Open VPN server op CentOS 7

software

installeer de nodige software door:
`yum install epel-release`

en vervolgens:
`yum install openvpn`

Keys & Certificaten

server en client TLS

Maak de signing request als volgt aan op de VPN server zelf:

`yum install openssl`

```
mkdir -p /etc/openvpn/certs/keys
chmod 400 /etc/openvpn/certs/keys
cd /etc/openvpn/certs
```

Maak een config file aan voor de server csr: `vi vpnserver.cnf`

en zet hier in:

```
# vpnserver.cnf
# This configuration file is used by the 'req' command when the server
certificate is created.
[ req ]
default_bits            = 2048
default_md              = sha2
encrypt_key             = no
prompt                  = no
string_mask             = utf8only
distinguished_name      = server_distinguished_name
req_extensions          = req_cert_extensions
# attributes              = req_attributes

[ server_distinguished_name ]
countryName             = NL
stateOrProvinceName     = zuid Holland
localityName            = Den Haag
organizationName        = Boerema CI&ND
organizationalUnitName  = IT Dept.
commonName              = vpnserver.auriel.nl
```

```
emailAddress            = hostmaster@auriel.nl

[ req_cert_extensions ]
nsCertType              = server
subjectAltName          = email:hostmaster@auriel.nl
```

en maak de CSR aan door:
`openssl req -new -config vpnserver.cnf -keyout vpnserver.key -out vpnserver.csr`
`chmod 400 server.key`

transporteer deze naar de CA server en sign deze.

Maak ook voor de client een certificaat-key pair aan (deze zullen we op alle clients gebruiken): `vi vpnclient.cnf`

en zet hier in:

```
# vpnclient.cnf
# This configuration file is used by the 'req' command when the server certificate is created.
[ req ]
default_bits            = 2048
default_md              = sha2
encrypt_key             = no
prompt                  = no
string_mask             = utf8only
distinguished_name      = client_distinguished_name
req_extensions          = req_cert_extensions
# attributes              = req_attributes

[ client_distinguished_name ]
countryName             = NL
stateOrProvinceName     = zuid Holland
localityName            = Den Haag
organizationName        = Boerema CI&ND
organizationalUnitName  = IT Dept.
commonName              = vpnclient.auriel.nl
emailAddress            = hostmaster@auriel.nl

[ req_cert_extensions ]
nsCertType              = client
subjectAltName          = email:hostmaster@auriel.nl
```

en maak de CSR aan door:
`openssl req -new -config vpnclient.cnf -keyout vpnclient.key -out vpnclient.csr`
`chmod 400 vpnclient.key`

transporteer deze naar de CA server en sign deze.

Diffie Hellman

```
openssl dhparam -out dh2048.pem 2048
```

zowel de clients als de server moeten deze file hebben.

HMAC key

```
openvpn --genkey --secret ta.key
chmod 400 ta.key
```

zowel de clients als de server moeten deze file hebben.

Server Setup

OpenVPN configuratie

Kopieer het voorbeeld configuratiefile naar de juiste locatie:

```
cp /usr/share/doc/openvpn-*/sample/sample-config-files/server.conf
/etc/openvpn
```

En pas deze aan: `vi /etc/openvpn/server.conf`

en zorg dat de volgende parameters als volgt staan:

```
port 1194
proto udp
dev tun

ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/vpnserver.auriel.nl.crt
key /etc/openvpn/certs/vpnserver.auriel.nl.key

dh /etc/openvpn/certs/dh2048.pem

server 10.8.1.0 255.255.255.0
ifconfig-pool-persist ipp.txt
duplicate-cn

comp-lzo
keepalive 10 120

cipher AES-256-CBC
tls-auth /etc/openvpn/certs/ta.key 0

user nobody
```

```
group nobody

persist-key
persist-tun

status openvpn-status.log
verb 3

explicit-exit-notify 1
```

Firewall

We routeren niet, we staan alleen een VPN verbinding toe. Open de firewall voor de poort die we net hebben geconfigureerd, 1194:

```
firewall-cmd --permanent --add-port=1194/tcp
firewall-cmd --reload
```

en start de applicatie nu en in de toekomst:

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

SELinux aanpassen

Als je OpenVPN op een andere poort wil draaien dan de standaard 1194 moet je OpenVPN toegang geven tot niet standaard poort voor SELinux.

Vindt de SELinux service naam door: `semanage port -l | grep openvpn` de output is:

```
openvpn_port_t                 tcp      1194
openvpn_port_t                 udp      1194
```

en geef openvpn toegang tot een niet standaard poort, bijvoorbeeld poort 123:
`semanage port -a -t openvpn_port_t -p udp 123`

http://sysadmin-notepad.blogspot.nl/2013/05/custom-openvpn-port-with-selinux-enabled.html

Client configuratie

We embedden de certificaten en keys hier in om configuratie op android enzovoort makkelijker te maken, De regels met een hash er voor zou de regel zijn als je de certificaten en key's niet zou embedden.

Maak een configuratie file: `vi /etc/openvpn/client/client.ovpn`

en zet hier in:

```
vpnclient.auriel.nl
dev tun
proto udp

pull

comp-lzo

remote vpnserver.auriel.nl 1194

#ca ca.crt
<ca>
-----BEGIN CERTIFICATE-----
MIID-etcetera.
-----END CERTIFICATE-----
</ca>

#cert vpnclient.crt
<cert>
-----BEGIN CERTIFICATE-----
MIID edcetera.
-----END CERTIFICATE-----
</cert>

#key vpnclient.key
<key>
-----BEGIN PRIVATE KEY-----
MIIE edcetera.
-----END PRIVATE KEY-----
</key>

cipher AES-256-CBC


#tls-auth ta.key 1
key-direction 1
<tls-auth>
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
e56c4aa7f938605d22f394247f7bf88f
edcetera.
-----END OpenVPN Static key V1-----
</tls-auth>
```

bronnen

https://www.digitalocean.com/community/tutorials/how-to-setup-and-configure-an-openvpn-server-on-centos-7

https://weakdh.org/sysadmin.html

http://www.macfreek.nl/memory/Create_a_OpenVPN_Certificate_Authority

https://forums.openvpn.net/viewtopic.php?t=11913

https://forums.openvpn.net/viewtopic.php?t=20860

https://www.sparklabs.com/forum/viewtopic.php?t=1888