

IPSec Roadwarrior-VPN via racoon

Dieses Dokument beschreibt die Konfiguration und den Betrieb eines VPN mit Preshared-Keys und Racoon unter Fedora Core 4.

- Falls nicht vorhanden, das Verzeichnis „/etc/racoon“ anlegen, hier werden alle Configfiles abgelegt

/etc/racoon/setkey.conf

```
#!/sbin/setkey -f

# Flush the SAD and SPD
flush;
spdflush;

#####
# Roadwarrior <-> Gateway

# 123.123.123.123 = externe IP des Gateways
# 192.168.1.0/24 = internes Netz auf Gateway-Seite

# HOST to HOST
spdadd 123.123.123.123 0.0.0.0 any -P out ipsec
    esp/tunnel/123.123.123.123-0.0.0.0/require;
spdadd 0.0.0.0 123.123.123.123 any -P in ipsec
    esp/tunnel/0.0.0.0-123.123.123.123/require;

# HOST to LAN
spdadd 192.168.1.0/24 0.0.0.0 any -P out ipsec
    esp/tunnel/123.123.123.123-0.0.0.0/require;
spdadd 0.0.0.0 192.168.1.0/24 any -P in ipsec
    esp/tunnel/0.0.0.0-123.123.123.123/require;
#####
```

- mit „chmod 0700 /etc/racoon/setkey.conf“ lesen/schreiben/ausführen für root setzen.

/etc/racoon/racoon.conf

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

# Preshared Keys
remote anonymous {
    exchange_mode aggressive, main, base;
    #doi ipsec_doi;
    nat_traversal on;
    generate_policy on;
    passive on;
    #my_identifier address 212.34.164.18;
    peers_identifier user_fqdn;
    proposal {
        encryption_algorithm 3des;
        hash_algorithm md5;
        authentication_method pre_shared_key;
        dh_group modp1024;
    }
}

sainfo anonymous {
    pfs_group modp1024;
    encryption_algorithm 3des;
    authentication_algorithm hmac_md5;
    compression_algorithm deflate;
}
```

- mit „chmod 0600 /etc/racoon/racoon.conf“ lesen/schreiben für root setzen.

/etc/racoon/psk.txt enthält die PresharedKeys in folgendem Format:

```
roadwarrior001@gateway.de MpfeEuwPEkov7ScUtKtmAa4FGWVda9jjtruesrkJKUx8sWC4u9
```

- mit „chmod 0600 /etc/racoon/psk.txt“ lesen/schreiben für root setzen.

/etc/sysconfig/racoon

```
OPTS="-f /etc/racoon/racoon.conf -l /var/log/racoon -v"
```

- mit „chmod 0644 /etc/sysconfig/racoon“ die Berechtigungen setzen

/etc/init.d/racoon

```
#!/bin/bash
#
# racoon                Start/Stop the racoon IKE daemon.
#
# chkconfig: 2345 90 60
# description: racoon is the IKE daemon of the KAME tools. Use it with \
#               the native Linux 2.6 IPsec-Stack

# processname: racoon
# config: /etc/racoon/racoon.conf
# pidfile: /var/run/racoon.pid

# Source function library.
. /etc/init.d/functions

OPTS=""

[ -f /etc/sysconfig/racoon ] && . /etc/sysconfig/racoon

RETVAL=0

prog="racoon"

start() {
    /etc/racoon/setkey.conf
    echo -n $"Starting $prog: "
    daemon racoon $OPTS
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && touch /var/lock/subsys/racoon
    return $RETVAL
}

stop() {
    echo -n $"Stopping $prog: "
    killproc racoon
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/racoon
    return $RETVAL
}

rhstatus () {
    status racoon
}

restart () {
    stop
    start
}

reload () {
```

```

    echo -n $"Reloading racoon daemon configuration: "
    killproc racoon -HUP
    RETVAL=$?
    echo
    return $RETVAL
}

case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    restart)
        restart
        ;;
    reload)
        reload
        ;;
    status)
        rhstatus
        ;;
    condrestart)
        [ -f /var/lock/subsys/crond ] && restart || :
        ;;
    *)
        echo $"Usage: $0 {start|stop|status|reload|restart|condrestart}"
        exit 1
esac

exit $?

```

- mit „chmod 0744 /etc/init.d/racoon“ die Berechtigungen setzen.
- ein „chkconfig --add racoon“ aktiviert das Script beim Booten
- mit „service racoon start“ die Security Policy Database (SPD) laden (setkey.conf) und den Racoon-Dämon starten
- geloggt wird nach /var/log/racoon
- Um den Debuglevel zu erhöhen ggf. in /etc/sysconfig/racoon die -v Option um weitere v ergänzen, z.B.

```
OPTS="-f /etc/racoon/racoon.conf -l /var/log/racoon -vvv"
```

Revision #1

Created 30 April 2021 12:08:33 by magenbrot

Updated 17 July 2021 14:45:39 by magenbrot