Kopie OPNSense Workshop - Vorumstellung auf markdown

Inhaltsverzeichnis

3. OpenVPN Einwahl - Roadwarrior
4. Bridges

10. Mailgateway

OPNSense

1. **Allgemein**
    1. **Links zu den Youtube Video und Nextcloud**

Workshop 09.04.2024 und 11.04.2024

Kostenpflichtiger Link für Videos

Die Aufzeichnungen findet ihr im Kurs, der wiederum auf ein Textdokument in der Nextcloud verweist!

Der Nextcloudlink ist immer im Kurs oben, bzw. hier

Kostenpflichtiger Link für Videos

2. **Virtuelle OPNSense auf ProxMox**

DNS Eintrag: opnws.sysops.de

Download: https://opnsense.org/download/

- Image Type: DVD (ISO)
- Mirror Location: Germany …. (Fulda)

Download Link kopieren

Im PVE funktioniert der „Download“ nicht, da ein .bz2 Datei

Auf ProxMox CLI:

- ```
  cd /var/lib/vz/template/iso
  wget <gepeicherten Download Link> —> OPNSense*.iso.bz2
  bunzip2 OPNSense*.iso.bz2
  ```

PVE GUI - anlegen der VM

- VM ID: 9999
- Name: opnws.sysops.de
- Start on boot: <Haken setzen>
- Tags: <auswählen bzw. erstellen>
- ISO Image: OPNsense.....iso —> Business Edition ist bei 23.x / Free Version 24.1
- Type: Other —> wegen BSD
- Maschine: q35
- BIOS: Default(SeaBIOS) —> UFI würde auch gehen
- SCSI Controller: VirtIO SCSI Single
- Quemu Agent: <Haken setzen>
- Bus / Device: SCSI 0
- Storage: local-zfs —> evtl. anderen Storage wählen
- Disk Size: 32 —> **Log Files: 100 oder 200 GB** - kein Weg bekannt für Vergrößerung
- SSD emulation: <Haken setzen>
- Discard: <Haken setzen>
- Sockets: 1
- Cores: 32 —> Chriz hat 32 CPU und will die komplette Power
- Type: Host —> wir sehen die CPU wirklich in der VM - Alternativ was mit AES
- Memory: 4096 - 4 GB für die meisten Fälle in Ordnung
- Bridge: vmbr0
- Model: VirtIO (paravirtualized)
- Firewall: <Haken entfernen>
  ```

Was fehlt hier noch ? Das WAN Interface

Wechseln zu Hardware:

- Add Network Device
  - Bridge: vmbr3 —> sollte man vorher im PVE bei sich nachschauen …
- Model: VirtIO (paravirtualized)
- Firewall: <Haken entfernen>

MAC Adressen aus dem PVE aufschreiben / merken !

PVE Console OPNSense:

- **Achtung: LAN IP Adresse (default): 192.168.1.1**
- OPNSense Doku: https://docs.opnsense.org/manual/install.html#
- Login: **installer** —> für Installation der OPNSense, root —> temporäre Eingaben bis zum nächsten reboot
- Password: opnsense
- Tastaturlayout: German auswählen
- Install Filesystem:
  - ProxMox: Install UFS —> ProxMox hat ja schon ZFS —> ZFS auf ZFS macht man nicht
  - Hardware: Install ZFS —> eigene Hardware für OPNSense, hier will man ZFS haben, wegen snapshots
- SWAP —> Willst Du es haben ? Ja wahrscheinlich willst Du es haben …
  - Sollte die Platte zu klein sein bleibt nur die Neuinstalliert und das **zurückspielen vom Backup und Plugins neuinstallierten**
- Root Passwort setzen
- Install and reboot auswählen, um die Installation zu starten
  - OPNSense ist sehr gesprächig beim booten und braucht recht lange zum Booten
- Login als root
- Konfiguration des LAN Interfaces
  - DCHP: N
  - IP: 192.168.50.99
  - Subnet Mask (bit counts - CIDR notation): 24

    - Gateway address: <leer lassen> —> machen wir später
    - IPv6 Address via WAN: N
    - IPv6 DHCP6: N
    - IPv6 IP Address: <ENTER> —> Keine IP Adresse
    - Enable DHCP Server on LAN: n
    - Do you want to change GUI protocol from HTTPS to HTTP: <ENTER>
    - Do you want to generate a new self-signed web GUI certificate: <ENTER>
    - Restore web GUI accès defaults: <Enter>
        - In der Ausgabe steht dann die IP Adresse: https://192.168.50.99

    - 2 —> Set Interface IP address
    - 1 —> LAN

3. **Sophos UTM9 Firewall**

In den Kurs wird immer mal wieder parallel auf die Sophos Firewall gegangen.

Bei ersten einloggen ist auf gefallen, dass die Lizenz abgelaufen oder herausgeflogen ist, dann kann man sich auch keine bestehenden Konfigurationen mehr anschauen.

Chriz hat die Lizenz wieder eingespielt und man kann sich wieder alles anschauen. Es muss der File aus dem myutm-sophos.com Portal heruntergeladen werden und dieser File muss eingespielt werden !

4. **OPNsense GUI - Einstiegskonfiguration**

In der Dokumentation werden nur die wichtigsten Felder der OPNsense beschrieben, um sich die Bilder vom Workshop anzuschauen, kann die Volltextsuche vom Kurs verwendet werden. Um die Dokumentation recht schlank zu halten, wird möglichst auf Bilder verzichtet.

Im **Webbrowser die GUI der OPNsense** starten

- Mit root einloggen

ProxMox CLI:

- `/etc/cron.daily/zfs-auto-snapshot`
  —> bei gewissen Aktion kann man sich von der OPNsense ausschließen und da ist ein zfs-auto-snapshot für den Rückfall sehr willkommen

Wieder **zurück im Webbrowser der OPNsense**

- System: Wizard: General Setup gestartet
  - *Einschub: Thema VDSL*
  - Hostname: openws
  - Domain: sysops.de
  - Language: English —> Chriz: würde es immer auf englisch belassen
  - Primary DNS Server: 1.1.1.1
  - Secondary DNS Server: 8.8.4.4
  - Override DNS: <Haken entfernen> - Allow DNS servers to be overwritten by DHCP/PPP on WAN
  - Enable Resolver: <Haken gesetzt lassen>
  - <Next> Button
  - Timezone: Amsterdam oder Berlin auswählen oder bei UTC belassen
  - <Next>-Button
  - IPv4 Configuration Type: PPPoE
  - PPPoe Configuration —> *Wir werden es nicht benutzen*
    - PPPoe Username: 1234567890120123456789012000l@t-online.de
    - PPPoe Password: 123123
  - RFC1918 Networks
    - Block RFC1918 private Networks: Haken standardmäßig gesetzt
    - Block boron networks: Haken standardmäßig gesetzt
    - **Anmerkung Fritz!Box**: Für Fritz!Box die beiden Haken entfernen
  - <Next>-Button
  - <Next>-Button
  - <Next>-Button
  - <Reload>-Button —> Button nicht gedrückt !!!
  - Ein Point-to-Point Device - vtnet1
  - + —> Add
    - Device: vlan0.7
    - Parent: vtnet1
    - VLAN tag: 7
    - Description: VDSL
    - <Save>-Button
    - <Apply>-Button
      - Edit VLAN —> Sophos -DSL (PPPOE) - mit VDSL
  - Link interface(s): vlan0.7

    - <Save>
        - <Next> Button
        - General Information
        - Time Server Information
        - Configure WAN Interface
        - Configure LAN Interface
        - Set Root Passwort
        - Reload Configuration
        - Unter Interface - Point-to-Point - Devices
        - Interface - Other Types - VLAN
        - Interface - Point to point - Devices

- ==> Hardware OPNsense mit PPPoE
- Interface - Point-to-Point - Log File
    - Debug

Einschub: Thema VDSL

- PVE GUI:
    - Network Device
        - Ergänzung: Tag 1 (Telefon), Tag 2 (TV) —> oder so was …
        - VLAN Tag: 7
    - VM: OPNSense (ID: 9999)

Im Textfile erklärt:

- BTX (Bildschirmtext)
- Anschlusskennung: 123456789012 (12-stellig)
- T-Online Nummer: 123456789012 (12-stellig) —> kürzer als 12 stellen # erforderlich - bedeutet sprint in das nächste Feld
- Mitbenutzer: 0001 (4-stellig)
- Password: xxxx (beliebig)
- DSL: @t-online.de

OPNsense VDSL

- Modem
- Interface
- Interface VLAN7
- PPPoe

Wieder **zurück im Webbrowser der OPNsense**

- PPPoE Konfiguration wieder aus der OPNsense löschen
- Wir machen jetzt richtiges Internet

- Interfaces - Assignments
  - Ändern auf vtnet1 —> in Klammern wird die MAC Adresse angezeigt
  - **MAC Adressen im ProxMox kontrollieren**
  - Basic configuration
    - Subnet mask: 24 —> Feld neben IP Adresse
      - Lock: <Haken setzen> —> Prevent interface removal
      - IPv4 configuration Type: Static IPv4 —> war vorher: PPPoE
      - IPv6 configuration Type: None —> Erwartet hier kein IPv6 im Kurs
      - MTU: —> Wenn z.B. beschießene Dialup Leitung
      - IPv4 address: 194.30.174.105 —> Achtung bei kopieren - z.B. Klammer oder …
      - <Save>
      - <Apply>

    - [LAN] lan vtnet0 —> in Klammern wird die MAC Adresse angezeigt
    - [WAN] WAN pppoe (missing)
    - <Save>
    - [WAN] ist ein Link auf Interfaces: [WAN]

In einer CLI:

Pingtest funktioniert noch nicht, da noch **kein Gateway**

Wieder **zurück im Webbrowser der OPNsense**

- Im Suchfeld (Lupe): Gateway eingeben
- System Gateways: Configuration
  - Edit gateway - war schon drin von PPPoE
    - IP Address: 194.130.174.1
    - Disable Gateway Monitoring: <Haken entfernen> —> wenn es pingbar ist
    - Monitor IP: 1.1.1.1 - evtl. ist die IP nicht optimal
    - <Save>
    - <Apply>

In einer CLI:

Pingtest funktioniert noch nicht

Wieder **zurück im Webbrowser der OPNsense**

- System: Gateways: Configuration
  - Status: offline

    - <Apply>
    - Status: grün —> online

In einer CLI:

Pingtest funktioniert noch nicht

Wieder **zurück im Webbrowser der OPNsense**

Im Suchfeld (Lupe): alias

- Firewall: Aliases
    - + —> Add
        - Name: sysops_Sites
        - Type: Network(s)
        - Content: 194.30.174.1/24 87.191.167.179/32
        - Description: Wo wir sind
        - <Save>
        - <Apply>

Wieder **zurück im Webbrowser der OPNsense**

- Im Suchfeld (Lupe): wan
- Firewall: Rules: WAN —> Erlaubende Regel

    - + - Add
        - Interface: WAN —> schon ausgewählt, da drüber eingestiegen
        - Direction: in —> Eingehende Pakete
        - Source: sysops_Sites
        - <Save>
        - <Apply>

In einer CLI:

Pingtest **funktioniert jetzt**

Sophos Interface - WAN angeschaut

Wieder **zurück im Webbrowser der OPNsense**

- Interfaces: Virtual IPs: Settings
  - + Add
    - Mode: IP Alias —> CARP könnte früher nicht mehr geändert werden
    - Interface: WAN
    - Network / Adress: 194.30.174.106/24
    - Description: Alternative IP Workshop
    - Edit Virtual IP
    - <Save>
    - <Apply>
    -

So jetzt haben wir zweite IP Adresse

Wieder **zurück im Webbrowser der OPNsense**

Im Suchfeld (Lupe): Gateways —> Wie ist das gedacht …

- System: Gateways: Configuration
  - + - Add
    - Name: OPNRZ
    - Description: OPNsense Produktiv
    - IP Adress: 192.168.50.113 —> Möchte ich eher für Routen als zum Surfen verwenden
    - Disable Gateway Monitoring: <Haken entfernt> —> ob sie ping wissen wir nicht
    - Monitor IP: 192.168.50.200 —> ProxMox könnte sich melden
    - <Save>
    - <Apply>
    - Missconfigured Gateway IP
    - Brauche ich jetzt auch nicht zwingend - so ist es gedacht
    - Remove ORNRZ Eintrag als Gateway
    - <Apply>
- Im Suchfeld (Lupe): Live
- Firewall: Log Files: Live View
- Action contrains block - + —> zeigt die block
  - —> Unter Action steht grau hinterlegt: action-block
  - Zeigt alles was geblockt wird
  - >> - new - Feld Template Name: block - <Enter>
  - Danach kann es später immer wieder ausgewählt werden
  - Protoname is icmp - + - >> - new - Feld Template Name: Block ping
  - —> Unter Action steht grau hinterlegt: action-block protname=icmp

    - Zeigt alle geblockten ping’s
    - Bei Lookup hostnames kann ein haken gesetzt werden - Bei Bedarf
- Im Suchfeld (Lupe): alias

Im anderen Browser Tab: Google

- Blocklisten
    - Local copy: download local copy —> diesen Link kopieren
        - firehol_level1:
        - firehol_level2:

Wieder **zurück im Webbrowser der OPNsense**

- Firewall: Aliases
    - + - Add
        - Name: Firehol L1
        - Type: URL Table (IPs) —> aktualisieren sich
        - Refresh Frequency: Days. Hours
            - Feld unter Days: 1
            - Feld unter Hours: 0
        - Content: <hier die kopierte URL eintragen>
        - Description: Firehol L1
        - <Save>
        - <Apply>
        - <Apply> - Nach dem zweiten Apply hat sich die Zahl oben rechts verändert von 92 auf 2090
        - Edit Alias

- Im Suchfeld (Lupe): alias
- Firewall: Diagnostics: Aliases
    - Feld: sysops_Sites
        - Zeigt zwei Treffen
    - Feld: Firehol L1
        - Zeigt mehr / viele Treffer

Frage: Firehol L1: ausgehend oder eingehend ?

Firehol L1 enthält private Netze, d.h. eingehend - L1 eingehend auf WAN

- Im Suchfeld (Lupe): WAN
- Firewall: Rules: WAN
    - + - add
        - Action: Block

    - Log: <Haken bei Bedarf>
    - Source: Firehol_L1
    - Description: Firehol L1
    - <Save>
    - <Apply>
    - Firewall:Rules: WAN

Was ich immer machen würde:

- Block Regel
    - Haken setzen bei Firehol L1
    - Dann oberste Regel - Pfeile —> Move selected rules before this rule —> damit steht die Firehol L1 Regel ganz oben
    - <Apply>

- **Immer erst die Block Listen und dann die Erlauben Listen**

- Im Suchfeld (Lupe): Live
    - Block auswählen
        - Es werde erste Firehol L1 Elemente geblockt

OPNsense Business License - hat Chriz für das RZ gekauft —> anderes Browser Tab

- OPNsense Business Edition (3Yr) - Angebot 359 € statt 447 €
    - Anderes Repository
    - GeoIP database
    - Free E-Book

Business Edition:

- Im Suchfeld (Lupe): alias
- Firewall: Aliases
    - Reiter: GeioIO settings
        - Edit Alias
            - z.B. Afrika
            - Unwanted Geolocations
        - Search Geo
    - Alias kann in einer Firewall Rule als Block definiert werden
    - In der **freien Version** muss man über einen Drittanbieter gehen …

5. **OPNsense GUI - Basiseinrichtung**

    1. **Einschub Aliases**

Für die Aliases wäre ein Konzept sinnvoll, aber Chriz meinte auf Grund der Kundenanzahl und … wird er es nicht konsequent umsetzen können. Darüber muss sich jeder selbst Gedanken machen, inwieweit das für einen sinnvoll ist.

- **N_DONTROURE Regel enthält alle privaten Netze**
  - 192.168.0.0/16
  - 10.0.0.0/8
  - 172.16.0.0/12

Wieder **zurück im Webbrowser der OPNsense**

- Firewall: Aliases
  - Name: N_Dont_Rroute
  - Type: Networks(s)
  - Content: 192.168.0.0/16 10.0.0.0/8 172.16.0.0/12
  - Description: Nicht aus dem Internet
  - <save>
  - <apply>
    - + - add

Sophos - Firewall - rules

—> gibt es so nicht in der OPNsense

Regel in der OPNsense im RZ angeschaut

- Firewall: Rules Firma X
  - Dadurch und die Aliases kann ein Regel auch schonmal komplex werden, aber dann muss man sich die Source und die Destination der Regel klar machen
    - Destination: N_DONTROUTE wird **negiert** in der Regel eingesetzt

- Für die Firma X gibt es ein **eigenes Interface**, bei **Source** wird das **Netz der Firma** angegeben

Chriz erklärt es noch mal anders:

- Firewall: rules: LAN
  - **Problem bei Chriz**: Er hat viele Kunden, die nicht untereinander zugreifen soll / dürfen - da kommt die N_DONTROUTE Regel zum Einsatz **aber negiert** im *Destination* und *Destination / invert* wird angeklickt —> Zeigt er wieder am Beispiel im RZ
    - D.h. ich könnte den Bereich *Destination:* N_Dont_Route setzen aber der *Destination / invert* muss angeklickt werden
  - \+ - add
  - <save>
  - <apply>
  - Damit wird eine Regel erstellt mit der man alles darf

Achtung: Hier ist die Reihenfolge der Regeln entscheidend. Erst verbieten dann erlauben. Eine erlauben Regel vor der verbieten Regel würde wieder z.B. ein Netz erlauben

2. **Basis Setup**

Wieder **zurück im Webbrowser der OPNsense**

- System: Settings: Administration
  - Server: Local Database - auswählen, das hilft - vorher **Nothing selected**
    - Protocol: HTTPS - ausgewählt
