Configurazione di ASA con regole di controllo di accesso dei servizi FirePOWER per filtrare il traffico dei client VPN per Internet

Sommario

Introduzione

In questo documento viene descritto come configurare le regole dei criteri di controllo dell'accesso (ACP) per ispezionare il traffico proveniente dai tunnel VPN (Virtual Private Network) o dagli utenti di Accesso remoto (RA) e utilizzare un'appliance Cisco Adaptive Security (ASA) con i servizi FirePOWER come gateway Internet.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- AnyConnect, VPN ad accesso remoto e/o VPN IPSec peer-to-peer.
- Configurazione ACP Firepower.
- ASA Modular Policy Framework (MPF).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA5506W versione 9.6(2.7) per esempio ASDM
- Modulo FirePOWER versione 6.1.0-330, ad esempio ASDM.
- ASA5506W versione 9.7(1), ad esempio FMC.
- FirePOWER versione 6.2.0 per FMC.
- Firepower Management Center (FMC) versione 6.2.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

ASA5500-X con servizi FirePOWER non è in grado di filtrare e/o ispezionare il traffico degli utenti AnyConnect come quello proveniente da altre postazioni connesse da tunnel IPSec che usano un singolo punto di sicurezza del contenuto permanente.

Un altro sintomo di questa soluzione è l'impossibilità di definire norme ACP specifiche per le fonti menzionate senza influire su altre fonti.

Questo scenario è molto comune e permette di verificare quando il design TunnelAll viene usato per le soluzioni VPN terminate su un'ASA.

Soluzione

Questo obiettivo può essere raggiunto in diversi modi. Tuttavia, questo scenario prevede ispezioni per zone.

Configurazione ASA

Passaggio 1. Identificare le interfacce su cui gli utenti AnyConnect o i tunnel VPN si connettono all'ASA.

Tunnel peer-to-peer

Questo è un ritaglio dell'output della **mappa crittografica show run**.

```
crypto map outside_map interface outside
```

Utenti AnyConnect

Il comando **show run webvpn** mostra dove è abilitato l'accesso AnyConnect.

```
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 questo scenario, l'interfaccia **esterna** riceve sia gli utenti RA che i tunnel peer-to-peer.

Passaggio 2. Reindirizzare il traffico dall'ASA al modulo FirePOWER con una policy globale.

La ricerca può essere effettuata **rispettando** una condizione o usando un Access Control List

(ACL) definito per il reindirizzamento del traffico.

Esempio con **corrispondenza qualsiasi** corrispondenza.

