# インターネットへの AnyConnect VPN Client のトラフィックをフィルタ処理するための FirePOWER サービス アクセス コントロール ルールを使用した ASA の設定

## 目次



## 概要

このドキュメントでは、バーチャル プライベート ネットワーク（VPN）トンネルまたはリモート アクセス（RA）ユーザからのトラフィックを検査し、FirePOWER サービスで Cisco 適応型セキュリティ アプライアンス（ASA）をインターネット ゲートウェイとして使用するようにアクセス コントロール ポリシー（ACP）ルールを設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識が推奨されます。

- AnyConnect、リモート アクセス VPN やピアツーピア IPsec VPN。
- FirePOWER ACP の設定。
- ASA モジュラ ポリシー フレームワーク（MPF）。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ASDM の例で ASA5506W バージョン 9.6(2.7)
- ASDM の例で FirePOWER モジュール バージョン 6.1.0-330。
- FMC の例で ASA5506W バージョン 9.7(1)。
- FMC の例で FirePOWER versoin 6.2.0。

- Firepower Management Center（FMC）バージョン 6.2.0

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

# 問題

FirePOWER サービスを使う ASA5500-X では、境界コンテンツ セキュリティのシングルポイントを使用する IPSec トンネルによって接続されている他の場所が送信元のトラフィックと同じようには AnyConnect のユーザ トラフィックのフィルタリングや検査を行うことはできません。

この解決策で対処できるもう 1 つの症状は、他のソースに影響することなく上記のソースへの特定の ACP ルールを定義できないというものです。

このシナリオは、ASA で終端する VPN ソリューションに使われている TunnelAll の設計の場合に非常によく起こります。

# 解決策

これは複数の方法で達成できます。 ただしこのシナリオでは、ゾーンによる検査について述べます。

## ASA の設定

ステップ 1： AnyConnect ユーザまたは VPN トンネルが ASA に接続するインターフェイスを特定します。

ピアツーピア トンネル

これは **show run crypto map** コマンドの出力のスクラップです。

```
crypto map outside_map interface outside
```

AnyConnect ユーザ

**show run webvpn** のコマンドは AnyConnect アクセスが有効になっている場所を表示します。

```
webvpn
 enable outside
 hostscan image disk0:/hostscan_4.3.05019-k9.pkg
 hostscan enable
 anyconnect image disk0:/anyconnect-win-4.4.01054-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnect-macos-4.4.01054-webdeploy-k9.pkg 2
 anyconnect enable
```

このシナリオでは、**outside** のインターフェイスは RA ユーザとピアツーピア トンネルの両方を受け取ります。

ステップ 2： ASA からのトラフィックをグローバル ポリシーの FirePOWER モジュールにリダ

イレクトします。

これは **match any** の条件を使うか、あるいはトラフィックのリダイレクション用のアクセス コントロール リスト（ACL）で定義できます。

以下は **match any** のマッチングの例です。

```
webvpn
 enable outside
 hostscan image disk0:/hostscan_4.3.05019-k9.pkg
 hostscan enable
 anyconnect image disk0:/anyconnect-win-4.4.01054-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnect-macos-4.4.01054-webdeploy-k9.pkg 2
 anyconnect enable
```

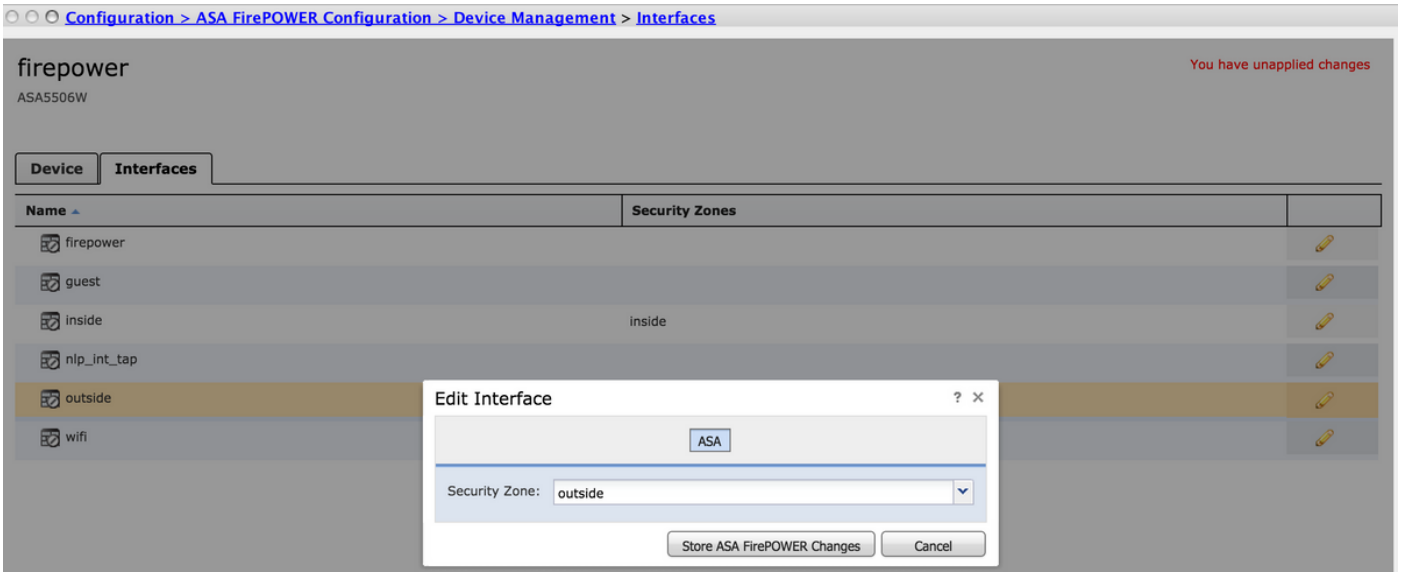
ACL マッチングの例。

```
webvpn
 enable outside
 hostscan image disk0:/hostscan_4.3.05019-k9.pkg
 hostscan enable
 anyconnect image disk0:/anyconnect-win-4.4.01054-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnect-macos-4.4.01054-webdeploy-k9.pkg 2
 anyconnect enable
```

