NAT 如何处理 ICMP 分段

目录

简介

本文档说明在配置 NAT 过载时，网络地址转换 (NAT) 如何处理 Internet Control Message Protocol (ICMP) 分段。有关 NAT 过载的信息，请参阅 NAT 常见问题。

ICMP 分段的处理方式取决于 NAT 转换表的状态以及 NAT 路由器接收 ICMP 分段的顺序。我们将查看三种不同的情况，从 172.16.0.1 向 172.17.1.2 发送两个 ping 命令，每个命令长度为 3600 字节（三个 IP 分段）。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

例 1

在此方案中，我们将看到 NAT 在转换表中创建一个完全扩展转换条目。完成后，如果 NAT 池中没有任何其他可用地址，NAT 便会丢弃在数据包第一个分段（分段 0）之前收到的所有分段。

开始时，池中只有一个地址出现过载；NAT 转换表为空；NAT 配置如下：

```
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
```

让我们看看当数据包开始到达 NAT 路由器时会发生何种情况。

1. 数据包 1 分段 0 到达，NAT 创建一个完全扩展转换条目。随后，NAT 转换并转发数据包 1 分段 0。此时转换表如下：`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`请注意上面转换表中的数字 24320。它是 IP 数据报的 ICMP 报头中包括的 ICMP 标识值。只有 IP 数据报的分段 0 包含此 ICMP 报头。要确定多个分段是否属于同一个数据包，NAT 需要跟踪 IP 标识值，该值位于来自原始 IP 数据报的所有分段的 IP 报头中。如果有多个分段与创建扩展转换的分段 0 具有相同的 IP 标识值，NAT 将使用相同的扩展转换条目转换这些分段。有关 IP 标识字段的更多信息，请参阅 RFC 791 。 有关 ICMP 标识字段的更多信息，请参阅 RFC 792 。
2. 数据包 1 分段 2 和数据包 1 分段 1 到达。由于这些分段属于包含（创建转换的）分段 0 的同一个数据包，因此 NAT 使用上述转换条目转换和转发这些分段。目标设备收到数据包 1 的所有分段并发送应答。
3. 数据包 2 分段 1 到达。由于这是新的数据包，其 IP 标识值与 NAT 所记录的任何值均不匹配。因此，NAT 无法使用现有转换。它也不能创建新的转换，因为已有一个完全扩展转换条目，而且没有用于创建另一个条目的 ICMP 标识。NAT 丢弃数据包 2 分段 1。
4. 数据包 2 分段 0 到达。NAT 可以使用上述转换，因为 ICMP 标识匹配。（一组 ping 中的所有 ping 使用同一个 ICMP 标识号。）这时，NAT 记录此数据包的 IP 标识。NAT 转换并转发数据包 2 分段 0。
5. 数据包 2 分段 2 到达。此时 NAT 可以使用上述转换，因为其 IP 标识值与上一步记录的一个 NAT 匹配。NAT 转换并转发数据包 2 分段 2。目标设备仅接收分段 0 和 2（分段 1 丢失），因此不发送应答。

案例 2

在此方案中可以看到，如果第一个分段（分段 0）之外的分段首先到达，NAT 将创建一个简单转换，前提是 NAT 池中有一个尚未用于完全扩展转换的地址。

开始时，NAT 池中只有一个地址，NAT 转换表为空，配置如下：

```
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. 数据包 1 分段 1 到达。NAT 无法在转换表中创建完全扩展转换，因为此分段中没有 ICMP 标识信息。但是，由于没有任何可用的完全扩展转换，NAT 将输入一个简单转换。随后，NAT 转换并转发数据包 1 分段 1。转换条目如下：`Pro  Inside global  Inside local  Outside local  Outside global`
   `---  10.10.10.3  172.16.0.1  ---  ---`
2. 数据包 1 分段 0 到达。由于此分段中包括 ICMP 标识信息，因此 NAT 输入一个完全扩展转换条目：`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`随后，NAT 记录 IP 标识信息，转换并转发数据包 1 分段 0。

3. 数据包 1 分段 2 到达。由于此分段的 IP 标识信息与 NAT 在步骤 2 中记录的相同，因此 NAT 使用完全扩展转换对数据包 1 分段 2 进行转换和转发。目标设备接收所有分段并进行应答。此时所有 ping 执行成功，直到清除 NAT 转换表或超时为止。

案例 3

在此方案中可以看到，如果第一个分段（分段 0）之外的分段首先到达，NAT 将创建一个简单转换，前提是 NAT 池中有一个尚未用于完全扩展转换的地址。如果 NAT 表中的某个扩展转换已使用该地址，则要承担 NAT 将其中每个分段源地址转换为不同地址的风险。

开始时，NAT 池中的多个地址出现过载，转换表已有一个可用的扩展转换，配置为：

```
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
```

转换表如下：

```
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. 数据包 1 分段 1 到达。NAT 无法创建完全扩展转换表条目，因为此分段中没有 ICMP 标识信息，它也无法为地址 10.10.10.3 创建简单转换条目，因为此 IP 地址已有一个扩展条目。NAT 选择下一个可用 IP 地址 (10.10.10.4) 并创建简单转换。随后，NAT 转换并转发数据包 1 分段 1。此时转换表如下：
   ```
   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. 数据包 1 分段 0 到达。由于此分段中包括 ICMP 标识信息，因此 NAT 为地址 10.10.10.3 输入一个完全扩展转换条目，并记录此数据包的 IP 标识信息。随后，NAT 转换并转发数据包 1 分段 0。此时转换表如下：
   ```
   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. 数据包 1 分段 2 到达。由于其 IP 标识信息与 NAT 在步骤 2 中记录的信息匹配，因此 NAT 使用步骤 2 中创建的完全扩展转换对数据包 1 分段 2 进行转换和转发。这时，目标设备接收数据包 1 的所有分段，但是分段 0 和 2 的源地址已转换为 10.10.10.3，分段 1 已转换为 10.10.10.4。因此目标设备无法重组数据包，也不会发送应答。
4. 数据包 2 分段 0 到达。NAT 使用上述完全扩展转换或创建新的完全扩展转换，具体取决于分段 ICMP 标识字段的值。无论采用何种方法，NAT 都会记录 IP 标识信息。随后，NAT 转换并转发数据包 2 分段 0。
5. 数据包 2 分段 2 到达。其 IP 标识信息与 NAT 在步骤 4 中记录的信息匹配，因此 NAT 使用步骤 4 中创建的第二个完全扩展转换对数据包 2 分段 2 进行转换和转发。
6. 数据包 2 分段 1 到达。其 IP 标识信息与 NAT 在步骤 4 中记录的信息匹配，因此 NAT 使用步骤 4 中创建的第二个完全扩展转换对数据包 2 分段 1 进行转换和转发。目标设备接收来自同一个源 (10.10.10.3) 的数据包 2 的全部三个分段，因此得以重组数据包并进行应答。

摘要

NAT 是丢弃还是转发 ICMP 分段取决于多个因素，例如 NAT 路由器接收分段的顺序以及当时转换表的状态。在某些情况下，NAT 会有区别地转换分段，导致目标设备无法重组数据包。

相关信息

- NAT 支持页
- IP 路由支持页
- 技术支持 - Cisco Systems