Cisco Firepower 次世代ファイアウォール 6.2 ラボ v1

最終更新日:2017 年 10 月 31 日

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

注:1 回のセッションですべての演習を行うことは**お勧めしません**。すべての演習を合わせると、約 6 時間かかります。どのシナリオの演習を行うかを決める場合は、次の依存関係を参考にしてください。

- すべてのシナリオはシナリオ 1 とシナリオ 2 に依存しています。シナリオ 1 とシナリオ 2 は必須です。必ずこの順序で行ってください。
- シナリオ 3 ～ 6 では、RA VPN について詳細に取り上げています。ただし RA VPN 設定の基本を理解するだけであれば、シナリオ 3 を完了すれば十分です。
- シナリオ 13 では、シナリオ 10 のスタティック NAT 設定を使用します。

要件

次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. 要件

必須	オプション
● ラップトップ	● Cisco AnyConnect®

このソリューションについて

今日の世界では、消費者、企業、政府がデジタル化によるイノベーションを進める中で、デジタル改革によってかつてないほど接続が増大しています。しかし相互に接続が進めば、サイバー犯罪が発生する機会も増えてしまいます。こうした状況で企業を効果的に運営していくには、現在の変化の激しい脅威状況における高度な脅威を阻止することに、セキュリティ対策を集中させる必要があります。

IT チームは、旧来の次世代ファイアウォール（NGFW）を始めとするサイロ化されたポイント製品を寄せ集めて、セキュリティを管理するよう求められてきました。それらの製品はアプリケーション中心に設計され、ベスト エフォートの脅威防御に積み重ねられたものです。そのためこれらのレガシー NGFW は、現在の最新の脅威に対応するために必要なコンテキスト情報、自動化、優先順位付けを企業に提供できずにいます。常に今日の巧妙なハッカーやマルウェアの先を行くには、包括的なネットワーク可視性、脅威インテリジェンス、レトロスペクティブ セキュリティ テクノロジーによって攻撃に迅速に対応できる、完全に統合されたセキュリティ ソリューションが必要です。

Cisco Firepower 4100 シリーズ次世代ファイアウォール（NGFW）は、脅威に焦点を当てた、業界初の完全統合型次世代ファイアウォールとしてこれらの問題に対応します。

Cisco Firepower NGFW は、組織の安全を向上させることを目的に設計されています。また、単一のインターフェイスで管理の負荷を軽減しながら、完全に統合されたセキュリティを実現し、レガシー NGFW に伴うコストと複雑性も抑制します。企業はすでに拡散したセキュリティ テクノロジーの「スタック」を管理しているため、シスコは新たにアプライアンスやコンソールを追加することはしません。

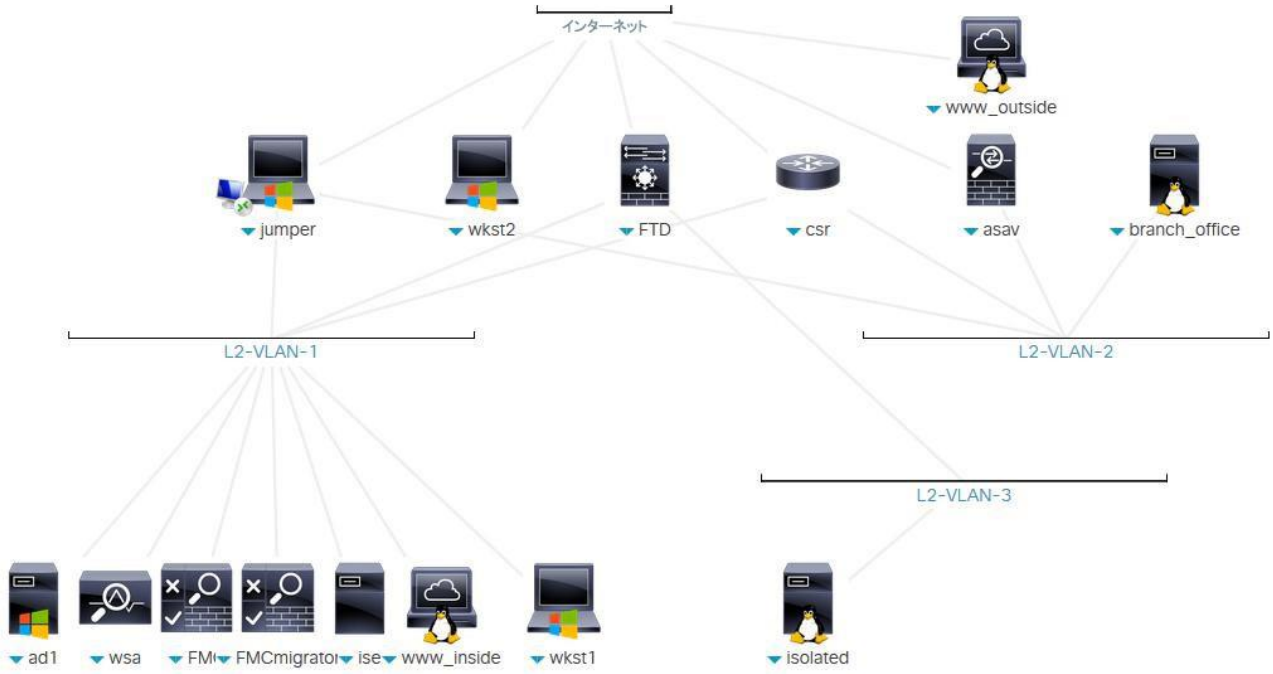
Cisco Firepower NGFW は、企業が最新の脅威に対するリアルタイムの阻止、優先順位付け、把握、対応自動化を図ることを焦点に進化することが可能です。Firepower NGFW は、包括的なネットワーク可視性、最善の脅威インテリジェンス、有効性の高い脅威防御を基盤にした脅威中心型を特徴とし、既知および未知の両方の脅威に対応します。また、Advanced Malware Protection によって、レトロスペクティブ セキュリティも可能にします。これは、防御を回避した巧妙な攻撃を「時間を遡って」迅速に特定し、修復するものです。それにより、業界の平均値に比べて検出時間（TTD）が大幅に短縮します。

Cisco Firepower NGFW は、ネットワークからエンドポイントにまで及ぶ、高度な脅威防御に関するお客様の課題にも対応します。このプラットフォームには、AMP for Endpoint、AMP Threat Grid、Cisco Identity Services Engine（ISE）がシームレスに統合されています。これにより、Firepower NGFW の優れた機能と可視性が、ネットワーク全体、そしてエンドポイントに直接適用されます。

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定されたユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント資格情報は、アクティブ セッションの [トポロジ（Topology）] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. dCloud のトポロジ



はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるためには、入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[手順を見る]

注: セッションがアクティブになるまで最長で 10 分かかることがあります。

2. Cisco dCloud リモート デスクトップ クライアントを使用してワークステーションに接続します [手順を見る] 。

注: **Cisco AnyConnect VPN** [手順を見る] **またはラップトップのローカル RDP クライアント** [手順を見る] を使用して、ワークステーションに接続することもできます。

Jumper: **198.18.133.50**、ユーザ名: **administrator**、パスワード: **C1sco12345**

シナリオ 1.　REST API によるデバイス導入

このラボでは、NGFW のシンプルな導入を行います。そのほとんどで REST API Python スクリプトを使用します。ただし、その前に必要な準備手順があります。また REST API ではルーティング設定がサポートされていないため、手動で設定する必要があります。

手順

FMC で NGFW を管理する設定にする

1. Jump Desktop で PuTTY リンクを開きます。[NGFW] という事前設定されたセッションをダブルクリックします。**admin** として、パスワード **C1sco12345** でログインします。

注：特殊文字の入力により問題が発生した場合は、Jump Desktop で *Strings to cut and paste.txt* というファイルを開きます。

2. コマンド **configure manager add fmc.dcloud.local C1sco12345** を入力します。
3. 警告を読みます。
4. 続行するかどうか尋ねられたら、「**yes**」と入力します。「**y**」とは入力しないでください。「**yes**」ではなく「**y**」と入力すると、コマンドはデフォルトの「**no**」になります。

NGFW が、オンボックス マネージャ（Firepower Device Manager（FDM））を有効にしてインストールされています。これはデフォルトの設定です。この警告が表示されたのはそのためです。このクラスではオンボックス管理のラボ演習は行いませんが、実施することは可能です。ただし、NGFW 設定を削除しないと、FMC と FDM を切り替えることはできません。

5. この PuTTY セッションは開いたままにします。これはラボ全体を通して使用します。

FMC でスマート ライセンスを有効にする

NGFW では、スマート ライセンスを使用する必要があります。このラボでは、組み込みの 90 日間の評価ライセンスを使用します。

注：このクラスではカスタマイズされたソフトウェアを使用します。実稼働用コードでは、評価ライセンスの RA VPN を導入することはできません。

1. Firefox を開き、Jump Desktop で Firepower Management Center（FMC ラベル）を開きます。ログイン名とパスワードは入力されています。
2. [ログイン（Log In）] をクリックします。
3. [システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）] に移動します。
4. [評価モード（Evaluation Mode）] をクリックし、プロンプトが表示されたら [はい（Yes）] をクリックします。

REST API スクリプトを実行して NGFW を登録/設定する

REST API の機能を確認するために、次のことを行う Python スクリプトを実行します。

1. アクセス コントロール ポリシーを作成する。
2. NGFW を FMC に登録する。
3. NGFW インターフェイスを設定する。

注:このスクリプトはトレーニングだけを目的としているため、完成されたものではありません。このスクリプトを調べるには、**/usr/local/bin** を確認します。これは **register_config.py** という名前で、**connect.py** で生成された Python モジュールを使用します。`runapiscript` コマンドは **register_config.py** に対するシンボリック リンクです。これらのスクリプトは、このガイドの付録 B にも記載されています。

4. Jump Desktop から PuTTY を起動します。[内部 Linux サーバ(Inside Linux server)] セッションをダブルクリックします。**root** として、パスワード **C1sco12345** でログインします。
5. 内部 Linux サーバの CLI で、**runapiscript** を実行します。
   a. [管理対象デバイスを登録しますか? [y/n](Would you like to register the managed device? [y/n])] と表示されたら、「**y**」と入力して **<Return>** を押します。
   b. [アクセス コントロール ポリシー名を入力(enter an access control policy name)] と表示されたら、**NGFW Access Control Policy** などの意味のある名前を入力します。
   c. 確認メッセージが表示されるまで待ちます。
   d. FMC UI でデバイス検出が完了したことを確認したら、**y** を押して続行するか、**n** を押して終了します。[y/n]
   e. スクリプトを続行する前に、次の手順を実行します。

注:検出が完了するまで待たないとエラーが発生します。その場合は、検出が完了するまで待ってから、スクリプトを再度実行します。ただし今度は、デバイスを登録するかどうか尋ねられたら「n」を入力します。

6. FMC で、[導入(Deploy)] ボタンの右にあるアイコンをクリックし、[タスク(Tasks)] タブを選択します。
   a. しばらく待ちます。タスクが開始するまで 1 分かかる場合があります。

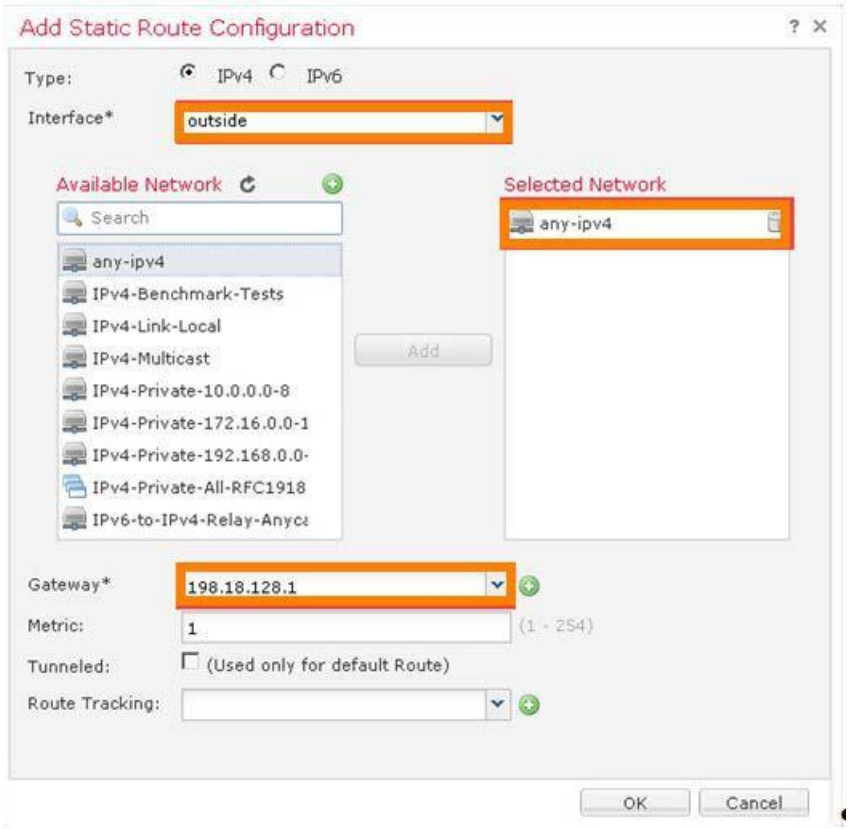
注:1 分を過ぎてもタスクが開始されない場合は、デモ スマート ライセンスが有効になっていることを確認してください。有効でなければ有効にして、**runapiscript** スクリプトを再度実行します。アクセス コントロール ポリシーには別の名前を使用するか、スクリプトによって作成されたポリシーを削除してください。

   b. 検出タスクが完了するまで待ちます。失敗したタスクは無視することができます。重要なのは、登録と検出が完了することです。

7. 内部 Linux サーバの CLI で、**runapiscript** スクリプトを続行します。
    a. 「**y**」と入力して **<Return>** を押します。
    b. [デバイスのインターフェイスを設定しますか? [y/n]（Would you like to configure device interfaces? [y/n]）] と表示されたら、「**y**」と入力して **<Return>** を押します。スクリプトが完了するまで待機します。
    c. この PuTTY セッションは開いたままにします。これはラボ全体を通して使用します。

デフォルト ルートを設定する

1. FMC で、[デバイス（Devices）] > [デバイス管理（Device Management）] に移動します。鉛筆アイコンをクリックして、デバイス設定を編集します。
2. [インターフェイス（Interfaces）] タブが選択されているはずです。REST API スクリプトによって、NGFW の内部インターフェイスと外部インターフェイスが設定されたことを確認します。
3. [ルーティング（Routing）] タブを選択します。
    a. [スタティックルート（Static Route）] を選択し、[ルートの追加（Add Route）] ボタンをクリックします。
    b. 次の図に示すように、外部インターフェイスでデフォルト ルートを **198.18.128.1** に設定します。
    c. [OK] をクリックします。



4. [保存（Save）] をクリックして、ルーティング設定を保存します。

注：時間を節約するために、ルーティング設定はまだ導入しないでください。また、時間を節約するために、**runapiscript** スクリプトにはインターフェイス設定の導入は含まれていません。次のラボ演習ではさらに設定手順を進め、すべての設定変更を合わせて導入します。

シナリオ 2.　基本設定

この演習は、次のタスクで構成されています。

- 演習に必要なオブジェクトを作成する
- アクセス コントロール ポリシーを変更する
- NAT ポリシーを作成する
- ネットワーク検出ポリシーを変更する
- 設定変更を導入する
- NGFW 設定をテストする
- アウトバウンド接続を許可し、他の接続試行をブロックする
- これらのアウトバウンド接続でファイル タイプ ブロックとマルウェア ブロックを実行する
- これらのアウトバウンド接続で侵入防御を可能にする

手順

演習に必要なオブジェクトを作成する

1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動します。
    a. [ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）] の順にクリックします。
    b. [名前（Name）] に「**Lab_Networks**」と入力します。
    c. 「`198.18.0.0/15`」と入力します。これには、ラボ ポッドで使用するすべての IP アドレスが含まれています。
    d. [保存（Save）] をクリックします。
2. 左側のナビゲーション パネルで、[インターフェイス（Interface）] を選択します。
    a. [追加（Add）] > [セキュリティ ゾーン（Security Zone）] の順にクリックします。

注：インターフェイス オブジェクトには、セキュリティ ゾーンとインターフェイス グループの 2 つのタイプがあります。主な違いは、インターフェイス グループが重複可能な点です。セキュリティ ゾーンは、アクセス コントロール ポリシー ルールでのみ使用できます。

    b. [名前（Name）] に「**InZone**」と入力します。[インターフェイス タイプ（Interface Type）] ドロップダウン メニューから [ルーテッド（Routed）] を選択します。
    c. 内部インターフェイスを選択します。[追加（Add）] をクリックし、次に [保存（Save）] をクリックします。
    d. [追加（Add）] > [セキュリティ ゾーン（Security Zone）] の順にクリックします。
    e. [名前（Name）] に「**OutZone**」と入力します。[インターフェイス タイプ（Interface Type）] ドロップダウン メニューから [ルーテッド（Routed）] を選択します。
    f. 外部インターフェイスを選択します。[追加（Add）] をクリックし、次に [保存（Save）] をクリックします。

アクセス コントロール ポリシーを変更する

1. [ポリシー(Policies)] > [アクセス制御(Access Control)] > [アクセス制御(Access Control)] の順に選択します。REST API スクリプトによってアクセス コントロール ポリシーが作成されました。
2. ポリシーの右にある**鉛筆アイコン**をクリックして、アクセス コントロール ポリシーを編集します。
3. [ルールの追加(Add Rule)] をクリックします。
    a. [名前(Name)] に「**Allow Outbound Connections**」と入力します。
    b. [挿入(Insert)] ドロップダウン リストから [デフォルトに挿入(into Default)] を選択します。

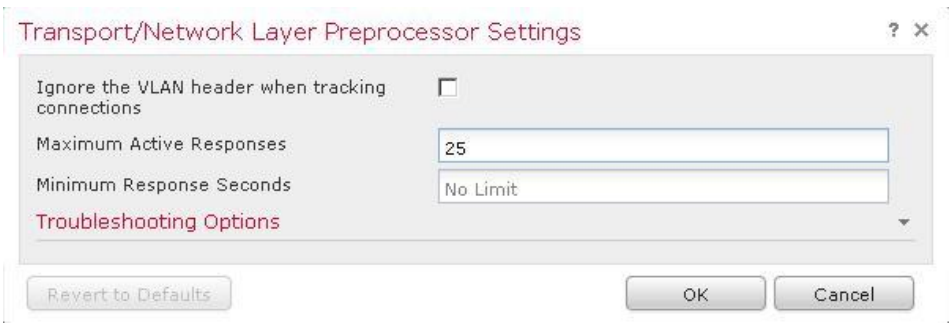
注:ルールは、ポリシー内の複数のセットに分割されます。2 つのセットが事前定義されています。
• 必須ルールは、子ポリシーのルールに優先します。
• デフォルト ルールは、子ポリシーのルールの後に評価されます。

この演習では子ポリシーは作成しませんが、このルールが最後に評価されるようにする簡単な方法として、デフォルト ルール セットを使用します。

    c. [ゾーン(Zones)] タブがすでに選択されているはずです。
        i. [InZone] を選択し、[送信元に追加(Add to Source)] をクリックします。
        ii. [OutZone] を選択し、[宛先に追加(Add to Destination)] をクリックします。
    d. [検査(Inspection)] タブを選択します。
        i. [侵入ポリシー(Intrusion Policy)] ドロップダウン リストから [デモ侵入ポリシー(Demo Intrusion Policy)] を選択します。
        ii. [ファイル ポリシー(File Policy)] ドロップダウン リストから [デモ ファイル ポリシー(Demo File Policy)] を選択します。

注:デモ侵入ポリシーおよびデモ ファイル ポリシーは、時間を節約するために、事前に設定されています。これらを作成する方法については、付録 A を参照してください。

    e. [追加(Add)] をクリックしてルールを追加します。
4. [HTTP 応答(HTTP Responses)] タブを選択します。
5. [ブロック応答ページ(Block Response Page)] ドロップダウン リストから [システムにより設定(System-provided)] を選択します。
6. [詳細設定(Advanced)] タブを選択します。
    a. **鉛筆アイコン**をクリックして、[トランスポート/ネットワーク層のプリプロセッサ設定(Transport/Network Layer Preprocessor Settings)] を編集します。
    b. [アクティブな応答の最大数(Maximum Active Responses)] テキスト フィールドに「**25**」と入力します。
    c. [OK] をクリックします。



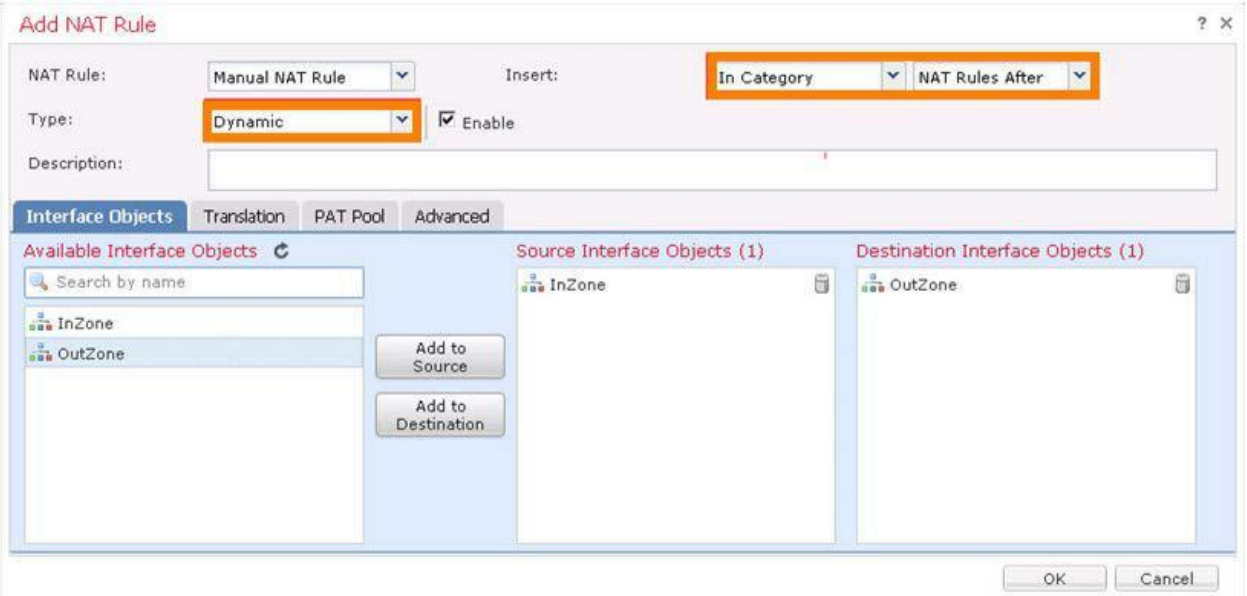
注:[アクティブな応答の最大数(Maximum Active Responses)] を 0 より大きい値に設定すると、パケットをドロップして TCP リセットを送信し、接続を終了するルールが有効になります。通常、クライアントとサーバの両方に TCP リセットが送信されます。以上のように設定すると、この接続を通じたトラフィックが追加された場合に、最大 25 のアクティブな応答(TCP リセット)が開始されます。

実稼働環境では、この設定はデフォルトのままにしておくことをお勧めします。そうすればリセットが送信されず、悪意のあるシステムは検出されたことを認識しません。ただし、テストとデモンストレーションでは、一般に、パケットがドロップ ルールに一致する場合はリセットを送信することをお勧めします。

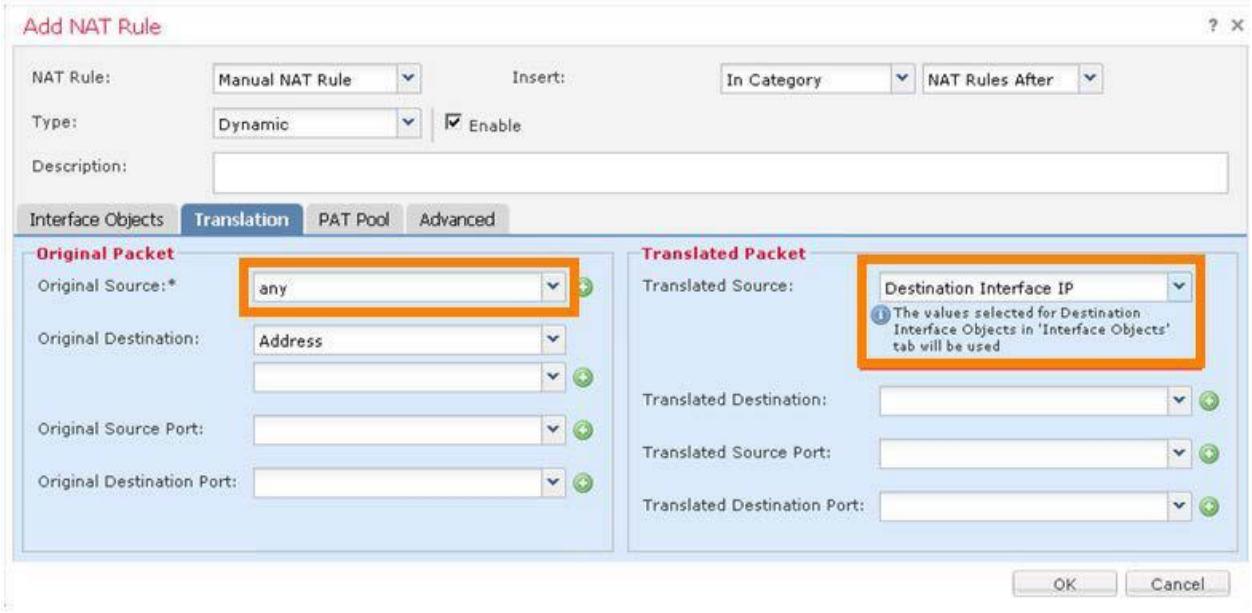
7. [保存(Save)] をクリックして、アクセス コントロール ポリシーの変更を保存します。

NAT ポリシーを作成する

1. [デバイス(Devices)] > [NAT] に移動します。
2. [新しいポリシー(New Policy)] ボタンをクリックし、[脅威防御 NAT(Threat Defense NAT)] を選択します。
    a. [名前(Name)] に「**Default PAT**」と入力します。
    b. [NGFW] を選択します。[ポリシーに追加(Add to Policy)] をクリックし、次に [保存(Save)] をクリックします。
    c. ポリシーが開き、編集できるようになります。
3. [ルールの追加(Add Rule)] をクリックします。
    a. [挿入(Insert)] ドロップダウン リストから [カテゴリに挿入(In Category)] と [次の後の NAT ルール(NAT Rules After)] を選択します。これによって、このルールが自動 NAT(オブジェクト NAT)ルールの後に評価されるようになります。
    b. [タイプ(Type)] ドロップダウン リストから [ダイナミック(Dynamic)] を選択します。
    c. [インターフェイス オブジェクト(Interface Objects)] タブが表示されます。[InZone] を選択し、[送信元に追加(Add to Source)] をクリックします。
    d. [OutZone] を選択し、[宛先に追加(Add to Destination)] をクリックします。



    e. [トランスレーション(Translation)] タブを選択します。
    f. [元の送信元(Original Source)] ドロップダウン リストから [任意(any)] を選択します。
    g. [変換済み送信元(Translated Source)] ドロップダウン リストから [宛先インターフェイス IP(Destination Interface IP)] を選択します。
    h. [OK] をクリックして NAT ルールを保存します。

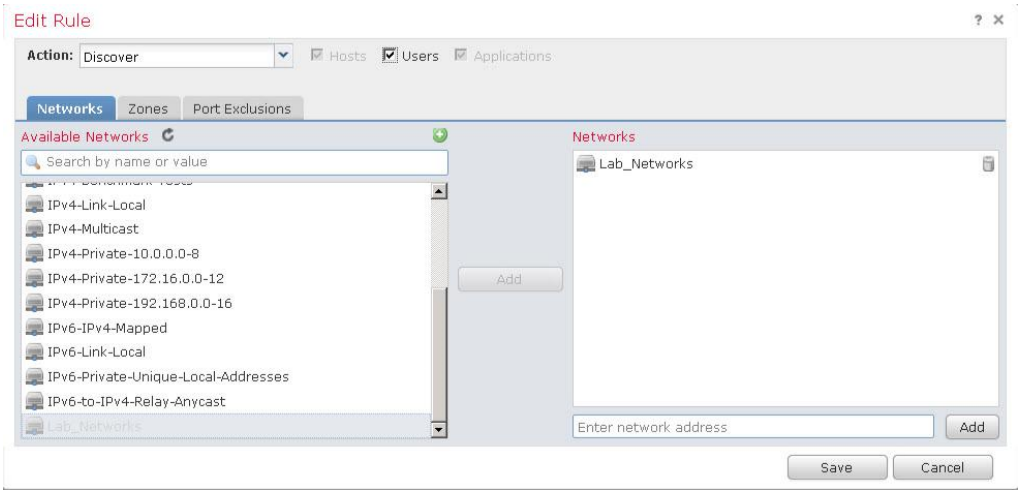


4. [保存(Save)] をクリックして NAT ポリシーを保存します。

ネットワーク検出ポリシーを変更する

デフォルトのネットワーク検出ポリシーは、内部と外部のすべてのアプリケーションを検出するように設定されています。ここにホストとユーザの検出を追加します。実稼働環境では、これにより FMC FirePOWER ホスト ライセンス数を超える場合があります。そのため、ポリシーを変更するのが適切です。

1. [ポリシー(Policies)] > [ネットワーク検出(Network Discovery)] の順に選択します。
    a. 既存のルールを編集するには、右側の**鉛筆アイコン**をクリックします。
    b. [ユーザ(Users)] チェックボックスをオンにします。[ホスト(Hosts)] チェックボックスが自動的にオンになります。
    c. [0.0.0.0/0] と [::/0] の両方を削除します。
2. [Lab_Networks] ネットワークを選択し、[追加(Add)] をクリックします。



3. [保存(Save)] をクリックします。

設定変更を導入する

1. FMC の右上隅の [導入（Deploy）] をクリックします。

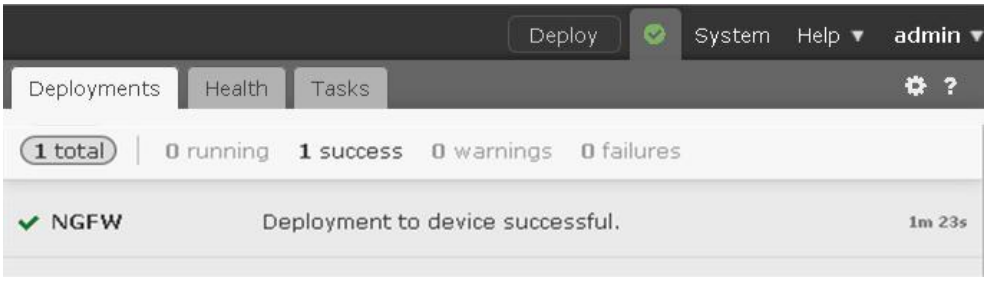
    a. NGFW デバイスのチェックボックスをオンにし、リストを展開して詳細を表示します。

    b. [デバイス設定（Device Configuration）] の右側にある [詳細（Details）] をマウス オーバーします。ページは次の図のようになります。

    c. **NGFW 設定**、NAT ポリシー ネットワーク検出、インターフェイスおよびスタティック ルート設定が変更されることを確認します。

    d. [導入（Deploy）] ボタンをクリックします。

    e. FMC の右上隅にある [導入（Deploy）] リンクの右の**アイコン**をクリックします。導入が完了するまで待ちます。



NGFW の導入をテストする

1. **内部 Linux サーバ**の CLI で次を実行します。
    a. 「**`wget cisco.com`**」と入力します。これは成功するはずです。これで、NAT とルーティングは確認できました。
    b. 「**`ping outside`**」と入力します。これは成功するはずです。Ctrl+C を押して ping を終了します。
    c. 「**`ftp outside`**」と入力します。**`guest`** として、パスワード **`C1sco12345`** でログインします。
    d. 「**`cd ~root`**」と入力します。次のメッセージが表示されます:[421 サービスが使用できません。リモート サーバは接続を閉じています(421 Service not available, remote server has closed connection)]。これで、IPS が機能していることを確認できます。

注:FTP セッションがハングした場合は、アクセス コントロール ポリシーでアクティブな応答を有効にしていない可能性があります。この動作を想定していれば、修正する必要はありません。

    e. 「**`quit`**」と入力して、FTP を終了します。

2. FMC で、[分析(Analysis)] > [侵入(Intrusions)]> [イベント(Events)] に移動します。

注:**Snort ルール 336 がトリガーされたこと**を確認します。[デモ侵入ポリシー(Demo Intrusion Policy)] で、このルールのルール状態は [イベントをドロップして生成(Drop and Generate Events)] に設定されています。このルールは、[バランスのとれたセキュリティと接続(Balanced Security and Connectivity)] など、システム定義の侵入ポリシーでは無効になっています。

注:実稼働環境で、イベントが表示されない状況が発生した場合は、最初に NGFW と FMC 間の時刻同期を確認します。ただし、このラボでは、イベント プロセスの問題である可能性があります。その場合は、次の手順で、これらのプロセスの再起動を試みてください。
NGFW CLI で、次のコマンドを実行します。

```
pmtool restartbytype EventProcessor
```

Jump Desktop から、事前定義されている PuTTY セッションを使用して FMC に接続します。「admin/FPlab123!」としてログインし、次のコマンドを実行します。

```
sudo pmtool restartbyid SFDataCorrelator
sudo pmtool restartbyid sftunnel
```

sudo のパスワードは **`FPlab123!`** です。

    a. 左側の**矢印をクリック**して、イベントのテーブル ビューにドリルダウンします。イベントの詳細が存在することを確認します。
    b. イベントの左側にある**矢印をクリック**して、さらにドリル ダウンします。Snort ルールの詳細を含む広範な情報が得られる点に注意してください。
    c. [アクション(Actions)] を展開すると、ここからルールを無効にできることがわかりますが、無効にはしないでください。
    d. [パケット バイト数(Packet Bytes)] を展開すると、ルールをトリガーしたパケットのコンテンツが表示されます。

3. ファイル ブロックおよびマルウェア ブロック機能をテストします。これらの Wget コマンドは、Jump Desktop の Strings というファイルからカットして貼り付けることができます。

    a. 制御テストとして、**WGET を使用して**、ブロックされていないファイルをダウンロードします。
    `wget -t 1 outside/files/ProjectX.pdf`
    これは成功するはずです。

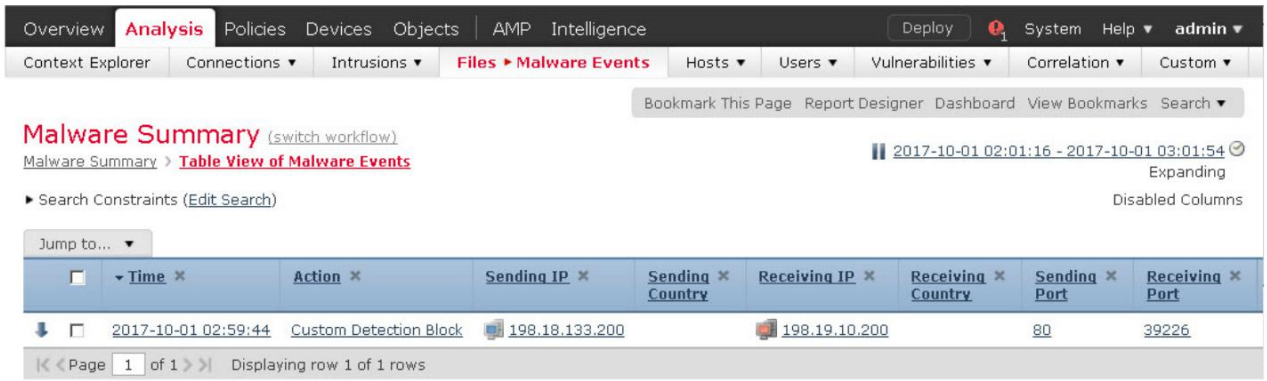
    b. 次に、タイプによってブロックされたファイルに対して **WGET を使用してダウンロードを試み**ます。
    `wget -t 1 outside/files/test3.avi`
    ファイルのごく一部しかダウンロードされないことに注意してください。これは、NGFW が、データの最初のブロックからファイル タイプを検出できるためです。デモ ファイル ポリシーは、AVI ファイルをブロックするように設定されています。

    c. 最後に、**WGET を使用してマルウェアのダウンロードを試み**ます。
    `wget -t 1 outside/files/Zombies.pdf`
    ファイルの 99 % がダウンロードされたことに注意してください。これは、NGRW が SHA の計算にファイル全体を必要とするためです。ハッシュが計算され、ルックアップされるまで、NGFW はデータの最後のブロックのダウンロードを保留します。デモ ファイル ポリシーは、PDF ファイルで検出されたマルウェアをブロックするように設定されています。

4. FMC で、[分析（Analysis）] > [ファイル（Files）] > [マルウェア イベント（Malware Events）] に移動します。

    a. 1 つのファイル、Zombies.pdf がブロックされたことを確認します。

    b. 左側の矢印をクリックして、イベントのテーブル ビューにドリルダウンします。ホスト **198.19.10.200** が赤色のアイコンで表されている点に注意してください。これは内部 Linux サーバです。赤色のアイコンは、ホストに侵入の痕跡が割り当てられていることを意味します。

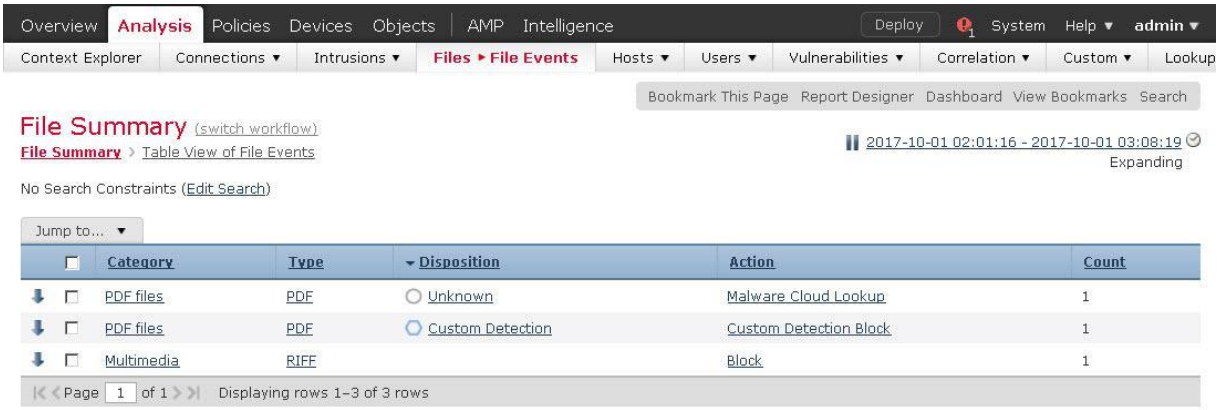


注：このアクションは、[マルウェアブロック（Malware Block）] ではなく、[カスタム検出ブロック（Custom Detection Block）] としてレポートされます。これは、カスタム検出リストに Zombies.pdf を追加したためで、ラボがクラウドに接続されている場合にのみ発生します。詳細については、付録 A を参照してください。

必要に応じて、以下を試行できます。
`wget -t 1 outside/malware/Buddy.exe`
これは [マルウェアブロック（Malware Block）] としてレポートされます。ただし、この特定のラボ環境では、クラウド ルックアップが失敗する場合があり、そのため、ファイルがブロックされないことがあります。

5. **赤色のコンピュータ アイコンをクリックします**。これにより、ホスト プロファイル ページが開きます。このページを確認してから、閉じます。

6. [分析（Analysis）] > [ファイル（Files）] > [ファイル イベント（File Events）] に移動します。3 つすべてのファイル イベントに関する情報が表示されます。



必要に応じてより詳細な情報にドリル ダウンできます。

シナリオ 3.　AnyConnect リモート アクセス VPN

この演習は、次のタスクで構成されています。

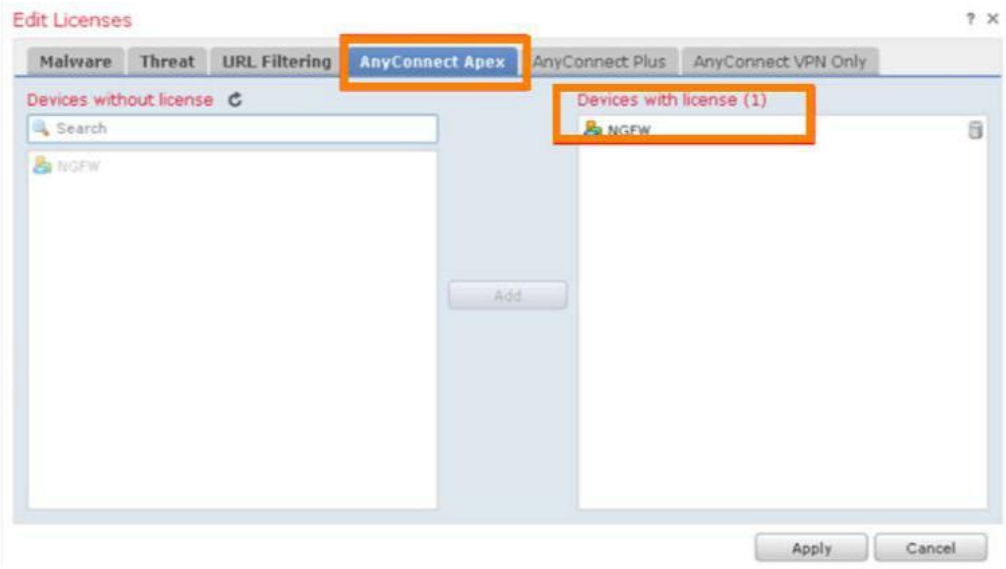
- AnyConnect スマート ライセンスを有効にする
- AnyConnect RA VPN オブジェクトを作成する
- デフォルトのグループ ポリシーを変更する
- RA VPN ウィザードを実行する
- デバイスの証明書を設定する
- アクセス コントロール ポリシーを変更して AnyConnect インバウンド アクセスを許可する
- NAT 適用除外を設定する
- VPN ロギングを設定する
- NGFW RA VPN 設定を導入し確認する
- 設定をテストする

