Konfigurieren des Server-Lastenausgleichs mithilfe von dynamischem NAT

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der TCP-Datenverkehr für den Lastenausgleich des Network Address Translation (NAT)-Servers auf Cisco IOS® Routern konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt. Dieses Dokument gilt für alle Cisco Router und Switches, auf denen Cisco IOS ausgeführt wird.

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.

Hintergrundinformationen

Zweck

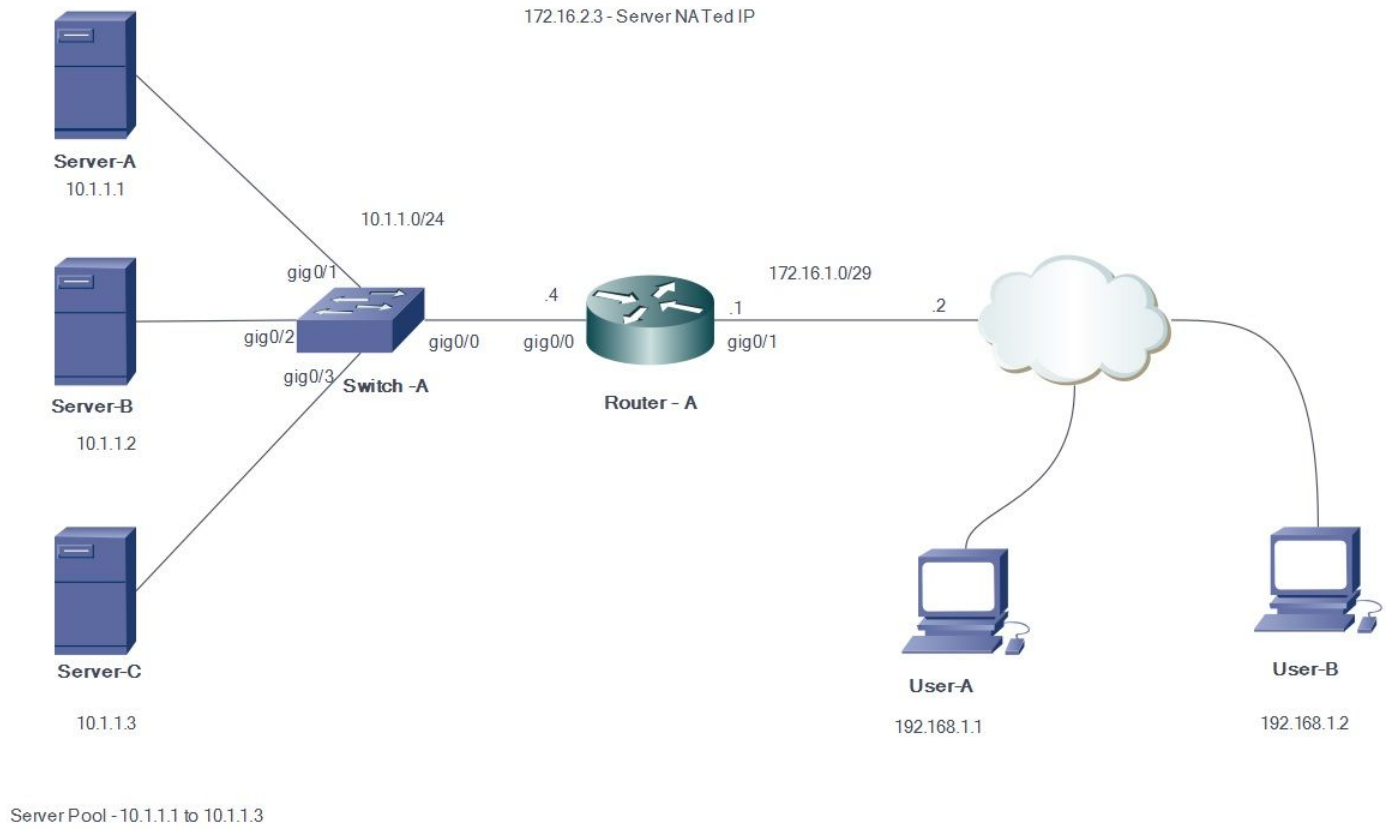
Benutzer, die von einem externen Internet auf den lokalen Server zugreifen, greifen über eine einzige URL oder IP-Adresse auf den Server zu. Das NAT-Gerät wird jedoch verwendet, um den Datenverkehr des Benutzers auf mehrere identische Server mit gespiegelten Inhalten zu laden.

