

Cisco Firepower次世代ファイアウォール 6.3 基本ラボ v2.4

最終更新日 : 2019 年 3 月 21 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](#)
- [このソリューションについて](#)
- [トポロジ](#)
- [はじめに](#)
- [シナリオ 1 : REST API によるデバイス導入](#)
- [シナリオ 2 : 基本設定](#)
- [シナリオ 3 : FlexConfig](#)
- [シナリオ 4 : NAT およびルーティング](#)
- [シナリオ 5 : プレフィルタ ポリシー](#)

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 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。

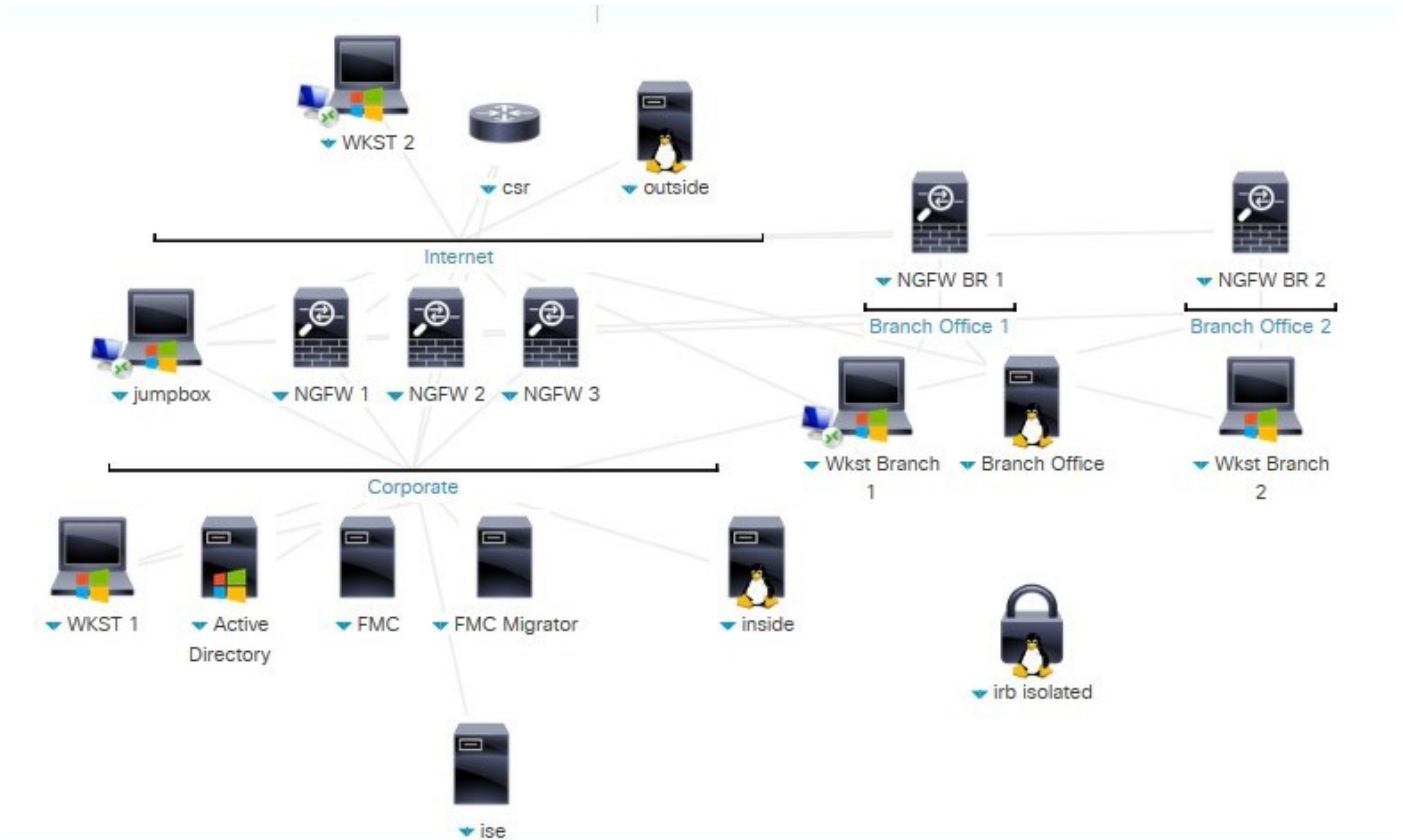
Cisco Firepower NGFW は、企業が最新の脅威に対するリアルタイムの阻止、優先順位付け、把握、対応自動化を図ることを焦点に進化することが可能です。Firepower NGFW は、包括的なネットワーク可視性、最善の脅威インテリジェンス、有効性の高い脅威防御を基盤にした脅威中心型を特徴とし、既知および未知の両方の脅威に対応します。また、Advanced Malware Protection によって、レトロスペクティブ セキュリティも可能にします。これは、防御を回避した巧妙な攻撃を「時間を遡って」迅速に特定し、修復するものです。それにより、業界の平均値に比べて検出時間 (TTD)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

このラボでは、企業サイトと 2 つのブランチ サイト間にマルチサイト 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、高可用性の NGFW を企業サイトに構築し、ブランチを管理します。このラボでは、FDM (Firepower Device Manager) を使用して NGFW も設定します。リモート アクセスおよびサイト間 VPN も設定し、NGFW デバイスに対するサード パーティの更新を受け入れて実装するための Cisco Threat Intelligence Director も設定します。

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。[\[手順を見る\]](#)

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 1 : **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。

シナリオ 1： REST API によるデバイス導入

このラボでは、NGFW のシンプルな導入を行います。そのほとんどで REST API Python スクリプトを使用します。ただし、その前に必要な準備手順があります。また REST API (6.2.2) ではルーティング設定がサポートされていないため、手動で設定する必要があります。

手順

FMC で NGFW を管理する設定にする

1. Jump Desktop で [PuTTY] リンクを開きます。[NGFW1] 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。ユーザー ID **admin**、パスワード **C1sco12345** でログインします。

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

2. 次のコマンドを入力します。
 - a. **show managers** : 次のいずれかが表示されます。
 - i. ローカル管理型
 - ii. マネージャ未設定
 - b. 次のコマンドを入力します。

```
configure manager add fmc.dcloud.local C1sco12345
```

3. 警告が表示され、続行するか尋ねられたら **yes** と答えます。y は入力しないでください。

注： NGFW2、NGFW3、NGFWBR1 は、オンボックス マネージャ (Firepower Device Manager、つまり FDM) が有効な状態でインストールされています。これはデフォルトの設定です。この警告が表示されたのはそのためです。この警告は、FTD がローカル管理型に設定されている場合にのみ表示されます。

オンボックス管理ラボの演習は、このクラスの後半で行います。

ただし、NGFW 設定を削除しないと、FMC と FDM を切り替えることはできません。

4. この PuTTY セッションはラボ全体で使用されるため、開いたままにします。

REST API スクリプトを実行して NGFW を登録および設定する

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

- アクセス コントロール ポリシーを作成する
- **NGFW1** を FMC に登録する
- NGFW インターフェイスを設定する

注：これらのスクリプトはトレーニング用であり、完成されたものではありません。最初のスクリプトを調べる場合は、`/usr/local/bin` にあります。スクリプトの名前は **register_config.py** で、**connect.py** で生成された Python モジュールを使用します。コマンド `runapiscript` は、`register_config.py` に対するシンボリック リンクです。

1. Jump Desktop から PuTTY を起動します。[内部Linuxサーバ (Inside Linux server)] セッションをダブルクリックします。**root** として、パスワード **C1sco12345** でログインします。
2. 内部 Linux サーバの CLI で、**runapiscript** を実行します。
3. [どのファイアウォールを登録しますか (Which firewall do you want to register?)] と表示されたら、1 (NGFW1) を入力して、**Enter** を押します。
4. [アクセスコントロールポリシー名を入力 (enter an access control policy name)] と表示されたら、**Base_Policy** Access Control Policy などの意味のある名前を入力します。
5. 登録プロセス全体でスクリプトが実行されるのを確認できます。
6. Firefox ブラウザを開き、FMC でログインして、[導入 (Deploy)] ボタンの右側にあるアイコンをクリックし、[タスク (Tasks)] タブを選択します。

注：タスクが開始されるまで数秒かかる場合があります。1分経過してもタスクが開始されない場合は、デモ スマート ライセンスが有効になっていることを確認してください。有効でない場合は有効にして、`runapiscript1` スクリプトを再度実行します。アクセス コントロール ポリシーには別の名前を使用するか、スクリプトによって作成されたポリシーを削除してください。

7. スクリプトによって検出プロセスが自動的に続行されます。
8. スクリプトによってインターフェイスが自動的に設定されます。
 - a. この PuTTY セッションは開いたままにします。これはラボ全体を通して使用します。

シナリオ 2： 基本設定

この演習は、次のタスクで構成されています。

- 演習に必要なオブジェクトを作成する
- アクセス コントロール ポリシーを変更する
- NAT ポリシーを作成する
- FMC を使用してブランチ 1 FTD を設定する
- FDM を使用してブランチ 2 FTD を設定する
- 設定変更を導入する
- ネットワーク検出ポリシーを変更する
- 設定変更を導入する

この演習の目的は、シンプルで効果的な NGFW の設定を導入することです。

- アウトバウンド接続を許可し、他の接続試行をブロックする
- これらのアウトバウンド接続でファイル タイプ ブロックとマルウェア ブロックを実行する
- これらのアウトバウンド接続で侵入防御を可能にする

手順

演習に必要なオブジェクトを作成する

1. FMC で、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] の順に選択します。
 - a. [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] の順にクリックします。



- b. [名前 (Name)] に Lab_Networks と入力します。
- c. 198.18.0.0/15 と入力します。これには、ラボ ボットで使用するすべての IP アドレスが含まれています。

Edit Network Object

Name: (1)

Description:

Network: Host Range (2) Network FQDN

(3)

Allow Overrides:

Save Cancel

d. [Network (ネットワーク)] をクリックします。

e. [保存 (Save)] をクリックします。

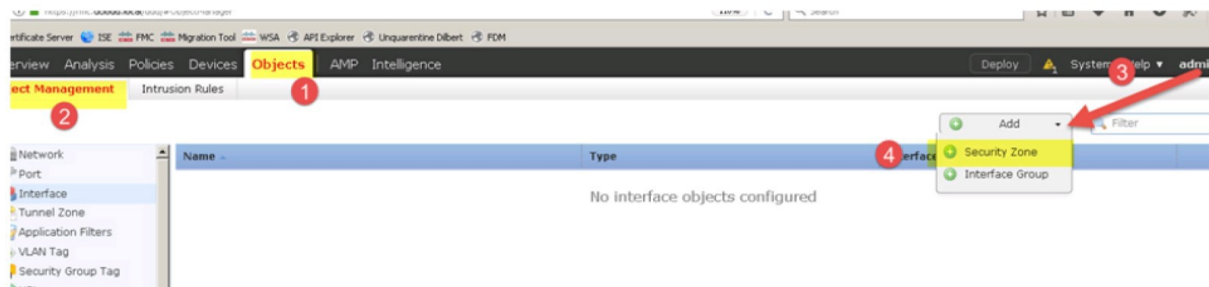
2. 左側のナビゲーション パネルで [インターフェイス (Interface)] を選択します。

a. セキュリティ ゾーン InZone と OutZone は、API スクリプトから設定されている必要があります。そうでない場合は、手順 2b-3 に従います。

b. [追加 (Add)] > [セキュリティゾーン (Security Zone)] の順にクリックします。

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

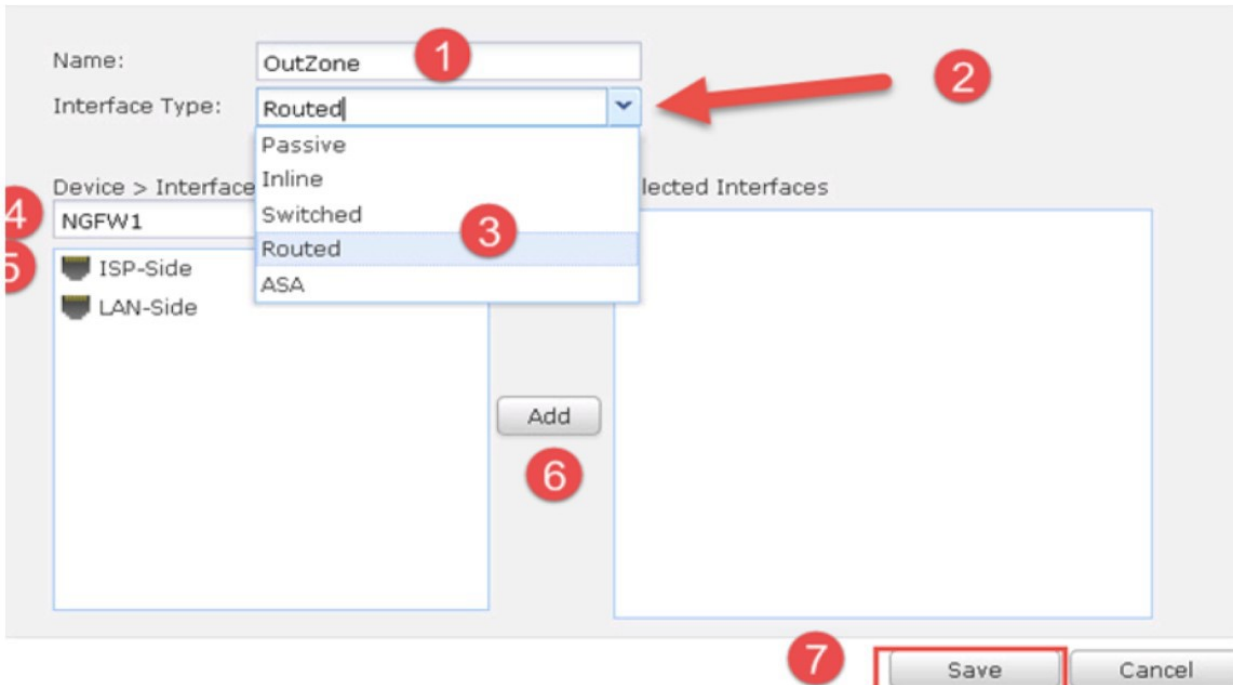
3. インターフェイスに追加されるセキュリティ ゾーン用のネットワーク オブジェクトを作成します。



4. [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] の順に移動し、[Outzone] の横にある鉛筆アイコンをクリックします。

5. [名前 (Name)] が未入力の場合は、**OutZone** と入力します。[インターフェイスタイプ (Interface Type)] ドロップダウンメニューから [ルーテッド (Routed)] を選択します。

- a. [ISP側 (ISP-Side)] インターフェイスを選択します。[追加 (Add)]、[保存 (Save)] の順にクリックします。(NGFW1 が表示されない場合は、[デバイス (Device)] > [インターフェイス (Interfaces)] の下にある矢印をクリックします)。



