

Konfiguration der Network Address Translation

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Schnellstartschritte für die Konfiguration und Bereitstellung von NAT](#)

[Definieren der internen und externen NAT-Schnittstellen](#)

[Beispiele](#)

[1. Internen Benutzern den Zugriff auf das Internet erlauben](#)

[NAT so konfigurieren, dass internen Benutzern der Zugriff auf das Internet ermöglicht wird](#)

[NAT so konfigurieren, dass internen Benutzern der Zugriff auf das Internet unter Überlastung ermöglicht wird](#)

[2. Internetzugriff auf interne Geräte zulassen](#)

[NAT so konfigurieren, dass das Internet auf interne Geräte zugreifen kann](#)

[3. Umleiten von TCP-Datenverkehr an einen anderen TCP-Port oder eine andere TCP-Adresse](#)

[NAT zum Umleiten von TCP-Datenverkehr an einen anderen TCP-Port oder eine andere TCP-Adresse konfigurieren](#)

[4. Verwenden Sie NAT für eine Netzwerkumstellung](#)

[Konfigurieren von NAT zur Verwendung während einer Netzwerkumstellung](#)

[5. Verwenden Sie NAT für Netzwerke, die sich überlappen](#)

[Unterschied zwischen 1:1- und Many-to-Many-Zuordnung](#)

[Überprüfen Sie den NAT-Betrieb](#)

[Schlussfolgerung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration der Network Address Translation (NAT) auf einem Cisco Router beschrieben.

Voraussetzungen

Anforderungen

Dieses Dokument erfordert grundlegende Kenntnisse der Begriffe, die im Zusammenhang mit NAT verwendet werden.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Router der Cisco 2500 Serie
- Cisco IOS® Softwareversion 12.2 (10b)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Schnellstartschritte für die Konfiguration und Bereitstellung von NAT

Anmerkung: In diesem Dokument bezieht sich der Begriff „Internet“ oder „Internetgerät“ auf ein Gerät in einem beliebigen externen Netzwerk.

Bei der Konfiguration von NAT ist es manchmal nicht einfach, den Einstieg zu finden, insbesondere wenn Sie mit NAT noch nicht vertraut sind. Anhand dieser Schritte können Sie definieren, was NAT tun soll und wie Sie es konfigurieren:

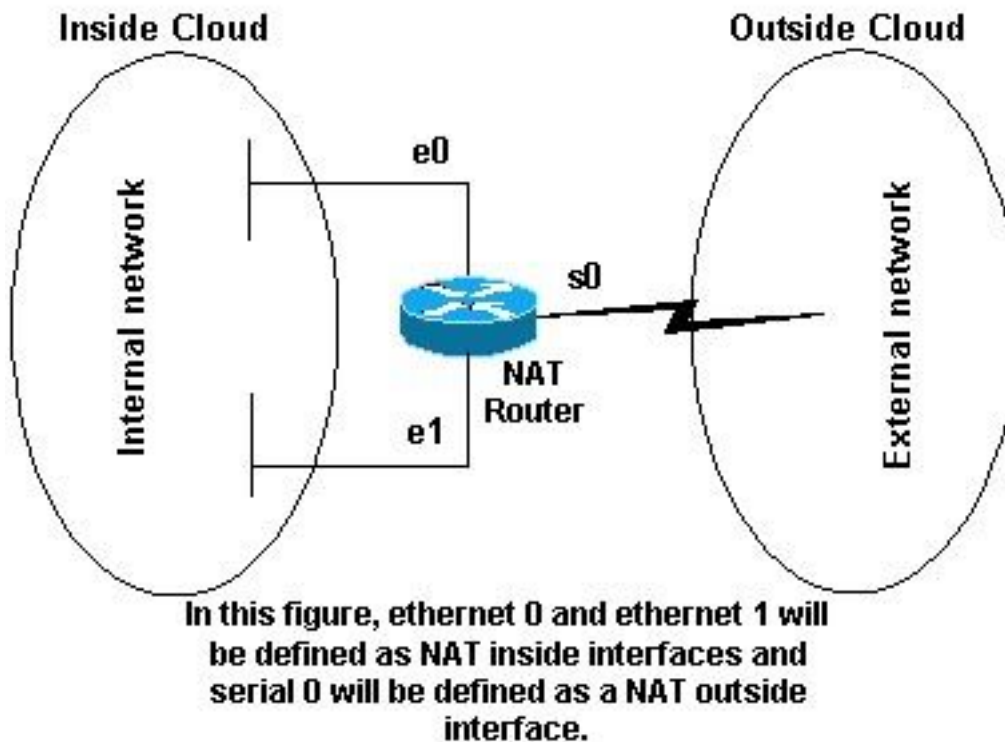
1. [Definition interner und externer NAT-Schnittstellen](#) Existieren Benutzer an mehreren Schnittstellen? Sind mehrere Schnittstellen für das Internet verfügbar?
2. Definieren Sie, was Sie mit NAT erreichen möchten. Möchten Sie [internen Benutzern den Zugriff auf das Internet ermöglichen](#)? Möchten Sie [dem Internet den Zugriff auf interne Geräte](#) (z. B. einen Mail- oder Webserver) ermöglichen? Möchten Sie den [TCP-Datenverkehr an einen anderen TCP-Port oder eine andere TCP-Adresse umleiten](#)? Möchten Sie [NAT während einer Netzwerkumstellung](#) verwenden (z. B. haben Sie eine Server-IP-Adresse geändert, bis Sie alle Clients aktualisieren können, von denen Sie möchten, dass die nicht aktualisierten Clients mit der ursprünglichen IP-Adresse auf den Server zugreifen können und den aktualisierten Clients erlauben, mit der neuen Adresse auf den Server zuzugreifen)? Möchten Sie die [Kommunikation von sich überschneidenden Netzwerken zulassen](#)?
3. Konfigurieren Sie NAT, um die zuvor definierten Ziele umzusetzen. Basierend auf Ihrer Definition in Schritt 2 müssen Sie bestimmen, welche der folgenden Funktionen Sie als Nächstes verwenden möchten: Statisches NAT, Dynamisches NAT, Overloading. Jede Kombination dieser Funktionen.
4. Überprüfen Sie den NAT-Betrieb.

Jedes dieser NAT-Beispiele führt Sie durch die Schritte 1 bis 3 der Schnellstartschritte im vorherigen Bild. Diese Beispiele beschreiben einige gängige Szenarien, in denen Cisco die Bereitstellung von NAT empfiehlt.

Definieren der internen und externen NAT-Schnittstellen

Der erste Schritt bei der Bereitstellung von NAT ist die Definition interner und externer NAT-

Schnittstellen. Sie finden es am einfachsten, Ihr internes Netzwerk als innen und das externe als außen zu definieren. Allerdings erfordern die Begriffe „intern“ und „extern“ eine Präzisierung. Die folgende Abbildung zeigt ein Beispiel dafür.



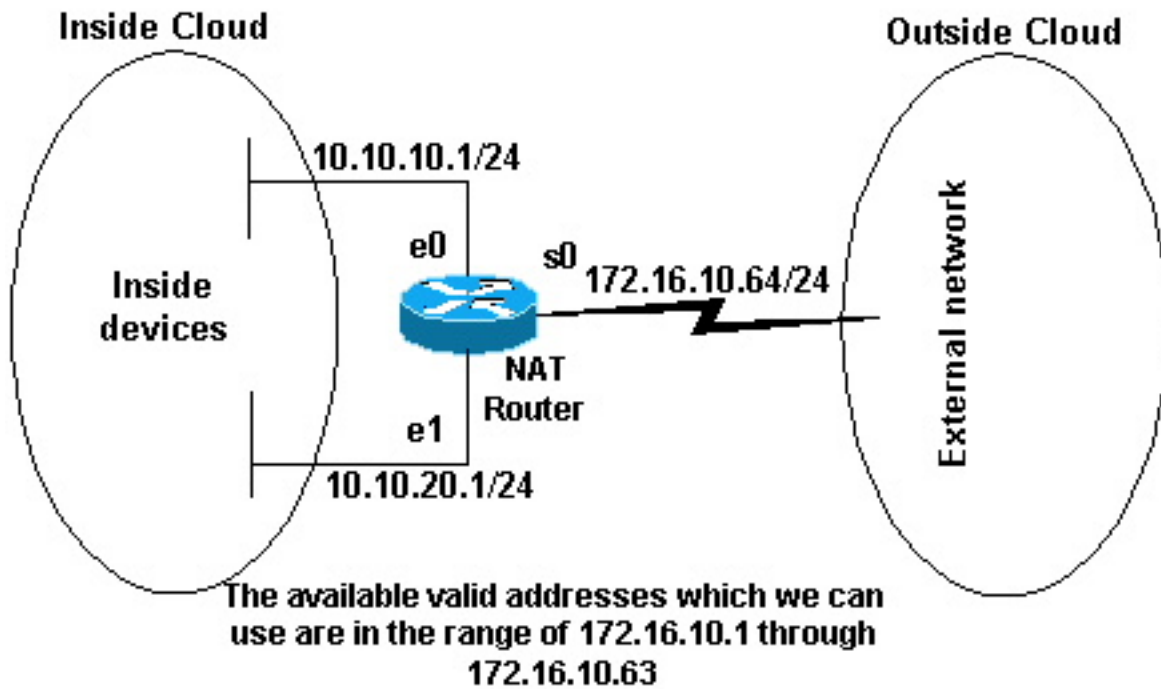
NAT-Topologie

Beispiele

1. Internen Benutzern den Zugriff auf das Internet erlauben

Es ist möglich, dass Sie internen Benutzern den Zugriff auf das Internet erlauben möchten, aber Sie haben nicht genügend gültige Adressen, um alle unterzubringen. Wenn die gesamte Kommunikation mit Geräten im Internet von den internen Geräten stammt, benötigen Sie eine einzige gültige Adresse oder einen Pool gültiger Adressen.

Diese Abbildung zeigt ein einfaches Netzwerkdiagramm mit den als intern und extern definierten Router-Schnittstellen.



Verfügbare gültige

Adressen

In diesem Beispiel soll NAT bestimmten Geräten (den ersten 31 von jedem Subnetz) innerhalb des Netzwerks erlauben, eine Kommunikation mit Geräten außerhalb des Netzwerks herzustellen, und die ungültige Adresse in eine gültige Adresse oder einen gültigen Adresspool übersetzen. Der Pool wurde als Adressbereich 172.16.10.1 bis 172.16.10.63 definiert.

NAT kann jetzt konfiguriert werden. Verwenden Sie die dynamische NAT, um die im vorherigen Image definierten Aufgaben durchzuführen. Bei dynamischer NAT ist die Übersetzungstabelle im Router zunächst leer und wird aufgefüllt, sobald der zu übersetzende Datenverkehr den Router passiert. Im Gegensatz dazu wird bei der statischen NAT eine Übersetzung statisch konfiguriert und in der Übersetzungstabelle platziert, ohne dass Datenverkehr erforderlich ist.

In diesem Beispiel können Sie NAT so konfigurieren, dass jedes interne Gerät in eine eindeutige gültige Adresse oder jedes interne Gerät in dieselbe gültige Adresse übersetzt wird. Diese zweite Methode ist bekannt als `overloading`. Ein Beispiel für die Konfiguration der einzelnen Methoden finden Sie hier.

NAT so konfigurieren, dass internen Benutzern der Zugriff auf das Internet ermöglicht wird

NAT-Router

```
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 serial 0 ip address 172.16.10.64 255.255.255.0 ip nat outside !--- Defines serial
an IP address and as a NAT outside interface. ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 2
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 p
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.
```

Anmerkung: Cisco empfiehlt dringend, keine Zugriffslisten zu konfigurieren, auf die von NAT-Befehlen verwiesen wird, mit **"permit any"**. Wenn Sie **"permit any"** in NAT verwenden, werden zu viele Router-Ressourcen verbraucht, die Netzwerkprobleme verursachen können.

Beachten Sie bei der vorherigen Konfiguration, dass nur die ersten 32 Adressen aus dem Subnetz 10.10.10.0 und die ersten 32 Adressen aus dem Subnetz 10.10.20.0 von **Zugriffsliste 7** zugelassen sind. Daher werden nur diese Quelladressen übersetzt. Es kann andere Geräte mit anderen Adressen im Netzwerk geben, aber diese werden nicht übersetzt.

Im letzten Schritt wird [überprüft, ob NAT wie vorgesehen funktioniert](#).

NAT so konfigurieren, dass internen Benutzern der Zugriff auf das Internet unter Überlastung ermöglicht wird

NAT-Router

```
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
an IP address and as a NAT outside interface. ip nat pool ovrlld 172.16.10.1 172.16.10.1 prefix 24
!--- Defines a NAT pool named ovrlld with a range of a single IP
!--- address, 172.16.10.1. ip nat inside source list 7 pool ovrlld overload !--- Indicates that any pack
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 ovrlld.
!--- 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 ac
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.
```

Hinweis in der vorherigen zweiten Konfiguration, dem NAT-Pool `ovrlld` hat nur einen Adressbereich. Das Schlüsselwort `overload` im Befehl `ip nat inside source list 7 pool ovrlld overload` ermöglicht NAT, mehrere interne Geräte in eine einzelne Adresse im Pool zu übersetzen.

Eine weitere Variante dieses Befehls ist `ip nat in Source List 7 Interface serial 0 overload`, wodurch NAT so konfiguriert wird, dass die der seriellen 0-Schnittstelle zugewiesene Adresse überlastet wird.

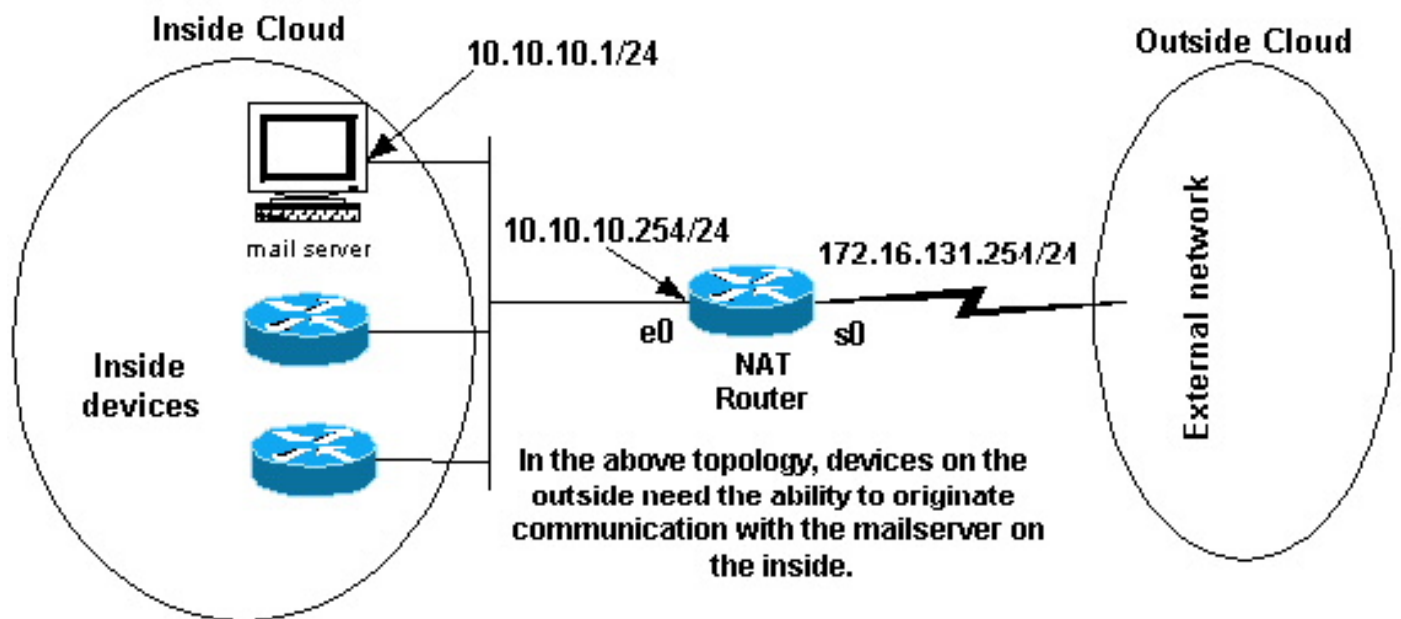
Wann `overloading` konfiguriert ist, speichert der Router genügend Informationen von übergeordneten Protokollen (z. B. TCP- oder UDP-Portnummern), um die globale Adresse wieder in die richtige lokale Adresse zu übersetzen. Definitionen für globale und lokale Adressen finden Sie unter NAT: [Globale und lokale Definitionen](#).

Im letzten Schritt wird [überprüft, ob NAT wie vorgesehen funktioniert](#).

2. Internetzugriff auf interne Geräte zulassen

Sie können interne Geräte benötigen, um Informationen mit Geräten im Internet auszutauschen,

wo die Kommunikation von den Internetgeräten, zum Beispiel E-Mail, initiiert wird. Es ist üblich, dass Geräte im Internet E-Mails an einen Mailserver im internen Netzwerk senden.



Kommunikation starten

NAT so konfigurieren, dass das Internet auf interne Geräte zugreifen kann

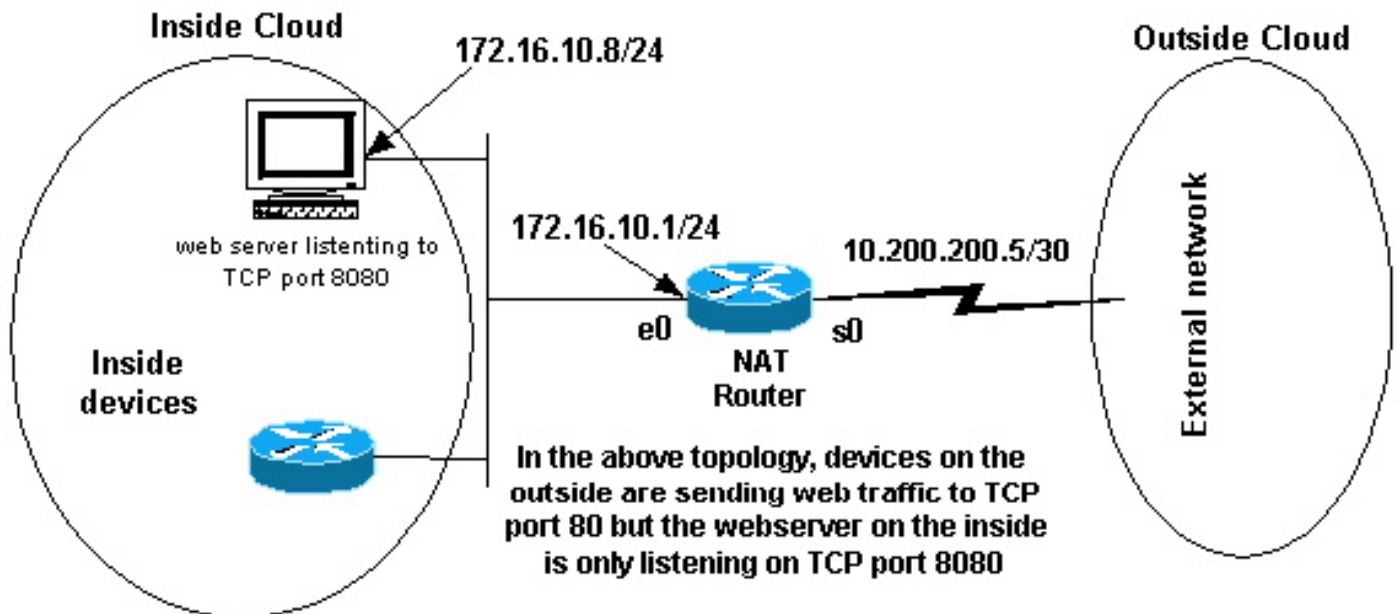
In diesem Beispiel definieren Sie zunächst die internen und externen NAT-Schnittstellen, wie im obigen Netzwerkdiagramm gezeigt.

Zweitens definieren Sie, dass Benutzer in der Lage sein sollen, die Kommunikation mit der Außenwelt zu initiieren. Geräte an der Außenseite müssen in der Lage sein, nur mit dem Mail-Server an der Innenseite zu kommunizieren.

Der dritte Schritt ist die Konfiguration von NAT. Um das zu erreichen, was Sie definiert haben, können Sie statische und dynamische NAT zusammen konfigurieren. Weitere Informationen zum Konfigurieren dieses Beispiels finden Sie unter [Gleichzeitige Konfiguration statischer und dynamischer NAT](#). Im letzten Schritt wird [überprüft, ob NAT wie vorgesehen funktioniert](#).

3. Umleiten von TCP-Datenverkehr an einen anderen TCP-Port oder eine andere TCP-Adresse

Ein Webserver im internen Netzwerk ist ein weiteres Beispiel dafür, wann Geräte im Internet die Kommunikation mit internen Geräten initiieren müssen. In einigen Fällen kann der interne Webserver so konfiguriert werden, dass er den Web-Datenverkehr über einen anderen TCP-Port als Port 80 überwacht. Beispielsweise kann der interne Webserver so konfiguriert werden, dass er den TCP-Port 8080 überwacht. In diesem Fall können Sie NAT verwenden, um an TCP-Port 80 gesendeten Datenverkehr zu TCP-Port 8080 umzuleiten.



TCP-Port für Webdatenverkehr

Nachdem Sie die Schnittstellen wie im vorherigen Netzwerkdiagramm dargestellt definiert haben, können Sie festlegen, dass die NAT Pakete von außen umleiten soll, die für 172.16.10.8:80 bis 172.16.10.8:8080 bestimmt sind. Sie können den Befehl `static nat` verwenden, um die TCP-Portnummer zu übersetzen, um dies zu erreichen. Hier sehen Sie eine Beispielkonfiguration.

NAT zum Umleiten von TCP-Datenverkehr an einen anderen TCP-Port oder eine andere TCP-Adresse konfigurieren

NAT-Router

```
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 outsi
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.
```

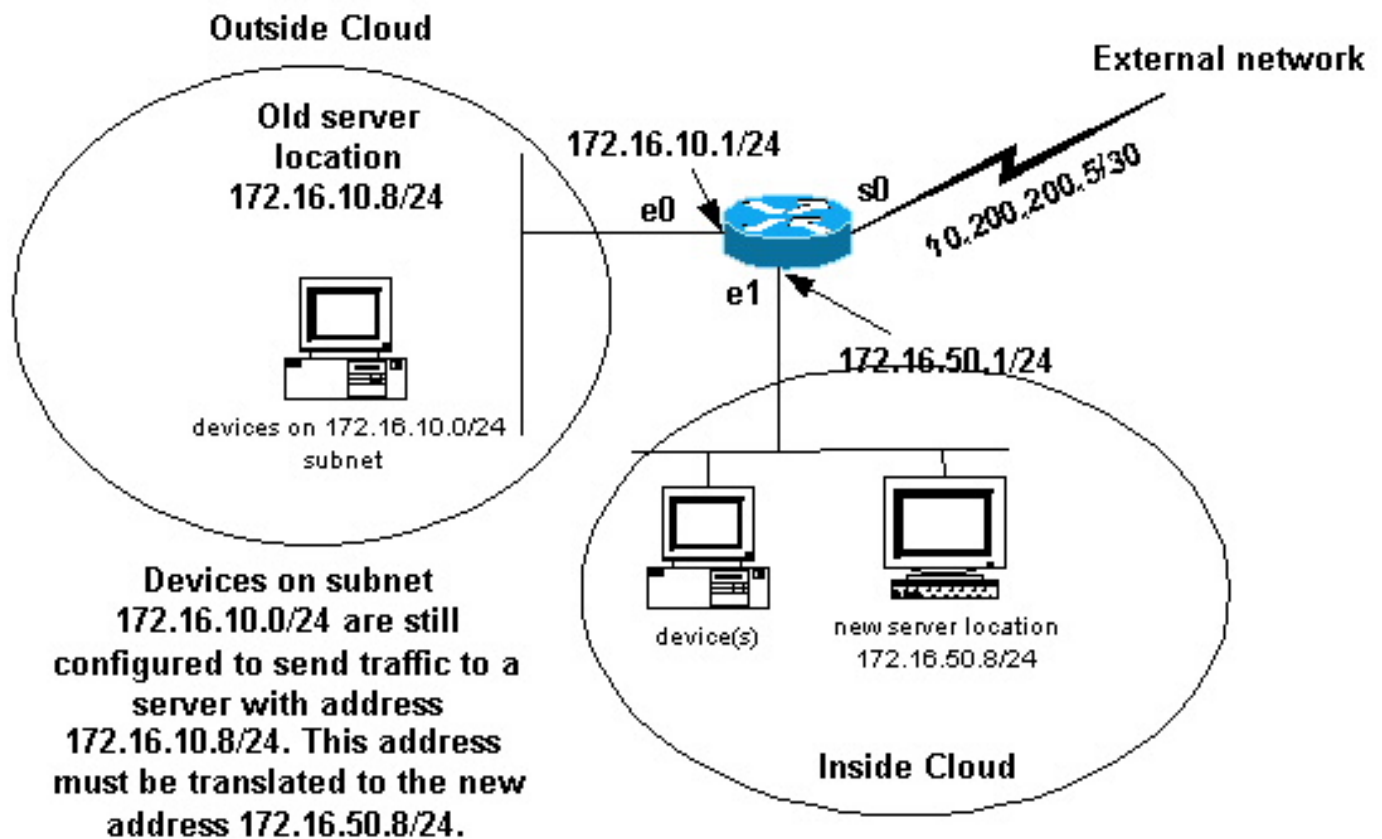
Anmerkung: Die Konfigurationsbeschreibung für den statischen NAT-Befehl gibt an, dass alle Pakete, die über die interne Schnittstelle empfangen werden, mit der Quelladresse 172.16.10.8:8080 in 172.16.10.8:80 übersetzt werden. Dies bedeutet auch, dass alle Pakete, die über die externe Schnittstelle empfangen werden, die Zieladresse 172.16.10.8:8 haben. 80 hat das Ziel in 172.16.10.8:8080 übersetzt.

Im letzten Schritt wird [überprüft, ob NAT wie vorgesehen funktioniert](#).

```
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. Verwenden Sie NAT für eine Netzwerkumstellung

NAT ist nützlich, wenn Sie Geräte im Netzwerk lesen müssen oder wenn Sie ein Gerät durch ein anderes ersetzen. Wenn beispielsweise alle Geräte im Netzwerk einen bestimmten Server verwenden und dieser Server durch einen neuen mit einer neuen IP-Adresse ersetzt werden muss, dauert die Neukonfiguration aller Netzwerkgeräte, um die neue Serveradresse zu verwenden, einige Zeit. In der Zwischenzeit können Sie NAT verwenden, um die Geräte mit der alten Adresse so zu konfigurieren, dass sie ihre Pakete für die Kommunikation mit dem neuen Server übersetzen.



NAT-Netzwerkumstellung

Nachdem Sie die NAT-Schnittstellen wie im vorherigen Bild dargestellt definiert haben, können Sie entscheiden, dass NAT die Übersetzung und Übertragung von Paketen von außen zulässt, die für die alte Serveradresse (172.16.10.8) bestimmt sind. Beachten Sie, dass sich der neue Server in einem anderen LAN befindet und dass Geräte in diesem LAN oder alle Geräte, die über dieses LAN erreichbar sind (Geräte im inneren Teil des Netzwerks), so konfiguriert werden müssen, dass sie die neue Server-IP-Adresse verwenden, wenn möglich.

Sie können statische NAT verwenden, um Ihre Anforderungen zu erfüllen. Hier eine Beispielformatierung:

Konfigurieren von NAT zur Verwendung während einer Netzwerkumstellung

NAT-Router

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

Anmerkung: Der Befehl `inside source NAT` in diesem Beispiel impliziert außerdem, dass Pakete, die an der externen Schnittstelle mit der Zieladresse 172.16.10.8 empfangen werden, die Zieladresse in 172.16.50.8 übersetzt haben.

Im letzten Schritt wird überprüft, ob [NAT wie vorgesehen funktioniert](#).

5. Verwenden Sie NAT für Netzwerke, die sich überlappen

Netzwerke, die sich überschneiden, ergeben sich, wenn Sie internen Geräten, die bereits von anderen Geräten im Internet verwendet werden, IP-Adressen zuweisen. Diese Netzwerke entstehen auch, wenn zwei Unternehmen, die beide [RFC 1918](#)-IP-Adressen in ihren Netzwerken verwenden, zusammengehen. Diese beiden Netzwerke müssen kommunizieren, vorzugsweise ohne dass alle ihre Geräte nachgerüstet werden.

Unterschied zwischen 1:1- und Many-to-Many-Zuordnung

Eine statische NAT-Konfiguration erstellt eine Eins-zu-Eins-Zuordnung und übersetzt eine bestimmte Adresse in eine andere. Diese Art von Konfiguration erstellt einen permanenten Eintrag in der NAT-Tabelle, solange die Konfiguration vorhanden ist, und ermöglicht internen und externen Hosts, eine Verbindung zu initiieren. Dies ist vor allem für Hosts nützlich, die Anwendungsservices wie E-Mail, Web, FTP usw. bereitstellen. Beispiele:

