Configure ASA with FirePOWER Services Access Control Rules to Filter AnyConnect VPN Client Traffic to Internet

Contents

Introduction

This document describes how to configure Access Control Policy (ACP) Rules to inspect traffic which comes from Virtual Private Network (VPN) tunnels or Remote Access (RA) users and use a Cisco Adaptive Security Appliance (ASA) with FirePOWER Services as Internet Gateway.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- AnyConnect, Remote Access VPN and/or Peer-to-Peer IPSec VPN.
- Firepower ACP configuration.
- ASA Modular Policy Framework (MPF).

Components Used

The information in this document is based on these software and hardware versions:

- ASA5506W version 9.6(2.7) for ASDM example
- FirePOWER module version 6.1.0-330 for ASDM example.
- ASA5506W version 9.7(1) for FMC example.
- FirePOWER versoin 6.2.0 for FMC example.
- Firepower Management Center (FMC) version 6.2.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Problem

ASA5500-X with FirePOWER Services is unable to filter and/or inspect AnyConnect users traffic as same as traffic sourced by other locations connected by IPSec tunnels that use a single point of permietral content security.

Another symptom this solution covers is to be unable to define specific ACP rules to the mentioned sources without other sources affectation.

This scenario is very common to see when TunnelAll design is used for VPN solutions terminated on an ASA.

Solution

This can be achieved through multiple ways. However, this scenario covers inspection by zones.

ASA configuration

Step 1. Identify the interfaces where AnyConnect users or VPN tunnels connect to the ASA.

Peer to Peer Tunnels

This is a scrap of the **show run crypto map** output.

```
crypto map outside_map interface outside
```

AnyConnect Users

The command **show run webvpn** shows where AnyConnect access is enabled.

```
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
```

In this scenario, interface **outside** receives, both, RA users and Peer to Peer tunnels.

Step 2. Redirect traffic from ASA to the FirePOWER module with a global policy.

It can either be done with a **match any** condition or a defined Access Control List (ACL) for traffic redirection.

Example with **match any** match.

```
class-map SFR
 match any

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

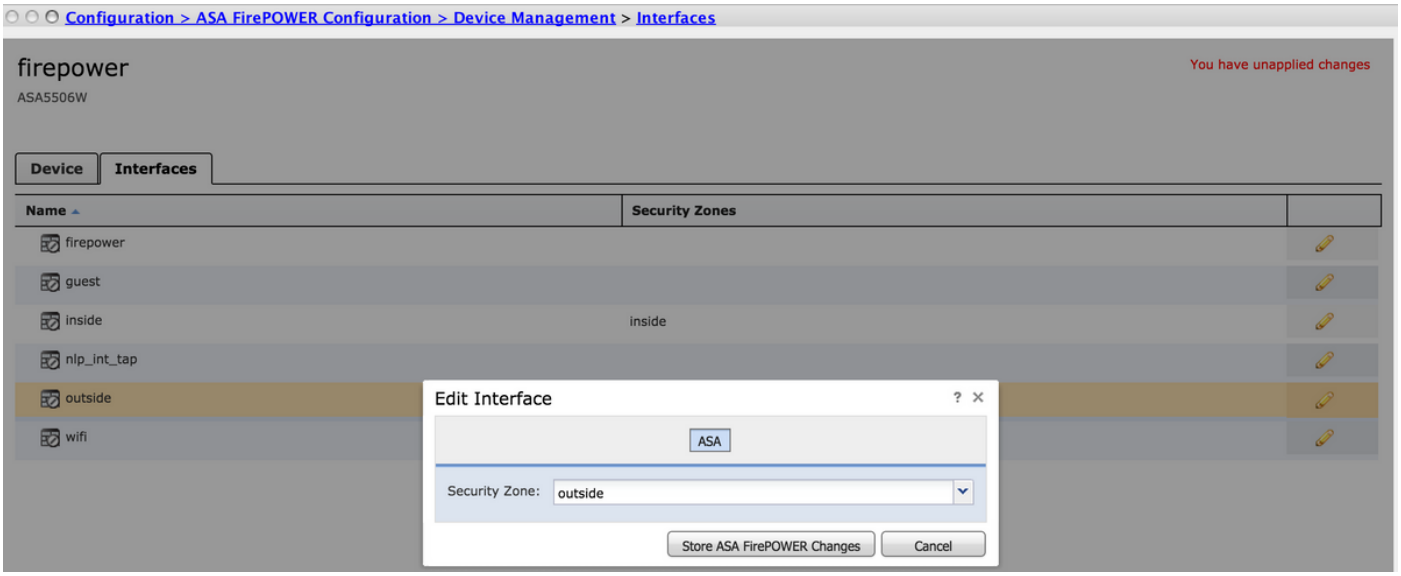
Example with ACL match.