この演習の目的は、Cisco Firepower NGFW で使用できる AnyConnect リモート アクセス VPN 機能について理解し、設定することです。

手順

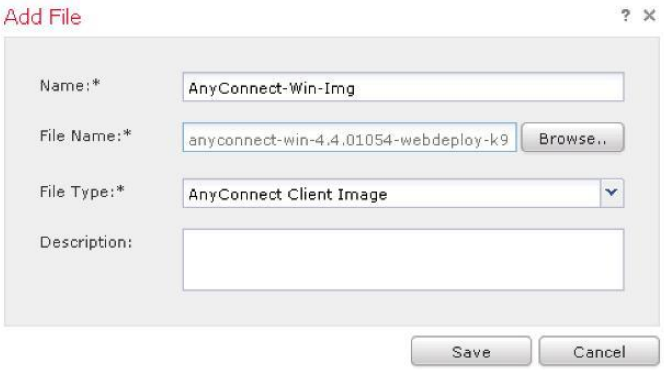
AnyConnect スマート ライセンスを有効にする

1. FMC で、[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）] に移動します。
    a. [ライセンスの編集（Edit Licenses）] をクリックします。
    b. [ライセンスの編集（Edit Licenses）] ウィンドウで、[AnyConnect Apex] タブを選択します。
    c. **NGFW** デバイスを選択します。[追加（Add）]、[適用（Apply）] の順にクリックします。

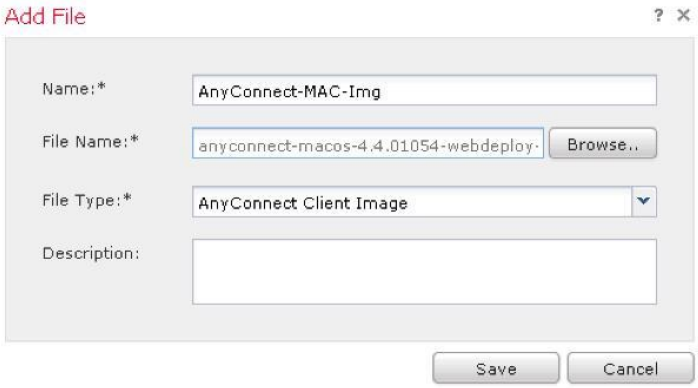


AnyConnect RA VPN オブジェクトを作成する

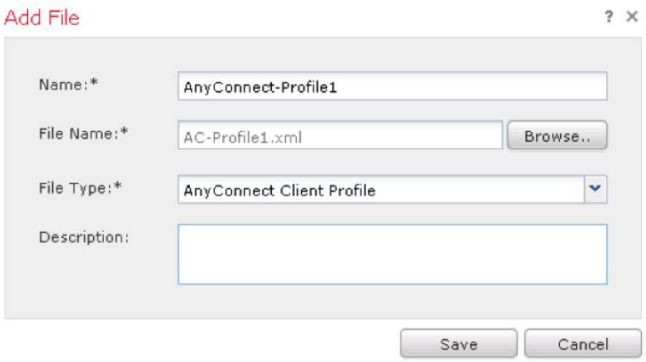
1. Windows 用の AnyConnect イメージ オブジェクトを作成します。
    a. FMC で、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [AnyConnect ファイル（AnyConnect File）] に移動します。
    b. [AnyConnect ファイルの追加（Add AnyConnect File）] をクリックします。
    c. [名前（Name）] に「**`AnyConnect-Win-Img`**」と入力します。
    d. [参照（Browse）] をクリックし、Jump Desktop の **RA VPN** フォルダに移動します。
    e. **anyconnect-win-4.4.01054-webdeploy-k9.pkg** ファイルを選択します。
    f. [開く（Open）] をクリックします。[ファイル タイプ（File Type）] テキスト フィールドには、正しい値が事前に入力されています。
    g. [保存（Save）] をクリックします。



2. MAC OS 用に別の AnyConnect イメージ オブジェクトを作成します。
    a. [AnyConnect ファイルの追加（Add AnyConnect File）] をクリックします。
    b. [名前（Name）] に「**`AnyConnect-MAC-Img`**」と入力します。
    c. [参照（Browse）] をクリックし、Jump Desktop の **RA VPN** フォルダから **anyconnect-macos-4.4.01054-webdeploy-k9.pkg** ファイルを選択します。
    d. [開く（Open）] をクリックします。[ファイル タイプ（File Type）] テキスト フィールドには、正しい値が事前に入力されています。
    e. [保存（Save）] をクリックします。

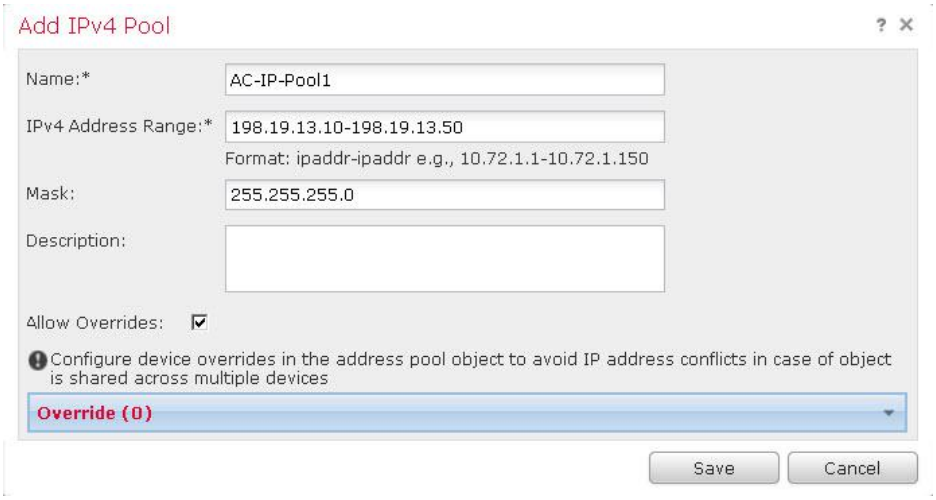


3. AnyConnect クライアント プロファイル オブジェクトを作成します。
    a. [AnyConnect ファイルの追加（Add AnyConnect File）] をクリックします。
    b. [名前（Name）] に「**AnyConnect-Profile1**」と入力します。
    c. [参照（Browse）] をクリックし、Jump Desktop の **RA VPN** フォルダから **AC-Profile1.xml** ファイルを選択します。
    d. [開く（Open）] をクリックします。[ファイル タイプ（File Type）] テキスト フィールドには、正しい値が事前に入力されています。
    e. [保存（Save）] をクリックします。

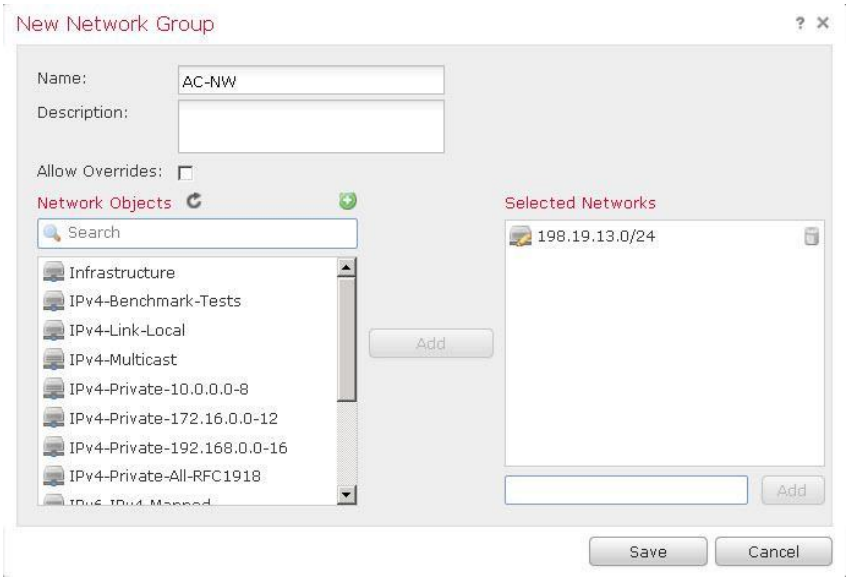


注：cisco.com にある *VPN Profile Editor* ツールを使用して、AnyConnect クライアント プロファイルを作成できます。*VPN Profile Editor* ツールは、Jump でも使用できます。[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect profile editor）] > [VPN Profile Editor] の順に選択してアクセスできます。

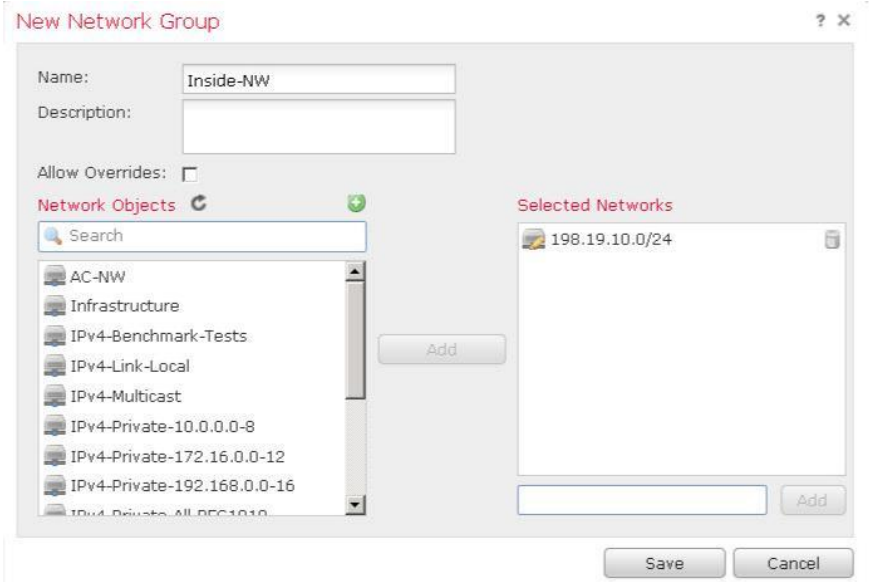
4. IP プールを作成します。
    a. FMC で、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレス プール（Address Pools）] > [IPv4 プール（IPv4 Pools）] に移動します。
    b. [IPv4 プールの追加（Add IPv4 Pools）] をクリックします。
    c. [名前（Name）] に「**AC-IP-Pool1**」と入力します。
    d. [IPv4 アドレス範囲（IPv4 Address Range）] に「**198.19.13.10-198.19.13.50**」と入力します。
    e. [マスク（Mask）] に「**255.255.255.0**」と入力します。
    f. [保存（Save）] をクリックします。



5. IPv4 プールに対応するネットワーク オブジェクトを作成します。
    a. FMC で、[オブジェクト(Object)]> [オブジェクト管理(Object Management)] > [ネットワーク(Network)] に移動します。
    b. [ネットワークの追加(Add Network)] をクリックし、[グループの追加(Add Group)] を選択します。
    c. [名前(Name)] に「**AC-NW**」と入力します。
    d. 下部にあるテキスト フィールドの [選択したネットワーク(Selected Networks)] に「**198.19.13.0/24**」と入力し、[追加(Add)] をクリックします。
    e. [保存(Save)] をクリックします。

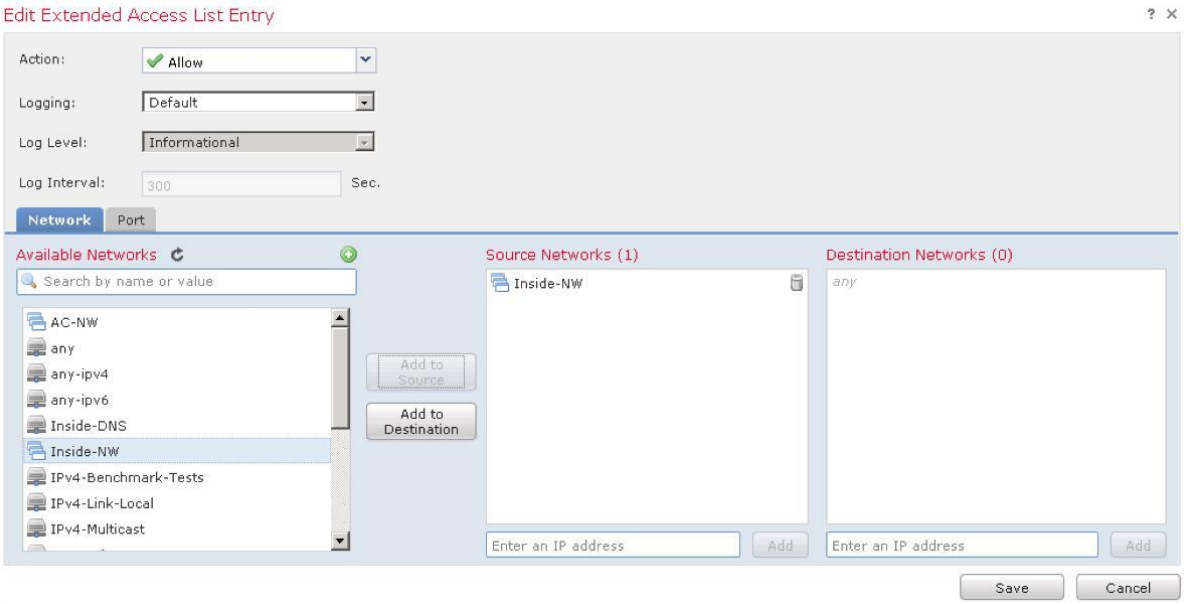


6. 内部ネットワーク用のネットワーク オブジェクトを作成します。
    a. [ネットワークの追加(Add Network)] をクリックし、[グループの追加(Add Group)] を選択します。
    b. [名前(Name)] に「**Inside-NW**」と入力します。
    c. 下部にあるテキスト フィールドの [選択したネットワーク(Selected Networks)] に「**198.19.10.0/24**」と入力し、[追加(Add)] をクリックします。
    d. [保存(Save)] をクリックします。

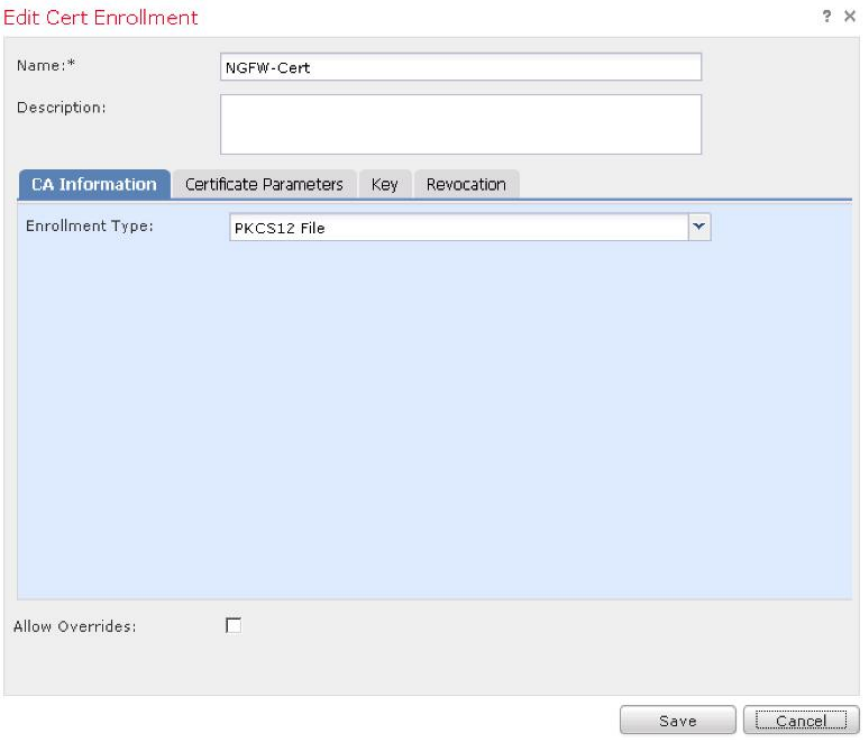


注:ネットワーク オブジェクトではなくネットワーク オブジェクト グループを使用するように指示されるのには理由があります。次のラボ演習では別のサブネットを追加します。ネットワーク グループを使用しているため、必要になるのはこのオブジェクトを変更することだけです。アクセス コントロール ポリシーと NAT ポリシーを直接変更する必要はありません。

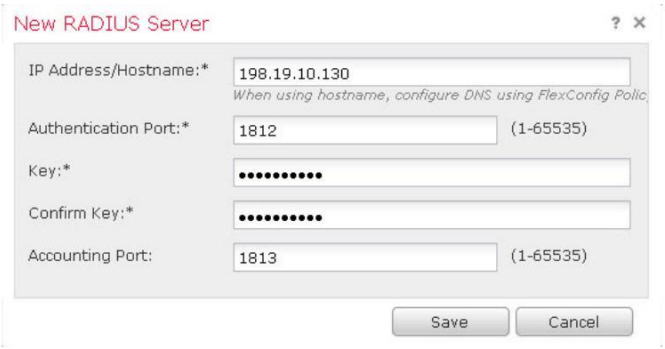
7. RA VPN スプリット トンネル設定用の ACL を作成します。
    a. FMC で、[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] > [アクセス リスト(Access List)] > [拡張(Extended)] に移動します。
    b. [拡張アクセス リストの追加(Add Extended Access List)] をクリックします。
    c. [名前(Name)] に「**AC-SplitTunnel1**」と入力します。
    d. [追加(Add)] をクリックします。
    e. [使用可能なネットワーク(Available Networks)] から [Inside-NW] を選択し、[送信元に追加(Add to Source)] をクリックします。
    f. [追加(Add)] をクリックします。
    g. [保存(Save)] をクリックします。



8. デバイス証明書オブジェクトを作成します。
    a. FMC で、[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] > [PKI] > [証明書の登録(Cert Enrollment)] に移動します。
    b. [証明書の登録の追加(Add Cert Enrollment)] をクリックします。
    c. [名前(Name)] に「**NGFW-Cert**」と入力します。
    d. [登録タイプ(Enrollment Type)] で、[PKCS12 ファイル(PKCS12 File)] を選択します。
    e. [保存(Save)] をクリックします。



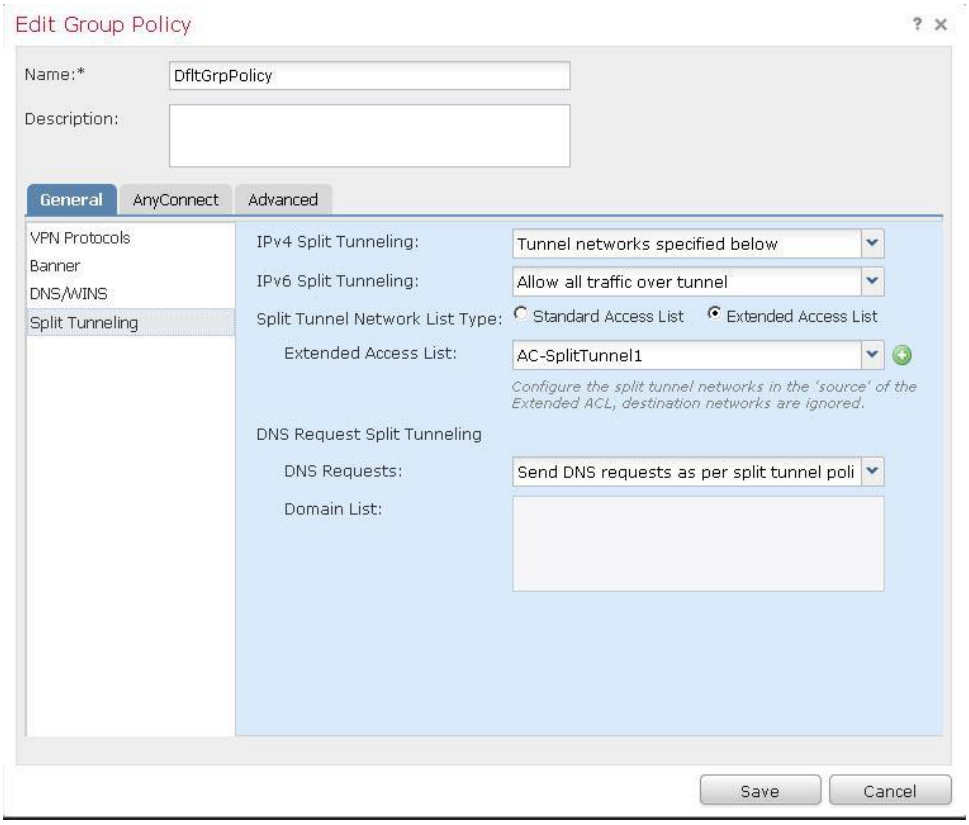
9. ISE RADIUS サーバ用のオブジェクトを作成します。
    a. FMC で、[オブジェクト(Object)] > [オブジェクト管理(Object Management)] > [RADIUS サーバ グループ(RADIUS Server Group)] に移動します。
    b. [RADIUS サーバ グループの追加(Add RADIUS Server Group)] をクリックします。
    c. [名前(Name)] に「**ISE-AAA**」と入力します。
    d. [RADIUS サーバ(RADIUS Servers)] セクションの [+] アイコンをクリックします。
    e. [IP アドレス(IP Address)] に「**198.19.10.130**」と入力します。
    f. [キー(Key)] と [キーの確認(Confirm Key)] に、「**C1sco12345**」と入力します。
    g. [新規 RADIUS サーバ(New RADIUS Server)] ページで [保存(Save)] をクリックします。
    h. [RADIUS サーバ グループの追加(Add RADIUS Server Group)] ページで [保存(Save)] をクリックします。



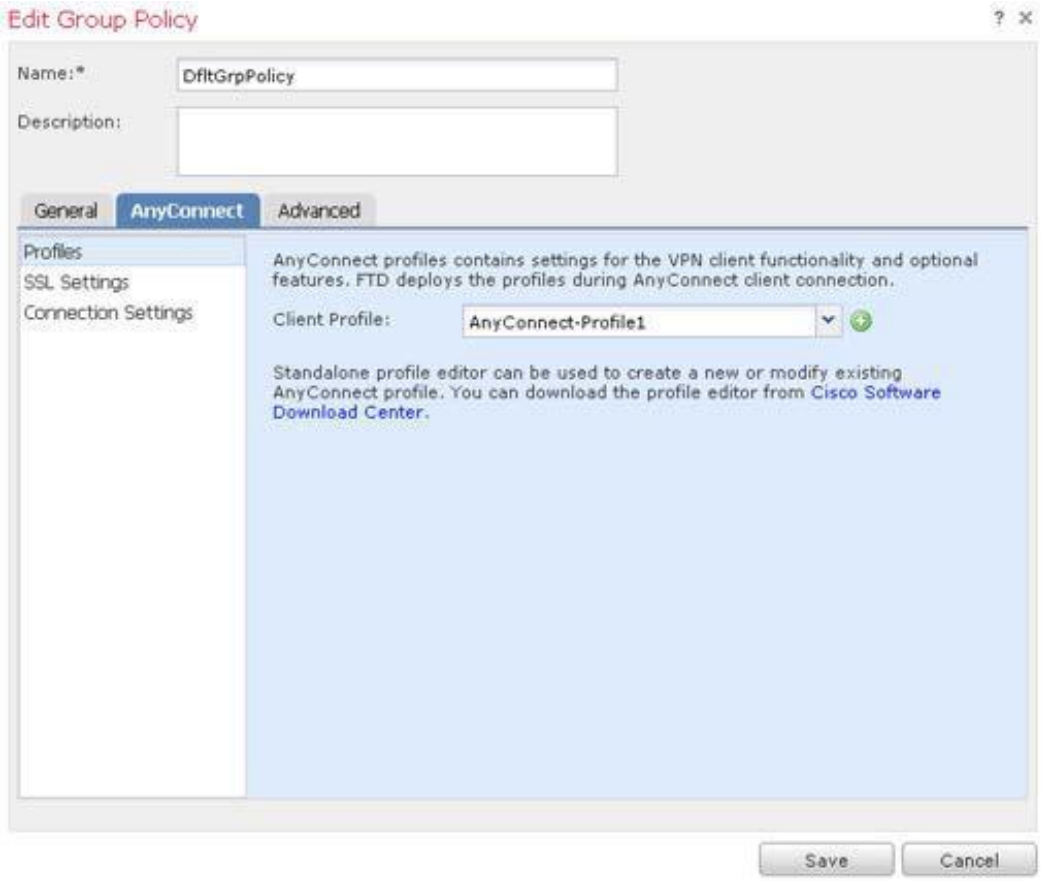
注:時間を節約するために、ISE では、ラボ演習で必要な設定が事前にすべて設定されています。ISE 設定を確認するには、付録 C を参照してください。

デフォルトのグループ ポリシーを変更する

1. FMC で、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）] に移動します。
2. [DfltGrpPolicy] を選択して編集します。
3. [全般（General）] タブで、[スプリット トンネリング（Split Tunneling）] を選択します。
    a. [IPv4 スプリット トンネリング（IPv4 Split Tunneling）] で、[以下に指定されたトンネル ネットワーク（Tunnel networks specified below）] を選択します。
    b. [拡張アクセス リスト（Extended Access List）] オプション ボタンを選択します。
    c. [アクセス リスト（Access List）] で、[AC-SplitTunnel1] を選択します。



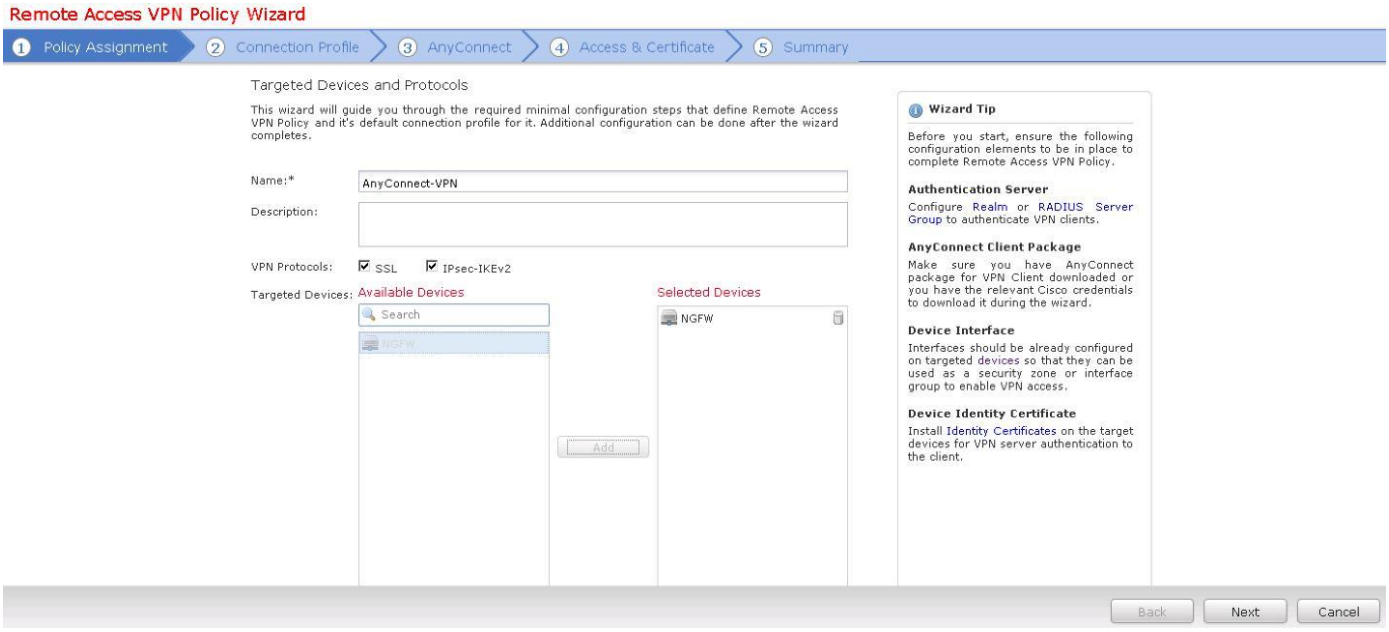
4. [全般（General）] タブで、[DNS/WINS] を選択します。
    a. [プライマリ DNS サーバ（Primary DNS Server）] で [+] アイコンをクリックします。
    b. [名前（Name）] に「**Inside-DNS**」と入力します。
    c. [ネットワーク（Network）] に「**198.19.10.100**」と入力します。
    d. [保存（Save）] をクリックします。
5. [AnyConnect] タブを選択します。[クライアント プロファイル（Client Profile）] で、[AnyConnect-Profile1] を選択します。



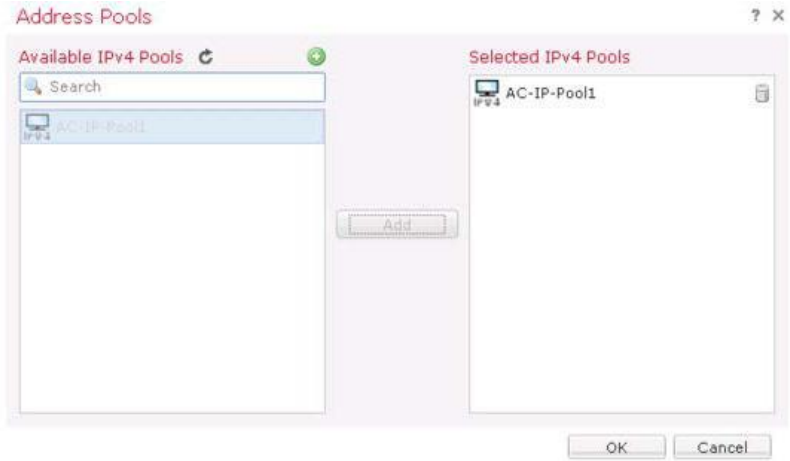
6. [保存（Save）] をクリックして、グループ ポリシーの変更を保存します。

RA VPN ウィザードを実行する

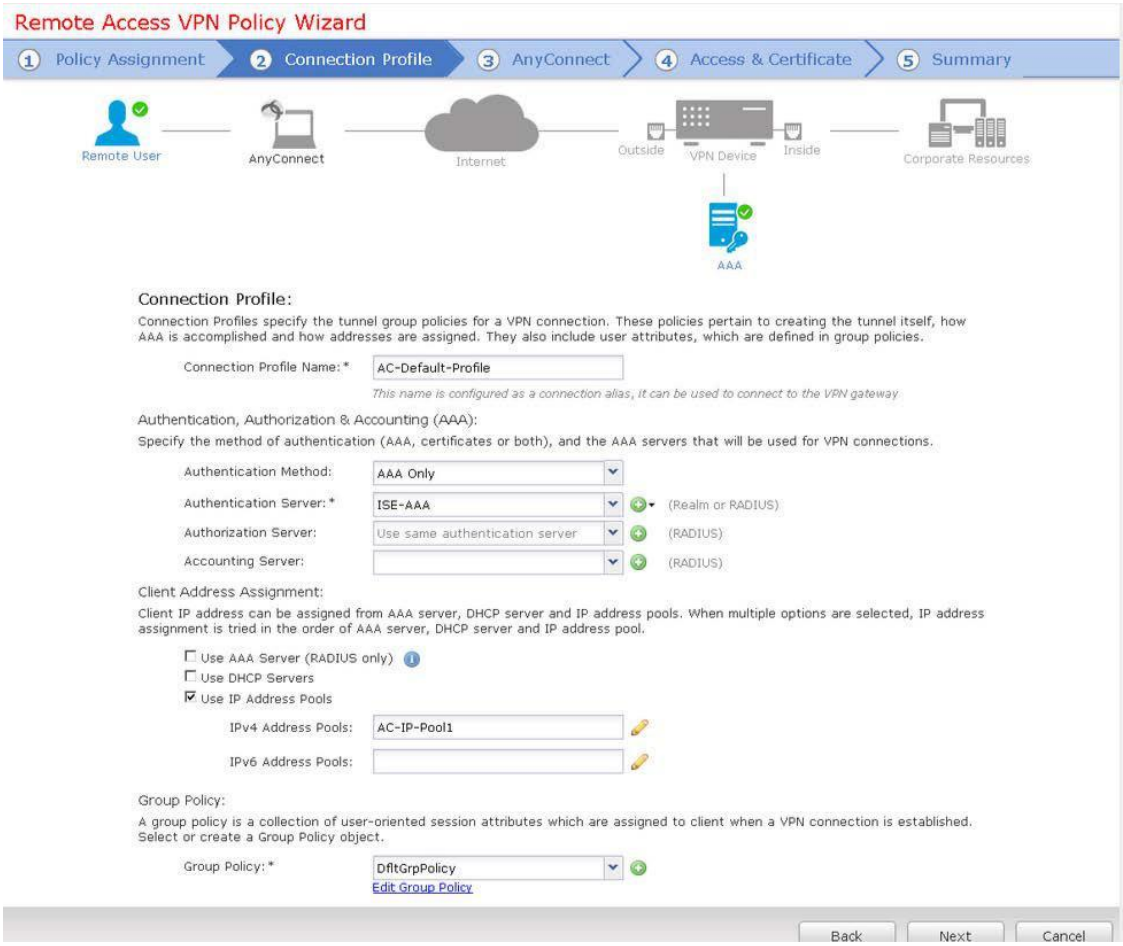
1. FMC で、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] に移動します。[追加（Add）] をクリックします。ウィザードが起動します。
2. ウィザードの [ポリシー割り当て（Policy Assignment）] ページに入力します。
    a. [名前（Name）] に「**AnyConnect-VPN**」と入力します。
    b. [ターゲット デバイス（Target Device）] から [NGFW] を選択します。[追加（Add）] をクリックします。
    c. [次へ（Next）] をクリックします。



3. ウィザードの [接続プロファイル（Connection Profile）] ページに入力します。
    a. [接続プロファイル名（Connection Profile Name）] に「**AC-Default-Profile**」と入力します。
    b. [認証方式（Authentication Method）] で [AAA のみ（AAA Only）] が選択されていることを確認します。
    c. [認証サーバ（Authentication Server）] で [ISE-AAA] を選択します。
    d. [アドレス プール（Address Pools）] で、[IPv4 アドレス プール（IPv4 Address Pools）] を編集します。
    e. [IPv4 アドレス プール（IPv4 Address Pools）] から [AC-IP Pool1] を選択します。[追加（Add）] をクリックし、[OK] をクリックします。



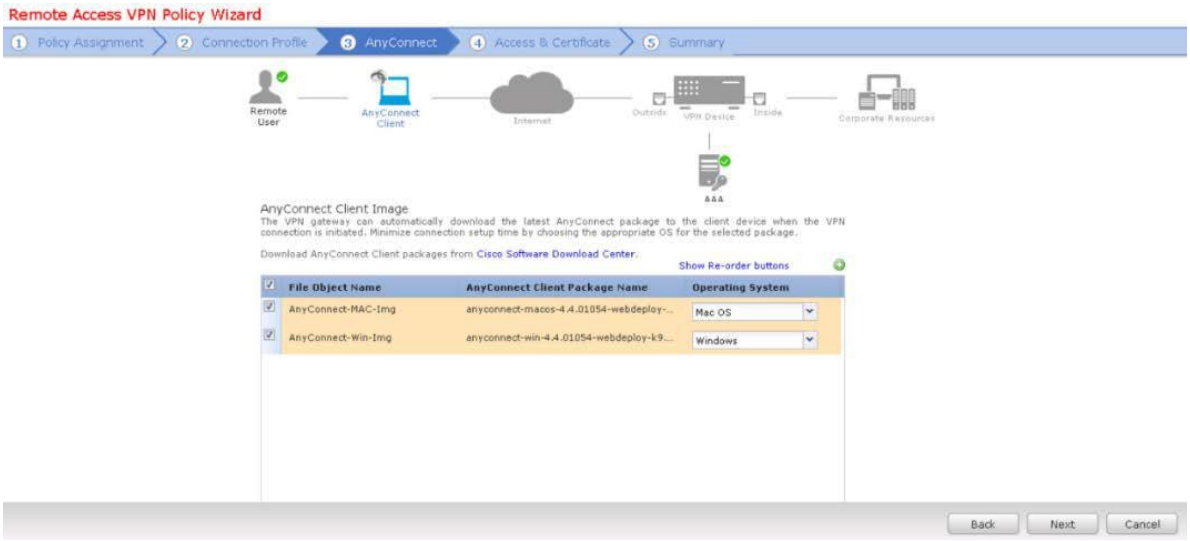
4. [グループ ポリシー（Group Policy）] が [DfltGrpPolicy] に設定されていることを確認します。[次へ（Next）] をクリックします。



5. ウィザードの [AnyConnect] ページに入力します。

   a. 両方のファイル オブジェクトのチェックボックスをオンにします。

   b. [次へ（Next）] をクリックします。

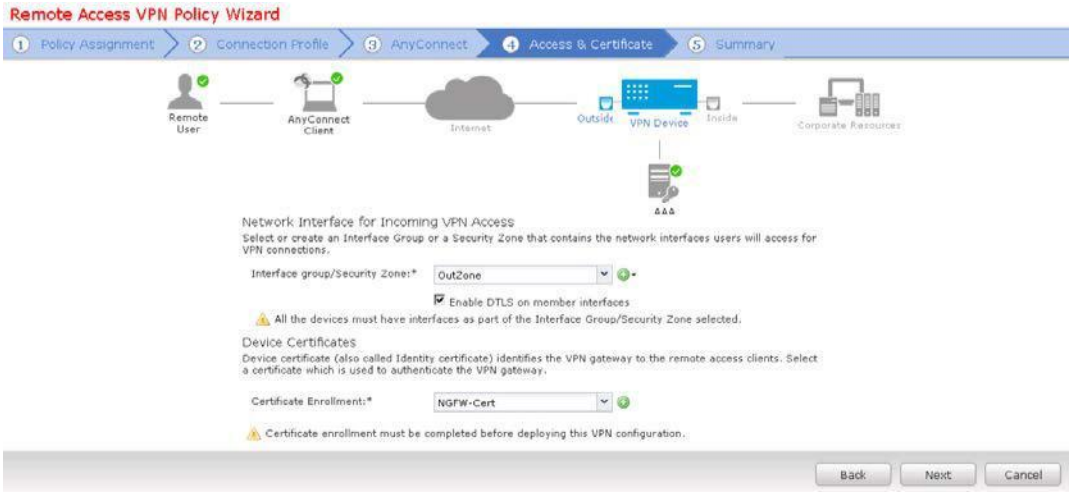


6. ウィザードの [アクセスおよび証明書（Access & Certificate）] ページに入力します。

    a. [インターフェイス グループ/セキュリティ ゾーン（Interface group/Security Zone）] で、[OutZone] を選択します。

    b. [証明書の登録（Certificate Enrollment）] で、[NGFW-Cert] を選択します。

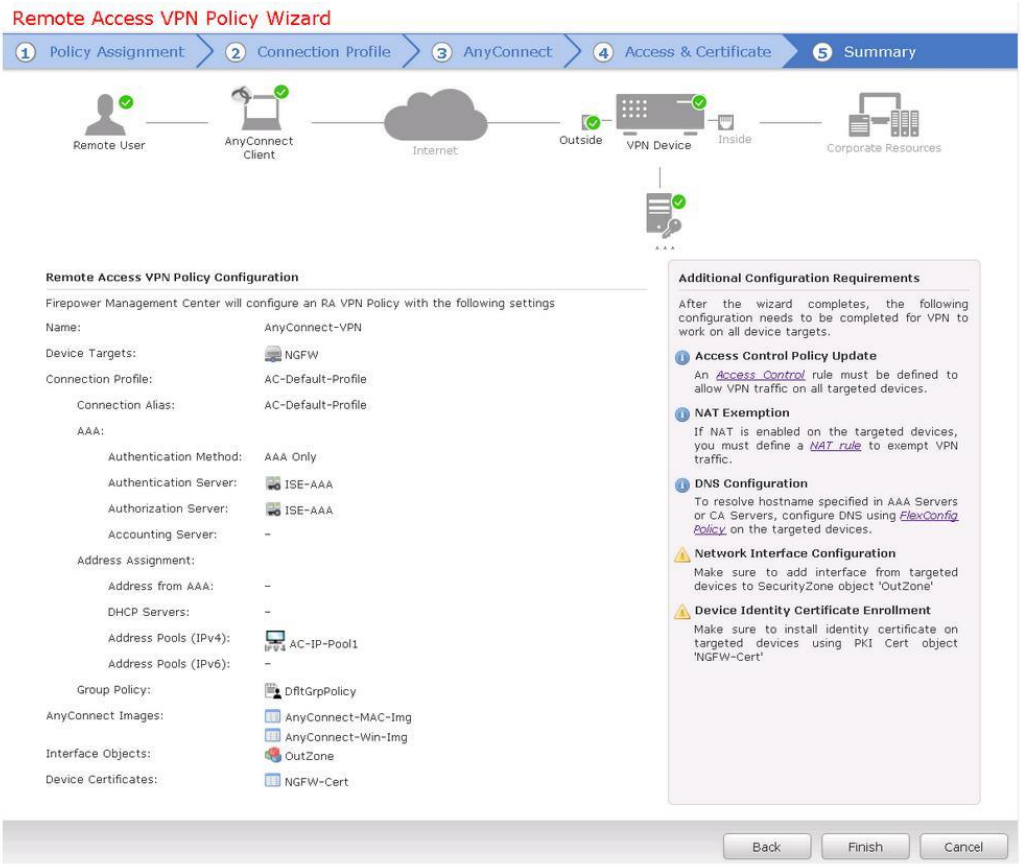
    c. [次へ（Next）] をクリックします。



7. ウィザードの [サマリー（Summary）] ページを確認します。

    a. このページに表示される設定を確認します。

    b. [完了（Finish）] をクリックします。

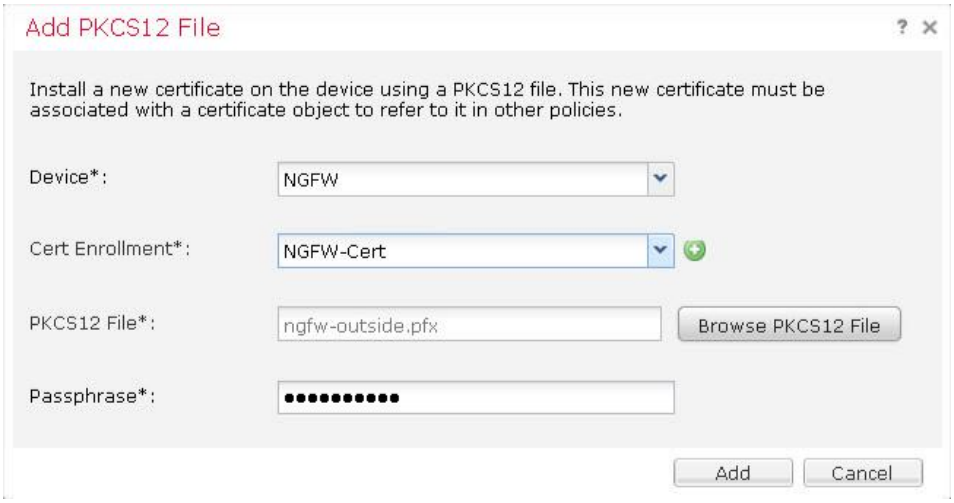


デバイスの証明書を設定する

1. FMC で、[デバイス（Devices）] > [証明書（Certificates）] に移動します。
2. [追加（Add）] をクリックし、[PKCS12 ファイル（PKCS12 File）] を選択します。
    a. [デバイス（Device）] で、[NGFW] を選択します。
    b. [証明書の登録（Cert Enrollment）] で、[NGFW-Cert] を選択します。

