Configurer la commande IP NAT Outside Source List

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)
- [Informations générales](#)
- [Conventions](#)

[Configurer](#)

- [Diagramme du réseau](#)
- [Configurations](#)

[Vérifier](#)

[Dépannage](#)

[Résumé](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer la commande `ip nat outside source list` et décrit ce qui arrive au paquet IP pendant le processus NAT.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les routeurs Cisco exécutant la version du logiciel Cisco IOS®.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Vous pouvez utiliser cette commande pour traduire l'adresse source des paquets IP qui circulent de l'extérieur du réseau vers l'intérieur du réseau. Cette action traduit l'adresse de destination des paquets IP qui voyagent dans la direction opposée, de l'intérieur vers l'extérieur du réseau. Cette commande est utile dans des situations telles que des réseaux qui se chevauchent, où les adresses réseau internes chevauchent des adresses qui se trouvent à l'extérieur du réseau. Prenons le schéma du réseau comme exemple.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous à Conventions des conseils techniques de Cisco.

Configurer

Dans cette section, vous trouverez les informations nécessaires à la configuration des fonctionnalités décrites dans ce document.

Remarque : Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'outil Command Lookup Tool (clients enregistrés uniquement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

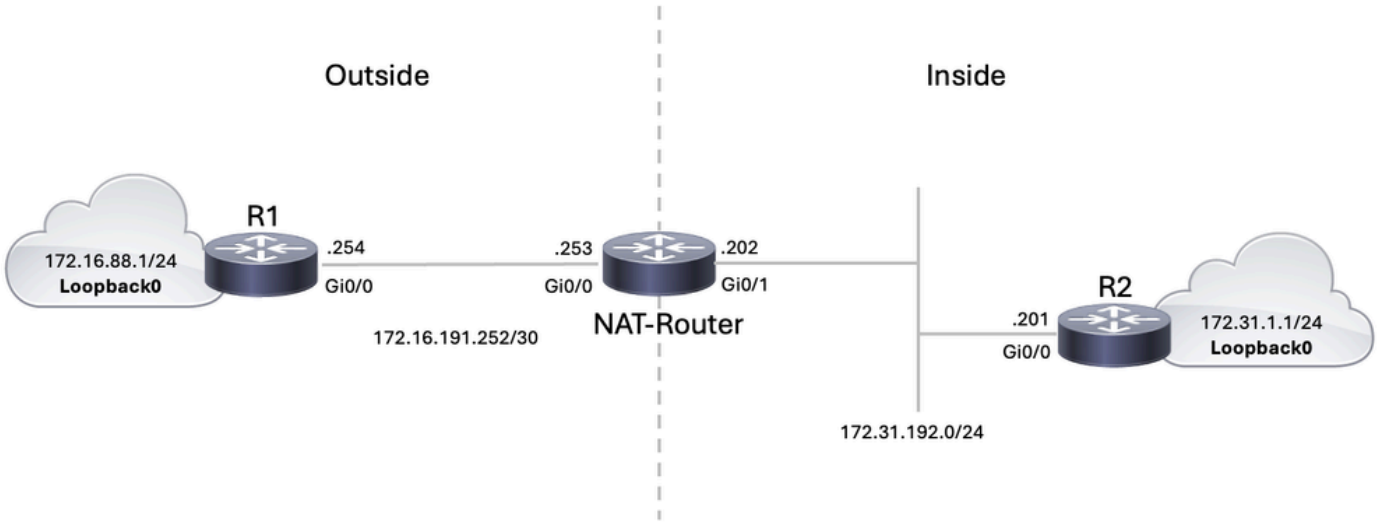


Diagramme du réseau

Lorsqu'une requête ping provient de l'interface Loopback0 du routeur R1 (172.16.88.1) vers l'interface Loopback0 du routeur R2 (172.31.1.1), la séquence d'événements suivante se produit :

1. Transfert de paquets : Le routeur R1 transfère les paquets au routeur NAT, car il est configuré avec une route par défaut. Sur l'interface externe du routeur NAT, le paquet a une

adresse source (SA) de 172.16.88.1 et une adresse de destination (DA) de 172.31.1.1.

