Cisco ONS 15454 e NAT

Sommario

Introduzione

Questo documento descrive i diversi tipi di NAT (Network Address Translation) e ne mappa ciascun tipo alla versione software ONS 15454 corrispondente.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ONS 15454
- CTC
- NAT

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Tutte le versioni di Cisco ONS 15454

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

In molti casi sul campo, sono in gioco diversi scenari NAT e non funzionano correttamente. È possibile identificare la maggior parte di questi scenari attraverso i sintomi. La maggior parte dei problemi deriva dall'impossibilità per l'elemento di rete (NE) di avviare una connessione alla workstation Cisco Transport Controller (CTC).

Spesso, quando CTC non supporta una particolare configurazione di NAT, CTC si disconnette e si riconnette ai nodi a intervalli specifici. Nelle versioni più recenti, CTC è in grado di ripristinare le disconnessioni senza uscire dalla visualizzazione. In tali versioni, è possibile notare questo problema durante l'interazione con il nodo tramite CTC.

Gli stessi sintomi si verificano anche a causa di configurazioni errate del firewall esterno in cui gli elenchi degli accessi impongono la sicurezza. Gli elenchi degli accessi non consentono al NEO di avviare determinate connessioni da o verso indirizzi IP e/o porte definiti, verso la workstation CTC. Disconnessioni frequenti possono inoltre verificarsi quando le impostazioni di timeout del firewall esterno sono troppo brevi.

Per un esempio di elenchi degli accessi ai firewall che è possibile utilizzare con ONS 15454, fare riferimento alla sezione External Firewall nel manuale di riferimento di Cisco ONS 15454, versione 5.0.

NAT

Il protocollo NAT consente a un singolo dispositivo, ad esempio un router, di fungere da agente tra Internet e una rete locale. In questa sezione vengono illustrati i vari tipi di NAT.

Per ulteriori informazioni, fare riferimento alla RFC 2663 - IP Network Address Translator Terminology and Considerations (Terminologia e considerazioni su IP Network Address Translator).

NAT tradizionale

Il tradizionale NAT consente agli host di una rete privata di accedere in modo trasparente agli host della rete esterna. Il protocollo NAT tradizionale avvia sessioni in uscita dalla rete privata.

Questa sezione descrive brevemente le due varianti del NAT tradizionale:

- **NAT di base**: Il protocollo NAT di base riserva un blocco di indirizzi esterni. Il protocollo NAT di base utilizza questi indirizzi per tradurre gli indirizzi degli host in un dominio privato quando gli host avviano sessioni con il dominio esterno.
- **NAPT (Network Address Port Translation)**: NAPT estende la nozione di traduzione di un

passo avanti. NAPT traduce anche gli identificatori di trasporto, ad esempio i numeri delle porte TCP e UDP e gli identificatori di query ICMP. Questa traduzione moltiplica gli identificativi di trasporto di un certo numero di host privati negli identificativi di trasporto di un singolo indirizzo esterno.**Nota:** NAPT è anche denominato Port Address Translation (PAT).

NAT bidirezionale

Un dispositivo nella rete esterna avvia una transazione con un dispositivo all'interno. Per consentire questo avvio, la versione base di NAT è stata migliorata per includere funzionalità avanzate. Questo miglioramento è più comunemente noto come NAT bidirezionale, ma è anche noto come NAT bidirezionale e NAT in entrata. Con un NAT bidirezionale, è possibile avviare sessioni dagli host nella rete pubblica e nella rete privata. Gli indirizzi di rete privati sono associati a indirizzi univoci globali, in modo statico o dinamico quando si stabiliscono connessioni in entrambe le direzioni.

Le prestazioni di NAT sulle transazioni in entrata sono più difficili di NAT in uscita. Il motivo è che la rete interna in genere conosce l'indirizzo IP dei dispositivi esterni, in quanto questi dispositivi sono pubblici. Tuttavia, la rete esterna non conosce gli indirizzi privati della rete interna. Anche se la rete esterna riconosce gli indirizzi IP delle reti private, non è mai possibile specificare questi indirizzi IP come destinazione di un datagramma IP avviato dall'esterno, in quanto non instradabili.

Per risolvere il problema relativo agli indirizzi nascosti, è possibile utilizzare uno dei due metodi seguenti:

- Mapping statico
- DNS (Domain Name System) TCP/IP

Nota: in questo documento, il NAT bidirezionale implica il NAT di base, ma il NAT di base non implica il NAT bidirezionale.

Due NAT

Due volte NAT è una variante di NAT. Due volte NAT modifica gli indirizzi di origine e di destinazione quando un datagramma attraversa i realm degli indirizzi. Questo concetto è in contrasto con il NAT tradizionale e il NAT bidirezionale, che traducono solo uno degli indirizzi (origine o destinazione).