    - TCP port: 4444 - 443 wollen wir später für was cooles haben, wir machen mal einen neuen Port 4444
    - HTTP Redirect: Haken setzen - damit redirect disabled wird, evtl. brauche ich den Port 80 später auch noch
    - Alternative Hostnames: opnws.sysops.de - DNS Name wegen rebind check
    - Access log: Haken setzen (enable)
    - Listen interfaces: ALL
    - Secure Shell Server: Haken setzen - enable
    - Root Login: Haken setzen - permit root user login
    - Authentication Method: Haken ***nicht*** setzen - ***disable*** permit password login - kein Passwort Login
    - Listen Interfaces: ALL
    - Authentication

    - <save>

OPNsense: Für jeden neuen Dienst muss eine Firewall Regel definiert werden

SOPHOS: da war das nicht so - dort werden Netze definiert, die im Hintergrund eine Firewall Regel gebaut haben

- Im Suchfeld (Lupe): User
- System: Access: Users
    - Authorized keys: **public key** des ssh key hinterlegen (System das Zugriff haben soll z.B. Laptop)
    - Root user —> Edit (Stift)
    - <save>

CLI:

- ssh root@opnws.sysops.de
    - Passwort loser Zugriff per CLI

Wieder **zurück im Webbrowser der OPNsense**

- System: Settings: Administration
    - Chriz zeigt es doch schon:
        - Zeigt QR Code
            - Jetzt kann Du den QR Code im z.B. Google Authentificator ab fotografieren, damit die „Verbindung“ zur OPNsense hergestellt ist für die Code Generierung
            - **Achtung:** bei so was kann man sich leicht aussperren - daher vorher eine Snapshot machen
        - OTP seed: haken setzen —> Generatenew secret (160 bit)
        - <save and to back>
        - OTP QR Code: <Click to unhide>
    - OTP seed: Hier könnte man jetzt noch one time password setzen / konfigurieren —> machen wir später

- Zum Testen aus und wieder einloggen
    - Hier ist noch nichts mit 2 Faktor aktiv !!!

Ob man das ssh auf WAN will muss man sich überlegen.

3. **Plugins**

Im Suchfeld (Lupe): Plugins

- System: Firmware
    - Unter der Reiterleiste gibt es den Punkt **Name** —> Suche (Eingabe zur Suche des Plugins)
        - acme
    - os-acme-client —> + Zeichen anklicken
        - Sollte die Installation starten, aber die Firmware ist nicht aktuell, d.h. es muss vorher ein Firmware Update durchgeführt werden —> Installation out of date
    - Reiter: Plugins

- Im Suchfeld (Lupe): firmware
    - System: Firmware
        - Info zum Update bestätigen
        - <update> - meist wird ein reboot benötigt - manchmal bootet er sogar 2 mal
        - <check for updates>

OPNSense: kann im laufenden Betrieb Netzwerkkarten hinzufügen

SOPHOS: da ging das nicht im laufenden Betrieb - Interface - um hinter Interface einzutragen muss die SOPHOS herunterfahren - eintragen und wieder starten - Bei HA muss beide heruntergefahren werden - das bedeutet RZ offline - ging dann nur abends

OPNSense: Wieder in die Oberfläche einloggen

- Im Suchfeld (Lupe): cron —> Updates automatisieren
  - System: Settings: Cron —> n**ur wenn ihr Zugang zur Firewall habt, Backups und snapshot vorhanden sind —> ALLOW_RISKY_MAJOR_UPGRADE**
    - Minutes: 0
    - Hours: 0
    - Command: Firmware update check
    - Description: C —> wie check
    - <save>
    - <apply>
    - Minutes: 0
    - Hours: 1
    - Command: Automatic firmware update
    - Parameters: ALLOW_RISKY_MAJOR_UPGRADE —> ohne Eintrag würde er keine großen Updates machen, Eintrag **nur mit Absicherung** - siehe oben
    - Description: U
    - <save>
    - <apply>

- Im Suchfeld (Lupe): Plugins
  - System: Firmware
    - Unter der Reiterleiste gibt es den Punkt **Name** —> Suche (Eingabe zur Suche des Plugins)
      - acme
    - os-acme-client —> + Zeichen anklicken
    - Unter der Reiterleiste gibt es den Punkt **Name** —> Suche (Eingabe zur Suche des Plugins)
      - Next
    - Os-nextcloud-backup —> + Zeichen anklicken
    - Unter der Reiterleiste gibt es den Punkt **Name** —> Suche (Eingabe zur Suche des Plugins)
      - ngi —> hätte ich gerne in meinen Kurs
    - os-nginx
    - Unter der Reiterleiste gibt es den Punkt **Name** —> Suche (Eingabe zur Suche des Plugins)
      - qem
    - os-qemu-guest-agent —> + Zeichen anklicken
    - Reiter: Plugins

        - Reiter: Plugins
        - WireGuard war früher ein Plugin, ist jetzt fest drin
        - Reiter: Plugins
        - HA Proxy —> Erklärung liegt in der Nextcloud —> Chriz benutzt es nicht
        - Reiter: Plugins
    - Dashboard
        - Starten —> <play Button>
        - QEMU Guest Agent

ProxMox GUI:

- VM 9999 opnws.sysops.de auswählen
    - Nach kurzer Zeit werden z.B. IPs angezeigt
        - Summary

QEMU Agent erlaubt es die VM sauber herunterzufahren

4. **Zertifikat für die Weboberfläche (GUI) der OPNsense**

Let’s encrypt war in der SOPHOS recht spät und richtig schlecht - Certificate Management - Reiter Certificate Authority - geht nur mit http challenge

- Im Suchfeld (Lupe): acme
    - Services: ACME Client: Settings
        - Show introduction pages: Haken entfernen —> haben wir alles hier gelernt
        - Enable Plugin: Haken setzen
        - <apply>
        - + / add
            - Name: sysops_le —> le für let’s encrypt
            - ACME CA: Let’s Encrypt (default)
            - E-Mail Address: christian@sysops.de
            - <save>
                - Edit Account
        - + / add
            - Name: sysops_zs

    - ACME CA: ZeroSSL —> anderer Anbieter
    - E-Mail Address: christian@sysops.de
    - <save>
        - Edit Account

- Symbol: Viereck mit Pfeil nach unten —> Account registrieren ==> bei sysop_le
    - <yes>
        - Conformation Required

- Symbol: Viereck mit Pfeil nach unten —> Account registrieren ==> bei sysop_zs
    - <yes>
        - Conformation Required

- + / add
    - Name: LE_HTTP
    - Description: HTTP Challenge
    - Challenge Type: HTTP-01
    - HTTP Service: OPsense Web Service (automatic port forward)
    - Interface: WAN
    - <save>
        - Edit Challenge Type

- + / add
    - Common Name: opnws.sysops.de —> DNS muss passen
    - Description:
    - ACME Account: sysops_de
    - Challenge Type: LE_HTTP
    - DNS Alias Mode: Not using DNS alias mode —> vorher: Not using DNS alias mode
    - <save>
    - Edit Certificate
- Reiter Settings
- Services: ACME Client: Accounts
- Services: ACME Client: Accounts
- Services: ACME Client: Challenge Types
- Service: ACME Client: Certificates
- Button unten: <Issue/Renew all Certifcates> - erneuert alle Zertifikate —> Chriz würd ich nicht machen
- Rechteck mit Pfeil als Kreis —> Issue or renew certificate —> erneuert nur das eine Certificate „Common Name: opnws.sysops.de
- Service: ACME Client: Log Files
- Dort sollte die Zertifikates Erzeugung und Ablage zu sehen sein

- Reiter ACME Log
- Services: ACME Client: Certificates
  - Dort ist das Zertifikat zu sehen
  - Es gibt einen Cron Job der die Erneuerung macht - normalerweise bringt dieser einen immer an —> Chriz hat es gerade nicht gefunden
- Wenn Dir Let’s Encrypt auf den „Sack“ geht könnte man auch ZeroSSL verwenden
- Services: ACME Client Challenge Types
  - Name: ZSSL_HTTP
  - Description: HTTP Challenge Zero SSL
  - <save>
  - Name: LE_HTTP Clonen —> Zwei Rechtecke übereinander als Symbol
  - Edit challenge Type —> Anpassungen vornehmen
- Service: ACME Client: Certificates
  - Edit Certificate
    - ACME Account: sysops_zsl
    - <save>
  - Clone Let’s Encrypt Eintrag —> zwei Rechtecke übereinander
  - Renew bei neuen Eintrag über den Pfeil als Kreis ausführen
- Services: ACME Client: Log Files
  - Auch hier sollte der Abruf des neuen Zertifikates sichtbar sein
  - Zero SSL lässt sich etwas mehr Zeit - ein sleep von 15s
  - Reiter: ACME Log
- Services: ACME Client Certifcates
  - Dort findet man jetzt zwei Zertifikate
- System: Trust: Certicates
  - Self-signed
  - Let’s Encrypt
  - Zero SSL
  - …
  - Dort landen alle Zertifikate

  - Services: ACME Client: Challenge Types —> Wildcard Certificate
    - Edit Challenge Type
      - Name: Hetzner
      - Description:
      - DNS Service: DNS-01
      - DNS Service: Hetzner
      - API Token: <Paste from Clipboard - siehe Hetzner unten>
      - <save>

    - + / add

  - Services: ACME Client: Certificates

- Edit Certificate
  - <yes>
    - Common Name: *.sysops.de —> Wild Card Zertifikate
    - Description: Wildcard
    - ACME Account: sysops_le
    - Challenge Type: Hetzner_DNS
    - <save> —> dauert ein paar Sekunden länger
    - Symbol Rechteck mit Pfeil als Kreis —> Zertifikat abholen
    - Conformation Required
  - + / add
- Services: ACME: Log Files
  - Reiter: ACME Log

DNS Anbieter: macht bloss 2 Faktor Authentifizierung rein

Browser Hetzner Login Seite

- DNS Console
  - Token Name: Workshop
  - Create access Token
    - API Token —> <Copy to Clippboard> Button
  - <Confirm>
  - Manage API tokens

Nachdem das Zertifikat in der OPNSense angefordert wurde, sieht man im Hetzner Portal —> Record deleted

Da heißt OPNsense steuert jetzt Deinen Hetzner.

Chriz hat anschließend gleich den Revoke token ausgeführt, damit ist der Token in der OPNsense unbrauchbar geworden.

- Services: ACME Client: Automations

        - Edit Automation
            - Name: NGINX
            - Description:
            - Run Command: Restart Nginx (OPNsense plugin)
            - <save>

        - + / add —> Das habe ich überall vergessen

    - Services: ACME Client: Certificates
        - Automation: NGINX —> Gibt es ein neues Zertifikat gibt, wird der NGINX durchgestartet - Bei der SOPHOS ging das alles automatisch

        - Common Name: *.sysops.de
        - Edit (Stift)

    - System: Settings: Administration
        - SSSL Ciphers: < hier kann jetzt unter verschiedenen Zertifikaten ausgewählt werden> —> z.B. Zero SSL
        - <save>

Browser:

- opnws.sysops.de:4444
    - Offizielles Zertifikat ohne jetwillige Warnung des Browsers

Frage: intern Domain .z.B. xxx.lan

- Du nimmst ein internet Domain mit der interne IP Adressen
- Der DNS Server läuft intern, trotzdem bekommst Du ein Zertifikat

5. **OPNSense HA**

Du könntest Dir jetzt das umständlich zusammen klicken, aber das machen wir hier nicht

- System: High Availability: Settings —> das ist richtig kompliziert

SOPHOS: High Availability —> war nicht der SOPHOS viel einfacher

Youtube Video

OPNsense High Availability, höher und günstiger denn je - Live 24.08.2023

Link: OPNSense HA

Wenn Du ein ProxMox Cluster hast

ProxMox GUI:

- VM 9999 opnws.sysops.de auswählen
  - Add
    - Schedule: */5 —> alle 5 min
    - <create>
  - <Schedule now>
  - <Log>
  - Migrate
    - Achtung: vorher ISO herausnehmen
      - CD/DVD
        - ISO … auf don’t Use this media setzen
      - Hardware
    - Output
      - Das braucht seine Zeit
        - Platte wird migriert
        - Auch der RAM muss migriert werden - da ist weniger mehr
      - Kann auf den anderen PVE (PVE3) umgezogen werden
      - <Migrate>
  - Replication
  - Rechte Maustaste auf VM 999

CLI:

- Über einen ping während der Migration sieht man das es nur einen kurzen aussetzen im ping Ablauf gibt

Chriz reduziert den RAM der OPNsense Workshop, dafür wird die VM heruntergefahren. Bei der offline Migration im ProxMox braucht nur der Storage migriert werden, durch ZFS werden nur die Änderungen übertragen. Anschließend wird der RAM auf 4096 MB reduziert, minimaler RAM auf 2048 gesetzt und wieder gestartet.

6. **OPNsense Hardware / Virtuell**

An hand der „Themenstruktur.md“:

- Thomas Krenn Hardware: Chriz braucht die Hardware nicht
- Mini Forum GK41
  - Ist doppelt so schnell wie eine SG230
  - Zwei Interface mit 1 Gbit/s

- Firma IPU - die hat Chriz noch nicht getestet
  - Kann man sich bauen lassen, wie man es haben will

- Mini PC 2.5 GHz und WLAN was auch mit der OPNsense funktioniert - mit N100
  - Es kann noch eine SATA SSD dazu gebaut werden
  - Standard wäre 128 GB SSD - das ist auch völlig ausreichend
    - Transcend 128 GB - könnten OK sein
    - KingSpec hat Chriz letztens gekauft, waren ganz OK
    - 3 * schneller als eine SG230 und wird gut warm
    - 2,5 Gbit/s

  - Evtl. mit 16 GB RAM, wenn Du sie bekommst —> ProxMox müssen es 16 GB seinSta
  - SSD sind zum Teil durch wachsen, d.h. sie können ausfallen

Virtuelle OPNsense Parameter an hand der „Themenstruktur.md“ durchgesprochen

- Disk size: 64 GB - da Vergrößerung schwierig …

7. **Migrationswege zur OPNSense**

    1. **Harter Tausch**

Als erstes müssen die Redbox (Red) los werden

Site to Site VPN und Fernzugriff

- IPsec
- OpenVPN

Praxis Beispiel:

- GK 41
  - IPsec
    - Strongworm können Sophos und OPNsense beide gut
  - OPNsense
  - Site to site VPN
  - NextCloud Backup
- OPNsense online bringen und Sicherheitslevel erhöhen IKEv2

- Wenig Config
- Wegfall Lizenz oder Hardware
- Home- und Monatslizenz

2. **Multivan**

Bei Multivan bringe beide Firewalls online auf verschiedenen IP's. Über Routen oder über DHCP Server ändern des Gateways auf ONPsense.

3. **Single WAN**

Auf der OPNSense wird alles durch geNATet.

Sophos Kabel für den Internet Zugang abziehen und auf die OPNsense umstecken.

Danach auf der Sophos auf Internal das „IPv4 default GW Address" auf die OPNsense ändern und das war's. Danach die NAT Regel auf der Sophos auf die OPNsense eintragen. D.h. Du NATest die Sophos raus und das hat den Nebeneffekt, dass Du siehst wie weit Du mit der Migration bist.

OPNSense:

- Firewall: Rules: WAN
  - In den Beispiel läuft gar nichts mehr über die alte Firewall (Sophos), d.h. die kann ausgeschaltet werden
    - Automatische Rules aufgrund von NAT haben keine Edit Knopf
    - Inspect - da sehe ich ob noch Traffic drüber geht

Sophos:

- Kaum noch Traffic drauf
- Eine Redbox ist online
    - Nutzt eigentlich auch schon VPN, kann also auch aus

Ausschalten der Sophos

Wichtig ist die Änderung der Gateway auf die neue Firewall. Im DHCP Server muss das neue Gateway eingetragen sein. Ist in diesen Fall so, da die OPNsense den DHCP Server spielt. Wo das Gateway von Hand eingetragen ist, muss es auch von Hand geändert werden.

Alles noch mal kontrollieren, ob alles auf die OPNSense umgestellt ist.

4. **OPNSense**

Es gibt zwei DHCP Server

- ISC (alt) - ist gut, er der besten DCHP Server
- Kea (neu) - hat sich Chriz noch nicht angeschaut

Unbound DNS

Backup

- System: Configuration: Backups
    - Enable: Haken setzen
        - Weitere Configuration …
    - Kannst ganz viele Backup’s in der Nextcloud aufheben, hat Chriz an einer anderen OPNsense gezeigt
        - Backup count: 50 - Chriz würde hier mal ein 50 reinschreiben
        - <save>
        - —> Backup im System
        - Backup kann man herunterladen
        - Backup Datei kann in Teilen wieder hergestellt werden
        - NextCloud Backup

Qemu Agent nochmal kurz angesprochen.

Sophos - NAT Regeln

- Masquarding ist von Hause aus an

OPNsense

- Masquarding muss nicht separat konfiguriert werden

PVE - Container anlegen (ID: 9998) - kleiner Webserver zu herauslegen

- PVE CLI:

```
apt install apache2
```

    - Keine Internet Verbindung

```
pct enter 9998
```

OPNSense

- Live View: Firewall: Log Files: Live View
    - icmp Block: Destination 192.168.50.99, Source 192.168.50.98
- Im Suchfeld (Lupe): lan
- Firewall: Rules LAN
    - Nicht eintragen
    - <save>
    - <apply>
        - LAN Rule darf eigentlich überall hin - sollte gehen
        - Regeln disabled bzw. löschen
        - Neu LAN Rule anlegen
        - Ping auf das Gateway funktioniert, aber kein Zugriff auf das Internet z.B. ping 1.1.1.1
- Geht trotzdem noch nicht ...
- Live View: Firewall: Log Files: Live View
    - Ping wird nicht geblockt
- Firewall: NAT: Port Forward
    - Kein Problem ersichtlich
- Im Suchfeld (Lupe): ping

    - Hostname or IP: web.de
        - Job: gelöscht
            - Job: läuft ewig weiter und erreicht web.de
    - Interfaces: Diagnostics: ping

PVE CLI

- pct enter 9998
  nslookup
  web.de —> keine Antwort
  Server 192.168.50.99
  web.de —> Firewall antwortet, aber lässt uns aber nicht ins Internet
    - ==> **Gateway Thema**
    - Nslookup test’s

OPNSense

- Im Suchfeld (Lupe): gateway
- System: Gateways: Configuration
    - Passt alles
        - Edit Gateway
- Firewall: NAT: Outbound
    - Hybrid outbound rule generation
        - Automatic outbound NAT rule generation
        - Viele gehen auch auf:
- Im Suchfeld (Lupe): live
    - Wir wollen sehen ob er etwas blockt: Block / Block ping
        - Es wird nichts geblockt
    - Firewall: Log Files: Live View
- Interfaces: [LAN]:
    - Ob LAN Interface richtig konfiguriert
- Interfaces: [WAN]:
    - IPv4 Upstream Gateway: Auto-dect (Ist Zustand)

    - IPv4 Upstream Gateway: WAN_GW: 194.30.174.1 (geändert auf) - Chriz hatte da schonmal ein Problem
    - <Save>
    - <Apply>
    - Das war’s der konnte sich hier nicht von alleine entscheiden - Am Anfang über Assistenten für VDSL PPoE eingetragen !!!

PVE CLI

