

Beispielkonfiguration mithilfe des Befehls "ip nat outside source list"

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zusammenfassung](#)

[Zugehörige Informationen](#)

[Einführung](#)

Dieses Dokument enthält eine Beispielkonfiguration mit dem Befehl **ip nat external source list** und eine kurze Beschreibung, was mit dem IP-Paket während des NAT-Prozesses geschieht. Mit diesem Befehl können Sie die Quelladresse der IP-Pakete übersetzen, die von außerhalb des Netzwerks in das Netzwerk übertragen werden. Bei dieser Aktion wird die Zieladresse der IP-Pakete übersetzt, die in die entgegengesetzte Richtung - von innen nach außen - übertragen werden. Dieser Befehl ist in Situationen nützlich, in denen sich die Netzwerkadressen überschneiden, wenn sich die Adressen außerhalb des Netzwerks befinden. Betrachten wir das [Netzwerkdiagramm](#) als Beispiel.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

[Verwendete Komponenten](#)

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt. Die Informationen in diesem Dokument basieren jedoch auf den folgenden Software- und Hardwareversionen:

- Cisco Router der Serie 2500

- Cisco IOS® Softwareversion 12.2(24a) auf allen Routern

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#).

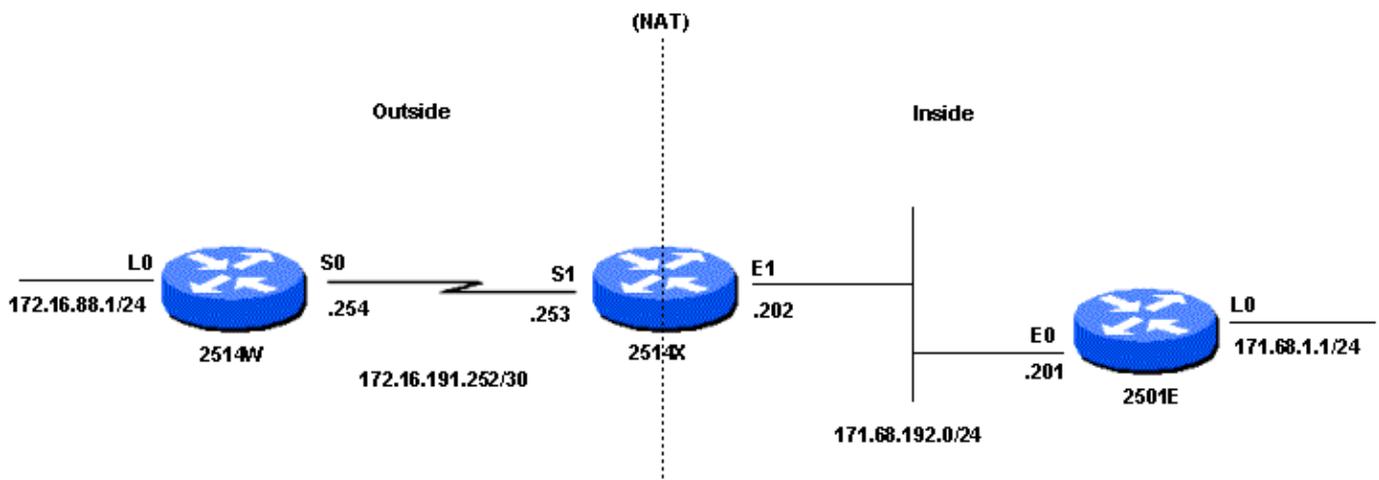
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das [Command Lookup Tool](#) ([nur registrierte Kunden](#)).

Netzwerkdigramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Wenn Ping von der Router 2514W Loopback0-Schnittstelle (172.16.88.1) an die Router 2501E Loopback0-Schnittstelle (171.68.1.1) gesendet wird, geschieht Folgendes:

Der Router 2514W leitet die Pakete an den Router 2514X weiter, da er mit einer Standardroute konfiguriert ist. Auf der externen Schnittstelle des Routers 2514X hat das Paket die Quelladresse (SA) 172.16.88.1 und die Zieladresse (DA) 171.68.1.1. Da die SA in der Zugriffsliste 1 zulässig ist, die vom Befehl `ip nat` außerhalb der **Quellliste** verwendet wird, wird sie in eine Adresse aus dem NAT-Pool Net171 übersetzt. Beachten Sie, dass der Befehl `ip nat outside source list` auf den [NAT-Pool "Net171"](#) verweist. In diesem Fall wird die Adresse in 171.68.16.10 übersetzt, die erste verfügbare Adresse im NAT-Pool. Nach der Übersetzung sucht der Router 2514X in der Routing-Tabelle nach dem Ziel und leitet das Paket weiter. Router 2501E erkennt das Paket an seiner eingehenden Schnittstelle mit einer SA von 171.68.16.10 und einer DA von 171.68.1.1. Die Antwort lautet: Senden Sie eine ICMP-Echoantwort (Internet Control Message Protocol) an

