IOS 및 IOS XE 라우터에서 P2P 통신을 활성화하기 위한 NAT 이해

목차

소개

이 문서에서는 STUN(Session Traversal Utilities for NAT) 서버의 필요성, STUN 서버와 관련된 NAT(Network Address Translation) 설정 유형, NAT로 인해 이 설정 및 솔루션에서 문제가 발생하는 방식 등에 대해 설명합니다.

배경 정보

NAT 장치의 주요 목적은 LAN(Local-Area Network)에서 사설 IP 주소를 사용하는 장치가 인터넷과 같은 공용 주소 공간의 장치와 통신할 수 있도록 허용하는 것입니다. 그러나 NAT 장치는 내부 호스트가 공용 공간과 연결할 수 있도록 허용해야 하지만, 최종 사용자가 클라이언트와 서버 역할을 모두 해야 하는 VoIP, 게임, WebRTC 및 파일 공유와 같은 P2P(Point-to-Point) 애플리케이션에 대해서는 NAT가 그러한 UDP 연결을 설정하는 데 어려움을 줍니다. 이러한 애플리케이션이 작동하게 하려면 일반적으로 NAT 통과 기술이 필요합니다.

NAT 접근 필요

인터넷상의 실시간 음성 및 화상 통신 현재 주류 오늘날 VoIP 통화를 지원하는 여러 인기 인스턴트 메신저(IM)가 있습니다. VoIP를 처음 채택하는 데 큰 걸림돌은 대부분의 PC 또는 기타 장치가 방화벽 뒤에 앉아 프라이빗 IP 주소를 사용한다는 사실이었습니다. 네트워크의 여러 개인 주소(IP 주소 및 포트)가 방화벽을 통해 단일 공용 주소에 매핑됩니다. NAT. 그러나 엔드 디바이스는 공용 주소를 인식하지 못하므로, VoIP 통신에서 광고하는 사설 주소의 원격 당사자로부터 음성 트래픽을 수신할 수 없습니다.

일방 UNSAF(Self-Address Fixing) 프로세스는 일부 시작 엔드포인트가 다른 엔드포인트에 알려진 주소(및 포트)를 확인하거나 수정하려고 시도하는 프로세스입니다. 예를 들어, u프로토콜 교환에서 주소 데이터를 사용하거나, 연결을 수신하는 공용 주소를 광고합니다.

논의 중인 P2P 연결은 따라서 UNSAF 프로세스입니다. P2P 애플리케이션이 피어링 세션을 설정하고 유지하는 한 가지 일반적인 방법 NAT 친화적(NAT-friendly)은 공용 주소 지정 가능 랑데부 서버를 사용하여 등록 및 피어 검색 목적.

NAT용 세션 이동 유틸리티

RFC 5389에 따라 STUN은 NAT를 처리하는 툴을 제공합니다. 엔드포인트가 전용 IP 주소 및 포트에 해당하는 NAT 디바이스에서 할당한 IP 주소 및 포트를 확인할 수 있는 수단을 제공합니다. 또한 엔드포인트가 NAT 바인딩을 활성 상태로 유지할 수 있는 방법도 제공합니다.

NAT 구현 유형

UDP의 NAT 처리는 구현에 따라 달라지는 것으로 관찰되었습니다. 구현에서 관찰된 4가지 치료는 다음과 같습니다.

Full Cone: Full Cone NAT는 동일한 내부 IP 주소 및 포트의 모든 요청이 동일한 외부 IP 주소 및 포트에 매핑되는 NAT입니다. 또한 외부 호스트는 패킷을 내부 호스트로 전송할 수 있으며 매핑된 외부 주소로 패킷을 전송합니다.

제한된 원추: 제한된 원추 NAT는 동일한 내부 IP 주소 및 포트의 모든 요청이 동일한 외부 IP 주소 및 포트에 매핑되는 원추 NAT입니다. 풀 콘 NAT와 달리 외부 호스트(IP 주소 X 포함)는 내부 호스트가 이전에 패킷을 IP 주소 X로 보낸 경우에만 내부 호스트로 패킷을 전송할 수 있습니다.

Port Restricted Cone(포트 제한 콘): 포트 제한 콘 NAT는 제한 콘 NAT와 같지만, 제한에는 포트 번호가 포함됩니다. 특히, 외부 호스트는 내부 호스트가 이전에 패킷을 IP 주소 X 및 포트 P로 전송한 경우에만 소스 IP 주소 X 및 소스 포트 P를 사용하여 패킷을 내부 호스트로 전송할 수 있습니다.

