lrz Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

pfSense – Virtuelle Firewalls am Leibniz-Rechenzentrum

Was ist eine Firewall?

- Beschränkt den Zugriff in bzw. aus einem Netz (VLAN)

- Regel-basierte Filterung des Netzverkehrs
  → Protokoll, Quelle, Ziel, Port

- Analyse von Paketinhalten und Netzverkehr durch Zusatzmodule
  → Intrusion Detection/Prevention System (IDS/IPS)
  → Content Filter für HTTP- und SMTP-Verbindungen

Was ist eine Firewall **nicht**?

- Ein vollständiger Ersatz für ein Sicherheitskonzept

- Ein Schutz vor unmittelbaren Risiken
  → Datenmanipulation und Datenverlust
  → Beeinträchtigung der Verfügbarkeit von Systemen
  → Offenlegung von Daten

- Ein Schutz vor Angriffen aus dem eigenen Netz

Dienst des LRZ: Virtuelle Firewalls

- Das LRZ stellt jedem Kunden eine **eigene Instanz** einer virtuellen Firewall bereit
- Ausfallsicherheit durch High-Availability
- Auf MWN zugeschnittenes, vorkonfiguriertes System
- Tägliche Sicherung der Konfiguration der Firewalls
- Absicherung gegen Stromausfall, Leitungsausfall, Hardwareschäden

Dienst des LRZ: Virtuelle Firewalls

- Software-Updates
- System-Monitoring und zentralisiertes Management
- Optional: dedizierte Interfaces (zusätzliche Kosten)

Evaluation verschiedener FW-Produkte

Gewinner: pfSense

- *pfSense ist eine Firewall-Distribution auf der Basis des Betriebssystems FreeBSD und des Paketfilters pf.*
- pfSense ist 2004 als Abspaltung von m0n0wall hervorgegangen

Website	https://www.pfsense.org/
Doku	https://doc.pfsense.org/index.php/Main_Page
Forum	https://forum.pfsense.org/index.php

Konfigurieren der Firewall

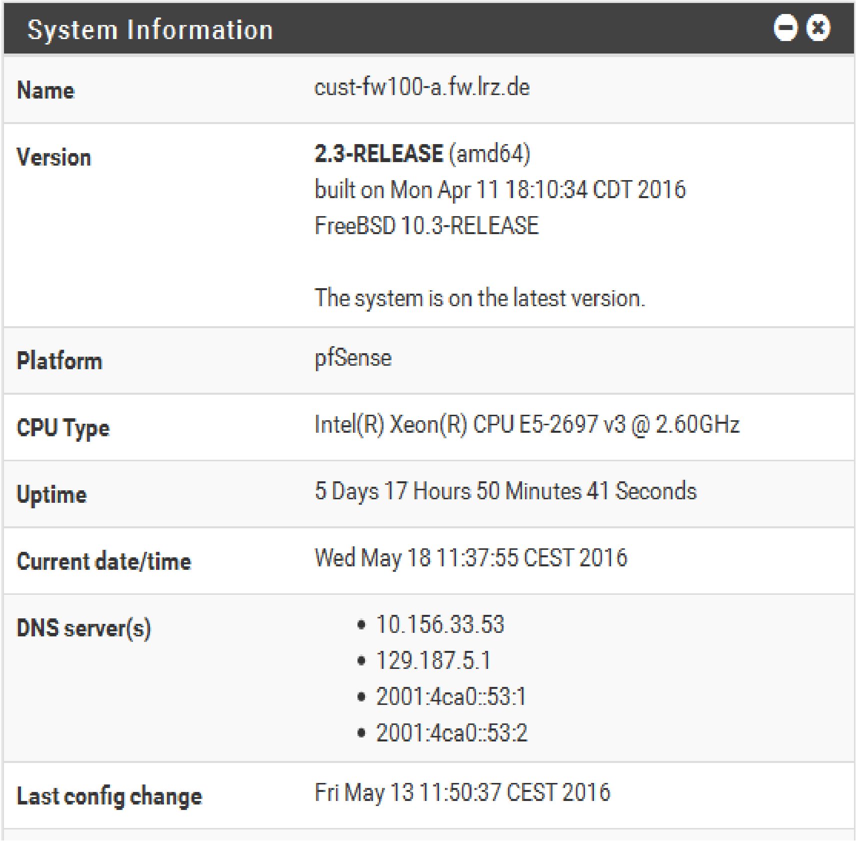
- Die Firewall kann über ihre **IP-Adresse** oder ihren **Hostname** (z.B. cust-fw<XX>.fw.lrz.de) erreicht werden

- Konfiguration über
  1. Webinterface *https://<Firewall-IP-Adresse>*
  2. Secure Shell *ssh <user>@<Firewall-IP-Adresse>*

- Authentifizierung per **LDAP** mit **LRZ-SIM-Kennung**

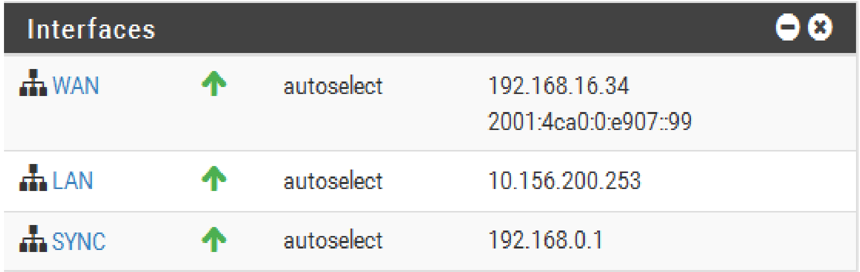
Das Dashboard

Bietet allgemeine Informationen über Status von **Hard-** und **Software**



System Information

Name	cust-fw100-a.fw.lrz.de
Version	**2.3-RELEASE** (amd64) built on Mon Apr 11 18:10:34 CDT 2016 FreeBSD 10.3-RELEASE The system is on the latest version.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz
Uptime	5 Days 17 Hours 50 Minutes 41 Seconds
Current date/time	Wed May 18 11:37:55 CEST 2016
DNS server(s)	• 10.156.33.53 • 129.187.5.1 • 2001:4ca0::53:1 • 2001:4ca0::53:2
Last config change	Fri May 13 11:50:37 CEST 2016

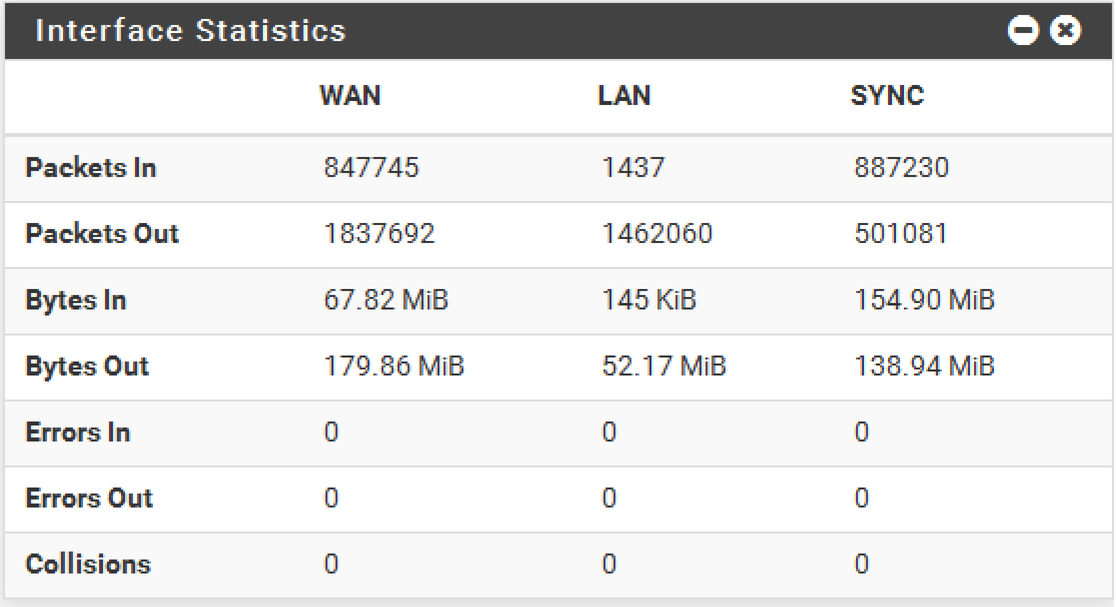


Interfaces

WAN	↑	autoselect	192.168.16.34 2001:4ca0:0:e907::99
LAN	↑	autoselect	10.156.200.253
SYNC	↑	autoselect	192.168.0.1

