

---

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b> .....	<b>1</b>
1.1	VPNs von der Antike bis heute .....	3
1.2	Eine sich ändernde Welt benötigt sichere Kommunikation ...	3
<b>2</b>	<b>Überlegungen zu VPN-Design und -Komponenten</b> .....	<b>7</b>
2.1	Es muss nicht immer ein VPN sein! .....	7
2.2	Authentifikation und Autorisation .....	10
2.3	Netzwerkarchitektur .....	11
2.4	VPN-Technologie .....	12
<b>3</b>	<b>Netzwerk ist nicht gleich Netzwerk</b> .....	<b>15</b>
3.1	Das ISO/OSI-Schichtenmodell .....	15
3.2	Routing und Bridging .....	17
3.3	Paketlängen und Fragmentierung .....	19
<b>4</b>	<b>Klassische Angriffe und deren Abwehr</b> .....	<b>23</b>
4.1	Die vier Grundpfeiler für sichere Kommunikation .....	23
4.1.1	Vertraulichkeit ( <i>Confidentiality</i> ) .....	23
4.1.2	Authentisierung ( <i>Authentication</i> ) .....	24
4.1.3	Integrität ( <i>Integrity</i> ) .....	25
4.1.4	Nachweisbarkeit ( <i>Non-repudiation</i> ) .....	26
4.2	Täuschen, Tarnen und Übernehmen .....	26
4.2.1	Mitlesen von Passwörtern: <i>Data-Sniffing</i> mit <i>MAC-Flooding</i> .....	26
4.2.2	ARP-Poisoning / ARP-Spoofing .....	27
4.2.3	IP-Spoofing .....	29
4.2.4	DoS-Attacken .....	30
<b>5</b>	<b>OpenVPN: Die Open-Source-Alternative</b> .....	<b>33</b>
5.1	Ein Blick zurück zur Motivation .....	33
5.2	Schlüsselaustausch mit <i>Transport Layer Security (TLS)</i> .....	36
5.2.1	OpenSSL .....	39
5.2.2	Erwerbbarer Zertifikate .....	43
5.3	Verschlüsselungsverfahren .....	44

5.4	Virtuelle Netzwerkschnittstellen.....	46
5.4.1	Das Tunnelprinzip .....	46
5.4.2	Hilfsmittel der Abstraktion: <i>tun</i> - und <i>tap</i> -Geräte .....	47
5.5	Kontroll- und Datenkanäle .....	50
5.6	Betriebsmodi: Server, Client, Point-to-Point und Server Mode .....	51
5.6.1	Point-to-Point .....	51
5.6.2	Server Mode.....	52
<b>6</b>	<b>Verwaltung einer Certificate Authority .....</b>	<b>55</b>
6.1	Wofür eine CA? .....	55
6.2	Anforderungen an eine CA .....	56
6.3	Einrichtung von OpenSSL .....	57
6.4	Erstellung einer einfachen CA .....	59
6.4.1	Linux.....	59
6.4.2	Windows.....	63
6.5	Hierarchische CAs .....	66
6.5.1	Erstellung der hierarchischen CA .....	67
6.5.2	Verwendung der hierarchischen CA mit OpenVPN ...	70
<b>7</b>	<b>Installation.....</b>	<b>73</b>
7.1	Linux .....	73
7.2	Windows .....	76
7.2.1	Windows-Installation mit OpenVPN GUI .....	77
7.2.2	<i>tun/tap</i> -Treiber für Windows.....	78
7.2.3	OpenVPN-Windows-Dienst .....	78
7.2.4	Automatischer Start von OpenVPN ohne Administratorrechte.....	79
7.3	Mac OS X .....	80
7.4	BSD-basierte Systeme .....	82
7.4.1	Virtuelle Interfaces .....	84
7.4.2	Routing und Bridging .....	84
<b>8</b>	<b>Aufbau einer Verbindung .....</b>	<b>87</b>
8.1	Der erste OpenVPN-Tunnel: <code>Hello Network!</code> .....	87
8.1.1	Erstellen der Zertifikate .....	89
8.1.2	Installation und Konfiguration des VPN-Servers .....	89
8.1.3	Clientkonfiguration .....	93
8.1.4	Der erste Verbindungsaufbau aus dem Blickwinkel des Servers .....	95
8.1.5	Der erste Verbindungsaufbau aus der Sichtweise des Clients .....	97
8.2	Sicher ist sicher: Redundante Server .....	99

8.3	Der Trick mit den /30-Subnetzen bei <i>Server-Mode</i> -Konfigurationen .....	103
8.4	Bandbreitenoptionen .....	105
8.4.1	Kompression .....	106
8.4.2	Limitierung .....	107
8.5	Optionen für abgebrochene oder ungenutzte Verbindungen ..	108
8.5.1	Automatischer Abbau einer ungenutzten Verbindung ..	109
8.5.2	Signalisierung des Verbindungsabbaus .....	110
8.6	Benutzerprofile und Adresspools .....	110
8.6.1	Adresspools für Routing und Bridging .....	110
8.6.2	Persistenz mit Hilfe von Zertifikaten: <i>client-config-dir</i> und Co. ....	112
8.6.3	Verbindung ohne besondere Privilegien: <i>duplicate-cn</i> ..	114
8.6.4	Adresszuweisung mittels <i>DHCP</i> .....	115
8.7	Übergabe von Parametern an den Tunnelpartner .....	117
8.7.1	Modifikation des Routings auf dem <i>Client</i> .....	119
8.7.2	Modifikation des Routings auf dem <i>Server</i> .....	120
8.7.3	Default-Gateways und <i>Split Tunneling</i> .....	122
8.7.4	Push-Optionen für spezifische <i>Clients</i> .....	124
8.8	Änderung der Netzwerkeigenschaften .....	124
8.8.1	Paketgrößen .....	124
8.8.2	<i>Type of Service</i> .....	128
8.8.3	Socket-Eigenschaften .....	128
<b>9</b>	<b>Authentisierung: Preshared Keys, Zertifikate &amp; Co. ....</b>	<b>131</b>
9.1	OpenVPN mit <i>Preshared Keys</i> (PSK) .....	131
9.2	Zertifikate und eine eigene CA .....	133
9.3	Authentisierung durch einen <i>RADIUS</i> -Server .....	134
9.3.1	Konfiguration eines <i>RADIUS</i> -Servers .....	135
9.3.2	Einrichtung des <i>RADIUS</i> -Plugins für PAM .....	137
9.3.3	Benutzung des PAM-Plugins in OpenVPN .....	138
9.4	Limitierte Gültigkeit des Passworts .....	139
<b>10</b>	<b>Management .....</b>	<b>143</b>
10.1	Managementinterface .....	143
10.1.1	Verfügbare Kommandos .....	145
10.2	Logging .....	148
10.3	Accounting mit <i>client-connect</i> -Skripten .....	149
<b>11</b>	<b>Weitere Sicherheitsoptionen .....</b>	<b>155</b>
11.1	Isolierung in einer <i>chroot</i> -Umgebung .....	155
11.2	<i>openvpn-down-root</i> .....	157
11.3	Optionen für den TLS-Modus .....	158

11.4	Kanalverschlüsselungsoptionen .....	170
11.5	Unterstützung durch Firewalls .....	177
11.5.1	Unterschied bei Routing und Bridging .....	178
11.5.2	Achtung bei <code>client-to-client</code> .....	179
11.6	DoS-Angriffe .....	179
<b>12</b>	<b>OpenVPN im Firmeneinsatz .....</b>	<b>181</b>
12.1	Kostengünstige Verbindung von Standorten .....	181
12.2	Beispiel für Bridging: Hilfe beim Umzug von Standorten ....	182
12.3	Überwindung von Barrieren beim Feldeinsatz .....	189
12.3.1	Network Address Translation (NAT) .....	189
12.3.2	Firewalls & Proxys .....	189
12.4	Integration von OpenVPN in ein Windows-Netzwerk .....	190
12.4.1	Konfiguration der Linux-Firewall .....	191
12.4.2	Installation des OpenVPN-Servers .....	192
12.4.3	Verwenden der Serverzertifikate einer OWA-Installation	192
12.4.4	Installation der Clients: OpenVPN GUI .....	194
<b>13</b>	<b>OpenVPN im Hausgebrauch .....</b>	<b>197</b>
13.1	Sicheres WLAN: Achtung, <i>Joe on the Road!</i> .....	197
13.1.1	OpenVPN auf Embedded-Systemen mit OpenWRT ..	201
13.2	Punkt-zu-Punkt-Kommunikation über klassische Barrieren ..	202
13.3	Die LAN-Party mit OpenVPN – Zocker-VPN .....	206
13.3.1	Linux-Clients .....	208
<b>14</b>	<b>Troubleshooting von OpenVPN .....</b>	<b>209</b>
14.1	Keine Verbindung .....	209
14.1.1	Initialization Sequence Completed – trotzdem arbeitet der Tunnel nicht .....	209
14.1.2	Login bricht mit <i>VERIFY ERROR</i> nach der Kennwort- eingabe ab .....	212
14.1.3	Unerwarteter Connection Reset unter Windows .....	212
14.1.4	Unroutable control packet received ....	213
14.1.5	Bad LZ0 decompression header byte: 243	214
14.2	Schlechter Durchsatz .....	215
14.3	Keine Verbindung durch <i>Network Address Translation</i> .....	217
14.4	Kein Zugriff auf andere Clients .....	219
14.4.1	Kein Zugriff auf andere OpenVPN-Clients am Server .	220
14.4.2	Kein Zugriff auf Rechner im Subnetz des OpenVPN- Gateways .....	220
14.4.3	Unter Windows werden keine Computer in der Netz- werkumgebung angezeigt .....	221

---

14.5	Programme zur Fehlersuche .....	222
14.5.1	<code>tcpdump</code> .....	222
14.5.2	Ethereal .....	223
14.5.3	<code>ping</code> .....	225
14.5.4	<code>traceroute</code> .....	226
14.5.5	Paketfilter <code>iptables</code> .....	227
<b>15</b>	<b>OpenVPN-Development .....</b>	<b>231</b>
15.1	Das Plugin-System von OpenVPN .....	231
15.2	Beispiel-Plugin <code>pgauth</code> .....	240
15.3	Kompilierung des Plugins und Stolpersteine .....	245
<b>16</b>	<b>Ausblick auf OpenVPN 2.1 .....</b>	<b>249</b>
16.1	Port Sharing - Forwarding von Verbindungen zu anderen lokalen Diensten .....	249
16.2	Mehrzeilige Parameterlisten .....	250
16.3	Automatische Erkennung von Proxy-Einstellungen .....	250
16.4	OpenVPN als Windows-Service ohne Administratorrechte ...	250
16.5	Inline-Zertifikate .....	251
16.6	<code>topology</code> .....	251
<b>A</b>	<b>OpenVPN-Ressourcen im Internet .....</b>	<b>253</b>
A.1	Websites .....	253
A.2	Mailinglisten .....	253
A.3	Foren und IRC .....	254
<b>B</b>	<b>Skripte fürs Bridging .....</b>	<b>255</b>
B.1	<code>bridge-start</code> von <code>bridge_a</code> .....	255
B.2	<code>bridge-start</code> von <code>bridge_b</code> .....	256
B.3	<code>bridge-stop</code> für <code>bridge_a</code> und <code>bridge_b</code> .....	257
	<b>Abbildungsverzeichnis .....</b>	<b>259</b>
	<b>Literaturverzeichnis .....</b>	<b>263</b>
	<b>Index .....</b>	<b>267</b>