VPN mit OpenVPN

1. Aufgabenstellung

Es soll OpenVPN aufgesetzt und konfiguriert werden.

2. Implementation

Wir haben uns dazu entschieden, OpenVPN auf Willinger's VPS, basierend auf Debian Wheezy, zu installieren.

Dieser wird in einem Rechenzentrum in Deutschland gehostet und hat eine öffentliche IP Adresse: 5.45.97.122.

Außerdem haben wir vollständige Root-Rechte, daher wurden die folgenden Schritte auch als root ausgeführt.

Installation

Die Installation ist auf Debian recht einfach:

```
apt-get install openvpn
```

Apt lädt damit alle Abhängigkeiten und OpenVPN selbst herunter und installiert diese.

Nun kann mit der Konfiguration fortgefahren werden.

Konfiguration

Zuallererst legt man ein neues Verzeichnis in /etc an, um die OpenVPN Konfigurations- dateien und Keys zu speichern.

```
mkdir -p /etc/openvpn/easy-rsa/
```

Im nächsten Schritt muss easy-rsa selbst kopiert werden:

```
cp -R /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
# In das easy-rsa Verzeichnis wechseln
cd /etc/openvpn/easy-rsa/
```

Und die vars Datei bearbeitet werden.

Diese beinhaltet die Variablen, die bei der Key/CA-Erstellung verwendet werden.

```
vi vars
```

```
export KEY_COUNTRY="DE"
export KEY_PROVINCE="Hessen"
export KEY_CITY="Frankfurt am Main"
export KEY_ORG="MyORG"
export KEY_EMAIL="awi95@gmx.at"
export KEY_CN="vpn.f-o-g.eu"
```

```
export KEY_NAME=""
export KEY_OU=""
```

Speichern und im folgenden, die Datei "sourcen" und die CA (Certificate Authority) erzeugen.

```
# Sourcen
. ./vars
./clean-all
# CA erzeugen
./build-ca
```

Dort kann man alle Werte auf Standard lassen, da diese sowieso aus der vars Datei, siehe oben, gelesen werden.

Lediglich der Common Name sollte, falls nötig, angepasst werden (in unserem Fall haben wir auch diesen in der vars gesetzt).

Jetzt kann der Server Key erzeugt werden:

```
./build-key-server vpn.f-o-g.eu
```

Hier auch den Common Name anpassen (wobei dieser von dem Aufrufparameter übernommen werden sollte).

Beide Fragen (Sign/Commit) mit yes beantworten.

Im Anschluss noch den Key für einen Client erzeugen. Diesen Befehl muss man für jeden Client ausführen, dem man VPN Zugriff geben will.

Logischerweise muss man den Parameter/CN anpassen.

```
./build-key client1
```

Hier die Daten des Clients eintragen und CN übernehmen.

Zum Schluss muss noch der Diffie-Helmann (DH) Key erzeugt werden.

```
# Erfordert keine Eingaben
./build-dh
```

Der folgende Schritt ist nicht zwingend, aber wir wollten alle Keys auf einem Ort haben.

```
# Kopiert alle Key Dateien in /etc/openvpn/keys
mkdir /etc/openvpn/keys
cp ./keys/*.crt /etc/openvpn/keys
cp ./keys/*.key /etc/openvpn/keys
cp ./keys/*.pem /etc/opnevpn/keys
```

Der Server selbst braucht auch noch eine Konfigurationsdatei, diese wird server.conf genannt und sieht bei uns wie folgt aus:

```
cd ..
vi server.conf
```

```
# IP Adresse auf der der Server lauschen soll
local 5.45.97.122
port 1194
# Kann auch TCP verwenden
proto udp
# Bridged Netzwerk
dev tap
# Pfade zu den Keys definieren (von build-ca/build-key-server)
ca keys/ca.crt
cert keys/vpn.f-o-g.eu.crt
key keys/vpn.f-o-g.eu.key  # This file should be kept secret
dh keys/dh2048.pem
# Server vergibt an Client 10.8.0.0/24 Adressen
server 10.8.0.0 255.255.255.0
# Nicht unbedingt notwendig
# Sorgt dafür, dass Clients immer dieselbe IP erhalten
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
# Wird benötigt, um den gesamten Internetverkehr von Clients
# über den VPN tunnel zu routen
push "redirect-gateway def1 bypass-dhcp"
# Clients können sich untereinander erreichen
client-to-client
keepalive 10 120
# Art der Verschlüsselung
cipher AES-256-CBC
# Kompression aktivieren
comp-lzo
max-clients 100
# OpenVPN server als Rechte-loser Benutzer ausführen
user nobody
group nogroup
# Erlaubt neustarts mit SIGUSR1 Signalen, wenn (wie oben zu sehen) user nobody
# verwendet wird.
# Es persisiert dazu die Keys über server neustarts hinweg
persist-key
# TUN/TAP Device nicht neustarten wenn SIGUSR1 Signal ausgelöst wird
persist-tun
# Status logging
status openvpn-status.log
log /var/log/openvpn.log
verb 3
```

Weitere Schritte

Damit Clients auch Internetzugriff haben, muss noch IP Forwarding eingeschaltet werden und eine Firewall Regel hinzugefügt werden.

```
# Forwarding sofort aktivieren
echo 1 > /proc/sys/net/ipv4/ip_forward
# Forwarding auch nach Server neustart einschalten
vi /etc/sysctl.conf
# Dort folgende Zeile anpassen:
```

```
net.ipv4.ip_forward=1

# Firewall Regel
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Die Konfiguration des Servers ist damit abgeschlossen.

Konfiguration Client

Auf Client-Seite kann unter Windows die OpenVPN GUI verwendet werden.

Diese speichert ihre Konfigurationsdateien in C:Program FilesOpenVPNconfig (vorausgesetzt, man hat den Installationspfad nicht geändert).

Vom Server müssen die Dateien ca.crt, client1.key, client1.crt kopiert werden und eine <Verbindungsname>.ovpn Datei erzeugt werden.

In unserem Fall, FoG VPN.ovpn, mit folgendem Inhalt:

```
# Gibt an, dass diese Konfiguration für einen Client ist
client

# IP/Hostname vom Server
remote 5.45.97.122 1194
proto udp

# Pfad zu den Zertifikaten
ca ca.crt
cert client1.crt
key client1.key
ns-cert-type server
cipher AES-256-CBC

dev tap

resolv-retry infinite

nobind

# Bedeuten dasselbe wie am Server
persist-key
persist-tun
user nobody
group nogroup

comp-lzo

verb 4

mute 20

# Damit der DNS gesetzt werden kann (und diverse andere Optionen)
pull dhcp-options
status openvpn-status.log
```

Wichtig: unter Windows MUSS die OpenVPN GUI als Administrator gestartet werden. Ansonsten ist es nicht möglich, das tunneling ordentlich einzurichten.

Starten

Unter Debian kann OpenVPN mittels "service" gestartet werden.

```
service openvpn start
```

Clients brauchen nun nur noch ihre Zertifikate und eine Client Konfiguration. Siehe dazu Abschnitt nach Client Key Generierung oben.

Testen

Client log:

```
Wed Mar 18 11:20:03 2015 NOTE: --user option is not implemented on Windows
Wed Mar 18 11:20:03 2015 NOTE: --group option is not implemented on Windows
Wed Mar 18 11:20:03 2015 Current Parameter Settings:
Wed Mar 18 11:20:03 2015   config = 'FoG VPN.ovpn'
Wed Mar 18 11:20:03 2015   mode = 0
Wed Mar 18 11:20:03 2015   show_ciphers = DISABLED
Wed Mar 18 11:20:03 2015   show_digests = DISABLED
Wed Mar 18 11:20:03 2015   show_engines = DISABLED
Wed Mar 18 11:20:03 2015   genkey = DISABLED
Wed Mar 18 11:20:03 2015   key_pass_file = '[UNDEF]'
Wed Mar 18 11:20:03 2015   show_tls_ciphers = DISABLED
Wed Mar 18 11:20:03 2015 Connection profiles [default]:
Wed Mar 18 11:20:03 2015   proto = udp
Wed Mar 18 11:20:03 2015   local = '[UNDEF]'
Wed Mar 18 11:20:03 2015   local_port = 0
Wed Mar 18 11:20:03 2015   remote = '5.45.97.122'
Wed Mar 18 11:20:03 2015   remote_port = 1194
Wed Mar 18 11:20:03 2015   remote_float = DISABLED
Wed Mar 18 11:20:03 2015   bind_defined = DISABLED
Wed Mar 18 11:20:03 2015   bind_local = DISABLED
Wed Mar 18 11:20:03 2015   connect_retry_seconds = 5
Wed Mar 18 11:20:03 2015   connect_timeout = 10
Wed Mar 18 11:20:03 2015 NOTE: --mute triggered...
Wed Mar 18 11:20:03 2015 265 variation(s) on previous 20 message(s) suppressed by --mute
Wed Mar 18 11:20:03 2015 OpenVPN 2.3.6 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [PKCS11] [IPv6] built on Dec  1 2014
Wed Mar 18 11:20:03 2015 library versions: OpenSSL 1.0.1j 15 Oct 2014, LZO 2.08
Wed Mar 18 11:20:03 2015 MANAGEMENT: TCP Socket listening on [AF_INET]127.0.0.1:25340
Wed Mar 18 11:20:03 2015 Need hold release from management interface, waiting...
Wed Mar 18 11:20:04 2015 MANAGEMENT: Client connected from [AF_INET]127.0.0.1:25340
Wed Mar 18 11:20:04 2015 MANAGEMENT: CMD 'state on'
Wed Mar 18 11:20:04 2015 MANAGEMENT: CMD 'log all on'
Wed Mar 18 11:20:04 2015 MANAGEMENT: CMD 'hold off'
Wed Mar 18 11:20:04 2015 MANAGEMENT: CMD 'hold release'
Wed Mar 18 11:20:04 2015 LZO compression initialized
Wed Mar 18 11:20:04 2015 Control Channel MTU parms [ L:1590 D:138 EF:38 EB:0 ET:0 EL:0 ]
Wed Mar 18 11:20:04 2015 Socket Buffers: R=[8192->8192] S=[8192->8192]
Wed Mar 18 11:20:04 2015 Data Channel MTU parms [ L:1590 D:1450 EF:58 EB:135 ET:32 EL:0 AF:3/1 ]
Wed Mar 18 11:20:04 2015 Local Options String: 'V4,dev-type tap,link-mtu 1590,tun-mtu 1532,proto UDPv4,comp-lzo,cipher AES-256-CBC,auth SHA1,keysize 256,key-method 2,tls-client'
Wed Mar 18 11:20:04 2015 Expected Remote Options String: 'V4,dev-type tap,link-mtu 1590,tun-mtu 1532,proto UDPv4,comp-lzo,cipher AES-256-CBC,auth SHA1,keysize 256,key-method 2,tls-server'
Wed Mar 18 11:20:04 2015 Local Options hash (VER=V4): 'c6c7c21a'
Wed Mar 18 11:20:04 2015 Expected Remote Options hash (VER=V4): '1a6d5c5d'
Wed Mar 18 11:20:04 2015 UDPv4 link local: [undef]
Wed Mar 18 11:20:04 2015 UDPv4 link remote: [AF_INET]5.45.97.122:1194
Wed Mar 18 11:20:04 2015 MANAGEMENT: >STATE:1426674004,WAIT,,,
Wed Mar 18 11:20:04 2015 MANAGEMENT: >STATE:1426674004,AUTH,,,
Wed Mar 18 11:20:04 2015 TLS: Initial packet from [AF_INET]5.45.97.122:1194, sid=edb66dc8 d05ac84c
Wed Mar 18 11:20:05 2015 VERIFY OK: depth=1, C=DE, ST=Hessen, L=Frankfurt am Main, O=Fortress of Gamers, CN=vpn.f-o-g.eu, emailAddress=awi95@gmx.at
Wed Mar 18 11:20:05 2015 VERIFY OK: nsCertType=SERVER
Wed Mar 18 11:20:05 2015 VERIFY OK: depth=0, C=DE, ST=Hessen, L=Frankfurt am Main, O=Fortress of Gamers, CN=vpn.f-o-g.eu, emailAddress=awi95@gmx.at
Wed Mar 18 11:20:05 2015 Data Channel Encrypt: Cipher 'AES-256-CBC' initialized with 256 bit key
Wed Mar 18 11:20:05 2015 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed Mar 18 11:20:05 2015 Data Channel Decrypt: Cipher 'AES-256-CBC' initialized with 256 bit key
Wed Mar 18 11:20:05 2015 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed Mar 18 11:20:05 2015 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
Wed Mar 18 11:20:05 2015 [vpn.f-o-g.eu] Peer Connection Initiated with [AF_INET]5.45.97.122:1194
Wed Mar 18 11:20:06 2015 MANAGEMENT: >STATE:1426674006,GET_CONFIG,,,
Wed Mar 18 11:20:07 2015 SENT CONTROL [vpn.f-o-g.eu]: 'PUSH_REQUEST' (status=1)
Wed Mar 18 11:20:07 2015 PUSH: Received control message: 'PUSH_REPLY,dhcp-option DNS 8.8.8.8,dhcp-option DNS 8.8.4.4,redirect-gateway def1 bypass-dhcp,route-gateway 10.8.0.1,ping 10,ping-restart 120,ifconfig 10.8.0.4 255.255.255.0'
Wed Mar 18 11:20:07 2015 OPTIONS IMPORT: timers and/or timeouts modified
Wed Mar 18 11:20:07 2015 OPTIONS IMPORT: --ifconfig/up options modified
Wed Mar 18 11:20:07 2015 OPTIONS IMPORT: route options modified
Wed Mar 18 11:20:07 2015 OPTIONS IMPORT: route-related options modified
Wed Mar 18 11:20:07 2015 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Wed Mar 18 11:20:07 2015 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Wed Mar 18 11:20:07 2015 MANAGEMENT: >STATE:1426674007,ASSIGN_IP,,10.8.0.4,
Wed Mar 18 11:20:07 2015 open_tun, tt->ipv6=0
Wed Mar 18 11:20:07 2015 TAP-WIN32 device [LAN-Verbindung 2] opened: \\.\Global\{DD57EE48-0710-46F4-9052-CA8DD6752A50}.tap
Wed Mar 18 11:20:07 2015 TAP-Windows Driver Version 9.21
Wed Mar 18 11:20:07 2015 TAP-Windows MTU=1500
Wed Mar 18 11:20:07 2015 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.8.0.4/255.255.255.0 on interface {DD57EE48-0710-46F4-9052-CA8DD6752A50} [DHCP-serv: 10.8.0.0, lease-time: 31536000]
Wed Mar 18 11:20:07 2015 DHCP option string: 06080808 08080808 0404
Wed Mar 18 11:20:07 2015 Successful ARP Flush on interface [38] {DD57EE48-0710-46F4-9052-CA8DD6752A50}
Wed Mar 18 11:20:12 2015 TEST ROUTES: 1/1 succeeded len=0 ret=1 a=0 u/d=up
Wed Mar 18 11:20:12 2015 C:\Windows\system32\route.exe ADD 5.45.97.122 MASK 255.255.255.255 10.0.100.1
Wed Mar 18 11:20:12 2015 ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=10 and dwForwardType=4
Wed Mar 18 11:20:12 2015 Route addition via IPAPI succeeded [adaptive]
Wed Mar 18 11:20:12 2015 C:\Windows\system32\route.exe ADD 10.2.24.153 MASK 255.255.255.255 10.0.100.1
Wed Mar 18 11:20:12 2015 ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=10 and dwForwardType=4
Wed Mar 18 11:20:12 2015 Route addition via IPAPI succeeded [adaptive]
Wed Mar 18 11:20:12 2015 C:\Windows\system32\route.exe ADD 0.0.0.0 MASK 128.0.0.0 10.8.0.1
Wed Mar 18 11:20:12 2015 ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=20 and dwForwardType=4
Wed Mar 18 11:20:12 2015 Route addition via IPAPI succeeded [adaptive]
Wed Mar 18 11:20:12 2015 C:\Windows\system32\route.exe ADD 128.0.0.0 MASK 128.0.0.0 10.8.0.1
Wed Mar 18 11:20:12 2015 ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=20 and dwForwardType=4
Wed Mar 18 11:20:12 2015 Route addition via IPAPI succeeded [adaptive]
Wed Mar 18 11:20:12 2015 Initialization Sequence Completed
Wed Mar 18 11:20:12 2015 MANAGEMENT: >STATE:1426674012,CONNECTED,SUCCESS,10.8.0.4,5.45.97.122
```

Server log:

```
Wed Mar 18 11:19:57 2015 MULTI: multi_create_instance called
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 Re-using SSL/TLS context
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 LZO compression initialized
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 Control Channel MTU parms [ L:1590 D:138 EF:38 EB:0 ET:0 EL:0 ]
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 Data Channel MTU parms [ L:1590 D:1450 EF:58 EB:135 ET:32 EL:0 AF:3/1 ]
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 Local Options hash (VER=V4): '1a6d5c5d'
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 Expected Remote Options hash (VER=V4): 'c6c7c21a'
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 TLS: Initial packet from [AF_INET]84.114.180.113:5119, sid=8bcd9a90 4e20c046
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 VERIFY OK: depth=1, /C=DE/ST=Hessen/L=Frankfurt_am_Main/O=Fortress_of_Gamers/CN=vpn.f-o-g.eu/emailAddress=awi95@gmx.at
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 VERIFY OK: depth=0, /C=AT/ST=Wien/L=Wien/O=Fortress_of_Gamers/CN=1337-Laptop/emailAddress=awi95@gmx.at
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 Data Channel Encrypt: Cipher 'AES-256-CBC' initialized with 256 bit key
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 Data Channel Decrypt: Cipher 'AES-256-CBC' initialized with 256 bit key
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
Wed Mar 18 11:19:57 2015 84.114.180.113:5119 [1337-Laptop] Peer Connection Initiated with [AF_INET]84.114.180.113:5119
Wed Mar 18 11:19:57 2015 1337-Laptop/84.114.180.113:5119 MULTI_sva: pool returned IPv4=10.8.0.4, IPv6=1::1f00:0:c37f:0
Wed Mar 18 11:20:00 2015 1337-Laptop/84.114.180.113:5119 PUSH: Received control message: 'PUSH_REQUEST'
Wed Mar 18 11:20:00 2015 1337-Laptop/84.114.180.113:5119 send_push_reply(): safe_cap=960
Wed Mar 18 11:20:00 2015 1337-Laptop/84.114.180.113:5119 SENT CONTROL [1337-Laptop]: 'PUSH_REPLY,dhcp-option DNS 8.8.8.8,dhcp-option DNS 8.8.4.4,redirect-gateway def1 bypass-dhcp,route-gateway 10.8.0.1,ping 10,ping-restart 120,ifconfig 10.8.0.4 255.255.255.0' (status=1)
Wed Mar 18 11:20:00 2015 1337-Laptop/84.114.180.113:5119 MULTI: Learn: 00:ff:dd:57:ee:48 -> 1337-Laptop/84.114.180.113:5119
```