Wstęp

Jak zestawić połączenie szyfrowane i przeroutować więcej niż jedną sieć.

Instalacja

Instalujemy pakiety **racoon** i **ipsec-tools**:

```
aptitude install racoon ipsec-tools
```

Konfiguracja

Plik /etc/racoon/psk.txt:

```
1.2.3.4 naszetajnehaslo
```

Plik /etc/racoon/racoon.conf:

```
log info;
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

listen {
        isakmp 11.22.33.44; #nasze IP
}

remote 1.2.3.4 {
        exchange_mode main;
        lifetime time 8 hour;
        ph1id 0;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group 2;
        }
}

sainfo anonymous {
        pfs_group 2;
        lifetime time 1 hour;
        encryption_algorithm 3des;
        authentication_algorithm hmac_sha1;
        compression_algorithm deflate;
        remoteid 0;
}
```

Plik /etc/ipsec-tools.conf:

```
#!/usr/sbin/setkey -f

flush;
spdflush;


spdadd 192.168.1.2/32 10.1.1.2/32 any -P out ipsec
          esp/tunnel/11.22.33.44-1.2.3.4/unique;

spdadd 10.1.1.2/32 192.168.1.2/32 any -P in ipsec
           esp/tunnel/1.2.3.4-11.22.33.44/unique;

spdadd 192.168.1.3/32 10.1.1.3/32 any -P out ipsec
          esp/tunnel/11.22.33.44-1.2.3.4/unique;

spdadd 10.1.1.3/32 192.168.1.3/32 any -P in ipsec
           esp/tunnel/1.2.3.4-11.22.33.44/unique;
```

Główna różnica dotycząca standardowego konfiga polega na słowie **unique** - domyślnie jest **require**.

Nadajemy uprawnienia i tworzymy linki symboliczne:

```
chmod 750 /etc/ipsec-tools.conf
ln -s /etc/ipsec-tools.conf /etc/racoon/ipsec-tools.conf
ln -s /var/log/racoon.log /etc/racoon/racoon.log
```

W pliku /etc/default/racoon ustawiamy:

```
RACOON_ARGS=" -l /var/log/racoon.log"
```

Dopisujemy do pliku /etc/logrotate.d/rsyslog plik /var/log/racoon.log, aby podlegał archiwizacji.

Firewall

Należy dopuścić ruch:

```
ethNet=eth0
iptables -A INPUT -i $ethNet -p tcp --dport 500 -j ACCEPT
iptables -A INPUT -i $ethNet -p tcp --dport 4500 -j ACCEPT
iptables -A INPUT -i $ethNet -p udp --dport 500 -j ACCEPT
iptables -A INPUT -i $ethNet -p udp --dport 4500 -j ACCEPT
iptables -A INPUT -i $ethNet -p esp -j ACCEPT
iptables -A INPUT -i $ethNet -p ah -j ACCEPT
iptables -A INPUT -i $ethNet -p ipcomp -j ACCEPT
```

Uruchomienie

```
/etc/ipsec-tools.conf
/etc/init.d/racoon restart
racoonctl vpn-connect 1.2.3.4
```