NAT の ICMP フラグメントの処理方法

内容

概要

このドキュメントでは、ネットワーク アドレス変換（NAT）オーバーロードを設定している場合に NAT によって Internet Control Message Protocol（ICMP）フラグメントが処理される方法について説明します。NAT オーバーロードについては、「NAT FAQ」を参照してください。

ICMP フラグメントの処理方法は、NAT 変換テーブルの状態と、NAT ルータが ICMP フラグメントを受け取った順番によって異なります。ここでは、3 通りの異なるケースについて調べます。その場合も、それぞれ 3600 バイト長のフラグメント（3 つの IP フラグメント）を使って、172.16.0.1 から 172.17.1.2 へ 2 回ずつ ping を送っています。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

ケース 1

このシナリオでは、NAT が変換テーブル内に完全拡張変換エントリを作成する様子を確認します。一旦それが実行されると、NAT プールには他の使用可能なアドレスは存在せず、NAT はパケットの第 1 フラグメント (フラグメント0) より前に受けとったすべてのフラグメントを廃棄します。

開始時点では、プールの 1 つのアドレスのみが過負荷の処理を行います。NAT 変換テーブルは空です。NAT 設定は次のように表示されます。

```
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
```

パケットが NAT のルータに到着し始めたときに、何が起きるのかを確認しましょう。

1. パケット 1 フラグメント 0 が到着すると、NAT は完全拡張変換エントリを作成します。次に、NATはパケット1フラグメント0を変換して転送します。変換テーブルは次のように表示されます。
   ```
   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
   ```
   上記の変換テーブル内の番号 24320 に着目してください。それは、IP データグラムの ICMP ヘッダーに含まれる ICMP ID 値です。IP データグラムのフラグメント 0 だけにこの ICMP ヘッダーが含まれています。複数のフラグメントが同一のパケットに属しているかどうかを判断するため、NAT はオリジナルの IP データグラムのすべてのフラグメントの IP ヘッダー内を検索し、IP ID 値を追跡する必要があります。複数のフラグメントが、既に拡張変換エントリが作成されているフラグメント 0 と同一の IP ID 値を持つ場合は、NATは同じ拡張変換エントリを使ってこれらのフラグメントを変換します。IP識別フィールドの詳細は、RFC 791を参照してください 。ICMP識別フィールドの詳細は 、RFC 792を参照してください。
2. パケット 1 フラグメント 2 とパケット 1 フラグメント 1 が到着します。これらのフラグメントは、フラグメント 0 を含むパケットと同一のパケット (すでに変換が作成されている) に属しているため、NAT は上記の変換エントリを使って、これらのフラグメントを変換して転送します。宛先デバイスは、パケット 1 のすべてのフラグメントを受け取ると、応答を送信します。
3. パケット 2 フラグメント 1 が到着します。これは新しいパケットであるため、IP ID 値は NAT によってこれまでに記録された値と一致しません。そのため、NAT では既存の変換を使用できません。また、それは既に完全拡張変換エントリを持っており、別のエントリを作成するための ICMP ID を持っていないため、新たな変換エントリを作成することもできません。NAT はパケット 2 フラグメント 1 を廃棄します。
4. パケット 2 フラグメント 0 が到着します。ICMP ID が合致するため、NAT は上記の変換エントリを使います。 (ping の 1 つのセットに含まれるすべての ping が同じ ICMP ID 番号を使用) 。 この時点で、NAT はこのパケットの IP ID 値を記録します。NAT はパケット 2 フラグメント 0 を変換し転送します。
5. パケット 2 フラグメント 2 が到着します。今度は、IP ID 値が以前のステップで NAT が記録した値に合致するため、NAT は上記の変換エントリを使用することができます。NATはパケット2フラグメント2を変換して転送します。宛先デバイスはフラグメント0と2 (フラグメント1が見つかりません) のみを受信するため、応答を送信しません。

ケース 2

このシナリオでは、第 1 フラグメント (フラグメント 0) 以外のフラグメントが最初に到着したときに、完全拡張変換でまだ使用されていないアドレスが NAT プール内にある限り、NAT は単純変換を作成することを確認します。

