マルチメディア通信と分散処理　106－20
コンピュータセキュリティ　16－20
（２００２．２．１５）

スター型 End-to-end-VPN を提供する VPN-exchange 方式のスケーラビリティ向上

岡田 浩一　　冨士 仁
koichi@isl.ntt.co.jp　fuji@slab.ntt.co.jp
NTT 情報流通プラットフォーム研究所
〒239-0847 神奈川県横須賀市光の丘 1-1
tel: 0468-59-2133　fax: 0468-59-3365

我々はメッシュ型 End-to-end-VPN における問題点を克服するために、スター型 End-to-end-VPN の利用が有効であると考え、スター型 End-to-end-VPN を実現する「VPN-exchange 方式」を提案してきた。しかし、現状では、この方式はハブ地点においてトラフィック負荷が集中するためスケーラビリティに乏しいという問題がある。本稿ではその解決方法として、認証結果をIPアドレスにマッピングする技術を利用し、認証機能とアクセス制御機能を分離することによりハブ地点の装置を分散設置する方法を導入することを提案する。

Achieving High Scalability in VPN-exchange, a Method of Constructing Star-type End-to-end VPN

Koichi Okada　　Hitoshi Fuji
NTT Information Sharing Platform Laboratories
1-1, Hikarinooka, Yokosuka-shi, Kanagawa 239-0847 Japan
tel: +81-468-59-2133　fax: +81-468-59-3365

In deploying end-to-end VPNs, while mesh-type structure is commonly adopted, our research result reveals that this structure has a number of inherent problems. To address these problems, we have previously proposed a new method of constructing end-to-end VPNs called "VPN-Exchange", which adopts star-type structure. However, our proposal had scalability problems since all traffic tend to concentrate at the point of exchange. In this paper, we aim to address this issue and enhance the scalability of the VPN-Exchange.

1　はじめに

近年、社内セキュリティの向上に有効な手段として End-to-end-VPN が注目されている。しかし、End-to-end-VPN に関して様々な問題点があり(表1)、筆者らは、[1]において、これらの問題点を解決する方法として「VPN-exchange」方式を提案している。これは、従来の end-to-end-VPN が、メッシュ型の構造をとることに対して、スター型(コンセントレータ型)の構造をとり、ハブ地点においてユーザ認証に応じたアクセス制御を行なうことが特徴である。この VPN-exchange 方式には様々なメリットがあるものの、複数の VPN トンネルの集まるハブ地点において負荷が集中するためスケーラビリティの確保が困難であるという問題があった。

本稿では、この VPN-exchange 方式を、ユーザが一つの VPN トンネルを確立するだけで複数の VPN に接続することができるというシングルサインオンを行なうものとして捉え、[2]に示した安全かつスケーラビリティが高いシングルサインオン方式を VPN-exchange の方式に適用し、VPN-exchange 方式におけるスケーラビリティを向上させる方法を提案する。

2　VPN-exchange

本章では、本研究においてスケーラビリティ向上の対象となる VPN-exchange[1]について解説する。

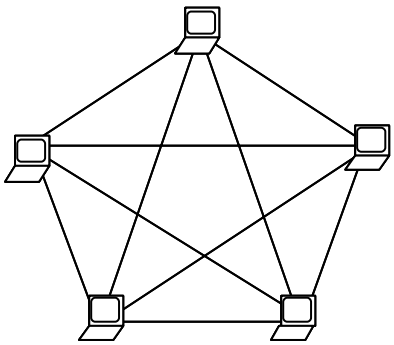

図1 従来のメッシュ型End-to-end-VPNの構成

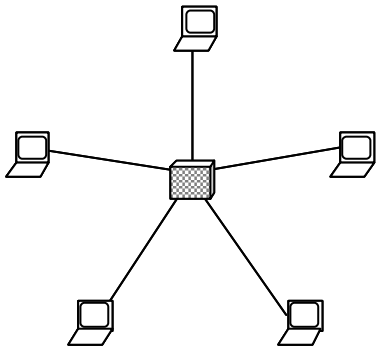

図2 VPN-exchangeによる、
スター型End-to-End-VPNの構成

2.1 VPN-exchange の概要

VPN-exchange 方式は、複数のユーザ間で、End-to-end の VPN を構築する際に、従来の様にメッシュ型の接続形態(図1)をとるのではなく、VPN 中継地点を中心とするスター型(コンセントレータ型)の接続形態(図 2)をとる。送信元および送信先となる各ユーザはそれぞれ一つの VPN トンネルを中継地点との間で確立し、中継地点におけるアクセス制御により、指定した特定ユーザ内に閉じた安全な通信が実現される。

