

## Portforwarding-to-Subnet

### 1. Allgemeines

Im hier dargestellten Anwendungsfall sollen Teilnehmer eines Subnetzes durch Portforwarding an ein übergeordnetes Netz gekoppelt werden. Portforwarding ist zwar keine echte „Net-to-Subnet-Kopplung“ (siehe Applikationsbeispiel „Net-to-Subnet.pdf“), kann aber im Falle nur wenige Subnetz-Teilnehmer vorhanden sind und nur TCP-Verbindungen mit bekannten Portnummern zu diesen Teilnehmern geplant sind, eine ausreichende und einfache Lösung sein.

### 2. Aufgabenstellung

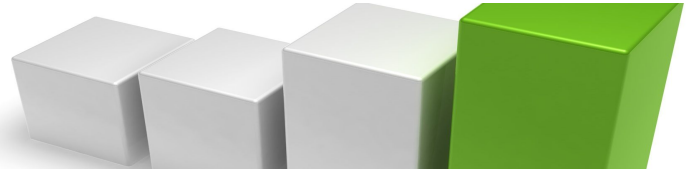
Mehrere CR220N sollen mit ihrem LAN2-Interface ein übergeordnetes Netz bilden. Auch PCs oder übergeordnete Router können Teilnehmer dieses Netzes sein. Das LAN1-Interface des CR220N soll jeweils ein vom übergeordneten Netz getrenntes Subnetz bilden.

Alle Teilnehmer des übergeordneten Netzes sollen die untergeordneten Subnetze nur durch TCP-Verbindungen erreichen können. Die Portnummern der TCP-Verbindungen sind bekannt. Andere Protokollarten, wie z.B. ICMP oder UDP sind nicht erlaubt (für andere Protokollarten dient unser Standardanwendungsfall „Net-to-Subnet.pdf“).

### 3. Lösungsprinzipien

Im CR220N lässt sich Portforwarding für bis zu 10 Teilnehmer konfigurieren. Es lassen sich also bis zu 10 Teilnehmer eines beliebigen Subnetzes an das übergeordnete Netz koppeln. Der Router benutzt einen speziellen Proxy-TCP-Server um das Portforwarding zu realisieren. Der Proxy-TCP-Server richtet selbst einen TCP-Socket ein und leitet alle Pakete, die an diesen TCP-Socket adressiert sind, zum Zielsocket weiter. Somit werden die Pakete nicht per „NAT“ verändert, sondern vom Proxy-TCP-Server empfangen und verändert an den TCP-Zielsocket weitergegeben. Das hat 2 Vorteile:

1. Der Proxy-TCP-Server empfängt Pakete aus einem übergeordneten Netz und sendet sie an ein untergeordnetes Netz weiter. Zum Weitersenden benutzt er die Router-IP des LAN1-Interfaces als Source-IP. Das Zielgerät erhält also eine Anfrage aus dem eigenen Subnet, obwohl die tatsächliche Anfrage aus dem übergeordneten Netz stammt. Somit müssen die Zielgeräte für Anfragen aus dem übergeordneten Netz kein „default Gateway“ konfigurieren. In der Praxis kommen tatsächlich immer wieder Geräte vor, die kein def. Gateway konfigurieren können.
2. Der Proxy-TCP-Server kann auch einen TCP-Socket einrichten, der https-tauglich ist und die empfangenen Pakete an einen normalen http-Webserver weitervermittelt (siehe CR220N-Menüpunkt „Proxies → Web → Web Proxy configuration“).



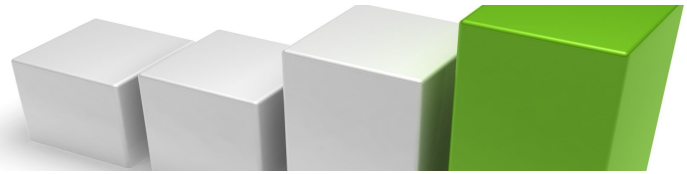
Neben dem TCP-Proxy-Server gibt es noch eine weitere Möglichkeit, Portforwarding im CR220N einzurichten, die USER-Firewall. Sie ist besonders für UDP-Pakete interessant, die sich mit einem Proxy-TCP-Server nicht weiterleiten lassen. Wir haben 2 USER-Firewall-Dateien vorbereitet:

1. „UDP\_Portforwarding.sh“ Für UDP-Portforwarding-Anwendungen.
2. „TCP\_Portforwarding.sh“ Für TCP-Portforwarding-Anwendungen, falls der Proxy-TCP-Server nicht erwünscht ist.

