Workshop OPNsense

OPNSense

Inhaltsverzeichnis

1. Allgemein

1.1. 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: <Harken 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: <Harken 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: <Harken setzen>

• Discard: <Harken 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: <Harken 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: <Harken 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

• 2 —> Set Interface IP address

• 1 —> LAN

• 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

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

• <Next> Button

• *Einschub: Thema VDSL*

• General Information

• 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: <Harken entfernen> - Allow DNS servers to be overwritten by DHCP/PPP on

WAN

• Enable Resolver: <Harken gesetzt lassen>

• <Next> Button

• Time Server Information

• Timezone: Amsterdam oder Berlin auswählen oder bei UTC belassen

• <Next>-Button

• Configure WAN Interface

• IPv4 Configuration Type: PPPoE

• PPPoe Configuration —> *Wir werden es nicht benutzen*

• PPPoe Username: 123456789012012345678901200001@t-online.de

• PPPoe Password: 123123

• RFC1918 Networks

• Block RFC1918 private Networks: Harken standardmäßig gesetzt

• Block boron networks: Harken standardmäßig gesetzt

• **Anmerkung Fritz!Box**: Für Fritz!Box die beiden Harken entfernen

• <Next>-Button

• Configure LAN Interface

• <Next>-Button

• Set Root Passwort

• <Next>-Button

• Reload Configuration

• <Reload>-Button —> Button nicht gedrückt !!!

• Unter Interface - Point-to-Point - Devices

• Ein Point-to-Point Device - vtnet1

• Interface - Other Types - VLAN

• + —> Add

• Edit VLAN —> Sophos -DSL (PPPOE) - mit VDSL

• Device: vlan0.7

• Parent: vtnet1

• VLAN tag: 7

• Description: VDSL

• <Save>-Button

• <Apply>-Button

• Interface - Point to point - Devices

• Link interface(s): vlan0.7

• <Save>

• ==> Hardware OPNsense mit PPPoE

• Interface - Point-to-Point - Log File

• Debug

Einschub: Thema VDSL

• PVE GUI:

• VM: OPNSense (ID: 9999)

• Network Device

• VLAN Tag: 7

• Ergänzung: Tag 1 (Telefon), Tag 2 (TV) —> oder so was …

•

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

• [LAN] lan vtnet0 —> in Klammern wird die MAC Adresse angezeigt

• [WAN] WAN pppoe (missing)

• Ändern auf vtnet1 —> in Klammern wird die MAC Adresse angezeigt

• MAC Adressen im ProxMox kontrollieren

• <Save>

• [WAN] ist ein Link auf Interfaces: [WAN]

• Basic configuration

• Lock: <Harken 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 ...

• Subnet mask: 24 —> Feld neben IP Adresse

• <Save>

• <Apply>

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: <Harken 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

• Edit Virtual IP

• Mode: IP Alias —> CARP könnte früher nicht mehr geändert werden

• Interface: WAN

• Network / Adress: 194.30.174.106/24

• Description: Alternative IP Workshop

• <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: <Harken 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 harken gesetzt werden - Bei Bedarf

Im Suchfeld (Lupe): alias

Im anderen Browser Tab: Goo

• Blocklisten

•firehol_level1:

• Local copy: download local copy —> diesen Link kopieren

•firehol_level2:

Wieder **zurück im Webbrowser der OPNsense**

Firewall: Aliases

• + - Add

• Edit Alias

• 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

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

• Firewall:Rules: WAN

• Action: Block

• Log: <Harken bei Bedarf>

• Source: Firehol_L1

• Description: Firehol L1

• <Save>

• <Apply>

Was ich immer machen würde:

• Block Regel

• Harken 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

• Search Geo

• Edit Alias

• Unwanted Geolocations

• z.B. Afrika

• Alias kann in einer Firewall Rule als Block definiert werden

• In der freien Version muss man über einen Drittanbieter gehen …

5. OPNsense GUI

-

Basiseinrichtung

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

• + - add

• 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>

Sophos - Firewall - rules

—> gibt es so nicht in der OPNsense

Regel in der OPNsense im RZ angeschaut

• Firewall: Rules Firma X

• 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

• 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

Chriz erklärt es noch mal anders:

• Firewall: rules: LAN

• + - add

• <save>

• <apply>

• Damit wird eine Regel erstellt mit der man alles darf

• **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

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

Basis Setup:

Wieder **zurück im Webbrowser der OPNsense**

• System: Settings: Administration

• Protocol: HTTPS - ausgewählt

• TCP port: 4444 - 443 wollen wir später für was cooles haben, wir machen mal einen neuen Port 4444

