

Aufbau eines VPN-Tunnels mittels OpenVPN

Technische Facharbeit für IT-Fachkräfte mit Netzwerkgrundkenntnissen

Autor: Jonas Böttcher

13. August 2008

Berufsbildende Schule 1 - Gewerbe und Technik, Mainz

Klasse FI06A



Autor: Jonas Böttcher (*GeckoNET.eu*)

Dieses Werk ist unter einer [Creative Commons-Lizenz](http://creativecommons.org/licenses/by-sa/3.0/) lizenziert. Siehe: <http://creativecommons.org/licenses/by-sa/3.0/>

Seite 1

Inhaltsverzeichnis

1	Einleitung.....	3
2	Definition „VPN“.....	3
3	Argumente für OpenVPN.....	4
4	Die Ausgangssituation.....	4
4.1	Die Netzstruktur.....	4
4.2	Der Server.....	5
4.3	Der Client.....	5
5	Installation und Konfiguration des OpenVPN-Servers.....	6
5.1	OpenVPN-Software beziehen.....	6
5.1.1	Versionsauswahl.....	6
5.1.2	Download.....	6
5.2	Installation.....	6
5.3	Konfiguration.....	7
5.3.1	Erstellen eines Pre-Shared Key.....	7
5.3.2	Erstellen der Konfigurationsdateien.....	8
5.3.2.1	Server-Konfigurationsdatei.....	8
5.3.2.2	Client-Konfigurationsdatei.....	8
6	Aufbau der VPN-Verbindung.....	9
6.1	Aufbau des Tunnels, serverseitig.....	9
6.2	Aufbau des Tunnels, clientseitig.....	10
6.3	Verbindung testen.....	11
7	Routing.....	11
8	Zeitplan und Kostenplan.....	12
8.1	Zeitplan.....	12
8.2	Kostenplan.....	12
9	Zusammenfassung.....	12
10	Glossar.....	13
11	Abbildungsverzeichnis.....	14
12	Tabellenverzeichnis.....	14
13	Quellenverzeichnis.....	14
13.1	Internetseiten.....	14
13.2	Bildquellen.....	14



1 Einleitung

Im folgenden Dokument geht es um die Implementation eines VPN-Tunnels zwischen einem Server in einem einfachen lokalen Netzwerk und einem Client, der über das Internet mit dem Server eine Verbindung aufbauen soll.

Mit dem vorliegenden Text soll das Ziel erreicht werden, IT-Fachkräften mit Netzwerkgrundkenntnissen einen Einstieg und einen schnellen Erfolg zur Implementation eines VPN-Zuganges zu ihrem bestehenden lokalen Netzwerk zu bieten.

Zunächst wird der Begriff „VPN“ definiert. Für die Umsetzung wird OpenVPN verwendet, was nachfolgend begründet wird. Nach der Versionswahl fängt der praktische Teil an, bestehend aus Installation, Konfiguration, Inbetriebnahme und Test des neuen VPN-Tunnels. Abschließend wird aufgezeigt, wie Routing ins reelle Netz des Servers möglich ist.

Dateinamen, Schaltflächen, Programmnamen, Dateipfade, Befehle, Konfigurationscode und ähnliche Zeichenketten sind in der Schriftart `Courier New` gekennzeichnet. Fremdwörter oder Fachbegriffe sind explizit verlinkt zur genauen Beschreibung bzw. [Definition im Glossar](#). Links sind hierbei unterstrichen. Sonstige Kommentare, Anmerkungen und Kurzinformationen sind als Fußnote auf der jeweiligen Seite vermerkt.

2 Definition „VPN“

Ein Virtuelles Privates Netzwerk (Virtual Private Network), kurz VPN, ist eine Lösung der Problematik, ein LAN über große geografische Distanz und über öffentliche Netze/Leitungen aufrecht zu erhalten.

