



THOMAS
KRENN®

Praxisbericht: Migration auf OPNsense HA-Cluster

Webinar am 22.11.2023

Christoph Mitasch, Thomas-Krenn.AG

THOMAS
KRENN®



Christoph Mitasch

- seit 2005 bei der Thomas-Krenn.AG, Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner (v1)
- IT-Sicherheitsbeauftragter

Agenda

Ablauf Migration

Sicherheitsfunktionen

OpenVPN

Monitoring

Backup

Diagnose Tools

Troubleshooting

Agenda

Ablauf Migration

Sicherheitsfunktionen

OpenVPN

Monitoring

Backup

Diagnose Tools

Troubleshooting

Ausgangslage

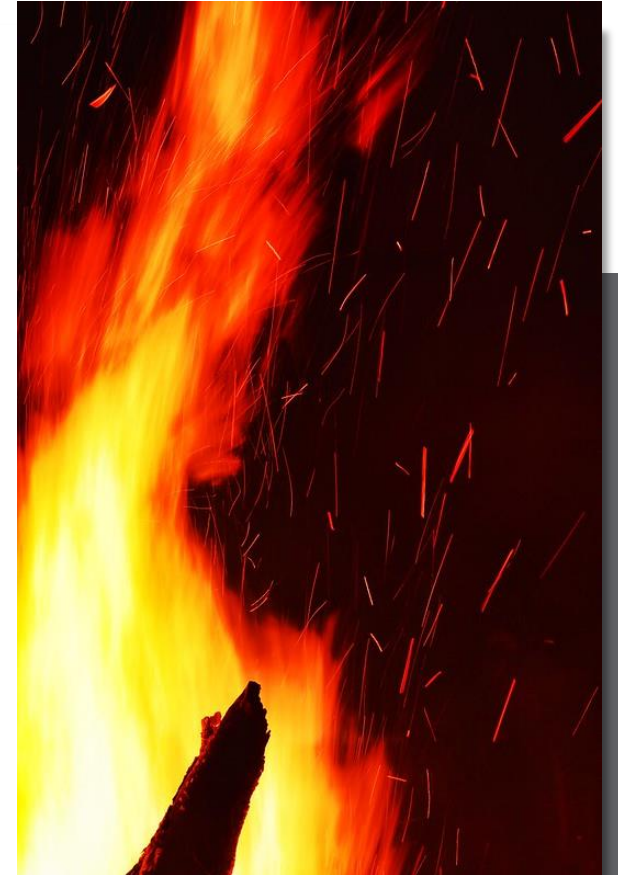
- 2x Sophos UTM 9 als HA-Cluster
- End of Life dafür absehbar (Juni 2026)
- wenig Weiterentwicklung (z.B. IKE v2 fehlt)
- Migration auf XGS vermutlich viel manuelle Arbeit
- Firmenerweiterung -> mehr Leistung und Ports notwendig
- hohe Lizenzkosten -> jährliche Kosten jetzt um vielfaches niedriger
- wollen eigene Produkte einsetzen



<https://utm-shop.de/firewall/sophos/sophos-sg/sg450/hardware-appliance/1344/sophos-sg-450-security-appliance-sg450>

Zahlen und Fakten

- ca. 100 VLANs
- ~300 Firewall Regeln
- ~800 Aliase
- 11x OpenVPN-Server
- 5x IPSec Verbindungen
- HAProxy als Load-Balancer für SMTP und HTTPS
- Unterstützung durch Michael Münz, m.a.x. IT
 - Zitat: „da werden wird nie fertig werden“

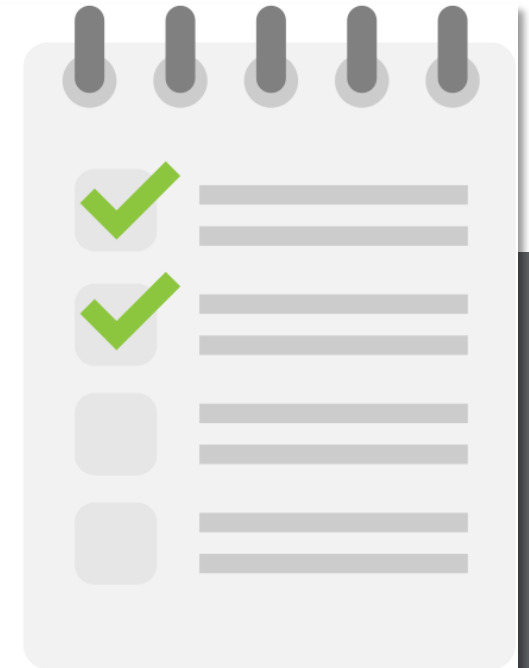


Quelle: <https://www.flickr.com/photos/marfis75/50383592156>

Zeitplan Migration

- 22.12.2021: Kick Off Teams Meeting mit Michael Münz
- Ende Januar 2022: Bestellung Hardware
- Ende März 2022: Inbetriebnahme Hardware
- Mitte Juli 2022: Alle Firewall Regeln migriert
- Anfang August 2022: erstes produktives Netz migriert
- Mitte August erste große Netzmigration
- Ende August restlichen Netze migriert
- 11.9.2022 Sophos ausgeschaltet

