Defense Center의 SNORT_BPF 변수 컨피그레이션

목차

소개

BPF(Berkeley Packet Filter)를 사용하여 Defense Center에서 호스트 또는 네트워크를 검사하지 않도록 제외할 수 있습니다. Snort는 침입 **정책**에서 트래픽을 제외하기 위해 Snort_BPF 변수를 사용합니다. 이 문서에서는 다양한 시나리오에서 Snort_BPF **변수를 사용하**는 방법에 대한 지침을 제공합니다.

> **팁**: 침입 정책의 BPF보다는 액세스 제어 정책에서 신뢰 규칙을 사용하여 어떤 트래픽이 검사되고 있는지 확인하는 것이 좋습니다. Snort_**BPF** 변수는 소프트웨어 버전 5.2에서 사용할 수 있으며 소프트웨어 버전 5.3 이상에서는 더 이상 사용되지 않습니다.

사전 요구 사항

요구 사항

Defense Center, 침입 정책, Berkeley Packet Filter 및 Snort 규칙에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- 방어 센터
- 소프트웨어 버전 5.2

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.

컨피그레이션 단계

Snort _BPF **변수**를 구성하려면 다음 단계를 수행하십시오.

1. Defense Center의 웹 사용자 인터페이스에 액세스합니다.
2. Policies(정책) **> Intrusion(침입) > Intrusion Policy(침입 정책)로 이동합니다**.
3. 침입 정책을 수정하려면 *연필* 아이콘을 클릭합니다.
4. 클릭 **변수** 왼쪽 메뉴에서 선택합니다.
5. 변수가 구성되면 변경 사항을 저장하고 침입 정책을 다시 적용해야 적용됩니다.

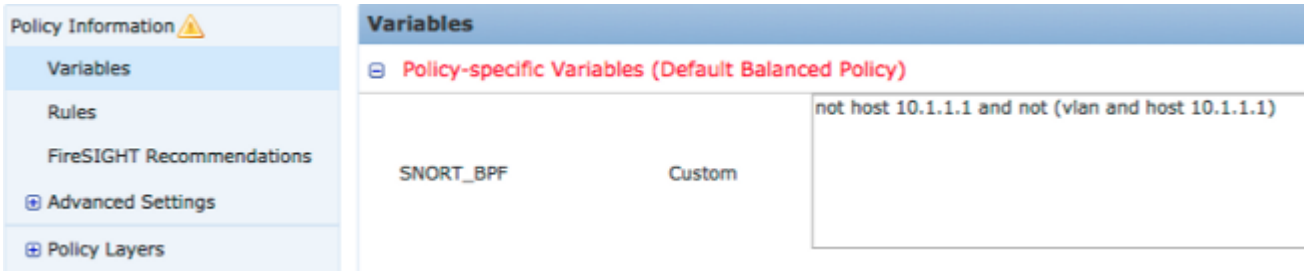

그림: Snort_BPF 변수 컨피그레이션 페이지의 스크린샷

컨피그레이션 예

몇 가지 기본 예는 참고용으로 아래에 나와 있습니다.

시나리오 1: 취약성 스캐너의 모든 트래픽, 수신 및 발신 무시

1. IP 주소 10.1.1.1에 취약성 스캐너가 있습니다.
2. 스캐너로 들어오고 나가는 모든 트래픽을 무시하려고 합니다.
3. 트래픽에는 802.1q(vlan) 태그가 있을 수도 있고 없을 수도 있습니다

SNORT_**BPF**는

```
not host 10.1.1.1 and not (vlan and host 10.1.1.1)
```

비교: 트래픽 *은 VLAN 태그가 지정되지 않았지만 1번 및 2번 포인트는 참입니다.

```
not host 10.1.1.1
```

일반 영어로, 이것은 엔드 포인트 중 하나가 10.1.1.1 (스캐너) 인 트래픽을 무시 합니다.

시나리오 2: 모든 트래픽, TO 및 FROM 2개 취약성 스캐너 무시

1. IP 주소 10.1.1.1에 취약성 스캐너가 있습니다.
2. IP 주소 10.2.1.1에 두 번째 취약성 스캐너가 있습니다.
3. 스캐너로 들어오고 나가는 모든 트래픽을 무시하려고 합니다.
4. 트래픽에는 802.11(vlan) 태그가 있을 수도 있고 없을 수도 있습니다

SNORT_BPF는

```
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan and (host 10.1.1.1 or host 10.2.1.1))
```

비교: 트래픽 *은 VLAN 태그가 지정되지 않았지만 1번 및 2번 포인트는 참입니다.

```
not (host 10.1.1.1 or host 10.2.1.1)
```

요약하면, 이는 엔드포인트 중 하나가 10.1.1.1 또는 10.2.1.1인 트래픽을 무시합니다.

> **참고**: vlan 태그는 거의 모든 경우에 지정된 BPF에서 한 번만 발생해야 합니다. 네트워크에서 중첩된 VLAN 태깅('QinQ'라고도 함)을 사용하는 경우에만 이 태그가 두 번 이상 표시됩니다.

시나리오 3: VLAN 태그 처리된 트래픽, TO 및 FROM 2개 취약성 스캐너 무시

1. IP 주소 10.1.1.1에 취약성 스캐너가 있습니다.
2. IP 주소 10.2.1.1에 두 번째 취약성 스캐너가 있습니다.
3. 스캐너로 들어오고 나가는 모든 트래픽을 무시하려고 합니다.
4. 트래픽은 802.11(vlan) 태그가 지정되며, vlan 101과 같이 특정(vlan) 태그를 사용하려는 경우

SNORT_BPF는

```
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan 101 and (10.1.1.1 or host 10.2.1.1))
```

시나리오 4: 백업 서버의 트래픽 무시

1. IP 주소 10.1.1.1에 네트워크 백업 서버가 있습니다.
2. 네트워크의 시스템이 포트 8080의 이 서버에 연결되어 야간 백업을 실행합니다
3. 이 백업 트래픽은 암호화되고 볼륨이 크기 때문에 무시하려고 합니다

SNORT_BPF는

```
not (dst host 10.1.1.1 and dst port 8080) and not (vlan and (dst host 10.1.1.1
and dst port 8080))
```

비교: 트래픽 *은 VLAN 태그가 지정되지 않았지만 1번 및 2번 포인트는 참입니다.

```
not (dst host 10.1.1.1 and dst port 8080)
```

변환하면 포트 8080(수신 대기 포트)에서 10.1.1.1(가상 백업 서버)에 대한 트래픽을 IPS 탐지 엔진에서 검사하지 않아야 합니다.

단일 호스트가 아닌 호스트 대신 net을 사용하여 네트워크 블록을 지정할 수도 있습니다. 예를 들

면 다음과 같습니다.

```
not net 10.1.1.0/24
```

일반적으로 BPF를 가능한 한 구체적으로 지정하는 것이 좋습니다. 제외해야 할 트래픽은 검사에서 제외하고, 익스플로잇 시도를 포함할 수 있는 관련 없는 트래픽은 제외하지 않는 것이 좋습니다.

시나리오 5: 개별 호스트 대신 네트워크 범위 사용

호스트 대신 BPF 변수에 네트워크 범위를 지정하여 변수의 길이를 줄일 수 있습니다. 이렇게 하려면 호스트 대신 net 키워드를 사용하고 CIDR 범위를 지정합니다. 다음은 그 예입니다.

```
not (dst net 10.8.0.0/16 and dst port 8080) and not (vlan and (dst net 10.8.0.0/16
and dst port 8080))
```

> **참고**: CIDR 표기법을 사용하여 네트워크 주소를 입력하고 CIDR 블록 주소 공간 내에서 사용 가능한 주소를 입력해야 합니다. 예를 들어 net 10.8.0.0/16 이 아니라 net 10.8.2.16/16을 사용합니다.

이 **SNORT_BPF** IPS 탐지 엔진이 특정 트래픽을 검사하지 않도록 하기 위해 변수를 사용합니다. 이는 성능상의 이유로 자주 사용됩니다. 이 변수는 표준 BPF(Berkeley Pack Filters) 형식을 사용합니다. 트래픽과 **SNORT_BPF** 변수가 검사됩니다. 트래픽이 **SNORT_BPF** IPS 탐지 엔진에서 변수를 검사하지 않습니다.

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.