인터넷에 대한 AnyConnect VPN 클라이언트 트래픽을 필터링하도록 Firepower 서비스 액세스 제어 규칙으로 ASA 구성

목차

소개

이 문서에서는 VPN(Virtual Private Network) 터널 또는 RA(Remote Access) 사용자로부터 오는 트래픽을 검사하고 Firepower 서비스가 포함된 Cisco ASA(Adaptive Security Appliance)를 인터넷 게이트웨이로 사용하도록 ACP(Access Control Policy) 규칙을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AnyConnect, 원격 액세스 VPN 및/또는 피어 투 피어 IPSec VPN
- Firepower ACP 구성
- ASA MPF(Modular Policy Framework).

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASDM의 경우 ASA5506W 버전 9.6(2.7)
- ASDM의 firepower 모듈 버전 6.1.0-330의 예.
- FMC의 경우 ASA5506W 버전 9.7(1).
- FMC의 경우 firepower 버전 6.2.0입니다.

- FMC(firepower Management Center) 버전 6.2.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

firepower Services가 포함된 ASA5500-X는 단일 허용 콘텐츠 보안 지점을 사용하는 IPSec 터널로 연결된 다른 위치에서 발생하는 트래픽과 마찬가지로 AnyConnect 사용자 트래픽을 필터링 및/또는 검사할 수 없습니다.

이 솔루션에서 다루는 또 다른 증상은 다른 소스의 영향을 받지 않고 언급된 소스에 대해 특정 ACP 규칙을 정의할 수 없는 것입니다.

이 시나리오는 ASA에서 종료되는 VPN 솔루션에 TunnelAll 설계가 사용되는 경우를 흔히 볼 수 있습니다.

솔루션

이는 여러 가지 방법을 통해 달성할 수 있습니다. 그러나 이 시나리오에서는 영역별 검사를 다룹니다.

ASA 컨피그레이션

1단계. AnyConnect 사용자 또는 VPN 터널이 ASA에 연결되는 인터페이스를 식별합니다.

피어 투 피어 터널

show run crypto map 출력의 스크랩입니다.

```
<#root>

crypto map outside_map interface

outside
```

AnyConnect 사용자

show run webvpn 명령은 AnyConnect 액세스가 활성화된 위치를 표시합니다.

```
<#root>

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
```

이 시나리오에서 interface outside는 RA 사용자 및 Peer to Peer 터널을 모두 수신합니다.

2단계. 글로벌 정책을 사용하여 ASA에서 Firepower 모듈로 트래픽을 리디렉션합니다.

이는 트래픽 리디렉션을 위해 정의된 ACL(Access Control List)이나 임의의 조건에 매칭하는 방식으로 수행할 수 있습니다.

