

VPN Router



Dokument Historie

Version	Bearbeitung	Veröffentlichung	Bemerkungen
DE01	10.07.2013	11.07.2013	
DE02	30.09.2013	15.10.2013	Neu getesteter Router: → Net Module NB 1600 → Der Vigor 2920 ist in seiner Konfiguration identisch jedoch ohne ADSL/VDSL Modem
DE03	2014-02-20	2014-02-120	Neues Firmenlogo



Inhalt

1	Tec	hnis	che Daten: Vigor 2xx0Vn, EuroGard Service Router V2 und Net Module NB	
160	00			4
2	Nut	zen	eines bestehenden Internet Zugangspunktes	5
2	2.1	Vor		5
	2.1	.1	Explizite Port-Weiterleitung (Forwarding)	6
	2.1	.2	Konfiguration einer DMZ	7
3	Vig	or 2× 	x0Vn DrayTek	. 10
3	3.1	Off	nen des Setup Menüs	. 10
3	3.2	Kor	nfigurieren des WAN-Ports	. 11
3	3.3	WA	N-Betrieb hinter einem Router/Firewall	. 11
3	3.4	Kor	nfiguration des VPN-Servers	. 12
3	8.5	Clie	ent Android System 4.1.2	. 16
3	8.6	Clie	ent IPhone / IPad	. 18
3	3.7	Clie	ent Microsoft Windows XP	. 20
3	8.8	Clie	ent Microsoft Windows 7	. 27
Э	3.9	Feł	lerbehandlung Windows:	. 34
4	Eur	oGa	rd Service Router 2	. 38
4	l.1	Öffı	nen des Setup Menüs	. 39
4	1.2	Kor	nfigurieren des LAN-Ports (Local Area Network)	. 40
4	1.3	Kor	nfigurieren des WAN Ports (Wide Area Network)	. 41
	4.3	.1	WAN over Ethernet	. 41
	4.3	.2	WAN over UMTS	. 42
4	1.4	Zei	konfiguration	. 43
4	1.5	Ser	ver-Zertifikat erstellen	. 43
4	1.6	Akt	ivieren des openVPN-Servers	. 44
	4.6	.1	VPN-Modus Server	. 44
	4.6	2	Zugänge erstellen	. 45
5	Eur	oGa	rd Service Router 2 VPN-Client	. 46
5	5.1	Clie	ent Software EurogardSRConnect	. 48
5	5.2	105	Sund Android Systeme	. 51
6	Net	Mod	ule VPN Router NB 1600 und 1600-U	. 52
6	6.1	Тес	hnische Daten	. 53
6	6.2	Öffı	nen des Setup Menü	. 54
VPN	I Route	r Dok	ument 30-004 ; Ausgabe DE03 2014-02-20 2	2/68

Saia-Burgess Controls AG



Bahnhofstrasse 18 I CH-3280 Murten I Switzerland
T +41 (0)26 672 72 72 I F +41 (0)26 672 74 99 I www.saia-pcd.com

	· · ·		
	6.3	Konfigurieren der WAN und LAN Ports (Wide Area Network)	55
	6.4	Zeitkonfiguration	56
	6.5	Erstellen der Server Zertifikate	57
	6.6	Aktivieren des openVPN Servers	58
	6.7	Anlegen eines Client Zuganges	59
7	Win	dows openVPN Client für Net Module Router	61
	7.1	Installation	61
	7.2	Entpacken des Konfigurationpakets	61
	7.3	Herstellen einer Verbindung	62
8	And	roid openVPN Client für Net Module Router	63
	8.1	Herstellen einer Verbindung	64
9	1-08	S openVPN Client für Net Module Router	66
	9.1	Herstellen einer Verbindung	67

Infos über dieses Dokument:

Ein sicherer Betrieb der PCD-Steuerungen am Internet ist nur mit zusätzlichen externen IT-Komponenten mit integrierten Schutzfunktionen wie VPN, Firewall, Proxy-Server, etc. gewährleistet.

Zu diesem Zweck haben wir mehrere VPN-Router evaluiert und mit unseren PCD-Steuerungen getestet. In diesem Dokument ist die detaillierte Beschreibung für die Konfiguration und Inbetriebnahme zu finden.

Getestete Geräte:

- DreyTek Vigor 2850Vn
- DreyTek Vigor 2920Vn
- EuroGard Service Router V2 (WLan)
- EuroGard Service Router V2 (UMTS)
- Net Module NB 1600
- Net Module NB 1600-U



1 Technische Daten: Vigor 2xx0Vn, EuroGard Service Router V2 und Net Module NB 1600

Der Vigor 2xx0 der Firma DreyTec ist ein Business Router zum Erstellen von VPN-Verbindungen und dem Managen von kleineren bis mittleren Business / Home- Netzwerken. Seine Funktionalität und Benutzeroberfläche sind leicht zu bedienen.

Der EuroGard Sevice Router V2 ist ein industrieller Router zum Erstellen von sicheren Verbindungen auf industriellen Anlagen. Das Konfigurationsmenü ist in mehreren Sprachen verfügbar. Die Benutzerführung ist einfach verständlich und das Erstellen einer VPN-Verbindung leicht realisierbar.

	DreyTek Vigor 2850Vn	DreyTek Vigor 2920Vn	EuroGard Service Router V2	EuroGard Service Router V2 (UMTS)	Net Module NB 1600-U
Bestelldaten	2850Vn	2920VN	ER 1201- WLAN	ER 1201-UMTS	NB 1600-U
Weitere Informationen	http://www.drayte k.de/produkte/mo dem- router/vigor2850- serie.html	http://www.dray tek.de/produkte /dual- wan/vigor2920- serie.html	http://www.euro gard.de	<u>http://www.euro</u> gard.de	http://www.netmo dule.de/products/i ndustrial- routers/mobile- router.html
Einsatz/Baufo rm	Business / Home	Business / Home	Industriell	Industriell	Industriell
Hutschienen- montage	Nein	Nein	Ja	Ja	Ja
Spannungs- versorgung	230 VAC	230 VAC	24 VDC	24 VDC	24 V DC (-15% +20%)
VPN Eigensch	aften				
Anzahl WAN Interfaces	3: LAN/Modem/USB	3: LAN/LAN/USB	1: LAN	2: LAN/UMTS	2; LAN, UMTS
Integriertes ADSL/VDSL Modem	Ja	Nein	Nein	Nein	Nein
VPN PPTP	Ja	Ja	Nein	Nein	Ja
VPN L2TP/IPSec	Ja	Ja	Nein	Nein	Nein
openVPN	Nein	Nein	Ja	Ja	Ja
Anz. VPN Clients	32 Verbindungen	32 Verbindungen	30 Verbindungen	30 Verbindungen	10
Windows Client	Ja (in Windows integriert)	Ja (in Windows integriert)	Ja (EurogardSRC onnect)	Ja (EurogardSRCo nnect)	Ja openVPN
IOS Client	Ja (IPSec/L2TP, integriert in IOS)	Ja (IPSec/L2TP, integriert in IOS)	Nein *	Nein *	Ja openVPN
Android Client	Ja (IPSec/L2TP, integriert in Android)	Ja (IPSec/L2TP, integriert in Android)	Nein *	Nein *	Ja openVPN
Erweiterunger	1				
3G / 4G Modem	Ja, mit USB-Stick	Ja, mit USB- Stick	Nein	Ja,mit integriertem UMTS Modem	3G (UMTS 7.2 Mbps)



* IOS oder Android Systeme können heute via WLAN an den Router angebunden werden. Dafür werden jeweils 2 Router benötigt. Ein VPN-Server sowie ein VPN-Client. Unterstützung von VPN auf mobilen Geräten ist in Vorbereitung.

2 Nutzen eines bestehenden Internet Zugangspunktes

2.1 Vorbereitung

Einrichten einer Verbindung in eine bestehende Ethernet-Infrastruktur: Die Internetverbindung zum InternetServiceProvider (ISP) wird dabei von einem bestehenden Gerät (in der unteren Grafik von Router 1) zur Verfügung gestellt.



Router 2 (VPN-Server) Router 1 (ISP)

Im oben gezeigten Fall wird die Internetverbindung zum ISP über den Router 1 hergestellt. Die bestehende Ethernet-Infrastruktur, soll oder kann nicht verändert werden. Der Router 2, welcher den VPN-Server beinhaltet, wird hinter dem Router 1 im bestehenden LAN installiert. Der Router 1 muss in diesem Fall so konfiguriert werden, dass alle relevanten VPN-Ports an die IP-Adresse des Router 2 übermittelt werden, oder die DMZ wird auf die IP-Adresse des Router 2 konfiguriert.

Je nach Konfiguration der VPN-Verbindung [Die Konfiguration der VPN-Verbindung kann z.B. das Point-to-Point Tunneling Protocol (PPTP) oder das Layer 2 Tunneling Protocol (L2TP) sein, welches meist in Kombination mit dem Internet Protocol Security (IPSec) angewendet wird] werden unterschiedliche Ports vom öffentlichen Netzwerk an der WAN-Schnittstelle des VPN-Servers benötigt. Ein Port stellt ein Tor zur Kommunikation mit einer Applikation, in diesem Fall der VPN-Server, über TPC/IP dar.

	Protokoll	Port
PPTP Standard	ТСР	1723
L2TP Standard	UDP	1701
IPSec Standard	UDP	500, 4500

In einer normalen Konfiguration werden die meisten Ports am Router, der die ISP-Verbindung verwaltet, von der internen Firewall geblockt. Daher ist es **nicht** möglich, ohne



kleine Änderungen an der bestehenden Ethernet-Infrastruktur, einen VPN-Server zu betreiben.

Firewall bedeutet grundsätzlich, dass alle Datenpakete die über nicht definierte Ports auf das LAN zugreifen wollen, vom ISP verwaltenden Router 1 verworfen werden. Somit kann der undefinierte Port keine Kommunikation mit den Geräten hinter der Firewall herstellen.

Damit eine Verbindung zum VPN-Server (Gerät hinter der Firewall) des ISP verwaltenden Routers 1 hergestellt werden kann, müssen die VPN-Verbindungsrelevanten Ports im ISP verwaltenden Router 1 in einer Firewall-Regel definiert werden

Die Konfiguration des 1 Routers zum Weiterleiten der Ports ist abhängig vom Fabrikat und Softwarestand des eingesetzten Gerätes. Grundsätzlich gibt es 2 Wege diese Ports an den VPN-Server weiterzuleiten.

2.1.1 Explizite Port-Weiterleitung (Forwarding)

Die Ports für das Herstellen einer VPN-Verbindung vom Client zum Server müssen vom ersten Router durch eine Firewall-Regel an den VPN-Server weitergereicht werden.

Ports:

PPTP Standard	=	TCP/UDP	→ 1723
L2TP Standard	=	UDP	→ 1701
IPSec Standard	=	UDP	→ 500, 4500
SSL	=	TCP/UDP	→ 443





Vorteil dieser Konfiguration:

Sehr sicher, da lediglich die oben genannten Ports am VPN-Server zur Verfügung stehen.

Nachteil dieser Konfiguration:

Die VPN-Ports sind standardmässig mit den oben beschriebenen Ports definiert. Diese sind jedoch nicht fest definiert, sondern können im Setup des VPN-Servers verändert werden. Ist die Portweiterleitung nicht vollständig identisch mit der Konfiguration des VPN-Servers, so kann keine Verbindung hergestellt werden.

