

Configura comando statico di origine esterna IP NAT

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Riepilogo](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta una configurazione che utilizza il comando `ip nat external source static` e i pacchetti IP risultanti dal processo NAT.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di questo argomento:

- [Usa termini NAT locali e globali](#)

Componenti usati

Per la stesura del documento, sono stati usati router Cisco con software Cisco IOS®.

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.

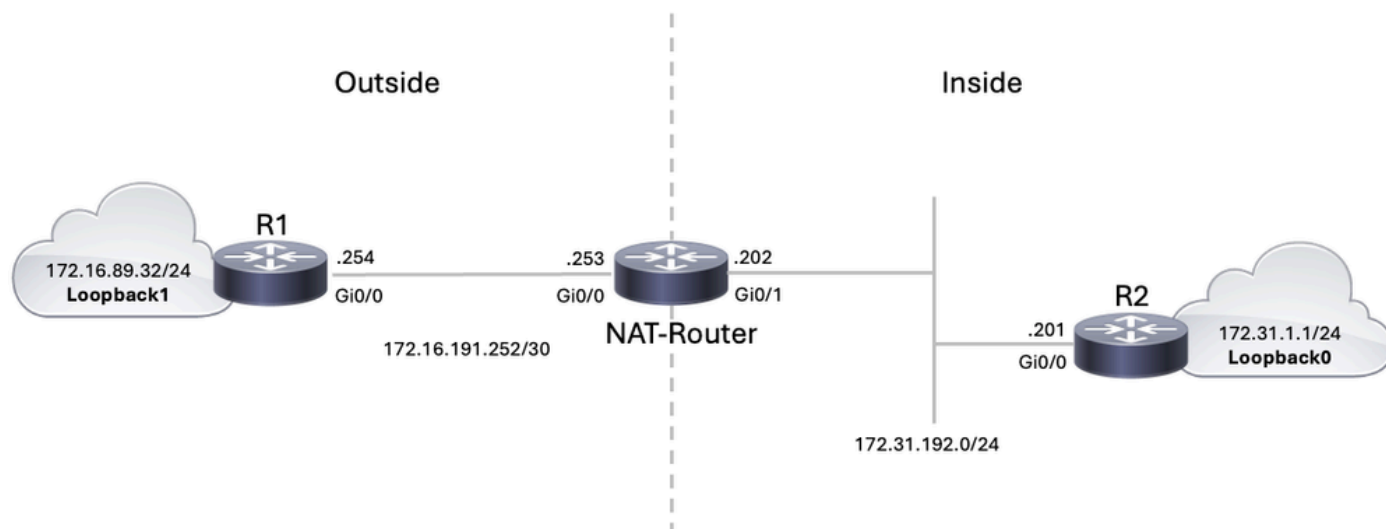
Premesse

In questo documento viene fornita una configurazione di esempio con l'uso del comando `ip nat outside source static` e viene fornita una breve descrizione di ciò che accade al pacchetto IP durante il processo NAT. Si consideri la topologia di rete in questo documento come esempio.

Configurazione

Esempio di rete

Il documento usa la seguente configurazione di rete.



Esempio di rete

Quando si esegue un ping proveniente dall'interfaccia di loopback1 del router R1 e destinato all'interfaccia di loopback0 del router R2, si verifica quanto segue:

1. Sull'interfaccia esterna (Gi0/0) del router NAT, il pacchetto ping viene visualizzato con un indirizzo di origine (SA) di 172.16.89.32 e un indirizzo di destinazione (DA) di 172.31.1.1.
2. NAT converte l'associazione di sicurezza nell'indirizzo locale esterno 172.31.16.5 (corrispondente al comando `ip nat external source static` configurato sul router NAT).
3. Il NAT-Router controlla quindi la tabella di routing per verificare che non sia presente un percorso verso 172.31.1.1.
 - Se il percorso non esiste, il router NAT scarta il pacchetto. Tuttavia, in questo caso, il router NAT ha un percorso verso 172.31.1.1 tramite la route statica configurata fino alla subnet 172.31.1.0/24. Inoltre il pacchetto alla destinazione.
4. Il router R2 riceve il pacchetto sull'interfaccia in entrata (Gi0/0), ora con un'ASA di 172.31.16.5 e un'ADA di 172.31.1.1.
5. Per rispondere, R2 invia una risposta echo ICMP (Internet Control Message Protocol) a 172.31.16.5 (l'indirizzo NAT).
 - Se R2 non ha un percorso, scarta il pacchetto. Tuttavia, in questo caso, ha un percorso predefinito verso il router NAT.
 - Pertanto, invia un pacchetto di risposta al router NAT, con un'ASA di 172.31.1.1 e un DA di 172.31.16.5.

