

SSH と iij-ppp を使った VPN 構築方法

IPsec などを使わずに、iij-ppp プロトコルを SSH 経由で通して VPN を構築する方法

また、IPsec などがカーネルに組み込めなかったころに無理矢理 VPN を張るために開発しました。

ここでは FreeBSD を利用していますので、適宜環境を読み変えること。

始めに

router2 から router1 へと SSH-VPN を張りにいくと仮定。

router1 のネットワークは 10.1.254.254/16、
router2 のネットワークは 10.2.254.254/16。

SSH の自動ログインの設定

router2 の root で ssh-keygen を使って ~root/.ssh/identity を作成。
このとき、パスフレーズには何も入力しない。

router1 にユーザ vpn-router2.network を作ります。
このとき、パスワードは*。

router1 の ~vpn-router2/.ssh/authorized_keys に router2 の ~root/.ssh/identity.pub の内容を書き加える。

router2 の root から router1 の vpn-router2 に接続を行ない、known_hosts に登録。

この時点で、パスワードなしで vpn-router2@router1 に login できる。

iij-ppp の設定

router1 の /etc/ppp/ppp.conf に以下を書き加える。

vpn-router2:

```
allow users vpn-router2
set timeout 0
set ifaddr 192.168.1.1/24 192.168.1.2/24 255.255.255.0
add 10.2.254.254/16 HISADDR
```

router2 の /etc/ppp/ppp.conf に以下を書き加える。

router1:

```
set timeout 0
```

```
set dial ""
set device "!ssh -x -l vpn-router2 router1 /usr/sbin/ppp -direct vpn-router2"
add 10.1.254.254/16 HISADDR
```

この時点で、 ppp -background router1 で VPN が接続できる。

自動接続設定

router2 の /etc/rc.conf に以下を書き加えると、立ち上げ時に自動で VPN が接続されるが、 default route が変えられてしまうという不具合がある。

```
ppp_enable="YES"          # Start user-ppp (or NO).
ppp_mode="auto"          # Choice of "auto", "ddial", "direct" or "dedicated".
ppp_nat="NO"             # Use PPP's internal network address translation or NO.
ppp_profile="router1"    # Which profile to use from /etc/ppp/ppp.conf.
```