）] スライダを青にスライドします。リンクローカル アドレスはインターフェイスの MAC アドレス（Modified EUI-64 形式）に基づいて生成されます。

（注） IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

ステップ 4 [RAを抑制（Suppress RA）]：ルータアドバタイズメントを抑制するかどうかを指定します。Firepower Threat Defense デバイスをルータアドバタイズメントに参加させると、ネイバーデバイスがデフォルトのルータアドレスをダイナミックに把握できるようになります。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

FTD デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージを抑制できます。

ステップ 5 [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティックグローバル IPv6 アドレスとネットワークプレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、「IPv6 アドレッシング」を参照してください。

ステップ 6 [スタンバイ IPアドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

ステップ 7 次の手順のいずれかに進みます。

- インターフェイスの詳細オプションの設定
- [保存（Save）] をクリックして、Firepower デバイスに変更を展開します。詳細については、「CDO から FTD への設定変更の展開」を参照してください。

高度なインターフェイス オプションの設定

ブリッジグループの**メンバー**インターフェイスに対して最も詳細なオプションを設定しますが、一部はブリッジ グループ インターフェイス自体でも使用できます。

手順

ステップ 1 詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 2 [OK] をクリックします。

ステップ 3 [保存（Save）] をクリックして、Firepower デバイスに変更を展開します。詳細については、「CDO から FTD への設定変更の展開」を参照してください。

次のタスク

- 使用する予定のすべてのメンバー インターフェイスが有効になっていることを確認します。
- ブリッジ グループの DHCP サーバを設定します。「DHCP サーバーの設定」を参照してください。
- メンバー インターフェイスを適切なセキュリティ ゾーンに追加します。
- アイデンティティ、NAT、アクセスなどのポリシーにより、ブリッジグループとメンバーインターフェイスに必要なサービスが提供されることを確認します。

FTD 設定におけるブリッジグループの互換性

各種設定でインターフェイスを指定する際、ブリッジ仮想インターフェイス（BVI）を指定できる場合もあれば、ブリッジグループのメンバーを指定できる場合もあります。次の表では、BVI をいつ使用でき、メンバーインターフェイスをいつ使用できるかを示します。

Firepower Threat Defense の設定タイプ	BVI が使用可能	BVI メンバーが使用可能
DHCP サーバー	対応	×
DNS サーバー	対応	対応
管理アクセス	対応	×
NAT（ネットワーク アドレス変換。）	×	対応
セキュリティ ゾーン	×	対応
サイト間 VPN アクセスポイント	×	対応
Syslog サーバー（Syslog Server）	対応	×

ブリッジグループの削除

ブリッジグループを削除すると、そのメンバーは標準のルーテッドインターフェイスになり、NATルールまたはセキュリティゾーンのメンバーシップはすべて維持されます。インターフェイスを編集して、IP アドレスを付与できます。新しいブリッジ グループを作成する必要がある場合は、まず既存のブリッジ グループを削除する必要があります。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、ブリッジグループを削除するデバイスを選択します。

ステップ 4 BVI ブリッジグループを選択し、操作ウィンドウで [削除（Remove）] をクリックします。

ステップ 5 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Firepower Threat Defense の EtherChannel インターフェイスの追加

EtherChannel インターフェイスの制限事項

EtherChannel は、デバイスモデルによっては、同じメディアタイプと容量のメンバーインターフェイスを複数含めることができますが、同じ速度とデュプレックスに設定する必要があります。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel インターフェイスには、物理設定とソフトウェアバージョンに基づいた多くの制限があります。詳細については、以下のセクションを参照してください。

インターフェイスの一般的な制限事項

- EtherChannel は、Firepower Threat Defense のバージョン 6.5 以降を実行しているデバイスでのみ使用できます。
- CDO は Firepower デバイス（1010、1120、1140、1150、2110、2120、2130、および 2140）で EtherChannel インターフェイス設定をサポートします。デバイスモデルごとのインターフェイスの制限については、「デバイス固有の制限事項」を参照してください。
- チャネルグループ内のすべてのインターフェイスは、同じメディアタイプと容量である必要があり、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインター

フェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。

- FTD EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。
- FTD は、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS vlan dot1Q tag native コマンドを使用して、隣接スイッチのネイティブ VLAN タギングを有効にすると、FTD はタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。
- すべての FTD 設定は、メンバー物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。
- ポートチャネル インターフェイスは物理インターフェイスとして表示されます。

デバイス固有の制限事項

次のデバイスには、特定のインターフェイスの制限事項があります。

1000 シリーズ

- Firepower 1010 は、最大 8 つの EtherChannel インターフェイスをサポートします。
- Firepower 1120、1140、1150 は、最大 12 の EtherChannel インターフェイスをサポートします。
- 1000 シリーズは、LACP 高速レートをサポートしていません。 LACP では常に通常のレートが使用されます。この値は設定不可能です。

2100 シリーズ

- Firepower 2110 および 2120 モデルは、最大 12 の EtherChannel インターフェイスをサポートします。
- Firepower 2130 および 2140 モデルは、最大 16 の EtherChannel インターフェイスをサポートします。
- 2100 シリーズは LACP 高速レートをサポートしていません。 LACP は常に通常のレートを使用します。この値は設定不可能です。

4100 シリーズおよび 9300 シリーズ

- 4100 および 9300 シリーズで EtherChannel を作成または設定することはできません。これらのデバイスの EtherChannel は、FXOS シャーシで設定する必要があります。
- 4100 および 9300 シリーズの EtherChannel は、物理インターフェイスとして CDO に表示されます。

関連トピック：

EtherChannel インターフェイスの追加

EtherChannel を FTD に追加するには、次の手順を実行します。

（注） 続けて別の EtherChannel を作成する場合は、[別のEtherChannelを作成（Create another）] チェックボックスをオンにして、[作成（Create）] をクリックします。

手順

ステップ 1 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、EtherChannel を追加するデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[インターフェイス（Interfaces）] を選択します。

ステップ 5 青色のプラスボタン をクリックし、[EtherChannel] を選択します。

ステップ 6 （任意）[論理名（Logical Name）] を入力します。

ステップ 7 （任意）説明を入力します。

ステップ 8 [EtherChannel ID] を入力します。

Firepower 1010 シリーズの場合は、1 ～ 8 の値を入力します。

Firepower 2100、4100、および 9300 シリーズの場合は、1 ～ 48 の値を入力します。

ステップ 9 [リンク集約制御プロトコル（Link Aggregation Control Protocol）] のドロップダウンボタンをクリックし、次の 2 つのオプションのいずれかを選択します。

- [アクティブ（Active）]：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブモードを使用する必要があります。
- [オン（On）]：EtherChannel は常にオンであり、LACP は使用されません。[オン（On）] の EtherChannel は、[オン（On）] と設定されている別の EtherChannel のみと接続できます。

ステップ 10 メンバーとして EtherChannel に含めるインターフェイスを検索して選択します。1 つ以上のインターフェースを含める**必要があります**。

警告：EtherChannelインターフェイスをメンバーとして追加し、すでにIPアドレスが設定されている場合、CDO はメンバーの IP アドレスを削除します。

ステップ 11 [作成（Create）] をクリックします。

関連情報：

- FTD の EtherChannel インターフェイスの編集または削除
- EtherChannel インターフェイスへのサブインターフェイスの追加
- EtherChannel のサブインターフェイスの編集または削除
- Firepower インターフェイス設定に関する注意事項と制約事項
- セキュリティゾーンへの FTD インターフェイスの割り当て

FTD の EtherChannel インターフェイスの編集または削除

既存の EtherChannel インターフェイスを変更、または EtherChannel インターフェイスを Firepower Threat Defense（FTD）から削除するには、次の手順を実行します。

EtherChannel の編集

EtherChannel には制限事項がいくつかあるため、変更時には注意が必要です。詳細については、「EtherChannel」を参照してください。

（注） EtherChannel には 1 つ以上のメンバーが必要です。

既存の EtherChannel を編集するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックし、変更する EtherChannel に関連付けられている FTD を選択します。

ステップ 4 右側にある [管理（Management）] ペインで、[インターフェイス（Interfaces）] をクリックします。

ステップ 5 [インターフェイス（Interfaces）] ページで、編集する EtherChannel インターフェイスを選択します。右側の操作ウィンドウで、編集アイコン をクリックします。

ステップ 6 次の項目のいずれかを変更します。

- 論理名
- 状態
- [説明（Description）]
- セキュリティゾーンの割り当て

- リンクアグリケーション制御プロトコルのステータス
- [IPv4]、[IPv6]、[詳細（Advanced）] タブのいずれかの IP アドレス設定
- EtherChannel メンバー

警告　**警告**：EtherChannelインターフェイスをメンバーとして追加し、すでにIPアドレスが設定されている場合、CDO はメンバーの IP アドレスを削除します。

ステップ 7 [保存（Save）] をクリックします。

EtherChannel インターフェイスの削除

（注）　高可用性（HA）またはその他の設定に関連付けられた EtherChannel インターフェイスの場合は、CDO から削除する前に、すべての設定から EtherChannel インターフェイスを手動で削除する必要があります。

FTD から EtherChannel インターフェイスを削除するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 [FTD] タブをクリックし、削除する EtherChannel に関連付けられている FTD を選択します。
ステップ 4 右側の [管理（Management）] ペインで、[インターフェイス（Interfaces）] を選択します。
ステップ 5 [インターフェイス（Interfaces）] ページで、編集する EtherChannel インターフェイスを選択します。右側の [アクション（Actions）] ペインで、[削除（Remove）] をクリックします。
ステップ 6 削除する EtherChannel インターフェイスを確認し、[OK] をクリックします。

EtherChannel インターフェイスへのサブインターフェイスの追加

EtherChannel サブインターフェイス

[インターフェイス（Interfaces）] ページでは、各インターフェイスを展開して、デバイスのどのインターフェイスにサブインターフェイスがあるかを表示できます。この展開されたビューには、一意の論理名、有効/無効状態、関連するセキュリティゾーン、およびサブインターフェイスのモードも表示されます。サブインターフェイスのインターフェイスタイプとモードは、親インターフェイスによって決定されます。

一般的な制限事項

CDO は、次のインターフェイスタイプのサブインターフェイスをサポートしていません。

- 管理専用に設定されたインターフェース
- スイッチポートモード用に設定されたインターフェイス
- パッシブインターフェイス
- VLAN インターフェイス
- ブリッジ仮想インターフェイス（BVI）
- すでに別の EtherChannel インターフェイスのメンバーになっているインターフェイス

次のサブインターフェイスを作成**できます**。

- ブリッジグループメンバー
- EtherChannel インターフェイス
- 物理インターフェイス

EtherChannel インターフェイスへのサブインターフェイスの追加

既存のインターフェイスにサブインターフェイスを追加するには、次の手順を実行します。

（注） 続けて別のサブインターフェイスを作成する場合は、[別のサブインターフェイスを作成（Create another）] チェックボックスをオンにして、[作成（Create）] をクリックします。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、EtherChannel を追加する FTD を選択します。右側の [管理（Management）] ペインで、[インターフェイス（Interfaces）] を選択します。

ステップ 4 サブインターフェイスをグループ化するインターフェイスを選択します。右側の操作ウィンドウで、 + New Subinterface ボタンをクリックします。

ステップ 5 （任意）[論理名（Logical Name）] を入力します。

ステップ 6 （任意）説明を入力します。

ステップ 7 （任意）セキュリティゾーンをサブインターフェイスに割り当てます。サブインターフェイスに論理名がない場合は、セキュリティゾーンを割り当てることができないので注意してください。

ステップ 8 VLAN ID を入力します。

ステップ 9 [EtherChannel ID] を入力します。1 ～ 48 の値を使用します。Firepower 1010 シリーズの場合は 1 ～ 8 の値を使用します。

ステップ 10 [IPv4]、[IPv6]、または [詳細設定（Advanced）] タブを選択して、サブインターフェイスの IP アドレスを設定します。

ステップ 11 [作成（Create）] をクリックします。

EtherChannel のサブインターフェイスの編集または削除

既存のサブインターフェイスを変更、またはサブインターフェイスを Etherchannel インターフェイスから削除するには、次の手順を実行します。

（注） サブインターフェイスと EtherChannel インターフェイスには、設定に関する一連のガイドラインと制限事項があります。詳細については、一般的な制限事項を参照してください。

サブインターフェイスの編集

EtherChannel インターフェイスに関連付けられている既存のサブインターフェイスを編集するには、次の手順を実行します。

手順

ステップ 1 CDO にログインします。

ステップ 2 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 3 [デバイス] タブをクリックします。

ステップ 4 [FTD] タブをクリックし、編集する EtherChannel およびサブインターフェイスに関連付けられている FTD を選択します。

ステップ 5 右側の [管理（Management）] ペインで、[インターフェイス（Interfaces）] を選択します。

ステップ 6 サブインターフェイスが属している Etherchannel インターフェイスを見つけて展開します。

ステップ 7 編集対象のサブインターフェイスを選択します。右側の操作ウィンドウで、編集アイコン をクリックします。

ステップ 8 次の項目のいずれかを変更します。

- 論理名
- 状態
- [説明（Description）]
- セキュリティゾーンの割り当て
- VLAN ID

- [IPv4]、[IPv6]、[詳細（Advanced）] タブのいずれかの IP アドレス設定

ステップ 9 [保存（Save）] をクリックします。

EtherChannel からのサブインターフェイスの削除

EtherChannel インターフェイスから既存のサブインターフェイスを削除するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックし、編集する EtherChannel およびサブインターフェイスに関連付けられている FTD を選択します。右側の [管理（Management）] ペインで、[インターフェイス（Interfaces）] を選択します。

ステップ 4 サブインターフェイスが属している Etherchannel インターフェイスを見つけて展開します。

ステップ 5 削除対象のサブインターフェイスを選択します。

ステップ 6 右側の [アクション（Actions）] ペインで、[削除（Remove）] をクリックします。

ステップ 7 削除するサブインターフェイスを確認し、[OK] をクリックします。

仮想 FTD へのインターフェイスの追加

FTDデバイスを導入する際は、その仮想マシンにインターフェイスを割り当てます。その後、ハードウェアデバイスの場合と同じように、FDM から仮想マシンのインターフェイスを設定します。

ただし、仮想マシンにさらに仮想インターフェイスを追加して、FDM に自動的に認識させることはできません。FTD Virtual デバイス向けに追加の物理インターフェイスが必要な場合は、基本的にもう一度やり直す必要があります。新しい仮想マシンを導入することもできれば、次の手順を使用することもできます。

⚠

注意 仮想マシンにインターフェイスを追加するには、FTD Virtual の設定を完全に消去する必要があります。設定でそのまま残しておける唯一の部分は、管理アドレスとゲートウェイ設定です。

はじめる前に

FDM で次の操作を行います。

- FTD Virtual の設定を調べ、新しい仮想マシンで複製する設定値を書き留めておきます。

- [デバイス（Devices）] > [スマートライセンス（Smart License）] > [設定の表示（View Configuration）] を選択し、すべての機能ライセンスを無効にします。

手順

ステップ 1 FTD 仮想デバイスの電源をオフにします。

ステップ 2 仮想マシンソフトウェアを使用して、FTD 仮想デバイスにインターフェイスを追加します。VMware の場合、仮想アプライアンスはデフォルトで e1000（1 Gbit/s）インターフェイスを使用します。また、vmxnet3 または ixgbe（10 Gbit/s）インターフェイスを使用することもできます。

ステップ 3 FTD 仮想デバイスの電源をオンにします。

ステップ 4 FTD仮想コンソールを開いて、ローカルマネージャを削除し、その後、ローカルマネージャを有効にします。ローカルマネージャを削除してから、それを有効にすると、デバイス設定がリセットされ、システムに新しいインターフェイスを認識させることができます。管理インターフェイス設定はリセットされません。次の SSH セッションはコマンドを表示します。

```
> show managers
Managed locally.
> configure manager delete
If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager. Otherwise, those licenses remain assigned to the
device in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled
> show managers
No managers configured.
> configure manager local
>
```

ステップ 5 FDM へのブラウザセッションを開き、デバイスのセットアップウィザードを完了して、デバイスを設定します。詳細については、『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager バージョン x.x.x 用）』の「使用する前に」の章にある「初期設定の完了」のセクションを参照してください。

FTD のスイッチ ポート モード インターフェイス

Firepower 1010 物理インターフェイスごとに、ファイアウォール インターフェイスまたはスイッチポートとしてその動作を設定できます。スイッチポートは、ハードウェアのスイッチ機能を使用して、レイヤ 2 でトラフィックを転送します。同じ VLAN 上のスイッチポートは、ハードウェアスイッチングを使用して相互に通信できます。トラフィックには、FTDセキュリティポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、単一の VLAN に割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数の VLAN に属することができます。バージョン 6.4 に再イメージ化されたデバイスの場合、イーサネット 1/2 ～ 1/8 は VLAN 1 のアクセススイッチポートとして設定されています。バージョン 6.4 以降に手動でアップグレードされたデバイスの場合、イーサネット構成はアップグレード前の構成を維持します。同じ VLAN 上のスイッチポートは、

ハードウェアスイッチングを使用して相互に通信でき、トラフィックには、FTDセキュリティポリシーは適用されないことに注意してください。

アクセスまたはトランク

スイッチポートとして設定されている物理インターフェイスは、アクセスポートまたはトランクポートとして割り当てることができます。

アクセスポートは、トラフィックを 1 つの VLAN にのみ転送し、タグなしのトラフィックのみを受け入れます。トラフィックを単一のホストまたはデバイスに転送する場合は、このオプションを強くお勧めします。また、インターフェイスに関連付ける VLAN を指定する必要があり、指定しないとデフォルトで VLAN 1 に設定されます。

トランクポートは、トラフィックを複数の VLAN に転送します。1 つの VLAN インターフェイスをネイティブトランクポートとして割り当て、少なくとも 1 つの VLAN を関連トランクポートとして割り当てる必要があります。最大 20 のインターフェイスを選択して、スイッチポート インターフェイスに関連付けることができます。これにより、異なる VLAN ID からのトラフィックがスイッチ ポート インターフェイスを通過できるようになります。タグなしのトラフィックがスイッチポートを通過する場合、そのトラフィックは、ネイティブ VLAN インターフェイスの VLAN ID でタグ付けされます。1002 ～ 1005 のデフォルトのファイバ分散データインターフェイス（FDDI）およびトークンリング ID は、VLAN ID に使用できないことに注意してください。

ポートモードの変更

ルーテッドモードに設定されているインターフェイスを VLAN メンバーとして選択すると、CDOは、そのインターフェイスをスイッチポートモードに自動的に変換し、デフォルトでは、そのインターフェイスをアクセスポートとして設定します。その結果、論理名と関連する静的 IP アドレスが、そのインターフェイスから削除されます。

設定の制限

次の制限事項に注意してください。

- 物理 FTD 1010 デバイスのみが、スイッチポートモード設定をサポートしています。仮想 FTD デバイスは、スイッチポートモードをサポートしていません。
- FTD 1010 デバイスは最大 60 の VLAN を許容します。
- スイッチポートモードに設定されるVLANインターフェイスは、名前のないインターフェイスである必要があります。これは、MTU を 1500 バイトに設定する**必要がある**ことを意味します。
- スイッチポートモードとして設定されているインターフェイスは削除**できません**。インターフェイスモードを**スイッチポート**モードから**ルーテッド**モードに手動で変更する必要があります。
- スイッチポートモードに設定されるインターフェイスは、IP アドレスをサポートしません。インターフェイスが現在、VPN、DHCP で参照されているか、それらのために設定さ

れているか、静的ルートに関連付けられている場合は、IPアドレスを手動で削除する**必要があります**。

- ブリッジ グループ インターフェイスのメンバーをスイッチポートとして使用することはできません。
- VLANインターフェイスのMTUは1500バイトである**必要があります**。名前のないVLANインターフェイスは、他の設定をサポートしません。
- スイッチポートモードは、次をサポートしていません。
  - 診断インターフェイス。
  - 動的、マルチキャスト、または等コストマルチパス（ECMP）ルーティング。
  - パッシブインターフェイス。
  - ポート EtherChannel（または EtherChannel のメンバーであるインターフェイスの使用）。
  - サブインターフェイス。
  - フェイルオーバーと状態リンク。

高可用性およびスイッチ ポート モード インターフェイス

高可用性を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。高可用性は、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の高い可用性ネットワーク設定では、両方のユニットのアクティブなスイッチポートがネットワークループにつながります。スイッチング機能には外部スイッチを使用することを推奨します。VLANインターフェイスはフェールオーバーによってモニターできますが、スイッチポートはモニターできません。

（注） ファイアウォール インターフェイスはフェールオーバー リンクとしてのみ使用できます。

テンプレートのスイッチポートモード設定

スイッチポートモード用に設定されたインターフェイスを持つデバイスのテンプレートを作成できます。テンプレートからデバイスにインターフェイスをマッピングするときは、次のシナリオに注意してください。

- テンプレートを適用する前にテンプレート インターフェイスに VLAN メンバーが含まれていない場合、CDO は、同じプロパティを持つ使用可能なデバイスインターフェイスにそれを自動的にマッピングします。

- VLAN メンバーを含まないテンプレートインターフェイスが、**N/A** として設定されているデバイスインターフェイスにマッピングされている場合、CDO は、テンプレートが適用されるデバイスにインターフェイスを自動的に作成します。
- VLAN メンバーを含むテンプレート インターフェイスが、存在しないデバイスインターフェイスにマッピングされている場合、テンプレートの適用は**失敗**します。
- テンプレートは、複数のテンプレートインターフェイスを同じデバイスインターフェイスにマッピングすることをサポートしていません。
- テンプレートの管理インターフェイスは、デバイスの管理インターフェイスにマッピングされる必要があります。

FTD VLAN の設定

サブインターフェイスまたはスイッチポートを設定する場合は、最初に VLAN インターフェイスを設定する必要があります。

（注） FTD デバイスは、最大 60 個の VLAN インターフェイスをサポートします。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、VLAN 作成の対象となるデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[インターフェイス（Interfaces）] をクリックします。

ステップ 5 [インターフェイス（Interfaces）] ページで、  ボタンをクリックします。

ステップ 6 次を設定します。

- [親インターフェイス（Parent Interface）]：サブインターフェイスの追加先となる物理インターフェイスです。いったん作成したサブインターフェイスの親インターフェイスは変更できません。
- （任意）[論理名（Logical Name）]：VLAN の名前を 48 文字以内で設定します。英字は小文字にする必要があります。VLAN と他の VLAN 間またはファイアウォールインターフェイス間をルーティングしない場合は、VLANインターフェイス名を空白のままにします。

  （注） 論理名を入力しない場合は、[詳細オプション（Advanced Options）] の [MTU] を 1500 に設定する必要があります。MTU を 1500 以外に変更する場合は、VLAN に名前を付ける必要があります。

- （任意）[説明（Description）]：説明は 200 文字以内で、改行を入れずに 1 行で入力します。
- （任意）[セキュリティゾーン（Security Zone）]：サブインターフェースをセキュリティゾーンに割り当てます。論理名がない場合は、サブインターフェイスを割り当てることができないので注意してください。サブインターフェイスの作成後にセキュリティゾーンを割り当てることもできます。詳細については、「Firepower インターフェイスの設定におけるセキュリティゾーンの使用」を参照してください。
- （任意）[VLAN ID]：VLAN ID を 1 ～ 4070 の範囲で入力します。これは、このサブインターフェイス上のパケットにタグを付けるために使用されます。

  （注） デフォルトでは VLAN インターフェイスがルーティングされます。後でこの VLAN インターフェイスをブリッジグループに追加すると、CDO では自動的にモードが [BridgeGroupMember] に切り替わります。同様に、この VLAN インターフェイスをスイッチポートモードに変更すると、CDO では自動的にモードが [スイッチポート（Switch Port）] に切り替わります。

- （任意）[サブインターフェイスID（Sub-Interface ID）]：サブインターフェイス ID を 1 ～ 4294967295 の範囲の整数で入力します。この ID は、インターフェイス ID に追加されます。たとえば、Ethernet1/1.100 のようになります。便宜上 VLAN ID を一致させることもできますが、必須ではありません。いったん作成したサブインターフェイスの ID は変更できません。

ステップ 7 [IPv4アドレス（IPv4 Address）] タブをクリックし、[タイプ（Type）] フィールドで次のオプションのいずれかを選択します。

- [スタティック（Static）]：変わらないアドレスを割り当てる必要がある場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

  （注） インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。詳細については、「DHCP サーバーの設定」を参照してください。

- [ダイナミック（Dynamic）]（DHCP）：ネットワーク上のDHCPサーバーからアドレスを取得する必要がある場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
  - [ルートメトリック（Route Metric）]：DHCPサーバーからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは1～255の間です。デフォルトは1です。
  - [デフォルトルートを取得（Obtain Default Route）]：チェックボックスをオンにすると、デフォルトルートがDHCPサーバーから取得されます。通常は、デフォルトのこのオプションを選択します。
- [DHCPアドレスプール（DHCP Address Pool）]：インターフェイスに対して設定されているDHCPサーバーがある場合は、その設定が表示されます。DHCPアドレス プールを編集または削除できます。インターフェイスのIPアドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCPサーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。

ステップ8 （任意）[IPv6アドレス（IPv6 Address）] タブをクリックして、以下を設定します。

- [状態（State）]：グローバルアドレスを設定しない場合にIPv6処理を有効にしてリンクローカルアドレスを自動的に設定するには、[状態（State）]スライダを青にスライドします。リンクローカル アドレスはインターフェイスのMACアドレス（Modified EUI-64形式）に基づいて生成されます。

  （注） IPv6を無効にしても、明示的なIPv6アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスのIPv6処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、チェックボックスをオンにします。IPv6ステートレス自動設定では、デバイスが存在するリンクで使用するIPv6グローバル プレフィックスのアドバタイズメントなどの、IPv6サービスを提供するようにルータが設定されている場合に限り、グローバルなIPv6アドレスが生成されます。IPv6ルーティング サービスがリンクで使用できない場合、リンクローカルIPv6アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスはModified EUI-64インターフェイスIDに基づいています。
- [RAを抑制（Suppress RA）]：ルータアドバタイズメントを抑制するかどうかを指定します。ネイバーデバイスがデフォルトのルータアドレスを動的に学習できるように、FTDはルータアドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各IPv6インターフェイスに定期的に送信されます。

  ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージを抑制することを推奨します。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティックグローバル IPv6 アドレスとネットワークプレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、「Firepower インターフェイスの IPv6 アドレッシング」を参照してください。
- [スタンバイIPアドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IPアドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

ステップ 9 （任意）[詳細（Advanced）] タブをクリックします。

- インターフェイスの状態を高可用性設定でピア装置にフェールオーバーするかどうか判断する際の要素にする場合は、[HAモニタリングの有効化（Enable for HA Monitoring）] を選択します。

  このオプションは、高可用性を設定しない場合は無視されます。インターフェイスの名前を設定しない場合も、無視されます。

- データインターフェイスを管理専用に指定する場合は、、[管理専用（Management Only）] を選択します。

  管理専用インターフェイスはトラフィックの通過を許可しないため、データインターフェイスを管理専用に設定する意味はあまりありません。管理/診断インターフェイスは、常に管理専用であるため、この設定を変更することはできません。

- [IPv6設定（IPv6 Configuration）] を変更します。
  - [IPv6アドレス設定でDHCPを有効化する（Enable DHCP for IPv6 address configuration）]：IPv6 ルータのアドバタイズメントパケットに、管理アドレスアクセス設定フラグを設定するかどうか。このフラグは、取得されるステートレス自動設定のアドレス以外のアドレスの取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。
  - [IPv6のアドレス以外の設定でDHCPを有効化する（Enable DHCP for IPv6 non-address configuration）]：IPv6 ルータのアドバタイズメントパケットに、その他のアドレス設定フラグを設定するかどうか。このフラグは、DHCPv6 から DNS サーバ アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。
  - [DAD の試行（DAD Attempts）]：インターフェイスが重複アドレス検出（DAD）を実行する頻度（0 ～ 600）。デフォルトは 1 です。ステートレス自動設定プロセスでは、DAD はアドレスがインターフェイスに割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を検証します。重複アドレスがインターフェイスのリンク

ローカル アドレスであれば、インターフェイス上で IPv6 パケットの処理は無効になります。重複アドレスがグローバルアドレスであれば、そのアドレスは使用されません。インターフェイスは、ネイバー送信要求メッセージを使用して、重複アドレス検出を実行します。重複アドレス検出（DAD）プロセスを無効にするには、この値を 0 に設定します。

- [MTU]（最大伝送ユニット）を目的の値に変更します。

  デフォルトの MTU は 1500 バイトです。64 ～ 9198（FTDv デバイスの場合は 9000、Firepower 4100/9300 の場合は 9184）の値を指定できます。ジャンボ フレームが頻繁にやり取りされるネットワークでは、大きな値に設定します。

  （注） ASA 5500-X シリーズデバイス、ISA 3000 シリーズデバイス、または FTDv デバイスで MTU を 1500 より大きい値に設定する場合は、VLAN の名前を未設定にし、デバイスを再起動する必要があります。CLI にログインし、reboot コマンドを使用します。HA にデバイスが設定されている場合、スタンバイデバイスも再起動する必要があります。ジャンボ フレームのサポートが常に有効な場合、Firepower モデルを再起動する必要はありません。

- （サブインターフェイスと HA ペアの場合は任意）**MAC アドレス**を設定します。

  デフォルトでは、システムはインターフェイスのネットワーク インターフェイス カード（NIC）に焼き込まれた MAC アドレスを使用します。したがって、インターフェイスのすべてのサブインターフェイスは同じ MAC アドレスを使用するため、サブインターフェイスごとに一意のアドレスを作成する必要がある場合があります。手動設定されたアクティブ/スタンバイ MAC アドレスも、高可用性を設定する場合に推奨されます。MAC アドレスを定義すると、フェールオーバー時にネットワークの一貫性を維持できます。

  - [MACアドレス（MAC Address）]：H.H.H 形式の Media Access Control。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は 000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。
  - [スタンバイ MAC アドレス（Standby MAC Address）]：HA ペアで使用します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 10 このデバイスに別のサブインターフェイスを作成する場合は、サブインターフェイスの設定を完了する前に、[別のサブインターフェイスを作成（Create another）] をオンにします。

ステップ 11 （任意）作成時にサブインターフェイスをアクティブにするには、ポップアップウィンドウの右上隅にある [状態（State）] スライダーを灰色から青色に切り替えます。

ステップ 12 [OK] をクリックします。

ステップ 13 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

スイッチポートモード用 FTD VLAN の設定

構成する前に、スイッチポートモードの制限事項を必ずお読みください。詳細については、『FTD のスイッチ ポート モード インターフェイス』を参照してください。

（注） VLAN メンバーの物理インターフェイスへの割り当てや編集はいつでも実行できます。新しい構成を確認したら、必ず変更をデバイスに展開してください。

スイッチポートモードでの VLAN インターフェイスの作成

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、インターフェイスを設定するデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[インターフェイス（Interfaces）] をクリックします。

ステップ 5 [インターフェイス（Interfaces）] ページで、  ボタンをクリックし、[VLANインターフェイス（VLAN Interface）] を選択します。

ステップ 6 [VLANメンバー（VLAN Members）] タブを表示し、目的の物理インターフェイスを選択します。

（注） アクセスまたはネイティブトランク用に設定された VLAN インターフェイスを参照するメンバーを追加する場合、1 つの VLAN のみをメンバーとして選択できます。関連トランク用に設定された VLAN インターフェイスを参照する物理インターフェイスには、最大 20 個のインターフェイスをメンバーとして追加できます。

ステップ 7 「FTD VLAN の設定」の説明に従って、残りの VLAN インターフェイスを設定します。

ステップ 8 [保存（Save）] をクリックします。VLAN 設定をリセットし、IP アドレスをインターフェイスに再割り当てすることを確認します。

ステップ 9 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、複数の変更を後から一度に展開します。

スイッチポートモードに使用する既存の物理インターフェイスの設定

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、インターフェイスを設定するデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[インターフェイス（Interfaces）] をクリックします。

ステップ 5 [インターフェイス（Interfaces）] ページで、変更する物理インターフェイスを選択します。右側の操作ウィンドウで、編集アイコン をクリックします。

ステップ 6 スイッチポートモードに設定されるインターフェイスは、論理名をサポートしません。インターフェイスに論理名がある場合は、削除します。

ステップ 7 [モード（Mode）] を見つけ、ドロップダウンメニューで [スイッチポート（Switch Port）] を選択します。

ステップ 8 スイッチポートモードの物理インターフェイスを設定します。

- （任意）このスイッチポートを保護対象として設定するには、[保護ポート（Protected Port）] チェックボックスをオンにします。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。スイッチポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートにこのオプションを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

- [使用タイプ（Usage Type）] で、[アクセス（Access）] または [トランク（Trunk）] を選択します。必要なポートタイプを判別するには、「FTD のスイッチ ポート モード インターフェイス」を参照してください。

  - [トランク（Trunk）] を選択した場合、1 つの VLAN インターフェイスをタグなしトラフィックを転送するための [ネイティブトランク VLAN（Native Trunk VLAN）] として選択し、1 つ以上をタグ付きトラフィックを転送するための [関連する VLAN（Associated VLAN）] として選択する必要があります。 アイコンをクリックして、既存の物理インターフェイスを表示します。関連する VLAN として最大 20 個の VLAN インターフェイスを選択できます。

  - [新しい VLAN を作成（Create new VLAN）] をクリックすると、アクセスモードに設定された新しい VLAN インターフェイスを作成できます。

ステップ 9 [保存（Save）] をクリックします。VLAN 設定をリセットし、IP アドレスをインターフェイスに再割り当てすることを確認します。

ステップ 10 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Firepower インターフェイスの表示とモニターリング

Firepower インターフェイスを表示するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、インターフェイスを表示するデバイスをクリックします。

ステップ 4 右側の [管理（Management）] ペインで [インターフェイス（Interfaces）] をクリックします。

ステップ 5 インターフェイステーブルでインターフェイスを選択します。

- インターフェイスの行を展開すると、サブインターフェイスの情報が表示されます。
- 右側には詳細なインターフェイス情報が表示されます。

CLI でのインターフェイスのモニタリング

SSH を使用してデバイスに接続し、以下のコマンドを実行することで、インターフェイスに関する基本的な情報、動作、および統計を表示できます。

SSH を使用してデバイスに簡単に接続するには、モニターリングする FTD を SSH デバイスとしてオンボードしてから、CDO で >_ コマンド ライン インターフェイスを使用します。

- **show interface** は、インターフェイスの統計情報および設定情報を表示します。このコマンドには多数のキーワードがあり、必要な情報を取得するために使用できます。使用可能なオプションを表示するには、「?」をキーワードとして使用します。
- **show ipv6 interface** は、インターフェイスに関する IPv6 設定情報を表示します。
- **show bridge-group** は、メンバー情報や IP アドレスを含む、ブリッジ仮想インターフェイス（BVI）に関する情報を表示します。
- **show conn** は、インターフェイスを介して現在確立されている接続に関する情報を表示します。

- **show traffic** は、各インターフェイスを介して移動するトラフィックに関する統計情報を表示します。
- **show ipv6 traffic** は、デバイスを介して移動する IPv6 トラフィックに関する統計情報を表示します。
- **show dhcpd** は、インターフェイスでの DHCP の使用状況、特にインターフェイスで設定されている DHCP サーバーに関する統計情報とその他の情報を表示します。

Firepower デバイスに追加したインターフェイスの FXOS を使用した同期

Firepower 4100 シリーズまたは 9300 シリーズデバイスで、Firepower eXtensible Operating System（FXOS）Chassis Manager を使用して Firepower デバイスにインターフェイスを追加すると、CDO では設定の変更が認識されず、設定の競合が報告されます。

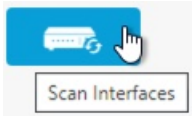
CDO に新しく追加されたインターフェイスを表示するには、次の手順に従います。

手順

ステップ 1 FDM にログインします。

ステップ 2 FDM のメインページの [インターフェイス（Interfaces）] パネルで、[すべてのインターフェイスの表示（View All Interfaces）] をクリックします。

ステップ 3 [インターフェイスのスキャン（Scan Interfaces）] ボタンをクリックします。



ステップ 4 インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。

ステップ 5 変更を FDM に展開します。

ステップ 6 管理者またはネットワーク管理者の権限で CDO にログインします。

ステップ 7 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 8 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 9 [FTD] タブをクリックし、新しいインターフェイスが想定どおりに設定されているデバイスを選択します。

ステップ 10 [変更の確認（Checking for Changes ）] をクリックすると、すぐにデバイスの設定のコピーが CDO に保存されている設定のコピーと比較されます。CDO ではインターフェイスの変更が検出され、デバイスの [デバイスとサービス（Devices & Services）] ページで「競合が検出されました」と状況が報告されます。

ステップ 11 検出された競合を解決するには、[競合の確認（Review Conflict）] をクリックして、アウトオブバンドの変更を受け入れます。

ルーティング

ルーティングは、送信元から宛先にネットワーク経由で情報を移動する行為のことです。その間に、通常は少なくとも 1 つの中間ノードがあります。ルーティングには、最適なルーティングパスの決定と、ネットワーク経由のパケットの転送という 2 つの基本的なアクティビティが含まれます。

Cisco Defense Orchestrator（CDO）を使用すると、Firepower Threat Defense（FTD）デバイスのデフォルトルートおよびその他の静的ルートを定義できます。ここでは、ルーティングの基本と CDO を使用して FTD デバイスで静的ルーティングを設定する方法について説明します。

- 静的ルーティングとデフォルトルートについて
- ルーティング テーブルとルート選択
- FTD デバイスのスタティックルートとデフォルトルートの設定
- ルーティングのモニタリング

静的ルーティングとデフォルトルートについて

接続されていないホストまたはネットワークにトラフィックをルーティングするには、ホストまたはネットワークへのルートを定義する必要があります。定義したルートは静的ルートになります。デフォルトルートを設定することも検討してください。デフォルトルートは、他の方法でデフォルトのネットワークゲートウェイにルーティングされていないすべてのトラフィックを対象とし、通常はネクストホップルータです。

関連情報：

- デフォルトルート
- スタティック ルート

デフォルトルート

特定のネットワークへのルートが不明な場合、最も単純なオプションは、すべてのトラフィックを上流に位置するルータに送信するデフォルトルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルトルートは、スタティックルートが定義されていない IP パケットすべてを、FTD デバイスが送信するゲートウェイの IP アドレスを特定するルートです。デフォルトルートとは、つまり宛先の IP アドレスとして 0.0.0.0/0（IPv4）または ::/0（IPv6）が指定されたスタティックルートのことです。

スタティック ルート

スタティックルートは、あるネットワークから別のネットワークへのルートであり、手動で定義してルーティングテーブルに入力します。次の場合は、スタティック ルートを使用します。

- ネットワークは小規模で安定しており、デバイス間のルートの追加や変更を手動で簡単に管理できます。
- ネットワークがサポート対象外のルータ ディスカバリ プロトコルを使用している。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。
- 場合によっては、デフォルトルートだけでは不十分である。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティックルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルトルートは、FTD デバイスに直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミック ルーティング プロトコルをサポートしていない機能を使用している。

制限事項

- CDO は、現在、ASA デバイスまたは FTD デバイス上の仮想トンネルインターフェイス（VTI）トンネルの管理、監視、使用をサポートしていません。VTI トンネルが設定されているデバイスを CDO にオンボーディングすることは可能ですが、VTI インターフェイスは無視されます。セキュリティゾーンまたはスタティックルートが VTI を参照する場合、CDO は VTI 参照を除いてセキュリティゾーンとスタティックルートを読み取ります。VTI トンネルに対する CDO のサポートは近日中に提供されます。
- ソフトウェアバージョン 7.0 以降を実行している FTD では、等コストマルチパス（ECMP）トラフィックゾーンを設定できます。FTD を CDO にオンボードすると、グローバル VRF ルートの ECMP 設定を読み込めますが、変更することはできません。同じメトリック値を持つ同じ宛先ネットワークへのルートが許可されないためです。FDM を使用して ECMP トラフィックゾーンを作成および変更すると、CDO に読み込むことができます。ECMP の詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager、バージョン 7.0 以降』[英語] で「Routing Basics and Static Routes」章の「Equal-Cost Multi-Path（ECMP）Routing」項を参照してください。

ルーティング テーブルとルート選択

NAT 変換（xlates）およびルールで出力インターフェイスを決定しない場合、システムはルーティングテーブルを使用してパケットのパスを決定します。

ルーティングテーブルのルートには、指定ルートに相対的な優先順位を定める「アドミニストレーティブ ディスタンス」というメトリックが含まれています。パケットが複数のルート エントリと一致する場合、最短距離のルート エントリが使用されます。直接接続されたネットワーク（インターフェイス上で定義されたネットワーク）の距離は 0 のため、これが常に優先

されます。スタティック ルートのデフォルトの距離は 1 ですが、1 ～ 254 の距離で作成できます。

特定の宛先が指定されたルートは、デフォルト ルート（宛先が 0.0.0.0/0 または ::/0 のルート）よりも優先されます。

ルーティング テーブルへの入力方法

Firepower Threat Defense デバイス ルーティング テーブルには、静的に定義されたルートと直接接続されたルートを入力できます。同じルートが複数の方法で入力される可能性があります。同じ宛先への 2 つのルートがルーティング テーブルに追加されると、ルーティング テーブルに残るルートは次のように決定されます。

- 2 つのルートのネットワーク プレフィックス長（ネットワーク マスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティングテーブルに入力されます。入力された後は、パケット転送ロジックが 2 つのうちどちらを使用するかを決定します。

たとえば、次のルートがルーティングテーブルに入力されているとします。

- 192.168.32.0/24
- 192.168.32.0/19

192.168.32.0/24 ルートの方がネットワークプレフィクスが長いにもかかわらず、両方のルートがルーティングテーブルにインストールされます。この 2 つのルートのプレフィックス長（サブネットマスク）がそれぞれ異なるためです。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- 同じ宛先への複数のパスがルーティングテーブルに入力されている場合、スタティック ルートの場合と同様に、より適切なメトリックを持つルートがルーティングテーブルに入力されます。

メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックの判定に使用されるパラメータは、ルーティング プロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティングテーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コスト パスに対してロード バランシングが行われます。

関連情報：

- 転送の決定方法

転送の決定方法

転送の決定は次の順序で行われます。

- NAT 変換（xlate）とルールによって、出力インターフェイスが決定されます。NAT ルールによって出力インターフェイスが決定されない場合、ルーティングテーブルを使用してパケットのパスが決定されます。

- 宛先が、ルーティング テーブル内のエントリと一致しない場合、パケットはデフォルトルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティング テーブル内の複数のエントリと一致し、パケットはネットワークプレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用してインターフェイスに到着したとします。
- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは10.1.1.2宛てに送信されます。このアドレスはまた、ルーティングテーブルの他のルートにも含まれますが、ルーティングテーブル内では192.168.32.0/24の方が長いプレフィックスを持ちます（24 ビットと 19 ビット）。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。

（注） ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

FTD デバイスのスタティックルートとデフォルトルートの設定

Firepower Threat Defense（FTD）デバイスでスタティックルートを定義して、システムのインターフェイスに直接接続されていないネットワークに向かうパケットの送信先をデバイスが認識できるようにします。

デフォルトルートの作成を検討してください。これは、ネットワーク 0.0.0.0/0 のルートです。このルートは、既存の NAT変換、スタティック NAT ルール、またはその他のスタティックルートでは出力インターフェイスを判別できないパケットの送信先を定義します。

デフォルト ゲートウェイを使用してもすべてのネットワークに到達できない場合、他のスタティック ルートが必要になる可能性があります。たとえば、デフォルト ルートは通常、外部インターフェイスの上流に位置するルータです。デバイスに直接接続されていない追加の内部ネットワークがあり、それらにデフォルト ゲートウェイを介してアクセスできない場合、これらそれぞれの内部ネットワークに対してスタティック ルートが必要です。

システムのインターフェイスに直接接続されたネットワークのスタティック ルートを定義することはできません。システムは自動でこれらのルートを作成します。

手順

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 **FTD** デバイスをクリックし、静的ルートを定義するデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ルーティング（Routing）] をクリックします。

ステップ 5 [ルーティングの選択（Select Routing）] ページで、次のいずれかを実行します。

- 新しい静的ルートを追加するには、プラスボタン をクリックします。
- 編集するルートの編集アイコンをクリックします。

ルートが不要になったら、ルートの [ごみ箱（trash can）] アイコンをクリックして削除します。

ステップ 6 ルート プロパティの設定

- [プロトコル（Protocol）]：ルートが IPv4 アドレス用か IPv6 アドレス用かを選択します。
- [インターフェイス（Interface）]：トラフィックの送信経路となるインターフェイスを選択します。ゲートウェイ アドレスは、このインターフェイスを介してアクセス可能である必要があります。
- [ゲートウェイ（Gateway）]：宛先ネットワークへのゲートウェイの IP アドレスを識別するネットワークオブジェクトを選択します。トラフィックはこのアドレスに送信されます。
- [メトリック（Metric）]：ルートのアドミニストレーティブ ディスタンス。1～254 の範囲で指定します。スタティック ルートのデフォルトは 1 です。インターフェイスとゲートウェイの間に追加ルータがある場合、アドミニストレーティブ ディスタンスとしてホップ数を入力します。

  アドミニストレーティブ ディスタンスは、ルートを比較するために使用されるパラメータです。番号が低いほど、ルートに高い優先順位が与えられます。接続されたルート（デバイスのインターフェイスに直接接続されているネットワーク）は、スタティック ルートよりも常に優先されます。
- [宛先ネットワーク（Destination Network）]：宛先ネットワークを識別するネットワークオブジェクトを選択します。ホストが含まれ、このルートのゲートウェイが使用される宛先ネットワークです。

  デフォルトルートを定義するには、事前定義された any-ipv4 または any-ipv6set ネットワークオブジェクトを使用するか、0.0.0.0/0（IPv4）または ::/0（IPv6）ネットワークのオブジェクトを作成します。

ステップ 7 [OK] をクリックします。

ステップ 8 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

静的ルートの例

この例で使用されるアドレスについては、「静的ルートのネットワーク構成図」を参照してください。

宛先ネットワーク 20.30.1.0/24 の 20.30.1.2 にあるホストへのリターントラフィックを許可する静的ルートを作成することを目的としています。

パケットは、宛先に到達するためにどのパスでも通過できます。ネットワークはインターフェイス上でパケットを受信すると、宛先への最適なルートを使用するためにパケットの転送先を決定します。

（注） DMZ はインターフェイスに直接接続されているため、静的ルートはありません。

たとえば、宛先に到達するための次の 2 つのルートについて考えます。

ルート 1：

手順

ステップ 1 パケットは外部インターフェイス **209.165.201.0/27** に戻り、**20.30.1.2** を探します。

ステップ 2 パケットに対して、宛先と同じネットワーク上にあるゲートウェイ 192.168.1.2 に**内部**インターフェイスを介して到達するように指示します。

ステップ 3 そこから、そのネットワークの**ゲートウェイアドレス** 20.30.1.1 によって宛先ネットワークを識別します。

ステップ 4 IP アドレス 20.30.1.2 は、20.30.1.1 と同じサブネット上にあります。ルータはパケットをスイッチに転送し、スイッチはそのパケットを 20.30.1.2 に転送します。

インターフェイス：内部、宛先ネットワーク：20.30.1.0/24、ゲートウェイ：192.168.1.2、メトリック：1

ルート 2：

手順

ステップ 1 パケットは外部インターフェイス **209.165.201.0/27** に戻り、**20.30.1.2** を探します。

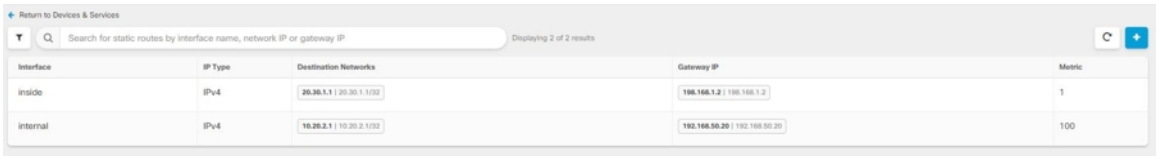
ステップ 2 パケットに対して、宛先ネットワークから複数ホップ離れたゲートウェイ 192.168.50.20 に**内部**インターフェイスを介して到達するように指示します。

ステップ 3 そこから、そのネットワークの**ゲートウェイアドレス** 20.30.1.1 によって宛先ネットワークを識別します。

ステップ 4 IP アドレス 20.30.1.2 は、20.30.1.0 と同じサブネット上にあります。ルータはパケットをスイッチに転送し、スイッチはそのパケットを 20.30.1.2 に転送します。

インターフェイス：内部、宛先ネットワーク：20.30.1.0/24、ゲートウェイ：192.168.50.20、メトリック：100

これらのルートの完成した静的ルートの追加テーブルは、次のようになります。



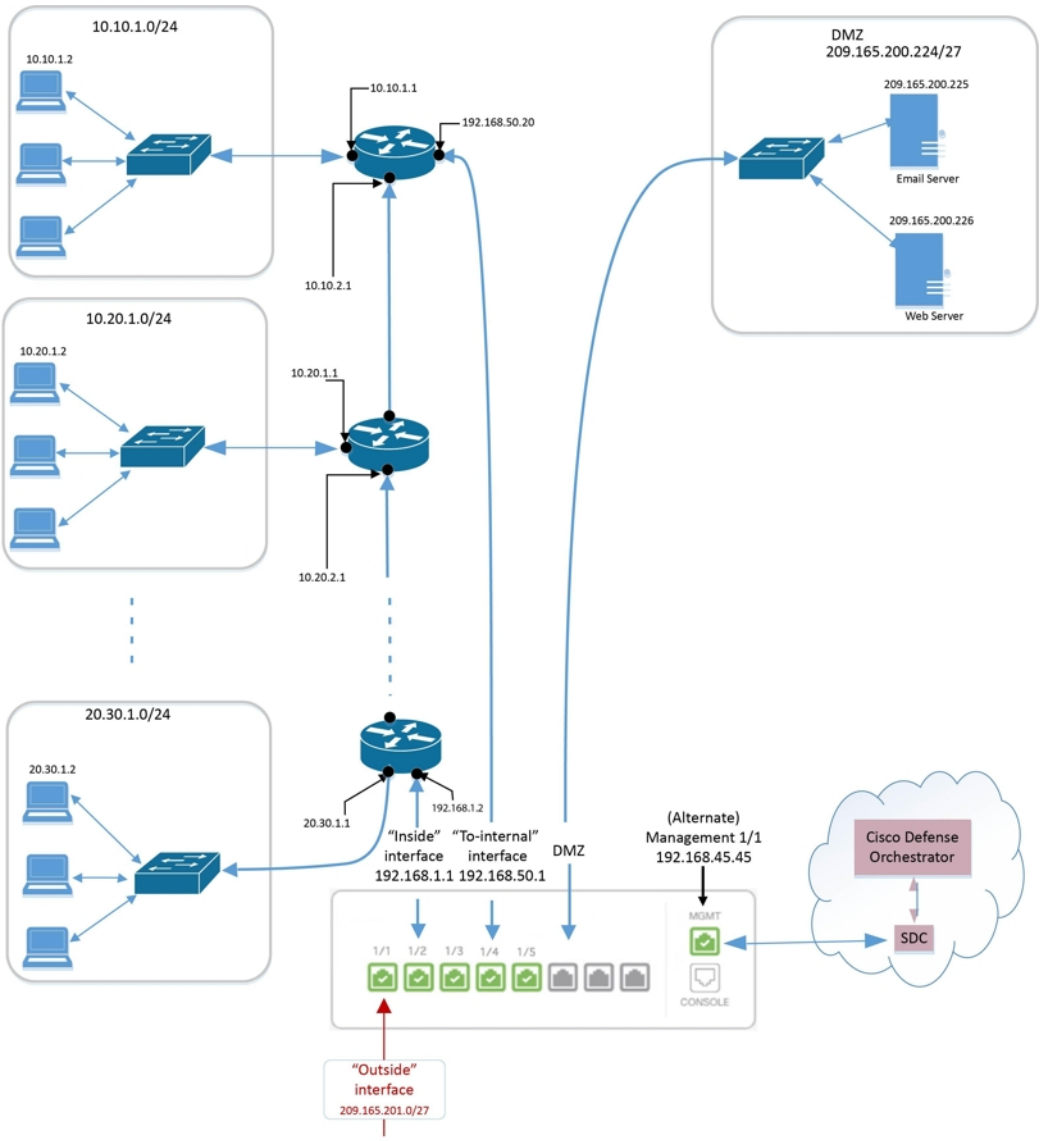
ルーティングのモニタリング

ルーティングをモニターリングし、トラブルシューティングを行うには、デバイスの Firepower Device Manager（FDM）を開いて CLI コンソールに移動するか、SSH を使用してデバイスの CLI にログインし、次のコマンドを使用します。

- `show route` は、直接接続されたネットワークのルートを含め、データ インターフェイスのルーティング テーブルを表示します。
- `show ipv6 route` は、直接接続されたネットワークのルートを含め、データ インターフェイスの IPv6 ルーティング テーブルを表示します。
- `show network` は、管理ゲートウェイを含め、仮想管理インターフェイスの設定を表示します。仮想インターフェイスを介したルーティングは、データインターフェイスを管理ゲートウェイに指定しなければ、データ インターフェイス ルーティング テーブルによって処理されません。
- `show network-static-routes` は、`configure network static-routes` コマンドを使用して仮想管理インターフェイス用に設定されたスタティック ルートを表示します。通常、ほとんどの場合、管理ゲートウェイは管理ルーティングに対して十分機能するため、スタティック ルートは存在しません。これらのルートは、データ インターフェイス上のトラフィックには使用できません。このコマンドは、CLI コンソールでは使用できません。

静的ルートのネットワーク構成図

次のネットワーク構成図に基づいてFTDデバイスのスタティックルートとデフォルトルートの設定について説明します。



仮想ルーティングおよびフォワーディングについて

VRF について

仮想ルーティングおよびフォワーディング（VRF）により、ルーティングテーブルの複数のインスタンスがルータに同時に存在できます。Firepower バージョン 6.6 では、デフォルトの VRF テーブルとユーザ作成の VRF テーブルを持つことができるようになりました。1 つの VRF テーブルで、EX、OSPF、BGP、IGRP などのさまざまなルーティングプロトコルを複数タイプ処理できます。VRF テーブル内の各ルーティングプロトコルは、エントリとしてリストされます。複数のタイプの一般的なルーティングプロトコルの処理に加えて、別の VRF のインターフェイスを参照するようにルーティングプロトコルを設定できます。これにより、複数のデバイスを使用せずにネットワークパスをセグメント化できます。

詳細については、「仮想ルータと、仮想ルーティングおよびフォワーディング（VRF）について」を参照してください。

CDO に搭載された VRF

この機能は Firepower バージョン 6.6 の新機能です。FTD が CDO にオンボードされると、デバイスルーティングページには、FTD デバイスのグローバルルータで定義された VRF のみが読み込まれてサポートされます。CDO でグローバル VRF を表示するには、[デバイスとサービス（Devices & Service）] ページでデバイスを選択し、ウィンドウの右側にある [管理（Management）] ペインで [ルーティング（Routing）] を選択します。ここでグローバル VRF を表示、変更、および削除できます。 CDO は FDM から設定を読み込む際に VRF の名前を保持します。

また、CDO ではユーザー定義の仮想ルータで設定した VRF は読み込まれません。FDM を介して VRF テーブルを作成および管理する必要があります。

グローバルルートおよびユーザ定義ルートの詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager、バージョン 7.0 以降』[英語] で「Virtual Routers」章の「Managing Virtual Routers」項を参照してください。

オブジェクト

オブジェクトは、1つ以上のセキュリティポリシーで使用できる情報のコンテナです。オブジェクトを使用すると、ポリシーの一貫性を簡単に維持できます。単一のオブジェクトを作成し、異なるポリシーを使用して、オブジェクトを変更すると、その変更がオブジェクトを使用するすべてのポリシーに伝播されます。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。

デバイスをオンボードすると、CDO はそのデバイスで使用されるすべてのオブジェクトを認識して保存し、[オブジェクト（Objects）] ページにリストします。[オブジェクト（Objects）] ページから、既存のオブジェクトを編集したり、セキュリティポリシーで使用する新しいオブジェクトを作成したりできます。

CDO では、複数のデバイスで使用されるオブジェクトを共有オブジェクトと呼び、[オブジェクト（Objects）] ページでこのバッジ でそれらを識別します。

共有オブジェクトが何らかの「問題」を引き起こし、複数のポリシーまたはデバイス間で完全に共有されなくなる場合があります。

- **重複オブジェクト**とは、同じデバイス上にある、名前は異なるが値は同じである2つ以上のオブジェクトです。通常、重複したオブジェクトは同じ目的を果たし、さまざまなポリシーによって使用されます。重複するオブジェクトは、この問題のアイコン で識別されます。
- **不整合オブジェクト**とは、2 つ以上のデバイス上にある、名前は同じだが値は異なるオブジェクトです。ユーザーは、さまざまな設定の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値

になり、不整合が生じます。不整合オブジェクトは、この問題のアイコン で識別されます。

- **未使用オブジェクト**は、デバイス構成に存在するものの、別のオブジェクト、アクセスリスト、NATルールによって参照されていないオブジェクトです。未使用オブジェクトは、この問題のアイコン で識別されます。

ルールやポリシーですぐに使用するためのオブジェクトを作成することもできます。ルールやポリシーに関連付けないオブジェクトを作成できます。関連付けられていないオブジェクトをルールまたはポリシーで使用すると、CDOはそのコピーを作成し、そのコピーを使用します。

[オブジェクト（Objects）]メニューに移動するか、ネットワークポリシーの詳細でオブジェクトを表示することにより、CDO によって管理されているオブジェクトを表示できます。

CDO を使用すると、サポートされているデバイス全体のネットワークオブジェクトとサービスオブジェクトを 1 つの場所から管理できます。CDO を使用すると、次の方法でオブジェクトを管理できます。

- さまざまな基準に基づいて、すべてのオブジェクトを検索してフィルタリングします。
- デバイス上の重複、未使用、および不整合のオブジェクトを見つけて、それらのオブジェクトの問題を統合、削除、または解決します。
- 関連付けられていないオブジェクトを見つけて、それらが未使用であれば削除します。
- デバイス間で共通の共有オブジェクトを検出します。
- 変更をコミットする前に、オブジェクトへの変更が一連のポリシーとデバイスに与える影響を評価します。
- 一連のオブジェクトとそれらの関係を、さまざまなポリシーやデバイスで比較します。
- デバイスが CDO にオンボードされた後、デバイスによって使用されているオブジェクトをキャプチャします。

オンボードされたデバイスからのオブジェクトの作成、編集、または読み取りで問題が発生した場合は、CDO のトラブルシューティングを参照してください。

オブジェクト

オブジェクトは、1つ以上のセキュリティポリシーで使用できる情報のコンテナです。オブジェクトを使用すると、ポリシーの一貫性を簡単に維持できます。単一のオブジェクトを作成し、異なるポリシーを使用して、オブジェクトを変更すると、その変更がオブジェクトを使用するすべてのポリシーに伝播されます。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。

デバイスをオンボードすると、CDO はそのデバイスで使用されるすべてのオブジェクトを認識して保存し、[オブジェクト（Objects）] ページにリストします。[オブジェクト（Objects）] ページから、既存のオブジェクトを編集したり、セキュリティポリシーで使用する新しいオブジェクトを作成したりできます。

CDO では、複数のデバイスで使用されるオブジェクトを共有オブジェクトと呼び、[オブジェクト（Objects）] ページでこのバッジ でそれらを識別します。

共有オブジェクトが何らかの「問題」を引き起こし、複数のポリシーまたはデバイス間で完全に共有されなくなる場合があります。

- **重複オブジェクト**とは、同じデバイス上にある、名前は異なるが値は同じである 2 つ以上のオブジェクトです。通常、重複したオブジェクトは同じ目的を果たし、さまざまなポリシーによって使用されます。重複するオブジェクトは、この問題のアイコン で識別されます。
- **不整合オブジェクト**とは、2 つ以上のデバイス上にある、名前は同じだが値は異なるオブジェクトです。ユーザーは、さまざまな設定の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値になり、不整合が生じます。不整合オブジェクトは、この問題のアイコン で識別されます。
- **未使用オブジェクト**は、デバイス構成に存在するものの、別のオブジェクト、アクセスリスト、NAT ルールによって参照されていないオブジェクトです。未使用オブジェクトは、この問題のアイコン で識別されます。

ルールやポリシーですぐに使用するためのオブジェクトを作成することもできます。ルールやポリシーに関連付けないオブジェクトを作成できます。関連付けられていないオブジェクトをルールまたはポリシーで使用すると、CDO はそのコピーを作成し、そのコピーを使用します。

[オブジェクト（Objects）] メニューに移動するか、ネットワークポリシーの詳細でオブジェクトを表示することにより、CDO によって管理されているオブジェクトを表示できます。

CDO を使用すると、サポートされているデバイス全体のネットワークオブジェクトとサービスオブジェクトを 1 つの場所から管理できます。CDO を使用すると、次の方法でオブジェクトを管理できます。

- さまざまな基準に基づいて、すべてのオブジェクトを検索してフィルタリングします。
- デバイス上の重複、未使用、および不整合のオブジェクトを見つけて、それらのオブジェクトの問題を統合、削除、または解決します。
- 関連付けられていないオブジェクトを見つけて、それらが未使用であれば削除します。
- デバイス間で共通の共有オブジェクトを検出します。
- 変更をコミットする前に、オブジェクトへの変更が一連のポリシーとデバイスに与える影響を評価します。
- 一連のオブジェクトとそれらの関係を、さまざまなポリシーやデバイスで比較します。
- デバイスが CDO にオンボードされた後、デバイスによって使用されているオブジェクトをキャプチャします。

オンボードされたデバイスからのオブジェクトの作成、編集、または読み取りで問題が発生した場合は、CDO のトラブルシューティングを参照してください。

オブジェクト タイプ

以下の表では、デバイス用に作成し、CDO を使用して管理できるオブジェクトについて説明します。

表 *1 : Firepower Threat Defense*（*FTD*）オブジェクトタイプ

オブジェクト	説明
アプリケーション フィルタ	アプリケーション フィルタ オブジェクトは、IP 接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタを定義します。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、トラフィックを制御できます。
RA VPN AnyConnect クライアントプロファイルのアップロード	AnyConnect クライアント プロファイル オブジェクトは、通常はリモートアクセス VPN ポリシーの構成で使用するファイルオブジェクトおよび表明ファイルです。このオブジェクトには、AnyConnect クライアントプロファイルと AnyConnect クライアントイメージファイルを含めることができます。
証明書フィルタ	デジタル証明書は、認証に使用されるデジタル ID を提供します。証明書は、SSL（セキュア ソケット レイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。
DNS Group	www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決するのには、DNS サーバーが必要です。管理インターフェイスとデータインターフェイスに異なる DNS グループオブジェクトを構成できます。
位置情報（GeoLocation）	地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IP アドレスを使用する代わりに、これらのオブジェクトをポリシーで使用してトラフィックを制御できます。

オブジェクト	説明
IKEv1ポリシー	IKEv1 ポリシーオブジェクトには、VPN 接続を定義する際に IKEv1 ポリシーに必要なパラメータが含まれています。
IKEv2 ポリシー	IKEv2 ポリシーオブジェクトには、VPN 接続を定義する際に IKEv2 ポリシーに必要なパラメータが含まれています。
IKEv1 IPSec プロポーザル	IPsec プロポーザル オブジェクトは、IKE フェーズ 1 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。
IKEv2 IPSec プロポーザル	IPsec プロポーザル オブジェクトは、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。
ネットワーク（Network）	ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ばれます）。
セキュリティ ゾーン	セキュリティ ゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。
サービス	サービスオブジェクト、サービスグループ、ポートグループは、TCP/IP プロトコルスイートの一部が考慮されたプロトコルまたはポートを含む再利用可能なコンポーネントです。
SGT グループ	SGT ダイナミックオブジェクトは、ISE によって割り当てられた SGT に基づいて送信元または宛先アドレスを識別し、着信トラフィックと照合できます。

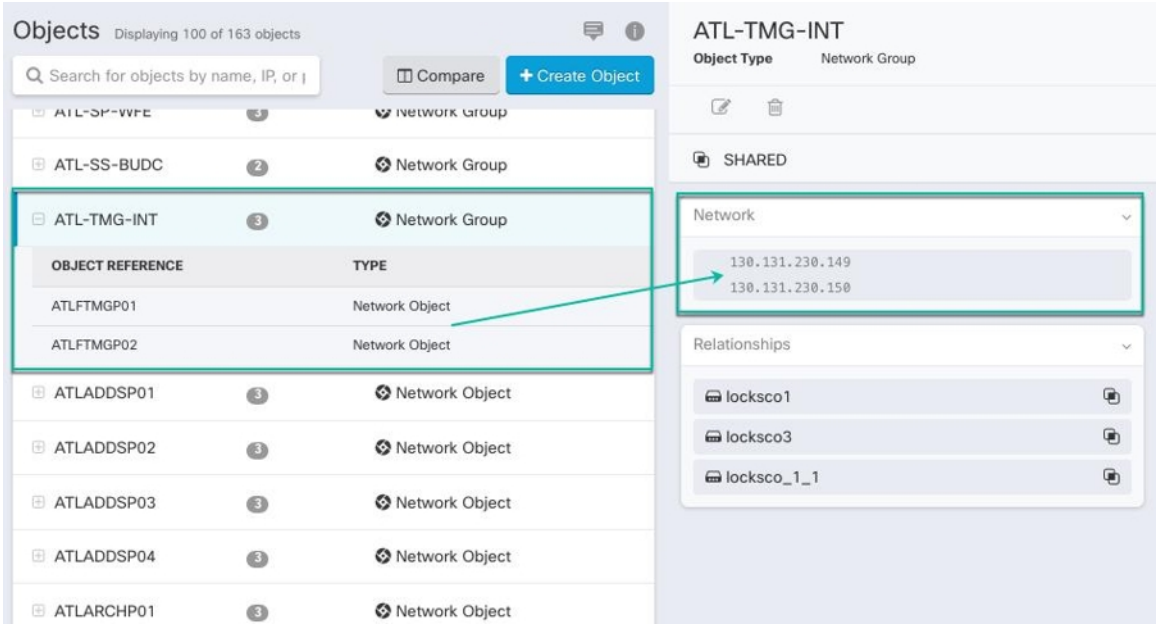
オブジェクト	説明
Syslog サーバー	syslog サーバーのオブジェクトはコネクション型メッセージまたは診断システム ログ（syslog）メッセージを受信できるサーバーを指定します。
URL	URL オブジェクトとグループ（URL オブジェクトと総称する）を使用して、Web リクエストの URL または IP アドレスを定義します。これらのオブジェクトを使用して、アクセス制御ポリシーに手動の URL フィルタリング、またはセキュリティ インテリジェンス ポリシーにブロッキングを実装できます。

共有オブジェクト

Cisco Defense Orchestrator（CDO）では、複数のデバイス上の同じ名前と同じ内容のオブジェクトを共有オブジェクトと呼びます。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 か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、CDO 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。CDO 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。



オブジェクトのオーバーライド

オブジェクトのオーバーライドを使用すると、特定のデバイス上の共有ネットワークオブジェクトの値をオーバーライドできます。CDO は、オーバーライドを構成するときに指定したデバイスに対応する値を使用します。これらのオブジェクトは、名前は同じで値が異なる複数のデバイス上にありますが、CDOは、これらの値がオーバーライドとして追加されただけでは、それらを**不整合オブジェクト**として識別しません。

ほとんどのデバイスに有効な定義を設定したオブジェクトを作成した後、異なる定義を必要とする少数のデバイスについて、オーバーライドを使用してオブジェクトに対する変更内容を指定できます。また、すべてのデバイスに対してオーバーライドする必要があるオブジェクトを作成し、そのオブジェクトを使用してすべてのデバイスに適用する単一のポリシーを作成することもできます。オブジェクトオーバーライドでは、デバイス全体で使用する共有ポリシーの小さなセットを作成し、個々のデバイスの必要に応じてポリシーを変更できます。

たとえば、各オフィスにプリンタサーバーがあり、プリンタサーバーオブジェクト`print-server`を作成しているシナリオを考えてみましょう。ACLには、プリンタサーバーのインターネットへのアクセスを拒否するルールを設定しています。プリンタ サーバー オブジェクトには、オフィスごとに変更できるデフォルト値があります。これを行うには、オブジェクトのオーバーライドを使用し、すべての場所でルールと「printer-server」オブジェクトの一貫性を維持します（値は異なる場合があります）。

（注） CDO を使用すると、ルールセット内のルールに関連付けられたオブジェクトを上書きできます。新しいオブジェクトをルールに追加する場合、デバイスをルールセットに接続して変更を保存しないと、オブジェクトを上書きできません。詳細については、「FTD に対するルールセットの設定」を参照してください。

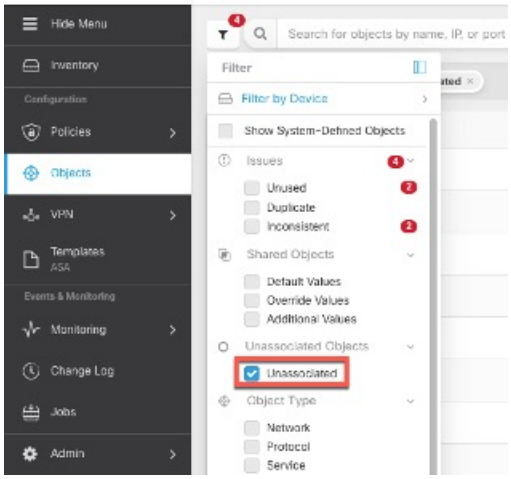
（注） 一貫性のないオブジェクトがある場合は、オーバーライドを使用してそれらを1つの共有オブジェクトに結合できます。詳細については、不整合オブジェクトの問題を解決するを参照してください。

関連付けのないオブジェクト

ルールやポリシーですぐに使用するためのオブジェクトを作成できますが、ルールやポリシーに関連付けないオブジェクトを作成することもできます。関連付けられていないオブジェクトをルールまたはポリシーで使用すると、CDO はそのコピーを作成し、そのコピーを使用します。関連付けられていない元のオブジェクトは、夜間のメンテナンスジョブによって削除されるか、ユーザーが削除するまで、使用可能なオブジェクトのリストに残ります。

関連付けられていないオブジェクトはコピーとして CDO に残り、オブジェクトに関連付けられたルールまたはポリシーが誤って削除された場合にすべての設定が失われないようにします。

関連付けられていないオブジェクトを表示するには、[オブジェクト（Objects）] タブの左側のペインにある クリックし、[関連付けなし（Unassociated）] チェックボックスをオンにします。



オブジェクトの比較

手順

ステップ 1 [オブジェクト（Objects）] ページを開きます。

ステップ 2 ページのオブジェクトをフィルタ処理して、比較するオブジェクトを見つけます。

ステップ 3 [比較（Compare）] Compare ボタンをクリックします。

ステップ 4 比較するオブジェクトを最大 3 つまで選択します。

ステップ 5 画面の下部にオブジェクトを並べて表示します。

- [オブジェクトの詳細（Object Details）] タイトルバーの上下の矢印をクリックして、表示するオブジェクト詳細を調整します。
- [詳細（Details）] ボックスと [関係（Relationships）] ボックスを展開するか折りたたんで、表示する情報を調整します。

ステップ 6 （オプション）[関係（Relationships）] ボックスには、オブジェクトの使用方法が表示されます。オブジェクトはデバイスまたはポリシーに関連付けられている場合があります。オブジェクトがデバイスに関連付けられている場合は、デバイス名をクリックしてから [構成の表示（View Configuration）] をクリックして、デバイスの構成を表示できます。CDO はデバイスの構成ファイルを表示し、そのオブジェクトのエントリをハイライトします。

フィルタ

[インベントリ（Inventory）] ページおよび [オブジェクト（Objects）] ページの各種フィルタを使用して、目的のデバイスやオブジェクトを見つけることができます。

フィルタ処理するには、[デバイスとサービス（Devices and Services）] タブ、[ポリシー（Policies）] タブ、および [オブジェクト（Object）] タブの左側のペインで をクリックします。

インベントリフィルタでは、デバイスタイプ、ハードウェアとソフトウェアのバージョン、Snort バージョン、設定ステータス、接続状態、競合検出、Secure Device Connector、およびラベルを指定してフィルタ処理できます。フィルタを適用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。フィルタを使用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。

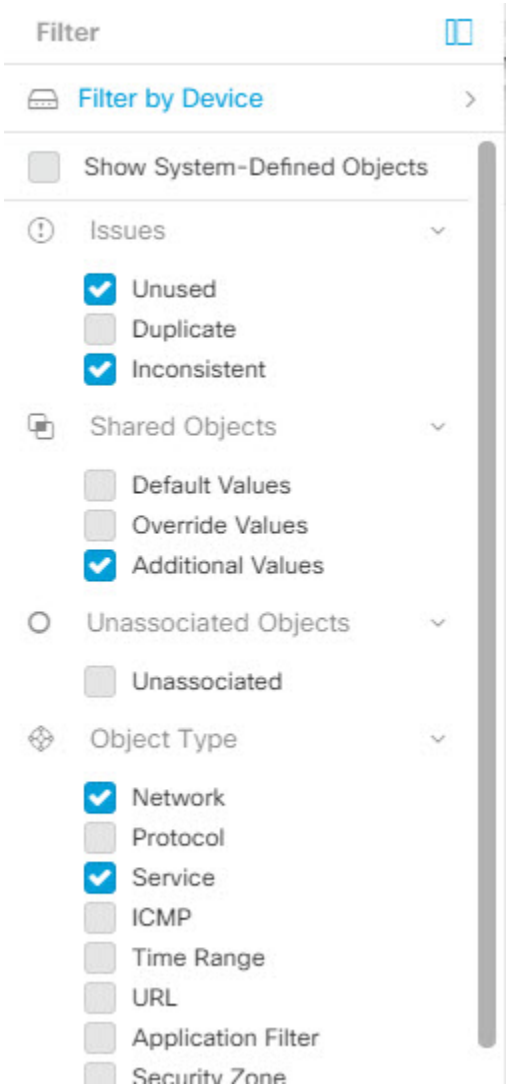
（注） [FTD] タブを開くと、フィルタペインでフィルタを使用できます。これにより、CDO からデバイスにアクセスするために使用されている管理アプリケーションに基づいて FTD デバイスが表示されます。

- FDM：FTD API または FDM を使用して管理される FTD。
- FMC-FTD：Firepower Management Center を使用して管理される FTD。
- FTD：FTD 管理を使用して管理される FTD。

オブジェクトフィルタを使用すると、デバイス、問題タイプ、共有オブジェクト、関連付けのないオブジェクト、およびオブジェクトタイプでフィルタ処理できます。結果にシステムオブジェクトを含めるかどうかを選択できます。検索フィールドを使用して、特定の名前、IP アドレス、またはポート番号を含むフィルタ結果内のオブジェクトを検索することもできます。

デバイスとオブジェクトをフィルタ処理する場合、検索用語を組み合わせて、関連する結果を見つけるためのいくつかの潜在的な検索戦略を作成できます。

次の例では、「問題（使用済みまたは不整合）があるオブジェクト、追加の値を持つ共有オブジェクト、特定タイプ（ネットワークまたはサービス）のオブジェクト」のすべての条件を満たすオブジェクトを検索するフィルタが適用されます。



オブジェクトフィルタ

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

- [すべてのオブジェクト（All Objects）] – このフィルタは、CDO にオンボーディングしたすべてのデバイスから使用可能なすべてのオブジェクトを提供します。このフィルタは、すべてのオブジェクトを参照するために、または検索の開始点としてや、さらにサブフィルタ適用するために役立ちます。
- [共有オブジェクト（Shared Objects）] – このクイックフィルタは、複数のデバイスで共有されていることが CDO によって検出されたすべてのオブジェクトを表示します。

- [デバイスごとのオブジェクト（Objects By Device）]–特定のデバイスを選択して、選択したデバイスで見つかったオブジェクトを表示できます。

サブフィルタ–各メインフィルタ内には、選択をさらに絞り込むために適用できるサブフィルタがあります。これらのサブフィルタは、オブジェクトタイプ（ネットワーク、サービス、プロトコルなど）に基づいています。

このフィルタバーで選択されたフィルタは、以下の条件に一致するオブジェクトを返します。

***** 2 つのデバイスのいずれかにあるオブジェクト（[デバイスでフィルタ処理（Filter by Device）] をクリックしてデバイスを指定します）。および

***** **一貫性のない**オブジェクト。および

***** **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。 および

***** オブジェクトの命名規則に「**グループ**」という単語が含まれているオブジェクト。

[システムオブジェクトの表示（Show System Objects）] がオンになっているため、結果にはシステムオブジェクトとユーザー定義オブジェクトの両方が含まれます。

システムオブジェクトの表示フィルタ

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。

[システムオブジェクトを表示（Show System Objects）] はデフォルトで「**オフ**」です。オブジェクトテーブルにシステムオブジェクトを表示するには、フィルターバーで [システムオブジェクトを表示（Show System Objects）] をオンにします。オブジェクトテーブルでシステムオブジェクトを非表示にするには、フィルターバーで [システムオブジェクトを表示（Show System Objects）] をオフのままにします。

システムオブジェクトを非表示にすると、それらは検索およびフィルタ処理の結果に含まれなくなります。システムオブジェクトを表示すると、それらはオブジェクトの検索とフィルタ処理の結果に含まれます。

オブジェクトフィルタを設定する

条件を必要な数だけ設定してフィルタリングできます。フィルタリングするカテゴリが多いほど、予想される結果は少なくなります。

手順

ステップ 1 ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 ページ上部のフィルタアイコン をクリックして、フィルタパネルを開きます。オブジェクトが誤って除外されないように、チェック付きのフィルタのチェックを外します。さらに、検索フィールドを見て、検索フィールドに入力された可能性のあるテキストを削除します。

ステップ 3 結果を特定のデバイスで見つかったものに限定したい場合：

1. **[デバイスでフィルタ処理（Filter By Device）]** をクリックします。
2. すべてのデバイスを検索するか、デバイスタブをクリックして特定の種類のデバイスのみを検索します。
3. フィルタ条件に含めるデバイスのチェックボックスをオンにします。
4. [OK] をクリックします。

ステップ 4 検索結果にシステムオブジェクトを含めるには、[システムオブジェクトを表示（Show System Objects）] をオンにします。検索結果でシステムオブジェクトを除外するには、[システムオブジェクトを表示（Show System Objects）] をオフにします。

ステップ 5 [問題（Issues）] で、フィルタリングするオブジェクトの問題のチェックボックスをオンにします。複数の問題をオンにすると、オンにしたいずれかのカテゴリのオブジェクトがフィルタ結果に含まれます。

ステップ 6 問題があったが管理者によって無視されたオブジェクトを表示する場合は、[無視（Ignored）] の問題をチェックします。

ステップ 7 2つ以上のデバイス間で共有されるオブジェクトをフィルタリングする場合は、[共有オブジェクト（Shared Objects）] で必要なフィルタをオンにします。

- [デフォルト値（Default Values）]：デフォルト値のみを持つオブジェクトをフィルタリングします。
- [オーバーライド値（Override Values）]：オーバーライドされた値を持つオブジェクトをフィルタリングします。
- [追加の値（Additional Values）]：追加の値を持つオブジェクトをフィルタリングします。

ステップ 8 ルールまたはポリシーの一部ではないオブジェクトをフィルタリングする場合は、[関連付けなし（Unassociated）] をオンにします。

ステップ 9 フィルタリングする [オブジェクトタイプ（Object Types）] をオンにします。

ステップ 10 オブジェクト名、IP アドレス、またはポート番号を [オブジェクト（Objects）] 検索フィールドに追加して、フィルタリングされた結果の中から検索条件に一致するオブジェクトを見つけることもできます。

フィルタ基準からデバイスを除外する場合

デバイスをフィルタリング基準に追加すると、結果にはデバイス上のオブジェクトは表示されますが、それらのオブジェクトと他のデバイスとの関係は表示されません。たとえば、**ObjectA** が ASA1 と ASA2 の間で共有されている場合、オブジェクトをフィルタリングして ASA1 上の共有オブジェクトを検索すると、**ObjectA** は見つかりますが、[関係（Relationships）] ペインには、オブジェクトが ASA1 にあることだけが表示されます。

オブジェクトが関連するすべてのデバイスを表示するには、検索条件でデバイスを指定しないでください。他の条件でフィルタリングし、必要に応じて検索条件を追加します。CDO が識

別するオブジェクトを選択し、[関係（Relationships）] ペインを調べます。そのオブジェクトに関連するすべてのデバイスとポリシーが表示されます。

オブジェクトの無視の解除

未使用、重複、不整合のオブジェクトを解決する方法の 1 つは、それらを無視することです。オブジェクトが未使用、重複、または不整合であっても、その状態には正当な理由があると判断し、オブジェクトの問題を未解決のままにすることを選択する場合もあります。将来のある時点で、これらの無視されたオブジェクトを解決することが必要になる場合があります。オブジェクトの問題を検索するときに CDO は無視されたオブジェクトを表示しないため、無視されたオブジェクトのオブジェクトリストをフィルタリングし、結果に基づいて操作する必要があります。

手順

ステップ 1 [オブジェクト（Objects）] ページを開きます。

ステップ 2 無視されたオブジェクトをフィルタリングして検索します。

ステップ 3 [オブジェクト（Object）] テーブルで、無視を解除するオブジェクトをすべて選択します。一度に 1 つのオブジェクトの無視を解除できます。

ステップ 4 詳細ペインで [無視の解除（Unignore）] をクリックします。

ステップ 5 要求を確認します。これで、オブジェクトを問題でフィルタリングすると、以前は無視されていたオブジェクトが見つかるはずです。

オブジェクトの削除

1 つのオブジェクトまたは複数のオブジェクトを削除できます。

1 つのオブジェクトの削除

1 つのオブジェクトを削除するには、次の手順を実行します。

手順

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、削除するオブジェクトを見つけ、それを選択します。

ステップ 3 [関係（Relationships）] ペインを確認します。オブジェクトがポリシーまたはオブジェクトグループで使用されている場合は、そのポリシーまたはグループから削除するまでオブジェクトを削除できません。

ステップ 4 [アクション（Actions）] ペインで、[削除（Remove）] アイコン をクリックします。

ステップ 5 [OK] をクリックしてオブジェクトの削除を確認します。

ステップ 6 行った変更をすべてのデバイスの設定変更のプレビューと展開か、複数の変更を後から一度に展開します。

未使用のオブジェクトのグループの削除

デバイスをオンボードしてオブジェクトの問題解決に取り組むと、多くの未使用のオブジェクトが見つかります。一度に最大 50 個の未使用オブジェクトを削除できます。

手順

ステップ 1 [問題（Issues）] フィルタを使用して、**未使用のオブジェクト**を見つけます。デバイスフィルタを使用する際に [デバイスなし（No Device）] を選択し、デバイスに関連付けられていないオブジェクトを検索することもできます。オブジェクトリストをフィルタ処理すると、オブジェクトのチェックボックスが表示されます。

ステップ 2 オブジェクトテーブルヘッダーの [すべて選択（Select all）] チェックボックスをオンにして、フィルタによって検出されオブジェクトテーブルに表示されるすべてのオブジェクトを選択するか、削除する個々のオブジェクトのチェックボックスを個別にオンにします。

ステップ 3 操作ウィンドウで、削除アイコン をクリックします。

ステップ 4 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ネットワーク オブジェクト

1 つのネットワークオブジェクトには、ホスト名、ネットワーク IP アドレス、IP アドレスの範囲、完全修飾ドメイン名（FQDN）または CIDR 表記のサブネットワークのいずれか 1 つを入れることができます。**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ワークの集合体です。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、ネットワークポリシー、および NAT ルールで使用されます。CDO 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、更新、および削除できます。

表 *2:* ネットワークオブジェクトで許可される値

デバイスタイプ	[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
FTD	IPv4 と IPv6	対応	対応	対応	対応

表 *3:* ネットワークグループで許可される内容

デバイスタイプ	IP 値	ネットワークオブジェクト	ネットワークグループ
FTD	×	対応	対応

ネットワークオブジェクトの表示

CDO を使用して作成するネットワークオブジェクトと、オンボーディングしたデバイスの設定から CDO が認識するネットワークオブジェクトは、[オブジェクト（Objects）] ページに表示されます。これらのネットワークオブジェクトには、それぞれのオブジェクトタイプのラベルが付けられています。これにより、オブジェクトタイプでフィルタリングして、探しているオブジェクトをすばやく見つけることができます。

[オブジェクト（Objects）]ページでネットワークオブジェクトを選択すると、オブジェクトの値が [詳細（Detail）] ペインに表示されます。[関係（Relationships）] ペインには、オブジェクトがポリシーで使用されているかどうか、およびオブジェクトが保存されているデバイスが表示されます。

ネットワークグループをクリックすると、そのグループの内容が表示されます。ネットワークグループは、ネットワークオブジェクトによってグループに与えられたすべての値の集合体です。

関連情報：

- 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作成または編集

ASA ネットワークオブジェクトおよびネットワークグループの作成または編集

ASA ネットワークオブジェクトには、CIDR 表記で表現されたホスト名、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、アクセスルール、ネットワークポリシー、および NAT ルールで使用されるネットワークオブジェクト、ネットワークグループ、および IP アドレスの集合体です。CDO 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	[IPv4 / IPv6]	シングル アドレス	アドレス範囲	部分修飾ドメイン名（PQDN）	CIDR 表記法によるサブネット
ASA	IPv4	対応	対応	対応	対応

ASA ネットワークオブジェクトの作成

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 **[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 （任意）オブジェクトの説明を入力します。

ステップ 7 [値（Value）] セクションで、次のいずれかの方法で IP アドレス情報を追加します。

- [eq] を選択し、単一の IP アドレス、CIDR 表記を使用したサブネットアドレス、または部分修飾ドメイン名（PQDN）を入力します。
- [範囲（range）] を選択し、IP アドレスの範囲を入力します。範囲の開始アドレスと終了アドレスをスペースで区切って入力します。例：10.1.1.1 10.1.1.255。

ステップ 8 [追加（Add）] をクリックします。

重要 新たに作成されたネットワークオブジェクトは、ルールやポリシーの一部ではないため、いずれの ASA デバイスにも関連付けられていません。それらのオブジェクトを表示するには、オブジェクトフィルタで [関連付けなし（Unassociated）] オブジェクトカテゴリを選択します。詳細については、「オブジェクトフィルタ」を参照してください。デバイスのルールやポリシーに関連付けられていないオブジェクトを使用すると、そのオブジェクトはそのデバイスに関連付けられます。

ASA ネットワーク グループの作成

[ネットワークグループ（Network Group）] には、IP アドレス値、ネットワークオブジェクト、およびネットワークグループを含めることができます。新しい [ネットワークグループ（Network Group）] を作成するときに、名前、IP アドレス、IP アドレス範囲、または FQDN で既存のオブジェクトを検索し、[ネットワークグループ（Network Group）] に追加できます。オブジェクトが存在しない場合は、同じインターフェイスでそのオブジェクトをすぐに作成し、[ネットワークグループ（Network Group）] に追加できます。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 **[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（Object Name）] 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 （任意）オブジェクトの説明を入力します。

ステップ 7 [値（Values）] フィールドに、値またはオブジェクト名を入力します。入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。

ステップ 8 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 9 CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。

ステップ 10 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。
- [値の追加（Add Value）] をクリックして、オブジェクトを使用せずにインライン値を作成します。値を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

（注） 編集アイコンをクリックして、詳細を変更できます。削除ボタンをクリックしても、オブジェクト自体は削除されず、代わりに、ネットワークグループから削除されます。

ステップ 11 必要なオブジェクトを追加したら、[保存（Save）] をクリックして新しいネットワークグループを作成します。

ステップ 12 すべてのデバイスの設定変更のプレビューと展開 （424 ページ）。

ASA ネットワークオブジェクトの編集

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 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 3 ネットワークオブジェクトを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 ダイアログボックスの値を、上記の手順で作成したときと同じ方法で編集します。

（注） ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 6 [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デバイスへの変更を確定します。

ASA ネットワークグループの編集

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトフィルタと [検索（Search）] フィールドを使用して、編集するネットワークグループを見つけます。

ステップ 3 ネットワークグループを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 ネットワークグループにすでに追加されているオブジェクトまたはネットワークグループを変更する場合は、次の手順を実行します。

1. オブジェクト名またはネットワークグループの横に表示される編集アイコン をクリックして、それらを変更します。
2. チェックマークをクリックして変更内容を保存します。

（注） 削除アイコンをクリックして、ネットワークグループから値を削除できます。

ステップ 5 ネットワークグループに新しい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を追加する場合は、次の手順を実行する必要があります。

1. [値（Values）] フィールドに、新しい値または既存のネットワークオブジェクトの名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。
2. CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。
3. 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。
- [値の追加（Add Value）] をクリックして、オブジェクトを使用せずにインライン値を作成します。値を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 6 [保存（Save）] をクリックします。CDO は、変更の影響を受けるポリシーを表示します。

ステップ 7 [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デバイスへの変更を確定します。

ステップ 8 すべてのデバイスの設定変更のプレビューと展開 （424 ページ）。

共有ネットワークグループへの追加の値の追加

関連付けられたすべてのデバイスに存在する共有ネットワークグループ内の値は、「デフォルト値」と呼ばれます。CDO を使用すると、共有ネットワークグループに「追加の値」を追加し、それらの値をその共有ネットワークグループに関連付けられたいくつかのデバイスに割り当てることができます。CDO がデバイスに変更を展開するときに、内容が決定され、「デフォルト値」が共有ネットワークグループに関連付けられているすべてのデバイスにプッシュされ、「追加の値」が指定されたデバイスにのみプッシュされます。

たとえば、本社に 4 つの AD メインサーバーがあり、すべての拠点からアクセスできる必要があるシナリオを考えてみます。この状況で、すべての拠点で使用する「Active-Directory」という名前のオブジェクトグループを作成しました。ここで、ブランチオフィスの 1 つにさらに 2 つの AD サーバーを追加します。これを行うには、オブジェクトグループ「Active-Directory」で、ブランチオフィスに固有の追加値として詳細を追加します。これら 2 つのサーバーは、オブジェクト「Active-Directory」が一貫しているか、または共有されているかの判断には関与しません。したがって、4 つの AD メインサーバーはすべての拠点からアクセスできますが、ブランチオフィス（2 つの追加サーバーがある）は 2 つの AD サーバーと 4 つの AD メインサーバーにアクセスできます。

（注） 一貫性のない共有ネットワークグループがある場合は、追加の値を使用してそれらを 1 つの共有ネットワークグループに結合できます。詳細については、「不整合オブジェクトの問題を解決する」を参照してください。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集する共有ネットワークグループを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

- [デバイス（Devices）] フィールドには、共有ネットワークグループが存在するデバイスが表示されます。
- [使用（Usage）] フィールドには、共有ネットワークグループに関連付けられたルールセットが表示されます。
- [デフォルト値] フィールドは、デフォルトのネットワークオブジェクトと、オブジェクトの作成時に指定された、共有ネットワークグループに関連付けられたオブジェクト値が示されます。このフィールドの横に、このデフォルト値を含むデバイスの数が表示され、クリックすると名前とデバイスタイプを表示できます。この値に関連付けられたルールセットも表示されます。

ステップ 4 [追加の値（Additional Values）] フィールドに、値または名前を入力します。 入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。

ステップ 5 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 6 CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。

ステップ 7 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。
- [値の追加（Add Value）] をクリックして、オブジェクトを使用せずにインライン値を作成します。値を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 8 [デバイス（Devices）] 列で、新しく追加されたオブジェクトに関連付けられているセルをクリックし、[デバイスの追加（Add Devices）] をクリックします。

ステップ 9 必要なデバイスを選択し、[OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 11 [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デバイスへの変更を確定します。

ステップ 12 すべてのデバイスの設定変更のプレビューと展開 （424 ページ）。

共有ネットワークグループの追加の値の編集

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集対象のオーバーライドがあるオブジェクトを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

ステップ 4 オーバーライド値を変更します。

- 値を変更するには、編集アイコンをクリックします。
- [デバイス（Devices）] 列のセルをクリックして、新しいデバイスを割り当てます。すでに割り当てられているデバイスを選択し、[オーバーライドの削除（Remove Overrides）] をクリックすると、そのデバイスのオーバーライドを削除できます。
- [デフォルト値（Default Values）] の 矢印をクリックすると、共有ネットワークグループの追加値にできます。共有ネットワークグループに関連付けられているすべてのデバイスが、自動的に割り当てられます。
- [オーバーライド値（Override Values）] の 矢印をクリックすると、共有ネットワークグループのデフォルト値にできます。
- ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 6 [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デバイスへの変更を確定します。

ステップ 7 すべてのデバイスの設定変更のプレビューと展開 （424 ページ）。

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作成または編集

Firepower ネットワークオブジェクトには、CIDR 表記で表現されたホスト名、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、アクセスルール、ネットワークポリシー、およびNATルールで使用されるネットワークオブジェクトとネッ

トワークグループの集合体です。CDO 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。

表 *4:* 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	[IPv4 / IPv6]	シングル アドレス	アドレス範囲	部分修飾ドメイン名（PQDN）	CIDR 表記によるサブネット
Firepower	[IPv4 / IPv6]	対応	対応	対応	対応

関連情報

- Firepower ネットワークオブジェクトの作成
- Firepower ネットワークオブジェクトの編集
- 共有ネットワークグループへの追加の値の追加
- 共有ネットワークグループの追加の値の編集

Firepower ネットワークオブジェクトの作成

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 **[FTD] > [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（Object Name）] 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、次の手順を実行します。

- [eq] を選択し、単一の IP アドレス、CIDR 表記で表されるサブネットアドレス、または部分修飾ドメイン名（PQDN）を入力します。
- [範囲（range）] を選択し、IP アドレスの範囲を入力します。

ステップ 7 [追加（Add）] をクリックします。

注意 : 新たに作成されたネットワークオブジェクトは、ルールやポリシーの一部ではないため、いずれの FTD デバイスにも関連付けられていません。それらのオブジェクトを表示するには、オブジェクトフィルタで [関連付けなし（Unassociated）] オブジェクトカテゴリを選択します。詳細については、「オブジェクトフィルタ」を参照してください。デバイスのルールやポリシーに関連付けられていないオブジェクトを使用すると、そのオブジェクトはそのデバイスに関連付けられます。

Firepower ネットワークグループの作成

[ネットワークグループ（Network Group）] には、ネットワークオブジェクトとネットワークグループを含めることができます。新しい [ネットワークグループ（Network Group）] を作成すると、名前、IP アドレス、IP アドレス範囲、または FQDN で既存のオブジェクトを検索し、[ネットワークグループ（Network Group）] に追加できます。オブジェクトが存在しない場合は、同じインターフェイスでそのオブジェクトをすぐに作成し、[ネットワークグループ（Network Group）] に追加できます。

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 **[FTD] > [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（Object Name）] 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 [値（Values）] フィールドに、値または名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。

ステップ 7 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 8 CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。

ステップ 9 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

注：編集アイコンをクリックして、詳細を変更できます。削除ボタンをクリックしても、オブジェクト自体は削除されず、代わりに、ネットワークグループから削除されます。

ステップ 10 必要なオブジェクトを追加したら、[保存（Save）] をクリックして新しいネットワークグループを作成します。

ステップ 11 すべてのデバイスの設定変更のプレビューと展開。

Firepower ネットワークオブジェクトの編集

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトフィルタと [検索（search）] 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 3 ネットワークオブジェクトを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 「Firepower ネットワークグループの作成」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。注：ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 6 [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デバイスへの変更を確定します。

Firepower ネットワークグループの編集

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトフィルタと [検索（Search）] フィールドを使用して、編集するネットワークグループを見つけます。

ステップ 3 ネットワークグループを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 オブジェクトの名前と説明を必要に応じて変更します。

ステップ 5 ネットワークグループにすでに追加されているオブジェクトまたはネットワークグループを変更する場合は、次の手順を実行します。

1. オブジェクト名またはネットワークグループの横に表示される編集アイコン をクリックして、それらを変更します。
2. チェックマークをクリックして変更内容を保存します。**注**：削除アイコンをクリックして、ネットワークグループから値を削除できます。

ステップ 6 ネットワークグループに新しい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を追加する場合は、次の手順を実行する必要があります。

1. [値（Values）] フィールドに、新しい値または既存のネットワークオブジェクトの名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が CDO によっ

て表示されます。表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

2. CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。

3. 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

   - [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
   - [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 7 [保存（Save）] をクリックします。CDO は、変更の影響を受けるポリシーを表示します。

ステップ 8 [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デバイスへの変更を確定します。

ステップ 9 すべてのデバイスの設定変更のプレビューと展開。

共有ネットワークグループへの追加の値の追加

関連付けられたすべてのデバイスに存在する共有ネットワークグループ内の値は、「デフォルト値」と呼ばれます。CDO を使用すると、共有ネットワークグループに「追加の値」を追加し、それらの値をその共有ネットワークグループに関連付けられたいくつかのデバイスに割り当てることができます。CDO がデバイスに変更を展開するときに、内容が決定され、「デフォルト値」が共有ネットワークグループに関連付けられているすべてのデバイスにプッシュされ、「追加の値」が指定されたデバイスにのみプッシュされます。

たとえば、本社に 4 つの AD メインサーバーがあり、すべての拠点からアクセスできる必要があるシナリオを考えてみます。この状況で、すべての拠点で使用する「Active-Directory」という名前のオブジェクトグループを作成しました。ここで、ブランチオフィスの 1 つにさらに 2 つの AD サーバーを追加します。これを行うには、オブジェクトグループ「Active-Directory」で、ブランチオフィスに固有の追加値として詳細を追加します。これら 2 つのサーバーは、オブジェクト「Active-Directory」が一貫しているか、または共有されているかの判断には関与しません。したがって、4 つの AD メインサーバーはすべての拠点からアクセスできますが、ブランチオフィス（2 つの追加サーバーがある）は 2 つの AD サーバーと 4 つの AD メインサーバーにアクセスできます。

（注） 一貫性のない共有ネットワークグループがある場合は、追加の値を使用してそれらを1つの共有ネットワークグループに結合できます。詳細については、不整合オブジェクトの問題を解決するを参照してください。

手順

ステップ1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ2 オブジェクトフィルタと検索フィールドを使用して、編集する共有ネットワークグループを見つけます。

ステップ3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

- [デバイス（Devices）] フィールドには、共有ネットワークグループが存在するデバイスが表示されます。
- [使用（Usage）] フィールドには、共有ネットワークグループに関連付けられたルールセットが表示されます。
- [デフォルト値] フィールドは、デフォルトのネットワークオブジェクトと、オブジェクトの作成時に指定された、共有ネットワークグループに関連付けられたオブジェクト値が示されます。このフィールドの横に、このデフォルト値を含むデバイスの数が表示され、クリックすると名前とデバイスタイプを表示できます。この値に関連付けられたルールセットも表示されます。

ステップ4 [追加の値（Additional Values）] フィールドに、値または名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。

ステップ5 表示されている既存のオブジェクトの1つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ6 CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。

ステップ7 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 8 [デバイス（Devices）] 列で、新しく追加されたオブジェクトに関連付けられているセルをクリックし、[デバイスの追加（Add Devices）] をクリックします。

ステップ 9 必要なデバイスを選択し、[OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 11 [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デバイスへの変更を確定します。

