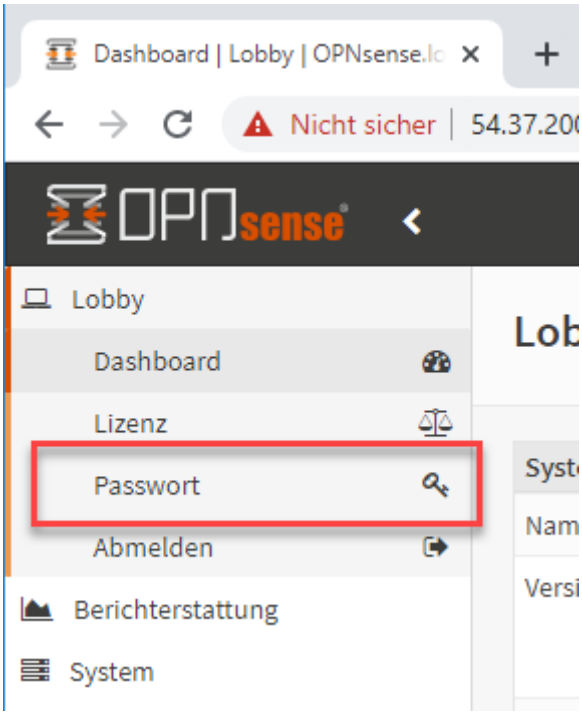
OPNSense Anleitung zur Nutzung mit dem RA-MICRO vSystem: basierend auf Version 20.1.9 – Stand: 11.01.2021

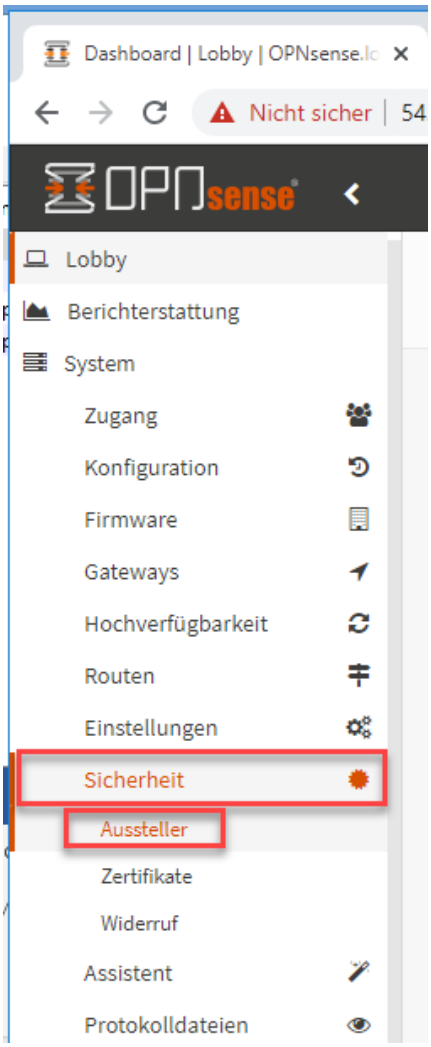
Nutzung ohne Anspruch auf Vollständigkeit und ohne Gewährleistung. Die eingetragenen Werte sind Vorschlagswerte. Letztlich obliegt die richtige Einstellungsauswahl dem jeweiligen Nutzer bzw. des Administrator. Die Felder Beliebiger_Name, usw. bitte mit eigenen Angaben versehen. Nach bestehender OpenVPN-Verbindung ist der vServer grundsätzlich unter der internen IP-Adresse: 172.25.0.2 erreichbar.

