M-63

VPN-exchangeにおける情報共有方式の提案
Information Sharing System in VPN-exchange

小宮輝之 Teruyuki Komiya　冨士仁 Hitoshi Fuji　岡田浩一 Koichi Okada　石川章史 Akifumi Ishikawa
日本電信電話株式会社 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories

1.はじめに

通信先サイトにおける安全性の保証が困難なエクストラネット通信において、インターネット上の脅威だけでなく、互いのサイト内における盗聴等に対処するためには、End-to-end-VPN を利用することが有効である。我々は、従来の End-to-end-VPN の問題点を克服するものとして VPN-exchange[1]を提案してきた。VPN-exchange では、アドレスマッピング型シングルサインオン[2]機能を用いて高いセキュリティを実現している。本稿では、VPN-exchange における中継地点の高機能化の一つとして、アドレスマッピング型シングルサインオンを利用したエクストラネット向けの情報共有方式を提案する。

2.VPN-exchange

2.1.VPN-exchangeの概要

VPN-exchange は、複数のユーザ間で End-to-end-VPN を構築する際に、従来のようにメッシュ型の接続形態をとるのではなく、VPN 中継地点を中心とするスター型(コンセントレータ型)の接続形態をとる。送信元および宛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間で閉じた安全な通信が実現される。

VPN-exchange 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ユーザ認証を行うことにより、個人単位の VPN を構築する事ができる。この二つの性質を統合すると、VPN-exchange は、複数の通信相手に対して必要な複数回のユーザ認証を、一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.アドレスマッピング型シングルサインオン

VPN-exchange で利用しているアドレスマッピング型シングルサインオンを実現するための構成は、アドレスマッピング機能、パケットフィルタリング機能、イングレスフィルタリング機能を備えたゲートウェイ装置、および、複数のゲートウェイ装置間を結んで中継地点を構成する中継網からなる(図 1)。

ユーザは、ゲートウェイ装置のアドレスマッピング機能によって認証を受けた後、この装置経由で通信相手にアクセスする。ゲートウェイ装置は、アドレスマッピング機能によってパケットの送信元アドレスを、あらかじめユーザ毎に個別に割り当てられた IP アドレスへ変換する。宛先側のゲートウェイ装置では、IP アドレスによってユーザを識別し、パケットフィルタリング機能によって許可された IP アドレスから送信されたパケットだけを通過させる。これにより、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宛先に配送するため、不特定ユーザからの不正アクセスを防止することができる。また、送信元 IP アドレスの偽装が行われないことが必要なため、ゲートウェイ装置は、イングレスフィルタリング機能も備える。

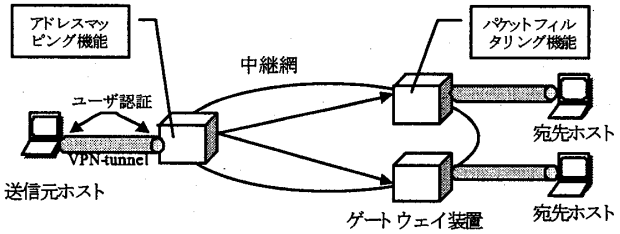

図 1　VPN-exchange の構成

2.3.エクストラネットにおける課題

VPN-exchange においても、End-to-end-VPN を利用した一般のエクストラネット通信と同様に、ユーザが通信グループ内の別のユーザとコミュニケーションを行う際に、下記の二つの課題がある。

(a) 利便性に関する課題

他ユーザへの情報提供や、ユーザ間でのファイル交換などを行うためには、双方とも同時に通信可能な状態であることと、一方が HTTP や FTP 等のサーバ機能を提供することが必要である。しかし、End-to-end-VPN を構築するホストの多くは、主にクライアントとしての用途で利用されているホストであり、必ずしも上記のような条件が満たされているとは限らない。ユーザのホストが、上記のような条件を満たしていなくともユーザ間のコミュニケーションが円滑に行えるようすることが課題である。

(b) セキュリティに関する課題

あるユーザが異なる通信グループへ同時に所属した場合、そのユーザの利用するホストは複数のグループに多重帰属している状態になる。それぞれのグループに所属する別のユーザからの視点では、多重帰属状態にあるホストが、グループ外部(もう一方のグループ)のホストからアクセスが可能になっている状態とみなすことができる。つまり、前記のアドレスマッピング型シングルサインオン方式で挙げた、不正アクセス防止のメリットが損なわれることになる。ユーザのホストが多重帰属状態にあっても、不正アクセスを防止することが課題である

3. Virtual-DMZ

3.1. Virtual-DMZ 方式

本節では、2.3節に挙げた課題を解決する Virtual-DMZ 方式について述べる。本方式は、アドレスマッピング型シングルサインオン方式と同様のゲートウェイ装置と中継網、および、情報共有に必要なサーバ機能を備えて中継地点に接続されたホストを構成要素として実現される。3 つ目の構成要素であるホストは、各ユーザからは自身(内部)と他のホスト(外部)の境界に用意された仮想的な DMZ (De-Militarized Zone)上に設置されたように見える。この中継地点に用意された仮想的な DMZ を Virtual-DMZ(以降、V-DMZ と表記)と呼ぶ。