6. Il router NAT vede il pacchetto e cerca un percorso verso l'indirizzo 172.31.16.5.
- In caso contrario, risponde con un messaggio ICMP "destinazione irraggiungibile".
 - In questo caso, la route statica è configurata per la subnet 172.31.16.0/24 e punta a R1.
 - Converte il pacchetto indietro all'indirizzo 172.16.89.32 e lo inoltra all'interfaccia esterna (Gi0/0).

Configurazioni

In questo documento vengono usate le seguenti configurazioni:

- [Router R1](#)
- [Router NAT-Router](#)
- [Router R2](#)

Router R1
<pre>hostname R1 ! !--- Output suppressed. ! interface Loopback1 ip address 172.16.89.32 255.255.255.0 ! interface GigabitEthernet0/0 ip address 172.16.191.254 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address shutdown ! !--- Output suppressed. ip route 0.0.0.0 0.0.0.0 172.16.191.253 !--- Default route to forward packets to NAT-Router. !--- Output suppressed.</pre>
Router NAT-Router
<pre>hostname NAT-Router ! !--- Output suppressed. !</pre>

```
interface GigabitEthernet0/0
ip address 172.16.191.253 255.255.255.252
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 172.31.192.202 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!

!--- ip nat command defines GigabitEthernet0/1 as a NAT inside interface and GigabitEthernet0/0 as a NAT outside interface.

!--- Output suppressed.

!
no ip http server
no ip http secure-server
ip nat outside source static 172.16.89.32 172.31.16.5
ip route 172.31.1.0 255.255.255.0 172.31.192.201
ip route 172.31.16.0 255.255.255.0 172.16.191.254
!

!--- Outside local address is defined as 172.31.16.5.
!--- Static routes for reaching the loopback interfaces on R2 and R1.
```

Router R2

```
hostname rp-R2
!

!--- Output suppressed.

!
interface Loopback0
ip address 172.31.1.1 255.255.255.0
!
interface GigabitEthernet0/0
ip address 172.31.192.201 255.255.255.0
duplex auto
speed auto
!

!--- Output suppressed.

ip route 0.0.0.0 0.0.0.0 172.31.192.202

!--- Default route to forward packets to NAT-Router.
!--- Output suppressed.
```

Verifica

Usare il comando `show ip nat translation` per controllare le voci di traduzione, come mostrato nell'output:

```
<#root>
```

```
NAT-Router#
```

