Hochverfügbare Firewall mit OPNsense für Filialen mit schlechter Erreichbarkeit

Nicht jeder Kunde hat gut erreichbare Außenstellen. Oft sind die Räume nicht besetzt oder die Kollegen wenig kooperativ.

Dazu kommt miserables Internet, z. B. Router mit LTE, Carrier graded NAT und IP 4/6 Umsetzung.

Filialen haben oft kein von außen erreichbares Internet

Daher unsere Ziele

- Schelle Firewall mit Schutz der Anwender **#opnsense #hardware**
- Spiegelung der SSDs mit ZFS #zpool #zfs **#raid1**
- Einfaches und schnelles VPN das ausgehend aufbaut **#wireguard**
- Zweites VPN zum Dienstleister für Notfälle **#openvpn**
- Zweite Internetverbindung gegen Ausfälle deren Funktion immer geprüft ist **#dhcp #nat #cgn #ip6to4**
- Zweite Hardware die bei Ausfall einspringt #ha **#opnsense #carp #pfsync**
- Administration und Monitoring vom Dienstleister über Hintertür VPN **#check_mk #bashclub**

Wir starten mit einer OPNsense Installation wie z. B. bei Thomas Krenn erklärt

https://www.thomas-krenn.com/de/wiki/OPNsense_installieren

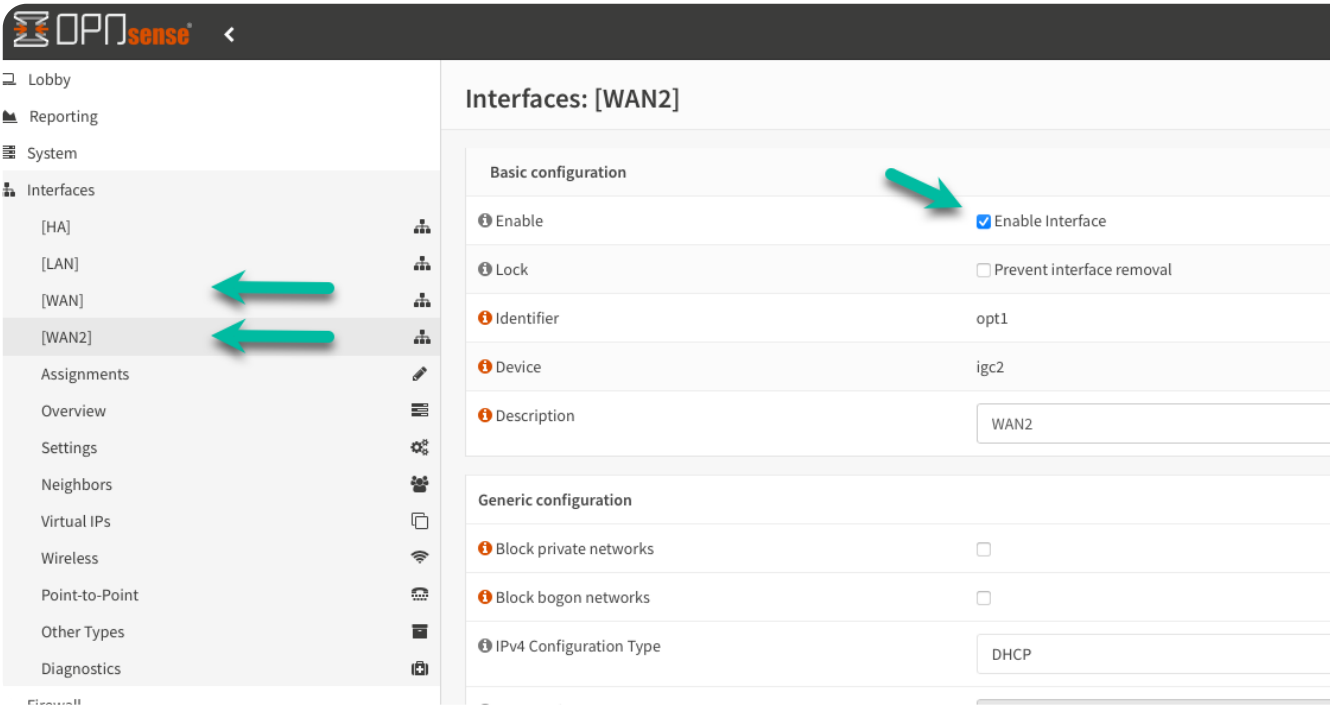
Hardware sind wie hier sehr flexibel

Gute Erfahrungen hiermit gemacht

https://amzn.to/3wgE0JX

Bessere Hardware gibt natürlich bei Thomas-Krenn und Servershop24, bitte direkt bei uns anfragen

