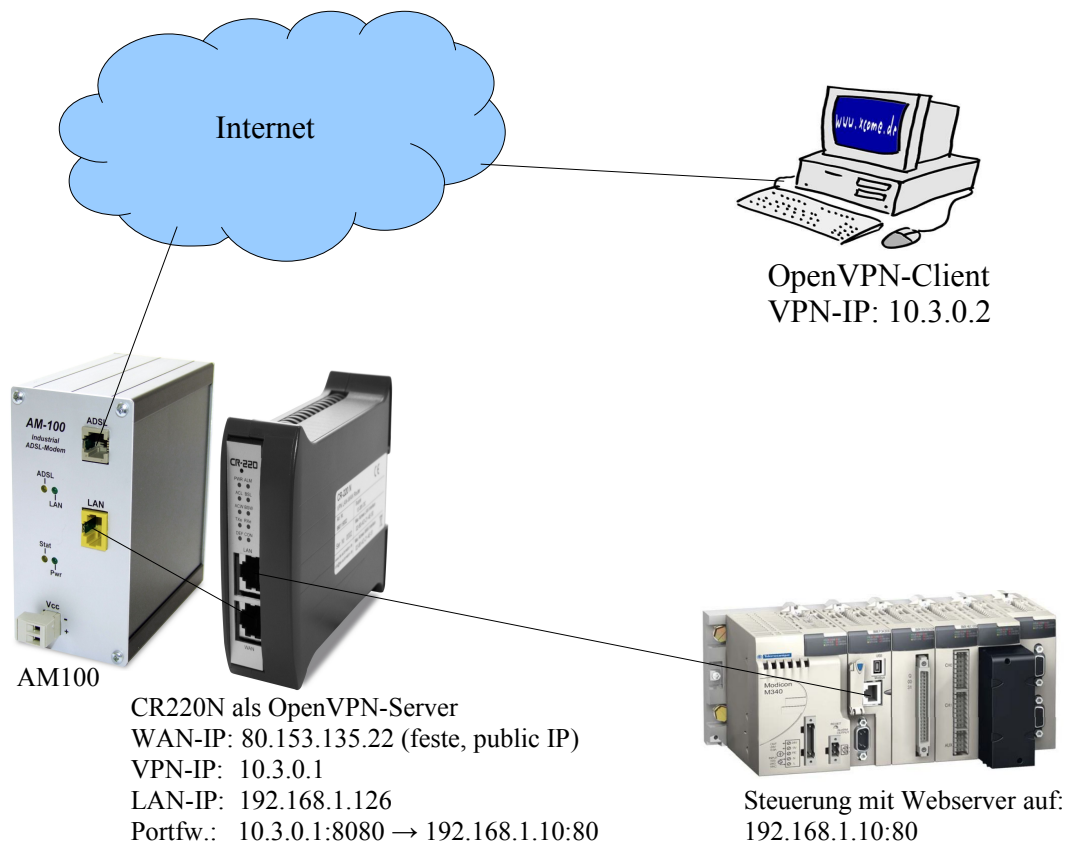


Der CR220N als OpenVPN-Server

1. Aufgabenstellung

Der VPN-Router CR220N soll als OpenVPN-Server konfiguriert werden. Für diese Betriebsart ist ein Internetzugang mit einer festen, public-IP erforderlich. Daher soll der Router in Zusammenarbeit mit dem DSL-Modem AM100 eine DSL-Verbindung zu einem Internetprovider aufbauen. Der ISP-Vertrag stellt eine feste IP-Adresse bereit. Zum Test des OpenVPN-Servers soll ein PC mit den vom CR220N erzeugten Zertifikaten ausgestattet werden und sich als OpenVPN-Client direkt in den CR220N einwählen. Der PC soll über den CR220N auf den Webserver einer Steuerung zugreifen. Dazu wird „Portforwarding“ auf dem CR220N eingerichtet.

