VPN 클라이언트 연결 해제 시 트래픽 루프로 인해 ASA의 CPU 사용량이 높음

목차

소개

이 문서에서는 VPN 클라이언트가 원격 액세스 VPN 헤드엔드로 실행되는 Cisco ASA(Adaptive Security Appliance)에서 연결을 끊을 때 발생하는 일반적인 문제에 대해 설명합니다.이 문서에서는 VPN 사용자가 ASA 방화벽에서 연결을 끊을 때 트래픽 루프가 발생하는 상황에 대해서도 설명합니다.이 문서에서는 VPN에 대한 원격 액세스를 구성하거나 설정하는 방법, 특정 공통 라우팅 컨피그레이션에서 발생하는 특정 상황에만 대해 다루지 않습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA의 원격 액세스 VPN 컨피그레이션
- 기본 레이어 3 라우팅 개념

사용되는 구성 요소

이 문서의 정보는 ASA 코드 버전 9.1(1)을 실행하는 ASA 모델 5520을 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.

관련 제품

이 문서는 다음 하드웨어 및 소프트웨어 버전과 함께 사용할 수 있습니다.

- 모든 ASA 모델
- 모든 ASA 코드 버전

배경 정보

사용자가 원격 액세스 VPN 집중기로 ASA에 연결할 때 ASA는 트래픽을 외부 인터페이스(인터넷)에서 해당 VPN 클라이언트로 라우팅하는 호스트 기반 경로를 ASA 라우팅 테이블에 설치합니다. 해당 사용자가 연결을 끊으면 해당 경로가 테이블에서 제거되고 내부 네트워크의 패킷(연결이 끊긴 VPN 사용자로 향하는)이 ASA와 내부 라우팅 디바이스 간에 루프될 수 있습니다.

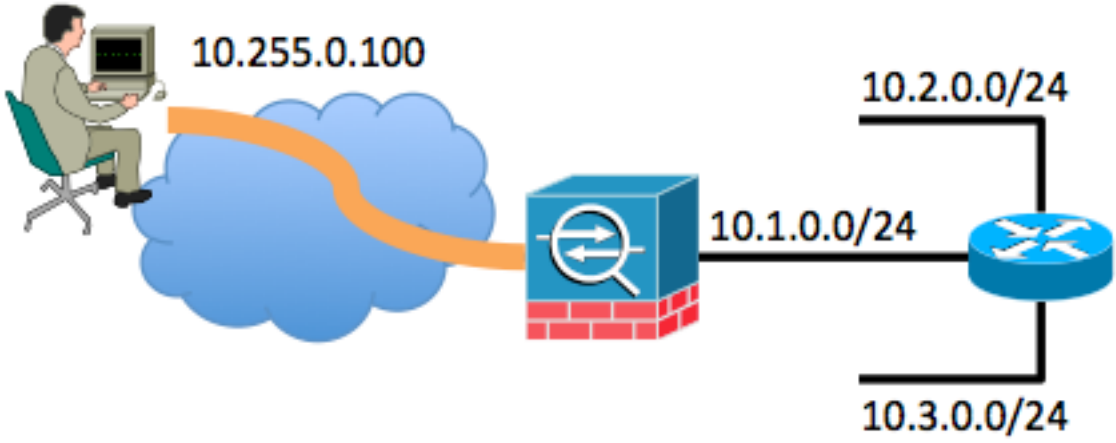
또 다른 문제는 ASA가 내부 네트워크를 향하는 유니캐스트 프레임으로 직접(네트워크) 브로드캐스트 패킷(VPN 클라이언트 제거로 생성)을 전달할 수 있다는 점입니다.그러면 ASA로 다시 전달될 수 있습니다. 그러면 TTL(Time to Live)이 만료될 때까지 패킷이 반복됩니다.

이 문서에서는 이러한 문제에 대해 설명하고 어떤 구성 기술을 사용하여 문제를 방지할 수 있는지 보여줍니다.