Wir werden zwei WAN Interface konfigurieren, am Beispiel der Installation mit DHCP auf WAN

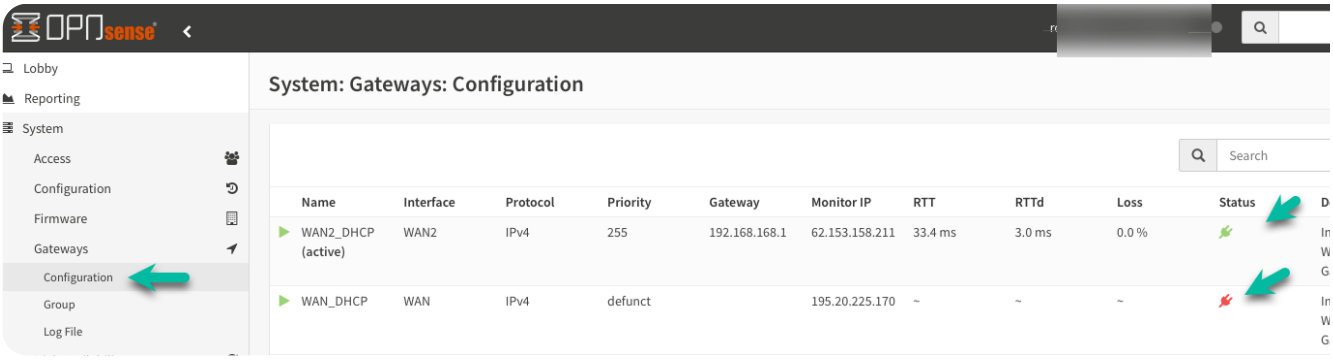


Für das ausgehende Surfen und VPN brauchen wir ein MultiWAN Setup. Grundlagen hier

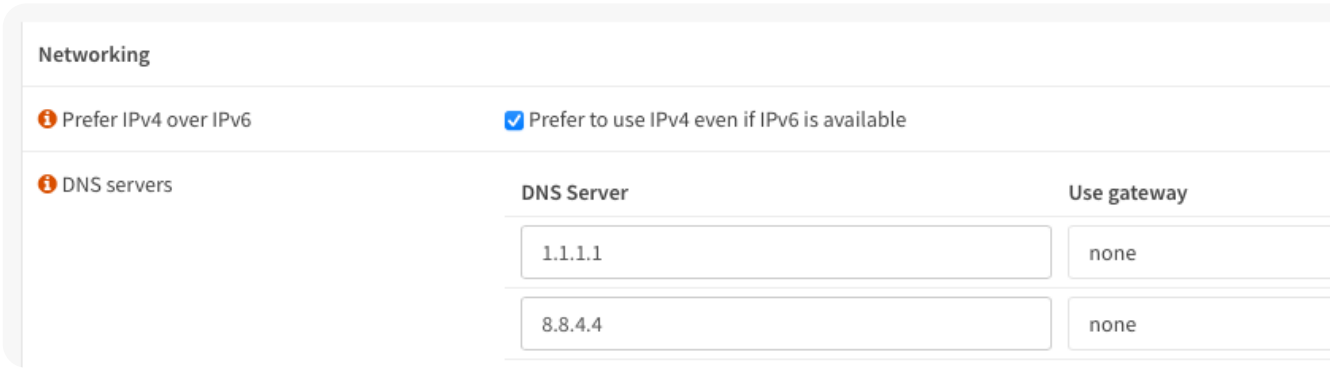
https://docs.opnsense.org/manual/how-tos/multiwan.html

Endlich merken wir wenn z. B. von zwei LTE Routern einer offline ist

Wichtig: Monitoring IP darf nicht mit den lokalen DNS Servern übereinstimmen, da diese sonst falsch geroutet werden.



Wichtig: Bei DHCP Internet, nicht den Provider DNS übernehmen!



