

Hoe NAT ICMP-fragmenten verwerkt

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Zaak 1](#)

[Zaak 2](#)

[Zaak 3](#)

[Samenvatting](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document legt uit hoe Network Address Translation (NAT) de fragmenten van Internet Control Message Protocol (ICMP) verwerkt wanneer u NAT-overlading configureert. Raadpleeg voor informatie over NAT-overlading de [NAT FAQ](#).

De verwerking van ICMP-fragmenten is afhankelijk van de status van de NAT-vertaaltabel en van de volgorde waarin de NAT-router de ICMP-fragmenten ontvangt. We kijken naar drie verschillende gevallen, waarin we twee pings sturen van 172.16.0.1 naar 172.17.1.2 met een lengte van 3600 bytes elk (drie IP fragmenten).

[Voorwaarden](#)

[Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

[Gebruikte componenten](#)

Dit document is niet beperkt tot specifieke software- en hardware-versies.

[Conventies](#)

Raadpleeg [Cisco Technical Tips Conventions](#) (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

[Zaak 1](#)

In dit scenario zien we dat NAT een volledig uitgebreid vertaaltabel creëert. Zodra dat is gedaan en er geen andere bruikbare adressen in de NAT-pool zijn, laat NAT alle fragmenten vallen die vóór het eerste fragment (fragment 0) van een pakje zijn ontvangen.

Als we beginnen, levert slechts één adres in de pool overbelasting. de NAT-vertaaltabel is leeg; en de NAT-configuratie wordt weergegeven als:

```
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
```

Laten we kijken wat er gebeurt wanneer pakketten bij de NAT router aankomen.

1. Packet 1 fragment 0 arriveert en NAT maakt een volledig uitgebreide vertaalingang. NAT vertaalt en doorstuurt pakket 1 fragment 0. De vertaaltabel verschijnt nu als volgt:

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

Noot het nummer 24320 op in de tabel hierboven. Dit is de ICMP-waarde die in de ICMP-header van het IP-datagram is opgenomen. Alleen fragment 0 van het IP-datagram bevat deze ICMP-header. Om te bepalen of meerdere fragmenten uit hetzelfde pakket bestaan, moet NAT de IP-waarde bijhouden die in de IP-header van alle fragmenten uit het oorspronkelijke IP-datagram is gevonden. Als meerdere fragmenten dezelfde IP-waarde hebben als fragment 0, dat de uitgebreide vertaling creëerde, vertaalt NAT deze fragmenten met dezelfde uitgebreide vertaalopdracht. Raadpleeg [RFC 791](#) voor meer informatie over het IP-identificatieveld. Raadpleeg [RFC 792](#) voor meer informatie over het ICMP-identificatienummer.

2. Packet 1 fragment 2 en pakket 1 fragment 1 arriveren. Aangezien deze fragmenten deel uitmaken van hetzelfde pakket dat fragment 0 bevat (dat de vertaling creëerde), gebruikt NAT de bovenstaande vertaalopdracht om deze fragmenten te vertalen en door te sturen. Het doelapparaat ontvangt alle fragmenten voor pakket 1 en stuurt een antwoord.
3. Packet 2 fragment 1 arriveert. Omdat dit een nieuw pakket is, komt de IP-waarde niet overeen met iets dat door NAT is geregistreerd. Daarom kan NAT de bestaande vertaling niet gebruiken. Het kan ook geen nieuwe vertaling creëren omdat het al een volledig uitgebreide vertaling heeft en het ICMP er niet toe heeft een andere te maken. NAT daalt pakket 2 fragment 1.
4. Packet 2 fragment 0 arriveert. NAT kan de bovenstaande vertaling gebruiken omdat het ICMP-venster overeenkomt. (Alle pings in één enkele reeks pings gebruiken hetzelfde ICMP-incidentnummer.) Op dit punt registreert NAT het IP-incident van dit pakket. NAT vertaalt en doorstuurt pakket 2 fragment 0.
5. Packet 2 fragment 2 arriveert. NAT kan de bovenstaande vertaling nu gebruiken omdat de IP-waarde overeenkomt met die van NAT die in de vorige stap is geregistreerd. NAT vertaalt en doorstuurt pakket 2 fragment. Het doelapparaat ontvangt alleen fragment 0 en 2 (fragment 1 ontbreekt), dus wordt er geen antwoord op verzonden.

[Zaak 2](#)

In dit scenario zien we dat als andere fragmenten dan het eerste fragment (fragment 0) als eerste aankomen, NAT een eenvoudige vertaling creëert zolang er een adres in het NAT-team is dat niet al in een volledig uitgebreide vertaling gebruikt is.

