Procédure installation Open VPN sur Xivo

Contenu

Installation du serveur OpenVPN sur le Xivo

Installation of OpenVPN and easy-rsa

Debian comes with precompiled packages for OpenVPN. This is an easy way to install OpenVPN.

Update the apt-sources

```
~# apt-get update

Get:1 http://ftp.de.debian.org etch Release.gpg [386B]

Hit http://ftp.de.debian.org etch Release

Ign http://ftp.de.debian.org etch/main Packages/DiffIndex

Ign http://ftp.de.debian.org etch/non-free Packages/DiffIndex

Ign http://ftp.de.debian.org etch/main Sources/DiffIndex

Ign http://ftp.de.debian.org etch/non-free Sources/DiffIndex

Hit http://ftp.de.debian.org etch/main Packages

Hit http://ftp.de.debian.org etch/non-free Packages

Hit http://ftp.de.debian.org etch/main Sources

Hit http://ftp.de.debian.org etch/non-free Sources
```

```
Fetched 1B in 0s (2B/s)

Reading package lists... Done

~#
```

Si il y a une erreur « W: GPG error: http://mirror.xivo.fr lenny Release: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 2D0C2DE0DFB0B268 »

Taper la commande : wget -q http://mirror.xivo.fr/xivo_current.key -O- | sudo apt-key add -

Puis relancer : apt-get update

Install OpenVPN packages

```
~# apt-get install openvpn

Reading package lists... Done

Building dependency tree... Done

The following extra packages will be installed:

  liblzo2-2

The following NEW packages will be installed:

  liblzo2-2 openvpn
```

```
0 upgraded, 2 newly installed, 0 to remove and 30 not upgraded.

Need to get 397kB of archives.

After unpacking 1114kB of additional disk space will be used.

Do you want to continue [Y/n]? y

Get:1 http://ftp.de.debian.org etch/main liblzo2-2 2.02-2 [59.5kB]

Get:2 http://ftp.de.debian.org etch/main openvpn 2.0.9-4etch1 [338kB]

Fetched 397kB in 1s (354kB/s)

Preconfiguring packages ...

Selecting previously deselected package liblzo2-2.

(Reading database ... 44213 files and directories currently installed.)

Unpacking liblzo2-2 (from .../liblzo2-2_2.02-2_i386.deb) ...

Selecting previously deselected package openvpn.

Unpacking openvpn (from .../openvpn_2.0.9-4etch1_i386.deb) ...

Setting up liblzo2-2 (2.02-2) ...



Setting up openvpn (2.0.9-4etch1) ...
```

```
Starting virtual private network daemon:.



~#
```

Copy easy-rsa

```
~# cp -R /usr/share/doc/openvpn/examples/easy-rsa/2.0 /etc/openvpn/easy-rsa
```

Configuration of OpenVPN

On Debian, OpenVPN load all files with the .conf extension in /etc/openvpn.

Create server configuration for OpenVPN

```
~# touch /etc/openvpn/server1194udp.conf
```

Edit the file with your favorit editor:

```
~# vi /etc/openvpn/server1194udp.conf
```

Paste the following content into the file:

```
port 1194
```

```
proto udp

dev tun

ca keys/ca.crt

cert keys/server.crt

key keys/server.key

dh keys/dh1024.pem

server 10.0.0.0 255.255.255.0

client-config-dir ccd

ifconfig-pool-persist ipp.txt

client-to-client

keepalive 10 120

persist-key

persist-tun

status /var/log/openvpn-status.log

verb 6
```

Create client/phone configuration for OpenVPN

The content of the configuration file is the same on all clients/phones. To avoid having to configure both files, client and server, in one directory, create a subfolder called client-config:

```
~# mkdir /etc/openvpn/client-config

~# mkdir /etc/openvpn/client-config/tmp
```

The configuration file for the phone must be called vpn.cnf:

```
~# touch /etc/openvpn/client-config/vpn.cnf
```

