

CR220N-Fernwartung über einen externen Internetzugang

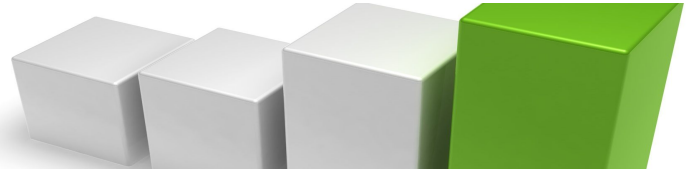
1. Allgemeines

In der Internet-Fernwartung wird es immer wichtiger, nicht nur einzelne IP-Adressen anzusprechen, sondern ein ganzes IP-Subnetz fernzuwarten. Der VPN-Router CR220N stellt ein solches Fernwartungs-Subnetz auf seinem LAN1-Interface zur Verfügung. Alle Netzwerkteilnehmer, die mit diesem Interface verbunden sind, nehmen an der Fernwartung teil. Es handelt sich um ein Klasse-C-Subnetz, das heißt, es können bis zu 252 Netzwerkteilnehmer ferngewartet werden. Das Fernwartungs-Subnetz ist frei konfigurierbar, indem die LAN1-IP-Adresse durch den Anwender konfiguriert wird.

Es können alle IP-Protokolle verwendet werden, also nicht nur TCP, sondern beispielsweise auch UDP und ICMP. Das ist für die Inbetriebnahme hilfreich, da somit alle fernzuwartenden Netzwerkteilnehmer auch per „ping-Befehl“ erreicht werden können.

Als Fernwartungs-Client dient ein PC, der ebenfalls mit dem Internet verbunden wird. Die Fernwartungs-Verbindung zwischen PC und CR220N ist durch einen OpenVPN-Tunnel gesichert. Damit ist die Übertragung der Anwenderdaten nach dem neuesten Stand der Technik gegen Fremdzugriffe geschützt. Als VPN-Vermittler arbeitet, für den Anwender unsichtbar, ein schneller OpenVPN-Server im Internet, der „ISK-CRASER“. Für eine komfortable Subnetz-Fernwartung nach heutigem technischen Stand ist die Vermittlung über den „ISK-CRASER“ unumgänglich. Dafür sprechen 3 gewichtige Gründe:

1. CRASER ist 24h Online und hat die Leistungsfähigkeit moderner Serversysteme. Dadurch wird eine gleichzeitige und sichere Kommunikation mit sehr vielen Clients möglich.
2. CRASER ist ein Open-VPN-Server mit einer festen IP-Adresse: Sowohl der Fernwartungs-PC als auch der Fernwartungsrouter melden sich als VPN-Client an. Damit ist weder beim Fernwartungs-PC noch beim Fernwartungsrouter eine public IP-Adresse bzw. eine feste IP-Adresse erforderlich.
3. CRASER kann Open-VPN-Verbindungen routen: Das bedeutet, der Fernwartungs-PC kann mit einer einzigen Open-VPN-Verbindung auch Fernwartungs-Subnetze mehrerer CR220N/CR230U gleichzeitig erreichen und die Fernwartungs-Subnetze mehrerer CR220N/CR230U können auch untereinander kommunizieren. Bei Bedarf sind mehrere Fernwartungs-PCs mit unterschiedlichen Zertifikaten möglich. Maximal 64 Fernwartungs-Subnetze lassen sich nach diesem Prinzip gleichzeitig durch den CRASER vermitteln. Die Zugriffsrechte aller Clients können variiert werden.



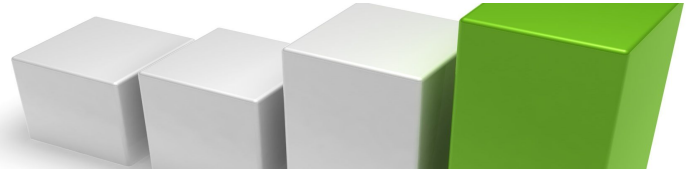
2. Aufgabenstellung

Der VPN-Router CR220N soll als Netzwerkteilnehmer hinter einem übergeordneten NAT-Router betrieben werden und dessen Internetzugang nutzen. Die Konfiguration des übergeordneten Routers darf nicht geändert werden, ein DHCP-Server ist auf diesem Router aktiv.

