Cisco ONS 15454 및 NAT

목차

소개

이 문서에서는 다양한 유형의 NAT(Network Address Translation)에 대해 설명하고 각 NAT 유형을 해당 유형을 지원하는 관련 ONS 15454 소프트웨어 버전에 매핑합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ONS 15454
- CTC
- NAT

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 모든 버전의 Cisco ONS 15454

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.

표기 규칙

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

배경 정보

대부분의 경우 현장에서 서로 다른 NAT 시나리오가 실행 중이며 제대로 작동하지 않습니다.이러한 시나리오의 대부분은 증상을 통해 식별할 수 있습니다.대부분의 문제는 NE(Network Element)에서 Cisco CTC(Transport Controller) 워크스테이션에 대한 연결을 다시 시작할 수 없기 때문입니다.

CTC가 NAT의 특정 컨피그레이션을 지원하지 않는 경우 CTC는 특정 간격으로 지속적으로 노드를 삭제하고 다시 연결합니다.최신 버전에서는 CTC가 보기에서 드롭하지 않고 연결을 해제할 수 있습니다.이러한 버전에서는 CTC를 통해 노드와 상호 작용하는 동안 이 문제를 확인할 수 있습니다.

또한 액세스 목록이 보안을 지정하는 외부 방화벽의 잘못된 컨피그레이션으로 인해 동일한 증상이 발생합니다.Access Lists(액세스 목록)에서는 NE가 정의된 IP 주소 및/또는 포트에 대한 특정 연결을 다시 CTC Workstation으로 시작할 수 없습니다.외부 방화벽 시간 제한 설정이 너무 짧을 때도 자주 연결이 끊어질 수 있습니다.

ONS 15454에서 사용할 수 있는 샘플 방화벽 액세스 목록은 Cisco ONS 15454 Reference Manual, Release 5.0의 External Firewalls 섹션을 참조하십시오.

NAT

NAT를 사용하면 단일 디바이스(예: 라우터)가 인터넷과 로컬 네트워크 간에 에이전트 역할을 수행할 수 있습니다.이 섹션에서는 다양한 유형의 NAT에 대해 설명합니다.

자세한 내용은 RFC 2663 - IP Network Address Translator 용어 및 고려 사항을 참조하십시오 .

기존 NAT

기존 NAT를 사용하면 프라이빗 네트워크 내의 호스트가 외부 네트워크의 호스트에 투명하게 액세스할 수 있습니다.기존 NAT는 프라이빗 네트워크에서 아웃바운드 세션을 시작합니다.

이 섹션에서는 기존 NAT의 두 가지 변형에 대해 간략하게 설명합니다.

- **기본 NAT**:기본 NAT는 외부 주소 블록을 별도로 설정합니다.기본 NAT는 호스트가 외부 도메인과 세션을 시작할 때 사설 도메인의 호스트 주소를 변환하기 위해 이러한 주소를 사용합니다.
- **NAPT(Network Address Port Translation)**:NAPT는 번역의 개념을 한 단계 더 확장합니다.또한 NAPT는 전송 식별자(예: TCP 및 UDP 포트 번호, ICMP 쿼리 식별자)를 변환합니다.이러한 변환은 여러 개인 호스트의 전송 식별자를 단일 외부 주소의 전송 식별자로 멀티플렉싱합니다.**참고:** NAPT는 PAT(Port Address Translation)라고도 합니다.

양방향 NAT

외부 네트워크의 디바이스는 내부의 디바이스와 트랜잭션을 시작합니다.이 시작을 허용하기 위해 NAT의 기본 버전이 고급 기능을 포함하도록 향상되었습니다.이러한 개선 사항은 대부분 양방향 NAT라고 하지만, 양방향 NAT 및 인바운드 NAT라고도 합니다.양방향 NAT를 사용하면 공용 네트워크 및 프라이빗 네트워크의 호스트에서 세션을 시작할 수 있습니다.사설 네트워크 주소는 어느

방향으로든 연결을 설정할 때 정적으로 또는 동적으로 전역 고유 주소에 바인딩됩니다.

인바운드 트랜잭션에 대한 NAT의 성능은 아웃바운드 NAT보다 더 어렵습니다.그 이유는 내부 네트워크가 일반적으로 외부 디바이스의 IP 주소를 알고 있기 때문입니다. 이러한 디바이스는 공개이기 때문입니다.그러나 외부 네트워크는 내부 네트워크의 개인 주소를 알지 못합니다.외부 네트워크에서 사설 네트워크의 IP 주소를 인식하더라도 이러한 IP 주소를 외부에서 시작하는 IP 데이터그램의 대상으로 지정할 수 없습니다. 라우팅할 수 없기 때문입니다.

다음 두 가지 방법 중 하나를 사용하여 숨겨진 주소 문제를 해결할 수 있습니다.

- 정적 매핑
- TCP/IP DNS(Domain Name System)

참고: 이 문서에서 양방향 NAT는 기본 NAT를 의미하지만 기본 NAT는 양방향 NAT를 의미하지는 않습니다.

Twice NAT

Twice NAT는 NAT의 변형입니다.Twice NAT는 데이터그램이 주소 영역을 교차할 때 소스 주소와 대상 주소를 모두 수정합니다.이 개념은 주소(소스 또는 대상) 중 하나만 변환하는 기존 NAT 및 양방향 NAT와 대조적입니다.

ONS 15454 및 NAT 호환성

다음 표에서는 ONS 15454 및 NAT 호환성을 보여 줍니다.

NAT 유형	CTC 보기	GNE(Gateway Network Element)의 인식	지원되는 CTC 버전
기본 NAT	GNE IP	변환된 IP	릴리스 3.3
NAPT	GNE IP	변환된 IP	릴리스 4.0
양방향 NAT	변환된 IP	CTC IP	릴리스 5.0
Twice NAT	변환된 IP	변환된 IP	릴리스 5.0

문제 해결

NE와 CTC 간의 통신 문제가 발생하는 경우 fhDebug 명령의 출력에는 다음 오류 메시지가 포함됩니다.

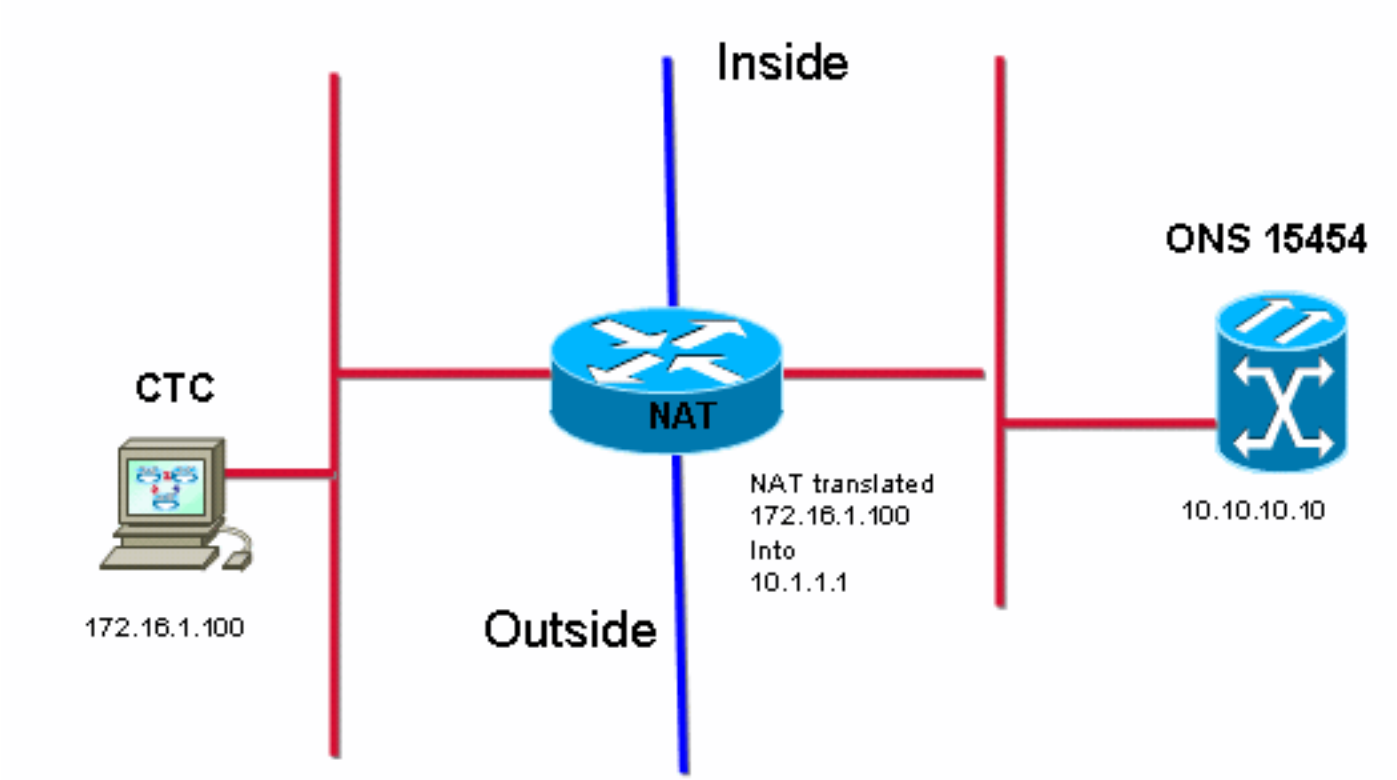
```
OCT 27 18:35:37.09 UTC ERROR     ObjectChange.cc:432   tEventMgr
 CORBA::NO_IMPLEMENT/0x3d0004 updating [192.168.1.100:EventReceiver].  Marking c

OCT 27 18:36:17.09 UTC DEBUG        AlarmImpl.cc:353   tEventMgr
 Removing corba client [192.168.1.100:EventReceiver] from auton msg list
```

