Cisco Firepower 次世代ファイアウォール 6.3 アドバンスド ラボ v2.4.1

最終更新日: 2019 年 3 月 18 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。

要件

次の表に、このデモンストレーションの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

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、そのようなレガシー NGFW では、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、および優先順位付けを企業に提供できません。

Cisco FirePOWER は、専用プラットフォームで展開されるか、ソフトウェ アソリューションとして展開されるネットワーク セキュリティおよびトラフィック管理製品の統合スイートです。このシステムは、組織のセキュリティ ポリシー（ネットワークを保護するためのガイドライン）に準拠する方法でネットワーク トラフィックを処理できるように設計されています。

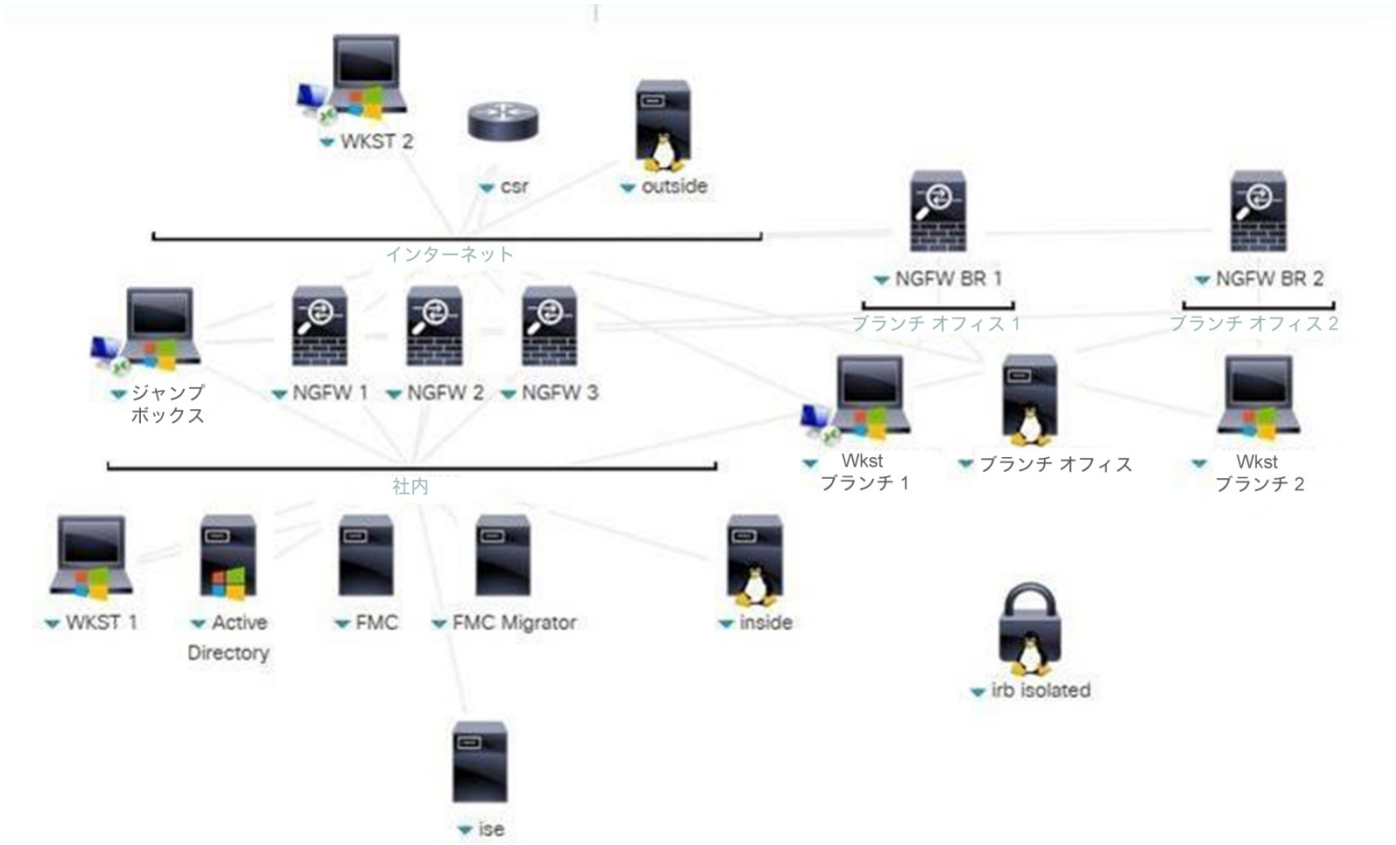
Cisco Firepower NGFW は、企業が最新の脅威に対するリアルタイムの阻止、優先順位付け、把握、対応自動化を図ることを焦点に進化することが可能です。Firepower NGFW は、包括的なネットワーク可視性、最善の脅威インテリジェンス、有効性の高い脅威防御を基盤にした脅威中心型を特徴とし、既知および未知の両方の脅威に対応します。また、Advanced Malware Protection によって、レトロスペクティブ セキュリティも可能にします。これは、防御を回避した巧妙な攻撃を「時間を遡って」迅速に特定し、修復するものです。それにより、業界の平均値に比べて検出時間（TTD）が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

このラボでは、企業と 2 つのブランチ サイト間で、マルチサイト ネットワークの次世代ファイアウォール（NGFW）ソリューションを構築します。Firepower Management Console（FMC）を使用して、企業サイトでハイアベイラビリティ NGFW を構築し、ブランチを管理します。また、FDM（Firepower Device Manager）を使用して NGFW の設定も実施します。リモート アクセスおよびサイト間 VPN も設定します。さらに、サードパーティ製のアップデートを承認して NGFW デバイスに導入するように、Cisco Threat Intelligence Director を設定します。

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管理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 クレデンシャルは、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するか、それらを必要とするシナリオ内の手順を調べることで確認できます。

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、このガイドのシナリオを完了し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] [英語]

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. 最適なパフォーマンスを得るためには、**Cisco AnyConnect VPN** [手順を見る] および**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します。

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

注: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することもできます [手順を見る]。dCloud リモート デスクトップ クライアントは、最小限の操作でアクティブ セッションにアクセスする場合に最適です。ただし、この方法では、接続ができない場合や、パフォーマンスが悪い場合があります。

注：Wkstbr2 のリモート デスクトップの接続を確認します。ログイン プロンプト パスワード C1sco12345 を取得していることを確認してください。

シナリオ 1： 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**、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

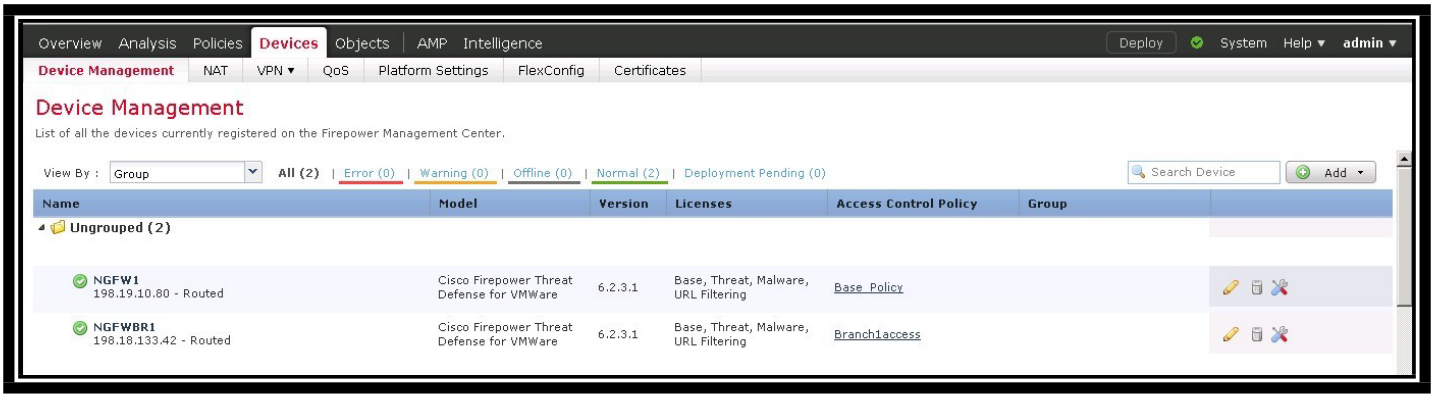
オブジェクトを作成する

このラボ演習に必要なオブジェクトを作成する

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. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [インターフェイス（Interface）] 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。
   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。
   b. [名前（Name）] に「**BViZone**」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 [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）] > [NGFW1] に移動します。



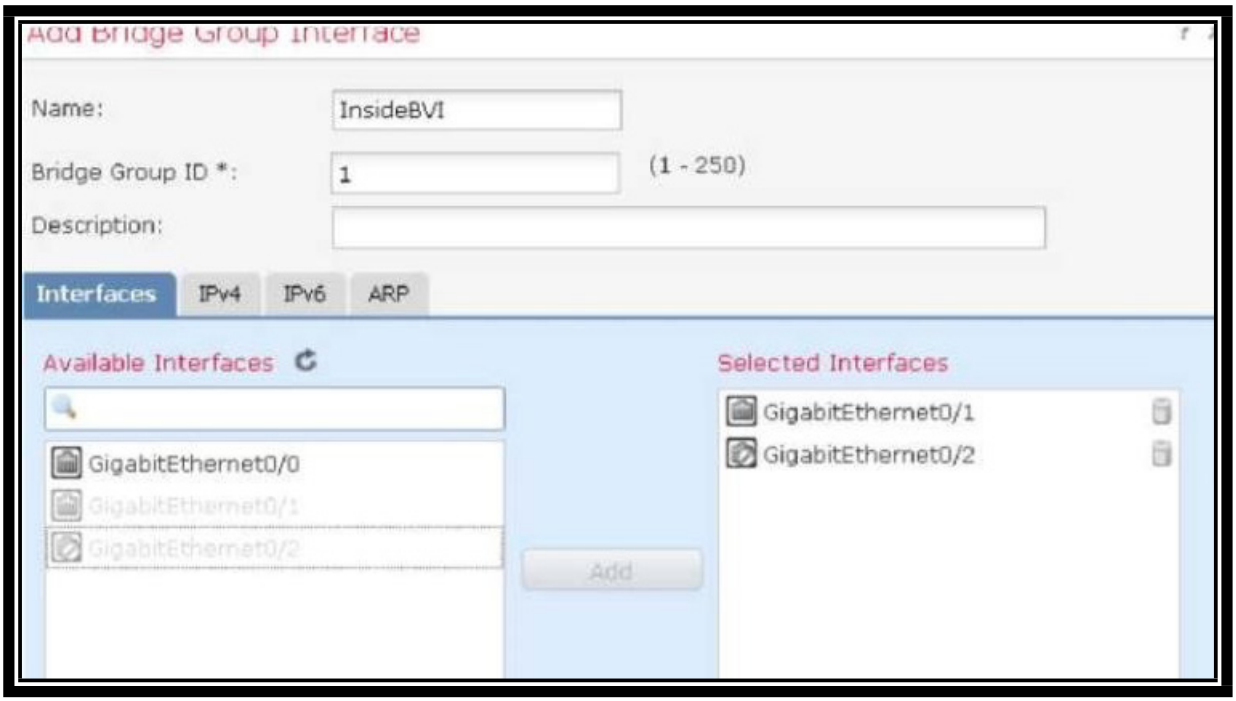
a. 鉛筆アイコンをクリックして NGFW デバイス設定を編集し、[インターフェイス（Interfaces）] タブを選択します。

b. 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。

c. **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。

d. [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。

e. [名前（Name）] に「**insideBVi**」と入力します。



f. [ブリッジ グループ ID（Bridge Group ID）] に「**1**」と入力します。

g. [GigabitEthernet0/1] と [GigabitEthernet0/2] を選択し、[追加（Add）] をクリックします。

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

i. [OK] をクリックします。

2. 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。

3. 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。

4. [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

注：基本ラボからのルーティング シナリオを実行していて、BVI インターフェイスにスタティック NAT ルールを適用する場合は、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ゾーンが許可されていないためです。

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。

a. [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。

b. [名前（NAME）] に「**inZone1**」と入力します。

c. [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。

d. インターフェイス **inside1** を選択し、[追加（Add）] をクリックします。

e. [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. **Default_PAT** ポリシーを編集します。

a. ルーティング シナリオを実行した場合は、すべての**自動 NAT ルール**で、**InZone** を **InZone1** に置き換えてください。

b. 他のすべてのルールで、**InZone** を **BVIZone** に置き換えます。

c. [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）] > [アクセスコントロール（Access Control）] > [アクセスコントロール（Access Control）] の順に選択します。

a. 鉛筆アイコンをクリックして、**Base_Policy** を編集します。

b. すべてのルールで **InZone** を **BVIZone** に置き換えます。

2. **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。

a. [名前（Name）] に「**Allow Internal Traffic**」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. [BVIZone] を選択し、[送信元に追加（Add to Source）] をクリックします。

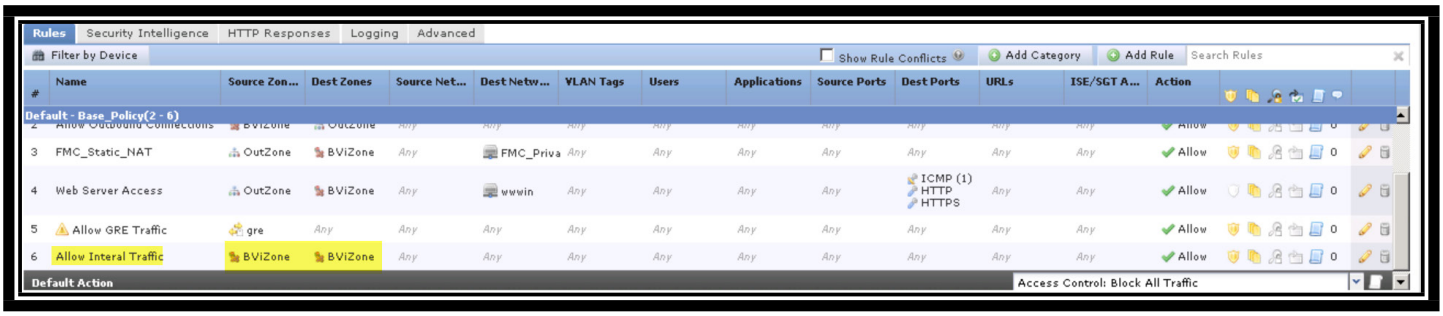
e. [BVIZone] を選択し、[宛先に追加（Add to Destination）] をクリックします。

f. [インスペクション（Inspection）] タブを選択します。

g. [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。

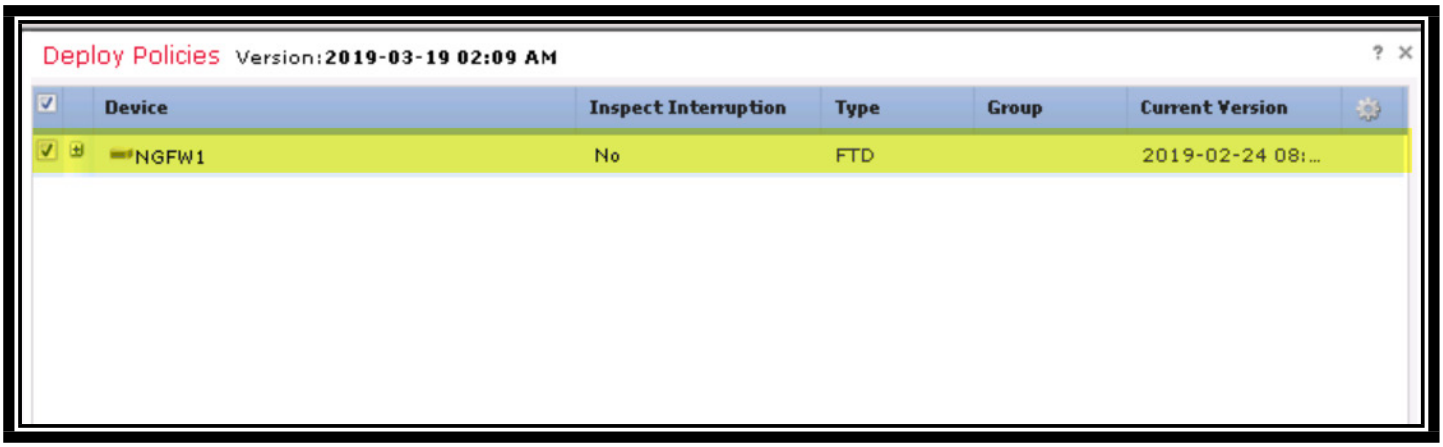
h. [ファイル ポリシー（File Policy）] ドロップダウン リストから [デモ ファイル ポリシー（Demo File Policy）] を選択します。

i. [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。

4. ポリシーを NGFW1 に導入して設定をテストします。



注：設定変更を導入し、導入が完了するまで待ちます。

5. **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。

6. 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、「**ftp isolated**」コマンドを実行します。

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

i. **cd ~root** と入力します。次のメッセージが表示されます。

ii. **[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）]**

c. 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。

iii. 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** ii. これは成功するはずです。iii. 次に、WGET を使用して、タイプ別にブロックされたファイルのダウンロードを試みます。**wget -t 1 isolated/files/test3.avi**

注：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。

iv. 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す。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。

シナリオ 2： ハイアベイラビリティ設定

この演習は、次のタスクで構成されています。

- バックアップ NGFW を導入して設定する
- ファイアウォールのハイアベイラビリティ ペアを作成する
- 仮想 MAC アドレスでアクティブ/スタンバイを設定する
- 設定をテストする

この演習の目的は、ハイアベイラビリティ NGFW について理解し、設定することです。2 番目のファイアウォールを設定し、ハイアベイラビリティ グループに追加します。

手順

IRB ラボ コンポーネントを削除する

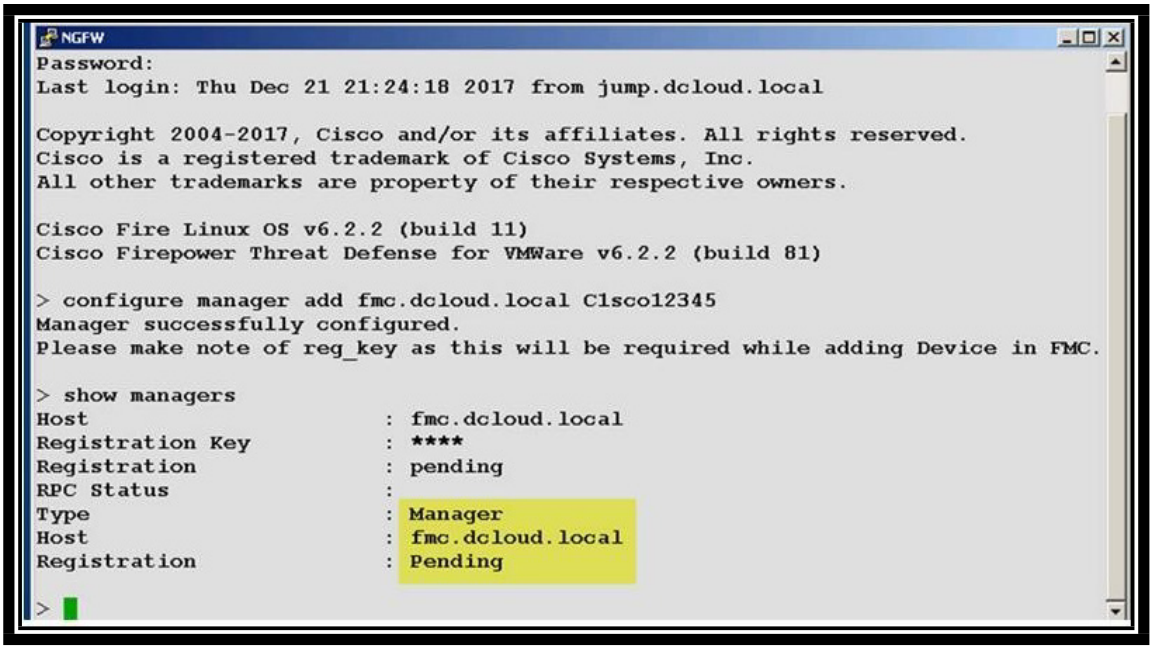
注：ラボに関する現行の制限により、**フェールオーバー HA リンクに GigabitEthernet 0/2 を使用する NGFW1** から、**IRB 設定を削除する必要があります。**

1. **[デバイス（Devices）] > [デバイス管理（Device Management）] に移動し、**NGFW1 **の行の**鉛筆**アイコンをクリックします。**
2. **BVI1 インターフェイス**で [アイコンの削除（Remove Icon）] をクリックします。
3. [GigiabitEthernet 0/1] に移動し、**鉛筆**アイコンをクリックします。
    a. [名前（Name）] : **LAN-Side**
    b. [有効（Enabled）] をクリックします。
    c. [セキュリティゾーン（Security Zone）] : **InZone**
    d. [IPv4] : **198.19.10.1/24**
    e. [OK] をクリックします。
    f. [保存（Save）] をクリックします。
4. GigabitEthernet 0/2 に移動し、インターフェイスから名前を削除して、それが有効になっていることを確認します。
5. [デバイスNAT（Device NAT）] の [デフォルトPAT（Default PAT）] に移動します。
    a. 「**inZone1 with InZone for all NAT Rules**」を置き換えます。
    b. [BVIZone] を [InZone] に置き換えます。
    c. [保存（Save）] をクリックします。
6. [ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [Base_Policy] に移動します。
    a. **鉛筆**アイコンをクリックします。
    b. [ALL BVIZone] を [InZone] に置き換えます。
    c. [BViZone to BViZone used for the Allow Internal Traffic] の行は削除することができます。d. [保存（Save）] をクリックします。
7. [展開（Deploy）] をクリックします。

8. ネットワークのテスト
    a. **内部 Linux サーバ**から
        i. **Outside** に ping します。
    b. **外部 Linux サーバ**から
        i. **198.18.133.120**（FMC の外部 NAT アドレス）**に ping します。**
        ii. **198.18.128.202**（内部 Linux サーバの外部 NAT アドレス）**に ping します。**
        ユーザ名：admin、パスワード：C1sco12345 で、NGFWBR1 への PuTTY セッションを開きます。
        iii. コマンド プロンプトを開きます。
            1. **198.18.133.120**（FMC の外部 NAT アドレス）**に ping します。**
            2. **198.18.128.202**（内部 Linux サーバの外部 NAT アドレス）**に ping します。**

REST API スクリプトを実行して NGFW2 を設定する

1. Jump PC に移動し、PuTTY セッションを開いて **NGFW2** を選択し、[ロード（Load）]、[開く（Open）] の順に選択します。
    a. ユーザ名：**admin**、パスワード：**C1sco12345**
    b. 「show managers」と入力します。
    c. マネージャが設定されていないと表示された場合には、次の手順を行います。
        i. 「configure manager add fmc.dcloud.local C1sco12345」と入力して、「**yes**」と入力します（「yes」とすべて入力する必要があります）。
        ii. コマンド プロンプトが戻ってきたら、「show managers」と入力し、fmc.dcoud.local のステータスが [保留中（pending）] になっていることを確認します。



注：次の情報がフェールオーバー リンク経由で伝達されています。

装置の状態（アクティブまたはスタンバイ）

Hello メッセージ（キープアライブ）
ネットワーク リンクの状態
MAC アドレス交換
コンフィギュレーションの複製および同期

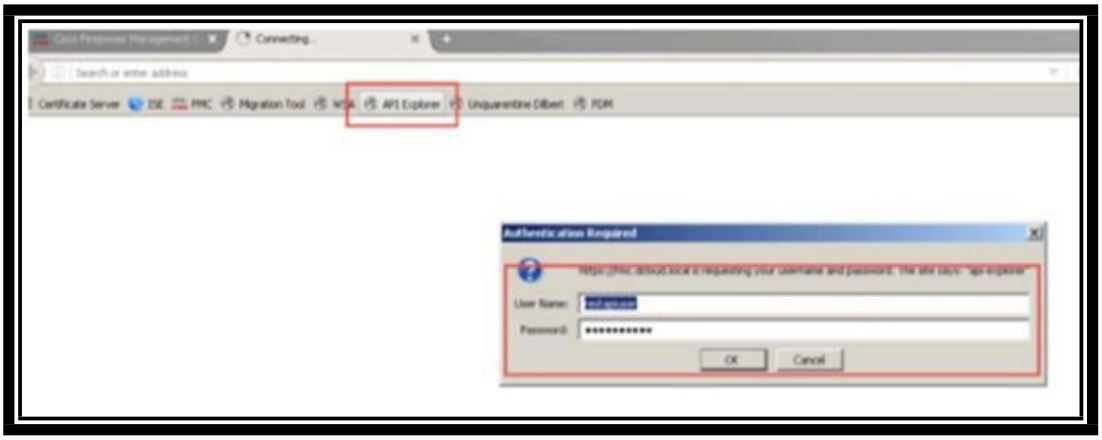
Firepower Threat Defense のハイアベイラビリティ ペアを作成または解除すると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスがただちに再開し、両方のデバイスでトラフィック検査が一時的に中断されます。この中断中にトラフィックをドロップするか、それ以上の検査を行わずにパスさせるかは、管理対象デバイスのモデルとそのトラフィックの処理方法によって異なります。詳細については、Snort® Restart Traffic Behavior を参照してください。ハイアベイラビリティ ペアの作成を続行すると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再開される警告が表示され、キャンセルできます。

注：シナリオ 1 から始めて基本ラボを完了している場合は、手順 2 に進みます。

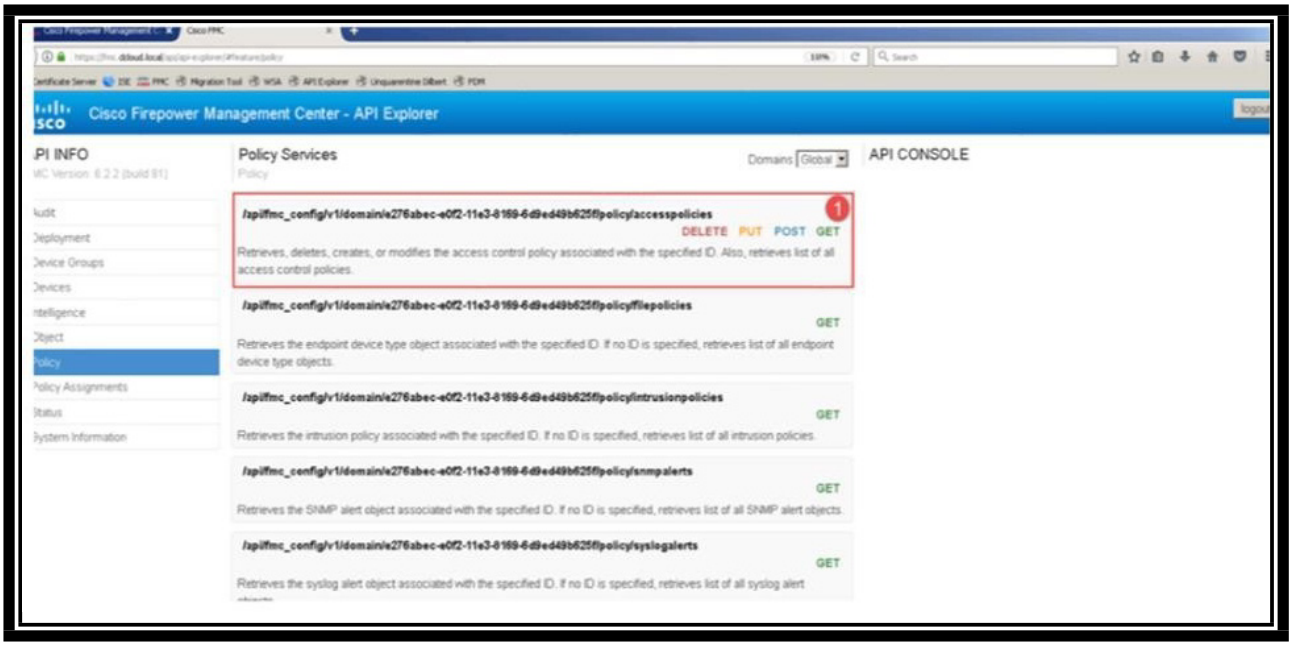
シナリオ 6 から始めてアドバンスド ラボを完了している場合は、以下の「REST API スクリプトを変更して NGFW を登録/設定する」手順を実行します。次に手順 2 から残りのラボを完了させます。

REST API スクリプトを変更して NGFW を登録/設定する

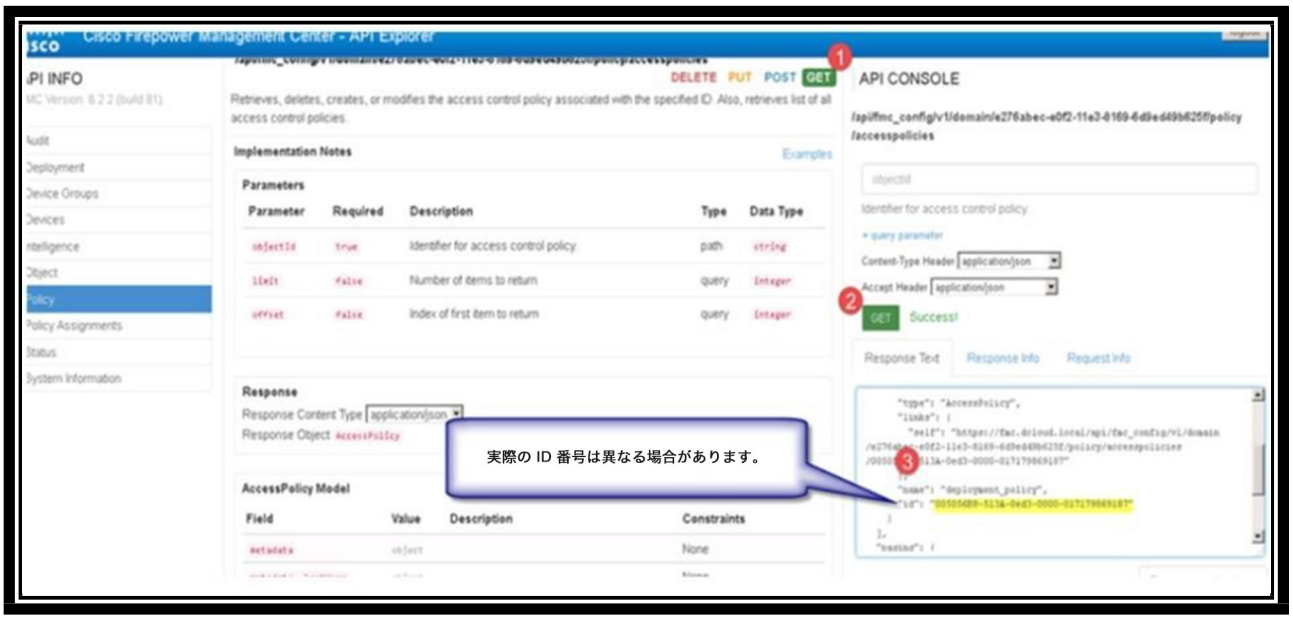
1. Jump PC の Firefox ブラウザで [+] タブをクリックして新しいタブを開きます。
2. FMC API（API Explorer）タブでは、ユーザ名/パスワード（restapiuser/C1sco12345）が事前に入力されています。



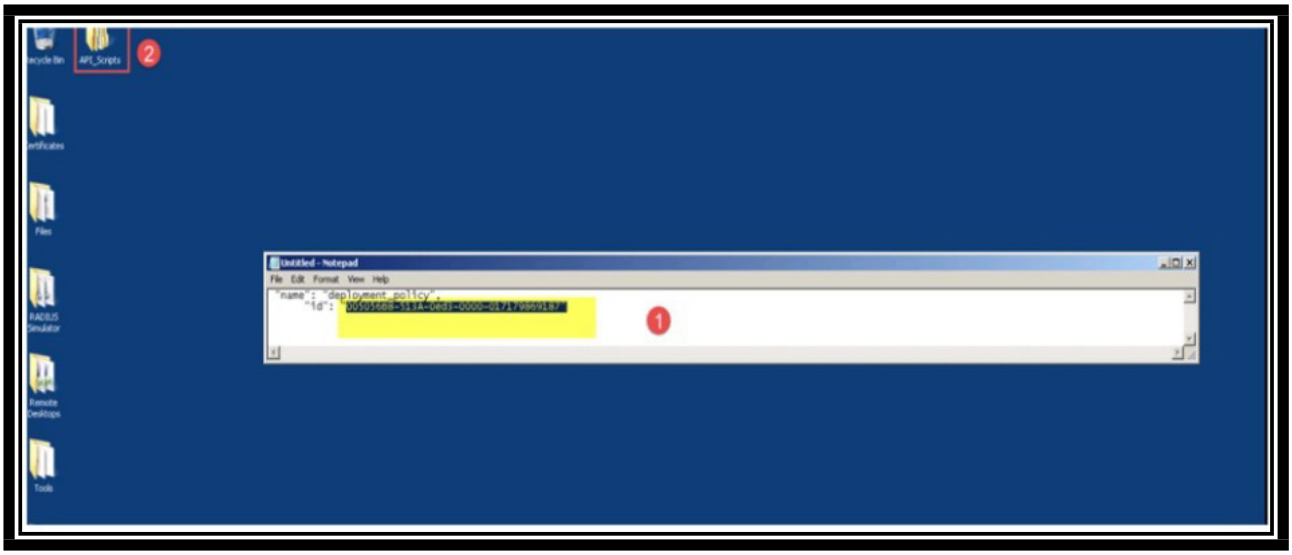
3. [ポリシー（Policy）] をクリックします。



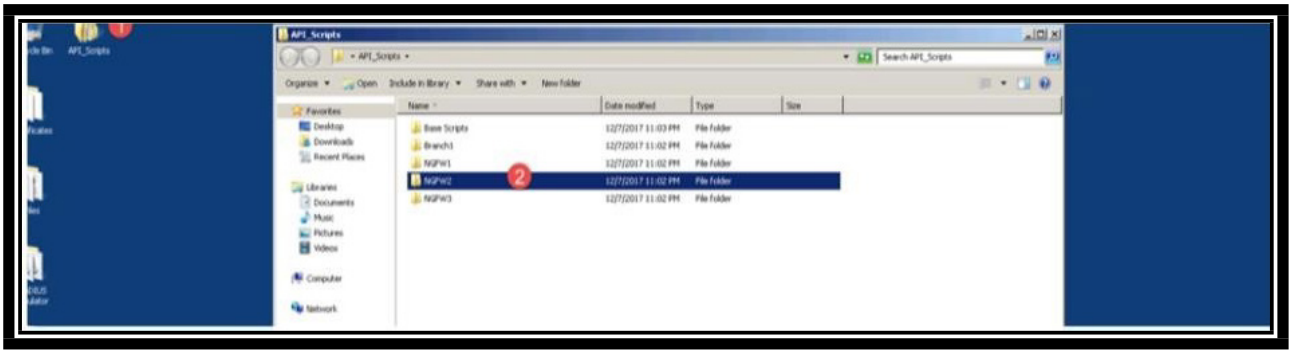
4. [ポリシー（Policy）] に移動し、最初のポリシー **accesspolicies** を選択し、**GET** アイコンをクリックします。
5. API コンソールの [取得（Get）] ボタンを選択します。
6. 作成したアクセス コントロール ポリシーの名前に一致する**アクセス ポリシー ID 番号**をコピーします。
    a. 基本ラボから続いて実施していない場合は、[Base_Policy] を探します。



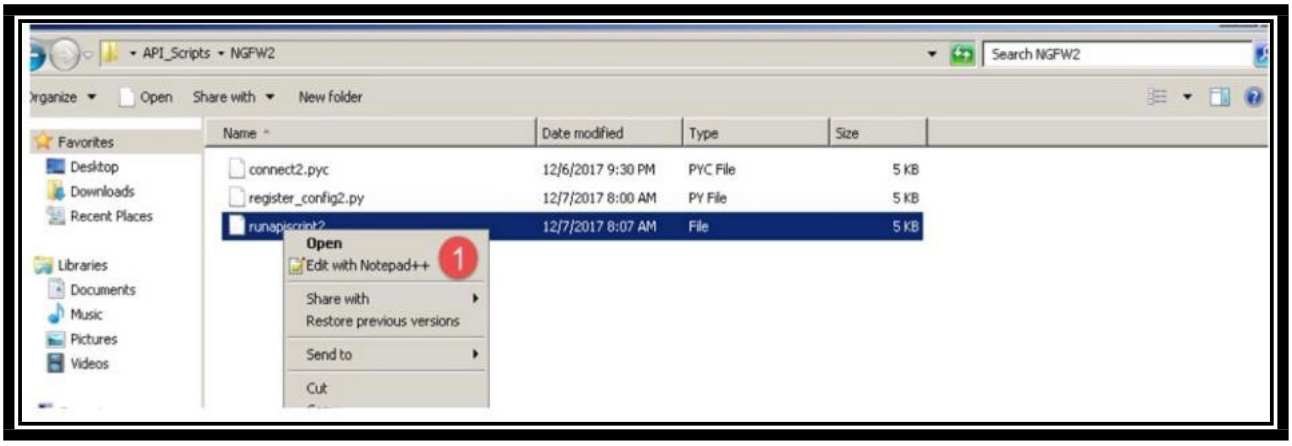
7. アクセス ポリシー ID 番号を Jump PC のメモ帳にコピーします。



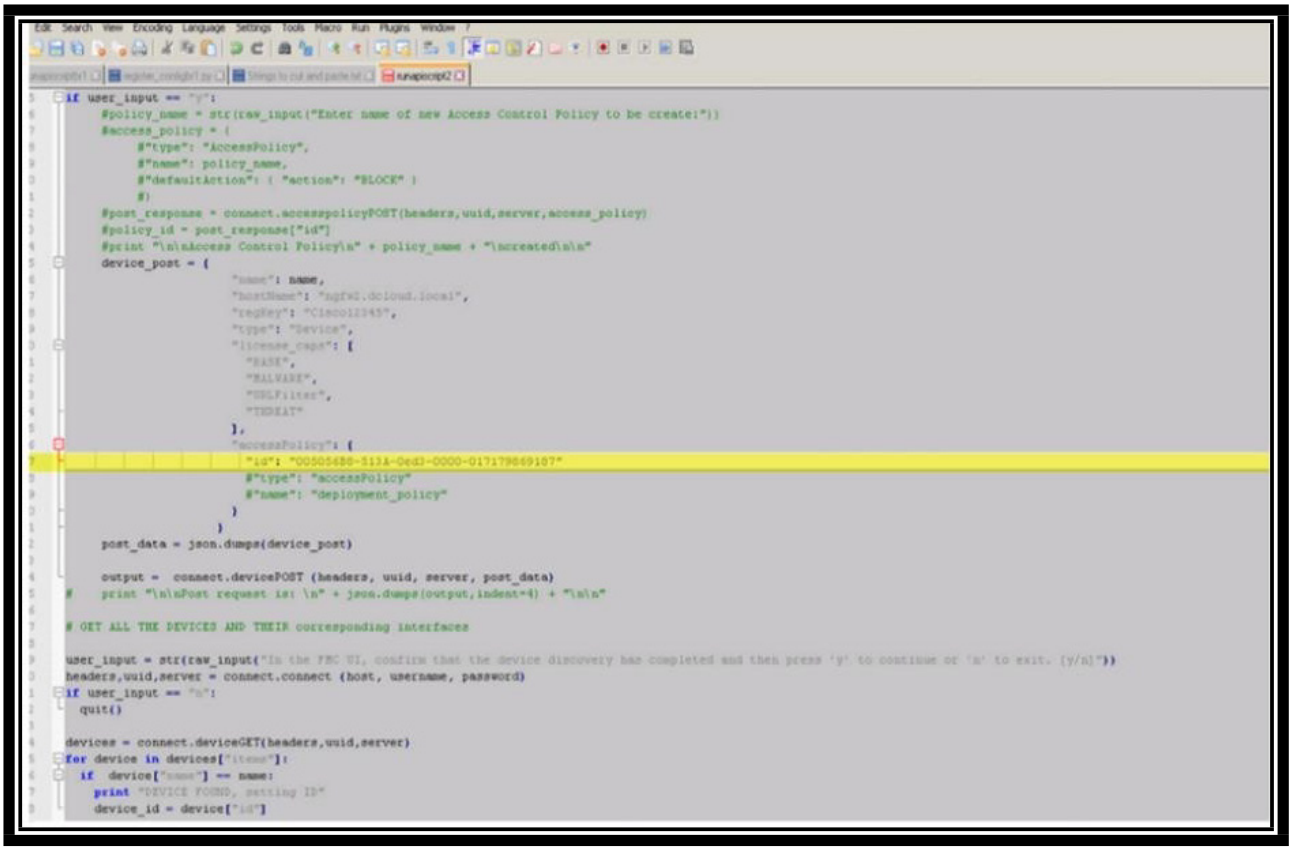
8. Jump PC Desktop の **API_Scripts** フォルダに移動し、**NGFW2** フォルダを選択します。



9. **Notepad++** を使用して、スクリプト フォルダから **runapiscript2** を選択して開きます。



10. **37 行目に移動して、**コピーしたアクセス ポリシー ID を引用符が付いた ID の箇所に貼り付けます。



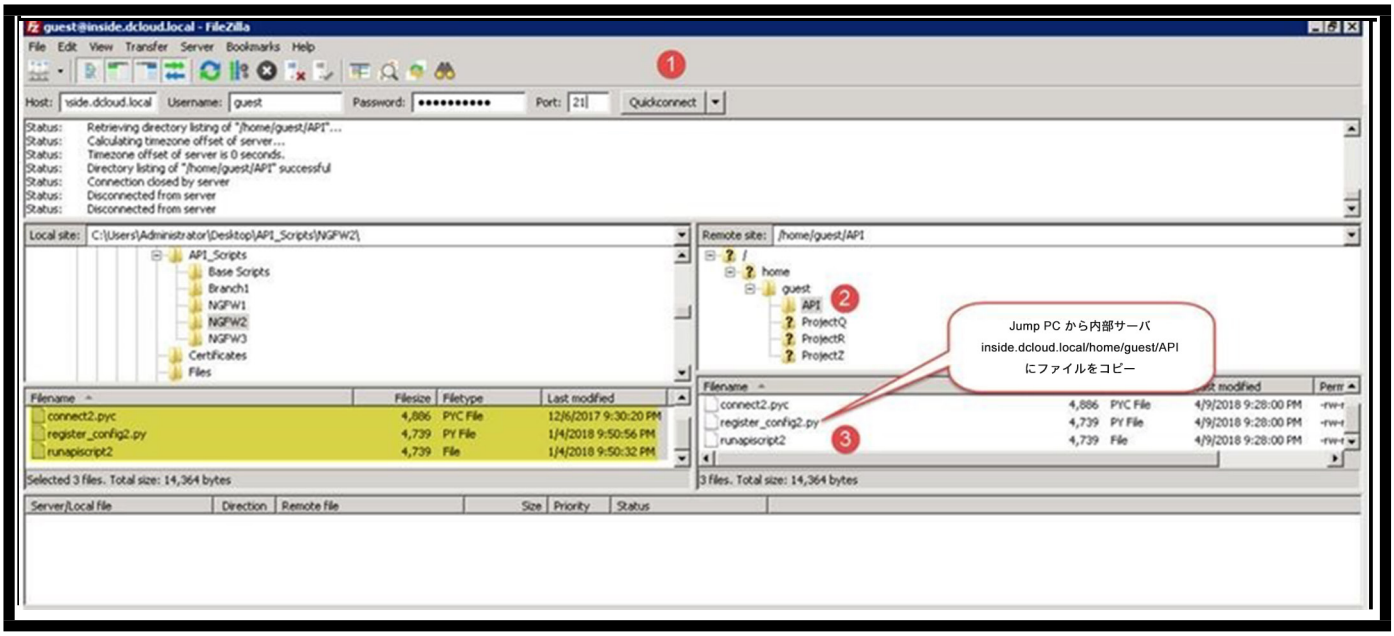
```
if user_input == "y":
    #policy_name = str(raw_input("Enter name of new Access Control Policy to be create:"))
    #access_policy = {
        #"type": "AccessPolicy",
        #"name": policy_name,
        #"defaultAction": { "action": "BLOCK" }
        #}
    #post_response = connect.accesspolicyPOST(headers,uuid,server,access_policy)
    #policy_id = post_response["id"]
    #print "\n\nAccess Control Policy\n" + policy_name + "\ncreated\n\n"
    device_post = {
                    "name": name,
                    "hostName": "ngfw2.dcloud.local",
                    "regKey": "Cisco12345",
                    "type": "Device",
                    "license_caps": [
                      "BASE",
                      "MALWARE",
                      "URLFilter",
                      "THREAT"
                    ],
                    "accessPolicy": {
                      "id": "00505680-113A-0ed3-0000-017179669187"
                      #"type": "accessPolicy"
                      #"name": "deployment_policy"
                    }
                  }
    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, getting ID"
    device_id = device["id"]
```

11. **Notepad++** のメニューから [保存（Save）] を選択します。

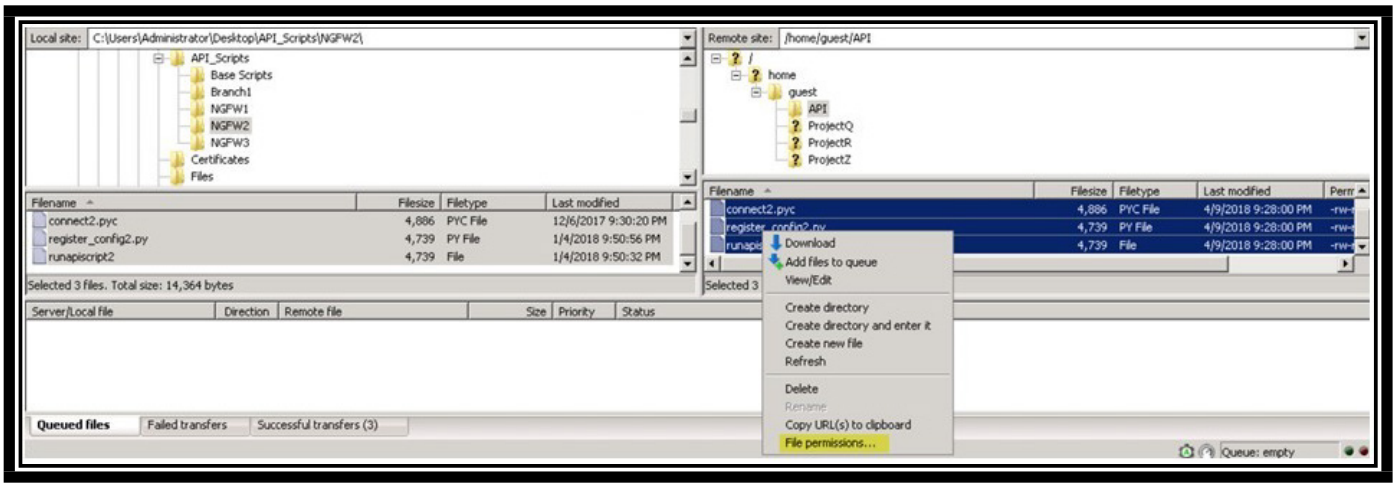
注：この場合は [保存（Save）] を使用し、[ファイル名を指定して保存（Save As）] は使用しないでください。同じファイル タイプのままにしてスクリプトで参照できるようにするためです。Register_Config2.py について繰り返します。

内部 Linux サーバにファイルをコピーする

1. Jump PC で **Filezilla** プログラムを開始します。
2. ホスト名フィールドに**「inside.dcloud.local」または「198.19.10.200」**と入力します。
3. ユーザ名：**guest**、パスワード：**C1sco12345**、ポート：**21** でログインします。
4. **home/guest/API** フォルダに移動し、Jump PC から**内部 Linux サーバ**にファイル（NGFW2 フォルダ）をコピーします。

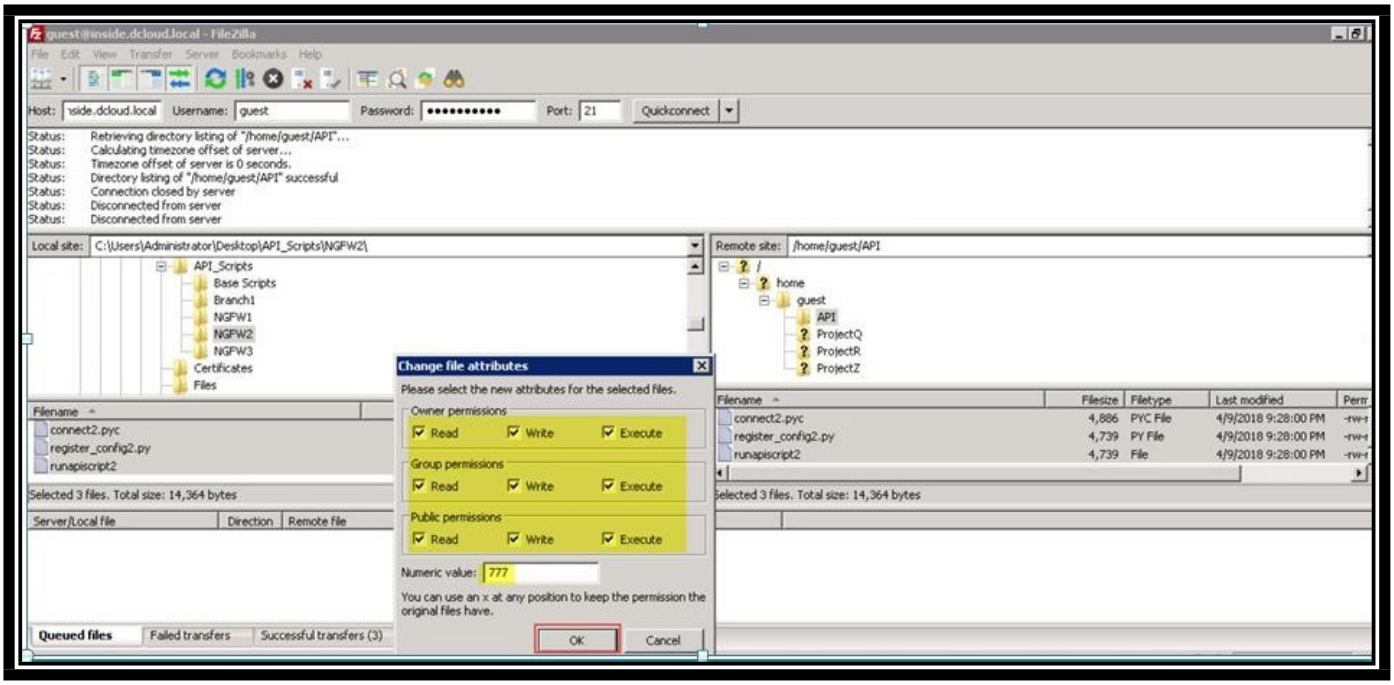


5. コピーしたファイルを右クリックして、[ファイルのアクセス許可（File Permissions）] を選択します。

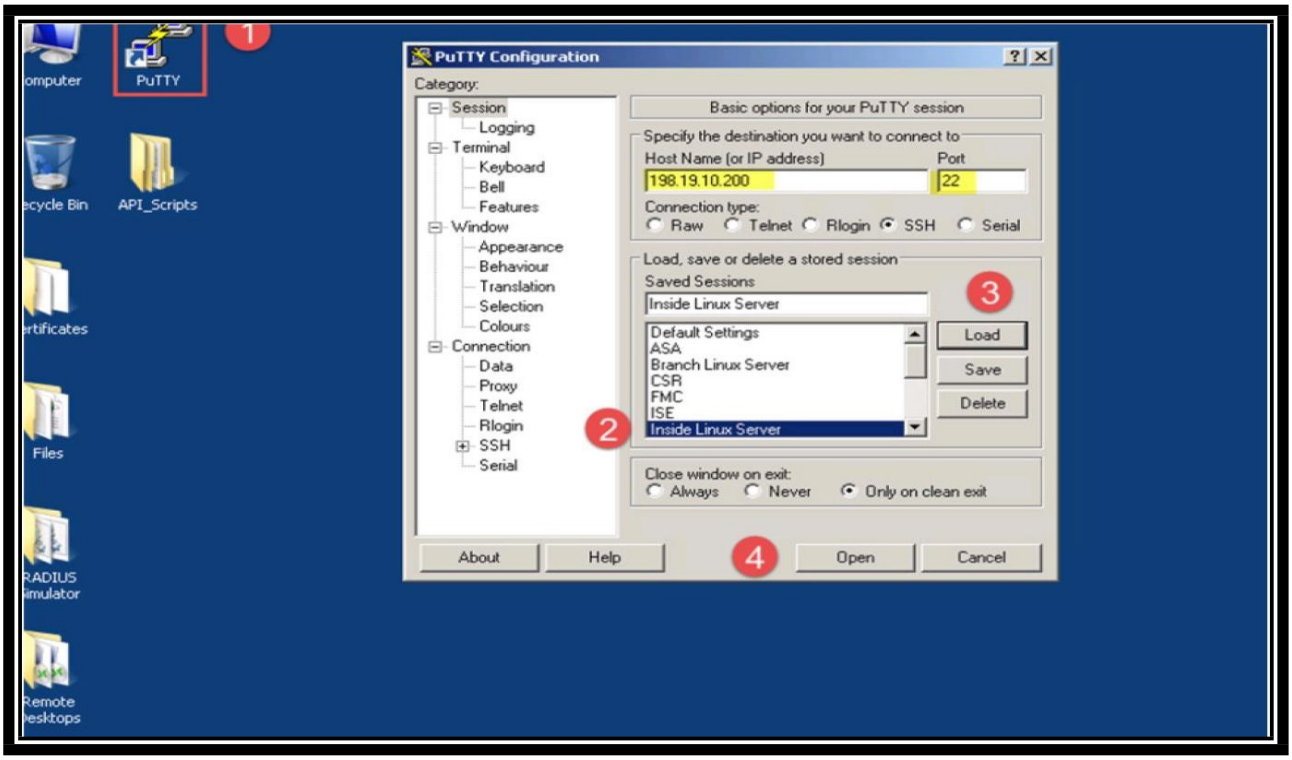


6. 数値が **777** になるように、すべての**ファイル属性**を選択します。

注 : それによりすべての属性が有効になり、Linux サーバでスクリプトを実行できるようになります。これはラボ テストに限定された設定です。有効にするファイルのアクセス許可については、IT チームに問い合わせてください。



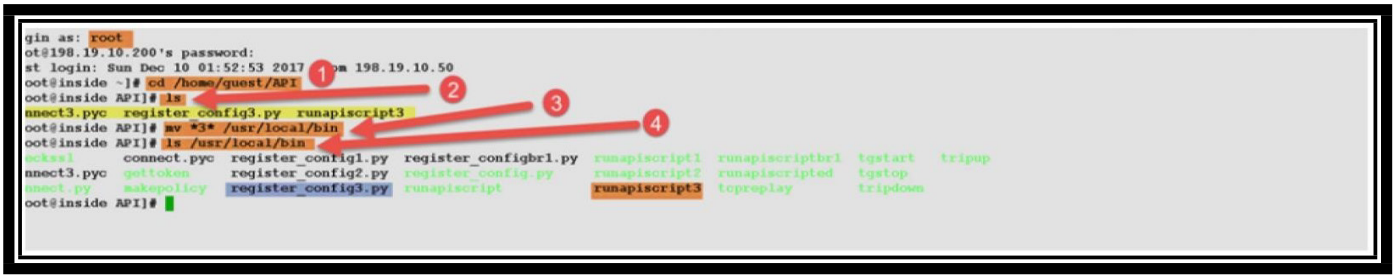
7. Jump PC で **PuTTY** を開きます。
8. **内部 Linux サーバ**に対する SSH セッションを開きます。



9. ユーザ ID：**root**、パスワード：**C1sco12345** でログインします。
10. 「**cd /home/guest/API**」と入力します。
11. 「**ls**」と入力します（ディレクトリの内容が表示されます）。

12. 「**mv *(x)* /usr/local/bin**」と入力します（名前に「x」が含まれるファイルが usr/local/bin ディレクトリに移動します。「x」はスクリプト番号を示します）。ファイルを上書きするか確認された場合は、[y] を選択します。

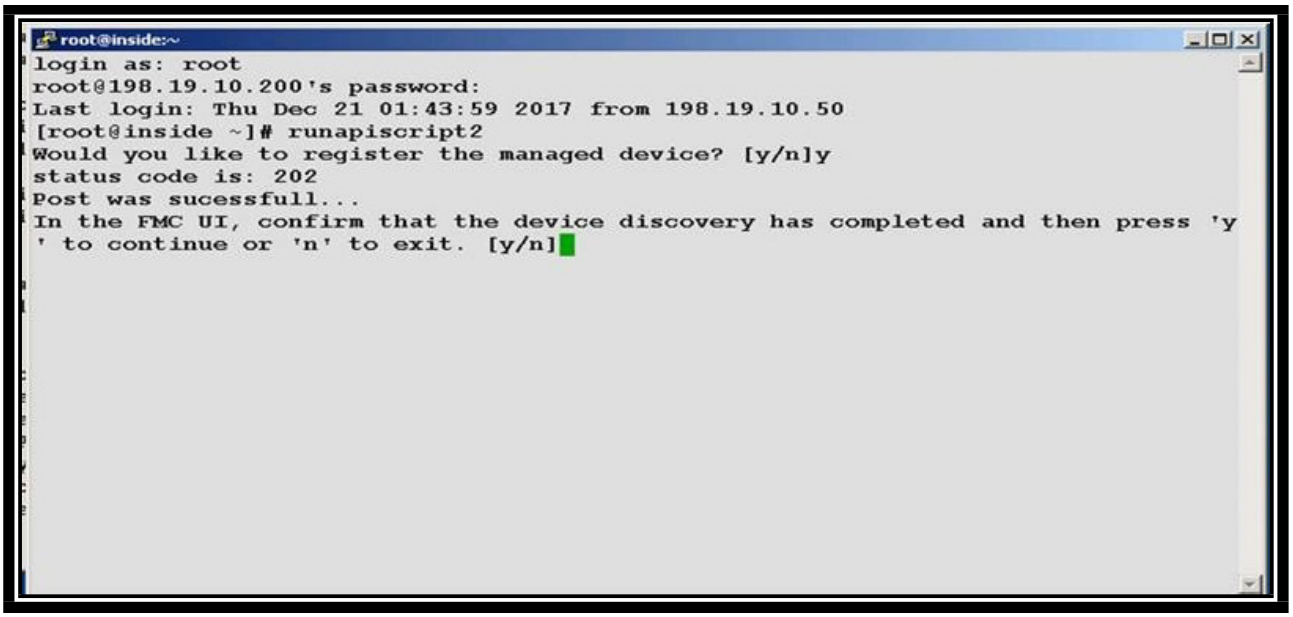
13. 「**ls/usr/local/bin**」と入力します（/usr/local/bin ディレクトリの内容が表示されます）。



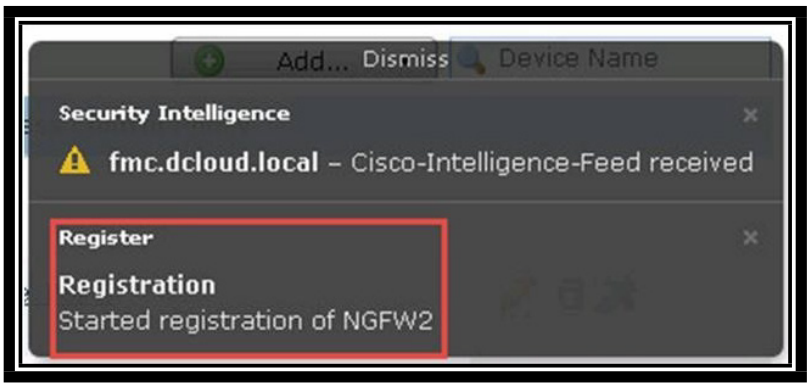
注: Jump PC からすべてのファイルを一括でコピーして移動させることも可能です。上記の手順は、スクリプトをホストサーバに移動させるプロセスを示したものです。

14. 内部 Linux サーバで次の手順を実行します。

    a. 「**runapiscript2**」と入力し、プロンプトが表示されたら「**y**」と入力します。



15. Firefox に戻り、FMC で NGFW2 の登録ステータスを確認します。



16. **検出**が完了したら、内部サーバの PuTTY セッションに戻り、スクリプトを続行します。

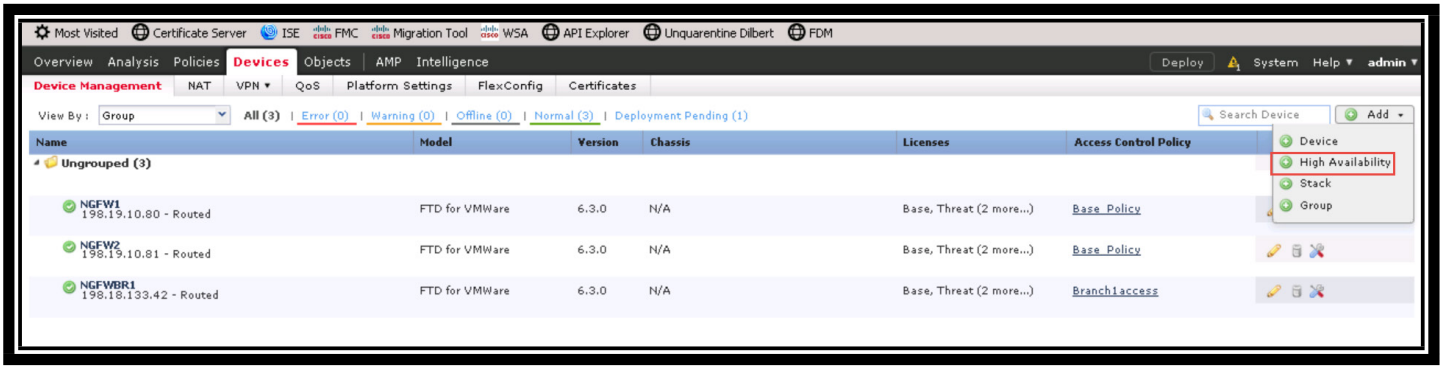
    a. この検出プロセスが完了するまで数分かかります。

    b. 「**y**」を選択してスクリプトを続行します。その後、スクリプトから、検出されたインターフェイスを設定するように求められます。「**y**」を選択します。

注：このスクリプトでは、アクセス ポリシー名の選択は要求されません。NGFW1 のセットアップで設定したスクリプト名の ID を使用するように、スクリプトを変更したためです。

ハイアベイラビリティ ペアを設定する

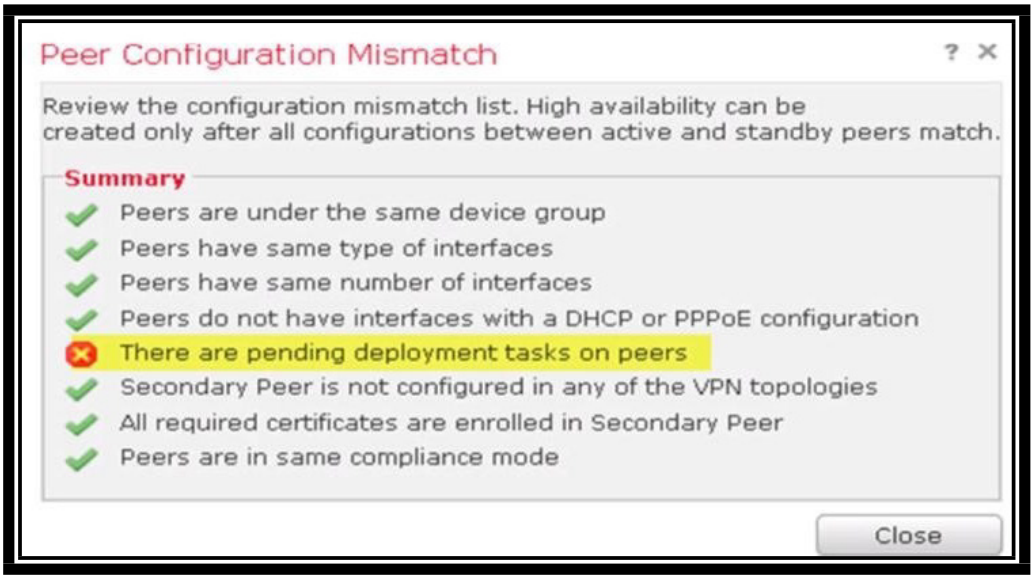
1. [デバイス(Devices)] > [デバイス管理(Device Management)] > [追加(Add)] > [ハイアベイラビリティの追加(Add High Availability)] に移動します。



注：NGFW2 管理インターフェイス（198.19.10.81）は初期設定中に事前設定されています。G0/0 および G0/1 インターフェイスはスクリプトによって設定されています。インターフェイスにはセキュリティ ゾーンがリストされていませんが、HA プロセスが実行されると、セキュリティ ゾーンとインターフェイスの IP アドレスが NGFW1 から継承されます。

2. [名前（Name）]：HA_Test Device
3. [タイプ（Type）]：Firepower Threat Defense
4. [プライマリ ピア（Primary Peer）]：NGFW1
5. [セカンダリ ピア（Secondary Peer）]：NGFW2
6. 続行します。

注：いずれかの HA ピアで設定タスクを行っていて、まだ導入していない場合は、次のメッセージが表示されます。



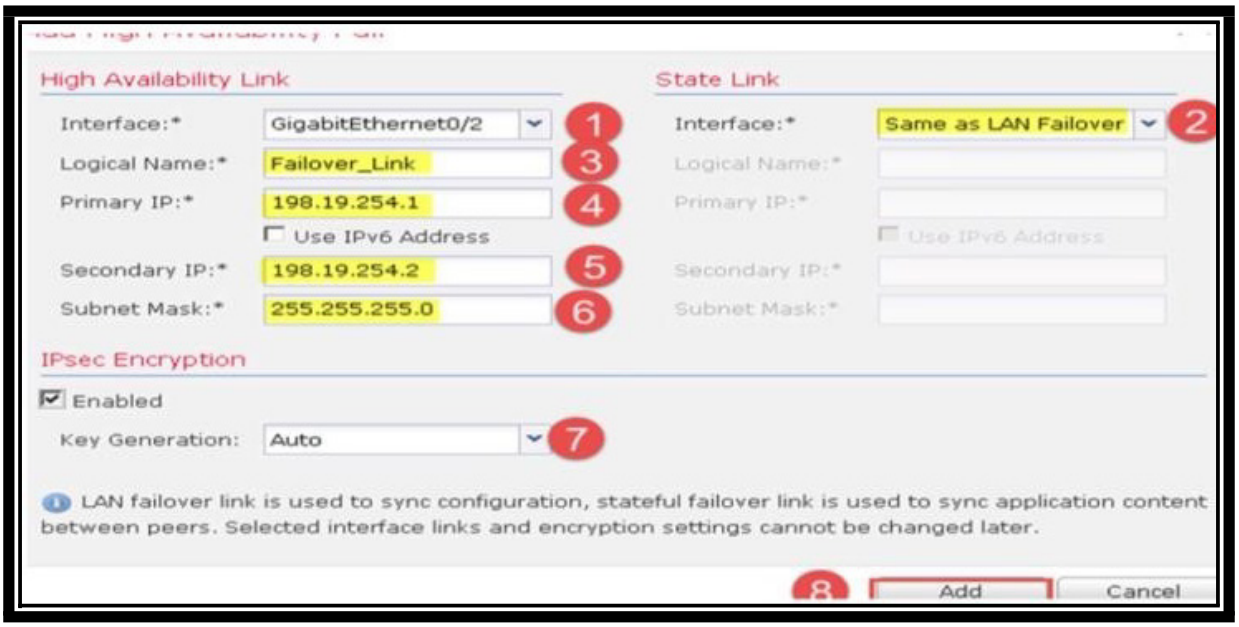
7. NGFW2 の変更を導入します。
8. 前に戻り、手順 2 を繰り返します。
9. インターフェイス「GigabitEtherent0/2」を選択します。
10. 名前：Failover_Link
11. プライマリ IP：198.19.254.1
12. セカンダリ IP：198.19.254.2

サブネット マスク：255.255.255.0

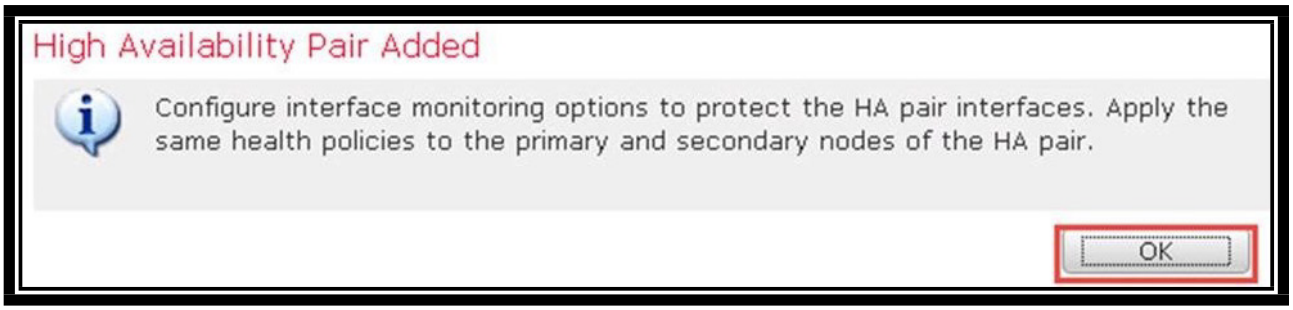
13. 状態リンク：LAN フェールオーバー IPsec と同じインターフェイス

14. 暗号化：有効（任意）

注：インターフェイスが表示されない場合は、[デバイス（Devices）] > [デバイス マネージャ（Device Manager）] に戻って各ファイアウォールの鉛筆アイコンをクリックし、インターフェイスをクリックして、有効であることと、インターフェイスに名前が付いていないことを確認します。



15. [OK] をクリックしてハイアベイラビリティ ペアを追加します。



注：HA の設定にはしばらく時間がかかります。導入ボタンの横の [タスク（Tasks）]を見れば、随時ステータスの更新を確認できます。

16. 完了すると次のように表示されます。

17. [デバイス（Devices）] > [デバイス管理（Device Management）] に移動し、HA ポリシーの横の鉛筆アイコンをクリックします。

注：MAC アドレスと IP アドレスがフェールオーバーされています。

インターフェイスを設定する場合、同じネットワーク上にアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。推奨されていますが、スタンバイ アドレスは必要ありません。スタンバイ IP アドレスがなければ、アクティブ装置はネットワーク テストを実行してスタンバイ インターフェイスの状態を確認することはできません。できることはリンク ステートの追跡のみです。また、管理目的でそのインターフェイス上のスタンバイ装置に接続することもできません。

プライマリ装置またはフェールオーバー グループがフェールオーバーすると、セカンダリ装置はプライマリ装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックの送信を開始します。

スタンバイ状態になった装置は、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。

ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

セカンダリ装置がプライマリ装置を検出せずにブートした場合、プライマリ装置の MAC アドレスを認識していないため、セカンダリ装置がアクティブ装置になり、自分の MAC アドレスを使用します。しかし、プライマリ装置が使用可能になると、セカンダリ装置（アクティブ）は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワーク トラフィックが中断されることがあります。同様に、新しいハードウェアでプライマリ装置をスワップ アウトすると新しい MAC アドレスが使用されます。

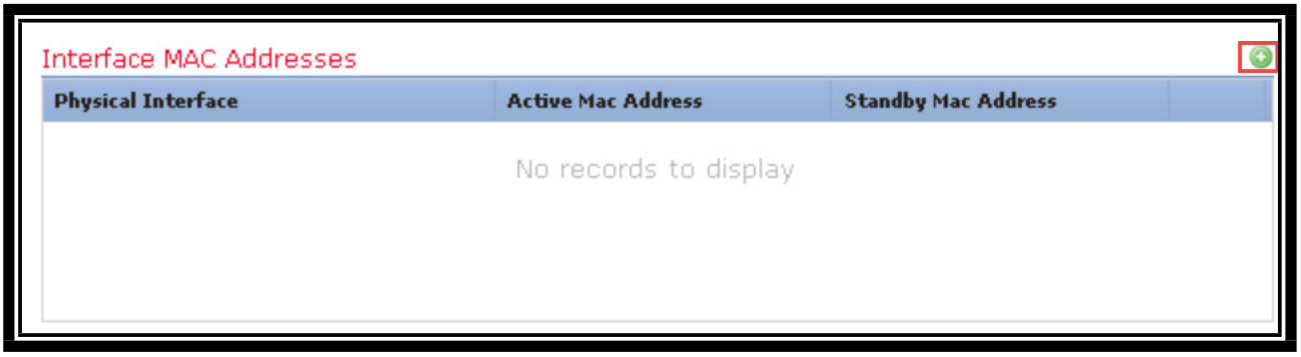
仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。マルチインスタンス機能では、FXOS シャーシはプライマリ MAC アドレスのみを自動生成します。プライマリおよびセカンダリ MAC アドレスの両方で、生成された MAC アドレスを仮想 MAC アドレスで上書きすることができますが、セカンダリ MAC アドレスを事前に定義することは必須ではありません。セカ

ンQダリ MAC アドレスを設定すると、セカンダリ装置のハードウェアが新しい場合に、to-the-box 管理トラフィックが中断されないようになります。

仮想 MAC アドレスを設定しなかった場合、トラフィック フローを復元するために、接続されたルータの ARP テーブルのクリアが必要になる場合があります。MAC アドレスを変更する場合、FTD はスタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。

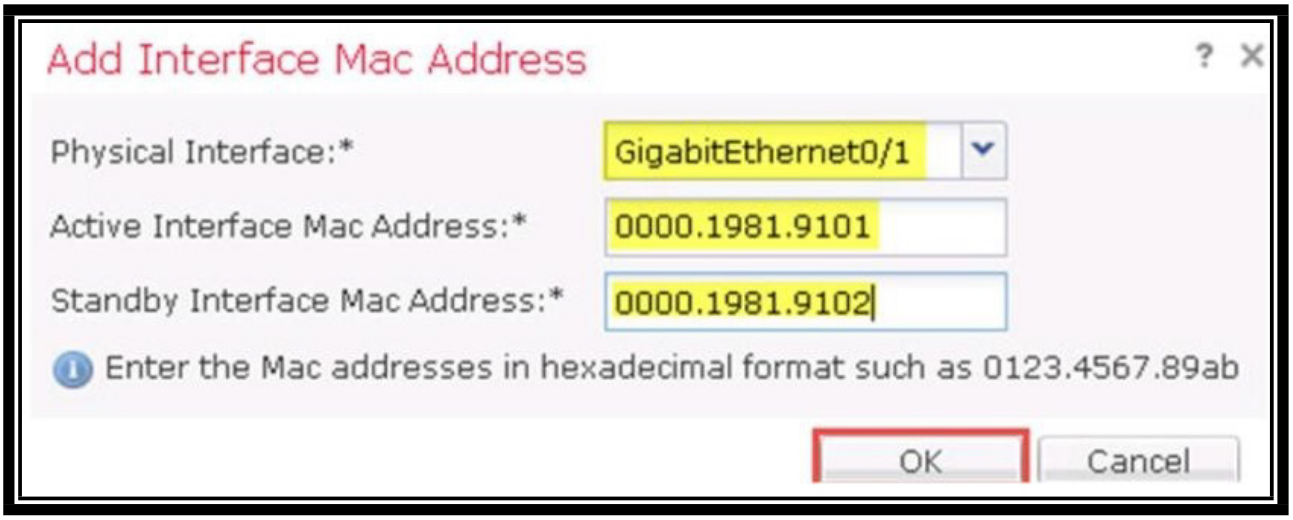
ステート リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。唯一の例外は、ステート リンクが通常のデータ インターフェイスに設定されている場合です。

18. インターフェイスの MAC アドレスの横の [+] アイコンをクリックします。



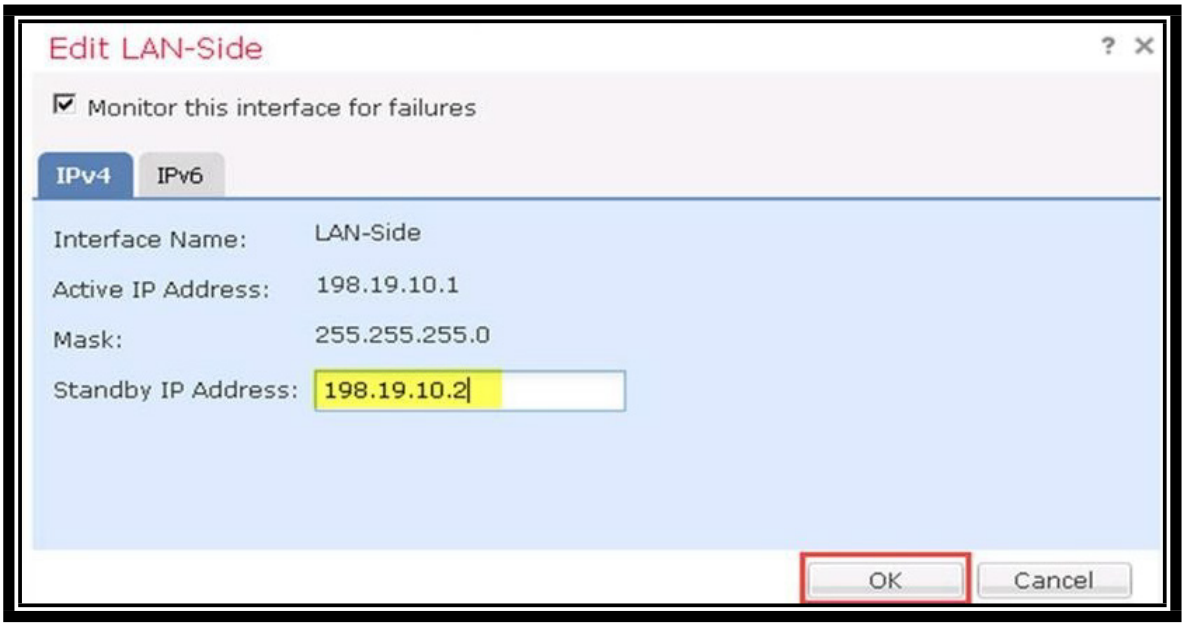
19. [物理インターフェイス（Physical Interface）]：GigabitEthernet0/1、[アクティブインターフェイスのMACアドレス（Active Interface MAC Address）]：受講者が選択（例で使用するインターフェイスの IP アドレス）、[スタンバイインターフェイスMACアドレス（Standby Interface Mac Address）]：受講者が選択。[OK] をクリックします。

注*：上記の手順は、インターフェイスの MAC アドレスを設定する方法の例です。

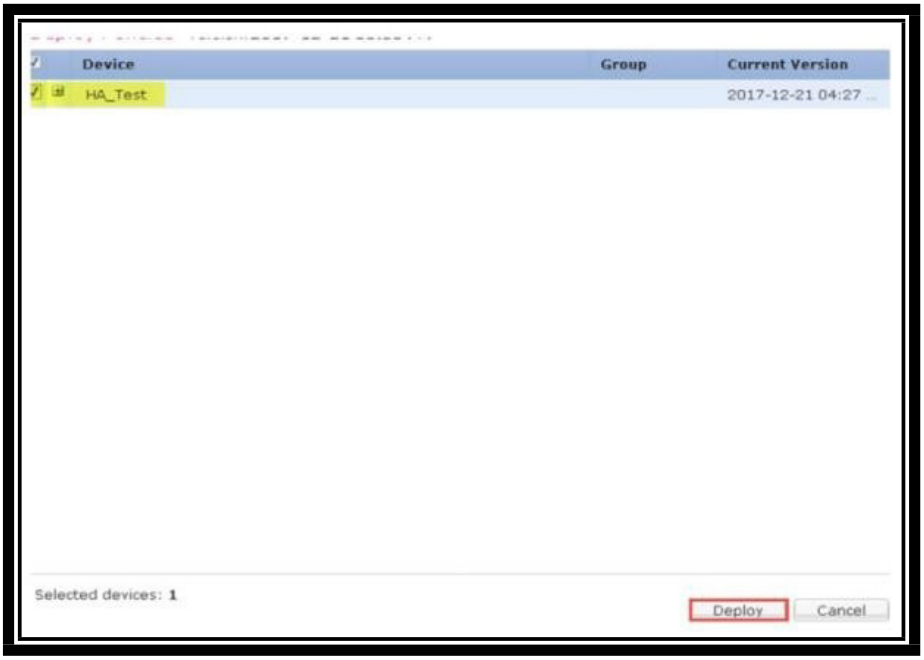


20. モニタ対象インターフェイスを設定します。モニタ対象インターフェイスの横にある鉛筆アイコンをクリックします。

10. [LAN-Side] を選択し、[スタンバイIPアドレス（Standby IP Address）]：198.19.10.2 を入力します。ISP-Side インターフェイス 198.18.133.3 についても繰り返します。



11. [保存（Save）]、[導入（Deploy）] の順にクリックし、HA_Test を選択して導入します。

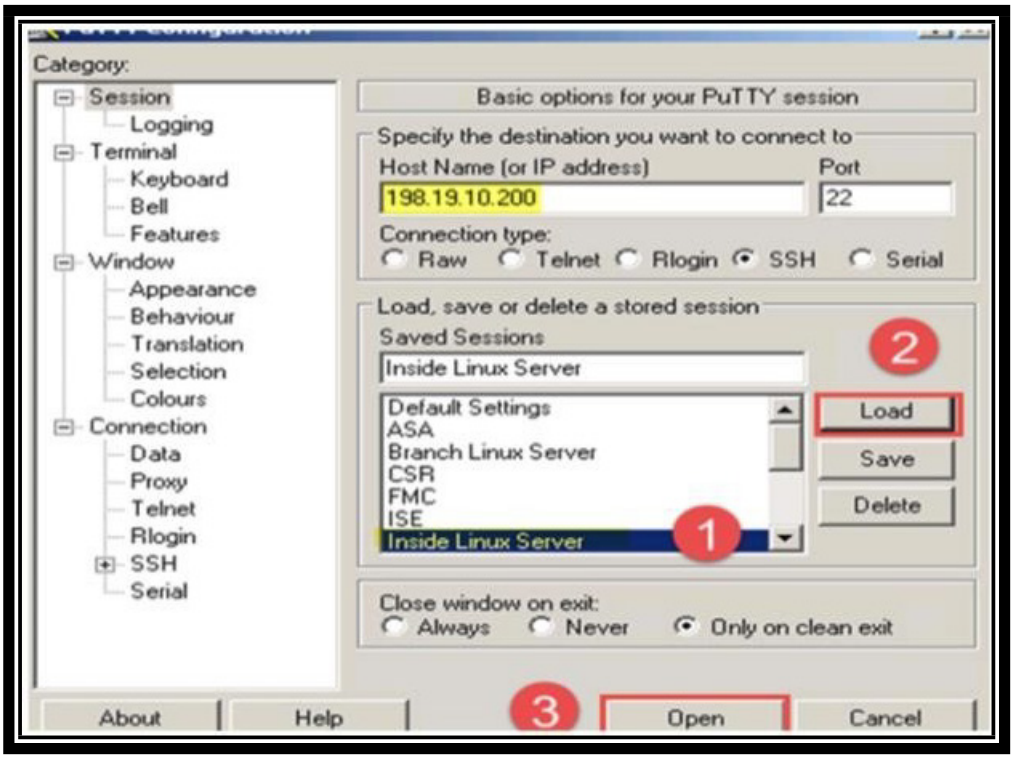


NGFW2 の設定

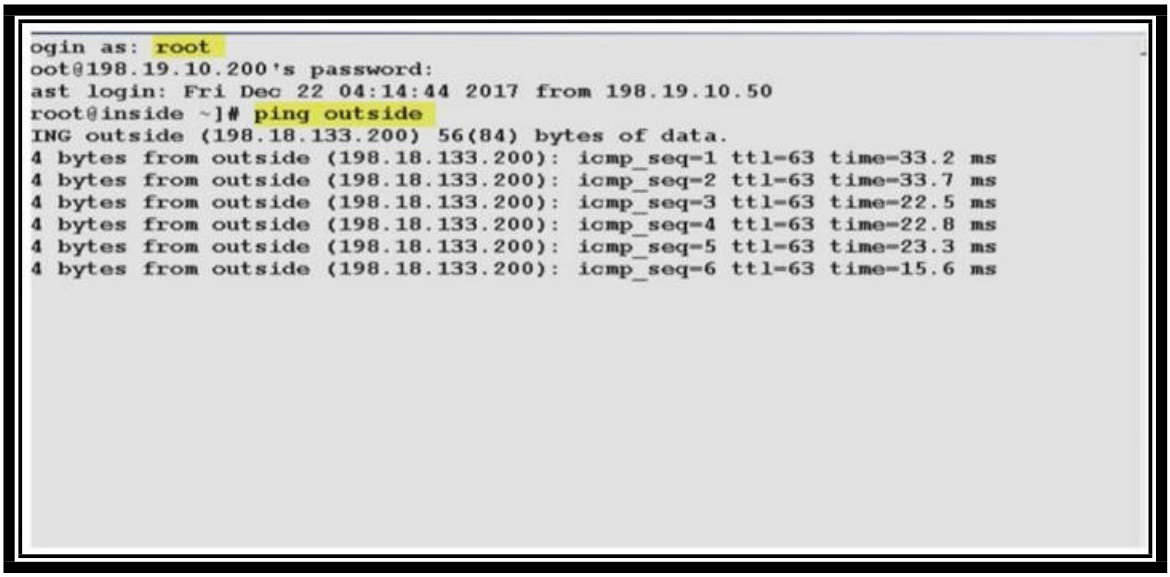
1. HA のセットアップ中に NGFW2 が受け取った設定パラメータを確認してみましょう。
2. Jump PC に移動して PuTTY を開き、NGFW2 を選択します。
3. ユーザ名：admin、パスワード：C1sco12345 で NGFW にログインし、以下を入力します。
    a show running-config interface
        i 各インターフェイスのプライマリ IP アドレスは何か。
        ii インターフェイスに関連付けられたスタンバイ IP アドレスはあるか。
    b show running-config failover
        i インターフェイス GigabitEthernet0/1 のフェールオーバー MAC アドレスは何か。
        ii Failover_Link のインターフェイスは何か。
        iii Failover_Link のインターフェイス IP アドレスは何か。

フェールオーバーをテストする

1. Jump PC で PuTTY に移動し、内部 Linux サーバに対するセッションを開きます。

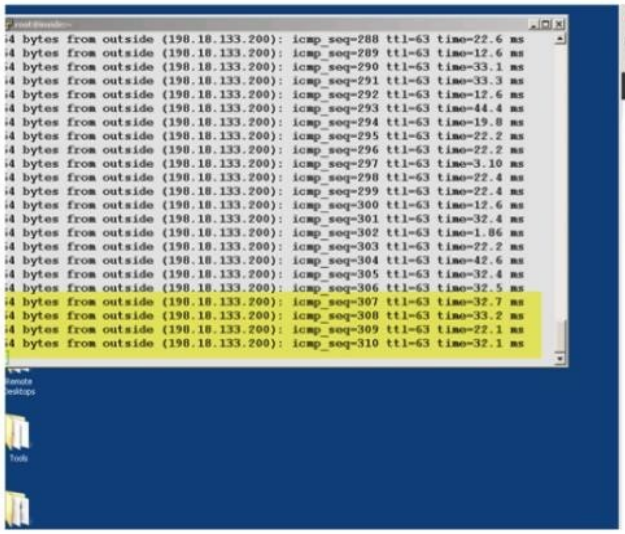


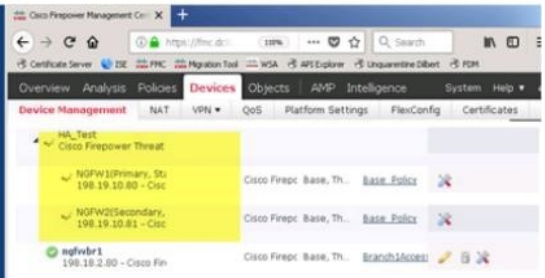
2. ユーザ名：**root**、パスワード：**C1sco12345** でログイン後、「ping outside」と入力し、スクリプトの実行を続行します。



3. FMC の Web インターフェイスで [デバイス(Devices)] > [デバイス管理(Device Management)] に移動し、[ピアをスイッチ(Switch Peers）] アイコンをクリックして、[はい（Yes）] をクリックします。

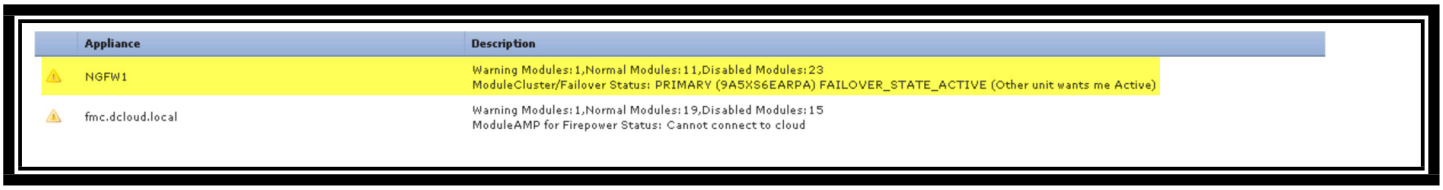
4. 内部 Linux サーバからの ping 結果も確認できるように、Firefox ウィンドウのサイズを変更します。






```
4 bytes from outside (198.18.133.200): icmp_seq=29 ttl=63 time=22.5 ms
4 bytes from outside (198.18.133.200): icmp_seq=30 ttl=63 time=32.6 ms
4 bytes from outside (198.18.133.200): icmp_seq=31 ttl=63 time=32.2 ms
4 bytes from outside (198.18.133.200): icmp_seq=32 ttl=63 time=12.3 ms
4 bytes from outside (198.18.133.200): icmp_seq=33 ttl=63 time=22.3 ms
4 bytes from outside (198.18.133.200): icmp_seq=34 ttl=63 time=20.8 ms
4 bytes from outside (198.18.133.200): icmp_seq=35 ttl=63 time=22.3 ms
4 bytes from outside (198.18.133.200): icmp_seq=36 ttl=63 time=24.0 ms
4 bytes from outside (198.18.133.200): icmp_seq=37 ttl=63 time=32.8 ms
4 bytes from outside (198.18.133.200): icmp_seq=38 ttl=63 time=44.1 ms
4 bytes from outside (198.18.133.200): icmp_seq=39 ttl=63 time=22.0 ms
4 bytes from outside (198.18.133.200): icmp_seq=40 ttl=63 time=22.4 ms
4 bytes from outside (198.18.133.200): icmp_seq=41 ttl=63 time=32.4 ms
4 bytes from outside (198.18.133.200): icmp_seq=42 ttl=63 time=22.4 ms
4 bytes from outside (198.18.133.200): icmp_seq=43 ttl=63 time=32.6 ms
4 bytes from outside (198.18.133.200): icmp_seq=49 ttl=63 time=32.5 ms
4 bytes from outside (198.18.133.200): icmp_seq=49 ttl=63 time=32.5 ms
4 bytes from outside (198.18.133.200): icmp_seq=50 ttl=63 time=32.6 ms
4 bytes from outside (198.18.133.200): icmp_seq=51 ttl=63 time=22.5 ms
4 bytes from outside (198.18.133.200): icmp_seq=52 ttl=63 time=22.3 ms
```

5. NGFW2 が現在アクティブになっていることを確認するには、「show running-config failover」を実行します。



Appliance	Description
NGFW1	Warning Modules:1,Normal Modules:11,Disabled Modules:23 ModuleCluster/Failover Status: PRIMARY (9A5XS6EARPA) FAILOVER_STATE_ACTIVE (Other unit wants me Active)
fmc.dcloud.local	Warning Modules:1,Normal Modules:19,Disabled Modules:15 ModuleAMP for Firepower Status: Cannot connect to cloud

注：NGFW1 が再度プライマリになるように切り替えます。

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。

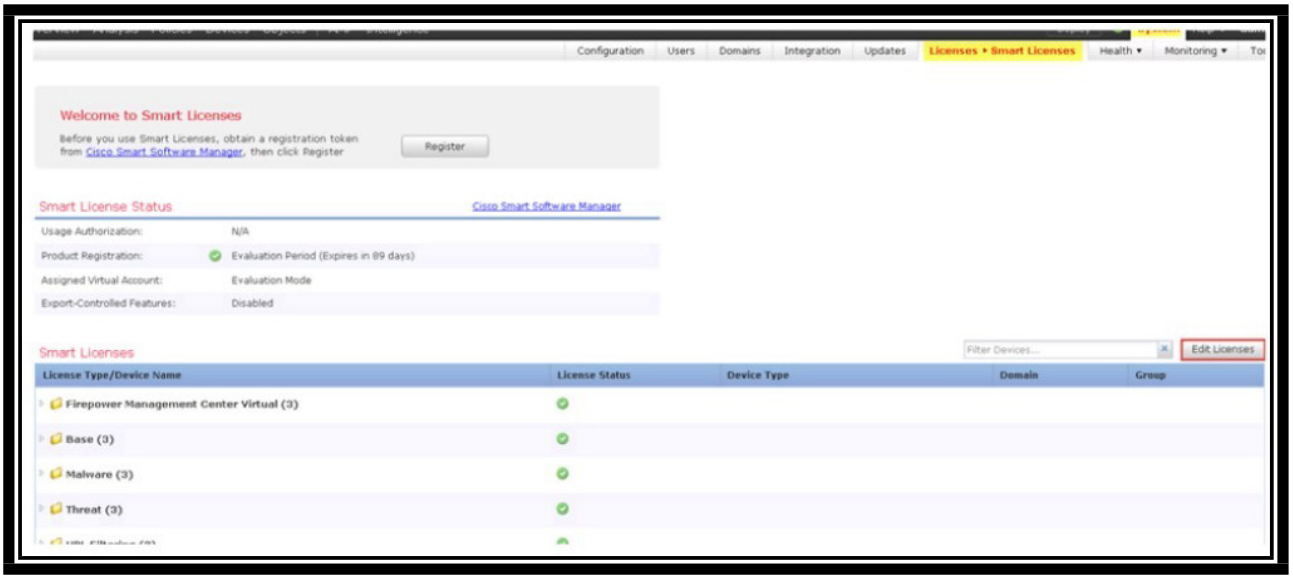
- AnyConnect スマート ライセンスを有効にする
- AnyConnect RA VPN オブジェクトを作成する
- デフォルトのグループ ポリシーを変更する
- RA VPN ウィザードを実行する
- デバイスの証明書を設定する
- アクセス コントロール ポリシーを変更して AnyConnect インバウンド アクセスを許可する
- NAT 適用除外を設定する
- NGFW RA VPN 設定を導入し確認する
- 設定をテストする

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

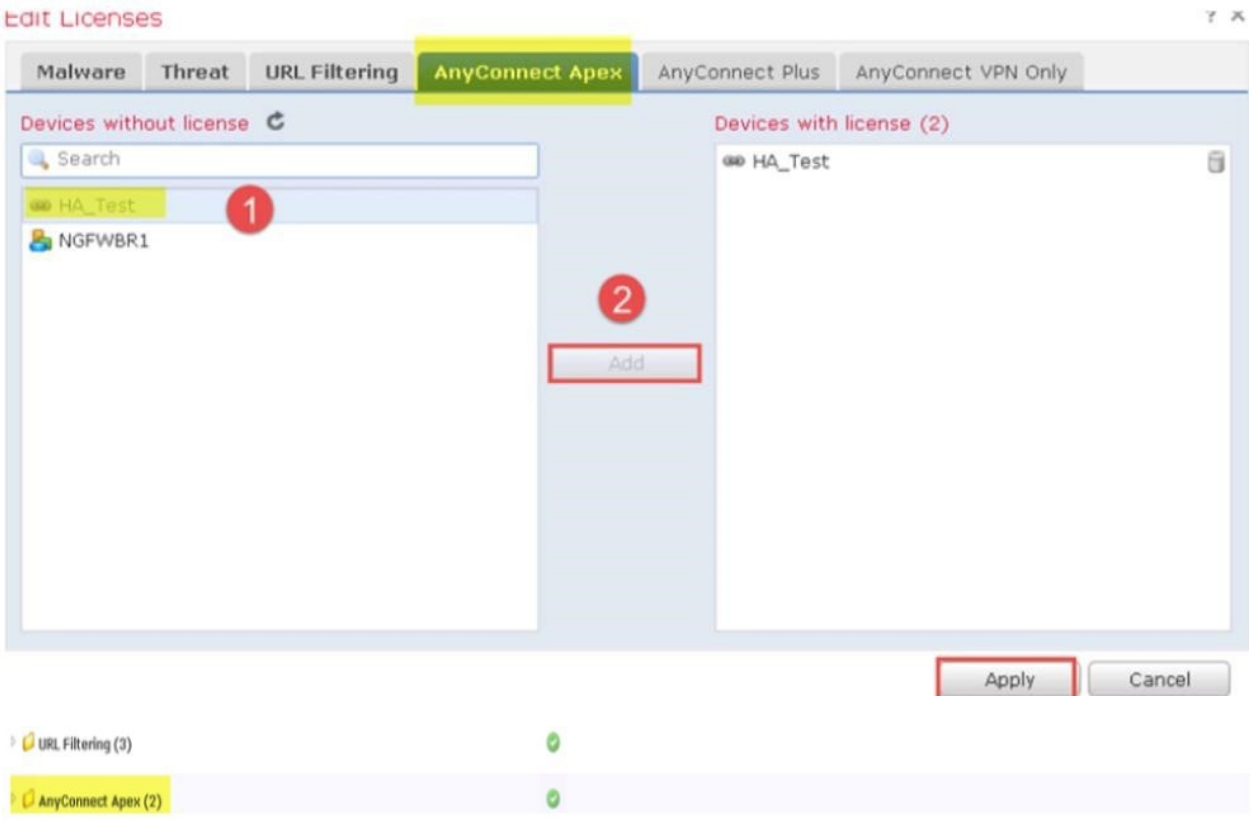
1. FMC で、[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] に移動します。



2. **[ライセンスの編集（Edit Licenses）] をクリックします。**

3. [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。

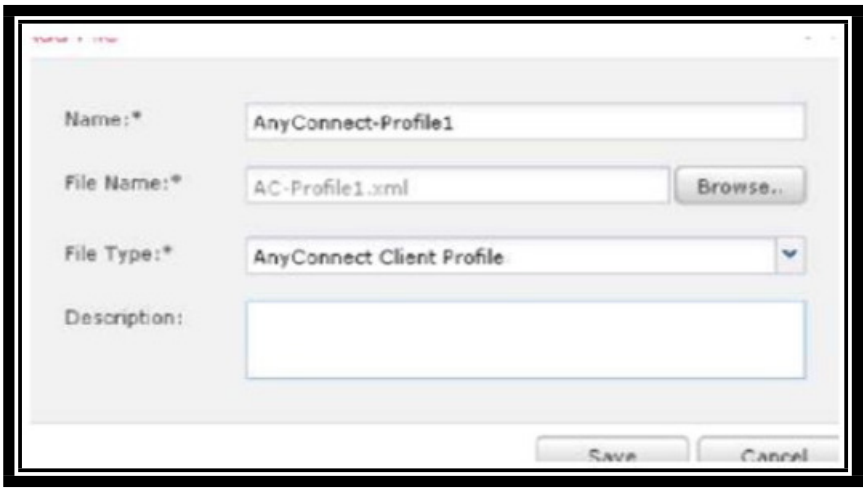
    a. **HA_Test** デバイスを選択します。[追加（Add）]、[適用（Apply）] の順にクリックします。



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. 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）]

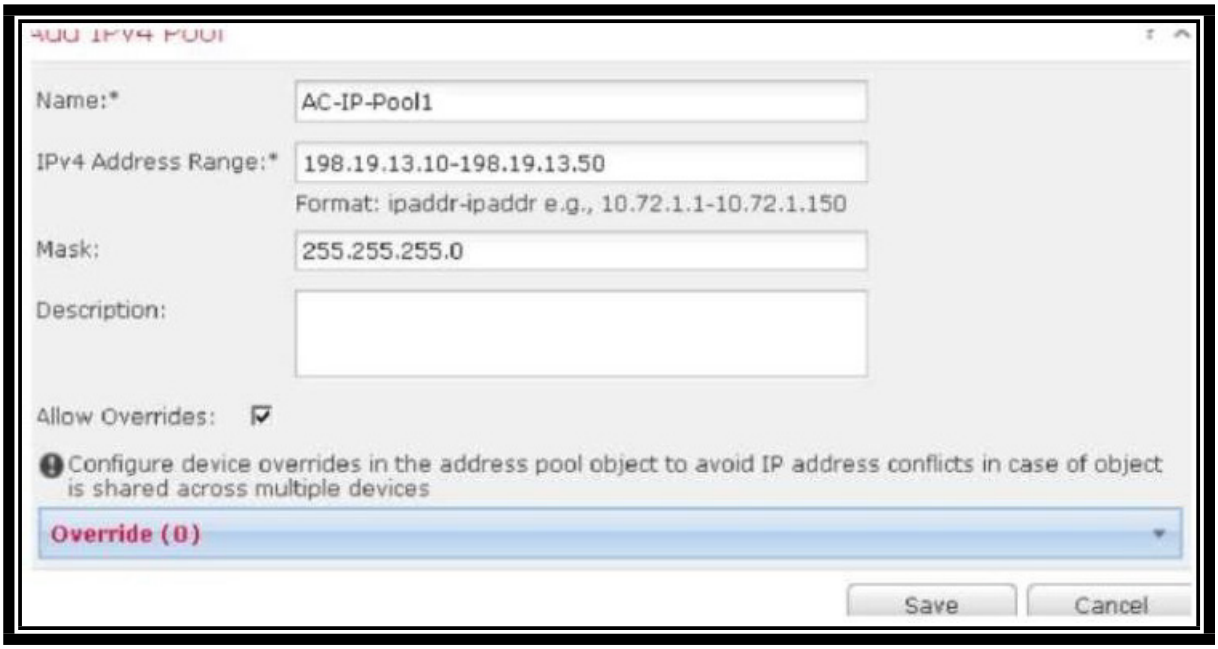
3. IP プールを作成します。
    a. FMC で、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレス プール（Address Pools）] > [IPv4 プール（IPv4 Pools）] に移動します。
    b. [IPv4プールの追加（Add IPv4 Pools）] をクリックします。

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。



4. 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。

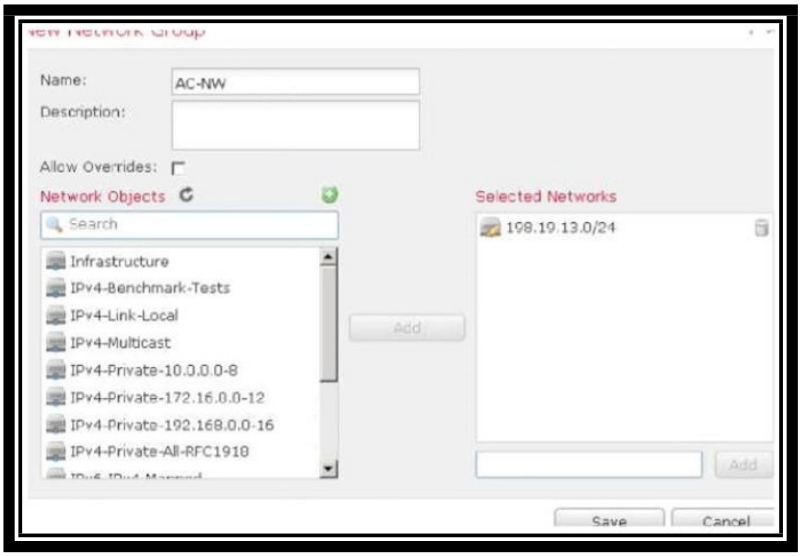
a. FMC で、[オブジェクト（Object）]> [オブジェクト管理（Object Management）] > [ネットワーク（Network）] に移動します。

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。

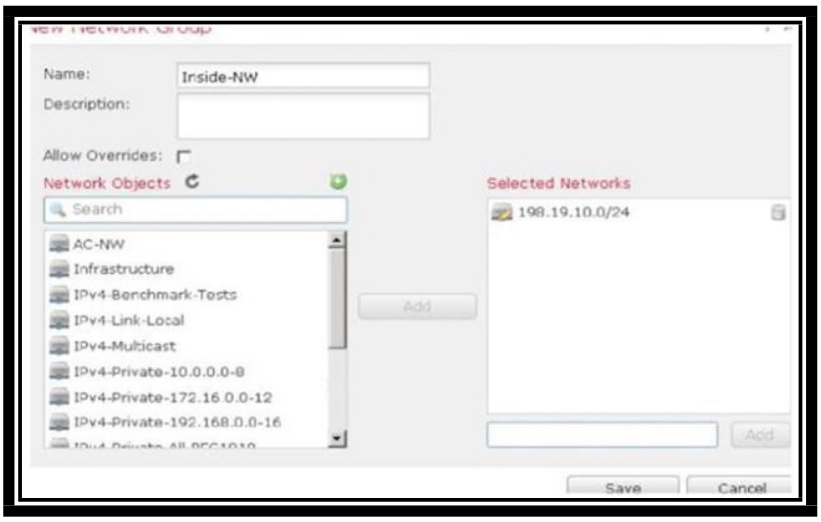
c. [名前（Name）] に「**AC-NW**」と入力します。

d. [選択したネットワーク（Selected Networks）] の下部にあるテキスト フィールドに「**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。



5. 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. [選択したネットワーク（Selected Networks）] の下部にあるテキスト フィールドに「**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。

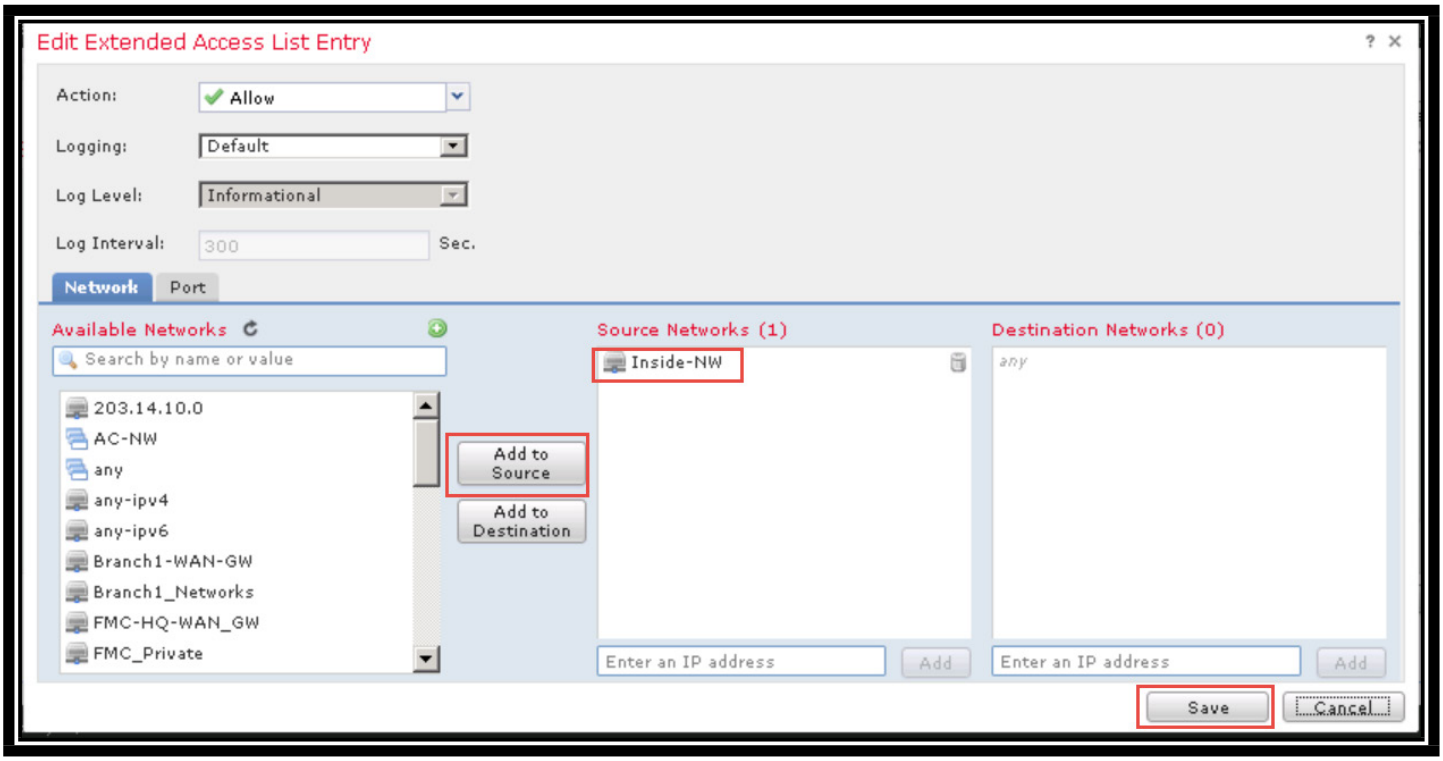
6. RA VPN スプリット トンネル設定用の ACL を作成します。
    a. FMC で、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アクセス リスト（Access List）] > [拡張（Extended）] に移動します。
    b. [拡張アクセスリストの追加（Add Extended Access List）] をクリックします。

c. [名前（Name）] に「AC-SplitTunnel1」と入力します。[追加（Add）] をクリックします。

d. [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。

e. [追加（Add）] をクリックします。

f. [保存（Save）] をクリックします。



7. 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。

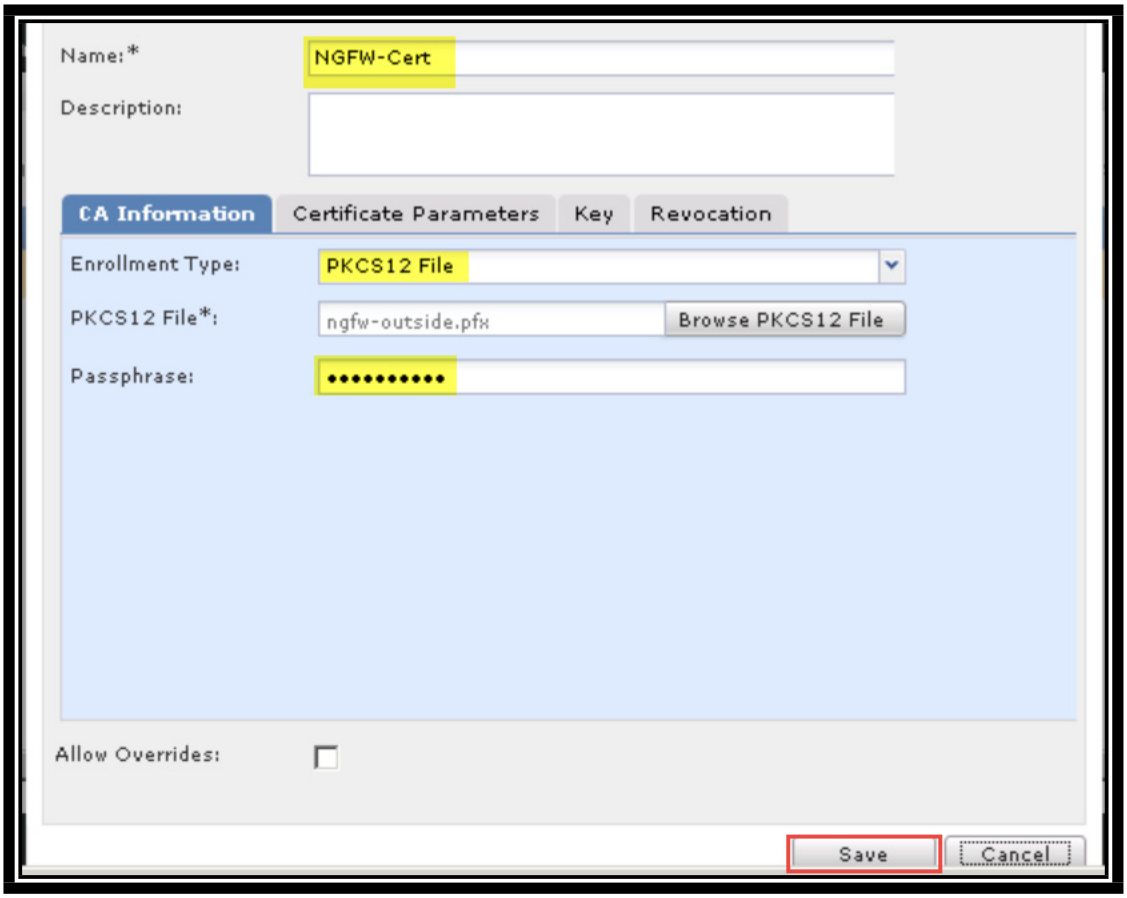
c. [名前（Name）] に「**NGFW-Cert**」と入力します。

d. [登録タイプ（Enrollment Type）] で、[PKCS12ファイル（PKCS12 File）] を選択します。

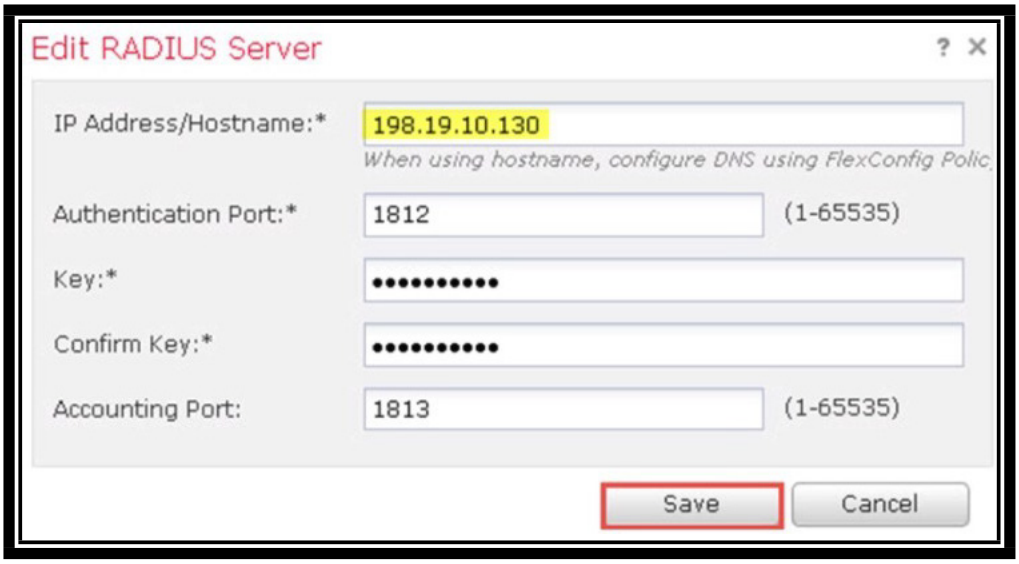
e. Jumpbox Desktop で **Certificates** フォルダを開き、**ngfw -outside** 証明書を選択して [開く（Open）] をクリックします。

f. パスフレーズに「**C1sco12345**」と入力します。

g. [保存（Save）] をクリックします。



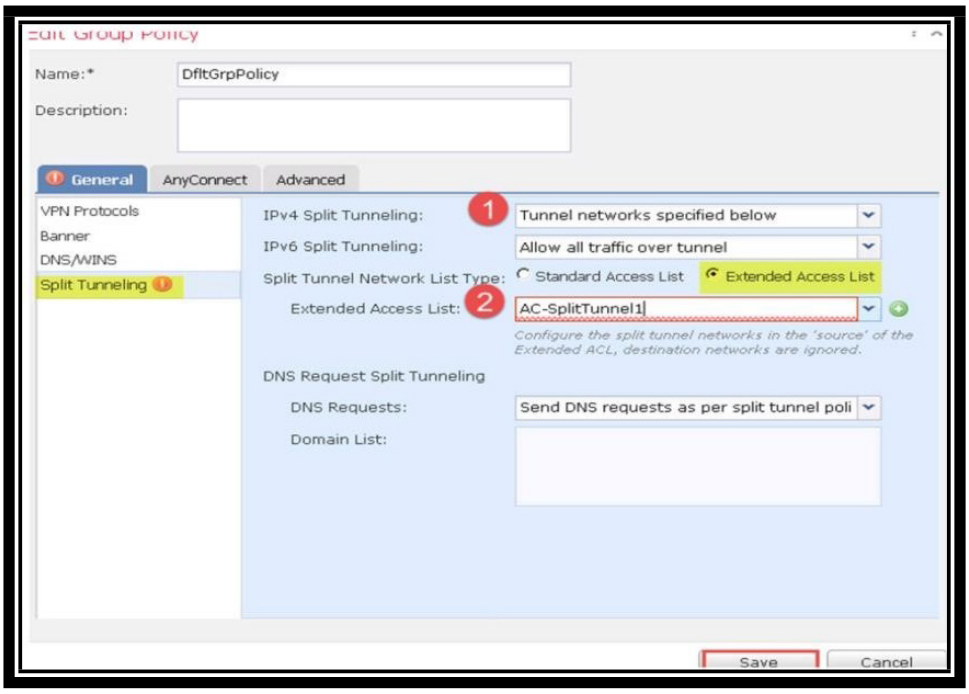
8. ISE RADIUS サーバ用のオブジェクトを作成します。
    a. FMC で、[オブジェクト（Object）] > [オブジェクト管理（Object Management）] > [RADIUSサーバグループ（RADIUS Server Group）] に移動します。
    b. [RADIUSサーバグループの追加（Add RADIUS Server Group）] をクリックします。
    c. [名前（Name）] に「**ISE-AAA**」と入力します。
    d. [RADIUSサーバ（RADIUS Servers）] セクションの [+] アイコンをクリックします。
    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。



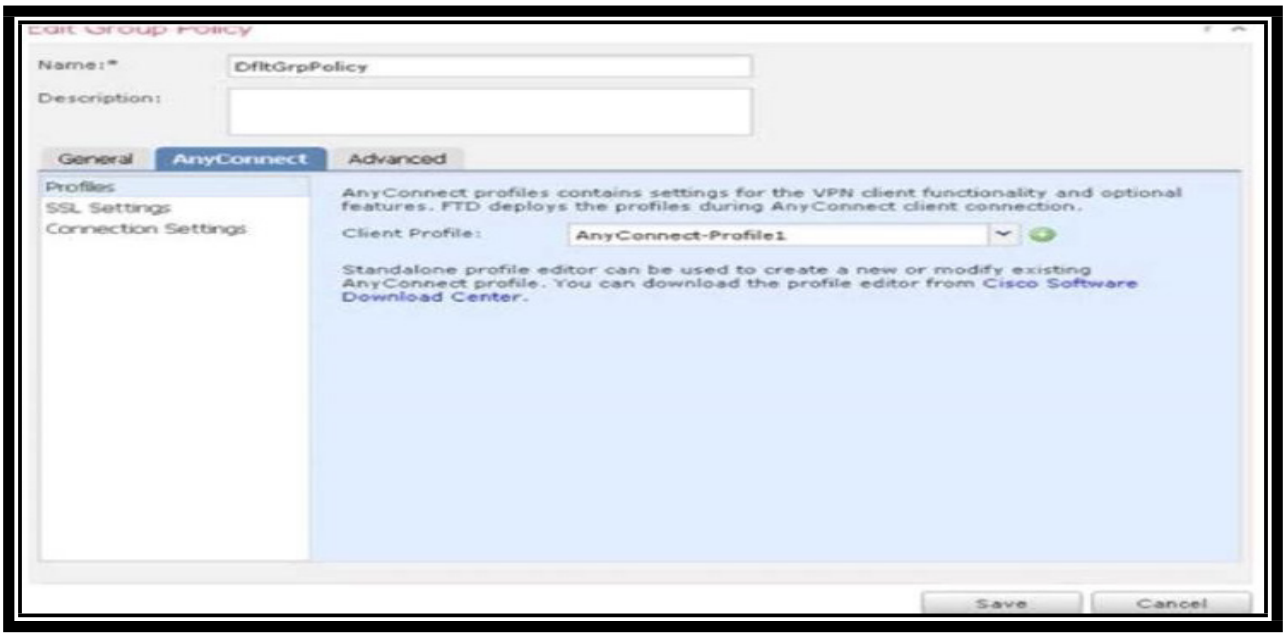
注：時間を節約するために、ISE では、ラボ演習で必要な設定が事前にすべて設定されています。ISE 設定を確認する場合は、付録 3 を参照してください。

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。
    a. [DfltGrpPolicy] を選択して編集します。
    b. [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。**
    c. [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。
    d. [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。
    e. [アクセスリスト（Access List）] **で、**[AC-SplitTunnel1] **を選択します。**



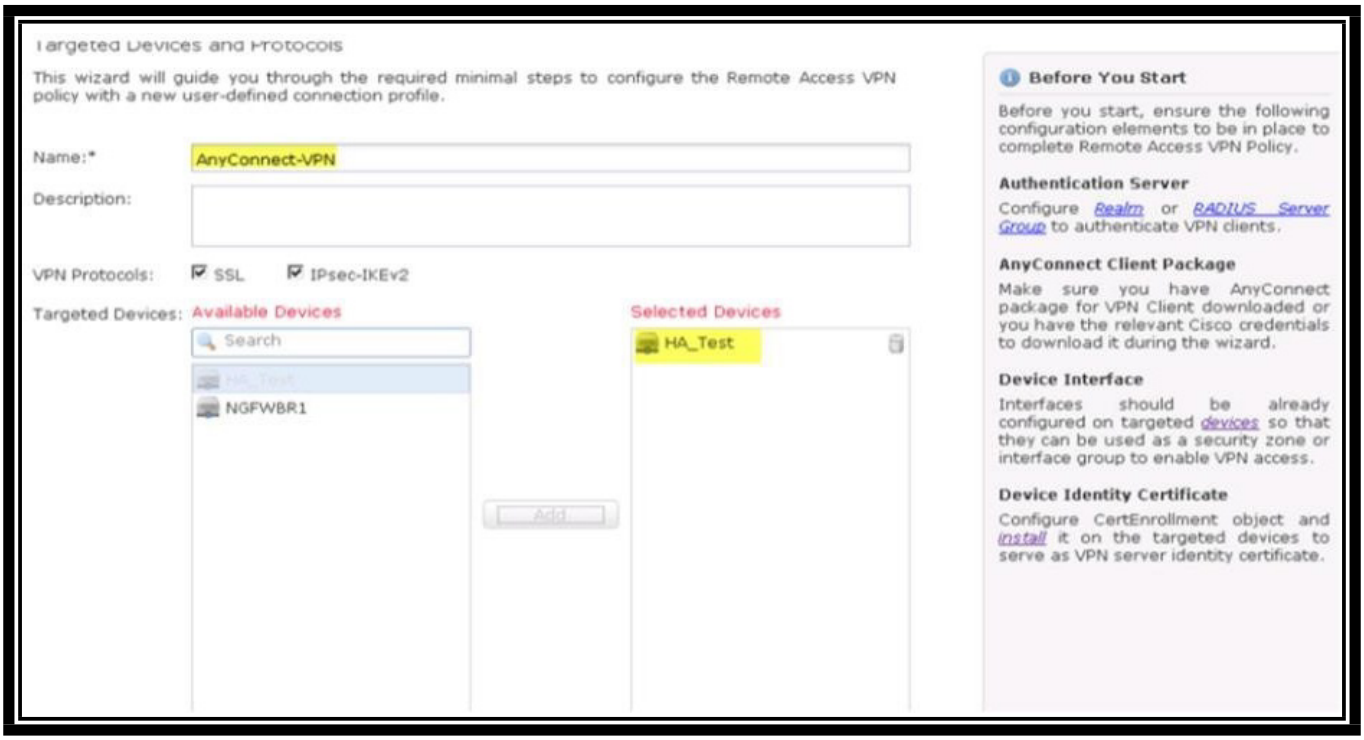
2. [全般（General）] タブで、[DNS/WINS] を選択します。
    a. [プライマリDNSサーバ（Primary DNS Server）] で [+] アイコンをクリックします。
    b. [名前（Name）] に「Inside-DNS」と入力します。
    c. [ネットワーク (Network)] で **[ホスト（Host）] オプション ボタンを選択します。**
    d. [ネットワーク（Network）] に「198.19.10.100」と入力します。
    e. [保存（Save）] をクリックします。
3. [AnyConnect] タブを選択し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



4. [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。

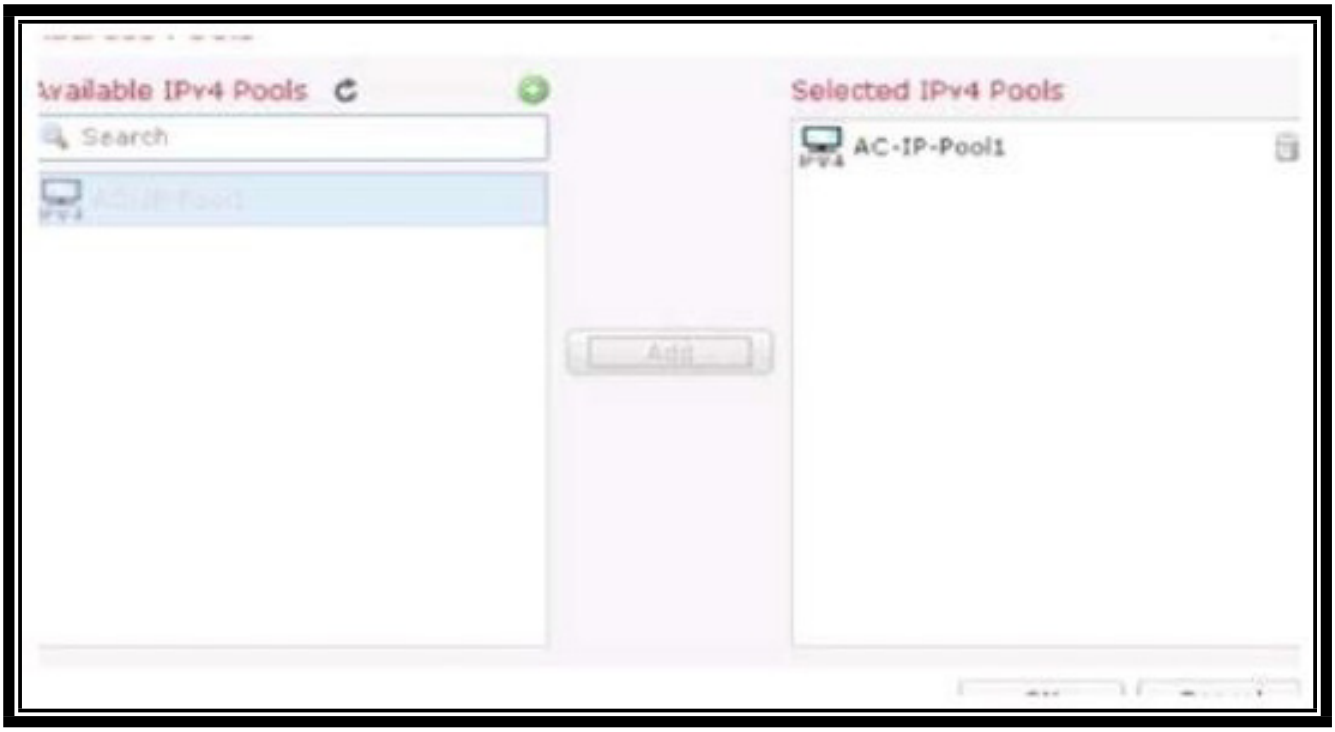
RA VPN ウィザードを実行する

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。
    a. 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。
    b. [名前（Name）] に「AnyConnect-VPN」と入力します。
    c. [ターゲットデバイス（Target Device）] から [HA_Test] を選択します。[追加（Add）] をクリックします。
    d. [次へ（Next）] をクリックします。

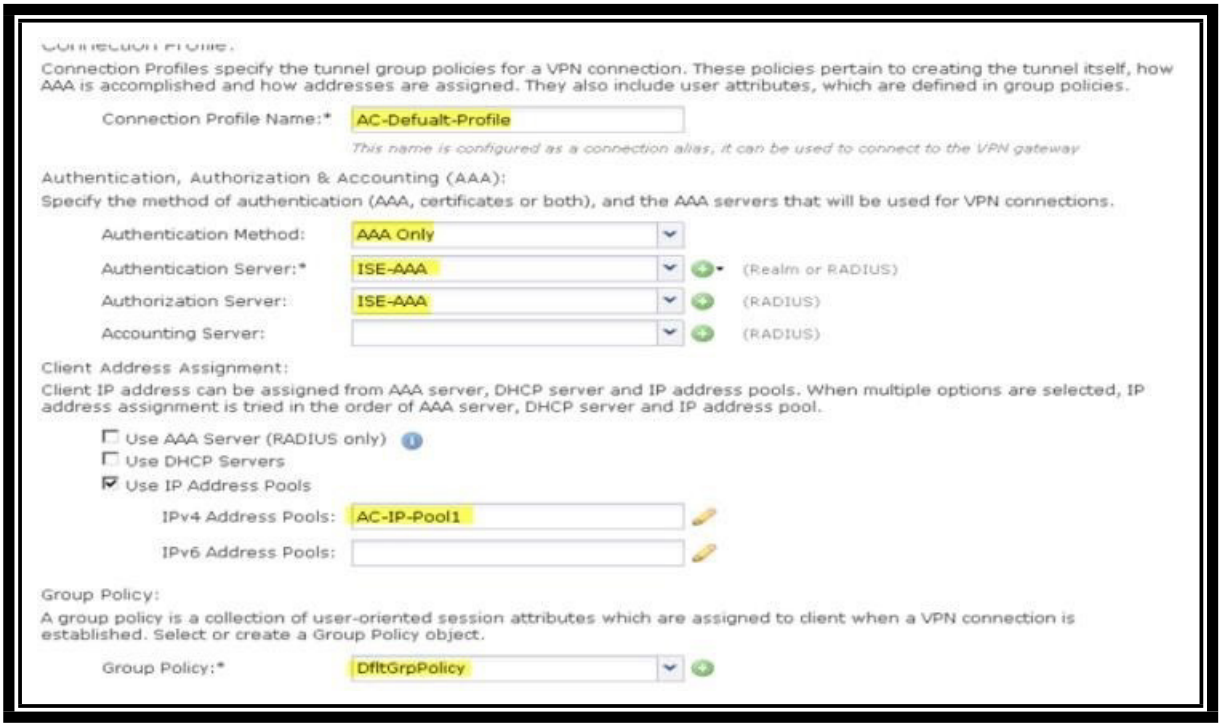


2. ウィザードの [接続プロファイル（Connection Profile）] ページに入力します。
    a. [接続プロファイル名（Connection Profile Name）] に「AC-Default-Profile」と入力します。
    b. [認証方式（Authentication Method）] で [AAAのみ（AAA Only）] が選択されていることを確認します。
    c. [認証サーバ（Authentication Server）] で [ISE-AAA] を選択します。
    d. [IPアドレスプールを使用する（Use IP Address Pools）] の [IPv4アドレスプール（IPv4 Address Pools）] で [AC-IP-Pool1] を選択します。

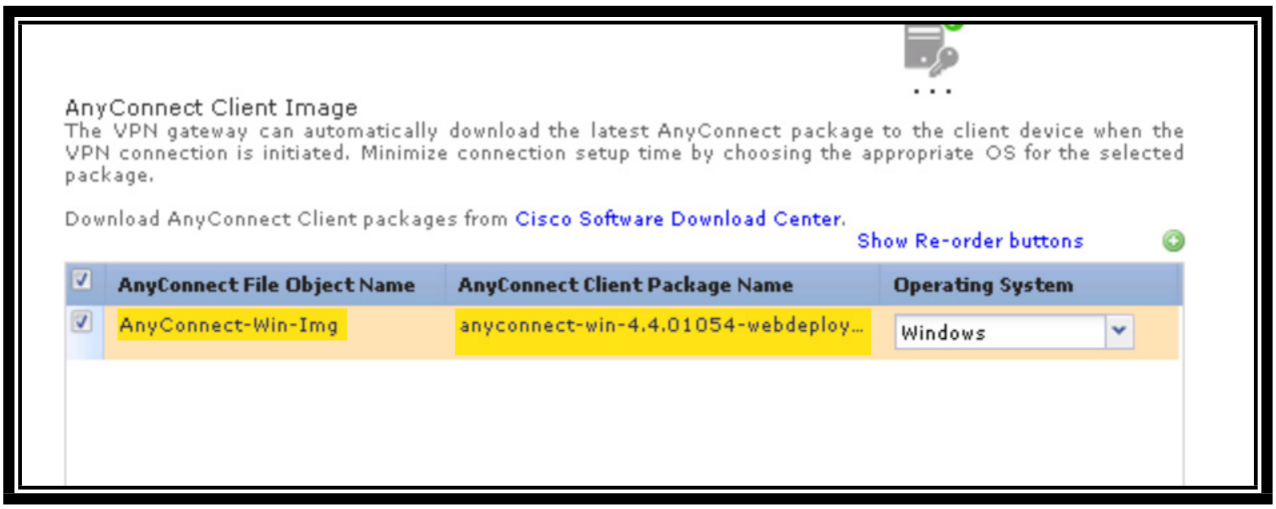
3. **[アドレスプール（Address Pools）] で、[IPv4アドレスプール（IPv4 Address Pools）] を編集します。**
4. **[IPv4アドレスプール（IPv4 Address Pools）] から [AC-IP Pool1] を選択します。**
5. **[追加（Add）] をクリックし、次に [OK] をクリックします。**



6. [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。
リモート アクセス VPN ポリシー ウィザード



