

Establish VPN connections with vpnc

Marcus Lange (marcus (at) lug-norderstedt.de)

v1.1 July, 01st 2007 Command lines and output with different font type
v1.0 April, 20th, 2007 initial documentation

How to establish a VPN connection with the "vpnc" software?

Table of Contents

1	About this documentation	2
2	Prerequisites	2
2.1	What is described here?	2
2.2	What is not described?	2
3	Needed components	2
4	Installation	3
5	Configuration	3
6	Connected, or not?	4
6.1	Establish the connection	5
6.2	Closing the connection	5
7	Trouble-shooting	5
7.1	Is the VPN connection working?	5
7.2	Data is going to be transferred but it stalls with a bigger volume	5
7.3	Connection cannot be created	6
8	Credits	7
9	Links	7
10	To-do's	7

1 About this documentation

This documentation describes how to establish a VPN connection with the "vpnc" software. The installation and documentation was done with Fedora Core 6.

Terminal commands that start with a \$ (dollar) can be issued as normal user and with # (pound sign) only as root user.

Most lines have some comments at the end what the command is doing (also starting with a #). Of course these must not be entered.

What is vpnc?

vpnc is a simple VPN client for UNIX and Linux with the goal to create connection to a Cisco 3000 VPN Concentrator. For the encrypted connections the IPSec protocol will be used.

Why using another software and not the original client from Cisco?

- vpnc is no kernel module but a so-called userland program. So, no need to re-compiled and configured again and again after just updating the kernel.
- vpnc can work out of the box with kernel 2.6.x, with the Cisco client this only working with bigger efforts and own programming work.
- The software is much more slim and therefore also faster in execution and performance
vpnc = ca. 49 kbyte, NetworkManager-vpnc = ca. 61 kbyte
Cisco Client = ca. 1,5 - 2 MB
- vpnc is licensed as GPL, the Cisco client has its own, non-GPL-compliant license

2 Prerequisites

2.1 What is described here?

- needed software and files
- installation of the software
- configuration of the software
- creating and closing of a connection
- trouble-shooting

2.2 What is not described?

It is assumed that the general network and Internet setup is already working or will be done elsewhere.

3 Needed components

Check that the Linux kernel was compiled with the following options (see e.g., /boot/config-2.6.19-1.2911.fc6):

- Tunnel support # CONFIG_TUN
- Encryption support # CONFIG_CRYPT*_* and the sub options
vpnc can handle many algorithms

Hint:

The default kernel of FC6 supports all these options already, so need to recompile.

- vpnc # for the VPN connections
- network manager for vpnc # special network manager for vpnc

4 Installation

After the network and Internet connection was successfully checked you can install the software. By default this is not included with FC6.

```
# yum install vpnc NetworkManager-vpnc # installs the packages and all dependencies
```

Here an excerpt from yum:

Dependencies Resolved

```
=====
Package                Arch      Version      Repository    Size
=====
Installing:
NetworkManager-vpnc    x86_64    1.0.6.4-3.fc6  extras        61 k
vpnc                   x86_64    0.3.3-13.fc6  extras        49 k
=====
```

Transaction Summary

```
=====
Install      2 Package(s)
Update      0 Package(s)
Remove      0 Package(s)
=====
```

```
Total download size: 111 k
Is this ok [y/N]: y
```

5 Configuration

vpnc was made that simple that it can work strictly speaking without configuration. Via the command line the vpnc tool can be run together with the connection data. But this is not very comfortable, so it is recommended to use a configuration file. The following is the file for the tunneled network:

```
# /etc/vpnc/default.conf
```

This file should be backup'ed first in order to prevent any unintended overwriting:

```
# cp /etc/vpnc/default.conf /etc/vpnc/default.conf.original
```

This file consists of the following data:

```
#IPSec gateway my.vpn.gateway
#IPSec ID my.ipsec.id
#IPSec secret mysecret
# your username goes here:
#Xauth username
# if you want to test rekeying specify nonzero seconds here:
#Rekeying interval 0
```

When there are several VPN access servers, you can save all configurations, to be able to use them later on. The only important point is that always a "default.conf" file is existing. For this a symlink can be helpful. It can be pointed to the respective file depending on the personal need. Here is an example:

```
# mv /etc/vpnc/default.conf /etc/vpnc/holland.conf
# cp /etc/vpnc/holland.conf /etc/vpnc/uk.conf
# ln -s /etc/vpnc/holland.conf /etc/vpnc/default.conf
```

Now the access data has to be adapted to the own requirements.

```
# vi /etc/vpnc/holland.conf

IPSec gateway vpn-holland.mydomain.com
IPSec ID vpn
IPSec secret vpn4me
Xauth username marcus
#Xauth password
```

Explanation:

IPSec gateway	The VPN server
IPSec ID	The group name of the VPN server
IPSec secret	The group secret of the VPN server
Xauth username	The user name of the user to login
Xauth password	Here the user's password can be inserted. Because it will be saved in clear text in an ASCII file, this should be avoided because of security reasons

For further options see the man page of vpnc or with "vpnc --help" and "vpnc --long-help".

