

OpenVPN - Die IPsec Alternative

Kurs 1017

© 2007-2011 OpenSource Training Ralf Spenneberg

Am Bahnhof 3 - 5

48565 Steinfurt

<http://www.opensource-training.de>

<http://www.os-t.de>

Copyright

Die in diesem Kurs zur Verfügung gestellten Folien, Unterlagen und Übungen sind urheberrechtlich geschützt. Wir behalten uns alle Rechte vor, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung ist nicht erlaubt.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit genutzt. Fast alle Hardware- und Softwarebezeichnungen, die in dieser Unterlage erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen.

Bei der Zusammenstellung der Texte und Abbildungen wurde mit größter Sorgfalt vorgegangen. Jedoch können Fehler nicht vollständig ausgeschlossen werden. Die Firma OpenSource Training Ralf Spenneberg kann für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind wir dankbar.

Inhaltsverzeichnis

1	Einführung	5
1.1	Installation	7
1.2	Start	9
1.3	Konfiguration	11
2	Einfacher Tunnel	13
2.1	Konfiguration des einfachen Tunnels	15
3	Erweiterungen	19
3.1	Kompression	19
3.2	Verbindungsabbrüche	21
3.3	Rechte	23
4	Zertifikate	25
4.1	Verschlüsselung	27
4.2	Einsatz von Zertifikaten	31
4.3	Aufbau einer Public Key Infrastructure	33
4.3.1	Erzeugung einer eigenen CA	35
4.3.2	Erzeugung von Server-Zertifikaten	37
4.3.3	Erzeugung von Client-Zertifikaten	39
4.4	Zertifikate im OpenVPN-Einsatz	41
4.5	Erkennung von Man in the middle-Angriffen	43
5	Automatische Zuweisung von IP-Adressen	45
5.1	Dynamische IP-Adressen	45
5.2	Persistente IP-Adressen	47
6	Benutzerspezifische Konfigurationen	49
7	Routing	53
7.1	Serverseitige Netze	55
7.2	Clientseitige Netze	57
7.3	Default-Gateway	59
8	Windows Clients	61
9	Einsatz von Smartcards/ Tokens	65
9.1	Public Key Cryptography Standards (PKCS)	67
9.2	PKCS-Standards	67
9.3	Werkzeuge für Smartcards	69

- 10 Fortgeschrittene Funktionen** **71**
- 10.1 Widerruf von Zertifikaten 73
- 10.2 Benutzerauthentifizierung mit Plugins 75
- 10.3 Benutzerauthentifizierung mit Skripten 77
- 10.4 DHCP-Optionen 79
- 10.5 Bandbreitenregulation 81
- 10.6 Clientverbindungen 83
- 10.7 Skripte bei IP-Änderungen 85
- 10.8 Lastverteilung 89
- 10.9 Hochverfügbarkeit 91
- 10.10 Proxy 93
- 10.11 Port-Sharing 95

- 11 Bridging** **97**

- 12 Management-Schnittstelle** **99**
- 12.1 Einrichten der Managementschnittstelle 99
- 12.2 Kommandos der Managementschnittstelle 101

- 13 Serverbasierte OpenVPN Verwaltung** **105**
- 13.1 OpenVPN Access Server 107

Index

- .conf, 11
- .ovpn, 11
- /dev/shm, 78
- \$bytes_received, 86
- \$bytes_sent, 86
- \$common_name, 86

- Access Server, 107
- add, 87
- asymmetrische Verschlüsselung, 27
- auth-user-pass, 78
- auth-user-pass-verify, 78, 87
- Authentifizierung
 - accountbasierte, 75
 - Kennwort, 13
 - Smartcard, 65
 - static Key, 14

- Bridging, 97
- bypass-dhcp, 60
- bypass-dns, 60
- bytecount, 102

- CA erstellen, 35
- Certificate-Revocation-List, 73
- client-config-dir, 86
- client-connect, 86
- client-disconnect, 86
- Client-Zertifikat, 39
- CryptoAPI, 65

- Dateien
 - /etc/openvpn/, 11
- deb-Paket, 7
- def1, 60
- delete, 87
- dev
 - tun, 15
- DHCP, 79
- Diffie-Hellman, 27
- down, 85
- down-pre, 85
- Dual Authentication, 75

- easy-rsa, 33
 - revoke-full, 73
- Eurephia, 76
- execve, 78

- Gateway, 59

- HA, 6, 91

- ifconfig, 45
- ifconfig-pool-linear, 46
- init, 86
- Installation, 7
- IP-Forwarding, 55
- ipchange, 86

- keepalive, 87
- Kompression, 6, 19
- Konfiguration, 11

- Lastverteilung, 6, 89
- link-mtu, 86
- local, 59
- LZO, 8

- Man in the middle, 43
- Management-Schnittstelle, 101, 102
 - auth-retry, 102
 - client-auth, 103
 - client-auth-nt, 103
 - client-deny, 103
 - client-kill, 103
 - client-pf, 103
 - exit, 101
 - forget-passwords, 102
 - help, 101
 - hold, 101
 - kill, 101
 - log, 101

- mute, 101
- need-ok, 103
- needstr, 103
- net, 102
- password, 102
- pid, 102
- pkcs11-id-count, 103
- pkcs11-id-get, 103
- signal, 102
- state, 102
- status, 102
- username, 102
- verb, 102
- MTU, 86
- Netzwerkkonfiguration, 45
 - Userspezifisch, 49
- OpenSC, 68
- OpenSSL, 8
- OpenVPN
 - Access Server, 107
 - GUIs, 61
 - Hintergrundprozess, 24
 - Management-Schnittstelle, 101, 102
 - starten , 9
- openvpn
 - genkey, 14
 - secret, 14
- openvpn-auth-ldap, 76
- openvpn-auth-pam, 75, 76
- Parameter
 - dh, 41
 - ca, 41
 - cert, 41
 - client, 45
 - client-config-dir, 49
 - client-to-client, 83
 - comp-lzo, 20
 - crl-verify, 73
 - cyrptoapicert, 66
 - daemon, 24
 - dev, 15
 - dev tap, 97
 - group, 24
 - http-proxy, 93
 - ifconfig, 15
 - ifconfig-pool-persist, 47
 - iroute, 57
 - keepalive, 22
 - key, 41
 - management, 99
 - client-auth, 100
 - forget-disconnect, 100
 - hold, 100
 - log-cache, 100
 - query-passwords, 100
 - signal, 100
 - mode, 41
 - ns-cert-type, 43
 - persist-key, 24
 - persist-tun, 24
 - ping-timer-rem, 22
 - pkcs11, 68
 - id, 68
 - id-type, 68
 - providers, 68
 - slot, 68
 - slot-type, 68
 - proto, 93
 - tcp, 93
 - pull, 55
 - push, 55
 - random-remote, 89
 - redirect-gateway, 59
 - remote, 15
 - remote-cert-tls, 43
 - route, 57
 - server, 45
 - server-bridge, 97
 - shaper, 81
 - tls-client, 42
 - tls-server, 41
 - user, 24
- pcscd, 68

Perfect Forward Secrecy, 13

Persistenz, 47

PKCS11, 67

PKCS12, 67

PKCS15, 67

PKI, 33

Plattformen, 5

Private Key, 25

Proxy, 93

Public Key, 25

redirect-gateway, 59

remote, 15

restart, 86

Revocation-List, 73

Routing, 53

rpm-Paket, 7

script-security, 77

Server-Zertifikat, 37

Smartcard, 6, 65

Start, 9

static Key, 13

symmetrische Verschlüsselung, 27

system, 78

tap, 86

TCPDump, 17

Telnet-Schnittstelle, 101, 102

tls-verify, 86

tmp-dir, 78, 86

topology, 46

Traffic Shaping, 6, 81

tun, 15, 46, 85

Tunnel testen, 17

up, 85

up-restart, 85

update, 87

USBauth, 76

User, 23

Verbindungsabbruch, 21

Verschlüsselung

asymmetrisch, 27, 29

symmetrisch, 27

via-env, 78

via-file, 78

Wireshark, 17

Zertifikate, 25, 31

Eigenschaften, 26

Widerruf, 73

Zertifikate mit OpenVPN, 41