Cisco ONS 15454 en NAT

Inhoud

Inleiding

In dit document worden de verschillende typen netwerkadresomzetting (NAT) beschreven en elk type NAT in kaart gebracht in de relevante ONS 15454-softwareversie die dit type ondersteunt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ONS 15454 kaart
- CTC
- NAT

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Alle versies van Cisco ONS 15454

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

In veel gevallen zijn er verschillende NAT-scenario's in het veld en werken deze niet goed. Je kunt de meeste van deze scenario's identificeren door de symptomen. De meeste problemen vloeien voort uit het onvermogen van het Network Element (NE) om een verbinding terug te openen naar het Cisco Transport Controller-werkstation (CTC).

Wanneer CTC een bepaalde configuratie van NAT niet ondersteunt, daalt CTC consequent en verbindt ze met knooppunten met specifieke intervallen opnieuw. In nieuwere versies kan CTC van de ontconnecties herstellen zonder van beeld te laten vallen. In dergelijke versies kunt u dit probleem tijdens interactie met het knooppunt merken via CTC.

De zelfde symptomen komen ook voor door onjuiste configuraties van de externe firewall waar de lijsten van de Toegang veiligheid voorschrijven. De toegangslijsten staan het netwerk niet toe om bepaalde verbindingen naar of van bepaalde IP-adressen en/of poorten te openen, terug naar het CTC-werkstation. Frequente afsluiten kan ook voorkomen als de externe instellingen van de firewall te kort zijn.

Voor voorbeelden van toegangslijsten voor firewalls die u kunt gebruiken met de ONS 15454, raadpleegt u het externe gedeelte van Cisco ONS 15454 Referentiekaart, release 5.0.

NAT

NAT staat één apparaat toe, bijvoorbeeld, een router, om als agent tussen het Internet en een lokaal netwerk te handelen. In deze sectie worden de verschillende typen NAT beschreven.

Raadpleeg voor meer informatie RFC 2663 - IP-netwerkadresomzetting in terminologie en overwegingen .

Traditionele NAT

Traditionele NAT staat hosts binnen een privaat netwerk toe om op transparante wijze toegang te krijgen tot hosts in het externe netwerk. Traditionele NAT initieert uitgaande sessies van het particuliere netwerk.

In dit gedeelte worden de twee variaties van Traditional NAT kort beschreven:

- **Basis NAT**: Basic NAT vernietigt een blok externe adressen. Basis NAT gebruikt deze adressen om adressen van hosts in een privé domein te vertalen wanneer de hosts sessies met het externe domein initiëren.
- **Network-adresomzetting (NAPT)**: Het NAPT breidt het begrip vertaling nog een stap verder uit. NAPT vertaalt ook transportidentificatoren, bijvoorbeeld TCP- en UDP-poortnummers en ICMP-query-identificatoren. Deze vertaling vermenigvuldigt de transportkenmerken van een aantal particuliere hosts in de transportkenmerken van één extern adres.**Opmerking:** NAPT

wordt ook poortadresomzetting (PAT) genoemd.

Bi-directionele NAT

Een apparaat op het buitennetwerk initieert een transactie met een apparaat binnen. Om deze start mogelijk te maken, werd de basisversie van NAT uitgebreid met geavanceerde mogelijkheden. Deze verbetering wordt meest bekend als bidirectionele NAT, maar wordt ook aangeduid als tweevoudige NAT en inkomende NAT. Met een bidirectionele NAT kunt u sessies van hosts in het openbare netwerk en in het particuliere netwerk initiëren. De privé netwerkadressen zijn gebonden aan globaal unieke adressen, statisch of dynamisch aangezien u verbindingen in één van beide richtingen instelt.

De prestaties van NAT bij inkomende transacties zijn moeilijker dan bij uitgaande NAT. De reden is dat het binnennetwerk over het algemeen het IP adres van buitenapparaten kent, omdat deze apparaten openbaar zijn. Het externe netwerk kent echter niet de privéadressen van het interne netwerk. Zelfs als het externe netwerk zich bewust is van de IP adressen van privé netwerken, kunt u deze IP adressen nooit specificeren als het doel van een IP datagram dat u van buiten initieert, omdat ze niet routeerbaar zijn.

U kunt één van deze twee methoden gebruiken om het verborgen adresprobleem op te lossen:

- Statische mapping
- TCP/IP-domeinnaamsysteem (DNS)

Opmerking: In dit document impliceert bidirectionele NAT basis-NAT, maar fundamentele NAT niet tweerichtingsverkeer.

Twice NAT

Twice NAT is een variatie van NAT. Twice NAT wijzigt zowel de bron- als doeladressen wanneer een datagram adresgebieden overschrijdt. Dit concept staat in tegenstelling tot Traditional NAT en Bi-Directional NAT, die slechts één van de adressen (bron of bestemming) vertalen.