Edit this file with your favorit editor:

```
~# vi /etc/openvpn/client-config/vpn.cnf
```

Paste the following content into the file, but remember to set the value for remote <Server-IP/-name> to your server's IP or fqdn: XXX.XXX.XXX.XXX ici, c'est l'adresse IP publique derrière laquelle le Xivo est connecté

```
client

dev tun

proto udp

remote XXX.XXX.XXX.XXX 1194

resolv-retry infinite
```

```
nobind

persist-key

persist-tun

ca /openvpn/ca.crt

cert /openvpn/client.crt

key /openvpn/client.key

ns-cert-type server

verb 0

ping 10

ping-restart 60
```

Creation of certificates with easy-rsa

Easy-rsa configuration setup

```
~# vi /etc/openvpn/easy-rsa/vars
```

The value for KEY_DIR must be set to the path configured in server1194udp.conf:

```
>> export KEY_DIR=" $EASY_RSA/../keys"
```

The values for the creation of the certificates have to be set. Here is an example:

```
export KEY_COUNTRY="FR"

export KEY_PROVINCE="57"

export KEY_CITY="Metz"

export KEY_ORG="Le Bureau"

export KEY_EMAIL="lebureau@lebureau.fr"
```

Certificate creation with easy-rsa

```
~# cd /etc/openvpn/easy-rsa

~# source ./vars

~# ./clean-all
```

Creation of the ca-certificate

```
~# ./build-ca

Generating a 1024 bit RSA private key

.....++++++

.....++++++
```

writing new private key to 'ca.key'

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [US]: DE

State or Province Name (full name) [CA]: BLN

Locality Name (eg, city) [SanFrancisco]: Berlin

Organization Name (eg, company) [Fort-Funston]: snom technology AG

Organizational Unit Name (eg, section) []: Administration

Common Name (eg, your name or your server's hostname) [Fort-Funston CA]: Servername

Email Address [me@myhost.mydomain]: noreply@snom.com

```
~#
```

Creation of the server certificate

```
~# ./build-key-server server

Country Name (2 letter code) [US]:DE

State or Province Name (full name) [CA]:BLN

Locality Name (eg, city) [SanFrancisco]:Berlin

Organization Name (eg, company) [Fort-Funston]:snom technology AG

Organizational Unit Name (eg, section) []:Administration

Common Name (eg, your name or your server's hostname) [server]:  Servername

Email Address [me@myhost.mydomain]:noreply@snom.com

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
```

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName :PRINTABLE:'DE'

stateOrProvinceName :PRINTABLE:'BLN'

localityName :PRINTABLE:'Berlin'

organizationName :PRINTABLE:'snom technology AG'

organizationalUnitName:PRINTABLE:'Administration'

commonName :PRINTABLE:'openvpn.intern.snom.de' ← ein Beispiel

emailAddress :IA5STRING:'noreply@snom.com'

Certificate is to be certified until Oct 21 12:04:51 2018 GMT (3650 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

Creation of Diffie Hellman parameter

```
~# ./build-dh

Generating DH parameters, 1024 bit long safe prime, generator 2

This is going to take a long time

..+.[...]

[...]....+....

~#
```

Création des configurations clients (.tar)

!! Il faut générer les fichiers de configuration du client à partir du serveur OpenVPN auquel il devra se connecter.

