

パーソナル用途向けインターネット VPN の自動設定方式

Automatic Configuration Method of Internet VPNs for Personal Usage

堀 賢治†
Kenji Hori堀内 浩規†
Hiroki Horiuchi

1. はじめに

会社や外出先から NAT(Network Address Translation)環境の自宅 PCにあるデータを自由に操作, また, 友人とネットワーク対戦ゲームをするなど, ネットワーク環境によらず, 情報共有を可能とするインターネット VPN 技術が注目されている. インターネット VPN(以下, VPNと呼ぶ)はインターネット上で IPSec 等のトンネリングプロトコルを使い, 複数のネットワークを接続して構築される.

従来, 顧客となる組織(カスタマ)に代わって SP(Service Provider)が VPN を構築する, プロバイダ提供型 VPN の検討や標準化がある[1],[2]. しかしながら, プロバイダ提供型 VPN は大規模な企業や複数組織にまたがる通信を想定しており, 通常, 拠点のネットワーク(サイト)間や VPN 間の接続に関する複雑なポリシー(フィルタリングや接続制限)の設定がともなう. このため SP 側の VPN 運用者がカスタマの個別詳細な要求に基づき, ポリシーを含む VPN の構築を行う必要があり, 結果, 相応の導入コストを要している.

一方, 上述のようなパーソナル用途の情報共有などでは, 必ずしも詳細なポリシーの設定が必要でなく, むしろ, 低導入コストで手軽に VPN を構築できることが望まれる.

そこで本稿では, 上述のようなパーソナル用途の情報共有手段を提供することを目的に, 複雑なポリシーを設定することなく, 手軽に VPN を構築できる, パーソナル用途向けインターネット VPN の自動設定方式を新たに提案する.

2. 想定環境と要件

2.1 想定環境

図 1 に, 本稿において想定する物理的なネットワーク構成, および各用語の定義を示す. また以下を仮定する.

- ・ サイトは全て一つのカスタマが所有する.
- ・ 各サイトは ADSL 等によるインターネット接続と, 動的に割当てられたグローバル IP アドレス 1 個を持つ.
- ・ 各 VPN ルータは VPN 管理サーバの IP アドレスまたは DNS 名を予め知っている. 例えば, ADSL において PPP セッションを確立する際に, それらの値を取得する方式が考えられる.

次に, 本稿では個人や中小企業が VPN を構築する場合の条件として, 以下を想定する.

- (1) VPN を導入するためのコストに制約がある.
- (2) カスタマ内に VPN やネットワークの専門知識を持った人材はいない.
- (3) 他のカスタマの VPN とは接続しない.

以上の想定を基, カスタマは全サイトについて重複の無いプライベート IP アドレスを割当て, 低コストで安全に情報共有できる環境の構築を望む.

2.2 VPN 構築方式に求められる要件

2.1 の想定環境において VPN 構築方式に求められる要件は以下のようになる.

- (1) 2.1 の(1)より, 低導入コストであること.
- (2) 2.1 の(2)より, カスタマに専門知識を持つ人材が不要であること.

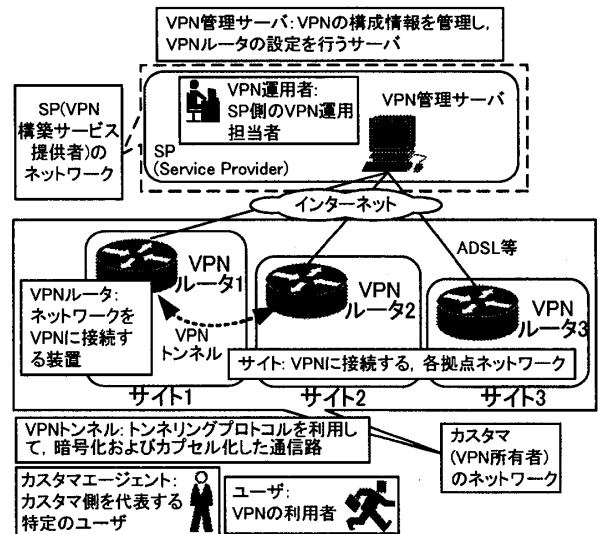


図1 想定するネットワーク構成例および用語定義

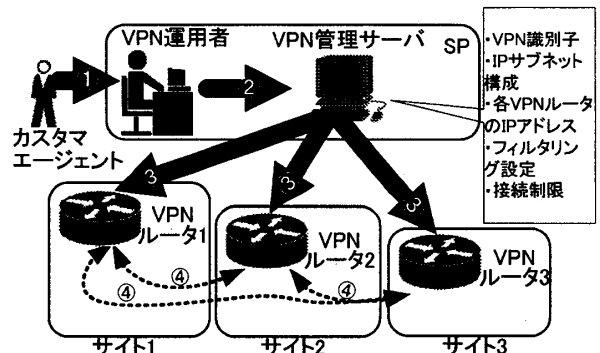


図2 従来のプロバイダ提供型VPNによるVPN構築過程

逆に, 2.1 の(3)により, 以下は要件としない.