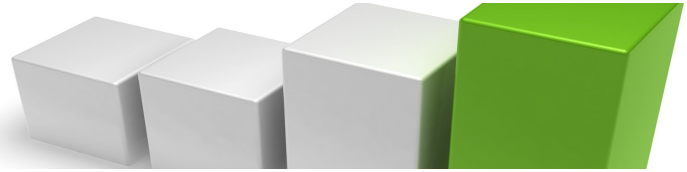
2. Netzwerkstruktur



Testzugriffe:

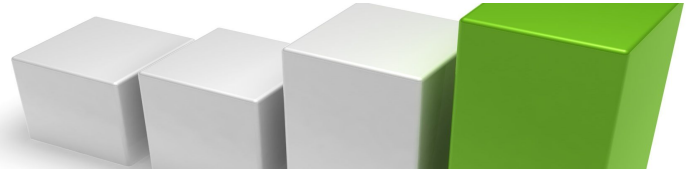
PC → CR220N: ping 10.3.0.1

PC → Steuerung: <http://10.3.0.1:8080>



3. Checkliste

1. Das mit „WAN“ bezeichnete Interface des CR220N wird mit dem DSL-Modem „AM100“ verbunden. Das mit „LAN“ bezeichnete Interface mit der Steuerung.
2. Web-Konfiguration des "CR220N" aufrufen: <http://192.168.0.126:7777>
 - login: admin
3. Werkseinstellung herstellen (siehe Bild1):
System → System management:
 - Schalter „DEFAULT“ betätigen.
 - 1 min warten.
 - login: admin
4. CR220N DSL-Interface konfigurieren (siehe Bild2)
Network → WAN:
 - DSL Enable/Disable auf „Enable“ konfigurieren.
 - Zugangsdaten zum ISP konfigurieren.
 - Connect type auf „System start, always reconnect“.
 - Apply-Schalter betätigen.
5. CR220N LAN-Interface konfigurieren:
Network → LAN → LAN1 configuration:
 - IP address: 192.168.1.126 (auf ein zur Steuerung passendes Subnetz konfigurieren).
 - Subnet mask: 255.255.255.0
 - Apply-Schalter betätigen.
6. OpenVPN-Server konfigurieren. (siehe Bild 3)
VPN → OpenVPN:
 - Enable/Disable Open VPN: aktivieren.
 - Work as: Server
 - Authentication: certificate.
 - OK-Schalter betätigen.
 - Create root CA key and certificate: zugehörigen Create-Schalter betätigen.
 - Create client key and certificate: key and cert1, zugehörigen Create-Schalter betätigen.
 - Export client1 key and certificate: Valid aktivieren.
 - Schalter „Apply“ betätigen.
 - Schalter „Root CA“ betätigen, Root-Zertifikat downloaden (Datei „ca.crt“).
 - Schalter „Key1 betätigen, Client-Key downloaden (Datei „client1.key“).
 - Schalter „Cert1 betätigen, Client-Zertifikat downloaden (Datei „client1.crt“).

