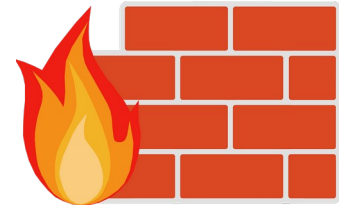
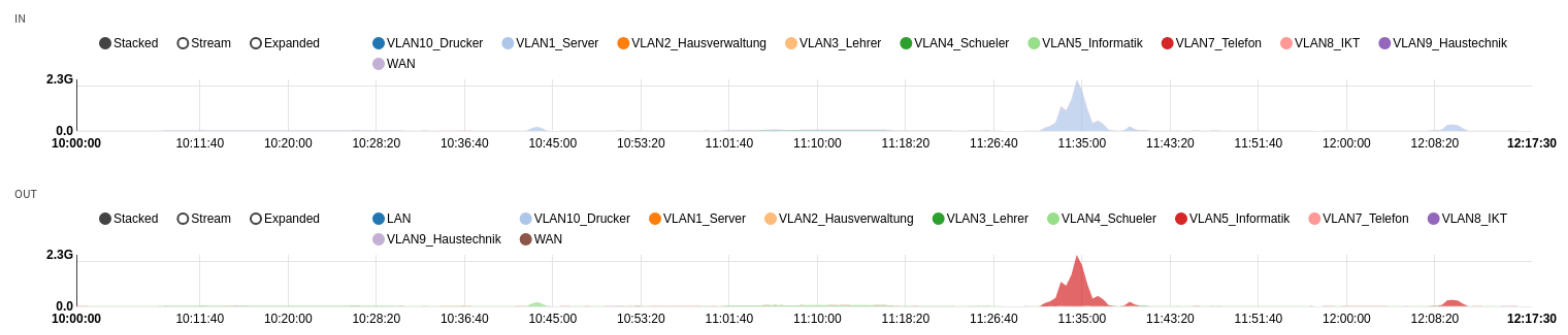

OPNsense



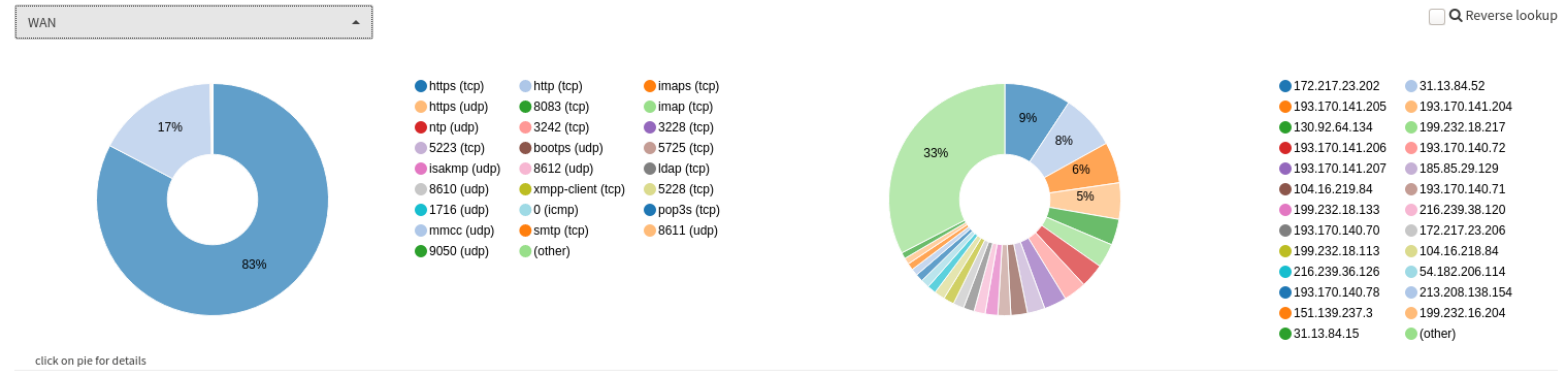
— Planung und Migration —

- Lobby
- Reporting
 - Health
 - Insight
 - NetFlow
 - Settings
 - Traffic
- System
- Interfaces
- Firewall
- VPN
- Services
- Power
- Help

Interface totals (bits/sec)

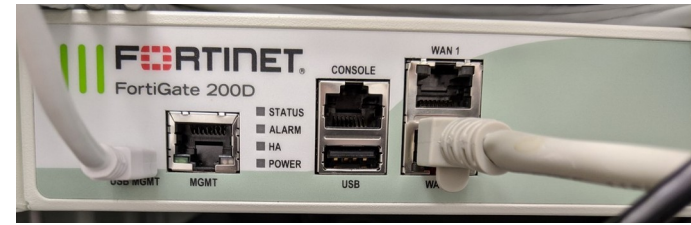


Top usage ports / sources (bytes)



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.

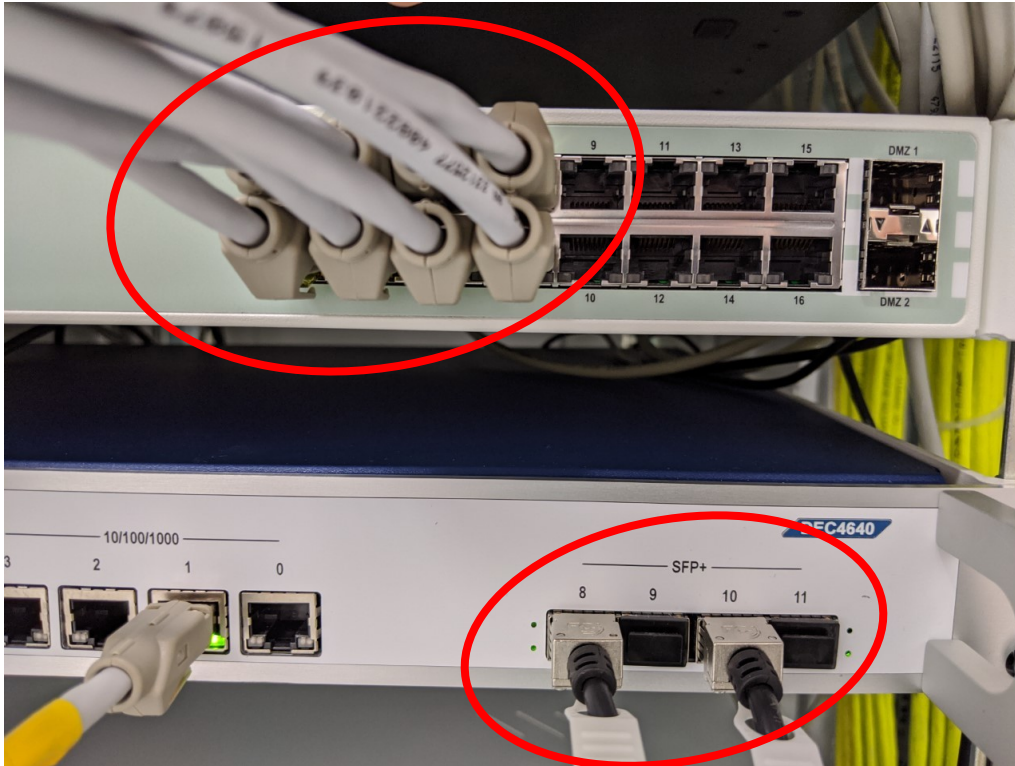
FOSS

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

applianceshop.eu (2800 €)