7. 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。



8. 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。**

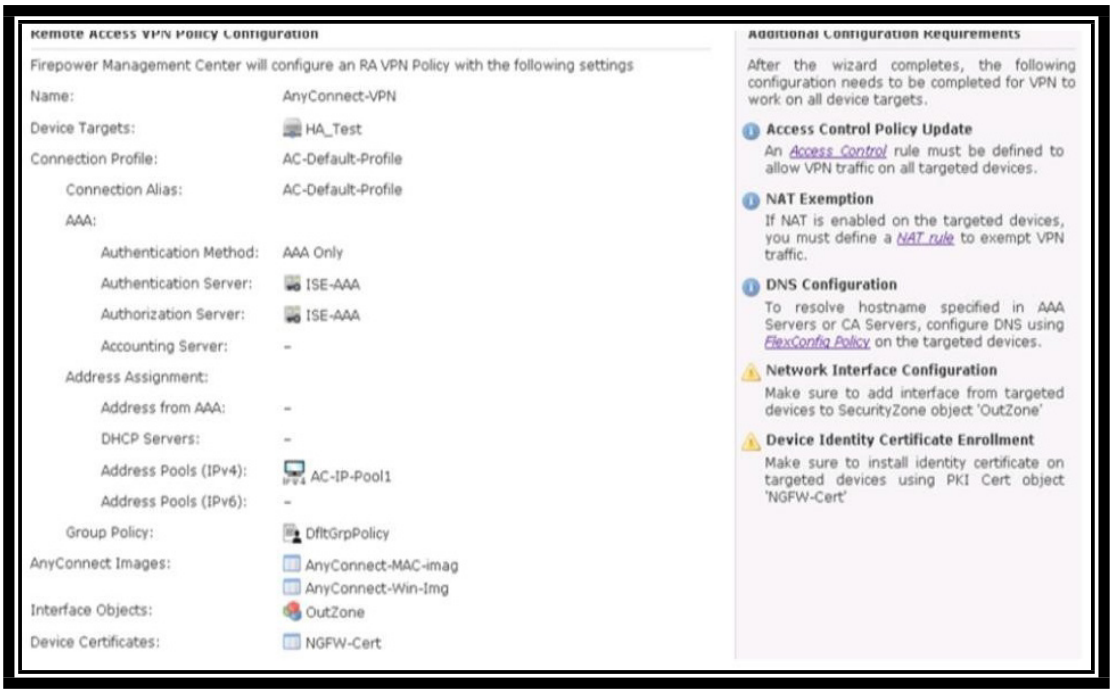
b. **[**証明書の登録（Certificate Enrollment）**] で、[**NGFW-Cert**] を選択します。**

c. [次へ（Next）] をクリックします。

9. ウィザードの [サマリー（Summary）] ページを確認します。

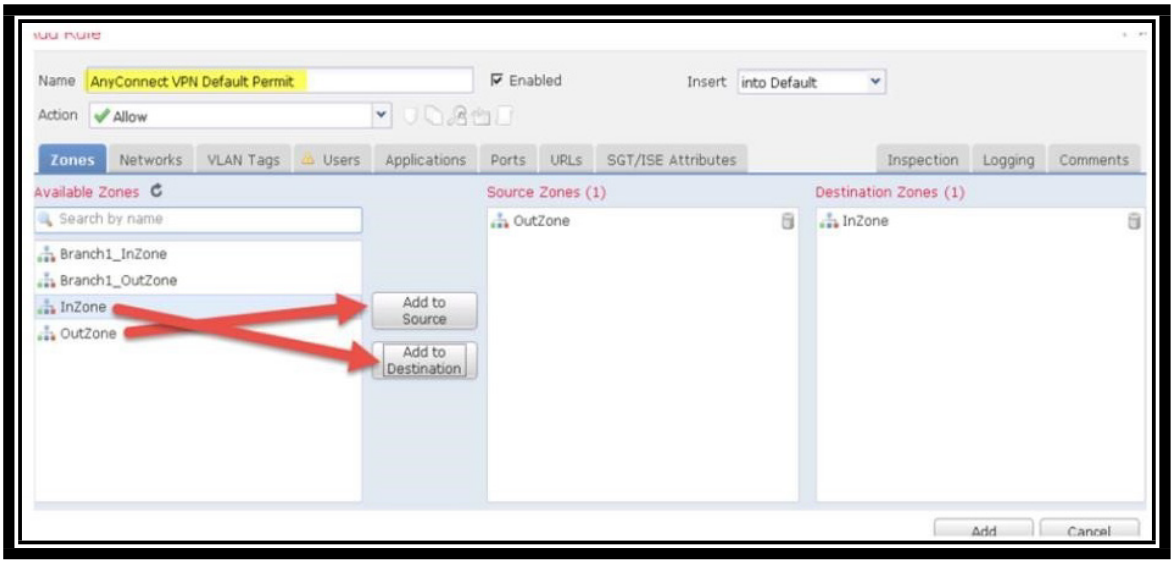
a. このページに表示される設定を確認します。

b. [完了（Finish）] をクリックします。

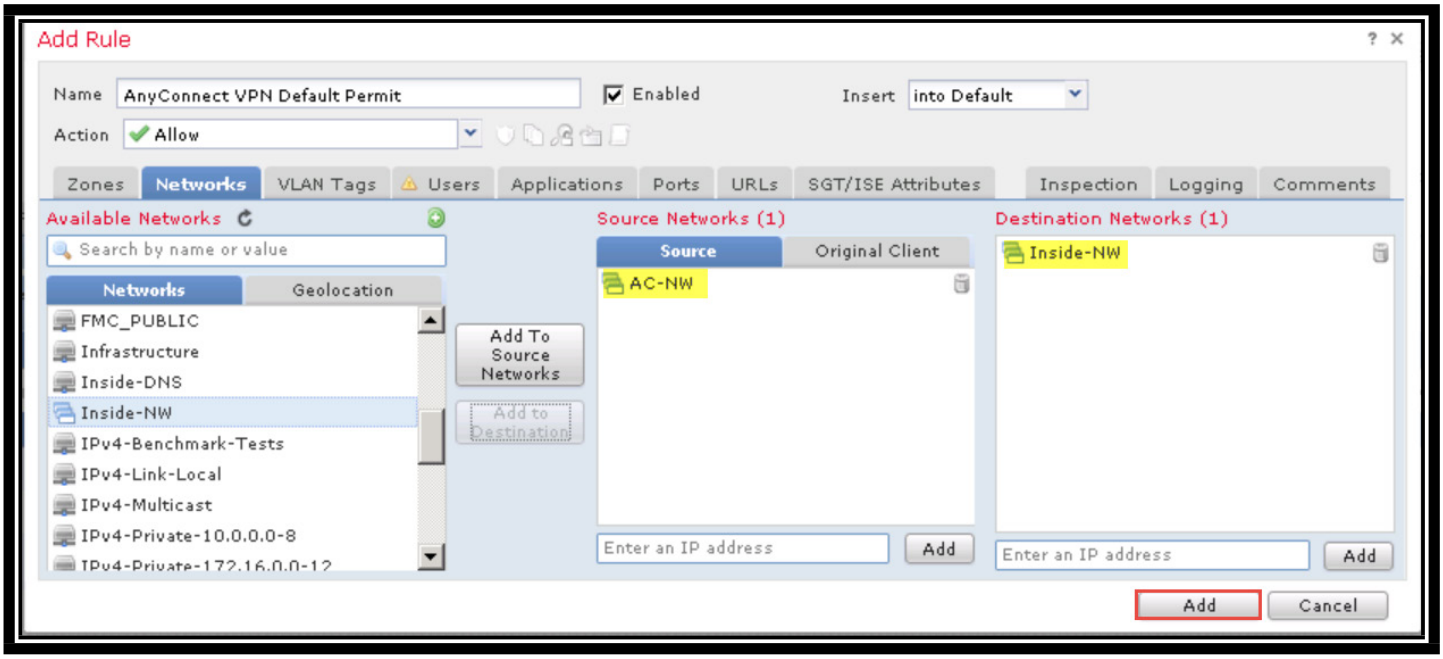


アクセス コントロール ポリシーを変更して AnyConnect インバウンド アクセスを許可する

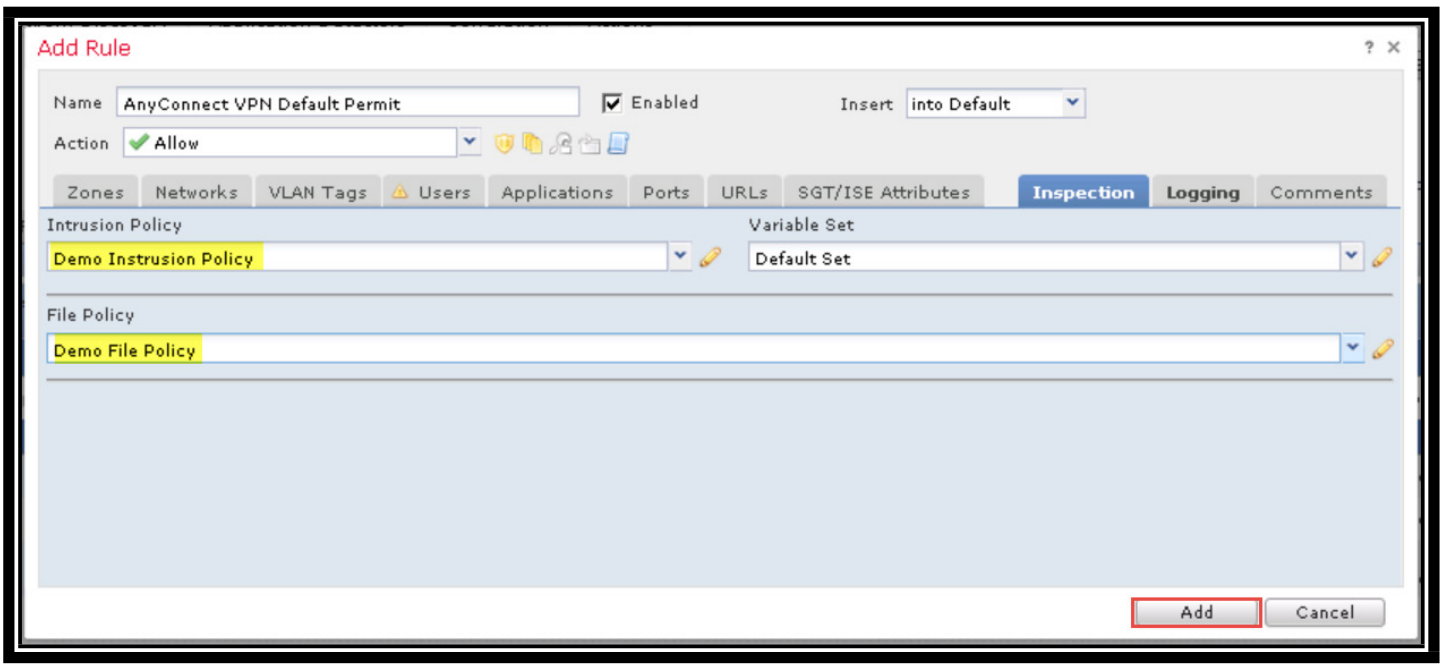
1. FMC で、[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [アクセスコントロール（Access Control）] の順に選択します。
2. アクセス コントロール ポリシー（**Base_Policy**）を選択して編集します。[ルールの追加（Add Rule）] をクリックします。
    a. [名前（Name）] に「**AnyConnect VPN Default Permit**」と入力します。
    b. [挿入（Insert）] ドロップダウン リストから [デフォルトに挿入（into Default）] を選択します。
    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。



3. [ネットワーク（Networks）] タブを選択します。
    a. [AC-NW] を選択し、[送信元に追加（Add to Source）] をクリックします。
    b. [Inside-NW] を選択し、[宛先に追加（Add to Destination）] をクリックします。



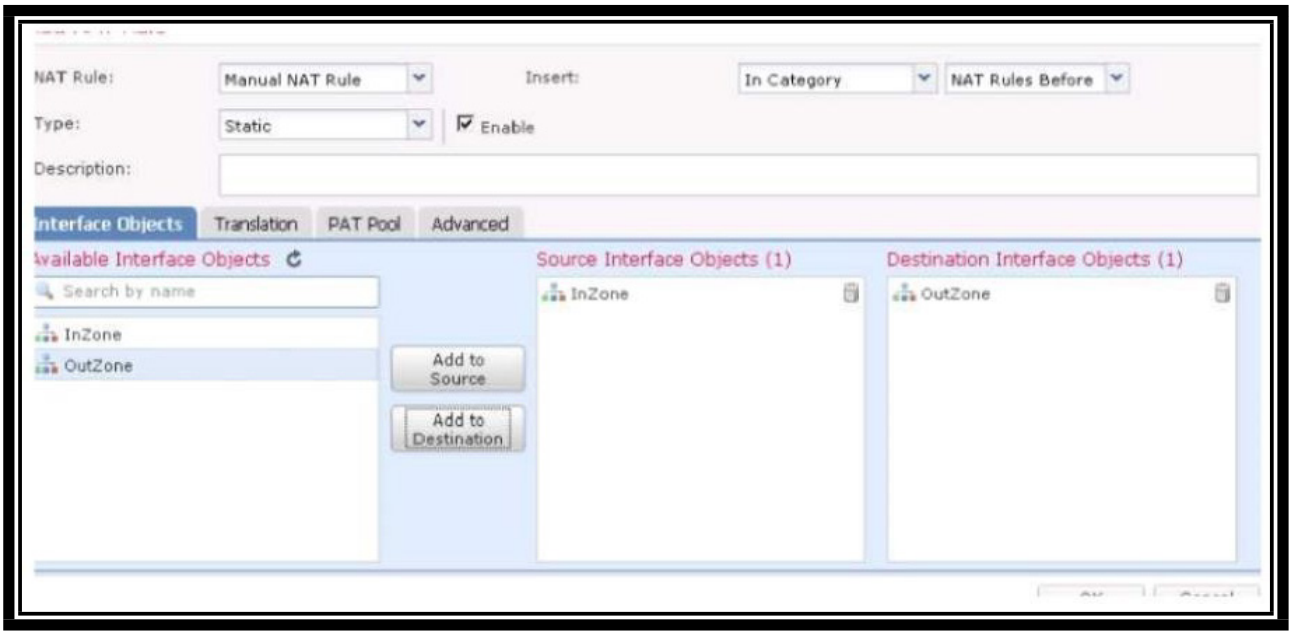
4. [インスペクション（Inspection）] タブを選択します。
    a. [侵入ポリシー（Intrusion Policy）] ドロップダウン リストから [デモ侵入ポリシー（Demo Intrusion Policy）] を選択します。
    b. [ファイル ポリシー（File Policy）] ドロップダウン リストから [デモ ファイル ポリシー（Demo File Policy）] を選択します。
    c. [追加（Add）] をクリックしてルールを追加します。
    d. [保存（Save）] をクリックして、アクセス コントロール ポリシーの変更を保存します。



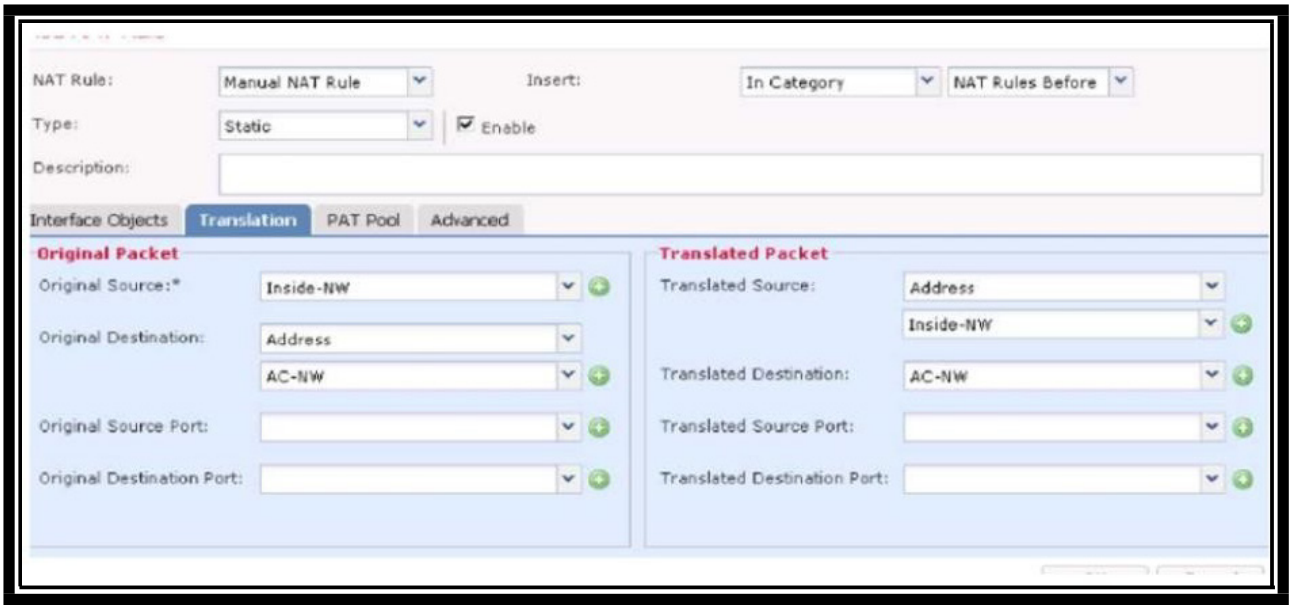
NAT 適用除外を設定する

注：NAT 適用除外は、VPN 接続で使用される IP アドレスが NAT によって変換されないようにするものです。ネットワークが変換されないように、このルールは、[処理前のNATルール（NAT Rules Before）] カテゴリ含める必要があります。

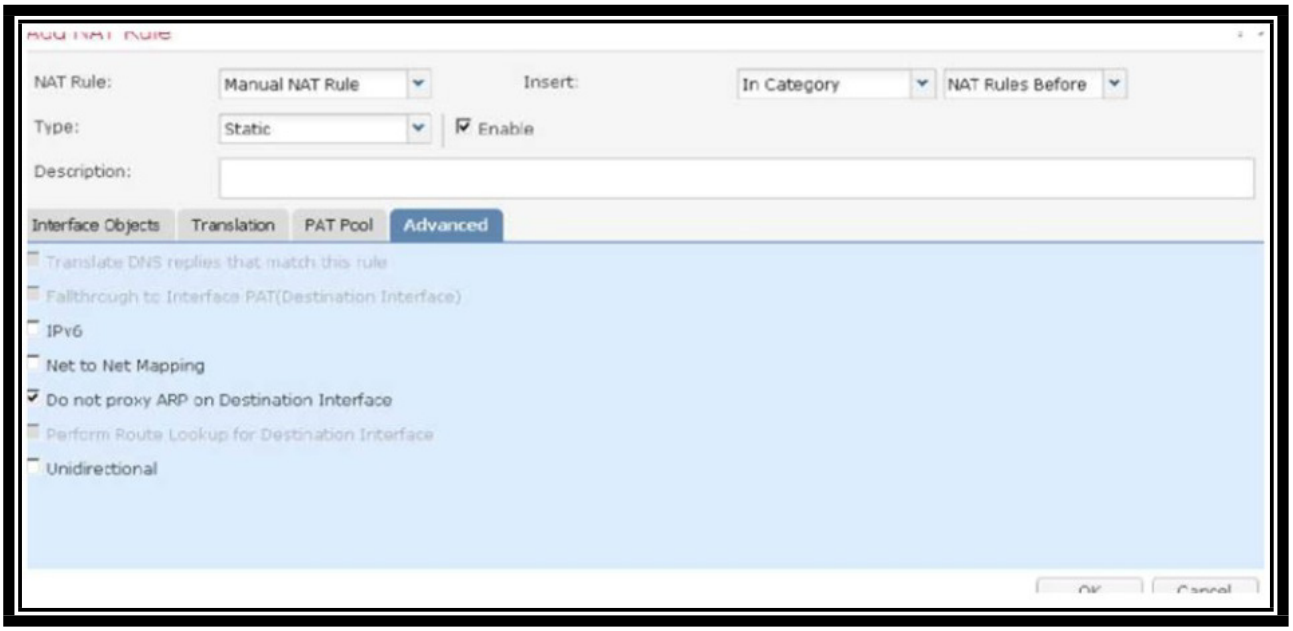
1. FMC で、[デバイス（Devices）] > [NAT] に移動します。
2. 既存の NAT ポリシー（**Default PAT**）を選択して編集します。[ルールの追加（Add Rule）] をクリックします。
    a. [インターフェイス オブジェクト（Interface Objects）] タブが表示されます。
    b. [InZone] を選択し、[送信元に追加（Add to Source）] をクリックします。
    c. [OutZone] を選択し、[宛先に追加（Add to Destination）] をクリックします。



3. [変換（Translation）] タブを選択します。
4. [元の送信元（Original Source）] で、[Inside-NW] を選択します。
5. [元の宛先（Original Destination）] で、[AC-NW] を選択します。
6. [変換後の送信元（Translated Source）] で、[Inside-NW] を選択します。
7. [変換後の宛先（Translated Destination）] で、[AC-NW] を選択します。



8. [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）] 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。

9. [OK] をクリックして NAT ルールを保存します。

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

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。
2. FMC で、[導入（Deploy）] ボタンをクリックします。
3. [HA_Test] を選択し、[導入（Deploy）] をクリックします。
4. 導入が完了するまで待ちます。
5. **NGFW1** 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**

```
> show running-config tunnel-group
tunnel-group AC-Default-Profile type remote-access
tunnel-group AC-Default-Profile general-attributes
 address-pool AC-IP-Pool1
 authentication-server-group ISE-AAA
tunnel-group AC-Default-Profile webvpn-attributes
 group-alias AC-Default-Profile enable
>
```

    b. **show running-config group-policy**

```
> show running-config group-policy
group-policy DfltGrpPolicy attributes
 dns-server value 198.19.10.100
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value AC-SplitTunnel1
 user-authentication-idle-timeout none
 webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
  anyconnect profiles value AnyConnect-Profile1 type user
  anyconnect ask none default anyconnect
  http-comp none
  activex-relay disable
  file-entry disable
  file-browsing disable
  url-entry disable
  deny-message none
>
```

    c. **show running-config crypto**
        i. crypto trustpoint が **NGFW-Cert** であることを確認します。
    d. **show running-config ip local pool**

```
> show running-config ip local pool
ip local pool AC-IP-Pool1 198.19.13.10-198.19.13.50 mask 255.255.255.0
>
```

e. **show running-config nat**

```
> show running-config nat
nat (LAN-Side,ISP-Side) source static Inside-NW Inside-NW destination static AC-NW AC-NW no-proxy-arp
!
object network FMC_Private
 nat (LAN-Side,ISP-Side) static FMC_PUBLIC
object network wwwin
 nat (LAN-Side,ISP-Side) static wwwout
!
nat (LAN-Side,ISP-Side) after-auto source dynamic any interface
>
```

6. NGFW1 CLI で次のコマンドを実行して、AAA をテストします。

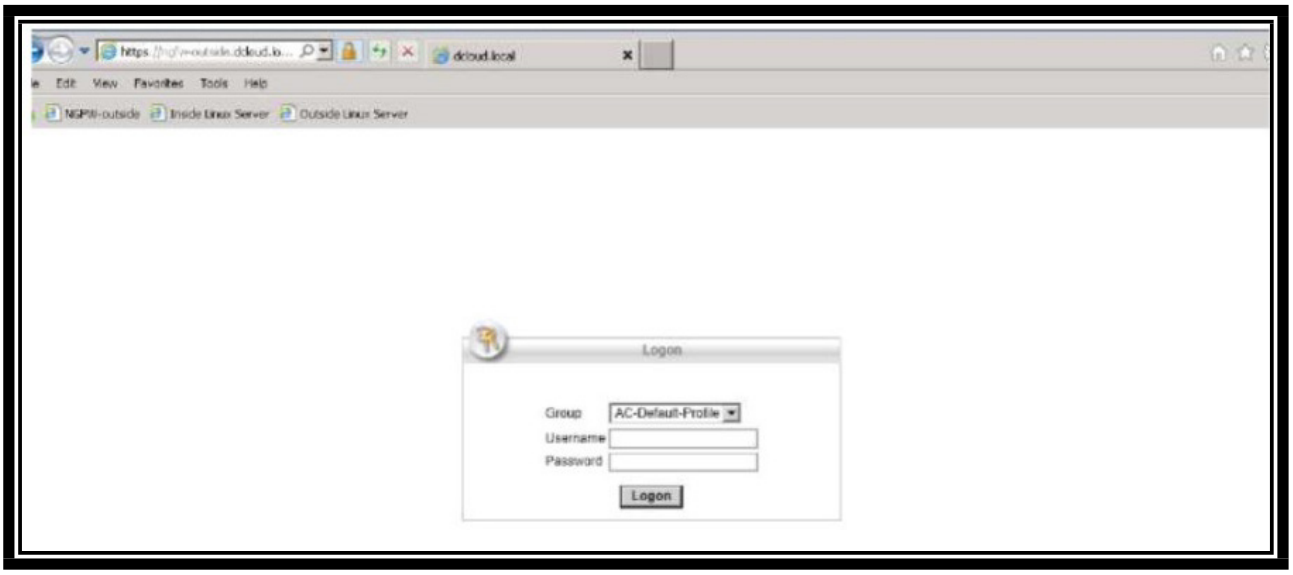
```
test aaa-server authentication ISE-AAA host 198.19.10.130 username ira password C1sco12345
```

7. 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。

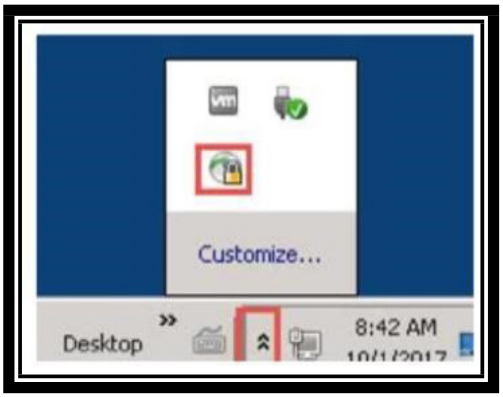
```
test aaa-server authentication ISE-AAA host 198.19.10.130 username ira password C1sco12345
IHFO: Attempting Authentication test to IE address (198.19.10.130) (timeout: 32 seconds) IHFO:
Authentication Successful
```

設定をテストする

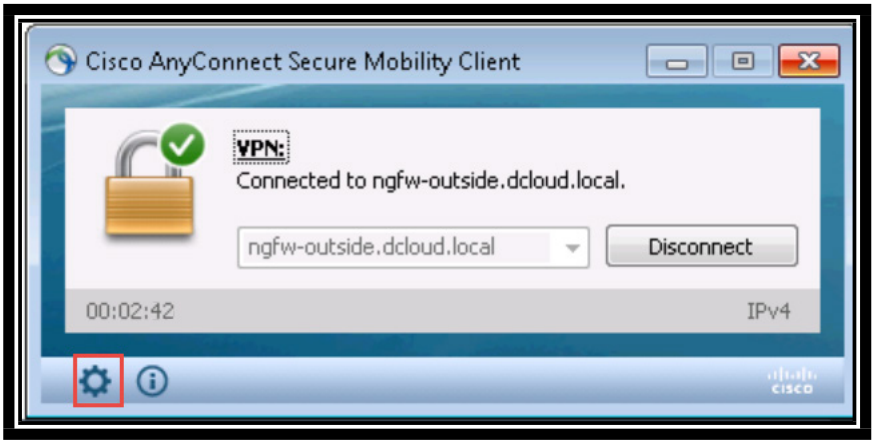
1. Jump Desktop の **Remote Desktop** フォルダを開き、**Outside-PC** をダブルクリックします。
2. ユーザ名：**Administrator**、パスワード：**C1sco12345** でログインします。
3. **Internet Explorer** を開き、お気に入りバーの **https://ngfw-outside.dcloud.local** をクリックします。（プロンプトが表示された場合は [続行（Continue）] をクリックして Web サイトに移動）。



4. [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、[ログオン（Logon）] をクリックします。
5. プロンプトが表示されたら、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。
6. インストールが完了すると、AnyConnect が自動的に接続されます。
7. 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。



8. 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。



9. [統計（Statistics）] タブを選択し、クライアントとサーバ IP アドレスを確認します。
10. [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。
11. NGFW CLI で次のコマンド

```
show vpn-sessiondb detail anyconnect on the NGFW1 CLI.
```

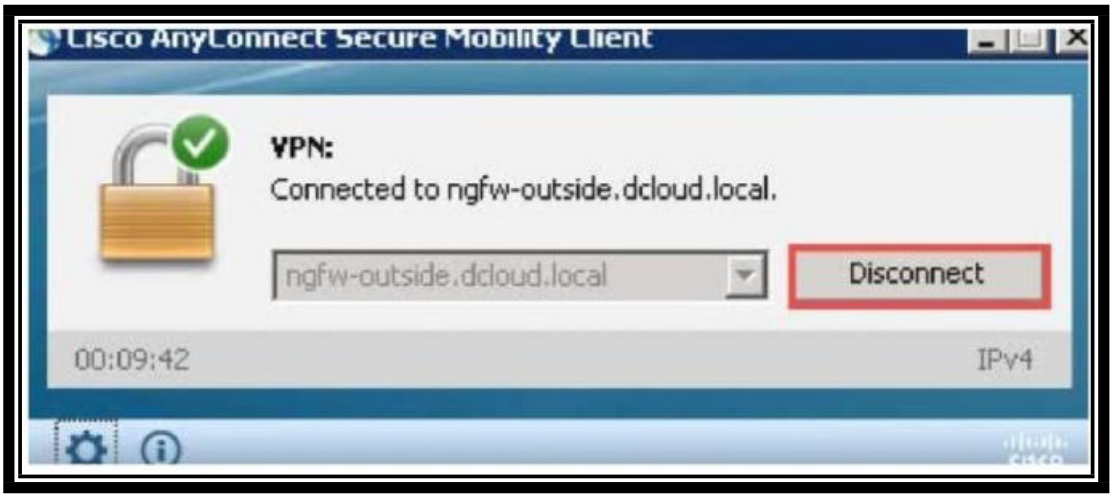
```
Session Type: AnyConnect

Username     : ira                    Index        : 23932
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)SHA1
Bytes Tx     : 122942                 Bytes Rx     : 19481
Group Policy : DfltGrpPolicy          Tunnel Group : AC-Default-Profile
Login Time   : 22:59:44 UTC Wed Dec 27 2017
Duration     : 0h:02m:34s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0000000005d7c0005a4425e0
Security Grp : none                   Tunnel Zone  : 0
>
```

12. 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. 「**ftp inside.dcloud.local**」コマンドを実行します。
    c. ユーザ名：**guest**、パスワード：**C1sco12345** でログインして内部サーバへのアクセスを確認します。
    d. **cd ~root** と入力します。次のメッセージが表示されます：`Connection closed by remote host`（リモート ホストによって接続がクローズされました）。これで、侵入防御が機能していることを確認できます。
13. 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。
14. [ファイル（Files）] リンクをクリックします。
15. **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。
16. **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。

注：Zombies.pdf が Firefox ブラウザからダウンロードされる場合は、Firefox ブラウザを閉じます。その後で再度、Internet Explorer から Zombies.pdf のダウンロードを試してください。

17. FMC で、[分析（Analysis）] > [侵入（Intrusions）]> [イベント（Events）] に移動します。
18. Snort ルール 336 がトリガーされていることを確認します。
19. [イベントのテーブル ビュー（Table 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。
20. 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。
21. **Zombies.pdf** がブロックされることを確認します。

22. [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、受信アドレスが VPN プールのものであることを確認します。
23. **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。

この演習の目的は次のとおりです。

- 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（198.19.10/24）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ることを確認する。
- 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ることを確認する。

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。

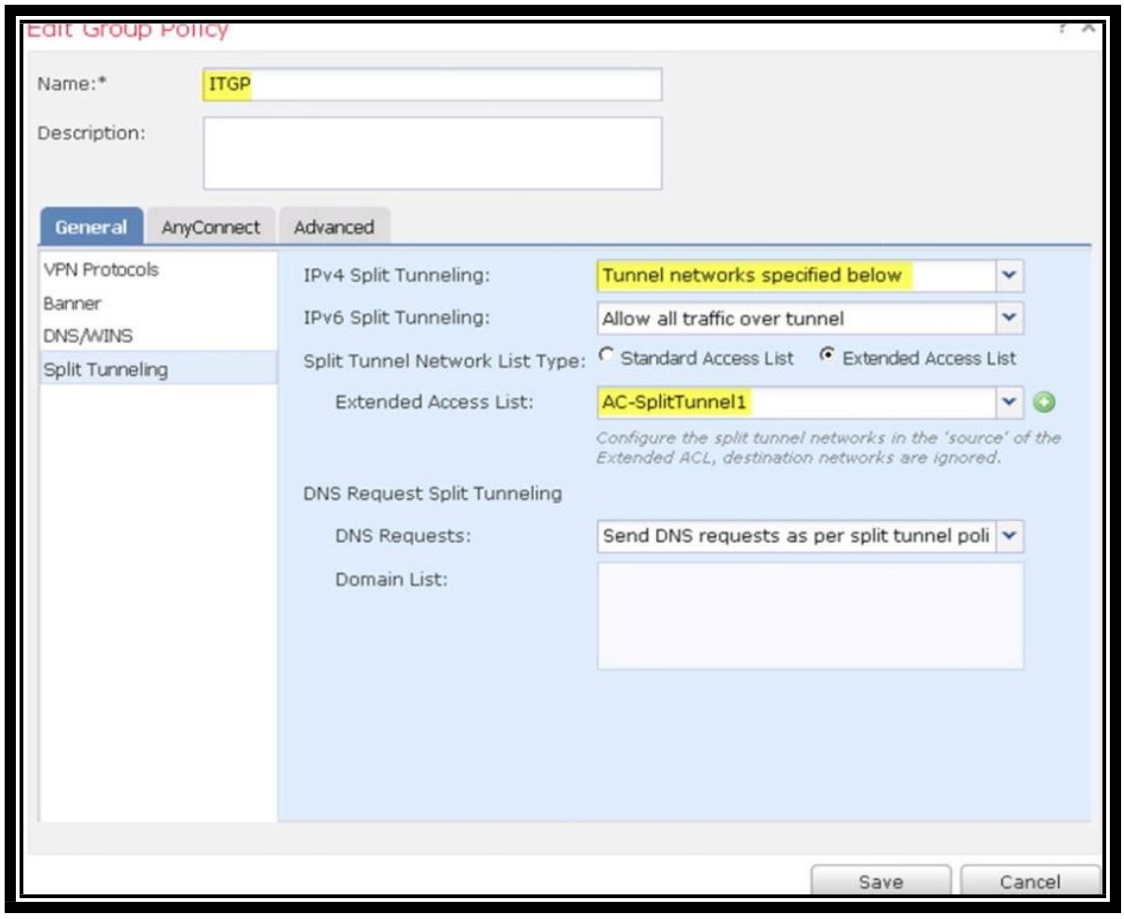
注：時間を節約するために、ISE では、ラボ演習で必要な設定が事前にすべて設定されています。そこでは、AD グループのメンバーシップに基づいて選択した、グループ ポリシーと IP プールも設定されています。**そのため、新しいグループ ポリシーと IP プールの名前は、手順に示す名前と正確に一致している必要があります。**ISE 設定を確認する場合は、付録 3 を参照してください。

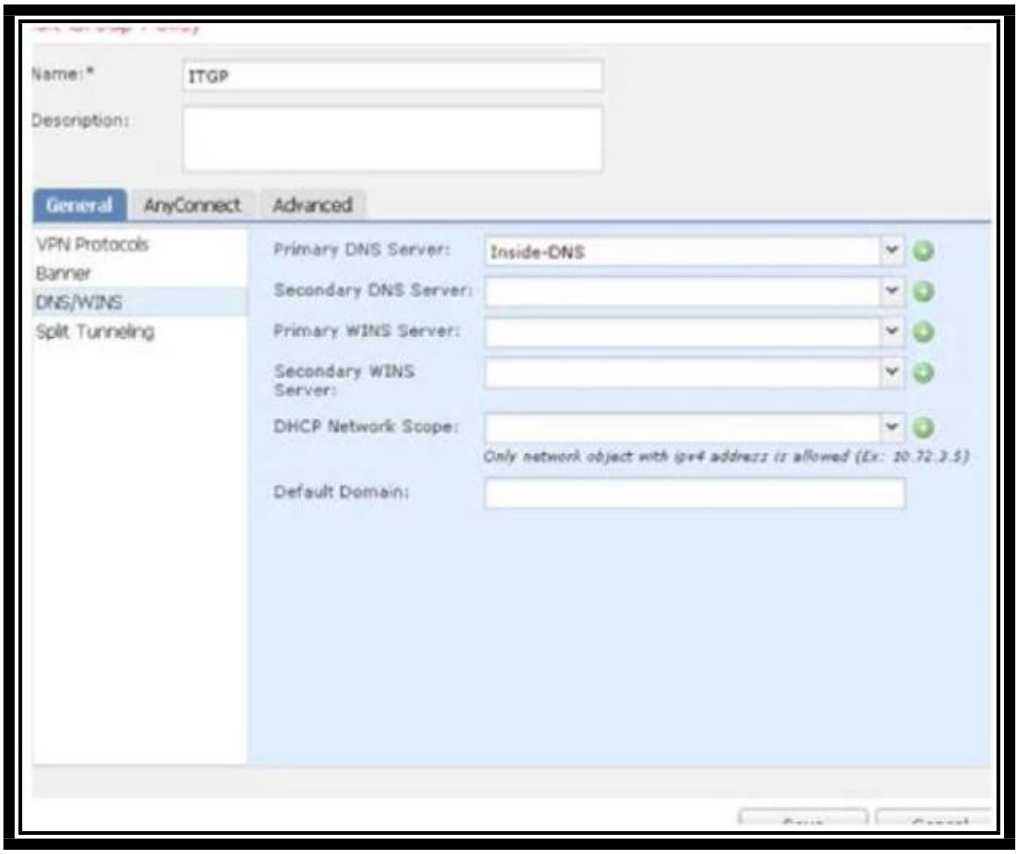
手順

新しいグループ ポリシーを作成する

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。この名前は 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、[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。
    d. [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、[保存（Save）] をクリックします。





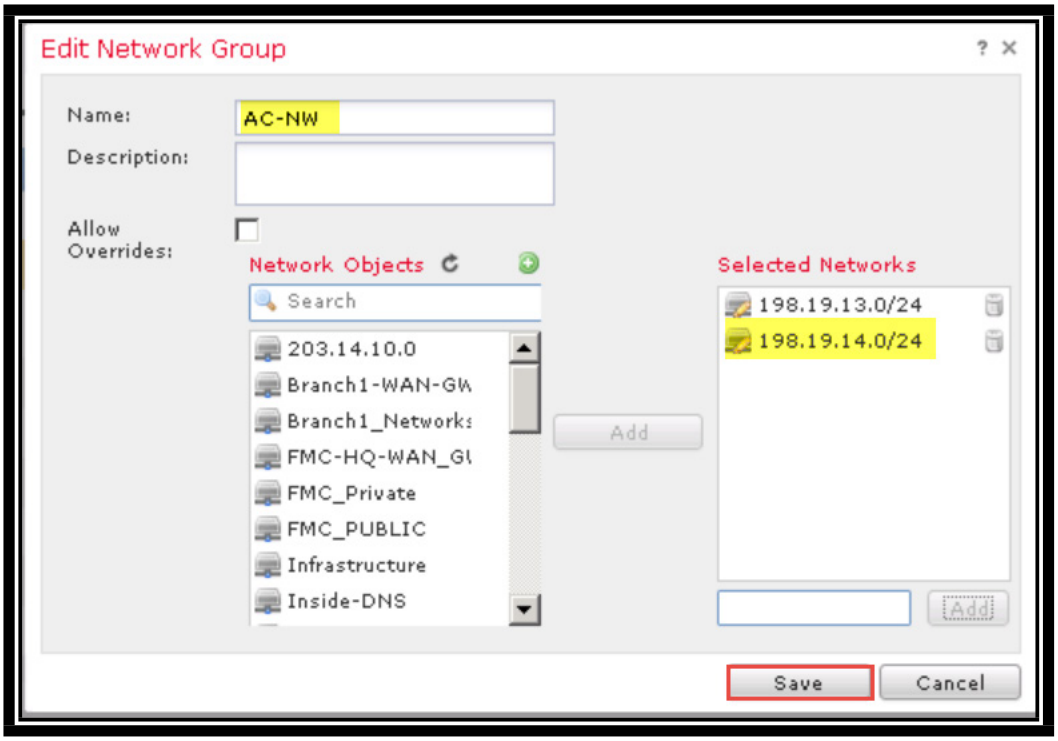
新しい IP プールを作成する

1. 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。
    a. [IPv4プールの追加（Add IPv4 Pools）] をクリックします。
    b. [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。
    c. [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。
    d. [マスク（Mask）] に「**255.255.255.0**」と入力します。
    e. [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

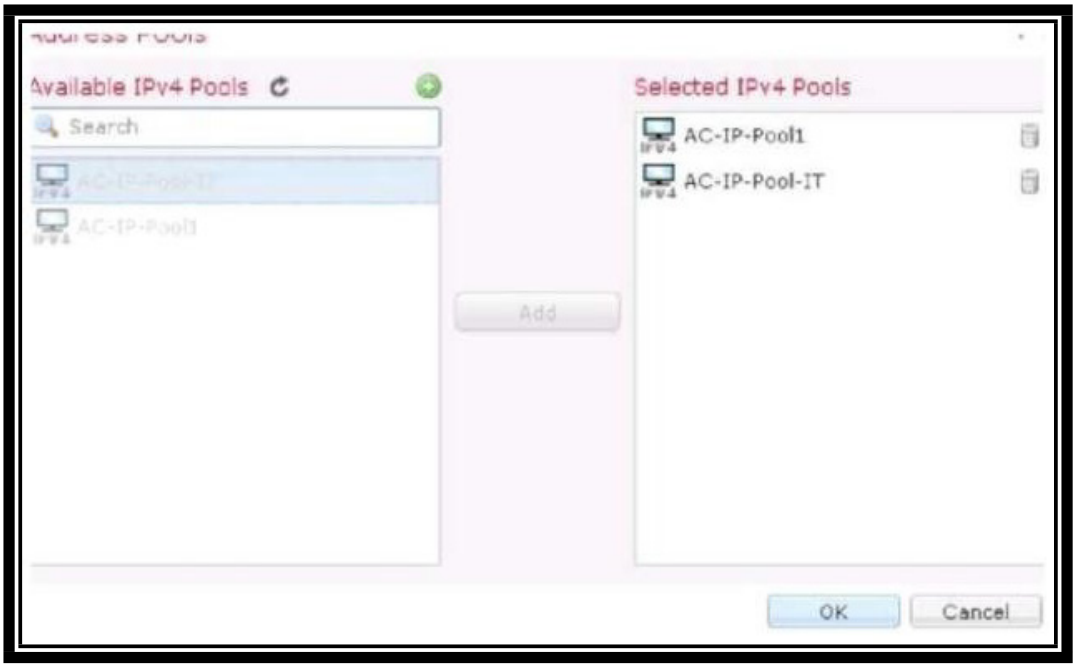
AC-NW ネットワーク グループ オブジェクトを変更すれば、アクセス制御と NAT ポリシーの両方を変更することができます。

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. [選択したネットワーク（Selected Networks）] の下部にあるテキスト フィールドに「**198.19.14.0/24**」と入力し、[追加（Add）] をクリックします。
    c. c. [保存（Save）] をクリックします。



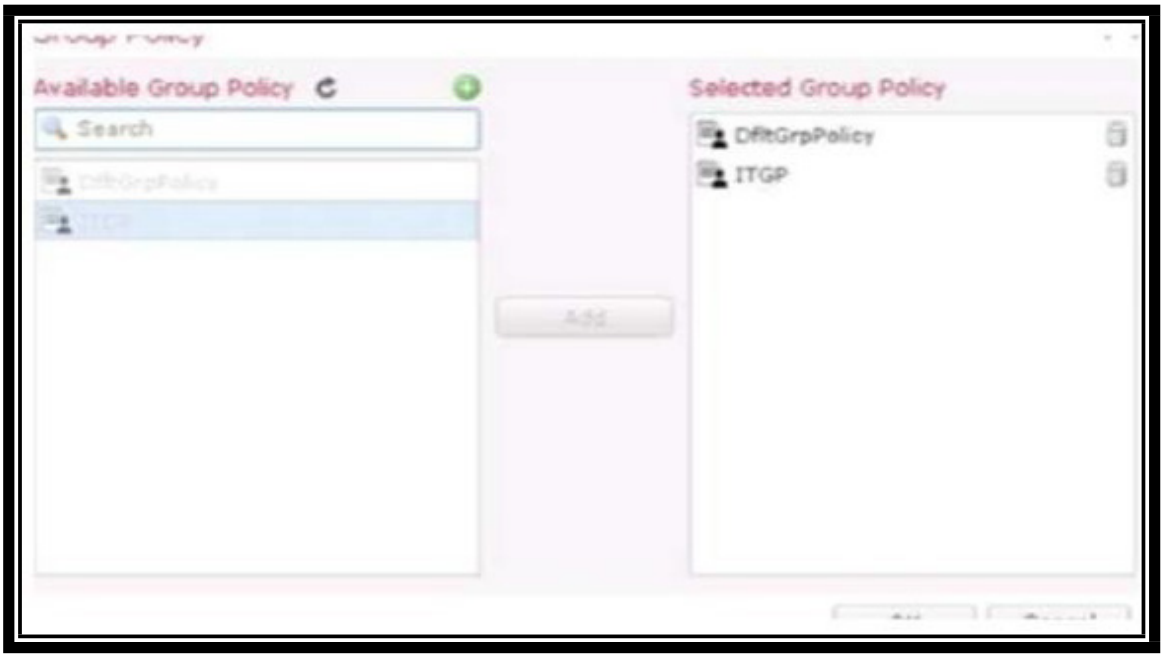
接続プロファイルを変更する

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。
    a. **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。
    b. 新しく作成された IP プールを追加します。
    c. 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。
    d. [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。
    e. [AC-IP-Pool-IT] を選択し、[追加（Add）] をクリックして [OK] をクリックします。



f. [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。

2. 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。
3. HA_Test の変更を導入します。導入が完了するまで待ちます。



