Configurer l'équilibrage de charge du serveur à l'aide de la NAT dynamique

Contenu

Introduction

Ce document décrit comment configurer le trafic TCP d'équilibrage de charge du serveur NAT (Network Address Translation) sur les routeurs Cisco IOS®.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. Ce document s’applique à tous les routeurs et à tous les commutateurs Cisco qui exécutent le 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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Objectif

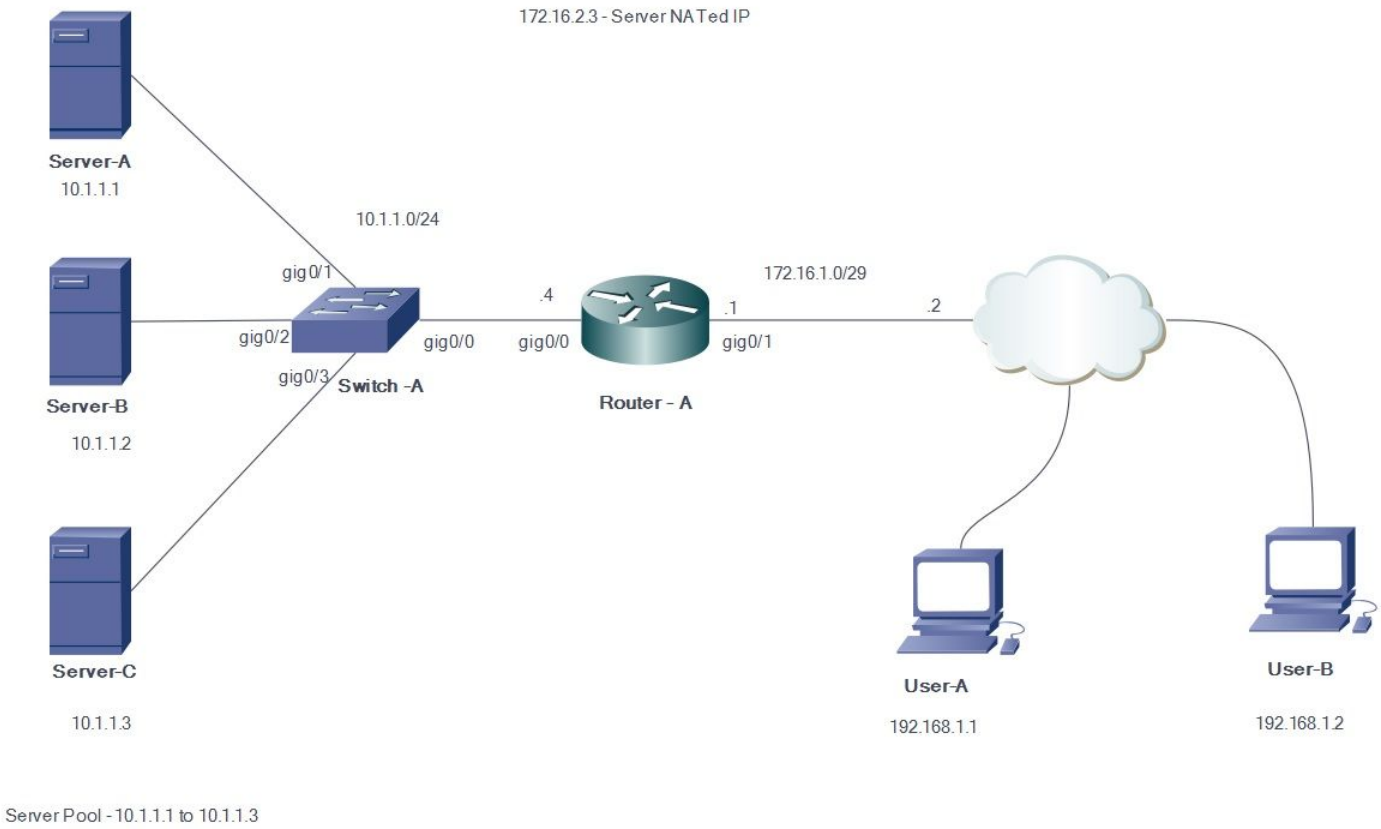
Les utilisateurs qui accèdent au serveur local depuis l'extérieur d'Internet accèdent au serveur à l'aide d'une URL ou d'une adresse IP unique. Toutefois, le périphérique NAT est utilisé pour charger le trafic utilisateur sur plusieurs serveurs identiques avec du contenu en miroir.

