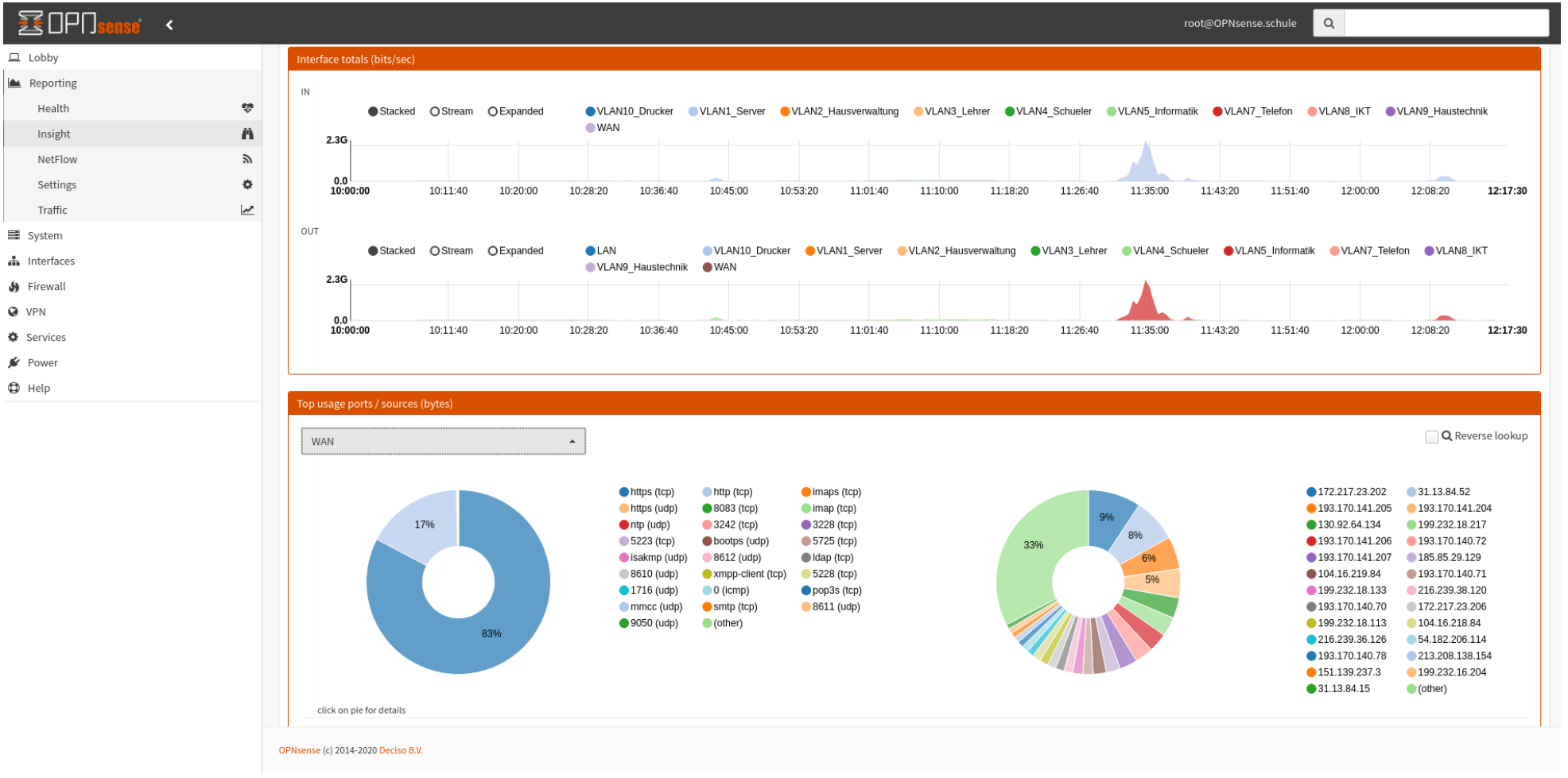
OPNsense

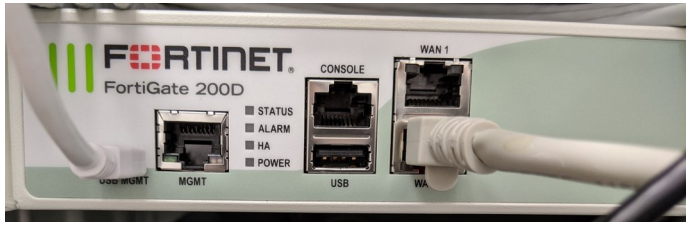
Planung und Migration

Rene Schwarzinger, Martin Gruber
April 2022



Rene Schwarzinger, Martin Gruber
April 2022

Ausgangssituation



- im Bestand:
  FortiGate FG-200D
  - grundsätzlich zufrieden
  - Lizenzen auslaufend
  - eigentlich überdimensioniert
  - Lizenzen für weitere 2 Jahre: ca. 4.300 €

Weiterführung FortiGate

- FG-100E UTM Bundle
  - ca. 8.500 € (5 Jahre)
  - Firewall Throughput: 7,4 Gbps
  - Max. packets per second: 6,6 Mpps
  - Ma. Concurrent Sessions: 2 Mio.
- FG-200E UTM Bundle
  - ca. 13.000 € (5 Jahre)
  - Firewall Throughput: 20 Gbps
  - Max. packets per second: 13,5 Mpps
  - Ma. Concurrent Sessions: 2 Mio.

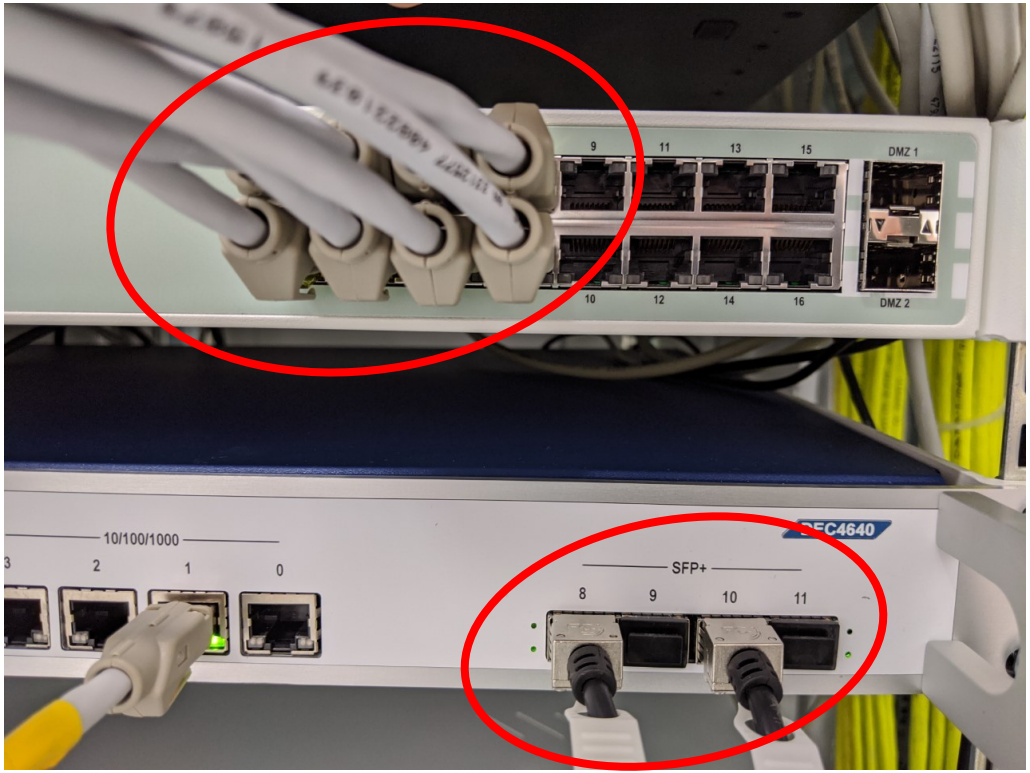
FOSS

- FortiGate passt als proprietäres Produkt nicht in unser Schulkonzept
- Abhängigkeit von einem Anbieter
- zudem insgesamt viel teurer als teuerste OPNSense Appliance

applianceshop.eu (2800 €)