문제/장애:내부 네트워크 내에서 연결이 끊긴 VPN 클라이언트 루프로 향하는 패킷

원격 액세스 VPN 사용자가 ASA 방화벽에서 연결을 끊으면 내부 네트워크에 여전히 있는 패킷(연결이 끊긴 사용자를 위한 패킷) 및 할당된 IP VPN 주소가 내부 네트워크 내에서 루프될 수 있습니다.이러한 패킷 루프는 IP 패킷 헤더의 IP TTL 값이 0으로 감소하여 루프가 중지될 때까지 ASA의 CPU 사용량이 증가할 수 있으며, 사용자가 다시 연결되고 IP 주소가 VPN 클라이언트에 다시 할당됩니다.

이 시나리오를 더 잘 이해하려면 다음 토폴로지를 고려하십시오.



이 예에서는 원격 액세스 클라이언트에 10.255.0.100의 IP 주소가 할당되었습니다. 이 예에서 ASA는 라우터와 함께 동일한 내부 네트워크 세그먼트에 연결됩니다.라우터에 2개의 추가 레이어 3 네트워크 세그먼트가 연결되어 있습니다.예에는 ASA 및 라우터의 관련 인터페이스(라우팅) 및 VPN 컨피그레이션이 나와 있습니다.

ASA 컨피그레이션 하이라이트는 다음 예에 나와 있습니다.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
!
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

다음 예에서는 라우터 컨피그레이션 하이라이트를 보여줍니다.

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
 description connected to network segment
 ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
 description connected to other network segment
 ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

ASA 내부에 연결된 라우터의 라우팅 테이블에는 ASA 내부 인터페이스 10.1.0.1을 가리키는 기본 경로가 있습니다.