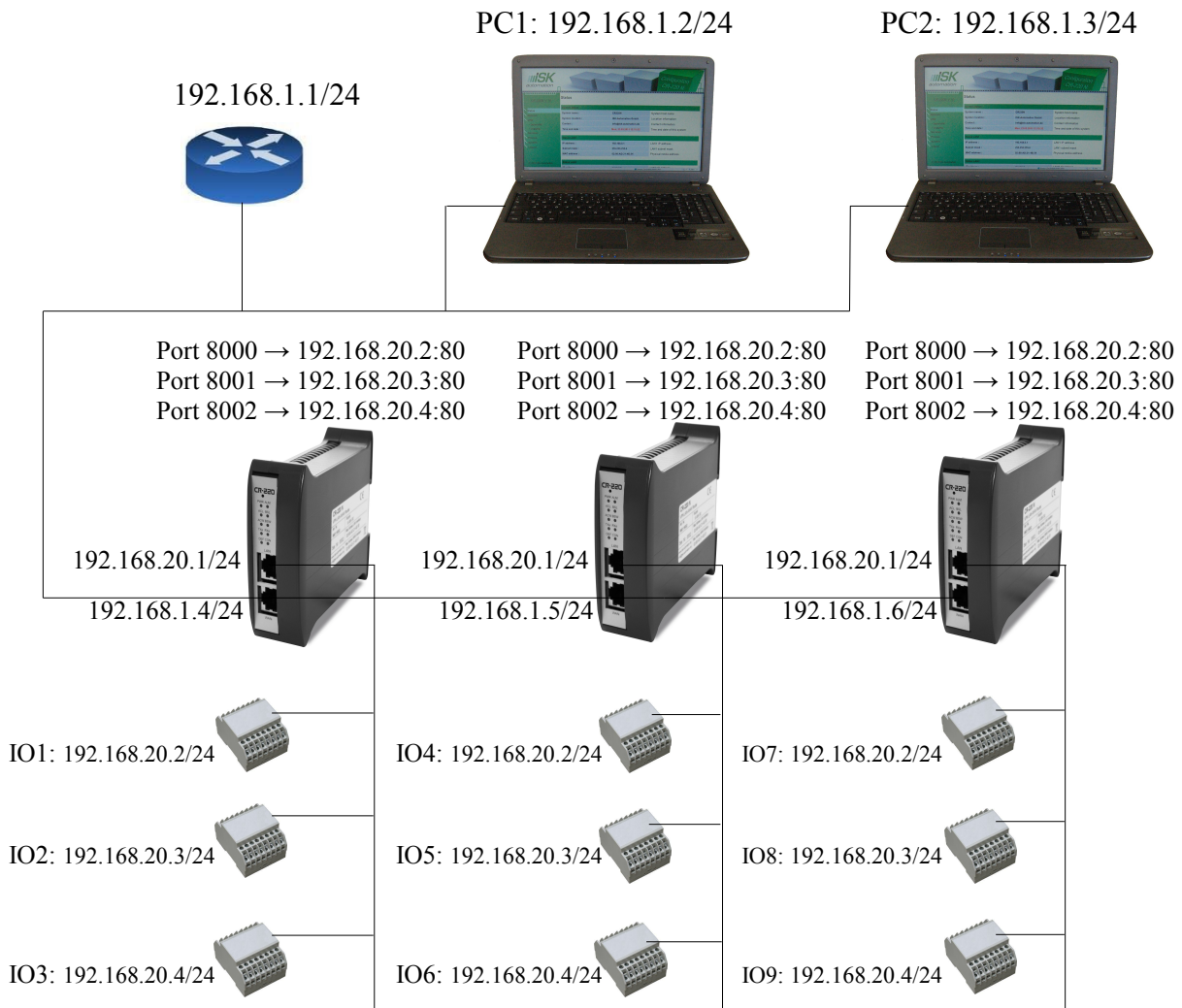
Beide Firewalls arbeiten mit DNAT und SNAT, sind also so konstruiert, dass das Zielgerät für Anfragen aus dem übergeordneten Netz ohne default Gateway auskommt. Beim Portforwarding mittels Firewall gibt es keine Beschränkung auf 10 Teilnehmer, allerdings sollte die Zahl der dort enthaltenen iptables-Regeln auch nicht Extremwerte erreichen, denn alle Regeln müssen vom Controller für jedes einzelne Netzwerkpaket abgearbeitet werden. Wie bei jeder Portforwarding-Firewall-Lösung, muss die Firewalldatei auch hier an die konkreten Portnummern und IP-Adressen der Anwendung angepasst werden, weshalb wir diese Lösung nicht als Standard-Anwendung ansehen, sondern als weitergehende Speziallösung, die mehr Freiheiten ermöglicht aber dafür spezielle Firewallkenntnisse des Anwenders voraussetzt.

