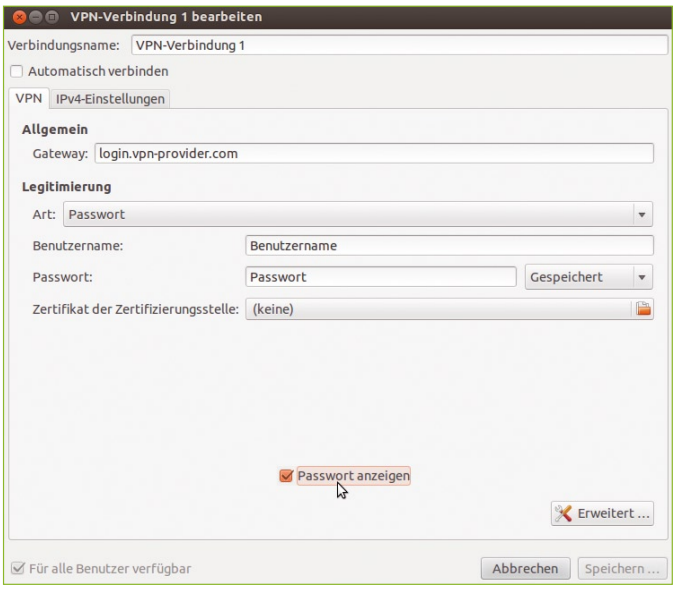
OpenVPN-Client unter Ubuntu nutzen

Privatweg

Über Virtual Private Networks gelangen Sie selbst in technisch unsicheren Umgebungen wie Internetcafés und über öffentliche Access Points sicher an Ihre Daten.

Daniel Salcher

Ist von den Gefahren des Internets die Rede, fällt häufig das Stichwort VPN, wenn es darum geht, sich zu schützen. Übersetzt bedeutet VPN „virtuelles privates Netzwerk“ und bezeichnet eine Technik, die vertrauliche Daten trotz einer unsicheren Verbindung (z. B. öffentliche Access Points oder das Internet allgemein) sicher zwischen zwei Endpunkten (Server, Client) austauscht. Ihr Rechner fungiert dabei als Client, der sich bei einem entfernten VPN-Server anmeldet. Dieses Vorgehen bezeichnet man auch als „tunneln“ von Daten, da Sie sozusagen einen verschlüsselten Tunnel durch unsichere Netze aufbauen und vertrauliche Daten verschlüsselt übertragen.



1 Unter Ubuntu hilft Ihnen ein NetworkManager-Modul dabei, eine Verbindung zum OpenVPN-Server herzustellen.

Abhängig von der gewählten Sicherheitsstufe authentifizieren Sie sich mit einem Benutzernamen und einem Passwort oder über ein Zertifikat beim Server. Die VPN-Technologie kommt häufig zum Einsatz, um ganze Netzwerke zu koppeln und um Außendienstmitarbeitern den Zugriff auf das Unternehmensnetzwerk zu ermöglichen.

Es gibt weitere nützliche Anwendungsbeispiele: Sind Sie zum Beispiel in China unterwegs, während Ihr VPN-Server in Deutschland steht, tricksen Sie die „Great Firewall“ aus, indem Sie eine VPN-Verbindung nach Hause aufbauen und den gesamten Traffic über diesen Tunnel leiten [1].

Auf das US-amerikanische Videoportal *hulu.com* dürfen Sie nur zugreifen, wenn Ihr Rechner über eine amerikanische IP-Adresse verfügt. Nutzen Sie einen amerikanischen VPN-Provider, können Sie sich solch eine IP temporär zulegen. Da weltweit sehr viele VPN-Provider existieren, würde es jedoch den Rahmen dieses Artikels sprengen, alle vorzustellen. Unter [2] gibt es eine kleine Liste.

Linux mit OpenVPN

OpenVPN ist eine quelloffene, sichere und schlanke VPN-Software, die unter der GPL steht und auf Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X sowie Windows 2000/XP/Vista/7 läuft. Für die sicherheitsrelevanten Auf-

gaben wie das Anmelden und Verschlüsseln setzt OpenVPN auf bewährte und vielfach getestete Techniken wie OpenSSL, das auf fast jedem Webserver zum Einsatz kommt. Daher wird OpenVPN als sehr sicher eingestuft. Die amerikanische Firma OpenVPN Technologies, Inc. [3] entwickelt die Software weiter; in Deutschland arbeitet seit 2006 eine lebhafte Community [4] damit, die auch ein Supportforum und ein Wiki anbietet.

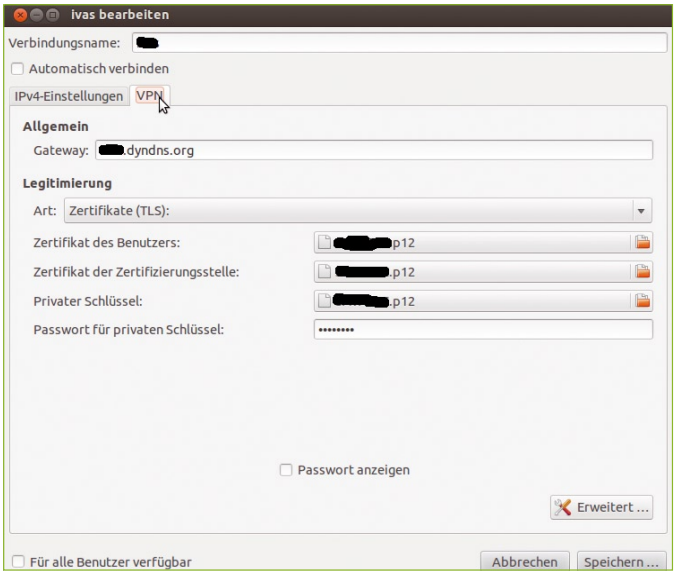
In vielen Produkten ist OpenVPN standardmäßig integriert: Dazu gehören einige Hardware-Firewalls (z. B. Securepoint, Insys Microelectronics), Firewall-Distributionen (IPCop) sowie Distributionen, die auf Routern laufen (DD-WRT).

Sie können OpenVPN natürlich auch auf Ihrem privaten PC einsetzen (Linux, Mac OS X, Windows), um z. B. von unterwegs auf Daten zuzugreifen, die sich auf dem heimischen PC befinden. Halten Sie sich öfter in Hotels auf oder nutzen Sie gern mal öffentliche WLAN-Access-Points (etwa in den besagten Internetcafés), möchten Sie sicher nicht, dass ein Nachbar sämtliche übertragenen Daten mitliest. Auch das verhindern Sie mit OpenVPN, das sämtliche Daten verschlüsselt überträgt und sie so vor neugierigen Blicken schützt.

Server einrichten

Die OpenVPN-Software setzen Sie wahlweise als Client oder Server ein. Betreiben Sie OpenVPN als Server, müssen Sie lediglich einen Port an Ihrem Router weiterleiten (Standard: *1194 UDP*), damit dieser Anfragen aus dem Internet an den Server weiterleitet. Da Sie einen OpenVPN-Server allerdings nicht mit zwei Mausklicks einrichten, sparen wir das Thema in diesem Artikel aus. Hilfe dazu finden Sie im Wiki des OpenVPN e. V. [4], das auch zahlreiche Howtos zum Thema anbietet, sowie im LinuxUser [5]. Scheuen Sie den Aufwand, oder benötigen Sie einen Server in einem anderen Land, versuchen Sie es mit einem kommerziellen OpenVPN-Anbieter. Wichtig ist, dass dieser OpenVPN anbietet – es gibt andere VPN-Varianten, die mit OpenVPN nicht kompatibel sind.

Die sicherste Variante einer OpenVPN-Verbindung setzt auf Zertifikate in Kombination mit einem statischen Schlüssel. Da die Zertifikate jedoch im Normalfall auf Ihrer Festplatte liegen, besteht die Gefahr, dass Viren oder Trojaner sie entwenden. Das unterbinden Sie, indem Sie eine USB-Smartcard verwenden. Das erzeugte Zertifikat befindet sich dann auf der Smartcard (die einer Karte für das Homebanking ähnelt), die es auch beim Entschlüsseln nicht verlässt, denn die Smartcard selbst bringt einen kleinen Prozessor mit, der diesen Job übernimmt. Setzt der gewählte Provider nicht auf Zertifikate, handeln Server und Client beim Verbindungsaufbau lediglich den statischen Schlüssel aus, den der Server standardmäßig jede Stunde neu generiert. Selbst wenn einem Angreifer die Entschlüsselung gelingt, kann er nur eine Stunde lang mitlesen.



❷ Auch das Verwalten von OpenVPN-Zertifikaten erledigen Sie problemlos über die grafische Oberfläche des NetworkManagers.

OpenVPN-Client unter Ubuntu 12.04

Als Client installieren Sie OpenVPN unter Ubuntu 12.04 über das Paket *openvpn* im Software-Center. Für den NetworkManager gibt es ein Plug-in, mit dessen Hilfe Sie das Einrichten und den Verbindungsaufbau komfortabel über eine grafische Oberfläche erledigen. Dazu installieren Sie das Paket *network-manager-openvpn*, klicken dann auf das NetworkManager-Icon und wählen *Verbindungen bearbeiten*.

Im Reiter *VPN* fügen Sie nun einfach eine OpenVPN-Verbindung hinzu. Dazu tragen Sie die Anmeldedaten ein (Abbildung ❶), die Sie vom OpenVPN-Provider erhalten haben (siehe Kasten *PKCS12-Zertifikate*). Da der Provider die wichtigsten OpenVPN-Parameter beim Verbindungsaufbau überträgt, müssen Sie in der Regel keine weiteren Details angeben. Auf unserem Testsystem – einer aktuellen Beta-2-Version von Ubuntu 12.04 – kamen *openvpn 2.2.1* und *network-manager-openvpn 0.9.4.0* zum Einsatz.

Datenschutz

Nutzen Sie einen ausländischen OpenVPN-Anbieter, sollten Sie sich vor Augen führen, dass dieser nicht unbedingt der deutschen Rechtsprechung unterliegt – Sie müssen selbst auf den Datenschutz achten. Laden Sie urheberrechtlich geschützte Dateien herunter, können Sie Probleme bekommen. Manchen VPN-Anbietern wird sogar nachgesagt, ohne Not mit amerikanischen Behörden zu kooperieren, andere gelten wieder als sehr datenschutzorientiert. Vertrauliche Informationen sollten Sie jedoch – wenn überhaupt – nur verschlüsselt durch so einen Tunnel schicken. (kki)

PKCS12-Zertifikate

Das Plug-in *network-manager-openvpn* kann inzwischen auch mit PKCS12-Zertifikaten umgehen. Dazu wählen Sie einfach in allen drei Zertifikatsfeldern (*Zertifikat des Benutzers*, *Zertifikat der Zertifizierungsstelle* und *Privater Schlüssel*) die PKCS12 Datei aus (Abbildung ❷).

Der Autor

Daniel Salcher ist Inhaber und Geschäftsführer von SAVATEC e.K. und betreut hauptberuflich die IT von Notaren. Daneben ist er Gründungsmitglied und Vorstand im OpenVPN e. V.

Info

[1] Marcus Feilner, Ronny Weiss, Daniel Salcher: „Löchrige Netze“, Linux-Magazin 10/2011, S. 48 ff.
[2] Kurze Liste mit OpenVPN-Anbietern: *[http://myvpnreviews.com/top-openvpn-service/]*
[3] Firma OpenVPN Technologies, Inc.: *[http://www.openvpn.net/]*
[4] OpenVPN e. V.: *[http://www.openvpn.eu/]*
[5] OpenVPN-Server einrichten: *[http://www.linux-community.de/Internal/Artikel/Print-Artikel/LinuxUser/2011/11/Geschuetzter-Netzzugriff-von-unterwegs-mit-OpenVPN]*