2007－DSM－44 (13)
2007／3／9

階層型VPNにおける利用者から透過な仮想リンク構成方式の提案

河合 洋明[1] 坂根 栄作[2] 豊田 博俊[3] 岡山 聖彦[4]
山井 成良[4] 石橋 勇人[1] 安倍 広多[1] 松浦 敏雄[1]

[1] 大阪市立大学大学院創造都市研究科
[2] 大阪大学サイバーメディアセンター
[3] 大阪産業大学教養部
[4] 岡山大学総合情報基盤センター

インターネットの発展にともない，インターネットを介して外部から組織ネットワーク内の資源に対して安全にアクセスするための技術であるVPN(Virtual Private Network)の必要性が高まっている．VPNでは，外部から保護するネットワークの範囲をVPNドメインというが，VPNドメインが階層的に構成されたネットワーク環境(階層型VPN)では，通信先に応じて次の階層のVPNゲートウェイ(VGW)を選択する必要がある．そこで本論文では，DNS，ICMP，TCPを用いて利用者に透過な経路制御手法をいくつか提案する．提案する方法では，DNSサーバへの問い合わせや，ICMPメッセージの応答，TCPの応答により次の階層のVGWを自動的に決定する．VTunを拡張することによって提案した方法を実装し，これを用いて提案法の有効性を確認した．

Transparently Establishing Methods of Virtual Links on Hierarchical VPN

Hiroaki Kawai[1] Eisaku Sakane[2] Hirotoshi Toyoda[3] Kiyohiko Okayama[4]
Nariyoshi Yamai[4] Hayato Ishibashi[1] Kota Abe[1] Toshio Matsuura[1]

[1]Graduate School for Creative Cities, Osaka City University
[2]Cybermedia Center, Osaka University
[3]College of General Education, Osaka Sangyo University
[4]Information Technology Center, Okayama University

As the Internet evolves, VPN (Virtual Private Network), which establishes secure connections between off-site clients and on-site servers, is getting important. In VPN, a part of network which is protected from the Internet is called "VPN domain." In the environment where VPN domains are hierarchically configured (Hierarchical VPN), the next hop VPN gateway (VGW) must be discovered depending on the destination host. In this paper, we propose some routing methods which are transparent from users. In these methods, the next hop VGW is automatically discovered by querying to DNS servers and/or receiving ICMP and TCP packets. We have implemented proposed methods by extending the VTun software. The effectiveness of these methods are experimentally confirmed.

1 はじめに

近年，インターネットを介して自組織のネットワークに安全にアクセスするための技術として，仮想プライベートネットワーク (Virtual Private Network，以後VPNとする) が注目されており，活発に研究されている．

VPNの技術によってネットワークの2点間に仮想的なリンクが張られ，これにより安全な通信を実現できる．しかしながら，組織によっては組織内の特定の部署のネットワークをその他の部署に対して非公開とせねばならない場合もあり得る．具体例として大学付属病院を考えれば，病院のネットワークを外部から護るのはもちろんのこと，同じ大学内からの不正アクセスから護るために大学内からのアクセスをも制限することが好ましいと考えられる．学外から付属病院のネットワークにアクセスしようとす

ると，組織の最外殻にあるファイアウォールを超えるだけでなく，学内からのアクセスを制限するためのファイアウォールも超えなければならない．このような異なるセキュリティポリシによって形成される階層構造を持つネットワークは情報管理の観点から必ずしも特殊なものとは言えなくなりつつあるのに対して，そこに仮想リンクを確立するのは容易ではないのが現状である．したがって，上述の階層構造を有するネットワークにおいて，容易に仮想リンクを確立するための手法を考案することは意義深いことである．また，その手法が有用なものとなるには，仮想リンク確立のための一連の手続きは利用者から見れば透過的に実行される必要がある．透過的とは，利用者が組織の階層を意識せずに，また VPN の確立を意識せずに VPN を利用できることである．これを実現するには，通信先に応じた VPN ゲートウェイ (以後，VGW) を自動的に決定する機構が必要となる．

