

Come NAT gestisce i frammenti ICMP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Caso 1](#)

[Caso 2](#)

[Caso 3](#)

[Riepilogo](#)

[Informazioni correlate](#)

Introduzione

Questo documento spiega come Network Address Translation (NAT) gestisce i frammenti ICMP (Internet Control Message Protocol) quando si configura l'overload NAT. Per informazioni sull'overload NAT, fare riferimento alle [domande frequenti su NAT](#).

La gestione dei frammenti ICMP dipende dallo stato della tabella di conversione NAT e dall'ordine in cui il router NAT riceve i frammenti ICMP. Esamineremo tre casi diversi, in cui invieremo due ping da 172.16.0.1 a 172.17.1.2 con una lunghezza di 3600 byte ciascuno (tre frammenti IP).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Caso 1

In questo scenario, NAT crea una voce di traduzione completamente estesa nella tabella di traduzione. Al termine, e se non sono presenti altri indirizzi utilizzabili nel pool NAT, NAT scarta i frammenti ricevuti prima del primo frammento (frammento 0) di un pacchetto.

All'inizio, solo un indirizzo nel pool esegue il sovraccarico. la tabella di conversione NAT è vuota; e la configurazione NAT viene visualizzata come:

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

Osserviamo cosa succede quando i pacchetti iniziano ad arrivare al router NAT.

1. Arriva il frammento 0 del pacchetto 1 e NAT crea una voce di traduzione completamente estesa. NAT quindi traduce e inoltra il pacchetto 1 e il frammento 0. La tabella di conversione viene visualizzata come segue:

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.10.10.3:24320	172.16.0.1:24320	172.17.1.2:24320	172.17.1.2:24320

Notate il numero 24320 nella tabella di conversione riportata sopra. È il valore del client ICMP incluso nell'intestazione ICMP del datagramma IP. Solo il frammento 0 del datagramma IP contiene questa intestazione ICMP. Per determinare se più frammenti fanno parte dello stesso pacchetto, NAT deve tenere traccia del valore del rientro IP presente nell'intestazione IP di tutti i frammenti del datagramma IP originale. Se più frammenti hanno lo stesso valore di ident IP del frammento 0, che ha creato la traduzione estesa, NAT li traduce utilizzando la stessa voce di traduzione estesa. Per ulteriori informazioni sul campo di identificazione IP, consultare la [RFC 791](#) . Per ulteriori informazioni sul campo di identificazione ICMP, consultare la [RFC 792](#) .

2. Arrivano il pacchetto 1, frammento 2, e il pacchetto 1, frammento 1. Poiché questi frammenti fanno parte dello stesso pacchetto contenente il frammento 0 (che ha creato la traduzione), NAT utilizza la voce di traduzione indicata sopra per tradurre e inoltrare questi frammenti. Il dispositivo di destinazione riceve tutti i frammenti del pacchetto 1 e invia una risposta.
3. Arriva il frammento 1 del pacchetto 2. Trattandosi di un nuovo pacchetto, il suo valore IP Identity non corrisponde a nulla che sia stato registrato da NAT. NAT non può pertanto utilizzare la traduzione esistente. Inoltre, non può creare una nuova traduzione poiché ha già una voce di traduzione completamente estesa e non ha il rientro ICMP per crearne un'altra. NAT scarta il pacchetto 2, frammento 1.
4. Arriva il frammento 0 del pacchetto 2. NAT può utilizzare la traduzione di cui sopra poiché l'ID ICMP corrisponde. Tutti i ping all'interno di un singolo set usano lo stesso numero di rientro ICMP. A questo punto, NAT registra l'ID IP di questo pacchetto. NAT converte e inoltra il pacchetto 2, frammento 0.
5. Arriva il frammento 2 del pacchetto. NAT può ora utilizzare la traduzione di cui sopra poiché il relativo valore di ID IP corrisponde a quello registrato nel passaggio precedente. NAT converte e inoltra il pacchetto 2, frammento 2. Il dispositivo di destinazione riceve solo i frammenti 0 e 2 (il frammento 1 è mancante), quindi non invia alcuna risposta.

Caso 2

In questo scenario, se i frammenti diversi dal primo (frammento 0) arrivano per primi, NAT crea una traduzione semplice, a condizione che nel pool NAT sia presente un indirizzo non ancora

utilizzato in una traduzione completamente estesa.

All'inizio, il pool NAT contiene un solo indirizzo, la tabella di conversione NAT è vuota e la configurazione viene visualizzata come segue:

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

1. Arriva il frammento 1 del pacchetto. NAT non può creare una traduzione completamente estesa nella tabella di traduzione perché non contiene le informazioni di ident ICMP in questo frammento. Tuttavia, poiché non sono disponibili traduzioni completamente estese, NAT inserisce una semplice traduzione. NAT quindi traduce e inoltra il pacchetto 1, frammento 1.

