ＶＰＮを利用したセキュアなＬＡＮ接続サービスについて

日下孝二　寺元貴幸　佐々井祐二　宮下卓也　岡田正　山本吉範

津山工業高等専門学校　総合情報センター

概要　　業務や研究の多様化により、学外から学内LANのリソースへ、自由にアクセスしたいという要望が増えてきている。しかし、学内には貴重な情報があり、学外と容易に接続できるような設定では、セキュリティ上問題となる。

そこで、VPN装置を利用して、高いセキュリティを確保した上で、学外との接続が可能なシステムを導入し、教職員にサービスを行う体制を構築したので、その様子について報告する。

1. はじめに

津山高専では、セキュリティ面を考慮し、基本的に学内LANとインターネットとは切り離したネットワークとなっている。しかし、大学との共同研究等で、学内コンピュータと外部ネットワークとを直接接続する必要もある。

その場合、現時点では、総合情報センターに利用申請書を提出することにより、学内LANからNATサーバ経由で、学外との直接接続を可能としている。

また、学外から学内LANへは、SSHのポートフォワーディングを使ったゲートウエイサーバ経由の接続が許可されているが、利用範囲が限られている。

最近、ネットワークインフラの充実により、出張等による、外出先から学内LANのリソースへ自由にアクセスし、研究や業務を行ないたいという要望が増えてきている。その内容としては、

・学内メールの確認
・スケジュールの確認
・共有ファイルの参照

等がある。

また、同時期に地元企業から、インターネット・リモートアクセスVPN接続の構築についての技術相談もあった。

以上の状況や理由により、昨年度からVPN接続サービスについて検討を開始した。[1]

テスト運用の手順としては、実際にVPN装置をインターネットに接続し、学内LAN側スイッチの代わりに、あえてセキュリティを弱くしたパソコンを接続した状態で、パケットモニタリングを行い、不要なパケットの侵入チェックを行った。

その結果、以上の接続方法は、特に問題ないと判断し、今年度から教職員にサービスを提供できる体制が整ったのでその様子について以下に報告する。

2. リモートアクセスVPN

2.1　セキュリティ統合アプライアンス

学外から学内LANにアクセスを可能とするVPN装置は、セキュリティ統合アプライアンスとしてシェアの高い、Juniper Networks社のSSG5を導入することにした。選定の理由としては実績のあるVPN機能を重視し、低価格であること、高機能といった点があげられる。

図１　セキュリティ統合アプライアンス［SSG5］

この装置には以下の様な特徴がある。

- ファイアウォール機能
- IPsec VPN機能
- NAT、NAT-Traversal機能
- 統合脅威管理（UTM）機能
- 高可用性（HA）機能

ファイアウォール機能、IPsecのパラメータ等は、この機種に特化した解説書の推奨設定を参考に行った。[2]

2.2　IPsecによるVPN

インターネット経由でリモートアクセスを行う場合、盗聴、データの改ざん、なりすまし等の脅威に対して対処する必要がある。

IPsecは、多数の暗号化方式や、セキュリティプロトコルの種類を選択して利用することで、安全な通信が確保できる。しかし、設定可能な組み合わせが多数存在するため、設定が煩雑になる。また、IPsecには標準でユーザ認証機能がサポートされていない。

リモートアクセスVPNでは、不特定IPアドレスからの接続を受けるため、認証が重要となる。より高いセキュリティを確保するため、「Xauth」機能を利用してユーザ認証を行っている。（図２）

図２　Xauth 認証画面

2.3　VPNリモートPC

IPsecはレイヤー３で動作するため、VPNさえ通過してしまえば、学内LANが外部からの危険にさらされてしまう。リモートPCからのアクセスは、安全なコネクションを確保する必要があるため、VPN装置と同じメーカが提供している、専用のソフトウェア「Netscreen-Remote」を利用することにした。価格は10ユーザライセンスで2万円程度になる。

インストール自体は特に問題なく［Next］ボタンを押していけば完了する。しかし、VPN接続を行う場合、本校側に設置したVPN装置と同じ設定にする必要がある。設定項目は多岐にわたるため、一般ユーザには敷居が高く、設定ミスが予想される。

そのためユーザには、あらかじめ基本部分を設定したファイルをインポートした後、ユーザ認証に必要な部分のメールアドレスのみを変更してもらう方法で対応することにした。（図３）