設定をテストする

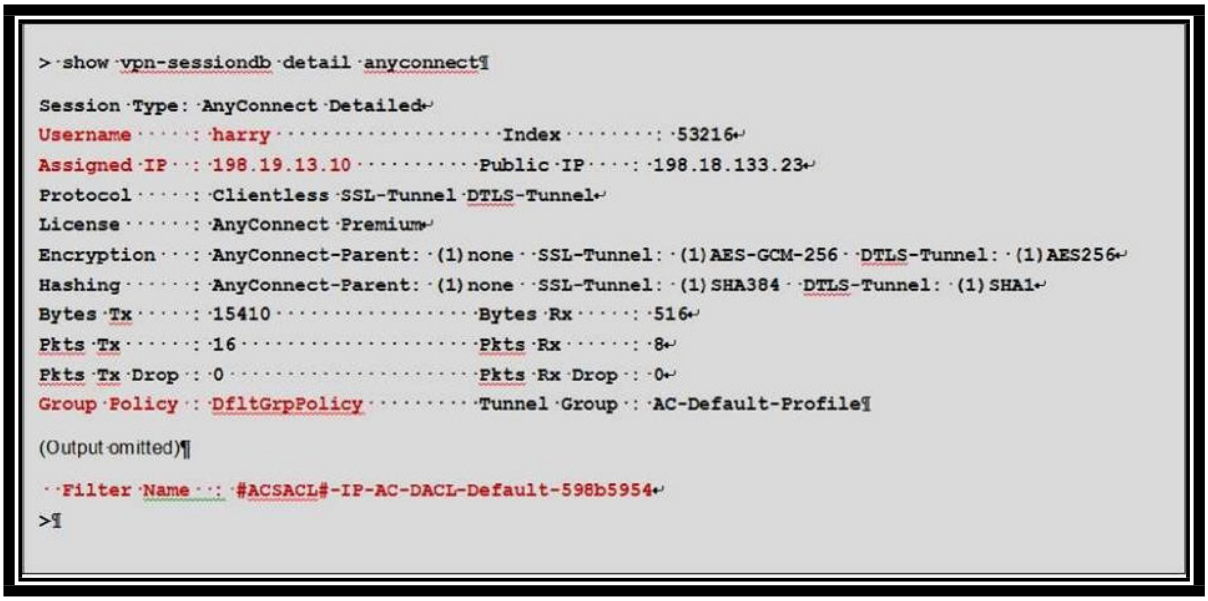
1. Outside-PC リモート デスクトップ セッションに戻ります。

    a. AnyConnect クライアントで [接続（Connect）] をクリックします。

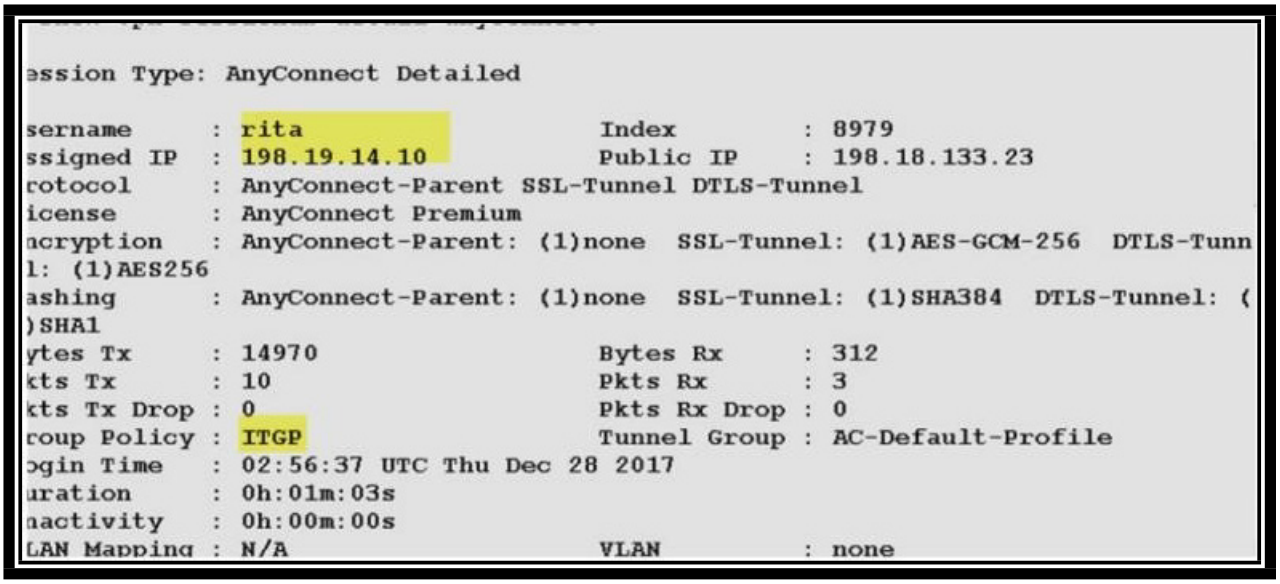
    b. ユーザ名：**harry**、パスワード：**C1sco12345** でログインします。harry は IT グループのメンバーではありません。

2. 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。

    a. ping **inside.dcloud.local** これは成功するはずです。
    b. ping **NGFW1.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。
    c. **NFGW1** CLI で、「**show vpn-sessiondb detail anyconnect**」コマンドを実行します。出力で次の値を確認します。
        i. [ユーザ名（Username）] : **harry**
        ii. [割り当てられたIP（Assigned IP）] : **198.19.13.x**
        iii. [グループポリシー（Group Policy）] : **DfltGrpPolicy**
        iv. [フィルタ名（Filter Name）] : **#ACSACL#-IP-AC-DACL- Default-x**



3. Outside-PC リモート デスクトップ セッションに戻ります。
4. AnyConnect VPN セッションを切断します。
5. 新しく AnyConnect VPN セッションを開始します。
6. ユーザ名：**rita**、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。
7. 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。
    a. ping **inside.dcloud.local** これは成功するはずです。
    b. ping **NGFW1.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。
8. **NFGW1 CLI** で、「**show vpn-sessiondb detail anyconnect**」コマンドを実行します。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



9. **AnyConnect VPN** クライアントを切断します。

シナリオ 5： 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
- エクストラネットを使用してサイト間 VPN を確立する（ブランチ 2 は FDM が管理）
- 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

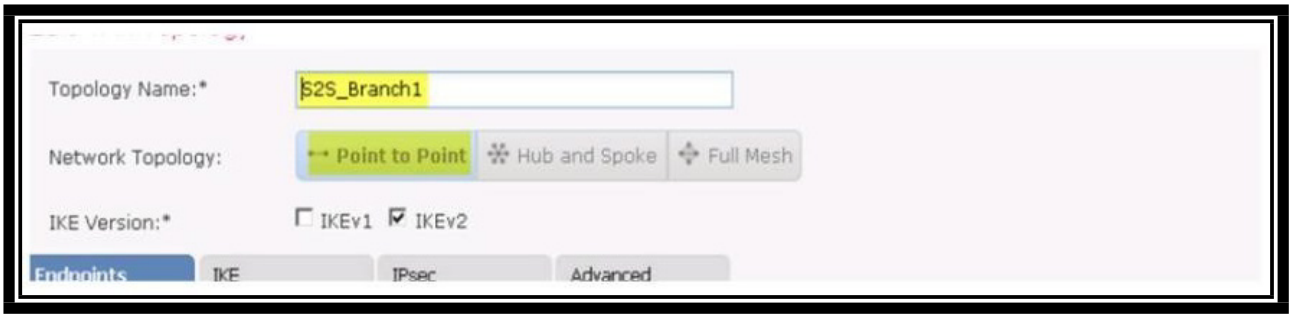
1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動します。[ネットワーク（Network）] オブジェクト ページが選択されます。
    a. [ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）] の順に選択します。
    b. [名前（Name）] に「**MainOfficeNetwork**」と入力します。
    c. [ネットワーク（Network）] オプション ボタンを選択します。
    d. 「**198.19.10.0/24**」と入力します。
    e. [保存（Save）] をクリックします。
2. [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。
    a. [名前（Name）] に「**Branch1OfficeNetwork**」と入力します。
    b. [ネットワーク（Network）] オプション ボタンをクリックします。
    c. 「**198.19.11.0/24**」と入力します。
    d. [保存（Save）] をクリックします。

サイト間 VPN を設定する

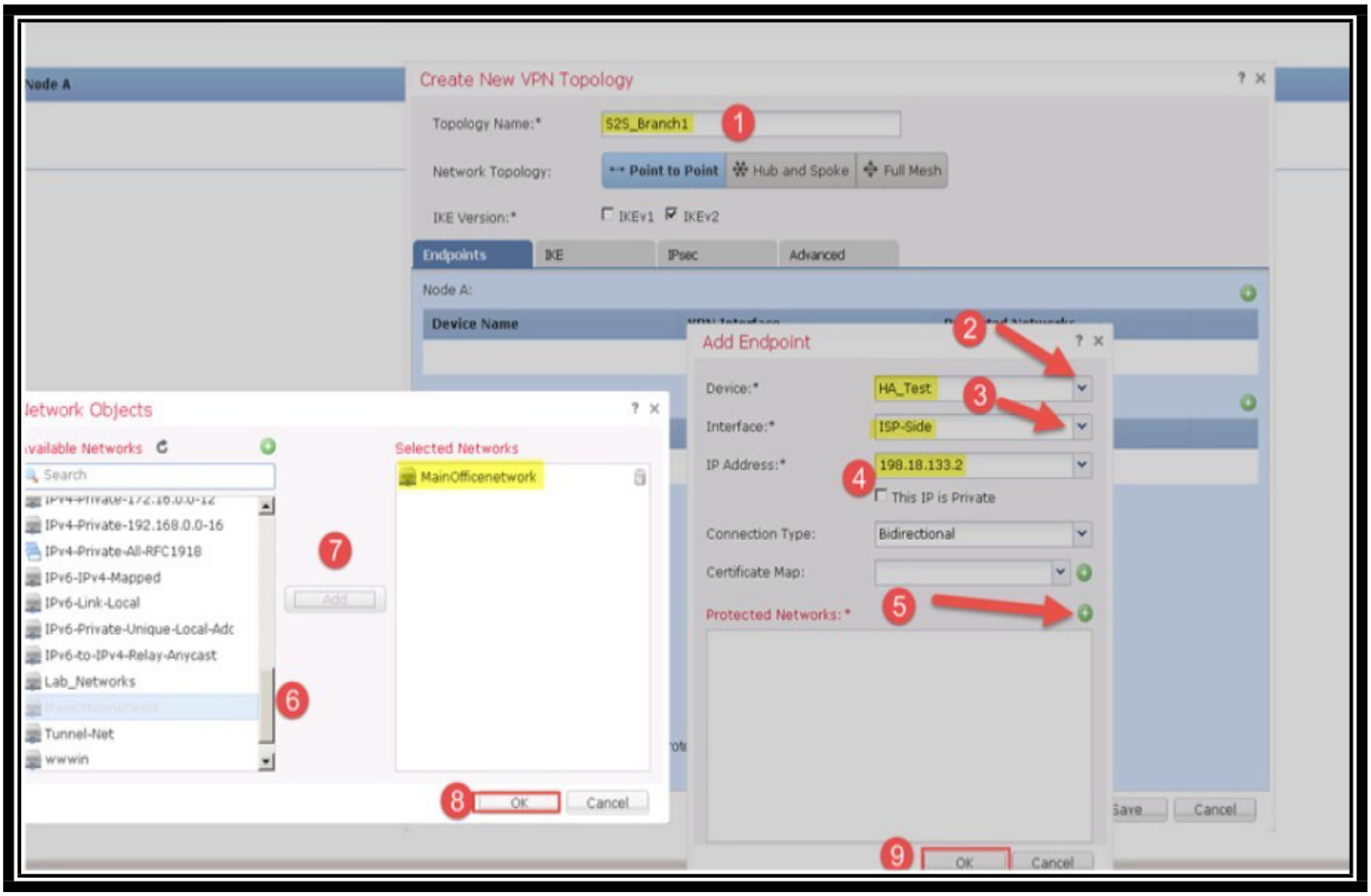
1. [デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] に移動します。[VPNの追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）] をクリックします。

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。

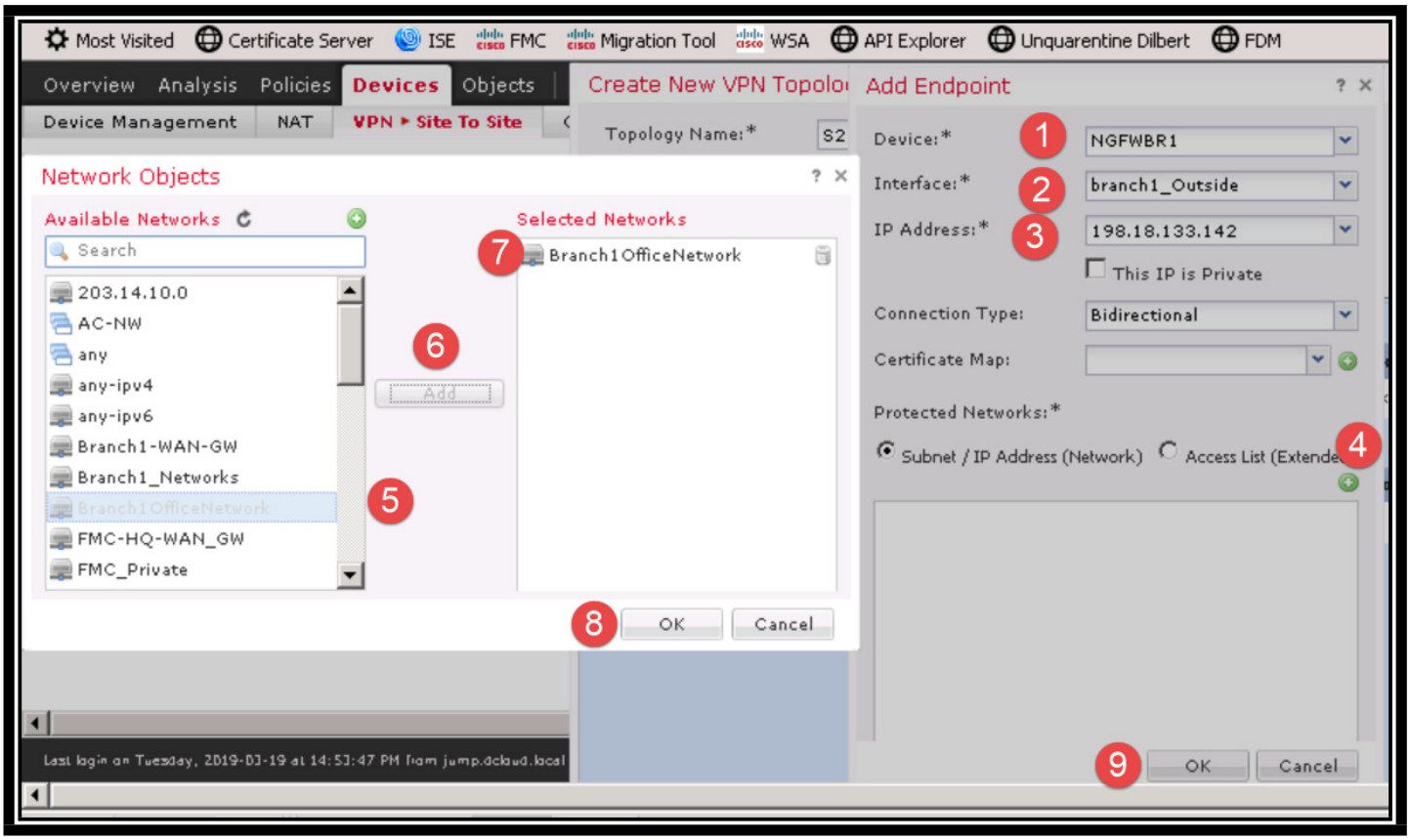
2. [名前（Name）] に「**S2S_Branch1**」と入力します。
    a. [ネットワークトポロジ（Network Topology）] で [ポイントツーポイント（Point to Point）] が選択されていることを確認します。[IKE バージョン（IKE Version）] で [IKEv1] がオフで、[IKEv2] がオンであることを確認します。



3. [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。

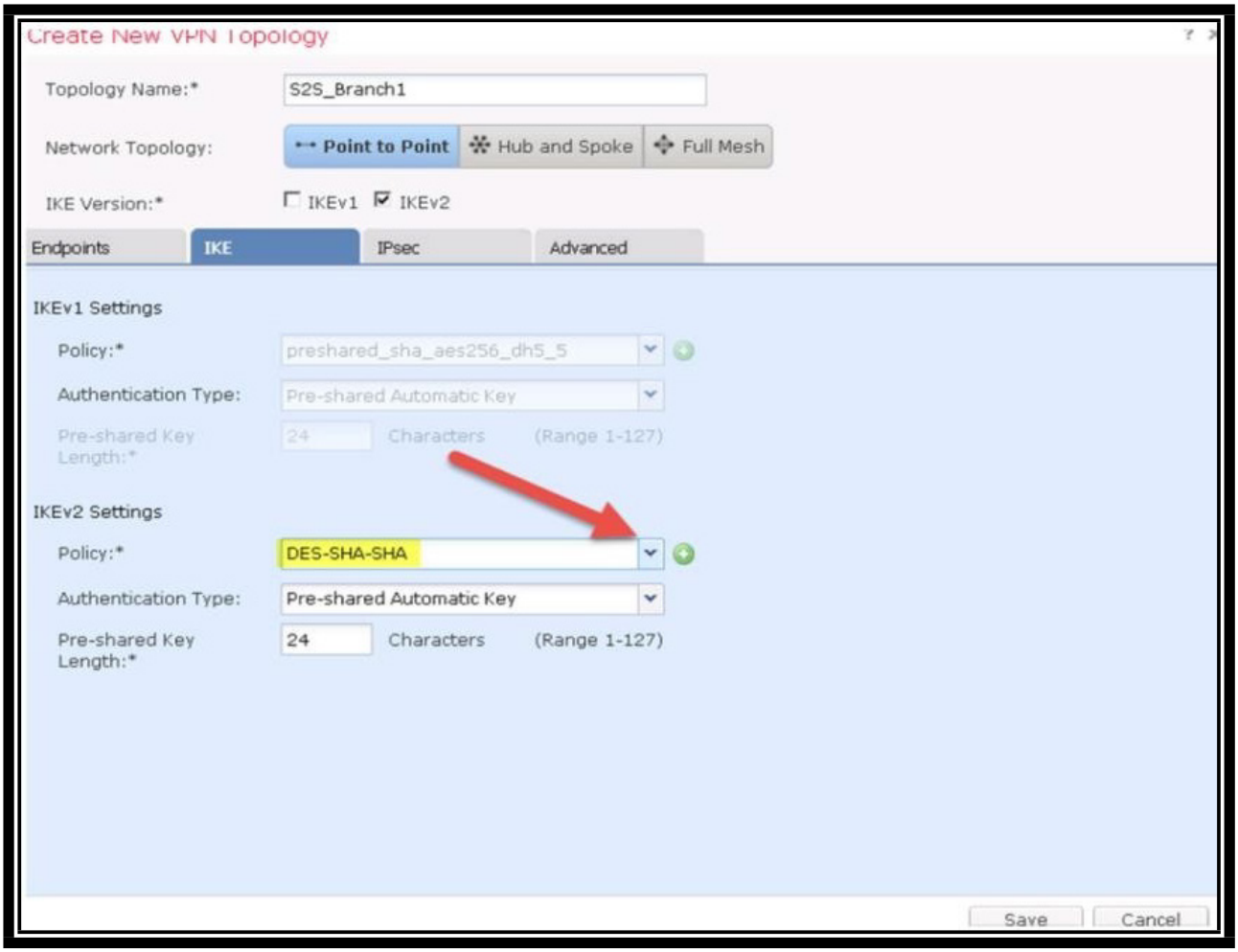


4. [ノードB（Node B）] の右側にある、**緑色のプラス**記号をクリックします。次の図のようにフィールドに入力し、[OK] をクリックします。

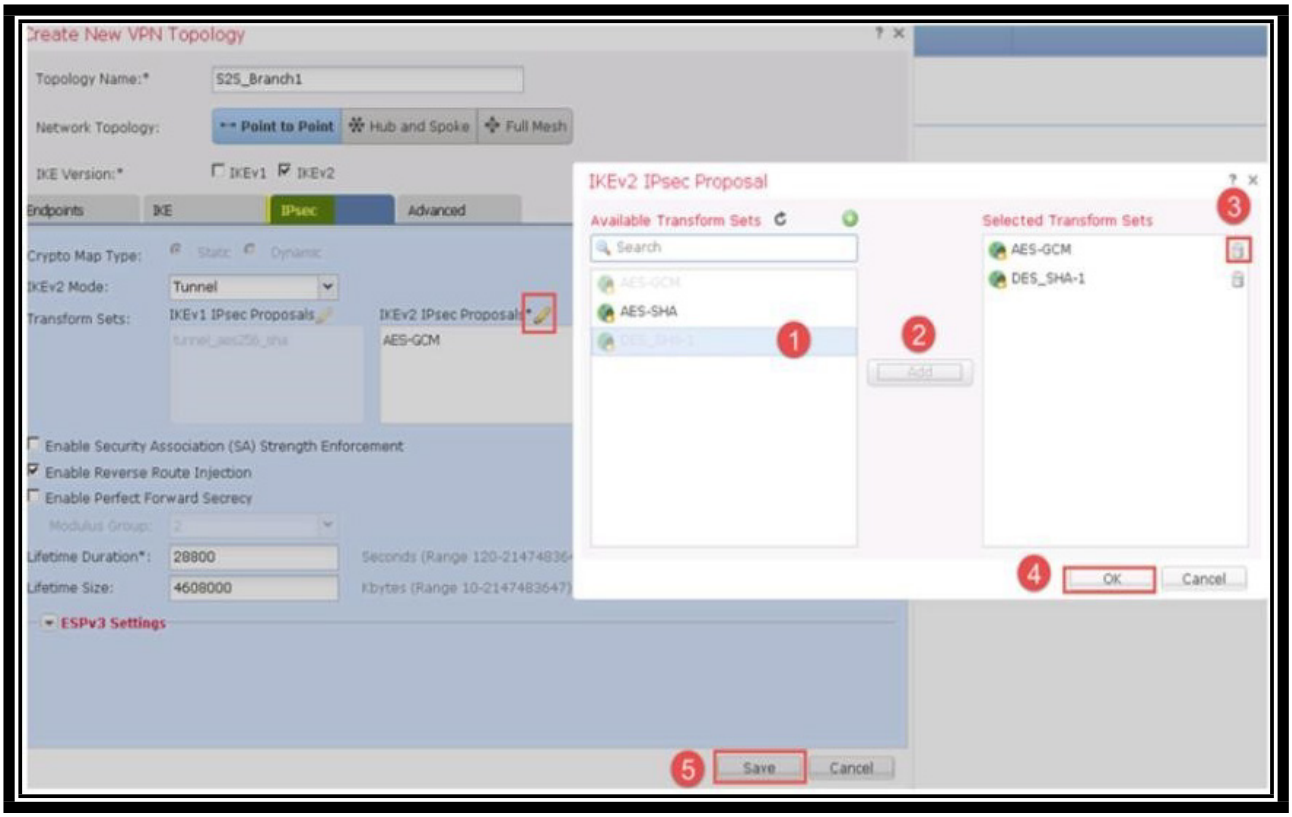


5. [IKE] タブを選択します。
6. [IKEv2設定（IKEv2 Settings）] の下の [ポリシー（Policy）] で、[DES-SHA-SHA] を選択します。
7. [IKEv2設定（IKEv2 Settings）] の下の [認証タイプ（Authentication Type）] で、[自動事前共有キー（Pre-shared Automatic Key）] を選択します。

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。



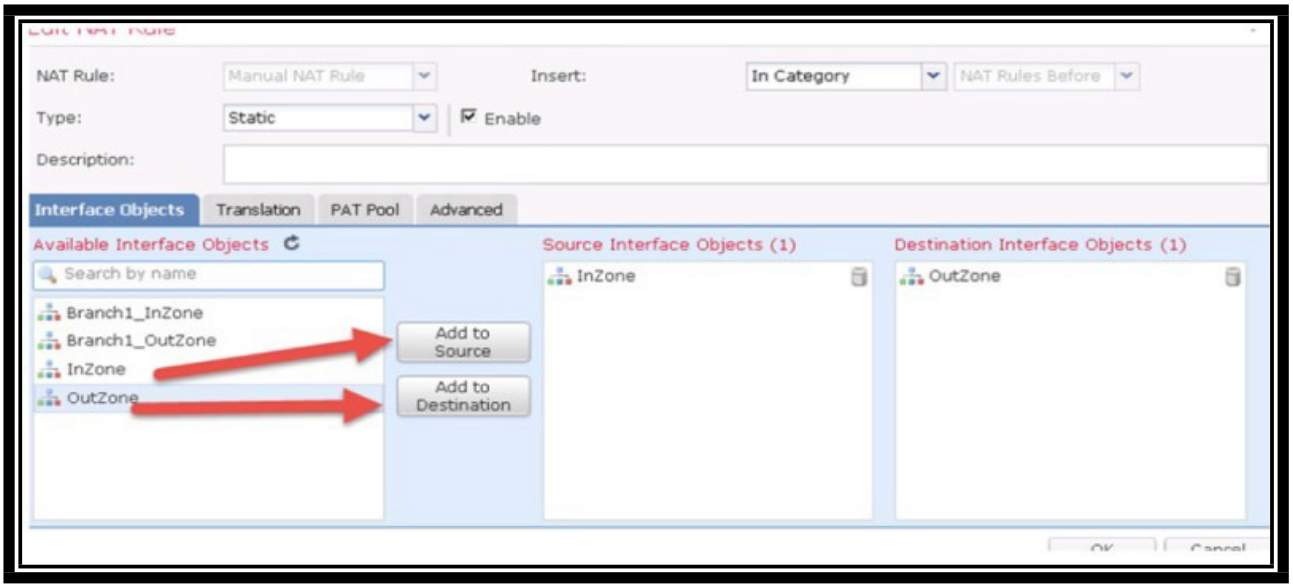
8. [IPsec] タブを選択して、[IKEv2 IPsecプロポーザル（IKEv2 IPsec Proposal）] を [DES_SHA-1] に変更します。
9. [IKEv2 IPsecプロポーザル（IKEv2 IPsec Proposal）] の**鉛筆**（編集）アイコンをクリックします。
10. [DES_SHA-1] をクリックし、[追加（Add）] をクリックします。
11. **AES-GCM** を削除します。
12. [OK] をクリックし、[保存（Save）] をクリックします。



HQ で NAT 適用除外を作成する

注：NAT 適用除外は、NAT によってアドレスが変換されないようにするためのものです。そのためには、NAT プロセスで変換されたパケットを元のアドレスに戻す必要があります。この処理は NAT ステートメントの前に実施する必要があるため、ルールを [処理前のNATルール（NAT Rules Before）] カテゴリに入れる必要があります。

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、**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。



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

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

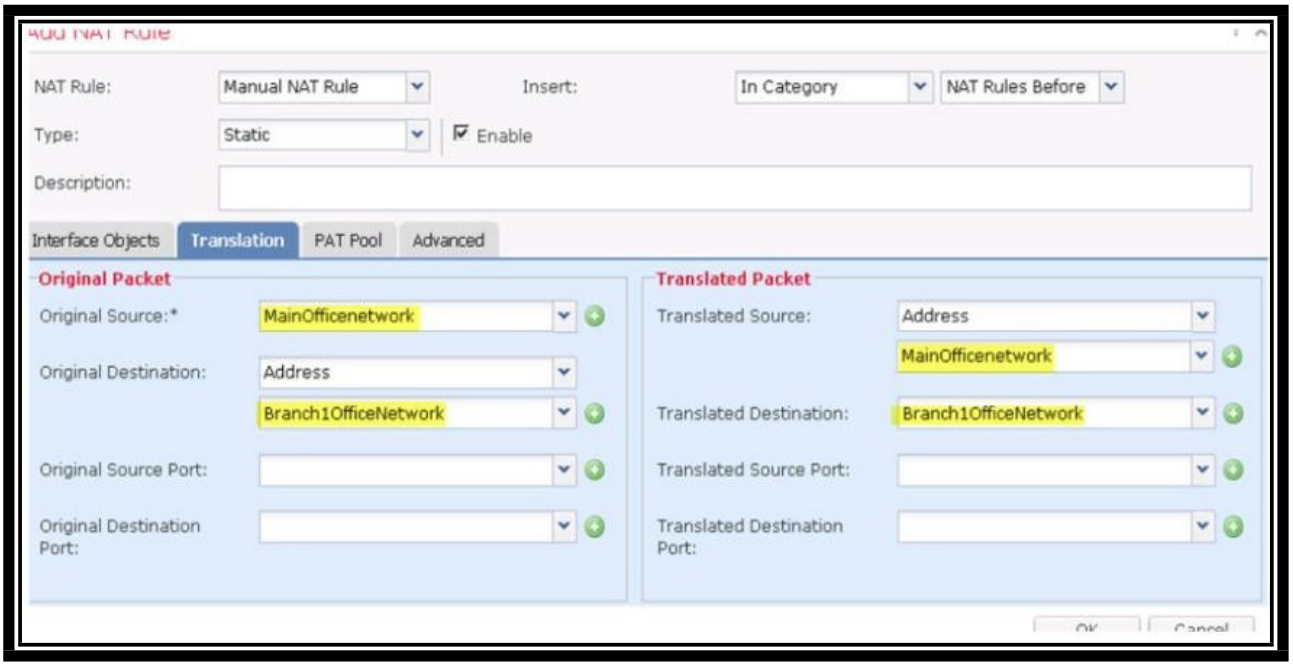
4. [変換（Translation）] タブを選択します。

a. [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。

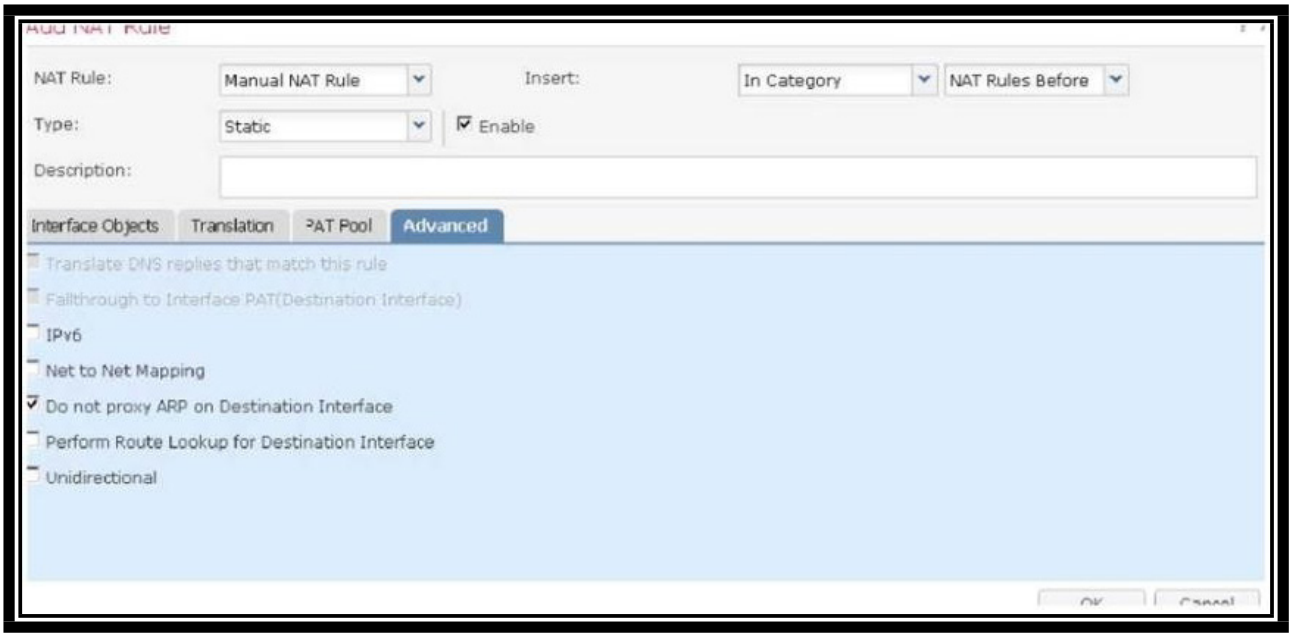
b. [変換済み送信元（Translated Source）] ドロップダウン リストから [MainOfficeNetwork] を選択します。

c. [元の宛先（Original Destination）] ドロップダウン リストから [Branch1OfficeNetwork] を選択します。

d. [変換後の宛先（Translated Destination）] ドロップダウン リストから [Branch1OfficeNetwork] を選択します。



5. [詳細（Advanced）] タブに移動し、宛先インターフェイスの [プロキシ ARP を有効にしない（Do not proxy ARP）] をオンにして、[OK] をクリックします。

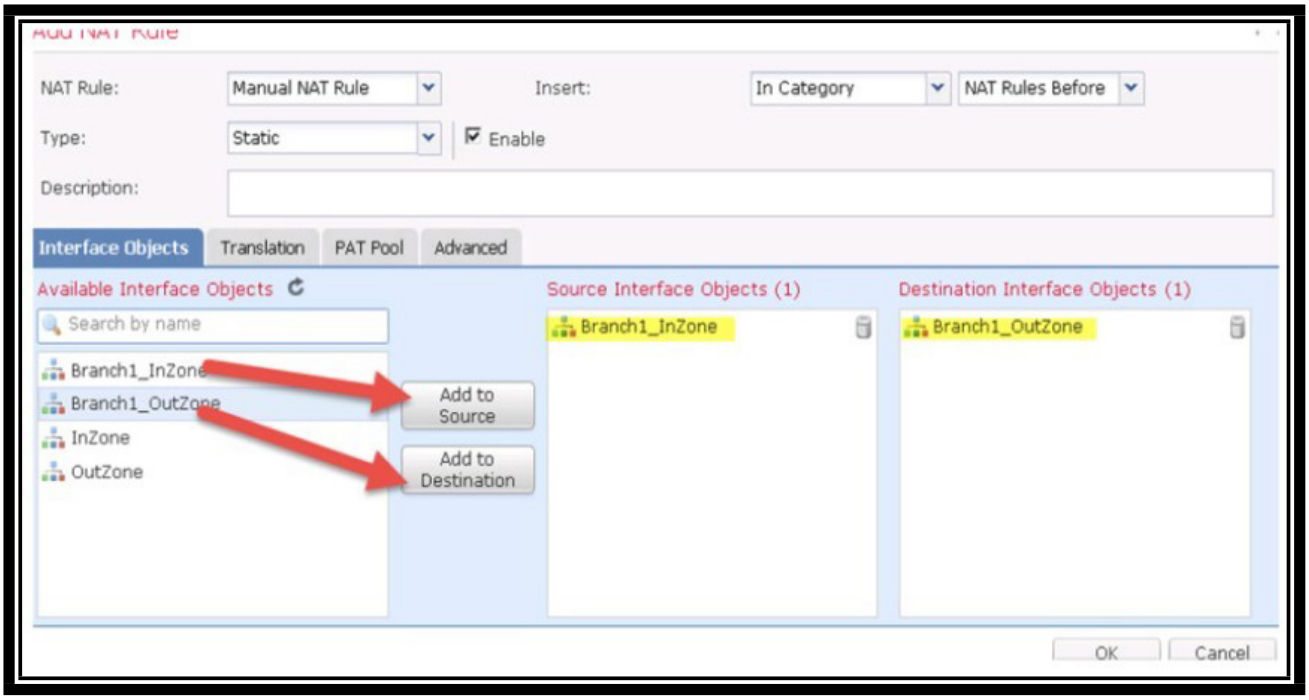


6. [保存（Save）] をクリックします。

Branch1 で NAT 適用除外を作成する

1. [デバイス（Devices）] > [NAT] > [Branch1 NAT] に移動し、鉛筆アイコンをクリックして該当の NAT ポリシーを編集します。

2. [ルールの追加（Add Rule）] をクリックします。
    a. [インターフェイスオブジェクト（Interface Objects）]
        i. [Branch1_InZone] をクリックし、[送信元に追加（Add to Source）] をクリックします。
        ii. [Branch1_OutZone] をクリックし、[宛先に追加（Add to Destination）] をクリックします。



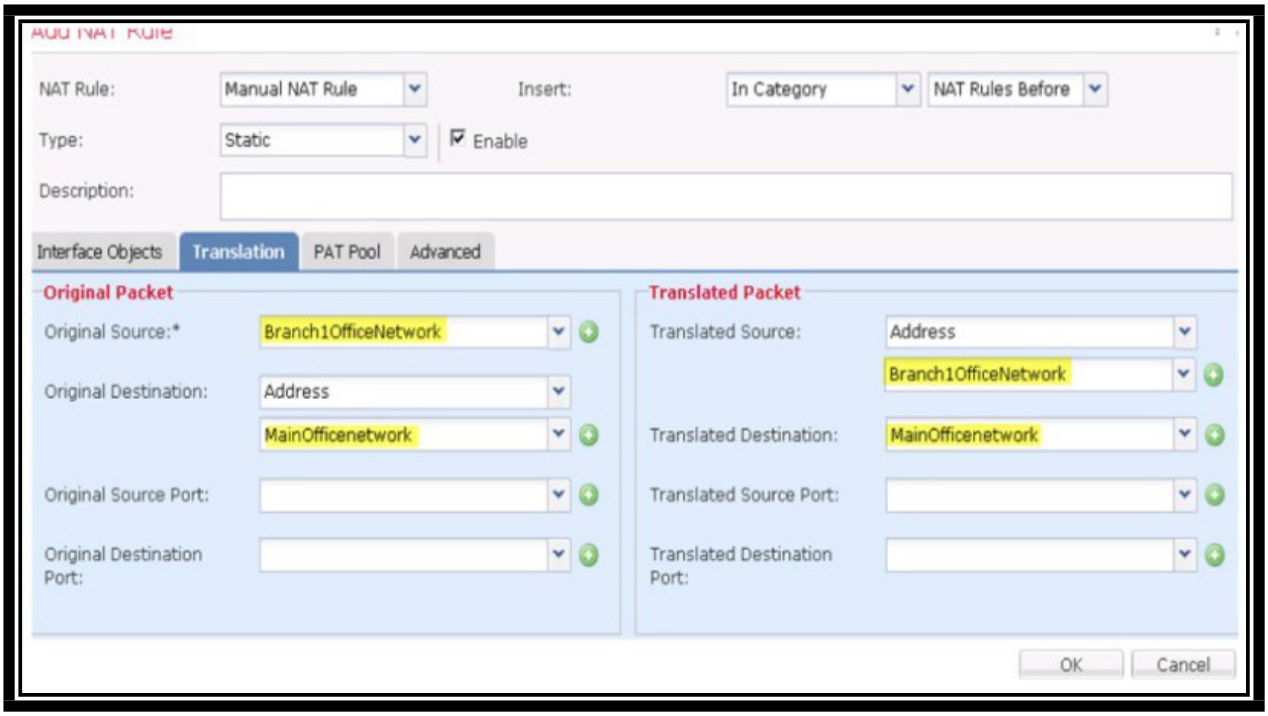
b. [変換（Translation）]

   i. [元のパケット（Original Packet）]

      1. [元の送信元（Original Source）]：Branch1OfficeNetwork
      2. [元の宛先（Original Destination）]：MainOfficenetwork

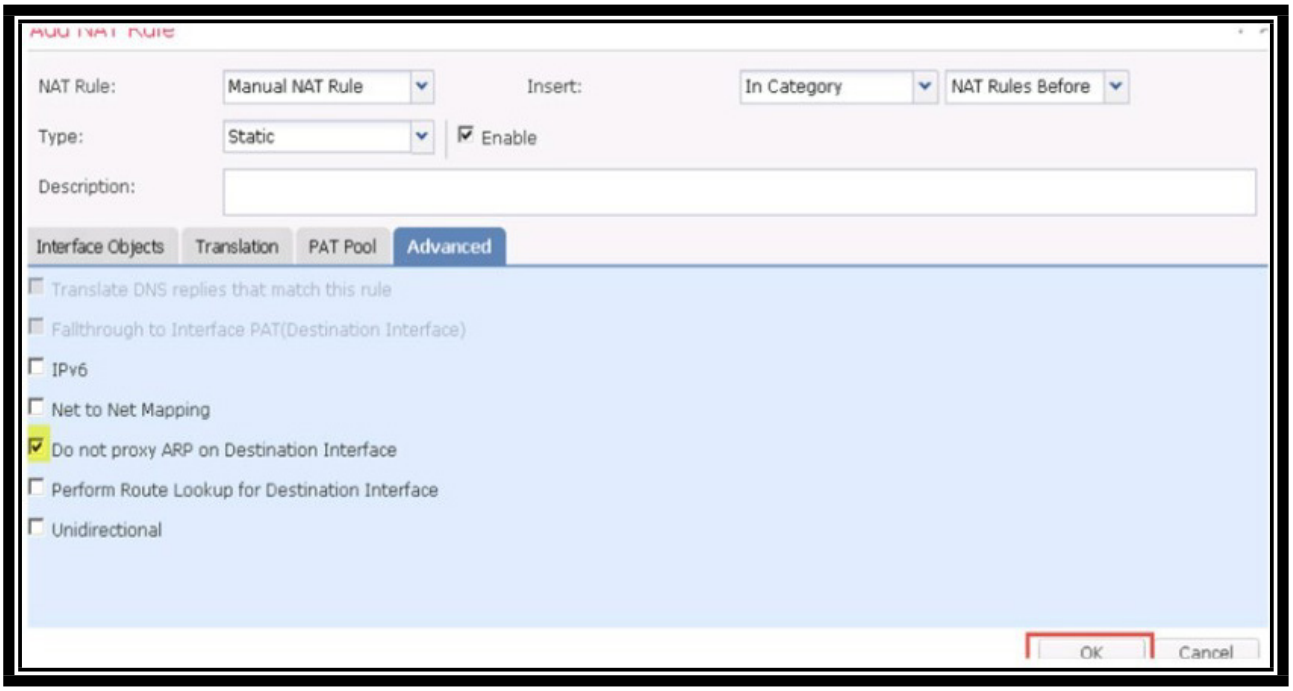
   ii. [変換後のパケット（Translated Packet）]

      1. [変換後の送信元（Translated Source）]：Branch1OfficeNetwork
      2. [変換後の宛先（Translated Destination）]：MainOfficenetwork



c. [詳細（Advanced）]

i. 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）] をクリックします。

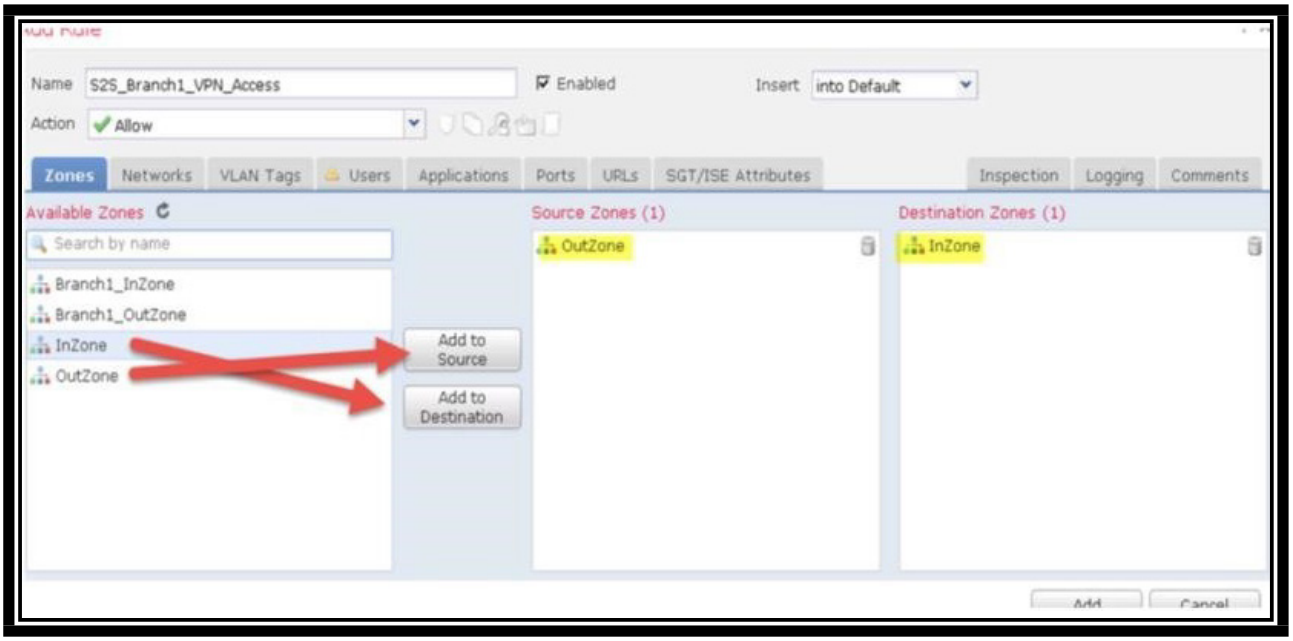


10. [OK] をクリックします。
11. [OK] をクリックして NAT ルールを保存します。
12. [保存（Save）] をクリックして NAT ポリシーを保存します。