6. [InZone] の横にある鉛筆アイコンをクリックします。

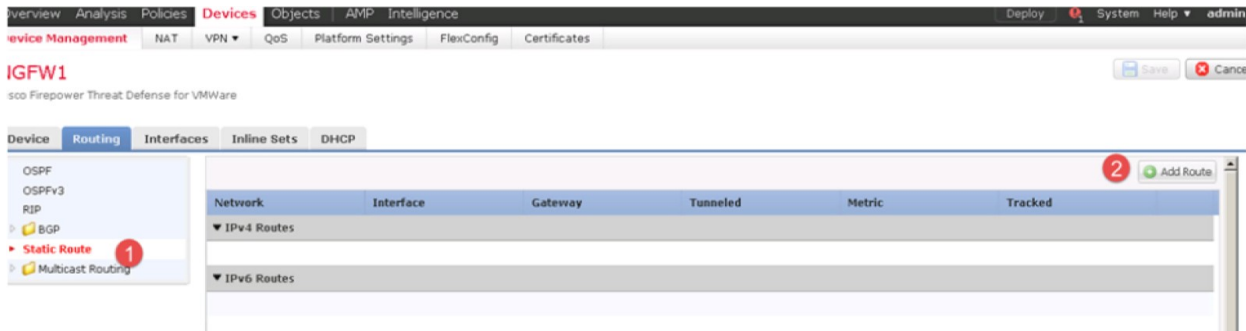
- a. [名前 (Name)] が未入力の場合は、**InZone** と入力します。[インターフェイスタイプ (Interface Type)] ドロップダウンメニューから [ルーテッド (Routed)] を選択します。
- b. [LAN側 (LAN-Side)] インターフェイスを選択します。[追加 (Add)]、[保存 (Save)] の順にクリックします。

デフォルト ルートを設定する

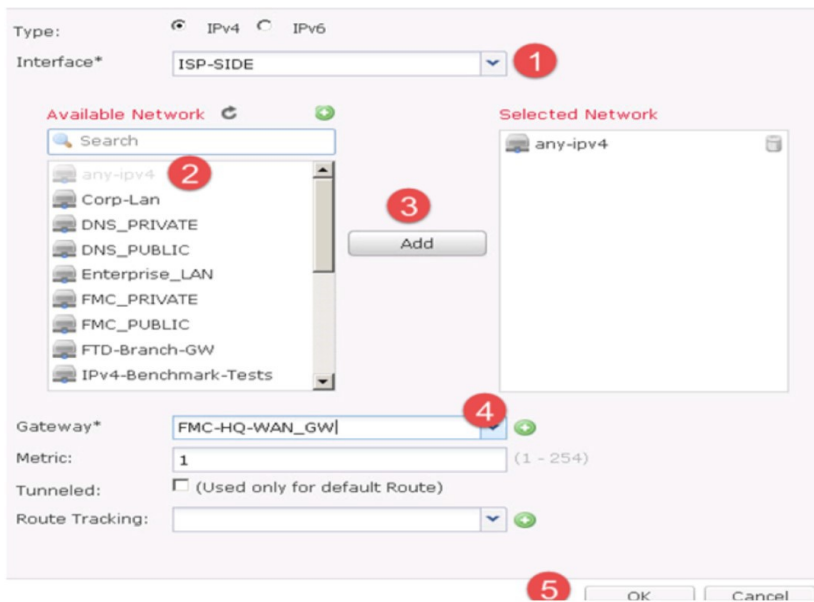
1. FMC で、[デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。鉛筆アイコンをクリックして、デバイス設定を編集します。
2. [インターフェイス (Interfaces)] タブが選択されているはずですが、REST API スクリプトによって、**NGFW1** の内部インターフェイスと外部インターフェイスが設定されたことを確認します。

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	ISP-Side	Physical	OutZone		198.18.133.2/18(Static)
GigabitEthernet0/1	LAN-Side	Physical	InZone		198.19.10.1/24(Static)
GigabitEthernet0/2		Physical			

3. [ルーティング (Routing)] > [スタティックルート (Static Route)] の順に選択し、[ルートの追加 (Add Route)] ボタンをクリックします。



4. [インターフェイス (Interface)] フィールドで [ISP側 (ISP-Side)] を選択します。
5. [利用可能なネットワーク (Available Network)] で [any-ipv4] を選択します (これはデフォルト ルートと同等です)。
6. [追加 (Add)] をクリックします。



7. [ゲートウェイ (Gateway)] で [+] アイコンをクリックして、新しいオブジェクトを作成します。
- [ゲートウェイ (Gateway)]* プルダウン メニューの横にある [+] 記号を選択します。
 - オブジェクトの名前を「FMC-HQ-WAN_GW」にします (このオブジェクトは後で再使用できます)。
 - ネットワーク IP アドレス : **198.18.128.1** を入力します (これは、WAN に面したファイアウォールの外部インターフェイスです)。
 - [保存 (Save)] をクリックします。

New Network Object

Name:

Description:

Network: Host Range Network FQDN

Allow Overrides:

8. [OK] をクリックして、スタティック ルート設定を追加します。

Cisco Firepower Management Center

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

VGFW1

Cisco Firepower Threat Defense for VMWare

You have unsaved changes

Device Routing Interfaces Inline Sets DHCP

OSPF OSPFv3 RIP BGP **Static Route** Multicast Routing

Network	Interface	Gateway	Tunneled	Metric	Tracked
any-ipv4	ISP-Side	FMC-HQ-WAN-GW	false	1	

9. [保存 (Save)] をクリックします。

アクセス コントロール ポリシーを変更する

1. メニューから [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。REST API スクリプトによってアクセス コントロール ポリシーが作成されていることを確認してください。
 - a. ポリシーの右側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。
 - b. 緑色の [+] 記号付きの [ルールの追加 (Add Rule)] をクリックします。
 - c. [名前 (Name)] に **Allow Outbound Connections** と入力します。
 - d. [挿入 (Insert)] ドロップダウン リストから [デフォルト (Default)] を選択します。

注： ルールは、ポリシー内の複数のセットに分割されます。2つのセットが事前定義されています。

必須ルールは、子ポリシーのルールに優先します。

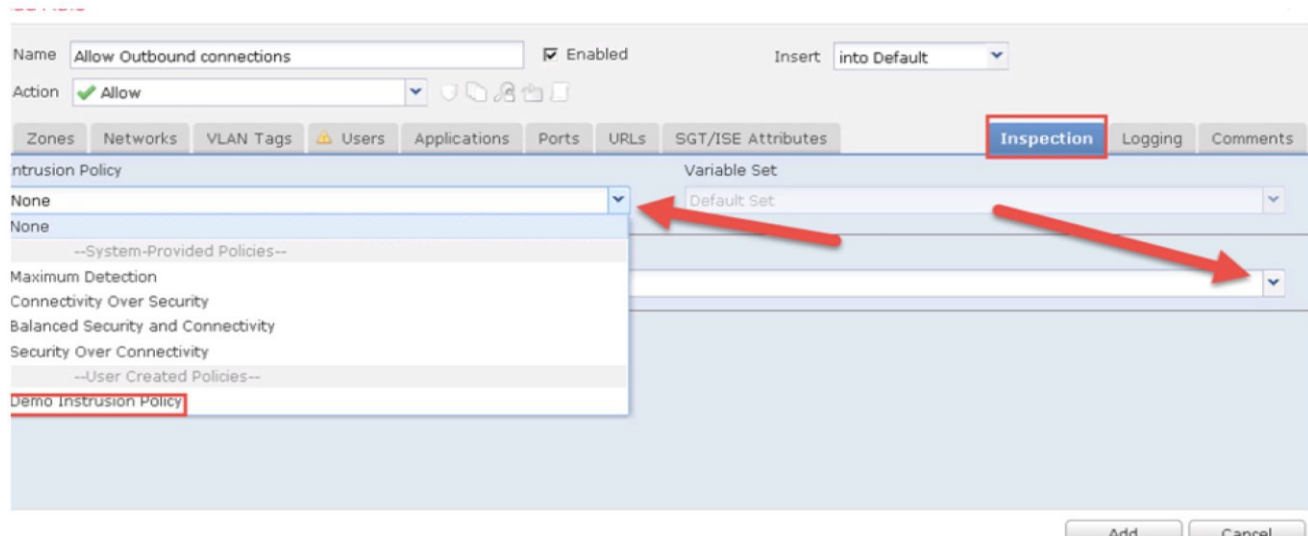
デフォルト ルールは、子ポリシーのルールの後に評価されます。

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

2. [ゾーン (Zones)]タブはすでに選択されている必要があります。
 - a. [InZone] を選択し、[送信元に追加 (Add to Source)] をクリックします。
 - b. [OutZone] を選択し、[宛先に追加 (Add to Destination)] をクリックします。

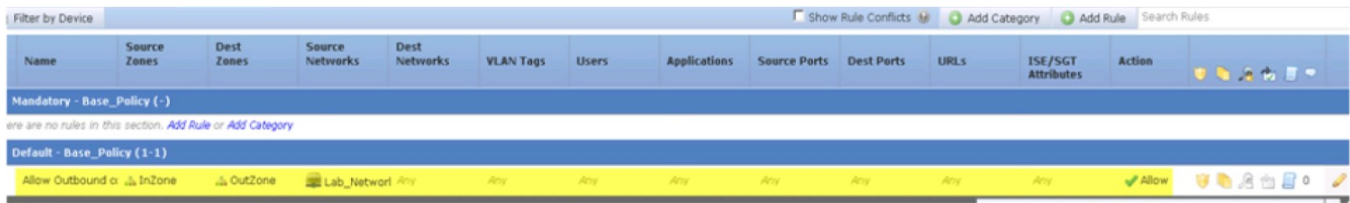


3. [インスペクション (Inspection)]タブを選択します。
 - a. [侵入ポリシー (Intrusion Policy)]ドロップダウン リストから [デモ侵入ポリシー (Demo Intrusion Policy)] を選択します。
 - b. [ファイルポリシー (File Policy)]ドロップダウン リストから [デモファイルポリシー (Demo File Policy)] を選択します。

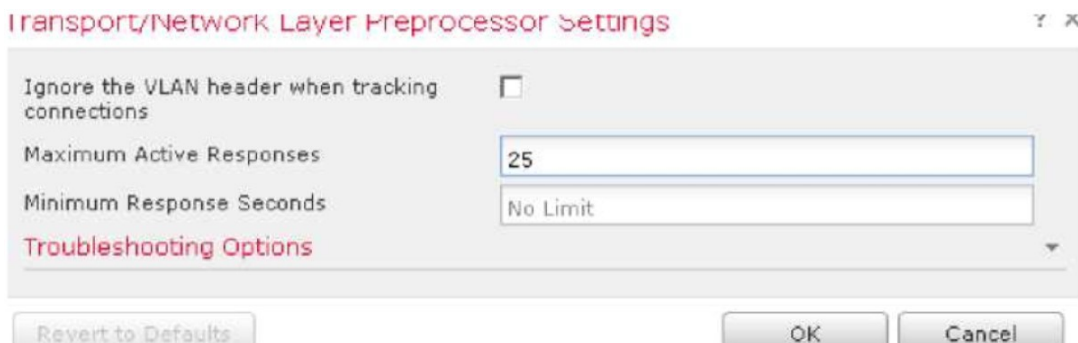


注： デモ侵入ポリシーとデモ ファイル ポリシーは、時間節約のために事前設定されています。これらのポリシーの作成方法については、『Firepower アドバンスド ラボ ガイド v2.4』の「付録 1」を参照してください。

4. [追加 (Add)] をクリックしてルールを追加します。
5. [HTTP 応答 (HTTP Responses)] タブを選択します。



6. [ブロック応答ページ (Block Response Page)] ドロップダウン リストから [システムにより設定 (System-Provided)] を選択します。
7. [詳細設定 (Advanced)] タブを選択します。
8. 鉛筆アイコンをクリックして、[トランスポート/ネットワーク層のプリプロセッサ設定 (Transport/Network Layer Preprocessor Settings)] を編集します。
9. [最大アクティブ応答 (Maximum Active Responses)] テキスト フィールドに **25** と入力します。
10. [OK] をクリックします。



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

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

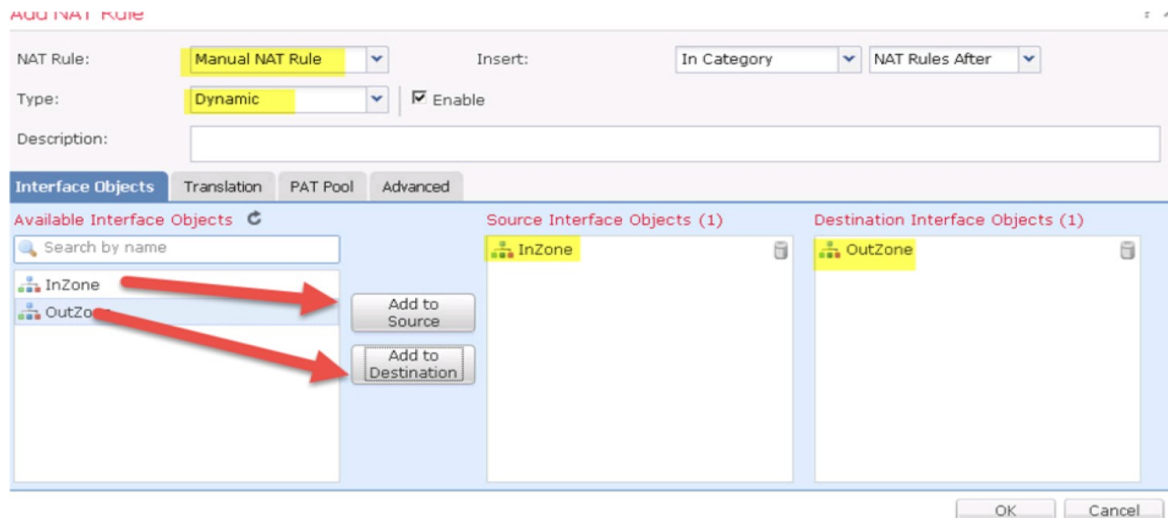
11. [保存 (Save)] をクリックして、アクセス コントロール ポリシーの変更を保存します。

NAT ポリシーを作成する

1. メニューから [デバイス (Devices)] > [NAT] の順に選択します。
2. [新しいポリシー (New Policy)] ボタンをクリックし、[脅威防御NAT (Threat Defense NAT)] を選択します。



3. [名前 (Name)] に **Default PAT** と入力します。
4. [NGFW] を選択します。[ポリシーに追加 (Add to Policy)] > [保存 (Save)] の順にクリックします。
5. ポリシーが開き、編集できるようになります。
6. [ルールの追加 (Add Rule)] をクリックします。
7. [挿入 (Insert)] ドロップダウン リストから [カテゴリに挿入 (In Category)] と [NATルール後 (NAT Rules After)] を選択します。これで、このルールが自動 NAT (オブジェクト NAT) ルールの後に評価されるようになります。



8. [タイプ (Type)] ドロップダウン リストから [ダイナミック (Dynamic)] を選択します。
 - 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。[InZone] を選択し、[送信元に追加 (Add to Source)] をクリックします。
 - b. [OutZone] を選択し、[宛先に追加 (Add to Destination)] をクリックします。
9. [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 [任意 (any)] 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 [宛先インターフェイスIP (Destination Interface IP)] を選択します。

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

Add NAT Rule ?

