

# Cisco Firepower 次世代ファイアウォール 6.5

## ラボ v1.1

最終更新日：2020年1月21日

**重要：**このコンテンツはコミュニティが開発したものであり、標準の dCloud の検証やサポートの対象にはなりません。詳細については、dCloud サポートにお問い合わせください。

## 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：ポリシー概要](#)
- [シナリオ 2：脅威管理](#)
  - [Cisco Threat Intelligence Director \(CTID\)](#)
  - [セキュリティ インテリジェンスによるブラックリスト作成](#)
  - [URL フィルタリング](#)
  - [アプリケーション制御](#)
- [シナリオ 3：6.5 GUI ツアー](#)
- [シナリオ 4：レポート](#)
- [シナリオ 5：RADIUS を使用したリモートアクセス VPN AnyConnect \(オプション\)](#)
- [シナリオ 6：ハイアベイラビリティ設定 \(オプション\)](#)
  
- [付録 A：FMC の事前設定](#)
- [付録 B：REST API スクリプト](#)
- [付録 C：ISE RA VPN 設定](#)

## 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
<ul style="list-style-type: none"> <li>● ラップトップ</li> </ul>	<ul style="list-style-type: none"> <li>● Cisco AnyConnect®</li> </ul>

## 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) をはじ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ており、ベストエフォートの脅威防御に付け加えられたものです。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。

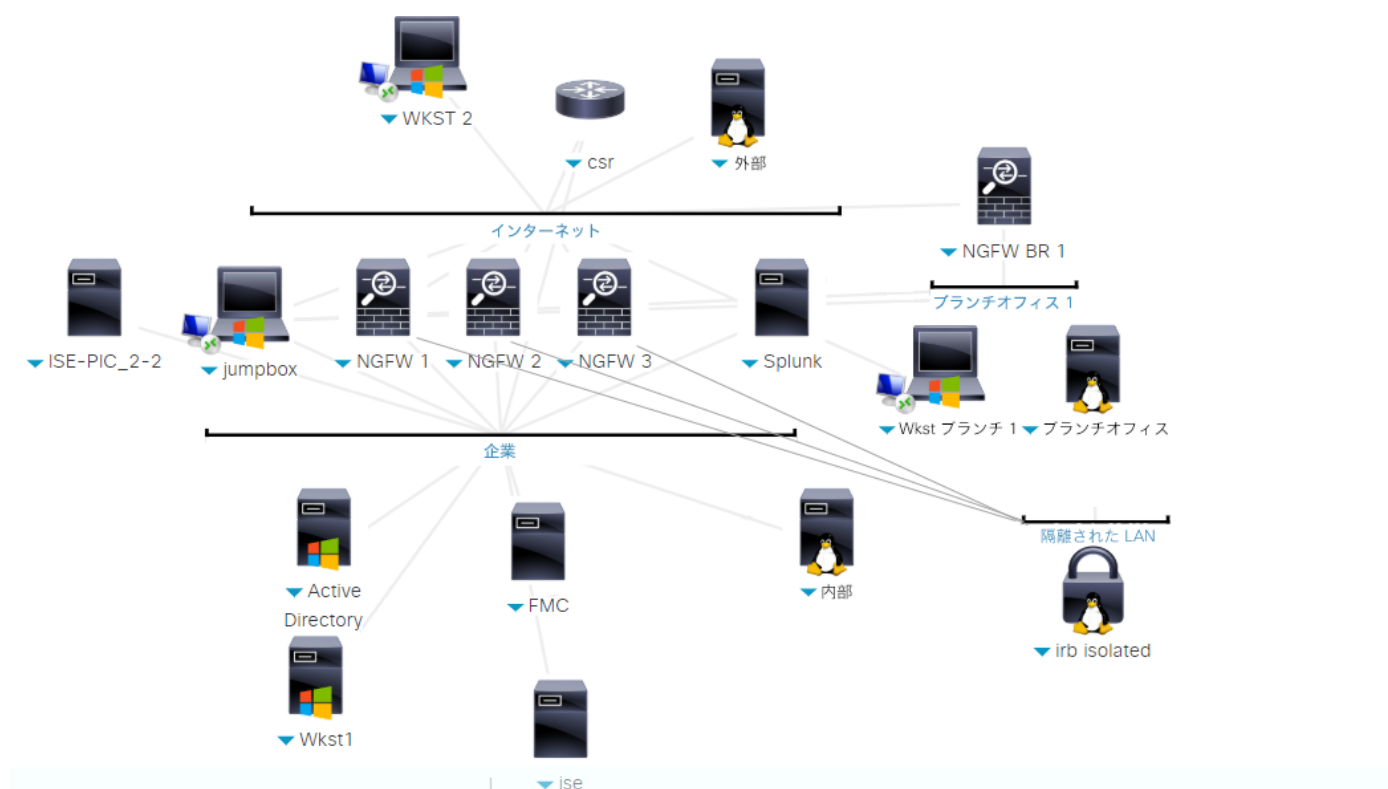
Cisco Firepower NGFW は、企業が最新の脅威に対するリアルタイムの阻止、優先順位付け、把握、対応自動化を図ることに焦点を合わせて進化することが可能です。Firepower NGFW は、包括的なネットワーク可視性、最高水準の脅威インテリジェンス、有効性の高い脅威防御を基盤にした脅威対策に重点を置いていることを特徴とし、既知の脅威と未知の脅威の両方に対応します。また、Advanced Malware Protection によって、レトロスペクティブセキュリティも可能にします。これは、防御を回避した巧妙な攻撃を「時間を遡って」迅速に特定し、修復するものです。これにより、業界平均と比較して、シスコのお客様の検出時間 (TTD) が大幅に短縮されます。

このラボでは、企業サイトと 2 つのブランチサイトの間に、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、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、このラボでは、FDM (Firepower Device Manager) を使用して NGFW を構成し、リモート アクセスおよびサイト間 VPN を設定し、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、あらかじめ定義された管理ユーザアカウントを使用してすべて設定できます。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して確認するか、クレデンシャルが必要となるシナリオ内の手順で確認できます。

図 1. dCloud のトポロジ



## はじめに

### プレゼンテーションの前に

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

場合によっては、環境を元の構成にリセットするため、このガイド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、最大で 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 : **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 デスクトップ接続を確認してください。ログインプロンプトのパスワードには C1sco12345 を入力していることを確認してください。

## シナリオ 1. 構成の概要

この演習は、次のタスクで構成されています。

- オブジェクトの確認
- ネットワーク検出ポリシーを変更する
- ベストプラクティスのポリシー設定を確認する
- アクセスコントロールポリシーの作成/変更
- 設定変更を展開する

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

## ステップ

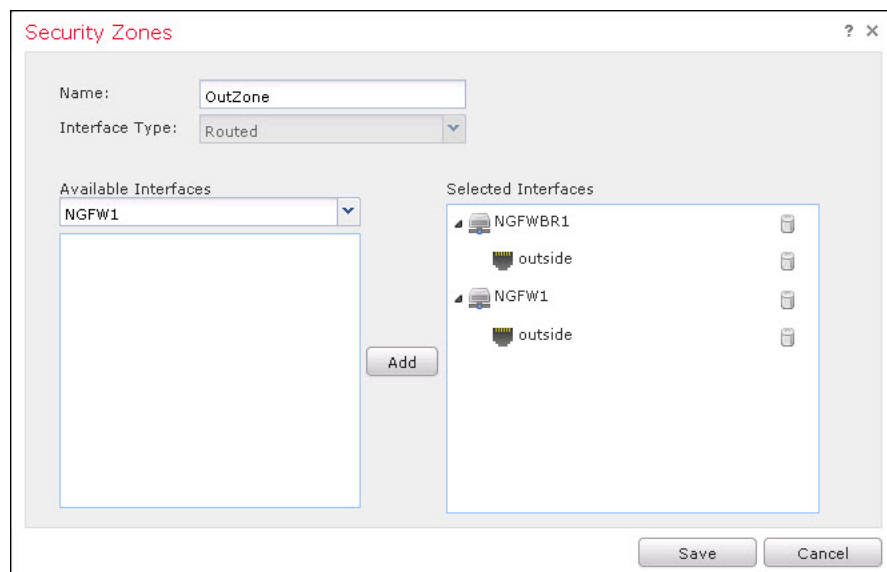
### 演習に必要なオブジェクトを確認する

1. Jump PC で Firefox ブラウザを開き、ブックマークを使用して、ログイン情報 admin/C1sco12345 で FMC にログインします。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. 左側の列で [ネットワーク (Network) ]を選択し、右上の検索ウィンドウで Lab と入力します。
  - b. Lab\_Networks の横にある鉛筆アイコンをクリックし、ネットワークオブジェクト構成を確認します。

The screenshot shows the 'Edit Network Object' dialog box. The 'Name' field contains 'Lab\_Networks'. The 'Network' type is set to 'Network' (selected). The 'Network' value is '198.18.0.0/15'. The 'Allow Overrides' checkbox is unchecked. The 'Save' and 'Cancel' buttons are at the bottom.

- c. [キャンセル (Cancel) ]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. Outzone の横にある鉛筆アイコンをクリックし、インターフェイスオブジェクトの構成を確認します。

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



b. [キャンセル (Cancel) ] をクリックします。

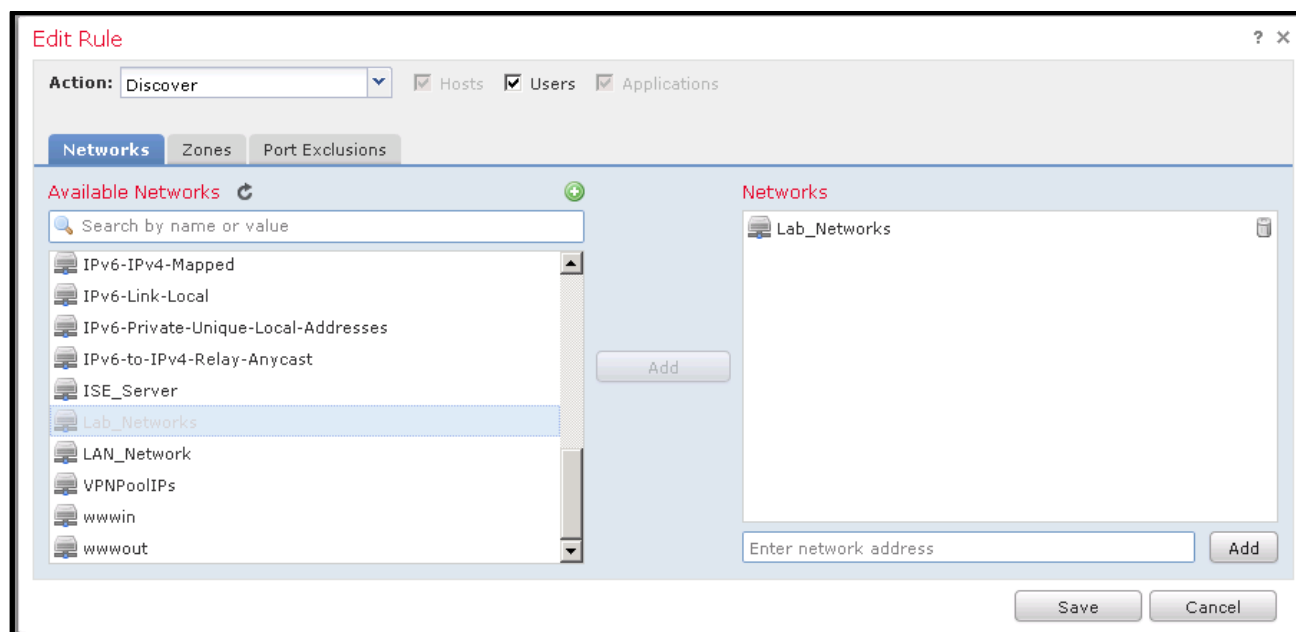
3. **必要に応じて**、InZone という名前のセキュリティゾーンを確認します。

### ネットワーク検出ポリシーの変更

Firepower システムは、ネットワーク検出ポリシーとアイデンティティポリシーを使用して、ネットワーク上のホスト、アプリケーション、およびトラフィックのユーザデータを収集します。いくつかのタイプの検出およびアイデンティティのデータを使用して、ネットワーク資産の包括的なマップを作成し、フォレンジック分析、動作プロファイリング、アクセスコントロールを実行し、組織で影響を受けやすい脆弱性とエクスプロイトの軽減および対応を行います

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、デフォルトでは FMC Firepower ホストライセンスの上限を超える場合があります。このため、ポリシーを変更して、プロファイルするネットワークセグメントを定義することをお勧めします。

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. **Lab\_Networks** を選択して、[追加 (Add) ] をクリックします。

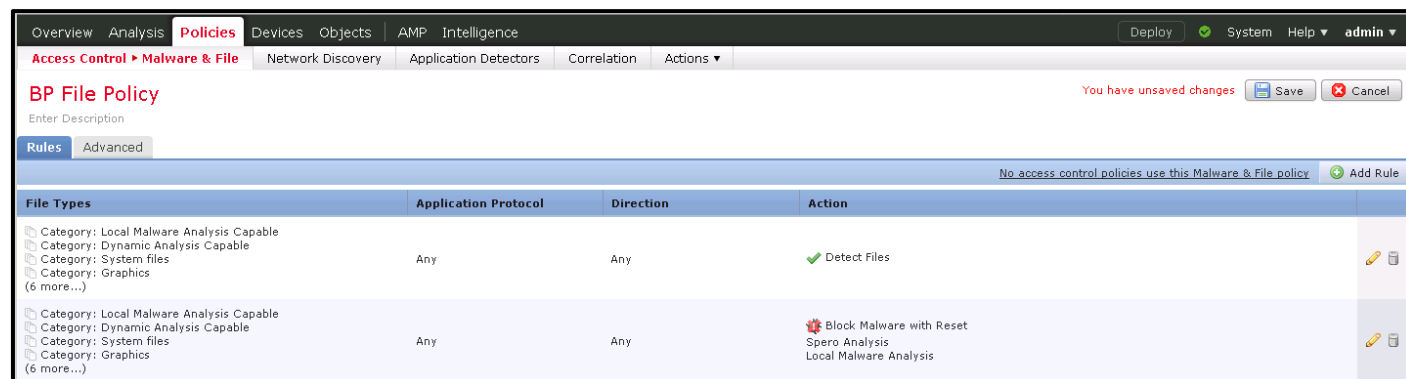


3. [保存 (Save) ] をクリックします。

### 事前定義済みポリシーの確認

検出ポリシーが更新されたので、次にマルウェアとファイルのポリシーを確認します。Firepower に対する高度なマルウェア防御により、ネットワークトラフィック内のマルウェアの送信を検出、キャプチャ、追跡、分析、記録、またブロック (オプション) することができます。Firepower Management Center の Web インターフェイスでは、この機能は AMP for Network と呼ばれます。高度なマルウェア防御では、インライン展開された管理対象デバイスおよび Cisco Cloud からの脅威データを使用してマルウェアを特定します。ファイルポリシーは、全体的なアクセスコントロール設定の一部として、マルウェア防御およびファイル制御を実行するためにシステムが使用する一連の設定です。この関連付けにより、アクセスコントロールルールの条件と一致するトラフィック内のファイルが、必ず最初に検査されるようになります。

1. メニューから、[ポリシー (Policies) ] > [アクセス制御 (Access Control) ] > [マルウェアとファイル (Malware & File) ] を選択します。
  - a. ポリシーの右側にある鉛筆アイコンをクリックして、BP ファイルポリシーを編集します。
  - b. 鉛筆アイコンをクリックして、[ルール (Rules) ] を表示します。
  - c. [キャンセル (Cancel) ] をクリックして、ポリシーを終了します。

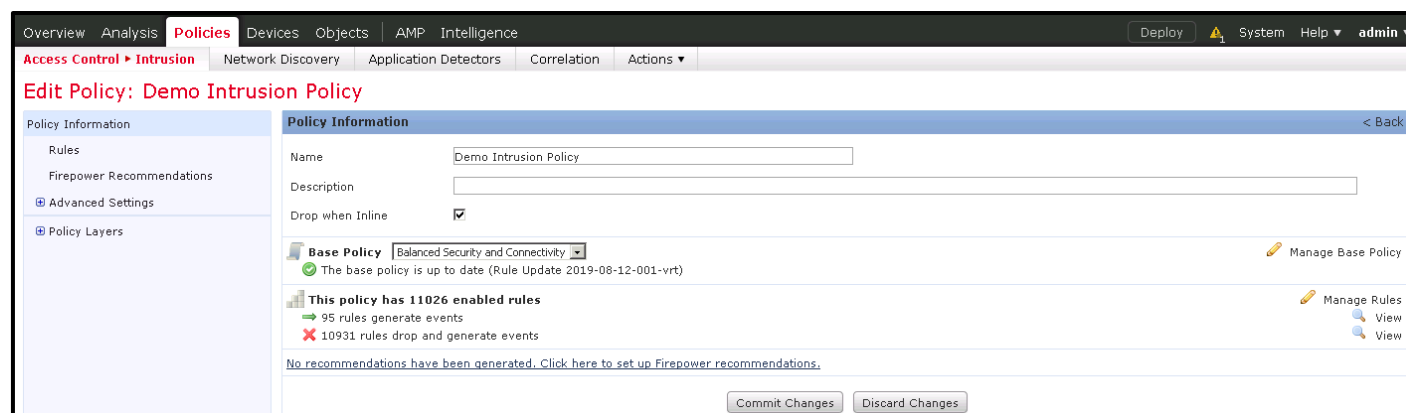


動的分析では、Cisco Threat Grid、シスコのファイル分析および脅威インテリジェンス プラットフォームを使用して、分析対象ファイルを送信します。デバイスは、対象となるファイルを Cisco Threat Grid（パブリッククラウドまたはオンプレミスアプライアンスのいずれか指定した方）に送信します。Cisco Threat Grid は、サンドボックス環境でファイルを実行し、ファイルの動作を分析してファイルに悪意があるかどうかを判断し、ファイルにマルウェアが含まれている可能性を示す脅威スコアを返します。

ネットワーク分析と侵入ポリシーは、Firepower システムの侵入検知および防御機能の一部として連携します。ネットワーク分析と侵入ポリシーはどちらも、親アクセス コントロール ポリシーによって呼び出されますが、そのタイミングは異なります。システムがトラフィックを分析するとき、ネットワーク分析の復号および前処理のフェーズは、侵入防御（追加の前処理と侵入ルール）のフェーズより前に、個別に発生します。ネットワーク分析ポリシーと侵入ポリシーは、共同で広範かつ深いパケット検査を提供します。これらによって、ホストとそのデータの可用性、整合性、および機密性を脅かす可能性があるネットワークトラフィックを検出、警告し、保護することができます。

Firepower システムでは、同じような名前（バランスのとれたセキュリティと接続性など）が付いた複数のネットワーク分析ポリシーと侵入ポリシーが提供され、それらのポリシーは相互に補完して連携します。システム提供のポリシーを使用することで、Cisco Talos Intelligence Group (Talos) のエクスペリエンスを活用できます。これらのポリシーに対して Talos は侵入とプリプロセスのルール状態を設定し、プリプロセッサの最初の設定とその他の高度な設定を行います。

2. メニューから [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] の順に選択します。
  - a. ポリシーの右側にある鉛筆アイコンをクリックして Demo Intrusion Policy（デモ侵入ポリシー）を編集します。
  - b. この侵入ポリシーの内容を確認し、基本ポリシーが「バランスの取れたセキュリティと接続性」に設定されていることに注目してください。これは推奨ポリシーです。
  - c. [変更の破棄 (Discard Changes)] をクリックしてポリシーを終了します。



## プレフィルタポリシー

プレフィルタリングは、システムがより多くのリソースを消費する評価を実行する前の、アクセス制御の初期段階です。このアイデアは、検査を必要としないトラフィックをできるだけ早く除外するためのものです。特定のタイプのプレーンテキストを Fastpass 処理またはブロックし、カプセル化された接続を検査することなく外側のカプセル化ヘッダーに基づいてトンネルをパススルーできます。また、早期処理のメリットがあるその他の接続についても、Fastpass 処理またはブロックできます。プレフィルタポリシーのルールでは、単純な 5 つのタプル条件が使用されます。



プレフィルタ段階でのトラフィックの Fastpath 処理により、以下を含む以降のすべての検査と処理がバイパスされます。

- セキュリティ インテリジェンス
- アイデンティティおよびアイデンティティポリシーによって課される認証要件
- SSL 復号
- アクセスコントロールルール
- パケットペイロードの詳細な検査
- 検出
- レート制限

## プレフィルタポリシーの確認

3. 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. ポリシーの右側にある鉛筆アイコンをクリックして、Demo Prefilter Policy を編集します。
  - b. フィルタポリシーの内容を確認します（これは実際のプレフィルタポリシーではなく、このラボ環境に固有の機能を提供します）。
  - c. [キャンセル (Cancel)] をクリックして、ウィンドウを閉じます。

#	Name	Rule Type	Source Interface Ob...	Destination Interface Ob...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone
1	Handle GRE Traffic	Tunnel	any	any	any	any	any	GRE (47)	any	Analyze	GRE
2	Fastpath Extranet1: Prefilter	Prefilter	InZone (Routed)	OutZone (Route	any	Extranet129	any	any	any	Fastpath	na
3	Fastpathed ICMP	Prefilter	InZone (Routed)	OutZone (Route	any	198.18.133.200	any	ICMP (1)	any	Fastpath	na
4	Analyzed ICMP	Prefilter	InZone (Routed)	OutZone (Route	any	198.18.133.201	any	ICMP (1)	any	Analyze	na
5	Blocked ICMP	Prefilter	InZone (Routed)	OutZone (Route	any	198.18.133.200	any	ICMP (1)	any	Block	na

Non-tunneled traffic is allowed      Default Action: Tunnel Traffic      Analyze all tunnel traffic

## アクセスコントロールポリシーを変更する

アクセスコントロールは、階層型のポリシーベースの機能であり、ネットワークトラフィックの指定、検査、およびログ記録（Fastpath 処理されていないもの）が可能です。各管理対象デバイスは、1つのアクセスコントロールポリシーによってターゲットにすることができます。

ポリシーのターゲットデバイスがネットワークトラフィックについて収集するデータは、以下に基づいてそのトラフィックをフィルタリングおよび制御するために使用できます。

- シンプルで簡単に決定されるトランスポート層およびネットワーク層の特性：送信元と宛先、ポート、プロトコルなど

- トラフィックに関する最新のコンテキスト情報（レピュテーション、リスク、ビジネスとの関連性、使用したアプリケーション、アクセスした URL などの特性）
  - レルム、ユーザ、ユーザグループ、または ISE 属性
  - カスタムセキュリティグループタグ (SGT)
  - 暗号化トラフィックの特性。このトラフィックを復号化して、詳細な分析を行うことも可能です。
  - 非暗号化トラフィックまたは復号化されたトラフィックに、禁止ファイル、検出されたマルウェア、侵入の試みが含まれているかどうか
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。
    - a. ポリシーの右側にある鉛筆アイコンをクリックして、Base\_Policy アクセス コントロール ポリシーを編集します。
    - b. ポリシーの右側にある鉛筆アイコンをクリックして、**Allow Outbound** ルールを編集します。

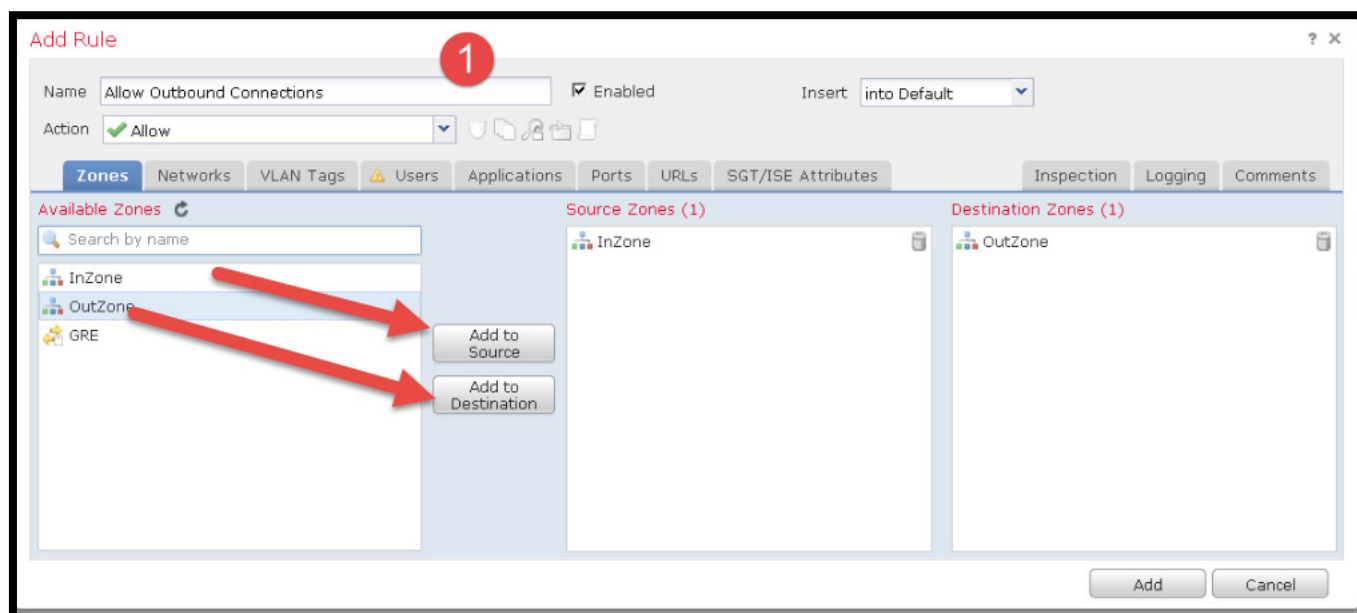
**注：**ルールは、ポリシー内の複数のセットに分割されます。次の 2 つのセットは事前に定義されています。

必須ルール：子ポリシーのルールに優先します。

デフォルトルール：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) ] タブがすでに選択されているはずですが。
  - a. [送信元ゾーン (Source Zone) ] には、**InZone** が示されています。
  - b. [宛先ゾーン (Destination Zone) ] には、**OutZone** が示されています。