上記より一般的ではないシナリオですが、サービス ポリシーは外部インターフェイスにも使用できます。 この例については、このドキュメントでは説明していません。

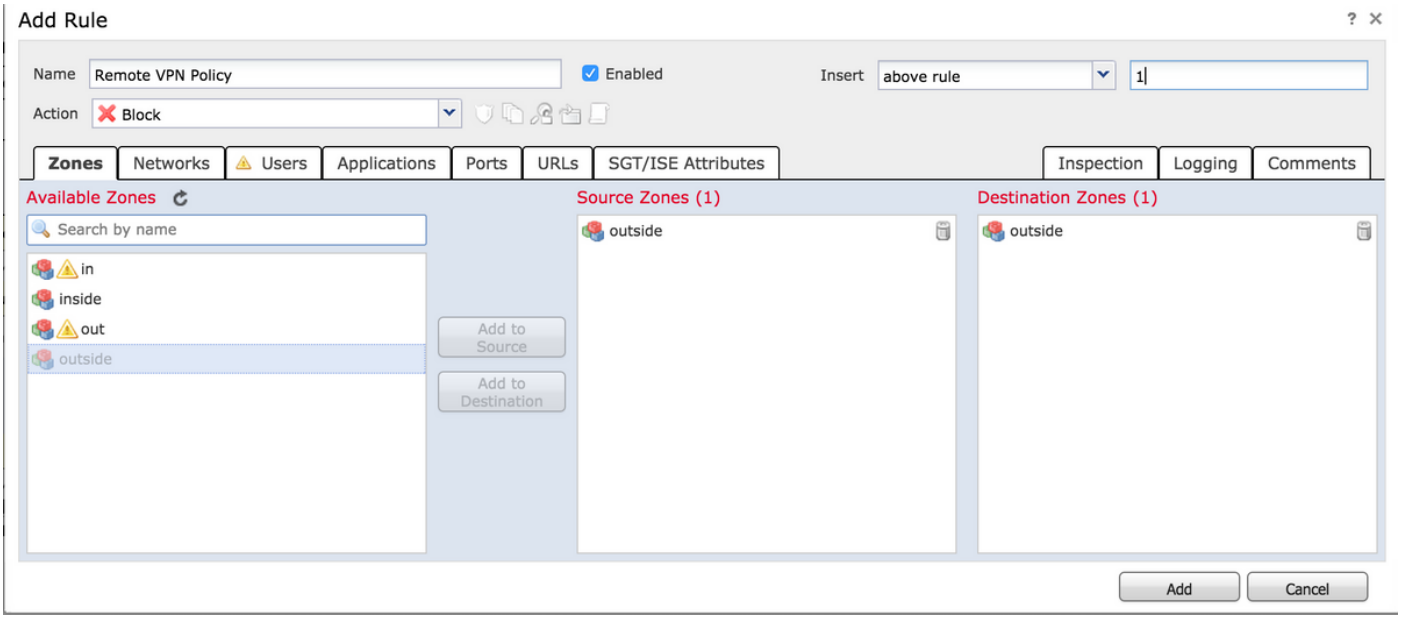
## ASDM の設定で管理する ASA FirePOWER モジュール

ステップ 1：[Configuration] > [ASA FirePOWER Configuration] > [Device Management] で外部インターフェイスに 1 つのゾーンを割り当てます。 この場合、そのゾーンは、**outside** と呼ばれます。




ステップ 2：[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] で [Add Rule] を選択します。

ステップ 3 [Zones] タブから [outside] のゾーンをルールの送信元と宛先として選択します。




ステップ 4：アクション、タイトルやその他の希望する条件を選択してこのルールを定義します。

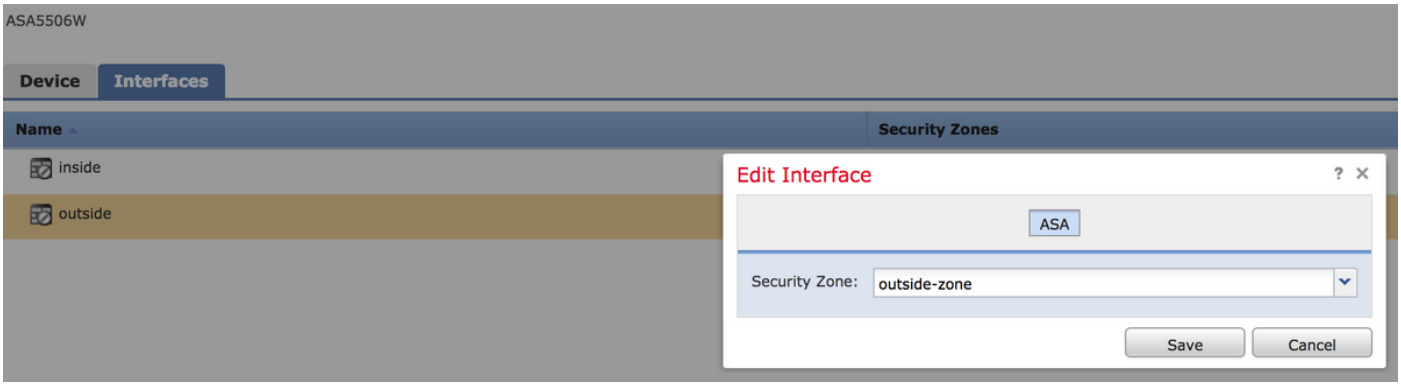
このトラフィック フロー向けに複数のルールを作成することができます。 送信元および宛先ゾーンは VPN の送信元とインターネットに割り当てられたゾーンでなければならない点に注意することが重要です。

これらのルールの前に一致する可能性のある、より一般的なその他のポリシーがないことを確認します。 **any** のゾーンに定義されているルールよりも上位にこれらのルールを置くことが推奨されます。