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:*

Original Destination:

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source:

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Destination:

Translated Source Port:

Translated Destination Port:

FMC のスタティック NAT ポリシー

FMC は NAT デバイスとして機能している **NGFW1** の背後にあります。スタティック NAT ポリシーを作成して、ブランチ FTD が HQ-FMC と通信できるようにする必要があります。

1. [NATルールの追加 (Add a NAT Rule)] をクリックします。
2. そのルールを [自動NATルール (Auto NAT Rule)] にします。
3. [インターフェイスオブジェクト (Interface Objects)] の下で [InZone]、[送信元に追加 (Add to Source)] の順に選択します。
4. [OutZone]、[宛先に追加 (Add to Destination)] の順に選択します。

Edit NAT Rule ? x

NAT Rule:

Type: Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

InZone OutZone

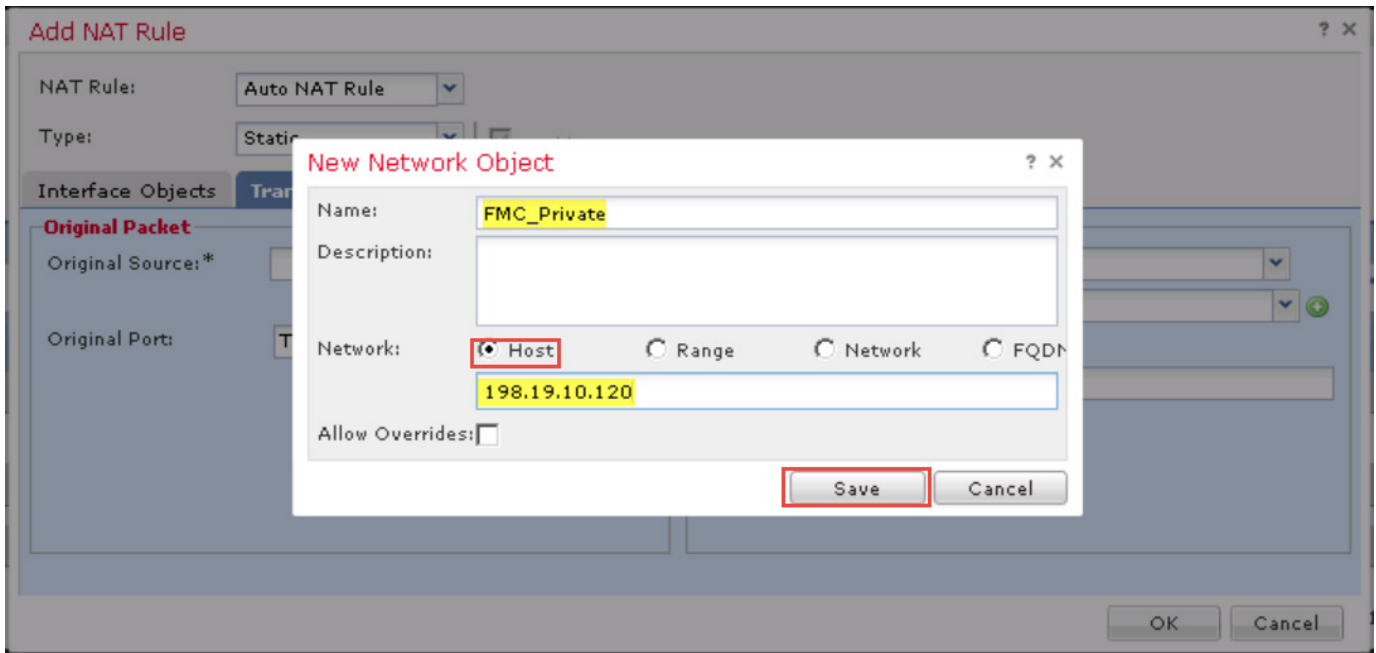
Source Interface Objects (1)

InZone

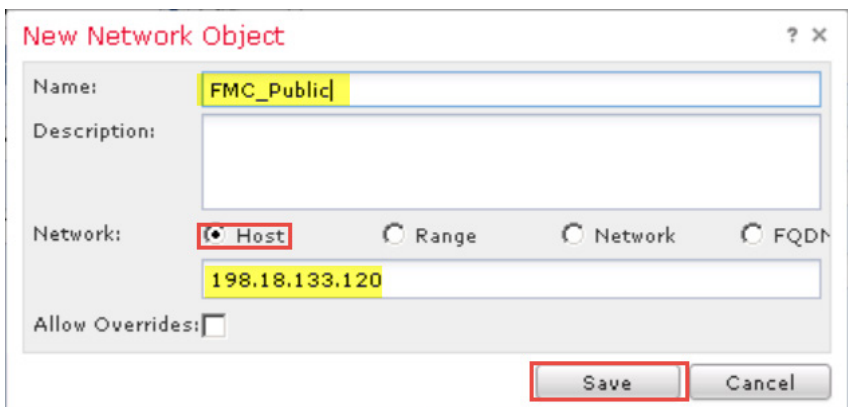
Destination Interface Objects (1)

OutZone

5. [トランスレーション (Translation)] の下で [(+)] 記号をクリックし、[名前 (Name)] に **FMC_PRIVATE** と入力します。
6. [ネットワーク (Network)] に **198.19.10.120** (HQ-FMC のアドレス) を入力します。
7. [保存 (Save)] をクリックします。



8. [(+)] 記号をもう一度クリックし、[名前 (Name)] に **FMC_PUBLIC** と入力します。
9. [ネットワーク (Network)] に **198.18.133.120** (WAN ネットワークのアドレス) を入力します。



NAT Rule: ▼

Type: ▼ Enable

Interface Objects: **Translation** PAT Pool Advanced

Original Packet

Original Source:* ▼ +

Original Port: ▼

Translated Packet

Translated Source: ▼

▼ +

Translated Port:

Filter by Device Add Rule +

Direction	Type	Original Packet		Translated Packet			Options
		Source Interface Ob...	Destination Interface Ob...	Original Sources	Original Destinations	Original Services	
NAT Rules Before							
Auto NAT Rules							
+	Static	+ InZone	+ OutZone	+ FMC_Private		+ FMC_Public	+ Dns:false ✎
NAT Rules After							
+	Dyn...	+ InZone	+ OutZone	+ any		+ Interface	+ Dns:false ✎

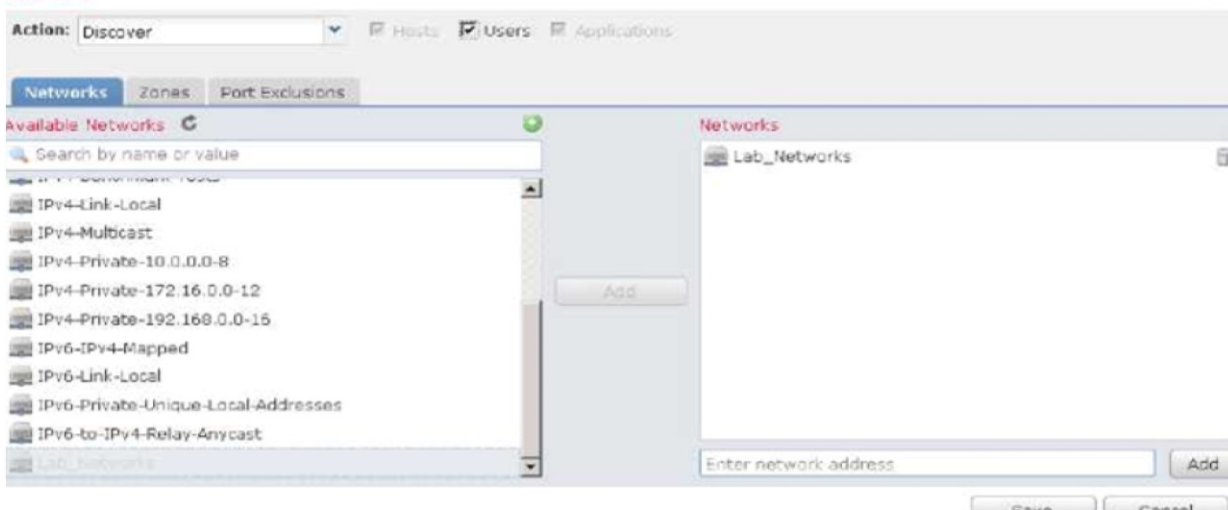
注* : 上記のスクリーンショットは [NATルール後 (NAT Rules After)] を示していますが、実際の画面は異なる場合があります。

10. [OK] をクリックし、Web ページの上部にある [保存 (Save)] をクリックします。
11. アクセスコントロールポリシー **Base_Policy** を変更して、プライベート FMC のインバウンドアクセスリストを作成します。
 - a. [ポリシー (Policies)] > [アクセスコントロールポリシー (Access Control Policies)] の順に選択します。
 - b. **Base_Policy** の近くにある鉛筆アイコンをクリックします。
 - c. FMC_Static_NAT という名前のルールを追加します。
 - d. [アクション (Action)] : [許可 (Allow)]。
 - e. [送信元ゾーン (Source Zone)] : **Outzone**、[宛先 (Destination)] : **InZone**。
 - f. [宛先ネットワーク (Destination Networks)] : **FMC_Private**。
 - g. [インスペクション (Inspection)] タブ。
 - i. [侵入ポリシー (Intrusion Policy)] : [デモ侵入ポリシー (Demo Intrusion Policy)]。
 - ii. [ファイルポリシー (File Policy)] : [デモファイルポリシー (Demo File Policy)]。
 - h. [Add (追加)]、[Save (保存)] の順にクリックします。

ネットワーク検出ポリシーの変更

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

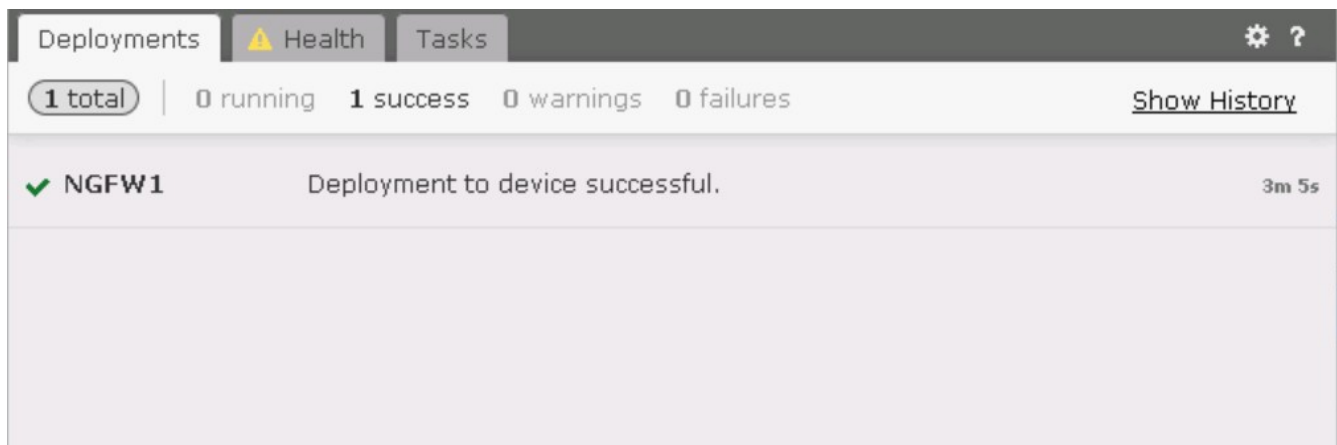
1. メニューから [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] の順に選択します。
 - a. 右側の鉛筆アイコンをクリックして、既存のルールを編集します。
 - b. [ユーザ (Users)] チェックボックスをオンにします。[ホスト (Hosts)] チェックボックスが自動的にオンになります。
 - c. [0.0.0.0/0] と [::/0] の両方を削除します。
2. [ラボネットワーク (Lab Networks)] を選択し、[追加 (Add)] をクリックします。



3. [保存 (Save)] をクリックします。
4. FMC の右上隅にある [導入 (Deploy)] をクリックします。
 - a. NGFW デバイスを選択し、リストを展開して詳細を表示します。ページの内容は次の図のようになります。バージョン 6.2.3 以降、Snort の割り込みが発生している場合は警告が表示されます。また、割り込みの発生原因も表示されます。後で導入する場合は、[キャンセル (Cancel)] ボタンをクリックできます。



5. **NGFW 設定**、NAT ポリシー ネットワーク検出、インターフェイスおよびスタティック ルート設定が変更されることを確認します。
 - a. [展開 (Deploy)] をクリックします。
 - b. FMC の右上隅にある [導入 (Deploy)] リンクの右側のアイコンをクリックします。導入が完了するまで待ちます。



NGFW の導入をテストする

1. 内部 Linux サーバの CLI で次の手順を実行します。
 - a. **wget cisco.com** と入力します。これは成功するはずですが、これで、NAT とルーティングは確認できました。
 - b. **ping outside** と入力します。これは成功するはずですが、Ctrl+C を押して ping を終了します。
 - c. **ftp outside** と入力します。 **guest**、パスワード **C1sco12345** でログインします。

2. `cd ~root` と入力します。次のメッセージが表示されます：`421 Service not available, remote server has closed connection.` これで、IPS が機能していることを確認できます。

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

3. `quit` と入力して、FTP を終了します。
4. FMC で、[分析 (Analysis)] > [侵入 (Intrusions)] > [イベント (Events)] の順に選択します。

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

The screenshot shows the Cisco FMC interface for 'Events By Priority and Classification'. The table below is a representation of the data shown in the image:

Message	Priority	Classification	Count
PROTOCOL-FTP CWD ~root attempt (1:335:17)	medium	Potentially Bad Traffic	1

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

NGFW の CLI で、次のコマンドを実行します。

```
pmtool restartbytype EventProcessor
```

Jump Desktop から、事前定義されている PuTTY セッションを使用して FMC に接続します。`admin/C1sco12345` でログインし、次のコマンドを実行します。

```
sudo pmtool restartbyid SFDataCorrelator
```

```
sudo pmtool restartbyid sftunnel
```

注：Sudo パスワードは `C1sco12345` です。

5. 左側の矢印をクリックして、イベントのテーブルビューにドリルダウンします。イベントの詳細が存在することを確認します。
 - a. イベントの左側にある矢印をクリックして、さらにドリルダウンします。Snort ルールの詳細を含む広範な情報が得られる点に注意してください。
 - b. [アクション (Actions)]を展開するとルールを無効化できますが、無効化しないでください。
6. ファイルブロックおよびマルウェアブロック機能をテストします。これらの Wget コマンドは、Jump Desktop の Strings というファイルからカットして貼り付けることができます。
7. 内部 Linux サーバから root/C1sco12345 でログインします。
 - a. 制御テストとして、WGET を使用して、ブロックされていないファイルをダウンロードします。 **wget -t 1 outside/files/ProjectX.pdf**。これは成功するはずですが。
 - b. 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 outside/files/test3.avi**。

注：ダウンロードされるのはファイルのごく一部です。これは、NGFW が、データの最初のブロックからファイルタイプを検出できるためです。デモファイルポリシーは、AVI ファイルをブロックするように設定されています。

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

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。

8. FMC で、[分析 (Analysis)]>[ファイル (Files)]>[マルウェアイベント (Malware Events)] の順に選択します。
 - a. 1 つのファイル、 **Zombies.pdf** がブロックされたことを確認します。
 - b. 左側の矢印をクリックして、イベントのテーブルビューにドリルダウンします。ホスト **198.19.10.200** が赤色のアイコンで表されている点に注意してください。これは内部 Linux サーバです。赤色のアイコンは、ホストに侵入の痕跡が割り当てられていることを意味します。

Time	Action	Sending IP	Sending Country	Receiving IP	Receiving Country	Sending Port	Receiving Port
2017-10-01 02:59:44	Custom Detection Block	198.18.133.200		198.19.10.200		80	39226

