OpenVPN (serveur)

De Docs du CCRI

Installation

```
sudo apt-get install openvpn openvpn-auth-ldap openssl ca-certificates easy-rsa
```

Pré-configuration

```
cd /etc/openvpn/
make-cadir easy-rsa
```

On édite le fichier **/etc/openvpn/easy-rsa/vars** :

```
export KEY_SIZE=2048
export KEY_COUNTRY="FR"
export KEY_PROVINCE="Essonne"
export KEY_CITY="Orsay"
export KEY_ORG="IUT Orsay"
export KEY_EMAIL="ccri.iut-orsay@u-psud.fr"
export KEY_OU="CCRI"
```

On fait appel au script :

```
source ./vars
```

On purge les anciens certificats (s'il y en a) :

```
./clean-all
```

On créé l'autorité de certificat :

```
./build-ca
```

On créé les paramètres Diffie Hellman (attention, c'est long) :

```
./build-dh
```

On créé le certificat du serveur (et on le signe) :

```
./build-key-server grievous
```

Afin d'utiliser l'authentification **tls-auth**, il faut générer une clef privée secrète.

```
openvpn --genkey --secret keys/ta.key
```

On créé un sous répertoire pour stocker les fichiers de configuration du serveur :

```
mkdir /etc/openvpn/server/
```

On recopie les fichiers nécessaires :

```
cd /etc/openvpn/server/
cp ../easy-rsa/keys/ca.crt .
cp ../easy-rsa/keys/grievous.crt .
cp ../easy-rsa/keys/grievous.key .
cp ../easy-rsa/keys/dh2048.pem .
cp ../easy-rsa/keys/ta.key .
```

Configuration

On créé le fichier de configuration **/etc/openvpn/server.conf** :

```
# OpenVPN Configuration file.
# Which local IP address should OpenVPN
# listen on? (optional)
local 192.70.36.52

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 443

# TCP or UDP server?
proto tcp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
```

```
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
dev tun

# VPN Topology
topology subnet

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).  Each client
# and the server must have their own cert and
# key file.  The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/grievous.crt
key /etc/openvpn/server/grievous.key

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh /etc/openvpn/server/dh2048.pem

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.42.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt

# Clients configuration directory
client-config-dir /etc/openvpn/clients-routes

# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
```

```
#
# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
tls-auth /etc/openvpn/server/ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
max-clients 30

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
;user nobody
;group nogroup

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status /var/log/openvpn/openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.  Use one
# or the other (but not both).
log         /var/log/openvpn/openvpn.log
log-append  /var/log/openvpn/openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 4
```

```
# Silence repeating messages.  At most 20
# sequential messages of the same message
# category will be output to the log.
mute 20

# LDAP Auth
plugin /usr/lib/openvpn/openvpn-auth-ldap.so "/etc/openvpn/external-auth/auth-ldap.conf"
```

On créé les dossiers nécessaires :

```
mkdir /etc/openvpn/external-auth/
mkdir /var/log/openvpn/
mkdir /etc/openvpn/clients-routes/
mkdir /etc/openvpn/clients-conf/
```

On créé le fichier **auth-ldap.conf**

```
<LDAP>
        # LDAP server URL
        #URL            ldap://ldap.iut.orsay.fr
        URL             ldap://ldap.iut-orsay.fr

        # Bind DN (If your LDAP server doesn't support anonymous binds)
        # BindDN                uid=Anonymous,ou=People,dc=iut-orsay,dc=fr

        # Bind Password
        # Password      SecretPassword

        # Network timeout (in seconds)
        Timeout         15

        # Enable Start TLS
        TLSEnable       no

        # Follow LDAP Referrals (anonymously)
        FollowReferrals yes

        # TLS CA Certificate File
        TLSCACertFile   /usr/local/etc/ssl/ca.pem

        # TLS CA Certificate Directory
        TLSCACertDir    /etc/ssl/certs

        # Client Certificate and key
        # If TLS client authentication is required
        TLSCertFile     /usr/local/etc/ssl/client-cert.pem
        TLSKeyFile      /usr/local/etc/ssl/client-key.pem

        # Cipher Suite
        # The defaults are usually fine here
        # TLSCipherSuite        ALL:!ADH:@STRENGTH
</LDAP>

<Authorization>
        # Base DN
        BaseDN          "ou=people,dc=iut-orsay,dc=fr"

        # User Search Filter
        SearchFilter    "(&(uid=%u))"
```

```
        # Require Group Membership
        RequireGroup    false

        # Add non-group members to a PF table (disabled)
        #PFTable        ips_vpn_users

        <Group>
                BaseDN          "ou=groups,dc=iut-orsay,dc=fr"
                SearchFilter    "(|(cn=developers)(cn=artists))"
                #MemberAttribute        uidNumber
                # Add group members to a PF table (disabled)
                #PFTable        ips_vpn_eng
        </Group>
</Authorization>
```

Récupérée de « https://ccri.iut-orsay.fr/docs/index.php?title=OpenVPN_(serveur)&oldid=3452 »