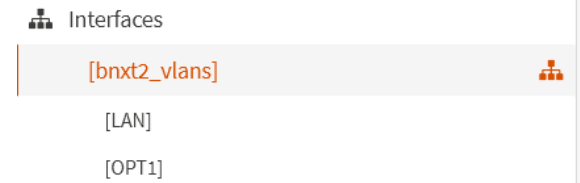
```
fwcluster26:/home/login # poweroff  
  
Broadcast message from root (pts/0) (Sun Sep 11 16:15:24 2022):  
  
The system is going down for system halt NOW!  
fwcluster26:/home/login # █
```



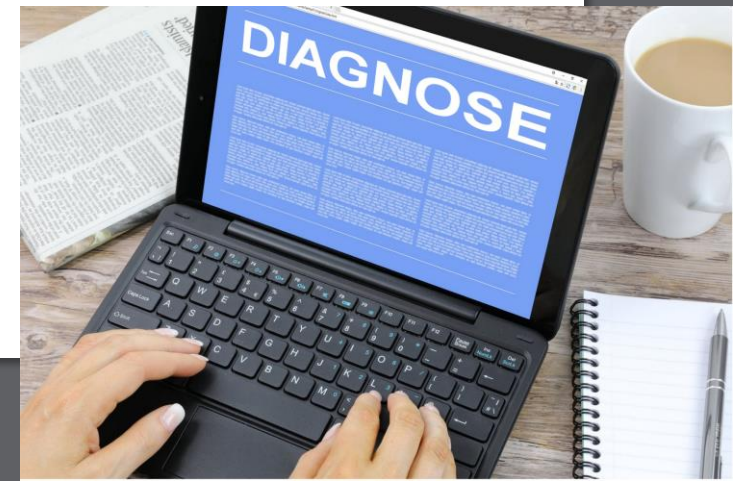
Quelle: https://commons.wikimedia.org/wiki/File:Checklist_Flat_Icon_Vector.svg

Lessons learned

- Firewall Regeln pro Interface machen bei viele VLANs eher keinen Sinn -> haben nur Floating im Einsatz
- „Firewall->Groups“ bei vielen VLANs sinnvoll zwecks Übersichtlichkeit
- Zu Beginn Probleme mit 25 Gbit Broadcom NICs zusammen mit VLANs
https://www.thomas-krenn.com/de/wiki/Broadcom_VLAN_Verbindungsproblem_unter_FreeBSD_mit_bnxt_Treiber
- Langer Parallel-Betrieb unumgänglich bei großen Netzwerken
-> Umstellung ist ein Marathon, kein Sprint
- Probleme löst man mit „Packet Capture“ und „Port Probe“
-> hilft wirklich fast immer ;)
- Achtung bei gleichzeitiger Bearbeitung von Firewall Rules
 - <https://redmine.pfsense.org/issues/13144?tab=history>
 - mit Umstellung auf MVC wird das Thema gelöst, z.B. für Aliase schon erfolgt
 - Fortschritt MVC-Umstellung in Roadmap <https://opnsense.org/about/road-map/>



<https://pix4free.org/photo/22701/diagnose.html>



Nachteile OPNsense

- HA-Modus mit CARP braucht 3 fixe IP-Adressen (auch öffentliche IPs!)
 - intern z.B. .1, als CARP, .251 und .252 als Interface-Adressen
- HA-gesyncte (XMLRPC) Config-Anpassung nur auf node1 möglich, sonst müsste man Richtung tauschen, Anpassungen auf node2 werden überschrieben
- Unterschiedliche UDP und TCP Ports können nicht gemischt werden in einer einzigen Regel -> führt zu mehr Regeln als davor



- Alias mit Ports ohne TCP/UDP als Eigenschaft
- Passives FTP Modul fehlt -> FTP ist generell nicht mehr zu empfehlen
- Load-Balancer HAProxy kann kein UDP (geht mit NGINX)
- EndUser-Portal für VPN-Config-Download fehlt bei OPNsense



Quelle: https://commons.wikimedia.org/wiki/File:OOUI_Talk_icon_-_Delete_vote.svg

Vorteile OPNsense

Kein langes Warten mehr ;-)



- schnelles und modernes Webinterface
- Webinterface ist nicht auf fixe Breite limitiert wie bei Sophos UTM



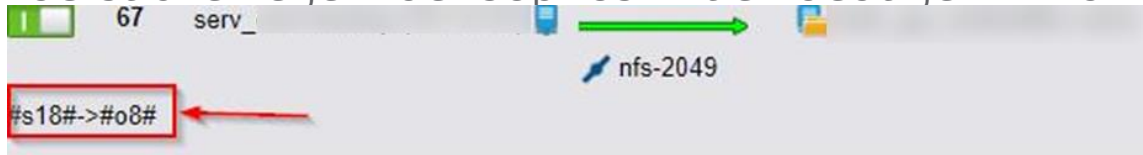
- aktuelle Softwarekomponenten
- IKEv2 bei IPSec, Sophos UTM wird das nie unterstützen
<https://www.ietf.org/archive/id/draft-ietf-ipsecme-ikev1-algo-to-historic-07.html>
- tolle Diagnose-Tools im Webinterface
- OpenSource – Entwicklungs-Firma in den Niederlanden (Decisio)
- keine Lizenzkosten, Business Edition Lizenz für Subscription ist sehr günstig (335 Euro für 3 Jahre)
- läuft auf Thomas-Krenn Hardware



