

Configurazione di Network Address Translation

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Procedura rapida per configurare e implementare la funzione NAT](#)

[Definizione delle interfacce NAT interna ed esterna](#)

[Esempi](#)

[1. Accesso a Internet da parte di utenti interni](#)

[Configurazione della funzione NAT per autorizzare gli utenti interni ad accedere a Internet](#)

[Configurazione della funzione NAT per autorizzare gli utenti interni ad accedere a Internet con sovraccarico](#)

[2. Accesso ai dispositivi interni da Internet](#)

[Configurazione della funzione NAT per autorizzare l'accesso ai dispositivi interni da Internet](#)

[3. Reindirizzamento del traffico TCP su un'altra porta o indirizzo TCP](#)

[Configurazione della funzione NAT per reindirizzare il traffico TCP su un'altra porta o indirizzo TCP](#)

[4. Uso della funzione NAT per una transizione di rete](#)

[Configurazione della funzione NAT per una transizione di rete](#)

[5. Uso della funzione NAT per le reti che si sovrappongono](#)

[Differenza tra mappatura uno-a-uno e molti-a-molti](#)

[Verificare il funzionamento del NAT](#)

[Conclusioni](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene spiegato come configurare la funzione NAT (Network Address Translation) su un router Cisco.

Prerequisiti

Requisiti

Per seguire gli argomenti trattati di seguito, è richiesta una conoscenza base della terminologia NAT.

Componenti usati

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

hardware:

- Cisco serie 2500 Router
- Cisco IOS® Software Release 12.2 (10b)

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.

Procedura rapida per configurare e implementare la funzione NAT

 Nota: in questo documento, quando si fa riferimento a Internet o a un dispositivo Internet, si intende un dispositivo di una rete esterna.

Quando si configura il NAT per la prima volta, può essere complicato capire come iniziare. La procedura illustrata aiuta a definire gli obiettivi che si intendono conseguire e come configurare il NAT:

1. [Definire le interfacce NAT interna ed esterna.](#)

- Gli utenti usano interfacce diverse?
- Per connettersi a Internet vengono usate più interfacce?

2. Definire gli obiettivi che si intendono conseguire con la conversione NAT.

- Si vuole [autorizzare gli utenti interni ad accedere a Internet](#)?
- Si vuole [autorizzare l'accesso ai dispositivi interni da Internet](#) (server di posta o server Web)?
- Si vuole [reindirizzare il traffico TCP su un'altra porta o indirizzo TCP](#)?
- Si intende usare la conversione [NAT per una transizione di rete \(ad esempio, l'indirizzo IP di un server è cambiato e finché tutti i client non saranno stati aggiornati, si desidera che i client non aggiornati possano accedere al server con l'indirizzo IP originale e che i client aggiornati possano accedere al server con il nuovo indirizzo\)](#)?
- Utilizzare per [consentire](#) la [comunicazione delle reti che si sovrappongono](#)?

3. Configurare la funzione NAT in modo da realizzare gli obiettivi definiti. A seconda di quanto deciso al passaggio 2, determinare quale delle seguenti funzioni usare:

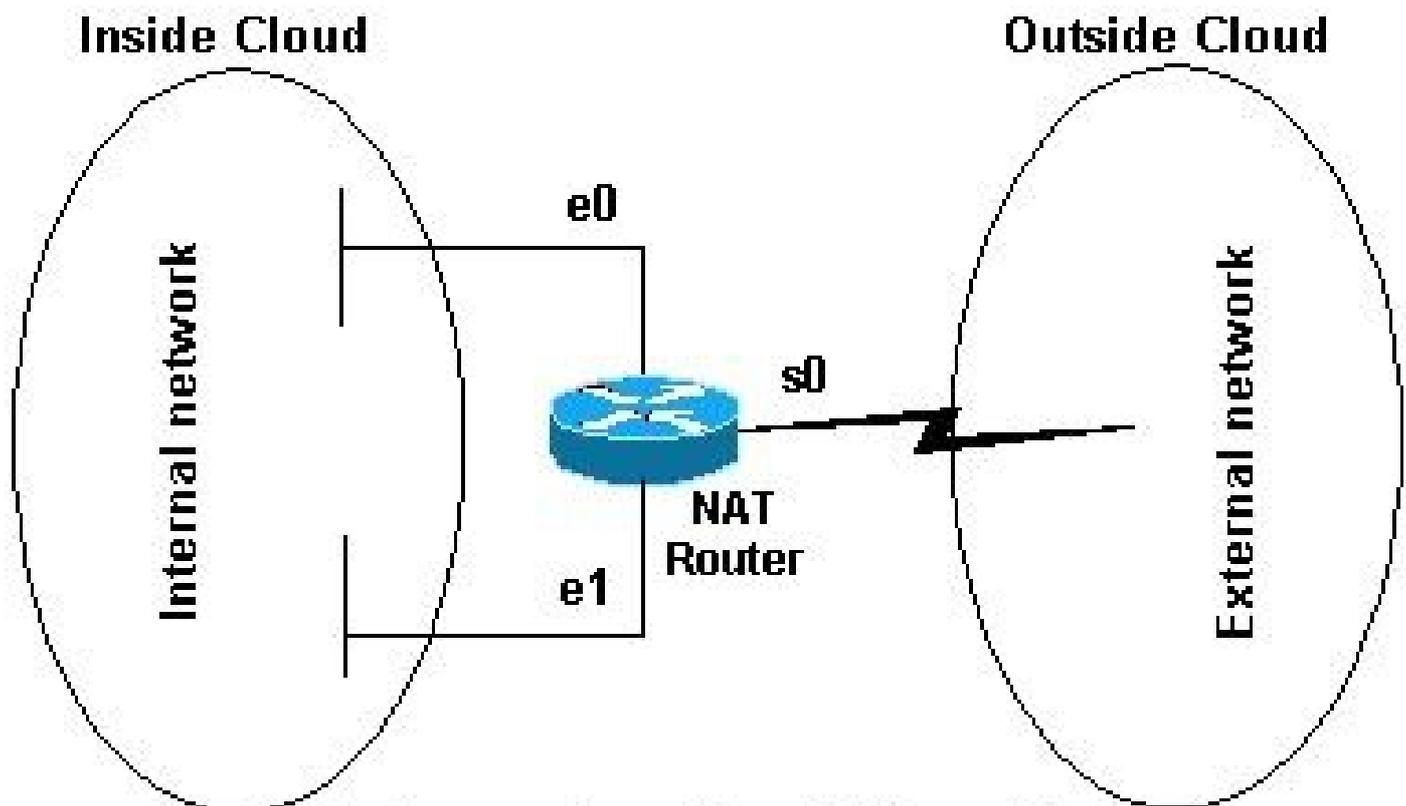
- NAT statico
- NAT dinamico
- Overloading
- Una combinazione di queste funzionalità.

4. Verificare il funzionamento del NAT.

Gli esempi proposti aiutano l'utente a completare i passaggi da 1 a 3 indicati nella procedura rapida nell'immagine precedente. e si basano su alcuni scenari comuni nei quali è consigliato implementare il NAT.

Definizione delle interfacce NAT interna ed esterna

Per implementare il NAT, occorre anzitutto definire le interfacce NAT interna ed esterna. Per semplificare, potremmo definire come interfaccia interna la rete interna e come interfaccia esterna la rete esterna. Tuttavia, l'assegnazione dei termini interna ed esterna è del tutto arbitraria. La figura seguente mostra un esempio di interfacce.



In this figure, ethernet 0 and ethernet 1 will be defined as NAT inside interfaces and serial 0 will be defined as a NAT outside interface.