Rene Schwarzinger, Martin Gruber
April 2022

Redundante DACs



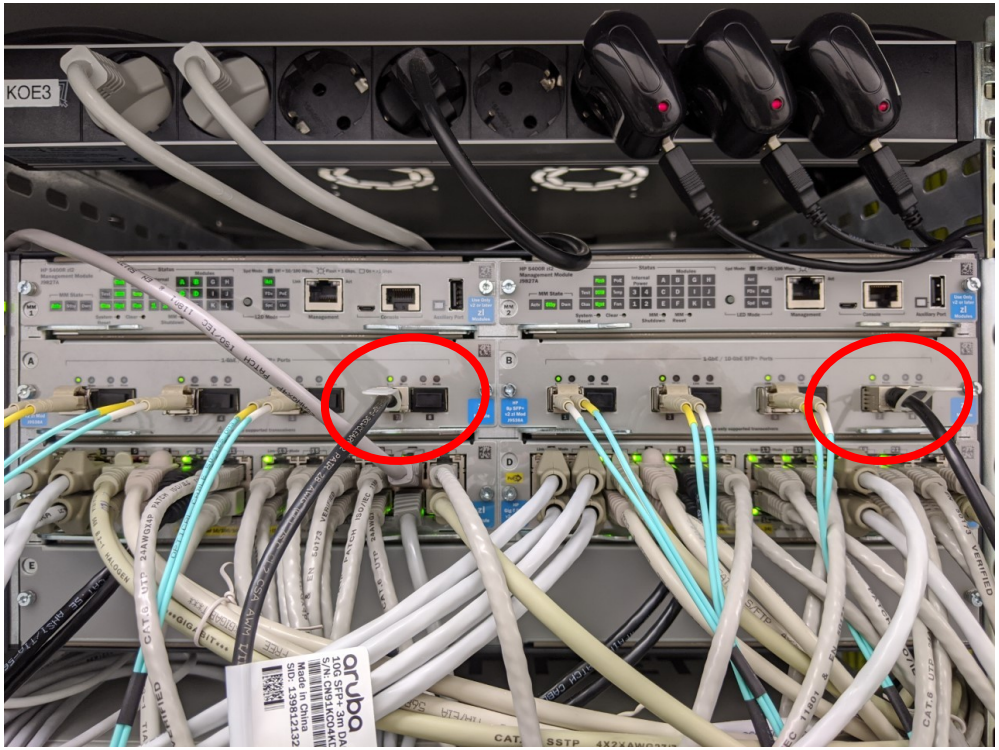
Vorher (Fortinet 100D):

4 redundante Trunks = 8 x LAN

Nachher (OPNsense):

1 redundanter Trunk = 2 x SFP+

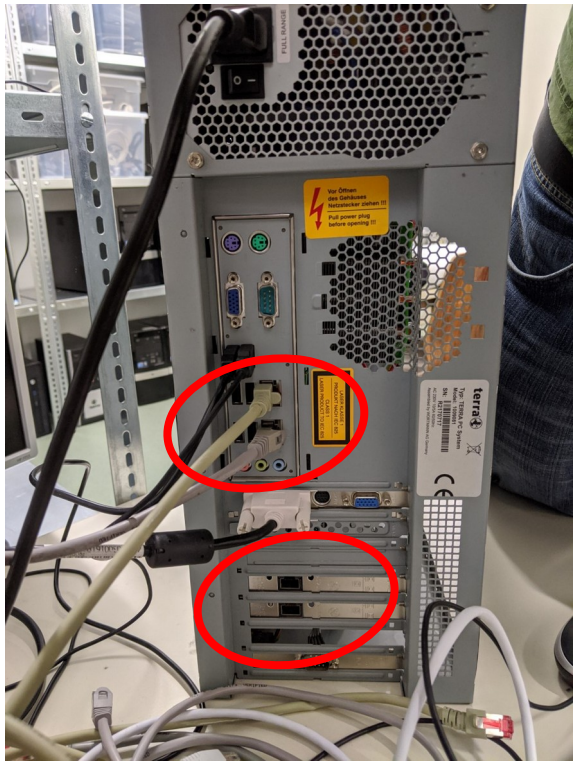
Gegenstelle HP5406R



1 GbE / 10 Gb SFP+ Ports

redundante Ausführung

Vorbereitung



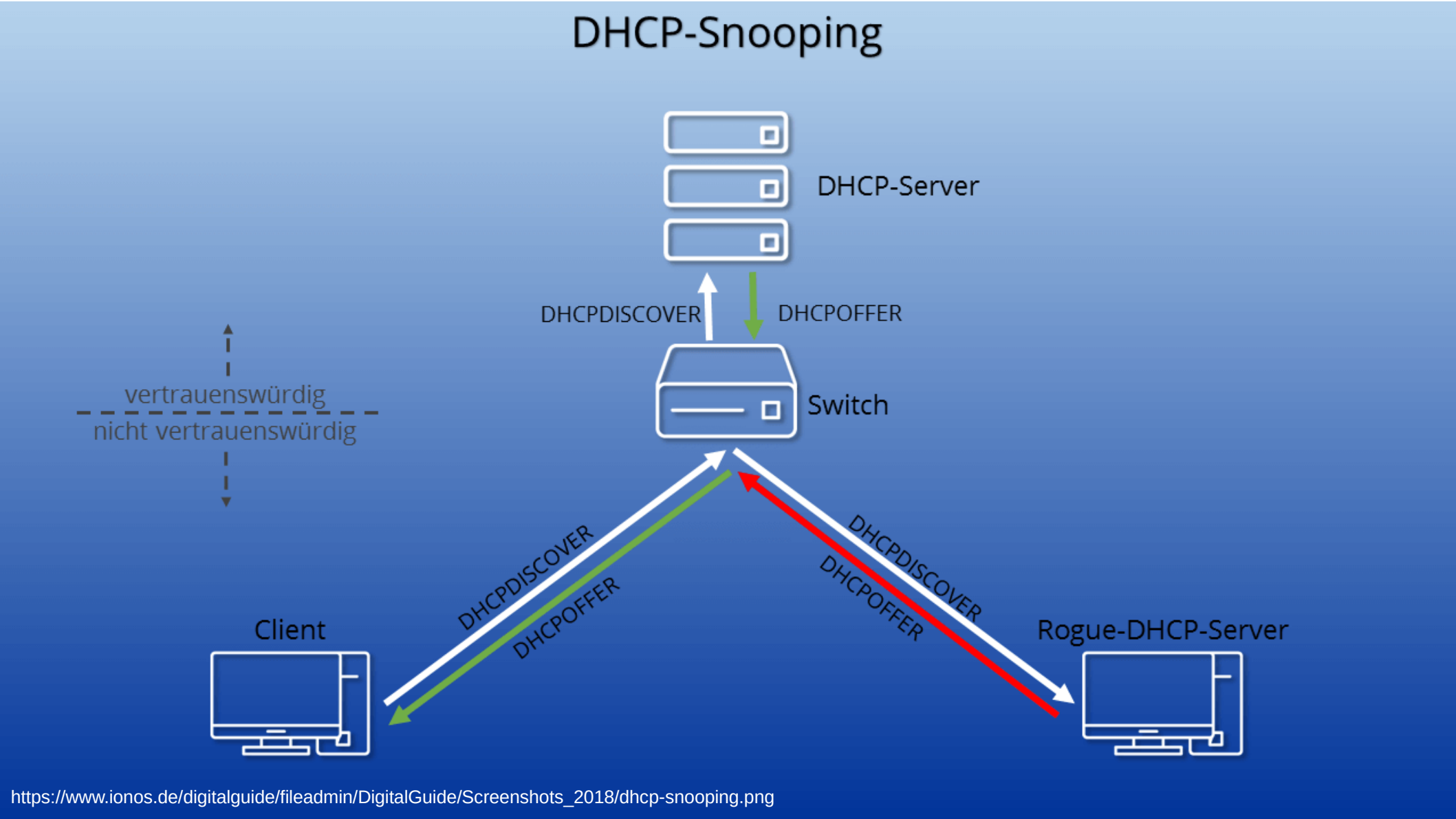
Rene Schwarzinger, Martin Gruber
April 2022