VPN-exchange 方式では、ユーザはただ一つの VPN トンネルを確立するだけで複数の通信先との間の安全な通信路を利用することができる。また、VPN トンネルの確立の際に行なう認証として、装置の認証ではなく、ユーザ認証を行なうことによって、個人単位の VPN を構築する事ができる。この2つの性質を総合すると、VPN-exchange は、複数の VPN トンネルの確立に必要な複数回のユーザ認証を 1 回のユーザ認証だけで済ますことができるというシングルサインオンとしての側面があることになる。

2.2 VPN-exchange のメリット・デメリット

メッシュ型の End-to-end-VPN と比較してスター型の End-to-end-VPN の構造を持つ VPN-exchange のメリッ

表1 従来方式(メッシュ型End-to-end-VPN)と提案方式(VPN-exchange方式)との比較

	メッシュ型End-to-end-VPN		スター型End-to-end-VPN (VPN-exchange方式)	
ポリシー運用	×	・エンド端末間で直接暗号通信を行なう場合、通信内容がポリシーに適合するかどうかの確認を経路上ではできない。	○	・中継地点において、通信パケットが復号されるため、通信内容がポリシーに適合するかどうかの確認が可能。
設定の容易さ	×	・エンド端末では、相手の数分の暗号通信路を設定する必要がある。 ・n台のエンド端末がある場合、o(n^2)の暗号通信路が利用される。	○	・エンド端末は、一つの暗号通信路を設定するだけで複数の相手と安全な通信を確立することができる。 ・n台のエンド端末がある場合でも、全体としてo(n)の暗号通信路が利用されるのみである。
相互接続性	×	・異なる暗号通信方式を利用する複数の相手と暗号通信を行なうためには、エンド端末は、複数の暗号通信方式をサポートする必要がある。	○	・中継地点で、様々な種類の暗号通信方式に対応していれば、エンド端末は複数の方式をサポートすることなく、異なる暗号通信方式を利用する複数の相手と安全な通信が可能となる。
宛先隠蔽	×	・パケットの宛先は暗号化されないため、経路上でパケットを盗聴することにより、通信相手が特定される。	○	・各エンド端末の通信相手は全てVPN中継地点になっているため、経路上でパケットを盗聴されることがあっても、実際の通信相手が特定されることはない。
第3者の非介在	○	・通信する当事者以外には通信内容を確認されることがない。	△	・通信する当事者以外にVPN中継地点の運営者も通信内容を確認する事が可能であるので、VPN中継地点の運営者を信頼する必要がある。
通信遅延	○	・片道の通信の際に、1回の暗号処理だけしか行なわれないので、遅延が比較的小さい。	△	・片道の通信の際に2回の暗号処理と、アクセス制御処理が行なわれるので遅延が比較的大きい。

トおよびデメリットは、表1のとおりである。

2.3 VPN-exchange の課題

VPN-exchange 方式における中継地点では、全エンド端末のトラフィックが集中するため、大規模の運用を行なう際に負荷が高くなることが問題となる。いかにしてこの問題を解決し、スケーラビリティを向上させるかが VPN-exchange 方式の課題である。

2.4 中継地点の要件

前節に示した、スケーラビリティ向上の課題を考慮する際に、中継地点として以下の機能を持つことが要件となる。

(1) VPN トンネル終端機能

クライアント端末と中継地点との間で VPN トンネルを利用する為に、中継装置にはVPNトンネルの終端機能が必要である。

(2) アクセス制御機能

中継地点において、あらかじめ設定しておいたアクセス制御ルールに従い、複数クライアント間の通信パケットを通過させる、あるいは破棄を行なう機能が必要である。このとき、単なるパケットフィルタリングによる IP アドレス単位のアクセス制御だけではなく、ユーザ認証等に基づく正確なアクセス制御を行なうことや、通信を許可されていないユーザからのパケットが利用者の端末に届くことがないようにすること等により、企業向けの IP-VPN[3]サービスと同等の高い安全性を確保する必要がある。