Description

Les utilisateurs externes A et B accèdent au contenu du serveur Web avec l'adresse IP externe visible 172.16.2.3 (adresse IP virtuelle des serveurs). Le routeur NAT traduit le trafic destiné à 172.16.1.3 en adresses IP internes 10.1.1.1, 10.1.1.2 et 10.1.1.3 de manière circulaire et le transmet au serveur respectif. Chaque nouvelle session initiée par l'utilisateur externe est traduite en adresse IP de serveur physique suivante.

Configuration

Diagramme du réseau



Étapes

1. L'utilisateur A initie une connexion TCP avec l'adresse IP du serveur virtuel 172.16.2.3.
2. Le routeur NAT, à la réception de la demande de connexion, crée une entrée de traduction NAT qui alloue l'adresse IP du serveur réel disponible suivant (par exemple, 10.1.1.1).
3. Le routeur NAT remplace l’adresse IP de destination par l’adresse IP réelle allouée et transfère le paquet.
4. Le serveur reçoit le paquet et répond à la source.

5. Le routeur NAT reçoit le paquet retourné par le serveur et effectue la recherche dans la table NAT. Le routeur traduit ensuite l'adresse source en adresse IP du serveur virtuel (172.16.2.3) et transfère le paquet.
6. L'utilisateur B lance une session TCP avec l'adresse IP virtuelle du serveur 172.16.2.3. À la réception de la demande de connexion, le routeur NAT la traduit en adresse IP réelle du serveur suivant (par exemple, 10.1.1.2), puis transfère le paquet au serveur.

Puisque la NAT statique est bidirectionnelle dans l'autre direction, la destination du paquet sera traduite. Lors de cette forme de NAT, elle est déclenchée par l'envoi de paquets TCP. L'envoi du protocole ICMP (Internet Control Message Protocol) peut ne pas déclencher la traduction NAT.

Le trafic non TCP est dirigé vers la première adresse du pool.

Contrairement à la NAT source interne statique et à la PAT source interne statique, le routeur ne répond pas aux requêtes ARP concernant l'adresse globale, sauf si cette adresse n'est pas attribuée à son interface.Par conséquent, il peut être nécessaire de l'ajouter à une interface comme l'interface secondaire. Il n'est pas possible de rediriger les ports avec cette méthode de traduction (par exemple, 80 et 1087). Les ports doivent correspondre.

> **Note**: L'adresse IP du pool NAT n'a pas besoin d'être identique à l'adresse IP de l'interface externe. Afin d'illustrer la même chose, l'exemple utilise une adresse IP d'un bloc différent 172.16.2.x par rapport au sous-réseau IP de l'interface réel 172.16.1.x.

1. Définissez un pool d'adresses contenant les adresses des vrais serveurs.
   ip nat pool NATPOOL 10.1.1.1 10.1.1.3 prefix-length 24 type rotary
2. Définissez une liste d'accès qui autorise l'adresse du serveur virtuel.
   access-list 1 permit host 172.16.2.3
3. Activez une traduction dynamique des adresses de destination internes.
   ip nat inside destination list pool

   ip nat inside destination list 1 pool NATPOOL
4. Définissez les interfaces internes et externes de NAT.
   ```
   Interface gig0/0
   ip address 10.1.1.4 255.255.255.0
   Ip nat inside

   Interface gig0/1
   ip address 172.16.1.1 255.255.255.248
   Ip nat outside
   ```
   Les adresses IP 10.1.1.1, 10.1.1.2 et 10.1.1.3 seront désormais distribuées de manière rotative lorsque quelqu'un tente d'accéder à l'adresse IP 172.16.2.3