대칭: 대칭 NAT는 동일한 내부 IP 주소 및 포트에서 특정 목적지 IP 주소 및 포트로의 모든 요청이 동일한 외부 IP 주소 및 포트에 매핑되는 대칭 NAT입니다. 동일한 호스트가 동일한 소스 주소 및 포트로 패킷을 전송하지만 다른 대상으로 전송할 경우 다른 매핑이 사용됩니다. 또한 패킷을 수신한 외부 호스트만 내부 호스트로 UDP 패킷을 다시 전송할 수 있습니다.

소스(A, Pa)(A는 IP 주소, Pa는 소스 포트)가 NAT 디바이스를 통해 목적지(B, Pb) 및 (C, PC)와 통신하는 토폴로지를 고려하십시오.

NAT 구현 유형	퍼블릭 소스 시간 대상: (B, Pb)	(으)로 이동할 때 공용 소스C, Pc)	대상 가능(예: (B, Pb) (A, Pa)로 트래픽을 전송합니까?
전체 원뿔	(X1,Px1)	(X1,Px1)	예
제한된 원뿔	(X1,픽셀1)	(X1,픽셀1)	(A, Pa)가 먼저 B에게 트래픽을 보낸 경우에만
포트 제한 원뿔	(X1,픽셀1)	(X1,픽셀1)	(A, Pa)가 먼저 (B, Pb)에 트래픽을 전송한 경우에만
대칭	(X1,픽셀1)	(X2,Px2)	(A, Pa)가 먼저 (B, Pb)에 트래픽을 전송한 경우에만

NAT 통과 및 대칭 NAT 문제

STUN 서버는 STUN 클라이언트에서 보낸 STUN 바인딩 요청에 응답하고 클라이언트의 공용 IP/포트를 제공합니다. 이 주소/포트는 조합은 STUN 클라이언트가 피어 투 피어 통신에서 사용합니다 신호. 그러나이제 엔드호스트 동일한 개인 주소/포트를 사용합니다(이 경우 경계 공용 IP/포트에 연결 STUN 응답에서 제공) NAT 장치는 대칭 NAT인 경우 동일한 IP로 변환하지만 다른 포트로 변환합니다 단순해나명시 을(를) 사용합니다. 이렇게 하면 UDP 통신이 끊어집니다. 신호 IP를 기반으로 연결을 설정했습니다.이전 포트.

Cisco IOS® 라우터 NAT 단순해나명시 PAT를 수행하는 경우 기본적으로 대칭입니다. 기타e앞, UDP 연결 문제가 발생할 수 있습니다 라우터를 통해 NAT.

그러나 Cisco IOS-XE 라우터가 PAT를 수행할 때 구현하는 NAT는 대칭적이지 않습니다. 두 가지 다른 것을 보낼 때 소스 IP와 포트는 동일하지만 대상이 다른 스트림에서는 소스가 동일한 내부 전역 IP와 포트에 NATE됩니다.

문제의 해결책

이 설명에서는 이(가) 다음을 수행하면 문제가 해결될 수 있습니다. 엔드포인트 독립적 매핑합니다.

RCFC에 따라 4787: 포함 EIM(Endpoint-Independent Mapping)에서는 동일한 내부 IP 주소 및 포트(X:x)을(를) 외부 IP 주소 및 포트에 연결합니다.

클라이언트에서 endhost가 **nc -p 23456 10.0.0.4 40000** 및 **nc -p 23456 10.0.0.5 50000**을 두 개의 다른 터미널 창에서 실행할 때 EIM을 사용하는 경우 NAT 변환의 결과는 다음과 같습니다.

```
Pro Inside global       Inside local            Outside local        Outside global

tcp 10.0.0.1:23456   192.168.0.2:23456  10.0.0.4:40000 10.0.0.4:40000

tcp 10.0.0.1:23456   192.168.0.2:23456  10.0.0.5:50000 10.0.0.5:50000
```

여기서 동일한 소스 주소와 포트를 갖는 서로 다른 트래픽 흐름이 목적지 포트/주소에 관계없이 동일한 주소/포트로 변환됨을 확인할 수 있습니다.

Cisco IOS 라우터에서 이 명령을 사용하여 엔드포인트에 구애받지 않는 포트 할당을 활성화할 수 있습니다 **ip nat service enable-sym- 포트.**

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/iadnat-fpg-port-alloc.html

요약

Cisco IOS NAT 구현은 PAT(Port Address Translation)를 사용할 때 기본적으로 대칭적이며, NAT 통과를 위해 STUN과 같은 서버가 필요한 P2P UDP 트래픽을 전달할 때 문제가 발생할 수 있습니다. 이 작업을 수행하려면 NAT 디바이스에서 EIM을 명시적으로 구성해야 합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.