Anpassungen Core-Switch

```
trunk A?,B? trk100 lacp

interface trk100

  dhcp-snooping trust

  arp-protect trust

  exit
```

- DHCP-Snooping im Switch erkennt, dass das Paket nicht von einem vertrauenswürdigen Server kommt bzw. falsche Informationen enthält, und blockiert die Weiterleitung.
- In a similar way to DHCP snooping, dynamic ARP protection allows you to configure VLAN interfaces in two categories: trusted and untrusted ports. ARP packets received on trusted ports are forwarded without validation.

DHCP-Snooping



https://www.ionos.de/digitalguide/fileadmin/DigitalGuide/Screenshots_2018/dhcp-snooping.png

Aufteilung Netzwerke

VLANs and assigning interfaces

If choose to do manual interface assignment or when no config file can be found then you are asked to assign Interfaces and VLANs. VLANs are optional. If you do not need VLANs then choose **no**. You can always configure VLANs at a later time.

LAN, WAN and optional interfaces

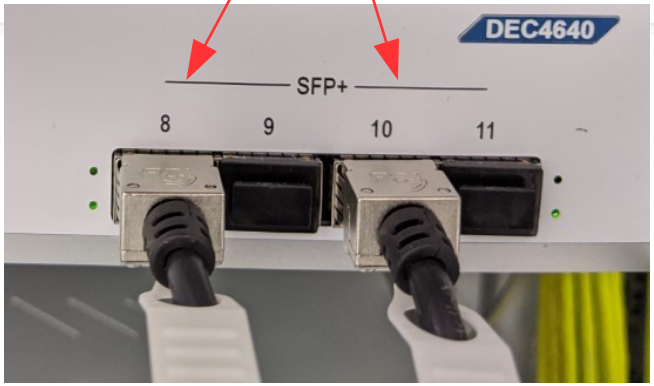
The first interface is the LAN interface. Type the appropriate interface name, for example “em0”. The second interface is the WAN interface. Type the appropriate interface name, eg. “em1” . Possible additional interfaces can be assigned as OPT interfaces. If you assigned all your interfaces you can press [ENTER] and confirm the settings. OPNsense will configure your system and present the login prompt when finished.

Rene Schwarzinger, Martin Gruber

Link Aggregation

Interface	Members	Protocol	Description
LAGG0	ixl0,ixl2	LACP	Trk100

LAGG allows for link aggregation, bonding and fault tolerance. Only unassigned interfaces can be added to LAGG.



