配置与FirePOWER服务访问控制规则的ASA过滤AnyConnect VPN客户端流量到互联网

目录

简介

本文描述如何配置访问控制策略(非加太)规则检查来自虚拟专用网络(VPN)通道或远程访问的流量(RA)用户并且以FirePOWER服务使用思科可适应安全工具(ASA)作为互联网网关。

先决条件

要求

Cisco 建议您了解以下主题：

- AnyConnect、远程访问VPN和点对点IPSec VPN。
- Firepower非加太配置。
- ASA模块化政策架构(MPF)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASDM示例的ASA5506W版本9.6(2.7)
- FirePOWER ASDM示例的模块版本6.1.0-330。
- FMC示例的ASA5506W版本9.7(1)。
- FMC示例的FirePOWER versoin 6.2.0。
- Firepower管理中心(FMC)版本6.2.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

与FirePOWER服务的ASA5500-X无法过滤并且/或者检查AnyConnect用户数据流作为同其他位置发出的流量一样连接由使用单点permietral内容安全的IPSec隧道。

此解决方案包括没有其他来源做作的另一症状是无法定义特定非加太规则到被提及的来源。

当Tunnelall设计使用在ASA时，终止的VPN解决方案此方案是非常普通发现。

解决方案

这可以通过多种方式达到。然而，此方案由区域包括检查。

ASA配置

步骤1.识别AnyConnect用户或VPN通道连接对ASA的接口。

对等通道

这是**show run加密映射**输出的报废。

```
crypto map outside_map interface outside
```

AnyConnect用户

show run命令**WebVPN**显示AnyConnect访问启用的地方。

```
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
```

在此方案，接口**外部**接收， RA用户和对等通道。

步骤2.重定向从ASA的流量到有一项全局策略的FirePOWER模块。

它可能执行与**匹配所有**条件或定义访问控制表(ACL)流量重定向的。

与**匹配的**示例其中**任一**配比。

```
class-map SFR
 match any

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

与ACL匹配的示例。

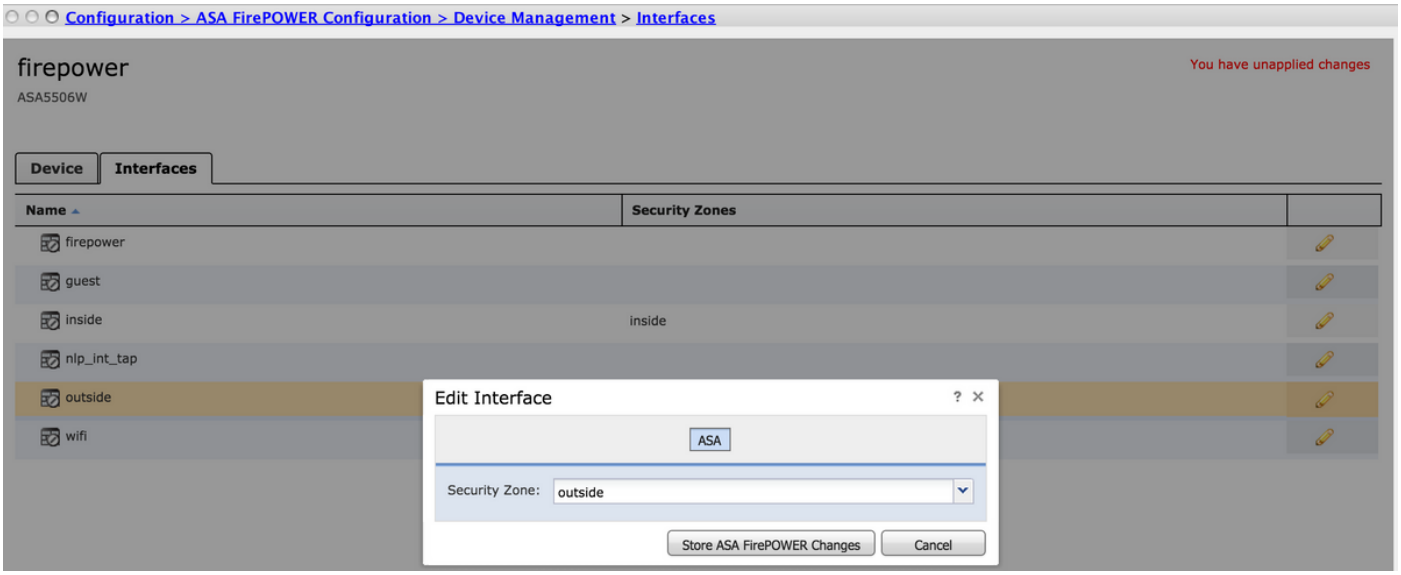
```
access-list sfr-acl extended permit ip any any