3 アドレスマッピング型シングルサインオン

本章では、2.3 節において示した課題を解決するために導入するアドレスマッピング型シングルサインオン方式[2]について解説する。 この方式は前述した、中継地点としての要件を満たし、かつ、この方式の持つ、スケーラビリティが高いという性質により、VPN-exchange 方式におけるスケーラビリティ向上を行なうことができる。

3.1 アドレスマッピング型シングルサインオン方式の概要

アドレスマッピング型シングルサインオン方式は、図 3 に示すような構成をとる。ユーザは、アドレスマッピング装置に対して認証を受けた後、この装置経由で通信先にアクセスする。アドレスマッピング装置ではパケットの送信元アドレスが、あらかじめユーザ毎に個別に割り当てられた IP アドレスになるようにアドレス変換を行なう。その後、通信先への配送経路上に設置されたパケットフィルタリング装置において、許可されたユーザから送信されたパケットであるかどうかを送信元 IP アドレスにより判別し、そのパケットだけを通過させる。これにより、通信を許可されていないユーザからのパケットが、通信先に到達することを防止する。この方式では、送信元 IP アドレスの偽装が行なわれないことを前提としているため、アドレスマッピング装置とパケットフィルタリング装置の間には、IP アドレス偽装防止対策が施された専用ネットワークを利用する。また、通信元とアドレスマッピング装置および、フィルタリング装置と通信先との間で VPN トンネルを利用することにより、通信元や通信先の所属するネットワーク内におけるアドレス偽装を防止する。

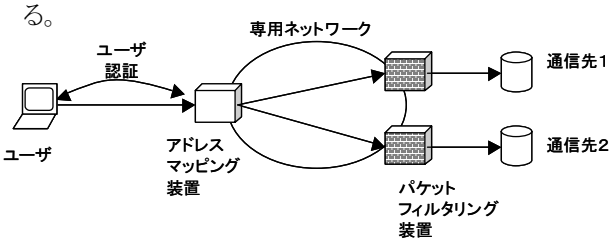

図 3 アドレスマッピング型シングルサインオン

3.2 アドレスマッピング型シングルサインオン方式のメリット

アドレスマッピング型シングルサインオン方式のメリットとしてまず、高い安全性を挙げることができる。その理由としては、アクセスを許可されたユーザから送信されたパケットだけをユーザ認証に基づき識別し、送信先に配送するため不特定ユーザからの不正アクセスを防ぐことができるということと、パケットフィルタリングというネットワーク層の処理だけによってアクセス制御を実現しているためサーバリソース消費型の DoS 攻撃に強いこと、の２つが挙げられる。この性質により、VPN-exchange 方式における、2. 4 節に示した要件を満たすことができる。

また、高いスケーラビリティ持つこともこの方式のメリッ

トの一つである。その理由は、ユーザ認証に基づいたアクセス制御を行なう際に、認証を行なうアドレスマッピング装置と、アクセス制御を行なうパケットフィルタリング装置という2つの装置に機能を分散している点にある。シングルサインオン方式のスケーラビリティ向上において大きな問題となるのは、同一のユーザが多数の通信先にアクセスを行なう際に、シングルサインオン処理装置の設定量および処理量が増大することである。シングルサインオンの定義は、一箇所で行なった認証の情報を複数の通信先において利用することであるので、基本的には、同一のユーザが利用する認証地点を分散させることができない。しかし、アドレスマッピング型シングルサインオン方式では、ユーザ認証を行なう装置と、送信先に応じてアクセス制御を行なう装置を分離しているので、送信先が増えた場合にはアクセス制御装置だけを分散設置すればよい。こうすれば同一のユーザが多数の通信先にアクセスする際にシングルサインオン処理装置の負荷が増大してしまうという問題が回避できる。