Im hier beschriebenen Standard-Applikationsbeispiel soll es um Portforwarding mit dem WEB-konfigurierbaren Proxy-TCP-Server des CR220N gehen.

Sehen wir uns zuerst die Netzwerkstruktur dieses Anwendungsfalles an:



#### 4. Netzwerkstruktur zum Anwendungsfall „Portforwarding to Subnet“



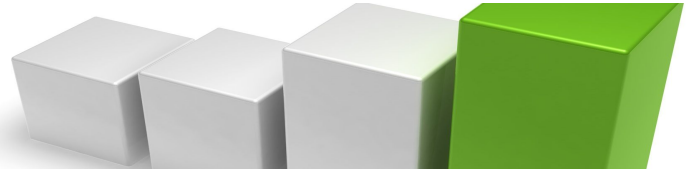
TCP-Testzugriffe vom übergeordneten Netz ins untergeordnete Subnetz:

PC1 → IO1: <http://192.168.1.4:8000>  
 PC1 → IO2: <http://192.168.1.4:8001>  
 PC1 → IO3: <http://192.168.1.4:8002>

PC1 → IO7: <http://192.168.1.6:8000>  
 PC1 → IO8: <http://192.168.1.6:8001>  
 PC1 → IO9: <http://192.168.1.6:8002>

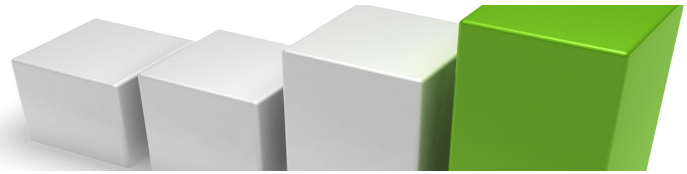
PC1 → IO4: <http://192.168.1.5:8000>  
 PC1 → IO5: <http://192.168.1.5:8001>  
 PC1 → IO6: <http://192.168.1.5:8002>

Achtung: Diese Testzugriffe (einschließlich Rückweg) sind ohne Konfiguration eines „default GW“ auf IO1 bis IO9 möglich. Es müssen auch keine speziellen „routen“ auf PC1 eingerichtet werden.