Beschreibung

Externe Benutzer A und B greifen auf den Inhalt des Webservers mit der von außen sichtbaren IP-Adresse 172.16.2.3 (virtuelle IP-Adresse der Server) zu. Der NAT-Router übersetzt den für 172.16.1.3 bestimmten Datenverkehr in Round-Robin-Form in die internen IP-Adressen 10.1.1.1, 10.1.1.2 und 10.1.1.3 und leitet ihn an den entsprechenden Server weiter. Jede neue vom externen Benutzer initiierte Sitzung wird in die nächste physische Server-IP-Adresse übersetzt.

Konfigurieren

Netzwerkdiagramm



Schritte

1. Benutzer-A initiiert eine TCP-Verbindung mit der IP-Adresse des virtuellen Servers 172.16.2.3.
2. Der NAT-Router erstellt beim Empfang der Verbindungsanforderung einen NAT-Übersetzungseintrag, der die nächste verfügbare tatsächliche Server-IP-Adresse zuweist (z. B. 10.1.1.1).
3. Der NAT-Router ersetzt die Ziel-IP-Adresse durch die zugewiesene tatsächliche IP-Adresse

und leitet das Paket weiter.
4. Der Server empfängt das Paket und antwortet zurück an die Quelle.
5. Der NAT-Router empfängt das vom Server zurückgegebene Paket und führt die NAT-Tabellensuche durch. Der Router übersetzt dann die Quelladresse in die IP-Adresse des virtuellen Servers (172.16.2.3) und leitet das Paket weiter.
6. Benutzer-B initiiert eine TCP-Sitzung mit der virtuellen IP-Adresse des Servers 172.16.2.3. Beim Empfang der Verbindungsanforderung übersetzt der NAT-Router diese in die nächste verfügbare tatsächliche Server-IP-Adresse (z. B. 10.1.1.2) und leitet das Paket dann an den Server weiter.

Da die statische NAT in die andere Richtung bidirektional verläuft, wird das Ziel des Pakets übersetzt. Bei dieser Form der NAT wird sie durch Senden von TCP-Paketen ausgelöst. Das Senden von ICMP (Internet Control Message Protocol) löst möglicherweise nicht die NAT-Übersetzung aus.

Nicht-TCP-Datenverkehr wird an die erste Adresse im Pool weitergeleitet.

Anders als statische interne NAT und statische interne PAT antwortet der Router nicht auf ARP-Anfragen zur globalen Adresse, es sei denn, diese Adresse ist seiner Schnittstelle nicht zugewiesen. Daher kann es erforderlich sein, sie einer Schnittstelle wie der sekundären hinzuzufügen. Es ist nicht möglich, Ports mit dieser Übersetzungsmethode umzuleiten (z. B. 80 und 1087). Die Ports müssen übereinstimmen.

> **Hinweis**: Die IP-Adresse des NAT-Pools muss nicht mit der IP-Adresse der externen Schnittstelle übereinstimmen. Um dies zu veranschaulichen, wird im Beispiel eine IP-Adresse aus einem anderen Block 172.16.2.x als das tatsächliche IP-Subnetz 172.16.1.x der Schnittstelle verwendet.

1. Definieren Sie einen Adresspool, der die Adressen der echten Server enthält.
   ```
   ip nat pool NATPOOL 10.1.1.1 10.1.1.3 prefix-length 24 type rotary
   ```
2. Definieren Sie eine Zugriffsliste, die die Adresse des virtuellen Servers zulässt.
   ```
   access-list 1 permit host 172.16.2.3
   ```
3. Aktivieren Sie eine dynamische Übersetzung von internen Zieladressen.
   ```
   ip nat inside destination list pool

   ip nat inside destination  list 1 pool NATPOOL
   ```
4. Definieren von NAT für interne und externe Schnittstellen
   ```
   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
   ```
   Die IP-Adressen 10.1.1.1, 10.1.1.2 und 10.1.1.3 werden jetzt rotierend ausgegeben, wenn jemand versucht, auf die IP-Adresse 172.16.2.3 zuzugreifen.

Überprüfen

Um dies zu überprüfen, starten Sie mehrere TCP-Sitzungen von externen Hosts zur virtuellen IP-Adresse. Debug-IP NAT tÜbersetzung/Ausgabe der ip nat ip kann zur Überprüfung verwendet werden.

```
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#
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Einschränkungen

- Sie kann nicht erkennen, ob ein interner Server in der Gruppe ausfällt. Das bedeutet, dass das Cisco IOS Datenverkehr unabhängig von seinem Betriebsstatus immer an die Server in der Gruppe weiterleitet.
- Sie kann die tatsächliche Last der internen Server nicht bestimmen, daher kann sie den Lastenausgleich nicht effizient durchführen.