ステップ 12 すべてのデバイスの設定変更のプレビューと展開。

共有ネットワークグループの追加の値の編集

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集対象のオーバーライドがあるオブジェクトを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

ステップ 4 オーバーライド値を変更します。

- 値を変更するには、編集アイコンをクリックします。
- [デバイス（Devices）] 列のセルをクリックして、新しいデバイスを割り当てます。すでに割り当てられているデバイスを選択し、[オーバーライドの削除（Remove Overrides）] をクリックすると、そのデバイスのオーバーライドを削除できます。
- [デフォルト値（Default Values）] の 矢印をクリックすると、共有ネットワークグループの追加値にできます。共有ネットワークグループに関連付けられているすべてのデバイスが、自動的に割り当てられます。
- [オーバーライド値（Override Values）] の 矢印をクリックすると、共有ネットワークグループのデフォルト値にできます。
- ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 6 [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デバイスへの変更を確定します。

ステップ 7 すべてのデバイスの設定変更のプレビューと展開。

アプリケーション フィルタ オブジェクト

アプリケーション フィルタ オブジェクトは、Firepower デバイスによって使用されます。アプリケーション フィルタ オブジェクトは、IP 接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタを定義します。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、トラフィックを制御できます。

個々のアプリケーションを指定することはできますが、アプリケーションフィルタはポリシーの作成や管理を簡素化します。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックする、アクセス コントロール ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションがブロックされます。

アプリケーション フィルタ オブジェクトを使用せず、ポリシーのアプリケーションとアプリケーション フィルタを直接選択できます。ただし、同じアプリケーションまたはフィルタ グループに対して複数のポリシーを作成する場合にはオブジェクトが便利です。システムには、事前に定義されたいくつかのアプリケーション フィルタが含まれていて、これらは編集または削除できません。

（注） シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーションディテクタを更新し追加しています。そのため、手動でルールを更新することなく、高リスクのアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

（注） FDM 管理の FTD デバイスが CDO にオンボードされると、アクセスルールまたは SSL 復号化で定義されたルールを変更することなく、アプリケーションフィルタがアプリケーション フィルタ オブジェクトに変換されます。設定が変更されたため、デバイスの設定ステータスが [非同期（Not Synced）] に変更されるので、CDO から設定を展開する必要があります。一般に、FDMは、フィルタを手動で保存するまで、アプリケーションフィルタをアプリケーション フィルタ オブジェクトに変換しません。

関連情報：

- Firepower アプリケーション フィルタ オブジェクトの作成と編集
- オブジェクトの削除

Firepower アプリケーション フィルタ オブジェクトの作成と編集

アプリケーション フィルタ オブジェクトを使用すると、厳選されたアプリケーションまたはフィルタによって識別されるアプリケーションのグループを対象にできます。このアプリケーション フィルタ オブジェクトは、ポリシーで使用できます。

Firepower アプリケーション フィルタ オブジェクトの作成

アプリケーション フィルタ オブジェクトを作成するには、次の手順を実行します。

手順

ステップ 1 [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

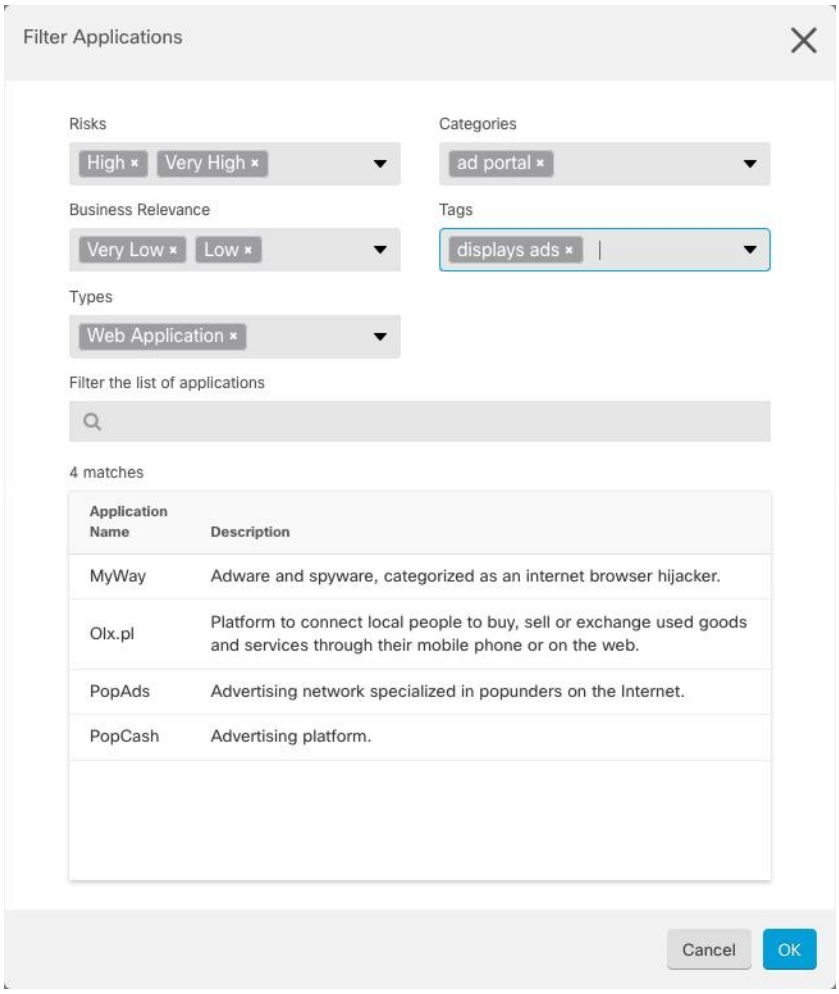
ステップ 2 [オブジェクトの作成（Create Object）] > [FTD] > [アプリケーションサービス（Application Service）] をクリックします。

ステップ 3 そのオブジェクトの**オブジェクト名**を入力し、任意で**説明**を入力します。

ステップ 4 [フィルタの追加（Add Filter）] をクリックし、オブジェクトに追加するアプリケーションとフィルタを選択します。

最初のリストには、継続的にスクロールするリストでアプリケーションが表示されます。[フィルタの詳細設定（Advanced Filter）] をクリックすると、フィルタ オプションが表示され、アプリケーションを容易に選択できます。選択したら、[追加（Add）] をクリックします。このプロセスを繰り返して、アプリケーションやフィルタを追加できます。

（注） 1 つのフィルタ条件内での複数の選択は OR 関係にあります。たとえば、リスクが「高（High）」または（OR）「非常に高い（Very High）」となります。フィルタ間の関係は「論理積（AND）」であるため、リスクが「高（High）」または（OR）「非常に高い（Very High）」であり、かつ（AND）ビジネスとの関連性が「低（Low）」または（OR）「非常に低い（Very Low）」となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりできます。



[リスク（Risks）]：アプリケーションが組織のセキュリティポリシーに反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

[ビジネスとの関連性（Business Relevance）]：アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

[タイプ（Types）]：アプリケーションのタイプ。

- [アプリケーションプロトコル（Application Protocol）]：HTTP や SSH などのホスト間の通信を表すアプリケーションプロトコル。
- [クライアントプロトコル（Client Protocol）]：Web ブラウザや電子メールクライアントなどのホスト上で動作しているソフトウェアを表すクライアント。
- [Webアプリケーション（Web Application）]：HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

[カテゴリ（Categories）]：アプリケーションの最も重要な機能を説明する一般分類。

[タグ（Tags）]：カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは[SSL Protocol]とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。また、システムは、復号されたトラフィック（暗号化された、または暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに[復号されたトラフィック（decrypted traffic）]タグを割り当てます。

[アプリケーションリスト（Applications List）]（画面下部）：上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを使用します。特定のアプリケーションまたは複数のアプリケーションをオブジェクトに追加するには、フィルタ処理されたリストからそれらを選択します。アプリケーションを選択すると、フィルタは適用されなくなります。フィルタ自体をオブジェクトにする場合は、リストからアプリケーションを選択しないでください。その後、そのオブジェクトは、常に、フィルタによって識別されたアプリケーションを表します。

ステップ 5 [OK] をクリックして変更を保存します。

Firepower アプリケーション フィルタ オブジェクトの編集

手順

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

ステップ 2 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 3 編集するオブジェクトを選択します。

ステップ 4 詳細パネルの [アクション（Actions）] ペインにある編集アイコン 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 CDO 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。

関連情報：

- オブジェクト
- オブジェクトフィルタ
- Firepower オブジェクトの削除

地理位置情報オブジェクト

地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IPアドレスを使用する代わりに、これらのオブジェクトをポリシーで使用してトラフィックを制御できます。たとえば、地理的な場所を使用して、使用されている可能性のある IP アドレスすべてを把握する必要なしに、特定の国へのアクセスを簡単に制限できます。

通常は、地理位置情報オブジェクトを使用せずに、地理的な場所をポリシーで直接選択できます。とはいえ、同じ国や大陸のグループのために複数のポリシーを作成する場合、オブジェクトが便利です。

地理位置情報データベースの更新

常に最新の地理位置情報データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。現時点で、これは Cisco Defense Orchestrator を使用して実行できるタスクではありません。GeoDB とその更新方法の詳細については、デバイスが実行しているバージョンの『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の次のセクションを参照してください。

- システム データベースとフィードの更新
- システム データベースの更新

Firepower 地理位置情報フィルタオブジェクトの作成と編集

地理位置情報オブジェクトは、オブジェクトページで単独で作成するか、セキュリティポリシーの作成時に作成することができます。この手順では、オブジェクトページから地理位置情報オブジェクトを作成します。

地理位置情報オブジェクトを作成するには、次の手順を実行します。

手順

ステップ 1 [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[FTD]** > **[地理位置情報（Geolocation）]** をクリックします。

ステップ 3 そのオブジェクトの**オブジェクト名**を入力し、任意で**説明**を入力します。

ステップ 4 フィルタバーで、国または地域の名前の入力を開始すると、一致する可能性のあるもののリストが表示されます。

ステップ 5 オブジェクトに追加する 1 つまたは複数の国や地域のチェックボックスをオンにします。

ステップ 6 [追加（Add）] をクリックします。

オブジェクトを追加する方法：地理位置情報

手順

ステップ 1 [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。
ステップ 2 フィルタパネルと検索フィールドを使用して、オブジェクトを見つけます。
ステップ 3 [アクション（Actions）] ペインで、[編集（Edit）] をクリックします。
ステップ 4 オブジェクト名を変更したり、オブジェクトに国や地域を追加または削除したりできます。
ステップ 5 [保存（Save）] をクリックします。
ステップ 6 影響を受けるデバイスがある場合は通知されます。[確認（Confirm）] をクリックします。
ステップ 7 デバイスまたはポリシーが影響を受けた場合は、[デバイスとサービス（Devices & Services）] ページを開き、変更をプレビューしてデバイスに展開します。

DNS グループオブジェクト

ドメインネームシステム（DNS）グループは、DNS サーバーおよび関連付けられているいくつかの属性のリストを定義します。www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決するのには、DNS サーバーが必要です。管理インターフェイスとデータインターフェイスに異なる DNS グループオブジェクトを構成できます。

新しい DNS グループオブジェクトを作成する前に、FTD デバイスに DNS サーバーが構成されている必要があります。CDO の DNS サーバの設定に DNS サーバーを追加するか、FDM で DNS サーバーを作成してから、FDM 構成を CDO に同期することができます。FDM で DNS サーバー設定を作成または変更するには、『Cisco Firepower Device Manager 構成ガイド』バージョン 6.4 以降の「**データおよび管理インターフェイスの DNS の構成**」を参照してください。またはそれ以降。

DNS グループオブジェクトの作成

CDO で新しい DNS グループオブジェクトを作成するには、次の手順を使用します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。
ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。
ステップ 3 C**[FTD] > [DNS グループ（DNS Group）]**をクリックします。
ステップ 4 [オブジェクト名（Object Name）] を入力します。
ステップ 5 （任意）説明を追加します。

ステップ 6 [DNSサーバー（DNS server）] の IPアドレスを入力します最大 6 台の DNS サーバーを追加できます。[DNS サーバーの追加（Add DNS Server）] をクリックします。サーバーアドレスを削除する場合は、削除アイコンをクリックします。

（注） リストは優先順です。リストの最初のサーバが常に使用されます。後続のサーバは、上位のサーバから応答が受信されない場合にのみ使用されます。最大 6 台のサーバーを追加できますが、リストされている最初の 3 台のサーバーのみが管理インターフェイスに使用されます。

ステップ 7 [ドメイン検索名（Domain Search Name）] を入力します。このドメインは、完全修飾されていないホスト名（たとえば、serverA.example.com ではなく serverA）に追加されます。

ステップ 8 [再試行（Retries）] の回数を入力します。システムが応答を受信しない場合に DNS サーバーのリストを再試行する回数です（0 ～ 10）。デフォルトは 2 です。この設定は、データインターフェイスのみで使用される DNS グループに適用されます。

ステップ 9 [タイムアウト（Timeout）] の値を入力します。次の DNS サーバーを試行する前に待機する秒数です（1 ～ 30）。デフォルト値は 2 秒です。システムがサーバーのリストを再試行するたびに、このタイムアウトは 2 倍になります。この設定は、データインターフェイスのみで使用される DNS グループに適用されます。

ステップ 10 [追加（Add）] をクリックします。

DNS グループオブジェクトの編集

CDO または FDM で作成された DNS グループオブジェクトを編集できます。次の手順を使用して、既存の DNS グループオブジェクトを編集します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトフィルタと [検索（search）] フィールドを使用して、編集する **DNS グループオブジェクト**を見つけます。

ステップ 3 オブジェクトを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 次のエントリのいずれかを編集します。

- オブジェクト名。
- [説明（Description）]
- DNS サーバー。このリストから DNS サーバーを編集、追加、または削除できます。
- ドメイン検索名。
- リトライ。
- タイムアウト。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 すべてのデバイスの設定変更のプレビューと展開。

DNS グループオブジェクトの削除

CDO から DNS グループオブジェクトを削除するには、次の手順を使用します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトフィルタと [検索（search）] フィールドを使用して、編集する **DNS グループオブジェクト**を見つけます。

ステップ 3 オブジェクトを選択し、[削除（remove）] アイコン をクリックします。

ステップ 4 DNS グループオブジェクトを削除することを確認し、[Ok] をクリックします。

ステップ 5 すべてのデバイスの設定変更のプレビューと展開。

DNS サーバー グループ オブジェクトを FTD DNS サーバーとして追加

DNS グループオブジェクトは、[データインターフェイス（Data Interface）] または [管理インターフェイス（Management Interface）] の優先 DNS グループとして追加できます。詳細については、「FTD の設定」を参照してください。

証明書オブジェクト

デジタル証明書は、認証に使用されるデジタル ID を提供します。証明書は、SSL（セキュアソケット レイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。

デバイスが実行しているバージョンについては、『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用』の「再利用可能なオブジェクト」の章にある「**証明書について**」および「**証明書の設定**」以降のセクションを参照してください。

証明書について

デジタル証明書は、認証に使用されるデジタルIDを提供します。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザーまたはデバイスを識別する情報が含まれます。デジタル証明書には、ユーザまたはデバイスの公開キーのコピーも含まれています。証明書は、SSL（セキュア ソケット レイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。

次のタイプの証明書を作成できます。

- **内部証明書**：内部 ID 証明書は、特定のシステムまたはホストの証明書です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名証明書を生成することもできます。

  システムには、そのまま、または置き換えて使用できる事前定義された内部証明書（**DefaultInternalCertificate** および **DefaultWebServerCertificate**）が付属します。

- **内部認証局（CA）証明書**：内部 CA 証明書は、他の証明書の署名にシステムが使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名内部 CA 証明書を生成することもできます。自己署名内部 CA 証明書を設定する場合は、CA はデバイス自体で稼働します。

  システムには、そのまま、または置き換えて使用できる事前定義された内部 CA 証明書（**NGFW-Default-InternalCA**）が付属します。

- **信頼できる認証局（CA）証明書**：信頼できる CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。

  認証局（CA）は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザーのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。CA は、信頼できるサードパーティ（VeriSign など）の場合もあれば、組織内に設置したプライベート CA（インハウス CA）の場合もあります。CA は、証明書要求の管理とデジタル証明書の発行を行います。

  システムには、第三者証明機関からの多数の信頼できる CA の証明書も含まれています。これらは再署名の復号アクションのために SSL 復号化ポリシーが使用します。

詳細については、デバイスが実行しているバージョンの Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）[英語] の「Reusable Objects」の章にある「Certificate Types Used by Feature」を参照してください。https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html

各機能で使用される証明書タイプ

各機能に適したタイプの証明書を作成する必要があります。次の機能は、証明書が必要です。

アイデンティティ ポリシー（キャプティブ ポータル）：内部証明書

（オプション）キャプティブ ポータルはアイデンティティ ポリシーで使用されます。この証明書は、ユーザーが自身を証明し、自分のユーザー名に関連付けられた IP アドレスを取得することを目的として、デバイスへの認証の際に承認する必要があります。証明書を提示しないと、デバイスは自動生成された証明書を使用します。

SSL 復号ポリシー：内部、内部 CA、および信頼できる CA 証明書。

（必須）SSL 復号ポリシーは、以下の目的のため証明書を使用します。

- 内部証明書は既知のキー復号ルールに使用されます。

- 内部 CA 証明書は、クライアントと FTD デバイス間のセッションを作成するときに、再署名の復号ルールに使用されます。
- 信頼できる CA 証明書
  - この証明書は、FTDデバイスとサーバー間のセッションを作成するときに、再署名の復号ルールに間接的に使用されます。その他の証明書とは異なり、これらの証明書はSSL復号ポリシーで直接設定しません。これらは単にシステムにアップロードする必要があります。システムには多数の信用できるCA証明書が含まれるため、追加の証明書をアップロードする必要はないことがあります。
  - Active Directory レルムオブジェクトを作成し、暗号化を使用するようにディレクトリサーバーを設定する場合。

証明書の設定

アイデンティティポリシーまたはSSL復号化ポリシーで使用される証明書は、PEMまたはDER形式のX509証明書である必要があります。OpenSSLを使用して必要に応じて証明書を生成したり、信頼できる認証局から取得したり、または自己署名証明書を作成したりできます。

以下の手順を使用して、証明書オブジェクトを構成します。

- 内部および内部 CA 証明書のアップロード
- 信頼できる CA 証明書のアップロード
- 自己署名内部および内部 CA 証明書の生成
- 証明書を表示または編集するには、証明書の編集アイコンまたは表示アイコンをクリックします。
- 証明書を削除するには、その証明書のごみ箱アイコン（削除アイコン）をクリックします。「オブジェクトの削除」を参照してください。

内部および内部 CA 証明書のアップロード

内部 ID 証明書は、特定のシステムまたはホストの証明書です。これらはOpenSSLツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名証明書を生成することもできます。

内部認証局（CA）証明書（内部 CA 証明書）は、他の証明書の署名にシステムが使用できる証明書です。これらの証明書は、基本制約拡張とCAフラグに関して内部アイデンティティ証明書と異なります。これらはCA証明書では有効ですが、アイデンティティ証明書では無効です。これらはOpenSSLツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名内部CA証明書を生成することもできます。自己署名内部CA証明書を設定する場合は、CAはデバイス自体で稼働します。

これらの証明書を使用する機能の詳細については、「Certificate Type Used by Feature」を参照してください。

手順

この手順では、証明書ファイルをアップロードするか、既存の証明書のテキストをテキストボックスに貼り付けて、内部証明書または内部CA証明書を作成します。自己署名証明書を生成する場合は、「自己署名内部および内部 CA 証明書の生成」を参照してください。

内部証明書または内部CA証明書オブジェクトを作成する場合、または新しい証明書オブジェクトをポリシーに追加する場合は、次の手順に従います。

手順

ステップ 1 次のいずれかを実行します。

- [オブジェクト（Objects）] ページで証明書オブジェクトを作成します。
  1. ナビゲーションバーで、[オブジェクト（Objects）] を選択します。
  2. プラスボタン をクリックして、**[FTD]** > **[証明書（Certificate）]** を選択します。
- ポリシーに新しい証明書オブジェクトを追加するときに、[新しいオブジェクトの作成（Create New Object）] をクリックします。

ステップ 2 [Name] に証明書の名前を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 ステップ 1 で、[内部証明書（Internal Certificate）] または [内部CA（Internal CA）] を選択します。

ステップ 4 ステップ 2 で、[アップロード（Upload）] を選択して証明書ファイルをアップロードします。

ステップ 5 ステップ 3 で、[サーバー証明書（Server Certificate）] 領域で、証明書の内容をテキストボックスに貼り付けるか、ウィザードの説明に従って証明書ファイルをアップロードします。証明書をテキストボックスに貼り付ける場合、証明書に BEGIN CERTIFICATE と END CERTIFICATE の行を含める必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
 MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

ステップ 6 ステップ 3 で、[証明書キー（Certificate Key）] 領域で、キーの内容を [証明書キー（Certificate Key）] テキストボックスに貼り付けるか、ウィザードの説明に従ってキーファイルをアップロードします。キーをテキストボックスに貼り付ける場合、キーには BEGIN PRIVATE KEY または BEGIN RSA PRIVATE KEY、および END PRIVATE KEY または END PRIVATE KEY 行が含まれている必要があります。

（注） キーは暗号化できません。

ステップ 7 [追加（Add）] をクリックします。

信頼できる CA 証明書のアップロード

信頼できる認証局（CA）の証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。

これらの証明書を使用する機能の詳細については、「Certificate Type Used by Feature」を参照してください。

外部の認証局から信頼できる CA 証明書を取得するか、自身の内部 CA を使用して（OpenSSL ツールを使用するなど）CA 証明書を作成します。その後、次の手順を使用して証明書をアップロードします。

手順

手順

ステップ 1 次のどちらかを実行します。

- [オブジェクト（Objects）] ページで証明書オブジェクトを作成します。
  1. ナビゲーションバーで、[オブジェクト（Objects）] を選択します。
  2. プラスボタン をクリックして、**[FTD]** > **[証明書（Certificate）]** を選択します。
- ポリシーに新しい証明書オブジェクトを追加するときに、[新しいオブジェクトの作成（Create New Object）] をクリックします。

ステップ 2 [Name] に証明書の名前を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 手順 1 では、[外部CA証明書（External CA Certificate）] を選択し、[続行（Continue）] をクリックします。ウィザードの手順が 3 に進みます。

ステップ 4 手順 3 では、[証明書の内容（Certificate Contents）] 領域にあるテキストボックスに証明書の内容を貼り付けるか、ウィザードの説明に従って証明書ファイルをアップロードします。

証明書は、次のガイドラインに合致している必要があります。

- 証明書内のサーバ名は、サーバのホスト名または IP アドレスと一致している必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。
- 証明書は PEM または DER 形式の X509 証明書である必要があります。
- 貼り付ける証明書は、BEGIN CERTIFICATE と END CERTIFICATE の行を含める必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

ステップ 5 [追加（Add）] をクリックします。

自己署名内部および内部 CA 証明書の生成

内部 ID 証明書は、特定のシステムまたはホストの証明書です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名証明書を生成することもできます。

内部認証局（CA）証明書（内部 CA 証明書）は、他の証明書の署名にシステムが使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名内部 CA 証明書を生成することもできます。自己署名内部 CA 証明書を設定する場合は、CA はデバイス自体で稼働します。

また、これらの証明書は、OpenSSL を使用して作成することも、信頼できる CA から取得してアップロードすることもできます。詳細は「内部および内部 CA 証明書のアップロード」を参照してください。

これらの証明書を使用する機能の詳細については、Certificate Type Used by Featureを参照してください。

（注） 新しい自己署名証明書は 5 年の有効期間で生成されます。期限が切れる前に必ず証明書を交換してください。

警告 自己署名証明書を持つデバイスをアップグレードすると、問題が発生する可能性があります。詳細については、「新しい証明書の検出」を参照してください。

手順

この手順では、ウィザードに適切な証明書フィールド値を入力することにより、自己署名証明書を生成します。証明書ファイルをアップロードして内部または内部 CA 証明書を作成する場合は、「内部および内部 CA 証明書のアップロード」を参照してください。

自己署名証明書を生成するには、次の手順を実行します。

手順

ステップ 1 次のいずれかを実行します。

- [オブジェクト（Objects）] ページで証明書オブジェクトを作成します。
  1. ナビゲーションバーで、[オブジェクト（Objects）] を選択します。
  2. プラスボタン をクリックして、**[FTD]** > **[証明書（Certificate）]** を選択します。
- ポリシーに新しい証明書オブジェクトを追加するときに、[新しいオブジェクトの作成（Create New Object）] をクリックします。

ステップ 2 [Name] に証明書の名前を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 ステップ 1 で、[内部証明書（Internal Certificate）] または [内部CA（Internal CA）] を選択します。

ステップ 4 ステップ 2 で、[自己署名（Self-Signed）] を選択して、この手順で自己署名証明書を作成します。

ステップ 5 証明書の件名および発行者の情報については、次の少なくとも 1 つを設定します。

- [国（C）（Country (C)）]：ドロップダウトリストから国コードを選択します。
- [都道府県（ST）（State or Province (ST)）]：証明書に含める都道府県。
- [地域または都市（L）（Locality or City (L)）]：都市の名前など、証明書に含める地域。
- [組織（O）（Organization (O)）]：証明書に含める組織または会社の名前。
- [組織単位（部門）（OU）（Organizational Unit (Department)）]：証明書に含める組織単位の名前（部門名など）。
- [共通名（CN）（Common Name (CN)）]：証明書に含める X.500 共通名。これは、デバイスの名前、Web サイト、または他の文字列にできます。この要素は、通常は正常な接続のために必要です。たとえば、リモート アクセス VPN で使用する内部証明書に CN を含める必要があります。

ステップ 6 [追加（Add）] をクリックします。

IPsec プロポーザルの設定

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供

されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2つのピア間のセキュアで論理的な通信パスです。IPsec トンネルを通過するトラフィックは、トランスフォーム セットと呼ばれるセキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。IPsec Security Association（SA：セキュリティ アソシエーション）のネゴシエーション中に、ピアでは、両方のピアに共通するトランスフォーム セットが検索されます。

IKE バージョン（IKEv1 または IKEv2）に基づいて、別個の IPsec プロポーザル オブジェクトがあります。

- IKEv1 IPsec プロポーザルを作成する場合、IPSec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。アルゴリズムには単一のオプションを選択できます。VPN で複数の組み合わせをサポートするには、複数の IKEv1 IPsec プロポーザル オブジェクトを作成して選択します。
- IKEv2 IPsec プロポーザルを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、マッチが見つかるまでピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

カプセル化セキュリティ プロトコル（ESP）は、IKEv1 と IKEv2 IPsec プロポーザルの両方に使用されます。これは認証、暗号化、およびアンチリプレイ サービスを提供します。ESP は、IP プロトコル タイプ 50 です。

（注） IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

次に、各 IKE バージョンの IPsec プロポーザルの設定方法を説明します。

- IKEv1 IPSec プロポーザルオブジェクトの作成および編集
- IKEv2 IPSec プロポーザルオブジェクトの作成および編集

IPsec プロポーザルオブジェクトの管理

IPsec プロポーザル オブジェクトは、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。IKEv1 と IKEv2 に対して、異なるオブジェクトがあります。現在、Cisco Defense Orchestrator（CDO）は IKEv1 IPsec プロポーザルオブジェクトをサポートしています。

カプセル化セキュリティ プロトコル（ESP）は、IKEv1 と IKEv2 IPsec プロポーザルの両方に使用されます。このプロトコルにより、認証、暗号化、およびアンチリプレイサービスが実現します。ESP は、IP プロトコル タイプ 50 です。

（注） IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

関連トピック

IKEv1 IPSec プロポーザルオブジェクトの作成または編集 （276 ページ）

FTD IKEv1 IPSec プロポーザルオブジェクトの作成または編集

定義済みの複数の IKEv1 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトの編集や削除はできません。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。サイト間 VPN 接続の IKEv1 IPSec 設定を編集している間に、オブジェクトリストに表示される [新規IKEv1プロポーザルの作成（Create New IKEv1 Proposal）] リンクをクリックして、IKEv1 IPSec プロポーザルオブジェクトを作成することもできます。

手順

ステップ 1 ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青色のプラスボタン  をクリックし、[FTD] > [IKEv1 IPSecプロポーザル（IKEv1 IPsec Proposal）] を選択して新しいオブジェクトを作成します。
- オブジェクトページで、編集する IPSec プロポーザルを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 新しいオブジェクトのオブジェクト名を入力します。

ステップ 4 IKEv1 IPSec プロポーザルオブジェクトが動作するモードを選択します。

- トンネルモードでは IP パケット全体がカプセル化されます。IPSec ヘッダーが、元の IP ヘッダーと新しい IP ヘッダーとの間に追加されます。これがデフォルトです。トンネルモードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネルモードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイアウォール（またはその他のセキュリティ ゲートウェイ）間で通常の IPSec が実装される標準の方法です。
- トランスポートモードでは IP パケットの上位層プロトコルだけがカプセル化されます。IPSec ヘッダーは、IP ヘッダーと上位層プロトコル ヘッダー（TCP など）との間に挿入されます。トランスポート モードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポート モードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。一般的に、トランスポート モード

は、レイヤ 2 またはレイヤ 3 のトンネリング プロトコル（GRE、L2TP、DLSW など）を保護する場合にだけ使用されます。

ステップ 5 このプロポーザルの [ESP暗号化（ESP Encryption）]（カプセル化セキュリティプロトコル暗号化）アルゴリズムを選択します。オプションの説明については、使用する暗号化アルゴリズムの決定 （261 ページ）を参照してください。

ステップ 6 認証に使用する [ESPハッシュ（ESP Hash）] または整合性アルゴリズムを選択します。オプションの説明については、使用するハッシュ アルゴリズムの決定 （262 ページ）を参照してください。

ステップ 7 [追加（Add）] をクリックします。

IKEv2 IPsec プロポーザルオブジェクトの管理

IPsec プロポーザル オブジェクトは、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。

IKEv2 IPsec プロポーザルを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、マッチが見つかるまでピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

関連トピック

IKEv2 IPSec プロポーザルオブジェクトの作成または編集 （277 ページ）

FTD IKEv2 IPSec プロポーザルオブジェクトの作成または編集

定義済みの複数の IKEv2 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトの編集や削除はできません。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。VPN 接続の IKEv2 IPsec 設定を編集している間に、オブジェクト リストに表示される [新規IPsecプロポーザルの作成（Create New IPsec Proposal）] リンクをクリックして、IKEv2 IPsec プロポーザル オブジェクトを作成することもできます。

手順

ステップ 1 ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青色のプラスボタン  をクリックし、[FTD] > [IKEv2 IPSecプロポーザル（IKEv2 IPsec Proposal）] を選択して新しいオブジェクトを作成します。

- オブジェクトページで、編集する IPSec プロポーザルを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 新しいオブジェクトのオブジェクト名を入力します。

ステップ 4 IKEv2 IPsec プロポーザルオブジェクトの設定：

- [暗号化（Encryption）]：このプロポーザルのカプセル化セキュリティプロトコル（ESP）暗号化アルゴリズム。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用する暗号化アルゴリズムの決定 （261 ページ）を参照してください。
- [整合性ハッシュ（Integrity Hash）]：認証に使用するハッシュまたは整合性アルゴリズム。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用するハッシュ アルゴリズムの決定 （262 ページ）を参照してください。

ステップ 5 [追加（Add）] をクリックします。

グローバル IKE ポリシーの設定

Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティアソシエーション）の自動的な確立に使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティアソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

IKE ポリシー オブジェクトはこれらのネゴシエーションに対して IKE プロポーザルを定義します。有効にするオブジェクトは、ピアが VPN 接続をネゴシエートするときに使用するものであり、接続ごとに異なる IKE ポリシーを指定することはできません。各オブジェクトの相対的な優先順位は、これらの中でどのポリシーを最初に試行するかを決定します。数が小さいほど、優先順位が高くなります。ネゴシエーションで両方のピアがサポートできるポリシーを見つけられなければ、接続は確立されません。

IKE グローバル ポリシーを定義するには、各 IKE バージョンを有効にするオブジェクトを選択します。事前定義されたオブジェクトが要件を満たさない場合、セキュリティ ポリシーを適用する新しいポリシーを作成します。

次に、オブジェクト ページでグローバル ポリシーを設定する方法について説明します。VPN 接続を編集しているときに IKE ポリシー設定の [編集（Edit）] をクリックすることで、ポリシーの有効化、無効化および作成が行えます。

次に、各バージョンの IKE ポリシーの設定方法を説明します。

- IKEv1 ポリシーの設定
- IKEv2 ポリシーの設定

IKEv1 ポリシーの管理

IKEv1 ポリシーを作成および編集する方法について説明します。

IKEv1 ポリシーについて

インターネット キー エクスチェンジ（IKE）バージョン 1 ポリシー オブジェクトには、VPN 接続を定義する際に必要な IKEv1 ポリシーが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動確立に使用されます。

複数の事前定義された IKEv1 ポリシーが存在します。必要に適したポリシーがあれば、[状態（State）] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

関連トピック

IKEv1 ポリシーの作成または編集 （271 ページ）

FTD IKEv1 ポリシーの作成または編集

次に、オブジェクト ページからオブジェクトを直接作成および編集する方法について説明します。サイト間 VPN 接続での IKE 設定の編集時に、オブジェクトリストに表示される [新しい IKEv1 ポリシーの作成（Create New IKEv1 Policy）] リンクをクリックして、IKEv1 ポリシーを作成することもできます。

手順

ステップ 1 ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青いプラスボタン  をクリックし、[FTD] > [IKEv1ポリシー（IKEv1 Policy）] を選択して、新しい IKEv1 ポリシーを作成します。
- オブジェクトのページで、編集する IKEv1 ポリシーを選択し、右側の [操作（Actions）] ウィンドウで [編集（Edit）] をクリックします。

ステップ 3 [オブジェクト名（Object Name）] を 128 文字以内で入力します。

ステップ 4 IKEv1 プロパティを設定します。

- [優先順位（Priority）]：IKE ポリシーの相対的優先順位（1 ～ 65,535）。このプライオリティによって、共通のセキュリティアソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最も高いプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。

- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティ アソシエーション（SA）の確立に使用される暗号化アルゴリズム。オプションの説明については、「使用する暗号化アルゴリズムの決定」を参照してください。

- [Diffie-Hellmanグループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。オプションの説明については、「使用する Diffie-Hellman 係数グループの決定」を参照してください。

- [ライフタイム（Lifetime）]：セキュリティアソシエーション（SA）のライフタイム（120 ～ 2147483647 までの秒数、または空白）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは 86400 です。無期限のライフタイムを指定するには、値を入力しません（フィールドを空白のままにします）。

- [認証（Authentication）]：2 つのピア間で使用される認証方式。詳細については、使用する認証方式の決定 （263 ページ）を参照してください。

  - [事前共有キー（Preshared Key）]：各デバイスで定義されている事前共有キーを使用します。事前共有キーを使用すると、秘密鍵を 2 つのピア間で共有し、認証フェーズ中に IKE で使用できます。ピアに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。

  - [証明書（Certificate）]：ピアのデバイス ID 証明書を使用して相互に識別します。認証局に各ピアを登録することによって、これらの証明書を取得する必要があります。また、各ピアでアイデンティティ証明書の署名に使用された、信頼できる CA ルート証明書および中間 CA 証明書もアップロードする必要があります。ピアは、同じ CA または別の CA に登録できます。どちらのピアにも自己署名証明書を使用することはできません。

- [ハッシュ（Hash）]：メッセージの整合性の確保に使用されるメッセージダイジェストを作成するためのハッシュ アルゴリズム。オプションの説明については、VPN で使用される暗号化アルゴリズムとハッシュアルゴリズム （260 ページ）を参照してください。

ステップ 5 [追加（Add）] をクリックします。

IKEv2 ポリシーの管理

IKEv2 ポリシーを作成および編集する方法について説明します。

IKEv2 ポリシーについて

インターネット キー エクスチェンジ（IKE）バージョン 2 ポリシー オブジェクトには、VPN 接続を定義する際に必要な IKEv2 ポリシーが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動確立に使用されます。

複数の事前定義された IKEv2 ポリシーがあります。必要に適したポリシーがあれば、[状態（State）] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

関連トピック

IKEv2 ポリシーの作成または編集 （273 ページ）

FTD IKEv2 ポリシーの作成または編集

次に、オブジェクトページからオブジェクトを直接作成および編集する方法について説明します。サイト間 VPN 接続での IKE 設定の編集時に、オブジェクトリストに表示される [新しい IKEv2ポリシーの作成（Create New IKEv2 Policy）] リンクをクリックして、IKEv2 ポリシーを作成することもできます。

手順

ステップ 1 CDO ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青いプラスボタン をクリックし、[FTD] > [IKEv2 ポリシー] を選択して、新しい IKEv2 ポリシーを作成します。
- オブジェクトページで、編集する IKEv2 ポリシーを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 [オブジェクト名（Object Name）] を 128 文字以内で入力します。

ステップ 4 IKEv2 プロパティを設定します。

- [優先順位（Priority）]：IKE ポリシーの相対的優先順位（1 ～ 65,535）。このプライオリティによって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエー

ションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最も高いプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。

- [状態（State）]：IKE ポリシーが有効か無効かを示します。トグルをクリックして状態を変更します。IKE ネゴシエーション中には、有効なポリシーのみが使用されます。
- [暗号化（Encryption）]：フェーズ2ネゴシエーションを保護するためのフェーズ1セキュリティ アソシエーション（SA）の確立に使用される暗号化アルゴリズム。有効にするすべてのアルゴリズムを選択します。ただし、同じポリシーに混合モード（AES-GCM）と通常モードのオプションを含めることはできません（通常モードでは整合性ハッシュを選択する必要がありますが、混合モードでは個別の整合性ハッシュの選択は禁止されています）。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用する暗号化アルゴリズムの決定 （261 ページ）を参照してください。
- [Diffie-Hellmanグループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。許可するすべてのアルゴリズムを選択します。システムは、最も強いグループから始めて最も弱いグループに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用する Diffie-Hellman 係数グループの決定 （263 ページ）を参照してください。
- [整合性ハッシュ（Integrity Hash）]：メッセージの整合性の確保に使用されるメッセージダイジェストを作成するためのハッシュ アルゴリズムの整合性部分。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。整合性ハッシュは、AES-GCM 暗号化オプションでは使用されません。オプションの説明については、VPN で使用される暗号化アルゴリズムとハッシュアルゴリズム （260 ページ）を参照してください。
- [擬似ランダム関数（PRF）ハッシュ（Pseudo-Random Function（PRF）Hash）]：ハッシュアルゴリズムの疑似ランダム関数（PRF）部分。このアルゴリズムはIKEv2 トンネル暗号化に必要なキー関連情報とハッシュ操作を取得するために使用されます。IKEv1 では、整合性と PRF アルゴリズムは別ですが、IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、VPN で使用される暗号化アルゴリズムとハッシュアルゴリズム （260 ページ）を参照してください。
- [ライフタイム（Lifetime）]：セキュリティ アソシエーション（SA）のライフタイム（120 ～ 2147483647 までの秒数、または空白）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは 86400 です。無期

限のライフタイムを指定するには、値を入力しません（フィールドを空白のままにします）。

ステップ 5 [追加（Add）] をクリックします。

RA VPN オブジェクト

AnyConnectクライアント プロファイル オブジェクト

AnyConnect クライアント プロファイル オブジェクトの作成および編集

手順

テキスト作成中

セキュリティ ゾーン オブジェクト

セキュリティゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中にのみ存在できます。

Firepower システムでは、初期設定中に次のゾーンが作成され、Defense Orchestrator のオブジェクトページに表示されます。ゾーンを編集してインターフェイスを追加または削除したり、使用しなくなったゾーンを削除したりできます。

- **inside_zone**：内部インターフェイスが含まれます。このゾーンは、内部ネットワークを表します。
- **outside_zone**：外部インターフェイスが含まれます。このゾーンは、インターネットなどの制御不可能な外部ネットワークを表すことを目的としています。

通常、ネットワーク内で果たす役割によって、インターフェイスをグループ化します。たとえば、インターネットに接続するインターフェイスを **outside_zone** セキュリティゾーンに配置し、内部ネットワークに接続するすべてのインターフェイスを **inside_zone** セキュリティゾーンに配置できます。次に、外部ゾーンから来て内部ゾーンへ向かうトラフィックにアクセスコントロール ルールを適用できます。

ゾーンを作成する前に、ネットワークに適用するアクセスルールや他のポリシーを検討してください。たとえば、すべての内部インターフェイスを同じゾーンに配置する必要はありません。4 つの内部ネットワークがあり、1 つだけ他の 3 つとは異なる処理をしたい場合、1 つではなく 2 つのゾーンを作成できます。パブリック Web サーバへの外部アクセスを許可するインターフェイスがある場合、そのインターフェイスに別のゾーンを使用できます。

関連情報：

- Firepowerセキュリティゾーンのオブジェクトを作成または編集する
- Firepower インターフェイスをセキュリティゾーンに割り当てる
- オブジェクトの削除

Firepower セキュリティ ゾーン オブジェクトの作成または編集

セキュリティゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中にのみ存在できます。詳細については、「セキュリティ ゾーン オブジェクト」を参照してください。

セキュリティ ゾーン オブジェクトは、デバイスのルールで使用されない限り、そのデバイスに関連付けられません。

セキュリティ ゾーン オブジェクトの作成

セキュリティ ゾーン オブジェクトを作成するには、以下の手順に従ってください。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 青いプラスボタン をクリックし、FTD セキュリティゾーンを選択してオブジェクトを作成します。 >

ステップ 3 オブジェクトに名前を付け、任意で説明を入力します。

ステップ 4 セキュリティゾーンに含めるインターフェイスを選択します。

ステップ 5 [追加（Add）] をクリックします。

セキュリティ ゾーン オブジェクトの編集

FTDをオンボーディングすると、少なくとも2つのセキュリティゾーンがすでに存在することがわかります。1 つは inside_zone で、もう 1 つは outside_zone です。これらのゾーンは編集または削除できます。セキュリティ ゾーン オブジェクトを編集するには、次の手順に従います。

手順

ステップ 1 編集するオブジェクトを見つけます。

- オブジェクトの名前がわかっている場合は、[オブジェクト（Objects）]ページで検索できます。
  - リストをセキュリティゾーンでフィルタリングします。

- オブジェクトの名前を検索フィールドに入力します。
- オブジェクトを選択します。

- オブジェクトがデバイスに関連付けられていることがわかっている場合は、[デバイスとサービス（Devices & Services）] ページから検索を開始できます。
  - ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。
  - [デバイス] タブをクリックします。
  - 適切なタブをクリックします。
  - デバイスフィルタと検索バーを使用して、デバイスを見つけます。
  - デバイスを選択します。
  - 右側の [管理（Management）] ペインで、  [オブジェクト（Objects）] をクリックします。
  - オブジェクトフィルタ と検索バーを使用して、探しているオブジェクトを見つけます。

（注） 作成したセキュリティ ゾーン オブジェクトがデバイスのポリシーに含まれるルールに関連付けられていない場合、そのオブジェクトは「関連付けられていない」と見なされ、デバイスの検索結果に表示されません。

ステップ 2 オブジェクトを選択します。

ステップ 3 右側の [操作（Actions）] ウィンドウで [編集（Edit）] アイコン をクリックします。

ステップ 4 オブジェクトの属性を編集した後、[保存（Save）] をクリックします。

ステップ 5 [保存（Save）] をクリックすると、加えた変更が他のデバイスにどのように影響するかを説明するメッセージが表示されます。[確認（Confirm）] をクリックして変更を確定するか、[キャンセル（Cancel）] をクリックして変更を取り消します。

サービス オブジェクト

Firepower サービスオブジェクト

FTD サービスオブジェクト、サービスグループ、およびポートグループは、IP プロトコルスイートの一部が考慮されたプロトコルまたはポートを含む再利用可能なコンポーネントです。

FTD サービスグループは、サービスオブジェクトのコレクションです。1 つのサービスグループには、1 つ以上のプロトコルのオブジェクトを含めることができます。その後、トラフィックの一致基準を定義するためのセキュリティポリシーでオブジェクトを使用して、たとえばア

クセスルールを使用して特定のTCPポートへのトラフィックを許可できます。システムには、一般的なサービス向けの複数の事前定義されたオブジェクトが含まれています。これらのオブジェクトはポリシーで使用できます。ただし、システムで定義されたオブジェクトは編集または削除ができません。

Firepower Defense Manager および Firepower Management Center では、サービスオブジェクトをポートオブジェクトとして、およびサービスグループとポートグループとして参照します。

詳細については、「Firepower Threat Defense サービスオブジェクトの作成と編集」を参照してください。

プロトコルオブジェクト

プロトコルオブジェクトは、使用頻度の低いプロトコルやレガシープロトコルを含むサービスオブジェクトの一種です。プロトコルオブジェクトは、名前とプロトコル番号で識別されます。CDO は、ASA および Firepower（FTD）設定でこれらのオブジェクトを認識し、これらに独自のフィルタ「プロトコル（Protocols"）」を適用します。そのため、これらのオブジェクトを簡単に見つけることができます。

詳細については、「Firepower Threat Defense サービスオブジェクトの作成と編集」を参照してください。

ICMP オブジェクト

Internet Control Message Protocol （ICMP）オブジェクトは、ICMP および IPv6-ICMP メッセージ専用のサービスオブジェクトです。CDO は、ASA および Firepower（FTD）がオンボードされたときにデバイスの設定でこれらのオブジェクトを認識し、これらに独自のフィルタ「ICMP」を適用します。そのため、これらのオブジェクトを簡単に見つけることができます。

CDO を使用して、ASA 設定から ICMP オブジェクトの名前を変更したり、ICMP オブジェクトを削除したりできます。CDO を使用して、Firepower 設定の ICMP および ICMPv6 オブジェクトを作成、更新、および削除できます。

（注） ICMPv6 プロトコルの場合、AWS は特定の引数の選択をサポートしていません。すべての ICMPv6 メッセージを許可するルールのみがサポートされます。

詳細については、「Firepower Threat Defense サービスオブジェクトの作成と編集」を参照してください。

関連情報：

- オブジェクトの削除

Firepower サービスオブジェクトの作成および編集

Firepower サービスオブジェクトを作成するには、次の手順を実行します。

Firepower Threat Defense（FTD）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。Firepower Defense Manager および Firepower Management Center では、それらのオブジェクトを「ポートオブジェクト」と呼びます。

手順

ステップ 1 左側のメインナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 右側の青色のボタン  をクリックしてオブジェクトを作成し、**[FTD]**>**[サービス（Service）]** を選択します。

ステップ 3 オブジェクト名と説明を入力します。

ステップ 4 [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 5 [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 6 次の手順に従い、プロトコルを設定します。

- **TCP**、**UDP**
  - [eq] を選択し、ポート番号またはプロトコル名を入力します。たとえば、ポート番号として 80 を入力したり、プロトコル名として HTTP を入力したりできます。
  - [範囲（range）] を選択して、ポート番号の範囲を入力することもできます（例、1 65535 （すべてのポートをカバーする場合））。
- **ICMP**、**IPv6-ICMP**：ICMP タイプを選択します。タイプをすべての ICMP メッセージに適用するには、[任意（Any）] を選択します。タイプとコードについての詳細は、次のページを参照してください。
  - [ICMP]：http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - [ICMPv6]：http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- [その他（Other）]：目的のプロトコルを選択します。

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すべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Firepower サービスグループの作成

サービスグループは、1 つ以上のプロトコルを表す 1 つ以上のサービスオブジェクトで構成できます。サービスオブジェクトは、グループに追加する前に作成する必要があります。Firepower Defense Manager および Firepower Management Center では、それらのオブジェクトを「ポートオブジェクト」と呼びます。

手順

ステップ 1 左側のメインナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 右側の青いボタン  をクリックしてオブジェクトを作成し、[FTD] > [サービス（Service）] を選択します。

ステップ 3 オブジェクト名と説明を入力します。

ステップ 4 [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 5 [オブジェクトの追加（Add Object）] をクリックして、オブジェクトをグループに追加します。

- 上記の「Firepower サービスオブジェクトの作成」で行ったように、[作成（Create）] をクリックして新しいオブジェクトを作成します。
- [選択（Choose）] をクリックして、既存のサービスオブジェクトをグループに追加します。この手順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 6 サービスグループへのサービスオブジェクトの追加が完了したら、[追加（Add）] をクリックします。

ステップ 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Firepower サービスオブジェクトまたはサービスグループの編集

手順

ステップ 1 左側のメインナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 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 3 [アクション（Actions）] ペインで、[編集（Edit）]  をクリックします。

ステップ 4 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 5 [保存（Save）] をクリックします。

ステップ 6 CDO 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 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

セキュリティ グループ タグ グループ

FTD セキュリティグループタグ

セキュリティグループタグについて

Cisco TrustSec ネットワークでトラフィックを分類するために Cisco Identity Services Engine（ISE）を使用して**セキュリティグループタグ**（SGT）を定義して使用する場合は、一致基準として SGT を使用するアクセス制御ルールを作成できます。これにより、IP アドレスではなく、セキュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することができます。

ISE で SGT を作成し、各タグにホストまたはネットワークの IP アドレスを割り当てることができます。ユーザー アカウントに SGT を割り当てた場合、SGT はユーザーのトラフィックに割り当てられます。ISE サーバーに接続するように FTD を構成して SGT をした後、CDO で SGT グループを作成し、それらに関するアクセスコントロールルールを構築できます。SGT を FTD デバイスに関連付ける前に、ISE の SGT 交換プロトコル（SXP）マッピングを構成する必要があることに注意してください。詳細は、現在実行しているバージョンの『Cisco Identity Services Engine 管理者ガイド』の「**セキュリティグループタグ交換プロトコル**」を参照してください。

FTD は、アクセス制御ルールのトラフィック一致基準として SGT を評価するときに、次の優先順位を使用します。

1. パケット内で定義されている送信元SGT（存在する場合）。宛先の照合は、この手法では行われません。SGTがパケットに含まれるようにするには、ネットワーク内のスイッチとルータがそれらを追加するように設定されている必要があります。このメソッドの実装方法については、ISE のマニュアルを参照してください。
2. ISEセッションディレクトリからダウンロードされるユーザーセッションに割り当てられた SGT。この種の SGT 照合では、セッションディレクトリ情報をリッスンするオプションを有効にする必要がありますが、このオプションは最初に ISE アイデンティティソースを作成するときにデフォルトでオンになっています。SGTは、送信元または宛先と照合することができます。必須ではありませんが、通常は ISE アイデンティティソースを AD レルムとともに使用してパッシブ認証アイデンティティルールを設定し、ユーザ ID 情報を収集します。
3. SXP を使用してダウンロードされた SGT-to-IP アドレス マッピング。IP アドレスが SGT の範囲内にある場合、トラフィックはSGTを使用するアクセス制御ルールと一致します。SGT は、送信元または宛先と照合することができます。

（注） ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりに、ウンロードした SGT 情報を参照する SGT グループを作成する必要があります。SGT グルーは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションに基づいてポリシーを適用できます。

バージョン サポート

CDO は現在、バージョン 6.5 以降を実行している FTD で SGT および SGT グループをサポートしています。FDM では、バージョン 6.5 以降で ISE サーバを構成して接続できますが、バージョン 6.7 までは FDM UI からの SGT 構成をサポートしていません。

これは、バージョン 6.5 以降を実行している FTD は SGT の SXP マッピングをダウンロードできますが、オブジェクトまたはアクセスコントロールルールに手動で追加できないことを意味します。バージョン 6.5 またはバージョン 6.6 を実行しているデバイスの SGT に変更を加えるには、ISE UI を使用する必要があります。ただし、バージョン 6.5 を実行しているデバイスが CDO にオンボーディングされている場合は、デバイスに関連付けられている現在の SGT を表示し、SGT グループを作成できます。

CDO の SGT

セキュリティグループタグ

SGT は、CDO では読み取り専用です。CDO で SGT を作成または編集することはできません。SGT を作成するには、現在実行しているバージョンの『Cisco Identity Services Engine 管理者ガイド』を参照してください。https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

SGT グループ

（注） FDM では、SGT のグループを SGT 動的オブジェクトと呼びます。CDO では、これらのタグのリストは現在 SGT グループと呼ばれています。FDM または ISE UI を参照せずに、CDO で SGT グループを作成できます。

SGT グループを使用して、ISE によって割り当てられた SGT に基づいて送信元または宛先アドレスを識別します。その後、トラフィックの一致基準を定義するためにアクセス制御ルールでオブジェクトを使用できます。ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりに、ダウンロードした SGT 情報を参照する SGT グループを作成する必要があります。

SGT グループは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションに基づいてポリシーを適用できます。

CDO で SGT グループを作成するには、少なくとも 1 つの構成済み SGT と、使用するデバイスの FDM コンソール用に構成された ISE サーバーからの SGT マッピングが必要です。複数の FTD が同じ ISE サーバに関連付けられている場合、SGT または SGT グループを複数のデバイスに適用できます。デバイスが ISE サーバに関連付けられていない場合、アクセスコントロールルールに SGT オブジェクトを含めたり、そのデバイス構成に SGT グループを適用したりすることはできません。

ルール内の SGT グループ

SGT グループをアクセスコントロールルールに追加できます。それらは、送信元または宛先のネットワークオブジェクトとして表示されます。ネットワークがルールでどのように機能するかの詳細は、『FTD アクセス コントロール ルールの送信元および宛先の基準』を参照してください。

[オブジェクト（Objects）] ページから SGT グループを作成できます。詳細については、FTD SGT グループの作成を参照してください。

FTD SGT グループの作成

アクセス制御ルールに使用できる SGT グループを作成するには、次の手順を実行します。

始める前に

セキュリティグループタグ（SGT）グループを作成する前に、次の構成または環境を設定しておく必要があります。

- FTD デバイスは、少なくともバージョン 6.5 を実行している必要があります。
- SXP マッピングを登録して変更を展開できるように ISE アイデンティティソースを設定する必要があります。SXP マッピングの管理については、使用しているバージョン（バージョン 6.7 以降）用の『Firepower Device Manager Configuration Guide』[英語] の「**Configure Security Groups and SXP Publishing in ISE**」を参照してください。
- すべての SGT は ISE で作成する必要があります。SGT の作成については、現在実行しているバージョンの『Cisco Identity Services Engine コンフィギュレーション ガイド』を参照してください。

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 [FTD] > [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（Object Name）] を入力します。

ステップ 5 （任意）説明を追加します。

ステップ 6 [SGT] をクリックし、ドロップダウンメニューを使用して、グループに含めるすべての SGT のチェックボックスをオンにします。SGT 名順にリストをソートできます。

ステップ 7 [保存（Save）] をクリックします。

（注） CDO で SGT を作成したり編集したりすることはできません。SGT グループへの追加やグループからの削除のみを実行できます。SGT を作成または編集するには、現在実行しているバージョンの『Cisco Identity Services Engine Configuration Guide』を参照してください。

FTD SGT グループの編集

SGT グループを編集するには、次の手順を使用します。

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 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 SGT グループを見つけます。

ステップ 3 SGT グループを選択し、[操作（Actions）] ウィンドウで編集アイコン をクリックします。

ステップ 4 SGT グループを変更します。グループに関連付けられた名前、説明、または SGT を編集します。

ステップ 5 [保存（Save）] をクリックします。

（注） CDO で SGT を作成したり編集したりすることはできません。SGT グループへの追加やグループからの削除のみを実行できます。SGT を作成または編集するには、現在実行しているバージョンの『Cisco Identity Services Engine Configuration Guide』を参照してください。

FTD SGT グループのアクセス制御ルールへの追加

SGT グループをアクセス制御ルールに追加するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、SGT グループを追加するデバイスを選択します。

ステップ 4 [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 5 [送信元（Source）] オブジェクトまたは [宛先（Destination）] オブジェクトの青いプラスボタン をクリックし、[SGTグループ（SGT Groups）] を選択します。

ステップ 6 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 SGT グループを見つけます。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 すべてのデバイスの設定変更のプレビューと展開。

（注） 追加のSGTグループを作成する必要がある場合は、[新しいオブジェクトを作成（Create New Object）] をクリックします。「FTD SGT グループの作成」に記載されている必須情報を入力し、SGT グループをルールに**追加**します。

Syslog サーバーオブジェクト

FTD ではイベントを保存するための容量が制限されています。イベントのストレージを最大化するために、外部サーバーを構成できます。システムログ（syslog）サーバーのオブジェクトはコネクション型メッセージまたは診断 syslog メッセージを受信できるサーバーを指定します。syslog サーバーにログ収集と分析のための設定がある場合は、Defense Orchestrator を使用してオブジェクトを作成してそれらを定義し、関連ポリシーでこのオブジェクトを使用します。

Syslog サーバーオブジェクトの作成および編集

新しい syslog サーバーオブジェクトを作成するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 新しいオブジェクトを作成するには、[オブジェクトの作成（Create Object）] ボタン  をクリックします。

ステップ 3 FTD オブジェクトタイプの下で [Syslog サーバ（Syslog Server）] を選択します。

ステップ 4 syslog サーバーオブジェクトのプロパティを設定します。

- [IPアドレス（IP Address）]：syslog サーバーの IP アドレスを入力します。
- [プロトコルタイプ（Protocol Type）]：syslog サーバーがメッセージの受信に使用するプロトコルを選択します。[TCP] を選択すると、システムは syslog サーバーが利用できない場合を認識して、サーバーが再度利用可能になるまでイベントの送信を停止できます。
- [ポート番号（Port Number）]：syslog に使用する有効なポート番号を入力します。syslog サーバーがデフォルトのポートを使用している場合は、デフォルトの UDP ポートとして 514 を入力するか、デフォルトの TCP ポートとして 1470 を入力します。サーバーがデフォルトのポートを使用していない場合は、正しいポート番号を入力します。1025 ～ 65535 の範囲のポートを使用してください。
- [インターフェイスの選択（Select an interface）]：診断 syslog メッセージの送信に使用するインターフェイスを選択します。接続および侵入イベントでは常に管理インターフェイス

を使用します。インターフェイスの選択によって、syslog メッセージに関連付けられる IP アドレスが決まります。以下にリストされているオプションで選択できるのは 1 つだけです。両方を選択することはできません。次のオプションのいずれかを選択します。

- [データインターフェイス（Data Interface）]：選択したデータ インターフェイスを診断 syslog メッセージに使用します。生成されたリストからインターフェイスを選択します。サーバーがブリッジグループのメンバーインターフェイスを介してアクセスできる場合、ブリッジグループ インターフェイス（BVI）を選択します。診断インターフェイス（物理的な管理インターフェイス）経由でアクセスできる場合は、このオプションではなく [管理インターフェイス（Management Interface）] を選択することを推奨します。パッシブ インターフェイスを選択することはできません。データインターフェイスで通信する場合、接続および侵入の syslog メッセージでは、送信元 IP アドレスが管理インターフェイスかゲートウェイ インターフェイスで使用されます。
- [管理インターフェイス（Management Interface）]：すべてのタイプの syslog メッセージに仮想管理インターフェイスを使用します。データインターフェイスで通信する場合、送信元 IP アドレスが管理インターフェイスかゲートウェイ インターフェイスで使用されます。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Syslog サーバーオブジェクトの編集

既存の syslog サーバーオブジェクトを編集するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 対象の syslog サーバーオブジェクトを見つけて選択します。オブジェクトリストは、syslog サーバーオブジェクトタイプでフィルタリング できます。

ステップ 3 [アクション（Actions）] ペインで、[編集（Edit）] をクリックします。

ステップ 4 必要な編集を行って、[保存（Save）] をクリックします。

ステップ 5 行った変更を確認します。

ステップ 6 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

関連情報：

- オブジェクトの削除

Secure Logging Analytics（SaaS）の Syslog サーバーオブジェクトの作成

イベントを送信する Secure Event Connector（SEC）の IP アドレス、TCP ポート、または UDP ポートを使用して、syslog サーバーオブジェクトを作成します。テナントにオンボーディングした SEC ごとに 1 つの syslog オブジェクトを作成しますが、1 つのルールから 1 つの SEC を表す 1 つの syslog オブジェクトのみにイベントを送信します。

前提条件

このタスクは、より大きなワークフローの一部です。開始する前に「FTD デバイスに安全なロギング分析（SaaS）を導入する」を参照してください。

手順

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 新しいオブジェクトを作成するには、[オブジェクトの作成（Create Object）] ボタン  をクリックします。

ステップ 3 FTD オブジェクトタイプの下で [Syslog サーバー（Syslog Server）] を選択します。

ステップ 4 syslog サーバーオブジェクトのプロパティを設定します。SEC のこれらのプロパティを見つけるには、アカウントメニューをクリックし、[セキュア コネクタ（Secure Connectors）] をクリックします。次に、syslog オブジェクトを設定する Secure Event Connector を選択し、右側の [詳細（Details）] ペインを調べます。

- [IP アドレス（IP Address）]：SEC の IP アドレスを入力します。
- [プロトコルタイプ（Protocol Type）]：TCP または UDP を選択します。
- [ポート番号（Port Number）]：TCP を選択した場合はポート 10125、UDP を選択した場合は 10025 を入力します。
- [インターフェイスの選択（Select an interface）]：SEC に到達するように設定されたインターフェイスを選択します。

（注） FTD は IP アドレスごとに 1 つの syslog オブジェクトをサポートするため、TCP と UDP のどちらを使用するかを選択する必要があります。

ステップ 5 [追加（Add）] をクリックします。

次のタスク

セキュアロギング分析（SaaS）を導入し、Secure Event Connector を介して Cisco Cloud にイベントを送信するための既存の CDO カスタマーワークフローのステップ 3 に進みます。

URL オブジェクト

URL オブジェクトと URL グループは、Firepower デバイスによって使用されます。URL オブジェクトとグループ（URL オブジェクトと総称する）を使用して、Web リクエストの URL または IP アドレスを定義します。これらのオブジェクトを使用して、アクセス制御ポリシーに手動の URL フィルタリング、またはセキュリティ インテリジェンス ポリシーにブロッキングを実装できます。URL オブジェクトは単一の URL または IP アドレスを定義するのに対して、URL グループは複数の URL または IP アドレスを定義します。

はじめる前に

URL オブジェクトを作成する場合は、次の点に注意してください。

- パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバーのホスト名のみに基づきます。ホスト名は、:// の区切り記号の後、またはホスト名のドットの後に来る場合、一致とみなされます。たとえば、ign.com は ign.com および www.ign.com と一致するが、verisign.com とは一致しません。
- 1 つ以上の / を含める場合、サーバ名、パス、およびクエリ パラメータを含む文字列の部分一致には URL 文字列全体が使用されます。ただし、サーバは再構成することができ、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部をブロックまたは許可するのに手動の URL フィルタリングは使用しないことをお勧めします。文字列の部分一致も予期しない一致となる可能性があり、URL オブジェクトに含める文字列が意図しないサーバ上のパスやクエリ パラメータ内の文字列とも一致することがあります。
- システムは、暗号化プロトコル（HTTP と HTTPS）を無視します。つまり、ある Web サイトをブロックした場合、アプリケーション条件で特定のプロトコルを対象にしない限り、その Web サイトに向かう HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、http://example.com の代わりに example.com を使用します。
- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

  ただし、証明書のサブジェクト共通名が Web サイトのドメイン名とはまったく関係ない場合があることをご了承ください。たとえば、youtube.com の証明書のサブジェクト共通名は *.google.com です（当然、これは随時変更される可能性があります）。SSL 復号ポリシーを使用して HTTPS トラフィックを復号し、URL フィルタリング ルールが復号されたトラフィックで動作するようにすると、より一貫性のある結果が得られるようになります。

（注） 証明書情報を利用できないためにブラウザがTLSセッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

FTD URL オブジェクトの作成または編集

Firepower Threat Defense（FTD）URL オブジェクトは、URL または IP アドレスを指定する再利用可能なコンポーネントです。Firepower Defense Manager および Firepower Management Center では、これらのオブジェクトは「URL オブジェクト」とも呼ばれます。

Firepower URL オブジェクトを作成するには、次の手順を実行します。

手順

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[FTD]** > **[URL]**をクリックします。

ステップ 3 オブジェクト名と説明を入力します。

ステップ 4 [URLオブジェクトの作成（Create a URL object）] を選択します。

ステップ 5 オブジェクトに固有の URL または IP アドレスを入力します。

ステップ 6 [追加（Add）] をクリックします。

Firepower URL グループの作成

URL グループは、1 つ以上の URL または IP アドレスを表す 1 つ以上の URL オブジェクトで構成できます。Firepower Defense Manager および Firepower Management Center では、これらのオブジェクトは「URL オブジェクト」とも呼ばれます。

手順

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[FTD]** > **[URL]**をクリックします。

ステップ 3 オブジェクト名と説明を入力します。

ステップ 4 [URLグループの作成（Create a URL group）] を選択します。

ステップ 5 [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 6 URL グループへの URL オブジェクトの追加が完了したら、[追加（Add）] をクリックします。

Firepower URL オブジェクトまたは URL グループの編集

手順

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

ステップ 2 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 3 詳細ペインで、編集する をクリックします。

ステップ 4 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 5 [保存（Save）] をクリックします。

ステップ 6 CDO 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。

セキュリティ ポリシー管理

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。CDO 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。

- FTD ポリシーの設定 （125 ページ）
- ネットワーク アドレス変換 （224 ページ）

FTD ポリシーの設定

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、セキュリティの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。CDO を使用して、Firepower Threat Defense のセキュリティポリシーの全コンポーネントを管理します。

FTD アクセス コントロール ポリシー

CDO を使用して、Firepower Threat Defense（FTD）アクセス コントロール ポリシーを管理できます。アクセス コントロール ポリシーは、アクセスコントロールルールに照らしてネットワークトラフィックを評価することで、ネットワークリソースへのアクセスを制御します。FTD は、アクセスコントロールルールの条件を、アクセス コントロール ポリシーに表示される順序で、ネットワークトラフィックと比較します。アクセスコントロールルールのすべてのトラフィック条件が次の場合の動作を以下に示します。

- [信頼（Trust）]：どのような種類のインスペクションも行わずにトラフィックを許可します。
- [許可（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。
- [ブロック（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。

アクセス コントロール ポリシーのどのルールもネットワーク トラフィックと一致しない場合、FTD はアクセスコントロールルールの下にリストされているデフォルトのアクションを実行します。

FTD アクセス コントロール ポリシーの読み込み

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、ポリシーを読み込むデバイスを選択します。

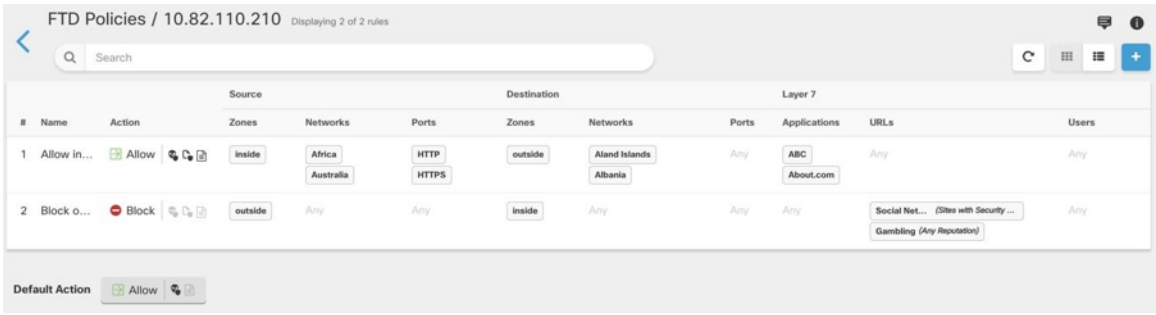
ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 5 ポリシー全体が表示されるようにするには、[フィルタ処理（Filter）] パネルで [すべて表示（Show All）] をクリックします。

ステップ 6 ルール列の表示を切り替えて、列の数を増やしたり減らしたりしてルールを表示します。Firepower Device Manager でアクセス制御ルールを確認することに慣れている場合は、ルール列の表示を切り替えて、より多くの列を表示します。

ポリシー内のルールを読み取る方法の例を次に示します。すべてのトラフィックは、最初にルール 1 に照らし合わせて一致しているかどうか評価されます。トラフィックがルール 1 に一致する場合、そのルールのアクションがトラフィックに適用されます。内部ゾーンに位置するアフリカまたはオーストラリアで HTTP または HTTPS ポートから開始されたトラフィックが、

外部ゾーンに位置するオーランド諸島またはアルバニアの任意のポートを経由して ABC または About.com に到達する場合に、送信元から宛先へのフローが許可されています。また、侵入ポリシーとファイルポリシーがルールに適用され、ルールから発生したイベントがログに記録されていることもわかります。



関連情報：

- FTD アクセス コントロール ポリシーの設定

FTD アクセス コントロール ポリシーの設定

Firepower Threat Defense（FTD）デバイスには単一のポリシーがあり、そのポリシーの一セクションにアクセス制御ルールがあります。議論を容易にするために、アクセス制御ルールを持つポリシーのセクションをアクセス コントロール ポリシーと呼びます。FTD をオンボーディングした後、アクセス コントロール ポリシーにルールを追加するか、ルールを編集します。

新しい FTD デバイスをオンボーディングしている場合、インポートされたポリシーにルールがない可能性があります。その場合、FTD ポリシーページを開くと、「結果が見つかりませんでした」というメッセージが表示されます。このメッセージが表示された場合は、FTD ポリシーへのルールの追加を開始し、CDO からデバイスにそれらのルールを展開できます。

始める前のヒント

条件をアクセス コントロール ルールに追加する場合は、次のヒントを参考にしてください。

- 条件をルールに追加するときに、一部の条件のカスタムオブジェクトを作成できます。カスタムオブジェクトを作成するためのリンクをダイアログボックスで探します。
- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールのすべての条件に一致する必要があります。たとえば、特定のホストまたはネットワークの URL フィルタリングを行う単一のルールを使用できます。
- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準のいずれかに一致するトラフィックはその条件を満たします。たとえば、最大 50 のアプリケーションまたはアプリケーション フィルタにアプリケーション制御を適用する単一のルールを使用できます。したがって、単一の条件では項目間に OR 関係がありますが、条件タイプ間（たとえば、送信元/宛先とアプリケーション間）には AND 関係があります。

- 一部の機能では、適切な Firepower ライセンスを有効にする必要があります。
- 一部の編集タスクでは、編集モードに入る必要がない場合もあります。ポリシーページでは、条件列内の [+] ボタンをクリックしてルールの条件を変更し、ポップアップ ダイアログボックスで希望するオブジェクトまたは要素を選択できます。オブジェクトまたは要素の [x] をクリックすると、そのオブジェクトまたは要素が削除されます。

FTD アクセス コントロール ポリシーの作成または編集

CDO を使用して FTD アクセス コントロール ポリシーを編集するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] 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 FTD を選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 5 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、青色のプラスボタン 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）]ペインの編集アイコン をクリックします。(単純な編集は、編集モードに移行せずにインラインで実行することも可能です。)
- 不要になったルールを削除するには、ルールを選択し、操作ウィンドウで削除アイコン 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。

ルールを編集または追加する場合は、引き続き残りの手順を実行します。

ステップ 6 [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。

ルールは最初に一致したものから順に適用されるため、限定的な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、汎用的な基準を持つルールよりも上に置く必要があります。

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 7 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：+ . _ -

ステップ 8 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。

- [信頼（Trust）]：どのような種類のインスペクションも行わずにトラフィックを許可します。
- [許可（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。
- [ブロック（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。

ステップ 9 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。

- [送信元（Source）]：[送信元（Source）]タブをクリックして、ネットワークトラフィックが発信されるセキュリティゾーン（インターフェイス）、ネットワーク（ネットワーク、大陸、カスタム地理位置情報を含む）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。
- [接続先（Destination）]：[接続先（Destination）] タブをクリックして、ネットワークトラフィックが到着するセキュリティゾーン（インターフェイス）、ネットワーク（ネットワーク、大陸、カスタム地理位置情報を含む）、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。「FTD アクセス コントロール ルールの送信元および宛先の基準」を参照してください。
- [アプリケーション（Application）]：[アプリケーション（Application）]タブをクリックして、Web アプリケーション、またはタイプ、カテゴリ、タグ、リスク、ビジネスとの関連性ごとにアプリケーションを定義するフィルタを追加または削除します。デフォルトはすべてのアプリケーションです。「FTD アクセス制御ルールの適用基準」を参照してください。
- [URL]：[URL] タブをクリックして、Web リクエストの URL や URL カテゴリを追加または削除します。デフォルトはすべての URL です。URL カテゴリとレピュテーションフィルタを使用してこの条件を微調整する方法については、「FTD アクセス制御ルールの URL 条件」を参照してください。
- [ユーザー（Users）]：Active Directory レルムオブジェクト、特別なアイデンティティ（失敗した認証、ゲスト、非認証、不明）や Firepower Device Manager からルールに追加されたユーザーグループがルール行に表示されますが、CDO ではまだ編集できません。

  注意 個々のユーザーオブジェクトは、CDO のアクセス コントロール ポリシー ルールではまだ表示されません。FDM にログインして、個々のユーザーオブジェクトがアクセス コントロール ポリシー ルールにどのように影響するかを確認します。

ステップ 10 （任意、許可アクションのあるルールの場合）侵入やエクスプロイトについてトラフィックを検査するには、[侵入ポリシー（Intrusion Policy）] タブをクリックして、侵入検査ポリシーを割り当てます。「FTD アクセスコントロールルールの侵入ポリシー設定」を参照してください。

1. 侵入ポリシールールによって生成された**侵入イベントをログに記録するには**、デバイスの「FTD の設定」を参照してください。

ステップ 11 （任意、許可アクションのあるルールの場合）[ファイルポリシー（File Policy）] タブをクリックして、マルウェアを含むファイルやブロックする必要があるファイルのトラフィックを検査するファイルポリシーを割り当てます。「FTD アクセスコントロールルールのファイルポリシーの設定」を参照してください。

1. ファイルポリシールールによって生成された**ファイルイベントをログに記録するには**、デバイスの「FTD の設定」を参照してください。

ステップ 12 （任意）[ロギング（Logging）] タブをクリックしてロギングを有効にし、アクセス制御ルールによって報告された**接続イベント**を収集します。

ロギング設定の詳細については、「FTD アクセスコントロールルールのロギング設定」を参照してください。

Cisco Security Analytics and Logging のサブスクリプションがある場合、SEC の IP アドレスとポートを使用して syslog オブジェクトを設定することで、CDO で接続イベントを設定して Secure Event Connector に送信できます。この機能の詳細については、「Cisco Security Analytics and Logging」を参照してください。テナントにオンボーディングした SEC ごとに 1 つの syslog オブジェクトを作成しますが、1 つのルールによって生成されたイベントのみを 1 つの SEC を表す 1 つの syslog オブジェクトに送信します。

ステップ 13 [保存（Save）] をクリックします。セキュリティポリシーの特定ルールの設定が完了しました。

ステップ 14 セキュリティポリシー全体の**デフォルトアクション**を設定できます。デフォルトアクションでは、ネットワークトラフィックがアクセスコントロールポリシー、侵入ポリシー、ファイル/マルウェアポリシーのどのルールにも適合しない場合の処理を定義します。

ステップ 15 ポリシーのデフォルトアクションをクリックします。

ステップ 16 上記のステップ 9 で行ったように侵入ポリシーを設定します。

ステップ 17 デフォルトアクションによって生成される接続イベントのロギングを設定します。

Cisco Security Analytics and Logging のサブスクリプションがある場合、SEC の IP アドレスとポートを使用して syslog オブジェクトを設定することで、デフォルトアクションによって生成されたイベントを Secure Event Connector（SEC）に送信できます。この機能の詳細については、「Cisco Security Analytics and Logging」を参照してください。テナントにオンボーディングした SEC ごとに 1 つの syslog オブジェクトを作成しますが、ルールによって生成されたイベントのみを 1 つの SEC を表す 1 つの syslog オブジェクトに送信します。

ステップ 18 （オプション）自分で作成したルールの場合、ルールを選択して、[コメントを追加（Add Comments）] フィールドでコメントを追加できます。ルールコメントに関する詳細については、「FTD ポリシーとルールセットのルールにコメントを追加する」を参照してください。

ステップ 19 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

アクセスポリシーの設定

ポリシー内の特定のルールではなく、アクセスポリシーを対象にした設定を行うことができます。

手順

次の設定は、ポリシー内の特定のルールではなく、アクセスポリシー全体を対象としています。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] 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 FTD を選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 5 [設定（Settings）] アイコンをクリックして、次の設定を行います。

- [TLSサーバーアイデンティティ検出]：TLS 1.3 証明書は暗号化されます。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたは URL フィルタリングを使用するアクセスルールに対応するには、システムが TLS 1.3 証明書を復号する必要があります。暗号化された接続が適切なアクセス制御ルールに適合していることを確認するために、このオプションを有効にすることを推奨します。この設定では、証明書のみが復号されます。接続は暗号化されたままになります。TLS 1.3 証明書を復号するには、このオプションを有効にするだけで十分です。対応する SSL 復号ルールを作成する必要はありません。バージョン 6.7 以降を実行している FTD デバイスで使用できます。
- [DNSトラフィックへのレピュテーション適用]：URL フィルタリングカテゴリとレピュテーションルールを DNS ルックアップ要求に適用するには、このオプションを有効にします。ルックアップ要求の完全修飾ドメイン名（FQDN）にブロックしているカテゴリやレピュテーションがある場合、システムは DNS 応答をブロックします。ユーザーは DNS 解決を受信しないため、ユーザーは接続を完了できません。非 Web トラフィックに URL カテゴリおよびレピュテーションフィルタリングを適用するには、このオプションを使用します。詳細については、「DNS 要求のフィルタリング」を参照してください。バージョン 7.0 以降を実行している FTD デバイスで使用できます。

ステップ 6 [保存（Save）] をクリックします。

TLS サーバーアイデンティティ検出について

通常、TLS 1.3 証明書は暗号化されます。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたはURL フィルタリングを使用するアクセスルールに対応するには、システムが TLS 1.3 証明書を復号する必要があります。暗号化された接続が適切なアクセス制御ルールに適合

していることを確認するために、早期アプリケーション検出と URL 分類を有効にすることを推奨します。この設定では、証明書のみが復号されます。接続は暗号化されたままになります。

（注） この機能は現在のところ、ソフトウェアバージョン 6.7 以降を実行している Firepower Threat Defense（FTD）デバイスで使用できます。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] 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 FTD を選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 5 設定ボタン をクリックします。

ステップ 6 [TLSサーバーアイデンティティ検出（TLS Server Identity Discovery）] の横にあるスライダをクリックして、暗号化された接続の早期アプリケーション検出と URL 分類を有効にします。

ステップ 7 [保存（Save）] をクリックします。

FTD アクセスコントロールルールをコピーする

アクセスコントロールルールをコピーするにはこの手順に従い、現在の位置からコピーして同じポリシー内の新しい位置に貼り付けるか、別の FTD のポリシーに貼り付けます。ルールはポリシー内の他のルールの前または後に貼り付けることができるため、ポリシー内における適切な順序でネットワークトラフィックを評価します。

FTD 内でのルールのコピー

FTD デバイス内でルールをコピーするには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、ポリシーを編集する FTD デバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 5 コピーする 1 つ以上のアクセス制御ルールを選択し、右側の [アクション（Actions）] ペインで [コピー（Copy）] をクリックします。

ステップ 6 ルールの貼り付け先のポリシーで、コピーしたルールを貼り付ける位置の上または下にあるルールを選択し、[アクション（Actions）] ペインで次のオプションのいずれかをクリックします。

- [前に貼り付け（Paste Before）]：選択したルールの上に 1 つ以上のルールを自動的に貼り付けます。これにより、コピーされたルールは、選択したルールの前に配置されます。
- [後に貼り付け（Paste After）]：選択したルールの下に 1 つ以上のルールを自動的に貼り付けます。これにより、コピーされたルールは、選択したルールの後に配置されます。

貼り付け操作は、必要な位置に複数回実行できます。

（注） ルールを FTD デバイス内に貼り付けるときに、同じ名前のルールが存在する場合、「- Copy」が元の名前に追加されます。この変更名も存在する場合は、元の名前に「- Copy n」が追加されます。たとえば、「rule name - Copy 2」になります。

ステップ 7 変更内容を確認し、「CDO から FTD への設定変更の展開」をすぐに実行するか、複数の変更を後から一度に展開します。

任意の FTD ポリシーから別の FTD ポリシーへのルールのコピー

任意の FTD ポリシーから別の FTD ポリシーにルールをコピーすると、ルールに関連付けられているオブジェクトも新しい FTD にコピーされます。

ルールを貼り付けるときに、いくつかの条件が CDO で検証されます。詳細については、「別の FTD にルールを貼り付けるときのオブジェクトの動作」を参照してください。

重要 **重要**：ソフトウェアのバージョンが両方のデバイスで同じ場合にのみ、CDO で任意の FTD から別の FTD にルールをコピーできます。ソフトウェアのバージョンが異なる場合、ルールを貼り付けようとすると、「このデバイスのバージョンと互換性がないため、ルールを貼り付けることができませんでした」というエラーが表示されます。[詳細（Details）] リンクをクリックすると、エラーの詳細が表示されます。

ルールを別の FTD デバイスにコピーするには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、ルールのコピー元のデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 5 コピーする 1 つ以上のアクセス制御ルールを選択し、右側の [アクション（Actions）] ペインで [コピー（Copy）] をクリックします。

ステップ 6 [デバイスとサービス（Devices & Services）] をクリックし、ルールを貼り付ける FTD デバイスに移動します。

ステップ 7 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 8 コピーしたルールの貼り付け先のポリシーで、貼り付ける位置の前または後にあるルールを選択し、[アクション（Actions）] ペインで [前に貼り付け（Paste Before）] または [後に貼り付け（Paste After）] をクリックします。

ステップ 9 コピーしたルールと一緒に貼り付けるアクセス制御ルールがある場合は選択し、[アクション（Actions）] ペインで次のオプションのいずれかをクリックします。

- [前に貼り付け（Paste Before）]：選択したルールの上に 1 つ以上のルールを自動的に貼り付けます。これにより、コピーされたルールは、選択したルールの前にネットワークトラフィックを評価します。
- [後に貼り付け（Paste After）]：選択したルールの下に 1 つ以上のルールを自動的に貼り付けます。これにより、コピーされたルールは、選択したルールの後にネットワークトラフィックを評価します。

貼り付け操作は、必要な位置に複数回実行できます。

（注） ルールを別の FTD デバイスに貼り付けるときに、同じ名前のルールが存在する場合、「-Copy」が元の名前に追加されます。この変更名も存在する場合は、元の名前に「-Copy n」が追加されます。たとえば、「rule name-Copy 2」になります。

ステップ 10 別の FTD にルールをコピーすると、コピー先のデバイスの [設定ステータス（Configuration Status）] は [非同期（Not Synced）] 状態になります。変更内容を確認し、「CDO から FTD への設定変更の展開」をすぐに実行するか、複数の変更を後から一度に展開します。

関連情報：

- FTD アクセスコントロールルールの移動
- 別の FTD にルールを貼り付けるときのオブジェクトの動作

FTD アクセスコントロールルールの移動

アクセスコントロールルールを移動するにはこの機能を使用し、現在の位置から切り取って同じポリシー内の新しい位置に貼り付けるか、別の FTD のポリシーに貼り付けます。ルールはポリシー内の他のルールの前または後に貼り付けることができるため、ポリシー内における適切な順序でネットワークトラフィックを評価します。

FTD 内でのルールの移動

FTD デバイス内でルールを移動するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、ポリシーを編集する FTD デバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 5 移動する 1 つ以上のアクセス制御ルールを選択し、右側の [アクション（Actions）] ペインで [切り取り（Cut）] をクリックします。選択したルールが黄色で強調表示されます。**注**：選択をキャンセルする場合は、任意のルールを選択して [コピー（Copy）] をクリックします。

ステップ 6 切り取ったルールの貼り付け先のポリシーで、貼り付ける位置の前または後にあるルールを選択し、[アクション（Actions）] ペインで次のオプションのいずれかをクリックします。

- [前に貼り付け（Paste Before）]：選択したルールの上に 1 つ以上のルールを自動的に貼り付けます。これにより、切り取ったルールは、選択したルールの前にネットワークトラフィックを評価します。
- [後に貼り付け（Paste After）]：選択したルールの下に 1 つ以上のルールを自動的に貼り付けます。これにより、切り取ったルールは、選択したルールの後にネットワークトラフィックを評価します。

貼り付け操作は、必要な位置に複数回実行できます。

（注） ルールを FTD デバイス内に貼り付けるときに、同じ名前のルールが存在する場合、「-Copy」が元の名前に追加されます。この変更名も存在する場合は、元の名前に「-Copy n」が追加されます。たとえば、「rule name - Copy 2」になります。

ステップ 7 変更内容を確認し、「CDO から FTD への設定変更の展開」をすぐに実行するか、複数の変更を後から一度に展開します。

任意の FTD ポリシーから別の FTD ポリシーへのルールの移動

任意の FTD ポリシーから別の FTD ポリシーにルールを移動すると、ルールに関連付けられているオブジェクトも新しい FTD にコピーされます。

ルールを貼り付けるときに、いくつかの条件が CDO で検証されます。これらの条件の詳細については、「別の FTD にルールを貼り付けるときのオブジェクトの動作」を参照してください。

ルールを別の FTD デバイスに移動するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、ルールのコピー元の FTD デバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 5 移動する 1 つ以上のアクセス制御ルールを選択し、右側の [アクション（Actions）] ペインで [切り取り（Cut）] をクリックします。

ステップ 6 [デバイスとサービス（Devices & Services）] をクリックし、1 つ以上のルールの移動先となる FTD デバイスに移動します。

ステップ 7 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 8 切り取ったルールの貼り付け先のポリシーで、貼り付ける位置の前または後にあるルールを選択し、[アクション（Actions）] ペインで [前に貼り付け（Paste Before）] または [後に貼り付け（Paste After）] をクリックします。

- [前に貼り付け（Paste Before）]：選択したルールの上に 1 つ以上のルールを自動的に貼り付けます。これにより、切り取ったルールは、選択したルールの前にネットワークトラフィックを評価します。
- [後に貼り付け（Paste After）]：選択したルールの下に 1 つ以上のルールを自動的に貼り付けます。これにより、切り取ったルールは、選択したルールの後にネットワークトラフィックを評価します。

貼り付け操作は、必要な位置に複数回実行できます。

（注） ルールを FTD デバイス内に貼り付けるときに、同じ名前のルールが存在する場合、「-Copy」が元の名前に追加されます。この変更名も存在する場合は、元の名前に「-Copy n」が追加されます。たとえば、「rule name - Copy 2」になります。

ステップ 9 別の FTD にルールをコピーすると、コピー元とコピー先のデバイスの [設定ステータス（Configuration Status）] は [非同期（Not Synced）] 状態になります。変更内容を確認し、「CDO から FTD への設定変更の展開」をすぐに実行するか、複数の変更を後から一度に展開します。

関連情報：

- FTD アクセスコントロールルールをコピーする
- 別の FTD にルールを貼り付けるときのオブジェクトの動作

別の FTD にルールを貼り付けるときのオブジェクトの動作

オブジェクトが含まれるルールを切り取りまたはコピーして別の FTD ポリシーに貼り付けた場合、次の条件のいずれかが満たされると、CDO はルール内のオブジェクトを貼り付け先の FTD にコピーします。

すべてのタイプのオブジェクト（セキュリティゾーンを除く）の場合

- コピー先のデバイス内にそのオブジェクトがない場合、CDO は最初にコピー先のデバイスにオブジェクトを作成してから、ルールを貼り付けます。
- コピー先のデバイスには、コピー元のデバイスと同じ名前と同じ値を持つオブジェクトが存在します。

セキュリティ ゾーン オブジェクトの場合

- コピー先のデバイスには、コピー元と同じ名前と同じインターフェイスを持つセキュリティゾーンが存在します。
- コピー先のデバイスには同じセキュリティ ゾーン オブジェクトは存在せず、コピー先で使用するためのインターフェイスがあります。
- コピー先のデバイスには空のセキュリティ ゾーン オブジェクトが存在し、コピー先で使用するためのインターフェイスがあります。

Active Directory（AD）レルムを含むオブジェクトの場合

- CDO は、同じ名前のレルムがターゲットデバイスにすでに存在する場合にのみ、Active Directory（AD）レルムオブジェクトを含むルールを貼り付けます。

重要 次の条件下では、貼り付け操作に失敗します。

- 2 つのデバイスバージョン間で脆弱性、地理位置情報、侵入、URL データベースに違いがある場合、CDO はルールをターゲットデバイスに貼り付けることができません。新しいデバイスでルールを手動で再作成する必要があります。
- 追加するルールに、「管理専用」タイプのインターフェースを含むセキュリティゾーンがある場合。

関連情報：

- FTD アクセスコントロールルールをコピーする
- FTD アクセスコントロールルールの移動

FTD アクセス コントロール ルールの送信元および宛先の基準

アクセスルールの送信元および宛先の基準によって、トラフィックが通過するセキュリティゾーン（インターフェイス）、IP アドレスや IP アドレスの国や大陸（地理的位置）、または

トラフィックで使用されるプロトコルとポートが定義されます。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。

アクセスコントロールルールの送信元または宛先の条件を変更する場合は、「FTD アクセスコントロールポリシーの設定」の手順を使用してルールを編集できます。簡単な編集は、編集モードに移行せずに実行できます。ポリシーページで、ルールを選択し、送信元または宛先条件列内で [+] ボタンをクリックし、ポップアップ ダイアログボックスで新しいオブジェクトまたは要素を選択することにより、ルールの条件を変更できます。オブジェクトまたは要素の [x] をクリックすると、そのオブジェクトまたは要素が削除されます。

次の基準を使用して、ルールに一致する送信元および宛先を特定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティ ゾーン オブジェクト。1 つの基準を定義する 、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、ホスト内部に向かうすべてのトラフィックが侵入検査を受けるようにする場合は、内部ゾーンを [送信先ゾーン（Destination Zones）] として選択し、送信元ゾーンは空白のままにします。侵入フィルタリングをルールに含めるには、ルールのアクションを [許可（Allow）] にし、ルールで侵入ポリシーを選択する必要があります。

（注） 1 つのルールにパッシブ セキュリティ ゾーンとルーテッド セキュリティ ゾーンを混在させることはできません。さらに、パッシブ セキュリティ ゾーンは送信元ゾーンとしてのみ指定でき、宛先ゾーンとして指定することはできません。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。

- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク（Network）]：制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。完全修飾ドメイン名（FQDN）を使用してアドレスを定義するオブジェクトを使用できます。このアドレスは DNS ルックアップによって判別されます。
- [地理位置情報（Geolocation）]：位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

（注） 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。TCP/UDP では、これにポートを含めることができます。ICMP では、コードとタイプを含めることができます。

- プロトコルまたはポートからのトラフィックを照合するには、[送信元ポート（Source Ports）] を設定します。送信元ポートを使用できるのは、TCP/UDP のみです。
- プロトコルまたはポートへのトラフィックを照合するには、[宛先ポート/プロトコル（Destination Ports/Protocols）] を設定します。宛先ポートだけを条件に追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。ICMP およびその他の非 TCP/UDP 仕様は、宛先ポートでのみ許可されます。送信元ポートでは許可されません。
- 特定の TCP/UDP ポートから発生し、特定の TCP/UDP ポートに向かうトラフィックを照合するには、両方設定します。送信元ポートと宛先ポートの両方を条件に追加する場合、単一のトランスポート プロトコル、TCP、または UDP を共有するポートのみを追加できます。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にできます。

FTD アクセス制御ルールの URL 条件

アクセス制御ルールの URL 条件では、Web 要求で使用される URL または要求された URL が属するカテゴリを定義します。カテゴリが一致する場合は、許可またはブロックするためのサイトの相対レピュテーションも指定できます。デフォルトでは、すべての URL が許可されます。

URL のカテゴリおよびレピュテーションにより、アクセス コントロール ルールの URL 条件をすぐに作成できます。たとえば、すべてのゲームサイトやリスクの高いすべてのソーシャル ネットワーキング サイトをブロックできます。ユーザがそのカテゴリとレピュテーションの組み合わせで URL を閲覧しようとすると、セッションがブロックされます。

カテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを期待通りに確実に制御します。最後に、脅威インテリジェンスは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して、要求された URL をフィルタします。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを展開したりするペースを上回って次々と出没する可能性があります。

アクセス制御ルールの URL や URL 条件を変更する場合は、「FTD アクセス コントロール ポリシーの設定」の手順を使用してルールを編集できます。簡単な編集は、編集モードに移行せずに実行できます。ポリシーページで、ルールを選択してから URL 条件列内で [+] ボタンをクリックし、ポップアップ ダイアログボックスで新しいオブジェクト、要素、URL レピュテーション、または URL カテゴリを選択すると、URL 条件を変更できます。オブジェクトまたは要素の [x] をクリックすると、そのオブジェクトまたは要素が削除されます。

青いプラスアイコン をクリックし、URL オブジェクト、グループ、または URL カテゴリを選択して [保存（Save）] をクリックします。必要な URL オブジェクトが存在しない場合は、[新しいオブジェクトの作成（Create New Object）] をクリックします。URL オブジェクトの詳細については、「FTD URL オブジェクトの作成と編集」を参照してください。

URL フィルタリングのライセンス要件

URL フィルタリングを使用するには、FDM で **URL フィルタリング**ライセンスを有効にする必要があります。

ルールで使用される URL カテゴリのレピュテーションの指定

デフォルトでは、URL カテゴリ内のすべての URL は、ルールに従って同じように扱われます。たとえば、ソーシャルネットワークの URL をブロックするルールがある場合、レピュテーションに関係なくすべてをブロックします。この設定を調整して、リスクの高いソーシャル ネットワークサイトのみをブロックできます。同様に、ある URL カテゴリにおいては、リスクの高いサイトを除くすべての URL を許可することができます。

アクセス制御ルールの URL カテゴリでレピュテーションフィルタを使用するには、次の手順を実行します。

手順

ステップ 1 [FTDポリシー（FTD Policy）] ページで、編集するルールを選択します。

ステップ 2 [編集（Edit）] をクリックします。

ステップ 3 [URLs] タブをクリックします。

ステップ 4 青色のプラスボタン をクリックし、URL カテゴリを選択します。

ステップ 5 [選択したカテゴリにすべてのレピュテーションを適用（Apply Reputation to Selected Categories）] または選択した URL カテゴリの [任意のレピュテーション（Any Reputation）] リンクをクリックします。

ステップ 6 [任意のレピュテーション（Any Reputation）] チェックボックスをオフにします。

ステップ 7 レピュテーションで URL をフィルタ処理します。

- ルールにブロックアクションがある場合は、レピュテーションスライダを右にスライドすると、レピュテーションが赤でマークされているサイトのみがブロックされます。たとえば、スライダを [セキュリティリスクのあるサイト（Sites with Security Risks）] にスライドすると、ブロックルールは「セキュリティリスクのあるサイト」、「疑わしいサイト」、および「リスクの高いサイト」をブロックしますが、「よく知られたサイト」と「無害のサイト」からのトラフィックは許可します。
- ルールに許可アクションがある場合は、レピュテーションスライダを右にスライドすると、レピュテーションが緑でマークされているサイトのみが許可されます。たとえば、スライダを [無害のサイト] にスライドすると、ルールは「既知のサイト」と「無害のサイト」からのトラフィックを許可しますが、「セキュリティリスクのあるサイト」、「疑わしいサイト」、および「リスクの高いサイト」からのトラフィックは許可しません。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 [選択（Select）] をクリックします。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

FTD アクセスコントロールルールの侵入ポリシー設定

Firepower システムには複数の侵入ポリシーが付属しています。これらのポリシーは、侵入ルールとプリプロセッサ ルールの状態を設定し、詳細設定を構成する Cisco Talos Security Intelligence and Research Group によって設計されています。

侵入ポリシーのためのライセンスおよび操作の要件

- **ライセンス** ：侵入ポリシーをルールに追加するには、Firepower Device Manager で次の脅威ライセンスを有効にする必要があります。
- **ルールアクション**：トラフィックのみを**許可**するルールに基づいて侵入ポリシーを設定できます。トラフィックを [信頼（trust）] または [ブロック（block）] するように設定されたルールではインスペクションは実行されません。さらに、アクセス コントロール ポリシーのデフォルトのアクションが [許可（allow）] の場合は、侵入ポリシーを設定できますが、ファイル ポリシーは設定できません。

アクセスコントロールルールに使用可能な侵入ポリシー

トラフィックを許可するアクセス コントロール ルールでは、次の侵入ポリシーのいずれかを選択して、トラフィックの侵入やエクスプロイトのインスペクションを実行できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。

ポリシーは、安全性の低いものから高いものへの順で表示されています。

- [セキュリティよりも接続性を優先（Connectivity over Security）]：このポリシーは、ネットワーク インフラストラクチャのセキュリティよりも接続性（すべてのリソースにアクセスできること）が優先される組織のために作成されています。この侵入ポリシーは、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールのみが有効にされます。このポリシーは、侵入からの保護を適用する必要があるが、ネットワークのセキュリティにかなり自信がある場合に選択します。
- [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）]：このポリシーは、全体的なネットワーク パフォーマンスとネットワーク インフラストラクチャのセキュリティのバランスを取るように設計されています。このポリシーは大部分のネットワークに適しています。このポリシーは、侵入防御を適用したい大部分の状況で選択できます。
- [接続性よりもセキュリティを優先（Security over Connectivity）]：このポリシーは、ユーザーの利便性よりもネットワーク インフラストラクチャのセキュリティが優先される組織のために作成されています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。このポリシーは、セキュリティが特に重要であるか、トラフィックのリスクが高い場合に選択します。
- [最大検出（Maximum Detection）]：このポリシーは、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシーよりもさらに、ネットワーク インフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイト キット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。このポリシーを選択する場合、正当なトラフィックが過剰にドロップされていないか慎重に評価してください。

関連情報

- FTD アクセス コントロール ポリシーでの侵入、ファイル、およびマルウェアの検査

FTD アクセスコントロールルールのファイルポリシーの設定

Advanced Malware Protection for Firepower（AMP for Firepower）を使用して悪意のあるソフトウェア、つまり、マルウェアを検出するファイル ポリシーを使用します。ファイル制御を実行するファイル ポリシーを使用して、ファイルにマルウェアが含まれているかどうかに関係なく、特定のタイプのすべてのファイルを制御することもできます。

AMP for Firepower は、ネットワーク トラフィックで検出された潜在的なマルウェアの性質を取得し、ローカルマルウェア ファイル分析と事前分類の更新を取得するために AMP クラウドを使用します。AMP クラウドにアクセスし、マルウェア ルックアップを実行するため、管理インターフェイスにはインターネットへのパスが必要です。デバイスが対象ファイルを検出すると、ファイルの SHA-256 ハッシュ値を使用してファイルの性質について AMP クラウドに問い合わせます。可能な性質を次に示します。

- マルウェア（Malware）：AMP クラウドはファイルをマルウェア クラウドとして分類しました。ファイル内のいずれかのファイルがマルウェアである場合、アーカイブ ファイル（たとえば zip ファイル）はマルウェアとしてマークされます。
- クリーン（Clean）：AMP クラウドはファイルをマルウェアが含まれないクリーンな状態であると分類しました。その中のすべてのファイルがクリーンであれば、アーカイブ ファイルはクリーンであるとマークされます。
- 不明（Unknown）：AMP クラウドがまだファイルの性質を指定していません。その中のすべてのファイルが不明であれば、アーカイブ ファイルは不明であるとマークされます。
- 利用不可（Unavailable）：システムは、ファイルの性質を判断するために AMP クラウドに問い合わせできませんでした。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。複数の「利用不可」イベントが連続して発生している場合、管理アドレスのインターネット接続が正常に機能していることを確認します。