Quelle: https://commons.wikimedia.org/wiki/File:OOUI_Talk_icon_-_Okay.svg

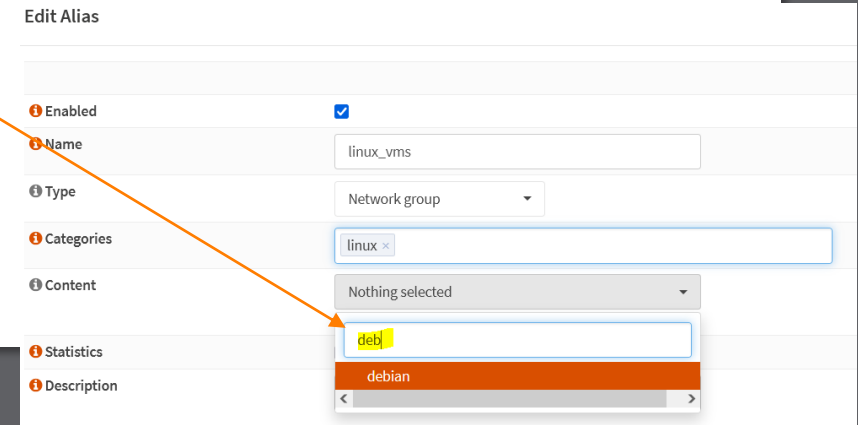
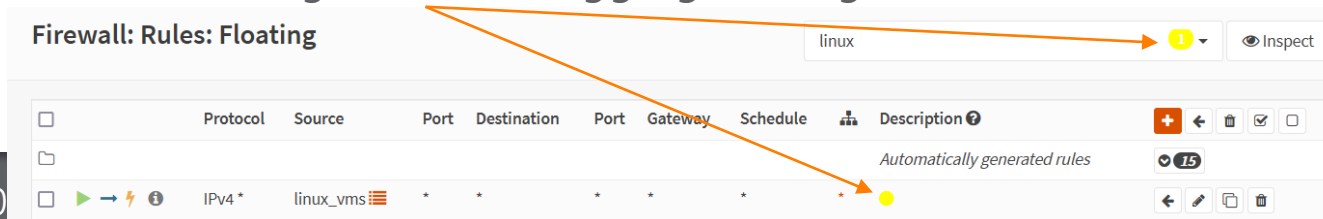
Ablauf Migration

- zuerst alle Regeln der Sophos mit eindeutiger ID nummerieren



#s18# ... Sophos Regel #18
-> ... migriert zu
#o8# ... OPNsense Regel #8

- Regel wird zu OPNsense migriert, das vermerkt man auf der Sophos mit der #o<ID>#
- sobald auch eine OPNsense ID hinterlegt ist, weiß der Mitarbeiter, dass er Anpassungen auf beiden Firewalls durchführen muss
- Alias mit „Network-Group“ sehr praktisch wegen Such-Option
- Firewall „Categories“ als Tagging für Regeln



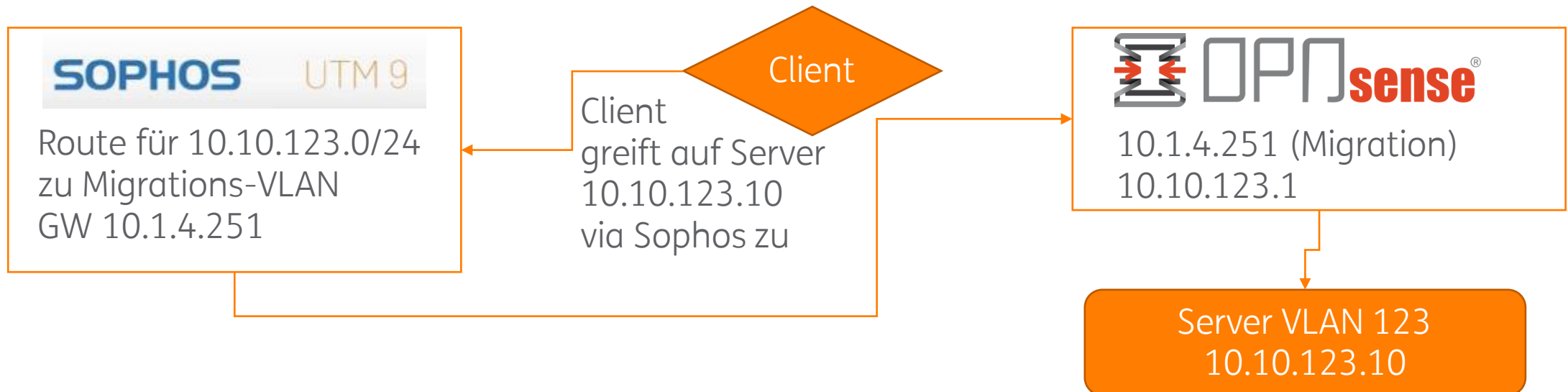
Quelle: https://commons.wikimedia.org/wiki/File:Sketch_of_Sharing_Knowledge_and_Lessons_Learned.jpg

Ablauf Migration



Quelle: <https://www.picpedia.org/keyboard/m/migration.html>

- Ablauf Migration Netz/VLAN:
 - > Interface IP-Adresse zuteilen auf beiden Nodes (X.X.X.251 und X.X.X.252)
 - > Interface auf der Sophos abdrehen
 - > CARP/Gateway-Adresse zuteilen X.X.X.1 (Interfaces -> Virtual IPs -> Settings)
 - > Gateway Route auf der Sophos zu OPNsense
 - > DHCP Relay auf der Firewall für das Interface aktivieren (falls DHCP im Netz notwendig)



Erfahrungen High Availability

- Anpassung der „Description“ bei Interface kann zu Failover führen
-> auf node2 zur Sicherheit CARP deaktivieren bei Änderungen

Interfaces: [OPT1]

Basic configuration

☒ Enable ☐ Enable Interface

☒ Lock ☐ Prevent interface removal

Device: vlan0.123

Description: OPT1

Enter a description (name) for the interface here.