また、この方式は、許可されたユーザからのアクセスだけを IP アドレスで識別して通過させるというアクセス制御型のシングルサインオン機能と、アプリケーションにおいて IP アドレスでユーザ識別を行なうシングルサインオン機能の2つを持っている。アプリケーションプログラムでユーザの識別を行なう必要がない場合は、前者の機能だけを利用することができる。その場合は、通信先側で一切のシステム変更が必要ないため導入容易性に優れているというメリットがある。

4　VPN-exchange のスケーラビリティ向上

本章では、前節に述べたアドレスマッピング型シングルサインオンの方式を、VPN-exchange 方式に導入し、スケーラビリティを向上させる方法について述べる。

4.1　アドレスマッピング型シングルサインオン方式の適用

2.1 節で述べたとおり、VPN-exchange には、複数の暗号通信路を確立するために必要な複数回のユーザ認証を、1 回のユーザ認証だけで済ますというシングルサインオンとしての側面がある。これは、アプリケーションでユーザ識別を行なうためのユーザ認証ではなく、通信経路上でのアクセス制御に限定している点で、アクセス制御型のシングルサインオンに相当する。したがって、アドレスマッピング型シングルサインオン方式におけるアクセス制御型シングルサインオン機能のみを利用して、VPN-exchange の中継地点としての機能を実現する。

4.2　アドレスマッピング型シングルサインオン方式を適用した場合の VPN-exchange 方式の構成

アドレスマッピング型シングルサインオン方式におけるアクセス制御型シングルサインオン機能は、アドレスマッピング装置と、パケットフィルタリング装置、およびその間を結ぶ専用ネットワークの3つの構成要素によって実現されている。この３つの構成要素を、VPN-exchange 方式における接続中継地点の機能を実現するために導入する。

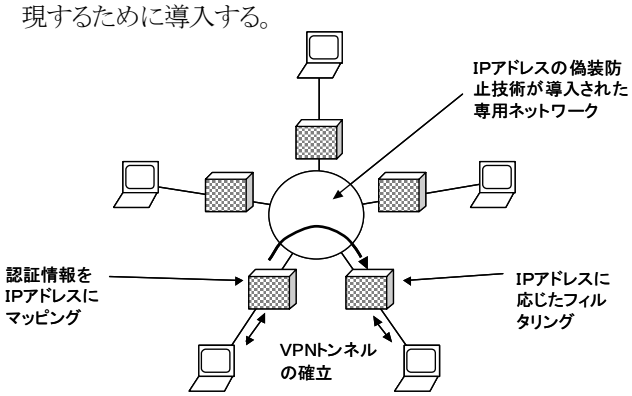

図 4　アドレスマッピング型シングルサインオン方式を導入した VPN-exchange の構成

2.4 節で述べた、VPN-exchange 方式における中継地点として必要な(1)VPN トンネル終端機能は、アドレスマッピング装置およびパケットフィルタリング装置の持つ VPN 終端機能によって提供され、(2)アクセス制御機能は、パケットフィルタリング装置によって提供される。このパケットフィルタリングはユーザ識別可能であるため、2. 4 節に示した正確なアクセス制御が可能である。

専用ネットワークの周囲に設置するゲートウェイ装置として、アドレスマッピング機能と、パケットフィルタリング機能の両方を備えることが必要である。これは、双方向の通信に対応するために、送信元に必要なアドレスマッピング機能と、送信先に必要なパケットフィルタリング機能の両方が、各ユーザが使用する装置として必要

になるためである。

また、専用ネットワークはアドレスを偽装したパケットの侵入を防止する必要があるため、専用ネットワークと外部との境界地点においてイングレスフィルタリング[4]機能を持つ必要がある。この様な対策を導入しているのであれば、専用ネットワークとして、ISP の広域バックボーンネットワーク等を採用することができる。

上記をまとめると、専用ネットワークと外部との境界地点に設置するゲートウェイ装置は、 (1)アドレスマッピング機能、(2)パケットフィルタリング機能、(3)イングレスフィルタリング機能、という3つの機能を持つ必要がある。