注：このアクションは、[マルウェアブロック (Malware Block)]ではなく、[カスタム検出ブロック (Custom Detection Block)]としてレポートされます。これは、カスタム検出リストに Zombies.pdf を追加したため、ラボがクラウドに接続されている場合にのみ発生します。詳細については、付録 1 を参照してください。

9. 代わりに、内部 Linux サーバから次のコマンドを試すこともできます。

```
wget -t 1 outside/malware/Buddy.exe
```

これは [マルウェアブロック (Malware Block)]としてレポートされます。ただし、この特定のラボ環境では、クラウド ルックアップが失敗する場合があります、そのため、ファイルがブロックされないことがあります。

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

11. メニューから [分析 (Analysis)] > [ファイル (Files)] > [ファイルイベント (File Events)] の順に選択します。3 つすべてのファイル イベントに関する情報が表示されます。

The screenshot shows the 'File Summary' page in the Cisco dCloud interface. The breadcrumb trail is 'File Summary > Table View of File Events'. The table below shows the following data:

Category	Type	Disposition	Action	Count
PDF files	PDE	Unknown	Malware Cloud Lookup	1
PDF files	PDE	Custom Detection	Custom Detection Block	1
Multimedia	RIFF		Block	1

注：必要に応じてドリル ダウンすることができます。

12. **外部 Linux サーバへの PuTTY 接続を開きます。**

- a. **root/C1sco12345** でログインします。
- b. **198.18.133.120** (FMC の外部 NAT アドレス) に ping を実行します。
- c. Ctrl + C を押して ping を停止します。
- d. PuTTY セッションを最小化します。

FTD ブランチ 1 をネットワークに追加する

1. FMC のスタティック NAT エントリはすでに作成しています。 **198.18.133.120**。
2. ここでは、NGFW ブランチ 1 を FMC でも管理されるように設定します。
3. Jump PC で、**NGFWBR1** (198.18.133.42 : 22) への PuTTY 接続を開き、**admin**、パスワード **C1sco12345** でログインします。