Als we beginnen is er slechts één adres in het NAT-team, is de NAT-vertaaltabel leeg en de configuratie wordt weergegeven als:

```
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. Packet 1 fragment 1 arriveert. NAT kan geen volledig uitgebreide vertaling in de vertaaltabel maken omdat het niet over de informatie van ICMP in dit fragment beschikt. Aangezien er echter geen volledig uitgebreide vertalingen zijn, geeft NAT een eenvoudige vertaling. NAT vertaalt en doorgeeft vervolgens pakketfragment 1. De vertaling verschijnt als volgt:

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.3	172.16.0.1	---	---

2. Packet 1 fragment 0 arriveert. Aangezien de informatie over de ongevallen van het ICMP in dit fragment is opgenomen, voert NAT een volledig uitgebreide vertaling in:

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 registreert vervolgens de IP analyse-informatie en vertaalt en doorstuurt pakket 1 fragment 0.

3. Packet 1 fragment 2 arriveert. Omdat dit fragment dezelfde IP-betrouwbaarheidsinformatie heeft die NAT in stap 2 heeft opgenomen, gebruikt NAT de volledig uitgebreide vertaling om pakket 1 fragment 2 te vertalen en door te sturen. Het doelapparaat ontvangt alle fragmenten en antwoorden. Op dit moment slagen alle pings in totdat de NAT-vertaaltabel is gewist of soms versleten.

Zaak 3

In dit scenario zien we dat als andere fragmenten dan het eerste fragment (fragment 0) als eerste aankomen, NAT een eenvoudige vertaling creëert zolang er een adres in het NAT-team is dat niet al in een volledig uitgebreide vertaling gebruikt is. Als een uitgebreide vertaling in de NAT-tabel al het adres gebruikt, loopt u het risico dat NAT elk van de fragment-bronadressen naar een ander adres vertaalt.

Terwijl we beginnen, wordt er door meer dan één adres in de NAT-pool overbelasting betaald. De vertaaltabel heeft al een uitgebreide vertaling en de configuratie is:

```
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
```

De vertaaltabel is als volgt:

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. Packet 1 fragment 1 arriveert. NAT kan geen volledig uitgebreide vertaaltabel-ingang maken omdat het niet de informatie van het ICMP in dit fragment heeft en het geen eenvoudige vertaalingang voor adres 10.10.10.3 kan maken omdat er een bestaande uitgebreide vermelding voor dit IP-adres is. NAT gebruikt het volgende gratis IP-adres (10.10.10.4) en maakt een eenvoudige vertaling. NAT vertaalt en doorgeeft vervolgens pakje 1. De vertaaltabel verschijnt nu als volgt:

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. Packet 1 fragment 0 arriveert. Aangezien de informatie over de gebeurtenissen van het ICMP in dit fragment is opgenomen, voert NAT een volledig uitgebreide vertaling in voor adres 10.10.10.3 en slaat NAT de informatie over de IP-gebeurtenis op voor dit pakket. NAT vertaalt en doorstuurt pakket 1 fragment 0. De vertaaltabel verschijnt nu als volgt:

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. Packet 1 fragment 2 arriveert. Aangezien zijn IP-betrouwbaarheidsinformatie overeenkomt met de informatie die NAT in stap 2 is opgenomen, gebruikt NAT de volledig uitgebreide vertaling die in stap 2 is gemaakt om pakketfragment 1 te vertalen en door te sturen. Op dit punt ontvangt het doelapparaat alle fragmenten van pakket 1, maar fragment 0 en 2 hebben hun bronadres vertaald naar 10.10.10.3 en fragment 1 is vertaald naar 10.10.10.4. Daarom kan het doelapparaat het pakket niet opnieuw assembleren en geen antwoord versturen.
4. Packet 2 fragment 0 arriveert. NAT gebruikt de bovenstaande volledig uitgebreide vertaling of maakt een nieuwe, volledig uitgebreide vertaling afhankelijk van de waarde van het lettertype van het fragment ICMP. In beide gevallen registreert NAT de IP-incidentinformatie. NAT vertaalt en doorstuurt pakket 2 fragment 0.
5. Packet 2 fragment 2 arriveert. Zijn IP-incidentinformatie komt overeen met wat NAT in stap 4 is opgenomen, zodat NAT de tweede volledig uitgebreide vertaling gebruikt die in stap 4 is gemaakt. NAT vertaalt en doorstuurt pakje 2-fragment.
6. Packet 2 fragment 1 arriveert. Zijn IP-incidentinformatie komt overeen met wat NAT in stap 4 is opgenomen, zodat NAT de tweede volledig uitgebreide vertaling gebruikt die in stap 4 is gemaakt. NAT vertaalt en doorstuurt pakje 2-fragment 1. Het doelapparaat ontvangt alle drie fragmenten van pakket 2 van dezelfde bron (10.10.10.3), zodat het opnieuw samenstelt van het pakket en de antwoorden.

Samenvatting

Of NAT een ICMP-fragment daalt of vooruitstuurt is afhankelijk van een aantal dingen, zoals de volgorde waarin de NAT-router de fragmenten ontvangt en de staat van de vertaaltabel op dat moment. Onder bepaalde omstandigheden vertaalt NAT de fragmenten anders, waardoor het doelapparaat niet meer in staat is het pakje te opnieuw te assembleren.

Gerelateerde informatie

- [NAT-ondersteuningspagina](#)
- [Ondersteuningspagina voor IP-routing](#)
- [Technische ondersteuning - Cisco-systemen](#)