LACP

- NONE
- LACP
- FAILOVER
- FEC
- LOADBALANCE
- ROUNDROBIN

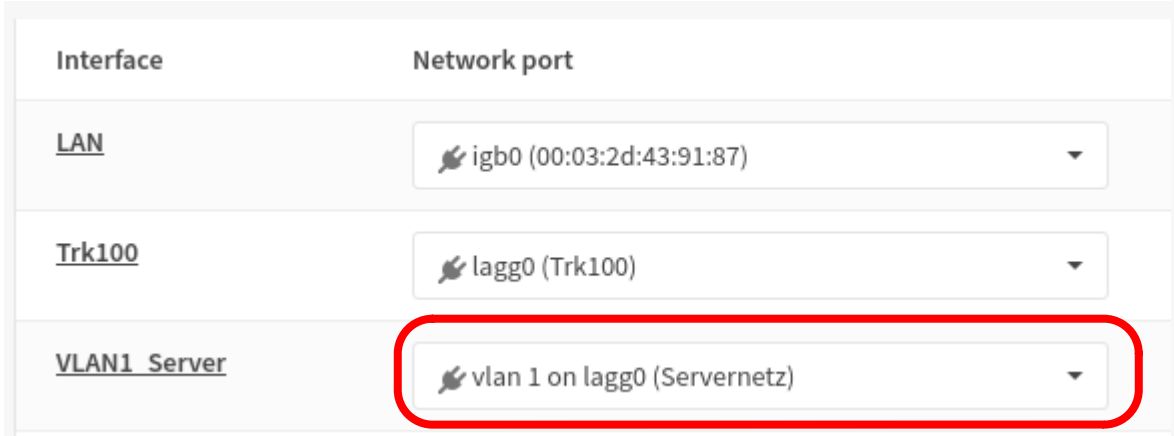
static

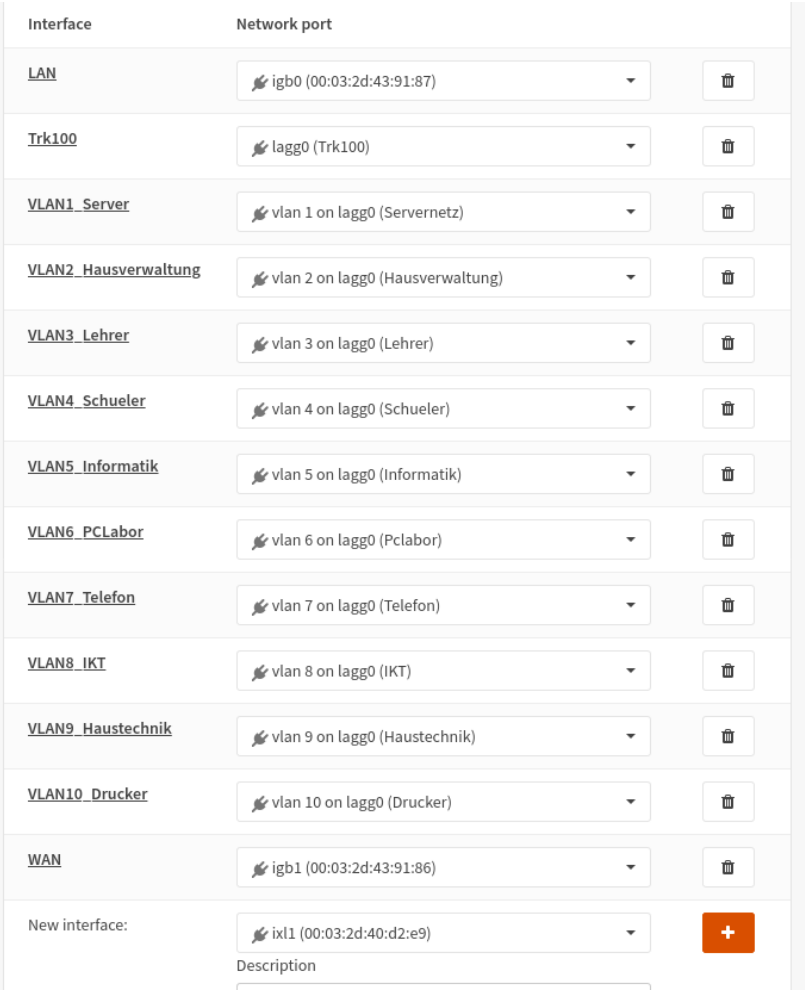
Redundanz +
höhere Bandbreite

VLANs

Interface	Tag	PCP	Description
lagg0	1	0	Servernetz
lagg0	2	0	Hausverwaltung
lagg0	3	0	Lehrer
lagg0	4	0	Schueler
lagg0	5	0	Informatik
lagg0	6	0	Pclabor
lagg0	7	0	Telefon
lagg0	8	0	IKT
lagg0	9	0	Haustechnik

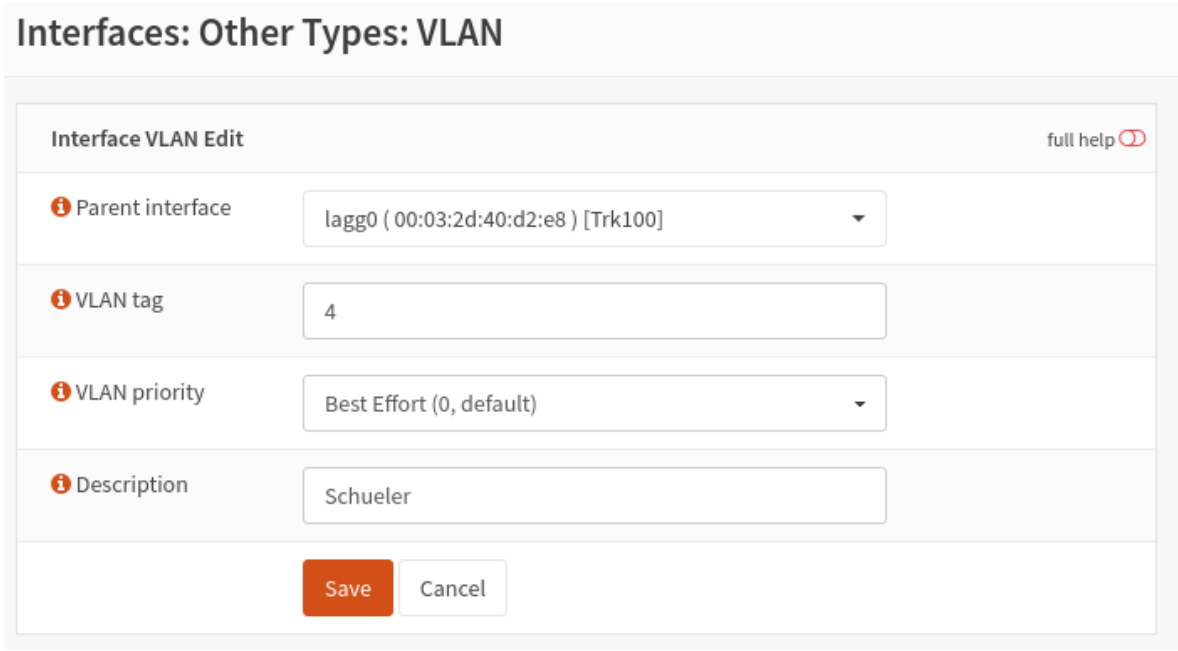
Assignments



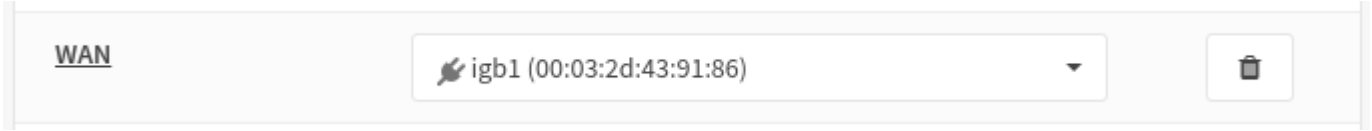


Assignments (Trk 100)

