Articles populaires

» Quel serveur choisir ? dédié ? VPS ? virtuel ? cloud ?

» Construire un VPN avec OpenVPN sur Debian 8

» Quelle distribution GNU/Linux pour votre serveur ?

» Migrer de Debian Wheezy (Debian 7) vers Debian Jessie (Debian 8)

» Comment avoir des sites rapides avec ISPConfig et Debian 8 ?

» Connexion SSH : Write failed: Broken pipe

» Installer un site PrestaShop avec ISPConfig basé sur NGINX

» Quels utilitaires installer par défaut sur votre serveur ?

» Installer Mumble sur un serveur Debian ou Ubuntu

» Mes premiers pas dans le « Public Cloud OVH » : introduction

Articles récents

» Quelle solution pour un serveur de sauvegarde ?

» Quelle infrastructure pour un serveur web ?

» Quel prompt shell amélioré utiliser sous Linux ?

» Connexion SSH : Write failed: Broken pipe

» Redémarrer son VPS Cloud ovh en mode rescue, s'y connecter en SSH et utiliser le chroot

Commentaires récents

xavier dans » Construire un VPN avec OpenVPN sur Debian 8

ernest random dans » Construire un VPN avec OpenVPN sur Debian 8

Clément dans » Construire un VPN avec OpenVPN sur Debian 8

Michel dans » Installer un site PrestaShop avec ISPConfig basé sur NGINX

Florent dans » Installer un site WordPress rapide avec ISPConfig et NGINX

Accueil » **Construire un VPN avec OpenVPN sur Debian 8**

Construire un VPN avec OpenVPN sur Debian 8

par Christophe Guilloux | Geek | 44 commentaires

Pourquoi mettre en place un VPN ?

Avant toute chose, un VPN **ne** vous rend **pas** ,en lui-même, anonyme. Je lis des tonnes de tutoriels sur Internet avec des arguments basés sur la peur pour vous vendre leur service VPN. Ils vous expliquent que vous pouvez surfer sur Internet anonymement. Vous devez vérifier si le fournisseur VPN enregistre ce que vous faites à travers son VPN et ensuite lui faire confiance quand il dit qu'il n'enregistre rien.

Un VPN sert à sécuriser les échanges entre un point A et un point B. Il crée un réseau privé et les échanges **à l'intérieur** de ce réseau restent privés. Si vous utilisez un VPN pour **ressortir** du réseau et aller sur Internet, le destinataire verra l'IP sortante du serveur VPN au lieu de votre IP. Il croira juste que vous dormez dans un datacenter dans un autre pays éventuellement. Mais votre fournisseur de VPN devient, de fait, aussi votre fournisseur d'**accès à Internet**, tout comme votre fournisseur d'accès à Internet standard. Dans les deux cas, votre fournisseur de VPN ou votre fournisseur d'accès à Internet standard, savent qui vous êtes et peut savoir ce que vous faites.

SI vous voulez être réellement anonyme, utilisez Tor à la place d'un VPN. Bien que sur le papier, il est possible de désanonymiser Tor, en pratique c'est impossible.

Installation du serveur VPN OpenVPN sur Debian 8

Connectez-vous sur votre serveur et lancez ceci :

```
apt install -y openvpn
cp -a /usr/share/easy-rsa /etc/openvpn/
cd /etc/openvpn/easy-rsa
source vars
./clean-all
```

Création des certificats

Créez les certificats de l'autorité de certification (il se trouve que ce sera sur le même serveur que le serveur VPN mais cette autorité pourrait être hébergée ailleurs) :

```
./build-ca
```

Vous verrez quelque chose comme ceci (laissez les paramètres par défaut sauf si ça vous fait plaisir de les changer) :

```
Generating a 2048 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]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:
```

Vous pouvez vérifier que les premiers fichiers ont bien été créés :

```
ls -la keys/
```

On voit le certificat de l'autorité de certification **ca.crt** et **ca.key** :

```
drwx------ 2 root root 4096 Jun 22 18:54 .
drwxr-xr-x 3 root root 4096 Jun 22 18:52 ..
-rw-r--r-- 1 root root 1818 Jun 22 18:54 ca.crt
-rw------- 1 root root 1708 Jun 22 18:54 ca.key
-rw-r--r-- 1 root root    0 Jun 22 18:52 index.txt
-rw-r--r-- 1 root root    3 Jun 22 18:52 serial
```

On génère la clé Diffie-Hellman qui sert à sécuriser les échanges :

```
./build-dh
```

L'opération prend un tout petit peu de temps (je mets juste un bout du résultat) :

```
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
..............+.....................................................................................
```

On génère les certificats du serveur :

```
./build-key-server srvcert
```

On obtient ceci (**remplacez gs-demo.dedinux.com** par le nom de votre serveur) :

```
Generating a 2048 bit RSA private key
....+++
.................................+++
writing new private key to 'srvcert.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]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [srvcert]:gs-demo.dedinux.com
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:

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-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'SanFrancisco'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName            :PRINTABLE:'gs-demo.dedinux.com'
name                  :PRINTABLE:'EasyRSA'
emailAddress          :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until Jun 19 19:40:11 2025 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
```

Configuration d'OpenVPN

Regardez quel est le DNS du serveur VPN et notez son adresse IP dans un coin :

```
cat /etc/resolv.conf
```

Copiez la configuration par défaut :

```
gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz > /etc/openvpn/server.conf
```

Éditez la configuration :

```
nano /etc/openvpn/server.conf
```

Nous voulons que le service tourne sous un utilisateur non dangereux, cherchez ces lignes et décommentez-les (enlevez le ';' en début de ligne) :

```
user nobody
group nogroup
```

Mettez les bons chemins pour qu'il puisse trouver ses clés :

```
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/srvcert.crt
key /etc/openvpn/easy-rsa/keys/srvcert.key  # This file should be kept secret
```

Un peu plus bas, vous remplacez et mettez ceci :

```
dh /etc/openvpn/easy-rsa/keys/dh2048.pem
```

Le serveur OpenVPN sera la passerelle par défaut et les clients qui s'y connecteront seront invités à router tout leur trafic vers le VPN donc on ajoute ceci :

```
push "redirect-gateway def1 bypass-dhcp"
```

Mettez le DNS que vous avez noté à la place de ICIIPDUDNS :

```
push "dhcp-option DNS ICIIPDUDNS"
```

Sauvegardez le fichier et quittez.

Lancement du serveur OpenVPN

```
openvpn /etc/openvpn/server.conf
```

Vous verrez quelque chose comme ceci:

```
Mon Jun 22 20:02:15 2015 OpenVPN 2.3.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH] [I
Mon Jun 22 20:02:15 2015 library versions: OpenSSL 1.0.1k 8 Jan 2015, LZO 2.08
Mon Jun 22 20:02:15 2015 Diffie-Hellman initialized with 2048 bit key
Mon Jun 22 20:02:15 2015 Socket Buffers: R=[212992->131072] S=[212992->131072]
Mon Jun 22 20:02:15 2015 ROUTE_GATEWAY 167.114.224.1
Mon Jun 22 20:02:15 2015 TUN/TAP device tun0 opened
Mon Jun 22 20:02:15 2015 TUN/TAP TX queue length set to 100
Mon Jun 22 20:02:15 2015 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Mon Jun 22 20:02:15 2015 /sbin/ip link set dev tun0 up mtu 1500
Mon Jun 22 20:02:15 2015 /sbin/ip addr add dev tun0 local 10.8.0.1 peer 10.8.0.2
Mon Jun 22 20:02:15 2015 /sbin/ip route add 10.8.0.0/24 via 10.8.0.2
Mon Jun 22 20:02:15 2015 GID set to nogroup
Mon Jun 22 20:02:15 2015 UID set to nobody
Mon Jun 22 20:02:15 2015 UDPv4 link local (bound): [undef]
Mon Jun 22 20:02:15 2015 UDPv4 link remote: [undef]
Mon Jun 22 20:02:15 2015 MULTI: multi_init called, r=256 v=256
Mon Jun 22 20:02:15 2015 IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0
Mon Jun 22 20:02:15 2015 IFCONFIG POOL LIST
Mon Jun 22 20:02:15 2015 Initialization Sequence Completed
```

Ouvrez une autre connexion SSH vers le serveur et vérifiez qu’il a ouvert un point d’accès vers son tunnel :

```
ifconfig tun0
```

Vous verrez quelque chose comme ceci :

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Le serveur doit pouvoir router votre trafic vers d’autres machines (Internet compris) :

Éditez le fichier /etc/sysctl.conf avec nano et décommentez la bonne ligne :

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Sauvegardez le fichier.

Rechargez la configuration :

```
sysctl -p /etc/sysctl.conf
```

Activez le NAT au niveau du pare-feu (translate votre adresse IP avec celle du serveur) :

```
apt remove ipmitool
apt install iptables-persistent
```

Pendant l’installation, répondre « Yes ». Chargez ces règles :

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
```

Sauvegardez les règles pour le prochain reboot :

```
/etc/init.d/netfilter-persistent save
```

Rebootez le serveur, normalement, tout est rechargé au redémarrage :

```
reboot
```

Connectez-vous de nouveau à votre serveur VPN en SSH.

Créez un certificat pour l’ordinateur qui va se connecter au VPN (votre PC Linux par exemple) et remplacez lap3.dedinux.com par le nom de votre ordinateur :

```
cd /etc/openvpn/easy-rsa/
source vars
./build-key monlaptopcert
```

Vous verrez quelque chose comme ceci :

```
Generating a 2048 bit RSA private key
...........................................+++
......................................................+++
writing new private key to 'monlaptopcert.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]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [monlaptopcert]:lap3.dedinux.com
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:

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-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'SanFrancisco'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName            :PRINTABLE:'lap3.dedinux.com'
name                  :PRINTABLE:'EasyRSA'
emailAddress          :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until Jun 19 20:05:45 2025 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
```

Sur votre station de travail Linux (faites l'équivalent des actions sur Windows ou tout autre système non digne de ce nom)

Télécgargez les certificats du client (par SFTP avec FIlezilla ou autre). Remplacez 'gs-demo' par le nom de votre serveur VPN. Les fichiers à télécharger sont : /etc/openvpn/easy-rsa/keys/ca.crt, /etc/openvpn/easy-rsa/keys/monlaptopcert.crt et /etc/openvpn/easy-rsa/keys/monlaptopcert.key :

```
scp root@gs-demo:/etc/openvpn/easy-rsa/keys/ca.crt /tmp
scp root@gs-demo:/etc/openvpn/easy-rsa/keys/monlaptopcert.crt /tmp
scp root@gs-demo:/etc/openvpn/easy-rsa/keys/monlaptopcert.key /tmp
```

Installation de OpenVPN sur votre station de travail Linux

Pour des raisons pédagogiques, on le fait en ligne de commande. Vous pouvez probablement le faire via l'interface graphique de configuration de votre réseau de votre système.

Connectez-vous en root sur votre station de travail et installez openvpn :

```
sudo su -
aptitude install openvpn
```

Copiez le fichier de configuration par défaut :

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/
cd /etc/openvpn
mkdir -p keys
cd keys
cp /tmp/ca.crt .
cp /tmp/monlaptopcert.key .
cp /tmp/monlaptopcert.crt .
```

Éditez le fichier **/etc/openvpn/client.conf** et **changez gs-demo.dedinux.com** par le nom de votre serveur VPN :

```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote gs-demo.dedinux.com 1194
```

Indiquez le chemin des certificats :

```
# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/monlaptopcert.crt
key /etc/openvpn/keys/monlaptopcert.key
```

Sauvegardez et quittez.

Lancez le client VPN (attention, vos connexions SSH vers le serveur VPN vont bloquer) :

```
openvpn /etc/openvpn/client.conf
```

La lancement montre :

```
Mon Jun 22 22:46:18 2015 OpenVPN 2.3.2 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [eureph
Mon Jun 22 22:46:18 2015 Socket Buffers: R=[212992->131072] S=[212992->131072]
Mon Jun 22 22:46:18 2015 NOTE: UID/GID downgrade will be delayed because of --client, --pull, or --up-del
Mon Jun 22 22:46:18 2015 UDPv4 link local: [undef]
Mon Jun 22 22:46:18 2015 UDPv4 link remote: [AF_INET]167.114.230.9:1194
Mon Jun 22 22:46:18 2015 TLS: Initial packet from [AF_INET]167.114.230.9:1194, sid=e7333b9f 220af87d
Mon Jun 22 22:46:19 2015 VERIFY OK: depth=1, C=US, ST=CA, L=SanFrancisco, O=Fort-Funston, OU=MyOrganizati
Mon Jun 22 22:46:19 2015 VERIFY OK: nsCertType=SERVER
Mon Jun 22 22:46:19 2015 VERIFY OK: depth=0, C=US, ST=CA, L=SanFrancisco, O=Fort-Funston, OU=MyOrganizati
Mon Jun 22 22:46:20 2015 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Mon Jun 22 22:46:20 2015 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Mon Jun 22 22:46:20 2015 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Mon Jun 22 22:46:20 2015 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Mon Jun 22 22:46:20 2015 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
Mon Jun 22 22:46:20 2015 [gs-demo.dedinux.com] Peer Connection Initiated with [AF_INET]167.114.230.9:1194
Mon Jun 22 22:46:22 2015 SENT CONTROL [gs-demo.dedinux.com]: 'PUSH_REQUEST' (status=1)
Mon Jun 22 22:46:22 2015 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,ro
Mon Jun 22 22:46:22 2015 OPTIONS IMPORT: timers and/or timeouts modified
Mon Jun 22 22:46:22 2015 OPTIONS IMPORT: --ifconfig/up options modified
Mon Jun 22 22:46:22 2015 OPTIONS IMPORT: route options modified
Mon Jun 22 22:46:22 2015 ROUTE_GATEWAY 192.168.1.254/255.255.255.0 IFACE=eth0 HWADDR=28:d2:44:57:bf:de
Mon Jun 22 22:46:22 2015 TUN/TAP device tun0 opened
Mon Jun 22 22:46:22 2015 TUN/TAP TX queue length set to 100
Mon Jun 22 22:46:22 2015 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Mon Jun 22 22:46:22 2015 /sbin/ip link set dev tun0 up mtu 1500
Mon Jun 22 22:46:22 2015 /sbin/ip addr add dev tun0 local 10.8.0.6 peer 10.8.0.5
Mon Jun 22 22:46:22 2015 /sbin/ip route add 167.114.230.9/32 via 192.168.1.254
Mon Jun 22 22:46:22 2015 /sbin/ip route add 0.0.0.0/1 via 10.8.0.5
Mon Jun 22 22:46:22 2015 /sbin/ip route add 128.0.0.0/1 via 10.8.0.5
Mon Jun 22 22:46:22 2015 /sbin/ip route add 10.8.0.1/32 via 10.8.0.5
Mon Jun 22 22:46:22 2015 GID set to nogroup
Mon Jun 22 22:46:22 2015 UID set to nobody
Mon Jun 22 22:46:22 2015 Initialization Sequence Completed
```

Vérifier que vous avez accès au tunnel :

```
ifconfig tun0
```

Vous verrez quelque chose comme ceci :

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet adr:10.8.0.6  P-t-P:10.8.0.5  Masque:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          Packets reçus:0 erreurs:0 :0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:100
          Octets reçus:0 (0.0 B) Octets transmis:0 (0.0 B)
```

Faites un ping pour tester que ça passe bien :

```
ping 10.8.0.1
```

Le ping répond :

```
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=61.2 ms
```

Testez votre accès VPN avec un navigateur et accédez à cette adresse : **https://www.whatismyip.com/**

Vous devez voir l’IP du serveur VPN à la place de l’IP de votre maison (ou cabane si vous êtes dans la cambrousse).

Il faut relancer votre client VPN à chaque besoin.

Pour commenter cet article, rendez-vous sur le forum de discussion

Anciens messages ci-dessous, rendez-vous sur le forum pour continuer la discussion

44 Commentaires

jayjay sur 11 juillet 2015 à 1 h 41 min

Bonjour,

Merci pour cet excellent tuto !

a ifconfig tun0
J’ai cette erreur: tun0: error fetching interface information: Device not found

Merci pour votre aide.
Connectez-vous pour répondre

Christophe Guilloux sur 11 juillet 2015 à 11 h 18 min

Pour lister toutes les interfaces, c’est la commande :
ifconfig -a

Si aucun tunX n’est listé alors c’est que le VPN ne s’est pas bien configuré.
Connectez-vous pour répondre

jayjay sur 12 juillet 2015 à 18 h 00 min

oui j’ai pas de tun x 🙁

jayjay sur 12 juillet 2015 à 18 h 28 min

Je suis pourtant à la lettre le tuto…
Connectez-vous pour répondre

Christophe Guilloux sur 12 juillet 2015 à 19 h 11 min

Est-ce possible d'avoir le résultat de la commande :
openvpn /etc/openvpn/server.conf

Il y a sans doute un indice.
Connectez-vous pour répondre

jayjay sur 12 juillet 2015 à 19 h 32 min

```
Sun Jul 12 17:30:58 2015 OpenVPN 2.3.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH] [IPv6] built on Dec 1 2014
Sun Jul 12 17:30:58 2015 library versions: OpenSSL 1.0.1k 8 Jan 2015, LZO 2.08
Sun Jul 12 17:30:58 2015 Diffie-Hellman initialized with 2048 bit key
Sun Jul 12 17:30:58 2015 Socket Buffers: R=[212992->131072] S=[212992->131072]
Sun Jul 12 17:30:58 2015 ROUTE_GATEWAY IP DE MON SERVEUR
Sun Jul 12 17:30:58 2015 TUN/TAP device tun0 opened
Sun Jul 12 17:30:58 2015 TUN/TAP TX queue length set to 100
Sun Jul 12 17:30:58 2015 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Sun Jul 12 17:30:58 2015 /sbin/ip link set dev tun0 up mtu 1500
Sun Jul 12 17:30:58 2015 /sbin/ip addr add dev tun0 local 10.8.0.1 peer 10.8.0.2
Sun Jul 12 17:30:58 2015 /sbin/ip route add 10.8.0.0/24 via 10.8.0.2
Sun Jul 12 17:30:58 2015 GID set to nogroup
Sun Jul 12 17:30:58 2015 UID set to nobody
Sun Jul 12 17:30:58 2015 UDPv4 link local (bound): [undef]
Sun Jul 12 17:30:58 2015 UDPv4 link remote: [undef]
Sun Jul 12 17:30:58 2015 MULTI: multi_init called, r=256 v=256
Sun Jul 12 17:30:58 2015 IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0
Sun Jul 12 17:30:58 2015 IFCONFIG POOL LIST
Sun Jul 12 17:30:58 2015 Initialization Sequence Completed
```

Connectez-vous pour répondre

Christophe Guilloux sur 12 juillet 2015 à 19 h 40 min

Le tun0 (celui du serveur) est bien lancé.
La première commande : ifconfig tun0
est à lancer… du côté serveur dans une autre fenêtre d'accès via SSH. Est-ce le cas ?
Connectez-vous pour répondre

jayjay sur 12 juillet 2015 à 19 h 50 min

c'est bon je n'avais pas bien lu qu'il fallait ouvrir une autre fenêtre via SSH ^^
Par contre avec fail2ban y a t'il une modification particulière à ce tuto ?

Y a t'il possibilité de générer un fichier .conf pour les clefs ?
Connectez-vous pour répondre

Christophe Guilloux sur 12 juillet 2015 à 22 h 14 min

Je ne vois rien qui empêche fail2ban de fonctionner.

Certains fournisseurs de VPN fournissent peut-être des fichiers .conf tout prêts mais là il faut mettre les mains dedans.
Connectez-vous pour répondre

jayjay sur 12 juillet 2015 à 22 h 42 min

Pas de soucis encore merci pour le tuto j'attend l'article sur munin 🙂
Connectez-vous pour répondre

rtripoux sur 4 août 2015 à 10 h 26 min

Bonjour,
Merci pour ce tuto très clair, il m'a aidé à me rafraîchir la mémoire 🙂

Je tiens juste à apporter une petite précision :
Vous générez la clé Diffie-Hellman afin de sécuriser les échanges mais ne l'utilisez pas.

Pour ça il faut rajouter dans la conf du server:

```
tls-auth /chemin/vers/ta.key 0
```

Puis copier ce même fichier ta.key vers le client et ajouter dans sa conf:

```
tls-auth /chemin/vers/ta.key 1
```

ce n'est que l'histoire de quelques minutes et ça renforcera la sécurité du tunnel VPN.

Bonne journée!
Connectez-vous pour répondre

Eugene sur 8 mars 2016 à 18 h 32 min

En effet cela augmente la sécurité de la liaisons vpn!
Ducoup il faut générer une clé supplémentaire coté serveur:

```
openvpn –genkey –secret ta.key
```

Cette clé doit être placé a la foi coté serveur et coté client.Prendre le chemin de cette clé et le
disposé dans les fichier client.conf et serf.conf comme expliquer ci-dessus par rtripoux.
Connectez-vous pour répondre

alternative sur 13 août 2015 à 21 h 58 min

Merci pour ce tuto !

Seul problème, au moment de faire /etc/init.d/netfilter-persistent save j'ai cette erreue :

```
[....] Saving netfilter rules...run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: /usr/share/netfilter-persistent/plugins.d/15-ip4tables exited with return code 1
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
run-parts: /usr/share/netfilter-persistent/plugins.d/25-ip6tables exited with return code 1
failed.
```

Je suis sur un kimsufi (debian 8)
Connectez-vous pour répondre

Christophe Guilloux sur 13 août 2015 à 22 h 39 min

Il vaut mieux mettre à jour les packages avant de lancer le tuto et de rebooter.
Certains font ça et il parait que ça passe :

```
set -e
/etc/init.d/netfilter-persistent save
```

Connectez-vous pour répondre

alternative sur 14 août 2015 à 1 h 27 min

Ca n'a pas fonctionné pour moi. J'ai pu lire que iptables-persistent ne fonctionne pas/mal sur les kimsufi… Il y a t'il une alternative à cette partie iptable du coup ?

D'ailleurs, lorsque je fais un iptables -L mes règles sont celles par défaut et je n'ai fais aucun reboot, je ne peux pas me le permettre, je redémarre simplement les services nécessaires.

J'ai réussi à faire fonctionner ma connexion malgré tout, mais ca me chagrine ^^

merci pour ta réponse !

Christophe Guilloux sur 14 août 2015 à 1 h 58 min

La commande suivante donnera des détails sur l'exécution :

```
sh -x /etc/init.d/netfilter-persistent save
```

Normalement, c'est censé marché. C'est le noyau d'OVH ?

```
uname -r
```

donne : 3.14.32-xxxx-grs-ipv6-64 ?

alternative sur 14 août 2015 à 10 h 04 min

Oui c'est bien ça : 3.14.32-xxxx-grs-ipv6-64

et la commande sh -x retourne ceci : http://pastebin.com/vqQvCtQa mes compétences ne me permettent pas de savoir ce qui ne tourne pas rond…
Connectez-vous pour répondre

Christophe Guilloux sur 16 août 2015 à 2 h 26 min

Y a-t-il déjà des règles de firewall ?
Que donne iptables -L -n ?
Et que donne iptables -L -n -t nat ?

Il se peut que ça fonctionne quand même.
Connectez-vous pour répondre

alternative sur 16 août 2015 à 2 h 43 min

Aucune, le serveur est fraichement installé.
iptables -L -n ne donne rien
iptables -L -n -t nat montre bien les règles

J'ai fais un iptables-save > /etc/iptables/rules.v4 entre temps pour sauvegarder les règles quelques part du coup comme je ne peux pas les rendre persistente. Vraiment bizarre ce problème sur les kimsufi

alternative sur 16 août 2015 à 15 h 05 min

Il y a autre chose que je ne comprend pas. Je lance mon server vpn : opnvpn /etc/openvpn/server.conf puis je me connecte via mon client. Maintenant si je ferme ma fenettre ssh sur mon server je suis déconnecté… Pas pratique. Openvpn ne peut pas tourner continuellement sur le server pour qu'on puisse s'y connecter n'importe quand sans avoir à le lancer en ssh ?
Connectez-vous pour répondre

Christophe Guilloux sur 19 août 2015 à 14 h 38 min

Le service openvpn est lancé automatiquement au démarrage du serveur. J'ai suggéré de faire un reboot en fin de configuration juste pour être certain que tout se lance correctement.
Connectez-vous pour répondre

Giles sur 26 août 2015 à 20 h 17 min

J'ai le même problème que alternative, je suis sur kimsufi Debian 8, je n'arrive pas à résoudre le problème, des pistes?

Christophe Guilloux sur 26 août 2015 à 20 h 25 min

C'est quel problème ? Il en a eu plusieurs.

Clément sur 16 avril 2016 à 17 h 04 min

Bonjour

j'ai eu le même problème

en lançant la commande de démarrage du server avec la commande suivante permet de détacher le serveur de la session ssh

nohup openvpn /etc/openvpn/server.conf &

Bonne journée

jp sur 5 septembre 2015 à 22 h 37 min

J'ai aussi le même problème sur un nouveau serveur Debian 8.1 avec la sauvegarde des régles d'iptables : /etc/init.d/netfilter-persistent save .
Quelqu'un a t il trouvé une solution ?
Connectez-vous pour répondre

Luc sur 10 octobre 2015 à 13 h 07 min

Hello,

Dans mes tutos perso j'ai résolu le problème avec :

Afin de rentre les nouvelles règles du firewall persistance même après un reboot de votre serveur, sauvegardez les règles actuelles dans le fichier iptables.rules

```
$ iptables-save > /etc/iptables.rules
```

Puis modifier le fichier /etc/network/interfaces (ou /etc/network/interfaces.tail, dans certaines configuration où le fichier insterfaces est généré automatiquement) pour y ajouter la ligne suivante à la fin du fichier (après la déclaration de votre carte réseau) :

```
$ nano /etc/network/interfaces.tail
pre-up iptables-restore < /etc/iptables.rules
```

Testé sur des serveurs Kimsufi (Ubuntu Server) et VPS d'OVH (Ubuntu server et Debian 8).
@+
Luc
Connectez-vous pour répondre

joel sur 10 octobre 2015 à 14 h 04 min

j'ai pas du tout touché au firewall… enfin mon iptables est vide… mais sa marche parfaitement ! merci
Connectez-vous pour répondre

Julien sur 8 novembre 2015 à 14 h 33 min

Bonjour,

Très bon tuto. L'ergonomie des blocs de code est gênante par contre, on passe la souris dessus (a priori pour copier/coller) et le texte descend d'une ligne pour afficher les boutons, faudrait que les boutons s'affichent par-dessus sans pousser le contenu vers le bas.
Connectez-vous pour répondre

Victor sur 14 novembre 2015 à 17 h 13 min

Bonjour,

Merci pour ce tutoriel. Je rencontre cependant un problème à la toute fin. Je parviens à me connecter à mon serveur VPN (debian 8) depuis mon laptop (ubuntu 12.04). Le ping 10.8.0.1 fonctionne, mais aucun autre ping ne fonctionne (sauf un ping sur mon serveur). Je n'ai donc aucun accès à Internet. En fait, je cependant peux me connecter à mon serveur (en SSH ou par mon navigateur étant donné que j'ai installé un serveur web dessus). Avez-vous une piste pour comprendre ce qui bloque ?

Merci 🙂
Connectez-vous pour répondre

patrick sur 17 novembre 2015 à 19 h 38 min

Bonjour,

Même chose de mon côté. Même config sur mon vps (debian8) et laptop (ubuntu). Ping 10.8.0.1 fonctionnel mais aucun autre. Merci
Connectez-vous pour répondre

Christophe Guilloux sur 17 novembre 2015 à 22 h 41 min

Que donne (sur le serveur) :

```
iptables -L -n -t nat
```

Patrick sur 18 novembre 2015 à 0 h 14 min

```
Chain PREROUTING (policy ACCEPT)
target prot opt source destination

Chain POSTROUTING (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

Christophe Guilloux sur 18 novembre 2015 à 0 h 22 min

Dans le tutoriel, il y a une partie sur le firewall à suivre :
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE

Patrick sur 21 novembre 2015 à 7 h 14 min

Pour votre information, j’ai résolu le problème dans mon iptables je dois utiliser venet0 aulieu de eth0

patrick sur 18 novembre 2015 à 5 h 03 min

Bonjour,

J’avais fait les lignes de commandes avec le POSTROUTING mais je me suis rendu compte que rien ne se restaurait automatiquement après le reboot, c’est pour ça que c’était vide. Après avoir ajouté les POSTROUTING, toujours pas accès à internet via mon vpn.

Après avoir démarrer le vpn client sur mon laptop, j’ai des erreurs qui apparaissent.

```
Tue Nov 17 22:58:13 2015 OpenVPN 2.3.2 i686-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [eurephia] [MH] [IPv6] built on Apr 13 2015
Tue Nov 17 22:58:13 2015 Socket Buffers: R=[163840->131072] S=[163840->131072]
Tue Nov 17 22:58:13 2015 UDPv4 link local: [undef]
Tue Nov 17 22:58:13 2015 UDPv4 link remote: [AF_INET]192.99.154.184:1194
Tue Nov 17 22:58:13 2015 TLS: Initial packet from [AF_INET]192.99.154.184:1194, sid=27d6e172 fa1fb0eb
Tue Nov 17 22:58:13 2015 VERIFY OK: depth=1, C=US, ST=CA, L=SanFrancisco, O=Fort-Funston, OU=MyOrganizationalUnit, CN=Fort-Funston CA, name=EasyRSA, emailAddress=me@myhost.mydomain
Tue Nov 17 22:58:13 2015 VERIFY OK: nsCertType=SERVER
Tue Nov 17 22:58:13 2015 VERIFY OK: depth=0, C=US, ST=CA, L=SanFrancisco, O=Fort-Funston, OU=MyOrganizationalUnit, CN=vps44648.vps.ovh.ca, name=EasyRSA, emailAddress=me@myhost.mydomain
Tue Nov 17 22:58:13 2015 Data Channel Encrypt: Cipher ‘BF-CBC’ initialized with 128 bit key
Tue Nov 17 22:58:13 2015 Data Channel Encrypt: Using 160 bit message hash ‘SHA1’ for HMAC authentication
Tue Nov 17 22:58:13 2015 Data Channel Decrypt: Cipher ‘BF-CBC’ initialized with 128 bit key
Tue Nov 17 22:58:13 2015 Data Channel Decrypt: Using 160 bit message hash ‘SHA1’ for HMAC authentication
Tue Nov 17 22:58:13 2015 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
Tue Nov 17 22:58:13 2015 [vps44648.vps.ovh.ca] Peer Connection Initiated with [AF_INET]192.99.154.184:1194
Tue Nov 17 22:58:16 2015 SENT CONTROL [vps44648.vps.ovh.ca]: ‘PUSH_REQUEST’ (status=1)
Tue Nov 17 22:58:16 2015 PUSH: Received control message: ‘PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 213.186.33.99,route 10.8.0.1,topology net30,ping 10,ping-restart 120,ifconfig 10.8.0.10 10.8.0.9’
Tue Nov 17 22:58:16 2015 OPTIONS IMPORT: timers and/or timeouts modified
Tue Nov 17 22:58:16 2015 OPTIONS IMPORT: –ifconfig/up options modified
Tue Nov 17 22:58:16 2015 OPTIONS IMPORT: route options modified
Tue Nov 17 22:58:16 2015 OPTIONS IMPORT: –ip-win32 and/or –dhcp-option options modified
Tue Nov 17 22:58:16 2015 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=wlan0 HWADDR=88:53:2e:1e:d5:02
Tue Nov 17 22:58:16 2015 TUN/TAP device tun1 opened
Tue Nov 17 22:58:16 2015 TUN/TAP TX queue length set to 100
Tue Nov 17 22:58:16 2015 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Tue Nov 17 22:58:16 2015 /sbin/ip link set dev tun1 up mtu 1500
Tue Nov 17 22:58:16 2015 /sbin/ip addr add dev tun1 local 10.8.0.10 peer 10.8.0.9
Tue Nov 17 22:58:16 2015 /sbin/ip route add 192.99.154.184/32 via 192.168.0.1
Tue Nov 17 22:58:16 2015 /sbin/ip route add 0.0.0.0/1 via 10.8.0.9
Tue Nov 17 22:58:16 2015 /sbin/ip route add 128.0.0.0/1 via 10.8.0.9
Tue Nov 17 22:58:16 2015 /sbin/ip route add 10.8.0.1/32 via 10.8.0.9
RTNETLINK answers: File exists
Tue Nov 17 22:58:16 2015 ERROR: Linux route add command failed: external program exited with error status: 2
Tue Nov 17 22:58:16 2015 Initialization Sequence Completed
```

Merci de votre aide
Connectez-vous pour répondre

caerulean sur 26 janvier 2016 à 22 h 04 min

Bonjour,

J'ai eu aussi le problème d'iptables-persistent sur un serveur kimsufi avec le kernel 3.14 d'OVH.
Une altenative qui marche très bien pour moi c'est l'utilisation d'ufw :
https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-debian-8

Merci pour ce guide qui fonctionne bien sous Debian 8 avec son kernel 3.16
Connectez-vous pour répondre

jo' sur 27 janvier 2016 à 19 h 19 min

Bonjour à tous,

Voilà mon soucis, depuis pas mal de temps déjà j'essaye d'installer sur mon serveur HP proliant ou j'ai actuellement un vmware ESXI (5.5 il me semble) un serveur OpenVPN.

Mais voilà, après beaucoup de tuto en tout genre (nicolargo, mondedie etc…) je n'ai jamais réussi à me connecter à mon VPN qui fonctionne (mon adresse IP publique ne change jamais !)

Au niveau de mon installation j'ai une box numéricable en bridge derrière un routeur Netgear R7000 qui gère mon wifi et DHCP.

Est-ce que quelqu'un si connais assez pour m'aider à configurer mon serveur, j'ai essayé déjà une install classique avec un debian 8 sur mon ESXI et une install par fichier OVA avec le OpenVPN Access server…

Je ne sais pas si je me trompe dans mes fichiers config du type server.conf et client.conf, j'ai écumé tellement de tuto que je suis perdus dans ce qu'il faut indiquer (différence entre fonction push , server par exemple)

Du coup je me casse la tête tout les soirs pour savoir si c'est un problème au niveau de la configuration de mon routeur, qu'elle port dois-je ouvrir ?

Beaucoup de blabla pour au final demander un peu d'aide car ça me ronge de l'intérieur 🙂

Merci à ceux qui liront
Connectez-vous pour répondre

Eugene sur 2 mars 2016 à 15 h 50 min

Merci, cela fonctionne!
Connectez-vous pour répondre

Louguel sur 9 mars 2016 à 16 h 29 min

Bonjour j'ai reussi cette installation jusqu'a la crétion des certificats, donc en général le openvpn est dejà prêt, maintenant ce je comprend pas comment je vais envoyé ces certificats au client je suis bloqué à ce niveau :

LE STATION DE TRAVAIL LINUX

```
scp root@gs-demo:/etc/openvpn/easy-rsa/keys/ca.crt /tmp
scp root@gs-demo:/etc/openvpn/easy-rsa/keys/monlaptopcert.crt /tmp
scp root@gs-demo:/etc/openvpn/easy-rsa/keys/monlaptopcert.key /tmp
```

ETANT DONNEES QUE LE NOM DE MES CERTIFICATS SE NOMME dadecertificat et le nom de mon server openvpn s'appel debian

Merci pour l'aide
Connectez-vous pour répondre

dadeTelimele sur 9 mars 2016 à 19 h 17 min

Bonsoir si le lance le client openvpn je reçoit cette erreur
pouvez vous m'aidé j'ai généré les clés et je les ai transféré dans mon client

```
openvpn /etc/openvpn/client.conf
```

```
Wed Mar 9 18:09:22 2016 Re-using SSL/TLS context
Wed Mar 9 18:09:22 2016 LZO compression initialized
Wed Mar 9 18:09:22 2016 Control Channel MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Wed Mar 9 18:09:22 2016 Socket Buffers: R=[229376->131072] S=[229376->131072]
Wed Mar 9 18:09:22 2016 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0 AF:3/1 ]
```

```
Wed Mar 9 18:09:22 2016 Local Options hash (VER=V4): '41690919'
Wed Mar 9 18:09:22 2016 Expected Remote Options hash (VER=V4): '530fdded'
Wed Mar 9 18:09:22 2016 UDPv4 link local: [undef]
Wed Mar 9 18:09:22 2016 UDPv4 link remote: [AF_INET]127.0.1.1:1194
Wed Mar 9 18:09:22 2016 read UDPv4 [ECONNREFUSED]: Connection refused (code=111)
Wed Mar 9 18:09:25 2016 read UDPv4 [ECONNREFUSED]: Connection refused (code=111)
Wed Mar 9 18:09:29 2016 read UDPv4 [ECONNREFUSED]: Connection refused (code=111)
Wed Mar 9 18:09:37 2016 read UDPv4 [ECONNREFUSED]: Connection refused (code=111)
```
Connectez-vous pour répondre

dadeTelimele sur 10 mars 2016 à 17 h 02 min

Bonsoir à tout le monde je suis là toujours pour cette erreur qui me fatigue j'aimerais vraiment votre aide après la 1ère erreur que j'ai posté au dessus, j'ai recommencé la configuration toute entière et toujours presque j'ai la même erreur dès que je test la connectivités ça ne passe pas et voila j'ai essayé plusieurs fois sans reussir je vous demande vraiment de l'aide

```
root@lap3:/etc/openvpn# openvpn /etc/openvpn/client.conf
Thu Mar 10 15:47:44 2016 OpenVPN 2.3.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH] [IPv6] built on Nov 12 2015
Thu Mar 10 15:47:44 2016 library versions: OpenSSL 1.0.1k 8 Jan 2015, LZO 2.08
Thu Mar 10 15:47:44 2016 Socket Buffers: R=[212992->131072] S=[212992->131072]
Thu Mar 10 15:47:45 2016 UDPv4 link local: [undef]
Thu Mar 10 15:47:45 2016 UDPv4 link remote: [AF_INET]92.222.92.81:1194
Thu Mar 10 15:48:45 2016 TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
Thu Mar 10 15:48:45 2016 TLS Error: TLS handshake failed
Thu Mar 10 15:48:45 2016 SIGUSR1[soft,tls-error] received, process restarting
Thu Mar 10 15:48:45 2016 Restart pause, 2 second(s)
Thu Mar 10 15:48:47 2016 Socket Buffers: R=[212992->131072] S=[212992->131072]
Thu Mar 10 15:48:47 2016 UDPv4 link local: [undef]
Thu Mar 10 15:48:47 2016 UDPv4 link remote: [AF_INET]92.222.92.81:1194
Thu Mar 10 15:49:47 2016 TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
```

NB:J'ai suivit à la lettre le tuto même le nom des machines j'avais adapté au tuto pour essayer !!

gs-demo.dedinux.com mon serveur
lap3.dedinux.com le client
Connectez-vous pour répondre

Christophe Guilloux sur 14 mars 2016 à 23 h 19 min

Le port du serveur VPN n'est peut-être pas joignable, firewall ?
Connectez-vous pour répondre

ernest random sur 15 janvier 2017 à 1 h 17 min

Grand merci pour ce tuto 🙂
Alors effectivement il faut bien mettre ses interfaces dans les commandes iptables (venet0 sur mon serveur) :

```
iptables -t nat -A POSTROUTING -o venet0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o venet0 -j MASQUERADE
```

Ensuite pour rendre persistant, j'utilise
`dpkg-reconfigure iptables-persistent`
pour éviter le bug du « /etc/init.d/netfilter-persistent save »
Connectez-vous pour répondre

xavier sur 10 avril 2017 à 10 h 36 min

Top, merci à toi Ernest.

La connexion était possible à mon VPN mais pas de trafic internet.

Et avec cette manip' it's all good !
Connectez-vous pour répondre