3. [インスペクション (Inspection)] タブを選択します。
  - a. **Demo Intrusion Policy** が、すでに侵入ポリシーとして設定されているはずです。
  - b. [ファイルポリシー (File Policy)] ドロップダウンリストから **BP File Policy** を選択します。

**注：** デモ用の侵入ポリシーとファイルポリシーは、時間を節約するため事前に設定済みです。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 v2.5』の「付録 1」を参照してください。

4. [保存 (Save)] をクリックして、このルールの変更内容を保存します。
5. [詳細設定 (Advanced)] タブを選択します。
6. [アクティブな応答の最大数 (Maximum Active Responses)] フィールドは **25** です (**25** に設定されていない場合)。

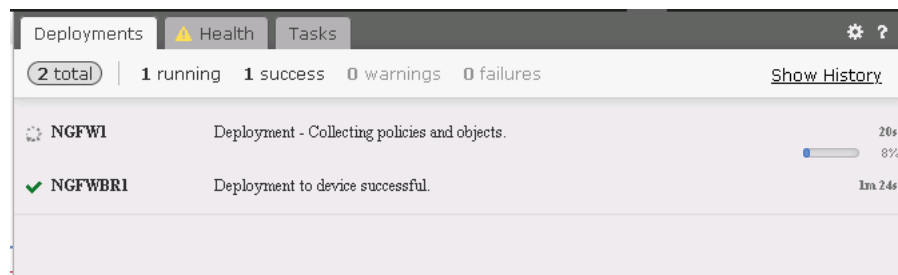
**注：** [アクティブな応答の最大数 (Maximum Active Responses)] を 0 より大きい値に設定すると、パケットをドロップする侵入ポリシードロップ (IPS) ルールが TCP リセットを送信して接続が閉じます。IPS ドロップをトリガーしない接続は、アクティブな応答の最大数の設定に関係なく、リセットしてブロック (Block with reset) がルールに適用されている場合や、Fastpath ブロックなどの LINA のみのドロップである場合に、FTD によってリセットされます。通常、クライアントとサーバの両方に TCP リセットが送信されます。以上のように設定すると、この接続からの追加のトラフィックが確認された場合に、最大 25 のアクティブな応答 (TCP リセット) が開始されます。

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

7. [保存 (Save) ]をクリックして、アクセス コントロール ポリシーの変更を保存します。
8. FMC の右上隅にある [展開 (Deploy) ]をクリックします。
  - a. NGFW1 デバイスのチェックボックスをオンにし、リストを展開して詳細を表示します。ページは次の図のようになります (正確に一致する必要はありません)。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。



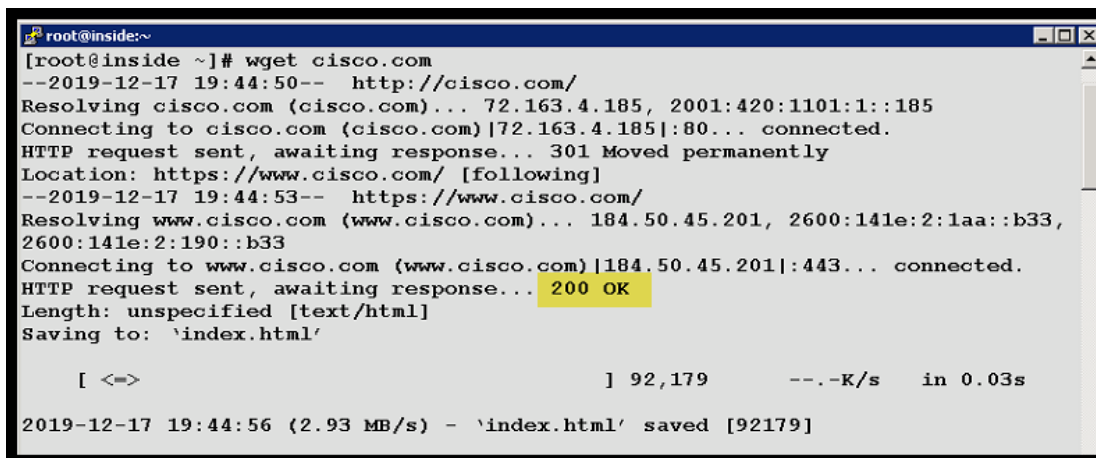
9. **NGFW1** の展開が変更されたことを確認し、アクセス コントロール ポリシー、ネットワーク検出、ファイルポリシーの設定が変更されることを確認します。他のポリシーや変更が表示されていても問題ありません。
  - a. [展開 (Deploy) ]をクリックします。
  - b. FMC の右上隅にある [展開 (Deploy) ]リンクの右側のアイコンをクリックします。展開が完了するまで待ちます。(完了のパーセンテージに注目してください)



## NGFW の展開をテストする

1. Jump PC で PuTTY を開き、内部 Linux サーバを選択して root/C1sco12345 でログインします。CLI で次の操作を行います。

- 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。



```

root@inside:~
[root@inside ~]# wget cisco.com
--2019-12-17 19:44:50-- http://cisco.com/
Resolving cisco.com (cisco.com)... 72.163.4.185, 2001:420:1101:1::185
Connecting to cisco.com (cisco.com)[72.163.4.185]:80... connected.
HTTP request sent, awaiting response... 301 Moved permanently
Location: https://www.cisco.com/ [following]
--2019-12-17 19:44:53-- https://www.cisco.com/
Resolving www.cisco.com (www.cisco.com)... 184.50.45.201, 2600:141e:2:1aa::b33,
2600:141e:2:190::b33
Connecting to www.cisco.com (www.cisco.com)[184.50.45.201]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `index.html'

[ <=> ] 92,179 --.-K/s in 0.03s

2019-12-17 19:44:56 (2.93 MB/s) - `index.html' saved [92179]

```

- 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. **attack0** と入力します。これにより、スクリプト化された iFrame イベントである Snort ルール 28796 がトリガーされます。

2. **ftp outside** と入力します。ユーザ名 : guest、パスワード : C1sco12345 でログインします。

**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。

- a. **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 : 550 エラーが発生した場合は、もう一度コマンドを入力する必要があります。
- b. **quit** と入力して、FTP を終了します。

3. 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 および 28796 がトリガーされたことを確認します。両方のイベントが表示されるまでに 2 ~ 3 分かかる場合があります。2 つのエントリが表示されない場合は、**attack0** と **ftp** 特権昇格ハッキングを再試行します。それでもイベントが表示されない場合は、図の下にある注記を参照してください。Demo Intrusion Policy で、336 のルール状態は [ドロップしてイベントを生成する (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。

Events By Priority and Classification (switch workflow)

[Drilldown of Event, Priority, and Classification](#) > [Table View of Events](#) > [Packets](#)

2019-12-05 21:25:26 - 2019-12-05 22:25:26 Expanding

No Search Constraints [\(Edit Search\)](#)

Jump to...

Message	Priority	Classification	Count
<input type="checkbox"/> EXPLOIT-KIT iFRAMer successful cnt.php redirection (1:28796:3)	high	A Network Trojan was Detected	1
<input type="checkbox"/> PROTOCOL-FTP CWD ~root attempt (1:336:17)	medium	Potentially Bad Traffic	1

« < Page 1 of 1 > » Displaying rows 1–2 of 2 rows

View Copy Delete Review Download Packets

View All Copy All Delete All Review All Download All Packets

**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。

- 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。イベントの詳細が表示されていることを確認します。注：優先順位は中程度として報告され、FTP イベントの [影響レベル (Impact Level)] は 2 です。その違いはどこにあるのでしょうか？優先順位は IPS ルールに基づいて設定されますが、影響レベルはネットワーク検出日（ホストプロファイル）と脆弱性情報の相関によって決定されます。影響レベル 2 は「潜在的に脆弱」を意味します。iFrame 攻撃に見られるような影響レベル 3 は、「知っておくと良いが、ターゲットは脆弱ではない」ということを意味します。
  - 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。
  - [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。
- ファイルとマルウェアの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 デスクトップの Strings ファイルからカットして貼り付けることができます。
- 内部 Linux サーバ**から root/C1sco12345 でログインします。これらの Wget コマンドは、Jump デスクトップの Strings ファイルからカットして貼り付けることができます。
  - 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** と入力します。これは成功するはずです。
  - 次に、WGET を使用して、**wget -t 1 outside/files/test3.avi** と入力し、ブロックされていないファイルのダウンロードを試みます。これは成功するはずです。
  - 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** と入力します。これは失敗するはずです。

**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。

7. 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。

The screenshot shows the 'Malware Summary' page in the Cisco FMC interface. The table below is a representation of the data shown in the screenshot.

Time	Action	Sending IP	Sending Country	Receiving IP	Receiving Country	Sending Port	Receiving Port	SSL Status
2019-12-12 19:19:34	Custom Detection Block	198.18.133.200		198.19.10.200		80	34038	Unknown (U)

8. 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が、転送の 99% で失敗します。

```
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。

9. マルウェアイベントのテーブルビューをクリックし、いずれかのマルウェアイベントの赤い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。
10. 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。また、オプションの Buddy.exe のダウンロードを試行し、ラボ環境からのクラウド接続が可能であった場合は 4 つのイベントが表示される場合があります。

The screenshot shows the 'File Summary' page in the Cisco FMC interface. The table below is a representation of the data shown in the screenshot.

Category	Type	Disposition	Action	Count
PDF files	PDF	Unknown	Malware Cloud Lookup	1
Executables	MSEXE	Malware	Malware Block	1
PDF files	PDF	Custom Detection	Custom Detection Block	1
Multimedia	RJFF		Detect	1

**注：**必要に応じてドリルダウンすることができます。

## シナリオ 2. 脅威の管理

### Cisco Threat Intelligence Director (CTID)

この演習は、次のタスクで構成されています。

- インシデントをトリガーする CTID に URL のリストをアップロードする
- 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オブザーバブルを生成します。NGFW は、オブザーバブルの検出を CTID にレポートします。CTID はそれらの観測結果がインシデントに該当するかどうかを判断します。

ソースには、オブザーバブルを含むインジケータが含まれています。インジケータは、脅威に関連付けられているすべての特性を示し、個々のオブザーバブルは、脅威に関連付けられた個別の特性 (SHA-256、IP アドレスなど) を表します。シンプルなインジケータは、1 つのオブザーバブルを含み、複雑なインジケータは 2 つ以上の観測対象が含まれます。

2 つのファイル形式がサポートされています。

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

これらのファイルを取得する方法は 3 つあります。

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

この演習の目的は、CTID を設定し、テストすることです。

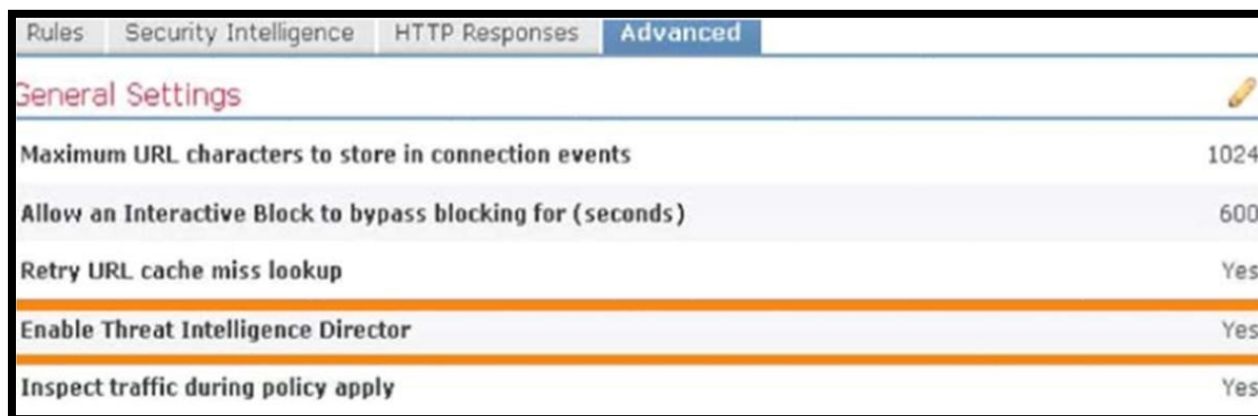
## 手順

### CTID がオブザーバブルを NGFW にパブリッシュすることを確認する

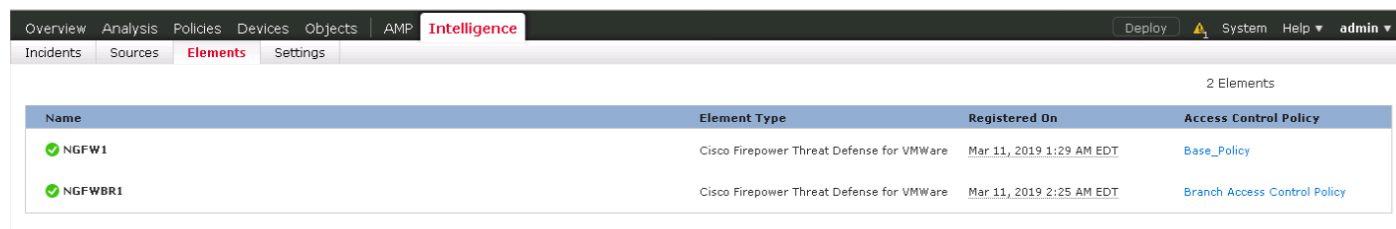
1. [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [アクセスコントロール (Access Control)] の順に選択します。
2. ポリシーの右側にある鉛筆アイコンをクリックして、**Base\_Policy** アクセス コントロール ポリシーを編集します。



3. [詳細設定 (Advanced) ] タブを選択します。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. メインメニューで、[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、STIX ファイルまたは Web サーバから取得したオブザーバブルを、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. 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. 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 デスクトップの **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。

The screenshot shows the 'Add Source' configuration interface. At the top, there are tabs for 'DELIVERY', 'TAXII', 'URL', and 'Upload'. The 'Upload' tab is active. Below the tabs, there are two dropdown menus: 'TYPE' is set to 'Flat File' and 'CONTENT' is set to 'URL'. A dashed box labeled 'FILE\*' contains the text 'Drag and drop or click to attach'. Below this, a message says 'File attached: URL\_List.txt (90 B)'. The 'NAME\*' field contains 'Local URL list'. The 'DESCRIPTION' field is empty. The 'ACTION' dropdown is set to 'Block'. The 'TTL (DAYS)' field is set to '90'. The 'PUBLISH' toggle is turned on. At the bottom right, there are 'Save' and 'Cancel' buttons.

9. [保存 (Save)] をクリックします。
10. 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。
11. [インテリジェンス (Intelligence)] > [ソース (Sources)] > [オブザーバブル (Observables)] に移動します。2つのタイプの URL オブザーバブル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:** [フィード (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。

**Add Source** ⓘ

DELIVERY TAXII URL Upload

URL\*  SSL Settings ▾

USERNAME

PASSWORD

⚠ Credentials will be sent using an unsecured HTTP connection

FEEDS\*  X ▾

Note: A separate source will be added for each feed selected. The name will default to the name of the feed and can be edited later.

ACTION

UPDATE EVERY (MINUTES)   Never Update

TTL (DAYS)

PUBLISH

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。これには数分かかる場合があります。解析には非常に時間がかかるため、ここでは解析の完了を待たずに次に進みます。
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 オブザーバブル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. オブザーバブル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、特定のオブザーバブルのパブリッシュを確認する方法を示します。Jump PC で PuTTY を使用して **NGFW1 CLI** に SSH で接続し、次の手順を実行します。(admin/C1sco12345 としてログイン)
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/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** (lf は小文字の l) と入力して、オブザーバブルがファイアウォールの観測対象リストにパブリッシュされていることを確認します。

URL タイプの CTID オブザーバブルを確認できます。

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

**注：**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。

## 内部 Linux サーバの CLI で次を実行します。

1. Jump PC で PuTTY を使用して、**内部 Linux** サーバに SSH 接続し、次の手順を実行します。(Root/C1sco12345 としてログイン)
  - a wget -t 1 outside/files/ProjectX.pdf を実行します。これは成功するはずです。
  - b wget -t 1 developmentserver.com/misc/Tron.html を実行します。これはブロックされるはずです。

- FMC で [インテリジェンス (Intelligence) ] > [インシデント (Incidents) ] に移動します。ブロックされた URL に対して、少なくとも 1 つのインシデントが表示されます。



- インシデント ID をクリックしてドリルダウンし、このインシデントの詳細を表示します。このインシデントのインジケータの URL タイプに注目します。[オブザベーション (Observations) ] の下で、矢印をクリックして展開すると、追加の詳細情報が表示されます。

● URL-20200115-1 ? X

Opened: [Jan 15, 2020 6:11 PM EST](#)

Name: [Name this incident](#)

Description: [Describe this inci...](#)

Observations <b>1</b>	Confidence Rating: ○○○○○	Action Taken <b>Blocked</b>	Category <a href="#">Category Name</a>	Status New
--------------------------	-----------------------------	--------------------------------	---	---------------

Indicator  
[developmentserver.com/misc/Tron...](#)

Observations ↻

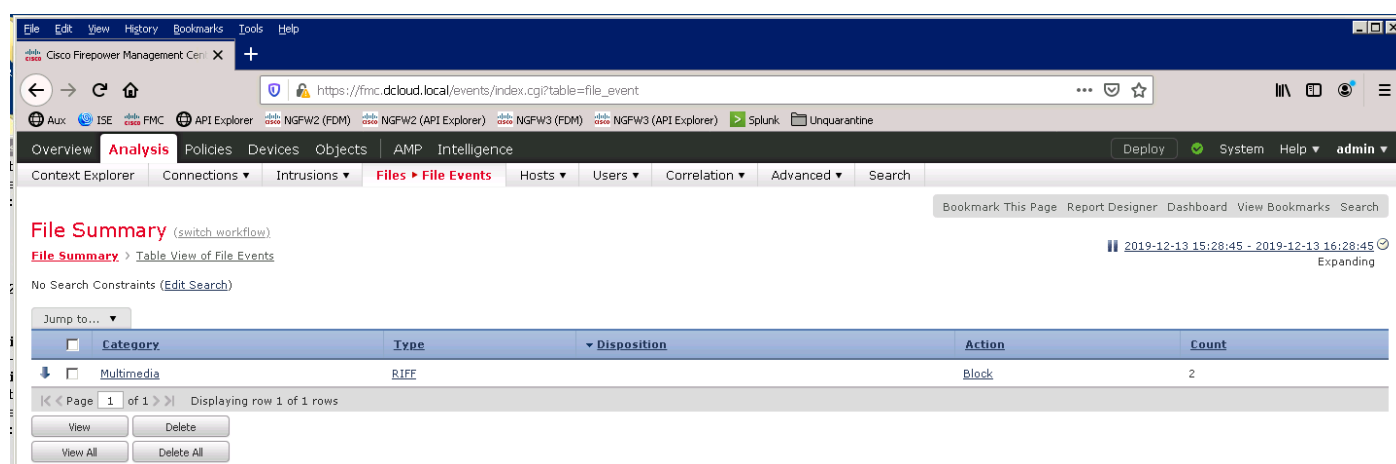
URL	1st	<a href="#">Jan 15, 2020 6:10 PM EST</a>	NGFW1	<b>Block</b>
developmentserver.com/misc/...				
SOURCE		DESTINATION		Events
IP: 198.19.10.200	Port: 57226 / TCP	IP: 66.96.146.102	Port: 80	
Zone: InZone		Zone: OutZone		
ADDITIONAL INFORMATION				
appId: HTTP	httpResponse: 0	srcZone: InZone	userId: Unknown	

## 特定のファイルタイプのブロック

- [ポリシー (Policy) ] > [アクセス制御 (Access Control) ] > [マルウェアとファイル (Malware & File) ] に移動し、鉛筆アイコンをクリックして **BP File Policy** を編集します。
- [ルールの追加 (Add Rule)] をクリックします。
  - [アクション (Action) ] を [ファイルブロック (Block Files) ] に設定します。
  - [ファイルタイプ (File type) ] 検索で **riff** を検索して **RIFF** ファイルタイプを選択し、[追加 (Add) ]、[保存 (Save) ] の順にクリックします。
  - [保存 (Save) ] を再度クリックして、ポリシーの変更を保存します。
- [展開 (Deploy) ] をクリックし、NGFW1 の横のチェックボックスをオンにして [展開 (Deploy) ] をクリックします。展開が完了するまで待機します。これは、上部のメニューバーの緑色のチェックマークをクリックすることで確認できます。
- ファイルブロック機能をテストするために、次の Wget コマンドを Jump デスクトップの Strings ファイルからカットして貼り付けることができます。

5. 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** と入力します。これは成功するはずです。
  - b. 次に、WGET を使用して、ブロックされたファイルのダウンロードを試みます。次のように入力します。 **wget -t 1 outside/files/test3.avi** これは失敗するはずです。
  - c. FMC で [分析 (Analysis)] > [ファイル (Files)] > [ファイルイベント (File Events)] に移動して、.avi ファイルのダウンロード試行がブロックされたことを確認します。

**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。



## セキュリティ インテリジェンス (SI) を使用した不審なアドレスのブラックリスト登録

この演習は、次のタスクで構成されています。

- SI のブラックリストの使用方法を理解する
- SI のブラックリストにカスタムアドレスを追加する
- カスタムホワイトリストを作成する

悪意のあるインターネットコンテンツに対する防御の前線として、セキュリティ インテリジェンスは疑わしい IP アドレス、URL、ドメイン名が関連する接続をレピュテーション インテリジェンスを使用して迅速にブロックします。これは、**セキュリティ インテリジェンスのブラックリスト**と呼ばれます。セキュリティ インテリジェンスは、システムがより多くのリソースを消費する評価を実行する前の、アクセス制御の初期段階です。ブラックリストへの登録は、検査の必要がないトラフィックを迅速に除外することで、パフォーマンスを向上させます。カスタムのブラックリストを設定できますが、シスコでは定期的に更新されるインテリジェンスフィードへのアクセスを提供しています。セキュリティに対する脅威（マルウェア、スパム、ボットネット、スパム、フィッシングなど）と見られるサイトが現れては消えるペースが早すぎて、カスタム設定を更新して導入するのが間に合わないことがあります。

## SI ブラックリストの作成

1. ファイアウォール上では、SI ファイルは /var/sf/iprep\_download に保存されます。ファイルタイプは次のとおりです。

- a. \*.bif (ブラックリストファイル)
- b. \*.wif (ホワイトリストファイル)

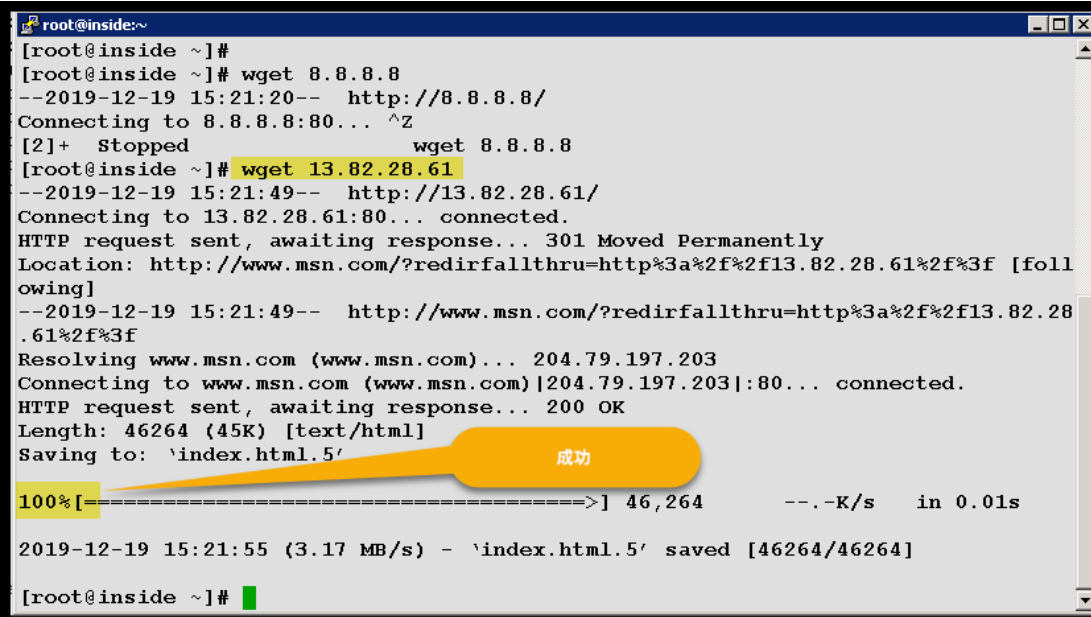
Jump デスクトップに移動して TS-Files\SI フォルダを開き、手動のブラックリストファイルとして使用されるファイルを調べます。また、次の 2 つのテキストファイルを確認します。

- c. Talos IP Blacklist
- d. Lab Blacklist 各 IP アドレスは個別の行に存在している必要があることに注意してください。各 IP アドレスをメモします。

2. Lab Blacklist をメモ帳で開きます。このリストの各 IP アドレスをメモします。

3. Jump PC から、内部 Linux サーバへの PuTTY セッションを開きます。

- a. Lab Blacklist 内の IP アドレスに対して、wget x.x.x.x コマンドを発行します。次に示すような、wget 成功の結果が返される IP アドレスをメモしておいてください。



```

root@inside:~
[root@inside ~]#
[root@inside ~]# wget 8.8.8.8
--2019-12-19 15:21:20-- http://8.8.8.8/
Connecting to 8.8.8.8:80... ^Z
[2]+  Stopped                  wget 8.8.8.8
[root@inside ~]# wget 13.82.28.61
--2019-12-19 15:21:49-- http://13.82.28.61/
Connecting to 13.82.28.61:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.msn.com/?redirfallthru=http%3a%2f%2f13.82.28.61%2f%3f [following]
--2019-12-19 15:21:49-- http://www.msn.com/?redirfallthru=http%3a%2f%2f13.82.28.61%2f%3f
Resolving www.msn.com (www.msn.com)... 204.79.197.203
Connecting to www.msn.com (www.msn.com)|204.79.197.203|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46264 (45K) [text/html]
Saving to: `index.html.5'