• HTTP Redirect: Harken 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: Harken setzen (enable)

• Listen interfaces: ALL

• Secure Shell Server: Harken setzen - enable

• Root Login: Harken setzen - permit root user login

• Authentication Method: Harken ***nicht*** setzen - ***disable*** permit password login - kein Passwort Login

• Listen Interfaces: ALL

• Authentication

• Server: Local Database - auswählen, das hilft - vorher **Nothing selected**

• <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

• Root user —> Edit (Stift)

• Authorized keys: public key des ssh key hinterlegen (System das Zugriff haben soll z.B. Laptop)

• <save>

CLI:

• ssh root@opnws.sysops.de

• Passwort loser Zugriff per CLI

Wieder **zurück im Webbrowser der OPNsense**

• System: Settings: Administration

• OTP seed: Hier könnte man jetzt noch one time password setzen / konfigurieren —> machen wir später

• Chriz zeigt es doch schon:

• OTP seed: harken setzen —> Generatenew secret (160 bit)

• <save and to back>

• OTP QR Code: <Click to unhide>

• 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

• 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.

Plugins:

Im Suchfeld (Lupe): Plugins

• System: Firmware

• Reiter: Plugins

• 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

Im Suchfeld (Lupe): firmware

• System: Firmware

• <check for updates>

• Info zum Update bestätigen

• <update> - meist wird ein reboot benötigt - manchmal bootet er sogar 2 mal

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**

• + / add

• Minutes: 0

• Hours: 0

• Command: Firmware update check

• Description: C —> wie check

• <save>

• <apply>

• + / add

• 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

• Reiter: Plugins

• Unter der Reiterleiste gibt es den Punkt **Name** —> Suche (Eingabe zur Suche des Plugins)

• acme

• os-acme-client —> + Zeichen anklicken

• Reiter: Plugins

• Unter der Reiterleiste gibt es den Punkt **Name** —> Suche (Eingabe zur Suche des Plugins)

• Next

• Os-nextcloud-backup —> + Zeichen anklicken

• WireGuard war früher ein Plugin, ist jetzt fest drin

• Reiter: Plugins

• Unter der Reiterleiste gibt es den Punkt **Name** —> Suche (Eingabe zur Suche des Plugins)

• ngi —> hätte ich gerne in meinen Kurs

• os-nginx

• HA Proxy —> Erklärung liegt in der Nextcloud —> Chriz benutzt es nicht

• Reiter: Plugins

• Unter der Reiterleiste gibt es den Punkt **Name** —> Suche (Eingabe zur Suche des Plugins)

• qem

• os-qemu-guest-agent —> + Zeichen anklicken

• Dashboard

• QEMU Guest Agent

• Starten —> <play Button>

ProxMox GUI:

• VM 9999 opnws.sysops.de auswählen

• Summary

• Nach kurzer Zeit werden z.B. IPs angezeigt

QEMU Agent erlaubt es die VM sauber herunterzufahren

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
- Reiter Settings
- Show introduction pages: Harken entfernen —> haben wir alles hier gelernt
- Enable Plugin: Harken setzen
- <apply>
- Services: ACME Client: Accounts
- + / add
- Edit Account
- Name: sysops_le —> le für let’s encrypt
- ACME CA: Let’s Encrypt (default)
- E-Mail Address: christian@sysops.de
- <save>
- + / add
- Edit Account
- Name: sysops_zs
- ACME CA: ZeroSSL —> anderer Anbieter
- E-Mail Address: christian@sysops.de
- <save>
- Services: ACME Client: Accounts
- Symbol: Viereck mit Pfeil nach unten —> Account registrieren ==> bei sysop_le
- Conformation Required
- <yes>
- Symbol: Viereck mit Pfeil nach unten —> Account registrieren ==> bei sysop_zs
- Conformation Required

• <yes>

• Services: ACME Client: Challenge Types

• + / add

• Edit Challenge Type

• Name: LE_HTTP

• Description: HTTP Challenge

• Challenge Type: HTTP-01

• HTTP Service: OPsense Web Service (automatic port forward)

• Interface: WAN

• <save>

• Service: ACME Client: Certificates

• + / add

• Edit Certificate

• 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>

• 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

• Reiter ACME Log

• Dort sollte die Zertifikates Erzeugung und Ablage zu sehen sein

• 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: LE_HTTP Clonen —> Zwei Rechtecke übereinander als Symbol