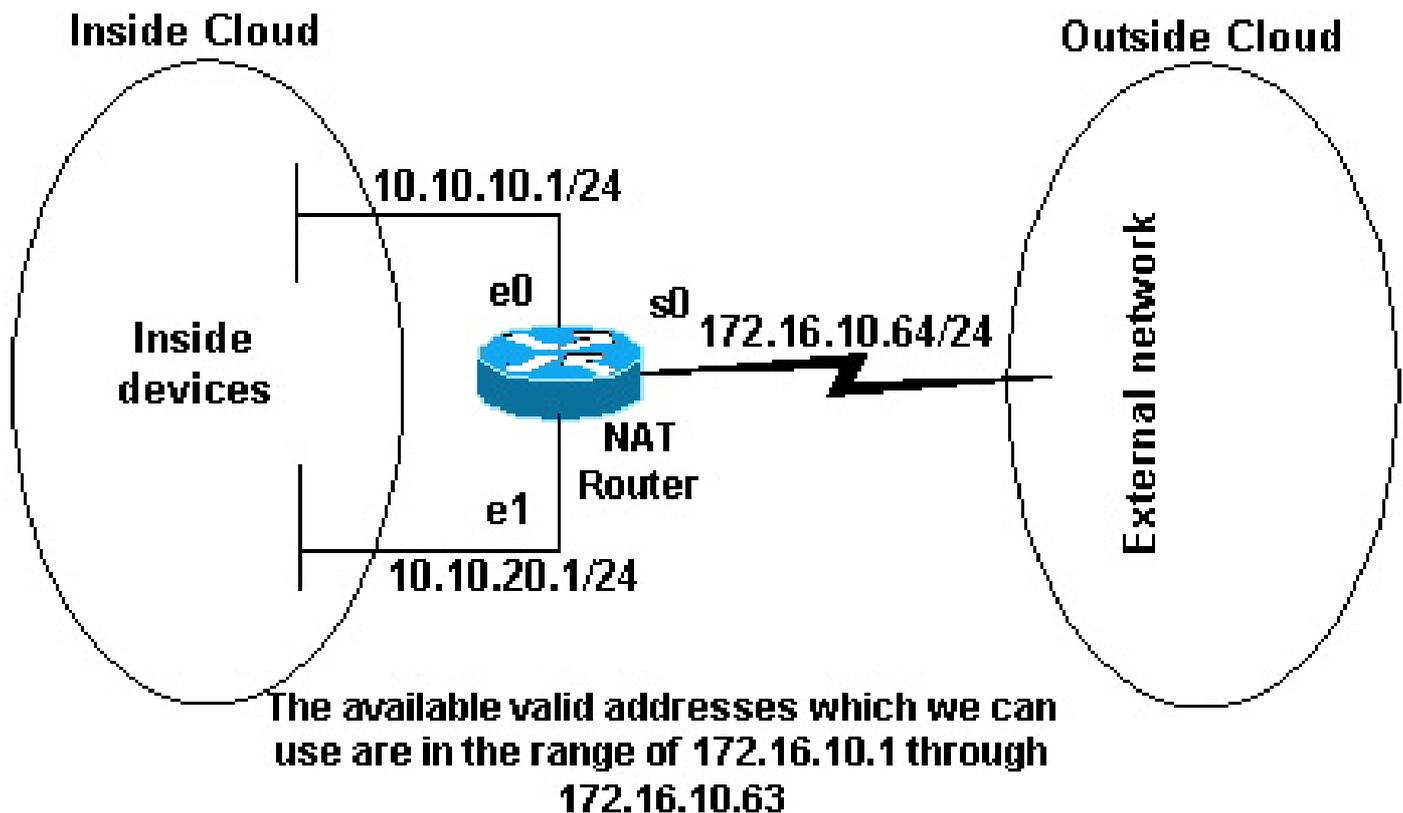
Topologia NAT

Esempi

1. Accesso a Internet da parte di utenti interni

Supponiamo che si desideri autorizzare gli utenti interni ad accedere a Internet, ma non si disponga di un numero adeguato di indirizzi validi da assegnare. Se tutte le comunicazioni tra i dispositivi e Internet hanno origine dai dispositivi interni, è necessario un unico indirizzo valido o un pool di indirizzi validi.

Nell'immagine viene mostrato un semplice diagramma di rete con le interfacce del router definite come interne ed esterne.



Indirizzi validi disponibili

Nell'esempio, si desidera che NAT consenta ad alcuni dispositivi interni (i primi 31 di ciascuna subnet) di avviare una comunicazione con i dispositivi esterni convertendo i propri indirizzi non validi in un indirizzo o in un pool di indirizzi valido. Il pool è stato definito come l'intervallo di indirizzi da 172.16.10.1 a 172.16.10.63.

Ora è possibile configurare la funzione NAT. Per realizzare l'obiettivo definito nell'immagine precedente, usare la NAT dinamica. Con il NAT dinamico, all'inizio la tabella di conversione del router è vuota e viene popolata dopo che il traffico che deve essere convertito ha attraversato il router. Con il NAT statico invece, la conversione viene configurata staticamente e inserita nella tabella di conversione senza nessuna trasmissione di dati.

Nell'esempio, è possibile configurare il NAT in modo che converta l'indirizzo di ciascun dispositivo interno in un indirizzo univoco valido oppure in uno stesso indirizzo valido. Questo secondo metodo è noto come `overloading`. Di seguito viene fornito un esempio per ciascun metodo.

