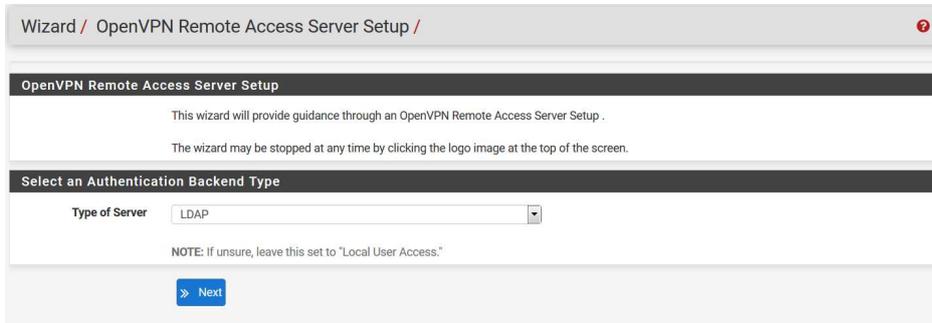


Einrichten von VPN mit dem OpenVPN-Wizard

Das Einrichten von VPN erfolgt durch den Punkt VPN -> OpenVPN, Hier den Punkt Wizard wählen



Wizard / OpenVPN Remote Access Server Setup /

OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .
The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

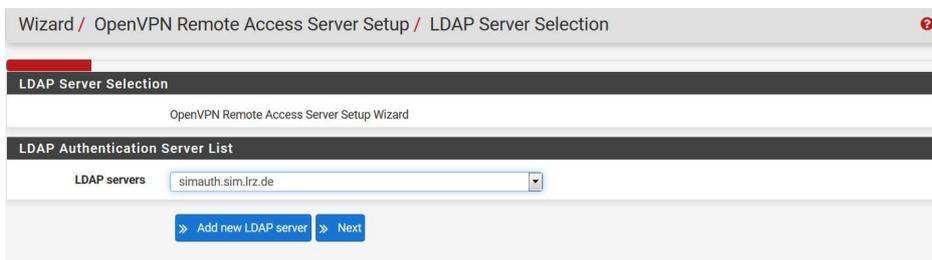
Type of Server

NOTE: If unsure, leave this set to "Local User Access."

[» Next](#)

Es gibt hier die drei Optionen: Local User Database, LDAP, Radius.
Eine lokale Authentifizierung ist in den meisten Fällen nicht gewünscht. Um gegen AD zu authentifizieren,
ist es natürlich nützlich, wenn dieser Server vorab bereits eingetragen ist.

Hier LDAP auswählen und den entsprechenden Server auswählen.



Wizard / OpenVPN Remote Access Server Setup / LDAP Server Selection

LDAP Server Selection

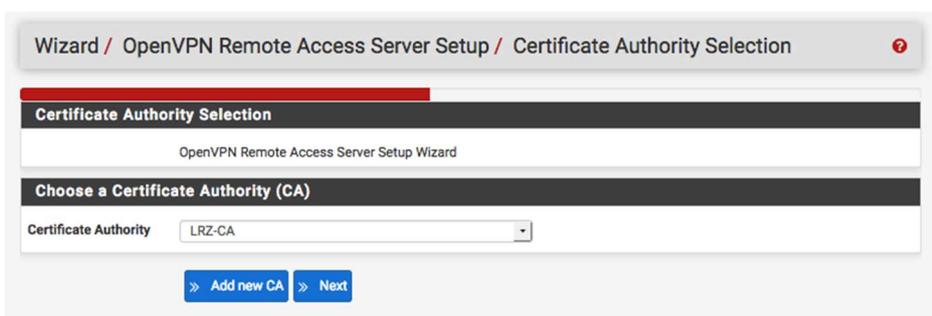
OpenVPN Remote Access Server Setup Wizard

LDAP Authentication Server List

LDAP servers

[» Add new LDAP server](#) [» Next](#)

Certificate Authority (CA)



Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection

Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Certificate Authority (CA)

Certificate Authority

[» Add new CA](#) [» Next](#)

Achtung: Hier muss eine **neue Zertifizierungsstelle hinzugefügt werden (Add new CA)**, der Name ist frei wählbar, z.B. VPN-CA. Die Zertifikate können im erst einmal Self-Signed sein, da das CA-Zertifikat in der OpenVPN-Konfiguration mitgeliefert wird.

Wizard / OpenVPN Remote Access Server Setup / Add Certificate Authority ?

Add Certificate Authority

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Descriptive name
A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.

Key length
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Country Code
Two-letter ISO country code (e.g. US, AU, CA)

State or Province
Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organization
Organization name, often the Company or Group name.

E-mail
E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate.

Als nächstes muss das Server-Zertifikat mit **Add new Certificate** erstellt werden...

Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection ?

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate

Der Name des Servers kann beliebig gewählt werden, da OpenVPN nur die IP-Adresse zum Kontaktieren des Servers verwendet.

Wizard / OpenVPN Remote Access Server Setup / Add a Server Certificate ?

Add a Server Certificate

OpenVPN Remote Access Server Setup Wizard

Create a New Server Certificate

Descriptive name
 A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."

Key length
 Size of the key which will be generated. The larger the key, the more security it offers, but larger keys are generally slower to use.

Lifetime
 Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Country Code
 Two-letter ISO country code (e.g. US, AU, CA)

State or Province
 Full State of Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City
 City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organization
 Organization name, often the Company or Group name.

E-mail
 E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate.

[» Create new Certificate](#)

Allgemeine Einstellungen

Sollte alles richtig sein, bekommt man den folgenden Dialog.

Wizard / OpenVPN Remote Access Server Setup / Server Setup ?

Server Setup

OpenVPN Remote Access Server Setup Wizard

Hier legt man das Interface und den UDP-Port, auf dem der OpenVPN-Server hört, fest.

General OpenVPN Server Information

Interface
 The interface where OpenVPN will listen for incoming connections (typically WAN.)

Protocol
 Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

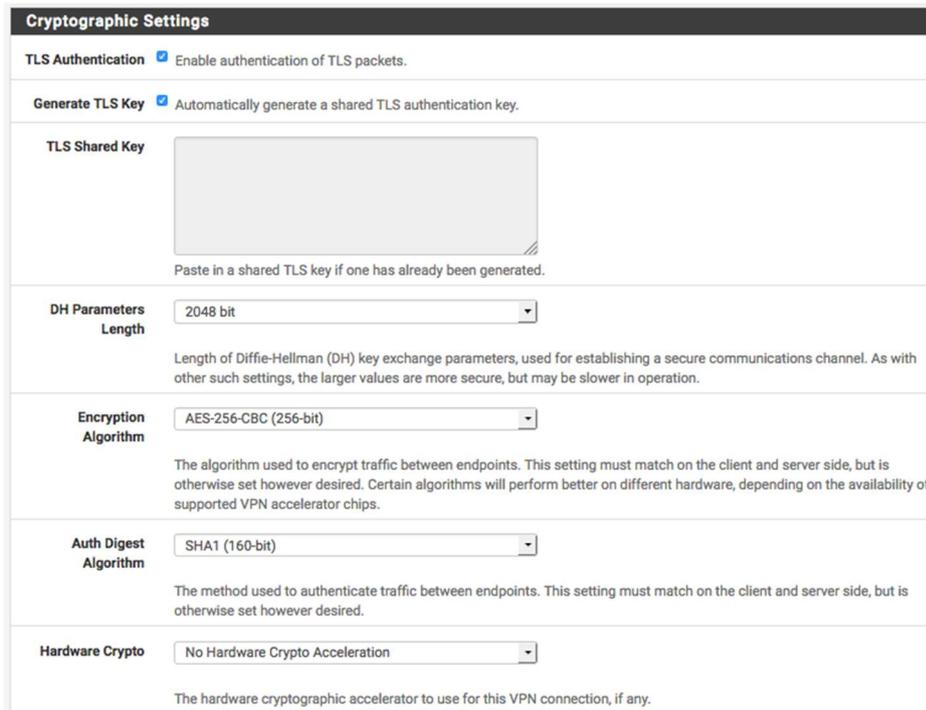
Local Port
 Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

Description
 A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Hier ist es wichtig, als Interface **nicht WAN**, sondern die vorher definierte offizielle **CARP-IP** auszuwählen, sonst bekommt man a) Probleme mit dem OpenVPN-Failover und b) ist der Server nur im MWN erreichbar. Das funktioniert allerdings erst nach Fertigstellen des Wizards beim Editieren der Serviereigenschaften.

Cryptographic settings

Hier kann man alles bei den Voreinstellungen belassen.



Cryptographic Settings	
TLS Authentication	<input checked="" type="checkbox"/> Enable authentication of TLS packets.
Generate TLS Key	<input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
TLS Shared Key	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p>Paste in a shared TLS key if one has already been generated.</p>
DH Parameters Length	<input type="text" value="2048 bit"/> <small>Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. As with other such settings, the larger values are more secure, but may be slower in operation.</small>
Encryption Algorithm	<input type="text" value="AES-256-CBC (256-bit)"/> <small>The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.</small>
Auth Digest Algorithm	<input type="text" value="SHA1 (160-bit)"/> <small>The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.</small>
Hardware Crypto	<input type="text" value="No Hardware Crypto Acceleration"/> <small>The hardware cryptographic accelerator to use for this VPN connection, if any.</small>

Tunnel Settings

Die Clients erhalten bei OpenVPN keine Adresse aus dem internen Netz, sondern landen in einem eigenen Subnetz, für das man auch eigene Zugriffsregeln festlegen kann. Da dieses Netz im Normalfall innerhalb der Firewall bleibt, kann es aus dem Bereich 10.0.0.0/16 vergeben werden, hier im Beispiel 10.0.1.0/24. **Redirect Gateway** bewirkt, dass der komplette Verkehr des Clients über die Firewall geleitet wird, das ist normalerweise nicht gewünscht. Bei **Local Network** müssen die Netze eingetragen werden, die vom OpenVPN-Client aus erreicht werden sollen. Der Server schickt dann beim Verbindungsaufbau diese Routen an den Client, damit dieser diese Netze über den Tunnel anspricht. Das Netz, das eingetragen werden muss, ist normalerweise das LAN.

Tunnel Settings	
Tunnel Network	<input type="text" value="10.0.1.0/24"/> This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
Redirect Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.
Local Network	<input type="text"/> This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent Connections	<input type="text"/> Specify the maximum number of clients allowed to concurrently connect to this server.
Compression	<input type="text" value="No Preference"/> Compress tunnel packets using the LZ0 algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	<input type="checkbox"/> Allow communication between clients connected to this server.
Duplicate Connections	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

Welche Netze sollen hier verwendet werden? Welche IPs ? Standort-Kopplungen ?

Client Settings

Hier werden verschiedene Clienteneinstellungen definiert. Im Beispiel sind hier die LRZ DNS- und NTP-Server angegeben.

Client Settings	
Dynamic IP	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Address Pool	<input checked="" type="checkbox"/> Provide a virtual adapter IP address to clients (see Tunnel Network).
Topology	Subnet – One IP address per client in a common subn <small>Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".</small>
DNS Default Domain	<input type="text"/> <small>Provide a default domain name to clients.</small>
DNS Server 1	10.156.33.53 <small>DNS server IP to provide to connecting clients.</small>
DNS Server 2	129.187.5.1 <small>DNS server IP to provide to connecting clients.</small>
DNS Server 3	<input type="text"/> <small>DNS server IP to provide to connecting clients.</small>
DNS Server 4	<input type="text"/> <small>DNS server IP to provide to connecting clients.</small>
NTP Server	129.187.254.32 <small>Network Time Protocol server to provide to connecting clients.</small>
NTP Server 2	10.156.33.123 <small>Network Time Protocol server to provide to connecting clients.</small>
NetBIOS Options	<input type="checkbox"/> Enable NetBIOS over TCP/IP. <small>If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.</small>
NetBIOS Node Type	none <small>Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).</small>
NetBIOS Scope ID	<input type="text"/> <small>A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.</small>
WINS Server 1	<input type="text"/> <small>A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.</small>
WINS Server 2	<input type="text"/> <small>A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.</small>
Advanced	<input type="text"/> <small>Enter any additional options to add to the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"</small>

Regeln für die Firewall

Ist bei **Traffic from clients to server** ein Haken gesetzt, so wird auf dem WAN/Outside Interface eine Regel angelegt, die den Zugriff über den oben benannten Port (Standard 1194) von beliebigen Absendeadressen erlaubt. Der Haken bei **Traffic from clients through VPN** bewirkt, dass eine **Allow all** Regel auf dem neuen OpenVPN-Interface angelegt wird.

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

Wizard / OpenVPN Remote Access Server Setup / Finished!

Finished!

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

The configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

[» Finish](#)

Damit ist der Wizard fertig.

Nun muss noch, falls konfiguriert, die CARP-Adresse ausgewählt werden. Dazu rechts in der Übersicht bei **Actions** auf das Bleistiftsymbol zum Editieren klicken.

General Information

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

Server mode Remote Access (SSL/TLS + User Auth)

Backend for authentication
TUM_Online
Test-Server-Inst-VPN
BADWLRZ_MA
Local Database

Protocol UDP

Device mode tun

Interface 129.187.255.123 (OpenVPN CARP)

Local port 1197

Description Test1
A description may be entered here for administrative reference (not parsed).

Unter **VPN > OpenVPN** kann man nachsehen, ob der Server läuft: (hier laufen 2 Stück auf Port 1194 und 1197)

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Servers			
Protocol / Port	Tunnel Network	Description	Actions
UDP / 1194	10.0.1.0/24 2001:4ca0:0:FF20::/64	129.187.43.56 EXT	
UDP / 1197	10.0.2.0/24 2001:4ca0:0:FF21::/64	129.187.43.56 EXT 1197	

Add

Status des VPN-Servers überprüfen

Dies geht unter Status > OpenVPN ggf. System Logs ansehen. Sollte alles richtig sein sieht es so aus:

Status / OpenVPN

VPN CIP-Pool UDP:1194 Client Connections					
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
▶ Running					

Hat man einen anderen Port gewählt, ist natürlich auch der Port anderes.

Im Log findet sich, die IPs sind je nach Firewall (hier: 192.168.15.83) verschieden.

Jul 22 08:58:11	openvpn	31588	OpenVPN 2.3.11 amd64-portbsd-freebsd10.3 [SSL (OpenSSL)] [LZO] [MH] [IPv6] built on May 16 2016
Jul 22 08:58:11	openvpn	31588	library versions: OpenSSL 1.0.1s-freebsd 1 Mar 2016, LZO 2.09
Jul 22 08:58:11	openvpn	31790	NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
Jul 22 08:58:11	openvpn	31790	WARNING: POTENTIALLY DANGEROUS OPTION --client-cert-not-required may accept clients which do not present a certificate
Jul 22 08:58:11	openvpn	31790	Control Channel Authentication: using '/var/etc/openvpn/server1.tls-auth' as a OpenVPN static key file
Jul 22 08:58:11	openvpn	31790	TUN/TAP device ovpn1 exists previously, keep at program end
Jul 22 08:58:11	openvpn	31790	TUN/TAP device /dev/tun1 opened
Jul 22 08:58:11	openvpn	31790	ioctl(TUNSIFFMODE): Device busy: Device busy (errno=16)
Jul 22 08:58:11	openvpn	31790	do_ifconfig, tt->ipv6=1, tt->did_ifconfig_ipv6_setup=0
Jul 22 08:58:11	openvpn	31790	/sbin/ifconfig ovpn1 10.0.179.1 10.0.179.2 mtu 1500 netmask 255.255.255.0 up
Jul 22 08:58:11	openvpn	31790	/usr/local/sbin/ovpn-linkup ovpn1 1500 1557 10.0.179.1 255.255.255.0 init
Jul 22 08:58:11	openvpn	31790	UDPv4 link local (bound): [AF_INET]192.168.15.83:1194
Jul 22 08:58:11	openvpn	31790	UDPv4 link remote: [undef]
Jul 22 08:58:11	openvpn	31790	Initialization Sequence Completed