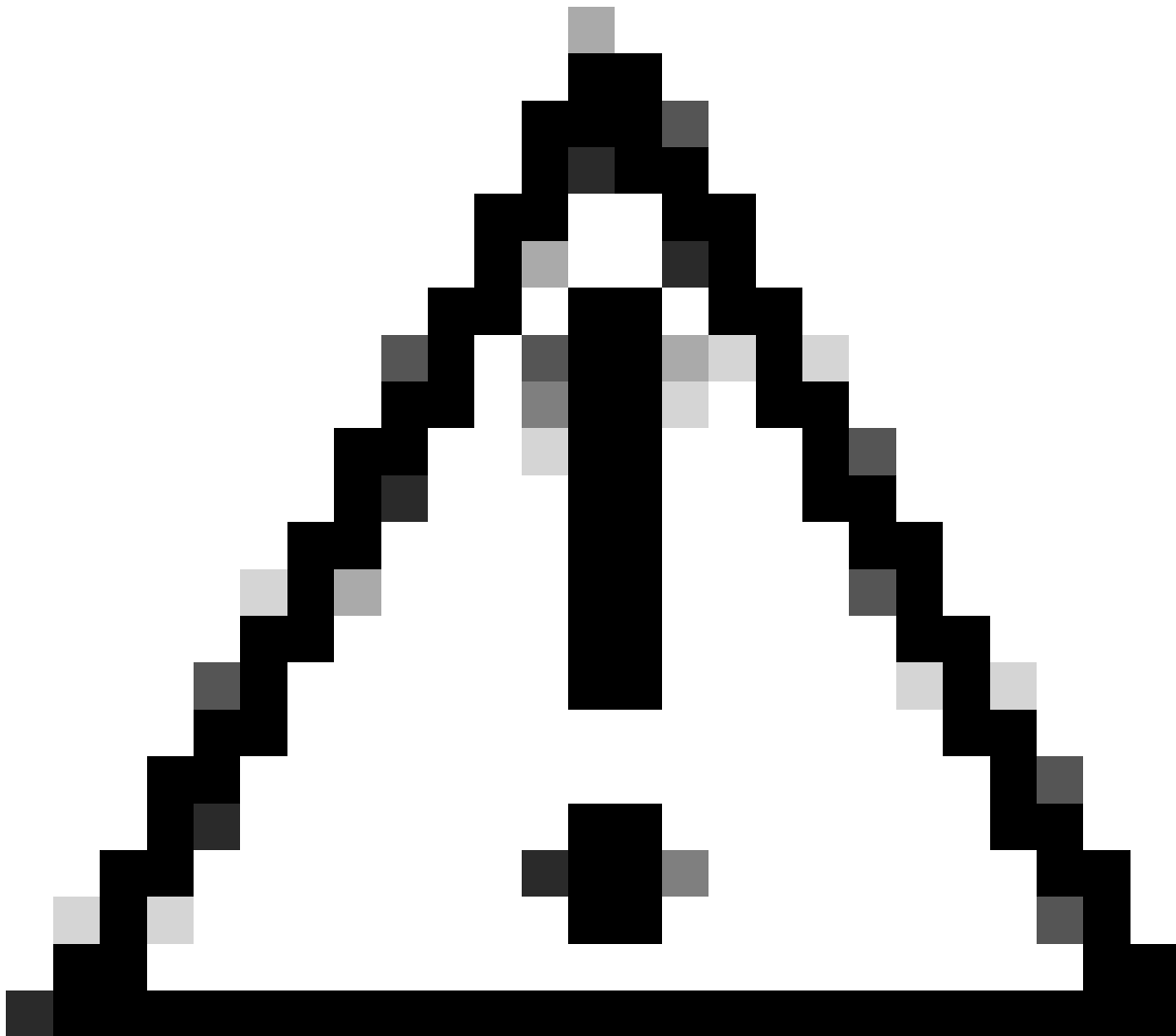
```
show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
---	---	---	172.31.16.5	172.16.89.32
icmp	172.31.1.1:21	172.31.1.1:21	172.31.16.5:21	172.16.89.32:21


```
NAT-Router#
```

Risoluzione dei problemi

In questo esempio vengono utilizzati il debug della conversione NAT e il debug dei pacchetti IP per dimostrare il processo NAT.



Attenzione: poiché 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 vengano influenzate negativamente.

 Nota: questi output di debug sono stati ottenuti da router con software Cisco IOS. La raccolta di questi output di debug può variare in base alla piattaforma in uso.

 Nota: fare riferimento a Informazioni importanti sui comandi di debug prima di usare i comandi debug.

Questo output è il risultato dell'uso simultaneo dei comandi [debug ip packet](#) e [debug ip nat](#) sul router NAT, durante il ping dall'indirizzo di interfaccia R1 loopback1 (172.16.89.32) all'indirizzo di interfaccia R2 loopback0 (172.31.1.1).

Questo output visualizza il primo pacchetto che arriva all'interfaccia esterna del router NAT. L'indirizzo di origine 172.16.89.32 viene convertito in 172.31.16.5. Il pacchetto ICMP viene

inoltrato alla destinazione dell'interfaccia Gigabit Ethernet 0/1.

<#root>

```
*Sep 19 15:34:39.925: NAT: s=172.16.89.32->172.31.16.5, d=172.31.1.1 [100]
*Sep 19 15:34:39.925: IP: s=172.31.16.5 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), len 10
*Sep 19 15:34:39.926: IP: s=172.31.16.5 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), len 10
*Sep 19 15:34:39.926: IP: s=172.31.16.5 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), len 10
*Sep 19 15:34:39.927: IP: s=172.31.16.5 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), len 10
*Sep 19 15:34:39.927: IP: s=172.31.16.5 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), g=172.
*Sep 19 15:34:39.928: IP: s=172.31.16.5 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), len 10
```

Questo output mostra il pacchetto restituito originato da 172.31.1.1 con un indirizzo di destinazione di 172.31.16.5, che viene convertito in 172.16.89.32. Il pacchetto ICMP risultante viene inoltrato dall'interfaccia Serial1.

<#root>

```
*Sep 19 15:34:39.930: NAT*: i: icmp (172.31.1.1, 20) -> (172.31.16.5, 20) [100]
*Sep 19 15:34:39.930: NAT*: s=172.31.1.1, d=172.31.16.5->172.16.89.32 [100]
```

Lo scambio di pacchetti ICMP continua. Il processo NAT per questo output di debug è lo stesso dell'output precedente.