Configurazione della funzione NAT per autorizzare gli utenti interni ad accedere a Internet

Router NAT
<pre>interface ethernet 0 ip address 10.10.10.1 255.255.255.0 ip nat inside</pre>

```
!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.

interface ethernet 1
ip address 10.10.20.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.

interface serial 0
ip address 172.16.10.64 255.255.255.0
ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.

ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 24

!--- Defines a NAT pool named no-overload with a range of addresses
!--- 172.16.10.1 - 172.16.10.63.

ip nat inside source list 7 pool no-overload

!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has
!--- the source address translated to an address out of the
!--- NAT pool "no-overload".

access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 permits packets with source addresses ranging from
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

 Nota: Cisco sconsiglia vivamente l'uso di permit any per configurare gli elenchi degli accessi a cui fanno riferimento i comandi NAT. L'uso di permit any nella conversione NAT potrebbe comportare il consumo di un numero eccessivo di risorse del router con conseguenti problemi di rete.

Nella configurazione precedente, solo i primi 32 indirizzi della subnet 10.10.10.0 e i primi 32 indirizzi della subnet 10.10.20.0 sono autorizzati dall'elenco degli accessi 7. Pertanto, vengono convertiti solo gli indirizzi che hanno questa origine. La rete interna potrebbe contenere altri dispositivi con indirizzi diversi, ma questi non verranno convertiti.

Al termine, verificare [che la conversione NAT funzioni come previsto](#).

Configurazione della funzione NAT per autorizzare gli utenti interni ad accedere a Internet con sovraccarico

Router NAT

```
interface ethernet 0
ip address 10.10.10.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.

interface ethernet 1
ip address 10.10.20.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.

interface serial 0
ip address 172.16.10.64 255.255.255.0
ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.

ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24

!--- Defines a NAT pool named ovrld with a range of a single IP
!--- address, 172.16.10.1.

ip nat inside source list 7 pool ovrld overload

!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has the source address
!--- translated to an address out of the NAT pool named ovrld.
!--- Translations are overloaded, which allows multiple inside
!--- devices to be translated to the same valid IP address.

access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 permits packets with source addresses ranging from
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

Nella seconda configurazione precedente, il pool `ovrld` NAT dispone solo di un intervallo di indirizzi. La parola chiave `overload` usata nel comando `ip nat inside source list 7 pool ovrld overload` permette di convertire gli indirizzi di più dispositivi interni in un pool con un unico indirizzo.

Un'altra variante di questo comando è `ip nat all'interno dell'interfaccia source list 7 serial 0 overload`, che configura NAT per l'overload sull'indirizzo assegnato all'interfaccia `serial 0`.

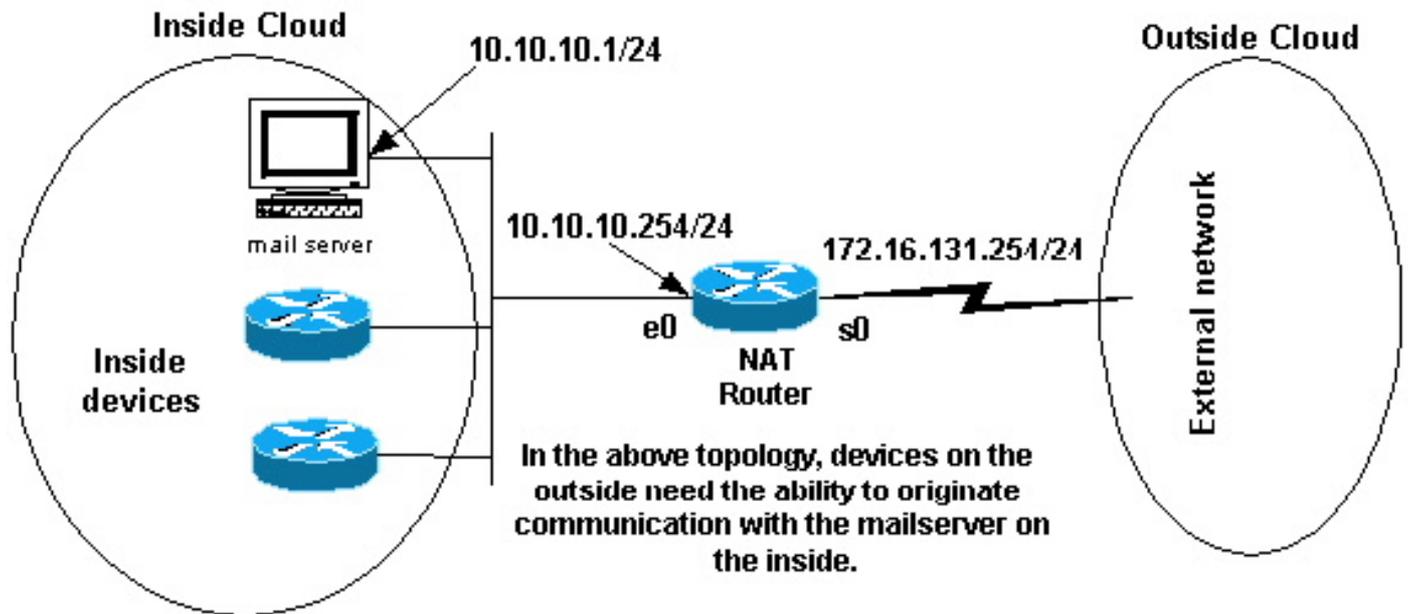
Quando `overloading` è configurato, il router conserva informazioni sufficienti dai protocolli di livello superiore (ad esempio, i numeri di porta TCP o UDP) per convertire nuovamente l'indirizzo globale nell'indirizzo locale corretto. Per le definizioni di indirizzo globale e indirizzo locale, fare riferimento

a [NAT: definizioni degli indirizzi locali e globali](#).

Al termine, verificare [che la conversione NAT funzioni come previsto](#).

2. Accesso ai dispositivi interni da Internet

In alcuni casi, è necessario che i dispositivi di una rete interna scambino informazioni con i dispositivi di una rete esterna, da cui è stata avviata la comunicazione, ad esempio per ricevere e-mail. In genere, i dispositivi della rete esterna inviano le e-mail a un server di posta che risiede sulla rete interna.



Origine delle comunicazioni

Configurazione della funzione NAT per autorizzare l'accesso ai dispositivi interni da Internet

Nell'esempio, occorre anzitutto definire le interfacce NAT interna ed esterna, come mostrato nel diagramma di rete precedente.

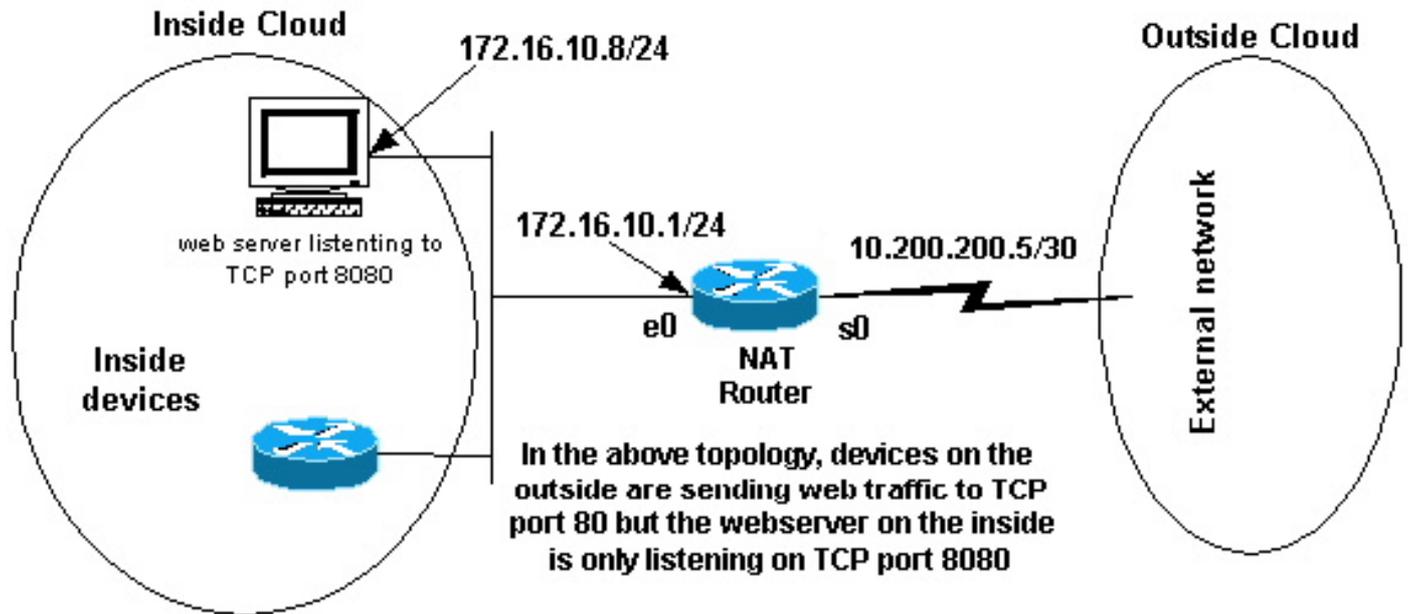
Quindi, occorre stabilire che gli utenti della rete interna possano avviare una comunicazione con i dispositivi della rete esterna. I dispositivi esterni devono poter avviare la comunicazione solo con il server di posta interno.

Infine, occorre configurare il NAT. Per realizzare gli obiettivi definiti, è possibile configurare insieme il NAT statico e il NAT dinamico. Per ulteriori informazioni sulla configurazione di questo esempio, fare riferimento a [Configurazione simultanea della NAT statica e dinamica](#). Al termine, verificare che la conversione NAT funzioni come previsto.

3. Reindirizzamento del traffico TCP su un'altra porta o indirizzo TCP

I dispositivi esterni devono poter avviare una comunicazione con i dispositivi interni anche in un'altra occasione, quando la rete interna ha un server Web. In alcune configurazioni, la porta

TCP su cui il server Web interno rimane in ascolto potrebbe essere diversa dalla porta 80. Ad esempio, potrebbe essere stata scelta la porta TCP 8080. In questo caso, il NAT permette di reindirizzare il traffico destinato alla porta TCP 80 in modo che venga diretto alla porta TCP 8080.



Porta TCP per il traffico Web

Dopo aver definito le interfacce come mostrato nel diagramma di rete precedente, si può decidere di voler reindirizzare a 172.16.10.8:8080 i pacchetti provenienti dalla rete esterna e destinati a 172.16.10.8:80. Per convertire il numero di porta TCP, è possibile usare il comando static nat. Qui di seguito viene mostrato un esempio di configurazione.

Configurazione della funzione NAT per reindirizzare il traffico TCP su un'altra porta o indirizzo TCP

```

Router NAT

interface ethernet 0
ip address 172.16.10.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.

interface serial 0
ip address 10.200.200.5 255.255.255.252
ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.

ip nat inside source static tcp 172.16.10.8 8080 172.16.10.8 80

!--- Static NAT command that states any packet received in the inside
!--- interface with a source IP address of 172.16.10.8:8080 is
!--- translated to 172.16.10.8:80.

```

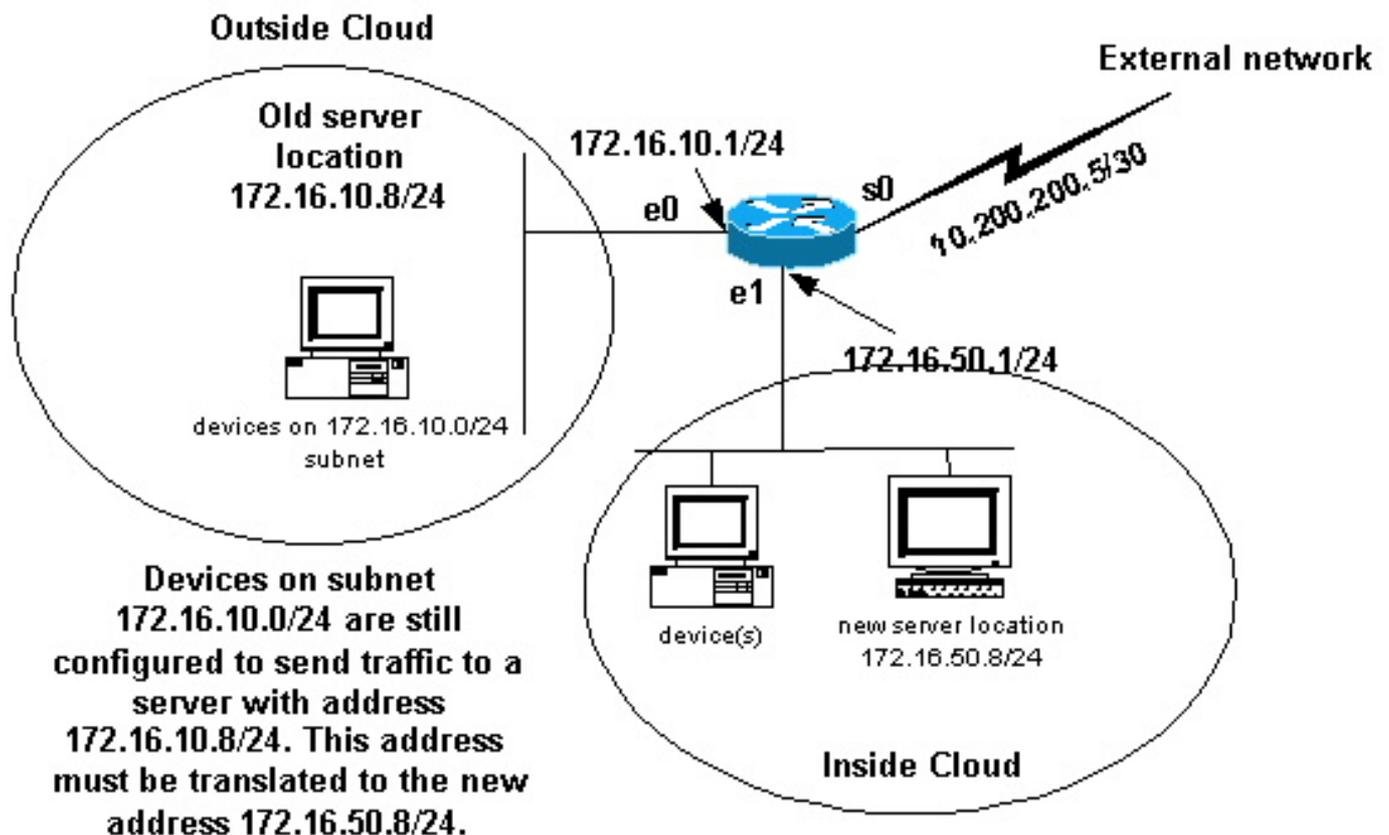
 Nota: tenere presente che nella configurazione con comando NAT statico, ogni pacchetto ricevuto sull'interfaccia interna con indirizzo di origine 172.16.10.8:8080 viene convertito in 172.16.10.8:80. Analogamente, ogni pacchetto ricevuto sull'interfaccia esterna con indirizzo di destinazione 172.16.10.8:80 viene convertito in 172.16.10.8:8080.

Al termine, verificare che la conversione NAT funzioni come previsto.

```
show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 172.16.10.8:80     172.16.10.8:8080 ---                ---
```

4. Uso della funzione NAT per una transizione di rete

La funzione NAT è utile quando si devono reindirizzare i dispositivi sulla rete o quando si deve sostituire un dispositivo. Supponiamo ad esempio di dover sostituire il server usato da tutti i dispositivi della rete con un server nuovo con nuovo indirizzo IP; riconfigurare tutti i dispositivi in modo che usino il nuovo indirizzo è un'operazione molto lunga. Nel frattempo, il NAT ci permette di convertire i pacchetti dei dispositivi con il vecchio indirizzo in modo che questi ultimi possano comunicare con il nuovo server.



Dopo aver definito le interfacce NAT come mostrato nell'immagine precedente, è possibile configurare la funzione NAT in modo che i pacchetti esterni destinati all'indirizzo del vecchio server (172.16.10.8) vengano convertiti e inviati all'indirizzo del nuovo server. Tenere presente che il nuovo server si trova su una LAN diversa e i dispositivi di questa LAN o raggiungibili tramite questa LAN (dispositivi all'interno della rete) devono essere configurati in modo che utilizzino l'indirizzo IP del nuovo server, se possibile.

Per realizzare questo obiettivo, è possibile usare il NAT statico. Ecco un esempio di configurazione.

Configurazione della funzione NAT per una transizione di rete

```
Router NAT

interface ethernet 0
ip address 172.16.10.1 255.255.255.0
ip nat outside

!--- Defines Ethernet 0 with an IP address and as a NAT outside interface.

interface ethernet 1
ip address 172.16.50.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.

interface serial 0
ip address 10.200.200.5 255.255.255.252

!--- Defines serial 0 with an IP address. This interface is not
!--- participating in NAT.

ip nat inside source static 172.16.50.8 172.16.10.8

!--- States that any packet received on the inside interface with a
!--- source IP address of 172.16.50.8 is translated to 172.16.10.8.
```

 Nota: in questo esempio, il comando NAT sull'origine interna implica anche che l'indirizzo di destinazione dei pacchetti ricevuti sull'interfaccia esterna venga convertito da 172.16.10.8 a 172.16.50.8.

Al termine, verificare [che la conversione NAT funzioni come previsto](#).

