

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

Interfaces: [WAN2]

Basic configuration

- ☒ Enable
- ☐ Lock
- ☐ Prevent interface removal
- Identifier: opt1
- Device: igc2
- Description: WAN2

Generic configuration

- ☐ Block private networks
- ☐ Block bogon networks
- IPv4 Configuration Type: DHCP

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.

System: Gateways: Configuration

Name	Interface	Protocol	Priority	Gateway	Monitor IP	RTT	RTTd	Loss	Status	Description
WAN2_DHCP (active)	WAN2	IPv4	255	192.168.168.1	62.153.158.211	33.4 ms	3.0 ms	0.0 %		Interface WAN_DHCP Gateway
WAN_DHCP	WAN	IPv4	defunct		195.20.225.170	~	~	~		Interface WAN_DHCP Gateway

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

Networking


☒ Prefer IPv4 over IPv6














DNS servers


DNS Server	Use gateway
1.1.1.1	none
8.8.4.4	none

Gatways anpassen

Edit Gateway

 advanced mode

 Disabled	<input type="checkbox"/>
 Name	<input type="text" value="WAN_DHCP"/>
 Description	<input type="text" value="Interface WAN_DHCP Gateway"/>
 Interface	<input type="text" value="WAN"/>
 Address Family	<input type="text" value="IPv4"/>
 IP Address	<input type="text"/>
 Upstream Gateway	<input type="checkbox"/>
 Far Gateway	<input type="checkbox"/>
 Disable Gateway Monitoring	<input type="checkbox"/>
 Disable Host Route	<input type="checkbox"/>
 Monitor IP	<input type="text" value="195.20.225.170"/>
 Mark Gateway as Down	<input type="checkbox"/>
 Priority	<input type="text" value="1"/>



Edit Gateway

advanced mode

Disabled

☐

Name

WAN2_DHCP

Description

Interface WAN_DHCP Gateway

Interface

WAN2

Address Family

IPv4

IP Address

Upstream Gateway

☐

Far Gateway

☐

Disable Gateway Monitoring

☐

Disable Host Route

☐

Monitor IP

62.153.158.211

Mark Gateway as Down

☐

Priority

255

Priorität eventuell nach Leistung der Leitungen oder Volumen setzen

System: Gateways: Group

Group Name

WAN_und_WAN2

Gateway Priority

Gateway	Tier	Description
WAN2_DHCP	Tier 2	Interface WAN_DHCP Gateway
WAN_DHCP	Tier 1	Interface WAN_DHCP Gateway

Trigger Level

Packet Loss

Pool Options:

Default

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.

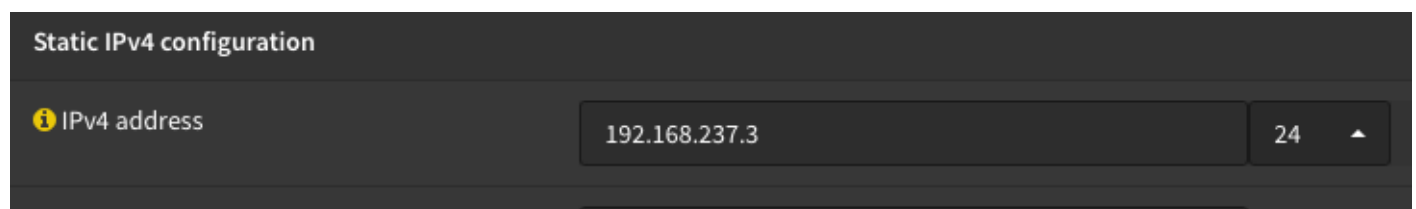
Die States und die Konfiguration wird **teilweise** auf die zweite Firewall übertragen.

Firewall 1



Static IPv4 configuration	
IPv4 address	192.168.237.2 24

Firewall 2 (Dunkles Theme hilft zum Unterscheiden)



Static IPv4 configuration	
IPv4 address	192.168.237.3 24

Beide Firewalls

Edit Virtual IP

advanced mode	
Mode	CARP
Interface	LAN
Network / Address	192.168.237.1/24
Deny service binding	<input type="checkbox"/>
Password	*****
VHID Group	1 Select an unassigned VHID
advbase	1
Description	LAN Common Carp

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

Firewall: Rules: LAN									
Select category									
<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description ?
	Automatically generated rules								
	Floating rules								
<input type="checkbox"/>	IPv4 *	LAN net	*	192.168.50.0/24	*	*			
<input type="checkbox"/>	IPv4 *	LAN net	*	*	*	WAN_und_WAN2	*		Default allow LAN to any rule
<input type="checkbox"/>	IPv6 *	LAN net	*	*	*	*	*		Default allow LAN IPv6 to any rule
<input type="checkbox"/>	IPv4 TCP/UDP	*	*	192.168.237.1	53 (DNS)	*	*		Local Route DNS

Die Verbindung zur Zentrale erfolgt via Wireguard VPN, unser Tool erleichtert 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

Edit instance

☐ advanced mode

Enabled ☒

Name

Instance 1

Public key

Private key

Listen port

Tunnel address

Clear All
 Copy
 Paste

Depend on (CARP)

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

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

❗ Peer Certificate Authority

❗ Peer Certificate Revocation List

**CA und Zertifikat wurden auf
Server vom Dienstleister erstellt**

❗ Server Certificate

nsen_Server (nsen_CA) *In Use

❗ Encryption algorithm
(deprecated)

None

❗ Auth Digest Algorithm

SHA512 (512-bit)

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 Schlüssel

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

Jetzt können wir das Client VPN einrichten

VPN: OpenVPN: Clients [legacy]

General information

i Disabled

☐

i Description

sysops

i Server Mode

Peer to Peer (SSL/TLS)

i Protocol

UDP

i Device mode

tun

i Interface

any

i Remote server

Host or address

Port

opnrz.sysops.de

☐ Select remote server at random

i Retry DNS resolution

☐ Infinitely resolve remote server

i Proxy host or address

i Proxy port

i Proxy authentication extra options

Authentication method

none

i Local port

User Authentication Settings

i User name/pass

Username

Password

i Renegotiate time

Cryptographic Settings

i TLS Authentication

Enabled - Authentication only

i TLS Shared Key

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

INTERFACES:

SEN]

Basic configuration

Enable

☒ Enable Interface

Lock

☐ Prevent interface removal

Identifier

opt13

Device

ovpns4

Description

nsen

Generic configuration

Block private networks

☐

Block bogon networks

☐

IPv4 Configuration Type

None

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

server	nsen	se...	.1...	172.31.31.2	2024-02-16 ...	190.59 KB	5.77 MB	ok
server	nsen	se...	.1...	172.31.31.3	2024-02-16 ...	258.92 KB	5.19 MB	ok

Glückwunsch du hast nun die perfekte Außenstellenfirewall