OpenVPN

The Situation

You want a secure way to make resources in your network available for your clients from everywhere with a standard internet connection.

What is OpenVPN?

OpenVPN is an OpenSSL based VPN solution, most commonly used for client-server VPN connections. It lets OpenSSL do all the encryption and authentication work, allowing OpenVPN to use all the ciphers available in the OpenSSL package.

It is good at working through NAT and getting out through firewalls. The server has the ability to "push" certain network configuration options to the clients. These include IP addresses, routing, dns, and a few connection options.

Why not use PPTP instead?

PPTP is known to be a faulty protocol. The designers of the protocol, Microsoft, recommend not to use it due to the inherent risks. Lots of people use PPTP anyway due to ease of use, but that doesn't mean it is any less hazardous. The maintainers of PPTP Client and Poptop recommend using OpenVPN (SSL based) or IPSec instead.

References:
http://pptpclient.sourceforge.net/protocol-security.phtml
http://www.schneier.com/pptp-faq.html

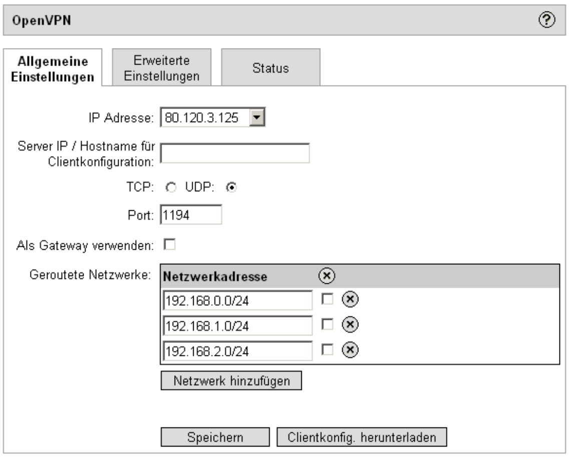
Gibraltar Configuration

1. Basic configuration

In the general configuration tab you need to enter or choose a server IP.

“Use as gateway” means that the openvpn server is telling the client to use Gibraltar as his default gateway, so all traffic from the client is going through VPN (good for mobile workers that do not trust their mobile internet providers)

Routed networks, are those networks you want to provide for client access. Be aware that you will also need to configure a firewall rule.



IP Adresse: 80.120.3.125

Server IP / Hostname für Clientkonfiguration:

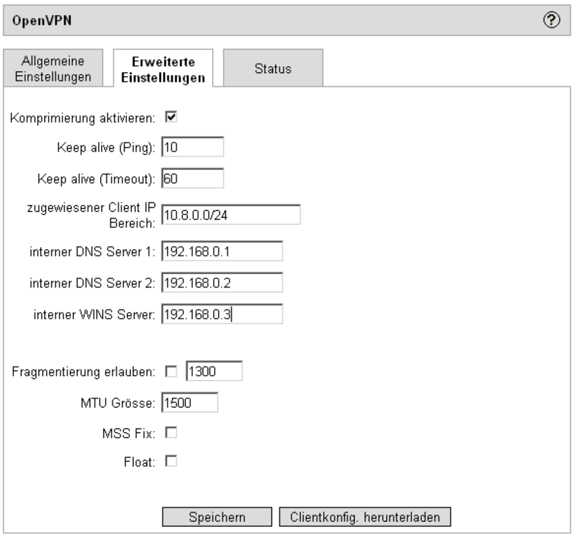
TCP: ○ UDP: ●

Port: 1194

Als Gateway verwenden: □

Geroutete Netzwerke:

Netzwerkadresse	
192.168.0.0/24	□
192.168.1.0/24	□
192.168.2.0/24	□



Komprimierung aktivieren: ☑

Keep alive (Ping): 10

Keep alive (Timeout): 60

zugewiesener Client IP Bereich: 10.8.0.0/24

interner DNS Server 1: 192.168.0.1

interner DNS Server 2: 192.168.0.2

interner WINS Server: 192.168.0.3

Fragmentierung erlauben: □ 1300

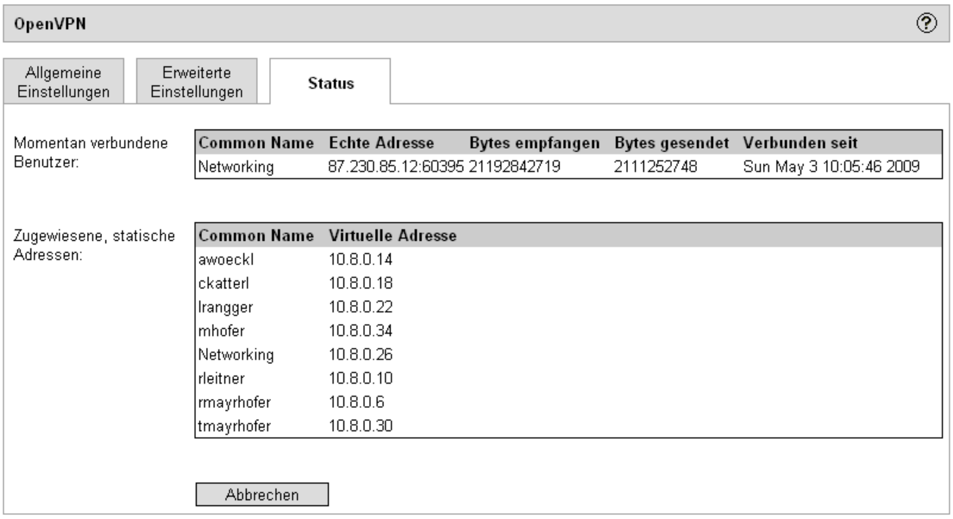
MTU Grösse: 1500

MSS Fix: □

Float: □

In the advanced configuration tab there are only 3 things a normal user will need. IP Range for VPN Clients (be sure to use a subnet that isn’t already present in your network), DNS 1 (primary), DNS 2 (secondary) and WINS Server. These settings are passed by the integrated OpenVPN “dhcp” to your clients.

The status tab shows currently connected users as well as all the assigned ip addresses. You might be wondering why there are always 3 addresses between each client. That is because every client gets his own 255.255.255.252 (/30) network. So each client has 2 usable ip adresses, one of those is used for openvpn internal routing and the second one is the actual client ip address.



Momentan verbundene Benutzer:

Common Name	Echte Adresse	Bytes empfangen	Bytes gesendet	Verbunden seit
Networking	87.230.85.12:60395	21192842719	2111252748	Sun May 3 10:05:46 2009

Zugewiesene, statische Adressen:

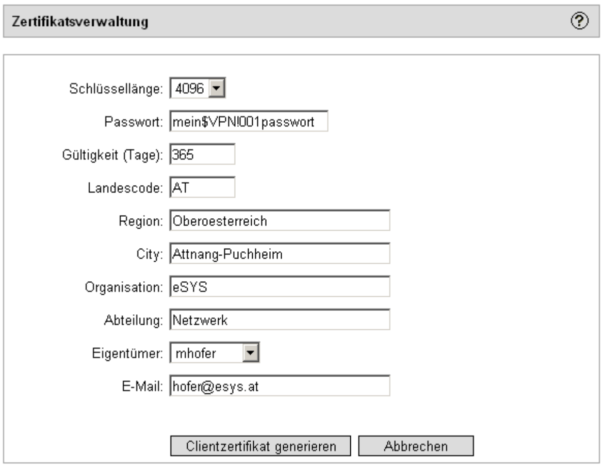
Common Name	Virtuelle Adresse
awoeckl	10.8.0.14
ckatterl	10.8.0.18
lrangger	10.8.0.22
mhofer	10.8.0.34
Networking	10.8.0.26
rleitner	10.8.0.10
rmayrhofer	10.8.0.6
tmayrhofer	10.8.0.30

2. Adding Clients

For managing your OpenVPN Clients there are two possibilities, the integrated LDAP Server or an external LDAP/Active Directory. For integrating your Gibraltar Security Gateway in your Active Directory please refer to the Gibraltar help pages.

Everything you have to do for creating an OpenVPN User is just simply create the user in your LDAP and create a client certificate for him. This is done by clicking on the “generate client certificate” in “VPN→Certificates” and fill out the form as requested. For maximum security we recommend the maximum key length for your certificates (4096), this does not affect performance of the VPN in any way!

3. Firewall (access restrictions)



Zertifikatsverwaltung

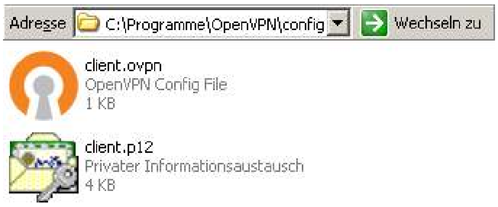
Schlüssellänge: 4096
Passwort: mein$VPN!001passwort
Gültigkeit (Tage): 365
Landescode: AT
Region: Oberoesterreich
City: Attnang-Puchheim
Organisation: eSYS
Abteilung: Netzwerk
Eigentümer: mhofer
E-Mail: hofer@esys.at

To control trafficflow in and out of your Virtual Private Network, the interface “tun+” is used. By default, the communication between OpenVPN Clients is not allowed and would require an extra firewall rule from “IN:tun+” to “OUT:tun+”. Be aware that only networks you added to the “routed networks” section in OpenVPN Configuration are reachable from your clients if you firewall rules allow it.

Client Configuration

1. Windows XP/Vista

Put the files client.ovpn and client.p12 to your “OpenVPN/config” folder.



Adresse C:\Programme\OpenVPN\config

client.ovpn
OpenVPN Config File
1 KB

client.p12
Privater Informationsaustausch
4 KB

After that start OpenVPN GUI from your start menue, you should see a red icon in your systray meaning that OpenVPN is currently disconnected. So rightclick on the icon and leftclick on connect. The icon will turn yellow and OpenVPN will ask for your password. After you clicked on OK, the icon should turn into green saying that you are connected with your OpenVPN now!

The newest client can be downloaded here:
http://openvpn.org/index.php/open-source/downloads.html