Interfaces: Virtual IPs: Status

Addresses: pfSense nodes

☐ Interface ☐ LAN VMIID: 247 (freq. 1/0)

☒ CARP allowed

☐ Persistent maintenance mode

Current CARP demotion level: 0

- Best Practice Updates HA-Cluster
 - Updates auf node2 einspielen
 - Umschalten auf node2 via „CARP Maintenance Mode“
 - ein paar Tage laufen lassen auf node2
 - Updates auf node1 einspielen
 - node1 wieder zum CARP Master machen
- Anderes Theme für node2, damit auch optisch unterscheidbar
- Outbound NAT für CARP-IP bei IPSec zusätzlich notwendig (Verbindung tlw. nicht von CARP-IP)

Theme: vicuna

Trust: vicuna

Abschaltung alte Firewall



- Übergeordnete Default Routen auf OPNsense zu Sophos entfernt
 - Private Netze mit Sophos als Default Gateway: 192.168/16, 10/8 und 172.16/12
-> sehr praktisch, da nur 3 Routen gesetzt werden müssen
 - und kleinere Netzsegmente auf der OPNsense dann immer Vorrang haben, d.h. direkt von der OPNsense geroutet werden
- Packet Capture im Migrations-VLAN (nur mehr VRRP und DNS)

<https://pixabay.com/de/vectors/schalten-energie-taste-gl%C3%A4nzend-29602/>

Agenda

Ablauf Migration

Sicherheitsfunktionen

OpenVPN

Monitoring

Backup

Diagnose Tools

Troubleshooting

Sicherheitsfunktionen

- 2FA
 - via TOTP / QR-Code
- AD-Anbindung
 - via LDAP
 - Auth-Tester sehr praktisch
- Interne CA
 - für OpenVPN verwendbar
 - Achtung: vor dem Entfernen von Certs noch einen Revoke machen
- URL-Tables
 - via TXT-Datei, auch Blocklists (z.B. Feodo) direkt einbindbar
- GeoIP – in der Business Edition kostenlos dabei



System: Access: Servers

Descriptive name

Type: LDAP + Timebased One Time Password

Hostname or IP address

Port value

LDAP

LDAP + Timebased One Time Password

Local + Timebased One Time Password

Radius

Voucher

System: Access: Tester

Authentication Server: ldap-test

Username: ldap-test

Password:

Test

Firewall: Aliases

Enabled	Name	Type	Description	Content	Loaded#	Last updated
<input checked="" type="checkbox"/>	Feodo_Block	URL Table (IPs)		https://feodotracker...	16	2023-11-15 11:01:10

Sicherheitsfunktionen

- Email Alerts via Monit-Dienst

- carp_status_change wird mitgeliefert, muss aber aktiviert werden
- z.B. Block-Lists via /var/log/filter/latest.log (ID in /tmp/rules.debug)
- oder Login von bestimmten User

Edit Service

☒ advanced mode

Enable service checks ☒

Name ROOT_Login_ALERT

Type File

Path /var/log/audit/latest.log

Start

Stop

Tests WEB_ROOT_login

[Clear All](#)

Depends Nothing selected

[Clear All](#)

Edit Service

☒ advanced mode

Enable service checks ☒

Name feodo_block_ALERT

Type File

Path /var/log/filter/latest.log

Start

Stop

Tests FIREWALL_feodo_block

[Clear All](#)

Edit Test NOTE: For a detailed description see monit(1) section "SERVICE TESTS".

Name feodo_block

Condition content ="52ef55e4d9fba7e428d1e7c2c8fa6c80"

Action Alert

Agenda

Ablauf Migration

Sicherheitsfunktionen

OpenVPN

Monitoring

Backup

Diagnose Tools

Troubleshooting

OpenVPN



- beliebig viele OpenVPN-Server
 - mit unterschiedlichen Ports und/oder IPs
- UDP für höhere Performance, TCP für Kompatibilität, z.B. Port 443 für WLANs
- unterschiedliche Auth-Backends, sogar mehrere pro User
- Server Modus: Shared Key, Username/Passwort, Username/Passwort + TLS-Cert
- „Strict User/CN Matching“ – CN in Cert und Username müssen übereinstimmen
- Fixe IPs pro User via „Client Specific Overrides“ (Match auf Common Name im Zertifikat)
- 2FA mit TOTP am Anfang oder Ende von Passwort-Feld
- Status-Seite

VPN: OpenVPN: Connection Status

Sessions								
Routes								
Type	Description	Common ...	Real Address	Virtual Ad...	Connected...	Bytes Sent	Bytes Rece...	Status
server					2023-11-15 09...	5.34 MB	2.58 MB	ok
server					2023-11-15 09...	767.04 KB	732.12 KB	ok
server					2023-11-15 08...	24.76 MB	1.90 MB	ok
server					2023-11-15 09...	175.85 KB	70.65 KB	ok
server					2023-11-14 16...	1.87 MB	3.16 MB	ok

Server Mode

Backend for authentication

Enforce local group

Protocol

Remote Access (SSL/TLS + User Auth)

Peer to Peer (SSL/TLS)