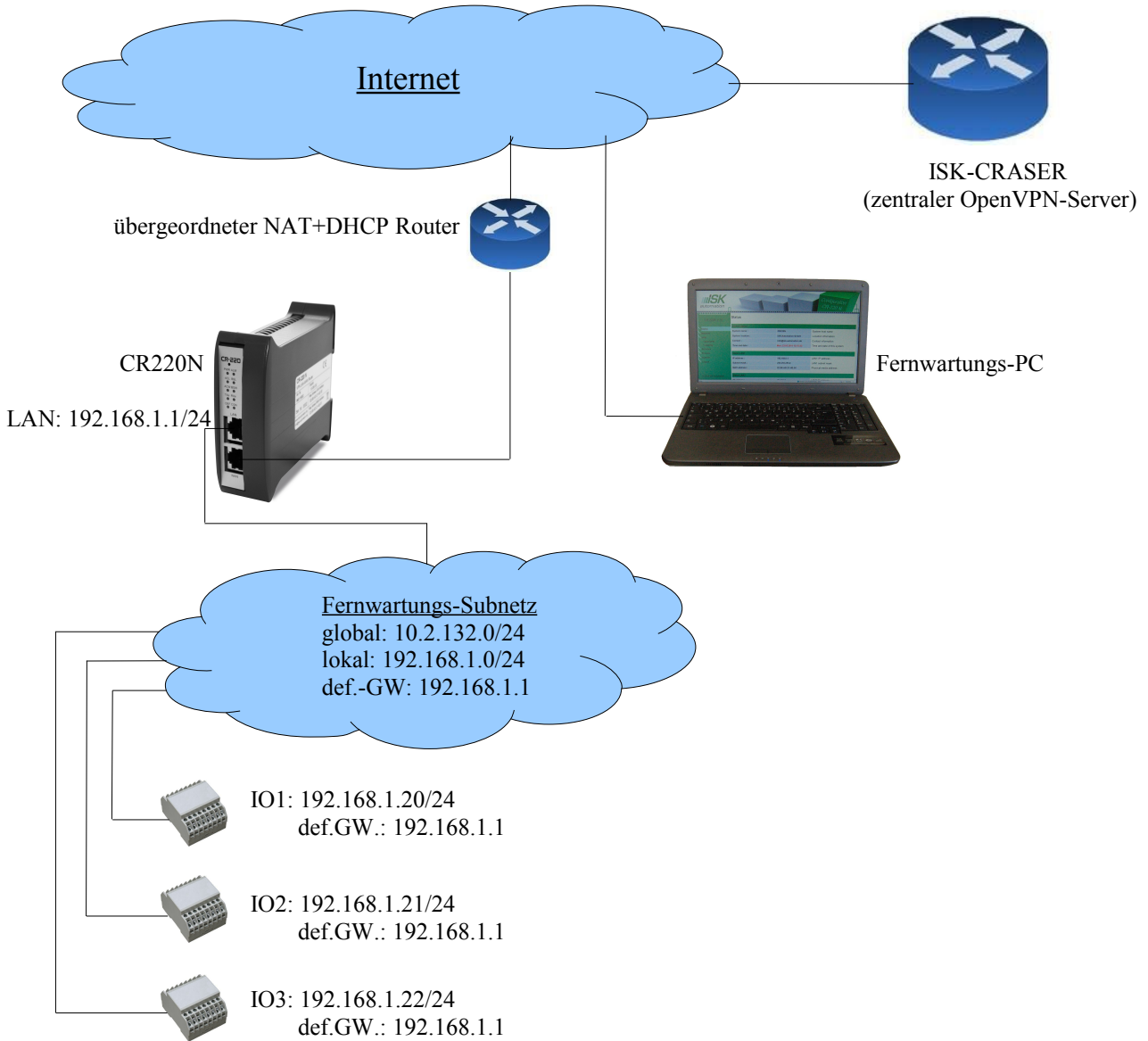
Es soll eine Verbindung zwischen einem Fernwartungs-PC und dem Fernwartungs-Subnet des CR220N über das Internet in Betrieb genommen werden. Diese Inbetriebnahme erfolgt in 5 Schritten:

1. Kabelverbindungen vorbereiten.
2. Fernwartungs-Subnetz (LAN1) auf eine zur Anwendung passende IP-Adresse konfigurieren und DHCP-Client auf LAN2 einrichten.
3. OpenVPN auf dem CR220N aktiv schalten und Verbindung zum CRASER herstellen.
4. Fernwartungs-PC konfigurieren und eine OpenVPN-Verbindung zum CRASER aufbauen.
5. Fernwartungs-Subnetz durch ping-Kommandos von der Konsole des Fernwartungs-PCs testen.

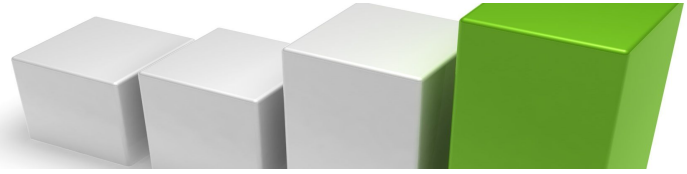
Werfen wir zunächst einen Blick auf die Netzwerkstruktur unserer Anwendung, bevor wir die 5 Schritte zur Inbetriebnahme abarbeiten:



3. Netzwerkstruktur der Fernwartung mit Beispieladressen



Testzugriffe:	PC → CR220N:	ping 10.2.132.1	(globaler Zugriff)
	PC → IO1:	ping 10.2.132.20	(globaler Zugriff)
	PC → IO2:	ping 10.2.132.21	(globaler Zugriff)
	PC → IO3:	ping 10.2.132.22	(globaler Zugriff)
	IO1 → IO2:	ping 192.168.1.21	(lokaler Zugriff)



Tipp1: Ein globaler Zugriff ist ein Zugriff auf ein Fernwartungs-Subnetz über das Internet.
Ein lokaler Zugriff ist ein Zugriff innerhalb eines Fernwartungs-Subnetzes.

Tipp2: Die globale IP-Adresse Ihres Fernwartungs-Subnets ist für jeden am CRASER arbeitenden Router einmalig und ist bereits auf Ihrem Router vorkonfiguriert (siehe VPN → OpenVPN → p12-certificate)

Tipp3: So finden Sie die Zieladresse für einen globalen Zugriff auf den Teilnehmer „IO1“ Ihres Fernwartungs-Subnetzes:

globale Adresse des Fernwartungs-Subnetzes:	10.2.132.0/24
gesuchte Zieladresse:	→ 10.2.132.20
lokale Adresse des Teilnehmers IO1:	192.168.1.20/24

Tipp4: Durch die Zuordnung der globalen IP-Adresse zur lokalen IP-Adresse des Fernwartungs-Subnetzes können Sie die lokale IP-Adresse frei konfigurieren, ohne Rücksicht auf später hinzukommende Fernwartungs-Subnetze nehmen zu müssen.

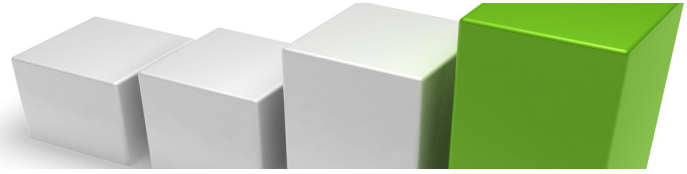
Tipp5: Die Teilnehmer des Fernwartungs-Subnetzes können das Internet benutzen. Eine Sperrung dieser Funktion ist durch Laden einer speziellen Firewalldatei möglich. Bei Bedarf stellen wir Ihnen diese Datei zur Verfügung.

Tipp6: Anstelle des übergeordneten Routers können auch spezielle Modems (z.B. Satellitenmodem) eingesetzt werden, die nur im PPPOE-Mode mit aktivem DHCP-Server arbeiten.

4. Checkliste zur Inbetriebnahme eines Fernwartungs-CR220N über einen externen Internetzugang

Ausgangszustand:

- ISK-Automation liefert einen für Fernwartungszwecke vorkonfigurierten CR220N. Das OpenVPN-Zertifikat und die Firewalldatei sind bereits installiert.
- ISK-Automation liefert die OpenVPN-Konfigurationsdateien für den Fernwartungs-PC. Für das Projekt2, PC1 der Firma ISK-Automation würde diese Datei „ISK-P2-PC1.zip“ heißen.