5. Uso della funzione NAT per le reti che si sovrappongono

Le reti sovrapposte si formano quando si assegnano ai dispositivi interni indirizzi IP già usati da altri dispositivi della rete esterna. Una rete sovrapposta si può formare anche in occasione di una fusione tra aziende, se entrambe usano indirizzi IP a norma [RFC 1918](#). Le due reti devono comunicare tra loro, possibilmente senza dover reindirizzare tutti i dispositivi.

Differenza tra mappatura uno-a-uno e molti-a-molti

Una configurazione NAT statica crea una mappatura uno-a-uno e converte un indirizzo specifico in un altro indirizzo. Questo tipo di configurazione crea una voce nella tabella NAT finché la configurazione è presente e consente agli host interni ed esterni di avviare una connessione. Ciò è particolarmente utile per gli host che forniscono servizi applicativi come posta, Web, FTP e così via. Ad esempio:

```
<#root>
```

```
Router(config)#
```

```
ip nat inside source static 10.3.2.11 10.41.10.12
```

```
Router(config)#
```

```
ip nat inside source static 10.3.2.12 10.41.10.13
```

il NAT dinamico è utile quando gli indirizzi disponibili sono inferiori al numero di host effettivo da convertire. Quando l'host avvia una connessione, nella tabella NAT viene creata una voce e tra gli indirizzi si stabilisce una mappatura uno-a-uno. Tuttavia, la mappatura può variare e dipende dall'indirizzo registrato disponibile nel pool al momento della comunicazione. Il NAT dinamico permette di avviare le sessioni solo dalla rete interna o dalla rete esterna per la quale è configurato. Se l'host non comunica per un determinato periodo di tempo, personalizzabile, le voci NAT dinamiche vengono rimosse dalla tabella di conversione. L'indirizzo viene quindi restituito al pool per essere usato da un altro host.

Completare questi passaggi della configurazione dettagliata come esercitazione:

1. Creare un pool di indirizzi.

```
<#root>
```

```
Router(config)#
```

```
ip nat pool MYPOOLEXAMPLE 10.41.10.1 10.41.10.41 netmask 255.255.255.0
```

2. Creare un elenco degli accessi per le reti interne da mappare.

```
<#root>
```

```
Router(config)#  
access-list 100 permit ip 10.3.2.0 0.0.0.255 any
```

3. Associare access-list 100, scegliendo di convertire l'indirizzo 10.3.2.0 0.0.0.255 della rete interna nel pool MYPOOLEXAMPLE, quindi sovraccaricare gli indirizzi.

<#root>

```
Router(config)#  
ip nat inside source list 100 pool MYPOOLEXAMPLE overload
```

Verificare il funzionamento del NAT

Al termine della configurazione, verificare che la conversione NAT funzioni come desiderato. Questa operazione può essere effettuata con un analizzatore di rete, i comandi show o i comandi di debug. Per un esempio dettagliato di verifica della NAT, fare riferimento a [Verifica del funzionamento della NAT e risoluzione dei problemi di base](#).

Conclusioni

Gli esempi riportati in questo documento illustrano le procedure di avvio rapido che possono essere utili per configurare e distribuire NAT.

La procedura rapida include:

1. Definire le interfacce NAT interna ed esterna.
2. Quali sono i risultati desiderati con la funzione NAT?
3. Configurare la funzione NAT in modo da realizzare gli obiettivi definiti nel passaggio 2.
4. Verificare il funzionamento del NAT.

In ciascuno degli esempi precedenti sono state utilizzate varie forme del comando ip nat insidecommand. Per raggiungere gli stessi obiettivi, è possibile anche utilizzare il comando ip nat outsideper tenere presente l'ordine delle operazioni NAT. Per gli esempi di configurazione che utilizzano i comandi ip nat outsidefare riferimento alla [configurazione di esempio che utilizza il comando IP NAT Outside Source List](#).

Negli esempi precedenti sono state illustrate queste azioni:

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

	<ul style="list-style-type: none">• Convertete la destinazione dei pacchetti IP trasmessi dall'esterno all'interno.
ip nat outside source	<ul style="list-style-type: none">• Convertete l'origine dei pacchetti IP trasmessi dall'esterno all'interno.• Convertete la destinazione dei pacchetti IP trasmessi dall'interno all'esterno.

Informazioni correlate

- [NAT: definizioni degli indirizzi locali e globali.](#)
- [Pagina di supporto NAT](#)
- [Pagina di supporto per i protocolli di routing IP](#)
- [Pagina di supporto per il routing IP](#)
- [Servizi di indirizzamento IP](#)
- [Ordine delle operazioni NAT](#)
- [Domande frequenti su Cisco IOS NAT](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

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).