Konfigurieren von Zugriffskontrollregeln für ASA mit FirePOWER-Services zum Filtern des AnyConnect VPN-Client-Datenverkehrs zum Internet

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie Zugriffskontrollrichtlinien (ACP, Access Control Policy)-Regeln konfigurieren, um Datenverkehr zu überprüfen, der von VPN-Tunneln (Virtual Private Network) oder Remote Access (RA)-Benutzern stammt, und eine Cisco Adaptive Security Appliance (ASA) mit FirePOWER-Services als Internet-Gateway zu verwenden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- AnyConnect, Remote Access VPN und/oder Peer-to-Peer IPSec VPN.
- FirePOWER-AKP-Konfiguration.
- ASA Modular Policy Framework (MPF)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA5506W Version 9.6(2.7) für ASDM - Beispiel
- FirePOWER-Modul, Version 6.1.0-330, für ASDM-Beispiel.
- ASA5506W Version 9.7(1) für FMC-Beispiel.

- FirePOWER-Version 6.2.0 für FMC-Beispiel.
- FirePOWER Management Center (FMC) Version 6.2.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Die ASA5500-X mit FirePOWER Services kann den AnyConnect-Benutzerdatenverkehr nicht filtern und/oder inspizieren, der dem von anderen Standorten stammenden Datenverkehr entspricht, die über IPSec-Tunnel verbunden sind, die einen zentralen Punkt für die Sicherheit von Inhalten verwenden.

Ein weiteres Symptom dieser Lösung besteht darin, dass es nicht möglich ist, spezifische AKP-Regeln für die genannten Quellen festzulegen, ohne dass andere Quellen davon betroffen sind.

Dieses Szenario ist sehr häufig zu beobachten, wenn TunnelAll-Design für VPN-Lösungen verwendet wird, die auf einer ASA terminiert werden.

Lösung

Dies kann auf verschiedene Weise erreicht werden. Dieses Szenario umfasst jedoch die Inspektion nach Zonen.

ASA-Konfiguration

Schritt 1: Identifizieren Sie die Schnittstellen, an denen AnyConnect-Benutzer oder VPN-Tunnel mit der ASA verbunden sind.

Peer-to-Peer-Tunnel

Dies ist ein Schrott der Ausgabe von **show run crypto map**.

```
crypto map outside_map interface outside
```

AnyConnect-Benutzer

Der Befehl **show run webvpn** zeigt an, wo der AnyConnect-Zugriff aktiviert ist.

```
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
```

In diesem Szenario empfängt die Schnittstelle **außerhalb** sowohl RA-Benutzer als auch Peer-to-Peer-Tunnel.

Schritt 2: Umleitung des Datenverkehrs von ASA zum FirePOWER-Modul mit einer globalen Richtlinie.

Dies kann entweder mit einer **Übereinstimmung mit einer beliebigen** Bedingung oder mit einer definierten Zugriffskontrollliste (ACL) für die Datenumleitung erfolgen.

Beispiel mit **jeder** Übereinstimmung.

```
class-map SFR
 match any

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

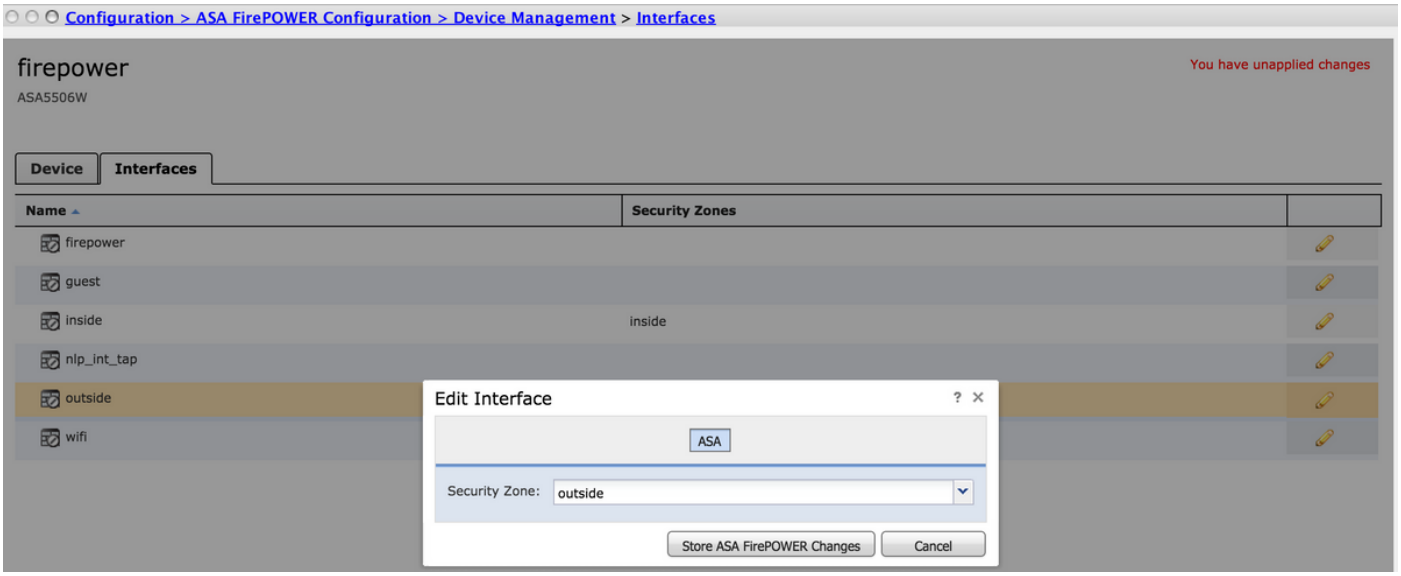
Beispiel mit ACL-Übereinstimmung.