Inbetriebnahme des Fernwartungsrouters CR220N über einen ext. Internetzugang in 5 Schritten:

1. Vorbereitungen

- Das mit "LAN" bezeichnete Interface wird mit dem Fernwartungs-Subnetz verbunden.
- Das mit "WAN" bezeichnete Interface wird mit dem Netzwerk des übergeordneten Routers verbunden.
- Die Alias-Adresse kann genutzt werden, um den CR220N während der Konfiguration ohne Umschaltung des PC-Subnets ansprechen zu können.
- Web-Konfiguration des "CR220N" aufrufen: <http://192.168.0.126:7777>
- login: admin

2. lokale Fernwartungs-Subnetzadresse konfigurieren und DHCP-Client einrichten (siehe Bild1)
Network → LAN → LAN1:

- IP address: 192.168.1.1 (Beispiel, die lokale Fernwartungsadresse können Sie selbst festlegen)
- Subnet mask: 255.255.255.0 (die Subnetzmaske muss auf 255.255.255.0 konfiguriert werden).

Network → LAN → LAN2:

- DHCP-client: aktiv
- Apply-Schalter betätigen.
- Statusseite des CR220N aufrufen (siehe Bild2)
Testen Sie, ob das LAN2-Interface eine IP-Adresse vom DHCP-Server bezogen hat. Im Falle keine Adresse per DHCP zugewiesen wurde, Router neu booten (power down/power up).
LAN1- und LAN2-Subnetz auf Überschneidungen testen (siehe Bild2).

3. OpenVPN-Client aktivieren. (siehe Bild3)

VPN → OpenVPN:

- Enable/Disable OpenVPN: aktivieren
- "Apply" betätigen.
- die Verbindung zum CRASER baut sich nach einigen Sekunden auf. Während des Verbindungsaufbaus blinkt die CON-LED. Nachdem die Verbindung aufgebaut ist, leuchtet die CON-LED statisch.

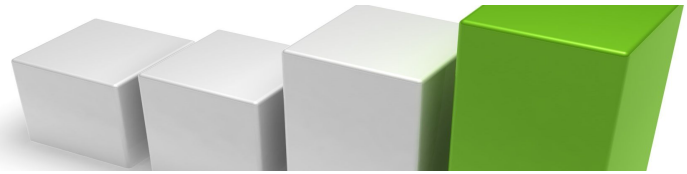
4. OpenVPN-Client auf dem Fernwartungs-PC konfigurieren und starten.

OpenVPN-Client nach unserer Anleitung „VPN_PC_Client_Install.pdf“ auf dem Fernwartungs-PC installieren und mit dem zu diesem Router gelieferten PC-Zertifikatepaket konfigurieren. Danach den OpenVPN-Client auf dem Fernwartungs-PC starten.

5. Subnet des CR220N vom Fernwartungs-PC her pingen:

ping-Befehle siehe Kapitel 3 dieser Dokumentation.

Achtung: Benutzen Sie bei den ping-Befehlen die globale Subnetzadresse Ihres konkreten Fernwartungs-Subnetzes. Diese Adresse ist auf Ihrem Router schon vorkonfiguriert. Sie finden sie unter VPN → OpenVPN → p12 certificate.



5. Darstellung der zugehörigen Konfigurationsseiten zum Kapitel 4 dieser Doku

Bild 1 lokale Fernwartungs-Subnetadresse (LAN1) und DHCP-client für LAN2 konfigurieren:

CR-220N V.10

Status

Network

- WAN
- LAN
- COM
- Logging

VPN

Services

Proxies

System

Logout

© 2010 ISK-Automation

LAN configuration

LAN1 configuration

Enable/Disable interface LAN1 :	<input checked="" type="checkbox"/>
DHCP-client :	<input type="checkbox"/>
Use the following IP address :	<input checked="" type="radio"/>
IP address :	192 . 168 . 1 . 1
Subnet mask :	255 . 255 . 255 . 0
Enable/Disable alias IP address :	<input checked="" type="checkbox"/>
Alias IP address :	192 . 168 . 0 . 126
Alias subnet mask :	255 . 255 . 255 . 0

