Meet OpenVPN

Dec 15, 2004 By Hans-Cees Speel (/user/801008)

in

Connecting road warriors with a full-blown open-source VPN solution.

If your company has people on the road, such as sales or technical people, a VPN is a good method for letting them access data on the company network. Many different VPN solutions can be bought, but many are free. Here, I discuss only solutions you can set up without buying a commercial VPN product.

The main VPN solution used for more complex tasks is IPsec; some people use PPTP. Although PPTP is usable, **security flaws** (http://www.schneier.com/pptp.html) have occurred in its past, and it simply does not match up to IPsec.

IPsec in tunnel mode would be a much better solution, were it not for the crippled Windows-client implementation: Windows XP/2000 clients can't use IPsec in tunnel mode without using L2TP. There is nothing wrong with L2TP security-wise, but it increases latency--through the need for both PPP and L2TP processes--and increases packet-overhead, slowing down connections. Open-source servers have not had much experience with L2TP yet, so using open source for it is problematic at this time.

A disadvantage of plain IPsec is its notorious complexity: many, many things can and do go wrong. To the rescue, then, comes **OpenVPN** (http://openvpn.net/), a full-blown open-source VPN solution based on SSL. OpenVPN offers the same functionality as IPsec in tunnel mode; you can tunnel entire networks through it. In this article, I focus on using OpenVPN as a road warrior's VPN solution.

Every VPN approach has its list of pros and cons. The pros of OpenVPN are:

- Same functionality as IPsec in tunnel mode: you can tunnel entire networks (IP tunnel or bridging tunnel).
- A Windows XP/2000 install.exe file with a GUI is available for starting the tunnel. The config files are text based.
- The OpenVPN server can push routes, DNS server IP addresses and other configuration details to the clients. This makes OpenVPN well suited for road-warrior setups, because you can modify the setup without touching far-away laptops.
- You can use a bridging or routing setup.
- The server/client code is the same: the config determines the role.
- SSL is as solidly proven as security protocols get, using RSA public key cryptography if you want. See **this paper** (http://www.sans.org/rr/whitepapers/vpns/1459.php) for more information on its security setup.
- OpenVPN costs you nothing in terms of money--a server, an Internet connection and know-how is all you need).
- Plenty of **man page** (http://openvpn.net/man.html) and **HOWTOs** (http://openvpn.net) are available to get you going.
- All encryption processes are handled in userland, meaning it is easy to install--much less complicated than IPsec.

The list of cons includes:

- The setup uses TUN/TAP devices. This can make things complicated to figure out when things go wrong. If Microsoft changes its code, it also might just break.
- The OpenVPN process is executed in userland and, thus, is relatively slow. TUN/TAP devices combine together with a userland-process to create a setup in which traffic has to cross userland/kernel borders relatively often. This setup might create rather high latency on connections.
- A packet overhead is present because IP/Ethernet is encapsulated in SSL and SSL in UDP/TCP.
- The latest version OpenVPN is beta; earlier versions have further drawbacks.
- Who can you call when things go wrong? Some companies want to pay to get support.

Considering these arguments, OpenVPN should be a serious option if you are setting up a VPN. The days when only money could get you a decent VPN definitely are over.

Setting Up an OpenVPN (Routing) Scenario

The rest of this article is a guide to setting up a road-warrior scenario using routing, not bridging, with TUN devices. Its aim is to make sure laptops on the Internet can connect safely to companies' networks, using internal servers and data.

The basic HOWTO I drew on when writing this article can be found **here** (http://sme.swerts-knudsen.dk/index.html?frame=http%3A//sme.swerts-knudsen.dk/howtos/howto_30.htm). It is a HOWTO for setting up OpenVPN in bridging mode on a Linux **SME-server** (http://contribs.org/). My setup is slightly different, because I do not use a bridging setup. Another good source is the **OpenVPN HOWTO** (http://openvpn.net/howto.html).

The Security Setup

Anyone setting up a VPN without considering the different kinds of security risks one faces is a fool. Therefore, you should start any VPN setup doing exactly that--considering security.

Connection Security

OpenVPN traffic flowing over the Internet is protected by **TLS** (http://www.ietf.org/rfc/rfc2246.txt). The setup here uses public key exchange; computer authentication is done by RSA-based public/private key-pairs (public keys also are called certificates). In this setup we make our own root certificate; that is, for our VPN scheme, we are our own Verisign, so to speak. We are the root of the Web of trust here. We make a server key pair and multiple client-key pairs. We sign those with our own root certificate. This setup is this basic cryptography design of OpenVPN.

The SSL/TLS connection is set up up with those keys. After authentication is done, **Diffie-Hellmann encryption** (http://www.rsasecurity.com/rsalabs/node.asp?id=2248) is used to exchange keys to set up the connection. New keys are negotiated every hour using perfect forward secrecy, or PFS--the next key used is not derived by using the former key. By default, the connection uses 128-bit Blowfish in Cipher Block Chaining mode, with SHA1 message digests.

Server Security

The OpenVPN server itself, of course, could be attacked. You can minimize that risk by:

- Using shared keys with the `tls-auth` option before public key exchange occurs. Doing so keeps people from exploiting the SSL setup, should this be possible.
- Setting options `user nobody` and `group nobody`. This makes sure the server does not run as root. You also can use a chroot-jail.
- Using a separate box in a DMZ. This way a successful hack is slowed down by the firewall protecting the internal network from the DMZ. Strange connects can be noticed in the firewall logging.
- By using iptables firewall rules on the OpenVPN server that prevent traffic from tunnel hosts entering the server, as well as all traffic from the Internet except for the need UDP

traffic.

Authentication of Users

The security setup of your client laptops is critical. If your road warriors are using laptops and can access your company's network, your data may become public in the future. No matter how good the SSL crypto, this is a separate risk. If a laptop can connect through an OpenVPN tunnel directly into your networks, you have a problem. To avoid this, you need to establish authentication of the user to the laptop or to the SSL keys.

Many ways exist to do this authentication. You can password-protect the SSL keys of the client, which is recommended. But if workers have the habit of writing down passwords near their laptops, password protection is not sufficient. An option is to get USB-based iKeys with a pincode that holds the client keys. Pincodes are easier to remember, so the need to write them down is smaller. Of course, the iKey should be carried on a keychain and not with the laptop itself. You should establish an AUP (acceptable user policy) to make sure all users understand this. Doing so may prevent a stolen laptop from becoming a disaster. In addition, you might use encrypted filesystems on laptops.

Another option is to set up your own custom authentication scheme. For instance, you can use strong authentication with hardware tokens, coupled with a Kerberos server. OpenVPN has the script hooks to do that. You also can use the server password file.

Network Setup

The network setup my configuration files is aiming for is this:

- The OpenVPN server at 65.66.45.x.
- The client is somewhere on the Internet.
- The client/server P2P network is 192.168.100.0/24 or, rather, a /32 network in that network.
- The company-network behind the OpenVPN server is 172.16.1.0/24.

So, the internal mailserver of this company might be at 172.16.1.3, the DC at 172.16.1.5 and the fileserver at 172.16.1.6. Schematically, this setup looks like this:

```
CLIENT -> [modem/adsl-router] -> Internet <-UDP-> OpenVPNserver
CLIENT - TUNInterFace <=tunnel=> TUNInterFace ==> Internal network
CLIENT - 192.168.100.6 <========> 192.168.100.5 <==> 172.16.1.0
```

I am using a **Linux SME-server** (http://www.contribs.org), which basically is a Red Hat system stripped down to what a file/printer/firewall/e-mail server needs, with a Perl/HTTP-based config panel. After being a problematic open-source project for a while, Linux SME-server is being developed further by Lycoris. I have used Linux SME-server for years and will migrate only if forced to--it is extremely easy to use.

Comments

Comment viewing options

Threaded list - expanded ▼ | Date - newest first ▼ | 50 comments per page ▼ | Save settings

Select your preferred way to display the comments and click "Save settings" to activate your changes.

Latest OpenVPN release has many new features (/article/7949#comment-359264)
Submitted by Mark Colred (http://www.ivpn.net) (not verified) on Tue, 11/16/2010 - 08:15.

The latest 2.1.4 release just came out about 1 week ago and has support for many new features. IP version 6 support is now available as part of the TUN driver. Random port binding is also now avalable using the --lport 0 parameter. We upgraded last week and had no issues.

I use open VPN from ibVPN I (/article/7949#comment-358241)
Submitted by Anelly (not verified) on Tue, 11/02/2010 - 08:05.

I use open VPN from ibVPN (http://www.ibvpn.com)
I think open VPN is faster and more secure then PPTP.

OpenVPN-AS (/article/7949#comment-356464)
Submitted by marky (not verified) on Fri, 10/01/2010 - 03:31.

Any possible thing to login on default administrator account password for open vpn web base instead of using our root user and password?
because I encounter a problem in during log-in on web based admin access on openvpn https://15.15.20.1:943/admin (https://15.15.20.1:943/admin) when it required to type username and password and that would be my root as my username and {password} as my password in root but it keeps saying "Invalid Login" for some couple of times i keep re-typing my correct root password but it still keep saying "Invalid Login", and i try to uninstall the openvpn rpm package and reinstalled it back to my linux server....after rpm package installed and trying to login in web base admin and typing root as user and {password} for my root password but still got the same problem?

Questions:

1. Is their a default administrator account andd password for openvpn to use for web admin login?
2. How to add username and password account in open vpn?

A comparison of advantages of (/article/7949#comment-356055)
Submitted by KeepNetOpen (not verified) on Mon, 09/20/2010 - 17:28.

A comparison of advantages of OpenVPN to L2TP over IPSec would be a great article. I use VyprVPN and they just rolled out L2TP as a third protocol.
https://www.goldenfrog.com/vyprvpn/vpn-service-provider (https://www.goldenfrog.com/vyprvpn/vpn-service-provider)

L2TP seems to have some of the advantages of OpenVPN, but you can use it on more devices, like your iPhone.

Open VPN (/article/7949#comment-353933)
Submitted by SuperVPN (http://www.supervpn.net/) (not verified) on Mon, 07/19/2010 - 18:50.

Open VPN is great free software which allow you incredible 2048 bits encryption. I tried many vpn software's but this one is the best so far.

I need help (/article/7949#comment-346759)
Submitted by Joe Graham (http://www.practicall.com) (not verified) on Fri, 12/25/2009 - 10:12.

I can't get by client software to connect on the local LAN. I have stopped iptables (just in case there was port blocking) and restarted the network service, but still no luck. I can't get to the web login either (port 7505). Here is the log file from my failed login attempt (I'll post later)

Thanks in advance for your help

Server log (/article/7949#comment-346760)
Submitted by Joe Graham (http://www.practicall.com) (not verified) on Fri, 12/25/2009 - 10:16.

2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 MULTI: multi_create_instance called'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Re-using SSL/TLS context'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 LZO compression

```
initialized'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Control Channel
MTU parms [ L:1544 D:168 EF:68 EB:0 ET:0 EL:0 ]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Data Channel MTU
parms [ L:1544 D:1350 EF:44 EB:135 ET:0 EL:0 AF:3/1 ]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Local Options hash
(VER=V4): 'bd577cd1"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Expected Remote
Options hash (VER=V4): 'ee93268d"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP connection
established with 192.168.1.104:53098'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket Buffers: R=
[131072->131072] S=[131072->131072]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket flags:
TCP_NODELAY=1 succeeded'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER
link local: [undef]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER
link remote: 192.168.1.104:53098'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009
192.168.1.104:53098 Non-OpenVPN client protocol detected'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009
192.168.1.104:53098 SIGTERM[soft,port-share-redirect] received, client-instance exiting'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP/UDP: Closing
socket'
2009-12-25 10:59:40-0500 [-] WEB-PP OUT: '2009-12-25 10:59:40-0500
[pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '127.0.0.1', 45843)'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 MULTI:
multi_create_instance called'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Re-using SSL/TLS
context'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 LZO compression
initialized'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Control Channel
MTU parms [ L:1544 D:168 EF:68 EB:0 ET:0 EL:0 ]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Data Channel MTU
parms [ L:1544 D:1350 EF:44 EB:135 ET:0 EL:0 AF:3/1 ]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Local Options hash
(VER=V4): 'bd577cd1"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Expected Remote
Options hash (VER=V4): 'ee93268d"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP connection
established with 192.168.1.104:53099'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket Buffers: R=
[131072->131072] S=[131072->131072]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket flags:
TCP_NODELAY=1 succeeded'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER
link local: [undef]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER
link remote: 192.168.1.104:53099'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009
192.168.1.104:53099 Non-OpenVPN client protocol detected'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009
192.168.1.104:53099 SIGTERM[soft,port-share-redirect] received, client-instance exiting'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP/UDP: Closing
socket'
2009-12-25 10:59:40-0500 [-] WEB-PP OUT: '2009-12-25 10:59:40-0500
[pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '127.0.0.1', 45844)'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 MULTI:
multi_create_instance called'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Re-using SSL/TLS
context'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 LZO compression
initialized'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Control Channel
MTU parms [ L:1544 D:168 EF:68 EB:0 ET:0 EL:0 ]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Data Channel MTU
parms [ L:1544 D:1350 EF:44 EB:135 ET:0 EL:0 AF:3/1 ]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Local Options hash
(VER=V4): 'bd577cd1"
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Expected Remote
Options hash (VER=V4): 'ee93268d"
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCP connection
established with 192.168.1.104:53100'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Socket Buffers: R=
[131072->131072] S=[131072->131072]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Socket flags:
TCP_NODELAY=1 succeeded'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCPv4_SERVER
link local: [undef]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCPv4_SERVER
```

link remote: 192.168.1.104:53100'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009
192.168.1.104:53100 Non-OpenVPN client protocol detected'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009
192.168.1.104:53100 SIGTERM[soft,port-share-redirect] received, client-instance exiting'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCP/UDP: Closing socket'
2009-12-25 10:59:43-0500 [-] WEB-PP OUT: '2009-12-25 10:59:43-0500 [pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '127.0.0.1', 45845)'
2009-12-25 10:59:48-0500 [-] WEB-PP OUT: '2009-12-25 10:59:48-0500 [pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '192.168.1.104', 56876)'
2009-12-25 10:59:48-0500 [-] WEB-PP OUT: '2009-12-25 10:59:48-0500 [pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '192.168.1.104', 56877)'
2009-12-25 10:59:51-0500 [-] WEB-PP OUT: '2009-12-25 10:59:51-0500 [pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '192.168.1.104', 56878)'

NeoRouter - the zero-config VPN solution (/article/7949#comment-332012)
Submitted by Anonymous (not verified) on Thu, 01/22/2009 - 13:28.

I found a better VPN solution - NeoRouter (www.neorouter.com (http://www.neorouter.com)). It's much simpler to setup than OpenVPN and does better job than OpenVPN. It can create unlimited nodes in a virtual network and it uses P2P technology as well. It support not only Linux, Window, but also router firmwares like OpenWrt and Tomato.

Highly suggest GUI version of OpenVPN (/article/7949#comment-317256)
Submitted by Anonymous (http://www.strongvpn.com) (not verified) on Sat, 02/16/2008 - 13:53.

I love OpenVPN, with my VPN provider http://www.strongvpn.com (http://www.strongvpn.com) they offered it to me since the regular VPN account they sold me the port was blocked. I installed the non GUI version of OpenVPN and I didn't like the way it would disconnect when I closed the window. The lastest GUI window one is sweet, and makes it easy to reconnect. I went to Openvpn.net and made a donation, please help the developers improve it!

I think anonymous vpn, i (/article/7949#comment-316445)
Submitted by anonymous vpn (http://vpnprivacy.com) (not verified) on Thu, 02/14/2008 - 06:24.

I think **anonymous vpn** (http://vpnprivacy.com) , i mean pptp vpn, is simply for regular user then openvpn setup for **anonymous surfing** (http://vpnprivacy.com) .

This article doesn't (/article/7949#comment-271378)
Submitted by smartcgi (not verified) on Fri, 07/27/2007 - 03:35.

This article doesn't describe one problem. Sometimes DHCP is disabled on PC and OpenVPN fails to get IP.

You'll see "Requesting IP address" running constantly on this OpenVPN connection.

Solution was taken from http://av5.com/docs/running_openvpn_client_on_windows_xp.html (http://av5.com/docs/running_openvpn_client_on_windows_xp.html) and shown below:

open "Control Panel / Administrative Tools / Services", make sure that the "DHCP Client Service" is started.

This is Linux Journal (/article/7949#comment-135946)
Submitted by Anonymous (not verified) on Sat, 04/15/2006 - 12:00.

This is Linux Journal, there's no mention of a linux side GUI client or how to set this up on a Linux client side.
Do you expect me to read something and then use a command line?

Linux GUI (/article/7949#comment-193937)
Submitted by Anonymous (not verified) on Mon, 11/06/2006 - 22:30.

haha right. its about setting up a server, reinstall windows and go home to mommy.

openvpn ikey (/article/7949#comment-15331)
Submitted by D. rodic (not verified) on Mon, 02/14/2005 - 14:32.

How do i setup an OpenVPN connection using smartcard (ikey) features?

Openvpn as a way to secure domain logins over internet (/article/7949#comment-14565)
Submitted by Anonymous (http://www.ctg.albany.edu) (not verified) on Wed, 12/22/2004 - 14:17.

I'm interested in openvpn as a service on a win2k/xp client machine. I would like the vpn to connect before/during the user trying to login to a windows domain account while traveling(their domain login's are not cached).
Is this a capability of openvpn ? Any resouces you can point me at ?
Thanks

Yes, There are many sources (/article/7949#comment-334155)
Submitted by Hank Freid (not verified) on Wed, 03/04/2009 - 13:41.

Yes, There are many sources from where you can use this openvpn, also many certifications available for this at TestKing (http://www.testkingsite.com) and VCP-310 (http://www.testkingsite.com/vmware/vcp-310.html) .

the howto mentioned above: h (/article/7949#comment-14574)
Submitted by Anonymous (not verified) on Thu, 12/23/2004 - 13:40.

the howto mentioned above:
http://sme.swerts-knudsen.dk/index.html?frame=http%3A//sme.swerts-knudse... (http://sme.swerts-knudsen.dk/index.html?frame=http%3A//sme.swerts-knudsen.dk/howtos/howto_30.htm).
does something like that. But I am not sure what you mean exactly. The vpn is a service under windows.

Cool Article (/article/7949#comment-14536)
Submitted by Freak (http://www.openvpn-forum.de) (not verified) on Sun, 12/19/2004 - 15:36.

Thanks for a cool article!
Discussion about OpenVPN @ OpenVPN-Forum.de (http://www.openvpn-forum.de)

Web layout (/article/7949#comment-14515)
Submitted by Anonymous (not verified) on Thu, 12/16/2004 - 16:35.

On my browser and monitor (Firefox, all defaults) the first line of this story is 141 characters.

People read text best at a width of 40-60 characters.

Even if you don't have to horizontal scroll, this layout is ridiculously hard to read.

The article was excellent - w (/article/7949#comment-14569)
Submitted by Anonymous (not verified) on Wed, 12/22/2004 - 20:47.

The article was excellent - why don't you chill with your comment on web settings?

Wow! What's this business (/article/7949#comment-14634)
Submitted by Anonymous (not verified) on Fri, 12/31/2004 - 19:07.

Wow!

What's this business with "why don't you chill with your comment on web settings?"?

Are you referring to the comments about line width? Man, that kind of stuff needs to be fixed--it's just a royal pain trying to read articles like that.

For RoadWarrior there's a goo (/article/7949#comment-14513)
Submitted by Anonymous (not verified) on Thu, 12/16/2004 - 13:07.

For RoadWarrior there's a good option you put in clients. It's the redirect-gateway option.

```
# man openvpn
...
--redirect-gateway
Automatically execute routing commands to cause all outgoing
IP traffic to be redirected over the VPN. Currently imple-
mented only on Linux and Windows.
This option performs three steps:
(1) Create a static route for the --remote address which for-
wards to the pre-existing default gateway. This is done so
that (3) will not create a routing loop.
(2) Delete the default gateway route.
(3) Set the new default gateway to be the VPN endpoint address
```

```
(derived either from --route-gateway or the second parameter
to --ifconfig when --dev tun is specified).
When the tunnel is torn down, all of the above steps are re-
versed so that the original default route is restored.
...
```

How well does this scale for multiple road-warriors? (/article/7949#comment-14509)
Submitted by SwedishChef (not verified) on Thu, 12/16/2004 - 09:48.

Thanks for your excellent article. It's always a pleasure to see something that is well documented and complete. However, I have a question about scaling clients that wasn't covered in the article.

I have implemented openVPN for a local organization that has offices in other nearby towns. Each office has access to bandwidth; one via DSL and the other via FTTH (fiber-to-the-home). I configured two separate openVPN servers on the home office router because I couldn't see - from the documentation - whether one openVPN server can monitor two ports; and two separate connections. So I built one server to watch port 5000 and another to watch port 5001 and used shared keys. The other end of both networks is another Linux box that is an openVPN client routing the entire complement of machines in to the home office. Interestingly enough, both client machines are behind a NAT router yet both connect to the VPN well. The openVPN server is the router/firewall (Shorewall) at the central office. Routing to the Internet is accomplished through a separate firewall in both cases.

So I guess my main question is: "How would two (or more) road warriors access your VPN?" I notice that you have a range of IP addresses in the server config file. Does this work for multiple remote clients?

I might add that I have also configured open-VPN in bridging mode for a client who had an IPX network running across a T-1 routed by two Livingston routers. This was all implemented on an old Novel 3x system that the client was reluctant to change but the $700-per-month T-1 costs were killing him. He had a FTTH connection at his main office and connected a DSL connection to his remote office. I installed two Linux boxes running openVPN in bridging mode; one client on the DSL and the one server at the other end on the fiber. The latency was incredible! IPX apparently broadcasts so much packet traffic that the DSL link was buried under it. However, even when we implemented a TCP Novell system as a test, the DSL was not capable of handling the traffic (although DSL in that same town does handle the SMB traffic of the network I described earlier). We ended up using a wireless connection to a location in the remote town that did have FTTH and then simply creating a VLAN to route traffic back to the home office. So the availability of bandwidth for some protocols is critical.

OpenVPN 2.0, which is in beta (/article/7949#comment-14510)
Submitted by Anonymous (not verified) on Thu, 12/16/2004 - 10:39.

OpenVPN 2.0, which is in beta does not require a separate port for each connection such as the 1.x branch did. The article above is specific to 2.0 and only requires port 1194 for multiple remote connections.

Thanks for such a well-writte (/article/7949#comment-14498)
Submitted by Anonymous (not verified) on Wed, 12/15/2004 - 07:57.

Thanks for such a well-written article!

One problem though: in the server config file, you have two route-up lines. The route-up lines are not stackable, i.e. the second will wipe out the first. Why not just use the "route" option?

In my setup a wring route app (/article/7949#comment-14526)
Submitted by hanscees (not verified) on Fri, 12/17/2004 - 14:01.

In my setup a wring route appeared automagically. The first line deltes that.

vpen in ubuntu festy 7.04 (/article/7949#comment-251857)
Submitted by krax (not verified) on Sun, 06/03/2007 - 01:02.

hello masters
great deaads have encountered to set a vpn connection to INERNET with UBUNTU desktop ver 7.04 festy but any result was out-come.
plz help me t set up this vpn on debian base genome UBUNTU festy 7.04
Email me at kraxadmin[@]gmail.com
waiting with possible awaite
bon rester
thatnks

Meet OpenVPN

Dec 15, 2004 By Hans-Cees Speel (/user/801008)

in

Connecting road warriors with a full-blown open-source VPN solution.

OpenVPN Server Install

Installing OpenVPN is easy to do. On the Linux server side, you must install one or two RPMs. On SME these RPMs are lzo.xxx.rpm and openvpn-2.0_beta17-1.i386.rpm. Most systems already include lzo. Your kernel should include TUN devices, most kernels do. If you run `openvpn` from /usr/sbin/openvpn, you should find a TUN device. With the settings we are going to use, it has a P2P connection.

The config file on my box is saved at /etc/openvpn/server.conf, but yours may be stored somewhere else. My server configuration file looks like the output shown below; see the **man page** (http://openvpn.net/man.html) to see what all the items reference. they mean):

```
###OpenVPN server config routing TUN setup########
port 1194
dev tun
tls-server
mode server
dh dh1024.pem
ca ca.crt
cert SERVER.crt
key SERVER.key
duplicate-cn
ifconfig 192.168.100.1 192.168.100.2
ifconfig-pool 192.168.100.5 192.168.100.200 # IP range clients
mtu-test
tun-mtu 1500
tun-mtu-extra 32
mssfix 1450
#keep tunnel open by ping
push "ping 10"
push "ping-restart 60"
ping 10
ping-restart 120
#route to be established on the server
route-up "route delete -net 192.168.100.0/24"
route-up "route add -net 192.168.100.0/24 tun0"
#route to push to clients
push "route 172.16.1.0 255.255.255.0" #route to company network
push "dhcp-option DOMAIN hansceess.net"  #push the DNS domain suffix
push "dhcp-option DNS 172.16.1.7"  #push DNS entries to client
push "route 192.168.100.1" # add route to protected network
comp-lzo
status-version 2
status openvpn-status.log
verb 5
######################## end server config ##############
```

Client Install

On the Windows client side, you should download the Windows installer and run it. The normal installer is available on the **OpenVPN Web site** (http://openvpn.net), while and the GUI version can be found **here** (http://www.nilings.se/openvpn/). I recommend using the latter: it gives you a tray-icon with which you can start the OpenVPN service. In the Network connections window under Settings, you should find a tap win32 adapter. You also should see that adapter in your routing table when you type `route print` in a DOSBox.

After the setup has installed everything, you should adjust the config settings in D:/Program Files/OpenVPN/config/*.ovpn to those you want. You might want to tune your personal firewall as well, if it sees the interface at all--mine didn't. My adjusted settings file looks like this:

```
####################client.ovpn######
port 1194 #udp by default
dev tun
##remote is the openvpn-server
remote 65.66.45.x
tls-client
ca ca.crt
cert CLIENT.crt
key CLIENT.key
mtu-test
tun-mtu 1500
tun-mtu-extra 32
mssfix 1450
pull
#ip-win32 ipapi|manual|dynamic|netsh (see man page, use
#when ip address on interface does not appear, but dhcp server
#is visible in ipconfig /all)
#ip-win32 ipapi
comp-lzo
verb 4
##############################end########
```

The OpenVPN process on the client is a Windows service you can start with a script or with the GUI, if you want. The TAP device (in tun-modus) can be tcpdumped, as can any interface, which makes it nice when troubleshooting. The rest of the configuration comes from the server.

Making RSA Keys

You can make keys for OpenVPN in the same way as you would make them for OpenSSL. But for those who like comfort, OpenVPN has an easy RSA set of scripts to help you out. You first must edit some variables in the vars file for the keys: names for server/clients keys, your company name, e-mail and so on. Next, run `./build-ca` to build your root private key. Then, run `./build-key server` to build the server key pair. Build the client key(s) with `./build-key client`. In this client step, you can add a passphrase in the keys for key-authentication, as discussed above. Finally, you must run `./build-dh` to generate the Diffie-Hellmann .pem file that the server needs. This file holds a large prime number and another parameter (see **this article** (http://www.rsasecurity.com/rsalabs/node.asp?id=2248) for details). Using these numbers, the server can generate new keys quickly, which it does every hour by default for standing connections.

You also need to copy the server keys, root certificate and *.pem file to /openvpn. The client needs the client keys and the root certificate. These should be transported over a secure medium, such as winscp.

There is one thing left to do: get the firewall iptables rules on the server. The rules I added were:

```
#  internet interface eth1 let OpenVPN udp port in
    /sbin/iptables --append INPUT -p udp --dport 1194 -m state --state     |
#block anything into the server from tun interface
        /sbin/iptables --append INPUT -i tun0 -j DROP
#tun0 debugging
```

```
    #/sbin/iptables --append INPUT -i tun0 -j LOG --log-prefix     tun0-inp
        #/sbin/iptables --append OUTPUT -o tun0 -j LOG --log-prefix tun0-ou
        #/sbin/iptables --append FORWARD -i tun0 -j LOG --log-prefix Forwar
        #/sbin/iptables --append FORWARD -o tun0 -j LOG --log-prefix Forwar

#OpenVPN Forward chain: if you have a Tun-device, the forward chain
#screens traffic from networks/hosts outside the tunnel, going to
#internal networks and back. we want this traffic to go through,
#default but first we might want to block some things: remember, the
#other side of the tunnel is not safe by default: he could be routing
#so we should log syns at least coming in
        /sbin/iptables --append FORWARD -i tun0 -m state --state NEW --jump
#you should know the networks allowed in and out through the tunnel
#let client network in.
        /sbin/iptables --append FORWARD -i tun0 --source 192.168.0.0/16 -j
#let company network out
        /sbin/iptables --append FORWARD -o tun0 --source 172.16.0.0/16
 -j ACCEPT
##troubleshoot: let all through
#       /sbin/iptables --append FORWARD -i tun0 -j ACCEPT
#       /sbin/iptables --append FORWARD -o tun0 -j ACCEPT
#you might want to allow some, but not all
#       /sbin/iptables --append FORWARD -i tun0 -p tcp --dport 25 -j ACCEPT
##drop the rest
        /sbin/iptables --append FORWARD -i tun0 -j DROP
        /sbin/iptables --append FORWARD -o tun+ -j DROP
```

Comments

Comment viewing options

Threaded list - expanded ▼ | Date - newest first ▼ | 50 comments per page ▼ | Save settings

Select your preferred way to display the comments and click "Save settings" to activate your changes.

Latest OpenVPN release has many new features (/article/7949#comment-359264)

Submitted by Mark Colred (http://www.ivpn.net) (not verified) on Tue, 11/16/2010 - 08:15.

The latest 2.1.4 release just came out about 1 week ago and has support for many new features. IP version 6 support is now available as part of the TUN driver. Random port binding is also now avalable using the --lport 0 parameter. We upgraded last week and had no issues.

I use open VPN from ibVPN I (/article/7949#comment-358241)

Submitted by Anelly (not verified) on Tue, 11/02/2010 - 08:05.

I use open VPN from ibVPN (http://www.ibvpn.com)
I think open VPN is faster and more secure then PPTP.

OpenVPN-AS (/article/7949#comment-356464)
Submitted by marky (not verified) on Fri, 10/01/2010 - 03:31.

Any possible thing to login on default administrator account password for open vpn web base instead of using our root user and password?
because I encounter a problem in during log-in on web based admin access on openvpn https://15.15.20.1:943/admin (https://15.15.20.1:943/admin) when it required to type username and password and that would be my root as my username and {password} as my password in root but it keeps saying "Invalid Login" for some couple of times i keep re-typing my correct root password but it still keep saying "Invalid Login", and i try to uninstall the openvpn rpm package and reinstalled it back to my linux server....after rpm package installed and trying to login in web base admin and typing root as user and {password} for my root password but still got the same problem?

Questions:

1. Is their a default administrator account andd password for openvpn to use for web admin login?
2. How to add username and password account in open vpn?

A comparison of advantages of (/article/7949#comment-356055)
Submitted by KeepNetOpen (not verified) on Mon, 09/20/2010 - 17:28.

A comparison of advantages of OpenVPN to L2TP over IPSec would be a great article. I use VyprVPN and they just rolled out L2TP as a third protocol.
https://www.goldenfrog.com/vyprvpn/vpn-service-provider (https://www.goldenfrog.com/vyprvpn/vpn-service-provider)

L2TP seems to have some of the advantages of OpenVPN, but you can use it on more devices, like your iPhone.

Open VPN (/article/7949#comment-353933)
Submitted by SuperVPN (http://www.supervpn.net/) (not verified) on Mon, 07/19/2010 - 18:50.

Open VPN is great free software which allow you incredible 2048 bits encryption. I tried many vpn software's but this one is the best so far.

I need help (/article/7949#comment-346759)
Submitted by Joe Graham (http://www.practicall.com) (not verified) on Fri, 12/25/2009 - 10:12.

I can't get by client software to connect on the local LAN. I have stopped iptables (just in case there was port blocking) and restarted the network service, but still no luck. I can't get to the web login either (port 7505). Here is the log file from my failed login attempt (I'll post later)

Thanks in advance for your help

Server log (/article/7949#comment-346760)
Submitted by Joe Graham (http://www.practicall.com) (not verified) on Fri, 12/25/2009 - 10:16.

2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 MULTI: multi_create_instance called'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Re-using SSL/TLS context'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 LZO compression initialized'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Control Channel MTU parms [L:1544 D:168 EF:68 EB:0 ET:0 EL:0]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Data Channel MTU parms [L:1544 D:1350 EF:44 EB:135 ET:0 EL:0 AF:3/1]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Local Options hash (VER=V4): 'bd577cd1"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Expected Remote Options hash (VER=V4): 'ee93268d"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP connection established with 192.168.1.104:53098'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket Buffers: R=[131072->131072] S=[131072->131072]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket flags: TCP_NODELAY=1 succeeded'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER link local: [undef]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER link remote: 192.168.1.104:53098'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 192.168.1.104:53098 Non-OpenVPN client protocol detected'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 192.168.1.104:53098 SIGTERM[soft,port-share-redirect] received, client-instance exiting'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP/UDP: Closing

socket'
2009-12-25 10:59:40-0500 [-] WEB-PP OUT: '2009-12-25 10:59:40-0500 [pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '127.0.0.1', 45843)'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 MULTI: multi_create_instance called'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Re-using SSL/TLS context'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 LZO compression initialized'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Control Channel MTU parms [L:1544 D:168 EF:68 EB:0 ET:0 EL:0]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Data Channel MTU parms [L:1544 D:1350 EF:44 EB:135 ET:0 EL:0 AF:3/1]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Local Options hash (VER=V4): 'bd577cd1"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Expected Remote Options hash (VER=V4): 'ee93268d"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP connection established with 192.168.1.104:53099'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket Buffers: R=[131072->131072] S=[131072->131072]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket flags: TCP_NODELAY=1 succeeded'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER link local: [undef]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER link remote: 192.168.1.104:53099'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 192.168.1.104:53099 Non-OpenVPN client protocol detected'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 192.168.1.104:53099 SIGTERM[soft,port-share-redirect] received, client-instance exiting'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP/UDP: Closing socket'
2009-12-25 10:59:40-0500 [-] WEB-PP OUT: '2009-12-25 10:59:40-0500 [pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '127.0.0.1', 45844)'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 MULTI: multi_create_instance called'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Re-using SSL/TLS context'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 LZO compression initialized'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Control Channel MTU parms [L:1544 D:168 EF:68 EB:0 ET:0 EL:0]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Data Channel MTU parms [L:1544 D:1350 EF:44 EB:135 ET:0 EL:0 AF:3/1]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Local Options hash (VER=V4): 'bd577cd1"
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Expected Remote Options hash (VER=V4): 'ee93268d"
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCP connection established with 192.168.1.104:53100'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Socket Buffers: R=[131072->131072] S=[131072->131072]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Socket flags: TCP_NODELAY=1 succeeded'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCPv4_SERVER link local: [undef]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCPv4_SERVER link remote: 192.168.1.104:53100'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 192.168.1.104:53100 Non-OpenVPN client protocol detected'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 192.168.1.104:53100 SIGTERM[soft,port-share-redirect] received, client-instance exiting'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCP/UDP: Closing socket'
2009-12-25 10:59:43-0500 [-] WEB-PP OUT: '2009-12-25 10:59:43-0500 [pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '127.0.0.1', 45845)'
2009-12-25 10:59:48-0500 [-] WEB-PP OUT: '2009-12-25 10:59:48-0500 [pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '192.168.1.104', 56876)'
2009-12-25 10:59:48-0500 [-] WEB-PP OUT: '2009-12-25 10:59:48-0500 [pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '192.168.1.104', 56877)'
2009-12-25 10:59:51-0500 [-] WEB-PP OUT: '2009-12-25 10:59:51-0500 [pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '192.168.1.104', 56878)'

NeoRouter - the zero-config VPN solution (/article/7949#comment-332012)
Submitted by Anonymous (not verified) on Thu, 01/22/2009 - 13:28.

I found a better VPN solution - NeoRouter (www.neorouter.com (http://www.neorouter.com)). It's much simpler to setup than OpenVPN and does better job than OpenVPN. It can create unlimited nodes in a virtual network and it uses P2P technology as well. It support not only Linux, Window, but also router firmwares like OpenWrt and Tomato.

Highly suggest GUI version of OpenVPN (/article/7949#comment-317256)
Submitted by Anonymous (http://www.strongvpn.com) (not verified) on Sat, 02/16/2008 - 13:53.

I love OpenVPN, with my VPN provider http://www.strongvpn.com (http://www.strongvpn.com) they offered it to me since the regular VPN account they sold me the port was blocked. I installed the non GUI version of OpenVPN and I didn't like the way it would disconnect when I closed the window. The lastest GUI window one is sweet, and makes it easy to reconnect. I went to Openvpn.net and made a donation, please help the developers improve it!

I think anonymous vpn, i (/article/7949#comment-316445)
Submitted by anonymous vpn (http://vpnprivacy.com) (not verified) on Thu, 02/14/2008 - 06:24.

I think **anonymous vpn** (http://vpnprivacy.com) , i mean pptp vpn, is simply for regular user then openvpn setup for **anonymous surfing** (http://vpnprivacy.com) .

This article doesn't (/article/7949#comment-271378)
Submitted by smartcgi (not verified) on Fri, 07/27/2007 - 03:35.

This article doesn't describe one problem. Sometimes DHCP is disabled on PC and OpenVPN fails to get IP.

You'll see "Requesting IP address" running constantly on this OpenVPN connection.

Solution was taken from http://av5.com/docs/running_openvpn_client_on_windows_xp.html (http://av5.com/docs/running_openvpn_client_on_windows_xp.html) and shown below:

open "Control Panel / Administrative Tools / Services", make sure that the "DHCP Client Service" is started.

This is Linux Journal (/article/7949#comment-135946)
Submitted by Anonymous (not verified) on Sat, 04/15/2006 - 12:00.

This is Linux Journal, there's no mention of a linux side GUI client or how to set this up on a Linux client side.
Do you expect me to read something and then use a command line?

Linux GUI (/article/7949#comment-193937)
Submitted by Anonymous (not verified) on Mon, 11/06/2006 - 22:30.

haha right. its about setting up a server, reinstall windows and go home to mommy.

openvpn ikey (/article/7949#comment-15331)
Submitted by D. rodic (not verified) on Mon, 02/14/2005 - 14:32.

How do i setup an OpenVPN connection using smartcard (ikey) features?

Openvpn as a way to secure domain logins over internet (/article/7949#comment-14565)
Submitted by Anonymous (http://www.ctg.albany.edu) (not verified) on Wed, 12/22/2004 - 14:17.

I'm interested in openvpn as a service on a win2k/xp client machine. I would like the vpn to connect before/during the user trying to login to a windows domain account while traveling(their domain login's are not cached).
Is this a capability of openvpn ? Any resouces you can point me at ?
Thanks

Yes, There are many sources (/article/7949#comment-334155)
Submitted by Hank Freid (not verified) on Wed, 03/04/2009 - 13:41.

Yes, There are many sources from where you can use this openvpn, also many certifications available for this at TestKing (http://www.testkingsite.com) and VCP-310 (http://www.testkingsite.com/vmware/vcp-310.html) .

the howto mentioned above: h (/article/7949#comment-14574)
Submitted by Anonymous (not verified) on Thu, 12/23/2004 - 13:40.

the howto mentioned above:
http://sme.swerts-knudsen.dk/index.html?frame=http%3A//sme.swerts-knudse... (http://sme.swerts-knudsen.dk/index.html?frame=http%3A//sme.swerts-knudsen.dk/howtos/howto_30.htm).
does something like that. But I am not sure what you mean exactly. The vpn is a service under windows.

Cool Article (/article/7949#comment-14536)
Submitted by Freak (http://www.openvpn-forum.de) (not verified) on Sun, 12/19/2004 - 15:36.

Thanks for a cool article!
Discussion about OpenVPN @ OpenVPN-Forum.de (http://www.openvpn-forum.de)

Web layout (/article/7949#comment-14515)
Submitted by Anonymous (not verified) on Thu, 12/16/2004 - 16:35.

On my browser and monitor (Firefox, all defaults) the first line of this story is 141 characters.

People read text best at a width of 40-60 characters.

Even if you don't have to horizontal scroll, this layout is ridiculously hard to read.

The article was excellent - w (/article/7949#comment-14569)
Submitted by Anonymous (not verified) on Wed, 12/22/2004 - 20:47.

The article was excellent - why don't you chill with your comment on web settings?

Wow! What's this business (/article/7949#comment-14634)
Submitted by Anonymous (not verified) on Fri, 12/31/2004 - 19:07.

Wow!

What's this business with "why don't you chill with your comment on web settings?"?

Are you referring to the comments about line width? Man, that kind of stuff needs to be fixed--it's just a royal pain trying to read articles like that.

For RoadWarrior there's a goo (/article/7949#comment-14513)
Submitted by Anonymous (not verified) on Thu, 12/16/2004 - 13:07.

For RoadWarrior there's a good option you put in clients. It's the redirect-gateway option.

```
# man openvpn
...
--redirect-gateway
Automatically execute routing commands to cause all outgoing
IP traffic to be redirected over the VPN. Currently imple-
mented only on Linux and Windows.
This option performs three steps:
(1) Create a static route for the --remote address which for-
wards to the pre-existing default gateway. This is done so
that (3) will not create a routing loop.
(2) Delete the default gateway route.
(3) Set the new default gateway to be the VPN endpoint address
(derived either from --route-gateway or the second parameter
to --ifconfig when --dev tun is specified).
When the tunnel is torn down, all of the above steps are re-
versed so that the original default route is restored.
...
```

How well does this scale for multiple road-warriors? (/article/7949#comment-14509)
Submitted by SwedishChef (not verified) on Thu, 12/16/2004 - 09:48.

Thanks for your excellent article. It's always a pleasure to see something that is well documented and complete. However, I have a question about scaling clients that wasn't covered in the article.

I have implemented openVPN for a local organization that has offices in other nearby towns. Each office has access to bandwidth; one via DSL and the other via FTTH (fiber-to-the-home). I configured two separate openVPN servers on the home office router because I couldn't see - from the documentation - whether one openVPN server can monitor two ports; and two separate connections. So I built one server to watch port 5000 and another to watch port 5001 and used shared keys. The other end of both networks is another Linux box that is an openVPN client routing the entire complement of machines in to the home office. Interestingly enough, both client machines are behind a NAT router yet both connect to the VPN well. The openVPN server is the router/firewall (Shorewall) at the central office. Routing to the Internet is accomplished through a separate firewall in both cases.

So I guess my main question is: "How would two (or more) road warriors access your VPN?" I notice that you have a range of IP addresses in the server config file. Does this work for multiple remote clients?

I might add that I have also configured open-VPN in bridging mode for a client who had an IPX network running across a T-1 routed by two Livingston routers. This was all implemented on an old Novel 3x system that the client was reluctant to change but the $700-per-month T-1 costs were killing him. He had a FTTH connection at his main office and connected a DSL connection to his remote office. I installed two Linux boxes running openVPN in bridging mode; one client on the DSL and the one server at the other end on the fiber. The latency was incredible! IPX apparently broadcasts so much packet traffic that the DSL link was buried under it. However, even when we implemented a TCP Novell system as a test, the DSL was not capable of handling the traffic (although DSL in that same town does handle the SMB traffic of the network I described earlier). We ended up using a wireless connection to a location in the remote town that did have FTTH and then simply creating a VLAN to route traffic back to the home office. So the availability of bandwidth for some protocols is critical.

OpenVPN 2.0, which is in beta (/article/7949#comment-14510)
Submitted by Anonymous (not verified) on Thu, 12/16/2004 - 10:39.

OpenVPN 2.0, which is in beta does not require a separate port for each connection such as the 1.x branch did. The article above is specific to 2.0 and only requires port 1194 for multiple remote connections.

Thanks for such a well-writte (/article/7949#comment-14498)
Submitted by Anonymous (not verified) on Wed, 12/15/2004 - 07:57.

Thanks for such a well-written article!

One problem though: in the server config file, you have two route-up lines. The route-up lines are not stackable, i.e. the second will wipe out the first. Why not just use the "route" option?

In my setup a wring route app (/article/7949#comment-14526)
Submitted by hanscees (not verified) on Fri, 12/17/2004 - 14:01.

In my setup a wring route appeared automagically. The first line deltes that.

vpen in ubuntu festy 7.04 (/article/7949#comment-251857)
Submitted by krax (not verified) on Sun, 06/03/2007 - 01:02.

hello masters
great deaads have encountered to set a vpn connection to INERNET with UBUNTU desktop ver 7.04 festy but any result was out-come.
plz help me t set up this vpn on debian base genome UBUNTU festy 7.04
Email me at kraxadmin[@]gmail.com
waiting with possible awaite
bon rester
thatnks

Meet OpenVPN

Dec 15, 2004 By Hans-Cees Speel (/user/801008)

in

Connecting road warriors with a full-blown open-source VPN solution.

Testing

Once you have installed OpenVPN, it is time to test it. Make sure the server process is started with `service openvpn [re]start`. You should see the TUN device with ifconfig. With my config, it shows:

```
Link: encap:Point-to-Point Protocol
Inet addr:192.168.100.1 P-t-P 192.168.100.2.
```

Now, start up the client OpenVPN service. A file found at D:/Program Files/Openvpn/*.log contains debugging information. With the `verb` setting, you can elaborate the logging. When you start the client service, the icon in your tray shouts it is connected. `Ipconfig /all` in a DOSBox shows an IP address on the tap interface, for instance, 192.168.100.10

```
Ethernet adapter Local Area Connection 8:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : TAP-Win32 Adapter V8
        Physical Address. . . . . . . . . : 00-FF-CF-10-9F-A6
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.100.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.252
        Default Gateway . . . . . . . . . :
        DHCP Server . . . . . . . . . . . : 192.168.100.5
```

`print route` gives you some routes:

```
192.168.100.1  255.255.255.255    192.168.100.9              4   1
192.168.100.8  255.255.255.252   192.168.100.10              4   1
192.168.100.10  255.255.255.255    127.0.0.1       127.0.0.1      1
192.168.100.255  255.255.255.255   192.168.100.10               4
```

Although this all may look quite odd, it works. You now can ping 192.168.100.1; if that succeeds the tunnel is okay. On the server you can see the pings coming in with `tcpdump -nlpi tun0`. Also, `tail -f /var/log/messages` supplies some information.

The routes on the server look something like this (`netstat -rn`) kernel IP routing table:

```
Destination     Gateway     Genmask          Flags   MSS Window  irtt Iface
192.168.100.2   0.0.0.0     255.255.255.255  UH        0 0          0  tun0
192.168.100.0   0.0.0.0     255.255.255.0    U         0 0          0  tun0
65.66.45.2      0.0.0.0     255.255.255.0    U         0 0          0  eth1
```

```
172.16.1.0      0.0.0.0     255.255.255.0   U         0 0          0 eth0
127.0.0.0       0.0.0.0     255.0.0.0       U         0 0          0 lo
0.0.0.0         65.66.45.1  0.0.0.0         UG        0 0          0 eth1
```

If all goes well, your connection should be there. If not, check the server routing table and tcpdump the TUN interfaces. You also can use the iptables debug rules.

Conclusion

In this article I have shown a simple setup for a OpenVPN. In real life, the setup will not be much more complex. Although the security implications of any VPN should be well thought-out, setting up OpenVPN turned out to be rather easy. If you do get into trouble, plenty of helping hands can be found on the mailing lists.

OpenVPN is a serious VPN product. It can contend with IPsec in many ways. It certainly is cheap--try buying a Cisco concentrator--easy to install and, in the open-source tradition, tinkerable.

If OpenVPN has a disadvantage, it might be latency. However, no real-life data exists yet to back up that claim.

Resources

"Exchange Functionality on Linux" (http://www.linuxjournal.com/article/6734)

"VPN Implementation in Cluster Computing" (http://www.linuxjournal.com/article/6142)

Hans-Cees Speel (**hanscees@hanscees.com** (mailto:hanscees@hanscees.com)) is a security consultant for **Tunix Firewall Support** (http://www.tunix.nl/nav/frmsupport.html). He spends his spare time building a Web guide for **North European trees** (http://www.bomengids.nl/uk/hoofdsleutel.html).

Comments

Comment viewing options

Threaded list - expanded ▼ | Date - newest first ▼ | 50 comments per page ▼ | Save settings

Select your preferred way to display the comments and click "Save settings" to activate your changes.

Latest OpenVPN release has many new features (/article/7949#comment-359264)
Submitted by Mark Colred (http://www.ivpn.net) (not verified) on Tue, 11/16/2010 - 08:15.

The latest 2.1.4 release just came out about 1 week ago and has support for many new features. IP version 6 support is now available as part of the TUN driver. Random port binding is also now avalable using the --lport 0 parameter. We upgraded last week and had no issues.

I use open VPN from ibVPN I (/article/7949#comment-358241)
Submitted by Anelly (not verified) on Tue, 11/02/2010 - 08:05.

I use open VPN from ibVPN (http://www.ibvpn.com)
I think open VPN is faster and more secure then PPTP.

OpenVPN-AS (/article/7949#comment-356464)
Submitted by marky (not verified) on Fri, 10/01/2010 - 03:31.

Any possible thing to login on default administrator account password for open vpn web base instead of using our root user and password?
because I encounter a problem in during log-in on web based admin access on openvpn https://15.15.20.1:943/admin (https://15.15.20.1:943/admin) when it required to type username and password and that would be my root as my username and {password} as my password in root but it keeps saying "Invalid Login" for some couple of times i keep re-typing my correct root password but it still keep saying "Invalid Login", and i try to uninstall the openvpn rpm package and reinstalled it back to my linux server....after rpm package installed and trying to login in web base admin and typing root as user and {password} for my root password but still got the same problem?

Questions:

1. Is their a default administrator account andd password for openvpn to use for web admin login?
2. How to add username and password account in open vpn?

A comparison of advantages of (/article/7949#comment-356055)
Submitted by KeepNetOpen (not verified) on Mon, 09/20/2010 - 17:28.

A comparison of advantages of OpenVPN to L2TP over IPSec would be a great article. I use VyprVPN and they just rolled out L2TP as a third protocol.
https://www.goldenfrog.com/vyprvpn/vpn-service-provider (https://www.goldenfrog.com/vyprvpn/vpn-service-provider)

L2TP seems to have some of the advantages of OpenVPN, but you can use it on more devices, like your iPhone.

Open VPN (/article/7949#comment-353933)
Submitted by SuperVPN (http://www.supervpn.net/) (not verified) on Mon, 07/19/2010 - 18:50.

Open VPN is great free software which allow you incredible 2048 bits encryption. I tried many vpn software's but this one is the best so far.

I need help (/article/7949#comment-346759)
Submitted by Joe Graham (http://www.practicall.com) (not verified) on Fri, 12/25/2009 - 10:12.

I can't get by client software to connect on the local LAN. I have stopped iptables (just in case there was port blocking) and restarted the network service, but still no luck. I can't get to the web login either (port 7505). Here is the log file from my failed login attempt (I'll post later)

Thanks in advance for your help

Server log (/article/7949#comment-346760)
Submitted by Joe Graham (http://www.practicall.com) (not verified) on Fri, 12/25/2009 - 10:16.

2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 MULTI: multi_create_instance called'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Re-using SSL/TLS context'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 LZO compression initialized'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Control Channel MTU parms [L:1544 D:168 EF:68 EB:0 ET:0 EL:0]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Data Channel MTU parms [L:1544 D:1350 EF:44 EB:135 ET:0 EL:0 AF:3/1]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Local Options hash (VER=V4): 'bd577cd1"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Expected Remote Options hash (VER=V4): 'ee93268d"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP connection established with 192.168.1.104:53098'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket Buffers: R=[131072->131072] S=[131072->131072]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket flags: TCP_NODELAY=1 succeeded'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER link local: [undef]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER

```
link remote: 192.168.1.104:53098'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009
192.168.1.104:53098 Non-OpenVPN client protocol detected'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009
192.168.1.104:53098 SIGTERM[soft,port-share-redirect] received, client-instance exiting'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP/UDP: Closing
socket'
2009-12-25 10:59:40-0500 [-] WEB-PP OUT: '2009-12-25 10:59:40-0500
[pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '127.0.0.1', 45843)'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 MULTI:
multi_create_instance called'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Re-using SSL/TLS
context'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 LZO compression
initialized'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Control Channel
MTU parms [ L:1544 D:168 EF:68 EB:0 ET:0 EL:0 ]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Data Channel MTU
parms [ L:1544 D:1350 EF:44 EB:135 ET:0 EL:0 AF:3/1 ]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Local Options hash
(VER=V4): 'bd577cd1"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Expected Remote
Options hash (VER=V4): 'ee93268d"
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP connection
established with 192.168.1.104:53099'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket Buffers: R=
[131072->131072] S=[131072->131072]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 Socket flags:
TCP_NODELAY=1 succeeded'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER
link local: [undef]'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCPv4_SERVER
link remote: 192.168.1.104:53099'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009
192.168.1.104:53099 Non-OpenVPN client protocol detected'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009
192.168.1.104:53099 SIGTERM[soft,port-share-redirect] received, client-instance exiting'
2009-12-25 10:59:40-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:40 2009 TCP/UDP: Closing
socket'
2009-12-25 10:59:40-0500 [-] WEB-PP OUT: '2009-12-25 10:59:40-0500
[pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '127.0.0.1', 45844)'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 MULTI:
multi_create_instance called'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Re-using SSL/TLS
context'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 LZO compression
initialized'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Control Channel
MTU parms [ L:1544 D:168 EF:68 EB:0 ET:0 EL:0 ]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Data Channel MTU
parms [ L:1544 D:1350 EF:44 EB:135 ET:0 EL:0 AF:3/1 ]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Local Options hash
(VER=V4): 'bd577cd1"
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Expected Remote
Options hash (VER=V4): 'ee93268d"
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCP connection
established with 192.168.1.104:53100'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Socket Buffers: R=
[131072->131072] S=[131072->131072]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 Socket flags:
TCP_NODELAY=1 succeeded'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCPv4_SERVER
link local: [undef]'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCPv4_SERVER
link remote: 192.168.1.104:53100'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009
192.168.1.104:53100 Non-OpenVPN client protocol detected'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009
192.168.1.104:53100 SIGTERM[soft,port-share-redirect] received, client-instance exiting'
2009-12-25 10:59:43-0500 [-] OVPN-PP 0 OUT: 'Fri Dec 25 10:59:43 2009 TCP/UDP: Closing
socket'
2009-12-25 10:59:43-0500 [-] WEB-PP OUT: '2009-12-25 10:59:43-0500
[pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '127.0.0.1', 45845)'
2009-12-25 10:59:48-0500 [-] WEB-PP OUT: '2009-12-25 10:59:48-0500
[pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '192.168.1.104',
56876)'
2009-12-25 10:59:48-0500 [-] WEB-PP OUT: '2009-12-25 10:59:48-0500
[pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '192.168.1.104',
56877)'
2009-12-25 10:59:51-0500 [-] WEB-PP OUT: '2009-12-25 10:59:51-0500
[pyovpn.web.webbase.MySiteBase] Connection from IPv4Address(TCP, '192.168.1.104',
56878)'
```

NeoRouter - the zero-config VPN solution (/article/7949#comment-332012)
Submitted by Anonymous (not verified) on Thu, 01/22/2009 - 13:28.

I found a better VPN solution - NeoRouter (www.neorouter.com (http://www.neorouter.com)). It's much simpler to setup than OpenVPN and does better job than OpenVPN. It can create unlimited nodes in a virtual network and it uses P2P technology as well. It support not only Linux, Window, but also router firmwares like OpenWrt and Tomato.

Highly suggest GUI version of OpenVPN (/article/7949#comment-317256)
Submitted by Anonymous (http://www.strongvpn.com) (not verified) on Sat, 02/16/2008 - 13:53.

I love OpenVPN, with my VPN provider http://www.strongvpn.com (http://www.strongvpn.com) they offered it to me since the regular VPN account they sold me the port was blocked. I installed the non GUI version of OpenVPN and I didn't like the way it would disconnect when I closed the window. The lastest GUI window one is sweet, and makes it easy to reconnect. I went to Openvpn.net and made a donation, please help the developers improve it!

I think anonymous vpn, i (/article/7949#comment-316445)
Submitted by anonymous vpn (http://vpnprivacy.com) (not verified) on Thu, 02/14/2008 - 06:24.

I think **anonymous vpn** (http://vpnprivacy.com) , i mean pptp vpn, is simply for regular user then openvpn setup for **anonymous surfing** (http://vpnprivacy.com) .

This article doesn't (/article/7949#comment-271378)
Submitted by smartcgi (not verified) on Fri, 07/27/2007 - 03:35.

This article doesn't describe one problem. Sometimes DHCP is disabled on PC and OpenVPN fails to get IP.

You'll see "Requesting IP address" running constantly on this OpenVPN connection.

Solution was taken from http://av5.com/docs/running_openvpn_client_on_windows_xp.html (http://av5.com/docs/running_openvpn_client_on_windows_xp.html) and shown below:

open "Control Panel / Administrative Tools / Services", make sure that the "DHCP Client Service" is started.

This is Linux Journal (/article/7949#comment-135946)
Submitted by Anonymous (not verified) on Sat, 04/15/2006 - 12:00.

This is Linux Journal, there's no mention of a linux side GUI client or how to set this up on a Linux client side.
Do you expect me to read something and then use a command line?

Linux GUI (/article/7949#comment-193937)
Submitted by Anonymous (not verified) on Mon, 11/06/2006 - 22:30.

haha right. its about setting up a server, reinstall windows and go home to mommy.

openvpn ikey (/article/7949#comment-15331)
Submitted by D. rodic (not verified) on Mon, 02/14/2005 - 14:32.

How do i setup an OpenVPN connection using smartcard (ikey) features?

Openvpn as a way to secure domain logins over internet (/article/7949#comment-14565)
Submitted by Anonymous (http://www.ctg.albany.edu) (not verified) on Wed, 12/22/2004 - 14:17.

I'm interested in openvpn as a service on a win2k/xp client machine. I would like the vpn to connect before/during the user trying to login to a windows domain account while traveling(their domain login's are not cached).
Is this a capability of openvpn ? Any resouces you can point me at ?
Thanks

Yes, There are many sources (/article/7949#comment-334155)
Submitted by Hank Freid (not verified) on Wed, 03/04/2009 - 13:41.

Yes, There are many sources from where you can use this openvpn, also many certifications available for this at TestKing (http://www.testkingsite.com) and VCP-310 (http://www.testkingsite.com/vmware/vcp-310.html) .

the howto mentioned above: h (/article/7949#comment-14574)
Submitted by Anonymous (not verified) on Thu, 12/23/2004 - 13:40.

the howto mentioned above:
http://sme.swerts-knudsen.dk/index.html?frame=http%3A//sme.swerts-knudse... (http://sme.swerts-knudsen.dk/index.html?frame=http%3A//sme.swerts-knudsen.dk/howtos/howto_30.htm)
does something like that. But I am not sure what you mean exactly. The vpn is a service under windows.

Cool Article (/article/7949#comment-14536)
Submitted by Freak (http://www.openvpn-forum.de) (not verified) on Sun, 12/19/2004 - 15:36.

Thanks for a cool article!
Discussion about OpenVPN @ OpenVPN-Forum.de (http://www.openvpn-forum.de)

Web layout (/article/7949#comment-14515)
Submitted by Anonymous (not verified) on Thu, 12/16/2004 - 16:35.

On my browser and monitor (Firefox, all defaults) the first line of this story is 141 characters.

People read text best at a width of 40-60 characters.

Even if you don't have to horizontal scroll, this layout is ridiculously hard to read.

The article was excellent - w (/article/7949#comment-14569)
Submitted by Anonymous (not verified) on Wed, 12/22/2004 - 20:47.

The article was excellent - why don't you chill with your comment on web settings?

Wow! What's this business (/article/7949#comment-14634)
Submitted by Anonymous (not verified) on Fri, 12/31/2004 - 19:07.

Wow!

What's this business with "why don't you chill with your comment on web settings?"?

Are you referring to the comments about line width? Man, that kind of stuff needs to be fixed--it's just a royal pain trying to read articles like that.

For RoadWarrior there's a goo (/article/7949#comment-14513)
Submitted by Anonymous (not verified) on Thu, 12/16/2004 - 13:07.

For RoadWarrior there's a good option you put in clients. It's the redirect-gateway option.

```
# man openvpn
...
--redirect-gateway
Automatically execute routing commands to cause all outgoing
IP traffic to be redirected over the VPN. Currently imple-
mented only on Linux and Windows.
This option performs three steps:
(1) Create a static route for the --remote address which for-
wards to the pre-existing default gateway. This is done so
that (3) will not create a routing loop.
(2) Delete the default gateway route.
(3) Set the new default gateway to be the VPN endpoint address
(derived either from --route-gateway or the second parameter
to --ifconfig when --dev tun is specified).
When the tunnel is torn down, all of the above steps are re-
versed so that the original default route is restored.
...
```

How well does this scale for multiple road-warriors? (/article/7949#comment-14509)
Submitted by SwedishChef (not verified) on Thu, 12/16/2004 - 09:48.

Thanks for your excellent article. It's always a pleasure to see something that is well documented and complete. However, I have a question about scaling clients that wasn't covered in the article.

I have implemented openVPN for a local organization that has offices in other nearby towns. Each office has access to bandwidth; one via DSL and the other via FTTH (fiber-to-the-home). I configured two separate openVPN servers on the home office router because I couldn't see - from the documentation - whether one openVPN server can monitor two ports; and two separate connections. So I built one server to watch port 5000 and another to watch port 5001 and used shared keys. The other end of both networks is another Linux box that is an openVPN client routing the entire complement of machines in to the home

office. Interestingly enough, both client machines are behind a NAT router yet both connect to the VPN well. The openVPN server is the router/firewall (Shorewall) at the central office. Routing to the Internet is accomplished through a separate firewall in both cases.

So I guess my main question is: "How would two (or more) road warriors access your VPN?" I notice that you have a range of IP addresses in the server config file. Does this work for multiple remote clients?

I might add that I have also configured open-VPN in bridging mode for a client who had an IPX network running across a T-1 routed by two Livingston routers. This was all implemented on an old Novel 3x system that the client was reluctant to change but the $700-per-month T-1 costs were killing him. He had a FTTH connection at his main office and connected a DSL connection to his remote office. I installed two Linux boxes running openVPN in bridging mode; one client on the DSL and the one server at the other end on the fiber. The latency was incredible! IPX apparently broadcasts so much packet traffic that the DSL link was buried under it. However, even when we implemented a TCP Novell system as a test, the DSL was not capable of handling the traffic (although DSL in that same town does handle the SMB traffic of the network I described earlier). We ended up using a wireless connection to a location in the remote town that did have FTTH and then simply creating a VLAN to route traffic back to the home office. So the availability of bandwidth for some protocols is critical.

OpenVPN 2.0, which is in beta (/article/7949#comment-14510)
Submitted by Anonymous (not verified) on Thu, 12/16/2004 - 10:39.

OpenVPN 2.0, which is in beta does not require a separate port for each connection such as the 1.x branch did. The article above is specific to 2.0 and only requires port 1194 for multiple remote connections.

Thanks for such a well-writte (/article/7949#comment-14498)
Submitted by Anonymous (not verified) on Wed, 12/15/2004 - 07:57.

Thanks for such a well-written article!

One problem though: in the server config file, you have two route-up lines. The route-up lines are not stackable, i.e. the second will wipe out the first. Why not just use the "route" option?

In my setup a wring route app (/article/7949#comment-14526)
Submitted by hanscees (not verified) on Fri, 12/17/2004 - 14:01.

In my setup a wring route appeared automagically. The first line deltes that.

vpen in ubuntu festy 7.04 (/article/7949#comment-251857)
Submitted by krax (not verified) on Sun, 06/03/2007 - 01:02.

hello masters
great deaads have encountered to set a vpn connection to INERNET with UBUNTU desktop ver 7.04 festy but any result was out-come.
plz help me t set up this vpn on debian base genome UBUNTU festy 7.04
Email me at kraxadmin[@]gmail.com
waiting with possible awaite
bon rester
thatnks