## 5. Checkliste zum Anwendungsfall „Portforwarding to Subnet“

1. Das mit "LAN" bezeichnete Interface (LAN1) wird mit dem zu koppelnden Subnet verbunden.  
Das mit "WAN" bezeichnete Interface (LAN2) wird mit dem übergeordneten Netz verbunden.  
Die Alias-Adresse kann genutzt werden, um den CR220N während der Netzwerkkonfiguration ohne Umschaltung des PC-Subnets ansprechen zu können.
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 LAN-Interface konfigurieren: (siehe Bild2)  
Network → LAN → LAN1:  
- IP address: 192.168.20.1 (Beispiel)  
- Subnet mask: 255.255.255.0  
Network → LAN → LAN2  
- Use the following IP address: aktiv  
- IP address: 192.168.1.4 (Beispiel)  
- Subnet mask: 255.255.255.0  
- Apply-Button betätigen.
5. Firewall konfigurieren: (siehe Bild3)  
Services → Firewall and NAT:  
- Enable/Disable firewall: disable  
- Button "Apply" betätigen und warten, bis die Firewall aktiviert ist.
6. TCP-Portforwarding einrichten: (siehe Bild4)  
Proxies → TCP  
- Enable/Disable proxy: aktiv  
- Relay to: 192.168.20.2 : 80  
- Listen on port: 8000  
- Apply-Button betätigen.  
- Relay to: 192.168.20.3 : 80  
- Listen on port: 8001  
- Apply-Button betätigen.  
- Relay to: 192.168.20.4 : 80  
- Listen on port: 8002  
- Apply-Button betätigen.
7. Subnet des CR220N von PC1 her ansprechen:  
Zum Test kann mit einem Web-Browser die Konfigseite der IOs gerufen werden.  
Adressdetails siehe Kapitel 4
8. fertig.



## 6. Darstellung der zugehörigen Konfigurationsseiten zu Kapitel 5

Bild 1 Werkseinstellung herstellen:

<b>Status</b> <b>Network</b> <b>VPN</b> <b>Services</b> <b>Proxies</b> <b>System</b> <ul style="list-style-type: none"> <li>• System identification</li> <li>• System management</li> </ul>	<b>System management</b>	
	Reboot system :	REBOOT
	Reload factory defaults:	DEFAULTS
	<b>System configuration</b>	
	Configuration download :	DOWNLOAD
	Configuration upload :	

Bild 2 LAN1, LAN2 konfigurieren:

<b>CR-220N V.10</b> <b>Status</b> <b>Network</b> <ul style="list-style-type: none"> <li>- WAN</li> <li>- LAN</li> <li>- COM</li> <li>- Logging</li> </ul> <b>VPN</b> <b>Services</b> <b>Proxies</b> <b>System</b> <b>Logout</b>  © 2010 ISK-Automation	<b>LAN configuration</b>	
	<b>LAN1 configuration</b>	
	Enable/Disable interface LAN1 :	<input checked="" type="checkbox"/>
	DHCP-client :	<input type="radio"/>
	Use the following IP address :	<input checked="" type="radio"/>
	IP address :	192 . 168 . 20 . 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
	<b>LAN2 configuration</b>	
	Enable/Disable interface LAN2 :	<input checked="" type="checkbox"/>
	Use device for DSL :	<input type="radio"/>
	DHCP-client :	<input type="radio"/>
	Use the following IP address :	<input checked="" type="radio"/>
	IP address :	192 . 168 . 1 . 4
	Subnet mask :	255 . 255 . 255 . 0
	<b>DNS configuration</b>	
	Use a DNS server address :	<input type="checkbox"/>
	<b>Default gateway configuration</b>	
Use a gateway address :	<input type="checkbox"/>	
OK <b>Apply</b> Cancel		

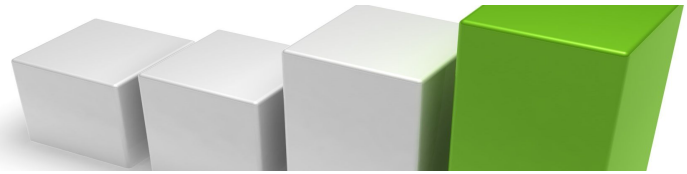


Bild 3 Firewall konfigurieren:

CR-220N V.10

**Firewall and NAT configuration**

Firewall configuration

Enable/Disable firewall :

Firewall and NAT rules script

Show current settings :

Upload and restart done. Firewall is **Off!**

Bild 4 TCP-Portforwarding einrichten:

CR-220N V.10

**TCP Proxy configuration**

General configuration

Enable/Disable proxy :

Proxy redirections

1 redirection : TCP :	**** : 8000 <=> 192.168.20.2 : 80
2 redirection : TCP :	**** : 8001 <=> 192.168.20.3 : 80

Create a redirection entry

Relay to :  .  .  .  :

Listen on port :