L_001

柔軟な割り当て可能な超高性能VPNシステム開発のための性能測定実験
Performance measurement experiments for a development of a high-performance and flexible network resource allocable VPN system

佐藤　聡† 中井　央†
山口喜教† 板野肯三†
Akira SATO,† Hisashi NAKAI,† Yoshinori YAMAGUCHI and Kouzo ITANO†

1. はじめに

現在、学内のネットワーク資源を学外から安全に利用するための方法として、ダイアルアップ接続を用いる方法が一般的である。近年のブロードバンド環境の整備が進むにつれて、学外から学内へのネットワーク資源への通信路の広帯域化の要望が高まってきている。このように、ファイアウォール外部から内部のネットワーク資源への安全な通信路の広帯域化手法としてVPN(Virtual Private Network)システムが有効である。その中でも、ソフトウェア型VPNシステムは、通常のPCにインストールして実行させるため、低コストで導入ができ、かつ、利用するPCの台数を増やすことにより規模を大きくできるため、スケーラビリティにも優れており、非常に有効な解決策のひとつになっている。

そこで、本研究では、学外から学内のネットワーク資源への通信路を広帯域かつ安全に実現可能なソフトウェア型VPNシステムについて、いくつかの異なるハードウェア環境上でのソフトウェア毎の性能、機能の違いについて比較調査することを目的とする。

2. 測定実験

2.1 実験の目的

本実験は、速度測定の対象とする各VPNソフトウェアが動作するVPNサーバーと、複数台のVPNクライアントとして動作するPC群とをVPN接続し、対となるVPNクライアント間で最大限にトラフィックを流したときの通信スループットを測定し、VPNサーバーの構成の違い、およびクライアント数の違いによる通信スループットの違いを比較することにある。ここで、「通信スループット」とは、VPNに対して、測定時間内に入力されたデータ量と出力されたデータ量の合計値を、測定時間で割った値と定義する。

2.2 調査対象となる環境

汎用のPC上で動作可能なVPNソフトウェアを調査対象とした。**表1**に調査対象のVPNソフトウェアシステムを、**表2**に調査対象ハードウェアを示す。また、調査対象間を接続するネットワークスイッチとしては、1000Base-Tを24ポート,10GbE XFPを2ポート搭載しているNortelNetworks社製Nortel Routing Switch 5530-24TFDをスタック接続したものを利用する。

VPNサーバーとなる計算機ついては64bitマシンと32bitマシンの双方を用いた。オペレーティングシステム(以下、OSと略す)として、Windows Server 2003 32bit版(以下、Windows 32bit版と略す)と64bit版(以下、Windows 64bit版と略す)、およびLinux (Fedora Core5)とした。32bitマシンでは、Windows 32bit版およびLinuxを用いた。また、64bitマシンでは、Windows 32bit版とWindows 64bit版を用いた。今回調査対象としたVPNソフトウェアのすべてはWindows 32bit版に対応している。Windows 64bit版については、OpenVPNが対応していないため、残りの2種のVPNソフトウェアを対象とした。また、Linuxについては、MS-PPTPが対応していないため、残り2種のVPNソフトウェアを対象とした。なお、OpenVPNについて、その性能が最大限に発揮されるようにUDPモードを用いた。

表1 調査対象としたソフトウェア

システム名	バージョン	開発元
PacketiX VPN 2.0	2.10.5080	ソフトイーサ株式会社
OpenVPN 2.0	2.0.7	OpenVPN Solutions LLC
MS-PPTP	5.2.3790	Microsoft Corporation

また、VPNクライアントとなる計算機には32bitマシンのみを用い、OSはWindows 32bit版を用いた。

2.3 通信スループットの最大性能の測定方法

本実験の環境は実環境を想定している。実環境の通信によって流されるパケットのうちトラフィックの大半を占めるのはユニキャストパケットである。したがって、本実験ではVPNシステム内に流すパケットとしてはユニキャストパケットを対象とした。

また、本実験の目的は、VPNシステムの性能評価である。従って、相互に通信を行う複数組のコンピュータ間にて同じ瞬間に最大限のトラフィックを発生している場合という一番最悪の環境下において、どの程度の帯域が確保されるかということを測定することにした。我々は、複数台のコンピュータ間で同期を取り、同じ瞬間にトラフィックを流し始め、その通信量の集計をし、通信スループットを計算する測定ツール「TrafficSpeed」を作成した。

TrafficSpeedツールは、測定クライアントと測定サーバーの2台のコンピュータ上で起動し、測定サーバーがTCPポートを待ち受け、測定クライアントが測定サーバーのTCPポートにTCPコネクションを複数本張り、その後各TCPコネクションで乱数として定義されているデータの送受信を行う。これにより、TCPウインドウサイズやRTTによる測定結果の影響を排除し、回線のより正確な最大スループット性能を測定することが可能となる。今回の実験では、32本のTCPコネクションを張る。データの送受信の時間は60秒間とし、時間経過後はデータの送受信を終了した。

今回の測定では、VPNを経由して接続している1対のコン

† 筑波大学 学術情報メディアセンター
Academic Computing & Communications Center, Universcity of Tsukuba