4. 「show managers」と入力します。
 - a. 応答が [マネージャ未設定 (No managers configured)] または [ローカルで管理 (Managed Locally)] の場合
5. 「configure manager add 198.18.133.120 C1sco12345 abcde」コマンドを入力し、
 - a. 質問が表示されたら **yes** と入力します。

```
> configure manager add 198.18.133.120 C1sco12345 abcde
If you enabled any feature licenses, you must disable them in Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco Smart Software Manager.
Do you want to continue[yes/no]: yes
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```

注: FMC の NAT アドレスを追加し、固有の NAT ID (この場合は abcde) も追加する必要があります。NAT ID は、NGFW 登録プロセスの実行時に FMC の NAT ID と一致する必要があります。

6. FMC の Web ページに戻り、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [追加 (Add)] > [デバイスの追加 (Add Device)] に移動します。

New Policy

7. [アクセスコントロールポリシー (Access Control Policy)] の下で下向き矢印を選択し、[新しいポリシーの作成 (Create New Policy)] を選択します。
8. [名前 (Name)]: **Branch1access**、[ベースポリシーの選択 (Select Base Policy)]: [なし (None)]、[デフォルトアクション (Default Action)]: [すべてのトラフィックをブロック (Block all traffic)]。[保存 (Save)] をクリックします。

Add Device



Host:

Display Name:

Registration Key:

Group:

Access Control Policy:

Smart Licensing

Malware:

Threat:

URL Filtering:

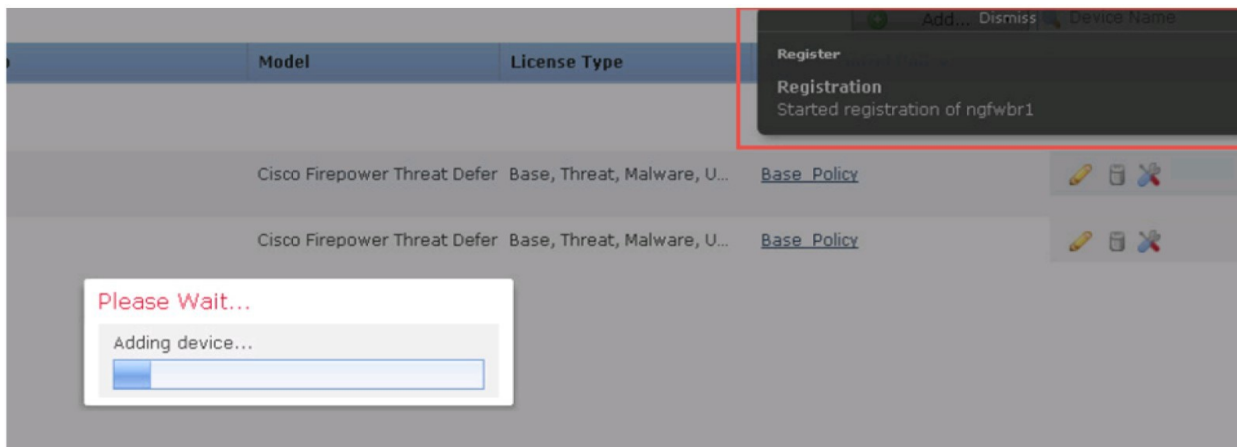
Advanced

Unique NAT ID:

Transfer Packets:

On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from [smart license page](#)

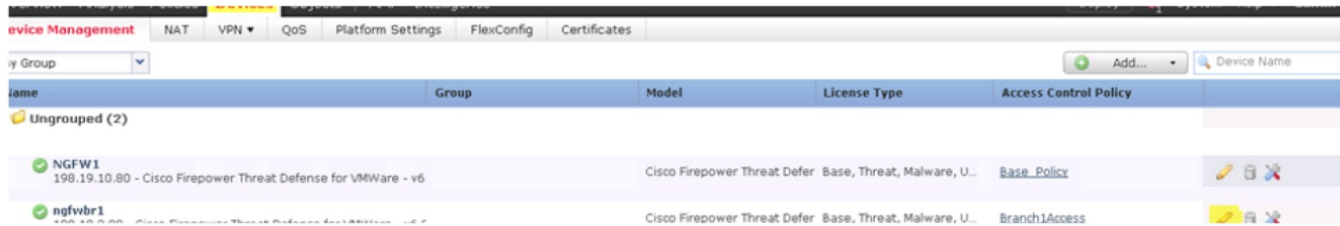
9. **Branch1Access** を選択し、[スマートライセンス (Smart Licensing)] で**すべてのボックスをオンにし**、[詳細設定 (Advanced)] の下で FTD の NAT コード (**abcde**) を入力します。
10. [登録 (Register)] をクリックします。



11. **ngfwbr1** が登録されるまで待ちます。

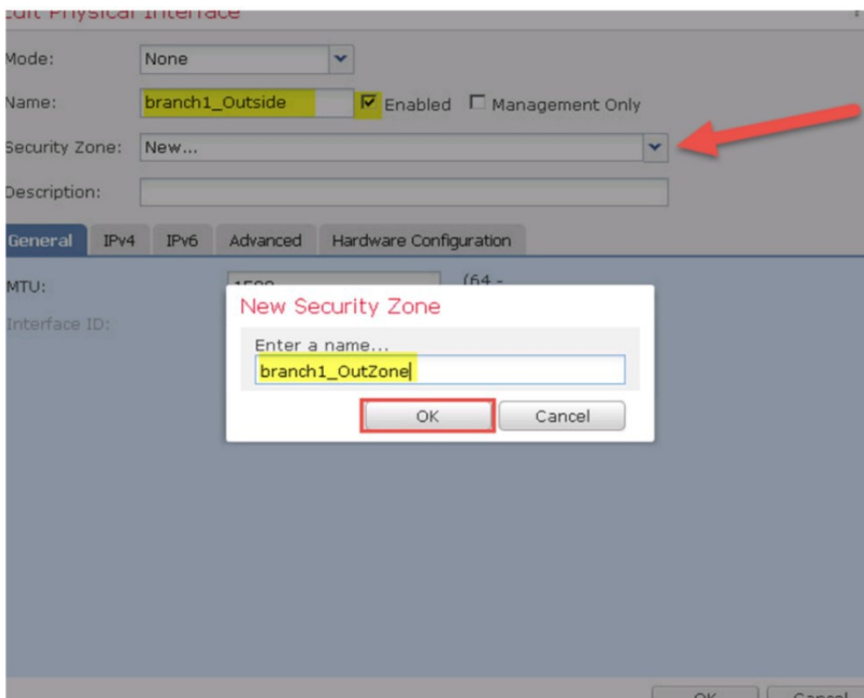
注：これで ngfwbr1 が追加されたので、インターフェイスの追加、デフォルト ルートの構築、NAT ポリシーの作成、アクセス ポリシーの更新を行う必要があります。

12. [デバイス (Devices)] > [デバイス管理 (Device Management)] に移動します。ngfwbr1 の横にある鉛筆アイコンをクリックします。



注：導入スクリプトを実行できなかったため、インターフェイスのアドレスは事前設定されていません。6.2.2 の REST API では NAT 機能はサポートされていません。この状況は今後のリリースで修正される予定です。

13. Gigabit Ethernet0/0 行の鉛筆アイコンをクリックします。
14. [ゾーン (Zones)] と [IPアドレス (IP address)] を設定します。



15. [名前 (Name)] : **branch1_Outside**、[セキュリティゾーン (Security Zone)] : [新規 (New)] をクリックし、名前 **branch1_Outzone** を入力します。
16. [IPv4アドレス (IPv4 address)] タブを選択します。

Edit Physical Interface ? x

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: Use Static IP ▾

IP Address: 198.18.133.142/18 eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

OK Cancel

17. [IPアドレス (IP Address)] : **198.18.133.142/18** (外部 WAN [ISP] のアドレス) 。

注 : このシナリオでは、ファイアウォールの**管理 IP アドレス**に 198.18.133.42/18 を使用しました。このアドレスは、コマンドラインから **show network** コマンドを入力して確認するか、FTD で**エキスパート モード**に移行して ifconfig コマンドを実行し、**br1 インターフェイス**で確認することができます。管理 IP アドレスは、オペレーティング システムにのみアクセスできます。そのため、WAN インターフェイスを外部インターフェイスとして作成する必要があります。外部インターフェイスは、ISP から DHCP を使用して設定することもできますが、このラボのシナリオにサーバを追加したくありませんでした。

18. GigabitEthernet0/1 行に対して同じ手順を繰り返します。

Edit Physical Interface

General IPv4 IPv6 Advanced Hardware Configuration

Name: Enabled Management Or

Description:

Mode:

Security Zone:

Interface ID:

MTU: (64 - 9000)

OK Cancel

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type:

IP Address: eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

OK Cancel

19. Web ページ上部にある [保存 (Save)] をクリックします。

20. [ルーティング (Routing)] > [スタティックルート (Static Route)] > [ルートの追加 (Add Route)] に移動して、インターネットへのスタティック ルートを作成します。

21. インターフェイス **branch1_Outside** を選択します。

22. [利用可能なネットワーク (Available Network)] で、ゲートウェイとして **any-ipv4** を選択します。

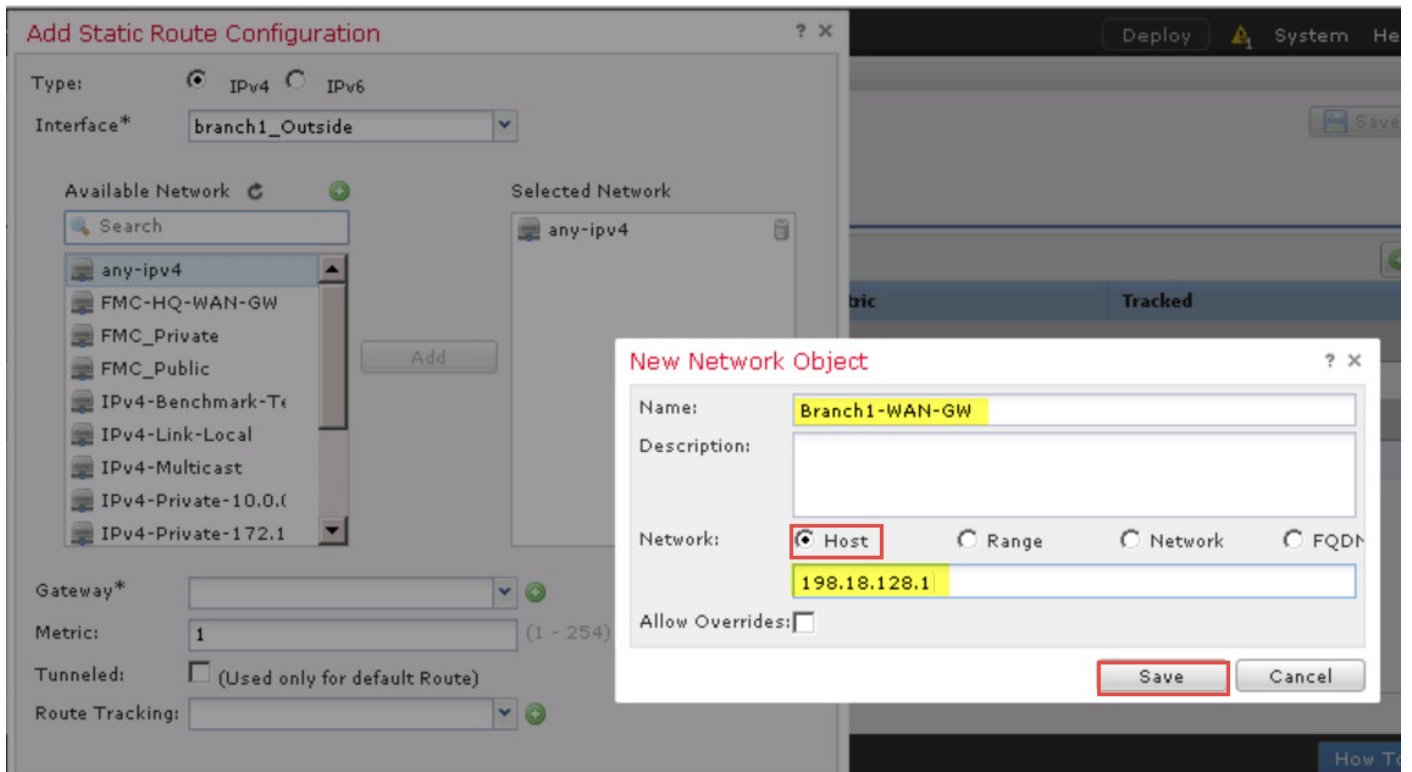
23. 緑色の [(+)] ボタンをクリックし、[新規ネットワークオブジェクト (New Network Object)] : **198.18.128.1** を設定します。

24. [保存 (Save)] をクリックします。

25. [OK] をクリックします。

注： インターフェイス **branch1_Outside** がプルダウン ボックスに表示されない場合は、画面の右上にある [保存 (Save)] ボタンをクリックします。

26. 終了したら、Web ページ上部にある [保存 (Save)] をクリックします。



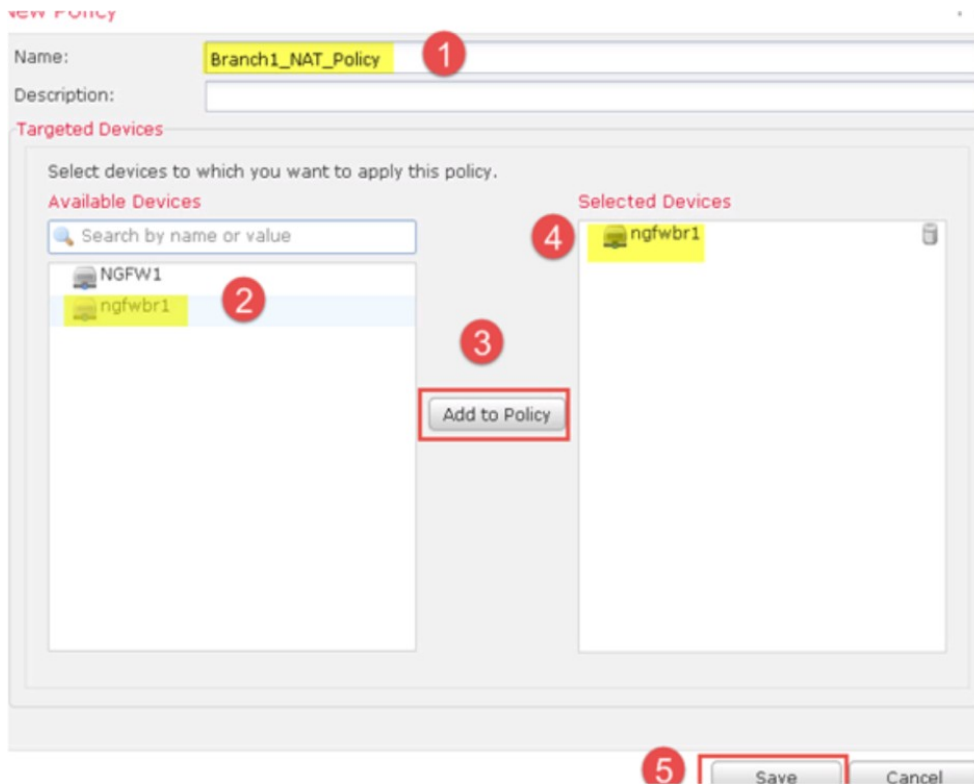
27. [デバイスNAT (Devices NAT)] > [新しいポリシー (New Policy)] > [脅威防御NAT (Threat Defense NAT)] に移動します。



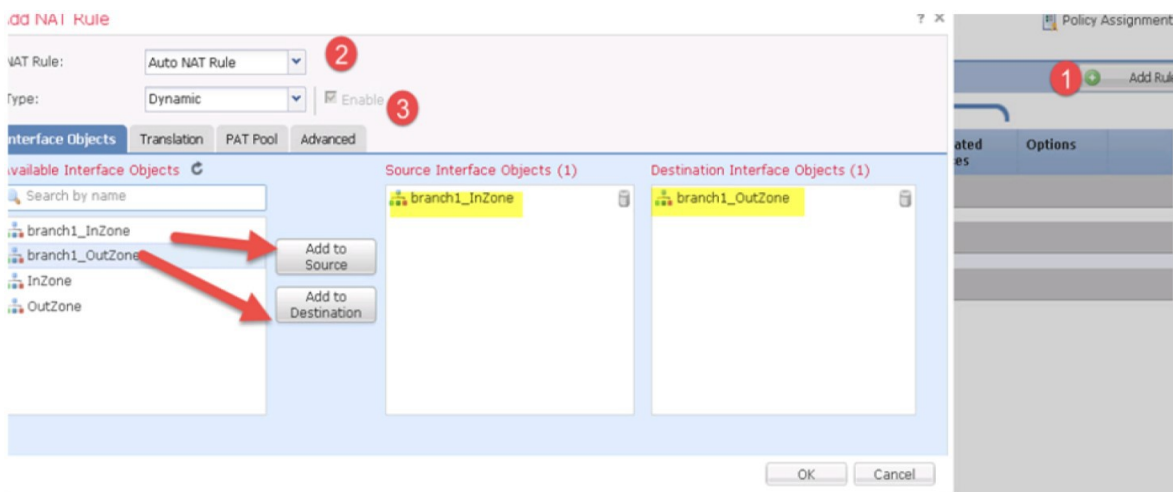
28. ポリシーに **Branch1_NAT** という名前を付け、[利用可能なデバイス (Available Devices)] の下で **ngfwbr1** を選択します。

29. [ポリシーに追加 (Add to Policy)] をクリックします。

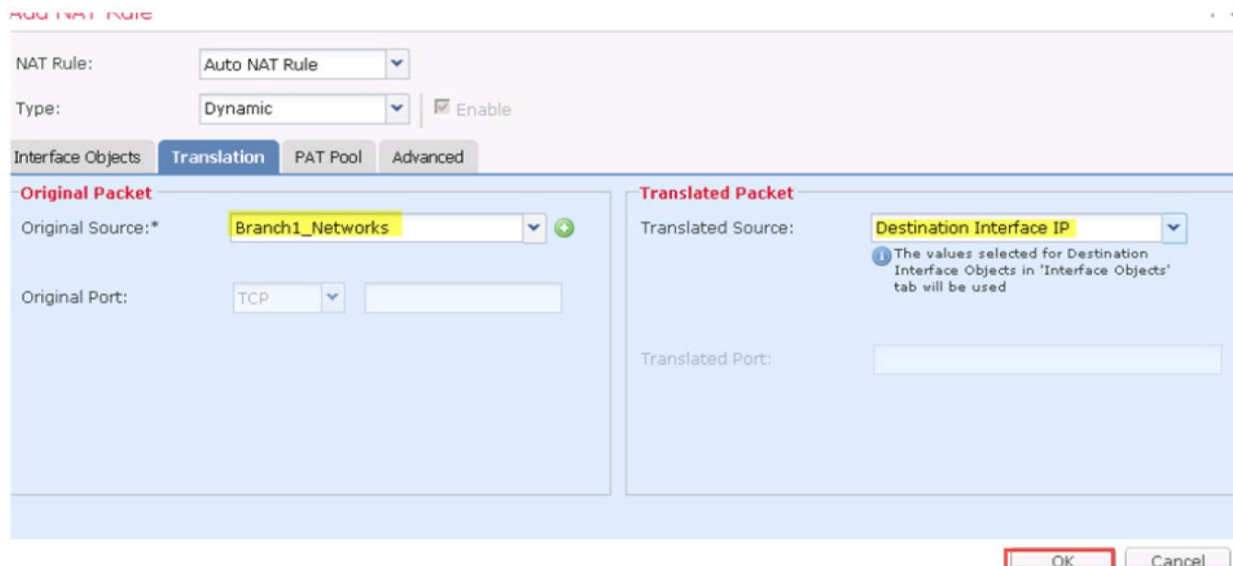
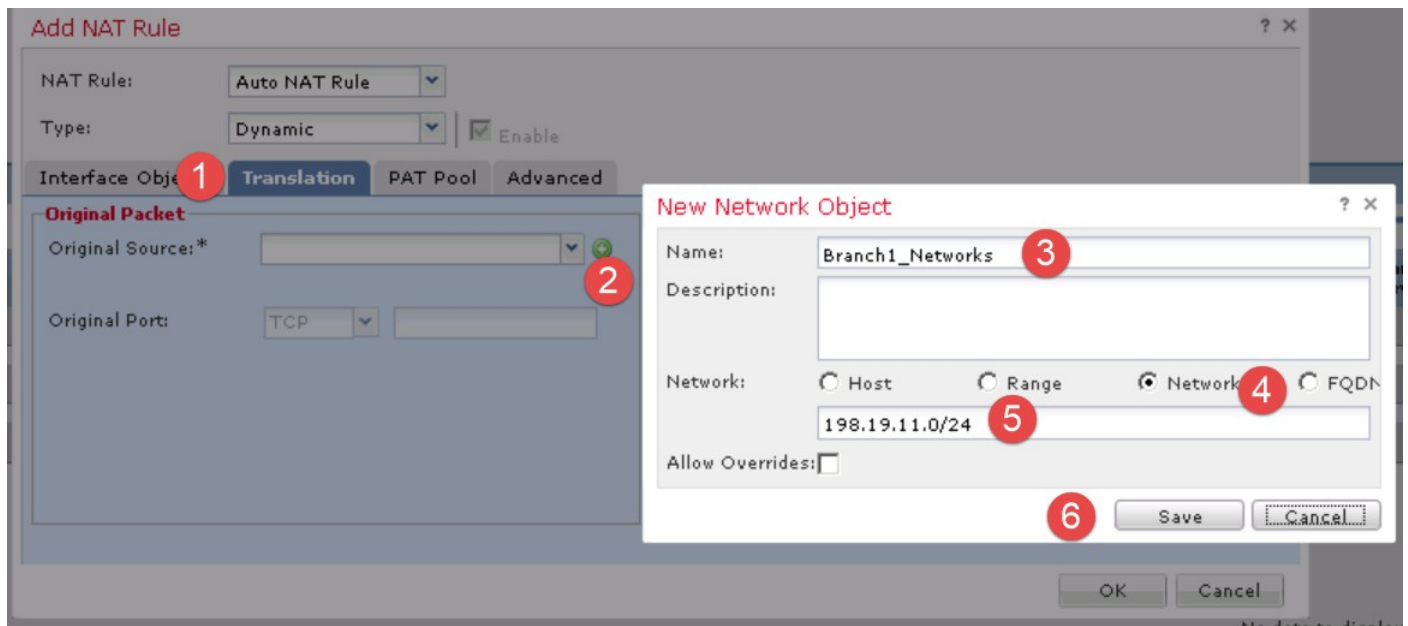
30. [保存 (Save)] をクリックします。



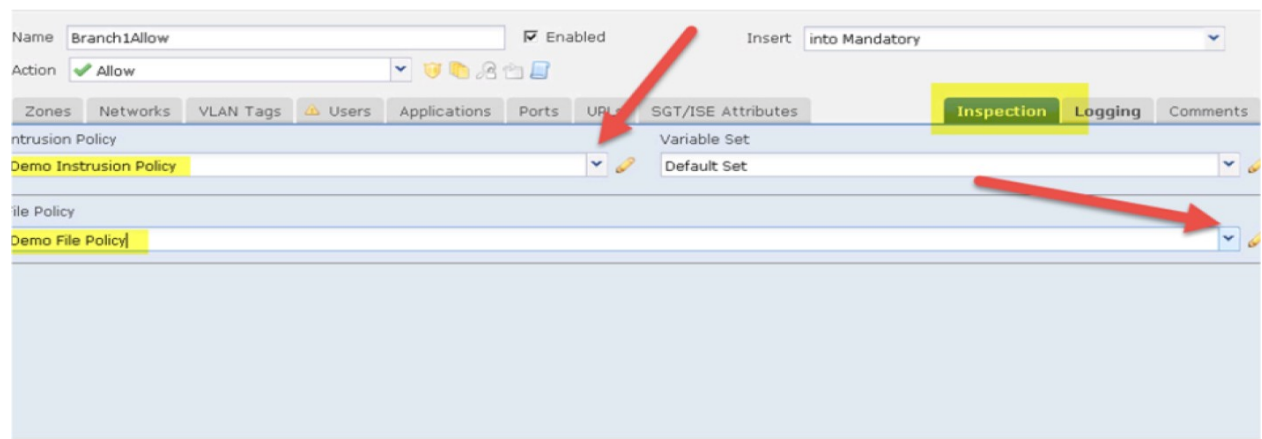
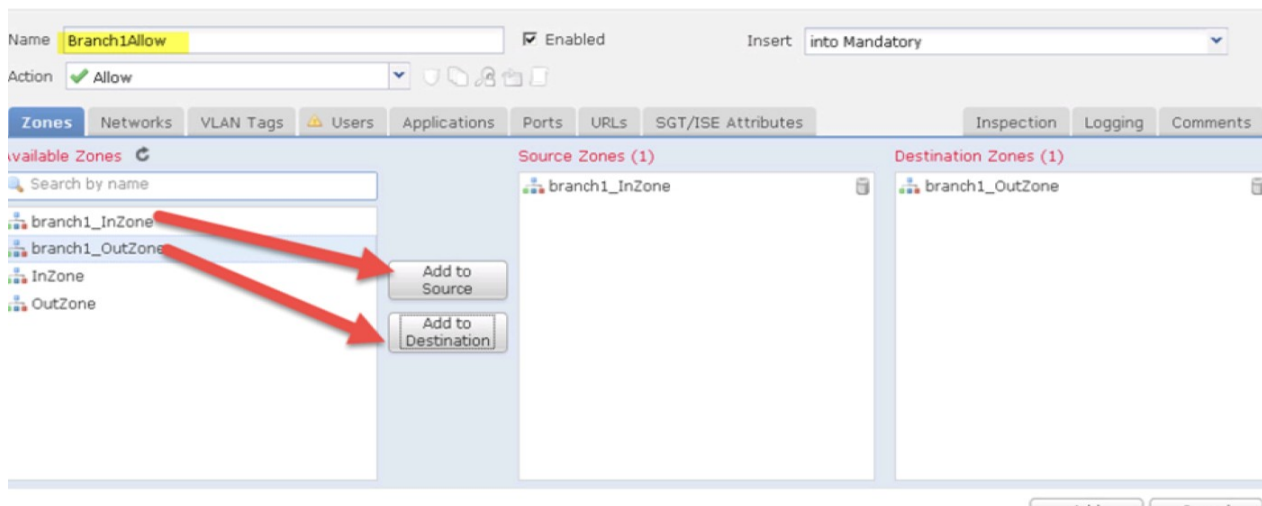
31. [ルール追加 (Add Rule)] をクリックします。
32. [自動NATルール (Auto NAT Rule)] を選択し、[タイプ (Type)] で [ダイナミック (Dynamic)] を選択します。
33. [インターフェイスオブジェクト (Interface Objects)] の下で **branch1_InZone** を選択します。[送信元に追加 (Add to Source)] をクリックします。
34. **branch1_Outzone**、[宛先に追加 (Add to Destination)] の順に選択します。



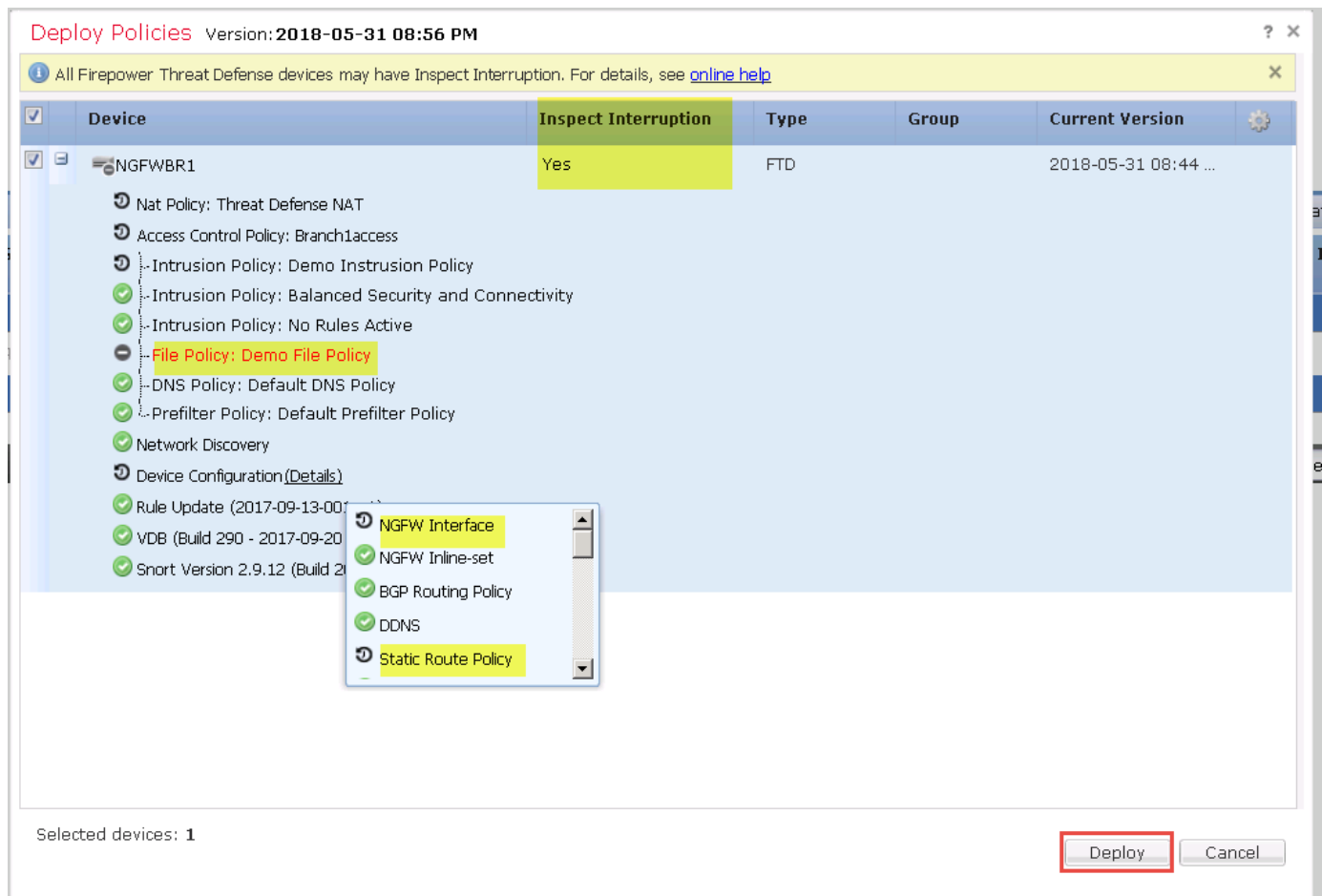
35. [トランスレーション (Translation)] タブの [元の packets (Original Packet)] の下で [(+)] を選択し、[新規ネットワークオブジェクト (New Network Object)] の [名前 (Name)] : **Branch1_Networks**、[ネットワーク (Network)] : **198.19.11.0/24** を設定します ([オブジェクト (Objects)] ページで、**198.18.0.0/15** などのラボ ネットワーク グループ全体を包含するオブジェクトを作成することもできます)。
36. [保存 (Save)] をクリックします。
37. [変換済みパケット (Translated Packet)] で [宛先インターフェイスIP (Destination Interface IP)] を選択します。
38. [OK] を選択し、Web ページの上部にある [保存 (Save)] を選択します。



39. アクセスコントロールポリシーを変更する場合は、[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)] に移動します。
40. 鉛筆アイコンをクリックして、Branch1 アクセスポリシーを編集します。
41. [ルールの追加 (Add Rule)] をクリックします。
42. ルールに **Branch1Allow** という名前を付けます。
43. 送信元として **branch1_InZone**、宛先として **branch1_OutZone** を選択します。
44. [インスペクションポリシー (Inspection Policy)] で、[デモ侵入ポリシー (Demo Intrusion Policy)] と [デモファイルポリシー (Demo File Policy)] を選択します。

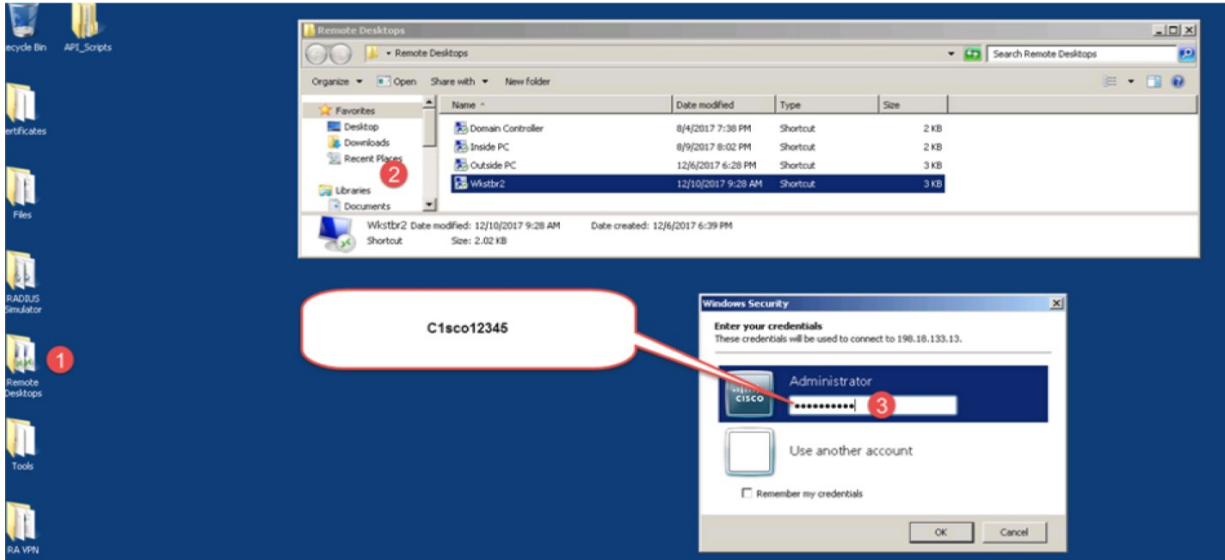


45. [追加 (Add)] をクリックし、Web ページ上部にある [保存 (Save)] をクリックします。[導入 (Deploy)] をクリックして、**ngfwbr1** を選択します。



Firepower Device Manager (FDM オンボックス) を使用したブランチ 2 の管理の設定