171.68.16.10. Wenn keine Route vorhanden ist, wird das Paket verworfen. In diesem Fall verfügt er über eine (Standard-)Route, daher sendet er ein Paket an Router 2514X, wobei die SA 171.68.1.1 und die DA 171.68.16.10 verwendet werden. Der Router 2514X erkennt das Paket an seiner internen Schnittstelle und prüft die Route zur Adresse 171.68.16.10. Verfügt sie nicht über eine Antwort, antwortet sie mit einer nicht erreichbaren ICMP-Antwort. In diesem Fall wird die Route nach [171.68.16.10](#) über die **Add-Route**-Option des Befehls **ip nat external source** hinzugefügt, der eine Hostroute auf Basis der Übersetzung zwischen der externen globalen und externen lokalen Adresse hinzufügt. Das Paket wird also zurück zur Adresse 172.16.88.1 übersetzt. und leitet das Paket über seine externe Schnittstelle weiter.

Konfigurationen

Router 2514 W

```
hostname 2514W
!
!--- Output suppressed. interface Loopback0 ip address
172.16.88.1 255.255.255.0 ! !--- Output suppressed.
interface Serial0 ip address 172.16.191.254
255.255.255.252 no ip mroute-cache ! !--- Output
suppressed. ip classless ip route 0.0.0.0 0.0.0.0
172.16.191.253 !--- Default route to forward packets to
2514X. ! !--- Output suppressed.
```

Router 2514X

```
hostname 2514X
!
!--- Output suppressed. ! interface Ethernet1 ip address
171.68.192.202 255.255.255.0 ip nat inside no ip mroute-
cache no ip route-cache ! !--- Output suppressed.
interface Serial1 ip address 172.16.191.253
255.255.255.252 ip nat outside no ip mroute-cache no ip
route-cache clockrate 2000000 ! ip nat pool Net171
171.68.16.10 171.68.16.254 netmask 255.255.255.0 !---
NAT pool defining Outside Local addresses to be used for
translation. ! ip nat outside source list 1 pool Net171
add-route !--- Configures translation for Outside Global
addresses !--- with the NAT pool. ip classless ip route
172.16.88.0 255.255.255.0 172.16.191.254 ip route
171.68.1.0 255.255.255.0 171.68.192.201 !--- Static
routes for reaching the loopback interfaces !--- on
2514W and 2501E. access-list 1 permit 172.16.88.0
0.0.0.255 !--- Access-list defining Outside Global
addresses to be translated. ! !--- Output suppressed. !
```

Router 2501E

```
hostname 2501E
!
!--- Output suppressed. interface Loopback0 ip address
171.68.1.1 255.255.255.0 ! interface Ethernet0 ip
address 171.68.192.201 255.255.255.0 ! !--- Output
suppressed. ip classless ip route 0.0.0.0 0.0.0.0
171.68.192.202 !--- Default route to forward packets to
2514X. ! !--- Output suppressed.
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Mit dem Befehl [show ip nat translations](#) können die Übersetzungseinträge überprüft werden, wie in der unten stehenden Ausgabe gezeigt.

```
2514X# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 171.68.1.1         171.68.1.1       171.68.16.10      172.16.88.1
--- ---                ---              171.68.16.10      172.16.88.1
```

2514X#

Die obige Ausgabe zeigt, dass die externe globale Adresse 172.16.88.1, die Adresse auf der Loopback0-Schnittstelle des Routers 2514W, in die externe lokale Adresse 171.68.16.10 übersetzt wird.

Sie können den Befehl [show ip route](#) verwenden, um die Einträge in der Routing-Tabelle zu überprüfen, wie folgt:

```
2514X# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is not set

```
171.68.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    171.68.192.0/24 is directly connected, Ethernet1
S    171.68.1.0/24 [1/0] via 171.68.192.201
S    171.68.16.10/32 [1/0] via 172.16.88.1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S    172.16.88.0/24 [1/0] via 172.16.191.254
C    172.16.191.252/30 is directly connected, Serial1
```

2514X#

Die Ausgabe zeigt eine /32-Route für die externe lokale Adresse 171.68.16.10, die aufgrund der **Add-Route**-Option des Befehls **ip nat external source** erstellt wird. Diese Route wird für das Routing und die Übersetzung von Paketen verwendet, die von innen nach außen über das Netzwerk übertragen werden.

