



OpenVPN Grundlagen, Server und Clients

PC-Treff-BB Aidlingen

Günter Waller
Roland Egeler

PC-Treff-BB Aidlingen

OpenVPN – Grundlagen, Server und Clients

© 2018 Günter Waller, Roland Egeler

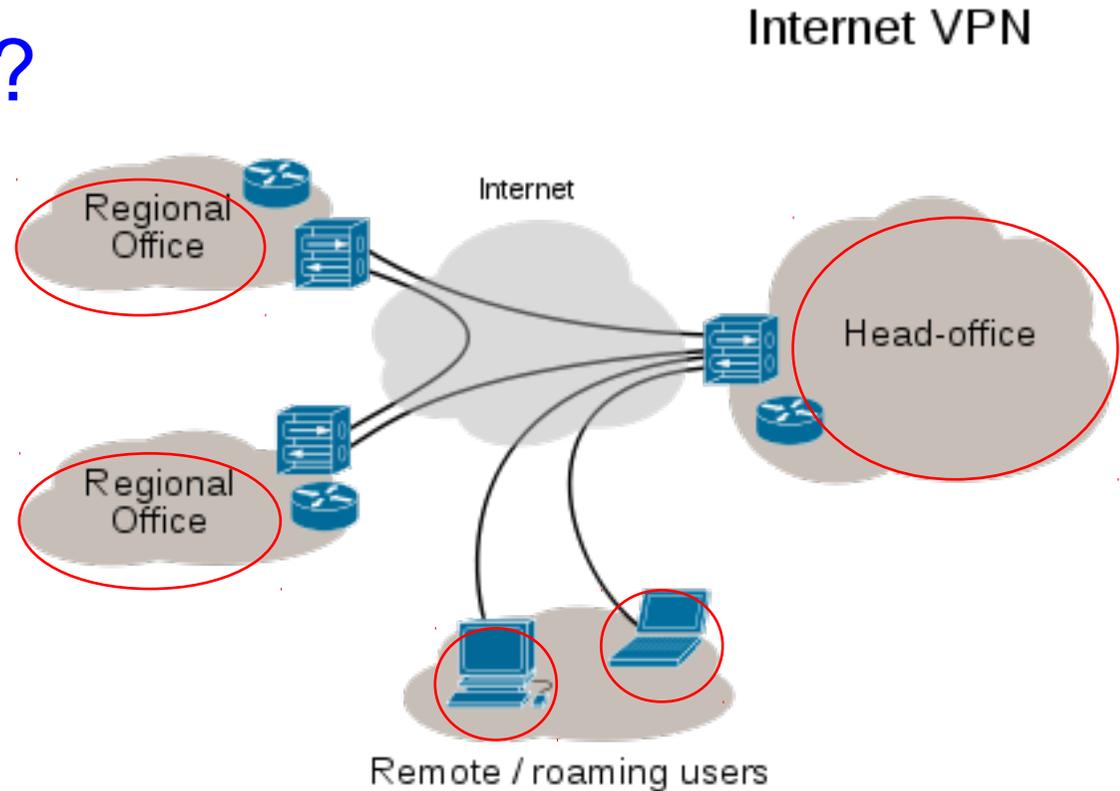
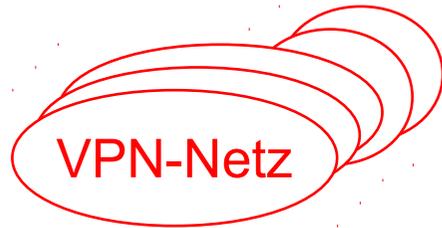
08.09.2018



Agenda

- Virtual Private Networks - Grundlagen
- Die wichtigsten VPN-Verfahren
- OpenVPN Basics
- Server auf OpenWRT
- Server auf pfSense
- Linux Client
- Android Client
- iOS Client
- Windows Client
- Links

Was ist ein VPN?



- Struktur eines VPNs: Unten abgebildet sind Heimarbeitsplätze, die sich per VPN durch das Internet hindurch in den Hauptsitz einer Firma einwählen, wobei der blaue Kasten ein VPN-Gateway ist (bzw. VPN-Server). Darüber hinaus ist der Hauptsitz per VPN auch mit zwei seiner Filialen verbunden, wobei das dazwischen liegende Netz auch hier das Internet ist, das dem VPN als Transportweg dient (**aus Sicht der VPN-Verbindung wird das Internet auf die Funktion eines Verlängerungskabels reduziert**).
- Es gibt also Netz-Netz-Verbindungen wie auch Einzelrechner-Netz-Verbindungen.
- Die Verbindungen über das öffentliche Internet sind verschlüsselt (**Tunnel**).
- Die beteiligten Netze bzw. Einzelrechner befinden sich scheinbar in einem Netz und kommunizieren ohne Kenntnis der (**transparenten**) Tunnel miteinander.

Die wichtigsten VPN-Verfahren

- OpenVPN
- PPTP
- IPSec
- SSTP
- SoftEther
- WireGuard
- ...

VPN-Verfahren: OpenVPN

- Open Source
- Benutzt TLS (wie HTTPS und SSH)
- Keine Probleme mit Firewalls
- Kryptoalgorithmen wählbar
- Viel Drittsoftware
- Benutzt Konfigurationsdateien
- Bei Fehlkonfiguration unsicher (PEBKAC)

VPN-Verfahren: PPTP

- Point to Point Tunneling Protocol
- Benutzt mit „GRE“ ein eventuell von der Firewall geblocktes Protokoll
- Von Microsoft initiiert
- Einfach zu konfigurieren, da mitgeliefert
- Schlecht implementiert
- Seit 2012 geknackt
- Nicht zu empfehlen

VPN-Verfahren: IPSEC

- Level-3-Protokoll wie IP
- Eventuell Probleme mit Firewalls
- Sichere Verschlüsselung, aber möglicherweise durch NSA geschwächt
- Braucht weitere Protokolle wie L2TP und IKEv2
- Beide langsam durch doppeltes Kapseln
- Einrichtung eher kompliziert

VPN-Verfahren: SSTP

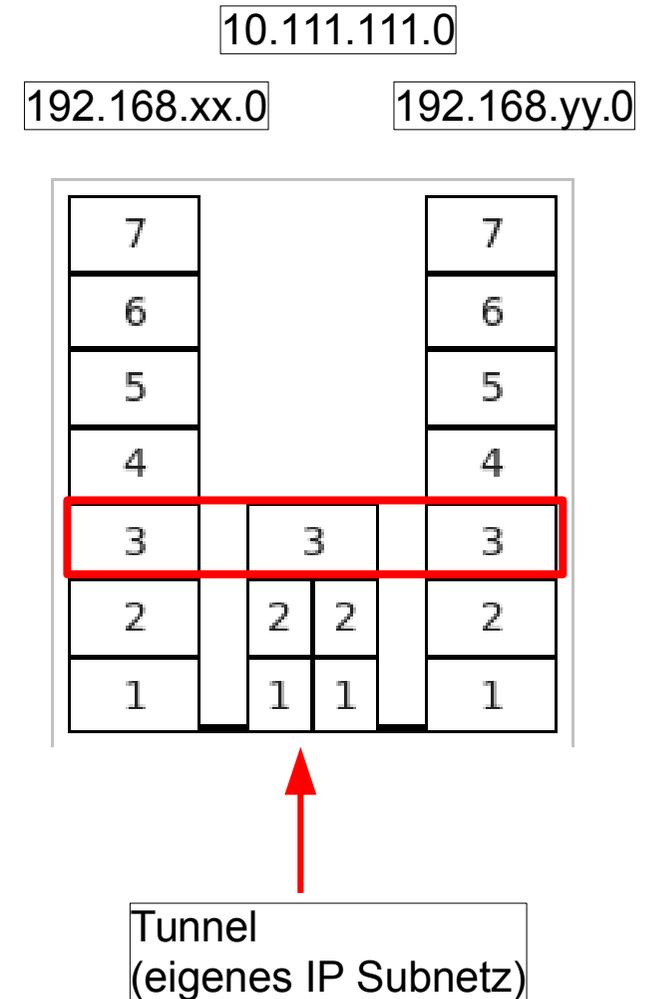
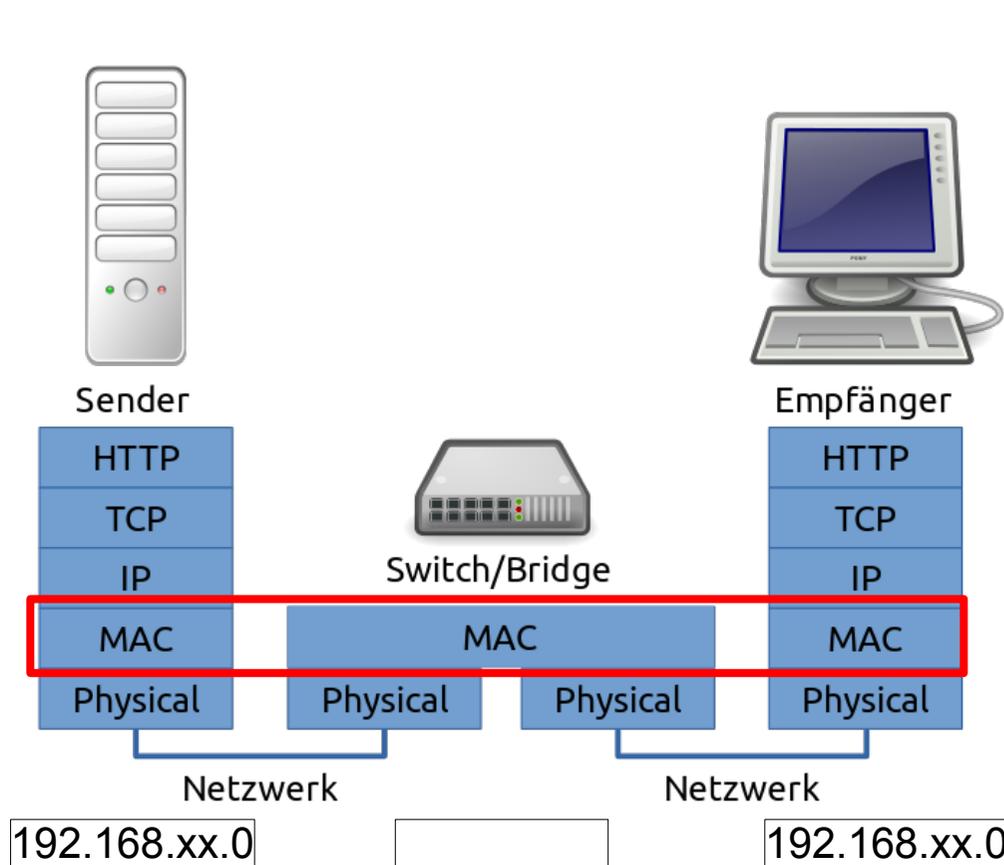
- Entwickelt von Microsoft
- Ziel: Weniger Support wie bei IPSec
- Benutzt TLS über Port 443 (wie HTTPS)
- Keine Probleme mit Firewalls
- Wenig Unterstützung für andere Betriebssysteme
- Kann nicht von Dritten überprüft werden
- Nicht zu empfehlen

OpenVPN - Basics

- Aktuelle Version 2.4.6
- Meine: 2.4.4
- Routed vs. Bridged
- IP-Adress-Plan
- **Eigene CA für Zertifikate und Schlüssel**
- Konfigurationsdateien für Server und Clients
- Starten, testen, Verbindungsaufbau
- Überwachen, steuern
- DHCP, Client-spezifische Regeln, Access Policies
- Alternative Authentifizierungsmethoden
- Hardening
- Clients entfernen

- [OpenVPN Quickstart.](#)
- [Installing OpenVPN.](#)
- [Determining whether to use a routed or bridged VPN.](#)
- [Numbering private subnets.](#)
- [Setting up your own Certificate Authority \(CA\) and generating certificates and keys for an OpenVPN server and multiple clients.](#)
- [Creating configuration files for server and clients.](#)
- [Starting up the VPN and testing for initial connectivity.](#)
- [Configuring OpenVPN to run automatically on system startup.](#)
- [Controlling a running OpenVPN process.](#)
- [Expanding the scope of the VPN to include additional machines on either the client or server subnet.](#)
- [Pushing DHCP options to clients.](#)
- [Configuring client-specific rules and access policies.](#)
- [Using alternative authentication methods.](#)
- [How to add dual-factor authentication to an OpenVPN configuration using client-side smart cards.](#)
- [Routing all client traffic \(including web-traffic\) through the VPN.](#)
- [Running an OpenVPN server on a dynamic IP address.](#)
- [Connecting to an OpenVPN server via an HTTP proxy.](#)
- [Connecting to a Samba share over OpenVPN.](#)
- [Implementing a load-balancing/failover configuration.](#)
- [Hardening OpenVPN Security.](#)
- [Revoking Certificates.](#)
- [Additional Security Notes.](#)

Einschub: Bridging vs. Routing



Bildquelle 1: https://de.wikipedia.org/wiki/Datei:IP-Paket_Switch.svg

Bildquelle 2: <https://de.wikipedia.org/wiki/Router>

OpenVPN vs. andere VPNs (Selbstzeugnis)

- Open Source (GPL)
- Cross Plattform, Portability
 - Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X, QNX, Windows, Android, iOS
 - OpenWRT, Fritz!Box, Dreambox, u.v.m.
- IP4 und IP6 Support
- Modularer Aufbau
- Management Interface (verschiedene GUIs)
- Smartcard Support (unter Windows)
- Robust über unzuverlässige Netze (Tunnel Recovery)
- Performance

<https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn#WhatdistinguishesOpenVPNfromotherVPNpackages>

OpenVPN - Voraussetzungen

- Port Forwarding für den VPN-Standardport 1194 ist Grundvoraussetzung. (Wir zeigen hier alle Ports, auch die für die Weboberfläche des Routers.)



Administrator Sprache Deutsch

STATUS BASIC **FORTGESCHRITTEN** DRAHTLOS SYSTEM

OPTIONEN
IP-FILTER
MAC-FILTER
PORT-FILTER
WEITERLEITUNG
PORT-TRIGGER
DMZ-HOST
FIREWALL
WI-FI RADAR

FORTGESCHRITTEN

Weiterleitung

Auf dieser Seite können Sie Weiterleitungen konfigurieren

Öffentlicher Port-Range	Lokale IP-Adresse	Ziel-Port-Range	Protokoll	Löschen
80-80	[Redacted]	80-80	TCP/UDP	<input type="checkbox"/>
443-443	[Redacted]	443-443	TCP/UDP	<input type="checkbox"/>
1194-1194	[Redacted]	1194-1194	TCP/UDP	<input type="checkbox"/>
			TCP/UDP	<input type="checkbox"/>

OpenVPN - Voraussetzungen

- Port-Forwarding auf der Fritzbox

Freigaben

Status	Bezeichnung	Protokoll	IP-Adresse im Internet	Port extern vergeben		
<input type="radio"/>	SSH-Server	TCP	IPv4	 (22)		
<input type="radio"/>	openVPN	UDP	IPv4	1194 (1194)		
<input type="radio"/>	HTTP-Server	TCP	IPv4	80 (80)		

Neue Freigabe

Firewall-Settings bei OpenWRT (automatisch erzeugt)

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping
lan: lan:   ⇒ wan vpn_turris	accept ▼	accept ▼	accept ▼	<input type="checkbox"/>	<input type="checkbox"/>
wan: wan:  wan6:  ⇒ REJECT	reject ▼	accept ▼	reject ▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
guest_turris: guest_turris: (empty) ⇒ wan	reject ▼	accept ▼	reject ▼	<input type="checkbox"/>	<input type="checkbox"/>
vpn_turris: vpn_turris:  ⇒ lan	accept ▼	accept ▼	reject ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Rule

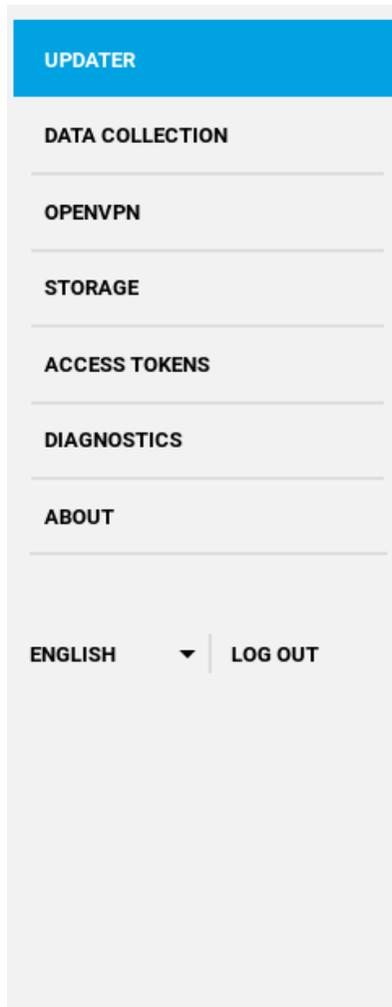
vpn_turris_rule	Any udp From <i>any host</i> in wan To <i>any router IP</i> at port 1194 on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>
-----------------	--	--------------	-------------------------------------

OpenVPN - Voraussetzungen

- Für Verbindung aus dem Internet in ein privates Netz ist ein DynDNS-Server hilfreich
- Früher dyndns.org
- Heute no-ip.org u.a.
- Strato bietet diesen Service auch an

Server auf OpenWRT (Turris Omnia Foris) vereinfachte Methode

- Installation nicht über den Paketinstaller sondern über den Updater, dadurch besser integriert mit dem OS
 - Gilt nicht für andere OpenWRT Implementierungen!



The screenshot shows the 'UPDATER' section of the OpenWRT LuCI interface. It features a sidebar menu with the following items: DATA COLLECTION, OPENVPN, STORAGE, ACCESS TOKENS, DIAGNOSTICS, and ABOUT. At the bottom of the sidebar, there is a language dropdown menu currently set to 'ENGLISH' and a 'LOG OUT' button.

Package lists

- | | |
|--|---|
| Cloud Backups | <input type="checkbox"/> Service for storing configuration backups on remote servers (EXPERIMENTAL). |
| Web camera | <input type="checkbox"/> Support to capture image with web camera. |
| Sound card | <input type="checkbox"/> Support for USB sound card. |
| Internet connection speed measurement | <input type="checkbox"/> Actively measures speed of Internet connection using netmetr.cz service. |
| Tor | <input type="checkbox"/> Service to increase anonymity on the Internet. |
| LuCI extensions | <input checked="" type="checkbox"/> Several additional tabs and controls for the advanced LuCI interface. |
| Squid | <input type="checkbox"/> HTTP caching proxy Squid. |
| Access tokens | <input checked="" type="checkbox"/> A Foris plugin allowing to manage remote API access tokens (for example for use in Spectator or Android application). |
| Majordomo | <input type="checkbox"/> Software for monitoring connections of devices in local network (obsolete). |
| NAS | <input checked="" type="checkbox"/> Services allowing to connect a disk to the router and use it as network data store. |
| LXC utilities | <input checked="" type="checkbox"/> Set of utilities to manage Linux Containers (lightweight virtualization technology). |
| Pakon | <input type="checkbox"/> Software for in depth monitoring of your traffic (EXPERIMENTAL). |
| Home automation | <input type="checkbox"/> Control software for home automation, including Turris Gadgets. |
| OpenVPN | <input checked="" type="checkbox"/> An easy setup of OpenVPN server from Foris. |

Server auf OpenWRT – eigene CA

- OpenVPN verwendet zertifikatsbasierte Authentifizierung
- Mein OpenWRT-Router (Turris Omnia) hat eine vereinfachte Konfiguration über die Web-Oberfläche
 - Vereinfachtes Installieren OpenVPN Paket, **kein bridged mode!**
 - **CA generieren** (dauert etwas). Ergebnis im Verzeichnis `/etc/ssl/ca/openvpn`
 - CA: Zertifikat und Private Key
 - Server (01): Zertifikat, Certificate Request, Private Key, Zertifikat im PEM Format

```

-rw-r--r--      1 root      root          6704 Sep  3 00:32 01.crt
-rw-r--r--      1 root      root          1582 Sep  3 00:32 01.csr
-r-----       1 root      root          3268 Sep  3 00:32 01.key
-rw-r--r--      1 root      root          6704 Sep  3 00:32 01.pem
-rw-r--r--      1 root      root          1862 Sep  3 00:32 ca.crt
-r-----       1 root      root          3272 Sep  3 00:32 ca.key
  
```

Server auf OpenWRT - Konfiguration

Es wird dann auf der gleichen Seite eine Konfiguration vorgeschlagen. Ich habe sie so gelassen und „applied“. Dabei geht es um die Networking-Aspekte.

Der VPN-Tunnel bekommt eine eigene Netzadresse: 10.111.111.0/24

Previous settings

If you haven't tried to set up OpenVPN server on our router yet, you can safely proceed to "**Apply configuration**" button.

Otherwise if you've tried to set up OpenVPN outside this plugin, there is a chance that your configuration might collide with the configuration created by this plugin. Therefore you might need to disable the old configuration first.

Configuration enabled

OpenVPN network

10.111.111.0/24

All traffic through vpn

?

Use DNS from vpn

?

Apply configuration

Current settings

Network: 10.111.111.0/24

Device: tun_turris

Protocol: udp

Port: 1194

Route: 192.168.1.1/24

Note that when you trigger "**Apply configuration**" button you might lose the connection to the router for a while. This means that you might need to reopen this admin page again.

Server auf OpenWRT - Networking

Das virtuelle Netz ist also ein Klasse-C Netz 10.111.111.0. Es entsteht dabei ein virtuelles Netzwerk-Device, welches hier **tun_turris** heißt. In der Literatur kommt meistens einfach **tun** vor. Protokoll udp und Port 1194 sind die Defaults.

Das Aktivieren dieser Einstellungen bedeutet gleichzeitig, dass eine Firewall-Regel für diesen Port angelegt und aktiviert wird.

vpn_turris_rule	Any udp	Accept input	<input checked="" type="checkbox"/>			 Edit	 Delete
	From <i>any host</i> in <i>wan</i>						
	To <i>any router IP</i> at port <i>1194</i> on <i>this device</i>						

Schließlich gibt es noch eine Route, die auf den Router selbst zeigt.

Die Konfigurationsdatei findet sich nicht, wie man annehmen könnte, in `/etc/openvpn/vpn.conf` (so steht es in manchen Internetseiten), sondern in `/etc/config/openvpn`. Tückisch!

Server auf OpenWRT - Konfigurationsdatei

```
config openvpn 'server_turris'  
option enabled '1'  
option port '1194'  
option proto 'udp'  
option dev 'tun_turris'  
option mssfix '1300'  
option ca '/etc/ssl/ca/openvpn/ca.crt'  
option crl_verify '/etc/ssl/ca/openvpn/ca.crl'  
option cert '/etc/ssl/ca/openvpn/01.crt'  
option key '/etc/ssl/ca/openvpn/01.key'  
option dh '/etc/dhparam/dh-default.pem'  
option server '10.111.111.0 255.255.255.0'  
option ifconfig_pool_persist '/tmp/ipp.txt'  
option duplicate_cn '0'  
option keepalive '10 120'  
option comp_lzo 'yes'  
option persist_key '1'  
option persist_tun '1'  
option status '/tmp/openvpn-status.log'  
option verb '3'  
option mute '20'  
list push 'route 192.168.xx.0 255.255.255.0'  
list push 'dhcp-option DNS 192.168.xx.1'  
list push 'dhcp-option DOMAIN lan'
```

Die rot markierten Parameter habe ich später eingefügt, weil nicht alles funktioniert hat. Probleme gab es (a) mit DNS (Auflösung der lokalen Namen ging nicht) und (b) mit HTTP (hatte offenbar mit MTU-Size zu tun). Die Lösungen kamen von Google, wurden nicht bis ins letzte Detail analysiert, sondern ausprobiert.

Vorsicht: evtl. Konflikt der Subnetze, wenn bei Server und Client identisch (192.168.xx.0)

Server auf OpenWRT - Zertifikate

In der Konfigurationsdatei finden sich folgende, mit Zertifikaten befassten Zeilen (CA ist hier separate Entity):

```
option ca '/etc/ssl/ca/openvpn/ca.crt'  
option crl_verify '/etc/ssl/ca/openvpn/ca.crl'  
option cert '/etc/ssl/ca/openvpn/01.crt'  
option key '/etc/ssl/ca/openvpn/01.key'  
option dh '/etc/dhparam/dh-default.pem'
```

OpenVPN arbeitet rein auf Zertifikatsbasis. Unter Turris/Foris werden die Clientzertifikate (hier: 02) auf dem Server erzeugt und dann - ggf. mit Nachbearbeitung - auf die Clients gebracht. Dateien pro Client:

-rw-r--r--	1	root	root	6911	Sep	3	01:04	02.crt
-rw-r--r--	1	root	root	1582	Sep	3	01:04	02.csr
-r-----	1	root	root	3272	Sep	3	01:04	02.key
-rw-r--r--	1	root	root	6911	Sep	3	01:04	02.pem

Server auf OpenWRT – Client-Generierung

Die mit „Get Config“ herunterladbare Datei enthält sowohl Konfigurationsparameter als auch den öffentlichen sowie den privaten Schlüssel. Das ist eher unüblich (unsicher?), erspart aber dem Client, einen privaten Schlüssel selbst erzeugen zu müssen.

Client configuration

Here you can create and revoke the client capability to connect to your OpenVPN network.

Client name

Create

Client	Status		
Stylus2	active	Get Config	Revoke
ipad	active	Get Config	Revoke

Be sure to check, that the server IP address provided in you configuration file actually matches the public IP address of your router. You can set this address manually when the autodetection fails.

Router address

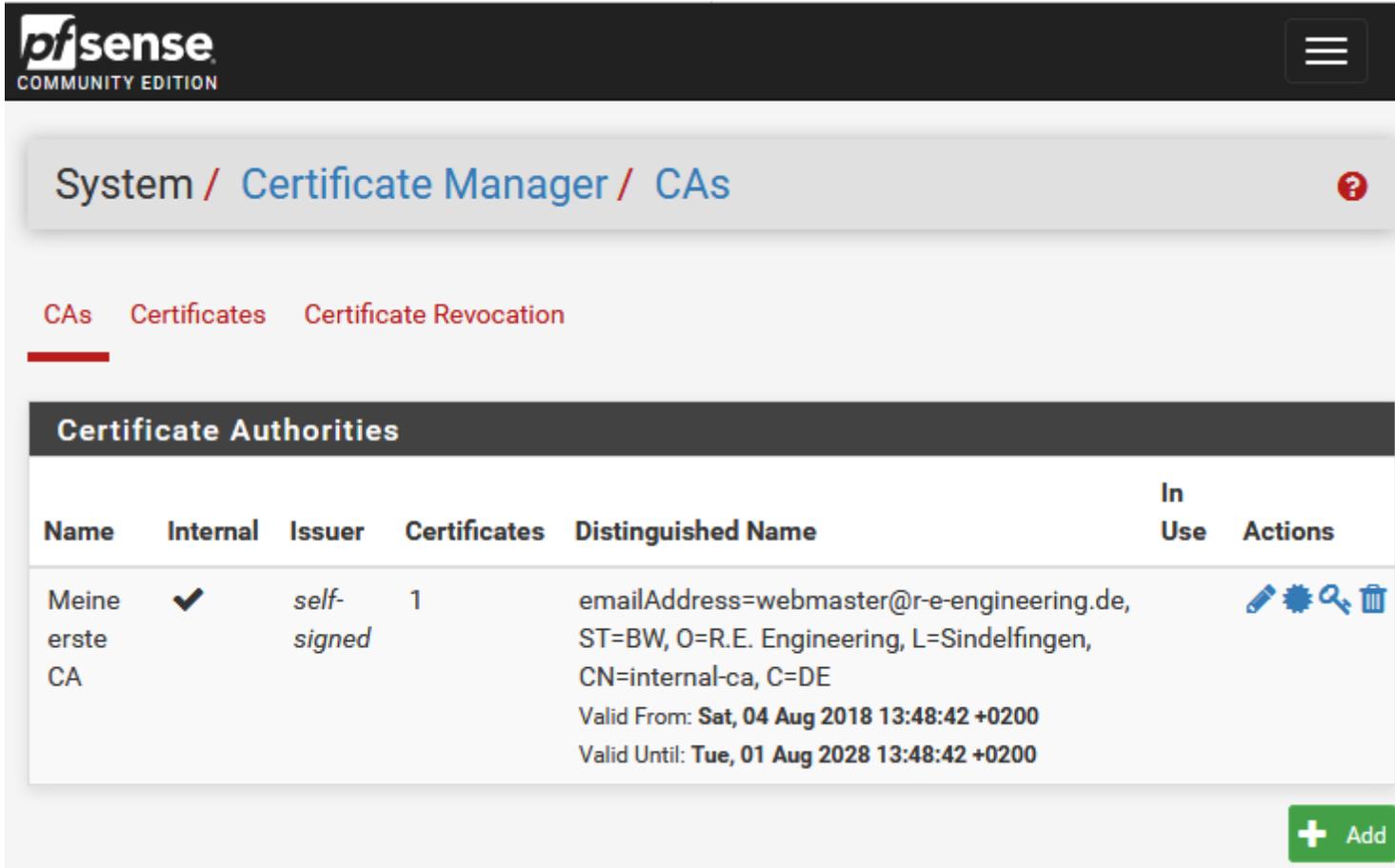
To apply the client configuration you need to download it and put it into the OpenVPN config directory or you might try to open it using your OpenVPN client directly. You might need to restart your client afterwards.

Server auf pfSense

- OpenVPN wird mitgeliefert und aktualisiert
- pfSense hat eigene CA (Certificate Authority)
- Verwaltet eigene Zertifikate und Schlüssel
- Konfiguration über Weboberfläche
- Unterstützt viele Szenarien

Server auf pfSense

- Certificate Manager



pfSense
 COMMUNITY EDITION

System / Certificate Manager / CAs

[CAs](#) [Certificates](#) [Certificate Revocation](#)

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Meine erste CA	✓	self-signed	1	emailAddress=webmaster@r-e-engineering.de, ST=BW, O=R.E. Engineering, L=Sindelfingen, CN=internal-ca, C=DE Valid From: Sat, 04 Aug 2018 13:48:42 +0200 Valid Until: Tue, 01 Aug 2028 13:48:42 +0200		   

[+ Add](#)

Server auf pfSense

- Konfiguration Überblick

The screenshot shows the pfSense web interface for configuring OpenVPN servers. The breadcrumb trail is 'VPN / OpenVPN / Servers'. The 'Servers' tab is selected. Below the breadcrumb, there are navigation links for 'Servers', 'Clients', 'Client Specific Overrides', and 'Wizards'. The main content area is titled 'OpenVPN Servers' and contains a table with the following data:

Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	192.168.249.0/30	Crypto: AES-256-CBC/SHA512	Versuch ischs wert (tun)	 

At the bottom right of the table area, there is a green '+ Add' button.

Server auf pfSense

- Konfigurationsdetails (Teile)

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards

General Information

Disabled Disable this server
Set this option to disable this server without removing it from the list.

Server mode Peer to Peer (Shared Key)

Protocol UDP on IPv4 only

Device mode tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Interface WAN
The interface or Virtual IP address where OpenVPN will receive client connections.

Server auf pfSense

- Konfigurationsmöglichkeiten

Server mode	Peer to Peer (Shared Key)
Protocol	Peer to Peer (Shared Key)
Device mode	Remote Access (SSL/TLS)
	Remote Access (User Auth)
	Remote Access (SSL/TLS + User Auth)

Cryptographic Settings

Shared Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 78ec5a56858cf75f7c07644aa5ca95d1 46ad2a8c80db591c0e92ad643e2e6456</pre>
-------------------	--

Paste the shared key here

Server auf pfSense

- Einfachste Konfiguration ist „Shared Key“
- Braucht keine CA
- Einzelnutzerlösung
- Jeder, der den Schlüssel hat, kommt rein
- Schlüssel nur auf kryptografisch gesicherten Medien aufbewahren
- VPN nur im Urlaub auf Fritzbox geöffnet

Android Client (1/2)

- App „**OpenVPN für Android**“ installieren.
- Für Android muss die Datei `turris.conf` nach `turris.ovpn` umbenannt werden. Auf diese Datei muss man gut aufpassen, sie enthält u.a. den Private Key. Durch Download via „Get Config“ Button (im Webinterface des Routers) gelangt sie auf das Handy.
 - In meinem konkreten Fall muss die Zeile
`remote 192.168.0.2 1194`
nach
`remote <Ihr-DynDNS-name> 1194`
geändert werden.
 - Der Server hält die vom Kabelrouter erhaltene Adresse auf seinem WAN-Interface für seine von außen erreichbare Internetadresse. Wir ersetzen dies durch den dynamischen Hostnamen (hier: von No-IP). **Dies gilt für alle so generierten und heruntergeladenen Client-Konfigurationen (Linux, iOS).**

Android Client (2/2)

- Öffnet man die heruntergeladene Datei mit der App, wird daraus ein VPN-Profil erzeugt. Damit hat die Verbindung auf Anhieb geklappt. Der Client bekam die IP 10.111.111.6, es entsteht offenbar ein Tunnel, an dessen anderem Ende 10.111.111.7 hängt. SSH war damit möglich.
- HTTP ging zunächst nicht, die Lösung der zusätzliche Parameter option mssfix '1300' auf der Serverseite (siehe dort), ohne Änderung am Client.
- Zweites Problem: Es gab keine Namensauflösung für das LAN. Die Lösung brachte ein Traceroute zu einer LAN-Adresse. Es tauchte die Adresse 10.111.111.1 als einziger Hop auf. Die Lösung war ein Eintrag in der Profilkonfiguration unter IP UND DNS:
DNS-Server 10.111.111.1

Linux Client

- Mit der Weboberfläche Foris werden eine Reihe von Schritten für jeden Client durchgeführt. Die resultierende Datei muß dann auf den Client gebracht werden. Sie heißt stets `turris.conf`. Unter Linux kann der Name beibehalten werden.
- Jetzt entweder Zertifikate extrahieren und an zentraler Stelle speichern oder die Datei so einbinden:

```
sudo openvpn --config turris.conf
```

- DNS-Auflösung klappt nicht. Lösung: [hier](#)
- Man muss das Skript erweitern, damit es dynamisch die `/etc/resolv.conf` anpasst. Dafür braucht man das Paket `resolvconf` (war schon vorhanden) oder `openresolv` (wie es an anderer Stelle gefordert wird). Damit ergänzt man `turris.conf` um folgende 3 Zeilen:

```
script-security 2  
up /etc/openvpn/update-resolv-conf  
down /etc/openvpn/update-resolv-conf
```

iOS Client

- Die zu installierende App heißt einfach **OpenVPN Connect**. Die in iOS enthaltene VPN-Unterstützung funktionierte nicht.
- Das Übertragen der wie zuvor (diesmal für iPad generierten, modifizierten und umbenannten) Konfigurationsdatei auf das iPad erwies sich als schwierig, weil die Daten unter iOS nicht ohne weiteres zwischen den Apps austauschbar sind. Am Ende wählte ich den nicht empfohlenen Weg über E-Mail.
- Das HTTP-Problem bestand auch hier (und wurde mit der gleichen Maßnahme auf dem Server mitgelöst)
- Das DNS-Problem bestand nicht.

Windows Client

- Bei der Windows-Version von OpenVPN wird mittlerweile ein GUI mitgeliefert
- Braucht Administratorrechte wegen Änderung der Netzwerkkonfiguration
- Kann Verbindung starten und anhalten
- Zeigt Verbindungsprotokoll in eigenem Fenster
- Eigentliche Konfiguration in Dateien im Verzeichnis „...\\config“

Windows Client

- Inhalt von Verzeichnis „...\\config“

Name	Änderungsdatum	Typ	Größe
 cert.txt	26.05.2013 16:56	Textdokument	1 KB
 Egeler_Home_Internet.ovpn	03.07.2018 14:21	OpenVPN Config File	1 KB
 Egeler_Home_WLAN.ovpn	03.07.2018 14:19	OpenVPN Config File	1 KB
 README.txt	30.01.2016 16:52	Textdokument	1 KB

Windows Client

- Inhalt von „.vpn“-Datei (Teile)
 - auth SHA512
 - cipher AES-256-CBC
 - secret cert.txt
 - dev tun
 - remote taking-it-seriously.de
 - ifconfig 192.168.249.2 192.168.249.1
 - ...

Windows Client

- Inhalt von „cert.txt“
 - #
 - # 2048 bit OpenVPN static key
 - #
 - -----BEGIN OpenVPN Static key V1-----
 - 78ec5a56858cf75f7c07644aa5ca95d1
 - ...
 - -----END OpenVPN Static key V1-----

Nützliche Links

- Grundsatzartikel Wikipedia zu Zertifikaten
 - https://de.wikipedia.org/wiki/Digitales_Zertifikat
- Wikipedia-Artikel zu OpenVPN
 - <https://de.wikipedia.org/wiki/OpenVPN>
- Turris Website: OpenVPN Anleitung für „advanced“ users
 - <https://www.turris.cz/doc/en/howto/openvpn>
- OpenVPN Website: HOWTO
 - <https://openvpn.net/index.php/open-source/documentation/howto.html>
- PfSense OpenVPN HOWTO
 - <https://www.netgate.com/docs/pfsense/vpn/openvpn/openvpn-remote-access-server.html>
- Vergleich VPN-Protokolle
 - <https://thebestvpn.com/pptp-l2tp-openvpn-sstp-ikev2-protocols/>