zur Übertragung
der VLANs

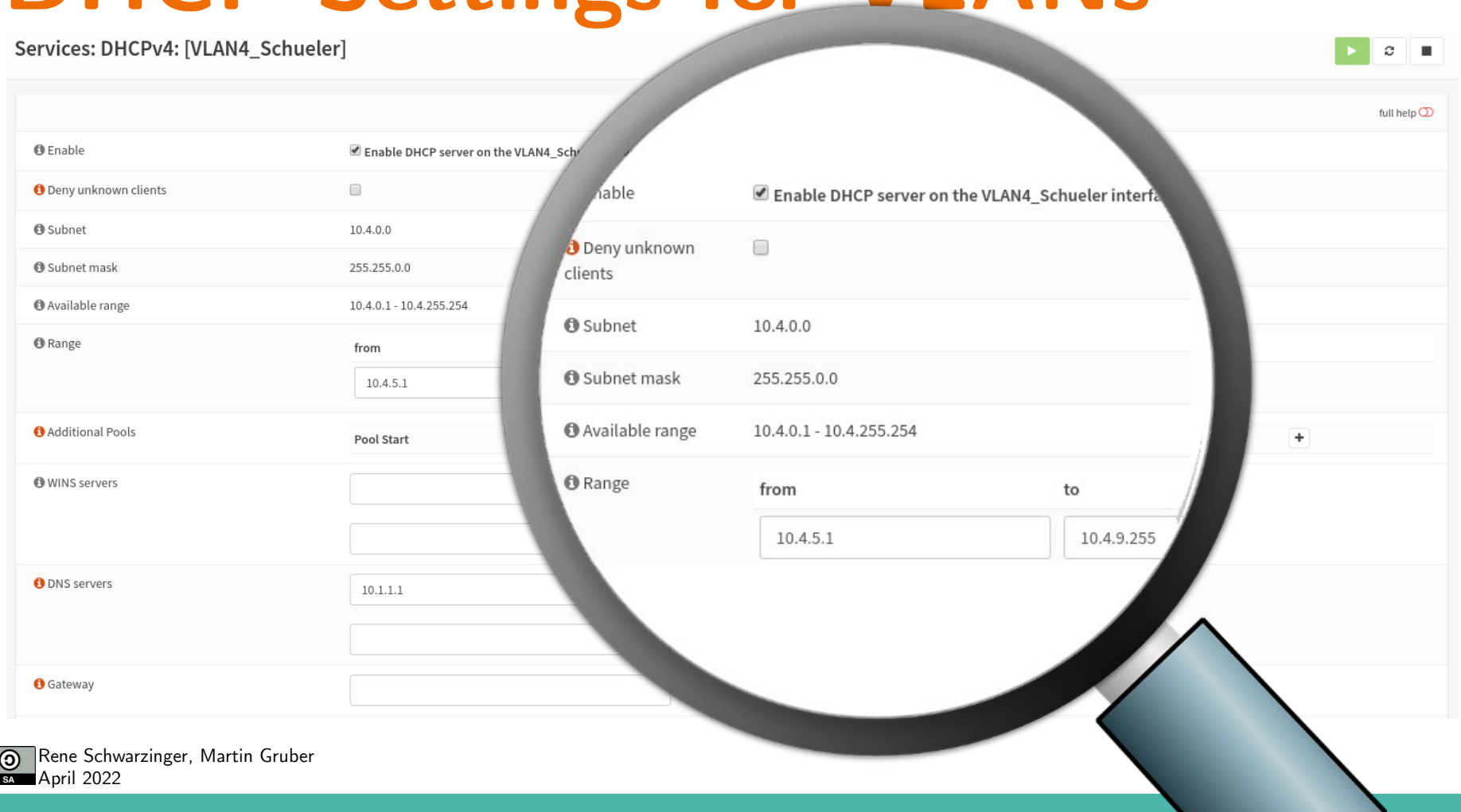


System Settings for WAN



zuvor Gateway nach außen hin definieren

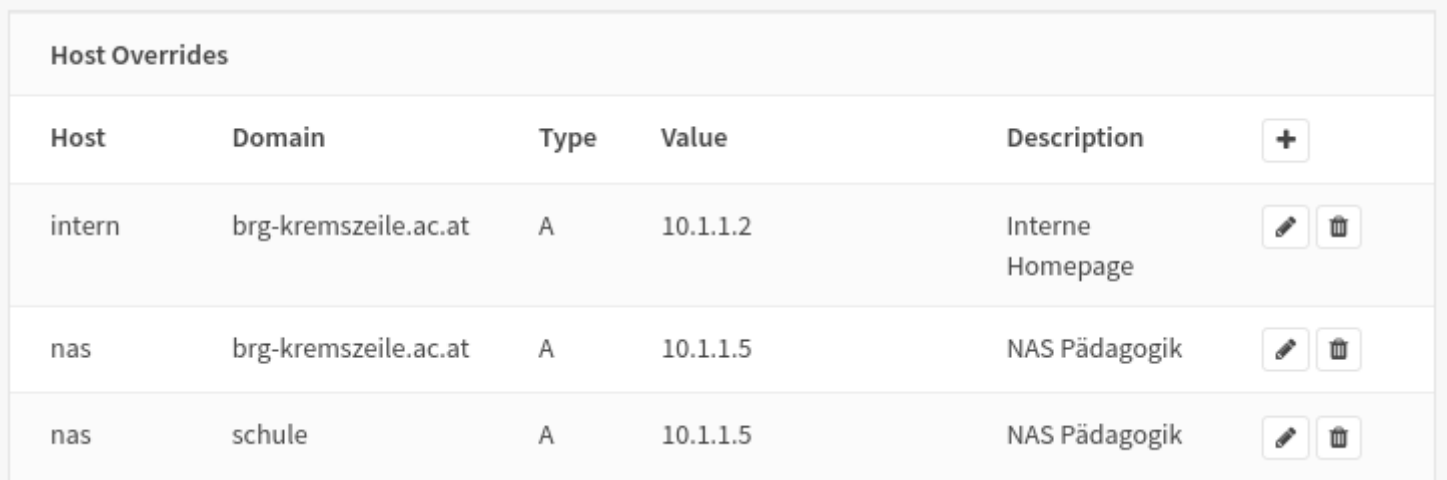
DHCP Settings for VLANs



Rene Schwarzinger, Martin Gruber
April 2022

Overrides

- Within the overrides section you can create separate host definition entries and specify if queries for a specific domain should be forwarded to a predefined server.



Host Overrides

Host	Domain	Type	Value	Description	+
intern	brg-kremszeile.ac.at	A	10.1.1.2	Interne Homepage	
nas	brg-kremszeile.ac.at	A	10.1.1.5	NAS Pädagogik	
nas	schule	A	10.1.1.5	NAS Pädagogik	