Als "*privates Netzwerk*" kann ein LAN wie ein Firmennetzwerk verstanden werden, in dem beispielsweise sensible Firmendaten verkehren und/oder bestimmte Serveranwendungen zu erreichen sind. All diese Vorzüge des Firmennetzes möchte man nun entweder zu Hause, unterwegs oder in einem anderen LAN auch



nutzen können.

Durch VPN wurde die Möglichkeit geschaffen, keine teuren, aufwendigen physikalischen Verbindungsleitungen legen zu müssen: Virtuell lassen sich private Netzwerke durch unsichere Medien oder große Entfernungen sicher durch eine "virtuelle" Standleitung miteinander verbinden.

3 Argumente für OpenVPN

Es gibt verschiedene Möglichkeiten, VPN zu implementieren. Mit OpenVPN hat dessen Entwicklergemeinde eine Lösung geschaffen, die kompatibel zu der meisten Hardware und vielen Betriebssystemen¹ ist.

Im Vergleich zu anderen Lösungen für VPN ist OpenVPN in einfachen, verständlichen Schritten zu installieren. Dennoch ist es stark skalierbar, um Projekte wie lastenverteilte VPN-Serverfarmen für tausende von VPN-Teilnehmern zu realisieren.²

Ein weiteres Argument für OpenVPN ist, dass es als [Open Source](#)-Produkt lizenziert ist.³ Dadurch lassen sich Lizenzgebühren sparen. Des Weiteren besteht eine sehr große Community in vielen Internetfachforen.

4 Die Ausgangssituation

Es wird die Ausgangssituation beschrieben, von der in dem gesamten Dokument zur Einrichtung eines VPN-Tunnels mittels OpenVPN ausgegangen wird.

4.1 Die Netzstruktur

Ein LAN befindet sich hinter einem Router mit Firewall-Funktionalität und Gateway ins Internet via DSL-Modem. Der Router beherrscht [NAT](#) und setzt es auch ein. Im Folgenden dazu eine schematische Grafik (Abb. 1):

1 OpenVPN läuft auf Linux, Windows 2000/XP und höher, OpenBSD, FreeBSD, NetBSD, Mac OS X, und Solaris. Eine Implementation für PocketPC ist in Entwicklung. Quelle:

<http://www.openvpn.net/index.php/component/content/article/55.html> [09.08.2008, 17:40]

