VPN構築

～SoftEther 2.0 Beta3.2 vs FreeBSD 5.X～

(NISOC版) 2005/07/24, (EBUG版補足) 2005/09/10
神保道夫(karl@nisoc.or.jp)

0. 目的

インターネットの普及とブロードバンドの普及に伴い、従来は専用線で接続されていた拠点が、インターネットを経由したVPNに置き換えられることが多くなっている。今回は、外出先から社内・自宅等のサーバーへのアクセスを目的としたVPN構築法を考えてみる。

1. VPNのおさらい

VPNとは、Virtual Private Networkの略で、社外の離れたところから社内のリソースにアクセスしたり、離れたネットワーク同士をインターネット等を経由して接続する手法の事である。

2. VPNの種類

VPNの実現方法としては、

- SOCKS アプリケーションプロトコルに依存せずに、トランスポート層の上でアクセス制御を行うためのプロトコル
- PPTP Microsoft社によって提案された暗号通信のためのプロトコル
- IPSec IETF(The Internet Engineering Task Force)が標準化を進めている暗号化通信方式

が代表的である。現在ではPPTPとIPSecがよく使われている。
そして、最近、SoftEther が登場した。SoftEtherは、ソフトイーサ(株)の開発したVPNソフトで、注目を浴びている。

3. PPTPとSoftEtherを比較する

PPTP　Microsoftが規格したプロトコルのため、Windows2000以降のPCであれば、クライアント機能を持っている。そのため、PPTPサーバーがあれば、簡単にVPN接続ができる。
YAMAHA RT57iやRTX1100などを用いれば、LAN間VPNも構築できる。
→手軽ではあるが、サーバーの設定には、費用面・スキルが必要かも。

SoftEther　ソフトイーサ社の規格したプロトコルのため、サーバにはSoftEther VPN Serverをインストールし、クライアントにはSoftEther VPN Clientをインストールする必要がある。しかし、ClientはWin98以降のWindowsに対応しているので、古い環境のマシンでは使えるかもしれない。また、LAN間VPNにも対応している。
フリーソフト扱いであるが、商用版のSoftEther CAも存在する。
現在はオープンソース化はされていないが、検討中である。また、Linux等への対応予定もある。
→完全無料でのVPNの構築も可能である。

4. インストールのポイント

PPTP Server on FreeBSD

FreeBSDでは、ports等で供給されている、poptopをインストールし、/etc/ppp.conf, /etc/secret, /usr/local/etc/pptpd.conf 等を設定することにより、実現できる。
しかし、FreeBSD 5.Xの場合、arp proxyに問題があるようで、FreeBSD 4.Xで動いていた設定をそのまま持ってきても動かない。そこで、

/etc/ppp/ppp.conf で、pptpを定義している部分の最初に、
enable proxy
を書くと、うまく動くようになる。FreeBSD 4.Xでは、enable proxyはどこに
書いても問題なかったので、FreeBSD 5.X固有の問題と思われる。

SoftEther on WindowsXP Professional

SoftEtherは、port 80や443経由でアクセスする機能があるが、一番単純な
直接モードでVPN Serverにアクセスする方法で試してみた。
直接モードでは、標準ではport 8888でVPN Serverが動いているので、LAN内に設置
したVPN Serverにアクセスするには、グローバルアドレスの8888番ポートへの
アクセスを、LAN内の8888番ポートにリダイレクトする必要がある。
自宅では、FreeBSDをゲートウェイにしていたので、/etc/rc.confで、

```
natd_program="/sbin/natd"       # path to natd, if you want a different one.
natd_enable="YES"               # Enable natd (if firewall_enable == YES).
natd_interface="vr0"            # Public interface or IPaddress to use.
natd_flags="-redirect_port tcp 192.168.4.234:8888 8888"         # Additional fla
gs for natd.
```

(192.168.4.234はVPN ServerのIPアドレス)
を書くことにより、LAN内のVPN Serverにアクセスすることができるようになる。
ブロードバンドルータで行う場合も、8888ポートをリダイレクトするように設定して
やれば、同じことができると思う。
あと、既知の問題として、SoftEther beta3.2のWinCapを使ってブリッジを組んで
外部の通信を行うと、FreeBSDのマシンで、「arplookup 0.0.0.0 failed : host is
not on local network」というメッセージが出続けるという問題が確認されているが、
beta4以降で修正されたかどうかは未確認である。

5. SoftEtherのBSD対応について

http://www.softether.com/jp/vpn2/beta4.aspx
のページに書かれていますが、FreeBSD 4.X, 5.Xへの対応が予定されています。予定期日は
9月末ですので、まもなく登場することでしょう。

6. まとめ

この原稿を書いている段階では、SoftEther 2.0はまだベータ版なので、マニュアル等がそろっている
SoftEther 1.0を使うというのも手であるが、SoftEther 2.0は慣れると非常に設定が楽なので、出先から
自宅内にあるサーバーをいじるような場合は、SoftEtherの方が便利だと思う。逆に、FreeBSDやLinux等の
スキルが高い方は、poptop(pptpd)をインストールして使ったほうが、WindowsXPの普及等を考えると、そちらの
方が管理が一元化できて便利だと思う。