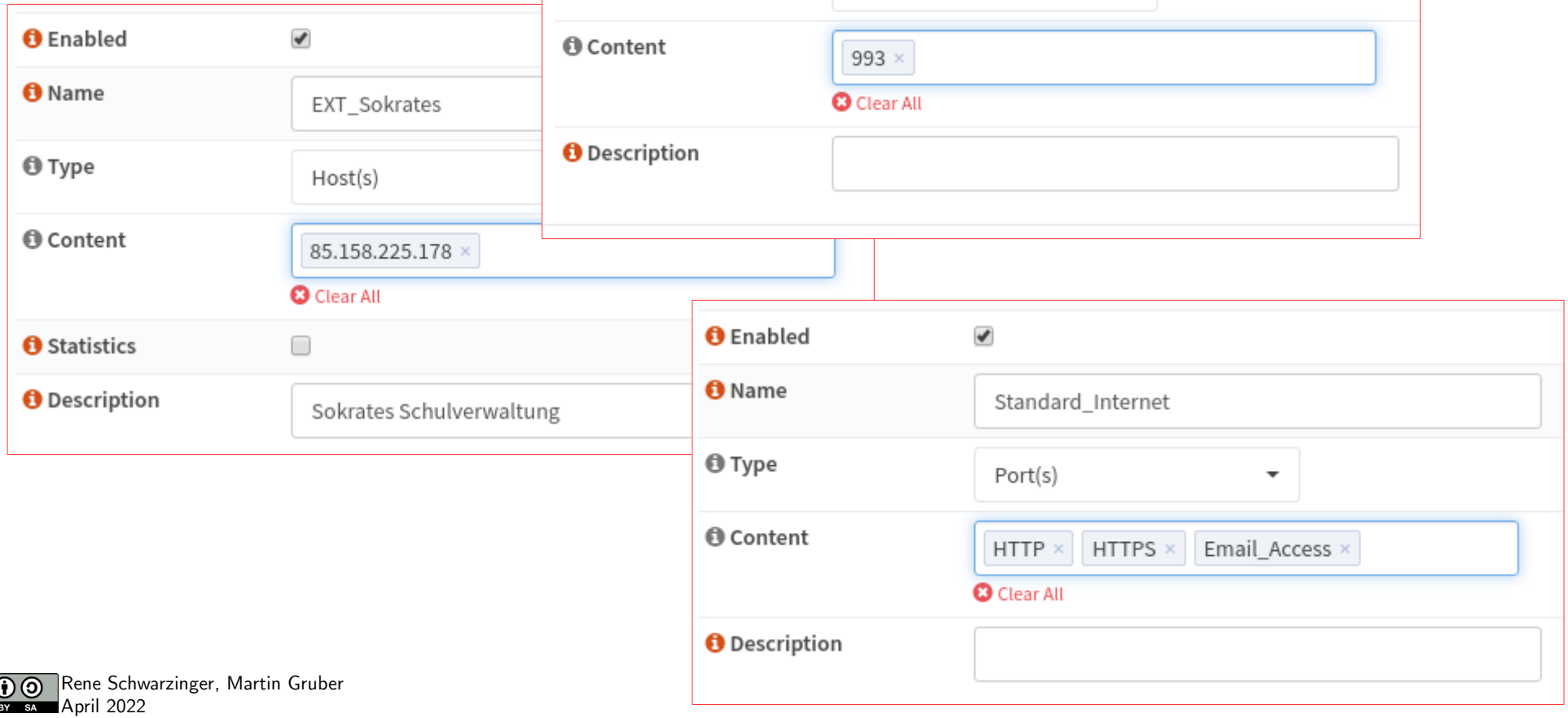
Aliases

Enabled	Name	Type	Description	Content	Commands
☑	EXT_Kieback_Peter	Host(s)	Kieback & Peter Regeltechnik GmbH	91.112.8.243	
☑	EXT_Ministerium	Host(s)	Bundesministerium für Bildung	85.158.228.26	
☑	EXT_Ministerium_HV	Host(s)	Bundesministerium für Bildung	193.46.171.50	
☑	EXT_Ministerium_PM_SAP	Host(s)	Bundesministerium für Bildung	193.46.171.13	
☑	EXT_Sokrates	Host(s)	Sokrates Schulverwaltung	85.158.225.178	
☑	EXT_WebUntis	Host(s)	WebUntis Elektronisches Klassenbuch	213.208.138.154	
☑	Email_Access	Port(s)		IMAP_STARTTLS,IMAP,IMAPS,POP3,POP3S,SMTP,SMTPS	

« ‹ 1 2 3 4 5 › »

Showing 15 to 21 of 148 entries

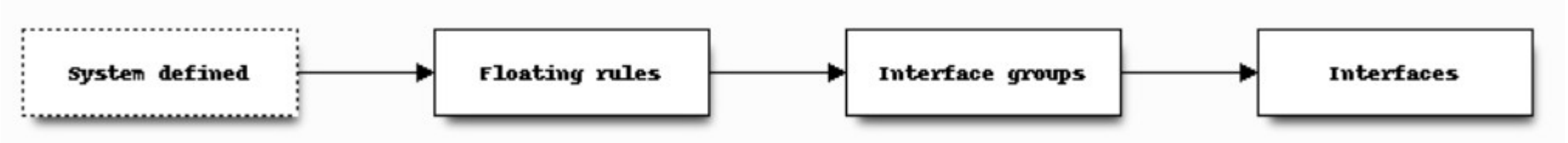
Aliases



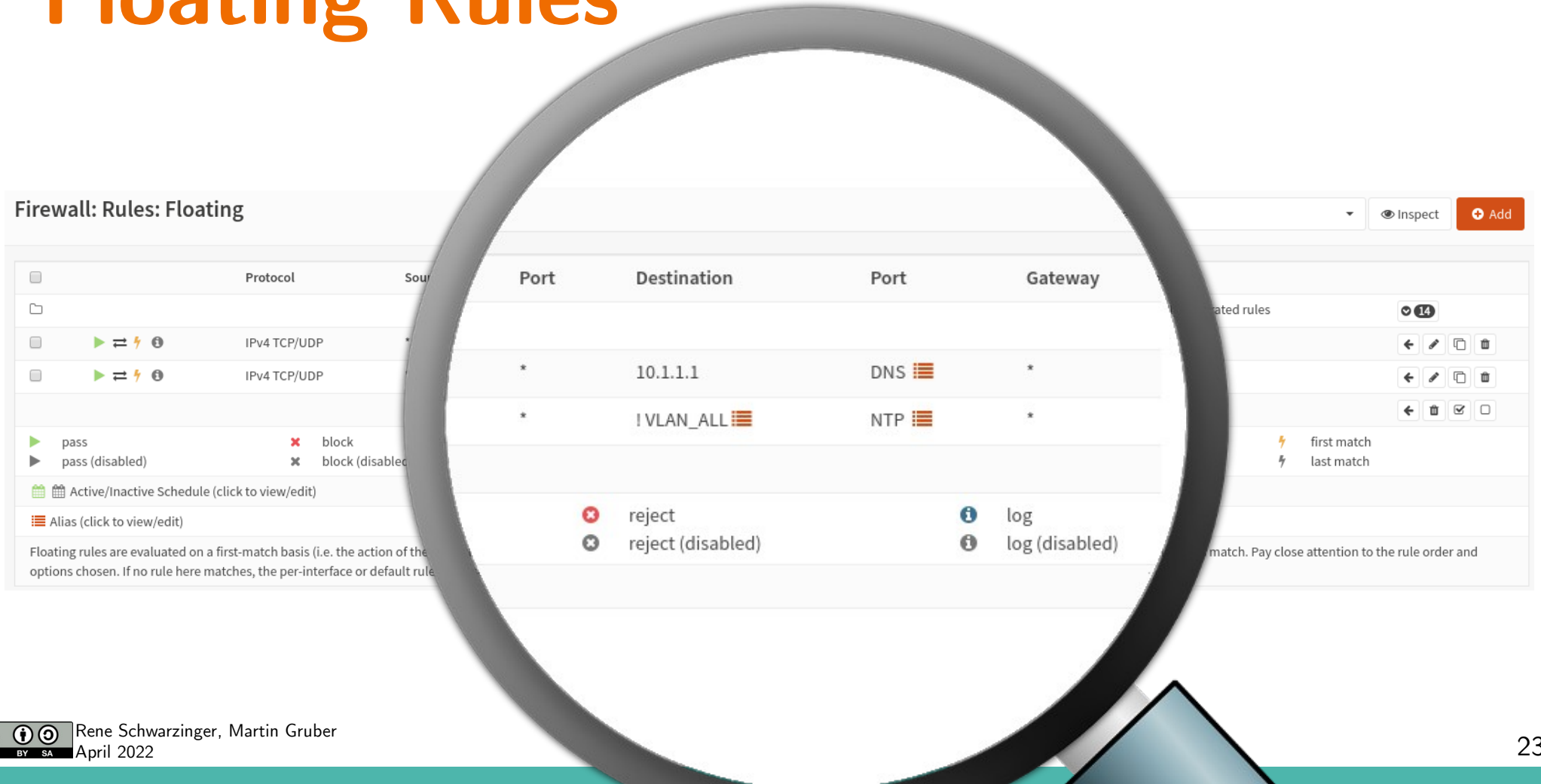
Rene Schwarzinger, Martin Gruber
April 2022

Rules

- Firewall rules are processed in sequence, first evaluating the Floating rules section followed by all rules which belong to interface groups and finally all interface rules.



