インターネットに AnyConnect VPN Client トラフィックをフィルタリングする FirePOWER サービス アクセスコントロール ルールの設定 ASA

目次

概要

この資料にトラフィックを検査する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をバーチャル 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）ユーザから来る記述されていますおよび FirePOWER サービスとインターネット ゲートウェイとして a を（ASA） Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア使用します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AnyConnect、リモートアクセス VPN や Peer-to-Peer IPSec VPN。
- Firepower ACP 設定。
- ASA モジュラ 政策の枠組（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 例のための ASA5506W バージョン 9.6(2.7)
- ASDM 例のための FirePOWER モジュール バージョン 6.1.0-330。
- FMC 例のための ASA5506W バージョン 9.7(1)。
- FMC 例のための FirePOWER versoin 6.2.0。

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

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

問題

FirePOWER サービスを用いる ASA5500-X は permietral コンテンツ セキュリティの一点を使用する IPSecトンネルによって接続される他の場所によってソースをたどられるトラフィックと同じとして AnyConnect ユーザ トラフィックをフィルタリングしておよび/または検査することができません。

このソリューションが力バーするもう一つの現象は他のソース見せかけなしで述べられたソースに特定の ACP ルールを定義することができないことです。

このシナリオは TunnelAll 設計が ASA で終わる VPN ソリューションのために使用されるとき見るために非常によくあります。

解決策

これを複数の方法を通して達成することができます。 ただし、このシナリオはゾーンによってインスペクションをカバーします。

ASA の設定

ステップ 1. AnyConnect ユーザか VPN トンネルが ASA に接続するインターフェイスを識別して下さい。

ピアツーピア トンネル

これは **show run クリプト マップ**出力のスクラップです。

```
crypto map outside_map interface outside
```

AnyConnect ユーザ

コマンド **show run webvpn は** AnyConnect アクセスがどこに有効に なるか示します。

```
webvpn
 enableoutside 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、インターフェイス**外部は**、両方、RA ユーザおよびピアツーピア トンネル受け取ります。

ステップ 2. ASA からグローバル な ポリシーの FirePOWER モジュールにトラフィックをリダイレクトして下さい。

それはトラフィック リダイレクションのための**あらゆる**条件か定義された Access Control List（ACL）**一致する**とすることができます。

例はとの一致を**一致する。**

