

# ip nat outside source list コマンドを使用した設定例

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[要約](#)

[関連情報](#)

## 概要

このドキュメントでは、ip nat outside source list コマンドを使用した設定例が紹介され、NAT プロセス中に IP パケットがどのように処理されるかについて簡単に説明されています。このコマンドを使用して、ネットワークの外部からネットワークの内部に送信される IP パケットの送信元アドレスを変換できます。このアクションによって、(ネットワークの内部から外部へ) 逆方向に送られる IP パケットの宛先アドレスが変換されます。このコマンドは、オーバーラップするネットワーク (内部のネットワーク アドレスがネットワークの外部アドレスにオーバーラップする) などの状況で役に立ちます。例として、下記の[ネットワーク ダイアグラム](#)を取り上げます。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。ただし、このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 2500 シリーズ ルータ
- すべてのルータで動作している Cisco IOS® ソフトウェア リリース 12.2(24a)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

## 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

## ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

ルータ 2514W の Loopback0 インターフェイス ( 172.16.88.1 ) からルータ 2501E の Loopback0 インターフェイス ( 171.68.1.1 ) への ping を実行すると、次の事象が発生します。

デフォルト ルートを使用して設定されているため、ルータ 2514W によりパケットがルータ 2514X に転送されます。ルータ 2514x の外部インターフェイスに到達した ping パケットには、送信元アドレス ( SA ) として 172.16.88.1、宛先アドレス ( DA ) として 171.68.1.1 が含まれています。SA が access-list 1 ( ip nat outside source list コマンドで使用される ) で許可されている場合、SA は NAT プール Net171 にあるアドレスに変換されます。ip nat outside source list コマンドでは、[NAT プール「Net171」](#)が参照されていることに注意してください。この場合、アドレスは、この NAT プールで最初に使用できるアドレスの 171.68.16.10 に変換されます。変換後、ルータ 2514x は、ルーティング テーブル内で宛先を検索し、パケットをルーティングします。ルータ 2501e の着信インターフェイスに到達したパケットには、SA として 171.68.16.10、DA として 171.68.1.1 が含まれています。ルータ 2501e はこのパケットに応答するために、Internet Control Message Protocol ( ICMP ) エコー応答を 171.68.16.10 に送信します。ルートがない場合はパケットを廃棄します。この例では、ルータ 2501e に ( デフォルト ) 経路が設定されているため、SA 171.68.1.1、DA 171.68.16.10 を使用して、ルータ 2514x にパケットが送信されます。ルータ 2514X では、その内部インターフェイスでパケットを受信すると、アドレス 171.68.16.10 へのルートがチェックされます。経路がない場合、ICMP 到達不能応答で応答します。この例では、[171.68.16.10](#) へのルートが存在するため、外部グローバル アドレスと外部ローカル アドレス間の変換に基づいてホスト ルートを追加する ip nat outside source コマンドの add-route オプションによって、パケットのアドレスが 172.16.88.1 に逆変換され、外部インターフェイスからパケットがルーティングされます。

## 設定

```
ルータ 2514w
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.
```

## ルータ 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. !
```

## ルータ 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.
```

## 確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

特定の **show** コマンドは、[Output Interpreter Tool](#) ( [登録ユーザ専用](#) ) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

[次の出力で示されているように、変換エントリを確認するために show ip nat translations コマンドを使用できます。](#)

```
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#
```

上記の出力には、ルータ 2514W の Loopback0 インターフェイス上のアドレスである外部グローバルアドレス 172.16.88.1 が外部ローカルアドレス 171.68.16.10 に変換されることが示されています。

[次に示されているように、ルーティングテーブルエントリを確認するために show ip route コマンドを使用できます。](#)

```
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#

上記の出力には、ip nat outside source コマンドの add-route オプションに従って作成される、外部ローカルアドレス 171.68.16.10 の /32 ルートが示されています。このルートは、ネットワークの内部から外部へ送信されるパケットのルーティングと変換に使用されます。

## トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

この出力はルータ 2514W loopback0 インターフェイス アドレスから ping している間、ルータ 2514X の debug ip packet および debug ip nat コマンドを実行した結果です ( 172.16.88.1 ) ルータ 2501E loopback0 インターフェイス アドレスに ( 171.68.1.1 ) :

```
*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 100, forward !--- The ICMP echo reply packet with the translated destination !--- address is forwarded on the outside interface.
```

上述の手順は、外部インターフェイス上で受信される各パケットで繰り返されます。

## 要約

ip nat outside source static コマンド ( スタティック NAT ) の代わりに ip nat outside source list コマンド ( ダイナミック NAT ) を使用した場合の大きな違いは、( NAT が設定された ) ルータによってパケットの変換基準が確認されるまで、変換テーブルにエントリがない点にあります。上記の例では、SA 172.16.88.1 を持つパケット ( ルータ 2514X の外部インターフェイスに到達したパケット ) は、ip nat outside source list コマンドで使用される基準、access-list 1 に適合しています。このため、内部ネットワークから送信されるパケットがルータ 2514W の loopback0 インターフェイスと通信するためには、まず外部ネットワークからパケットが発信される必要があります。

この例には、重要事項が 2 点含まれています。

第 1 に、外部から内部へパケットが送られるときは、最初に変換が行われてから、ルーティングテーブル内で宛先がチェックされます。内部から外部へパケットが送られるときは、最初にルーティングテーブル内で宛先がチェックされてから、変換が行われます。

第 2 に、上記の各コマンドを使用したときに、IP パケットのどの部分が変換されるかを確認することが重要です。次の表に、ガイドラインを示します。

コマンド	Action
------	--------

<b>ip nat outside source list</b>	<ul style="list-style-type: none"><li>• 外部から内部へ送られる IP パケットの送信元が変換される。</li><li>• 内部から外部へ送られる IP パケットの宛先が変換される。</li></ul>
<b>ip nat inside source list</b>	<ul style="list-style-type: none"><li>• 内部から外部へ送られる IP パケットの送信元が変換される。</li><li>• 外部から内部へ送られる IP パケットの宛先が変換される。</li></ul>

上記のガイドラインが示しているのは、パケットの変換方法が 1 通りではないということです。固有のニーズに従って、NAT インターフェイスの定義方法（内部または外部）と、変換前後にルーティング テーブルに含まれる経路を決定する必要があります。パケットの変換される部分は、パケットが送られる方向と、NAT の設定方法によって異なる点に留意してください。

## **関連情報**

- [スティック上のネットワーク アドレス変換](#)
- [NAT テクノロジーに関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)