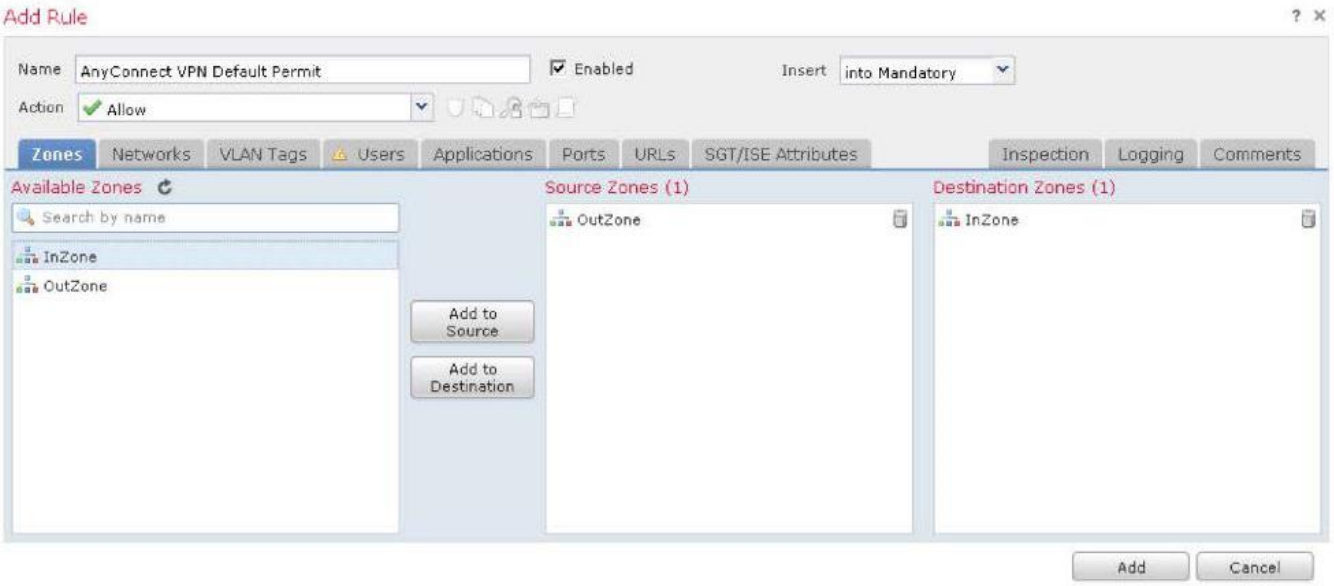
注：テキスト フィールドの右にある下向き矢印をクリックします。テキスト領域をクリックすると、文字列 **admin** が表示されます。これはブラウザの異常です。

    c. [PKCS12 ファイル（PKCS12 File）] で、[PKCS12 ファイルを参照（Browse PKCS12 File）] をクリックします。Jump Desktop の **Certificates** フォルダに移動し、[ngfw-outside] を選択します。[開く（Open）] をクリックします。
    d. [パスフレーズ（Passphrase）] に「`C1sco12345`」と入力します。
    e. [追加（Add）] をクリックします。



アクセス コントロール ポリシーを変更して AnyConnect インバウンド アクセスを許可する

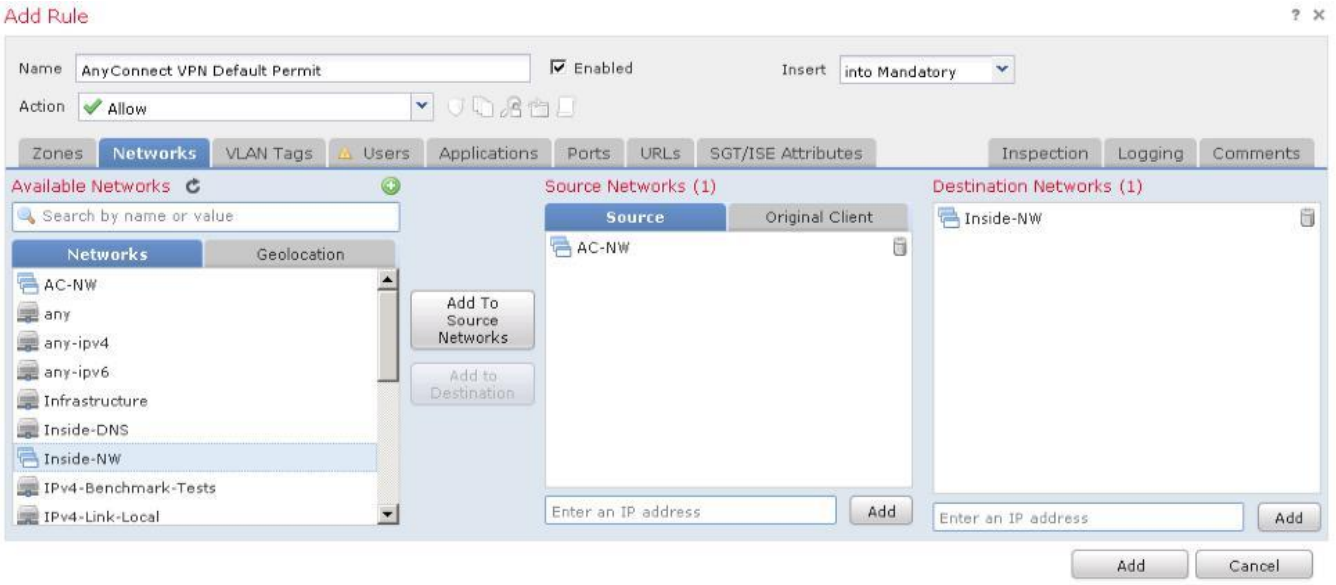
1. FMC で、[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] に移動します。
2. アクセス コントロール ポリシーを選択して編集します。[ルールの追加（Add Rule）] をクリックします。
    a. [名前（Name）] に「**AnyConnect VPN Default Permit**」と入力します。
    b. [挿入（Insert）] ドロップダウン リストから [デフォルトに挿入（into Default）] を選択します。
    c. [ゾーン（Zones）] タブがすでに選択されているはずです。
    d. [OutZone] を選択し、[送信元に追加（Add to Source）] をクリックします。
    e. [InZone] を選択し、[宛先に追加（Add to Destination）] をクリックします。



f. [ネットワーク（Networks）] タブを選択します。

i. [AC-NW] を選択し、[送信元に追加（Add to Source）] をクリックします。

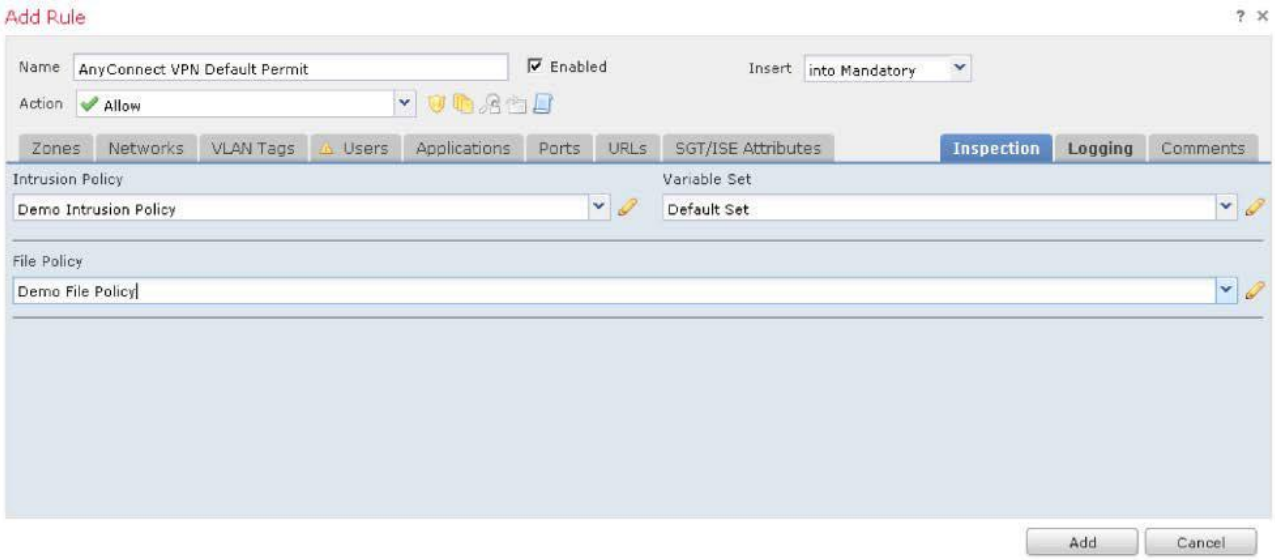
ii. [Inside-NW] を選択し、[宛先に追加（Add to Destination）] をクリックします。



g. [検査（Inspection）] タブを選択します。

i. [侵入ポリシー（Intrusion Policy）] ドロップダウン リストから [デモ侵入ポリシー（Demo Intrusion Policy）] を選択します。

ii. [ファイル ポリシー（File Policy）] ドロップダウン リストから [デモ ファイル ポリシー（Demo File Policy）] を選択します。



h. [追加（Add）] をクリックしてルールを追加します。

i. [保存（Save）] をクリックして、アクセス コントロール ポリシーの変更を保存します。

NAT 適用除外を設定する

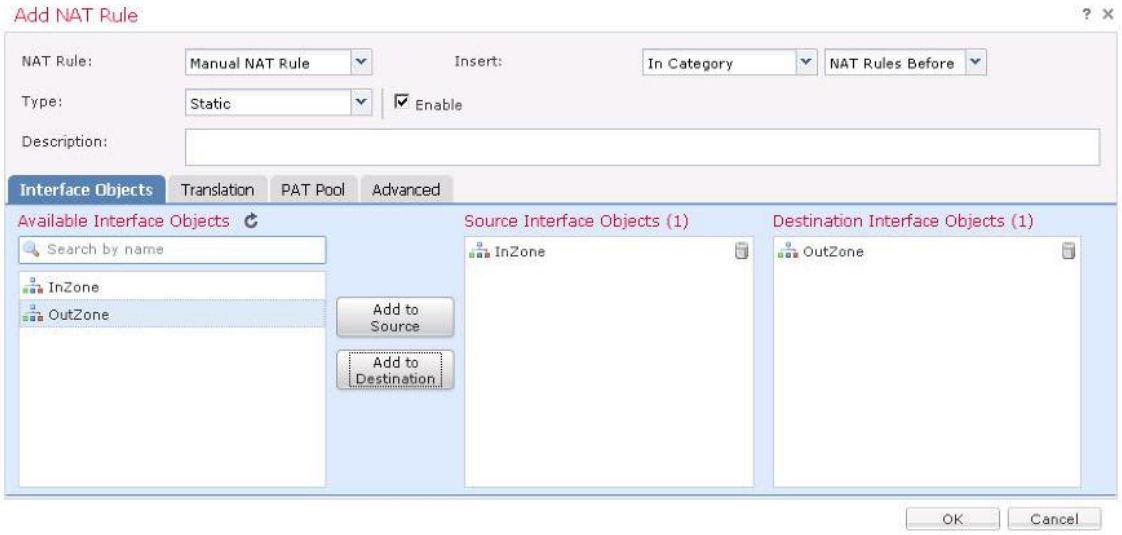
1. FMC で、[デバイス（Devices）] > [NAT] に移動します。
2. 既存の **NAT ポリシー**を選択して編集します。右上の [保存（Save）] ボタンがグレー表示になっていることを確認します。グレー表示になっていない場合は、一度戻って再度編集します。これは既知のバグです。

3. [ルールの追加（Add Rule）] をクリックします。

[インターフェイス オブジェクト（Interface Objects）] タブが表示されます。

i. [InZone] を選択し、[送信元に追加（Add to Source）] をクリックします。

ii. [OutZone] を選択し、[宛先に追加（Add to Destination）] をクリックします。



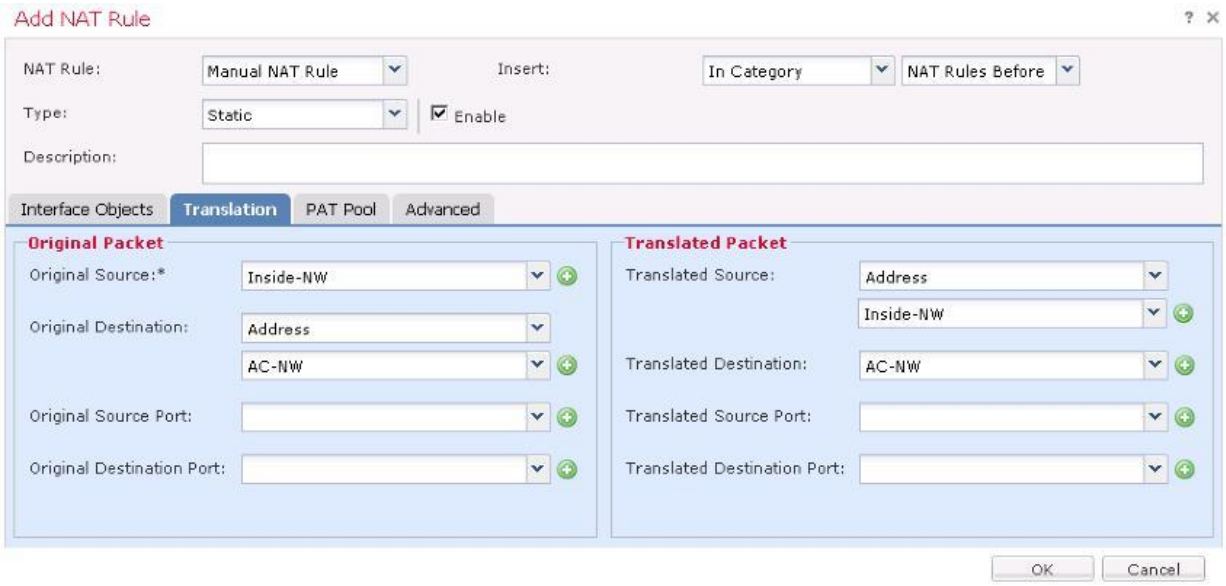
b. [トランスレーション（Translation）] タブを選択します。

   i. [元の送信元（Original Source）] で、[Inside-NW] を選択します。

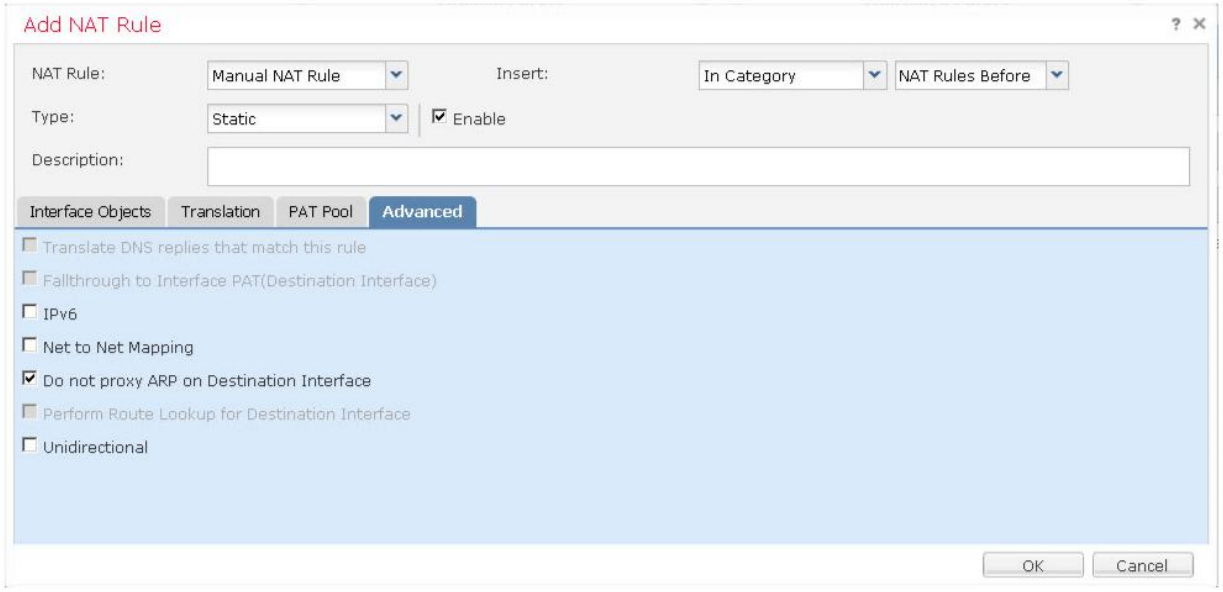
   ii. [元の宛先（Original Destination）] で、[AC-NW] を選択します。

   iii. [変換済み送信元（Translated Source）] で、[Inside-NW] を選択します。

   iv. [変換済み宛先（Translated Destination）] で、[AC-NW] を選択します。



c. [詳細（Advanced）] タブを選択し、[宛先インターフェイスでプロキシ ARP を有効にしない（Do not proxy ARP on Destination Interface）] を選択します。



注:このラボ演習では、[宛先インターフェイスでプロキシ ARP を有効にしない(Do not proxy ARP on Destination Interface)] を有効にすることが非常に重要です。すべてのデバイスがイン バンドで管理されているため、この手順を実行しないと、ポッドにアクセス上の問題が発生する可能性があります。

d. [OK] をクリックして NAT ルールを保存します。

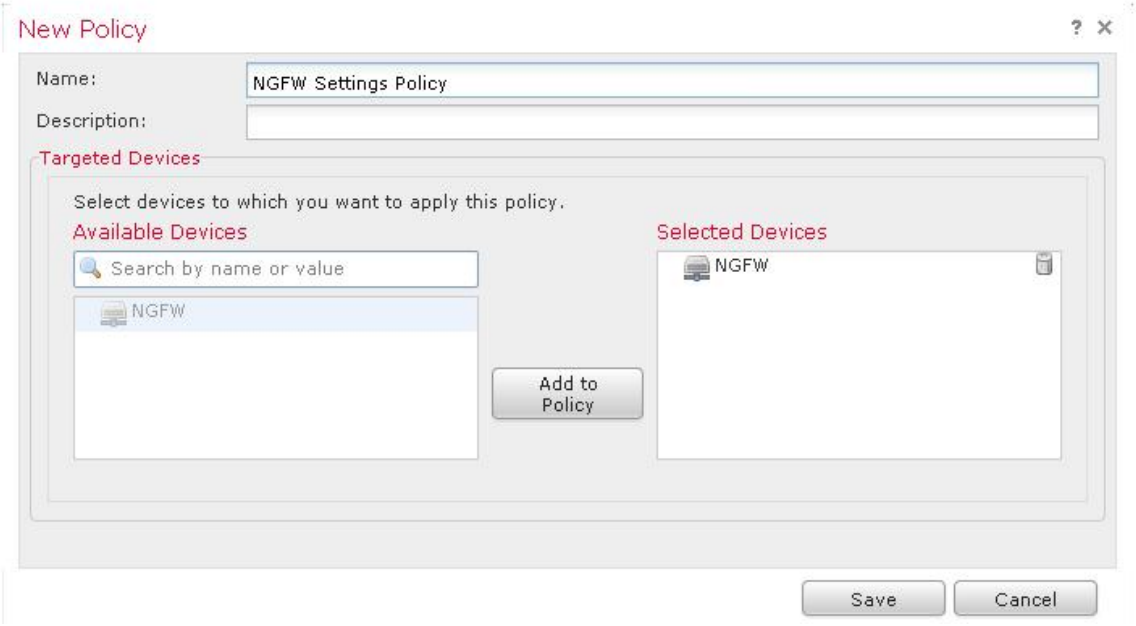
e. [保存(Save)] をクリックして、NAT ポリシーの変更を保存します。

VPN ロギングを設定する

トラブルシューティングを促進するために、VPN ロギング レベルをデフォルト([エラー(errors)])から [情報(informational)] に変更します。ラボの任意の時点で、[デバイス(Device)] > [VPN] > [トラブルシューティング(Troubleshooting)] に移動してログに記録された情報を表示し、設定のトラブルシューティングに役立てることができます。

注:実稼働環境では、VPN ロギングを [情報(informational)] に設定しないほうがいいでしょう。

1. FMC で、[デバイス(Devices)] > [プラットフォーム設定(Platform Settings)] に移動します。
   a. 青いテキスト [脅威対策設定ポリシー(Threat Defense Settings Policy)] をクリックします。
   b. ポリシーに「**`NGFW Settings Policy`**」という名前を付けます。
   c. **NGFW** デバイスを選択し、[ポリシーに追加(Add to Policy)] をクリックします。

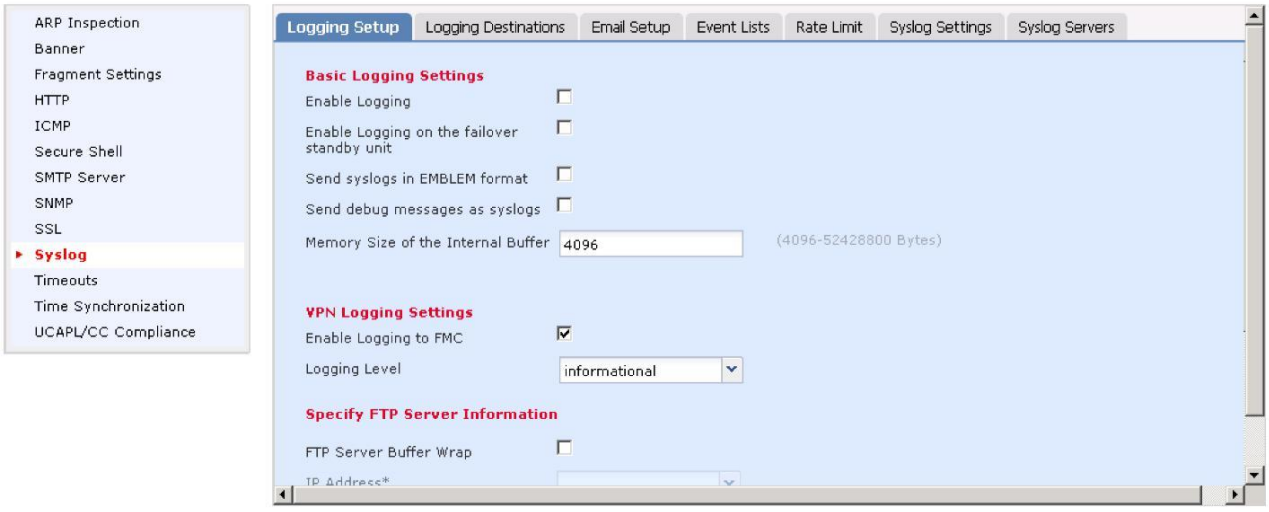


d. [保存（Save）] をクリックします。ポリシーが開き、編集できるようになります。

e. 左側のナビゲーション ペインで、[Syslog] を選択します。

f. [VPN ロギング設定（VPN Logging Settings）] で、ロギング レベルを [情報（informational）] に変更します。実稼働環境では、[エラー（errors）] または [アラート（alerts）] に設定することをお勧めします。

g. [保存（Save）] をクリックします。



NGFW RA VPN 設定を導入し確認する

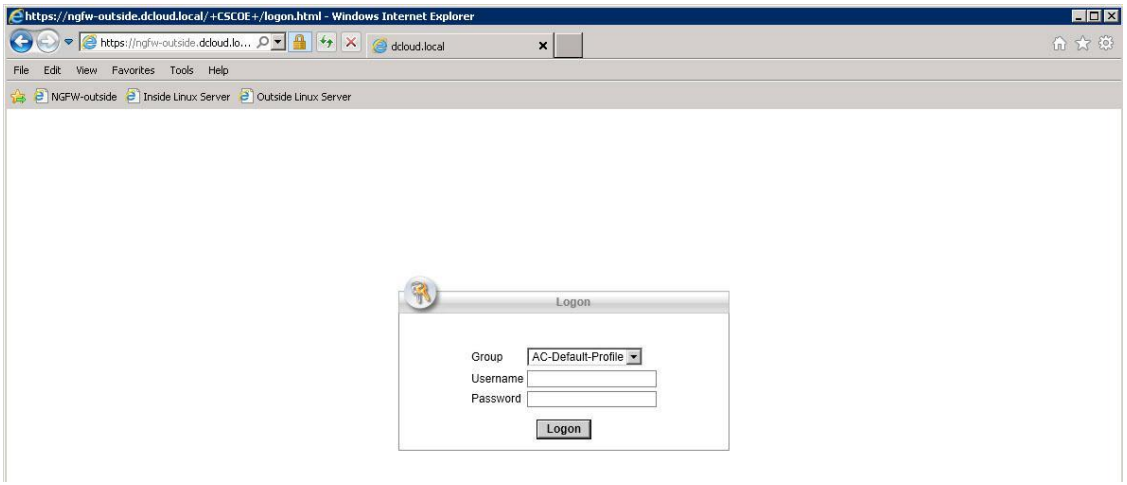
1. デバイスにポリシーを導入します。
    a. FMC で、[導入（Deploy）] ボタンをクリックします。
    b. [NGFW] を選択し、[導入（Deploy）] をクリックします。
    c. 導入が完了するまで待ちます。
2. NGFW CLI に対して、まだ PuTTY セッションを開いているはずです。次のコマンドの一部またはすべてを実行します。
    a. **`show running-config tunnel-group`**
    b. **`show running-config group-policy`**
    c. **`show running-config crypto`**
    d. **`show running-config ip local pool`**
    e. **`show running-config nat`**
3. NGFW CLI で次のコマンドを実行して、AAA をテストします。
   `test aaa-server authentication ISE-AAA host 198.19.10.130 username ira password 'C1sco12345'`

   このコマンドは、Jump Desktop の Strings to cut and paste.txt テキスト ファイルからカットして貼り付けることができます。

```
> test aaa-server authentication ISE-AAA host 198.19.10.130 username ira password 'C1sco12345'
INFO: Attempting Authentication test to IP address (198.19.10.130) (timeout: 32 seconds)
INFO: Authentication Successful
>
```

設定をテストする

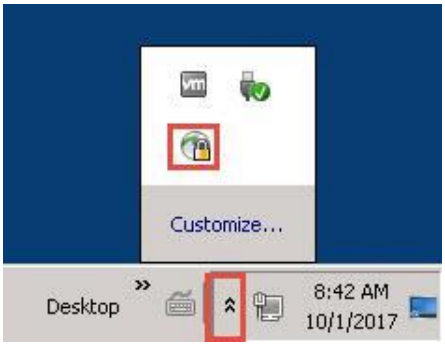
1. Jump Desktop の [リモート デスクトップ（Remote Desktop）] フォルダを開き、[Outside-PC] をダブルクリックします。
    a. **Internet Explorer** を開き、お気に入りバーの [NGFW-outside] をクリックします。



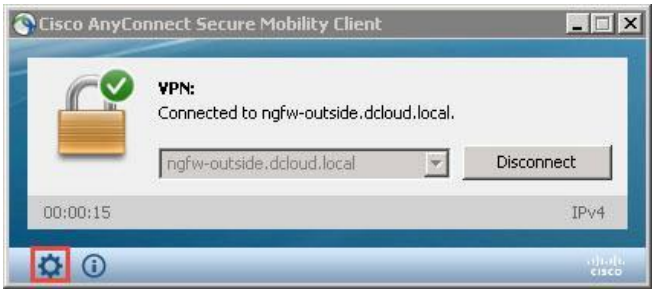
    b. [ユーザ名（Username）] に「**`ira`**」と入力します。[パスワード（Password）] に「**`C1sco12345`**」と入力します。[ログオン（Logon）] をクリックします。
    c. ページ下部にある [インストール（Install）] ボタンをクリックします。プロンプトが表示されたら、[インストール（Install）] を再度クリックします。

d. インストールが完了すると、AnyConnect が自動的に接続されます。

e. 次に示すように、Outside-PC の右下から AnyConnect クライアント UI を開きます。



2. 次に示す歯車アイコンをクリックして、AnyConnect クライアント UI の**詳細設定ウィンドウ**を開きます。



a. [統計（Statistics）] タブを選択し、サーバ IP アドレスを持つクライアントを確認します。

b. [ルートの詳細（Route Details）] タブを選択して、スプリット トンネリングを確認します。198.19.10.0/24 を宛先とするトラフィックだけがセキュアなルートであると考えられます。つまり、198.19.10.0/24 を宛先とするトラフィックだけが、VPN を通じてトンネリングされます。198.19.10.100/32 はセキュアなルートとしてもリストされています。これは、VPN グループ ポリシーが DNS サーバとして 198.19.10.100 をクライアントに割り当てるためです。

3. NGFW CLI で次のコマンド
`show vpn-sessiondb detail anyconnect`
を実行してこのセッションを確認します。

```
> show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username     : ira                    Index        : 60244
Assigned IP  : 198.19.13.10           Public IP    : 198.18.133.23
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : Clientless: (1)AES256  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (
1)AES256
Hashing      : Clientless: (1)SHA256  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA          1
（出力省略）
```

4. Outside-PC でコマンド プロンプトを開きます。
    a. **`nslookup inside.dcloud.local`** を実行します。Outside-PC が、198.19.10.100 を IP アドレスとする内部 DNS サーバを使用していることを確認します。
    b. 次のコマンドを実行します。
    `ftp inside.dcloud.local`
    `guest` として、パスワード **`C1sco12345`** でログインします。ログインすることで内部サーバへのアクセスが確認されます。
    c. 「**`cd ~root`**」と入力します。次のメッセージが表示されます。
    `Connection closed by remote host.`
    これで、侵入防御が機能していることを確認できます。
5. Internet Explorer のお気に入りバーで、[内部 Linux サーバ(Inside Linux Server)] をクリックします。
    a. [ファイル(Files)] リンクをクリックします。
    b. [ProjectX.pdf] リンクをクリックし、Web ページの下部にある [開く(Open)] ボタンをクリックして、PDF をダウンロードできることを確認します。
    c. [Zombies.pdf] リンクをクリックし、Web ページの下部にある [開く(Open)] ボタンをクリックします。Web ページの下部に次のメッセージが表示されます。AMP for Networks によってファイルがブロックされたためです。

6. FMC で、[分析(Analysis)] > [侵入(Intrusions)]> [イベント(Events)] に移動します。
    a. Snort ルール 336 がトリガーされたことを確認します。
    b. [イベントのテーブル ビュー(**T**able View of Events)] にドリルダウンして、送信元 IP アドレスが VPN プールのものであることを確認します。
7. FMC で、[分析(Analysis)] > [ファイル(Files)] > [マルウェア イベント(Malware Events)] に移動します。
    a. **Zombies.pdf** がブロックされたことを確認します。
    b. [マルウェア イベントのテーブル ビュー(Table View of Malware Events)] にドリルダウンして、送信元アドレスが VPN プールのものであることを確認します。
8. AnyConnect VPN を切断してから、次のラボ演習に進みます。

シナリオ 4.　RADIUS 属性を使用した AnyConnect

この演習は、次のタスクで構成されています。

- 新しいグループ ポリシーを作成する
- 新しい IP プールを作成する
- アクセス制御と NAT ポリシーを変更する
- 接続プロファイルを変更する
- 設定を導入しテストする

この演習では ISE RADIUS 属性を使用し、ユーザの AD グループに基づいて、グループ ポリシー、IP プール、およびダウンロード可能 ACL（DACL）を動的に割り当てます。

- RA VPN ユーザが IT グループのメンバーである場合は、内部ネットワーク（174.16.1.0/24）上のすべてのデバイスに対するフルアクセス権を持っています。
- RA VPN ユーザが IT グループのメンバーではない場合は、次の 2 つの内部デバイスだけにアクセスできます。
    - ドメイン コントローラ、ad1.dcloud.local（198.19.10.100）
    - 内部 Linux サーバ、inside.dcloud.local（198.19.10.200）
- IT グループのメンバーであるユーザには、別の IP プールから IP アドレスが割り当てられます。

時間を節約するために、ISE では、ラボ演習で必要な設定が事前にすべて設定されています。そこでは、AD グループのメンバーシップに基づいて選択した、グループ ポリシーと IP プールも設定されています。**そのため、新しいグループ ポリシーと IP プールの名前は、手順に示す名前と正確に一致している必要があります。**ISE 設定を確認するには、付録 C を参照してください。

手順

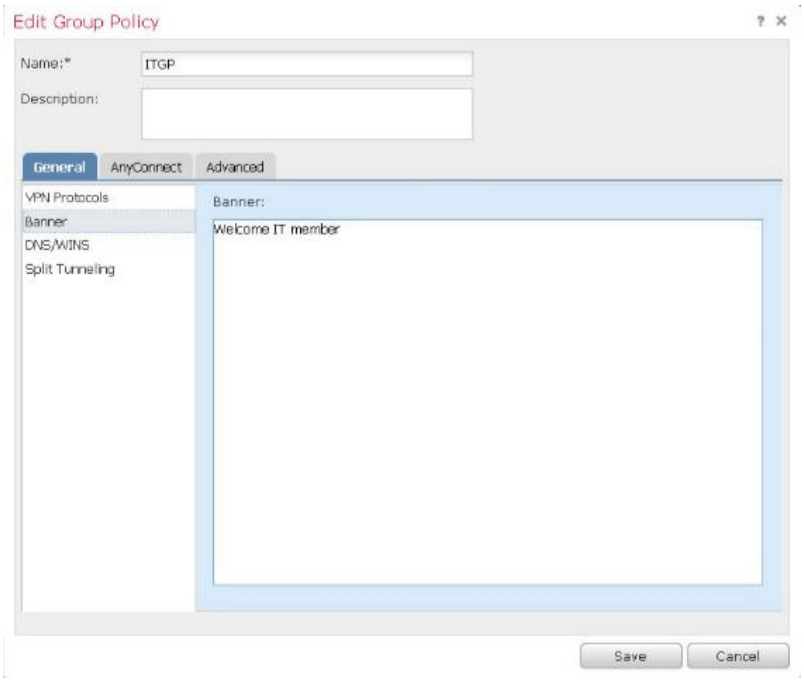
新しいグループ ポリシーを作成する

DfltGrpPolicy と基本的に同一であるグループ ポリシーを作成します。ここでは、ISE がユーザの Active Directory グループに基づいてグループ ポリシーを割り当てる方法を確認します。なんらかのカスタマイズを加えたほうがより興味深いものになりますが、このシナリオでは重要なことではありません。

1. FMC で、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）] に移動します。
2. [グループ ポリシーの追加（Add Group Policy）] をクリックします。

3. [名前（Name）] に「**ITGP**」と入力します。これは ISE 設定のために、正確なグループ名にする必要があります。

4. [全般（General）] タブで、[バナー（Banner）] を選択します。「**Welcome IT Member**」と入力します。



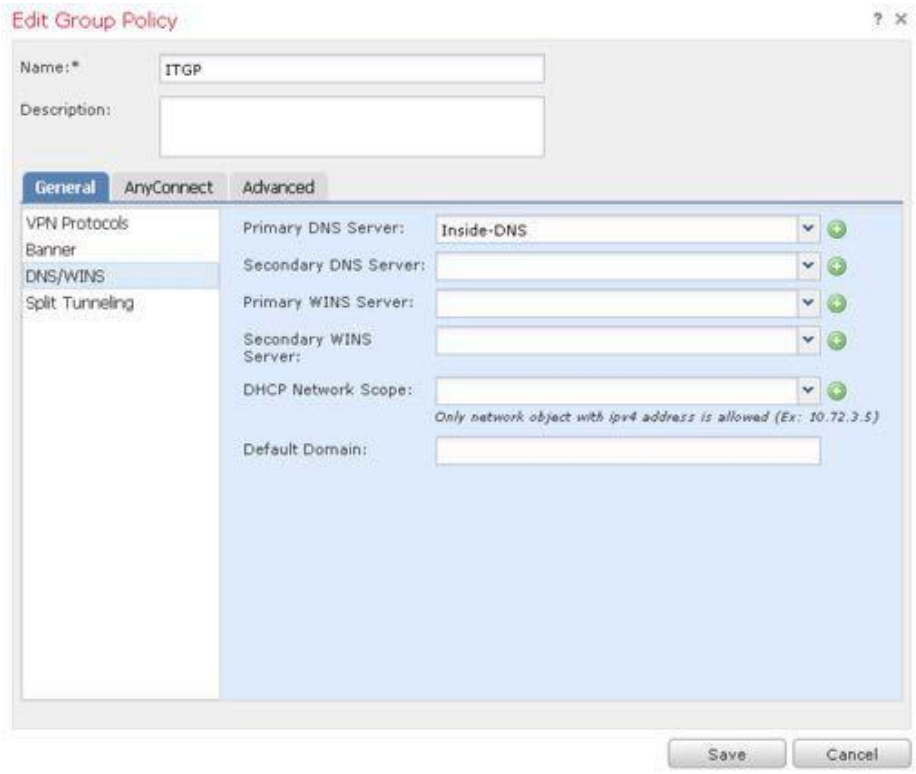
5. [全般（General）] タブで、[スプリット トンネリング（Split Tunneling）] を選択します。

    a. [IPv4 スプリット トンネリング（IPv4 Split Tunneling）] で、[以下に指定されたトンネル ネットワーク（Tunnel networks specified below）] を選択します。

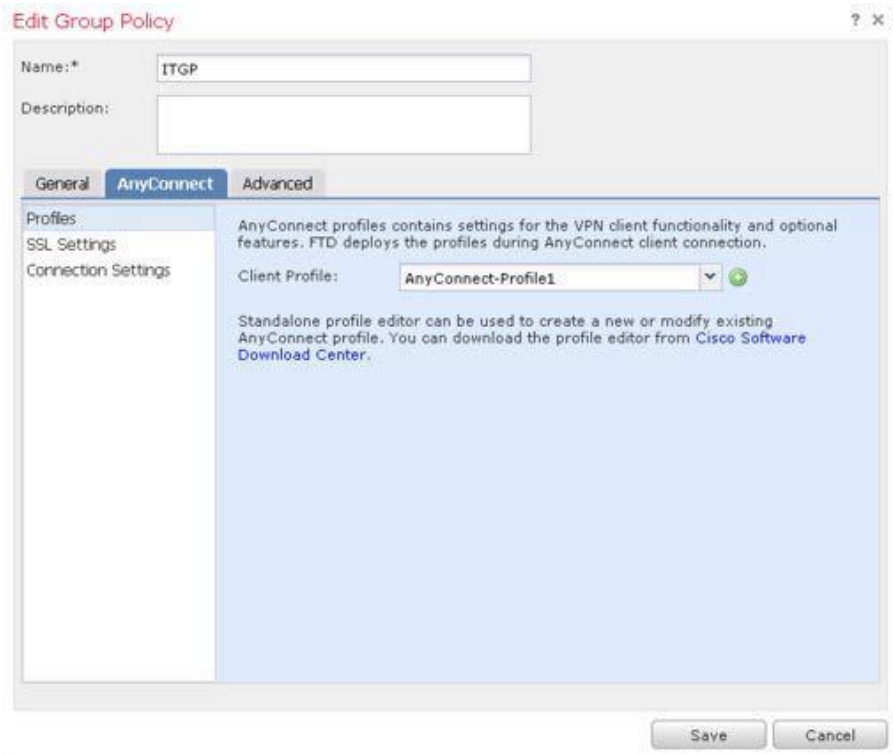
    b. [拡張アクセス リスト（Extended Access List）] オプション ボタンを選択します。

    c. [アクセス リスト（Access List）] で、[AC-SplitTunnel1] を選択します。

6. [全般（General）] タブで、[DNS/WINS] を選択します。[プライマリ DNS サーバ（Primary DNS Server）] で [Inside-DNS] を選択します。