Das Dashboard

Statistiken und Traffic Graphen (Live) der Netzinterfaces

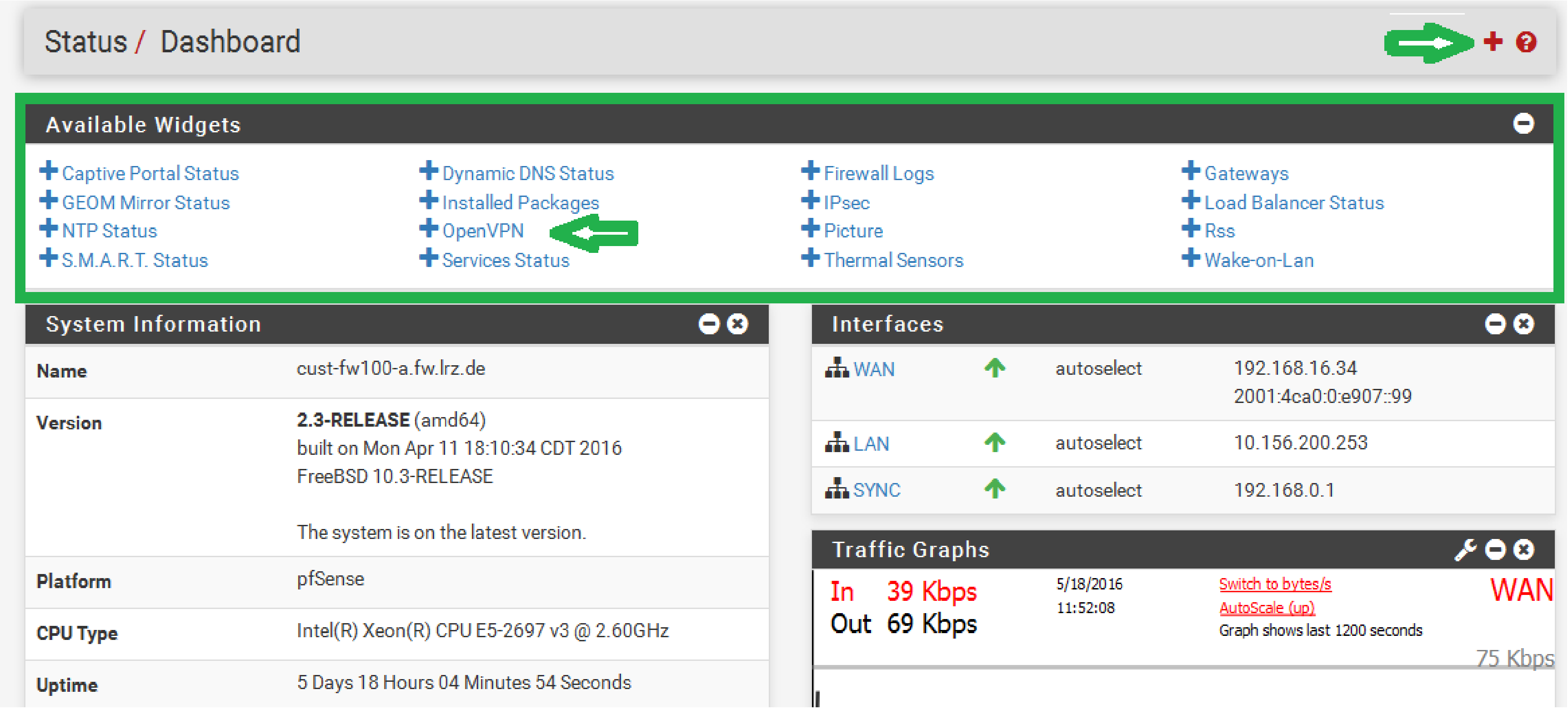


Interface Statistics

	WAN	LAN	SYNC
Packets In	847745	1437	887230
Packets Out	1837692	1462060	501081
Bytes In	67.82 MiB	145 KiB	154.90 MiB
Bytes Out	179.86 MiB	52.17 MiB	138.94 MiB
Errors In	0	0	0
Errors Out	0	0	0
Collisions	0	0	0

Das Dashboard

Weitere Widgets können dem Dashboard hinzugefügt werden (z.B. Informationen zum **OpenVPN**)



Status / Dashboard

Available Widgets

- Captive Portal Status
- GEOM Mirror Status
- NTP Status
- S.M.A.R.T. Status
- Dynamic DNS Status
- Installed Packages
- OpenVPN
- Services Status
- Firewall Logs
- IPsec
- Picture
- Thermal Sensors
- Gateways
- Load Balancer Status
- Rss
- Wake-on-Lan

System Information

Name	cust-fw100-a.fw.lrz.de
Version	**2.3-RELEASE** (amd64) built on Mon Apr 11 18:10:34 CDT 2016 FreeBSD 10.3-RELEASE The system is on the latest version.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz
Uptime	5 Days 18 Hours 04 Minutes 54 Seconds

Interfaces

WAN	↑	autoselect	192.168.16.34 2001:4ca0:0:e907::99
LAN	↑	autoselect	10.156.200.253
SYNC	↑	autoselect	192.168.0.1