- (3) 他のVPNとの接続ポリシーを詳細に設定できること.

2.3 従来のプロバイダ提供型VPN

従来のプロバイダ提供型VPNによってVPNを新設し, カスタマのサイトをVPNに追加していく過程を以下に示す.

まず, カスタマエージェントがVPN運用者に, VPN構成予備情報(図2①)を通知し, VPN運用者はこれを基に, IPサブネット構成や, フィルタ, 接続制限等の接続ポリシーといったVPNの構成を決定し, VPN管理サーバ上に新規登録する(図2②). VPN管理サーバは各VPNルータにIPアドレス等を設定し(図2③), 他のVPNルータに対するVPNトンネル(図2④)を作成させ, VPNの新設が完了する. ここでVPN構成予備情報とは, 会社内の部署構成や拠点配置といった, VPN構成決定のための予備情報である.

このように, 従来のプロバイダ提供型VPNでは, 構築過程でVPN運用者が介入するため, 詳細な接続ポリシー等を設定できる反面, カスタマは相応のVPN導入コストを求められる.

図3に, 2.2で示した(1),(2),(3)の点に関して, 2.1の想定環境で求められる性質(図3①)と, 従来のプロバイダ提供型VPNの性質(図3②)を示す. 図3①の性質に比して, 従来のプロバイダ提供型VPNでは導入コストが高い. その反面, 詳細な接続ポリシー設定が可能という特徴を持つ.

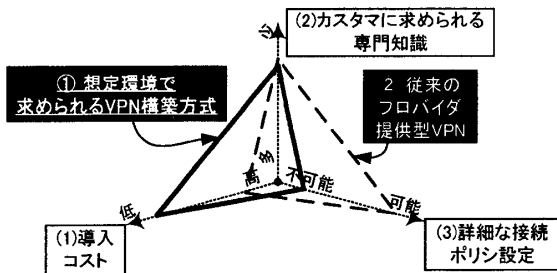


図3 VPN構築方式に求められる性質

3. VPN自動設定方式

本稿で提案するVPN自動設定方式では、従来のプロバイダ提供型VPNと比べて、VPN構築過程にVPN運用者が介在しない点異なる。これによって詳細な接続ポリシー設定等を省く代わりに、導入コストを下げ、図3①の性質を持つ方式とする。

3.1 設計方針

(方針1) VPNおよびVPNルータの構成情報をVPN構成予備情報から自動決定する

VPN管理サーバは、カスタマの通知するVPN構成予備情報に基づき、VPNおよびVPNルータの構成情報を、既定値を基に自動決定する。またVPN構成予備情報はカスタマがVPNルータのVPN管理用web画面から入力し、VPNルータがVPN管理サーバに送信する。これにより、VPN運用者の介在なしにVPNルータを設定する。

(方針2) VPNおよびVPNルータの構成情報を単純化する

VPN管理サーバに登録されるVPNの最低限の構成情報は、①VPN名称(カスタマがVPNに付ける可読な名前)、②VPNに属するVPNルータ、③各サイトで使用するIPサブネットの3点のみとする。更に、VPNルータの構成情報は、①サイト内側のIPアドレス、②他のサイトに対する静的経路、③VPNトンネルの接続先IPアドレス、④VPNトンネリングプロトコルの4点とする。これにより、構成情報の単純化を図る。例えば、サイトによってトンネリングプロトコルの詳細設定が異なる場合等は除いて考え、全てのVPNおよびサイトで構成情報をなるべく共通化する。

(方針3) ユーザは単純かつ僅かな項目のみを指示する

VPNの新設・削除およびVPNに対するVPNルータの追加・削除といったVPNの構成変更操作は、ユーザ自身がVPNルータに対して所定の入力を行うことで開始される。専門知識の無い人物が構成変更操作を行うために、VPNはカスタマにとって分かりやすいVPN名称により識別する。VPN名称をユーザ自ら選択しない場合は、VPNを新設したユーザ名をVPN名称とする。ここで言う分かりやすいVPN名称の例としては、人名や組織名といった、ユーザにとって意味があり、覚えやすく、伝えやすい単語がある。更に、追加・削除対象となるVPNルータに対し「追加・削除」といった操作内容を直接入力するため、ユーザはIPアドレス等、追加・削除対象の特別な識別子を意識する必要がない。従って基本的に、ユーザは「何々というVPN」に対して「追加・削除」する、というように、単純かつ僅かな項目を指示するのみで操作を完了できる。