Creation of client/phone certificates

Every client/phone should have its own certificate. It is necessary to give each certificate an individual name, e.g. the phone's MAC address, for example 00041370F7FB:

```
~# cd /etc/openvpn/easy-rsa

~# source ./vars

~# ./build-key  00041370F7FB

Generating a 1024 bit RSA private key

.............++++++

.....................................++++++

writing new private key to ' 00041370F7FB.key'

-----

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.
```

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [US]:DE

State or Province Name (full name) [CA]:BLN

Locality Name (eg, city) [SanFrancisco]:Berlin

Organization Name (eg, company) [Fort-Funston]:snom technology AG

Organizational Unit Name (eg, section) []:Administration

Common Name (eg, your name or your server's hostname) [00041370F7FB]: 00041370F7FB

Email Address [me@myhost.mydomain]:noreply.snom.com

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

```
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName          :PRINTABLE:'DE'

stateOrProvinceName   :PRINTABLE:'BLN'

localityName         :PRINTABLE:'Berlin'

organizationName      :PRINTABLE:'snom technology AG'

organizationalUnitName:PRINTABLE:'Administration'

commonName           :PRINTABLE:'00041370F7FB'

emailAddress         :IA5STRING:'noreply.snom.com'

Certificate is to be certified until Oct 21 12:32:41 2018 GMT (3650 days)

Sign the certificate? [y/n]:y



1 out of 1 certificate requests certified, commit? [y/n]y
```


```
Write out database with 1 new entries

Data Base Updated

~#
```

Creation of the VPN tarball

As an example I am using the same MAC we used to create the certificates:

```
~# cp /etc/openvpn/client-config/vpn.cnf /etc/openvpn/client-config/tmp/

~# cp /etc/openvpn/keys/00041370F7FB.crt /etc/openvpn/client-config/tmp/client.crt

~# cp /etc/openvpn/keys/00041370F7FB.key /etc/openvpn/client-config/tmp/client.key

~# cp /etc/openvpn/keys/ca.crt /etc/openvpn/client-config/tmp/ca.crt

~# cd /etc/openvpn/client-config/tmp/

~# chown -Rf root:root *

~# chmod -R 700 *

~# tar cvpf vpnclient-00041370F7FB.tar *

~# rm client.*
```

Copier le *.tar généré par cette commande dans un tftp

Configure the phone

VPN settings

You will find the settings for VPN on the web interface at Advanced → QOS/Security → Security. Set the value of VPN to "on" and save. A new configuration field will appear called "Unzipped VPN config tarball". For our example you have to paste

"tftp://192.168.XXX.XXX/vpnclient-0004132FFFFF.tar" into it.

Identity settings

Let's assume that OpenVPN is installed on the SIP-server. Now you have to look for the IP address of the tunnel device.

```
~# ifconfig

eth0      Link encap:Ethernet  HWaddr 00:00:00:00:00:00

          inet addr:192.168.10.59  Bcast:192.168.255.255  Mask:255.255.0.0

          inet6 addr: 2001:db8::20c:29ff:fedb:1a9b/64 Scope:Global

          inet6 addr: fe80::20c:29ff:fedb:1a9b/64 Scope:Link

          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

          RX packets:10330779 errors:0 dropped:0 overruns:0 frame:0

          TX packets:2582071 errors:0 dropped:0 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:1000
          RX bytes:954308825 (910.0 MiB)  TX bytes:515281166 (491.4 MiB)
          Interrupt:177 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1425 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1425 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:767072 (749.0 KiB)  TX bytes:767072 (749.0 KiB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.0.0.1  P-t-P:10.0.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
```