```
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
```

In einem selteneren Szenario kann eine Dienstrichtlinie für die externe Schnittstelle verwendet werden. Dieses Beispiel wird in diesem Dokument nicht behandelt.

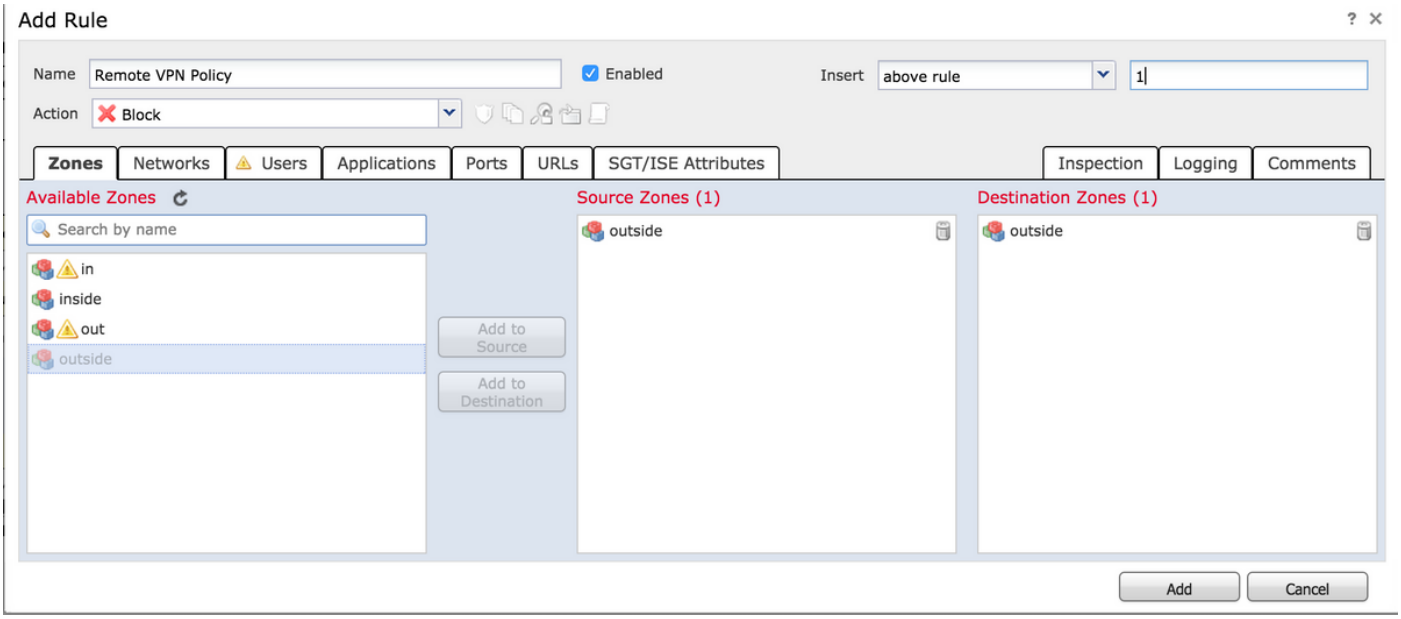
ASA FirePOWER-Modul wird durch ASDM-Konfiguration verwaltet

Schritt 1: Weisen Sie der externen Schnittstelle eine Zone unter **Configuration > ASA FirePOWER Configuration > Device Management zu**. In diesem Fall wird diese Zone **außerhalb** genannt.



Schritt 2: Wählen Sie **Regel** bei **Konfiguration hinzufügen > ASA FirePOWER-Konfiguration > Richtlinien > Zugriffskontrollrichtlinie aus**.

Schritt 3: Wählen Sie auf der Registerkarte **Zonen** als Quelle und Ziel für Ihre Regel die **externe** Zone aus.



Schritt 4: Wählen Sie die Aktion, den Titel und alle anderen gewünschten Bedingungen aus, um diese Regel zu definieren.

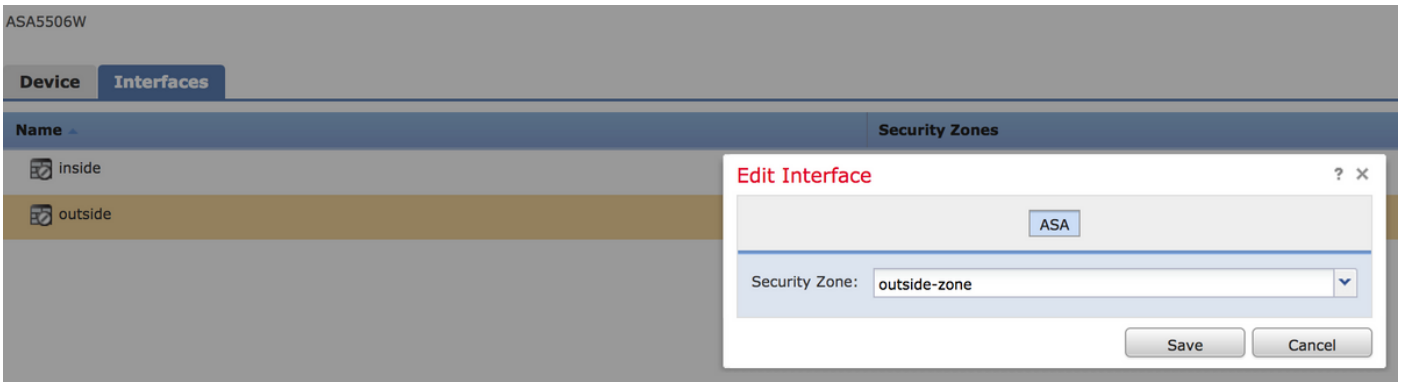
Für diesen Datenverkehrsfluss können mehrere Regeln erstellt werden. Dabei ist zu beachten, dass Quell- und Zielzonen die Zone sein müssen, die VPN-Quellen und dem Internet zugewiesen ist.

Stellen Sie sicher, dass es vor diesen Regeln keine weiteren allgemeinen Richtlinien gibt, die übereinstimmen könnten. Es ist vorzuziehen, dass diese Regeln über die Regeln für **jede** Zone hinausgehen.

Schritt 5: Klicken Sie auf **Store ASA FirePOWER Changes** und dann **Deploy FirePOWER Changes** um diese Änderungen wirksam zu machen.