ONS 15454 kaart en NAT-compatibiliteit

In deze tabel worden de ONS 15454 en NAT-compatibiliteit weergegeven:

Type NAT	CTC-bestanden	GNE Series-netwerkelement (Gateway Network Element)	Ondersteunde CTC-versie
Basis NAT	GNE IP	Vertaalde IP	release 3.3
NAPT	GNE IP	Vertaalde IP	release 4.0
Bi-directionele NAT	Vertaalde IP	CTC-IP	release 5.0
Twice NAT	Vertaalde IP	Vertaalde IP	release 5.0

Problemen oplossen

In het geval van een communicatieprobleem tussen het netwerk en de CTC, bevat de uitvoer van de opdracht **fhDebug** deze foutmelding:

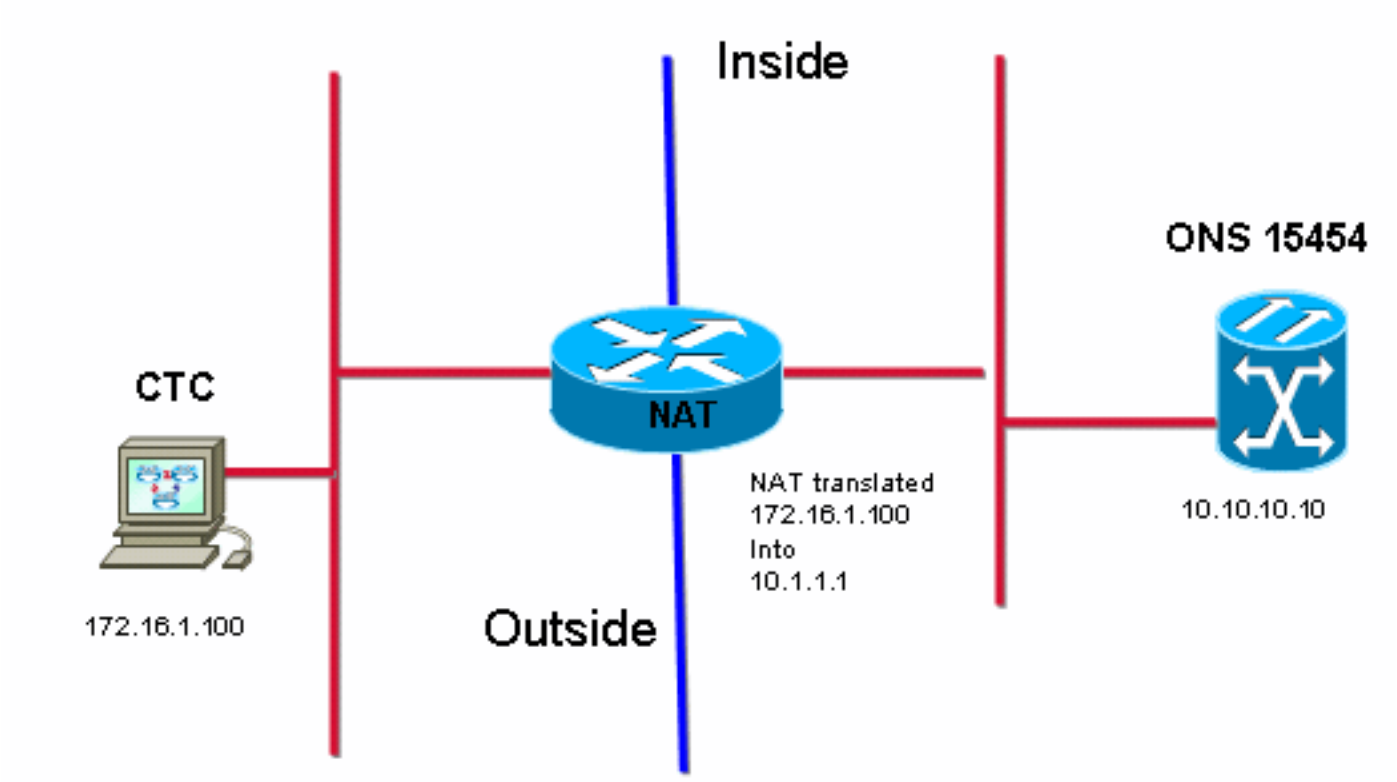
```
OCT 27 18:35:37.09 UTC ERROR     ObjectChange.cc:432   tEventMgr
 CORBA::NO_IMPLEMENT/0x3d0004 updating [192.168.1.100:EventReceiver].  Marking c

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

Deze fout kan meerdere redenen hebben. Als de fout echter met regelmatige voorspelbare intervallen (gewoonlijk ~2 of ~4 minuten) optreedt, kan de reden de aanwezigheid zijn van een type NAT dat CTC niet ondersteunt of van een firewall zonder de benodigde poortrechten.

Let erop dat 172.16.1.100 het IP-adres van het CTC-werkstation is en 10.1.1.1 het NAT-adres (zie afbeelding 1).

Afbeelding 1 - Topologie



Hier is de gedeeltelijke uitvoer van de opdracht **InetstatShow**:

```
-> 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
```

Deze output toont geen bewijs van dit adres. De output toont het openbare adres dat de ISP gebruikt, wat bewijs is van een traditioneel NAT-scenario.

Om bidirectionele NAT en Twice NAT te kunnen identificeren, hebt u een snuifspoor van hetzelfde netwerksegment nodig als het CTC-werkstation. Idealiter is een sniffer die op het CTC-werkstation werkt het meest geschikt.

Gerelateerde informatie

- Cisco ONS 15454 handleiding, release 5.0
- Technische ondersteuning en documentatie – Cisco Systems