DNS server options | Allow DNS server list to be overridden by DHCP/PPP on W

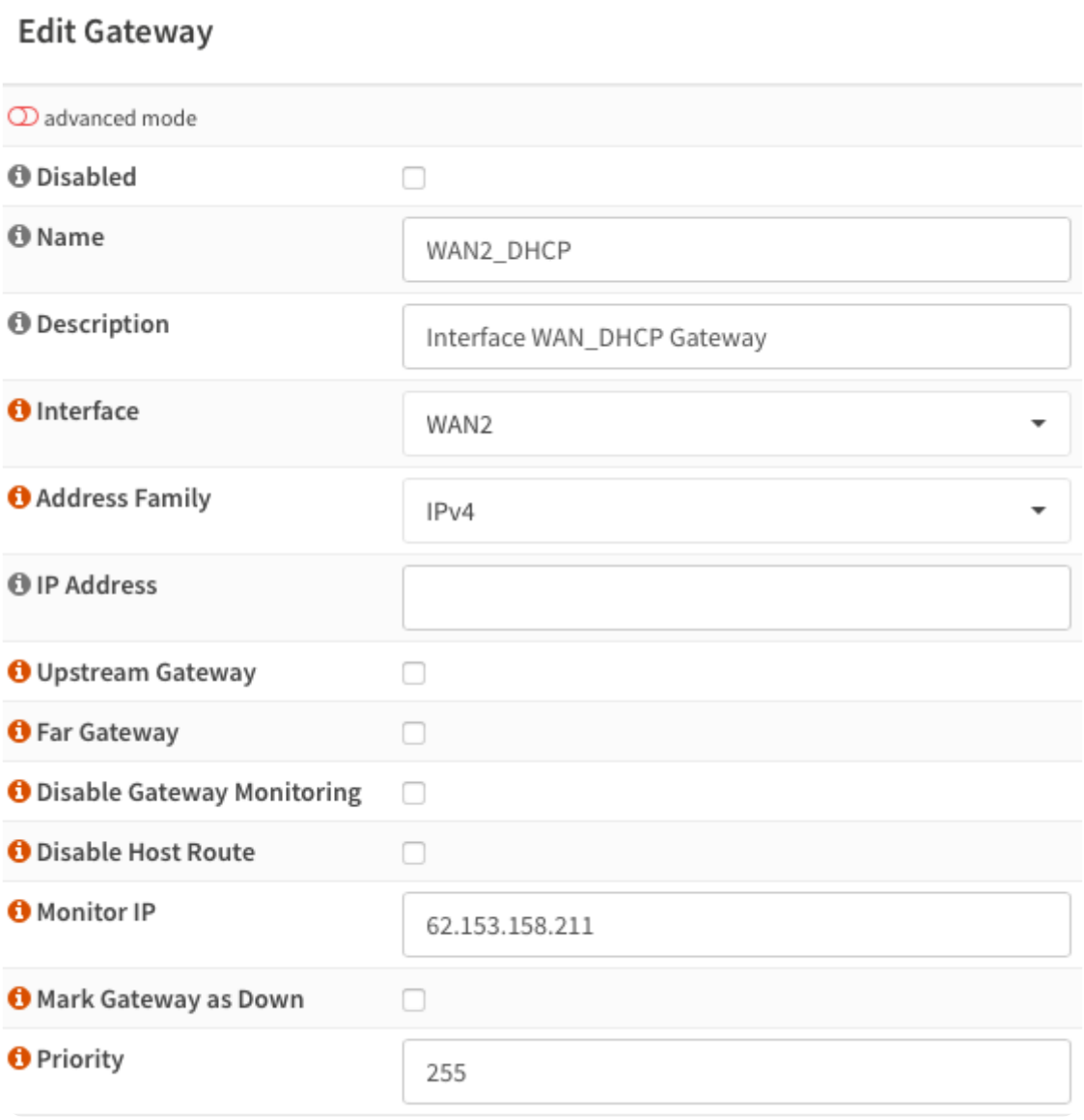
Gatways anpassen

Edit Gateway

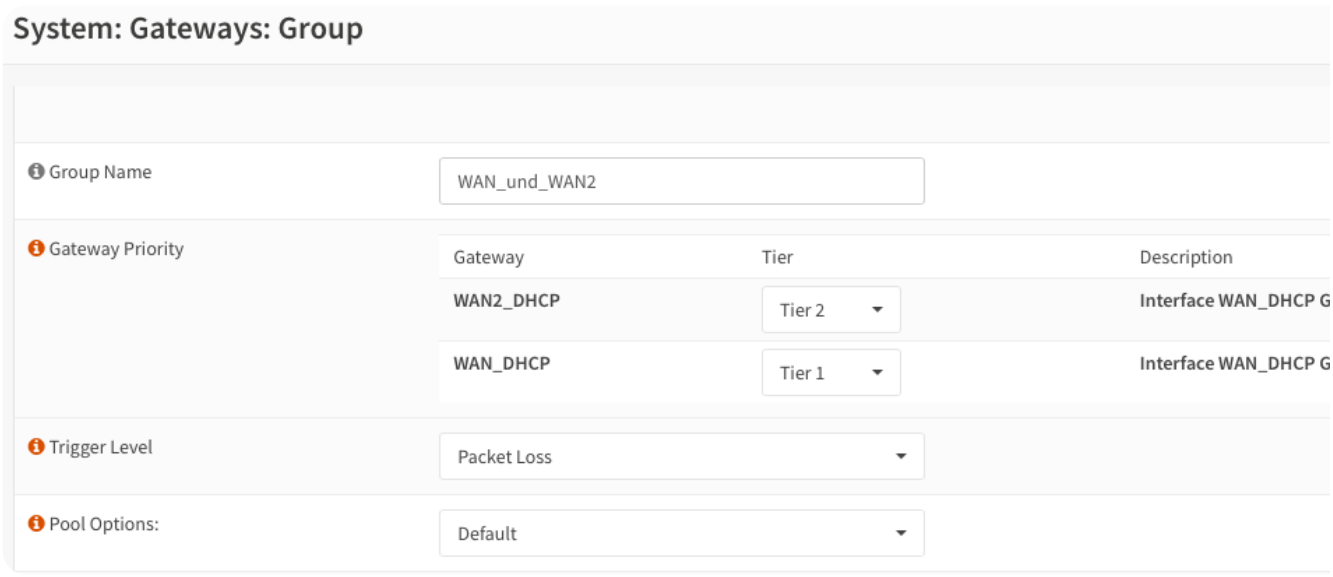
advanced mode

Disabled	☐
Name	WAN_DHCP
Description	Interface WAN_DHCP Gateway
Interface	WAN
Address Family	IPv4
IP Address	
Upstream Gateway	☐
Far Gateway	☐
Disable Gateway Monitoring	☐
Disable Host Route	☐
Monitor IP	195.20.225.170
Mark Gateway as Down	☐
Priority	1





Priorität eventuell nach Leistung der Leitungen oder Volumen setzen



Jetzt gehts um die Hochverfügbarkeit beider Maschinen, eine Anleitung findet sich hier

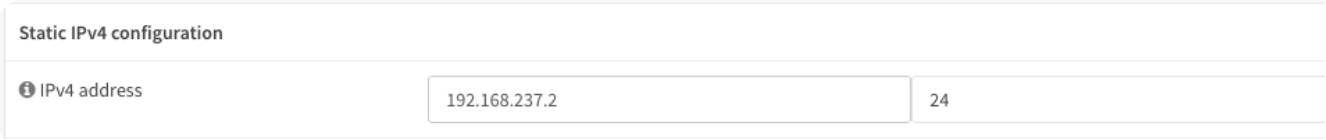
https://docs.opnsense.org/manual/hacarp.html#workflow

Damit die beiden Systeme für die Anwender immer erreichbar sind, nutzen wir CARP für eine gemeinsame IP.

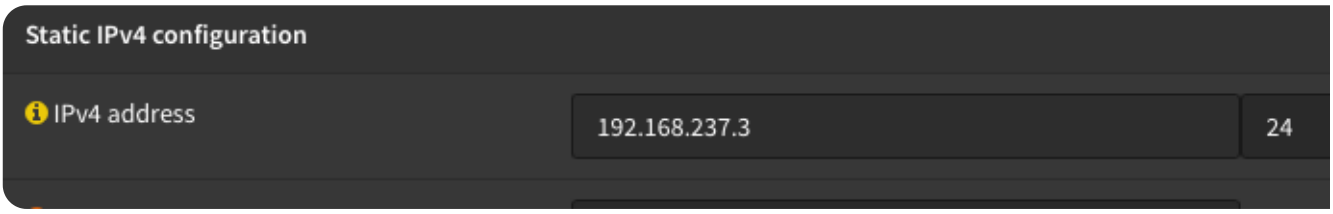
Jedes System erhält eine weitere LAN IP Adresse für Updates, Management, Monitoring, etc.