100%[=====>] 46,264    --.-K/s   in 0.01s

2019-12-19 15:21:55 (3.17 MB/s) - `index.html.5' saved [46264/46264]

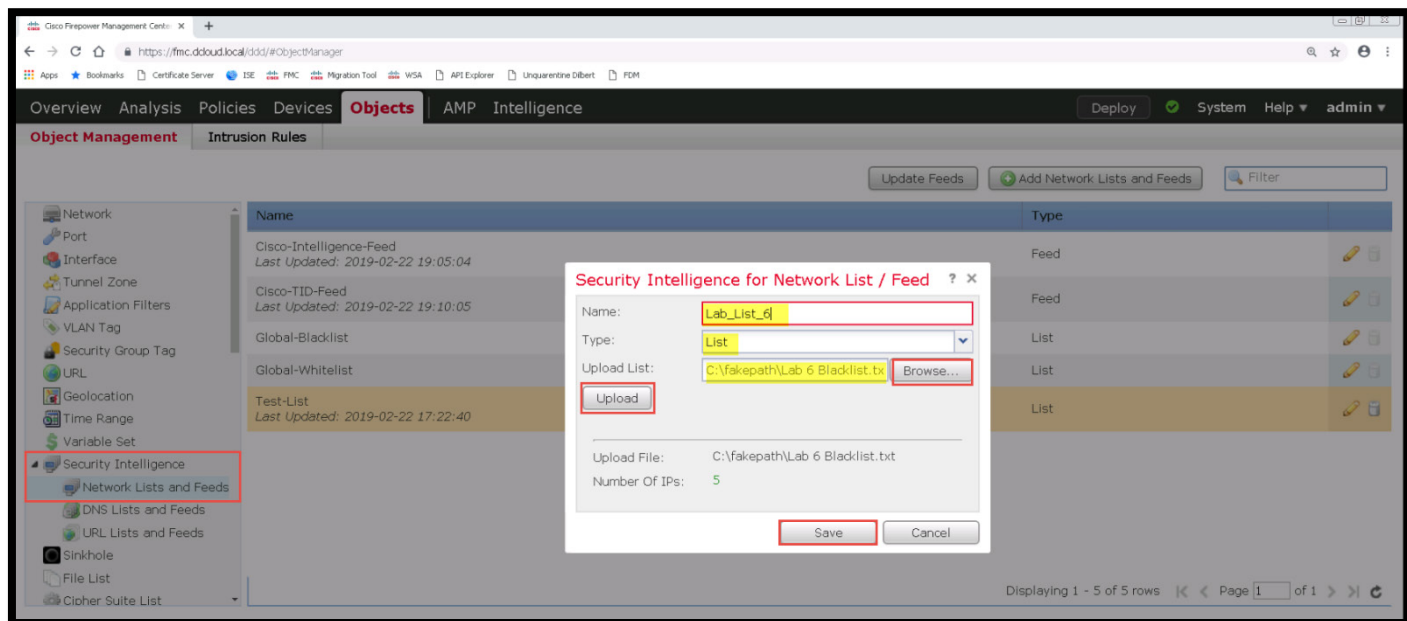
[root@inside ~]#

```

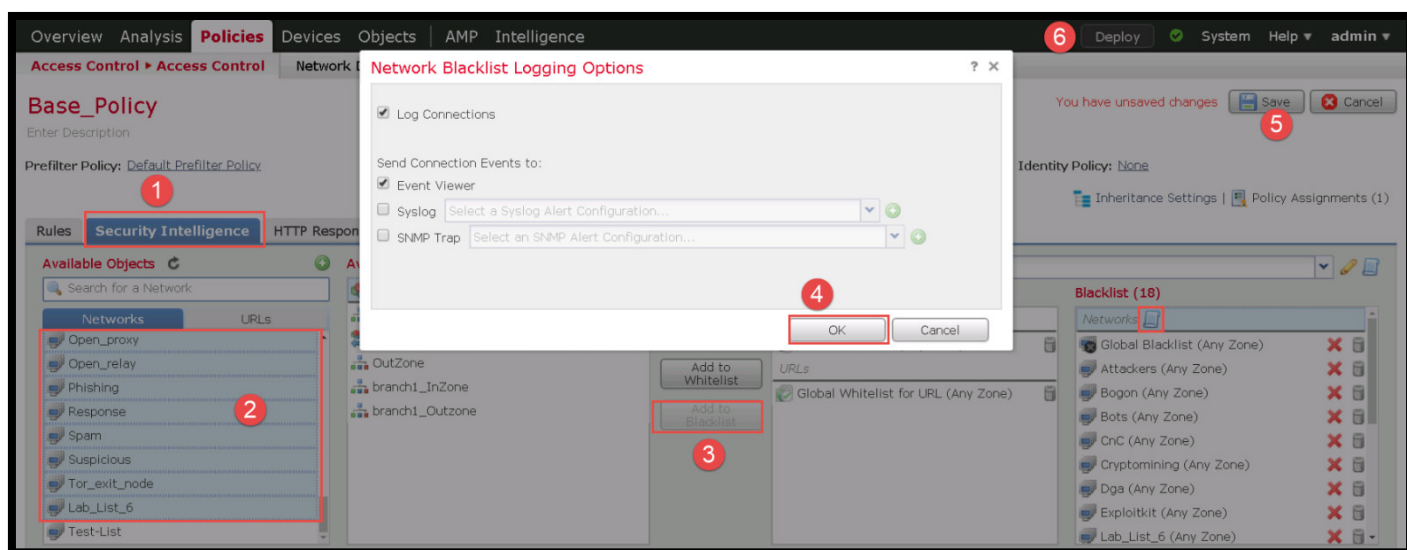
4. Lab 6 Blacklist ファイルの IP アドレスのうち少なくとも 1 つに正常に到達できることが証明されたので、このリストをブラックリストとして FMC にロードしてみましょう。

5. FMC で、[オブジェクト (Object) ]>[オブジェクト管理 (Object Management) ]の順に選択します。

- a. 左側の列で、[セキュリティインテリジェンス (Security Intelligence) ]>[ネットワークリストおよびフィード (Network Lists and Feeds) ]を選択します。
- b. [ネットワークリストとフィードの追加 (Add Network Lists and Feeds) ]をクリックして、次のパラメータを使用してリストを追加します。
  - i. [名前 (Name)]: Custom\_List
  - ii. [タイプ (Type)]: リスト (List)
  - iii. [リストのアップロード (Upload List)]: [参照 (Browse) ]をクリックし、Jump PC \Desktop\TS-Files\SI\Lab 6 blacklist.txt ファイルを使用します。
  - iv. [アップロード (Upload) ]をクリックします。
  - v. [保存 (Save) ]をクリックします。



- c. ここで、このブラックリストを Base\_Policy に適用してみましょう。[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。
- i. Base\_Policy の右にある鉛筆アイコンを選択します。
  - ii. [セキュリティインテリジェンス (Security Intelligence)] タブを選択します。
    1. [使用可能なオブジェクト (Available Objects)] > [ネットワーク (Networks)] で、[攻撃者 (Attackers)] までスクロールします。[攻撃者 (Attackers)] を選択して、その下で最後の項目となる Custom\_List を含むすべての項目を選択します。リストの最後の項目の上部のみが表示されている場合は、ウィンドウのサイズを変更する必要があります。
    2. [ブラックリストに追加 (Add to Blacklist)] を選択し、[ネットワーク (Networks)] の右側にある [ブラックリスト (Blacklist)] セクションにある **ロギングアイコン** をクリックします。次の画面キャプチャに示すように、[Log Connections (ログ接続)] が有効になっていることを確認します。





- d. [OK] をクリックし、次に [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。
- e. [展開 (Deploy)] をクリックして、NGFW1 に変更を展開します。
- f. 展開タスクが完了したら、基本アクセスコントロールポリシーに適用したブラックリストにより、以前に到達可能だったアドレスへのトラフィックがブロックされていることを確認しましょう。
- g. Jump PC で、内部 Linux サーバへの PuTTY セッションを開始します (まだ開いていない場合)。
  - i. 以前の手順で正常に到達した IP アドレスの 1 つに対して、**wget** を入力します。今回は、wget コマンドがハングしているように見えます。

```

root@inside:~
--2019-12-19 15:21:20-- http://8.8.8.8/
Connecting to 8.8.8.8:80... ^Z
[2]+  Stopped                  wget 8.8.8.8
[root@inside ~]# wget 13.82.28.61
--2019-12-19 15:21:49-- http://13.82.28.61/
Connecting to 13.82.28.61:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.msn.com/?redirfallthru=http%3a%2f%2f13.82.28.61%2f%3f [following]
--2019-12-19 15:21:49-- http://www.msn.com/?redirfallthru=http%3a%2f%2f13.82.28.61%2f%3f
Resolving www.msn.com (www.msn.com)... 204.79.197.203
Connecting to www.msn.com (www.msn.com)|204.79.197.203|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46264 (45K) [text/html]
Saving to: `index.html.5'

100%[=====>] 46,264      ---.K/s   in 0.01s

2019-12-19 15:21:55 (3.17 MB/s) - `index.html.5' saved [46264/46264]

[root@inside ~]# wget 13.82.28.61
--2019-12-19 15:42:45-- http://13.82.28.61/
Connecting to 13.82.28.61:80... █

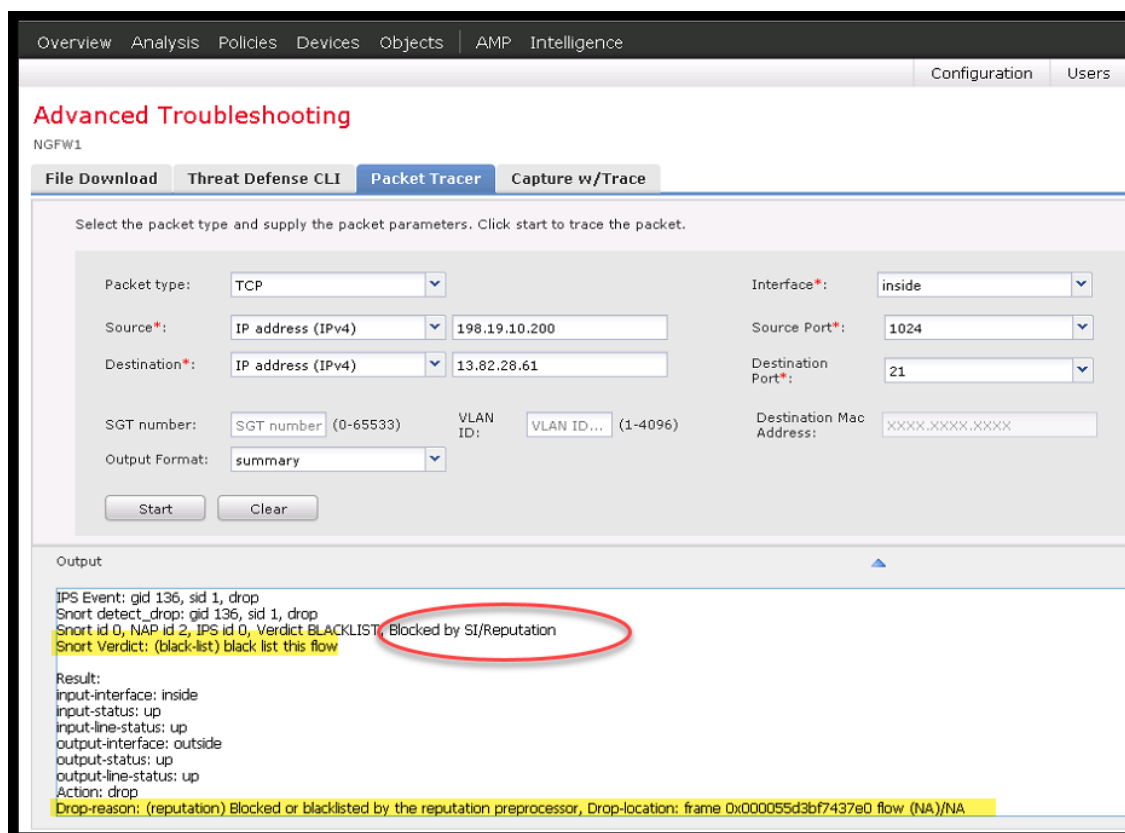
```

- ii. [分析 (Analysis)] > [接続 (Connections)] > [セキュリティインテリジェンスイベント (Security Intelligence Events)] の順に選択します。
- iii. ログを確認します。内容を確認してみましょう。これは SI Custom\_List によってブロックされたものです。

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category
	2019-12-19 15:45:56		Block	IP Block	198.19.10.200		13.82.28.61	USA	List Lab 6

1. パケットトレーサを使用して、テストが FTP で実施された場合に確認したであろう結果を検証します。
  - a. [デバイス (Devices)] > [デバイス管理 (Device Management)] に移動します。

- b. NGFW1 で、[ツール (Tools) ] アイコンをクリックして、[トラブルシューティング (Troubleshoot) ] ウィンドウを開きます。
- c. [ヘルスマニタ (Health Monitor) ] セクションで [高度なトラブルシューティング (Advanced Troubleshooting) ] をクリックして、[パケットトレーサ (Packet Tracer) ] タブをクリックします。パケットトレーサ要求の入力方法と想定される結果を確認するための詳細については、以下のスクリーンキャプチャを参照してください。[開始 (Start) ] を押して、内部 Linux サーバから [FTP 13.82.28.61](http://13.82.28.61) を実行します。



6. SI イベントからブラックリストとホワイトリストを作成します。
  - a. [分析 (Analysis) ] > [接続 (Connections) ] > [イベント (Events) ] に移動します。
    - i. [レスポンド IP (Responder IP) ] 列で、以前の手順で正常にブロックした IP アドレスにカーソルを合わせ、IP アドレスを右クリックして、[IP を今すぐブラックリストに登録 (Blacklist IP Now) ] を選択します。

Overview **Analysis** Policies Devices Objects AMP Intelligence

Context Explorer **Connections ▶ Events** Intrusions ▼ Files ▼ Hosts ▼ Users ▼ Correlation ▼ Advanced ▼ Se

**Connection Events** (switch workflow)

[Connections with Application Details](#) > Table View of Connection Events

No Search Constraints ([Edit Search](#))

Jump to... ▼

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security
↓	2019-12-19 16:01:06		Block	IP Block	198.19.10.100		8.8.8.8	USA	InZone
↓	2019-12-19 16:00:48		Block	IP Block	198.19.10.100		8.8.8.8	USA	InZone
↓	2019-12-19 16:00:19		Block	IP Block	198.19.10.200		13.82.28.61	USA	InZone
↓	2019-12-19 16:00:10		Block	IP Block	198.19.10.100		8.8.8.8		
↓	2019-12-19 15:59:07		Block	IP Block	198.19.10.200		13.82.28.61		
↓	2019-12-19 15:58:34		Block	IP Block	198.19.10.100		8.8.8.8		
↓	2019-12-19 15:58:17		Block	IP Block	198.19.10.100		8.8.8.8		
↓	2019-12-19 15:58:09		Block	IP Block	198.19.10.100		8.8.8.8		
↓	2019-12-19 15:58:04		Block	IP Block	198.19.10.200		13.82.28.61		
↓	2019-12-19 15:56:52		Block	IP Block	198.19.10.200		13.82.28.61		
↓	2019-12-19 15:56:35		Block	IP Block	198.19.10.100		8.8.8.8		
↓	2019-12-19 15:56:18		Block	IP Block	198.19.10.100		8.8.8.8		
↓	2019-12-19 15:56:03		Block	IP Block	198.19.10.100		8.8.8.8		
↓	2019-12-19 15:55:49		Block	IP Block	198.19.10.200		13.82.28.61		

- a. [今すぐブラックリストに登録 (Blacklist Now) ]をクリックして確認します。
- b. これにより、選択されたレスポンドの IP アドレスがグローバルブラックリストに追加されます。
  - i. 内部 Linux サーバに戻り、この IP アドレスに対して **wget** コマンドを再度実行します。Ctrl+C で、以前の wget コマンドを停止する必要がある場合があります。
  - ii. 結果を見てみましょう。この IP アドレスが Custom\_List にあったときと理由が同じです。でも、本当にそうなのでしょうか。
  - iii. FMC に移動し、[分析 (Analysis) ] > [接続 (Connections) ] > [セキュリティインテリジェンスイベント (Security Intelligence Events) ] に移動して、ブロックの理由を確認します。今回はグローバルブラックリストによりブロックされました。また、ブラックリストに IP アドレスを追加する場合は、保存や展開が不要であることに気づきましたか? 変更はすぐに有効になります。

Overview Analysis Policies Devices Objects AMP Intelligence

Context Explorer **Connections > Security Intelligence Events** Intrusions Files Hosts Users Correlation Advanced

## Security Intelligence Events (switch workflow)

**Security Intelligence with Application Details** > Table View of Security Intelligence Events

No Search Constraints [\(Edit Search\)](#)

Jump to... ▾

<input type="checkbox"/>	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category
↓ <input type="checkbox"/>	2019-12-19 16:06:07		Block	IP Block	198.19.10.100		8.8.8.8	USA	List_Lab_6
↓ <input type="checkbox"/>	2019-12-19 16:05:53		Block	IP Block	198.19.10.200		13.82.28.61	USA	Global-Blacklist

- iv. (オプション) パケットトレーサを使用して、その IP アドレスに FTP 接続した場合にはどのような結果になるかを確認します。

Overview Analysis Policies Devices Objects AMP Intelligence

Configuration

## Advanced Troubleshooting

NGFW1

File Download Threat Defense CLI **Packet Tracer** Capture w/Trace

Select the packet type and supply the packet parameters. Click start to trace the packet.

Packet type: TCP Interface\*: inside

Source\*: IP address (IPv4) 198.19.10.100 Source Port\*: 1024

Destination\*: IP address (IPv4) 13.82.28.61 Destination Port\*: 21

SGT number: SGT number (0-65533) VLAN ID: VLAN ID... (1-4096) Destination Mac Address: XXXX.XXXX.XXXX

Output Format: summary

Start Clear

Output

IPS Event: gid 136, sid 1, drop  
 Snort detect\_drop: gid 136, sid 1, drop  
 Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST, Blocked by SI/Reputation  
 Snort Verdict: (black-list) black list this flow

Result:  
 input-interface: inside  
 input-status: up  
 input-line-status: up  
 output-interface: outside  
 output-status: up  
 output-line-status: up  
 Action: drop  
 Drop-reason: (reputation) Blocked or blacklisted by the reputation preprocessor, Drop-location: frame 0x000055d3bf7437e0 flow (NA)/NA

- ii. IP アドレスをホワイトリストに移動します。
1. 前の手順でブラックリストに追加したたものと同じ IP アドレスを使用します。
    - a. [分析 (Analysis)] > [接続 (Connections)] > [イベント (Events)] の順に選択します。
    - b. IP アドレスを右クリックします。
    - c. [IP を今すぐホワイトリストに登録 (Whitelist IP Now)] を選択します。

Overview **Analysis** Policies Devices Objects AMP Intelligence

Context Explorer **Connections > Events** Intrusions ▾ Files ▾ Hosts ▾ Users ▾ Correlation ▾ Advanced ▾ Search

## Connection Events (switch workflow)

**Connections with Application Details** > Table View of Connection Events

No Search Constraints (Edit Search)

Jump to... ▾

<input type="checkbox"/>	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone
<input type="checkbox"/>	<a href="#">2019-12-19 16:15:09</a>		Block	IP Block	<a href="#">198.19.10.100</a>		<a href="#">8.8.8.8</a>	<a href="#">USA</a>	InZone
<input type="checkbox"/>	<a href="#">2019-12-19 16:14:32</a>		Block	IP Block	<a href="#">198.19.10.200</a>		<a href="#">13.82.28.61</a>	<a href="#">USA</a>	InZone
<input type="checkbox"/>	<a href="#">2019-12-19 16:13:24</a>		Block	IP Block	<a href="#">198.19.10.200</a>		<a href="#">13.82.28.61</a>		
<input type="checkbox"/>	<a href="#">2019-12-19 16:13:03</a>		Block	IP Block	<a href="#">198.19.10.100</a>		<a href="#">13.82.28.61</a>		
<input type="checkbox"/>	<a href="#">2019-12-19 16:12:30</a>		Block	IP Block	<a href="#">198.19.10.100</a>		<a href="#">8.8.8.8</a>		
<input type="checkbox"/>	<a href="#">2019-12-19 16:12:21</a>		Block	IP Block	<a href="#">198.19.10.200</a>		<a href="#">8.8.8.8</a>		
<input type="checkbox"/>	<a href="#">2019-12-19 16:12:16</a>		Block	IP Block	<a href="#">198.19.10.100</a>		<a href="#">8.8.8.8</a>		
<input type="checkbox"/>	<a href="#">2019-12-19 16:11:45</a>		Block	IP Block	<a href="#">198.19.10.100</a>		<a href="#">8.8.8.8</a>		
<input type="checkbox"/>	<a href="#">2019-12-19 16:11:14</a>		Block	IP Block	<a href="#">198.19.10.200</a>		<a href="#">13.82.28.61</a>		
<input type="checkbox"/>	<a href="#">2019-12-19 16:10:34</a>		Block	IP Block	<a href="#">198.19.10.100</a>		<a href="#">8.8.8.8</a>		
<input type="checkbox"/>	<a href="#">2019-12-19 16:10:17</a>		Block	IP Block	<a href="#">198.19.10.100</a>		<a href="#">8.8.8.8</a>		
<input type="checkbox"/>	<a href="#">2019-12-19 16:10:11</a>		Block	IP Block	<a href="#">198.19.10.200</a>		<a href="#">13.82.28.61</a>		
<input type="checkbox"/>	<a href="#">2019-12-19 16:10:09</a>		Block	IP Block	<a href="#">198.19.10.100</a>		<a href="#">8.8.8.8</a>		

Context menu for IP 13.82.28.61:

- Open in New Window
- Exclude
- Whois
- View Host Profile
- Blacklist IP Now
- Whitelist IP Now**
- Open in Context Explorer
- AlienVault IP
- IBM X-Force Exchange IP
- Looking Glass IP
- Recorded Future IP
- Talos IP
- Threat Grid IP
- Threat Response IP
- Umbrella IP
- Virus Total IP

d. [今すぐホワイトリストに登録 (Whitelist now)] をクリックして確定します。

e. これにより、グローバルホワイトリストに x.x.x.x が追加されます。

- 内部 Linux サーバに戻り、**wget** コマンドを再度発行します。新しい wget コマンドを発行する前に、Ctrl+C を使用して前のコマンドをキャンセルする必要がある場合があります。これで、先に進みます。(説明が入る)。

```

root@inside:~
Connecting to 13.82.28.61:80... failed: Connection timed out.
Retrying.

--2019-12-19 16:12:22-- (try: 4) http://13.82.28.61/
Connecting to 13.82.28.61:80... failed: Connection timed out.
Retrying.

--2019-12-19 16:14:33-- (try: 5) http://13.82.28.61/
Connecting to 13.82.28.61:80... failed: Connection timed out.
Retrying.