このゲートウェイ装置は、ユーザの所属組織毎に個別に用意し、同一組織に所属するユーザは、同一のゲートウェイ装置においてユーザ認証および VPN トンネルの確立を行なう。これは、ゲートウェイ装置は通信ポリシーの運用単位毎に個別に用意し、通信ポリシーは組織毎に個別に運用されるという前提によるものである。

4.3 利用手順

本節では、アドレスマッピング型シングルサインオン方式を導入した VPN-exchange 方式の利用手順を示す(図 5)。

まず事前準備として、次の(1)から(3)に示す設定を行なう。

(1) 送信元および送信先は、ゲートウェイ装置との間で利用する VPN トンネルのための設定を行なう。

(2) ゲートウェイ装置において、その装置との間で VPN トンネルを確立するユーザのための設定を行なう。これには、VPN トンネルの設定と、ユーザ認証のための設定が含まれる。

(3) 送信先側のゲートウェイでは、送信先ユーザが受け入れる通信に関するポリシーを設定する。

(4) 以上の事前設定を終えた後、実際の通信を行なう前に、ユーザはゲートウェイ装置との間で、ユーザ認証を行ない、VPN トンネルを確立する。この操作を VPN-exchange へのログインと呼ぶ。

以上の操作の後、実際に送信元から送信先に通信パケットの配送が行なわれる。その過程は、次の(5)から(9)に分かれる。

(5) まず、送信元は送信先に向けてパケットを送信する。送信元側の暗号通信のための設定により送信先へのパケットは自動的に暗号化されゲートウェイ宛のパケットとしてカプセル化される。その後、パケットはゲートウェイに向けて配送される。ゲートウェイに到着するとパケットはデカプセル化された後、復号される。