Weitere Möglichkeiten bietet der Einsatz einer DMZ.

2.1.2 Konfiguration einer DMZ

Eine DMZ erlaubt es, alle Ports die auf der WAN-Schnittstelle angefragt werden und der erste Router keine Regel kennt, an eine bestimmte IP-Adresse weiter zu leiten.





Vorbereitung des bestehenden Routers DMZ/NAT:

Damit der bestehende Router, der mit dem ISP verbunden ist, Anfragen auf nicht bekannten Port`s verteilt, muss eine DMZ eingerichtet werden. Diese Konfiguration kann von Router zu Router unterschiedlich sein, sie wird jedoch meistens in der Hilfe des Setups oder im Handbuch des Routers gut beschrieben.

DMZ stellt eine "Demilitarized Zone" dar. Sie ist für Geräte die selbst keine Sicherheitseinrichtungen besitzen, ein ungeschützter und nicht sicherer Bereich. In der DMZ besitzt jedes Gerät vergleichbare Eigenschaften, als ob es tatsächlich am Internet



angeschlossen ist. Grund ist, dass der mit dem Internet physikalisch verbundene Router, alle ihm nicht bekannten Datenpakete an oder in die DMZ weiterleitet. In den meisten Fällen wird die DMZ durch das Angeben einer bestimmten IP-Adresse konfiguriert. **Achtung:**

Ports für die der erste Router eine Regel kennt, werden meist nicht in die DMZ weitergeleitet.



Nachteil:

Der VPN-Server benötigt eine eigene Schutzeinrichtung (Firewall usw...)

Vorteil:

Sehr leicht zu konfigurieren und zu administrieren.



3 Vigor 2xx0Vn DrayTek

Im Dokument werden die Konfiguration des DreyTec Routers Vigor 2850 und 2920 beschreiben. Beide besitzen dieselbe Konfigurationsoberfläche zur Konfiguration der Grundeinstellungen und VPN. Im Gegensatz zum Vigor 2850 besitzt der Vigor 2920 kein integriertes ADLS/VDSL Modem.

3.1 Öffnen des Setup Menüs

Zum Einrichten des Vigor 2xx0 muss der PC mit einer LAN-Schnittstelle verbunden werden. Der Router wird mit einem aktivierten DHCP-Server ausgeliefert. Es sollte deshalb vermieden werden, den Vigor 2xx0 mit Werkskonfiguration in eine Ethernet-Infrastruktur mit bereits vorhandenem DHCP-Server zu konfigurieren.

Empfohlen:

Trennen Sie ihren PC von allen bestehenden Netzwerkverbindungen. Verbinden Sie ihren PC direkt mit dem Router.

Die IP-Adresse des Routers ist standartmässig auf "192.168.1.1" konfiguriert. Der DHCP-Server des Routers wird dem angeschlossenen PC eine Adresse im Adressraum des DHCP-Servers zur Verfügung stellen (erstes Gerät normalerweise "192.168.1.10").

Der Router wird in einem Browser konfiguriert.

Damit die Konfigurationsoberfläche im Browser geladen wird, muss die IP-Adresse des Routers im Browser aufgerufen werden.

Standartmässig wird der Vigor 2xx0 mit dem Benutzer "admin" und dem dazugehörigem Password "admin" ausgeliefert. Sie finden die Benutzer und Passwörter auch im Handbuch des Routers.

🕒 Vigor Login Page 🛛 🗙		
← → C 🗋 178.83.186.183/web	ogin.htm	☆ =
Username Password	admin	
		Login
Copyright@, DrayTek Corp. All	Rights Reserved.	Dray Tek



3.2 Konfigurieren des WAN-Ports

WAN steht für "Wide Area Network". Dies ist bei einem Router immer die öffentliche Schnittstelle in einen öffentlichen, ungeschützten Bereich.





3.3 WAN-Betrieb hinter einem Router/Firewall

Der Vigor 2xx0 ermöglicht das Konfigurieren von 3 unterschiedlichen WAN Ports.

Achtung: Der Vigor 2920 besitzt kein integriertes ADSL/VDSL Modem

Übersicht der möglichen Verbindungsarten:

1) ADSL/VDSL Modem \rightarrow (Nur Vigor 2850)

diese Konfiguration erlaubt es, den Router direkt an einen ADSL/VDSL-Anschluss eines ISP (Internet Service Provider) mit dem integrierten Modem zu verbinden. Für diese Anschlussart werden die Konfigurationsparameter des ISP benötigt.

2) Ethernet \rightarrow

diese Konfiguration erlaubt es, den Router hinter einem bestehenden Router oder ADSL/VDSL Modem zu betreiben. Dabei stellt der bestehende Router die Verbindung zum ISP zur Verfügung.

3) USB \rightarrow

diese Konfiguration erlaubt es, ein angeschlossenes Modem (3G/4G) für den Verbindungsaufbau zu einem ISP zu verwenden. Für diese Anschlussart werden die Konfigurationsparameter des ISP benötigt.

In diesem Dokument wird die Verbindungsart 2 beschrieben. Bei dieser Verbindungsart wird der Router mit VPN-Server hinter einem bestehenden Router positioniert. Der bestehende Router verwaltet in diesem Fall die Internetverbindung zum Internet Service Provider (ISP) und besitzt die öffentliche IP-Adresse des Systems.



3.4 Konfiguration des VPN-Servers

Der Vigor 2xx0 unterstützt die folgenden Remote Access Möglichkeiten:

1) Tunneling Protokolle:

a. PPTP VPN-Service (Point-to-Point Tunneling Protocol)
 Mittels PPTP wird ein VPN geschaffen, indem ein Tunnel für das Point-to-Point
 Protocol gebildet wird. Es lässt Raum für jede denkbare Form der
 Authentifizierung und Verschlüsselung. Meist wird der TCP-Port 1723 verwendet.

b. IPSec VPN-Service (Internet Protocol Security)

IPsec ist eine Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze ermöglicht, wie beispielsweise dem Internet.

c. L2TP VPN-Service (Layer 2 Tunneling Protocol)

Tunneling auf der Layer 2 Ebene des OSI Schichtenmodells (Sicherungsschicht). Eine Verschlüsselung ist in L2TP nicht direkt enthalten und wird daher meist in Kombination mit IPSec betrieben.

Vigor2850 VDSL2 Security Fit	Series	Dray 1
Auto Logout 💌 🛛 🛛 🕞	VPN and Remote Access >> Remote Access Control Setup	
Quick Start Wizard Service Activation Wizard	Remote Access Control Setup	
Online Status	Enable PPTP VPN Service	
	Enable IPSec VPN Service	
WAN LAN	Enable L2TP VPN Service	
NAT Firewall User Management Objects Setting CSM Bandwidth Management Applications VPN and Remote Access	Note: If you intend running a VPN server inside your LAN, you should un above to allow pass-through, as well as the appropriate NAT settings. OK Clear Cancel	check the appropriate protocol

Remote Access Control Setup

Für den Aufbau der VPN-Verbindung wird in diesem Dokument L2TP beschrieben: Aktivieren Sie den Service für IPSec und L2TP.

L2TP erlaubt das Routen von Netzwerken NAT (Netwok Address Translation). Der VPN-Tunnel wird dabei über IPSec hergestellt.



2) IPSec Einstellungen Pre-Shared Key (PSK)

Der PSK wird beim Einstellen der Verbindungsoptionen des Clients benötigt, falls eine Verbindungsart mit IPSec gewählt wurde.

VDSL2 Security Fire	ewall	
Auto Logout 💌 📭	VPN and Remote Access >> IPsec General Setup	
Quick Start Wizard Service Activation Wizard Online Status VDSL	VPN IKE/IPsec General Setup Dial-in Set un for Remote Dial-in users and Dynamic II IKE Authentication Method	P Client (LAN to LAN)
WAN LAN NAT Firewall User Management Objects Setting CSM Bandwidth Management Applications VPN Client Wizard VPN Client Wizard VPN Client Wizard VPN Client Wizard VPN Genere Wizard News Concernal Setup IPsec General Setup IPsec Peer Identity Remote DiaLin User LAN to LAN VPN TRUNK Management Connection Management Connection Management Connection Management Connection Management Connection Management Connection Management Connection Management Connection Management Connection Management Diagnostics	Pre-Shared Key Confirm Pre-Shared Key IPsec Security Method Medium (AH) Data will be authentic, but will not be enc High (ESP) ØDES Ø3DES ØAES Data will be encrypted and authentic. OK	rypted. Cancel

IPSec General Setup

Der PSK sollte auf keinen Fall ein Wort aus einem Wörterbuch sein. Es wird empfohlen das Passwort mit Sonderzeichen, Zahlenkombinationen sowie eine Mindestlänge von 12 Zeichen zu definieren.



3) Remote Dial-in User

Hier können bis zu 32 Benutzer konfiguriert werden. Jeder dieser Benutzer kann sich am VPN-Server anmelden. Zum Anlegen eines neuen Benutzers muss der Index der entsprechenden Zeile angeklickt werden.

Möchten Sie, dass Ihr Passw	ort von Google	Chrome gesp	eichert wird?	Passwort sp	peichern	Für diese Wel	bsite niem als	•
Vigor2850 s VDSL2 Security Fire	Series wall	<						Dray
Auto Logout 🔹 IR6	VPN and I	Remote Access	>> Remote [)ial-in User				
ervice Activation Wizard	Remote A	ccess User Acc	ounts:				Set t	o Factory Default
Inline Status /DSL	Index	User	Active	Status	Index	User	Active	Status
	7	Daniel		LAN1-DHCP	<u>1/.</u>	777		
AN	<u>Z.</u>	Daniel 2		LAN1-DHCP	<u>18.</u>	111		
IAT Firewall	<u>3.</u>				<u>19.</u> 20			
lser Management	4.	222			20.	222		
bjects Setting	<u>.</u>	222			21.	222		
Bandwidth Management	<u>0.</u> 7	222			22.	222		
/PN and Remote Access	<u>1.</u>	222			23.	111		
VPN Client Wizard	<u>o.</u>	222			25	222		
Remote Access Control	<u>5.</u> 10	222			25.	222		
PPP General Setup IPsec General Setup	10.	222			20.	222		
IPsec Peer Identity	12	222			28	222		
LAN to LAN	13	222			29	222		
VPN TRUNK Management	14	222			30.	222		
Certificate Management	15	222			31	222		
ISB Application	16	222			32	222		
liagnostics	10.							
xternal Devices				OK	Can	icel		

32 Remote Dial-in User



- 4) Remote Dial-in User Konfiguration
 - 1) Den aktuell selektierten Benutzer auf aktiven Benutzer setzen: Das Timeout auf den Wert "60" Sekunden setzen.
 - Dial-in Möglichkeiten des aktuell selektierten Benutzers: Bevorzugte Einstellung ist L2TP with IPSec Policy (Must). In diesem Fall wird ein geschützter IPSec Tunnel zum Server hergestellt. In diesem Tunnel wiederum wird ein weiterer L2TP Tunnel aufgebaut, der erlaubt das Netzwerk zwischen Server und Client zu routen.
 - 3) Specifiy Remote Node aktivieren.
 - 4) Definition eines Benutzernamens und Password für die Authentifizierung.

