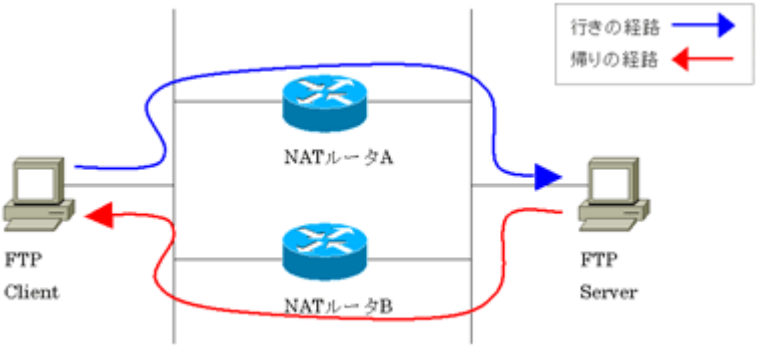
NAT ルータを経由する通信の経路が行きと帰りで異なる場合に FTP 通信が失敗する

2012 年 8 月 更新
2007 年 10 月 初版

目次

概要

このドキュメントでは、NAT ルータが以下のように 2 台存在し、その行きと帰りの FTP 通信の経路が異なる場合（非対称ルーティング、Asymmetric Routing）にその通信が失敗する問題について説明しております。



※ 画像をクリックすると、大きく表示されます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- NAT の基礎知識
- FTP 通信に関する基礎知識
- TCP に関する基礎知識
- ALG（Application Level Gateway）機能に関する基礎知識

また、このドキュメントは、以下の条件、構成のすべてに該当する場合に発生する問題となります。

- 2 台以上の NAT ルータがあり、同一の static NAT エントリを持つ場合の構成
- それぞれの NAT ルータを経由する通信の行きと帰りのパケットの経路が異なる場合（非対称ルーティング）。※なお、dynamic NAT の場合、非対称ルーティングをサポートしませんので、本件は、static NAT における問題となります。
- FTP 通信など、ALG 機能を必要とし、NAT 変換によりパケットサイズが変化する通信の場合

使用するコンポーネント

このドキュメントは、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が、NAT ルータが動作する IOS ルータプロダクトを対象としております。

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。

障害内容

NAT ルータでは、アプリケーションレイヤにおいてのアドレス変換をサポートしております。DNS クエリや FTP、NetBIOS などが典型的な例です。データ部分に埋め込まれた IP アドレス情報が、NAT 変換の対象となる場合、その IP アドレスに対する NAT 変換も実施します（ALG 機能）。

本障害は、2 台の NAT ルータが、非対称ルーティングを利用し、NAT 変換の ALG 機能を利用している際、パケットサイズが変化することが原因で、その FTP 通信が失敗する問題となります。

解説と解決策

解説

本事象は、非対称ルーティングを利用した場合における、NAT 変換の ALG 機能における期待された動作となります。以下に順を追って説明します。

1. まず、FTP におけるアドレスデータは、FTP PORT コマンドに使用されております。
2. PORT コマンドは、対象となるクライアント IP アドレスとポート番号の組み合わせを16進数表記ではなく、ASCII 文字列として表記しています。
   例：クライアントの IP アドレスが 10.1.1.1 で、データ転送用のポートが3090番の場合
   PORT 10,1,1,1,12,18
3. この際、上記 PORT コマンドの IP アドレス表記に必要なバイト数は、8byte（8文字）となります。
4. この IP アドレスに対し、NAT 変換が発生した場合、PORT コマンドも変化します。
   例：10.1.1.1 を192.168.10.1 にNAT変換した場合　PORT 10,1,1,1,12,18 → PORT 192,168,10,1,12,18
5. 上記例では、IP アドレス表記に必要なバイト数が、12byte（12文字）に変わりますので、NAT 変換後の TCP パケットサイズも変化します。
6. ここで問題となるのが、TCP のシーケンス番号です。パケットサイズが変化したことにより、送信元のホストが次に期待する ACK 番号と、実際に対向から送られてくる ACK 番号に不一致が発生します。
7. そこで、Cisco IOS ルータでは、ALG 機能による NAT 変換前の TCP のシーケンス番号、データサイズを把握します。戻りのパケットに対しては、変動したフレームサイズを考慮し、これらの情報の書き換えを実施します。
8. ここで、行きと帰りが異なる NAT ルータを通過する非対称ルーティングの場合には、これらの書き換えができず、ACK 番号の不一致により TCP 通信が失敗します。

解決策

解決策 1

非対称ルーティングを同一の NAT ルータを通るルーティングデザインに変更します。

関連資料

- Cisco Network Address Translation（NAT; ネットワーク アドレス変換）に関する FAQ

テクニカルサポートトップへ