- ```
  pct enter 9998
  ```

    - Web Server antwortet
    - ```
      apt update
      apt install apache2
      apt install curl
      curl localhost
      ```

OPNSense

- Im Suchfeld (Lupe): nat
    - + / add
        - Interface: WAN
        - TCP/IP Version: IPv4
        - Protocol: TCP
        - Destination: WAN address —> oder Alternative —> Kurs: WAN address gewählt
            - *Destination: 194.30.174.106 (Alternative IP Workshop)*
        - Destination Port range: from: HTTP to: HTTP
        - Redirect target IP: single host or Network
            - Sauber wäre: Speichern, alias anlegen, Regel auf alias anpassen - wird man in der Regel nicht tun, Anmerkung Chriz
            - IP Address: 192.168.50.99
        - Redirect target port: HTTP
        - <save>
        - <apply>
            - Edit Entry
        - Firewall: NAT: Port Forward

Browser:

- opnws.sysops.de
    - Browser macht daraus https !!! Umleitung auf http auf https

Terminal:

- curl <link aus Browser kopiert>
    - Da sieht man https://opnws.sysops.de/

- curl http://opnws.sysops.de —> auf **http** geändert
    - Gibt Seite des Web Servers aus

PVE CLI

- ```
  pct enter 9998
  ```

    - acme
        - Dann kann ich aber nur einen WebServer herauslegen
    - Daher nimmt man einen Reverse Proxy
        - Wie bekomme ich jetzt https für den Webserver

Fritz!Box oder OPNSense

- NAT regel für Port 80 und 443 auf NGINX

Browser

- NGINX einloggen
    - Installiert über
        - Docker
        - PVE gibt es ein fertigen Installer
    - IP Adresse des NGINX nach draußen NATen (http und https)
    - Edit Proxy Host
        - Domain Name: home.eesy.de
        - Scheme: http
        - Forward Hostname / IP: 10.x.y.z
        - Forward Port: 8123
        - SSL Certificate: Request a new SSL Certificate
            - Reiter: Details
            - Reiter: SSL
    - E-Mail Adresse / Passwort
  ```

    - Proxy Hosts

Für kleine Setup.

Richtige Weg wäre … ist mühsam …bietet aber auch mehr Möglichkeiten

OPNSense

- Im Suchfeld (Lupe): nat
  - Evtl. vorhandene NAT Regel für Port 80 und 443 entfernen
  - <apply>
    - Firewall: NAT: Port Forward

- Im Suchfeld (Lupe): nginx
  - Reiter: General Settings
    - Enable nginix: Haken setzen —> Erst mal einschalten
    - <apply>

  - Reiter gib es einige
    - Viele haben dann noch Unterpunkte …

  - Also nicht für schwache Nerven
  - Reiter: Upstream - Upstream Server
    - Edit Upstream
      - Description: webserver_host
      - Server: 192.168.50.98
      - Port: 80 —> hat kein SSL
      - Server Priority: 1
      - <save>

    - + / add

  - Reiter: Upstream - Upstream
    - Edit Upstream
      - Description: webserver_upstream —> der alle Webserver zusammenfasst
      - Server Entries: webserver_host —> Wir haben jetzt nur einen Webserver
      - Enable TLS (https): keinen haken setzen —> Webserver hat noch kein TLS
      - <save>

        - —> Ein Webserver ist alleine in einer Gruppe
    - + / add
- Reiter: HTTP(S) - Location
    - Edit Location
        - Description: webserver_host_root
        - URL Pattern: / —> oder /webapp oder …
        - Upstream Servers: webserver_upstream
        - Force HTTPS: Haken setzen
        - <save>
    - + / add
- Reiter: HTTP(S) - HTTP Server —> der veröffentlich dann wirklich
    - Edit HTTP Server
        - *HTTP Listen Address: 80 [::]:80* —> das würde auf allen Adressen veröffentlichen !!
        - HTTP Listen Address: 194.30.174.105:80 —> Veröffentlichung auf der Hauptadresse
        - *HTTPS Listen Address: 443 [::]:443*
        - HTTPS Listen Address: 194.30.174.105:443
        - Server Name: opnws.sysops.de
        - Locations: webserver_host_root
        - TLS Certificate: *.sysops.de (ACME Client) —> wild card certificate
        - Client CA Certificate: R3 (ACME Client)
        - Enable Let’s Encrypt Plugin Support: haken ist schon gesetzt —> Er kann ein neues Zertifikat haben, wenn es ein neues gibt
        - HTTPS only: haken setzen
        - <save>
        - Rechteck mit Pfeifen im Kreis neben dem + Button —> wichtig
        -
    - + / add
- Services: Nginx: Configuration

Browser

- opnws.sysops.de
    - Browser hat eine sichere Verbindung, ob der Webserver kein gültiges Zertifikat hat
    - *.sysops.de —> Wild Card Certificate
        - Zeigt die Demo Seite von Apache 2 Debian Default Page
        - Im Browser kann man sich das Zertifikat anzeigen lassen

Für einen weiteren Eintrag müssen alle 4 Schritte wiederholt werden …

Im Schnelldurchgang weitere Einträge in der OPNsense:

- Upstream Server - webserver_host clone
  - Anpassen
- Upstream - webserver_upstream clone
  - Anpassen
- HTTP(s) - Location - webserver_host_root clone
  - Anpassen
- HTTP(s) - HTTP Server - opnws.sysops.de clone
  - Anpassen

Nginx in der OPNsense bietet noch mehr

- ACL IP’s
- Zusatz login
- …

OPNSense

- Im Suchfeld (Lupe): nginx
  - Services: NGINX: LOGS / HTTP ACCES —> bietet viele verschiedne Ansichten, wie Traffic Statistik, …

SOPHOS- Web Application Firewall (WAF) - verschiedene Reiter

Nextcloud - Kurs Files - Cynfo Setup - OPNSENSE_HA_PROXY.docx

- Wenn es interessiert kann sich den HA_Proxy in diesen Dokument anschauen, ist nicht Teil des Kurses

ISPConfig funktioniert nicht hinter einen NGINX Proxy, da braucht man den HA_Proxy —> Dafür hat Chriz die Anleitung schon ein paarmal benötigt

Wie bekommen wir raus, ob alles funktioniert ?

- Dashboard anschauen
  - Alles grün
  - Available Widgets können nach Bedarf hinzufügt werden wie z.B. IPsec, Interface Statics, Firewall log, WireGard, TrafficGraph

Browser

- GitHub.com/bashclub —> **bashclub**
  - Checkmk-opnsense-agent
    - How to install - 3 Zeilen
  - ssh auf die OPNsense —> ssh root@opnws.sysops.de
  - Geht mit 8 auf die shell
    - Einfügen der 3 Zeile in die Shell —> Plugin wird installiert
  - Sucht auf der Seite nach opnsense
- Geht mit dem Browser auf Deinen Check_MK —> **Check_MK**
  - Setup - Hosts - Add host
    - Hostname (required): hostname eintragen —> IP Adresse mit der ich da komme muss im Paket Filter drin sein
    - Save & run connection Tests
    - Run tests
    - Save and go properties
    - Accept all
  - Activate on selected sites
  - Suche mir den Host
  - Man sieht die ganzen Services
    - Einloggen
    - Monitor

Sophos - Network Protection - Firewall

- z.B. Nur zwei Server dürfen auf das Backup Netz zugreifen
  - Sources:
  - Destinations:

Um das in der OPNSense abzubilden muss man sich vorher eine Alias für Sources und Destinations bauen, um das abgebildet zu bekommen … - dann als Firewall Regel anlegen

OPNSense

- Im Suchfeld (Lupe): history

    - Backup (compare)
        - Hier kann man einen zweiten Zeitpunkt wählen und man kann sehen was zwischen den beiden Schritten konfiguriert wurde
        - Unter dem ersten Auswahl Fenster kann ein Zugang in der Vergangenheit ausgewählt werden, um auf diesen zurück zu springen, wenn man sich vierkonfiguriert hat

    - Sytem: Configuration: History

Chriz zeigt nochmal einige in seiner Firewall

- Wozu brauche ich Firewall Regeln im LAN ?
- Firewall Rule im WAN
    - Button <Inspect>
        - Welche Regeln greifen und welche greifen nicht ?
        - Die **Description** sollte immer ausgefüllt werden, da sonst der Sinn der Regel nur anhand der Regel selbst ermittelt werden kann
        - Frage offen: Welcher Zeitraum wird angezeigt ?
            - **Vermutlich nur seit dem Start von Inspect**
    - Selbst erzeugte Regeln erkennt man am Stift - Editierter !
    - Regeln die durch die NAT Rules kommen - die kann man nur löschen !
    - Was braucht man noch davon ?
- Firewall Regeln könnten kategorisiert werden
    - Darauf können dann auch wieder Regeln aufgesetzt werden - Nutzt Chriz nicht
- Gibt es z.B. 3 Regeln von unterschiedlichen Source auf den gleichen Port
    - Regeln könnten über einen Alias für die Source auf eine Regel reduziert werden
- Port Range für eine Aufgabe z.B. OpenVPN könnten auf eine Regel reduziert werden und es müsste nicht für jeden Port ein eigene Regel geben ...
- Umstellung Redbox können dir mit Logs vollgeschrieben werden
    - Auf die Destination localhost schicken und das Log der Sophos wird nicht mehr vollgeschrieben

2. Tag 11.04.2024

8. **DNS Server (alter: ISC)**

Anmerkung: Neuer DNS Kea

OPNSense

- Im Suchfeld (Lupe): DNS

    - Jetzt kann man sich den DHCP Range anschauen
        - Range: ....
    - Services: DHCPv4: [LAN]

Wie kann man das Testen ?

Linux Server mit nmap - dort gibt es ein Script: broadcast-dhcp-discover

LInux CLI mit nmap

- nmap --script broadcast-dhcp-discover
    - Interface: vmbr0
    - IP offered: <IP Adress>
    - ...
    - IP Address Lease Time: 4h00m00s
    - ...
    - Domain Name Server: <IP Adress>, 1.1.1.1
    - ...

OPNSense

- Im Suchfeld (Lupe): DHCP
    - System X suchen und MAC Adresse merken
        - machender.com —> kommst auf eine grüne Seite
            - Gibt Apple aus
                - Mac Adress eingeben
        - 3 stellen aa:bb:cc ist der Vendor
        - Browser suchen: Mac address vendor
    - Services: DHCPv4: Leases
- Im Suchfeld (Lupe): DHCP
    - Hinweis: hat verschiedene Level
        - Je nachdem was man braucht
            - Über Multi select können dann alle Level angeklickt werden
    - Services: ISC DCHPv4: Log File

DHCP gibt es pro Interface, wenn er aktiviert ist.