ASA FirePOWER-Modul wird durch FMC-Konfiguration verwaltet

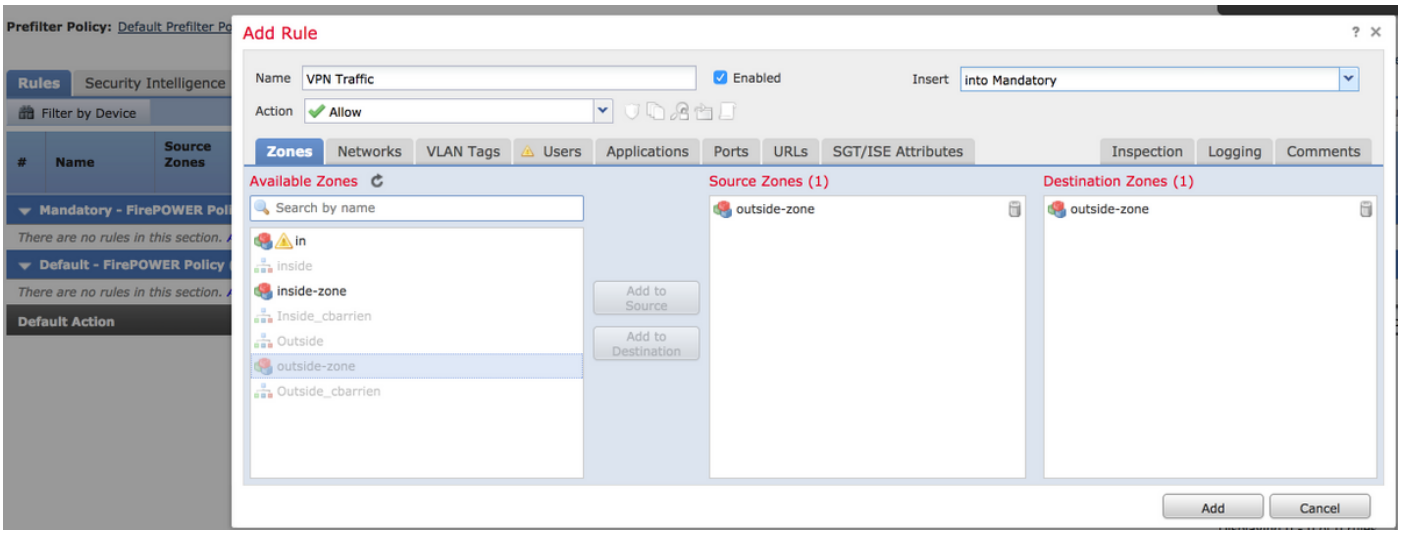
Schritt 1: Zuweisung einer Zone für die externe Schnittstelle an **Geräten > Management > Schnittstellen**. In diesem Fall wird diese Zone als **außerhalb**.



Schritt 2: Wählen Sie **Regel hinzufügen** unter **Richtlinien > Zugriffskontrolle > Bearbeiten aus**.

Schritt 3: Wählen Sie auf der Registerkarte **Zonen** als Quelle und Ziel für Ihre Regel die Zone

außerhalb der Zone aus.



Schritt 4: Wählen Sie die Aktion, den Titel und alle anderen gewünschten Bedingungen aus, um diese Regel zu definieren.

Für diesen Datenverkehrsfluss können mehrere Regeln erstellt werden. Dabei ist zu beachten, dass Quell- und Zielzonen die Zone sein müssen, die VPN-Quellen und dem Internet zugewiesen ist.

Stellen Sie sicher, dass es vor diesen Regeln keine weiteren allgemeinen Richtlinien gibt, die übereinstimmen könnten. Es ist vorzuziehen, dass diese Regeln über die Regeln für **jede** Zone hinausgehen.

Schritt 5: Klicken Sie auf **Speichern** und dann auf **Bereitstellen**, damit diese Änderungen wirksam werden.

Ergebnis

Nach Abschluss der Bereitstellung wird der AnyConnect-Datenverkehr nun anhand der angewendeten AKP-Regeln gefiltert/überprüft. In diesem Beispiel wurde eine URL erfolgreich blockiert.

Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.