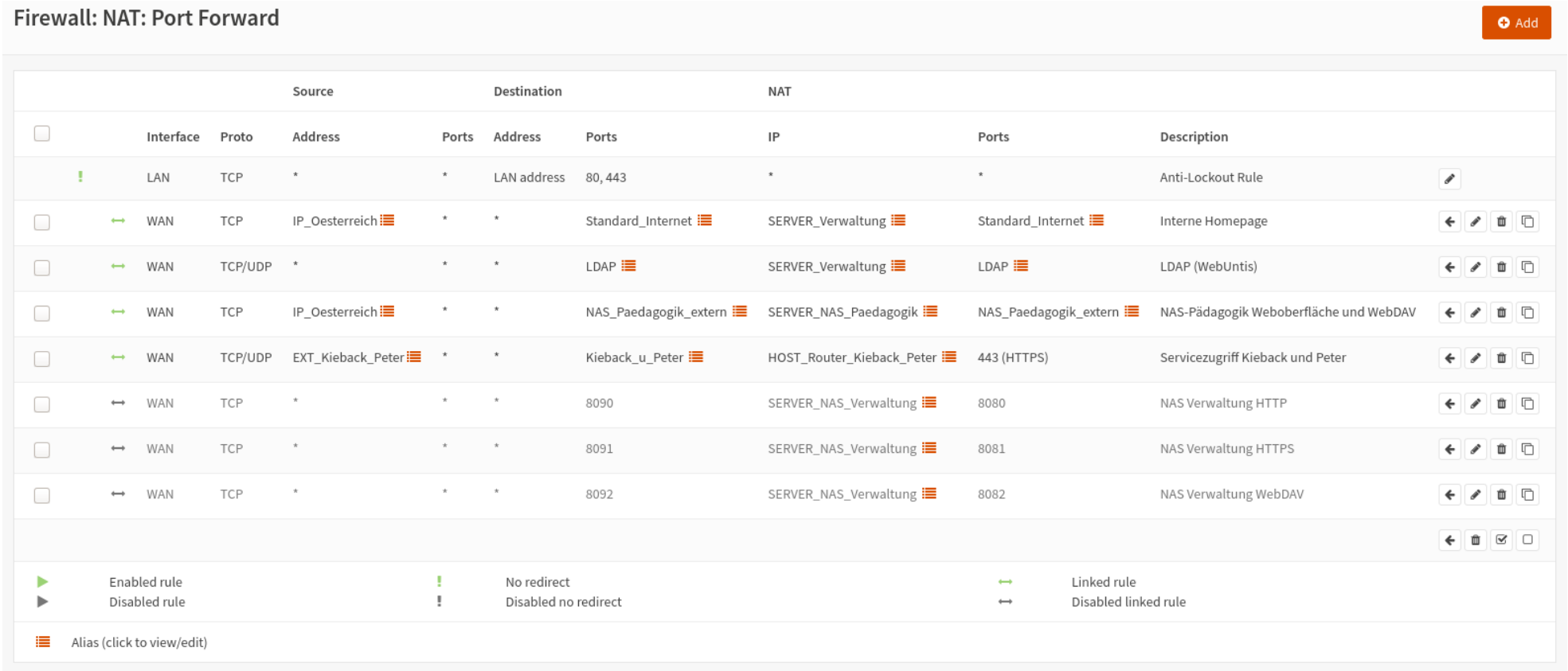
Floating Rules



Rules

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
							Automatically generated rules
IPv4 UDP	SERVER_RasPi_WOL_VLAN4	*	255.255.255.255	9	*	*	WOL in VLAN4 erlauben
IPv4 ICMP	*	*	*	*	*	*	PING
IPv4 TCP	HOST_Matura_Vorbereitungsraum	*	SERVER_Paedagogik	Papercut_intern	*	*	Matura-Vorbereitung Drucken
IPv4 TCP	BEcomputer	*	SERVER_Paedagogik	Papercut_intern	*	*	BE-Säle drucken
IPv4 TCP	*	*	SERVER_NAS_Paedagogik	NAS_Paedagogik	*	*	NAS Pädagogik
IPv4 TCP	*	*	SERVER_aptcache	APTCACHER	*	*	aptcache / Blockpage
IPv4 TCP	*	*	SERVER_Verwaltung	Standard_Internet	*	*	Interne Homepage
IPv4 TCP	*	*	SERVER_FOG	SSH	*	*	ssh auf FOG verhindern
IPv4 *	FOG_VLAN4	*	SERVER_FOG	*	*	*	Imaging mit FOG
IPv4 TCP/UDP	*	*	10.4.1.1	*	*	*	Blockieren des Gateways 10.4.1.1 (OPNSense
IPv4 TCP/UDP	*	*	192.168.1.1	*	*	*	Blockieren des Gateways 192.168.1.1 (OPNSense)
IPv4 *	*	*	VLAN4	*	*	*	SCHUELERNETZ
IPv4 *	*	*	10.0.0.0/8	*	*	*	INTERN
IPv4 TCP	*	*	*	Standard_Internet	*	*	INTERNET

Port Forwarding



Firewall: NAT: Port Forward

Add

			Source		Destination		NAT		
Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description	
LAN	TCP	*	*	LAN address	80, 443	*	*	Anti-Lockout Rule	
WAN	TCP	IP_Oesterreich	*	*	Standard_Internet	SERVER_Verwaltung	Standard_Internet	Interne Homepage	
WAN	TCP/UDP	*	*	*	LDAP	SERVER_Verwaltung	LDAP	LDAP (WebUntis)	
WAN	TCP	IP_Oesterreich	*	*	NAS_Paedagogik_extern	SERVER_NAS_Paedagogik	NAS_Paedagogik_extern	NAS-Pädagogik Weboberfläche und WebDAV	
WAN	TCP/UDP	EXT_Kieback_Peter	*	*	Kieback_u_Peter	HOST_Router_Kieback_Peter	443 (HTTPS)	Servicezugriff Kieback und Peter	
WAN	TCP	*	*	*	8090	SERVER_NAS_Verwaltung	8080	NAS Verwaltung HTTP	
WAN	TCP	*	*	*	8091	SERVER_NAS_Verwaltung	8081	NAS Verwaltung HTTPS	
WAN	TCP	*	*	*	8092	SERVER_NAS_Verwaltung	8082	NAS Verwaltung WebDAV	

Enabled rule
Disabled rule
No redirect
Disabled no redirect
Linked rule
Disabled linked rule
Alias (click to view/edit)