class-map SFR
 match access-list sfr-acl

policy-map global_policy
 class SFR
   sfr fail-open
```

```
service-policy global_policy global
```

在一较少常见情况中，服务策略可以用于外部接口。此示例在本文没有报道。

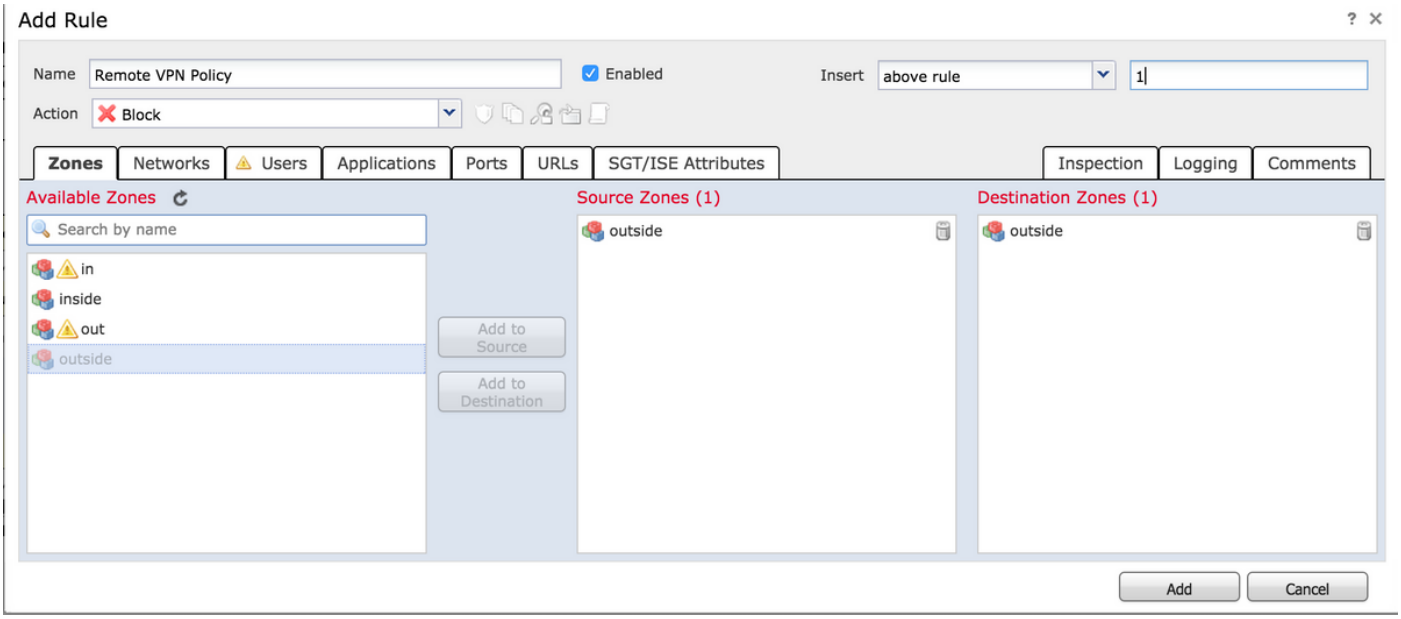
ASDM配置管理的ASA FirePOWER模块

步骤1.分配外部接口一个区域在**Configuration> ASA FirePOWER Configuration>设备管理**。在这种情况下，该区域**从外部**呼叫。



步骤2.选择**增加规则**在**Configuration> ASA FirePOWER Configuration>策略>访问控制策略**。

第三步：从**区域请**选中，挑选**外部**区域作为您的规则的源和目的。



步骤4.选择操作、标题和所有其他希望的情况定义此规则。

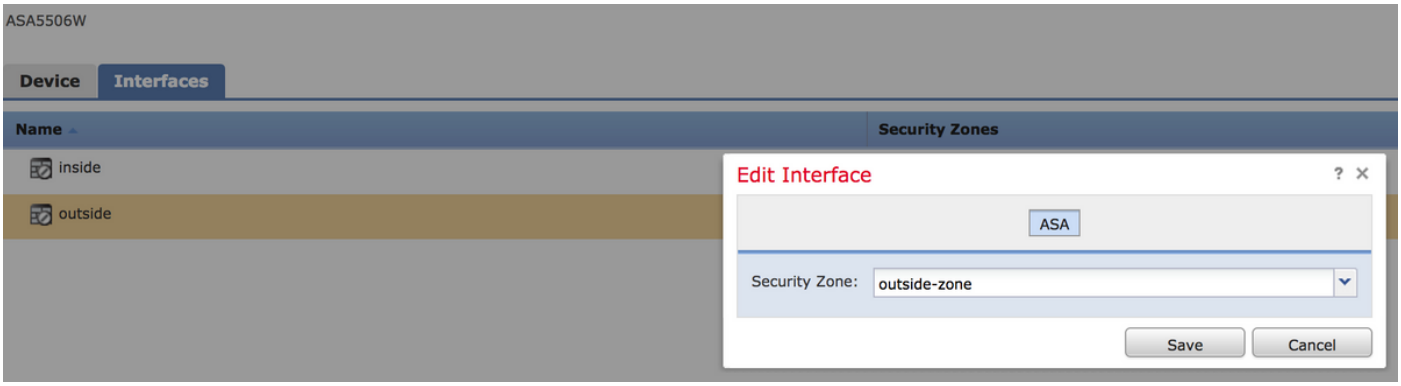
多个规则可以为此通信流创建。记住是公正重要的源和目的区域必须是区域分配到VPN来源和互联网。