Die States und die Konfiguration wird **teilweise** auf die zweite Firewall übertragen.

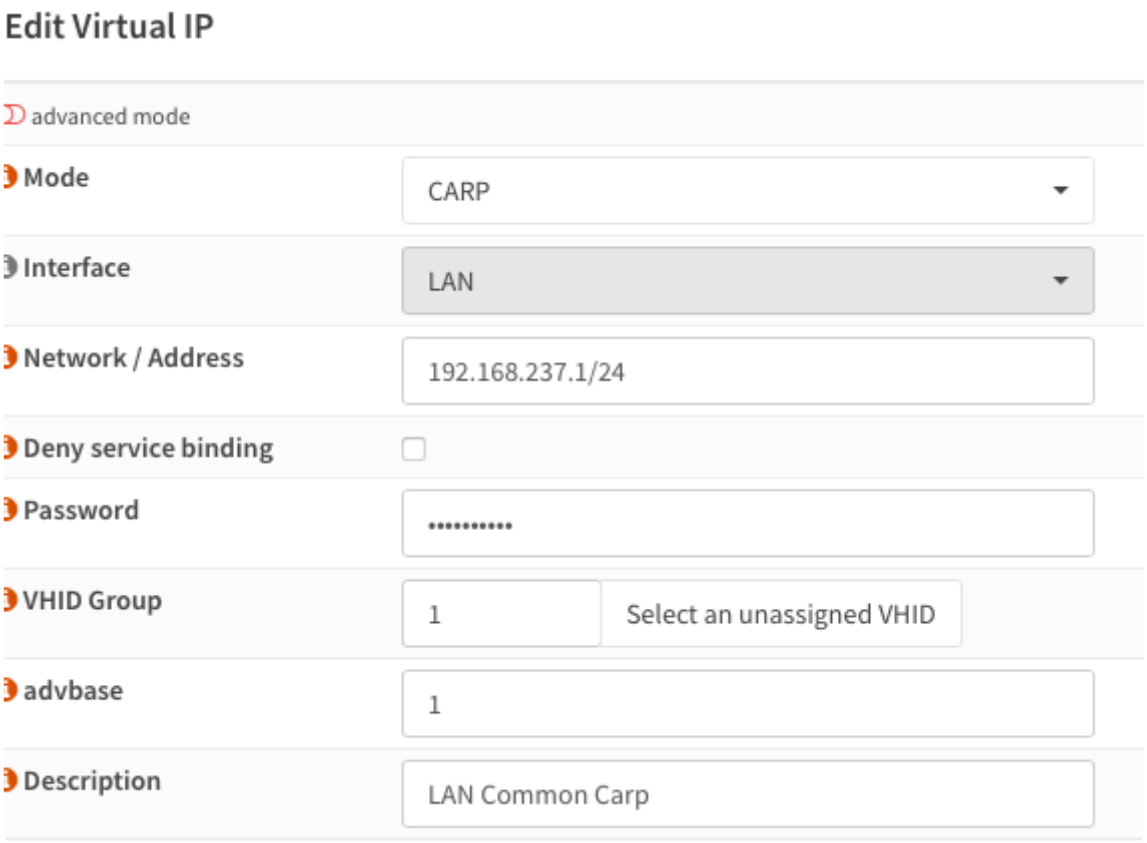
Firewall 1



Firewall 2 (Dunkles Theme hilft zum Unterscheiden)



Beide Firewalls



DHCP nicht die Failover vergessen:

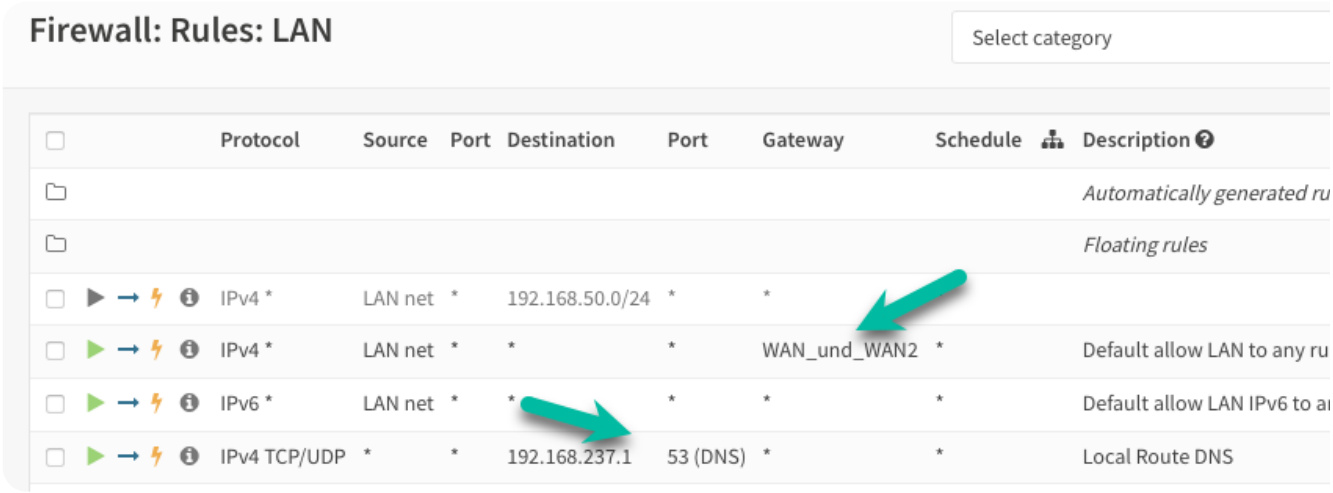
Failover peer IP:	Zweite Sense

Folgende Einstellungen werden zwischen beiden Firewalls gesynct, diverse sind pro System individuell geregelt.

Dashboard, Users, Certificates, DHCP, Virtual IPs, Static Routes, Network Time, Cron, Tunables, Web GUI, SSH, alles mit Firewall, Aliase, NAT, ID, DNS, Wireguard

Nicht syncen werden wir OpenVPN, da diese Tunnel das verwalten aus fremden Netzen ermöglichen.

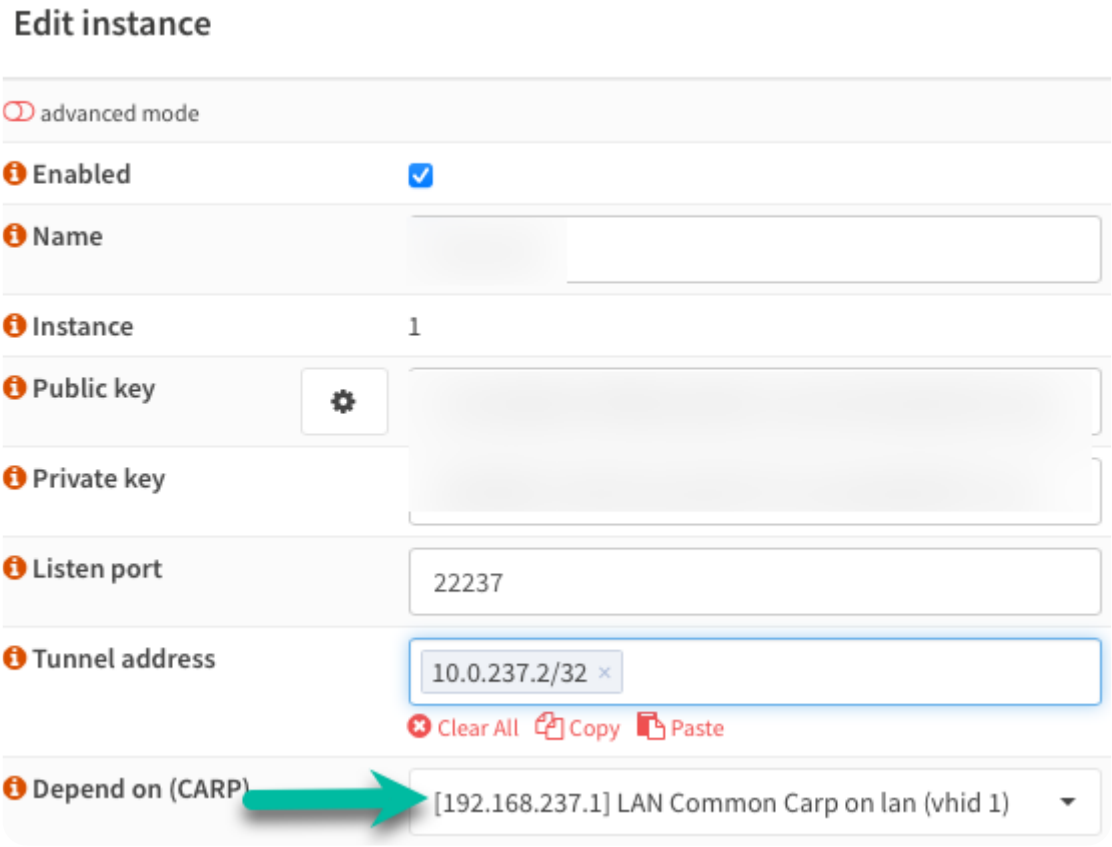
Firewall Regel müssen die Multi WAN berücksichtigen



