1T－9

多段ファイアウォール環境に対応したVPN構築方式の通信実装

藤山 達也† 萱島 信† 寺田 真敏† 小泉 稔† 勝俣 修‡
（株）日立製作所 システム開発研究所†
（株）日立製作所 ソフトウェア開発本部‡

1. はじめに

VPN(仮想プライベートネットワーク)は、一対のファイアウォールまたはルータ間で通信データを暗号化することによりネットワークを仮想的な専用線として利用する技術の１つである。

報告者らは、企業や事業部内の各部門でファイアウォールが設置されているような多段ファイアウォール環境下での透過的なアクセスを実現するVPN構築方式として「シームレスVPN」[1]を提案し、その開発を行っている。シームレスVPNは、従来のVPNの持つデータ暗号化機能に加え、(1)ユーザベースアクセス制御機能、および(2)中継経路制御機能を持つ。

本稿では、「シームレスVPN」の実装方式のうち、特にユーザベースアクセス制御機能の実装について報告する。

2. ユーザベースアクセス制御機能の特徴

ユーザベースアクセス制御機能は以下の特徴を持つ。

(1)ユーザ認証操作の軽減

通常、ファイアウォールにおけるユーザ認証は、ユーザとファイアウォールの間で決められた認証方式に従い、ユーザが認証操作を行っている。このため、多段にファイアウォールが組まれた環境では、ユーザはファイアウォール毎に認証操作を繰り返す必要がある。例えば、図１に示す多段ファイアウォール環境において、ユーザ１がB部門のサーバにアクセスするには、本社とB部門のファイアウォールに対して認証操作を行う必要がある。本方式では、シームレスVPNシステムの内部で認証操作を処理することにより、ユーザが行う認証操作のわずらわしさを軽減する。

(2)ユーザ単位のアクセス制御

従来のファイアウォールでは、IPアドレスに基づくアクセス制御、即ち計算機単位のパケットフィルタリング型のアクセス制御を行うものが多い。しかし、現在利用者が増加しつつあるダイアルアップ接続によるアクセスのように、動的にIPアドレスが変わる計算機に対しては、計算機単位のアクセス制御ができない。そこで、本方式では、個々のユーザに対してアクセス可能な範囲や利用できるサービスを設定する機能をファイアウォールに持たせることにより、ユーザ単位のアクセス制御を実現する。

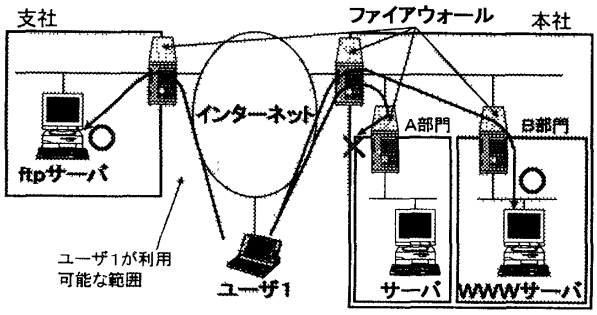

図1：多段ファイアウォール環境

3. 実装方式

3.1 システム構成と機能

シームレスVPNシステムの構成を図２に示す。本システムは、クライアント計算機に実装したセキュリティ機能付きソケットライブラリとファイアウォール上で稼動するゲートウェイプログラムから構成される。以下にそれぞれの機能を示す。

(1)セキュリティ機能付きソケットライブラリ

通常のソケットライブラリの機能に加え、認証処理の機能を持つ。ユーザがクライアントアプリケーションを実行すると、ソケットライブラリは通信経路上のファイアウォールとの認証処理を行う。

(2)ゲートウェイプログラム

ユーザ認証、中継経路選択、アクセス制御からなる

Implementation of VPN construction method for multiple firewall environment
Tatsuya FUJIYAMA†, Makoto KAYASHIMA†,
Masato TERADA†, Minoru KOIZUMI†,
Osamu KATSUMATA‡,
HITACHI, Ltd.