本研究の目的は，既存のアプリケーションに変更を加えずに階層構造を有する組織に対して利用者から透過的に仮想リンクを確立できるシステムを考案し，その有効性を確認することである．ただし，VPN 確立時の認証や，各階層におけるアクセス権の認証などについては先行研究 [3, 4] で行われているので本研究では言及しない．

以下 2 章では透過的に階層型 VPN を確立するために必要な機能について述べる．3 章では階層構造を有する組織に対して利用者にとって透過的で，容易に仮想リンクを確立する方法について述べる．4 章では提案した方法を実装して行った性能評価実験および結果について述べる．5 章で結論と今後の課題について述べる．

2 仮想リンク構成に必要な機能とその実現方法

透過的に階層型 VPN を確立するには，アプリケーションの通信をモニタし，VPN の必要性を自動的に判断する必要がある．ここでは，VPN の必要性を判断するために，(1)DNS クエリを契機とする方法と，(2) エラー応答を契機とする方法を提案する．

2.1 DNS クエリを契機とする方法

この方法は，アプリケーションがサーバの FQDN を指定して通信する際に発生する DNS クエリ (A レコード) をクライアント上で動作させる VPN ソフトウェアが横取りして，VPN の必要性を判断する．

DNS クエリを横取りした後の動作の違いにより 2 通りの方式を提案する．

方式 1 VPN を利用したアクセス対象となるサーバの FQDN の SRV レコードに VGW の情報 (IP アドレスとポート番号) を組織の管理者が設定しておく[*1]．VPN ソフトウェアはこれを問い合わせることで VGW の情報を得て，VPN を確立する．VPN 確立後にサーバの A レコードを VPN ソフトウェアが問い合わせ，最初に横取りした DNS クエリの応答としてアプリケーションに知らせる．

方式 2 VPN ソフトウェアはサーバの FQDN からサーバの IP アドレスを得て，サーバ宛の ICMP エコー要求を送信し，クライアントからサーバまで直接通信できるか調査する．直接通信できない場合は，経路上のルータから ICMP 到達不可メッセージ (ICMP ホスト到達不可，ICMP ネットワーク到達不可など) が返る．組織の管理者は ICMP 到達不可メッセージを応答するルータの IP アドレスに対して (逆引きと同様な方法で) TXT レコードに VGW の情報を設定しておく．VPN ソフトウェアはこれを問い合わせることで VGW の

[*1] 組織内からアクセスする際に VPN を確立しないように，SRV レコードの問い合わせ元により応答を変更するように設定する．

情報を得て，VPN を確立する．VPN 確立後にサーバの A レコードを再度問い合わせ，最初に横取りした DNS クエリの応答としてアプリケーションに知らせる．

2.2 エラー応答を契機とする方法

組織外から組織内のサーバへの通信を許可していない場合などに組織外から通信を試みると，経路上のルータから直接通信できない旨のエラー応答が返ることが期待できる．クライアント上で，通信を監視する VPN ソフトウェアがこのエラー応答を横取りし VPN の必要性を判断する．

エラー応答を横取りした後の動作の違いにより 3 通りの方式を提案する．

方式 3 アプリケーションがサーバ宛の通信を開始し，ICMP 到達不可メッセージが返ると方式 2 と同様な方法で VGW の情報を得る．

方式 4 方式 3 と同様，アプリケーションがサーバ宛の通信を開始し，その応答として返る ICMP 到達不可メッセージを利用するが，方式 3 とは異なり，ルータが送信する ICMP 到達不可メッセージに VGW の情報を付加して応答する．

方式 5 VGW の情報を付加した TCP の非標準の応答[*2]を利用する．

方式 3, 4, 5 では，アプリケーションがサーバ宛の通信を開始してそのエラー応答を契機とするため，契機とする最初のパケットがサーバに届かないという問題がある．この問題を解決するためには，VPN ソフトウェア側でパケットを適宜再送すればよい．ただし，最初のパケットには送信元 IP アドレスとしてクライアントの物理インタフェースの IP アドレスが付与されているが，サーバはクライアントの IP アドレスとして “VPN 確立後の”IP アドレスを期待しているという点に注意する必要がある．このため，VPN ソフトウェアはこれらの 2 つの IP アドレスを相互に変換する必要がある．