Peer to Peer (Shared Key)

Remote Access (SSL/TLS)

Remote Access (User Auth)

Remote Access (SSL/TLS + User Auth)

TCP4

Agenda

Ablauf Migration

Sicherheitsfunktionen

OpenVPN

Monitoring

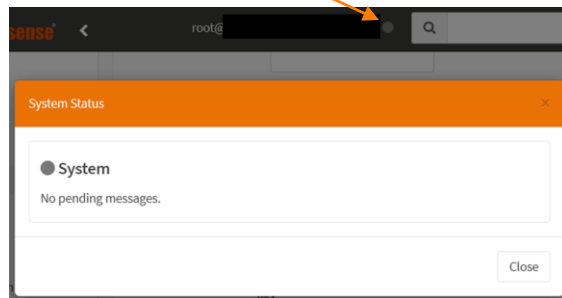
Backup

Diagnose Tools

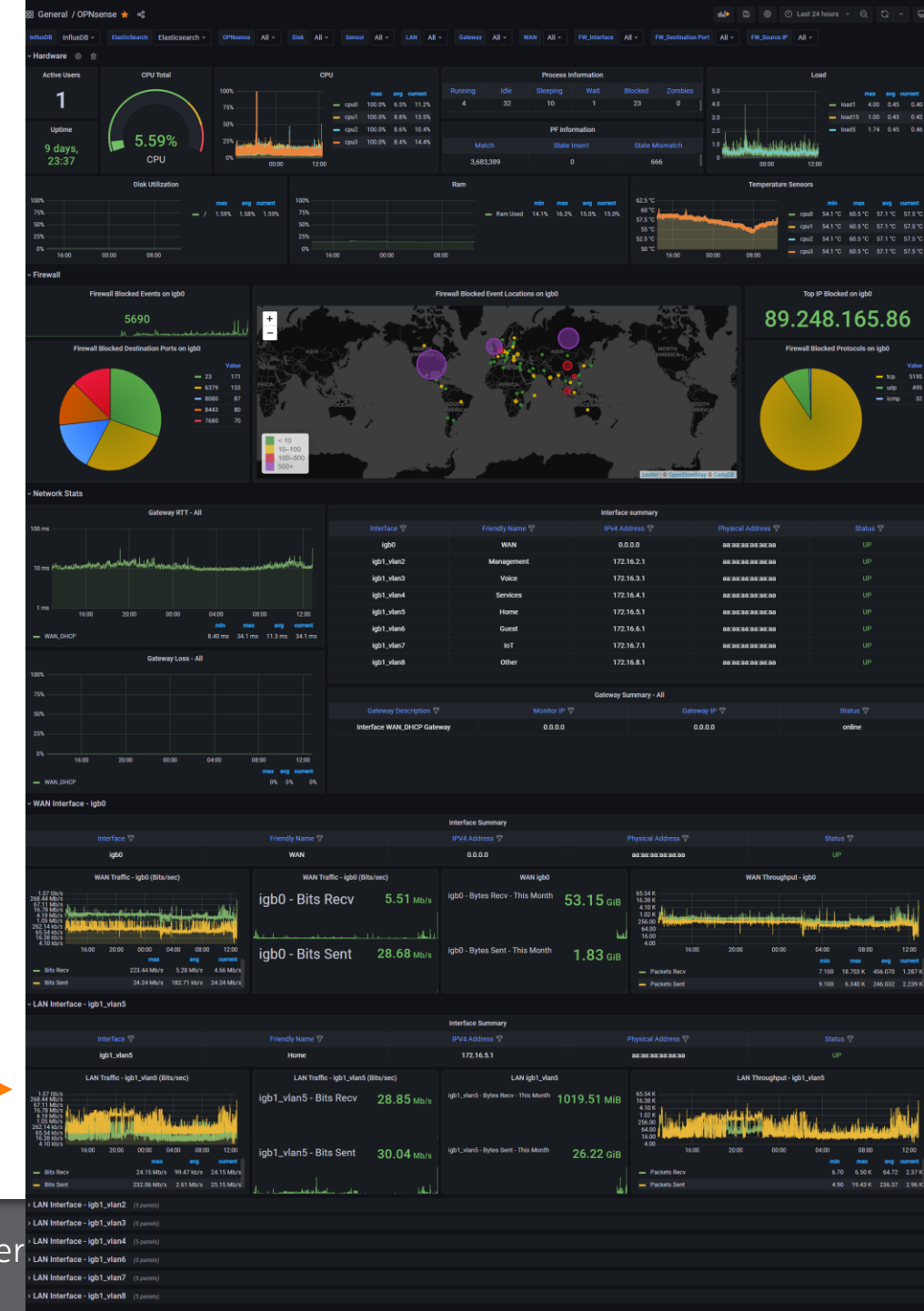
Troubleshooting

Monitoring

- Monit Emails
- Icinga Einbindung via NRPE (Plugin „os-nrpe“)
 - eigene Checks nach /usr/local/libexec/nagios/ kopieren
 - pfSense Checks größtenteils kompatibel
<https://github.com/oneoffdallas/pfsense-nagios-checks>
 - API für weitere Status-Daten
 - ergänzt durch Crash Reporter Check via /api/core/system/status



- Grafana (InfluxDB, Graylog) →
 - <https://github.com/BSmithIO/OPNsense-Dashboard/>



