How to Setup and Configure an OpenVPN Server on Debian 6

8

Posted May 3, 2013 160.3k VPN DEBIAN

Getting Started

You will need to open an SSH connection on your cloud server as the root user or an SSH connection to a user with sudo access. This guide assumes a user with sudo access. However you can set things up using root just by stripping the 'sudo' from the start of each command. If your system is running on Linux or Mac, you can use SSH with the Terminal program. If you are using Windows, you can use SSH with PuTTY. Once you have the Terminal opened, assuming you're using a Linux/Mac system, you can login by typing the following command:

```
ssh username@ipaddress
```

Enter the password when you're asked to, and you're ready to start setting up OpenVPN.

Install OpenVPN and generate necessary files

Before we start installing OpenVPN and its prerequisites, we should make sure all of the packages on our system are up to date. We can do that with the following command:

```
sudo apt-get update
```

This should have apt, Debian's package manager. Download all the updates for any packages that have them.

```
sudo apt-get upgrade
```

After our system has downloaded all its updates, we can finally install OpenVPN.

```
sudo apt-get install openvpn udev
```

Once the installation is done, you are ready to begin configuring OpenVPN. To begin, you should copy all the files for encryption from their default directory into the directory they should be in for the cloud server to read them.

```
sudo cp -r /usr/share/doc/openvpn/examples/easy-rsa /etc/openvpn
```

Now that you've done that, you can begin generating the RSA algorithm files for your VPN. You will be asked to provide various values when you're generating these keys. You can set these to whatever you would like to, but bear in mind that they will be included in the certificates you generate.
To begin, access into the following directory:

```
cd /etc/openvpn/easy-rsa/2.0/
```

Then generate the RSA files:

```
source ./vars

sudo ./clean-all

sudo ./build-ca
```

After the certificate is generated, you can make the private key for the server. To do this, type the following command, and change 'server' to what you'd like the name of your OpenVPN server to be. This script will also ask you for information.

```
sudo . /etc/openvpn/easy-rsa/2.0/build-key-server server
```

Generate the Diffie Hellman key exchange parameters.

```
sudo . /etc/openvpn/easy-rsa/2.0/build-dh
```

Now generate the keys for each client this installation of OpenVPN will host. You should do this step for each client this installation will host, making sure each client's key identifier is unique.

```
sudo . /etc/openvpn/easy-rsa/2.0/build-key client
```

Move the files for the server certificates and keys to the /etc/openvpn directory now. Replace server.crt and server.key with the file names that you used.

```
sudo cp /etc/openvpn/easy-rsa/2.0/keys/ca.crt /etc/openvpn

sudo cp /etc/openvpn/easy-rsa/2.0/keys/ca.key /etc/openvpn

sudo cp /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem /etc/openvpn
sudo cp /etc/openvpn/easy-rsa/2.0/keys/server.crt /etc/openvpn
sudo cp /etc/openvpn/easy-rsa/2.0/keys/server.key /etc/openvpn
```

If you need to remove someone's access to the VPN, just send the following two commands. Replacing 'client' with the name of the client to be removed.

```
sudo . /etc/openvpn/easy-rsa/2.0/vars
sudo . /etc/openvpn/easy-rsa/2.0/revoke-full client1
```

Configure OpenVPN

Now that you have generated the files for our configuration, you can go ahead and configure your OpenVPN server and client. To retrieve the files, execute the following commands:

```
sudo gunzip -d /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz

sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf /etc/openvpn

sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/
cd
```

You should modify the client configuration file to match what you'd like it to do. You can also modify several values in the following file to match what you'd like. In order to do this, you first change the 'remote' option so it can connect to your cloud server's IP address on whichever port you configured your OpenVPN to run on. Then change the 'cert' and 'key' values to reflect the names of your own certificate and key. After these values have been edited you can save the file by typing in Ctrl+X, type 'y', then hit Enter.
Now copy the client configuration file, along with the client keys and certificates located in /etc/openvpn/easy-rsa/2.0/keys to the local machines of the clients.

```
nano ~/client.conf
```

After you've done this, you just need to make a few changes to your server configuration file before we finalize. Change the files that the 'cert' and 'key' options point to in the following file to match the certificate and key that your server is using.

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

After that's finished, you're ready to go! Just restart OpenVPN and you've got a working OpenVPN installation on Debian 6!

```
sudo /etc/init.d/openvpn restart
```

Upvote (8) Subscribe Share

Related Tutorials

How To Create a Point-To-Point VPN with WireGuard on Ubuntu 16.04

How To Run a Secure MongoDB Server with OpenVPN and Docker on Ubuntu 16.04

How to Set Up an IKEv2 VPN Server with StrongSwan on Ubuntu 16.04

Technical Recommendations and Best Practices for DigitalOcean's Tutorials

How To Encrypt Traffic to Redis with PeerVPN on Ubuntu 16.04

33 Comments

Leave a comment...

Log In to Comment

filipe *May 21, 2013*

0 Is this the same to install in a Ubuntu box? I've been stuck when generating the RSA files.

grep: /etc/openvpn/easy-rsa/2.0/openssl.cnf: No such file or directory
pkitool: KEY_CONFIG (set by the ./vars script) is pointing to the wrong
version of openssl.cnf: /etc/openvpn/easy-rsa/2.0/openssl.cnf
The correct version should have a comment that says: easy-rsa version 2.x

p.h.i.l *June 11, 2013*

0 Filipe Kiss: the directory in ubuntu is /etc/openvpn/easy-rsa2/

p.h.i.l *June 11, 2013*

0 sorry I think I got that wrong.

p.h.i.l *June 11, 2013*

0 ./vars permission denied

tried it both on Ubuntu 12.04LTS x64 and Debian 7 x64

p.h.i.l *June 11, 2013*

0 damn.. I was trying to make vars executable using "-x" instead of "+x", in any case it should be added to the tutorial.

rsmvdl *June 19, 2013*

0 Thats Trash!

kamaln7 MOD *June 22, 2013*

0 @Robin: Is there anything I can help you with?

DigitalOcean105256 *June 24, 2013*

0 I got stuck in sudo ./vars it says sudo: vars: command not found

do167763 *June 25, 2013*

0 you '. vars' or 'source ./vars'.

it just loads variables into the environment, it doesn't actually execute anything, per se.

dragan *June 25, 2013*

0

Before the configuration, don't forget to install the pkcs15-tool include in opensc library with this command:
apt-get install opensc
And edit the file ./vars with your correct informations.

dragan *June 26, 2013*

0 And create the keys folder ...

dragan *June 26, 2013*

0 If you are loged as root from the folder /etc/openvpn/easy-rsa/2.0/ type the command: "source ./vars" instead of ./vars ...

kamaln7 **MOD** *June 26, 2013*

0 @DigitalOcean please see @do's @dragan's comments.

as *August 10, 2013*

0 I don't know why this tutorial has so many bugs. Could you please fix it ?

kamaln7 **MOD** *August 10, 2013*

0 @as: What do you mean?

mitropoulos.spiros.1994 *August 12, 2013*

0 In order to work and with dns you must install dnsmasq. Also need some iptable rules..Post and that part

erik.hennerfors *September 13, 2013*

0 *@*:/etc/openvpn/easy-rsa/2.0# source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/2.0/keys

why?

kamaln7 **MOD** *September 13, 2013*

0 @erik.hennerfors: It's not an error -- it's just warning you that if you run ./clean_all it will delete everything in the keys directory.

ozgur293184 *December 7, 2013*

0 how about the firewall rules ?

core.hor *January 23, 2014*

0 Yup, what about firewall rules? I configured all as described. I can connect to my server without troubles. But internet doesn't work - i need some forward rule for iptables.

Load More Comments