```
class-map SFR
 match any

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

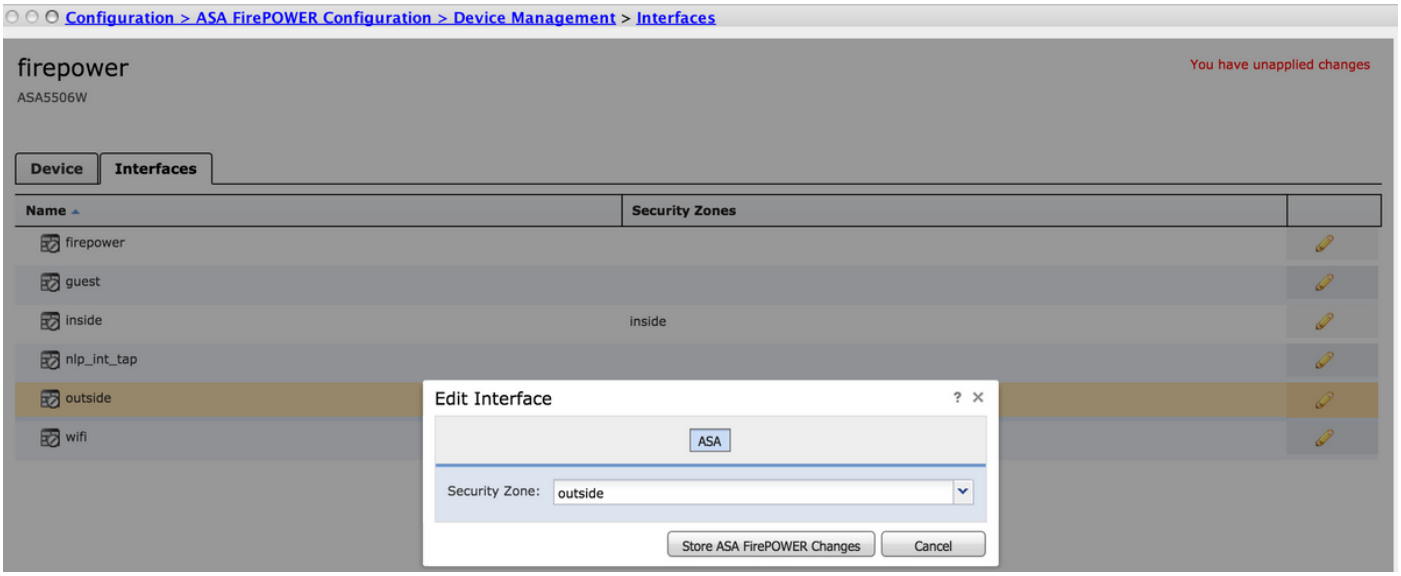
Esempio di corrispondenza ACL.

```
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 uno scenario meno comune, è possibile utilizzare un criterio di servizio per l'interfaccia esterna. L'esempio non è trattato nel presente documento.

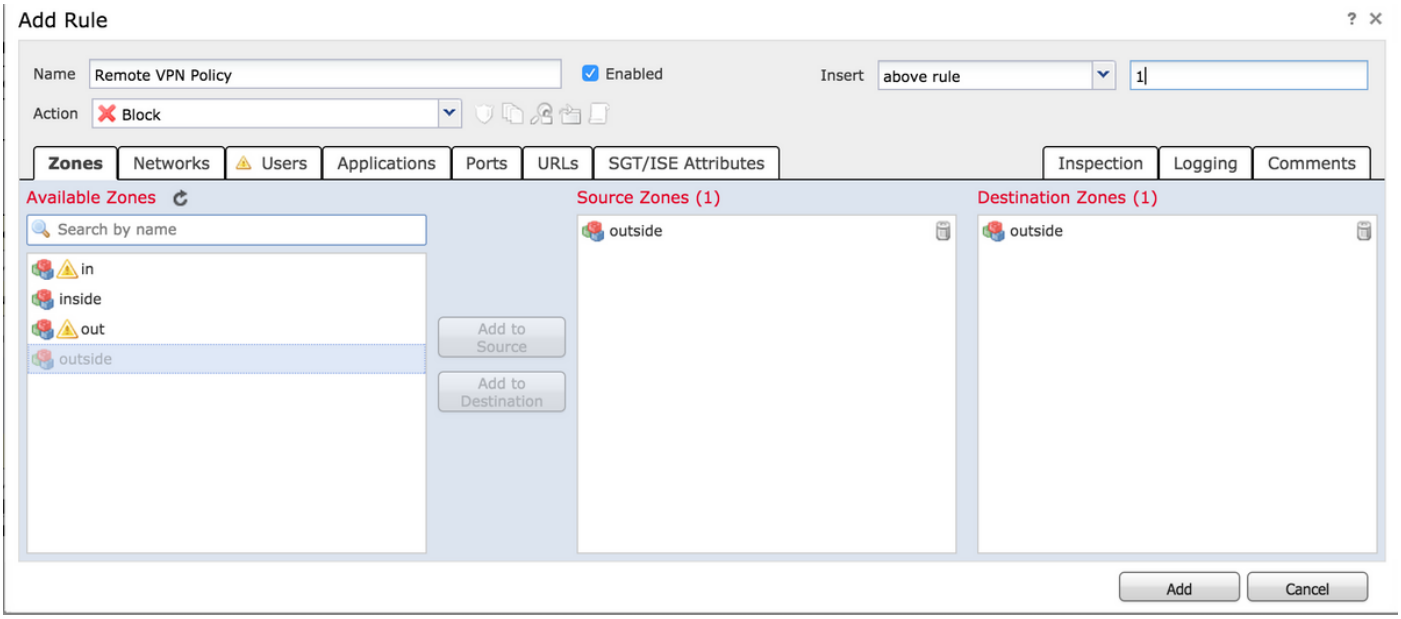
Modulo ASA FirePOWER gestito dalla configurazione ASDM

Passaggio 1. Assegnare l'interfaccia esterna a una zona in **Configuration > ASA FirePOWER Configuration > Device Management**. In questo caso, la zona è denominata **esterna**.



Passaggio 2. Selezionare **Add Rule** at **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy** (Aggiungi regola in fase di configurazione > Configurazione FirePOWER ASA > Criteri > Criteri di controllo di accesso).

Passaggio 3. Dalla scheda **Zone**, selezionare **area esterna** come origine e destinazione per la regola.



Passaggio 4. Selezionare l'azione, il titolo e qualsiasi altra condizione desiderata per definire questa regola.

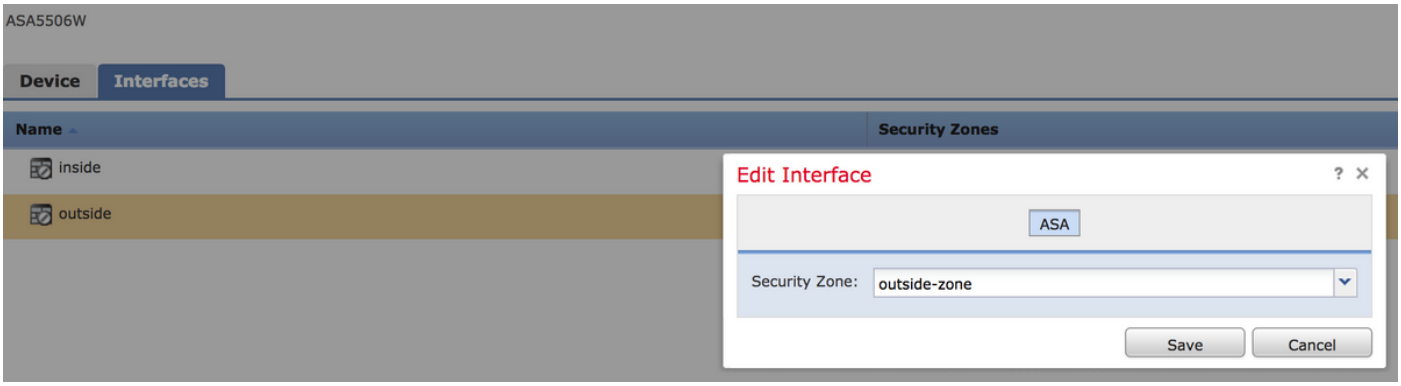
Èpossibile creare più regole per questo flusso di traffico. È importante ricordare che le zone di origine e di destinazione devono essere le zone assegnate alle origini VPN e a Internet.

Verificare che non vi siano altri criteri generali che potrebbero corrispondere prima di queste regole. È preferibile che queste regole siano più severe di quelle definite per **qualsiasi** zona.