2. Traduction NAT : Comme la SA est autorisée par access-list 1, qui est utilisée par la commande ip nat outside source list, elle est traduite en une adresse du pool NAT « NET ». Dans ce cas, l'adresse est traduite en 172.31.16.10, qui est la première adresse disponible dans le pool NAT.
3. Routage vers la destination : Après la traduction, le routeur NAT recherche la destination dans sa table de routage et achemine le paquet. Le routeur R2 reçoit le paquet sur son interface d'entrée avec une SA de 172.31.16.10 et une DA de 172.31.1.1. Le routeur R2 répond en envoyant une réponse d'écho ICMP (Internet Control Message Protocol) à 172.31.16.10. Si le routeur R2 n'a pas de route vers 172.31.16.10, il abandonne le paquet.
4. Traitement des réponses : Dans ce cas, le routeur R2 a une route par défaut, de sorte qu'il envoie le paquet de réponse au routeur NAT, à l'aide d'une SA de 172.31.1.1 et d'une DA de 172.31.16.10. Le routeur NAT reçoit le paquet sur son interface interne et recherche une route vers l'adresse 172.31.16.10. S'il n'a pas de route, il répond par une réponse ICMP inaccessible.
5. Traduction et routage arrière : Dans ce cas, le routeur NAT a une route vers 172.31.16.10 en raison de l'option add-route de la commande ip nat outside source, qui ajoute une route hôte basée sur la traduction entre l'adresse globale externe et l'adresse locale externe. Le routeur NAT retraduit le paquet en l'adresse source d'origine (172.16.88.1) et le route de son interface externe vers le routeur R1.

Configurations

Routeur R1

```
hostname R1
!

!--- Output suppressed.

!
interface Loopback0
 ip address 172.16.88.1 255.255.255.0
!

!--- Output suppressed.

!
interface GigabitEthernet0/0
 ip address 172.16.191.254 255.255.255.252
 duplex auto
 speed auto
!

!--- 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.
```

Routeur NAT-Router

```
hostname NAT-Router
!

!--- Output suppressed.

!
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 pool NET 172.31.16.10 172.31.16.254 netmask 255.255.255.0

!--- NAT pool defining Outside Local addresses to be used for translation.

!
ip nat outside source list 1 pool NET add-route
!

!--- Configures translation for Outside Global addresses !--- with the NAT pool.

!
ip route 172.16.88.0 255.255.255.0 172.16.191.254
ip route 172.31.1.0 255.255.255.0 172.31.192.201
!

!--- Static routes for reaching the loopback interfaces on R1 and R2.

!
access-list 1 permit 172.16.88.0 0.0.0.255
!

!--- Access-list defining Outside Global addresses to be translated.
!--- Output suppressed.
```

Routeur R2

```
hostname 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.
```

Vérifier

Cette section fournit des informations que vous pouvez utiliser pour confirmer que votre configuration fonctionne correctement.

Certaines commandes show sont prises en charge par l'outil Output Interpreter Tool (clients enregistrés uniquement), qui vous permet d'afficher une analyse du résultat des **show** commandes.

La commande show ip nat translations peut être utilisée pour vérifier les entrées de traduction, comme indiqué dans ce résultat :

<#root>

NAT-Router#

show ip nat translations

```
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                172.31.16.10       172.16.88.1
icmp 172.31.1.1:0      172.31.1.1:0       172.31.16.10:0     172.16.88.1:0
NAT-Router#
```

Le résultat montre que l'adresse globale externe 172.16.88.1, qui est l'adresse sur l'interface Loopback0 du routeur R1, est traduite en l'adresse locale externe 172.31.16.10.

Vous pouvez utiliser la commande show ip route pour vérifier les entrées de la table de routage, comme indiqué :

<#root>

NAT-Router#

show ip route

```
Codes: L - local, C - connected, S - static, 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
       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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
S        172.16.88.0/24 [1/0] via 172.16.191.254
C        172.16.191.252/30 is directly connected, GigabitEthernet0/0
L        172.16.191.253/32 is directly connected, GigabitEthernet0/0
      172.31.0.0/16 is variably subnetted, 4 subnets, 2 masks
S        172.31.1.0/24 [1/0] via 172.31.192.201

S        172.31.16.10/32 [1/0] via 172.16.88.1

C        172.31.192.0/24 is directly connected, GigabitEthernet0/1
L        172.31.192.202/32 is directly connected, GigabitEthernet0/1
NAT-Router#
```

