

Serveur VPN : Racoon

Debian GNU/Linux



Matthieu Vogelweith

13 janvier 2009

Résumé

Racoon IPsec

...

L'objectif de ce document est de détailler la mise en place d'un VPN IPsec avec authentification LDAP (via FreeRadius) entre 2 passerelles puis entre un "roadwarrior" et une passerelle.

Ce document a été rédigé en LaTeX en utilisant l'excellent Vim sous Debian GNU/Linux. Il est disponible aux formats XHTML et PDF. Les sources LaTeX sont disponibles ici : [L^AT_EX](#)

Licence

Copyright ©2009 Matthieu VOGELWEITH <matthieu@vogelweith.com>.

Vous avez le droit de copier, distribuer et/ou modifier ce document selon les termes de la GNU Free Documentation License, Version 1.3 ou ultérieure publiée par la Free Software Foundation ; avec aucune section inaltérable, aucun texte de première page de couverture, et aucun texte de dernière page de couverture. Une copie de la licence est disponible dans la page [GNU Free Documentation License](#).

Table des matières

Table des matières	3
1 Introduction	4
2 Préparation de la passerelle	5
2.1 Installation des paquets	5
2.2 Certificats SSL	5
2.3 Configuration de base	5
2.4 Configuration de Shorewall	6
3 Tunnel de passerelle à passerelle	7
3.1 Principe	7
4 Configuration en mode "RoadWarrior"	8
4.1 Principe	8
4.2 Configuration de la passerelle	8
5 Clients "RoadWarrior" Linux	10
5.1 Installation des paquets	10
5.2 Configuration de Racoon	10
5.3 Configuration de Shorewall	11
5.4 Gestion du tunnel	11
6 Clients "RoadWarrior" Mac OS X	12
7 Clients "RoadWarrior" Windows	13
8 Références	14

Chapitre 1

Introduction

- Permet d'établir un tunnel inter-site, éventuellement avec un concentrateur matériel (Cisco PIX, Netopia, ...)
- Permet de donner un accès complet aux roadwarriors

Chapitre 2

Préparation de la passerelle

2.1 Installation des paquets

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

2.2 Certificats SSL

Création de l'autorité de certification

```
# openssl genrsa -des3 -out /etc/ssl/private/ca.key 2048
# openssl req -new -x509 -days 3650 -key /etc/ssl/private/ca.key -out /etc/ssl/certs/ca.
pem
```

Création de la demande de signature :

```
# openssl genrsa -out /etc/ssl/private/vpn.key 2048
# openssl req -new -key /etc/ssl/private/vpn.key -out /etc/ssl/certs/vpn.csr
```

Signature du certificat :

```
# openssl x509 -req -days 3650 -CAcreateserial \
-in /etc/ssl/certs/vpn.csr -out /etc/ssl/certs/vpn.pem \
-CA /etc/ssl/certs/ca.pem -CAkey /etc/ssl/private/ca.key \
```

2.3 Configuration de base

- distribution des routes
- distribution des DNS

2.4 Configuration de Shorewall

Dans /etc/shorewall/zones :

```
net    ipv4
lan    ipv4
vpn    ipsec
```

Dans /etc/shorewall/tunnels :

```
ipsec    net    0.0.0.0/0    vpn
ipsecnat net    0.0.0.0/0    vpn
```

Dans /etc/shorewall/hosts :

```
vpn      ppp0:0.0.0.0/0
```

Dans /etc/shorewall/policy :

```
vpn      lan    ACCEPT
```

Chapitre 3

Tunnel de passerelle à passerelle

3.1 Principe

- schéma

Chapitre 4

Configuration en mode "RoadWarrior"