Because the network is completely bent over to the VPN connection (at least for the used network card), other DNS server will be necessary for name resolution. Even when vpnc will backup the original file, you should backup the current DNS configuration yourself:

```
# cp /etc/resolv.conf /etc/resolv.conf_without_vpn
```

That's all for configuration.

6 Connected, or not?

6.1 Establish the connection

Having vpnc installed and configured, you can now test the connection:

```
# vpnc

Enter password for marcus@vpn-holland.mydomain.com
Connect Banner:
| WARNING: This is a restricted
| access server. If you do not
| have explicit permission to
| be accessing this system,
| please leave immediately.
| Unauthorized access to this
| system is illegal. Attempts
| to access this server by any
| person not authorized will be
| reported to the appropriate
| law enforcement agencies
| including the FBI.
|
| http://vpn.internal
```

VPNC started in background (pid: 4634)...

The VPN connection was established successfully.

6.2 Closing the connection

To close the connection enter the following to the command line:

```
# vpnc-disconnect
Terminating vpnc daemon (pid: 4634)
```

7 Trouble-shooting

7.1 Is the VPN connection working?

The following commands are helpful to any trouble-shooting:

```
# lsmod | grep tun           # was the "tun" kernel module loaded?
# ps -ef | grep vpn         # is the vpnc process running with the ID?
# ifconfig -a              # has the tun0 interface an IP address?
```

7.2 Data is going to be transferred but it stalls with a bigger volume

This phenomenon can be seen often with e-mails and attachments and complex websites. When transferring data it will be split into smaller, more handy packages in order to send them via TCP/IP. However, these can have different sizes, so that some packages are too big for the VPN connection. This package size is known as MTU (Maximum Transfer Unit) and can be defined differently for every network interface. With "ifconfig" it can be checked and also modified:

```
# ifconfig -a                # show details for all network interfaces

tun0  Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
      inet addr:129.150.124.46  P-t-P:129.150.124.46  Mask:255.255.255.255
      UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1412  Metric:1
      RX packets:4 errors:0 dropped:0 overruns:0 frame:0
      TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:500
      RX bytes:572 (572.0 b)  TX bytes:8644 (8.4 KiB)
```

The MTU is 1412 byte. Packages that are bigger will be either split by the VPN server. Then it is possible that the transfer will may work (perhaps with a lower speed). But when the server is ignoring and dropping all oversized packages, then the data transfer is interrupted.

In order to decrease the MTU size, use the following command:

```
# ifconfig tun0 mtu 1200
```

To get the optimal MTU size, you have to play a bit. However, the administrator for the VPN server can give helpful advice.

7.3 Connection cannot be created

If the Linux system is secured by a firewall, this can maybe interfere the VPN connection. Check the firewall rules with the following command:

```
# iptables -L
```

These rules are normally saved here:

```
# /etc/sysconfig/iptables
```

With FC6 the following rules are active by default:

```

Chain INPUT (policy ACCEPT)
target     prot opt source                destination
RH-Firewall-1-INPUT  all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
RH-Firewall-1-INPUT  all  --  anywhere              anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
ACCEPT     icmp --  anywhere              anywhere      icmp any
ACCEPT     esp  --  anywhere              anywhere
ACCEPT     ah   --  anywhere              anywhere
ACCEPT     udp  --  anywhere              224.0.0.251      udp dpt:mdns
ACCEPT     udp  --  anywhere              anywhere          udp dpt:ipp
ACCEPT     tcp  --  anywhere              anywhere          tcp dpt:ipp
ACCEPT     all  --  anywhere              anywhere          state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere              anywhere          state NEW tcp dpt:ssh
ACCEPT     udp  --  anywhere              anywhere          state NEW udp dpt:netbios-ns
ACCEPT     udp  --  anywhere              anywhere          state NEW udp dpt:netbios-dgm
ACCEPT     tcp  --  anywhere              anywhere          state NEW tcp dpt:netbios-ssn
ACCEPT     tcp  --  anywhere              anywhere          state NEW tcp dpt:microsoft-ds
REJECT     all  --  anywhere              anywhere          reject-with icmp-host-prohibited

```

With these rules there are no problems to establish the VPN connection. Also an already established connection is not interfered.

Due to this it could be advisable to verify the active rules and to adapt them if necessary.

8 Credits

My thank goes to Geoffrey Keating for the initial development and Maurice Massar at university of Kiel (Germany) for the further development.

9 Links

```

vpnc      http://www.unix-ag.uni-kl.de/~massar/vpnc/
IPSec    http://www.elektronik-kompendium.de/sites/net/0906191.htm
MTU      http://www.elektronik-kompendium.de/sites/net/0812211.htm
MTU      http://www.linux-club.de/faq/Internetverbindungsprobleme_-_IPv6_MTU_DNS

```

10 To-do's

- create and close VPN connection via a graphical program