Настройте ASA с правилами управления доступом FirePOWER Services фильтровать трафик клиента AnyConnect VPN Client к Интернету

Содержание

Введение

Этот документ описывает, как настроить Правила Политики контроля доступа (ACP) осмотреть трафик, который прибывает из туннелей Виртуальной частной сети (VPN) или пользователей Удаленного доступа (RA), и используйте устройство адаптивной защиты Cisco (ASA) с FirePOWER Services как интернет-шлюз.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- AnyConnect, VPN для удаленного доступа и/или Одноранговый IPSEC VPN.
- Конфигурация ACP огневой мощи.
- Модульная система политик (MPF) ASA.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 9.6 (2.7) ASA5506W для примера ASDM
- Версия модуля 6.1.0-330 FirePOWER для примера ASDM.
- Версия 9.7 (1) ASA5506W для примера FMC.

- FirePOWER versoin 6.2.0 для примера FMC.
- Версия 6.2.0 Центра управления огневой мощи (FMC)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Проблема

ASA5500-X с FirePOWER Services неспособен фильтровать и/или осмотреть пользовательский трафик AnyConnect как то же как трафик, полученный другими местоположениями, связанными Туннелями IPSec, которые используют одиночную точку permietral безопасности содержания.

Другой признак, который покрывает это решение, должен быть неспособен определить определенные правила ACP к упомянутым источникам без другой исходной аффектации.

Когда дизайн TunnelAll используется для решений для VPN, завершенных на ASA, этот сценарий очень распространен для наблюдения.

Решение

Это может быть достигнуто через несколька способов. Однако этот сценарий касается контроля зонами.

Конфигурация ASA

Шаг 1. Определите интерфейсы, где пользователи AnyConnect или VPN-туннели соединяются с ASA.

Узел в одноранговые туннели

Это - фрагмент **показа выполненные** выходные данные **криптокарты**.

```
crypto map outside_map interface outside
```

Пользователи AnyConnect

Webvpn команды show run показывает, где включен доступ AnyConnect.

```
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
```

В этом сценарии интерфейс **снаружи** получает, оба, пользователи RA и Узел в Одноранговые туннели.

Шаг 2. Трафик перенаправления от ASA до модуля FirePOWER с глобальной политикой.

Это может или быть сделано с **соответствием любое** условие или определенный Список контроля доступа (ACL) для переадресации трафика.

Пример с **соответствием любое** соответствие.

```
class-map SFR
 match any

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

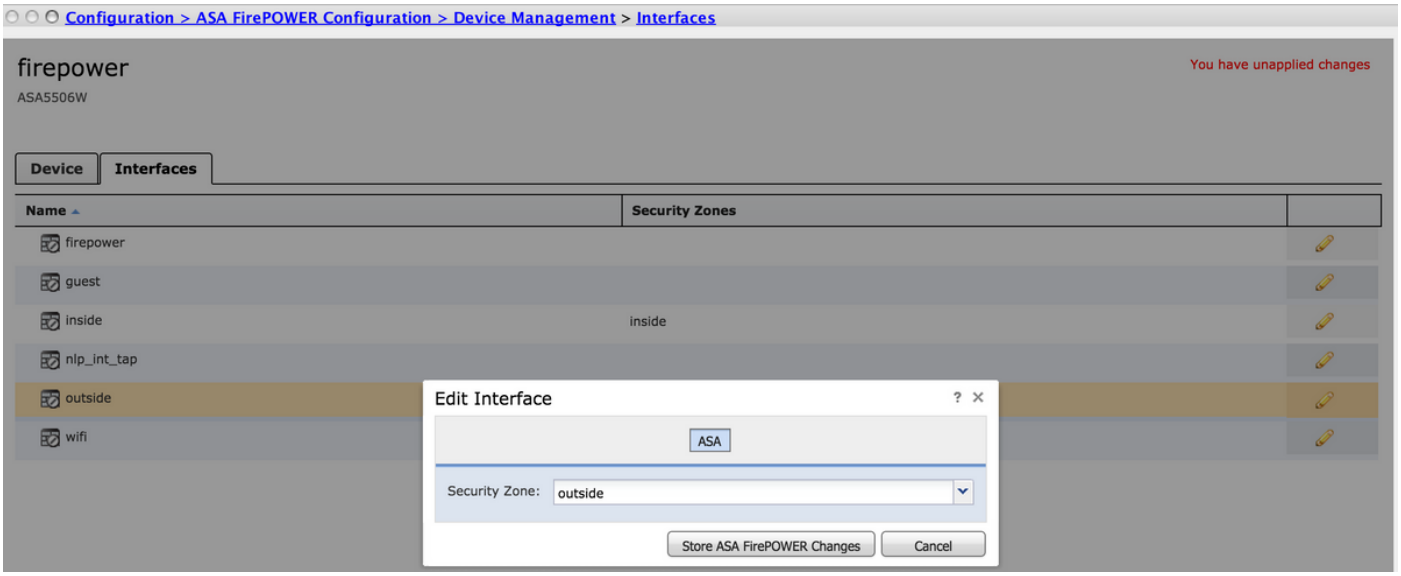
Пример с соответствием ACL.