2 Quelle: <http://www.openvpn.net/index.php/component/content/article/55.html> [09.08.2008, 17:47]

3 Weiterführende Informationen: <http://openvpn.net/index.php/licensing.html> [07.08.2008, 17:35]



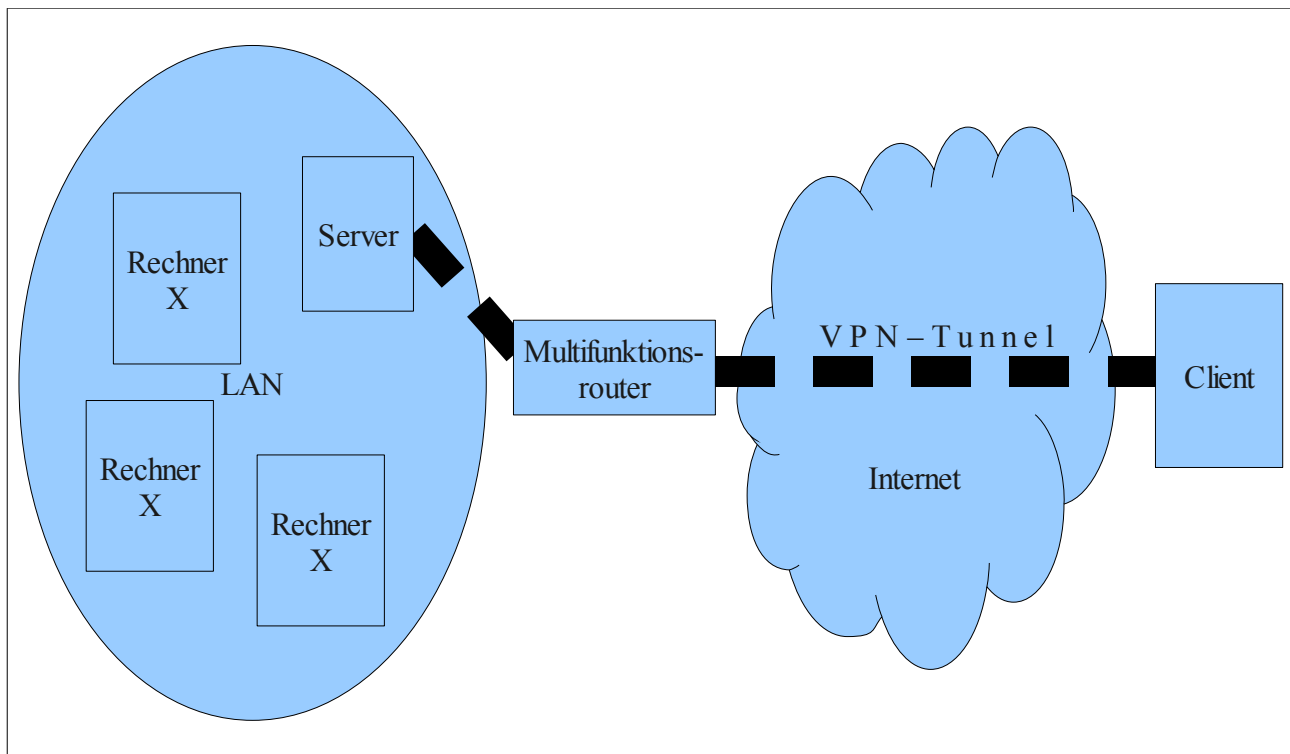


Abbildung 1: Schema des VPN-Tunnels durch LAN, Router und Internet

Die IP-Adressen aller Rechner im LAN werden statisch vergeben. Der Netzbereich geht von 192.168.0.1 bis 192.168.0.255. Der Router ist aus dem Internet über [DynDNS](#) unter der Domain `beispiel.domain.net` zu erreichen.

Die Firewall auf dem Router leitet eingehende Anfragen auf UDP-Port 5000 an den Server-Rechner weiter.

4.2 Der Server

Als Server dient ein Rechner ohne besondere technische Ausstattung. Das Betriebssystem ist Microsoft Windows XP Home Edition mit Service-Pack 3. Der Server besitzt eine feste IP-Adresse.

4.3 Der Client

Als Client dient ein Rechner ohne besondere technische Ausstattung. Das Betriebssystem ist Microsoft Windows XP Home Edition mit Service-Pack 3. Der Client hat im Gegensatz zum Server keine feste IP-Adresse.

5 Installation und Konfiguration des OpenVPN-Servers

Es wird die Installation der OpenVPN-Software auf einem Rechner mit dem Betriebssystem Windows XP (Service-Pack 3) von Microsoft beschrieben.

5.1 OpenVPN-Software beziehen

5.1.1 Versionsauswahl

In diesem Text wird die Version 2.1 RC9, freigegeben am 31.07.2008, behandelt. Sie unterscheidet sich von Vorgängerversionen im Wesentlichen durch [Bugfixes](#), Sicherheitsupdates und neue Funktionen, die kaum Auswirkung auf Grundfunktionen und die Windows-Installationsroutine haben.⁴ Des Weiteren handelt es sich um einen [Release Candidate](#). Die Entwickler empfehlen daher: „*The OpenVPN 2.1 beta series is ready for testing and limited production usage.*“⁵

Um die Aktualität des Dokumentes länger zu gewährleisten, wird der oben beschriebene Release Candidate verwendet – es wird von einem baldigen Erscheinen eines [Release](#) ausgegangen.