ステップ 5：[Store ASA FirePOWER Changes] 、次に [Deploy FirePOWER Changes] をクリックしてこれらの変更を適用します。

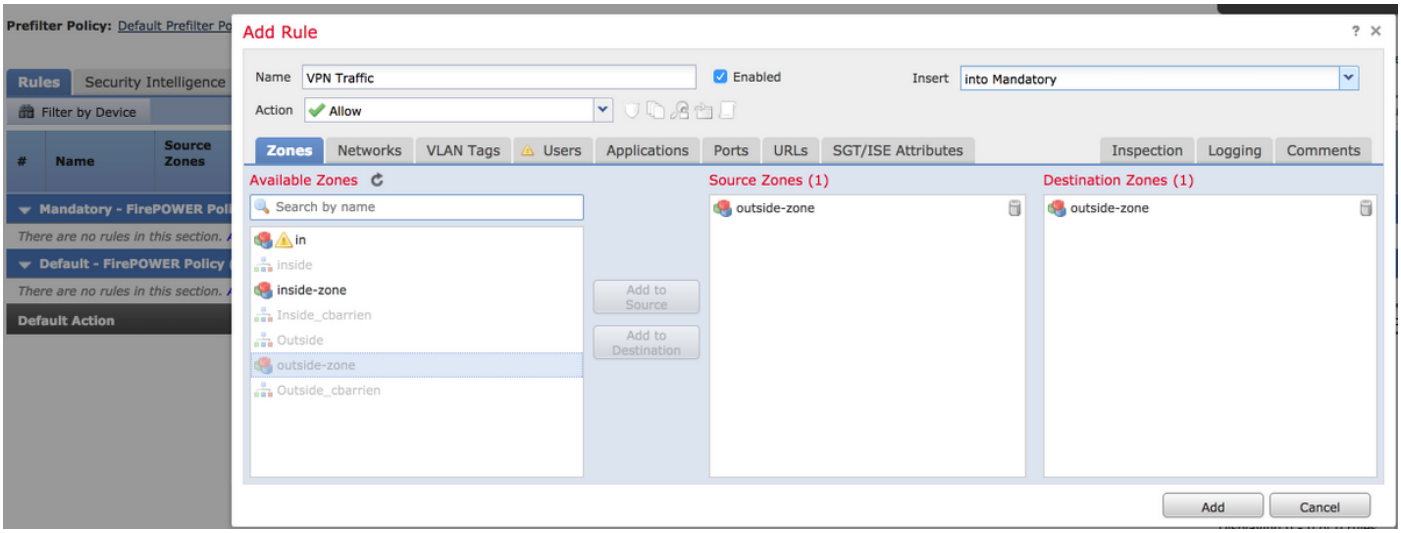
## FMC の設定で管理する ASA FirePOWER モジュール

ステップ 1：[Devices] > [Management] > [Interfaces] で外部インターフェイスに 1 つのゾーンを割り当てます。 この場合、そのゾーンは [outside-zone] という名前です。




ステップ 2：[Policies] > [Access Control] > [Edit] で [Add Rule] を選択します。

ステップ 3 [Zones] タブからルールの送信元と宛先として [outside-zone] のゾーンを選択します。




ステップ 4：アクション、タイトルやその他の希望する条件を選択してこのルールを定義します。

このトラフィック フロー向けに複数のルールを作成することができます。 送信元および宛先ゾーンは VPN の送信元とインターネットに割り当てられたゾーンでなければならない点に注意することが重要です。

これらのルールの前に一致する可能性のある、より一般的なその他のポリシーがないことを確認します。 **any** のゾーンに定義されているルールよりも上位にこれらのルールを置くことが推奨されます。

ステップ 5：[Save] 、次に [Deploy] をクリックしてこれらの変更を適用します。

# 結果

展開が完了すると、AnyConnect トラフィックは適用した ACP ルールによってフィルタリング/検査されるようになります。 この例では、URL は正常にブロックされました。