Using Cisco VPN client on Linux

Šarūnas Burdulis

August 24, 2006

Contents

1 Install

1.1 Become root

```
host:$ su -
```

1.2 Get Cisco VPN client for Linux

Download form Dartmouth Computing website, Resources/Connectivity/Linux section. As of August 24, 2006 Cisco VPN client can be downloaded as

`http://software.dartmouth.edu/secured/Linux/Connectivity/vpnclient-linux.tar.gz`

1.3 Unpack the .tar.gz:

```
host:/usr/local/src# tar -xvzf vpnclient-linux.tar.gz
host:/usr/local/src# cd vpnclient
host:/usr/local/src/vpnclient#
```

1.4 Run the installer script

The script will ask several questions, but the guessed values should be correct. If the script cannot guess the value (empty [] brackets in the prompt, that indicates a problem and the install won't be successful anyway). It is important to have kernel source tree of the running kernel not-cleaned: the installer needs it to compile the driver.

A sample install session:

```
host:/usr/local/src/vpnclient# ./vpn_install
Cisco Systems VPN Client Version 4.8.00 (0490) Linux Installer
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.

By installing this product you agree that you have read the
license.txt file (The VPN Client license) and will comply with
its terms.

Directory where binaries will be installed [/usr/local/bin]

Automatically start the VPN service at boot time [yes]

In order to build the VPN kernel module, you must have the
kernel headers for the version of the kernel you are running.

Directory containing linux kernel source code [/lib/modules/2.6.15-26-686/build]

* Binaries will be installed in "/usr/local/bin".
* Modules will be installed in "/lib/modules/2.6.15-26-686/CiscoVPN".
* The VPN service will be started AUTOMATICALLY at boot time.
* Kernel source from "/lib/modules/2.6.15-26-686/build" will be used to build the module.

Is the above correct [y]

<... ... ...>

Setting permissions.
    /opt/cisco-vpnclient/bin/cvpnd (setuid root)
    /opt/cisco-vpnclient (group bin readable)
    /etc/opt/cisco-vpnclient (permissions not changed)
* You may wish to change these permissions to restrict access to root.
* You must run "/etc/init.d/vpnclient_init start" before using the client.
* This script will be run AUTOMATICALLY every time you reboot your computer.
```

Check/create appropriate startup script links. This depends on Linux distribution. For Debian/Ubuntu:

```
host:# ls -s /etc/init.d/vpnclient_init /etc/rc2.d/S85vpnclient_init
```

It is important to understand that running the `vpnclient_init` script does not create VPN yet. The script only checks whether the system is configured properly and loads the necessary kernel module.

2 Configuration

Cisco VPN client configuration files are in `/etc/CiscoSystemsVPNClient`. `*.ini` files are normally OK and can be left as they are.

A connection profile containing several essential parameters however is needed to make a particular VPN connection (it is still possible to make a connection without the profile file, but you'll be prompted for those parameters every time you initiate a connection). The following is the contents of a minimal profile file for connecting to Dartmouth VPN:

```
[main]
Description=Dartmouth VPN
Host=vpn.dartmouth.edu
AuthType=1
GroupName=<secret>
GroupPwd=<secret>
Username=<your DND name here>
```

To obtain secrets for `GroupName` and `GroupPwd`, go to

`http://www.dartmouth.edu/comp/support/library/safecomputing/defenses/network/transit/vpn/win/authen-dnd.`

and look for **Name** and **Password**. You will need Kerberos to access this page. Save the file as `/etc/CiscoSystemsVPNClient/Profiles/dartmouth.pcf`, for example.

3 Making a connection

To make a connection a cisco_ipsec module must be loaded. If you have just installed the VPN client, it may not be running yet. To load it 'manually' do (as root):

```
# /etc/init.d/vpnclient_init start
```

which does some checks on the system and then loads the module. To make a connection (no need to be root) do:

```
$ vpnclient connect dartmouth
```

('dartmouth' is the name of the profile you created in step 2.)

A sample connection session:

```
$ vpnclient connect dartmouth
Cisco Systems VPN Client Version 4.8.00 (0490)
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.6.15-26-686 #1 SMP PREEMPT Thu Aug 3 03:13:28 UTC 2006 i686
Config file directory: /etc/opt/cisco-vpnclient

Initializing the VPN connection.
Contacting the gateway at 129.170.3.254
Contacting the gateway at 129.170.3.10 (balancing)
```

```
User Authentication for dartmouth...

Enter Username and Password.

Username [sarunas]:
Password []:
Authenticating user.
Negotiating security policies.
Securing communication channel.

Your VPN connection is secure.

VPN tunnel information.
Client address: 129.170.84.89
Server address: 129.170.3.10
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: LZS
NAT passthrough is active on port UDP 10000
Local LAN Access is disabled
```

The VPN between your host and the Dartmouth VPN server was created.

To bring the session to the background press Ctrl-Z and type 'bg':

```
  [1]+  Stopped                 vpnclient connect sample
  host:~$ bg
  [1]+ vpnclient connect dartmouth &
```

The VPN has been created. It can be checked by tracing the route to some other host (www.cisco.com in this example):

```
$ traceroute www.cisco.com
traceroute to www.cisco.com (198.133.219.25), 30 hops max, 38 byte packets
 1  public.vpn2.dartmouth.edu (129.170.3.11)  0.761 ms  0.674 ms  0.740 ms
 2  vpn.berry1-crt.dartmouth.edu (129.170.84.1)  0.872 ms  0.827 ms  0.865 ms
 3  ropeferry-berry.ropeferry1-crt.dartmouth.edu (129.170.2.2)  0.871 ms  0.957 ms  0.992 ms
 4  core.border1-rt.dartmouth.edu (129.170.2.195)  0.996 ms  0.957 ms  0.993 ms
 5  A5-0-0-241.G-RTR1.MAN.verizon-gni.net (64.223.133.161)  43.186 ms  25.247 ms  25.326 ms
   ...
```

The output shows the Dartmouth VPN server (public.vpn2.dartmouth.edu) as the nearest gateway. Though actually there are probably several physical routers before public.vpn2.dartmouth.edu is reached. The communication between your host and the VPN server takes place via virtual "wire" and is also encrypted.

4 Disconnecting

Enter:

```
host:~$ vpnclient disconnect
```

```
Cisco Systems VPN Client Version 4.8.00 (0490)
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.6.15-26-686 #1 SMP PREEMPT Thu Aug 3 03:13:28 UTC 2006 i686
Config file directory: /etc/opt/cisco-vpnclient

Disconnecting the VPN connection.
Your VPN connection has been terminated.
```

The VPN has been destroyed and your system should have returned to the normal operation via default routing table. Again, this can be tested by traceroute:

```
$ traceroute www.cisco.com
traceroute to www.cisco.com (198.133.219.25), 30 hops max, 38 byte packets
 1  bradley.berry1-crt.dartmouth.edu (129.170.28.254)  0.414 ms  0.452 ms  0.391 ms
 2  ropeferry-berry.ropeferry1-crt.dartmouth.edu (129.170.2.2)  0.465 ms  0.601 ms  0.509 ms
 3  core.border1-rt.dartmouth.edu (129.170.2.195)  0.471 ms  0.476 ms  0.511 ms
 ...
```

The nearest gateway is now your usual default gateway.