Comprendere l'ordine di funzionamento NAT

Sommario

Introduzione

Questo documento descrive che le transazioni dell'ordine vengono elaborate con NAT in base alla direzione in cui un pacchetto viaggia all'interno o all'esterno della rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di questo argomento:

- Network Address Translation (NAT). Per ulteriori informazioni su NAT, vedere Funzionamento di NAT.

Componenti usati

Per la stesura del documento, è stato usato il software Cisco IOS® versione 12.2(27).

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

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Questo documento descrive che l'ordine in cui le transazioni vengono elaborate con Network

Address Translation (NAT) si basa sul tipo di pacchetto che viene inviato dalla rete interna alla rete esterna o dalla rete esterna alla rete interna.

Panoramica NAT

In questa tabella, quando NAT esegue la conversione da globale a locale o da locale a globale, ogni flusso presenta differenze.

Da interno a esterno

- Se IPSec, controllare l'elenco degli accessi di input
- decrittografia - per CET (Cisco Encryption Technology) o IPSec
- controllare l'elenco degli accessi di input
- controlla limiti di velocità di input
- contabilità di input
- reindirizzare a web cache
- policy routing
- instradamento
- **NAT dall'interno all'esterno (traduzione locale-globale)**
- crypto (verificare la mappa e contrassegnare per la crittografia)
- controllare l'elenco degli accessi di output
- inspect (CBAC (Context-based Access Control))
- TCP intercept
- crittografia
- coda

Da esterno a interno

- Se IPSec, controllare l'elenco degli accessi d input
- decrittografia - per CET o IPSec
- controllare l'elenco degli accessi di input
- controlla limiti di velocità di input
- contabilità di input
- reindirizzare a web cache
- **NAT dall'esterno all'interno (traduzione globa locale)**
- policy routing
- instradamento
- crypto (verificare la mappa e contrassegnare la crittografia)
- controllare l'elenco degli accessi di output
- ispezionare CBAC
- TCP intercept
- crittografia
- coda

Configurazione e output NAT

Nell'esempio viene mostrato come l'ordine delle operazioni può influire su NAT. In questo caso, vengono mostrati solo NAT e routing.

Nell'esempio precedente, il router A è configurato per convertire l'indirizzo locale interno da 172.31.200.48 a 172.16.47.150, come mostrato nella configurazione.

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
enable password ww
!
ip nat inside source static 172.31.200.48 172.16.47.150

!--- This command creates a static NAT translation
!--- between 172.31.200.48 and 172.16.47.150 ip domain-name cisco.com ip name-server
172.31.2.132 ! interface Ethernet0 no ip address shutdown ! interface Serial0 ip address
172.16.47.161 255.255.255.240 ip nat inside
```

```
!--- Configures Serial0 as the NAT inside interface no ip mroute-cache no ip route-cache no
fair-queue ! interface Serial1 ip address 172.16.47.146 255.255.255.240 ip nat outside

!--- Configures Serial1 as the NAT outside interface no ip mroute-cache no ip route-cache ! no
ip classless ip route 0.0.0.0 0.0.0.0 172.16.47.145

!--- Configures a default route to 172.16.47.145 ip route 172.31.200.0 255.255.255.0
172.16.47.162 ! ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 password ww login ! end
```

La tabella di traduzione indica che la traduzione desiderata esiste.

```
Router-A#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      172.31.200.48      ---                ---
```

Questo output viene generato dal router-A con i **dettagli del pacchetto ip di debug** e il **nat di ip di debug** abilitato, e da un ping emesso dal dispositivo 172.31.200.48 destinato a 172.16.47.142.

> **Nota**: i comandi di debug generano una quantità significativa di output. Utilizzarli solo quando il traffico sulla rete IP è basso, in modo che le altre attività del sistema non siano influenzate negativamente. Prima di usare il comando **debug**, consultare le informazioni importanti sui comandi di debug.

```
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
```

Poiché nell'output precedente non sono presenti messaggi di debug NAT, la conversione statica corrente non viene utilizzata e il router non dispone di un percorso per l'indirizzo di destinazione (172.16.47.142) nella relativa tabella di routing. Il risultato del pacchetto non instradabile è un messaggio ICMP Unreachable che viene inviato al dispositivo interno.

Tuttavia, il router A ha un percorso predefinito di 172.16.47.145, quindi perché il percorso viene considerato non instradabile?

Sul router A **non** è configurato **alcun indirizzo ip senza classe**, ossia se un pacchetto destinato a un indirizzo di rete "principale" (in questo caso, 172.16.0.0) per il quale esistono subnet nella tabella di routing, il router non si basa sul percorso predefinito. In altre parole, se si usa il comando **no ip classless**, il router non può cercare la route con il bit più lungo corrispondente. Per modificare questo comportamento, è necessario configurare **ip classless** sul router A. Il comando **ip classless** è abilitato per impostazione predefinita sui router Cisco con software Cisco IOS versione 11.3 e successive.

```
Router-A#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Router-A(config)#ip classless
Router-A(config)#end

Router-A#show ip nat translation
%SYS-5-CONFIG_I: Configured from console by console nat tr
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      172.31.200.48      ---                ---
```

Quando si ripete lo stesso test ping precedentemente eseguito, si osserverà che il pacchetto viene tradotto e il ping ha esito positivo.

```
Ping Response on device 172.31.200.48

D:\>ping 172.16.47.142
Pinging 172.16.47.142 with 32 bytes of data:

Reply from 172.16.47.142: bytes=32 time=10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255

Ping statistics for 172.16.47.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2ms

Debug messages on Router A indicating that the packets generated by device
172.31.200.48 are getting translated by NAT.

Router-A#
*Mar 28 03:34:28: IP: tableid=0, s=172.31.200.48 (Serial0), d=172.16.47.142
(Serial1), routed via RIB
*Mar 28 03:34:28: NAT: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [160]
*Mar 28 03:34:28: IP: s=172.16.47.150 (Serial0), d=172.16.47.142 (Serial1),
 g=172.16.47.145, len 100, forward
*Mar 28 03:34:28: ICMP type=8, code=0
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [160]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [161]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [161]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [162]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [162]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [163]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [163]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
```

```
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [164]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [164]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0

Router-A#undebug all
All possible debugging has been turned off
```

Nell'esempio precedente viene mostrato come quando un pacchetto attraversa la destinazione interna verso l'esterno, un router NAT controlla la tabella di routing alla ricerca di un percorso all'indirizzo esterno prima di continuare a tradurre il pacchetto. Pertanto, è importante che il router NAT disponga di un percorso valido per la rete esterna. Il percorso alla rete di destinazione deve essere noto tramite un'interfaccia definita come NAT all'esterno nella configurazione del router.

Èimportante notare che i pacchetti restituiti vengono tradotti prima di essere inoltrati. Pertanto, il router NAT deve avere anche un percorso valido per l'indirizzo locale interno nella relativa tabella di routing.

Informazioni correlate

- Configurazione di Network Address Translation
- Verifica del funzionamento e risoluzione dei problemi base del protocollo NAT
- NAT: definizioni locali e globali
- Come funziona il multicast NAT sui router Cisco?
- Pagina di supporto NAT
- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).