Agenda

Ablauf Migration

Sicherheitsfunktionen

OpenVPN

Monitoring

Backup

Diagnose Tools

Troubleshooting

Backup der Config



- Google Drive Backup
 - Kein Plugin notwendig
 - Verschlüsselung der Config sinnvoll!
- Nextcloud
 - Plugin „os-nextcloud-backup“
 - Verschlüsselung Config
- Git
 - Plugin „os-git-backup“
 - lokaler Commit bei jeder Änderung (/conf/backup/git)
 - Push ins Repo nur 1x pro Tag, kann aber via Cron-Job erhöht werden
 - „diff“ mit Git sehr praktisch
- Achtung: Anpassungen, Erweiterungen via SSH-Konsole oder auch Logs fehlen in der XML
- Selektiver Restore aus Config-Datei möglich

Edit job

enabled	<input checked="" type="checkbox"/>
Minutes	0
Hours	*
Day of the month	*
Months	*
Days of the week	*
Command	Remote backup
Parameters	
Description	

Restore

Restore area:

ALL
ALL
OPNsense Additions
Bridge Devices
SSL Certificate Authorities

Agenda

Ablauf Migration

Sicherheitsfunktionen

OpenVPN

Monitoring

Backup

Diagnose Tools

Troubleshooting

Diagnose

- Probleme löst man mit „Packet Capture“ und „Port Probe“
 - > hilft wirklich fast immer ;)
 - > optional Export in Wireshark
- Name bei „Description“ vergeben, dann findet man den Capture unter „Jobs“ wieder und kann ihn danach auch nochmal starten

Interfaces: Diagnostics: Packet Capture

Capture Jobs

Interface: vmx0 [LAN] ☒

Promiscuous: ☐

Address Family: any

Invert Protocol: ☐

Protocol: any

Host Address: 8.8.8.8

Invert Port: ☐

Port:

Packet Length:

Count: 100

Description: google DNS

Start

Interfaces: Diagnostics: Packet Capture

Capture Jobs

Search

view capture (high detail)

google DNS

Showing 1 to 1 of 1 entries

Diagnose

- Port Probe und Traceroute – noch keine Jobs (MVC fehlt noch)
- Ping – mit Jobs

Interfaces: Diagnostics: Port Probe

This page allows you to perform a simple TCP connection test to determine if a host is up and accepting connections on a given port. This test does not function for UDP since there is no way to reliably determine if a UDP port accepts connections in this manner. No data is transmitted to the remote host during this test, it will only attempt to open a connection and optionally display the data sent back from the server.

full help ⓘ

Hostname or IP: 8.8.8.8

Destination Port: 53

Address Family: IPv4

Source address: [REDACTED]

Source Port: [REDACTED]

Show Remote Text: ☒

Apply

Response

➤ Connection to 8.8.8.8 53 port [tcp/domain] succeeded!

Interfaces: Diagnostics: Ping

Ping

Jobs

Search

<input type="checkbox"/>	Description	Hostname	Source	Send	Received	Min	Max	Avg	loss	Error	Comman
<input checked="" type="checkbox"/>	google DNS	8.8.8.8		13	13	3.296	3.347	3.318	0.00 %		<input type="button" value="x"/> <input type="button" value="▶"/>

Interfaces: Diagnostics: Trace Route

Hostname or IP: 8.8.8.8

Address Family: IPv4

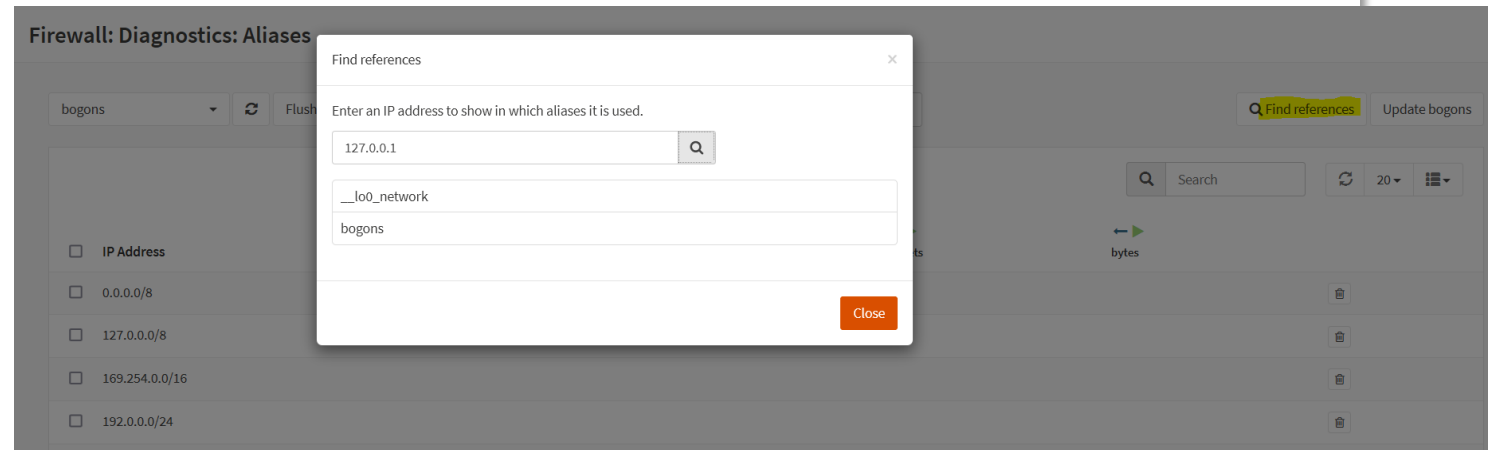
Protocol: UDP

Source address: [REDACTED]