```
class-map SFR
 match any

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

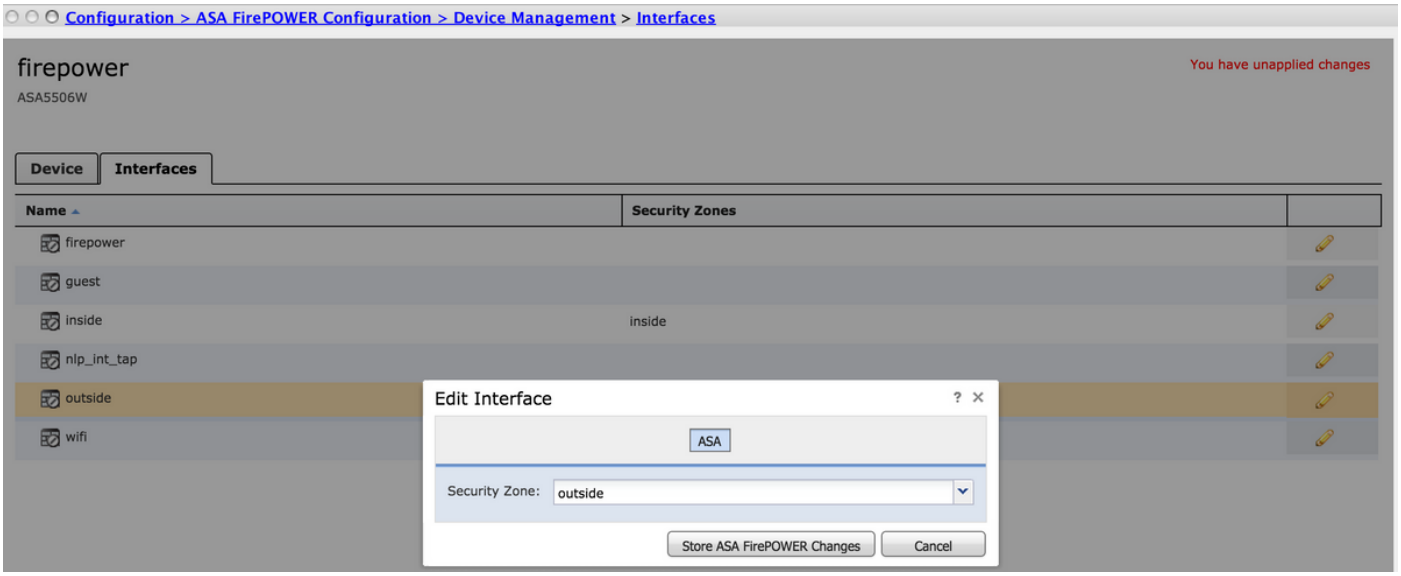
ACL 一致との例。

```
access-list sfr-acl extended permit ip any any

class-map SFR
 match access-list sfr-acl

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

より少ない一般的 な シナリオでは、サービス ポリシーは outside インターフェイスに使用することができます。 この例はこの資料でカバーされません。

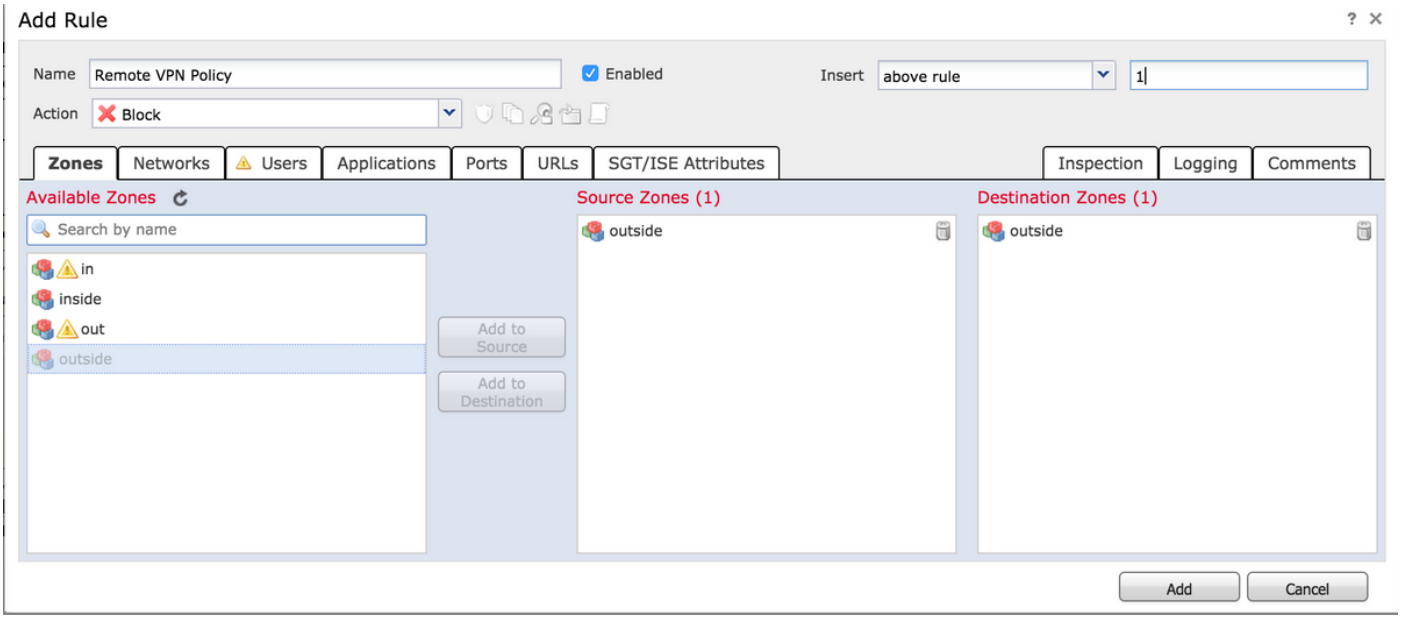
ASDM 設定によって管理される ASA FirePOWER モジュール

ステップ 1.**設定 > ASA FirePOWER 設定 > デバイス管理**で outside インターフェイスに 1 つのゾーンを割り当てて下さい。 この場合、そのゾーンは**外部で**呼出されます。



ステップ 2.**設定 > ASA FirePOWER 設定 > ポリシー > アクセスコントロール ポリシー**で『Add rule』 を選択 して下さい。

ステップ 3 **ゾーン**からルールのための**送信元および宛先としてゾーンを記録して下さい、『outside』 を選択 して下さい。**



ステップ 4.このルールを定義する操作、タイトルおよび他のどの望ましい状態も選択して下さい。

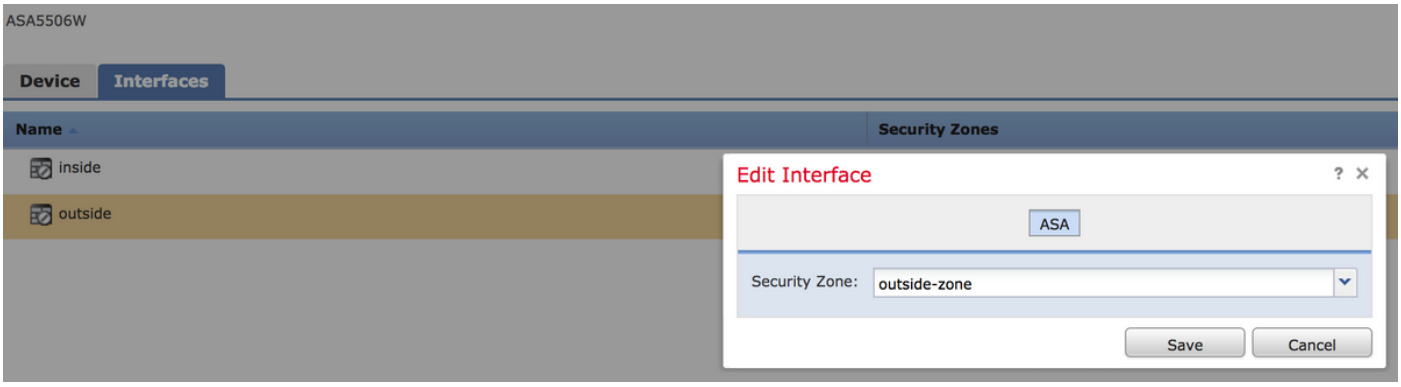
複数のルールはこのトラフィックフローのために作成することができます。 送信元および宛先 ゾーンが VPN ソースおよびインターネットに割り当てられるゾーンである必要があることに留意することはちょうど重要です。

これらのルールの前に一致する可能性がある他のより多くの総合 政策がないことを確かめて下さい。 それは preferrable **あらゆる**ゾーンに定義される物の上のこれらのルールがあるためにです。

ステップ 5.**ストア ASA FirePOWER 変更を**クリックし、次にこれらの変更を実施されてもらうように **FirePOWER 変更を展開して下さい。**

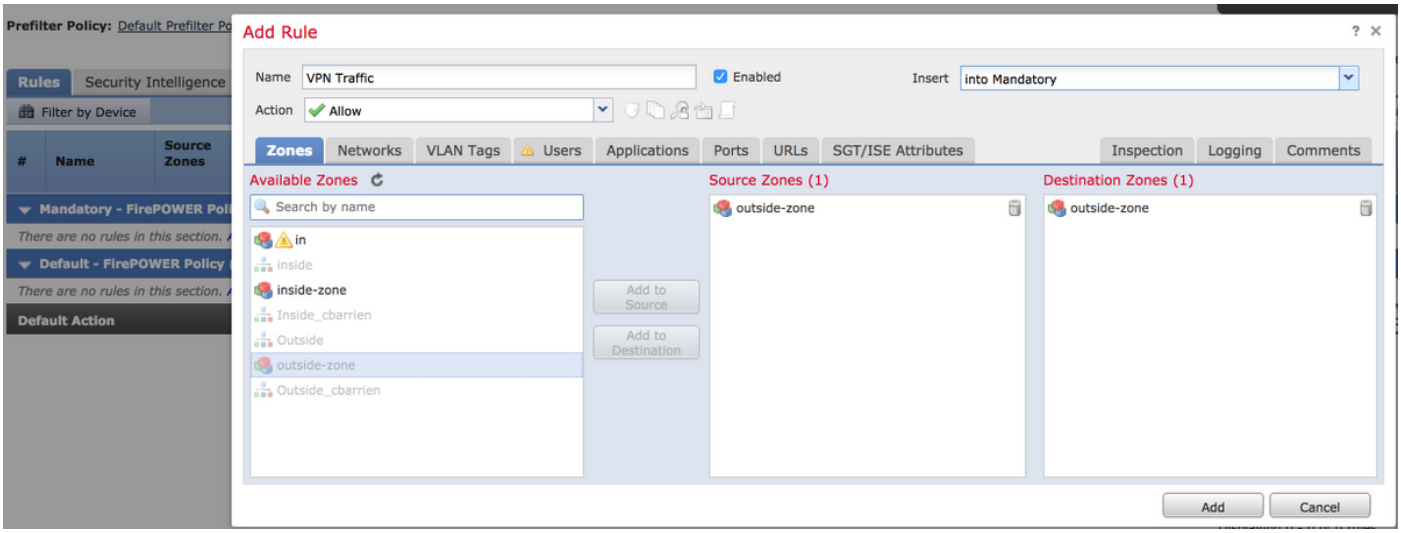
FMC 設定によって管理される ASA FirePOWER モジュール

ステップ 1.**デバイス > 管理 > インターフェイス**で outside インターフェイスに 1 つのゾーンを割り当てて下さい。 この場合、そのゾーンは外部**ゾーンと**呼ばれます。



ステップ 2.**ポリシー > アクセスコントロール > Edit** で『Add rule』 を選択 して下さい。

ステップ 3 **ゾーン**からルールに送信元および宛先として外部**ゾーン** ゾーンを記録して下さい、選択して下さい。



ステップ 4.このルールを定義する操作、タイトルおよび他のどの望ましい状態も選択して下さい。

複数のルールはこのトラフィックフローのために作成することができます。 送信元および宛先 ゾーンが VPN ソースおよびインターネットに割り当てられるゾーンである必要があることに留意することはちょうど重要です。

これらのルールの前に一致する可能性がある他のより多くの総合 政策がないことを確かめて下さい。 それは preferrable **あらゆる**ゾーンに定義される物の上のこれらのルールがあるためにです。

ステップ 5. 『SAVE』 をクリック し、これらの変更を実施されてもらうために次に**展開して下さい**。

結果

配備完了の後で、AnyConnect トラフィックは適用される ACP ルールによって今フィルタリングされましたり/検査されます。 この例では、URL は正常にブロックされました。