VPN style are GO!
～PPTP編～

Jun.7.2003
at NISOC mini workshop

YOSHIDA “千年技術者” Ken-ichi
5hed@nisoc.or.jp

おしながき

- VPNについて
- PPTPによるVPN構築
  - サーバの構築、設定
  - クライアント側の設定

拠点を結ぶ

- 拠点間をネットワークで結びたい
  - 本社と支社を結んでデータ交換
  - 出先から社内のサーバへアクセス
- いままでは…
  - 専用線で結ぶ→高くて遅い
  - 携帯電話やPHSで会社に接続
    →遠距離だと通話料金が高額に

専用線からVPNへ

- インターネットの普及
  - ブロードバンド回線（ADSL、光ファイバ）
  - アクセスポイントの増加
  - 低価格化
- インターネットを使ってなんとかできないものだろうか？

VPN（Virtual Private Network）

VPN（Virtual Private Network）

- ネットワーク（インターネット）を専用線のように使うことができる
  - バーチャルなプライベートネットワーク

VPNいろいろ

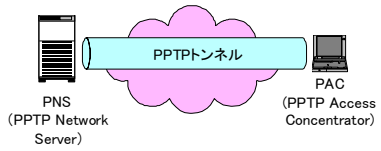
- レイヤー2でトンネリング
  - PPTP
  - L2TP
- レイヤー3でトンネリング
  - IPSec

PPTP

- レイヤー2（データリンク層）でのトンネル
- Microsoft、Ascend（今のLucent）、US.Robotics（今の3Com）などが共同開発
- RFC2637で規定
- PNS（サーバ）とPAC（クライアント）で構成

PNSとPAC

- PNS（PPTP Network Server）
  - いわゆるサーバ（待ち受け側）
- PAC（PPTP Access Concentrator）
  - いわゆるクライアント（リクエスト側）



PPTPセッション確立まで

- PPPやPPPoEなどでインターネットへ接続
- PACからPNSへトンネル制御用コネクションを設定
  - 受け側は1723番ポートを使用
- 拡張GREを使ってPPTPトンネル生成
  - 47番ポート
- PPTPトンネル内でPPPセッション開始
  - ユーザ認証、IPアドレス、圧縮など
- セッション確立

PPTPの特徴

- わりとお手軽にVPNができる
  - Windows系ならPAC機能が標準
  - NT/2kサーバにはPNS機能つき
  - PNS対応の低価格ブロードバンドルータも
- 標準では暗号化しない
  - Win系はMS-CHAP-V2とMPPEで対応
- IPネットワーク上でしか使えない
  - ATMやフレームリレーでは使用不可

L2TP

- レイヤー2（データリンク層）でのトンネル
- CiscoやNorthern Telecom（今のNortel Networks）が策定したL2FとPPTPをIETFが統合
- RFC 2661で規定
- LNS（サーバ）とLAC（クライアント）から構成

L2TPの特徴

- 1本の仮想トンネルで複数セッションを張ることが可能
- トンネル生成時の認証が可能
- ATMやフレームリレーでも使える
- 暗号化機能を持たない
  - Win系ではL2TP＋IPSecによる暗号化を提供

IPSec

- レイヤー3（ネットワーク層）でのトンネル
- 従来のIPを拡張したもの
  - 上位層のアプリはそのままで暗号化通信が可能
- 発信者や改ざんがないことをプロトコルで保証

IPSecを支える技術

- IKE（Internet Key Exchange）
  - 暗号化のための鍵を交換する
  - 独自の暗号化を行う
- ESP（Encapsulating Security Payload）
  - 暗号化したパケットの入れ物
- AH（Authentication Header）
  - 認証と完全性のみを保証
  - 暗号化は行わない

さて今回は

- PPTPでVPNしてみよう
  - Windows Serverなんて持ってないんです
  - IPSecできるルータもないんです
- LinuxをPNSに仕立て上げる

材料

- Linuxマシン1台
  - PNS（サーバ）として使用
  - 今回はGentoo Linuxを使用
- Windows 2000 Profeccionalマシン1台
  - PAC（クライアント）として使用
- ネットワーク環境
  - Bフレッツ＋OCN
  - Linuxマシンにグローバルを振る

Linuxマシンの設定

- カーネルにパッチをあてる
- カーネルを再構築
  - PPPを有効にしておく
- pppサーバのインストール
  - MS-CHAPv2パッチを当てる
- pptpサーバのインストール
- 設定ファイルの書き換え
- ppp接続アカウントの作成（pap/chap）