Le résultat montre une route /32 pour l'adresse locale externe 172.31.16.10, qui est créée en raison de l'option add-route de la commande ip nat outside source. Cette route est utilisée pour le routage et la traduction des paquets qui circulent de l’intérieur vers l’extérieur du réseau.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Ce résultat est le résultat de l'exécution des commandes debug ip packet et debug ip nat sur le routeur NAT-Router, tout en envoyant une requête ping à partir de l'adresse d'interface loopback0 du routeur R1 (172.16.88.1) vers l'adresse d'interface loopback0 du routeur R2 (172.31.1.1) :

```
<#root>

!--- The source address in the first packet arriving on the outside interface is first translated.

*Oct  4 20:26:48.839: NAT: s=172.16.88.1->172.31.16.10, d=172.31.1.1 [0]

!--- The ICMP echo request packet with the translated source address is routed and forwarded on the ins

*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), len 1
*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), len 1
*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), len 1
*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), len 1

*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), g=172.

*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), len 1
```

```
!--- The ICMP echo reply packet arriving on the inside interface, is first routed based on the destinat

Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.31.16.10, len 100, input feature, Com
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.31.16.10, len 100, input feature, St
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.31.16.10, len 100, input feature, Vi
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.31.16.10, len 100, input feature, Vi
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.31.16.10, len 100, input feature, MC

!--- The destination address in the packet is then translated.


*Oct 4 20:26:48.841: NAT: s=172.31.1.1, d=172.31.16.10->172.16.88.1 [0]


!--- The ICMP echo reply packet with the translated destination address is forwarded on the outside int

*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), len 10
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), len 10
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), len 10
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), len 10

*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), g=172.1

*Oct  4 20:26:48.843: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), len 10


*Oct  4 20:26:48.845: NAT*: s=172.16.88.1->172.31.16.10, d=172.31.1.1 [1]
*Oct  4 20:26:48.846: NAT*: s=172.31.1.1, d=172.31.16.10->172.16.88.1 [1]
*Oct  4 20:26:48.848: NAT*: s=172.16.88.1->172.31.16.10, d=172.31.1.1 [2]
*Oct  4 20:26:48.849: NAT*: s=172.31.1.1, d=172.31.16.10->172.16.88.1 [2]
*Oct  4 20:26:48.851: NAT*: s=172.16.88.1->172.31.16.10, d=172.31.1.1 [3]
*Oct  4 20:26:48.852: NAT*: s=172.31.1.1, d=172.31.16.10->172.16.88.1 [3]
*Oct  4 20:26:48.854: NAT*: s=172.16.88.1->172.31.16.10, d=172.31.1.1 [4]
*Oct  4 20:26:48.855: NAT*: s=172.31.1.1, d=172.31.16.10->172.16.88.1 [4]
```

La procédure précédente est répétée pour chaque paquet reçu sur l’interface externe.

Résumé

La principale différence entre l'utilisation de la commande ip nat outside source list (NAT dynamique) au lieu de la commande ip nat outside source static (NAT statique) est qu'il n'y a aucune entrée dans la table de traduction jusqu'à ce que le routeur (configuré pour NAT) vérifie les critères de traduction du paquet. Dans l'exemple précédent, le paquet avec la SA 172.16.88.1 (qui vient dans l'interface externe de NAT-Router) satisfait access-list 1, les critères utilisés par la commande ip nat outside source list. Pour cette raison, les paquets doivent provenir du réseau externe avant que les paquets du réseau interne puissent communiquer avec l’interface loopback0 du routeur R1.

Il y a deux choses importantes à noter dans cet exemple :

1. Lorsque le paquet se déplace de l’extérieur vers l’intérieur, la traduction se produit en premier, puis la table de routage est vérifiée pour la destination. Lorsque le paquet se déplace de l’intérieur vers l’extérieur, la table de routage est d’abord vérifiée pour la destination, puis la traduction se produit.

2. Il est important de noter quelle partie du paquet IP est traduite lors de l'utilisation de chacune des commandes précédentes. Le tableau suivant fournit une ligne directrice :

Commande	Action
ip nat outside source list	• traduit la source des paquets IP qui circulent de l'extérieur vers l'intérieur • traduit la destination des paquets IP qui circulent de l'intérieur vers l'extérieur
ip nat inside source list	• traduit la source des paquets IP qui circulent de l'intérieur vers l'extérieur • traduit la destination des paquets IP qui circulent de l'extérieur vers l'intérieur

Ces directives indiquent qu'il existe plusieurs façons de traduire un paquet. Selon vos besoins spécifiques, vous pouvez déterminer comment définir les interfaces NAT (internes ou externes) et quelles routes la table de routage contient avant ou après la traduction. Gardez à l'esprit que la partie du paquet qui est traduite dépend de la direction dans laquelle le paquet se déplace et de la façon dont vous avez configuré la NAT.

Informations connexes

- Traduction d'adresses réseau sur un bâton
- Page d'assistance technologique NAT
- Support technique - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.