開始時には、NAT プール内にはアドレスが 1 つしか存在せず、NAT 変換テーブルは空で、設定は次のようになっています。

```
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. パケット 1 フラグメント 1 が到着します。それはフラグメント内に ICMP ID 情報を持っていないため、NAT は完全拡張変変換エントリを作成できません。ただし、完全拡張変換はまだ実行されていないため、NAT は単純変換エントリを入力します。次に、NATはパケット1フラグメント1を変換して転送します。変換エントリは次のように表示されます。

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

2. パケット 1 フラグメント 0 が到着します。ICMP ID 情報がこのフラグメントに含まれているため、NAT は完全拡張変換エントリを入力します。

   ```
   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
   ```

   その後、NAT は IP ID 情報を記録し、パケット 1 フラグメント 0 を変換し転送します。
3. パケット 1 フラグメント 2 が到着します。このフラグメントは、NAT がステップ 2 で記録した情報と同じ IP ID 情報を持っているため、NAT は完全拡張変換を使用して、パケット 1 フラグメント 2 を変換し転送します。宛先デバイスは、すべてのフラグメントを受け取り、応答を返します。この時点では、NAT 変換テーブルがクリアされるか、タイムアウトになるまで、すべての ping が成功します。

ケース 3

このシナリオでは、第 1 フラグメント (フラグメント 0) 以外のフラグメントが最初に到着したときに、完全拡張変換でまだ使用されていないアドレスが NAT プール内にある限り、NAT は単純変換を作成することを確認します。NAT テーブル内の拡張変換がすでにアドレスを使用している場合は、各フラグメントの発信元アドレスを別のアドレスへ NAT 変換するという危険を冒すことになります。

開始時に、NAT プール内の複数のアドレスがオーバーロードを実施するため、変換テーブルにはすでに拡張変換が登録されており、設定は次のようになります。

```
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
```

変換テーブルは次のように表示されます。

```
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. パケット 1 フラグメント 1 が到着します。このフラグメントには ICMP ID 情報がないため、NAT は完全拡張変換テーブル エントリを作成できません。また、IP アドレス 10.10.10.3 に対応する既存の拡張エントリが存在するため、この IP アドレスの単純変換エントリは作

成できません。NAT は解放されている次の IP アドレス (10.10.10.4) を使って、単純変換エントリを作成します。次に、NATはパケット1フラグメント1を変換して転送します。変換テーブルは次のように表示されます。

```
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. パケット 1 フラグメント 0 が到着します。このフラグメントには ICMP ID 情報が含まれているため、NAT はアドレス 10.10.10.3 に対応する完全拡張変換エントリを入力し、このパケットの IP ID 情報を記録します。次に、NATはパケット1フラグメント0を変換して転送します。変換テーブルは次のように表示されます。

```
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. パケット 1 フラグメント 2 が到着します。その IP ID 情報は NAT がステップ 2 で記録した情報と合致するため、NAT はステップ 2 で作成した完全拡張変換エントリを使って、パケット 1 フラグメント 2 を変換し転送します。この時点で、宛先デバイスはパケット1のすべてのフラグメントを受信しますが、フラグメント0と2の送信元アドレスは10.10.10.3、フラグメント1は10.10.10.4に変換されています。したがって、宛先デバイスはパケットを再構成できず、応答を送信しません。
4. パケット 2 フラグメント 0 が到着します。NAT は、フラグメントの ICMP ID フィールドの値に応じて、上記の完全拡張変換を使うか、新たな完全拡張変換を作成します。どちらも場合も、NAT は IP ID 情報を記録します。その後、NAT はパケット 2 フラグメント 0 を変換し転送します。
5. パケット 2 フラグメント 2 が到着します。その IP ID 情報は、ステップ 4 で NAT が記録した情報に合致するため、NAT はステップ 4 で作成した 2 番目の完全拡張変換エントリを使用します。NAT はパケット 2 フラグメント 2 を変換し転送します。
6. パケット 2 フラグメント 1 が到着します。その IP ID 情報は、ステップ 4 で NAT が記録した情報に合致するため、NAT はステップ 4 で作成した 2 番目の完全拡張変換エントリを使用します。NAT は、パケット 2 フラグメント 1 を変換し転送します。宛先デバイスは、パケット 2 のこれらのフラグメントをすべて、同一の送信元 (10.10.10.3) から受け取ったため、パケットを再組立てし、応答を返します。

要約

NAT は、NAT ルータがフラグメントを受け取った順番、そのときの変換テーブルの状態など多数の要因に応じて、ICMP フラグメントを廃棄するか転送します。一部の状況では、NAT によるフラグメントの変換が異なるため、宛先デバイスによるパケットの再構成が不可能になります。

関連情報

- NAT に関するサポート ページ
- IP ルーティングに関するサポート ページ
- テクニカルサポート - Cisco Systems