カーネルへのパッチあて

- カーネルソースを展開
  - 今回は2.4.20を使用
- カーネルをMS-CHAPv2対応にする
  - http://planetmirror.com/pub/mppe/ から linux-2.4.19-openssl-0.9.6b-mppe.patchをダウンロード
  - バージョンが違うけど、パッチは当たる

```
Pacifica# tar zxf linux-2.4.20.tar.gz
<カーネルソースを展開>
Pacifica# cd linux-2.4.20 ; patch -p1 < ../linux-2.4.19-openssl-0.9.6b-mppe.patch
```

カーネルの再構築

- 「Network device support」内の「PPP (point-to-point protocol) support」を有効にする
- で、makeしてインストールしておく

```
<PPPを有効にしてカーネルを再構築しておく>

Pacifica# make dep ; make clean ; make bzImage
<カーネルが再コンパイルされる>
Pacifica# cp arch/i386/boot/bzImage /boot/vmlinuz-2.4.20
Pacifica# make modules ; make modules_install
```

pppサーバのインストール

- ppp-2.4.1.tar.gz を拾ってくる
  - ftp://cs/anu.edu.ac/pub/software/pppなど
- 展開した後、MS-CHAPv2パッチを当てる
  - http://planetmirror.com/pub/mppe/から ppp-2.4.1-openssl-0.9.6-mppe-patch.gzを落としておく
- configure ; make ; make install

```
Pacifica# tar zxf ppp-2.4.1.tar.gz
Pacifica# cd ppp-2.4.1 ; patch -p1 < ../ppp-2.4.1-openssl-
mppe.patch
Pacifica# configure ; make ; make install
```

pptpサーバのインストール

- PopTopをダウンロード
  - http://www.poptop.org/ からpptpd-1.1.4-b4.tar.gzをダウンロードしておく
- configure ; make ; make install

```
Pacifica# tar zxf pptpd-1.1.4-b4.tar.gz
Pacifica# cd poptop-1.1.4
Pacifica# configure ; make ; make install
```

設定ファイルの書き換え

- options.pptpd
  - ホスト名をnameに設定する
  - MS-CHAP/v2とMPPEを有効に
  - 必要ならWINSの設定も

```
name pacifica.example.co.jp
-chap
+chapms
+chapms-v2
mppe-40
mppe-128
mppe-stateless
#ms-wins your.server.here
#ms-dns your.server.here
```

設定ファイルの書き換え

- pptpd.conf
  - localipとremoteipにLANと同じアドレスブロックの一部を振る

```
localip 192.168.199.18
remoteip 192.168.199.230-238
```

- chap-secrets
  - PPP用のchap-secretと同じようにユーザを設定

```
Kiku    pacifica.example.co.jp"ysukumo"       *
Yuri    pacifica.example.co.jp"fuyude"        *
```

WindowsをPACにする

- 「マイ ネットワーク」のプロパティを開き、「新しい接続」をクリックする
- 「インターネット経由でプライベートネットワークに接続する」を選ぶ
- 必要ならダイヤルアップ先を設定
- 接続先のアドレスを入力
- 接続を許可するユーザ（本人or全員）
- 接続名を入力

つないでみよう

- 「ネットワークとダイヤルアップ接続」から先ほど作った設定を起動する

確認

- コマンドプロンプトを開き、「ipconfig /all」で確認
  - PPPの状態が表示される（はず）

```
PPP adapter 仮想プライベート接続 test:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . : WAN (PPP/SLIP)
Interface
        Physical Address. . . . . : 00-AA-BB-CC-00-00
        DHCP Enabled. . . . . . . : No
        IP Address. . . . . . . . : 192.168.199.230
        Subnet Mask . . . . . . . : 255.255.255.255
        Default Gateway . . . . . : 192.168.199.230
        DNS Servers . . . . . . . :
```

Windows2kでPNS

- 実はWindows 2000 ProfessionalもPNSになれる
  - ユーザは1名に限定されるが、個人ユースなら十分
  - セキュリティに十分注意
- 新しい接続を作り、接続方法の選択時に「着信接続を受け付ける」を選ぶ

PPTPだけじゃイヤッ

- L2TPの実装：l2tpd
  - LinuxやBSDで使えるL2TPデーモン
  - http://www.l2tpd.org/
- IPSecの実装：FreeS/WAN
  - http://www.freeswan.org/
  - インストールがやや大変らしい
- 検証は諸君への宿題にしておこう