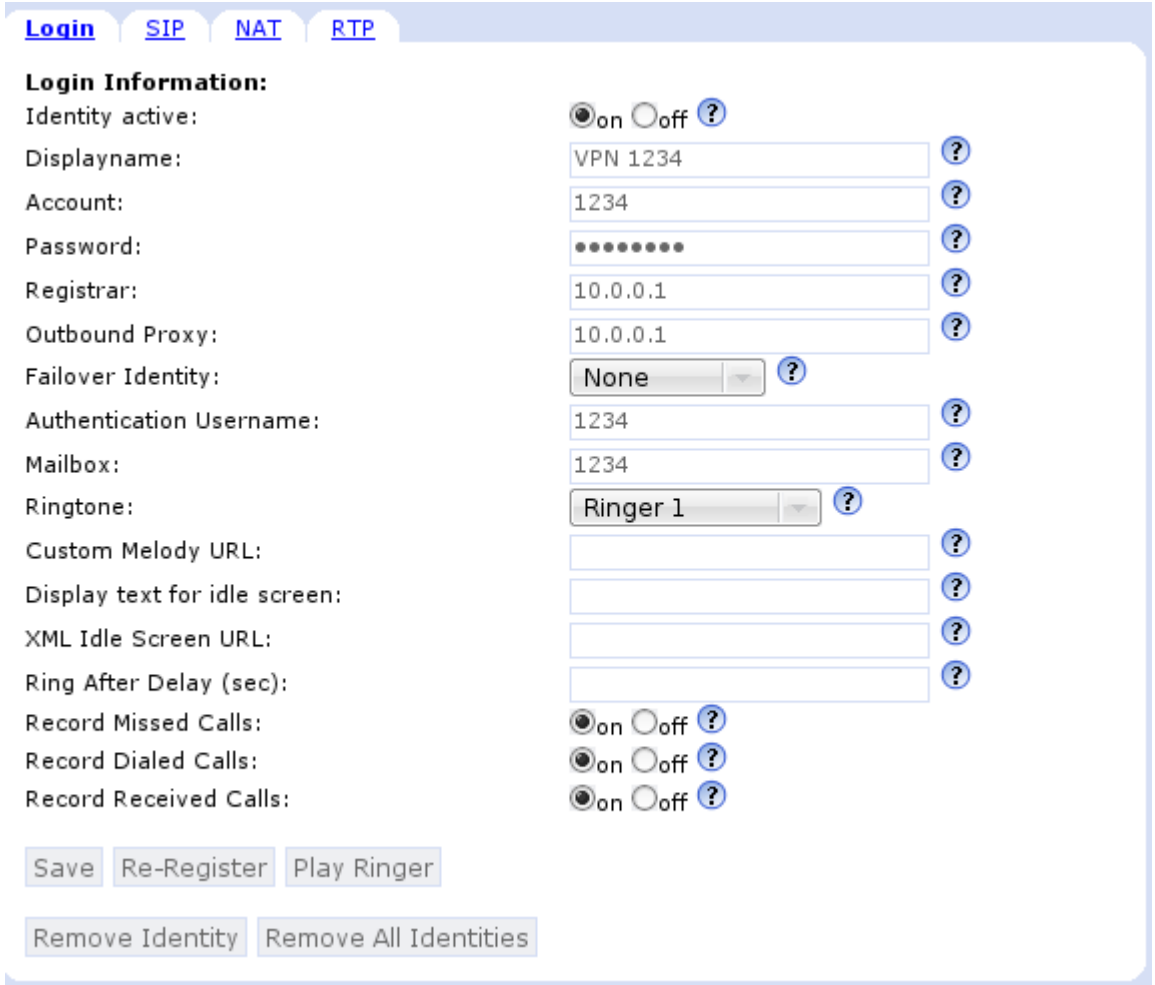
RX packets:6 errors:0 dropped:0 overruns:0 frame:0