```
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
```

В меньшем количестве общего сценария политика обслуживания может использоваться для внешнего интерфейса. Данный пример не покрыт этим документом.

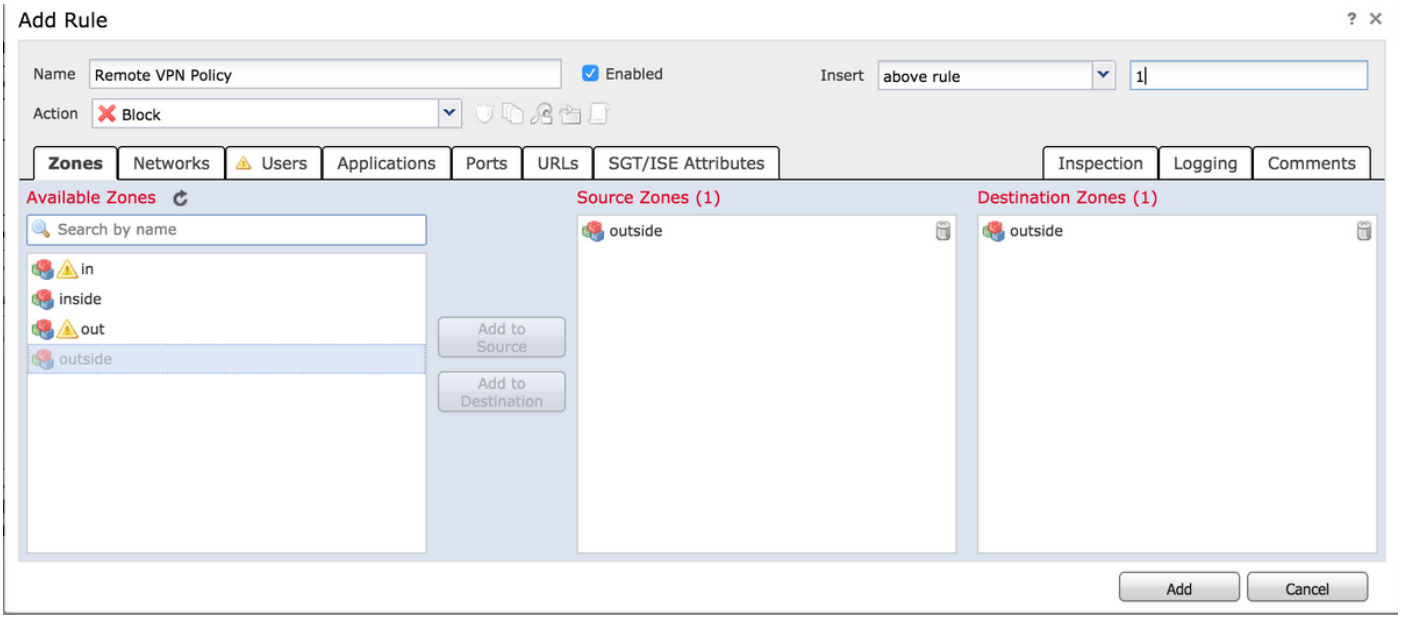
Модуль ASA FirePOWER, которым управляет конфигурация ASDM

Шаг 1. Назначьте внешний интерфейс одна зона в **Конфигурации> конфигурация ASA FirePOWER> Управление устройствами**. В этом случае ту зону вызывают **снаружи**.



Шаг 2. Выберите **Add Rule at Configuration > ASA FirePOWER Configuration> Policies> Access Control Policy**.

Шаг 3. От вкладки **Zones** выберите **внешнюю** зону как источник и назначение для вашего правила.



Шаг 4. . Выберите действие, название и любые другие желаемые условия определить это правило.

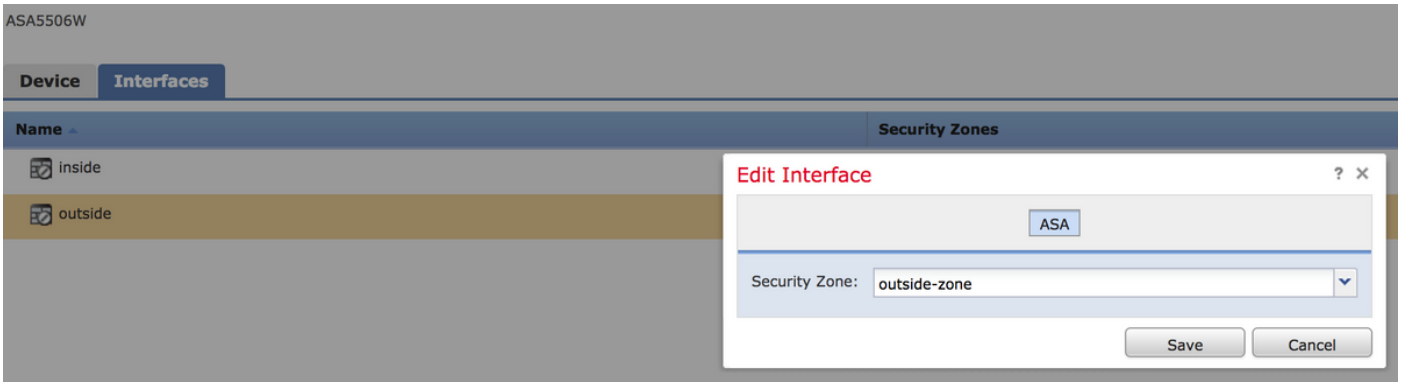
Множественные правила могут быть созданы для этого трафика. Просто важно иметь в виду, что источник и зоны назначения должны быть зоной, назначенной на источники VPN и Интернет.

Удостоверьтесь, что нет никакой другой более общей политики, которая могла совпасть перед этими правилами. Предпочтительно иметь эти правила выше тех определенных к **любой** зоне.

