FireSIGHT 시스템의 규칙 프로파일링 지침

목차

소개

FirePOWER 어플라이언스 또는 NGIPS 가상 어플라이언스가 초과 서브스크립션된 경우, 일부 추가 데이터를 수집하여 디바이스의 어떤 구성 요소가 시스템 속도를 늦추는지 확인해야 합니다.규칙 프로파일링을 사용하면 FireSIGHT 시스템에서 탐지 엔진의 규칙 및 하위 시스템에서 CPU 사이클을 가장 많이 사용하는 추가 데이터를 생성할 수 있습니다.이 문서에서는 FireSIGHT 어플라이언스 및 NGIPS 가상 어플라이언스에서 규칙 프로파일링을 실행하는 방법에 대한 지침을 제공합니다.

사전 요구 사항

요구 사항

FirePOWER 어플라이언스 및 가상 어플라이언스 모델에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- FirePOWER 7000 Series 어플라이언스, 8000 Series 어플라이언스 및 NGIPS 가상 어플라이언스
- 소프트웨어 버전 5.2 이상

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.

> **경고:**규칙 프로파일링 명령을 실행하면 네트워크 성능에 영향을 줄 수 있습니다.따라서 Cisco Technical Support에서 규칙 프로파일링 데이터를 요청하는 경우에만 이 명령을 실행해야 합니다.

규칙 프로파일링 실행 단계

1단계:관리되는 디바이스의 CLI에 액세스합니다.

2단계:특정 시간에 대해 다음 규칙 프로파일링 명령을 실행합니다.시간은 15분에서 120분 사이여야 합니다.다음 예에서는 스크립트가 15분 동안 실행됩니다.

```
> system support run-rule-profiling 15
```

3단계:명령 실행을 확인합니다.y**를** 입력하고 Enter **키를 누릅니다**.

> **경고:** 규칙 프로파일링 명령은 탐지 기능에 영향을 줄 수 있는 탐지 엔진을 다시 시작하고 CPU 사용률을 높입니다.

```
> system support run-rule-profiling 15

You are about to profile
 DE    Primary Detection Engine (94854a60-cb17-11e3-a2f5-8de07680f9f3)
 Time  15 minutes

WARNING!!  Detection Engine will be restarted.
Intrusion Detection / Prevention will be affected

Please confirm by entering 'y': y
```

실행을 확인한 후 규칙 프로파일링이 시작됩니다.프로파일링을 완료하는 시간은 0분으로 줄어듭니다.

```
Restarting DE for profiling...done
Profiling for 15 more minutes...
```

완료되면 셸 프롬프트가 다시 나타납니다.

```
Restarting DE for profiling...done
Profiling...done
Restarting DE with original configuration...in progress
>
```

4단계:rule profiling 명령은 .tgz 파일을 생성합니다.셸에서 다음 명령을 실행하여 파일을 찾을 수 있습니다.

```
> system file list
May 12 15:53 99364308 profiling.94854a60-cb17-11e3-a2f5-8de07680f9f3.1399909945.tgz
```

5단계:추가 분석을 위해 Cisco 기술 지원 팀에 파일을 제공합니다.