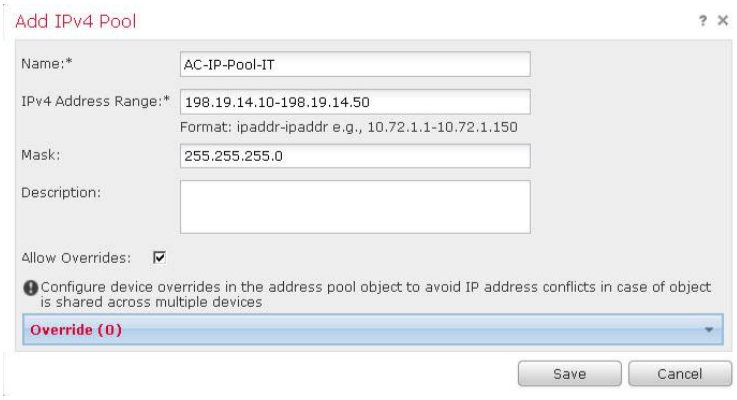
7. [AnyConnect] タブを選択します。[クライアント プロファイル（Client Profile）] で、[AnyConnect-Profile1] を選択します。



8. [保存（Save）] をクリックして、グループ ポリシーを保存します。

新しい IP プールを作成する

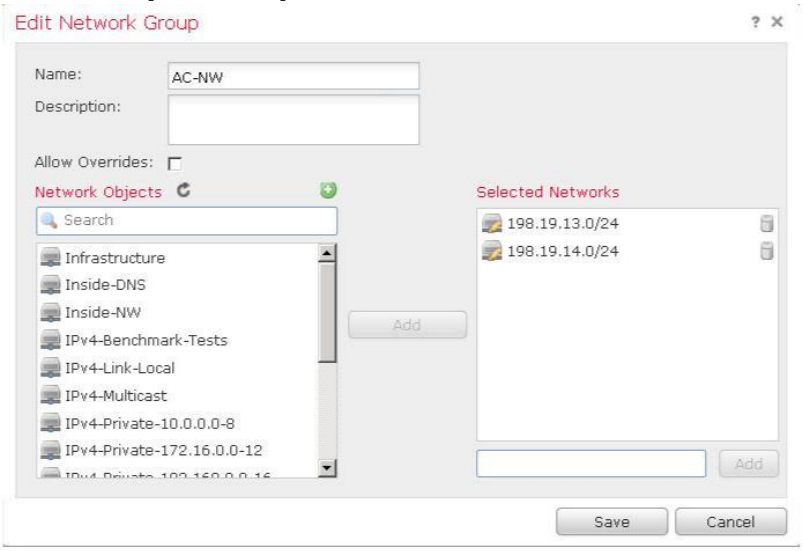
1. IP プールを作成します。
    a. FMC で、[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] > [アドレス プール(Address Pools)] > [IPv4 プール(IPv4 Pools)] に移動します。
    b. [IPv4 プールの追加(Add IPv4 Pools)] をクリックします。
    c. [名前(Name)] に「**AC-IP-Pool-IT**」と入力します。これは ISE 設定のために、正確なグループ名にする必要があります。
    d. [IPv4 アドレス範囲(IPv4 Address Range)] に「**198.19.14.10-198.19.14.50**」と入力します。
    e. [マスク(Mask)] に「**255.255.255.0**」と入力します。
    f. [保存(Save)] をクリックします。



アクセス制御と NAT ポリシーを変更する

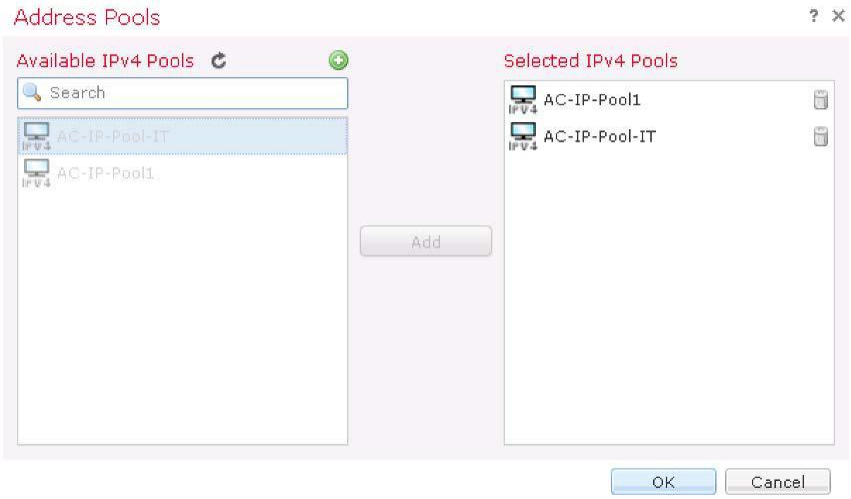
AC-NW ネットワーク グループ オブジェクトを変更すれば、アクセス制御と NAT ポリシーの両方を変更することができます。

1. FMC で、[オブジェクト(Object)]> [オブジェクト管理(Object Management)] > [ネットワーク(Network)] に移動します。
    a. ネットワーク グループ **AC-NW** を選択して編集します。
    b. 下部にあるテキスト フィールドの [選択したネットワーク(Selected Networks)] に「**198.19.14.0/24**」と入力し、[追加(Add)] をクリックします。
    c. [保存(Save)] をクリックします。

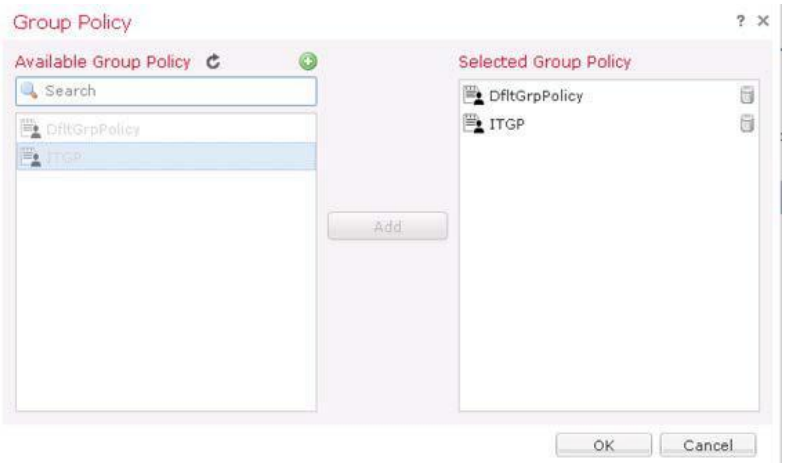


接続プロファイルを変更する

1. FMC で、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] に移動します。
2. **AnyConnect-VPN** を編集します。次に **AC-Default-Profile** 接続プロファイルを選択して編集します。
3. 新しく作成された IP プールを追加します。
    a. クライアントの [アドレス割り当て（Address Assignment）] タブがすでに選択されているはずです。
    b. [アドレス プール（Address Pools）] で、[+] アイコンをクリックし、[IPv4] を選択します。
    c. [AC-IP-Pool-IT] を選択し、[追加（Add）] をクリックします。



    d. [OK] をクリックします。
    e. [接続プロファイルの編集（Edit Connection Profile）] ウィンドウで [保存（Save）] をクリックします。
4. 新しく作成されたグループ ポリシーを追加します。
    a. AnyConnect-VPN ページの [詳細設定（Advanced）] タブで、左側のナビゲーション ペインから [グループ ポリシー（Group Policies）] を選択します。
    b. [+] アイコンをクリックします。
    c. [ITGP] を選択して [追加（Add）] をクリックします。



    d. [OK] をクリックし、次に [保存（Save）] をクリックします。

設定を導入しテストする

1. NGFW の変更を導入します。導入が完了するまで待ちます。
2. Outside-PC リモート デスクトップ セッションに戻ります。
    a. AnyConnect クライアントで [接続(Connect)] をクリックします。

    b. **harry** として、パスワード **C1sco12345** でログインします。Harry は IT グループのメンバーではありません。

    c. AnyConnect が接続されたら、Outside-PC のコマンド プロンプトから次の 2 つのコマンドを実行します。
        i. **ping inside.dcloud.local** これは成功するはずです。
        ii. **ping altinside.dcloud.local** これは失敗するはずです。ISE がデフォルトで割り当てる DACL では、ドメイン コントローラと内部 Linux サーバへのアクセスのみ許可されます。
3. NFGW CLI で、次のコマンドを実行します。
   show vpn-sessiondb detail anyconnect
   出力で次の値を確認します。
    a. [ユーザ名(Username)]:**harry**
    b. [割り当てられた IP(Assigned IP)]:**198.19.13.x**
    c. [グループ ポリシー(Group Policy)]:**DfltGrpPolicy**
    d. [フィルタ名(Filter Name)]:**#ACSACL#-IP-AC-DACL- Default-x**

```
> show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username     : harry                   Index        : 53216
Assigned IP  : 198.19.13.10           Public IP    : 198.18.133.23
Protocol     : Clientless 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     : 15410                   Bytes Rx     : 516
Pkts Tx      : 16                      Pkts Rx      : 8
Pkts Tx Drop : 0                       Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group : AC-Default-Profile
(出力省略)

> Filter Name  : #ACSACL#-IP-AC-DACL-Default-598b5954
```

4. Outside-PC リモート デスクトップ セッションに戻ります。

    a. AnyConnect VPN セッションを切断します。

    b. 新しく AnyConnect VPN セッションを開始します。

    c. **rita** として、パスワード **C1sco12345** でログインします。Rita は IT グループのメンバーです。

    d. ITGP で設定したバナーが表示されていることを確認して、[承認(Accept)] をクリックします。

    e. AnyConnect が接続されたら、Outside-PC のコマンド プロンプトから次の 2 つのコマンドを実行します。

        i. **ping inside.dcloud.local** これは成功するはずです。

        ii. **ping altinside.dcloud.local** これも成功するはずです。ISE が IT グループに割り当てる DACL では、すべての内部デバイスへのアクセスが許可されます。

5. NFGW CLI で、次のコマンドを実行します。
   show vpn-sessiondb detail anyconnect
   出力で次の値を確認します。

    a. [ユーザ名(Username)]:**rita**

    b. [割り当てられた IP(Assigned IP)]:**198.18.14.x**

    c. [グループ ポリシー(Group Policy)]:ITGP

    d. [フィルタ名(Filter Name)]:**#ACSACL#-IP-AC-DACL-IT-x**

```
> show vpn-sessiondb detail anyconnect
Username      : rita                    Index        : 4998
Assigned IP   : 198.19.14.10            Public IP    : 198.18.133.23
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      : 15375                   Bytes Rx     : 691
Pkts Tx       : 16                      Pkts Rx      : 9
Pkts Tx Drop  : 0                       Pkts Rx Drop : 0
Group Policy  : ITGP                    Tunnel Group : AC-Default-Profile(出力省略)
 (出力省略)


> Filter Name   : #ACSACL#-IP-AC-DACL-IT-598b1f19
```

6. AnyConnect VPN クライアントを切断します。

シナリオ 5.　クライアント証明書を使用した AnyConnect

この演習は、次のタスクで構成されています。

- 接続プロファイルを変更する
- 設定を導入しテストする

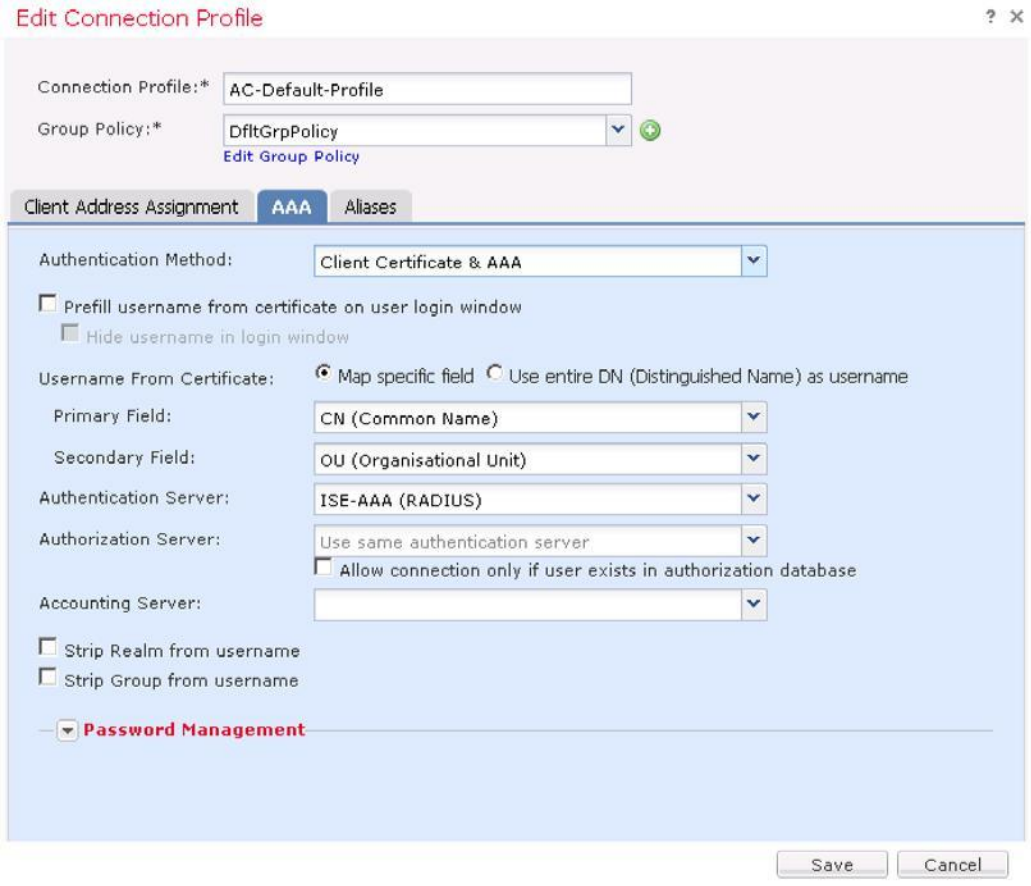
この演習では、RA VPN の二重認証（証明書と AAA）を設定します。

注：時間を節約するために、クライアント証明書はすでに Outside-PC にインストールされています。

手順

接続プロファイルを変更する

1. FMC で、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] に移動します。**AnyConnect-VPN** を編集します。
    a. [接続プロファイル（Connection Profile）] で、**AC-Default-Profile** 接続プロファイルを選択して編集します。
    b. [AAA] タブを選択し、[認証方式（Authentication Method）] を [クライアント証明書 & AAA（Client Certificate & AAA）] に変更します。



    c. [接続プロファイルの編集（Edit Connection Profile）] ページで [保存（Save）] をクリックします。
    d. [AnyConnect-VPN] ページで [保存（Save）] をクリックします。

設定を導入しテストする

1. NGFW の変更を導入します。導入が完了するまで待ちます。
2. Outside-PC リモート デスクトップに戻ります。
    a. AnyConnect クライアントを接続します。
    b. **rita** として、パスワード **C1sco12345** でログインします。このラボ演習では、どのユーザであるかは関係ありません。
3. NFGW CLI で、次のコマンドを実行します。
   show vpn-sessiondb detail anyconnect
   [認証モード(Auth Mode)] が [証明書およびユーザ パスワード(Certificate and userPassword)] になっていることを確認します。

```
> show vpn-sessiondb detail anyconnect
 (出力省略)
AnyConnect-Parent:
  Tunnel ID    : 52614.1
  Public IP    : 198.18.133.23
  Encryption   : none                  Hashing      : none
  TCP Src Port : 49286                 TCP Dst Port : 443
  Auth Mode    : Certificate and userPassword


>(出力省略)
```

4. **AnyConnect VPN は切断しないでください**。次のラボ演習にすぐに進んでください。

シナリオ 6.　モニタリングとトラブルシューティング

この演習は、次のタスクで構成されています。

- AnyConnect ユーザ アクティビティのモニタリング
- トラブルシューティング

FMC を使用して、AnyConnect ユーザ アクティビティのモニタリングとトラブルシューティングを行います。

手順

AnyConnect ユーザ アクティビティのモニタリング

このセクションでは、AnyConnect を通じてログインした、すべてのアクティブ ユーザをモニタリングできます。

1. FMC で、[概要（Overview）] > [ダッシュボード（Dashboards）] > [アクセス制御されたユーザの統計情報（Access Controlled User Statistics）] に移動します。
2. [VPN] タブを選択します。VPN トラフィック専用のウィジェットが 7 つあります。
3. [分析（Analysis）] > [ユーザ（Users）] > [アクティブ セッション（Active Sessions）] に移動します。
    a. Rita の VPN セッションが表示されています。
    b. Rita のセッションの左側にあるチェックボックスをオンにして、[ログアウト（Logout）] をクリックします。プロンプトが表示されたら、[続行（Continue）] をクリックします。

ネットワーク検出によって検出された、他のアクティブ セッションも表示される場合があります。たとえば、FTP セッションを通じて検出されたゲストが表示される場合です。簡略にするために、それらのセッションは上の図には含まれていません。ユーザ、およびユーザが検出された方法の詳細を確認するには、[分析（Analysis）] > [ユーザ（Users）] > [ユーザ（Users）] に移動します。

4. Outside-PC で、Rita がログアウトしていることを確認します。
5. FMC で、[分析（Analysis）] > [ユーザ（Users）] > [ユーザ アクティビティ（User Activity）] に移動します。このウィンドウには、現在および過去のユーザ セッションの詳細が表示されます。数分間かけてこのページの情報を確認してください。

トラブルシューティング

このセクションでは、NGFW の VPN イベントの Syslog レベルを変更します。NGFW CLI から、基本的なトラブルシューティング コマンドも実行します。

1. FMC で、[デバイス（Device）] > [VPN] > [トラブルシューティング（Troubleshooting）] に移動します。レコードが表示されます。
    表示されない場合は、このページの時間枠を調整してください。

2. NGFW CLI で次のコマンドのいくつかを実行し、トラブルシューティング機能の概略を把握します。これらのコマンドは RA VPN のトラブルシューティングに役立ちます。主に参照用に用意されているものです。

    a. **`show vpn-sessiondb ?`**

    b. **`test aaa-server ?`**

    c. **`debug crypto ca ?`（証明書の問題のトラブルシューティングに有効）**

    d. **`debug crypto ipsec ?`**

    e. **`debug ldap ?`**

    f. **`debug aaa ?`**

シナリオ 7.　Cisco Threat Intelligence Director（CTID）

この演習は、次のタスクで構成されています。

- Web サーバから STIX ファイルを取得する
- 複雑なインジケータと、関連する監視対象を分析する
- インシデントをトリガーする CTID に URL のリストをアップロードする
- TAXII フィードに CTID を登録する
- CTID インシデントを生成する

CTID は、サードパーティ製サイバー脅威インテリジェンス インジケータを使用できる FMC のコンポーネントです。CTID はこれらのインジケータを解析して、NGFW によって検出可能な監視対象を生成します。NGFW は、監視対象の検出を CTID にレポートします。CTID はそれらの監視結果がインシデントに該当するかどうかを判断します。

2 つのファイル形式がサポートされています。

- フラット ファイル：IP アドレス、URL、SHA256 ハッシュなど、シンプルなインジケータがリストされます。
- STIX ファイル：シンプルなインジケータでも複雑なインジケータでも記述できる XML ファイルです。

これらのファイルを取得する方法は 3 つあります。

- FMC UI が実行されているコンピュータからアップロードする
- リモート Web サーバの URL から取得する
- TAXII フィードから取得する（STIX ファイルのみ）

この演習の目的は、CTID を設定し、テストすることです。

手順

CTID が監視対象を NGFW にパブリッシュすることを確認する

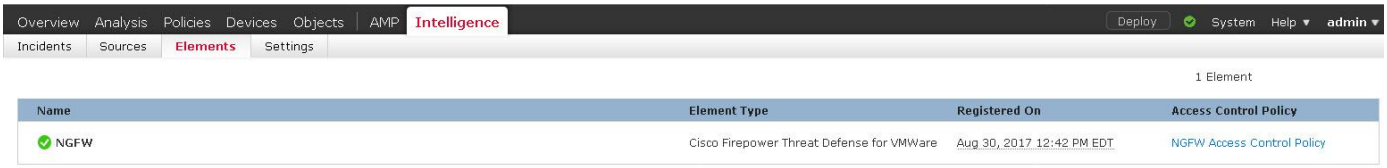
1. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] の順に選択します。
2. ポリシーの右にある**鉛筆アイコン**をクリックして、アクセス コントロール ポリシーを編集します。
3. [詳細設定（Advanced）] タブを選択します。

4. [Threat Intelligence Director を有効にする（Enable Threat Intelligence Director）] がデフォルトで有効になっていることを確認します。

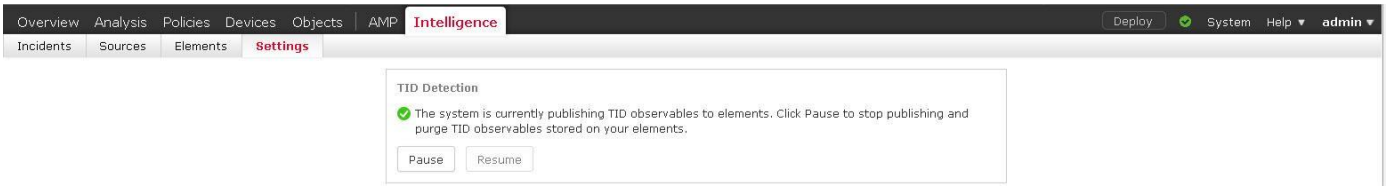
5. この高度な設定を使用して、CTID をアクセス ポリシー レベルで有効または無効にすることができます。

6. [インテリジェンス（Intelligence）] > [要素（Elements）] に移動します。

7. **NGFW** が要素になっていることを確認します。これは、CTID が監視対象を NGFW にパブリッシュできることを意味します。



8. [インテリジェンス（Intelligence）] > [設定（Settings）] に移動します。監視対象を CTID 要素にパブリッシュするように設定されていることを確認します。



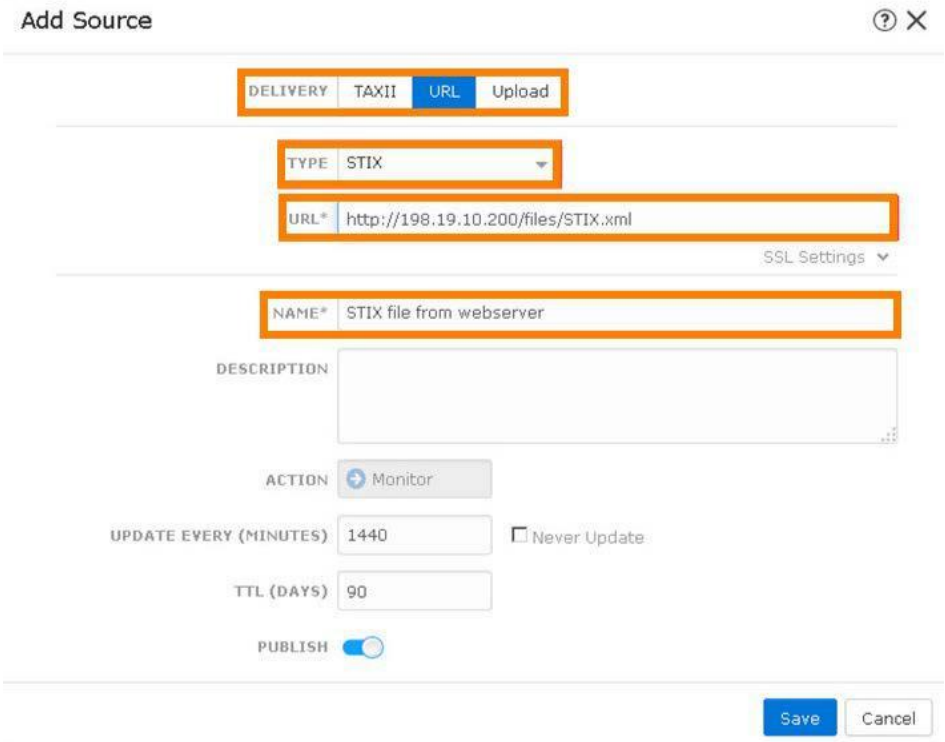
注：ここでは CTID をグローバルに有効または無効にすることができます。[一時停止（Pause）] をクリックすると、すべての要素に対する CTID のパブリッシュが停止されます。

Web サーバから STIX ファイルを取得する

1. [インテリジェンス（Intelligence）] > [ソース（Sources）] > [ソース（Sources）] に移動します。

2. 右側のプラス記号（+）をクリックして、インテリジェンスのソースを追加します。

3. [配信(DELIVERY)] で [URL] を選択します。
4. [タイプ(TYPE)] で、[STIX] が選択されていることを確認します。
5. [URL] に「**`http://198.19.10.200/files/STIX.xml`**」と入力します。
6. [名前(NAME)] に「**`STIX file from webserver`**」と入力します。



7. [保存(Save)] をクリックします。

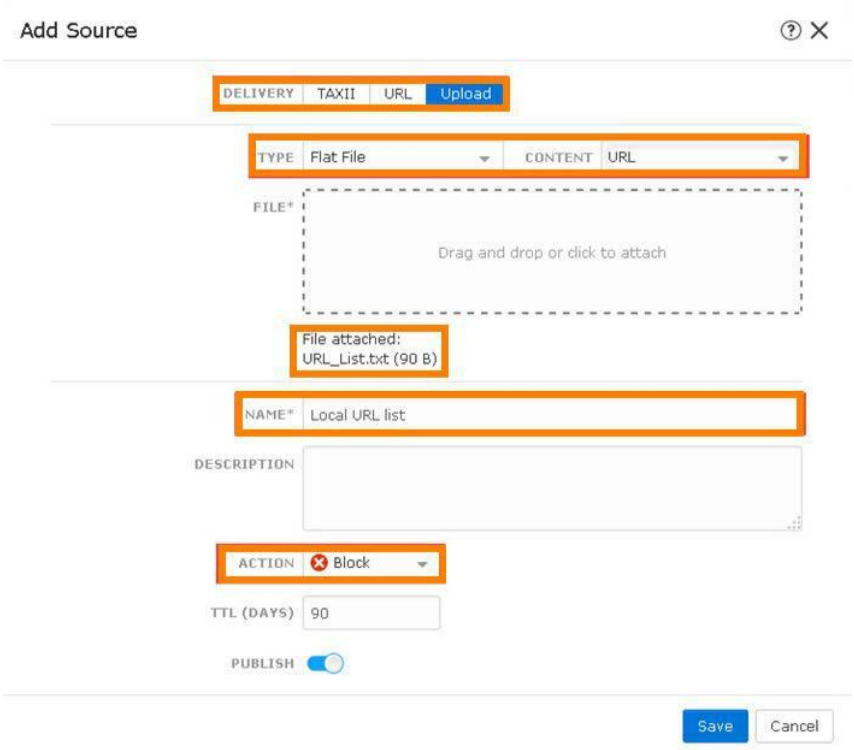
注:STIX ファイルについて、アクションを [モニタ(Monitor)] から [ブロック(Block)] に変更することはできません。STIX ファイルは複雑なインジケータを表す場合があるため、NGFW が監視対象に基づいて、インジケータの基準に適合しているかどうかを判断することはできません。

ただし複雑なインジケータの場合でも、個々の監視対象に対するアクションを [ブロック(Block)] に設定することはできます。

8. 数秒間待ちます。[インテリジェンス(Intelligence)] > [ソース(Sources)] > [インジケータ(Indicators)] に移動します。複雑なインジケータが追加されたことを確認します。
9. インジケータ名 [Weatherman PUA] をクリックします。インジケータの詳細を確認します。
10. [閉じる(Close)] をクリックして、[インジケータの詳細(Indicator Details)] ページを閉じます。
11. [インテリジェンス(Intelligence)] > [ソース(Sources)] > [監視対象(Observables)] に移動します。SHA-256 が 2 つと IPv4 が 1 つ監視対象に追加されていることを確認します。

インシデントをトリガーする CTID に URL のリストをアップロードする

1. [インテリジェンス（Intelligence）] > [ソース（Sources）] > [ソース（Sources）] に移動します。右側のプラス記号（+）をクリックして、インテリジェンスのソースを追加します。
2. [配信（DELIVERY）] で [アップロード（Upload）] を選択します。
3. [タイプ（TYPE）] で [フラット ファイル（Flat File）] を選択します。[コンテンツ（CONTENT）] ドロップダウン リストが表示されます。
4. [コンテンツ（CONTENT）] で [URL] を選択します。
5. [ファイル（FILE）] 領域をクリックし、Jump Desktop の Files フォルダから **URL_LIST.txt** を選択します。
6. [名前（NAME）] に「**`Local URL list`**」と入力します。
7. [アクション（ACTION）] で、[ブロック（Block）] を選択します。



8. [保存（Save）] をクリックします。
9. 数秒間待ちます。[インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ（Indicators）] に移動します。2 つの URL インジケータが追加されたことを確認します。
10. [インテリジェンス（Intelligence）] > [ソース（Sources）] > [監視対象（Observables）] に移動します。2 つのタイプの URL 監視対象が追加されたことを確認します。

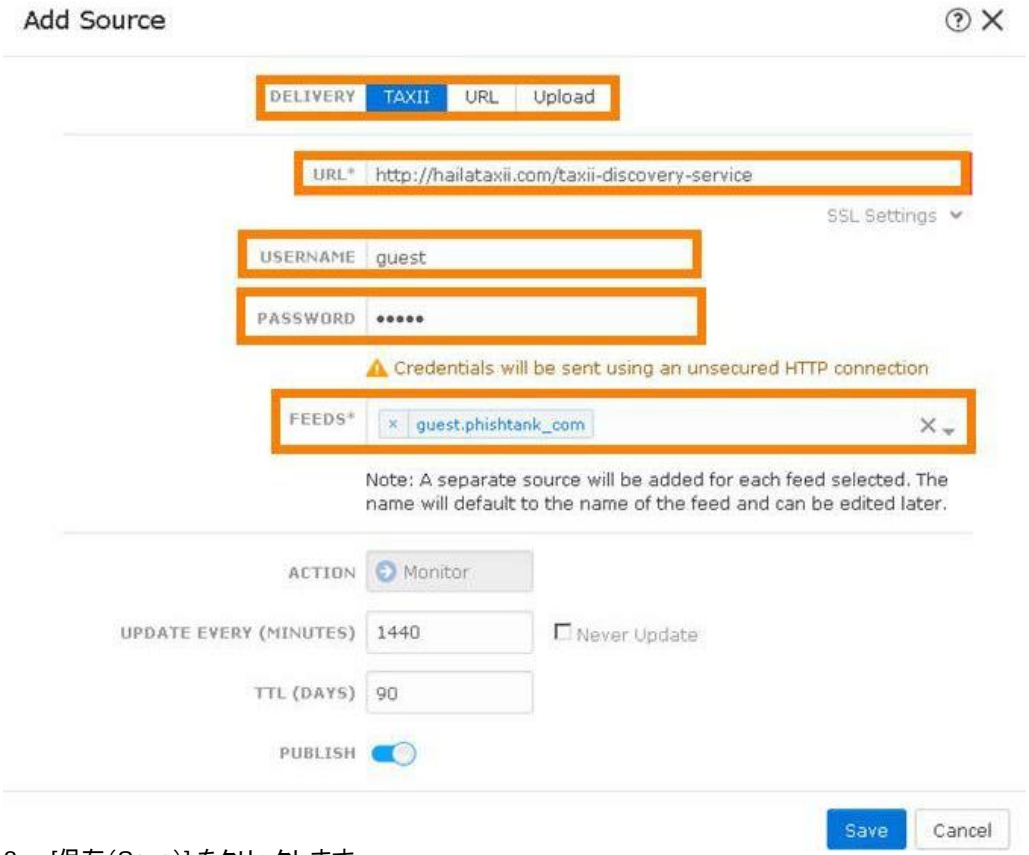
TAXII フィードに CTID を登録する

注:ここで使用される TAXII フィードは Hail a TAXII のものです。これらのフィードに問題がある場合は、Alien Vault を使用できます。詳細については、付録 D を参照してください。

1. [インテリジェンス(Intelligence)] > [ソース(Sources)] > [ソース(Sources)] に移動します。右側のプラス記号(+)をクリックして、インテリジェンスのソースを追加します。
2. [配信(DELIVERY)] で [TAXII] を選択します。
3. [URL] に「**`http://hailataxii.com/taxii-discovery-service`**」と入力します。
4. [ユーザ名(USERNAME)] に「**guest**」と入力します。
5. [パスワード(PASSWORD)] に「**`guest`**」と入力します。
6. [フィード(FEEDS)] で [guest_phishtank_com] を選択します。

注:FEEDS ドロップダウン リストが表示されるまで数秒かかる場合があります。

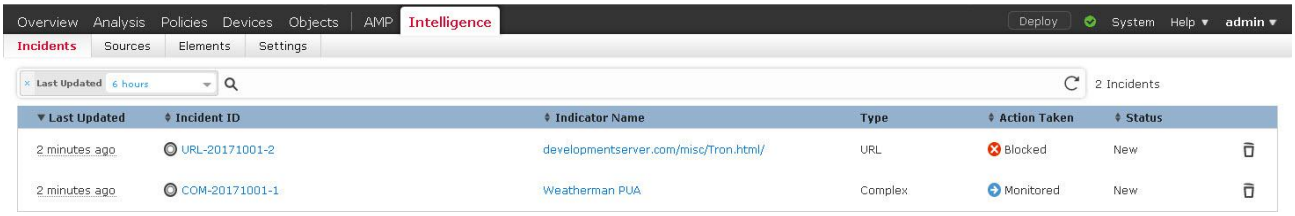
7. 次のような画面が表示されることを確認します。



8. [保存(Save)] をクリックします。
9. このソースの [ステータス(Status)] 列が [解析中(Parsing)] に変わるまで待ちます。解析には非常に時間がかかるため、完了するまでは待ちません。
10. [インテリジェンス(Intelligence)] > [ソース(Sources)] > [インジケータ(Indicators)] に移動します。複数の URL インジケータが追加されたことを確認します。
11. [インテリジェンス(Intelligence)] > [ソース(Sources)] > [監視対象(Observables)] に移動します。複数の URL 監視対象が追加されたことを確認します。

CTID インシデントを生成する

1. FMC には、監視対象と NGFM を 5 分に 1 回同期させるデーモンがあります。そのため、監視対象がセンサーにパブリッシュされるまで数分かかる場合があります。この手順では、特定の監視対象のパブリッシュを確認する方法を示します。NGFW CLI で次の手順を実行します。
    a. 「**expert**」と入力してエキスパート モードにします。
    b. 「**ls -d /var/sf/*download**」と入力します。複数のディレクトリが表示されることを確認します。
    admin@ngfw:~$ ls -d /var/sf/*download
    /var/sf/clamupd_download /var/sf/iprep_download /var/sf/sifile_download
    /var/sf/cloud_download/var/sf/sidns_download /var/sf/siurl_download
    これらのうち 4 つ（iprep_download、sidns_download、sifile_download、siurl_download）が、セキュリティ インテリジェンスと CTID で使用されます。
    c. 「**grep developmentserver /var/sf/*download/*lf**
    admin@ngfw:~$ grep developmentserver /var/sf/*download/*lf」
    と入力します。**/var/sf/siurl_download/731625d4-9512-11e7-915c-7e7252ae92ac.lf:developmentserver.com/misc/Tron.html/**
    これが表示されない場合は、数分待ってからもう一度試してください。これがパブリッシュされてから次に進む必要があります。引き続き失敗する場合は、CTID ソースを削除してから再度追加します。
    d. 「**grep 198.18.133.200 /var/sf/*download/*lf**
    admin@ngfw:~$ grep 198.18.133.200 /var/sf/*download/*lf」と入力します。
    /var/sf/iprep_download/730f187a-9512-11e7-915c-7e7252ae92ac.blf:198.18.133.200
    これが表示されない場合は、数分待ってからもう一度試してください。これがパブリッシュされてから次に進む必要があります。引き続き失敗する場合は、CTID ソースを削除してから再度追加します。
    e. 「**exit**」と入力してエキスパート モードを終了します。
2. 内部 Linux サーバの CLI で次を実行します。
    a. **wget -t 1 outside/files/ProjectX.doc** を実行します。これは成功するはずです。
    b. **wget -t 1 developmentserver.com/misc/Tron.html** を実行します。これはブロックされるはずです。
3. FMC で [インテリジェンス（Intelligence）] > [インシデント（Incidents）] に移動します。2 つのインシデントがあることを確認します。



4. インシデントにドリルダウンし、インシデントの詳細を確認します。
5. URL インジケータのインシデントがあることを確認します。インシデントにドリルダウンし、インシデントの詳細を確認します。

シナリオ 8.　FlexConfig

この演習は、次のタスクで構成されています。

- ユーザ定義の FlexConfig オブジェクトを作成する
- システム定義の FlexConfig オブジェクトで使用されるテキスト オブジェクトを変更する
- FlexConfig ポリシーを作成して設定する
- 変更を導入して設定をテストする

FlexConfig は、設定を FTD の Lina（ASA）設定に直接導入できる機能です。これは、まだ FTD では使用できない機能を導入するために使用できます。このラボ演習の目的は、次の 2 つです。

- ユーザ定義の FlexConfig オブジェクトを使用して EIGRP を設定します。
- システム定義の FlexConfig オブジェクトを使用して SIP 検査を無効にします。

注：EIGRP の設定用には、別のシステム定義の FlexConfig オブジェクトがあります。時間の経過とともに変化する設定には、これらのオブジェクトが適しています。ただし、FlexConfig のシンプルさと機能を示すために、ここではユーザ定義の FlexConfig オブジェクトを使用します。

FTD を NetFlow データの送信元として設定するには、システム定義の FlexConfig オブジェクトを使用します。

ユーザ定義の FlexConfig オブジェクトを作成する

1. FMC UI で、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動します。
2. 左側のナビゲーション パネルの下部にある [FlexConfig] で、[FlexConfig オブジェクト（FlexConfig Object）] を選択します。
3. [FlexConfig オブジェクトの追加（Add FlexConfig Object）] をクリックします。
    a. [名前（Name）] に「**myEIGRP**」と入力します。
    b. メインのテキスト領域に次のコマンドを入力します。ネットマスクが /24 ではなく /18 になっていることを確認します。
    ```
    router eigrp 10
     network 198.18.128.0 255.255.192.0
    ```
    c. [保存（Save）] をクリックします。

システム定義の FlexConfig オブジェクトで使用されるテキスト オブジェクトを変更する

1. FMC UI の [オブジェクト管理（Object Management）] ページが表示されていることを確認します。
2. **Default_Inspect_Protocol_Disable** という Flex オブジェクトの右にある虫眼鏡アイコンをクリックします。このオブジェクトを編集することはできませんが、必要に応じてコピーすることができます。

注：FlexConfig オブジェクトは Apache Velocity 言語で記述されています。この言語ではループと if ステートメントがサポートされています。ループと if ステートメントの先頭には # が付きます。これはコメントではありません。出力に含まれるリテラル テキストではないということです。コメントの先頭には ## が付きます。

この FlexConfig オブジェクトは **disableInspectProtocolList** というテキスト オブジェクトに対してループします。このテキスト オブジェクトを編集します。

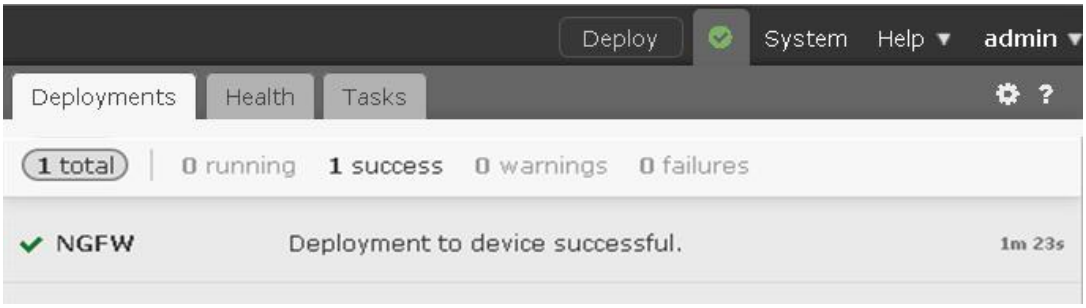
3. [閉じる（Close）] をクリックします。
4. [オブジェクト管理（Object Management）] ページの左側のナビゲーション ペインの下部にある [FlexConfig] で、[テキスト オブジェクト（Text Object）] を選択します。
5. **disableInspectProtocolList** というテキスト オブジェクトを編集します。
6. この変数は複数の値を取ります。値は **1** に設定したままにします。
7. 値「**`sip`**」を入力します。
8. [保存（Save）] をクリックします。