```
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 a less common scenario, a service policy can be used for the outside interface. This example is not covered in this document.

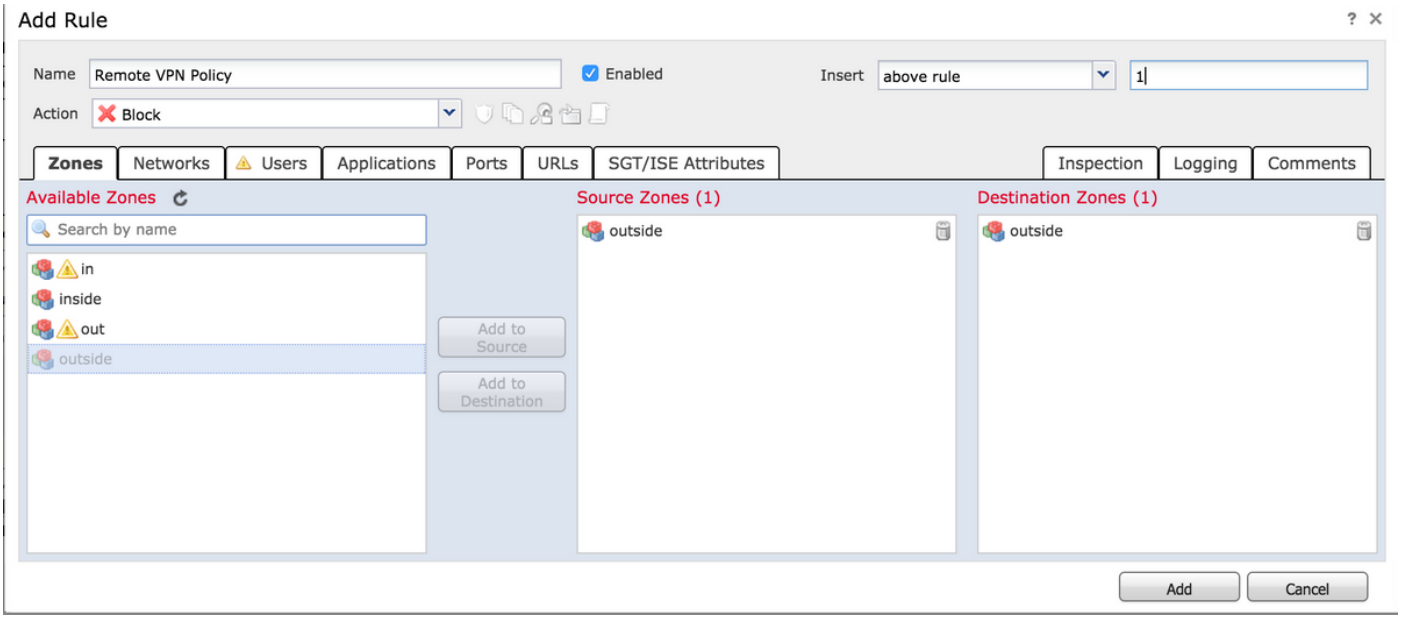
ASA FirePOWER module managed by ASDM configuration

Step 1. Assign the outside interface one zone at **Configuration > ASA FirePOWER Configuration > Device Management**. In this case, that zone is called **outside**.



Step 2. Select **Add Rule** at **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**.

Step 3. From **Zones** tab, select **outside** zone as source and destination for your rule.



Step 4. Select the action, title and any other desired conditions to define this rule.

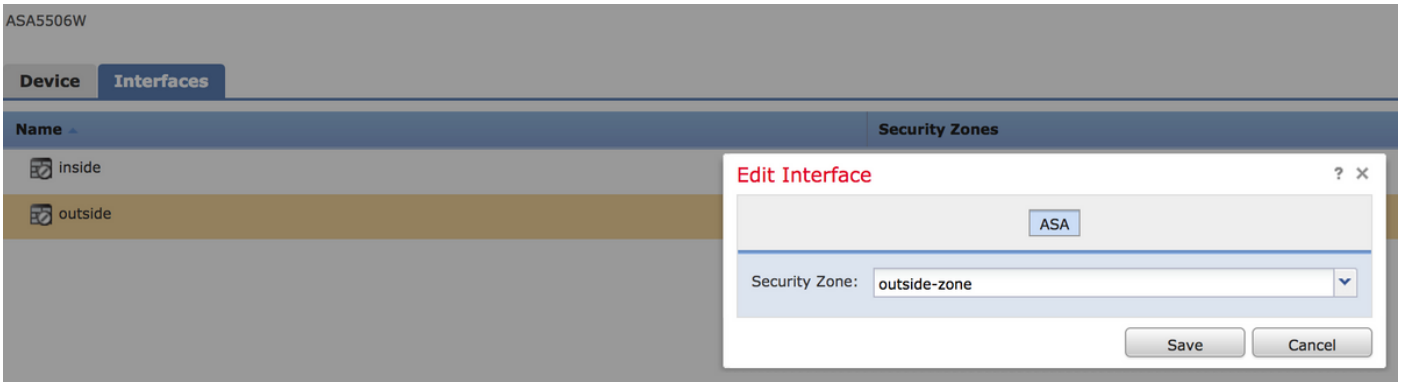
Multiple rules can be created for this traffic flow. It is just important to keep in mind that source and destination zones must be the zone assigned to VPN sources and Internet.