表 2　調査対象計算機

項目	64bit マシン	32bit マシン
CPU	Dual Core AMD Opteron Processor 270 (2.0GHz) × 4	Intel Xeon 3.2GHz × 2
MM	4 GB DDR SDRAM	2 GB DDR SDRAM
HDD	250 GB SATA 7200rpm × 2 (RAID-1)	146.8 GB SCSI 10000rpm × 3 (RAID-5)
チップセット	NVIDIA nForce4 Professional 2200 / 2050	ServerWorks GC-LE
NIC	Intel PRO/10GbE SR Server Adapter	Dual Broadcom 5721 PCI-Express Gigabit controllers

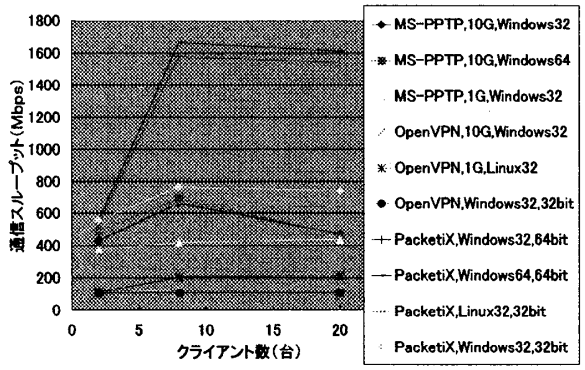

図 1　暗号化ありの場合の最大通信スループット

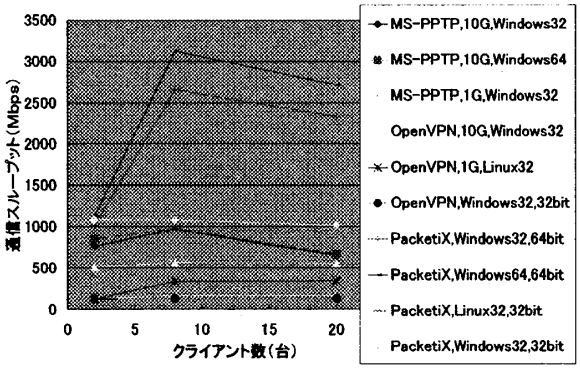

図 2　暗号化なしの場合の最大通信スループット

ピュータ間の 32 本の TCP コネクションを半分にわけ、それぞれが別方向にデータ通信するように設定した。そして、それぞれの計算機での全 TCP コネクションの総受信データ量と総送信データ量の合計値を測定時間で割った値を通信スループットとして用いた。

また、VPN においては、暗号化は通信スループットの値に大きな影響を与える。本研究では、暗号化をする場合としない場合の双方について測定実験を行った。

2.4 測定結果

暗号化ありで通信をした場合の測定結果を図 **1**、暗号化なしで通信した場合の測定結果を図 **2** に示す。

図 1、図 2 を比較することから、暗号化しない場合の通信スループットは暗号化する場合の通信スループットよりも 1 倍以上から 2 倍程度大きいことがわかる。

また、図 1、図 2 から、VPN サーバーとして 64bit マシン (10Giga Ethernet Interface 搭載) を用いた場合はどのソフトウェアでも大きな通信スループットが出ていることがわかる。しかしながら、32bit マシンの場合と比較して非常に大きな値にはなっていない。

また、いずれの場合もクライアント台数が 8 台の時、もっとも大きな値を示している。これは、クライアント台数が増えることよりサーバーがセッションを管理する部分のオーバヘッドが増大し、通信性能が低下したと思われる。

全体的には、今回測定に用いた様々なサーバー環境のいずれにおいても高いスループットを出したものは PacketiX 2.0 であり、逆に低いスループットとなったものは、OpenVPN となっている。今回の実験ではクライアント計算機の OS を Windows に限定して行ったためにこのような結果となったが、様々なクライアントに対応可能かという観点で調査をすれば、これとは異なる結果になるものと思われる。これらについては今後の課題としたい。

3. 終わりに

本研究では、学外から学内のネットワーク資源への通信路を広帯域かつ安全に実現可能なソフトウェア型 VPN システムのうち、汎用のＰＣ上で動作可能な VPN ソフトウェアを対象に通信スループットがどの程度になるかについて比較調査を行った。本研究ではクライアント計算機の OS として Windows 32bit 版として実験を行った。その結果、もっとも高い通信スループットを出したのは、64bit マシンかつ Windows 64bit 版上で動作させた PacketiX VPN 2.0 であった。

今後の課題としては、様々な OS を搭載したクライアントでの同様な実験、および、ネットワークインタフェースを 2 つ持つサーバー計算機について片側を trust なセグメントに、もう片側を untrust なセグメントに接続した環境での実験を行う予定である。

謝　辞

本研究を遂行するにあたり、Windows x64 版の PacketiX VPN 2.0 のソフトウェアについてはソフトイーサ社から開発中のサーバをお借りした。ここに感謝の意を呈する。

なお、本研究は、平成 17 年度の大学共同利用機関法人　情報・システム研究機構からの受託事業「グリッド・認証技術による大規模データ・計算資源の連携基盤の構築」の一部として実施した。

参考文献

1) PacketiX VPN 2.0,
http://www.softether.com/jp/products/
2) Microsoft PPTP,
http://www.microsoft.com/windows2000/en/advanced/help/access_pptp.htm
3) OpenVPN ,
http://openvpn.net/