FlexConfig ポリシーを作成して設定する

1. [デバイス（Devices）] > [FlexConfig] に移動します。[新しいポリシー（New Policy）] をクリックします。
    a. [名前（Name）] に「**`NGFW Flex Policy`**」と入力します。
    b. デバイス **NGFW** を選択します。[ポリシーに追加（Add to Policy）] をクリックします。
    c. [保存（Save）] をクリックします。
2. 数秒後にポリシーが開き、編集できるようになります。
    a. 左側の列の [ユーザ定義（User Defined）] で、[myEIGRP] を選択します。  をクリックして、ポリシーに FlexConfig オブジェクトを追加します。
    b. 左側の列の [システム定義（System Defined）] で、[Default_Inspect_Protocol_Disable] を選択します。  をクリックして、ポリシーに FlexConfig オブジェクトを追加します。
    c. [保存（Save）] をクリックします。
3. [設定のプレビュー（Preview Config）] をクリックします。
    a. [デバイスの選択（Select Device）] ドロップダウン リストから [NGFW] を選択します。
    b. 数秒後に設定の変更が表示されます。コマンドが正しいことを確認します。いくつかの余分な VPN コマンドが表示されていることがわかります。この不具合は設定に影響しませんが、今後のリリースで修正されます。
    c. [閉じる（Close）] をクリックします。

変更を導入して設定をテストする

1. NGFW CLI から **show running-config policy-map** を実行します。SIP 検査が有効になっていることを確認します。
2. 内部 Linux サーバ セッションで、「**ping 204.44.14.1**」と入力します。これは失敗するはずです。
3. 変更を導入します。導入が完了するまで待ちます。



4. NGFW CLI から **show running-config policy-map** を実行します。SIP 検査が無効になっていることを確認します。
5. NGFW CLI で、次のコマンドを実行します。
    a. **show eigrp neighbors** を実行します。FTD と CSR ルータ間で隣接関係が形成されていることを確認します。
    b. **show eigrp topology** を実行します。EIGRP ルートが受信されていることを確認します。
    c. **show route eigrp** を実行します。NGFW で、EIGRP が認識したルートがルーティング テーブル内にあることを確認します。
6. 内部 Linux サーバ セッションで、「**ping 204.44.14.1**」と入力します。これは成功するはずです。

シナリオ 9.　ASA から NGFW への移行

この演習は、次のタスクで構成されています。

- FMC を移行ツールに変換する
- ASA オブジェクトを移行する
- NAT とサポートされていない機能を移行し、オブジェクトの再利用を検討する

この演習の目的は、受講者が移行ツールに慣れ、次の内容を理解できるようにすることです。

- 設定方法
- 使用方法

FMC を移行ツールに変換すると、2 つの設定が移行されます。オブジェクトの平坦化や、サポートされていない機能の処理方法など、移行に関するいくつかの側面が明らかになります。

手順

FMC を移行ツールに変換する

1. Jump Desktop で PuTTY リンクを開きます。[Migrator] という事前設定されたセッションをダブルクリックします。**admin** として、パスワード **C1sco12345** でログインします。

注:移行用のツールとして、変更された FMC が必要になります。この変更は、スクリプトによって実行できます。この FMC は一般的に、実稼働 FMC とは別の仮想 FMC です。実稼働 FMC は移行ツールとして使用すべきではありません。

2. 「**sudo enableMigrationTool.pl**」と入力します。
    a. プロンプトが表示されたら、パスワード **C1sco12345** を入力します。
    b. 警告を必ず読んでください。
    c. 続行するかどうか尋ねられたら、「**Y**」と入力します。
    d. スクリプトが完了するまで待機します。これは 1 分未満で完了します。
3. Firefox ブラウザで新しいタブを開きます。
    a. ブックマーク バーの [移行ツール（Migration Tool）] リンクをクリックします。[詳細設定（Advanced）] をクリックし、[例外の追加（Add Exception）] をクリックします。プロンプトが表示されたら、[セキュリティ承認の確認（Confirm Security Acceptation）] をクリックします。

注:移行ツールとして使用するこの FMC は、インストール後に変更されていません。ここまでに使用してきた FMC は、事前設定されたものです。この事前設定には、信頼できる証明書の追加が含まれています。詳細については「付録 A」を参照してください。

    b. **admin** として、パスワード **C1sco12345** でログインします。

c. UI の上部に、次のような赤いバナーが表示されていることを確認します。

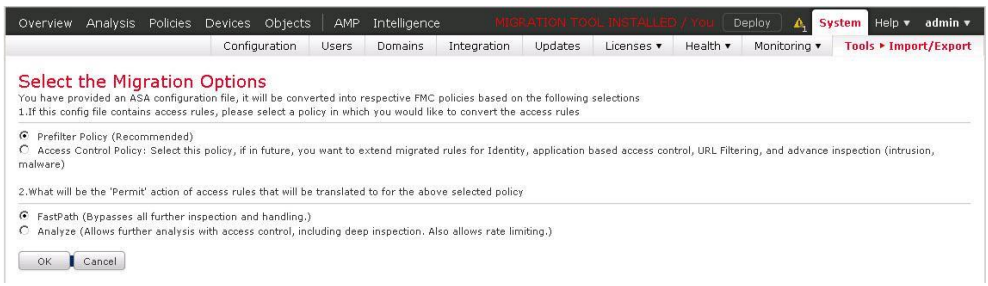
[移行ツールがインストール済み/ASA の変換に限定（MIGRATION TOOL INSTALLED / You are limited to ASA conversions only）]

ASA オブジェクトを移行する

この演習の目的は次のとおりです。

- 移行プロセスについて学習する
- ネットワーク、サービス オブジェクト、オブジェクト グループを移行する方法を理解する

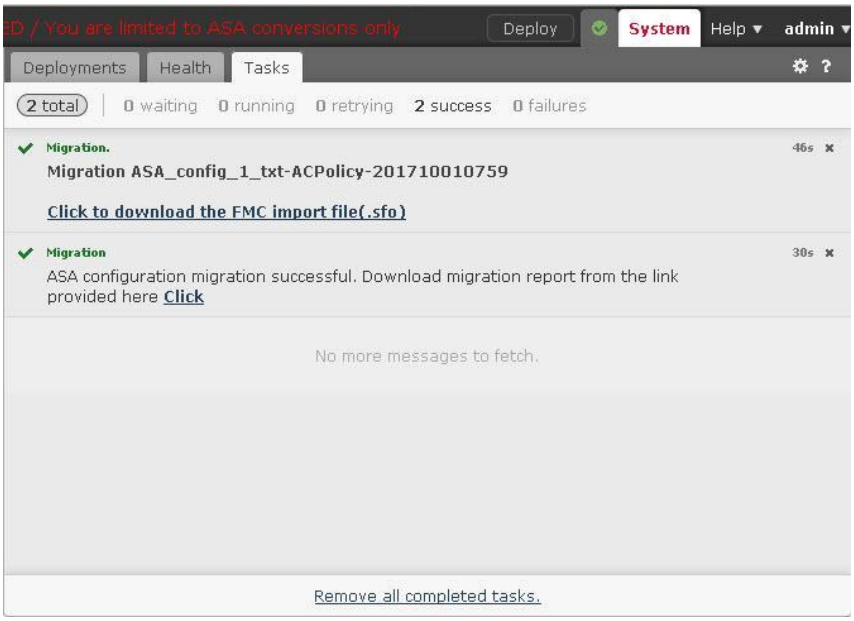
1. Jump の Files フォルダで、**ASA_config_1.txt** ファイルを開きます。
   a. ネストされたネットワークとサービス オブジェクトがあることを確認します。
   b. これらのオブジェクトを参照するアクセス リストとアクセス グループがあることを確認します。オブジェクトはポリシー設定に影響しないため、アクセス グループがないとオブジェクトが移行されません。
2. Migrator の UI（FMC ではない）で、[システム（System）] > [ツール（Tools）] > [インポート/エクスポート（Import/Export）] に移動します。
   a. [パッケージのアップロード（Upload Package）] をクリックします。
   b. [参照（Browse）] をクリックし、**Files** フォルダから **ASA_config_1.txt** ファイルを選択します。
   c. [アップロード（Upload）] をクリックします。
3. 次のページでは、次のようにすべての設定を変更せずに [OK] をクリックします。



4. [アップロード（Upload）] ページに戻るまで待ちます。

    a. [導入（Deploy）] ボタンの右にあるアイコンをクリックします。

    b. [タスク（Task）] タブをクリックし、タスクが完了するまで待ちます。



    a. [クリックして FMC インポート ファイル（.sfo）をダウンロード（Click to download the FMC import file(.sfo)）] というテキストをクリックして、SFO ファイルを保存します。

    b. [クリック（Click）] というテキストをクリックし、デフォルトの [Google Chrome で開く（Open with Google Chrome）] を選択すると、新しいタブで移行レポートが開きます。変換レポートにエラーがないことを確認します。Chrome を閉じます。

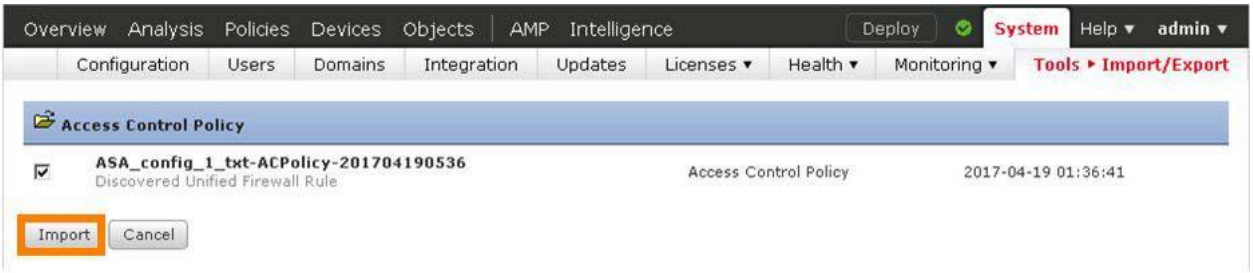
5. （実稼働環境の）FMC UI で、[システム（System）] > [ツール（Tools）] > [インポート/エクスポート（Import/Export）] に移動します。

    a. [パッケージのアップロード（Upload Package）] をクリックします。

    b. [参照（Browse）] をクリックし、**Downloads** フォルダから SFO ファイルを選択します。このファイルの名前は、**ExportForMigration-<some UUID>.sfo** の形式になっています。[開く（Open）] をクリックします。

    c. [アップロード（Upload）] をクリックします。

6. 次のページで [インポート(Import)] をクリックします。



7. インポートが完了するまで待ちます。

8. [オブジェクト(Objects)] > [オブジェクト管理(Object Management)] に移動します。

   a. [ネットワーク(Network)] オブジェクト ページが選択されます。次のオブジェクトが作成されていることを確認します。

      - 4 つのネットワーク オブジェクト **net1**、**net2**、**net3**、**net4**
      - 2 つのネットワーク グループ **net12**、**net34**
      - 1 つのネストされたネットワーク グループ **net1234**

注:これらは、ASA 設定内に存在したネットワーク オブジェクトとネットワーク グループ オブジェクトとまったく同じです。

   b. 左側のナビゲーション ペインで、[ポート(Port)] を選択します。次のオブジェクトが作成されていることを確認します。

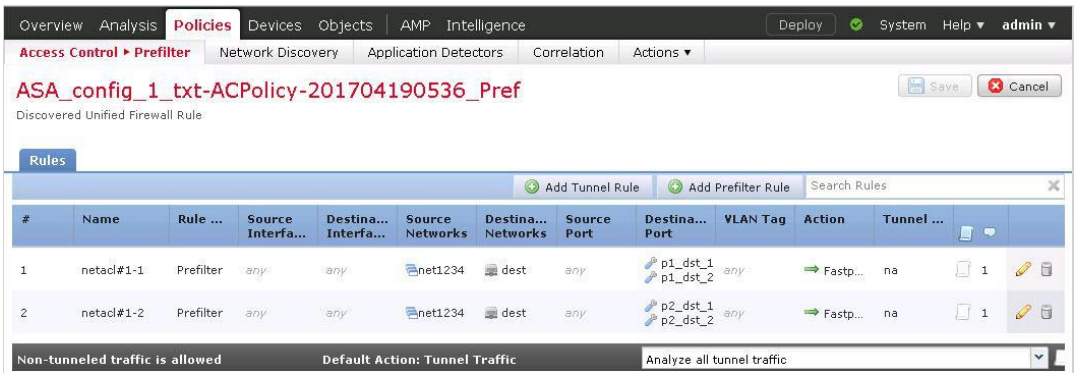
      - 4 つのポート オブジェクト **p1_dst_1**、**p1_dst_2**、**p2_dst_1**、**p2_dst_2**
      - ポート グループはなし

注:ASA ポート グループ p1 と p2 が平坦化され、p12 はありません。

9. [ポリシー(Policies)] > [アクセス制御(Access Control)] > [プレフィルタ(Prefilter)] に移動します。

   a. 新しいプレフィルタ ポリシーがあることを確認してください。ルールを検査できるように、このポリシーを編集します。

   b. この 1 つの ACE が、ASA 設定として 2 つのプレフィルタ ルールに分かれています。



10. [ポリシー(Policies)] > [アクセス制御(Access Control)] > [アクセス制御(Access Control)] の順に選択します。

   a. 新しいアクセス コントロール ポリシーがあります。検査できるように編集します。

   b. デフォルトのアクションがブロックに設定されているルールはありません。

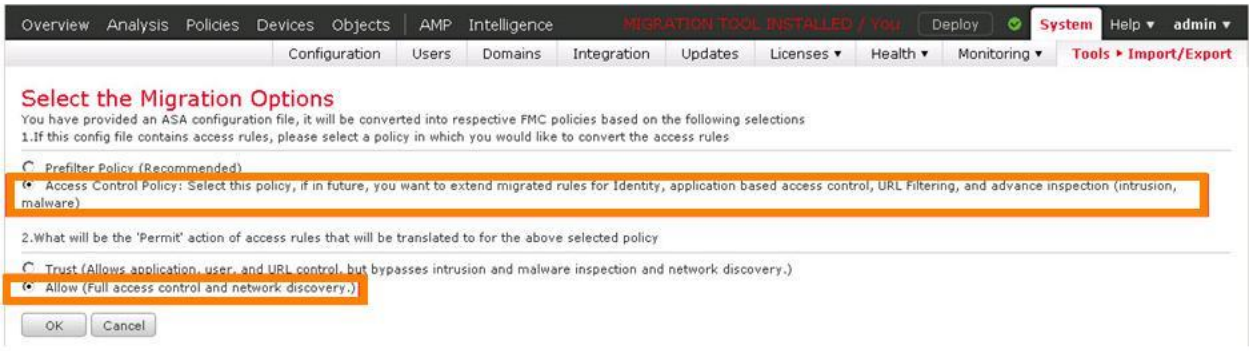
   c. プレフィルタ ポリシーは、前の手順で検査したプレフィルタ ポリシーに設定されています。

NAT とサポートされていない機能を移行し、オブジェクトの再利用を検討する

このタスクには次の 3 つの目的があります。それらに直接的な関係はありません。便宜上まとめられたものです。

- NAT ポリシーを移行する
- オブジェクトの再利用について理解する
- 時間ベースの ACL の移行を試み、サポートされていない機能の扱いを確認する

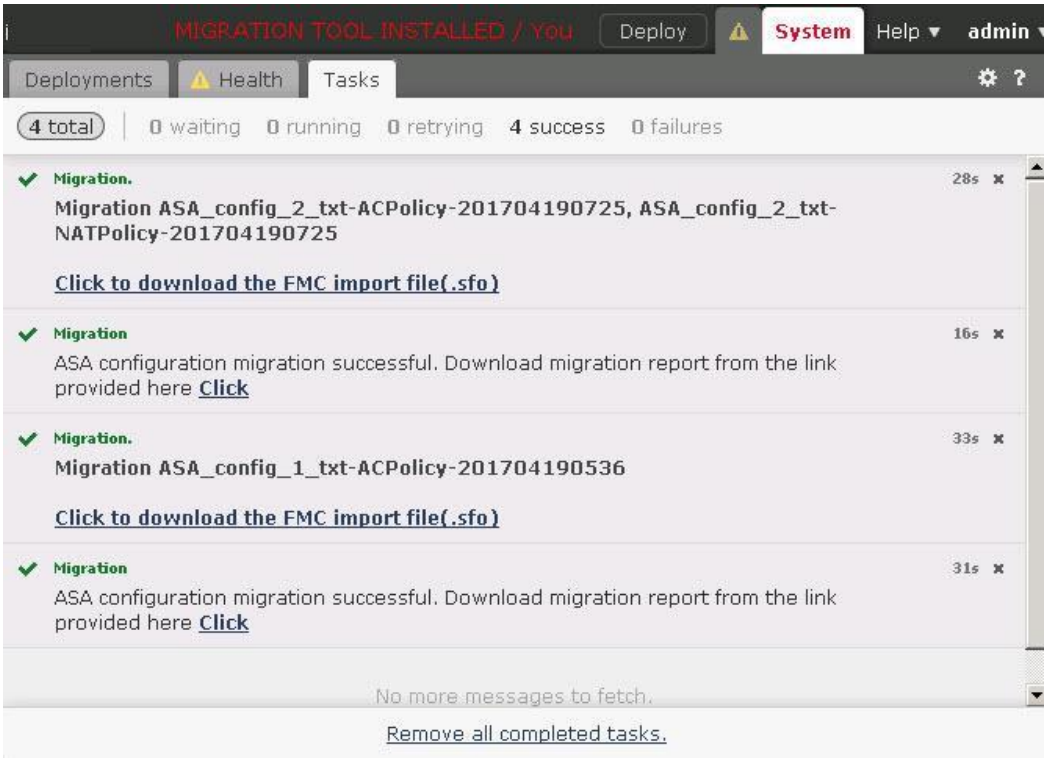
1. Jump の **Files** フォルダで、**ASA_config_2.txt** ファイルを開きます。
    a. ASA 設定で、FMC 内にすでに 2 つのネットワーク オブジェクトが存在することを確認します。
        - 同じ名前の既存のオブジェクトとは定義が異なる、ネットワーク オブジェクト **net1**
        - 同じ名前の既存のオブジェクトと定義が同じである、ネットワーク オブジェクト **net2**
    b. スタティック NAT ルールがあることを確認します。
    c. 時間ベースの ACL があることを確認します。この機能は現在サポートされていません。
2. Migrator の UI（FMC ではない）で、[システム（System）] > [ツール（Tools）] > [インポート/エクスポート（Import/Export）] に移動します。
    a. [パッケージのアップロード（Upload Package）] をクリックします。
    b. [参照（Browse）] をクリックし、**Files** フォルダから **ASA_config_2.txt** ファイルを選択します。[開く（Open）] をクリックします。
    c. [アップロード（Upload）] をクリックします。
3. 次のページで、以下に示すように [アクセス コントロール ポリシー（Access Control Policy）] および [許可（Allow）] オプション ボタンをオンにします。[OK] をクリックします。



4. アップロード ページに戻ります。

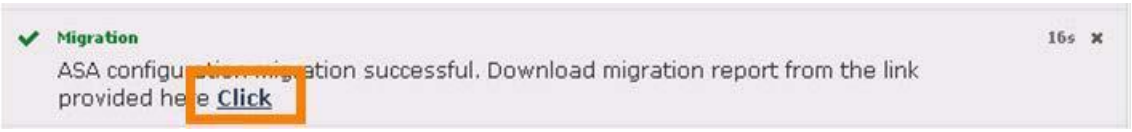
    a. [導入（Deploy）] ボタンの右にあるアイコンをクリックします。

    b. [タスク（Task）] タブをクリックし、タスクが完了するまで待ちます。

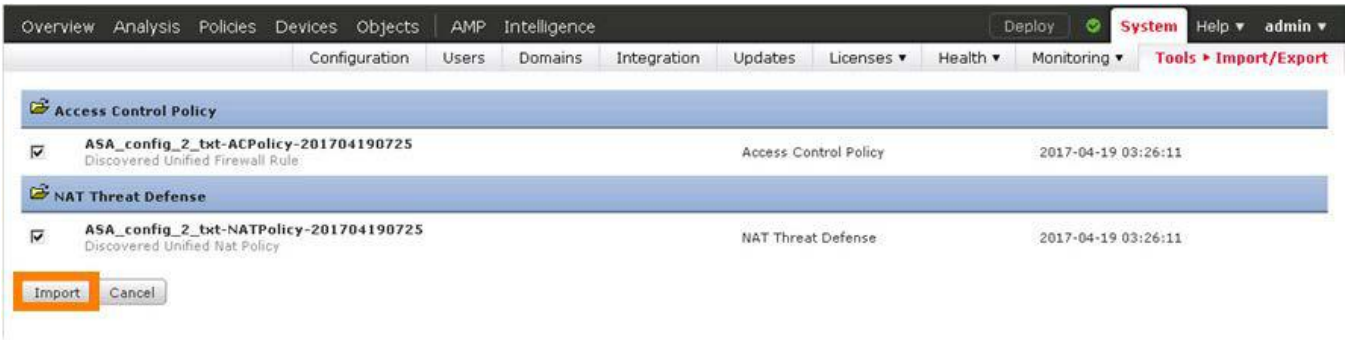


    c. [クリックして FMC インポート ファイル（.sfo）をダウンロード（Click to download the FMC import file(.sfo)）] というテキストをクリックして、SFO ファイルを保存します。

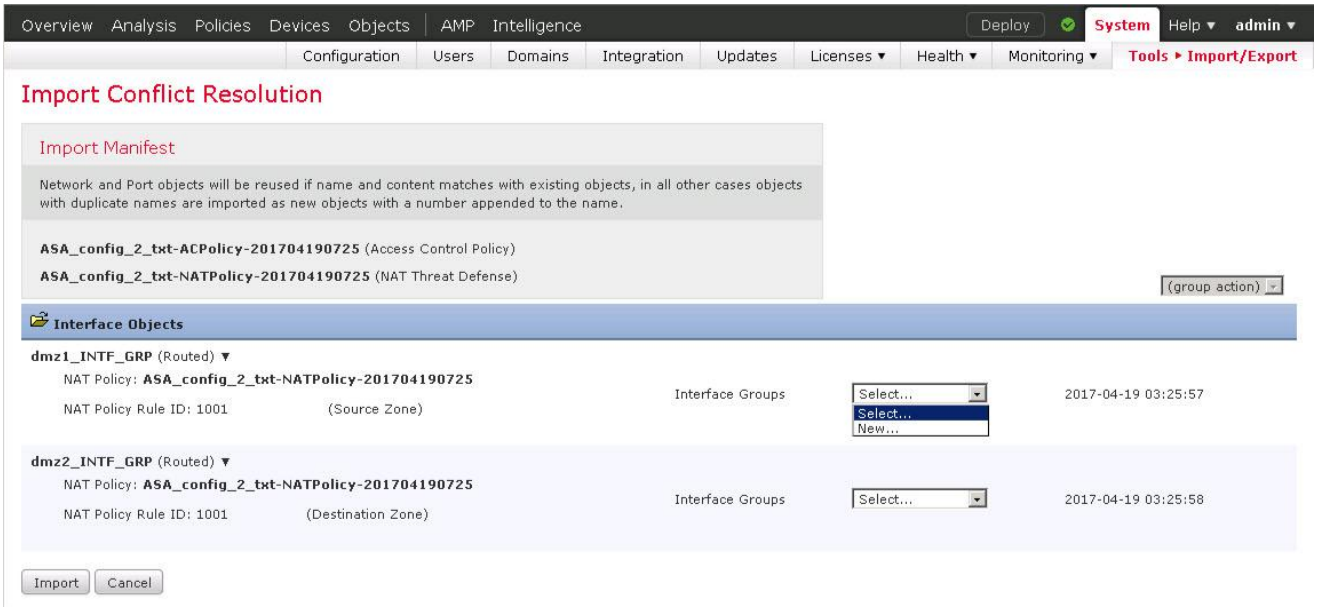
    d. [クリック（Click）] というテキストをクリックし、デフォルトの [Google Chrome で開く（Open with Google Chrome）] を選択すると、新しいタブで移行レポートが開きます。この移行レポートで、時間ベースの ACL がサポートされていないことが警告されていることを確認します。Chrome を閉じます。



5. （実稼働環境の）FMC UI で、[システム（System）] > [ツール（Tools）] > [インポート/エクスポート（Import/Export）] に移動します。
    a. [パッケージのアップロード（Upload Package）] ボタンをクリックします。
    b. [参照（Browse）] をクリックし、Downloads フォルダから SFO を選択します。このファイルの名前は、**ExportForMigration-<some UUID>.sfo** の形式になっています。できるだけ最近作成された SFO ファイルを選択してください。
    c. [アップロード（Upload）] をクリックします。
6. 次のページで [インポート（Import）] をクリックします。



7. 次のページで、次のサブ手順を実行します。次の図を参照してください。



    a. オブジェクトの競合の解決に関する情報を読みます。
    b. このページのドロップダウン リストを使用して、2 つのインターフェイス グループを作成します。移行された NAT ルールのインターフェイス参照は、インターフェイス グループに配置する必要があります。セキュリティ ゾーンは許可されていません。それらには **IF1** および **IF2** という名前を付けることができます。
    c. [インポート（Import）] をクリックします。

8. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動します。[ネットワーク（Network）] オブジェクト ページが選択されます。

    a. オブジェクト **net1_1** が作成されています。これは、移行された 2 つの ASA 設定で **net1** の定義が異なるためです。そのため、オブジェクトの名前が変更されています。

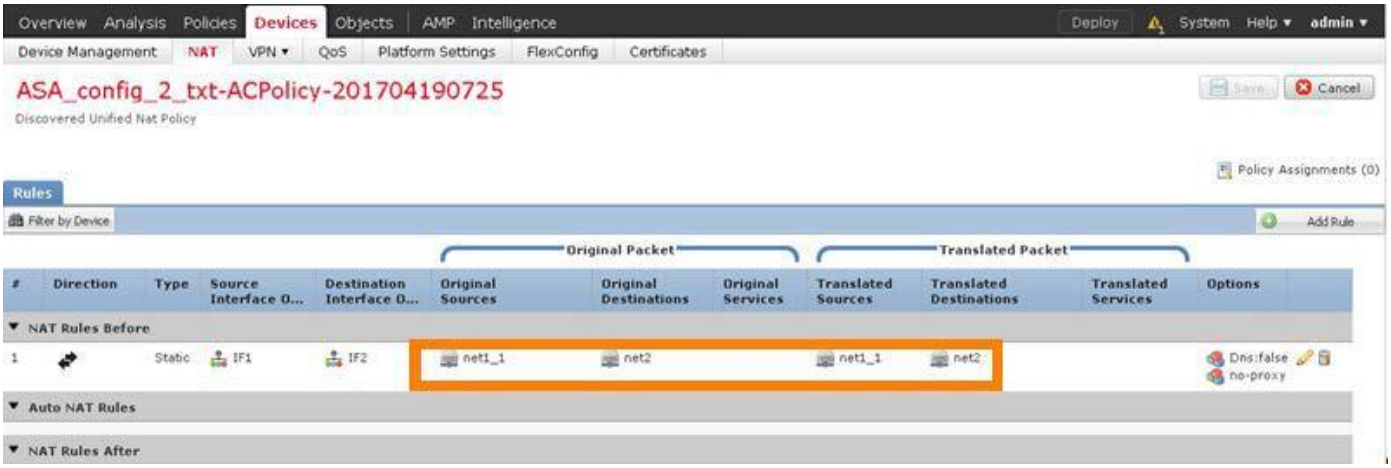
    b. オブジェクト **net2_1** は作成されていません。これは、移行された 2 つの ASA 設定で **net2** の定義が同じであるためです。そのため、オブジェクトが再利用されています。

注：この動作は、Firepower 6.2.1 リリースでは変更されています。Firepower 6.2 では、両方のオブジェクトの名前が変更されます。

9. [デバイス（Devices）] > [NAT] に移動します。

    a. 新しい NAT ポリシーがあることを確認してください。ルールを検査できるように、このポリシーを編集します。

    b. このポリシーでは、オブジェクト **net1_1** と **net2** が参照されています。

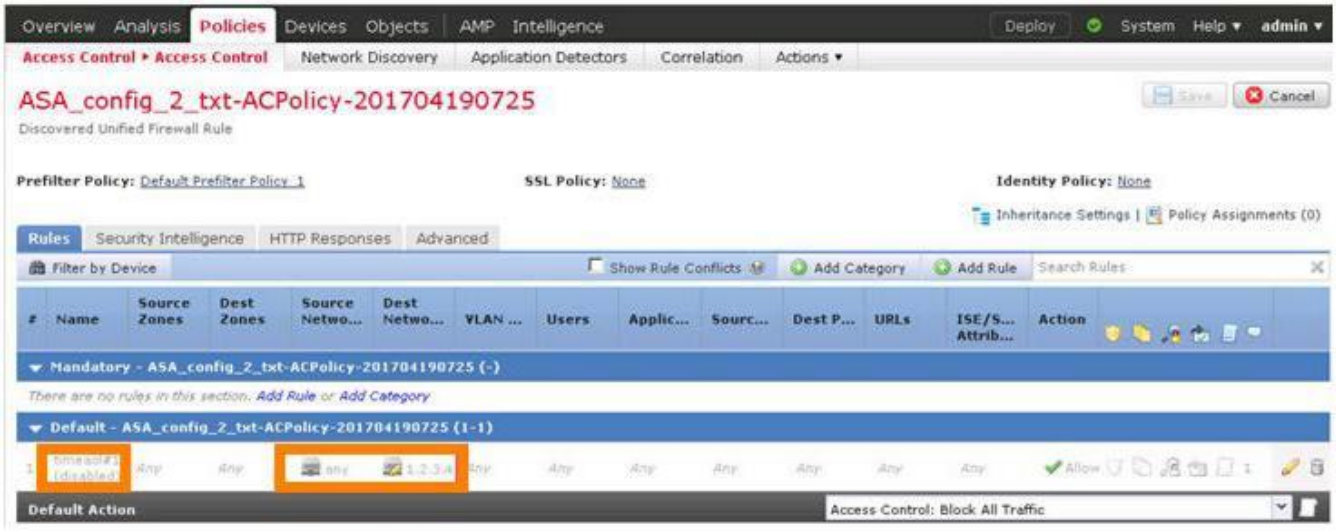


10. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] に移動します。

    a. 新しいアクセス コントロール ポリシーがあります。ルールを検査できるように、このポリシーを編集します。

    b. 元の ASA 設定の ACL は次のようになっていました。
    access-list timeacl extended permit ip any host 1.2.3.4 time-range office_hours
    これは、送信元と宛先が同じであるアクセス コントロール ポリシー ルールに変換されました。ただし、このアクセス コントロール ポリシー ルールには時間範囲属性がありません。

c. ルールが無効になっていることを確認してください。このルールは必要に応じて有効にすることができます。



注:移行ツールは、ネットワークと時間ベースの両方の基準が設定された ACL と合わせて提供されています。時間ベースの ACL は現在サポートされていないため、移行されたルールにはネットワーク基準のみが含まれます。これでは許容できない場合があるため、ルールを無効にし、手動で有効にしなければならないようにしています。

シナリオ 10.　NAT およびルーティング

この演習は、次のタスクで構成されています。

- このラボ演習に必要なオブジェクトを作成する
- スタティック NAT を設定する
- アクセス コントロール ポリシーを変更して wwwin への外部アクセスを許可する
- BGP を設定する
- 変更を導入して設定をテストする
- パブリック Web サーバを作成する
- BGP を設定する

最初の目的には、ネットワーク オブジェクトの作成とアクセス コントロール リストの作成が含まれます。また、スタティック NAT とダイナミック ルーティングも設定します。

手順

このラボ演習に必要なオブジェクトを作成する

1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動します。[ネットワーク（Network）] オブジェクト ページが選択されます。
    a. [ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）] の順にクリックします。
    b. [名前（Name）] に「**wwwin**」と入力します。
    c. [ネットワーク（Network）] に「**198.19.10.202**」と入力します。
    d. [保存（Save）] をクリックします。
    e. [ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）] の順にクリックします。
    f. [名前（Name）] に「**wwwout**」と入力します。
    g. [ネットワーク（Network）] に「**198.18.128.202**」と入力します。
    h. [保存（Save）] をクリックします。
    i. [ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）] の順にクリックします。
    j. [名前（Name）] に「**203.14.10.0**」と入力します。
    k. [ネットワーク（Network）] に「**203.14.10.0/24**」と入力します。
    l. [保存（Save）] をクリックします。

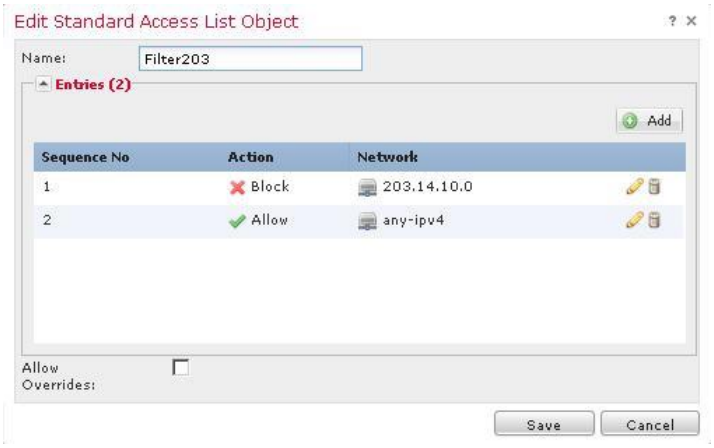
2. 左側のナビゲーション ペインで、[アクセス リスト（Access List）] > [標準（Standard）] の順に選択します。

    a. [標準アクセス リストを追加（Add Standard Access List）] をクリックします。

    b. [名前（Name）] で「**Filter203**」と入力します。

    c. 次に示す 2 つのアクセス制御エントリを追加します。2 番目のエントリは、リストの最後にあるすべてを対象とした暗黙の deny であるため、非常に重要です。

    d. [保存（Save）] をクリックします。



スタティック NAT を設定する

1. [デバイス（Devices）] > [NAT] に移動します。
2. 鉛筆アイコンをクリックして、[デフォルト PAT（Default PAT）] ポリシーを編集します。右上の [保存（Save）] ボタンがグレー表示になっていることを確認します。グレー表示になっていない場合は、一度戻って再度編集します。これは既知のバグです。

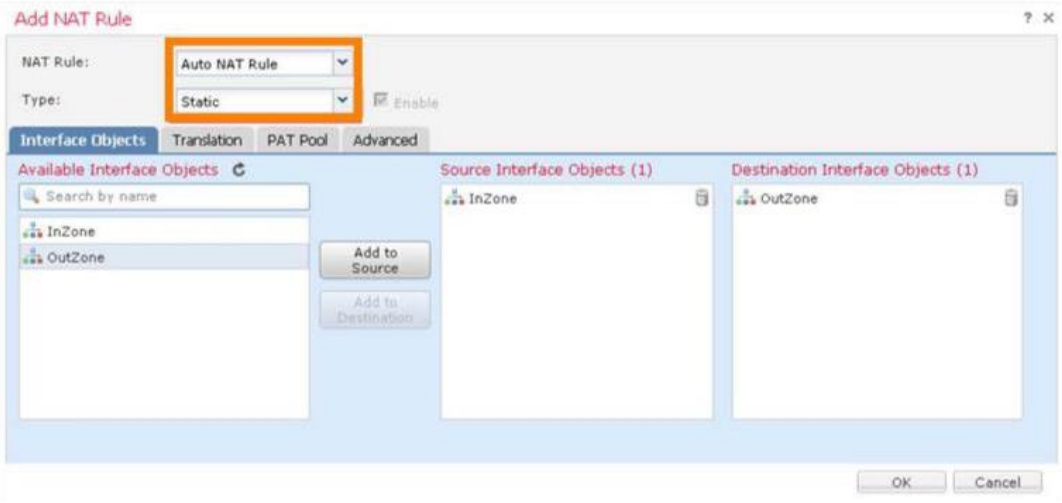
3. [ルールの追加（Add Rule）] をクリックします。

    a. [タイプ（Type）] ドロップダウン リストから [自動 NAT ルール（Auto NAT Rule）] を選択します。

    b. [インターフェイス オブジェクト（Interface Objects）] タブが表示されます。[InZone] を選択し、[送信元に追加（Add to Source）] をクリックします。

    移行シナリオを実行した場合は、2 つのインターフェイス グループから選択できます。これらは無視できます。

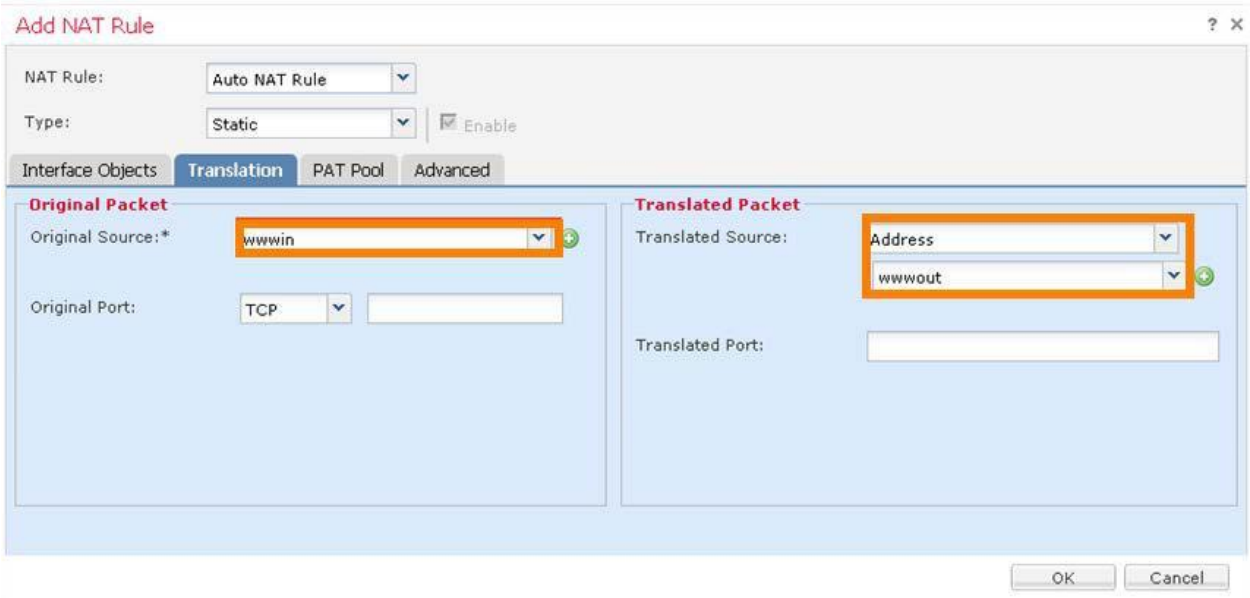
    c. [OutZone] を選択し、[宛先に追加（Add to Destination）] をクリックします。



d. [トランスレーション（Translation）] タブを選択します。

e. [元の送信元（Original Source）] ドロップダウン リストから [wwwin] を選択します。

f. [変換済み送信元（Translated Source）] ドロップダウン リストから [アドレス（Address）] と [wwwout] を選択します。



g. [OK] をクリックして NAT ルールを保存します。

4. [保存（Save）] をクリックして NAT ポリシーを保存します。

アクセス コントロール ポリシーを変更して wwwin への外部アクセスを許可する

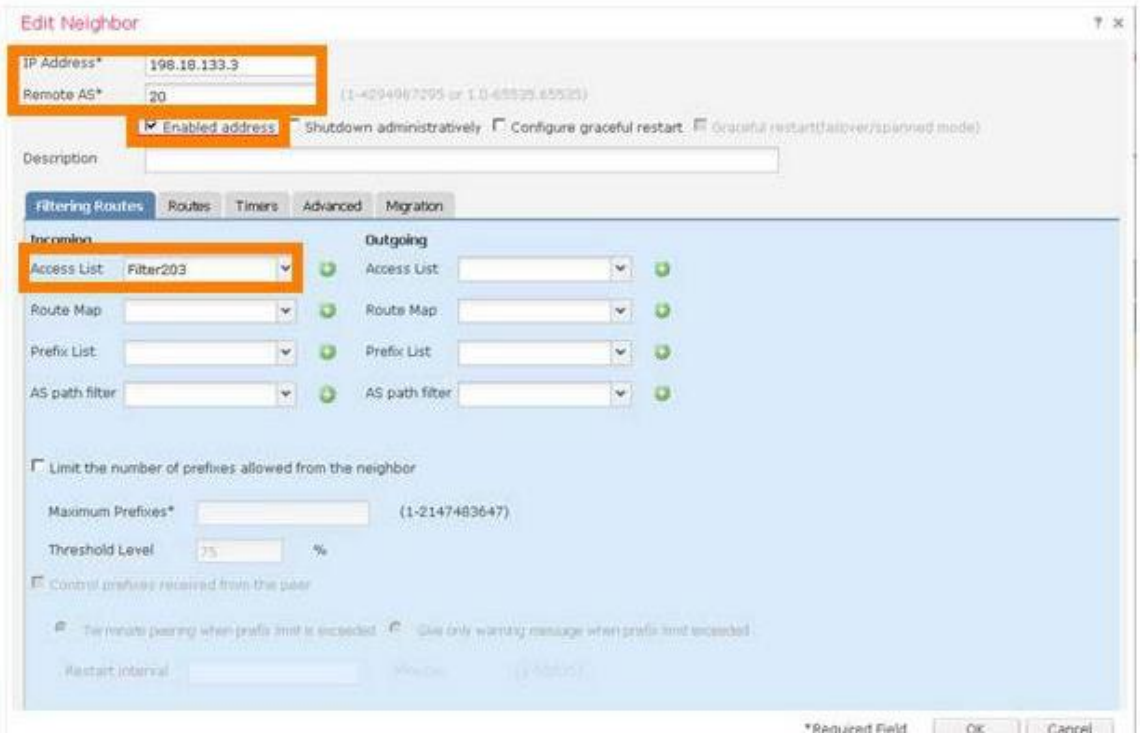
1. [ポリシー(Policies)] > [アクセス制御(Access Control)] > [アクセス制御(Access Control)] の順に選択します。[NGFW アクセス コントロール ポリシー(NGFW Access Control Policy)] を編集します。
2. [ルールの追加(Add Rule)] をクリックします。
    a. [名前(Name)] に「**`Web Server Access`**」と入力します。
    b. [挿入(Insert)] ドロップダウン リストから [デフォルトに挿入(into Default)] を選択します。
    c. [ゾーン(Zones)] タブがすでに選択されているはずです。[InZone] を選択し、[宛先に追加(Add to Destination)] をクリックします。
    d. [OutZone] を選択し、[送信元に追加(Add to Source)] をクリックします。
    e. [ネットワーク(Networks)] タブを選択します。
    f. [wwwin] を選択し、[宛先に追加(Add to Destination)] をクリックします。

