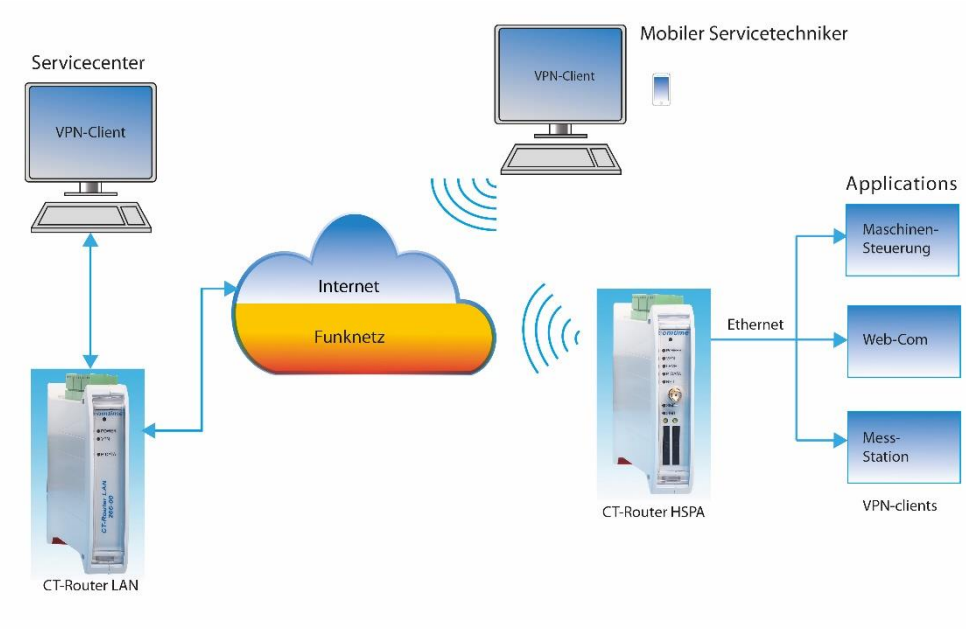
Benutzerhandbuch

CT-VPN Server



Copyright © comtime GmbH

comtime GmbH
Gutenbergring 22
22848 Norderstedt
Germany

Tel: +49 (0)40 55 44 89 40
Fax: +49 (0)40 55 44 89 45

Internet: http://www.comtime-com.de
email: support@comtime-com.de

Technische Änderungen vorbehalten.

Artikel-Nr.:

Inhalt

Allgemeines **4**
Server Konfiguration **5**
Hauptmenü **6**
VPN Server Konfigurieren **6**
Gruppen anlegen **9**
Clients anlegen **10**
Verbindung Staus **11**

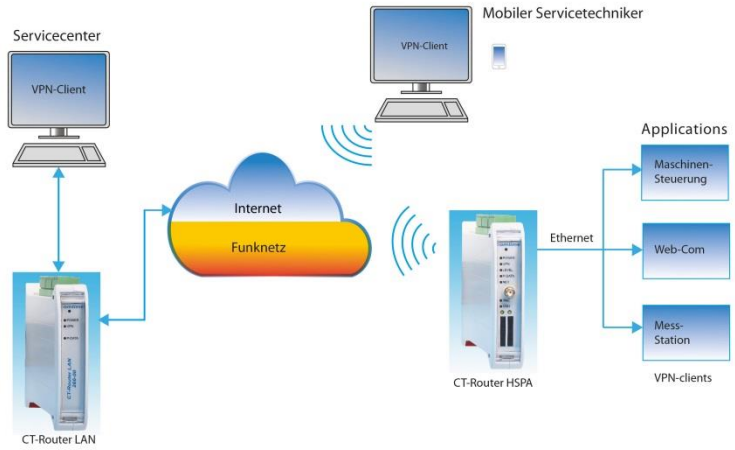
Allgemeines

Mit dem CT-VPN Server können Sie Ihre kompletten Netzwerke, Maschinen, Anlagen und Leitstellen flexibel und einfach miteinander verbinden und bedienen. Durch die 1:1 NAT Unterstützung können Maschinen, Steuerungen, Anlagen, etc. immer mit den gleichen IP-Adressen miteinander vernetzt werden.
Zertifikate für die zu verbindenden Geräte und für PC`s werden automatisch erstellt. Für die CT-Router Serie (LAN, ADSL, GPRS, UMTS, LTS) wird auch die VPN-Konfiguration Datei automatisch erstellt und kann inkl. Zertifikat in den Router eingespielt werden.
Fremdgerät können ebenso in das VPN-Portal eingebunden werden, vorausgesetzt sie unterstützen OpenVPN, p12 Zertifikate und TLS Authentication.

Den CT-VPN Server gibt es als gehostete Lösung in einem Rechenzentrum, als Virtuelle Maschine (VM) beim Kunden, oder als Server-Hardware Variante. Die Anzahl der VPN-Verbindungen ist frei skalierbar was Ihnen einen individuellen Aufbau Ihrer Projekte ermöglicht.

Grundfunktionen

- Anzahl der VPN-Tunnel frei skalierbar
- Autom. Erstellung von Zertifikaten
- Freie Wahl der IP-Adressen
- Automatische Erzeugung der Router-Konfiguration
- Gruppenbildung und Verbindungskontrolle
- Administrations- und Mandantenverwaltung
- Vergabe von Zugriffsrechten innerhalb von Gruppen und Benutzern



Systemanforderung:

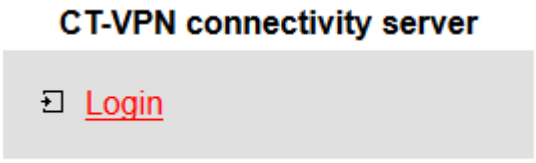
- Linux Debian 8.x
- 1 GB RAM
- 100 MB Programm Speicher

Die Konfiguration des CT-VPN Server erfolgt über eine Webbrowser.
Hierfür müssen zunächst folgende Bedingungen erfüllt sein:

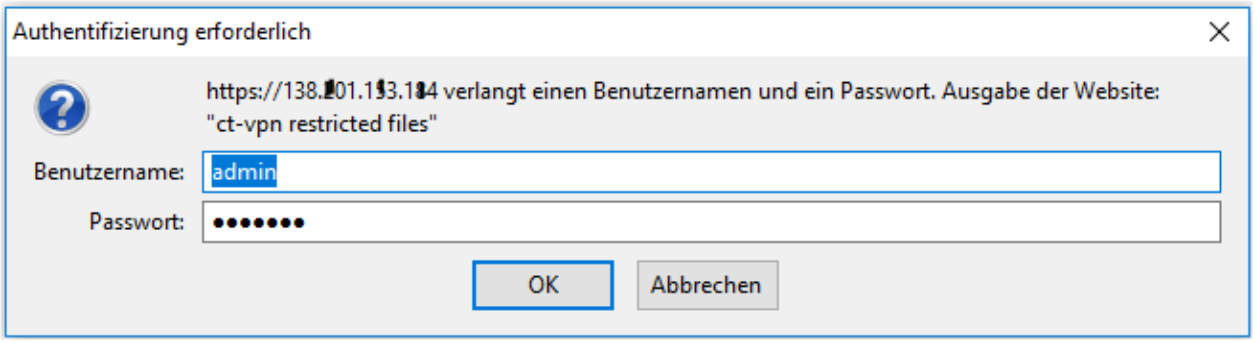
- Der Computer, der zur Konfiguration verwendet wird, verfügt über einen Zugang zum Internet.
- Auf dem Computer ist ein Webbrowser installiert (z.B. Google Chrome, Mozilla Firefox, Microsoft Internet Explorer).

Start der Konfiguration

- Webbrowser öffnen.
- Die IP-Adresse CT-VCS (z.B. 78.46.137.159) in das Adressfeld des Browsers eingeben und mit Eingabe bestätigen.
- Login anklicken.



- Anschließend erfolgt eine Benutzername/Passwort-Abfrage.



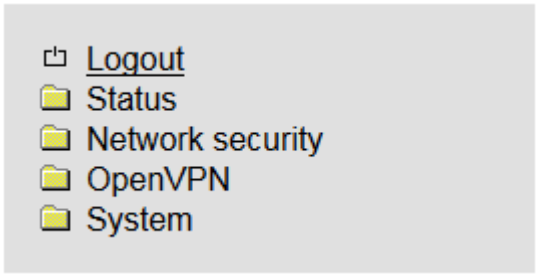
Im Auslieferungszustand lautet der Benutzername „admin“ und das Passwort „admin“ (das Ändern des Passwortes wird unter dem Punkt „System“ >> „User“ beschrieben).
Es gibt zwei User-Level:

- User: Lesezugriff auf „Device Information“
- Admin: Lese- und Schreibzugriff auf alle Bereiche

Nach der Eingabe des Benutzernamens und des Passwortes öffnet sich das Hauptmenü des CT-VCS.

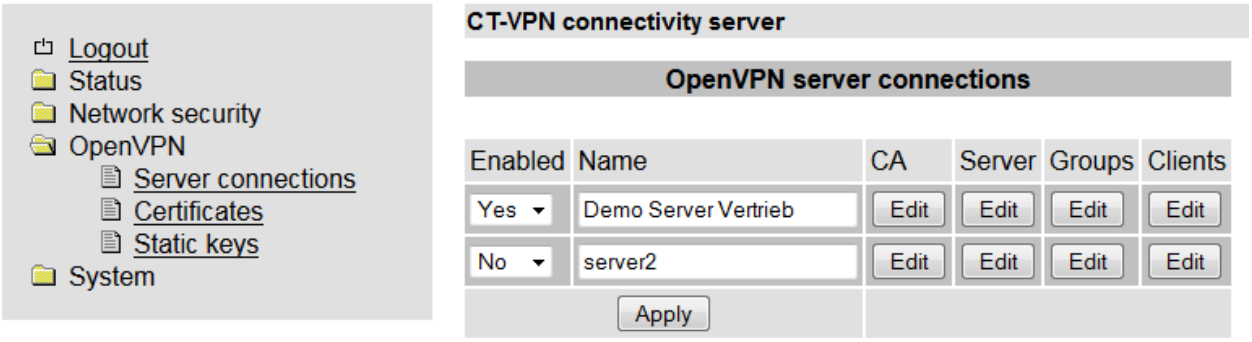
Server Konfiguration

Hauptmenü



VPN Server Konfigurieren

Rufen Sie den Menüpunkt „OpenVPN“ und starten Sie mit der Konfiguration des Server1



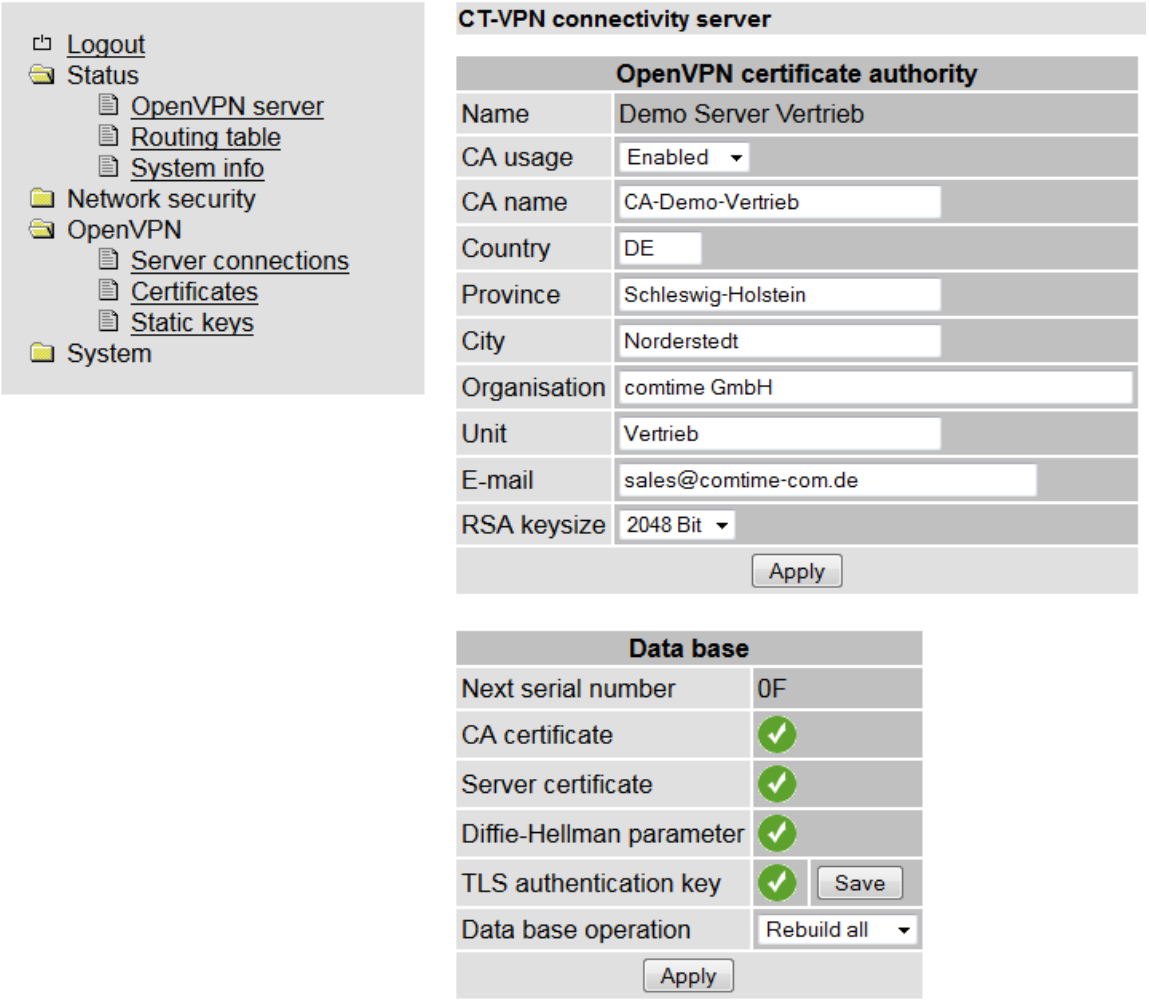
Tragen Sie den gewünschten Namen in das Feld von „Server1“ ein und bestätigen dies mit „Apply“.
Nun können Sie die weiter Konfiguration des Servers durchführen, beginnend mit der CA Erstellung.

Nach Abschluss der Konfiguration stellen Sie den Server1 im Feld „Enable“ von „no“ auf „Yes“ und bestätigen dies mit „Apply“.

CA (Master - Zertifikat) für die Server erstellen

Tragen Sie die Daten für das Zertifikat in en vorgegebenen Feldern ein und bestätigen Sie mit „Apply“
Danach aktivieren Sie die Zertifikate indem Sie „Data base operation“ auf „Rebuild all“ stellen und mit „Apply“ bestätigen.

ACHTUNG: Wenn das „Master“ CA später in Betrieb neu erstellt wird werden alle Client Zertifikate ungültig und müssen wieder neu erstellt werden



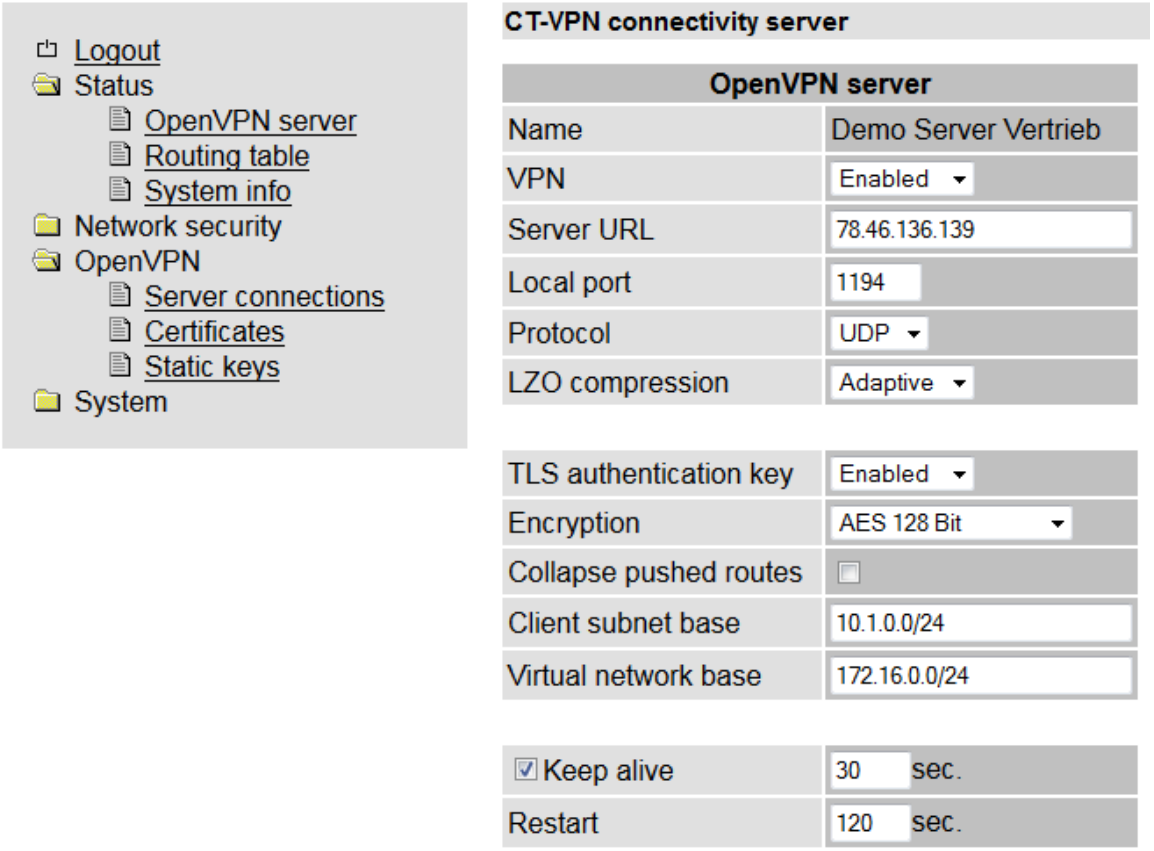
Server connections	
OpenVPN certificate authority	
CA usage	Enable -> Zertifkate und VPN-Konfiguration kann erstellt werden Disable -> keine Zertifkate und VPN-Konfiguration Erstellung möglich
CA name	Vergeben Sie ein CA Namen für diesen Server (z.B. den Servernamen)
Country	z.B. DE (Deutschland)
Province	z.B. SH (Schleswig-Holstein)
City	z.B. Norderstedt
Organisation	z.B. Comtime GmbH
Unit	z.B. Vertrieb
E-mail	z.B. sales@comtime-com.de
RSA keysize	1024 oder 2048 (höchste Sicherheit)

Server Konfiguration

Konfiguration der Server

Es können bis zu 16 VPN-Server Instanzen mit unterschiedlicher Konfiguration angelegt werden

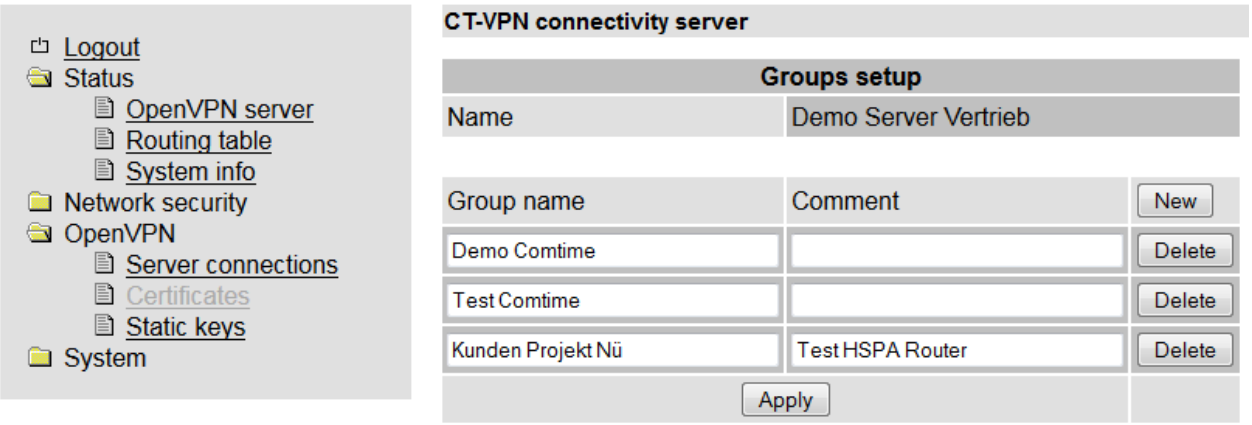
ACHTUNG: Die Port`s, die „Client subnet base“ und die „Virtuel network base“ Adressen müssen zwischen den einzelnen Server Instanzen unterschiedlich sein.



Server connections	
OpenVPN Server	
VPN	Server aktivieren (=Yes) oder deaktivieren (=No)
Server URL	IP-Adresse oder URL des Servers eintragen
Local Port	Port des Servers (default 1194) **Achtung:** Die Ports von den einzelnen Server müssen unterschiedlich sein
Protocol	UDP oder TCP (default UDP)
LZO compression	Komprimierung: Ein/Ausschalten, (default Adaptive)
TLS authentication key	Aktiveren/deaktivieren
Encrypion	Verschlüsselungsalgorithmus auswählen
Collpse pushed routes	Fast einzelne Routen zusammen (experimentelle Funktion)
Client subnet base	Adressen mit denen die Clients (Geräte , Netze) erreicht werden
Virtual network base	
Keep alive	Zeitintervall in Sekunden von Keep Alive-Anfragen an die Gegenstelle
Restart	Zeitspanne in Sekunden nach der die Verbindung neu gestartet werden soll, falls keine Antwort auf die Keep Alive-Anfragen erfolgt.

Gruppen für die Server anlegen

Es können max. 64 Gruppen pro Server vergeben werden.

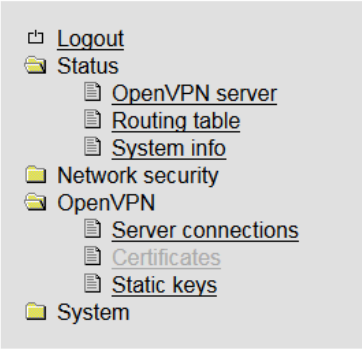


Group name und bei Bedarf Comment eintragen und mit „Apply“ bestätigen.
Die Zuordnung der Clients zu den einzelnen Gruppen erfolgt unter dem Pkt. „Clients“ >> „Access“

Clients anlegen

Clients für die Server anlegen

Unter „Server“ und „Virtual network base“ kann die Anzahl der Client eingestellt werden
Bei einem z.B. 172.18.0.0**/24** Netz sind die 62 Client bei einem **/20** Netz 1022 Clients

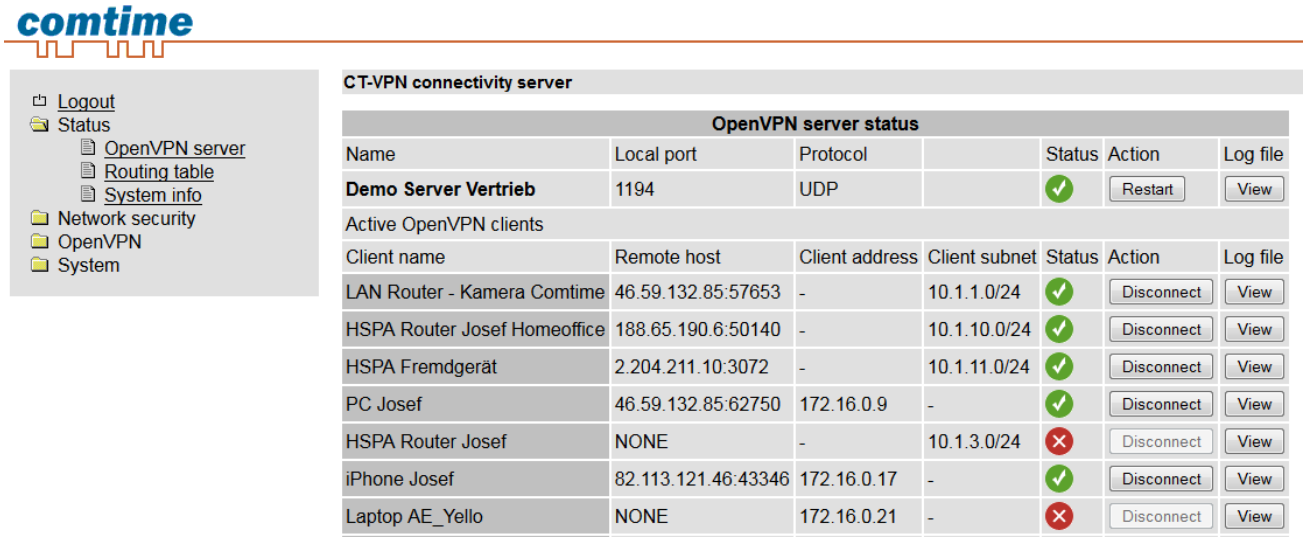


CT-VPN connectivity server

OpenVPN clients					
Name	Demo Server Vertrieb				
Client table (62 max)					
Enabled/Client name	Client address	Client subnet	Service	Access	New
#1 ☑ LAN Router - Kamera Comtime	172.16.0.5	☑ 10.1.1.0/24	Entry	Edit	Delete
#2 ☑ PC Josef	172.16.0.9	☐ 10.1.2.0/24	Entry	Edit	Delete
#3 ☑ HSPA Router Josef	172.16.0.13	☑ 10.1.3.0/24	Entry	Edit	Delete
#4 ☑ iPhone Josef	172.16.0.17	☐ 10.1.4.0/24	Entry	Edit	Delete
#5 ☑ Laptop AE_Yello	172.16.0.21	☐ 10.1.5.0/24	Entry	Edit	Delete
#6 ☑ Homeoffice PC Josef	172.16.0.25	☐ 10.1.6.0/24	Entry	Edit	Delete
#7 ☑ Testplatz PC Josef	172.16.0.29	☐ 10.1.7.0/24	Entry	Edit	Delete

- Mit dem Button „New“ einen neuen Client anfordern.
- Client name eintragen und mit „Apply“ bestätigen
- Unter „Access“ >> „Edit“ dem Client der gewünschten Gruppe (Member of group) zuordnen und mit Save abspeichern
- Unter „Service“ >> „Entry“ und **“Client router configuration”** Tunnel auswählen (nur bei Router-zertifikat -> #1 bis #8) und das Zertifikat durch drücken der „Save“ – Taste downloaden
  - für die PC-Seite ist dies eine xxx.ovpn Datei
  - für den Router eine xxx.xml Datei (Zertifikat + VPN-Konfiguration)

Statusanzeige der Client Verbindungen



Angezeigt werden:

- Remote host address
- Client address
- Client subnet address

Mit der Button “Disconnect” wird die VPN-Verbindung getrennt und wieder neu gestartet (ca. 2 Minuten)
Mit der Button „View“ kann man die Verbindungsdaten (Zeit und Datenmenge) sehen und downloaden.