Möchten Sie, dass Ihr Passwor	t von Google Chrome gespeichert wird?	Passwort speichern	Für diese Website ni	emals
Vigor2850 Se VDSL2 Security Firew	all	ial in Hear		Dray T
uick Start Wizard ervice Activation Wizard nline Status	Upw and Remote Access >> Remote Dr	Jserr	name (4)	Daniel
AN AN AT Towall	Inable this account Idle Timeout	second(s)	word(Max 19 char) nable Mobile One-Time N Code	e Passwords(mOTP)
ser Management bjects Setting SM andwidth Management polications	PPTP IPsec Tunnel L2TP with IPsec Policy Must	Se IKE A	ecret uthentication Method	
PN and Remote Access VPN Client Wizard VPN Server Wizard Remote Access Control PPP General Setup	Specify Remote Node Remote Client IP	P IKE D None	re-Shared Key Pre-Shared Key igital Signature(X.509)
IPsec General Setup IPsec Peer Identity Remote Dial-in User LAN to LAN VPN TRUNK Management Connection Management	or Peer ID Netbios Naming Packet Pass Multicast via VPN Pass (for some IGMP,IP-Camera,DHCP R	○ Block IPsec	Security Method Iedium(AH) ESP) V DES V 3	DES 🖉 AES
ertificate Management SB Application /stem Maintenance agnostics cternal Devices	Subnet LAN 1 💌 Assign Static IP Address	Local	ID (optional)	
	0.0.0			

- 5) Der VPN-Server ist nun vollständig konfiguriert und wartet auf die Verbindungen von Clients.
- 6) Wenn der Client verbunden ist, kann einfach durch das Aufrufen der IP und .html Datei im Micro-Browser eine Verbindung zu Applikation hergestellt werden.



7)

3.5 Client Android System 4.1.2

Öffnen des Menüs \rightarrow Einstellungen \rightarrow Weiter Einstellungen:



Im Untermenü befindet sich der Eintrag VPN (Virtual Private Networks), welcher es ermöglicht den Client zu konfigurieren:





Hinzufügen einer VPN-Netzwerkverbindung:

- → Name = Frei definierbar
- → Server-Adresse = Öffentliche IP-Adresse oder DNS-Name des DSL-Routers
- → L2TP-Schlüssel = wird bei aktueller Router-Konfiguration nicht verwendet
- ➔ IPSec Pre-shared Key = Schlüssel, welcher im Router IPSec General Setup hinterlegt wurde
- ➔ Speichern

Öffnen der angelegten VPN-Netzwerkverbindung:

🌵 📟 🛋 62% 🛱 🛱 🛱 🖓 🔐 💈 17:10	🜵 🔤 🗛 💷 🛱 🛱 🛱 👘 🕌 📶 📴 17:10	🜵 🕶 🖬 🗛 💷 🛱 🛱 🛱 🛱 🕌 📶 💈 17:10
Mit L2TP verbinden	< 🔯 VPN	< 🗔 VPN
Benutzername	L2TP Verbinden	L2TP Verbunden
Passwort	VPN-Netzwerk hinzufügen	VPN-Netzwerk hinzufügen
Kontoinformationen		
Abbruch Verbinden		
Daniels Daniel DaniellpSec 🗸		
qwertzuiop		
asdfghjkl		
🕇 y x c v b n m 🛙		
123 Sym 🌣 🛄 . Weiter		

➔ Benuztername und Password, die in der Remote Dial-in User Konfiguration hinterlegt wurden:

Username	Daniel
Password(Max 19 char)	
🔲 Enable Mobile One-Ti	me Passwords(mOTP)
PIN Code	
Secret	



3.6 Client IPhone / IPad

Zum Erstellen einer L2TP/IPSec Verbindung, sind mit einem I-OS Gerät folgende Schritte notwendig:

1) Öffnen der "Einstellungen". Unter dem Menü Punkt "Allgemein" "VPN" wählen:

III. Swisscom 🔶 👘	10:07	Þ
Einstellungen Allg	jemein	
Info		>
Softwareaktual	isierung	>
Benutzung		>
Siri		>
Mobiles Netz	Ein	>
VPN	Nicht verbunden	>
iTunes-WLAN-S	Sync	>
Spotlight-Suche	9	>

2) Hinzufügen einer neuen VPN Verbindung:





- 3) Erstellen einer L2TP-IPSec Verbindung mit einem entfernten VPN-Server. Benötigte Einstellungen oder Angaben:
- → Beschreibung: Frei definierbar
- → Server: IP-Adresse oder DNS des VPN-Servers
- → Account: User Profil mit VPN-Zugriffsrechte auf den VPN-Server
- → Kennwort: Das für dieses User Profil hinterlegte Password
- → Shared Secret: Der für den VPN-Tunnel hinterlegte Pre-Shared Key (PSK)

📶 Swisscom 🗢	10:08	Ē
Abbrechen K	onfiguratio	Sichern
L2TP	РРТР	IPSec
Beschreibu	ng Vigor	
Server	178.83.186	.183
Account	Daniel	
RSA-Secur	ID	$\bigcirc \bigcirc$
Kennwort	•••••	••••
Shared Sec	ret •••••	•••••
Für alle Dat	ten	
Proxy		
Aus	Manuell	Autom.

 Selektieren des f
ür den VPN-Zugriff verwendeten Tunnels und aktiveren dieses Tunnels. Es ist im Statusfeld ersichtlich, dass der Tunnel erfolgreich aufgebaut wurde:





3.7 Client Microsoft Windows XP

1) Öffnen der Netzwerk-Konfiguration:



2) Neue Verbindung erstellen:

Setwork Connections	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> o	ools Adva <u>n</u> ced <u>H</u> elp
🕞 Back 👻 🕥 👻 🤌	Search 😥 Folders 📰 🕶
Address 🔕 Network Connections	
	▲ Name
Network Tasks 🛛 🗢	LAN or High-Speed Internet
Create a new connection	
Set up a home or small office network	
Change Windows Firewall settings	
	▼ [4]



3) Wizard zum Erstellen einer neuen Verbindung wird geladen:



4) Verbindung mit Arbeitsplatz herstellen (VPN):





5) Virtual Private Network Verbindung (VPN):

New Connection Wizard	
Network Connection How do you want to connect to the network at your workplace?	
Create the following connection:	
© Dial-up connection	
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.	
Virtual Private Network connection Connect to the network using a virtual private network (VPN) connection over the Internet.	
< <u>B</u> ack <u>N</u> ext > Cancel	

6) Name des VPN:

lew Connection Wizard			
Connection Name Specify a name for this connection to your w	orkplace.		Ì
Type a name for this connection in the followin Company N <u>a</u> me	ng box.		
Vigor 2850	workplace or the	a name of a serv	er vou
will connect to.	workplace of the	s name or a serv	ei you
	< <u>B</u> ack	<u>N</u> ext >	Cancel



7) VPN-Server Adresse:

New Connection Wizard
VPN Server Selection What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting. Host name or IP address (for example, microsoft.com or 157,54.0.1);
178.83.186.183
< <u>B</u> ack <u>N</u> ext > Cancel

8) Wizard beenden:

New Connection Wizard		
	Completing the New Connection Wizard You have successfully completed the steps needed to create the following connection:	
	Vigor 2850 • Share with all users of this computer	
	The connection will be saved in the Network Connections folder. Add a <u>s</u> hortcut to this connection to my desktop	
	To create the connection and close this wizard, click Finish.	
	< <u>B</u> ack Finish Cancel	



9) Im Verbindungsdialog Eigenschaften selektieren:

onnect Vigor 2	850	<u>? ×</u>
R		
User name:		
Password:		
Save this us	er name and password for th	e following users:
C Anyone	who uses this computer	
Connect	Cancel Properti	es <u>H</u> elp

10) Tab Sicherheit \rightarrow IPSec Einstellungen \rightarrow IPSec Schlüssel eingeben:

Vigor 2850 Properties	×
General Options Security Networking Advanced	1
Security options ✓ <u>Ivpical (recommended settings)</u> ✓alidate my identity as follows:	
Require secured password	
 Automatically use my Windows logon name and password (and domain if any) 	
Require data encryption (disconnect if none)	
C Advanced (custom settings)	
Using these settings requires a knowledge <u>Settings</u>	
Settings 21x	
✓ Use pre-shared key for authentication Key:	
OK Cancel OK Cancel	



11) Benutzername und Passwort des VPN-Benutzers eingeben:



12) Verbindung wurde Hergestellt:

Connecting Vigor 2850	
2	Connecting to 178.83.186.183
	Cancel
Connecti	ing Vigor
2	Verifying username and password
	Cancel
Connecti	ng Vigor
2	Registering your computer on the network
	[Cancel]



13) Der PC ist nun ein Teilnehmer des gegenüberliegenden Netzwerkes. Der Zugriff auf die Geräte ist mit allen Applikationen die Ethernet unterstützen möglich:





3.8 Client Microsoft Windows 7

Einrichten einer VPN-Verbindung in einem Windows 7 System. Für das Einrichten einer VPN-Verbindung werden Administrationsrechte benötigt.

1) Öffnen des Netzwerk und Freigabecenters:



2) Neue Verbindung zu einem Netzwerk einrichten:





3) Verbindung mit dem Arbeitsplatz herstellen:



4) Die Internetverbindung verwenden:





5) Internetadresse und Name der Verbindung definieren:

	Geben Sie die Internetadresse zum Herstellen einer Verbindung ein.					
	Diese Adresse können	Sie vom Netzwerkadministrator erhalten.				
	Internetadresse:	178.83.186.183				
	Zielname:	Vigor 2850				
	 Eine Smartcard verwenden Martcard verwenden, diese Verbindung zu verwenden Erlaubt jedem, der Zugang zu diesem Computer hat, diese Verbindung zu verwenden. Jetzt nicht verbinden, nur für spätere Verwendung einrichten 					
		Weiter				
G	Verbindung mit der	m Arbeitsplatz herstellen				
	Geben Sie den Be	nutzernamen und das Kennwort ein.				
	Benutzername:	Daniel				
	Kennwort:	********				
	Kennwort:	 ✓ Zeichen anzeigen ✓ Dieses Kennwort speichern 				
	Kennwort: Domäne (optional):	 Zeichen anzeigen Dieses Kennwort speichern 				
	Kennwort: Domäne (optional):	 Zeichen anzeigen Dieses Kennwort speichern 				
	Kennwort: Domäne (optional):	 Zeichen anzeigen Dieses Kennwort speichern 				



7) Den Wizard beenden:



8) Öffnen des Netzwerk und Freigabecenters \rightarrow Adaptereinstellungen ändern





9) Eigenschaften der VPN-Verbindung öffnen:

🗿 🗇 😨 🕨 Systemsteuerung 🕨 Netzwer	k und Internet 🔸 Netzwerkverbindungen 🕨	• [4 ₂] [1	Netzwerkverbindungen durchsuchen 👂
Organisieren 👻 Verbindung starten V	erbindung umbenennen Verbindung lösch	en Einstellungen dieser Verbindung ändern	
Bluetooth-Netzwerkverbindung Nicht verbunden Bluetooth-Gerät (PAN)	Drahtlosnetzwerkverbindung Nicht verbunden Intel(R) Centrino(R) Ultimate-N 6	Drahtlosnetzwerkverbindung 2 Nicht verbunden Microsoft Virtual WiFi Miniport A	
LAN-Verbindung Netzwerk: 4 Intel(R) 82579LM Gigabit Network	LAN-Verbindung 2 Netzwerkkabel wurde entfernt TAP-Win32 Adapter V9	Vigor 2850 Verbindung getrennt WAN Miniport (IKEv2)	The ball of the State
VMware Network Adapter VMnet1	VMware Network Adapter VMnet8		Status
Nicht identifiziertes Netzwerk VMware Virtual Ethernet Adapter	Nicht identifiziertes Netzwerk VMware Virtual Ethernet Adapter		Als Standardverbindung festlegen
			Kopie erstellen
			Verknüpfung erstellen
		•	Löschen
		8	Umbenennen
		*	Eigenschaften

10) Einstellen der L2TP/IPSec Verbindung und setzen des IPSec Pre-Shared Key (PSK):

Eigenschaften von Vigor 2850	Erweiterte Eigenschaften
Allgemein Optionen Sicherheit Netzwerk Freigabe	L2TP
VPN-Typ: Layer-2-Tunneling-Protokoll mit IPsec (L2TP/IPSec)	Vorinstallierten Schlüssel für Authentifizierung verwenden Schlüssel: ************************************
Datenverschlusserung. Erforderlich (Verbindung trennen, falls Server dies ablehnt)	 Zertifikat für die Authentifizierung verwenden Die Namen- und Verwendungsattribute des Serverzertifikats überprüfen
Extensible-Authentication-Protokoll (EAP) verwenden	
Eigenschaften Eigenschaften	OK Abbrechen
🕅 Unverschlüsseltes Kennwort (PAP)	
📝 Challenge Handshake Authentication-Protokoll (CHAP)	
Microsoft CHAP, Version 2 (MS-CHAP v2)	
Automatisch eigenen Windows-Anmeldenamen und Kennwort (und Domäne, falls vorhanden) verwenden	
OK Abbrechen	



11) Öffnen der VPN-Verbindung und Verbindung herstellen

🐓 Verbindung m	Verbindung mit "Vigor 2850" herstellen					
Benutzername:	Daniel					
Kennwort:	[Klicken Sie hier, um das Kennwort zu är	ndern]				
Domäne:						
 Ø Benutzernamen und Kennwort speichern für: Nur für eigene Verwendung Alle Benutzer dieses Computers Verbinden Abbrechen Eigenschaften Hilfe 						
Verbindung wird hergestellt mit Vigor 2850						
Benutzername und Kennwort werden überprüft						
Abbrechen						
Verbindung wird hergestellt mit Vigor 2850						
Der Co	Der Computer wird im Netzwerk registriert					
	Abbrechen					



12) Verbindung wurde aufgebaut, IP-Adressen vom DHCP-Servers des Routers wurden vergeben

Status von Vigor 2850	Status von Vigor 2850
Allgemein Details	Allgemein Details
Verbindung IPv4-Konnektivität: Internet IPv6-Konnektivität: Kein Netzwerkzugriff Medienstatus: Verbindung hergestellt Dauer: 00:00:57 Details Aktivität Gesendet Empfangen Bytes: 1.768 543 Komprimierung: 0 % 0 % Fehler: 0 0	EigenschaftWertGerätenameWAN Miniport (L2TP)GerätetypvpnAuthentifizierungM5 CHAP V2Komprimierung(keine)PPP-MultilinkframingInaktivClient-IPv4-Adresse192.168.1.11Server-IPv4-Adresse192.168.1.1NAP-StatusNicht NAP-fähigVerwendeter NetzwerLAN-VerbindungUrsprüngliche Adresse168.152.35.150Zieladresse178.83.186.183
Eigenschaften Trennen Diagnose	
Schließen	Schließen

- 13) Der PC ist nun ein Teilnehmer des gegenüberliegenden Netzwerkes. Der Zugriff auf die Geräte ist mit allen Applikationen die Ethernet unterstützen möglich.
- ➔ Browser
- → PG5





3.9 Fehlerbehandlung Windows:

Im Fall, dass die Verbindung nicht erfolgreich hergestellt wurde, überprüfen Sie bitte die folgenden Punkte und wiederholen Sie den Vorgang ab Punkt 15 erneut. Aktivieren des IPSec Policy Agent und des IKE and AuthIP IPSec Keying Modules.

1) Systemsteuerung öffnen:

		The set of		
0	0	Microsoft Visual Studio 2010	+	
	D	Git Bash		Schossmaier Daniel
٩	ł	VMware Player	۲	Dokumente
	V	Microsoft Office Word 2003	۲	Bilder
6	2	Snipping Tool		Musik
	D	Microsoft Office PowerPoint 2003	•	Computer
		Erste Schritte	•	Systemsteuerung
		Verbindung mit einem Projektor		Geräte und Drucker
	0	Rechner		Standardprogramme
	8	IrfanView - Thumbnails		
)		Alle Programme		
	Pro	ogramme/Dateien durchsuchen 🖇	>	Iterunterfahren ►
(9	6 👩 0		O 🏪 🚌



2) Verwaltung öffnen:



3) Fenster der Dienste öffnen:





- 4) Dienste starten
 - (IPsec-Richtlinien-Agent und IKE und AuthIP IPsec-Schlüsselerstellungsmodule) a. IPsec-Richtlinien-

rigent	
ovente Detei Alton Anscht ? ♦ ♦ 🐨 🗟 🔄 📔 🗊 🕨 🖩 II IÞ	
Denste (Lokal) Denste (Status Starttyp Anmelden als natrechnolosue, Gratettet Automatisch Leichaler Sostem wathentflörenz, Gratettet Automatisch Metzwirklænst mote Draktop Manuell Lokaler System
Eigenschaften von IPsec-Richtlinien-Agent (L	okaler Computer)
Allgemein Anmelden Wiederherstellung At	bhängigkeiten
Dienstname: PolicyAgent	
Anzeigename: IPsec-Richtlinien-Agent	
Beschreibung: IPsec (Internet Protocol Se Peerauthentifizierung auf N	ecurity) unterstützt die letzwerkebene,
Pfad zur EXE-Datei: C:\Windows\system32\svchost.exe -k Netwo	rkServiceNetworkRestricted
Starttyp: Automatisch	•
Unterstützung beim Konfigurieren der Startopti	onen für Dienste
Dienststatus: Gestartet	
Starten Reenden An	halten Fortsetzen
Sie können die Startparameter angeben, die ü wenn der Dienst von hier aus gestartet wird.	ibernommen werden sollen,
Sie können die Startparameter angeben, die ü wenn der Dienst von hier aus gestartet wird. Startparameter:	ibernommen werden sollen,
Sie können die Startparameter angeben, die ü wenn der Dienst von hier aus gestartet wird. Startparameter:	ibernommen werden sollen,



b. IKE- und AuthIP IPsec-Schlüsselerstellungsmodule:

Eigenschaften von IKE- und AuthIP IPsec-Schlüsselerstellungsmo 🛛 🖾							
Allgemein Anmel	den Wiederherstellung Abhängigkeiten						
Dienstname: IKEEXT							
Anzeigename:	Anzeigename: IKE- und AuthIP IPsec-Schlüsselerstellungsmodule						
Beschreibung:	Die IKEEXT-Diensthosts der Schlüsselerstellungsmodule für IKE (Internet Key						
Pfad zur EXE-Da C:\Windows\sys	itei: tem32\svchost.exe -k netsvcs						
Starttyp:	Starttyp: Automatisch 👻						
Unterstützung beim Konfigurieren der Startoptionen für Dienste							
Dienststatus:	Dienststatus: Gestartet						
Starten	Starten Beenden Anhalten Fortsetzen						
Sie können die Startparameter angeben, die übernommen werden sollen, wenn der Dienst von hier aus gestartet wird.							
Startparameter:							
OK Abbrechen Übernehmen							



4 EuroGard Service Router 2

Der Router sollte immer beginnend mit den Einstellungen für das lokalen Netzwerk (LAN) und anschließend für den VPN-Server konfiguriert werden. Grund hierfür ist, dass Parameter der lokalen Konfiguration und die Systemzeit beim Generieren des Server-Zertifikates im Router verwendet



Wide Area Network (WAN) \rightarrow Verbindung zum Router mit öffentlichen IP-Adresse Local Area Network (LAN) \rightarrow Verbindung zum lokalen Netzwerk



4.1 Öffnen des Setup Menüs

Zum Einrichten des Eurogard Service Router V2 muss der PC mit einer LAN-Schnittstelle des Routers verbunden werden. Der Router wird mit einem aktivierten DHCP-Server ausgeliefert. Es sollte deshalb vermieden werden, den Eurogard Service Router V2 zu mit Werkskonfiguration in eine Ethernet-Infrastruktur mit bereits vorhandenem DHCP-Server zu konfigurieren.

Empfohlen:

Trennen Sie ihren PC von allen bestehenden Netzwerkverbindungen. Verbinden Sie ihren PC direkt mit dem Router.

Die Standard IP-Adresse des Routers ist von Werk auf "192.168.155.1" eingestellt. Der DHCP-Server des Routers wird dem angeschlossenen PC eine Adresse im Adressraum des DHCP-Servers zur Verfügung stellen.

Die Konfiguration des Routers wird mit Hilfe eines Browsers erstellt. Damit die Konfigurationsoberfläche im Browser geladen wird, muss die IP-Adresse des Routers im Browser aufgerufen werden.

Ab Werk wird der Eurogard Service Router V2 mit dem Benutzer "eurogard" und dem dazugehörigem Password "eurogard" ausgeliefert. Sie finden die Benutzer und Passwörter auch im Handbuch des Routers.

ServiceRouter V2 ×		
← → C 🕼 bttps://wer	k2.pcd-demo.com	☆ =
euro gard Info SPS Benutzer	Authentifizierung erforderlich 23 Für den Server https://werk2.pcd-demo.com:443 ist ein Nutzername und ein Passwort erforderlich. Der Server meldet Folgendes: admin. Nutzername: eurogard Passwort: Manelden Abbrechen	Adminlogin Hostname: Werk2 Gerätezeit: 12.06.2013 08:11 Laufzeit: 1 day Last: 0.32, 0.55, 0.61 Softwareversion: 4.3.1 Sprache: deutsch •
<	Tel.: + 49 (0) 24 07- 95 16 - 0 Fax: + 49 (0) 24 07 - 95 16 - 23 E-Mail: info@eurogard.de Web: www.eurogard.de '''	



4.2 Konfigurieren des LAN-Ports (Local Area Network)

Öffnen der Router Konfiguration und setzen der Grundeinstellungen des lokalen Netzwerkes: Verwenden Sie die Adressen im Adressraum Ihrer bestehenden Applikation oder definieren Sie einen neuen Adressraum für eine neue Anlage. Es sollten mindestens der Hostname, Domänenname sowie der Standort geändert werden. Grund hierfür ist, dass diese für das später generierte Server-Zertifikat verwendet werden. Der Domänenname wird im später generierten Zertifikat als Verbindungsname zum VPN-Server eingetragen.