5.1.2 Download

Da, wie oben beschrieben, der OpenVPN-Installation als Plattform das Betriebssystem Windows XP (Service-Pack 3) von Microsoft dient, fällt die Downloadauswahl auf den Windows Installer. Im Folgenden der Internetlink zur Installationsdatei:

Direkter Internetlink zur Installationsdatei:

- http://openvpn.net/release/openvpn-2.1_rc9-install.exe

Übersicht aller Downloads: <http://openvpn.net/index.php/downloads.html>

5.2 Installation

Nach erfolgreichem Download wird die EXE-Datei gestartet und der

4 Bezug auf Release-Notes unter: <http://openvpn.net/index.php/documentation/change-log/changelog-21.html> [07.08.2008, 16:46]

5 Zitat aus: <http://openvpn.net/index.php/downloads.html> [07.08.2008, 17:16]



Installationsprozess ohne Veränderung der Standardeinstellungen durchlaufen. Der Installation eines unsignierten Treibers muss zugestimmt werden.

5.3 Konfiguration

5.3.1 Erstellen eines Pre-Shared Key

Zur Authentifizierung eines autorisierten Clients um eine sichere VPN-Verbindung herzustellen wird zuerst ein Pre-Shared Key generiert und dem autorisierten Client übermittelt. Der Schlüssel ist statisch, wird also einmalig generiert und nachher nicht mehr verändert. Aus Sicherheitsgründen wird empfohlen, den Schlüssel periodisch ca. alle 3 Monate neu zu erzeugen und zu verteilen.

Um den statischen Pre-Shared Key zu erzeugen geht man auf dem Server auf das Startmenü von Windows in der Taskleiste und ruft folgendes Programm auf:

„OpenVPN“ → „Utilities“ → „Generate a static OpenVPN key“

Es folgt die Bestätigung, siehe Abb. 2.

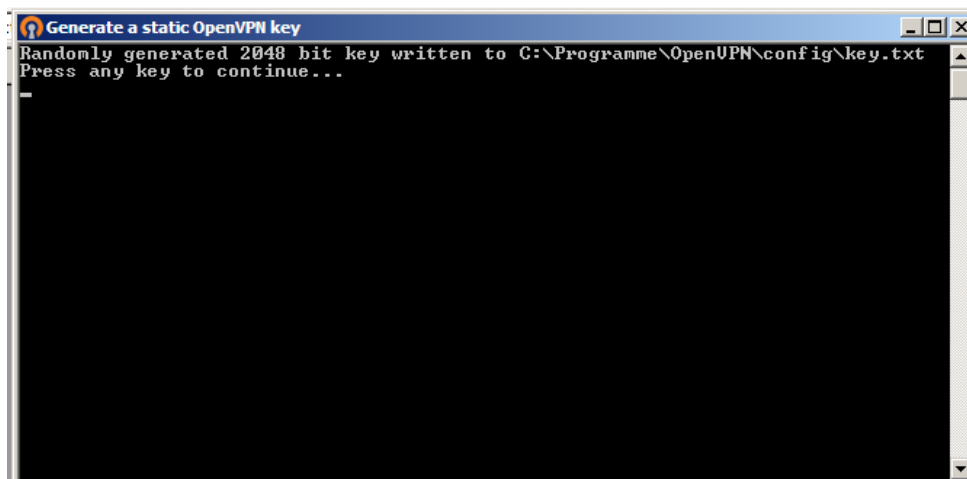


Abbildung 2: Statischen Schlüssel erstellen

Der neue Key (Schlüssel) wurde unter
C:\Programme\OpenVPN\config\key.txt
abgespeichert. Damit beim (versehentlichen) Generieren neuer Schlüssel der alte

Schlüssel nicht überschrieben wird, sollte der neu erzeugte Schlüssel sinnvoll umbenannt werden.

5.3.2 Erstellen der Konfigurationsdateien

Neben dem Schlüssel müssen zwei verschiedene Konfigurationsdateien erstellt werden. Nachfolgend wird von der Server- und der Client-Konfigurationsdatei gesprochen.