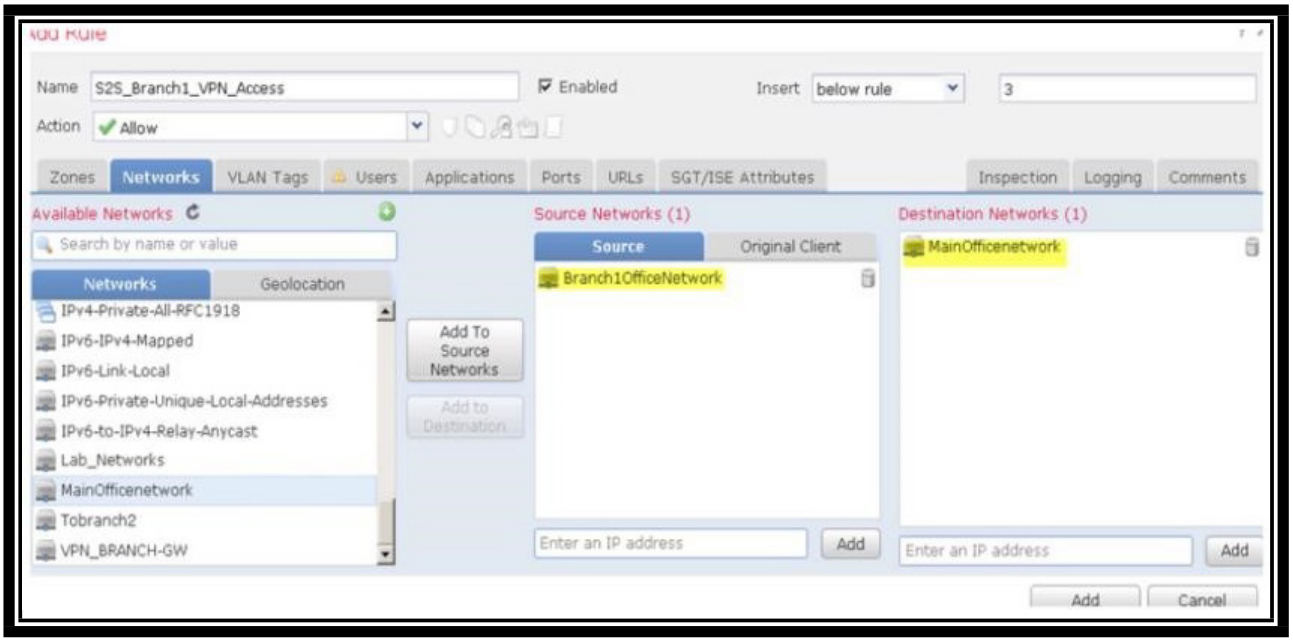
アクセス コントロール ポリシーを変更し、変更を導入する

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）] > [アクセスコントロール（Access Control）] > [アクセスコントロール（Access Control）] の順に選択します。**Base_Policy アクセス コントロール ポリシー**を編集します。
2. [ルールの追加（Add Rule）] をクリックします。
    a. **S2S_Branch1_VPN_Access** ルールを呼び出します。
3. [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。
4. アクションは [許可（Allow）] のままにします。
5. [ゾーン（Zones）] タブがすでに選択されているはずです。
6. [OutZone] を選択し、[送信元に追加（Add to Source）] をクリックします。
7. [InZone] を選択し、[宛先に追加（Add to Destination）] をクリックします。



8. [ネットワーク（Networks）] タブから [Branch1OfficeNetwork] を選択し、[送信元に追加（Add to Source）] をクリックします。
9. [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。



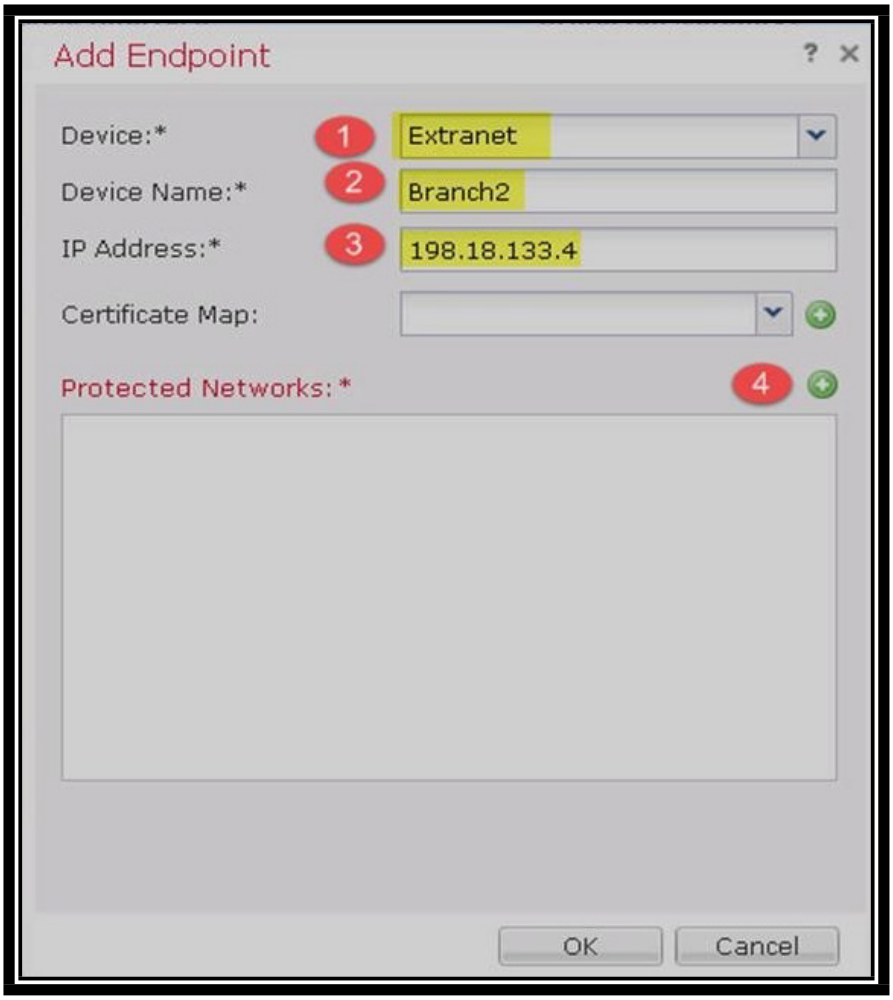
10. [インスペクション（Inspection）] タブを選択します。
11. [侵入ポリシー（Intrusion Policy）] ドロップダウン リストから [デモ侵入ポリシー（Demo Intrusion Policy）] を選択します。
12. [ファイル ポリシー（File Policy）] ドロップダウン リストから [デモ ファイル ポリシー（Demo File Policy）] を選択します。
13. [追加（Add）] をクリックして、このルールをアクセス コントロール ポリシーに追加します。
14. [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。
15. インバウンド接続を許可するように **Branch1 アクセス ポリシーを変更します。**

Branch2 サイト間に FMC を設定する

注 : シナリオ 6 から開始してこのセクションを完了する場合は、シナリオ 2 の基本ラボの「Firepower Device Manager（FDM ON BOX）を使用したブランチ 2 管理の設定」セクションを実施する必要があります。これはライセンス制限によるものです。

注：この設定では、ブランチ 2 は FDM（On Box Manager）によって管理されます。サイト間 VPN はエクストラネットに設定されるため、IKEv2 キーを手動で設定する必要があります。

1. [デバイス（Devices）] > [VPN] > [サイト間（Site to Site）] > [VPNの追加（Add VPN）] > [Firepower Threat Defense] に移動します。
2. [トポロジ名（Topology Name）] : **Branch2_S2S**
3. ノード A の場合は、ノード A **[S2S_Branch1]** の設定**手順 2 および 3** に従い、任意の接続名に変更します。
4. ノード B
    a. **Extranet** を選択します（FMC の管理対象外）。
    b. [デバイス名（Device Name）] : **Branch2**
    c. [IP アドレス（IP Address）] : 198.18.133.4



d. [保護されたネットワーク (Protected Networks)] のプラス記号をクリックし、ネットワーク オブジェクトを作成します。

e. [名前（Name）]：**Branch2Officenetwork**

f. [ネットワーク（Network）] オプション ボタンをクリックします。

g. [アドレス（Address）]：**192.168.45.0/24**

h. [保存（Save）] をクリックします。

i. [Branch2Officenetwork] をクリックします。

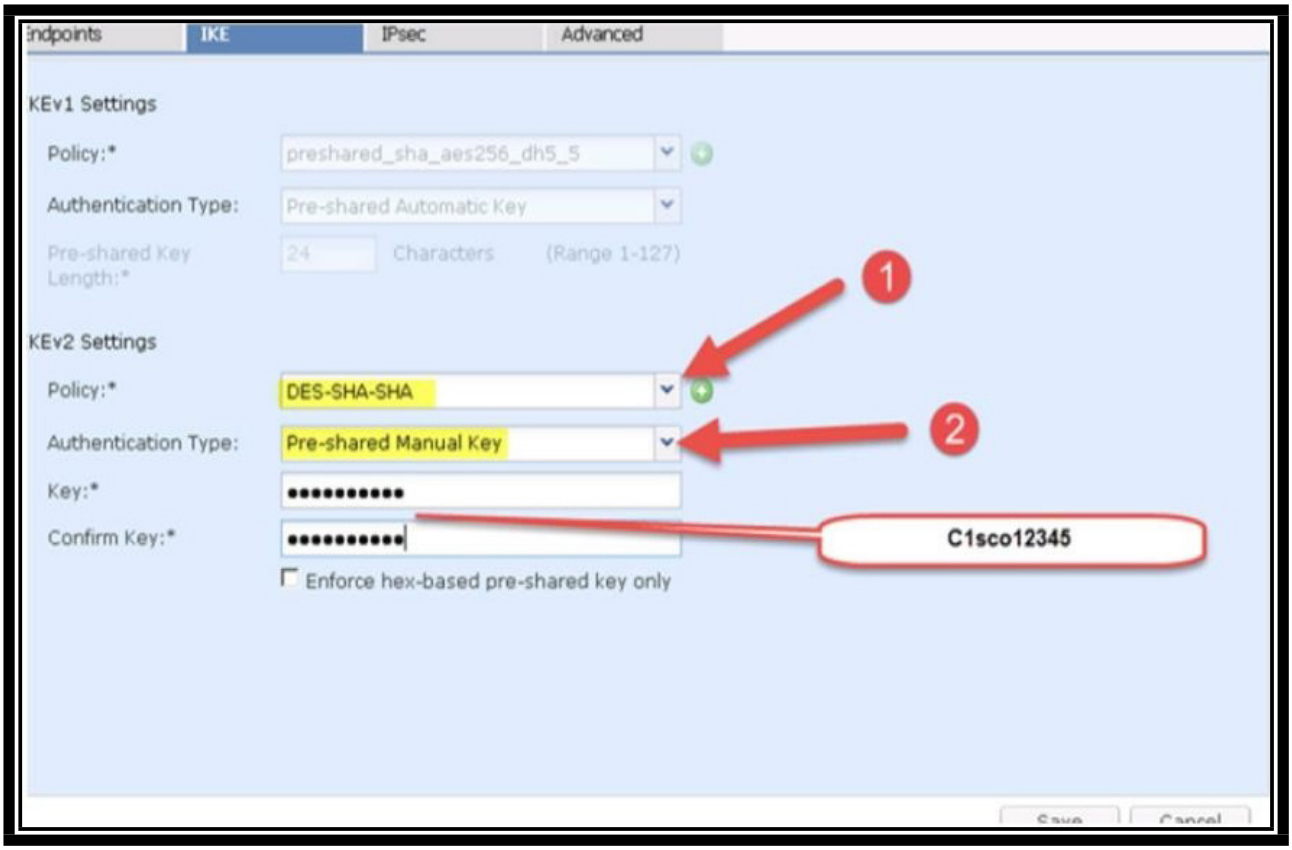
j. [追加（Add）] をクリックします。

k. [OK] をクリックし、さらに [OK] をクリックします。

5. [IKEポリシー（IKE Policy）] で [DES-SHA-SHA] を選択します。

6. 認証タイプ：[手動事前共有キー（Pre-shared Manual Key）]

7. [キー（Key）]：**C1sco12345**、[キーの確認（Confirm Key）]：**C1sco12345**



8. [IPsec] をクリックします。
    a. IKEv2 IPsec Proposals を編集します。
    b. **DES_SHA-1** を追加し、**AES GCM** を削除します。
    c. [OK] をクリックします。
9. [保存（Save）] をクリックします。
10. S2S_Branch2 の NAT 適用除外ポリシーを作成します。
11. S2S_Branch2 のアクセス ポリシーを作成します。

ブランチ 2 サイト間設定

1. Jump PC で Remote Desktop フォルダに移動し、Wkstbr2 をダブルクリックします。
2. ユーザ名：**Administrator**、パスワード：**C1sco12345**
3. ワークステーションで PuTTY を開き、「**192.168.45.45**」と入力して、**admin/C1sco12345!**、**ポート 22**（SSH）でログインします。

注：GUI を使用してパスワードを変更する場合は、パスワードに特殊文字を含める必要があります。そのため、パスワードに「**!**」を入れています。CLI でパスワードを設定する場合は、特殊文字は不要です。

4. 「**show managers**」と入力します。
    a. [ローカルで管理（Managed Locally）] と表示されます。

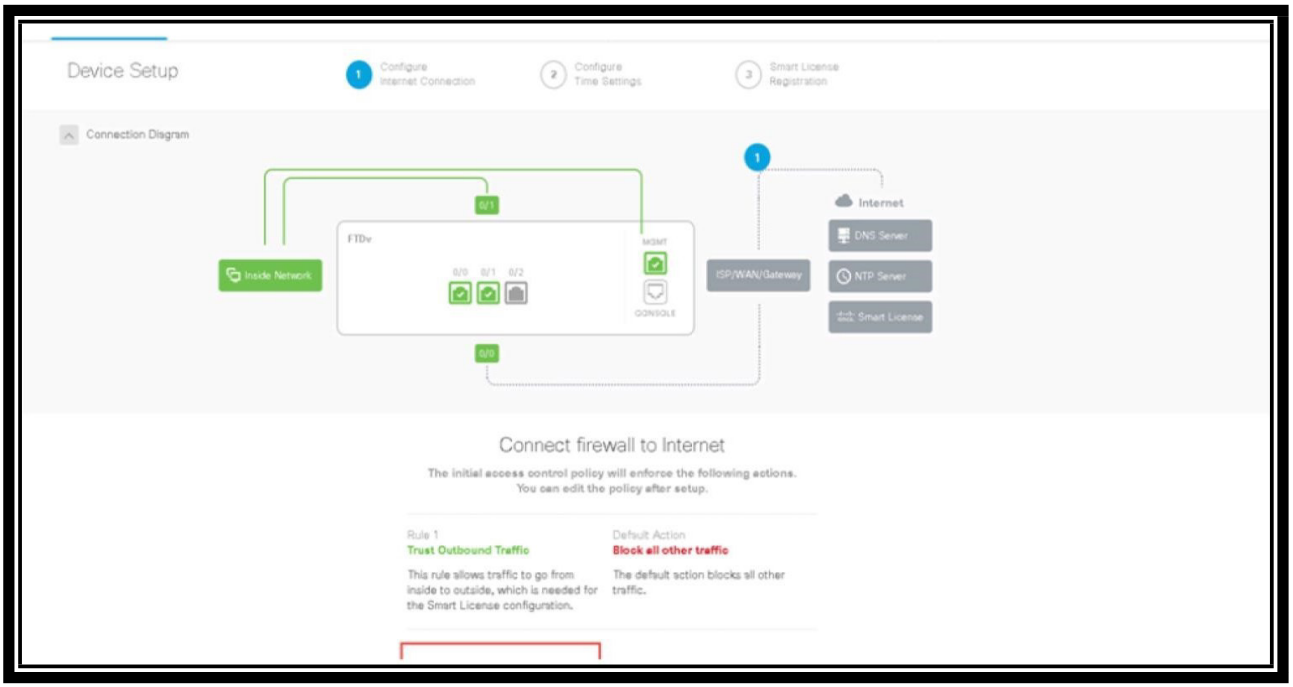
b. **configure manager delete**

c. 「**yes**」と入力します。

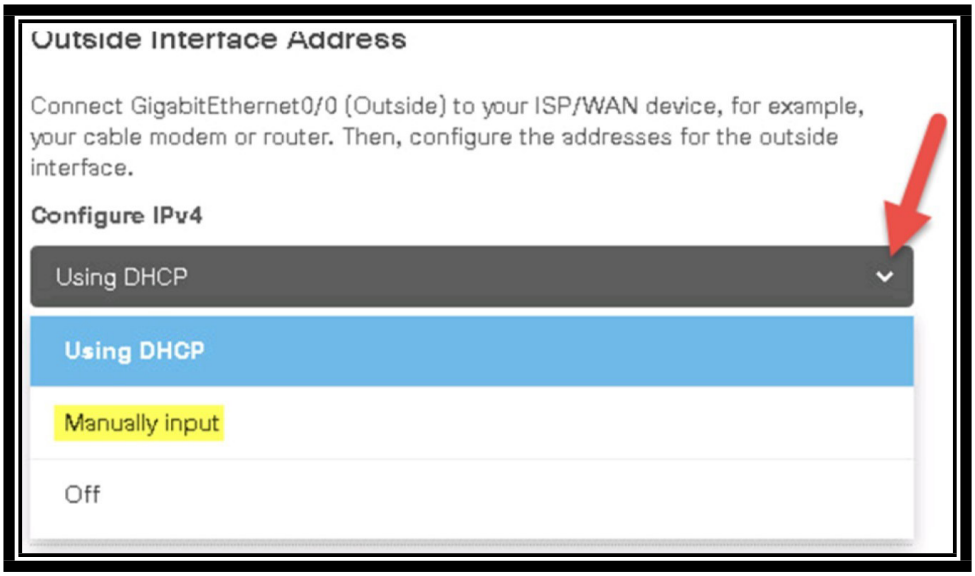
d. プロンプトから制御が戻るのを待ち、「**configure manager local** 」と入力して Enter を押します。

注：ソフトウェアのアップグレードのために、FDM（On Box Manager）が事前に設定されています。前述のコマンドを実行することで、一部の設定パラメータがクリアされ、評価ライセンスもリセットされます。

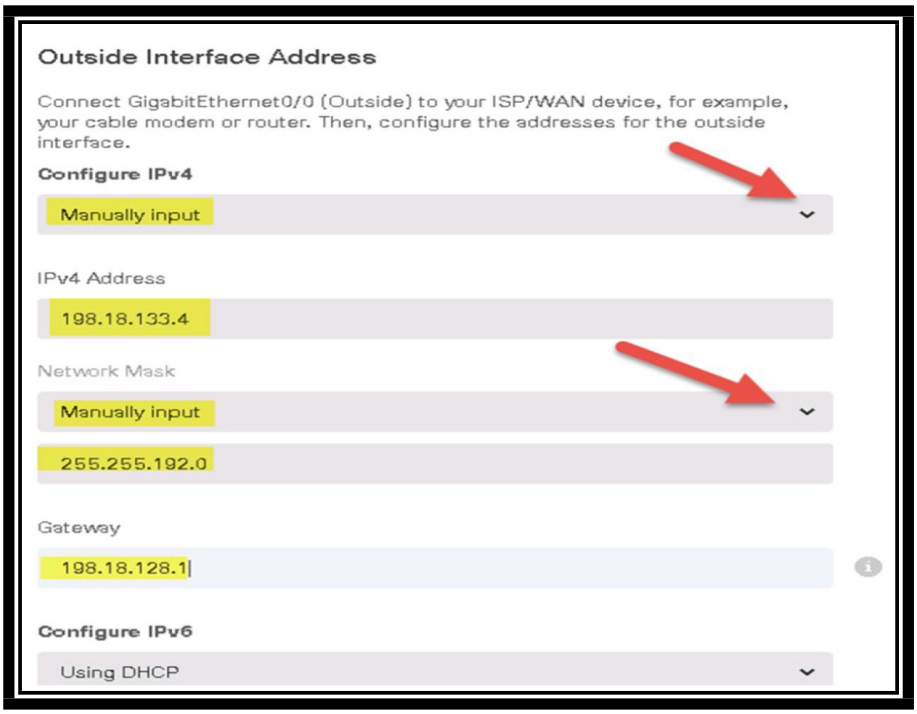
5. Firefox ブラウザを開きます。**192.168.45.45** に移動します。
6. [詳細設定（Advanced）]、[例外の追加（Add Exception）]、[セキュリティ例外の確認（Confirm Security Exception）] の順にクリックします。
7. ユーザ名：**admin**、パスワード：**C1sco12345!**
8. 次の画面が開き、FTD 接続が表示されます。[外部インターフェイスアドレス（Outside Interface Address）] まで下方向にスクロールします。



9. [DHCP を使用（Using DHCP）] の横にある**矢印**を選択します。
10. [手動入力（Manual Input）] をクリックします。



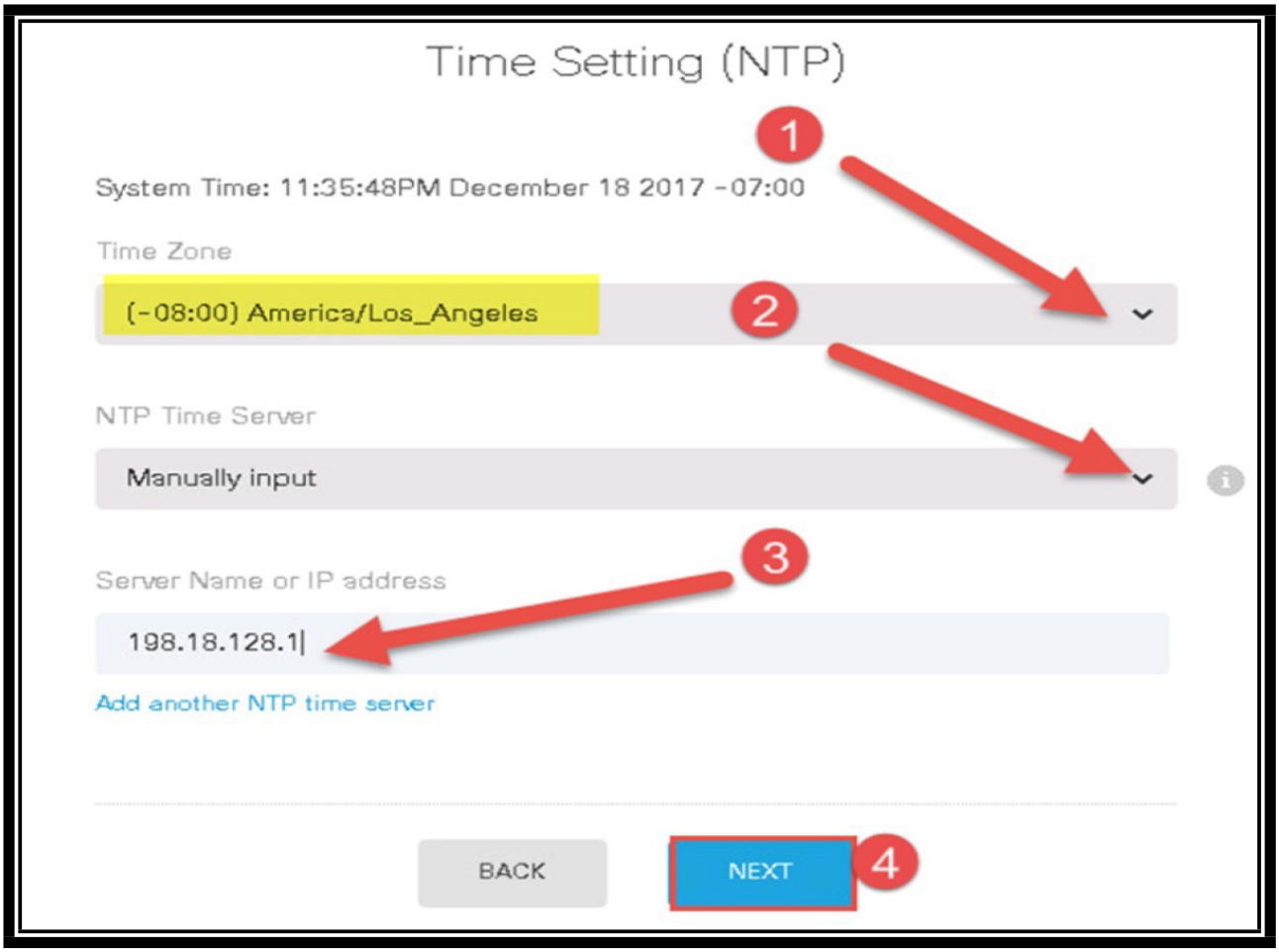
11. [外部インターフェイス アドレス（Outside Interface Address）] を設定します。
    - [IP アドレス（IP Address）] : **198.18.133.4**
    - [ネットワーク マスク（Network Mask）] : **255.255.192.0**
    - [ゲートウェイ（Gateway）] : **198.18.128.1**



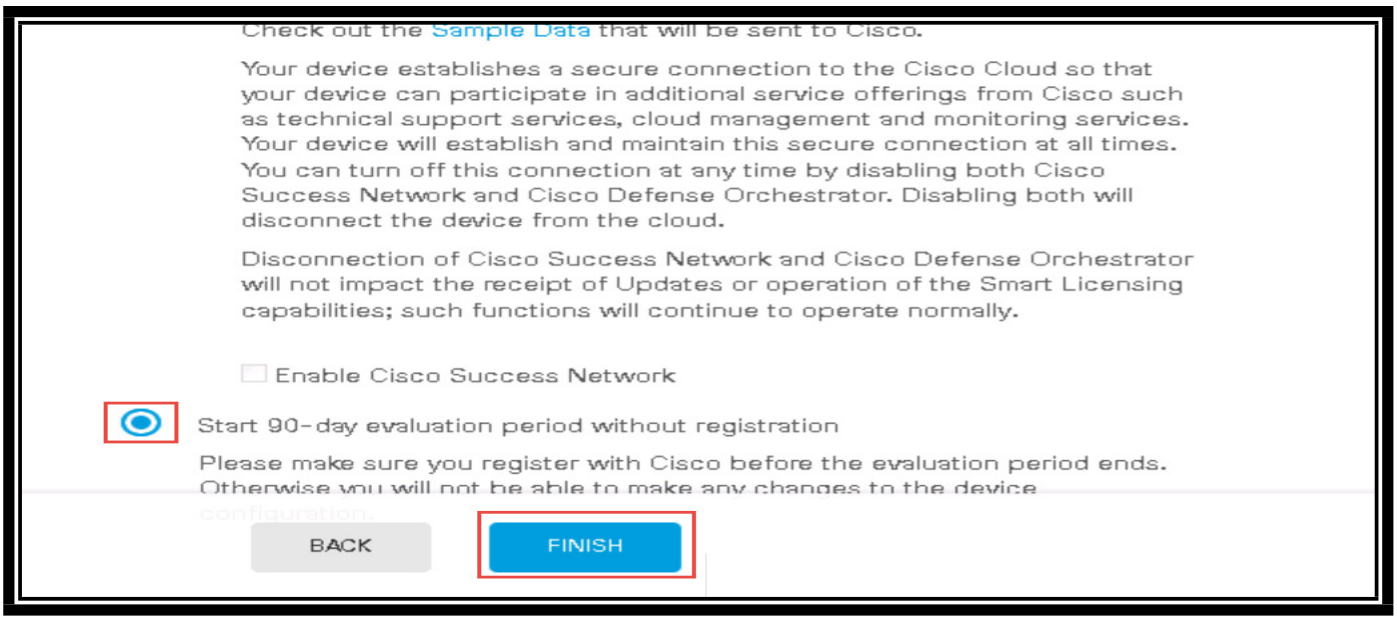
12. OpenDNS サーバを使用して、管理インターフェイスを設定します。
13. ターシャリ サーバ **198.18.128.1** をチェックします。
14. ホスト名 **NGFWBR2** をチェックし、[次へ（Next）] をクリックします。

15. www.cisco.com への接続に失敗したというメッセージが表示されてもそれは無視し、NTP サービスの設定に移動します。

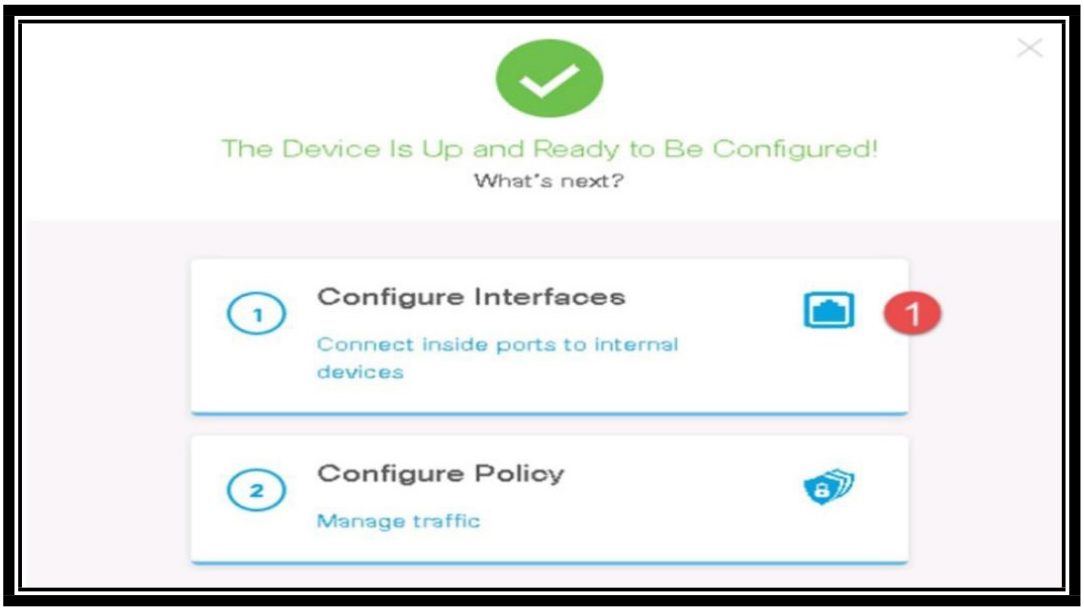
16. NTP サーバを手動で設定します。
    a. [タイム ゾーン（Time Zone）] で自分のタイム ゾーンを選択します。
    b. [NTP タイム サーバ（NTP Time Server）] で [手動入力（Manually input）] を選択します。
    c. IP アドレスに「**198.18.128.1**」を入力します。
    d. [次へ（Next）] をクリックします。



17. これで [スマート ライセンス（Smart License）] が表示されるので、[登録不要の 90 日間の評価期間を開始する（Start 90-day evaluation period without registration）] を選択します。

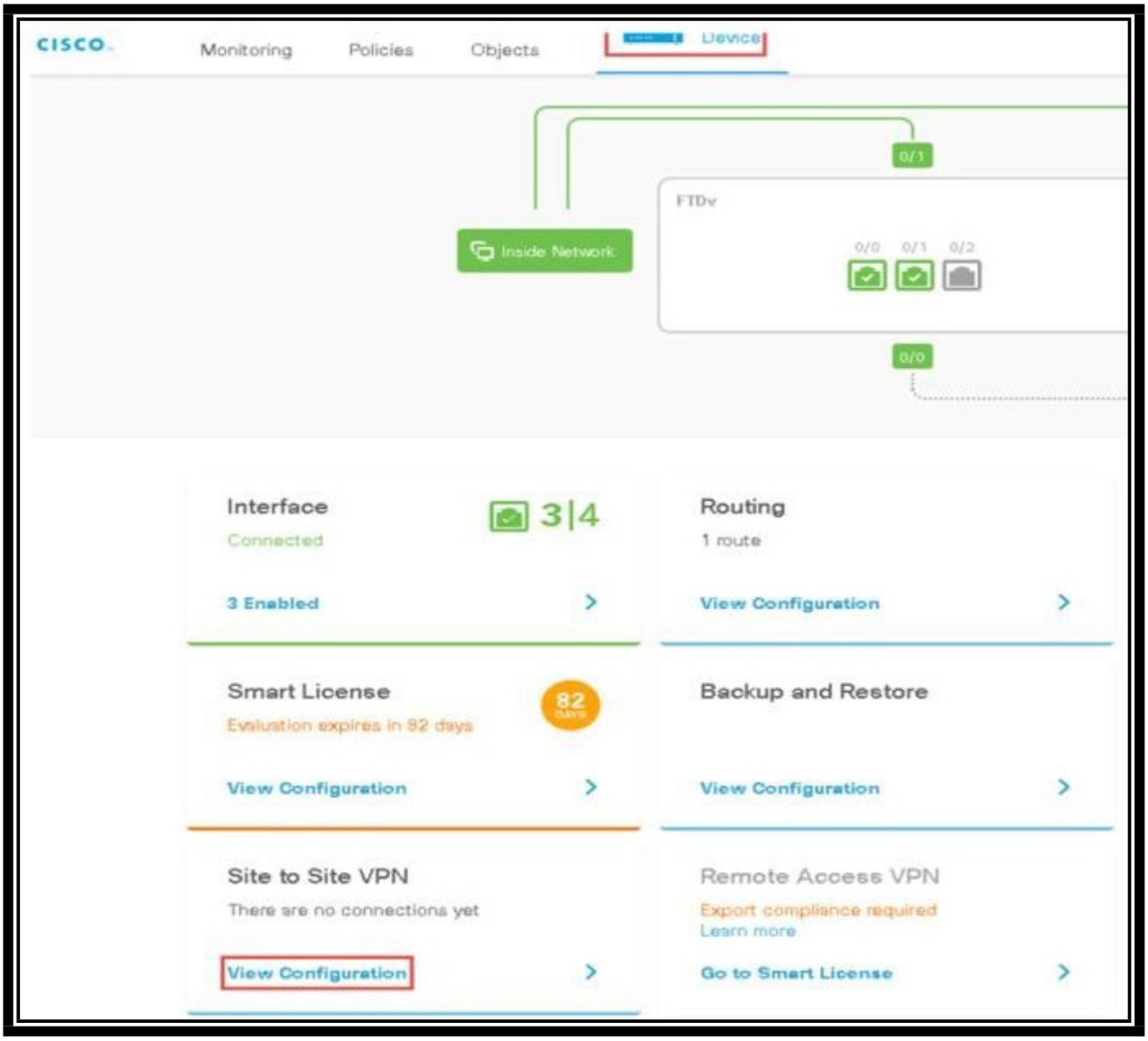


18. 次の画面で [インターフェイス（Interfaces）] または [ポリシー（Policy）] の設定を求められます。
19. [インターフェイス（Interfaces）] を選択して、画面を確認します。

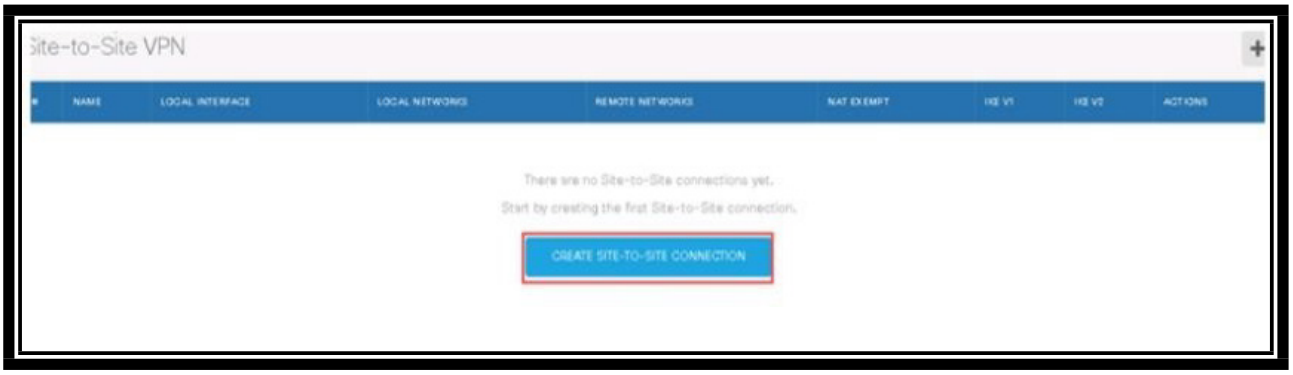


注: インターフェイス GigabitEthernet 0/1 が 192.168.45.1 であることを確認できます。また、外部インターフェイス GigabitEthernet 0/0 には手動で設定された外部インターフェイスがあることを確認できます。このデバイスには、後でサイト間 VPN を設定するために戻ります。

20. [デバイス（Device）] に移動し、[サイト間VPN（Site to Site VPN）] の [設定の表示（View Configuration）] まで下方向にスクロールします。

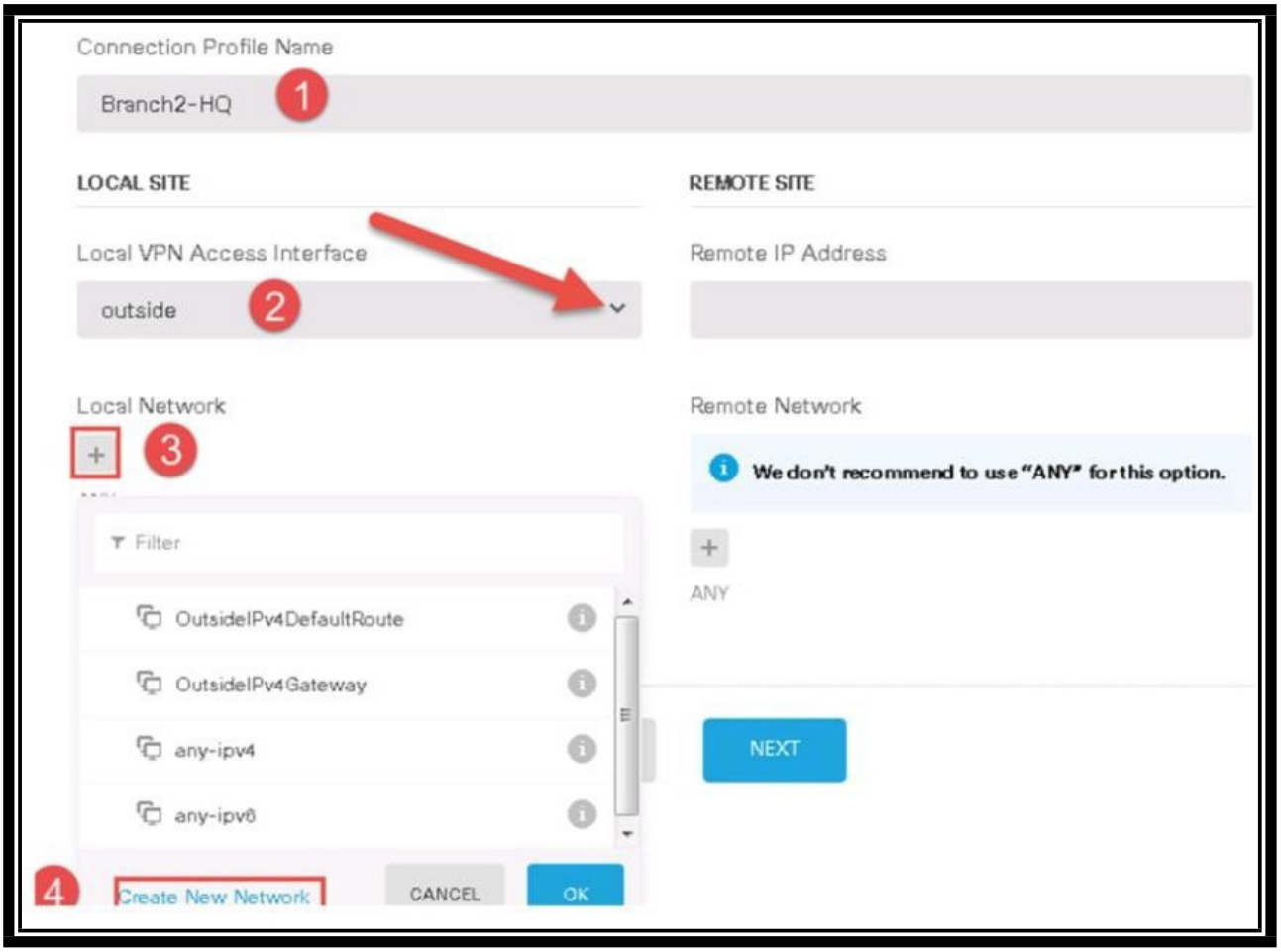


21. [サイト間接続を作成（Create Site-To-Site Connection）] をクリックします。



22. [名前（Name）] : **Branch2-HQ**
23. [ローカルVPNアクセスインターフェイス（Local VPN Access Interface）] : **outside**