_	Info → System			
«Info»				
Routerkonfiguration	Grundeinstellungen/LAN			Logout:Admin
Geräte	Netzzugang/WAN	euro S	erviceRouter V2	Hostname: Werk2 Gerätezeit: 12.06.2013 08:16 Laufzeit: 1 day
Messaging	Zeit			Last: 0.43, 0.54, 0.59 Softwareversion: 4.3.1 Sprache: deutsch
Status-Logs	dDNS		Routerkonfiguration $ ightarrow$ Grundeinstellungen/LAN	
Backup-Wartung	Zertifikate	Info «Routerkonfiguration»	Grundeinstellungen/LAN	
	OpenVPN	Geräte	Systemeinstellungen	
	Zugänge	Messaging	Hostname	Werk2
	WLAN	Status-Logs	Domänenname	werk2.pcd-demo.com
	Logs	Backup-Wartung	IP-Adresse des Routers im SPS-Netz	192.168.155.1
	Firewall		Netzmaske	255.255.255.0
	Routing		Router ist DHCP-Server für SPS-Netz DHCP-Bereich Start	aktiviert 192.168.155. 100
			DHCP-Bereich Ende	192.168.155. 120
			OpenVPN Modus	off
			HTTPS-Port Weboberfläche (default:443)	443
			Standort	Murten
				Hilfe
			speichern	-



4.3 Konfigurieren des WAN Ports (Wide Area Network)

Der Eurogard Service Router V2 ermöglicht das Konfigurieren von 4 unterschiedlichen WAN Ports:

Ethernet	-
Ethernet	
DSL/PPPoE	
Wi-Fi	
UMTS	

1) Ethernet \rightarrow

diese Konfiguration erlaubt es, den Router hinter einem bestehenden Router zu betreiben. Dabei stellt der bestehende Router die Verbindung zum ISP zur Verfügung.

- DSL/PPPoE → (ein externes ADSL/VDSL Modem wird benötigt) diese Konfiguration erlaubt es, den Router direkt an ein ADSL/VDLS Modem zu verbinden. Für diese Anschlussart werden die Konfigurationsparameter des ISP benötigt.
- 3) UMTS \rightarrow

diese Konfiguration erlaubt es, das integrierte UMTS-Modem für den Verbindungsaufbau zu einem ISP zu verwenden. Für diese Anschlussart werden die Konfigurationsparameter des ISP benötigt.

ACHTUNG: In dieser Konfiguration (UMTS) kann der Router nur als VPN-Client betrieben werden.

4.3.1 WAN over Ethernet

Wenn Sie eine bereits bestehende Internetverbindung verwenden.

DHCP: Die IP-Adresse des Gerätes wird vom DHCP-Server der WAN-Schnittstelle bezogen. Statisch: Die IP-Adresse wird fest definiert.

«Info» Routerkonfiguration Geräte Messanion	Grundeinstellungen/LAN Netzzugang/WAN Zeit	evro S gard	erviceRouter V2		Logout:Admin Hostname: Werk2 Gerëtezeit: 12.06.2013 08:18 Laufzeit: 1 day Last: 0.53, 0.56, 0.59 Softwareversion: 4.3.1 Sprache: deutsch 💌
messaging Status-Logs Backup-Wartung	dDNS Zertifikate OpenVPN Zugänge WLAN Logs Firewall Routing	Info «Routerkonfiguration» Geräte Messaging Status-Logs Backup-Wartung	Routerkonfiguration → Netzzugang/WAV WAN-Konfiguration WAN-Konfiguration WAN-Medium Anschlusskonfiguration MTU (leer lassen für autom. Eintrag) speichern	Ethernet • DHCP/dynamisch •	
			Ethernet ■ SL/PPPoE Wi-Fi UMTS	DHCP/dynamis DHCP/dynamis statisch	ch 💌 Hilfo



4.3.2 WAN over UMTS

Wenn der Router mit einem integrierten UMTS Modem ausgestattet ist, kann das UMTS-Modem als WAN-Schnittstelle verwendet werden.

Achtung, eine Verbindung via UMTS unterstützt nur VPN-Client Funktionalitäten. Der Router kann dabei nicht als VPN-Server verwendet werden.

Die für die Einwahl erforderlichen Parameter werden von Ihrem ISP zur Verfügung gestellt.

e u r o S gard		V2
Info «Routerkonfiguration» Geräte	WAN-Konfiguration WAN-Konfiguration	
Messaging	WAN-Medium	UMTS
Status-Logs	APN	gprs.swisscom.ch
Backup-Wartung	PIN	
	Benutzername	any
	Passwort	
	Datenzähler	an 💌
	Monatliches Rücksetzen am:	1
	Logdatei führen	aktiviert
		speichern



4.4 Zeitkonfiguration

Bevor das Zertifikat generiert wird, ist es notwendig die Uhrzeit des Routers zu prüfen und gegebenenfalls den Zeitserver zu aktivieren oder die Zeit manuell zu setzen.

«Info» Routerkonfiguration Geräte Messaging	Grundeinstellungen/LAN Netzzugang/WAN Zeit	e v r o S gard	erviceRout	ter V2		Logout:Admin Hostname: Werk2 Gerätezeit: 12:06:2013 08:20 Laufzeit: 1 day Last: 0:68; 0:62; 0:60 Softwareversion: 4:3.1 Sprache: deutsch 💌
	dDNS		Routerkonfiguration $ ightarrow$ Zeit			
Status-Logs Backup-Wartung	Zertifikate	Info	Zait			
	OpenVPN	«Routerkonfiguration»	Len			
	Zugänge	Geräte	Aktuelle Zeit: 08:20:27 Wed	12 Jun 2013 CEST		
	WLAN	Messaging	Zeitkonfiguration			
	Logs	Status-Logs	Zeitquelle		NTP	
	Firewall	- Backup-Wartung	Zeitzone		Europe/Berlin	
	Routing					
			Server-Adresse	Aktion		
			0.pool.ntp.org	🗙 del		
			1.pool.ntp.org	🗶 del		
			2.pool.ntp.org	🗶 del		
			3.pool.ntp.org	🗙 del		
				💠 hinzufügen		
				speichern	I	Hile

4.5 Server-Zertifikat erstellen

Zum Erstellen des Server-Zertifikates werden die in den oberen Schritten hinterlegten Informationen als auch zusätzliche Parameter verwendet, welche Sie auf der Seite "Zertifikat" hinzufügen müssen. Daher ist es wichtig, dass vor der Erstellung des Zertifikates die oberen Schritte abgeschlossen sind.

«Info»	Into -> System	Info	Zertifikate	
Routerkonfiguration	Grundeinstellungen/LAN	«Routerkonfiguration»	Zertifikateinbalt	
Geräte	Netzzugang/WAN	Geräte		
Messaging	Zeit	Messaging	Länderkürzel	CH
Status-Logs	dDNS	Status-Logs	Bundestaat/Region	FR
Backup-Wartung	Zertifikate	Backup-Wartung	Ort	Murten
	OpenVPN Zugänge		Firma/Organisation	Saia Burgess Controls
	WLAN		Abteilung	ТРМ
	Logs Firewall		Info-E-Mail	daniel.schossmaier@saia
	Routing		Gültigkeitsdauer in Tagen	9125
			Zertifikate auch auf WAN-IP ausstellen	deaktiviert 💌
			Zertifikate auch auf LAN-IP ausstellen	aktiviert
			Neue Serverzertifikate	generieren
			Wurzelzertifikat in Browser importieren	importieren
			Serverzertifikat anzeigen	anzeigen
			speichern	Hilfe



4.6 Aktivieren des openVPN-Servers

4.6.1 VPN-Modus Server

Zum Aktivieren der VPN Funktionalität muss der Server aktiviert werden. Zusätzlich sollten der IP-Adressen-Bereich definiert werden, innerhalb welchem der VPN Client vom DHCP-Server eine IP-Adresse erhält.



Achtung:

Es sollte keine IP-Adresse statisch im Bereich der VPN-Client IP Adressen konfiguriert sein.

«Info» Routerkonfiguration Gerate	Grundeinstellungen/LAN Netzzugang/WAN	e u r o S gard	erviceRouter V2		Logout:Admin Hostname: Werk2 Gerätezeit: 12.06.0203 08:22 Laufzeit: 1 day Last: 0.40, 0.55, 0.58 Softwareversion: 4.3. Sprache: deutsch w
Messaging	Zeit		Routerkonfiguration> OpenVPN		
Status-Logs	dDNS	Info			
Backup-Wartung	Zertifikate	«Routerkonfiguration»	Орентири		
	OpenVPN	Geräte	Grundeinstellungen OpenVPN		
	Zugänge	Messaging	VPN-Modus	Server 💌	Server 🔹
	WLAN	Status-Logs	Erste IP des DHCP-Bereichs für VPN- Teilnehmer	192.168.155. 130	aus Server
	Logs	Backup-Wartung	Letzte IP des DHCP-Bereichs für VPN- Teilnehmer	192.168.155. 140	Client
	Firewall		VPN-Transportprotokoll	UDP	
	Routing		Port	1194	
			Client-zu-Clientverbindungen erlauben	ein 💌	
			VPN-Paketgrösse limitieren auf	1400 Byte 💌	
			Logdatei führen	aus	
			Intervall für Keepalive-Pakete in Sekunden	60	
			VPN-Neustart nach wieviel erfolglosen Pings (min. 2)	4	
			Kryptoalgorithmus	Kompatibilitätsmodus 💌	
			VPN-Netz übersetzen (wird üblicherweise nicht benötigt)		
			speict	hern	Hilfo

In den meisten Fällen müssen die Default Werte nicht verändert werden.



4.6.2 Zugänge erstellen

Erstellen eines neuen Zuganges. Jeder Client benötigt einen Zugang und das damit verbundene Zertifikat. Der "Bereich" (siehe Bild unten) stellt dabei die Berechtigung des Zuganges dar. Der Bereich "user" hat keine Rechte, die Router Konfiguration zu ändern. Er kann sich jedoch als VPN-Client oder über den SSL Proxy Server verbinden. "Admin" hingegen berechtigt den Zugang zum Bearbeiten der Router Konfiguration.

