ASA 처리량 및 연결 속도 문제 해결 및 패킷 캡처 분석

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance) 처리량 및 연결 속도 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco ASA(Adaptive Security Appliance)를 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.

배경 정보

일부 고객은 ASA를 처음 구축하거나 새로운 연결을 테스트할 때 문제가 발생할 수 있습니다.문제는 ASA를 통해 이동하는 연결의 TCP 처리량이 연결 경로에 없거나 ASA가 네트워크에 구현되기 전보다 훨씬 느리다는 것입니다.

예를 들어, 고객은 로우엔드 D-Link 라우터(또는 기타 라우팅 디바이스)를 ASA 5505 또는 ASA 5510으로 교체할 수 있습니다.그러나 라우터를 교체하면 연결 속도가 크게 줄어듭니다.고객은

ASA가 연결 속도를 줄였다고 믿기 때문에 Cisco TAC에 케이스를 제기할 수 있습니다.

문제 해결 방법론

네트워크에서 패킷 손실 또는 패킷 지연이 발생할 경우 TCP 흐름의 속도가 느려집니다.문제의 정확한 원인을 파악하기 위해 데이터는 해당 연결의 와이어 상에 있는 실제 TCP 패킷과 네트워크에 미치는 영향을 표시해야 합니다.일반적으로 네트워크 관리자는 FTP 파일 전송 또는 온라인 속도 테스트와 같은 특정 작업을 수행할 때 해당 문제에 대해 알림을 받습니다.대부분의 경우 문제가 재현될 수 있습니다.따라서 관리자는 근본 원인을 찾기 위해 필요한 데이터를 수집할 수 있습니다.

필요한 데이터를 수집하려면 **show tech** 명령을 테스트 전후에 ASA에서 실행해야 합니다.이 명령은 컨피그레이션 및 패킷 통계(주로 **show service-policy**에서 제공)를 표시하고 인터페이스 오류가 증가하는지 여부도 표시합니다.

문제의 원인을 완전히 진단하려면 양방향 동시 패킷 캡처(연결이 통과하는 영향을 받는 두 ASA 인터페이스에서 가져옴)가 필요합니다.

ASA에 패킷 캡처를 적용하는 방법의 예는 다음 문서를 참조하십시오.

- PIX 및 ASA를 통한 연결 문제 해결
- TAC 보안 팟캐스트 에피소드 #1 - 문제 해결을 위해 ASA 패킷 캡처 유틸리티 사용

데이터 분석

필요한 데이터를 수집하면 패킷 캡처를 사용하여 다음 중 어떤 문제가 발생했는지 확인할 수 있습니다.

- 외부 호스트의 패킷은 ASA의 외부 인터페이스에 도달하기 전에 삭제되거나 지연됩니다.
- 패킷이 ASA에 의해 지연되거나 삭제됩니다.
- 패킷은 내부 네트워크의 어딘가에서 지연되거나 삭제됩니다.

  참고:이 분석에서는 데이터가 외부 인터페이스의 호스트에서 내부 인터페이스의 호스트로 전송되는 것으로 가정합니다.

이 비디오에서는 패킷 캡처에 대한 분석을 수행하는 방법의 예를 보여줍니다.

*TCP 스트림 병합*은 이 문제와 관련된 기술적인 고려 사항입니다. ASA에서 특정 기능을 사용할 경우 방화벽은 이를 통과하는 TCP 스트림을 완전히 통합하기 때문입니다.

예를 들어 ASA가 네트워크에서 누락된 패킷을 검색하면(ASA에서 수신되지 않기 때문에) 누락된 데이터에 대해 다른 TCP 엔드포인트 대신 ACK를 전송합니다.이 시나리오는 가장 일반적입니다.ASA에서 순서가 잘못된 패킷을 발견하면 ASA는 패킷을 다시 주문하고 적절한 순서로 수신자에게 전달합니다.네트워크 삭제 또는 패킷 순서 변경이 없는 경우 이 기능을 활성화하는 데 아무런 부작용이 없습니다.두 TCP 엔드포인트에서 전송한 모든 패킷이 네트워크와 ASA를 통해 성공적으로 전달된 경우 패킷 플로우에 대해 조치를 취하지 않으므로 이 기능이 활성화되었는지 알 수 없습니다.네트워크에서 TCP 연결에 문제가 있는 경우에만 이 기능을 활성화하면 네트워크 트래픽이 더욱 느려집니다.TCP 스트림을 병합하는 작업은 ASA에서 리소스를 매우 많이 사용합니다.네트워크에서 삭제된 모든 패킷에 대해 ASA는 해당 패킷의 재전송을 TCP 패킷 요청을 전송할 뿐만 아니라 패킷이 누락된 후 발신자가 계속 전송한 패킷을 버퍼링해야 합니다.

일반적인 문제

ASA를 인접 디바이스에 연결하는 인터페이스에서 잘못 구성된 속도 및 이중 값

이 문제는 디바이스가 ASA로 교체될 때 종종 발생합니다.ASA 인터페이스의 속도 및 듀플렉스 값이 인접 디바이스의 값과 동일하지 않으면 해당 인터페이스에서 패킷이 삭제됩니다.ASA 인터페이스 및 인접 인터페이스의 속도 및 듀플렉스 값을 확인합니다.

ASA의 **show interface** 출력에서 이 문제의 증상인 명백한 오류를 확인합니다.

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0019.2f58.c324, MTU 1500
IP address 192.168.222.122, subnet mask 255.255.255.252
124047996 packets input, 35340918453 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
156918660 packets output, 40931551514 bytes, 0 underruns
1 output errors, 4286634 collisions, 0 interface resets
0 babbles, 123332 late collisions, 4752834 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/245) software (0/0)
Traffic Statistics for "Outside":
124047995 packets input, 33107957301 bytes
157041993 packets output, 38195084709 bytes
103480 packets dropped
1 minute input rate 2140 pkts/sec, 477200 bytes/sec
1 minute output rate 2630 pkts/sec, 396763 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2152 pkts/sec, 525496 bytes/sec
5 minute output rate 2701 pkts/sec, 421215 bytes/sec
5 minute drop rate, 0 pkts/sec
```

IPS 모듈에 트래픽 전송

ASA가 IPS 모듈로 트래픽을 전송하도록 구성된 경우 ASA에서 TCP 스트림 병합 기능이 연결됩니다.TCP 스트림 병합 기능에 대한 자세한 내용은 이 문서의 *데이터 분석* 섹션을 참조하십시오.

ASA Modification of TCP MSS Option으로 인해 성능이 약간 저하됨

기본적으로 ASA는 SYN 패킷의 TCP MSS 옵션을 1380으로 설정합니다.따라서 TCP 엔드포인트는 1380바이트보다 큰 TCP 세그먼트를 전송해서는 안 됩니다.이 값은 자주 사용하는 기본값 1460바이트보다 낮으며 약 6%(6%)의 TCP 성능 저하를 나타냅니다. ASA에서 최대 MSS 설정을 늘리거나 MSS 조정을 비활성화하면 성능이 향상될 수 있습니다.ASA에서 기본 명령을 수정하기 전에, 패킷이 경로에 더 캡슐화된 경우 잠재적인 조각화와 관련된 위험을 파악합니다.

자세한 내용은 *Cisco ASA 5500 Series 명령 참조*의 sysopt connection tcpmss 섹션을 참조하십시오.

관련 정보

- Cisco ASA 5500 Series 명령 참조, 8.2
- 기술 지원 및 문서 – Cisco Systems