1. Jump PC からリモート デスクトップ フォルダを開きます。
2. **Wkstbr2** を選択します。
3. Windows セキュリティ プロンプトが表示されたら、パスワード : **C1sco12345** を使用します。
4. [OK] をクリックします。



注： オンボックス マネージャを使用して FTD を設定するには、**192.168.45.0/24 サブネット**上にいる必要があります。デフォルトの FTD アドレスは **192.168.45.45/32** で、デフォルト ゲートウェイは **192.168.45.1** です。ワークステーションでセカンダリ NIC カードの RDP セッションを開き、ワークステーションと FTD 間のローカル接続をシミュレーションできるようにします。FTD と同じサブネット上に存在させるために、ワークステーションの IP アドレスは **192.168.45.225/32** になっています。

5. ワークステーションで PuTTY を開き、192.168.45.45 と入力し、**admin/C1sco12345!**、ポート 22 (SSH) でログインします。

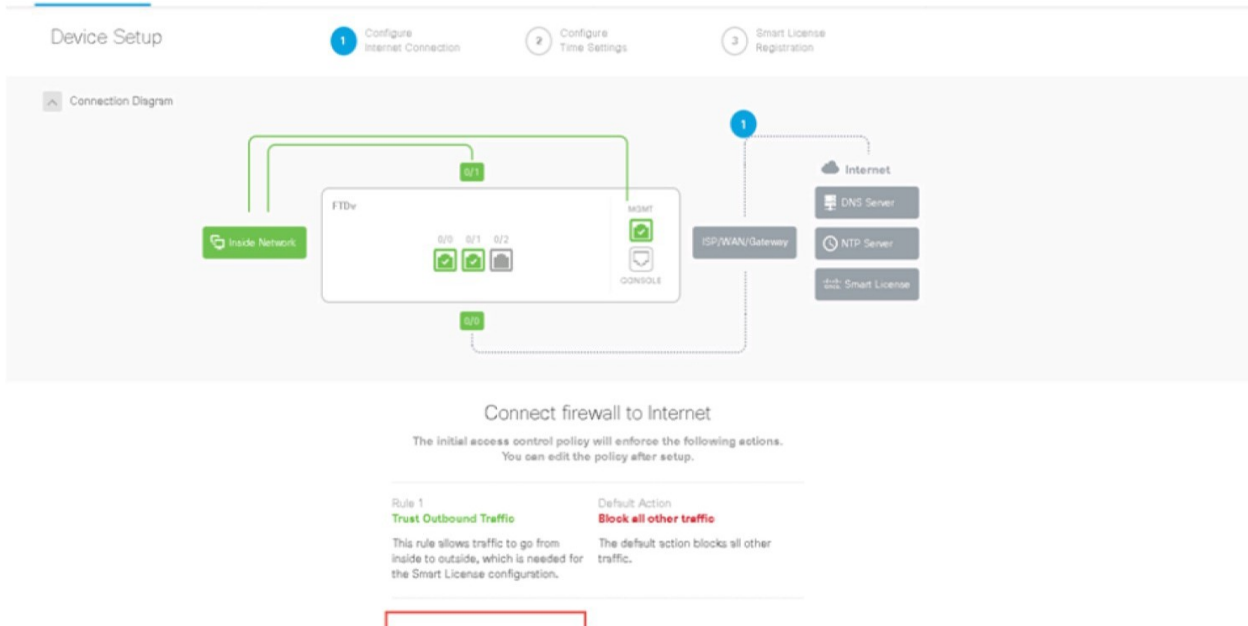
注： GUI を使用してパスワードを変更する場合は、パスワードに特殊文字を含める必要があります。そのため、パスワードに「!」を入れています。CLI を使用してパスワードを設定する場合、特殊文字は必要ありません。

6. **configure manager delete** と入力します。
 - a. **yes** と入力します。
 - b. 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： FDM (オンボックス マネージャ) は、ソフトウェアのアップグレードのために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。Web サービスが利用可能になるには少し時間がかかります。

7. Firefox ブラウザを開くと、192.168.45.45 に移動します。
8. [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。
9. **admin/C1sco12345!** でログインします。

10. 次の画面が開き、FTD の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)] まで下方方向にスクロールします。

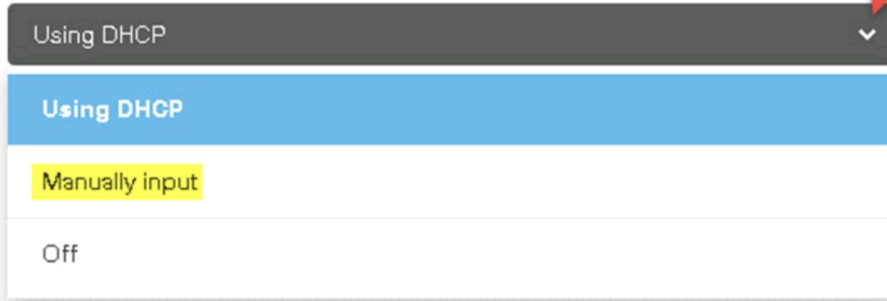


11. [DHCPを使用 (Using DHCP)] の横の矢印をクリックします。
12. [手動入力 (Manual Input)] をクリックします。

Outside Interface Address

Connect GigabitEthernet0/0 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4



13. [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**

Outside Interface Address

Connect GigabitEthernet0/0 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4

Manually input

IPv4 Address

198.18.133.4

Network Mask

Manually input

255.255.192.0

Gateway

198.18.128.1

Configure IPv6

Using DHCP

14. 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。
15. ターシャリ サーバ **198.18.128.1** をチェックします。
16. ホスト名 **NGFWBR2** をチェックし、[次へ (Next)] をクリックします。

Management Interface

Configure DNS Servers

USE OPENDNS

Primary DNS IP Address

208.67.222.222

Secondary DNS IP Address

208.67.220.220

Tertiary DNS IP Address

198.18.128.1

Firewall Hostname

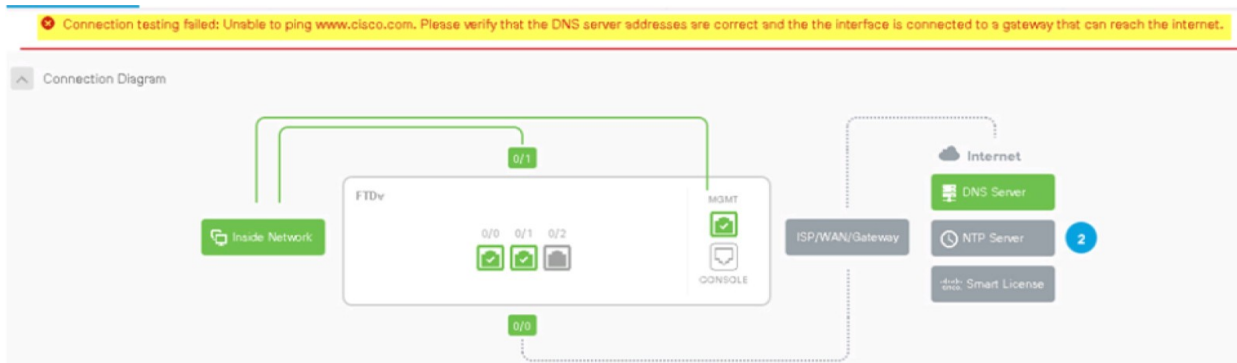
NGFWBR2

NEXT

Don't have internet connection?

[Skip device setup](#)

17. 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、問題はありません。NTP サービスの設定に進みます。



18. NTP サーバを手動で設定します。

- a. [タイムゾーン (Time Zone)] を選択します。
- b. [NTPタイムサーバ (NTP Time Server)] : ユーザ定義
- c. [アドレス (Address)] : **198.18.128.1**
- d. [次へ (Next)] をクリックします。

System Time: 10:39:42PM March 21 2019 -06:00

Time Zone

[UTC-04:00] America/New_York

NTP Time Server

User-Defined NTP Servers

Server Name or IP address

198.18.128.1|

Add another NTP time server

BACK

NEXT

19. 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。

that your device can participate in additional service offerings from Cisco such as technical support services, cloud management and monitoring services. Your device will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling both Cisco Success Network and Cisco Defense Orchestrator. Disabling both will disconnect the device from the cloud.

Disconnection of Cisco Success Network and Cisco Defense Orchestrator will not impact the receipt of updates or operation of the Smart Licensing capabilities; such functions will continue to operate normally.

Enable Cisco Success Network

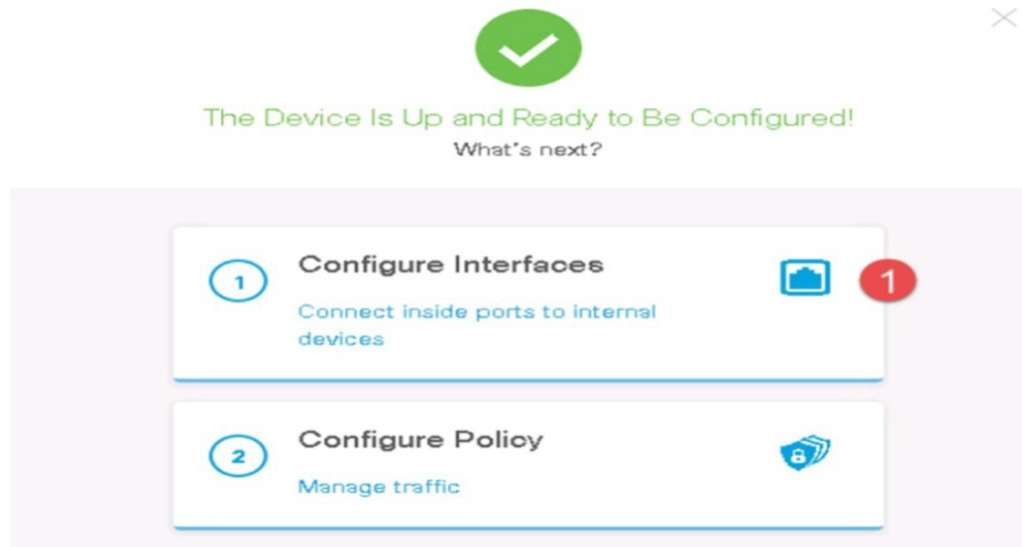
Start 90-day evaluation period without registration

Please make sure you register with Cisco before the evaluation period ends. Otherwise you will not be able to make any changes to the device configuration.

BACK FINISH

20. 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。

21. [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。

シナリオ 3 : FlexConfig

この演習は、次のタスクで構成されています。

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

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

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

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

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

手順

ユーザ定義の FlexConfig オブジェクトを作成する

1. FMC UI で、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] の順に選択します。
2. 左側のナビゲーション パネルの下部にある [FlexConfig] で、[FlexConfig オブジェクト (FlexConfig Object)] を選択します。
3. [FlexConfig オブジェクトの追加 (Add FlexConfig Object)] をクリックします。
 - a. [名前 (Name)] に **myEIGRP** と入力します。
 - b. メインのテキスト領域に次のコマンドを入力します。
 - i. `router eigrp 10`
 - ii. `network 198.18.128.0 255.255.192.0`
 - c. [保存 (Save)] をクリックします。

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

FMC UI の [オブジェクト管理 (Object Management)] ページが表示されていることを確認します。

1. **Default_Inspection_Protocol_Disable** という Flex オブジェクトの右側にある虫めがねアイコンをクリックします。このオブジェクトを編集することはできませんが、必要に応じてコピーすることができます。

注： FlexConfig オブジェクトは Apache Velocity 言語で記述されています。この言語ではループと if ステートメントがサポートされています。

ループと if ステートメントの先頭には # が付きます。これはコメントではありません。出力に含まれるリテラル テキストではないということです。コメントの先頭には ## が付きます。

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

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

FlexConfig ポリシーを作成して設定する

1. メニューから [デバイス (Devices)] > [FlexConfig] の順に選択します。[新しいポリシー (New Policy)] をクリックします。
 - a. [名前 (Name)] に **NGFW1_Test Flex Policy** と入力します。
 - b. デバイス **NGFW1** を選択します。[ポリシーに追加 (Add to Policy)] をクリックします。
2. [保存 (Save)] をクリックします。
3. 数秒後にポリシーが開き、編集できるようになります。
 - a. 左側の列の [ユーザ定義 (User Defined)] で、[myEIGRP] を選択します。[追加 (Add)] をクリックして、FlexConfig オブジェクトをポリシーに追加します。
 - b. 左側の列の [システム定義 (System Defined)] で、[Default_Inspection_Protocol_Disable] を選択します。[追加 (Add)] をクリックして、FlexConfig オブジェクトをポリシーに追加します。
4. [保存 (Save)] をクリックします。
5. [設定のプレビュー (Preview Config)] をクリックします。

6. [デバイスの選択 (Select Device)] ドロップダウン リストから [NGFW1] を選択します。