Nachtrag zum ersten Tag:

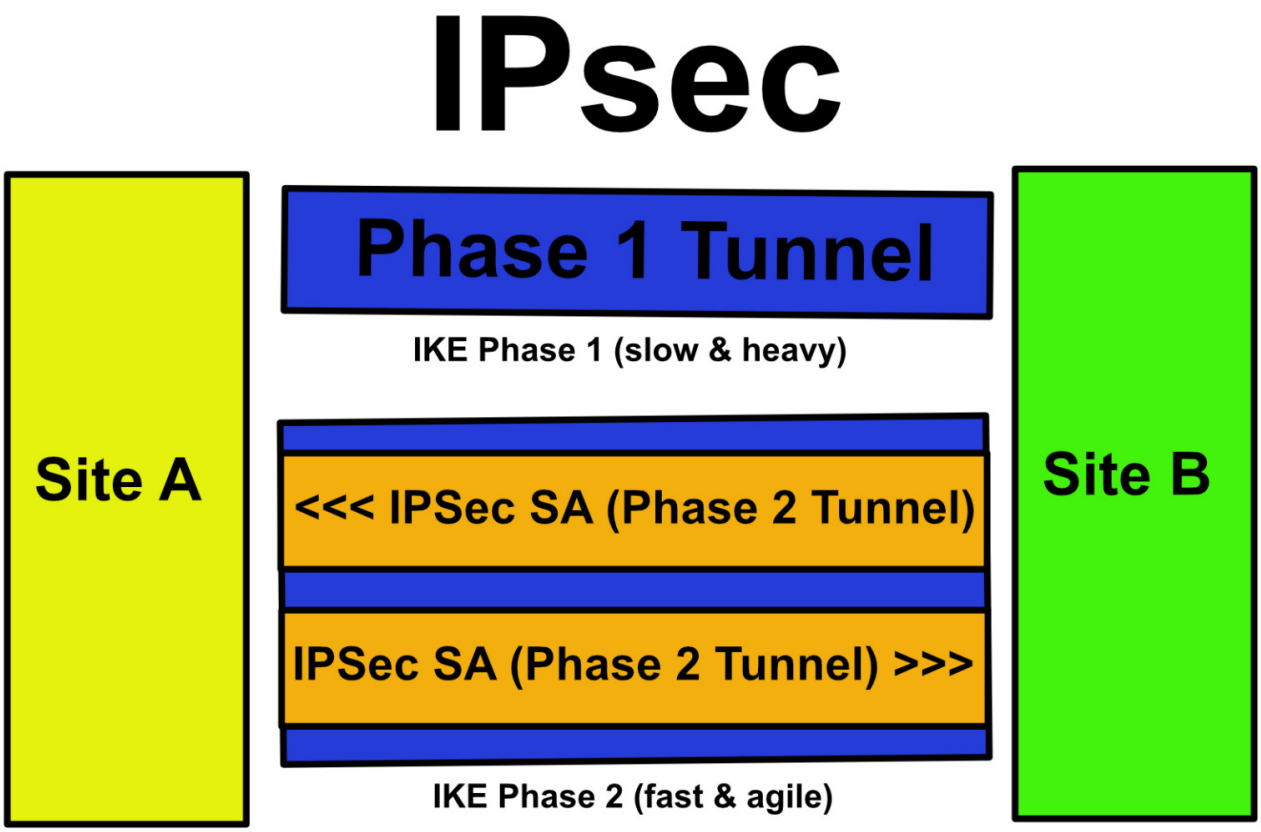
OPNsense

- Interfaces: Assigments
- [WAN] WAN
    - Device von PPoE auf vtnet1 umstellen

9. **VPN**

    1. **IPSec**

SOPHOS: Site-to-Site VPN - IPSec



OPNSense

- Im Suchfeld (Lupe): IPSec
    - Im Kurs werden wir noch **Tunnel Settings (legacy)** nutzen
    - Im *nächsten Kurs* wird **Connections** verwendet
    - Ist nur ein anderes FrontEnd beides ist Strongswan
        - VPN: IPsec: Connection

OPNSense

- Im Suchfeld (Lupe): IPSec
  - Es gibt zwei Phasen - Phase 1 ist zwischen den Sites
  - 2 Phase: da hast Du alle Subnetze
    - VPN: IPsec: Tunnel Settings [legacy]
      - Encryption algorithm: **Standard:** *256 bit AES-GCM with 128 bit ICV*
      - Encryption algorithm: AES —> zweite Fenster geht auf !
        - Zweites Feld: 256
      - Hash algorithm: MD5
      - DH key group: 5
        - Key Exchange version: v1 —> besser v2 - SOHOPS kann nur v1
        - Interface: TelekomFTTHPPoE
        - Remote Gateway: sophos.sysops.de
        - Discription: AB DMZ nach RZ Sophos
        - Phase 1 proposal (Authentication)
      - + / add —> add phase 1 entry
    - VPN: IPsec: Tunnel Settings [legacy]

Gegenseite SOPHOS:

- Wir geben der SOPHOS eine externe IP Adresse - Interfaces - WAN
- Es gibt noch ein alte IP Adresse: 194.30.174.96

Anmerkung: Geht nicht mit der Schulung OPNsense wegen Routing

CLI:

```
ping 194.30.174.96 # —> ergibt keine Antwort
```

PVE GUI:

- Suchen nach Sophos

    - Hardware
        - Einige Netzwerk Interface sind down

    - VM1002

Gegenseite SOPHOS:

- IP Adresse liegt auf dem Interface eth2 und hat die MAC Adresse ..:..:57

PVE GUI:

- Suchen nach Sophos
    - Hardware
        - Bridge: vmbr3
        - Disconnect: Haken entfernen —> Interface wird wieder aktiv

    - VM1002

CLI:

```
ping 194.30.174.96 # —> ping gibt eine Antwort - IP Adresse aktiv
```

OPNSense

        - Fortsetzen der Konfiguration / Ändern Remote gateway
            - Remote Gateway: 194.30.174.96
            - Fest IP Adressen
                - My identifier: My IP Address
                - Peer identifier: Peer IP Address

            - DynDNS - Chriz testet damit - funktioniert wahrscheinlich nicht
                - 2. Feld: sysops2024
                - 2. Feld: sysops2024
                - My identifier: Auswahl Distinguished name
                - Peer identifier: Auswahl Distinguished name

            - Pre-Shared Key: sysops2024sysops2024

Gegenseite SOPHOS:

- Was bietet uns die SOPHOS auf der Gegenseite an, was gehen würde …
    - …

Chriz will erstmal ein Erfolgserlebnis, darum nehmen wir jetzt die festen IP Adressen …

SOPHOS:

- New Remote Gateway
    - Add network Definition
        - Name: DMZ-WS
        - IPv4 address: 192.168.66.0
        - <save>

        - Name: loftdmzws
        - Gateway: office.sysops.de —> Stand noch zur Verfügung
        - Authenticaton Type: Preshared key
        - Key: <heraus kopierten> einfügen
        - Repeat: <heraus kopierten> einfügen
        - VPN ID type: IP address
        - Remote networks:

OPNSense

        - Fortsetzen der Konfiguration / Ändern Remote gateway
            - Dead Peer Detection: Haken setzen —> eingeschaltet - nur bei OPNSense zu OPNSense
            - Dead Peer Detection: Haken setzen —> AUS - bei OPNSense zu SOPHOS
            - Lifetime: 7800 —> bei SOPHOS - wichtig muss eingetragen sein
            - <save>
            - <apply>

        - Netz kommen die Netze
            - VPN: IPsec: Tunnel Settings [legacy]
                - Address:
                    - Type: DMZ-subnet
                    - Remote Network

                - + / Add

SOPHOS:

- Wir brauchen ein neues Netzwerk
  - Name: Workshop
  - Type: Ethernet
  - Hardware: eth3 —> nehme eine freie Netzwerkkarte, vorher eine freigemacht
    - Wir haben keine Karte mehr übrig - löschen etwas: eth3 Pandora
  - IPv4 address: 192.168.65.1
  - IPv4 netmask: /24 (255.255.255.0)
  - IPv4 default GW: kein Haken setzen —> brauchen wir nicht
  - <save>
    - New Interface
    - Interface muss eingeschaltet werden

OPNSense

- Fortsetzen der Konfiguration / Ändern Remote gateway
- Netz kommen die Netze
  - VPN: IPsec: Tunnel Settings [legacy]
    - Address: 192.168.67.0
      - Zweites Feld: /27
    - Type: DMZ-subnet
    - Remote Network
  - Phase 2 Proposal (SA/Key Exchange)
    - Encryption algorithms: AES256
    - Hash algorithms: SHA256 —> MD5 nicht mehr auswahlbar - SOPHOS was passendes finden …
  - + / Add

SOPHOS:

- Policy - AES-256-PFS
  - IKE authentication algorithm: SHA2-256 —> Zukunft sicher
  - IPsec authentication algorithm: SHA2-256 —> Zukunft sicher
  - IPsec PFS group: Group 1: MODP 2048 —> eine Gruppe höher gestellt

OPNSense

- Fortsetzen der Konfiguration / Ändern Remote gateway

        - Netz kommen die Netze
            - Phase 2 Proposal (SA/Key Exchange)
                - PFS key group: 14 (2048 bits)
                - Lifetime: 3600

            - VPN: IPSec: Tunnel Settings [legacy]
                - Hash algorithm: SHA256
                - DH key Group: 14 (2048 bits)

            - + / Add
            - <save>
            - Zurück auf die 1. Phase gehen und die Anpassungen durchführen
            - <save>
            - <apply>

SOPHOS:

- 2.Phase
    - Name: WS
    - Remote gateway: loftdmzws
    - Local Interface: external
    - Policy: AES-256-PFS —> normaler kopieren und dann editieren
    - Local Networks:
        - Workshop (Network)

    - Automatic firewall rules: haken davor gesetzt
    - <save>
        - New IPsec Connection

- Jetzt schauen wir ob es schon passt
    - IPsec Connection hat er schon angeschaltet

- Site-to-Site VPN Tunnel Status
    - Da geht noch nichts - dann prüfen wir das gleich

OPNSense

- Falsche Subnet Mask /27 gesetzt in der Phase 2
    - 192.168.67.0
    - /24

    - <save>
    - <apply>
        - Anpassung der Subnet Mask

SOPHOS und **OPNSense** Ansichten müssen aktualisiert werden

OPNSense

- VPN: IPsec: Status Overview
    - Status links ist jetzt grün geworden
        - Rechts gibt es einen Play Button für reconnect
        - Die 2. Phase wird noch nicht angezeigt

SOPHOS

- SOPHOS will noch gar nichts davon wissen - alles rot

OPNSense

- VPN: IPsec: Log File
    - Evtl. über Multiselect alle Level auswählen, um etwas zu sehen

SOPHOS

- Button Log File - geht im neuen Fenster —> evtl. versteckt sich das Fenster

Preshared Key von der OPNSense auf die SOPHOS nochmal kopiert

Auch nach die Änderung des Preshared Keys hat nicht gebracht, die IPsec Verbindungen werden nicht komplett aktiv.

Problem der Ursache gerade nicht bekannt.

Wir schauen uns jetzt ein erfolgreiche Verbindung an, die gestern konfiguriert wurde.

OPNSense

- VPN: IPsec: Status Overview
    - Dort sehen wir gerade keine zweite Phase ==> Tunnel steht nicht - Test über ping
    - IPSec Verbindung über Play Button gestartet und die zweite Phase wird angezeigt

- Andere Seite auch noch mal angeschaut und dort gibt es auch eine zweite Phase
- Manchmal funktioniert der ping noch nicht, dann ping stoppen und wieder starten

OPNSense - DynDNS

- Services: Dynamic DNS: Settings
  - Edit **VDSL Eintrag**
    - Relativ einfach:
      - Check ip method: **Interface (IPv4)**
  - Edit **DynDNS Eintrag**
    - Check ip method: **loopia** —> Damit hat Chriz gute Erfahrungen gemacht
    - Current IP darf keine private Adresse der Fritz!Box stehen

IPSec funktioniert immer in beide Richtungen

Bein OPENVPN und WireGuard braucht nur eine Richtung für den Aufbau funktionieren.

2. **WireGuard**

Wir löschen die IPSec Verbindung und wollen sie durch WireGard ersetzten

Bei WireGuard ist die SOPHOS raus.