Redundante DACs



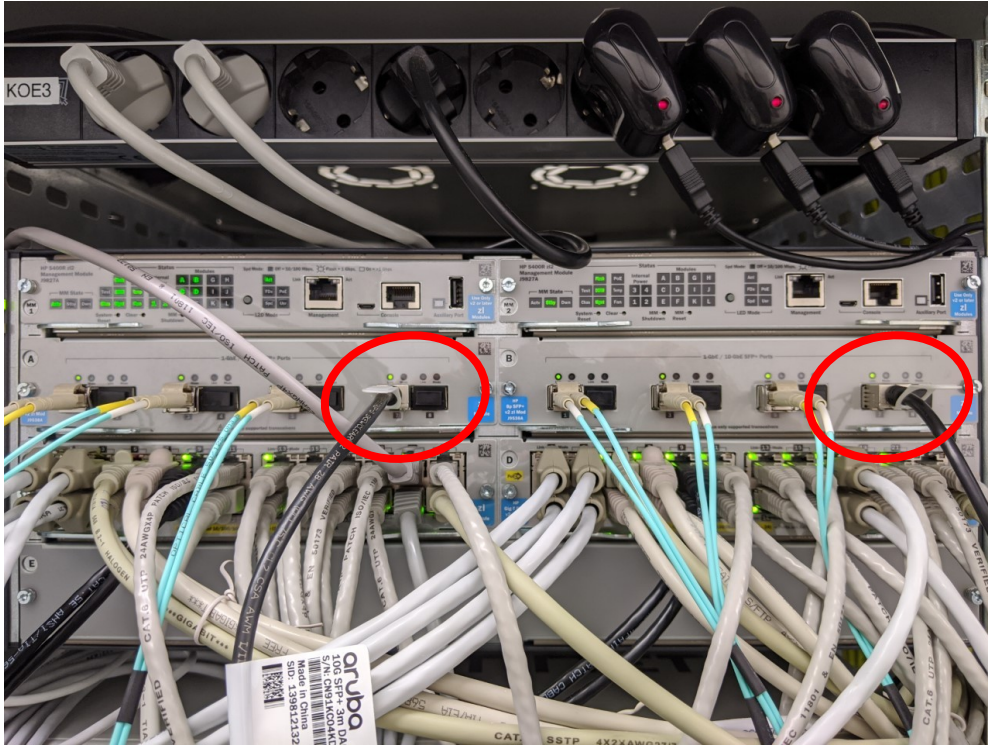
Vorher (Fortinet 100D):

4 redundante Trunks = 8 x LAN

Nachher (OPNsense):

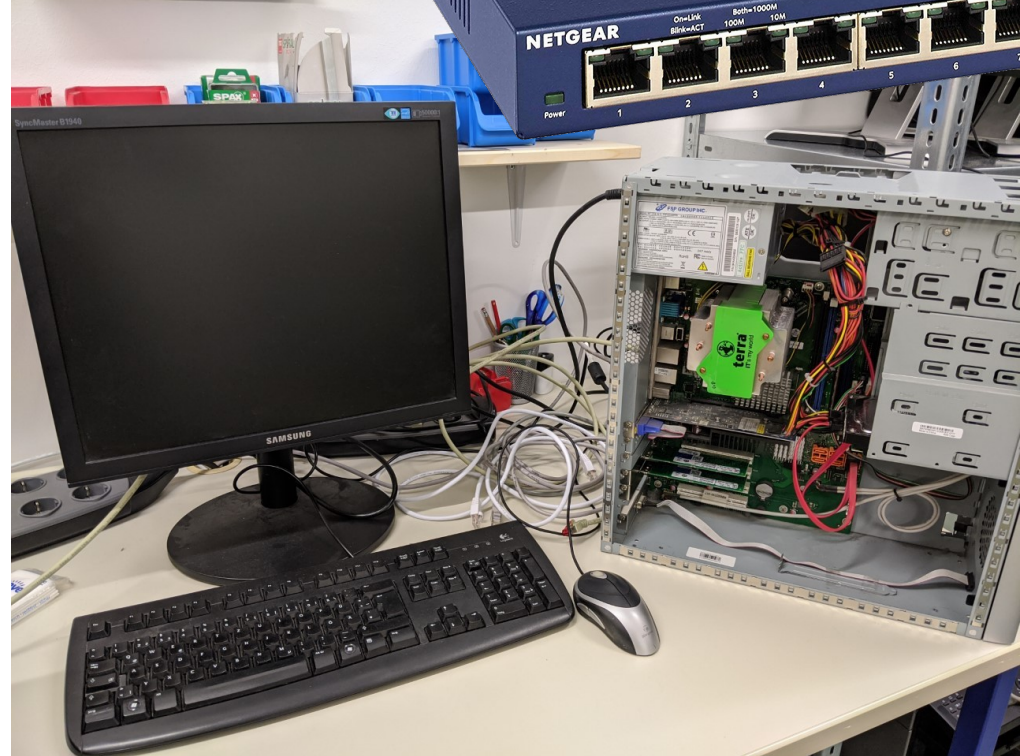
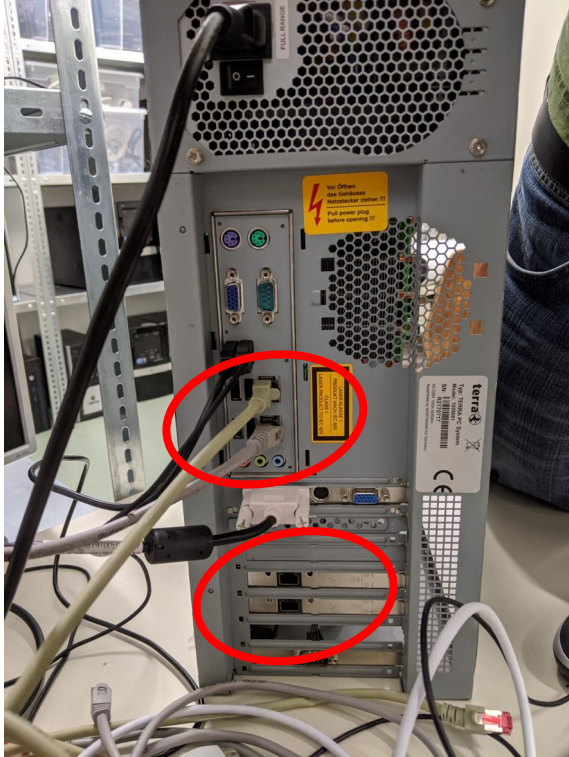
1 redundanter Trunk = 2 x SFP+