(6) ゲートウェイにおいてパケットの送信元アドレスは、予めユーザ毎に設定されたアドレスに変換される(アド

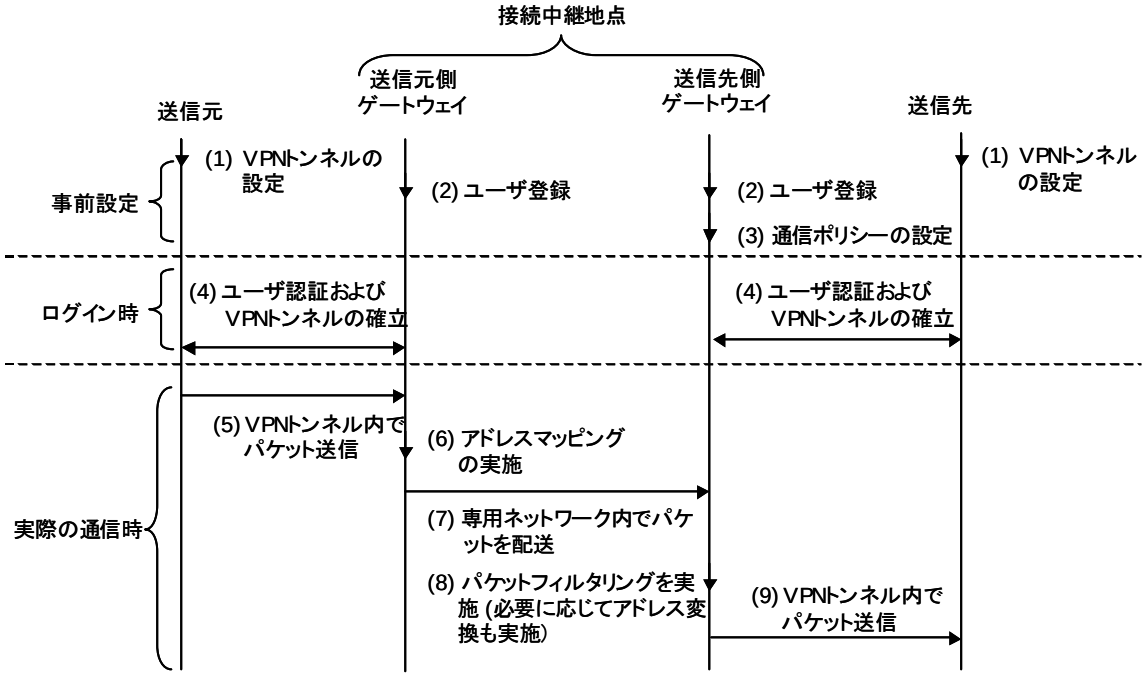

図5 アドレスマッピング型シングルサインオン方式を導入した場合のVPN-exchangeの設定・動作

レスマッピングの実施)。

(7) 送信元側ゲートウェイを出たパケットは、平文のまま、専用ネットワーク内を送信先ゲートウェイに向けて配送される。

(8) 送信先側ゲートウェイにおいて、通信内容が、送信先の所属する組織のポリシーと適合するかどうかの確認が行なわれる。認証情報が送信元アドレスとしてマッピングされているため、IP アドレスに応じたパケットフィルタリングによって、通信が許可されたユーザからのパケットのみを通過させることができる。また、送信先の実際のアドレスが、送信先のアドレスとして公開されたものと異なっている場合はここでアドレス変換処理が行なわれる。

(9) 送信先とゲートウェイの間で確立された VPN トンネルを経由して、パケットは送信先に到着する。このとき暗号化と復号が行なわれる。

4.4 スケーラビリティ比較

本稿で提案したスケーラビリティ向上の方法を導入する前と後とで、装置にかかる負荷を2つの通信モデルにおいて比較する。ここでユーザ数に応じて増加する負荷を表すものとして、装置を通過するパケットの送信元と送信先の組の数を使用する。

まず、ユーザ数を n とし、その間で平均して通信が行なわれるという通信モデルを仮定する。VPN-exchange 方式の中継地点が一つの装置として実現されている場合、その装置にかかる負荷は n 中の 2 者の組合せとなり、

$$ {}_nC_2 = n(n-1)/2 \qquad (1) $$

となるが、本提案方法によってVPN-exchange方式の中継地点をアドレスマッピング型シングルサインオン方式の専用ネットワークとして広域に拡大し、ゲートウェイ装置が m 台に分散されるとき、各装置には、

$$ (n-1)n/m \qquad (m>2) \quad (2) $$

の負荷がかかる。ここで m>2 とあるのは、一つの通信において、アドレスマッピングのために 1 回と、パケットフィルタリングのために 1 回、ゲートウェイ装置としては合計 2 回経由する必要があるためである。装置数 m はユーザ数nに比例して増加すると考えるのは自然であるので、m= kn と表わすと、(2)式は

$$ (n-1)/k \qquad (2') $$

となる。(1)式が n の 2 乗オーダーであることに対して、(2')式は n のオーダーとなり、n の増加に対して大幅に負荷を軽減させたことになる。

次に、別の利用モデルとして、1ユーザあたりの通信先が VPN-exchange の利用者数に無関係に一定の値 p であるとした場合、1つの装置だけの場合は、その装置にかかる負荷は

$$ np/2 \qquad (3) $$

となるが、アドレスマッピング方式を採用し負荷分散を行なうと、

$$ np/m = p/k \qquad (4) $$

となり、1 台当たりの負荷はnの増加に対して一定となる。この利用モデルでも大幅にスケーラビリティが向上することになる。

5 今後の課題

アドレスマッピング型シングルサインオン方式では、ユーザ毎に一意にかつ静的に割り当てられた IP アドレスが必要であり、ユーザ数が増えた場合にはそれに応じて大量の IP アドレスが必要になる。しかし、現在広く使われている IPv4 の IP アドレスは、近い将来、新規割り当てのための IP アドレスが枯渇すると言われている。そのため、IPv6アドレスを利用する方法や、IPv4 におけるプライベートアドレスを利用する方法が考えられるので、その方法を詳細化する。

6 参考文献

[1] 岡田、冨士: 個人単位のVPNを実現するネットワークサービス「VPN-exchange」, 情報処理学会 CSS2001 論文集, pp.67-72, Oct 01.

[2] 岡田、冨士: 安全かつスケーラビリティが高いシングルサインオン方式, 電子情報通信学会 SCIS2002, Jan 02.

[3] B.Glesson et al: "A Framework for IP Based Virtual Private Networks", RFC 2764, Feb 00.

[4] P.Fergunson, D.Senie: "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Address Spoofing", RFC2267, Jan 98.