注:クライアントが接続する NAT されたアドレスではなく、Web サーバの正しい IP を使用している点に注意してください。

    g. [ポート(Ports)] タブを選択します。
    h. [HTTP] と [HTTPS] を選択し、[宛先に追加(Add to Destination)] をクリックします。
    i. [検査(Inspection)] タブを選択します。
    j. [侵入ポリシー(Intrusion Policy)] ドロップダウン リストから [デモ侵入ポリシー(Demo Intrusion Policy)] を選択します。
    k. [ファイル ポリシー(File Policy)] ドロップダウン リストから [デモ ファイル ポリシー(Demo File Policy)] を選択します。
    l. [追加(Add)] をクリックしてルールを追加します。
3. [保存(Save)] をクリックして、アクセス コントロール ポリシーの変更を保存します。

BGP を設定する

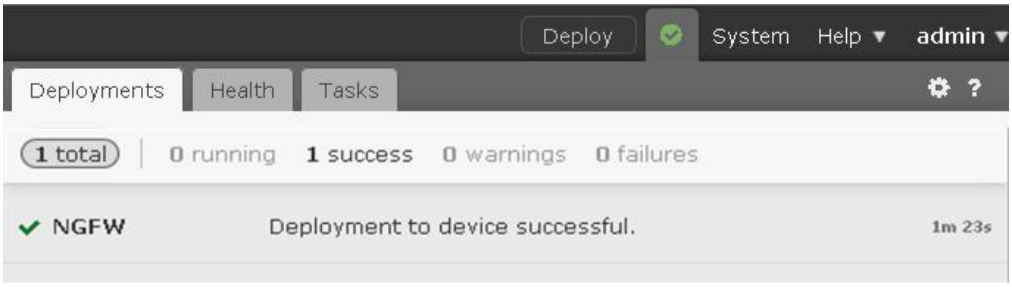
1. [デバイス(Devices)] > [デバイス管理(Device Management)] に移動します。
2. 鉛筆アイコンをクリックして、デバイス **NGFW** のデバイス設定を編集します。
3. [ルーティング(Routing)] タブを選択します。
    a. [BGP] を選択し、[BGP を有効にする(Enable BGP)] チェックボックスをオンにします。
    b. [AS 番号(AS Number)] を 10 に設定します。
    c. 左側のナビゲーション ペインで [BGP] を展開し、[IPv4] を選択します。
    d. [IPv4 を有効にする(Enable IPv4)] チェックボックスをオンにします。
    e. [ネイバー(Neighbor)] タブをクリックし、[追加(Add)] をクリックします。
        i. [IP アドレス(IP Address)] に「**`198.18.133.3`**」と入力します。
        ii. [リモート AS(Remote AS)] に「**`20`**」と入力します。
        iii. [アドレスを有効にする(Enable address)] チェックボックスをオンにします。
        iv. [着信アクセス リスト(Incoming Access List)] ドロップダウン リストから [Filter203] を選択します。
        v. [OK] をクリックして、ネイバーを追加します。



f. [保存(Save)] をクリックして BGP 設定を保存します。

変更を導入して設定をテストする

1. 変更を導入し、導入が完了するまで待ちます。



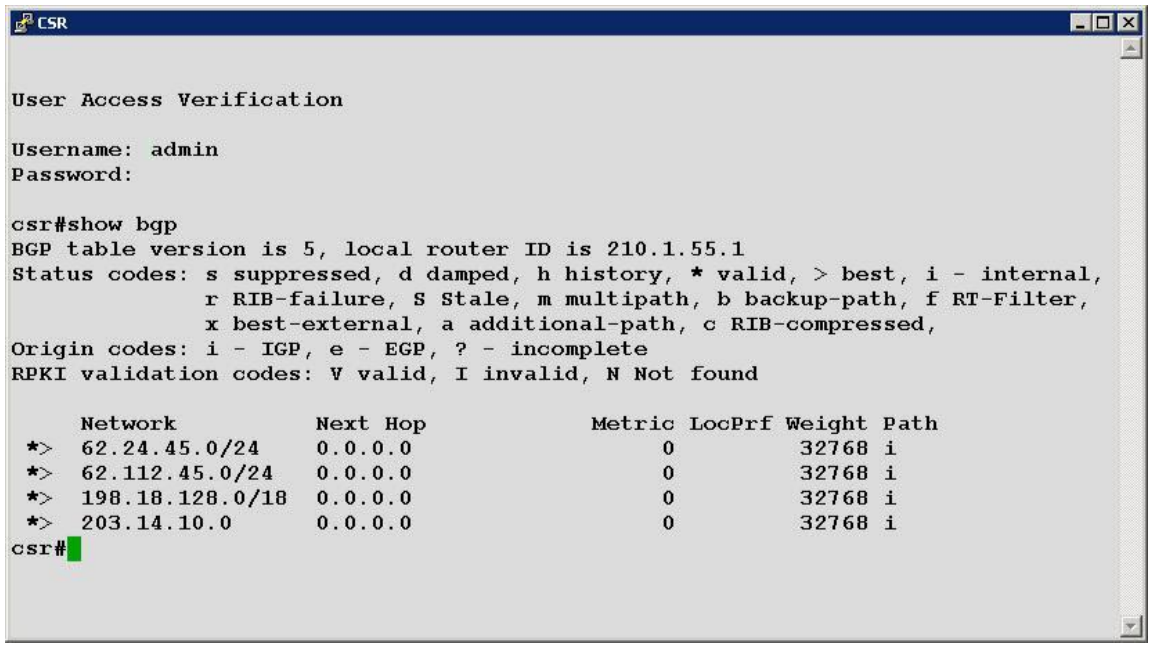
2. Jump Desktop で PuTTY リンクを開きます。[外部 Linux サーバ(Outside Linux Server)] という事前設定されたセッションをダブルクリックします。**root** として、パスワード **C1sco12345** でログインします。

   a. 「**curl wwwout**」と入力します。これは成功するはずです。

   b. 「**ssh wwwout**」と入力します。これは失敗するはずです。

3. Jump Desktop で PuTTY リンクを開きます。[CSR] という事前設定されたセッションをダブルクリックします。**admin** として、パスワード **C1sco12345** でログインします。

4. CSR の CLI で、show bgp コマンドを実行し、4 つのルートが表示されることを確認します。



5. NGFW の CLI で次を実行します。

   a. **`show route`** を実行します。BGP から学習した唯一のルートが 62.24.45.0/24 および 62.112.24.0/24 であることを確認します。203.14.10.0/24 が BGP から正常に除外されている点に注意してください。ただし FlexConfig シナリオを実行した場合は、このルートが外部 EIGRP ルートとして表示されます。

   b. **`show bgp`** および **`show bgp rib-failure`** を実行します。これにより、198.18.128.0/18 ルートは、より適したルート（接続済み）が存在したために、ルーティング テーブルに挿入されなかったことがわかります。

注：このコマンドは、FMC から実行することもできます。
1. [デバイス（Devices）] > [デバイス管理（Device Management）] に移動します。
2. **NGFW** デバイスを編集し、[デバイス（Devices）] タブを選択します。
3. [ヘルス（Health）] セクションで [ステータス（Status）] の右側にあるアイコンをクリックします。
4. [高度なトラブルシューティング（Advanced Troubleshooting）] をクリックします。
4. [脅威対策 CLI（Threat Defense CLI）] タブを選択します。
ここから複数の NGFW CLI コマンドを実行できます。

6. 内部 Linux サーバ セッションで、「**`ping 62.24.45.1`**」と入力します。これは成功するはずです。

シナリオ 11.　サイト間 VPN

この演習は、次のタスクで構成されています。

- このラボ演習に必要なオブジェクトを作成する
- サイト間 VPN を設定する
- NAT 適用除外を作成する
- アクセス コントロール ポリシーを変更し、変更を導入する
- 変更を導入して設定をテストする

この演習の目的は、NGFW と ASA の間にサイト間 VPN トンネルを設定することです。

手順

このラボ演習に必要なオブジェクトを作成する

1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動します。[ネットワーク（Network）] オブジェクト ページが選択されます。
    a. [ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）] の順にクリックします。
    b. [名前（Name）] に「**MainOfficeNetwork**」と入力します。
    c. [ネットワーク（Network）] に「**198.19.10.0/24**」と入力します。
    d. [保存（Save）] をクリックします。
    e. [ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）] の順にクリックします。
    f. [名前（Name）] に「**BranchOfficeNetwork**」と入力します。
    g. [ネットワーク（Network）] に「**198.19.11.0/24**」と入力します。
    h. [保存（Save）] をクリックします。

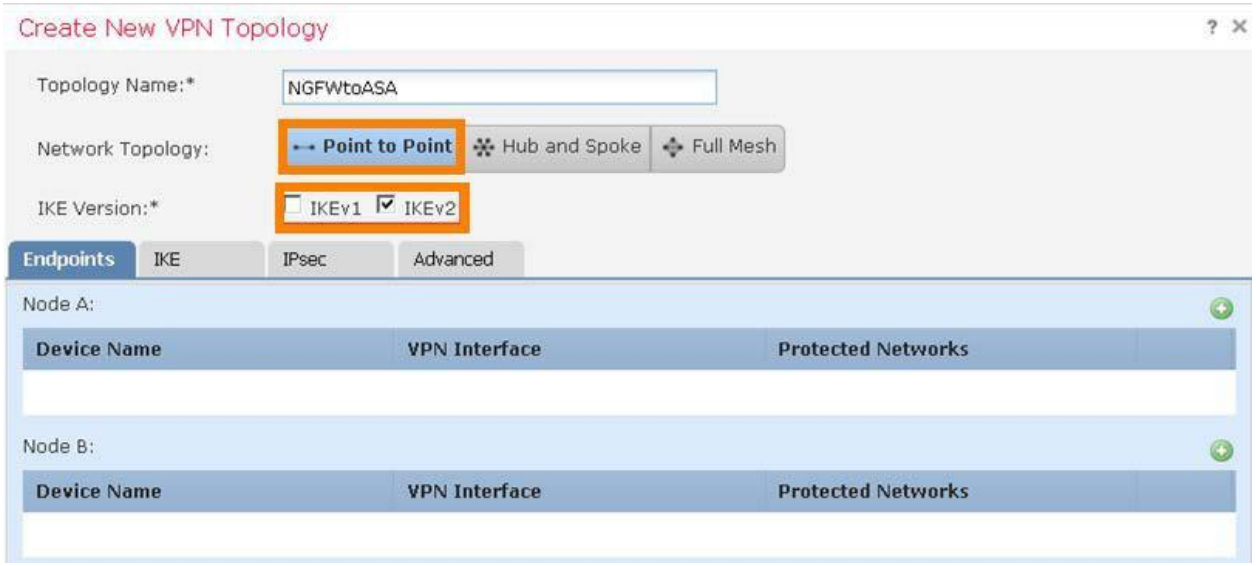
サイト間 VPN を設定する

1. [デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] に移動します。[VPN の追加（Add VPN）] > [Firepower 脅威対策デバイス（Firepower Threat Defense Device）] をクリックします。

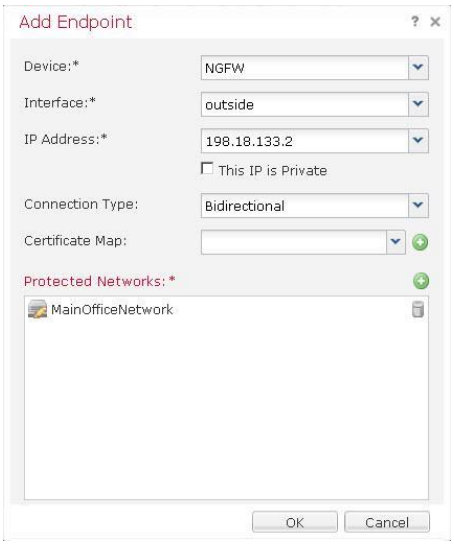
注:もう 1 つの VPN の選択肢、[Firepower デバイス（Firepower Device）] は、Firepower デバイス間でのセキュア トンネルの設定用です。

2. [名前（Name）] に「**NGFWtoASA**」と入力します。

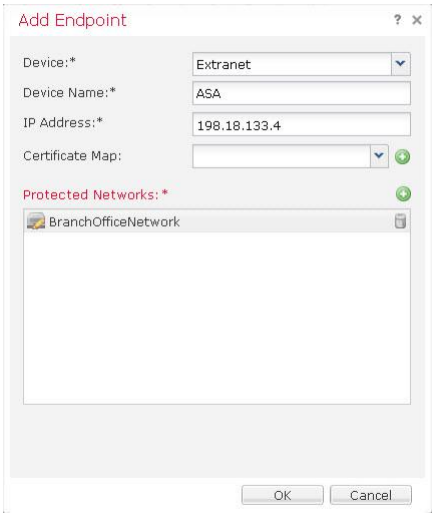
3. [ネットワークトポロジ（Network Topology）] で [ポイントツーポイント（Point to Point）] が選択されていることを確認します。[IKE バージョン（IKE Version）] で [IKEv1] がオフで、[IKEv2] がオンであることを確認します。



4. [ノード A（Node A）] の右側にある、緑色のプラス記号をクリックします。次の図のように入力し、[OK] をクリックします。



5. [ノード B（Node B）] の右側にある、緑色のプラス記号をクリックします。次の図のように入力し、[OK] をクリックします。



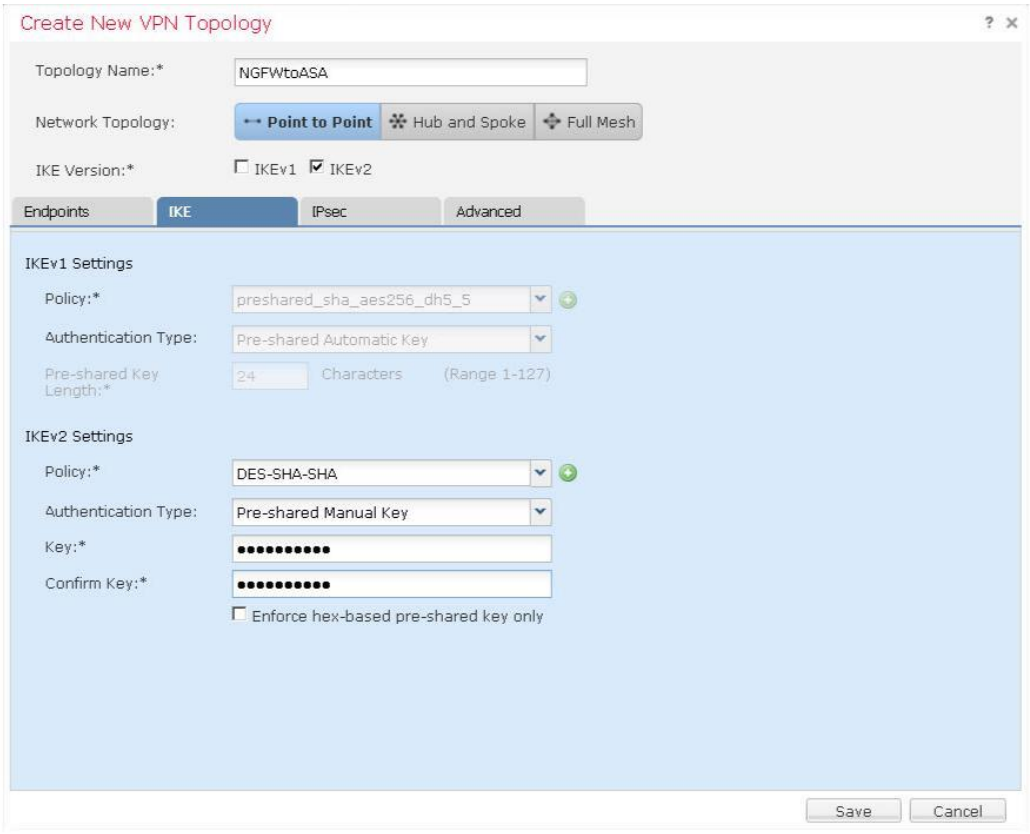
6. [IKE] タブを選択します。

   a. [IKEv2 設定（IKEv2 Settings）] の下の [ポリシー（Policy）] で、[DES-SHA-SHA] を選択します。

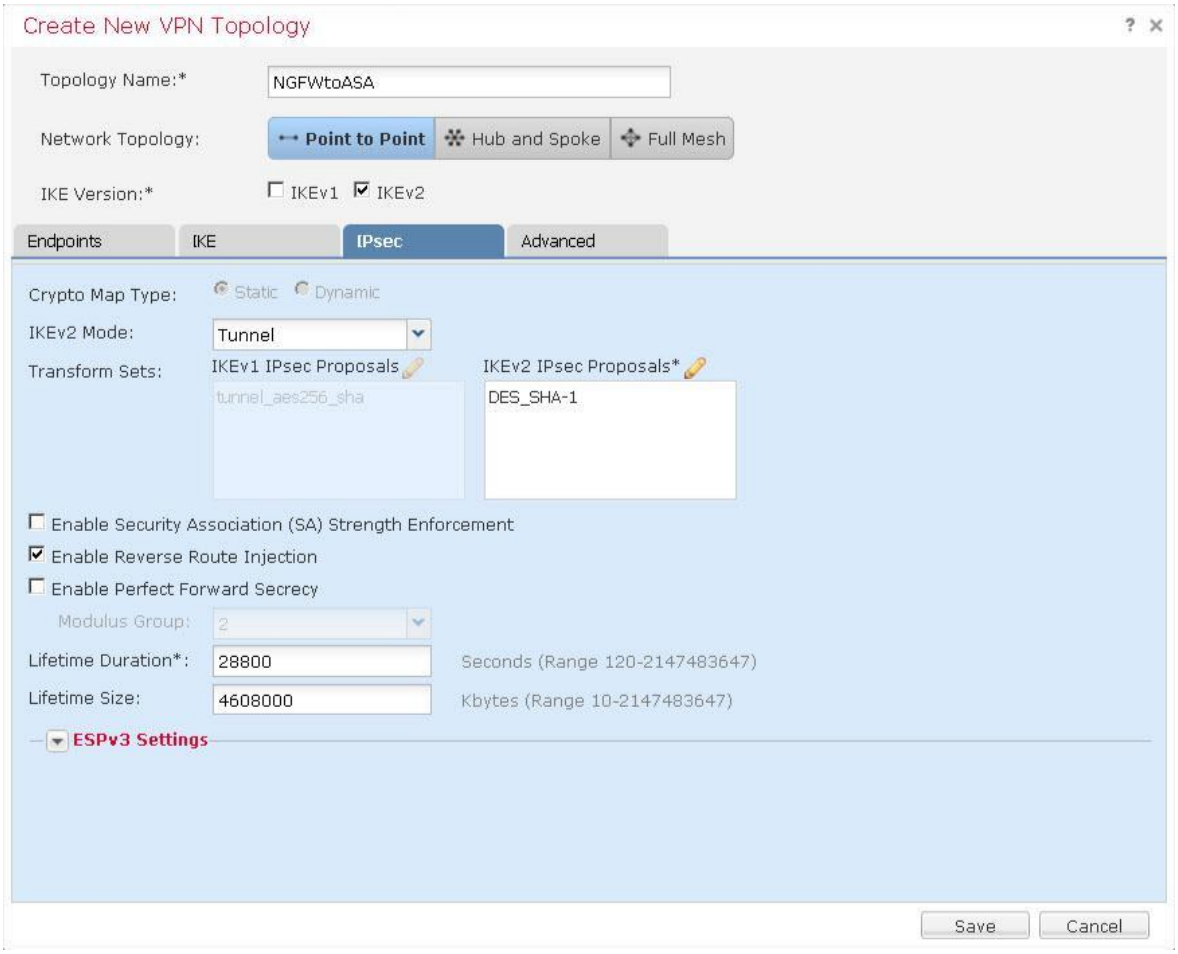
   b. [IKEv2 設定（IKEv2 Settings）] の下の [認証タイプ（Authentication Type）] で、[事前共有手動キー（Pre-shared Manual Key）] を選択します。

注：[自動（Automatic）] 設定は、FMC が両方のエンドポイントを管理している場合にのみ使用できます。この場合、FMC はランダム共有キーを生成できます。

   c. [IKEv2 設定（IKEv2 Settings）] の下の [キー（Key）] で、「**C1sco12345**」と入力し、エントリを確認します。



7. [IPsec] タブを選択して、[IKEv2 IPsec プロポーザル（IKEv2 IPsec Proposal）] を [DES_SHA-1] に変更します。



8. [保存（Save）] をクリックして VPN 設定を保存します。

NAT 適用除外を作成する

1. [デバイス（Devices）] > [NAT] に移動します。
2. 鉛筆アイコンをクリックして、[デフォルト PAT（Default PAT）] ポリシーを編集します。
3. [ルールの追加（Add Rule）] をクリックします。
    a. [NAT ルール（NAT Rule）] ドロップダウン リストで [カテゴリに挿入（In Category）] と [次の前の NAT ルール（NAT Rules Before）] が選択されたままにします。
    b. [インターフェイス オブジェクト（Interface Objects）] タブが表示されます。
        i. [InZone] を選択し、[送信元に追加（Add to Source）] をクリックします。
        ii. [OutZone] を選択し、[宛先に追加（Add to Destination）] をクリックします。

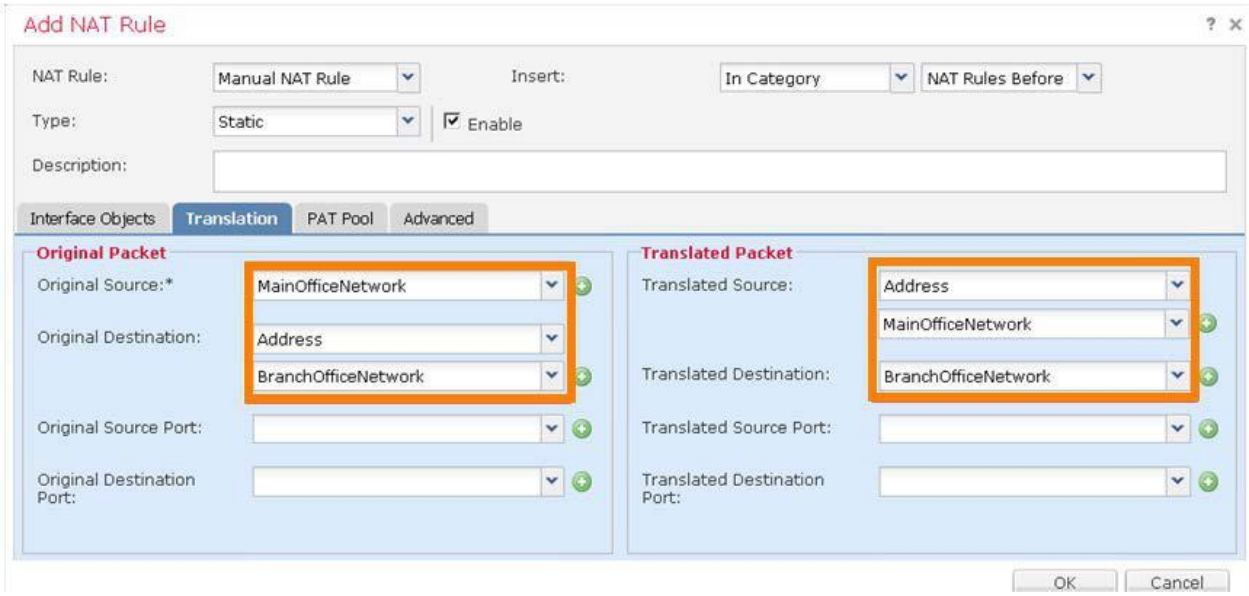
c. [トランスレーション（Translation）] タブを選択します。

i. [元の送信元（Original Source）] ドロップダウン リストから [MainOfficeNetwork] を選択します。

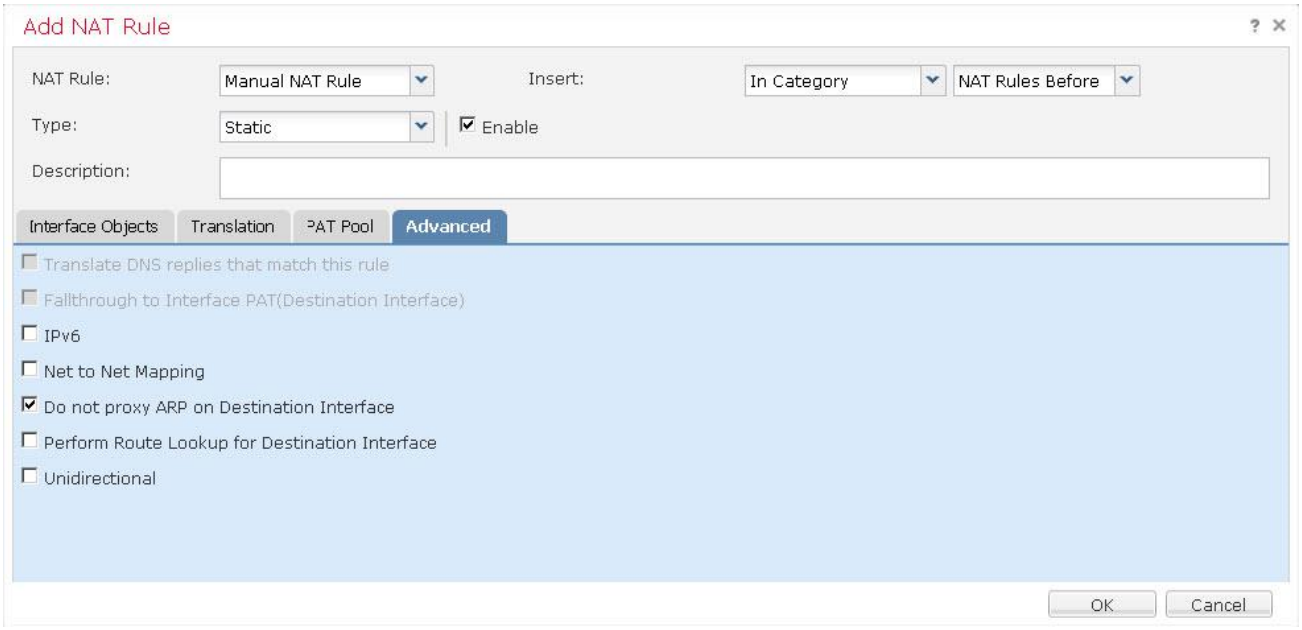
ii. [変換済み送信元（Translated Source）] ドロップダウン リストから [MainOfficeNetwork] を選択します。

iii. [元の宛先（Original Destination）] ドロップダウン リストから [BranchOfficeNetwork] を選択します。

iv. [変換済み宛先（Translated Destination）] ドロップダウン リストから [BranchOfficeNetwork] を選択します。



d. [詳細（Advanced）] タブを選択して、[宛先インターフェイスでプロキシ ARP を有効にしない（Do not proxy ARP on Destination Interface）] チェックボックスをオンにします。



e. [OK] をクリックして NAT ルールを保存します。

4. [保存（Save）] をクリックして NAT ポリシーを保存します。

アクセス コントロール ポリシーを変更し、変更を導入する

ブランチ オフィスと本社の間のトラフィックを許可するルールを作成します。

1. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] の順に選択します。[NGFW アクセス コントロール ポリシー（NGFW Access Control Policy）] を編集します。
2. [ルールの追加（Add Rule）] をクリックします。
    a. このルールを「**VPN Access**」という名前にします。
    b. [挿入（Insert）] ドロップダウン リストから [デフォルトに挿入（into Default）] を選択します。これは、アクセス コントロール ポリシーで最後のルールになります。
    c. アクションは [許可（Allow）] のままにします。
    d. [ゾーン（Zones）] タブがすでに選択されているはずです。
    e. [OutZone] を選択し、[送信元に追加（Add to Source）] をクリックします。
    f. [InZone] を選択し、[宛先に追加（Add to Destination）] をクリックします。
    g. [ネットワーク（Networks）] タブから [BranchOfficeNetwork] を選択し、[送信元に追加（Add to Source）] をクリックします。
    h. [ネットワーク（Networks）] タブから [MainOfficeNetwork] を選択し、[宛先に追加（Add to Destination）] をクリックします。
    i. [検査（Inspection）] タブを選択します。
        i. [侵入ポリシー（Intrusion Policy）] ドロップダウン リストから [デモ侵入ポリシー（Demo Intrusion Policy）] を選択します。
        ii. [ファイル ポリシー（File Policy）] ドロップダウン リストから [デモ ファイル ポリシー（Demo File Policy）] を選択します。
    j. [追加（Add）] をクリックして、このルールをアクセス コントロール ポリシーに追加します。
3. [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

変更を導入して設定をテストする

1. 変更を導入し、導入が完了するまで待ちます。
2. NGFW の CLI で「**show crypto ipsec sa**」と入力します。IPSec セキュリティ アソシエーションは存在しないはずです。
3. 内部 Linux サーバの CLI で、「**ping branch**」と入力します。数秒後に、ping は成功します。
4. NGFW の CLI で「**show crypto ipsec sa**」と入力します。今度は、IPSec セキュリティ アソシエーションが存在します。
5. Jump Desktop で PuTTY リンクを開きます。[ブランチ Linux サーバ（Branch Linux Server）] という事前設定されたセッションをダブルクリックします。
    a. **root** として、パスワード **C1sco12345** でログインします。
    b. 「**curl inside**」と入力します。これは成功するはずです。

シナリオ 12.　Web プロキシの統合

この演習は、次のタスクで構成されています。

- WSA の設定を変更する
- XFF タイプのヘッダーの使用を設定する
- アクセス コントロール ポリシーを導入する
- 変更を導入して設定をテストする

NGFW では XFF タイプのヘッダーを使用して、プロキシ サーバではなく実際のクライアントにポリシーを適用できます。この演習の目的は、受講者が True-Client-IP 機能に慣れるようにすることです。この機能では、Web プロキシを通じてトラフィックを送信するエンドポイントに、NGFW がポリシーを適用できます。

ここで設定するルールは人為的なものですが、テストを簡単にすることを目的としています。

手順

WSA の設定を変更する

1. Jump Desktop で PuTTY リンクを開きます。[WSA] という事前設定されたセッションをダブルクリックします。**admin** として、パスワード **C1sco12345** でログインします。
2. WSA の CLI で次の CLI コマンドを実行します。

```
wsa.dcloud.local> setgateway

Warning: setting an incorrect default gateway may cause the current connection to be
interrupted when the changes are committed.
Set the default gateway for:
1. IPv4
2. IPv6
[1]> 1

Enter new default gateway:
[198.19.10.11]> 198.19.10.1

wsa.dcloud.local> commit

Please enter some comments describing your changes:
[]> Changing gateway

Changes committed: Mon Oct 02 00:01:11 2017 GMT
wsa.dcloud.local>
```

3. WSA が、X-Forwarded-For ヘッダーを生成するように設定されていることを確認します。これはデフォルトの設定ではありません。
    a. Firefox ブラウザで新しいタブを開きます。
    b. ブックマーク バーのリンク [WSA] をクリックします。**admin** として、パスワード **C1sco12345** でログインします（このクレデンシャルは事前に入力されているはずです）。
    c. WSA の UI で、[セキュリティ サービス（Security Services）] > [Web プロキシ（Web Proxy）] に移動します。
    d. [詳細設定（Advanced Settings）] の下の [ヘッダーの生成（Generate Headers）] で、**X_Forwarded-For** ヘッダーが送信されていることを確認します。

XFF タイプのヘッダーの使用を設定する

1. [FMC] タブで、[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] に移動します。[NGFW アクセス コントロール ポリシー（NGFW Access Control Policy）] を編集します。
2. [ルールの追加（Add Rule）] をクリックします。
    a. このルールを「**Test XFF Feature**」という名前にします。
    b. [アクション（Action）] を [ブロックしてリセット（Block with reset）] に設定します。
    c. [挿入（Insert）] ドロップダウン リストから [必須ルールに挿入（into Mandatory）] を選択します。
    d. [ゾーン（Zones）] タブで [InZone] を選択し、[送信元に追加（Add to Source）] をクリックします。
    e. [ゾーン（Zones）] タブで [OutZone] を選択し、[宛先に追加（Add to Destination）] をクリックします。
    f. [ネットワーク（Networks）] タブを選択します。
        i. [送信元ネットワーク（Source Networks）] 領域で、[送信元（Source）] サブタブを選択します。ページの下部で「**198.19.10.101**」と入力し、[追加（Add）] をクリックします。これが WSA プロキシ サーバの IP アドレスです。
        ii. [送信元ネットワーク（Source Networks）] 領域で、[元のクライアント（Original Client）] サブタブを選択します。ページの下部で「**198.19.10.201**」と入力し、[追加（Add）] をクリックします。
        iii. [宛先ネットワーク（Destination Networks）] 領域のページの下部で、「**198.18.133.201**」と入力し、[追加（Add）] をクリックします。
    g. [ロギング（Logging）] タブを選択します。[接続開始時にロギング（Log at Beginning of Connection）] チェックボックスをオンにします。
    h. [追加（Add）] をクリックして、ポリシーにルールを追加します。
    i. [保存（Save）] をクリックしてポリシーの変更を保存します。

変更を導入して設定をテストする

1. 変更を導入し、導入が完了するまで待ちます。
2. 内部 Linux サーバ PuTTY セッションに戻ります。次のコマンドを実行して、設定をテストします。
    a. 次のコマンド(1 行)を実行します。
    `wget --bind-address=198.19.10.201 -e use_proxy=yes -e http_proxy=198.19.10.101 198.18.133.201`
    403(禁止)応答コードが返されます。
    b. 次のコマンド(1 行)を実行します。
    `wget --bind-address=198.19.10.200 -e use_proxy=yes -e http_proxy=198.19.10.101 198.18.133.201`
    これは成功するはずです。

注:ファイルが WSA でキャッシュされたため、手順 2a を繰り返すと、ファイルがダウンロードされます。実稼働環境でこれを回避するには、クライアントと WSA 間に NGFW を導入する必要があります。テストのために、「**`diagnostic`**」、「**`PROXY`**」、「**`CACHE`**」と入力して、WSA CLI から WSA プロキシ キャッシュをクリアします。

3. FMC で、[分析(Analysis)] > [接続(Connections)] > [イベント(Events)] に移動します。
    a. テキスト [接続イベントのテーブル ビュー(Table View of Connection Event)] をクリックします。
    b. デフォルトでは [元のクライアント IP(Original Client IP)] 列が表示されません。ここでそれを追加します。
    c. 追加するには、次の手順を実行します。
        i. 使用されていない任意の列の上部にある [X] をクリックします。
        ii. 列セレクタを、[無効な列(Disabled Columns)] まで下方向にスクロールします。
        iii. [元のクライアント IP(Original Client IP)] チェックボックスをオンにします。
        iv. 列セレクタの最下部までスクロールし、[適用(Apply)] をクリックします。
    d. WSA の IP(198.19.10.101)とクライアント IP(198.19.10.201)の両方が表示されていることを確認します。

シナリオ 13.　プレフィルタ ポリシー

この演習は、次のタスクで構成されています。

- トンネリングされたトラフィックに関する NGFW のデフォルト動作を調査する
- トンネル ゾーンを作成する
- プレフィルタ ポリシーを作成する
- アクセス コントロール ポリシーを変更する
- 変更を導入して設定をテストする

プレフィルタ ポリシーには、2 つのタイプのルール（プレフィルタおよびトンネル）があります。一般にはプレフィルタ ルールが使用されています。これらのルールは、Lina データプレーンでドロップされるトラフィック、Snort をバイパスするトラフィック、Snort に送信されるトラフィックを指定します。これはパフォーマンスの向上につながります。このシナリオでは後でプレフィルタを設定しますが、シナリオの中心になるのは、より詳細なトンネル ルールです。

クリアテキスト トンネルが存在する場合は、**トンネリングされた**トラフィックに NGFW アクセス コントロール ポリシーが適用されます。プレフィルタ ポリシーにより、**トンネリング** プロトコルに対する制御が可能になります。次のトンネリング プロトコルがサポートされています。

- GRE
- IP-in-IP
- IPv6-in-IP
- Teredo

プレフィルタ ポリシーは、トンネル タグを利用してアクセス コントロール ポリシーと通信します。プレフィルタ ポリシーは、トンネル タグを指定されたトンネルに割り当てます。その結果、指定されたトンネル経由でトンネリングされたトラフィックにのみ適用されるルールを、アクセス コントロール ポリシーに含めることができるようになります。

この演習では、内部 CentOS サーバと外部 CentOS サーバ間の GRE トンネルを作成します。

その後、この GRE トンネルで ICMP をブロックするよう NGFW を設定します。

注:この演習では、シナリオ 10 を終了していることが前提条件になります。これは、198.19.10.202 を 198.18.128.202 に変換するスタティック NAT ルールをこの演習で使用するためです。トンネル インターフェイスの設定を理解するには、内部および外部サーバの **`/etc/sysconfig/network-scripts/ifcfg-tun0`** を確認します。

手順

トンネリングされたトラフィックに関する NGFW のデフォルト動作を調査する

このタスクでは、アクセス コントロール ポリシー ルールがトンネリングされたトラフィックに適用されることを確認します。

1. SSH セッションが内部 Linux サーバに対して今も開いている必要があります。
2. 外部 Linux サーバに対する SSH セッションがない場合は、Jump Desktop で PuTTY を起動し、事前定義されている [外部 Linux サーバ（Outside Linux Server）] セッションをダブルクリックします。**root** として、パスワード **C1sco12345** でログインします。
3. 内部 Linux サーバと外部 Linux サーバの間に GRE トンネルを作成します。
    a. 外部 Linux サーバの CLI で、「**ifup tun0**」と入力します。
    b. 内部 Linux サーバの CLI で、「**ifup tun0**」と入力します。
    c. 内部 Linux サーバで、トンネルを通じて ping を送信できることを次のコマンドで確認します。
    ping 10.3.0.2
4. IPS 機能をテストします。
    a. 内部 Linux サーバの CLI から、次のコマンドを実行します。
    ftp 10.3.0.2
    b. **guest** として、パスワード **C1sco12345** でログインします。
    c. 「**cd ~root**」と入力します。次のメッセージが表示されます。
    [421 サービスが使用できません。リモート サーバは接続を閉じています（421 Service not available, remote server has closed connection）]
    d. 「**quit**」と入力して、FTP を終了します。
5. FMC で、[分析（Analysis）] > [侵入（Intrusions）]> [イベント（Events）] に移動します。
    a. 左側の矢印をクリックして、イベントのテーブル ビューにドリルダウンします。
    b. 送信元および宛先 IP が、それぞれ 10.3.0.1 と 10.3.0.2 であることを確認します。
6. 内部 Linux サーバの CLI で次のコマンドを実行して、ファイル ブロックおよびマルウェア ブロック機能をテストします。

注：これらの Wget コマンドは、Jump Desktop の Strings to cut and paste.txt ファイルからカットして貼り付けることができます。

    a. 制御テストとして、WGET を使用してブロックされていないファイルをダウンロードします。
    wget -t 1 10.3.0.2/files/ProjectX.pdf
    これは成功するはずです。
    b. 次に、WGET を使用して、タイプによってブロックされたファイルをダウンロードします。
    wget -t 1 10.3.0.2/files/test3.avi
    ファイルのごく一部しかダウンロードされないことに注意してください。これは、NGFW が、データの最初のブロックからファイル タイプを検出できるためです。
    c. 最後に、WGET を使用してマルウェアをダウンロードします。
    wget -t 1 10.3.0.2/files/Zombies.pdf
    ファイルの 99 % がダウンロードされたことに注意してください。これは、NGFW が SHA の計算にファイル全体を必要とするためです。ハッシュが計算され、ルックアップされるまで、NGFW はデータの最後のブロックのダウンロードを保留します。