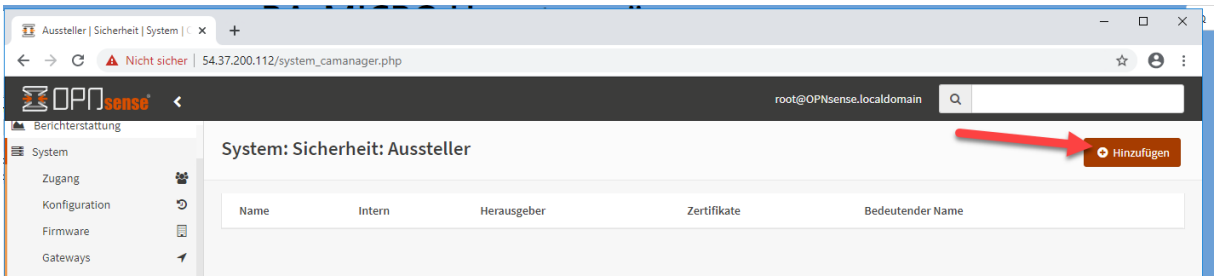
---

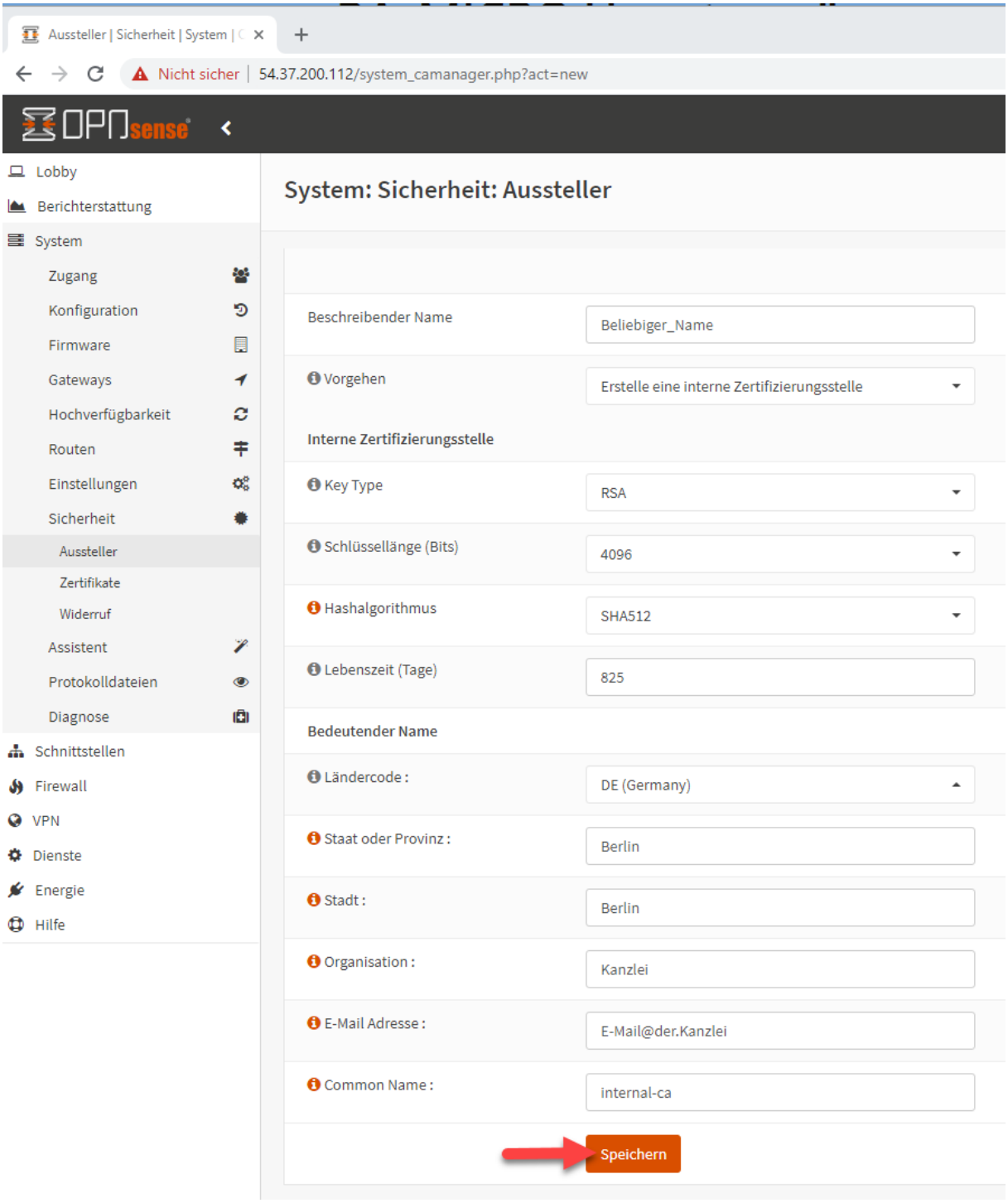
1. Zunächst das Passwort individuell ändern



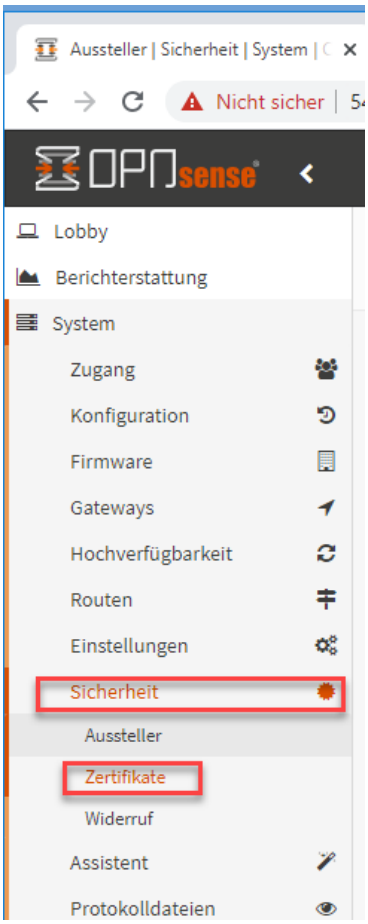
2. Vorbereitung: eigenes Ausstellerzertifikat auf der OPNSense erstellen

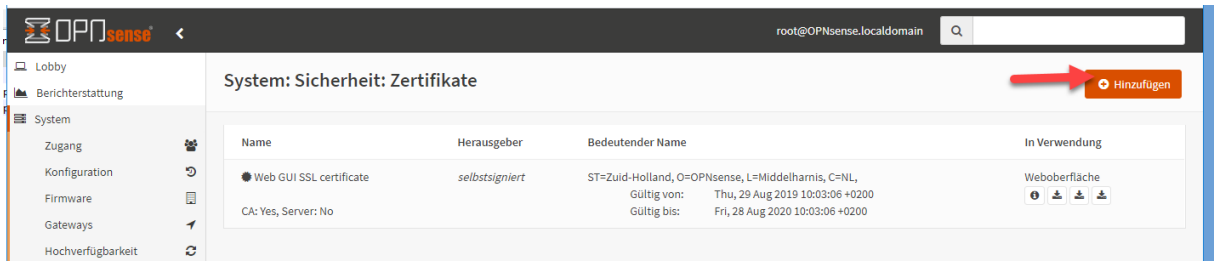


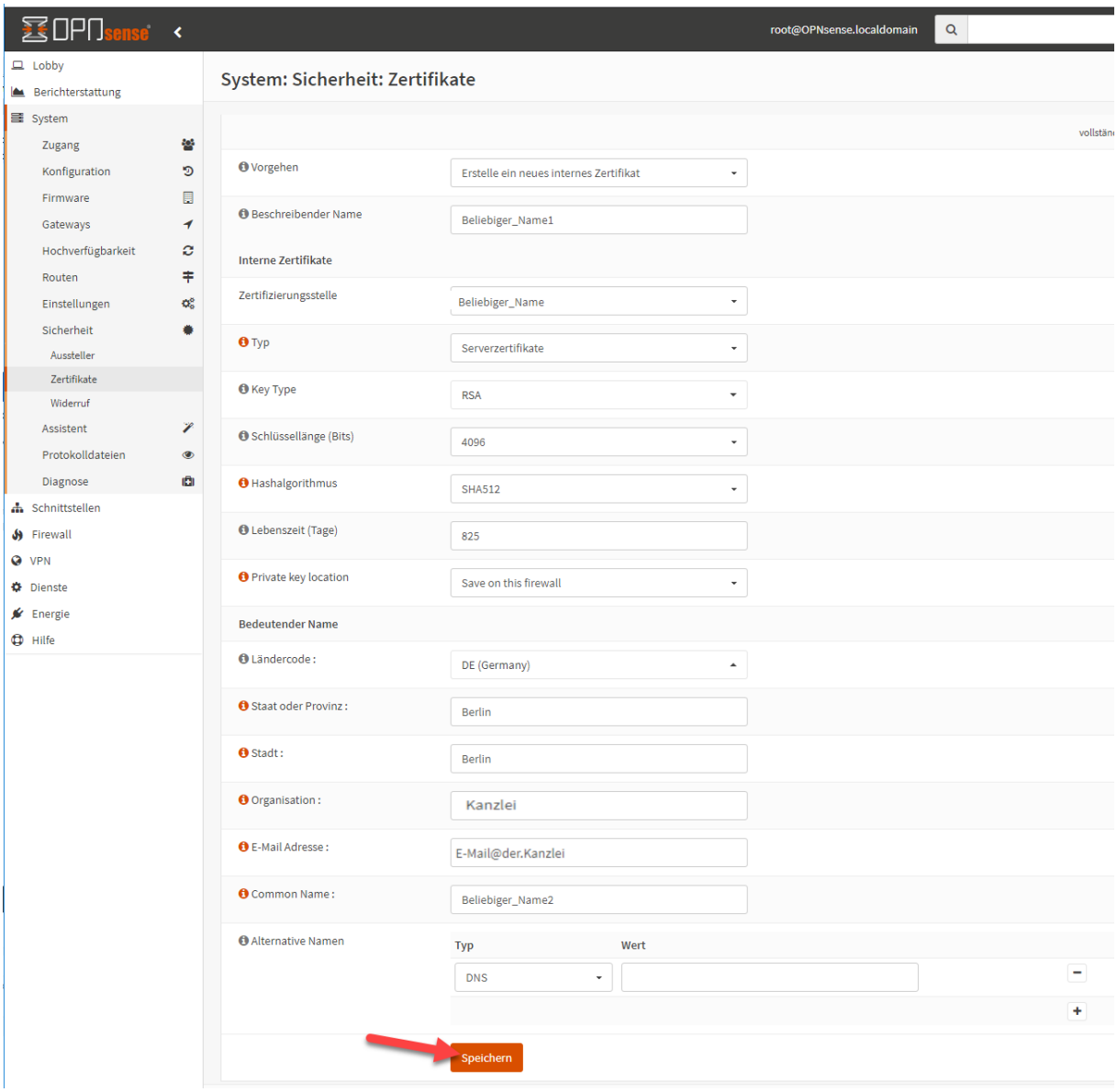



Aussteller | Sicherheit | System |
Nicht sicher | 54.37.200.112/system_camanager.php?act=new
Lobby
Berichterstattung
System
Zugang
Konfiguration
Firmware
Gateways
Hochverfügbarkeit
Routen
Einstellungen
Sicherheit
Aussteller
Zertifikate
Widerruf
Assistent
Protokolldateien
Diagnose
Schnittstellen
Firewall
VPN
Dienste
Energie
Hilfe
System: Sicherheit: Aussteller
Beschreibender Name
Beliebiger_Name
Vorgehen
Erstelle eine interne Zertifizierungsstelle
Interne Zertifizierungsstelle
Key Type
RSA
Schlüssellänge (Bits)
4096
Hashalgorithmus
SHA512
Lebenszeit (Tage)
825
Bedeutender Name
Ländercode :
DE (Germany)
Staat oder Provinz :
Berlin
Stadt :
Berlin
Organisation :
Kanzlei
E-Mail Adresse :
E-Mail@der.Kanzlei
Common Name :
internal-ca
Speichern

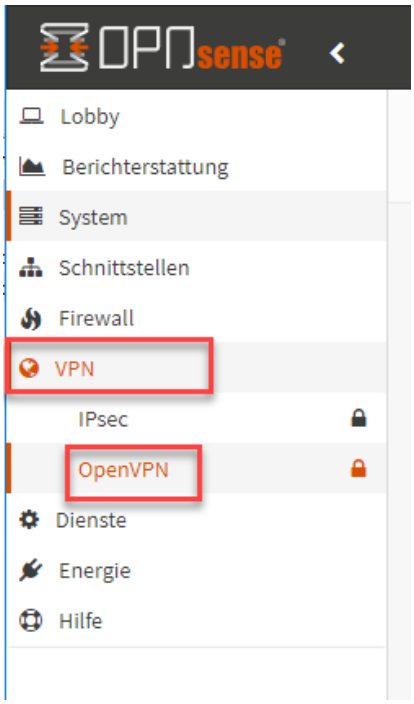
3. Vorbereitung: Serverzertifikat erstellen

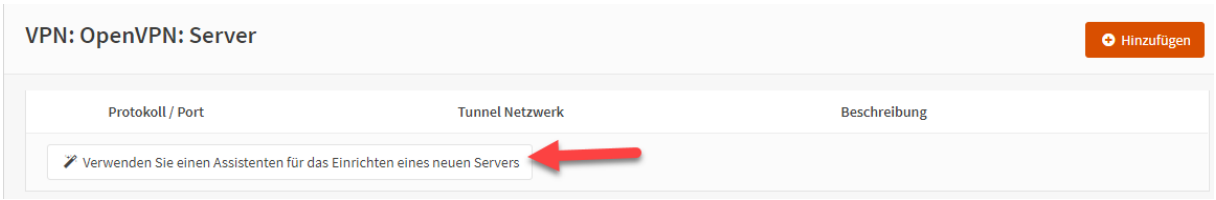


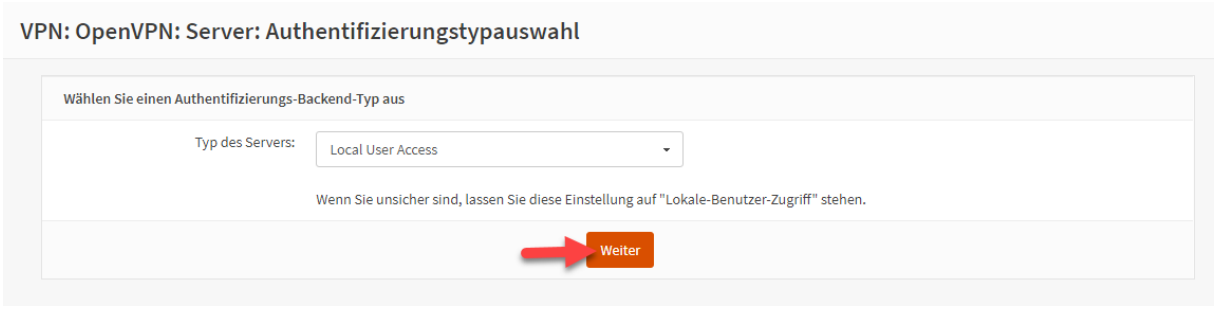


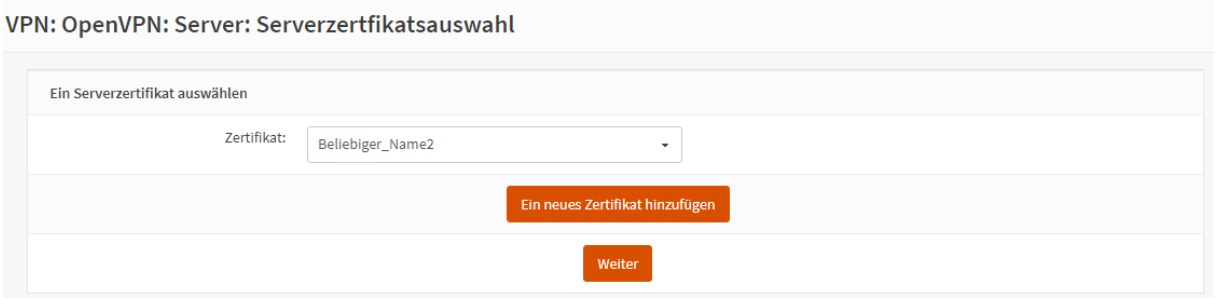

root@OPNsense.localdomain
Lobby
Berichterstattung
System
Zugang
Konfiguration
Firmware
Gateways
Hochverfügbarkeit
Routen
Einstellungen
Sicherheit
Aussteller
Zertifikate
Widerruf
Assistent
Protokolldateien
Diagnose
Schnittstellen
Firewall
VPN
Dienste
Energie
Hilfe
System: Sicherheit: Zertifikate
Vorgehen
Erstelle ein neues internes Zertifikat
Beschreibender Name
Beliebiger_Name1
Interne Zertifikate
Zertifizierungsstelle
Beliebiger_Name
Typ
Serverzertifikate
Key Type
RSA
Schlüssellänge (Bits)
4096
Hashalgorithmus
SHA512
Lebenszeit (Tage)
825
Private key location
Save on this firewall
Bedeutender Name
Ländercode :
DE (Germany)
Staat oder Provinz :
Berlin
Stadt :
Berlin
Organisation :
Kanzlei
E-Mail Adresse :
E-Mail@der.Kanzlei
Common Name :
Beliebiger_Name2
Alternative Namen
Typ
Wert
DNS
Speichern

4. OpenVPN-Server einrichten per Assistent:









VPN: OpenVPN: Server: Servereinrichtung

Allgemeine OpenVPN-Serverinformation

Schnittstelle: WAN

Die Schnittstelle, über die OpenVPN auf eingehende Verbindungen wartet.

Protokoll: UDP

Protokoll für OpenVPN-Verbindungen. Wenn Sie unsicher sind, lassen Sie diese Einstellung auf UDP.

Lokaler Port: 1194

Lokaler Port, auf dem OpenVPN auf Verbindungen wartet. Der Standard-Port ist 1194. Lassen Sie dieses Feld leer, um einen unbenutzten Port automatisch auszuwählen.

Beschreibung: Beliebiger__Name_OpenVPN

Ein Name für diese OpenVPN-Instanz zu Ihrer Referenz. Er kann auf alles gesetzt werden, was Sie wollen aber es wird oft genutzt, um den Zweck des Dienstes (z. B. "Technische Außenstellen") anzugeben.

Kryptografische Einstellungen

TLS Authentifikation: ☑ Aktiviere die Authentifizierung von TLS-Paketen.

Generiere einen TLS-Schlüssel: ☑ Automatisch einen gemeinsamen TLS-Authentifizierungsschlüssel generieren.

Gemeinsamer TLS-Schlüssel:

Fügen Sie einen gemeinsamen TLS-Schlüssel ein, falls bereits einer generiert wurde.

DH Parameterlänge: 4096 bit

Länge der Diffie-Hellman (DH) Schlüsselaustausch Parameter. Wird für den Aufbau eines sicheren Kommunikationskanals verwendet. Je grösser diese Werte umso sicherer ist der Kanal allerdings könnte es aber auch den Betrieb verlangsamen.

Verschlüsselungsalgorithmus: AES-256-CBC (256 bit key, 128 bit block)

The method used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however you like. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.

Authentifizierungs-Digestalgorithmus: SHA512 (512-bit)

The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however you like.

Hardwarekryptografie:	No Hardware Crypto Acceleration Der zu verwendende Hardware-Beschleuniger für diese VPN Verbindung. Falls überhaupt einer verwendet werden kann.
Tunneleinstellungen	
IPv4 Tunnelnetzwerk:	10.10.0.0/24 Dies ist das virtuelle IPv4-Netzwerk, welches für die private Kommunikation zwischen diesem Server und den Client-Hosts, dargestellt als CIDR (z. B. 10.0.8.0/24), verwendet wird. Die erste Netzwerkadresse wird der virtuellen Serverschnittstelle zugewiesen. Die verbleibenden Netzwerkadressen können optional den verbindungsaufbauenden Clients zugewiesen werden. (siehe Adresspool)
IPv6 Tunnelnetzwerk:	Dies ist das virtuelle IPv6-Netzwerk, welches für die private Kommunikation zwischen Server und Client-Hosts verwendet wird, das als CIDR (z. B. fe80::/64) angegeben wird. Die erste Adresse wird der virtuellen Schnittstelle des Servers zugewiesen, die verbleibenden Adressen können optional den verbindenden Clients zugewiesen werden. (siehe Adresspool)
Weiterleitungs Gateway:	Erzwinge, dass sämtlicher vom Client generierter Datenberkehr durch den Tunnel geleitet wird.
Lokales IPv4-Netzwerk:	172.25.0.0/24 These are the IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
Lokales IPv6-Netzwerk:	These are the IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
Fernes IPv4-Netzwerk:	These are the IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. You may leave this blank if you don't want a site-to-site VPN.
Fernes IPv6-Netzwerk:	These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN/s here. You may leave this blank if you don't want a site-to-site VPN.
Gleichzeitige Verbindungen:	Geben Sie die maximale Anzahl an Clients an, die gleichzeitig mit diesem Server verbunden sein dürfen.
Komprimierung:	Keine Einstellung Komprimiere Tunnelpakete mit dem LZO-Algorithmus. Die adaptive Kompression wird dynamisch die Komprimierung für eine gewisse Zeitdauer deaktivieren, falls OpenVPN erkennt, dass die Daten nicht effizient genug komprimiert werden.

Typ des Dienstes:	☐ Setze die TOS-IP-Kopfzeile von Tunnelpaketen auf den Wert, den das gekapselte Paket hat.
Kommunikation zwischen den Clients:	☐ Erlaube die Kommunikation zwischen den Clients, die mit diesem Server verbunden sind.
Doppelte Verbindungen:	☐ Allow multiple concurrent connections from clients using the same Common Name. This is not generally recommended, but may be needed for some scenarios.

Client Einstellungen

Dynamische IP:	☑ Erlaube verbundenen Clients, die Verbindung beizubehalten, wenn deren IP-Adresse sich ändert.
Adresspool:	☑ Stelle den Clients eine virtuelle Adapter-IP-Adresse zur Verfügung (siehe Tunnelnetzwerk).
DNS Standard Domain:	Stelle einen Standarddomainnamen den Clients zur Verfügung.
DNS-Server 1:	DNS-Server, der den verbindenden Clients zur Verfügung gestellt wird.
DNS-Server 2:	DNS-Server, der den verbindenden Clients zur Verfügung gestellt wird.
DNS-Server 3:	DNS-Server, der den verbindenden Clients zur Verfügung gestellt wird.
DNS-Server 4:	DNS-Server, der den verbindenden Clients zur Verfügung gestellt wird.
NTP-Server:	Netzwerkzeitprotokollserver, der den verbindenden Clients zur Verfügung gestellt wird.
NTP-Server 2:	Netzwerkzeitprotokollserver, der den verbindenden Clients zur Verfügung gestellt wird.
NetBIOS Optionen:	☐ Aktivierung von NetBIOS über TCP. Ist diese Option nicht aktiviert, so werden auch alle NetBIOS-TCP Optionen (inklusive WINS) deaktiviert.
NetBIOS-Knotentyp:	none Mögliche Optionen b-node (Broadcasts), p-node (Punkt-zu-Punkt-Namensabfragen an einen WINS-Server), m-node (Broadcast, dann Namensserver abfragen), und h-node (Namensserver Abfragen, dann Broadcast)
NetBIOS-Scope-ID:	Eine NetBIOS-Scope-IP stellt einen erweiterten Benennungsdienst für NetBIOS über TCP/IP zur Verfügung. Die NetBIOS-Scope-ID isoliert NetBIOS-Datenverkehr auf einem einzelnen Netzwerk auf die Knoten mit der gleichen NetBIOS-Scope-ID.
WINS-Server 1:	Stellt einen Windows Internet Name Service (WINS) Server für verbindende Clients bereit, welcher es erlaubt Windows Freigaben anzuzeigen. Dies ist typischerweise ein Active Directory Domain Controller, designierter WINS Server oder Samba Server
WINS-Server 2:	Stellt einen Windows Internet Name Service (WINS) Server für verbindende Clients bereit, welcher es erlaubt Windows Freigaben anzuzeigen. Dies ist typischerweise ein Active Directory Domain Controller, designierter WINS Server oder Samba Server

Weiter

VPN: OpenVPN: Server: Firewallregelkonfiguration

Firewallregelkonfiguration

Firewallregeln steuern, welcher Datenverkehr erlaubt ist. Sie müssen Regeln erstellen, die Datenverkehr zur IP und dem Port des OpenVPN-Servers zurlassen sowie Datenverkehr, der von verbundenen Clients durch den Tunnel gesendet wird. Diese Regeln können hier automatisch hinzugefügt werden oder manuell nach Abschluss des Assistenten hinzugefügt werden.

Datenverkehr von Clients an den Server

Firewallregel: ☑ Fügen Sie eine Regel hinzu, um Datenverkehr von Clients im Internet zum OpenVPN-Serverprozess zu erlauben.

Datenverkehr von Clients durch das VPN

OpenVPN-Regel: ☑ Fügen Sie eine Regel hinzu, um jeglichen Datenverkehr von Clients durch den Tunnel zu erlauben.

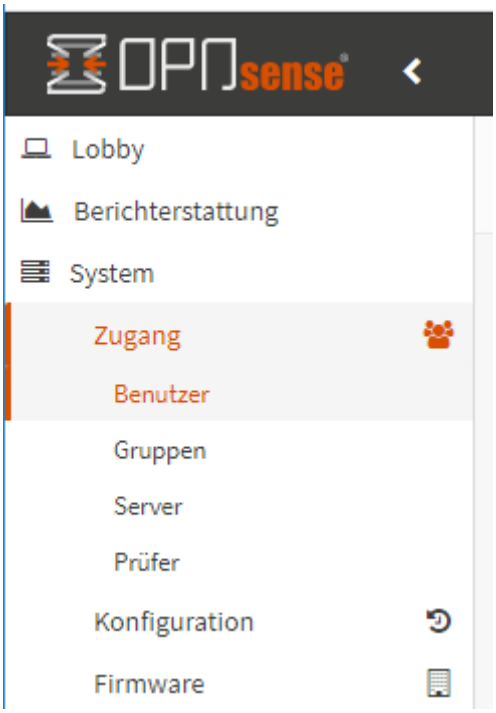
Weiter

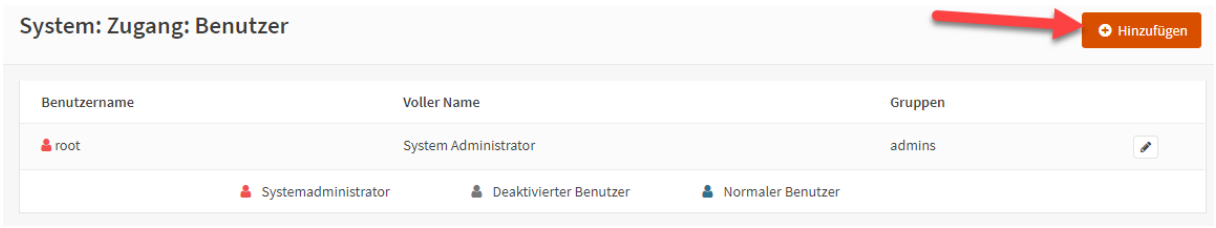
VPN: OpenVPN: Server: Abgeschlossen!

Ihre Konfiguration ist nun vollständig.

Fertigstellen

5. Benutzer + Benutzerzertifikate anlegen, die per OpenVPN zugreifen können sollen:





System: Zugang: Benutzer

vollständige Hilfe

Definiert durch	USER
Deaktiviert	☐
Benutzername	Benutzer_Name
Passwort	••••••••••••••••
	•••••••••••••••• (Bestätigung)
	☐ Generiere ein zufälliges Passwort, um für diesen Nutzer lokale Zugriffe auf die Datenbank zu verhindern.
Voller Name	Vorname und Nachname
E-Mail	e-mail@des.Benutzers
Beschreibung	
Preferred landing page	
Sprache	Standard
Anmeldeshell	/sbin/nologin
Ablaufdatum	
Gruppenmitgliedschaften	Kein Mitglied von: admins → Mitglied von:
Zertifikat	☑ Klicken Sie hier um ein Benutzerzertifikat zu erstellen.
OTP-Seed	
	☐ Erstelle ein neues Geheimnis (160 Bit)
Autorisierte Schlüssel	Hier einfügen eines autorisierten Schlüssels.
IPsec Pre-Shared Schlüssel	

Speichern | Speichern und zurückkehren | Abbrechen

System: Sicherheit: Zertifikate

vollständige Hilfe

Vorgehen	Erstelle ein neues internes Zertifikat
Beschreibender Name	Benutzer_Name

Interne Zertifikate

Zertifizierungsstelle	Beliebiger_Name
Typ	Client Zertifikat
Key Type	RSA
Schlüssellänge (Bits)	4096
Hashalgorithmus	SHA512
Lebenszeit (Tage)	825
Private key location	Save on this firewall

Bedeutender Name

Ländercode :	DE (Germany)
Staat oder Provinz :	Berlin
Stadt :	Berlin
Organisation :	Kanzlei
E-Mail Adresse :	e-mail@des.Benutzers
Common Name :	Benutzer_Name

Alternative Namen

Typ	Wert
DNS	

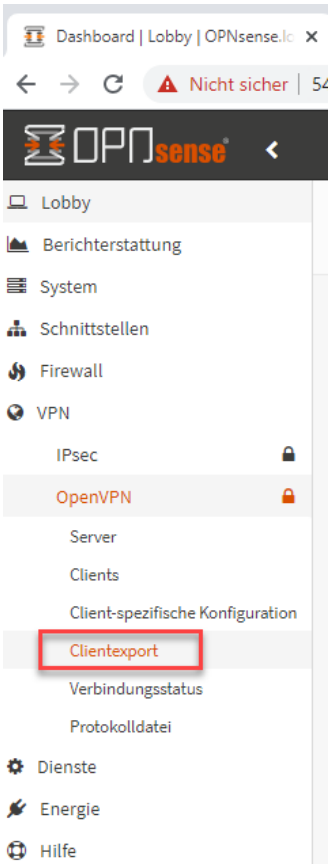
Speichern

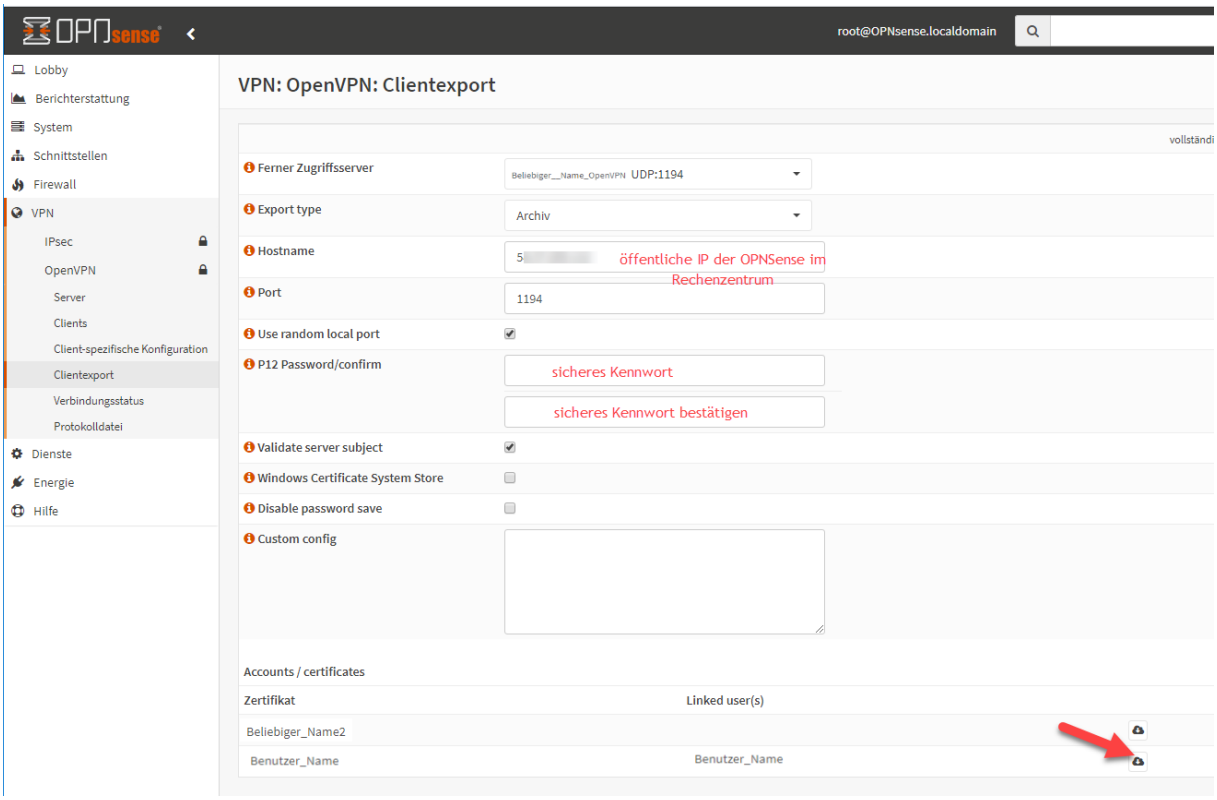
Effektive Berechtigungen	Geerbt von / Typ / Name
Benutzerzertifikate	Name: Benutzer_Name; CA: Beliebiger_Name; Gültig von: Wed, 18 Mar 2020 10:38:16 +0100; Valid To: Tue, 21 Jun 2022 11:38:16 +0200
API-Schlüssel	Schlüssel
OTP-Seed	Erstelle ein neues Geheimnis (160 Bit)
Autorisierte Schlüssel	Hier einfügen eines autorisierten Schlüssels.
IPsec Pre-Shared Schlüssel	

Speichern | Speichern und zurückkehren | Abbrechen

6. Benutzerkonfiguration und -zertifikate für OpenVPN-Client exportieren und herunterladen

Entweder als archiv/zip (PC) oder als „Nur Datei" für MacOS, iOS und Android.





7. Client Installation

Windows 10 PCs:

Den notwendigen OpenVPN-Client für den PC finden Sie aktuell unter https://swupdate.openvpn.org/community/releases/OpenVPN-2.5.0-I601-amd64.msi

Die heruntergeladene msi-Datei starten und dem Assistenten folgen (immer mit weiter bzw. next).

Danach Icon „OpenVPN" auf dem Desktop starten und den angezeigten Speicherpfad in der folgenden Meldung notieren.

Die heruntergeladene ZIP Datei „hier entpacken" und den angezeigten entpackten Ordner in das Benutzerverzeichnis in den Speicherpfad aus der o.g. Meldung idR C:\Benutzer\BENUTZERNAME\OpenVPN\config kopieren.

Anschließend in der Taskleiste auf „verbinden" gehen und OpenVPN Benutzername und Passwort sowie das p12-Kennwort eintragen und ggf. lokal speichern.

Bei den folgenden Betriebssystemen ist es empfehlenswert beim Clientexport (siehe oben unter 6.) das Exportformat „**Nur Datei**" zu wählen. Dabei sollte die exportierte Datei aus **Sicherheitsgründen nicht per E-Mail verschickt** werden sondern idealerweise auf einem Gerät, das direkt mit der OpnSense im Rechenzentrum per Browser verbunden ist, heruntergeladen und z.B. per iTunes mit Kabelverbindung oder sonst per USB-Verbindung in die entsprechende App direkt übertragen werden.

MacOS:

Den Link für den Tunnelblick-OpenVPN-Client für MacOS finden Sie hier: https://tunnelblick.net/release/Tunnelblick_3.8.4_build_5600.dmg

Die offizielle Installations- und Einrichtungsanleitung finden Sie unter https://tunnelblick.net/cInstall.html

iOS/iPadOS:

https://apps.apple.com/de/app/openvpn-connect/id590379981

Android:

https://play.google.com/store/apps/details?id=net.openvpn.openvpn