2.3 各方式の比較

方式 1，2 は VPN 確立後にサーバの A レコードを問い合わせるため，VPN を確立して通信したいサーバにプライベート IP アドレスを割り当てることができる[*3] が，方式 3，4，5 ではグローバル IP アドレスを割り当てなければならない．

方式 1，2 では，DNS クエリを契機とするため，アプリケーションはサーバの IP アドレスではなく，FQDN を指定して通信しなければならないが，方式 3，4，5 はサーバの IP アドレスを指定して通信する場合でも利用可能である．

方式 2，3，4 では ICMP パケットを利用するため，クライアントとサーバ間の経路上で ICMP パケットがフィルタリングされている場合には利用できないが，方式 1，5 は ICMP パケットがフィルタリングされていても利用可能である．

3 実装

2 章で述べた方式の中から方式 2 と方式 5 を実装した．以下，詳細を述べる．

3.1 方式 2 の詳細

方式 2 の実装は，DNS クエリを横取りする DNS Proxy と，実際の VPN 接続を担当する VTun[6] 改造版 (以下，VTun2 と呼ぶ) からなる．

クライアント上では DNS Proxy がアプリ

[*2] TCP の SYN に対して FIN で応答するなど

[*3] 方式 2 でサーバにプライベート IP アドレスを割り当てるためには以下のようにすればよい．組織外からのサーバに対する A レコードの問い合わせに対して組織に割り当てられたあるグローバル IP アドレスを返すようにし，このアドレスに ICMP エコー要求を送信することで VGW を見つけられるようにする．サーバの実際の IP アドレスは VPN 確立後に取得する．

ケーションの DNS クエリを横取りし，必要に応じて VTun2 クライアントを起動する．また，VGW 上では VTun2 サーバを動作させておく．

以下，クライアント (C1) がサーバ (S1) と通信する場合を例に方式の詳細を述べる (図 1 参照)．

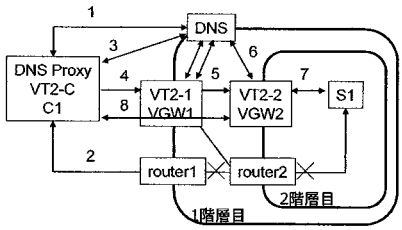

図 1　方式 2 による VPN 確立手順例

1. C1 上のアプリケーションは S1 の IP アドレスを取得するために DNS クエリを送信する．アプリケーションが送信する DNS クエリを DNS Proxy は横取りし，A レコードを問い合わせ，S1 の IP アドレスを受け取る．
2. DNS Proxy は S1 宛の ICMP エコー要求を送信し，S1 までの経路上のルータ (router1) から ICMP 到達不可メッセージを受信する．
3. DNS Proxy は ICMP 到達不可メッセージの送信元である router1 の IP アドレスの TXT レコードを DNS サーバに問い合わせ，VGW_1 の情報を受け取る．
4. DNS Proxy は C1 上で VTun2 を起動し (以下 VT2–C)，S1 の FQDN を VT2–C に渡す．VT2-C は S1 の FQDN を VGW_1 上の VTun2(以下 VT2–1) に渡して，VT2–1 に VPN 接続要求を行い，VT2–1 からの応答を待つ．
5. VT2–1 は VT2–C から受け取った S1 の FQDN を DNS サーバに問い合わせて S1 の IP アドレスを取得する．2 から 4 までの DNS Proxy，VT2–C と同様の動作を行い，VT2–1 は VGW_2 上の VTun2(以下 VT2–2) に S1 の FQDN を渡して VPN 接続要求を行い，VT2–2 からの応答を待つ．以後 VT2–1 は VT2–C と VT2–2 の通信を中継する．
6. VPN 接続要求を受けた VT2–2 は VT2–1 から渡された S1 の FQDN を DNS サーバに問い合わせ，S1 の IP アドレスを取得する．
7. VT2–2 は S1 宛の ICMP エコー要求を送信し，S1 から ICMP エコー応答を受け取る．
8. ICMP エコー応答を受け取った VT2–2 は VGW_1 からの VPN 接続要求に応答し，VPN を確立する．VPN 確立後，VT2–2 は 6 で取得した S1 の IP アドレスを DNS Proxy に転送し，DNS Proxy は，横取りした DNS クエリの応答としてこの IP アドレスをアプリケーションへ返す．