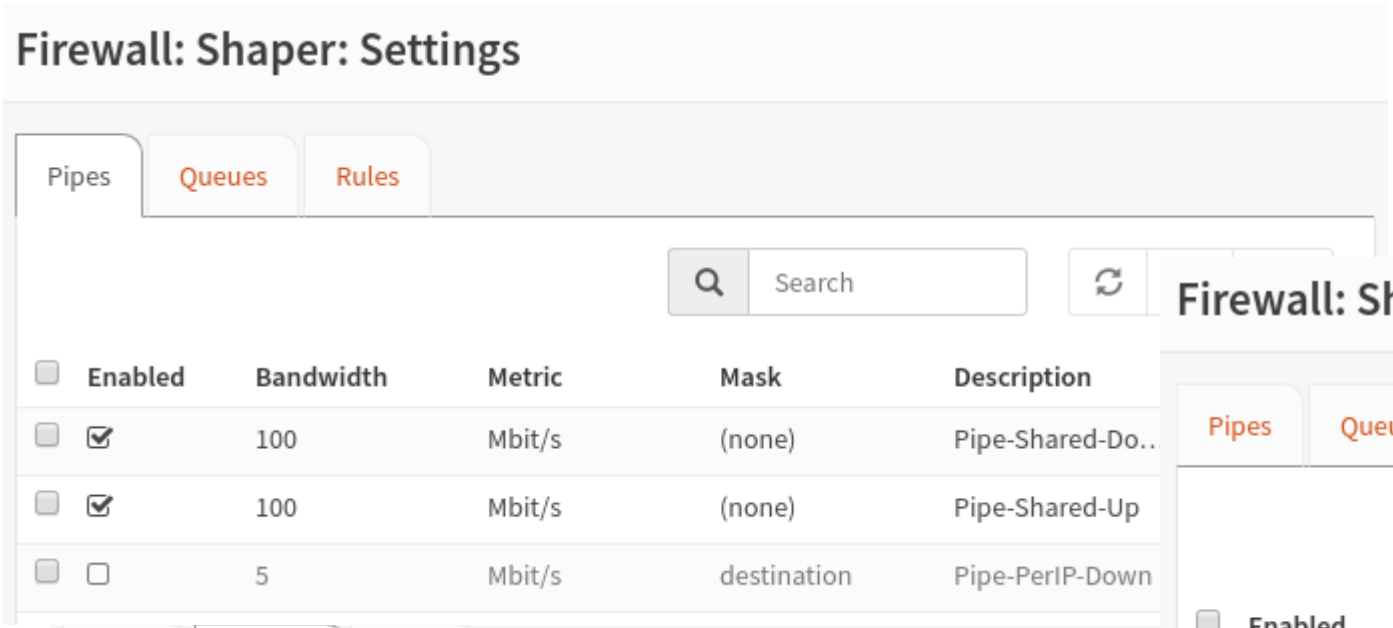
Traffic Shaper

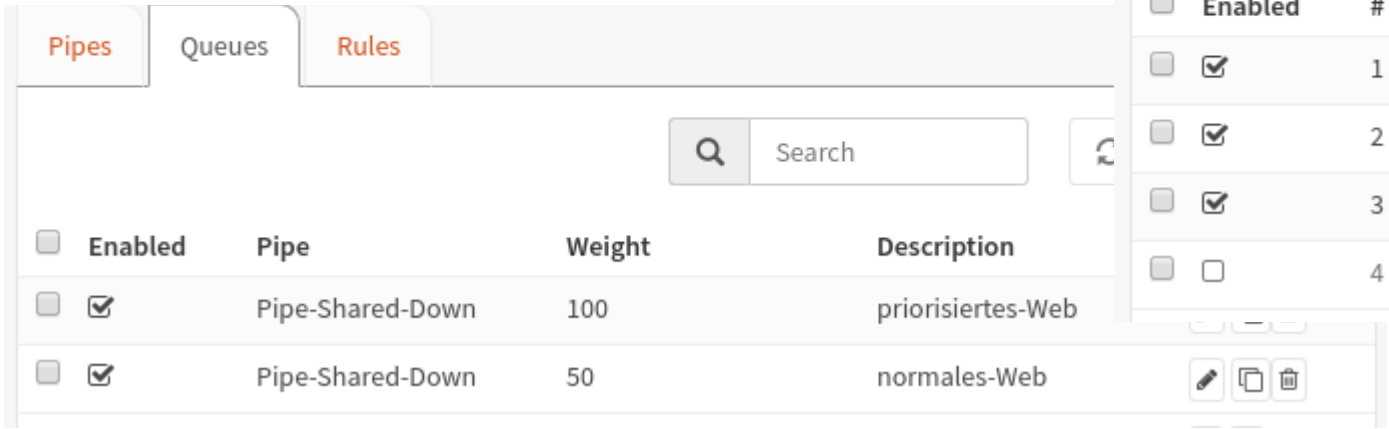
- Reserve dedicated bandwidth for a realtime traffic such as (hosted) Voice Over IP (VOIP) server.
- Share internet bandwidth amongst users evenly
- Limit maximum internet bandwidth users can consume
- Prioritize Applications (Weighted) using Queues
- Multi Interface shaping for a GuestNet

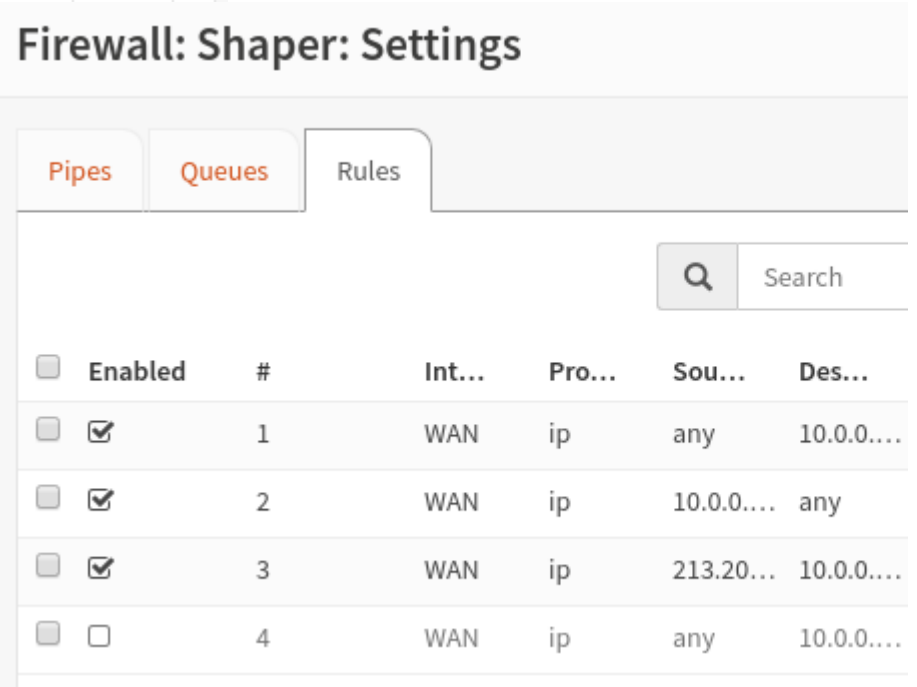
Download-Geschwindigkeit:
95.246 kbit/s

Upload-Geschwindigkeit:
79.387 kbit/s

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


Firewall: Shaper: Settings
Pipes
Queues
Rules
Search
Enabled
Bandwidth
Metric
Mask
Description
100
Mbit/s
(none)
Pipe-Shared-Do..
100
Mbit/s
(none)
Pipe-Shared-Up
5
Mbit/s
destination
Pipe-PerIP-Down


Pipes
Queues
Rules
Search
Enabled
Pipe
Weight
Description
Pipe-Shared-Down
100
priorisiertes-Web
Pipe-Shared-Down
50
normales-Web


Firewall: Shaper: Settings
Pipes
Queues
Rules
Search
Enabled
#
Int...
Pro...
Sou...
Des...
1
WAN
ip
any
10.0.0....
2
WAN
ip
10.0.0....
any
3
WAN
ip
213.20...
10.0.0....
4
WAN
ip
any
10.0.0....

Shaper Rules

Source	Destination	Target	Description
any	10.0.0.0/8	normales-Web	Rule-Shared-Down
10.0.0.0/8	any	Pipe-Shared-Up	Rule-Shared-Up
213.208.138.154/32,85.158.225....	10.0.0.0/8	priorisiertes-Web	Rule-Shared-Down-Priorisiert - ...
any	10.0.0.0/8	normales-Web	Rule-PerIP-Down

OPNsense

Fazit