Traffic Graphs

In 39 Kbps
Out 69 Kbps

5/18/2016
11:52:08

Switch to bytes/s
AutoScale (up)
Graph shows last 1200 seconds

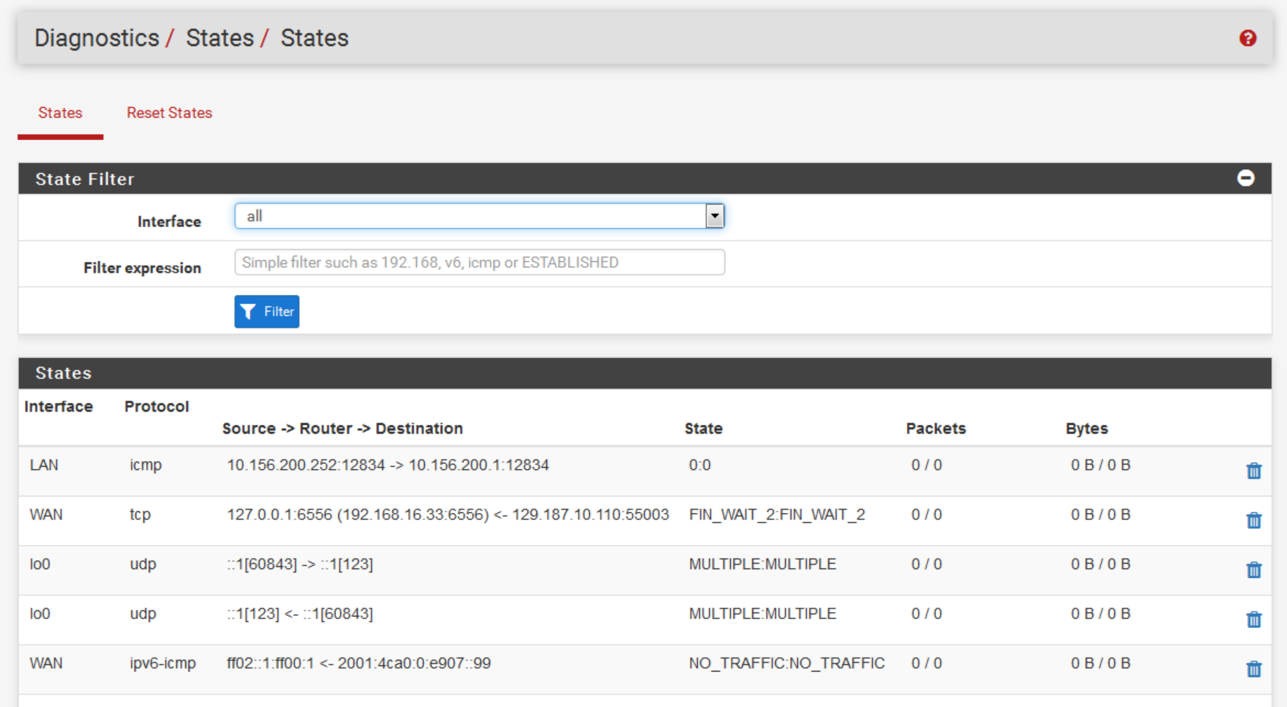
WAN

75 Kbps

State table

Status aktiver Verbindungen

Diagnostics → States



Diagnostics / States / States

State Filter

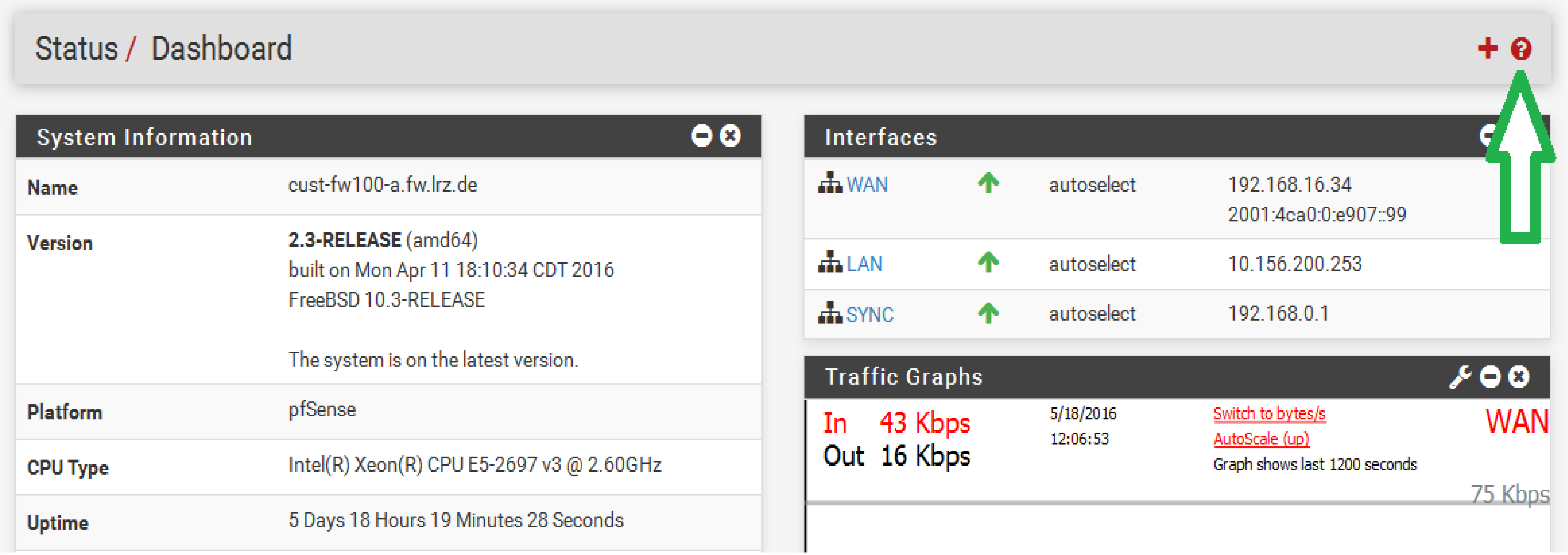
Interface	all
Filter expression	Simple filter such as 192.168, v6, icmp or ESTABLISHED
	Filter

States

Interface	Protocol	Source -> Router -> Destination	State	Packets	Bytes	
LAN	icmp	10.156.200.252:12834 -> 10.156.200.1:12834	0:0	0 / 0	0 B / 0 B	🗑
WAN	tcp	127.0.0.1:6556 (192.168.16.33:6556) <- 129.187.10.110:55003	FIN_WAIT_2:FIN_WAIT_2	0 / 0	0 B / 0 B	🗑
lo0	udp	::1[60843] -> ::1[123]	MULTIPLE:MULTIPLE	0 / 0	0 B / 0 B	🗑
lo0	udp	::1[123] <- ::1[60843]	MULTIPLE:MULTIPLE	0 / 0	0 B / 0 B	🗑
WAN	ipv6-icmp	ff02::1:ff00:1 <- 2001:4ca0:0:e907::99	NO_TRAFFIC:NO_TRAFFIC	0 / 0	0 B / 0 B	🗑

Hilfe auf der pfSense

Auf jeder Seite der pfSense gibt es eine dazugehörige dokumentierte **Hilfe**



Status / Dashboard

System Information

Name	cust-fw100-a.fw.lrz.de
Version	**2.3-RELEASE** (amd64) built on Mon Apr 11 18:10:34 CDT 2016 FreeBSD 10.3-RELEASE The system is on the latest version.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz
Uptime	5 Days 18 Hours 19 Minutes 28 Seconds

Interfaces

WAN	↑	autoselect	192.168.16.34 2001:4ca0:0:e907::99
LAN	↑	autoselect	10.156.200.253
SYNC	↑	autoselect	192.168.0.1

Traffic Graphs

In 43 Kbps
Out 16 Kbps

5/18/2016
12:06:53

Switch to bytes/s
AutoScale (up)
Graph shows last 1200 seconds

WAN

75 Kbps

Online: https://doc.pfsense.org/index.php/MainPage

Regeln des Paketfilters – Ausgangslage

- Standardregelung:

Inside			
	any	any	deny
Outside			
	any	any	deny

Diese Regeln werden implizit angewendet, falls keine expliziten Regeln definiert sind

- Der gesamte Verkehr wird geblockt!

Erstellen von Regeln – Beispiele

Regeln werden der Reihe nach abgearbeitet!

Beispiel 1

Abarbeitungsreihenfolge

Inside

10.1.2.3	129.187.255.234	http	permit
any	any	http	deny

→ **Erlaubt** den Zugriff des Systems mit der IP-Adresse 10.1.2.3 auf http://www.lrz.de

Beispiel 2

Abarbeitungsreihenfolge

Inside

any	any	http	deny
10.1.2.3	129.187.255.234	http	permit

→ **Verhindert** den Zugriff auf http://www.lrz.de, da die oberste Regel zuerst angewandt wird

Erstellen von Regeln – Beispiele

Stateful packet inspection:

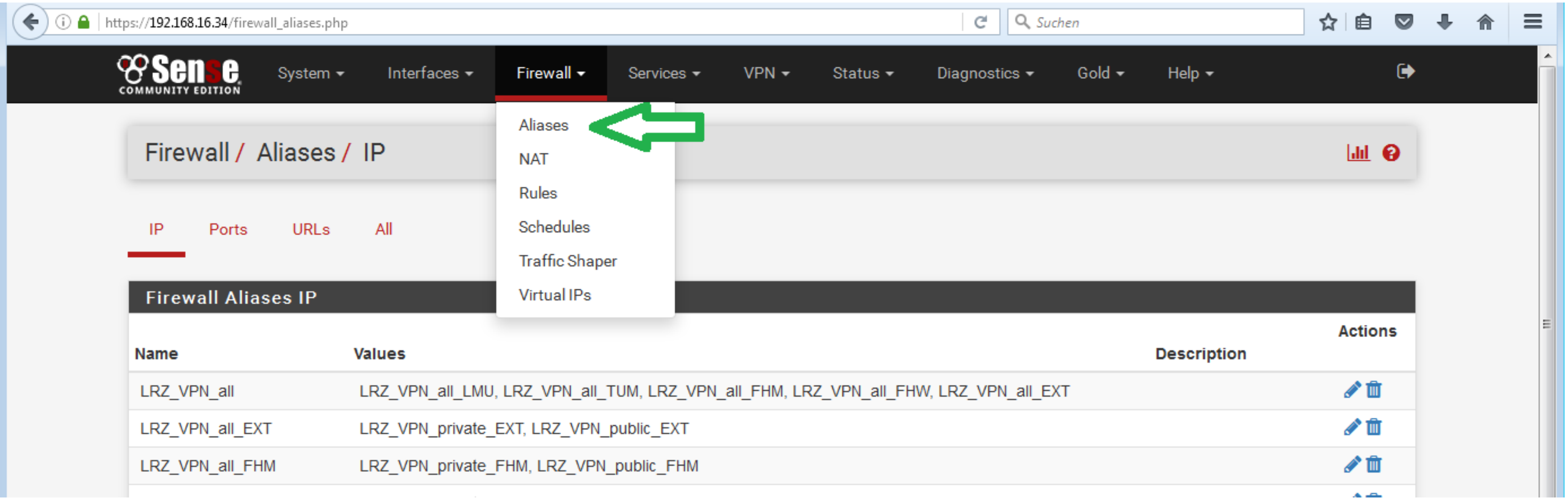
- Antworten auf Anfragen aus dem Inside-Netz werden nicht geblockt

- Hingegen Anfragen, aus dem Outside-Netz in das Inside-Netz, ohne vorherige Anfrage, werden geblockt

Aliase

Platzhalter („sprechende Namen“) und Gruppierung einzelner Hosts, Netze und Ports

Firewall → Aliases



Firewall / Aliases / IP

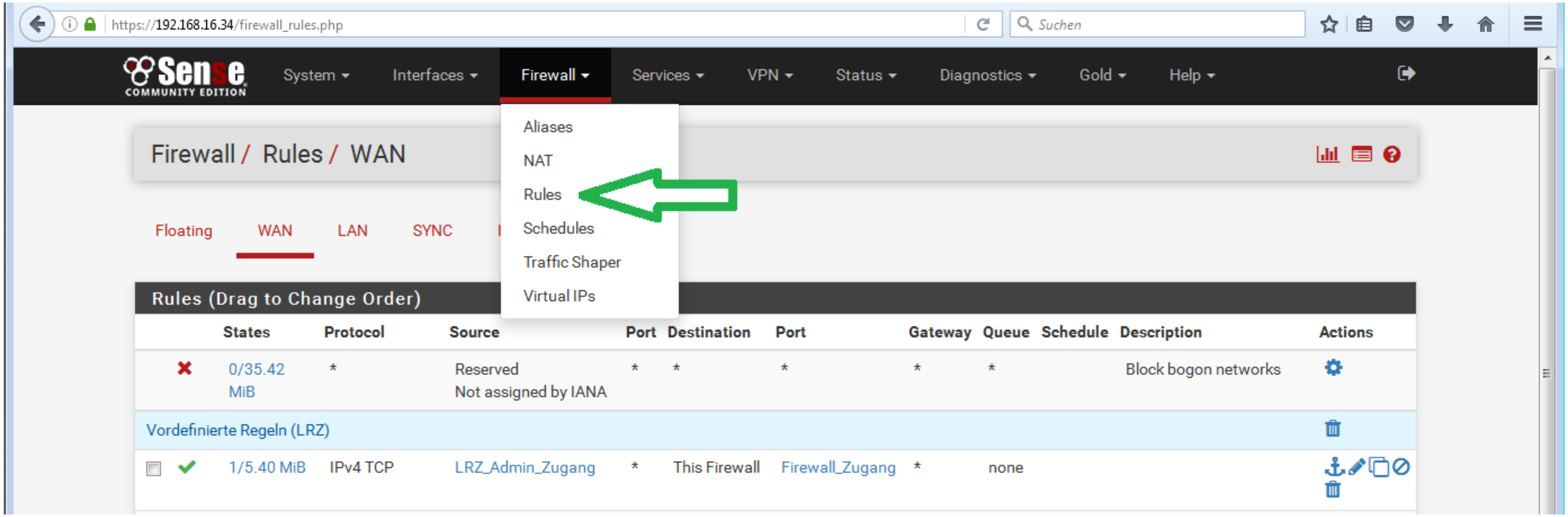
Firewall Aliases IP

Name	Values	Description	Actions
LRZ_VPN_all	LRZ_VPN_all_LMU, LRZ_VPN_all_TUM, LRZ_VPN_all_FHM, LRZ_VPN_all_FHW, LRZ_VPN_all_EXT		
LRZ_VPN_all_EXT	LRZ_VPN_private_EXT, LRZ_VPN_public_EXT		
LRZ_VPN_all_FHM	LRZ_VPN_private_FHM, LRZ_VPN_public_FHM		

Regeln auf der pfSense

Die Regeln können aufgerufen werden unter

Firewall → Rules

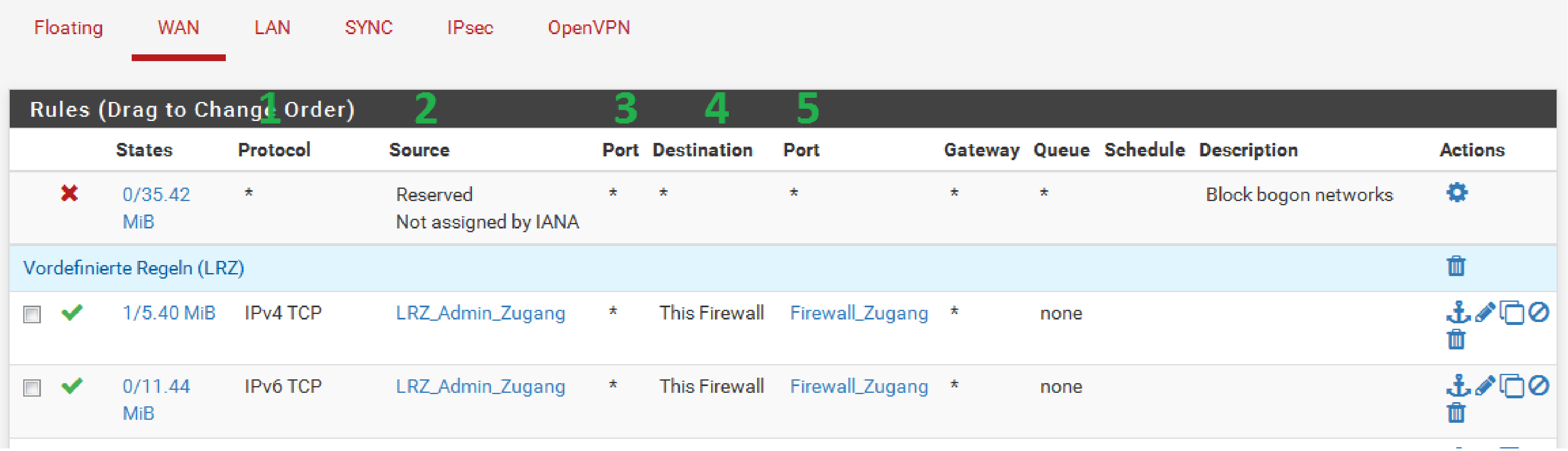


Firewall / Rules / WAN

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/35.42 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
Vordefinierte Regeln (LRZ)												🗑
□	✓	1/5.40 MiB	IPv4 TCP	LRZ_Admin_Zugang	*	This Firewall	Firewall_Zugang	*	none			⚓✎⧉⊘ 🗑

Regeln auf der pfSense



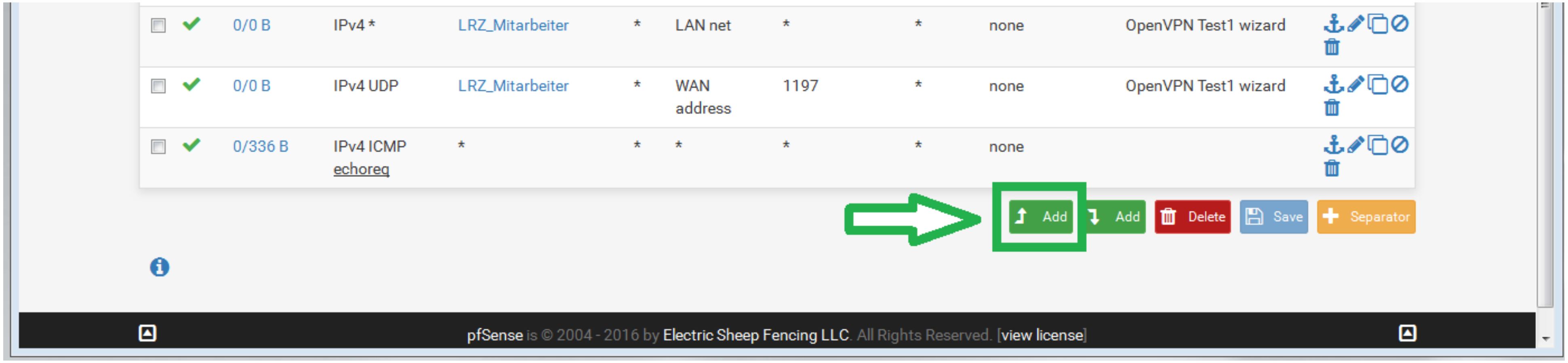
Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/35.42 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
Vordefinierte Regeln (LRZ)												🗑
□	✓	1/5.40 MiB	IPv4 TCP	LRZ_Admin_Zugang	*	This Firewall	Firewall_Zugang	*	none			⚓ ✎ ❐ ⊘ 🗑
□	✓	0/11.44 MiB	IPv6 TCP	LRZ_Admin_Zugang	*	This Firewall	Firewall_Zugang	*	none			⚓ ✎ ❐ ⊘ 🗑

1. Relevantes Protokoll
2. Quell-IP-Adresse
3. Quell-Port
4. Ziel-IP-Adresse
5. Ziel-Port

Eine neue Regel hinzufügen

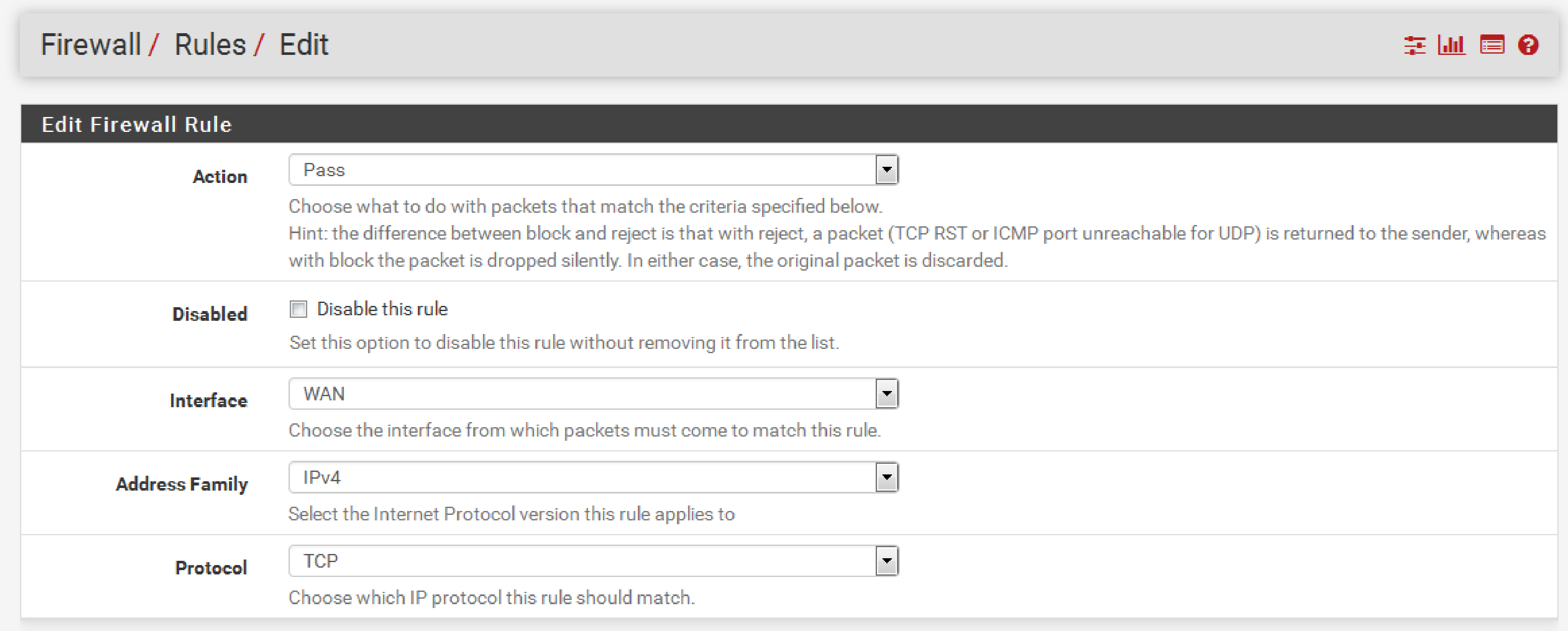
Am unteren Ende der Liste befindet sich ein Button zum Hinzufügen einer Regel an den ersten Listenplatz.