WireGuard site-to-site

- WireGard ist Multiprozessor fähig und mehrere Prozesse
- Server: das ist die Instanz
- Gegenstelle: das ist die Peer

OPENSense Kunde

- VPN: IPsec: Connections - Auf beiden OPNSensen löschen
  - Die zweite Phase löscht sich automatisch
  - Oberste Verbindung löschen (Phase 1), aber schauen, dass man die richtige löscht
  - Enable IPsec: Haken entfernen —> IPsec aus machen
  - <apply>
- VPN: WireGuard

    - \+ / Add
        - Name: sysops
        - Public key: —> Public key von der „Gegenstelle“ also vom Server / Instance
        - Pre-shared key: Zahnrad drücken —> erzeugt den Pre shared key in einen neuen Feld —> beide Seiten identisch
        - Allowed IPs: —> ip der Gegenstelle intern plus Netze
        - Endpoint address: —> interne Adresse
        - Endpoint Port: —> Port

    - Man muss erstmal eine Instanz erzeugen
    - \+ / Add
        - Public key: <erzeugter Public key>
        - Private key: <erzeugter Private key>
        - Name: sysops-rz
        - Public key: Zahnrad erzeugt Public und private key in zwei Feldern
        - Listen port: 52451
        - Tunnel address: 172.16.12.2/32 —> wir brauchen ein Netz, was es auf beiden Seiten noch nicht gibt - muss erst noch herausgesucht werden - gefunden: 172.16.12.0
        - <save>
    - Reiter: Peers —> Gegenstelle
    - Reiter: Peer generator —> **Client Einwahl**
    - Reiter: Instances
- Im Suchfeld (Lupe): routes
    - System: Routes: Status —> **zeigt keine IPsec Netze an !!!**
        - Hier kann man nach vorhanden Netze in der Liste der Netze suchen
    - Das gleiche muss auf der Gegen OPNSense auch geschaut werden
        - **IPSec Netze** werden **nicht angezeigt**, sonder nur WireGard Netze
    - Netz: 172.16.12. als freies Netz gefunden —> Ist oben schon eingetragen

OPENSense OPNrz

- VPN: WireGuard
    - \+ / add
        - Public key: Zahnrad erzeugt Public und Privat key in zwei neuen Feldern
            - Public key: <erzeugter Public key>
            - Private key: <erzeugter Private key>
        - Listen Port: 52451
        - Tunnel Address: 172.16.12.1/32
        - <save>
        - <apply>

        - Name: Leister

    - Reiter: Instances

OPENSense Kunde

- VPN: WireGuard
    - + / add
        - Name: sysops
        - Public key: <public key OPNsense opnrz>
        - Pre-shared key: <pre-shared Key OPNSense opnrz>
        - Allowed IPs: 10.0.0.0/24
        - Endpoint address: opnrz.sysops.de
        - Endpoint Port: 52451
        - Instances: sysops-rz
        - Keepalive internal: 25
        - <save>
        - <apply>

    - Reiter Peers

OPENSense OPNrz

- VPN: WireGuard
    - + / add
        - Name: Leister
        - Public key: <public key OPNsense Kunde>
        - Pre-shared key: <pre-shared Key OPNSense Kunde>
        - Allowed IPs: 192.168.50.0/24
        - Endpoint address: leister.dyndns.ws
        - Endpoint Port: 52451
        - Instances: Leister
        - Keepalive internal: 25
        - <save>
        - <apply>

    - Reiter: Peer

OPENSense Kunde

- VPN: WireGuard: Status
    - Zeile in Status braucht einen Handshake fehlt noch …

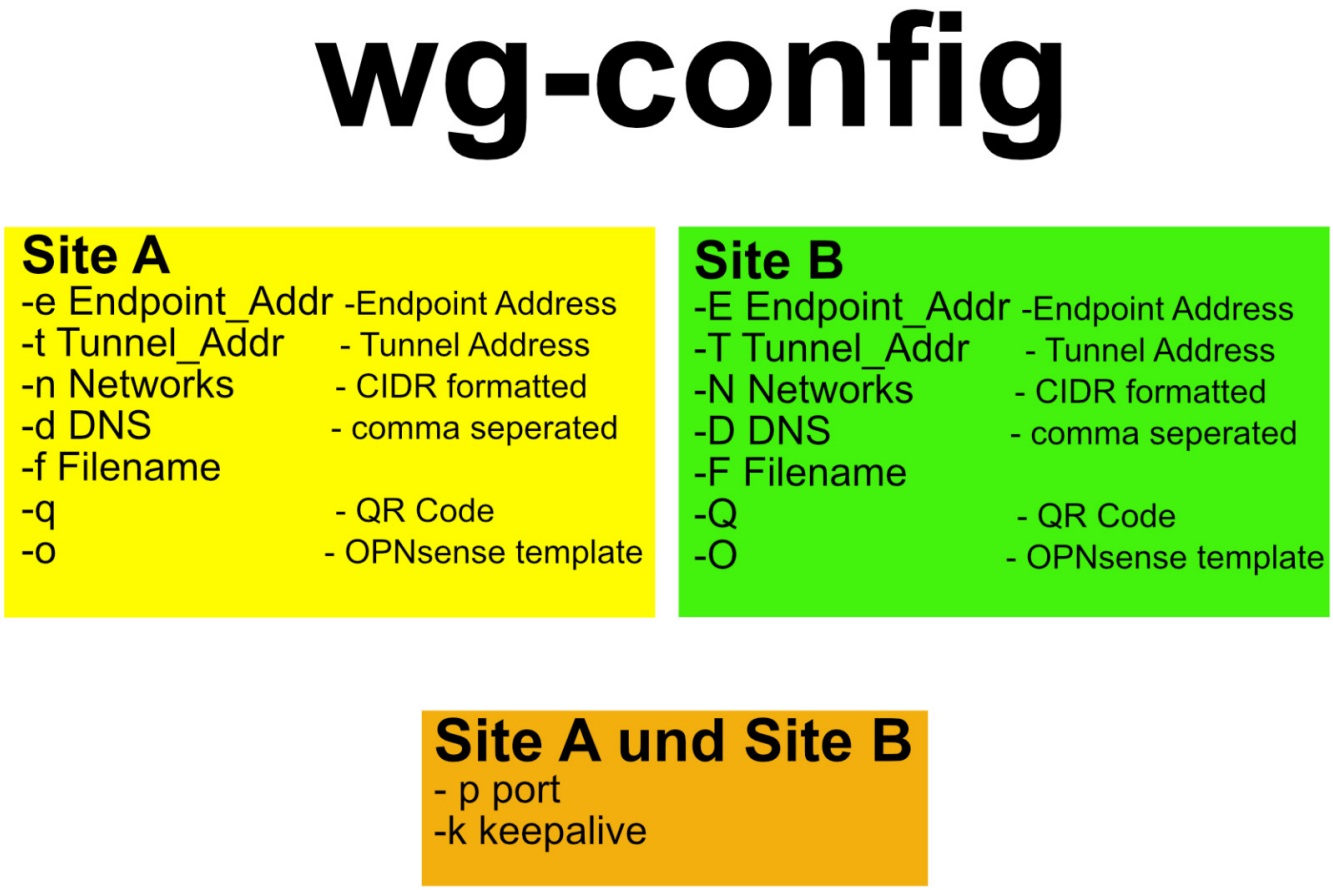
- Firewall: Rules: WireGuard (Group)
    - <save> —> d.h. im WireGuard ist alles offen

- + / add

Frage: Wie geht es einfacher ?

Browser:

- GitHub.com/bashclub
  - Nimmst die Installationsanleitung
    - Wg-config



Du gehst auf eine Linux Kiste

CLI:

- ```
  apt install wireguard qrencode
  wget -O /usr/local/bin/wg-config \
  https://git.bashclub.org/bashclub/wg-config/raw/branch/main/wg-config
  chmod +x /usr/local/bin/wg-config
  wg-config -h
  clear
  ```
  ```