[Fehlerbehebung](#)

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Diese Ausgabe ist das Ergebnis der Ausführung der Befehle **debug ip packet** und **debug ip nat** auf Router 2514X, während vom Router 2514W Loopback0-Schnittstellenadresse (172.16.88.1) an die Router 2501E Loopback0-Schnittstellenadresse (11) gepingt wird 71.68.1.1):

```

*Mar 1 00:02:48.079: NAT*: s=172.16.88.1->171.68.16.10, d=171.68.1.1 [95]
!--- The source address in the first packet arriving on !--- the outside interface is first
translated. *Mar 1 00:02:48.119: IP: tableid=0, s=171.68.16.10 (Serial1), d=171.68.1.1
(Ethernet1), routed via
RIB
*Mar 1 00:02:48.087: IP: s=171.68.16.10 (Serial1), d=171.68.1.1 (Ethernet1), g=171.68.192.201,
len
100, forward
!--- The ICMP echo request packet with the translated source address !--- is routed and
forwarded on the inside interface. *Mar 1 00:02:48.095: IP: tableid=0, s=171.68.1.1 (Ethernet1),
d=171.68.16.10 (Serial1), routed via
RIB
!--- The ICMP echo reply packet arriving on the inside interface !--- is first routed based on
the destination address. *Mar 1 00:02:48.099: NAT: s=171.68.1.1, d=171.68.16.10->172.16.88.1
[95]
!--- The destination address in the packet is then translated. *Mar 1 00:02:48.103: IP:
s=171.68.1.1 (Ethernet1), d=172.16.88.1 (Serial1), g=172.16.191.254, len 1
00, forward
!--- The ICMP echo reply packet with the translated destination !--- address is forwarded on the
outside interface.

```

Das oben beschriebene Verfahren wird für jedes auf der externen Schnittstelle empfangene Paket wiederholt.

Zusammenfassung

Der Hauptunterschied zwischen der Verwendung des Befehls **ip nat external source list** (dynamic NAT) anstelle des Befehls **ip nat external static** (static NAT) besteht darin, dass in der Übersetzungstabelle keine Einträge vorhanden sind, bis der Router (für NAT konfiguriert) die Übersetzungskriterien des Pakets überprüft. Im obigen Beispiel erfüllt das Paket mit dem SA 172.16.88.1 (das in die externe Schnittstelle des Routers 2514X integriert ist) die Zugriffsliste 1, die Kriterien, die der Befehl **ip nat außerhalb der Quellliste** verwendet. Aus diesem Grund müssen Pakete vom externen Netzwerk stammen, bevor Pakete aus dem internen Netzwerk mit der Router 2514W Loopback0-Schnittstelle kommunizieren können.

In diesem Beispiel sind zwei wichtige Punkte zu beachten.

Zunächst wird bei der Übertragung des Pakets von außen nach innen zuerst die Übersetzung durchgeführt, und anschließend wird die Routing-Tabelle auf das Ziel überprüft. Wenn das Paket von innen nach außen übertragen wird, wird zuerst die Routing-Tabelle für das Ziel geprüft, und anschließend wird die Übersetzung durchgeführt.

Zweitens ist zu beachten, welcher Teil des IP-Pakets bei Verwendung der oben angegebenen Befehle übersetzt wird. Die folgende Tabelle enthält eine Richtlinie:

Befehl	Aktion
ip nat außerhalb der Quellliste	<ul style="list-style-type: none"> • übersetzt die Quelle der IP-Pakete, die von außen nach innen reisen • übersetzt das Ziel der IP-Pakete, die innerhalb eines Gebiets nach außen übertragen werden.
ip nat in der Quellliste	<ul style="list-style-type: none"> • übersetzt die Quelle von IP-Paketen, die von innen nach außen übertragen werden

- | | |
|--|--|
| | <ul style="list-style-type: none">• übersetzt das Ziel der IP-Pakete, die von außen nach innen reisen. |
|--|--|

Die oben genannten Richtlinien deuten darauf hin, dass es mehr als eine Möglichkeit gibt, ein Paket zu übersetzen. Abhängig von Ihren spezifischen Anforderungen sollten Sie festlegen, wie die NAT-Schnittstellen (innerhalb oder außerhalb) definiert werden und welche Routen die Routing-Tabelle vor oder nach der Übersetzung enthalten soll. Beachten Sie, dass der Teil des Pakets, der übersetzt werden soll, von der Route des Pakets und der Konfiguration von NAT abhängt.

Zugehörige Informationen

- [Network Address Translation auf einem Stick](#)
- [Support-Seite für NAT-Technologie](#)
- [Technischer Support - Cisco Systems](#)