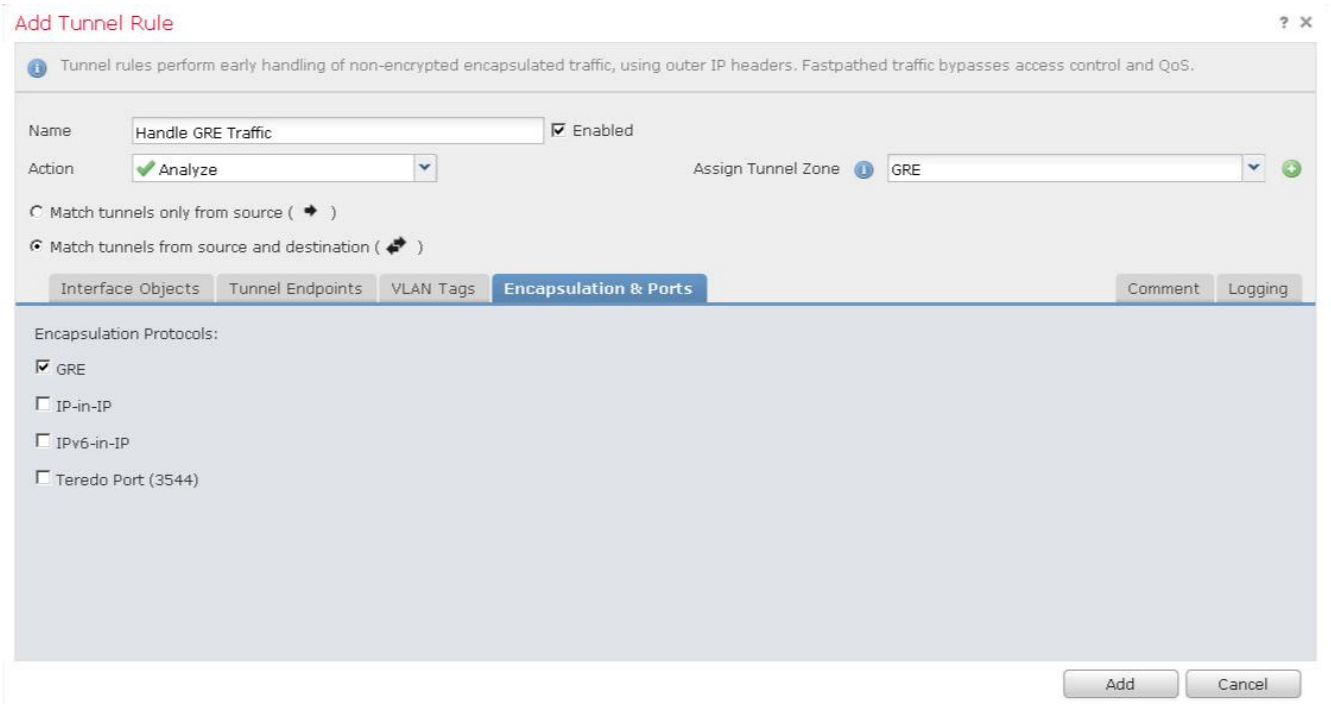
7. FMC で、[分析（Analysis）] > [ファイル（Files）] > [ファイル イベント（File Events）] に移動します。
    a. [ファイル イベントのテーブル ビュー（Table View of File Events）] をクリックします。
    b. 送信 IP と受信 IP が、それぞれ **10.3.0.2** と **10.3.0.1** であることを確認します。

トンネル ゾーンを作成する

1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動します。
    a. 左側のナビゲーション ペインで [トンネル ゾーン（Tunnel Zone）] を選択します。
    b. [トンネル ゾーンの追加（Add Tunnel Zone）] をクリックします。
    c. [名前（Name）] に「**GRE**」と入力します。
    d. [保存（Save）] をクリックします。

プレフィルタ ポリシーを作成する

1. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [プレフィルタ（Prefilter）] に移動します。
2. [新しいポリシー（New Policy）] をクリックします。「**NGFW Prefilter Policy**」などの名前を入力します。[保存（Save）] をクリックします。
3. 数秒後にポリシーが開き、編集できるようになります。
4. [トンネル ルールの追加（Add Tunnel Rule）] をクリックします。
    a. [名前（Name）] に「**Handle GRE Traffic**」と入力します。
    b. [トンネル ゾーンの割り当て（Assign Tunnel Zone）] ドロップダウン リストから [GRE] を選択します。
    c. [カプセル化およびポート（Encapsulation & Ports）] タブを選択し、[GRE] チェックボックスをオンにします。



注:3 つのアクションがあります。
• [分析(Analyze)]:トラフィックが Snort に送信され、アクセス ポリシー ルールが適用される
• [ブロック(Block)]:トラフィックがブロックされる
• [ファストパス(Fastpath)]:トラフィックが許可され、それ以上の検査がバイパスされる
このポリシーに対するプレフィルタ ルールを作成することもできます。これにより、レイヤ 2 から 4 の情報に基づいて、トラフィックの分析、ブロック、ファストパスが可能になります。

d. [追加(Add)] をクリックしてルールを追加します。

5. 次に、宛先が 198.18.133.202 であるトラフィックが Snort をバイパスするルールを追加します。このアドレスは信頼されています。[プレフィルタ ルールの追加(Add Prefilter Rule)] をクリックします。
   a. [名前(Name)] に「**`Example of Fastpath`**」と入力します。
   b. [Action(アクション)] ドロップダウン リストから [ファストパス(Fastpath)] を選択します。
   c. [ネットワーク(Networks)] タブを選択します。
   d. [宛先ネットワーク(Destination Networks)] 列の最下部に「**`198.18.133.202`**」と入力します。
   e. [追加(Add)] をクリックして宛先ネットワークを追加します。
6. [追加(Add)] をクリックして、プレフィルタ ルールを追加します。
7. [保存(Save)] をクリックして、プレフィルタ ポリシーを保存します。

アクセス コントロール ポリシーを変更する

1. [ポリシー(Policies)] > [アクセス制御(Access Control)] > [アクセス制御(Access Control)] の順に選択します。[NGFW アクセス コントロール ポリシー(NGFW Access Control Policy)] を編集します。
2. ポリシー ルール上の文字列 [プレフィルタ ポリシー(Prefilter Policy)] の右側のリンク [デフォルト プレフィルタ ポリシー(Default Prefilter Policy)] をクリックします。[NGFW プレフィルタ ポリシー(NGFW Prefilter Policy)] を選択します。[OK] をクリックします。
3. [ルール(Rules)] タブを選択します。
4. [ルールの追加(Add Rule)] をクリックします。
   a. このルールを「**`Block ICMP Over GRE`**」という名前にします。
   b. [挿入(Insert)] ドロップダウン リストから [必須ルールに挿入(into Mandatory)] を選択します。
   c. [アクション(Action)] を [ブロックしてリセット(Block with reset)] に設定します。
   d. [使用可能なゾーン(Available Zones)] 列で [GRE] を選択して、[送信元に追加(Add to Source)] をクリックします。
   e. [アプリケーション(Applications)] 列で [ICMP] を選択して、[ルールに追加(Add to Rule)] をクリックします。
   f. [ロギング(Logging)] タブを選択します。[接続開始時にロギング(Log at Beginning of Connection)] チェックボックスをオンにします。
   g. [追加(Add)] をクリックして、ポリシーにルールを追加します。
5. [ルールの追加(Add Rule)] をクリックします。
   a. 「**Allow GRE Traffic**」ルールを呼び出します。
   b. [挿入(Insert)] ドロップダウン リストから [デフォルトに挿入(into Default)] を選択します。これは、アクセス コントロール ポリシーで最後のルールになります。
   c. [使用可能なゾーン(Available Zones)] 列で [GRE] を選択して、[送信元に追加(Add to Source)] をクリックします。

d. [検査（Inspection）] タブを選択します。

   i. [侵入ポリシー（Intrusion Policy）] ドロップダウン リストから [デモ侵入ポリシー（Demo Intrusion Policy）] を選択します。

   ii. [ファイル ポリシー（File Policy）] ドロップダウン リストから [デモ ファイル ポリシー（Demo File Policy）] を選択します。

e. [追加（Add）] をクリックして、ポリシーにルールを追加します。

6. [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

変更を導入して設定をテストする

1. 以前と同様に、変更内容を導入します。導入が完了するまで待ちます。
2. 外部 Linux サーバで、**tcpdump -n -i tun0** を実行してトンネル トラフィックをモニタします。
3. 内部 Linux サーバの CLI で、次のコマンドを実行します。

   a. **wget 10.3.0.2**
   これは成功するはずです。

   b. **ping 10.3.0.2**
   ping がブロックされていることを示す次の出力が表示されます。
   From 10.3.0.2 icmp_seq=1 Packet filtered

4. 外部 Linux サーバの `tcpdump` コマンドの出力を調べて、ping が 10.3.0.2 に送信されていないことを確認します。
5. トンネルを切断します。

   a. 外部 Linux サーバの CLI で、「`ifdown tun0`」と入力します。

   b. 内部 Linux サーバの CLI で、「`ifdown tun0`」と入力します。

6. 次にプレフィルタ ルールをテストします。

   a. 次のように入力します。
   wget -t 1 198.18.133.200/files/Zombies.pdf
   This should be blocked.

   b. 次のように入力します。
   wget -t 1 198.18.133.202/files/Zombies.pdf
   トラフィックが Snort をバイパスしたため、これは許可されるはずです。

シナリオ 14.　Integrated Routing and Bridging（IRB）

この演習は、次のタスクで構成されています。

- このラボ演習に必要なオブジェクトを作成する
- NGFW インターフェイス設定を変更する
- NAT ポリシーを変更する
- アクセス コントロール ポリシーを変更する
- 設定を導入しテストする

このラボでは、GigabitEthernet0/2 に接続されている別の VLAN に Linux サーバがあります。このサーバの FQDN は **isolated.dcloud.local** で、IP アドレスは 198.19.10.220/24 です。このアドレスは、内部ネットワークと同じサブネット内にあります。

この演習の目的は、NGFW のブリッジ グループを使用して、これらの VLAN に参加することです。これらの VLAN 間のトラフィックが検査されます。

注:この演習では、ブリッジ グループ内の両方のインターフェイスが同じセキュリティ ゾーン内に配置されています。ただし、これは必須ではありません。ブリッジ グループには、異なるセキュリティ ゾーン内のインターフェイスを含めることができます。そのため、同じブリッジ グループ内のインターフェイス間のトラフィックをさらに詳細に制御できます。

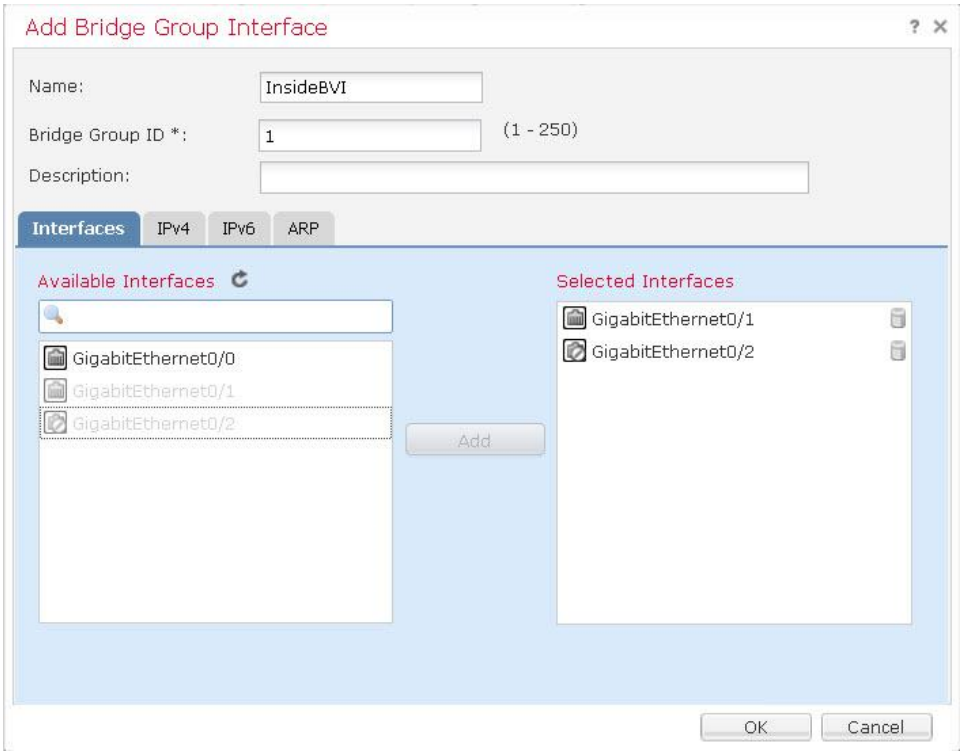
手順

このラボ演習に必要なオブジェクトを作成する

1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動します。左側のナビゲーション パネルで、[インターフェイス（Interface）] を選択します。
2. [追加（Add）] > [セキュリティ ゾーン（Security Zone）] の順にクリックします。
    a. [名前（Name）] に「**`BVIZone`**」と入力します。
    b. [インターフェイス タイプ（Interface Type）] ドロップダウン メニューから [スイッチド（Switched）] を選択します。
    c. [保存（Save）] をクリックします。

NGFW インターフェイス設定を変更する

1. [デバイス（Devices）] > [デバイス管理（Device Management）] に移動します。
2. 鉛筆アイコンをクリックして NGFW デバイス設定を編集し、[インターフェイス（Interfaces）] タブを選択します。
3. 鉛筆アイコンをクリックして、[GigabitEthernet0/1] インターフェイスを編集します。
4. **IPv4 アドレス**を削除し、[OK] をクリックします。この IP は、別のインターフェイスで使用できるように削除する必要があります。
5. [インターフェイスの追加（Add Interfaces）] をクリックし、[ブリッジ グループ インターフェイス（Bridge Group Interface）] を選択します。
    a. [名前（Name）] に「**`InsideBVI`**」と入力します。
    b. [ブリッジ グループ ID（Bridge Group ID）] に「**1**」と入力します。
    c. [GigabitEthernet0/1] と [GigabitEthernet0/2] を選択し、[追加（Add）] をクリックします。



d. [IPv4] タブを選択し、IP アドレス **198.19.10.1/24** を入力します。

e. [OK] をクリックします。確認を要求されたら、メッセージを読み、[はい（Yes）] をクリックします。

6. 鉛筆アイコンをクリックして、[GigabitEthernet0/1] インターフェイスを編集します。

a. [名前（Name）] に「**`inside1`**」と入力します。

b. [有効化（Enabled）] チェックボックスがオンになっていることを確認します。

c. [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから [BVIZone] を選択します。

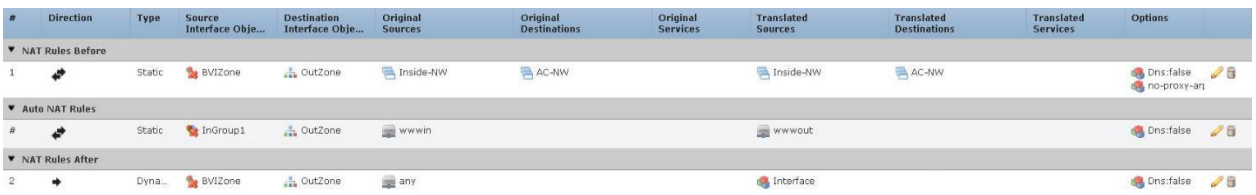
d. [OK] をクリックします。

7. **鉛筆アイコン**をクリックして、[GigabitEthernet0/2] インターフェイスを編集します。
    a. [名前（Name）] に「**inside2**」と入力します。
    b. [有効化（Enabled）] チェックボックスをオンにします。
    c. [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから [BVIZone] を選択します。
    d. [OK] をクリックします。
8. [保存（Save）] をクリックしてデバイス設定を保存します。

NAT ポリシーを変更する

1. シナリオ 10 を実行して、スタティック NAT ルールが BVI インターフェイスで機能するようにするには、この手順を実行する必要があります。これは、オブジェクト NAT では、複数のインターフェイスがあるインターフェイス オブジェクトが許可されていないためです。
    a. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動します。左側のナビゲーション パネルで、[インターフェイス（Interface）] を選択します。
    b. [追加（Add）] > [インターフェイス グループ（Interface Group）] の順にクリックします。
        i. [名前（NAME）] に「**InGroup1**」と入力します。
        ii. [インターフェイス タイプ（Interface Type）] で、[スイッチド（Switched）] を選択します。
        iii. インターフェイス **inside1** を選択し、[追加（Add）] をクリックします。
        iv. [保存（Save）] をクリックします。
2. [デバイス（Devices）] > [NAT] に移動します。
3. [デフォルト PAT（Default PAT）] ポリシーを編集します。右上の [保存（Save）] ボタンがグレー表示になっていることを確認します。グレー表示になっていない場合は、一度戻って再度編集します。

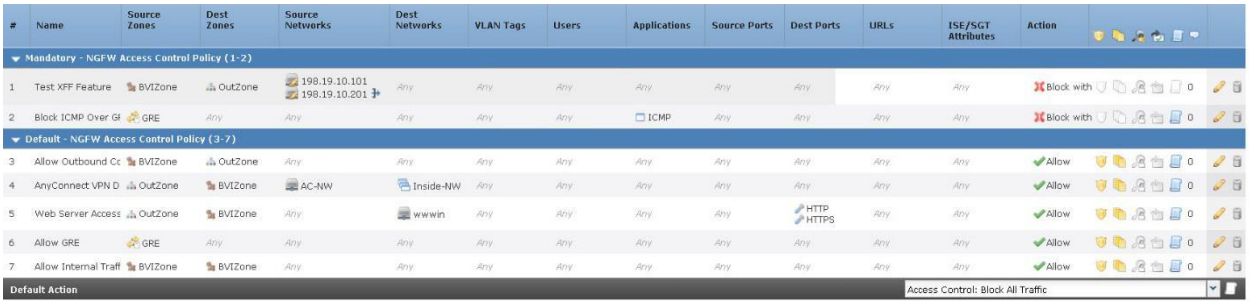
    a. シナリオ 10 でスタティック NAT 設定を行った場合は、自動 NAT ルールで **InZone** を **InGroup1** に置き換えます。自動 NAT では複数のインターフェイスがあるセキュリティ ゾーンは許可されていないため、**BVIZone** を使用することはできません。インターフェイス グループを作成することが回避策になります。
    b. 他のすべてのルールで、**InZone** を **BVIZone** に置き換えます。
    c. NAT ポリシーは次のようになります。ルールの数は実行したシナリオに応じて異なる場合があります。



    d. [保存（Save）] をクリックして NAT ポリシーを保存します。

アクセス コントロール ポリシーを変更する

1. [ポリシー(Policies)] > [アクセス制御(Access Control)] > [アクセス制御(Access Control)] に移動し、アクセス コントロール ポリシーを編集します。
2. **鉛筆アイコン**をクリックして NGFW デバイス設定を編集し、[インターフェイス(Interfaces)] タブを選択します。
    a. すべてのルールで **InZone** を **BVIZone** に置き換えます。
    b. **BVIZone** 内のインターフェイス間のトラフィックを許可する(検査は実行する)アクセス制御ルールを追加します。
        i. [名前(Name)] に「**`Allow Internal Traffic`**」と入力します。
        ii. [挿入(Insert)] ドロップダウン リストから、[デフォルトに挿入(into Default)] を選択します。
        iii. [ゾーン(Zones)] タブがすでに選択されているはずです。
        iv. [BVIZone] を選択し、[送信元に追加(Add to Source)] をクリックします。
        v. [BVIZone] を選択し、[宛先に追加(Add to Destination)] をクリックします。
        vi. [検査(Inspection)] タブを選択します。
        vii. [侵入ポリシー(Intrusion Policy)] ドロップダウン リストから [デモ侵入ポリシー(Demo Intrusion Policy)] を選択します。
        viii. [ファイル ポリシー(File Policy)] ドロップダウン リストから [デモ ファイル ポリシー(Demo File Policy)] を選択します。
        ix. [追加(Add)] をクリックしてルールを追加します。
    c. アクセス コントロール ポリシーは次のようになります。ルールの数は実行したシナリオに応じて異なる場合があります。



    d. [保存(Save)] をクリックして、アクセス コントロール ポリシーの変更を保存します。

設定を導入しテストする

1. 設定変更を導入し、導入が完了するまで待ちます。
2. 内部 Linux サーバの CLI で、「**`ping isolated`**」と入力して接続をテストします。これは成功するはずです。
3. 内部 Linux サーバの CLI から、IPS の機能をテストします。
    a. 内部 Linux サーバの CLI から、次のコマンドを実行します。
    `ftp isolated`
    b. **`guest`** として、パスワード **`C1sco12345`** でログインします。
    c. 「**`cd ~root`**」と入力します。次のメッセージが表示されます。
    `[421 サービスが使用できません。リモート サーバは接続を閉じています(421 Service not available, remote server has closed connection)]`

4. 内部 Linux サーバの CLI から、ファイル ブロックおよびマルウェア ブロックの機能をテストします。

   a. 制御テストとして、WGET を使用してブロックされていないファイルをダウンロードします。
   `wget -t 1 isolated/files/ProjectX.pdf`
   これは成功するはずです。

   b. 次に、タイプによってブロックされたファイルに対して WGET を使用してダウンロードを試みます。
   `wget -t 1 isolated/files/test3.avi`

   ファイルのごく一部しかダウンロードされないことに注意してください。これは、NGFW が、データの最初のブロックからファイル タイプを検出できるためです。*デモ ファイル ポリシー*は、AVI ファイルをブロックするように設定されています。

   c. 最後に、WGET を使用してマルウェアのダウンロードを試みます。
   `wget -t 1 isolated/files/Zombies.pdf`

注:ファイルの約 99 % がダウンロードされました。これは、NGFW が SHA の計算にファイル全体を必要とするためです。ハッシュが計算され、ルックアップされるまで、NGFW はデータの最後のブロックのダウンロードを保留します。*デモ ファイル ポリシー*は、PDF ファイルで検出されたマルウェアをブロックするように設定されています。

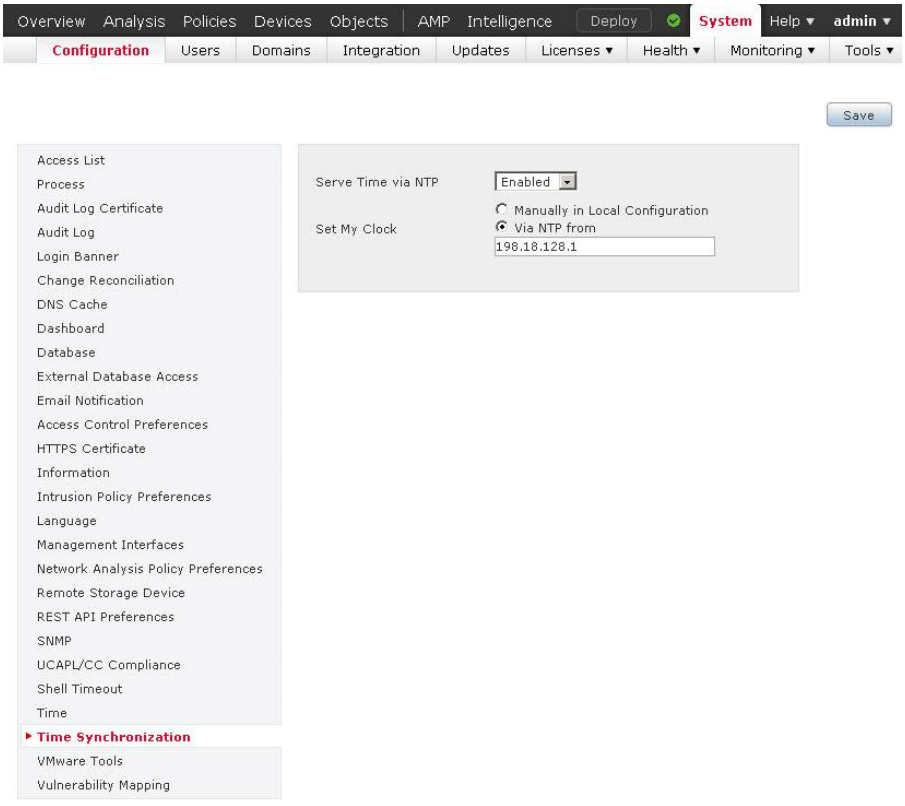
付録 A.　FMC の事前設定

ラボ演習を迅速化するため、初期インストール後に FMC でいくつかの設定手順が事前実行されています。この付録では、実行された設定手順について説明します。

- 設定 A1.1：NTP 設定
- 設定 A1.2：デモ ファイル ポリシー
- 設定 A1.3：デモ侵入ポリシー
- 設定 A1.4：デモ SSL ポリシー
- 設定 A1.5：カスタム検出リスト
- 設定 A1.6：restapiuser の追加
- 設定 A1.7：サーバ証明書のインストール

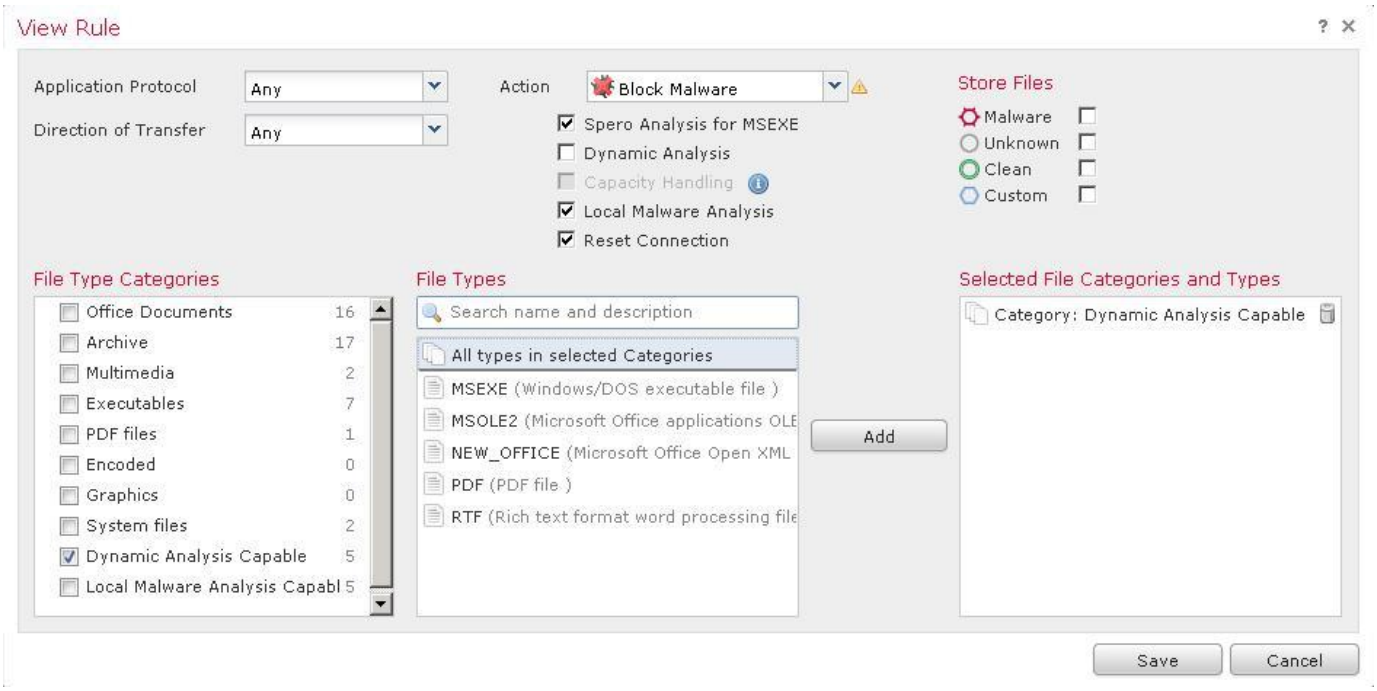
設定 A1.1：NTP 設定

1. FMC で NTP を設定します。
    a. FMC で、[システム（System）] > [設定（Configuration）] に移動します。
    b. 左側のナビゲーション ペインから [時間の同期（Time Synchronization）] を選択します。
    c. デフォルトの NTP サーバを **198.18.128.1** に置き換えます。
    d. [保存（Save）] をクリックします。

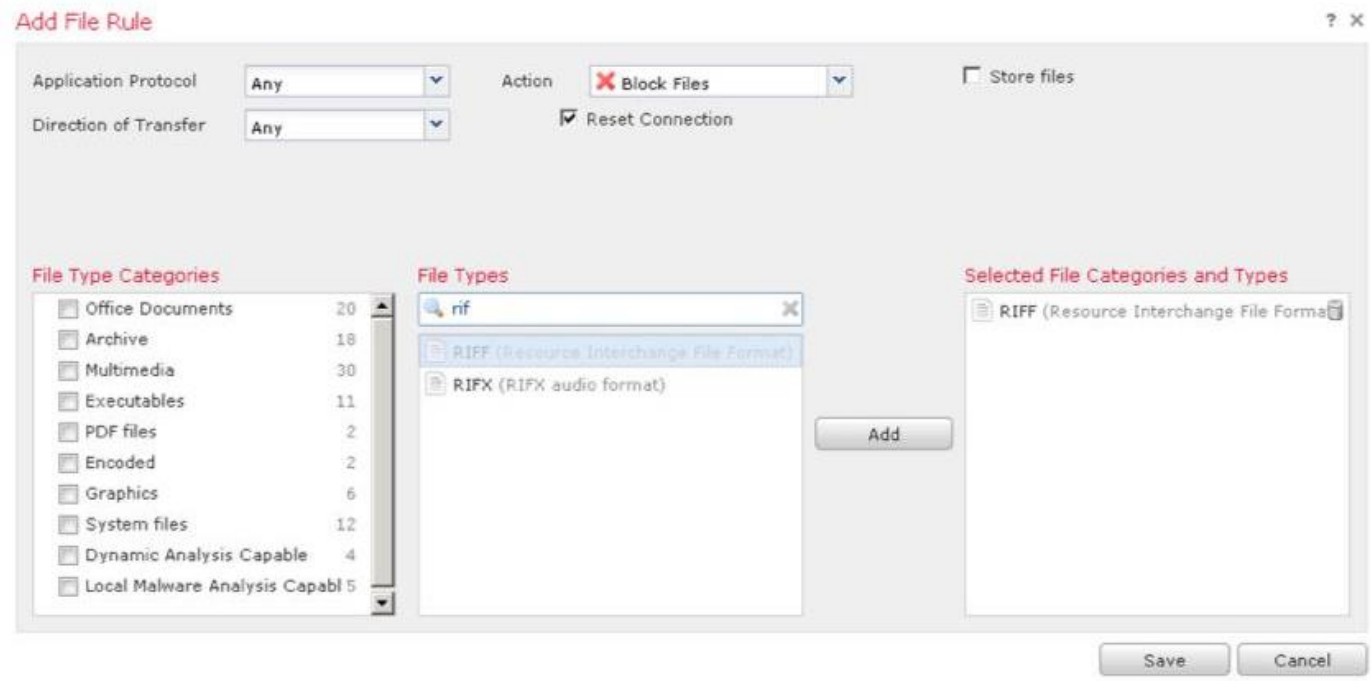


設定 A1.2：デモ ファイル ポリシー

1. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [マルウェア & ファイル（Malware & File）] に移動します。
2. [新しいファイル ポリシー（New File Policy）] をクリックします。「**Demo File Policy**」という名前を入力します。[保存（Save）] をクリックします。
3. [ファイル ルールを追加（Add File Rule）] をクリックします。このルールにより、MSEXE、MSOLE2、NEW_OFFICE、PDF の各ファイルで検出されたマルウェアがブロックされます。
    a. [アクション（Action）] で、[マルウェアをブロック（Block Malware）] を選択します。
    b. [Spero 分析（Spero Analysis）] および [ローカル マルウェア分析（Local Malware Analysis）] チェックボックスをオンにします。
    c. [ファイル タイプのカテゴリ（File Type Categories）] で、[動的分析の有効化（Dynamic Analysis Capable）] をオンにします。このカテゴリには、複数のファイル タイプが属しています。[追加（Add）] をクリックします。
    d. 画面は下の図のようになります。



    e. [保存（Save）] をクリックします。プロンプトが表示されたら、警告を無視して [OK] をクリックします。
4. [ファイル ルールを追加（Add File Rule）] をクリックします。このルールによって RIFF ファイルがブロックされます。AVI ファイルは RIFF ファイルの 1 つのタイプであるため、このルールのテストには AVI ファイルを使用します。ただし、AVI は別のファイル タイプとしてはリストされていません。
    a. [アクション（Action）] で [ファイルをブロック（Block Files）] を選択します。
    b. [ファイル タイプ（File Types）] で、検索ボックスに「**rif**」と入力します。リストから [RIFF] を選択します。[追加（Add）] をクリックします。
    c. その他の設定にはデフォルト値を使用します。画面は下の図のようになります。
    d. [保存（Save）] をクリックします。



注:作成したルールの順序は変更できません。ルールの順序は重要ではありません。ルールの優先度は、そのアクションによって決まります。アクションの優先度は次のとおりです。

1.ファイルのブロック

2 マルウェアのブロック

3. マルウェア クラウド ルックアップ

4. ファイルの検出

5. [詳細設定(Advanced)] タブを選択します。[カスタム検出リストを有効にする(Enable Custom Detection List)] が選択されていることを確認します。[アーカイブの検査(Inspect Archives)] チェックボックスをオンにします。

注:検査できないアーカイブは、壊れたアーカイブ、または深度が [アーカイブの最大深度(Max Archive Depth)] を超えているアーカイブです。

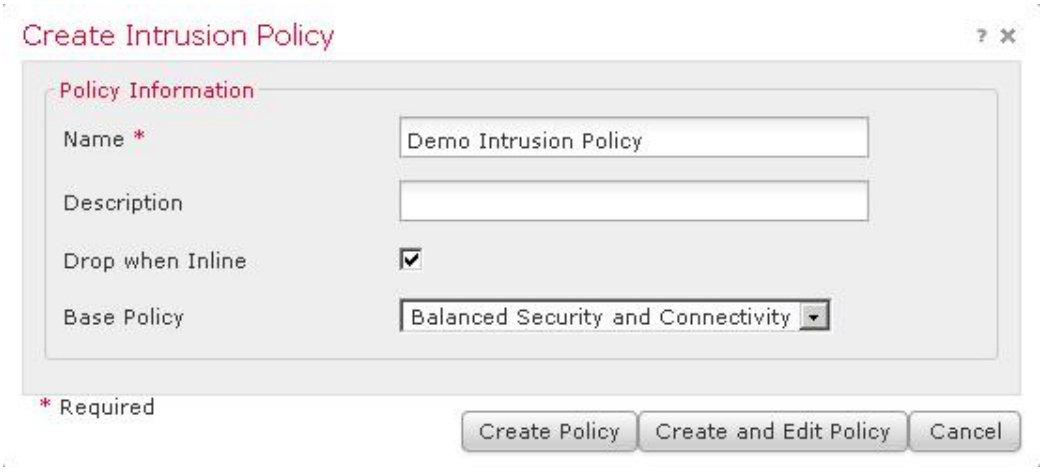
6. 右上の [保存(Save)] ボタンをクリックして、ファイル ポリシーを保存します。

設定 A1.3：デモ侵入ポリシー

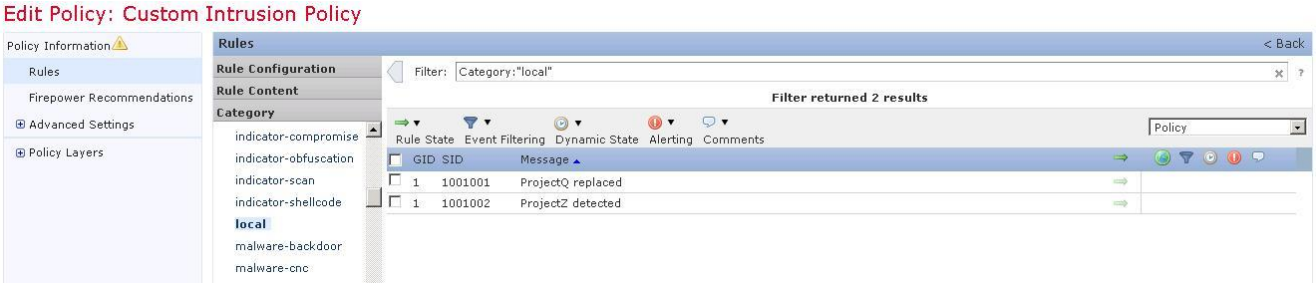
1. [オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）] に移動します。[ルールのインポート（Import Rules）] をクリックします。
    a. [アップロードおよびインストールするルール更新またはテキスト ルール ファイル（Rule update or text rule file to upload and install）] オプション ボタンを選択します。
    b. [参照（Browse）] をクリックして、Jump Desktop の **Files** フォルダで **Snort_Rules.txt** ファイルを開きます。

注：このファイルには、IPS のテストに役立つ 2 つの簡単な Snort ルールが含まれています。これらは公開 Snort ルールとは異なります。
alert tcp any any -> any any (msg:"ProjectQ replaced"; content:"ProjectQ"; replace:"ProjectR"; sid: 1001001; rev:1;)
alert tcp any any -> any any (msg:"ProjectZ detected"; content:"ProjectZ"; sid: 1001002; rev:1;)
最初のルールにより、文字列「ProjectQ」が「ProjectR」に置き換わります。2 番目のルールにより、文字列「ProjectZ」が検出されます。ルールは文字列がフローのどこに位置するかを指定しないため、実稼働環境で問題を引き起こす可能性があります。

    c. [インポート（Import）] をクリックします。インポート プロセスには 1 ～ 2 分かかります。完了すると、[ルール更新インポート ログ（Rule Update Import Log）] ページが表示されます。2 つのルールが正しくインポートされたことを確認します。
2. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [侵入（Intrusion）] に移動します。
3. [ポリシーの作成（Create Policy）] をクリックします。
    a. [名前（Name）] を「**Demo Intrusion Policy**」に設定します。
    b. [インラインの場合はドロップ（Drop when Inline）] がオンになっていることを確認します。
    c. [基本ポリシー（Base Policy）] として [バランスのとれたセキュリティと接続（Balanced Security and Connectivity）] を選択します。



    d. [ポリシーの作成および編集（Create and Edit Policy）] をクリックします。
4. 次に、この新しいポリシーのルール状態を変更します。
    a. [ポリシーの編集（Edit Policy）] ページ左側の [ポリシー情報（Policy Information）] メニューで、[ルール（Rules）] をクリックします。
    b. ルールの [カテゴリ（Category）] セクションで、[ローカル（local）] を選択します。アップロードされた 2 つのルールが表示されます。各ルールの右にある薄緑色の矢印は、このポリシーについてそのルールが無効になっていることを示します。



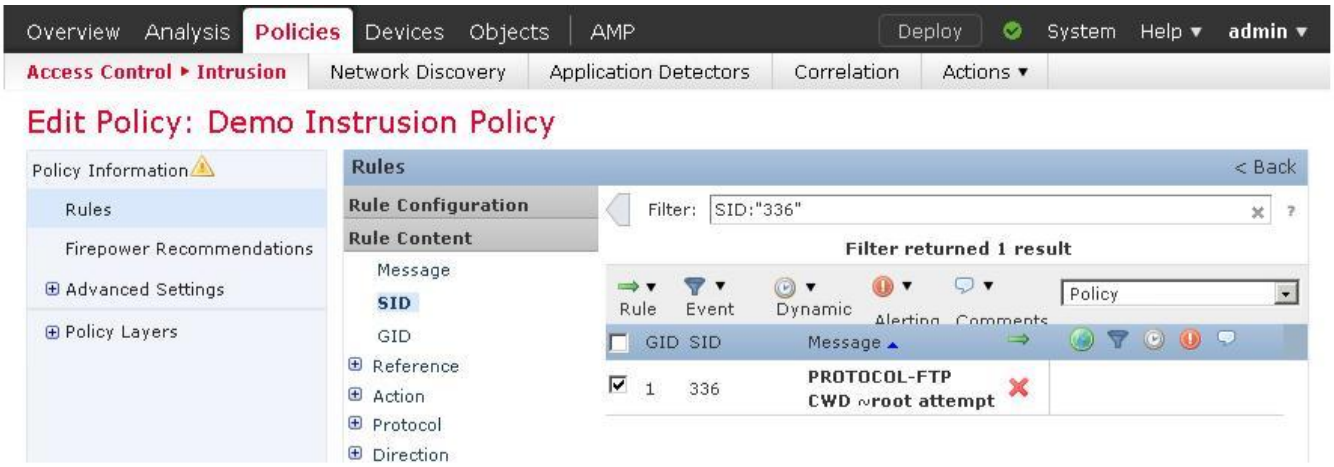
c. 最初のルールの横にあるチェックボックスをオンにします。[ルールの状態(Rule State)] ドロップダウン メニューから [イベントを生成(Generate Events)] を選択します。[OK] をクリックします。最初のルールの横にあるチェックボックスをオフにします。

d. 2 番目のルールの横にあるチェックボックスをオンにします。[ルールの状態(Rule State)] ドロップダウン メニューから [イベントをドロップして生成(Drop and Generate Events)] を選択します。[OK] をクリックします。

e. [フィルタ(Filter)] テキスト フィールドの右側にある X をクリックしてフィルタをクリアします。

f. ルールの [ルール コンテンツ(Rule Content)] セクションで、[SID] を選択します。[SID フィルタの入力(Enter the SID filter)] ポップアップに「336」と入力します。[OK] をクリックします。

g. ルールの横にあるチェックボックスをオンにします。[ルールの状態(Rule State)] ドロップダウン メニューから [イベントをドロップして生成(Drop and Generate Events)] を選択します。[OK] をクリックします。



注:このルールは、ポート 21 で確立された FTP トラフィックのルート ホーム ディレクトリに対する変更を検索します。外部ネットワークからのトラフィックのみを検索しますが、このラボでは $EXTERNAL_NET のデフォルト値 any を使用するため、ルールが両方向でトリガーされる可能性があります。