ファイルポリシーのライセンスおよび操作の要件

ライセンス：ファイルポリシーをルールに追加するには、Firepower Device Manager で次の 2 つのライセンスを有効にする必要があります。

- 脅威ライセンス
- マルウェアライセンス

ルールアクション：トラフィックのみを許可するルールに基づいてファイルポリシーを設定できます。トラフィックを [信頼（trust）] または [ブロック（block）] するように設定されたルールではインスペクションは実行されません。さらに、アクセス コントロール ポリシーのデフォルトのアクションが [許可（allow）] の場合は、侵入ポリシーを設定できますが、ファイル ポリシーは設定できません。

アクセスコントロールルールに使用可能なファイルポリシー

- [なし（None）] は、送信したファイルでマルウェアの評価を行わず、特定のファイルをブロックしません。このオプションは、ファイル送信が信頼されている、またはファイル送信の可能性が低い（または不可能である）、あるいはアプリケーションを信頼している、または URL フィルタリングがネットワークを適切に保護しているルールに対して選択します。

- [マルウェアをすべてブロック（Block Malware All）] は、AMPクラウドに問い合わせてネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。
- [クラウドをすべてルックアップ（Cloud Lookup All）] は、AMPクラウドに問い合わせてネットワークを通過するファイルの傾向を取得して記録したうえでその伝送を許可します。
- [オフラインドキュメントとアップロードされたPDFをブロック、その他のマルウェアをブロック（Block Office Document and PDF Upload, Block Malware Others）] は、ユーザーによる Microsoft Office のドキュメントと PDF のアップロードをブロックします。AMPクラウドに問い合わせてネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。
- [オフラインドキュメントのアップロードをブロック、その他のマルウェアをブロック（Block Office Documents Upload, Block Malware Others）] は、ユーザーによる Microsoft Office のドキュメントのアップロードをブロックします。AMPクラウドに問い合わせてネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。

関連情報：

- FTD アクセスコントロールルールの侵入ポリシー設定

FTD アクセスコントロールルールのロギング設定

アクセス制御ルールのロギング設定

アクセスルールのロギング設定は、接続イベントがルールに一致するトラフィックに対して発行されるかどうかを決定します。

組織のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。生成するイベントの数を抑え、パフォーマンスを向上させることが目標である場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワーク トラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。

⚠

注意 サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイスを対象としているかどうかを検討します。

手順

手順

ステップ 1 FTD アクセス コントロール ポリシーの設定、[ロギング（Logging）] タブをクリックします。

ステップ 2 ログアクションを指定します。

- [接続の開始時と終了時にログを記録する（Log at Beginning and End of Connection）]：接続の開始時と終了時にイベントを発行します。接続終了イベントには接続開始イベントに含まれるすべての情報と、接続中に拾うことができるすべての情報が含まれているため、許可しようとしているトラフィックではこのオプションを選択しないことをお勧めします。両方のイベントのロギングは、システム パフォーマンスに影響する可能性があります。ただし、これはブロックされているトラフィックに許可されている唯一のオプションです。
- [接続終了時にログを記録する（Log at End of Connection）]：接続の終了時に接続ログの記録を許可する場合は、このオプションを選択します。これは許可されている、または信頼されているトラフィックに推奨されます。
- [ロギングなし（Log None）]：ルールのロギングを無効にするには、このオプションを選択します。これがデフォルトです。

（注） アクセス制御ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を自動的にロギングします。侵入がブロックされた接続では、接続ログ内の接続のアクションは [ブロック（Block）]、理由は [侵入ブロック（Intrusion Block）] ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。

ステップ 3 接続イベントの送信先を指定します。

外部 syslog サーバーにイベントのコピーを送信するには、syslog サーバーを定義するサーバーオブジェクトを選択します。必要なオブジェクトがまだ存在しない場合は、作成する必要があります。詳細については、「Syslog サーバーオブジェクトの作成および編集」を参照してください。

デバイスのイベントストレージは限られているため、外部syslogサーバーにイベントを送信すると、長期的な保存が可能になり、イベント分析が強化されます。

シスコのセキュリティ分析とロギングに登録している場合：

- Secure Event Connector（SEC）を介して Cisco Cloud にイベントを送信する場合は、syslog サーバーとして SEC を指定します。これらのイベントは、ファイルポリシーとマルウェアポリシーの接続イベントとともに表示されます。
- SEC を介さずに Cisco Cloud に直接イベントを送信する場合は、イベントを記録するタイミング （接続の開始時または終了時）を指定しますが、SEC を syslog サーバーとして 指定しないでください。

ステップ 4 ファイル イベント

禁止されたファイルまたはマルウェアイベントのロギングを有効にするには、[ファイルのロギング（Log Files）] のチェックボックスをオンにします。このオプションを設定するには、ルールでファイル ポリシーを選択する必要があります。ルールにファイル ポリシーを選択している場合、このオプションはデフォルトで有効になっています。このオプションを有効のままにすることを推奨します。

システムは、禁止されたファイルを検出すると、次のタイプのイベントのいずれか1つをFDM内部バッファに自動的にロギングします。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します。
- マルウェア イベント：検出されたまたはブロックされたマルウェア ファイルのみを表します。
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます。

ファイルがブロックされた接続では、接続ログ内の接続のアクションは [ブロック（Block）] ですが、ファイルおよびマルウェアのインスペクションを実行するには、許可ルールを使用する必要があります。接続の原因は、[ファイルモニター（File Monitor）]（ファイルタイプまたはマルウェアが検出された）、[マルウェアブロック（Malware Block）]、[ファイルブロック（File Block）]（ファイルがブロックされた）のいずれかです。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

FTD セキュリティグループタグ

セキュリティグループタグについて

Cisco TrustSec ネットワークでトラフィックを分類するために Cisco Identity Services Engine（ISE）を使用して**セキュリティグループタグ**（SGT）を定義して使用する場合は、一致基準として SGT を使用するアクセス制御ルールを作成できます。これにより、IP アドレスではなく、セキュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することができます。

ISE で SGT を作成し、各タグにホストまたはネットワークの IP アドレスを割り当てることができます。ユーザー アカウントに SGT を割り当てた場合、SGT はユーザーのトラフィックに割り当てられます。ISE サーバーに接続するように FTD を構成して SGT をした後、CDO で SGT グループを作成し、それらに関するアクセスコントロールルールを構築できます。SGT を FTD デバイスに関連付ける前に、ISE の SGT 交換プロトコル（SXP）マッピングを構成する必要があることに注意してください。詳細は、現在実行しているバージョンの『Cisco Identity

Services Engine 管理者ガイド』の「**セキュリティグループタグ交換プロトコル**」を参照してください。

FTD は、アクセス制御ルールのトラフィック一致基準として SGT を評価するときに、次の優先順位を使用します。

1. パケット内で定義されている送信元SGT（存在する場合）。宛先の照合は、この手法では行われません。SGTがパケットに含まれるようにするには、ネットワーク内のスイッチとルータがそれらを追加するように設定されている必要があります。このメソッドの実装方法については、ISE のマニュアルを参照してください。
2. ISEセッションディレクトリからダウンロードされるユーザーセッションに割り当てられた SGT。この種の SGT 照合では、セッションディレクトリ情報をリッスンするオプションを有効にする必要がありますが、このオプションは最初に ISE アイデンティティソースを作成するときにデフォルトでオンになっています。SGTは、送信元または宛先と照合することができます。必須ではありませんが、通常は ISE アイデンティティソースを AD レルムとともに使用してパッシブ認証アイデンティティルールを設定し、ユーザ ID 情報を収集します。
3. SXP を使用してダウンロードされた SGT-to-IP アドレス マッピング。IP アドレスが SGT の範囲内にある場合、トラフィックはSGTを使用するアクセス制御ルールと一致します。SGT は、送信元または宛先と照合することができます。

（注） ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりにウンロードした SGT 情報を参照する SGT グループを作成する必要があります。SGT グルは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションづいてポリシーを適用できます。

バージョン サポート

CDO は現在、バージョン 6.5 以降を実行している FTD で SGT および SGT グループをサポートしています。FDM では、バージョン 6.5 以降で ISE サーバを構成して接続できますが、バージョン 6.7 までは FDM UI からの SGT 構成をサポートしていません。

これは、バージョン 6.5 以降を実行している FTD は SGT の SXP マッピングをダウンロードできますが、オブジェクトまたはアクセスコントロールルールに手動で追加できないことを意味します。バージョン 6.5 またはバージョン 6.6 を実行しているデバイスの SGT に変更を加えるには、ISE UI を使用する必要があります。ただし、バージョン 6.5 を実行しているデバイスが CDO にオンボーディングされている場合は、デバイスに関連付けられている現在の SGT を表示し、SGT グループを作成できます。

CDO の SGT

セキュリティグループタグ

SGT は、CDO では読み取り専用です。CDO で SGT を作成または編集することはできません。SGT を作成するには、現在実行しているバージョンの『Cisco Identity Services Engine 管理者ガイド』を参照してください。https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

SGT グループ

（注） FDM では、SGT のグループを SGT 動的オブジェクトと呼びます。CDO では、これらのタグのリストは現在 SGT グループと呼ばれています。FDM または ISE UI を参照せずに、CDO で SGT グループを作成できます。

SGT グループを使用して、ISE によって割り当てられた SGT に基づいて送信元または宛先アドレスを識別します。その後、トラフィックの一致基準を定義するためにアクセス制御ルールでオブジェクトを使用できます。ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりに、ダウンロードした SGT 情報を参照する SGT グループを作成する必要があります。

SGT グループは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションに基づいてポリシーを適用できます。

CDO で SGT グループを作成するには、少なくとも 1 つの構成済み SGT と、使用するデバイスの FDM コンソール用に構成された ISE サーバーからの SGT マッピングが必要です。複数の FTD が同じ ISE サーバに関連付けられている場合、SGT または SGT グループを複数のデバイスに適用できます。デバイスが ISE サーバに関連付けられていない場合、アクセスコントロールルールに SGT オブジェクトを含めたり、そのデバイス構成に SGT グループを適用したりすることはできません。

ルール内の SGT グループ

SGT グループをアクセスコントロールルールに追加できます。それらは、送信元または宛先のネットワークオブジェクトとして表示されます。ネットワークがルールでどのように機能するかの詳細は、『FTD アクセス コントロール ルールの送信元および宛先の基準』を参照してください。

[オブジェクト（Objects）] ページから SGT グループを作成できます。詳細については、FTD SGT グループの作成を参照してください。

FTD SGT グループの作成

アクセス制御ルールに使用できる SGT グループを作成するには、次の手順を実行します。

始める前に

セキュリティグループタグ（SGT）グループを作成する前に、次の構成または環境を設定しておく必要があります。

- FTD デバイスは、少なくともバージョン 6.5 を実行している必要があります。
- SXP マッピングを登録して変更を展開できるように ISE アイデンティティソースを設定する必要があります。SXP マッピングの管理については、使用しているバージョン（バージョン 6.7 以降）用の『Firepower Device Manager Configuration Guide』[英語] の「**Configure Security Groups and SXP Publishing in ISE**」を参照してください。
- すべての SGT は ISE で作成する必要があります。SGT の作成については、現在実行しているバージョンの『Cisco Identity Services Engine コンフィギュレーション ガイド』を参照してください。

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 [FTD] > [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（Object Name）] を入力します。

ステップ 5 （任意）説明を追加します。

ステップ 6 [SGT] をクリックし、ドロップダウンメニューを使用して、グループに含めるすべての SGT のチェックボックスをオンにします。SGT 名順にリストをソートできます。

ステップ 7 [保存（Save）] をクリックします。

（注） CDO で SGT を作成したり編集したりすることはできません。SGT グループへの追加やグループからの削除のみを実行できます。SGT を作成または編集するには、現在実行しているバージョンの『Cisco Identity Services Engine Configuration Guide』を参照してください。

FTD SGT グループの編集

SGT グループを編集するには、次の手順を使用します。

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 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 SGT グループを見つけます。

ステップ 3 SGT グループを選択し、[操作（Actions）] ウィンドウで編集アイコン  をクリックします。

ステップ 4 SGT グループを変更します。グループに関連付けられた名前、説明、または SGT を編集します。

ステップ 5 [保存（Save）] をクリックします。

（注） CDO で SGT を作成したり編集したりすることはできません。SGT グループへの追加やグループからの削除のみを実行できます。SGT を作成または編集するには、現在実行しているバージョンの『Cisco Identity Services Engine Configuration Guide』を参照してください。

FTD SGT グループのアクセス制御ルールへの追加

SGT グループをアクセス制御ルールに追加するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、SGT グループを追加するデバイスを選択します。

ステップ 4 [管理（Management）] ペインで、 [ポリシー（Policy）] を選択します。

ステップ 5 [送信元（Source）] オブジェクトまたは [宛先（Destination）] オブジェクトの青いプラスボタン  をクリックし、[SGTグループ（SGT Groups）] を選択します。

ステップ 6 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 SGT グループを見つけます。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 すべてのデバイスの設定変更のプレビューと展開。

（注） 追加のSGTグループを作成する必要がある場合は、[新しいオブジェクトを作成（Create New Object）] をクリックします。「FTD SGT グループの作成」に記載されている必須情報を入力し、SGT グループをルールに**追加**します。

FTD アクセス制御ルールの適用基準

アクセス ルールのアプリケーション基準では、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタが規定されます。デフォルトは任意のアプリケーションです。

ルールで個別のアプリケーションを指定できますが、アプリケーション フィルタを使用すれば、ポリシーの作成と管理が簡単になります。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックする、アクセス コントロール ルールを作

成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションがブロックされます。

また、シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーションディテクタを更新し追加します。そのため、ルールを手動で更新せずに、高リスクアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

アプリケーションとフィルタをルールで直接指定することも、これらの特性を定義するアプリケーションフィルタ オブジェクトを作成することもできます。指示は同じですが、複雑なルールを作成する場合、オブジェクトを使用した方が 基準当たり 50 項目のシステム上限範囲を超えにくくなります。アプリケーション フィルタ オブジェクトの作成の詳細については、「Firepower アプリケーション フィルタ オブジェクトの作成と編集」を参照してください。

ルールで使用されるアプリケーションやアプリケーションフィルタを変更するには、「FTD アクセス コントロール ポリシー」の手順に従ってルールを編集します。簡単な編集は、編集モードに移行せずに実行できます。ポリシーページでルールのアプリケーション条件を変更するには、ルールを選択してアプリケーション条件列内で [+] ボタンをクリックし、ポップアップ ダイアログボックスで新しいオブジェクトや要素を選択します。オブジェクトまたは要素の [x] をクリックすると、そのオブジェクトまたは要素が削除されます。

FTD アクセス コントロール ポリシーでの侵入、ファイル、およびマルウェアの検査

侵入ポリシーとファイル ポリシーは、トラフィックが宛先に対して許可される前の最後のとりでとして連携して動作します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。
- ファイル ポリシーは、システムのファイル コントロールと AMP for Firepower の機能を制御します。

他のトラフィック処理はすべて、侵入、禁止されたファイル、およびマルウェアについて、ネットワーク トラフィックが調べられる前に実行されます。侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシー（またはその両方）を使ってトラフィックのインスペクションを実行するよう、システムに指示できます。

トラフィックを [許可（allow）] するのみの侵入ポリシーおよびファイル ポリシーを設定できます。トラフィックを [信頼（trust）] または [ブロック（block）] するように設定されたルールではインスペクションは実行されません。さらに、アクセス コントロール ポリシーのデフォルトのアクションが [許可（allow）] の場合は、侵入ポリシーを設定できますが、ファイル ポリシーは設定できません。

アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイル ポリシーによってブロックされたファイルを検査しません。ファイル インスペクション内では、タイプによる単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。ファイルがセッションで検出されてブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

（注） デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイルインスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。暗号化されていないトラフィックのみのインスペクションが実行されます。

関連情報：

- FTD アクセスコントロールルールの侵入ポリシー設定
- FTD アクセスコントロールルールのファイルポリシーの設定

FTD アクセス制御ルールのカスタム IPS ポリシーの設定

同じカスタム IPS ポリシーの複数のインスタンスを 1 つのデバイスに関連付けることはできません。

（注） IPS ポリシーをアクセス制御ルールに関連付けるということは、通過するトラフィックがディープパケットインスペクションに送信されることを意味します。IPS ポリシーが設定されたアクセス制御ルールで唯一サポートされているルールアクションは、**許可**です。

カスタム IPS ポリシーを FTD デバイスに関連付けるには、次の手順を実行します。

手順

ステップ 1 カスタム IPS ポリシーを作成します。詳細については、「Firepower カスタム IPS ポリシーの設定」を参照してください。

ステップ 2 CDO ナビゲーションウィンドウで、[ポリシー（Policies）] を選択します。[FTD/Meraki/AWS ポリシー（FTD/Meraki/AWS Policies）] をクリックします。

ステップ 3 FTD ポリシーのリストをスクロールまたはフィルタ処理して、カスタム IPS ポリシーに関連付けるポリシーを選択します。

ステップ 4 青色のプラスボタン  をクリックします。

ステップ 5 [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。

ステップ 6 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：+ . _ -

ステップ 7 [侵入ポリシー（Intrusion Policy）] タブを選択します。ドロップダウンメニューを展開して、使用可能なすべての侵入ポリシーを表示し、目的のカスタム IPS ポリシーを選択します。

ステップ 8 残りのタブ（[送信元/宛先（Source/Destination）]、[URL]、[アプリケーション（Applications）]、[ファイルポリシー（File Policy）]）の属性を任意に組み合わせて、トラフィックの一致基準を定義します。

ステップ 9 （任意）[ロギング（Logging）] タブをクリックしてロギングを有効にし、アクセス制御ルールによって報告された**接続イベント**を収集します。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Firepower Threat Defense の TLS サーバーアイデンティティ検出

FTD 独自の TLS サーバーアイデンティティ検出機能を使用して、改善された URL のフィルタ処理とトラフィックのアプリケーション制御を実行し、ネットワーク環境における制御と精度を高めることが可能になりました。この機能が動作するためにトラフィックを復号化する必要はありません。

（注） サーバーアイデンティティ検出機能は、バージョン 6.7 以降でのみサポートされています。

TLS サーバーアイデンティティ検出の有効化

FTD アクセス コントロール ポリシーの TLS サーバーアイデンティティ検出機能を有効または無効にするには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、デバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 5 テーブルの右上隅にあるアクセスポリシー設定の歯車アイコン をクリックします。

ステップ 6 トグルをスライドして、TLS サーバーアイデンティティ検出機能を有効にします。

ステップ 7 [保存（Save）] をクリックします。

侵入防御システム

Cisco Talos Intelligence Group（Talos）は、脅威をリアルタイムで検出して関連付けし、数十億のファイルのレピュテーション傾向を維持管理します。Cisco IOS 侵入防御システム（IPS）は、ネットワークへの攻撃を軽減するインラインのディープ パケット インスペクション機能

です。Talos から取得した脅威インテリジェンスデータを使用して、悪意のあるトラフィックをリアルタイムで正確に識別、分類、およびドロップします。

Cisco Defense Orchestrator（CDO）は、ソフトウェアバージョン 6.4.xx から 6.6.0.x および 6.6.1.x を実行する Firepower Threat Defense（FTD）デバイスで IPS 機能をアクティブ化して調整する機能を提供します。CDO は現在、FTD 6.7 での IPS ルールの調整をサポートしていません。

CDO メニューバーで、[ポリシー（Policies）] > [署名のオーバーライド（Signature Overrides）] に移動して、次のタスクを実行します。

- 複数のデバイスにわたるオーバーライドの不整合を解決します。
- 脅威イベントを表示および非表示にします。
- ルール アクションを変更して、脅威イベントの処理方法をオーバーライドします。

関連情報：

- Firepower 侵入ポリシーの署名のオーバーライド
- 脅威イベント
- 侵入防御システムのトラブルシュート

脅威イベント

脅威イベントレポートは、Cisco Talos の侵入ポリシーの 1 つに一致した後にドロップされたか、アラートを生成したトラフィックのレポートです。ほとんどの場合、IPS ルールを調整する必要はありません。必要に応じて、CDO の一致ルールアクションを変更して、イベントの処理方法をオーバーライドするオプションが用意されています。

[脅威（Threats）] ページの次の動作に注意してください。

- 表示される脅威イベントはライブではありません。デバイスは、追加の脅威イベントについて 1 時間ごとにポーリングされます。
- ライブビューまたは履歴ビューに含まれていない脅威イベントは、Cisco Security Analytics and Logging の一部ではありません。ライブイベントを表示する
- 非表示にした脅威イベントを表示するには、フィルタアイコンをクリックし、[非表示を表示（View Hidden）] オプションをオンにします。
- Cisco Security Analytics and Logging のサブスクライバである場合、脅威イベントテーブルに表示されるイベントには、Secure Event Connector に送信されたイベントは含まれません。

手順

ステップ 1 ナビゲーションウィンドウから、**[モニタリング（Monitoring）] > [脅威（Threats）]** を選択します。表示されるイベントをフィルタリングし、送信元IPアドレスで検索できます。オブジェクトフィルタ

ステップ 2 脅威イベントをクリックして、右側の詳細パネルを展開します。

a) ルールの詳細については、[ルールの詳細（Rule Details）] セクションで [ルールドキュメント（Rule Document）] の URL をクリックしてください。

b) このイベントを非表示にするには、[イベントを非表示（Hide Events）] のトグルスイッチをオンにします。イベント処理はそのまま続行されますが、[非表示を表示（View Hidden）] をクリックするか、このイベントの非表示を解除しない限り、ここには表示されません。

c) ルールのオーバーライドを編集するには、[ルールの調整（Tune Rule）] をクリックします。CDO でルールアクションを変更すると、事前定義されたすべてのポリシーにオーバーライドが適用されます。この点は、各ルールがポリシーごとに異なる可能性がある FDM とは異なります。

（注） Cisco Defense Orchestrator（CDO）は、ソフトウェアバージョン 6.4.xx から 6.6.0.x および 6.6.1.x を実行する Firepower Threat Defense（FTD）デバイスでルールを調整する機能を提供します。CDO は現在、FTD 6.7 でのルールの調整をサポートしていません。

- [すべてのデバイスをオーバーライド（Override All devices）] プルダウンで、アクションを選択して [保存（Save）] をクリックします。
  - [ドロップ（Drop）]：選択すると、このルールがトラフィックと一致するとイベントが作成され、接続がドロップされます。このアクションを使用して、特定のルールのセキュリティを強化します。たとえば、[ドロップ（Drop）] を指定すると、アクセスコントロールルールに「セキュリティよりも接続性を優先（Connectivity over Security）」ポリシーが指定されている場合でも、Talos ルールに一致するとセキュリティが厳しくなります。
  - [アラート（Alert）]：選択すると、このルールがトラフィックと一致するとイベントは作成されますが、接続はドロップされません。[アラート（Alert）] のユースケースは、トラフィックがブロックされているが、お客様がトラフィックを許可し、ルールを無効にする前にアラートを確認したい場合です。
  - [無効（Disabled）]：選択すると、トラフィックがルールに一致しないようになります。イベントは生成されません。[無効（Disabled）] のユースケースは、レポートの誤検出を停止するか、httpd を使用しない場合に Apache httpd ルールを無効にするなど、使用環境に当てはまらないルールを削除することです。
  - [デフォルト（Default）]：選択すると、リストされている侵入ポリシーに対して、Talos によって割り当てられたデフォルトアクションにルールを戻します。侵入ルールを [デフォルト（Default）] に戻すことは、アクションを「セキュリティよりも接続性を優先（Connectivity over Security）」ポリシーの [アラート（Alert）] と「バランスのと

れたセキュリティと接続性（Balanced Security and Connectivity」ポリシーの [ブロック（Block）] に戻すことを意味する場合があります。

- デバイスごとにルールのオーバーライドを編集するには、[詳細オプション（Advanced Options）] スライダをオンにします。このセクションには、各デバイスに設定されたルールアクションが表示されます。アクションは、影響を受けるデバイスをチェックし、オーバーライドアクションを選択して [保存（Save）] をクリックすることで変更できます。
- [影響を受けるデバイス（Affected Devices）] は、送信元デバイスを示していません。代わりに、イベントを報告している FTD デバイスが表示されます。

（注）
- 更新（ ）ボタンをクリックして、現在の検索フィルタに基づいて脅威を表示するテーブルを更新します。
- エクスポート（ ）ボタンをクリックして、脅威の現在の概要をコンマ区切り値（.csv）ファイルにダウンロードします。Microsoft Excel などのスプレッドシートアプリケーションで .csv ファイルを開いて、リストの項目を並べ替えたり、フィルタ処理したりできます。CDO は、時間、送信元、デバイスなどの追加情報を除き、基本的な脅威の詳細をファイルにエクスポートします。

ステップ 3 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Firepower 侵入ポリシーの署名のオーバーライド

ほとんどの場合、IPS ルールを調整する必要はありません。必要に応じて、CDO の一致ルールアクションを変更して、イベントの処理方法をオーバーライドするオプションが用意されています。CDO には、オーバーライドの問題を解決するオプションがあります。

署名オーバーライドの管理

手順

ステップ 1 メインナビゲーションバーから、[ポリシー（Policies）] > [署名のオーバーライド（Signature Overrides）] をクリックします。表示するデバイスとポリシー オーバーライドポリシーはフィルタ処理できます。名前または侵入ルール SID で侵入ポリシーを検索することもできます。

ステップ 2 ポリシーオーバーライドのポリシー名をクリックして、右側に詳細パネルを展開します。

ステップ 3 [問題（Issues）] ペインの バッジは、デバイス間でオーバーライドの整合性がないことを示しています。次のように、[不整合（INCONSISTENT）] フィールドでは、影響を受けるデバイスの数を確認できます。 INCONSISTENT 2 Resolve | Ignore

a) **問題を無視するには**、[無視（Ignore）] をクリックします。問題の状況に変化はありませんが、[問題（Issues）] 列からインジケーターバッジが削除されます。

b) **問題を解決するには**、[解決（Resolve）] をクリックします。左側のパネルで、比較するポリシーを選択し、整合性のあるオーバーライドと整合性のないオーバーライドを表示します。

- ポリシーをマージするには、次の手順を実行します。
  1. [マージして解決（Resolve by Merging）] をクリックして 1 つのポリシーに結合し、そのすべてのデバイスで同じオーバーライドを使用します。
  2. [確認（Confirm）] をクリックします。
- ポリシーの名前を変更するには、次の手順を実行します。
  1. ポリシーのセクションで、[名前の変更（Rename）] をクリックして、別の名前を付けます。
  2. [確認（Confirm）] をクリックします。
- ポリシーを無視するには、次の手順を実行します。
  1. ポリシーのセクションで、[無視（Ignore）] をクリックします。
  2. [確認（Confirm）] をクリックします。
- すべての不整合を無視するには、[すべて無視（Ignore All）] をクリックします。

ステップ 4 Firepower Device Manager（FDM）を使用してデバイス上で変更された個別の Talos 侵入ルールがある場合は、[オーバーライド（Overrides）] ペインに表示されます。侵入ルールのオーバーライドアクションを変更するには、[調整（Tune）] リンクをクリックしてオーバーライドアクションを選択します。このアクションは、使用されているすべての Talos 侵入ポリシーのルールに適用されます。デフォルトのアクションルール（[デフォルト（Default）) の復元を選択した場合、環境によっては侵入ルールがトリガーされるまで、再度調整することはできません。

- セキュリティよりも接続性を優先
- バランスのとれたセキュリティと接続性
- 接続性よりもセキュリティを優先
- 最大検出

デバイス間の一貫性を保つために、オーバーライドアクションは、侵入オーバーライドポリシーに関連付けられているすべてのデバイスに保存されます。

オーバーライドアクションの効果は次のとおりです。

- [ドロップ（Drop）]：選択すると、このルールがトラフィックと一致するとイベントが作成され、接続がドロップされます。このアクションを使用して、特定のルールのセキュリティを強化します。たとえば、[ドロップ（Drop）] を指定すると、アクセスコントロールルールに「セキュリティよりも接続性を優先（Connectivity over Security）」ポリシーが指定されている場合でも、Talos ルールに一致するとセキュリティが厳しくなります。

- [アラート（Alert）]：選択すると、このルールがトラフィックと一致するとイベントは作成されますが、接続はドロップされません。[アラート（Alert）]のユースケースは、トラフィックがブロックされているが、お客様がトラフィックを許可し、ルールを無効にする前にアラートを確認したい場合です。
- [無効（Disabled）]：選択すると、トラフィックがルールに一致しないようになります。イベントは生成されません。[無効（Disabled）]のユースケースは、レポートの誤検出を停止するか、httpd を使用しない場合に Apache httpd ルールを無効にするなど、使用環境に当てはまらないルールを削除することです。
- [デフォルト（Default）]：ルールのデフォルトアクションが Talos 侵入ポリシーのレベルで異なる場合にのみ適用されます。たとえば、侵入ルールを[デフォルト（Default）]に戻すことは、アクションを「セキュリティよりも接続性を優先（Connectivity over Security）」ポリシーの [アラート（Alert）] と「バランスのとれたセキュリティと接続性（Balanced Security and Connectivity」ポリシーの [ブロック（Block）] に戻すことを意味する場合があります。
- 次のオプションを使用してルールのオーバーライドを編集します。
  - [すべてのデバイスのオーバーライド（Override for all devices）]：このオプションを選択すると、CDO によって管理されるすべてのデバイスに必要なアクションが設定されます。オプションはドロップダウンメニューから選択します。侵入オーバーライドポリシーごとに、ルールのオーバーライド値が異なる場合、ドロップダウンオプションはデフォルトで [複数（Multiple）] になります。
  - **デバイスごとにルールのオーバーライドを編集する**：[詳細オプション（Advanced Options）] スライダをオンにして、[デバイスごとのオーバーライド（Overrides by Devices）] タブを選択します。このオプションには、各デバイスに設定されたルールアクションが表示されます。アクションを変更するには、対象デバイスのチェックボックスをオンにし、オーバーライドアクションを選択して [保存（Save）] をクリックします。
  - **ポリシーごとにルールのオーバーライドを編集する**：[詳細オプション（Advanced Options）] スライダをオンにして、[すべてのオーバーライド（All Overrides）] タブを選択します。このセクションは、テナントに複数の IPS ポリシーが設定されている場合にのみ適用されます。このページでは、複数のデバイスが関連付けられているポリシーを含むすべての IP ポリシーを管理できます。

ステップ 5 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

署名のオーバーライドの作成

FTD デバイスですでにトリガーされている IPS ルールの署名オーバーライドのみを作成できます。CDO で署名のオーバーライドを作成すると、そのオーバーライドによって設定されたアクション（[ドロップ（Drop）]、[アラート（Alert）]、[無効化（Disabled）]、[デフォルト（Default）]）がすべてのポリシーレベルに自動的に適用されます。

手順

ステップ 1 メインナビゲーションバーから、[モニターリング（Monitoring）]>[脅威（Threats）] をクリックします。

ステップ 2 テーブルで脅威を選択して展開します。[調整アクション（Tune Actions）] ペインで、[調整（Tune）] をクリックします。

ステップ 3 「**Firepower 侵入ポリシーの署名のオーバーライド**」手順のFirepower 侵入ポリシーの署名のオーバーライドの説明に従いルールを調整します。

ステップ 4 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

署名のオーバーライドの削除

手順

ステップ 1 メインナビゲーションバーから、[ポリシー（Policies）] > [署名のオーバーライド（Signature Overrides）] をクリックします。

ステップ 2 オーバーライド名をクリックして、右側に詳細パネルを展開します。

ステップ 3 [オーバーライド（Overrides）] ペインを展開し、削除するオーバーライドを選択して、[調整（Tune）] をクリックします。

ステップ 4 デフォルトアクションを [デフォルト（Default）] に設定します。

ステップ 5 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Firepower 侵入防御システムのカスタムポリシー

IPS のカスタムポリシーについて

Firepower Version 6.7 の導入に伴い改善された Snort 3 処理エンジンにより、Cisco Talos Intelligence Group（Talos）が提供するルールを使用して侵入防御システム（IPS）ポリシーを作成およびカスタマイズできるようになりました。ベストプラクティスは、提供されている Talos ポリシーテンプレートに基づいて独自のポリシーを作成し、ルールアクションを調整する必要がある場合はそれを変更することです。

（注） 現時点では、CDO はカスタム IPS ルールをサポートしていません。Talos が提供するルールを使用してカスタム IPS ポリシーを作成および変更できますが、独自の IPS ルールを作成して、カスタム IPS ポリシーに適用することはできません。

基本テンプレートには一連の同じ侵入ルール（署名とも呼ばれます）が含まれていますが、各ルールに対して実行する操作は異なります。たとえば、あるポリシーでは有効化され、別のポリシーでは無効化されるルールがあります。他の例を挙げると、誤検出が非常に多く、ブロックして欲しくないトラフィックをブロックする特定のルールがあるとします。そのような場合には、安全性の低い侵入ポリシーに切り替えることなく、そのルールを無効にできます。または、トラフィックをドロップせずに、一致すると警告するように変更することもできます。

IPS ポリシーの基本テンプレート

基本テンプレートには一連の同じ侵入ルール（署名とも呼ばれます）が含まれていますが、各ルールに対して実行する操作は異なります。たとえば、あるポリシーでは有効化され、別のポリシーでは無効化されるルールがあります。他の例を挙げると、誤検出が非常に多く、ブロックして欲しくないトラフィックをブロックする特定のルールがあるとします。そのような場合には、安全性の低い侵入ポリシーに切り替えることなく、そのルールを無効にできます。または、トラフィックをドロップせずに、一致すると警告するように変更することもできます。

提供される基本テンプレートは、ネットワークで必要性の高い保護タイプに基づく推奨設定になっています。新しいポリシーを作成するときは、次のテンプレートのいずれかをベースとして使用できます。

注意 Snort 3 が有効になっている FTD で提供されるデフォルトの IPS ポリシーは変更**しないでください**。以下のテンプレートに基づいて新しいカスタム IPS ポリシーを作成し、下記のデフォルトの IPS ポリシー名とは異なる一意の名前を新しいポリシーに付けることを**強く**お勧めします。ポリシーのトラブルシューティングが必要になった場合、Cisco TAC はカスタムポリシーからデフォルトポリシーに簡単に戻すことができます。このとき、カスタマイズした変更を失うことなくネットワークを保護できます。

提供される基本テンプレートは、ネットワークで必要性の高い保護タイプに基づく推奨設定になっています。新しいポリシーを作成するときは、次のテンプレートのいずれかをベースとして使用できます。

- [最大検出（Maximum Detection）]：このポリシーは、[接続よりもセキュリティを優先（Security over Connectivity）] ポリシーよりもさらにネットワーク インフラストラクチャのセキュリティを重視するネットワーク向けです。運用に対する影響がさらに大きくなる可能性があります。
- [接続性よりもセキュリティを優先（Security over Connectivity）]：このポリシーは、ユーザーの利便性よりもネットワーク インフラストラクチャのセキュリティが優先されるネットワーク向けです。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。
- [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）]：このポリシーは、速度と検出の両方を兼ね備えていますこれらを一緒に使用すると、ほとんどの種類のネットワークおよび展開に適した出発点として機能します。
- [セキュリティより接続性を優先（Connectivity Over Security）]：このポリシーは、接続性やすべてのリソースを取得する機能が、ネットワーク インフラストラクチャのセキュリ

ティよりも優先されるネットワーク向けです。トラフィックをブロックする最も重要なルールだけが有効にされます。

- [アクティブなルールなし（No Rules Active）]：ポリシーに含まれるルールは、デフォルトで無効になっています。

ヒント [最大検出（Maximum Detection）]の基本テンプレートを効果的に機能させるには、大容量メモリと高性能 CPU が必要です。CDO では、このテンプレートを使用して IPS ポリシーを 2100、4100、または FTD 仮想などのモデルに展開することを推奨しています。

新たな脆弱性が既知になると、Talos は侵入ルールの更新をリリースします。侵入ルールが更新されると、シスコが提供するネットワーク分析ポリシーや侵入ポリシーが変更される場合があります。また、侵入ルールやプリプロセッサルールが新たに提供または更新され、既存のルールやポリシー設定に自動的に適用されます。ルールの更新によって、既存の基本テンプレートからルールが削除され、新しいルールカテゴリが提供されるとともに、デフォルトの変数セットが変更される場合もあります。

IPS ポリシーモード

デフォルトでは、IPS を実装するため、すべての侵入ポリシーが**防御**モードで動作します。防御インスペクションモードでは、トラフィックを切断するアクションの侵入ルールと接続が一致する場合、接続は能動的にブロックされます。

代わりに、ネットワーク上で侵入ポリシーの影響をテストするには、侵入検知システム（IDS）を実装する**検出**にモードを変更します。このインスペクションモードでは、切断ルールはアラートルールと同様に扱われます。この場合、一致する接続が通知されますが、アクションの結果は「ブロック相当」となり、実際に接続がブロックされることはありません。

IPS ルールグループのセキュリティレベル

CDO では、ポリシーに含まれるルールグループのセキュリティレベルを変更できます。このセキュリティレベルは、個々のルールではなく、ルールグループ内のすべてのルールに適用されることに注意してください。

（注） ルールグループのセキュリティレベルに対する変更は自動的に送信され、元に戻すことはできません。セキュリティレベルの変更を送信する際に[保存（Save）]をクリックする必要はありません。セキュリティレベルを元に戻す場合は、手動で行う必要があります。

IPS ルールアクション

個々のルールアクションまたはルールグループ内の複数のルールアクションは、いつでも変更できます。IPS ルールは、次のオプションで設定できます。

- [無効（Disabled）]：このルールではトラフィックは一致しません。イベントは生成されません。
- [アラート（Alert）]：このルールがトラフィックと一致するとイベントを作成しますが、接続はドロップしません。
- [ドロップ（Drop）]：このルールがトラフィックと一致するとイベントを作成し、接続をドロップします。

FTD テンプレートとカスタム IPS ポリシー

Snort 3 が有効になっているデバイスから取得されたテンプレートは、Snort 3 が有効になっているデバイスにのみ適用できます。Snort 2 および Snort 3 でサポートおよび処理されるルールにはばらつきがあるため、Snort 3 で設定されたテンプレートは、Snort 2 で設定されたデバイスを完全にサポートおよび保護することはできません。詳細については、「Snort 2 から Snort 3 への切り替え」を参照してください。

ASA 移行ツールを使用して ASA 設定から FTD テンプレートを作成する場合は、IPS ポリシーを設定または設定解除しないことを**強く**お勧めします。ASA デバイスは Snort エンジンをサポートしていないため、IPS ポリシーを ASA 設定から FTD 設定に移行すると問題が発生する可能性があります。ASA 移行ツールを使用する場合は、テンプレートを作成して展開した後に、デバイスのカスタム IPS ポリシーを作成することをお勧めします。

テンプレートの詳細については、「FTD テンプレート」を参照してください。

FTD ルールセットとカスタム IPS ポリシー

ルールセットは、Snort 3 用に設定されたデバイスではまだサポートされていません。次の制限が適用されます。

- Snort 3 対応デバイスにルールセットをアタッチすることはできません。
- Snort 3 がインストールされている既存のデバイスからルールセットを作成することはできません。
- カスタム IPS ポリシーをルールセットに関連付けることはできません。

前提条件

[侵入ポリシー（Intrusion Policies）] ページから使用可能な IPS ポリシーを表示できますが、カスタム IPS ポリシーを作成または変更するには、次の前提条件を満たす必要があります。

デバイス サポート

- FTD 1000 シリーズ
- FTD 2100 シリーズ
- FTD 4100 シリーズ
- AWS を搭載した FTD 仮想

- AWS を搭載した FTD 仮想

ソフトウェア サポート

デバイスは、少なくとも FTD バージョン 6.7 と Snort 3 を実行している**必要があります**。

デバイスが 6.7 より前のバージョンを実行している場合は、デバイスをアップグレードしてください。詳細については、「FTD のアップグレード」を参照してください。

デバイスが Snort 2 搭載のバージョンを実行している場合は、Snort 2.0 の一部の侵入ルールが Snort 3.0 に存在しない可能性があるので注意してください。詳細については、「Snort 2 から Snort 3 への切り替え」を参照してください。

（注） デバイスで実行されている Firepower および Snort エンジンのバージョンを確認するには、[インベントリ（Inventory）] ページでデバイスを見つけて選択し、[デバイスの詳細（Device Details）] を確認します。

関連情報：

- Firepower カスタム IPS ポリシーの設定
- FTD アクセス制御ルールのカスタム IPS ポリシーの設定

Firepower カスタム IPS ポリシーの設定

CDO で FTD デバイスのカスタム IPS ポリシーを作成または変更する前に、「Firepower 侵入防御システムのカスタムポリシー」を必ずお読みください。

現時点では、CDO はカスタム IPS ルールをサポート**していません**。Talos が提供するルールを使用してカスタム IPS ポリシーを作成および変更できますが、独自の IPS ルールを作成して、カスタム IPS ポリシーに適用することはできません。

CDO で IPS ポリシーを作成または編集する際に問題が発生した場合は、侵入防御システムのトラブルシュート で詳細を確認してください。

（注） カスタム IPS ポリシーのルールグループ内のルールを削除または並べ替えることはできません。

カスタム *IPS* ポリシーの作成

Talos が提供する IPS ルールで新しいカスタム IPS ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 CDO ナビゲーションウィンドウで、[ポリシー（Policies）] をクリックします。

ステップ 2 [侵入ポリシー（Intrusion Policies）] を選択します。

ステップ 3 青色のプラスボタン  をクリックします。

ステップ 4 [基本テンプレート（Base Template）] のドロップダウンメニューを展開し、ポリシーに適したテンプレートを選択します。選択できるテンプレートは次のとおりです。

- [最大検出（Maximum Detection）]：このポリシーは、[接続よりもセキュリティを優先（Security over Connectivity）] ポリシーよりもさらにネットワーク インフラストラクチャのセキュリティを重視するネットワーク向けです。運用に対する影響がさらに大きくなる可能性があります。
- [接続性よりもセキュリティを優先（Security over Connectivity）]：このポリシーは、ユーザーの利便性よりもネットワークインフラストラクチャのセキュリティが優先されるネットワーク向けです。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。
- [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）]：このポリシーは、速度と検出の両方を兼ね備えていますこれらを一緒に使用すると、ほとんどの種類のネットワークおよび展開に適した出発点として機能します。
- [セキュリティより接続性を優先（Connectivity Over Security）]：このポリシーは、接続性やすべてのリソースを取得する機能が、ネットワーク インフラストラクチャのセキュリティよりも優先されるネットワーク向けです。トラフィックをブロックする最も重要なルールだけが有効にされます。
- [アクティブなルールなし（No Rules Active）]：ポリシーに含まれるルールは、デフォルトで無効になっています。

ヒント [最大検出（Maximum Detection）] の基本テンプレートを効果的に機能させるには、大容量メモリと高性能 CPU が必要です。CDO では、このテンプレートを使用して IPS ポリシーを 2100、4100、または FTD 仮想などのモデルに展開することを推奨しています。

ステップ 5 [名前（Name）] にポリシー名を入力します。

デフォルトの基本テンプレートとは異なる一意の名前を使用することを**強く**推奨します。IPS ポリシーのトラブルシューティングが必要になった場合、Cisco TAC はカスタムポリシーからデフォルトポリシーに簡単に戻すことができます。このとき、カスタマイズした変更を失うことなくネットワークを保護できます。

ステップ 6 （任意）[説明（Description）] にポリシーの説明を入力します。

ステップ 7 [モード（Mode）] を次から選択します。

- [防御（Prevention）]：トラフィックを切断するアクションの侵入ルールと接続が一致する場合、接続は能動的にブロックされます。

- [検出（Detection）]：トラフィックをドロップするアクションの侵入ルールと接続が一致する場合、アクションの結果は [ブロック対象の可能性（Would Have Blocked）] になり、アクションは実行されません。

ステップ 8 [保存（Save）] をクリックします。

次のステップ

IPS ポリシーを FTD アクセス制御ルールに追加します。詳細については、「FTD アクセス制御ルールのカスタム IPS ポリシーの設定」を参照してください。

カスタム *IPS* ポリシーの編集

すでに IPS ポリシーが設定されている FTD デバイスをオンボードした場合、FDM で IPS ポリシーを作成し、CDO が展開された設定からポリシーを読み取る場合、または新しい IPS ポリシーを作成したばかりの場合、既存の IPS ポリシーを編集できます。

既存のカスタム IPS ポリシーを変更するには、次の手順を実行します。

手順

ステップ 1 CDO ナビゲーションウィンドウで、[ポリシー（Policies）] をクリックします。

ステップ 2 [侵入ポリシー（Intrusion Policies）] を選択します。

ステップ 3 編集する IPS ポリシーを特定します。[編集（Edit）] をクリックします。

ステップ 4 ページ上部で、 編集アイコン をクリックします。

ステップ 5 次に示す目的のフィールドを編集します。

- [基本テンプレート（Base Template）]
- 名前
- [説明（Description）]
- [IPSモード（IPS Mode）]

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

カスタム *IPS* ポリシーのルールグループの編集

ルールグループ内のルールのデフォルトアクションは上書きできます。ルールグループに含まれるルールを編集するには、次の手順を実行します。

手順

ステップ 1 CDO ナビゲーションウィンドウで、[ポリシー（Policies）] をクリックします。

ステップ 2 [侵入ポリシー（Intrusion Policies）] を選択します。

ステップ 3 編集する IPS ポリシーを特定します。[編集（Edit）] をクリックします。

ステップ 4 左側の [ルールグループ（Rule Group）] タブで目的のルールグループを展開します。展開されたリストから、グループを選択します。

ステップ 5 ルールグループを編集します。

a) セキュリティレベルバーを選択して、ルールグループ全体の [セキュリティレベル（Security Level）] を編集します。ルールグループ全体に適用するセキュリティタイプまで、セキュリティレベルを手動でドラッグします。[Submit（送信）] をクリックします。

b) 右側にあるルールのドロップダウンメニューを展開して、個々のルールの [ルールアクション（Rule Action）] を編集します。

c) 目的のルールのチェックボックスをオンにして、ルールのテーブルの上にあるドロップダウンメニューを展開し、複数のルールの [ルールアクション（Rule Action）] を編集します。選択したルールアクションは、選択したすべてのルールに影響します。

d) テーブルのタイトル行のチェックボックスをオンにして、ルールのテーブルの上にあるドロップダウンメニューを展開し、すべてのルールの [ルールアクション（Rule Action）] を編集します。選択したルールアクションは、ルールグループ内のすべてのルールに影響します。

ステップ 6 ポリシーページの最上部にある [保存（Save）] をクリックします。

ステップ 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

カスタム *IPS* ポリシーの削除

CDO から IPS ポリシーを削除するには、次の手順を使用します。

手順

ステップ 1 CDO ナビゲーションウィンドウで、[ポリシー（Policies）] をクリックします。

ステップ 2 [侵入ポリシー（Intrusion Policies）] を選択します。

ステップ 3 編集する IPS ポリシーを特定します。[Delete（削除）] をクリックします。

ステップ 4 [OK] をクリックしてポリシーを削除します。

ステップ 5 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

FTD セキュリティ インテリジェンス ポリシー

セキュリティ インテリジェンスについて

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。システムは、トラフィックをアクセス コントロール ポリシーで評価する前にドロップすることにより、使用されるシステムリソースの量を減らします。

次のものに基づいてトラフィックをブロックできます。

- **Cisco Talos フィード**：Cisco Talos は、定期的に更新されるセキュリティ インテリジェンス フィードへのアクセスを提供します。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。システムはフィードの更新を定期的にダウンロードするため、設定を再導入する必要なく新しい脅威インテリジェンスを利用できます。

（注） Cisco Talos フィードはデフォルトで 1 時間ごとに更新されます。更新頻度を変更でき、またフィードをオンデマンドで更新することもできます。そのためには、Firepower Device Manager にログインし、ホームページから [デバイス（Device）]>[更新（Updates）] > [設定の表示（View Configuration）] に移動します。

- **ネットワークおよび URL オブジェクト**：ブロック対象の IP アドレスまたは URL が既知の場合は、それらのオブジェクトを作成し、それらをブロックリストまたは許可リストに追加することができます。

IP アドレス（ネットワーク）と URL で別のブロックリストと許可リストを作成します。

セキュリティ インテリジェンスのためのライセンス要件

セキュリティ インテリジェンスを使用するには、FTD の**脅威**ライセンスを有効にする必要があります。

詳細については、該当する『Cisco FTD Configuration Guide for Firepower Device Manager』の「セキュリティポリシー」の章の「**セキュリティ インテリジェンス フィード カテゴリ**」セクションを参照してください。

Firepower セキュリティ インテリジェンス ポリシーの作成

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセス コントロール ポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティインテリジェンスを使用するには、脅威ライセンスを有効にする必要があります。

Firepower セキュリティ インテリジェンス ポリシーの設定

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、セキュリティインテリジェンスポリシーを作成または編集する FTD デバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、 [ポリシー（Policy）] をクリックします。

ステップ 5 [FTDポリシー（FTD Policies）] ページで、ポリシーバーの [セキュリティインテリジェンス（Security Intelligence）] をクリックします。

ステップ 6 ポリシーが有効になっていない場合は、[セキュリティインテリジェンス（Security Intelligence）] スライダをクリックして有効にするか、[セキュリティインテリジェンスについて（About Security Intelligence）] 情報ボックスで [有効化（Enable）] をクリックします。

（注） [セキュリティインテリジェンス（Security Intelligence）] をクリックしてオフに切り替えることで、いつでもセキュリティインテリジェンスを無効にできます。設定は維持されるため、ポリシーを再度有効にするときに再設定する必要はありません。

ステップ 7 [ブロックリスト（Blocked List）] の行を選択します。テーブルビューによっては、ネットワーク、ネットワークオブジェクト、ネットワークフィード、URL、URL オブジェクト、および URL フィードの列にプラス記号 があることに留意してください。

- [ブロックリストへのネットワークの追加（Add Networks to Blocked List）] ダイアログボックスと [ブロックリストへのURLオブジェクトの追加（Add URL Object to Blocked List）] ダイアログボックスで、既存のオブジェクトを検索するか、必要に応じてオブジェクトを作成できます。ブロックするオブジェクトにチェックを入れ、[選択（Select）] をクリックします。

  （注） セキュリティ インテリジェンスは、/0 ネットマスクを使用して、IP アドレス ブロックを無視します。これには、any-ipv4 と any-ipv6 のネットワーク オブジェクトが含まれます。ネットワークのブロックリストのためにこれらのオブジェクトを選択しないでください。

- [ブロックリストへのURLオブジェクトの追加（Add URL Objects to Blocked List）] および [ブロックリストへのネットワークフィードの追加（Add Network Feeds to Blocked List）] ダイアログで、ブロックするフィードにチェックを入れ、[選択（Select）] をクリックします。フィードの行の端にある下矢印をクリックすると、フィードの説明を読むことができます。「Firepower セキュリティ インテリジェンス ポリシー用セキュリティ インテリジェンスのフィード」でも説明されています。

ステップ 8 例外とするネットワーク、IP アドレス、または URL が、前の手順で指定したネットワークグループ、ネットワークフィード、URL オブジェクト、または URL フィードのいずれかに含まれることがわかっている場合は、[許可リスト（Allowed List）] の行をクリックします。

ステップ 9 例外とするネットワーク、IP アドレス、および URL のオブジェクトを選択または作成します。[選択（Select）] または [追加（Add）] をクリックすると、[許可リスト（Allowed List）] の行に追加されます。

ステップ 10 （オプション）セキュリティ インテリジェンス ポリシーによって生成されたイベントをログに記録するには、次の手順を実行します。

a) ロギングの設定  アイコンをクリックして、ロギングを設定します。ロギングを有効にした場合は、ブロックリストのエントリに一致するものが記録されます。ロギングを有効にして、除外された接続がアクセス制御ルールに一致した場合、ログメッセージは取得しますが例外エントリに一致するものは記録されません。

b) [接続イベントロギング（Connection Events Logging）] トグルをクリックして、イベントのロギングを有効にします。

c) イベントの送信先を選択します。

- [なし（None）] をクリックすると、イベントが FTD に保存されます。イベントは FDM イベントビューアに表示されます。FTD の記憶容量は非常に限られています。[なし（None）] を選択する代わりに、syslog サーバーオブジェクトを定義して、syslog サーバーに接続イベントを保存することをお勧めします。
- [作成（Create）] または [選択（Choose）] をクリックすると、syslog サーバーオブジェクトで表される syslog サーバーを作成または選択して、ロギングイベントを送信できます。デバイスのイベントストレージは限られているため、外部 syslog サーバーにイベントを送信すると、長期的な保存が可能になり、イベント分析が強化されます。

Cisco Security Analytics and Logging のサブスクリプションがある場合は、SEC の IP アドレスとポートを使用して syslog オブジェクトを設定することにより、イベントを Secure Event Connector に送信します。この機能の詳細については、「Cisco Security Analytics and Logging」を参照してください。

ステップ 11 （オプション）自分で作成したルールの場合、ルールを選択して、[コメントを追加（Add Comments）] フィールドでコメントを追加できます。ルールコメントに関する詳細については、「FTD ポリシーとルールセットのルールにコメントを追加する」を参照してください。

ステップ 12 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Firepower のセキュリティ インテリジェンス ポリシー ブロックリストに対する例外の作成

Firepower セキュリティ インテリジェンス ポリシーの作成で作成するブロックリストごとに、関連する許可リストを作成できます。許可リストの唯一の目的は、ブロックリストに表示される IP アドレスまたは URL の例外を作成することです。つまり、使用する必要があり、安全で

あることがわかっているアドレスや URL が、ブラックリストに設定されているフィードにある場合、許可リストに追加することで、そのアドレスやURL を除外できます。これにより、1つのアドレスや URL のためにブロックリストからフィード全体を削除する必要がなくなります。

許可されたトラフィックはセキュリティ インテリジェンス ポリシーを通過した後、アクセスコントロールポリシーによって評価されます。接続が許可またはドロップされたかどうかの最終決定は、接続に一致するアクセス制御ルールに基づきます。また、アクセス ルールは接続に侵入やマルウェア検査を適用するかどうかも判断します。

Firepower セキュリティ インテリジェンス ポリシー用セキュリティ インテリジェンスのフィード

次の表では、Cisco Talos フィードで利用可能なカテゴリについて説明します。これらのカテゴリは、ネットワークブロックリストと URL ブロックリストの両方で使用できます。

カテゴリ（**Category**）	説明
attackers	アクティブスキャナと悪意のある発信アクティビティが知られているブラックリストのホスト。
bogon	bogon ネットワークと未割り当て IP アドレス。
bots	バイナリ マルウェア ドロッパーをホストするサイト。
CnC	ボットネットの指示管理サーバをホストするサイト。
dga	指示管理サーバでランデブー ポイントとして動作する多数のドメイン名の生成に使用されるマルウェア アルゴリズム。
exploitkit	クライアントでのソフトウェアの脆弱性を識別するために設計されたソフトウェアキット。
malware	マルウェア バイナリまたはエクスプロイトキットをホストするサイト。
open_proxy	匿名での Web ブラウジングを許可するオープン プロキシ。
open_relay	スパムに使用されることが知られているオープン メール リレー。
phishing	フィッシング詐欺のページをホストするサイト。

カテゴリ（Category）	説明
response	悪意のある、または不審なアクティビティに積極的に参加している IP アドレスおよび URL。
spam	スパムの送信で知られているメール ホスト。
suspicious	疑わしく、既知のマルウェアのような特性を持っていると思われるファイル。
tor_exit_node	Tor の出口ノード。

FTD ID ポリシー

アイデンティティ ポリシーの概要

IDポリシーを使用して、接続からユーザーアイデンティティ情報を収集できます。その後で、ダッシュボードにユーザーアイデンティティに基づく使用状況を表示し、ユーザーまたはユーザーグループに基づくアクセスコントロールを設定できます。ネットワーク動作、トラフィック、およびイベントを個別のユーザーやグループに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。

たとえば、侵入イベントのターゲットとされたホストを誰が所有し、誰が内部攻撃やポートスキャンを開始したかを確認できます。また、高帯域幅のユーザーや、望ましくない Web サイトまたはアプリケーションにアクセスしているユーザーを確認することもできます。

次に、ユーザー ID に基づいて使用状況をダッシュボードに表示し、Active Directory（AD）レルムオブジェクト（その AD 上のすべてのユーザーに一致するオブジェクト）、特殊なアイデンティティ（認証失敗、ゲスト、認証不要、不明なアイデンティ）、またはユーザーグループに基づいてアクセス制御を設定できます。

ユーザ アイデンティティは、次の方法で取得できます。

- パッシブ認証：すべてのタイプの接続で、ユーザ名とパスワードを求められることなく、その他の認証サービスからユーザ アイデンティティを取得します。
- アクティブ認証：HTTP 接続でのみ、ユーザ名とパスワードの入力が求められ、送信元 IP アドレスのユーザ アイデンティティを取得するために指定のアイデンティティ ソースに対する認証が行われます。

パッシブ認証によるユーザー アイデンティティの確立

パッシブ認証では、ユーザーにユーザー名とパスワードを求めることなくユーザー ID を収集します。システムは、指定したアイデンティティ ソースからマッピングを取得します。

ユーザと IP アドレスのマッピングは次のソースから受動的に取得できます。

- リモートアクセス VPN ログイン。パッシブ アイデンティティについては次のユーザ タイプがサポートされています。
  - 外部認証サーバで定義されたユーザ アカウント。
  - Firepower Device Manager で定義されたローカル ユーザ アカウント。
- Cisco Identity Services Engine（ISE）、Cisco Identity Services Engine Passive Identity Connector（ISE PIC）。

特定のユーザーが複数のソースによって識別される場合は、リモートアクセス VPN ログイン アイデンティティが優先されます。

アクティブ認証によるユーザー ID の確立

認証は、ユーザのアイデンティティを確認する動作です。

アクティブ認証を使用すると、HTTP トラフィック フローがユーザー ID のマッピングがないシステムの IP アドレスから送られてきたときに、ネットワークに設定されたディレクトリを使用して、トラフィック フローを開始したユーザーを認証するかどうかを決定できます。ユーザーが正常に認証された場合、IP アドレスは認証されたユーザーの識別情報を保持していると見なされます。

認証が失敗しても、ユーザーのネットワーク アクセスは妨げられません。アクセス ルールは最終的に、これらのユーザーにどのアクセスを提供するか決定します。

不明なユーザーの対処

Firepower Device Manager（FDM）を使用してアイデンティティポリシーのディレクトリサーバーを設定すると、FDM はディレクトリサーバーからユーザーおよびグループメンバーシップ情報をダウンロードします。Active Directory 情報は、24 時間ごとに夜間に更新されるか、またはディレクトリ設定を編集して保存するたびに（変更がなくても）更新されます。

アクティブな認証アイデンティティルールによって求められた認証に成功したにも関わらず、ユーザー名がダウンロードしたユーザー ID 情報の中に存在しない場合、不明なユーザーとしてマークされます。ID 関連のダッシュボードにそのユーザーの ID は表示されず、ユーザー一致グループルールにも検出されません。

ただし、不明なユーザーに対するアクセス コントロール ルールが適用されます。たとえば、不明なユーザーの接続をブロックすると、これらのユーザーは、たとえ認証に成功（ディレクトリ サーバーがユーザーとパスワードが有効であると認識したことを意味する）してもブロックされます。

そのため、ユーザーの追加や削除、グループ メンバーシップの変更などをディレクトリ サーバーに加えた場合、システムがディレクトリから更新情報をダウンロードするまで、これらの変更はポリシーの適用に反映されません。

夜間の日次更新を待たずに、ただちに更新を実行する必要がある場合は、ディレクトリのレルム情報を編集します（FDM にログインして、[オブジェクト（Objects）] > [アイデンティティ ソース（Identity Sources）] に移動し、レルムを編集）。[OK] をクリックし、変更を展開します。システムはただちに更新情報をダウンロードします。

（注） 新規に追加したユーザー、または削除したユーザーの情報が FDM システムに反映されているかを確認するには、[ポリシー（Policies）] > [アクセス制御（Access Control）] に移動して、[ルールの追加（Add Rule）]（+）ボタンをクリックし、[ユーザー（Users）] タブに表示されるユーザーリストを確認してください。新規ユーザーがリスト上に見つからない場合、または削除されたユーザーがリスト上にある場合、システム内の情報は古いままです。

Firepower アイデンティティポリシーの導入方法

Cisco Defense Orchestrator（CDO）を使用して Firepower Threat Defense（FTD）デバイスの ID ポリシーを管理する場合は、最初に ID ソースを作成する必要があります。残りの設定は、Defense Orchestrator を使用して構成できます。

正しく設定されている場合、FDM の監視ダッシュボードおよびイベントでユーザー名を確認できます。ユーザーアイデンティティは、アクセス制御ルールや SSL 復号化ルールでもトラフィック一致基準として使用できます。

（注） 現時点では、CDO は、リモートアクセス VPN や Cisco Identity Services Engine などのアイデンティティポリシーの実装に必要な一部のコンポーネントを設定できません。これらのコンポーネントは、FTD デバイスのローカルマネージャである FDM で設定する必要があります。次に示す手順の一部は、アイデンティティポリシーを実装するため、FDM を使用して一部のアイデンティティ コンポーネントを設定する必要があることを示しています。

手順

次の手順では、アイデンティティポリシーを機能させるために必要な設定の概要を示します。

手順

ステップ 1 ADアイデンティティレルムを設定します。ユーザーアイデンティティをアクティブまたはパッシブに収集して、ユーザーアイデンティティ情報を含む Active Directory（AD）サーバーを設定する必要があります。詳細は「FTD アクティブ ディレクトリ レルム オブジェクトの作成」を参照してください。

ステップ 2 パッシブ認証アイデンティティルールを使用する場合は、**FDM を使用して**パッシブ アイデンティティ ソースを設定します。

デバイスに実装しているサービスおよびネットワークで使用可能なサービスに基づき、次のいずれかを設定できます。

- リモートアクセス VPN：デバイスへのリモートアクセス VPN 接続をサポートする場合は、AD サーバーまたは（FDM に定義されている）ローカルユーザーに基づいて、ユーザーログイン時にアイデンティティを提供できます。リモートアクセス VPN の設定については、デバイスが実行しているバージョンの『Cisco Firepower Threat Defense コンフィギュレー

ション ガイド（Firepower Device Manager 用』の「リモートアクセス VPN の設定」の章を参照してください。

- Cisco Identity Services Engine（ISE）または Cisco Identity Services Engine Passive Identity Connector（ISE PIC）：これらの製品を使用する場合は、デバイスを pxGrid サブスクライバとして設定し、ISE からユーザ アイデンティティを取得できます。手順については、『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』の「Identity Services Engine の設定」を参照してください。

ステップ 3 **Defense Orchestrator を使用して**、アイデンティティポリシーを有効にし、パッシブまたはアクティブ認証を設定します。詳細については、「アイデンティティポリシー設定の構成」を参照してください。

ステップ 4 **Defense Orchestrator を使用して**、Firepower アイデンティティポリシーのデフォルトアクションの設定。 パッシブ認証だけを使用する場合は、パッシブ認証に対するデフォルト アクションを設定でき、特定のルールを作成する必要はありません。

ステップ 5 **Defense Orchestrator を使用して**、アイデンティティ ルールの設定。関連するネットワークからパッシブまたはアクティブ ユーザー アイデンティティを収集するルールを作成します。

ステップ 6 （オプション）自分で作成したルールの場合、ルールを選択して、[コメントを追加（Add Comments）] フィールドでコメントを追加できます。ルールコメントに関する詳細については、「FTD ポリシーとルールセットのルールにコメントを追加する」を参照してください。

ステップ 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

アイデンティティポリシーの設定

アイデンティティポリシーを使用して、接続からユーザーアイデンティティ情報を収集できます。その後、FDM ダッシュボードにユーザーアイデンティティに基づく使用状況を表示し、ユーザーまたはユーザーグループに基づくアクセス制御を設定できます。

次に、アイデンティティポリシーでユーザーアイデンティティを取得するために必要な要素を設定する方法の概要を示します。

手順

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、アイデンティティポリシーを構成するデバイスを選択して、右側の [管理（Management）] ペインで [ポリシー（Policy）] をクリックします。

ステップ 4 [ポリシー（Policy）] バーで [アイデンティティ（Identity）] をクリックします。

ステップ 5 アイデンティティポリシーをまだ有効にしていない場合は、パッシブ認証とアクティブ認証について確認し、[有効化（Enable）] をクリックします。これにより、パッシブ認証ポリシーやアクティブ認証ポリシーではなく、アイデンティティポリシーが有効になります。ポリシーのルールでは、アクティブ認証またはパッシブ認証が指定されます。

ステップ 6 アイデンティティポリシーを管理します。

アイデンティティ設定を行うと、このページにすべてのルールが順番にリストアップされます。上から下に向かってルールがトラフィックと照合され、最初に適合したルールによって、適用されるアクションが決定されます。このページで次の操作を実行できます。

- **アイデンティティポリシーを有効または無効にするには**、アイデンティティトグルをクリックします。詳細については、「アイデンティティポリシー設定の構成」を参照してください。
- **パッシブ認証の設定を確認するには**、アイデンティティバーの [パッシブ認証（Passive Auth）] ラベルの横にあるボタンをクリックします。詳細については、「アイデンティティポリシー設定の構成」を参照してください。
- **アクティブ認証を有効にするには**、アイデンティティバーの [アクティブ認証（Active Auth）] ラベルの横にあるボタンをクリックします。詳細については、「アイデンティティポリシー設定の構成」を参照してください。
- **デフォルトアクションを変更するには**、デフォルトアクションのボタンをクリックし、目的のアクションを選択します。「Firepower アイデンティティポリシーのデフォルトアクションの設定」を参照してください。
- **テーブル内でルールを移動させるには**、ル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矢印または下矢印をクリックします。
- **テーブル内でルールを移動させるには**、ル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矢印または下矢印をクリックします。
- **ルールを設定するには**、次の手順を実行します。
  - 新しいルールを作成するには、プラス  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（Edit）] をクリックします。テーブルでプロパティをクリックして、選択的にルールのプロパティを編集することもできます。
  - 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）] をクリックします。

アイデンティティルールの作成と変更の詳細については、「アイデンティティルールの設定」を参照してください。

ステップ 7 （オプション）自分で作成したルールの場合、ルールを選択して、[コメントを追加（Add Comments）] フィールドでコメントを追加できます。ルールコメントに関する詳細については、「FTD ポリシーとルールセットのルールにコメントを追加する」を参照してください。

ステップ 8 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

アイデンティティ ポリシー設定の構成

アイデンティティ ポリシーを機能させるには、ユーザ アイデンティティ情報を提供する送信元を設定する必要があります。必要な設定は、設定するルールのタイプ（パッシブ、アクティブ、または両方）によって異なります。

（注） 現時点では、CDOは、Active Directoryアイデンティティレルム、リモートアクセスVPN、Cisco Identity Services Engineなどのアイデンティティポリシーの実装に必要な一部のコンポーネントを設定できません。これらのコンポーネントは、FTDデバイスのローカルマネージャであるFDMで設定する必要があります。次に示す手順の一部は、アイデンティティポリシーを実装するため、FDMを使用して一部のアイデンティティ コンポーネントを設定する必要があることを示しています。

手順

始める前に

ディレクトリサーバー、FTDデバイス、およびクライアント間で、時刻設定が一致していることを確認します。これらのデバイス間で時刻にずれがあると、ユーザ認証が成功しない場合があります。「一致」とは、別のタイムゾーンを使用できますが、たとえば、10 AM PST = 1 PM ESTなど、それらのゾーンに対して相対的に同じになっている必要があることを意味しています。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、アイデンティティポリシーを構成するデバイスを選択して、右側の [管理（Management）] ペインで [ポリシー（Policy）] をクリックします。

ステップ 4 [アイデンティティ（Identity）] トグルをクリックして、**アイデンティティポリシー**を有効にします。または、ボタンをクリックし、パッシブ認証とアクティブ認証の説明を確認して、ダイアログで [有効化（Enable）] をクリックします。

ステップ 5 **パッシブ認証の設定を読みます**。アイデンティティバーの [パッシブ認証（Passive Auth）] ボタンをクリックします。

Firepower Device Manager を使用してリモートアクセス VPN または Cisco Identity Services エンジンを構成している場合、パッシブ認証ボタンには [有効（Enabled）] と表示されます。

パッシブ認証ルールを作成するには、少なくとも 1 つのパッシブ アイデンティティ ソースを設定している必要があります。

ステップ 6 **アクティブ認証を構成します。**アイデンティティ ルールにユーザのアクティブ認証が必要な場合、ユーザは接続されているインターフェイスのキャプティブ ポータル ポートにリダイレクトされ、その後、認証を要求されます。

a) アイデンティティバーの [アクティブ認証（Active Auth）] ボタンをクリックします。

b) まだ有効にしていない場合は、[有効化（Enable）] リンクをクリックして SSL の説明を有効化します。[有効化（Enable）] リンクが表示されない場合は、手順「c」にスキップします。

1. [再署名証明書の復号選択（Select Decrypt Re-Sign Certificate）] メニューで、再署名証明書での復号を実装するルールに使用する内部 CA 証明書を選択します。

   事前定義された **NGFW-Default-InternalCA** 証明書を使用するか、メニューをクリックして [作成（Create）] を選択することで新しい証明書を作成するか、すでに FTD にアップロードした証明書を選択します。

   クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（  ）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。『再署名の復号ルールの CA 証明書のダウンロード』も参照してください。再署名の復号ルールの CA 証明書のダウンロード （205 ページ）

   （注） SSL 復号ポリシーをまだ構成していない場合にのみ SSL 復号の設定が求められます。ID ポリシーを有効にした後、これらの設定を変更するには、SSL 復号ポリシー設定を編集します。

2. [保存（Save）] をクリックします。

c) [サーバ証明書（Server Certificate）] メニューをクリックし、アクティブ認証時にユーザに提示する内部証明書を選択します。必要な証明書をまだ作成していない場合は、[作成（Create）] をクリックします。ブラウザが信頼している証明書をアップロードしない場合、ユーザは証明書を許可する必要があります。

d) [ポート（Port）] フィールドにキャプティブポータルのポート番号を入力します。デフォルトは、885（TCP）です。別のポートを設定する場合は、1025 ～ 65535 の範囲にする必要があります。

（注） HTTP Basic、HTTP 応答ページ、および NTLM 認証方式では、ユーザはインターフェイスの IP アドレスを使用してキャプティブ ポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、ユーザは完全修飾 DNS 名「firewall-hostname.AD-domain-name」を使用してリダイレクトされます。HTTP ネゴシエートを使用する場合、アクティブ認証を必要としているすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバを更新する必要があります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。

e) [保存（Save）] をクリックします。

ステップ 7 「Firepower アイデンティティポリシーのデフォルトアクションの設定」を続けます。

Firepower アイデンティティポリシーのデフォルトアクションの設定

アイデンティティ ポリシーにはデフォルトアクションがあり、これは個別のアイデンティティ ルールに一致しない接続に対して実行されます。

実際には、ルールがないことがポリシーの有効な設定になります。すべてのトラフィックの送信元でパッシブ認証を使用する予定の場合は、単純にパッシブ認証をデフォルトアクションとして設定します。

手順

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、アイデンティティポリシーを構成するデバイスを選択して、右側の [管理（Management）] ペインで [ポリシー（Policy）] をクリックします。

ステップ 4 [ポリシー（Policy）] バーで [アイデンティティ（Identity）] をクリックします。

ステップ 5 「アイデンティティ ポリシー設定の構成」が完了していない場合は行います。

ステップ 6 画面の下部にある [デフォルトアクション（Default Action）] ボタンをクリックして、次のいずれかを選択します。

- [パッシブ認証（Passive Auth）]：ユーザ—アイデンティティは、任意のアイデンティティ ルールに一致しない接続に対して、設定されたすべてのパッシブ アイデンティティ ソースを使用して特定されます。パッシブ アイデンティティ ソースを設定しない場合は、パッシブ認証をデフォルトとして使用すると [認証なし（No Auth）] を使用することと同じになります。

- [認証なし（No Auth）]：ユーザ—アイデンティティは、任意のアイデンティティルールに一致しない接続について特定されません。

ステップ 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

アイデンティティ ルールの設定

アイデンティティルールは、一致するトラフィックに対してユーザ識別情報を収集する必要があるかどうかを定義します。一致するトラフィックのユーザーアイデンティティ情報を収集しない場合は、[認証なし（No Authentication）] を設定できます。

ルール設定に関係なく、アクティブ認証はHTTP トラフィックに対してのみ実行されることに注意してください。したがって、HTTP以外のトラフィックをアクティブ認証から除外するルールを作成する必要はありません。すべてのHTTP トラフィックに対してユーザ識別情報を取得する場合は、アクティブ認証ルールをすべての送信元および宛先に適用するだけで済みます。

（注） また、認証に失敗してもネットワークアクセスには影響しません。アイデンティティポリシーは、ユーザ識別情報のみを収集します。認証に失敗したユーザがネットワークにアクセスできないようにするには、アクセス ルールを使用する必要があります。

手順

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、アイデンティティポリシーを構成するデバイスを選択して、右側の [管理（Management）] ペインで [ポリシー（Policy）] をクリックします。

ステップ 4 [ポリシー（Policy）] バーで [アイデンティティ（Identity）] をクリックします。

ステップ 5 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、プラス ボタンをクリックします。アイデンティティソース オブジェクトとそれがルールに与える影響については、「FTD のアイデンティティソースの設定」を参照してください。
- 既存ルールを編集するには、編集するルールを選択し、右側の操作ウィンドウで [編集（Edit）] をクリックします。

- 不要になったルールを削除するには、削除するルールを選択し、右側の操作ウィンドウで[削除（Remove）] をクリックします。

ステップ 6 [順序（Order）] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

ルールは最初に一致したものから順に適用されるため、限定的な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、汎用的な基準を持つルールよりも上に置く必要があります。

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 7 [名前（Name）] にルール名を入力します。

ステップ 8 [アクション（Action）] でルールに適合した場合に FTD に適用するアクションを選択し、必要に応じて Active Directory（AD）のアイデンティティソースを選択します。

パッシブおよびアクティブ認証ルールのユーザーアカウントが含まれる AD アイデンティティレルムを選択する必要があります。選択肢は以下のとおりです。

- [パッシブ認証（Passive Auth）] : パッシブ認証を使用して、ユーザアイデンティティを判断します。設定されたすべてのアイデンティティ ソースが表示されます。ルールでは、設定されたすべてのソースが自動的に使用されます。
- [アクティブ認証（Active Auth）] : アクティブ認証を使用して、ユーザーアイデンティティを判断します。アクティブ認証は HTTP トラフィックのみに適用されます。他のタイプのトラフィックが、アクティブ認証を要求または許可するアイデンティティポリシーに適合した場合、アクティブ認証は試行されません。
- [認証なし（No Auth）] : ユーザ識別情報を取得しません。このトラフィックに、アイデンティティベースのアクセス ルールは適用されません。これらのユーザは、[認証不要（No Authentication Required）] とマークが付けられます。

（注） [パッシブ認証（Passive Auth）] と [アクティブ認証（Active Auth）] の両方で、AD レルムのアイデンティティソースを選択できます。アイデンティティ ソース オブジェクトを準備していない場合は、[新しいオブジェクトの作成（Create new object）] をクリックして、アイデンティティ ソース オブジェクト ウィザードを起動します。詳細は「FTD アクティブ ディレクトリ レルム オブジェクトの作成または編集」を参照してください。

ステップ 9 （アクティブ認証のみ）[アクティブ認証] タブをクリックして、ディレクトリサーバーでサポートする認証方法（タイプ）を選択します。

- [HTTP基本（HTTP Basic）] : 暗号化されていない HTTP 基本認証接続を使用して、ユーザーを認証します。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。これがデフォルトです。
- [NTLM] : NT LAN マネージャ（NTLM）接続を使用して、ユーザを認証します。この選択は AD レルムを選択するときにのみ使用できます。ユーザーはブラウザのデフォルトの認証ポップアップウィンドウを使用してネットワークにログインします。Windows ドメイン

のログインを使ってトランスペアレント認証が行われるように、Internet Explorer と Firefox ブラウザを設定することもできます。このタスクはFDMで実行します。手順については、『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』>「セキュリティポリシー」>「アイデンティティポリシー」>「**トランスペアレントユーザー認証の有効化**」を参照してください。

- [HTTPネゴシエート（HTTP Negotiate）]：ユーザ エージェント（トラフィック フローを開始するためにユーザが使用しているアプリケーション）方式と Active Directory サーバ方式の間でデバイスがネゴシエーションできるようになります。ネゴシエーションの結果は、NTLM、ベーシックの順に、共通にサポートされ、使用されている最も強力な方式になります。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。
- [HTTP応答ページ（HTTP Response Page）]：システムが提供する Web ページを使用して、ユーザーに認証を求めるプロンプトを表示します。これは、HTTP 基本認証の 1 つの形式です。

（注） HTTP Basic、HTTP 応答ページ、および NTLM 認証方式では、ユーザはインターフェイスの IP アドレスを使用してキャプティブ ポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、ユーザーは完全修飾 DNS 名「*firewall-hostname.AD-domain-name*」を使用してリダイレクトされます。HTTP ネゴシエートを使用する場合、アクティブ認証を必要としているすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバを更新する必要があります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。

ステップ 10 （アクティブ認証のみ）アクティブ認証に失敗したユーザーをゲストユーザーとしてラベル付けするかどうかを決めるには、[ゲストとしてフォールバック（Fall Back as Guest）]>[オン/オフ（On/Off）] を選択します。

ユーザは、正常に認証する 3 つの機会が得られます。失敗した場合、このオプションの選択により、ユーザがどのようにマーク付けされるかが決まります。これらの値に基づき、アクセスルールを展開できます。

- [ゲストとしてフォールバック（Fall Back as Guest）]>[オン（On）]：ユーザーは [ゲスト（Guest）] としてマーク付けされます。
- [ゲストとしてフォールバック（Fall Back as Guest）]>[オフ（Off）]：ユーザ—は [失敗した認証（Failed Authentication）] としてマーク付けされます。

ステップ 11 パッシブ認証、アクティブ認証、または認証なしのルールアクションについて、[送信元（Source）] タブと [宛先（Destination）] タブで、トラフィックの適合基準を定義します。

アクティブ認証は、HTTP トラフィックに対してのみ試されることに注意してください。したがって、HTTP 以外のトラフィックに対して 「認証なし」のルールを設定は不要で、HTTP 以外のトラフィックに対してアクティブ認証ルールを作成するポイントもありません。ただし、パッシブ認証は任意のタイプのトラフィックに有効です。

アイデンティティ ルールの送信元/宛先基準は、トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレス、または IP アドレスの国または大陸（地理的位置）、またはトラフィックで使用されるプロトコルおよびポートを定義します。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。

条件を変更するには、条件内の  ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップダイアログボックスの [OK] をクリックします。条件で必要とされているオブジェクトが存在しない場合は、[新規オブジェクトの作成（Create New Object）] をクリックします。

条件からオブジェクトを削除するには、オブジェクトにカーソルを合わせて [X] をクリックします。

次のトラフィック一致基準を設定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティ ゾーン オブジェクト。1 つの基準を定義する 、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、内部ネットワークから発信されるすべてのトラフィックからユーザ識別情報を収集する場合、内部ゾーンを [送信元ゾーン（Source Zones）] として選択し、宛先ゾーンを空のままにします。

（注） 1 つのルールにパッシブ セキュリティ ゾーンとルーテッド セキュリティ ゾーンを混在させることはできません。さらに、パッシブ セキュリティ ゾーンは送信元ゾーンとしてのみ指定でき、宛先ゾーンとして指定することはできません。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。

- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク（Network）]：制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワークオブジェクトまたはグループを選択します。
- [国/大陸（Country/Continent）]：地理的な位置を選択して、その送信元または宛先の国や大陸に基づきトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。
- [カスタム地理位置情報（Custom Geolocation）]：指定した国と大陸を正確に含む地理位置情報オブジェクトを選択（または作成）します。

（注） 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。詳細については、「地理位置情報データベースの更新」を参照してください。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。TCP/UDP では、これにポートを含めることができます。

- プロトコルまたはポートからのトラフィックを照合するには、[送信元ポート（Source Ports）] を設定します。送信元ポートを使用できるのは、TCP/UDP のみです。
- プロトコルまたはポートへのトラフィックを照合するには、[宛先ポート/プロトコル（Destination Ports/Protocols）] を設定します。
- 特定の TCP/UDP ポートから発生し、特定の TCP/UDP ポートに向かうトラフィックを照合するには、両方設定します。送信元ポートと宛先ポートの両方を条件に追加する場合、単一のトランスポート プロトコル、TCP、または UDP を共有するポートのみを追加できます。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にできます。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 [デバイスとサービス（Devices & Services）] ページに戻ります。

ステップ 14 ルールを追加したアイデンティティポリシーがあるデバイスを選択します。

ステップ 15 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

FTD SSL 復号ポリシー

HTTPS など一部のプロトコルは、セキュア ソケット レイヤ（SSL）またはその後継バージョンである Transport Layer Security（TLS）を使用して、セキュアな転送のためにトラフィックを暗号化します。システムでは暗号化された接続を検査できないため、アクセス判断のために上位層のトラフィック特性を考慮したアクセスルールを適用する場合は、SSL 復号ポリシーを適用して暗号化された接続を復号する必要があります。

注意 トラフィックの復号とその後の再暗号化は、全体的なシステムパフォーマンスを低下させるデバイスの処理負荷が増加することに注意してください。

次のトピックに進みます。

- SSL 復号について
- SSL 復号ポリシーの実装および管理方法
- SSL 復号ポリシーの設定
- 既知のキーと復号の再署名の証明書の設定
- 再署名の復号ルールの CA 証明書のダウンロード
- SSL 暗号解読の問題のトラブルシューティング

SSL 復号ポリシーの実装および管理方法

URL フィルタリング、侵入、マルウェア コントロール、および詳細なパケット検査を必要とするその他のサービスを適用できるように、SSL 復号ポリシーを使用して暗号化されたトラフィックをプレーン テキスト トラフィックにできます。ポリシーがトラフィックを許可する場合、そのトラフィックはデバイスから出る前に再暗号化されます。

SSL 復号ポリシーは、暗号化されたトラフィックにのみ適用されます。暗号化されていない接続は SSL 復号ルールに対して評価されません。

他のセキュリティ ポリシーの場合とは異なり、SSL 復号ポリシーは、監視して積極的に保守する必要があります。これは、証明書の期限が切れたり、宛先サーバで変更されたりするためです。さらに、クライアント ソフトウェアの変更により特定の接続を復号する能力が変わる場合もあります。これは、再署名の復号アクションを中間者攻撃と区別できないためです。

次の手順では、SSL 復号ポリシーの実装と保守のエンドツーエンド プロセスを説明します。

手順

手順	
ステップ 1	再署名の復号ルールを実装する場合は、必要な内部 CA 証明書を作成します。

内部認証局（CA）証明書を使用する必要があります。次の選択肢があります。ユーザは証明書を信頼する必要があるため、すでに信頼されると設定されているクライアントブラウザに証明書をアップロードするか、またはアップロードする証明書がブラウザの信頼ストアに追加されるようにします。

- デバイス自体によって署名される自己署名内部CA証明書を作成します。『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』で「再利用可能なオブジェクト」>「証明書」>「自己署名内部および内部CA証明書の生成」を参照してください。
- 外部の信頼できるCAまたは組織内部のCAによって署名される内部CA証明書およびキーをアップロードします。『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』で「再利用可能なオブジェクト」>「証明書」>「内部および内部 CA 証明書のアップロード」を参照してください。

ステップ 2 既知のキーの復号ルールを実装する場合は、各内部サーバーから証明書とキーを収集します。

サーバーから証明書とキーを取得する必要があるため、既知のキーの復号は自分で制御しているサーバーでのみ使用できます。これらの証明書とキーを内部証明書（内部 CA 証明書ではない）としてアップロードします。『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』で「再利用可能なオブジェクト」>「証明書」>「内部および内部 CA 証明書のアップロード」を参照してください。

ステップ 3 SSL 復号ポリシーの設定

ポリシーを有効にする際に、いくつかの基本的な設定も構成します。

ステップ 4 SSL 復号のデフォルト アクションの設定

不確かな場合は、デフォルトアクションとして[復号しない（Do not decrypt）]を選択します。この場合でも、アクセス コントロール ポリシーは、デフォルトの SSL 復号ルールに一致するトラフィックを適切であればドロップできます。

ステップ 5 SSL 復号ルールの設定

復号するトラフィック、および適用する復号のタイプを識別します。

ステップ 6 既知のキーでの復号を設定する場合は、これらの証明書を含めるようにSSL復号ポリシー設定を編集します。「既知のキーと復号の再署名の証明書の設定」を参照してください。

ステップ 7 必要に応じて、再署名の復号ルールに使用するCA証明書をダウンロードして、クライアントワークステーションのブラウザにアップロードします。

証明書のダウンロードおよびクライアントへの配布については、「再署名の復号ルールの CA 証明書のダウンロード」を参照してください。

ステップ 8 定期的に、再署名証明書および既知のキーの証明書を更新します。

- 再署名証明書：期限切れになる前にこの証明書を更新します。Firepower Device Managerを使用して証明書を生成する場合は、5 年間有効です。証明書の有効期限を確認するには、[オブジェクト（Objects）] ページで証明書の表示アイコンをクリックします。

- 既知のキーの証明書：既知のキーによる復号ルールの場合、宛先サーバーの現在の証明書とキーがアップロードされていることを確認する必要があります。サポートされるサーバで証明書およびキーが変更されるたびに、新しい証明書およびキーを（内部証明書として）アップロードし、新しい証明書を使用するようにSSL復号設定を更新する必要があります。

ステップ 9 外部サーバで不足している信頼できる CA 証明書をアップロードします。

システムには、サードパーティによって発行された、広範な信頼できるCAルート証明書および信頼できるCA中間証明書が含まれています。これらは、再署名の復号ルールについてFTDと宛先サーバーの間で接続をネゴシエートするときに必要です。

信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。[オブジェクト（Objects）] > [証明書（Certificates）] ページで証明書をアップロードします。『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』で「再利用可能なオブジェクト」>「証明書」>「信頼できる CA 証明書のアップロード」を参照してください。

SSL 復号について

通常、ネットワーク接続が許可されるかブロックされるかを決定するのはアクセス コントロール ポリシーです。ただし、SSL 復号ポリシーを有効にする場合、暗号化された接続は最初にSSL復号ポリシー経由で送信され、復号化するかブロックする必要があるかが判断されます。ブロックされていない接続は、復号化の有無にかかわらず、許可/ブロックの最終的な決定のためにアクセス コントロール ポリシーを経由します。

（注） アイデンティティ ポリシーでアクティブな認証ルールを実装するためには、SSL 復号ポリシーを有効にする必要があります。SSL 復号を有効にして ID ポリシーを有効にするが、SSL 復号は実装しない場合、[SSL復号（SSL Decryption）] ページでデフォルトのアクションに [復号しない（Do Not Decrypt）] を選択し、追加の SSL 復号ルールは作成しないでください。アイデンティティ ポリシーでは、必要なルールを自動的に生成します。

ここでは、暗号化トラフィック フロー管理と復号化についてさらに詳しく説明します。

- SSL 復号を実装する理由
- 自動的に生成された SSL 復号ルール
- 復号できないトラフィックの処理

SSL 復号を実装する理由

HTTPS 接続などの暗号化されたトラフィックは検査することができません。銀行や他の金融機関への接続など、多くの接続は合法的に暗号化されます。多くの Web サイトでは、プライバシーや機密性の高いデータを保護するために暗号化を使用します。たとえば、Firepower Device Manager への接続は暗号化されます。ただし、暗号化された接続の中ではユーザが望ましくないトラフィックを隠すこともできます。

SSL復号を実装することによって、接続を復号して脅威またはその他の望ましくないトラフィックが含まれていないかを確認するために検査し、再度暗号化してから接続の続行を許可できます。（復号されたトラフィックは、アクセス制御ポリシーを通過し、暗号化された特性ではなく、復号された接続の検査特性に基づいたルールに一致します。）これは、アクセス制御ポリシーを適用する必要性とユーザーの機密情報を保護する必要性との間でバランスをとります。

ネットワークを利用させたくない種類の暗号化されたトラフィックをブロックする SSL 復号ルールを構成することもできます。

注意 トラフィックの復号とその後の再暗号化は、全体的なシステム パフォーマンスを低下させるデバイスの処理負荷が増加することに注意してください。

暗号化されたトラフィックに適用できるアクション

SSL復号ルールを設定する場合は、次のトピックで説明しているアクションを適用できます。これらのアクションは、明示的なルールと一致しないすべてのトラフィックに適用されるデフォルトのアクションにも使用できます。

- 再署名の復号
- 既知のキーの復号
- 復号禁止
- ブロック

（注） SSL 復号ポリシーを経由するすべてのトラフィックは、アクセス コントロール ポリシーを経由する必要があります。SSL復号ポリシーにドロップするトラフィックを除き、許可またはドロップの最終的な決定はアクセス コントロール ポリシーに委ねられます。

再署名の復号

トラフィックを復号し再署名する場合、システムは中間者として機能します。

たとえば、ユーザーがブラウザで https://www.cisco.com と入力します。トラフィックが FTD デバイスに達すると、デバイスはルールで指定された CA 証明書を使用するユーザーとネゴシエーションを行い、ユーザーと FTD デバイス間に SSL トンネルを構築します。同時に、デバ

イスは https://www.cisco.com に接続し、サーバーと FTD デバイス間に SSL トンネルを作成します。

このため、ユーザには、www.cisco.com からの証明書ではなく、SSL 復号ルールで設定された CA 証明書が表示されます。ユーザは、接続を完了するために証明書を信頼する必要があります。FTD デバイスは、ユーザーと宛先サーバー間のトラフィックで両方向に復号/再暗号化を実行します。

（注） サーバー証明書の再署名に使用する CA をクライアントが信頼していない場合、証明書が信頼できないという警告がユーザーに出されます。これを防止するには、クライアントの信用できる CA ストアに CA 証明書をインポートします。または組織にプライベート PKI がある場合は、組織の全クライアントで自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。

[復号-再署名（Decrypt - Resign）] アクションをルールに設定すると、ルールによるトラフィックの照合は、設定されている他のルール条件に加えて、参照する内部 CA 証明書の署名アルゴリズムタイプに基づいて実施されます。SSL 復号ポリシーに 1 つの再署名証明書を選択できるため、これによって再署名ルールのトラフィック一致を制限できます。

たとえば、楕円曲線（EC）アルゴリズムで暗号化された発信トラフィックは、再署名証明書が EC ベースの CA 証明書の場合にのみ、再署名の復号ルールと一致します。同様に、RSA アルゴリズムで暗号化されたトラフィックは、グローバル再署名証明書が RSA の場合にのみ、再署名の復号ルールと一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されたその他すべてのルール条件が一致していても、このルールとは一致しません。

既知のキーの復号

宛先サーバを所有している場合、既知のキーで復号化を実装できます。この場合、ユーザーが https://www.cisco.com への接続を開くと、証明書を提示しているのが FTD デバイスであっても、www.cisco.com の実際の証明書がユーザーに表示されます。

ドメインおよび証明書の所有者は、所属組織でなければなりません。cisco.com を例として取り上げると、エンドユーザーにシスコの証明書が表示されるのは、組織が実際にドメイン cisco.com の所有者であり（つまり、所属企業が Cisco Systems であること）、パブリック CA

によって署名された cisco.com 証明書の所有権を持っている場合のみです。復号できるのは、所属組織が所有するサイトの既存のキーを使用する場合のみです。

既知のキーを使用して復号する主な目的は、HTTPS サーバへのトラフィックを復号して、社内サーバを外部の攻撃から保護することです。外部 HTTPS サイトへのクライアント側のトラフィックを検査する場合は、サーバを所有していないので、再署名の復号を使用する必要があります。

（注） 既知のキーの復号を使用するには、サーバーの証明書およびキーを内部アイデンティティ証明書としてアップロードし、SSL復号ポリシー設定で既知のキーの証明書一覧に追加する必要があります。その後は、サーバーのアドレスを宛先アドレスとして使用して、既知のキーの復号ルールを展開できます。SSL復号ポリシーに証明書を追加する方法については、「SSL復号ポリシーの設定」を参照してください。

復号禁止

特定の種類のトラフィックで復号をバイパスする場合、トラフィックの処理は行われません。暗号化されたトラフィックはアクセス コントロール ポリシーに渡され、一致するアクセス制御ルールに基づいて許可またはドロップされます。

ブロック

単にSSL復号ルールと一致する暗号化されたトラフィックをブロックできます。SSL復号ポリシーのブロックでは、アクセス コントロール ポリシーに接続が達することを防ぎます。

HTTPS 接続をブロックすると、ユーザにはシステムのデフォルトのブロック応答ページが表示されません。代わりに、セキュアな接続で障害が発生した際のブラウザのデフォルトページが表示されます。エラーメッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

自動的に生成された SSL 復号ルール

SSL復号ポリシーを有効にしてもしなくても、FTDはアクティブ認証を実装する各IDポリシールールに対して再署名の復号ルールを自動的に生成します。これは、HTTPS 接続でアクティブな認証を有効にするために必要です。

SSL復号ポリシーを有効にすると、アイデンティティ ポリシーのアクティブな認証ルールの見出しの下にこれらのルールが表示されます。これらのルールは、SSL復号ポリシーの上部にグループ化されます。ルールは読み取り専用です。ルールは ID ポリシーを変更することによってのみ変更できます。

復号できないトラフィックの処理

接続が復号できなくなる特性は複数あります。接続に次の特性のいずれかがある場合、接続で一致するルールがあっても接続にはデフォルトのアクションが適用されます。（[復号しない

（Do Not Decrypt）] ではなく）デフォルト アクションとしてブロックを選択する場合、正当なトラフィックの過剰なドロップなどの問題があることがあります。

- 圧縮されたセッション：データ圧縮が接続に適用されています。
- SSLv2 セッション：サポートされている最下位の SSL バージョンは SSLv3 です。
- 不明な暗号スイート：システムで接続の暗号スイートが認識されません。
- サポート外の暗号スイート：システムで、検出された暗号スイートに基づく復号化がサポートされません。
- キャッシュされないセッション：SSL セッションにおいてセッションの再利用が可能になっていて、クライアントとサーバがセッション ID でセッションを再確立したときに、システムがそのセッション ID をキャッシュに入れなかったことを意味します。
- ハンドシェイク エラー：SSL ハンドシェイクのネゴシエーション中にエラーが発生しました。
- 復号エラー：復号処理中にエラーが発生しました。
- パッシブ インターフェイス トラフィック：パッシブ インターフェイス（パッシブ セキュリティ ゾーン）のすべてのトラフィックが復号不能です。

SSL 復号ポリシーのライセンス要件

SSL 復号ポリシーを使用するのに特別なライセンスは必要ありません。

ただし、URL カテゴリおよびレピュテーションを一致基準として使用するルールを作成するには、URL フィルタリング ライセンスが必要です。ライセンスの設定については、『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』>「システムのライセンス」>「オプションライセンスの有効化と無効化」を参照してください。

SSL 復号のガイドライン

SSL 復号ポリシーを設定してモニターする場合は、次の点に注意してください。

- SSL復号ポリシーは、次のようなアクセス制御ルールがトラフィックを信頼またはブロックするように設定されている場合に、それらのルールに一致する接続に関してバイパスされます。
  - セキュリティゾーン、ネットワーク、地理位置情報、およびポートだけをトラフィック照合基準として使用する。
  - 検査を必要とする他のルール（アプリケーションまたは URL に基づいて接続を照合するルールなど）に先立つか、侵入またはファイル検査を適用するルールを許可する。
- URL カテゴリのマッチングを使用するときは、サイトのログイン ページがサイトそのものと異なるカテゴリにある場合に注意してください。たとえば、Gmail は「Web ベースの電子メール」カテゴリにあり、ログインページは「インターネットポータル」カテゴリに

あります。これらのサイトへの接続を復号するには、両方のカテゴリをルールに含める必要があります。

- アクティブ認証ルールを使用している場合は、SSL復号ポリシーを無効にすることができません。SSL 復号ポリシーを無効にするには、アイデンティティ ポリシーを無効にするか、またはアクティブ認証を使用するアイデンティティ ルールを削除する必要があります。

SSL 復号ポリシーの設定

URL フィルタリング、侵入、マルウェア コントロール、および詳細なパケット検査を必要とするその他のサービスを適用できるように、SSL 復号ポリシーを使用して暗号化されたトラフィックをプレーン テキスト トラフィックにできます。ポリシーがトラフィックを許可する場合、そのトラフィックはデバイスから出る前に再暗号化されます。

SSL復号ポリシーは、暗号化されたトラフィックにのみ適用されます。暗号化されていない接続は SSL 復号ルールに対して評価されません。

注意 トラフィックの復号とその後の再暗号化は、全体的なシステムパフォーマンスを低下させるデバイスの処理負荷が増加することに注意してください。

（注） VPN トンネルは SSL 復号ポリシーが評価される前に復号されるので、トンネル自体にはポリシーは適用されません。ただし、トンネル内で暗号化された接続はSSL復号ポリシーによる評価の対象となります。

以下の手順で、SSL復号ポリシーを設定する方法を説明します。SSL復号を作成および管理するエンドツーエンドプロセスの説明については、「SSL復号ポリシーの実装および管理方法」を参照してください。

手順

始める前に

SSL 復号ルール テーブルには、2 つのセクションが含まれています。

- [アイデンティティポリシーアクティブ認証ルール（Identity Policy Active Authentication Rules）]：アイデンティティ ポリシーを有効にしてアクティブ認証を使用するルールを作成すると、システムがこれらのポリシーの動作に必要なSSL復号ルールを自動的に作成します。これらのルールは、常に自分で作成したSSL復号ルールの前に評価されます。アイデンティティポリシーに変更することによって、間接的にのみこれらのルール変更できます。
- [SSLネイティブルール（SSL Native Rules）]：これらは自分で構成したルールです。このセクションにのみルールを追加できます。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、SSL ポリシーを作成するデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 5 ポリシーバーの [SSL復号化（SSL Decryption）] をクリックします。

ステップ 6 ポリシーをまだ有効化していない場合は、[SSL復号の有効化（Enable SSL Decryption）] をクリックし、「SSL 復号ポリシーの有効化」の説明に従ってポリシーを設定します。

ステップ 7 ポリシーのデフォルト アクションを設定します。最も安全な選択肢は、[復号しない（Do Not Decrypt）] です。詳細については、デバイスが実行しているバージョンの『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用』で、「セキュリティポリシー」章の「**SSL 復号のデフォルトアクションの設定**」項を参照してください。

ステップ 8 SSL 復号ポリシーを管理します。

SSL復号を設定した後、このページにすべてのルールが順番に一覧表示されます。上から下に向かってルールがトラフィックと照合され、最初に適合したルールによって、適用されるアクションが決定されます。このページで次の操作を実行できます。

- ポリシーを無効にするには、[SSL復号ポリシー（SSL Decryption Policy）] トグルをクリックします。[SSL複合を有効化（Enable SSL Decryption）] をクリックすると再度有効にできます。
- ポリシーで使用する証明書リストを含むポリシー設定を編集するには、SSL ツールバーの設定 ボタン 