LAN2 configuration

Enable/Disable interface LAN2 :	<input checked="" type="checkbox"/>
Use device for DSL :	<input type="checkbox"/>
DHCP-client :	<input checked="" type="radio"/>
Use the following IP address :	<input type="radio"/>
IP address :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet mask :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

DNS configuration

Use a DNS server address :	<input type="checkbox"/>
----------------------------	--------------------------

Default gateway configuration

Use a gateway address :	<input type="checkbox"/>
-------------------------	--------------------------

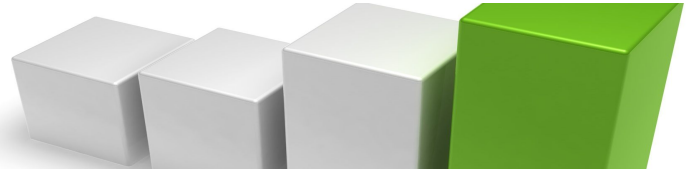


Bild 2 Status des CR220N
(DHCP-Zuweisungen für LAN2 vom übergeordneten Router überprüfen).

CR-220N V.10		Status	
<ul style="list-style-type: none"> Status Network <ul style="list-style-type: none"> • WAN • LAN • COM • Logging VPN Services Proxies System Logout 	System status		
	System name :	CR220N	System host name
	System location :	ISK-Automation GmbH	Location information
	Contact :	info@isk-automation.de	Contact information
	Time and date :	Tue, 31.05.2011 16:21:00	Time and date of this system
	Status LAN1		
	IP address :	192.168.1.1	LAN1 IP address
	Subnet mask :	255.255.255.0	LAN1 subnet mask
	MAC address :	02:80:AD:21:32:56	Physical media address
	Alias IP address :	192.168.0.126	LAN1 alias IP address
	Alias subnet mask :	255.255.255.0	LAN1 alias subnet mask
	Status LAN2		
IP address :	192.168.0.22	LAN2 IP address	
Subnet mask :	255.255.255.0	LAN2 subnet mask	
MAC address :	02:80:AD:21:32:57	Physical media address	
Status DNS			
Primary DNS server :	192.168.0.1	1st DNS server address	
Status route			
Default gateway :	192.168.0.1	Default gateway for device	

© 2010 ISK-Automation

Achtung: Das per DHCP zugewiesene LAN2-Subnetz darf sich nicht mit dem konfigurierten LAN1-Subnetz überschneiden. Ändern Sie in einem solchen Fall das LAN1-Subnetz.

Beispiel: LAN1 192.168.1.1/255.255.255.0 ← vom Anwender konfiguriert.
 LAN2 192.168.1.20/255.255.255.0 ← per DHCP zugewiesen.

→ LAN1 ändern auf z.B.: 192.168.2.1/255.255.255.0

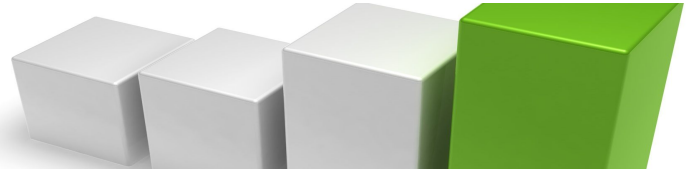


Bild 3 OpenVPN aktivieren:

CR-220N V.10

OpenVPN configuration

OpenVPN configuration	
Enable/Disable OpenVPN :	<input checked="" type="checkbox"/>
Work as :	<input type="radio"/> Server <input checked="" type="radio"/> Client
Status :	Running

OpenVPN client configuration

Server address :	<input type="text" value="83.169.44.109"/>
Protocol :	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Port :	<input type="text" value="1194"/>
VPN compression :	Enable ▾

OpenVPN certificates and keys

Authentication :	p12-Certificate ▾		
P12-certificate :	ISK-P2-NET5(10.2.132.0).p12	Info	
Import p12-certificate :	<input type="text"/>	Durchsuchen...	Import

OK **Apply** Cancel