여러 가지 이유로 이 오류가 발생할 수 있습니다.그러나 오류가 정기적으로 예측 가능한 간격(일반적으로 2분 또는 4분)으로 발생하는 경우 CTC가 지원하지 않는 NAT 유형 또는 필요한 포트 권한이 없는 방화벽이 있을 수 있습니다.

172.16.1.100은 CTC 워크스테이션의 IP 주소이고 10.1.1.1은 NAT 주소인지 확인합니다(그림 1 참조).

그림 1 - 토폴로지



다음은 inetstatShow 명령의 부분 **출력입니다**.

```
-> inetstatShow
Active Internet connections (including servers)
PCB      Typ Rx-Q Tx-Q Local Address      Foreign Address (state)
-------- --- ---- ---- ------------------ --------------- -------
2145984 TCP    0   0 10.10.10.10:1052   10.1.1.1:1029   SYN_SENT
21457f8 TCP    0   0 10.10.10.10:80     10.1.1.1:1246   TIME_WAIT
2145900 TCP    0   0 10.10.10.10:57790  10.1.1.1:1245   ESTABLISHED --- ISP assigned address
21453d8 TCP    0   0 10.10.10.10:80     10.1.1.1:1244   TIME_WAIT
2144f34 TCP    0   0 10.10.10.10:80     10.1.1.1:1238   TIME_WAIT
2144eb0 TCP    0   0 10.10.10.10:1080   10.1.1.1:1224   ESTABLISHED --- ISP assigned address
```

이 출력에는 이 주소의 증거가 표시되지 않습니다.출력에는 ISP에서 사용하는 공용 주소가 표시되며, 이는 기존 NAT 시나리오의 증거입니다.

양방향 NAT 및 Twice NAT를 식별하려면 CTC 워크스테이션과 동일한 네트워크 세그먼트에서 스니퍼 추적이 필요합니다.CTC 워크스테이션에서 실행되는 스니퍼가 가장 적합합니다.

관련 정보

- Cisco ONS 15454 참조 설명서, 릴리스 5.0
- 기술 지원 및 문서 – Cisco Systems