をクリックします。また、クライアントに配布できるように、再署名の復号ルールで使用する証明書をダウンロードできます。デバイスで実行しているバージョンの『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』で「セキュリティポリシー」章の次の項を参照してください。
  - 既知のキーと復号の再署名の証明書の設定
  - 再署名の復号ルールの CA 証明書のダウンロード
- ルールを設定するには、次の手順を実行します。
  - 新しいルールを作成し、そのルールによりログイベントを生成するには、青色のプラスボタン  をクリックします。「SSL 復号ルールの設定」を参照してください。
  - 既存のルールを編集するには、ルールテーブル内のルールを選択し、操作ウィンドウで [編集（Edit）] をクリックします。テーブルでプロパティをクリックして、選択的にルールのプロパティを編集することもできます。

- 不要になったルールを削除するには、ルールテーブル内のルールを選択し、操作ウィンドウで [削除（Remove）] をクリックします。
- ルールを移動するには、ルールテーブル内の該当するルールにカーソルを合わせます。行の最後にある上下の矢印を使用して、ルール テーブルでその位置を移動します。
- （オプション）自分で作成したルールの場合、ルールを選択して、[コメントを追加（Add Comments）] フィールドでコメントを追加できます。ルールコメントに関する詳細については、「FTD ポリシーとルールセットのルールにコメントを追加する」を参照してください。

ステップ 9 「SSL 復号ポリシーの有効化」に進みます。

SSL 復号ポリシーの有効化

SSL復号ルールを設定する前に、ポリシーを有効にして、いくつかの基本的な設定を構成する必要があります。以下の手順で、ポリシーを直接有効にする方法を説明します。アイデンティティ ポリシーを有効にするときにこのポリシーを有効にすることもできます。アイデンティティ ポリシーでは、SSL 復号ポリシーを有効にする必要があります。

手順

始める前に

SSL復号ポリシーを持たないリリースからアップグレードし、アクティブな認証ルールを使用してアイデンティティポリシーを設定した場合、SSL復号ポリシーはすでに有効になっています。必ず使用する再署名の復号証明書を選択し、必要に応じて事前定義されたルールを有効にします。

まだ行っていない場合は、「SSL 復号ポリシーの設定」を確認してください。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、SSL 復号ポリシーを有効化するデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 5 ポリシーバーの [SSL復号化（SSL Decryption）] をクリックします。

ステップ 6 SSL バーの [SSL復号（SSL Decryption）] トグルをクリックして、SSL 復号ポリシーを有効にします。

- 初めてポリシーを有効にした場合は、既知のキーの復号および再署名のSSL復号についての説明に目を通し、[有効化（enable）] をクリックします。
- 以前にこのポリシーを設定した後で無効にした場合は、前の設定とルールを使用してポリシーが再度有効になります。SSL復号の設定ボタン 

をクリックし、「既知のキーと復号の再署名の証明書の設定」に記載されている説明に従って設定できます。

ステップ 7 [再署名証明書の復号（Decrypt Re-Sign Certificate）] では、再署名証明書での復号を実装するルールに使用する内部 CA 証明書を選択します。

事前定義済みの NGFW-Default-InternalCA 証明書か、作成またはアップロードしたものを使用できます。証明書がまだ存在しない場合は、[作成（Create）] をクリックして FTD 内部 CA 証明書を追加します。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（  ）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。「再署名の復号ルールの CA 証明書のダウンロード」も参照してください。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 「SSL復号のデフォルトアクションの設定」に進み、ポリシーのデフォルトアクションを設定します。

SSL 復号のデフォルト アクションの設定

暗号化された接続が特定のSSL復号ルールに一致しない場合、SSL復号ポリシーのデフォルトアクションに基づいて処理されます。

手順

始める前に

次の手順をまだ実行していない場合は、手順を確認して実行してください。

1. SSL 復号ポリシーの設定
2. SSL 復号ポリシーの有効化

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、デフォルトの SSL 復号アクションを設定するデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 5 ポリシーバーの [SSL復号化（SSL Decryption）] をクリックします。

ステップ 6 [デフォルトアクション（Default Action）] ボタンをクリックします。

ステップ 7 一致するトラフィックに適用するアクションを選択します。

- [復号しない（Do Not Decrypt）]：暗号化された接続を許可します。次にアクセス制御ポリシーは、暗号化された接続を評価し、アクセス制御ルールに基づいてドロップまたは許可します。
- [ブロック（Block）]：接続をすぐに切断します。接続はアクセス制御ポリシーに渡されません。

ステップ 8 （オプション）デフォルトアクションのロギングを設定します。SSL復号ポリシーからイベントをキャプチャするには、ロギングを有効にする必要があります。次のオプションから選択します。

- [接続終了時（At End of Connection）]：接続の終了時にイベントを生成します。
  - [接続イベントの送信先（Send Connection Events To）]：外部の syslog サーバーにイベントのコピーを送信するには、syslog サーバーを定義するサーバーオブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバーの新規作成（Create New Syslog Server）] をクリックして作成します（syslog サーバへのロギングを無効化するには、サーバのリストから [任意（Any）] を選択します）。

    デバイスのイベント ストレージは限られているため、外部 syslog サーバーへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

    Cisco Security Analytics and Logging のサブスクリプションがある場合は、Secure Event Connector の IP アドレスとポートを使用して syslog サーバーを指定または作成します。この機能の詳細については、「Cisco Security Analytics and Logging」を参照してください。
- [ロギングなし（No Logging）]：イベントを生成しません。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

SSL 復号ルールの設定

SSL 復号ルールを使用して、暗号化された接続を処理する方法を決定します。SSL 復号ポリシーに設定されたルールは、上から下への順に評価されます。トラフィックに適用されるルールは、すべてのトラフィック基準が一致する最初のルールです。

[SSLネイティブルール（SSL Native Rules）] セクションでのみルールを作成し、編集できます。

注意 トラフィックの復号とその後の再暗号化は、全体的なシステムパフォーマンスを低下させるデバイスの処理負荷が増加することに注意してください。

（注） SSL 復号ポリシーが接続を評価する前に、VPN 接続（サイト間とリモート アクセスの両方）のトラフィックが復号されます。したがって、SSL 復号ルールが VPN 接続に適用されることはなく、これらのルールを作成するときに VPN 接続を考慮する必要はありません。ただし、VPN トンネル内で暗号化された接続を使用する場合は評価されます。たとえば、RA VPN トンネル自体は（すでに復号されているので）評価されなくても、RA VPN 接続経由の内部サーバーへの HTTPS 接続は、SSL 復号ルールによって評価されます。

手順

始める前に

「SSL 復号ポリシーの設定」、「SSL 復号ポリシーの有効化」、および「SSL 復号のデフォルト アクションの設定」がまだの場合は内容を確認し、ルールを追加する SSL 復号ポリシーを設定します。

既知のキーの復号ルールを作成する場合は、宛先サーバーのための証明書とキーを（内部証明書として）アップロードし、証明書を使用するために SSL 復号ポリシーの設定も編集します。既知のキーのルールは通常、ルールの宛先ネットワークの条件で宛先サーバーを指定します。詳細については、「既知のキーと復号の再署名の証明書の設定」を参照してください。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、SSL 復号ポリシーを有効化するデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 5 ポリシーバーの [SSL復号化（SSL Decryption）] をクリックします。

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、青色のプラスボタン をクリックします。
- 既存のルールを編集するには、ルールの編集アイコン をクリックします。

- 不要になったルールを削除するには、ルールの削除アイコン をクリックします。

ステップ 7 [順序（Order）] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

[SSLネイティブルール（SSL Native Rules）] セクションにのみルールを挿入できます。アイデンティティ ポリシーアクティブ認証ルールはアイデンティティ ポリシーから自動的に生成され、読み取り専用です。

ルールは最初に一致したものから順に適用されるため、限定的な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、汎用的な基準を持つルールよりも上に置く必要があります。

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 [名前（Name）] にルール名を入力します。

この名前にスペースを含めることはできません。英数字と以下の特殊文字を使用できます：+ . _ -

ステップ 9 一致するトラフィックに適用するアクションを選択します。各オプションの詳細については、次を参照してください。

- 再署名の復号
- 既知のキーの復号
- 復号禁止
- ブロック

ステップ 10 次のタブの任意の組み合わせを使用して、トラフィック一致基準を定義します。

- [送信元/送信先（Source/Destination）]：トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレスまたは IP アドレスの国/大陸（地理的ロケーション）、トラフィックで使用されている TCP ポート。デフォルトでは、すべてのゾーン、アドレス、地理的ロケーション、TCP ポートが対象になります。「SSL 復号ルールの送信元/送信先基準」を参照してください。
- [URL]：Web 要求の URL カテゴリ。デフォルトでは URL カテゴリおよびレピュテーションはマッチングの目的では考慮されません。「SSL 復号ルールの URL 基準」を参照してください。
- [アプリケーション（Application）]：アプリケーション、またはタイプ、カテゴリ、タグ、リスク、ビジネスとの関連性ごとにアプリケーションを定義するフィルタ。デフォルトは任意の暗号化されたアプリケーションです。「SSL 復号ルールのアプリケーション基準」を参照してください。
- [ユーザ（Users）]：ユーザとユーザ グループ。アイデンティティ ポリシーは、ユーザーとグループの情報がトラフィックの照合に使用できるかどうかを定義します。この基準を使用するには、アイデンティティ ポリシーを設定する必要があります。「SSL 復号ルールのユーザー基準」を参照してください。

- [拡張（Advanced）]：SSL/TLS バージョンや証明書のステータスなどの接続に使用する証明書に由来する特性。「SSL 復号ルールの詳細条件」を参照してください。

条件を変更するには、条件内の青色のプラスボタン  をクリックして該当するオブジェクトまたは要素を選択し、ポップアップダイアログボックスで [選択（Select）] をクリックします。条件で必要とされているオブジェクトが存在しない場合は、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

条件を SSL 復号ルールに追加する際は、以下のヒントを参考にしてください。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールのすべての条件に一致する必要があります。たとえば、URL カテゴリに基づいて復号するために単一のルールを使用できます。
- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準のいずれかに一致するトラフィックはその条件を満たします。たとえば、最大 50 のアプリケーションまたはアプリケーション フィルタにアプリケーション制御を適用する単一のルールを使用できます。したがって、単一の条件では項目間に OR 関係がありますが、条件タイプ間（たとえば、送信元/宛先とアプリケーション間）には AND 関係があります。
- URL カテゴリのマッチングには、URL フィルタ リング機能のライセンスが必要です。

ステップ 11 （オプション）ルールのロギングを設定します。

ルールと一致するトラフィックをダッシュボード データまたはイベント ビューアに含めるには、ロギングを有効にする必要があります。次のオプションから選択します。

- [ロギングなし（No Logging）]：イベントを生成しません。
- [接続イベントの送信先（Send Connection Events To）]：外部の syslog サーバにイベントのコピーを送信するには、syslog サーバを定義するサーバ オブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[作成（Create）] をクリックしてそのオブジェクトを作成します（syslog サーバへのロギングを無効化するには、サーバのリストから [任意（Any）] を選択します）。
- [接続終了時（At End of Connection）]：接続の終了時にイベントを生成します。デバイスのイベント ストレージは限られているため、外部 syslog サーバーへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

Cisco Security Analytics and Logging のサブスクリプションがある場合は、Secure Event Connector の IP アドレスとポートを使用して syslog サーバーオブジェクトを指定または作成します。詳細については、「Cisco Security Analytics and Logging」を参照してください。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 （オプション）自分で作成したルールの場合、ルールを選択して、[コメントを追加（Add Comments）] フィールドでコメントを追加できます。ルールコメントに関する詳細については、「FTD ポリシーとルールセットのルールにコメントを追加する」を参照してください。

ステップ 14 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

SSL 復号ルールの送信元/送信先基準

SSL 復号ルールの [送信元/送信先（Source/Destination）] 基準で、トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレスまたは IP アドレスの国/大陸（地理的ロケーション）、トラフィックで使用されている TCP ポートを定義します。デフォルトでは、すべてのゾーン、アドレス、地理的ロケーション、TCP ポートが対象になります。TCP は、SSL 復号ルールに一致する唯一のプロトコルです。

条件を変更するには、その条件内の青色ボタン  をクリックして、目的のオブジェクトまたは要素を選択し、[選択（Select）] をクリックします。条件で必要とされているオブジェクトが存在しない場合は、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティ ゾーン オブジェクト。1 つの基準を定義する 、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、外部ホストから内部ホストへのすべてのトラフィックが復号されたことを確認したい場合、[送信元ゾーン（Source Zones）] で外部ゾーンを選択し、[送信先ゾーン（Destination Zones）] で内部ゾーンを選択します。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のメニューオプションから選択します。

- [ネットワーク（Network）]：制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。

（注） 既知のキーの復号ルールの場合、証明書とアップロードしたキーを使用する送信先サーバーの IP アドレスを持つオブジェクトを選択します。

- [国/大陸（Country/Continent）]：地理的な位置を選択して、その送信元または宛先の国や大陸に基づきトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。
- [カスタム地理位置情報（Custom Geolocation）]：作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。SSL 復号ルールに対してのみ TCP プロトコルとポートを指定できます。

- TCP ポートからのトラフィックを一致させるには、[送信元ポート（Source Ports）] を設定します。
- TCP ポートへのトラフィックを一致させるには、[送信先ポート/プロトコル（Destination Ports/Protocols）] を設定します。

特定の TCP ポートから特定の TCP ポートへ発信されるトラフィックを一致させるには、両方のポートを設定します。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にできます。

ステップ 10

SSL 復号ルールのアプリケーション基準

SSL 復号ルールのアプリケーション基準では、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタ処理が定義されます。デフォルトは、SSL プロトコル タグを持つアプリケーションです。暗号化されていないアプリケーションは SSL 復号ルールと一致できません。

ルールで個別のアプリケーションを指定できますが、アプリケーション フィルタを使用すれば、ポリシーの作成と管理が簡単になります。たとえば、リスクが高くビジネスとの関連性が低いすべてのアプリケーションを復号またはブロックする SSL 復号ルールを作成できます。

ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションが復号またはブロックされます。

また、シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーション ディテクタを更新し追加します。これにより、リスクの高いアプリケーションのルールが新しいアプリケーションに自動的に適用される可能性があり、手動でルールを更新する必要がなくなります。

アプリケーションとフィルタをルールで直接指定することも、これらの特性を定義するアプリケーションフィルタ オブジェクトを作成することもできます。指示は同じですが、複雑なルールを作成する場合、オブジェクトを使用した方が 基準当たり 50 項目のシステム上限範囲を超えにくくなります。

アプリケーションとフィルタリストを変更するには、条件内の  ボタンをクリックし、目的のアプリケーションまたはアプリケーション フィルタ オブジェクトを選択してから、ポップアップ ダイアログボックスで [選択（Select）] をクリックし、次に [保存（Save）] をクリックします。ポリシーからそれを削除するアプリケーション、フィルタ、またはオブジェクトの [x] をクリックします。[フィルタとして保存（Save As Filter）] リンクをクリックして、すでにオブジェクトではない結合基準を新しいアプリケーション フィルタ オブジェクトとして保存します。

アプリケーション基準と、高度なフィルタを設定してアプリケーションを選択する方法の詳細については、「アプリケーション フィルタ オブジェクトの設定」を参照してください。

SSL 復号ルールでアプリケーション基準を使用する場合は、次のヒントを考慮してください。

- このシステムでは、StartTLS を使用して暗号化される非暗号化アプリケーションを識別できます。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、TLS ClientHello メッセージ内の Server Name Indication、またはサーバー証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。
- システムは、サーバ証明書の交換後にのみアプリケーションを識別できます。SSL ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により、ハンドシェイクが完了し、アプリケーションを識別できるようになります。システムによる識別が完了すると、アプリケーション条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。

ステップ 10

SSL 復号ルールの URL 基準

SSL 復号ルールの URL の基準は、Web 要求の URL が属するカテゴリを定義します。また、復号、ブロック、または復号せずに許可するサイトの相対的なレピュテーションも指定できます。デフォルトでは、URL カテゴリに基づき接続と一致しません。

たとえば、すべての暗号化されたゲームサイトをブロックしたり、リスクの高いすべてのソーシャルネットワーキングサイトを復号できます。該当するカテゴリとレピュテーションのURLをユーザが参照しようとすると、セッションがブロックされるか、または復号されます。

SSL 復号ルールに URL 基準を追加するには、次の手順を実行します。

手順

ステップ 1 [URL] タブをクリックして、SSL 復号ルールに URL カテゴリを追加します。

ステップ 2 ブロックする URL カテゴリを検索して選択します。

ステップ 3 デフォルトでは、選択したカテゴリの URL からのトラフィックは、セキュリティ レピュテーションに関係なく、SSL 復号ルールによって復号されます。ただし、ルール内の特定の URL カテゴリまたはすべての URL カテゴリを微調整し、レピュテーションに基づいて一部のサイトを復号の対象から除外できます。

- URL 内の 1 つのカテゴリのレピュテーションを微調整するには、次の手順を実行します。
  1. 選択した URL カテゴリをクリックします。
  2. [任意のレピュテーション（Any Reputation）] のチェックボックスをオフにします。
  3. 緑色のスライダを右にスライドして、ルールから除外する URL レピュテーションの設定を選択し、[保存（Save）] をクリックします。

     スライダでカバーされたレピュテーションには、ルールが適用されません。たとえば、緑色のスライダを [無害のサイト（Benign Sites）] にスライドすると、よく知られているサイトと無害のサイトには、選択したカテゴリの SSL 復号ルールが適用されません。セキュリティリスクのあるサイト、疑わしいサイト、および高リスクサイトと見なされる URL には、その URL カテゴリのルールが適用されます。

- ルールに追加したすべての URL カテゴリのレピュテーションを微調整するには、次の手順を実行します。
  1. SSL 復号ルール対象のすべてのカテゴリを選択したら、[選択したカテゴリにレピュテーションを適用（Apply Reputation to Selected Categories）] をクリックします。
  2. [すべてのレピュテーション（Any Reputation）] のチェックボックスをオフにします。
  3. 緑色のスライダを右にスライドして、ルールから除外する URL レピュテーションの設定を選択し、[保存（Save）] をクリックします。

     スライダでカバーされたレピュテーションには、ルールが適用されません。たとえば、緑色のスライダを [無害のサイト（Benign Sites）] にスライドすると、よく知られているサイトと無害のサイトには、すべてのカテゴリの SSL 復号ルールが適用されません。セキュリティリスクのあるサイト、疑わしいサイト、および高リスクサイトと見なされる URL は、すべての URL カテゴリのルールが適用されます。

ステップ 4 [選択（Select）] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

ステップ 10

SSL 復号ルールのユーザー基準

SSL 復号ルールのユーザ基準は、IP 接続のユーザまたはユーザ グループを定義します。ルールにユーザまたはユーザ グループの基準を含めるように、アイデンティティ ポリシーと関連ディレクトリ サーバを設定する必要があります。

アイデンティティ ポリシーは、特定の接続に関してユーザー アイデンティティを収集するかどうかを決定します。アイデンティティが確立されると、ホストの IP アドレスに識別されたユーザーが関連付けられます。したがって、送信元 IP アドレスがユーザーにマッピングされているトラフィックは、そのユーザーからのものとみなされます。IP パケット自体にはユーザー アイデンティティ情報は含まれていないため、この IP アドレスとユーザー間のマッピングが使用可能な中での最良近似となります。

1 つのルールに最大 50 のユーザーまたはグループを追加できるため、通常は、グループを選択する方が個々のユーザーを選択するより有意義です。たとえば、外部ネットワークからエンジニアリンググループへのトラフィックを復号するルールを作成し、そのグループからの発信トラフィックを復号しない別のルールを作成できます。その後、ルールを新しいエンジニアに適用するには、エンジニアをディレクトリ サーバーのエンジニアリング グループに追加するだけです。

ユーザーリストを変更するには、条件内の [+] ボタンをクリックして、目的のユーザー グループを選択し、[選択（Select）] をクリックします。

ステップ 10

SSL 復号ルールの詳細条件

詳細のトラフィックの一致条件は、接続に使用する証明書に由来する特徴に関連します。次のオプションのいずれかまたはすべてを設定できます。

証明書のプロパティ

トラフィックは、選択したプロパティのいずれかに一致する場合、ルールの証明書プロパティのオプションに一致します。次の設定を行えます。

- [証明書ステータス（Certificate Status）]：証明書が [有効（Valid）] か [無効（Invalid）] か。証明書のステータスを気にしない場合は、[任意（Any）]（デフォルト）を選択します。 証明書は、次の条件のすべてが満たされている場合に有効とみなされ、それ以外の場合は無効とみなされます。
  - ポリシーが証明書を発行した CA を信用できる。
  - 証明書の署名を証明書の内容に対して正しく検証できる。
  - 発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されている。
  - ポリシーの信頼できる CA のいずれでも証明書が失効していない。

- 現在の日付が証明書の [有効期間の開始（Valid From）] と [有効期間の終了（Valid To）] の期間内にある。

- [自己署名（Self-Signed）]：サーバー証明書に同じサブジェクトおよび発行元識別名が含まれているかどうか。次のいずれかを選択します。
- [自己署名（Self-Signing）]：サーバー証明書は自己署名されています。
  - [CA 署名（CA-Signing）]：サーバー証明書は認証局によって署名されています。 つまり、発行元とサブジェクトは同じではありません。
  - [任意（Any）]：証明書が自己署名されているかどうかを一致条件として考慮しません。

サポートされるバージョン

一致する SSL/TLS バージョン。ルールは、選択したいずれかのバージョンを使用するトラフィックにのみ適用されます。デフォルトは全バージョンです。[SSLv3.0]、[TLSv1.0]、[TLSv1.1]、[TLSv1.2] から選択します。

たとえば、TLSv1.2 の接続のみを許可する場合は、TLSv1.2 以外のバージョンにブロック ルールを作成できます。記載されていない SSL v2.0 などのバージョンを使用するトラフィックは、SSL 復号ポリシーのデフォルトのアクションによって処理されます。

ステップ 10

既知のキーと復号の再署名の証明書の設定

再署名によってまたは既知のキーを使用して復号を実装する場合は、SSL 復号ルールが使用できる証明書を特定する必要があります。すべての証明書が有効で、期限が切れていないことを確認します。

特に既知のキーを復号する場合は、復号する接続の各宛先サーバーの現在の証明書とキーがシステムにあることを確認する必要があります。既知のキーの復号ルールでは、復号の宛先サーバーからの実際の証明書とキーを使用します。したがって、常に FTD デバイスに最新の証明書とキーがあることを確認する必要があります。そうでない場合復号は失敗します。

既知のキーのルールで宛先サーバーの証明書またはキーを変更するたびに新しい内部証明書とキーをアップロードします。それらを内部証明書（内部 CA 証明書ではありません）としてアップロードします。以下の手順の間に証明書をアップロードするか、  ボタンをクリックして [FTD] > [証明書（Certificate）] を選択することで、[オブジェクト（Object）] ページに証明書をアップロードできます。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、SSL ポリシーを作成するデバイスを選択して、右側の [管理（Management）] ペインで [ポリシー（Policy）] をクリックします。

ステップ 4 ポリシーバーの [SSL復号化（SSL Decryption）] をクリックします。

ステップ 5 SSL 復号化ポリシーのポリシーバーの証明書ボタン 

をクリックします。

ステップ 6 SSL 複合化構成ダイアログで、[再署名証明書の復号（Decrypt Re-Sign Certificate）] メニューをクリックし、再署名証明書での復号を実装するルールに使用するための内部 CA 証明書を選択または作成します。事前定義済みの **NGFW-Default-InternalCA** 証明書か、作成またはアップロードしたものを使用できます。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（  ）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。また、デバイスが実行しているバージョンに対応する『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド』の「セキュリティポリシー」の章で、「**再署名の復号ルールの CA 証明書のダウンロード**」も参照してください。

ステップ 7 既知のキーを使用して復号するルールごとに、宛先サーバの内部証明書とキーをアップロードします。

ステップ 8 [既知のキーの証明書の復号（Decrypt Known-Key Certificates）] で  をクリックします。

ステップ 9 内部 ID の証明書を選択するか、[新しい内部証明書の作成（Create New Internal Certificate）] をクリックし、ここでそれをアップロードします。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

再署名の復号ルールの CA 証明書のダウンロード

トラフィックを復号する場合、ユーザは、TLS/SSL を使用するアプリケーションで信頼できるルート認証局として定義された暗号化プロセスで使用される、内部 CA 証明書を持っている必要があります。通常、証明書を生成した場合や、証明書をインポートした場合であっても、これらのアプリケーションで証明書がすでに信頼されているものとして定義されることはありません。ユーザーが HTTPS 要求を送信すると、大部分の Web ブラウザでは、デフォルトで、Web サイトのセキュリティ証明書に問題があることを知らせる警告メッセージがクライアントアプリケーションによって表示されます。通常、このエラーメッセージでは、Web サイトのセキュリティ証明書が信頼された認証機関から発行されたものではないこと、または Web サイトが不明な認証機関で証明されたものであることが示されますが、処理中の中間者攻撃の可能性が警告で示唆される場合もあります。クライアントアプリケーションによっては、この警告メッセージがユーザに示されず、ユーザは承認されない証明書を受け入れることができません。

以下のいくつかの方法で、ユーザに必要な証明書を提供できます。

ルート証明書を受け入れるようにユーザに通知する

組織内のユーザに、企業の新しいポリシーについて通知し、組織が提供したルート証明書を、信頼できる認証局として受け入れるように指示できます。ユーザは証明書を受け入れ、信頼されたルート認証局のストレージエリアにそれを保存して、次にサイトにアクセスしたときにプロンプトが再度表示されないようにする必要があります。

（注） ユーザは、代替証明書を作成したCA証明書を受け入れて、信頼する必要があります。そうではなく、単に代替サーバ証明書を信頼した場合は、異なるHTTPSサイトを訪問するたびに、警告が表示される状況が続きます。

クライアントデバイスにルート証明書を追加する

ネットワーク上のすべてのクライアントデバイスに、信頼できるルート認証局としてルート証明書を追加できます。そうすれば、クライアントアプリケーションは自動的にルート証明書を持つトランザクションを受け入れるようになります。

証明書を電子メールで送信するか、共有サイトに置くことで、ユーザが証明書を入手できるようにします。または、会社のワークステーション イメージに証明書を組み込み、アプリケーションの更新機能を使用して、ユーザに証明書を自動的に配布することもできます。

次に、内部CA証明書をダウンロードして、Windowsクライアントにインストールする方法を説明します。

手順

プロセスは、オペレーティングシステムとブラウザの種類によって異なります。たとえば、Windows上で実行されているInternet ExplorerおよびChromeの場合は次のプロセスを使用できます。（Firefoxの場合は、[ツール（Tools）] > [オプション（Options）] > [詳細（Advanced）] ページでインストールします。）

メッセージは、インポートが成功したことを示しているはずです。ユーザがよく知られたサードパーティの認証局から証明書を取得するのではなく自己署名証明書を生成した場合は、途中でWindowsが証明書を検証できなかったことを警告するダイアログ ボックスが表示される場合があります。

[証明書（Certificates）] ダイアログ ボックスと [インターネットオプション（Internet Options）] ダイアログ ボックスを閉じることができます。

手順

ステップ1 Firepower Device Managerから証明書をダウンロードします。

a) ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

b) [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。
c) [FTD] タブをクリックし、証明書が保存されているデバイスを選択します。
d) 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。
e) ポリシーバーの [SSL復号化（SSL Decryption）] をクリックします。
f) SSL 復号ポリシーのポリシーバーの SSL 復号設定ボタン 

をクリックします。
g) ダウンロードボタン  をクリックします。
h) ダウンロード場所を選択して、必要に応じてファイル名を変更し（拡張子はそのまま）、[Save] をクリックします。
i) これで、[SSL復号設定（SSL Decryption Settings）] ダイアログ ボックスからキャンセルできます。

ステップ 2 クライアント システムの Web ブラウザにある信頼されたルート認証局のストレージ エリアに証明書をインストールするか、クライアント自体が証明書をインストールできるようにします。この手順は、ブラウザやオペレーティングシステムによって異なります。

警告（Warning）

FDM を介して設定された CA 証明書

CDO では複数のデバイスを管理できますが、デバイス設定の保存時に保存対象となる追加情報に制限があるため、内部CA証明書の処理で問題が発生する可能性があります。CDOでは、FDM コンソールを介して設定した CA 証明書の証明書情報やキー情報が保存**されません**。セカンダリデバイスに展開された SSL ポリシーに FDM で設定した CA 証明書を適用しようとすると、CDOでCA証明書のローカルコピーは作成されますが、キー情報はコピーされません。その結果、CDOにもセカンダリデバイスにもキー情報がないため、CA証明書は正常に展開されません。これは、CA 証明書のローカルコピーのダウンロードリンクが利用できないことも意味します。

FDM を使用して追加のデバイス用に別の CA 証明書を設定するか、CDO UI を使用して CA 証明書を作成することを強く推奨します。

FTD ルールセット

FTD ルールセットについて

FTD ルールセットは、複数の FTD デバイスと共有できるアクセス制御ルールのコレクションです。ルールセットのルールに加えられた変更は、このルールセットを使用する他の管理対象 FTD デバイスに影響します。FTD デバイスには、デバイス固有の（ローカル）ルールと共有（ルールセット）ルールを含めることができます。FTD デバイスの既存のルールからルールセットを作成することもできます。

重要 「ルールセット」機能は現在、FTD バージョン 6.5 以降を実行しているデバイスで使用できます。ルールセットは Snort 3 が有効になっているデバイスをサポートしていないことにも注意してください。

次の制限が適用されます。

- Snort 3 対応デバイスにルールセットをアタッチすることはできません。
- Snort 3 がインストールされている既存のデバイスからルールセットを作成することはできません。
- カスタム IPS ポリシーをルールセットに関連付けることはできません。

ルールセットに関連付けられたルールのコピーまたは移動

ルールセット内または異なるルールセット間でアクセス制御ルールをコピーまたは移動できます。また、ローカルとルールセット間でルールをコピーまたは移動することもできます。詳細については、「FTD アクセスコントロールルールをコピーする」および「FTD アクセスコントロールルールの移動」を参照してください。

既存のルールセットの自動検出

デバイスをオンボードすると、CDO はデバイス上の既存のルールセットを自動検出し、デバイス上のルールと一致させようとします。一致が成功すると、CDO はルールセットを新しくオンボードされたデバイスに自動的にアタッチします。ただし、デバイス上の同じルールセットに一致するルールセットが複数ある場合、それらはどれもアタッチされないため、手動で割り当てる必要があります。

FTD に対するルールセットの設定

以下のセクションを使用して、ルールセットを作成し展開します。

手順

ステップ 1 FTD に対するルールセットの設定。

a) 新しいルールセットを作成し、それにルールを割り当てます。
b) オブジェクトをルールに割り当てます。
c) ルールセットの優先順位を設定します。
d) 必要に応じてルールの順序を変更します。

ステップ 2 FTD に対するルールセットの設定。

a) 複数のデバイスをルールセットに割り当てます。
b) ルールセットを確認してデバイスに展開します。

ルールセットの作成または編集

ルールセットを作成し、新しいアクセス制御ルールをそのルールセットに追加できます。

複数の FTD デバイスのルールセットを作成するには、次の手順を使用します。

手順

ステップ 1 ナビゲーションウィンドウで、[ポリシー（Policies）]>[FTDルールセット（FTD Rulesets）]を選択します。

ステップ 2 プラス  ボタンをクリックして、新しいルールセットを作成します。

（注） 既存のルールを編集するには、ルールセットを選択して、編集アイコン をクリックします。

ステップ 3 ルールセット名を入力し、[作成（Create）]をクリックします。

ステップ 4 アクセス制御ルールを作成して、ルールセットに追加します。詳細については、「FTD アクセス コントロール ポリシーの設定」を参照してください。

（注） ルールセットのアクセス制御ルールは、ユーザー基準をサポートしていません。

ステップ 5 ウィンドウの右上隅で、ルールセットの優先順位 

を選択します。優先順位は、デバイスがルールセットに割り当てられていないときに設定できます。選択した優先順位は、このルールセットに含まれるすべてのルールと、デバイスでの処理方法に影響します。

- [最上位（Top）]：このルールセットは、デバイス上の他のすべてのルールの前に処理されます。ルールがルールリストの一番上に配置され、最初に処理されます。このポリシーのルールの前に他のルールセットを配置することはできません。デバイスごとに最上位ルールセットを 1 つだけ設定できます。
- [最下位（Bottom）]：このルールセットは、デバイス上の他のすべてのルールの後に処理されます。ポリシーのデフォルトアクションを除き、他のルールセットはこのポリシーのルールを継承できません。デバイスごとに最下位ルールセットを 1 つだけ設定できます。デフォルトでは、優先順位は [最下位（Bottom）] に設定されます。

[ローカルルール（Local Rules）] には、そのデバイス固有のルールがすべて表示されます。

（注） ルールセットがデバイスに割り当てられている場合、優先順位は変更できません。デバイスを切り離してから優先順位を変更する必要があります。

ステップ 6 [保存（Save）]をクリックします。必要な数だけルールを作成できます。

ステップ 7 （オプション）自分で作成したルールの場合、ルールを選択して、[コメントを追加（Add Comments）]フィールドでコメントを追加できます。ルールコメントに関する詳細については、「FTD ポリシーとルールセットのルールにコメントを追加する」を参照してください。

（注）
- ルールセットにデバイスが割り当てられている場合でも、ルールセット内のルールの順序を変更できます。ルールセットの優先順位を変更するには、次の手順を実行します。
  1. ナビゲーションウィンドウで、[ポリシー（Policies）] > [ルールセット（Rulesets）] をクリックし、変更するルールセットを選択します。
  2. 移動するルールを選択します。
  3. ルールの行内にカーソルを置き、上向き または下向き 矢印を使用して、ルールを目的の順序に移動します。
- CDO では、ルールセット内のルールに関連付けられたオブジェクトを上書きできます。新しいオブジェクトをルールに追加する場合、デバイスをルールセットに接続して変更を保存しないと、オブジェクトを上書きできません。

複数の FTD デバイスまたはテンプレートにルールセットを展開する

ルールを適用するには、デバイスまたはテンプレートにルールセットを割り当てる必要があります。変更を確認したら、デバイスに設定を展開できます。テンプレートを新しい FTD デバイスに適用すると、テンプレートに含まれるルールセットがデバイスにプッシュされます。

詳細については、「FTD ルールセットと FTD テンプレート」を参照してください。

はじめる前に知っておくべき情報は以下のとおりです。

- ルールセットは、CDO にオンボード済みの FTD デバイスにのみ割り当てることができます。
- デバイスには、下位または上位のルールセットを **1 つ**だけ設定できます。
- ルールセットにデバイスを割り当てまたは割り当て解除すると、変更は CDO にステージングされますが展開されないため、デバイスは CDO と**非同期**の状態になります。画面の右上隅にある アイコンをクリックして、変更をデバイスに展開します。
- デバイスを割り当てた後、ルールセットに関連付けられた新しいルールは、デバイスに関連付けられている既存のルールを上書きしません。

次の 2 つの方法で、ルールセットをデバイスに関連付けることができます。

- [ルールセット（Ruleset）] ページでルールセットにデバイスを追加する。
- [デバイスポリシー（Device Policy）] ページでデバイスにルールセットを追加する。

[ルールセット（Ruleset）] ページでルールセットにデバイスを追加する

手順

ステップ 1 ナビゲーションウィンドウで、[ポリシー（Policies）]>[FTDルールセット（FTD Rulesets）] を選択します。

ステップ 2 FTD デバイスに割り当てるルールセットを選択し、[アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 右上の [ルールセットの対象（Ruleset for）] の横にある [デバイス（Device）] ボタン 

をクリックします。

ステップ 4 FTD デバイスを候補リストから選択します。

ステップ 5 歯車アイコンをクリックして、ルールセット内のルールとデバイス固有のルールとの間で重複した名前が特定された場合にシステムが実行するアクションを次から 1 つ選択します。

- [競合するルールで処理中断（Fail on conflicting rules）]（デフォルトオプション）：CDO はルールセットをデバイスに追加しません。重複するルール名を手動で変更してから、ルールセットを追加する必要があります。
- [競合するルール名を変更（Rename conflicting rules）]：CDO は、デバイス上の競合するルール名を変更します（ローカルルール）。

ステップ 6 [保存（Save）] をクリックします。[デバイスに割り当てられたルールセット（Attached Ruleset to Devices）] ウィザードが閉じられます。

ステップ 7 右上隅の [保存（Save）] をクリックして、ルールセットの変更内容を保存します。ルールセットを保存すると、変更は CDO にステージングされます。

（注） ルールセットを変更するたびに、[保存（Save）] をクリックする必要があります。この操作を行うと、すべての変更が CDO にステージングされます。変更は手動で展開する必要があります。

ステップ 8 [確認（Confirm）] をクリックします。ルールセットを保存すると、変更は CDO にステージングされます。

ステップ 9 行った変更をすべてのデバイスの設定変更のプレビューと展開か、複数の変更を後から一度に展開します。デバイスでステージングされたルールセットの変更を変更の破棄（Discard Changes）する場合は、「ステージングされたルールセットの変更破棄による影響」を参照してください。

[デバイスポリシー（Device Policy）] ページでデバイスにルールセットを追加する

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、該当するデバイスをリストから選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 5 ウィンドウの右上隅に表示される  ボタンをクリックします。

ステップ 6 必要なルールセットを選択します。

ステップ 7 歯車アイコンをクリックして、ルールセット内のルールとデバイス固有のルールとの間で重複した名前が特定された場合にシステムが実行するアクションを次から 1 つ選択します。

- [競合するルールで処理中断（Fail on conflicting rules）]（デフォルトオプション）：CDO はルールセットをデバイスに追加しません。重複するルール名を手動で変更してから、ルールセットを追加する必要があります。
- [競合するルール名を変更（Rename conflicting rules）]：CDO は、デバイス上の競合するルール名を変更します（ローカルルール）。

（注） 選択したデバイスに競合するルールがない場合、CDO はルールセットを変更せずにデバイスに関連付けます。

ステップ 8 [ルールセットの割り当て（Attach Ruleset）] をクリックします。ルールセットは、ルールセットの優先順位に基づいてデバイスに追加されます。

ステップ 9 行った変更をすべてのデバイスの設定変更のプレビューと展開か、複数の変更を後から一度に展開します。デバイスでステージングされたルールセットの変更を変更の破棄（Discard Changes）する場合は、「ステージングされたルールセットの変更破棄による影響」を参照してください。

関連情報：

- FTD ルールセット
- FTD ルールセットと FTD テンプレート
- 選択したルールセットからの FTD デバイスの分離
- ルールとルールセットの削除
- ルールセットのアウトオブバンド変更による影響
- FTD ルールとルールセットの表示

- ルールセット作成後のログエントリの変更
- 既存のデバイスルールを使用したルールセットの作成

FTD ルールセットと FTD テンプレート

CDO では、FTD テンプレートにルールセットを割り当てることができます。

- ルールセットを使用して FTD デバイスでテンプレートを作成すると、CDO では、ソースデバイスの既存のルールセットにテンプレートが自動的に追加されます。テンプレートはルールセットから管理できます。
- ルールセットが割り当てられたテンプレートをターゲット FTD デバイスに適用すると、CDO ではターゲットデバイスがルールセットに自動的に追加されるため、ターゲットデバイスはルールセットから管理されます。
- ルールセットが割り当てられたテンプレートを別のルールセットを持つターゲット FTD デバイスに適用すると、CDO ではターゲットデバイスから既存のルールセットが削除され、テンプレートに関連付けられた新しいルールセットが追加されます。

詳細については、「複数の FTD デバイスまたはテンプレートにルールセットを展開する」を参照してください。

関連情報：

- FTD ルールセット
- FTD に対するルールセットの設定
- 既存のデバイスルールを使用したルールセットの作成
- ルールセットのアウトオブバンド変更による影響
- FTD ルールとルールセットの表示
- ルールセット作成後のログエントリの変更
- 選択したルールセットからの FTD デバイスの分離
- ルールとルールセットの削除

既存のデバイスルールを使用したルールセットの作成

FTD デバイスで既存のルールを選択することで、ルールセットを作成できます。

既存のデバイスルールからルールセットを作成するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、該当するデバイスをリストから選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。デバイスの既存のルールが表示されます。

ステップ 5 要件に基づいて、以下を実行します。

a) [上位（Top）] ルールを作成するには、最上位のルールから順にルールを選択します。

b) [下位（Bottom）] ルールを作成するには、最下位のルールが最後になるように順番にルールを選択します。

ステップ 6 右側の [アクション（Actions）] ペインで [ルールセットの作成（Create Ruleset）] をクリックします。

（注） 選択に最初または最後のルールを含めると、[ルールセットの作成（Create Ruleset）] リンクをクリックできるようにするになります。

ステップ 7 [ルールセット名（Ruleset Name）] フィールドに名前を指定し、[作成（Create）] をクリックします。対応するルールセットがデバイスに作成されます。

デバイス内の残りのルールを使用して、引き続きルールセットを作成できます。

ルールセットのアウトオブバンド変更による影響

FDM を使用して新しいルールを追加するか、既存のルールを変更すると、FTD に対する CDO の競合検出が有効になっている場合、CDO ではアウトオブバンドの変更が検出され、デバイスの設定ステータスに [競合検出（Conflict Detected）] と表示されます。設定の競合の解決。

デバイスの変更を受け入れると、最後に認識された設定がデバイスでの新しい変更によって上書きされます。変更は次のように行われます。

- 変更の影響を受けるルールセットは、デバイスとの関連付けを失います。
- これらのルールセットに関連付けられたルールは、ローカルルールに変換されます。

デバイスの変更を拒否すると、CDO は新しい変更を拒否し、デバイスの設定を CDO で最後に同期された設定に置き換えます。

関連情報：

- FTD ルールセット
- FTD に対するルールセットの設定
- 既存のデバイスルールを使用したルールセットの作成
- ステージングされたルールセットの変更破棄による影響
- FTD ルールとルールセットの表示

- ルールセット作成後のログエントリの変更
- 選択したルールセットからの FTD デバイスの分離
- ルールとルールセットの削除

ステージングされたルールセットの変更破棄による影響

ルールセットに新しいルールを追加したり、CDO を使用してルールセットに関連付けられた既存のルールを変更すると、変更内容は設定ファイルの独自のコピーに保存されます。これらの変更は、デバイスに「展開」されるまで、CDO で「保留中」と見なされます。

デバイスで保留中のルールセットの変更を変更の破棄（Discard Changes）すると、CDO はデバイスに保存されている設定でデバイス設定のローカルコピーを**完全に上書き**します。

ルールセットおよび関連するデバイスでは、次の変更が発生します。

- 変更の影響を受けるルールセットは、デバイスとの関連付けを失います。
- これらのルールセットに関連付けられたルールは、ローカルルールに変換されます。
- CDO では、新たにステージングされた変更が破棄されて、デバイスに存在する設定が保持されます。

関連情報：

- FTD ルールセット
- FTD に対するルールセットの設定
- 既存のデバイスルールを使用したルールセットの作成
- ルールセットのアウトオブバンド変更による影響
- FTD ルールとルールセットの表示
- ルールセット作成後のログエントリの変更
- 選択したルールセットからの FTD デバイスの分離
- ルールとルールセットの削除

FTD ルールとルールセットの表示

[デバイスポリシー（Device Policy）] ページでルールを表示する

FTD の [デバイスポリシー（Device Policy）] ページには、個別（ローカル）および共有ルール（ルールセットに関連付けられている）が表示されます。

ポリシーページから FTD ルールセットを表示するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、該当するデバイスを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。設定に基づいて、次のルールが表示されます。

- [上位ルール（Top Rules）]：デバイス上の他のすべてのルールの前に処理される必須の共有ルールが表示されます。
- [ローカルルール（Local Rules）]：デバイスの必須ルールの後に処理されるデバイス固有のルールが表示されます。
- [下位（Bottom）]：デバイス上の他のすべてのルールの後に処理されるデフォルトの共有ルールが表示されます。

（注） 対応するルールセットページに移動して、ルールセットを編集できます。

a) ルールセットヘッダーの右上隅で、[ルールセットに移動（Go to ruleset）] をクリックします。
b) ルールを変更したら、[保存（Save）] をクリックします。新しい変更は、ルールセットに関連付けられているすべてのデバイスで更新されます。

ルールセットの表示

[ルールセット（Rulesets）] ページには、テナントで使用可能なすべてのルールセットが表示されます。また、ルールセットに関連付けられたデバイスについての情報も提供します。

[ルールセット（Rulesets ）] ページからすべてのルールセットを表示するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[ポリシー（Policies）]>[ルールセット（Rulesets）] を選択します。テナントで使用可能なルールが表示されます。

ステップ 2 ルールセットをクリックして、その詳細を表示します。[デバイス（Rulesets）] 列には、各ルールセットに割り当てられている FTD デバイスの数が表示されます。

ステップ 3 [管理（Management）] ペインで、[ワークフロー（Workflows）] をクリックします。このページには、デバイスで実行したすべての操作が表示されます。[ダイアグラム（Diagram）] をクリックすると、ワークフローが図で示されます。

ルールセットの検索

[デバイスでフィルタ処理（Filter by Device）] のフィルタ機能でデバイスを選択し、そのデバイスに割り当てられたルールセットを表示できます。

手順

ステップ 1 ナビゲーションウィンドウで、[ポリシー（Policies）]>[ルールセット（Rulesets）] を選択します。

ステップ 2 フィルタアイコンをクリックし、[デバイスでフィルタ処理（Filter by Device）] をクリックします。

ステップ 3 リストから 1 つ以上のデバイスを選択し、[OK] をクリックします。

選択したデバイスに基づいてルールセットが表示されます。

ルールセットと関連するジョブの表示

[ジョブ（Jobs）] ページには、ルールセットを FTD デバイスに適用したとき、または FTD デバイスからルールセットを削除したときのアクションが記録されます。また、アクションが成功したか失敗したかが示されています。

手順

ステップ 1 ナビゲーションウィンドウで、[ポリシー（Policies）]>[ルールセット（Rulesets）] を選択します。

ステップ 2 ルールセットをクリックして、その詳細を表示します。

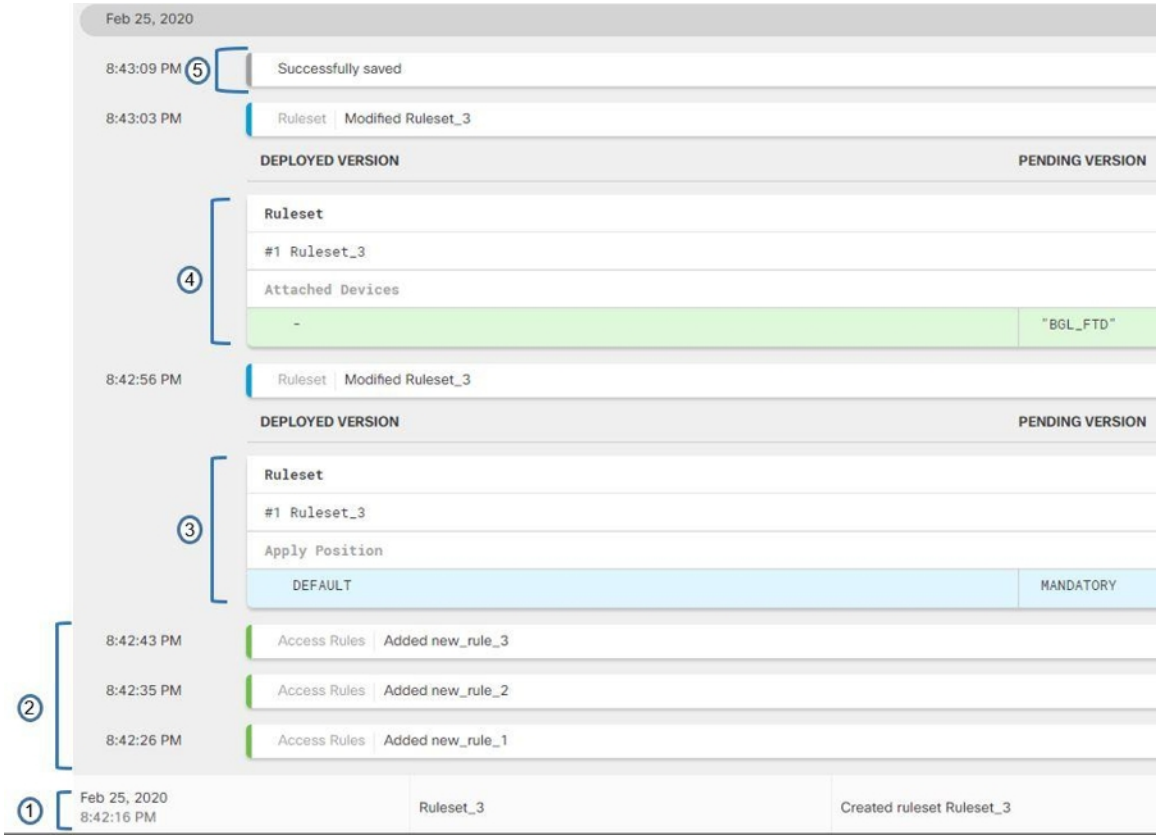
ステップ 3 [管理（Management）] ペインで、[ジョブ（Jobs）] をクリックします。このページには、ルールセットで実行したアクションが表示されます。

ルールセット作成後のログエントリの変更

CDO はルールセットで変更を検出すると、そのルールセットで実行されたすべてのアクションに関する変更ログエントリを作成します。

変更ログエントリの行にある青色の [差分（Diff）] リンクをクリックすると、実行コンフィギュレーション ファイルのコンテキストで変更が並べて表示されるため、変更を対比できます。変更ログの差分の表示

次の例では、3 つのルールが追加された新しいルールセットに関するエントリが変更ログに示されています。また、ルールセットの優先順位とルールセットに割り当てられている FTD デバイスの設定に関する情報も表示されます。



図の番号	説明
1	新しいルールセット「Ruleset_3」は、2020 年 2 月 25 日の午前 11:03:18 に作成されています。
2	ルールセット内に、新しいアクセスルール「new_rule_1」、「new_rule_3」、「new_rule_3」が作成されます。
3	ルールセットの優先順位は「必須」に設定されます。
4	ルールセットは「BGL_FTD」デバイスに割り当てられます。
5	ルールセットの変更が保存されます。

選択したルールセットからの FTD デバイスの分離

ルールセットからデバイスを分離するには、次の手順を使用します。

手順

ステップ 1 ナビゲーションウィンドウで、[ポリシー（Policies）]>[ルールセット（Rulesets）] を選択します。

ステップ 2 編集するルールセットを選択し、[アクション（Actions）] ペインの [編集（Edit）] リンクをクリックします。

ステップ 3 右上の [ルールセットの対象（Ruleset for）] の横にある [デバイス（Device）] ボタンをクリックします。

ステップ 4 ルールセットに現在割り当てられているデバイスのチェックボックスをオフにするか、[クリア（Clear）] をクリックしてすべてのデバイスを一度に削除します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 右上のウィンドウで [保存（Save）] をクリックして、ルールセットを保存します。ポリシーを保存すると、変更は CDO にステージングされます。

ステップ 7 行った変更をすべてのデバイスの設定変更のプレビューと展開か、複数の変更を後から一度に展開します。

関連情報：

- FTD ルールセット
- FTD に対するルールセットの設定
- 既存のデバイスルールを使用したルールセットの作成
- ルールセットのアウトオブバンド変更による影響
- FTD ルールとルールセットの表示
- ルールセット作成後のログエントリの変更
- ルールとルールセットの削除

ルールとルールセットの削除

ルールセットからのルールの削除

ルールセットで不要になったルールを削除できます。

ルールを削除するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[ポリシー（Policies）]>[ルールセット（Rulesets）]をクリックし、ルールセットを選択します。

ステップ 2 [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 削除するルールを選択し、[アクション（Actions）] の下の [削除（Remove）] をクリックします。

ステップ 4 [OK] をクリックして、削除を実行します。

ステップ 5 右上隅の [保存（Save）]をクリックして、ルールセットの変更内容を保存します。ルールセットを保存すると、変更は CDO にステージングされます。

ステップ 6 変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、複数の変更を後から一度に展開します。

ルールセットの削除

ルールセットを削除できるのは、ルールセットに関連付けられているすべてのデバイスを切り離した後に限られます。「ルールとルールセットの削除」を参照してください。

ルールセットを削除するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、[ポリシー（Policies）]>[ルールセット（Rulesets）]をクリックし、削除するルールセットを選択します。

ステップ 2 ルールセット行内の [削除（Remove）] をクリックします。

ステップ 3 [確認（Confirm）] をクリックして、ルールセットを完全に削除します。

ステップ 4 変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、後から複数の変更を一度に展開します。

- FTD ルールセット
- FTD に対するルールセットの設定
- 選択したルールセットからの FTD デバイスの分離

選択した FTD デバイスからのルールセットの削除

選択した FTD デバイスからルールセットを削除する方法は 2 通りあり、操作が若干異なります。

- 選択した FTD デバイスからのルールセットの削除：この機能は、選択した FTD デバイスからルールセットとそれに関連付けられた共有ルールを削除します。

- 選択した FTD デバイスとルールセットの関連付け解除：この機能は共有ルールを削除しません。代わりに、共有ルールをローカルルールに変換します。

選択した FTD デバイスからのルールセットの削除

選択したFTDデバイスからルールセットとそれに関連付けられた共有ルールを削除できます。ルールセットページでは、選択したルールセットからのFTDデバイスの分離こともできます。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、該当するデバイスをリストから選択します。

ステップ 4 ルールセットの右上隅に表示される削除アイコンをクリックします。

ステップ 5 [確認（Confirm）] をクリックします。

ステップ 6 行った変更をすべてのデバイスの設定変更のプレビューと展開か、複数の変更を後から一度に展開します。

選択した FTD デバイスとルールセットの関連付け解除

新しいデバイス固有のルールを FTD デバイスのルールセットに追加する場合は、そのルールセットと FTD の関連付けを解除する必要があります。これにより、関連付けられている共有ルールがローカルルールに変換されます。その後、ローカルルールに必要なルールを追加できます。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、該当するデバイスをリストから選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] をクリックします。

ステップ 5 ルールセットの右上隅に表示される アイコンをクリックします。

ステップ 6 [確認（Confirm）] をクリックします。

ステップ 7 行った変更をすべてのデバイスの設定変更のプレビューと展開か、複数の変更を後から一度に展開します。

FTD ポリシーとルールセットのルールにコメントを追加する

FTDポリシーのルールおよびルールセットのルールにコメントを追加して、ルールのいくつかの特性を文書化できます。ルールコメントは CDO でのみ表示されます。FTD に書き込まれることも、FDM に表示されることもありません。

コメントは、ルールが作成されて CDO に保存された後で、ルールに追加されます。ルールコメントはCDOの機能にすぎないため、ルールコメントを作成、変更、または削除しても、CDO 内のデバイスの設定ステータスは [未同期（Not Synced）] に変更されません。ルールコメントを保存するために、CDO から FTD に変更を書き込む必要はありません。

FTDポリシーのルールに関連付けられたコメントは、デバイスのポリシーページで表示および編集できます。FTDルールセットのルールに関連付けられたコメントは、ルールセットページで表示および編集できます。ルールセットがポリシーで使用されている場合、ルールセット内のいずれかのルールに関連付けられているコメントは、ポリシーのコメント領域に表示されます。コメントは読み取り専用です。

ポリシー、ルールセット、または変更ログで文字列を検索すると、CDO は、ルールに関連付けられたコメントで文字列を検索し、ルールのその他の属性や値も検索します。

ルールのコメントが追加または編集されると、そのアクションが変更ログに記録されます。ルールコメントは CDO でのみ記録および維持されるため、変更ログでは「CDO-only change」というラベルが付けられます。

⚠

注意 FTD デバイスの設定にアウトオブバンドの変更があり、CDO がその設定をデータベースに読み込んだ場合、ルールに関連付けられたコメントはすべて消去されます。

ルールへのコメントの追加

手順

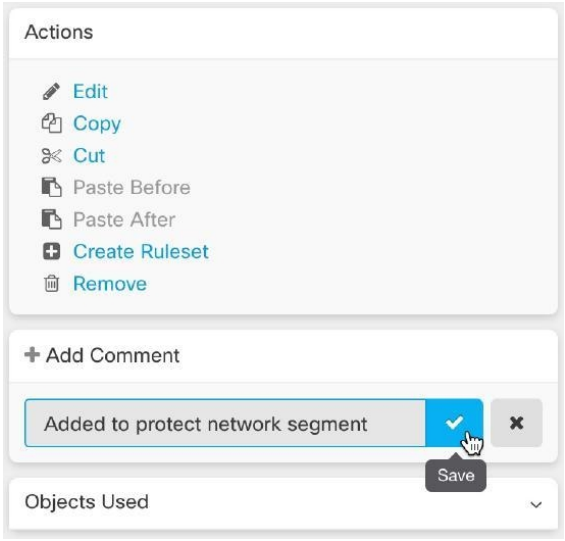
ステップ 1 コメントするルールがあるポリシーまたはルールセットを開きます。

ステップ 2 ルールを選択します。

ステップ 3 ルールの [コメントの追加（Add Comment）] 領域で [コメントの追加（Add Comment）] をクリックします。

ステップ 4 テキストボックスにコメントを入力します。

ステップ 5 [保存（Save）] をクリックします。



FTD ポリシーとルールセット内のルールに関するコメントの編集

ポリシー内のルールに関するコメントの編集

FTD ポリシー内のルールに関するコメントを編集するには、次の手順を実行します。

手順

ステップ 1 CDO メニューバーから、[ポリシー（Policies）]>[FTD/Meraki/AWSポリシー（FTD/Meraki/AWS Policies）] を選択します。

ステップ 2 コメントを追加するローカルルールがある FTD ポリシーを選択します。ポリシー内のルールセットのルールにコメントを追加することはできません。

ステップ 3 [コメント（Comment）] ペインで、編集アイコン をクリックします。

ステップ 4 コメントを編集して、[保存（Save）] をクリックします。[コメント（Comment）] 領域にコメントの変更がすぐに反映されます。

ルールセット内のルールに関するコメントの編集

ルールセット内のルールに関するコメントの変更がポリシーページに反映されるようにするには、コメントとルールを特定の順序で変更する必要があります。

手順

ステップ 1 CDO ナビゲーションパネルから、[ポリシー（Policies）] > [FTDルールセット（FTD Rulesets）] を選択します。

ステップ 2 コメントを追加するルールを含むルールセットを選択します。

ステップ 3 [アクション（Actions）] ペインで、[編集（Edit）] をクリックします。

ステップ 4 ルールを選択します。

ステップ 5 [コメント（Comment）] ペインで、編集アイコン をクリックします。

ステップ 6 コメントを編集して、[保存（Save）] をクリックします。ルールセットページのコメント領域にコメントの変更がすぐに反映されます。

ステップ 7 変更するルールを選択し、操作ウィンドウで [編集（Edit）] をクリックします。

ステップ 8 ルールを編集したら、青いチェックボタンをクリックして変更を保存します。

ステップ 9 ルールセットページの上部で、[保存（Save）] をクリックしてルールセットを保存します。ルールセット内のルールの新しいコメントがすぐにポリシーページに反映されます。

ステップ 10 ポリシーページでコメントの変更を確認するには、次の手順を実行します。

a) CDO メニューバーから、[ポリシー（Policies）] > [FTD/Meraki/AWSポリシー（FTD/Meraki/AWS Policies）] を選択します。

b) 編集したルールセットを含む FTD ポリシーを選択します。

c) コメントを編集したルールを選択します。[コメント（Comment）] ウィンドウに新しいコメントが表示されることを確認します。

ネットワーク アドレス変換

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、企業のプライベートネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

ネットワーク アドレス変換（NAT）の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベート アドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アドレスを節約します。これは、ネットワーク全体に対して 1 つのパ

ブリック アドレスだけを外部に最小限にアドバタイズするように NAT を設定できるためです。

NAT の他の機能には、次のおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティングソリューション：NAT を使用する際に、重複 IP アドレスが問題になりません。
- 柔軟性：外部で使用可能なパブリックアドレスに影響を与えずに、内部 IP アドレス方式を変更できます。たとえば、インターネットにアクセス可能なサーバーの場合、インターネット用に固定 IP アドレスを維持できますが、内部向けにサーバーのアドレスを変更することができます。
- IPv4 と IPv6（ルーテッドモードのみ）の間の変換：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換を行うことができます。

Cisco Defense Orchestrator を使用して、さまざまな使用例の NAT ルールを作成できます。NAT ルールウィザードまたは次のトピックを使用して、さまざまな NAT ルールを作成します。

NAT ルールの処理命令

ネットワークオブジェクトの NAT ルールおよび Twice NAT ルールは、3 つセクションに分割された 1 つのテーブルに格納されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

表 *5 : NAT* ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	Twice NAT（ASA） 手動 NAT（FTD）	設定に登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、Twice NAT ルールはセクション 1 に追加されます。

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 2	ネットワークオブジェクト NAT（ASA） 自動 NAT（FTD）	セクション1で一致が見つからない場合、セクション2のルールが次の順序で適用されます。 **1.** スタティック ルール **2.** ダイナミック ルール **各ルールタイプでは、次の順序ガイドラインが使用されます。** **1.** 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 **2.** 数量が同じ場合には、IP アドレス番号（最小から最大まで）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 **3.** 同じIPアドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、オブジェクト「Arlington」はオブジェクト「Detroit」の前に評価されます。
セクション 3	Twice NAT（ASA） 手動 NAT（FTD）	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24（スタティック）
- 192.168.1.0/24（ダイナミック）
- 10.1.1.0/24（スタティック）
- 192.168.1.1/32（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト Detroit）

- 172.16.1.0/24（ダイナミック）（オブジェクト Arlington）

この結果、使用される順序は次のとおりです。

- 192.168.1.1/32（スタティック）
- 10.1.1.0/24（スタティック）
- 192.168.1.0/24（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト Arlington）
- 172.16.1.0/24（ダイナミック）（オブジェクト Detroit）
- 192.168.1.0/24（ダイナミック）

ネットワークアドレス変換ウィザード

ネットワークアドレス変換（NAT）ウィザードは、次のタイプのアクセスに使用するNATルールをデバイスで作成する際に役立ちます。

- **内部ユーザーのインターネットアクセスを有効にする**。この NAT ルールを使用して、内部ネットワーク上のユーザーがインターネットにアクセスできるようにすることができます。
- **内部サーバーをインターネットに公開する**。この NAT ルールを使用して、ネットワーク外のユーザーが内部 Web サーバーまたは電子メールサーバーにアクセスできるようにすることができます。

「内部ユーザーのインターネットアクセスを有効にする」ための前提条件

NAT ルールを作成する前に、次の情報を収集します。

- ユーザーに最も近いインターフェイス。通常これは「内部」インターフェイスと呼ばれます。
- インターネット接続に最も近いインターフェイス。通常これは「外部」インターフェイスと呼ばれます。
- 特定のユーザーのみにインターネットへのアクセスを許可する場合は、それらのユーザーのサブネットアドレスが必要です。

「内部サーバーをインターネットに公開する」ための前提条件

NAT ルールを作成する前に、次の情報を収集します。

- ユーザーに最も近いインターフェイス。通常これは「内部」インターフェイスと呼ばれます。
- インターネット接続に最も近いインターフェイス。通常これは「外部」インターフェイスと呼ばれます。

- インターネット側の IP アドレスに変換する、ネットワーク内のサーバーの IP アドレス。
- サーバーが使用するパブリック IP アドレス。

次の作業

NAT ウィザードを使用した NAT ルールの作成 （228 ページ） を参照してください。

NAT ウィザードを使用した NAT ルールの作成

始める前に

NAT ウィザードを使用して NAT ルールを作成するために必要な前提条件については、 ネットワークアドレス変換ウィザード （227 ページ）を参照してください。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 フィルタと 検索フィールドを使用して、NAT ルールを作成するデバイスを見つけます。

ステップ 5 詳細パネルの [管理（Management）] 領域で、[NAT] NAT をクリックします。

ステップ 6 + > [NAT ウィザード（NAT Wizard）] をクリックします。

ステップ 7 NAT ウィザードの質問に回答し、画面の指示に従います。

- NAT ウィザードはネットワーク オブジェクトを使用してルールを作成します。ドロップダウンメニューから既存のオブジェクトを選択するか、作成ボタン + Create... で新しいオブジェクトを作成します。
- NAT ルールを保存する前に、すべての IP アドレスをネットワークオブジェクトとして定義する必要があります。

ステップ 8 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

NAT の一般的な使用例

Twice NAT と手動 NAT

「自動 NAT」とも呼ばれる「ネットワークオブジェクト NAT」を使用して達成できるいくつかの一般的なタスクを次に示します。

- 内部ネットワーク上のサーバーがパブリック IP アドレスを使用してインターネットに到達できるようにする （229 ページ）
- 内部ネットワーク上のユーザーが外部インターフェイスのパブリック IP アドレスを使用してインターネットにアクセスできるようにする （231 ページ）
- 内部ネットワーク上のサーバーをパブリック IP アドレスの特定のポートで使用できるようにする （232 ページ）
- プライベート IP アドレス範囲のパブリック IP アドレス範囲への変換 （236 ページ）

ネットワークオブジェクト NAT と自動 NAT

「手動 NAT」とも呼ばれる「Twice NAT」を使用して達成できる一般的なタスクを次に示します。

- 外部インターフェイスを通過する際に IP アドレスの範囲が変換されるのを防ぐ （237 ページ）

内部ネットワーク上のサーバーがパブリック IP アドレスを使用してインターネットに到達できるようにする

使用例

インターネットからアクセスする必要があるプライベート IP アドレスを持つサーバーがあり、1 つのパブリック IP アドレスからプライベート IP アドレスへの NAT に十分なパブリック IP アドレスがある場合は、この NAT 戦略を使用します。パブリック IP アドレスの数に限りがある場合は、「内部ネットワーク上のサーバーをパブリック IP アドレスの特定のポートで使用できるようにする」を参照してください（このソリューションの方が適している可能性があります）。

方法

サーバーは静的なプライベート IP アドレスを持ち、そのサーバーにネットワークの外部のユーザーがアクセスできる必要があります。静的プライベート IP アドレスを静的パブリック IP アドレスに変換するネットワークオブジェクト NAT ルールを作成します。その後、そのパブリック IP アドレスからのトラフィックがプライベート IP アドレスに到達できるようにするアクセスポリシーを作成します。最後に、これらの変更をデバイスに展開します。

始める前に

まず始めに、2 つのネットワークオブジェクトを作成します。一方のオブジェクトを「*servername*_inside」と名前を付け、もう一方のオブジェクトに「*servername*_outside」という名前を付けます。*servername*_inside ネットワークオブジェクトには、サーバーのプライベート IP アドレスが含まれている必要があります。*servername*_outside ネットワークオブジェクトには、サーバーのパブリック IP アドレスが含まれている必要があります。手順については、「ネットワークオブジェクトの作成」を参照してください。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6 + > [ネットワーク オブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1の [タイプ（Type）] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

1. [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、**servername_inside** オブジェクトを選択します。
2. [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、**servername_outside** オブジェクトを選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 ASA の場合はネットワークポリシールールを展開し、FTD の場合はアクセス制御ポリシールールを展開して、*servername*_inside から *servername*_outside へのトラフィックフローを可能にします。

ステップ 14 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

内部ネットワーク上のユーザーが外部インターフェイスのパブリックIPアドレスを使用してインターネットにアクセスできるようにする

使用例

外部インターフェイスのパブリックアドレスを共有することにより、プライベートネットワーク内のユーザーとコンピューターがインターネットに接続できるようにします。

方法

プライベートネットワーク上のすべてのユーザーがデバイスの外部インターフェイスのパブリック IP アドレスを共有できるようにするポートアドレス変換（PAT）ルールを作成します。

プライベートアドレスがパブリックアドレスとポート番号にマッピングされると、デバイスはそのマッピングを記録します。そのパブリック IP アドレスとポート宛の着信トラフィックを受信すると、デバイスはトラフィックを要求したプライベート IP アドレスにトラフィックを送り返します。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6  [ネットワークオブジェクトNAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1 の [タイプ（Type）] で、[ダイナミック（Dynamic）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション2の[インターフェイス（Interfaces）]で、送信元インターフェイスには[任意（any）]を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

1. [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、ネットワーク構成に応じて [any-ipv4] オブジェクトまたは [any-ipv6] オブジェクトを選択します。
2. [変換済みアドレス（Translated Address）] メニューを展開し、利用可能なリストから [インターフェイス（interface）] を選択します。インターフェイスにより、外部インターフェイスのパブリックアドレスを使用することが示唆されています。

ステップ 10 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

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すべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ASA の保存済み構成ファイルのエントリ

この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD デバイスには適用されません。

この手順によって作成されるオブジェクト：

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

この手順によって作成される *NAT* ルール：

```
object network any_network
nat (any,outside) dynamic interface
```

内部ネットワーク上のサーバーをパブリックIPアドレスの特定のポートで使用できるようにする

使用例

パブリック IP アドレスが 1 つしかない場合、または数が非常に限られている場合は、静的 IP アドレスとポートにバインドされた受信トラフィックを内部アドレスに変換するネットワークオブジェクト NAT ルールを作成できます。特定のケースの手順を提供していますが、これらはサポートされている他のアプリケーションのモデルとして使用できます。

前提条件

まず始めに、FTP、HTTP、および SMTP サーバーのネットワークオブジェクトを 1 つずつ、合計 3 つの個別のオブジェクトを作成します。この手順のために、これらのオブジェクトを **ftp-server-object**、**http-server-object**、および **smtp-server-object** と呼びます。手順については、「」「ネットワークオブジェクトの作成」を参照してください。

FTP サーバーへの NAT 着信 FTP トラフィック

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6 > [ネットワーク オブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1の [タイプ（Type）] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

- [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、**ftp**-server-object を選択します。
- [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、[インターフェイス（Inerface）] を選択します。
- [ポート変換の使用（Use Port Translation）] にチェックを付けます。
- [tcp]、[ftp]、[ftp] を選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [保存（Save）] をクリックします。NAT テーブルの NAT ルールの処理命令 に新しいルールが作成されます。

ステップ 13 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

HTTP サーバーへの NAT 着信 HTTP トラフィック

パブリック IP アドレスが 1 つしかない場合、または数が非常に限られている場合は、静的 IP アドレスとポートにバインドされた受信トラフィックを内部アドレスに変換するネットワークオブジェクト NAT ルールを作成できます。特定のケースの手順を提供していますが、これらはサポートされている他のアプリケーションのモデルとして使用できます。

始める前に

まず始めに、HTTP サーバーのネットワークオブジェクトを作成します。この手順のために、オブジェクトを **http-object** と呼びます。手順については、「」「ネットワークオブジェクトの

作成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作成または編集」を参照してください。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6 > [ネットワーク オブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1の [タイプ（Type）] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

- [オリジナルアドレス（Original Address）] メニューを展開し、[選択]（Choose）] をクリックして、**http** オブジェクトを選択します。
- [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、[インターフェイス（Inerface）] を選択します。
- [ポート変換の使用（Use Port Translation）] にチェックを付けます。
- **tcp**、**http**、http を選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [保存（Save）] をクリックします。NAT テーブルの NAT ルールの処理命令 に新しいルールが作成されます。

ステップ 13 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

SMTP サーバーへの NAT 着信 SMTP トラフィック

パブリック IP アドレスが 1 つしかない場合、または数が非常に限られている場合は、静的 IP アドレスとポートにバインドされた受信トラフィックを内部アドレスに変換するネットワークオブジェクト NAT ルールを作成できます。特定のケースの手順を提供していますが、これらはサポートされている他のアプリケーションのモデルとして使用できます。

始める前に

まず始めに、smtp サーバーのネットワークオブジェクトを作成します。この手順の説明では、オブジェクトを **smtp-object** と呼びます。手順については、「」「ネットワークオブジェクトの作成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作成または編集」を参照してください。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6  > [ネットワーク オブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1の [タイプ（Type）] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

- [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、smtp-server-object を選択します。
- [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、[インターフェイス（Inerface）] を選択します。
- [ポート変換の使用（Use Port Translation）] にチェックを付けます。
- tcp、smtp、smtp を選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [保存（Save）] をクリックします。NAT テーブルの NAT ルールの処理命令 に新しいルールが作成されます。

ステップ 13 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

プライベート IP アドレス範囲のパブリック IP アドレス範囲への変換

使用例

特定のデバイスタイプまたはユーザータイプのグループがあり、IPアドレスを特定の範囲に変換して、受信側デバイス（トランザクションの反対側のデバイス）がトラフィックを許可する必要がある場合は、このアプローチを使用します。

内部アドレスのプールを外部アドレスのプールに変換

始める前に

変換するプライベート IP アドレスプールのネットワークオブジェクトを作成し、それらのプライベート IP アドレスの変換先となるパブリックアドレスプールのネットワークオブジェクトも作成します。

（注） ASA FTD の場合、「変換されたアドレス」のプールを定義するネットワークグループは、サブネットを定義するネットワークオブジェクトにすることはできません。

これらのアドレスプールを作成する場合は、と『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作成または編集』を参照してください。

以下の手順のために、プライベートアドレスプールを**inside_pool**、パブリックアドレスプールを**outside_pool** と名付けました。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6 > [ネットワーク オブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1 の [タイプ（Type）] で [ダイナミック（Dynamic）] を選択し、[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスを [内部（inside）] に設定し、接続先インターフェイスを [外部（outside）] に設定します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、以下のタスクを実行します。

- [元アドレス（Original Address）] で、[選択（Choose）] をクリックし、上記の前提条件セクションで作成した **inside_pool** 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) を選択します。
- [変換されたアドレス（Translated Address）] で、[選択（Choose）] をクリックし、上記の前提条件セクションで作成した **outside_pool** 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) を選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

外部インターフェイスを通過する際に IP アドレスの範囲が変換されるのを防ぐ

使用例

この Twice NAT ユースケースを使用して、サイト間 VPN を有効にします。

方法

IP アドレスのプールをそれ自体に変換して、ネットワークのある場所の IP アドレスが変更されずに別の場所に届くようにします。

Twice NATルールの作成

始める前に

それ自体に変換する IP アドレスプールを定義する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を作成します。FTD の場合、アドレスの範囲は、サブネットを定義するネットワークオブジェクト、または範囲内のすべてのアドレスを含むネットワーク グループ オブジェクトによって定義できます。

ネットワークオブジェクトやネットワークグループを作成する場合は、「」と「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作成または編集」を参照してください。

次の手順では、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を Site-to-Site-PC-Pool と呼びます。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6  > [Twice NAT] をクリックします。。

ステップ 7 セクション 1の [タイプ（Type）] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次の変更を行います。

- [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、前提条件セクションで作成した Site-to-Site-PC-Pool オブジェクトを選択します。
- [変換済みアドレス（Translated Address）] メニューを展開し、[選択（Choose）] をクリックして、前提条件セクションで作成した Site-to-Site-PC-Pool オブジェクトを選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 ASA の場合、クリプトマップを作成します。クリプトマップの作成方法の詳細については、『CLI ブック 3：Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド』の「LAN-to-LAN IPsec VPN」の章を確認してください。

ステップ 14 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

バーチャル プライベートネット ワークの管理

バーチャルプライベートネットワーク（VPN）接続は、インターネットなどのパブリック ネットワークを介してエンドポイント間の安全なトンネルを確立します。

このセクションは、Firepower Threat Defense（FTD）デバイスのリモートアクセスおよびサイト間 VPN についてです。FTD でサイト間 VPN 接続を構築するためのインターネット プロトコル セキュリティ（IPsec）標準について説明しています。また、FTD で VPN 接続を構築し、リモートでアクセスするために使用する SSL 標準についても説明します。

CDO は以下のタイプの VPN 接続をサポートします。

- サイト間仮想プライベートネットワーク （239 ページ）
- リモートアクセス仮想プライベートネットワーク

バーチャルプライベートネットワークの詳細は、『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド』を参照してください。

サイト間仮想プライベートネットワーク

サイト間 VPN トンネルは、地理的に異なる場所にあるネットワークを接続します。管理対象デバイス間、および管理対象デバイスと関連するすべての規格に準拠するその他のシスコまたはサードパーティのピアとの間で、サイト間IPsec接続を作成できます。これらのピアは、IPv4 アドレスと IPv6 アドレスの内部と外部の任意の組み合わせを持つことができます。サイト間トンネルは、Internet Protocol Security（IPsec）プロトコルスイートとインターネット キー エクスチェンジ バージョン 2（IKEv2）を使用して構築されます。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続することができます。

VPN トポロジ

新しいサイト間VPNトポロジを作成するには、一意の名前を付け、トポロジタイプを指定し、IPsec IKEv1 または IKEv2 あるいはその両方に使用される IKE バージョンと認証方式を選択する必要があります。設定したら、トポロジを Firepower Threat Defense デバイスに展開します。

IPsec と IKE

CDO では、サイト間 VPN は、VPN トポロジに割り当てられた IKE ポリシーおよび IPsec プロポーザルに基づいて設定されます。ポリシーとプロポーザルはパラメータのセットであり、これらのパラメータによって、IPsec トンネル内のトラフィックでセキュリティを確保するために使用されるセキュリティ プロトコルやアルゴリズムなど、サイト間 VPN の特性が定義されます。VPN トポロジに割り当て可能な完全な設定イメージを定義するために、複数のポリシータイプが必要となる場合があります。

認証

VPN接続の認証には、各デバイスのトポロジ内で事前共有キーを設定します。事前共有キーにより、IKE 認証フェーズで使用する秘密鍵を 2 つのピア間で共有できます。

バーチャル トンネル インターフェイス（VTI）

CDOは、現在、ASAデバイスまたはFTDデバイス上の仮想トンネルインターフェイス（VTI）トンネルの管理、監視、使用をサポートしていません。VTIトンネルが設定されているデバイスをCDOにオンボーディングすることは可能ですが、VTIインターフェイスは無視されます。セキュリティゾーンまたはスタティックルートが VTI を参照する場合、CDO は VTI 参照を除いてセキュリティゾーンとスタティックルートを読み取ります。VTI トンネルに対する CDO のサポートは近日中に提供されます。

関連情報：

- FTD サイト間仮想プライベートネットワークのモニタリング
- FTD のサイト間 VPN の設定 （248 ページ）

FTD サイト間仮想プライベートネットワークのモニタリング

CDOを使用すると、オンボードFTDデバイスで既存または新たに作成されたサイト間VPN設定を監視、変更、および削除できます。

サイト間 VPN トンネルの接続の確認

[接続の確認（Check Connectivity）]ボタンを使用して、トンネルに対するリアルタイムの接続確認をトリガーし、トンネルの現在の状態（アクティブまたはアイドル）を確認します。サイト間 VPN トンネルを検索してフィルタ処理する （244 ページ）[オンデマンド接続確認（on-demand connectivity check）]ボタンをクリックしていない場合、オンボーディングされているすべてのデバイスで利用可能なすべてトンネルに対する確認が 1 時間に一度実行されます。

（注）
- CDOは、トンネルがアクティブかアイドルかを判断するために、ASAおよびFTDで次の接続確認コマンドを実行します。

  ```
  show vpn-sessiondb l2l sort ipaddress
  ```

- ASA モデルデバイストンネルは常に [アイドル（Idle）] と表示されます。

[VPN] ページからトンネル接続を確認するには、次の手順を実行します。

手順

ステップ 1 メインのナビゲーションバーで、[VPN] > [サイト間VPN（Site-to-Site VPN）] をクリックします。

ステップ 2 サイト間 VPN トンネルのトンネルのリストをサイト間 VPN トンネルを検索してフィルタ処理するして、選択します。

ステップ 3 右側の [アクション（Actions）] ペインで、[接続の確認（Check Connectivity）] をクリックします。

VPN の問題の特定

CDO によって、ASA および FTD デバイスの VPN の問題を特定できます（この機能は、AWS VPC サイト間 VPN トンネルではまだ利用できません）。この記事では次のことを説明します。

- ピアが欠落している VPN トンネルを見つける
- 暗号化キーの問題がある VPN ピアを見つける
- トンネルに対して定義された不完全な、または誤った設定のアクセスリストを見つける
- トンネル設定の問題を見つける

トンネル設定の問題の解決 （243 ページ）

ピアが欠落している *VPN* トンネルを見つける

「Missing IP Peer」状態は、FTD デバイスよりも ASA デバイスで発生する可能性が高くなります。

手順

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN] > [サイト間 VPN（Site-to-Site VPN）]** をクリックして VPN ページを開きます。

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 4 検出された問題を確認します。

ステップ 5 問題を報告している各デバイスを選択し、右側の [ピア（Peers）] ペインを確認します。1 つのピア名がリストされます。CDO は、他のピア名を「[Missing peer IP.]」として報告します。

暗号化キーの問題がある *VPN* ピアを見つける

このアプローチを使用して、以下のような暗号化キーの問題がある VPN ピアを見つけます。

- IKEv1 または IKEv2 キーが無効、欠落しているか、一致しない
- トンネルが古くなっているか、暗号化レベルが低い

手順

ステップ 1 CDO ナビゲーションバーで、[VPN] > [サイト間 VPN（Site-to-Site VPN）] をクリックして VPN ページを開きます。 >

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 4 問題を報告している各デバイスを選択し、右側の [ピア（Peers）] ペインを確認します。ピア情報には、両方のピアが表示されます。

ステップ 5 いずれかのデバイスの [ピアの表示（View Peers）] をクリックします。

ステップ 6 ダイアグラムビューで、問題を報告しているデバイスをダブルクリックします。

ステップ 7 下部の [トンネルの詳細（Tunnel Details）] パネルで [Key Exchange（キー交換）] をクリックします。両方のデバイスを表示して、そこでキーの問題を診断できます。

トンネルに対して定義された不完全な、または誤った設定のアクセスリストを見つける

「アクセスリストが不完全または正しく設定されていない」状態は、ASA デバイスでのみ発生する可能性があります。

手順

ステップ 1 CDO ナビゲーションバーで、[VPN] > [サイト間 VPN（Site-to-Site VPN）] をクリックして VPN ページを開きます。 >

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 4 問題を報告している各デバイスを選択し、右側の [ピア（Peers）] ペインを確認します。ピア情報には、両方のピアが表示されています。

ステップ 5 いずれかのデバイスの [ピアの表示（View Peers）] をクリックします。

ステップ 6 ダイアグラムビューで、問題を報告しているデバイスをダブルクリックします。

ステップ 7 下部の [トンネルの詳細（Tunnel Details）] パネルで [トンネルの詳細（Tunnel Details）] をクリックします。「ネットワーク ポリシー：不完全（Network Policy: Incomplete）」というメッセージが表示されます。

トンネル設定の問題を見つける

トンネル設定のエラーは、次のシナリオで FTD デバイスで発生する可能性があります。

- サイト間 VPN インターフェイスの IP アドレスが変更れたときの、「ピア IP アドレス値が変更されました（Peer IP Address Value has changed）」。

- VPN トンネルの IKE 値が他の VPN トンネルと一致しない場合、「IKE 値が一致しません（IKE value Mismatch）」というメッセージが表示されます。

手順

ステップ 1 CDO ナビゲーションバーで、[VPN] > [サイト間 VPN（Site-to-Site VPN）] をクリックして VPN ページを開きます。 >

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 4 [トンネルの問題（Tunnel Issues）] で、[検出された問題（Detected Issues）] をクリックして、エラーを報告している VPN 設定を表示します。問題を報告している（⚠）設定を表示できます。

ステップ 5 問題を報告している VPN 設定を選択します。

ステップ 6 右側の [ピア（Peers）] ペインに、問題のあるピアに ⚠ アイコンが表示されます。⚠ アイコンにカーソルを合わせると、問題と解決策が表示されます。

次のステップ：トンネル設定の問題の解決。

トンネル設定の問題の解決

この手順では、次のトンネル設定の問題を解決を試みます。

- サイト間 VPN インターフェイスの IP アドレスが変更れたときの、「ピア IP アドレス値が変更されました（Peer IP Address Value has changed）」。
- VPN トンネルの IKE 値が他の VPN トンネルと一致しない場合、「IKE 値が一致しません（IKE value Mismatch）」というメッセージが表示されます。

詳細については、「トンネル設定の問題を見つける」を参照してください。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、問題を報告している VPN 設定に関連付けられているデバイスを選択します。

ステップ 4 [競合検出（Conflict Detected）] ステータスの解決。

ステップ 5 CDO ナビゲーションウィンドウで、**[VPN] > [サイト間 VPN（Site-to-Site VPN）]**をクリックして VPN ページを開きます。

ステップ 6 この問題を報告している VPN 設定を選択します。

ステップ 7 [アクション（Actions）] ペインで、[編集（Edit）] アイコンをクリックします。

ステップ 8 各手順で [次へ（Next）] をクリックして、最後に手順 4 で [完了（Fnish）] ボタンをクリックします。

ステップ 9 すべてのデバイスの設定変更のプレビューと展開 （424 ページ）。

管理対象外 VPN ピアの導入準備

ピアの 1 つがオンボードされると、CDO はサイト間 VPN トンネルを検出します。2 番目のピアが CDO によって管理されていない場合は、VPN トンネルのリストをフィルタリングして、管理されていないデバイスを見つけてオンボードすることができます。

手順

ステップ 1 メインナビゲーションバーで、**[VPN]** > **[サイト間VPN（Site-to-Site VPN）]**を選択して VPN ページを開きます。

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 をクリックしてフィルタパネルを開きます。

ステップ 4 [管理対象外（Unmanaged）] にチェックを入れます。

ステップ 5 結果から管理対象外のデバイスを選択します。

ステップ 6 右側の [ピア（Peers）] ペインで、[デバイスのオンボード（Onboard Device）] をクリックし、画面の指示に従います。

関連情報：

- デバイスとサービスのオンボーディング
- FTD のオンボーディング

サイト間 VPN トンネルを検索してフィルタ処理する

フィルタサイドバーを検索フィールドと組み合わせて使用して、VPN トンネル図に示されている VPN トンネルの検索を絞り込みます。

手順

ステップ 1 メインのナビゲーションバーで、[VPN] > [サイト間 VPN（Site-to-Site VPN）] に進みます。

ステップ 2 フィルタアイコンをクリックしてフィルタペインを開きます。

ステップ 3 これらのフィルタを使用して検索を絞り込みます。

- [デバイスによるフィルタ（Filter by Device）] - [デバイスによるフィルタ（Filter by Device）] をクリックし、[デバイスタイプ（Device Type）] タブを選択し、フィルタ処理で検索するデバイスをチェックします。

- [トンネルの問題（Tunnel Issues）] - トンネルの各サイドで問題が検出されたかどうかでフィルタ処理します。問題のあるデバイスの例には、関連するインターフェイス、ピア IP アドレス、アクセスリストが欠落している、IKEv1 プロポーザルが一致しないなどがありますが、これらに限定されません（トンネルの問題の検出は、AWS VPC VPN トンネルではまだ使用できません）。
- [デバイス/サービス（Devices/Services）] - デバイスのタイプでフィルタ処理します。
- [ステータス（Status）] – トンネルのステータスには、アクティブとアイドルがあります。
  - [アクティブ（Active）] - セッションが開かれ、ネットワークパケットが VPN トンネルを通過している、または正常なセッションが確立され、タイムアウトになっていない場合。アクティブのステータスは、トンネルが有効で関連していることを示します。
  - [アイドル（Idle）] - CDO が該当のトンネル用のセッションが開かれていることを検出できない、トンネルが使用されていない、または、問題がある場合。
- [オンボーディング済み（Onborded）] - デバイスは、CDO によって管理される場合と、CDO によって管理されない場合（管理対象外）があります。
- [デバイスタイプ（Device Types）] - トンネルの各サイドがライブデバイス（接続されたデバイス）かモデルデバイスかでフィルタ処理します。

ステップ 4 検索バーにデバイス名または IP アドレスを入力して、フィルタ処理された結果を検索することもできます。検索では大文字と小文字は区別されません。

サイト間 VPN トンネルの IKE オブジェクトの詳細の表示

選択したトンネルのピア/デバイスで設定されている IKE オブジェクトの詳細を表示できます。それらの詳細は、IKE ポリシーオブジェクトの優先順位に基づいた階層のツリー構造に表示されます。

（注） エクストラネットデバイスには、IKE オブジェクトの詳細が表示されません。

手順

ステップ 1 左側の CDO ナビゲーションバーで、[VPN] > [サイト間VPN（Site-to-Site VPN）] をクリックします。

ステップ 2 [VPNトンネル（VPN Tunnels）] ページで、ピアを接続する VPN トンネルの名前をクリックします。

ステップ 3 右側の [関係（Relationships）] で、詳細を表示するオブジェクトを展開します。

サイト間 VPN トンネルが最後に正常に確立された日を表示する

手順

ステップ 1 サイト間 VPN トンネル情報の表示。

ステップ 2 [トンネルの詳細（Tunnel Details）] ペインをクリックします。

ステップ 3 [最終アクティブ確認日（Last Seen Active）] フィールドを表示します。

サイト間 VPN トンネル情報の表示

サイト間 VPN テーブルビューは、CDO にオンボーディングされたすべてのデバイスで使用可能なすべてのサイト間 VPN トンネルの完全なリストです。トンネルは、このリストに 1 つだけ存在します。表にリストされているトンネルをクリックすると、右側のサイドバーにオプションが表示され、トンネルのピアに直接移動して詳細に調査できます。

CDO がトンネルの両側を管理していない場合は、[オンボードデバイス（Onboard Device）] をクリックして、管理対象外のピアをオンボードするメインのオンボーディングページを開くことができます。管理対象外 VPN ピアの導入準備 （244 ページ） CDO がトンネルの両側を管理する場合、[ピア2（Peer 2）] 列には管理対象デバイスの名前が含まれます。ただし、AWS VPC の場合、[ピア2（Peer 2）] 列には VPN ゲートウェイの IP アドレスが含まれています。

テーブルビューでサイト間 VPN 接続を表示するには、次の手順を実行します。

手順

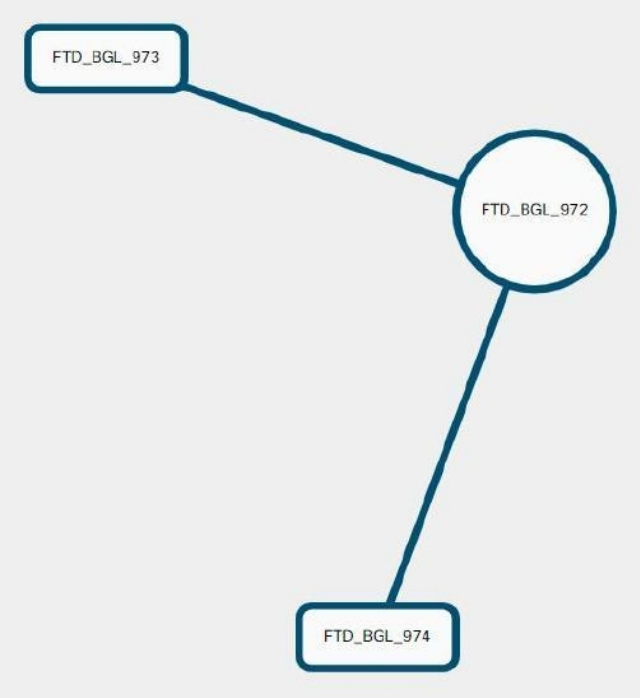
ステップ 1 メインのナビゲーションバーで、[VPN] > [サイト間VPN（Site-to-Site VPN）] をクリックします。

ステップ 2 [テーブルビュー（Table view）] ボタンをクリックします。

ステップ 3 「サイト間 VPN トンネルを検索してフィルタ処理する」を使用して特定のトンネルを見つけるか、グローバルビューのグラフィックを拡大して、探している VPN ゲートウェイとそのピアを見つけます。

サイト間 *VPN* のグローバル表示

これは、グローバルビューの例です。この図では、「FTD_BGL_972」に FTD_BGL_973 デバイスと FTD_BGL_974 デバイスのサイト間接続があります。



手順

ステップ 1 メインのナビゲーションバーで、[VPN] > [サイト間VPN（Site-to-Site VPN）] をクリックします。

ステップ 2 [グローバルビュー（Global view）] ボタンをクリックします。

ステップ 3 「サイト間 VPN トンネルを検索してフィルタ処理する」を使用して特定のトンネルを見つけるか、グローバルビューのグラフィックを拡大して、探している VPN ゲートウェイとそのピアを見つけます。

ステップ 4 グローバルビューに表示されているピアのいずれかを選択します。

ステップ 5 **[詳細の表示（View Details）]** をクリックします。

ステップ 6 VPN トンネルのもう一方の端をクリックすると、その接続のトンネルの詳細、NAT 情報、およびキー交換情報が CDO に表示されます。

- [トンネルの詳細（Tunnel Details）]：トンネルの名前と接続情報が表示されます。[更新（Refresh）] アイコンをクリックすると、トンネルの接続情報が更新されます。
- [AWS接続固有のトンネルの詳細（Tunnel Details specific to AWS connections）]：AWS サイト間接続のトンネルの詳細は、他の接続の場合と若干異なります。AWS VPC から VPN ゲートウェイへの接続ごとに、AWS は 2 つの VPN トンネルを作成します。これは、高可用性を実現するためです。

- トンネルの名前は、VPN ゲートウェイが接続されている VPC の名前を表します。トンネルの名前に含まれている IP アドレスは、VPN ゲートウェイが VPC として認識している IP アドレスです。
- CDO 接続の状態が「active」の場合、AWS トンネルの状態は「Up」です。CDO 接続の状態が「inactive」の場合、AWS トンネルの状態は「Down」です。

- [NAT情報（NAT Information）]：使用されている NAT ルールのタイプ、元のパケットの情報、および変換されたパケットの情報が表示され、そのトンネルの NAT ルールを確認できる NAT テーブルへのリンクが提供されます（AWS VPC サイト間 VPN ではまだ利用できません）。
- [キー交換（Key Exchange）]：トンネルで使用されている暗号キーと、キー交換の問題が表示されます（AWS VPC サイト間 VPN ではまだ利用できません）。

トンネルペイン

[トンネル（Tunnels）] ペインには、特定の VPN ゲートウェイに関連付けられているすべてのトンネルのリストが表示されます。VPN ゲートウェイと AWS VPC のサイト間 VPN 接続の場合、[トンネル（Tunnels）] ペインには、VPN ゲートウェイから VPC へのすべてのトンネルが表示されます。VPN ゲートウェイと AWS VPC のサイト間 VPN 接続にはそれぞれ 2 つのトンネルがあるため、他のデバイスで通常表示される 2 倍の数のトンネルが表示されます。

VPN ゲートウェイの詳細

VPN ゲートウェイに接続されているピア数と、VPN ゲートウェイの IP アドレスが表示されます。これは、[VPNトンネル（VPN Tunnels）] ページにのみ表示されます。

[ピア（Peers）] ペイン

サイト間 VPN ピアのペアを選択すると、ペアリングされた 2 つのデバイスのリストが [ピア（Peers）] ペインに表示され、いずれかのデバイスで [ピアの表示（View Peers）] をクリックできます。[ピアの表示（View Peers] をクリックすると、そのデバイスが関連付けられている他のサイト間ピアが表示されます。これは、テーブルビューとグローバルビューに表示されます。

FTD のサイト間 VPN の設定

Cisco Defense Orchestrator（CDO）は、Firepower Threat Defense デバイスの備えるサイト間 VPN 機能の次の側面をサポートしています。

- IPsec IKEv1 および IKEv2 プロトコルの両方をサポート。
- 自動または手動の事前共有認証キー。
- IPv4 および IPv6 内部、外部のすべての組み合わせをサポート。

- IPsec IKEv2 サイト間 VPN トポロジにより、セキュリティ認定に準拠するための設定を提供。
- スタティック インターフェイスおよびダイナミック インターフェイス。
- エクストラネットデバイスのダイナミック IP アドレスをエンドポイントとしてサポート。

エクストラネット デバイス

各トポロジタイプには、CDO で管理しないエクストラネットデバイスが含まれる可能性があります。次のようなものがあります。

- CDO ではサポートされているものの、ユーザーの部門が担当していないシスコデバイス。たとえば、社内の他の部門が管理するネットワーク内のスポークや、サービス プロバイダーやパートナー ネットワークへの接続などです。
- 管理対象外デバイス。CDO を使用して、管理対象外デバイスの設定を作成および展開することはできません。管理対象外デバイスを VPN トポロジに「エクストラネット」デバイスとして追加します。また、各リモートデバイスの IP アドレスも指定します。

動的にアドレス指定されたピアによるサイト間 VPN 接続の設定

CDO を使用すると、ピアのいずれかの VPN インターフェイス IP アドレスが不明な場合、またはインターフェイスが DHCP サーバーからアドレスを取得する場合に、ピア間にサイト間 VPN 接続を作成できます。事前共有キー、IKE 設定、および IPsec 設定が別のピアと一致するダイナミックピアは、サイト間 VPN 接続を確立できます。

A と B の 2 つのピアがあるとします。スタティックピアは、VPN インターフェイスの IP アドレスが固定されているデバイスであり、ダイナミックピアは、VPN インターフェイスの IP アドレスが不明であるか、一時的な IP アドレスを持つデバイスです。

次の使用例では、動的にアドレス指定されたピアとの安全なサイト間 VPN 接続を確立するためのさまざまなシナリオについて説明します。

- A はスタティックピア、B はダイナミックピア、またはその逆です。
- A はスタティックピア、B は DHCP サーバーから解決された IP アドレスを持つダイナミックピア、またはその逆です。[VPNを割り当てられたIPにバインドする（Bind VPN to the assigned IP）] を選択して、スタティックピアの IP アドレスと、ダイナミックピアの DHCP によって割り当てられた IP アドレスの間に VPN 接続を確立できます。
- A と B はダイナミックピアであり、DHCP サーバーからの解決済み IP アドレスを使用します。このような場合、スタティックピアの IP アドレスと、ダイナミックピアの DHCP によって割り当てられた IP アドレスとの間に VPN 接続を確立するために、少なくとも 1 つのピアに対して [VPNを割り当てられたIPにバインドする（Bind VPN to the assigned IP）] を選択する必要があります。
- A はダイナミックピアで、B はスタティックまたはダイナミック IP アドレスを持つエクストラネットデバイスです。

- A は DHCP サーバーからの解決済み IP アドレスを持つダイナミックピアで、B はスタティックまたはダイナミック IP アドレスを持つエクストラネットデバイスです。[VPNを割り当てられたIPにバインドする（Bind VPN to the assigned IP）] を選択して、スタティックピアの IP アドレスと、ダイナミックピアの DHCP によって割り当てられた IP アドレスの間に VPN 接続を確立できます。

重要 [VPNを割り当てられたIPにバインドする（Bind VPN to the assigned IP）] を選択すると、VPN は DHCP によって割り当てられた IP アドレスに静的にバインドします。ただし、このダイナミックインターフェイスは、ピアの再起動後に多くの新しいIPアドレスを受信できます。VPN トンネルは新しい IP アドレスを更新しますが、もう一方のピアは新しい設定で更新されません。他のピアでのアウトオブバンドの変更については、サイト間設定を再度展開する必要があります。

（注） Firepower Threat Defense Manage（FDM）などのローカルマネージャを使用してインターフェイスの IP アドレスを変更すると、CDO では、そのピアの [設定ステータス（Configuration Status）] に [競合検出（Conflict Detected）] と表示されます。設定の競合の解決すると、他方のピアの [設定ステータス（Configuration Status）] が [非同期（Not Synced）] 状態に変わります。[非同期（Not Synced）] 状態のデバイスに CDO 設定を展開する必要があります。

通常、ダイナミックピアの IP アドレスを他方のピアは把握していないため、ダイナミックピアから接続を開始する必要があります。リモートピアが接続を確立しようとすると、他方のピアは事前共有キー、IKE 設定、および IPsec 設定を使用して接続を検証します。