• Edit challenge Type —> Anpassungen vornehmen

• Name: ZSSL_HTTP

• Description: HTTP Challenge Zero SSL

• <save>

• Service: ACME Client: Certificates

• Clone Let’s Encrypt Eintrag —> zwei Rechtecke übereinander

• Edit Certificate

• ACME Account: sysops_zsl

• <save>

• Renew bei neuen Eintrag über den Pfeil als Kreis ausführen

• Services: ACME Client: Log Files

• Reiter: ACME Log

• Auch hier sollte der Abruf des neuen Zertifikates sichtbar sein

• Zero SSL lässt sich etwas mehr Zeit - ein sleep von 15s

• Services: ACME Client Certifcates

• Dort findet man jetzt zwei Zertifikate

• System: Trust: Certicates

• Dort landen alle Zertifikate

• Self-signed

• Let’s Encrypt

• Zero SSL

•

…

• Services: ACME Client: Challenge Types —> Wildcard Certificate

• + / add

• Edit Challenge Type

• Name: Hetzner

• Description:

• DNS Service: DNS-01

• DNS Service: Hetzner

• API Token: <Paste from Clipboard - siehe Hetzner unten>

• <save>

• Services: ACME Client: Certificates

• + / add

• Edit Certificate

• 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

• <yes>

• Services: ACME: Log Files

• Reiter: ACME Log

•

DNS Anbieter: macht bloss 2 Faktor Authentifizierung rein

Browser Hetzner Login Seite

• DNS Console

• Manage API tokens

• Token Name: Workshop

• Create access Token

• API Token —> <Copy to Clippboard> Button

• <Confirm>

•

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

• + / add —> Das habe ich überall vergessen

• Edit Automation

• Name: NGINX

• Description:

• Run Command: Restart Nginx (OPNsense plugin)

• <save>

• Services: ACME Client: Certificates

• Common Name: *.sysops.de

• Edit (Stift)

• Automation: NGINX —> Gibt es ein neues Zertifikat gibt, wird der NGINX durchgestartet -

Bei der SOPHOS ging das alles automatisch

• 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

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

• Replication

• Add

• Schedule: */5 —> alle 5 min

• <create>

• <Schedule now>

• <Log>

• Rechte Maustaste auf VM 999

• Migrate

• Kann auf den anderen PVE (PVE3) umgezogen werden

• Achtung: vorher ISO herausnehmen

• Hardware

• CD/DVD

• ISO … auf don’t Use this media setzen

• <Migrate>

• Output

• Platte wird migriert

• Auch der RAM muss migriert werden - da ist weniger mehr

• Das braucht seine Zeit

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

• 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

• 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

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

• Disk size: 64 GB - da Vergrößerung schwierig …

7. Migrationswege zur OPNSense

Harter Tausch

Als erstes müssen die Redbox (Red) los werden

Site to Site VPN und Fernzugriff

• IPsec

• OpenVPN

Praxis Beispiel:

• GK 41

• OPNsense

• Site to site VPN

• IPsec

• Strongworm können Sophos und OPNsense beide gut

• NextCloud Backup

• OPNsense online bringen und Sicherheitslevel erhöhen IKEv2

• Wenig Config

• Wegfall Lizenz oder Hardware

• Home- und Monatslizenz

Multivan

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

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

• Automatische Rules aufgrund von NAT haben keine Edit Knopf

• Inspect - da sehe ich ob noch Traffic drüber geht

• In den Beispiel läuft gar nichts mehr über die alte Firewall (Sophos), d.h. die kann ausgeschaltet werden

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.

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

• 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

• Enable: Harken setzen

• Weitere Configuration …

• Kannst ganz viele Backup’s in der Nextcloud aufheben, hat Chriz an einer anderen

OPNsense gezeigt

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:

• pct enter 9998

• apt install apache2

• Keine Internet Verbindung

OPNSense

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

• LAN Rule darf eigentlich überall hin - sollte gehen

• Regeln disabled bzw. löschen

• Neu LAN Rule anlegen

• Nicht eintragen

• <save>

• <apply>

• 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

• Interfaces: Diagnostics: ping

• Hostname or IP: web.de

• Job: läuft ewig weiter und erreicht web.de

• Job: gelöscht

PVE CLI

• pct enter 9998

• Nslookup test’s

• nslookup

• web.de —> keine Antwort

• Server 192.168.50.99

• web.de —> Firewall antwortet, aber lässt uns aber nicht ins Internet

• ==> **Gateway Thema**

OPNSense

• Im Suchfeld (Lupe): gateway

• System: Gateways: Configuration

• Edit Gateway

• Passt alles

• Firewall: NAT: Outbound

• Automatic outbound NAT rule generation

• Viele gehen auch auf:

• Hybrid outbound rule generation

• Im Suchfeld (Lupe): live

• Firewall: Log Files: Live View

• Wir wollen sehen ob er etwas blockt: Block / Block ping

• Es wird nichts geblockt

• 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 !!!

