So behandelt NAT ICMP-Fragmente

Inhalt

Einführung

In diesem Dokument wird erläutert, wie Network Address Translation (NAT) bei der Konfiguration der NAT-Überladung ICMP-Fragmente (Internet Control Message Protocol) behandelt. Informationen zur NAT-Überladung finden Sie in der FAQ zu NAT.

Die Bearbeitung von ICMP-Fragmenten hängt vom Zustand der NAT-Übersetzungstabelle und der Reihenfolge ab, in der der NAT-Router die ICMP-Fragmente empfängt. Wir werden uns drei verschiedene Fälle ansehen, in denen wir zwei Pings von 172.16.0.1 bis 172.17.1.2 mit einer Länge von je 3600 Byte (drei IP-Fragmente) senden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Fall 1

In diesem Szenario wird NAT einen vollständig erweiterten Übersetzungseintrag in der Übersetzungstabelle erstellen. Sobald dies geschehen ist und es keine anderen verwendbaren Adressen im NAT-Pool gibt, verwirft NAT alle Fragmente, die vor dem ersten Fragment (Fragment 0) eines Pakets empfangen wurden.

Zu Beginn führt nur eine Adresse im Pool eine Überlastung durch. Die NAT-Übersetzungstabelle ist leer. und die NAT-Konfiguration wird wie folgt angezeigt:

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

Sehen wir uns an, was passiert, wenn Pakete am NAT-Router ankommen.

1. Paket 1 fragmentiert 0 ein, und NAT erstellt einen vollständig erweiterten Übersetzungseintrag. NAT übersetzt und leitet anschließend Paket 1 Fragment 0 weiter. Die Übersetzungstabelle erscheint nun wie folgt:
   ```
   Pro   Inside global         Inside local        Outside local       Outside global
   icmp  10.10.10.3:24320      172.16.0.1:24320    172.17.1.2:24320    172.17.1.2:24320
   ```
   Beachten Sie die Nummer 24320 in der oben stehenden Übersetzungstabelle. Dies ist der ICMP-ident-Wert, der im ICMP-Header des IP-Datagramms enthalten ist. Nur Fragment 0 des IP-Datagramms enthält diesen ICMP-Header. Um festzustellen, ob mehrere Fragmente Teil desselben Pakets sind, muss NAT den IP-ident-Wert verfolgen, der im IP-Header aller Fragmente aus dem ursprünglichen IP-Datagramm gefunden wurde. Wenn mehrere Fragmente den gleichen IP-Wert für den Identent wie Fragment 0 haben, das die erweiterte Übersetzung erstellt hat, übersetzt NAT diese Fragmente mit demselben erweiterten Übersetzungseintrag. Weitere Informationen zum IP-Identifikationsfeld finden Sie in RFC 791 . Weitere Informationen zum ICMP-Identifikationsfeld finden Sie in RFC 792 .
2. Paket 1 Fragment 2 und Paket 1 Fragment 1 kommen an. Da diese Fragmente Teil desselben Pakets sind, das Fragment 0 enthält (das die Übersetzung erstellt hat), verwendet NAT den obigen Übersetzungseintrag, um diese Fragmente zu übersetzen und weiterzuleiten. Das Zielgerät empfängt alle Fragmente für Paket 1 und sendet eine Antwort.
3. Paket 2 Fragment 1 erreicht. Da es sich um ein neues Paket handelt, stimmt der IP-ID-Wert nicht mit dem von NAT aufgezeichneten Wert überein. Daher kann NAT die vorhandene Übersetzung nicht verwenden. Es kann auch keine neue Übersetzung erstellen, da es bereits über einen vollständig erweiterten Übersetzungseintrag verfügt und keinen weiteren ICMP-Eintrag erstellt hat. NAT verwirft Paket 2 Fragment 1.
4. Paket 2 fragmentiert 0. NAT kann die obige Übersetzung verwenden, da die ICMP-IDs übereinstimmen. (Für alle Pings innerhalb eines Pings wird dieselbe ICMP-ID-Nummer verwendet.) An diesem Punkt zeichnet NAT die IP-ID dieses Pakets auf. NAT übersetzt und leitet Paket 2 Fragment 0 weiter.
5. Paket 2 fragmentiert 2. NAT kann jetzt die obige Übersetzung verwenden, da der IP-ident-Wert mit der im vorherigen Schritt aufgezeichneten NAT übereinstimmt. NAT übersetzt und leitet Paket 2 Fragment 2 weiter. Das Zielgerät empfängt nur Fragment 0 und 2 (Fragment 1 fehlt), daher sendet es keine Antwort.

