

OpenVPN mit CAcert

Graben eines VPN-Tunnels mittels
freien Zertifikaten

OpenVPN mit CAcert

Veranstalter: Linux User Group Ravensberg

Referent: Ralf Neumann

3.5.2007

OpenVPN mit CAcert

Eine kleine Einweisung mit Demonstration (so GPRS/UMTS uns gnädig ist) in 4 Akten

Ausgangssituation

Server-Seite

- Linux-Box
- 192.168.1.1
- meinekiste.dyndns.org
- Eigenständiger Router
- VPN-Netzwerk
10.1.1.0/24

Client-Seite

- Windows-Kiste
- beliebige IP (ausser
10.1.1.x) fest oder per
DHCP

Das Ziel

Sicher und komfortabel von überall aus ins eigene Netz gelangen!

VPN-Möglichkeiten

- IP-Sec Übelst einzurichten
- MS PPTP Unsicher (MS!)
- Hamachi Vertrauen? Udp-punch?
- OpenVPN ...

OpenVPN ist einfach

GENIAL!

Warum?

- Bewährte Technologien (SSL/TLS)
- Skalierbare Sicherheit (PSK/Auth/PKI)
- 1 Port (frei wählbar, udp/tcp)
- Portierbar (Linux/OSX/win32)
- Einfach zu konfigurieren
- Hervorragend dokumentiert
- Routing (einfacher) / Bridging (effizienter)
- Cool: OpenVPN für Fritz-Box / PocketPC

1. Akt (Prelude)

Voraussetzungen schaffen

Voraussetzungen allgemein

- DynDNS-Account eingerichtet
- Router registriert *meinekiste.dyndns.org*
- Postfach vpnuser@meinekiste.dyndns.org ist abrufbar
- CAcert-Account ist angelegt und verfügt über ausreichend Assurance-Punkte
- Email-Adresse (s.o.) ist verifiziert

Voraussetzungen Server

- Server: OpenSSL und OpenVPN installiert
- Firewall für VPN-Subnetz geöffnet, z.b.
**iptables -A FORWARD -i tun0 -s 10.1.1.0/24
-d 192.169.1.0/24 -j ACCEPT**

Voraussetzungen Client

- Win-Client: OpenVPN-Gui installiert (enthält OpenSSL)
- (Linux-Client: OpenSSL/OpenVPN installiert)

Vorraussetzungen Router

- Forward-Regel für Port 1194 (tcp oder udp) vom Router zum VPN-Server

2. Akt

Der Server

Vorbereitungen Server

```
cd /etc/openvpn  
mkdir cacert  
cd cacert  
mkdir certs private  
chmod 0700 private  
cd certs  
wget http://www.cacert.org/certs/root.crt
```

Server-Zertifikat erzeugen 1/2

- **/etc/openvpn/cacert**
- (neues) Zertifikat für *meinekiste.dyndns.org* erzeugen
- Hierzu www.cacert.org, einloggen -> server certificate -> new
- Class1 auswählen
- Certificate Signing Request (CSR)
- **openssl req -new -newkey rsa:1024 -out certs/servercsr.pem -nodes -keyout private/serverkey.pem**

Server-Zertifikat erzeugen 2/2

- Wichtig: CN 'common name':
meinekiste.dyndns.org
- **servercsr.pem** mittels c&p in das Feld CSR komplett einfügen
- Resultat per c&p komplett in **servercert.pem** einfügen
- CSR löschen
- Diffie-Hellmann Parameter erzeugen:
openssl dhparam -out dh1024.pem 1024

Beispielkonfiguration Server

```
port 1194
#port 443
proto tcp
dev tap
ca /etc/openvpn/cacert/certs/root.crt
cert /etc/openvpn/cacert/certs/servercert.pem
key /etc/openvpn/cacert/private/serverkey.pem
dh /etc/openvpn/dh1024.pem
server 10.1.1.0 255.255.255.0
ifconfig-pool-persist /etc/openvpn/ipp.txt
push "route 192.168.1.0 255.255.255.0"
keepalive 10 30
auth SHA1
cipher BF-CBC
user nobody
group nobody
persist-key
persist-tun
log      openvpn.log
verb 3
mute 10
```

Spezial-Konfiguration Server

Kompletter Traffic durch den Tunnel leiten,
hierzu Server-Konfiguration erweitern um:

```
push "redirect-gateway def1"  
push "dhcp-option DNS 10.1.1.1"
```

Server-Firewall nicht vergessen:

```
iptables -t nat -A POSTROUTING -s  
10.1.1.0/24 -o eth0 -j MASQUERADE
```

3. Akt

Der Client

Client-Zertifikat erzeugen 1/2

- (neues) Zertifikat für vpnuser@meinekiste.dyndns.org erzeugen
- Hierzu www.cacert.org, einloggen -> client certificate -> new
- Class1, 1024 erzeugen
- Dieses wird im Zertifikat-Speicher des Browsers gehalten
- Von dort aus exportieren als *client-cacert.p12*

Client-Zertifikat erzeugen 2/2

- **openssl pkcs12 -in client-cacert.p12 -clcerts -out client-cacert.pem**
- .p12 löschen

Beispielkonfigurationen Client

- Klassischer LAN-Tunnel
- WAP-Tunnel (O2 Genion mit WAP-Flatrate für 5 EUR/Monat) (port 443 !!!)

LAN-Tunnel.ovpn

```
client
dev tap
dev-node OpenVPN
proto tcp
remote meinekiste.dyndns.org 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca root.crt
cert client-cacert.pem
key client-cacert.pem
auth SHA1
cipher BF-CBC
verb 4
mute 20
```

WAP-Tunnel.ovpn

```
client
dev tap
dev-node OpenVPN
proto tcp
remote meinekiste.dyndns.org 443
resolv-retry infinite
nobind
persist-key
persist-tun
http-proxy-retry 5
http-proxy 195.182.114.52 8080
http-proxy-option AGENT Mozilla/4.1 (compatible; MSIE 5.0; Symbian OS; Series
60;452) Opera 6.20 [de]
ca root.crt
cert client-cacert.pem
key client-cacert.pem
auth SHA1
cipher BF-CBC
verb 4
mute 20
```

4. Akt (Finale)

„Action!“

Links & Literatur

- www.openvpn.net
- www.cacert.org
- www.openvpn.se

Server/Client/howto
Zertifikate
OpenVPN-GUI

- OpenVPN
(Grundlagen,
Konfiguration,
Praxis)

ISBN 3-89864-396-4