确保没有可能在这些规则前配比的其他更多一般策略。它是preferrable有在那个上的这些规则定义对**所有**区域。

步骤5.点击**存储ASA FirePOWER更改**然后**部署FirePOWER更改**安排这些更改生效。

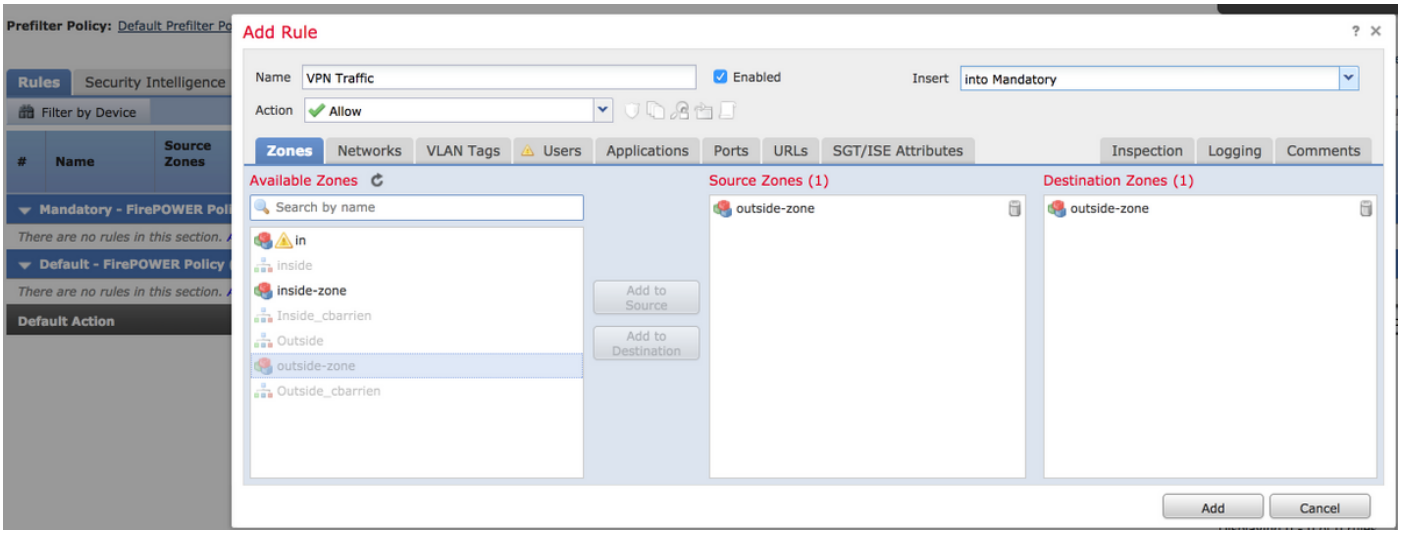
FMC配置管理的ASA FirePOWER模块

步骤1.分配外部接口一个区域在**设备> Management>接口**。在这种情况下，该区域呼叫外部**区域**。



步骤2.选择**增加规则**在**策略>访问控制> Edit**。

第三步：从**区域请**选中，挑选外部**区域**区域作为您的规则的源和目的。



步骤4.选择操作、标题和所有其他希望的情况定义此规则。

多个规则可以为此通信流创建。记住是公正重要的源和目的区域必须是区域分配到VPN来源和互联网。

确保没有可能在这些规则前配比的其他更多一般策略。它是preferrable有在那个上的这些规则定义对**所有**区域。

步骤5.点击**"Save"**然后**部署**安排这些更改生效。

结果

在部署完成后， AnyConnect流量由应用的非加太规则当前过滤/检查。 在本例中， URL顺利地阻塞。

Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.