사용자가 VPN을 통해 ASA에 연결되어 있는 동안 ASA 라우팅 테이블은 다음과 같습니다.

```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

이 문제는 원격 액세스 VPN 사용자가 VPN에서 연결을 끊을 때 발생합니다.이때 호스트 기반 경로가 ASA 라우팅 테이블에서 제거됩니다.네트워크 내부의 호스트가 VPN 클라이언트로 트래픽을 전송하려고 시도하면 해당 트래픽은 라우터에서 ASA 내부 인터페이스로 라우팅됩니다.이 일련의 단계가 발생합니다.

1. 10.255.0.100으로 향하는 패킷이 ASA의 내부 인터페이스에 도착합니다.

2. 표준 ACL 검사가 수행됩니다.

3. 이 트래픽에 대한 이그레스 인터페이스를 확인하기 위해 ASA 라우팅 테이블이 선택됩니다.

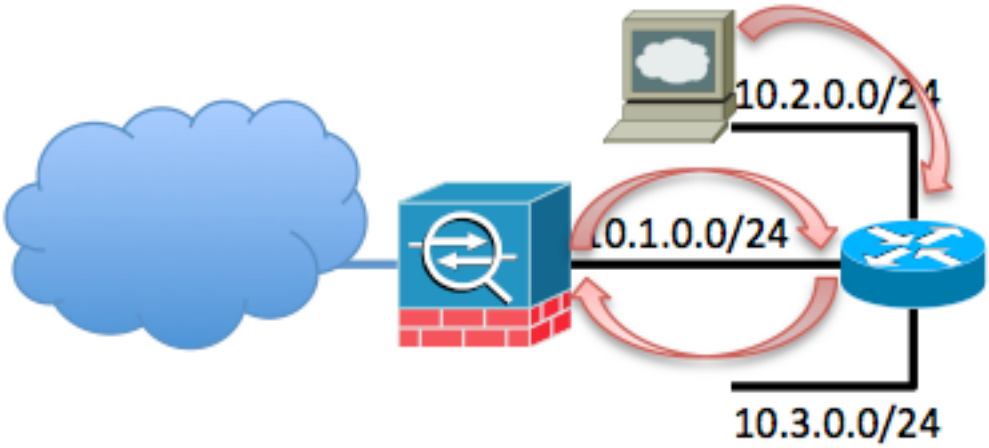
4. 패킷의 대상은 라우터를 향하는 내부 인터페이스에서 다시 가리키는 광범위한 10.0.0.0/8 경로와 일치합니다.

5. ASA는 헤어피닝 트래픽이 허용되는지 확인합니다. **동일한 보안 허용**을 검색하여 **인터페이스 내**에서 허용되는지 확인합니다.

6. 연결은 내부 인터페이스와 내부 간에 구축되며 패킷은 다음 홉으로 라우터로 다시 전송됩니다.

7. 라우터는 ASA를 향하는 인터페이스에서 10.255.0.100으로 향하는 패킷을 수신합니다.라우터는 라우팅 테이블에서 적합한 다음 홉을 확인합니다.라우터는 다음 홉이 ASA 내부 인터페이스임을 확인하고 패킷이 ASA로 전송됩니다.
8. 1단계로 돌아갑니다.

다음은 예입니다.



이 루프는 이 패킷의 TTL이 0으로 감소할 때까지 발생합니다. ASA 방화벽은 패킷을 처리할 때 기본적으로 TTL 값을 감소시키지 **않습니다**.라우터는 패킷을 라우팅할 때 TTL을 줄입니다.이렇게 하면 이 루프가 무기한 발생하지 않지만 이 루프는 ASA의 트래픽 로드를 증가시키고 CPU 사용량이 급증하게 됩니다.

문제/장애:직접(네트워크) VPN 클라이언트에서 생성된 브로드캐스트 패킷은 내부 네트워크에서 반복됨

이 문제는 첫 번째 문제와 유사합니다.VPN 클라이언트가 지정된 IP 서브넷(이전 예의 10.255.0.255)에 지정 브로드캐스트 패킷을 생성하는 경우 해당 패킷은 ASA가 내부 라우터에 유니캐스트 프레임으로 전달될 수 있습니다.그런 다음 내부 라우터가 ASA로 다시 전달하여 TTL이 만료될 때까지 패킷이 루프됩니다.

이 일련의 이벤트가 발생합니다.

1. VPN 클라이언트 시스템은 네트워크 브로드캐스트 주소 10.255.0.255으로 향하는 패킷을 생

성하고 패킷이 ASA에 도착합니다.
2. ASA는 라우팅 테이블 때문에 이 패킷을 유니캐스트 프레임으로 처리하고 내부 라우터로 전달합니다.

3. 패킷을 유니캐스트 프레임으로도 처리하는 내부 라우터는 패킷의 TTL을 줄이고 이를 ASA로 다시 전달합니다.

4. 패킷의 TTL이 0으로 감소할 때까지 프로세스가 반복됩니다.

문제 해결

이 문제에 대한 몇 가지 잠재적인 해결책이 있습니다.네트워크 토폴로지 및 특정 상황에 따라 한 솔루션을 다른 솔루션보다 쉽게 구현할 수 있습니다.

솔루션 1 - Null0 인터페이스에 대한 고정 경로(ASA 버전 9.2.1 이상)

트래픽을 **Null0** 인터페이스로 전송하면 지정된 네트워크로 향하는 패킷이 삭제됩니다.이 기능은 BGP(Border Gateway Protocol)에 대해 RTBH(Remotely Triggered Black Hole)를 구성할 때 유용합니다. 이 경우 원격 액세스 클라이언트 서브넷에 대해 Null0으로 경로를 구성하는 경우 더 구체적인 경로(역방향 경로 주입 방식으로 제공)가 없는 경우 ASA가 해당 서브넷의 호스트로 향하는 트래픽을 강제로 삭제합니다.

