NAT如何處理ICMP片段

目錄

簡介

本檔案將說明設定NAT過載時，網路位址轉譯(NAT)如何處理網際網路控制訊息通訊協定(ICMP)片段。有關NAT過載的資訊，請參閱NAT常見問題。

ICMP片段的處理取決於NAT轉換表的狀態以及NAT路由器接收ICMP片段的順序。我們將檢視三種不同的情況，其中我們從172.16.0.1到172.17.1.2傳送兩個ping，每個ping的長度為3600位元組（三個IP片段）。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

案例1

在此場景中，我們看到NAT在轉換表中建立一個完全擴展的轉換條目。完成此操作後，如果NAT池中沒有任何其他可用地址，NAT將丟棄資料包第一個片段（片段0）之前接收的任何片段。

開始時，池中只有一個地址執行過載；nat轉換表為空；並且NAT配置顯示為：

```
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
```

讓我們看一看當資料包開始到達NAT路由器時會發生什麼情況。

1. 資料包1分段0到達，NAT建立完全擴展轉換條目。然後，NAT轉換和轉發資料包1片段0。轉換表現在顯示為：
   ```
   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
   ```
   請注意上24320轉換表中的數字。它是IP資料包的ICMP標頭中包含的ICMP標頭值。IP資料包中只有片段0包含此ICMP標頭。要確定多個片段是否為同一資料包的一部分，NAT需要跟蹤在原始IP資料包中所有片段的IP報頭中找到的IP標識值。如果多個片段的IP標識值與片段0相同（該片段建立了擴展轉換），則NAT使用相同的擴展轉換條目轉換這些片段。有關IP標識欄位的詳細資訊，請參閱RFC 791 。如需ICMP識別欄位的詳細資訊，請參閱RFC 792 。
2. 封包1片段2和封包1片段1到達。由於這些片段是包含片段0（其建立了轉換）的同一封包的一部分，因此NAT使用上述轉換專案來轉換和轉送這些片段。目的地裝置接收封包1的所有片段並傳送回覆。
3. 資料包2片段1到達。由於這是一個新資料包，其IP標識值與NAT記錄的任何內容都不匹配。因此，NAT無法使用現有的轉換。它也不能建立新轉換，因為它已經有一個完全擴展的轉換條目，並且它沒有ICMP標識來建立另一個轉換。NAT丟棄資料包2片段1。
4. 資料包2片段0到達。由於ICMP標識匹配，NAT可以使用上述轉換。（一組ping內的所有ping都使用相同的ICMP標識號。）此時，NAT將記錄此資料包的IP標識。NAT轉換和轉發資料包2片段0。
5. 封包2片段2到達。NAT現在可以使用上述轉換，因為其IP標識值與上一步中記錄的一個NAT匹配。NAT轉換和轉發資料包2片段2。目的裝置僅接收片段0和2（缺少片段1），因此不會傳送應答。

案例2

在此案例中，我們看到如果第一個片段（片段0）以外的片段第一個到達，只要NAT池中存在尚未用於完全擴展轉換的地址，NAT就會建立簡單的轉換。

開始時，NAT池中只有一個地址，NAT轉換表為空，配置顯示為：

```
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. 資料包1片段1到達。NAT無法在轉換表中建立完全擴展轉換，因為它在此片段中沒有ICMP標識資訊。但是，由於沒有任何完全擴展的轉換，NAT會進入簡單轉換。然後，NAT轉換和轉發資料包1片段1。轉換條目顯示為：
   ```
   Pro   Inside global     Inside local        Outside local       Outside global
   ---   10.10.10.3        172.16.0.1          ---                 ---
   ```
2. 資料包1片段0到達。由於ICMP標識資訊包含在此片段中，因此NAT輸入完全擴展轉換條目：
   ```
   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
   ```
   然後，NAT記錄IP標識資訊，並轉換和轉發資料包1片段0。

3. 封包1片段2到達。由於此分段的IP標識資訊與NAT在步驟2中記錄的IP標識資訊相同，因此NAT使用完全擴展轉換來轉換和轉發資料包1分段2。目的地裝置接收所有片段和回覆。此時，所有ping操作都會成功，直到NAT轉換表被清除或超時。

案例3

在此案例中，我們看到如果第一個片段（片段0）以外的片段第一個到達，只要NAT池中存在尚未用於完全擴展轉換的地址，NAT就會建立簡單的轉換。如果NAT表中的擴展轉換已使用該地址，則會產生NAT將每個片段源地址轉換為不同地址的風險。

開始時，NAT池中的多個地址會執行過載，轉換表已經有了擴展轉換，配置如下：

```
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
```

轉換表顯示為：

```
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. 資料包1片段1到達。NAT無法建立完全擴展轉換表條目，因為它在此片段中沒有ICMP標識資訊，並且它無法為地址10.10.10.3建立簡單轉換條目，因為此IP地址存在現有的擴展條目。NAT選擇下一個可用IP地址(10.10.10.4)並建立簡單轉換。然後，NAT轉換和轉發資料包1片段1。轉換表現在顯示為：

   ```
   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. 資料包1片段0到達。由於ICMP標識資訊包含在此片段中，因此NAT為地址10.10.10.3輸入完全擴展轉換條目，並記錄此資料包的IP標識資訊。然後，NAT轉換和轉發資料包1片段0。轉換表現在顯示為：

   ```
   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. 封包1片段2到達。由於其IP標識資訊與步驟2中記錄的一個NAT相匹配，NAT使用步驟2中建立的完全擴展轉換來轉換和轉發資料包1片段2。此時，目的地裝置接收封包1的所有片段，但片段0和2的來源位址已轉換為10.10.10.3，片段1已轉換為10.10.10.4。因此，目的地裝置無法重組封包，且不會傳送回覆。
4. 資料包2片段0到達。NAT根據分段ICMP標識欄位的值使用上述完全擴展轉換或建立新的完全擴展轉換。無論哪種情況，NAT都會記錄IP標識資訊。然後，NAT轉換和轉發資料包2片段0。
5. 封包2片段2到達。其IP標識資訊與步驟4中記錄的NAT相匹配，因此NAT使用步驟4中建立的第二個完全擴展轉換。 NAT轉換和轉發資料包2片段2。
6. 資料包2片段1到達。其IP標識資訊與步驟4中記錄的NAT相匹配，因此NAT使用步驟4中建立的第二個完全擴展轉換。 NAT轉換和轉發資料包2片段1。目的地裝置接收來自同一來源(10.10.10.3)的封包2的所有三個片段，因此會重組封包並回覆。

摘要

NAT是捨棄還是轉送ICMP片段取決於許多因素，例如NAT路由器接收片段的順序以及當時轉譯表的狀態。在特定條件下，NAT以不同的方式轉換片段，使得目的裝置無法重組資料包。

相關資訊

- NAT支援頁面
- IP 路由支援頁面
- 技術支援 - Cisco Systems