- → Neuer Zugang (Eingabe von Benutzername, Bereich und Passwort)
- → Neues Zertifikat → Client Zertifikat erstellen.
- → Download des für den Zugang benötigten Zertifikates.

	info -> Syster	" (g a r d								Laufzeit: 1 d Last: 0.66, 0.59, 0. Softwareversion: 4.3 Sonacher deutsch
«Into»			Routerkonfiguratio	n → Zugänge						sprucine, oronacia
Routerkonfiguratio	n Grundeinstellu	ingen/LAN Info								
Geräte	Netzzugang/V	VAN «Routerkonfiguration	Zugänge							
Messaging	Zeit	Geräte	10 💌 0	inträge anzeigen					Su	ichen
Charling Loope	dDNS	Messaging	Account- Name	Servicenetz *	Zertifikat	Online- Status			Aktion	
Status-Logs	Testificate	Status-Logs	Admin	admin	11:17:00 2038 GMT	offline	download	Passwort ändern	X Zugang löschen	e neues Nutzerzertifikat
Backup-Wartung	Zertinkate	Backup-Wartung	Daniel	admin	11:18:20 2038 GMT gültig bis Jun 4	offline	download	Passwort ändern	Zugang löschen	** neues Nutzerzert/fikat
	OpenVPN		1 bis 3 v	on 3 Einträgen	16:12:16 2038 GMT	omme	Ed commond	#" Passwort andem	A zugang ioschen	reurs reazerzeninkat
	Zugänge		Status aktual	isieren 🗼 neuen Zut	ang hinzufügen					
	WLAN									
	Logs		User	Zugangsname	user .		asswort		asswort wiederho	speichern
	Eirow all									
	Filewaii									
	Routing									
10 💌 Ein	träge anzeigen							S	uchen	
Account- Name	Servicenetz 🔺	Zertifikat	Online- Status				Akti	on		
Admin	admin	gültig bis Jun 4 11:17:00 2038 GMT	offline	do 🖬	wnload 🔎 Pa	sswort änderr	n 🗶 Zu	gang löschen	e neues	Nutzerzertifikat
Daniel	admin	gültig bis Jun 4 11:18:20 2038 GMT	offline	🖬 do	wnload 🔎 Pa	sswort änderr	n 🔀 Zu	gang löschen	e neues	Nutzerzertifikat
Android	user	gültig bis Jun 4 16:12:16 2038 GMT	offline	do 🖬	wnload 🔎 Pa	sswort änderr	n 🗶 Zu	gang löschen	e neues	Nutzerzertifikat
User	user	nicht vorhanden	offline	🖬 do	wnload 🖋 Pa	sswort änderr	n) 🔀 Zu	gang löschen	e neues	Nutzerzertifikat
1 DIS 4 VOR	i 4 Eintragen									• •
User	user	gültig bis Jun 6	offline	H do	wnload	asswort ände	m 🔀 Z	ugang lösche	n eue	s Nutzerzertifikat
		06:28:09 2038 GMT								
User	user	gültig bis Jun 6 06:28:09 2038 CMT	offline	🖬 dov	vnload 🔎 Pa	sswort änderr	n 🔀 Zu	igang löschen	e neues	Nutzerzertifikat
		50120107 2000 dill1								
					♥					
			F	User@Werk2s	werk2.p_tar *	1				
				-						

Achtung:

Beim erstellen eines neuen Server Zertifikates müssen alle Client Zertifikate neu erstellt werden.



5 EuroGard Service Router 2 VPN-Client

Der EuroGard Service Router kann auch als VPN-Client Verwendet werden:



 Als VPN-Server kommt ebenfalls ein EuroGard Router zum Einsatz. Konfigurieren des OpenVPN-Zugangs als

Client:			
-	Info -> System		
«Info»			
Routerkonfiguration	Grundeinstellungen/LAN		
Geräte	Netzzugang/WAN		
Messaging	Zeit		
Status-Logs	dDNS	OpenVPN	
Backup-Wartung	Zertifikate	Coundeinstellungen OnenVDN	
	OpenVPN	Grundeinstellungen OpenvPN	
	Zugänge	VPN-Modus	
	WLAN		aus
	Logs		Server
	Firewall		
	Routing		speichern

 Laden des vom Server erstellen Zertifikates beim Erstellen der Zugänge. Dieses Zertifikat enthält alle Schlüssel und Informationen zum Aufbau der Verbindung zum VPN Server



Server.

OpenVPN Grundeinstellungen OpenVDN				
Grundenstellungen Openverv				
VPN-Modus	Client			
Logdatei führen	ein 💌	Open Look in		<u> </u>
Detailstufe der Logs	5		UMTS@Werk2.werk2.pcd-demo.com.vpr	itar
Maximale Grösse der Logs	10MiB	My Recent Documents		
HTTP-Proxy-Server nutzen	п	Desktop		
	Haltharkeit des			
Status 🔿 Benutzerkonto 🌥 Server 🖓	Zertifikates	Zielport My Documents		
	Keine Einträge v	orhanden.		
0 bis 0 von 0 Einträgen		My Computer		
neue Konfigurationsdatei hochlader Choose	File No file chosen		File name: UMTS@Werk2.werk2.p	cd-demo.com.vpn.tar 💌 🛄pen
		My Network	Files of type: All Files	Cancel
	speich	iern Places	C Open as read-only	

3) Der VPN-Server wird in der Tabelle eingetragen. Aktivieren des Zuganges in der Liste.

Status 🔶	Benutzerkonto 🔺	Server 🔶	Haltbarkeit des	Protokoll (Zielport (Paketgrößenlimit 🌖	Kryptoalgorithmus	Aktion
aktiviert	UMTS	werk2.pcd- demo.com	Jun 6 09:44:45 2038 GMT	udp	1194	1400	Kompatibilitätsmodus für v1-Router	Xugang löschen
1 bis 1	von 1 Einträgen							~ ~

 Wenn der VPN Tunnel erfolgreich hergestellt wurde, ist der aktuelle Zustand unter Status-Logs → Netzwerke ersichtlich (CONNECTED)

_	Status-Logs> Netzwerk		
Info Routerkonfiguration	Netzwerk	•	
Geräte	IP-Adressen		
Messaging	WAN-IP:	VPN-Status	
«Status-Logs»	Netzwerk	Parameter	
Backup-Wartung	Logs	VPN-Modus:	client
,, ,		Port:	1194
	Firewall	Server:	werk2.pcd-demo.com
	dDNS	Protokoll:	udp
	Diagnose	Paketgrößenlimit:	1400
	Routing	Kryptoalgorithmus:	Kompatibilitätsmodus für v1-Router
		übertragene Daten: durch VPN-Tunnel empfangen: 898 Byte durch VPN-Tunnel gesendet: 660 Byte Rohdaten empfangen: 7 KiByte Rohdaten gesendet: 6 KiByte Letzte 3 Statusmeldungen: 7 KiByte Thu Jun 13 07:50:09 2013 GET_CONFIG Thu Jun 13 07:50:11 2013 ASSIGN_IP Thu Jun 13 07:50:11 2013 CONNECTED Verbunden mit: 92.104.90.64 Zugewiesene VPN-IP: 192.168.155.131	



5.1 Client Software EurogardSRConnect

Die Client Software wird benötigt, um eine openVPN Verbindung mit dem Server des Eurogard Routers aufzubauen. Für die Installation des openVPN Client benötigen Sie Administrationsrechte.

Die Software EuroGardSRConnect ist auf der Homepage von EuroGard erhältlich <u>http://www.eurogard.de</u>

Software Tool EuroGardSRConnect

14) Hinzufügen eines neuen Routers:

EurogardSRConnect - Version: 2.0.0.6 -	[Startfenster]					
weitere Datenbanken nach XML exportieren	Benutzerverwaltung					
euro gard	Verbinde erreichbare Teilnehmer	Settings Verbindungslog gnzeigen	<u>D</u> etail	Löschen	<u>N</u> euer Rou	ter
IDnr Bezeichnung	Kommentar	OpenVPN_Port	SSL_Port	ISO_Tsap_Port	Zeitprotokol	Admin_Option
Filter.	Bezeichnung filtern	<u>Eilter entfernen</u>				
🥣 wartend						

15) Laden Sie das vom Router generierte Benutzer-Zertifikat in die Applikation. Alle Schlüssel und Informationen sind in diesem Zertifikat enthalten.





16) Speichern Sie das geladene Benutzer-Zertifikat ab. Nach dem Speichern sehen Sie die Verbindungparameter im unteren Fenster. Im Normalfall müssen diese Parameter nicht bearbeitet werden.

EurogardSRConnect - Version: 2.0.0.6 -	[Konfiguration Detail]	
weitere Datenbanken nach XML exportieren	Benutzerverwaltung	
euro gard	greichbare Vetbinde Verbindungslog anzeigen Werk 2 OpenVpn Tar Datei C:\Documents and Settin Chommentar Commentar	Speichein Löschen Zurück
	L Administratorrechte fi	ir die Verbindung verwenden
	Informationen über die Erreichbarkeit des ServiceRo	uters wird nicht zur Verbindung verwendet)
	Oper/VPN Port 1194 SSL Port 44	13 SSH Port 22
	Inhalt der OpenVPN Config Datei Iremote werk2.pcd-demo. client	com
	Lonfig Speichern pott 1194 Config geuladen robind Config geuladen comp-izo Config neuladen comp-izo complexent 1400 pull ca Verk2 werk2, werk2, werk2 cert User@Werk2, werk2	mo.com.ca.cit 2 pod-demo.com.cit
wartend		ii.

17) Verbinden Sie sich mit dem VPN-Server

🖨 EurogardSRConnect - Yersion: 2.0.0.6 - [Konfiguration Detail]	
weitere Datenbanken nach XML exportieren Benutzerverwaltung	
EUTO greichbare Verbinde Speichegn Löschen Zurück Utbindungslog grezigen	
C Verbindungslog OpenVPN	
Thu Jun 2017:24:04 2013 0pen/VPN 2.31 i686-w64-mingw32 [SSL (0penSSL)] [LZ0] [PKCS11] [eurephia] [IPv6] built on Mar 28 2013 Thu Jun 2017:24:04 2013 NOTE: 0pen/VPN 2.1 requires '-script-security 2' or higher to call user-defined scripts or executables Image: Straight of the straig	
Wartend	.::
Anwenderhinweis Image: Comparison of the second	



- 18) Der PC ist nun ein Teilnehmer des gegenüberliegenden Netzwerkes. Der Zugriff auf die Geräte ist mit allen Applikationen die Ethernet unterstützen möglich.
- ➔ Browser
- → PG 5





5.2 IOS und Android Systeme

Werden 2 Router im Client / Server Betrieb verwendet, so ist es möglich I-OS Systeme sowie Android Systeme kabellos am Netzwerk des EuroGard Service Router 2 anzumelden.

Dafür muss der Router, an welchem die Systeme verbunden werden sollen, mit einer W-LAN Option ausgestattet sein.

Der Euro Gard Client Router kann entweder über Kabel oder auch über UMTS mit dem Server verbunden werden.





6 Net Module VPN Router NB 1600 und 1600-U

Konfigurieren des NB 1600 oder NB 1600-U als openVPN-Server im Modus TUN.



Wide Area Network (WAN) \rightarrow Verbindung zum Router mit öffentlichen IP-Adresse Local Area Network (LAN) \rightarrow Verbindung zum lokalen Netzwerk



6.1 Technische Daten

	Net Module NB 1600	Net Module NB 1600-U
Bestelldaten	NB 1600	NB 1600-U
Weitere	http://www.netmodule.de/prod	http://www.netmodule.de/products/indu
Informationen	ucts/industrial-routers/wireline-	strial-routers/mobile-router.html
	router.html	
Einsatz/Bauform	Industriell	Industriell
Hutschienen-	Hutschienenmontage	Hutschienenmontage
montage		
Spannungs-	24 V DC (-15% +20%)	24 V DC (-15% +20%)
versorgung		
VPN		
Eigenschaften		
Anzahl WAN	1; LAN	2; LAN, UMTS
Interfaces		
Integriertes	Nein	Nein
ADSL/VDSL		
Modem		
VPN PPTP	Ja	Ja
VPN	Nein	Nein
L2TP/IPSec		
openVPN	Ja	Ja
Anz. VPN	10	10
Clients		
Windows Client	Ja openVPN	Ja openVPN
IOS Client	Ja openVPN	Ja openVPN
Android Client	Ja openVPN	Ja openVPN
Erweiterungen		
3G / 4G Modem	Nein	3G (UMTS 7.2 Mbps)



6.2 Öffnen des Setup Menü

Zum Einrichten des Net Module Routers muss der PC mit einer LAN-Schnittstelle des Routers verbunden werden. Der Router wird mit einem aktivierten DHCP-Server ausgeliefert. Es sollte deshalb vermieden werden, den Net Module Router mit Werkskonfiguration in eine Ethernet-Infrastruktur mit bereits vorhandenem DHCP-Server zu konfigurieren.

Empfohlen:

Trennen Sie ihren PC von allen bestehenden Netzwerkverbindungen. Verbinden Sie ihren PC direkt mit dem Router.

Die Standard IP-Adresse des Routers ist von Werk auf "192.168.1.1" eingestellt. Der DHCP-Server des Routers wird dem angeschlossenen PC eine Adresse im Adressraum des DHCP-Servers zur Verfügung stellen.

Die Konfiguration des Routers wird mit Hilfe eines Browsers erstellt. Damit die Konfigurationsoberfläche im Browser geladen wird, muss die IP-Adresse des Routers im Browser aufgerufen werden.

Der Router startet bei der ersten Verbindung einen Konfigurationsassistenten bei welchem die Passwörter und Benutzer Namen gesetzt werden.

net SS		
Ш.	NB1600 Login Please provide username and password to log in:	
ANAG	Username:	
/EB M	Login	
600 M		
R		



6.3 Konfigurieren der WAN und LAN Ports (Wide Area Network)

Konfigurieren der LAN 1 Schnittstelle als WAN Interface. Die IP-Adresse des WAN Interfaces wird vom vorher positionierten Router bereitgestellt oder kann statisch vergeben werden im Bereich ausserhalb des vorhergehenden DHCP-Servers.

net S		RFACES ROUTING	FIREWALL	VPN	SERVICES	SYSTEM	LOGOU
WAN Link Management Settings	3 LAN1	AN2					
Ethernet Port Settings	Mode:		l V				
Link Cettings IP Settings	WAN Mode:		CP client				
USB Serial Port		5 C stati O PPF	ic IP PoE				
Digital I/O	MTU:						

Die LAN 2 Schnittstelle wird für das Automationsnetzwerk verwendet und sollte eine IP-Adresse in dessen Bereich erhalten. Im folgenden Beispiel befindet sich das Automationsnetzwerk im IP-Adressen Bereich 192.168.155.0/24

LAN1 LAN2]	
IP Settings LAN2		
Mode:		
Static Configuration		
IP address:	3 192.168.155.12	
Subnet mask:	255.255.255.0	
IP address:		
Subnet mask:		





Wenn DHCP-Client für die WAN Schnittstelle aktiviert wurde kann die vom DHCP-Server erhaltene IP-Adresse im Bereich HOME überprüft werden



Connection Details LAN1

Description	Value
Administrative state	enabled
Operational state	up
Link is up since	2013-09-30 07:09:30
IP address	192.168.0.19
Gateway	192.168.0.1
Transfer rate down / up	7.37 KByte/s / 1.79 KByte/s
Data downloaded / uploaded since 2013-04-12 04:53:33	878.13 MB / 6.17 MB Reset

6.4 Zeitkonfiguration

Die Zeitkonfiguration des Routers muss vor dem Erstellen von Zertifikaten geprüft werden. Setzen Sie gegebenen falls die Zeit manuell oder aktivieren Sie die Time Synchronisation.

 \rightarrow Eine Internet Verbindung ist für die Time Synchronisation erforderlich.

	0.0		
	Module	HOME INTERFACES	ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
\overline{c}	System Settings Time & Region	System Time Current system time:	2013-09-30 08:16:27 Set time
N	System Information Restart	Time Synchronisation	
MA	Authentication	NTP server:	0.pool.ntp.org
8	User Accounts Remote Authentication	NTP server 2 (optional):	1.pool.ntp.org
\geq	Software Update	Time zone	
00	Manual Software Update Automatic Software Update	Time zone:	UTC+01:00 Amsterdam, Berlin, Bern, Rome, Stockholm 💌
316	Configuration	Daylight saving changes:	N
NE	Automatic File Configuration Factory Configuration	Apply Sync	



6.5 Erstellen der Server Zertifikate

Die Server Zertifikate werden benötigt um einen openVPN Benutzer zu erstellen. Die im Router hinterlegten Informationen wie Hostname, e-Mail Adressen und mehr werden für das Zertifikat verwendet.

r Mo	net 💦	HOME	INTERFACES	5 ROUTIN	IG FIRE\	WALL	VPN	SERVICES	SYSTEM	LOGOUT
System	1	Root CA	HTTPS	SSH	OpenVPN1					
Setting Time &	gs & Region	Root CA								
Syste	m Information	Root CA certi	ficate:	mis	sing					
Resta	n	Root CA key:		mis	sing					
Authe User / Remot Softwa Manua Autor	ntication Accounts te Authentication re Update al Software Update natic Software Update	3 Initialize	Processi The device Step 1: Init Step 2: Ge Step 3: Ge	ing e is processir tializing certifi nerating rand nerating Diffi	g a key/certi cate databas om bits a-Hellmann	ficate requ se parameter	iest, ple r file	ase stand by		
Configi Manua	uration al File Configuration		Root CA							
Autor	natic File Configuration		Root CA ce	rtificate:		View				
Tractor	ry configuration		Root CA ke	y:		View				
Netwo Syste	eshooting ork Debugging m Debugging						J			

Nach dem Erstellen des Server-Zertifikates muss ein Zertifikat für den openVPN-Tunnel erstellt werden.

	4.0				-		
	Module SS	HOME INTERFAC		FIREWALL VI	PN SERVICES	SYSTEM	LOGOUT
NAGER	System Settings Time & Region System Information Restart	Root CA HTTPS OpenVPN1 Tunnel1 is running in serve	SSH Open	nVPN1 es (configure)			
BMA	Authentication Authentication User Accounts Remote Authentication	 generate keys/certificates upload pre-generated keys/certificates 					
N	Software Update	Server certificate:	missing missing				
000	Manual Software Update Automatic Software Update	CA root certificate:	missing				
NB16	Configuration Manual File Configuration Automatic File Configuration Factory Configuration	4 Create Processing The device is pro Step 1: Generating Step 2: Creating	cessing a key/certificate reques g key for open/pn-tunnel0 :ertification request for	st, please stand by.			
	Troubleshooting Network Debugging System Debugging Tech Support	- //CN=NB160/dm Step 3: Signing c Step 4: Copying i Step 5: Ventiging	ailAddress=router@support.ne ertificate for operrypn-tunnel0 w :A root certificate/key pperrypn-tunnel0 certificate aga ficato:	etmodule.com/O=NetModu rith config from /tmp/openy inst root CA	le/OU=NetModule/C=CH/S pn-tunnel0-ca.conf	:T=Switzerland/L:	
(2)	Keys & Certificates	Private key:	ncate.	View			
\sim		CA root cer	iificate:	View			



6.6 Aktivieren des openVPN Servers

Aktivieren des open VPN Servers

				(1)				
	Module SS	HOME INTERFACES	ROUTING	FIREWALL VP	N SERVICES	SYSTEM	LOGOUT	1
(2)	OpenVPN Administration	OpenVPN Administration		hed				
IAG	Tunnel Configuration Client Management	Destation link shange:	O disa	bled				
MAN	IPsec Administration Tunnel Configuration	4 Apply Restart	M					
WEB	PPTP Administration Tunnel Configuration	OpenVPN Tunnel Status						
0		Tunnel 1:	Server is	s running				
00		Tunnel 2:	disabled	ł				
16		Tunnel 3:	disabled	Ł				
9		Tunnel 4:	disabled	ł				

Damit sich ein Client anmelden kann muss der Tunnel Konfiguriert werden. Der Net Module Router ermöglicht das Konfigurieren von einem VPN-Server Tunnel oder 4 Client Tunnels.

Aktivieren Sie den Tunnel als Server.

Wenn mobile Geräte mit Android oder I-OS System sich am openVPN Server anmelden müssen, muss der TUN Modus mit Routing aktiviert werden.

	3	
OpenVPN	Tunnel 1 Tunnel	2 Tunnel 3 Tunnel 4
Tunnel Configuration	OpenVPN Tunnel 1 Co	ifiguration
Client Management	Operation mode:	C disabled
IPsec Administration		A client © standard
Tunnel Configuration		- opport
PPTP Administration	Server port:	1194
Tunnel Configuration	Туре:	
	Network mode:	6 routed C bridged
	Cipher:	BF-CBC •
	Use compression:	V
	Use keepalive:	
	Redirect gateway:	
	Protocol:	udp 💌
	Authentication:	certificate-based



6.7 Anlegen eines Client Zuganges

Aktivieren eines Clients in dem die Checkbox markiert wird es empfiehlt sich dem Client einen Namen zu vergeben.

OpenVPN	Clients	Networking Routes	Download	
Administration Tunnel Configuration	Client Manager	nent		
Client Management	Enabled	Client	Connection info	
IPsec Administration	(3) ☑	Daniel		
Tunnel Configuration		Client2		
PPTP Administration		Client3		
Tunnel Configuration		Client4		
		Client5		
		Client6		
		Client7		
		Client8		
		Client9		
		Client10	-	

Die Tunnel Adresse als auch die Client Netzwerk Adresse müssen bei der aktuellen Tunnelkonfiguration nicht verändert werden.

Module &	HOME INTERFACES	ROUTING	FIREWALL VPN SERVICES	SYSTEM	LOCOUT	_
	(3)				100001	6
Administration	Clients Networking	Routes	Download			
2 Client Management	Client Networking This menu can be used to config	ure a fixed tunne	el endpoint address for each client.			
IPsec Administration Tunnel Configuration	You may also specify a network, v Select client:	whose packets :	should get routed towards the client.			
PPTP Administration Tunnel Configuration	Tunnel address:	⊙ dynar ⊜ fixed	nic			
	Client network:	⊙ none	O specify			



Damit die Netze hinter dem VPN-Tunnel bekannt gemacht werden müssen die Routen gesetzt werden. Hier muss die Netzadresse des Automationsnetzes eingetragen werden.

	net 🔊		
	Module 🐼	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT	ļ
C	OpenVPN	Clients Networking Routes Download	
	Administration Tunnel Configuration Client Management	Client Routes This list of network routes will be pushed to each client, so that matching packets will be routed back to the server.	
MAN	IPsec Administration Tunnel Configuration	Network Netmask 192.168.155.0 255.255.255.0	
N F B	PPTP Administration	4 192.168.0.0 255.255.2	
600 \			
NB1			
		Enable routing between clients:	
	(

Die Konfigurationsfiles für den Client können vom Router geladen werden. Achten Sie darauf das die Serveradresse korrekt geschrieben und erreichbar ist

OpenVPN Clients Network Administration Tunnel Configuration OpenVPN Clients Client Management Download OpenVPN Client Client Version	ES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT (3 king Routes Download
OpenVPN Administration Tunnel Configuration Client Management Download OpenVPN Clie	king Routes Download
Tunnel Configuration Client Management Download OpenVPN Clie	
	ent
IPsec Windows Administration Linux	
PPTP Download Expert Mode F	Files 4
Administration Server address/hostname: Tunnel Configuration	178.83.186.183



7 Windows openVPN Client für Net Module Router

7.1 Installation

Installieren Sie die Applikation openVPN 2.2.2 (<u>http://www.netmodule.com/download/openvpn-client/windows</u>) Für die Installation benötigen Sie Administrationsrechte.