La voce di traduzione viene visualizzata come segue:

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.3	172.16.0.1	---	---

2. Arriva il frammento 0 del pacchetto 1. Poiché le informazioni sui client ICMP sono incluse in questo frammento, NAT immette una voce di traduzione completamente estesa:

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.3	172.16.0.1	---	---
icmp	10.10.10.3:24321	172.16.0.1:24321	172.17.1.2:24321	172.17.1.2:24321

NAT registra quindi le informazioni sull'ID IP e converte e inoltra il pacchetto 1 e il frammento 0.

3. Arriva il pacchetto 1 e il frammento 2. Poiché questo frammento ha le stesse informazioni sull'ID IP registrate da NAT nel passaggio 2, NAT utilizza la traduzione completamente estesa per tradurre e inoltrare il pacchetto 1, frammento 2. Il dispositivo di destinazione riceve tutti i frammenti e le risposte. A questo punto, tutti i ping hanno esito positivo finché la tabella di conversione NAT non viene cancellata o non si verifica un timeout.

Caso 3

In questo scenario, se i frammenti diversi dal primo (frammento 0) arrivano per primi, NAT crea una traduzione semplice, a condizione che nel pool NAT sia presente un indirizzo non ancora utilizzato in una traduzione completamente estesa. Se una traduzione estesa nella tabella NAT utilizza già l'indirizzo, si corre il rischio che NAT converta ogni indirizzo di origine del frammento in un indirizzo diverso.

Come si inizia, più di un indirizzo nel pool NAT esegue il sovraccarico, la tabella di conversione dispone già di una traduzione estesa e la configurazione è:

```
ip nat pool POOL1 10.10.10.3 10.10.10.5 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

La tabella di conversione viene visualizzata nel modo seguente:

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322

1. Arriva il frammento 1 del pacchetto. NAT non può creare una voce della tabella di traduzione completamente estesa perché non contiene le informazioni di ident ICMP in questo frammento e non può creare una voce di traduzione semplice per l'indirizzo 10.10.10.3,

poiché esiste una voce estesa per questo indirizzo IP. NAT sceglie il successivo indirizzo IP gratuito (10.10.10.4) e crea una semplice traduzione. NAT quindi traduce e inoltra il pacchetto 1, frammento 1. La tabella di conversione viene visualizzata come segue:

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.4	172.16.0.1	---	---
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322

2. Arriva il frammento 0 del pacchetto 1. Poiché le informazioni sui client ICMP sono incluse in questo frammento, NAT immette una voce di traduzione completamente estesa per l'indirizzo 10.10.10.3 e registra le informazioni sui client IP per questo pacchetto. NAT quindi traduce e inoltra il pacchetto 1 e il frammento 0. La tabella di conversione viene visualizzata come segue:

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.4	172.16.0.1	---	---
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322
icmp	10.10.10.3:24323	172.16.0.1:24323	172.17.1.2:24323	172.17.1.2:24323

3. Arriva il pacchetto 1 e il frammento 2. Poiché le informazioni sull'ID IP corrispondono a quelle registrate da NAT nel passaggio 2, NAT utilizza la traduzione completamente estesa creata nel passaggio 2 per tradurre e inoltrare il pacchetto 1, frammento 2. A questo punto, il dispositivo di destinazione riceve tutti i frammenti del pacchetto 1, ma l'indirizzo di origine dei frammenti 0 e 2 è stato tradotto in 10.10.10.3 e il frammento 1 è stato tradotto in 10.10.10.4. Il dispositivo di destinazione non può quindi ricomporre il pacchetto e non invia alcuna risposta.
4. Arriva il frammento 0 del pacchetto 2. NAT utilizza la traduzione completamente estesa sopra indicata o crea una nuova traduzione completamente estesa a seconda del valore del campo del rientro ICMP del frammento. In entrambi i casi, NAT registra le informazioni sull'ID IP. NAT quindi converte e inoltra il pacchetto 2 e il frammento 0.
5. Arriva il frammento 2 del pacchetto. Le sue informazioni sull'ID IP corrispondono a quelle registrate da NAT nel passaggio 4, quindi NAT utilizza la seconda traduzione completamente estesa creata nel passaggio 4. NAT traduce e inoltra il pacchetto 2, frammento 2.
6. Arriva il frammento 1 del pacchetto 2. Le sue informazioni sull'ID IP corrispondono a quelle registrate da NAT nel passaggio 4, quindi NAT utilizza la seconda traduzione completamente estesa creata nel passaggio 4. NAT traduce e inoltra il pacchetto 2, frammento 1. Il dispositivo di destinazione riceve tutti e tre i frammenti del pacchetto 2 dalla stessa origine (10.10.10.3), quindi ricompone il pacchetto e risponde.

Riepilogo

Il rilascio o l'inoltro di un frammento ICMP da parte del NAT dipende da diversi fattori, ad esempio l'ordine in cui il router NAT riceve i frammenti e lo stato della tabella di conversione in tale momento. In alcune condizioni, NAT converte i frammenti in modo diverso, rendendo impossibile per il dispositivo di destinazione ricomporre il pacchetto.

Informazioni correlate

- [Pagina di supporto NAT](#)
- [Pagina di supporto per il routing IP](#)
- [Supporto tecnico – Cisco Systems](#)