3.2　方式 5

方式 5 の実装は，クライアントの通信を監視する VPN Agent と，実際の VPN 接続を担当する VTun 改造版 (以下，VTun5 と呼ぶ) と，エラー応答に VGW の情報を付加する TCP FIN Responder(以下，TFR と呼ぶ) からなる．

VPN Agent はクライアントの通信を監視し，必要に応じて VTun5 クライアントを起動する．また，組織のルータでは TFR を，VGW では VTun5 サーバを動作させておく．

C1 が S1 と TCP で通信する場合を例に方式の詳細を述べる (図 2 参照)．

1. C1 上のアプリケーションは S1 と TCP を用いて通信するために S1 宛の SYN パケットを送信する．VPN Agent はこの SYN パケットを記録しておく．ルータ (router1) 上で動作している TFR は S1

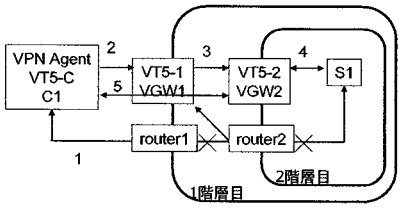

図2　方式5によるVPN確立手順例

宛のSYNパケットに対してVGW_1の情報を付加したFINパケットで応答する．VPN Agentは経路上のルータからVGW_1の情報が付加されているFINパケットを受信する．

2. VPN Agentは C1上でVTun5を起動し(以下VT5–C)，SYNパケットをVT5–Cに渡す．VT5–CはSYNパケットをVGW_1上のVTun5(以下VT5–1)に渡して，VT5–1にVPN接続要求を行い，VT5–1からの応答を待つ．
3. VT5–1はVPN接続要求を受けると，VPN用に確保しているIPアドレスの中から1つを取り出してクライアント用に予約し(以下，IP_1と呼ぶ)，FreeBSDのdivert機能を利用してIP_1を宛先とするパケットを受信できるようにIPFWの設定を変更する．VT5–1はVT5–Cから受け取ったSYNパケットの送信元IPアドレスをIP_1に書き換えてS1に送信し，1と2のVPN Agent，VT5–Cと同様の動作を行い，IP_1を確保しているIPアドレスの中に戻し，VT5–1はVGW_2上のVTun5(以下VT5–2)にVPN接続要求を行い，VT5–2からの応答を待つ．以後VT5–1はVT5–CとVT5–2の通信を中継する．
4. VT5–2はVPN接続要求を受けると，VPN用に確保しているIPアドレスの中から1つを取り出してクライアント用に予約し(以下，IP_2と呼ぶ)，divert機能を利用してIP_2を宛先とするパケットを受信できるようにIPFWの設定を変更する．VT5–2はVT5–1から受け取ったSYNパケットの送信元IPアドレスをIP_2に書き換えてS1に送信し，S1からSYN+ACKパケットを受け取る．
5. VT5–2はVT5–1からのVPN接続要求に応答し，VPNを確立する．VT5–2はVPN用のアドレスとしてIP_2をC1に割り当て，以後C1の物理インタフェースのIPアドレスとIP_2を相互にアドレス変換する．
6. VPN確立後，VT5–2はS1から受け取ったSYN+ACKパケットをVPNを利用してC1に送信し，C1は，ACKパケットをVPNを利用してS1に送信し，TCPコネクションを確立する．