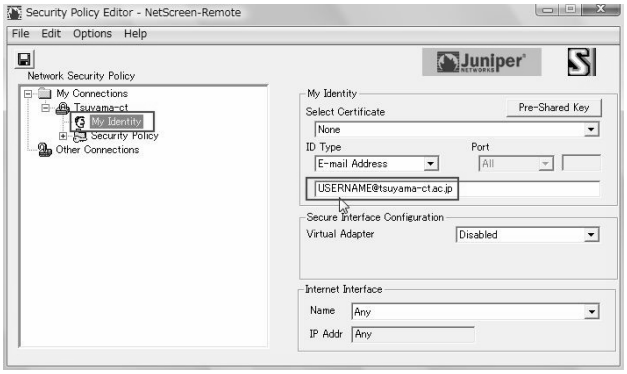

図３　メールアドレスの変更

実際にVPN接続を行ってみると、コネクション接続の開始部分と切断部分の操作が、ユーザにとって非常に分かりづらい。

特にVPN接続中の確認は、タスクトレイの小さなアイコンの表示に頼るため、ユーザは必要な操作を終了した時点でVPN接続を切断したと思い込み、VPN接続中のまま他の操作を続行するケースがある。

そうすると、無意識のまま1ライセンスを使用していることになる。（図４）

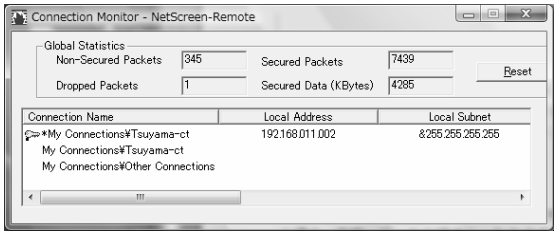

図４　Connection Monitor

この状態でリモートPCの再起動を行うと再度

VPN接続を開始するため（図２）のユーザ認証画面が数秒おきに表示されてしまい、対処できない状態になる。

この問題を解消するため、VPN接続の開始および切断をコマンドラインで動作するバッチファイルを作成し、ユーザが簡単に操作できるように対応した。

2.4　Windows 7への対応

本校でもWindows 7ユーザが徐々に増えてきている。現行バージョンのNetscreen-RemoteをWindows 7にインストールすると仮想アダプタ作成時にエラーとなり、利用することができない。

この場合は、Windows XPまたはVistaが動作する仮想マシンを作成し、その上で実行しなければならない。XPモード、VirtualBoxそれぞれの仮想環境下において、VPN接続が正常に行えることの確認はとれた。

しかし、VPN接続を行うためだけに仮想化環境を構築することには課題が残る。

3.　運用・管理

導入したVPN装置は小規模拠点仕様のため、最大トンネル数は25となっている。これに合わせ、リモートPC用のNetscreen-Remoteを20ライセンス準備した。

VPN接続希望ユーザは、事前に利用申請書を提出してもらうことになっている。なお、無条件にVPN接続が許可されるものではなく、必要と認められた場合のみ、短期間の接続が許可される。接続が許可される例としては

・出張、留学等により学内LANへの接続が困難な場合
・特別な理由により一時的に学内LANを利用する必要性が高い場合
・システム管理上必要と認められた場合

等となっている。

ユーザ登録は、VPNポリシーを最小限にするため、ユーザグループ単位で管理することにした。VPN接続時に使用するゲートウエイ（仮想トンネル）とユーザグループを割り当てることにより、ユーザ毎に必要なVPNポリシーをひとつにまとめることが可能になる。また、ライセンス数の管理も容易になる。（図５）

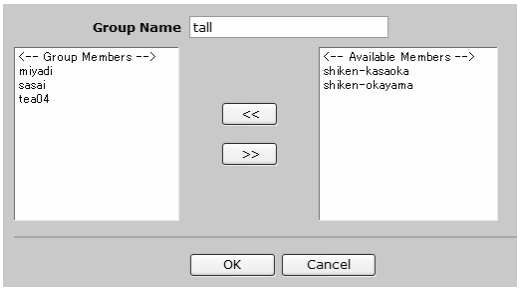

図５　グループに所属するユーザ

4.　あとがき

以上で示した様に、約1年間テスト運用を行ってきたが、特に問題が認められなかったため、運用を開始した。

教職員の出張等で個人ユーザの利用率はまだ少ないが、平成22年度学力入学試験実施の際には、VPN接続環境が、サブ的通信手段として準備された。本校の入試本部と各試験会場との連絡はメインとしてFAXで行っているが、不測の事態に備えておくためである。インターネット接続が可能であれば、遠隔地においても学内で操作しているのと同じ環境で業務が行える。

インターネットを利用しているため、通信コストが抑えられ、尚且つ、リモートアクセスVPNにより、専用線並みの安全性を確保した通信環境を提供することが可能となった。

最新のクライアントOSへの対応など、いくつかの問題点もあるが今後も検討を重ね、より安全性の高いシステムの構築を目指したい。

参　考　文　献

[1]　寺元貴幸,佐々井祐二,宮下卓也,日下孝二,岡田正,田辺茂:”津山高専のセキュリティ対策について”,情報処理教育研究発表会論文集第 29 号, pp.323-325,2009.

[2]　粕淵卓,藤田政博,山崎善実:”NetScreen/SSG設定ガイド”,技術評論社,2008.