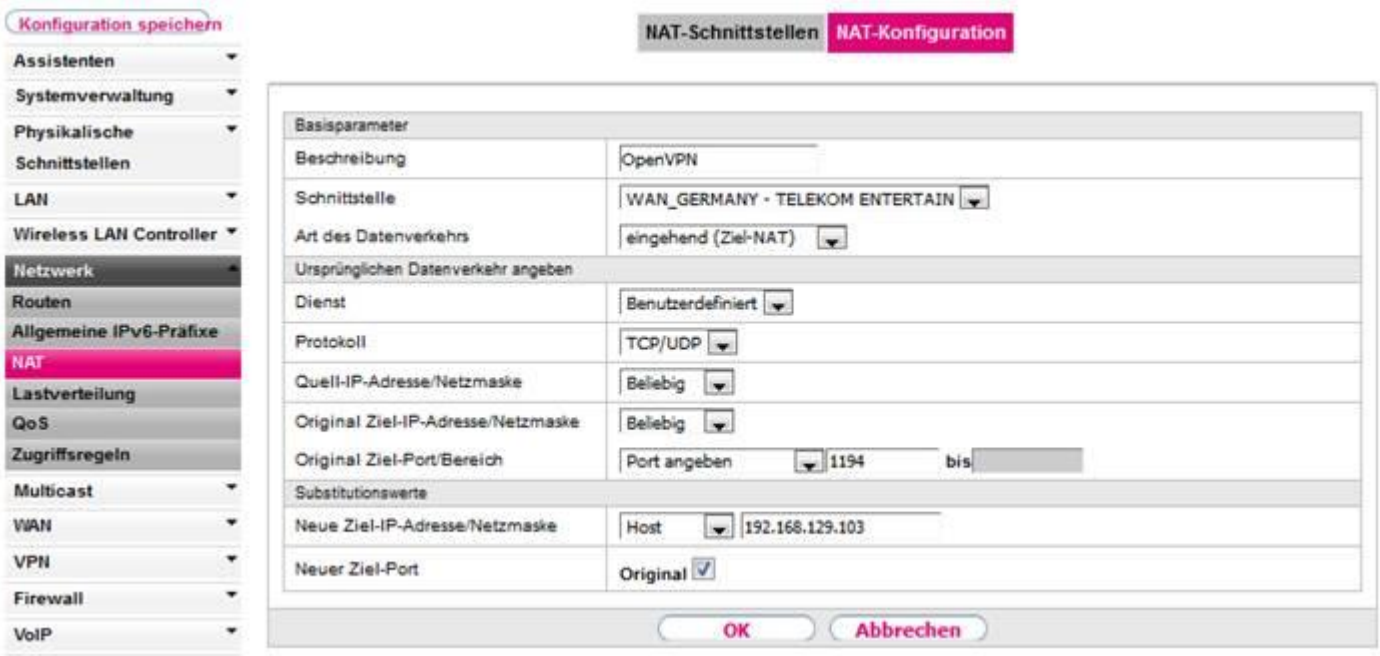
Um bei einer Digitalisierungsbox OpenVPN Verbindungen eingehend aus dem WAN zum VPN-Server zu erlauben, benötigen Sie 2 Konfigurationsschritte:

- NAT Portforwarding
- Firewallregel, die den Zugriff aus dem WAN auf den VPN-Server im LAN erlaubt

Die folgenden Screenshots beziehen sich auf die Softwareversion 10. 1 Rev. 3 und sind für alle Patchlevel gültig. Von einer gültigen Adresslage im LAN und der Verwendung der Digitalisierungsbox als Standardgateway beim VPN-Server gehe ich aus.

NAT Portforwarding:
Gehen Sie in das Menü
Netzwerk – NAT, Registerkarte „NAT-Konfiguration“
und erstellen mit „NEU“ einen neuen Eintrag, der bei der beschriebenen Konstellation etwa so aussehen sollte:



Nach der Bestätigung mit „OK“ finden Sie in der Übersicht zwei neue Einträge, einen für TCP und einen für UDP. Beides steht bei OpenVPN ja zur Auswahl.

Firewall:
Um keine pauschalen Freigaben in den Firewallregeln vorzunehmen zu müssen, definieren Sie bitte zuerst jeweils einen Alias für die IP-Adresse des OpenVPN-Server und für den benutzten Dienst. Damit kann im letzten Schritt die Regel definiert werden, die nur diesen Dienst zu dieser IP-Adresse als initiale Anfrage eingehend erlaubt. Der Rest wir nach wie vor geblockt.
Für den Alias der IP-Adresse des Servers gehen Sie zu
Firewall – Adressen, Registerkarte „Adressliste“ -> „Neu“
und legen ihn entsprechend an. Beachten Sie, dass für nur diese eine Adresse das Subnetz 255.255.255.255 (/32) einzutragen ist.

Den Alias für den Dienst legen Sie an unter
Firewall – Dienste, Registerkarte „Diensteliste“ -> „Neu“

Als letzten Schritt erstellen Sie unter
Firewall – Richtlinien, Registerkarte „IPv4-Filterregeln“ -> „Neu“
mit Hilfe der vorher erstellten Aliasse die entsprechende Regel:

Testen Sie jetzt eine eingehende VPN-Verbindung aus dem WAN (nicht aus dem eigenen LAN) und speichern bei Erfolg die vorgenommene Konfiguration

Konfiguration speichern