ファイアウォール対応Mobile IPの実現方式について

5C－9

窪田 歩 片岸 一起 浅見 徹
国際電信電話株式会社 研究所

1. はじめに

インターネット/イントラネット環境における携帯型コンピュータの使用に際し, 端末の移動に伴うIPアドレスの変更を不要とするMobile IPの検討がIETFで進められている。当初Mobile IPはファイアウォールの存在を考慮していなかったが, 企業ユーザにとってファイアウォールの存在が当然のこととなっている現在では, IETFにおいてもMobile IPのファイアウォールへの対応について議論されている。本稿ではMobile IPの認証機構を利用したファイアウォールの制御方式について提案し, 他の方式との比較, 検討を行う。

2. Mobile IPのファイアウォールへの対応方式

Mobile IPをファイアウォールへ対応させるための手法としてはSOCKSバージョン5を用いる方法や, SKIPを用いる方法が挙げられている[2]。SOCKSを用いると, 移動端末(以下MH)が移動した際に行うHome Agent(以下HA)への新たな登録の度毎にSOCKSの認証のための4～6回のラウンドトリップが必要であることなどから, IETFではSKIPを用いたIP層でのファイアウォール横断機構を中心に議論している。SKIPを用いた場合, MHが送出するパケットや, HAからMHへ送出されるパケットにMH-FW用もしくはHA-FW用の認証用ヘッダを付加し, SKIP対応のファイアウォールがこの認証ヘッダを基に, ファイアウォールの通過を許可することになる。

3. 既存方式の問題点

現在のドラフトはMHがForeign Agent(以下FA)を利用しない場合のみを対象にしている。SKIPを用いた場合, MHからHAへ出されるRegistration Requestのパケットに, MH-FW間の認証用ヘッダを付加する。MHがFAを利用した場合, MHから出されるRegistration Requestは, まずFAで処理され, 再構成されてFWへ送出されることになるが, ここでFAがMH-FW間認証用ヘッダを生成することができないことが問題となり, 中継パケットがFWを通過できないこととなる。そのため, FAが付加すべき認証用ヘッダをMHがあらかじめ計算しておき, FAがRegistration Requestを中継する際にそれを挿入することも考えられているが, その場合, FAが生成するIPヘッダの識別子フィールドまでMHが用意する必要があるなどの問題点が挙げられている。

4. 提案方式

IP層でのファイアウォール認証機構を用いると前節の問題があるため, 本稿では, Mobile IPにおける認証機構をそのままファイアウォールにおける認証に用いることを提案する。ファイアウォールにおいてMobile IPのRegistrationメッセージを解釈することで, Mobile IP用のファイアウォール制御をより単純化することが可能である。仮にMobile IPで規定されているMH-HA間, FA-HA間の認証結果をそのままファイアウォール通過の許可に用いて良いものとした場合, Registration RequestとRegistration Replyは常にファイアウォールが中継することとし, 登録の成功を通知するRegistration Replyを基に, 以降のMH-HA間のデータ用トラヒックの通過をファイアウォールが許可するだけでよいことになる。MH-FW間の認証が必要な場合には, 登録メッセージの拡張部分を利用するものとする。Mobile IPの認証フィールドの計算にはIPやUDPのヘッダ情報は用いないので, MHが付加した認証フィールドは登録メッセージの中継によって無効化することはない。以下に, 提案方式によるFA利用時の通信手順について述べる。

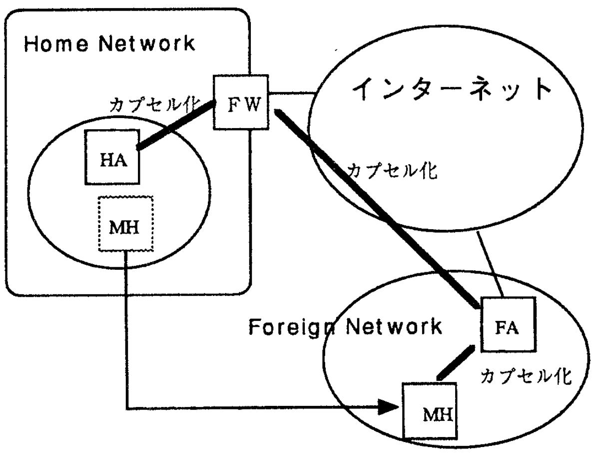

図1: ネットワーク構成

4.1 MHの登録手続き

図1にネットワーク構成を示す。ファイアウォールを構築している場合, 内部ではプライベートアドレスを使用している場合が多く, 外部から直接HAのアドレスを

"Study on A Firewall Traversal Mechanism for Mobile IP Traffic" by Ayumu KUBOTA, Kazuki KATAGISHI and Tohru ASAMI
KDD R & D Laboratories

ポイントすることができない。そのため, Registration Request は FW へ向けて送出する必要がある。このため, MH は利用する FA のアドレスを基に, FW の内にいるか外にいるかを判定し, 外にいる場合には HA のアドレスの代りに FW のアドレスを指定して Registration Request を出すこととする。HA のアドレスは, 登録メッセージ中に FW 用の拡張フィールドを用意し, その中で指定するものとする。また, MH から FW 内部のホストへのパケットは FW 宛てのパケットにカプセル化して送出する必要があるので, MH の Registration Request は[3]で提案されている双方向トンネルを用いた接続を要求するものとする。

Registration Request を受け取った FW は MH-FW 間認証用のフィールドをチェックし, HA へ転送する。HA からの Registration Reply はまず FW に送るものとする。Reply の内容が "accepted" であれば, FW は以降の HA-MH 間のデータ用トラヒックを通すようにフィルタとルーティングテーブルを設定し, 次節で述べる中継を行うものとする。

HA や FA における MH の登録には時間制限が設けられており, MH は登録が失効する前に再度 Registration Request を送出し続けることになっている。これにより FW においても, この手続きによって登録がリフレッシュされない限り, 一定時間後にデータ用トラヒックの中継を無効とするものとする。

4.2 データ用トラヒック

インターネット上にプライベートアドレスを送信先または送信元とするパケットを送出したり, FW 内部に外部アドレスを送信先または送信元とするパケットを送出した場合, それらは廃棄される可能性がある。そのため, HA-MH 間の通信は以下に述べる手順でカプセル化して送受される必要がある。

MH 宛てのパケットに関しては, HA がこれを受取り, まず送信元アドレスを HA, 送信先アドレスを FA とする IP ヘッダを付加する。この段階では送信元アドレスがプライベートアドレス, 送信先が外部アドレスとなっているので, 更に送信先を FW の内部向けのアドレス, 送信元を HA とするヘッダを付加し FW に送出する。FW において最外のヘッダを外し, 今度は送信元アドレスを FW の外部向けのアドレス, 送信先アドレスを FA とするヘッダを付加してインターネットへ送出する。FA はこのパケットを受取ると, 外側のヘッダをはずして, 元のパケットを取り出し, MH に送出する。

逆に, MH から FW の内部ホストへの通信は MH においてまず MH を 送信元, HA を送信先とするヘッダを付加し, FA をデフォルトルータにして送信する。このパケットを受け取った FA は送信元を FA, 送信先を FW の外部向けアドレスとするヘッダを付加し, FW に送信する。FW は最外のヘッダを外し, 元々 MH が HA 宛てにカプセル化したパケットを HA に送出する。HA では外側のヘッダを外して, 最初のパケットを取りだし, 本来の送信先へ転送する。

5. 考察

本提案では, Mobile IP の登録メッセージを用いて FW 通過のための認証も行い, FW においては IPSEC を用いず, フィルタとルーティングの設定のみでパケットの通過を決定させることとした。この場合 FW のフィルタにおいて, カプセル化されたパケットの内側のヘッダも検査することで FA 経由のパケットで MH から HA 宛てでないものを廃棄すれば, FW を通過して HA に達するパケットは MH 発のものだけになる。MH が最初に行うカプセル化の際に, IPSEC を用いて MH-HA 間の認証のためのヘッダを生成し, "don't fragment" をマークして送出すれば, MH-HA 間の IP 層での認証は問題なく行えるため, FA 経由の不正の侵入は防止できる。

本方式の問題として, FW-MH の認証のために Mobile IP の登録メッセージに拡張フィールドを設ける必要があること, FW による中継を意図した登録メッセージの送受が必要であることが挙げられる。ただし, ファイアウォールが多段化した場合等にも登録メッセージへの認証用フィールドの追加で対応することが可能である。

IPSEC を用いる方式の場合, ファイアウォールが多段化し, 更に各ネットワークがプライベートアドレスを使用している場合などを考えると, MH-HA 間の通信には途中経路でのカプセル化が繰り返されることになり, IPSEC を用いた認証用のヘッダを MH が各 FW 用毎にあらかじめ生成することが困難である。そのため, FW における認証に関しては Mobile IP の登録メッセージを利用することが有用であると考えられる。

今後は更に Foreign Network 側にもファイアウォールが構築されている場合についても検討していく必要がある。

6. おわりに

本稿では, Mobile IP の認証機構を利用した Mobile IP のファイアウォール対応化について述べた。最後に日頃ご指導いただいている KDD 研究所村上所長に感謝します。

参考文献

[1] C. Perkins, "IP Mobility Support", RFC 2002, October 1996 .
[2] G. Montenegro, V. Gupta, "Firewall Support for Mobile IP", Internet Draft - work in progress.
[3] G. Montenegro, "Bi-directional Tunneling for Mobile IP", Internet Draft - work in progress.