Einstellung von OpenVPN auf Servern mit Debian 8 Jessie

(23.8.2016) In diesem Artikel schreiten wir in unserer Miniserie über OpenVPN fort und erklären wir uns die Aktivierung von OpenVPN auf einem Linux-Server mit Debian 8. Lesen Sie unsere Anleitung durch und Sie werden Ihren virtuellen Server auch für den Aufbau eines verschlüsselten Tunnels ausnutzen können, der Sie mit Ihrem Ziel sicher verbinden wird.

Installierung von OpenVPN

In dem ersten Schritt müssen Sie natürlich Ihren Server mit der betreffenden Software ausstatten. In Linux ist die Installierung einfach. Sie brauchen das Paket OpenVPN nur mit der folgenden Befehlszeile zu implementieren:

```
apt-get install openvpn
```

Das ist alles.

Erstellung von Schlüsseln

Die Zertifizierungsstelle (CA – Certificate authority) und die Client-Zertifikate können Sie zwar in OpenSSL selbständig erstellen, aber Sie können sich auch nutzvoller Skripts bedienen und sich die Arbeit vereinfachen.

Erstellen Sie einen Ordner für die Schlüssel

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

und den Ordner stellen Sie als Defaultordner für die CA ein:

```
make-cadir /etc/openvpn/easy-rsa
```

Fügen Sie in ihn die vorbereiteten Skripts ein:

```
cp -R /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
```

Nachfolgend passen Sie die Variablen fürs Generieren von Zertifikaten an, damit die Angaben Ihren Vorstellungen entsprechen. Öffnen Sie die Konfigurationsdatei

```
nano /etc/openvpn/easy-rsa/vars
```

und bearbeiten Sie die betreffende Sektion, zum Beispiel

```
export KEY_COUNTRY="DE"
export KEY_PROVINCE="DE"
export KEY_CITY="Muenchen"
export KEY_ORG="Test"
export KEY_EMAIL="test@domainname.de"
```

Danach stoßen Sie das Generieren von Schlüsseln an. Das Skript wird Ihnen ein Client Zertifikat generieren; falls Sie mehrere Clients haben, benötigen Sie für jeden von ihnen ein selbständiges Zertifikat – die weiteren erstellen Sie mit ./build-key Name-des-Clients.

```
cd /etc/openvpn/easy-rsa
chown -R root:root .
chmod g+w .

source ./vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server

./build-key vpnclient1
```

Für eine höhere Sicherheit können wir noch einen Schlüssel generieren, mit dem die Pakete signiert werden (HMAC signature). Er wird die Authentizität der Nachrichten gewährleisten und sicherstellen, dass sie auf dem Weg über das Netz nicht geändert werden. In der Konfiguration ist für diese Signierung die Option *tls-auth* bestimmt. Den Schlüssel werden Sie auch für den Client benötigen.

```
cd keys
openvpn --genkey --secret ta.key
```

Nachfolgend kopieren Sie alles in den richtigen Ordner OpenVPN ein.

```
cp server.crt server.key ca.crt dh1024.pem ta.key ../../
```

Nun ist der größere Teil der Arbeit hinter uns und wir können mit der Anpassung der Konfigurationsdatei OpenVPN beginnen.

Konfigurationsdatei des Servers

Die Datei öffnen Sie mit der folgenden Befehlszeile:

```
nano /etc/openvpn/server.conf
```

Fügen Sie in die Datei die folgende Konfiguration ein:

```
mode server
port 1194
proto udp
dev tun
```

```
ca ca.crt
cert server.crt
key server.key # privater Schlüssel des Servers, nicht übertragen!
dh dh2048.pem

server 10.8.0.0 255.255.255.0

push "redirect-gateway autolocal" #Umleitung von allem Traffic in den Tunnel

push "dhcp-option DNS 8.8.8.8" #Sie werden geöffnete Resolver von Google verwenden

push "dhcp-option DNS 8.8.4.4"

tls-server
tls-auth ta.key 0
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
user nobody
group users
status openvpn-status.log
verb 3
```

Aus der Konfiguration ist offensichtlich, dass der Server für VPN IP-Adressen aus dem Umfang 10.8.0.0/24 (also IP 10.8.0.1-10.8.0.254) verwenden wird.

Netzwerk und Firewall

Um auf dem Server über den Tunnel „surfen“ zu können, müssen Sie die Einstellung des Netzwerkes und der Firewall ein bisschen anpassen.

Schalten Sie die Umleitung von Paketen an; mit Deaktivierung (uncomment) der folgenden Zeile in der Datei /etc/sysctl.conf:

```
net.ipv4.ip_forward = 1
```

Nachfolgend rufen Sie den unten stehenden Befehl auf, damit sich die Änderung aktiviert, oder starten Sie den Server neu.

```
sysctl -p /etc/sysctl.conf
```

Damit die Kommunikation richtig geleitet wird, müssen Sie noch das folgende Kommando einschreiben und das Skript für die von dem Tunnel abgesendeten Pakete erlauben:

```
iptables -t nat -I POSTROUTING -s 10.8.0.0/24 -j MASQUERADE
```

Nach der Verbindung des Clients zu dem VPN Netz muss die Kommunikation von dem Server abgesendet werden. Dieses können Sie einfach überprüfen:

```
ping 8.8.4.4
```

Es ist empfehlenswert, auch die folgenden Einstellungen zu applizieren, die die Verbindung nur in der Richtung von dem VPN Client ins Internet aufbauen werden, und nicht umgekehrt. Mit dieser Vorkehrung werden Sie verhindern, dass sich zu den VPN Clients (zu Ihnen) jemand vom Internet aus verbinden oder geöffnete Ports scannen wird.

```
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i tun+ -s 10.8.0.0/24 -j ACCEPT
iptables -P FORWARD DROP
```

Hinweis: Die richtige Einstellung der Firewall und Aktivierung gewünschter Dienste liegt völlig in Hand des jeweiligen Benutzers und Serververwalters. Diese Problematik ist sehr individuell und überschreitet den Rahmen unserer Anleitung. Zum Beispiel für Aktivierung von VPN auf dem Port 1194 können Sie das Kommando *-A INPUT -p udp --dport 1194 -j ACCEPT* verwenden und somit andere nicht genutzte Ports deaktivieren. Bestimmt jedoch nicht den Port 22, ohne den Sie sich zu dem Server nicht verbinden könnten.

Aktivierung von OpenVPN

Den OpenVPN-Dämon bringen Sie mit der folgenden Befehlszeile zum Laufen, die ihn ebenfalls in die nach dem Start ausgelösten Prozesse ergänzt.

```
systemctl enable openvpn.service && systemctl start openvpn.service
```

Führen Sie die Kontrolle durch:

```
systemctl status openvpn*.service
```

In dem Log werden Sie dann Details des angesteuerten Dienstes sehen. Den Auszug wird Ihnen der Befehl

```
journalctl -f | grep vpn
```

anzeigen.

Das Log wird in der realen Zeit dargestellt. Sie schließen es mit Ctrl+C. Nach der Auslösung des OpenVPN-Dämons muss sich in den Netzschnittstellen *tun0* befinden – sehen Sie die Ergebnisse von dem *iconfig*-Kommando oben.

Nun brauchen Sie nur den VPN Client zur Verbindung zu diesem Server zu verwenden. Wie Sie die Clients in Windows und Mac OSX einstellen können, schauen wir uns in den weiteren Anleitungen an. Auf jeden Fall werden Sie das CA Zertifikat und Zertifikat + den privaten Schlüssel benötigen, die für den jeweiligen Client erstellt worden sind. Diese Schlüssel laden Sie von dem Server herunter.

Quellen und weitere Informationen

- Linode.com - Set up a Hardened OpenVPN Server on Debian 8.
- Pontikis.net - How to setup OpenVPN on Debian server.