TX packets:8 errors:0 dropped:0 overruns:0 carrier:0

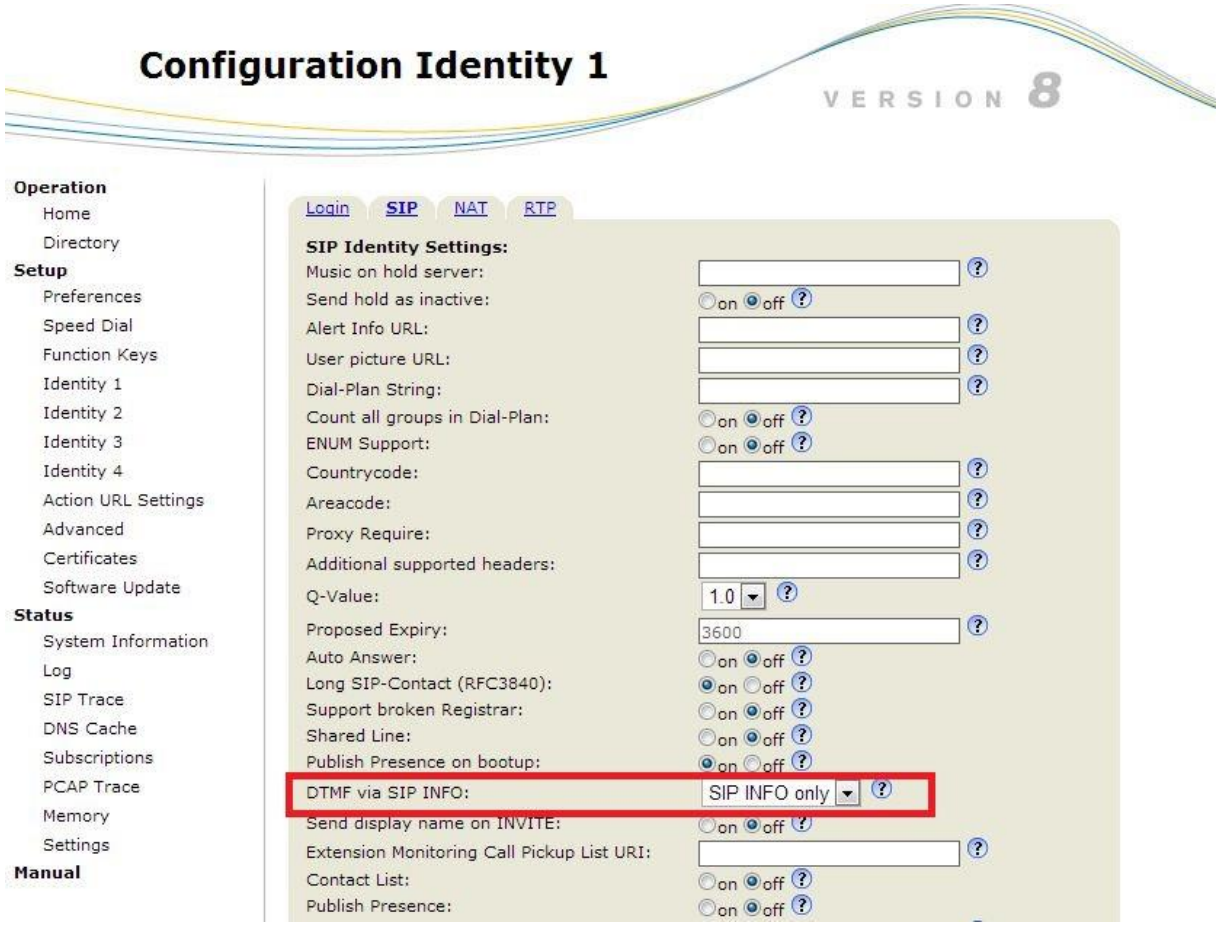
collisions:0 txqueuelen:100

RX bytes:3062 (2.9 KiB) TX bytes:4177 (4.0 KiB)

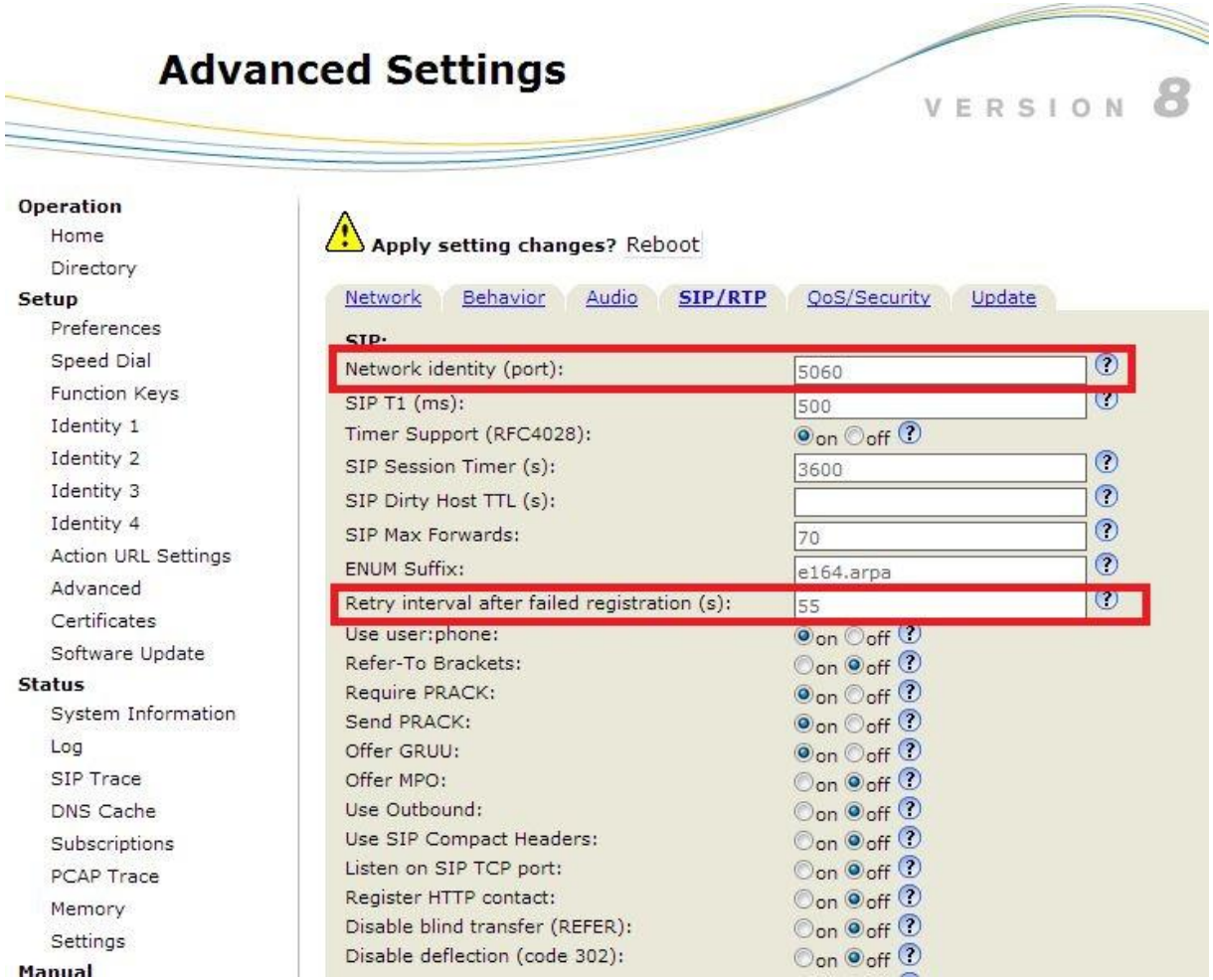
In this example tun0 is the OpenVPN tunnel device. You will find the IP address of the server next to the "inet addr" string (10.0.0.1).
Enter the server's IP address as registrar and proxy in Configuration Identity/Login.