--2019-12-19 16:16:46-- (try: 6) http://13.82.28.61/
Connecting to 13.82.28.61:80... ^C
[root@inside ~]# wget 13.82.28.61
--2019-12-19 16:19:43-- http://13.82.28.61/
Connecting to 13.82.28.61:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.msn.com/?redirfallthru=http%3a%2f%2f13.82.28.61%2f%3f [following]
--2019-12-19 16:19:43-- http://www.msn.com/?redirfallthru=http%3a%2f%2f13.82.28.61%2f%3f
Resolving www.msn.com (www.msn.com)... failed: Name or service not known.
wget: unable to resolve host address 'www.msn.com'
[root@inside ~]#

```

注：上の画面キャプチャでは、ブラックリスト/ホワイトリストテストで使用した IP アドレスに正常に接続されていることがわかりますが、8.8.8.8 と 4.4.4.4 がブラックリストとして使用されている Lab\_6 ファイル上に存在するため、その後の名前解決が失敗しています。

7. グローバルホワイトリスト/ブラックリストを確認します。

- a. FMC で、[オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] に移動します。
  - i. [セキュリティインテリジェンス (Security Intelligence) ] > [ネットワークリストおよびフィード (Network Lists and Feeds) ] を選択します。
  - ii. Global-Blacklist 行と Global-Whitelist 行の右にある鉛筆のアイコンをクリックします。
    1. 両方のリストに x.x.x.x があることがわかります。ホワイトリストはブラックリストよりも優先されます。

8. アクセスコントロールポリシーとオブジェクトからすべてのリストを削除します。

- a. [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。鉛筆アイコンをクリックして、Base\_Policy を編集します。[セキュリティインテリジェンス (Security Intelligence) ] タブを選択します。
- b. [ブラックリスト (Blacklist) ] セクションの [ネットワーク (Networks)] で、グローバルブラックリスト (すべてのゾーン) を除くすべてのエントリを削除します。
- c. ポリシーへの変更を保存し、[展開 (Deploy) ] をクリックして NGFW1 に展開します。

## カテゴリ、リスク、およびレピュテーションに基づく URL のフィルタリング

この演習は、次のタスクで構成されています。

- URL フィルタリングの必須項目の設定
- URL カテゴリとレピュテーションの設定

URL フィルタリング機能を使用して、ネットワーク上のユーザがアクセスできる Web サイトを制御します。

- カテゴリおよびレピュテーション ベースの URL フィルタリング：URL フィルタリングライセンスにより、URL の一般的な分類（カテゴリ）とリスクレベル（レピュテーション）に基づいて、Web サイトへのアクセスを制御できます。これは推奨オプションです。
- 手動での URL フィルタリング：どのライセンスでも、個々の URL、URL グループ、URL リスト、およびフィードを指定して、Web トラフィックに対する制御をより細かくカスタマイズできます。

URL データセットは、高速ルックアップのためにメモリにロードされます。自動更新が有効になっている場合、FMC はクラウドから更新を受信します。Snort エンジンには、ローカル URL データベースでルックアップを実行します。URL が使用できない場合は、FMC に転送されます。

## 手順

### ブロックされた URL の ACP Base\_Policy への追加

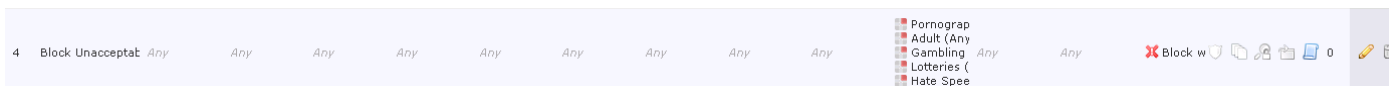
1. [ポリシー (Policies)] > [アクセスコントロール (Access Control)] に移動します。
  - a. **Base\_Policy** の行にある鉛筆のアイコンを選択して編集します。
  - b. [許容されないコンテンツをブロック (Block Unacceptable Content)] ルールを編集して [URL] タブを選択します。
    - i. [ギャンブルに関する通知 (すべてのレピュテーション) (Notice Gambling (Any Reputation))] は、ルールに含まれるカテゴリの 1 つです。
2. テストを実行するには、内部 Linux サーバに対する PuTTY セッションを開きます。
  - a. **wget poker.com** と入力します。これは「403 error: Forbidden」を返すはずですが、
  - i. [分析 (Analysis)] > [接続イベント (Connection Events)] にアクセスして、46.32.240.43 への接続のステータスを確認します。



- ii. NGFW1 の CLI プロンプトに移動して、**system support firewall-engine-debug** と入力します。次のパラメータを入力します。
  1. Protocol : **tcp**
  2. IP Address : **46.32.240.43** (debug コマンドでは「Please specify a client IP address」と表示されますが、これは宛先サーバの IP アドレスです。)
  3. Client Port : **80** (debug コマンドでは「Client port」と表示されますが、これはサーバポートです。)
  4. Server IP : <ブランク>
  5. Server Port : <ブランク>
- iii. 内部 Linux サーバの PuTTY セッションに戻り、**wget poker.com** と入力します。
  1. デバッグを確認する
  2. 示されているのは、どのようなものですか。
  3. ブロックしているのは、どのようなルールですか。

```
198.19.10.200-60472 > 46.32.240.43-80 6 AS 1 I 0 rule order 10, 'Block Unacceptable Content', URL Lookup Success: poker.com waited: 0ms
198.19.10.200-60472 > 46.32.240.43-80 6 AS 1 I 0 rule order 10, 'Block Unacceptable Content', URL poker.com Matched Category: 2049:30 waited: 0ms
198.19.10.200-60472 > 46.32.240.43-80 6 AS 1 I 0 match rule order 10, 'Block Unacceptable Content', action Reset
198.19.10.200-60472 > 46.32.240.43-80 6 AS 1 I 0 Logging SOF with rule_id = 268437505 ruleAction = 5 ruleReason = 0
```

4. **Ctrl+C** キーを押してコマンドラインに戻ります。
5. NGFW1 の **Base\_Policy** アクセス コントロール ポリシーには、許容できない Web カテゴリをブロックするルールがあります。そのうちの 1 つがギャンブルです。

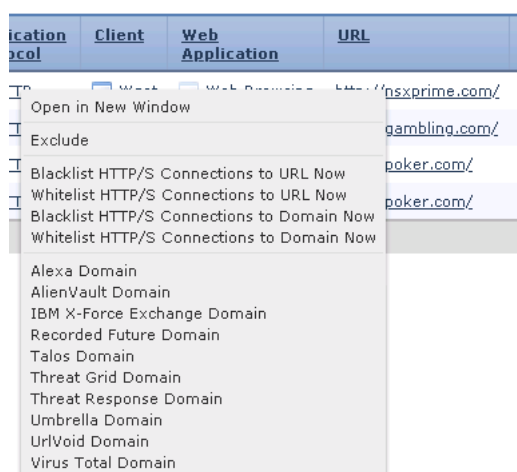


## URL の手動追加

1. 許可された接続のロギングは、演習の進行を容易にするために、この時点では有効ではありませんでした。このセクションでは、ロギングを一時的に有効にします。[ポリシー (Policies)] > [アクセスコントロール (Access Control)] に移動します。
  - a. **Base\_Policy** にある鉛筆アイコンを選択して編集します。
  - b. [発信を許可 (Allow Outbound)] ルールを編集し、右側のロギングアイコン (📄) をクリックします。
  - c. [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て、[保存 (Save)] をクリックします。
  - d. [保存 (Save)] を再度クリックしてポリシーの変更を保存し、[展開 (Deploy)] をクリックして **NGFW1** に展開します。
2. 展開が完了したら内部 Linux サーバに移動し、次のように入力します。
  - a. `wget poker.com - is blocked`
  - b. `wget gambling.com - is blocked`



- c. `wget nsxprime.com - is allowed`
3. 最後のサイトが許可されています。ブロックする URL を手動で追加して、もう一度テストします。
- FMC で、[分析 (Analysis)] > [接続 (Connections)] > [イベント (Events)] の順に移動して、接続イベントを確認します。
    - [Edit Search (検索の編集)] をクリックして URL にスクロールし、次のように入力します。
      - `nsxprime.com, poker.com, gambling.com`
    - [検索 (Search)] をクリックすると [接続イベント (Connection Events)] に戻り、[許可 (Allow)] と [ブロック (Block)] に、実行した `wget` 要求からの `reset` イベントが示されます。
  - 右にスクロールし、[Http://nsxprime.com](http://nsxprime.com) URL を右クリックして、ポップアップメニューから [URL への HTTP/S 接続を今すぐブラックリストに登録 (Blacklist HTTP/S Connections to URL Now)] をクリックして、[今すぐブラックリストに登録 (Blacklist Now)] をクリックします。(ドメインを調査するために使用できるその他のオプションに注目し、適宜 **Talos ドメイン**を試してください。) 前のセクションで IP アドレスをブロックしたときの動作と同様に、URL がブロックされるようになります。`wget` 要求を再実行して確認することができます。



## ネットワーク アプリケーションの検出とアプリケーション トราフィックの制御

この演習は、次のタスクで構成されています。

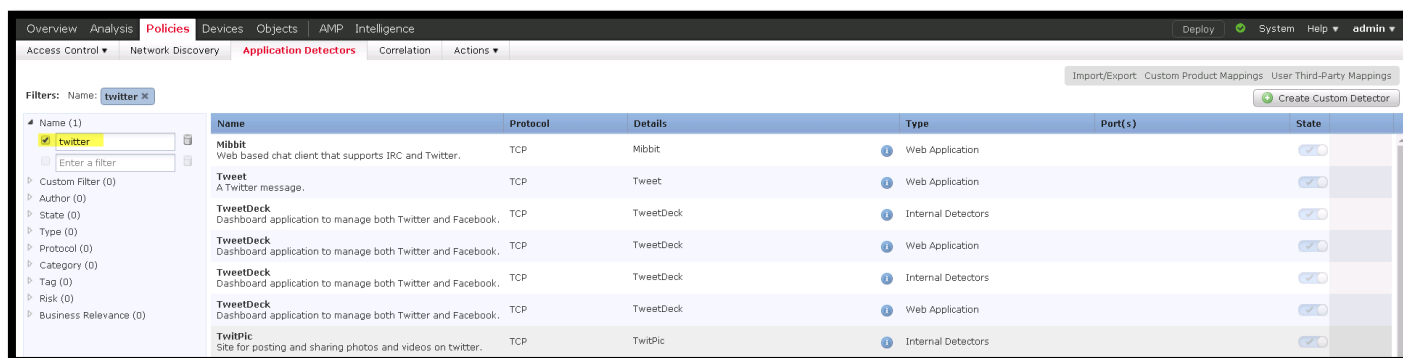
- ネットワーク検出ルールを作成する
- ホストとアプリケーションの検出をモニタする

Firepower システムは、ホストと、ネットワークで動作しているアプリケーションを識別できます。これにより、NGFW は、アプリケーションのタイプに基づいて特定のトラフィックをブロックできます。このラボのセクションでは、AVC (アプリケーションの可視性と制御) を有効にするネットワーク検出ポリシーを設定します。FTD は、アプリケーションルールを適用せずに、セッションの最初の数パケットを分析するだけで、アプリケーションを制御できます。フローが識別されるまでは、アクティブ ACP のデフォルトの侵入ポリシーを使用します。フローが識別されると、アプリケーションフィルタリング用に作成されたアクセスルールが、そのフローの残りのトラフィックに使用されます。

## 手順

### アプリケーションディテクタの概要

1. FMC で、[ポリシー (Policies)] > [アプリケーションディテクタ (Application Detectors)] に移動します。
  - a. ソリューションが提供するアプリケーションディテクタがリスト表示され、名前、プロトコル、詳細、タイプ、ポート、およびそれぞれの状態が示されます。
  - b. 左側の列の入力ボックスに twitter と入力し、チェックボックスをオンにします。



- c. 右側には、Twitter によって使用されるアプリケーションの名前とその他の詳細情報が表示されます。
  - i. 別の名前 (Netflix, Amazon, Apple, Cisco, Facebook など) も試してください。
  - ii. これらのサイトのさまざまなタイプのアプリケーションに注目してください。

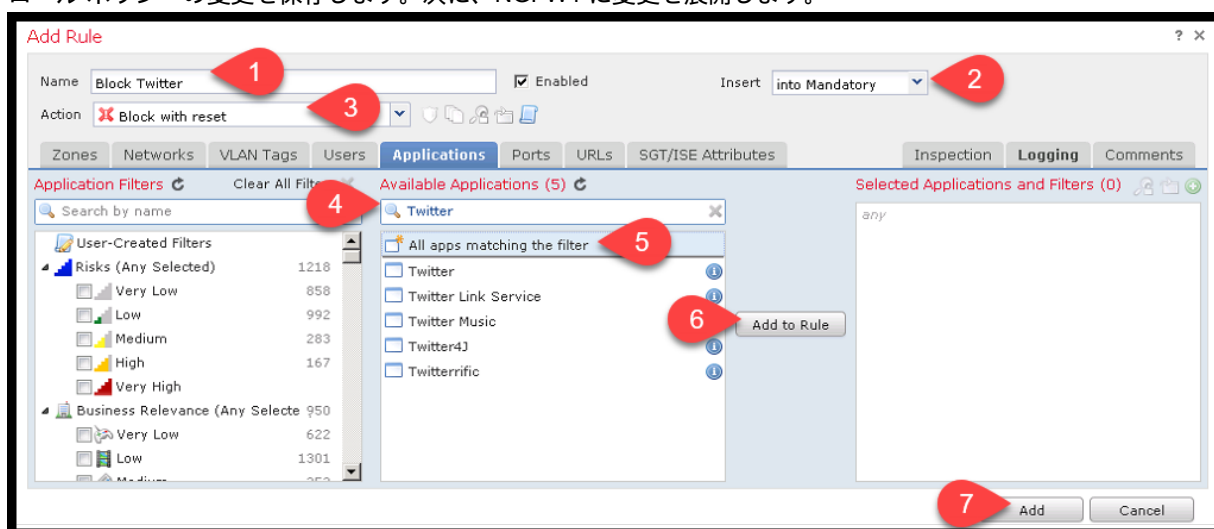
**注：これらのアプリケーションは、デフォルトで定期的に更新される VDB (脆弱性データベース) を使用して更新されます。**

2. FMC で確認するために、[概要 (Overview)] > [ダッシュボード (Dashboards)] > [アプリケーション統計 (Application Statistics)] に移動します。

- a. 最初のシナリオで設定された検出ポリシーによりネットワーク上で確認されたアプリケーションに関する情報を示す、複数のウィジェットが表示されます。
3. FMC で、[分析 (Analysis)] > [ホスト (Hosts)] > [検出イベント (Discovery Events)] の順に移動します。
    - a. 示されているのは、どのようなものですか。
    - b. [ホスト (Hosts)] に移動します。
      - i. 何が示されているでしょうか。
      - ii. Jump のデスクトップフォルダ、Desktop\Remote Desktops に移動し、**ad1.Domain Controller** をクリックします。
      - iii. Ad1 上のリモートデスクトップ接続からスタートボタンをクリックし、**Internet Explorer** を選択します。Explorer がすでに開いている場合は、閉じてから再度開きます。Internet Explorer を設定するように指示されたら、[OK] をクリックします。[www.cisco.com/jp](http://www.cisco.com/jp) に移動して、トラフィックが Firepower のファイアウォールを通過し、パッシブ検出が行われるようにします。
      - iv. FMC に戻り、[分析 (Analysis)] > [ホスト (Hosts)] > [ホスト (Hosts)] を選択します。
        1. Ad1 から生成された Web トラフィックから、Microsoft を含む複数の OS ベンダーがリストされています。
      - v. [分析 (Analysis)] > [ホスト (Hosts)] > [検出イベント (Discovery Events)] に戻ります。
        1. ad1 のアドレスである IP アドレス 198.19.10.100 を探します。
        2. [新しい OS (New OS)] の [説明 (Description)] 列には何が表示されていますか。
      - vi. [分析 (Analysis)] > [ホスト (Hosts)] > [ネットワークマップ (Network Map)] に移動します。
        1. ホスト数は、サブネットごとに括弧で囲まれて表示されます。
        2. ネットワーク 198 の [ホスト [IPv4] (Hosts [IPv4])] で、左側にある展開ボタン (+ 記号) をクリックします。
          - a. 示されているのは、どのようなものですか。
            - i. 2 つのサブネットでホストが確認されました。
          - b. + 記号をクリックして、198.19 を展開します。
          - c. **198.19.10.100** をクリックします。
            - i. どのような情報が表示されますか。ホストプロファイルは、ホストに関する有益な情報を提供し、攻撃が成功した可能性を判断するために侵入イベントの影響スコアに使用されます。
          - d. 198.19.10.200 のチェックボックスをオンにして、ホストプロファイル情報を確認します。
        - vii. [分析 (Analysis)] > [ホスト (Hosts)] > [アプリケーション (Applications)] に移動します。
          1. Sourcefire.com のチェックボックスをオンにして下にスクロールし、[表示 (View)] をクリックします。
            - a. IP アドレス、カテゴリ、リスク、およびビジネスとの関連性を確認します。

#### 4. Base\_Policy のアプリケーション検出を使用して、Twitter をブロックしてリセットします。

- i. Twitter のブロックを開始する前に、Twitter にアクセス可能であることを確認します。
  1. ad1 への RDP セッションで、Internet Explorer を使用して <http://twitter.com> を参照します。これは成功するはずですが。
- ii. [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) ] に移動して、Base\_Policy を編集します。
- iii. [ルールの追加 (Add Rule) ] をクリックし、ルールに **Block Twitter** という名前を付けます。
- iv. [アクション (Action) ] で、[リセットしてブロック (Block with Reset) ] を選択します。
- v. [挿入 (Insert) ] で、[必須に挿入 (into Mandatory) ] を選択します。
- vi. [アプリケーション (Application) ] タブをクリックします。[使用可能なアプリケーション (Available Applications) ] セクションの下の検索ボックスに、**Twitter** と入力します。[このフィルタに一致するすべてのアプリケーション (All apps matching this filter) ] を選択し、[ルールに追加 (Add to Rule) ] をクリックします。
- vii. [ロギング (Logging) ] タブを選択して、[接続開始時にロギング (Log at Beginning of Connection) ] をオンにします。[追加 (Add) ] をクリックしてルールを保存し、[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。次に、NGFW1 に変更を展開します。



- viii. ad1 で、Internet Explorer を閉じてから、再度開きます。[Http://twitter.com](http://twitter.com) の参照を試みます。**This page can't be displayed** というメッセージが表示されるはずですが。
- ix. [分析 (Analysis) ] > [接続イベント (Connection Events) ] に移動します。[検索の編集 (Edit Search) ] をクリックし、[Web アプリケーション (Web Application) ] までスクロールして **twitter** と入力し、[検索 (Search) ] をクリックします。

Twitter は、URL フィルタリングによってブロックされるのではなく、アプリケーションフィルタによってブロックされることに注意してください。

## シナリオ 3： 6.5 FMC ユーザーインターフェイスの機能強化

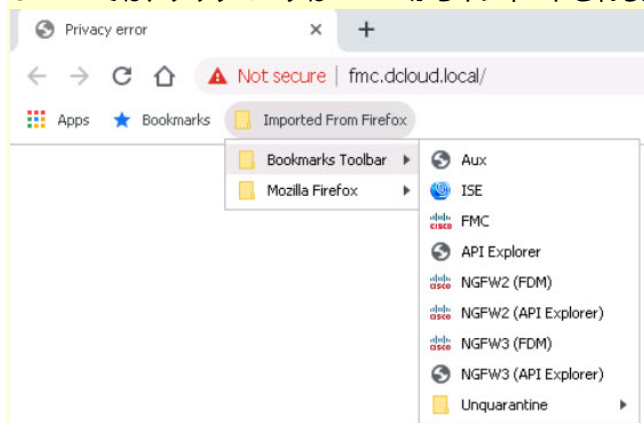
6.5 リリースでは、FMC ユーザーインターフェイスの複数の機能が強化されています。

このシナリオの目的：

- FMC UI のライトテーマを有効にする。
- アクセス コントロール ポリシー ルール フィルタを使用する
- 新しい FMC SSH CLI を使用する

受講者は、これらの機能強化に加えて、改善された How-To 機能を検証することを求められています。

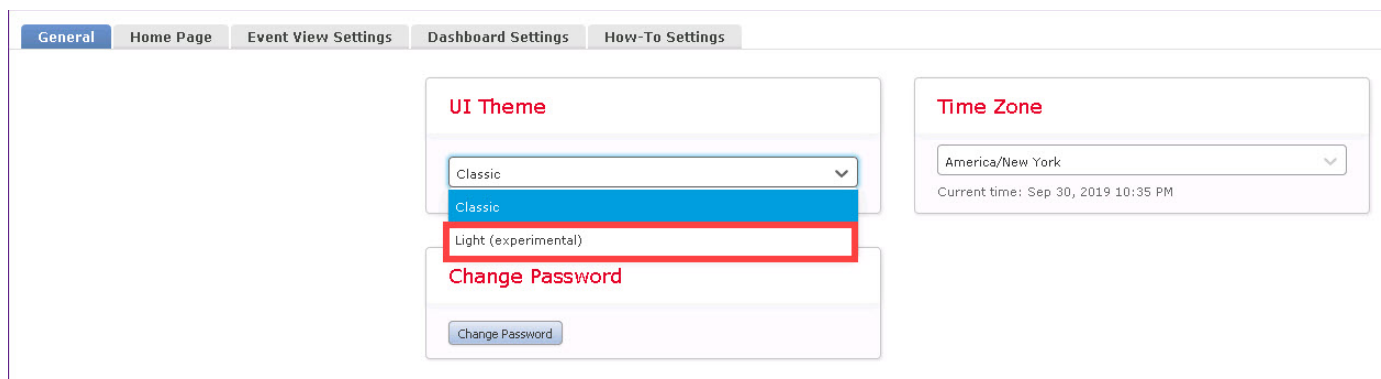
**注：** Chrome は Firefox よりも速くページを読み込みます（特に FMC の場合）。ただし、Chrome では、セキュリティ警告がより頻繁に表示され、NGFW2 と NGFW3 のログイン情報がキャッシュされません。いずれか、または両方のブラウザを使用できます。Chrome では、ブックマークは Firefox からインポートされるため、次に示すようにブックマークバーのサブフォルダ内にあります。



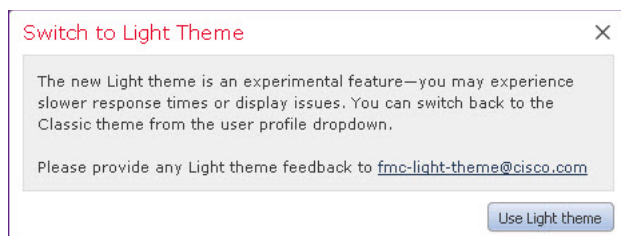
好みに応じて、Chrome と Firefox の間で選択します。

### FMC UI のライトテーマを有効にする

1. Jump PC で Firefox を開きます。ホームページは FMC UI で、ログイン情報（ログイン **admin**、パスワード **C1sco12345**）は自動入力されます。
2. FMC の右上隅で、[管理 (admin) ] > [ユーザ設定 (User Preferences) ] の順に選択します。
3. UI テーマのドロップダウンメニューから [ライト (試験版) (Light (experimental))] を選択します。

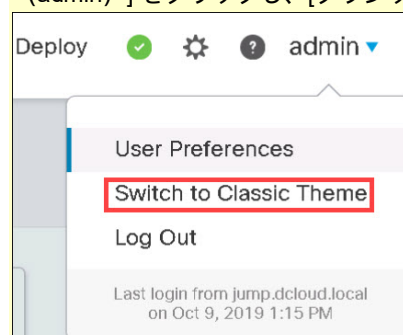


4. [ライトテーマに切り替え (Switch to Light Theme) ] ダイアログボックスが表示されたら、[ライトテーマの使用 (Use Light theme) ] を選択します。



5. 残りのシナリオでは、ライト UI テーマを使用します。

**注：**新しいテーマが使いつらい場合は、いつでもクラシックテーマに切り替えることができます。FMC UI の右上にある [管理者 (admin) ] をクリックし、[クラシックテーマに切り替え (Switch to Classic Theme) ] を選択します。



ただし、このガイドの手順とスクリーンショットは、ライトテーマに基づいています。

## アクセスコントロール ポリシー ルール フィルタを使用する

6. 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。Base\_Policy を編集します。
7. 検索ボックスに 198.18.129.0 と入力し、Enter を押します。



**注：**ワイルドカードと名前と値のペアがサポートされています。例：src:198.18.1\*9.0

8. このネットワークを使用するルールが強調表示されていることを確認します。

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Application	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
Mandatory - Base_Policy(1 - 5)	Any	Any	Any	Any	Any	Unknown...	SSH	Any	Any	Any	Any	Any	Block
Block Extranet129	InZone	OutZone	Any	Extranet1...	Any	Any	Any	Any	Any	Any	Any	Any	Block
Block ICMP Over GRE	GRE	Any	Any	Any	Any	Any	ICMP ICMP for ...	Any	Any	Any	Any	Any	Block
Block Unacceptable Content	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Block
Block Extra to Infra	OutZone	InZone	Extranets	Infrastruc...	Any	Any	Any	Any	Any	Any	Any	Any	Block

**注：**この機能は 6.4 ですでに利用できていました。

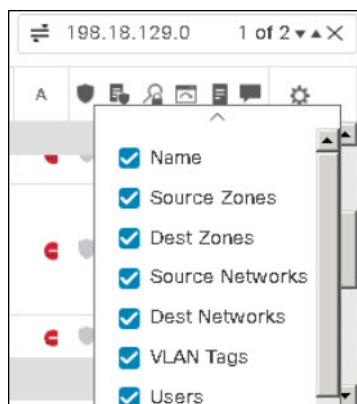
9. 検索ボックスに、6.5 で追加された [フィルタ (Filter) ] アイコンがあることに注意してください。このアイコンをクリックすると、検索がフィルタに変換されます。アイコンをクリックします。



10. 現在は 2 つのルールのみ表示されていることに注意してください。アイコンをもう一度クリックすると、フィルタが検索に戻ります。

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Application...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
Mandatory - Base_Policy(1 - 5)	Any	Any	Any	Any	Any	UCROU...	SSH	Any	Any	Any	Any	Any	Block
2 Block Extranet129	InZone	OutZone	Any	Extranet1	Any	Any	Any	Any	Any	Any	Any	Any	Block
3 Block ICMP Over GRE	GRE	Any	Any	Any	Any	Any	ICMP ICMP For ...	Any	Any	Any	Any	Any	Block
4 Block Unacceptable Content	Any	Any	Any	Any	Any	Any	Any	Any	Any	Pornogra... Adult (An... Gambling... Lotteries... Hate Spe...	Any	Any	Block
5 Block Extra to Infra	OutZone	InZone	Extranets	Infrastruc...	Any	Any	Any	Any	Any	Any	Any	Any	Block

11. [ポリシーの編集 (Edit Policy) ] ページでは、もう 1 つの追加機能を確認できます。FMC では、必要に応じてルール内の列を非表示にできます。ページの右上にある歯車をクリックし、非表示にする列の選択を解除します。



## シナリオ 4： レポート

このシナリオでは、FMC ダッシュボードとレポートの概要に焦点を当てていきます。FMC では、カスタマイズ可能なデータ分析とレポートを数多く提供します。

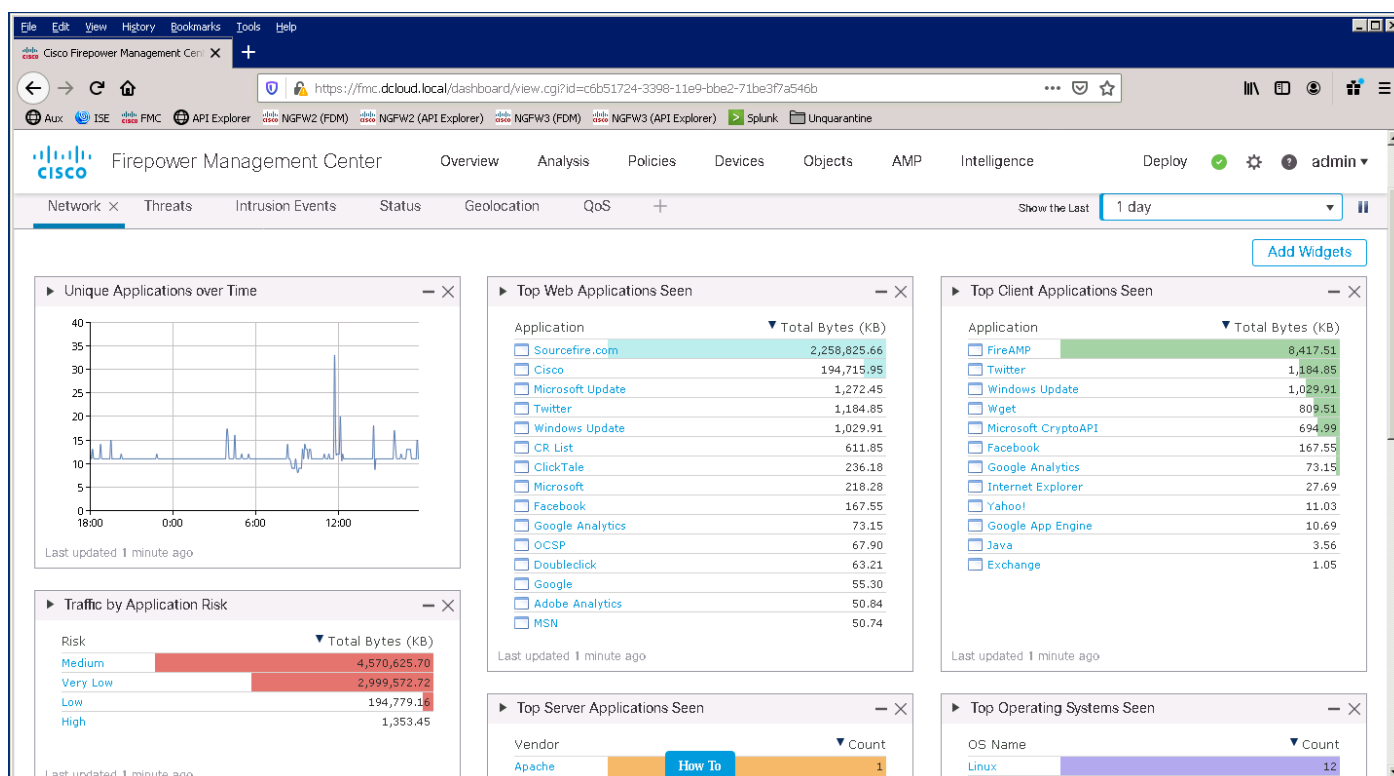
このシナリオの目的：

- ダッシュボードとレポートの設計を確認する。
- カスタムダッシュボードを作成する
- 新しい FMC SSH CLI を使用する。

### ダッシュボード

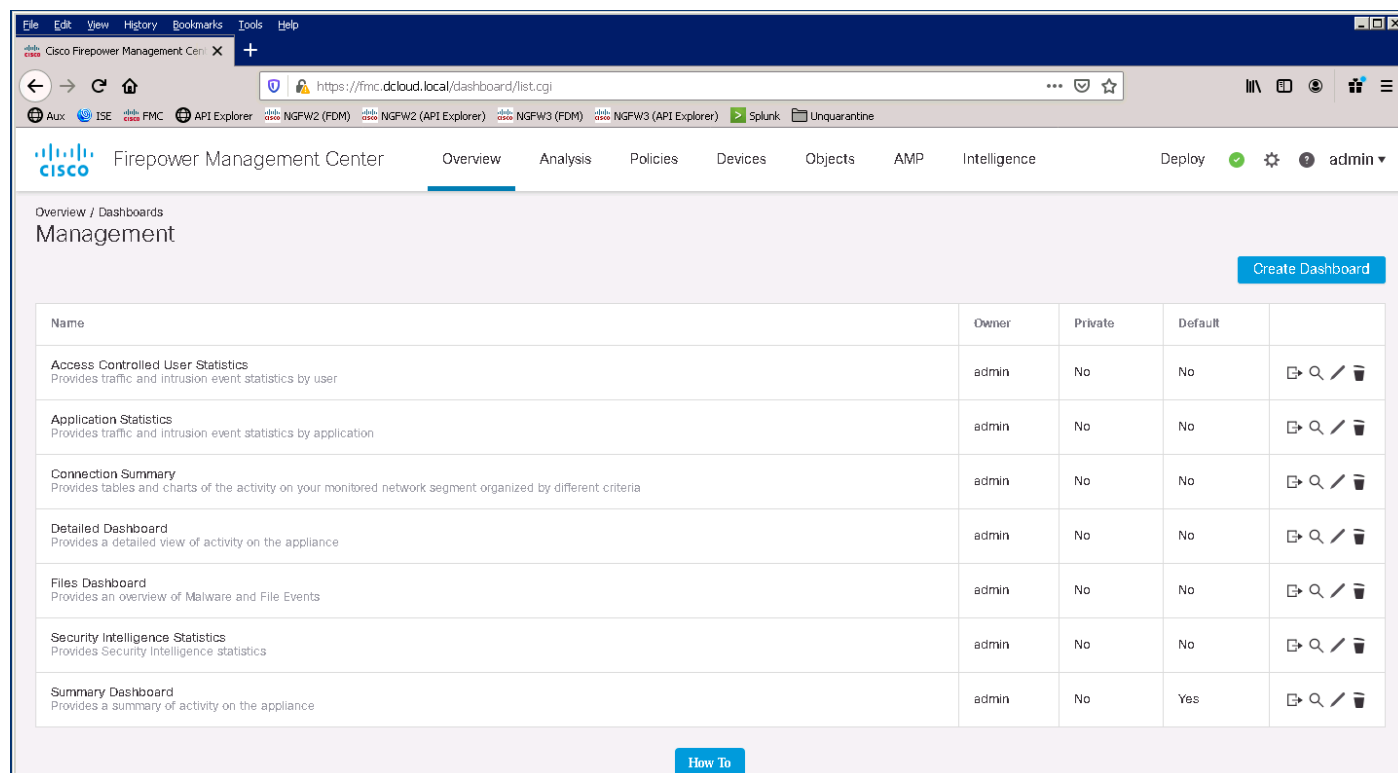
1. **Jump PC** で Firefox を開きます。ホームページは FMC UI で、ログイン情報（ログイン **admin**、パスワード **C1sco12345**）は自動入力されます。
2. FMC で [概要 (Overview)] > [ダッシュボード (Dashboards)] に移動します。（サマリーダッシュボードが表示されます。表示されない場合は、[ダッシュボードの切り替え (switch dashboard)] をクリックして、リストから [概要ダッシュボード (Summary Dashboard)] を選択します。）

**注：**定義済みダッシュボードが豊富に用意されています（アクセス制御されたユーザ統計情報、アプリケーション統計情報、接続サマリー、詳細ダッシュボード、ファイルダッシュボード、セキュリティインテリジェンス統計情報）。ダッシュボードは、オンデマンドまたはスケジュールされたレポートの概要をグラフィカルに示したものとして使用できます。一方、ダッシュボードは、ウィジェット内のいずれかのリンクをクリックするだけで、詳細な分析のドリルダウンにも使用できます。





3. [概要 (Overview)] > [ダッシュボード (Dashboards)] > [管理 (Management)] を選択すると、ダッシュボードのエクスポートやインポート、独自のダッシュボードの作成が可能になります。



4. [ダッシュボードの作成 (Create Dashboard)] をクリックして、[ダッシュボードのコピー (Copy Dashboard)] の下矢印をクリックし、[サマリーダッシュボード (Summary Dashboard)] を選択します。新しいダッシュボードに **MyDashboard** と名前を付けて、[作成 (Create)] をクリックします。

### Create Dashboard

Copy Dashboard Summary Dashboard ▼

Name MyDashboard

Description |

Change Tabs Every 0 minutes (Set to 0 to disable)

Refresh Page Every 0 minutes (Set to 0 to disable)

Save As Private

Cancel
Create

5. 新しいダッシュボードで、右上隅にある [ウィジェットの追加 (Add Widgets)] をクリックします。
6. [カスタム分析 (Custom Analysis)] ウィジェットの右側にある [追加 (Add)] をクリックします。これは、任意のテーブルからのデータを表示してそれをカスタマイズするために使用する非常に柔軟なウィジェットです。次に、ページの下部にある [完了 (Done)] をクリックして、MyDashboard に戻ります。

Message	Count
DNS ping response for 192.168.1.100 address	218
BACKLOG_IPsec_request_for_access_failure	21
IPsec_receive_authenticating_authentication_request	17
IPsec_client_authenticating_authentication_request	16
BACKLOG_IPsec_request_for_access_failure	15
IPsec_receive_authenticating_authentication_request	14
IPsec_client_authenticating_authentication_request	13
IPsec_receive_authenticating_authentication_request	12
IPsec_client_authenticating_authentication_request	11
IPsec_receive_authenticating_authentication_request	10
IPsec_client_authenticating_authentication_request	9
IPsec_receive_authenticating_authentication_request	8
IPsec_client_authenticating_authentication_request	7
IPsec_receive_authenticating_authentication_request	6
IPsec_client_authenticating_authentication_request	5
IPsec_receive_authenticating_authentication_request	4
IPsec_client_authenticating_authentication_request	3
IPsec_receive_authenticating_authentication_request	2
IPsec_client_authenticating_authentication_request	1

### Custom Analysis

The Custom Analysis widget shows the top or bottom set of events (5, 10, 15, 20, or 25 events) from a user-selectable event table, search, and field.

Add

12 on Tab

- [ネットワーク (Network)] タブが選択されている状態で (最初に選択されているはずですが)、[ユーザごとのトラフィック (Traffic by User)] まで下にスクロールして、右上隅の X をクリックして [OK] をクリックし このウィジェットを削除します。これは、この時点でユーザの統合が設定されていないためです。
- さらにページの下部にスクロールして、ダッシュボードに追加されたばかりの新しいウィジェットを見つけます。これは、[カスタム分析 - 侵入イベント (Custom Analysis - Intrusion Events)] というタイトルです。
- ウィジェットをカスタマイズするには、左上隅にある矢印をクリックします。タイトルを **Intrusion Events Requiring Analysis** とし、検索フィールドを [影響度 1/ドロップされていないイベント (Impact 1/Not Dropped Events)] に設定します。このウィジェットは、確認されたが IPS によりドロップされていない侵入イベントに焦点を当てます。これらの侵入イベントは、SoC による詳細な調査が必要となります。(注：このウィジェットでは、データが全く表示されない可能性が高いです。これは、デフォルトの IPS ポリシーではごく少数のルールがアラート用に設定されているためです。これは SoC チームには歓迎されます。) ウィジェットの他のオプションを自由に試してみてください。

▼ Intrusion Events Requiring Analysis

Title:

Preset:

Table:

Field:

Aggregate:

Search:

Show:

Results:

- 下向き矢印をクリックして、ウィジェットのオプションを閉じます。
- ページの上部に戻り、[レポートデザイナー (Report Designer)] ボタンに注目します。ダッシュボードをレポートテンプレートに変換することができます。また、このボタンは FMC GUI の他のページにも表示されます。これは、迅速かつ簡単にレポートを作成する際に非常に役立ちます。[レポートデザイナー (Report Designer)] ボタンをクリックします。これにより、レポートテンプレートをデザインするページに移動し、レポートのベースとして先ほど作成したダッシュボードが使用されます。ここから、レポートの変更、テキストの追加、グラフの変更などを行うことができます。

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy ✔ ⚙️ 👤 admin

Overview / Dashboards Report Designer

MyDashboard (switch dashboard)

Network × Threats Intrusion Events Status Geolocation QoS +

Show the Last 1 day

12. 完了したら、[保存 (Save)] をクリックして、次に [生成 (Generate)] をクリックし、PDF を選択解除して HTML を選択します (PDF リーダーがインストールされていないため)。次に、[はい (Yes)] をクリックしてレポートを作成します。

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy ✔ ⚙️ 👤 admin

Reports Report Templates

Report Title  + Generate Advanced Save

Report Sections 📊 📄 📁 📄 📄 📄

Unique Applications over Time + 🗑️

**Generate Report**

Report Generation Information

File Name  +

Output Format HTML PDF HTML

Relay Host No Relay Host Configured! ✎

Close Generate

13. レポートを表示するには、[概要 (Overview)] > [レポート (Reporting)] > [レポート (Reports)] に進むか、現在のページの [レポート (Reports)] タブを選択します。

Firepower Management Center Overview Analysis Policies Devices Objects AMP

Overview / Reporting

Reports Report Templates

<input type="checkbox"/>	Name	Time Requested	Time Completed
<input type="checkbox"/>	<a href="#">MyDashboard-20200117165413-16385.zip</a> Reports	2020-01-17 11:54:13	2020-01-17 11:54:21
<input type="checkbox"/>	<a href="#">MyDashboard-20200117165055-15655.pdf</a> Reports	2020-01-17 11:50:55	2020-01-17 11:51:05

Download Delete Move


14. レポートテンプレートタブを再度選択すると、リスクレポートテンプレートが3つ表示されます。これらは、経営陣向けの概要レベルの情報を提供します。いずれかのリスクレポートの横にある [レポートの生成 (Generate Report) ] アイコンをクリックし、ポップアップウィンドウで [生成 (Generate) ] をクリックします。

Risk Report Templates	
Advanced Malware Risk Report	
Attacks Risk Report	
Network Risk Report	

15. レポートが完了したことを示すポップ通知で [HTML の表示 (View HTML) ] をクリックします。または、[通知 (Notifications) ] アイコンをクリックして、[タスク (Tasks) ] タブを選択し、次に表示された [レポートの生成 (Generate Report) ] タスクで [HTML の表示 (View HTML) ] を選択します。

 Generate Report

Generated Advanced\_Malware\_Risk\_Report 5s X  
View [HTML](#).









## I. EXECUTIVE SUMMARY

---

Cisco has determined that your company is at a high risk due to the observation of attack by 0 different families of malware. Cisco Advanced Malware Protection (AMP) was deployed for an assessment period of 1 week. This report is a record of what was found on the network during this time.

**Assessment Period: Fri Jan 10 2020 12:06:49 to Fri Jan 17 2020 12:06:49**

<p><b>Malware Detected</b></p> <p style="font-size: 2em; color: #c00000;">0</p> 	<p><b>Hosts Displaying IOCs</b></p> <p style="font-size: 2em; color: #c00000;">0</p> 	<p><b>Infection Protocols</b></p> <p style="font-size: 2em; color: #c00000;">0</p> 
<p><b>Hosts Connected to CnC Servers</b></p> <p style="font-size: 2em; color: #c00000;">0</p> 	<p><b>Malware Comms</b></p> <p style="font-size: 2em; color: #c00000;">0</p> 	<p><b>Malware URLs</b></p> <p style="font-size: 2em; color: #c00000;">0</p> 

## シナリオ 5. RADIUS を使用したリモートアクセス VPN AnyConnect (オプション)

この演習は、次のタスクで構成されています。

- グループポリシーの作成
- IP プールの作成
- アクセスコントロールと NAT ポリシーの変更
- 設定の展開とテスト

この演習では、ISE RADIUS を使って VPN ユーザを検証します。

この演習の目的は次のとおりです。

- NGFW に接続するように AnyConnect VPN クライアントを設定する
- NGFW の侵入防御とマルウェア設定をテストする

**注：**時間を節約するために、ISE では、ラボ演習に必要な設定が事前にすべて設定されています。その設定には、AD グループのメンバーシップに基づくグループポリシーと IP プールの選択も含まれます。**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。

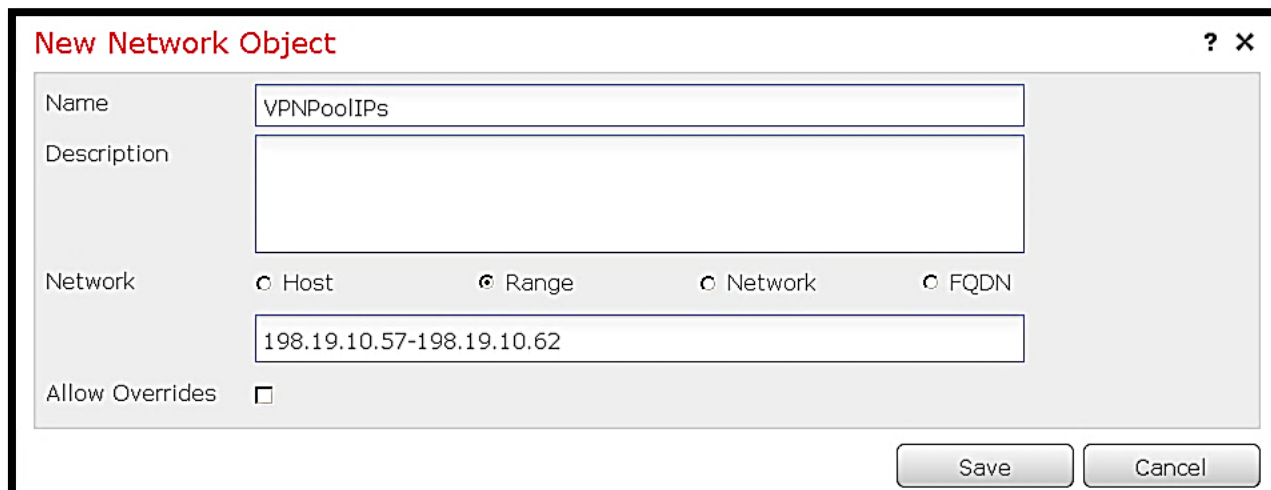
### 手順

1. [システム (System) ] > [ライセンス (Licenses) ] > [スマートライセンス (Smart Licenses) ] に移動します。
  - a. [ライセンスの編集 (Edit Licenses) ] をクリックします。
  - b. **AnyConnect Apex** を選択します。
    - i **HA\_Test** または **NGFW1** を選択します。シナリオ 2 HA ラボを実施していない場合
      - 1 [追加 (Add) ] をクリックし、[適用 (Apply) ] をクリックします。

### このシナリオに必要なオブジェクトを作成する

**注：**これらのオブジェクトのほとんどは、RA VPN ウィザードを実行しながら作成できます。RA VPN 設定のコンポーネントに慣れていない管理者には、ウィザードの方が効率的なアプローチかもしれませんが、このシナリオでは、いくつかのオブジェクトを個別に作成します。これにより、後工程の RA VPN ウィザードの実行が簡素化されます。

1. FMC で、[オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] に移動します。
2. [ネットワーク (Network) ] > [フィルタ (Filter) ] をクリックすると、事前に作成されたオブジェクトを確認できます。
  - a. **VPNPoolIPs** IP アドレス範囲 198.19.10.57-198.19.10.62 次のスクリーンキャプチャは、オブジェクトが設定されている状態を示しています。



**New Network Object** ? X

Name: VPNPoolIPs

Description:

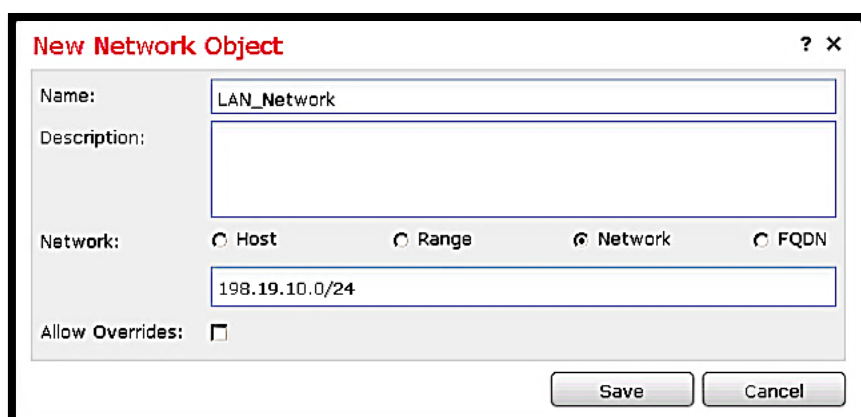
Network:  Host  Range  Network  FQDN

198.19.10.57-198.19.10.62

Allow Overrides:

Save Cancel

3. [ネットワーク (Network)] をクリックして、IP アドレスが 198.19.10.0/24 の LAN\_NETWORK をクリックし、オブジェクトの設定を表示します。



**New Network Object** ? X

Name: LAN\_Network

Description:

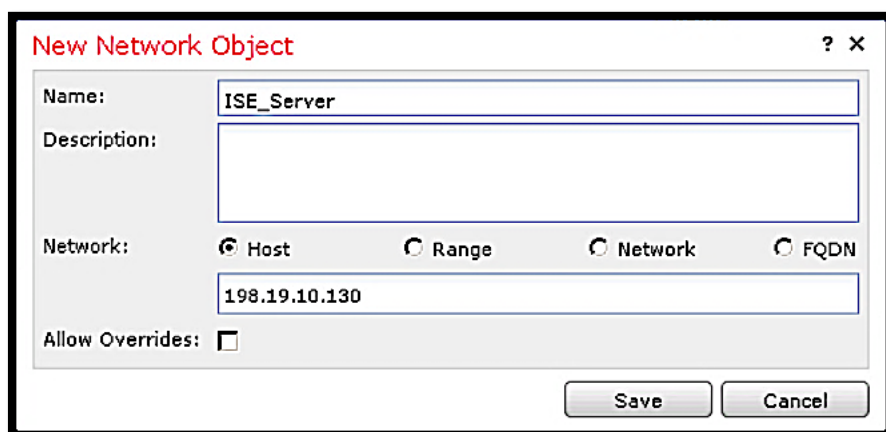
Network:  Host  Range  Network  FQDN

198.19.10.0/24

Allow Overrides:

Save Cancel

4. [ネットワーク (Network)] をクリックして、IP アドレスが 198.19.10.130 の ISE\_Server をクリックし、オブジェクトの設定を表示します。



**New Network Object** ? X

Name: ISE\_Server

Description:

Network:  Host  Range  Network  FQDN

198.19.10.130

Allow Overrides:

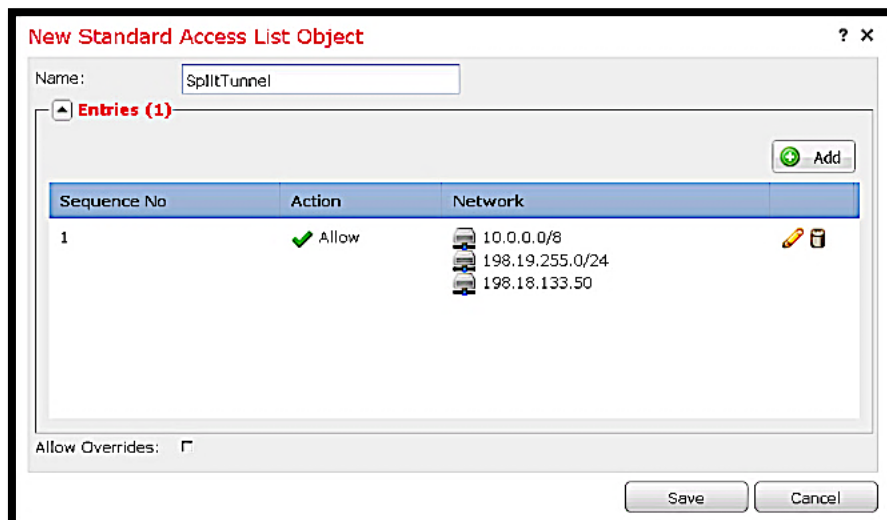
Save Cancel

- [ネットワーク (Network)] をクリックして、IP アドレスが 198.19.10.100 の DNS\_Server をクリックし、オブジェクトの設定を表示します。

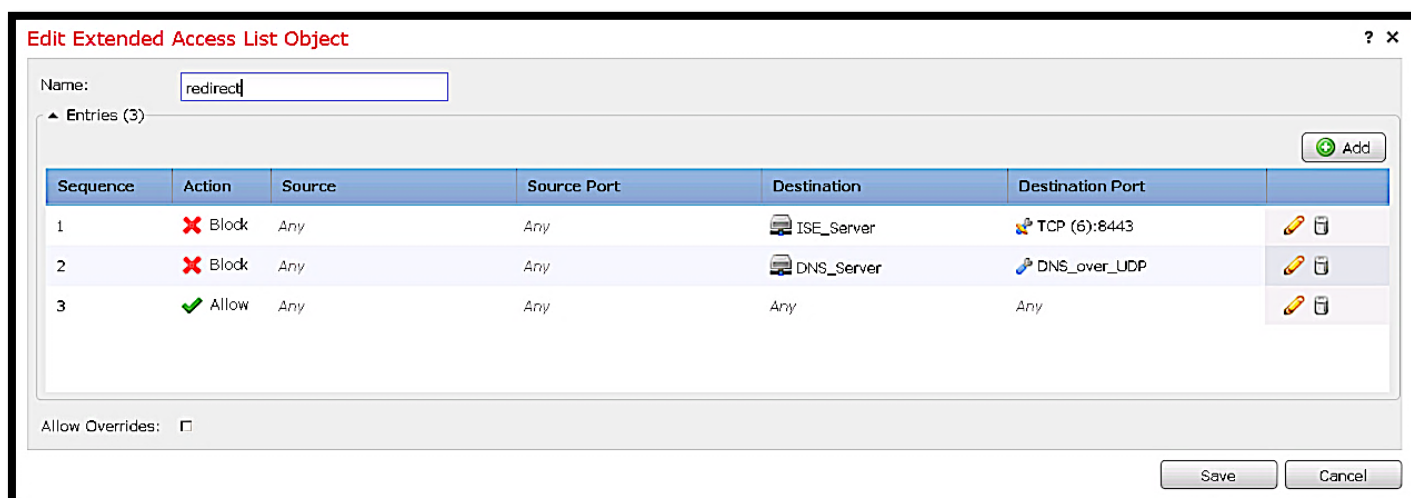
**注：**最も強力なセキュリティを実現するために、スプリットトンネリングは使用しないことをお勧めします。ただし、AnyConnect を実行するエンドポイントのコンソールにアクセスできないため、このシナリオではスプリットトンネリングを使用する必要があります。dCloud 内のエンドポイントにアクセスするにはさまざまな方法があるため、これらすべての可能性があるアクセスアドレスをバイパスする標準 ACL を作成する必要があります。これを、ここで行います。

- 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)] を選択します。[標準アクセスリストを追加 (Add Standard Access List)] をクリックします。
- 10.0.0.0/8、198.19.255.0/24、および 198.18.133.50 を許可する ACE を使用して、「SplitTunnel」という名前の標準アクセスリストを作成します。これを行うには、[追加 (Add)] をクリックして、次に [選択済みネットワーク (Selected Network)] ボックスの下のテキストボックスにこれらのネットワークを入力し、[追加 (Add)] をクリックします。

- [保存 (Save)] をクリックしてアクセスリストを保存します。



9. 左側のナビゲーションペインで、[アクセスリスト (Access List)] > [拡張 (Extended)] を選択します。[拡張アクセスリストの追加 (Add Extended Access List)] をクリックします。
10. 「redirect」という名前の以下のような拡張アクセスリストを作成します。これは、ポスチャ評価の実行時に ISE にリダイレクトされるトラフィックの決定に使用されます。[アクション (Action)] が [ブロック (Block)] の ACE は、リダイレクトから除外されます。



11. 左側のナビゲーションペインで、[アドレスプール (Address Pools)] > [IPv4 プール (IPv4 Pools)] を選択します。[IPv4 プールの追加 (Add IPv4 Pools)] をクリックします。
  - a. [名前 (Name)] に VPNPool と入力します。
    - i. [IPv4 アドレス範囲 (IPv4 Address Range)] に 198.19.10.57-198.19.10.62 と入力します。
    - ii. [マスク (Mask)] に 255.255.255.248 と入力します。
    - iii. [保存 (Save)] をクリックします。



**Add IPv4 Pool** ? X

Name\*

IPv4 Address Range\*   
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

Allow Overrides

ⓘ Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Override (0) ▼

Save Cancel

**注** : VPNPoolIPs オブジェクトと VPNPool オブジェクトは IP アドレス範囲が同じですが、オブジェクトタイプは異なります。VPNPool は RA VPN オブジェクトで参照され、VPNPoolIPs は NAT 免除の設定に使用されます。

12. [オブジェクト管理 (Object Management) ] に留まり、左側のナビゲーションペインで、[VPN] > [AnyConnect ファイル (AnyConnect Files) ] を選択します。
13. [AnyConnect ファイルの追加 (Add AnyConnect File) ] をクリックします。[参照 (Browse) ] をクリックし、Jump デスクトップの RA VPN フォルダから AnyConnectProfile.xml ファイル (拡張子 .xml は非表示の場合があります) を選択します。残りのフィールドには自動入力されます。

**Add AnyConnect File** ? X

Name:\*

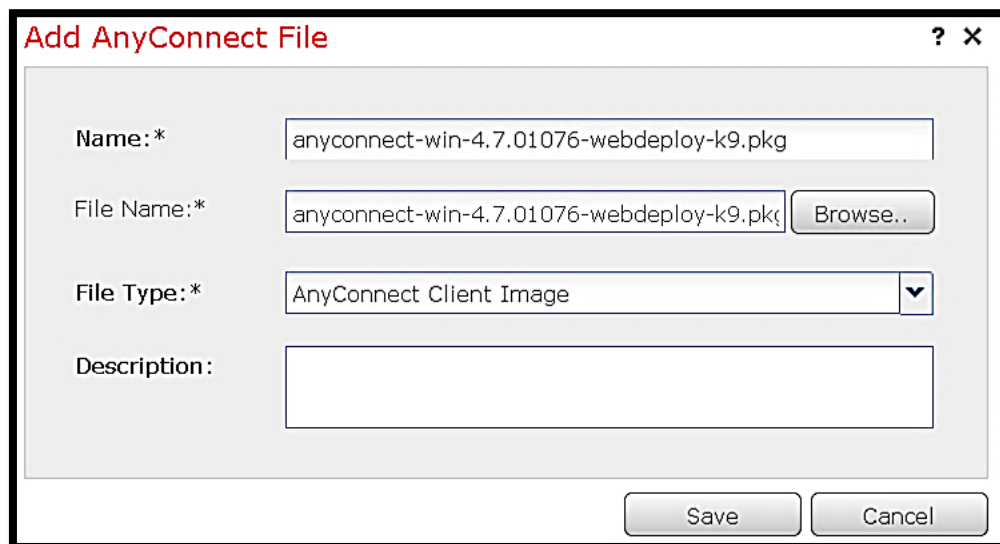
File Name:\*  Browse..

File Type:\*  ▼

Description:

Save Cancel

14. [AnyConnect ファイルの追加 (Add AnyConnect File)] をクリックします。[参照 (Browse)] をクリックし、Jump デスクトップの RA VPN フォルダから anyconnect-win-4.7.01076-webdeploy-k9.pkg を選択します。残りのフィールドには自動入力されます。



**Add AnyConnect File** ? X

Name:\* anyconnect-win-4.7.01076-webdeploy-k9.pkg

File Name:\* anyconnect-win-4.7.01076-webdeploy-k9.pkg Browse..

File Type:\* AnyConnect Client Image ▼

Description:

Save Cancel

15. 左側のナビゲーションペインで、[PKI] > [証明書の登録 (Cert Enrollment)] を選択します。[証明書の登録の追加 (Add Cert Enrollment)] をクリックします。
- [名前 (Name)] に、**NGFW1\_Outside** と入力します。（高可用性ラボを完了した場合は、必要に応じて「HA」という名前も可能）。
  - [登録タイプ (Enrollment Type)] ドロップダウンメニューから [PKCS12 ファイル (PKCS12 File)] を選択します。
  - [参照 (Browse)] をクリックし、Jump デスクトップの Certificates\Other Certificates フォルダから **ngfw-dcloud.pfx** (拡張子は非表示の場合があります) を選択します。
  - [パスワード (Passphrase)] に、**C1sco12345** を入力します。

**Add Cert Enrollment** ? X

Name\* NGFW1\_Outside

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File\*: ngfw-dcloud.pfx Browse PKCS12 File

Passphrase: ●●●●●●●●●●

Allow Overrides

Save Cancel

## ISE の RADIUS サーバグループの作成および設定

1. 左側のナビゲーションペインで、[RADIUS サーバグループ (RADIUS Server Group)] を選択します。[RADIUS サーバグループの追加 (Add RADIUS Server Group)] をクリックします。
  - a. グループ名を **ISE\_RADIUS** にします。
  - b. [動的な許可を有効にする (Enable dynamic authorization)] チェックボックスをオンにします。
  - c. 緑色の [+] 記号をクリックして RADIUS サーバを追加します。
2. 次の情報を入力します (その他の属性はデフォルトのまま)。
  - a. [IP アドレス/ホスト名 (IP Address/Hostname)] に 198.19.10.130 と入力します。
  - b. [キー (Key)] に、**C1sco12345** を入力します。[キーの確認 (Confirm Key)] フィールドに同じ値を入力します。
  - c. [特定のインターフェイス (Specific interface)] ラジオボタンを選択し、ドロップダウンメニューから **InZone** を選択します。
  - d. [リダイレクト ACL (Redirect ACL)] で [redirect] を選択します。

**Edit RADIUS Server** ? X

IP Address/Hostname:\*   
*Configure DNS at Threat Defense Platform Settings to resolve hostname*

Authentication Port:\*  (1-65535)

Key:\*

Confirm Key:\*

Accounting Port:  (1-65535)

Timeout:  (1-300) Seconds

Connect using:  Routing  Specific Interface ⓘ

+

Redirect ACL:  +

Save Cancel

3. [保存 (Save)] をクリックしてこの RADIUS サーバを RADIUS サーバグループに追加します。もう一度 [保存 (Save)] をクリックします。

## NGFW1 の DNS サーバの設定

1. [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [DNS サーバグループ (DNS Server Group)] に移動します。[DNS サーバグループの追加 (Add DNS Server Group)] をクリックします。
  - a. [名前 (Name)] に DCloud-DNS と入力します。
  - b. [デフォルトドメイン (Default Domain)] に dcloud.local と入力します。
  - c. [DNS サーバ (DNS Server)] に 198.19.10.100 と入力します。
  - d. [保存 (Save)] をクリックします。

**New DNS Server Group Object** ? X

Name\*:

Default Domain:

Timeout:   
*Range: 1 - 30 Seconds*

Retries:   
*Range: 0 - 10*

DNS Servers:   
*(Multiple values in IPv4 or IPv6 addresses can be specified as comma separated entries)*

## デフォルトグループポリシー (DfltGrpPolicy) の編集

注：通常、VPN グループポリシーの編集（または新しいグループポリシーの追加）は、RA VPN ウィザードの実行中に行いません。ここでは、作業の明確化のためと RA VPN ウィザードの実行を容易にするために、このタスクを独立して行います。

1. 左側のナビゲーションウィンドウで、[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。鉛筆のアイコンをクリックして、**DfltGrpPolicy** を編集します。
2. [一般 (General)] > [VPN プロトコル (VPN Protocols)] を選択し、[IPsec-IKEv2] をオフにします。

**Edit Group Policy** ? X

Name\*:

Description:

**General** AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:  
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

3. [一般 (General) ] > [DNS/Wins] を選択します。
  - a. [プライマリ DNS サーバ (Primary DNS Server) ] ドロップダウンリストから **DNS\_Server** を選択します。
  - b. [デフォルトドメイン (Default Domain) ] に **dcloud.local** と入力します。

The screenshot shows the 'Edit Group Policy' dialog box with the 'General' tab selected. The 'Name' field contains 'DfltGrpPolicy'. The 'Description' field is empty. The 'DNS/WINS' section is expanded, showing the following settings:

- Primary DNS Server: **DNS\_Server** (highlighted with a red box)
- Secondary DNS Server: (empty)
- Primary WINS Server: (empty)
- Secondary WINS Server: (empty)
- DHCP Network Scope: (empty)
- Default Domain: **dcloud.local** (highlighted with a red box)

Below the DHCP Network Scope field, there is a note: "Only network object with ipv4 address is allowed (Ex: 10.72.3.5)". At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

4. [一般 (General) ] > [スプリットトンネル (Split Tunnel) ] を選択します。
  - a. [IPv4 スプリットトンネリング (IPv4 Split Tunneling) ] ドロップダウンリストから、[以下に指定したネットワークを除外する (Exclude networks specified below) ] を選択します。
  - b. [標準アクセスリスト (Standard Access List) ] ドロップダウンリストから、**SplitTunnel** を選択します。

**Edit Group Policy** ? X

Name:\* DfltGrpPolicy

Description:

**General** AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling: Exclude networks specified below

IPv6 Split Tunneling: Allow all traffic over tunnel

Split Tunnel Network List Type:  Standard Access List  Extended Access List

Standard Access List: SplitTunnel

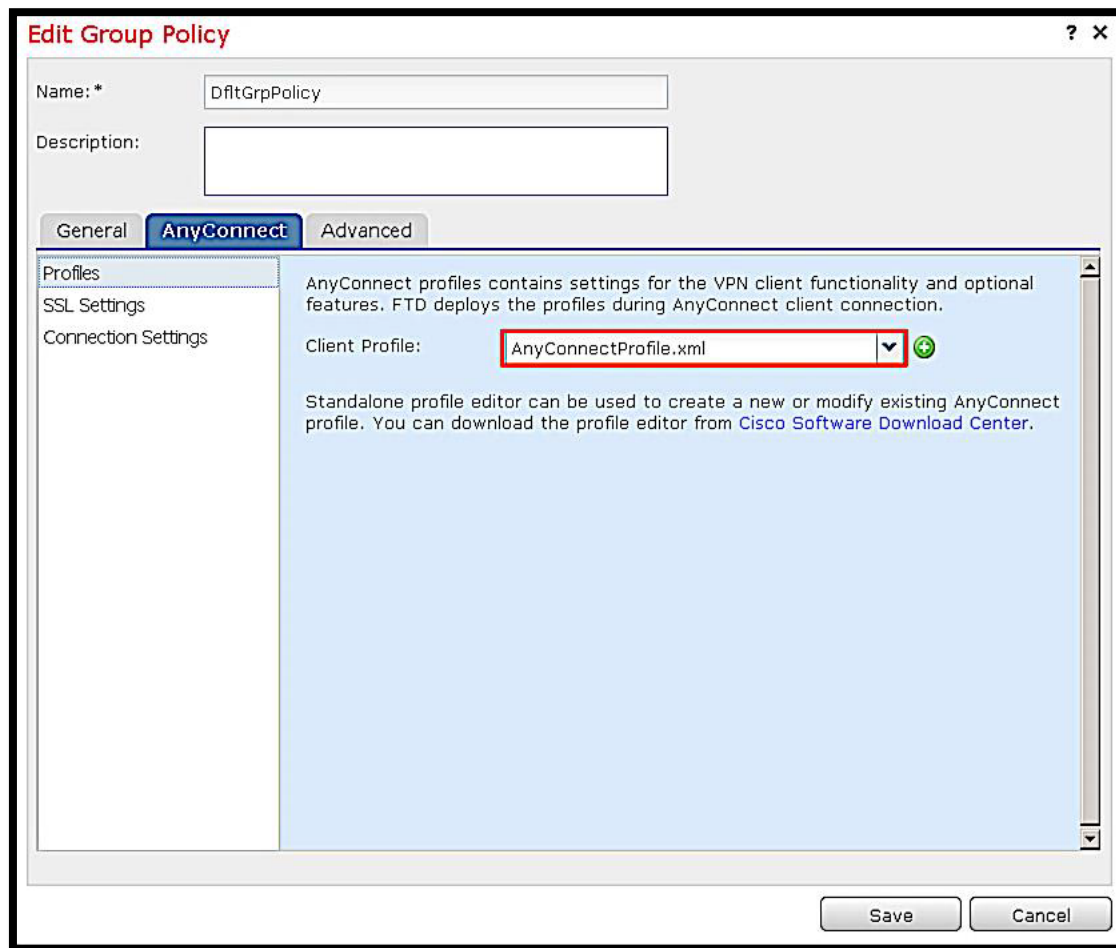
DNS Request Split Tunneling

DNS Requests: Send DNS requests as per split tunnel policy

Domain List:

Save Cancel

5. [AnyConnect] > [プロファイル (Profiles)] で、[クライアントプロファイル (Client Profile)] ドロップダウンリストから、AnyConnectProfile.xml を選択します。



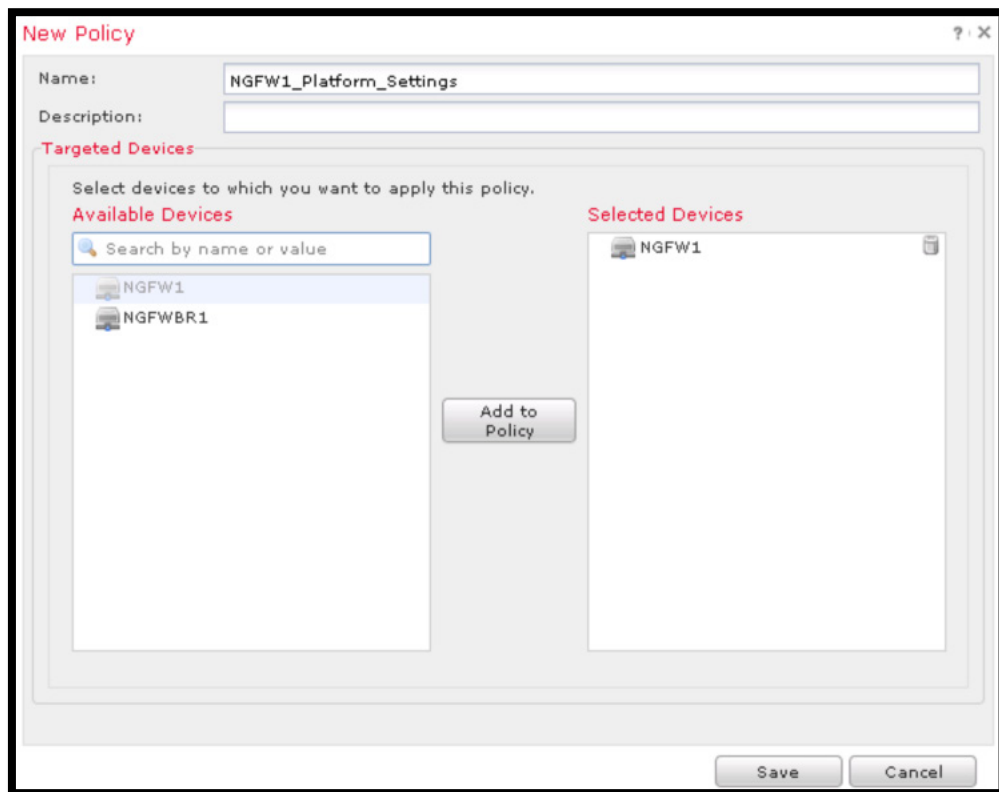
6. [保存 (Save) ]をクリックして DfltGrpPolicy への変更を保存します。

**注：**通常は、この時点で AnyConnect ライセンスも有効にしますが、これは設定済みです。それを確認するには [システム (System) ] > [ライセンス (Licenses) ] > [スマートライセンス (Smart License) ] に移動します。FMC で評価ライセンスが使用されている一方で、輸出規制対象の機能が有効になっていることが分かります。通常はこのことは不可能であるため、評価ライセンスでは SSL VPN をライセンス供与できません。

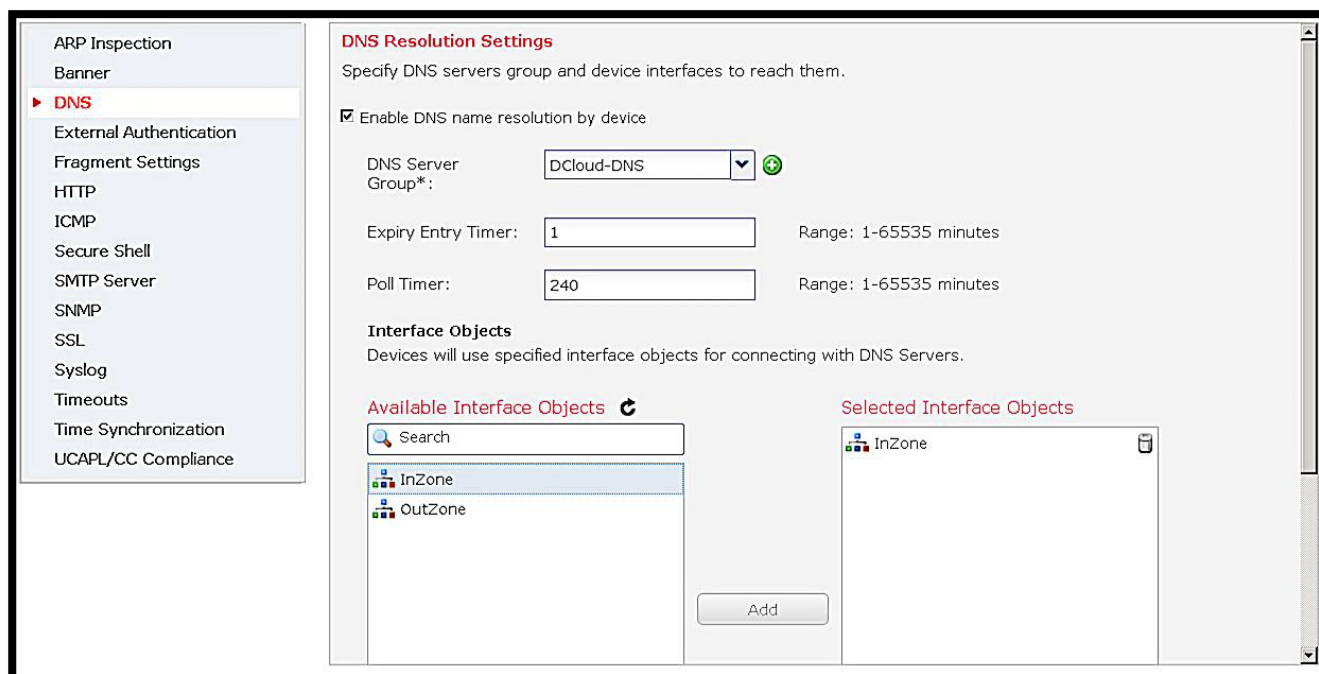
### プラットフォーム設定を変更する

1. [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] に移動して、NGFW1\_Platform\_Settings プラットフォーム設定を編集します。





2. [プラットフォーム設定 (Platform Settings)] ウィンドウで、[DNS] に移動します。
  - a. [デバイスによる DNS 名解決を有効にする (Enable DNS name resolution by device)] をオンにします。
  - b. [DNS サーバグループ (DNS Server Group)] ドロップダウンから **DCloud-DNS** を選択します。
  - c. [インターフェイスオブジェクト (Interface Objects)] に **InZone** を追加します。
  - d. [保存 (Save)] をクリックします。



## RA VPN ウィザードの実行

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 **RAVPN** と入力します。
  - c. [ターゲットデバイス (Target Device) ] から **NGFW** を選択します。[追加 (Add) ] をクリックします。
  - d. IPsec-IKEv2 のチェックボックスをオフにします。
  - e. 右下隅にある [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 **RAVPN** 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) ] と [認可サーバ (Authorization Server) ] で **ISE-RADIUS** を選択します。
  - d. [IP アドレスプール (Use IP Address Pools) ] の [IPv4 アドレスプール (IPv4 Address Pools) ] で、次の手順を実行します。
    - i. 鉛筆アイコンをクリックし、[アドレスプール (Address)] ウィンドウから **VPNPool** を選択して、[追加 (Add) ] をクリックします。
  - e. [OK] をクリックします。
  - f. [次へ (Next) ] をクリックします。
3. [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

4. 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。
5. 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、**NGFW1\_Outside** を選択します。
  - c. [次へ (Next) ] をクリックします。
  - d. 設定の概要を確認し、[完了 (Finish) ] をクリックします。

### アクセスコントロールと NAT ポリシーの変更

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) ] に移動します。
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-S3-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. **VPNPoolIPs** を選択し、[送信元に追加 (Add to Source) ] をクリックします。
  - b. **LAN\_Network** を選択し、[宛先に追加 (Add to Destination) ] をクリックします。

4. [検査 (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 **BP ファイルポリシー** 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。
5. [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 適用除外の設定

1. FMC で、[デバイス (Devices) ] > [NAT] に移動します。
2. 既存の NAT ポリシー (デフォルト NAT ポリシー) を選択して編集します。[ルールの追加 (Add Rule) ] をクリックします。
  - a. [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) ] では、最初のボックスで [アドレス (Address) ] を選択し、2 番目のボックスで LAN\_Network を選択します。
5. [元の宛先 (Original Destination) ] では、最初のボックスで [アドレス (Address) ] を選択し、2 番目のボックスで VPNPoolIPs を選択します。
6. [変換後の送信元 (Translated Source) ] で、**LAN\_Network** を選択します。
7. [変換後の宛先 (Translated Destination) ] で、**VPNPoolIPs** 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 ARP をプロキシしない (Do not proxy ARP on Destination Interface) ] を選択します。

**注：**このラボ演習では、[宛先インターフェイスで ARP をプロキシしない (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. NAT ポリシーの最後のルールを編集します。
  - a. [送信元インターフェイスオブジェクト (Source Interface Objects) ] を **InZone** から [すべて (any) ] に変更します。これで、インターネットを送信先とする VPN クライアントからのトラフィックが正しく NAT 処理されるようになります。
  - b. [OK] をクリックして NAT ルールの変更を保存します。
11. [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 設定を展開して確認する

1. デバイスにポリシーを導入します。FMC で、[展開 (Deploy) ] ボタンをクリックします。
2. **NGFW1** を選択し、[展開 (Deploy) ] をクリックします。[HA 環境ではない場合、NGFW3 に関する警告は無視します]
3. 展開が完了するまで待ちます。
4. **NGFW1 CLI** への PuTTY セッションを開きます。admin/C1sco12345 でログインし、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