```
wg-config —help
wg-config -e oparz.sysops.de -E leister.dyndns.ws - t 172.16.12.1/32 \
-T 172.16.12.2/32 -d 1.1.1.1 -n 192.168.50.0/24 -N 10.0.0.0/24
Erzeugt eine WireGard Config und zeigt diese an
wg-config -e oparz.sysops.de -E leister.dyndns.ws - t 172.16.12.1/32 \
-T 172.16.12.2/32 -d 1.1.1.1 -n 192.168.50.0/24 -N 10.0.0.0/24 -o -O
# Ausgabe im OPNSense Format
```

Jetzt macht man nur noch Copy & Paste - ist doch viel einfacher - wichtig alles kopieren und nicht das letzte Zeichen vergessen

OPENSense OPNrz

- VPN: WireGuard
  - + / add
    - Public key: Zahnrad erzeugt Public und Privat key in zwei neuen Feldern
      - Public key: <erzeugter Public key>
      - Private key: <erzeugter Private key>
    - Listen Port: 52451
    - Tunnel Address: 172.16.12.1/32
    - Peer: Leister
    - <save>
      - Name: Leister
  - Reiter: Instances

OPENSense OPNrz

- VPN: WireGuard
  - + / add
    - Name: Leister
    - Public key: <public key OPNsense Kunde>
    - Pre-shared key: <pre-shared Key OPNSense Kunde>
    - Allowed IPs: 192.168.50.0/24
    - Endpoint address: leister.dyndns.ws
    - Endpoint Port: 52451
    - Instances: Leister
    - Keepalive internal: 25

        - <save>
        - <apply>

    - Reiter: Peer

OPENSense Kunde

    - Reiter: Instances
        - Name: sysops-rz
        - Public key: Zahnrad erzeugt Public und private key in zwei Feldern
            - Public key: <erzeugter Public key>
            - Private key: <erzeugter Private key>

        - Listen port: 52451
        - Tunnel address: 172.16.12.2/32
        - Peer: sysops
        - <save>
            - + / Add

OPENSense Kunde

- VPN: WireGuard
    - + / add
        - Name: sysops
        - Public key: <public key OPNsense opnrz>
        - Pre-shared key: <pre-shared Key OPNSense opnrz>
        - Allowed IPs: 172.16.12.1/32 192.168.50.0/24
        - Endpoint address: opnrz.sysops.de
        - Endpoint Port: 52451
        - Instances: sysops-rz
        - Keepalive internal: 25
        - <save>
        - <apply>

    - Reiter Peers

OPENSense OPNrz

- Im Suchfeld (Lupe): Live
    - WireGard Port wird geblockt
        - Firewall: Log Files: Live view

- Im Suchfeld (Lupe): WAN

    - Regel Clones und Anpassen
        - Destination Port range:
            - From: 52451
            - To: 52451
        - Description: wg Leister
        - <save>
        - <apply>
            - Edit
        - Firewall: Rules: WAN

OPENSense Kunde

- Im Suchfeld (Lupe): Live
    - WireGard Port wird nicht geblockt —> es scheint das die neuere OPNSense die WireGard Ports von selbst auf machen - Chriz ist sich nicht sicher
    - Immer noch nicht OK
        - Firewall: Log Files: Live view
        - VPN: WireGuard: Status

Überprüfung der WireGuard Config.

Ein Pre-Shared key war falsch, aber funktioniert immer noch nicht.

Nochmal überprüft im Live Log beider OPNSense das der Port nicht blockt wird. Keine Block Meldungen gefunden.

Wir machen die Config noch mal neu.

Jetzt wird alles aus wg-config kopiert außer dem Port 52451

CLI:

- wg-config -e oparz.sysops.de -E leister.dyndns.ws - t 172.16.12.1/32 -T 172.16.12.2/32 -d 1.1.1.1 -n 192.168.50.0/24 -N 10.0.0.0/24 -o -O -p 52451
    - Ausgabe im OPNSense Format

Mit dieser Ausgabe können wir jetzt wirklich copy & Paste machen - wir generieren nichts

Bei DynDNS braucht man auf der DynDNS Seite bei Peer keine Endpoint Address eintragen, es **reicht auf einer Seite**.

OPENSense Kunde

- VPN: WireGuard: Status
    - Sieht man das es jetzt geklappt hat —> Handshake ist jetzt da

Der ping funktioniert auch wieder !!!

Braucht man mehrere braucht trägt man die im Peer eine weitere Netz unter Allowed IPs ein. Die Paket Filter müssen auch passen.

Wichtig bei Tunnel Address muss die Subnet Mask eingegeben werden, sonst sucht man eine Fehler der nicht da ist !!! (War in der Instance)

Hinweis: WireGuard Regeln müssen erstellt werden

- Firewall: Rules: WireGuard (Group)

3. **OpenVPN Einwahl - Roadwarrior**

Mit IPsec und Einwahl ist nicht geil, gibt kaum clients.

OPNSense

- OPNSense hat ein neues FrontEnd für OpenVPN, die Software hinten dran ist die selbe
- VPN: OpenVPN: Instances
    - Reiter Instances

- Wir nehmen Legacy
- VPN: OpenVPN: Servers [legacy]
    - Server Mode:
        - **Peer to Peer** —> **wäre Site-to-Site** —> Chriz: besser bedient mit IPSec und WireGuard

        - SSL/TLS
        - Shared Key
    - **Remote Access**
        - SSL/TLS —> Zertifikat —> **CA**
        - User Auth
        - SSL/TLS + User Auth
    - Sprung zum anderen Bereich
        - Verschiedene Auswahl Möglichkeiten:
    - + / add

- System: Trust: Authorities
    - Descriptive Name: vpn_ca
    - Method: Create an internal Certificate Authority
    - Key Type: RSA
    - Key length (bits(: 4096
    - Digest Algorithm: SHA256
    - Lifetime (days): 9999 -> Chriz macht immer 9999
    - Country Code: DE (German)
    - State or Province: by —> Was Du hier reinschreibst - siehe keine, gilt auch für die folgenden Felder
    - City: ab
    - Organization;: sysops
    - Email Address: christian@sysops.de
    - Comman Name: vpn-ca
    - <save>
    - + / add
        - Method: Create an internal Certificate
        - Descriptive name: vpn_cert
        - Certificate authority: vpn_ca
        - Type: Server Certificate
        - Key Type: RSA
        - Key length (bits): 4096
        - Digest Alorithm: SHA256
        - Lifetime (days): 9999
        - Private key location: save on this firewall
        - Common Name: vpn_cert
        - <save>
    - + / add
    - System: Trust: Certificates

OPNSense

- Im Suchfeld (Lupe): Server
  - + / add
    - TLS Authentication: Enabled - Auhtetication only
    - TLS Shared Key: Automatic generate a share TLS authentication key - Standard Haken gesetzt
      - Man kann auch seinen eigenen Eintragen
    - Peer Certificate Authority: vpn_ca
    - Server Certificate: vpn_cert (vpn_ca)
    - Encryption algorithm (depicted): None —> am besten frei lassen - es wird ausgehandelt
    - Auth digest Algorithm: SHA256 (256 bit)
    - IPv4 Tunnel Network:172.16.13.0/24
    - IPv4 Local Network: 10.0.0.0/24
    - Compression: Legacy - Disabled LZO algorithm (--comp-lzo no) —> macht man auch nicht mehr
      - Standard: No Preference
    - Duplicate Connections: Haken setzen
      - Description: Roadwarrior
      - Server Mode: Remote Access (SSL/TLS + Auth User) —> evtl. später 2 FA
      - Backend for authentication: Local Database —> Zur Zeit nur Local Database —> d.h. nur User root
      - Protocal: UDP
      - Device Mode: tun
      - Interface: WAN —> WAN hat mehr Upstream
      - Local Port: 1194
      - Cryptographics Settings:
      - Tunnel settings;
  - Client Settings —> Hängt vom Client ab, ob er drauf Block hat …
    - Server #1: 10.0.0.4
    - Server #2: 1.1.1.1
      - DNS Default Domain: leister-schuhe.local
      - DNS Domain search List: leister-schuhe.local
      - DNS Servers:
  - VPN: OpenVPN: Servers [legacy]
  - <save>

SOPHOS

- War sehr schön gelöst gewesen - vorbildlich
- Site-to-site VPN

    - SSL
        - Encryption algorithm: AES-128-CBC
            - Problem Werte sind zu alt und müssten neu gemacht werden, d.h. jeder Client braucht ein neues Zertifikat
            - CBC ist seit einen Jahr auf dem iPhone nicht mehr möglich - das war das Ende von SOHOPS und iPhone, deshalb wird bei der OPNSense diese Feld mittlerweile leer gelassen

        - Reiter Profiles
        - Reiter Settings
        - Reiter Advanced

    - Remote Access

- Egal wieviel Du klickst, da ist eine Instanz mit einen Kern

OPNSense

- Im Suchfeld (Lupe): WAN
    - + / add
        - From: 1194
        - To: 1194
            - Protocol: UDP —> wichtig !
            - Destination port range:
            - <save>

    - Firewall: Rules: WAN

- Im Suchfeld (Lupe): Export
        - VPN: OpenVPN: Client Export
            - Remote Access Server: Roadwarrior UDP:1194
            - Export type: File only
            - Hostname: leister.dyndns.ws —> Ich trage die Internet Adresse ein
            - vpn_cert: hinten download Button drücken

Mac von Chriz:

- Finder —> Windows Explorer für Windows User
    - Roadwarrior_vpn_cert.ovpn
    - Open with … - OpenVPN Connect

    - Download

- OpenVPN connect
    - User: root
    - Password: <passwort von root>
    - <CONNECT>
    - <Schalter> auf ON stellen
    - Verbindung geht noch nicht
    - Troubleshooting
        - Import Profile

OPNSense

- Im Suchfeld (Lupe): Log
    - Fehlermeldung im Browser googeln
    - Edit
        - Encryption algorithm: AES-256-GCM —> Hat Chriz die letzten Jahre genommen, eigentlich soll man es leer lassen - Test, ob es daran liegt
        - <save>

    - VPN: OpenVPN Log File
    - VPN: OpenVPN: Servers [legacy]

- Wenn man seine Reihenfolge im Kurs ändert …
- Im Suchfeld (Lupe): User
    - Root User - Edit
        - + / add
            - Method: Create an internal Certificate
            - Key length (bits): 4096
            - Lifetime (days): 9999
            - <save>

        - User Certificates:

    - System: Access: Users —> **für jeden User wird ein eigenes Zertifikat benötigt, auch für alle LDAP User - das geht nicht automatisch**

- Danach sieht man im User das User certificate(s), dass wir gerade erzeugt haben
- Im Suchfeld (Lupe): Export
    - Root
        - <Download>

    - Certificate

Browser download

- Zertifikate auswählen und anklicken
- Wird in derApplikation geöffnet
    - <Retry>
    - <cancel>
    - Username: root
    - Password: <password root>
    - <CONNECT>
    - <Schalter> auf ON stellen
    - Verbindung klappt

CLI

- traceroute -d 10.0.0.4 ==> keine Antwort
- ping 10.0.0.4 ==> keine Antwort

OPNSense

- Im Suchfeld (Lupe): live
- Firewall: Log Files: Live View
    - 10.0.0.4 —> icmp
    - Block Regel erweitern und unter neuen Namen speichern
        - Portname is icmp
        - + / neue Regel machen
        - Name eingeben: block ping <Return / Enter> oder Diskette anklicken

    - Block

- Im Suchfeld (Lupe): openvpn
    - + / add
        - <save> —> Chriz: Ich erlaube erstmal alles
        - <apply>

    - Firewall: Rules: OpenVPN

CLI

- traceroute -d 10.0.0.4 ==> Antwort
    - Geht über das Transfer Netz: 172.16.15.1
    - Zum Ziel: 10.0.0.4

- ping 10.0.0.4 ==> Antwort

Bei Chriz: kein VPN sondern eine Bridge zum RZ

Jetzt mit LDAP oder Windows AD

OPNSense

- Im Suchfeld (Lupe): user
- System: Access: Server
  - Descriptive Name: LDAP-UCS
  - Type: LDAP —> wir machen jetzt nur LDAP ohne 2 FA
  - Hostname or IP address: 10.0.0.4
  - Port value: 7389 —> Standardwert: 389 Windows AD
  - Bind credentials:
    - User DN:
    - Password:

  - \+ / add

Browser UCS Server

- 10.0.0.4
  - Users
    - Einfaches Authentiisierungskonto
    - <weiter>
    - Benutzername: ldapopn
    - Passwort: <ldapopn Password>
    - Passwort (Wiederholung): <ldapopn Password>
    - <LDAP-Object erzeugen>
      - Neues LDAP-Objekt hinzufügen

  - System- und Domäneinstellungen —> Chriz: Bei UCS ist es besonders schön
  - LDAP-Verzeichnis

CLI UCS Server

- ssh root@10.0.0.4
- univention-ldapsearch --LLL uid=ldapopn
  - dn: **uid=ldapopn,cn=users,dc=leister-schuhe,dc=local** —> Bei Windows ist vorne ein cn=ldapopv

OPNSense

- Im Suchfeld (Lupe): user

- System: Access: Server
  - Descriptive Name: LDAP-UCS
  - Type: LDAP —> wir machen jetzt nur LDAP ohne 2 FA
  - Hostname or IP address: 10.0.0.4
  - Port value: 7389 —> Standardwert: 389 Windows AD
  - Bind credentials:
    - User DN: **uid=ldapopn,cn=users,dc=leister-schuhe,dc=local**
    - Password: <ldapopn Password>
  - Base DN: cn=users,dc=leister-schuhe,dc=local
  - Authentication containers: <select> Button anklicken
    - cn=users,dc=leister-schuhe,dc=local
    - <save>
    - Es wird in das Feld davor übernommen
      - cn=users,dc=leister-schuhe,dc=local
    - Fenster: Please select which containers to Authenticate against:
  - User naming attribute: uid —> Standard: cn, Univention: cid
  - Read properties: Haken setzen
  - Synchronize groups: Haken setzen
  - Automatic user creation: Haken setzen
  - <save>
    - + / add
- System: Access: Tester
  - Gibt einen Output zurück das funktioniert hat + weitere Info’s zum User
    - Authentication Server: LDAP-UCS
    - Username: o.leister
    - Password: <Password>
    - <Test>

SOPHOS

- Authentifcation Services
  - Bind DN:
  - Tester
    - Username:
    - Password:
    - <Test>
  - SOPHOS hat zu einer bestimmten Zeit die User erzeugt und gleichzeitig auch die Zertifikate für die User angelegt
    - Edit LDAP
    - Advanced

An dieser Stelle kann Du Dich aussperren !

CLI

- **/etc/cron.daily/zfs-auto-snapshot**

OPNSense

- Im Suchfeld (Lupe): user
- System: Access: Server
  - —> Immer noch keine Auswahl

- Im Suchfeld (Lupe): Administration
- **Setting - Administration**
  - Server: LDAP-UCS und Local Database anklicken —> Bei Auswahl erscheint **hinter dem Eintrag ein Haken**
    - **Wählt Du nur LDAP UCS aus, hast Du Dich ausgesperrt !!! —> LDAP User haben keine Rechte auf der OPNSense**

  - <save>
  - Authentication

- Im Suchfeld (Lupe): user
  - Gibt es neben dem + Zeichen - die **Wolke**
    - Haken hinter dem Eintrag setzen