図 2は、本方式の構成例である。ユーザ *a*～*d* は VPN-exchange のユーザであり、ユーザ *a,b,c* は通信グループ *G1* に、ユーザ *c,d* は通信グループ *G2* に所属しており、ユーザ *c* は二つの通信グループに多重帰属している。V-DMZ *V1* は通信グループ *G1* 用、V-DMZ *V2* は通信グループ *G2* 用にそれぞれ用意されている。

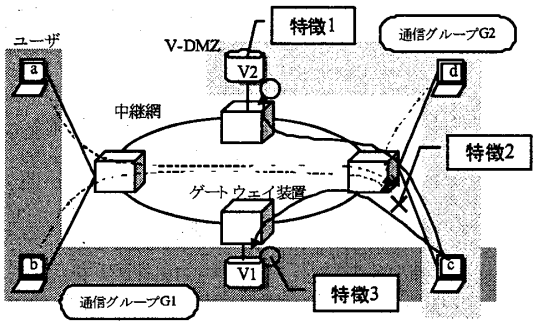

図 2 Virtual-DMZ 方式の構成

3.2. Virtual-DMZ の特徴

[特徴 1] 同時接続を必須としない非同期情報共有

2.3 節の課題(a)は、中継地点に設置された V-DMZ 上のホストが備えるサーバ機能によって解決する。図の例においてユーザ *c* とユーザ *d* の間でデータの公開やファイル交換などを行う際、まず、ユーザ *c* (提供側)が V-DMZ 上のホストへデータをアップロードする。次に、ユーザ *d* (利用側)が V-DMZ 上のホストからデータをダウンロードする。ユーザ間のコミュニケーションは直接行うのではなく、V-DMZ を介して間接的に行う。

[特徴 2] 多重帰属に対応した不正アクセス防止

2.3 節の課題(b)は、ゲートウェイ装置のパケットフィルタリング機能と、通信グループごとに V-DMZ を用意することで解決する。図の例では、ユーザ *c* が二つの通信グループに多重帰属しているが、通信グループ内の他のユーザ *a,b* およびユーザ *d* からユーザ *c* への方向のアクセスをゲートウェイ装置のパケットフィルタリングで禁止する。通信グループ *G1* 用の V-DMZ *V1* はユーザ *a,b,c* から、通信グループ *G2* 用の V-DMZ *V2* はユーザ *c,d* からのみアクセスを許可する。また、各 V-DMZ 上のホストから各ユーザへの方向のアクセスも禁止する。多重帰属状態にあるユーザへのアクセスを禁止することと、一つの V-DMZ へのアクセスは単一の通信グループのユーザのみに限定することにより、不正アクセスを防止する。

[特徴 3] アドレスマッピング型シングルサインオン対応

特徴 2 に示したように、V-DMZ は通信グループごとに用意されるが、アドレスマッピング型シングルサインオンに対応しているため、個々の V-DMZ ごとに認証を行う必要は無い。図の例においてユーザ *c* は、ゲートウェイ装置による一回のユーザ認証により、通信グループ *G1* 用の V-DMZ *V1* と通信グループ *G2* 用の V-DMZ *V2* の双方へのアクセスが可能になる。V-DMZ 上のホストは、ユーザの視点からは常時 VPN-exchange に接続され、サーバ機能を提供し、多重帰属することの無いユーザの一人とみなすことができる。

3.3. セキュリティ面の考察

3.2 節に挙げた特徴 2 について、多重帰属状態にある情報共有サーバに関する不正アクセス防止について、V-DMZ 方式を用いないユーザ間の直接通信と、V-DMZ 方式を用いた間接通信の場合を、次の 4 つの観点で比較する。

A. サーバが所属する全通信グループの外部からの不正アクセス
B. サーバが所属する他の通信グループ内部からの不正アクセス
C. サーバを踏み台とした、他の通信グループへの二次的な不正アクセス
D. サーバを踏み台とした、サーバの設置された LAN への二次的な不正アクセス

表 1 V-DMZ の有無による不正アクセス防止の比較

	V-DMZ 非利用	V-DMZ 利用
A	○: アドレスマッピング型シングルサインオンにより許可されないユーザからのパケットは IP レベルでフィルタリングする。	
B	×: IP レベルでのアクセスが可能であり、DoS 攻撃やセキュリティホールを利用した攻撃の可能性がある。	○: グループごとに V-DMZ を分けるため、他の通信グループからは IP レベルでフィルタリングする。
C	△: 利用形態によってはサーバから別のサーバへのアクセスが許可されている。	○: V-DMZ からの接続要求は禁止される。
D	×: LAN 内部のアクセス制御を適切に行わなければならない。	○: V-DMZ 上に他のホストは設置しない。

上表より、V-DMZ を利用した形態の方が、より不正アクセスに対する安全性が高いと言える。

4. おわりに

本稿では V-DMZ 方式を提案し、VPN-exchange の提供するアドレスマッピング型シングルサインオンを利用した一種のストレージサービスの提供方式を示した。VPN-exchange の中継地点は従来、「通信の中継地点」として位置付けてきたが、V-DMZ 方式により「仮想的な緩衝地帯」としての位置付けが加わることになる。今後、VPN-exchange をプラットフォームとした他のセキュリティサービスを展開していく予定である。

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, 2001.
[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, pp.555-560, 2002.