VPN 接続はリモートピアが接続を開始した後にのみ確立されるため、VPN トンネルのトラフィックを許可するアクセス制御ルールに一致するすべての発信トラフィックは、接続が確立されるまでドロップされます。これにより、適切な暗号化と VPN 保護のないデータがネットワークから流出しないようになります。

（注） 次のシナリオでは、サイト間 VPN 接続を設定できません。

- 両方のピアに DHCP によって割り当てられた IP アドレスがある場合。
  - **回避策**：どちらか一方のピアに DHCP サーバーからの解決済み IP アドレスがある場合は、サイト間 VPN を設定できます。このような場合、サイト間 VPN を設定するには [VPNを割り当てられたIPにバインドする（Bind VPN to the assigned IP）] を選択する必要があります。

- 1 台のデバイスに複数のダイナミックピア接続がある場合。
  - **回避策**：次の手順を実行して、サイト間 VPN を設定できます。
    - 3 台のデバイス A、B、C があるとします。

- A（スタティックピア）と B（ダイナミックピア）間のサイト間 VPN 接続を設定します。
- エクストラネットデバイスを作成して、A と C（ダイナミックピア）間のサイト間 VPN 接続を設定します。A のスタティック VPN インターフェイス IP アドレスをエクストラネットデバイスに割り当て、C との接続を確立します。

FTD サイト間 VPN ガイドラインと制約事項

- CDO は、S2S VPN の対象トラフィックを設計するための crypto-acl をサポートしていません。保護されたネットワークのみをサポートします。
- CDO は、現在、ASA デバイスまたは FTD デバイス上の仮想トンネルインターフェイス（VTI）トンネルの管理、監視、使用をサポートしていません。VTI トンネルが設定されているデバイスを CDO にオンボーディングすることは可能ですが、VTI インターフェイスは無視されます。セキュリティゾーンまたはスタティックルートが VTI を参照する場合、CDO は VTI 参照を除いてセキュリティゾーンとスタティックルートを読み取ります。VTI トンネルに対する CDO のサポートは近日中に提供されます。
- IKE ポート 500/4500 が使用されている場合、またはアクティブな PAT 変換がある場合は、これらのポートでサービスを開始できないため、サイト間 VPN を同じポートに設定することはできません。
- トンネルモードにのみ対応し、トランスポートモードには対応していません。IPsec トンネル モードは、新しい IP パケットのペイロードになる元の IP データグラム全体を暗号化します。トンネルモードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネルモードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイアウォール（またはその他のセキュリティゲートウェイ）間で通常の IPsec が実装される標準の方法です。
- このリリースでは、1 つ以上の VPN トンネルを含む PTP トポロジのみがサポートされています。ポイントツーポイント（PTP）型の展開は、2 つのエンドポイント間で VPN トンネルを確立します。

関連情報：

- サイト間 VPN の作成
- 既存の CDO サイト間 VPN の編集
- VPN で使用される暗号化アルゴリズムとハッシュアルゴリズム
- NAT からのサイト間 VPN トラフィックの除外

サイト間 VPN の作成

簡易設定か詳細設定のいずれかの方法で、サイト間 VPN を作成できます。簡易設定では、サイト間 VPN 接続の確立にデフォルト設定が使用されます。[詳細（Advanced）] モードの設定は変更できます。

各サイト間 VPN トポロジには、CDO で管理しないエクストラネットデバイスが含まれる可能性があります。エクストラネットデバイスは、CDO の管理対象ではない任意のデバイス（シスコまたはサードパーティ）である可能性があります。

このリリースでは、サイト間接続ごとに 1 つのトンネルを含む PTP トポロジのみがサポートされています。ポイントツーポイント（PTP）型の展開は、2 つのエンドポイント間で VPN トンネルを確立します。

関連情報：

- シンプルな設定を使用したサイト間 VPN の作成 （252 ページ）
- 高度な設定を使用したサイト間 VPN の作成 （253 ページ）
- サイト間ピア間の保護されたトラフィックのネットワークの設定 （256 ページ）

シンプルな設定を使用したサイト間 *VPN* の作成

手順

ステップ 1 ナビゲーションウィンドウで、**[VPN]** > **[サイト間VPN（Site-to-Site VPN）]** を選択します。

ステップ 2 青色のプラスボタン  をクリックして、VPN トンネルを作成します。

（注） または、[デバイスとサービス（Devices & Services）] ページからサイト間 VPN 接続を作成できます。

1. ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
2. 設定する 2 つの FTD デバイスを選択します。エクストラネットデバイスを選択した場合は、エクストラネットデバイスの IP アドレスを指定します。
3. 右側のページの [デバイスアクション（Device Actions）] で、[サイト間VPNの作成（Create Site-to-Site VPN）] をクリックします。

ステップ 3 一意のトポロジ [設定名（Configuration Name）] を入力します。トポロジには、FTD VPN であること、およびトポロジタイプを示す名前を付けることをお勧めします。

ステップ 4 [デバイス（Devices）] から、この VPN 展開のエンドポイントデバイスを選択します。

ステップ 5 [ピア2（Peer2）] でエクストラネットデバイスを選択する場合は、[静的（Static）] を選択して IP アドレスを指定するか、DHCP が割り当てられた IP を持つエクストラネットデバイスの場合は [動的（Dynamic）] を選択します。[IPアドレス（IP Address）] には、静的インターフェイスの IP アドレスまたは動的インターフェイスの [DHCP割り当て（DHCP Assigned）] が表示されます。

ステップ 6 エンドポイントデバイスの [VPNアクセスインターフェイス（VPN Access Interface）] を選択します。

（注） 1つまたは両方のエンドポイントデバイスに動的IPアドレスがある場合、追加の手順については、「動的にアドレス指定されたピアによるサイト間 VPN 接続の設定」を参照してください。

ステップ 7 青いプラスボタン をクリックして、参加デバイスの [保護されたネットワーク（Protected Networks）] を追加します。

ステップ 8 （任意）[NAT免除（NAT Exempt）] を選択して、VPN トラフィックをローカル VPN アクセスインターフェイス上の NAT ポリシーから除外します。個々のピアに対して手動で設定する必要があります。NAT ルールをローカル ネットワークに適用しない場合、ローカル ネットワークをホストするインターフェイスを選択します。このオプションは、ローカルネットワークが1つのルーテッドインターフェイス（ブリッジグループ メンバーではない）の背後にある場合にのみ機能します。ローカルネットワークが複数のルーテッドインターフェイスまたは1つ以上のブリッジグループのメンバーの背後にある場合、NAT 免除ルールを手動で作成する必要があります。必要なルールを手動で作成する方法については、「NAT からのサイト間 VPN トラフィックの除外 」を参照してください。

ステップ 9 [VPNの作成（Create VPN）] をクリックし、[終了（Finish）] をクリックします。

ステップ 10 追加の必須設定を実行します。「サイト間ピア間の保護されたトラフィックのネットワークの設定」を参照してください。

サイト間 VPN が設定されます。

高度な設定を使用したサイト間 *VPN* の作成

手順

ステップ 1 ナビゲーションバーで、[VPN] を選択します。

ステップ 2 青いプラスボタン をクリックして、VPN トンネルを作成します。

ステップ 3 [ピアデバイス（Peer Devices）] セクションで、次のデバイス設定を指定します。

1. 一意のトポロジ [設定名（Configuration Name）] を入力します。トポロジには、FTD VPN であること、およびトポロジタイプを示す名前を付けることをお勧めします。
2. [デバイス（Devices）] から、この VPN 展開のエンドポイントデバイスを選択します。
3. エクストラネットデバイスを選択する場合は、[静的（Static）] を選択して IP アドレスを指定し、DHCP が割り当てられた IP を持つエクストラネットデバイスの場合は [動的（Dynamic）] を選択します。[IPアドレス（IP Address）] には、静的インターフェイスの IP アドレスまたは動的インターフェイスの [DHCP割り当て（DHCP Assigned）] が表示されます。

4. エンドポイントデバイスの [VPNアクセスインターフェイス（VPN Access Interface）] を選択します。

（注） 1つまたは両方のエンドポイントデバイスに動的IPアドレスがある場合、追加の手順については、「動的にアドレス指定されたピアによるサイト間 VPN 接続の設定」を参照してください。

ステップ 4 青いプラスボタン をクリックして、参加デバイスの [保護されたネットワーク（Protected Networks）] を追加します。

ステップ 5 [詳細設定（Advanced）] をクリックします。

ステップ 6 [IKE設定（IKE Settings）] セクションで、インターネット キー エクスチェンジ（IKE）ネゴシエーション中に使用する IKE バージョンを選択し、プライバシー設定を指定します。IKE ポリシーの詳細については、「グローバル IKE ポリシーの設定」を参照してください。

（注） IKEポリシーはデバイスに対してグローバルであり、デバイスに関連付けられたすべてのVPNトンネルに適用されます。したがって、ポリシーを追加または削除すると、このデバイスが参加しているすべての VPN トンネルに影響します。

1. 必要に応じて、いずれかまたは両方のオプションを選択します。

（注） デフォルトでは、[IKEVバージョン2（IKEV Version 2）] と [IKEV2ポリシー（IKEV2 POLICIES）] が有効になっています。

2. 青いプラスボタン をクリックし、IKEv2 ポリシーを選択します。

[新しいIKEv2ポリシーの作成（Create New IKEv2 Policy）] をクリックして、新しい IKEv2 ポリシーを作成します。または、CDO ナビゲーションバーに移動し、**[オブジェクト（Objects）] > [オブジェクト の作成（Create Object +）] > [IKEv2ポリシー（IKEv2 Policy）]** をクリックします。新しい IKEv2 ポリシーの作成の詳細については、「IKEv2 ポリシーの設定」を参照してください。既存の IKEv2 ポリシーを削除するには、選択したポリシーにカーソルを合わせ、[x] アイコンをクリックします。

3. [IKEバージョン1（IKE Version 1）] をクリックして有効にします。

4. 青いプラスボタン をクリックし、IKEv1 ポリシーを選択します。[新しいIKEv1ポリシーの作成（Create New IKEv1 Policy）] をクリックして、新しい IKEv1 ポリシーを作成します。または、CDO ナビゲーションバーに移動し、[オブジェクト（Objects）] > [オブジェクト の作成（Create Object +）] > [IKEv1ポリシー（IKEv1 Policy）] をクリックします。新しい IKEv1 ポリシーの作成の詳細については、「IKEv1 ポリシーの設定」を参照してください。既存の IKEv1 ポリシーを削除するには、選択したポリシーにカーソルを合わせ、[x] アイコンをクリックします。

5. 参加デバイスの [事前共有キー（Pre-Shared Key）] を入力します。事前共有キーは、接続内の各ピアで設定された秘密鍵文字列です。これらのキーは、IKE が認証フェーズで使用します。

   - （IKEv2）[ピア1事前共有キー（Peer 1 Pre-shared Key）]、[ピア2事前共有キー（Peer 2 Pre-shared Key）]：IKEv2 の場合、各ピアで固有のキーを設定できます。[事前共有キー（Pre-shared Key）] を入力します。[オーバーライドの表示（Show Override）] ボタンをクリックして、ピアに適切な事前共有キーを入力できます。このキーには 1 ～ 127 の英数字を指定できます。次の表で、両方のピアにおける事前共有キーの目的について説明します。

	ローカル事前共有キー	リモートピア事前共有キー
ピア 1	ピア 1 事前共有キー	ピア 2 事前共有キー
ピア 2	ピア 2 事前共有キー	ピア 1 事前共有キー

   - （IKEv1）[事前共有キー（Pre-shared Key）]：IKEv1 の場合は、各ピアで同じ事前共有キーを設定する必要があります。このキーには 1 ～ 127 の英数字を指定できます。このシナリオでは、ピア 1 とピア 2 は同じ事前共有キーを使用してデータを暗号化および復号します。

6. [次へ（Next）] をクリックします。

ステップ 7 [IPSec設定（IPSec Settings）] セクションで、IPSec 設定を指定します。[IPSec設定（IPSec Settings）] ステップでの選択に応じて、対応する IKEv プロポーザルを使用できます。

IPSec 設定の詳細については、「IPsec プロポーザルの設定」を参照してください。

1. 青いプラスボタン をクリックし、IKEv2 プロポーザルを選択します。既存の IKEv2 プロポーザルを削除するには、選択したプロポーザルにカーソルを合わせ、[x] アイコンをクリックします。

   （注） [新しいIKEv2プロポーザルの作成（Create New IKEv2 Proposal）] をクリックして、新しい IKEv2 プロポーザルを作成します。または、CDO ナビゲーションバーに移動し、[オブジェクト（Objects）] > [オブジェクト の作成（Create Object +）] > [IKEv2 IPSecプロポーザル（IKEv2 IPSec Proposal）] をクリックします。

   新しい IKEv2 プロポーザルの作成の詳細については、「IKEv2 の IPsec プロポーザルの設定」を参照してください。

2. [Perfect Forward Secrecy対応のDiffie-Hellmanグループ（Diffie-Hellman Group for Perfect Forward Secrecy）] を選択します。詳細については、「使用する Diffie-Hellman 係数グループの決定」を参照してください。

3. [Create VPN] をクリックします。

4. 設定を確認し、問題がなければ [完了（Finish）] をクリックします。

5. 追加の必須設定を実行します。「サイト間ピア間の保護されたトラフィックのネットワークの設定」を参照してください。

サイト間ピア間の保護されたトラフィックのネットワークの設定

サイト間接続の設定が完了したら、VPNがすべての対象デバイスで機能するように、次の設定を実行してください。

手順

ステップ1 ACポリシーを設定します。

両方のピアの背後にある保護されたネットワーク間の双方向トラフィックを許可するためのACポリシーを設定します。ACポリシーは、パケットがドロップされることなく目的の宛先に到達するのに役立ちます。

（注） 両方のピアで着信トラフィックと発信トラフィックのACポリシーを作成する必要があります。

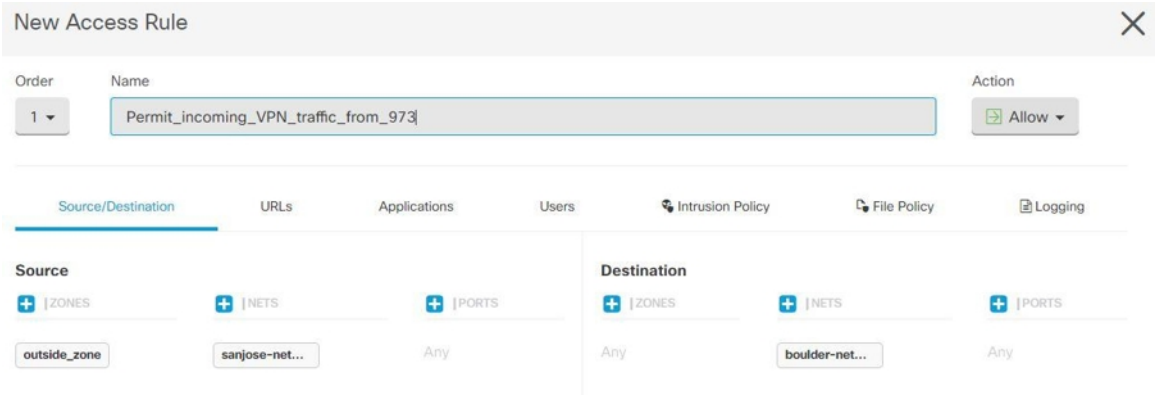
1. 左側のCDOナビゲーションバーで[ポリシー（Policies）]をクリックし、必要なオプションを選択します。
2. 両方のピアで着信トラフィックと発信トラフィックのポリシーを作成します。ACポリシーの作成の詳細については、「FTD アクセス コントロール ポリシーの設定」を参照してください。

   次の例は、両方のピアでACポリシーを作成する手順を示しています。

   それぞれ2つの保護されたネットワーク「boulder-network」および「sanjose-network」間のサイト間VPN接続を備えた2つのFTDデバイス「FTD_BGL_972」および「FTD_BGL_973」について考えてみます。

   着信トラフィックを許可する*AC*ポリシーの作成：

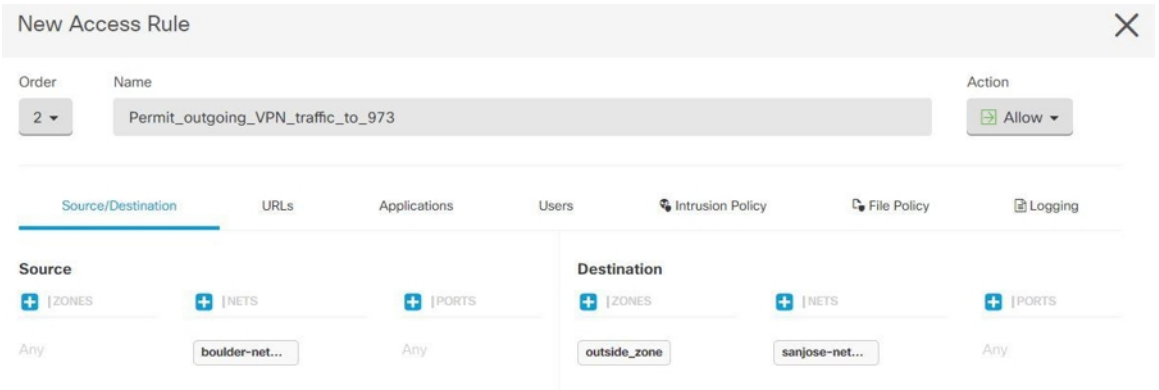
   ポリシー「Permit_incoming_VPN_traffic_from_973」は、ピア「FTD_BGL_973」からの着信トラフィックを許可するために「FTD_BGL_972」デバイスで作成されます。



- **送信元ゾーン**：ネットワークトラフィックの発信元であるピアデバイスのゾーンを設定します。この例では、トラフィックはFTD_BGL_973から発信され、FTD_BGL_972に到達します。
- **送信元ネットワーク** ：ネットワークトラフィックの発信元であるピアデバイスの保護されたネットワークを設定します。この例では、トラフィックはピアデバイス（FTD_BGL_973）の背後にある保護されたネットワークである「sanjose-network」から発信されています。
- **宛先ネットワーク**：ネットワークトラフィックが到着するデバイスの保護されたネットワークを設定します。この例では、トラフィックはピアデバイス（FTD_BGL_972）の背後にある保護されたネットワークである「boulder-network」に到着しています。
  注：残りのフィールドは、デフォルト値（「Any」）にできます。
- 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するには、[アクション（Action）] を [許可（Allow）] に設定します。

発信トラフィックを許可する *AC* ポリシーの作成：

ポリシー「Permit_outgoing_VPN_traffic_to_973」は、ピア「FTD_BGL_973」への発信トラフィックを許可するために「FTD_BGL_972」デバイスで作成されます。



- **送信元ネットワーク** ：ネットワークトラフィックの発信元であるピアデバイスの保護されたネットワークを設定します。この例では、トラフィックはピアデバイス

（FTD_BGL_972）の背後にある保護されたネットワークである「boulder-network」から発信されています。

- **宛先ゾーン**：ネットワークトラフィックが到着するピアデバイスのゾーンを設定します。この例では、トラフィックは FTD_BGL_972 から着信し、FTD_BGL_973 に到達しています。
- **宛先ネットワーク**：ネットワークトラフィックが到着するピアの保護されたネットワークを設定します。この例では、トラフィックはピアデバイス（FTD_BGL_972）の背後にある保護されたネットワークである「sanjose-network」に到着しています。**注**：残りのフィールドは、デフォルト値（「Any」）にできます。
- 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するには、[アクション（Action）] を [許可（Allow）] に設定します。

1 つのデバイスで AC ポリシーを作成したら、そのデバイスのピアで同様のポリシーを作成する必要があります。

ステップ 2 いずれかのピアデバイスで NAT が設定されている場合は、NAT 免除ルールを手動で設定する必要があります。「NAT からのサイト間 VPN トラフィックの除外 」を参照してください。

ステップ 3 各ピアでリターン VPN トラフィックを受信するためのルーティングを設定します。詳細については、「FTDデバイスのスタティックルートとデフォルトルートの設定」を参照してください。

1. [ゲートウェイ（Gateway）]：宛先ネットワークへのゲートウェイの IP アドレスを識別するネットワークオブジェクトを選択します。トラフィックはこのアドレスに送信されます。
2. [インターフェイス（Interface）]：トラフィックの送信経路となるインターフェイスを選択します。この例では、トラフィックは「外部」インターフェースを介して送信されます。
3. [宛先ネットワーク（Destination Networks）]：宛先ネットワークを識別する 1 つまたは複数のネットワークオブジェクトを選択します。この例では、宛先はピア（FTD_BGL_973）の背後にある「sanjose-network」です。

1 つのデバイスでルーティングの設定をしたら、そのデバイスのピアで同様の設定をする必要があります。

既存の CDO サイト間 VPN の編集

高度な設定ウィザードは、デフォルトで既存のサイト間 VPN 設定を変更するために使用します。

手順

ステップ 1 ナビゲーションバーで、**[VPN]** > **[サイト間VPN（Site-to-Site VPN）]**を選択します。

ステップ 2 編集するサイト間 VPN トンネルを選択します。

ステップ 3 [アクション（Actions）] ペインで、[編集（Edit）] をクリックします。

（注） または、次を実行して設定を編集することもできます。

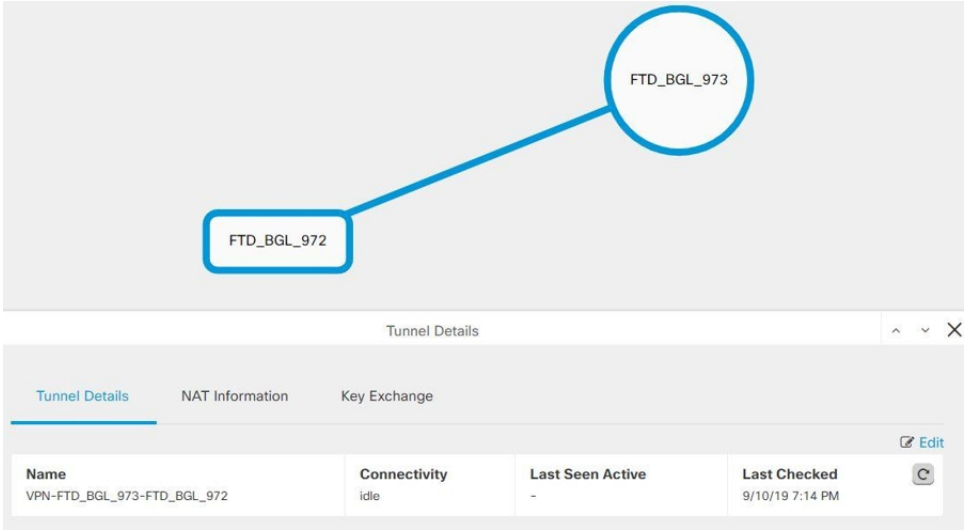
1. VPN ページを開き、[フィルター（filter）] パネルの [グローバルビュー（Global View）] ボタンをクリックします。（詳細については、「サイト間 VPN トンネルを検索してフィルタ処理する」を参照してください）。

   すべてのデバイスで使用可能なすべてのサイト間 VPN トンネルの図が表示されます。

   設定を編集するには、ピアの 1 つが FTD である必要があります。

2. ボックスをクリックしてデバイスを選択します。
3. ピアを表示するには、[詳細の表示（View Details）] をクリックします。
4. ピアのデバイスをクリックして、トンネルの詳細を表示します。

   トンネルの詳細、NAT 情報、およびデバイスに関するキー交換情報を表示できます。



5. [トンネルの詳細（Tunnel Details）] で [編集（Edit）] をクリックします。

ステップ 4 [ピアデバイス（Peer Devices）] セクションでは、次のデバイス設定を変更できます：設定名、VPN アクセスインターフェイス、および保護されたネットワーク。

（注） 参加デバイスを変更することはできません。

ステップ 5 [IKE 設定（IKE Settings）] セクションでは、次の IKEv2 ポリシー設定を変更できます。

1. それぞれのデバイスの青いプラス  ボタンをクリックし、新しい IKEv2 ポリシーを選択します。既存の IKEv2 ポリシーを削除するには、選択したポリシーにカーソルを合わせ、[x] アイコンをクリックします。
2. 参加デバイスの**事前共有キー**を変更します。エンドポイントデバイスの事前共有キーが異なる場合は、青い設定  ボタンをクリックして、デバイスの適切な事前共有キーを入力します。
3. [次へ（Next）] をクリックします。

ステップ 6 [IPSec設定（IPSec Settings）] セクションでは、次の IPSec 設定を変更できます。

1. 青いプラス  ボタンをクリックして、新しい IKEv2 プロポーザルを選択します。既存の IKEv2 プロポーザルを削除するには、選択したプロポーザルにカーソルを合わせ、[x] アイコンをクリックします。
2. [Perfect Forward Secrecy対応のDiffie-Hellmanグループ（Diffie-Hellman Group for Perfect Forward Secrecy）] を選択します。
3. [VPN の編集（Edit VPN）] をクリックし、[完了（Finish）] をクリックします。

ポイントツーポイントの VPN が変更され、行ったすべての変更が反映されます。

既存の *CDO* サイト間 *VPN* の削除

手順

ステップ 1 ナビゲーションバーで、[VPN] > [サイト間VPN（Site-to-Site VPN）] を選択します。
ステップ 2 削除するサイト間 VPN トンネルを選択します。
ステップ 3 [アクション（Actions）] ペインで、[削除（Delete）] をクリックします。

選択したサイト間 VPN トンネルが削除されます。

VPN で使用される暗号化アルゴリズムとハッシュアルゴリズム

VPN トンネルは通常、インターネットなどのパブリック ネットワークを経由するため、トラフィックを保護するために接続を暗号化する必要があります。IKE ポリシーと IPsec プロポーサルを使用して、暗号化とその他のセキュリティ技術を定義し、適用します。

デバイス ライセンスによって強力な暗号化を適用できる場合は、広範な暗号化とハッシュ アルゴリズム、および Diffie-Hellman グループがあり、その中から選択できます。ただし、一般に、トンネルに適用する暗号化が強力なほど、システムパフォーマンスは低下します。効率を

損なうことなく十分な保護を提供するセキュリティとパフォーマンスのバランスを見出します。

シスコでは、どのオプションを選択するかについての特定のガイダンスは提供できません。比較的大規模な企業またはその他の組織内で運用している場合は、すでに、満たす必要がある標準が定義されている可能性があります。定義されていない場合は、時間を割いてオプションを調べてください。

以降のトピックでは、使用可能なオプションについて説明します。

使用する暗号化アルゴリズムの決定

IKE ポリシーまたは IPsec プロポーザルに対して使用する暗号化アルゴリズムを決定する場合は、VPN 内のデバイスによってサポートされるアルゴリズムに限定されます。

IKEv2 では、複数の暗号化アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

IPsec プロポーザルでは、認証、暗号化、およびアンチリプレイ サービスを提供するカプセル化セキュリティ プロトコル（ESP）によってアルゴリズムが使用されます。ESP は、IP プロトコル タイプ 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の接頭辞が「ESP」となります。

デバイス ライセンスが強力な暗号化を適用できる場合、次の暗号化アルゴリズムを選択できます。強力な暗号化の対象ではない場合、DES のみ選択できます。

- 1AES-GCM：（IKEv2 のみ）ガロア/カウンタモードの Advanced Encryption Standard は、機密性とデータ発信元認証を提供するブロック暗号モードの操作であり、AES より優れたセキュリティを実現します。AES-GCM には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。GCM は NSA Suite B をサポートするために必要となる AES モードです。NSA Suite B は、暗号化強度に関する連邦標準規格を満たすためにデバイスがサポートすべき一連の暗号化アルゴリズムです。

- AES-GMAC：（IKEv2 IPsec プロポーザルのみ）Advanced Encryption Standard のガロア メッセージ認証コード（GMAC）は、データ発信元認証だけを行う操作のブロック暗号モードです。これは AES-GCM の一種であり、データを暗号化せずにデータ認証が行えます。AES-GMAC には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。

- AES（Advanced Encryption Standard）は DES よりも高度なセキュリティを提供する対称暗号化アルゴリズムであり、計算の効率は 3DES よりも高いです。AES には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。

- DES（Data Encryption Standard）は、56 ビットキーを使用して暗号化する対称秘密鍵ブロック アルゴリズムです。ライセンス アカウントが輸出規制の要件を満たしていない場合、これは唯一のオプションです。3DES よりも高速であり、使用するシステム リソースも少な

いですが、安全性は劣ります。堅牢なデータ機密保持が必要ない場合、およびシステム リソースや速度が重要である場合には、DES を選択します。

- 3DES（トリプル DES）：56 ビットキーを使用して暗号化を 3 回行います。異なるキーを使用してデータの各ブロックを 3 回処理するため、DES よりも安全です。ただし、使用するシステム リソースが多くなり、DES よりも速度が遅くなります。
- Null：ヌル暗号化アルゴリズムは暗号化なしで認証します。通常はテスト目的にのみ使用されます。

使用するハッシュ アルゴリズムの決定

IKE ポリシーでは、ハッシュ アルゴリズムがメッセージ ダイジェストを作成します。これは、メッセージの整合性を保証するために使用されます。IKEv2 では、ハッシュ アルゴリズムは 2 つのオプションに分かれています。1 つは整合性アルゴリズムに使用され、もう 1 つは擬似乱数関数（PRF）に使用されます。

IPsec プロポーザルでは、ハッシュ アルゴリズムはカプセル化セキュリティ プロトコル（ESP）による認証のために使用されます。IKEv2 IPsec プロポーザルでは、これは整合性のハッシュと呼ばれます。IKEv1 IPsec プロポーザルでは、アルゴリズム名の接頭辞が「ESP-」となり、「-HMAC」（Hash Method Authentication Code）という接尾辞も使用されます。

IKEv2 では、複数のハッシュ アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

次のハッシュ アルゴリズムから選択できます。

- [SHA (Secure Hash Algorithm)]：標準の SHA（SHA-1）は、160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。ただし、MD5 よりも多くのリソースを消費します。最大レベルのセキュリティを必要とする実装には、SHA ハッシュ アルゴリズムを使用してください。
- IKEv2 の設定では、以下の SHA-2 オプションを指定して、より高度なセキュリティを実現できます。NSA Suite B 暗号化仕様を実装するには、次のいずれかを選択します。
  - SHA256：256 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA-2 を指定します。
  - SHA384：384 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA-2 を指定します。
  - SHA512：512 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA-2 を指定します。
- MD5 (Message Digest 5)：128 ビットのダイジェストを生成します。MD5 は処理時間が短いため、全体的なパフォーマンスが SHA より高速ですが、SHA より強度は低いと考えられています。
- NULL またはなし（NULL、ESP-NONE）：（IPsec プロポーザルのみ）NULL ハッシュ アルゴリズム。通常はテスト目的のみに使用されます。しかし、暗号化オプションとしてい

ずれかのAES-GCM/GMACオプションを選択した場合は、NULL整合性アルゴリズムを選択する必要があります。NULL以外のオプションを選択した場合、これらの暗号化標準に対しては、整合性ハッシュは無視されます。

使用する Diffie-Hellman 係数グループの決定

次の Diffie-Hellman キー導出アルゴリズムを使用して、IPsec Security Association（SA：セキュリティアソシエーション）キーを生成することができます。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。両方のピアに、一致する係数グループが存在する必要があります。

AES 暗号化を選択する場合は、AES で必要な大きいキー サイズをサポートするために、Diffie-Hellman（DH：デフィーヘルマン）グループ 5 以降を使用する必要があります。IKEv1 ポリシーは、以下に示すすべてのグループをサポートしているわけではありません。

NSA Suite-B の暗号化の仕様を実装するには、IKEv2 を使用して楕円曲線 Diffie-Hellman（ECDH）オプション：19、20、21 のいずれか 1 つを選択します。楕円曲線オプションと、2048 ビット係数を使用するグループは、Logjam のような攻撃にさらされる可能性が低くなります。

IKEv2 では、複数のグループを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

- 2：Diffie-Hellman グループ 2（1024 ビット Modular Exponential（MODP）グループ）。このオプションは十分な保護レベルとは見なされなくなりました。
- 5：Diffie-Hellman グループ 5（1536 ビット MODP グループ）。以前は 128 ビットキーの十分な保護レベルと見なされていましたが、このオプションは十分な保護レベルとは見なされなくなりました。
- 14：Diffie-Hellman グループ 14（2048 ビット Modular Exponential（MODP）グループ）。192 ビットのキーでは十分な保護レベルです。
- 19：Diffie-Hellman グループ 19（国立標準技術研究所（NIST）256 ビット楕円曲線モジュロプライム（ECP）グループ）。
- 20：Diffie-Hellman グループ 20（NIST 384 ビット ECP グループ）。
- 21：Diffie-Hellman グループ 21（NIST 521 ビット ECP グループ）。
- 24：Diffie-Hellman グループ 24（2048 ビット MODP グループと 256 ビット素数位数部分群）。このオプションは推奨されなくなりました。

使用する認証方式の決定

次の方法を使用して、サイト間 VPN 接続でピアを認証できます。

事前共有キー

事前共有キーは、接続内の各ピアで設定された秘密鍵文字列です。これらのキーは、IKEが認証フェーズで使用します。IKEv1 の場合は、各ピアで同じ事前共有キーを設定する必要があります。IKEv2 の場合は、各ピアに一意のキーを設定できます。

事前共有キーは、証明書に比べて拡張性がありません。多数のサイト間 VPN 接続を設定する必要がある場合は、事前共有キー方式ではなく証明書方式を使用します。

NAT からのサイト間 VPN トラフィックの除外

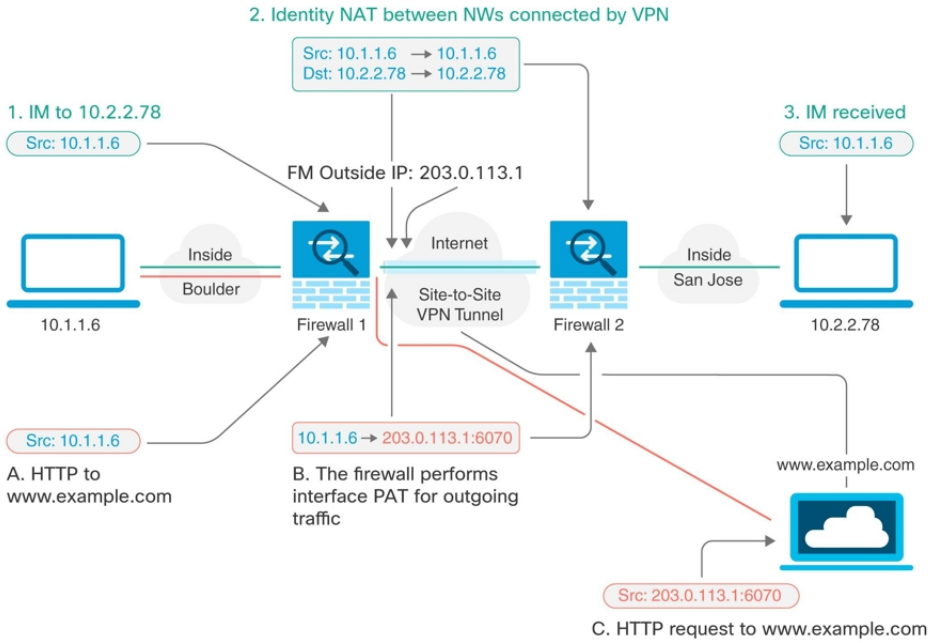
インターフェイスでサイト間 VPN 接続が定義されていて、かつそのインターフェイス向けの NAT ルールを指定している場合、NAT ルールから VPN 上のトラフィックを任意で除外できます。この操作は、VPN 接続のリモート エンドが内部アドレスを処理できる場合に行うと便利です。

VPN 接続を作成するときに、[NATを除外（NAT Exempt）] オプションを選択すると、ルールが自動的に作成されます。ただし、これはローカルで保護されたネットワークが単一のルーテッド インターフェイス（ブリッジ グループ メンバーではない）を介して接続されている場合のみ動作します。その代わりに、接続内のローカルネットワークが複数のルーテッド インターフェイス、または 1 つ以上のブリッジ グループ メンバーの背後に存在する場合、NAT 免除ルールを手動で設定する必要があります。

NAT ルールから VPN トラフィックを除外するには、宛先がリモート ネットワークのときにローカル トラフィックの手動アイデンティティ NAT ルールを作成します。次に、任意の宛先（インターネットなど）のトラフィックに NAT を適用します。ローカル ネットワークに複数のインターフェイスがある場合、各インターフェイスにルールを作成します。次の点も考慮してください。

- 接続内に複数のローカル ネットワークがある場合、ネットワークを定義するオブジェクトを保持するネットワーク オブジェクト グループを作成します。
- VPN に IPv4 ネットワークと IPv6 ネットワークの両方を含める場合、それぞれに個別のアイデンティティ NAT ルールを作成します。

次の例では、ボールダーとサンノゼのオフィスを接続するサイトツーサイト トンネルを示します。インターネットに渡すトラフィックについて（たとえばボールダーの 10.1.1.6 から www.example.com へ）、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス ポート アドレス変換（PAT）ルールを使用しています。ただし、VPN トンネルを経由するトラフィックについては（たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。



次の例は、Firewall1（ボールダー）の設定を示します。例では、内部インターフェイスがブリッジ グループであると仮定するため、各メンバー インターフェイスにルールを記述する必要があります。ルーティングされた内部インターフェイスが 1 つある場合も複数ある場合も、プロセスは同じです。

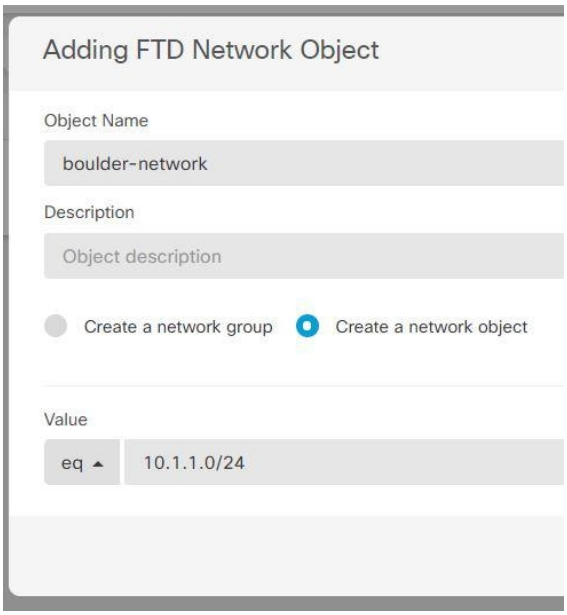
（注） この例では、IPv4 のみと仮定します。VPN に IPv6 ネットワークも含まれる場合、IPv6 にはパラレル ルールを作成します。IPv6 インターフェイス PAT は実装できないため、PAT を使用するには固有の IPv6 アドレスを持つホスト オブジェクトを作成する必要があることに注意してください。

手順

ステップ 1 さまざまなネットワークを定義するには、オブジェクトを作成します。

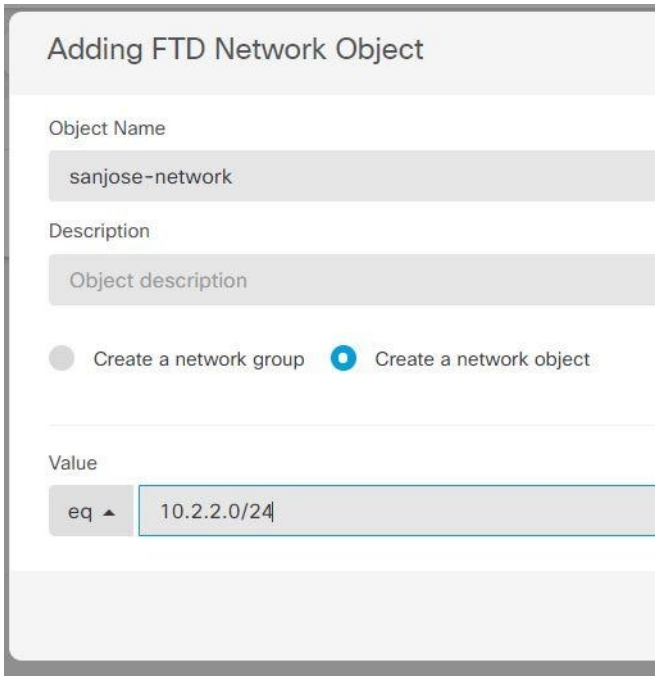
1. 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。
2. 青色のプラスボタン をクリックして、オブジェクトを作成します。
3. **[FTD] > [ネットワーク（Network）]** をクリックします。
4. ネットワーク内でボールダーを特定します。
5. オブジェクト名を入力します（例：boulder-network）。
6. [ネットワークオブジェクトの作成（Create a network object）] を選択します。

7. [値（Value）] セクションで、次の手順を実行します。
   - [eq] を選択して、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。
   - [範囲（range）] を選択し、IP アドレスの範囲を入力します。たとえば、ネットワークアドレスを 10.1.1.0/24 と入力します。



8. [追加（Add）] をクリックします。
9. 青色のプラスボタン をクリックして、オブジェクトを作成します。
10. サンノゼの内部ネットワークを定義します。
11. オブジェクト名を入力します（例：san-jose）。
12. [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。
13. [値（Value）] セクションで、次の手順を実行します。
    - [eq] を選択して、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。

- [範囲（range）] を選択し、IP アドレスの範囲を入力します。たとえば、ネットワークアドレスを 10.1.1.0/24 と入力します。

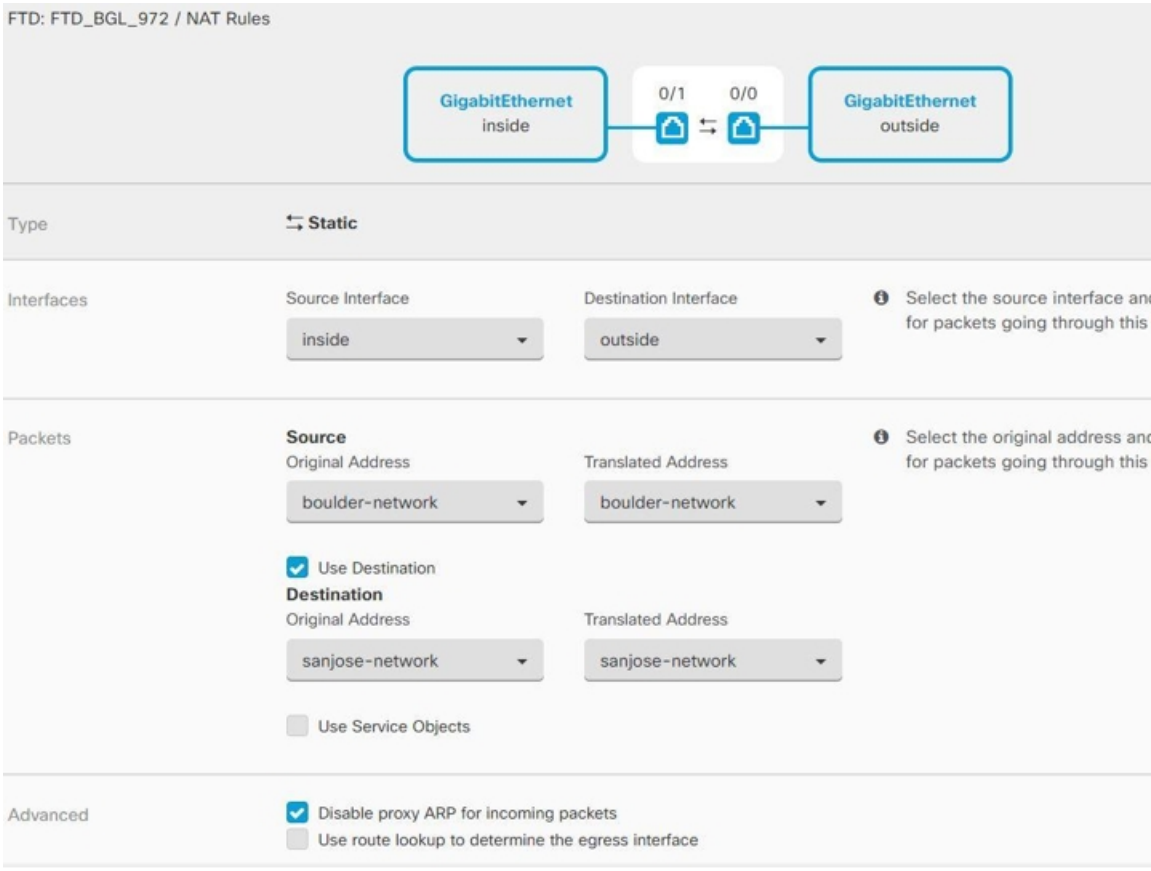


14. [追加（Add）] をクリックします。

ステップ 2 Firewall1（ボールダー）上で VPN 経由でサンノゼに向かう場合、ボールダー ネットワークの手動アイデンティティ NAT を設定します。

1. CDO ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。
2. フィルタを使用して、NAT ルールを作成するデバイスを見つけます。
3. 詳細パネルの [管理（Management）] 領域で、[NAT] NAT をクリックします。
4. + > [Twice NAT] をクリックします。
   - セクション 1 で、[静的（Static）] を選択します。 [続行（Continue）] をクリックします。
   - セクション 2 で、[送信元インターフェイス（Source Interface）] = [内部（inside）] および [宛先インターフェイス（Destination Interface）] = [外部（outside）] を選択します。[続行（Continue）] をクリックします。
   - セクション 3 で、[送信元の元のアドレス（Source Original Address）] = 'boulder-network' および [送信元の変換後アドレス（Source Translated Address）] = 'boulder-network' を選択します。
   - [宛先を使用（Use Destination）] を選択します。

- [宛先の元のアドレス（Destination Original Address）] = 'sanjose-network' および [送信元の変換後アドレス（Source Translated Address）] = 'sanjose-network' を選択します。**注**：宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート（Port）] フィールドはすべて空白のままにします。このルールは、送信元と宛先の両方のアイデンティティ NAT を設定します。

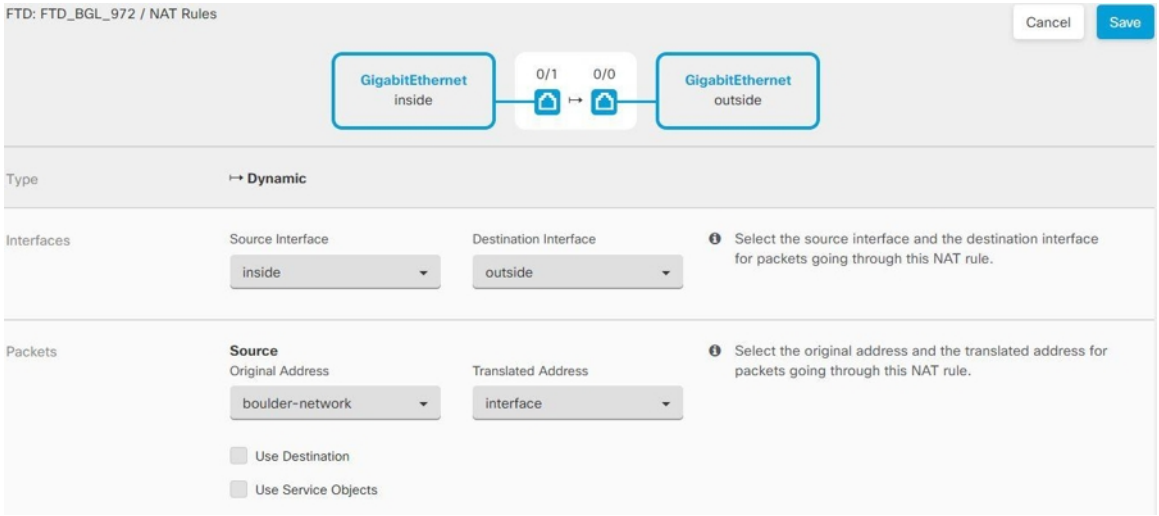


- [着信パケットのプロキシ ARP の無効化（Disable proxy ARP for incoming packets）] を選択します。
- [保存（Save）] をクリックします。
- 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

ステップ 3 Firewall1（ボールダー）上でボールダーの内部ネットワークのインターネットに入る場合、手動ダイナミック インターフェイス PAT を設定します。注：IPv4 トラフィックを対象とする内部インターフェイス用ダイナミック インターフェイス PAT ルールは、初期設定時にデフォルトで作成されるので、既に存在する可能性があります。ただし、この設定は説明を完結させるために示しています。この手順を完了する前に、内部インターフェイスとネットワークをカ

バーするルールがすでに存在していることを確認して、存在している場合はこの手順をスキップしてください。

1. + > [Twice NAT] をクリックします。
2. セクション 1 で、[ダイナミック（Dynamic）] を選択します。[続行（Continue）] をクリックします。
3. セクション 2 で、[送信元インターフェイス（Source Interface）] = [内部（inside）] および [宛先インターフェイス（Destination Interface）] = [外部（outside）] を選択します。[続行（Continue）] をクリックします。
4. セクション 3 で、[送信元の元のアドレス（Source Original Address）] = 'boulder-network' および [送信元の変換後アドレス（Source Translated Address）]='インターフェイス（interface）' を選択します。



5. [保存（Save）] をクリックします。
6. 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

ステップ 4 設定変更を CDO に展開します。詳細については、「CDO から FTD への設定変更の展開」を参照してください。

ステップ 5 Firewall2（サンノゼ）の管理を行っている場合、そのデバイスに同様のルールを設定できます。

- 手動アイデンティティ NAT ルールは、宛先が boulder-network の場合は sanjose-network 向けになります。Firewall2 の内部および外部ネットワーク向けに新しいインターフェイスオブジェクトを作成します。
- 手動ダイナミックインターフェイス PAT ルールは、宛先が「任意」の場合は sanjose-network 向けになります。

グローバル IKE ポリシーの設定

Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

IKE ポリシー オブジェクトはこれらのネゴシエーションに対して IKE プロポーザルを定義します。有効にするオブジェクトは、ピアが VPN 接続をネゴシエートするときに使用するものであり、接続ごとに異なる IKE ポリシーを指定することはできません。各オブジェクトの相対的な優先順位は、これらの中でどのポリシーを最初に試行するかを決定します。数が小さいほど、優先順位が高くなります。ネゴシエーションで両方のピアがサポートできるポリシーを見つけられなければ、接続は確立されません。

IKE グローバル ポリシーを定義するには、各 IKE バージョンを有効にするオブジェクトを選択します。事前定義されたオブジェクトが要件を満たさない場合、セキュリティ ポリシーを適用する新しいポリシーを作成します。

次に、オブジェクト ページでグローバル ポリシーを設定する方法について説明します。VPN 接続を編集しているときに IKE ポリシー設定の [編集（Edit）] をクリックすることで、ポリシーの有効化、無効化および作成が行えます。

次に、各バージョンの IKE ポリシーの設定方法を説明します。

- IKEv1 ポリシーの設定
- IKEv2 ポリシーの設定

IKEv1 ポリシーの管理

IKEv1 ポリシーを作成および編集する方法について説明します。

IKEv1 ポリシーについて

インターネット キー エクスチェンジ（IKE）バージョン 1 ポリシー オブジェクトには、VPN 接続を定義する際に必要な IKEv1 ポリシーが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動確立に使用されます。

複数の事前定義された IKEv1 ポリシーが存在します。必要に適したポリシーがあれば、[状態（State）] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

関連トピック

IKEv1 ポリシーの作成または編集 （271 ページ）

IKEv1 ポリシーの作成または編集

次に、オブジェクトページからオブジェクトを直接作成および編集する方法について説明します。サイト間 VPN 接続での IKE 設定の編集時に、オブジェクトリストに表示される [新しい IKEv1 ポリシーの作成（Create New IKEv1 Policy）] リンクをクリックして、IKEv1 ポリシーを作成することもできます。

手順

ステップ 1 CDO ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青色のプラスボタン  をクリックし、**[FTD]** > **[IKEv1 ポリシー（IKEv1 Policy）]** を選択して、新しい IKEv1 ポリシーを作成します。
- オブジェクトのページで、編集する IKEv1 ポリシーを選択し、右側の [操作（Actions）] ウィンドウで [編集（Edit）] をクリックします。

ステップ 3 [オブジェクト名（Object Name）] を 128 文字以内で入力します。

ステップ 4 IKEv1 プロパティを設定します。

- [優先順位（Priority）]：IKE ポリシーの相対的優先順位（1 ～ 65,535）。このプライオリティによって、共通のセキュリティアソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最も高いプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。
- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティ アソシエーション（SA）の確立に使用される暗号化アルゴリズム。オプションの説明については、「使用する暗号化アルゴリズムの決定」を参照してください。
- [Diffie-Hellmanグループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密を互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。オプションの説明については、「使用する Diffie-Hellman 係数グループの決定」を参照してください。

- [ライフタイム（Lifetime）]：セキュリティアソシエーション（SA）のライフタイム（120～2147483647までの秒数、または空白）。このライフタイムを超えると、SAの期限が切れ、2つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKEネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後のIPsecセキュリティアソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは86400です。無期限のライフタイムを指定するには、値を入力しません（フィールドを空白のままにします）。
- [認証（Authentication）]：2つのピア間で使用される認証方式。詳細については、「使用する認証方式の決定」を参照してください。
  - [事前共有キー（Preshared Key）]：各デバイスで定義されている事前共有キーを使用します。事前共有キーを使用すると、秘密鍵を2つのピア間で共有し、認証フェーズ中にIKEで使用できます。ピアに同じ事前共有キーが設定されていない場合は、IKE SAを確立できません。
  - [証明書（Certificate）]：ピアのデバイスID証明書を使用して相互に識別します。認証局に各ピアを登録することによって、これらの証明書を取得する必要があります。また、各ピアでアイデンティティ証明書の署名に使用された、信頼できるCAルート証明書および中間CA証明書もアップロードする必要があります。ピアは、同じCAまたは別のCAに登録できます。どちらのピアにも自己署名証明書を使用することはできません。
- [ハッシュ（Hash）]：メッセージの整合性の確保に使用されるメッセージダイジェストを作成するためのハッシュアルゴリズム。オプションの説明については、「使用するDiffie-Hellman係数グループの決定」を参照してください。

ステップ5 [追加（Add）]をクリックします。

IKEv2 ポリシーの管理

IKEv2ポリシーを作成および編集する方法について説明します。

IKEv2 ポリシーについて

インターネットキーエクスチェンジ（IKE）バージョン2ポリシーオブジェクトには、VPN接続を定義する際に必要なIKEv2ポリシーが含まれています。IKEは、IPsecベースの通信の管理を簡易化するキー管理プロトコルです。IPsecピアの認証、IPsec暗号キーのネゴシエーションと配布、およびIPsecセキュリティアソシエーション（SA）の自動確立に使用されます。

複数の事前定義されたIKEv2ポリシーがあります。必要に適したポリシーがあれば、[状態（State）]トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

関連トピック

IKEv2 ポリシーの作成または編集 （273 ページ）

IKEv2 ポリシーの作成または編集

次に、オブジェクトページからオブジェクトを直接作成および編集する方法について説明します。サイト間 VPN 接続での IKE 設定の編集時に、オブジェクトリストに表示される [新しいIKEv2ポリシーの作成（Create New IKEv2 Policy）] リンクをクリックして、IKEv2 ポリシーを作成することもできます。

手順

ステップ 1 CDO ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青色のプラスボタン  をクリックし、**[FTD]** > **[IKEv2ポリシー（IKEv2 Policy）]** を選択して、新しい IKEv2 ポリシーを作成します。
- オブジェクトページで、編集する IKEv2 ポリシーを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 [オブジェクト名（Object Name）] を 128 文字以内で入力します。

ステップ 4 IKEv2 プロパティを設定します。

- [優先順位（Priority）]：IKE ポリシーの相対的優先順位（1 ～ 65,535）。このプライオリティによって、共通のセキュリティアソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最も高いプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。
- [状態（State）]：IKE ポリシーが有効か無効かを示します。トグルをクリックして状態を変更します。IKE ネゴシエーション中には、有効なポリシーのみが使用されます。
- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティ アソシエーション（SA）の確立に使用される暗号化アルゴリズム。有効にするすべてのアルゴリズムを選択します。ただし、同じポリシーに混合モード（AES-GCM）と通常モードのオプションを含めることはできません（通常モードでは整合性ハッシュを選択する必要がありますが、混合モードでは個別の整合性ハッシュの選択は禁止されています）。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、「使用する暗号化アルゴリズムの決定」を参照してください。
- [Diffie-Hellmanグループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密を互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほど

セキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。許可するすべてのアルゴリズムを選択します。システムは、最も強いグループから始めて最も弱いグループに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、「使用する Diffie-Hellman 係数グループの決定」を参照してください。

- [整合性ハッシュ（Integrity Hash）]：メッセージの整合性の確保に使用されるメッセージダイジェストを作成するためのハッシュアルゴリズムの整合性部分。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。整合性ハッシュは、AES-GCM 暗号化オプションでは使用されません。オプションの説明については、「使用するハッシュ アルゴリズムの決定」を参照してください。
- [擬似ランダム関数（PRF）ハッシュ（Pseudo-Random Function (PRF) Hash）]：ハッシュアルゴリズムの疑似ランダム関数（PRF）部分。このアルゴリズムは IKEv2 トンネル暗号化に必要なキー関連情報とハッシュ操作を取得するために使用されます。IKEv1 では、整合性と PRF アルゴリズムは別ですが、IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、「使用するハッシュアルゴリズムの決定」を参照してください。
- [ライフタイム（Lifetime）]：セキュリティアソシエーション（SA）のライフタイム（120 ～ 2147483647 までの秒数、または空白）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは 86400 です。無期限のライフタイムを指定するには、値を入力しません（フィールドを空白のままにします）。

ステップ 5 [追加（Add）] をクリックします。

IPsec プロポーザルの設定

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2 つのピア間のセキュアで論理的な通信パスです。IPsec トンネルを通過するトラフィックは、トランスフォーム セットと呼ばれるセキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。IPsec Security Association（SA：セキュリティアソシエーション）のネゴシエーション中に、ピアでは、両方のピアに共通するトランスフォーム セットが検索されます。

IKE バージョン（IKEv1 または IKEv2）に基づいて、別個の IPsec プロポーザル オブジェクトがあります。

- IKEv1 IPsec プロポーザルを作成する場合、IPSec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。アルゴリズムには単一のオプションを選択できます。VPN で複数の組み合わせをサポートするには、複数の IKEv1 IPsec プロポーザル オブジェクトを作成して選択します。
- IKEv2 IPsec プロポーザルを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュアルゴリズムを選択できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、マッチが見つかるまでピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

カプセル化セキュリティ プロトコル（ESP）は、IKEv1 と IKEv2 IPsec プロポーザルの両方に使用されます。これは認証、暗号化、およびアンチリプレイ サービスを提供します。ESP は、IP プロトコル タイプ 50 です。

（注） IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

次に、各 IKE バージョンの IPsec プロポーザルの設定方法を説明します。

- IKEv1 IPSec プロポーザルオブジェクトの作成および編集
- IKEv2 IPSec プロポーザルオブジェクトの作成および編集

IPsec プロポーザルオブジェクトの管理

IPsec プロポーザル オブジェクトは、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。IKEv1 と IKEv2 に対して、異なるオブジェクトがあります。現在、Cisco Defense Orchestrator（CDO）は IKEv1 IPsec プロポーザルオブジェクトをサポートしています。

カプセル化セキュリティ プロトコル（ESP）は、IKEv1 と IKEv2 IPsec プロポーザルの両方に使用されます。このプロトコルにより、認証、暗号化、およびアンチリプレイサービスが実現します。ESP は、IP プロトコル タイプ 50 です。

（注） IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

関連トピック

IKEv1 IPSec プロポーザルオブジェクトの作成または編集 （276 ページ）

IKEv1 IPSec プロポーザルオブジェクトの作成または編集

定義済みの複数の IKEv1 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトの編集や削除はできません。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。サイト間 VPN 接続の IKEv1 IPSec 設定を編集している間に、オブジェクトリストに表示される [新規IKEv1プロポーザルの作成（Create New IKEv1 Proposal）] リンクをクリックして、IKEv1 IPSec プロポーザルオブジェクトを作成することもできます。

手順

ステップ 1 CDO ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青色のプラスボタン をクリックし、**[FTD] > [IKEv1 IPSecプロポーザル（IKEv1 IPsec Proposal）]** を選択して新しいオブジェクトを作成します。
- オブジェクトページで、編集する IPSec プロポーザルを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 新しいオブジェクトのオブジェクト名を入力します。

ステップ 4 IKEv1 IPSec プロポーザルオブジェクトが動作するモードを選択します。

- トンネルモードでは IP パケット全体がカプセル化されます。IPSec ヘッダーが、元の IP ヘッダーと新しい IP ヘッダーとの間に追加されます。これがデフォルトです。トンネルモードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネルモードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイアウォール（またはその他のセキュリティ ゲートウェイ）間で通常の IPSec が実装される標準の方法です。
- トランスポートモードでは IP パケットの上位層プロトコルだけがカプセル化されます。IPSec ヘッダーは、IP ヘッダーと上位層プロトコル ヘッダー（TCP など）との間に挿入されます。トランスポート モードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポート モードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。一般的に、トランスポート モードは、レイヤ 2 またはレイヤ 3 のトンネリング プロトコル（GRE、L2TP、DLSW など）を保護する場合にだけ使用されます。

ステップ 5 このプロポーザルの [ESP暗号化（ESP Encryption）]（カプセル化セキュリティプロトコル暗号化）アルゴリズムを選択します。オプションの説明については、「使用する暗号化アルゴリズムの決定」を参照してください。

ステップ 6 認証に使用する [ESPハッシュ（ESP Hash）] または整合性アルゴリズムを選択します。オプションの説明については、「使用するハッシュ アルゴリズムの決定」を参照してください。

ステップ 7 [追加（Add）] をクリックします。

IKEv2 IPsec プロポーザルオブジェクトの管理

IPsec プロポーザル オブジェクトは、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。

IKEv2 IPsec プロポーザルを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、マッチが見つかるまでピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

関連トピック

IKEv2 IPSec プロポーザルオブジェクトの作成または編集 （277 ページ）

IKEv2 IPSec プロポーザルオブジェクトの作成または編集

定義済みの複数の IKEv2 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトの編集や削除はできません。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。VPN 接続の IKEv2 IPsec 設定を編集している間に、オブジェクト リストに表示される [新規IPsecプロポーザルの作成（Create New IPsec Proposal）] リンクをクリックして、IKEv2 IPsec プロポーザル オブジェクトを作成することもできます。

手順

ステップ 1 CDO ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青色のプラスボタン  をクリックし、**[FTD]> [IKEv2 IPSecプロポーザル（IKEv2 IPsec Proposal）]** を選択して新しいオブジェクトを作成します。
- オブジェクトページで、編集する IPSec プロポーザルを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 新しいオブジェクトのオブジェクト名を入力します。

ステップ 4 IKEv2 IPsec プロポーザルオブジェクトの設定：

- [暗号化（Encryption）]：このプロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できる

までピアとネゴシエートします。オプションの説明については、「使用する暗号化アルゴリズムの決定」を参照してください。

- [整合性ハッシュ（Integrity Hash）]：認証に使用するハッシュまたは整合性アルゴリズム。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、「使用するハッシュアルゴリズムの決定」を参照してください。

ステップ 5 [追加（Add）] をクリックします。

リモートアクセス仮想プライベートネットワーク

リモートアクセス仮想プライベートネットワーク（RA VPN）では、各ユーザーがインターネットに接続されたコンピュータまたはその他のサポート対象の iOS または Android デバイスを使用して、離れた場所からネットワークに接続できます。これにより、モバイルワーカーが各自のホームネットワークや公共のWi-Fiネットワークから接続できるようになります。

RA VPN 設定は、次のコンポーネントで構成されています。

- 接続プロファイル：リモートアクセス VPN 接続プロファイルを作成すると、ホームネットワークなどの外部ネットワークからでも、ユーザーは内部ネットワークに接続できるようになります。異なる認証方式に対応するために、個別のプロファイルを作成します。接続プロファイルは、アイデンティティソースとグループポリシーで構成されます。

関連情報：

-
- FTD のリモートアクセス VPN を設定する

リモートアクセス仮想プライベート ネットワーク セッションのモニタリング

リモートアクセス仮想プライベートネットワーク（RA VPN）は、モバイルユーザーや在宅勤務者などのリモートユーザーにセキュアな接続を提供します。これらの接続をモニタリングすることで、接続とユーザーセッションのパフォーマンスの重要なインジケータを一目で把握できます。CDO リモートアクセス VPNのモニタリング機能を使用すると、リモートアクセス VPN の問題が存在するかどうか、および存在する場所を迅速に特定できます。この情報を利用し、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。また、必要に応じてリモートアクセス VPN ユーザーをログアウトできます。

[リモートアクセス仮想プライベートモニタリング（Remote Access Virtual Private Monitoring）] ページには、[ライブ（Live）] と [履歴（Historical）] の 2 つのビューがあります。テナント内のすべての Firepower Threat Defense（FTD） VPN ヘッドエンドの AnyConnect リモートアクセス VPN セッションからリアルタイムデータまたは履歴データをモニタリングするために必要なビューを選択できます。

[リモートアクセス仮想プライベートモニタリング（Remote Access Virtual Private Monitoring）] ページには、各 RA VPN セッションからの次の情報が表示されます。

- RA VPN セッションからのライブデータと履歴データを提供します。
- CDO が管理するすべてのアクティブな VPN ヘッドエンドから一目でわかるビューを提供する直感的なグラフィカルビジュアルを表示します。
- ライブセッション画面には、CDO テナントで最も使用されているオペレーティングシステムと VPN 接続プロファイルが表示されます。また、平均セッション時間とアップロードおよびダウンロードされたデータも表示されます。
- ライブセッション画面には、RA VPN ヘッドエンドに接続されているユーザーの場所を可視化するためのインタラクティブなヒートマップが表示されます。
- 履歴セッション画面には、過去 24 時間、7 日間、および 30 日間にすべてのデバイスについて記録されたデータを示す棒グラフがプロットされます。
- デバイスの種類、セッションの長さ、アップロードとダウンロードのデータ範囲などの基準に基づいて検索を絞り込むための新しいフィルタリング機能を提供します。
- ユーザー名、ログイン時間、期間、およびセッションが非アクティブだった時間。
- エンタープライズ ネットワーク内で割り当てられた IP アドレスと、セッションが開始されたパブリック IP アドレス。
- セッションに関連付けられた接続プロファイルとグループポリシー情報。
- ユーザーセッションで使用される AnyConnect のバージョンとオペレーティングシステムのタイプ。
- セッションタイムアウトまでの残りのアイドル時間。

関連情報：

- AnyConnect リモートアクセス VPN ライブセッションのモニタリング （279 ページ）
- AnyConnect リモートアクセス VPN セッション履歴のモニタリング （281 ページ）
- リモートアクセス VPN セッションの検索とフィルタ処理
- リモートアクセス VPN モニタリングビューのカスタマイズ
- RA VPN セッションの CSV ファイルへのエクスポート
- FTD でのアクティブなリモートアクセス VPN セッションの切断

AnyConnect リモートアクセス VPN ライブセッションのモニタリング

デバイス上のアクティブな AnyConnect RA VPN セッションからのリアルタイムデータを監視できます。このデータは 10 分ごとに更新されます。画面の右隅に表示されるリロードアイコン をクリックすると、最新のデータを確認できます。

始める前に

- RA VPN ヘッドエンドを CDO にオンボーディングします。
- ライブデータを監視するデバイスの接続ステータスは、[インベントリ（Inventory）] ページで「オンライン」になっています。

手順

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）]** をクリックします。

または、CDO ホームページで [アクティブリモートアクセスVPNセッションの表示（View Active Remote Access VPN Sessions）] をクリックするか、**[VPN]** > **[リモートアクセスVPN（Remote Access VPN）]** に移動して、右上隅の アイコンをクリックします。

ステップ 2 [ライブ（Live）] をクリックします。

CDO はデバイスからのライブ情報の取得を開始し、[リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）] ビューに RA VPN セッションを表示します。

（注） CDO がデバイスから情報を取得しないようにする場合は、[キャンセル（Cancel）] をクリックします。

ライブデータの表示

ライブデータは、ダッシュボードと表形式の両方で表示されます。

[ダッシュボード（Dashboard）] ビュー

ダッシュボードを表示するには、画面の右上隅に表示される [v] アイコンをクリックする必要があります。

ダッシュボードには、CDO によって管理されるすべてのアクティブな VPN ヘッドエンドからの一目でわかるビューが表示されます。

- [内訳（すべてのデバイス）（Breakdown (All Devices)）]：ライブセッションの合計数が表示されます。また、4 つの弧の長さに分割された円グラフも表示されます。これは、セッション数が最も多い上位 3 つのデバイスの VPN セッションの割合を示しています。残りの弧の長さは、他のデバイスの総計を表します。
- CDO テナントで最も使用されているオペレーティングシステムと接続プロファイルが表示されます。
- 平均セッション時間とアップロードおよびダウンロードされたデータが表示されます。

- [国別のアクティブセッション（Active Sessions by Country）]：RA VPN ヘッドエンドに接続されているユーザーの場所を可視化するためのインタラクティブなヒートマップが表示されます。
  - ユーザーセッションがある国は、青の色合いで表示されます。
  - マップの下部にある凡例は、国のセッション数とその国の色に使用される青の色合いとの相関関係を示すスケールが表示されます。
  - 地図上にマウスポインタを合わせると、国名とアクティブなユーザーセッションの総数が表示されます。
  - テーブルにマウスポインタを合わせると、その国の場所とアクティブなユーザーセッションの総数が地図上に表示されます。

表形式のビュー

表形式のビューのみを表示するには、画面の右上隅に表示される[表形式のビューを表示（Show Tabular View）]アイコンをクリックする必要があります。

表形式のビューには、現在接続している VPN ユーザーの完全なリストが表示されます。

- [場所（Location）]列には、パブリック IP アドレスを地理的に配置することにより、VPN ヘッドエンドに接続されているすべてのユーザーの場所が表示されます。行をクリックして、ユーザーの詳細を表示します。左ペインのロケーションリンクをクリックすると、ユーザーの場所が Google マップ上に表示されます。

重要 CDO は、ライブデータに標準フィルタを適用し、ダッシュボードにデータを表示します。ダッシュボードではカスタムフィルタはサポートされていないため、表形式のデータが表示されている場合にのみ、新しいフィルタを適用できます。新たに適用されたフィルタをクリアすると、ダッシュボードが再起動します（画面で[クリア（Clear）]をクリックして、適用されたフィルタを手動で削除します）。標準フィルタは削除できません。

[RA VPNセッションの検索およびフィルタリング（Search and Filter RA VPN Sessions）]機能を使用して、デバイスタイプ、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの基準に基づいて検索を絞り込むことができます。リモートアクセス VPN セッションの検索とフィルタ処理 （283 ページ）一度に表示できる結果は最大 10,000 件です。

ステータス列の「アクティブ（Active）」ラベルの付いた緑色の点は、アクティブな VPN ユーザーのセッションを示します。

AnyConnect リモートアクセス VPN セッション履歴のモニタリング

過去 3 か月間に記録された AnyConnect リモートアクセス VPN セッションの履歴データをモニタリングできます。

始める前に

- RA VPN ヘッドエンドの CDO への導入準備をします。
- 履歴データを監視するデバイスの接続状態は、[インベントリ（Inventory）] ページで「オンライン」になっています。

手順

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）]** をクリックします。

または、CDO ホームページで [アクティブリモートアクセスVPNセッションの表示（View Active Remote Access VPN Sessions）] をクリックするか、**[VPN]** > **[リモートアクセスVPN]（Remote Access VPN）** に移動して、右上隅の アイコンをクリックします。

ステップ 2 [履歴（Historical）] をクリックします。

CDO には、過去 3 か月間に記録された RA VPN セッションの履歴データが表示されます。

（注） CDO がデバイスから情報を取得しないようにする場合は、[キャンセル（Cancel）] をクリックします。

履歴データの表示

履歴データは、ダッシュボードと表形式の両方で表示されます。

[ダッシュボード（Dashboard）] ビュー

ダッシュボードを表示するには、画面の右上隅に表示される [チャートビューの表示（Show Charts View）] アイコンをクリックする必要があります。表形式のビューとともに、ダッシュボードビューが表示されます。

ダッシュボードには、CDO によって管理されるすべてのアクティブな VPN ヘッドエンドからの一目でわかるビューが表示されます。過去 24 時間、7 日間、および 30 日間にすべてのデバイスで記録された VPN セッションを示す棒グラフが表示されます。ドロップダウンから期間を選択できます。個々のバーにカーソルを合わせると、日付とその日の合計セッション数が表示されます。

表形式のビュー

表形式のビューのみを表示するには、画面の右上隅に表示される [表形式のビューを表示（Show Tabular View）] アイコンをクリックする必要があります。表形式には、過去 3 か月間に接続した VPN ユーザーの完全なリストが表示されます。

[場所（Location）] 列には、パブリック IP アドレスを地理的に配置することにより、VPN ヘッドエンドに接続されているすべてのユーザーの場所が表示されます。行をクリックして、ユー

ザーの詳細を表示します。左ペインのロケーションリンクをクリックすると、ユーザーの場所が Google マップ上に表示されます。

重要 CDO は、履歴データに標準フィルタを適用し、ダッシュボードに表示します。ダッシュボードではカスタムフィルタはサポートされていないため、表形式のデータが表示されている場合にのみ、新しいフィルタを適用できます。新たに適用されたフィルタをクリアすると、ダッシュボードが再起動します（画面で [クリア（Clear）] をクリックして、適用されたフィルタを手動で削除します）。標準フィルタは削除できません。

[RA VPNセッションの検索およびフィルタリング（Search and Filter RA VPN Sessions）]リモートアクセスVPNセッションの検索とフィルタ処理（283ページ）機能を使用して、セッションの日と時間の範囲、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの条件に基づいて検索を絞り込むことができます。一度に表示できる結果は最大10,000件です。

ステータス列の「アクティブ（Active）」ラベルの付いた緑色の点は、アクティブなVPNユーザーのセッションを示します。

リモートアクセス VPN セッションの検索とフィルタ処理

検索（Search）

検索バー機能を使用して、RA VPN セッションを検索します。検索バーにデバイス名、IP アドレス、またはシリアル番号を入力し始めると、検索条件に一致するRA VPNセッションが表示されます。検索では大文字と小文字が区別されません。

Filter

フィルタサイドバーを使用して、セッション時間の範囲、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの条件に基づいてRA VPNを特定できます。フィルタ機能は、ライブビューと履歴ビューの両方で使用できます。

- [デバイス（Device）]：1つまたはすべてのデバイスを選択して、選択したデバイスからのセッションを表示します。
- [セッションの時間範囲（Sessions Time Range）]（履歴データにのみ適用）：指定した日時範囲のセッションの履歴を表示します。表示できるのは、過去 3 か月間に記録されたデータのみです。
- [セッションの長さ（Sessions Length）]：指定されたセッションの継続時間に基づいてセッションを表示します。時間の単位（時間、分、または秒）を設定し、スライダを動かして、継続時間の最小長と最大長を指定します。表示されたフィールドで長さを指定することもできます。
- [アップロード（TX）（Upload (TX)）]：セキュリティで保護されたネットワークにアップロードまたは転送されたデータの指定量に基づいてセッションを表示します。単位（GB、MB、またはKB）を設定し、スライダを適宜動かして範囲を選択します。表示されるフィールドに値を指定することもできます。

- [ダウンロード（RX）（Download (RX)）]：セキュリティで保護されたネットワークからダウンロードまたは受信したデータの指定量に基づいてセッションを表示します。単位（GB、MB、または KB）を設定し、スライダを適宜動かして範囲を選択します。表示されるフィールドに値を指定することもできます。

リモートアクセス VPN モニタリングビューのカスタマイズ

ライブモードと履歴モードの両方のリモートアクセス VPN モニタリングビューを変更して、必要なビューに適用される列ヘッダーのみを含めることができます。列の右側にある列フィルタアイコン をクリックし、必要な列を選択または選択解除します。

CDO に次回サインインしたとき、選択した内容が CDO に記憶されています。

RA VPN セッションの CSV ファイルへのエクスポート

1 つ以上のデバイスの RA VPN セッションをコンマ区切り値（.csv）ファイルにエクスポートできます。Microsoft Excel などのスプレッドシート アプリケーションで .csv ファイルを開いて、リストの項目を並べ替えたり、フィルタ処理したりできます。この情報は、RA VPN セッションの分析に役立ちます。セッションをエクスポートするたびに、CDO は new.csv ファイルを作成します。作成されるファイルの名前には日付と時刻が含まれます。

CDO は、最大 100,000 のアクティブセッションを CSV ファイルにエクスポートできます。すべてのデバイスからのセッションの合計数が上限を超えている場合は、[デバイス別表示（View By Device）] フィルタを使用して、個々のデバイスのレポートを生成できます。

手順

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）]** をクリックします。

ステップ 2 [デバイス別表示（View By Devices）] 領域で、次のいずれかを選択します。

- [すべてのデバイス（All Devices）] は、その下に一覧表示されているすべてのデバイスからアクティブセッションをエクスポートします。
- セッションをエクスポートするデバイスをクリックします。

ステップ 3 右上隅の アイコンをクリックします。CDO は、画面に表示されているルールを .csv ファイルにエクスポートします。

ステップ 4 スプレッドシート アプリケーションで .csv ファイルを開いて、結果を並べ替えたりフィルタリングしたりすることができます。

FTD でのアクティブなリモートアクセス VPN セッションの切断

現在のところ、CDO インターフェイスを使用して FTD で RA VPN セッションを終了できません。代わりに、SSH を使用して FTD CLI に接続し、目的のユーザーを切断できます。このタスクは、CDO にオンボードされたオンライン FTD デバイスで実行できます。

手順

ステップ 1 デバイスが実行しているバージョンの『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）』で、「使用する前に」章の「**CLI（コマンドライン インターフェイス）へのログイン**」項の説明に従い、FDM にログオンしてデバイス CLI を使用します。

ステップ 2 `vpn-sessionsdb logoff {name}` コマンドを実行します（**name** はユーザー名に置き換えます）。このコマンドは、指定したユーザー名のすべてのセッションを終了します。

FTD のリモートアクセス VPN を設定する

CDO は、新しいリモートアクセス仮想プライベートネットワーク（RA VPN）を設定するための直感的なユーザーインターフェイスを提供します。また、CDO に搭載されている複数の FTD デバイスの RA VPN 接続をすばやく簡単に設定することもできます。AnyConnect はエンドポイントデバイスでサポートされている唯一のクライアントで、FTD デバイスへの RA VPN 接続が可能です。

AnyConnect クライアントが FTD デバイスと SSL VPN 接続をネゴシエートする際、Transport Layer Security（TLS）または Datagram Transport Layer Security（DTLS）を使用して接続します。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。クライアントおよび FTD デバイスは、使用する TLS/DTLS バージョンをネゴシエートします。DTLS はクライアントがサポートする場合に使用されます。

CDO は、FTD デバイスでの RA VPN 機能の次の側面をサポートします。

- SSL クライアントベースのリモートアクセス
- IPv4 および IPv6 のアドレッシング
- 複数の FTD デバイス間での共有 RA VPN 設定

重要 オンボード FTD デバイス（ソフトウェアバージョン 6.7 以降で実行）に SAML サーバーを認証ソースとして使用する RA VPN 構成が含まれている場合、CDO は現在のリリースの SAML サーバーオブジェクトを管理しないため、接続プロファイルに AAA 詳細を入力しません。したがって、CDO からそのような RA VPN 設定を管理することはできません。ただし、CDO は RA VPN 接続プロファイルと、関連する信頼できる CA 証明書と SAML サーバーオブジェクトを読み取ります。

関連情報：

- RADIUS およびグループポリシーを使用したユーザーの権限および属性の制御
- FTD のためのエンドツーエンドの FTD リモートアクセス VPN 設定プロセス
  - AnyConnect クライアント ソフトウェア パッケージのダウンロード
  - AnyConnect ソフトウェアパッケージの FTD バージョン 6.4.0 へのアップロード
  - AnyConnect ソフトウェアパッケージの FTD バージョン 6.5 以降が動作する FTD デバイスへのアップロード
  - RA VPN AnyConnect クライアントプロファイルのアップロード （348 ページ）
  - FTD のアイデンティティソースの設定
    - FTD アクティブ ディレクトリ レルム オブジェクトの作成または編集
    - FTD RADIUS サーバーオブジェクトまたはグループの作成または編集
  - 新しい FTD RA VPN グループポリシーの作成
  - FTD RA VPN 設定の作成
  - FTD RA VPN 接続プロファイルの設定
  - リモート アクセス VPN によるトラフィックの許可
  - FTD バージョン 6.4.0 での AnyConnect パッケージのアップグレード
- FTD のリモートアクセス VPN のガイドラインと制限事項
- ユーザーが AnyConnect クライアントソフトウェアを FTD にインストールする方法
- リモート アクセス VPN のライセンス要件
- デバイス モデル別の同時 VPN セッションの最大数
- RADIUS 許可の変更
  - FTD デバイスでの認可変更の設定
- RA VPN ユーザー用のスプリットトンネリング（ヘアピニング）
- FTD のリモートアクセス VPN 設定の確認
- FTD のリモートアクセス VPN 設定の詳細表示

RA VPN ユーザー用のスプリットトンネリング（ヘアピニング）

この記事では、RA VPN でのスプリットトンネリングについて説明します。

通常、リモートアクセス VPN では、VPN ユーザーに自社のデバイスを介してインターネットにアクセスさせます。ただし、RA VPN に接続している VPN ユーザーに、外部ネットワーク

へのアクセスを許可することができます。この技術は、スプリットトンネリングまたはヘアピニングと呼ばれます。スプリットトンネルでは、セキュアトンネル経由のリモートネットワークへの VPN 接続が可能ですが、VPN トンネル外のネットワークにも接続できます。スプリットトンネリングは、FTDデバイスのネットワーク負荷を軽減し、外部インターフェイスの帯域幅を拡大します。

スプリットトンネル リストを設定するには、標準アクセス リストまたは拡張アクセス リストを作成する必要があります。実行中のデバイスバージョンの『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Virtual Private Networks (VPN)」の章にある「**How to Provide Internet Access on the Outside Interface for Remote Access VPN Users (Hair Pinning)**」セクションで説明されている手順に従ってください。

RADIUS およびグループポリシーを使用したユーザーの権限および属性の制御

ここでは、外部 RADIUS サーバーまたはグループポリシーから RA VPN 接続に属性を適用する方法について説明します。

外部RADIUSサーバーまたはFTDデバイスで定義されているグループポリシーから、RA VPN接続にユーザーの認可属性（ユーザーの権利または権限とも呼ばれる）を適用できます。FTDデバイスが、グループポリシーに設定されている属性と競合する属性を外部 AAA サーバーから受信した場合は、AAA サーバーからの属性が常に優先されます。

FTD デバイスは次の順序で属性を適用します。

手順

ステップ 1 AAA サーバー上で定義されたユーザー属性：ユーザー認証や認可が成功すると、サーバーからこの属性が返されます。

ステップ 2 FTDデバイス上で設定されているグループポリシー：RADIUSサーバーからユーザーのRADIUS CLASS 属性 IETF-Class-25（OU=group-policy）の値が返された場合は、FTD デバイスはそのユーザーを同じ名前のグループポリシーに入れて、そのグループポリシーの属性のうち、サーバーから返されないものを適用します。

ステップ 3 接続プロファイルによって割り当てられたグループポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザーに適用されるデフォルトのグループポリシーが含まれています。FTDデバイスに接続するすべてのユーザーは、最初にこのグループに所属します。このグループでは、AAA サーバーから返されるユーザー属性、またはユーザーに割り当てられたグループポリシーにはない属性が定義されています。

FTDデバイスは、ベンダー ID 3076 の RADIUS 属性をサポートします。使用する RADIUS サーバーにこれらの属性が定義されていない場合は、手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダー コード（3076）を使用します。

次のトピックでは、サポートされている属性値について、値がRADIUSサーバーで定義されるかどうか、またはRADIUSサーバーにシステムが送信する値であるかどうかに基づいて説明します。

RADIUS サーバーに送信された属性

RADIUS 属性 146 および 150 は、認証および許可の要求の場合に FTD デバイスから RADIUS サーバーに送信されます。次の属性はすべて、アカウンティング開始、中間アップデート、および終了の要求の場合に FTD デバイスから RADIUS サーバーに送信されます。

表 *6 : FTD* から *RADIUS* に送信される属性

属性（Attribute）	属性（Attribute）	構文、タイプ	シングルまたはマルチ値	説明または値
クライアント タイプ（Client Type）	150	整数	シングル	VPN に接続しているクライアントのタイプは次のとおりです。 2 = AnyConnect クライアント SSL VPN
セッション タイプ	151	整数	シングル	接続の種類： 1 = AnyConnect クライアント SSL VPN
Tunnel Group Name	146	文字列	シングル	FTDデバイスで定義されているセッションの確立に使用された接続プロファイルの名前。名前には 1 ～ 253 文字を使用できます。

RADIUS サーバーから受信した属性

次のユーザー認可属性が RADIUS サーバーから FTD デバイスに送信されます。

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Access-List-Inbound	86	文字列	シングル	両方の Access-List 属性が、FTDデバイスで設定されている ACL の名前を使用します。スマート CLI 拡張アクセスリストのオブジェクトタイプを使用して、これらの ACL を FDM で作成します（[デバイス（Device）] > [詳細設定（Advanced Configuration）] > [スマートCLI（Smart CLI）] > [オブジェクト（Object）] を選択します）。これらの ACL は、着信（ FTD デバイスに入るトラフィック）または発信（FTDデバイスから出るトラフィック）方向のトラフィックフローを制御します。
Access-List-Outbound	87	文字列	シングル	

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Address-Pools	217	文字列	シングル	FTDデバイスで定義されたネットワークオブジェクトの名前。RA VPN へのクライアント接続のアドレスプールとして使用されるサブネットを識別します。[オブジェクト（Objects）] ページでネットワークオブジェクトを定義します。
Banner1	15	文字列	シングル	ユーザーがログインしたときに表示されるバナー。
Banner2	36	文字列	シングル	ユーザーがログインするときに表示されるバナーの 2 番目の部分。Banner2 は Banner1 に付加されます。

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Group-Policy	25	文字列	シングル	接続に使用されるグループポリシー。RA VPN の [グループポリシー（Group Policy）] ページでグループポリシーを作成する必要があります。次の形式のいずれかを使用できます。 • グループ ポリシー名 • OU=グループポリシー名 • OU=グループポリシー名;
Simultaneous-Logins	2	整数	シングル	ユーザーが確立できる個別の同時接続数。0 ～ 2147483647。
VLAN	140	整数	シングル	ユーザーの接続を制限する VLAN。0 ～ 4094。FTD デバイスのサブインターフェイスでも、この VLAN を設定する必要があります。

二要素認証

RA VPNの二要素認証を設定できます。二要素認証を使用する場合、ユーザーはユーザー名と静的パスワードに加えて、Duoパスコードなどの追加項目を指定する必要があります。二要素認証が 2 番目の認証ソースを使用することと異なるのは、1 つの認証ソースで 2 つの要素が設定され、Duo サーバーとの関係がプライマリ認証ソースに関連付けられている点です。Duo LDAPは例外で、Duo LDAP サーバーをセカンダリ認証ソースとして設定します。

- RADIUS を使用した Duo 二要素認証 （292 ページ）
- LDAP を使用した Duo 二要素認証 （297 ページ）

RADIUS を使用した *Duo* 二要素認証

Duo RADIUS サーバーはプライマリ認証ソースとして設定できます。このアプローチでは、Duo RADIUS 認証プロキシを使用します。

Duo の設定手順の詳細については、https://duo.com/docs/cisco-firepower を参照してください。

その後、最初の認証要素として別の RADIUS サーバーまたは Microsoft Active Directory（AD）サーバーを使用し、2 番目の要素として Duo クラウドサービスを使用するため、プロキシサーバー宛の認証要求を転送するように Duo を設定します。

このアプローチを使用する場合、ユーザーは、Duo 認証プロキシおよび関連する RADIUS/AD サーバーの両方で設定されているユーザー名と、RADIUS/AD サーバーで設定されたユーザー名のパスワード（その後に次のいずれかの Duo コードが続く）を使用して認証する必要があります。

Duo-passcode。my-password,12345 など

push。たとえば、*my-password*,**push** など。**push** は、ユーザーによるインストールと登録が完了している Duo モバイルアプリに認証をプッシュ送信するように Duo に指示する場合に使用します。

sms。たとえば、*my-password*,**sms** など。sms は、ユーザーのモバイルデバイスにパスコードの新しいバッチと SMS メッセージを送信するように Duo に指示する場合に使用します。sms を使用すると、ユーザーの認証試行は失敗します。ユーザーは再認証し、2 番目の要素として新しいパスコードを入力する必要があります。

phone。たとえば、*my-password*,**phone** など。phone は、電話コールバック認証を実行するように Duo に指示する場合に使用します。

ユーザー名とパスワードが認証されると、Duo 認証プロキシは Duo クラウドサービスに接続し、Duo クラウドサービスは、その要求が設定されている有効なプロキシデバイスからのものであることを検証してから、指示に従ってユーザーのモバイルデバイスに一時的なパスコードをプッシュ送信します。ユーザーがこのパスコードを受け入れると、セッションは Duo で認証済みとマークされ、RA VPN が確立されます。

詳細な説明については、Duo RADIUS を使用した二要素認証の設定方法 （292 ページ）を参照してください。

Duo RADIUS を使用した二要素認証の設定方法

Duo RADIUS サーバーはプライマリ認証ソースとして設定できます。このアプローチでは、Duo RADIUS 認証プロキシを使用します。

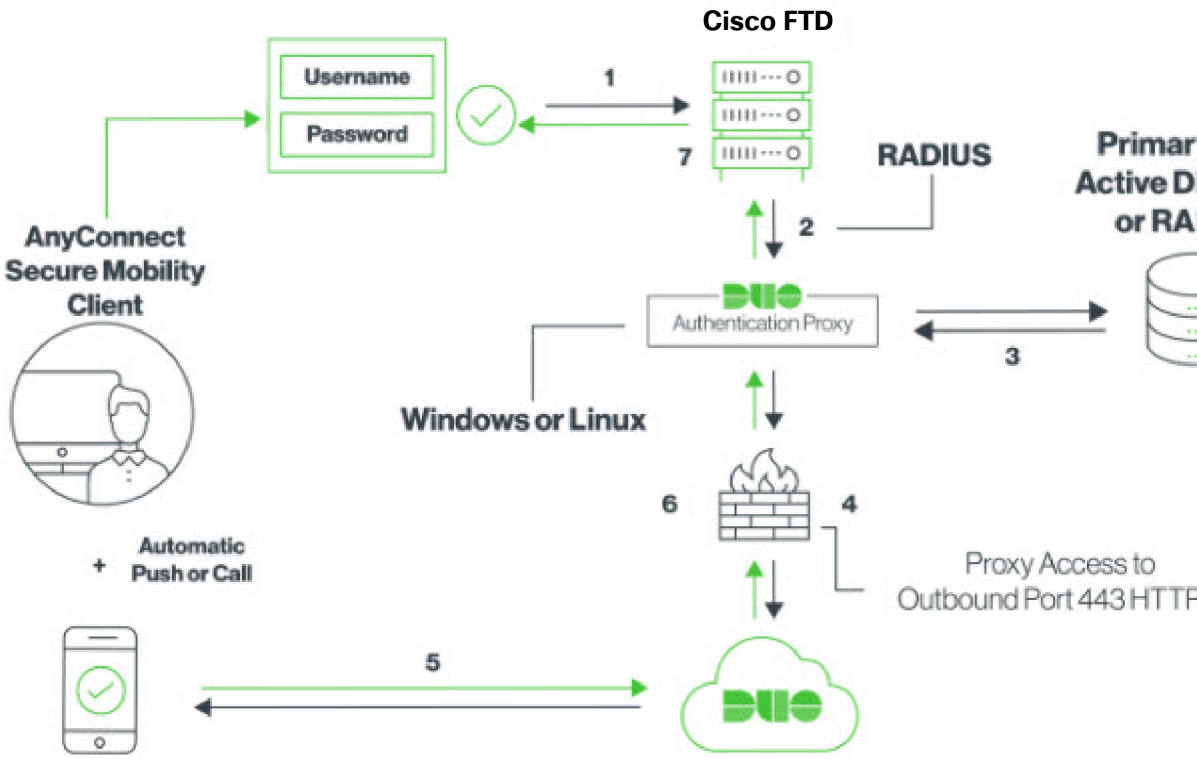
その後、最初の認証要素として別の RADIUS サーバー（または AD サーバー）を使用し、2 番目の要素として Duo クラウド サービスを使用するため、プロキシ サーバー宛の認証要求を転送するように Duo を設定します。

以降のトピックでは設定についてさらに詳しく説明します。

- Duo RADIUS セカンダリ認証のシステムフロー （293 ページ）
- CDO を使用した Duo RADIUS の FTD の設定 （294 ページ）

Duo RADIUS セカンダリ認証のシステムフロー

次に、システムフローについて説明します。



1. ユーザーはFTDデバイスへのリモートアクセスVPN接続を確立し、RADIUS/ADサーバーに関連付けられたユーザー名、RADIUS/AD サーバーで設定されたユーザー名のパスワード、続いていずれかの DUO コード（Duo パスワード、プッシュ、SMS または電話番号）を指定します。詳細については、RADIUS を使用した Duo 二要素認証 （292 ページ）
2. FTD は、認証要求を Duo 認証プロキシに送信します。
3. Duo Authentication Proxy は、プライマリ認証サーバー（Active Directory や RADIUS など）でプライマリ認証の試行を認証します。
4. ログイン情報が認証されると、Duo Security への Duo Authentication Proxy 接続が TCP ポート 443 経由で確立されます。
5. 要求を受けたDuoは、プッシュ通知、パスコード付きのテキストメッセージ、または電話コールによって、ユーザーを個別に認証します。ユーザーはこの認証を正常に完了する必要があります。
6. Duo Authentication Proxy が認証応答を受信します。
7. セカンダリ認証が成功すると、FTD デバイスは、ユーザーの AnyConnect クライアントとのリモート アクセス VPN 接続を確立します。

Duo RADIUS セカンダリ認証の設定

Duo Authentication Proxy は、プライマリ認証サーバー（Active Directory や RADIUS など）でプライマリ認証の試行を認証します。

Duo アカウントの作成

Duo アカウントを作成し、統合鍵、秘密鍵、および API ホスト名を取得します。

次に、プロセスの概要を示します。詳細については、Duo の Web サイトを参照してください。

手順

ステップ 1 Duo アカウントにサインアップします。

ステップ 2 Duo Admin Panel にログインし、[アプリケーション（Applications）] に移動します。

ステップ 3 [アプリケーションの保護（Protect an Application）] をクリックし、アプリケーションリストで **Cisco Firepower Threat Defense VPN** を探します。

ステップ 4 [アプリケーションの保護（Protect this Application）] をクリックし、統合鍵、秘密鍵、および API ホスト名を取得します。この情報は、プロキシを設定するときに必要になります。詳細については、*Duo Getting Started* ガイド（https://duo.com/docs/getting-started）を参照してください。

ステップ 5 Duo Authentication Proxy をインストールして設定します。手順については、https://duo.com/docs/cisco-firepower の「Install the Duo Authentication Proxy」を参照してください。

ステップ 6 認証プロキシを開始します。手順については、https://duo.com/docs/cisco-firepower の「Start the Proxy」を参照してください。

Duo に新しいユーザーを登録する手順については、https://duo.com/docs/enrolling-users を参照してください。

CDO を使用した Duo RADIUS の FTD の設定

手順

ステップ 1 FTD RADIUS サーバーオブジェクトを設定します。

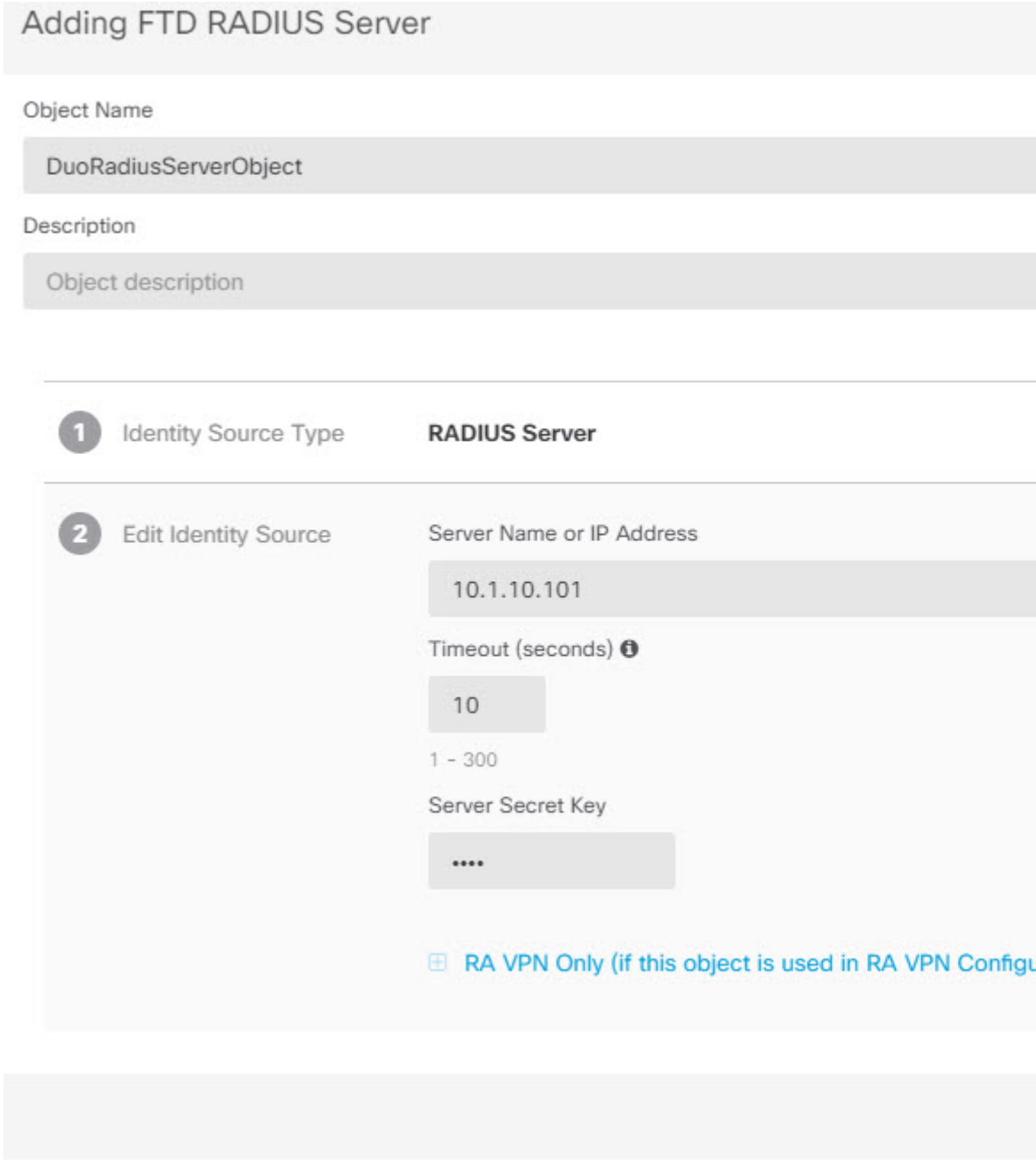
a) CDO ナビゲーションメニューで、[オブジェクト（Objects）] >  > [RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [IDソース（Identity Source）] をクリックします。

b) 名前を指定し、[デバイスタイプ（Device Type）] を [FTD] に設定します。

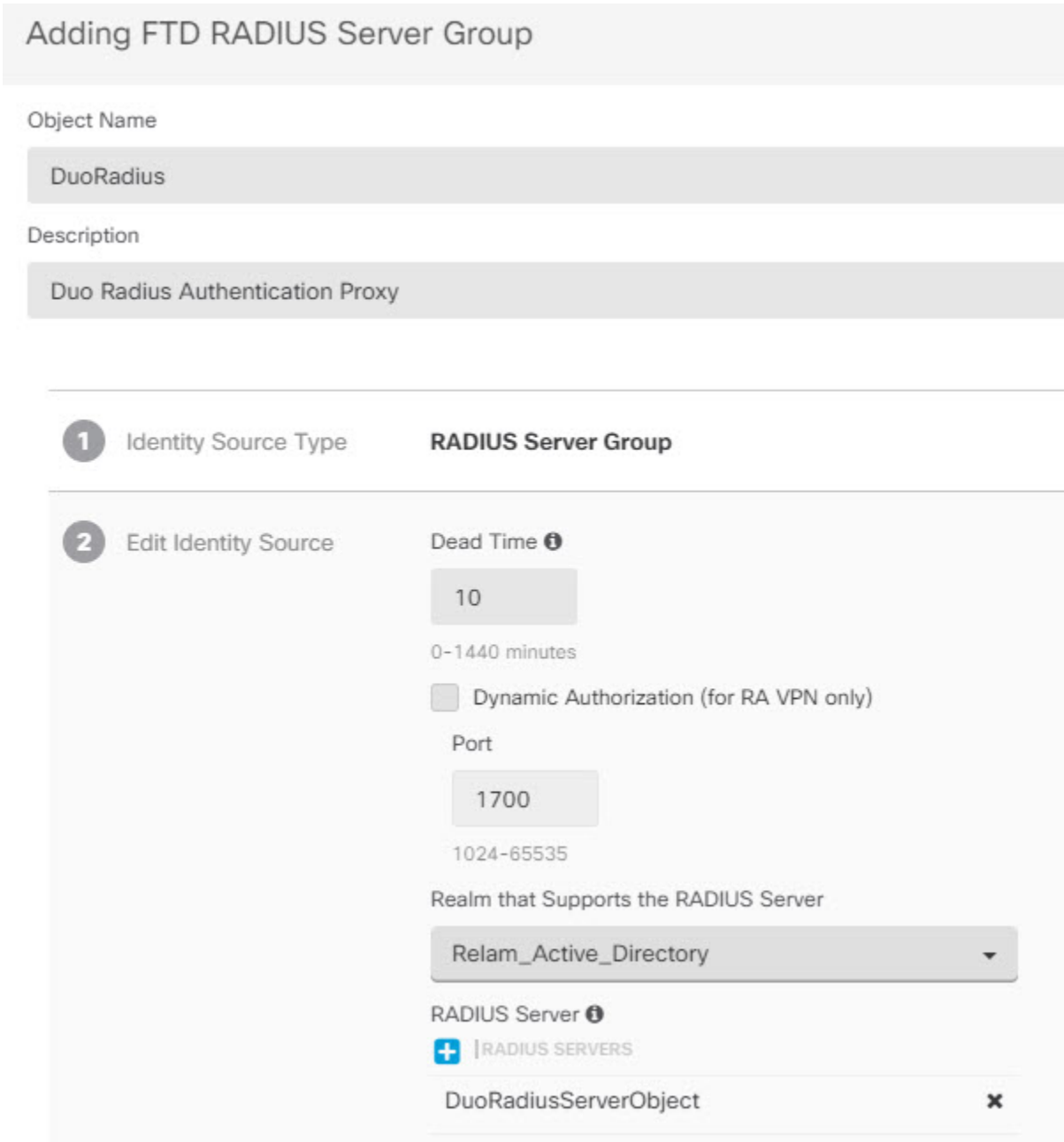
c) [RADIUSサーバーグループ（Radius Server Group）] を選択し、[続行（Continue）] をクリックします。詳細については、RADIUS サーバーグループの作成 （324 ページ）のステップ 6 を参照してください。

d) [RADIUSサーバー（Radius Server）] セクションで、[追加（Add）] ボタンをクリックし、[新しいRADIUSサーバーの作成（Create New Radius Server）] をクリックします。RADIUS サーバーオブジェクトの作成 （323 ページ）を参照してください

[サーバー名またはIPアドレス（Server Name or IP Address）] フィールドに Duo Authentication Proxy サーバーの完全修飾ホスト名か IP アドレスを入力します。



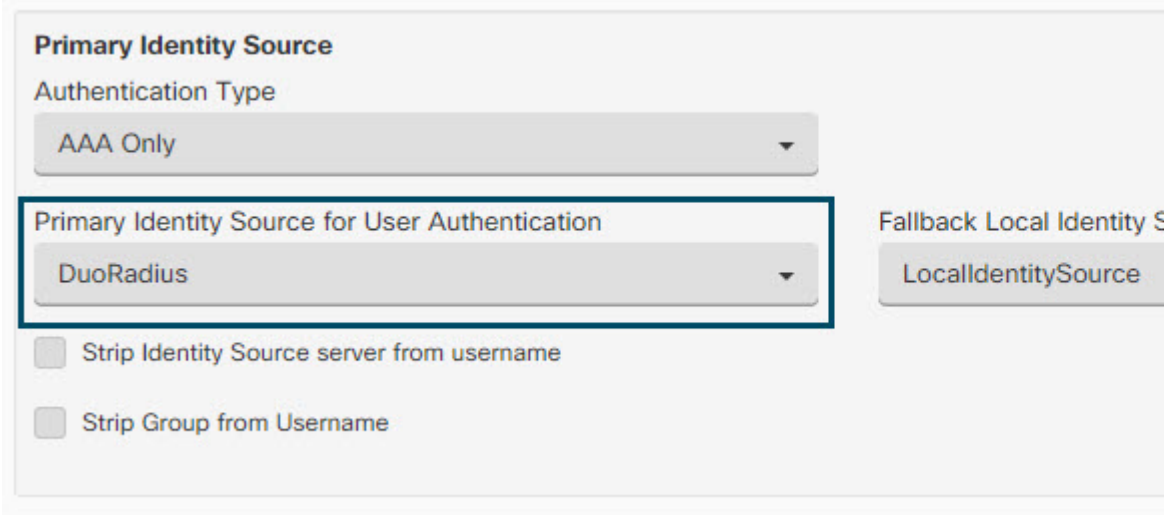
e) Duo RADIUS サーバーをグループに追加したら、[追加（Add）] をクリックして新しい Duo RADIUS サーバーグループを作成します。



ステップ 2 [リモートアクセスVPN認証方式（Remote Access VPN Authentication Method）] を [Duo RADIUS] に変更します。

a) CDO ナビゲーションメニューで、[VPN] > [リモートアクセスVPNの設定（Remote Access VPN Configuration）] をクリックします。
b) VPN の設定を展開し、Duo を追加する接続プロファイルをクリックします。
c) 右側の [アクション（Actions）] ペインで、[編集（Edit）] をクリックします。

d) [認証タイプ（Authentication Type）]（[AAA] または [AAAとクライアント証明書（AAA and Client Certificate）]）のいずれかを選択します。
e) [ユーザー認証用のプライマリIDソース（Primary Identity Source for User Authentication）] リストで、以前作成したサーバーグループを選択します。



f) 通常は [承認サーバー（Authorization Server）] や [アカウンティングサーバー（Accounting Server）] を選択する必要はありません。
g) [続行（Continue）] をクリックします。
h) [概要と手順（Summary and Instructions）] のステップで、[完了（Done）] をクリックして設定を保存します。

ステップ 3 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

LDAP を使用した *Duo* 二要素認証

プライマリソースとしての Microsoft Active Directory（AD）または RADIUS サーバとともに、セカンダリ認証ソースとして Duo LDAP サーバを使用できます。Duo LDAP を使用すると、セカンダリ認証により、プライマリ認証が Duo パスコード、プッシュ通知、または電話コールで検証されます。

（注） Duo の 二要素認証機能は、Firepower Threat バージョン 6.5 以降を実行しているデバイスに対して CDO で使用できます。

FTD デバイスは、ポート TCP/636 経由で LDAPS を使用して、Duo LDAP と通信します。

このアプローチを使用する場合は、AD/RADIUS サーバと Duo LDAP サーバの両方で設定されているユーザ名を使用して認証する必要があります。AnyConnect によってログインするように求められた場合は、プライマリ [パスワード（Password）] フィールドに AD/RADIUS のパスワードを入力します。[セカンダリパスワード（Secondary Password）]では、次のいずれかを使

用して Duo で認証します。詳細については、https://guide.duo.com/anyconnect の「要素選択用の 2 つ目のパスワード」セクションを参照してください。

- [Duoパスコード（Duo passcode）]：Duo Mobile で生成され、SMS を介して送信され、ハードウェア トークンによって生成されるパスコード、または管理者によって提供されるパスコードを使用して、認証します。1234567 などです。
- [プッシュ（push）]：Duo Mobile アプリをインストールしてアクティブにしている場合は、ログイン要求を電話機にプッシュします。要求を確認し、[承認（Approve）] をタップしてログインします。
- [電話（phone）]：電話機のコールバックを使用して認証します。
- [sms]：Duo パスコードをテキスト メッセージで要求します。ログイン試行は失敗します。新しいパスコードを使用して再度ログインします。

詳細な説明については、Duo LDAP を使用した二要素認証の設定方法 （298 ページ）を参照してください。

Duo LDAP を使用した二要素認証の設定方法

プライマリ ソースとしての Microsoft Active Directory（AD）または RADIUS サーバとともに、セカンダリ認証ソースとして Duo LDAP サーバを使用できます。Duo LDAP を使用すると、セカンダリ認証により、プライマリ認証が Duo パスコード、プッシュ通知、または電話コールで検証されます。

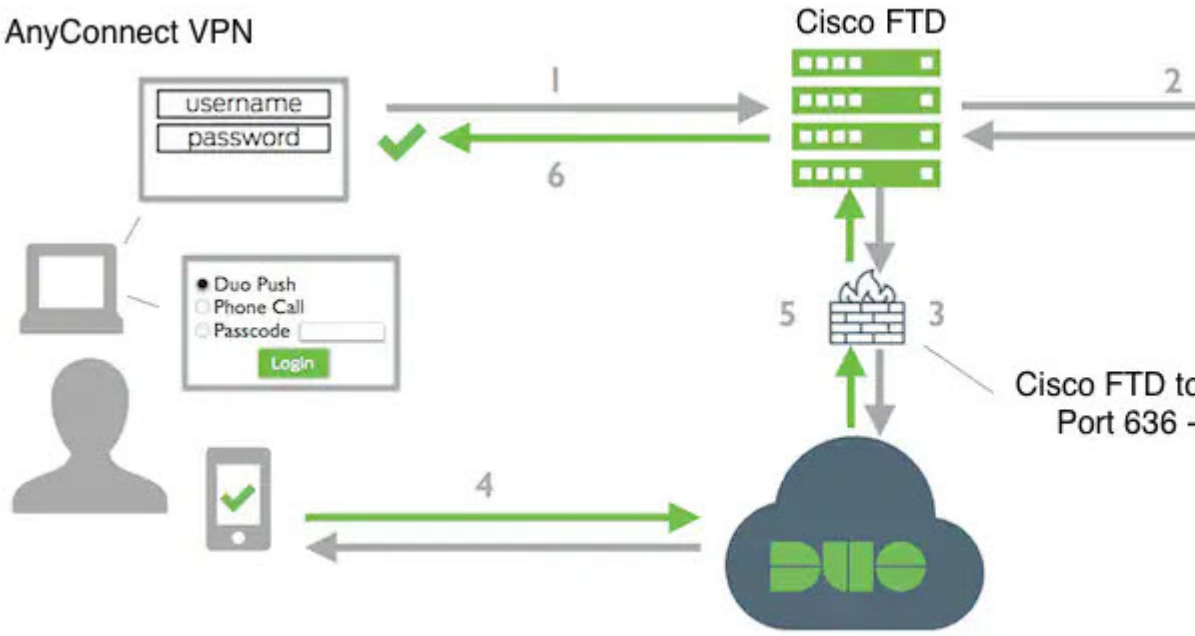
以降のトピックでは設定についてさらに詳しく説明します。

- Duo LDAP セカンダリ認証のシステム フロー （298 ページ）
- Duo LDAP セカンダリ認証の設定 （299 ページ）

Duo LDAP セカンダリ認証のシステム フロー

次の図は、LDAP を使用した二要素認証を実現するために、FTD と Duo がどのように連携するかを示しています。

次に、システムフローについて説明します。



1. ユーザーは、FTD デバイスへのリモートアクセス VPN 接続を確立し、ユーザー名とパスワードを提供します。
2. FTD は、プライマリ認証サーバー（Active Directory や RADIUS など）でプライマリ認証の試行を認証します。
3. プライマリ認証が機能する場合、FTD は Duo LDAP サーバーにセカンダリ認証の要求を送信します。
4. 要求を受けた Duo は、プッシュ構成、パスコード付きのテキストメッセージ、または電話コールによって、ユーザーを個別に認証します。ユーザーはこの認証を正常に完了する必要があります。
5. Duo は FTD デバイスに応答して、ユーザーが正常に認証されたかどうかを示します。
6. セカンダリ認証が成功すると、FTD デバイスは、ユーザーの AnyConnect クライアントとのリモート アクセス VPN 接続を確立します。

Duo LDAP セカンダリ認証の設定

次の手順では、セカンダリ認証ソースとして Duo LDAP を使用して、リモートアクセス VPN の二要素認証を設定するエンドツーエンドのプロセスについて説明します。この設定を完了するには、Duo のアカウントを取得し、Duo から情報を取得する必要があります。

Duo アカウントの作成

Duo アカウントを作成し、統合鍵、秘密鍵、および API ホスト名を取得します。

次に、プロセスの概要を示します。詳細については、Duo の Web サイトを参照してください。

手順

ステップ 1 Duo アカウントにサインアップします。

ステップ 2 Duo Admin Panel にログインし、[アプリケーション（Applications）] に移動します。

ステップ 3 [アプリケーションの保護（Protect an Application）] をクリックし、アプリケーションリストで **Cisco Firepower Threat Defense VPN** を探します。

ステップ 4 [アプリケーションの保護（Protect this Application）] をクリックして、**統合鍵**、**秘密鍵**、および **API ホスト名**を取得します。詳細については、*Duo Getting Started*（https://duo.com/docs/getting-started）を参照してください。

Duo に新しいユーザーを登録する手順については、https://duo.com/docs/enrolling-users を参照してください。

FDM を使用した、信頼できる CA 証明書の FTD へのアップロード

FTD デバイスには、Duo LDAP サーバーへの接続を検証するために必要な、信頼できる CA 証明書がなければなりません。https://www.digicert.com/digicert-root-certificates.htm に直接アクセスし、**DigiCertSHA2HighAssuranceServerCA** または **DigiCert High Assurance EV Root CA** をダウンロードし、これを Firepower Device Manager（FDM）を使用してアップロードできます。

手順

ステップ 1 FTD デバイスの FDM ページにアクセスし、[オブジェクト（Objects）]>[証明書（Certificates）] を選択します。

ステップ 2 [+] > [信頼できる CA の証明書の追加（Add Trusted CA Certificate）] をクリックします。

ステップ 3 証明書の名前を入力します（例：DigiCert_High_Assurance_EV_Root_CA）(スペースは使用できません)。

ステップ 4 [証明書のアップロード（Upload Certificate）] をクリックし、ダウンロードしたファイルを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 デバイスをまだオンボーディングしていない場合は、CDO にオンボーディングします。

ステップ 7 すべてのデバイス設定の読み取り

CDO での Duo LDAP 用 FTD の設定

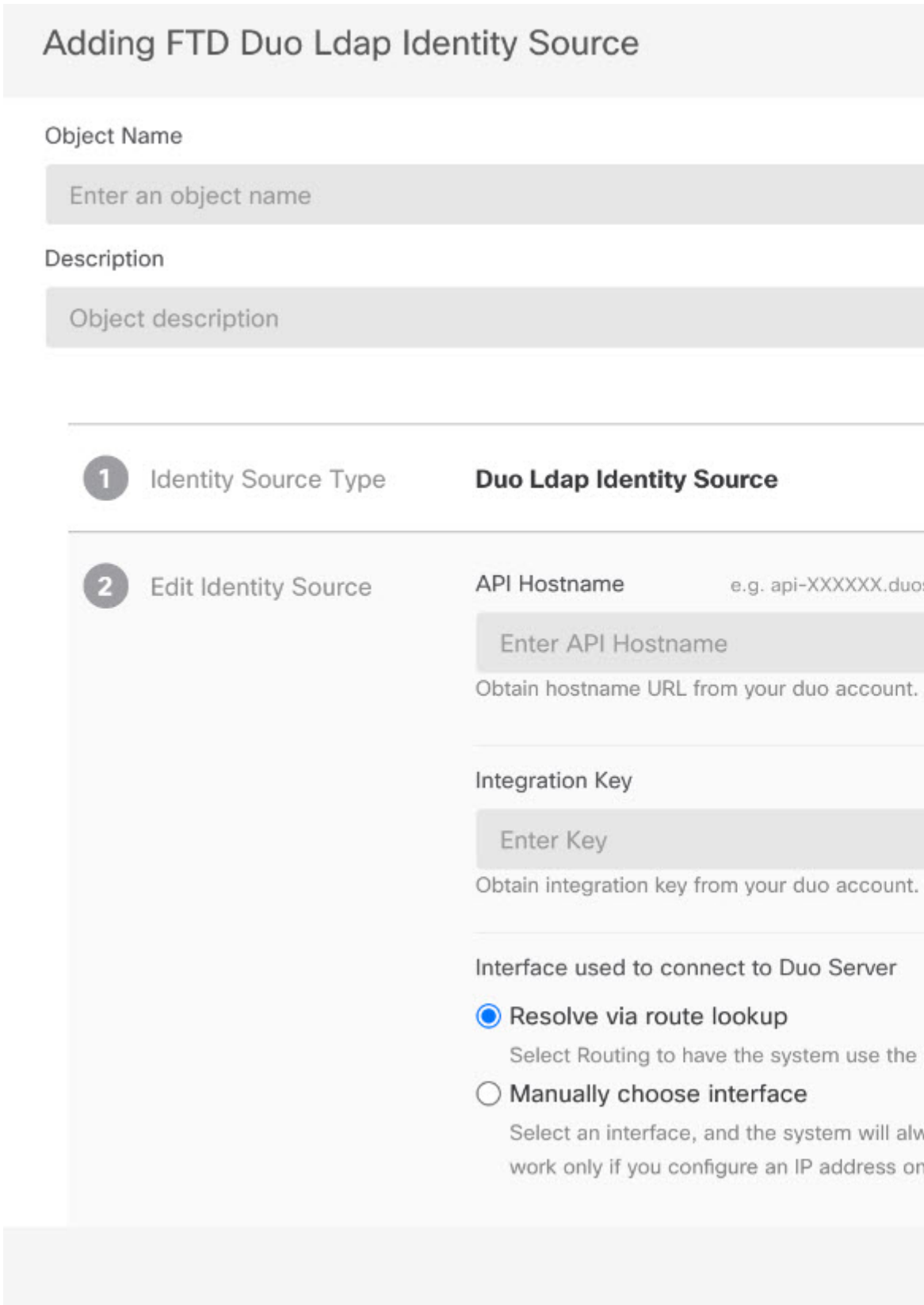
手順

ステップ 1 Duo LDAP サーバーの Duo LDAP アイデンティティ ソース オブジェクトを作成します。

a) CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

b)  > [RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [アイデンティティソース（Identity Source）] をクリックしてオブジェクトを作成します。
c) オブジェクトの名前（Duo-LDAP-server など）を入力します。
d) [デバイスタイプ（Device Type）] として [FTD] を選択します。

e) [Duo LDAPアイデンティティソース（Duo LDAP Identity Source）] をクリックして、[続行（Continue）] をクリックします。


Adding FTD Duo Ldap Identity Source
Object Name
Enter an object name
Description
Object description
1
Identity Source Type
Duo Ldap Identity Source
2
Edit Identity Source
API Hostname
e.g. api-XXXXXX.duos
Enter API Hostname
Obtain hostname URL from your duo account.
Integration Key
Enter Key
Obtain integration key from your duo account.
Interface used to connect to Duo Server
Resolve via route lookup
Select Routing to have the system use the
Manually choose interface
Select an interface, and the system will alw
work only if you configure an IP address on

f) [アイデンティティソースの編集（Edit Identity Source）] 領域で、次の詳細を指定します。

- [APIホスト名（API Hostname）] には、Duo アカウントから取得した API ホスト名を入力します。ホスト名は API-XXXXXXXX.DUOSECURITY.COM のような形式になります。X を一意の値に置き換えます。大文字は必須ではありません。
- [ポートPort] には、LDAPS に使用する TCP ポートを入力します。Duo から別のポートを使用するように指示されていない限り、この値は 636 になります。アクセス制御リストで、必ずこのポートを介した Duo LDAP サーバーへのトラフィックを許可してください。
- [タイムアウト（Timeout）]：Duo サーバーに接続する際のタイムアウトを秒単位で入力します。値は 1 ー 300 秒です。デフォルトは 120 です。デフォルトを使用するには、120 を入力するか、属性行を削除します。
- [統合鍵（Integration Key）]：Duo アカウントから取得した統合鍵を入力します。
- [秘密鍵（Secret Key）]：Duo アカウントから取得した秘密鍵を入力します。この鍵はその後マスクされます。
- [Duoサーバーへの接続に使用するインターフェイス（Interface used to connect to Duo Server）]：Duo サーバーへの接続に使用するインターフェイスを選択します。
  - [ルートルックアップ経由で解決する（Resolve via Route Lookup）]：ルーティングテーブルを使用して正しいパスを見つけるには、このオプションを選択します。ルーティングテーブルの作成については、「ルーティング」を参照してください。
  - [インターフェイスを手動で選択する（Manually Choose Interface）]：このオプションを選択し、リストからいずれかのインターフェイスを選択します。デフォルトのインターフェイスは診断インターフェイスですが、これはインターフェイスで IP アドレスを設定する場合にのみ動作します。注：選択したインターフェイスが、Duo サーバーに接続するデバイスに存在することを確認してください。
  - [追加（Add）] をクリックします。

ステップ 2 （オプション）AnyConnect プロファイルエディタを使用して、 60 秒以上の認証タイムアウトを指定するプロファイルを作成します。

ユーザーが Duo のパスコードを取得し、セカンダリ認証を完了できるように、指定する時間に余裕を持たせる必要があります。60 秒以上を推奨します。次の手順では、認証タイムアウトのみを設定してから、FTD にプロファイルをアップロードする方法について説明します。他の設定を変更する場合は、ここで行ってください。

a) AnyConnect プロファイルエディタ パッケージをダウンロードしてインストールします（まだ行っていない場合）。このパッケージは、Cisco Software Center（software.cisco.com）の使用している AnyConnect バージョンのフォルダにあります。このマニュアルの執筆時点におけるベースパスは、[ダウンロードホーム（Downloads Home）] > [セキュリティ（Security）] > [VPNおよびエンドポイントセキュリティクライアント（VPN and Endpoint

Security Clients）] > [Cisco VPNクライアント（Cisco VPN Clients）] > [AnyConnectセキュアモビリティクライアント（AnyConnect Secure Mobility Client）] です。

b) [AnyConnect VPNプロファイルエディタ（AnyConnect VPN Profile Editor）] を開きます。

c) 目次の [設定（パート2）（Preferences (Part 2)）] を選択し、ページの最後までスクロールして、[認証タイムアウト（Authentication Timeout）] を 60 以上に変更します。次の図は AnyConnect 4.7 VPN プロファイルエディタからの引用です。それより前のバージョンや後のバージョンでは、内容が異なる場合があります。

d) [ファイル（File）] > [保存（Save）] を選択し、プロファイル XML ファイルに適切な名前（duo-ldap-profile.xml など）を付けてワークステーションに保存します。

e) これで、**VPN プロファイル エディタ** アプリケーションを閉じることができます。

f) CDO で「RA VPN AnyConnect クライアントプロファイルのアップロード」を実行します。

ステップ 3 グループポリシーを作成し、ポリシーで AnyConnect プロファイルを選択します。

ユーザーに割り当てるグループポリシーは、接続のさまざまな側面を制御します。次の手順では、プロファイル XML ファイルをグループに割り当てる方法について説明します。詳細については、「新しい FTD RA VPN グループポリシーの作成」を参照してください。

a) CDO ナビゲーションページで、[オブジェクト（Objects）] をクリックします。

b) 既存のグループポリシーを編集するには、[RA VPNグループポリシー（RA VPN Group Policy）] フィルタを使用して既存のグループポリシーのみを表示し、必要なポリシーを変更して保存します。

c) 新しいグループポリシーを作成するには、[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [RA VPNグループポリシー（RA VPN Group Policy）] をクリックします。

d) [全般（General）] ページで、次のプロパティを設定します。

- [名前（Name）]：新しいプロファイルの場合は、名前を入力します。たとえば、Duo-LDAP-group と入力します。
- [AnyConnectクライアントプロファイル（AnyConnect Client Profiles）]：作成した AnyConnect クライアントプロファイルを選択します。

e) [追加（Add）] をクリックして、オブジェクトを保存します。

f) [VPN] > [リモートアクセスVPNの設定（Remote Access VPN Configuration）] をクリックします。

g) 更新するリモートアクセス VPN の設定をクリックします。

h) 右側の [操作（Actions）] ウィンドウで、[グループポリシー（Group Policies）] をクリックします。

i) [+] をクリックして、VPN 設定に関連付けるグループポリシーを選択します。

j) [保存（Save）] をクリックして、グループポリシーを保存します。

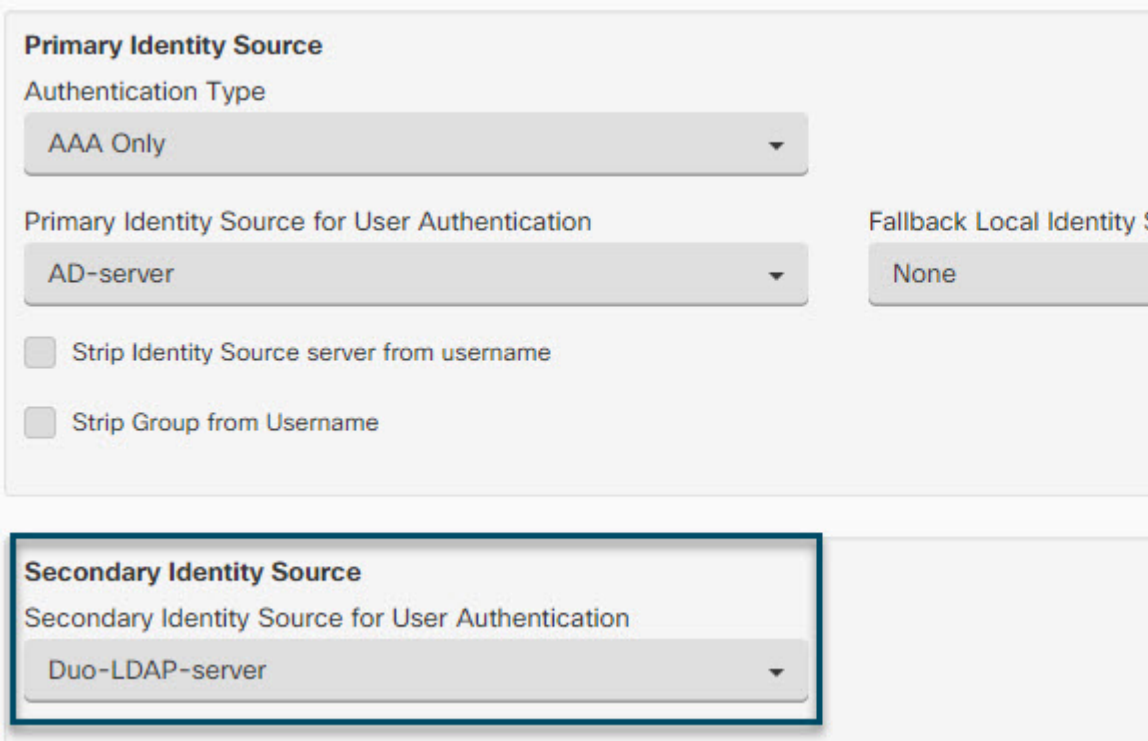
ステップ 4 Duo LDAP セカンダリ認証に使用するリモートアクセス VPN 接続プロファイルを作成または編集します。

次の手順では、Duo LDAP をセカンダリ認証ソースとして有効にし、AnyConnect クライアントプロファイルを適用するための主な変更について説明します。新しい接続プロファイルの場合

は、残りの必須フィールドも設定する必要があります。この手順では、既存の接続プロファイルを編集しており、これら 2 つの設定のみを変更する必要があると仮定しています。

a) CDO ナビゲーションページで、[VPN] > [リモートアクセスVPNの設定（Remote Access VPN Configuration）] をクリックします。
b) リモートアクセス VPN の設定を展開し、更新する接続プロファイルをクリックします。
c) 右側の [操作（Actions）] ウィンドウで、[編集（Edit）] をクリックします。
d) [プライマリアイデンティティソース（Primary Identity Source）] で、次を設定します。

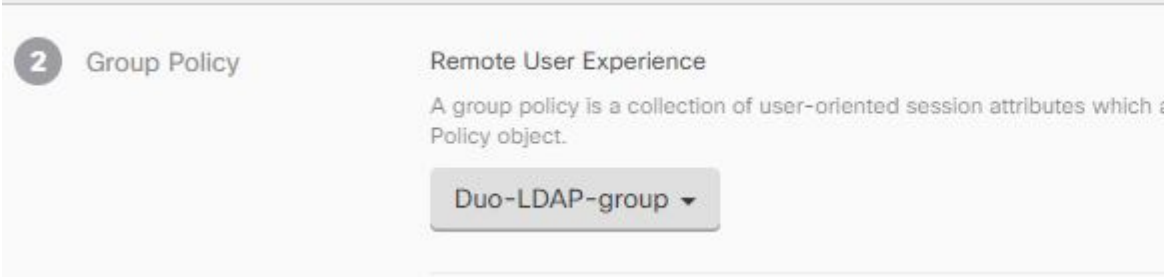
- [認証タイプ（Authentication Type）]：[AAAのみ（AAA Only）] または [AAAとクライアント証明書（AAA and Client Certificate）] のいずれかを選択します。AAA を使用していない場合、二要素認証を設定できません。
- [ユーザー認証のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]：プライマリ Active Directory または RADIUS サーバーを選択します。プライマリソースとして Duo-LDAP アイデンティティソースを選択できることに注意してください。ただし、Duo-LDAP は認証サービスのみを提供し、アイデンティティサービスは提供しないため、プライマリ認証ソースとして Duo-LDAP を使用する場合、どのダッシュボードにも RA VPN 接続に関連付けられているユーザー名は表示されず、これらのユーザーに対してアクセス制御ルールを作成することはできません（必要に応じて、ローカル アイデンティティ ソースへのフォールバックを設定できます）。
- [セカンダリアイデンティティソース（Secondary Identity Source）]：Duo-LDAP のアイデンティティソースを選択します。



（注） [プライマリアイデンティティソース（Primary Identity Source）] と [セカンダリアイデンティティソース（Secondary Identity Source）] のユーザー名が同じ場合は、接続プロファイルの [詳細（Advanced）] オプションで、[セカンダリログインにプライマリユーザー名を使用（Use Primary Username for Secondary Login）] を有効にすることをお勧めします。このように設定すると、エンドユーザーは、プライマリとセカンダリの両方のアイデンティティソースに単一のユーザー名を使用できます。

e) [続行（Continue）] をクリックします。

f) [グループポリシー（Group Policy）] ページで、作成または編集したグループポリシーを選択します。



g) [続行（Continue）] をクリックします。

h) [完了（Done）] をクリックして、接続プロファイルへの変更を保存します。

ステップ 5 すべてのデバイスの設定変更のプレビューと展開 （424 ページ）。

FTD のためのエンドツーエンドの FTD リモートアクセス VPN 設定プロセス

このセクションでは、CDO にオンボードされた FTD デバイスでリモートアクセス仮想プライベートネットワーク（RA VPN）を設定するためのエンドツーエンドの手順を提供します。

クライアントのリモートアクセス VPN を有効化するには、いくつかの異なる項目を設定する必要があります。次の手順では、エンドツーエンドのプロセスについて説明します。

手順

ステップ 1 2 つのライセンスを有効にします。

- デバイスを登録する際に、エクスポート制御機能に対して有効化された Smart Software Manager アカウントによってエクスポートを制御する必要があります。リモートアクセス VPN を設定するには、基本ライセンスが輸出規制要件を満たしている必要があります。また、評価ライセンスを使用して機能を設定することはできません。Firepower Threat Defense デバイスを購入すると、自動的に基本ライセンスが付いてきます。基本ライセンスは、オプションライセンスではカバーされないすべての機能をカバーしています。これは永久ライセンスです。デバイスは FDM から登録する必要があります。詳細については、デバイスが実行しているバージョンの Cisco Firepower Threat Defense コンフィギュレーション ガ

イド（Firepower Device Manager 用）[英語] の「Licensing the System」の章にある「Registering the Device」を参照してください。https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html

- リモート アクセス VPN ライセンス。詳細については、「リモート アクセス VPN のライセンス要件」を参照してください。
  - ライセンスを有効にするには、デバイスが実行しているバージョンの Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）[英語] の「Licensing the System 」の章にある「Enabling or Disabling Optional Licenses」を参照してください。https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html

ステップ 2 証明書を設定します。

証明書は、クライアントとデバイスの間の SSL 接続を認証するために必要です。VPN 用の事前定義された DefaultInternalCertificate を使用できます。または、独自に作成できます。

認証に使われるディレクトリ レルムに暗号化接続を使用する場合は、信頼される CA 証明書をアップロードする必要があります。証明書、および証明書のアップロード方法の詳細については、「証明書の設定」を参照してください。

ステップ 3 リモート ユーザを認証する目的で使用されるアイデンティティ ソースを設定します。

次のソースを使用して、RA VPN を使用してネットワークに接続しようとするユーザーを認証できます。さらに、クライアント証明書を単独で、またはアイデンティティソースと連携させて、認証に使用できます。

- Active Directory アイデンティティレルム：プライマリ認証ソースとして使用できます。ユーザ アカウントは Active Directory（AD）サーバで定義されます。「AD アイデンティティレルムの設定」を参照してください。「FTD アクティブ ディレクトリ レルム オブジェクトの作成または編集」を参照してください。
- RADIUS サーバーグループ：プライマリまたはセカンダリ認証ソースとして使用でき、認可およびアカウンティングに使用できます。「FTD RADIUS サーバーオブジェクトまたはグループの作成または編集」を参照してください。
- ローカル ID ソース（ローカル ユーザー データベース）：プライマリ ソースまたはフォールバック ソースとして使用できます。デバイスで直接ユーザを定義できます。外部サーバを使用することはできません。フォールバック ソースとしてローカルデータベースを使用する場合は、必ず外部サーバーで定義したものと同じユーザー名/パスワードを定義します。

  （注） Firepower Device Management（FDM）からのみ FTD デバイスに直接ユーザーアカウントを作成できます。「ローカルユーザーの設定」を参照してください。

ステップ 4 （オプション）新しい FTD RA VPN グループポリシーの作成。

グループポリシーは、ユーザーに関連する属性を定義します。グループメンバーシップに基づいて、リソースへの差分アクセスを提供するためにグループポリシーを設定することができます。または、すべての接続でデフォルトポリシーを使用します。

ステップ 5 FTD RA VPN 設定の作成。

ステップ 6 FTD RA VPN 接続プロファイルの設定。

ステップ 7 すべてのデバイスの設定変更のプレビューと展開。

ステップ 8 リモート アクセス VPN によるトラフィックの許可。

ステップ 9 （オプション）アイデンティティ ポリシーを有効にして、パッシブ認証のルールを設定します。パッシブ ユーザ認証を有効にすると、リモート アクセス VPN 経由でログインするユーザがダッシュボードに表示され、ポリシー内のトラフィック一致基準としても使用できます。パッシブ認証を有効にしない場合、RA VPN ユーザはアクティブ認証ポリシーに一致する場合にのみ使用できます。ダッシュボードのユーザー情報またはトラフィック照合用のユーザー情報を取得するには、アイデンティティ ポリシーを有効にする必要があります。「アイデンティティポリシーの設定」を参照してください。

重要 Firepower Threat Defense Manage（FDM）などのローカルマネージャを使用してリモートアクセス VPN の設定を変更すると、CDO では、そのデバイスの [設定ステータス（Configuration Status）] に [競合検出（Conflict Detected）] と表示されます。「デバイスのアウトオブバンド変更」を参照してください。この FTD で設定の競合の解決できます。

次のタスク

RA VPN 設定が FTD デバイスにダウンロードされると、ユーザーは、インターネットに接続されているコンピュータやその他のサポートされている iOS または Android デバイスを使用して、リモートの場所からネットワークに接続できます。テナント内のすべてのオンボード FTD RA VPN ヘッドエンドから、ライブ AnyConnect リモートアクセス仮想プライベートネットワーク（RA VPN）セッションを監視できます。「リモートアクセス仮想プライベート ネットワーク セッションのモニタリング」を参照してください。

AnyConnect クライアント ソフトウェア パッケージのダウンロード

リモートアクセス VPN を設定する前に、https://software.cisco.com/download/home/283000185 から AnyConnect ソフトウェアパッケージをワークステーションにダウンロードする必要があります。必要なオペレーティングシステム用の「AnyConnect ヘッドエンド展開パッケージ」をダウンロードしていることを確認してください。後で、VPN を定義するときに、これらのパッケージを Firepower Threat Defense（FTD）デバイスにアップロードできます。

最新の機能、バグ修正、セキュリティパッチを確保するには、常に最新の AnyConnect バージョンをダウンロードする必要があります。デバイスのパッケージは定期的に更新してください。

（注） オペレーティングシステム（OS）（Windows、Mac、Linux）ごとに 1 つの AnyConnect をアップロードできます。1 つの OS タイプに対して複数のバージョンをアップロードすることはできません。

AnyConnect ソフトウェアパッケージの *FTD* バージョン *6.4.0* へのアップロード

FDM API エクスプローラを使用して、AnyConnect ソフトウェアパッケージを FTD デバイスバージョン 6.4.0 にアップロードできます。RA VPN 接続を作成するには、デバイスに少なくとも 1 つの AnyConnect ソフトウェアパッケージが存在する必要があります。

重要 この手順は、FTD バージョン 6.4 にのみ適用されます。FTD バージョン 6.5 以降を使用している場合は、CDO インターフェイスを使用して AnyConnect ソフトウェアパッケージの FTD バージョン 6.5 以降が動作する FTD デバイスへのアップロードしてください。

新しい AnyConnect パッケージを FTD バージョン 6.4.0 にアップロードするには、次の手順を使用します。

手順

ステップ 1 https://software.cisco.com/download/home/283000185 から AnyConnect パッケージをダウンロードします。

- EULA に同意し、K9（暗号化されたイメージ）の権限を持っていることを確認してください。
- 使用しているオペレーティングシステム用の「AnyConnect ヘッドエンド展開パッケージ」を選択します。パッケージ名は「anyconnect-win-4.7.04056-webdeploy-k9.pkg」のようになります。Windows、macOS、Linux それぞれに向けたヘッドエンド Web 展開パッケージがあります。

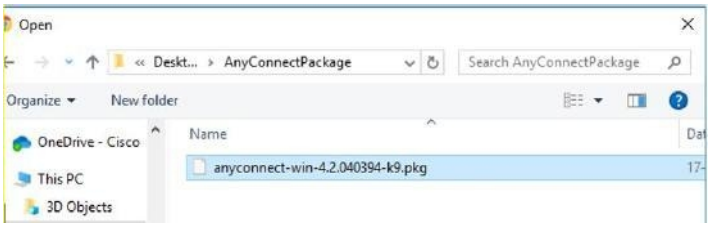
ステップ 2 ブラウザを使用して、システムのホームページを開きます。例：https://ftd.example.com。

ステップ 3 Firepower Device Manager にログインします。

ステップ 4 /#/Api-explorer を指すように URL を編集します（たとえば、https://ftd.example.com/#/api-explorer）。

ステップ 5 下にスクロールして、**[アップロード（Upload）]** > **[/action/uploaddiskfile]** をクリックします。

ステップ 6 [fileToUpload] フィールドで [ファイルの選択（Choose File）] をクリックして、必要な AnyConnect パッケージを選択します。複数のパッケージを一度にアップロードできます。



ステップ 7 [開く（Open）] をクリックします。

ステップ 8 下にスクロールして、[試す（TRY IT OUT!）] をクリックします。 パッケージが完全にアップロードされるまで待ちます。[応答本文（Response Body）] には、API 応答が次の形式で表示されます。

{ "version": null, "name": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"fileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"id": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"type": "fileuploadstatus",
"links": {
"self":
「https://ftd.example.com:972/api/fdm/...90d111e9-a361-%20cf32937ce0df.pkg」
} }

応答からパッケージの **fileName** を記録します。POST 操作を実行するときに、この文字列を入力する必要があります。この例では、fileName は **691f47e1-90c7-11e9-a361-79e2452f0c57.pkg** です。

ステップ 9 FTD REST API ページの上部近くまでスクロールして、**[AnyConnectPackageFile]** > **[POST /object/anyconnectpackagefiles]** をクリックします。API に対して POST 操作を実行し、パッケージファイルの一時的にステージングされた diskFilename と OS タイプをペイロードで指定します。このアクションにより、AnyConnect パッケージファイルが作成されます。

ステップ 10 **body** フィールドに、パッケージの詳細を次の形式でのみ入力します。

{ "platformType": "WINDOWS",
"diskFileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"type": "anyconnectpackagefile",
"name": "AnyConnectWindowsBGL" }

1. **platformType** フィールドに、OS プラットフォームを WINDOWS、MACOS、または LINUX として入力します。
2. **diskFileName** フィールドに、ディスクファイルのアップロード後に記録した **fileName** を入力します。
3. **name** フィールドに、パッケージに設定する名前を入力します。
4. [試す（TRY IT OUT!）] をクリックします。

   [応答本文（Response Body）] フィールドには、POST が正常に動作した後に API 応答が次の形式で表示されます。

{ "version": "ni7xeneslft3p",
"name": "AnyConnectWindowsBGL" }
"description": null,
"diskFileName": "41d592e3-90ca-11e9-a361-6d05320a165d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": { "self":
"https:/>/ftd.example.com:972...1-cf32937ce0df"
}
}

AnyConnect パッケージが FDM で作成されます。

ステップ 11 **[AnyConnectPackageFile] > [GET /object/anyconnectpackagefiles] > [試す（TRY IT OUT!）]** をクリックします。

[応答本文（Response Body）] に、すべての AnyConnect パッケージファイルが表示されます。

応答の例を次に示します。

{
"items": [
{
"version": "la4nwceqk2sg4",
"name": "AnyConnectWindowsBGL" }
"description": null,
"diskFileName": "82f1e362-9cd8-11e9-a361-9758ba07962d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": {
"self":
"https://ftd.example.com:972...1-23534f081c43"
}
}
],

ステップ 12 OS タイプごとに他の AnyConnect パッケージをアップロードします。手順 4 から 10 を繰り返します。

ステップ 13 Web ページをポイントするように URL を編集します（例：https://ftd.example.com）。https://ftd.example.com/#/api-explorer

ステップ 14 Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。このアイコンは、展開されていない変更がある場合にドット マークで強調表示されます。

ステップ 15 変更内容に問題がない場合は、[今すぐ展開（Deploy Now）] をクリックして、ジョブをすぐに開始できます。ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。

（注） FTD デバイスからパッケージを削除するには、**[AnyConnectPackageFile]** > **[削除（Delete）]** をクリックします。[objID] フィールドにパッケージ ID を入力し、[試す（TRY IT OUT!）] をクリックします。

VPN 接続を完了するには、ユーザーは AnyConnect クライアントソフトウェアをワークステーションにインストールする必要があります。詳細については、「ユーザーが AnyConnect クライアントソフトウェアを FTD にインストールする方法」を参照してください。

AnyConnect ソフトウェアパッケージの *FTD* バージョン *6.5* 以降が動作する *FTD* デバイスへのアップロード

RA VPN の構成に FTD バージョン 6.5 以降を実行する FTD デバイスを使用している場合は、CDO の RA VPN ウィザードを使用して AnyConnect ソフトウェアパッケージを FTD にアップロードできます。RA VPN ウィザードでは、AnyConnect パッケージがプリロードされているリモート HTTP または HTTPS サーバの URL を指定する必要があります。

（注） AnyConnect ソフトウェアパッケージの FTD バージョン 6.4.0 へのアップロードを使用して AnyConnect パッケージをアップロードすることもできます。

CDO リポジトリから AnyConnect パッケージをアップロードする

リモートアクセス VPN 設定ウィザードには、CDO リポジトリからオペレーティングシステムごとに AnyConnect パッケージが表示されるため、選択してデバイスにアップロードできます。デバイスがインターネットにアクセスでき、DNS が適切に設定されていることを確認してください。

（注） 目的のパッケージが表示されたリストにない場合、またはデバイスがインターネットにアクセスできない場合は、AnyConnect パッケージがプリロードされているサーバーを使用してパッケージをアップロードできます。

手順

ステップ 1 オペレーティングシステムに対応するフィールドをクリックし、AnyConnect パッケージを選択します。

ステップ 2  をクリックして、パッケージをアップロードします。チェックサムが一致しない場合、AnyConnectパッケージのアップロードは失敗します。失敗の詳細については、デバイスの[ワークフロー（workflow）] タブで確認できます。

はじめる前に

必要なオペレーティングシステム用の「AnyConnect ヘッドエンド展開パッケージ」をダウンロードしていることを確認してください。最新の機能、バグ修正、セキュリティパッチを確保するには、常に最新の AnyConnect バージョンをダウンロードする必要があります。デバイスのパッケージは定期的に更新してください。

（注） オペレーティングシステム（OS）（Windows、Mac、Linux）ごとに 1 つの AnyConnect をアップロードできます。1 つの OS タイプに対して複数のバージョンをアップロードすることはできません。

手順

ステップ 1 https://software.cisco.com/download/home/283000185 から AnyConnect パッケージをダウンロードします。

- EULA に同意し、K9（暗号化されたイメージ）の権限を持っていることを確認してください。
- 使用しているオペレーティングシステム用の「AnyConnectヘッドエンド展開パッケージ」を選択します。パッケージ名は「anyconnect-win-4.7.04056-webdeploy-k9.pkg」のようになります。Windows、macOS、Linux それぞれに向けたヘッドエンドパッケージがあります。

ステップ 2 AnyConnect パッケージをリモート HTTP または HTTPS サーバーにアップロードします。FTD デバイスから HTTP または HTTPS サーバーへのネットワークルートがあることを確認します。

（注） AnyConnect パッケージを HTTPS サーバーにアップロードする場合は、以下の手順を実行してください。

- HTTPS サーバーの信頼できる CA 証明書を FDM から FTD デバイスにアップロードします。証明書のアップロードについては、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version X.Y』の「Certificates」の章にある「Uploading Trusted CA Certificates」セクションを参照してください。
- 信頼できる CA 証明書を HTTPS サーバーにインストールします。

ステップ 3 リモートサーバーの URL は、認証を求めない直接リンクである必要があります。URL が事前認証されている場合は、RA VPN ウィザードの URL を指定してファイルをダウンロードできます。

ステップ 4 リモートサーバーの IP アドレスが NAT 処理されている場合は、リモートサーバーのロケーションの NAT 処理済みパブリック IP アドレスを指定する必要があります。

新規 AnyConnect パッケージのアップロード

新しい AnyConnect パッケージを FTD バージョン 6.5.0 デバイスにアップロードするには、次の手順を使用します。

手順

ステップ 1 FTD RA VPN 設定の作成

ステップ 2 [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] で、Windows、Mac、Linux のエンドポイントに対して別々のパッケージをアップロードできます。

ステップ 3 対応するプラットフォームフィールドで、Windows、Mac、および Linux と互換性のある AnyConnect パッケージが事前にアップロードされているサーバーのパスを指定します。サーバーパスの例：
'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg',
'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'.

ステップ 4 をクリックして、パッケージをアップロードします。CDO は、パスが到達可能であり、指定されたファイル名が有効なパッケージかどうかを検証します。検証が成功すると、AnyConnect パッケージの名前が表示されます。RA VPN 設定にさらに FTD デバイスを追加すると、それらに AnyConnect パッケージをアップロードできます。

ステップ 5 [OK] をクリックします。AnyConnect パッケージが RA VPN 設定に追加されます。

ステップ 6 ステップ 6 から、「FTD RA VPN 設定の作成」に進みます。

次のタスク

VPN 接続を完了するには、ユーザーは AnyConnect クライアントソフトウェアをワークステーションにインストールする必要があります。詳細については、「ユーザーが AnyConnect クライアントソフトウェアを FTD にインストールする方法」を参照してください。

既存の AnyConnect パッケージの置換

AnyConnect パッケージがデバイスにすでに存在している場合、これらは RA VPN ウィザードに表示されます。オペレーティングシステムで利用可能なすべての AnyConnect パッケージが、ドロップダウンリストに表示されます。既存のパッケージをリストから選択して、新しいパッケージと置き換えることができます。ただし、新しいパッケージをリストに追加することはできません。

（注） 既存のパッケージを新しいパッケージに置き換える場合は、新しいAnyConnectパッケージが、FTDが到達できるネットワーク上のサーバーにすでにアップロードされていることを確認してください。

手順

ステップ 1 左側の CDO ナビゲーションバーで、**[VPN] > [リモートアクセスVPN（Remote Access VPN）]** をクリックします。

ステップ 2 変更する RA VPN 設定を選択し、[アクション（Actions）] で [編集（Edit）] をクリックします。

ステップ 3 [検出された AnyConnect パッケージ（AnyConnect Packages Detected）] で、既存の AnyConnect パッケージの横に表示される アイコンをクリックします。オペレーティングシステムに複数のバージョンの AnyConnect パッケージがある場合は、置き換えるパッケージをリストから選択して [編集（Edit）] をクリックします。既存のパッケージが対応するフィールドから消去されます。

ステップ 4 新しい AnyConnect パッケージがプリロードされているサーバーのパスを指定し、 をクリックしてパッケージをアップロードします。

ステップ 5 [OK] をクリックします。新しい AnyConnect パッケージが RA VPN 設定に追加されます。

ステップ 6 ステップ 6 から、「FTD RA VPN 設定の作成」に進みます。

AnyConnect パッケージの削除

手順

ステップ 1 左側の CDO ナビゲーションバーで、**[VPN] > [リモートアクセスVPN（Remote Access VPN）]** をクリックします。

ステップ 2 変更する RA VPN 設定を選択し、[アクション（Actions）] で [編集（Edit）] をクリックします。

ステップ 3 [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] で、削除する AnyConnect パッケージの横に表示される アイコンをクリックします。オペレーティングシステムに複数のバージョンの AnyConnect パッケージがある場合は、リストから削除するパッケージを選択します。既存のパッケージが対応するフィールドから消去されます。

（注） [キャンセル（Cancel）] をクリックすると削除操作を停止し、既存のパッケージが保持されます。

ステップ 4 [OK] をクリックします。 デバイスの [設定ステータス（Configuration Status）] は [未同期（Not Synced）] となります。

（注） この段階で削除アクションを取り消す場合は、[デバイスとサービス（Device & Services）] ページに移動し、[変更の破棄（Discard Changes）] をクリックして、既存の AnyConnect パッケージを保持します。

ステップ 5 すべてのデバイスの設定変更のプレビューと展開。

FTD のアイデンティティソースの設定

Microsoft AD レルムや RADIUS サーバーなどのアイデンティティソースは、組織内のユーザーのユーザーアカウントを定義する AAA サーバーおよびデータベースです。この情報は、IP アドレスに関連付けられているユーザー ID の提供や、CDO へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。

[オブジェクト（Objects）] > [オブジェクトの作成（Create Objects）]（  ）> [RA VPNオブジェクト（ASA & FTD）（RA VPN Objects（ASA & FTD））] > [アイデンティティソース（Identity Source）] をクリックしてソースを作成します。> > アイデンティティ ソースを必要とするサービスを設定するときに、次のオブジェクトを使用します。適切なフィルタを適用して既存のソースを検索し、それらを管理できます。

Active Directory レルム

Active Directory は、ユーザーアカウントおよび認証情報を提供します。AD レルムを含む設定を FTD デバイスに展開すると、CDO は AD サーバーからユーザーとグループを取得します。

このソースは、以下の目的で使用できます。

- リモートアクセス VPN（プライマリ アイデンティティ ソースとして）。AD は RADIUS サーバーと組み合わせて使用可能。
- アイデンティティポリシー（アクティブ認証用、およびパッシブ認証で使用されるユーザー アイデンティティ ソースとして）。
- ユーザーのアクティブ認証に向けたアイデンティティルール。

ユーザーアイデンティティを使用してアクセスコントロールルールを作成可能。詳細は、『Firepower アイデンティティポリシーの導入方法』を参照してください。

CDO は、24 時間ごとに最新のユーザーグループのリストを要求します。1 つのルールに最大 50 のユーザーまたはグループを追加できるため、通常は、グループを選択する方が個々のユーザーを選択するより有意義です。たとえば、エンジニアリング グループに開発ネットワークへのアクセスを許可するルールを作成し、それに続くルールとして、そのネットワークへの他のすべてのアクセスを拒否するルールを作成できます。その後、ルールを新しいエンジニアに適用するには、エンジニアをディレクトリ サーバーのエンジニアリング グループに追加するだけです。

CDO の Active Directory レルム

AD アイデンティティ オブジェクトを作成するときに、AD レルムを構成します。アイデンティティ ソース オブジェクト ウィザードは、AD サーバーへの接続方法と、AD サーバーがネットワーク内のどこに配置されているかを判断するために役立ちます。

（注） CDO で AD レルムを作成すると、アフィリエイト アイデンティティ ソース オブジェクトを作成するとき、およびそれらのオブジェクトをアイデンティティ ルールに追加するときに、CDO は AD パスワードを記憶します。

FDM の Active Directory レルム

CDO オブジェクト ウィザードから、FDM で作成された AD レルム オブジェクトを指定できます。CDO は、FDM で作成された AD レルム オブジェクトの AD パスワードを**読み取らない**ことに注意してください。CDO に正しい AD パスワードを手動で入力する必要があります。

FDM で AD レルムを設定するには、デバイスが実行しているバージョンの『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド』で、「再利用可能なオブジェクト」の章の「**AD アイデンティティ レルムの構成**」を参照してください。

サポートされるディレクトリ サーバー

Windows サーバー 2008 および 2012 で AD を使用できます。

サーバーの設定に関して次の点に注意してください。

- ユーザー グループまたはグループ内のユーザーに対してユーザー制御を実行する場合、ディレクトリ サーバーでユーザー グループを設定する必要があります。サーバーが基本的なオブジェクト階層でユーザーを整理している場合、システムはユーザーグループ制御を実行できません。
- ディレクトリ サーバーは、次の表に示すフィールド名を使用して、システムがそのフィールドのサーバーからユーザー メタデータを取得できるようにする必要があります。

メタデータ（Metadata）	Active Directory フィールド
LDAP ユーザ名	samaccountname
名（First name）	givename
姓	sn
メール アドレス	メール アドレス userprincipalname（mail に値が設定されていない場合）

メタデータ（Metadata）	Active Directory フィールド
部署名（Department）	部署 distinguishedname（department に値が設定されていない場合）
電話番号	telephonenumber

ディレクトリ ベースの DN の決定

ディレクトリの各プロパティを設定する際、ユーザおよびグループに共通のベース識別名（DN）を指定する必要があります。ベースはディレクトリサーバー内で定義され、ネットワークごとに異なります。アイデンティティポリシーが正しく機能するには、適切なベースを入力する必要があります。ベースが誤っていると、ユーザ名またはグループ名が特定されず、アイデンティティに基づくポリシーが機能しなくなります。

（注） 正しいベースを取得するには、ディレクトリ サーバを担当する管理者に確認してください。

Active Directory の場合、ドメイン管理者として AD サーバにログインし、コマンドプロンプトで **dsquery** のコマンドを次のように使用することで、正しいベースを判別できます。

ユーザ検索ベース

dsquery user コマンドを入力し、ベース識別名を調べたい既知のユーザー名（一部または全体）を指定します。たとえば、次のコマンドでは、「John*」という部分名を使用して、「John」から始まるすべてのユーザーの情報を返します。

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

ベース DN は「DC=csc-lab,DC=example,DC=com」となります。

グループ検索ベース

既知のグループ名を使用して、**dsquery group** コマンドを入力し、ベース DN を判断します。たとえば次のコマンドでは、グループ名「Employees」を使用して識別名を返します。

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

グループのベース DN は、「DC=csc-lab,DC=example,DC=com」となります。

ADSI Edit プログラムを使用して、AD 構造を参照することもできます（**[スタート]**>**[ファイル名を指定して実行]**>**[adsiedit.msc]**）。ADSI Edit で、組織単位（OU）、グループ、ユーザなど任意のオブジェクトを右クリックし、[プロパティ（Properties）] を選択すると、識別名が表示されます。DC 値の文字列を、ベースとしてコピーします。

正しいベースであることを確認するには、次の手順を実行します。

手順

ステップ 1 ディレクトリ プロパティの [テスト接続（Test Connection）] ボタンをクリックし、接続を確認します。問題があった場合には修正して、ディレクトリ プロパティを保存します。

ステップ 2 変更をデバイスに適用します。

ステップ 3 アクセス ルールを作成して、[ユーザ（Users）] タブを選択し、ディレクトリから既知のユーザおよびグループ名の追加を試みます。ディレクトリを含むレルム内の一致ユーザ名およびグループ名を入力すると、入力中にオートコンプリートによる候補が表示されます。ドロップダウンリストに候補が表示される場合は、システムがディレクトリに適切に照会できたことを意味します。入力した文字列がユーザ名またはグループ名として表示されることが確かであるにもかかわらず、候補が表示されない場合は、対応する検索ベースを修正する必要があります。

次のタスク

詳細は「FTD アクティブ ディレクトリ レルム オブジェクトの作成または編集」を参照してください。

RADIUS サーバおよびグループ

RADIUS サーバーを使用して、管理ユーザーを認証および認可できます。

RADIUS サーバを使用するように機能を設定する場合は、個別のサーバではなく RADIUS グループを選択します。RADIUS グループは、相互にコピーである RADIUS サーバの集合です。グループに複数のサーバがある場合は、それらは、1 つのサーバが使用できなくなった場合に冗長性を提供する一連のバックアップ サーバを形成します。ただし、サーバが 1 つしかない場合でも、機能の RADIUS サポートを設定するには、メンバーが 1 つのグループを作成する必要があります。

このソースは、以下の目的で使用できます。

- 認証、および許可、アカウンティングのアイデンティティ ソースとしてのリモートアクセス VPN。AD は RADIUS サーバーと組み合わせて使用できます。
- アイデンティティ ポリシー（リモート アクセス VPN ログインからユーザー アイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

詳細については、「FTD RADIUS サーバーオブジェクトまたはグループの作成または編集」を参照してください。

関連情報：

- FTD アクティブ ディレクトリ レルム オブジェクトの作成または編集
- FTD RADIUS サーバーオブジェクトまたはグループの作成または編集
- アイデンティティポリシーの設定

FTD アクティブ ディレクトリ レルム オブジェクトの作成または編集

Active Directory レルムオブジェクトについて

AD レルムオブジェクトなどの ID ソースオブジェクトを作成または編集すると、CDO は SDC を介して FTD デバイスに設定要求を送信します。次に FTD は、設定された AD レルムと通信します。

CDO は、FDM コンソールを介して設定された AD レルムのディレクトリパスワードを読み取らないことに注意してください。元々 FDM で作成された AD レルムオブジェクトを使用する場合は、ディレクトリパスワードを手動で入力する必要があります。

FTD アクティブ ディレクトリ レルム オブジェクトの作成

次の手順を使用して、オブジェクトを作成します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）]** > **[アイデンティティソース（Identity Source）]**をクリックします。

ステップ 3 オブジェクトの [オブジェクト名（Object Name）] を入力します。

ステップ 4 [デバイスタイプ（Device Type）] として [FTD] を選択します。

ステップ 5 ウィザードの最初の部分で、[IDソースタイプ（Identity Source Type）]として [Active Directory レルム（Active Directory Realm）] を選択します。[続行（Continue）] をクリックします。

ステップ 6 基本レルムのプロパティを設定します。

- [ディレクトリユーザー名（Directory Username）]、[ディレクトリパスワード（Directory Password）]：取得するユーザー情報に対して適切な権限を持つユーザーの識別用ユーザー名とパスワード。AD では、昇格されたユーザー特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザー名は Administrator@example.com などの完全修飾名である必要があります（Administrator だけでなく）。

  （注） この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=administrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザーは、共通名の「users」フォルダの下で設定する必要があります。

- [ベース識別名（Base Distinguished Name）]：ユーザーおよびグループ情報、つまり、ユーザーとグループの共通の親を検索またはクエリするためのディレクトリツリー。例、cn=users,dc=example,dc=com。
- [ADプライマリドメイン（AD Primary Domain）]：デバイスが参加する必要がある完全修飾 AD ドメイン名。例、example.com。

ステップ 7 ディレクトリ サーバのプロパティを設定します。

- [ホスト名またはIPアドレス（Hostname/IP Address）]：ディレクトリサーバーのホスト名または IP アドレス。サーバに対して暗号化された接続を使用する場合、IP アドレスではなく、完全修飾ドメイン名を入力する必要があります。
- [ポート（Port）]：サーバーとの通信に使用するポート番号。デフォルトは 389 です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。
- [暗号化（Encryption）]：ユーザーおよびグループの情報のダウンロードに暗号化された接続を使用するには、希望の方法（[STARTTLS] または [LDAPS]）を選択します。デフォルトでは [なし（None）] になっており、ユーザおよびグループの情報がクリア テキストでダウンロードされます。
  - [STARTTLS] では、暗号化方式をネゴシエートし、ディレクトリサーバーでサポートされる最も強力な方式を使用します。ポート 389 を使用します。このオプションは、リモート アクセス VPN にレルムを使用する場合はサポートされません。
  - [LDAPS] では、LDAP over SSL が必要です。ポート 636 を使用します。
- [信頼できるCA証明書（Trusted CA Certificate）]：暗号化方式を選択する場合、認証局（CA）の証明書をアップロードして、システムとディレクトリサーバーの間で信頼できる接続を有効化します。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IPアドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。

ステップ 8 （オプション）[テスト（Test）] ボタンを使用して、構成を検証します。

ステップ 9 （オプション）[別の構成を追加（Add another configuration）] をクリックして、複数の AD サーバーを AD レルムに追加します。AD サーバーは互いの複製である必要があり、同じ AD ドメインをサポートする必要があります。したがって、ディレクトリ名、ディレクトリパスワード、ベース識別名などの基本的なレルムプロパティは、その AD レルムに関連付けられたすべての AD サーバーで同じである必要があります。

ステップ 10 [追加（Add）] をクリックします。

ステップ 11 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

FTD アクティブ ディレクトリ レルム オブジェクトの編集

アイデンティティ ソース オブジェクトの編集時にアイデンティティ ソース タイプを変更できないことに注意してください。正しいタイプの新しいオブジェクトを作成する必要があります。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 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 3 編集するオブジェクトを選択します。

ステップ 4 詳細パネルの [アクション（Actions）] ペインにある編集アイコン をクリックします。

ステップ 5 ダイアログボックスの値を、上記の手順で作成したときと同じ方法で編集します。下に表示される設定バーを展開し、ホスト名/IP アドレスや暗号化情報を編集またはテストします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 CDO 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 8 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

関連情報：

- FTD RADIUS サーバーオブジェクトまたはグループの作成または編集
- アイデンティティポリシーの設定
- アイデンティティ ルールの設定
- アイデンティティ ポリシー設定の構成

FTD RADIUS サーバーオブジェクトまたはグループの作成または編集

RADIUS サーバーオブジェクトまたはグループについて

RADIUS サーバーオブジェクトや RADIUS サーバーオブジェクトのグループなどの ID ソースオブジェクトを作成または編集すると、CDO は SDC を介して設定要求を FTD デバイスに送信します。次に FTD デバイスは、設定された AD レルムと通信します。

RADIUS サーバーオブジェクトの作成

RADIUS サーバーは、AAA（認証、認可、アカウンティング）サービスを提供します。

次の手順を使用して、オブジェクトを作成します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）]** > **[アイデンティティソース（Identity Source）]**をクリックします。

ステップ 3 オブジェクトの [オブジェクト名（Object name）] を入力します。

ステップ 4 [デバイスタイプ（Device Type）] として [FTD] を選択します。

ステップ 5 [アイデンティティソース（Identity Source）] タイプとして [RADIUSサーバー（RADIUS Server）] を選択します。[続行（Continue）] をクリックします。

ステップ 6 次のプロパティを使用して ID ソース設定を編集します。

- [サーバー名または IP アドレス（Server Name or IP Address）]：サーバーの完全修飾ホスト名（FQDN）または IP アドレス。
- [認証ポート（Authentication Port）]（オプション）：RADIUS 認証および承認が行われるポートです。デフォルトは 1812 です。
- [タイムアウト（Timeout）]：次のサーバーに要求を送信する前にサーバーからの応答を待機する時間の長さ（1 ～ 300 秒）。デフォルトは 10 秒です。
- [サーバー秘密キー（Server Secret Key）] の入力（オプション）：Firepower Threat Defense デバイスと RADIUS サーバー間でデータを暗号化するために使用される共有秘密。キーは、大文字と小文字が区別される最大 64 文字の英数字文字列です。スペースは使用できません。キーは、英数字または下線で開始する必要があります。特殊文字 $ & - _ . + @ を使用できます。文字列は、RADIUS サーバーで設定された文字列と一致している必要があります。秘密キーを設定していない場合、接続は暗号化されません。

ステップ 7 ネットワークで Cisco Identity Services Engine（ISE）をすでに設定してて、リモートアクセス VPN の認可変更設定のためにサーバーを使用している場合は、[RA VPNのみ（RA VPN Only）] リンクをクリックし、次の項目を設定します。

- [ACLのリダイレクト（Redirect ACL）]：RA VPN リダイレクト ACL を使用する拡張アクセス制御リスト（ACL）を選択します。拡張 ACL がない場合は、FDM コンソールの Smart CLI テンプレートから必要な拡張 ACL オブジェクトを作成する必要があります。デバイスが実行しているバージョンについては、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Advanced Configuration」の章の「**Configuring Smart CLI Objects**」セクションを参照してください。リダイレクト ACL の目的は、クライアントポスチャを評価するために、初期トラフィックを ISE に送信することです。ACL は、ISE に HTTPS トラフィックを送信しますが、ISE 宛てのトラフィックや、名前解決のために DNS サーバーに送信されるトラフィックは送信しません。デバイスが実行しているバージョンについては、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Virtual Private Networks (VPN)」の章の「**Configure Change of Authorization**」セクションを参照してください。
- [診断インターフェース（Diagnostic Interface）]：このオプションを有効にすると、システムは常に「診断」インターフェースを使用してサーバーと通信できるようになります。このオプションを無効のままにすると、CDO はデフォルトでルーティングテーブルを使用して、使用するインターフェイスを決定します。

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すべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

RADIUS サーバーグループの作成

RADIUS サーバーグループには、1 つまたは複数の RADIUS サーバーオブジェクトが含まれています。グループ内のサーバーは、相互にコピーされる必要があります。グループ内のサー

バーでバックアップサーバーのチェーンが形成されるため、最初のサーバーが利用できなった場合、システムはリスト上の次のサーバーを試すことができます。

次の手順を使用して、オブジェクトグループを作成します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[FTD]** > **[IDソース（Identity Source）]** をクリックします。

ステップ 3 オブジェクトの [オブジェクト名（Object name）] を入力します。

ステップ 4 [デバイスタイプ（Device Type）] として [FTD] を選択します。

ステップ 5 [IDソースタイプ（Identity Source Type）] として [RADIUSサーバーグループ（RADIUS Server Group）] を選択します。[続行（Continue）] をクリックします。

ステップ 6 次のプロパティを使用して ID ソース設定を編集します。

- [デッドタイム（Dead Time）]：失敗したサーバーは、すべてのサーバーが失敗した後にのみ再アクティブ化されます。デッドタイムは、最後のサーバーが失敗した後にすべてのサーバーを再アクティブ化するまで待機する時間の長さです。
- [最大失敗試行回数（Maximum Failed Attempts）]：次のサーバーを試行する前に、グループ内の RADIUS サーバーに送信されて失敗した要求の数（応答がなかった要求の数）。最大失敗試行回数を超えると、システムはそのサーバーを故障としてマークします。特定の機能について、ローカルデータベースを使用するフォールバック方式を設定していて、グループ内のすべてのサーバーが応答に失敗した場合、そのグループは非応答と見なされ、フォールバック方式が試行されます。サーバー グループはデッド タイムの間、非応答とマークされたままになるため、その期間内に追加の AAA 要求でサーバー グループへの接続は試行されず、フォールバック方式がすぐに使用されます。
- （任意）[ダイナミック認証/ポート（Dynamic Authorization/Port）]：RADIUS サーバーグループ向けの RADIUS ダイナミック認証または認可変更（CoA）サービスを有効にすると、そのグループは CoA 通知用に登録され、Cisco Identity Services Engine（ISE）からの CoA ポリシー更新を指定したポートでリッスンします。このサーバー グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ動的認可をイネーブルにします。

ステップ 7 ドロップダウンメニューから、RADIUS サーバーをサポートする AD レルムを選択します。AD レルムをまだ作成していない場合は、ドロップダウンメニューの [作成（Create）] をクリックします。

ステップ 8 [追加（Add）] ボタン  をクリックして、既存の RADIUS サーバーオブジェクトを追加します。必要に応じて、このウィンドウから新しい RADIUS サーバーオブジェクトを作成できます。

（注） リストの最初のサーバーは応答しなくなるまで使用されるため、作成したサーバーオブジェクトを優先して追加します。その後、FTD はデフォルトでリスト内の次のサーバーに設定されます。

ステップ 9 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

RADIUS サーバーオブジェクトまたはグループの編集

RADIUS サーバーオブジェクトまたはRADIUS サーバーグループを編集するには、次の手順を使用します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 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 3 編集するオブジェクトを選択します。

ステップ 4 詳細パネルの [アクション（Actions）] ペインにある編集アイコン 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。ホスト名/IP アドレスまたは暗号化情報を編集またはテストするには、設定バーを展開します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 CDO 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 8 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を同時に展開します。

新しい *FTD RA VPN* グループポリシーの作成

グループポリシーは、リモートアクセス VPN ユーザーの一連のユーザー指向属性値ペアです。接続プロファイルでは、トンネル確立後、ユーザー接続の条件を設定するグループポリシーが使用されます。グループ ポリシーを使用すると、ユーザーまたはユーザーのグループに属性セット全体を適用できるので、ユーザーごとに各属性を個別に指定する必要がありません。

システムには、「DfltGrpPolicy」という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

（注） 不整合のあるグループ ポリシー オブジェクトを RA VPN 設定に追加することはできません。グループポリシーを RA VPN 設定に追加する前に、すべての不整合を解決してください。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 青色のプラス  ボタンをクリックします。

ステップ 3 **[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [RA VPNグループポリシー（RA VPN Group Policy）]** をクリックします。

ステップ 4 グループ ポリシーの名前を入力します。名前には最大 64 文字の長さを使用でき、スペースも使用できます。

ステップ 5 [デバイスタイプ（Device Type）] ドロップダウンで、[FTD] を選択します。

ステップ 6 次のいずれかを実行します。

- 該当するタブをクリックし、そのページで属性を設定します。
  - FTD RA VPN グループポリシー属性
  - AnyConnect クライアント プロファイル （328 ページ）
  - セッション設定属性 （329 ページ）
  - アドレス割り当て属性 （330 ページ）
  - スプリット トンネリング属性 （330 ページ）
  - AnyConnect 属性 （331 ページ）
  - トラフィック フィルタ属性 （333 ページ）
  - Windows ブラウザ プロキシ属性 （334 ページ）

ステップ 7 [保存（Save）] をクリックしてグループポリシーを作成します。

FTD RA VPN グループポリシー属性

グループポリシーの全般的な属性では、グループの名前およびその他の基本設定を定義します。名前属性は唯一の必須属性です。

- [DNSサーバー（DNS Server）]：VPN に接続する際、クライアントがドメイン名の解決に使用する DNS サーバークライアントを定義する DNS サーバーグループを選択します。必要なグループがまだ定義されていない場合は、[DNSグループの作成（Create DNS Group）] をクリックしてすぐに作成します。
- **Banner**：ユーザーのログイン時に表示するバナーテキストまたはウェルカムメッセージです。デフォルトでは、バナーは表示されません。最大文字数は496 文字です。AnyConnect クライアントは、部分的な HTML をサポートしています。リモート ユーザーへバナーが適切に表示されることを確認するには、
 タグを使用して改行を示します。
- [デフォルトドメイン（Default Domain）]：RA VPN 内のユーザーのデフォルトドメインの名前。例、example.com。このドメインは、完全修飾されていないホスト名（たとえば、serverA.example.com ではなく serverA）に追加されます。
- [AnyConnectクライアントプロファイル（AnyConnect Client Profiles）]：[+] をクリックし、このグループに使用する AnyConnect クライアントプロファイルを選択します。「RA VPN

AnyConnect クライアントプロファイルのアップロード」を参照してください。外部インターフェイスの完全修飾ドメイン名を設定すると（接続プロファイルで）、デフォルトプロファイルが自動的に作成されます。代わりに、自分用のクライアントプロファイルをアップロードすることもできます。スタンドアロン AnyConnect プロファイルエディタを使用してこれらのプロファイルを作成します。スタンドアロン AnyConnect プロファイルエディタは、software.cisco.com からダウンロードしてインストールできます。クライアントプロファイルを選択しない場合、AnyConnect クライアントはすべてのオプションにデフォルト値を使用します。このリストの項目は、プロファイル自体ではなく AnyConnect クライアント プロファイル オブジェクトです。新しいプロファイルを作成（およびアップロード）するには、ドロップダウンリストで [新規 AnyConnectクライアントプロファイルの作成（Create New AnyConnect Client Profile）] をクリックします。

AnyConnect クライアント プロファイル

この機能は、ソフトウェアバージョン 6.7 以降のバージョンを実行している FTD でサポートされています。

Cisco AnyConnect VPN クライアントは、さまざまな組み込みモジュールによって、強化されたセキュリティを提供します。これらのモジュールは、Web セキュリティ、エンドポイントフローに対するネットワークの可視性、オフネットワークローミング保護などのサービスを提供します。各クライアントモジュールには、要件に応じたカスタム設定のグループを含むクライアントプロファイルが含まれています。

VPN ユーザーが VPN AnyConnect クライアントソフトウェアをダウンロードするときに、クライアントにダウンロードする AnyConnect VPN プロファイルオブジェクトと AnyConnect モジュールを選択できます。

1. AnyConnect VPN プロファイルオブジェクトを選択または作成します。RA VPN AnyConnect クライアントプロファイルのアップロード （348 ページ）を参照してください。DART および Start Before Login モジュールを除き、AnyConnect VPN プロファイルオブジェクトを選択する必要があります。

2. [AnyConnectクライアントモジュールの追加（Add Any Connect Client Module）] をクリックします。

   次の AnyConnect モジュールはオプションであり、VPN AnyConnect クライアントソフトウェアとともに各モジュールがダウンロードされるように設定できます。

   - **AMP イネーブラ**：エンドポイント向けの高度なマルウェア防御（AMP）を導入します。
   - **DART**：システムログのスナップショットおよびその他の診断情報がキャプチャされて、.zip ファイルがデスクトップに作成されるため、トラブルシューティング情報を簡単に Cisco TAC に送信できます。
   - **フィードバック**：お客様が有効にして使用している機能とモジュールに関する情報を提供します。
   - **ISE ポスチャ**：OPSWAT ライブラリを使用してポスチャチェックを実行し、エンドポイントの適合性を評価します。

- **Network Access Manager**：有線とワイヤレスの両方のネットワークにアクセスするための 802.1X（レイヤ 2）とデバイス認証を備えています。
- **Network Visibility**：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。
- **Start Before Login**：Windows のログインダイアログボックスが表示される前に AnyConnect を開始することにより、Windows にログインする前のユーザーを VPN 接続を介して企業インフラストラクチャに強制的に接続させます。
- **Cisco Umbrella Roaming Security**：アクティブな VPN がないときに DNS レイヤセキュリティを提供します。
- **Web セキュリティ**：定義されているセキュリティポリシーに基づいて、Web ページの要素を分析し、許容可能なコンテンツを許可し、悪意のあるコンテンツまたは許容できないコンテンツをブロックします。

3. [クライアントモジュール（Client Module）] リストで [AnyConnect] モジュールを選択します。
4. [プロファイル（Profile）] リストで、AnyConnect クライアントプロファイルを含むプロファイルオブジェクトを選択または作成します。
5. [モジュールのダウンロードを有効化（Enable Module Download）] をオンにすると、エンドポイントでプロファイルとともにクライアントモジュールをダウンロードできます。オフの場合、エンドポイントはクライアントプロファイルだけをダウンロードできます。

セッション設定属性

グループポリシーのセッションの設定は、VPN を通じて接続できる時間と、接続を確立できる個別の接続数を制御します。

- [最大接続時間（Maximum Connection Time）]：ユーザーがログアウト、再接続せずに VPN に接続したままにできる最大時間（分）で、1 ～ 4473924 または空白で指定します。デフォルトは無制限（空白）ですが、その場合でもアイドル タイムアウトは適用されます。
- [接続時間のアラート間隔（Connection Time Alert Interval）]：最大接続時間を指定した場合、アラート間隔は、次回の自動切断についてユーザーに警告を表示する最大時間に達するまでの時間を定義します。ユーザーは、接続を終了し、再接続してタイマーを再起動することを選択できます。デフォルトは 1 分です。1 ～ 30 分を指定できます。
- [アイドルタイム（Idle Time）]：VPN 接続が自動的に閉じられる前にアイドル状態になる時間（分）で、1 ～ 35791394 で指定します。指定した時間、接続で通信アクティビティがない場合、システムは接続を停止します。デフォルトは 30 分です。
- [アイドル時間のアラート間隔（Idle Time Alert Interval）]：アイドルセッションが原因の次回の自動切断について、ユーザーに警告を表示するアイドル時間に達するまでの時間。アクティビティがあるとタイマーがリセットされます。デフォルトは 1 分です。1 ～ 30 分を指定できます。

- [ユーザーあたりの同時ログイン数（Simultaneous Login Per User）]：ユーザーに許可する同時接続の最大数。デフォルトは3です。1～2147483647個の接続を指定できます。多数の同時接続を許可するとセキュリティの低下を招き、パフォーマンスに影響を及ぼす可能性があります。

アドレス割り当て属性

グループポリシーのアドレスの割り当て属性は、グループのIPアドレスプールを定義します。ここで定義されているプールで、このグループを使用するすべての接続プロファイルで定義済みのプールがオーバーライドされます。接続プロファイルで定義済みのプールを使用する場合は、これらの設定を空白のままにします。

- [IPv4アドレスプール（IPv4 Address Pool）]、[IPv6アドレスプール（IPv6 Address Pool）]：これらのオプションは、リモートエンドポイントのアドレスプールを定義します。クライアントには、VPN 接続のために使用する IP バージョンに基づき、これらのプールからアドレスが割り当てられます。サポートする IP タイプごとにサブネットを定義するネットワーク オブジェクトを選択します。当該 IP バージョンをサポートしない場合は、リストを空のままにします。たとえば、IPv4 プールを「10.100.10.0/24」と定義できます。アドレス プールは、外部インターフェイスの IP アドレスと同じサブネット上に存在することはできません。ローカルアドレスの割り当てに使用する最大6個のアドレスプールのリストを指定できます。プールの指定順序は重要です。システムでは、プールの表示順に従いプールからアドレスが割り当てられます。

- [DHCPスコープ（DHCP Scope）]：接続プロファイルのアドレスプールに DHCP サーバーを設定した場合、DHCP スコープはこのグループのプールに使用するサブネットを識別します。DHCP サーバーには、そのスコープによって識別される同じプール内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用する DHCP サーバーで定義されているアドレスプールのサブセットを選択できます。ネットワーク スコープを定義しない場合、DHCP サーバーはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。スコープを指定するには、ネットワーク番号のホストアドレスを含むネットワークオブジェクトを選択します。オブジェクトがまだ存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックします。たとえば、192.168.5.0/24 サブネットプールのアドレスを使用するように DHCP サーバーに指示するには、ホストアドレスとして192.168.5.0を指定するネットワークオブジェクトを選択します。DHCP は IPv4 アドレス指定にのみ使用することができます。

スプリット トンネリング属性

グループポリシーのスプリットトンネリング属性は、システムが内部ネットワーク用のトラフィックと外部方向トラフィックを処理する方法を定義します。スプリットトンネリングは、VPN トンネル（暗号化）と VPN トンネル外の残りのネットワークトラフィック（非暗号化、つまりクリアテキスト）を介して一部のネットワークトラフィックを誘導します。

- [IPv4スプリットトンネリング（IPv4 Split Tunneling）]、[IPv6スプリットトンネリング（IPv6 Split Tunneling）]：トラフィックが IPv4 または IPv6 アドレスを使用するかどうかに基づいて、さまざまなオプションを指定できますが、それぞれのオプションは同じです。スプ

リットトンネリングを有効にする場合は、ネットワークオブジェクトを選択する必要があるいずれかのオプションを指定します。

- [トンネル経由のトラフィックをすべて許可する（Allow all traffic over tunnel）]：スプリットトンネリングを行いません。ユーザーがRA VPN接続を行うと、そのユーザーのトラフィックはすべて保護されたトンネルを通過します。これがデフォルトです。最も安全なオプションであるとも考えられます。
- [トンネル経由で指定されたトラフィックを許可する（Allow specified traffic over the tunnel）]：宛先ネットワークとホストアドレスを定義するネットワークオブジェクトを選択します。これらの宛先へのトラフィックすべては、保護されたトンネルを通過します。その他すべての宛先へのトラフィックは、クライアントによって、トンネル外の接続（ローカル Wi-Fi やネットワーク接続など）にルーティングされます。
- [以下に指定したネットワークを除外する（Exclude networks specified below）]：宛先ネットワークまたはホストアドレスを定義するネットワークオブジェクトを選択します。クライアントは、指定された宛先へのトラフィックをトンネル外の接続にルーティングします。他の宛先へのトラフィックはトンネルを通過します。

- [スプリットDNS（Split DNS）]：クライアントが、そのクライアントで設定されているDNS サーバーに他の DNS 要求を送信することを許可しながら、セキュアな接続を介して一部の DNS 要求を送信するようにシステムを設定できます。次の DNS 動作を設定できます。
  - [スプリットトンネルポリシーに従ってDNS要求を送信する（Send DNS Request as per split tunnel policy）]：このオプションを選択すると、スプリット トンネル オプションが定義されているのと同じ方法で DNS 要求が処理されます。スプリットトンネリングを有効にすると、DNS要求は宛先アドレスに基づいて送信されます。スプリットトンネリングを有効にしていない場合、DNS要求はすべて保護された接続を介します。
  - [常にトンネル経由でDNS要求を送信する（Always send DNS requests over tunnel）]：スプリットトンネリングを有効にするが、すべての DNS 要求を保護された接続を介して、グループで定義された DNS サーバーに送信する場合は、このオプションを選択します。
  - [指定したドメインのみをトンネル経由で送信（Send only specified domains over tunnel）]：保護された DNS サーバーが特定のドメインのアドレスだけを解決するようする場合は、このオプションを選択します。次に、ドメインを指定します。ドメイン名はコンマで区切ります。例：example.com, example1.com。内部 DNS サーバーが内部ドメインの名前を解決し、外部 DNS サーバーが他のすべてのインターネットトラフィックを処理するようにする場合は、このオプションを使用します。

AnyConnect 属性

グループポリシーの AnyConnect 属性は、AnyConnect クライアントでリモートアクセス VPN 接続に使用されるいくつかの SSL および接続設定を定義します。

- **SSL 設定**

- [Datagram Transport Layer Security（DTLS）の有効化（Enable Datagram Transport Layer Security (DTLS)）]：AnyConnect クライアントが SSL トンネルと DTLS トンネルの 2 つのトンネルを同時に使用することを許可するかどうかを指定します。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。DTLS をイネーブルにしない場合、SSL VPN 接続を確立している AnyConnect クライアント ユーザーは SSL トンネルのみで接続します。

- [DTLS圧縮（DTLS Compression）]：LZS を使用してこのグループの Datagram Transport Layer Security（DTLS）接続を圧縮するかどうかを指定します。[DTLS圧縮（DTLS Compression）] はデフォルトで無効になっています。

- [SSL圧縮（SSL Compression）]：データ圧縮を有効にするかどうかを指定します。有効にする場合、使用するデータ圧縮の方法は（[圧縮（Deflate）] または [LZS]）です。[SSL圧縮（SSL Compression）] はデフォルトで無効になっています。データ圧縮により、伝送速度は上がりますが、各ユーザーセッションのメモリ要件と CPU 使用率も高くなるため、SSL 圧縮はデバイスの全体的なスループットを低下させます。

- [SSLキーの再生成方法（SSL Rekey Method）]、[SSLキーの再生成間隔（SSL Rekey Interval）]：クライアントは、暗号キーと初期化ベクトルを再ネゴシエーションしながら VPN 接続キーを再生成して、接続のセキュリティを強化します。[なし（None）] を選択して、キーの再生成を無効にします。キーの再生成を有効にするには、新しいトンネルを作成するたびに [新しいトンネル（New Tunnel）] を選択します（[既存のトンネル（Existing Tunnel）] オプションは、[新しいトンネル（New Tunnel）] と同じアクションになります）。キーの再生成を有効にする場合は、キーの再生成間隔も設定します。デフォルトは 4 分です。間隔は、4 ～ 10080 分（1 週間）の範囲で設定できます。

• 接続の設定

- [DF（Don't Fragment）ビットを無視する（Ignore the DF (Don't Fragment) bit）]：フラグメント化が必要なパケットの Don't Fragment（DF）ビットを無視するかどうかを指定します。DF ビットが設定されているパケットの強制フラグメンテーションを許可し、それらのパケットがトンネルを通過できるようにするには、このオプションを選択します。

- [クライアントバイパスプロトコル（Client Bypass Protocol）]：セキュアゲートウェイによる（IPv6 トラフィックだけを予期しているときの）IPv4 トラフィックの管理方法や、（IPv4 トラフィックだけを予期しているときの）IPv6 トラフィックの管理方法を設定することができます。

  AnyConnect クライアントがヘッドエンドに VPN 接続するときに、ヘッドエンドは IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ヘッドエンドが AnyConnect 接続に IPv4 アドレスのみ、または IPv6 アドレスのみを割り当てた場合、ヘッドエンドが IP アドレスを割り当てなかったネットワークトラフィックについて、Client Bypass Protocol によってそのトラフィックをドロップさせるか（デフォルト、無効、オフ）、またはヘッドエンドをバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するか（有効、オン）を設定できます。

たとえば、セキュア ゲートウェイが AnyConnect 接続に IPv4 アドレスだけを割り当て、エンドポイントがデュアルスタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコルが無効の場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルが有効の場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

- [MTU]：Cisco AnyConnect VPN Client によって確立された SSL VPN 接続の最大伝送ユニット（MTU）サイズ。デフォルトは 1406 バイトで、範囲は 576 ー 1462 バイトです。
  - [AnyConnectとVPNゲートウェイ間のキープアライブメッセージ（Keepalive Messages Between AnyConnect and VPN Gateway）]：トンネルでのデータの送受信にピアを使用できることを示すために、ピア間でキープアライブメッセージを交換するかどうかを指定します。キープアライブ メッセージは、設定された間隔で送信されます。デフォルトの間隔は 20 秒、有効な範囲は 15 ～ 600 秒です。
  - [ゲートウェイ側の間隔でのDPD（DPD on Gateway Side Interval）]、[クライアント側の間隔でのDPD（DPD on Client Side Interval）]：ピアが応答しなくなったときに VPN ゲートウェイまたは VPN クライアントによる迅速な検出を確実に実行するには、Dead Peer Detection（DPD; デッドピア検出）を有効にします。ゲートウェイまたはクライアント DPD を個別に有効にすることができます。DPD メッセージのデフォルトの送信間隔は 30 秒です。間隔は、5～3600 秒にすることができます。

トラフィック フィルタ属性

グループポリシーのトラフィックフィルタ属性は、グループに割り当てられているユーザーに適用する制限を定義します。アクセス コントロール ポリシー ルールを作成する代わりにこれらの属性を使用することで、ホストまたはサブネットアドレスとプロトコル、または VLAN に基づいて、RA VPN ユーザーのアクセスを特定のリソースに制限できます。デフォルトでは、RA VPN ユーザーは、保護されたネットワーク上の宛先へのアクセスがグループポリシーによって制限されることはありません。

- [アクセスリストフィルタ（Access List Filter）]：拡張アクセス制御リスト（ACL）を使用してアクセスを制限します。Smart CLI 拡張 ACL オブジェクトを選択します。拡張 ACL では、送信元アドレス、宛先アドレス、およびプロトコル（IP や TCP など）に基づいてフィルタリングできます。ACL はトップダウン方式で最初に一致したものから評価されるため、具体的なルールはより一般的なルールの前に配置してください。ACL の末尾には、暗黙的な「deny any」があるため、いくつかのサブネットへのアクセスを拒否しながら、他のすべてのアクセスを許可する場合は、ACL の最後に「permit any」ルールを含めてください。拡張 ACL スマート CLI オブジェクトを編集しながらネットワークオブジェクトを作成することはできないため、グループポリシーを編集する前に、ACL を作成する必要があります。そうしないと、単純にオブジェクトを作成し、後でもう一度ネットワークオブジェクトを作成し、その後で必要なすべてのアクセス制御エントリを作成する必要があります。ACL を作成するには、FDM にログインして、**[デバイス（Device）]** > **[詳細設定**

（**Advanced Configuration**）] > **[スマートCLI（Smart CLI）]** > **[オブジェクト（Objects）]** に移動し、オブジェクトを作成して、オブジェクトタイプとして [拡張アクセスリスト（Extended Access List）] を選択します。

- [VPNをVLANに制限（Restrict Access to VLAN）]：「VLAN マッピング」とも呼ばれるこの属性で、このグループポリシーが適用されるセッションの出力 VLAN インターフェイスを指定します。システムは、このグループからのトラフィックすべてを、選択したVLANに転送します。この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。デバイスのサブインターフェイスで定義されている VLAN 番号を指定していることを確認します。値の範囲は 1 ～ 4094 です。

Windows ブラウザ プロキシ属性

グループポリシーの Windows ブラウザプロキシ属性は、ユーザーのブラウザで定義されたプロキシが動作しているかどうか、およびその動作方法を判断します。

[VPNセッション中のブラウザプロキシ（Browser Proxy During VPN Session）] に対して次のいずれかの値を選択できます。

- [エンドポイント設定のまま（No change in endpoint settings）]：HTTP のブラウザプロキシを設定するかどうかをユーザーが決定できます。設定されている場合、そのプロキシが使用されます。
- [ブラウザプロキシの無効化（Disable browser proxy）]：ブラウザに定義されているプロキシ（ある場合）を使用しません。どのブラウザ接続もプロキシを経由しません。
- [自動検出設定（Auto detect settings）]：クライアントデバイスのブラウザでの自動プロキシサーバー検出の使用を有効にします。
- [カスタム設定を使用（Use custom settings）]：HTTP トラフィックに対してすべてのクライアントデバイスで使用する必要があるプロキシを定義します。次を設定します。
  - [プロキシサーバーのIPまたはホスト名（Proxy Server IP or Hostname）]、[ポート（Port）]：プロキシサーバーの IP アドレスまたはホスト名、およびプロキシサーバーが使用するプロキシ接続のポート。ホストとポートを組み合わせた文字数が 100 文字を超えることはできません。
  - [ブラウザプロキシ免除リスト（Browser Proxy Exemption List）]：免除リストにあるホスト/ポートへの接続はプロキシを経由しません。プロキシを使用すべきでない宛先のすべてのホスト/ポート値を追加します。例：www.example.com ポート 80。[プロキシ例外の追加（Add proxy exception）] をクリックしてリストに項目を追加します。項目を削除するには、ごみ箱アイコンをクリックします。すべてのアドレスとポートを合わせたプロキシ例外リスト全体で、255 文字を超えることはできません。

FTD RA VPN 設定の作成

CDO を使用して、1 つ以上の FTD デバイスを RA VPN 設定ウィザードに追加し、デバイスに関連付けられた VPN インターフェイス、アクセス制御、および NAT 免除設定ができます。したがって、各 RA VPN 設定には、RA VPN 設定に関連付けられた複数の FTD デバイス間で共有される接続プロファイルとグループポリシーを含めることができます。さらに、接続プロファイルとグループポリシーを作成して、設定を拡張できます。

RA VPN 設定がすでに完了している ASA デバイス、または RA VPN 設定のない新しいデバイスをオンボーディングできます。RA VPN 設定がすでにある FTD デバイスをオンボーディングすると、CDO は自動的に「デフォルトの RA VPN 設定」を作成し、ASA デバイスをこの設定に関連付けます。このデフォルト設定には、デバイスで定義されているすべての接続プロファイルオブジェクトを含めることができます。

重要

- 同じリモートアクセス VPN 設定に ASA と FTD を追加することはできません。
- FTD デバイスは、1 つ以上の RA VPN 設定を持つことはできません。

前提条件

FTD デバイスを RA VPN 設定に追加する前に、次の前提条件が満たされている必要があります。

- FTD デバイスが次の状態であることを確認してください。
  - 有効な RA VPN ライセンスがある。詳細については、「リモート アクセス VPN のライセンス要件」を参照してください。
  - FTD バージョン 6.4.0 の場合、少なくとも 1 つの AnyConnect ソフトウェアパッケージがデバイスに事前にアップロードされていることを確認してください。詳細については、「FTD バージョン 6.4.0 での AnyConnect パッケージのアップグレード」を参照してください。
  - FTD バージョン 6.5.0 以降では、CDO を使用して AnyConnect パッケージをアップロードできます。詳細については、「AnyConnect ソフトウェアパッケージの FTD バージョン 6.5 以降が動作する FTD デバイスへのアップロード」を参照してください。
  - 保留中の設定展開がない。
- FTD の変更は CDO に同期されている。
  1. 左側の CDO ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックし、同期する 1 つ以上の FTD デバイスを検索します。
  2. 1 つ以上のデバイスを選択し、[変更の確認（Check for changes）] をクリックします。CDO は 1 つ以上の FTD デバイスと通信して、変更を同期します。
- RA VPN 設定グループポリシーのオブジェクトは一貫しています。

- 一貫性のないすべてのグループポリシーのオブジェクトはRA VPN設定に追加できないため、それらが解決されていることを確認します。問題に対処するか、一貫性のないグループポリシーのオブジェクトを[オブジェクト（Objects）]ページから削除します。詳細については、「重複オブジェクト問題の解決」および「一貫性のないオブジェクト問題の解決」を参照してください。

- FTD デバイスの RA VPN グループポリシーが、RA VPN 設定グループ ポリシーと一致している。

手順

手順

ステップ 1 左側の CDO ナビゲーションバーで、**[VPN]** > **[リモートアクセスVPNの設定（Remote Access VPN Configuration）]** をクリックします。

ステップ 2 青色のプラス ボタンをクリックして、新しい RA VPN 設定を作成します。

ステップ 3 リモートアクセス VPN の設定の名前を入力します。

ステップ 4 青色のプラス ボタンをクリックして、FTD デバイスを設定に追加します。デバイスの詳細を追加し、デバイスに関連付けられたネットワークトラフィック関連の権限を設定できます。

1. 次のデバイスの詳細を提供します。

   - [デバイス（Device）]：追加する FTD デバイスを選択し、[選択（Select）] をクリックします。

     重要 同じリモートアクセス VPN 設定に ASA と FTD を追加することはできません。

   - [デバイスアイデンティティ証明書（Certificate of Device Identity）]：デバイスのアイデンティティを確立するために使用する内部証明書を選択します。内部証明書は、AnyConnect クライアントがデバイスへの接続を行うときにデバイスのアイデンティティを確立します。安全な VPN 接続を完了するには、クライアントがこの証明書を承認する必要があります。まだ証明書がない場合、ドロップダウンリストの [新規内部証明書の作成（Create New Internal Certificate）] をクリックします。「自己署名内部および内部 CA 証明書の生成」を参照してください。

   - [外部インターフェイス（Outside Interface）]：リモートアクセス VPN 接続を確立するときにユーザーが接続するインターフェイス。これは、通常外部（インターネットに接続された）インターフェイスですが、デバイスとこの接続プロファイルがサポートしているエンドユーザー間のいずれかのインターフェイスを選択します。新しいサブインターフェイスを作成するには、「Firepower VLAN サブインターフェイスと 802.1Q トランキングの設定」を参照してください。

- [外部インターフェイスの完全修飾ドメイン名またはIP（Fully-qualified Domain Name or IP for the Outside Interface）]：インターフェイスの名前（例、ravpn.example.com）または IP アドレスを指定する必要があります。名前を指定すると、クライアント プロファイルが作成されます。**注**：ユーザーは、クライアントによって VPN で使用される DNS サーバーが、この名前から外部インターフェイスの IP アドレスを解決できるようにする必要があります。関連する DNS サーバーに FQDN を追加します。

2. [続行（Continue）] をクリックして、トラフィックの権限を設定します。

- [復号されたトラフィック（sysopt permit-vpn）に対するバイパスアクセスコントロールポリシー（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：デフォルトでは、復号されたトラフィックは、アクセス コントロール ポリシーの検査の対象になります。このオプション [複合されたトラフィックのバイパス（bypasses the decrypted traffic）] オプションを有効にすると、アクセス コントロール ポリシーの検査がバイパスされますが、AAA サーバーからダウンロードされた VPN フィルタ ACL と認証 ACL は、VPN トラフィックに引き続き適用されます。このオプションを選択すると、システムによりグローバル設定である sysopt connection permit-vpn コマンドが設定されることに注意してください。これは、サイト間 VPN 接続の動作にも影響を及ぼします。このオプションを選択しない場合、外部ユーザーがリモートアクセス VPN アドレスプール内の IP アドレスをスプーフィングし、ネットワークにアクセスするおそれがあります。この理由は、アドレスプールに内部リソースへのアクセスを許可するアクセスコントロールルールを作成する必要があるためです。アクセスコントロールルールを使用する場合は、送信元 IP アドレスだけではなく、ユーザーの仕様を使用してアクセスを制御することを検討してください。このオプションを選択することの欠点は、VPN トラフィックが検査されないことです。つまり、侵入およびファイル保護、URL フィルタリング、またはその他の高度な機能がトラフィックに適用されません。つまり、このトラフィックに対する接続イベントは生成されず、VPN 接続は統計ダッシュボードには反映されません。

- [NAT免除（NAT Exempt）]：リモートアクセス VPN エンドポイントとの入出力トラフィックに対する NAT 変換を免除するには、NAT 免除を有効にします。VPN トラフィックを NAT 免除にしない場合は、外部および内部インターフェイスに対する既存の NAT ルールが RA VPN アドレス プールに適用されないことを確認してください。NAT 免除 ルールは特定の送信元/宛先インターフェイスとネットワークの組み合わせに対する手動スタティック アイデンティティ NAT ルールですが、NAT ポリシーには反映されず、非表示になります。NAT 免除を有効にした場合、以下も設定する必要があります。