```
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
```

Dynamische NAT ist nützlich, wenn weniger Adressen verfügbar sind als die tatsächliche Anzahl der zu übersetzenden Hosts. Sie erstellt einen Eintrag in der NAT-Tabelle, wenn der Host eine Verbindung initiiert, und stellt eine Eins-zu-Eins-Zuordnung zwischen den Adressen her. Die Zuordnung kann jedoch variieren und hängt von der registrierten Adresse ab, die zum Zeitpunkt der Kommunikation im Pool verfügbar ist. Mit dynamischer NAT können Sitzungen nur von internen oder externen Netzwerken initiiert werden, für die sie konfiguriert ist. Dynamische NAT-Einträge werden aus der Übersetzungstabelle entfernt, wenn der Host über einen konfigurierbaren Zeitraum nicht kommuniziert. Die Adresse wird dann zur Verwendung durch einen anderen Host an den Pool zurückgegeben.

Führen Sie beispielsweise die folgenden Schritte der detaillierten Konfiguration aus:

1. Erstellen Sie einen Pool von Adressen

```
Router(config)#ip nat pool MYPOOLEXAMPLE 10.41.10.1 10.41.10.41 netmask 255.255.255.0
```

2. Erstellen Sie eine Zugriffsliste für die internen Netzwerke, die zugeordnet werden müssen.

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

3. Verknüpfen Sie die Zugriffsliste 100, die das interne Netzwerk 10.3.2.0 0.0.0.255 auswählen, um es dem Pool MYPOOLEXAMPLE zuzuordnen und dann die Adressen zu überladen.

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

Überprüfen Sie den NAT-Betrieb

Überprüfen Sie nach der Konfiguration von NAT, ob es wie erwartet funktioniert. Sie können dies auf verschiedene Weise tun: mit einem Netzwerkanalysator, **show**-Befehlen oder **debug**-Befehlen. Ein detailliertes Beispiel für die NAT-Verifizierung finden Sie unter [Überprüfung des NAT-Betriebs und der grundlegenden NAT](#) .

Schlussfolgerung

Die Beispiele in diesem Dokument veranschaulichen Schnellstart-Schritte, die Sie bei der Konfiguration und Bereitstellung von NAT unterstützen.

Zu diesen Schnellstart-Schritten gehören:

1. Definition interner und externer NAT-Schnittstellen
2. Was möchten Sie mit NAT erreichen?
3. Konfigurieren Sie NAT, um die in Schritt 2 definierten Ziele zu erreichen.
4. Überprüfen Sie den NAT-Betrieb.

In jedem der obigen Beispiele wurden verschiedene Formen des Befehls `ip nat inside` verwendet. Sie können auch den Befehl `ip nat outside` verwenden, um die gleichen Ziele zu erreichen. Beachten Sie jedoch die NAT-Reihenfolge der Vorgänge. Konfigurationsbeispiele, die die Befehle `ip nat outside` verwenden, finden Sie unter [Beispielkonfiguration, die den Befehl "IP NAT Outside Source List" verwendet](#) und unter [Beispielkonfiguration, die den Befehl "IP NAT Outside Source Static" verwendet](#).

In den obigen Beispielen wurden außerdem folgende Aktionen demonstriert:

Command	Aktion
<code>ip nat inside source</code>	<ul style="list-style-type: none">• Übersetzt die Quelle von IP-Paketen, die von innen nach außen übertragen werden.• Übersetzt das Ziel der IP-Pakete, die von außen nach innen übertragen werden• Übersetzt die Quelle der IP-Pakete, die von außen nach innen übertragen werden.
<code>ip nat outside source</code>	<ul style="list-style-type: none">• Übersetzt das Ziel der IP-Pakete, die von innen nach außen übertragen werden

Zugehörige Informationen

- [NAT: Lokale und globale Definitionen.](#)
- [NAT-Support-Seite](#)
- [Support-Seite für IP-Routed-Protokolle](#)
- [IP Routing-Support-Seite](#)
- [IP-Adressierungsdienste](#)
- [NAT Order of Operation](#)
- [Häufig gestellte Fragen zu NAT in Cisco IOS](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.