Die Verbindung zur Zentrale erfolgt via Wireguard VPN, unser Tool erleichert die Einrichtung

https://github.com/bashclub/wg-config

Wireguard wird nun an das Carp LAN Interface gebunden, so kommt es nicht zu doppeltem Aufbau des VPNs



Erfahrungsgemäß baut bei Hardwareausfall oder WAN Wechsel das VPN unter fünf Sekunden neu auf!

Für Hintertüre nehmen wir OpenVPN und bauen ein Setup wie für einen Roadwarrior auf der Seite des

IT Dienstleister

Erstelle eine CA

Erstelle ein Server Zertifikat mit dieser CA

Erstelle pro OPNsense ein Client Zertifikat

Dann erstelle einen Open VPN Server und vergiss nicht den Port auf deiner Firewall freizugeben

VPN: OPENVPN: SERVERS

General information

Disabled	☐
Description	
Server Mode	Remote Access (SSL/TLS)
Protocol	UDP
Device Mode	tun
Interface	any
Local port	1207

Cryptographic Settings

TLS Authentication	Enabled - Authentication only
TLS Shared Key	
Peer Certificate Authority	
Peer Certificate Revocation List	
Server Certificate	nsen_Server sen_CA) *In Use
Encryption algorithm (deprecated)	None
Auth Digest Algorithm	SHA512 (512-bit)

Dieser Key wird automatisch erstellt und muss dann auch auf die Client Seite

CA und Zertifikat wurden auf Server vom Dienstleister erstellt

Das VPN für die Filialsysteme einfach exportieren, pro System ein Zertifikat, wichtig!

Öffne die .ovpn Datei

Auf der Filiale unter Authorities das Public CA Zertifikat importieren

- <ca>
  -----BEGIN CERTIFICATE-----
- Inhalt
- -----END CERTIFICATE-----

Das Zertifikat erscheint nun unter Authorities

Das Selbe gilt für den Import des Client Zertifikat und seinem Schküssel

- -----BEGIN PRIVATE KEY-----
- Inhalt
- -----END PRIVATE KEY-----

Jetzt können wir das Client VPN einrichten

VPN: OpenVPN: Clients [legacy]

General information

Disabled	☐
Description	sysops
Server Mode	Peer to Peer (SSL/TLS)
Protocol	UDP
Device mode	tun
Interface	any
Remote server	Host or address: opnrz.sysops.de — Port: 12(
	☐ Select remote server at random
Retry DNS resolution	☐ Infinitely resolve remote server
Proxy host or address	
Proxy port	
Proxy authentication extra options	Authentication method: none
Local port	