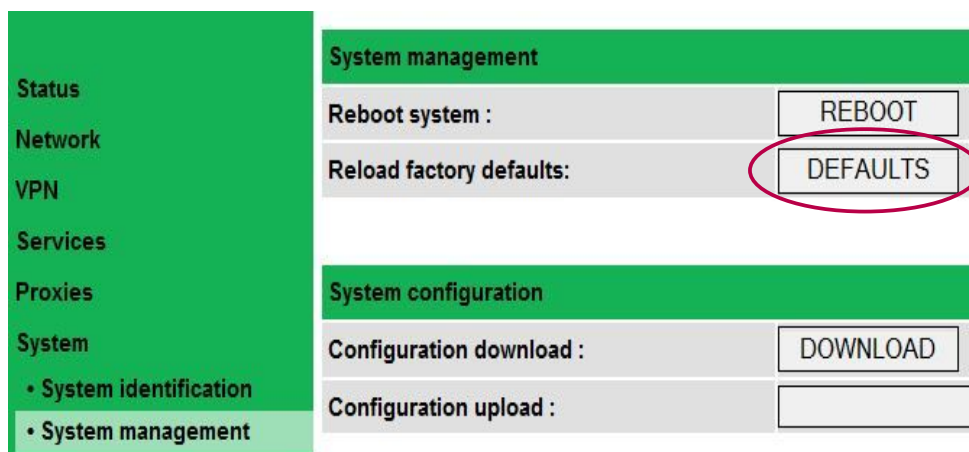


7. OpenVPN-Client-PC konfigurieren. (Bild4)
 - Alle 3 Zertifikate (ca.crt, client1.crt, client1.key) und die Datei „client1.ovpn“ in das OpenVPN-config-Verzeichnis des PCs laden. Vorher den „remote“-Parameter der Datei „client1.ovpn“ auf die feste, public-IP des OpenVPN-Servers setzen. Beispieldatei „client1.ovpn“ beachten, siehe Bild5.
8. OpenVPN-Client auf dem WIN-PC starten, client1 auswählen und nach dem Verbindungsaufbau die Verbindung zum Server testen:
 - ping 10.3.0.1
9. Portforwarding auf dem CR220N einrichten (siehe Bild 6)
Proxy → TCP:
 - Enable/Disable Proxy: aktivieren
 - Relay to: IP-Adresse der Steuerung (Zielgerät) eintragen, z.B. 192.168.1.10. Hinter dem Doppelpunkt dann die Portnummer des Dienstes auf dem Zielgerät, z.B. 80.
 - Listen on Port: Portnummer eintragen, die zur Erkennung einer Weiterleitung dienen soll, z.B. .8080.
 - Apply-Schalter betätigen.
10. Über den OpenVPN-Client-PC kann jetzt auf die Website der Steuerung zugegriffen werden. Dazu ist folgende URL im Browser einzugeben:

<http://10.3.0.1:8080>
11. Die Website der Steuerung (des Zielgerätes) meldet sich.

4. Darstellung der zugehörigen Konfigurationsseiten zu Kapitel 3

Bild 1 Werkseinstellung herstellen:



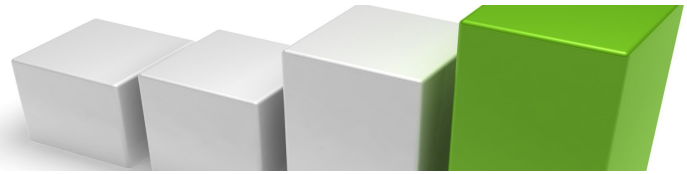


Bild 2 DSL-Interface konfigurieren:

CR-220N V.06

WAN configuration

DSL activation

DSL Enable/Disable:

ISP settings

Login name :

Password :

Confirm password :

DNS :

Gateway :

Connection settings

Connect type :

Manuell test :

Connection State : **Connected**

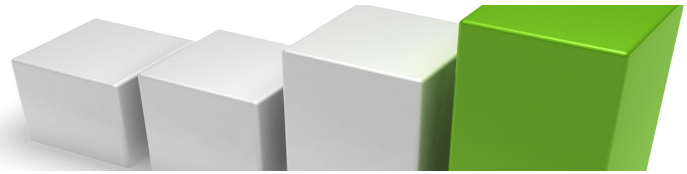


Bild 3 OpenVPN-Server konfigurieren:

CR-220N V.06

OpenVPN configuration

| | |
|--|--|
| OpenVPN configuration | |
| Enable/Disable OpenVPN : | <input checked="" type="checkbox"/> 1. |
| Work as : | <input checked="" type="radio"/> Server <input type="radio"/> Client |
| Status : | Running |
| OpenVPN server configuration | |
| Protocol : | <input checked="" type="radio"/> UDP <input type="radio"/> TCP |
| Port : | <input type="text" value="1194"/> |
| VPN compression : | Disable ▾ |
| Client mode : | Roadwarrior ▾ |
| Network : | <input type="text" value="10"/> . <input type="text" value="3"/> . <input type="text" value="0"/> . <input type="text" value="0"/> |
| Subnet mask : | <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/> |
| OpenVPN certificates and keys | |
| Authentication : | 2. Certificate ▾ |
| Root CA certificate modification : | Fri Mar 4 12:25:52 2011 Info |
| Server key modification : | Fri Mar 4 12:25:52 2011 Info |
| Server certificate modification : | Fri Mar 4 12:25:52 2011 Info |
| Diffie hellman parameters modification : | Fri Mar 4 12:25:52 2011 Info |
| OpenVPN create certificates | |
| Create root CA key and certificate : | 4. <input type="button" value="Create"/> |
| Create client key and certificate : | 5. Key and Cert 1 ▾ 6. <input type="button" value="Create"/> |
| OpenVPN export certificates | |
| Export root CA certificate : | 9. <input type="button" value="Root CA"/> Info |
| Export client 1 key and certificate : | <input checked="" type="checkbox"/> Valid 7. 10., 11. <input type="button" value="Key 1"/> <input type="button" value="Cert 1"/> Info |
| Export client 2 key and certificate : | <input type="checkbox"/> Valid <input type="button" value="Key 2"/> <input type="button" value="Cert 2"/> Info |

3.
8.

© 2010 ISK-Automation

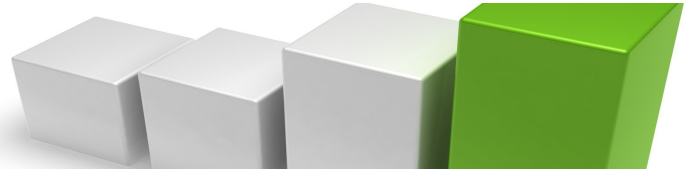


Bild 4 OpenVPN-Client konfigurieren:

| Name | Änderungsdatum | Typ | Größe |
|--------------|------------------|-----------------------|-------|
| ca.crt | 11.03.2011 20:25 | Sicherheitszertifikat | 2 KB |
| client1.crt | 11.03.2011 20:27 | Sicherheitszertifikat | 4 KB |
| client1.key | 03.03.2011 16:42 | KEY-Datei | 1 KB |
| client1.ovpn | 08.04.2011 20:43 | OpenVPN Config ... | 1 KB |

Diese 4 Dateien müssen in folgendes WIN-PC-Verzeichnis kopiert werden:

C:\Programme\OpenVPN\config

Tip: Es kann auch ein Unterverzeichnis angelegt werden und die 4 Dateien in dieses Unterverzeichnis kopiert werden. Dadurch behält man bei mehreren im PC konfigurierten VPN-Clients besser die Übersicht. Beispiel für ein solches Unterverzeichnis:

C:\Programme\OpenVPN\Config\client1

Bild 5 Inhalt der Beispieldatei client1.ovpn:

```
client1.ovpn *
client
dev tap
proto udp
resolv-retry infinite
keepalive 50 150
ca ca.crt
cert client1.crt
key client1.key
remote 80.153.135.22 1194
nobind
explicit-exit-notify 1
```

Achtung: Beachten Sie, dass hinter dem Schlüsselwort „remote“ die feste public IP Ihres CR220N eingetragen werden muss. 1194 ist die offizielle Portnummer für OpenVPN.

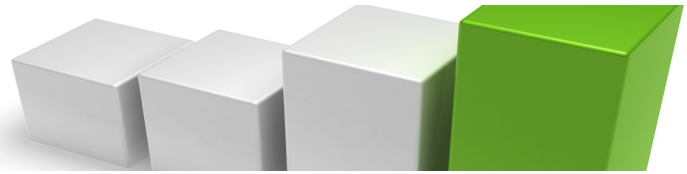


Bild 6 Portforwarding einrichten:

CR-220N V.06

Status
Network
VPN
Services
Proxies
• Web
• DNS
• Filetransfer
• TCP
System
Logout

TCP Proxy configuration

General configuration

Enable/Disable proxy :

Proxy redirections

1 redirection : TCP : **** : 8080 <=> 192.168.1.10 : 80

Create a redirection entry

Relay to : 192 . 168 . 1 . 10 : 80

Listen on port : 8080

OK Apply Cancel