일치 항목이 있는 예.

```
class-map SFR
 match any

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

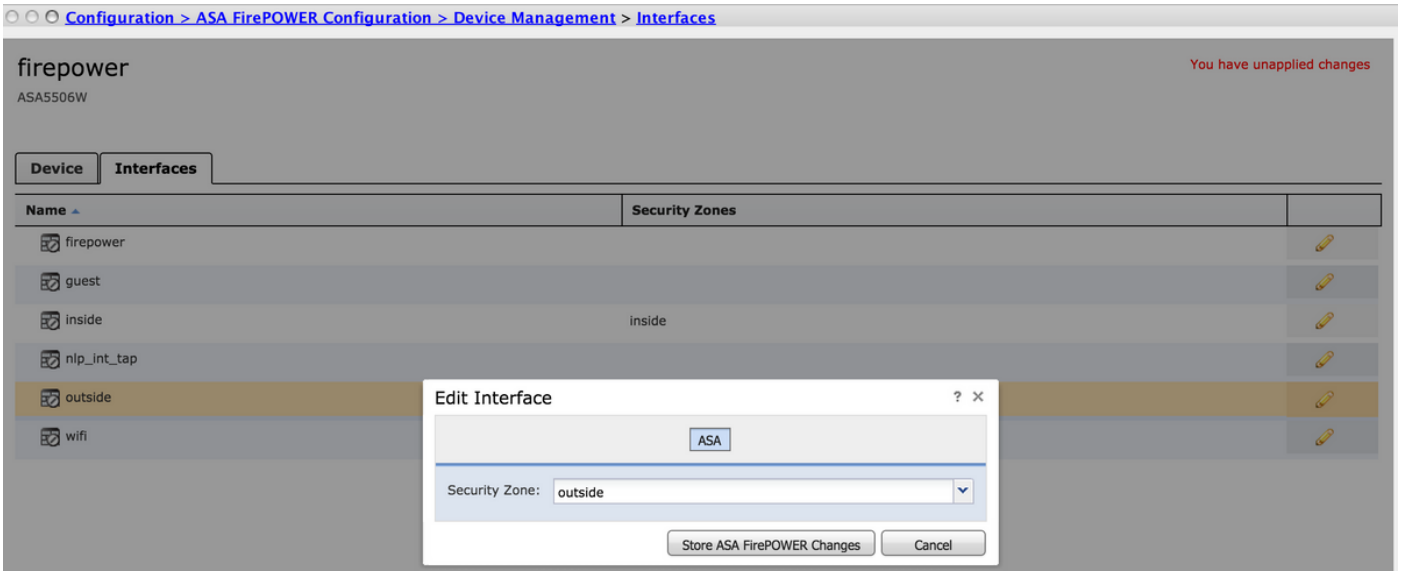
ACL 일치의 예