Gegenstelle HP5406R



1 GbE / 10 Gb SFP+ Ports
redundante Ausführung

Vorbereitung



Anpassungen Core-Switch

```
trunk A?,B? trk100 lacp

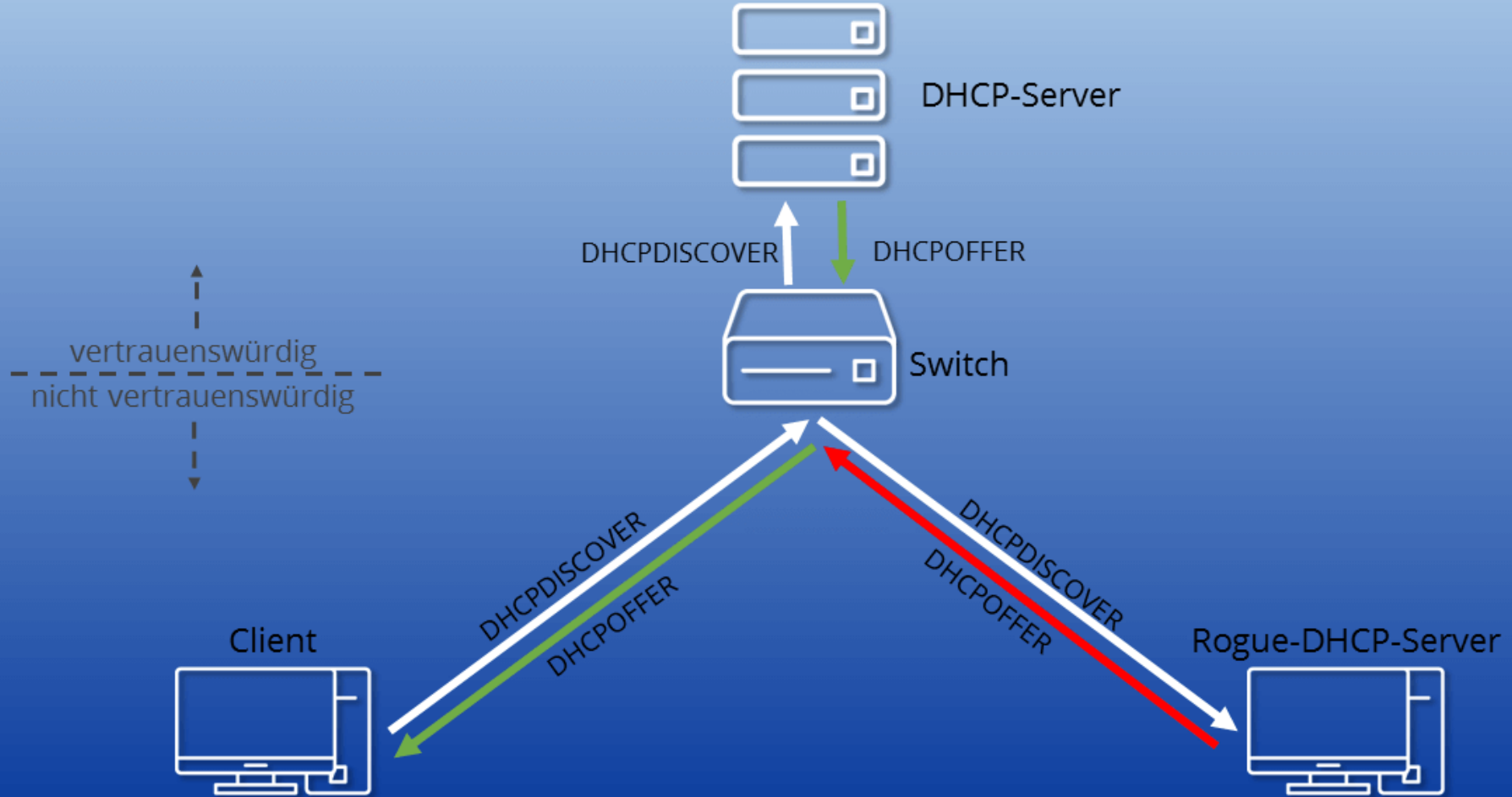
interface trk100

    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



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

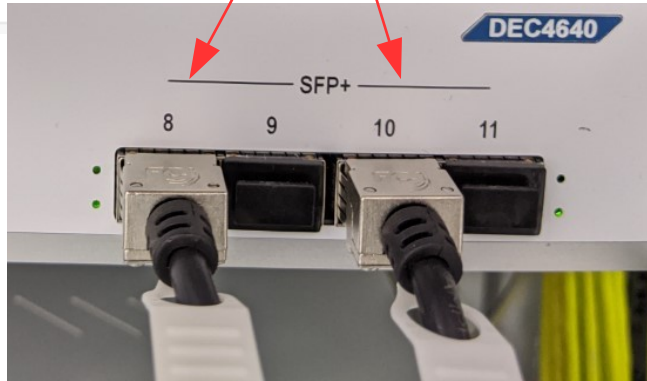
The first interface is the LAN interface. Type the appropriate interface name, for example "em0". The second interface is the WAN interface. Type the appropriate interface name, eg. "em1". Possible additional interfaces can be assigned as OPT interfaces. If you assigned all your interfaces you can press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



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 static
- ROUNDROBIN




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	 

OPNsense (c) 2014-2020 Deciso B.V.

Assignments

Interface	Network port
<u>LAN</u>	 igb0 (00:03:2d:43:91:87) ▼
<u>Trk100</u>	 lagg0 (Trk100) ▼
<u>VLAN1_Server</u>	 vlan 1 on lagg0 (Servernetz) ▼

Interface	Network port
<u>LAN</u>	 igb0 (00:03:2d:43:91:87) ▼ 
<u>Trk100</u>	 lagg0 (Trk100) ▼ 
<u>VLAN1_Server</u>	 vlan 1 on lagg0 (Servernetz) ▼ 
<u>VLAN2_Hausverwaltung</u>	 vlan 2 on lagg0 (Hausverwaltung) ▼ 
<u>VLAN3_Lehrer</u>	 vlan 3 on lagg0 (Lehrer) ▼ 
<u>VLAN4_Schueler</u>	 vlan 4 on lagg0 (Schueler) ▼ 
<u>VLAN5_Informatik</u>	 vlan 5 on lagg0 (Informatik) ▼ 
<u>VLAN6_PCLabor</u>	 vlan 6 on lagg0 (Pclabor) ▼ 
<u>VLAN7_Telefon</u>	 vlan 7 on lagg0 (Telefon) ▼ 
<u>VLAN8_IKT</u>	 vlan 8 on lagg0 (IKT) ▼ 
<u>VLAN9_Haustechnik</u>	 vlan 9 on lagg0 (Haustechnik) ▼ 
<u>VLAN10_Drucker</u>	 vlan 10 on lagg0 (Drucker) ▼ 
<u>WAN</u>	 igb1 (00:03:2d:43:91:86) ▼ 
New interface:	 ixl1 (00:03:2d:40:d2:e9) ▼  
	Description <input type="text"/>

Assignments (Trk 100)

Trk100 lagg0 (Trk100) 🗑️

zur Übertragung
der VLANs

Interfaces: Other Types: VLAN

Interface VLAN Edit full help

i Parent interface lagg0 (00:03:2d:40:d2:e8) [Trk100]

i VLAN tag 4

i VLAN priority Best Effort (0, default)

i Description Schueler

Save Cancel

System Settings for WAN

System: Gateways: Single



Name	Interface	Protocol	Priority	Gateway	Monitor IP	RTT	RTTd	Loss	Status	Description
<input type="checkbox"/> WAN_GWv4 (active)	WAN	IPv4	255 (upstream)	193.171.231.141	193.171.231.141	0.8 ms	1.8 ms	0.0 %	Online	

WAN