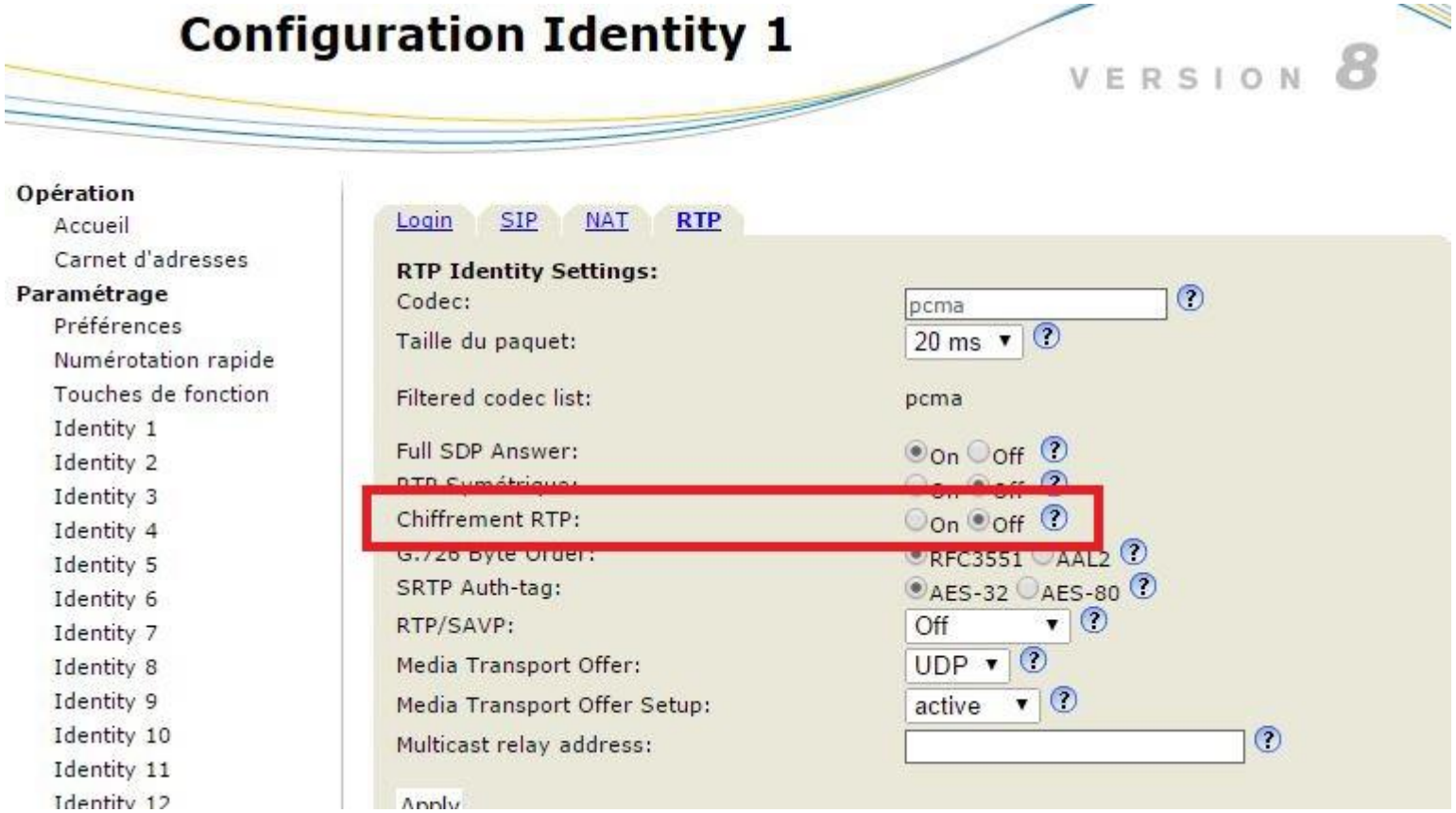
Modifier l'option "DTMF via SIP INFO" à "SIP INFO only"



Modifier les options “Network identity (port)” à “5060” et “Retry interval after failed registration (s)” à “55”



Enfin, placer le chiffrement RTP à OFF dans l'onglet → Identity 1 → RTP



Procédure écrite à partir de http://wiki.snom.com/Networking/Virtual_Private_Network_(VPN)/How_To_for_Debian