OpenVPN @ LuXeria

VPN für die LuXeria

Emanuel Duss

2013-12-18

OpenVPN

Virtual Private Network

- VPN: Tunnel zwischen zwei Rechnern
- Sichere Kommunikation
- Aufsatz Netzwerkstack-VPN (IPSec)
- SSL VPN (OpenVPN)

OpenVPN

- Läuft ausserhalb des Kernels
- VPN Funktioniert auch über HTTP-Proxies (Port `443/tcp`)
- Virtueller Netzwerkadapter
  - `tun`: Routing (Layer 3)
  - `tap`: Bridging (Layer 2)

Installation Server

Aktuell ist OpenVPN 2.3.2

```
# pacman -S openvpn
# cp -vr /usr/share/openvpn/easy-rsa/ /etc/openvpn/
```

Zertifikatbasierte Authentifizierung

Easy-RSA

- Skripts für die Erstellung und Verwaltung von SSL-Zertifikaten
- Erstellen und Signieren von Clientzertifikaten
- Certificate Revocation List
- Verwendet OpenSSL (auch manuell mit OpenSSL möglich)

Easy-RSA: Konfiguration

```
# cd /etc/openvpn/easy-rsa/

# vi +$ vars
export KEY_COUNTRY="CH"
export KEY_PROVINCE="Luzern"
export KEY_CITY="Adligenswil"
export KEY_ORG="Luxeria"
export KEY_EMAIL="admin@luxeria.ch"
export KEY_CN=luxeria
export KEY_NAME=luxeria
export KEY_OU=luxeria
export PKCS11_MODULE_PATH=luxeria
export PKCS11_PIN=1234

# . ./vars
```

Easy-RSA: Certificate Authority (CA)

Erstellen einer CA:

```
# ./clean-all
# ./build-ca
```

Output

- `keys/ca.crt`: Zertifikat der CA
- `keys/ca.key`: Schlüssel der CA
- `keys/index.txt`
- `keys/serial`

Easy-RSA: Keys für Server

Schlüsselpaar für den Server erstellen:

```
# ./build-key-server luxeria.ch # 2x mit y bestaetigen
```

Output

- `keys/luxeria.ch.csr`: Certificate Request
- `keys/luxeria.ch.key`: Private Key

Easy-RSA: Diffie-Hellmann

Parameterdatei für Schlüsselaustausch erstellen:

```
# ./build-dh
```

Output

- `keys/dh1024.pem`

Easy-RSA: Keys für Clients

Schlüsselpaar für Client erstellen:

```
# ./build-key emanuel
```

Output

- `keys/emanuel.csr`: Certificate Request
- `keys/emanuel.crt`: Certificate Request
- `keys/emanuel.key`: Private Key

Skript: Alle Clients @ Luxeria

```
# cd /etc/openvpn/easy-rsa
# for i in emanuel gandro hops roland zoepfe
do
    ./build-key $i && \
    cd keys && \
    tar -cvzf $i.tar.gz ca.crt $i.crt $i.key && \
    mv $i.tar.gz /home/$i && \
    chmod 600 /home/$i/$i.tar.gz && \
    chown $i.users /home/$i/$i.tar.gz && \
    cd ..
done
```

Konfiguration Server (1)

Beispiel kopieren:

```
# cp /usr/share/openvpn/examples/server.conf /etc/openvpn/
# vi /etc/openvpn/server.conf
```

Arbeitsverzeichnis

```
cd /etc/openvpn/
```

Protokoll

```
port 1194
proto udp
```

Konfiguration Server (2)

Zertifikate

```
ca easy-rsa/keys/ca.crt
cert easy-rsa/keys/server.crt
key easy-rsa/keys/server.key
dh easy-rsa/keys/dh1024.pem
```

Route

```
push "redirect-gateway def1 bypass-dhcp"
client-to-client
```

Skript

```
script-security 2
up start.sh
```

Konfiguration Server (3)

Skript für NAT und IP forwarding (`/etc/openvpn/start.sh`):

```
#!/bin/bash
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o enp3s0 -j MASQUERADE
```

Server starten

Testen

```
# openvpn /etc/server.conf
```

Aktivieren (für `server.conf`)

```
# systemctl enable openvpn@server.service
# systemctl start openvpn@server.service
```

Konfiguration Clients (Variante 1)

```
# pacman -S openvpn

# cp /usr/share/openvpn/examples/client.conf /etc/openvpn/
# cd /etc/openvpn

# tar -xvzf emanuel.tar.gz

# vi client.conf
remote 212.47.178.101 1194
ca ca.crt
cert emanuel.crt
key emanuel.key
```

Konfiguration Clients (Variante 2)

```
<ca>
-----BEGIN CERTIFICATE-----
MIIE6DCCA9CgAwIBAgIJAMnsLzW4Agc2MA0GCSqGSIb3DQEBCwUAMIGoMQswCQYD
VQQGEwJDSDEPMA0GA1UECBMGTHV6ZXJuMRQwEgYDVQQHEwtBZGxpZ2VuZHdpbDEQ
...
42H0Y5LmHM1x3AxLBbWAUtkD4kf3KEZ+/BN9jIx+CQ0EyCqH9Ug7FYQCdMtHmbME
YqxOMaLLTiEbsk69
-----END CERTIFICATE-----
</ca>

<cert>
...
</cert>

<key>
...
</key>
```

Neue User hinzufügen

Alles in einem Schritt mit einem Skript:

```
# cd /etc/openvpn
# sudo ./newuser freddy
# sudo ls -l userconfigs/luxeria_freddy.ovpn
```

Diese Datei `luxeria_freddy.ovpn` beinhaltet die gesamte Client Konfiguration inkl. CA, Client Zertifikat und private Key.

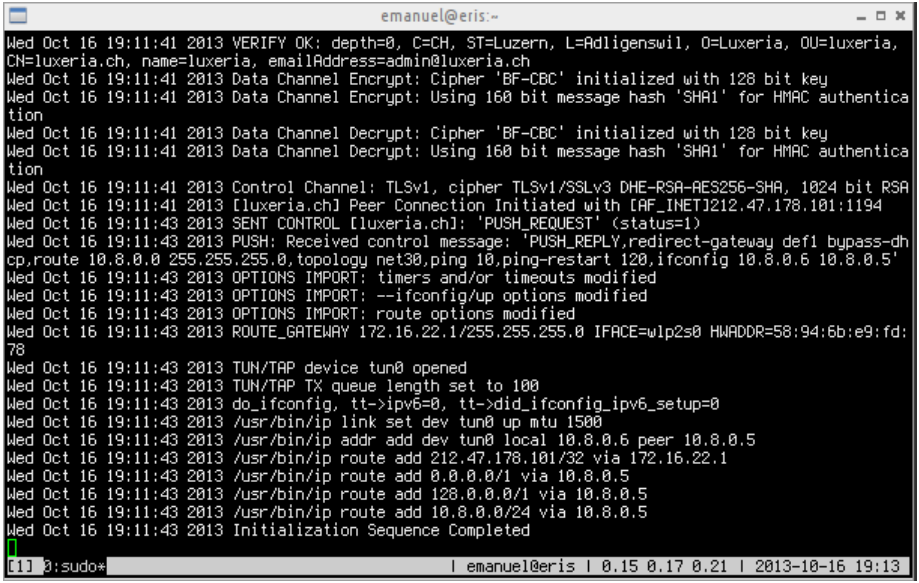
IPv6

- Der Server baut ein Tunnel zu Hurricane Electric (HE) auf.
- Clients bekommen über HE IPv6 Zugang.

Weitere Infos

- `https://openvpn.net/`
- `man openvpn`
- `man openssl`
- O'Reilly. Kurz & Gut. OpenVPN

#!/bin/demo


emanuel@eris:~
Wed Oct 16 19:11:41 2013 VERIFY OK: depth=0, C=CH, ST=Luzern, L=Adligenswil, O=Luxeria, OU=luxeria, CN=luxeria.ch, name=luxeria, emailAddress=admin@luxeria.ch
Wed Oct 16 19:11:41 2013 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed Oct 16 19:11:41 2013 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed Oct 16 19:11:41 2013 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed Oct 16 19:11:41 2013 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed Oct 16 19:11:41 2013 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Wed Oct 16 19:11:41 2013 [luxeria.ch] Peer Connection Initiated with [AF_INET]212.47.178.101:1194
Wed Oct 16 19:11:43 2013 SENT CONTROL [luxeria.ch]: 'PUSH_REQUEST' (status=1)
Wed Oct 16 19:11:43 2013 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,route 10.8.0.0 255.255.255.0,topology net30,ping 10,ping-restart 120,ifconfig 10.8.0.6 10.8.0.5'
Wed Oct 16 19:11:43 2013 OPTIONS IMPORT: timers and/or timeouts modified
Wed Oct 16 19:11:43 2013 OPTIONS IMPORT: --ifconfig/up options modified
Wed Oct 16 19:11:43 2013 OPTIONS IMPORT: route options modified
Wed Oct 16 19:11:43 2013 ROUTE_GATEWAY 172.16.22.1/255.255.255.0 IFACE=wlp2s0 HWADDR=58:94:6b:e9:fd:78
Wed Oct 16 19:11:43 2013 TUN/TAP device tun0 opened
Wed Oct 16 19:11:43 2013 TUN/TAP TX queue length set to 100
Wed Oct 16 19:11:43 2013 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Wed Oct 16 19:11:43 2013 /usr/bin/ip link set dev tun0 up mtu 1500
Wed Oct 16 19:11:43 2013 /usr/bin/ip addr add dev tun0 local 10.8.0.6 peer 10.8.0.5
Wed Oct 16 19:11:43 2013 /usr/bin/ip route add 212.47.178.101/32 via 172.16.22.1
Wed Oct 16 19:11:43 2013 /usr/bin/ip route add 0.0.0.0/1 via 10.8.0.5
Wed Oct 16 19:11:43 2013 /usr/bin/ip route add 128.0.0.0/1 via 10.8.0.5
Wed Oct 16 19:11:43 2013 /usr/bin/ip route add 10.8.0.0/24 via 10.8.0.5
Wed Oct 16 19:11:43 2013 Initialization Sequence Completed
[1] 0:sudo*
emanuel@eris | 0.15 0.17 0.21 | 2013-10-16 19:13

Fragen

?