```

NGFW1
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 28 07:08:05 UTC 2019 from jump.dcloud.local on pts/0

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.4.0 (build 2)
Cisco Firepower Threat Defense for VMWare v6.4.0 (build 102)

> show running-config tunnel-group
tunnel-group RAVPN type remote-access
tunnel-group RAVPN general-attributes
  address-pool VPNPool
  authentication-server-group ISE RADIUS
  accounting-server-group ISE RADIUS
tunnel-group RAVPN webvpn-attributes
group-alias RAVPN 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 ssl-client
  split-tunnel-policy excludespecified
  split-tunnel-network-list value SplitTunnel
  default-domain value dcloud.local
  user-authentication-idle-timeout none
  webvpn
    anyconnect keep-installer none
    anyconnect modules value dart
    anyconnect profiles value AnyConnectProfile.xml 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 のトラストポイントは NGFW1\_Outside or HA です。

d. show running-config ip local pool

```

> show running-config ip local pool
ip local pool VPNPool 198.19.10.57-198.19.10.62 mask 255.255.255.248
>

```

e. show running-config nat

```

> show running-config nat
nat (inside,outside) source static LAN_Network LAN_Network destination static VPNPoolIPs VPNPoolIPs no-proxy-arp
object network FMC Private
nat (inside,outside) static FMC_Public
object network wwwin
nat (inside,outside) static wwwout
nat (inside,outside) after-auto source dynamic any interface
>

```

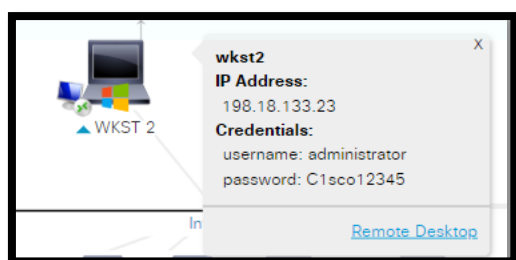
5. NGFW1 CLI で次のコマンドを実行して、AAA をテストします。

```
test aaa-server authentication ISE_RADIUS host 198.19.10.130 username vpnuser password C1sco12345
```