      - Erscheint ein neues Fenster aus dem Du Dir die User heraussuchen kannst
      - <save>
      - —> Die User müssen von hand importiert werden —> Kein Cron Job dafür bekannt

  - Über und unter dem root User sind die User zu sehen
  - **Jeden User einzeln editieren**
    - + Zeichen anklicken
      - Method: create an internal Certificate
      - Key length (bits): 4096
      - Lifetime (days): 9999
      - <save>

    - User Certificates

  - System: Access: Users

- VPN: OpenVPN: Servers [legacy]

    - Backend for authentication: LDAP-UCS —> anklicken —> Haken dahinter
        - LDAP-UCS
        - Local Database
        - <save>

    - Edit

- Im Suchfeld (Lupe): export
    - User suchen und auf <download Button> klicken - OpenVPN File wird heruntergeladen

Browser

- Auf den Download File klicken und in der App OpenVPN importieren
    - Username: o.leister
    - Vor Save password —> haken setzen
    - Password: <Password vom User>
    - <CONNECT>
    - —> OpenVPN funktioniert nachdem auf der LDAP_UCS für die Authentifikation eingetragen wurde

CLI

- traceroute -d 10.0.0.4
    - Zeigt wieder den gleichen Weg wie oben, Transfer Netz und dann Ziel

Jetzt kommt noch 2 FA dazu

OPNSense

- Im Suchfeld (Lupe): Server
    - Descriptive Name: LDAP-UCS 2fa
    - Type: LDAP + Timebase One Time Password —> LDAP mit 2 FA
    - Hostname or IP address: 10.0.0.4
    - Port value: 7389 —> Standardwert: 389 Windows AD
    - Bind credentials:
        - User DN: **uid=ldapopn,cn=users,dc=leister-schuhe,dc=local**
        - Password: <ldapopn Password>

    - Base DN: cn=users,dc=leister-schuhe,dc=local
    - Authentication containers: <select> Button anklicken
        - cn=users,dc=leister-schuhe,dc=local
        - <save>
        - Es wird in das Feld davor übernommen

        - cn=users,dc=leister-schuhe,dc=local

    - Fenster: Please select which containers to Authenticate against:

  - User naming attribute: uid —> Standard: cn, Univention: cid
  - Read properties: Haken setzen
  - Synchronize groups: Haken setzen
  - Automatic user creation: Haken setzen
  - Reverse token order: haken setzen —> **token after password - Standard: kein Haken token before Password**
    - **Hinweis: Damit 2 FA richtig funktioniert darf der Haken nicht gesetzt sein** - siehe weiter hinten in der Doku

  - <save>
    - System: Access: Servers
    - + / add —> Leider gibt es hier kein Clone, also komplett neu anlegen

- Im Suchfeld (Lupe): Server
  - Backend for authentication: LDAP-UCS 2fa haken setzen
    - **Wichtig: LDAP-UCS** —> Haken entfernen

  - VPN: OpenVPN: Server [legacy
  - Description: Roadwarrior - Stift (Edit) anklicken
  - <save>]

- Im Suchfeld (Lupe): User
- System: Access: User
  - OTP seed
    - Generate new secret (160 bit): Haken davor setzen

  - <save> —> und **nicht** <save and go back>
  - OTP QR Code: <Click to unhide>
    - QR Code wird angezeigt

  - Edit User z.B. o.leister

QR Code mit dem Handy in der 2 FA App einlesen

Zurück im OpenVPN Client

- Entsprechende Open VPN Verbindung editieren

    - Password Abfrage:
        - Passwort gefolgt von OTP
        - <OK>

    - Save Password muss raus - zu mindest für einen Moment
    - <save>
    - Connection aktivieren
    - Connection wieder trennen

Im Browser

- Suche: opensense openvpn ask top
    - Code: static-challenge „Please enter your OpenOTP PIN“ 1

OPNSense

- Im Suchfeld (Lupe): export
    - Custom config: static-challenge „Please enter your OpenOTP PIN“ 1
    - Hier gibt es keine <Save Button> - einmal raus aus dem Feld und es wird automatisch gespeichert !!
    - User: o.leister - <download> anklicken
        - VPN: OpenVPN: Client Export

Browser download

- Zertifikate auswählen und anklicken
- Wird in derApplikation geöffnet

Zurück im OpenVPN Client

- Import .opn profile
    - <OK>

- Username: o.leister
- <CONNECT>
    - Please enter your OpenOTP PIN
    - Response: <PIN aus der Handy App>
    - <Send>
    - Authentication failed —> **falsche Reihenfolge** …
        - Abfrage Password: <password von o.leister>
        - <OK>
        - Multi-factor authentication

OPNSense

- System: Access: Server
  - Reverse token order: Haken herausnehmen —> **kein Haken gesetzt**
  - <save>
    - LDAP-UCS 2fa - Stift (Edit)

Zurück im OpenVPN Client

- Richtige Profil auswählen
- Connect Schalter auf ON schieben
  - Password: <password von o.leister>
  - <OK>
  - Please enter your OpenOTP PIN
  - Response: <OTP PIN aus Handy App>
  - <SEND>
  - **Verbindung steht —> grün connect Button**
    - Enter Password
    - Multi-factor authentication

- Verbindung wieder trennen
- **Jetzt kann der User sein Passwort wieder im Profil speichern**
- Richtige Profile auswählen
- Edit
    - Haken vor Save Password
    - Password: <password von User o.leister>
    - <save>

- Richtiges Profil auswählen
- Connect Schalter auf ON schieben
  - Please enter your OpenOTP PIN
  - Response: <OTP PIN aus Handy App>
  - <SEND>
  - **Verbindung steht —> grün connect Button**
    - Multi-factor authentication

- Verbindung wieder trennen

4. **Bridges**

OPNSense (Bridge Server)

- Im Suchfeld (Lupe): open
- VPN: OpenVPN: Servers [legacy]
  - Description: BridgeServer
  - Server Mode: Peer to Peer (Shared Key)
  - Device Mode: tap
  - Shared key: Haken vor Automatically generate a shared key
  - Auth Digest Algorithm: SHA256 (256 bit)
  - <save>
  - Shared key: zeigt den Static key an
    - + /add
    - Edit Eintrag

- Im Suchfeld (Lupe): Assign
- Interfaces: Assignments
  - Device: opnsl (OpenVPN Server BridgeServer)
  - Description: Bridgeinterface
  - <Add>
  - Interfaces: [Bridgeinterface]
  - Enable. Haken setzen
  - **Hinweis:** Es wird nichts konfiguriert
  - <save>
  - <apply>
    - + Assign a new Interface
    - Interface [Bridgeinterace] —> Link in eckiger Klammer anklicken

- Im Suchfeld (Lupe): Bridge
- Interfaces: Other Types: Bridge
  - Member interfaces: Bridgeinterface, LAN
  - Description: Bridge
  - <save>
  - + / add

Da es gerade im Netzwerk ist, werde ich das mal ändern.

Browser

- PVE: PVE3 im RZ
  - Hardware
    - Bridge: vmbr0
    - Disconnect: Haken setzen
    - <ok>
    - Bridge: vmbr99

        - Disconnect Haken heraus nehmen
        - <ok>
            - Edit Network Device net0
            - Edit Network Device net0 - vmbr0 wird auf Tote Bridge vmbr99 umgehängt - damit da ja nichts passiert

    - opnws.sysops.de

CLI Studio

- ping 192.168.0.99 —> wird nicht mehr erreicht

Browser

- OPNSense in Aschaffenburg - office.sysops.de:4444
    - Im Suchfeld (Lupe): open
        - Clone von OPVN Bridge RZ
            - Host or Adress: openws.sysops.de
            - Port: 1194
            - Shared key: <Hier den Shared von opnws.sysops.de (Server) herein kopieren>
            - Encryption algorithm (deprecated): None —> soll er selber verhandeln
            - Auth Digest Algorithm: SHA256 (256 bit)
                - Description: OVPN Bridge WS
                - Server Mode: Peer to Peer (Shared Key)
                - Device Mode: tap
                - Interface: TelekomFTTHPPoE
                - Remote Server:
                - Cryptographic Settings
                - <save>

        - Man sieht an den Bytes Sent und Bytes Received das die beiden Verbunden sind
            - VPN: OpenVPN: Clients [legacy]
            - VPN: OpenVPN: Connection Status

    - Im Suchfeld (Lupe): assig
        - Device: opnc3 (OpenVPN Client OVPN Bridge WS
        - Description: OVPNBridgeWS
        - <add>

        - Interfaces: Assignments
        - + Assign new interface

    - Interface: [OVPNBrigdeWS] - anklicken
        - Enable: Haken setzen
        - **Hinweis:** es wird nicht konfiguriert
        - <save>
        - <apply>

    - Im Suchfeld (Lupe): Bridge
        - Edit
            - LAN, OVPNBridge, OVPNBridgeWS
            - <save>

        - Interfaces: Other Types: Bridge

    - **OPNSense (Bridge Server)**

CLI

- ping 192.168.0.99 —> geht nicht, vermutlich eine Kleinigkeit übersehen

Es bringt nichts, da ich keine Standorte habe mit denen ich das Testen kann.

Rückabwicklung der Bridge

Chriz zeigt es nochmal am Beispiel RZ.

SOPHOS

- Redboxen sind die Clients
- Evtl wird noch ein LAN da gesteckt, damit die alle in einen Netz sind

Hinweis von Chriz: Es gibt einen alias Typ **OpenVPN group**, aber hat sich Chriz noch nicht weiter angeschaut. Damit kann man Regeln auf User Ebene machen. (IP Address) Chriz nutzt die Group nicht.

Unter Firewall: Diagnostics: Aliases sieht man die eingewählten IP Adressen.

Im Stammtisch gab es die Frage, ob das auch mit LDAP funktioniert.

LDAP Gruppen können vermutlich nicht importiert werden, damit können die auch nicht OpenVPN group verwendet werden.

Es kann nur eine local Gruppe angelegt werden und dort können die LDAP User hinzugefügt werden.

Und dann kann man einen Alias machen.

10. **Mailgateway**

SOPHOS

- Email Protection
    - SMTP
    - SMTP Profiles

ProxMox Mail Gateway müssen wir raus NATen, wir schauen das mal bei uns an.

Browser

- Opensense RZ
    - Quelle: Internet
    - Ziel: Mail Gateway
    - Port für Quelle und Ziel gleich
        - Port: 8006 —> Web Interface
        - Port: 26 —> Port 26 muss nicht zwingend nach draußen gelegt werden, über den Port werden die Mail raus geschickt, je nachdem wie Du aufgestellt bist
        - Port 25

    - Im Suchfeld (Lupe): nat
    - Firewall: NAT: Port Forward

ProxMox

- Local Data Store
    - Reiter Templates
        - Template wird heruntergeladen
            - ProxMox Mail Gateway Version …
            - Download

    - CT Templates

- Create Container

    - CT ID: 101
    - Hostname: pmgtest
    - Password: <password>
    - Confirm password: <password>
    - <Next>
    - Template: ProxMox Mail Gateway auswählen

Die Installation des ProxMox Mail Gateways sollte jeder hin bekommen, Chriz spart sich die Installation.

Browser

- ProxMox Mail Gateway im Browser mit dem Port 8006 aufrufen
    - Einrichtung: Bilder zur Einrichtung
    - Dazu gibt es ein Video, das wird gleich in die Themenstruktur aufgenommen
        - Einrichtung dauert min. 1 Stunde
            - Die Bilder zeigen das stupide Einrichten des Mail Gateways

    - Configuration
        - Reiter Relaying
        - Reiter Domains —> diese Domain relayen wir
        - Reiter Ports —> Hier können die Ports angepasst werden
            - Bei Chriz ist mehr auf dem UCS los
            - tail .f /var/log/mail.log
                - Test Mail nach außen geht über das ProxMox Mail Gateway und es geht an den Mail Piler

            - Beispiel Leister UCS: mail/relayhost: 192.168.50.253:26

        - Reiter options
            - Message Size (bytes) —> Mail Größe für eingehende und ausgehende Mail - Empfehlung 10 MB
            - DNSBL Sites: —> weniger ist mehr …
            - Use Greylisting for IPv4: yes —> Mehrfach Anfragen
            - Use SPF: yes —> SPF Record muss vorhanden sein
            - SMTPD Banner: -> so meldet sich unser Server

        - Reiter Transports —> Server Eintrag wohin die Domain gehen soll - kein MX - **eingehend**
            - Host: —> eintragen
            - Protocol: SMTP
            - Port: 25

        - Use MX: kein Haken setzen

    - Reiter Networks —> für das Relayen von eben - kannst Du nur an **Port 26 schicken**, wenn es in der Liste steht
    - Reiter TLS —> gibt es in der Webseite und im SMTP Server
        - Enable TLS: yes
        - Enable TLS Logging: yes
        - Add TLS receiver header: yes

    - Reiter ACME Accounts/Challenges
        - Hetzner
        - Zertifikat für Web Oberfläche
        - Zertifikate für SMTP
            - Challenge Plugins
            - Certificates

    - Reiter DKIM
        - Mail wird raus geschickt und mit DKIM signiert
        - Empfänger vergleicht den DKIM mit dem DNS Eintrage der Domain

    - Reiter Whiteliste —> Wunderbar Whitelisten
        - Mail Proxy —> der wichtigste Part
        - Certificates —> Wer sich erinnert Hetzner Plugin
        - Mail Proxy —> zurück zum Mail Proxy - restliche Reiter

- User Management
    - Nur **Whiteliste** zu pflegen oder eine **Quarantäne Mail** freizuschalten
        - Reiter LDAP

- Virus Charts
    - Avast —> ist gut (findet Betrugsmaschen), ist aber sehr teuer und zickig - findet viel mehr als clam AV

- Reiter Summary
    - Hängen hier Sachen
    - Button <Flush Queue>

- Reiter Deferred Mail —> wo geht das Zeug hin
- Filter: ...
    - Dann sieht man was da hängt

    - Einloggen
    - **Hinweis:** In der Themenstruktur findet man die ganzen Bezüge dafür
    - Wir schauen uns an was es bedeutet
    - Mail Filter —> Hier würde Chriz nichts verändern, er ist damit gescheitert

- Cluster —> Du kannst das PMG sehr geil Clustern
- Subscription —> Hab ich auch
- Statitistics
- Queues
- Tracking Center —> wissen was passiert ist
- User Whitelist —> Mail kann Whiteliste hingefügt werden
- User Blacklist —> Mail kann aber auch der Blackliste hinzugefügt werden
- **Hinweis:** Über die Quarantäne Mail kann auch ohne Web Login auf die Blacklist oder Whiteliste eingestellt werden

SOPHOS

- Gab es den geilen Mailmanager, den gibt es im PMG nicht

Version #1
Erstellt: 29 Oktober 2024 16:40:36 von Udo Huber
Zuletzt aktualisiert: 29 Oktober 2024 16:40:36 von Udo Huber