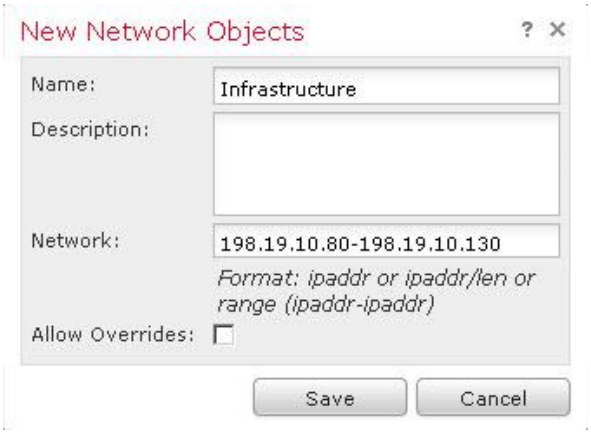
このルールを変更して、あらゆる方向の FTP トラフィックを検索し、appid 属性を使用してすべてのポートの FTP トラフィックを検出することは、興味深い演習になります。

5. 左上のメニューで [ポリシー情報(Policy Information)] をクリックします。

6. [変更内容を確定(Commit Changes)] をクリックします。[OK] をクリックします。

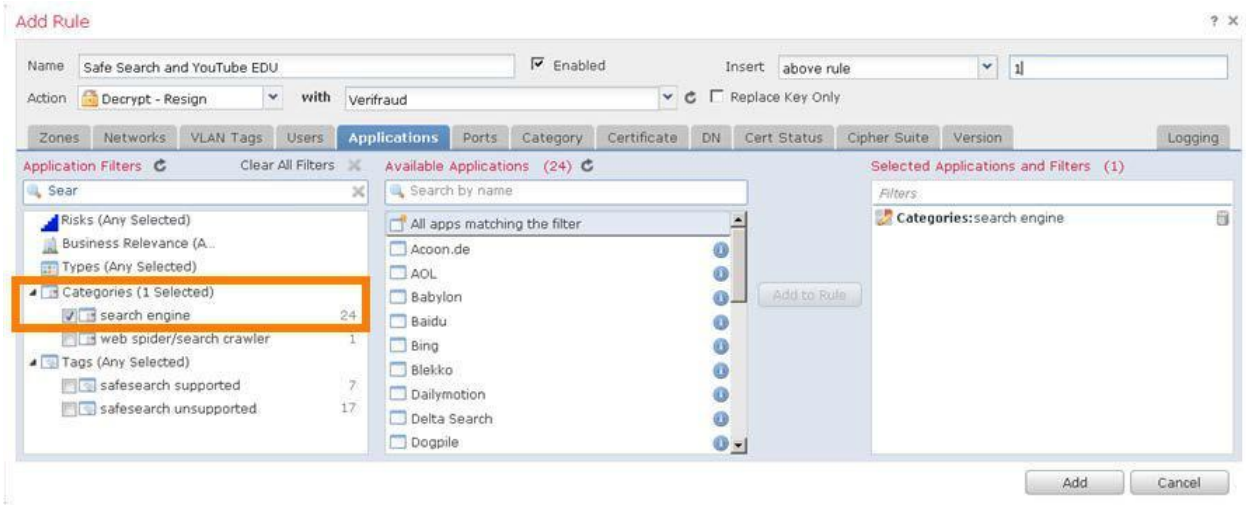
設定 A1.4：デモ SSL ポリシー

1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [PKI] > [内部 CA（Internal CAs）] に移動します。
    a. [CA のインポート（Import CA）] をクリックします。
    b. [名前（Name）] に「**Verifraud**」と入力します。
    c. [証明書データ、またはファイルを選択（Certificate Data or, choose a file）] の右にある [参照（Browse）] ボタンをクリックします。
    d. Jump Desktop の [証明書（Certificates）] フォルダに移動します。
    e. [Verifraud_CA.cer] をアップロードします。
    f. [キー、またはファイルを選択（Key or, choose a file）] の右にある [参照（Browse）] ボタンをクリックします。
    g. [Verifraud_CA.key] をアップロードします。
    h. [保存（Save）] をクリックします。
2. FMC や AMP プライベート クラウドなどの復号化インフラストラクチャ デバイスから除外します。除外するには、これらのデバイスを含むネットワーク オブジェクトを作成します。
    a. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ネットワーク（Network）] に移動します。
    b. [ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）] の順にクリックします。
    c. [名前（Name）] に「**Infrastructure**」と入力します。
    d. [ネットワーク（Network）] に「**198.19.10.80-198.19.10.130**」と入力します。



    e. [保存（Save）] をクリックして、ネットワーク オブジェクトを保存します。
3. [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [SSL] の順に選択します。
4. [新しいポリシーを追加（Add a new policy）] をクリックするか、[新しいポリシー（New Policy）] ボタンをクリックします。
    a. [名前（Name）] に「**Demo SSL Policy**」と入力します。
    b. デフォルトのアクションは [復号しない（Do not decrypt）] のままにします。
    c. [保存（Save）] をクリックします。数秒後にポリシーが開き、編集可能になります。

5. [ルールの追加(Add Rule)] をクリックします。
    a. [名前(Name)] に「**Exempt Infrastructure**」と入力します。
    b. [アクション(Action)] は [復号しない(Do Not decrypt)] に設定したままにします。
    c. [ネットワーク(Networks)] タブの [ネットワーク(Networks)] で [インフラストラクチャ(Infrastructure)] を選択して、[ソースに追加(Add to Source)] をクリックします。
    d. [追加(Add)] をクリックして、このルールを SSL ポリシーに追加します。
6. [ルールの追加(Add Rule)] をクリックします。
    a. [名前(Name)] に「**Decrypt Search Engines**」と入力します。
    b. [アクション(Action)] を [復号 - 再署名(Decrypt – Resign)] に設定します。
    c. [対象(with)] の右にあるドロップダウン リストから [Verifraud] を選択します。
    d. [アプリケーション(Applications)] タブの [アプリケーション フィルタ(Application Filters)] で、**Sear** を検索します。[カテゴリ(Categories)] に [検索エンジン(Search Engine)] が表示されます。このチェックボックスをオンにし、[ルールに追加(Add to Rule)] をクリックします。



    e. [ロギング(Logging)] タブを選択し、[接続終了時にロギング(Log at End of Connection)] チェックボックスをオンにします。
    f. [追加(Add)] をクリックして、このルールを SSL ポリシーに追加します。
7. [ルールの追加(Add Rule)] をクリックします。
    a. [名前(Name)] に「**Decrypt Other**」と入力します。
    b. [アクション(Action)] を [復号 - 再署名(Decrypt – Resign)] に設定します。
    c. [対象(with)] の右にあるドロップダウン リストから [Verifraud] を選択します。
    d. [ロギング(Logging)] タブを選択し、[接続終了時にロギング(Log at End of Connection)] チェックボックスをオンにします。
    e. [追加(Add)] をクリックして、このルールを SSL ポリシーに追加します。

8. [保存(Save)] をクリックして SSL ポリシーを保存します。

注:[キーを置換(Replace Key)] チェックボックスについて説明します。アクションを [復号 - 再署名(Decrypt – Resign)] に設定すると、Firepower では公開鍵が置換されます。[キーを置換(Replace Key)] チェックボックスにより、復号アクションが自己署名サーバ証明書にどのように適用されるかが決定されます。

• [キーを置換(Replace Key)] の選択を解除すると、自己署名証明書はその他のサーバ証明書と同様に処理されます。Firepower はキーを置換し、証明書を再署名します。通常、エンドポイントは Firepower を信頼するように設定されるため、再署名されたこの証明書を信頼します。

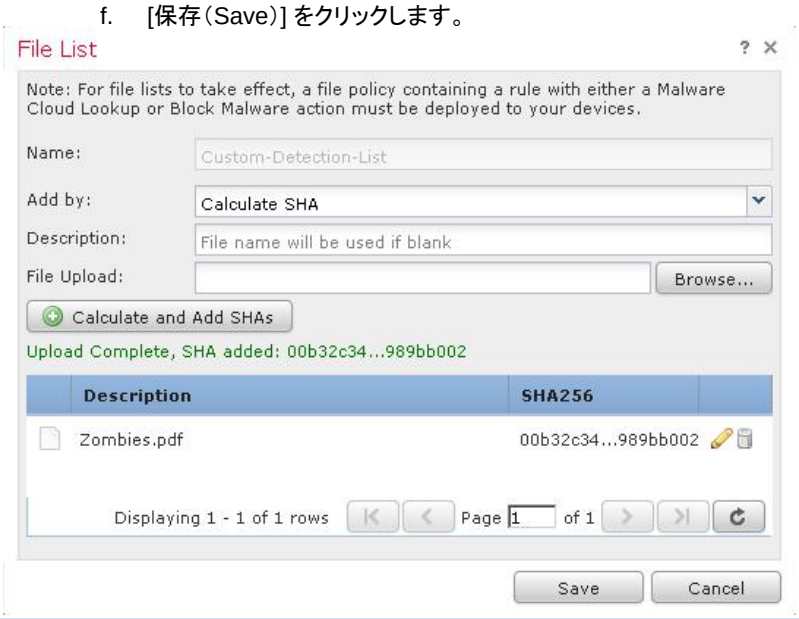
• [キーを置換(Replace Key)] を選択すると、自己署名された証明書の処理が変わります。Firepower はキーを置換し、新しい自己署名証明書を生成します。エンドポイントのブラウザは証明書警告を生成します。

言い換えれば、[キーを置換(Replace Key)] チェックボックスをオンにすると、再署名アクションで lack-of-trust が自己署名証明書用に保持されます。

設定 A1.5:カスタム検出リスト

クラウド ルックアップが成功することを前提として、マルウェア イベントをトリガーする Zombies.pdf という安全性に問題のないファイルがあります。ラボにクラウドの接続性の問題が発生する場合もあります。そのため、このファイルをカスタム検出リストに追加して、マルウェア イベントをトリガーすることを確認します。

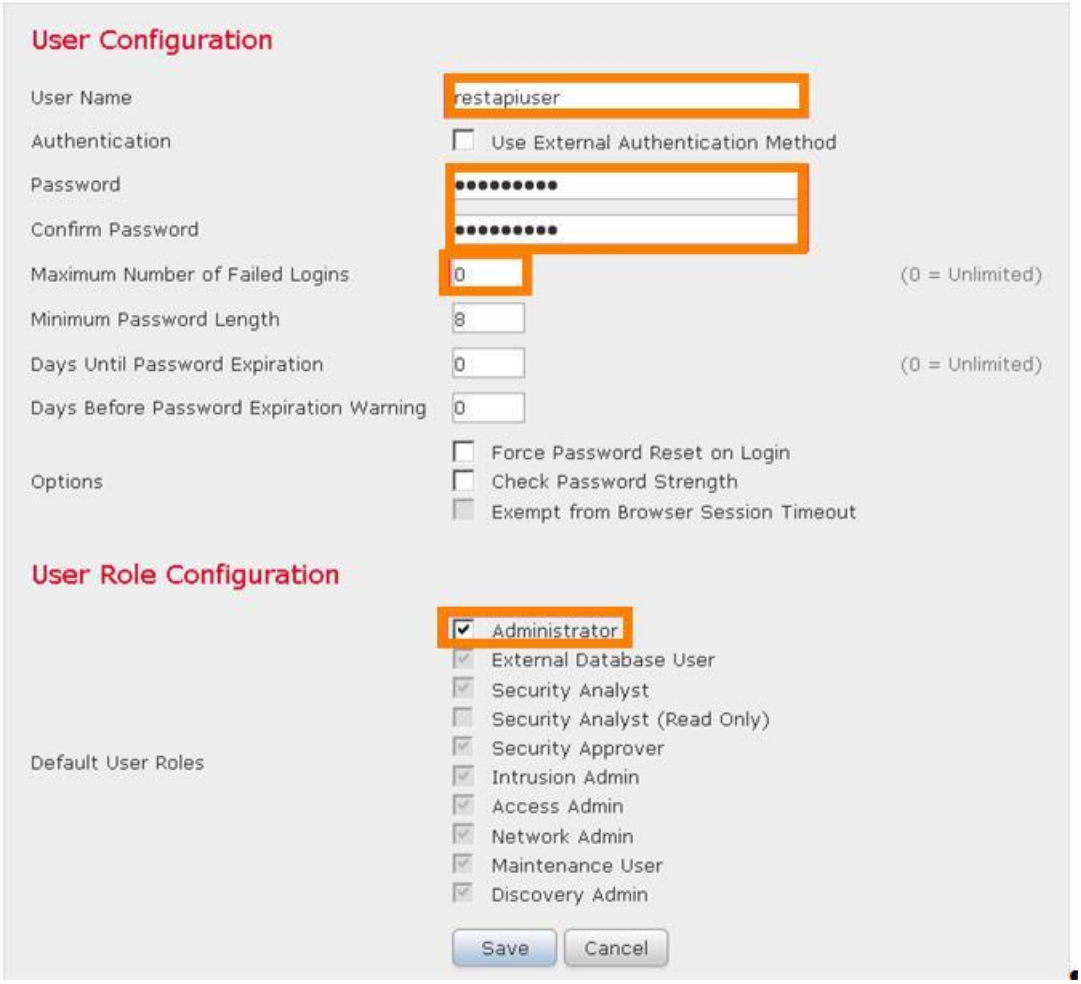
1. [オブジェクト(Objects)] > [オブジェクト管理(Object Management)] > [ファイル リスト(File List)] に移動します。
2. 鉛筆アイコンをクリックして、**カスタム検出リスト**を編集します。
    a. [追加方法(Add by)] ドロップダウン リストから [SHA の計算(Calculate SHA)] を選択します。
    b. [参照(Browse)] をクリックします。
    c. Jump Desktop の [ファイル(Files)] フォルダに移動します。
    d. [Zombies.pdf] を選択して [OK] をクリックします。
    e. [SHA を計算して追加(Calculate and Add SHAs)] をクリックします。
    f. [保存(Save)] をクリックします。



設定 A1.6：restapiuser の追加

API Explorer を使用する際、別個のユーザを使用すると便利です。これにより、FMC と API Explorer の両方を同時に使用できます。

1. [システム（System）] > [ユーザ（Users）] に移動します。[ユーザの作成（Create User）] をクリックします。
    a. [ユーザ名（User Name）] に「**restapiuser**」と入力します。
    b. [パスワード（Password）] に「**C1sco12345**」と入力します。パスワードを確認します。
    c. [失敗したログインの最大数（Maximum Number of Failed Logins）] を 0 に設定します。
    d. [管理者（Administrator）] チェックボックスをオンにします。



設定 A1.7：サーバ証明書のインストール

FMC UI では、デフォルトで自己署名証明書が使用されます。これは、Jump ブラウザが信頼する、ポッド AD サーバによって署名された証明書によって置き換えられます。

1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [PKI] > [信頼できる CA（Trusted CAs）] に移動します。
    a. 信頼できる CA の追加（Add Trusted CA）] をクリックします。
    b. [名前（Name）] に「**dCloud**」と入力します。
    c. [証明書データ、またはファイルを選択（Certificate Data or, choose a file）] の右にある [参照（Browse）] ボタンをクリックします。
    d. Jump Desktop の [証明書（Certificates）] フォルダに移動します。
    e. **AD-ROOT-CA-CERT.cer** をアップロードします。
    f. [保存（Save）] をクリックします。
2. FMC CLI に SSH で接続します。「**sudo -i**」と入力して root になります。Sudo のパスワードは **C1sco12345** です。
    a. 「**cd /etc/ssl**」入力し、「**cp server* /root**」と入力します。
    b. 「**cat > /etc/ssl/server.crt**」と入力します。
    c. Jump Desktop の [証明書（Certificates）] フォルダで、Notepad++ を使用して **fmc.cer** ファイルを編集します。
    d. すべてを選択し、コピーして FMC CLI に貼り付けます。
    e. Ctrl+D を押します。
    f. 「**cat > /etc/ssl/server.key**」と入力します。
    g. Jump Desktop の [証明書（Certificates）] フォルダで、Notepad++ を使用して **fmc.key** ファイルを編集します。
    h. すべてを選択し、コピーして FMC CLI に貼り付けます。
    i. Ctrl+D を押します。
    j. 「**pmtool restartbyid httpsd**」と入力します。

付録 B.　REST API スクリプト

ここでは、最初のラボ演習で使用した 2 つの Python スクリプトを示します。最初のスクリプト **register_config.py** だけを実行してください。**register_config.py** から 2 番目のスクリプト **connect.py** が呼び出され、コンパイルされたファイル **connect.pyc** が作成されます。

Python スクリプト register_config.py

```
#!/usr/bin/python
import json
import connect
import sys

host = "fmc.example.com"
username = "restapiuser"
password = "C1sco12345"
name="NGFW"

#connect to the FMC API
headers,uuid,server = connect.connect (host, username, password)

user_input = str(raw_input("Would you like to register the managed device? [y/n]"))
if user_input == "y":
 policy_name = str(raw_input("Enter name of new Access Control Policy to be create:"))
 access_policy = {
 "type": "AccessPolicy",
 "name": policy_name,
 "defaultAction": { "action": "BLOCK" }
 }
 post_response = connect.accesspolicyPOST(headers,uuid,server,access_policy)
 policy_id = post_response["id"]
 print "\n\nAccess Control Policy\n" + policy_name + "\ncreated\n\n"
 device_post = {
 "name": name,
 "hostName": "ngfw.example.com",
 "regKey": "C1sco12345",
 "type": "Device",
 "license_caps": [
 "BASE",
 "MALWARE",
 "URLFilter",
 "THREAT"
 ],
 "accessPolicy": {
 "id": policy_id,
 "type": "AccessPolicy"
 }
 }
 post_data = json.dumps(device_post)

 output = connect.devicePOST (headers, uuid, server, post_data)
# print "\n\nPost request is: \n" + json.dumps(output,indent=4) + "\n\n"

# GET ALL THE DEVICES AND THEIR corresponding interfaces

user_input = str(raw_input("In the FMC UI, confirm that the device discovery has completed and then
press 'y' to continue or 'n' to exit.[y/n]"))
headers,uuid,server = connect.connect (host, username, password)
```

```
if user_input == "n":
 quit()

devices = connect.deviceGET(headers,uuid,server)
for device in devices["items"]:
 if device["name"] == name:
 print "DEVICE FOUND, setting ID"
 device_id = device["id"]

# NOW THAT WE HAVE THE DEVICE ID WE NEED TO GET ALL THE INTERFACES

interfaces = connect.interfaceGET(headers,uuid,server,device_id)
# Interfaces i want to change
interface_1 = "GigabitEthernet0/0"
interface_2 = "GigabitEthernet0/1"

for interface in interfaces["items"]:
 if interface["name"] == interface_1:
 interface_1_id = interface["id"]
 print "interface 1 found"
 if interface["name"] == interface_2:
 interface_2_id = interface["id"]
 print "interface 2 found"

user_input = str(raw_input("Would you like to configure device interfaces? [y/n]"))

if user_input == "y":
 interface_put = {
 "type": "PhysicalInterface",
 "hardware": {
 "duplex": "AUTO",
 "speed": "AUTO"
 },
 "enabled": True,
 "MTU": 1500,
 "managementOnly": False,
 "ifname": "outside",
 "enableAntiSpoofing": False,
 "name": "GigabitEthernet0/0",
 "id": interface_1_id,
 "ipv4" : {
 "static": {
 "address":"198.18.133.2",
 "netmask":"18"
 }
 }
 }
 put_data = json.dumps(interface_put)
 connect.interfacePUT (headers, uuid, server, put_data,device_id,interface_1_id)
 interface_put = {
 "type": "PhysicalInterface",
 "hardware": {
 "duplex": "AUTO",
 "speed": "AUTO"
 },
 "enabled": True,
 "MTU": 1500,
 "managementOnly": False,
 "ifname": "inside",
```

```
 "enableAntiSpoofing": False,
 "name": "GigabitEthernet0/1",
 "id": interface_2_id,
 "ipv4" : {
 "static": {
 "address":"198.19.10.1",
 "netmask":"24"
 }
 }
 }
 put_data = json.dumps(interface_put)
 connect.interfacePUT (headers, uuid, server, put_data,device_id,interface_2_id)
```

Python スクリプト connect.py

```
#!/usr/bin/python
import json
import sys
import requests
#Surpress HTTPS insecure errors for cleaner output
from requests.packages.urllib3.exceptions import InsecureRequestWarning

requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

#define fuction to connect to the FMC API and generate authentication
token def connect (host, username, password):
 headers = {'Content-Type': 'application/json'}
 path = "/api/fmc_platform/v1/auth/generatetoken"
 server = "https://"+host
 url = server + path
 try:
 r = requests.post(url, headers=headers, auth=requests.auth.HTTPBasicAuth(username,password),
verify=False)
 auth_headers = r.headers
 token = auth_headers.get('X-auth-access-token', default=None)
 uuid = auth_headers.get('DOMAIN_UUID', default=None)
 if token == None:
 print("No Token found, I'll be back terminating....")
 sys.exit()
 except Exception as err:
 print ("Error in generating token --> "+ str(err))
 sys.exit()
 headers['X-auth-access-token'] = token

 return headers,uuid,server


def devicePOST (headers, uuid, server, post_data):
 api_path= "/api/fmc_config/v1/domain/" + uuid + "/devices/devicerecords"
 url = server+api_path
 try:
 r = requests.post(url, data=post_data, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
```

```
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 201 or status_code == 202:
 print("Post was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response



def deviceGET (headers, uuid, server):
 api_path= "/api/fmc_config/v1/domain/" + uuid + "/devices/devicerecords"
 url = server+api_path
 try:
 r = requests.get(url, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 200:
 print("GET was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response

def interfaceGET (headers, uuid, server, device_id):
 api_path= "/api/fmc_config/v1/domain/" + uuid +
"/devices/devicerecords/"+device_id+"/physicalinterfaces"
 url = server+api_path
 try:
 r = requests.get(url, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 200:
 print("GET was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response

def interfacePUT (headers, uuid, server, put_data,device_id, interface_id):
 api_path= "/api/fmc_config/v1/domain/" + uuid +
"/devices/devicerecords/"+device_id+"/physicalinterfaces/"+interface_id
```

```
 url = server+api_path
 try:
 r = requests.put(url, data=put_data, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 200 :
 print("Put was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response

def accesspolicyPOST (headers, uuid, server, post_data):
    api_path= "/api/fmc_config/v1/domain/" + uuid + "/policy/accesspolicies"
    url = server+api_path
    try:
            r = requests.post(url, data=json.dumps(post_data), headers=headers, verify=False)
            status_code = r.status_code
            resp = r.text
            json_response = json.loads(resp)
            print("status code is: "+ str(status_code))
            if status_code == 201 or status_code == 202:
                    print("Post was sucessfull...")
            else:
                    r.raise_for_status()
                    print("error occured in POST -->"+resp)
    except requests.exceptions.HTTPError as err:
            print ("Error in connection --> "+str(err))
    finally:
            if r: r.close()
    return json_response
```

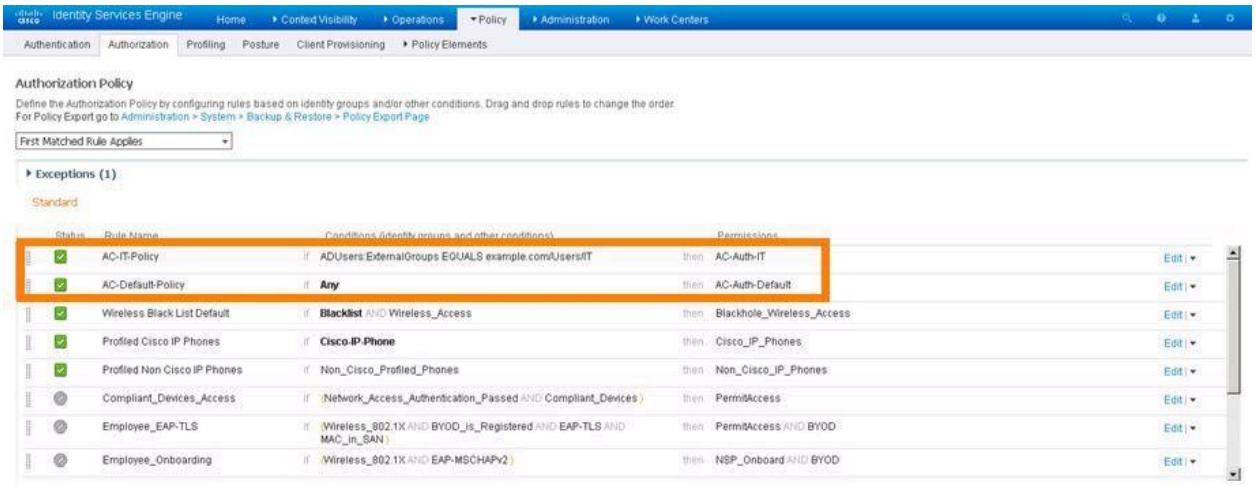
付録 C.　ISE RA VPN 設定

ISE はすべてのラボ演習をサポートするように設定されています。この付録では、その設定の概要を示します。Firefox ブックマーク ツールバーには ISE リンクがあります。クレデンシャルは事前に入力されています。ユーザ名 **admin**、パスワード **C1sco12345** です。

注:この付録は ISE に関するチュートリアルではありません。ISE の設定方法の詳細については説明していません。このガイドのラボ演習での RA VPN コンポーネントの設定に必要な詳細だけを示しています。設定はトップダウン方式で説明しています。この設定を作成するには、これらのオブジェクトをボトムアップで構築することもできます。

認可ポリシー

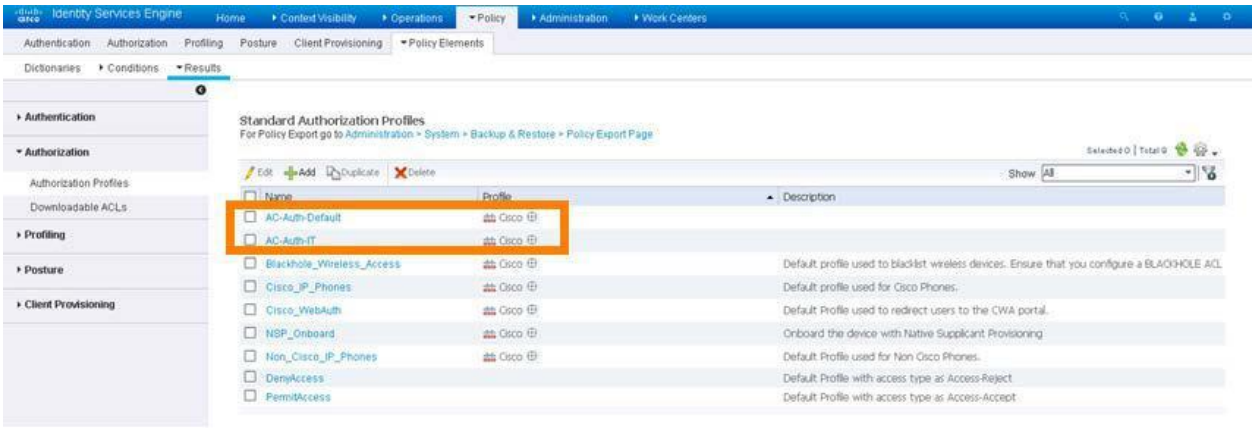
1. [ポリシー(Policy)] > [認可(Authorization)] に移動します。最初の 2 つのポリシー、**AC-IT-Policy** と **AC-Default-Policy** は、このラボ用に作成されたものです。これらは、以下に説明する 2 つの認可プロファイル、**AC-Auth-IT** と **AC-Auth-Default** を参照しています。



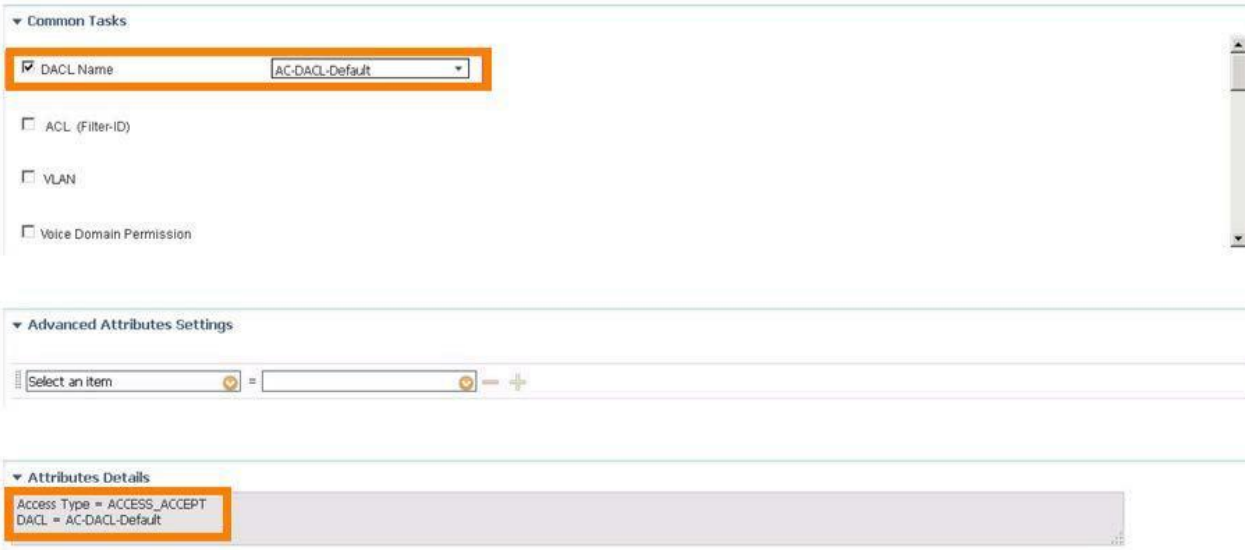
これらのポリシーは、2 つの認可プロファイル、AC-Auth-IT と AC-Auth-Default を参照しています。

認可プロファイル

1. [ポリシー(Policy)] > [ポリシー要素(Policy Elements)] > [結果(Results)] > [認可(Authorization)] > [認可プロファイル(Authorization Profiles)] に移動します。最初の 2 つのプロファイル、**AC-Auth-Default** と **AC-Auth-IT** は、このラボ用に作成されたものです。



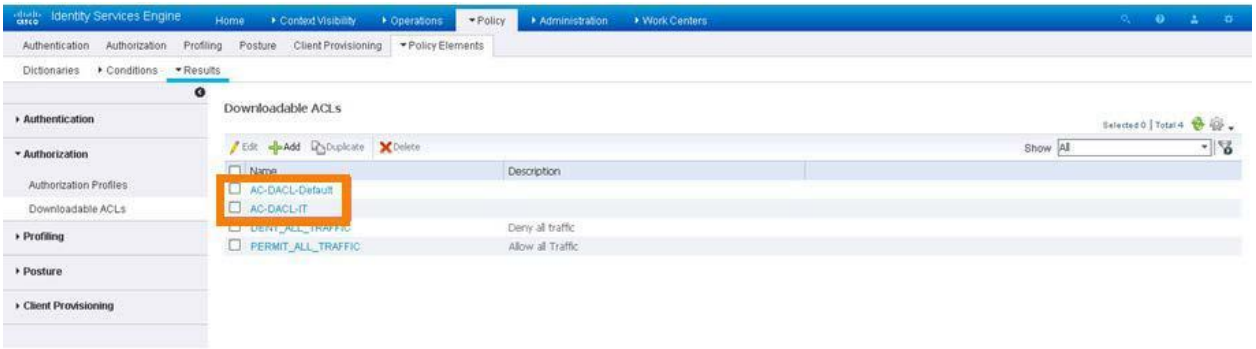
2. **AC-Auth-Default** をドリルダウンすると、以下に説明する **DACL AC-DACL-Default** を参照していることがわかります。



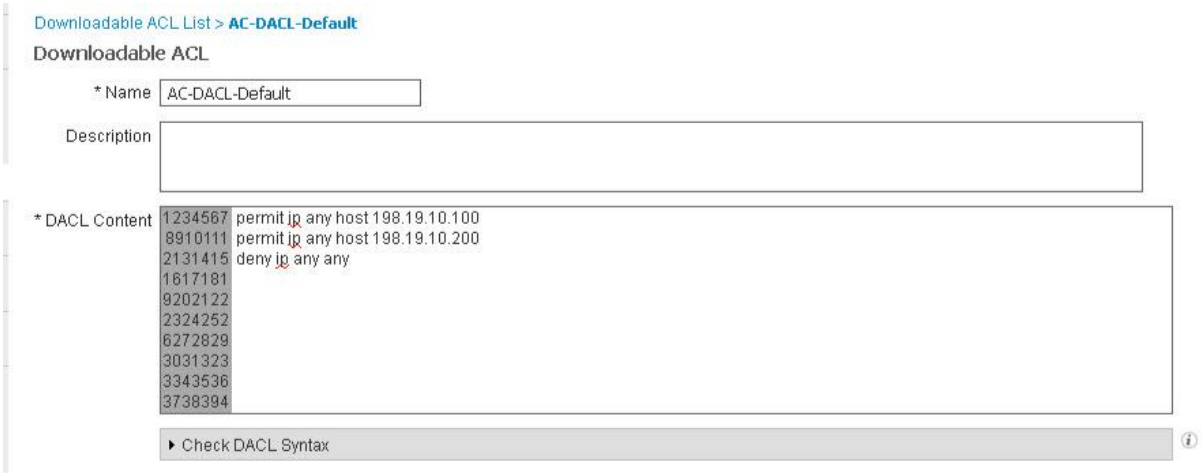
3. **AC-Auth-IT** をドリルダウンすると、以下に説明する **DACL AC-DACL-IT** を参照していることがわかります。また、2 つの高度な属性があります。1 つはアドレス プール用で、もう 1 つはグループ ポリシー用です。

ダウンロード可能 ACL

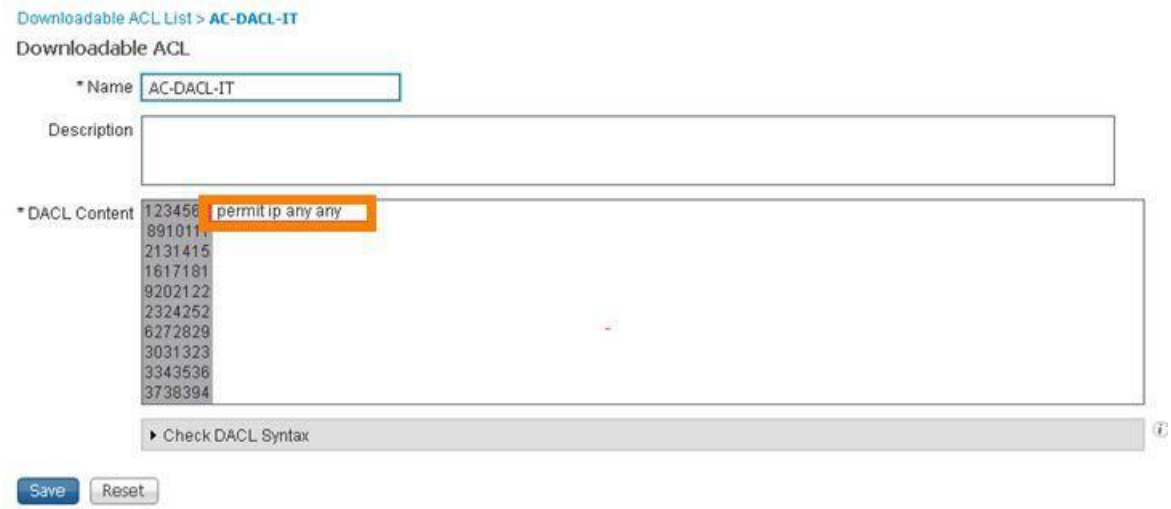
1. [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [認可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] に移動します。最初の 2 つの DACL、**AC-DACL-Default** と AC-DACL-IT は、このラボ用に作成されたものです。



2. **AC-DACL-Default** をドリルダウンすると、198.19.10.100 と 198.19.10.200 へのアクセスを制限していることがわかります。



3. **AC-DACL-IT** をドリルダウンすると、制限がないことがわかります。



付録 D.　Alien Vault を TAXII フィードとして使用

この付録では、Hail a TAXII の代わりに、無料の TAXII フィードをソースとして使用する方法を示します。これは次のタスクで構成されています。

- Alien Vault でアカウントを作成する
- API トークンを取得する
- Alien Vault TAXII フィードに CTID を登録する

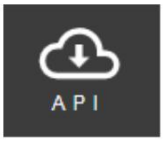
手順

Alien Vault でアカウントを作成する

1. https://otx.alienvault.com に移動します。
    a. ユーザ名、有効な電子メール アドレス、パスワードを入力します。
    b. [サインアップ（SIGN UP）] をクリックします。
2. 手順 1a で使用した電子メール アカウントにログインし、確認リンクをクリックします。
    a. 確認リンクをクリックします。
    不明なアカウントからの電子メールのリンクをクリックするのでしょうか。そうです。
    b. [確認（Confirm）] ボタンが表示されたらクリックします。
    c. [ログイン（LOGIN）] をクリックして、Alien Vault アカウントにログインします。

API トークンを取得する

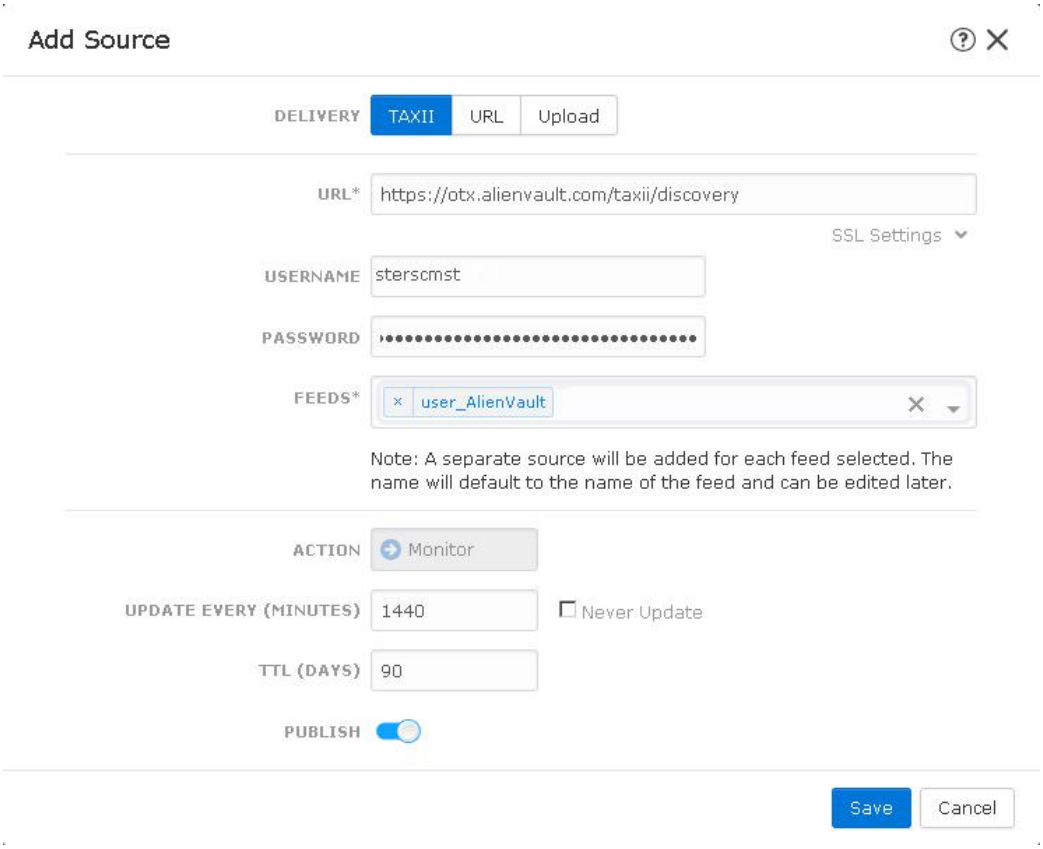
1. Alien Vault アカウントで、ページ中央上部にある API リンクをクリックします。



2. ページの右側で、API トークンの右にあるコピー ボタンをクリックします。ファイルに保存することができます。

Alien Vault TAXII フィードに CTID を登録する

1. [インテリジェンス（Intelligence）] > [ソース（Sources）] > [ソース（Sources）] に移動します。右側のプラス記号をクリックして、インテリジェンスのソースを追加します。
    a. [配信（DELIVERY）] で [TAXII] を選択します。
    b. [URL] に「**https://otx.alienvault.com/taxii/discovery**」と入力します。
    c. [ユーザ名（USERNAME）] に、Alien Vault のログイン名を入力します。
    d. [パスワード（PASSWORD）] には、Alien Vault アカウントからコピーした API トークンを貼り付けます。
    e. [フィード（FEEDS）] で、[user_AlienVault] を選択します。[フィード（FEEDS）] ドロップダウン リストに入力されるまで数秒かかる場合があります。
    f. 次のような画面が表示されることを確認します。



    g. [保存（Save）] をクリックします。

2. このソースの [ステータス（Status）] 列が [ダウンロード中（Downloading）] から [解析中（Parsing）] に変わるまで待ちます。解析には非常に時間がかかるため、完了するまでは待ちません。
3. [インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ（Indicators）] に移動します。複数の URL インジケータが追加されたことを確認します。
4. [インテリジェンス（Intelligence）] > [ソース（Sources）] > [監視対象（Observables）] に移動します。複数の URL 監視対象が追加されたことを確認します。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp