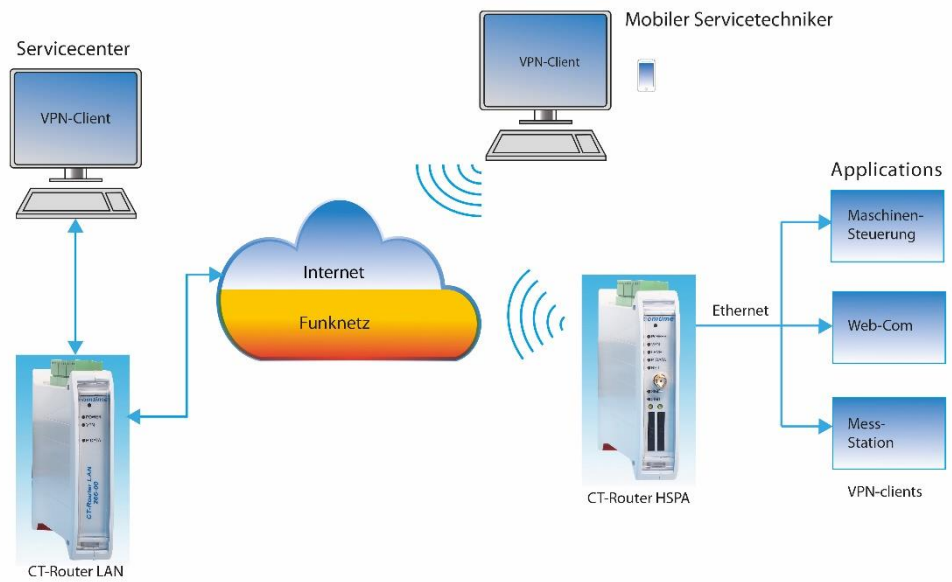


CT-VPN Server



Die in dieser Publikation veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzungen, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen bedürfen der ausdrücklichen Genehmigung der comtime GmbH.

© 2011 comtime GmbH

Alle Rechte vorbehalten.

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.

Alle Warenzeichen und Produktbezeichnungen sind Warenzeichen, eingetragene Warenzeichen oder Produktbezeichnungen der jeweiligen Inhaber.

Alle Lieferungen und Leistungen erbringt die comtime GmbH auf der Grundlage der Allgemeinen Geschäftsbedingungen der comtime GmbH in der jeweils aktuellen Fassung. Alle Angaben basieren auf Herstellerangaben. Keine Gewähr oder Haftung bei fehlerhaften und unterbliebenen Eintragungen. Die Beschreibungen der Spezifikationen in diesem Handbuch stellen keinen Vertrag da.

Artikel-Nr.:

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

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.

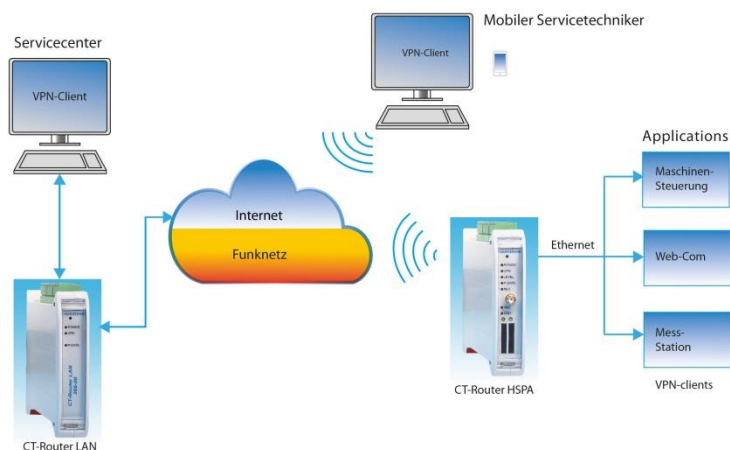
Zertifikate für die zu verbindenden Geräte und für PC's werden automatisch erstellt. Für die CT-Router Serie (LAN, ADSL, GPRS, UMTS, LTS) wird auch die VPN-Konfiguration Datei automatisch erstellt und kann inkl. Zertifikat in den Router eingespielt werden.

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:

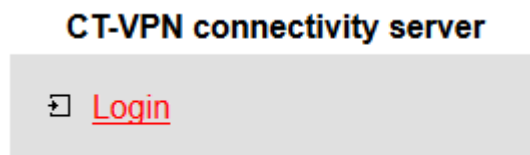
- Linux Debian 8.x
- 1 GB RAM
- 100 MB Programm Speicher

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

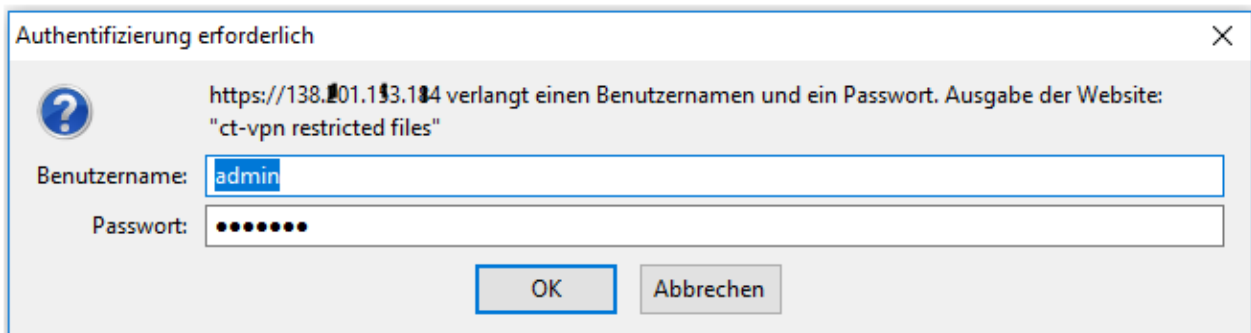
- Der Computer, der zur Konfiguration verwendet wird, verfügt über einen Zugang zum Internet.
- Auf dem Computer ist ein Webbrowser installiert (z.B. Google Chrome, Mozilla Firefox, Microsoft Internet Explorer).

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.

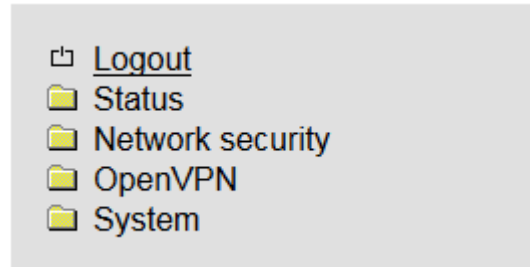


Im Auslieferungszustand lautet der Benutzername „admin“ und das Passwort „admin“ (das Ändern des Passwortes wird unter dem Punkt „System“ >> „User“ beschrieben).
Es gibt zwei User-Level:

- 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.

Hauptmenü



VPN Server Konfigurieren

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

- Logout
- Status
- Network security
- OpenVPN
 - Server connections
 - Certificates
 - Static keys
- System

CT-VPN connectivity server

OpenVPN server connections

Enabled	Name	CA	Server	Groups	Clients
Yes ▾	Demo Server Vertrieb	Edit	Edit	Edit	Edit
No ▾	server2	Edit	Edit	Edit	Edit

Apply

Tragen Sie den gewünschten Namen in das Feld von „Server1“ ein und bestätigen dies mit „Apply“. Nun können Sie die weitere 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 den 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

- Logout
- Status
 - OpenVPN server
 - Routing table
 - System info
- Network security
- OpenVPN
 - Server connections
 - Certificates
 - Static keys
- System

CT-VPN connectivity server

OpenVPN certificate authority

Name	Demo Server Vertrieb
CA usage	Enabled ▾
CA name	CA-Demo-Vertrieb
Country	DE
Province	Schleswig-Holstein
City	Norderstedt
Organisation	comtime GmbH
Unit	Vertrieb
E-mail	sales@comtime-com.de
RSA keysize	2048 Bit ▾

Data base

Next serial number	0F
CA certificate	<input checked="" type="checkbox"/>
Server certificate	<input checked="" type="checkbox"/>
Diffie-Hellman parameter	<input checked="" type="checkbox"/>
TLS authentication key	<input checked="" type="checkbox"/> <input type="button" value="Save"/>
Data base operation	Rebuild all ▾

Server connections	
OpenVPN certificate authority	
CA usage	Enable -> Zertifikat und VPN-Konfiguration kann erstellt werden Disable -> keine Zertifikat 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)

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 „Virtual network base“ Adressen müssen zwischen den einzelnen Server Instanzen unterschiedlich sein.

- Logout
- Status
 - OpenVPN server
 - Routing table
 - System info
- Network security
- OpenVPN
 - Server connections
 - Certificates
 - Static keys
- System

CT-VPN connectivity server

OpenVPN server	
Name	Demo Server Vertrieb
VPN	Enabled ▾
Server URL	78.46.136.139
Local port	1194
Protocol	UDP ▾
LZO compression	Adaptive ▾
TLS authentication key	Enabled ▾
Encryption	AES 128 Bit ▾
Collapse pushed routes	<input type="checkbox"/>
Client subnet base	10.1.0.0/24
Virtual network base	172.16.0.0/24
<input checked="" type="checkbox"/> Keep alive	30 sec.
Restart	120 sec.

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
Encryption	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.

Groups setup		
Name	Demo Server Vertrieb	
Group name	Comment	
Demo Comtime		New Delete
Test Comtime		Delete
Kunden Projekt Nü	Test HSPA Router	Delete

Apply

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 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

- Logout
- Status
 - OpenVPN server
 - Routing table
 - System info
- Network security
- OpenVPN
 - Server connections
 - Certificates
 - Static keys
- System

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 <input checked="" type="checkbox"/> LAN Router - Kamera Comtime	172.16.0.5	<input checked="" type="checkbox"/> 10.1.1.0/24	Entry	Edit	Delete
#2 <input checked="" type="checkbox"/> PC Josef	172.16.0.9	<input type="checkbox"/> 10.1.2.0/24	Entry	Edit	Delete
#3 <input checked="" type="checkbox"/> HSPA Router Josef	172.16.0.13	<input checked="" type="checkbox"/> 10.1.3.0/24	Entry	Edit	Delete
#4 <input checked="" type="checkbox"/> iPhone Josef	172.16.0.17	<input type="checkbox"/> 10.1.4.0/24	Entry	Edit	Delete
#5 <input checked="" type="checkbox"/> Laptop AE_Yello	172.16.0.21	<input type="checkbox"/> 10.1.5.0/24	Entry	Edit	Delete
#6 <input checked="" type="checkbox"/> Homeoffice PC Josef	172.16.0.25	<input type="checkbox"/> 10.1.6.0/24	Entry	Edit	Delete
#7 <input checked="" type="checkbox"/> Testplatz PC Josef	172.16.0.29	<input type="checkbox"/> 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



- Logout
- Status
 - OpenVPN server
 - Routing table
 - System info
- Network security
- OpenVPN
- System

CT-VPN connectivity server

OpenVPN server status						
Name	Local port	Protocol		Status	Action	Log file
Demo Server Vertrieb	1194	UDP		✓	Restart	View
Active OpenVPN clients						
Client name	Remote host	Client address	Client subnet	Status	Action	Log file
LAN Router - Kamera Comtime	46.59.132.85:57653	-	10.1.1.0/24	✓	Disconnect	View
HSPA Router Josef Homeoffice	188.65.190.6:50140	-	10.1.10.0/24	✓	Disconnect	View
HSPA Fremdgerät	2.204.211.10:3072	-	10.1.11.0/24	✓	Disconnect	View
PC Josef	46.59.132.85:62750	172.16.0.9	-	✓	Disconnect	View
HSPA Router Josef	NONE	-	10.1.3.0/24	✗	Disconnect	View
iPhone Josef	82.113.121.46:43346	172.16.0.17	-	✓	Disconnect	View
Laptop AE_Yello	NONE	172.16.0.21	-	✗	Disconnect	View

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.