7.2 Entpacken des Konfigurationpakets

Entpacken Sie das vom Router geladene Konfigurationspacket. Kopieren Sie den Inhalt in den Ordner "config" welchen Sie im Installationsverzeichnis des openVPN Clients finden "C:\Program Files\OpenVPN\config".





7.3 Herstellen einer Verbindung

Starten des openVPN Client. Dieser wird mit einem kleinen Symbol in der Statusleiste des Betriebssystems angezeigt und bauen Sie einer Verbindung zum openVPN-Server auf.







🦻 OpenYPN Yerbindung (Daniel)	
Aktueler Status: Verbunden	
Addition Status: Verturation Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 MAMAGENETIN: TCP Socket listering on [AF_INET]127.00.1:25340 Mon Seg 30100338 2013 <t< th=""><th></th></t<>	
Mon Sep 30 1003 44 2013 PUTIONS IMPORT:itconlig/up options modified	
Men Sep 30 1003 44 2013 OPTIONS IMPORT: router Men Sep 30 1003 44 2013 do, icorrig, to:pyte-0, to:s Men Sep 30 1003 44 2013 do, icorrig, to:pyte-0, to:s Men Sep 30 1003 44 2013 open_tun, to:pyte-0 Men Sep 30 1003 44 2013 TAP-Windows Driver Vesia Men Sep 30 1003 44 2013 TAP-Windows Driver Vesia Men Sep 30 1003 44 2013 Successful APP Fluth on in Men Sep 30 1003 44 2013 Successful APP Fluth on in Men Sep 30 1003 44 2013 Successful APP Fluth on in Men Sep 30 1003 44 2013 Successful APP Fluth on in Men Sep 30 1003 44 2013 Successful APP Fluth on in Men Sep 30 1003 44 2013 Successful APP Fluth on in Men Sep 30 1003 44 2013 Successful APP Fluth on in Men Sep 30 1003 44 2013 Successful APP Fluth on in Men Sep 30 1003 44 2013 Revent AP	
Mon Sep 30 10.03 49 2013 C: VwINDDW/S Vystem32/w Mon Sep 30 10.03 49 2013 Initialization Sequence Com Mon Sep 30 10.03 49 2013 Initialization Sequence Com Mon Sep 30 10.03 49 2013 MANAGEMENT: >STATE:)3
Trennen Neu Verbinden Minimier	ren

Die im VPN-Server hinterlegten Routen werden aktiviert.

Achtung hierfür muss der eingeloggte Windows Benutzer rechte zum Erstellen von Routingtabellen besitzen.



8 Android openVPN Client für Net Module Router

Laden Sie die App OpenVPN Connect oder OpenVPN für Android über den Android Play Store herunter.

Verbinden Sie das Gerät mit ihrem PC, auf welchem sich die vom Router geladenen Konfigurationsdateien befinden.

Achtung: Der openVPN Server muss für Android Client Systeme im TUN Modus konfiguriert sein.

Kopieren Sie die Konfigurationsdateien auf das Gerät in das Verzeichnis "config"

Beispiel: "Computer\GT-I9100\Phone\config"



Starten Sie die App OpenVPN für Android und öffen Sie die vom PC geladene openVPN Konfigurationsdatei.

🜵 80% 🞓 <u>↑</u> 🖻		h. 🕅 🖇	13:49	🌵 📥 80% 🚖	<u>1 1 2 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 </u>	13:50	🌵 ⊾ 👓 🖈 İ 🖻 👘 🖇 😤 📶 🙆 13:50	
Apps		Widgets	👤	OpenVPN for Android		A Import configuration file		
0	(3)	\bigcirc		Profiles	Settings F	AQ	File Explorer	
droid VNC server	VNC_server	Screenshot UX Trial	Quadris				Location: /storage/sdcard0 WhatsApp	
TEIGH	•	۲					🖿 bluetooth	
TETRIS®	Swisscom Apps	WebOfCam	Dolphin Browser	No VPN profiles defined.			🖿 burstlyImageCache	
	Q		NCP.			Lice the 🕀 ison to add a new VPN		
Cisco VPN strongSwan		n OpenVPN for NCP VPN				🛋 com.webofcam		
Group		Android	Client (Trial)	Use the icon to import an existing (.ovpn or .conf) profile from your sdcard.		(.ovpn or	🖿 config	
u 🙂			~	Be sure to also check out the FAQ. There is a a divide.		🖿 documents		
FortiClient	WhatsApp	SBC Micro Browser Lite	Net Ping	ч ў	quick stan guide.		🖿 external_sd	
	SBC						🖿 log	
OpenVPN Connect	SBC Micro Browser						🖿 media	
		• •		\oplus			Select	

Das Profil ist nun in openVPN Client für Android importiert und verfügbar.

Saving screenshot	Saving screenshot		Saving screenshot		
R Import configuration file	😭 Convert Config File		OpenVPN for Android		
File Explorer	Importing config file from source file:/storage/sdcard0/config/		Profiles	Settings	FAQ
Location: /storage/sdcard0/config	Daniel.ovpn				
i /	Your configuration had a few configuration options that are not		Daniel		
in/	mapped to UI configurations.				
Daniel.conf	These options were added as custom configuration options. The custom configuration is displayed below:				
Daniel.crt					
📕 Daniel.key	resolv-retry infinite				
Daniel.ovpn					
Daniel.p12	Done reading config file.				
Ca.crt					
dh1024. Copied to clipboard	Copied to clipboard				
Select	×	H	\oplus		

8.1 Herstellen einer Verbindung

Verbinden Sie sich mit dem openVPN Server.

Das Betriebssystem Android wird Sie bezüglich der Netzwerkkonfiguration fragen ob Sie dieser Applikation vertrauen. Damit eine Verbindung hergestellt werden kann, müssen Sie den Dialog bestätigen.

Wenn die Verbindung erfolgreich hergestellt wurde wird das Schlüssel Icon in der Statusleiste von Android angezeigt.







9 I-OS openVPN Client für Net Module Router

Installieren Sie die App openVPN aus dem Apple App Store

Installieren Sie die Applikation I-Tunes auf ihrem PC und Verbinden Sie das I-Pad mit ihrem PC.

Achtung: Der openVPN Server muss für I-OS Client Systeme im TUN Modus konfiguriert sein.

Öffnen Sie das iPad oder I-OS Gerät in I-Tunes

• • • •	-0	ú			Qr Mediathek
🞜 Musik 🗧	Titel Alben	Interpreten Genres	Wiedergabelisten Radio	Match	☐ iPad ▲ iTunes Store
			et iTunes fåe	Edit View Controls Store	Advanced Window Help

Laden Sie die vom Router entpackten Dateien für die openVPN Tunnel Konfiguration über den Reiter Apps \rightarrow OpenVPN in die Applikation.

Übersicht Info Apps Musik Filme TV Fotos Auf Nach Art sortieren ‡ Q Nach Art sortieren ‡ Q	f diesem iPad
Ubersicht Info Apps Musik Filme TV Fotos Aut	f diesem iPad 2 Apps
Nach Artsortieren	
Nachrichten Ralender	
Nachrichten Kalender	
Nachrichten Kalender	
	Kontakte iTunes
and the second se	1
Program Files\OpenVPN\config\Daniel Erinnerungen Notizen	Mail App Store
Edit View Favorites Iools Help	
Back + 🕥 - 🏂 🔎 Search 🌔 Folders 🛄 -	
ss C:\Program Files\OpenVPN\config\Daniel	Fotos Videos
le and Folder Tasks *	
Make a new folder	3
Publish this folder to the Daniel, key	
Web Daniel.crt	The second second
Daniel.cont	Strate Str
ther Places *	4
a config	
	- H-
Einstellung	en Safari
Neue Apps automatisch installieren Wählen Sie Appszum Installierer	n auf Ihrem iPad aus oder bewegen Siesie auf einen bestimmten
Home-Bildschirm. Ordnen Sie	e App-Symbole und Home-Bildschirme über Bewegen neu an
\sim	
Freigabe	
Mit folgenden Apps können Sie Dokumente zwischen dem iPad und diesem Compute übertrager	n.
Apps Dokumente von "OpenVPN":	
Daniel.conf	Heute 14:27 8 KB
OpenVPN Some Daniel.p12	Heute 14:27 8 KB
I-PAD.conf	20.08.2013 14:14 8 KB
LPAD.p12	20.08.2013 14:14 8 KB
	Hinzutugen Sichern unter



Öffnen Sie die App OpenVPN. Die geladene openVPN Server Konfiguration wird selbstständig erkannt und kann durch den Add Button bestätigt werden.

Swisscom '주'	OpenVPN	Xädt nich			
New profiles a	e available				
🕕 1 new (DpenVPN profile is available for import.	0			
(178.83.1 Autologin p	178.83.186.183/Daniel Autologin profile				
OpenVPN	I Connect				
Profile	178.83.186.183-2/IPAD@SR2.178.83.186.183.tun.vpn Autologin profile	>			
Status	Disconnected	>			
Connection	$\bigcirc \bigcirc$				
More from Ope	nVPN Technologies				
priva	tetunnel.com Your Secure and Private Path to the Internet	>			
	NVPN Access Server VPN Solution for your Business	>			

9.1 Herstellen einer Verbindung

Verbinden Sie sich mit dem openVPN Server indem Sie den Schieberegler bewegen

wisscom 🙃	14:44	🕴 Lädt nicht 🔳
out	OpenVPN	Help
🔞 OpenVPN Conne	ot	
Profile Q 17	8.83.186.183/Daniel ologin profile	
Status 🤘 Co	nnecting	>
Connection		
Connection Details		
Duration 0:00:01	Last packet received < 1 second ago	
Bytes In 48	Bytes Out 106 -	



Wenn Sie den Status Connected erhalten wurde der VPN-Tunnel erfolgreich aufgebaut.

Swisscom 🔶 🔤]		14:45		Lädt nic	sht 🔜		
out		(DpenVPN			Help		
၇ Open	VPN Connect	Philos # 47 40 - Calco						
Profile	Autologin profile	183/Daniel			Constitution of the second sec			
Status	Connected			>	unit of the State (In America			
Connect	ion					Provide Control of Control o		
Connectio	n Details					And the second sec		
Duration	0:00:08 La	ast packet receiv	acket received 1 second ago					
Bytes In	Bytes In 3.88 KB		Bytes Out 3.84 KB -					
VPN IPv	6	VPN IPv4	10.8.0.6					
User		Client IP						
Server	178.83.186.183	Server IP	178.83.186.183					
Port	1194	Protocol	UDPv4					
More from	OpenVPN Technologies	5						
	privatetunnel.com Yo	our Secure and P	rivate Path to the I	nternet	>			
?	OpenVPN Access Serv	er VPN Solutio	n for your Busines	s	>			