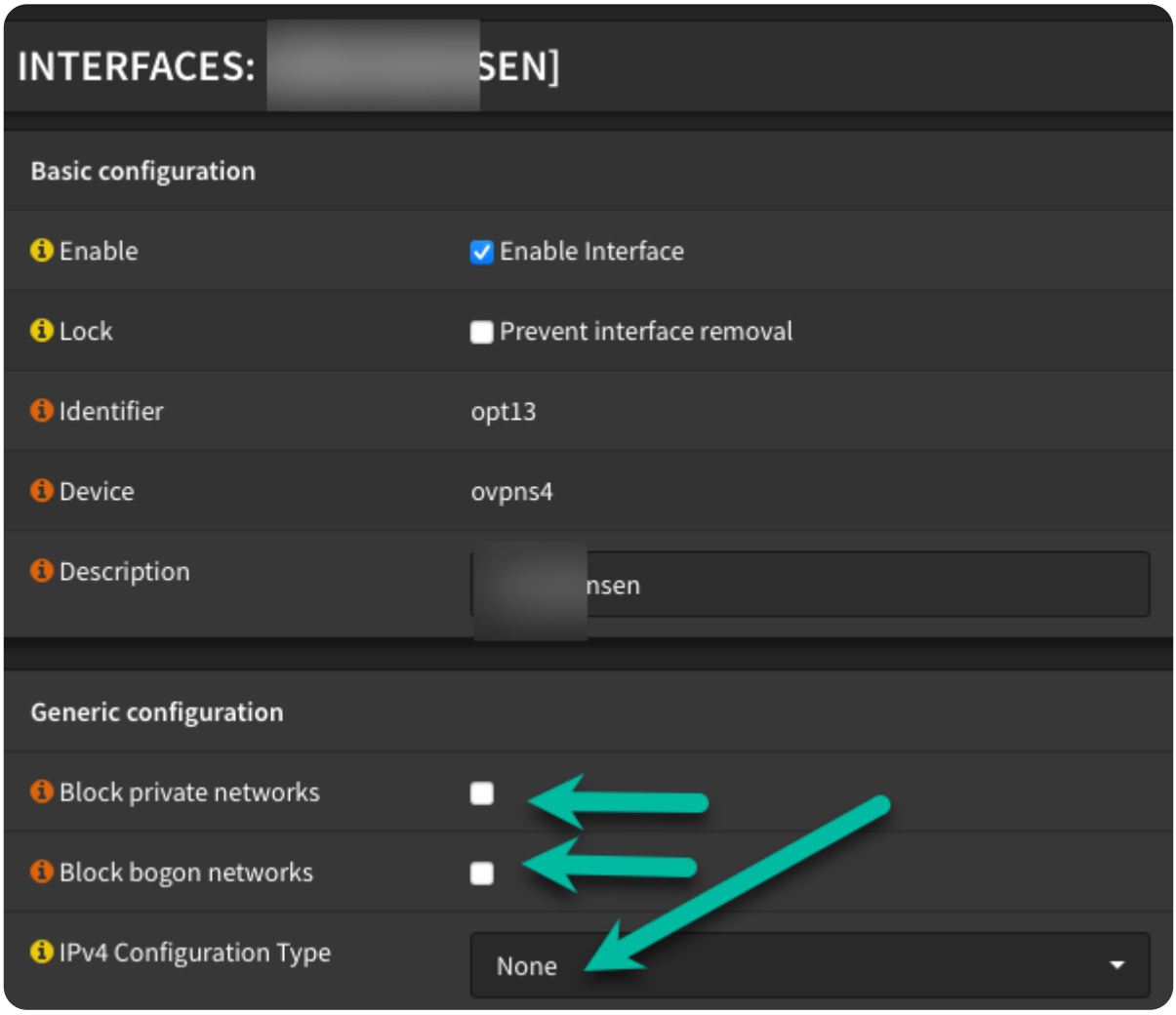
User Authentication Settings

User name/pass	Username
	Password
Renegotiate time	

Cryptographic Settings

TLS Authentication	Enabled - Authentication only
TLS Shared Key	

Damit wir am Ende aus dem Dienstleister Netz Zugreifen können, erstellen wir noch ein unkonfiguriertes Interface auf der Server Firewall

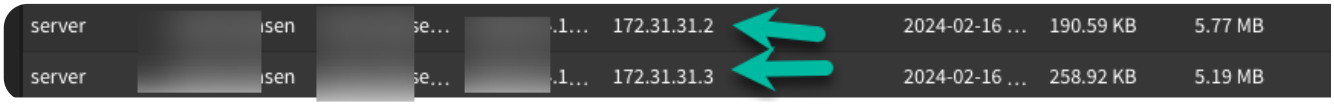


Wir empfehlen noch unser Check_MK Plugin von Nils

https://github.com/bashclub/checkmk-opnsense-agent

Die IP Adressen der Sensen erfahren wir hier

VPN: OPENVPN: CONNECTION STATUS



Glückwunsch du hast nun die perfekte Außenstellenfirewall

Version #7
Erstellt: 2024-02-16 14:20:48 UTC von Christian Zengel (sysops GmbH)
Zuletzt aktualisiert: 2024-02-18 11:05:04 UTC von Christian Zengel (sysops GmbH)