Шаг 5. . Щелкните **по Store ASA FirePOWER Changes** и затем **Развернитесь, Изменения FirePOWER** для имения этих изменений вступают в силу.

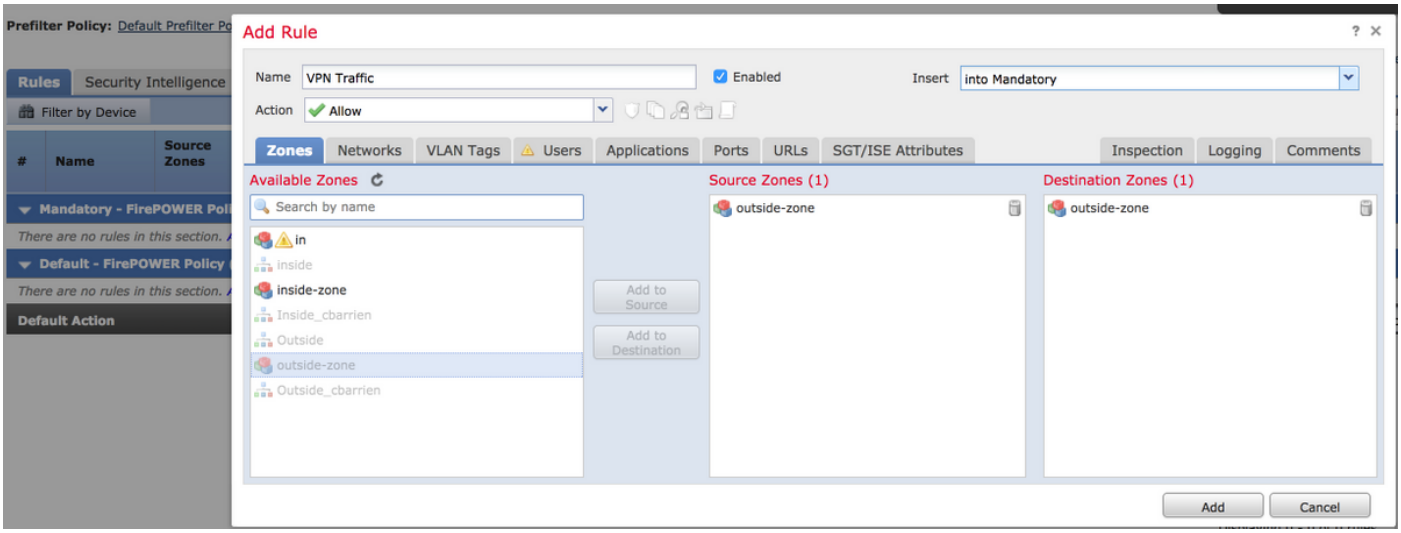
Модуль ASA FirePOWER, которым управляет конфигурация FMC

Шаг 1. Назначьте внешний интерфейс одна зона в **Устройствах > менеджмент > Интерфейсы**. В этом случае ту зону называют **внешней зоной**.



Шаг 2. Выберите **Add Rule at Policies > Access Control > Edit**.

Шаг 3. От вкладки **Zones** выберите **внешнюю зональную** зону как источник и назначение для вашего правила.



Шаг 4. . Выберите действие, название и любые другие желаемые условия определить это правило.

Множественные правила могут быть созданы для этого трафика. Просто важно иметь в виду, что источник и зоны назначения должны быть зоной, назначенной на источники VPN и Интернет.

Удостоверьтесь, что нет никакой другой более общей политики, которая могла совпасть перед этими правилами. Предпочтительно иметь эти правила выше тех определенных к **любой** зоне.

Шаг 5. . Щелкните **по Save** и затем **Разверните**сь для имения этих изменений, вступают в силу.

Результат

После концов развертываний трафик AnyConnect теперь фильтруется/осматривается примененными правилами ACP. В данном примере был успешно заблокирован URL.