

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:

Basisparameter	
Beschreibung	OpenVPN
Schnittstelle	WAN_GERMANY - TELEKOM ENTERTAIN
Art des Datenverkehrs	eingehend (Ziel-NAT)
Ursprünglichen Datenverkehr angeben	
Dienst	Benutzerdefiniert
Protokoll	TCP/UDP
Quell-IP-Adresse/Netzmaske	Beliebig
Original Ziel-IP-Adresse/Netzmaske	Beliebig
Original Ziel-Port/Bereich	Port angeben 1194 bis
Substitutionswerte	
Neue Ziel-IP-Adresse/Netzmaske	Host 192.168.129.103
Neuer Ziel-Port	Original <input checked="" type="checkbox"/>

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 wird 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.

Konfiguration speichern

Assistenten
Systemverwaltung
Physikalische Schnittstellen
LAN
Wireless LAN Controller
Netzwerk
Multicast
WAN
VPN
Firewall
Richtlinien
Schnittstellen
Adressen
Dienste

Adressliste Gruppen

Basisparameter	
Beschreibung	VPN-Server
IPv4	<input checked="" type="checkbox"/> Aktiviert
Adresstyp	<input checked="" type="radio"/> Adresse/Subnetz <input type="radio"/> Adressbereich
Adresse/Subnetz	192.168.129.103 255.255.255.255
IPv6	<input type="checkbox"/> Aktiviert

OK Abbrechen

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

Konfiguration speichern

Assistenten
Systemverwaltung
Physikalische Schnittstellen
LAN
Wireless LAN Controller
Netzwerk
Multicast
WAN
VPN
Firewall
Richtlinien
Schnittstellen
Adressen
Dienste

Dienstliste Gruppen

Basisparameter	
Beschreibung	OpenVPN
Protokoll	UDP/TCP
Zielportbereich	1194 1194
Quellportbereich	0 1 <input checked="" type="checkbox"/> Nicht beachten

OK Abbrechen

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

Konfiguration speichern

Assistenten
Systemverwaltung
Physikalische Schnittstellen
LAN
Wireless LAN Controller
Netzwerk
Multicast
WAN
VPN
Firewall
Richtlinien
Schnittstellen

IPv4-Filterregeln IPv6-Filterregeln Optionen

Basisparameter	
Quelle	WAN_GERMANY - TELEKOM ENTERTAIN
Ziel	VPN-Server
Dienst	OpenVPN
Aktion	Zugriff

OK Abbrechen

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

Konfiguration speichern