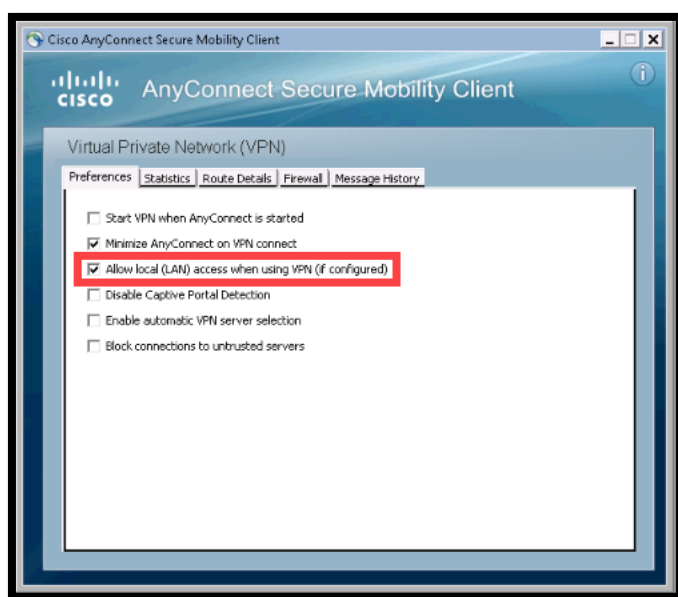
## AnyConnect による接続

**注：このシナリオでは、コンプライアンス対応システムの定義は、デスクトップに `compliant.txt` というファイルを持つシステムです。この演習では、Wkst2 は非コンプライアンス対応として開始されます。また、Wkst2 には、ポスチャモジュールがインストールされています。**

1. Wkst2 に接続します。管理者として自動的にログインされます。2 つの方法のいずれかを使用して接続できます。
  - a. 以下に示すトポロジマップから接続します。これは推奨される方法です。

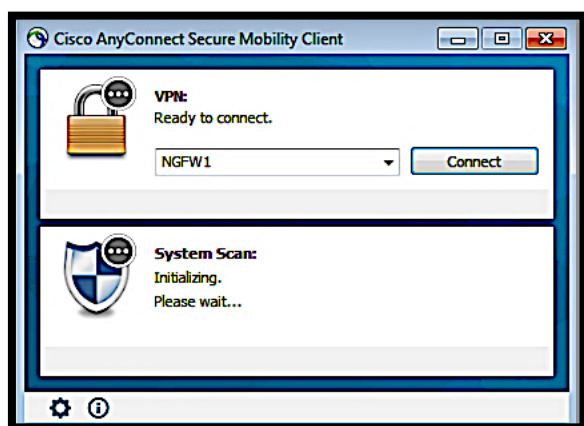


- b. Jump デスクトップの Remote Desktops フォルダの Wkst2 (Outside PC) ショートカットをクリックします。ただし、これを行う場合は、AnyConnect クライアントでローカル LAN アクセスを許可する必要があります。



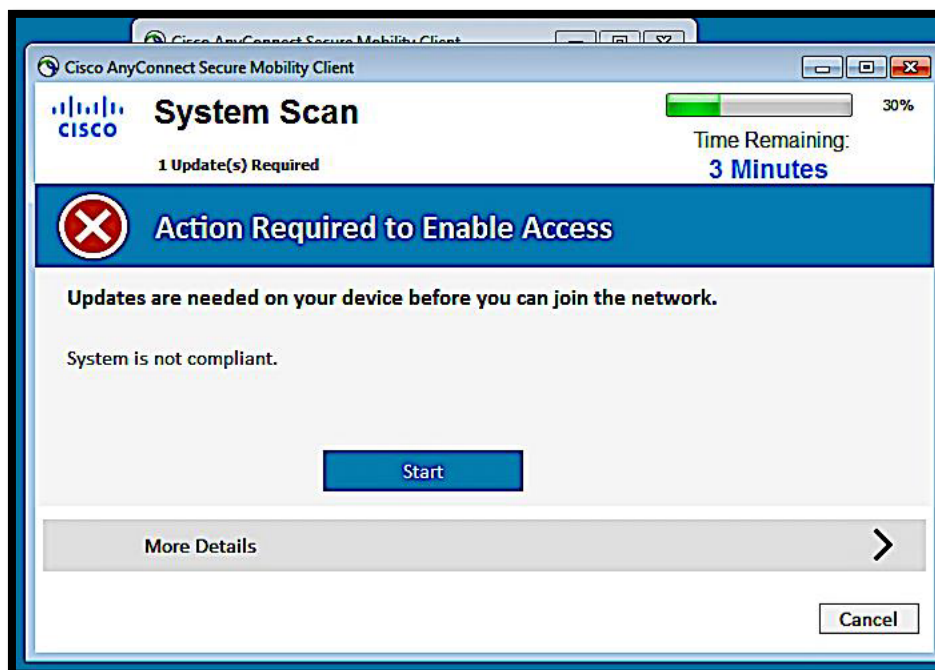
- c. VPN 経由でポッドに接続している場合は、ラップトップ上の RDP クライアントを使用して 198.18.133.23 に接続します。管理者として、パスワード C1sco12345 でログインします。

2. WKST2 のデスクトップから、[スタート (Start)] メニューから AnyConnect を開きます。[接続先 (Connect To) ] フィールドには **NGFW1** を選択する必要があります。[接続 (Connect) ] をクリックします。

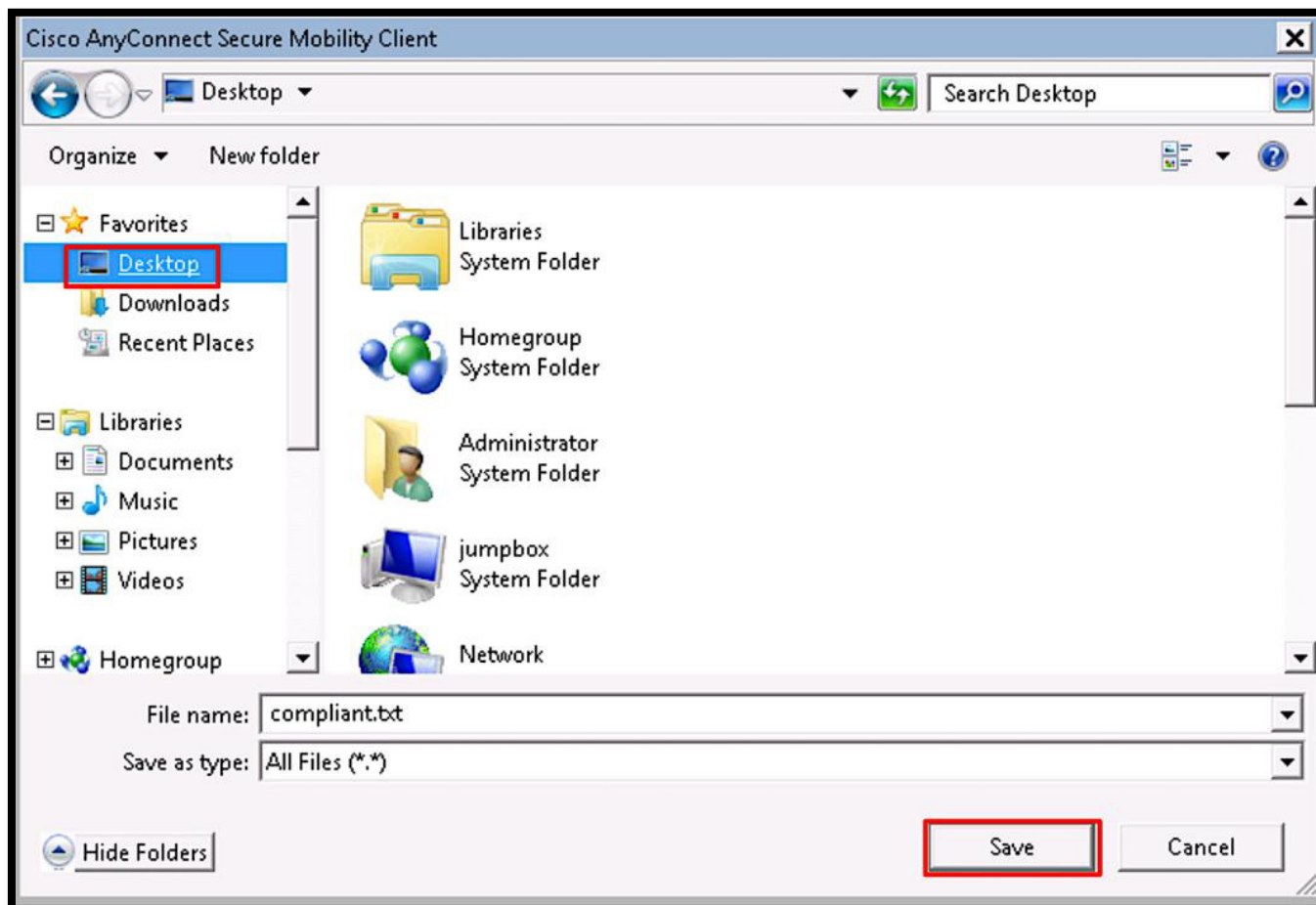


ログインプロンプトが表示されたら、ログイン名 **harry**、パスワード **C1sco12345** でログインします。最初の接続で、AnyConnect コンプライアンスモジュールがダウンロードされていることを確認できます。

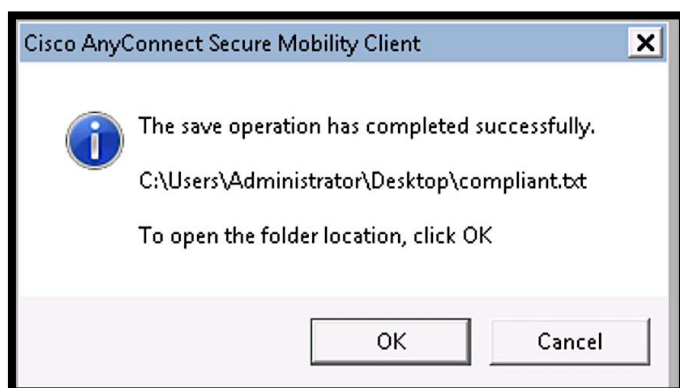
3. 最初の接続ではシステムが基準を満たしていないため、準拠の対応を求めるプロンプトが表示されます。[開始 (Start) ] をクリックします。



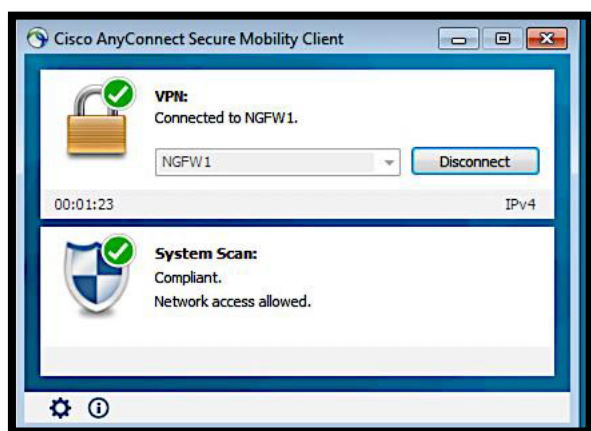
- compliant.txt ファイルの保存を促すプロンプトが表示されます。Compliant.txt ファイルを保存するためのウィンドウは、[ システムスキャン (System Scan) ] ウィンドウの背後に表示されることがあります。保存先フォルダをデスクトップに変更します。



- 「保存操作が正常に完了しました」というメッセージが表示されたダイアログボックスでは、[ キャンセル (Cancel) ] をクリックできます。フォルダを開く必要はありません。



6. ファイルがインストールされると、クライアントはシステムに準拠していることを宣言し、システムトレイを調べて、Cisco AnyConnect アイコン（南京錠のある地球儀）をクリックすることで、確認できるようになります。次のウィンドウが開きます。



7. Wkst2 上の Firefox ブラウザのブックマークを使用して、ブックマークが登録されている 2 つの内部 Web サイト（Inside、Alt Inside）にアクセスできることを確認します。
8. これらの内部サーバのいずれかで Files リンクをクリックし、Zombies.pdf をクリックします。ファイルがブロックされることを確認します。ProjectX.pdf のような無害のファイルがブロックされていないことを確認します。

**注：クラウド ルックアップ タイムアウト（これらのポッドで発生することがあります）によって演習が中断されないように、Zombies.pdf ファイルは FMC カスタム検出リストに追加されています。実際にクラウドルックアップを必要とするテストを実行する場合は、URL として「http://altoutside.dcloud.local/malware」と入力し、Buddy.exe のダウンロードを試みてください。**

9. 侵入がブロックされていることを確認します。これは、Wkst2 でコマンドプロンプトを開き、inside.dcloud.local への FTP 接続を確立することによって実行できます。接続を許可されるはずですが、ユーザ名：guest、パスワード：C1sco12345 でログインします。ログインしたら、cd ~root と入力します。接続がリセットされるはずですが、これは、Snort シグネチャ 336 がトリガされたためです。

```

Administrator: Command Prompt - ftp inside.dcloud.local
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp inside.dcloud.local
Connected to inside.dcloud.local.
220 (vsFTPD 3.0.2)
User (inside.dcloud.local:(none)): guest
331 Please specify the password.
Password:
230 Login successful.
ftp> cd ~root
Connection closed by remote host.
ftp> _

```

10. (オプション) FMC で、マルウェアイベント ([分析 (Analyze)] > [ファイル (Files)] > [マルウェアイベント (Malware Events)]) と侵入イベント ([分析 (Analyze)] > [侵入 (Intrusions)] > [イベント (Events)]) を調べます。また、[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)] > [VPN] に移動して、RA VPN ユーザの統計情報を調べることもできます。



11. NGFW1 の PuTTY セッションで、次のコマンドを入力します。 **show vpn-sessiondb detail anyconnect**

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID      : 1.1
Public IP     : 198.18.133.23
Encryption    : none
TCP Src Port  : 49215
Auth Mode     : userPassword
Idle Time Out: 30 Minutes
Client OS     : win
Client OS Ver: 6.1.7601 Service Pack 1
Client Type   : AnyConnect
Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.7.02036
Bytes Tx      : 3235874
Pkts Tx       : 6
Pkts Tx Drop  : 0
Bytes Rx      : 605
Pkts Rx       : 0
Pkts Rx Drop  : 0
Hashing       : none
TCP Dst Port  : 443
Idle TO Left  : 26 Minutes

SSL-Tunnel:
Tunnel ID      : 1.2
Assigned IP    : 198.19.10.57
Public IP     : 198.18.133.23
Encryption    : AES-GCM-256
Hashing       : SHA384
Ciphersuite   : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation : TLSv1.2
TCP Src Port  : 49223
TCP Dst Port  : 443
Auth Mode     : userPassword
Idle Time Out: 30 Minutes
Client OS     : Windows
Client Type   : SSL VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.7.02036
Bytes Tx      : 8106
Pkts Tx       : 6
Pkts Tx Drop  : 0
Bytes Rx      : 448
Pkts Rx       : 6
Pkts Rx Drop  : 0
Filter Name   : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-57f6b0d3

DTLS-Tunnel:
Tunnel ID      : 1.3
Assigned IP    : 198.19.10.57
Public IP     : 198.18.133.23
Encryption    : AES256
Hashing       : SHA1
Ciphersuite   : DHE-RSA-AES256-SHA
Encapsulation : DTLSv1.0
UDP Src Port  : 49786
UDP Dst Port  : 443
Auth Mode     : userPassword
Idle Time Out: 30 Minutes
Client OS     : Windows
Client Type   : DTLS VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.7.02036
Bytes Tx      : 14895898
Pkts Tx       : 10996
Pkts Tx Drop  : 0
Bytes Rx      : 324974
Pkts Rx       : 6291
Pkts Rx Drop  : 0
Filter Name   : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-57f6b0d3
```

## シナリオ 6. ハイアベイラビリティ設定 (オプション)

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 を設定して展開する
- 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

#### REST API スクリプトを実行して NGFW3 を設定する

1. Jump PC に移動し、PuTTY セッションを開いて **NGFW3** 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. 出力は、「Registration Pending or Completed」となります。
  - d. 「Managed Locally (ローカルで管理) 」と表示された場合には、
    - a. **configure manager delete** と入力して **yes** を選択し、次に下記のステップ [e] に従います。
  - e. 「**No managers**」と表示される場合、または上記のステップでローカルマネージャを削除した場合は、
    - i. **configure manager add fmc.dcloud.local C1sco12345** と入力します。
    - ii. コマンドプロンプトが再び表示されたら **show managers** と入力し、fmc.dcloud.local のステータスが pending になっていることを確認します。

```

NGFW3
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Nov 27 19:04:47 UTC 2019 from jump.dcloud.local on pts/0

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

> show managers
Managed locally.

> configure manager delete

If you enabled any feature licenses, you must disable them in Firepower Device M
anager 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
> configure manager add fmc.dcloud.local C1sco12345
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

> show managers
Host                : fmc.dcloud.local
Registration Key     : ****
Registration        : pending
RPC Status          :
>

```

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

設定の複製および同期

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。この中断の間にトラフィックをドロップするか、さらに検査せずにパスさせるかは、管理対象デバイスのモデルとトラフィックの処理方法によって決まります。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という警告が表示され、操作をキャンセルできます。

2. 内部 Linux サーバから root/C1sco12345 でログインします。
  - a. 「runapiscrpt2」と入力し、プロンプトが表示されるまで待ちます。
  - b. 「Which Firewall do you want to register? (どのファイアウォールを登録しますか)」と表示されたら、番号「3」を入力します。

- c. 「Enter name of new Access Control Policy to be create (作成する新しいアクセス コントロール ポリシーの名前を入力してください)」と表示された場合には、名前に **HA** と入力します。

**注** : FMC UI を使用して、NGFW を **FMC に追加して管理することができます**。ただし、ここでは REST API を使用して自動化されたソリューションの機能を確認します。Python スクリプトは、**内部 Linux サーバ上で、runapiscript という名前で /usr/local/bin に置かれています**。このスクリプトは、FMC で REST API を呼び出し、NGFW3 を FMC に登録し、正常性ポリシーを NGFW3 に適用し、インターフェイスを検出して、IP アドレスを設定し、スクリプトの実行中に指定された名前ですべてのアクセス コントロール ポリシーを展開します。

```

root@inside:~
[root@inside ~]# runapiscript
Specify firewall to register.
Enter 1 for NGFW1.
Enter 2 for NGFW2.
Enter 3 for NGFW3.
Which firewall do you want to register? 3
Enter name of new Access Control Policy to be create: HA
status code is: 201
Post was successfull...
Access Control Policy HA created.

Attempting to register NGFW3.
status code is: 202
Post was successfull...
Registration is in progress. (1)
Registration is in progress. (2)
Registration is in progress. (3)
Registration is in progress. (4)
Registration is in progress. (5)
Registration is in progress. (6)
Registration is in progress. (7)
Registration is in progress. (8)
Registration is in progress. (9)
Registration completed.

status code is: 200
GET was successfull...
Device found; setting ID.
Interface discovery is in progress. (1)
Interface discovery is in progress. (2)
Interface discovery completed.

status code is: 200
GET was successfull...
interface 1 found
interface 2 found
Attempting to set outside interface IP address to 198.18.133.83/18.
status code is: 200
Put was successfull...
Attempting to set inside interface IP address to 198.19.10.3/24.
status code is: 200
Put was successfull...
[root@inside ~]#