```
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
```

덜 일반적인 시나리오에서 외부 인터페이스에 서비스 정책을 사용할 수 있습니다. 이 예시는 이 문서에서 다루지 않습니다.

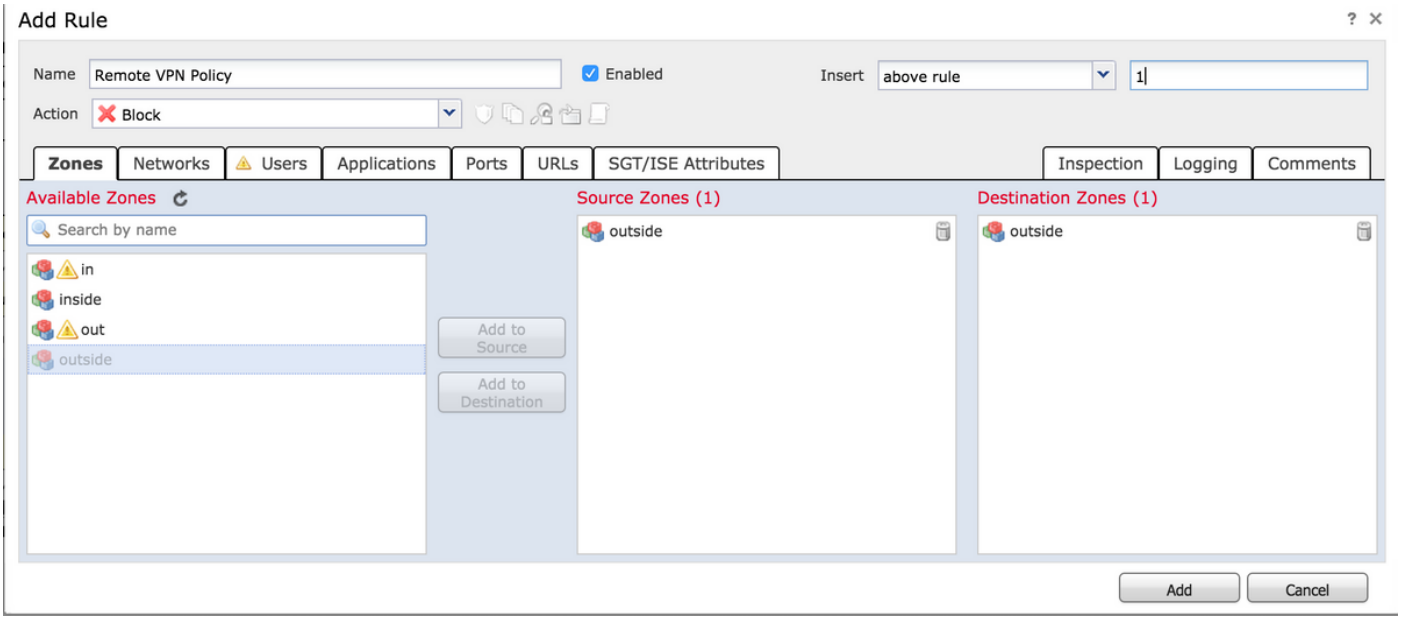
ASDM 컨피그레이션에 의해 관리되는 ASA Firepower 모듈

1단계. Configuration(컨피그레이션) > ASA Domain Configuration(ASA Firepower 컨피그레이션) > Device Management(디바이스 관리)에서 외부 인터페이스에 한 영역을 할당합니다. 이 경우에는 해당 영역을 외부 영역이라고 합니다.



2단계. Configuration(컨피그레이션) > ASA Configuration(ASA Firepower 컨피그레이션) > Policies(정책) > Access Control Policy(액세스 제어 정책)에서 Add Rule(규칙 추가)을 선택합니다.

3단계. Zones 탭에서 규칙의 소스와 대상으로 outside zone을 선택합니다.



4단계. 이 규칙을 정의하려면 작업, 제목 및 원하는 기타 조건을 선택합니다.

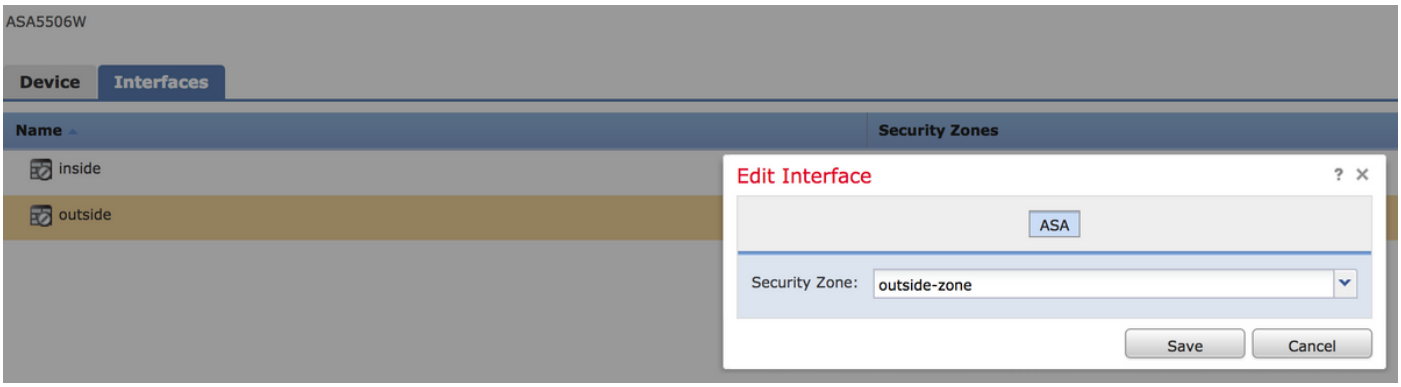
이 트래픽 흐름에 대해 여러 규칙을 생성할 수 있습니다. 소스 및 대상 영역은 VPN 소스 및 인터넷에 할당된 영역이어야 한다는 점을 염두에 두어야 합니다.

이러한 규칙 앞에 일치할 수 있는 다른 일반 정책이 없는지 확인합니다. 이러한 규칙은 모든 영역에 정의된 규칙 위에 있는 것이 좋습니다.