```
*Sep 19 15:34:39.932: NAT*: o: icmp (172.16.89.32, 20) -> (172.31.1.1, 20) [101]
*Sep 19 15:34:39.932: NAT*: s=172.16.89.32->172.31.16.5, d=172.31.1.1 [101]
*Sep 19 15:34:39.933: NAT*: i: icmp (172.31.1.1, 20) -> (172.31.16.5, 20) [101]
*Sep 19 15:34:39.933: NAT*: s=172.31.1.1, d=172.31.16.5->172.16.89.32 [101]
*Sep 19 15:34:39.935: NAT*: o: icmp (172.16.89.32, 20) -> (172.31.1.1, 20) [102]
*Sep 19 15:34:39.935: NAT*: s=172.16.89.32->172.31.16.5, d=172.31.1.1 [102]
*Sep 19 15:34:39.936: NAT*: i: icmp (172.31.1.1, 20) -> (172.31.16.5, 20) [102]
*Sep 19 15:34:39.936: NAT*: s=172.31.1.1, d=172.31.16.5->172.16.89.32 [102]
*Sep 19 15:34:39.938: NAT*: o: icmp (172.16.89.32, 20) -> (172.31.1.1, 20) [103]
*Sep 19 15:34:39.938: NAT*: s=172.16.89.32->172.31.16.5, d=172.31.1.1 [103]
*Sep 19 15:34:39.939: NAT*: i: icmp (172.31.1.1, 20) -> (172.31.16.5, 20) [103]
*Sep 19 15:34:39.939: NAT*: s=172.31.1.1, d=172.31.16.5->172.16.89.32 [103]
*Sep 19 15:34:39.940: NAT*: o: icmp (172.16.89.32, 20) -> (172.31.1.1, 20) [104]
*Sep 19 15:34:39.940: NAT*: s=172.16.89.32->172.31.16.5, d=172.31.1.1 [104]
*Sep 19 15:34:39.942: NAT*: i: icmp (172.31.1.1, 20) -> (172.31.16.5, 20) [104]
*Sep 19 15:34:39.942: NAT*: s=172.31.1.1, d=172.31.16.5->172.16.89.32 [104]
```

Riepilogo

Quando il pacchetto si sposta dall'esterno verso l'interno, la conversione viene eseguita per prima, quindi viene controllata la tabella di routing per individuare la destinazione.

Quando il pacchetto viene spostato dall'interno all'esterno, la tabella di routing viene controllata prima per individuare la destinazione, quindi viene eseguita la traduzione.

Per ulteriori informazioni, fare riferimento all'[ordine di funzionamento NAT](#).

Prendere nota della parte del pacchetto IP che viene convertita quando viene utilizzata con ciascuno dei comandi precedenti. La tabella contiene le linee guida:

Comando	Azione
statico origine esterna ip nat	<ul style="list-style-type: none">• Convertire l'origine dei pacchetti IP trasmessi dall'esterno all'interno.• Convertire la destinazione dei pacchetti IP trasmessi dall'interno all'esterno.
statico origine ip nat inside	<ul style="list-style-type: none">• Convertire l'origine dei pacchetti IP trasmessi dall'interno all'esterno.• Convertire la destinazione dei pacchetti IP trasmessi dall'esterno all'interno.

Queste linee guida indicano che esiste più di un modo per tradurre un pacchetto. In base alle esigenze specifiche, determinare come definire le interfacce NAT (interne o esterne) e i percorsi contenuti nella tabella di routing prima o dopo la traduzione. Tenere presente che la parte di pacchetto tradotta dipende dalla direzione in cui viaggia il pacchetto e dal modo in cui si configura il NAT.

Informazioni correlate

- [Esempio di configurazione con il comando ip nat outside source list](#)
- [Configurazione di Network Address Translation](#)
- [Servizi di indirizzamento IP NAT](#)
- [Supporto tecnico Cisco e download](#)

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).