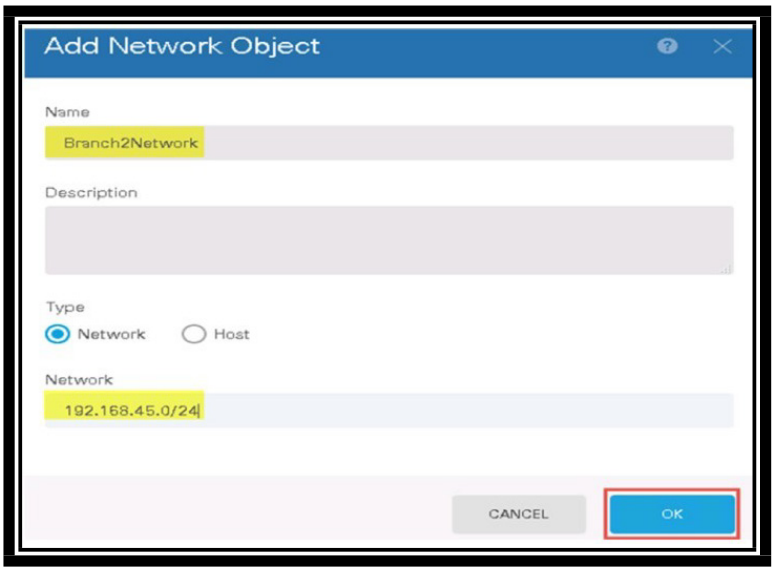
24. [ローカルネットワーク（Local Network）] で [+] をクリックし、[新規ネットワークの作成（Create New Network）] をクリックします。



a. ネットワーク オブジェクトの追加

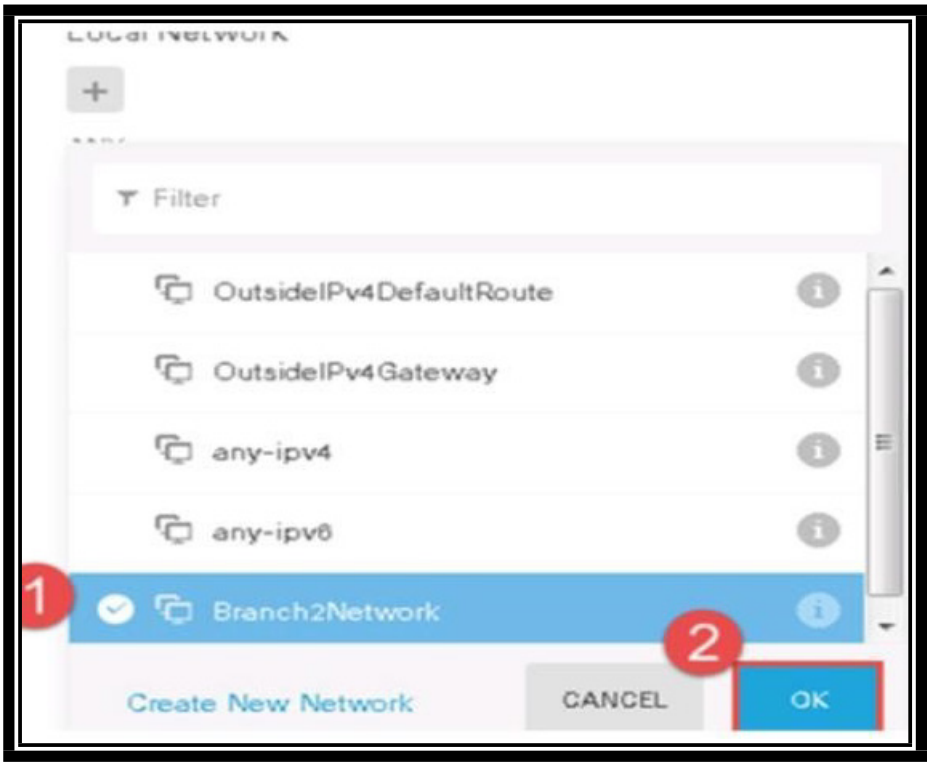
   i. [名前（Name）] : **Branch2Network**

   ii. [ネットワーク（Network）] に「**192.168.45.0/24**」と入力します。



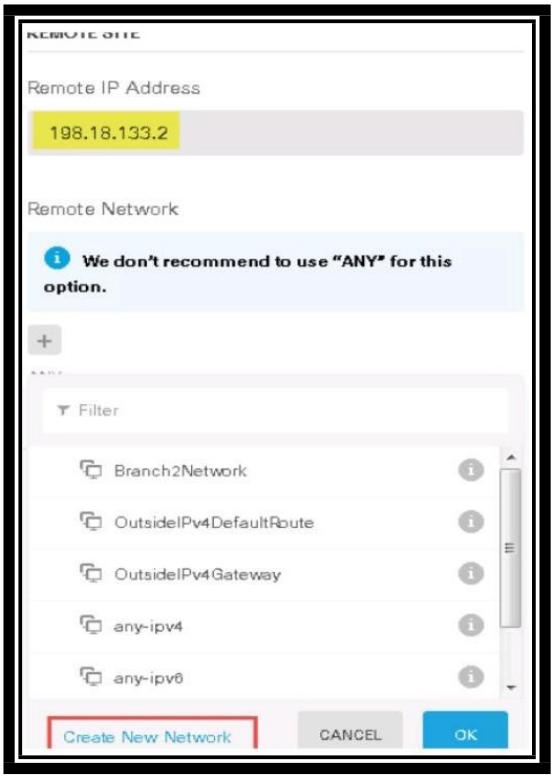
b. [OK] をクリックします。

25. 新しく作成したネットワークを選択し、[OK] をクリックします。

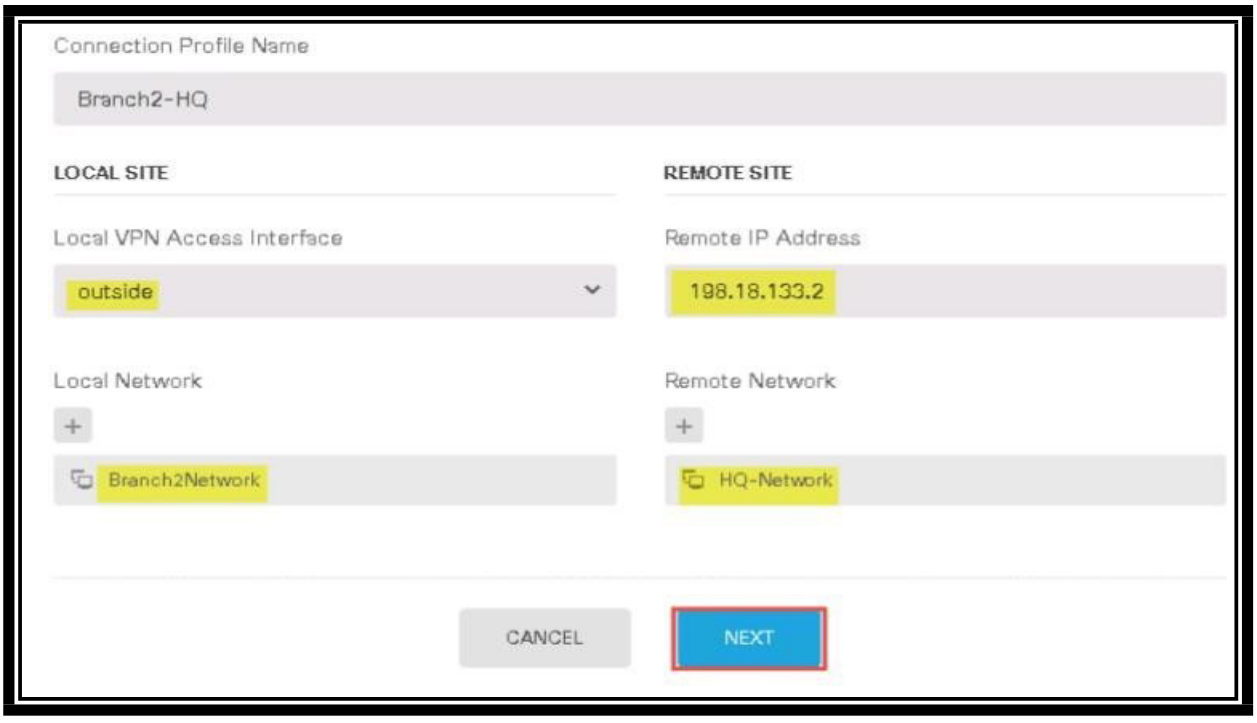


26. [リモートIPアドレス（Remote IP Address）] に「**198.18.133.2**」（NGFW1 の外部アドレス）と入力します。

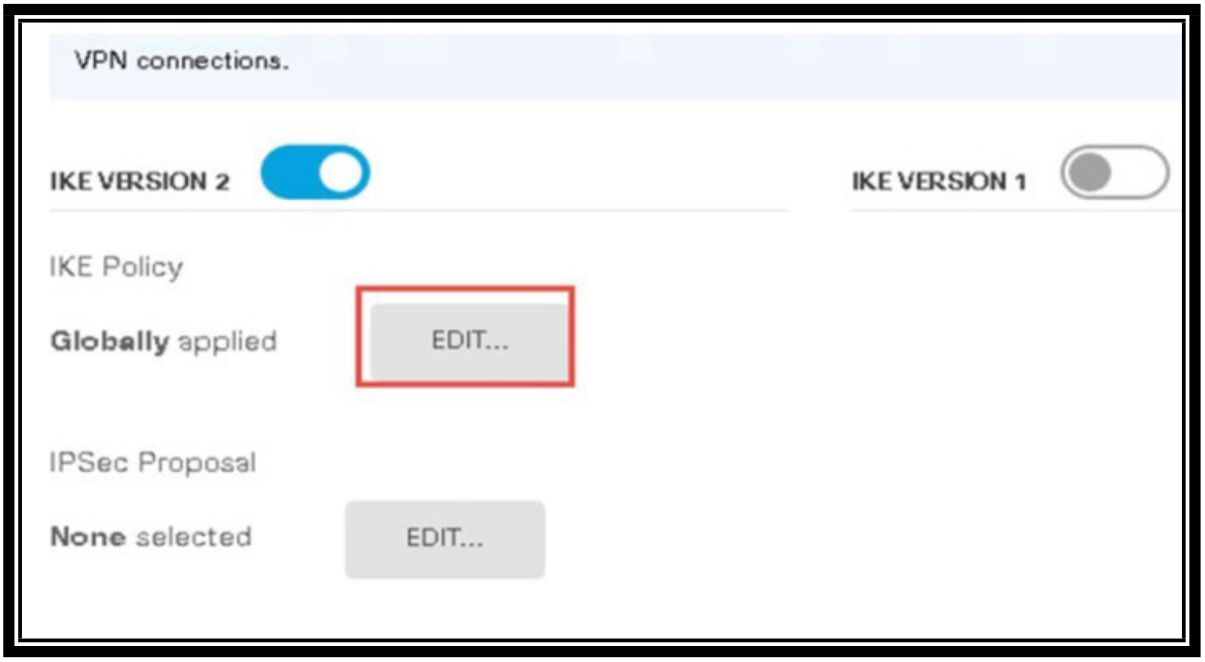
27. [リモートネットワーク（Remote Network）] でネットワーク オブジェクトを作成するには、[+] をクリックして [新規ネットワークの作成（Create New Network）] をクリックします。



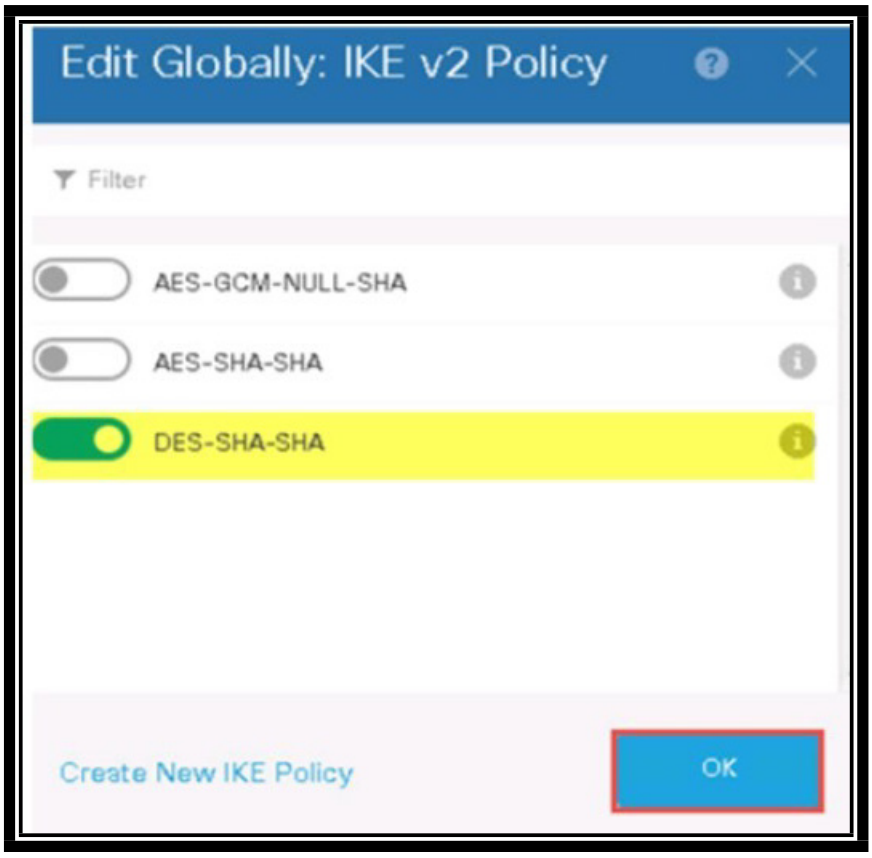
28. [名前（Name）]：**HQ-Network**
29. [ネットワーク（Network）]：198.19.10.0/24（社内ネットワーク）
30. HQ-Network を選択して [OK] をクリックします。
31. 接続プロファイルは次のようになります。



32. [IKEポリシー（IKE Policies）] で [編集（Edit）] をクリックします。



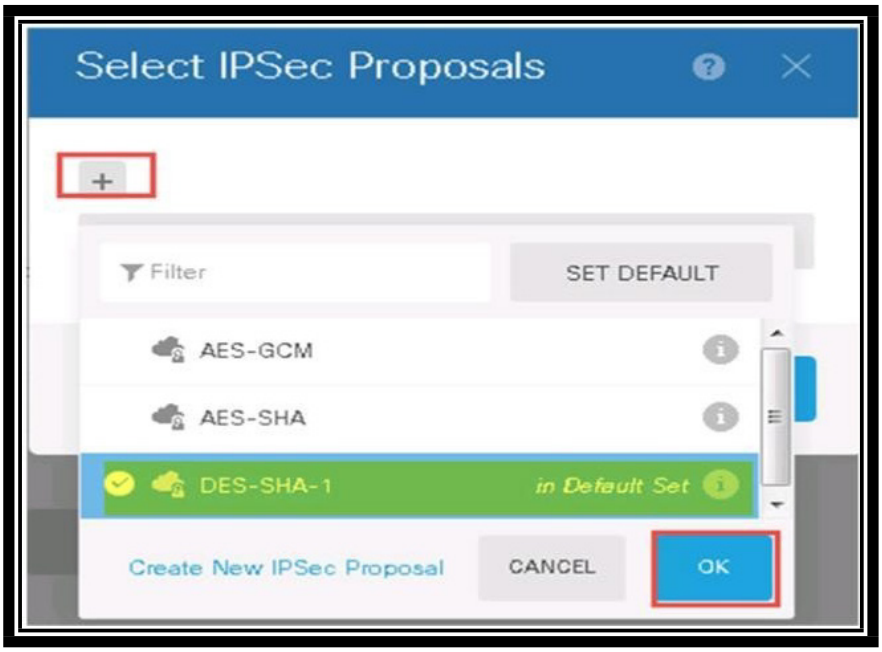
33. [DES-SHA-SHA] を選択して [OK] をクリックします。



34. [IPSecプロポーザル（IPSec Proposal）] で [編集（EDIT）] をクリックします。

35. [+] アイコンをクリックします。

36. [デフォルト設定（in Default Set）] となっている [DES-SHA-1] を選択し、[OK] をクリックします。



37. その他のオプション

    a. [ローカル事前共有キー（Local Pre-shared Key）]

        i. **C1sco12345**

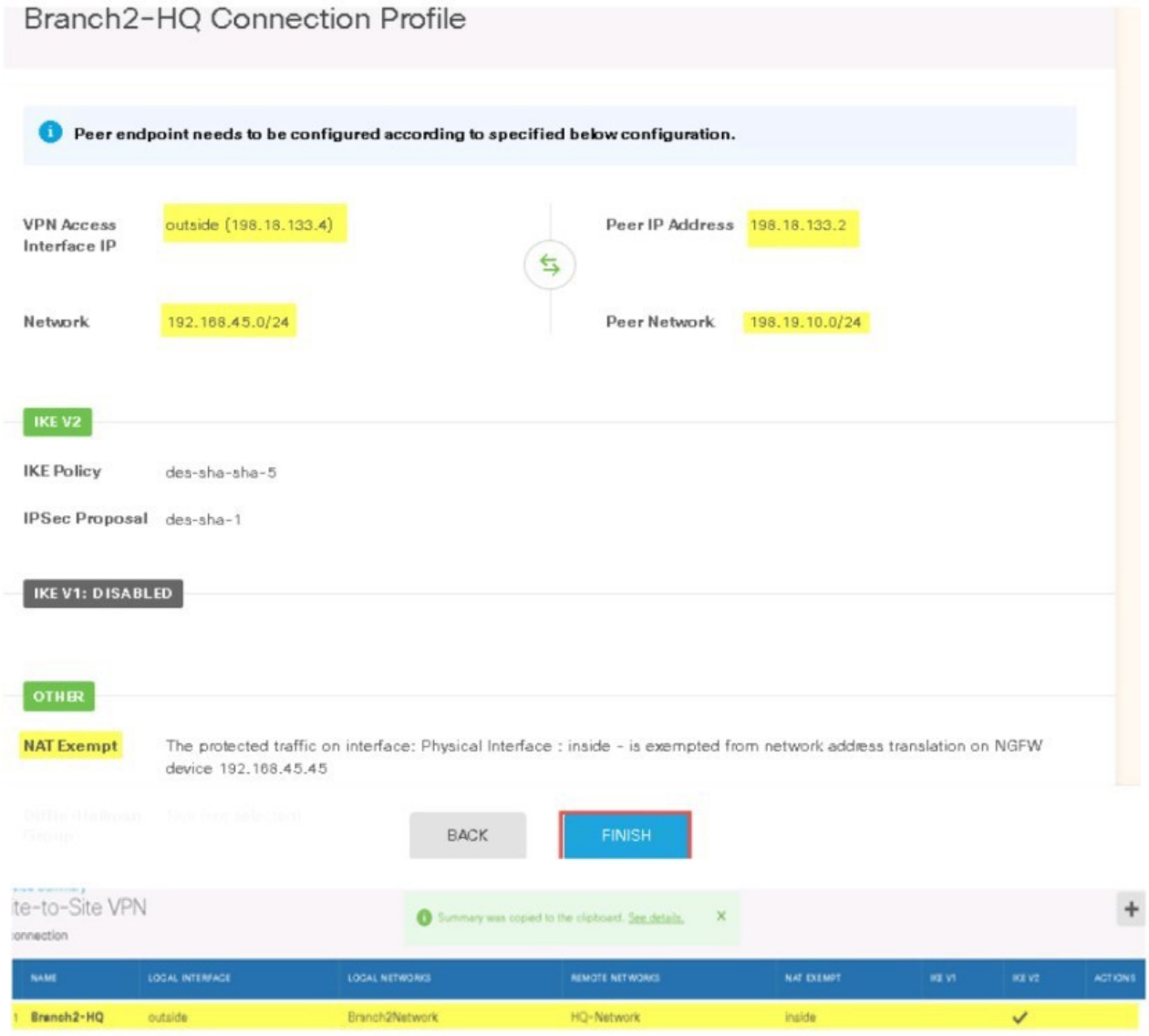
    b. [リモートピア事前共有キー（Remote Peer Pre-shared Key）]

        i. **C1sco12345**

    c. [NAT適用除外（NAT Exempt）] をクリックして、[内部インターフェイス（Inside Interface）] を選択します。

    d. [次へ（Next）] を選択します。

    e. 確認して [完了（Finish）] をクリックします。



38. FDM で ACP を構築し、インバウンド接続を許可します。
39. **変更の展開**

変更を導入して設定をテストする

1. **FMC で変更を導入し、導入が完了するまで待ちます。**
2. Jump PC で、 **NGFW1 NGFWBR1** への PuTTY 接続を開き、ユーザ名：**admin**、パスワード：**C1sco12345** でログインします。
3. **NGFW1 CLI** で「**show crypto ipsec sa peer 198.18.133.142**」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。

```
> show crypto ipsec sa peer 198.18.133.142

There are no ipsec sas
>
```

4. NGFWBR1 に移動して「**show crypto ipsec sa peer 198.18.133.2**」と入力します。接続はありません。

```
> show crypto ipsec sa peer 198.18.133.2

There are no ipsec sas
>
```

5. 内部 Linux サーバに対する PuTTY セッションを開き、ユーザ名：**root**、パスワード：**C1sco12345** でログインします。
6. 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。

```
root@inside ~]# ping branch
ING branch (198.19.11.200) 56(84) bytes of data.
4 bytes from branch (198.19.11.200): icmp_seq=2 ttl=64 time=48.0 ms
4 bytes from branch (198.19.11.200): icmp_seq=3 ttl=64 time=54.4 ms
4 bytes from branch (198.19.11.200): icmp_seq=4 ttl=64 time=56.1 ms
4 bytes from branch (198.19.11.200): icmp_seq=5 ttl=64 time=54.3 ms
4 bytes from branch (198.19.11.200): icmp_seq=6 ttl=64 time=24.4 ms
4 bytes from branch (198.19.11.200): icmp_seq=7 ttl=64 time=33.8 ms
4 bytes from branch (198.19.11.200): icmp_seq=8 ttl=64 time=64.7 ms
4 bytes from branch (198.19.11.200): icmp_seq=9 ttl=64 time=43.9 ms
4 bytes from branch (198.19.11.200): icmp_seq=10 ttl=64 time=54.4 ms
4 bytes from branch (198.19.11.200): icmp_seq=11 ttl=64 time=46.4 ms
4 bytes from branch (198.19.11.200): icmp_seq=12 ttl=64 time=54.3 ms
4 bytes from branch (198.19.11.200): icmp_seq=13 ttl=64 time=44.2 ms
4 bytes from branch (198.19.11.200): icmp_seq=14 ttl=64 time=54.7 ms
4 bytes from branch (198.19.11.200): icmp_seq=15 ttl=64 time=44.1 ms
C
-- branch ping statistics ---
5 packets transmitted, 14 received, 6% packet loss, time 14021ms
```

7. NGFW1 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。

```
> show crypto ipsec sa
interface: ISP-Side
    Crypto map tag: CSM_ISP-Side_map, seq num: 1, local addr: 198.18.133.2

      access-list CSM_IPSEC_ACL_1 extended permit ip 198.19.10.0 255.255.255.0 198.19.11.0 255.255.255.0
      local ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (198.19.11.0/255.255.255.0/0/0)
      current_peer: 198.18.133.142


      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 198.18.133.2/500, remote crypto endpt.: 198.18.133.142/500
      path mtu 1500, ipsec overhead 58(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
```

8. 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。
9. ユーザ名 **root**、パスワード **C1sco12345** でログインします。
10. 「**curl inside**」と入力します。これは成功するはずです。
11. 内部 Linux サーバに戻り、「**ping 192.168.45.225**」と入力します。これは成功するはずです。

```
root@inside:~
root@inside ~]# ping 192.168.45.225
ING 192.168.45.225 (192.168.45.225) 56(84) bytes of data.
C
-- 192.168.45.225 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 16999ms

root@inside ~]# ping 192.168.45.225
ING 192.168.45.225 (192.168.45.225) 56(84) bytes of data.
4 bytes from 192.168.45.225: icmp_seq=2 ttl=128 time=35.6 ms
4 bytes from 192.168.45.225: icmp_seq=3 ttl=128 time=23.2 ms
4 bytes from 192.168.45.225: icmp_seq=4 ttl=128 time=23.3 ms
4 bytes from 192.168.45.225: icmp_seq=5 ttl=128 time=33.5 ms
4 bytes from 192.168.45.225: icmp_seq=6 ttl=128 time=15.8 ms
4 bytes from 192.168.45.225: icmp_seq=7 ttl=128 time=54.0 ms
4 bytes from 192.168.45.225: icmp_seq=8 ttl=128 time=35.2 ms
4 bytes from 192.168.45.225: icmp_seq=9 ttl=128 time=46.8 ms
4 bytes from 192.168.45.225: icmp_seq=10 ttl=128 time=33.3 ms
4 bytes from 192.168.45.225: icmp_seq=11 ttl=128 time=33.2 ms
C
-- 192.168.45.225 ping statistics ---
1 packets transmitted, 10 received, 9% packet loss, time 10014ms
tt min/avg/max/mdev = 15.895/33.465/54.045/10.617 ms
root@inside ~]#
```

12. NGFW1 CLI に戻り、「**show ipsec sa peer 198.18.133.4**」と入力します。

```
> show crypto ipsec sa peer 198.18.133.4
peer address: 198.18.133.4
    Crypto map tag: CSM_ISP-Side_map, seq num: 2, local addr: 198.18.133.2

      access-list CSM_IPSEC_ACL_2 extended permit ip 198.19.10.0 255.255.255.0 192.168.45.0 255.255.255.0
      local ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.45.0/255.255.255.0/0/0)
      current_peer: 198.18.133.4


      #pkts encaps: 55, #pkts encrypt: 55, #pkts digest: 55
      #pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 55, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 198.18.133.2/500, remote crypto endpt.: 198.18.133.4/500
```

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. Jump PC からリモート デスクトップ フォルダを開きます。
    a. [外部PC（Outside PC）] をクリックします。
    b. ユーザ名：Administrator、パスワード：C1sco12345 でログインします。
    c. AnyConnect セッションを開始します。
        i Windows デスクトップの下部のトレイをクリックします。
        ii または、スタート メニューの検索バーに「Anyconnect」と入力します。
    d. [接続（Connect）] ボタンをクリックします（ngfw-outside.dcloud.local に接続するはずです）。
        i ユーザ名：Rita
        ii パスワード：C1sco12345
2. 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。
3. **[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。
4. [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。

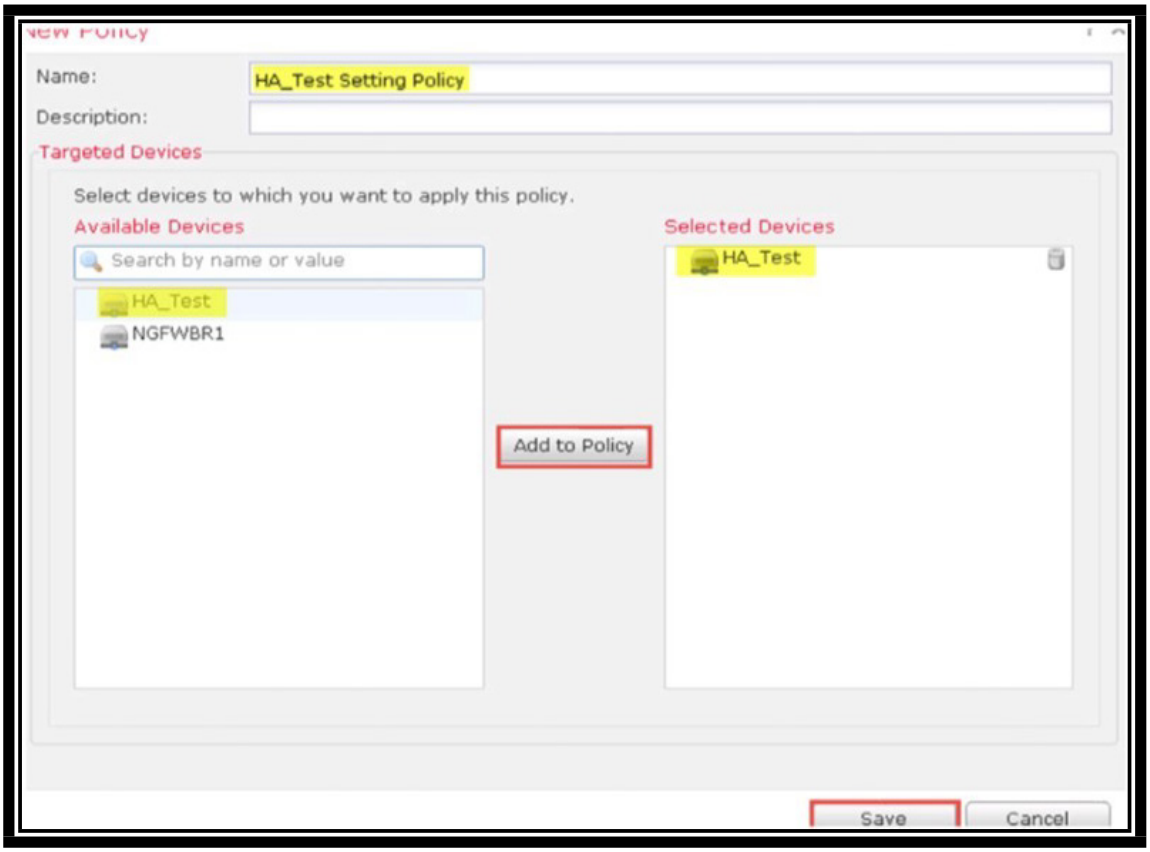
注：ネットワーク検出によって検出された、他のアクティブ セッションも表示される場合があります。たとえば、FTP セッションを通じて検出されたゲストが表示される場合です。簡略にするために、それらのセッションは上の図には含まれていません。ユーザ、およびユーザが検出された方法の詳細を確認するには、[分析（Analysis）] > [ユーザ（Users）] > [ユーザ（Users）] に移動します。

5. Outside-PC で、Rita がログアウトしていることを確認します。
6. 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。

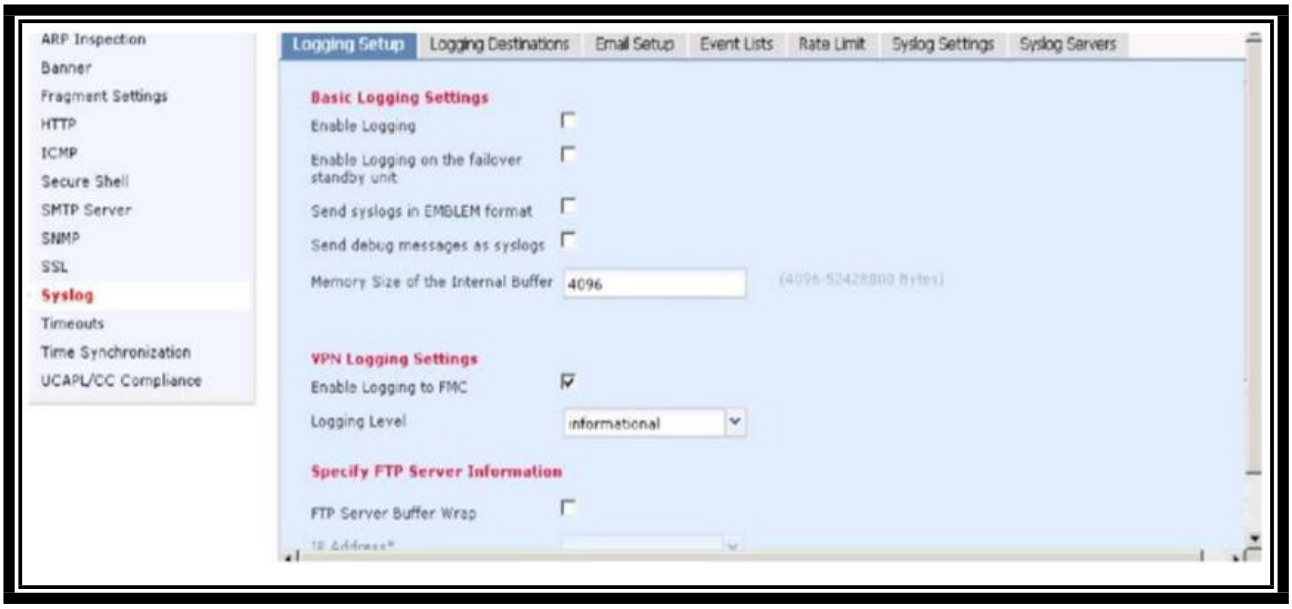
トラブルシューティング

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。NGFW1 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ていないことに注意してください。
2. 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「HA_Test Settings Policy」という名前を付けます。
    c. HA_Test 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。



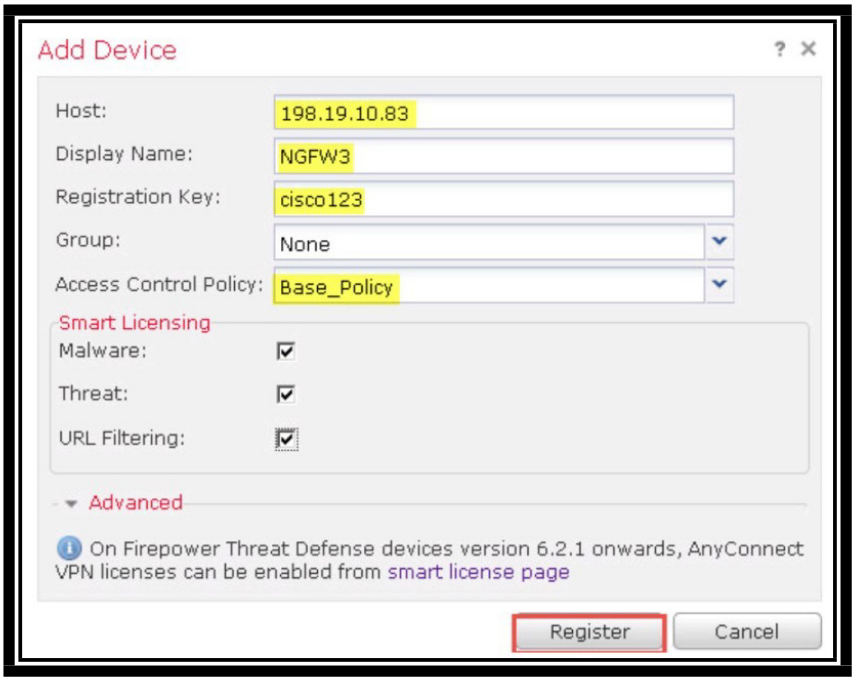
3. [保存（Save）] をクリックします。ポリシーが開き、編集できるようになります。
4. 左側のナビゲーション ペインで、[Syslog] を選択します。
    a. [VPNロギング設定（VPN Logging Settings）] で、ロギング レベルを [情報（informational）] に変更します。実稼働環境では、[エラー（errors）] または [アラート（alerts）] に設定することをお勧めします。
    b. [保存（Save）] をクリックします。



5. **HA_Test** の変更を導入します。
6. Outside-PC で、いくつかの VPN アクティビティを生成します。たとえば VPN セッションを接続または切断するアクティビティです。
7. FMC で、[デバイス（Device）] > [VPN] > [トラブルシューティング（Troubleshooting）] に戻ります。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。
8. **NGFW1** 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 ?

ピグテール登録に関するトラブルシューティング

1. Jump PC に移動し、**NGFW3** に対する PuTTY セッションを開きます。
    a. ユーザ名：**admin**、パスワード：**C1sco12345** でログインします。
    b. 「show managers」と入力します。
        i. マネージャの登録ステータスが保留として表示されます。
2. FMC Web ページに移動します。
    a. [デバイス（Devices）] > [デバイス管理（Device Management）] に移動し、[追加（Add）] > [デバイス（Device）] の順にクリックします。



3. デバイスの追加
    a. [ホスト（Host）]：198.19.10.83
    b. [表示名（Display Name）]：NGFW3
    c. [登録キー（Registration Key）]：cisco123
    d. [アクセスコントロールポリシー（Access Control Policy）]：Base_Policy
    e. ライセンス
        i. [マルウェア（Malware）] をチェック
        ii. [脅威（Threat）] をチェック
        iii. [URLフィルタリング（URL Filtering）] をチェック
    f. [登録] をクリック
4. 登録が失敗します。
5. 「**ping system fmc.dcloud.local (198.19.10.120)**」と入力して、**NGFW3** から FMC に到達できるかを確認します。
6. NGFW3 で「**Pigtail ALL**」と入力します。
    a. Enter を数回押します。
    b. 登録ボタンを再度押します。
    c. **NGFW3** からの出力を確認します。

注：PuTTY セッションで出力を確認することも、Jump PC の Notepad++ に出力をコピーして確認することもできます。

7. エラー メッセージが表示されているかどうか確認します（出力に認証エラーが示されている場合があります）。
8. Ctrl+C を押してプロンプトに戻ります。

9. 「**sftunnel-status**」と入力します。
    a. トンネルが作成されていないことを確認できます。

注：認証エラー（*hint check password*）が見つからない場合、**NGFW3** のコマンド プロンプトで「**expert**」と入力します。

10. 「cat /etc/sf/sftunnel.conf」と入力します。

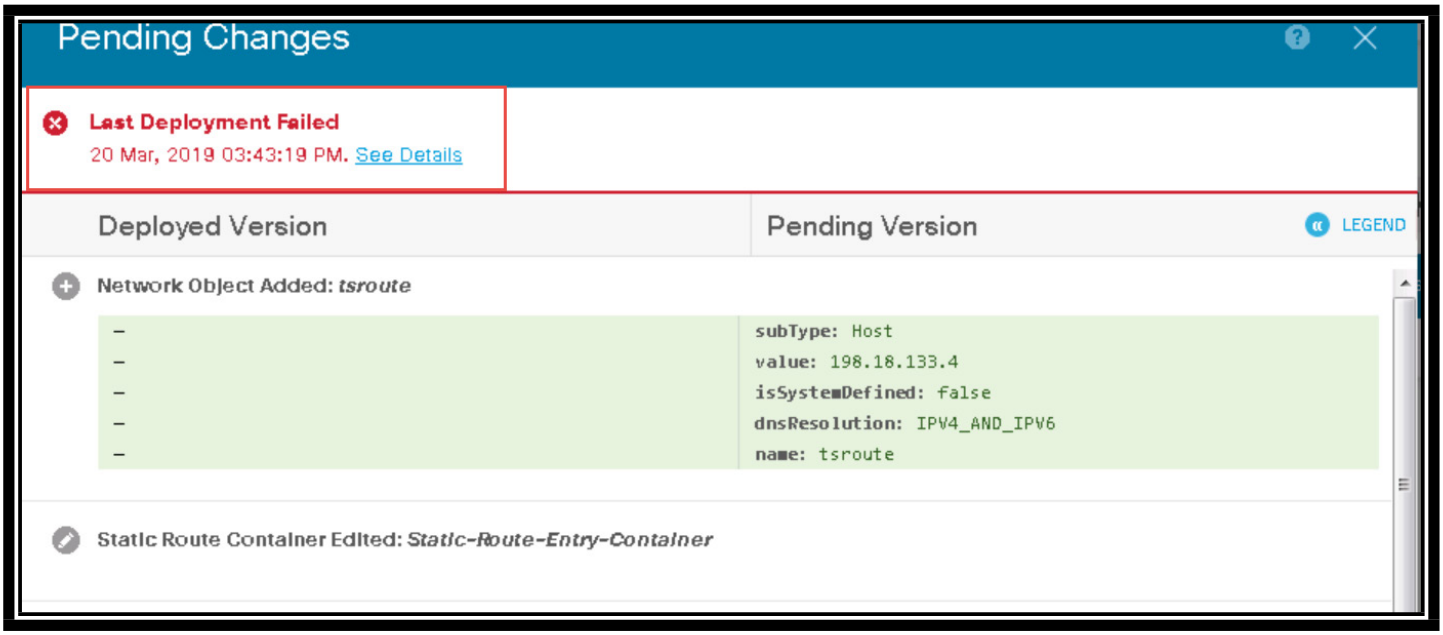
11. exit と入力します。
12. 「show managers」と入力すると、登録が保留中であることがわかります。
13. FMC の Web ページに戻り、エラー メッセージに対して [OK] をクリックします。
14. sftunel.conf ファイルの内容に合わせて登録キーを変更し、[登録（Register）] をクリックします。

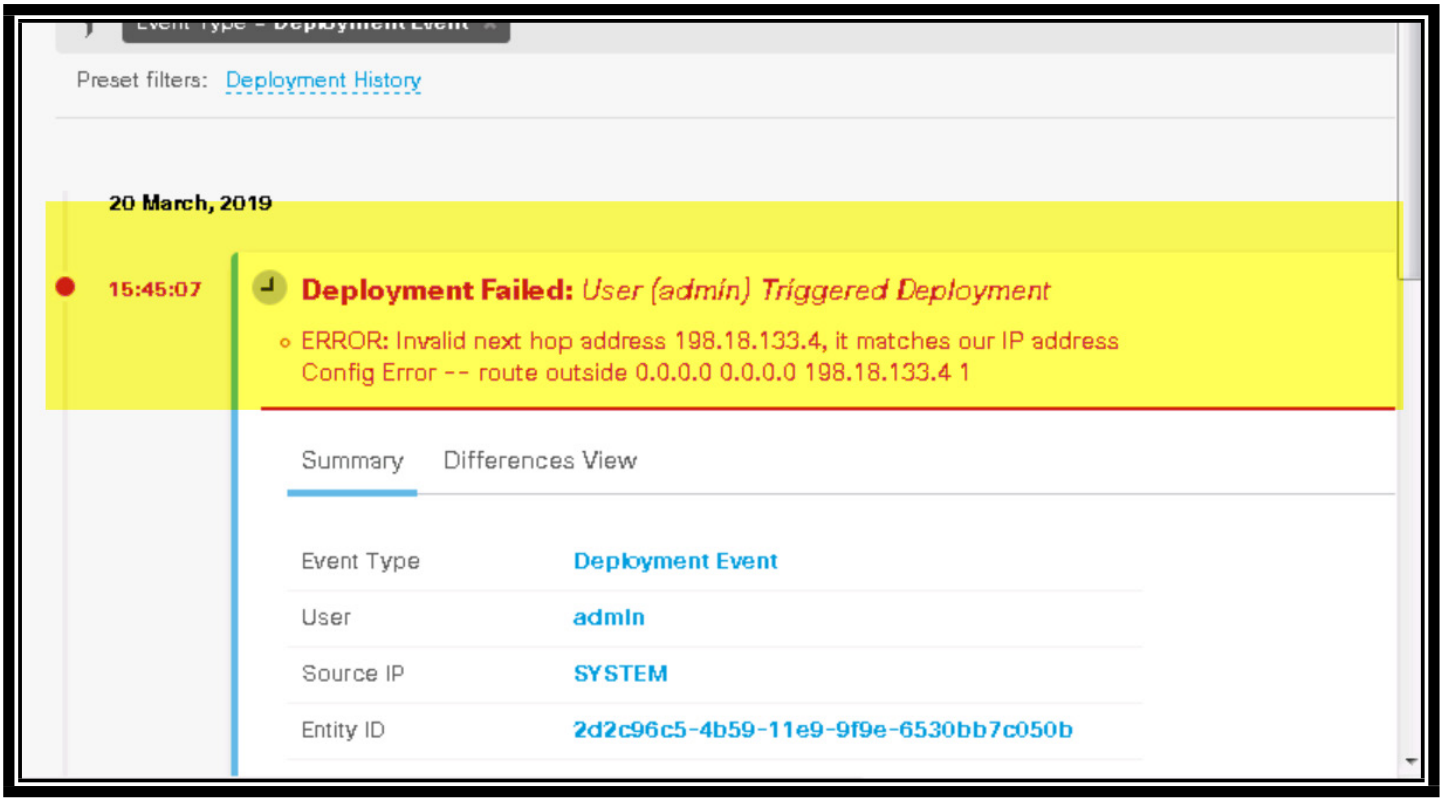
注：「pigtail」と入力すると、pigtail を再度オンにして、登録プロセスを表示することができます。

FDM 登録に関するトラブルシューティング

1. Jump PC のリモート デスクトップ フォルダに移動します。
    a. Wkstrbr2 をクリックします（パスワード：C1sco12345）。
    b. Firefox ブラウザをクリックし、FDM（https://192.168.45.45）を開きます。
    c. ユーザ名：admin、パスワード：C1sco12345! で、**FDM** にログインします。
2. [デバイス（Device）] > [ルーティング（Routing）] > [設定の表示（View Configuration）] の順にクリックします。
3. [アクション（Actions）] 列に移動します。
4. 1 行目の**鉛筆**アイコンをクリックします。
5. ゲートウェイの**ドロップダウン矢印**をクリックします。

6. [新規ネットワークの作成（Create New Network）] を選択します。
    a. [名前（Name）] : **tsroute**
    b. [ホスト（Host）] : **198.18.133.4**。[OK] をクリックします。
7. [ゲートウェイ（Gateway）] で、新しく作成されたゲートウェイ **tsroute** を選択します。
8. [インターフェイス（Interface）] で **outside** を選択します。
9. [OK] をクリックします。
10. [展開（Deploy）] をクリックします。
11. 導入が完了するまで待ちます。
12. [ステータス（Status）] に [失敗（Failed）] と表示されます。
13. クリックすると詳細が表示されます。





14. ネクスト ホップ アドレスに関するエラーが表示されます。
    a. FDM に戻って問題を修正します。

パケット トレーサとパケット キャプチャを使用したトラブルシューティング

1. パケット トレーサを使用する場合
    a. 特定のポート宛のトラフィックが Lina Data パスと Snort によって許可されていることを確認します。
        i. セキュリティ インテリジェンス（IP レピュテーション）
        ii. L3/L4 IPS 侵入ルール
    b. パケット トレーサが現在**機能しない**（L7 パケットをエミュレートできないため）
        i. ID ベースのルール
        ii. ii. L7 関連（SI DNS/URL、App ID、ファイル ポリシー、L7 侵入ルール）

パケット トレーサ ラボ

1. FMC で、[ポリシー（Policies）] > [アクセスコントロール（Access Control）] に移動し、Base_Policy を編集します。
2. [新規ルールの追加（Add New Rule）] をクリックします。
    a. [名前（Name）] : Packet-Trace Rule
    b. ルール 1 の上位のルールを設定します。
    c. [アクション（Action）] で [ブロック（Block）] または [ブロックしてリセット（Block with reset）] を選択

d. [ゾーン（Zones）]：[送信元ゾーン（Source Zone）]：InZone、[宛先ゾーン（Destination Zone）]：Outzone

e. [ネットワーク(Networks)]:[送信元ネットワーク(Source Networks)]:[MainOfficenetwork]、[宛先ネットワーク(Destination Networks）]：any-ipv4

f. [アプリケーション（Applications）]：[使用可能なアプリケーション（Available Applications）] に「ICMP」と入力し、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] を選択し、[ルールに追加（Add to Rule）] をクリックします。

g. [使用可能なアプリケーション（Available Applications）] に「FTP」と入力し、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] を選択して、[ルールに追加（Add to Rule）] をクリックします。

h. [ロギング（Logging）] をクリックします。

   i. [接続開始時にロギング（Log at Beginning of Connections）] をクリックします。

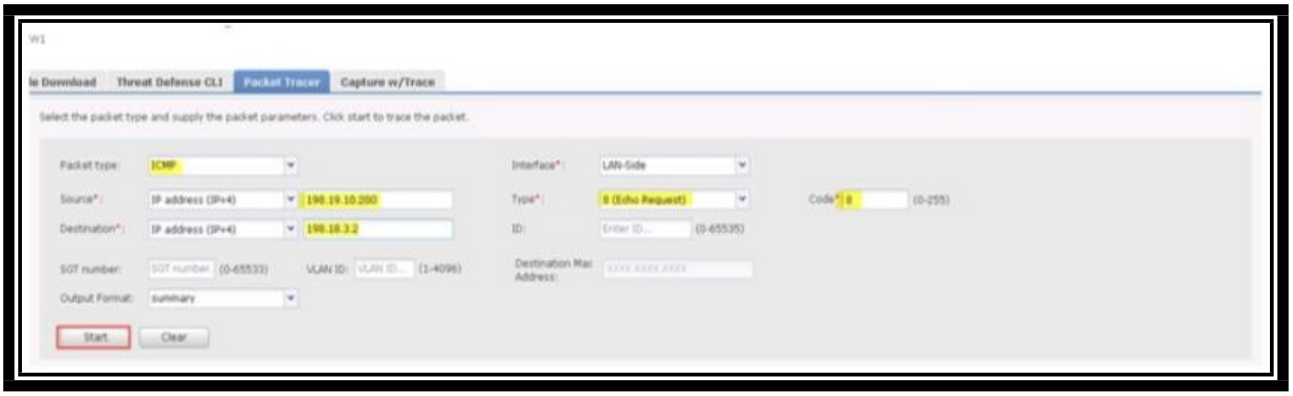
i. [追加（Add）] をクリックします。

j. [保存して導入（Save and Deploy）] をクリックして **HA_Test** に導入します。

注：ここでは実稼働環境の **ICMP と FTP** に関連するすべてのアプリケーションを選択しましたが、ブロックする特定のアプリケーションをより細かく指定できます。

3. ユーザ名：**admin**、パスワード：**C1sco12345** で、**NGFW1** への PuTTY セッションを開きます。
4. 「**packet-tracer input LAN-Side icmp 198.19.10.200 8 8 198.18.133.200**」と入力します。
   a. フェーズを確認すると、パケットが SNORT に渡されてさらに処理が進められたことがわかります。
   b. SNORT で、ブロックしてリセットするルール ID が使用され、パケットのドロップが指示されたことを確認できます。
5. 次に FMC で Packet-Trace コマンドを確認します。
6. [デバイス（Devices）] > [デバイス管理（Device Management）] > [NGFW1] に移動し、**トラブルシューティング** アイコンをクリックします。