5단계. Store ASA Firepower Changes(ASA Firepower 변경 사항 저장)를 클릭한 다음 Deploy Domain Changes(변경 사항 구축)를 클릭하여 변경 사항을 적용합니다.

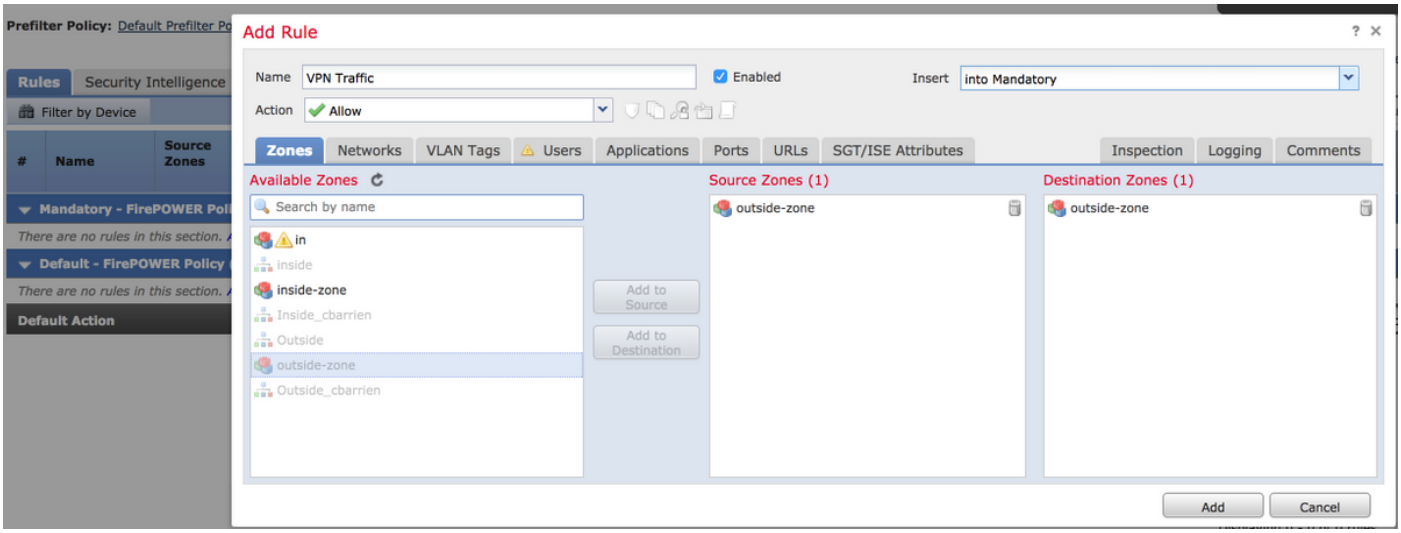
FMC 컨피그레이션에 의해 관리되는 ASA Firepower 모듈

1단계. 외부 인터페이스에 디바이스에서 하나의 영역을 할당합니다 > 관리 > 인터페이스. 이 경우 해당 영역을 호출합니다 외부 영역.



2단계. Policies(정책) > Access Control(액세스 제어) > Edit(수정)에서 Add Rule(규칙 추가)을 선택합니다.

3단계. Zones(영역) 탭에서 규칙의 소스 및 대상으로 outside-zone zone(외부 영역)을 선택합니다.



4단계. 이 규칙을 정의하려면 작업, 제목 및 원하는 기타 조건을 선택합니다.

이 트래픽 흐름에 대해 여러 규칙을 생성할 수 있습니다. 소스 및 대상 영역은 VPN 소스 및 인터넷에 할당된 영역이어야 한다는 점을 염두에 두어야 합니다.

이러한 규칙 앞에 일치할 수 있는 다른 일반 정책이 없는지 확인합니다. 이러한 규칙은 모든 영역에 정의된 규칙 위에 있는 것이 좋습니다.

5단계. Save(저장)를 클릭한 다음 Deploy(구축)를 클릭하여 변경 사항을 적용합니다.

결과

구축이 완료되면 이제 AnyConnect 트래픽이 적용된 ACP 규칙에 의해 필터링/검사됩니다. 이 예에서는 URL이 성공적으로 차단되었습니다.

Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.