Vérification

Afin de vérifier cela, initialisez plusieurs sessions TCP depuis des hôtes externes vers l'adresse IP virtuelle. Debug IP NAT tla sortie de traduction ranslation/show ip nat translation peut être utilisée pour la vérification.

```
Router#
Router#
*Jul 24 13:27:41.193: NAT*: s=192.168.1.1, d=172.16.2.3->10.1.1.3 [22864]
*Jul 24 13:27:41.196: NAT*: s=10.1.1.3->172.16.2.3, d=192.168.1.1 [18226]
Router#
```

```
*Jul 24 13:27:44.329: NAT*: s=192.168.2.1, d=172.16.2.3->10.1.1.1 [35533]
*Jul 24 13:27:44.331: NAT*: s=10.1.1.1->172.16.2.3, d=192.168.2.1 [14573]
*Jul 24 13:27:44.332: NAT*: s=192.168.2.1, d=172.16.2.3->10.1.1.1 [35534]
*Jul 24 13:27:44.332: NAT*: s=192.168.2.1, d=172.16.2.3->10.1.1.1 [35535]
*Jul 24 13:27:44.332: NAT*: s=192.168.2.1, d=172.16.2.3->10.1.1.1 [35536]
*Jul 24 13:27:44.333: NAT*: s=10.1.1.1->172.16.2.3, d=192.168.2.1 [14574]
*Jul 24 13:27:44.365: NAT*: s=10.1.1.1->172.16.2.3, d=192.168.2.1 [14575]
*Jul 24 13:27:44.365: NAT*: s=10.1.1.1->172.16.2.3, d=192.168.2.1 [14576]
*Jul 24 13:27:44.368: NAT*: s=192.168.2.1, d=172.16.2.3->10.1.1.1 [35537]
Router#
*Jul 24 13:27:44.369: NAT*: s=192.168.2.1, d=172.16.2.3->10.1.1.1 [35538]
*Jul 24 13:27:44.369: NAT*: s=192.168.2.1, d=172.16.2.3->10.1.1.1 [35539]
*Jul 24 13:27:44.369: NAT*: s=192.168.2.1, d=172.16.2.3->10.1.1.1 [35540]
*Jul 24 13:27:44.371: NAT*: s=10.1.1.1->172.16.2.3, d=192.168.2.1 [14577]
*Jul 24 13:27:44.574: NAT*: s=10.1.1.1->172.16.2.3, d=192.168.2.1 [14578]
Router#
*Jul 24 13:27:46.474: NAT*: s=10.1.1.1->172.16.2.3, d=192.168.2.1 [14579]
*Jul 24 13:27:46.478: NAT*: s=192.168.2.1, d=172.16.2.3->10.1.1.1 [35541]
*Jul 24 13:27:46.478: NAT*: s=192.168.2.1, d=172.16.2.3->10.1.1.1 [35542]
*Jul 24 13:27:46.479: NAT*: s=10.1.1.1->172.16.2.3, d=192.168.2.1 [14580]
Router#sh ip nat tr
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.16.2.3:23      10.1.1.1:23        192.168.2.1:49703  192.168.2.1:49703
tcp 172.16.2.3:23      10.1.1.2:23        192.168.2.1:50421  192.168.2.1:50421
tcp 172.16.2.3:80      10.1.1.3:80        192.168.1.1:26621  192.168.1.1:26621
Router#
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Limites

- Il ne peut pas détecter si un serveur interne du groupe échoue. Cela signifie que Cisco IOS transfère toujours le trafic vers les serveurs du groupe, quel que soit leur état de fonctionnement.
- Il ne peut pas déterminer les charges réelles des serveurs internes, de sorte qu'il ne peut pas effectuer l'équilibrage de charge efficacement.