4　評価

実験環境として図3のようなネットワークを構築した．それぞれの計算機は100BASE-TXにより接続されている．なお，各計算機のCPUはPentium M 2.00GHz，メモリは1GB，OSはFreeBSD6.1-RELEASEである．

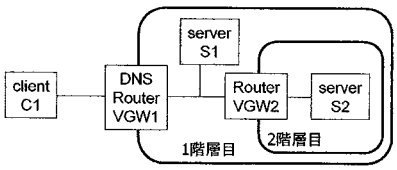

図3　実験環境

この実験環境において方式2，方式5の動作実験を行い，利用者に組織の階層を意識させることなくVPNを利用することができることを確認した．

また，C1がS1と通信するためにVGW1とVPNを確立する場合と，C1がS2と通信する

ために VGW2 と VPN を確立する場合のそれぞれで仮想リンクの確立に要する時間を 10 回計測し，平均値を算出した (表 1).

	平均 (ミリ秒)	
	1 階層	2 階層
方式 2	115	117
方式 5	133	147

表 1　VPN 確立時間

方式 2，方式 5 を実装して実験した結果，利用者に組織の階層を意識させることなく VPN を利用することができることを確認した．また，VPN 確立までにかかる時間は約 0.1 秒であり，実用上問題ないと考えられる．

VPN 確立に要するステップの少ない方式 5 が方式 2 より VPN 確立に時間がかかったのは方式 5 の動作手順の 3，4 で行う IPFW の設定変更に時間がかかっているためであると考えられる．

表 1 の結果より，1 階層を辿るのにかかる時間は方式 2 では 2 ミリ秒，方式 5 では 14 ミリ秒である．組織の規模によっては多数の階層を辿ることもあり得るが，この程度の時間ならば許容範囲であると考える．

5　おわりに

本論文では，企業や大学などの大規模で階層構造を有する組織に対して利用者から透過的に仮想リンクを確立できるシステムを提案し，実装した．さらに動作実験を行い提案法が実用上問題ないことを確認した．

今後の課題としては，提案した方式はそれぞれ使用するための制限があるので，どのような条件下でも使用できるように提案した方法を混在させて，クライアントの環境によってどの方式を利用するかを自動的に決定するような方法の考案があげられる．

参考文献

[1] 岡山聖彦, 山井成良, 石橋勇人, 安倍広多, 松浦敏雄; 代理ゲートウェイを用いた SOCKS ベースの階層的 VPN 構成法. 情報処理学会論文誌, Vol.42, No.12, pp.2860–2868, December 2001.

[2] 岡山聖彦, 山井成良, 金出地友治, 石橋勇人, 安倍広多, 松浦敏雄; 階層型 VPN のための LDAP サーバを用いた経路制御手法. 情報処理学会論文誌, Vol.45, No.1, pp.46–55, January 2004.

[3] 福井健太, 岡山聖彦, 山井成良, 石橋勇人, 松浦敏雄; 階層型 VPN における効率的なアクセスポリシ管理手法. 情報処理学会論文誌, Vol.47, No.4. pp.1136–1145, June 2006.

[4] 大西宇泰, 岡山聖彦, 山井成良, 石橋勇人, 松浦敏雄; 階層型 VPN における証明書を利用したアクセス制御手法. 情報処理学会研究報告 2004-DSM-34, Vol.2004, No.77. pp.25–30, July 2004.

[5] 萱嶋信, 寺田真敏, 藤山達也, 小泉稔, 加藤恵理; 多重ファイアウォール環境に適した VPN 構築方式の提案. 電子情報通信学会論文誌 D-I Vol. J82-D-I No.6 pp.772–778, June 1999.

[6] Virtual Tunnels over TCP/IP networks. http://vtun.sourceforge.net/ February 2007.

[7] 河合洋明; 階層型 VPN における利用者から透過な仮想リンク構成方式とその実装. 大阪市立大学大学院創造都市研究科修士学位論文, January 2007.