Apply

Diagnose

- Firewall -> Diagnostics -> Alias
 - für verschachtelte Aliase wichtig
 - Inhalt von URL-Listen anschauen
- Firewall-Logs
 - Firewall -> Log-Files -> Live View
 - Kommandozeile /var/log/filter/latest.log
 - Vorhaltezeit Logs



Firewall: Log Files: Live View

protoname contains [] + >> google ping refresh 25

protoname=icmp
click on badge to remove filter
☐ Select any of given criteria (or)

Interface	Time	Source	Destination	Proto	Label
▶ LAN	← 2023-11-20T11:08:19	10.10.10.152	8.8.8.8	icmp	let out anything from firewall host itself (force gw) ⓘ

System: Settings: Logging

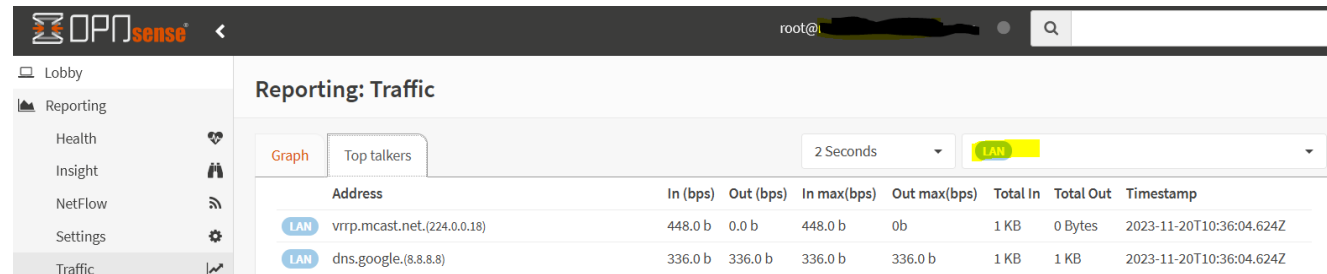
Local Logging Options

ⓘ Preserve logs (Days)

Number of log to preserve. By default 31 logs are preserved.

Diagnose

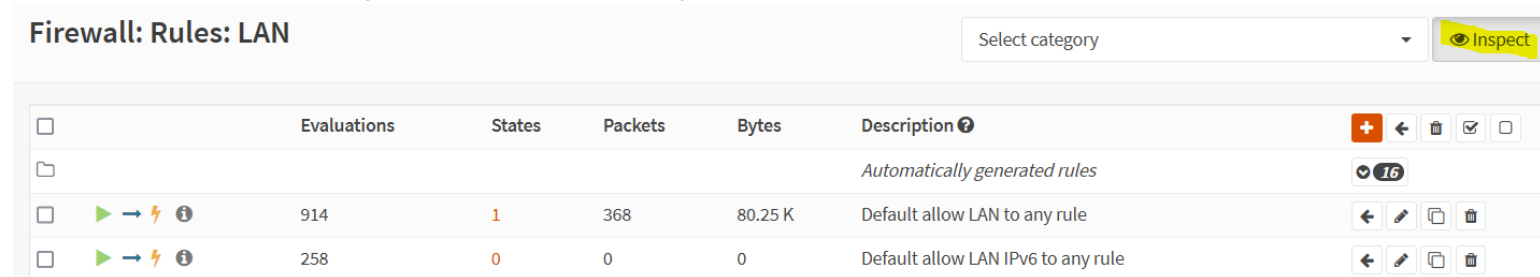
- Top Talkers



The screenshot shows the OPNsense web interface. The left sidebar has a menu with 'Reporting' selected. The main content area is titled 'Reporting: Traffic' and shows a 'Top talkers' tab. A table lists the top traffic sources. The first two entries are 'vrp.mcast.net.(224.0.0.18)' and 'dns.google.(8.8.8.8)', both showing significant traffic volume.

Address	In (bps)	Out (bps)	In max(bps)	Out max(bps)	Total In	Total Out	Timestamp
LAN vrp.mcast.net.(224.0.0.18)	448.0 b	0.0 b	448.0 b	0b	1 KB	0 Bytes	2023-11-20T10:36:04.624Z
LAN dns.google.(8.8.8.8)	336.0 b	336.0 b	336.0 b	336.0 b	1 KB	1 KB	2023-11-20T10:36:04.624Z

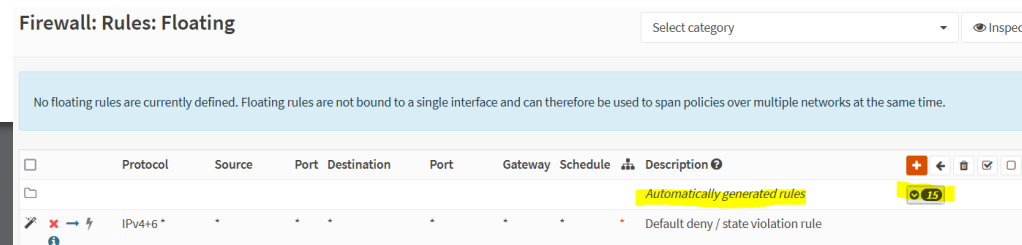
- Anwendung von Firewall Rules prüfen via „Inspect“



The screenshot shows the 'Firewall: Rules: LAN' page in OPNsense. The 'Inspect' button is highlighted. A table displays the status of firewall rules. The first two rules are 'Default allow LAN to any rule' and 'Default allow LAN IPv6 to any rule', both showing active status and traffic volume.

