NAT を意識しない個人ネットワークを管理する Home Fire Wall の提案

加藤 尚樹† 渡邊 晃‡
名城大学理工学部† 名城大学理工学部‡

1. はじめに

ADSL をはじめとするブロードバンドの普及に伴い、家庭環境においても複数台の計算機において、高速なインターネット通信を行うことができるようになった。しかし、その反面一般家庭ユーザがハッキングやクラッキング、コンピュータウィルス感染などの危険にさらされる可能性が高くなった。よって、我々は家庭内ネットワークにおいても安全かつ便利に通信を行うために、DHCP による IP の自動割当て、DDNS による動的な名前解決処理および DNS サーバ機能、Personal Fire Wall) 機能など複数の機能を有する Home Fire Wall(以下 HFW)をプライベートネットワークとグローバルネットワーク間に設置することを考えている。

一方、モバイル端末の普及により PC を家庭内のプライベートネットワークからグローバルネットワークへと持ち出した場合においても、プライベートネットワーク内の端末とこれまで通り通信を行いたいというニーズもある。この要求にこたえるため、グローバルネットワーク端末からプライベートネットワーク端末へのアクセスを可能とするパケット転送方式について提案する。

2. NAT

現在の NAT においては、基本的にグローバルネットワークの端末からプライベートネットワークの端末へ通信を開始することはできない。これは、NAT がグローバルネットワーク側から受信されるパケットに関する NAT テーブルを持っていないためである。一方、プライベートネットワークの端末から通信を開始する場合においては通信開始時のパケット情報から NAT テーブルを作成するため、応答のパケットはグローバルネットワーク側からでも NAT は受信し、転送を行うので通信を正しく行うことができる。

この問題を解決するために NAT ではポートフォワード機能というがある。この機能はポート番号ごとに転送先をあらかじめ設定することによって NAT テーブルを静的に作成し、グローバルネットワークから受信したパケットをローカルネットワーク側の端末へと転送することができる(図 1)。しかし、この方式ではひとつのポートに対して 1 台の端末しか設定することができないという課題がある。

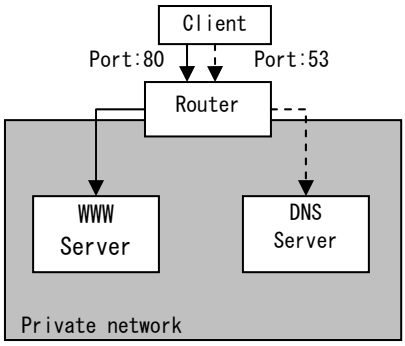

図 1 : NAT のポートフォワード機能

3. 既存技術による解決策と課題

NAT 外部からのアクセスを可能とするための方式として NATS(Network Address Translation with Sub-Address) [1]がある。NATS は NAT の拡張として提案されている技術でプライベートネットワークの各端末のプライベート IP をサブアドレスと呼ばれる識別を DNS レコードとして設定し、それに応じてパケットを転送する機能である。しかし、DNS 問い合わせシーケンスが追加されておりオーバヘッドが大きい。また、IP in IP のカプセル化によるパケットの冗長が発生するという課題がある。

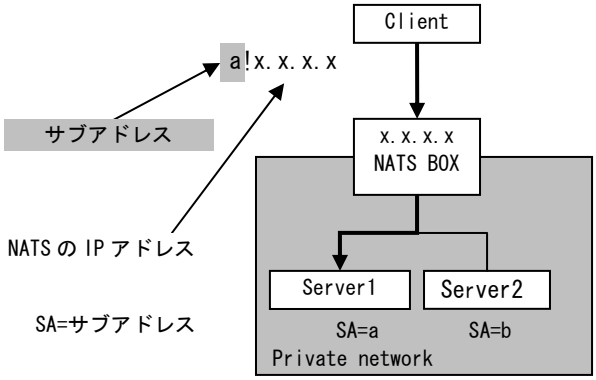

図 2 : NATS の動作

4. 提案方式

本提案方式では HFW が DNS 機能と NAT 機能を有することを前提とする。HFW がクライアントからの DNS 問い合わせを受け付けた時、その内容がプライベートネットワークに対するものであった場合、そのパケット情報及び DNS 情報から NAT テーブルを生成する。又、クライアントはパケット送受信時に送信元ポート番号の変換を行う。

"The proposal of Home Fire Wall which manages the individual network which is not conscious of NAT"
†Naoki Kato MEIJO UNIVERSITY
‡Akira Watanabe MEIJO UNIVERSITY

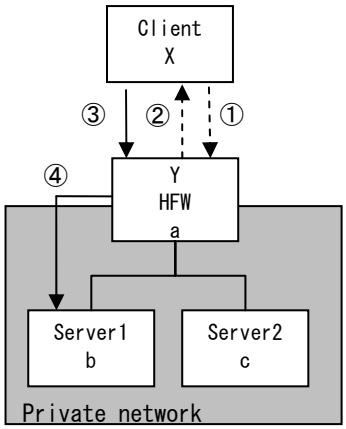

図 3:ネットワーク構成

図３は Client が Server1 と通信を行う場合、最初のパケットが Server1 に到達するまでを表した図である。太字で示したアルファベットは IP アドレスを示す。HFW に関しては『Y』がグローバル IP アドレス、『a』がプライベート IP アドレスであり、Client はグローバル IP アドレスを、Server1, Server2 はプライベート IP アドレスを持つものとする。また、点線で示した矢印①、②は DNS に関するパケット、実線で示した③、④は実際に通信を行うパケットである。図 4 は図 3 における Clinet,HFW,Server1 の通信シーケンス図であり、図中①～④は図 3 の番号と同じパケットを示す。

始めにパケット①による DNS 問い合わせが行われる。このとき HFW では①のパケットの送信情報及び DNS 情報より図 4 に示す NAT テーブルを生成する。また、パケット②では DNS の応答として Server1 の IP アドレスを返すところであるが、Server1 の IP アドレスは、プライベート IP であるため、グローバル IP を持つ HFW の IP アドレス Y を返す。
また、DNS のレコードとして本提案方式であることを示すフラグを定義しておき、これを ON とする。

Client 側では DNS の応答中に含まれる上記フラグが ON であることを確認し、ポート変換テーブルを作成する。データパケット③の送信時にポート変換テーブルに従い送信元ポート番号を p へと変換する。この変換は IP 層以下で行うためアプリケーションには影響を与えない。
データパケット③を HFW が受信すると HFW は最初に作成した NAT テーブルにしたがって③のパケットを④として Server1 へと転送する。

これ以後の HFW の動作は通常の NAT と全く同様である。Client は全パケットに対しポート変換テーブルにしたがってポート番号を変換する。

5. 比較

以下に既存技術と本提案の比較を表としてまとめる。本提案方式と NATS は複数代の端末をグローバルネットワークからアクセスできる利点がある。また、本提案方式においては DNS の特殊性があるもののカプセル化を行わないためパケット長に変化を与えない。

表 1:既存技術との比較

	ポート フォワード	NATS	本提案
複数台で可能であるか	×	○	○
パケットの変化	変化なし	カプセル化による冗長	変化なし
DNS の特殊性	なし	レコード追加	レコード追加

6. まとめ

本稿ではポート番号の書き換えによるグローバルネットワーク端末からプライベートネットワーク端末へのアクセスを可能とする方法について提案した。今後は提案方式を実装し、その有効性を確認する。

7. 参考文献

[1] http://www.nats-project.org

送信元 IP	変換 ポート
X	p

Client で作成されるポート変換テーブル

送信元 IP	送信元 ポート	宛先 IP	宛先 ポート	転送先 IP	転送先 ポート
X	p	Y	-	c	-

HFW で作成される NAT テーブル

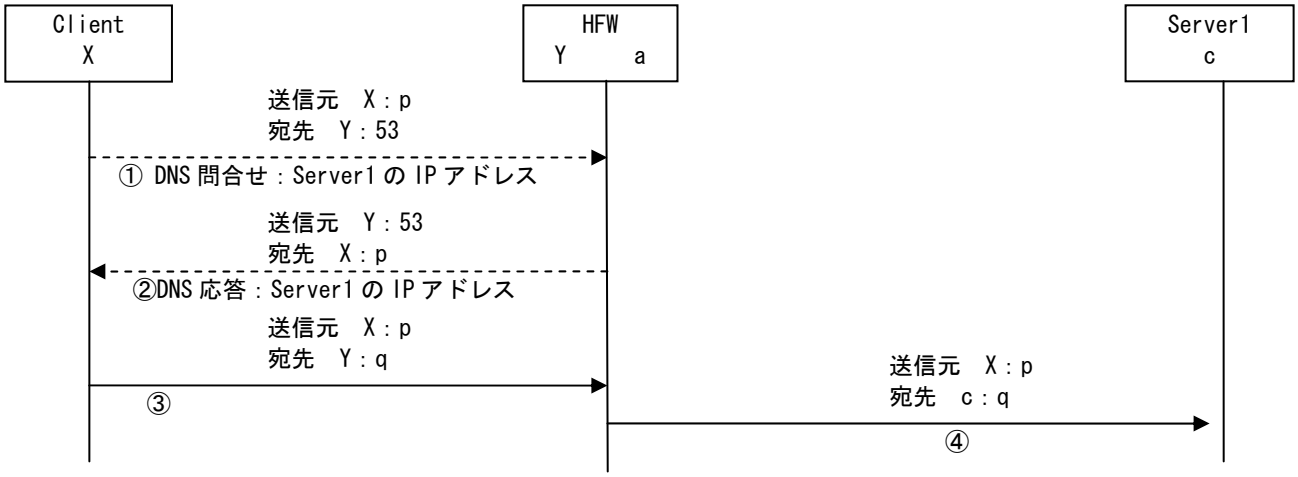

図４：提案方式のシーケンス図