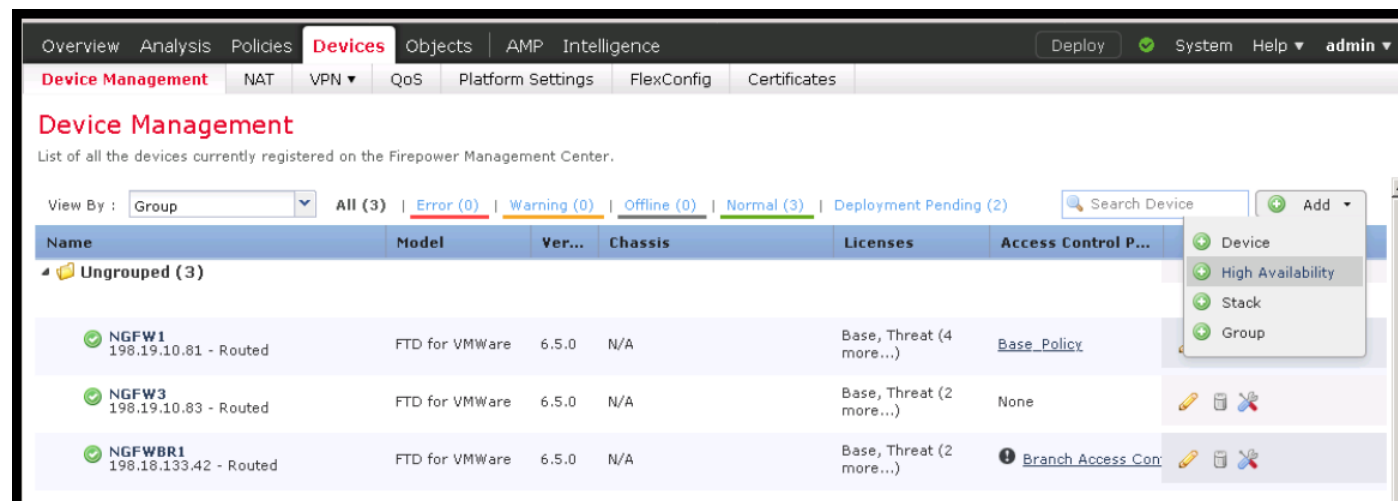
```

**注** : 「Registration is in progress (登録の進行中)」の数は、変動する場合があります。

- d. Firefox に戻り、FMC で NGFW3 の登録ステータスを確認して、デバイスの登録を許可します。

## ハイアベイラビリティペアの設定

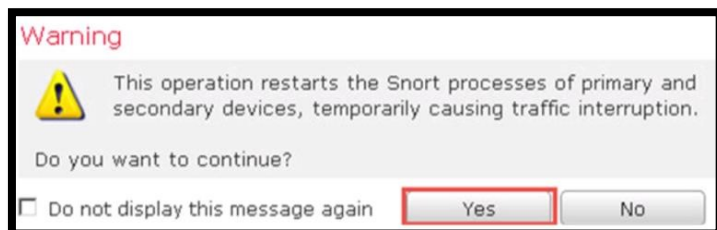
1. [デバイス (Devices) ] > [デバイス管理 (Device Management) ] > [追加 (Add) ] > [ハイアベイラビリティ (High Availability) ] に移動します。



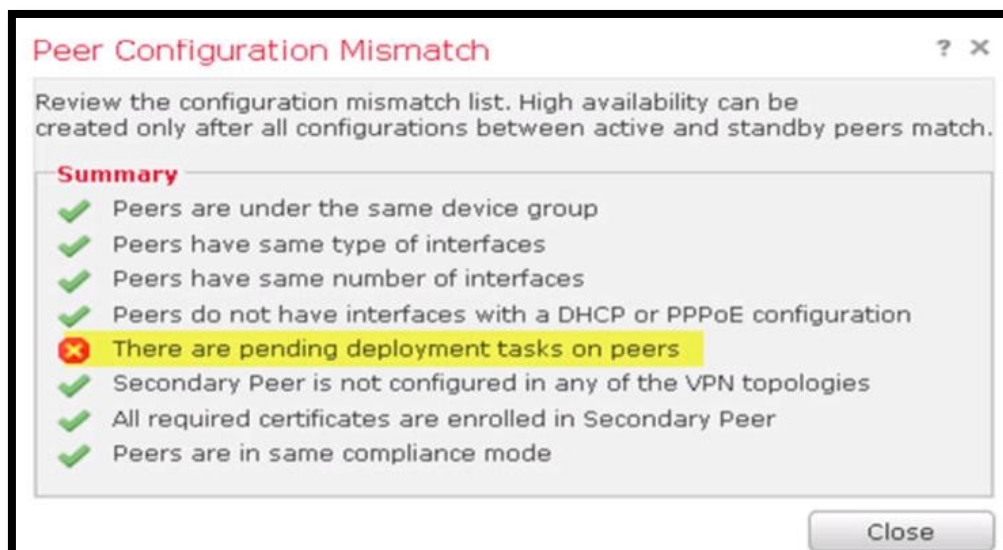
注：NGFW3 管理インターフェイス (198.19.10.83) は初期設定中に事前設定されています。G0/0 および G0/1 インターフェイスはスクリプトによって設定されています。インターフェイスにはセキュリティゾーンのリストが表示されませんが、HA プロセスが実行されると、セキュリティゾーンとインターフェイスの IP アドレスが NGFW1 から継承されます。

- a [名前 (Name)] : HA\_Test
- b [デバイスタイプ (Device Type) ] : Firepower Threat Defense
- c [プライマリピア (Primary Peer) ] : NGFW1
- d [セカンダリピア (Secondary Peer) ] : NGFW3
- e 次に [続行 (Continue) ] をクリックします。





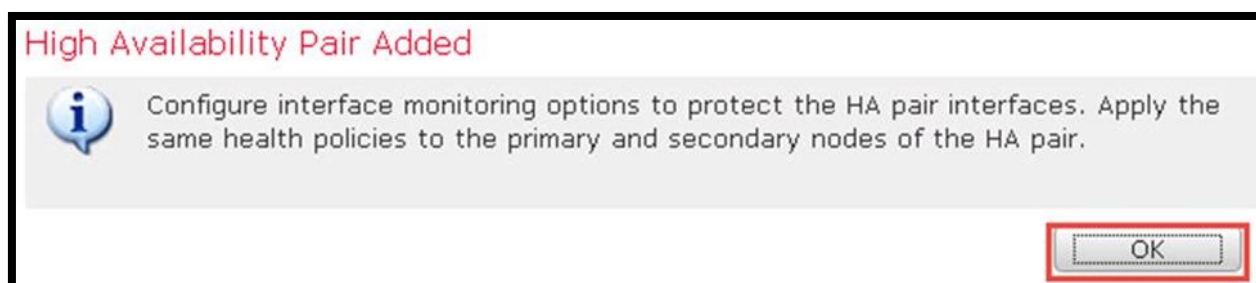
注：いずれかの HA ピアで設定タスクが完了しているものの、まだ展開していない場合には、次のメッセージが表示されます。



2. NGFW3 に変更を展開します。
3. 前に戻り、手順 1 を繰り返します。
4. [インターフェイスの選択 (Select Interface)] : GigabitEthernet0/2
5. [名前 (Name)] : Failover\_Link
6. [プライマリ IP (Primary IP)] : 198.19.254.1  
[セカンダリ IP (Secondary IP)] : 198.19.254.2 [サブネットマスク (Subnet Mask)] : 255.255.255.0
7. [ステートリンク (State Link)] : LAN フェールオーバーと同じインターフェイス
8. [IPsec 暗号化 (IPsec Encryption)] : 有効 (オプション)

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。

9. [追加 (Add)] 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。次の図のようにプロンプトが表示されたら、[OK] をクリックします。



注：HA の設定にはしばらく時間がかかります。展開ボタンの横の [タスク (Tasks)] を見ると、随時最新のステータスを確認できます。

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (2)					
HA_Test High Availability					
NGFW1(Primary, Unknown) 198.19.10.81 - Routed	FTD for VMWare	6.5.0	N/A	Base, Threat (2 more...)	Base_Policy
NGFW3(Secondary, Unknown) 198.19.10.83 - Routed	FTD for VMWare	6.5.0	N/A	Base, Threat (2 more...)	Base_Policy

10. 完了すると次のように表示されます。

Name	Model	Versi...	Chassis	Licenses	Access Control Policy	
Ungrouped (2)						
HA_Test High Availability						
NGFW1(Primary, Active) 198.19.10.81 - Routed	FTD for VMWare	6.5.0	N/A	Base, Threat (2 more...)	Base_Policy	
NGFW3(Secondary, Standby) 198.19.10.83 - Routed	FTD for VMWare	6.5.0	N/A	Base, Threat (2 more...)	Base_Policy	

11. [デバイス (Devices) ] > [デバイス管理 (Device Management) ] に移動し、鉛筆アイコンをクリックして HA ポリシーを編集します。

Name	Model	Versi...	Chassis	Licenses	Access Control Policy	
Ungrouped (2)						
HA_Test High Availability						
NGFW1(Primary, Active) 198.19.10.81 - Routed	FTD for VMWare	6.5.0	N/A	Base, Threat (2 more...)	Base_Policy	
NGFW3(Secondary, Standby) 198.19.10.83 - Routed	FTD for VMWare	6.5.0	N/A	Base, Threat (2 more...)	Base_Policy	

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。推奨されてはいますが、スタンバイアドレスは必須ではありません。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、トラフィックを通過させます。

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。しかしながら、プライマリ装置が使用可能になると、セカンダリ (アクティブ) 装置は 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。その結果、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 アドレスであれば、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ため、この中断を回避できます。マルチインスタンス機能では、FXOS シャーシはプライマリ

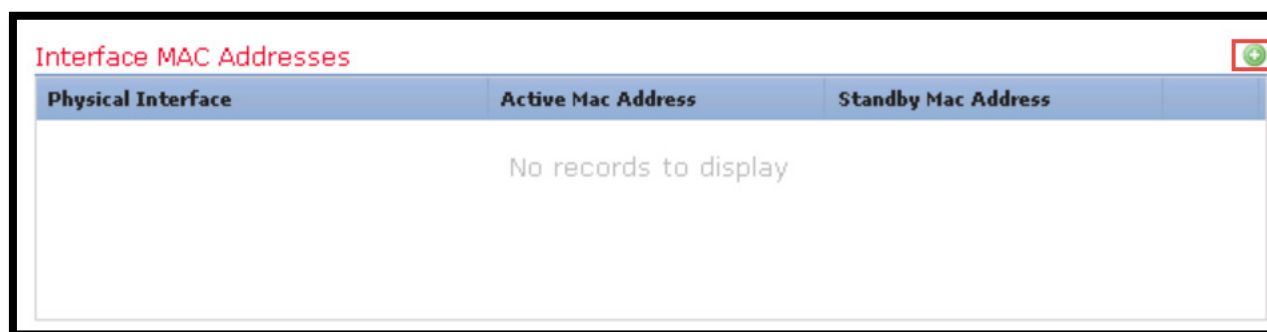


MAC アドレスのみを自動生成します。プライマリおよびセカンダリ MAC アドレスの両方で、生成された MAC アドレスを仮想 MAC アドレスで上書きすることができ、セカンダリ MAC アドレスを設定すると、セカンダリ ユニットのハードウェアが新しくなった場合に、to-the-box 管理トラフィックが中断されないようになります。

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 アドレスが変わった場合、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。

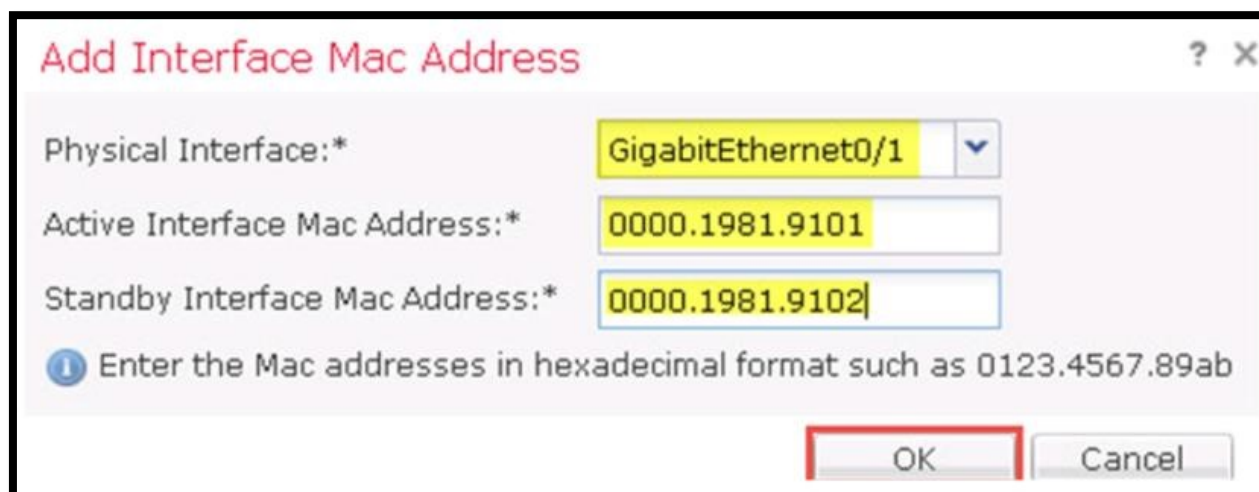
ステートリンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。唯一の例外は、ステートリンクが通常のデータ インターフェイスに設定されている場合です。

12. 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。



13. [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)]: 受講者が選択する入力 (下の例)。[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。



14. 内部インターフェ이스の横にある鉛筆アイコンをクリックします。

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	
outside	198.18.133.81					✓	✎
diagnostic						✓	✎
inside	198.19.10.1					✓	✎

15. [スタンバイ IP アドレス (Standby IP Address) ] に 198.19.10.31 と入力し、[OK] をクリックします。外部インターフェイス 198.18.133.132 について繰り返します。

**Edit outside** ? x

Monitor this interface for failures

IPv4 IPv6

Interface Name: outside

Active IP Address: 198.18.133.81

Mask: 18

Standby IP Address:

OK Cancel

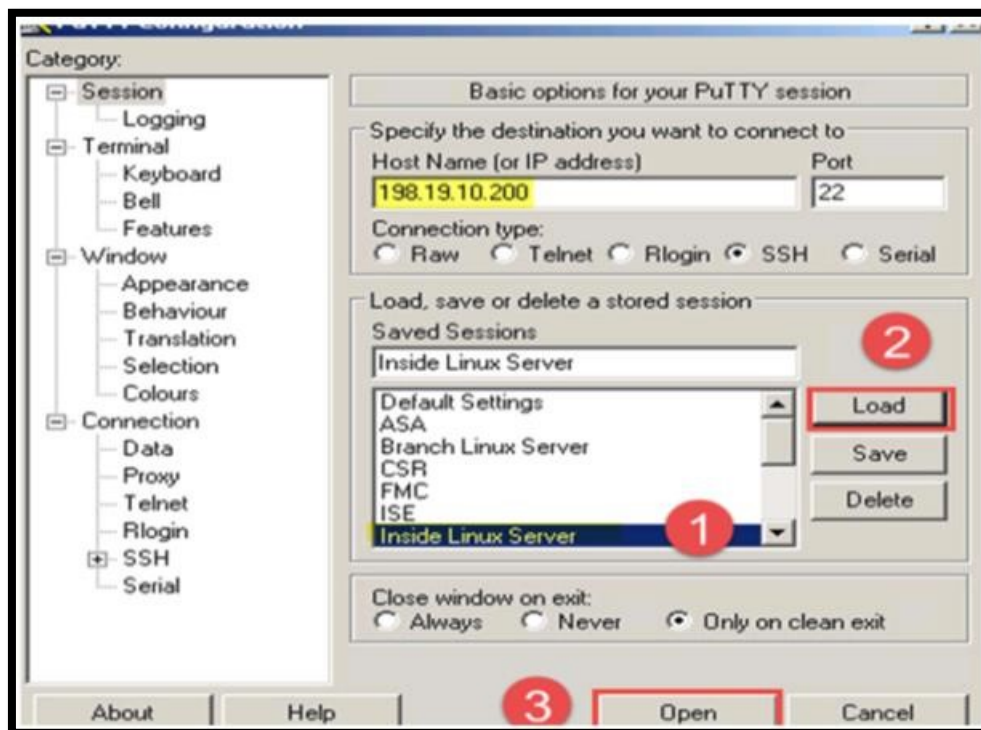
16. [OK]、[保存 (Save) ]、[展開 (Deploy) ]の順にクリックします。**HA\_Test** を選択し、[展開 (Deploy) ]をクリックします。

### NGFW3 の設定を確認します。

1. HA のセットアップ中に NGFW3 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、**NGFW3** 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、次のように入力します。
  - 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 のフェイルオーバー 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、ping の実行を続行します。

```
[root@inside ~]# ping outside
PING outside (198.18.133.200) 56(84) bytes of data.
64 bytes from outside (198.18.133.200): icmp_seq=1 ttl=64 time=4.51 ms
64 bytes from outside (198.18.133.200): icmp_seq=2 ttl=64 time=1.37 ms
64 bytes from outside (198.18.133.200): icmp_seq=3 ttl=64 time=1.39 ms
64 bytes from outside (198.18.133.200): icmp_seq=4 ttl=64 time=1.48 ms
64 bytes from outside (198.18.133.200): icmp_seq=5 ttl=64 time=1.47 ms
64 bytes from outside (198.18.133.200): icmp_seq=6 ttl=64 time=1.68 ms
64 bytes from outside (198.18.133.200): icmp_seq=7 ttl=64 time=1.07 ms
64 bytes from outside (198.18.133.200): icmp_seq=8 ttl=64 time=1.48 ms
```

3. FMC の Web インターフェイスに移動して、[デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。ピア切り替えアイコンをクリックして、[はい (Yes) ] をクリックします。

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (2)					
HA_Test High Availability					
NGFW1(Primary, Active) 198.19.10.81 - Routed	FTD for vMware	6.4.0	N/A	Base, Threat (2 more...)	Base_Policy
NGFW3(Secondary, Standby) 198.19.10.83 - Routed	FTD for vMware	6.4.0	N/A	Base, Threat (2 more...)	Base_Policy

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。

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (2)					
HA_Test High Availability					
NGFW1(Primary, Standby) 198.19.10.81 - Routed	FTD for VMWare	6.5.0	N/A	Base, Threat (2 more...)	<a href="#">Base_Policy</a>
NGFW3(Secondary, Active) 198.19.10.83 - Routed	FTD for VMWare	6.5.0	N/A	Base, Threat (2 more...)	<a href="#">Base_Policy</a>

```

root@inside:~
64 bytes from outside (198.18.133.200): icmp_seq=2 ttl=64 time=2.07 ms
64 bytes from outside (198.18.133.200): icmp_seq=3 ttl=64 time=1.41 ms
64 bytes from outside (198.18.133.200): icmp_seq=4 ttl=64 time=1.49 ms
64 bytes from outside (198.18.133.200): icmp_seq=5 ttl=64 time=1.43 ms
64 bytes from outside (198.18.133.200): icmp_seq=6 ttl=64 time=1.59 ms
64 bytes from outside (198.18.133.200): icmp_seq=7 ttl=64 time=1.40 ms
64 bytes from outside (198.18.133.200): icmp_seq=8 ttl=64 time=1.44 ms
64 bytes from outside (198.18.133.200): icmp_seq=9 ttl=64 time=1.43 ms
64 bytes from outside (198.18.133.200): icmp_seq=10 ttl=64 time=1.43 ms
64 bytes from outside (198.18.133.200): icmp_seq=11 ttl=64 time=1.29 ms
64 bytes from outside (198.18.133.200): icmp_seq=12 ttl=64 time=1.41 ms
64 bytes from outside (198.18.133.200): icmp_seq=13 ttl=64 time=2.01 ms
64 bytes from outside (198.18.133.200): icmp_seq=14 ttl=64 time=1.92 ms
64 bytes from outside (198.18.133.200): icmp_seq=15 ttl=64 time=1.28 ms
64 bytes from outside (198.18.133.200): icmp_seq=16 ttl=64 time=1.37 ms
64 bytes from outside (198.18.133.200): icmp_seq=17 ttl=64 time=1.89 ms
64 bytes from outside (198.18.133.200): icmp_seq=18 ttl=64 time=6.46 ms
64 bytes from outside (198.18.133.200): icmp_seq=30 ttl=64 time=1.55 ms
64 bytes from outside (198.18.133.200): icmp_seq=31 ttl=64 time=1.40 ms
64 bytes from outside (198.18.133.200): icmp_seq=32 ttl=64 time=1.21 ms
64 bytes from outside (198.18.133.200): icmp_seq=33 ttl=64 time=1.73 ms
64 bytes from outside (198.18.133.200): icmp_seq=34 ttl=64 time=1.30 ms
64 bytes from outside (198.18.133.200): icmp_seq=35 ttl=64 time=1.23 ms

```

## 5. スイッチバックします。

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (2)					
HA_Test High Availability					
⚠ NGFW1(Primary, Active) 198.19.10.81 - Routed	FTD for VMWare	6.5.0	N/A	Base, Threat (2 more...)	<a href="#">Base_Policy</a>
🟢 NGFW3(Secondary, Standby) 198.19.10.83 - Routed	FTD for VMWare	6.5.0	N/A	Base, Threat (2 more...)	<a href="#">Base_Policy</a>

**注** : NGFW1 が再度プライマリになるように切り替えます。警告サインが表示される場合があります。これは数分だけの一時的なものです。

## 付録 A : FMC の事前設定

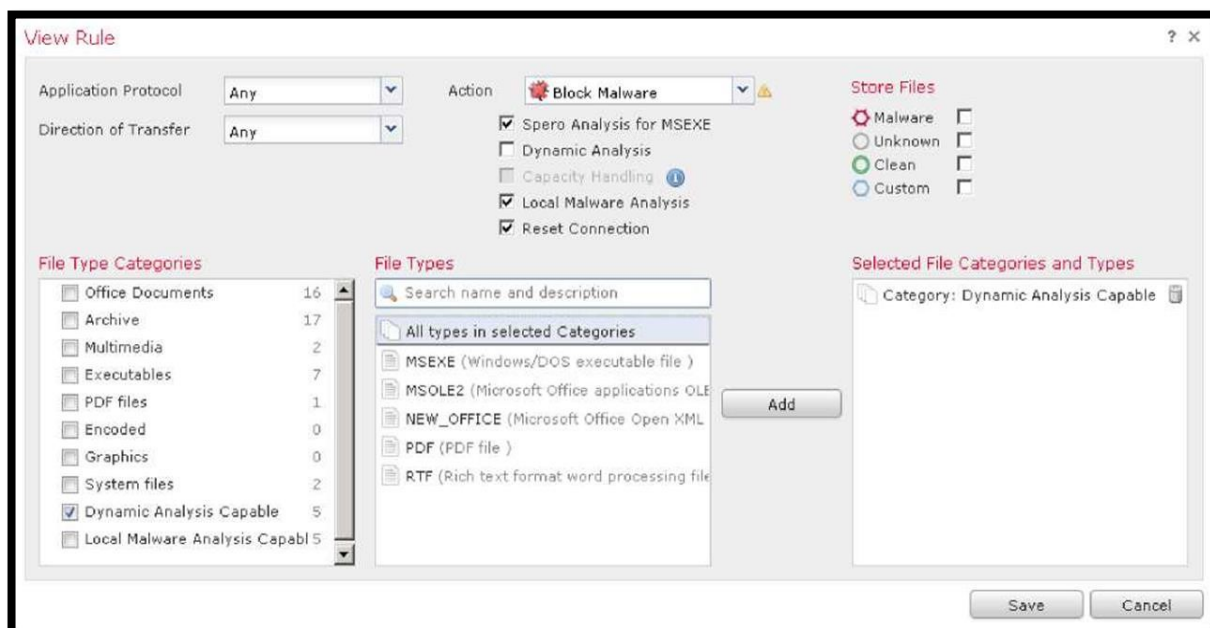
ラボ演習を迅速化するため、初期インストール後に FMC でいくつかの設定手順が事前実行されています。この付録では、実行された設定手順について説明します。

- 設定 A1,2 : 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 : resetapiuser の追加
- 設定 A1,7 : サーバ証明書のインストール

## 手順

### 設定 A1,2 : 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。  
注 : このカテゴリには、複数のファイルタイプが属しています。[追加 (Add) ] をクリックします。
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ないことに注意してください。
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。

**Add File Rule**

Application Protocol → Any

Direction of Transfer → Any

Action:  Block Files

Store files

Reset Connection

**File Type Categories**

IT-Office Documents	20
[r]-Archive	18
[H]-Multimedia	30
O-Executables	1
[p]-PDF files	21
[r]-Encoded Graphics	2
[g]-System files	12
[d]-Dynamic Analysis Capable	4
[l]-Local Malware Analysis Capable	5

**File Types**

RIFF (Resource Interchange File Formats)

BEX (BEX audio format)

**Selected File Categories and Types**

RIFF (Resource Interchange File Formats)

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 - ファイルをブロック
- 2 - マルウェアをブロック
- 3 - マルウェアのクラウド ルックアップ
- 4 - ファイルを検出
- 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。

**General**

First Time File Analysis

Enable Custom Detection List

Enable Clean List

Mark files as malware based on dynamic analysis threat score  Very High

**Archive File Inspection**

Inspect Archives

Block Encrypted Archives

Block Uninspectable Archives

Max Archive Depth 2 → Enter a value between 1 and 3

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 デスクトップの **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 [ドロップしてイベントを生成 (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 [ドロップしてイベントを生成 (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 トラフィック内で、root ホームディレクトリに対する変更を探します。外部ネットワークからのトラフィックのみを調査しますが、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 トラフィックを調査したり、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したりすることは、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

- [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。
  - [CA のインポート (Import CA)] をクリックします。
  - [名前 (Name)] に Verifraud と入力します。
  - [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。
  - Jump デスクトップの **Certificates** フォルダに移動します。
  - Verifraud\_CA.cer を**アップロード**します。
  - [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。
  - Verifraud\_CA.key を**アップロード**します。
  - [保存 (Save)] をクリックします。
- 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 デバイスを除外します。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。
  - [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。
  - [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] を**クリック**します。
  - [名前 (Name)] に Infrastructure と入力します。
  - [ネットワーク (Network)] に 198.19.10.80-198.19.10.130 と入力します。
  - [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自己署名証明書に対する信頼欠如状態が保持されます。

#### 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存在しています。ラボにクラウドの接続性の問題が発生する場合があります。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がトリガーされるようにしています。

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、**Custom-Detection-List** 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 デスクトップの [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 を追加する

API Explorer を使用する際、別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 デスクトップの **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。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。
  - g. `cd /etc/ssl` と入力後、`cp server* /root` と入力します。
  - h. `cat > /etc/ssl/server.crt` と入力します。
  - i. Jump デスクトップの **Certificates** フォルダで、Notepad++ を使用して **fmc.cer** ファイルを編集します。
  - j. すべてを選択し、コピーして FMC CLI に貼り付けます。
  - k. **Ctrl+D** を押します。
  - l. `cat > /etc/ssl/server.key` と入力します。
  - m. Jump デスクトップの **Certificates** フォルダで、Notepad++ を使用して **fmc.key** ファイルを編集します。
  - n. すべてを選択し、コピーして FMC CLI に貼り付けます。
  - o. **Ctrl+D** を押します。
  - p. `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 ocured
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 ocured
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 ocured
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 ocured 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 のブックマークツールバーには ISE のリンクがあります。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。

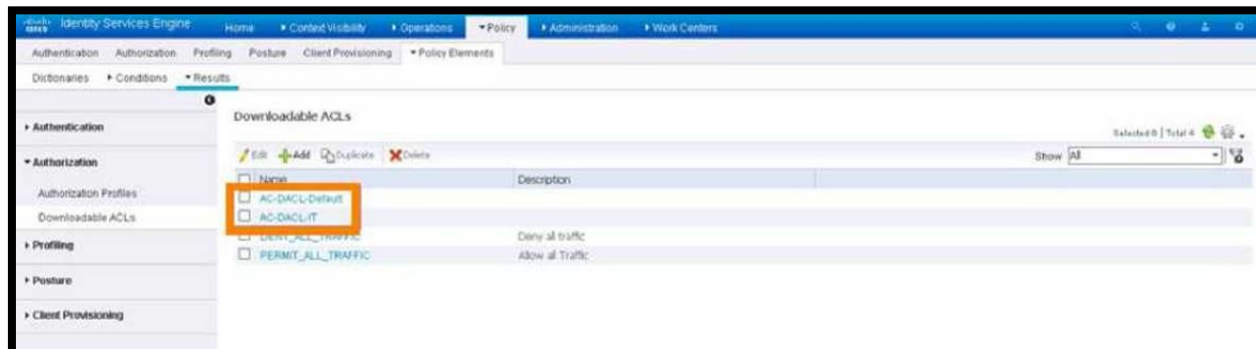
### 認可プロファイル

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** にドリルダウンすると、以下に説明する **DAACL AC-DAACL-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 **DAACL AC-DAACL-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。

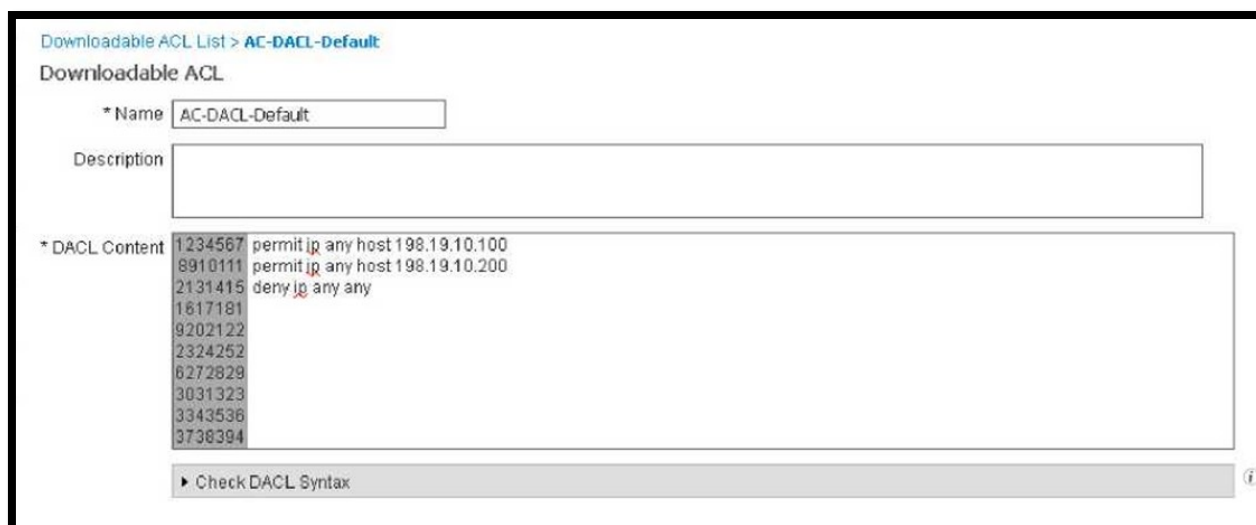


## ダウンロード可能 ACL

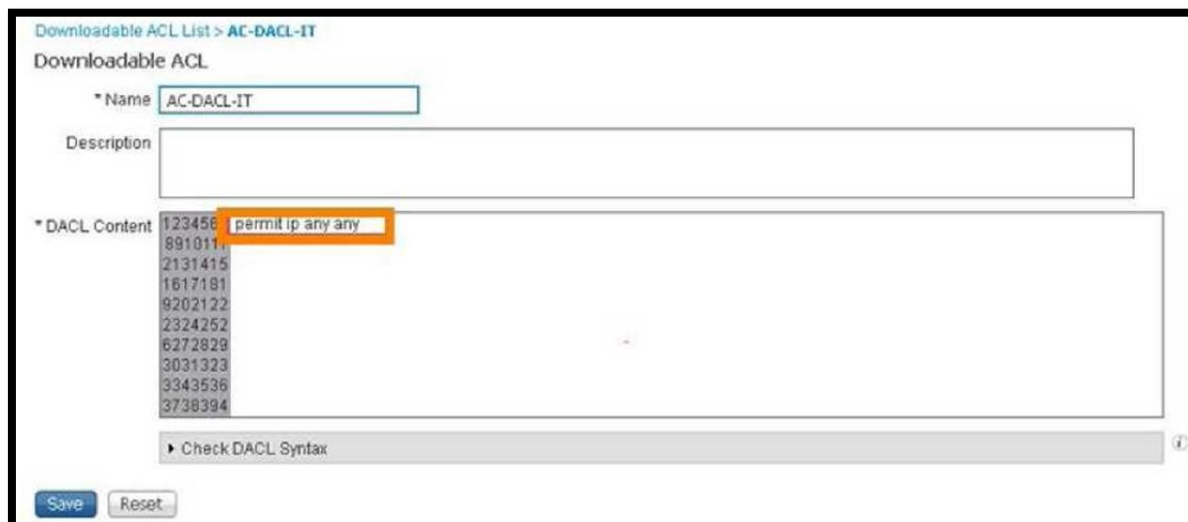
1. [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [認可 (Authorization)] > [ダウンロード可能 ACL (Downloadable ACLs)] に移動します。最初の 2 つの DACL、**AC-DACL-Default** と AC-DACL-IT は、このラボ用に作成されたものです。



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。



©2020 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2020年4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