	Evaluations	States	Packets	Bytes	Description ?
Automatically generated rules					
<input type="checkbox"/>	914	1	368	80.25 K	Default allow LAN to any rule
<input type="checkbox"/>	258	0	0	0	Default allow LAN IPv6 to any rule

- Automatische Firewall-Rules berücksichtigen



The screenshot shows the 'Firewall: Rules: Floating' page in OPNsense. The 'Inspect' button is highlighted. A message states: 'No floating rules are currently defined. Floating rules are not bound to a single interface and can therefore be used to span policies over multiple networks at the same time.' Below this, a table shows the status of floating rules. The first rule is 'Default deny / state violation rule', which is active and shows traffic volume.

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description ?
Automatically generated rules								
<input type="checkbox"/>	IPv4+6	*	*	*	*	*	*	Default deny / state violation rule

Agenda

Ablauf Migration

Sicherheitsfunktionen

OpenVPN

Monitoring

Backup

Diagnose Tools

Troubleshooting

Troubleshooting

- Konsole
 - SSH
 - seriell
 - Monitor, IPMI
- Direct-Access Netzwerk-Port für Notfall vorsehen
- Config in /conf/conf.xml
 - Config-Backup in /conf/backup/
 - diff-Kommando für Vergleich
 - Restore via Option “13” möglich

```
$ ssh root@192.168.20.102
Password:
Last login: Fri Jul 3 10:37:09 2020 from 192.168.20.10

-----
      Hello, this is OPNsense 20.1
-----
Website:  https://opnsense.org/
Handbook: https://docs.opnsense.org/
Forums:   https://forum.opnsense.org/
Lists:    https://lists.opnsense.org/
Code:     https://github.com/opnsense

*** OPNsense.localdomain: OPNsense 20.1.8 (amd64/OpenSSL) ***

LAN (em1)      -> v4/DHCP4: 192.168.20.102/24
WAN (em0)      -> v4/DHCP4: 192.168.20.101/24

HTTPS: SHA256 76 60 81 1B 4B B5 B0 0F 13 A4 22 08 1A FF C0 AE
        BE 45 48 C1 34 F8 98 08 3D AD 84 93 99 01 18 9B
SSH:    SHA256 ibySKBjnGxiTun9KLXMmtdjcrInG0+zV0pwLP+jk3iM (ECDSA)
SSH:    SHA256 zrLTCAnj2jcrLHttidECWJdXx58bxyMjh9JKvisoL4E (ED25519)
SSH:    SHA256 rxssyNH9Yc2vcSbC0AavJ6Vq75D38Rf0LfQ8MFNnE7A (RSA)

0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option: █
```

https://docs.opnsense.org/_images/opnsense-ssh-login.png

```
0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option: 13

1.  Fri May 26 14:00:56 CEST 2023
2.  Fri May 26 14:00:41 CEST 2023
3.  Fri May 26 13:59:50 CEST 2023
4.  Fri May 26 13:59:46 CEST 2023
5.  Fri May 26 13:59:09 CEST 2023
6.  Fri May 26 13:57:47 CEST 2023
```

Info-Material

- OPNsense
 - <https://docs.opnsense.org/>
 - <https://forum.opnsense.org/>
 - <https://docs.opnsense.org/plugins.html>
 - <https://github.com/opnsense/core/issues>
- PfSense-Doku mit Vorsicht, hat aber oft zusätzliche Infos
<https://docs.netgate.com/pfsense/en/latest/>
- TK Wiki
 - <https://www.thomas-krenn.com/de/wiki/Kategorie:OPNsense>
- OPNsense-Praktiker (E-Book)
 - <https://der-opnsense-praktiker.github.io/>
 - Labornetzwerk wird mit VMs aufgebaut zum Üben
 - bei Business Edition kostenlos als PDF dabei
https://downloads.opnsense.com/<Subscription_ID>



https://commons.wikimedia.org/wiki/File:Information_orange.svg

The logo consists of a dark, textured, brush-stroke-like background. The word "ORANGE" is written in a bold, orange, sans-serif font, and the word "FRIDAY" is written in a bold, white, sans-serif font directly below it.

**ORANGE
FRIDAY**

Doppelter RAM zum gleichen Preis!

Am 24.11. schlägt der Cyberdealer wieder zu

Mittlerweile kennt und fürchtet man bei Thomas-Krenn seine gnadenlos günstigen Deals: Der mysteriöse Cyberdealer ist zurück, und er macht keine halben Sachen. Ganz im Gegenteil – **zum Orange Friday am 24. November verdoppelt er ohne Aufpreis den Arbeitsspeicher für Ihre Bestellung***! Sie entscheiden sich für Riegel mit 8, 16 und 32 GB RAM? Egal, der Cyberdealer verdoppelt gnadenlos die Speicherkapazität. Orange Friday bei Thomas-Krenn bedeutet für Sie: **zweifacher RAM zum einfachen Preis**, ohne Haken oder versteckte Kosten.

The background features a large graphic composed of several diagonal stripes in shades of orange and grey. In the upper right corner, there is a photograph of a modern, multi-story building with a flat roof, situated in a grassy field. The sun is setting behind a hill in the background, creating a warm, golden glow and long shadows.

THOMAS KRENN®

Vielen Dank für Ihre
Aufmerksamkeit!