Passaggio 5. Per rendere effettive le modifiche, fare clic su **Store ASA FirePOWER Changes** e quindi su **Deploy FirePOWER Changes**.

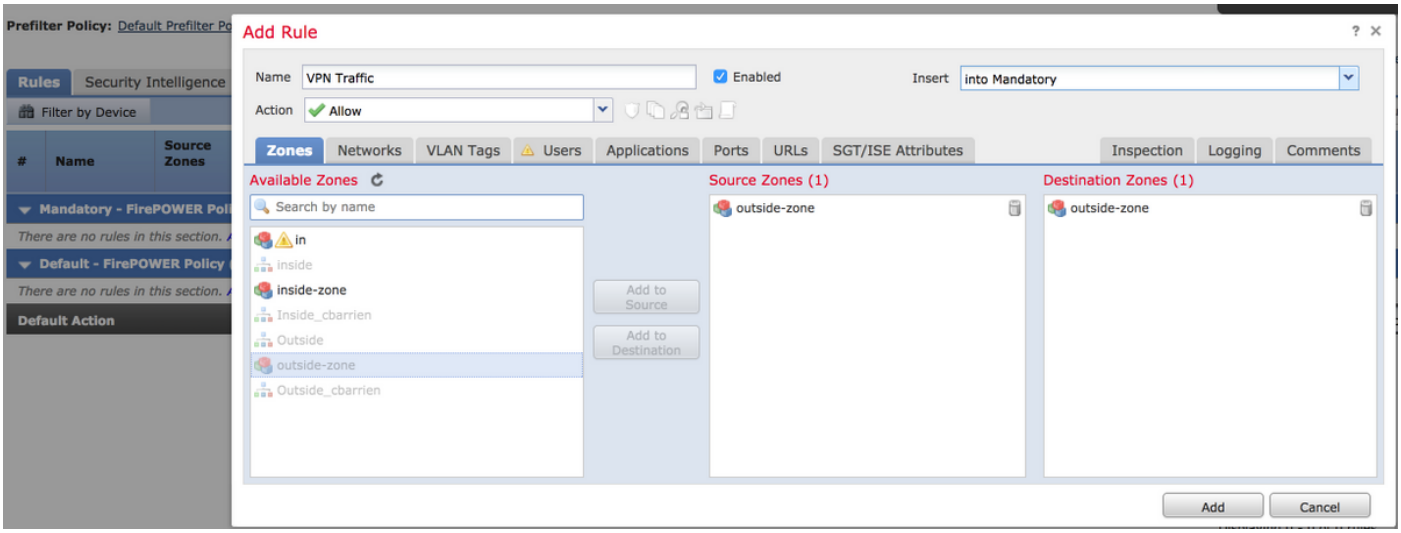
Modulo ASA FirePOWER gestito dalla configurazione FMC

Passaggio 1. Assegnare l'interfaccia esterna a una zona in **Devices > Gestione > Interfacce**. In questo caso, la zona è denominata **zona esterna**.



Passaggio 2. Selezionare **Add Rule** in **Policies > Access Control > Edit**.

Passaggio 3. Dalla scheda **Zone**, selezionare la zona **esterna** come origine e destinazione per la regola.



Passaggio 4. Selezionare l'azione, il titolo e qualsiasi altra condizione desiderata per definire questa regola.

Èpossibile creare più regole per questo flusso di traffico. È importante ricordare che le zone di origine e di destinazione devono essere le zone assegnate alle origini VPN e a Internet.

Verificare che non vi siano altri criteri generali che potrebbero corrispondere prima di queste regole. È preferibile che queste regole siano più severe di quelle definite per **qualsiasi** zona.

Passaggio 5. Per rendere effettive le modifiche, fare clic su **Salva**, quindi su **Distribuisci**.

Risultato

Al termine della distribuzione, il traffico AnyConnect viene filtrato/ispezionato dalle regole ACP applicate. Nell'esempio, un URL è stato bloccato.