Make sure that there are no other more general policies that could match before these rules. It is preferrable to have these rules above the ones defined to **any** zone.

Step 5. Click on **Store ASA FirePOWER Changes** and then **Deploy FirePOWER Changes** to have these changes take effect.

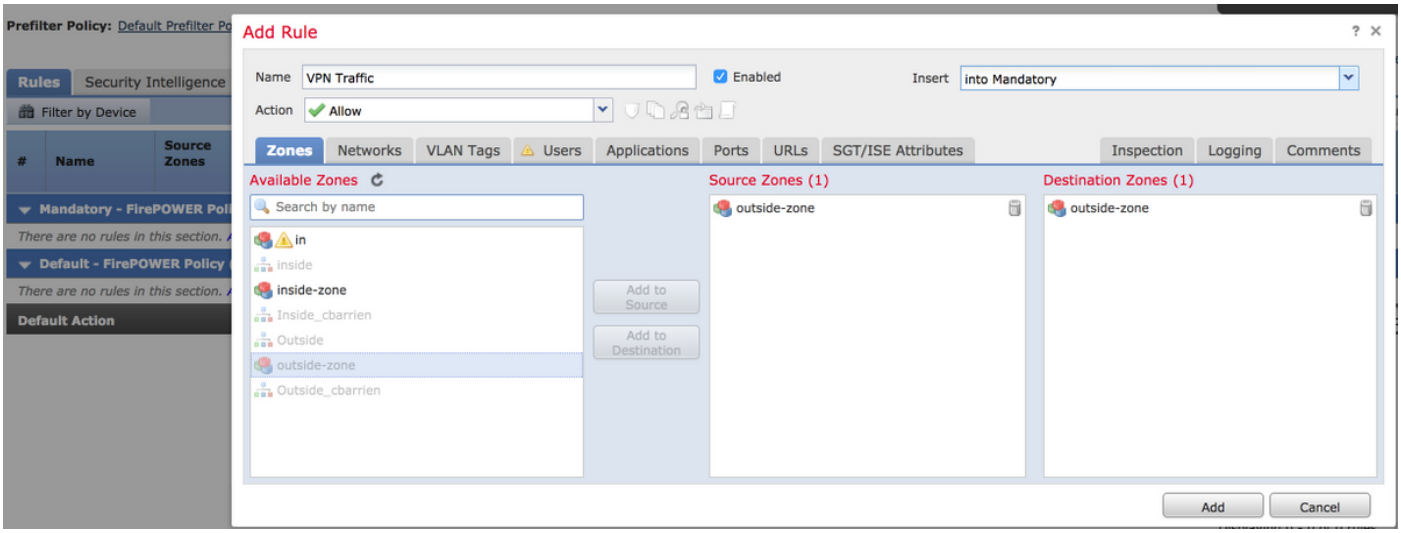
ASA FirePOWER module managed by FMC configuration

Step 1. Assign the outside interface one zone at **Devices > Management > Interfaces**. In this case, that zone is called **outside-zone**.



Step 2. Select **Add Rule** at **Policies > Access Control > Edit**.

Step 3. From **Zones** tab, select **outside-zone** zone as source and destination for your rule.



Step 4. Select the action, title and any other desired conditions to define this rule.

Multiple rules can be created for this traffic flow. It is just important to keep in mind that source and destination zones must be the zone assigned to VPN sources and Internet.

Make sure that there are no other more general policies that could match before these rules. It is preferrable to have these rules above the ones defined to **any** zone.

Step 5. Click on **Save** and then **Deploy** to have these changes take effect.

Result

After the deployment finishes, the AnyConnect traffic is now filtered/inspected by the ACP rules applied. In this example, a URL was succesfully blocked.