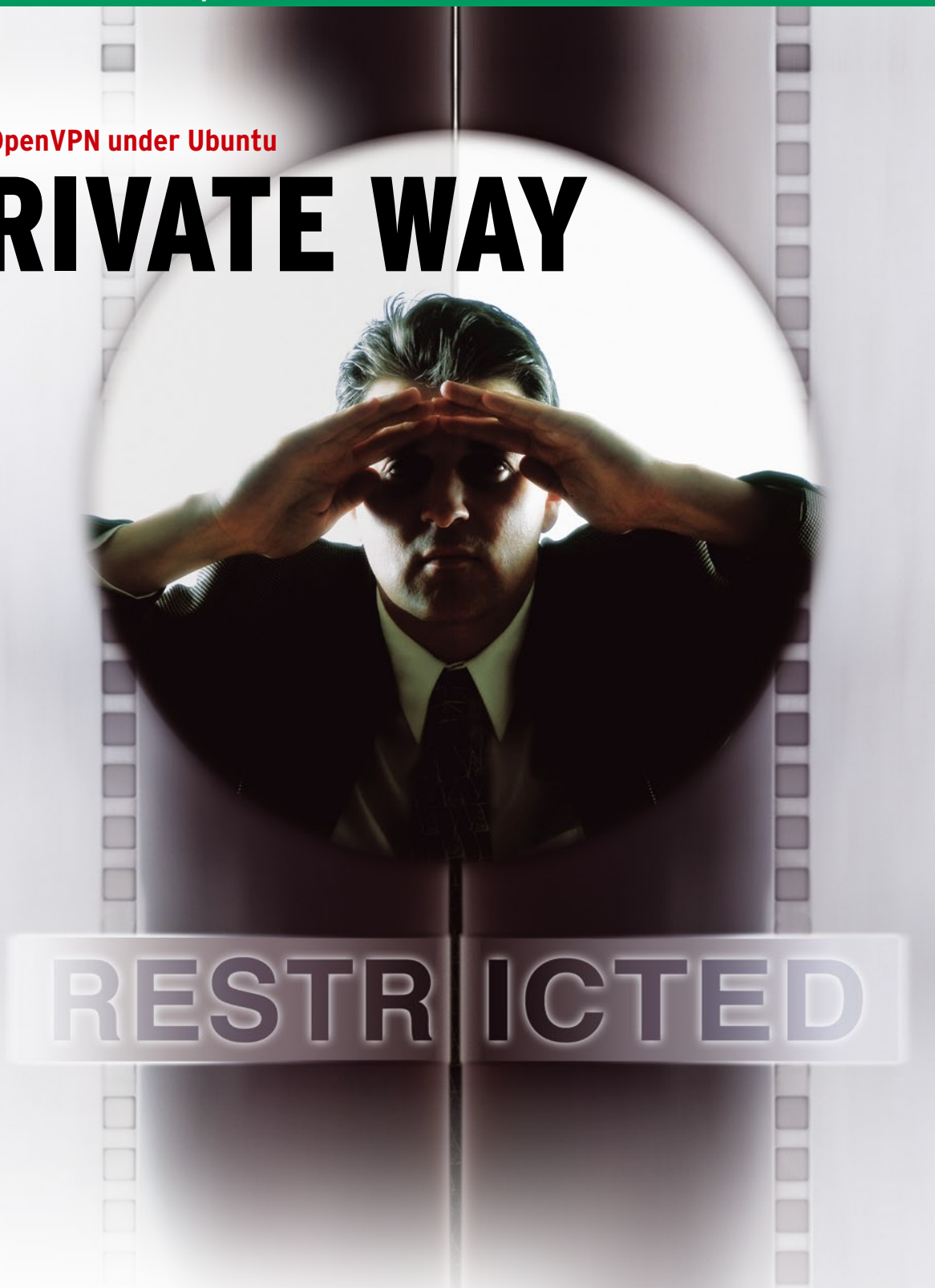
Using OpenVPN under Ubuntu

PRIVATE WAY



Using virtual private networks can provide some data security in environments such as Internet cafés and areas with public access points. **BY DANIEL SALCHER**

In discussions about protecting against the perils of the Internet, the term virtual private network (VPN) often comes up. VPN refers to a method whereby two end points – client and server – can exchange confidential data over an insecure connection, such as a public wireless access point or the Internet in general. Your computer acts as client that logs into a remote VPN server; this action is often known as *tunneling* because the data is tunneled in an encrypted state through an insecure network to preserve confidentiality. Depending on the security level, you authenticate yourself at the server with a username and password, or through a certificate.

VPN technology often is involved when connecting wide networks and allowing remote workers to connect to the corporate network securely. VPNs have other useful applications. For example, if you travel to China, a VPN can help you build a connection to home and allow all traffic to run undetected through its tunnel [1].

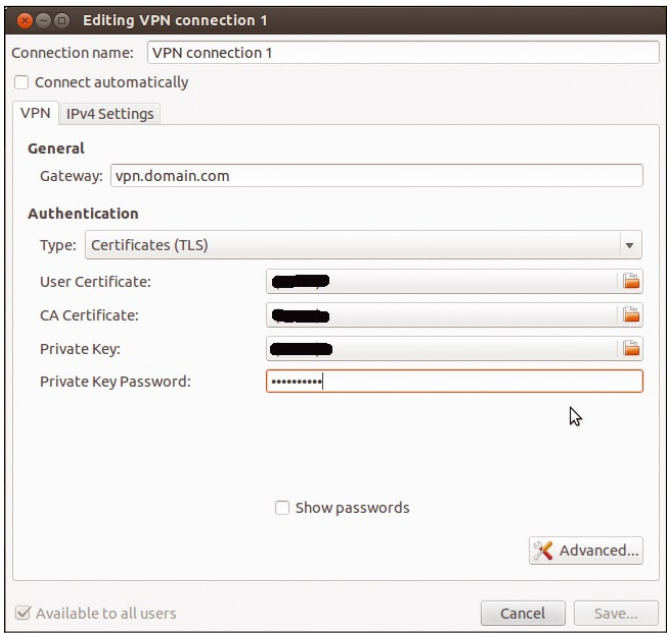


Figure 1: Under Ubuntu, a NetworkManager module helps in making a connection to your OpenVPN server.

PKCS12 Certificates

The *network-manager-openvpn* plug-in can now also handle PKCS12 certificates. Simply specify all three certificate types (*User Certificates*, *CA Certificates*, and *Private Key*) when setting up authentication.

When you are outside the United States, you can still access the *hulu.com* video site when you have a US IP address. If you go through a US VPN provider, you can get one temporarily. Because there are so many VPN providers worldwide, listing them all is beyond the scope of this article, but you can find a list online [2].

Linux with OpenVPN

OpenVPN is an open source, secure, and streamlined bit of software that is under the GPL and runs on Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X, and Windows 2000/XP/Vista/7. For security-related tasks such as logging in and encryption, OpenVPN uses reliable techniques such as OpenSSL, which almost every web server uses. Thus, OpenVPN is considered safe.

The American company OpenVPN Technologies, Inc. [3] developed the software further, and there are vital communities dedicated to supporting the software in support forums and extensive wikis [4].

Many products have included OpenVPN by default, such as hardware firewalls (from vendors like Securepoint and Insys Microelectronics), firewall distributions (IPCop), and distributions that run on routers (dd-wrt).

Of course, you can use OpenVPN on your home system (Linux, Mac OS X, Windows), including to access home data remotely. If you are often in hotels or like to use public wireless access points, such as Internet cafés, you will want to be sure that your neighbors aren't snooping in your personal data. OpenVPN can be valuable in that respect, because it encrypts the data and keeps it away from prying eyes and potential attackers.

Server Configuration

When using OpenVPN, you can choose to use it as a client or server. When using it as a server, you need to reserve only one port connection (well-known port number 1194 over UDP) with your router so that it forwards requests to your server [4]. If you want to save yourself the work or need a server in another country, try using a commercial OpenVPN provider. Be sure that the provider offers OpenVPN, because some other VPN versions aren't compatible with OpenVPN.

The most secure OpenVPN implementation uses certificates together with static keys; however, because certificates usually sit on your computer, there could be a risk of viruses or trojans compromising them. To avoid the risk, use a USB smart card, where the certificate can be on the card and with you securely. The card also does the encryption, because it even has a small resident processor to do the job.

If your provider doesn't support certificates, server and client connections can also use static keys that the server generates in short time intervals. Even if an attacker can decrypt your message, it will only be briefly.

OpenVPN Client with Ubuntu 12.04

To install the OpenVPN client under Ubuntu 12.04, download the *openvpn* package from the Ubuntu Software Center. NetworkManager also provides a convenient GUI plug-in that helps you set up connectivity. To set up connectivity, install the package *network-manager-openvpn*, click the NetworkManager icon, and select *Edit Connections*.

On the *VPN* tab, simply open an OpenVPN connection. Enter the credentials (Figure 1) that you get from your OpenVPN provider (see the "PKCS12 Certificates" box).

Because your provider sends the vital credentials when setting up the connection, you should not need to provide further details. Our test system, which was a beta-2 version of Ubuntu 12.04, used *openvpn 2.2.1* and *network-manager-openvpn 0.9.4.0*.

Data Protection

If you use a foreign OpenVPN provider, always consider local data protection laws. Downloading copyrighted files can cause problems. Some providers are rumored not to cooperate with local authorities, others put their foot down on data protection. In any case, always send confidential data encrypted through the tunnel. ■

AUTHOR

Daniel Salcher is owner and CEO of SAVATEC e.K and does IT work primarily for notaries. Salcher is also a founding member and on the board of OpenVPN e.V.

INFO

[1] Set up OpenVPN in Four steps: *http://www.linuxpromagazine.com/Online/Features/Set-up-OpenVPN-in-four-steps/*

[2] Short list of OpenVPN providers: *http://myvpnreviews.com/top-openvpn-service/*

[3] OpenVPN Technologies, Inc.: *http://www.openvpn.net*

[4] OpenVPN e.V.: *http://www.openvpn.eu*