5.3.2.1 Server-Konfigurationsdatei

Unter `C:\Programme\OpenVPN\config` wird auf dem Server eine Textdatei mit beliebigem Namen und der Extension `*.ovpn` angelegt. Diese Datei kann mit einem beliebigen Texteditor bearbeitet werden und muss mindestens folgende Zeilen beinhalten (unter Berücksichtigung der Ausgangssituation, Kapitel 4):

```
1 dev tun
2 ifconfig 10.0.0.1 10.0.0.2
3 secret schlüssel.txt
4 port 5000
```

Erklärung:

Zeile 1: Das virtuelle Gerät `tun` zum Tunneln aller Informationen ab [OSI-Modell-Schicht 3](#) wird angesprochen.

Zeile 2: Die neuen IP-Adressen für den Tunnel werden festgelegt. Der Server bekommt die IP `10.0.0.1` und der Client die IP `10.0.0.2`.

Zeile 3: Der statische Pre-Shared Key aus Kapitel 5.3.1 wird mitgeteilt.

Zeile 4: Port `5000` wird verwendet, siehe Stichwort „Firewall“ im Kapitel 4.1.

5.3.2.2 Client-Konfigurationsdatei

Unter einem beliebigen Verzeichnis wird eine Textdatei mit beliebigem Namen und der Extension `*.ovpn` angelegt. Diese Datei kann mit einem beliebigen Texteditor bearbeitet werden und muss mindestens folgende Zeilen beinhalten (unter Berücksichtigung der Ausgangssituation, Kapitel 4):



```
1 remote beispiel.domain.net
2 dev tun
3 ifconfig 10.0.0.2 10.0.0.1
4 secret schlussel.txt
5 port 5000
```

Erklärung:

Zeile 1: Eine Remoteverbindung zur Dynamischen DNS (siehe Kapitel 4.1, Stichwort „DynDNS“) des Servers wird aufgebaut.

Zeile 2: Das virtuelle Gerät zum Tunneln aller Informationen ab OSI-Modell Schicht 3 wird angesprochen.

Zeile 3: Die neuen IP-Adressen für den Tunnel werden festgelegt. Der Clients bekommt die IP 10.0.0.2 und der Server die IP 10.0.0.1.

Zeile 4: Der statische Pre-Shared Key wird mitgeteilt.

Zeile 5: Port 5000 wird verwendet.

6 Aufbau der VPN-Verbindung

6.1 Aufbau des Tunnels, serverseitig

Damit auf der Serverseite der Dienst für eingehende VPN-Anfragen nicht bei jedem Verbindungsversuch manuell gestartet werden muss, ist es sinnvoll, den `OpenVPN Service` beim Hochfahren des Betriebssystems gleich automatisch starten zu lassen.

Zum Aufrufen der Übersicht der lokalen Dienste auf dem Server gibt man unter `START` → „Ausführen...“ den Befehl `services.msc` ein. In der Übersichtsliste klickt man nun auf die Eigenschaften von `OpenVPN Service` und stellt den Starttyp auf `Automatisch`, siehe dazu Abb. 3.