OPNSense

PVE CLI

• pct enter 9998

• apt update

• apt install apache2

• apt install curl

• curl localhost

• Web Server antwortet

OPNSense

• Im Suchfeld (Lupe): nat

• Firewall: NAT: Port Forward

• + / add

• Edit Entry

• 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

• IP Address: 192.168.50.99

• Sauber wäre: Speichern, alias anlegen, Regel auf alias anpassen - wird man in der

Regel nicht tun, Anmerkung Chriz

• Redirect target port: HTTP

• <save>

• <apply>

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

• Wie bekomme ich jetzt https für den Webserver

• acme

• Dann kann ich aber nur einen WebServer herauslegen

• Daher nimmt man einen Reverse Proxy

Fritz!Box oder OPNSense

• NAT regel für Port 80 und 443 auf NGINX

Browser

• NGINX einloggen

• E-Mail Adresse / Passwort

• Installiert über

• Docker

• PVE gibt es ein fertigen Installer

• IP Adresse des NGINX nach draußen NATen (http und https)

• Proxy Hosts

• Edit Proxy Host

• Reiter: Details

• Domain Name: home.eesy.de

• Scheme: http

• Forward Hostname / IP: 10.x.y.z

• Forward Port: 8123

• Reiter: SSL

• SSL Certificate: Request a new SSL Certificate

Für kleine Setup.

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

OPNSense

• Im Suchfeld (Lupe): nat

• Firewall: NAT: Port Forward

• Evtl. vorhandene NAT Regel für Port 80 und 443 entfernen

• <apply>

• Im Suchfeld (Lupe): nginx

• Services: Nginx: Configuration

• Reiter: General Settings

• Enable nginix: Harken setzen —> Erst mal einschalten

• <apply>

• Reiter gib es einige

• Viele haben dann noch Unterpunkte …

• Also nicht für schwache Nerven

• Reiter: Upstream - Upstream Server

• + / add

• Edit Upstream

• Description: webserver_host

• Server: 192.168.50.98

• Port: 80 —> hat kein SSL

• Server Priority: 1

• <save>

• Reiter: Upstream - Upstream

• + / add

• Edit Upstream

• Description: webserver_upstream —> der alle Webserver zusammenfasst

• Server Entries: webserver_host —> Wir haben jetzt nur einen Webserver

• Enable TLS (https): keinen harken setzen —> Webserver hat noch kein TLS

• <save>

• —> Ein Webserver ist alleine in einer Gruppe

• Reiter: HTTP(S) - Location

• + / add

• Edit Location

• Description: webserver_host_root

• URL Pattern: / —> oder /webapp oder …

• Upstream Servers: webserver_upstream

• Force HTTPS: Harken setzen

• <save>

• Reiter: HTTP(S) - HTTP Server —> der veröffentlich dann wirklich

• + / add

• 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: harken ist schon gesetzt —> Er kann ein neues

Zertifikat haben, wenn es ein neues gibt

• HTTPS only: harken setzen

• <save>

• Rechteck mit Pfeifen im Kreis neben dem + Button —> wichtig

•

Browser

• opnws.sysops.de

• Zeigt die Demo Seite von Apache 2 Debian Default Page

• Browser hat eine sichere Verbindung, ob der Webserver kein gültiges Zertifikat hat

• Im Browser kann man sich das Zertifikat anzeigen lassen

• *.sysops.de —> Wild Card Certificate

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**

• Sucht auf der Seite nach opnsense

• 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

• Geht mit dem Browser auf Deinen Check_MK —> **Check_MK**

• Einloggen

• 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

• Monitor

• Suche mir den Host

• Man sieht die ganzen Services

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

• Sytem: Configuration: 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

Chriz zeigt nochmal einige in seiner Firewall

• Wozu brauche ich Firewall Regeln im LAN ?

• Firewall Rule im WAN

• 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 ?

• 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

• 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

•

Version #1
Erstellt: 24 April 2024 10:02:12 von Christian Zengel (sysops GmbH)
Zuletzt aktualisiert: 10 Mai 2024 10:18:36 von Christian Zengel (sysops GmbH)