Fall 2

Wenn in diesem Szenario zunächst andere Fragmente als das erste Fragment (Fragment 0)

eintreffen, erstellt die NAT eine einfache Übersetzung, sofern sich im NAT-Pool eine Adresse befindet, die noch nicht in einer vollständig erweiterten Übersetzung verwendet wurde.

Beim Start befindet sich nur eine Adresse im NAT-Pool, die NAT-Übersetzungstabelle ist leer, und die Konfiguration wird wie folgt angezeigt:

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

1. Paket 1 Fragment 1 geht ein. NAT kann in der Übersetzungstabelle keine vollständig erweiterte Übersetzung erstellen, da in diesem Fragment keine Informationen zu ICMP-IDs enthalten sind. Da jedoch keine vollständig erweiterten Übersetzungen vorhanden sind, gibt NAT eine einfache Übersetzung ein. NAT übersetzt und leitet anschließend Paket 1 Fragment 1 weiter. Der Übersetzungseintrag erscheint wie folgt:
   ```
   Pro   Inside global     Inside local          Outside local       Outside global
   ---   10.10.10.3        172.16.0.1            ---                 ---
   ```
2. Paket 1 Fragment 0 erreicht. Da die ICMP-ID-Informationen in diesem Fragment enthalten sind, gibt NAT einen vollständig erweiterten Übersetzungseintrag ein:
   ```
   Pro     Inside global         Inside local        Outside local       Outside global
   ---     10.10.10.3            172.16.0.1          ---                 ---
   icmp    10.10.10.3:24321      172.16.0.1:24321    172.17.1.2:24321    172.17.1.2:24321
   ```
   NAT zeichnet dann die IP-ID-Informationen auf und übersetzt und leitet Paket 1 Fragment 0 weiter.
3. Paket 1 Fragment 2 geht ein. Da dieses Fragment dieselben Informationen über die IP-ID enthält wie die in Schritt 2 aufgezeichnete NAT, verwendet NAT die vollständig erweiterte Übersetzung, um Paket 1 Fragment 2 zu übersetzen und weiterzuleiten.Das Zielgerät empfängt alle Fragmente und Antworten. An diesem Punkt sind alle Pings erfolgreich, bis die NAT-Übersetzungstabelle gelöscht wird oder das Programm nach einem Time-Out ausgeführt wird.

Fall 3

Wenn in diesem Szenario zunächst andere Fragmente als das erste Fragment (Fragment 0) eintreffen, erstellt die NAT eine einfache Übersetzung, sofern sich im NAT-Pool eine Adresse befindet, die noch nicht in einer vollständig erweiterten Übersetzung verwendet wurde. Wenn eine erweiterte Übersetzung in der NAT-Tabelle die Adresse bereits verwendet, besteht das Risiko, dass NAT jede der Quelladressen des Fragments in eine andere Adresse übersetzt.

Zu Beginn führt eine Überlastung von mehr als einer Adresse im NAT-Pool durch. Die Übersetzungstabelle verfügt bereits über eine erweiterte Übersetzung, und die Konfiguration lautet:

```
ip nat pool POOL1 10.10.10.3 10.10.10.5 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

Die Übersetzungstabelle wird wie folgt angezeigt:

```
Pro     Inside global         Inside local        Outside local       Outside global
icmp    10.10.10.3:24322      172.16.0.1:24322    172.17.1.2:24322    172.17.1.2:24322
```

1. Paket 1 Fragment 1 geht ein. NAT kann keinen vollständig erweiterten Eintrag für Übersetzungstabellen erstellen, da er nicht über die ICMP-ident-Informationen in diesem Fragment verfügt, und es kann keinen einfachen Übersetzungseintrag für die Adresse 10.10.10.3 erstellen, da für diese IP-Adresse ein erweiterter Eintrag vorhanden ist. NAT wählt die nächste freie IP-Adresse (10.10.10.4) aus und erstellt eine einfache Übersetzung. NAT übersetzt und leitet anschließend Paket 1 Fragment 1 weiter. Die Übersetzungstabelle erscheint nun wie folgt:

```
Pro     Inside global         Inside local       Outside local      Outside global
---     10.10.10.4            172.16.0.1         ---                ---
icmp    10.10.10.3:24322      172.16.0.1:24322   172.17.1.2:24322   172.17.1.2:24322
```

2. Paket 1 Fragment 0 erreicht. Da die ICMP-ID-Informationen in diesem Fragment enthalten sind, gibt NAT einen vollständig erweiterten Übersetzungseintrag für die Adresse 10.10.10.3 ein und zeichnet die IP-ID-Informationen für dieses Paket auf. NAT übersetzt und leitet anschließend Paket 1 Fragment 0 weiter. Die Übersetzungstabelle erscheint nun wie folgt:

```
Pro     Inside global         Inside local       Outside local      Outside global
---     10.10.10.4            172.16.0.1         ---                ---
icmp    10.10.10.3:24322      172.16.0.1:24322   172.17.1.2:24322   172.17.1.2:24322
icmp    10.10.10.3:24323      172.16.0.1:24323   172.17.1.2:24323   172.17.1.2:24323
```

3. Paket 1 Fragment 2 geht ein. Da die IP-Adressinformationen mit der in Schritt 2 gespeicherten NAT übereinstimmen, verwendet NAT die in Schritt 2 erstellte erweiterte Übersetzung, um Paket 1 Fragment 2 zu übersetzen und weiterzuleiten.An diesem Punkt empfängt das Zielgerät alle Fragmente von Paket 1, aber die Quelladresse von Fragment 0 und 2 wurde in 10.10.10.3 übersetzt, und Fragment 1 wurde in 10.10.10.4 übersetzt. Daher kann das Zielgerät das Paket nicht neu zusammenbauen und sendet keine Antwort.
4. Paket 2 fragmentiert 0. NAT verwendet entweder die oben vollständig erweiterte Übersetzung oder erstellt eine neue, vollständig erweiterte Übersetzung, abhängig vom Wert des ICMP-Fragment-Identalfelds. In beiden Fällen zeichnet die NAT die IP-ID-Informationen auf. NAT übersetzt und leitet anschließend Paket 2 Fragment 0 weiter.
5. Paket 2 fragmentiert 2. Die IP-ID-Informationen stimmen mit den in Schritt 4 erfassten NAT-Daten überein. NAT verwendet daher die zweite vollständig erweiterte Übersetzung, die in Schritt 4 erstellt wurde. NAT übersetzt und leitet Paket 2 Fragment 2 weiter.
6. Paket 2 Fragment 1 erreicht. Die IP-ID-Informationen stimmen mit den in Schritt 4 erfassten NAT-Daten überein. NAT verwendet daher die zweite vollständig erweiterte Übersetzung, die in Schritt 4 erstellt wurde. NAT übersetzt und leitet Paket 2 Fragment 1 weiter.Das Zielgerät empfängt alle drei Fragmente von Paket 2 von derselben Quelle (10.10.10.3), sodass es das Paket neu zusammenfügt und antwortet.

Zusammenfassung

Ob NAT ein ICMP-Fragment verwirft oder weiterleitet, hängt von mehreren Faktoren ab, z. B. von der Reihenfolge, in der der NAT-Router die Fragmente empfängt, und vom Zustand der zu diesem Zeitpunkt übersetzten Tabelle. Unter bestimmten Bedingungen übersetzt NAT die Fragmente unterschiedlich, wodurch es dem Zielgerät unmöglich wird, das Paket neu zusammenzubauen.

Zugehörige Informationen

- NAT-Support-Seite

- Support-Seite für IP-Routing
- Technischer Support - Cisco Systems