igb1 (00:03:2d:43:91:86) ▼



zuvor Gateway nach
außen hin definieren

DNS servers

DNS Server

Use gateway

9.9.9.9

none ▼

8.8.8.8


none ▼

DHCP Settings for VLANs

Services: DHCPv4: [VLAN4_Schueler] ▶ ↺ ◻







[full help](#)

Enable	<input checked="" type="checkbox"/>	Enable DHCP server on the VLAN4_Schueler interface
Deny unknown clients	<input type="checkbox"/>	Deny unknown clients
Subnet	10.4.0.0	Subnet
Subnet mask	255.255.0.0	Subnet mask
Available range	10.4.0.1 - 10.4.255.254	Available range
Range	from 10.4.5.1	Range
Additional Pools	Pool Start	+
WINS servers		
DNS servers	10.1.1.1	
Gateway		




























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

<input type="checkbox"/>	Enabled	Name	Type	Description	Content	Commands
<input type="checkbox"/>	<input checked="" type="checkbox"/>	EXT_Kieback_Peter	Host(s)	Kieback & Peter Regeltechnik GmbH	91.112.8.243	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	EXT_Ministerium	Host(s)	Bundesministerium für Bildung	85.158.228.26	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	EXT_Ministerium_HV	Host(s)	Bundesministerium für Bildung	193.46.171.50	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	EXT_Ministerium_PM_SAP	Host(s)	Bundesministerium für Bildung	193.46.171.13	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	EXT_Sokrates	Host(s)	Sokrates Schulverwaltung	85.158.225.178	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	EXT_WebUntis	Host(s)	WebUntis Elektronisches Klassenbuch	213.208.138.154	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	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

Enabled

Name EXT_Sokrates

Type Host(s)

Content 85.158.225.178 ×
[Clear All](#)

Statistics

Description Sokrates Schulverwaltung

Enabled

Name IMAPS

Type Port(s)

Content 993 ×
[Clear All](#)

Description

Enabled

Name Standard_Internet

Type Port(s)

Content HTTP × HTTPS × Email_Access ×
[Clear All](#)

Description

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

Firewall: Rules: Floating

Inspect Add

Port	Destination	Port	Gateway
*	10.1.1.1	DNS	*
*	VLAN_ALL	NTP	*
reject		log	
reject (disabled)		log (disabled)	

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

Floating rules are evaluated on a first-match basis (i.e. the action of the first rule that matches is the action chosen. If no rule here matches, the per-interface or default rule is used).

Matched rules 14

first match last match

match. Pay close attention to the rule order and

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 ⓘ	APTACHER ⓘ	*	*	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					
<input type="checkbox"/>	Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description	
<input type="checkbox"/>	LAN	TCP	*	*	LAN address	80, 443	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	WAN	TCP	IP_Oesterreich	*	*	Standard_Internet	SERVER_Verwaltung	Standard_Internet	Interne Homepage	
<input type="checkbox"/>	WAN	TCP/UDP	*	*	*	LDAP	SERVER_Verwaltung	LDAP	LDAP (WebUntis)	
<input type="checkbox"/>	WAN	TCP	IP_Oesterreich	*	*	NAS_Paedagogik_extern	SERVER_NAS_Paedagogik	NAS_Paedagogik_extern	NAS-Pädagogik Weboberfläche und WebDAV	
<input type="checkbox"/>	WAN	TCP/UDP	EXT_Kieback_Peter	*	*	Kieback_u_Peter	HOST_Router_Kieback_Peter	443 (HTTPS)	Servicezugriff Kieback und Peter	
<input type="checkbox"/>	WAN	TCP	*	*	*		8090	SERVER_NAS_Verwaltung	8080	NAS Verwaltung HTTP
<input type="checkbox"/>	WAN	TCP	*	*	*		8091	SERVER_NAS_Verwaltung	8081	NAS Verwaltung HTTPS
<input type="checkbox"/>	WAN	TCP	*	*	*		8092	SERVER_NAS_Verwaltung	8082	NAS Verwaltung WebDAV
	Enabled rule			No redirect			Linked rule			
	Disabled rule			Disabled no redirect			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

Firewall: Shaper: Settings

Pipes Queues Rules

Search

<input type="checkbox"/> Enabled	Bandwidth	Metric	Mask	Description
<input checked="" type="checkbox"/>	100	Mbit/s	(none)	Pipe-Shared-Do...
<input checked="" type="checkbox"/>	100	Mbit/s	(none)	Pipe-Shared-Up
<input type="checkbox"/>	5	Mbit/s	destination	Pipe-PerIP-Down

Firewall: Shaper: Settings

Pipes Queues Rules




Search

<input type="checkbox"/> Enabled	#	Int...	Pro...	Sou...	Des...
<input checked="" type="checkbox"/>	1	WAN	ip	any	10.0.0....
<input checked="" type="checkbox"/>	2	WAN	ip	10.0.0....	any
<input checked="" type="checkbox"/>	3	WAN	ip	213.20...	10.0.0....
<input type="checkbox"/>	4	WAN	ip	any	10.0.0....

Pipes Queues Rules

Search

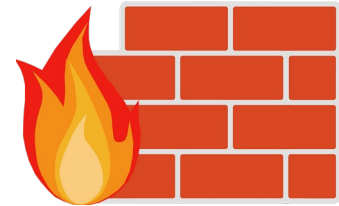
<input type="checkbox"/> Enabled	Pipe	Weight	Description
<input checked="" type="checkbox"/>	Pipe-Shared-Down	100	priorisiertes-Web
<input checked="" type="checkbox"/>	Pipe-Shared-Down	50	normales-Web

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

—