  - [内部インターフェイス（Inside Interfaces）]：リモートユーザーがアクセスする内部ネットワークのインターフェイスを選択します。これらのインターフェイスには NAT ルールが作成されます。

  - [内部ネットワーク（Inside Networks）]：リモートユーザーがアクセスする内部ネットワークを表すネットワークオブジェクトを選択します。ネットワーク リストには、サポートしているアドレス プールと同じ IP タイプを含める必要があります。

ステップ 5 [OK] をクリックします。

- FTD バージョン 6.4.0 デバイスをオンボードしている場合、[検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] には、デバイスで使用可能な AnyConnect パッケージが表示されます。
- FTD バージョン 6.5.0 以降のデバイスをオンボードしている場合は、AnyConnect パッケージが事前にアップロードされているサーバーから AnyConnect パッケージを追加する必要があります。手順については、「AnyConnect ソフトウェアパッケージの FTD バージョン 6.5 以降が動作する FTD デバイスへのアップロード」を参照してください。

ステップ 6 [OK] をクリックします。デバイスが設定に追加されます。

次のタスク

（注） 設定を選択し、[アクション（Actions）] で適切なアクションをクリックします。

- [グループポリシー（Group Policies）]：グループポリシーを追加または削除します。
  - [+] をクリックして、必要なグループポリシーを選択します。新しい RA VPN グループポリシーを作成するには、「新しい FTD RA VPN グループポリシーの作成」を参照してください。
- [削除（Remove）]：選択した RA VPN 設定を削除します。

RA VPN 設定の変更

既存の RA VPN 設定の名前とデバイスの詳細を変更できます。

手順

変更する設定を選択し、[アクション（Actions）] の下で [編集（Edit）] をクリックします。

- 必要に応じて名前を変更します。
- 青色のプラス ボタンをクリックして、新しいデバイスを追加します。
- をクリックして、FTD デバイスで次の手順を実行します。
  - [編集（Edit）] をクリックして、既存の RA VPN 設定を変更します。
  - [削除（Remove）] をクリックして、RA VPN 設定から FTD デバイスを削除します。グループポリシーを除き、そのデバイスに関連付けられているすべての接続プロファイルと RA VPN 設定が削除されます。グループポリシーは、オブジェクトページから

明示的に削除できます。**注**：設定を使用しているデバイスがその FTD だけの場合、FTD を削除できません。代わりに、RA VPN 設定を削除できます。

設定またはデバイスの名前を入力して、リモートアクセス VPN 設定を検索することもできます。

関連情報：

- FTD RA VPN 接続プロファイルの設定。
- すべてのデバイスの設定変更のプレビューと展開。
- リモート アクセス VPN によるトラフィックの許可。

FTD RA VPN 接続プロファイルの設定

RA VPN 接続プロファイルの定義する接続特性では、外部ユーザーが AnyConnect クライアントを使用してシステムに VPN 接続することを許可します。各プロファイルは、ユーザーの認証に使用される AAA サーバーと証明書、ユーザーの IP アドレスを割り当てるためのアドレスプール、およびさまざまなユーザー関連の属性を定義するグループポリシーを定義します。

異なるユーザーグループに異なるサービスを提供する必要がある場合、または異なる認証ソースがある場合は、RA VPN 設定内に複数のプロファイルを作成できます。たとえば、自分の組織が異なる認証サーバーを使用する別の組織とマージする場合、別の組織の認証サーバーを使用する新しいグループのプロファイルを作成できます。

RA VPN 接続プロファイルを作成すると、ユーザーは、ホームネットワークなどの外部ネットワークから内部ネットワークに接続できるようになります。異なる認証方式に対応するために、個別のプロファイルを作成します。

はじめる前に

リモート アクセス（RA）VPN 接続を設定する前に、以下のことを行います。

- リモート アクセス VPN 接続を終了する外部インターフェイスは、HTTPS 接続を許可する管理アクセス リストを持つこともできません。RA VPN を設定する前に、外部インターフェイスから HTTPS ルールを削除します。『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド（バージョン X.Y）』内の「システム管理」の章の「管理アクセスリストの構成」を参照してください。
- RA VPN 構成を作成します。『FTD RA VPN 設定の作成』を参照してください。

手順

手順

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNの設定（Remote Access VPN Configuration）]** をクリックします。VPN 設定をクリックして、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報を表示できます。

ステップ 2 接続プロファイルをクリックし、右側のサイドバーの [アクション（Actions）] で [接続プロファイルの追加（Add Connection Profile）] をクリックします。

ステップ 3 基本接続の属性を設定します。

- [接続プロファイル名（Connection Profile Name）]：スペースを含めずに最大 50 文字で、この接続の名前を指定します。例、MainOffice。

  （注） ここで入力する名前が、AnyConnect クライアントの接続リストに表示されます。ユーザーにとって意味のある名前を選択します。

- [グループエイリアス（Group Alias）]、[グループURL（Group URL）]：エイリアスには特定の接続プロファイルの代替名または URL が含まれます。VPN ユーザーは、FTD デバイスへの接続時に、AnyConnect クライアントの接続リストでエイリアス名を選択できます。接続プロファイル名はグループのエイリアスとして自動的に追加されます。グループ URL のリストも設定できます。このリストは、リモートアクセス VPN 接続を開始するときにエンドポイントが選択できるリストです。ユーザーがグループ URL を使用して接続すると、システムはその URL に一致する接続プロファイルを自動的に使用します。この URL は、AnyConnect クライアントをまだインストールしていないクライアントによって使用されます。グループエイリアスと URL を必要な数だけ追加します。これらのエイリアスと URL は、デバイスで定義されているすべての接続プロファイルで一意である必要があります。グループ URL は https:// で始まる必要があります。

- たとえば、エイリアスは Contractor、グループ URL は https://ravpn.example.com/contractor のように指定できます。AnyConnect クライアントをインストールすると、ユーザーは単純に AnyConnect VPN の接続ドロップダウンリストでグループエイリアスを選択します。

ステップ 4 プライマリ アイデンティティ ソース、および必要に応じてセカンダリ ソースを設定します。これらのオプションにより、リモートアクセス VPN 接続を有効にするための、デバイスへのユーザー認証方法が決定されます。最も簡単なアプローチは、AAA のみを使用し、AD レルムを選択するか、または LocalIdentitySource を使用する方法です。[認証タイプ（Authentication Type）] として次のアプローチを使用できます。

- [AAAのみ（AAA Only）]：ユーザー名とパスワードに基づいてユーザーを認証および認可します。詳細については、「接続プロファイルのための AAA の設定」を参照してください。

- [クライアント証明書のみ（Client Certificate Only）]：クライアント デバイス アイデンティティ証明書に基づいてユーザーを認証します。詳細については、「接続プロファイルのための証明書認証の設定」を参照してください。

- [AAAおよびクライアント認証（AAA and Client Certificate）]：ユーザー名/パスワードと、クライアント デバイス アイデンティティ証明書の両方を使用します。

ステップ 5 クライアントのアドレスプールを設定します。アドレスプールは、リモートクライアントが VPN 接続を確立するときに、システムがリモートクライアントに割り当てることができる IP アドレスを定義します。詳細については、「クライアントアドレスプール割り当ての設定」を参照してください。

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 リストからこのプロファイルに対して使用する [グループポリシー（Group Policy）] を選択し、[選択（Select）] をクリックします。グループポリシーは、トンネル確立後のユーザー接続の期間を設定します。システムには、DfltGrpPolicy という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

（注） 必要なグループポリシーがまだ存在しない場合は、[オブジェクト（Objects）] ページでグループポリシーを作成し、そのポリシーを RA VPN 設定に関連付けます。グループポリシーの詳細については、「新しい FTD RA VPN グループポリシーの作成」を参照してください。

ステップ 8 [続行（Continue）] をクリックします。

ステップ 9 サマリーを確認します。最初に、サマリーが正しいことを確認します。AnyConnect ソフトウェアをインストールし、VPN 接続を完了できることをテストするために、エンドユーザーが最初に行う必要がある内容を確認できます。  をクリックしてこれらの手順をクリップボードにコピーし、ユーザーに配布します。

ステップ 10 [完了（Done）] をクリックします。

次のタスク

「リモート アクセス VPN によるトラフィックの許可」で説明したように、トラフィックが VPN トンネルで許可されていることを確認します。

接続プロファイルのための AAA の設定

認証、許可、およびアカウンティング（AAA） サーバーは、ユーザー名とパスワードを使用して、ユーザーのリモートアクセス VPN へのアクセスを許可するかどうかを判断します。RADIUS サーバを使用する場合は、認証されたユーザー間で許可レベルを区別して、保護されたリソースへの差別化されたアクセスを提供できます。使用状況を追跡するために RADIUS アカウンティングサービスを使用することもできます。

AAA を設定する場合は、プライマリ アイデンティティ ソースを設定する必要があります。セカンダリソースとフォールバックソースはオプションです。RSA トークンや DUO などを使用する二重認証を実装する場合は、セカンダリソースを使用します。

プライマリ アイデンティティ ソースのオプション

- [ユーザー認証用のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]：リモート ユーザーの認証に使用されるプライマリ アイデンティティ ソース。VPN 接続を完了するには、エンド ユーザがこのソースか任意のフォールバック ソースで定義されている必要があります。次のいずれかを選択します。
  - Active Directory（AD）のアイデンティ レルム。必要なレルムがまだ存在していない場合は、[新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックします。
  - RADIUS サーバーグループ。
  - LocalIdentitySource（ローカル ユーザー データベース）：デバイスで直接ユーザーを定義できます。外部サーバーを使用することはできません。
- [フォールバックローカルアイデンティティソース（Fallback Local Identity Source）]：プライマリ ソースが外部サーバーの場合、プライマリサーバーが使用できない場合のフォールバックとして LocalIdentitySource を選択できます。フォールバック ソースとしてローカル データベースを使用する場合は、必ず外部サーバで定義したものと同じローカル ユーザ名/パスワードを定義します。
- [削除オプション（Strip options）]：レルムとは管理ドメインのことです。次のオプションを有効にすると、ユーザー名だけに基づいて認証できます。これらのオプションを任意に組み合わせて有効にできます。ただし、サーバーが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。
  - [ユーザー名からアイデンティティソースサーバーを削除（Strip Identity Source Server from Username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からアイデンティティソース名を削除するかどうか。たとえば、このオプションを選択してユーザーがユーザー名として domain\username を入力すると、ドメインがユーザー名から取り除かれ、認証用に AAA サーバーに送信されます。デフォルトでは、このオプションはオフになります。
  - [ユーザー名からグループを削除（Strip Group from username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からグループを削除するかどうか。このオプションは、username@domain 形式で指定された名前に適用されます。選択すると、domain と @ 記号が削除されます。デフォルトでは、このオプションはオフになります。

セカンダリ アイデンティティ ソース

- [ユーザー認証用のセカンダリアイデンティティソース（Secondary Identity Source for User Authentication）]：オプションの 2 番目のアイデンティティソースです。ユーザーがプライマリ ソースで正常に認証されると、セカンダリ ソースでの認証が求められます。AD レルム、RADIUS サーバーグループ、またはローカル アイデンティティ ソースを選択することができます。
- [詳細オプション（Advanced options）]：[詳細（Advanced）] リンクをクリックし、次のオプションを設定します。

- [セカンダリ用フォールバックローカルアイデンティティソース（Fallback Local Identity Source for Secondary）]：セカンダリソースが外部サーバーの場合、セカンダリサーバーが使用できない場合のフォールバックとしてLocalIdentitySourceを選択できます。フォールバックソースとしてローカルデータベースを使用する場合は、必ずセカンダリ外部サーバーで定義したものと同じローカルユーザー名/パスワードを定義します。

- [セカンダリログインにプライマリユーザー名を使用（Use Primary Username for Secondary Login）]：デフォルトでは、セカンダリアイデンティティソースを使用する場合、セカンダリ ソースに対してユーザー名とパスワードの両方が求められます。このオプションを選択すると、システムはセカンダリパスワードの入力のみを求め、プライマリ アイデンティティ ソースに対して認証されたものと同じユーザー名をセカンダリソースに対して使用します。プライマリとセカンダリの両方のアイデンティティソースで同じユーザー名を設定する場合は、このオプションを選択します。

  - [セッションサーバーのユーザー名（Username for Session Server）]：認証に成功すると、ユーザー名はイベントと統計ダッシュボードに表示されます。ユーザー名はユーザーベースまたはグループベースのSSL復号化およびアクセス制御ルールに一致するものを判断するために使用され、アカウンティングに使用されます。2つの認証ソースを使用しているため、ユーザーアイデンティティとして、プライマリまたはセカンダリのどちらのユーザー名を使用するのかシステムに通知する必要があります。デフォルトでは、プライマリ名が使用されます。

  - [パスワードタイプ（Password Type）]：セカンダリサーバーのパスワードを取得する方法。デフォルトは[プロンプト（Prompt）]で、ユーザーはパスワードの入力が求められることを意味します。プライマリサーバーへのユーザー認証時に入力したパスワードを自動的に使用するには、[プライマリアイデンティティソースのパスワード（Primary Identity Source Password）]を選択します。すべてのユーザーに同じパスワードを使用するには[共通パスワード（Common Password）]を選択し、[共通パスワード（Common Password）]フィールドにそのパスワードを入力します。

- [認証サーバー（Authorization Server）]：リモートアクセスVPNユーザーを認証するように設定されたRADIUSサーバーグループです。認証の完了後、認可によって、認証済みの各ユーザーが使用できるサービスおよびコマンドが制御されます。認可は、ユーザーが実行を認可されていることを示す属性のセット、実際の機能、および制限事項をアセンブルすることによって機能します。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザーに対して同じアクセス権を提供します。認証のためにRADIUSを構成する方法については、『RADIUSおよびグループポリシーを使用したユーザーの権限および属性の制御』システムがグループポリシーで定義されているものと重複する認可属性をRADIUSサーバーから取得した場合、RADIUS属性は、グループポリシー属性をオーバーライドすることに注意してください。

- [アカウンティングサーバー（Accounting Server）]：（オプション）リモートアクセスVPNセッションへのアカウンティングに使用するRADIUSサーバーグループ。アカウンティングは、ユーザーがアクセスしているサービスや、ユーザーが消費しているネットワークリソースの数を追跡します。FTDデバイスは、RADIUSサーバにユーザアクティビティを報告します。アカウンティング情報には、セッションの開始時刻と

停止時刻、ユーザー名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

接続プロファイルのための証明書認証の設定

（注） このセクションは、**認証タイプ**が **AAA のみ**の場合には適用されません。

リモート アクセス VPN 接続を認証するために、クライアント デバイスにインストールされた証明書を使用することができます。

クライアント証明書を使用していても、セカンダリ アイデンティティ ソース、フォールバック ソース、および認証およびアカウンティングサーバーを引き続き設定できます。これらは AAA オプションです。詳細については、『FTD RA VPN 接続プロファイルの設定』を参照してください。

以下に、証明書固有の属性を示します。これらの属性は、プライマリ アイデンティティ ソースとセカンダリ アイデンティティ ソースに対して個別に設定できます。セカンダリソースの設定はオプションです。

- [証明書のユーザー名（Username from Certificate）]：次のいずれかを選択します。
  - [マップ固有フィールド（Map Specific Field）]：証明書の要素を [プライマリフィールド（Primary Field）] および [セカンダリフィールド（Secondary Field）] の順番で使用します。デフォルトはCN（共通名）とOU（組織単位）です。組織に適したオプションを選択します。これらのフィールドを組み合わせてユーザー名が提供され、このユーザー名がイベント、ダッシュボード、さらにSSL復号とアクセス制御ルールでのマッチング目的に使用されます。
  - [DN（識別名）全体をユーザー名として使用（Use entire DN (distinguished name) as username）]：システムが自動的に DN フィールドからユーザー名を導出します。•
- [詳細オプション（Advanced options）]：（[認証タイプ（Authentication Type）] が [クライアント証明書のみ（Client Certificate Only）] の場合には適用されません）：[詳細（Advanced）] リンクをクリックし、次のオプションを設定します。
  - [ユーザーログインウィンドウの証明書からユーザー名を事前入力（Prefill username from certificate on user login window）]：ユーザーに認証を要求するときに、取得したユーザー名をユーザー名フィールドに入力するかどうか。
  - [ログインウィンドウでユーザー名を非表示にする（Hide username in login window）]：[事前入力（Prefill）] オプションを選択すると、ユーザー名を非表示にできます。これは、ユーザーがパスワードプロンプトでユーザー名を編集できないことを意味します。

クライアントアドレスプール割り当ての設定

リモートアクセス VPN に接続するエンドポイントにシステムが IP アドレスを提供するための方法が必要です。AAA サーバーは、これらのアドレス、DHCP サーバー、グループポリシーで設定されている IP アドレスプール、または接続プロファイルで設定された IP アドレスプールを提供できます。システムは、この順序でこれらのリソースを試行し、使用可能なアドレスを取得すると停止し、次にアドレスをクライアントに割り当てます。このように、同時接続数が異常な場合のフェールセーフを作成するために複数のオプションを設定できます。

接続プロファイルのアドレスプールを設定するには、次の方法の 1 つ以上を使用します。

- [IPv4アドレスプール（IPv4 Address Pool）] および [IPv4アドレスプール（IPv4 Address Pool）]：まず、サブネットを指定する最大 6 つのネットワークオブジェクトを作成します。IPv4 と IPv6 に別々のプールを設定できます。次に、グループポリシーまたは接続プロファイルの [IPv4アドレスプール（IPv4 Address Pool）] および [IPv6アドレスプール（IPv6 Address Pool）] オプションで、これらのオブジェクトを選択します。IPv4 と IPv6 の両方を設定する必要はありません。サポートするアドレス方式を設定してください。また、グループポリシーと接続プロファイルの両方でプールを設定する必要もありません。グループポリシーは接続プロファイル設定をオーバーライドします。そのため、グループポリシーでプールを設定する場合は、接続プロファイルのオプションを空白のままにしてください。プールはリストの順序で使用されることに注意してください。

- [DHCPサーバー（DHCP Servers）]：まず、1 つ以上の IPv4 アドレス範囲を持つ RA VPN の DHCP サーバーを設定します（DHCP を使用して IPv6 プールを設定することはできません）。次に、DHCP サーバーの IP アドレスを使用してホスト ネットワーク オブジェクトを作成します。その後、このオブジェクトは接続プロファイルの [DHCPサーバー（DHCP Servers）] 属性で選択できます。複数の DHCP サーバーを設定することができます。DHCP サーバーに複数のアドレスプールがある場合、[DHCPスコープ（DHCP Scope）] 属性を接続プロファイルにアタッチするグループポリシーで使用して、使用するプールを選択することができます。プールのネットワークアドレスを使用して、ホスト ネットワーク オブジェクトを作成します。たとえば、DHCP プールに 192.168.15.0/24 および 192.168.16.0/24 が含まれている場合、DHCP スコープを 192.168.16.0 に設定すると、192.168.16.0/24 サブネットからのアドレスが必ず選択されるようになります。

リモート アクセス *VPN* によるトラフィックの許可

リモートアクセス VPN トンネル内のトラフィックフローを有効にするには、次の方法のいずれかを使用します。

- **sysopt connection permit-vpn** コマンドを設定すると、VPN 接続と一致するトラフィックがアクセス コントロール ポリシーから除外されます。このコマンドのデフォルトは **no sysopt connection permit-vpn** で、VPN トラフィックをアクセス コントロール ポリシーでも許可する必要があることを意味します。これは、外部ユーザーがリモートアクセス VPN アドレスプール内の IP アドレスをスプーフィングできないため、VPN でトラフィックを許可するよりも安全な方法です。欠点は VPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。つまり、このトラフィックに対する接続イベントは生成されず、VPN 接続は統計ダッシュボードには反映されません。このコマンドを設定するには、RA VPN 設定で

[復号されたトラフィックに対するバイパスアクセスコントロールポリシー（Bypass Access Control policy for decrypted traffic）] オプションを選択します。「FTD RA VPN 設定の作成」を参照してください。

- リモート アクセス VPN アドレス プールからの接続を許可するアクセス制御ルールを作成します。この方法では、VPN トラフィックが確実に検査され、アドバンスドサービスを接続に適用できます。欠点は、外部のユーザーが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。「FTD アクセス コントロール ポリシーの設定」を参照してください。

FTD バージョン *6.4.0* での *AnyConnect* パッケージのアップグレード

CDO を使用して、Firepower Threat Defense（FTD）デバイスで使用可能な AnyConnect パッケージをアップグレードし、RA VPN ユーザーに配布できるようにすることができます。

AnyConnect パッケージのアップグレードに関連した主な手順は次のとおりです。

手順

ステップ 1 Firepower Device Manager（FDM）を使用して AnyConnect パッケージを削除し、パッケージの新しいバージョンをアップロードします。このタスクを実行するには、次のいずれかの方法を使用します。

- 古いパッケージを削除し、FDM UI から新しいパッケージをアップロードします。
- 古いパッケージを削除し、FDM API エクスプローラから新しいパッケージをアップロードします。

ステップ 2 FDM への変更を FTD に展開します。

ステップ 3 新しい設定情報を CDO に読み込みます。

ステップ 4 RA VPN 接続プロファイルで新しいパッケージを確認します。

前提条件

- 接続プロファイルを持つ少なくとも 1 つの RA VPN 設定が、すでに FTD に展開されています。
- https://software.cisco.com/download/home/283000185 から必要な AnyConnect パッケージをダウンロードします。シスコでは、入手可能な最新のパッケージにアップグレードすることを推奨しています。

FDM を使用した必要な AnyConnect パッケージの FTD へのアップロード

手順

ステップ 1 ブラウザを使用して、システムのホームページを開きます。例：https://ftd.example.com

ステップ 2 FDM にログインします。

ステップ 3 **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 4 表示ボタン  （設定表示ボタン）をクリックして、接続プロファイルの概要と接続手順を開きます。

（注） いずれかの接続プロファイルを編集して、AnyConnect パッケージを FTD デバイスにアップロードできます。

ステップ 5 [編集（Edit）] ボタンをクリックして変更を加えます。

ステップ 6 [グローバル設定（Global Settings）] 画面が表示されるまで [次へ] をクリックします。[AnyConnect パッケージ（AnyConnect Package）] には、FTD デバイスで使用可能な AnyConnect パッケージが表示されます。

ステップ 7 [X] ボタンをクリックして、置き換える AnyConnect パッケージを削除します。

ステップ 8 [パッケージのアップロード（Upload Package）] をクリックし、互換性のあるパッケージのアップロードに使用する OS をクリックします。

ステップ 9 パッケージを選択したら、[開く（Open）] をクリックします。FDM の UI でアップロードされているパッケージを確認できます。

ステップ 10 [終了（Finish）] をクリックします。設定が保存されます。

（注） または、FDM API エクスプローラを使用して、AnyConnect パッケージを削除して新しいパッケージをアップロードすることもできます。

1. /#/Api-explorer を指すように URL を編集します（たとえば、https://ftd.example.com/#/api-explorer）。
2. FTD デバイスからパッケージを削除します。**[AnyConnectPackageFile]** > **[削除（Delete）]** をクリックします。[objID] フィールドにパッケージ ID を入力し、[試す（TRY IT OUT!）] をクリックします。

3. AnyConnect ソフトウェアパッケージの FTD バージョン 6.4.0 へのアップロードに関するセクションで説明されている手順を実行して、新しいパッケージをアップロードします。

ステップ 11 Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。このアイコンは、展開されていない変更がある場合にドット マークで強調表示されます。

ステップ 12 変更内容に問題がない場合は、[今すぐ展開（Deploy Now）] をクリックして、ジョブをすぐに開始できます。ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。

RA VPN 接続プロファイルで新しいパッケージが参照されていることを確認する

手順

ステップ 1 左側の CDO ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックし、アップグレードされた AnyConnect パッケージがある FTD デバイスを選択します。このデバイスは競合を報告します。

ステップ 4 [承認（Accept）] : アウトオブバンド変更を承認して、**CDO に保存されている設定と保留中の変更**を、デバイスの実行中の設定で上書きします。詳細については、「[競合検出（Conflict Detected）] ステータスの解決」を参照してください。

ステップ 5 次の手順を実行して、新しい AnyConnect パッケージを表示します。

- **[VPN]** > **[リモートアクセスVPN（Remote Access VPN）]** をクリックします。
- この FTD デバイスに関連付けられている RA VPN 設定をクリックします。
- [アクション（Actions）] の [編集（Edit）] をクリックします。新しいパッケージが [デバイス（Devices）] に表示されます。

RA VPN AnyConnect クライアントプロファイルのアップロード

リモートアクセス VPN AnyConnect クライアントプロファイルは、ファイルに保存されている設定パラメータのグループです。AnyConnect クライアントプロファイルにはさまざまな種類があり、コアクライアント VPN 機能とオプション クライアント モジュールであるネットワーク アクセス マネージャ、AMP イネーブラ、ISE ポスチャ、ネットワークの可視性、カスタマー フィードバック エクスペリエンス プロファイル、Umbrella ローミングセキュリティ、Web セキュリティの構成設定が含まれています。

CDO では、後でグループポリシーで使用できるオブジェクトとしてこれらのプロファイルをアップロードできます。

- [AnyConnect VPNプロファイル（AnyConnect VPN Profile）]：AnyConnect クライアントプロファイルは、VPN AnyConnect クライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザーが AnyConnect クライアントの設定および詳細設定からオプションを変更できるかどうかを定義します。CDO は XML ファイル形式をサポートしています。
- [AMPイネーブラサービスプロファイル（AMP Enabler Service Profile）]：このプロファイルは AnyConnect AMP イネーブラに使用されます。リモートアクセス VPN ユーザーが VPN に接続すると、AMP イネーブラがこのプロファイルと共に FTD からエンドポイントにプッシュされます。CDO は、XML および ASP ファイル形式をサポートしています。
- [フィードバックプロファイル（Feedback Profile）]：カスタマー エクスペリエンス フィードバック プロファイルを追加し、このタイプを選択すると、顧客が有効にして使用している機能およびモジュールに関する情報を受信できます。CDO は FSP ファイル形式をサポートしています。
- [ISEポスチャプロファイル（ISE Posture Profile）]：AnyConnect ISE ポスチャモジュールのプロファイルファイルを追加する場合は、このオプションを選択します。CDO は、XML および ISP ファイル形式をサポートしています。
- [ネットワークアクセスマネージャサービスプロファイル（Network Access Manager Service Profile）]：ネットワーク アクセス マネージャのプロファイルエディタを使用して、NAM プロファイルファイルを設定および追加します。CDO は、XML および NSP ファイル形式をサポートしています。
- [ネットワーク可視性サービスプロファイル（Network Visibility Service Profile）]：AnyConnect Network Visibility Module のプロファイルファイル。NVM プロファイルエディタを使用してプロファイルを作成できます。CDO は、XML および NVMSP ファイル形式をサポートしています。
- [Umbrellaローミングセキュリティプロファイル（Umbrella Roaming Security Profile）]：Umbrella ローミング セキュリティ モジュールを展開する場合は、このファイルタイプを選択する必要があります。CDO は、XML および JSON ファイル形式をサポートしています。
- [Webセキュリティサービスプロファイル（Web Security Service Profile）]：Web セキュリティモジュールのプロファイルファイルを追加するときに、このファイルタイプを選択します。CDO は、XML、WSO、および WSP ファイル形式をサポートします。

始める前に

適切な GUI ベースの AnyConnect プロファイルエディタを使用して、必要なプロファイルを作成します。AnyConnect セキュア モビリティ クライアント カテゴリの Cisco Software Download Center からプロファイルエディタをダウンロードし、AnyConnect の「プロファイルエディタ - Windows / スタンドアロンインストーラ（MSI）」をインストールできます。プロファイルエディタのインストーラには、スタンドアロンバージョンのプロファイルエディタが含まれています。このインストール ファイルは Windows 専用で、ファイル名は

anyconnect-profileeditor-win-<version>-k9.msi です。ここで、<version> は AnyConnect のバージョンです。たとえば、anyconnect-profileeditor-win-4.3.04027-k9.msi のような名前になります。プロファイル エディタをインストールする前に、Java JRE（1.6 以降）もインストールする必要があります。

このパッケージには、Umbrella ローミング セキュリティ プロファイル エディタを除き、モジュールの作成に必要なすべてのプロファイルエディタが含まれています。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するリリースの「*AnyConnect* プロファイルエディタ」の章を参照してください。Umbrella ダッシュボードから Umbrella ローミング セキュリティ プロファイルを個別にダウンロードします。詳細については、『Cisco Umbrella User Guide』の「Umbrella ローミングセキュリティ」章の「Umbrella ダッシュボードから AnyConnect ローミング セキュリティ プロファイルをダウンロードする」セクションを参照してください。

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 青色のプラス ボタンをクリックします。

ステップ 3 **[RA VPNオブジェクト（ASA & FTD）（RA VPN Objects (ASA & FTD)）] > [AnyConnectクライアントプロファイル（AnyConnect Client Profile）]**をクリックします。

ステップ 4 [オブジェクト名（Object Name）] フィールドに、AnyConnect クライアントプロファイルの名前を入力します。

ステップ 5 [参照（Browse）]をクリックし、プロファイルエディタを使って作成したファイルを選択します。

ステップ 6 [開く（Open）] をクリックしてプロファイルをアップロードします。

ステップ 7 [追加（Add）] をクリックしてオブジェクトを追加します。

関連情報：

- RA VPN グループポリシーウィンドウで、クライアントモジュールを AnyConnect VPN プロファイルに関連付けます。「新しい FTD RA VPN グループポリシーの作成」を参照してください。

（注） クライアントモジュールの関連付けは、すべての ASA バージョン、およびソフトウェアバージョン 6.7 以降を実行している FTD でサポートされています。

FTD のリモートアクセス VPN のガイドラインと制限事項

RA VPN を設定する際は、次のガイドラインと制限事項に留意してください。

- AnyConnect パッケージは、FDM を使用して FTD バージョン 6.4.0 に事前にロードしておく必要があります。

（注） CDO のリモートアクセス VPN 設定ウィザードを使用して、AnyConnect パッケージを別個に FTD バージョン 6.5.0 にアップロードします。

- CDO から RA VPN を設定する前に、以下の操作を実行します。
  - FDM から FTD デバイスの RA VPN ライセンスを登録します。
  - エクスポート制御機能を使用して FDM から AnyConnect ライセンスを有効にします。
- CDO は、拡張アクセスリストオブジェクトをサポートしていません。FDM で Smart CLI を使用してオブジェクトを設定してから、VPN フィルタおよび認可変更（CoA）リダイレクト ACL で使用します。
- FTD デバイスから作成するテンプレートに、RA VPN 設定は含まれません。
- IP プールオブジェクトと RADIUS アイデンティティソースには、デバイス固有のオーバーライドが必要です。
- 同じ TCP ポートの同じインターフェイスで、FDM アクセス（管理アクセスリストの HTTPS アクセス）と AnyConnect リモートアクセス SSL VPN の両方を設定することはできません。たとえば、外部インターフェイスにリモートアクセス SSL VPN を設定する場合、ポート 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。FDM ではこれらの機能に使用されるポートを設定できないため、同じインターフェイスで両方の機能を設定することはできません。
- RADIUS トークンと RSA トークンを使用して二要素認証を設定すると、ほとんどの場合、デフォルトの 12 秒の認証タイムアウトでは短すぎて正常な認証が行われません。「RA VPN AnyConnect クライアントプロファイルのアップロード（348 ページ）」の説明に従って、カスタム AnyConnect クライアントプロファイルを作成し、それを RA VPN 接続プロファイルに適用することにより、認証タイムアウト値を増やします。認証タイムアウトを 60 秒以上にすることをお勧めします。これにより、ユーザーの認証および RSA トークンの貼り付けと、トークンのラウンドトリップ検証のための十分な時間が得られます。

ユーザーが AnyConnect クライアントソフトウェアを FTD にインストールする方法

FDM API を使用して AnyConnect クライアント ソフトウェア パッケージを FTD にアップロードし、ユーザーに配布します。「AnyConnect ソフトウェアパッケージの FTD バージョン 6.4.0 へのアップロード」を参照してください。

VPN 接続を完了するには、ユーザは AnyConnect クライアント ソフトウェアをインストールする必要があります。既存のソフトウェア配布方式を使用して、ソフトウェアを直接インストールできます。または、FTD デバイスから AnyConnect クライアントを直接インストールすることもできます。

（注） ソフトウェアをインストールするには、ユーザにワークステーションでの管理者権限が必要です。

ソフトウェアの最初のインストールを FTD デバイスからユーザーに行ってもらう場合、以下の手順を実行するようにユーザーに指示します。

（注） Android および iOS のユーザは、適切な App Store から AnyConnect をダウンロードする必要があります。

手順

ステップ 1 Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。このインターフェイスは、リモート アクセス VPN を設定する際に指定します。ログインを指示するメッセージがユーザに示されます。

ステップ 2 サイトにログインします。ユーザは、リモート アクセス VPN 用に設定されたディレクトリ サーバを使用して認証されます。続行するには、ログインが正常に行われる必要があります。ログインが成功すると、システムは、必要となる AnyConnect クライアントのバージョンがインストールされているかを確認します。AnyConnect クライアントがユーザーのコンピュータにないか、下位のバージョンである場合、システムは自動的に AnyConnect ソフトウェアのインストールを開始します。インストールが終了すると、AnyConnect がリモートアクセス VPN 接続を完了します。

AnyConnect クライアント ソフトウェア バージョンの配信

AnyConnectクライアントソフトウェアの新しいバージョンをユーザーに配信するには、旧バージョンを削除せずに新しいバージョンを FTD にアップロードします。AnyConnect クライアントが正常にアップロードされたら、旧バージョンを削除できます。

ユーザーが次回 VPN 接続を確立すると、AnyConnect クライアントは新しいバージョンを検出します。更新されたクライアント ソフトウェアのダウンロードとインストールを指示するメッセージが自動的に表示されます。この自動化により、ソフトウェアの配布が容易になります。

次の図は、Windows OS 用の 2 つのバージョンの AnyConnect クライアントソフトウェア（**AnyConnectWindows_3.2_BGL** と **AnyConnectWindows_4.2_BGL**）を備えた FTD デバイスの例を示しています。

RA VPN AnyConnect クライアントプロファイルのアップロード

リモートアクセス VPN AnyConnect クライアントプロファイルは、ファイルに保存されている設定パラメータのグループです。AnyConnect クライアントプロファイルにはさまざまな種類があり、コアクライアント VPN 機能とオプション クライアント モジュールであるネットワーク アクセス マネージャ、AMP イネーブラ、ISE ポスチャ、ネットワークの可視性、カスタマー フィードバック エクスペリエンス プロファイル、Umbrella ローミングセキュリティ、Web セキュリティの構成設定が含まれています。

CDO では、後でグループポリシーで使用できるオブジェクトとしてこれらのプロファイルをアップロードできます。

- [AnyConnect VPNプロファイル（AnyConnect VPN Profile）]：AnyConnect クライアントプロファイルは、VPN AnyConnect クライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザーが AnyConnect クライアントの設定および詳細設定からオプションを変更できるかどうかを定義します。CDO は XML ファイル形式をサポートしています。
- [AMPイネーブラサービスプロファイル（AMP Enabler Service Profile）]：このプロファイルは AnyConnect AMP イネーブラに使用されます。リモートアクセス VPN ユーザーが VPN に接続すると、AMP イネーブラがこのプロファイルと共に FTD からエンドポイントにプッシュされます。CDO は、XML および ASP ファイル形式をサポートしています。
- [フィードバックプロファイル（Feedback Profile）]：カスタマー エクスペリエンス フィードバック プロファイルを追加し、このタイプを選択すると、顧客が有効にして使用している機能およびモジュールに関する情報を受信できます。CDO は FSP ファイル形式をサポートしています。
- [ISEポスチャプロファイル（ISE Posture Profile）]：AnyConnect ISE ポスチャモジュールのプロファイルファイルを追加する場合は、このオプションを選択します。CDO は、XML および ISP ファイル形式をサポートしています。

- [ネットワークアクセスマネージャサービスプロファイル（Network Access Manager Service Profile）]：ネットワーク アクセス マネージャのプロファイルエディタを使用して、NAM プロファイルファイルを設定および追加します。CDO は、XML および NSP ファイル形式をサポートしています。
- [ネットワーク可視性サービスプロファイル（Network Visibility Service Profile）]：AnyConnect Network Visibility Module のプロファイルファイル。NVM プロファイルエディタを使用してプロファイルを作成できます。CDO は、XML および NVMSP ファイル形式をサポートしています。
- [Umbrellaローミングセキュリティプロファイル（Umbrella Roaming Security Profile）]：Umbrella ローミング セキュリティ モジュールを展開する場合は、このファイルタイプを選択する必要があります。CDO は、XML および JSON ファイル形式をサポートしています。
- [Webセキュリティサービスプロファイル（Web Security Service Profile）]：Web セキュリティモジュールのプロファイルファイルを追加するときに、このファイルタイプを選択します。CDO は、XML、WSO、および WSP ファイル形式をサポートします。

始める前に

適切な GUI ベースの AnyConnect プロファイルエディタを使用して、必要なプロファイルを作成します。AnyConnect セキュア モビリティ クライアント カテゴリの Cisco Software Download Center からプロファイルエディタをダウンロードし、AnyConnect の「プロファイルエディタ - Windows / スタンドアロンインストーラ（MSI）」をインストールできます。プロファイルエディタのインストーラには、スタンドアロンバージョンのプロファイルエディタが含まれています。このインストール ファイルは Windows 専用で、ファイル名は anyconnect-profileeditor-win-<version>-k9.msi です。ここで、<version> は AnyConnect のバージョンです。たとえば、anyconnect-profileeditor-win-4.3.04027-k9.msi のような名前になります。プロファイル エディタをインストールする前に、Java JRE（1.6 以降）もインストールする必要があります。

このパッケージには、Umbrella ローミング セキュリティ プロファイル エディタを除き、モジュールの作成に必要なすべてのプロファイルエディタが含まれています。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するリリースの「*AnyConnect* プロファイルエディタ」の章を参照してください。Umbrella ダッシュボードから Umbrella ローミング セキュリティ プロファイルを個別にダウンロードします。詳細については、『Cisco Umbrella User Guide』の「Umbrella ローミングセキュリティ」章の「Umbrella ダッシュボードから AnyConnect ローミング セキュリティ プロファイルをダウンロードする」セクションを参照してください。

手順

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 青色のプラス  ボタンをクリックします。

ステップ 3 **[RA VPNオブジェクト（ASA & FTD）（RA VPN Objects (ASA & FTD)）] > [AnyConnectクライアントプロファイル（AnyConnect Client Profile）]**をクリックします。

ステップ 4 [オブジェクト名（Object Name）] フィールドに、AnyConnect クライアントプロファイルの名前を入力します。

ステップ 5 [参照（Browse）] をクリックし、プロファイルエディタを使って作成したファイルを選択します。

ステップ 6 [開く（Open）] をクリックしてプロファイルをアップロードします。

ステップ 7 [追加（Add）] をクリックしてオブジェクトを追加します。

関連情報：

- RA VPN グループポリシーウィンドウで、クライアントモジュールを AnyConnect VPN プロファイルに関連付けます。「新しい FTD RA VPN グループポリシーの作成」を参照してください。

（注） クライアントモジュールの関連付けは、すべての ASA バージョン、およびソフトウェアバージョン 6.7 以降を実行している FTD でサポートされています。

リモート アクセス VPN のライセンス要件

FDM から FTD デバイスの RA VPN ライセンスを有効化（登録）して、RA VPN 接続を設定します。デバイスを登録する際に、エクスポート制御機能に対して有効化された Smart Software Manager（SSM）アカウントに登録する必要があります。また、評価ライセンスを使用して機能を設定することはできません。

また、いずれかの RA VPN ライセンス（AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN Only）を購入して、有効にする必要があります。これらのライセンスは、ASA ソフトウェアベースのヘッドエンドで使用される場合、さまざまな機能セットを許可するように設計されていますが、FTD デバイスでは同様に扱われます。

FDM からのライセンスの有効化の詳細については、デバイスが実行しているバージョンの Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）[英語] の「Remote Access VPN」の章にある「Licensing Requirements for Remote Access VPN」を参照してください。https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html#anchor531

詳細については、*Cisco AnyConnect* 発注ガイド [英語] を参照してください。http://www.cisco.com/c/en/us/product...t-listing.html には、他のデータシートもあります。

RA VPN ライセンスステータスを表示するには、次の手順を実行します。

手順

ステップ 1 左側の CDO ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、必要なデバイスを選択します。

ステップ 4 右側の [デバイスアクション（Device Actions）] ペインで、[ライセンスの管理（Manage Licenses）] をクリックします。RA VPN ライセンスが有効な場合、[ステータス（Status ）] には [有効（Enabled）] と表示されます。

デバイス モデル別の同時 VPN セッションの最大数

デバイスモデルに基づいて、1台のデバイスで許可される同時リモートアクセスVPNセッション数に上限が設けられます。この制限は、システムパフォーマンスが許容できないレベルまで低下しないように設計されています。これらの制限は、キャパシティプランニングに使用します。

デバイス モデル	最大同時リモート アクセス VPN セッション数
Firepower 2110	1,500
Firepower 2120	3,500
Firepower 2130	7,500
Firepower 2140	10,000
Firepower Threat Defense Virtual	250

RADIUS 許可の変更

RADIUS認可変更（CoA）機能は、認証、許可、アカウンティング（AAA）セッションの属性を、セッション認証後に変更するためのメカニズムを提供します。RA VPN の重要な課題は、侵害されたエンドポイントに対して内部ネットワークを保護し、ウイルスやマルウェアの影響を受けたときに、エンドポイントへの攻撃を修復することによって、エンドポイント自体を保護することです。エンドポイントと内部ネットワークは、RA VPNセッションの前、最中、および後のすべてのフェーズで保護する必要があります。RADIUS CoA機能は、この目標を達成するのに役に立ちます。

Cisco Identity Services Engine（ISE）RADIUS サーバーを使用する場合は、認可変更ポリシーの適用を設定できます。AAA のユーザーまたはユーザーグループのポリシーが変更されると、ISE は CoA メッセージを FTD デバイスに送信して認証を再初期化し、新しいポリシーを適用します。Inline Posture Enforcement Point（IPEP）では、FTD デバイスによって確立された各 VPN セッションにアクセスコントロールリスト（ACL）を適用する必要はありません。

関連情報：

- FTD デバイスでの認可変更の設定

FTD デバイスでの認可変更の設定

認可変更ポリシーのほとんどは、ISE サーバーで設定されます。ただし、FTD デバイスは適切に ISE に接続するように設定する必要があります。

はじめる前に

いずれかのオブジェクトでホスト名を使用する場合は、デバイスが実行しているバージョンに向けた『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド』の「システム設定」章の「**データおよび管理インターフェイス用の DNS 設定**」セクションで説明されているようにデータインターフェイスで使用する DNS サーバーを構成してください。通常、システムを完全に機能させるには、いずれにしても DNS を構成する必要があります。

手順

手順

ステップ 1 FTD デバイスの FDM にログインします。

ステップ 2 ISE への初期接続をリダイレクトするように、拡張アクセスコントロールリスト（ACL）を設定します。リダイレクト ACL の目的は、ISE がクライアントポスチャを評価できるように、初期トラフィックを ISE に送信することです。ACL は、ISE に HTTPS トラフィックを送信しますが、ISE 宛てのトラフィックや、名前解決のために DNS サーバーに送信されるトラフィックは送信しません。リダイレクト ACL の例を次に示します。

access-list redirect extended deny ip any host <ISE server IP>

access-list redirect extended deny ip any host <DNS server IP>

access-list redirect extended deny icmp any any

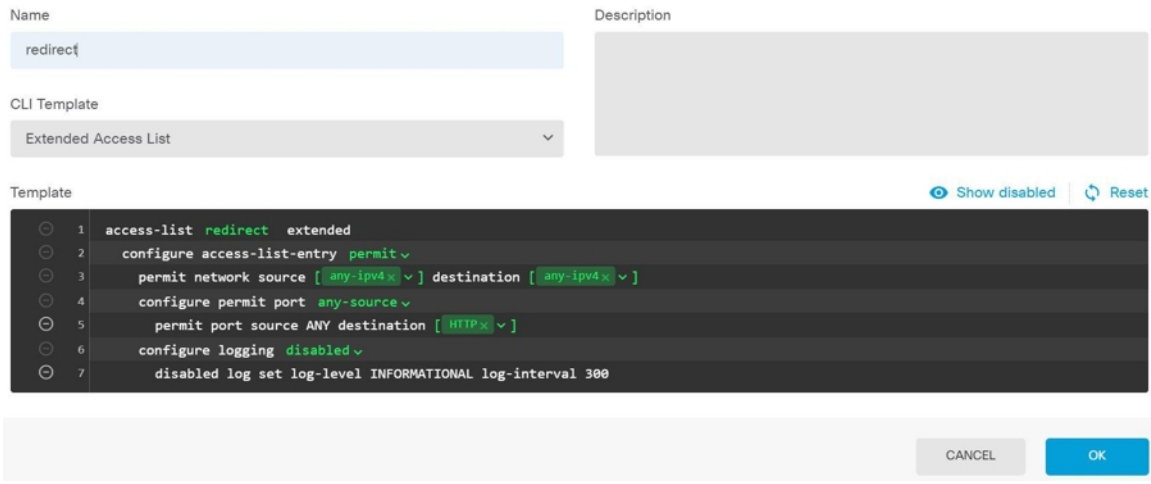
access-list redirect extended permit tcp any any eq www

ただし、ACL には、最後のアクセス制御エントリ（ACE）として暗黙の「deny any any」が含まれることに注意してください。この例では、TCP ポート www（つまりポート 80）に一致する最後の ACE は、最初の 3 つの ACE に一致するすべてのトラフィックと一致しないため、これらは冗長となります。単純に最後の ACE を使用して ACL を作成し、同じ結果を得ることもできます。リダイレクト ACL では、permit および deny アクションによって、ACL に一致するトラフィックが特定されることに注意してください（permit は一致、deny は不一致）。トラフィックは実際にはドロップされず、拒否されたトラフィックは ISE にリダイレクトされません。リダイレクト ACL を作成するには、Smart CLI オブジェクトを設定する必要があります。

1. **[デバイス（Device）] > [詳細設定（Advanced Configuration）] > [Smart CLI] > [オブジェクト（Objects）]** を選択します。
2. [+] をクリックして新しいオブジェクトを作成します。
3. ACL の名前を入力します。たとえば、**redirect** などと入力します。
4. [CLIテンプレート（CLI Template）] の場合は、[拡張アクセスリスト（Extended Access List）] を選択します。
5. [テンプレート（Template）] 本文で次のように設定します。

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = any-ipv4
- configure permit port = any-source
- destination-port = HTTP
- configure logging = disabled

ACE は次のようになります。



6. [OK] をクリックします。

   この ACL は、次に変更を展開するときに設定されます。別のポリシーでオブジェクトを使用して強制的に展開する必要はありません。

   （注） この ACL は IPv4 にのみ適用されます。IPv6 のサポートも追加したい場合は、属性がすべて同じ 2 つ目の ACE を追加します。ただし、送信元ネットワークと宛先ネットワークに any-ipv6 を選択します。ISE または DNS サーバーへのトラフィックはリダイレクトされないようにするために、他の ACE を追加することもできます。最初に、それらのサーバーの IP アドレスを保持するホスト ネットワーク オブジェクトを作成する必要があります。

ステップ 3 RADIUS サーバーグループをダイナミック認証用に設定します。

「FTD RADIUS サーバーオブジェクトまたはグループの作成または編集」セクションの説明に従って、以下の手順を実行します。

1. RADIUS サーバーオブジェクトの作成
2. RADIUS サーバーグループの作成

ステップ 4 この RADIUS サーバーグループを使用する接続プロファイルを作成します。「FTD RA VPN 接続プロファイルの設定」を参照してください。[AAA認証（AAA Authentication）] を使用し（単

独または証明書と一緒に）、[ユーザー認証用のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]、[認可（Authorization）]、および [アカウンティング（Accounting）] オプションでサーバー グループを選択します。

FTD のリモートアクセス VPN 設定の確認

リモートアクセス VPN を設定し、設定をデバイスに展開した後で、リモート接続できることを確認します。

手順

ステップ 1 外部ネットワークから、AnyConnect クライアントを使用して VPN 接続を確立します。Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。必要に応じて、クライアント ソフトウェアをインストールし、接続を完了します。「ユーザーが AnyConnect クライアントソフトウェアを FTD にインストールする方法」を参照してください。グループ URL を設定した場合は、それらの URL も試みてください。

ステップ 2 [デバイスとサービス（Devices & Services）]ページで、確認するデバイスを選択し、[デバイスアクション（Device Actions）] の下の [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 3 **show vpn-sessiondb** コマンドを使用して、現在の VPN セッションに関する概要情報を表示します。

ステップ 4 統計情報では、アクティブな AnyConnect クライアント セッション、および累積セッション数、ピーク同時セッション数、非アクティブ セッション数の情報が示されます。次は、コマンドからの出力例です。

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------------


   Total Active and Inactive    :      1             Total Cumulative :     50
   Device Total VPN Capacity    :  10000
   Device Load                  :     0%
   --------------------------------------------------------------------------------

   --------------------------------------------------------------------------------
   Tunnels Summary
   --------------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                              ----------------------------------------
   Clientless                 :      0 :          1 :               1
   AnyConnect-Parent          :      1 :         49 :               3
   SSL-Tunnel                 :      1 :         46 :               3
   DTLS-Tunnel                :      1 :         46 :               3
   --------------------------------------------------------------------------------
   Totals                     :      3 :        142
   --------------------------------------------------------------------------------

   --------------------------------------------------------------------------------
   IPv6 Usage Summary
   --------------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                              ----------------------------------------
   AnyConnect SSL/TLS/DTLS    :        :            :
     Tunneled IPv6            :      1 :         20 :           2
   --------------------------------------------------------------------------------
```

ステップ 5 **show vpn-sessiondb anyconnect** コマンドを使用して、現在の AnyConnect VPN セッションに関する詳細情報を表示します。詳細情報には、使用されている暗号化、送信バイト数と受信バイト数などの統計情報が含まれます。VPN接続を使用する場合、このコマンドを再発行すると送信バイト数と受信バイト数が変わるのがわかります。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

FTD のリモートアクセス VPN 設定の詳細表示

手順

ステップ 1 左側の CDO ナビゲーションバーで、**[VPN]** > **[リモートアクセスVPNの設定（Remote Access VPN Configuration）]**をクリックします。

ステップ 2 表示された VPN 設定オブジェクトをクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

- RA VPN 設定を展開して、それらに関連付けられているすべての接続プロファイルを表示します。
  - 追加 + ボタンをクリックして新しい接続プロファイルを追加します。
  - 表示ボタン（  ）をクリックして、接続プロファイルの概要と接続手順を開きます。[アクション（Actions）] で、[編集（Edit）] をクリックして変更を変更できます。
- [アクション（Actions）] で次のオプションのいずれかをクリックすると、追加のタスクを実行できます。
  - グループポリシーを割り当て/追加するには、[グループポリシー（Group Policies）] をクリックします。
  - 不要になった設定オブジェクトまたは接続プロファイルをクリックし、[削除（Remove）] をクリックして削除します。

テンプレート

テンプレートは、汎用のデバイス構成ファイルの開発手法を提供します。

- テンプレートは、既存の基本構成ファイルから作成されます。
- IP アドレスやポート番号など、予想される値を簡単にカスタマイズできる値パラメータをサポートしています。
- また、複数のデバイス間で使用するために、パラメータ置換を使用してエクスポートできます。

関連情報

- FTD テンプレート （362 ページ）
  - FTD テンプレートの設定 （363 ページ）

• FTD へのテンプレートの適用 （368 ページ）

FTD テンプレート

FTD テンプレートについて

CDO では、オンボード FTD デバイスの設定の FTD テンプレートを作成できます。テンプレートを作成するときに、FTD テンプレートに含めるパーツ（オブジェクト、ポリシー、設定、インターフェイス、および NAT）を選択します。その後、そのテンプレートを変更し、それを使用して管理する他の FTD デバイスを設定できます。FTD テンプレートは、FTD デバイス間のポリシーの一貫性を推進する方法です。

FTD テンプレートを作成する際、完全なテンプレートまたはカスタムテンプレートの作成を選択できます。

- 完全なテンプレートには、FTD 設定のすべてのパーツが含まれており、すべてを他の FTD デバイスに適用します。
- カスタムテンプレートには、選択した FTD 設定の 1 つ以上のパーツのみが含まれ、そのパーツと他の FTD デバイスに関連付けられたエンティティのみが適用されます。

重要 FTD テンプレートには、証明書、Radius、AD、および RA VPN オブジェクトは含まれません。

FTD テンプレートの使用方法

FTD テンプレートの使用方法をいくつか示します。

- 別の FTD の設定テンプレートを適用して、1 つの FTD を設定します。適用するテンプレートは、すべての FTD デバイスで使用する「ベストプラクティス」設定を表す場合があります。
- テンプレートをメソッドとして使用して、デバイス設定の変更を行い、それらの変更をライブ FTD デバイスに適用する前に、ラボ環境でシミュレートして機能をテストします。
- テンプレートを作成するときに、インターフェイスとサブインターフェイスの属性をパラメーター化します。テンプレートの適用時に、インターフェイスおよびサブインターフェイスのパラメータ化された値を変更できます。

変更ログに表示される内容

テンプレートをデバイスに適用すると、そのデバイスの設定全体が上書きされます。CDO 変更ログには、結果として加えられたすべての変更が記録されます。そのため、テンプレートをデバイスに適用した後の変更ログエントリは非常に長くなります。

関連情報：

- FTD テンプレートの設定

FTD テンプレートの設定

前提条件

FTD テンプレートを作成する前に、テンプレートを作成する FTD を CDO にオンボーディングします。オンボーディング済みの FTD デバイスからのみ FTD テンプレートを作成できます。

環境に追加される新しい FTD デバイスを設定するときに、テンプレートを使用することを**強く**お勧めします。

（注） FTD デバイスからテンプレートを作成すると、RA VPN オブジェクトはテンプレートに含められません。

FTD テンプレートの作成

テンプレートを作成する際にすべてのパーツを選択すると、テンプレートにはそのデバイス構成のすべての側面が組み込まれます。管理 IP アドレス、インターフェース構成、ポリシー情報などです。

一部のパーツを選択すると、カスタムテンプレートには次のエンティティが組み込まれます。

テンプレートパーツ	カスタムテンプレートに含まれるパーツ
アクセル ルール	アクセス制御ルールと、そのルールに関連するエンティティが組み込まれます。たとえば、オブジェクトとインターフェイス（サブインターフェイスを含む）です。
NAT ルール	NAT ルールと、その NAT ルールに必要な関連エンティティが組み込まれます。たとえば、オブジェクトとインターフェイス（サブインターフェイスを含む）です。
設定	システム設定と、その設定に必要な関連エンティティが組み込まれます。たとえば、オブジェクトとインターフェイス（サブインターフェイスを含む）です。
インターフェイス	インターフェイスとサブインターフェイスが組み込まれます。
オブジェクト	オブジェクトと、そのオブジェクトに必要な関連エンティティが組み込まれます。たとえば、インターフェイスとサブインターフェイスです。

FTD テンプレートを作成するには、次の手順を実行します。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、該当するデバイスをリストから選択します。

ステップ 4 フィルタや検索フィールドを使用して、テンプレートを作成する FTD を見つけます。

ステップ 5 右側の [デバイスアクション（Device Actions）] ペインで、[テンプレートの作成（Create Template）] をクリックします。[名前テンプレート（Name Template）] には、デバイス上の各パーツの数が表示されます。サブインターフェースがある場合は、その数も表示されます。

ステップ 6 テンプレートに含めるパーツを選択します。

ステップ 7 テンプレートに付ける名前を入力します。

ステップ 8 [テンプレートの作成（Create Template）] をクリックします。

ステップ 9 [テンプレートのパラメータ化（Parameterize Template）] 領域では、次のことを実行できます。

- インターフェイスをパラメータ化するには、そのインターフェイスに対応するセルにカーソルを合わせて（中括弧が表示されるまで）クリックします。
- サブインターフェースをパラメータ化するには、サブインターフェースがあるインターフェースを展開し、そのサブインターフェースに対応するセルにカーソルを合わせて（中括弧が表示されるまで）クリックします。

次の属性をパラメータ化すると、デバイスごとにカスタマイズできます。

- **論理名（Logical Name）**
- **状態**
- **IP Address/Netmask**

（注） これらの属性は、パラメータごとに 1 つの値のみをサポートします。

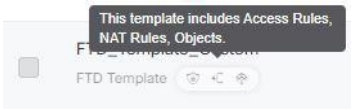
ステップ 10 [続行（Continue）] をクリックします。

ステップ 11 テンプレートとパラメーター化した値を確認します。[完了（Done）] をクリックしてテンプレートを作成します。

[デバイスとサービス（Devices & Services）] ページに、作成した FTD テンプレートが表示されます。

（注） テンプレートの作成後、[デバイスとサービス（Devices & Services）] ペインには対応するテンプレートパーツアイコンが表示され、テンプレートに含まれるパーツが示されます。デバイスをクリックするか、アイコンにマウスポインタを合わせると、[デバイスの詳細（Device Details）] ペインにもこの情報が表示されます。

次の図は、テンプレートに「アクセスルール」、「NAT ルール」、「オブジェクト」が含まれていることを示すパーツアイコンの例を示しています。



FTD テンプレートの編集

次の手順でテンプレートパラメータを編集します。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [テンプレート（Templates）] タブをクリックします。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 モデルまたはテンプレートフィルタを使用して、変更するテンプレートを見つけます。

ステップ 5 右側の [デバイスアクション（Device Actions）] ペインで、[パラメータの編集（Edit Parameters）] をクリックします。

ステップ 6 （任意）テキストボックスを直接編集して、パラメータを変更します。

ステップ 7 [保存（Save）] をクリックします。

ライブ FTD デバイスを設定する場合と同様に、FTD テンプレートの残りの部分を編集できます。FTD テンプレートを編集する際、次の設定に関する説明に従ってください。

- FTD の設定
- バーチャル プライベートネット ワークの管理
- FTD RA VPN 設定の作成
- FTD ポリシーの設定
- ポリシーと構成の一貫性を促進する

FTD テンプレートの削除

FTD の削除は、CDO から FTD デバイスを削除する場合と同じです。

手順

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [テンプレート（Templates）] タブをクリックします。
ステップ 3 [FTD] タブをクリックします。
ステップ 4 フィルタと検索フィールドを使用して、削除する FTD テンプレートを見つけます。
ステップ 5 [デバイスアクション（Device Actions）] ペインで、[削除（Remove）] をクリックします。
ステップ 6 警告メッセージの内容を確認し、[OK] をクリックします。

関連情報：

- FTD テンプレート
- FTD テンプレートの適用

FTD テンプレートの適用

テンプレートを適用する前に、[デバイスとサービス（Devices & Services）] ページに移動し、[モデル/テンプレート（Model/Template）] でフィルタ処理すると、テンプレートの内容を確認できます。CDO には対応するテンプレートパーツアイコンが表示されるため、そのテンプレートに含まれるパーツが分かります。デバイスをクリックするか、アイコンにマウスポインタを合わせると、[デバイスの詳細（Device Details）] ペインにもこの情報が表示されます。

次の属性をパラメータ化すると、デバイスごとのカスタマイズが可能です。つまり、テンプレートの適用時にデバイス固有の値を適用できます。

FTDテンプレートを作成して適用する際に、インターフェイスおよびサブインターフェイスのパラメータ化した値を変更できます。

完成したテンプレートの適用

完成した FTD テンプレートを適用して新しい FTD を作成すると、FTD の既存の設定がすべて上書きされます。CDO からデバイスへの展開が完了していないステージング中の変更も含まれます。デバイス上でテンプレートに含まれていない設定はすべて失われます。

カスタムテンプレートの適用

カスタム FTD テンプレートを他の FTD に適用すると、テンプレートパーツに基づいて既存の設定が保持または削除されます。次の表に、他の FTD デバイスにカスタムテンプレートを適用した後に発生する変更を示します。

テンプレートパーツ	カスタムテンプレートの適用後
アクセル ルール	• カスタムテンプレート内の新しいアクセス制御ルールは、デバイス上の既存のアクセス制御ルールを上書きします。 • カスタムテンプレート内に新しいオブジェクトやインターフェイス（サブインターフェイスを含む）がある場合は、既存のオブジェクトやインターフェイスを削除せずにデバイスに適用されます。

テンプレートパーツ	カスタムテンプレートの適用後
NAT ルール	• デバイス上の既存の NAT ルールは、カスタムテンプレート内の新しい NAT ルールを上書きします。 • カスタムテンプレート内に新しいオブジェクトやインターフェイス（サブインターフェイスを含む）がある場合は、既存のオブジェクトやインターフェイスを削除せずにデバイスに適用されます。
設定	• カスタムテンプレートの新しいシステム設定は、既存のシステム設定を削除せずにデバイスに適用されます。 • カスタムテンプレート内に新しいオブジェクトやインターフェイス（サブインターフェイスを含む）がある場合は、既存のオブジェクトやインターフェイスを削除せずにデバイスに適用されます。
インターフェイス	• カスタムテンプレートの新しいインターフェイスとサブインターフェイスは、既存のインターフェイスとサブインターフェイスを削除せずにデバイスに適用されます。
オブジェクト	• カスタムテンプレートの新しいオブジェクトは、既存のオブジェクトを削除せずにデバイスに適用されます。 • カスタムテンプレート内に新しいインターフェイスやサブインターフェイスがある場合は、既存のインターフェイスとサブインターフェイスを削除せずにデバイスに適用されます。

前提条件

テンプレートを適用する前に、次の条件を満たす必要があります。

- テンプレートを使用する際、テンプレートへの変更がすべてコミットされていること、およびテンプレートが [デバイスとサービス（Devices & Services）] ページで [同期（Synced）] 状態になっていることを確認してください。
- FTD デバイスをテンプレートとして使用する場合は、デバイスへの展開対象となる CDO の変更が展開されていること、および展開されていない FDM コンソールからの変更がないことを確認してください。デバイスは、[デバイスとサービス（Devices & Services）] ページで同期状態を示している必要があります。

テンプレートをデバイスに適用するには、3 段階のプロセスがあります。

1. 完成したテンプレートの適用
2. デバイスとネットワークの設定を確認する
3. 変更のデバイスへの展開

FTD へのテンプレートの適用

重要 変更をデバイスに展開する前に、次の手順に進みます。

デバイスとネットワークの設定を確認する

テンプレートを適用する前に、変更リクエストのトラッキング機能を使用して、変更にトラッキングラベルを適用できます。FTD テンプレートを適用するには、次の手順を実行します。

手順

ステップ 1 （任意）始める前に、FTDデバイスのテンプレートを作成してから、別のテンプレートをそれに適用します。これにより、デバイスやネットワーク設定の再適用が必要になったときに、参照可能な設定のバックアップが提供されます。

ステップ 2 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

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 [FTD] タブをクリックします。

ステップ 5 フィルタと検索フィールドを使用して、テンプレートを適用する FTD デバイスまたはテンプレートを見つけます。

（注） この時点でテンプレート名を変更すると、完全なデバイス設定またはテンプレートを *DeviceName* に適用することになります。この変更を *DeviceName* に展開すると、そのデバイスで実行されている設定全体が上書きされます。

ステップ 6 右側の [デバイスアクション（Device Actions）] ペインで、[テンプレートの適用（Apply Template）] をクリックします。

ステップ 7 [テンプレートの選択（Select Template）] をクリックし、目的のテンプレートを選択して [続行（Continue）] をクリックします。

ステップ 8 以下の設定を行い、各画面に表示される [続行（Continue）] をクリックします。

1. [マップインターフェイス（Map Interface）]：テンプレートとデバイス間のインターフェースのマッピングを確認または変更します。 1 つのデバイスインターフェイスに複数のテンプレートインターフェイスをマッピングできないことに注意してください。インターフェイス設定がサポートされていない場合、続行してテンプレートを適用できません。
2. [パラメーターの入力（Fill Parameters）]：テンプレートを適用するデバイスのインターフェースまたはサブインターフェースのパラメータ値をカスタマイズします。
3. [レビュー（Review）]：テンプレートの設定を確認し、既存のデバイス設定をテンプレートの設定で上書きする準備ができたら、[テンプレートの適用（Apply Template）] をクリックします。

ステップ 9 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開するか、後から複数の変更を一度に展開します。

デバイスとネットワークの設定を確認する

FTD テンプレートを作成する際、CDO はデバイス構成全体をテンプレートにコピーします。そのため、元のデバイスの管理 IP アドレスなどがテンプレートに含まれています。テンプレートをデバイスに適用する前に、デバイスとネットワークの設定を確認してください。

手順

ステップ 1 以下の FTD デバイス設定を確認して、それらが新しい FTD デバイスの正確な情報を反映していることを確認します。

- FTD の設定
- 管理インターフェイス
- ホスト名（Hostname）

ステップ 2 FTD アクセス コントロール ポリシーの設定を確認して、ルールが必要に応じて新しい FTD の IP アドレスを参照していることを確認します。

ステップ 3 inside_zone および outside_zone のセキュリティオブジェクトを確認して、それらが新しい FTD の正確な IP アドレスを参照していることを確認します。

ステップ 4 NAT ポリシーを確認して、それらが新しい FTD の正確な IP アドレスを参照していることを確認します。

ステップ 5 インターフェイスの構成を確認して、それらが新しい FTD の正確な構成を反映していることを確認します。

変更のデバイスへの展開

行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

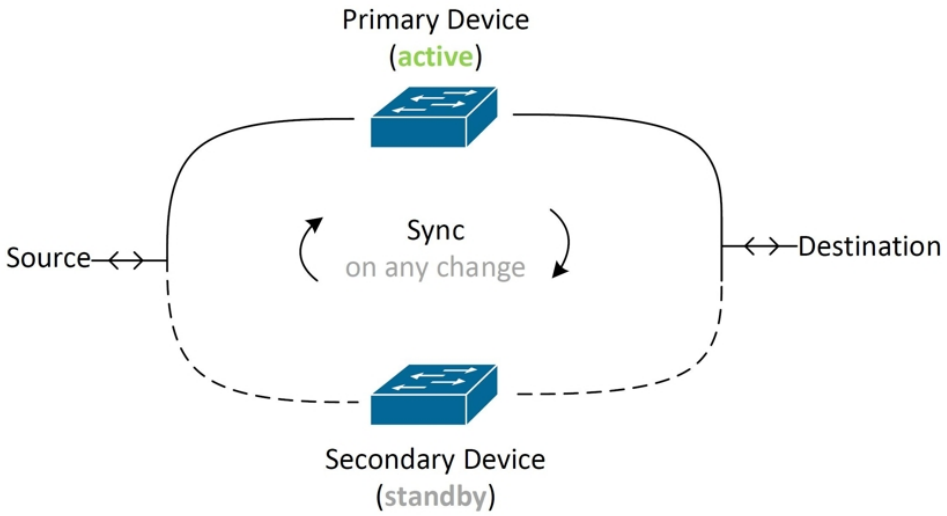
関連情報：

- FTD テンプレート
- FTD テンプレートの設定

FTD の高可用性

ハイ アベイラビリティについて

高可用性（HA）やフェールオーバー設定では、プライマリデバイスの障害時にセカンダリデバイスで引き継ぐことができるように、2つのデバイスをプライマリ/セカンダリ設定に結び付けます。フェールオーバーとも呼ばれる高可用性を設定するには、専用フェールオーバーリンク（および任意でステートリンク）を介して相互に接続された 2 つの同じ FTD デバイスが必要です。アクティブ装置（ハードウェア、インターフェイス、ソフトウェアおよび環境ステータス）の状態は、特定のフェールオーバー条件に一致しているかどうかを確認するためにモニターされます。所定の条件に一致すると、フェールオーバーが行われます。これにより、デバイスに障害が発生した場合や、デバイスがアップグレードされているメンテナンス期間中に、ネットワークの運用を維持できます。詳しくは下の関連記事をご覧ください。



この装置はアクティブ/スタンバイペアを形成します。プライマリ装置がアクティブな装置となり、トラフィックを送信します。セカンダリ（スタンバイ）装置はアクティブにトラフィックを送信しませんが、アクティブ装置の設定やその他のステータス情報を同期します。2 台の装置はフェールオーバーリンク経由で通信して、各装置の動作ステータスを確認しています。

（注） FTD HA ペアからの変更を受け入れるか FTD HA ペアに変更を展開することを選択すると、HA ペアのアクティブデバイスと通信することになります。これは、設定とバックアップがアクティブデバイスからのみ取得されることを意味します。

高可用性ペアの証明書

HA FTD ペアに証明書を適用すると、CDO ではアクティブデバイスにのみ証明書が適用されます。つまり、アクティブデバイスの展開時にのみ、設定と証明書がスタンバイデバイスと同期されます。FDM を介してアクティブデバイスに新しい証明書を適用すると、アクティブデバイスとスタンバイデバイスには、2つの異なる証明書が存在する場合があります。これにより、フェイルオーバーやフェイルオーバー履歴などで問題が発生する可能性があります。2 つのデ

バイスが正常に機能するには、同じ証明書が必要です。FDM を介して証明書を変更する必要がある場合は、変更を展開して HA ペア内で証明書を同期する必要があります。

関連情報：

- FTD 高可用性のフェールオーバーとステートフルリンク
- FTD ハイアベイラビリティペアの要件
- FTD ハイアベイラビリティペアの作成
- バージョン 6.4 またはバージョン 6.5 を実行する FTD HA ペアのオンボーディング
- バージョン 6.6 またはバージョン 6.7 以降を実行する FTD HA ペアのオンボーディング
- FTD 高可用性ページ
- FTD 高可用性ペアリングの解除
- FTD の高可用性フェールオーバーの履歴
- FTD の高可用性ステータスの更新
- FTD ハイアベイラビリティペアでフェールオーバーを強制する
- FTD 高可用性ペアのアップグレード
- 変更の読み取り、破棄、チェック、および展開
- FTD から CDO への設定変更の読み取り
- CDO から FTD への設定変更の展開

FTD ハイアベイラビリティペアの要件

ハイ アベイラビリティ要件

高可用性（HA）ペアを作成する前に、いくつかの要件を満たす必要があります。

HA の物理デバイスおよび仮想デバイスの要件

次のハードウェア要件を満たしている必要があります。

- デバイスは、同じハードウェアモデルである必要があります。
- デバイスには同じモジュールが取り付けられている必要があります。たとえば、一方にオプションのネットワークモジュールがある場合は、もう一方のデバイスにも同じネットワークモジュールを取り付ける必要があります。
- デバイスは、同じタイプの同じ数のインターフェイスを備えている必要があります。
- CDO で HA ペアを作成するには、両方のデバイスで管理インターフェイスが設定されている必要があります。デバイスにデータインターフェイスが設定されている場合は、FDM

UI を使用して HA ペアを作成してから、そのペアを CDO にオンボードする必要があります。

（注） HA ペアで FTD テンプレートを使用することは**できません**。

HA のソフトウェア要件

物理 FTD と仮想 FTD の両方で、次のソフトウェア要件を満たす必要があります。

- Defense Orchestrator には 2 つのスタンドアロン FTD デバイスがオンボードされています。
- デバイスは、まったく同じバージョンのソフトウェア（つまり、1 番目のメジャー番号、2 番目のマイナー番号、および 3 番目のメンテナンス番号が同じ）を実行する必要があります。バージョンは、[インベントリ（Inventory）] ページの [デバイスの詳細（Device Details）] ウィンドウで確認できます。また、CLI で show version コマンドを使用して確認することもできます。

（注） 異なるバージョンを実行するデバイスでも参加できますが、設定がスタンバイ装置にインポートされず、装置を同じソフトウェアバージョンにアップグレードしないとフェールオーバーは機能しません。

- 両方のデバイスがローカルマネージャモードになっている必要があります。つまり、FDM を使用して設定されている必要があります。両方のデバイスで FDM にログインできる場合は、それらがローカルマネージャモードになっています。CLI で show managers コマンドを使用して確認することもできます。
- CDO にオンボードする前に、各デバイスの初期セットアップウィザードを完了する必要があります。
- 各デバイスに固有の管理 IP アドレスが必要です。管理インターフェイスの設定は、デバイス間で同期されません。
- デバイスの NTP 設定が同じである必要があります。
- DHCP を使用してアドレスを取得するようにインターフェイスを設定することはできません。つまり、すべてのインターフェイスに静的 IP アドレスが必要です。

  注：インターフェイスの設定を変更する場合は、HA を確立する前に、その変更をデバイスに展開する必要があります。
- 両方のデバイスを**同期**させる必要があります。保留中の変更や競合が検出された場合は、「設定の競合の解決」を参照してください。「設定の競合の解決」に詳細が記載されています。

（注） FTD HA ペアからの変更を受け入れるか FTD HA ペアに変更を展開すると、HA ペアのアクティブデバイスと通信することになります。これは、設定とバックアップがアクティブデバイスからのみ取得されることを意味します。

HA のスマートライセンス要件

物理 FTD と仮想 FTD の両方で、次のライセンス要件を満たす必要があります。

- HA ペアの両方のデバイスに、登録済みライセンスまたは評価ライセンスが必要です。デバイスが登録されている場合は、それらを異なる Cisco Smart Software Manager アカウントに登録できますが、それらのアカウントは、エクスポート制御機能設定が同じ状態（両方有効または両方無効）である必要があります。ただし、デバイスごとに異なるオプションライセンスを有効にすることは可能です。
- HA ペア内の両方のデバイスでは、運用時に同じライセンスが必要です。ライセンスが不足している場合、一方のデバイスではコンプライアンスが適用され、もう一方のデバイスではコンプライアンス適用外になる可能性があります。スマート ライセンス アカウントに購入済みの十分な権限付与が含まれていない場合は、正しい数のライセンスが購入されるまで、アカウントがコンプライアンス適用外（一方のデバイスにコンプライアンスが適用されていても）になります。

なお、デバイスが評価モードの場合は、デバイスでの Cisco Defense Orchestrator の登録ステータスが同じであることを確認する必要があります。また、Cisco Success Network への参加の選択が同じであることも確認する必要があります。登録されたデバイスについては、装置ごとに異なる設定が可能ですが、プライマリ（アクティブ）デバイスで設定すると、セカンダリデバイスが登録または登録解除されます。プライマリ デバイスでの Cisco Success Network への参加の同意は、セカンダリ デバイスでの同意を意味します。

輸出規制対象の機能の設定が異なるアカウントにデバイスを登録した場合、または 1 つの装置が登録済みで、もう 1 つが評価モードにある HA ペアを作成しようすると、HA の参加が失敗する可能性があります。輸出規制機能に関する設定が不整合な状態で IPsec 暗号化鍵を設定すると、HA を有効化した後に両方のデバイスがアクティブになります。これはサポートされているネットワーク セグメント上のルーティングに影響を与え、回復させるにはセカンダリ装置で HA を手動で中断する必要があります。

HA のクラウドサービス設定

HA ペア内の両方のデバイスで、[Cisco Cloudにイベントを送信（Send Events to the Cisco Cloud）] が有効になっている必要があります。この機能は、FDM UI で使用できます。この機能を有効にするには、[システム設定（System Settings）]に移動し、[クラウドサービス（Cloud Services）] をクリックします。このオプションを有効にしないと、CDO で HA ペアを形成できず、イベント説明エラーが発生します。詳細については、実行しているバージョンの Firepower Device Manager 設定ガイド [英語] の「Configuring Cloud Services」の章を参照してください。

https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html

関連情報：

- バージョン 6.6 またはバージョン 6.7 以降を実行する FTD HA ペアのオンボーディング
- バージョン 6.4 またはバージョン 6.5 を実行する FTD HA ペアのオンボーディング
- ユーザー名、パスワード、IP アドレスを使用した FTD HA ペアの導入準備

FTD ハイアベイラビリティペアの作成

Defense Orchestrator で FTD HA ペアを作成する前に、「FTD ハイアベイラビリティペアの要件」で説明されている要件を満たす2つのスタンドアロンFTDデバイスを最初にオンボーディングする必要があります。

（注） CDO で HA ペアを作成するには、両方のデバイスで管理インターフェイスが設定されている必要があります。デバイスにデータインターフェイスが設定されている場合は、FDM コンソールを使用して HA ペアを作成してから、そのペアを CDO にオンボーディングする必要があります。

FTD HA ペアを作成すると、デフォルトでプライマリ デバイスが**アクティブ**になり、セカンダリデバイスが**スタンバイ**になります。すべての設定変更または展開はプライマリデバイスを介して行われ、セカンダリデバイスは、プライマリユニットが使用できなくなるまでスタンバイモードが維持されます。

設定変更の FTD HA ペアからの受け入れ、または FTD HA ペアへの展開を選択すると、HA ペアのアクティブデバイスと通信することなります。プライマリデバイスに加えられた変更は、プライマリデバイスとセカンダリデバイス間のリンクを介して転送されます。CDO は、プライマリ デバイスにのみを対象に変更の展開と受け入れを行います。したがって、[インベントリ（Inventory）] ページには、ペアの単一のエントリが表示されます。展開が行われると、プライマリデバイスは設定変更をセカンダリデバイスに同期します。

FTD HA ペアのバックアップをスケジュールまたは選択する場合も、同様にCDOがアクティブデバイスのみと通信するため、アクティブデバイスのみがバックアップの対象となります。

（注） 作成プロセス中に HA デバイスで問題が発生した場合、または HA ペアが正常なステータスにならない場合は、ペアを再度作成する前に、HA 構成を手動で解除する必要があります。

手順

次の手順で、2 つのスタンドアロン FTD デバイスから HA ペアを作成します。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、プライマリデバイスとして設定するデバイスを選択します。

（注） CDO では、DHCP で設定されたデバイスと HA ペアを作成できません。

ステップ 4 [管理（Management）] ペインで、[高可用性（High Availability）] をクリックします。

ステップ 5 セカンダリデバイスの領域で [デバイスの選択（Select Device）] をクリックし、デバイス候補リストからデバイスを選択します。

ステップ 6 フェールオーバーリンクを設定します。

1. [物理インターフェイス（Physical Interface）] をクリックし、ドロップダウンメニューからインターフェイスを選択します。
2. 該当する **IP タイプ**を選択します。
3. **プライマリ IP** アドレスを入力します。
4. **セカンダリ IP** アドレスを入力します。
5. **ネットマスク**を入力します。デフォルト値は 24 です。
6. 該当する場合は、有効な **IPSec 暗号化キー**を入力します。

ステップ 7 ステートフルリンクを設定します。フェールオーバーリンクと同じ設定を使用する場合は、[フェールオーバーリンクと同じ（The same as Failover Link）] チェックボックスをオンにします。別の設定を使用する場合は、次の手順を実行します。

1. [物理インターフェイス（Physical Interface）] をクリックし、ドロップダウンメニューからインターフェイスを選択します。プライマリデバイスとセカンダリデバイスの両方で、同じ数の物理インターフェイスが**必要でです**。
2. 該当する **IP タイプ**を選択します。
3. **プライマリ IP** アドレスを入力します。
4. **セカンダリ IP** アドレスを入力します。
5. **ネットマスク**を入力します。デフォルト値は 24 です。

ステップ 8 画面の右上隅にある [作成（Create）] をクリックして、ウィザードを終了します。すぐに [高可用性ステータス（High Availability Status）] ページにリダイレクトされます。このページから、HA 作成のステータスをモニターリングできます。HA ペアが作成されると、[インベントリ（Inventory）] ページにはペアが 1 行で表示されることに注意してください。

ステップ 9 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

FTD 高可用性ページ

FTD 高可用性（HA）管理ページは、FTD デバイス用の多目的ページです。このページは、HA ペアとして設定済みのデバイスでのみ使用できます。FTD HA ペアをオンボードするか、2 つのスタンドアロン FTD デバイで FTD HA ペアを作成できます。

[インベントリ（Inventory）] ページでスタンドアロン FTD を選択した場合、このページは HA ペアを作成するためのウィザードとして機能します。現時点では、ペアを作成するには、2 つの FTD デバイスを CDO にオンボードする必要があります。CDO で FTD HA ペアを作成する方法については、「FTD ハイアベイラビリティペアの作成」を参照してください。

すでに設定されている FTD HA ペアをオンボードする際には、ログイン情報を使用することを推奨します。詳細については、ユーザー名、パスワード、IP アドレスを使用した FTD HA ペアの導入準備を参照してください。登録キーを使用して別の方法で HA ペアをオンボードする必要がある場合は、登録キーを使用した FTD HA ペアの導入準備 を参照してください。

[インベントリ（Inventory）] ページで FTD HA ペアを選択した場合、このページは概要ページとして機能します。このページでは、HA 構成とフェールオーバー履歴に加えて、フェールオーバーの強制実行、フェイルオーバー基準の編集、HA リンクの削除などの実行可能な操作を表示できます。

高可用性の管理ページ

[高可用性（High Availability）] ページを表示するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックし、スタンドアロン FTD デバイス**または** FTD HA ペアのアクティブデバイスを選択します。

ステップ 4 [管理（Management）] ペインで、[高可用性（High Availability）] をクリックします。

関連情報：

- FTD の高可用性フェールオーバーの履歴
- ハイ アベイラビリティ フェールオーバー基準の編集
- FTD ハイアベイラビリティペアでフェールオーバーを強制する
- FTD 高可用性ペアリングの解除

- FTD の高可用性ステータスの更新

ハイ アベイラビリティ フェールオーバー基準の編集

FTD HA ペアの作成後にフェールオーバー基準を編集できます。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。
ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。
ステップ 3 [FTD] タブをクリックし、FTD HA ペアのアクティブデバイスを選択します。
ステップ 4 [管理（Management）] ペインで、[高可用性（High Availability）] をクリックします。
ステップ 5 [フェールオーバー基準（Failover Criteria）] ウィンドウで、[編集（Edit）] をクリックします。
ステップ 6 必要な変更を行って、[保存（Save）] をクリックします。
ステップ 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、複数の変更を後から一度に展開します。

FTD 高可用性ペアリングの解除

HA を解除すると、スタンバイデバイスで設定されたインターフェイスが自動的に無効になります。このプロセス中に、デバイスのトラフィックが中断する場合があります。HA ペアが正常に削除されると、ステータスページから [高可用性（High Availability）] ページにリダイレクトされ、同じプライマリデバイスで別の HA ペアを作成するオプションが表示されます。

（注） HA ペアが正常に削除されるまで、いずれのデバイスにも展開できません。

管理インターフェイスを使用した HA の解除

管理インターフェイスを使用して設定されているペアの HA を解除すると、解除完了まで 10 分以上かかる場合があり、両方のデバイスはこのプロセス中オフラインになります。HA 設定が正常に削除されると、CDO は両方のユニットをスタンドアロンデバイスとして [サービスとデバイス（Services & Devices）] ページに表示します。

データインターフェイスを使用した HA の解除

データインターフェイスを使用して設定されているペアの HA を解除すると、解除完了まで 20 分以上かかる場合があり、両方のデバイスがオフラインになります。 HA 設定を削除後、アクティブデバイスを手動で再接続する必要があります。

ただし、スタンバイデバイスではHA設定が保持され、アクティブデバイスと同じ設定であるため、到達不能になります。CDO の外部で IP インターフェイスを手動で再設定してから、デバイスをスタンドアロンとして再度オンボードする必要があります。

高可用性の解除

2 つの FTD デバイスの HA ペアリングを削除するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションバーで [インベントリ（Inventory）] をクリックし、FTD HA ペアのアクティブデバイスを選択します。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 [管理（Management）] ペインで、[高可用性（High Availability）] をクリックします。

ステップ 5 [ハイ アベイラビリティを無効にする（Break High Availability）] をクリックします。

ステップ 6 CDO で HA の設定が削除され、両方のデバイスが [インベントリ（Inventory）] ページにスタンドアロンデバイスとして表示されます。

ステップ 7 「CDO から FTD への設定変更の展開」を参照して、両方のデバイスに新しい設定を展開します。

ステップ 8 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、複数の変更を後から一度に展開します。

アウトオブバンド高可用性の解除

FDM インターフェイスを使用して FTD の HA ペアを解除すると、CDO で HA ペアの設定ステータスが [競合検出（Conflict Detected）] に変わります。 HA を解除した後、FDM を介してプライマリデバイスに変更を展開してから、設定の競合の解決する必要があります。

デバイスが同期状態に戻ったら、CDO で行った設定変更をデバイスに展開できます。

FDM インターフェイスを使用して HA を解除した後、CDO で行った変更を元に戻すことは**推奨しません**。

関連情報：

- FTD の高可用性フェールオーバーの履歴
- FTD の高可用性ステータスの更新
- FTD ハイアベイラビリティペアでフェールオーバーを強制する
- 変更の読み取り、破棄、チェック、および展開

FTD ハイアベイラビリティペアでフェールオーバーを強制する

フェールオーバーを強制することで、FTD HA ペア内のアクティブデバイスとスタンバイデバイスを切り替えます。最近新しい証明書をアクティブデバイスに適用し、変更を展開**していない**場合、スタンバイデバイスは元の証明書を保持し、フェールオーバーは失敗することに注意してください。アクティブデバイスとスタンバイデバイスには、同じ証明書が適用されている必要があります。次の手順を使用して、フェールオーバーを手動で強制します。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。
ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。
ステップ 3 [FTD] タブをクリックします。
ステップ 4 FTD HA ペアのアクティブデバイスを選択します。
ステップ 5 [管理（Management）] ペインで、[高可用性（High Availability）] をクリックします。
ステップ 6 [オプション（options）] アイコン をクリックします。
ステップ 7 [モードの切り替え（Switch Mode）] をクリックします。アクティブデバイスがスタンバイになり、スタンバイデバイスがアクティブになります。

関連情報：

- FTD 高可用性ペアリングの解除
- FTD の高可用性フェールオーバーの履歴
- FTD の高可用性ステータスの更新
- FTD ハイアベイラビリティペアでフェールオーバーを強制する

FTD の高可用性フェールオーバーの履歴

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。
ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。
ステップ 3 [FTD] タブをクリックします。
ステップ 4 FTD HA ペアのアクティブデバイスを選択します。
ステップ 5 [管理（Management）] ペインで、[高可用性（High Availability）] をクリックします。
ステップ 6 [フェールオーバー履歴（Failover History）] をクリックします。CDO は、HA ペアが形成されてからのプライマリデバイスとセカンダリデバイス両方のフェールオーバー履歴に関する詳細を示すウィンドウを生成します。

（注） フェールオーバー履歴は、[インベントリ（Inventory）] ページから利用できるペアの変更ログにも表示されます。

関連情報：

- FTD 高可用性ペアリングの解除
- FTD の高可用性フェールオーバーの履歴
- FTD の高可用性ステータスの更新
- FTD ハイアベイラビリティペアでフェールオーバーを強制する

FTD の高可用性ステータスの更新

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。
ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。
ステップ 3 [FTD] タブをクリックし、FTD デバイスまたは FTD HA ペアを選択します。
ステップ 4 [管理（Management）] ペインで、[高可用性（High Availability）] をクリックします。
ステップ 5 [オプション（options）] アイコン をクリックします。
ステップ 6 [最新のステータスを取得（Get Latest Status）] をクリックします。CDO は、プライマリデバイスにヘルスステータスを要求します。

関連情報：

- FTD 高可用性ペアリングの解除
- FTD の高可用性フェールオーバーの履歴
- FTD の高可用性ステータスの更新
- FTD ハイアベイラビリティペアでフェールオーバーを強制する

FTD 高可用性のフェールオーバーとステートフルリンク

フェールオーバーリンクと（任意の）ステートフルリンク

フェールオーバー リンクは 2 つの装置の間の専用接続です。ステートフル フェールオーバー リンクも専用接続ですが、1 つのフェールオーバー リンクをフェールオーバー リンクとステート リンクが組み合わされたものとして使用することも、個別の専用ステート リンクを作成することもできます。フェールオーバー リンクだけを使用する場合は、ステートフルな情報もそのリンクを経由し、ステートフル フェールオーバー機能は失われません。デフォルトでは、

フェールオーバー リンクおよびステートフル フェールオーバー リンク上の通信はプレーン テキスト（暗号化されない）です。IPsec 暗号キーを設定することにより、通信を暗号化してセキュリティを強化できます。

未使用のデータ物理インターフェイスは、フェールオーバーリンクやオプションの専用ステートリンクとして使用できます。ただし、現在名前が設定されているインターフェイスやサブインターフェイスを持つインターフェイスは選択できません。フェールオーバーおよびステートフル フェールオーバー リンク インターフェイスは、通常のネットワーキング インターフェイスとして設定されません。フェールオーバー通信用にのみ存在し、通過トラフィックや管理アクセスに使用することはできません。設定がデバイス間で同期されるため、リンクの両端に同じポート番号を選択する必要があります。たとえば、フェールオーバー リンクの場合は両方のデバイスで GigabitEthernet 1/3 を使用します。

（注） FTDは、ユーザーデータとフェールオーバーリンク間でのインターフェイスの共有をサポートしていません。

フェールオーバー リンク

フェールオーバーペアの2台の装置は、フェールオーバーリンク経由で常に通信して、各装置の動作ステータスを確認し、設定の変更を同期します。次の情報がリンク上で共有されます。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

使用されていないデータインターフェイス（物理、冗長、または EtherChannel）はどれでも、フェールオーバーリンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。サブインターフェイスをフェールオーバーリンクとして使用**しないでください**。

フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステート リンク用としても使用できます）。

ステートフルリンク

アクティブ装置は、ステートリンクを使用して接続状態の情報をスタンバイデバイスに渡します。これは、スタンバイ装置がユーザーに影響を与えずに特定のタイプの接続を維持できることを意味します。この情報は、フェールオーバーが発生したときにスタンバイ装置が既存の接続を維持するために役立ちます。

ステートリンク専用のデータインターフェイス（物理、冗長、またはEtherChannel）を使用できます。ステートリンクとして使用されるEtherChannelの場合は、順序が不正なパケットを防止するために、EtherChannel内の1つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel内の次のリンクが使用されます。

フェールオーバーリンクとステートフル フェールオーバー リンクの両方に単一のリンクを使用することは、インターフェイスを節約する最善の方法です。ただし、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステート リンクとフェールオーバーリンク専用のインターフェイスを検討する必要があります。ステートフル フェールオーバーリンクの帯域幅は、デバイス上のデータインターフェイスの最大帯域幅と一致させることを推奨します。

FTD の設定

FTD デバイスのシステム設定の設定

単一の FTD デバイスで設定を行うには、次の手順を使用します。

手順

ステップ 1 [デバイスとサービス（Devices & Services）] ページを開きます。
ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。
ステップ 3 [FTD] タブをクリックし、設定を行うデバイスを選択します。
ステップ 4 右側の [管理（Management）] ペインで、[設定（Settings）] をクリックします。
ステップ 5 [システム設定（System Settings）] タブをクリックします。
ステップ 6 次のデバイス設定のいずれかを編集します。

- 管理アクセスの設定
- ロギング設定の設定
- DHCP サーバーの設定
- DNS サーバの設定
- ホスト名（Hostname）
- NTP サーバの設定
- URL フィルタリングの設定
- クラウド サービス（Cloud Services）
- Web 分析の有効化と無効化

管理アクセスの設定

デフォルトでは、任意の IP アドレスから、デバイスの管理アドレスにアクセスできます。システムアクセスは、ユーザー名とパスワードのみによって保護されます。ただし、特定の IP アドレスまたはサブネットのみからの接続を許可するようアクセスリストを設定し、さらにレベルの高い保護を提供できます。

また、データインターフェイスを開いて、FDM または SSH による CLI 接続を許可することもできます。これにより、管理アドレスを使用せずにデバイスを管理できます。たとえば、外部インターフェイスへの管理アクセスを許可し、デバイスをリモートで設定できます。ユーザー名とパスワードは、望ましくない接続を阻止します。デフォルトでは、データインターフェイスへの HTTPS 管理アクセスは内部インターフェイスで有効になっていますが、外部インターフェイスでは無効になっています。デフォルトの「内部」ブリッジグループを持つデバイスモデルの場合、ブリッジグループ内の任意のデータインターフェイスを介して、ブリッジグループ IP アドレス（デフォルトは 192.168.1.1）への FDM 接続が可能になります。管理接続は、デバイスに入るインターフェイス上でのみ開くことができます。

注意 特定のアドレスへのアクセスを制限すると、システムから簡単にロックアウトできます。現在使用している IP アドレスのアクセスを削除し、「任意」のアドレスのエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。アクセスリストを設定するときは、このことに注意してください。

管理インターフェイスのルールの作成

管理インターフェースのルールを作成するには、次の手順を実行します。

手順

ステップ 1 [管理インターフェイス（Management Interface）] セクションで [新規アクセス（New Access）] をクリックします。

- [Protocol]： ルールが HTTPS（ポート 443）または SSH（ポート 22）用かを選択します。
- [許可ネットワーク（Allowed Networks）]：システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワークオブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4]（0.0.0.0/0）および [any-ipv6]（::/0）を選択します。

ステップ 2 [保存（Save）] をクリックします。

データインターフェイスのルールの作成

データインターフェイスのルールを作成するには、次の手順を実行します。

手順

ステップ 1 [データインターフェイス（Data Interface）] セクションで [新規アクセス（New Access）] をクリックします。

- [インターフェイス（Interface）]。管理アクセスを許可するインターフェイスを選択します。
- [Protocol]：ルールが HTTPS（ポート 443）または SSH（ポート 22）、またはその両方用かを選択します。外部インターフェイスがリモートアクセス VPN 接続プロファイルで使用されている場合、その外部インターフェイスに HTTPS ルールを設定することはできません。
- [許可ネットワーク（Allowed Networks）]：システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワークオブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4] (0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

ステップ 2 [保存（Save）] をクリックします。

ステップ 3 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ロギング設定の設定

この手順では、診断（データ）メッセージ、ファイルイベントとマルウェアイベント、侵入イベント、およびコンソールイベントのログを有効にする方法について説明します。これらの設定の結果として、接続イベントはログに記録されません。アクセスルール、セキュリティインテリジェンス ポリシー、または SSL 復号化ルールで接続ログが構成されている場合、接続イベントがログに記録されます。

手順

ステップ 1 FTD デバイスのシステム設定の設定。

ステップ 2 [システム設定（System Settings）] ページで、設定メニューの [ロギング（Logging）] をクリックします。

ステップ 3 [データロギング（Data logging）] [データロギング（Data logging）] スライダを 「オン」にスライドして、診断ログの syslog メッセージをキャプチャします。プラスボタン をクリックして、イベントの送信先となる syslog サーバーを表す syslog サーバーオブジェクトを指定します（この時点で、syslog サーバーオブジェクトの作成も可能です）。さらに、ログに記録するメッセージの重大度の最小レベルを選択します。

これにより、任意のタイプのsyslogメッセージのデータロギングイベントが、選択した最小の重大度レベルで syslog サーバーに送信されます。

（注） CDO は現在、データロギング用のカスタムログフィルタの作成をサポートしていません。syslog サーバーに送信するメッセージをより細かく制御するには、この設定をFDM で定義することをお勧めします。これを行うには、FDMにログオンし、[システム設定（System Settings）] > [ロギングの設定（Logging Settings）] に移動します。

ヒント Cisco Security Analytics and Logging のユーザーは、データロギングを有効にする際は、必ずデータロギングイベントを Secure Event Connector 以外の syslog サーバーに転送してください。データイベント（診断イベント）はトラフィックイベントではありません。データイベントを別のsyslogサーバーに送信すると、SECがそれらを分析してフィルタリングする負担がなくなります。

ステップ 4 [ファイル/マルウェアのログ設定（File/Malware Log Settings）]。このスライダを「オン」にスライドして、ファイルイベントとマルウェアイベントをキャプチャします。イベントの送信先となる syslog サーバーを表す syslog サーバーオブジェクトを指定します。Syslog サーバー オブジェクトをまだ作成していない場合は、この時点で作成することもできます。

ファイルイベントとマルウェアイベントは、同じ重大度レベルで生成されます。選択したメッセージの重大度の最小レベルは、すべてのファイルイベントおよびマルウェアイベントに割り当てられます。

ファイルイベントとマルウェアイベントは、アクセスコントロールルールのファイルポリシーまたはマルウェアポリシーがトリガーされたときに報告されます。これは接続イベントとは異なります。ファイルイベントおよびマルウェアイベントのsyslog設定は、脅威ライセンスとマルウェアライセンスを必要とするファイルまたはマルウェアのポリシーを適用する場合にのみ該当します。

シスコのセキュリティ分析とロギングに登録している場合：

- Secure Event Connector（SEC）を介して Cisco Cloud にイベントを送信する場合は、syslog サーバーとして SEC を指定します。これらのイベントは、ファイルポリシーとマルウェアポリシーの接続イベントとともに表示されます。
- SEC を使用せずに Cisco Cloud に直接イベントを送信する場合は、この設定を有効にする必要はありません。アクセスコントロールルールで接続イベントを送信するように設定されている場合、ファイルイベントとマルウェアイベントが送信されます。

ステップ 5 [侵入ロギング（Intrusion Logging）]。イベントの送信先となる syslog サーバーを表す syslog サーバーオブジェクトを指定して、侵入イベントを syslog サーバーに送信します。Syslog サーバー オブジェクトをまだ作成していない場合は、この時点で作成することもできます。

侵入イベントは、アクセスコントロールルールの侵入ポリシーがトリガーされたときに報告されます。これは接続イベントとは異なります。進入イベントのsyslog設定は、脅威ライセンスを必要とする侵入ポリシーを適用する場合にのみ該当します。

シスコのセキュリティ分析とロギングに登録している場合：

- Secure Event Connector（SEC）を介して Cisco Cloud にイベントを送信する場合は、syslog サーバーとして SEC を指定します。これらのイベントは、ファイルポリシーとマルウェアポリシーの接続イベントとともに表示されます。
- SEC を使用せずに Cisco Cloud に直接イベントを送信する場合は、この設定を有効にする必要はありません。アクセスコントロールルールで接続イベントを送信するように設定されている場合、侵入イベントが Cisco Cloud に送信されます。

ステップ 6 [コンソールフィルタ（Console Filter）]。このスライダを 「オン」にスライドして、データロギング（診断ロギング）イベントを syslog サーバーではなくコンソールに送信します。さらに、ログに記録するイベント重大度の最小レベルを選択します。これにより、任意のタイプの syslog メッセージのデータロギングイベントが、選択した最小の重大度レベルで送信されます。

これらのメッセージは、FTD のコンソールポート上の CLI にログインしたときに表示されます。これらのログは、**show console-output** コマンドを使用して、その他のインターフェイス（管理インターフェイスを含む）への SSH セッションでも確認できます。さらに、メイン CLI から **system support diagnostic-cli** と入力すると、診断 CLI でリアルタイムでこれらのメッセージを表示できます。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

メッセージの重大度

次の表に、syslog メッセージの重大度の一覧を示します。

レベル番号	重大度	説明
[0]	**emergencies**	システムが使用不可能な状態です。
1	**alert**	すぐに措置する必要があります。
2	**critical**	深刻な状況です。
3	**error**	エラー状態です。
4	**warning**	警告状態です。
5	**notification**	正常ですが、注意を必要とする状況です。
6	**informational**	情報メッセージです。
7	**debugging**	デバッグ メッセージです。
（注）	FTD は、重大度 0（緊急）の syslog メッセージを生成しません。	

DHCP サーバーの設定

Dynamic Host Configuration Protocol（DHCP）サーバは、IP アドレスなどのネットワーク設定パラメータを DHCP クライアントに提供します。接続されたネットワークで DHCP クライアントに構成パラメータを提供するように、インターフェイスで DHCP サーバを設定できます。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャストアドレスよりもブロードキャストを使用します。DHCP クライアントは、UDP ポート 68 でメッセージをリッスンします。DHCP サーバーは、UDP ポート 67 でメッセージをリッスンします。DHCP サーバは、BOOTP 要求をサポートしていません。

DHCP クライアントは、サーバが有効になっているインターフェイスと同じネットワークに属している必要があります。スイッチがあるとしても、サーバーとクライアントの間にルータを介在させることはできません。

⚠

注意 すでに DHCP サーバが動作しているネットワークで DHCP サーバを設定しないでください。2 つのサーバーがお互いに競合するため、結果は予測不可能になります。

手順

ステップ 1 このセクションには 2 つのエリアがあります。最初は、[構成（Configuration）] セクションにグローバルパラメータが表示されます。[DHCPサーバ（DHCP Servers）] エリアには、サーバーを設定したインターフェイスと、サーバーが有効にされているかどうか、そしてサーバーのアドレスプールが表示されます。

ステップ 2 [構成（Configuration）] セクションで、自動設定とグローバル設定を構成します。

DHCP 自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバー、ドメイン名、および WINS サーバーの情報が、DHCP サーバーから DHCP クライアントに提供されます。通常、外部インターフェイスで DHCP を使用してアドレスを取得する場合には自動設定を使用しますが、DHCP を介してアドレスを取得するインターフェイスを選択することもできます。自動設定を使用できない場合には、必要なオプションを手動で定義できます。

1. 自動設定を利用する場合、[自動設定を有効にする（Enable Auto Configuration）] をクリックして [オン（On）] にしてから、DHCP を介してアドレスを取得するインターフェイスを [次のインターフェイスから取得（From Interface）] プルダウンで選択します。
2. 自動設定を有効にしない場合、または自動設定された設定を上書きするには、次のグローバルオプションを設定します。これらの設定は、DHCP サーバーをホストするすべてのインターフェイスで DHCP クライアントに送信されます。
    1. **プライマリ WINS IP アドレス**、**セカンダリ WINS IP アドレス**。クライアントが NetBIOS の名前解決に使用する Windows インターネット ネーム サービス（WINS）サーバーのアドレス。

2. **プライマリ DNS IP アドレス**、**セカンダリ DNS IP アドレス**。クライアントがドメイン名の解決に使用するドメインネームシステム（DNS）サーバーのアドレス。DNS IP アドレスフィールドに Cisco Umbrella DNS サーバーを入力する場合は、[Apply Umbrella Settings（Umbrella 設定を適用）] をクリックします。ボタンをクリックすると、適切な IP アドレスがフィールドにロードされます。

3. [保存（Save）] をクリックします。

ステップ 3 [DHCPサーバー（DHCP Servers）]セクションで、既存のサーバーを編集するか、[新しいDHCPサーバー（New DHCP サーバー）] をクリックして新しいサーバーを追加および構成します。

1. サーバ プロパティを設定します。

   1. [DHCPサーバーの有効化（Enable DHCP Server）] サーバーを有効にするかどうかを決定します。サーバを設定できますが、使用する準備が整うまでサーバは無効にしておきます。

   2. [インターフェイス（Interface）]。クライアントにDHCPアドレスを提供するインターフェイスを選択します。インターフェイスは静的IPアドレスを持っている必要があります。インターフェイスでDHCPサーバを実行する場合、インターフェイスアドレスの取得に DHCP を使用することはできません。ブリッジ グループの場合、 メンバー インターフェイスではなく、ブリッジ仮想インターフェイス（BVI）で DHCP サーバを設定します。そうすると、サーバはすべてのメンバーインターフェイスで有効になります。診断インターフェイスでDHCPサーバを設定することはできません。[デバイス（Device）]>[システム設定（System Settings）]>[管理インターフェイス（Management Interface）] ページの管理インターフェイスで設定します。

   3. [アドレスプール（Address Pool）]。DHCP サーバーの単一の IP アドレスまたは IP アドレス範囲を追加します。アドレスを要求するクライアントにサーバが提供できる IP アドレスの最小から最大までの範囲です。IPアドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自体の IP アドレス、ブロードキャスト アドレス、またはサブネット ネットワーク アドレスを含めることはできません。プールの開始アドレスと終了アドレスをハイフンで区切って指定します。たとえば、 10.100.10.12-10.100.10.250 のように指定します。

2. [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

DNS サーバの設定

ドメインネームシステム（DNS）サーバーは、IPアドレスのホスト名の解決に使用されます。DNS サーバーは、管理インターフェイスによって使用されます。

手順

ステップ 1 [プライマリ、セカンダリ、ターシャリDNS IPアドレス（Primary, Secondary, Tertiary DNS IP Address）] に、DNS サーバーの IP アドレスを優先順位に従って 3 つまで入力します。使用していたプライマリ DNS サーバーからの応答がなくなると、セカンダリが使用され、最後にターシャリが使用されます。DNS IP アドレスフィールドに Cisco Umbrella DNS サーバーを入力する場合は、[Apply Umbrella Settings（Umbrella 設定を適用）] をクリックします。ボタンをクリックすると、適切な IP アドレスがフィールドにロードされます。

ステップ 2 [ドメイン検索名（Domain Search Name）] に、ネットワークのドメイン名（example.com など）を入力します。このドメインは、完全修飾されていないホスト名に付加されます（たとえば、serverA は serverA.example.com になります）。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

管理インターフェイス

管理インターフェイスは物理的な管理ポートに接続されている仮想インターフェイスです。物理ポートは診断インターフェイスと呼ばれ、他の物理ポートとともにインターフェイスページで設定できます。FTD Virtual ではどちらのインターフェイスも仮想ですが、この二重性は保持されます。

管理インターフェイスには 2 つの使い方があります。

- IP アドレスへの Web および SSH 接続を開き、インターフェイスからデバイスを設定できます。
- システムはこの IP アドレスを使用してスマート ライセンスおよびデータベースの更新情報を取得します。

CLI セットアップ ウィザードを使用すると、システムの初期設定時にデバイスの管理アドレスとゲートウェイを設定します。FDM のセットアップウィザードを使用すると、管理アドレスとゲートウェイアドレスはデフォルトのまま変更されません。

必要に応じて、FDM を使用してこれらのアドレスを変更できます。また、CLI で **configure network ipv4 manual** および **configure network ipv6 manual** コマンドを使用することで、管理アドレスとゲートウェイアドレスを変更することもできます。

管理ネットワーク上の他のデバイスが DHCP サーバーとして機能している場合、スタティックアドレスを定義するか、または DHCP を介してアドレスを取得できます。デフォルトでは、管理アドレスは静的で、DHCP サーバーはポートで動作します（DHCP サーバーのない FTD Virtual を除く）。そのため、デバイスを管理ポートに直接接続し、ワークステーションの DHCP アドレスを取得できます。これにより、デバイスの接続と設定が容易になります。

⚠

注意 現在接続されているアドレスを変更した場合は、その変更がすぐに適用されるため、変更の保存と同時に、FDM（またはCLI）にアクセスできなくなります。デバイスに接続し直す必要があります。新しいアドレスが管理ネットワークで使用できることを確認します。

手順

ステップ 1 管理 IP アドレス、ネットワークマスクまたは IPv6 プレフィックス、および IPv4、IPv6、またはその両方のゲートウェイ（必要に応じて）を設定します。少なくとも 1 組のプロパティを設定する必要があります。1 組は空白にし、そのアドレッシング方式を無効にします。

ステップ 2 **[タイプ（Type）]** > **[DHCP]** を選択し、DHCP または IPv6 自動設定によってアドレスおよびゲートウェイを取得します。ただし、ゲートウェイとしてデータインターフェイスを使用している場合、DHCP を使用することはできません。この場合はスタティックアドレスを使用する必要があります。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ホスト名（Hostname）

デバイス ホスト名を変更できます。

手順

ステップ 1 [ファイアウォールホスト名（Firewall Hostname）] フィールドに、デバイスの新しいホスト名を入力します。

ステップ 2 [保存（Save）] をクリックします。

ステップ 3 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

NTP サーバの設定

システムの時刻を設定するには、Network Time Protocol（NTP）サーバーを設定する必要があります。

手順

ステップ 1 独自のタイムサーバー（手動）を使用するか、シスコのタイムサーバーを使用するかを選択します。

- [新規 NTP サーバー（New NTP Server）]。使用する NTP サーバの完全修飾名または IP アドレスを入力します。例、ntp1.example.com または 10.100.10.10。
- [デフォルトを使用（Use Default）]。

ステップ 2 [保存（Save）] をクリックします。

ステップ 3 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

URL フィルタリングの設定

システムは、Cisco Collective Security Intelligence（CSI）から URL カテゴリとレピュテーションデータベースを取得します。これらの設定により、データベースの更新とシステムが不明なカテゴリまたはレピュテーションの URL を処理する方法が制御されます。これらの設定を行うには、URL フィルタリング ライセンスを有効にする必要があります。

注意 URL フィルタリング スマート ライセンスがなくても [URL フィルタリングの設定（URL Filtering Preferences）] を設定することはできますが、展開するにはスマートライセンスが必要です。URL フィルタリング スマート ライセンスを追加するまでは、展開がブロックされます。

手順

ステップ 1 該当するオプションを有効にします。

- カテゴリとレピュテーションを含む更新された URL データが自動的にチェックされ、ダウンロードされるようにするには、[自動更新の有効化（Enable Automatic Updates）] スライダをクリックしてオンにします。展開後、FTD は、30 分ごとに更新をチェックします。
- ローカル URL フィルタリングデータベースのカテゴリおよびレピュテーションのデータを含まない URL に関する更新情報について Cisco CSI をチェックするには、[不明な URL に対する Cisco CSI のクエリ（Query Cisco CSI for Unknown URLs）] スライダをクリックしてオンにします。
- [URL 存続可能時間（URL Time to Live）] は、[不明な URL に対する Cisco CSI のクエリ（Query Cisco CSI for Unknown URLs）] オプションを有効にしている場合にのみ有効になります。これにより、指定された URL のカテゴリおよびレピュテーション ルックアップ値を保持する時間が決まります。存続可能時間が経過すると、次に試行される URL のア

クセスが新規のカテゴリ/レピュテーション ルックアップになります。時間が短いほど URL フィルタリングが正確になり、時間が長いほど未知の URL に対するパフォーマンスが向上します。デフォルトでは [なし（Never）] が選択されています。

ステップ 2 [保存（Save）] をクリックします。

ステップ 3 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

クラウド サービス（Cloud Services）

[クラウドサービス（Cloud Services）]ページを使用して、クラウドベースのサービスを管理できます。

（注） Cisco Success Network への接続と、Cisco Cloud に送信されるイベントの設定は、ソフトウェア バージョン 6.6 以降を実行している FTD デバイスで設定できる機能です。

Cisco Success Network への接続

Cisco Success Network を有効にすると、テクニカル サポートを提供するために不可欠な使用状況の情報と統計情報がシスコに提供されます。またこの情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。

接続を有効にすると、デバイスが Cisco Cloud へのセキュアな接続を確立し、シスコから提供されているテクニカルサポートサービス、クラウド管理および監視サービスなどの追加サービスに参加できるようになります。お使いのデバイスは、いつでもこのセキュアな接続を確立して維持できます。

はじめる前に

Cisco Success Network を有効にするには、FDM を使用してデバイスをクラウドに登録する必要があります。デバイスを登録するには、（[スマートライセンス（Smart Licensing）]ページで）Cisco Smart Software Manager にデバイスを登録するか、または登録キーを入力して Cisco Defense Orchestrator に登録します。

注目 高可用性グループのアクティブ装置で Cisco Success Network を有効にする場合、スタンバイ装置での接続も有効にします。

手順

ステップ 1 [クラウドサービス（Cloud Services）] タブをクリックします。

ステップ 2 必要に応じて Cisco Success Network 機能の [有効化（Enable）] スライダをクリックして設定を変更します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Cisco Cloud へのイベントの送信

Cisco Cloud サーバーにイベントを送信できます。このサーバーから、各種のシスコ クラウド サービスがイベントにアクセスできます。次に、Cisco Threat Response などのクラウドアプリケーションを使用して、イベントを分析したり、デバイスが遭遇した可能性のある脅威を評価したりできます。

はじめる前に

このサービスを有効にするには、事前に Cisco Smart Software Manager にデバイスを登録する必要があります。

米国地域では https://visibility.amp.cisco.com/ で、EU 地域では https://visibility.amp.cisco.com/ で、Cisco Threat Response に接続できます。アプリケーションの使い方と利点についての動画は、YouTube でご視聴いただけます（http://cs.co/CTRvideos）。FTD での Cisco Threat Response の使い方の詳細については、『*Firepower And CTR Integration Guide*』[英語] を参照してください（https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html）。

手順

ステップ 1 [クラウドサービス（Cloud Services）] タブをクリックします。

ステップ 2 必要に応じて [Cisco Cloudにイベントを送信（Send Events to the Cisco Cloud）] オプションの [有効化（Enable）] スライダをクリックして設定を変更します。

ステップ 3 サービスを有効にすると、クラウドに送信するイベントを選択するように求められます。

- [ファイル/マルウェア（File/Malware）]：任意のアクセス制御ルールで適用した任意のファイルポリシー用。
- [侵入（Intrusion）]：任意のアクセス制御ルールで適用した任意の侵入ポリシー用。
- [接続（Connection）]：ロギングを有効にしたアクセス制御ルール用。このオプションを選択すると、すべての接続イベントを送信するか、優先度の高い接続イベントのみを送信するかを選択することも可能です。優先度の高い接続イベントとは、侵入、ファイル、またはマルウェアイベントをトリガーする接続、またはセキュリティインテリジェンスブロッキング ポリシーに一致する接続に関連するイベントです。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Web 分析の有効化と無効化

Web分析を有効にすると、ページのヒット数に基づいて匿名の製品使用情報をシスコに提供できます。情報には、表示したページ、ページで費やした時間、ブラウザのバージョン、製品バージョン、デバイスのホスト名などが含まれます。この情報は、シスコが機能の使用状況パターンを確認し、製品を改善するのに使用されます。すべての使用状況データは匿名で、センシティブ データは送信されません。CDO を使用して、FTD のすべてのバージョンでこの機能を設定できます。

Web 分析はデフォルトで有効になっています。

手順

ステップ 1 [Web 分析（Web Analytics）] タブをクリックします。

ステップ 2 必要に応じて [Web 分析（Web Analytics）] 機能の [有効化（Enable）] スライダをクリックして設定を変更します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

CDO コマンドライン インターフェイスの使用

CDO では、コマンドライン インターフェイス（CLI）を使用して FTD デバイスを管理できます。コマンドは、単一のデバイスに送信することも、複数のデバイスに同時に送信することも可能です。ここでは、CLI コマンドを単一の デバイスに送信する方法について説明します。

関連情報：

- FTD SSH CLI ドキュメントについては、『Cisco Firepower Threat Defense Command Reference』を参照してください。FTD デバイスの CLI 機能は制限されていることに注意してください。FTD デバイスでは、`show`、`ping`、`traceroute`、`packet-tracer`、`failover`、および `shutdown` コマンドのみ使用できます。

コマンドの入力方法

1 つのコマンドを 1 行に入力することも、複数のコマンドを複数の行に連続して入力することも可能で、CDO は、入力されたコマンドをバッチとして順番に実行します。次の ASA の例で

は、3つのネットワークオブジェクトと、それらのネットワークオブジェクトを含むネットワーク オブジェクト グループを作成するコマンドのバッチを送信します。

[ASAデバイスコマンドの入力（Entering ASA device Commands）]：CDO は、グローバル コンフィギュレーション モードでコマンドの実行を開始します。

[FTDデバイスコマンドの入力（Entering FTD device Commands）]：CLI コンソールは基本 FTD CLI を使用します。CLI コンソールを使用して、診断CLI、エキスパート モード、およびFXOS CLI（FXOS を使用するモデル）に入ることはできません。このような他の CLI モードに入る必要がある場合は、SSH を使用します。

長いコマンド：非常に長いコマンドを入力すると、CDO は、コマンドを複数のコマンドに分割して、すべてのコマンドを ASA API に対して実行できるようにします。コマンドの適切な区切りを CDO が判断できない場合、コマンドのリストをどこで区切るかのヒントを求めるプロンプトが表示されます。次に例を示します。

