Adaptive Security Appliances의 로그와 디버그 간의 차이점

목차

소개

이 문서에서는 버전 8.4 이상을 실행하는 ASA(Adaptive Security Appliances)의 디버깅 기능에 대한 간단한 설명을 제공합니다.그러나 일부 기능은 버전 9.5(2) 이상에서만 사용할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA 5506-X with ASA Software 버전 9.5(2)
- Cisco ASDM(Adaptive Security Device Manager) 버전 7.5.2

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.

기본 로깅 기능

ASA는 디버그 메시지를 Cisco IOS® 디바이스와 다르게 처리합니다.기본적으로 "logging debug-trace"가 사용되지 않는 경우 콘솔 포트를 통해 연결되거나 텔넷/보안 셸(SSH)을 통해 연결되지만 완전히 독립적입니다.콘솔을 사용하면 debug 명령을 입력한 후 즉시 나타납니다.SSH 세션도 동일한 작업을 수행합니다.

독립성은 콘솔 포트에서 디버깅을 활성화하고 SSH를 통해 연결된 경우 디버그가 SSH에 나타나지

않음을 의미합니다.수동으로 다시 활성화해야 합니다.또한 한 SSH 세션에서 디버그가 활성화된 경우 다른 세션에는 전혀 표시되지 않습니다.**세션 디버깅**에 **따라** 참조할 수 있습니다.

SSH에서 활성화된 디버그 또는 텔넷 세션이 이 명령에 관계없이 나타나므로 디버그를 표시하려면 ASA에서 **terminal monitor** 명령을 입력할 필요가 없습니다.이 명령의 목적은 Cisco IOS 디바이스와 크게 다르며, ASA Syslog 컨피그레이션 예는 해당 기능을 자세히 설명합니다.

Syslog와 디버그 메시지 간의 차이

디버그는 ASA의 특정 프로토콜 또는 기능에 대해 지정된 메시지입니다.디버깅 수준이 없습니다. 대신 디버깅 수준이 매우 상세하고 세부 수준을 변경할 수 있습니다.또한 타임스탬프, 메시지 코드 또는 심각도 수준이 없을 수도 있습니다.이는 특정 디버그에 종속됩니다.

이 예에서는 동일한 ping 요청과 관련하여 디버깅 및 syslog 메시지 간의 차이를 보여줍니다.

다음은 debug icmp trace 명령을 입력한 후 디버그 출력**의** 예입니다.

```
ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1 seq=29 len=32

ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1 seq=29 len=32
```

다음은 동일한 ICMP 요청에 대한 **syslog** 메시지의 예입니다.

```
Jan 01 2016 13:29:22: %ASA-6-302020: Built inbound ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0

Jan 01 2016 13:29:22: %ASA-6-302021: Teardown ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0
```

디버그 수집

SSH 또는 텔넷에 대한 기본 시간 제한은 5분이며 이 시간 동안 사용하지 않으면 세션이 끊어집니다 .콘솔 연결의 기본 시간 제한은 0입니다. 즉 사용자가 수동으로 로그아웃할 때까지 로그인됩니다.

안타깝게도 로깅 기능은 특정 관리 방법에 설정된 시간 초과로 제한되므로 SSH 세션이 종료되면 디버그도 중지됩니다.

장기간 동안 디버그를 계속 수집하려면 콘솔 연결을 사용한 다음 logging debug-**trace** 명령을 사용하여 syslog 서버로 리디렉션할 수 있습니다.심각도 수준 7에서 syslog 메시지 711001이 발급되어 리디렉션됩니다. 이 메시지를 로그로 보내는 것을 중지하려면 명령 앞에 "no"를 삽입하십시오.

```
logging debug-trace
no logging debug-trace
```

버전 9.5.2에서 ASA는 시간 제한 후 디버깅을 syslog 메시지로 전송하거나 SSH/텔넷/콘솔 연결에서 로그아웃할 수 있습니다.debug-**trace persistent** 명령을 입력하면 다른 세션에서 한 세션에서 활성화된 디버그를 선택적으로 지울 수 있으며 백그라운드에서 활성 상태로 유지됩니다.이 기능을 비활성화하려면 명령 앞에 "no"를 삽입합니다.

```
logging debug-trace persistent
no logging debug-trace persistent
```

기본적으로 모든 디버그 메시지의 심각도는 7입니다. 원하지 않는 메시지에서 필터링하려면 이 메시지의 심각도를 3으로 높여 디버깅 옆에 있는 오류 메시지만 수집할 수 있습니다.이 리디렉션을 비활성화하려면 "no"를 삽입합니다.

```
logging message 711001 level 3
no logging message 711001 level 3
```

샘플 컨피그레이션

```
logging enable
logging host 10.0.0.1
logging trap errors
logging debug-trace persistent
logging message 711001 level errors
debug icmp trace
```

이 명령을 사용하면 오류 메시지와 오류로도 표시된 ICMP(Internet Control Message Protocol) 디버그를 syslog 서버에 보낼 수 있습니다.

```
Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1
 seq=29 len=32

Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1
 seq=29 len=32
```

관련 정보

- ASA Syslog 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems