Subject: OpenVPN for more than One Client
Posted by imransaeed on Fri, 02 Jul 2010 09:51:41 GMT
View Forum Message <> Reply to Message

Dear All ,

Can some one tell how to configure more than one client for the VPS (VPN) and also if poosible to use VPN tunnel for other devices like ip phones and all other stuff ?

Subject: Re: OpenVPN for more than One Client
Posted by lewdfinger on Sun, 12 Dec 2010 04:59:49 GMT
View Forum Message <> Reply to Message

There's a pretty good HowTo here
http://openvpn.net/index.php/open-source/documentation/howto .html#server

Trouble is when you run the build-ca script it can't find openssl - i.e. command not found. I tried apt-get install and I get a 403 error when apt tries to download it.

Apparently I'm doing something wrong and/or openssl is not installed on the openvpn template.

I'll post back if I get it to work.
KD

Subject: Re: OpenVPN for more than One Client
Posted by staff on Sun, 12 Dec 2010 11:41:06 GMT
View Forum Message <> Reply to Message

You may need to upgrade the template first to the latest version of Debian.

Edit /etc/apt/sources.list and replace 'etch' with 'lenny'. Then run

apt-get update && apt-get dist-upgrade

Subject: Re: OpenVPN for more than One Client
Posted by lewdfinger on Sat, 18 Dec 2010 07:48:29 GMT
View Forum Message <> Reply to Message

Which I did and after some diddling around I have it working! Please let me know if you see any mistakes. I'm a little shaky on IP addressing, but it seems to work. So far I've only tested with two concurrent connections.

Note: This setup is to allow tunneling out to the internet via your VPS. It is set to route all traffic by default.

1. First thing is to upgrade to Lenny (see previous post)
2. Go to VPSVille Control Panel (Advanced) and add Tun device.
3. Generate the keys and certificates using PKI. These are command-line entries, not a script.

```
 cd /usr/share/doc/openvpn/examples/easy-rsa/2.0/

#(Edit the vars file if you like - I didn't)
. ./vars
./clean-all
./build-ca
#(I just hit return for all the prompts but entered 'server' for the server name)
./build-key-server server
./build-key client1
./build-key client2
./build-key client3
#(I used actual usernames for client1, etc)
./build-dh

#all the keys you just generated are in the 'keys' subdirectory
#make a keys directory in /etc/opnvpn and copy them all there

mkdir /etc/openvpn/keys
cd keys
cp * /etc/openvpn/keys
```

4. Copy clientx.keys, clientx.certs and ca.crt to your OpenVPN config directory on your client computer using SCP or something secure.
5. I am running two daemons, one for udp port 1129 and one tcp port 443 as a fallback if my client's LAN is firewalled. Therefore two server.conf files, and two private IP subnets.

```
nano /etc/openvpn/server_udp_1129.conf
```

```
dev tun
local xx.xx.xx.xx #insert the IP of your VPS that you want to listen on (optional)
server 172.16.10.0 255.255.255.0
# Use this if you have an OpenDNS account and Windows clients for DNS
# push "dhcp-option DNS 208.67.222.222"
keepalive 10 60
proto udp
port 1129
user nobody
group nogroup
persist-tun
persist-key
comp-lzo
verb 3
key /etc/openvpn/keys/server.key
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server.crt
dh /etc/openvpn/keys/dh1024.pem
```

```
nano /etc/openvpn/server_tcp_443.conf
```

```
dev tun
local xx.xx.xx.xx #(Listen IP of your VPS)
server 172.16.11.0 255.255.255.0 #different subnet
# Use this if you have an OpenDNS account and Windows clients for DNS
# push "dhcp-option DNS 208.67.222.222"
keepalive 10 60
proto tcp-server
port 443
user nobody
group nogroup
persist-tun
persist-key
comp-lzo
verb 3
key /etc/openvpn/keys/server.key
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server.crt
dh /etc/openvpn/keys/dh1024.pem
```

6. Edit /etc/rc.local to allow postrouting from the private IP's

nano /etc/rc.local #(the last line is the important one)

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

#
# VPSVille OpenVPN template.
#

#
# DNAT (services redir)
# Uncomment to forward port 80 to your VPN client machine
#
#iptables -t nat -A PREROUTING -p tcp --dport 80 -i venet0 -j DNAT --to 172.16.10.2:80

#
# NAT (masq for vpn)
# Uncomment and change xx.xx.xx.xx to your servers IP if you wish to tunnel all traffic
#
iptables -t nat -A POSTROUTING -s 172.16.10.0/23 -o venet0 -j SNAT --to xx.xx.xx.xx #(insert your VPS's public IP address)

exit 0
```

7. Reboot - your machine should be ready

8. Fire up a text editor and make a file 'YourConnection.ovpn' and put it in your client's openVPN config folder with the keys.

```
dev tun
client 172.16.0.0 255.255.0.0

# Try UDP first
<connection>
remote xx.xx.xx.xx 1129 udp #(insert your VPS IP here)
</connection>

# use TCP if unsuccessful
<connection>
remote xx.xx.xx.xx 443 tcp #(insert your VPS IP here)
</connection>

# comment the line below if you don't want all traffic routed
redirect-gateway def1
keepalive 10 60
persist-tun
persist-key
comp-lzo
verb 3

# These are the client keys and the ca certificate you copied from the server
ca ca.crt
cert clientx.crt
key clientx.key
```

9. Try connecting with OpenVPN your client. Make sure your client's firewall allows outgoing connections on 1129 (or whatever port your pick) and 443.
10. Set up a firewall on your server - I haven't done that yet but there's a good example in /usr/share/doc/openvpn/examples/sample-config-files/firewall .sh - and secure your server (disable root login, change ssh port, enable shared keys, etc).
11. If you get an error about unusable packets during the TLS handshake (can't remember the exact error) you may have to synchronize your server's time zone setting with your client's. My server is two time zones away so I used the dpkg-reconfigure tzdata command on my server to match where I live - worked great.

Peace be with you

Lewd

"Freedom of Speech: Priceless. For everything else there's MasterCard"

Subject: Re: OpenVPN for more than One Client
Posted by staff on Tue, 21 Dec 2010 06:59:48 GMT
View Forum Message <> Reply to Message

Fantastic, thank you lewdfinger!

Subject: Re: OpenVPN for more than One Client
Posted by lewdfinger on Tue, 21 Dec 2010 21:34:47 GMT
View Forum Message <> Reply to Message

Other things I have learned:

1. You need to specify DNS, otherwise you can connect to your server and go to any IP but domain names don't resolve. I created an OpenDNS account, added my server's IP address as a network in my OpenDNS control panel, and added the line:

push "dhcp-option DNS 208.67.222.222"

to both server config files. (I think Google's public DNS 8.8.8.8 would work as well)

Everything worked great at home behind my Smoothwall without this option, but out in the wild I had no DNS.

I think the 'push' option works with Windows clients only. You may have to set up MacOS and Linux clients with DNS independently.

2. The Windows OpenVPN GUI from openvpn.se doesn't work with these client config files. Only the one from openvpn.net.

Lewd