中継制御機能とクライアントーサーバ間の通信データを中継するデータ中継機能を持つ。クライアントがファイアウォールに接続されると、ゲートウェイプログラムはクライアントに対して上記の中継制御を実施した後、ファイアウォールの通過を許可したユーザとサーバの間の通信データのみ中継する。

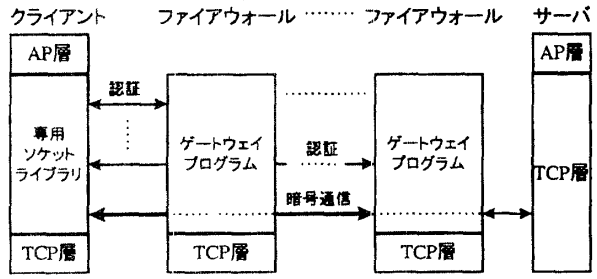

図2：シームレス VPN システム構成

3.2 ユーザベースアクセス制御機能の実装

3.2.1 ユーザ認証

ユーザ認証には ISO/IEC9798-2[2]に規定された共有鍵による相互認証を使用する。そのため、各ファイアウォールには、ユーザ ID とユーザ固有の共有鍵(ユーザ鍵)を作成し登録しておく。また、このユーザ ID とユーザ鍵はユーザにも配布しておく。

多段ファイアウォール環境においては、クライアントは、中継経路上のすべてのファイアウォールとの間で、上記のユーザ登録データを使用してユーザ認証処理を行う。クライアントが目的のサーバと通信するためには、中継経路上のすべてのファイアウォールで認証処理が成功しなければならない(図3)。

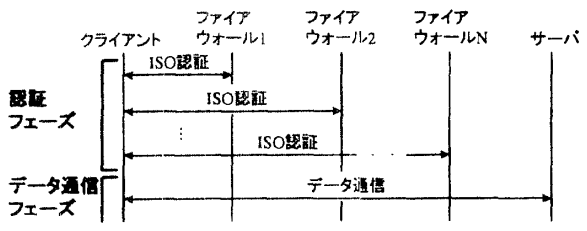

図3：多段認証方式

3.2.2 アクセス制御

3.2.1 のユーザ認証に成功したユーザに対してアクセス制御を行う。ユーザ単位のアクセス制御を実施するために、ユーザ毎に、(1)アクセスを許可するユーザ ID、(2)(1)で指定したユーザに対して、アクセスを許可する接続元アドレスと接続先アドレス、(3)(1)で指定したユーザが利用可能なサービス、を記述したアクセス制御リストを各ファイアウォールに持たせる。ファイアウォールでは、ゲートウェイプログラムがアクセス制御リストを参照してアクセス制御を行うことにより、ファイアウォールで保護されたネットワーク毎にリソースを使用できるユーザを制限する。

図1のシームレス VPN 環境下の各ファイアウォールにおけるアクセス制御リストの設定例を図4に示す。

ユーザID	接続元アドレス	接続先アドレス	利用可能サービス
本社ファイアウォール			
ユーザ1	インターネット	本社ドメイン	すべてのサービス
ユーザ2	インターネット	本社ドメイン	httpサービス
事業所Aファイアウォール			
ユーザ2	本社ドメイン	事業所Bドメイン	httpサービス
事業所Bファイアウォール			
ユーザ1	本社ドメイン	事業所Bドメイン	httpサービス
ユーザ2	本社ドメイン	事業所Bドメイン	telnetサービス
支社ファイアウォール			
ユーザ1	インターネット	支社ドメイン	ftpサービス

図4：アクセス制御リストの設定

図4の設定では、インターネットからアクセスするユーザ1は、本社事業所Bネットワークと支社ネットワークのすべてのサービスを利用できるが、事業所Aネットワークへのアクセスは拒否されることになる。その他のユーザについても同様にきめ細かなアクセス制御を実施することができる。

4. おわりに

本稿では、大規模なイントラネットを想定した多段ファイアウォール環境において、透過的なアクセスを実現するシームレス VPN システムの実装方式について述べた。ユーザはシームレス VPN を利用することにより、ファイアウォール毎の認証処理を意識する必要のない透過的なアクセスが可能となる。また、管理者はインター/イントラネット環境においてユーザ毎のきめ細かなアクセス制御を行うことができる。

参考文献

[1] 萱島他: 多段ファイアウォール環境に対応した VPN 構築方式の提案, 第 54 回全国大会 1T-08, 1996

[2]ISO/IEC9798-2, Information technology - Security techniques - Entity authentication