콘텐츠 보안 어플라이언스 FAQ:Cisco Content Security Appliance에서 패킷 캡처를 어떻게 수행합니까?

목차

소개

이 문서에서는 Cisco Content Security Appliance에서 패킷 캡처를 수행하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA(Email Security Appliance)
- Cisco WSA(Web Security Appliance)
- Cisco SMA(Security Management Appliance)
- AsyncOS

사용되는 구성 요소

이 문서의 정보는 모든 버전의 AsyncOS를 기반으로 합니다.

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.

Cisco Content Security Appliance에서 패킷 캡처를 어떻게 수행합니까?

GUI를 사용하여 패킷 캡처(tcpdump 명령)를 수행하려면 다음 단계를 완료합니다.

1. GUI에서 **Help and Support(도움말 및 지원) > Packet Capture(패킷 캡처)**로 이동합니다.
2. 패킷 캡처가 실행되는 네트워크 인터페이스와 같이 필요에 따라 패킷 캡처 설정을 수정합니다 .미리 정의된 필터 중 하나를 사용하거나, Unix tcpdump 명령에서 지원하는 구문을 사용하여 사용자 지정 필터를 생성할 수 **있습니다**.
3. 캡처 **시작**을 클릭하여 캡처를 시작합니다.
4. 캡처 **중지**를 클릭하여 캡처를 종료합니다.
5. 패킷 캡처를 다운로드합니다.

CLI에서 패킷 캡처(tcpdump 명령)를 수행하려면 다음 단계를 완료합니다.

1. CLI에 다음 명령을 입력합니다.

```
wsa.run> packetcapture

Status: No capture running


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     (tcp port 80 or tcp port 3128)
```

2. 수행할 작업을 선택합니다.

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> setup
```

3. 캡처 파일의 최대 허용 크기(MB)를 입력합니다.

```
[200]> 200

Do you want to stop the capture when the file size is reached? (If not, a new
 file will be started and the older capture data will be discarded.)

[N]> n

The following interfaces are configured:
```

```
1. Management

2. T1

3. T2
```

4. 패킷을 캡처할 하나 이상의 인터페이스의 이름 또는 번호를 쉼표로 구분하여 입력합니다.

```
[1]> 1
```

5. 캡처에 사용할 필터를 입력합니다.필터를 지우고 선택한 인터페이스의 모든 패킷을 캡처하려면 **CLEAR**라는 단어를 입력합니다.

```
[(tcp port 80 or tcp port 3128)]> host 10.10.10.10 && port 80

Status: No capture running

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     host 10.10.10.10 && port 80
```

6. 캡처를 시작하려면 **시작** 작업을 선택합니다.

```
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> start

Status: Capture in progress (Duration: 0s)
File Name: S650-00137262569A-8RVFDB1-20080919-174302.cap (Size: 0K)

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     host 10.10.10.10 && port 80
```

7. 캡처를 종료하려면 **중지** 작업을 선택합니다.

```
- STOP - Stop packet capture.
- STATUS - Display current capture status.
```

```
- SETUP - Change packet capture settings.

[]> stop

Status: No capture running (Capture stopped by user)

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     host 10.10.10.10 && port 80
```