```
route Null0 10.255.0.0 255.255.255.0
```

솔루션 2 - VPN 클라이언트에 다른 IP 풀 사용

이 솔루션은 원격 VPN 사용자에게 내부 네트워크 서브넷과 겹치지 않는 IP 주소를 할당하는 것입니다.그러면 VPN 사용자가 연결되지 않은 경우 ASA가 해당 VPN 서브넷으로 향하는 패킷을 다시 내부 라우터로 전달하지 못하게 됩니다.

솔루션 3 - 내부 경로에 대해 ASA 라우팅 테이블을 더욱 구체적으로 지정

이 솔루션은 ASA의 라우팅 테이블에 VPN IP 풀과 겹치는 매우 광범위한 경로가 없는지 확인하는 것입니다.이 특정 네트워크 예에서는 ASA에서 10.0.0.0/8 경로를 제거하고 내부 인터페이스 외부에 있는 서브넷에 대해 좀 더 구체적인 고정 경로를 구성합니다.서브넷 수 및 네트워크 토폴로지에 따라 이는 많은 고정 경로일 수 있으며 가능하지 않을 수 있습니다.

솔루션 4 - 외부 인터페이스에서 VPN 서브넷에 대해 더 구체적인 경로 추가

이 솔루션은 이 문서에 설명된 다른 솔루션보다 복잡합니다.Cisco에서는 이 섹션의 뒷부분에서 설명한 상황으로 인해 먼저 다른 솔루션을 사용할 것을 권장합니다.이 솔루션은 ASA가 VPN IP 서브넷에서 제공된 IP 패킷을 다시 내부 라우터로 전달하지 못하도록 합니다.외부 인터페이스에서 VPN 서브넷에 대해 더 구체적인 경로를 추가하는 경우 이 작업을 수행할 수 있습니다.이 IP 서브넷은 외부 VPN 사용자용으로 예약되어 있으므로 이 VPN IP 서브넷의 소스 IP 주소가 있는 패킷은 ASA 내부 인터페이스에서 인바운드에 도달해서는 안 됩니다.이를 위한 가장 쉬운 방법은 업스트림 ISP 라우터의 다음 hop IP 주소를 사용하여 외부 인터페이스에서 원격 액세스 VPN IP 풀에 대한 경로를 추가하는 것입니다.

이 네트워크 토폴로지 예에서는 해당 경로가 다음과 같습니다.

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

이 경로 외에 ASA가 외부 인터페이스에 존재하는 더 선호하는 경로로 인해 VPN IP 서브넷에서 소싱된 내부 인터페이스에서 수신되는 모든 패킷을 삭제하도록 하려면 **ip verify reverse-path inside** 명령을 추가합니다.

```
ip verify reverse-path inside
```

이러한 명령을 구현한 후에는 사용자가 연결될 때 ASA 라우팅 테이블이 이와 비슷하게 보입니다.

```
ASA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

VPN 클라이언트가 연결되면 해당 VPN IP 주소에 대한 호스트 기반 경로가 테이블에 표시되며 기본 설정입니다.VPN 클라이언트가 연결을 끊으면 내부 인터페이스에 도착하는 클라이언트 IP 주소에서 제공된 트래픽이 라우팅 테이블을 기준으로 확인되고 ip verify reverse-path inside 명령으로 인해 삭제됩니다.

VPN 클라이언트가 VPN IP 서브넷에 대한 지정 네트워크 브로드캐스트를 생성하는 경우 해당 패킷이 내부 라우터로 전달되고 라우터가 다시 ASA로 전달되며, 여기서 **ip verify reverse-path inside** 명령으로 인해 **삭제됩니다**.

> **참고:**이 솔루션이 구현된 후 **동일한 보안 permit intra-interface** 명령이 컨피그레이션에 있고 액세스 정책이 이를 허용하는 경우, 연결되지 않은 사용자의 VPN IP 풀에 있는 IP 주소로 향하는 VPN 사용자로부터의 트래픽은 clear-text로 외부 인터페이스에서 다시 라우팅될 수 있습니다.이는 드문 상황이며 VPN 정책 내에서 vpn-filters를 사용하여 완화될 수 있습니다.이 상황은 **same-security permit intra-interface** 명령이 ASA 컨피그레이션에 있는 경우에만 발생합니다.
>
> 마찬가지로, 내부 호스트가 VPN 풀의 IP 주소로 향하는 트래픽을 생성하고 해당 IP 주소가 원격 VPN 사용자에게 할당되지 않은 경우 해당 트래픽이 ASA 외부에서 일반 텍스트로 이그레스될 수 있습니다.