7. 数秒後に設定の変更が表示されます。コマンドが正しいことを確認します。
8. [閉じる (Close)] をクリックします。

変更を導入して設定をテストする

NGFW1 CLI から `show running-config policy-map type inspect sip global_policy` を実行します。SIP 検査が有効になっていることを確認します。

1. 内部 Linux サーバ セッションで、`ping 204.44.14.1` と入力します。これは失敗するはずですが。
2. 変更を導入します。導入が完了するまで待ちます。

2 total 0 running 2 success 0 warnings 0 failures		Show History
✓ NGFW1	Deployment to device successful.	2m 26s
✓ ngfwbr1	Deployment to device successful.	1m 16s

3. **NGFW1 CLI** から `show running-config policy-map type inspect sip global_policy` を実行します。SIP 検査が無効になっていることを確認します。
4. **NGFW1 CLI** から `show eigrp neighbors` を実行します。FTD と CSR ルータ間で隣接関係が形成されていることを確認します。
5. **NGFW1 CLI** から `show eigrp topology` を実行します。EIGRP ルートが受信されていることを確認します。
 - a. ネットワーク **203.14.10.0/24** を探します。

注：サクセサのないルートもいくつか表示されます。それらのルートは次のセクション BGP で使用されます。

6. `show route eigrp` を実行します。**NGFW1** で、EIGRP が認識したルートがルーティング テーブル内にあることを確認します。

シナリオ 4： NAT およびルーティング

この演習は、次のタスクで構成されています。

- このラボ演習に必要なオブジェクトを作成する
- スタティック NAT を設定する
- アクセス コントロール ポリシーを変更して `wwwin` への外部アクセスを許可する
- BGP を設定する
- 変更を導入して設定をテストする このラボ演習の目的は次の 2 つです。
- パブリック Web サーバを作成する
- BGP を設定する

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

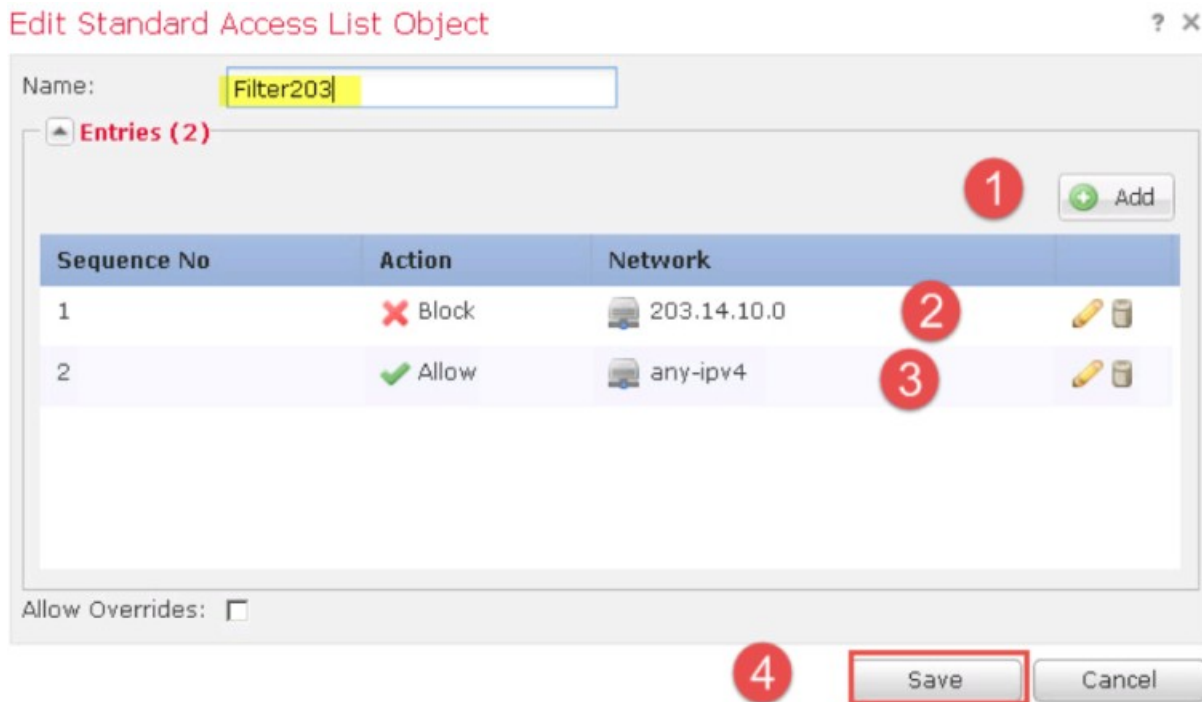
注：パブリック サーバは、内部ネットワークに導入されます。これは DMZ に導入する方がより現実的ですが、手間も増えます。ただし、ラボ ポッドにはこの機能が用意されています。ラボ ポッドで DMZ を作成する方法の詳細については、付録 4 を参照してください。

手順

このラボ演習に必要なオブジェクトを作成する

1. メニューから [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] の順に選択します。[ネットワーク (Network)] オブジェクト ページが選択されます。
 - a. [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] の順にクリックします。
 - b. [名前 (Name)] に `wwwin` と入力します。
 - c. [ホスト (Host)] オプション ボタンをクリックします。
 - d. または、[ネットワーク (Network)] に `198.19.10.202` と入力します。
 - e. [保存 (Save)] をクリックします。
 - f. [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。
 - g. [名前 (Name)] に `wwwout` と入力します。
 - h. [ホスト (Host)] オプション ボタンをクリックします。
 - i. [ネットワーク (Network)] に `198.18.128.202` と入力します。

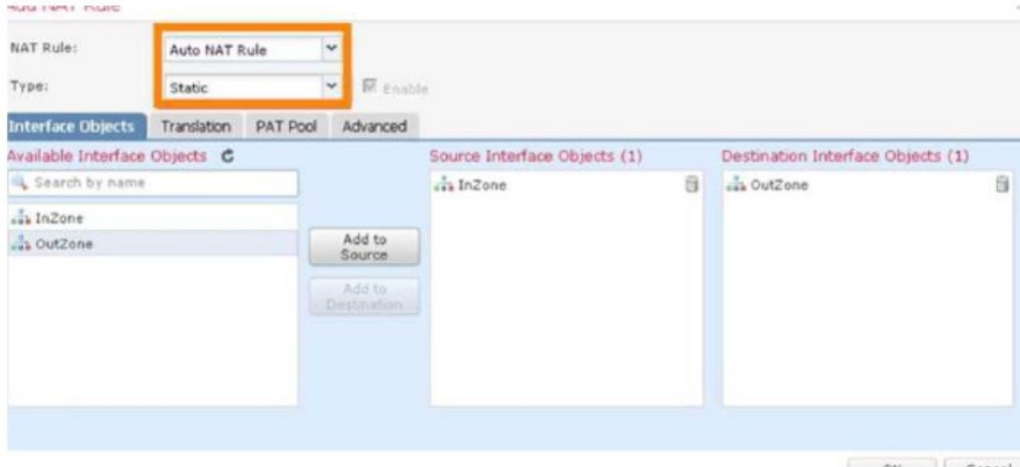
- j. [保存 (Save)] をクリックします。
2. [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] の順にクリックします。
 - a. [名前 (Name)] に **203.14.10.0** と入力します。
 - b. [ネットワーク (Network)] をクリックします。
 - c. **203.14.10.0/24** と入力します。
 - d. [保存 (Save)] をクリックします。
3. 左側のナビゲーション ペインで、[アクセスリスト (Access List)] > [標準 (Standard)] の順に選択します。
 - a. [標準アクセスリストを追加 (Add Standard Access List)] をクリックします。
 - b. [名前 (Name)] に **Filter203** と入力します。
 - c. 次に示す 2 つのアクセス制御エントリを追加します。2 番目のエントリは、リストの最後にあるすべてを対象とした暗黙の deny であるため、非常に重要です。
 - d. [保存 (Save)] をクリックします。



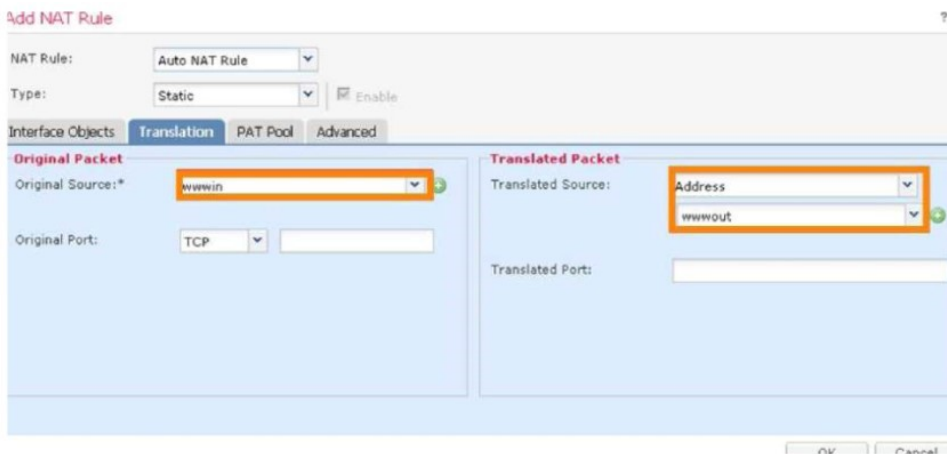
スタティック NAT を設定する

1. メニューから [デバイス (Devices)] > [NAT] の順に選択します。
2. 鉛筆アイコンをクリックして、[デフォルトPAT (Default PAT)] ポリシーを編集します。
3. [ルールの追加 (Add Rule)] をクリックします。
 - a. [タイプ (Type)] ドロップダウン リストから [自動NATルール (Auto NAT Rule)] を選択します。

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



- c. [OK] をクリックして NAT ルールを保存します。

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

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

1. メニューから [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. NGFW アクセス コントロール ポリシー (Base_Policy など) を編集します。

- a. [ルールの追加 (Add Rule)] をクリックします。
- b. [名前 (Name)] に **Web Server Access** と入力します。
- c. [挿入 (Insert)] ドロップダウン リストから [デフォルト (Default)] を選択します。
- d. [ゾーン (Zones)] タブはすでに選択されている必要があります。[InZone] を選択し、[宛先に追加 (Add to Destination)] をクリックします。
- e. [OutZone] を選択し、[送信元に追加 (Add to Source)] をクリックします。
- f. [ネットワーク (Networks)] タブを選択します。
- g. [wwwin] を選択し、[宛先に追加 (Add to Destination)] をクリックします。
- h. [ポート (Ports)] を選択します。[利用可能なポート (Available Ports)] の下で、**HTTP** と入力し、[HTTP] と [HTTPS] を選択して宛先に追加します。
- i. [選択した宛先ポート (Selected Destination Ports)] の下にある [プロトコル (Protocol)] ボックスに **ICMP select** と入力します。[追加 (Add)] をクリックします。

注： クライアントが接続する NAT されたアドレスではなく、Web サーバの正しい IP を使用しています。

- j. [インスペクション (Inspection)] タブを選択します。
 - k. [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。
 - l. [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。
 - m. [追加 (Add)] をクリックしてルールを追加します。
3. [保存 (Save)] をクリックして、アクセス コントロール ポリシーの変更を保存します。

BGP を設定する

1. メニューから [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。
2. 鉛筆アイコンをクリックして、デバイス **NGFW1** のデバイス設定を編集します。
 - a. [ルーティング (Routing)] タブを選択します。
 - b. [BGP] を選択し、[BGPを有効にする (Enable BGP)] チェックボックスをオンにします。
 - c. [AS番号 (AS Number)] を 10 に設定します。
 - d. 左側のナビゲーション ウィンドウで [BGP] を展開し、[IPv4] を選択します。
 - e. [IPv4を有効にする (Enable IPv4)] チェックボックスをオンにします。
 - f. [ネイバー (Neighbor)] タブをクリックし、[追加 (Add)] をクリックします。

- g. [IPアドレス (IP Address)] に **198.18.133.3** と入力します。
- h. [リモートAS (Remote AS)] に **20** と入力します。
- i. [アドレスを有効にする (Enable address)] チェックボックスをオンにします。
- j. [着信アクセスリスト (Incoming Access List)] ドロップダウン リストから [Filter203] を選択します。
- k. [OK] をクリックして、ネイバーを追加します。

The screenshot shows the configuration page for a BGP neighbor in Cisco dCloud. The 'IP Address*' field contains '198.18.133.3' and 'Remote AS*' contains '20'. The 'Enabled address' checkbox is checked. The 'Filtering Routes' tab is active, and the 'Incoming Access List' dropdown is set to 'Filter203', highlighted with a red arrow. Below this, there are sections for 'Limit the number of prefixes allowed from the neighbor' and 'Control prefixes received from the peer'.

3. [保存 (Save)] をクリックして BGP 設定を保存します。

変更を導入して設定をテストする

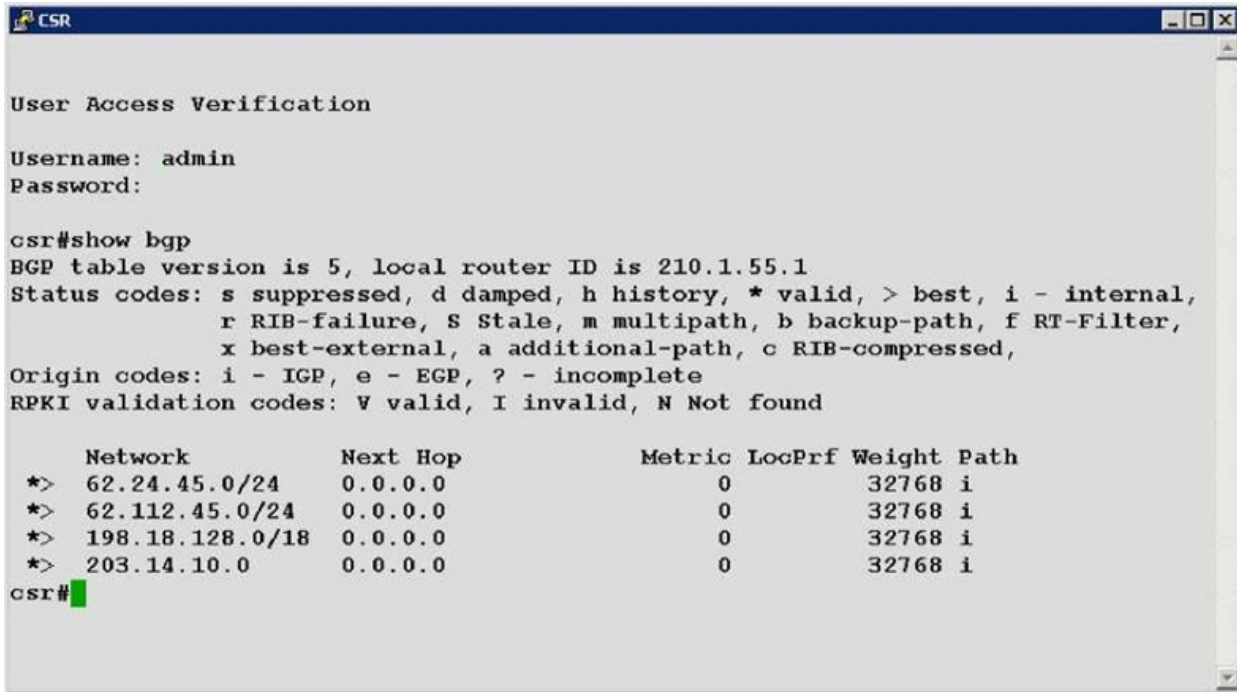
1. 変更を導入し、導入が完了するまで待ちます。
2. Jump Desktop で [PuTTY] リンクを開きます。[外部Linuxサーバ (Outside Linux Server)] という事前設定されたセッションをダブルクリックします。

root、パスワード C1sco12345 でログインします。

- a. **curl wwwout** と入力します。これは成功するはずですが。
- b. **ssh wwwout** と入力します。これは失敗するはずですが。

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

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



```

CSR
User Access Verification

Username: admin
Password:

csr#show bgp
BGP table version is 5, local router ID is 210.1.55.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
  *> 62.24.45.0/24   0.0.0.0           0         32768 i
  *> 62.112.45.0/24  0.0.0.0           0         32768 i
  *> 198.18.128.0/18 0.0.0.0           0         32768 i
  *> 203.14.10.0     0.0.0.0           0         32768 i
csr#

```

4. **NGFW1** の CLI から次の手順を実行します。
5. **show route** を実行します。BGP から学習した唯一のルートが **62.24.45.0/24** および **62.112.24.0/24** であることを確認します。**203.14.10.0/24** が BGP から正常に除外されている点に注目してください。ただし FlexConfig シナリオを実行した場合、このルートは外部 EIGRP ルートとして表示されます。
6. **show bgp** と **show bgp rib-failure** を実行します。これにより、198.18.128.0/18 ルートは、より適したルート（接続済み）が存在したために、ルーティングテーブルに挿入されなかったことがわかります。

注：このコマンドは、FMC から実行することもできます。

7. メニューから [デバイス (Device)] > [デバイス管理 (Device Management)] の順に選択します。
8. **NGFW1** デバイスを編集し、[デバイス (Devices)] タブを選択します。
9. レンチとドライバのアイコンをクリックします。
10. [高度なトラブルシューティング (Advanced Troubleshooting)] をクリックします。
11. [脅威対策CLI (Threat Defense CLI)] タブを選択します。このタブから複数の NGFW CLI コマンドを実行できます。

注：このコマンドは、FMC から実行することもできます。

12. コマンドの表示 :

- a. ルートと [実行 (Execute)] ボタン
- b. BGP と [実行 (Execute)] ボタン
- c. eigrp ネイバーと [実行 (Execute)] ボタン

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

シナリオ 5： プレフィルタ ポリシー

この演習は、次のタスクで構成されています。

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

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

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

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

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



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

注：この演習は、シナリオ 4 を終了していることが前提条件になります。これは、198.19.10.202 を 198.18.128.202 に変換するスタティック NAT ルールをこの演習で使用するためです。トンネル インターフェイスの設定を確認するために、内部および外部サーバの `/etc/sysconfig/network-scripts/ifcfg-tunO` を検査できます。

手順

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

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

1. SSH セッションが内部 Linux サーバに対して今も開いている必要があります。
2. 外部 Linux サーバに対する SSH セッションがない場合は、Jump Desktop で PuTTY を起動し、事前定義されている [外部 Linuxサーバ (Outside Linux Server)] セッションをダブルクリックします。**root**、パスワード **C1sco12345** でログインします。
3. 内部 Linux サーバと外部 Linux サーバの間に GRE トンネルを作成します。
 - a. 外部 Linux サーバの CLI で、**ifup tun0** と入力します。
 - b. 内部 Linux サーバの CLI で、**ifup tun0** と入力します。
 - c. 内部 Linux サーバで次のコマンドを使用して、トンネルを通じて ping を送信できることを確認します。**ping 10.3.0.2**.

IPS 機能をテストします。

1. 内部 Linux サーバの CLI から、次のコマンドを実行します。[ftp 10.3.0.2](#)
 - a. **guest**、パスワード **C1sco12345** でログインします。
 - b. **cd ~root** と入力します。次のメッセージが表示されます。
 - c. 421 Service not available, remote server has closed connection.
 - d. **quit** と入力して、FTP を終了します。
2. FMC で、メニューから [分析 (Analysis)] > [侵入 (Intrusions)] > [イベント (Events)] の順に選択します。
 - a. 左側の矢印をクリックして、イベントのテーブル ビューにドリル ダウンします。
 - b. 送信元および宛先 IP が、それぞれ 10.3.0.1 と 10.3.0.2 であることを確認します。
3. **内部 Linux サーバの CLI** で次のコマンドを実行して、ファイル ブロックおよびマルウェア ブロック機能をテストします。

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

- a. 制御テストとして、WGET を使用して、ブロックされていないファイルをダウンロードします。**wget -t 1 10.3.0.2/files/ProjectX.pdf**.
- b. これは成功するはずです。
- c. 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 10.3.0.2/files/test3.avi**.

注：ダウンロードされるのはファイルのごく一部です。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。

d. 最後に、WGET を使用してマルウェアをダウンロードします。

e. `wget -t 1 10.3.0.2/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。

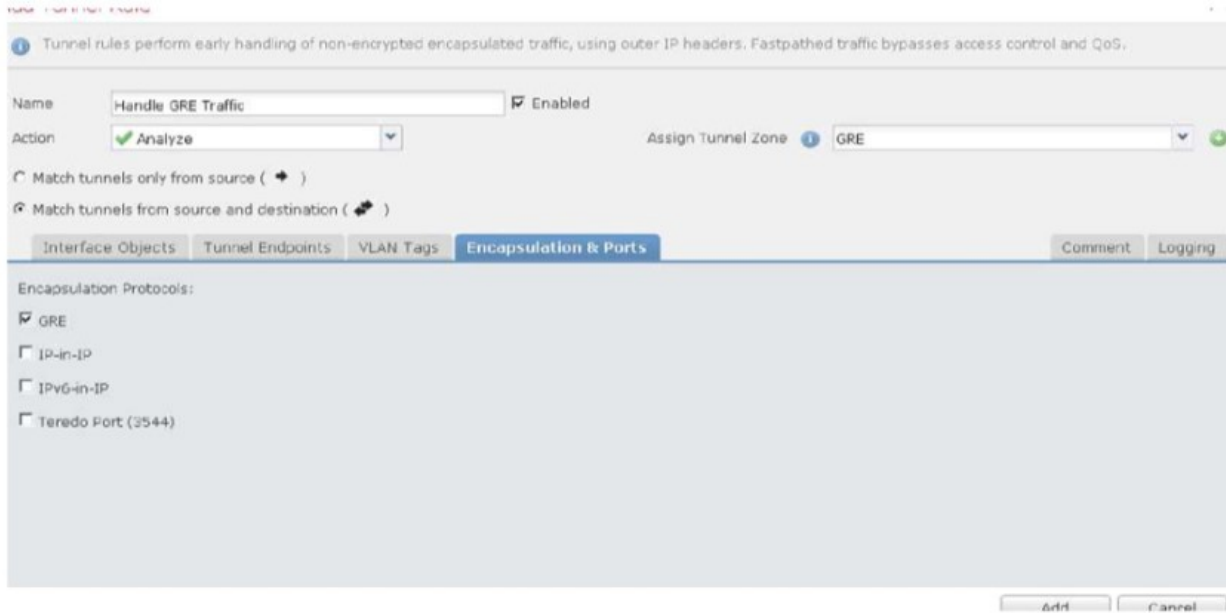
4. FMC で、メニューから [分析 (Analysis)] > [ファイル (Files)] > [ファイルイベント (File Events)] の順に選択します。
 - a. [ファイルイベントのテーブルビュー (Table View of File Events)] をクリックします。
 - b. 送信 IP と受信 IP が、それぞれ 10.3.0.2 と 10.3.0.1 であることを確認します。

トンネル ゾーンを作成する

1. メニューから [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] の順に選択します。
 - a. 左側のナビゲーション ペインで [トンネルゾーン (Tunnel Zone)] を選択します。
 - b. [トンネルゾーンの追加 (Add Tunnel Zone)] をクリックします。
 - c. [名前 (Name)] に **gre** と入力します。
 - d. [保存 (Save)] をクリックします。

プレフィルタ ポリシーを作成する

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



注： 次の 3 つのアクションがあります。

- [分析 (Analyze)] : トラフィックが Snort に送信され、アクセス ポリシー ルールが適用されます。
- [ブロック (Block)] : トラフィックがブロックされます。
- [ファストパス (Fastpath)] : トラフィックが許可され、以降の検査がバイパスされます。

注： このポリシーに対するプレフィルタ ルールを作成することもできます。これにより、レイヤ 2 から 4 の情報に基づいて、トラフィックの分析、ブロック、ファストパスが可能になります。

4. [追加 (Add)] をクリックしてルールを追加します。
5. [保存 (Save)] をクリックして、プレフィルタ ポリシーを保存します。

アクセス コントロール ポリシーを変更する

1. メニューから [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)] の順に選択して、NGFW Base_Policy アクセス コントロール ポリシーを編集します。
2. ポリシー ルール上の文字列 [プレフィルタポリシー (Prefilter Policy)] の右側にある [デフォルトプレフィルタポリシー (Default Prefilter Policy)] リンクをクリックします。
3. [NGFWプレフィルタポリシー (NGFW Prefilter Policy)] を選択します。
4. [OK] をクリックします。
 - a. [ルール (Rules)] タブを選択します。
 - b. [ルールの追加 (Add Rule)] をクリックします。
 - c. 「**Block ICMP Over GRE**」ルールを呼び出します。

- d. [挿入 (Insert)] ドロップダウン リストから [必須ルールに挿入 (into Mandatory)] を選択します。
 - e. [アクション (Action)] を [ブロックしてリセット (Block with reset)] に設定します。
 - f. [使用可能なゾーン (Available Zones)] 列で [GRE] を選択して、[送信元に追加 (Add to Source)] をクリックします。
 - g. [使用可能なアプリケーション (Available Applications)] 列で [ICMP] を選択して、[ルールに追加 (Add to Rule)] をクリックします。
 - h. [ロギング (Logging)] タブを選択します。[接続開始時にロギング (Log at Beginning of Connection)] チェックボックスをオンにします。
 - i. [追加 (Add)] をクリックして、ポリシーにルールを追加します。
5. [ルールの追加 (Add Rule)] をクリックします。
- a. 「**Allow GRE Traffic**」ルールを呼び出します。
 - b. [挿入 (Insert)] ドロップダウン リストから [デフォルト (Default)] を選択します。これは、アクセス コントロール ポリシーで最後のルールになります。
 - c. [使用可能なゾーン (Available Zones)] 列で [GRE] を選択して、[送信元に追加 (Add to Source)] をクリックします。
 - d. [インスペクション (Inspection)] タブを選択します。
 - e. [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。
 - f. [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。
 - g. [追加 (Add)] をクリックして、ポリシーにルールを追加します。
 - h. [保存 (Save)] をクリックして、アクセス コントロール ポリシーを保存します。

変更を導入して設定をテストする

1. 以前と同様に、変更内容を導入します。導入が完了するまで待ちます。
2. 外部 Linux サーバで、**tcpdump -n -i tun0** を実行してトンネル トラフィックをモニタします。
 - a. 内部 Linux サーバの CLI で、次のコマンドを実行します。
 - b. **wget 10.3.0.2**。これは成功するはずです。
 - c. **ping 10.3.0.2**

ping がブロックされていることを示す次の出力が表示されます。

```
From 10.3.0.2 icmp_seq=1 Packet filtered
```

3. 外部 Linux サーバで **tcpdump** コマンドの出力を調べて、ping が 10.3.0.2 に送信されていないことを確認します。

4. 上記の結果を取得していない場合

- a. トンネルを切断します。
 - i. 外部 Linux サーバの CLI で、**ifdown tun0** と入力します。
 - ii. 内部 Linux サーバの CLI で、**ifdown tun0** と入力します。
- b. トンネルを再確立します。
 - i. 再テストします。
 - ii. それでも上記の結果が表示されない場合
 1. FMC で、[分析 (Analysis)] > [接続 (Connections)] > [イベント (Events)] の順に選択します。
 - a. 10.3.0.1 から 10.3.0.2 へのトラフィックを探します。
 - i. ICMP トラフィックがリセットされたブロックがあるはずです。
- c. トンネルを切断します。

©2019 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2019 年 7 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



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>

お問い合わせ先