```
Error: CDO attempted to execute a portion of this command with a length that exceeded
600 characters. You can give a hint to CDO at where a proper command separation point
is by breaking up your list of commands with an additional empty line between them.
```

このエラーメッセージを受信した場合、次の手順を実行します。

手順

ステップ 1 CLI履歴ペインでエラーの原因となったコマンドをクリックします。CDOは、コマンドボックスにコマンドの長いリストを入力します。

ステップ 2 関連するコマンドのグループの後に空行を挿入して、コマンドの長いリストを編集します。たとえば、上記の例のように、ネットワークオブジェクトのリストを定義し、それらをグループに追加した後に空の行を追加します。この作業を、コマンドリストのいくつかの箇所で実行することになる場合があります。

ステップ 3 [送信（Send）] をクリックします。

単一デバイスで CLI を使用する

手順

ステップ 1 [デバイスとサービス（Devices & Services）] ページを開きます。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 コマンド ライン インターフェイスを使用して、管理するデバイスを選択します。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、[>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 上部の「コマンドペイン」にコマンドを入力し、[送信（Send）] をクリックします。コマンドに対するデバイスの応答は、「応答ペイン」の下に表示されます。

（注） 選択したデバイスが同期されていない場合、次のコマンドのみが許可されます：`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy`

コマンド履歴での動作

CLI コマンドを送信すると、CDO はそのコマンドを [コマンド ラインインターフェイス（Command Line Interface）] ページの履歴ペインに記録します。履歴ペインに保存されたコマンドは、再実行することも、コマンドをテンプレートとして使用することもできます。

手順

ステップ 1 [デバイスとサービス（Devices & Services）] ページで、設定するデバイスを選択します。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 5 履歴ペインがまだ展開されていない場合は、時計アイコン をクリックして展開します。

ステップ 6 [履歴（History）] ペインで変更または再送信するコマンドを選択します。

ステップ 7 コマンドをそのまま再利用するか、コマンドペインでコマンドを編集し、[送信（Send）] をクリックします。CDO は、応答ペインにコマンドの結果を表示します。

（注） 次の 2 つの状況で「完了しました（Done!）」というメッセージが CDO の応答ペインに表示されます。

- OpenStack の導入要件
- コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。この正規表現の条件に合致する設定エントリがなかった場合、CDO は「完了しました（Done!）」を返します。

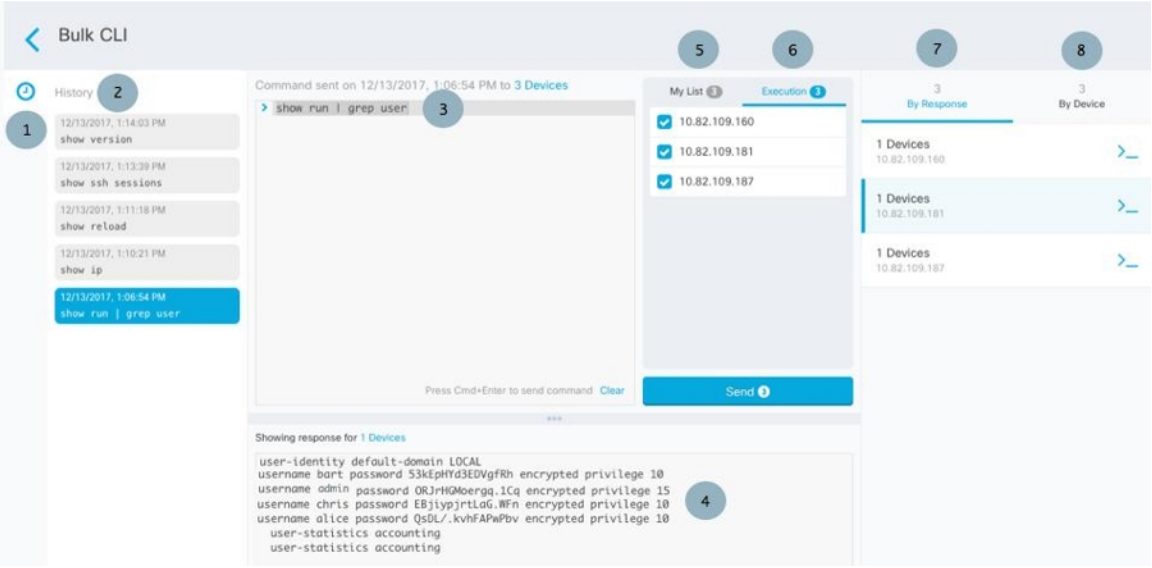
一括コマンド ライン インターフェイス

CDO では、コマンドライン インターフェイス（CLI）を使用して FTD デバイスを管理できます。コマンドは、単一のデバイスに送信することも、同じ種類の複数のデバイスに同時に送信することも可能です。この項目では、CLI コマンドを複数のデバイスに一度に送信する方法について説明します。

関連情報：

- Cisco IOS CLI のドキュメントについては、お使いの IOS バージョンの「Networking Software（IOS & NX-OS）」を参照してください。https://www.cisco.com/c/en/us/support/ios-nx-os-software/index.html
- FTD については、CDO はベース FTD CLI のみをサポートします。FTD デバイスでは、`show`、`ping`、`traceroute`、`packet-tracer`、`failover`、および `shutdown` コマンドのみ使用できます。FTD SSH CLI ドキュメントについては、『Cisco Firepower Threat Defense Command Reference』を参照してください。

一括 CLI インターフェイス



（注） 次の 2 つの状況で「**完了しました（Done!）**」というメッセージが CDO に表示されます。

- OpenStack の導入要件
- コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。この正規表現の条件に合致する設定エントリがなかった場合、CDO は「**完了しました（Done!）**」を返します。

ケース	説明
1	コマンド履歴ペインを展開したり折りたたんだりするには、時計アイコンをクリックします。
2	コマンド履歴。コマンドを送信すると、CDO はこの履歴ペインにコマンドを記録するので、コマンドをもう一度選択し、再度実行できます。
3	コマンドペイン。このペインのプロンプトにコマンドを入力します。

ケース	説明
4	応答ペイン。CDO は、コマンドに対するデバイスの応答と CDO メッセージを表示します。複数のデバイスの応答が同じだった場合、応答ペインに「X デバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが CDO に表示されます。 （注） 次の 2 つの状況で「**完了しました（Done!）**」というメッセージが CDO に表示されます。 • OpenStack の導入要件 • コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。この正規表現の条件に合致する設定エントリがなかった場合、CDO は「**完了しました（Done!）**」を返します。
5	[マイリスト（My List）] タブには、[インベントリ（Inventory）] テーブルから選択したデバイスが表示されます。このタブで、コマンドを送信するデバイスを含めたり除外したりすることができます。
[6]	上の図で強調表示されている [実行（Execution）] タブには、履歴ペインで選択されているコマンドの対象デバイスが表示されます。この例では、履歴ペインで show run | grep user コマンドが選択され、[実行（Execution）] タブに、10.82.109.160、10.82.109.181、および 10.82.10.9.187 に送信されたことが表示されます。
7	[応答別（By Response）] タブをクリックすると、コマンドによって生成された応答のリストが表示されます。同一の応答は 1 行にグループ化されます。[応答別] タブで行を選択すると、CDO はそのコマンドへの応答を応答ペインに表示します。
8	[デバイス別（By Device）] タブをクリックすると、各デバイスからの個別の応答が表示されます。リスト内のいずれかのデバイスをクリックすると、特定のデバイスからのコマンドへの応答を表示できます。

コマンドの一括送信

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 CLI を使用して管理するデバイスを特定して、それらを選択します。

ステップ 5 詳細ペインで、>_ [コマンド ライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 6 コマンドペインにコマンドを入力して、[送信（Send）] をクリックします。コマンド出力が応答ペインに表示されます。コマンドは変更ログに記録され、CDO はコマンドを [一括CLI（Bulk CLI）] ウィンドウの [履歴（History）] ペインに記録します。

（注） 選択したデバイスが到達可能で同期されていることを確認してください。

一括コマンド履歴での動作

一括 CLI コマンドを送信すると、CDO はそのコマンドを一括 CLI ページの履歴ペインに記録します。履歴ペインに保存されたコマンドは、再実行することも、コマンドをテンプレートとして使用することもできます。履歴ペインのコマンドは、それらが実行された元のデバイスに関連付けられています。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックし、設定するデバイスを選択します。

ステップ 4 [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 5 [履歴（History）] ペインで変更または再送信するコマンドを選択します。選択したコマンドは特定のデバイスに関連付けられており、最初のステップで選択したものとは限らないことに注意してください。

ステップ 6 [マイリスト（My List）] タブを見て、送信しようとしているコマンドが対象のデバイスに送信されることを確認します。

ステップ 7 コマンドペインでコマンドを編集し、[送信（Send）] をクリックします。CDO は、応答ペインにコマンドの結果を表示します。

（注） 選択したデバイスのいずれかが同期されていない場合、次のコマンドのみが許可されます：`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy`

一括コマンドフィルタでの動作

一括 CLI コマンドを実行後、[応答別（By Response）] フィルタと [デバイス別（By Device）] フィルタを使用して、デバイスの設定を続行できます。

応答別フィルタ

一括コマンドの実行後、CDO は [応答別（By Response）] タブに、コマンドを送信したデバイスから返された応答のリストを入力します。同じ応答のデバイスは1行にまとめられます。[応答別（By Response）] タブの行をクリックすると、応答ペインにデバイスからの応答が表示されます。応答ペインに複数のデバイスの応答が表示される場合、「Xデバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが

CDO に表示されます。

コマンド応答に関連付けられたデバイスのリストにコマンドを送信するには、次の手順に従います。

手順

ステップ 1 [応答別（By Response）] タブの行にあるコマンドシンボルをクリックします。

ステップ 2 コマンドペインでコマンドを確認し、[送信（Send）] をクリックしてコマンドを再送信するか、[クリア（Clear）] をクリックしてコマンドペインをクリアし、新しいコマンドを入力してデバイスに送信してから、[送信（Send）] をクリックします。

ステップ 3 コマンドから受け取った応答を確認します。

ステップ 4 選択したデバイスの実行コンフィギュレーションファイルに変更が反映されていることが確実な場合は、コマンドペインに「deploy memory」と入力し、[送信（Send）] をクリックします。この操作により、実行コンフィギュレーションがスタートアップコンフィギュレーションに保存されます。

デバイス別フィルタ

一括コマンドの実行後、CDO は [実行（Execution）] タブと [デバイス別（By Device）] タブに、コマンドを送信したデバイスのリストを入力します。[デバイス別（By Device）] タブの行をクリックすると、各デバイスの応答が表示されます。

同じデバイスリストでコマンドを実行するには、次の手順に従います。

手順

ステップ 1 [デバイス別（By Device）] タブをクリックします。

ステップ 2 [>_これらのデバイスでコマンドを実行（>_Execute a command on these devices）] をクリックします。

ステップ 3 [クリア（Clear）] をクリックしてコマンドペインをクリアし、新しいコマンドを入力します。

ステップ 4 [マイリスト（My List）] ペインで、リスト内の個々のデバイスを選択または選択解除して、コマンドを送信するデバイスのリストを指定します。

ステップ 5 [送信（Send）] をクリックします。コマンドへの応答が応答ペインに表示されます。応答ペインに複数のデバイスの応答が表示される場合、「X デバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[X デバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが CDO に表示されます。

ステップ 6 選択したデバイスの実行コンフィギュレーションファイルに変更が反映されていることが確実な場合は、コマンドペインに「deploy memory」と入力し、[送信（Send）] をクリックします。

デバイスの管理用 CLI マクロ

CLI マクロは、すぐに使用できる完全な形式の CLI コマンド、または実行前に変更できる CLI コマンドのテンプレートです。すべてのマクロは、1 つ以上の FTD デバイスで同時に実行できます。

テンプレートに似た CLI マクロを使用して、複数のデバイスで同じコマンドを同時に実行します。CLI マクロは、デバイスの設定と管理の一貫性を促進します。完全な形式の CLI マクロを使用して、デバイスに関する情報を取得します。FTD デバイスですぐに使用できるさまざまな CLI マクロがあります。

頻繁に実行するタスクを監視するための CLI マクロを作成できます。詳細については、「CLI マクロの作成」を参照してください。

CLI マクロは、システム定義またはユーザー定義です。システム定義マクロは CDO によって提供され、編集も削除もできません。ユーザー定義マクロはユーザーが作成し、編集または削除できます。

（注） デバイスが CDO にオンボードされた後にのみ、デバイスのマクロを作成できます。

例として ASA を使用すると、いずれかの ASA で特定のユーザーを検索する場合は、次のコマンドを実行できます。

```
show running-config | grep username
```

このコマンドを実行すると、検索しているユーザーのユーザー名が username に置き換わります。このコマンドからマクロを作成するには、同じコマンドを使用して、username を中括弧で囲みます。

```
> show running-config | grep {{username}}
```

パラメータには任意の名前を付けることができ、そのパラメータ名で同じマクロを作成することもできます。

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

パラメータ名は説明的な名前にでき、英数字と下線を使用する必要があります。この場合、コマンドシンタックスは次のようになります。

```
show running-config | grep
```

コマンドの一部として、コマンドの送信先のデバイスに適した CLI シンタックスを使用する必要があります。

新規コマンドからの CLI マクロの作成

手順

ステップ 1 CLI マクロを作成する前に CDO のコマンド ライン インターフェイスでコマンドをテストして、コマンドの構文が正しく、信頼できる結果が返されることを確認します

（注）
- FTD デバイスの場合、CDO は FDM の CLI コンソールで実行できるコマンド（`show`、`ping`、`traceroute`、`packet-tracer`、`failover`、`reboot`、`shutdown`）のみをサポートします。これらのコマンドの構文の完全な説明については、『Cisco Firepower Threat Defense コマンドリファレンス』を参照してください。

ステップ 2 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 3 [デバイス（Devices）] タブをクリックしてデバイスを見つけます。

ステップ 4 適切なデバイスタイプのタブをクリックし、オンラインかつ同期されているデバイスを選択します。

ステップ 5 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 CLI マクロのお気に入りのスター をクリックして、すでに存在するマクロを確認します。

ステップ 7 プラスボタン をクリックします。

ステップ 8 マクロに一意の名前を指定します。必要に応じて、CLI マクロの説明とメモを入力します。

ステップ 9 [コマンド（Command）] フィールドにコマンドを入力します。

ステップ 10 コマンドの実行時に変更したいコマンドの部分を、中括弧で囲まれたパラメータ名に置き換えます。

ステップ 11 [作成（Create）] をクリックします。作成したマクロは、最初に指定したデバイスだけでなく、そのタイプのすべてのデバイスで使用できます。

コマンドを実行するには、『デバイスでの CLI マクロの実行』を参照してください。

CLI 履歴または既存の CLI マクロからの CLI マクロの作成

この手順では、すでに実行したコマンド、別のユーザー定義マクロ、またはシステム定義マクロからユーザー定義マクロを作成します。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

（注） CLI 履歴からユーザー定義マクロを作成する場合は、コマンドを実行したデバイスを選択します。CLI マクロは、同じアカウントのデバイス間で共有されますが、CLI 履歴は共有されません。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、オンラインかつ同期されているデバイスを選択します。

ステップ 4 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 5 CLI マクロを作成するコマンドを見つけて選択します。次のいずれかの方法を使用してください。

- クロック をクリックして、そのデバイスで実行したコマンドを表示します。マクロに変換するコマンドを選択すると、コマンドペインにそのコマンドが表示されます。
- CLI マクロのお気に入りのスター をクリックして、すでに存在するマクロを確認します。変更するユーザー定義またはシステム定義の CLI マクロを選択します。コマンドがコマンドペインに表示されます。

ステップ 6 コマンドがコマンドペインに表示された状態で、CLI マクロの金色の星 をクリックします。このコマンドが、新しい CLI マクロの基礎になります。

ステップ 7 マクロに一意の名前を指定します。必要に応じて、CLI マクロの説明とメモを入力します。

ステップ 8 [コマンド（Command）] フィールドのコマンドを確認し、必要な変更を加えます。

ステップ 9 コマンドの実行時に変更したいコマンドの部分を、中括弧で囲まれたパラメータ名に置き換えます。

ステップ 10 [作成（Create）]をクリックします。作成したマクロは、最初に指定したデバイスだけでなく、そのタイプのすべてのデバイスで使用できます。

コマンドを実行するには、CLI マクロの実行を参照してください。

CLI マクロの実行

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、1 つ以上のデバイスを選択します。

ステップ 4 [>_ コマンド ライン インターフェイス（>_Command Line Interface）] をクリックします。

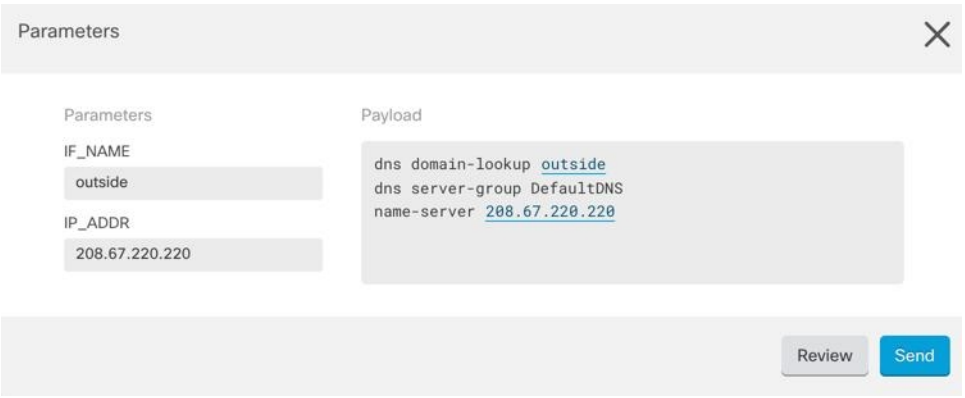
ステップ 5 コマンドパネルで、スター ★ をクリックします。

ステップ 6 コマンドパネルから CLI マクロを選択します。

ステップ 7 次のいずれかの方法でマクロを実行します。

- 定義するパラメータがマクロに含まれていない場合は、[送信（Send）] をクリックします。コマンドへの応答が応答ペインに表示されます。これで完了です。
- マクロにパラメータが含まれている場合（下の Configure DNS マクロなど）、[>_ パラメータの表示（>_ View Parameters）] をクリックします。

ステップ 8 [パラメータ（Parameters）] ペインで、パラメータの値を [パラメータ（Parameters）] の各フィールドに入力します。



ステップ 9 [送信（Send）] をクリックします。CDO が正常にコマンドを送信し、デバイスの構成を更新すると、「完了」というメッセージが表示されます。

- FTD の場合は、デバイスのアクティブな構成が更新されます。

ステップ 10 コマンドを送信した後で、「一部のコマンドが実行コンフィギュレーションに変更を加えた可能性があります」というメッセージが 2 つのリンクとともに表示されることがあります。

- [ディスクへの書き込み（Write to Disk）] をクリックすると、このコマンドによって加えられた変更と、実行コンフィギュレーションのその他の変更がデバイスのスタートアップ構成に保存されます。
- [取り消す（Dismiss）] をクリックすると、メッセージが取り消されます。

CLI マクロの編集

ユーザー定義の CLI マクロは編集できますが、システム定義のマクロは編集できません。CLI マクロを編集すると、すべての FTD デバイスでマクロが変更されます。マクロは特定のデバイス固有のものではありません。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 デバイスを選択します。
ステップ 5 [コマンドラインインターフェイス（Command Line Interface）] をクリックします。
ステップ 6 編集するユーザー定義マクロを選択します。
ステップ 7 マクロラベルの編集アイコンをクリックします。
ステップ 8 [マクロの編集（Edit Macro）] ダイアログボックスで CLI マクロを編集します。
ステップ 9 [保存（Save）] をクリックします。

CLI マクロの実行方法については、「CLI マクロの実行」を参照してください。

CLI マクロの削除

ユーザー定義の CLI マクロは削除できますが、システム定義のマクロは削除できません。CLI マクロを削除すると、すべてのデバイスでマクロが削除されます。マクロは特定のデバイス固有のものではありません。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 デバイスを選択します。
ステップ 5 [コマンド ライン インターフェイス（Command Line Interface）] をクリックします。
ステップ 6 削除するユーザー定義 CLI マクロを選択します。
ステップ 7 CLI マクロラベルのゴミ箱アイコン をクリックします。
ステップ 8 CLI マクロを削除することを確認します。

FTD コマンド ライン インターフェイスのドキュメント

CDO は、FTD コマンド ライン インターフェイスの一部をサポートしています。ユーザーが単一のデバイスおよび複数のデバイスにコマンドアンドレスポンス形式で同時にコマンドを送信できるように、CDO ではターミナル型のインターフェイスを提供しています。CDO でサポートされていないコマンドについては PuTTy や SSH クライアントなどのデバイス GUI ターミナルを使用してデバイスにアクセスし、『FTD CLI リファレンス』ドキュメントでさらに多くのコマンドを参照してください。

CLI コマンドの結果のエクスポート

スタンドアロンデバイスまたは複数のデバイスに発行された CLI コマンドの結果をコンマ区切り値（.csv）ファイルにエクスポートして、必要に応じて情報をフィルタリングおよび並べ替えることができます。単一のデバイスまたは多数のデバイスの CLI 結果を一度にエクスポートできます。エクスポートされた情報には、次のものが含まれます。

- Device
- 日付（Date）
- User
- コマンド
- 出力

CLI コマンドの結果のエクスポート

コマンドウィンドウで実行したコマンドの結果を .csv ファイルにエクスポートできます。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、>_ [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 6 [コマンドラインインターフェイス（Command Line Interface）] ペインでコマンドを入力し、[送信（Send）] をクリックしてデバイスに送ります。

ステップ 7 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 8 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

CLI マクロの結果のエクスポート

コマンドウィンドウで実行されたマクロの結果をエクスポートできます。次の手順で、1 つまたは複数のデバイスで実行された CLI マクロの結果を .csv ファイルにエクスポートします。

手順

ステップ 1 [デバイスとサービス（Devices & Services）] ページを開きます。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、>_ [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。

ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信（Send）] をクリックします。

ステップ 8 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 9 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

CLI コマンド履歴のエクスポート

次の手順を使用して、1 つまたは複数のデバイスの CLI 履歴を .csv ファイルにエクスポートします。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、[>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 履歴ペインがまだ展開されていない場合は、[時計（Clock）] アイコン をクリックして展開します。

ステップ 7 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 8 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

関連情報：

- CDO コマンドライン インターフェイスの使用
- CLI マクロの作成
- CLI マクロの削除
- CLI マクロの編集
- CLI マクロの実行
- FTD コマンド ライン インターフェイスのドキュメント
- 一括コマンド ライン インターフェイス

CLI マクロのリストをエクスポートする

コマンドウィンドウで実行されたマクロのみをエクスポートできます。次の手順で、1 つまたは複数のデバイスの CLI マクロを .csv ファイルにエクスポートします。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの[デバイスアクション]ペインで、[>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。

ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信（Send）] をクリックします。

ステップ 8 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 9 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。

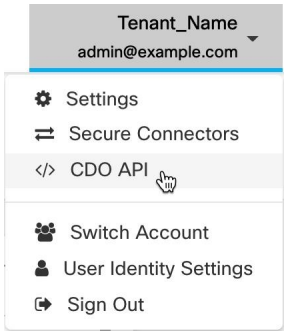
CDO パブリック API

CDO はパブリック API を公開しており、ドキュメント、例、実験用のプレイグラウンドを提供しています。パブリック API の目標は、通常は CDO UI で実行できる多くのことをコードで実行するためのシンプルで効果的な方法を提供することです。

この API を使用するには、GraphQL の知識が必要です。詳細でありながら読みやすい公式ガイド（https://graphql.org/learn/）が提供されています。

完全なスキーマドキュメントを見つけるには、GraphQL Playground に移動し、ページの右側にある [ドキュメント（docs）] タブをクリックしてください。

ユーザーメニューから選択して、CDO パブリック API を起動できます。



REST API マクロを作成する

FTD API ツールを使用する

CDO は、FTD デバイスで高度なアクションを実行するための FTD Representational State Transfer（REST）アプリケーションプログラミング（API）要求を実行するための API ツールインター

フェイスを提供します。REST API は、JavaScript Object Notation（JSON）形式を使用してオブジェクトを表します。

インターフェイスは、システム定義またはユーザー定義の API マクロを提供します。システム定義マクロは CDO によって提供され、編集も削除もできません。ユーザー定義マクロはユーザーが作成し、編集または削除できます。FDM API Explorer でサポートされているすべてのリソースグループを使用できます。

（注） CDO は、JSON を返す FDM API エンドポイントのみをサポートしています。

前提

プログラミングの一般的な知識と、REST API および JSON の一定の理解があることを想定しています。これらのテクノロジーになじみがない場合は、最初に REST API の一般的なガイドをお読みください。

サポートドキュメント

- 詳細については、『Cisco Firepower Threat Defense REST API ガイド』を参照してください。
- Cisco DevNet サイトでは、参照情報と例をオンラインで検索することもできます。

サポートされる HTTP メソッド

次の HTTP メソッドのみを使用できます。

重要 読み取り専用ロールを持つユーザーは、GET 操作のみを実行できます。

属性	説明
GET	デバイスからデータを読み取ります。
POST	あるリソースタイプの新しいオブジェクトを作成します。たとえば、POST を使用して新しいネットワーク オブジェクトを作成します。
PUT	既存のリソースの属性を変更します。PUT を使用する場合は、JSON オブジェクト全体を含める必要があります。オブジェクト内の個々の属性を選択的に更新することはできません。たとえば、PUT を使用して、既存のネットワークオブジェクトに含まれているアドレスを変更します。

属性	説明
DELETE	自分または他のユーザーが作成したリソースを削除します。たとえば、不要になったネットワーク オブジェクトを削除するには、DELETE を使用します。

関連情報：

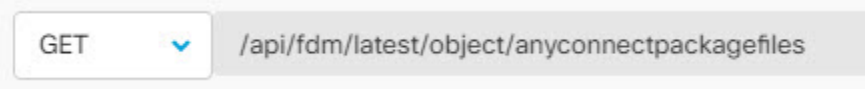
- FTD REST API リクエストの入力方法
- FTD REST API マクロについて
  - REST API マクロを作成する
  - REST API マクロの実行
  - REST API マクロの編集
  - REST API マクロの削除

FTD REST API リクエストの入力方法

FTDデバイスを選択して単一のコマンドを指定するか、追加のパラメータが必要なコマンドを実行できます。

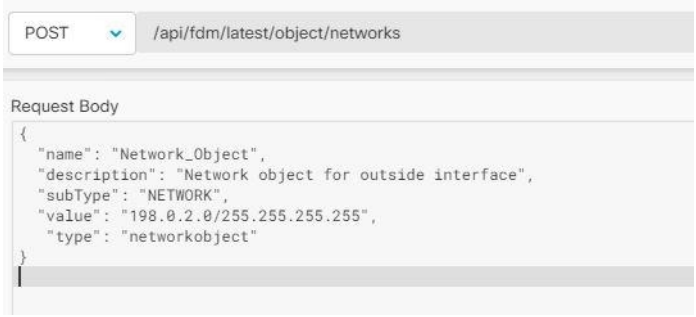
REST API リクエストのシンタックスを確認する場合は、デバイスの [API Explorer] ページ（https://ftd.example.com/#/api-explorer など）にログオンし、必要なリソースグループをクリックして、実行するコマンドのシンタックスを確認します。例：https://10.10.5.84/#/api-explorer。

次の図は、CDO での単一の REST API リクエストの例を示しています。



次の図は、追加のパラメータが必要なREST APIリクエストの例を示しています。[リクエストの本文（Request Body）]でデータを手動で指定する必要があります。コマンドのシンタックスを確認するには、デバイスの [API Explorer] ページにログオンします。

（注） POST リクエストを実行するには、デバイスが同期状態である必要があります。



手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 REST API を使用して管理する FTD デバイスを選択し、右側の [デバイスアクション（Device Actions）] で、[APIツール（API Tool）] をクリックします。

ステップ 5 ドロップダウンからリクエスト方式を選択し、**/api/fdm/latest/** に続けて実行するコマンドを入力します。POST または PUT コマンドを実行している場合は、リクエストの本文を入力します。

ステップ 6 [送信（Send）] をクリックします。[リクエストの本文（Response Body）] には、実行されたコマンドの応答が表示されます。

重要 POST リクエストは、通常、デバイスのステージングされた設定に変更を加えます。[FDMの変更をコミット（Commit Changes in FDM）] をクリックして、変更を FTD デバイスに送信します。

関連情報：

- FTD API ツールを使用する （410 ページ）
- FTD REST API マクロについて
  - REST API マクロを作成する
  - REST API マクロの実行
  - REST API マクロの編集
  - REST API マクロの削除

FTD REST API マクロについて

REST API マクロは、すぐに使用できる完全な形式の REST API コマンド、または実行前に変更できる REST API コマンドのテンプレートです。すべての REST API マクロは、1 つ以上の FTD デバイスで同時に実行できます。

テンプレートに似た REST API マクロを使用して、同じコマンドを複数のデバイスで同時に実行します。REST API マクロは、デバイスの設定と管理の一貫性を促進します。完全な形式の REST API マクロを使用して、デバイスに関する情報を取得します。FTD デバイスですぐに使用できるさまざまな REST API マクロがあります。

頻繁に実行するタスク用に REST API マクロを作成できます。詳細については、「REST API マクロを作成する」を参照してください。

REST API マクロは、システム定義またはユーザー定義です。システム定義マクロは CDO によって提供され、編集も削除もできません。ユーザー定義マクロはユーザーが作成し、編集または削除できます。

（注） デバイスが CDO にオンボードされた後にのみ、デバイスのマクロを作成できます。

関連情報：

- REST API マクロを作成する
- REST API マクロの実行
- REST API マクロの編集
- REST API マクロの削除

REST API マクロを作成する

新コマンドを使用した REST API マクロの作成

手順

ステップ 1 REST APマクロを作成する前にCDOのREST APIインターフェイスでコマンドをテストして、コマンドの構文が正しく、信頼できる結果が返されることを確認します

（注） デバイスが CDO にオンボードされた後にのみ、デバイスのマクロを作成できます。

ステップ 2 REST API を使用して管理する FTD デバイスを選択し、右側の [デバイスアクション（Device Actions）] で、[APIツール（API Tool）] をクリックします。

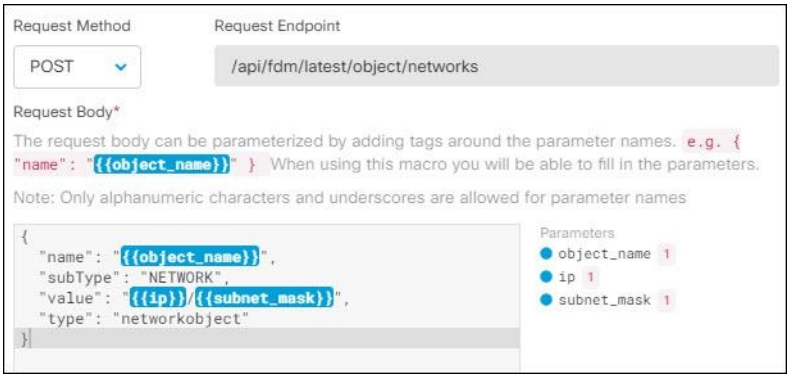
ステップ 3 REST APIマクロのお気に入りのスター★をクリックして、すでに存在するマクロを確認します。

ステップ 4 プラスボタン をクリックします。

ステップ 5 マクロに一意の名前を指定します。必要に応じて、REST API マクロの説明と注意点を入力します。

ステップ 6 [要求メソッド（Request Method）] を選択し、[要求エンドポイント（Request Endpoint）] フィールドにエンドポイント URL を入力します。詳細については、『Cisco Firepower Threat Defense REST API ガイド』を参照してください。

ステップ 7 コマンドの実行時に変更したいコマンドの部分を、中括弧で囲まれたパラメータ名に置き換えます。



ステップ 8 [OK] をクリックします。作成したマクロは、最初に指定したデバイスだけでなく、そのタイプのすべてのデバイスで使用できます。

コマンドの実行については、「REST API マクロの実行」を参照してください。

履歴または既存の REST API マクロを使用した REST API マクロの作成

この手順では、すでに実行したコマンド、別のユーザー定義マクロ、またはシステム定義マクロからユーザー定義 REST API マクロを作成します。

手順

ステップ 1 REST API を使用して管理する FTD デバイスを選択し、右側の [デバイスアクション（Device Actions）] で、[APIツール（API Tool）] をクリックします。

（注） REST API 履歴からユーザー定義マクロを作成する場合は、コマンドを実行したデバイスを選択します。REST API マクロは、同じアカウントのデバイス間で共有されますが、REST API 履歴は共有されません。

ステップ 2 API マクロを作成するコマンドを見つけて選択します。次のいずれかの方法を使用してください。

- クロック をクリックして、そのデバイスで実行したコマンドを表示します。マクロに変換するコマンドをダブルクリックして選択すると、コマンドペインにそのコマンドが表示されます。
- API マクロのお気に入りのスター をクリックして、すでに存在するマクロを確認します。変更するユーザー定義またはシステム定義の API マクロを選択します。コマンドがコマンドペインに表示されます。

ステップ 3 コマンドがコマンドペインに表示された状態で、API マクロの金色のスター をクリックします。このコマンドが、新しい API マクロの基礎になります。

ステップ 4 マクロに一意の名前を指定します。必要に応じて、API マクロの説明と注意点を入力します。

ステップ 5 [コマンド（Command）] フィールドのコマンドを確認し、必要な変更を加えます。

ステップ 6 コマンドの実行時に変更したいコマンドの部分を、中括弧で囲まれたパラメータ名に置き換えます。

ステップ 7 [作成（Create）]をクリックします。作成したマクロは、最初に指定したデバイスだけでなく、そのタイプのすべてのデバイスで使用できます。

コマンドの実行については、「REST API マクロの実行」を参照してください。

関連情報：

FTD REST API マクロについて

REST API マクロの実行

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

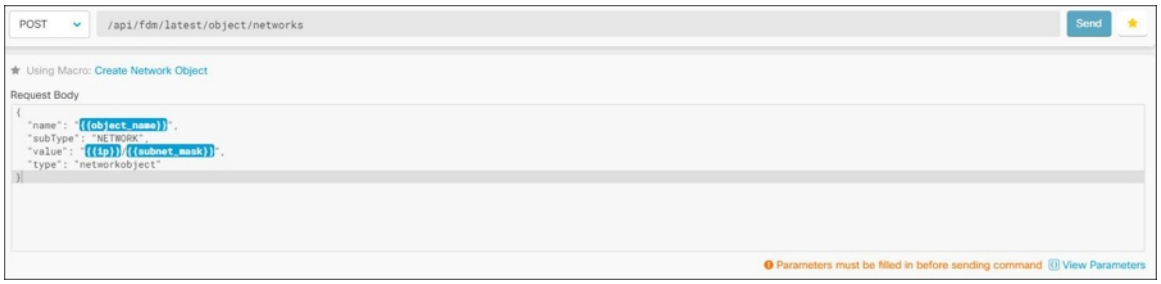
ステップ 4 右側の [デバイスアクション（Device Actions）] ペインで、[API ツール（API Tool）] をクリックします。

ステップ 5 コマンドパネルで、スター をクリックして REST API マクロを表示します。

ステップ 6 コマンドパネルから REST API マクロを選択します。

ステップ 7 次のいずれかの方法でマクロを実行します。

- 定義するパラメータがマクロに含まれていない場合は、[送信（Send）] をクリックします。コマンドへの応答が応答ペインに表示されます。これで完了です。
- マクロにパラメータが含まれている場合（下の Create Network Object マクロなど）、[パラメーターの表示（View Parameters）] をクリックします。



ステップ 8 [パラメータ（Parameters）] ペインで、パラメータの値を [パラメータ（Parameters）] の各フィールドに入力します。

ステップ 9 [送信（Send）] をクリックします。

（注） FTD デバイスのアクティブな設定が更新されます。

関連情報：

FTD REST API マクロについて

REST API マクロの編集

ユーザー定義の REST API マクロは編集できますが、システム定義のマクロは編集できません。REST API マクロを編集すると、すべての FTD デバイスでマクロが変更されます。マクロは特定のデバイス固有のものではありません。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 REST API を使用して管理する FTD デバイスを選択し、右側の [デバイスアクション（Device Actions）] で、[APIツール（API Tool）] をクリックします。

ステップ 5 編集するユーザー定義マクロを選択します。

ステップ 6 マクロラベルの編集アイコンをクリックします。

ステップ 7 [マクロの編集（Edit Macro）] ダイアログボックスで REST API マクロを編集します。

ステップ 8 [保存（Save）] をクリックします。

REST API マクロの実行方法については、「REST API マクロの実行」を参照してください。

関連情報：

FTD REST API マクロについて

REST API マクロの削除

ユーザー定義の REST API マクロは削除できますが、システム定義のマクロは削除できません。REST API マクロを削除すると、すべてのデバイスでマクロが削除されます。マクロは特定のデバイス固有のものではありません。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 デバイスを選択して、右側の [デバイスアクション（Device Actions）] で、[API ツール（API Tool）] をクリックします。

ステップ 5 削除するユーザー定義 REST API マクロを選択します。

ステップ 6 REST API マクロ ラベルのゴミ箱アイコン をクリックします。

ステップ 7 REST API マクロを削除することを確認します。

関連情報：

FTD REST API マクロについて

変更の読み取り、破棄、チェック、および展開

デバイスを管理するために、CDO は、デバイスの設定のコピーを独自のデータベースに保存する必要があります。CDO が管理対象デバイスから設定を「読み取る」とき、CDO はデバイス設定のコピーを作成し、それを保存します。CDO が最初にデバイスの設定のコピーを読み取って保存するのは、デバイスがオンボーディングされたときです。以下の選択肢のように、さまざまな目的に応じて設定を読み取ります。

- [変更の破棄（Discard Changes）] は、デバイスの設定ステータスが「未同期」の場合に使用できます。未同期の状態では、デバイスの設定に対する変更が CDO で保留中になっています。このオプションを使用すると、保留中のすべての変更を取り消すことができます。保留中の変更は削除され、CDO は設定のコピーをデバイスに保存されている設定のコピーで上書きします。
- [変更の確認（Check for Changes）]。このアクションは、デバイスの設定ステータスが同期済みの場合に使用できます。[変更の確認（Checking for Changes）] をクリックすると、CDO は、デバイスの設定のコピーを、デバイスに保存されている設定のコピーと比較するように指示します。違いがある場合、CDO はデバイスに保存されているコピーでそのデバイスの設定のコピーをすぐに上書きします。
- [競合の確認（Review Conflict）] と [レビューなしで承認（Accept Without Review）]。 。デバイスで [競合検出（Conflict Detection）] を有効にすると、CDO はデバイスに加えられた設定の変更を 10 分ごとにチェックします。https://docs.defenseorchestrator.com/Welcome_to_Cisco_Defense_Orchestrator/Basics_of_Cisco_Defense_Orchestrator/Synchronizing_Configurations_Between_Defense_Orchestrator_and_Device/0010_Conflict_Detectionデバイスに保存されている設定のコピーが変更された場合、CDO は「競合が検出されました」という設定ステータスを表示して通知します。
  - [競合の確認（Review Conflict）]。[競合の確認（Review Conflict）] をクリックすると、デバイスで直接行われた変更を確認し、それらを受け入れるか拒否するかを選択できます。
  - [レビューなしで承認（Accept Without Review）]。このアクションは、デバイスの設定の CDO のコピーを、デバイスに保存されている設定のコピーで上書きします。CDO は、上書きアクションを実行する前に、設定の 2 つのコピーの違いを確認するように求めません。

[すべて読み取り（Read All）] は一括操作です。任意の状態の複数のデバイスを選択し、[すべて読み取り（Read All）] をクリックして、CDO に保存されているすべてのデバイスの設定を、デバイスに保存されている設定で上書きすることができます。

変更の配置

デバイスの設定に変更を加えると、CDO では、加えた変更が独自のコピーに保存されます。これらの変更は、デバイスに展開されるまで CDO で「保留」されています。デバイスの設定に変更があり、それがデバイスに展開されていない場合、デバイスは未同期構成状態になります。

保留中の設定変更は、デバイスを通過するネットワークトラフィックには影響しません。変更は、CDO がデバイスに展開した後にのみ影響を及ぼします。CDO がデバイスの設定に変更を展開すると、変更された設定の要素のみが上書きされます。デバイスに保存されている構成ファイル全体を上書きすることはありません。展開は、1 つのデバイスに対して開始することも、複数のデバイスに対して同時に開始することもできます。

（注） 展開や繰り返しの展開をスケジュールできます。詳細については、自動展開のスケジュール（429 ページ）を参照してください。

[すべて破棄（Discard All）] は、[プレビューして展開...（Preview and Deploy..）] をクリックした後にのみ使用できるオプションです。 。[プレビューして展開（Preview and Deploy）] をクリックすると、CDO で保留中の変更のプレビューが CDO に表示されます。[すべて破棄（Discard All）] をクリックすると、保留中のすべての変更が CDO から削除され、選択したデバイスには何も展開されません。上述の [変更の破棄（Discard Changes）] とは異なり、保留中の変更を削除すると操作が終了します。

すべてのデバイス設定の読み取り

Cisco Defense Orchestrator（CDO）の外部にあるデバイスの設定が変更された場合、CDO に保存されているデバイスの設定と、当該デバイスの設定のローカルコピーは同じではなくなります。多くの場合、CDO にあるデバイスの設定のコピーをデバイスに保存されている設定で上書きして、設定を再び同じにしたいと考えます。[すべて読み取り（Read All）] リンクを使用して、多くのデバイスでこのタスクを同時に実行できます。

CDO によるデバイス設定の 2 つのコピーの管理方法の詳細については、「変更の読み取り、破棄、チェック、および展開」を参照してください。

[すべて読み取り（Read All）] をクリックした場合に、CDO にあるデバイスの設定のコピーがデバイスの設定のコピーで上書きされる 3 つの設定ステータスを次に示します。

- [競合検出（Conflict Detected）]：競合検出が有効になっている場合、CDO は、設定に加えられた変更について、管理するデバイスを 10 分ごとにポーリングします。CDO は、デバイスの設定が変更されたことを検出した場合、デバイスの [競合検出（Conflict Detected）] 設定ステータスを表示します。
- [同期（Synced）]：デバイスが [同期（Synced）] 状態の場合に、[すべて読み取り（Read All）] をクリックしすると、CDO はすぐにデバイスをチェックして、設定に直接変更が加えられているかどうかを判断します。[すべて読み取り（Read All）] をクリックすると、CDO はデバイスの設定のコピーを上書きすることを確認し、上書きを実行します。
- [非同期（Not Synced）]：デバイスが [非同期（Not Synced）] 状態の場合に、[すべて読み取り（Read All）] をクリックすると、CDO を使用したデバイスの設定に対する保留中の変更があること、および [すべて読み取り（Read All）] 操作を続行すると保留中の変更が削除されてから、CDO にある設定のコピーがデバイス上の設定で上書きされることが警告されます。この [すべて読み取り（Read All）] は、[変更の破棄（Discard Changes）] と同様に機能します。変更の破棄（Discard Changes） （432 ページ）

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 （任意）変更ログでこの一括アクションの結果を簡単に識別できるように、変更リクエストラベルを作成します。

ステップ 5 CDO を保存する設定のデバイスを選択します。CDO では、選択したすべてのデバイスに適用できるアクションのコマンドボタンのみ提供されることに注意してください。

ステップ 6 [すべて読み取り（Read All）] をクリックします。

ステップ 7 選択したデバイスのいずれかについて、CDO で設定変更がステージングされている場合、CDO は警告を表示し、設定の一括読み取りアクションを続行するかどうかを尋ねられます。[すべて読み取り（Read All）] をクリックして続行します。

ステップ 8 設定の [すべて読み取り（Read All）] 操作の進行状況については、[通知（notifications）] タブで確認します。一括操作の個々のアクションの成功または失敗に関する詳細を確認する場合は、青色の [レビュー（Review）] リンクをクリックすると、[ジョブ（Jobs）] ページに移動します。 [ジョブ（Jobs）] ページ

ステップ 9 変更リクエストラベルを作成してアクティブ化した場合は、他の設定変更を誤ってこのイベントに関連付けないように、忘れずにラベルをクリアしてください。

関連情報

- 変更の読み取り、破棄、チェック、および展開
- 変更の破棄（Discard Changes）
- 設定変更の確認

FTD から CDO への設定変更の読み取り

Cisco Defense Orchestrator が FTD 設定を読み取るのはなぜですか？

FTD を管理するには、CDO には FTD の設定の独自の保存されたコピーが必要になります。CDO は、FTD から設定を読み取るときに FTD の展開された設定のコピーを取得し、それを独自のデータベースに保存します。CDO が最初にデバイスの設定ファイルのコピーを読み取って保存するのは、デバイスをオンボーディングするときです。詳細については、「変更の読み取り、破棄、チェック、および展開」を参照してください。

保留中および展開済みの変更

Firepower Device Manager（FDM）またはその CLI を介して直接 FTD に加えられた設定変更は、それらが展開されるまで、FTD での段階的な変更と呼ばれます。段階的な変更または保留中の変更は、FTD を通過するトラフィックに影響を与えることなく編集または削除できます。ただ

し、保留中の変更が展開されると、それらの変更は FTD によって適用され、デバイスを通過するトラフィックに影響を与えます。

競合が検出されました

デバイスで [競合検出（Conflict Detection）] を有効にすると、CDO は 10 分ごとに設定の変更をチェックします。競合検出 （434 ページ）デバイスに保存されている設定のコピーが変更された場合、CDO は「競合が検出されました」という設定ステータスを表示して通知します。競合検出を有効にしていない場合、または 10 分間の自動ポーリング間隔以内にデバイスの設定に変更が加えられた場合、[変更の確認（Check for Changes）] をクリックすると、CDO はデバイス上の設定のコピーと CDO に保存された設定のコピーを即時に比較します。[競合の確認（Review Conflict）] を選択してデバイス設定と CDO に保存された設定との違いを調べ、その後 [変更の破棄（Discard Changes）] を選択して段階的な変更を削除し、保存された設定に戻すか、変更を確定することができます。[レビューなしで受け入れる（Accept without Review）] を選択することもできます。このオプションを選択すると、設定が取得され、現在 CDO に保存されている設定が上書きされます。

変更の破棄手順

FTD からの設定変更を破棄するには、次の手順に従います。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 構成が [競合が検出されました（Conflict Detected）] に設定されているデバイスを選択すると、[保留中の変更を元に戻す（Revert Pending Changes）] リンクが表示されます。メッセージで、リンクをクリックすると保留中の変更を元に戻すことができること、またはローカルマネージャ FDM を使用して FTD にログオンし、最初に変更を展開できることが説明されます。フィルタを使用して、競合状態にあるデバイスを見つけることができます。

注意 [保留中の変更を元に戻す（Revert Pending Changes）] リンクをクリックすると、FTD の保留中の変更がすぐに削除されます。最初に変更を確認する機会はありません。

ステップ 5 [保留中の変更を元に戻す（Revert Pending Changes）] をクリックする前に、FDM で変更を確認するには、次の手順を実行します。

1. ブラウザウィンドウを開き、https://< IP_address_of_the_FTD > と入力します。
2. FDM で展開アイコンを探します。コンソールにはオレンジ色の円が表示されており、展開する準備が整った変更があることを示しています  。
3. アイコンをクリックして、保留中の変更を確認します。

- 変更を削除しても構わない場合は、CDO に戻り、[保留中の変更を元に戻す（Revert Pending Changes）] をクリックします。この時点で、FTD の構成と CDO の構成のコピーは同じである必要があります。これで追加されました。
- 変更をデバイスに展開する場合は、[今すぐ展開（Deploy Now）] をクリックします。これで、FTD に展開された構成と CDO に保存された構成が同じではなくなりました。その後、CDO に戻り、設定変更の確認できます。CDO は、FTD に変更があったことを識別し、競合を確認する機会が得られます。その状態を解決するには、「競合検出」を参照してください。

保留中の変更を元に戻すことに失敗した場合

システムデータベースとセキュリティフィードへの変更は、CDO で元に戻すことはできません。CDO は保留中の変更があることを認識し、それらの変更を元に戻そうとしますが、失敗します。元に戻せなかった原因が、保留中のデータベースの更新やセキュリティフィードの更新なのかどうかを判断するには、デバイスの FDM コンソールにログインします。コンソールにはオレンジ色の円が表示されており、展開する準備が整った変更があることを示しています  。[展開（Deploy）] ボタンをクリックして保留中の変更を確認し、必要に応じて展開または破棄します。

競合の確認手順

FTD からの設定変更を確認するには、次の手順に従います。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 設定が [競合検出（Conflict Detected）] とマークされているデバイスを選択すると、右側の [競合検出（Conflict Detected）] ペインに [競合の確認（Review Conflict）] へのリンクが表示されます。

ステップ 5 [競合の確認（Review Conflict）] をクリックします。

ステップ 6 提示された 2 つの設定を比較します。

ステップ 7 次のいずれかの操作を行います。

- [承認（Accept）] をクリックして、CDO で最後に認識された設定をデバイスで検出された設定で上書きします。**注**：CDO に保存されている設定全体が、デバイスで検出された設定によって完全に上書きされます。

- [拒否（Reject）] をクリックして、デバイスに加えられた変更を拒否し、CDO で最後に認識された設定に置き換えます。
- 削除を中止するには、[キャンセル（Cancel）] をクリックします。

（注） デバイスが同期状態のときに [変更の確認（Check for Changes）]設定変更の確認 （431 ページ）をクリックすると、アウトオブバンドの変更についてデバイスをすぐに確認するように CDO に指示できます。

レビューなしで承認する手順

FTD からの設定変更を確認せずに受け入れるには、次の手順に従います。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 設定が [競合検出（Conflict Detected）] とマークされているデバイスを選択すると、右側の [競合検出（Conflict Detected）] ペインに [レビューなしで承認（Accept Without Review）] へのリンクが表示されます。

ステップ 5 [レビューなしで承認（Accept Without Review）] をクリックします。CDO は、現在の設定を受け入れて上書きします。

関連情報：

- 変更の読み取り、破棄、チェック、および展開
- 競合検出
- 変更の破棄

すべてのデバイスの設定変更のプレビューと展開

テナント上のデバイスに構成変更を加えたものの、その変更をまだ展開していない場合に、CDO は展開アイコンにオレンジ色のドットを表示して通知します。

。これらの変更の影響を受けるデバイスには、[デバイスとサービス（Devices and Services）] ページに「非同期（Not Synced）」のステータスが表示されます。[展開（Deploy）] をクリックすると、保留中の変更があるデバイスを確認し、それらのデバイスに変更を展開できます。

この展開方法は、サポートされているすべてのデバイスで使用できます。

この展開方法を使用して、単一の構成変更を展開することも、待機して複数の変更を一度に展開することもできます。

手順

ステップ 1 画面の右上で [デプロイ（Deploy）] アイコン をクリックします。

ステップ 2 展開する変更があるデバイスを選択します。デバイスに黄色の三角の注意マークが付いている場合、そのデバイスに変更を展開することはできません。黄色の三角の注意マークにマウスを合わせると、そのデバイスに変更を展開できない理由を確認できます。

ステップ 3 デバイスを選択したら、右側のパネルにデバイスを拡大し、具体的な変更をプレビューできます。

ステップ 4 （オプション）保留中の変更に関する詳細情報を表示する場合は、[詳細な変更ログを表示（View Detailed Changelog）] リンクをクリックして、その変更に関連付けられた変更ログを開きます。[展開（Deploy）] アイコンをクリックして、[保留中の変更があるデバイス（Devices with Pending Changes）] ページに戻ります。

ステップ 5 （オプション）[保留中の変更があるデバイス（Devices with Pending Changes）] ページを離れずに、変更を追跡する変更リクエストを作成します。

ステップ 6 [今すぐ展開（Deploy Now）] をクリックして、選択したデバイスに今すぐ変更を展開します。[ジョブ（Jobs）] トレイの [アクティブなジョブ（Active jobs）] インジケータに進行状況が表示されます。

ステップ 7 （オプション）展開が完了したら、CDO ナビゲーションバーの [ジョブ（Jobs）] をクリックします。展開の結果を示す最近の「変更の展開（Deploy Changes）」ジョブが表示されます。

ステップ 8 変更リクエストラベルを作成し、それに関連付ける構成変更がない場合は、それをクリアします。

次のタスク

- スケジュールされた自動展開
- CDO から FTD への設定変更の展開 （426 ページ）
- FTD への展開後のログエントリの変更

CDO から FTD への設定変更の展開

CDO が FTD に変更を展開する理由

CDO を使用してデバイスの設定を管理および変更すると、CDO により構成ファイルの独自のコピーに加えた変更が保存されます。それらの変更は、デバイスに展開されるまで CDO でステージングされたと見なされます。ステージングされた設定変更は、デバイスを通過するネットワークトラフィックには影響しません。変更は、CDO がデバイスに展開した後にのみ、デバイスを通過するトラフィックに影響を及ぼします。CDO がデバイスの設定に変更を展開すると、変更された設定の要素のみが上書きされます。デバイスに保存されている構成ファイル全体が上書きされることはありません。

CDO と同様に、FTD には保留中の変更と展開された変更の概念があります。FTD の保留中の変更は、CDO のステージングされた変更に相当します。保留中の変更は、FTD を通過するトラフィックに影響を与えることなく編集または削除できます。ただし、保留中の変更が展開されると、それらの変更は FTD によって適用され、デバイスを通過するトラフィックに影響を与えます。

FTD の構成ファイルの編集プロセスは 2 段階であるため、CDO は、管理する他のデバイスへの展開とは若干異なる方法で FTD への変更を展開します。CDO は最初に変更を FTD に展開しますが、変更は保留状態になります。次に、CDO が変更をデバイスに展開すると、変更が有効になります。変更は展開されると適用されるため、FTD を通過するトラフィックに影響を与えます。これは、スタンドアロンデバイスと高可用性（HA）デバイスの両方に適用されます。

展開は、1 つのデバイスに対して開始することも、複数のデバイスに対して同時に開始することもできます。単一のデバイスに対して、個別の展開や繰り返しの展開をスケジュールできます。

CDO が FTD に変更を展開することを妨げる 2 つの要因は次のとおりです。

- FTD にステージングされた変更がある場合。この状態を解決する方法の詳細については、「競合検出」を参照してください。
- FTD に展開されるプロセスに変更がある場合、CDO は変更を展開しません。

自動展開のスケジュール

スケジュールされた自動展開保留中の変更を使用して、単一のデバイスへの展開をスケジュールするようにテナントを設定することもできます。

変更のデバイスへの展開

手順

ステップ 1 CDO を使用してデバイスの設定を変更して保存すると、その変更はデバイスの設定の CDO インスタンスに保存されます。

ステップ 2 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 3 [デバイス] タブをクリックします。

ステップ 4 適切なデバイスタイプのタブをクリックします。変更を加えたデバイスの設定ステータスが [非同期（Not Synced）] と表示されます。

ステップ 5 次のいずれかの方法を使用して、変更を展開します。

- デバイスを選択し、右側の [非同期（Not Synced）] ペインで [プレビューして展開（Preview and Deploy）] をクリックします。[保留中の変更（Pending Changes）] 画面で、変更を確認します。保留中のバージョンに問題がなければ、[今すぐ展開（Deploy Now）] をクリックします。変更が正常に展開されたら、変更ログを表示して、展開の結果を確認できます。

- 画面右上の [展開（Deploy）] アイコン をクリックします。詳細については、すべてのデバイスの設定変更のプレビューと展開 （424 ページ）を参照してください。

変更をキャンセルする

CDO からデバイスに変更を展開するときに [キャンセル（Cancel）] をクリックすると、行った変更はデバイスに展開されません。プロセスはキャンセルされます。行った変更はまだCDO で保留中であり、最終的に FTD に展開する前に編集を加えることができます。

変更の破棄

変更をプレビューしているときに [すべて破棄（Discard all）] をクリックすると、自分が行った変更と、他のユーザーが行ったもののデバイスに展開しなかったその他の変更が削除されます。CDO は、保留中の構成を、変更が行われる前に最後に読み取られた構成またはデプロイされた構成に戻します。

デバイス設定の一括展開

共有オブジェクトを編集するなどして複数のデバイスに変更を加えた場合、影響を受けるすべてのデバイスにそれらの変更を一度に適用できます。

手順

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 CDO で設定を変更した、すべてのデバイスを選択します。これらのデバイスは、「未同期」ステータスが表示されているはずです。

ステップ 5 次のいずれかの方法を使用して、変更を展開します。

- 画面右上の [展開（Deploy）] ボタン をクリックします。これにより、選択したデバイス上の保留中の変更を展開する前に確認することができます。変更を展開するには、[今すぐ展開（Deploy Now）] をクリックします。

  （注） [保留中の変更があるデバイス（Devices with Pending Changes）] 画面でデバイスの横に黄色の警告三角形が表示されている場合、そのデバイスに変更を展開することはできません。そのデバイスに変更を展開できない理由を確認するには、警告三角形の上にマウスカーソルを置きます。

- 詳細ペインで [すべて展開（Deploy All）] をクリックします。 すべての警告を確認し、[OK] をクリックします。一括展開は、変更を確認せずにすぐに開始します。

ステップ 6 （任意）ナビゲーションバーの [ジョブ（Jobs）] アイコン  をクリックして、一括展開の結果を表示します。

関連情報：

- 自動展開のスケジュール （429 ページ）

スケジュールされた自動展開

CDO を使用すると、CDO が管理する 1 つ以上のデバイスの構成を変更し、都合のよいタイミングでそれらのデバイスに変更を展開するようにスケジュールできます。

[設定（Settings）] ページの [テナント設定（Tenant Settings）] タブで 自動展開をスケジュールするオプションを有効にする をした場合のみ、展開をスケジュールできます。このオプションを有効にすると、展開スケジュールを作成、編集、削除できます。展開スケジュールによって、CDO に保存されたすべてのステージング済みの変更が、設定した日時に展開されます。[ジョブ] ページから、展開スケジュールを表示および削除することもできます。

CDOに変更の読み取り、破棄、チェック、および展開デバイスに直接変更が加えられた場合、その競合が解決されるまで、展開スケジュールはスキップされます。[ジョブ（Jobs）] ページには、スケジュールされた展開が失敗したインスタンスが一覧表示されます。[自動展開をス

ケジュールするオプションを有効にする（Enable the Option to Schedule Automatic Deployments）] をオフにすると、スケジュールされたすべての展開が削除されます。

注意 複数のデバイスの新しい展開をスケジュールし、それらのデバイスの一部に展開が既にスケジュールされている場合、既存の展開スケジュールが新しい展開スケジュールで上書きされます。

（注） 展開スケジュールを作成すると、スケジュールはデバイスのタイムゾーンではなく現地時間で作成されます。展開スケジュールは、サマータイムに合わせて自動的に調整されません。

自動展開のスケジュール

展開スケジュールは、単一のイベントまたは繰り返し行われるイベントにすることができます。繰り返し行われる自動展開は、繰り返し行われる展開をメンテナンス期間に合わせるための便利な方法です。次の手順に従って、単一のデバイスに対して1回限りまたは繰り返し行われる展開をスケジュールします。

（注） 既存の展開がスケジュールされているデバイスへの展開をスケジュールすると、新しくスケジュールされた展開によって既存の展開が上書きされます。

手順

ステップ1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ2 [デバイス] タブをクリックします。

ステップ3 適切なデバイスタイプのタブをクリックします。

ステップ4 1 つ以上のデバイスを選択します。

ステップ5 [デバイスの詳細（Device Details）] ペインで、[スケジュールされた展開（ Scheduled Deployments）] タブを見つけて、[スケジュール（Schedule）] をクリックします。

ステップ6 展開をいつ実行するかを選択します。

- 1 回限りの展開の場合は、[1回限り（Once on）] オプションをクリックして、カレンダーから日付と時刻を選択します。
- 繰り返し展開する場合は、[定期（Every）] オプションをクリックします。日に 1 回と週に1回のいずれかの展開を選択できます。展開を実行する [曜日（Day）] と [時刻（Time）] を選択します。

ステップ 7 [保存（Save）] をクリックします。

スケジュールされた展開の編集

スケジュールされた展開を編集するには、次の手順に従います。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 1 つ以上のデバイスを選択します。
ステップ 5 [デバイスの詳細（Device Details）] ペインで、[スケジュールされた展開（ Scheduled Deployments）] タブを見つけて、[編集（Edit）] をクリックします。

ステップ 6 スケジュールされた展開の繰り返し回数、日付、または時刻を編集します。
ステップ 7 [保存（Save）] をクリックします。

スケジュールされた展開の削除

スケジュールされた展開を削除するには、次の手順に従います。

（注） 複数のデバイスの展開をスケジュールしてから、一部のデバイスのスケジュールを変更または削除した場合は、残りのデバイスの元のスケジュールされた展開が保持されます。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 1 つ以上のデバイスを選択します。
ステップ 5 [デバイスの詳細（Device Details）] ペインで、[スケジュールされた展開（ Scheduled Deployments）] タブを見つけて、[削除（Delete）] をクリックします。

次のタスク

- 変更の読み取り、破棄、チェック、および展開
- すべてのデバイス設定の読み取り （420 ページ）
- CDO から FTD への設定変更の展開 （426 ページ）
- すべてのデバイスの設定変更のプレビューと展開 （424 ページ）

設定変更の確認

[変更の確認（Check for Changes）] をクリックして、デバイスの設定がデバイス上で直接変更されているか、CDO に保存されている設定のコピーと異なっているかどうかを確認します。このオプションは、デバイスが [同期（Synced）] 状態のときに表示されます。

変更を確認するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 設定がデバイス上で直接変更された可能性があるデバイスを選択します。

ステップ 5 右側の [同期（Synced）] ペインで [変更の確認（Check for Changes）] をクリックします。

ステップ 6 次の動作は、デバイスによって若干異なります。

- FTDデバイスの場合、デバイスの設定に変更があった場合、次のメッセージが表示されます。

```
Reading the policy from the device. If there are active deployments on the device,
reading will start after they are finished.
```

  - [OK] をクリックして、先へ進みます。デバイスの設定で、CDO に保存されている設定が上書きされます。
  - 操作をキャンセルするには、[キャンセル（Cancel）] をクリックします。

- デバイスの場合：

1. 提示された 2 つの設定を比較します。[続行（Continue）] をクリックします。**最後に認識されたデバイス設定（Last Known Device Configuration）**というラベルの付いた設定は、CDO に保存されている設定です。**デバイスで検出（Found on Device）**というラベルの付いた設定は、ASA に保存されている設定です。
2. 次のいずれかを選択します。

1. [拒否（Reject）] : アウトオブバンド変更を拒否して、「最後に認識されたデバイス設定（Last Known Device Configuration）」を維持します。
2. [承認（Accept）] : アウトオブバンド変更を承認して、CDO に保存されているデバイスの設定を、デバイスで見つかった設定で上書きします。

3. [続行（Continue）] をクリックします。

変更の破棄（Discard Changes）

CDO を使用してデバイスの構成に加えた、展開されていない構成変更のすべてを「元に戻す」場合は、[変更の破棄（Discard Changes）] をクリックします。[変更の破棄（Discard Changes）] をクリックすると、CDO は、デバイスに保存されている構成でデバイスの構成のローカルコピーを完全に上書きします。

[変更の破棄（Discard Changes）] をクリックすると、デバイスの構成ステータスは [非同期（Not Synced）] 状態になります。変更を破棄すると、CDO 上の構成のコピーは、デバイス上の構成のコピーと同じになり、CDO の構成ステータスは [同期済み（Synced）] に戻ります。

デバイスの展開されていない構成変更のすべてを破棄する（つまり「元に戻す」）には、次の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 構成変更を実行中のデバイスを選択します。
ステップ 5 右側の [非同期（Not Synced）] ペインで [変更の破棄（Discard Changes）] をクリックします。

- FTD デバイスの場合は、「CDO で保留中の変更は破棄され、このデバイスに関する CDO の設定は、デバイスで現在稼働中の設定に置き換えられます」という警告メッセージが表示されます。[続行（Continue）] をクリックして変更を破棄します。
- Meraki デバイスの場合は、変更がすぐに削除されます。
- AWS デバイスの場合は、削除しようとしているものが表示されます。[同意する（Accept）] または [キャンセル（Cancel）] をクリックします。

デバイスのアウトオブバンド変更

アウトオブバンド変更とは、CDO を使用せずにデバイス上で直接行われた変更を指します。アウトオブバンド変更は、SSH 接続を介してデバイスのコマンドライン インターフェイスを使用して、または、ASA の場合は Adaptive Security Device Manager（ASDM）、FTD の場合は FDM などのローカルマネージャを使用して行うことができます。アウトオブバンド変更により、CDO に保存されているデバイスの設定とデバイス自体に保存されている設定との間で競合が発生します。

デバイスでのアウトオブバンド変更の検出

ASA、FTD、または Cisco IOS デバイスに対して競合検出が有効になっている場合、CDO は 10 分ごとにデバイスをチェックし、CDO の外部でデバイスの設定に直接加えられた新たな変更を検索します。

CDO は、CDO に保存されていないデバイスの設定に対する変更を検出した場合、そのデバイスの [設定ステータス（Configuration Status）] を [競合検出（Conflict Detected）] 状態に変更します。

Defense Orchestrator が競合を検出した場合、次の 2 つの状態が考えられます。

- CDO のデータベースに保存されていない設定変更が、デバイスに直接加えられています。
- FTD の場合、展開されていない「保留中」の設定変更がある可能性があります。

Defense Orchestrator とデバイス間の設定を同期する

設定の競合について

[デバイスとサービス（Devices & Services）] ページで、デバイスまたはサービスのステータスが [同期済み（Synced）]、[未同期（Not Synced）]、または [競合が検出されました（Conflict Detected）] になっていることがあります。

- デバイスが [同期済み（Synced）] の場合、Cisco Defense Orchestrator（CDO）の設定と、デバイスにローカルに保存されている設定は同じです。
- デバイスが [未同期（Not Synced）] の場合、CDO に保存された設定が変更され、デバイスにローカルに保存されている設定とは異なっています。CDO からデバイスに変更を展開すると、CDO のバージョンに一致するようにデバイスの設定が変更されます。
- CDO の外部でデバイスに加えられた変更は、**アウトオブバンドの変更**と呼ばれます。デバイスの競合検出が有効になっている場合、アウトオブバンドの変更が行われると、デバイスのステータスが [競合が検出されました（Conflict Detected）] に変わります。アウトオブバンドの変更を受け入れると、CDO の設定がデバイスの設定と一致するように変更されます。

競合検出

競合検出が有効になっている場合、Cisco Defense Orchestrator（CDO）はデフォルトの間隔でデバイスをポーリングして、CDO の外部でデバイスの構成が変更されたかどうかを判断します。変更が行われたことを検出すると、CDO はデバイスの構成ステータスを [競合検出（Conflict Detected）] に変更します。CDO の外部でデバイスに加えられた変更は、「アウトオブバンドの」変更と呼ばれます。

このオプションを有効にすると、デバイスごとに競合または OOB 変更を検出する頻度を設定できます。詳細については、デバイス変更のポーリングのスケジュール（438 ページ）を参照してください。

競合検出の有効化

競合検出を有効にすると、Defense Orchestrator の外部でデバイスに変更が加えられた場合に警告が表示されます。

手順

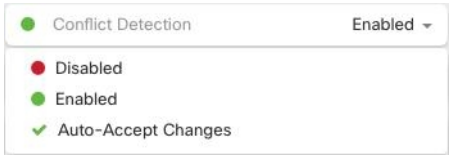
ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブを選択します。

ステップ 4 競合検出を有効にする 1 台または複数のデバイスを選択します。

ステップ 5 デバイステーブルの右側にある [競合検出（Conflict Detection）] ボックスで、リストから [有効（Enabled）] を選択します。



デバイスからのアウトオブバンド変更の自動的な受け入れ

変更の自動的な受け入れを有効にすることで、管理対象デバイスに直接加えられた変更を自動的に受け入れるように Cisco Defense Orchestrator（CDO）を設定できます。CDO を使用せずにデバイスに直接加えられた変更は、アウトオブバンド変更と呼ばれます。アウトオブバンドの

変更により、CDO に保存されているデバイスの設定とデバイス自体に保存されている設定との間で競合が発生します。

変更の自動受け入れ機能は、競合検出のための強化機能です。デバイスで変更の自動受け入れを有効にしている場合、CDO は 10 分ごとに変更をチェックして、デバイスの設定に対してアウトオブバンドの変更が行われたかどうかを確認します。設定が変更されていた場合、CDO は、プロンプトを表示することなく、デバイスの設定のローカルバージョンを自動的に更新します。

CDO で行われたいずれかの設定変更がデバイスにまだ展開されていない場合、CDO は設定変更を自動的に**受け入れません**。画面上のプロンプトに従って、次のアクションを決定します。

変更の自動受け入れを使用するには、最初に、テナントが [デバイスとサービス（Devices & Services）] ページの [競合検出（Conflict Detection）] メニューで自動受け入れオプションを表示できるようにします。次に、個々のデバイスでの変更の自動受け入れを有効にします。

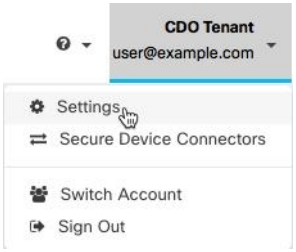
CDO でアウトオブバンドの変更を検出するものの、変更を手動で受け入れたり拒否したりするオプションを選択する場合は、代わりに 競合検出 （434 ページ） を有効にします。

自動承認変更の設定

手順

ステップ 1 管理者またはスーパー管理者権限を持つアカウントを使用して CDO にログインします。

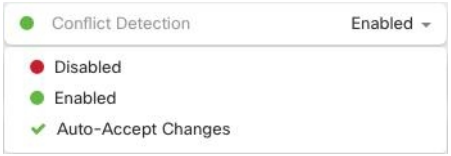
ステップ 2 ユーザーメニューから [設定（Settings）] をクリックして、[設定（Settings）] ページにアクセスします。



ステップ 3 [テナント設定（Tenant Settings）] エリアで、[デバイスの変更を自動承認するオプションの有効化（Enable the Option to Auto-accept Device Changes）] のトグルをクリックします。これにより、[デバイスとサービス（Devices & Services）] ページの [競合検出（Conflict Detection）] メニューに [変更の自動承認（Auto-Accept Changes）] メニューオプションが表示されるようになります。

ステップ 4 [デバイスとサービス（Devices & Services）] ページを開き、アウトオブバンドの変更を自動承認するデバイスを選択します。

ステップ 5 [競合の検出（Devices & Services）] メニューで、ドロップダウンメニューから [変更の自動承認（Auto-Accept Changes）] を選択します。



テナント上のすべてのデバイスの自動承認変更の無効化

手順

ステップ 1 管理者またはスーパー管理者権限を持つアカウントを使用して CDO にログインします。

ステップ 2 ユーザーメニューから [設定（Settings）] をクリックして、[設定（Settings）] ページにアクセスします。

ステップ 3 [テナント設定（Tenant Settings）] 領域で、トグルを左にスライドして灰色の X を表示し、[デバイスの変更を自動承認するオプションを有効にする（Enable the option to auto-accept device changes）] を無効にします。これにより、競合検出メニューの [変更の自動承認（Auto-Accept Changes）] オプションが無効になり、テナント上のすべてのデバイスでこの機能が無効になります。

（注） [自動承認（Auto-Accept）] を無効にした場合、CDO で承認する前に、各デバイスの競合を確認する必要があります。これまで変更の自動承認が設定されていたデバイスも対象になります。

設定の競合の解決

このセクションでは、デバイスで発生する設定の競合の解決に関する情報を提供します。

「未同期」ステータスの解決

次の手順を使用して、「未同期」の設定ステータスのデバイスを解決します。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 未同期と報告されたデバイスを選択します。

ステップ 5 右側の [未同期（Not synced）] パネルで、次のいずれかを選択します。

- [プレビューして展開...（Preview and Deploy..）]：設定の変更を CDO からデバイスにプッシュする場合は、今行った変更をすべてのデバイスの設定変更のプレビューと展開か、待ってから一度に複数の変更を展開します。
- [変更の破棄（Discard Changes）]：設定の変更を CDO からデバイスにプッシュ**したくない**場合、または CDO で開始した設定の変更を「元に戻す」場合。このオプションは、CDO に保存されている設定を、デバイスに保存されている実行中の設定で上書きします。

[競合検出（Conflict Detected）] ステータスの解決

CDO を使用すると、ライブデバイスごとに競合検出を有効化または無効化できます。競合検出 （434 ページ） が有効になっていて、CDO を使用せずにデバイスの設定に変更が加えられた場合、デバイスの設定ステータスには [競合検出（Conflict Detected）] と表示されます。

[競合検出（Conflict Detected）] ステータスを解決するには、次の手順に従います。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 競合を報告しているデバイスを選択し、右側の詳細ペインで [競合の確認（Review Conflict）] をクリックします。

ステップ 5 [デバイスの同期（Device Sync）] ページで、強調表示されている相違点を確認して、2 つの設定を比較します。

- 「最後に認識されたデバイス設定（Last Known Device Configuration）」というラベルの付いたパネルは、CDO に保存されているデバイス設定です。
- 「デバイスで検出（Found on Device）」というラベルの付いたパネルは、ASA の実行コンフィギュレーションに保存されている設定です。

ステップ 6 次のいずれかを選択して、競合を解決します。

- [デバイスの変更を承認（Accept Device changes）]：設定と、CDO に保存されている保留中の変更がデバイスの実行コンフィギュレーションで上書きされます。

  （注） CDO はコマンド ライン インターフェイス以外での Cisco IOS デバイスへの変更の展開をサポートしていないため、競合を解決する際の Cisco IOS デバイスの唯一の選択肢は [レビューなしで承認（Accept Without Review）] です。

- [デバイスの変更を拒否（Reject Device Changes）]：デバイスに保存されている設定をCDOに保存されている設定で上書きします。

（注） 拒否または承認されたすべての設定変更は、変更ログに記録されます。

デバイス変更のポーリングのスケジュール

競合検出（434ページ）を有効にしている場合、または[設定（Settings）]ページで[デバイスの変更を自動承認するオプションの有効化（Enable the Option to Auto-accept Device Changes）]を設定している場合、CDOはデフォルトの間隔でデバイスをポーリングして、CDOの外部でデバイスの設定に変更が加えられたかどうかを判断します。CDOによる変更のポーリング間隔は、デバイスごとにカスタマイズできます。ポーリング間隔の変更は、複数のデバイスに適用できます。

デバイスでこの間隔が選択されていない場合は、間隔は「テナントのデフォルト」に自動的に設定されます。

（注） [デバイスとサービス（Devices & Services）]ページでデバイスごとの間隔をカスタマイズすると、[全般設定（General Settings）]ページの[デフォルトの競合検出間隔（Default Conflict Detection Interval）]デフォルトの競合検出間隔で選択したポーリング間隔が上書きされます。

[デバイスとサービス（Conflict Detection）]ページで[競合検出（Conflict Detection）]を有効にするか、[設定（Settings）]ページで[デバイスの変更を自動承認するオプションの有効化（Enable the Option to Auto-accept Device Changes）]を設定したら、次の手順に従いCDOによるデバイスのポーリング間隔をスケジュールします。

手順

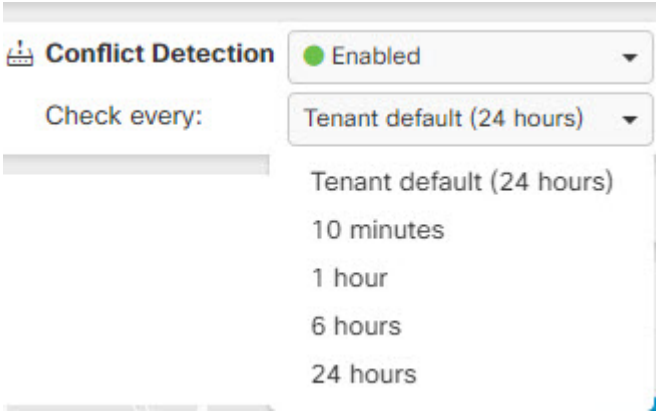
ステップ1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）]をクリックします。

ステップ2 [デバイス（Devices）]タブをクリックして、デバイスを見つけます。

ステップ3 適切なデバイスタイプのタブをクリックします。

ステップ4 競合検出を有効にする1台または複数のデバイスを選択します。

ステップ5 [競合検出（Conflict Detection）]と同じ領域で、[チェック間隔（Check every）]のドロップダウンメニューをクリックし、目的のポーリング間隔を選択します。



セキュリティデータベース更新のスケジュール設定

このセクションでは、デバイスでのセキュリティデータベースの更新スケジュール設定に関する情報を提供します。

セキュリティデータベースの更新スケジュールの作成

次の手順を使用して、FTD デバイスのセキュリティデータベースを確認および更新するスケジュールされたタスクを作成します。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 デバイスを選択します。

ステップ 5 [アクション（Actions）] ペインで、[セキュリティデータベースの更新（Security Database Updates）] セクションを見つけて、追加ボタン [+] をクリックします。

（注） 選択したデバイスに既存のスケジュールされたタスクがある場合は、編集アイコン をクリックして新しいタスクを作成します。新しいタスクを作成すると、既存のタスクが上書きされます。

ステップ 6 スケジュールされたタスクを次のように設定します。

- [頻度（Frequency）]。日次、週次、または 月次から更新の頻度を選択します。
- [時刻（Time）]。時刻を選択します。時刻はUTC で表示されることに注意してください。

- [曜日の選択（Select Days）]。更新を実行する曜日を選択します。

ステップ 7 [保存（Save）] をクリックします。

デバイスの [設定ステータス（Configuration Status）] が [データベースの更新中（Updating Databases）] に変わります。

セキュリティデータベースの更新スケジュールの編集

FTDデバイスのセキュリティデータベースの検証および更新を実行する既存のスケジュール済みタスクを編集するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。
ステップ 3 [FTD] タブをクリックします。
ステップ 4 デバイスを選択します。
ステップ 5 [アクション（Actions）] ペインで、[セキュリティデータベースの更新（Security Database Updates）] セクションを見つけて、編集アイコン をクリックします。
ステップ 6 次の項目を使用して、スケジュールされたタスクを編集します。

- [頻度（Frequency）]。日次、週次、または 月次から更新の頻度を選択します。
- [時刻（Time）]。時刻を選択します。時刻はUTC で表示されることに注意してください。
- [曜日の選択（Select Days）]。更新を実行する曜日を選択します。

ステップ 7 [保存（Save）] をクリックします。
ステップ 8 デバイスの [設定ステータス（Configuration Status）] が [データベースの更新中（Updating Databases）] に変わります。

FTD セキュリティデータベースの更新

FTD デバイスのセキュリティデータベースを更新することにより、SRU（侵入ルール）、セキュリティインテリジェンス（SI）、脆弱性データベース（VDB）、地理位置情報データベースが更新されます。CDO UI を使用してセキュリティデータベースを更新することを選択した場合、言及されている**すべての**データベースが更新されることに注意してください。更新するデータベースを選択することはできません。

セキュリティデータベースの更新は元に戻せないことに注意してください。

（注） セキュリティデータベースを更新すると、一部のパケットがドロップされるか、検査されずに通過する場合があります。メンテナンス期間中に、セキュリティデータベースの更新をスケジュールすることをお勧めします。

オンボーディング中に FTD セキュリティデータベースを更新する

FTD デバイスを CDO にオンボーディングする場合、オンボーディングプロセスの一部を使用して、[データベースのスケジュール済み定期更新の有効化（Enable scheduled recurring updates for databases）] を実行できます。このオプションは、デフォルトでオンです。有効にすると、CDO はすぐにセキュリティの更新を確認して適用し、追加の更新を確認するようにデバイスを自動的にスケジュールします。また、デバイスがオンボードされた後は、スケジュール済みのタスクの日時を変更することもできます。

オンボーディングプロセス中に自動スケジューラを有効にして、セキュリティデータベースの更新を定期的に確認して適用することをお勧めします。この方法により、デバイスが常に最新の状態になります。FTDデバイスのオンボーディング中にセキュリティデータベースを更新するには、「登録キーを使用した FTD のオンボーディング」を参照してください。

（注） 登録キー方式でデバイスをオンボーディングする場合、デバイスをスマートライセンスに登録することは**できません**。基本ライセンスを登録するようお勧めします。別の方法として、デバイスのユーザー名、パスワード、および IP アドレスを使用してデバイスをオンボーディングすることができます。

オンボーディング後に FTD セキュリティデータベースを更新する

FTD デバイスが CDO にオンボーディングされた後、更新をスケジュールすることにより、セキュリティデータベースの更新を確認するようにデバイスを設定できます。更新がスケジュールされているデバイスを選択して、スケジュールされたタスクをいつでも変更できます。詳細については、「セキュリティデータベース更新のスケジュール設定」を参照してください。

ワークフロー

デバイスライセンス

ライセンスがない場合、CDO はセキュリティデータベースを更新できません。FTD デバイスに少なくとも基本ライセンスを適用することをお勧めします。

ライセンスのないデバイスをオンボーディングしている場合、CDOがこのデバイスをオンボーディングすることは禁止されません。代わりに、デバイスには「ライセンスが不足しています（Insufficient Licenses）」という**接続**ステータスが表示されます。この問題を解決するには、FDM の UI を使用して正しいライセンスを適用する必要があります。

（注） FTDデバイスをオンボーディングして、今後のセキュリティデータベースの更新をスケジュールすることを選択し、デバイスにライセンスが登録されていない場合でも、CDOはスケジュールされたタスクを作成しますが、適切なライセンスが適用されてデバイスが正常に同期されるまで、タスクをトリガーしません。

セキュリティデータベースの更新が FDM で保留中

FDM の UI を使用してセキュリティデータベースを更新し、デバイスで**競合検出**を有効にしている場合、CDO は保留中の更新を競合として検出します。

（注） FTDデバイスをオンボーディングし、更新をスケジュールすることを選択した場合、CDOは、次回の展開中に、保存された設定に対するその他の保留中の変更と同様に、セキュリティデータベースを自動的に更新します。**設定の展開である必要はありません。**

セキュリティデータベースの更新中に、デバイスに OOB 変更またはステージングされた変更がある

アウトオブバンド（OOB）の変更がある 、または展開されていないステージング済みの変更がある FTD デバイスのセキュリティデータベースの更新をスケジュールした場合、CDO はセキュリティデータベースのチェックと更新のみを行います。CDO は、OOB またはステージングされた変更をデプロイしません。

セキュリティデータベースを更新するためのスケジュールされたタスクがデバイスに既に存在する

各デバイスは、スケジュールされたタスクを1つだけ持つことができます。セキュリティデータベースを更新するためのスケジュールされたタスクがデバイスに既に存在する場合、新しいタスクを作成すると既存のタスクが上書きされます。これは、CDOおよびFDMで作成されたタスクの両方に適用されます。

セキュリティデータベースの更新が存在しない

更新が存在しない場合、CDO はデバイスに何も展開しません。

FTD 高可用性（HA）ペアのセキュリティデータベースの更新

セキュリティデータベースの更新は、HA ペアのプライマリデバイスにのみ適用されます。

関連情報：

- 登録キーを使用した FTD のオンボーディング
- ユーザー名、パスワード、IP アドレスを使用した FTD のオンボーディング
- セキュリティデータベース更新のスケジュール設定