3.2 VPN自動設定方式の動作概要

上記の設計方針に基づくVPN自動設定方式の動作概要を述べる。図4において、まずVPNを新設し、次いで新設したVPNに各サイトを追加する動作例を示す。

• VPNの新設

- ① ユーザ1はVPNルータ1のVPN管理用web画面を開き、所定のVPN新設操作を行う。この際ユーザが実際に入力するVPN構成予備情報は、新設するVPNの名称(ここではVPN1とする)のみである。

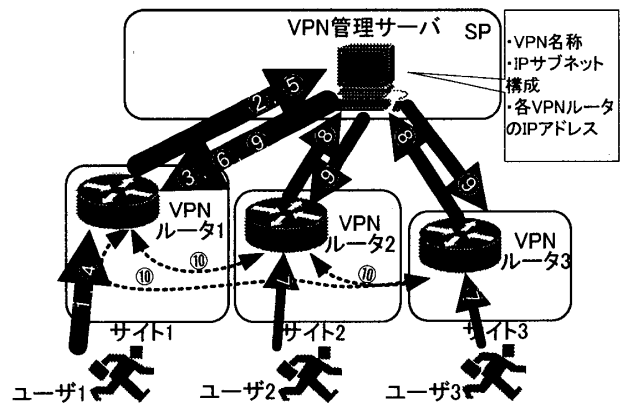


図4 VPN自動設定方式によるVPN構築過程

- ② VPNルータ1が①で入力された情報をVPN管理サーバに送信すると、VPN管理サーバにVPN1が新規登録され、VPN1を所有するカスタマとしてユーザ1が登録される。
- ③ VPN管理サーバはVPN1の管理パスワードをVPNルータ1に送信する。VPNルータ1の管理web画面上に表示される管理パスワードとVPN名称は、ユーザ1と他のユーザ2,3とで、トークンデバイス等によって共有する。
- VPNへのサイト追加
- ④ ユーザ1はVPNルータ1のVPN管理用web画面を開き、所定のサイト追加操作を行う。ここで入力の必要なVPN構成予備情報は①で決定したVPN名称と管理パスワードである。
- ⑤ VPNルータ1は④で入力された情報をVPN管理サーバに送信する。これを契機としてVPN1に属するVPNルータにVPNルータ1のグローバルIPアドレスが追加登録される。さらに、VPN管理サーバはVPNルータ1の構成情報を自動決定する。実際に決定すべき値は、ここではサイト1の使用するIPサブネットだけに単純化される。例えば既定のプライベートIPアドレス範囲より、未使用の10.0.1.0/24を決定する。
- ⑥ VPN管理サーバはVPNルータ1がサイト内で10.0.1.1を使うように設定する。
- ⑦~⑧ サイト2,3についても同様に、ユーザ2,3がサイト追加操作を行うことで、VPN管理サーバはVPN1に属するVPNルータにVPNルータ2,3のグローバルIPアドレスを追加登録し、サイト2,3のIPサブネットを10.0.2.0/24, 10.0.3.0/24と自動決定する。
- ⑨~⑩ VPN管理サーバはVPNルータ2,3に対してIPアドレスを設定すると共に、各VPNルータに、互いのサイトへの静的経路と、VPNトンネルを作成させる。ここでもVPNトンネル作成時にはトンネリングプロトコルだけを指定し、構成情報の単純化を図る。

4. おわりに

本稿では導入コストを抑えつつ、利用者にネットワークの専門知識を要求しない手軽なVPNの構築方式として、パーソナル用途向けのVPN自動設定方式を新たに提案した。今後は提案方式の有効性を、ソフトウェアへの実装を行って評価する。

最後に、日頃ご指導頂く(株)KDDI研究所浅見所長、ならびに長谷川執行役員に感謝する。

参考文献

- [1] R.Calloon et al, "A Framework for Layer 3 Provider Provisioned Virtual Private Networks," IETF Internet Draft, draft-ietf-l3vpn-framework-00.txt, Mar.2003.
- [2] J.D.Clercq et al, "An Architecture for Provider Provisioned CE-based Virtual Private Network using IPSec," IETF Internet Draft, draft-ietf-ppvpn-ce-based-03.txt, Mar.2003.