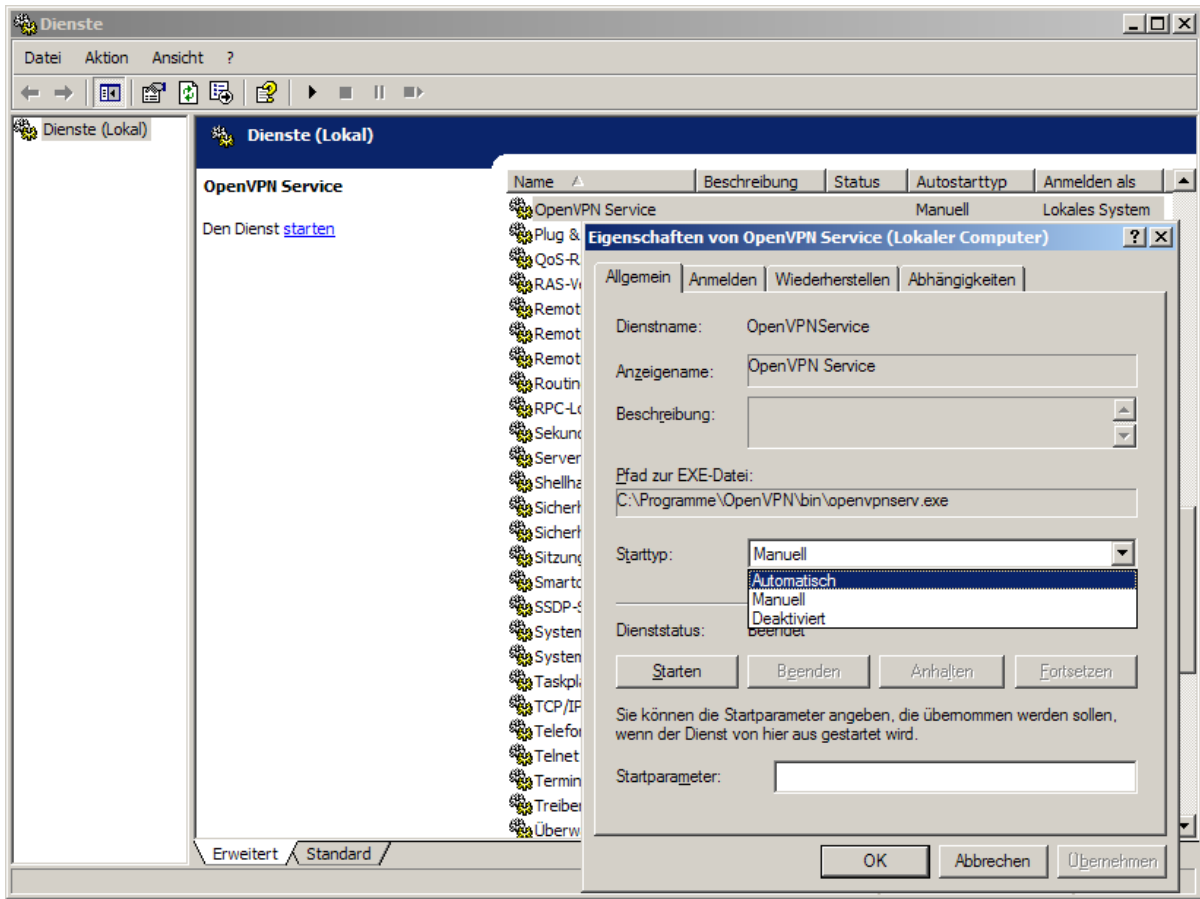


Abbildung 3: Eigenschaften von "OpenVPN Service"

Außerdem muss beim ersten Mal der Dienst über die Schaltfläche `Starten` manuell gestartet werden.

Durch das Starten des OpenVPN Services werden alle konfigurierten OpenVPN-Verbindungen (siehe Kapitel 5.3.2.1) unter `C:\Programme\OpenVPN\config` gestartet. In diesem Fall ist es nur eine Verbindung.

6.2 Aufbau des Tunnels, clientseitig

Auf dem Client wird die Verbindung durch den zweiten Eintrag des Kontextmenüs „Start OpenVPN on this config file“ der *.ovpn-Datei aus Kapitel 5.3.2.2 gestartet (siehe Abb. 4).

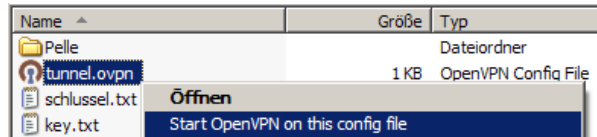


Abbildung 4: VPN-Tunnel starten

Nach erfolgreichem Aufbau des Tunnels erscheint folgende Bestätigung (Abb. 5).



Abbildung 5: Erfolgsmeldung nach Tunnelaufbau beim Client

6.3 Verbindung testen

Zum Testen der Verbindung kann jeweils die IP-Adresse der Gegenstelle (Server: 10.0.0.1, Client: 10.0.0.2) mit dem Programm `ping` „angepingt“ werden. Verläuft der Test erfolgreich, können Server und Client grundsätzlich über alle Schichten ab Schicht 3 des OSI-7-Schichten-Modells miteinander kommunizieren.

7 Routing

Damit nicht nur Server und Client miteinander kommunizieren können, sondern der Client auch weitere Rechner im LAN des Servers erreichen kann, muss folgende Zeile der Konfigurationsdatei des Clients (siehe Kapitel 5.3.2.2) hinzugefügt werden:

```
push "route 192.168.0.0 255.255.255.0"
```

Die IP-Netzadresse `192.168.0.0` beschreibt das ganze (reale) Subnetz, in das der Server integriert ist (nicht das virtuelle Netz). Gemäß dieser Netzadresse muss der Server eine IP-Adresse zwischen `192.168.0.1` und `192.168.0.255` haben.

Der Client leitet nun alle Anfragen an `192.168.0.1-255` an den Server weiter.

8 Zeitplan und Kostenplan

8.1 Zeitplan

Die folgende Tabelle zeigt eine detaillierte Auflistung der Arbeitsschritte zur Implementation eines OpenVPN-Tunnels. Die Arbeitszeit ist geschätzt und kann, abhängig der Kenntnisse der Fachkraft, unterschiedlich ausfallen. Des weiteren wird davon ausgegangen, dass die Ausgangssituation der Beschreibung in Kapitel 4 entspricht.

Tabelle 1: Zeitplan für den Aufbau einer VPN-Verbindung mittels OpenVPN

Nr.	Beschreibung des Arbeitsschrittes	Dauer
1	Download der Software	5-10 Minuten
2	Installation der Software	5-15 Minuten
3	Erstellen der Konfigurationsdateien	10 Minuten
4	Aufbau und Test des VPN-Tunnels	10-15 Minuten
5	Einstellung der Routing-Funktionalität	5-10 Minuten
Summe:		<u>35-45 Minuten</u>

8.2 Kostenplan

Bis auf mögliche Personalkosten o. ä. fallen bei dem Aufbau eines VPN-Tunnels mittels VPN keine weiteren Kosten an (unter Berücksichtigung der Ausgangssituation, Kapitel 4). Der Arbeitsaufwand liegt unter einer Stunde. Auch die Software OpenVPN ist kostenlos zu beziehen.

9 Zusammenfassung

Nach einer Definition des Begriffes „VPN“ werden in diesem Dokument Gründe für die Open Source-Implementation OpenVPN offen gelegt. Die genaue Version wird gewählt und dessen Auswahl begründet. Es folgen Download und Installation der Setup-Datei. Das anschließende Konfigurieren beinhaltet das Generieren eines Pre-Shared Key und zweier Konfigurationsdateien für Server und Client. Nach Inbetriebnahme und Test des VPN-Tunnels wird abschließend eine Methode des Routings beschrieben.



10 Glossar

Bugfix: Behobener Fehler in der Programmierung

DynDNS: Kostenloser Dienst im Internet, der es ermöglicht, ständig wechselnde öffentliche IP-Adressen von DSL-Routern mit einer festen (dynamischen) Domain erreichbar zu machen. Dazu muss man sich unter <http://www.dyndns.com/> kostenlos registrieren, sich eine Domain aussuchen und dem DSL-Router diese Informationen mitteilen. Der Router teilt dadurch regelmäßig dem Dienst seine neue IP-Adresse mit. Der DSL-Router muss die DynDNS-Funktion beherrschen.⁶

NAT: englisch „network address translation“, wird verwendet um private IP-Adressen aus dem privaten Netz in eine öffentliche IP-Adresse zu übersetzen (um das Routing durch das Internet zu ermöglichen). In den meisten Fällen werden *mehrere* private IP-Adressen durch *eine* öffentliche Adresse ersetzt, mit der der Router mit dem Internet verbunden ist.⁷

Open Source: Der Programmquellcode wird von den Entwicklern frei veröffentlicht. Nach dieser Idee ist es jedem erlaubt, das Programm oder Programmteile seinen Bedürfnissen anzupassen. Weiterführende Informationen unter: http://de.wikipedia.org/wiki/Open_source [07.08.2008, 17:43]

OSI-Referenzmodell: Das OSI-Referenzmodell teilt die Datenkommunikation über das Netzwerk in 7 Schichten ein. Schicht 3 baut bspw. auf das Internetprotokoll (IP) auf. Weiterführende Informationen unter: <http://www.selflinux.org/selflinux/html/osi.html> [12.08.2008, 22:47]

Release: Die für den Produktiveinsatz freigegebene Version einer Software

Release Candidate: Stadium der Programmierarbeit kurz vor Veröffentlichung der finalen bzw. stabilen Version.

⁶ Weiterführende Informationen unter: <http://www.easy-network.de/dyndns-einrichten.html> [12.08.2008, 22:50]

⁷ Weiterführende Informationen unter: <http://www.netplanet.org/aufbau/nat.shtml> [12.08.2008, 19:07]



VPN: Siehe Kapitel [Definition „VPN“](#)

11 Abbildungsverzeichnis

Folgende Abbildungen wurden ausschließlich vom Autor erstellt. Detaillierte Angaben zur abgebildeten Software sind dem gesamten Dokument zu entnehmen.

Abbildung 1: Schema des VPN-Tunnels durch LAN, Router und Internet.....	5
Abbildung 2: Statischen Schlüssel erstellen.....	7
Abbildung 3: Eigenschaften von "OpenVPN Service".....	10
Abbildung 4: VPN-Tunnel starten.....	11
Abbildung 5: Erfolgsmeldung nach Tunnelaufbau beim Client.....	11

12 Tabellenverzeichnis

Tabelle 1: Zeitplan für den Aufbau einer VPN-Verbindung mittels OpenVPN.....	12
--	----

13 Quellenverzeichnis

13.1 Internetseiten

- Freifunk Wiki: OpenVPN Howto. http://wiki.freifunk.net/OpenVPN_Howto
[09.08.2008, 15:06]
- Humboldt-Universität Informatik: OpenVPN (deutsch).
[http://sarwiki.informatik.hu-berlin.de/OpenVPN_\(deutsch\)](http://sarwiki.informatik.hu-berlin.de/OpenVPN_(deutsch)) [12.08.2008, 22:38]
- Kröner, Tim: Definition VPN. <http://www.voip-information.de/vpn/definition-vpn.html> [09.08.2008, 16:48]
- Online-tutorials.net: OpenVPN Tutorial. <http://www.online-tutorials.net/security/openvpn-tutorial/tutorials-t-69-209.html#routing>
[13.08.2008, 19:40]

13.2 Bildquellen

Seitenzahlen der Abbildungen siehe Kapitel 11 „Abbildungsverzeichnis“. Quellen wie folgt:



Abbildung 1: Angefertigt durch den Author.

Abbildung 2: Screenshot angefertigt durch den Author. Zeigt Programmausschnitt der Software OpenVPN.

Abbildung 3 - 5: Screenshots angefertigt durch den Author. Zeigen Teile des Betriebssystems Microsoft Windows XP Home Tablet Edition.

Abbildung im Fußbereich jeder Seite: <http://i.creativecommons.org/l/by-sa/3.0/88x31.png>, Übersicht: <http://creativecommons.org/about/licenses>