4.1 Principe

- l'adresse du clients n'est pas déterminable à l'avance
- schéma

4.2 Configuration de la passerelle

Dans `/etc/racoon/racoon.conf` :

```
listen {
    adminsock disabled;
}

remote anonymous {
    exchange_mode aggressive;
    certificate_type x509 "/etc/ssl/certs/vpn.pem" "/etc/ssl/private/vpn.key";
    ca_type x509 "/etc/ssl/certs/ca.pem";
    my_identifier asn1dn;
    proposal_check claim;
    generate_policy on;
    nat_traversal on;
    dpd_delay 20;
    ike_frag on;
    proposal {
        encryption_algorithm aes;
        hash_algorithm sha1;
        authentication_method hybrid_rsa_server;
        dh_group 2;
    }
}

mode_cfg {
    network4 192.168.100.1;      # 192.168.100.1 est la premiere adresse allouee aux
        clients VPN
    pool_size 20;
    netmask4 255.255.255.0;
    auth_source system;
    dns4 192.168.200.254;      # 192.168.200.254 est l'adresse du DNS dans le reseau
        local distant
    banner "/etc/racoon/motd";
    pfs_group 2;
}

sainfo anonymous {
```

```
pfs_group 2;  
lifetime time 1 hour;  
encryption_algorithm aes;  
authentication_algorithm hmac_sha1;  
compression_algorithm deflate;  
}
```

Chapitre 5

Clients "RoadWarrior" Linux

5.1 Installation des paquets

Les clients Linux utilisent également Racoon pour établir le tunnel avec le concentrateur VPN.

```
# aptitude install racoon ipsec-tools
# cp /usr/share/doc/racoon/examples/samples/roadwarrior/client/phase1-*.sh /etc/racoon/
```

5.2 Configuration de Racoon

Dans `/etc/racoon/racoon.conf` :

```
path pre_shared_key "/etc/racoon/psk.txt";

listen {
    adminsock "/var/run/racoon/racoon.sock" "root" "operator" 0660;
}

# 1.2.3.4 est l'adresse publique de la passerelle VPN
remote 1.2.3.4 {

    exchange_mode aggressive;
    ca_type x509 "/etc/ssl/certs/vpn.pem";
    proposal_check obey;
    nat_traversal on;
    ike_frag on;
    mode_cfg on;

    script "/etc/racoon/phase1-up.sh" phase1_up;
    script "/etc/racoon/phase1-down.sh" phase1_down;

    verify_cert off;
    passive off;

    proposal {
        encryption_algorithm aes;
        hash_algorithm sha1;
        authentication_method hybrid_rsa_client;
        dh_group 2;
    }
}

sainfo anonymous {
    pfs_group 2;
}
```

```
lifetime time 1 hour;
encryption_algorithm aes;
authentication_algorithm hmac_sha1;
compression_algorithm deflate ;
}
```

5.3 Configuration de Shorewall

Dans /etc/shorewall/zones :

```
net    ipv4
wlan   ipv4
vpn    ipsec
```

Dans /etc/shorewall/tunnels :

```
ipsec    net      0.0.0.0/0    vpn
ipsecnat net      0.0.0.0/0    vpn
ipsec    wlan     0.0.0.0/0    vpn
ipsecnat wlan     0.0.0.0/0    vpn
```

Dans /etc/shorewall/hosts :

```
vpn      eth0:0.0.0.0/0
vpn      wlan0:0.0.0.0/0
```

5.4 Gestion du tunnel

- établissement du tunnel :

```
# racoonctl vc -u <mon_login> 1.2.3.4
```

- fermeture du tunnel :

```
# racoonctl vd 1.2.3.4
```

Chapitre 6

Clients "RoadWarrior" Mac OS X

Sous MacOS X, c'est également Racoon qui est utilisé pour établir les tunnels IPSec. Il existe ensuite plusieurs interfaces graphiques permettant de configurer Racoon le plus simplement possible.

Sous MacOS 10.4, l'interface native fournie par Apple est assez simpliste et ne permet pas d'établir le tunnel IPSec dans tous les cas de figure. Il y a donc deux solutions pour configurer correctement Racoon :

- Configuration manuelle comme sous linux.
- Utilisation d'une autre interface à Racoon comme IPSecuritas [1].

Avec MacOS 10.5 le support des VPN IPSec est beaucoup plus complet et il est possible de tout faire avec le client natif. <http://www.jacco2.dds.nl/networking/openswan-macosx.html#Certs>

Chapitre 7

Clients "RoadWarrior" Windows

Le client natif de windows est assez limité mais il existe un très bon client IPSec gratuit développé par Shrew Soft [2].

Chapitre 8

Références

- [1] Client ipsec pour macos x : Ipsecuritas. www.lobotomo.com/products/IPSecuritas/.
- [2] Client ipsec pour windows : Shrewsoft vpn client. shrew.net/?page=download&prod=vpn.
- [3] Site officiel du projet debian. www.debian.org.
- [4] Site officiel des ipsec-tools. ipsec-tools.sourceforge.net.