이중 ISP 설정에서 기본 ISP 링크가 다시 온라인 상태가 된 후 ASA를 통한 UDP 트래픽이 실패합니다.

목차

소개

ASA(Adaptive Security Appliance)에 대상 서브넷당 두 개의 이그레스 인터페이스가 있고 목적지에 대한 기본 경로가 일정 시간 동안 라우팅 테이블에서 제거된 경우 기본 경로가 라우팅 테이블에 다시 추가될 때 UDP(User Datagram Protocol) 연결이 실패할 수 있습니다.TCP 연결도 문제의 영향을 받을 수 있지만, TCP가 패킷 손실을 감지하기 때문에 이러한 연결은 엔드포인트에 의해 자동으로 해제되며 경로가 변경된 후 더 최적의 경로를 사용하여 다시 구축됩니다.

이 문제는 라우팅 프로토콜이 사용되고 토폴로지 변경이 ASA의 라우팅 테이블에서 변경을 트리거하는 경우에도 확인할 수 있습니다.

시작하기 전에

요구 사항

이 문제를 해결하려면 ASA의 라우팅 테이블을 변경해야 합니다.이는 이중화된 방식으로 이중 ISP 링크 또는 ASA가 IGP(OSPF, EIGRP, RIP)를 통해 경로를 학습하는 경우 일반적으로 발생합니다.

이 문제는 기본 ISP 링크가 다시 온라인 상태가 되거나 해당 IGP에서 ASA에서 사용하던 우선순위가 더 낮은 경로가 기본 설정 하위 메트릭 경로로 대체되는 것으로 인해 재컨버전스가 확인될 때 발생합니다.그런 다음 기본 또는 기본 경로가 ASA의 라우팅 테이블에 다시 설치되면 UDP SIP 등록, GRE 등과 같은 장기 연결이 실패합니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- 모든 Cisco ASA 5500 Series Adaptive Security Appliance
- ASA 버전 8.2(5), 8.3(2)12, 8.4(1)1, 8.5(1) 이상

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

문제

라우팅 테이블 항목이 ASA의 라우팅 테이블에서 제거되고 인터페이스에 도달하기 위한 경로가 없는 경우, 해당 외부 대상을 사용하여 방화벽을 통해 구축된 연결이 ASA에서 삭제됩니다.이러한 상황은 존재하는 대상에 대한 라우팅 엔트리와 다른 인터페이스를 사용하여 연결을 다시 빌드할 수 있도록 합니다.

그러나 더 구체적인 경로가 테이블에 다시 추가되면 연결은 더 구체적인 새 경로를 사용하도록 업데이트되지 않으며 최적화되지 않은 인터페이스를 계속 사용합니다.

예를 들어 방화벽에 인터넷을 접하는 두 개의 인터페이스("외부" 및 "백업")가 있으며 이러한 두 경로는 ASA 컨피그레이션에 존재합니다.

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

외부 인터페이스와 백업 인터페이스가 모두 "up"인 경우, 방화벽을 통해 아웃바운드된 연결은 기본 메트릭이 1인 외부 인터페이스를 사용합니다. 외부 인터페이스가 종료되거나 경로를 추적하는 SLA 모니터링 기능이 추적되는 IP에 대한 연결 손실을 감지하는 경우, 백업 인터페이스가 목적지로 향하는 유일한 인터페이스이므로 외부 인터페이스를 사용하는 연결은 백업 인터페이스를 사용하여 해제되고 다시 빌드됩니다.

이 문제는 외부 인터페이스가 다시 작동되거나 추적된 경로가 다시 선호 경로가 될 때 발생합니다.라우팅 테이블은 원래 경로를 선호하도록 업데이트되지만, 기존 연결은 ASA에 계속 존재하며 백업 인터페이스를 통과하며 더 선호하는 메트릭을 사용하여 외부 인터페이스에서 삭제 및 재생성되지 않습니다.이는 백업 기본 경로가 ASA의 인터페이스별 라우팅 테이블에 여전히 존재하기 때문입니다.연결이 삭제될 때까지 연결은 선호도가 낮은 경로를 사용하여 인터페이스를 계속 사용합니다.UDP의 경우 이 값은 무한대가 될 수 있습니다.

이러한 상황은 외부 SIP 등록 또는 기타 UDP 연결과 같은 장기 연결 문제를 일으킬 수 있습니다.

솔루션

이 특정 문제를 해결하기 위해, 대상에 대한 더 선호하는 경로가 라우팅 테이블에 추가된 경우 새 인터페이스에서 연결이 해제되고 재구축되는 새로운 기능이 ASA에 추가되었습니다.기능을 활성화하려면(기본적으로 비활성화됨) 0이 아닌 시간 제한을 timeout floating-conn 명령**으로** 설정합니다.이 시간 초과(HH:MM:SS로 지정)는 더 많은 기본 경로가 라우팅 테이블에 다시 추가되면 ASA가 연결을 끊기 전에 대기하는 시간을 지정합니다.

이 CLI는 기능을 활성화하는 예입니다.이 CLI를 사용하면, 대상에 대한 더 선호되는 다른 경로가 있는 기존 연결에서 패킷이 수신되는 경우 1분 후에 연결이 해제되고(보다 선호되는 새로운 경로를 사용하여 재구축됨):

```
ASA# config terminal
ASA(config)# timeout floating-conn 0:01:00
ASA(config)# end
ASA# show run timeout
timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:01:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout xlate 0:01:00
timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00
ASA#
```

이 기능은 최신 버전의 ASA 소프트웨어를 포함하여 버전 8.2(5), 8.3(2)12, 8.4(1)1 및 8.5(1)에서 ASA 플랫폼에 추가됩니다.

이 기능을 구현하지 않는 ASA 코드 버전을 실행하는 경우, 문제를 해결하려면 **명확한 로컬 호스트 *<IP>*** 또는 **clear-conn *<IP>***를 통해 사용할 수 있는 더 나은 경로를 제공하면서도 계속 덜 선호되는 경로를 계속 사용하는 UDP 연결을 수동으로 플러시하는 것이 좋습니다.

명령 참조에는 이 새 기능이 시간 제한 섹션 아래에 나열됩니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems