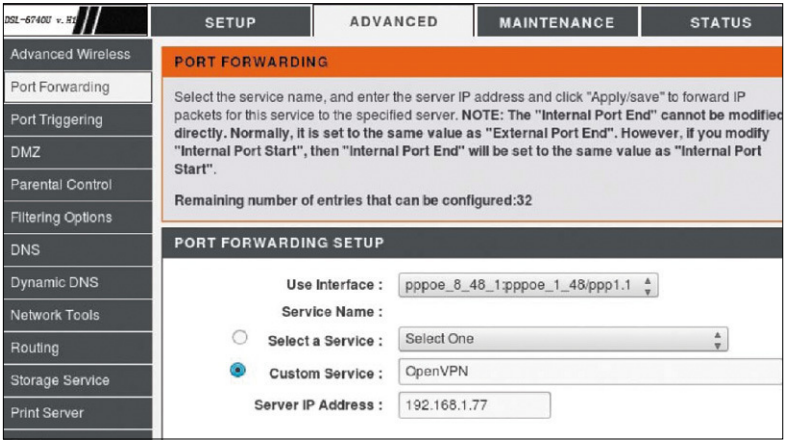
3.10 OpenVPN: Sicher unterwegs in unsicheren Netzwerken

Die Rolle des abhörsicheren Open-VPN-Servers ist ein Heimspiel für Linux-Systeme. Aber auch mit Windows ist es möglich, mit der Open-Source-Lösung ein Virtual Private Network (VPN) für den sicheren Zugriff von außen aufzubauen.

Ein Virtual Private Network (VPN) stellt eine verschlüsselte und abhörsichere Verbindung zu einem internen Netzwerk über einen VPN-Server her. Eine bewährte Lösung dafür ist Open VPN. Die Open-Source-Software ist nicht nur für Linux geeignet, sondern liegt für Clients und Server auch in einer Windows-Version vor. Der Vorteil ist, dass Open VPN eine reine Softwarelösung ist und keine zusätzliche Hardware oder VPN-fähige Router benötigt.

Die Software ist allerdings für den professionellen Einsatz geschaffen, und die erste Konfiguration eines Open-VPN-Servers und der Clients stellt auch unter Windows eine gewisse Hürde dar, denn die Einstellung führt Sie in die Kommandozeile. Mitgelieferte Batch-Dateien von Open VPN vereinfachen aber die Konfiguration. Dieser Beitrag zeigt Schritt für Schritt, wie Sie ein einfaches VPN zwischen zwei Windows-PCs mit Open VPN 2.3.x einrichten. Grundlegende Kenntnisse zur Netzwerkadministration sind dabei hilfreich.



Portforwarding auf dem Router: Damit der Open-VPN-Server im LAN erreichbar ist, muss der Router den verwendeten Port 1194 für Open VPN zum richtigen PC durchreichen (hier 192.168.1.77).

Vorbereitung: den Server erreichbar machen

Auf dem PC, der als Open-VPN-Server agieren soll, müssen Sie die Windows-Firewall abschalten, da diese mit Open VPN nicht kompatibel ist. Dies ist kein Sicher-

heitsproblem, wenn der Rechner sowieso hinter einem Router mit NAT steht, was in den meisten Büro- und Heimnetzwerken der Fall ist. Der Router muss außerdem wissen, welche Anfragen aus dem Internet er durchlassen soll und welcher Rechner im Netzwerk der Open-VPN-Server ist. Dazu richten Sie auf dem Router Portforwarding ein, um gezielt einen einzigen Port nach außen zu öffnen und an die passende Adresse im LAN weiterzuleiten. Ein Beispiel dazu: Der übliche Port für Open VPN ist Port 1194.

Wenn der Open-VPN-Server im LAN die IP 192.168.1.77 hat, dann leiten Sie vom Router den Traffic vom Typ UDP des Ports 1194 auf die interne IP-Adresse und den dortigen Port 1194 um. Der Server, der von außen die VPN-Verbindungen akzeptieren soll, muss zudem aus dem Internet erreichbar sein, und zwar über eine feste IP-Adresse oder über einen eindeutigen DNS-Namen.

Bei DSL-Anbindung gibt es keine feste IP, da bei jedem Verbindungsaufbau der Provider neue IP-Adressen vergibt. Für diesen Fall leistet ein dynamischer DNS-Dienst wie beispielsweise das kostenlose No-IP Hilfestellung, das einer sich ändernden IP-Adresse nach Rückmeldung durch den Router einen festen Host-Namen im DNS zuteilt. Die meisten DSL-Router unterstützen No-IP und teilen dem Dienst automatisch die neue, zugeteilte IP mit.

3.10.1 Open VPN installieren und Schlüssel erzeugen

Auf dem als Server ausgewählten Windows-System installieren Sie **Open VPN** (https://openvpn.net), das in seinem Installationspaket sowohl die Serversoftware als auch die Programme für den Client bietet.

Installieren Sie Open VPN mit allen Komponenten, und markieren Sie dazu unbedingt bei der Installation die optionalen Komponenten „OpenSSL Utilities“ und „OpenVPN RSA Certificate Management Scripts“.

Letztere werden zur Erstellung der eigenen Schlüsselpaare benötigt. Open VPN richtet den neuen, virtuellen Netzwerkadapter „TAPWin32 Adapter V9“ ein, der dann in der Systemsteuerung unter den Netzwerkverbindungen auftaucht. Der Installation des dafür mitgebrachten Treibers müssen Sie in einem angezeigten Dialogfenster wie bei anderen Gerätetreibern manuell zustimmen. Wichtig: Damit der Server später Open-VPN-Verbindungen akzeptieren kann, müssen Sie die Windows-Firewall in der Systemsteuerung deaktivieren, da diese nicht mit Open-VPN-Verbindungen umgehen kann.

Schritt 1: Bevor Sie den Open-VPN-Server starten können, müssen Sie die Schlüsseldateien mithilfe einiger Batch-Dateien erzeugen und die Netzwerkeinstellungen vornehmen. Gehen Sie mit dem Windows Explorer ins Programmverzeichnis von Open VPN. Dieses finden Sie üblicherweise unter „C:\Program Files\Open-VPN“. Gehen Sie dort ins Unterverzeichnis „easy-rsa“: Benennen Sie die Batch-Datei vars. bat.sample nach vars.bat um, und überschreiben Sie damit die bereits vorhandene vars.bat. Öffnen Sie dann eine Eingabeaufforderung mit Administrator-

rechten, was durch einen Rechtsklick auf die entsprechende Verknüpfung im Startmenü und dem Kontextmenüpunkt „Als Administrator“ gelingt. Gehen Sie dann mit „pushd“ in das genannte Verzeichnis, und führen Sie diese beiden Batch-Dateien aus:

```
pushd "C:\Program Files\OpenVPN\ easy-rsa" vars.bat
➥ clean-all.bat
```

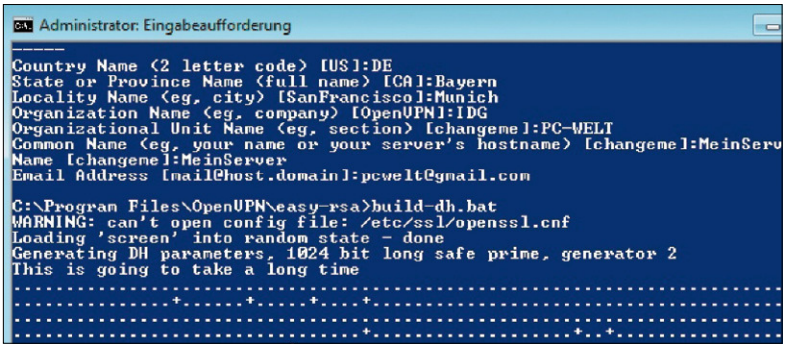
Diese beiden Batch-Dateien geben zunächst die nötigen Umgebungsvariablen vor und erstellen im Programmordner von Open VPN das neue Unterverzeichnis „keys“. Bei einer Standardinstallation von Open VPN auf Windows 7 und 8 liegt dieses beispielsweise unter C:\Program Files\OpenVPN\easy-rsa\keys.

Schritt 2: Für die verwendete Verschlüsselung von Open VPN brauchen Sie auf Ihrem künftigen VPN-Server ein Zertifikat für Ihre eigene Certificate Authority (CA). Dazu führen Sie die Batch-Datei

```
build-ca.bat
```

aus und geben in der Eingabeaufforderung die benötigten Eigenschaften ein. Die abgefragten Eingaben erscheinen umfangreich, sind aber weitgehend beliebig. Die folgende Übersicht erklärt alle Parameter und die erwarteten Eingaben:

Country Name: Landeskürzel, etwa „DE“ für Deutschland
State or Province Name: Bundesland, beliebig
Locality Name: Ortsangabe, beliebig
Organization Name: beliebig
Organizational Unit Name: beliebig und optional
Common Name: Name des VPN-Servers, etwa „MeinServer“
Name: Name der VPN-Verbindung, identisch mit „Common Name“, etwa „MeinServer“
Email Address: Ihre E-Mail-Adresse



Serverzertifikate erstellen: Open VPN bringt für die Erzeugung aller benötigten Schlüssel und Zertifikate einige Batch-Dateien mit, die dann jeweils in der Eingabeaufforderung Ihre Eingaben erwarten.

Schritt 3: Open VPN benötigt für den Verbindungsaufbau einige kryptografische Parameter (Diffie-Hellman-Parameter), die Sie einmalig bei der Installation des Servers erzeugen müssen. Die dafür benötigte Konfigurationsdatei für den Verschlüsselungsalgorithmus erzeugen Sie ganz einfach mit dem Aufruf dieser Batch-Datei:

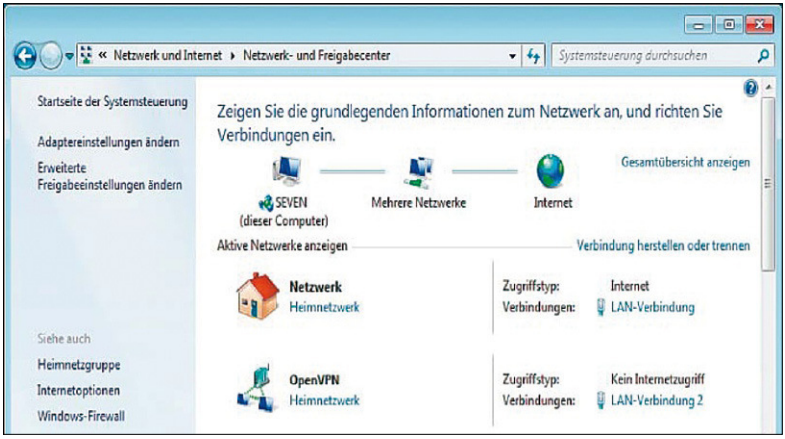
```
build-dh.bat
```

Hier ist keine Angabe von Parametern erforderlich.

Schritt 4: Als Nächstes erstellen Sie das eigentliche Schlüsselpaar für Ihren neuen VPN-Server. Dies gelingt mit der Batch-Datei build-keyserver.bat, der Sie den zuvor eingegeben Namen der VPN-Verbindung aus Schritt 2 als Parameter mitgeben. In unserem Beispiel wäre dies die folgende Eingabe:

```
build-key-server.bat MeinServer
```

Diese Batch-Datei verlangt wiederum die Eingabe der Schlüsselinformationen wie in Schritt 2. Die Angaben sind die gleichen wie beim vorangegangenen Aufruf der Datei build-ca.bat. Nur haben Sie hier die Wahl, zum Abschluss noch ein Passwort zu definieren, mit dem der Schlüssel zusätzlich chiffriert wird. Das Passwort ist optional, und Sie sollten es in dieser Anleitung leer lassen, um die Konfiguration vorerst nicht komplizierter als nötig zu machen. Ebenfalls leer lassen Sie die Eingabe von „An optional company name", da diese nicht wirklich notwendig ist. Am Ende bestätigen Sie noch die beiden Rückfragen „Sign the certificate" jeweils mit „y".



Das VPN als Heimnetzwerk: Nach der Verbindungsaufnahme des Clients mit dem Open- VPN-Server fragt Windows nach, um welchen Typ es sich handelt. Wählen Sie das „Heimnetzwerk".

Schritt 5: Der Server hat nun alle benötigten Schlüssel und Zertifikate. Damit Sie sich aber mit einem VPN-Client später verbinden können, braucht der Client seinen

eigenen Schlüsselbund. Diesen erzeugen Sie in diesem Schritt mit dem Aufruf der Batch-Datei build-key.bat, die Sie jetzt mit dem gewünschten Client-Namen als Parameter aufrufen. In diesem Beispiel soll der Client einfach „MeinClient“ heißen:

```
build-key.bat MeinClient
```

Es erfolgen wieder die Rückfragen zu den bereits bekannten Feldern wie in Schritt 2, allerdings mit einem wichtigen Unterschied: Bei den Fragen nach „Common Name“ und „Name“ geben Sie jetzt den gewünschten Client-Namen an, beispielsweise „MeinClient“ – nicht den Servernamen. Nach dem Signieren erhalten Sie ein Unterverzeichnis „keys“ mit den neuen Schlüsseldateien. Für die Einrichtung des Open-VPN-Clients auf einem anderen Windows-PC benötigen Sie dort später nur diese drei Dateien: MeinClient.crt, MeinClient.key, ca.crt. Kopieren Sie diese Dateien auf einen USB-Stick oder auf eine Netzwerkfreigabe, um sie später auf dem Client einzurichten.

3.10.2 Open VPN für den ersten Start konfigurieren

Nach der Erzeugung aller Schlüssel kommt nun die eigentliche Serverkonfiguration für Open VPN. Die Konfiguration erfolgt hier nach Linux-Tradition in einer Textdatei, was Maus-verwöhnte Windows-Anwender erst mal abschrecken wird. Textdateien haben allerdings den Vorteil, dass alle Einstellungen und Optionen übersichtlich an einem Ort untergebracht sind. Für den Server begnügen wir uns mit einer möglichst einfachen Konfiguration für die Verbindung eines Clients, ohne Routing. Erstellen Sie eine neue Textdatei mit dem Namen server. ovpn im Verzeichnis „C:\Program Files\Open-VPN\config“.

Hinweis: Für die Bearbeitung der Konfigurationsdateien empfiehlt sich ein fähiger Text-Editor wie etwa das Freeware-Programm Notepad++. Das traditionelle Notepad von Windows ist wenig hilfreich, da es die UNIX-Zeilenumbrüche in den Konfigurationsdateien nicht richtig erkennt.

Für das folgende Konfigurationsbeispiel gehen wir von diesen Netzwerkadressen aus: Die Adresse des Open-VPN-Servers im internen LAN ist 192.168.1.77. Das VPN wird im Subnetz 192.168.10.0 aufgebaut. Ausgehend von diesen Beispieladressen bekommt die Konfigurationsdatei server.ovpn die Zeilen aus dem Kasten „Open VPN: Server-Konfiguration“ als Inhalt.

Im ersten Abschnitt dieser Konfigurationsdatei sind die Pfade der benötigten Zertifikate definiert. Beachten Sie hier, dass die Pfadangaben von Anführungszeichen eingefasst sind und dass Sie jeweils einen doppelten Backslash angeben müssen. Im Abschnitt „# Server und Netzwerk“ erscheint zunächst die Angabe der lokalen IP-Adresse des Servers im LAN, in diesem Beispiel 192.168.1.77. Passen Sie diese Adresse so an, dass hier die tatsächliche interne IP Ihres Open-VPN-Server steht.

Darunter folgt die Angabe des Ports, hier 1194. Welches Subnetz für das VPN verwendet wird, gibt die Zeile „server 192.168.10.0 255. 255.255.0 #Subnetz“ an. Der

Open-VPN-Server bekommt so auf seiner VPN-Schnittstelle automatisch die Adresse 192.168.10.1 zugeteilt und der Client die Adresse 192.168.10.x. Im Abschnitt „# Log“ definieren Sie die Pfade zu Log-Dateien im Programmordner von Open VPN. Diese Dateien müssen noch nicht existieren, da sie der Server beim ersten Start selbstständig anlegt.

Open-VPN-Server-Konfiguration

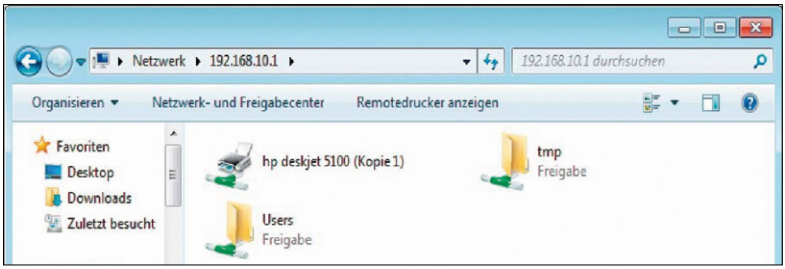
```
# Zertifikateca "C:\\\\Program Files\\\\OpenVPN\\\\
easy-rsa\\\\keys\\\\ca.crt"cert "C:\\\\Program Files\\\\
OpenVPN\\\\easy-rsa\\\\keys\\\\MeinServer.crt"key "C:\\\\
Program Files\\\\OpenVPN\\\\easy-rsa\\\\keys\\\\
MeinServer.key"dh "C:\\\\Program Files\\\\OpenVPN\\\\
easy-rsa\\\\keys\\\\dh1024.pem"

# Server und Netzwerklocal 192.168.1.77

# LAN-Adresse des Serversport 1194proto udpdev tapserver
192.168.10.0 255.255.255.0

#Subnetzifconfig-pool-persist ipp.txtcomp-lzopersist-key-
persist-tunkeepalive 10 120

# Logstatus "C:\\\\Program Files\\\\Open-VPN\\\\log\\\\
openvpn-status.log"log "C:\\\\Program Files\\\\OpenVPN\\\\
log\\\\openvpn.log"log-append "C:\\\\Program Files\\\\
OpenVPN\\\\log\\\\openvpn.log"verb 3
```



Auf Freigaben über VPN zugreifen: Der verbundene Client kann auf den Server zugreifen und beispielsweise dessen Windows-Freigaben anhand der IP-Adresse über das verschlüsselte VPN nutzen.

Wenn die Konfiguration fertig ist, starten Sie auf dem Server den Open-VPN-Dienst. Dies geht am schnellsten in der Eingabeaufforderung (mit Administratorrechten), in der Sie mit

```
net start OpenVPNService
```

den Dienst starten. Es empfiehlt sich, gleich einen Blick auf die Logdateien im Verzeichnis „C:\Program Files\OpenVPN\log“ zu werfen. Sollte die Konfiguration