7. [高度なトラブルシューティング（Advanced Troubleshooting）] をクリックします。
8. パケットトレーサを選択します。



a. [パケット タイプ（Packet Type）]：**ICMP**

b. [インターフェイス（Interface）]：**LAN-Side**

c. [送信元（Source）] : **198.19.10.200**

d. [タイプ（Type）] : **8（エコー要求）（8 (Echo Request)）**、[コード（Code）] : **8**

e. [宛先（Destination）] : **198.18.133.42**

f. [スタート（Start）] をクリックします。

注：ウィンドウに表示されている **NGFW1** のコマンド ラインの結果と同じ結果が得られます。

9. **FTP** に対するパケット トレーサをセットアップします。

   a. [パケット タイプ（Packet Type）] : **TCP**

   b. [送信元（Source）] : **198.19.10.200**

   c. [送信元ポート（Source Port）] : **1111**

   d. [宛先（Destination）] : **198.18.133.200**（外部 Linux Server）

   e. [宛先ポート（Destination Port）] : **FTP**

   f. [クリア（Clear）] をクリックします。

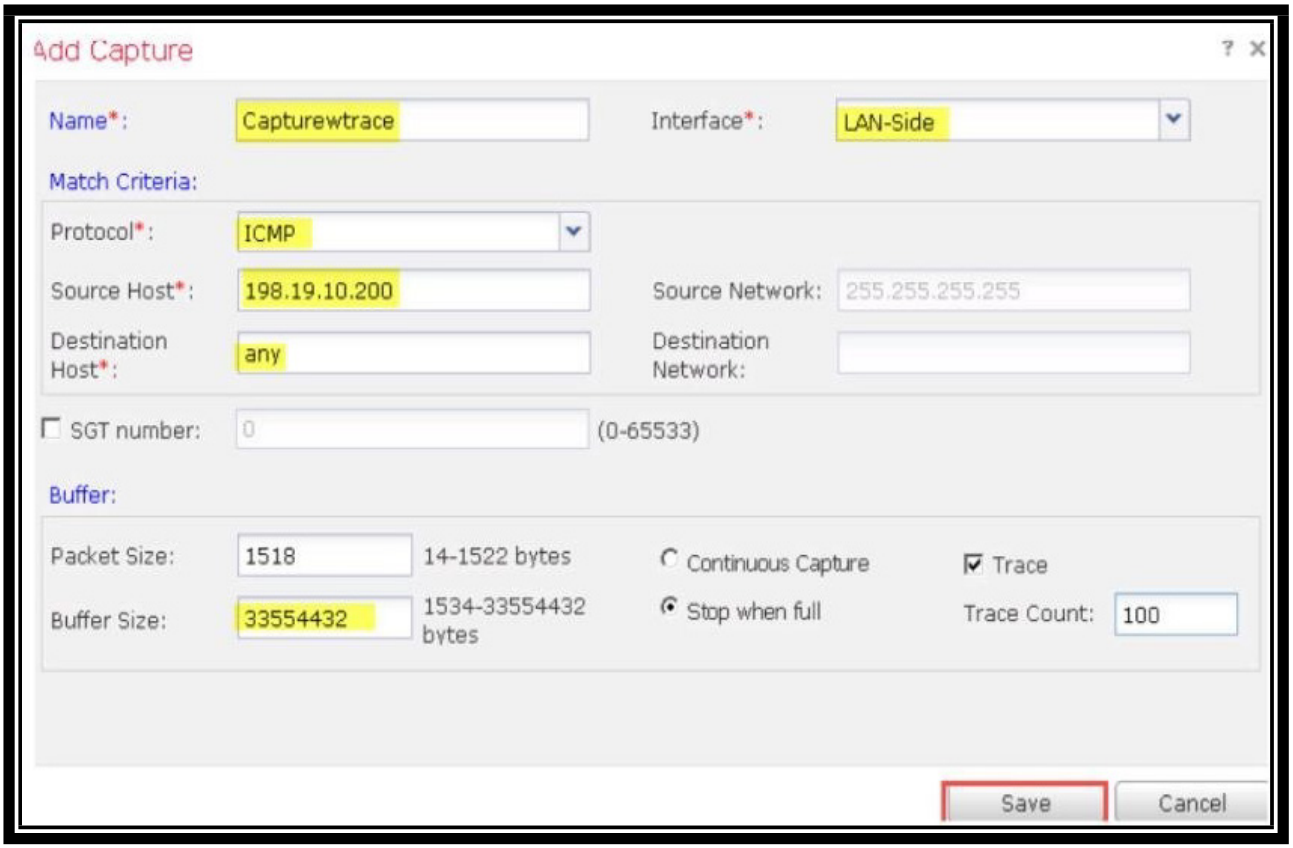
   g. [スタート（Start）] をクリックします。

注：フェーズ 2 は作成したルールのチェック中です。**フェーズ 14** では、SNORT でルールが確認され、パケットを送信すると判断されました。パケットの最初の部分は送信されますが、以降のパケットは送信されません。これをテストするに、Jump PC に移動して**内部 Linux サーバに対するセッションを開き、「ftp outside」と入力します。プロンプトが表示されたら guest でログインします。**コマンドに対して管理接続がないことを示すメッセージが表示されます。トランスポート エンドポイントが接続されていません。[接続イベント分析（Analysis Connection Events）] に移動し、**FTD がブロックされ、リセットされたこと**を確認します。

キャプチャ（トレース付き）ラボ

注：トラフィック キャプチャには、**Lina ベースと Snort ベース**の 2 つのタイプがあります。

1. Lina レベル：**capture**
2. SNORT レベル：**capture-traffic**

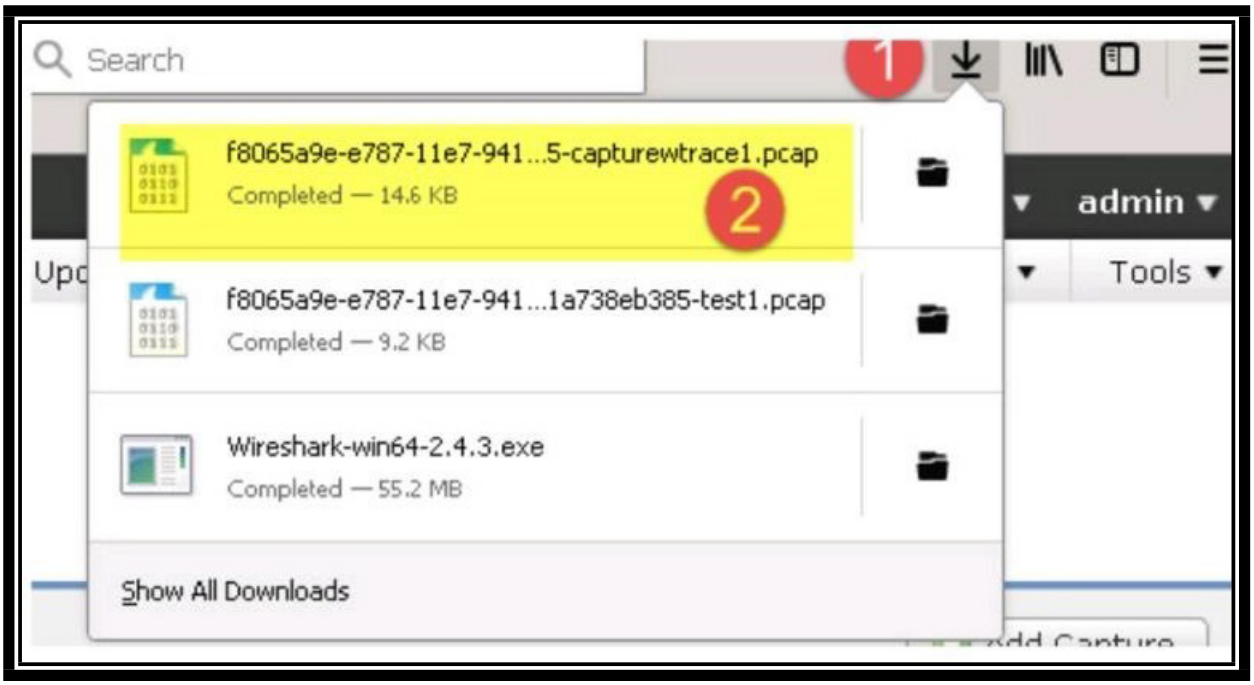


3. [デバイス（Devices）] > [デバイス管理（Device Management）] に移動し、**NGFW1** のトラブルシューティング アイコンをクリックします。
4. [高度なトラブルシューティング（Advanced Troubleshooting）] をクリックします。
5. [キャプチャ（トレース付き）（Capture w/Trace）] をクリックします。
6. [キャプチャの追加（Add Capture）] をクリックします。
    a. [名前（Name）]：Capturewtrace
    b. [インターフェイス（Interface）]：[LAN-Side]
    c. [プロトコル（Protocol）]：ICMP
    d. [送信元ホスト（Source Host）]：198.19.10.200（内部 Linux サーバ）
    e. [宛先ホスト（Destination Host）]：any
    f. [バッファサイズ（Buffer Size）]: 33554432（32 MB）
    g. [トレース数（Trace Count）]：100
    h. 保存（Save）

注：ICMP を拒否するアクセス ポリシーを削除していないため、ping が失敗しますが、パケットは表示されます。また、ファイルを PCAP 形式でこのラボの Wireshark **にエクスポートできます。**

7. Jump PC に移動し、内部 Linux サーバで「**ping outside**」と入力します。
8. 約 10 秒経過してもパケット表示ウィンドウに情報が表示されない場合は、更新ボタンをクリックします。

9. **パケットが表示されたら、ping を停止します。**
10. 作成したパケット キャプチャについて [保存（Save）] アイコンをクリックします。
    a. ファイルを PCAP 形式で保存します。
11. プロンプトが表示されたら [ファイルの保存（Save File）] を選択し、[OK] をクリックします。
12. Firefox のダウンロード矢印から、ダウンロードしたファイルを選択します。



13. ブラウザを最小にすると、**Wireshark** で開いたファイルが表示されます。
14. メッセージには**管理上フィルタが適用されている**ことに注意してください。

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

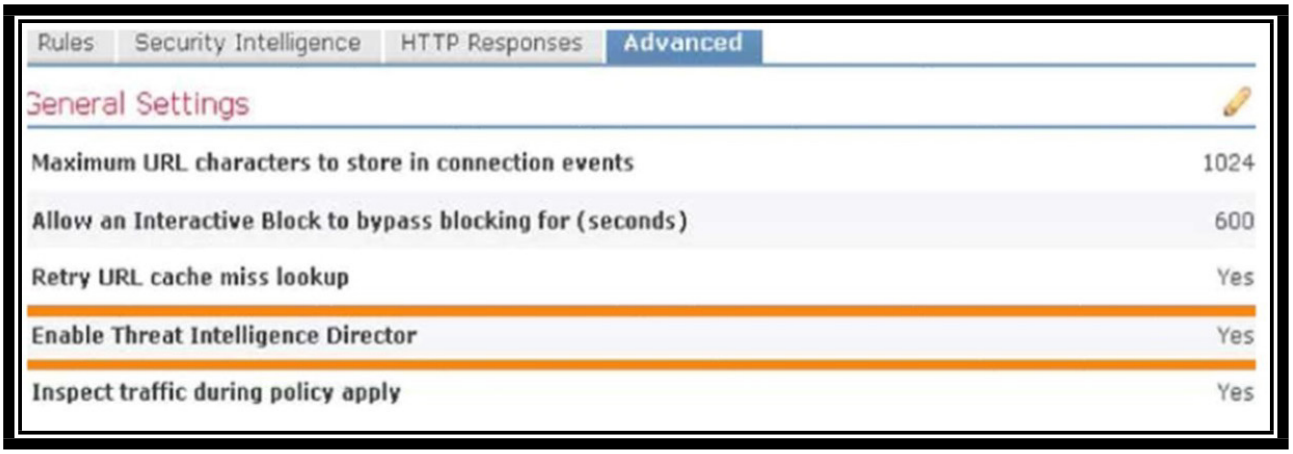
この演習は、次のタスクで構成されています。

- 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。
- デフォルトで Threat Intelligence Director が有効になっています。[ポリシー（Policies）] > [アクセスコントロール（Access Control）] に移動し、[詳細（Advanced）] のポリシーで確認できます。



STIX ファイル：シンプルなインジケータも複雑なインジケータも記述できる XML ファイルです。ファイルを取得する方法には次の 3 つがあります。

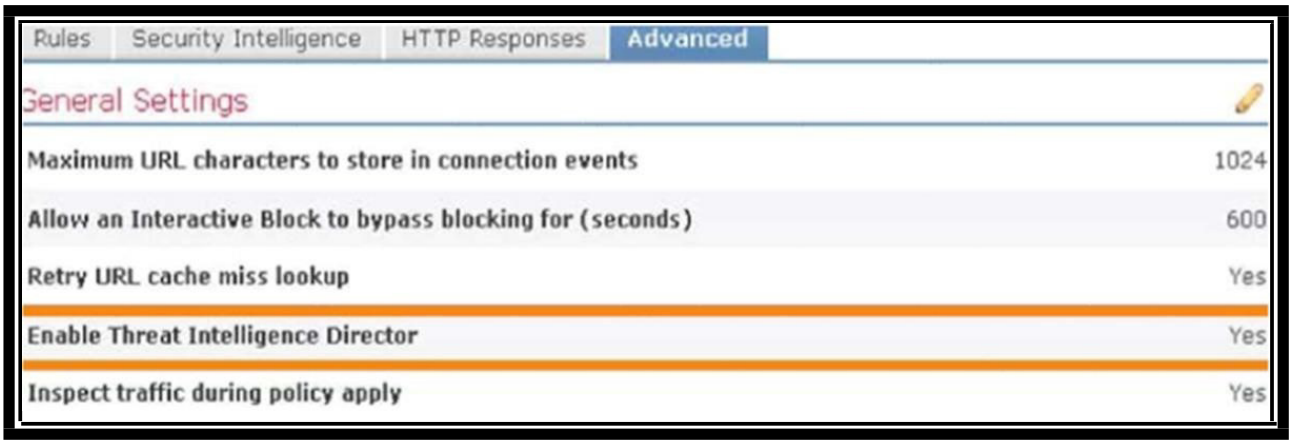
- FMC UI が実行されているコンピュータからアップロードする
- リモート Web サーバの URL から取得する
- TAXII フィードから取得する（STIX ファイルのみ）

この演習の目的は、CTID を設定し、テストすることです。

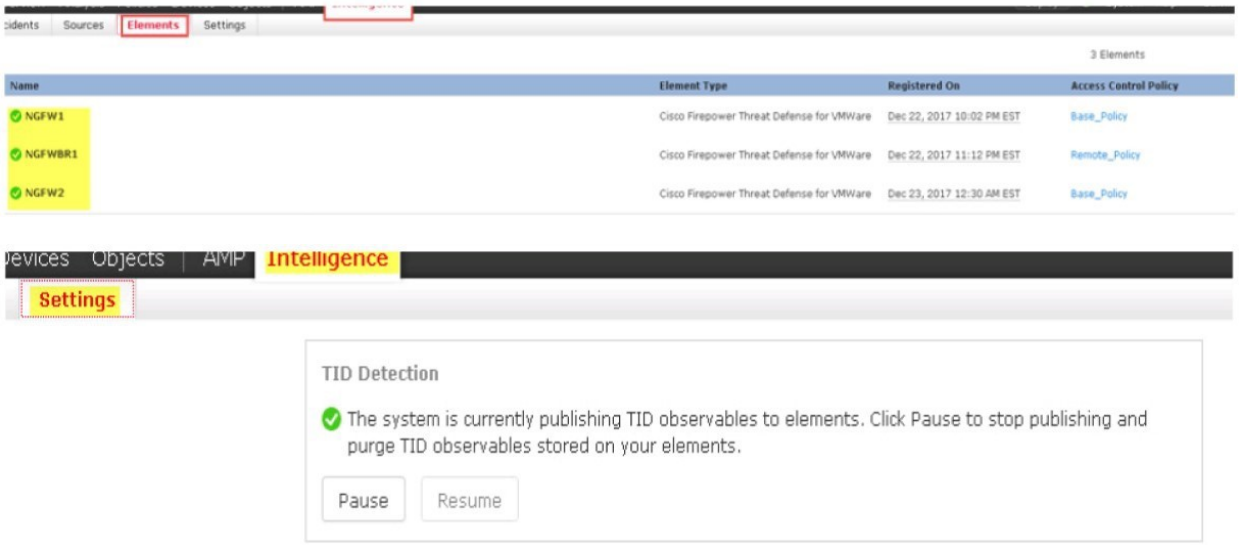
手順

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（Advanced）] タブを選択します。この詳細設定を使用して、アクセス ポリシー レベルで CTID を有効または無効にすることができます。



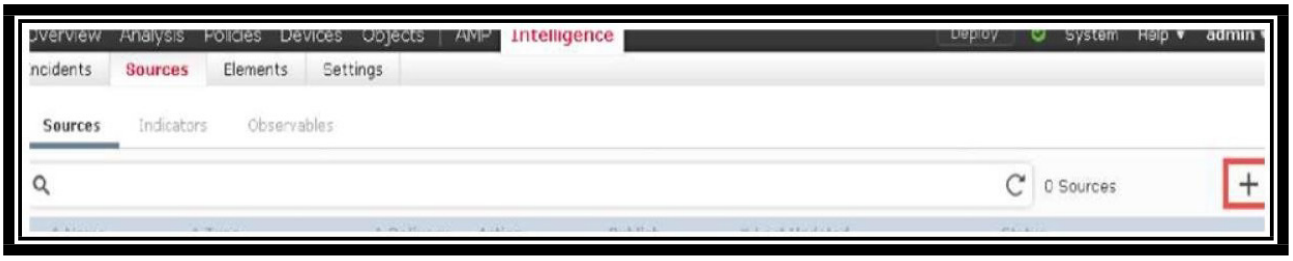
4. [インテリジェンス（Intelligence）] > [要素（Elements）] に移動します。
5. NGFW1 が要素になっていることを確認します。これは、CTID が、Web サーバから取得した STIX ファイルから監視対象を抽出し、NGFW1 にパブリッシュできることを意味します。



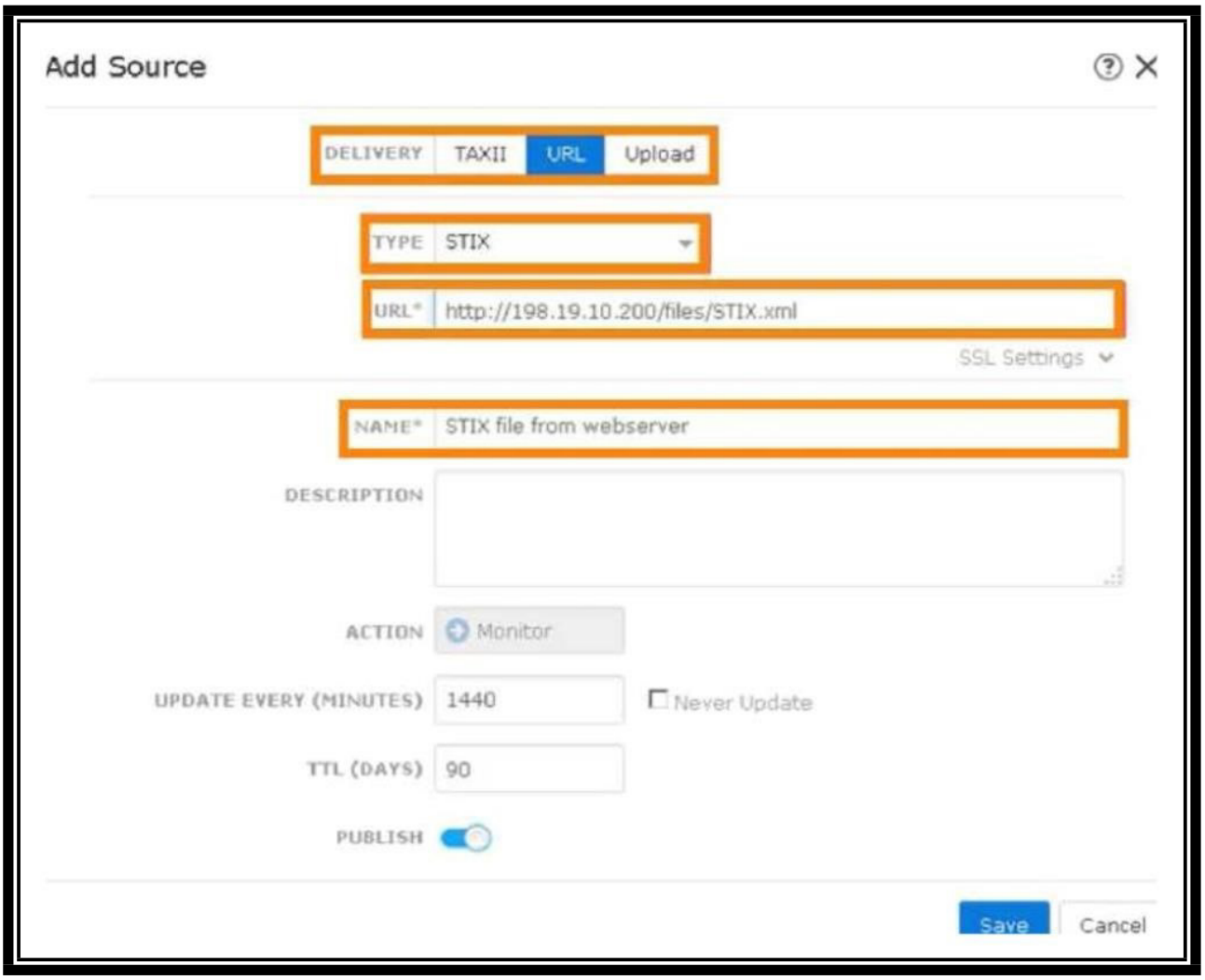
注：CTID はグローバルで有効または無効にすることができます。[一時停止（Pause）] をクリックすると、すべての要素に対する CTID のパブリッシュが停止されます。

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

7. 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。



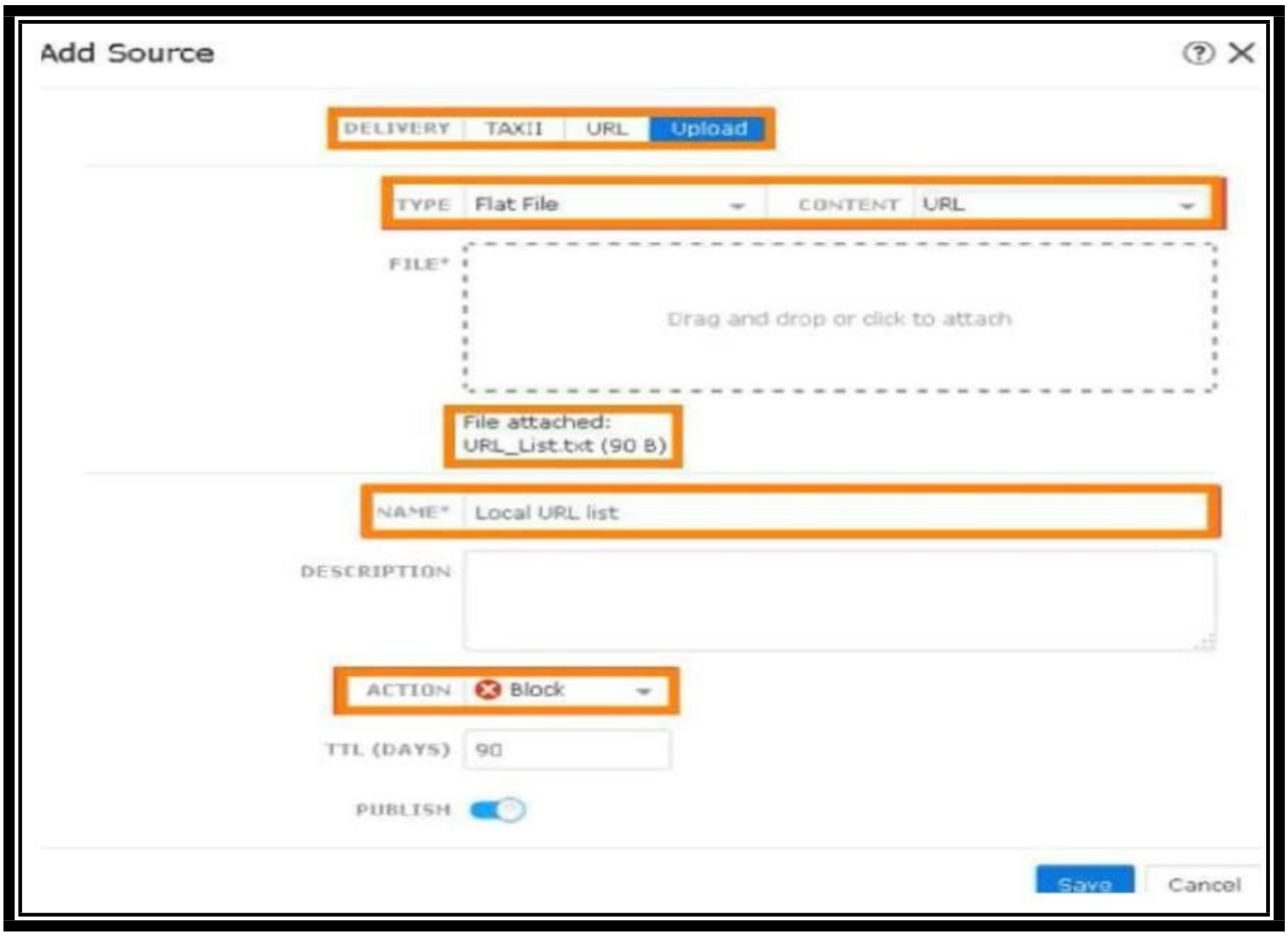
8. [配信（DELIVERY）] で [URL] を選択します。
9. [タイプ（TYPE）] で、[STIX] が選択されていることを確認します。
10. [URL] に「http://198.19.10.200/files/STIX.xml」と入力します。
11. [名前（NAME）] に「STIX file from Webserver」と入力します。



12. [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。

13. 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。
14. 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。
15. [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。
16. [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。
17. 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
    a. [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。
    b. [配信（DELIVERY）] で [アップロード（Upload）] を選択します。
    c. [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。
    d. [コンテンツ（CONTENT）] で [URL] を選択します。
    e. [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。
    f. [名前（NAME）] に「Local URL list」と入力します。
    g. [アクション（ACTION）] で、[ブロック（Block）] を選択します。



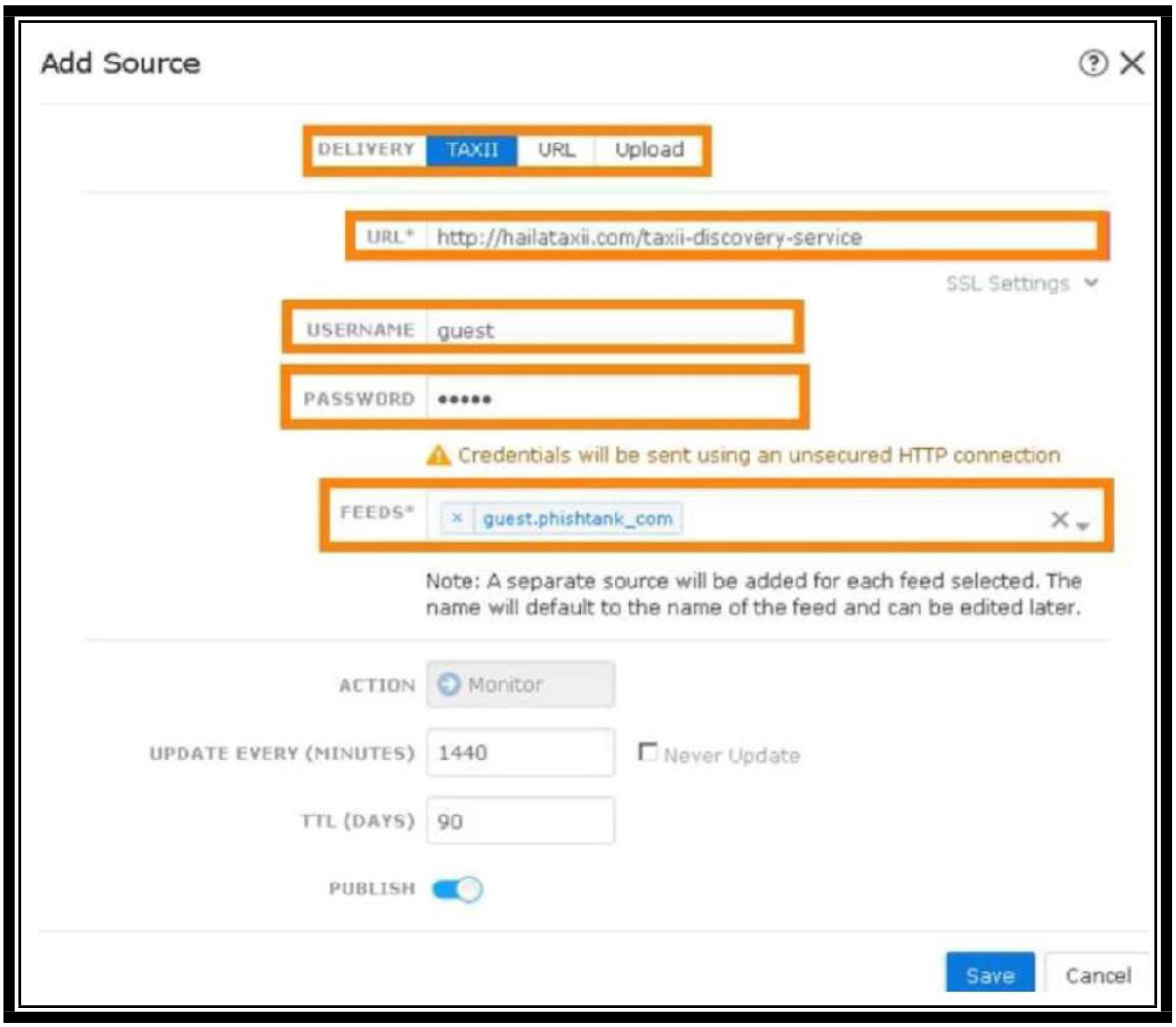
18. [保存（Save）] をクリックします。
19. 数秒間待ちます。[インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ（Indicators）] に移動します。2 つの URL インジケータが追加されたことを確認します。
20. [インテリジェンス（Intelligence）] > [ソース（Sources）] > [監視対象（Observables）] に移動します。2 つのタイプの URL 監視対象が追加されたことを確認します。

TAXII フィードに CTID を登録する

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. 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。**NGFW1 CLI** で次の手順を実行します。
2. 「**expert**」と入力してエキスパート モードにします。
3. 「**ls -d /var/sf/*download**」と入力します。

注：いくつかのディレクトリがリストされます。admin@ngfw:~$ ls -d /var/sf/*download

ls –d /var/sf/clamupd_download
ls –d /var/sf/iprep_download
ls –d /var/sf/sifile_download
ls –d /var/sf/cloud_download
ls –d /var/sf/sidns_download
ls –d /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。

4. 「grep developmentserver /var/sf/*download/*lf」と入力します。
5. URL タイプの CTID 監視対象を確認できます。

/var/sf/siurl_download/731625d4-9512-11e7-915c-7e7252ae92ac.lf:developmentserver.com/misc/Tron.html/

注：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。

6. 「grep 198.18.133.200 /var/sf/*download/*lf」と入力します。URL タイプの CTID 監視対象を確認できます。

/var/sf/iprep_download/731625d4-9512-11e7-915c-7252ae92ac.blf:198.18.133.200

注：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。

7. 「exit」と入力してエキスパート モードを終了します。

内部 Linux サーバの CLI で次を実行する

1. wget -t 1 outside/files/ProjectX.pdf を実行します。これは成功するはずです。
2. 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。

付録 A：FMC の事前設定

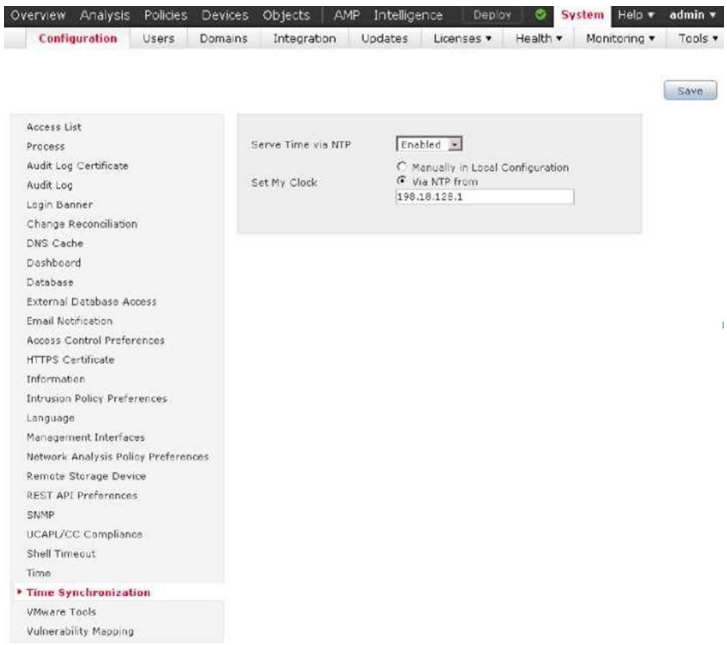
ラボ演習を迅速化するため、初期インストール後に FMC でいくつかの設定手順が事前実行されています。この付録では、実行された設定手順について説明します。

- 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

手順

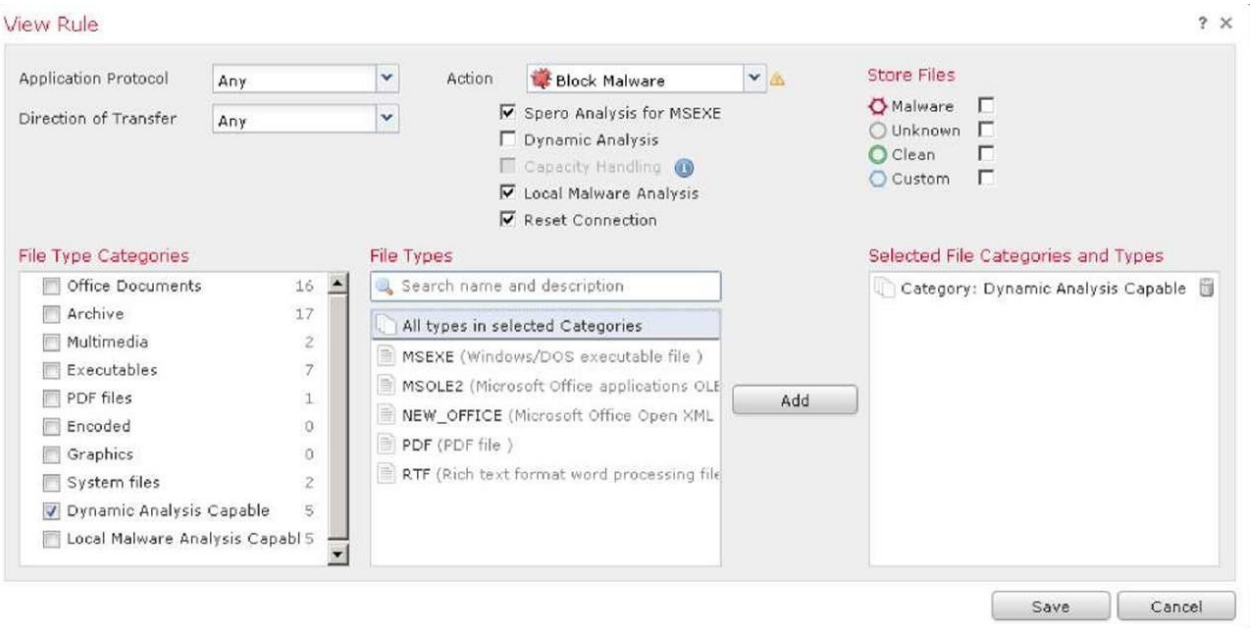
設定 A1.1：NTP 設定

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

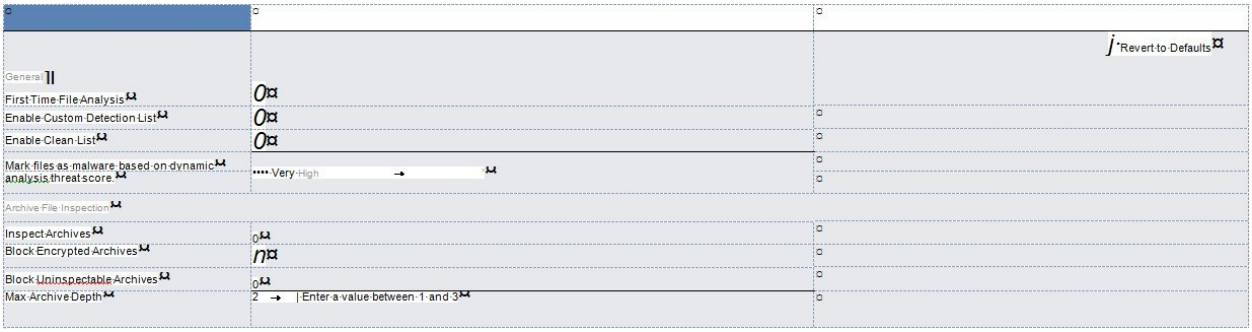
1. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [マルウェア&ファイル（Malware & File）] **に移動します。**
2. [新しいファイル ポリシー（New File Policy）] をクリックします。「Demo File Policy」**という名前を入力します。**[保存（Save）] **をクリックします。**
3. [ファイルルールを追加（Add File Rule）] をクリックします。このルールにより、MSEXE、MSOLE2、NEW_OFFICE、PDF の各ファイルで検出されたマルウェアがブロックされます。
4. [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。**
5. [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。
6. [ファイルタイプのカテゴリ（File Type Categories）] で、[動的分析可能（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。クリックして [Add（追加）] **をクリックします。**
7. 画面は下の図のようになります。



8. [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。
9. [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。
10. **[アクション（Action）] で [ファイルをブロック（Block Files）] を選択します。**
11. [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。
12. 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。
13. [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 - マルウェアをブロック
3 - マルウェア クラウドのルックアップ
4 - ファイル検出
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。
6 - [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。

14. 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。

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。

15. 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** フォルダの **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。

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

[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 **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。
3. [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。

4. [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）] を [復号しない（Do Not decrypt）] の設定のままにします。**
   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、[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。
5. [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。
6. [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。
7. [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、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 **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」**と入力後、**「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 **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 **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。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

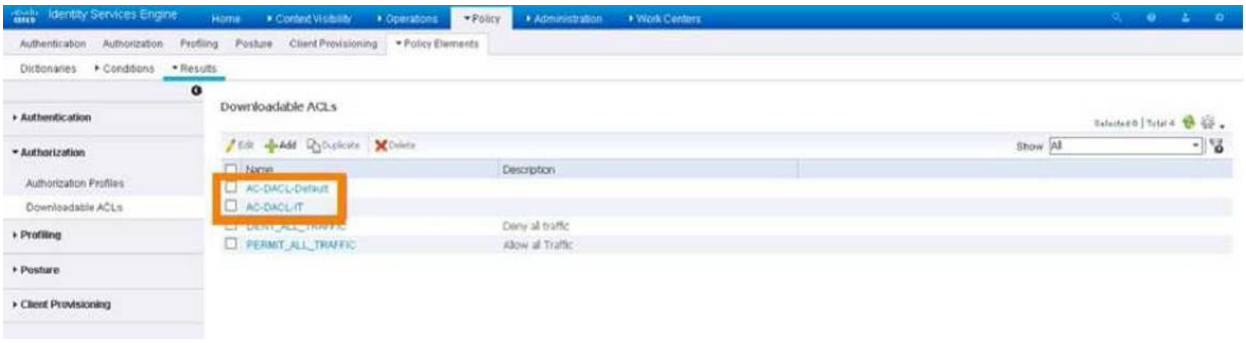
1. [ポリシー（Policy）] > [認可（Authorization）] に移動します。最初の 2 つのポリシー、**AC-IT-Policy** と **AC-Default-Policy** は、このラボ用に作成されたものです。これらのポリシーは、2 つの認可プロファイル、AC-Auth-IT と AC-Auth-Default を参照しています。

認可プロファイル

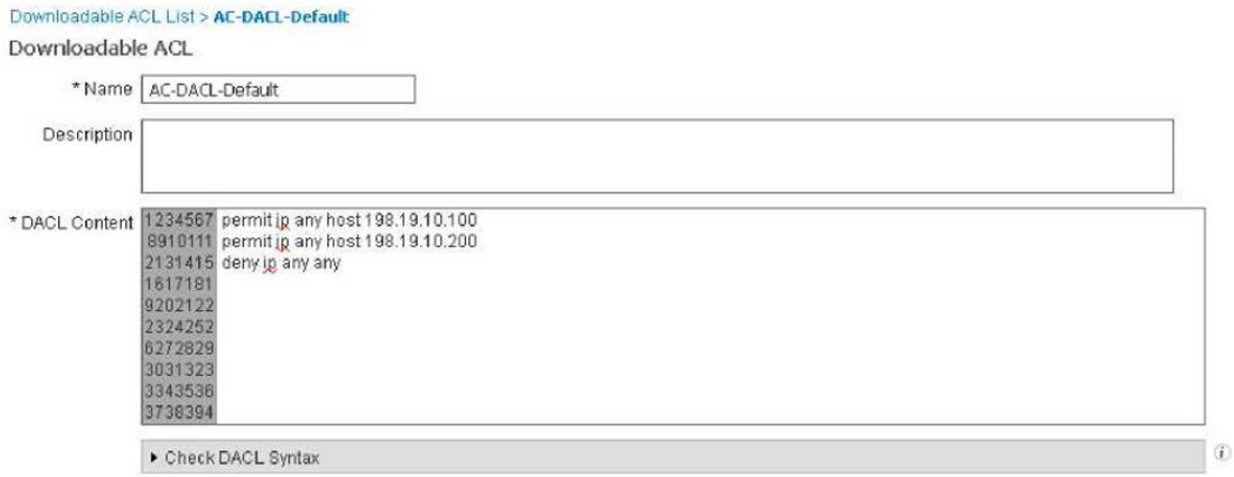
1. **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認可（Authorization）] > [認可プロファイル（Authorization Profiles）] に移動します。最初の 2 つのプロファイル、**AC-Auth-Default **と** AC-Auth-IT **は、このラボ用に作成されたものです。**
2. **AC-Auth-Default** をドリルダウンすると、以下に説明する **DACL AC-DACL-Default** を参照していることがわかります。
3. **AC-Auth-IT** に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

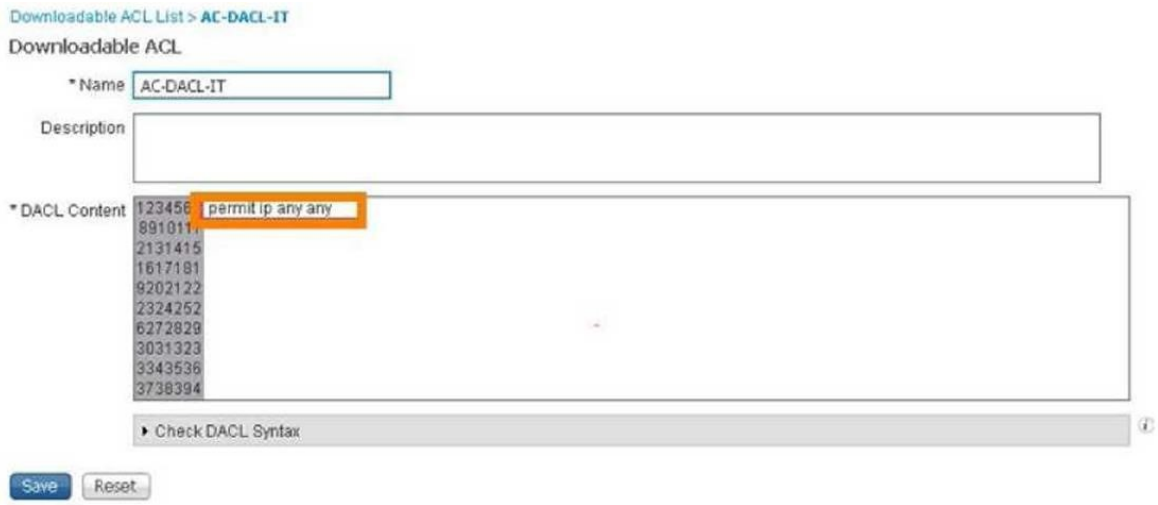
1. [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [認可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] に移動します。最初の 2 つの DACL、**AC-DACL-Default** と AC-DACL-IT は、このラボ用に作成されたものです。



2. **AC-DACL-Default** に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** にドリルダウンすると、制限がないことがわかります。



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