ONS 15454 e compatibilità NAT

La tabella seguente mostra la compatibilità con ONS 15454 e NAT:

Tipo di NAT	Sedi CTC	Viste di elementi di rete gateway (GNE)	Versione CTC supportata
NAT di base	IP GNE	IP tradotto	Release 3.3
NAPT	IP GNE	IP tradotto	Release 4.0
NAT bidireziona	IP tradott	IP CTC	Release 5.0

le	o		
Due NAT	IP tradotto	IP tradotto	Release 5.0

Risoluzione dei problemi

In caso di problemi di comunicazione tra il sistema operativo e il CTC, l'output del comando **fhDebug** contiene questo messaggio di errore:

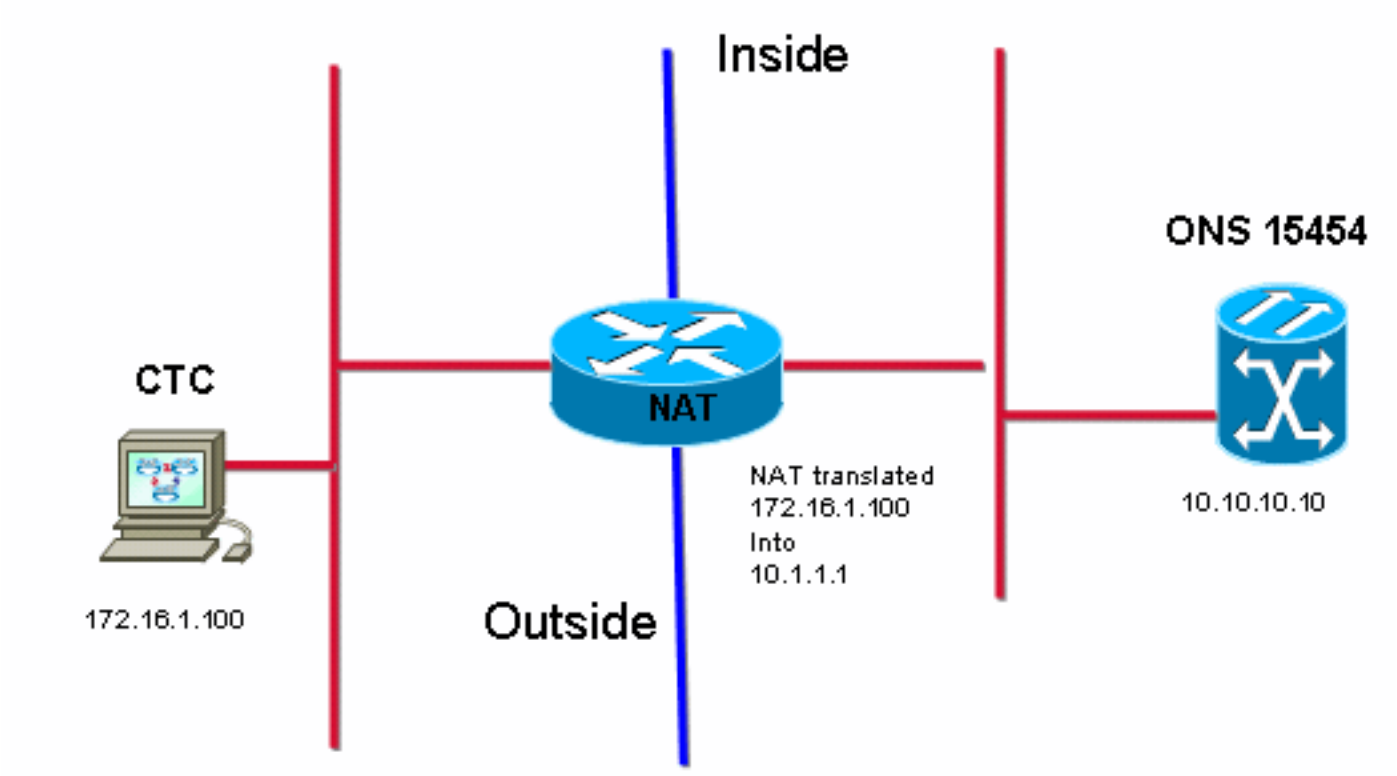
```
OCT 27 18:35:37.09 UTC ERROR     ObjectChange.cc:432   tEventMgr
 CORBA::NO_IMPLEMENT/0x3d0004 updating [192.168.1.100:EventReceiver].  Marking c

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

Questo errore può essere causato da diversi motivi. Tuttavia, se l'errore si verifica a intervalli regolari prevedibili (generalmente ~2 o ~4 minuti), la causa può essere la presenza di un tipo di NAT non supportato da CTC o la presenza di un firewall senza le necessarie autorizzazioni della porta.

Notare che 172.16.1.100 è l'indirizzo IP della workstation CTC e 10.1.1.1 è l'indirizzo NAT (vedere la Figura 1).

Figura 1 - Topologia



Di seguito viene riportato l'output parziale del comando **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
```

L'output mostrato non mostra alcuna prova di questo indirizzo. L'output mostra l'indirizzo pubblico utilizzato dall'ISP, che è la prova di uno scenario NAT tradizionale.

Per identificare il NAT bidirezionale e il NAT doppio, è necessaria una traccia sniffer dallo stesso segmento di rete della workstation CTC. Idealmente, una sniffer in esecuzione sulla workstation CTC è la più adatta.

Informazioni correlate

- Manuale di riferimento di Cisco ONS 15454, release 5.0
- Documentazione e supporto tecnico – Cisco Systems