□	✓	0/0 B	IPv4 *	LRZ_Mitarbeiter	*	LAN net	*	*	none	OpenVPN Test1 wizard	
□	✓	0/0 B	IPv4 UDP	LRZ_Mitarbeiter	*	WAN address	1197	*	none	OpenVPN Test1 wizard	
□	✓	0/336 B	IPv4 ICMP echoreq	*	*	*	*	*	none		

pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

Eine neue Regel hinzufügen – Schritt 1

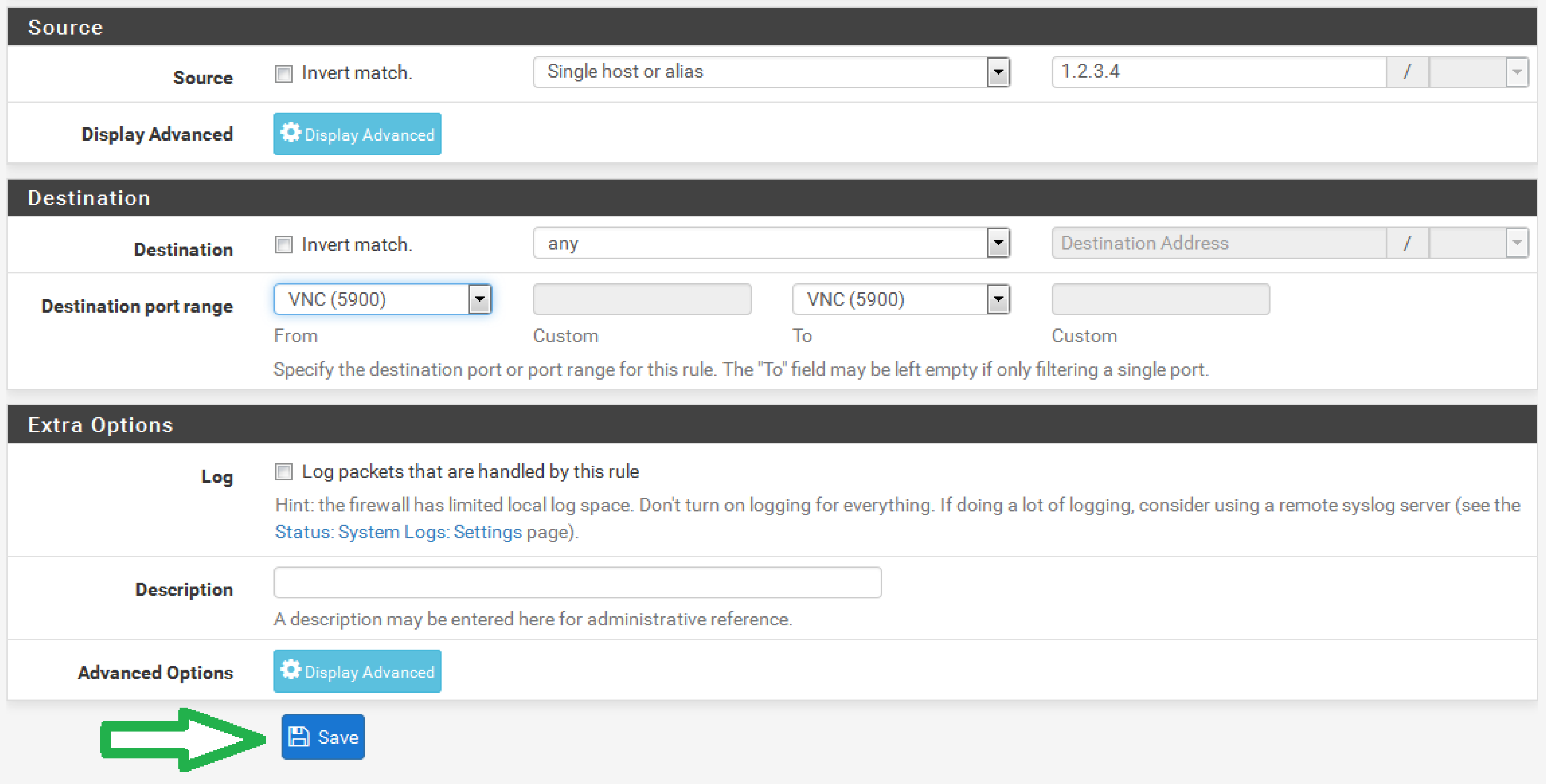


Firewall / Rules / Edit

Edit Firewall Rule

Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to
Protocol	TCP Choose which IP protocol this rule should match.

Eine neue Regel hinzufügen – Schritt 2



Source

Source □ Invert match. Single host or alias 1.2.3.4 /

Display Advanced

Destination

Destination □ Invert match. any Destination Address /

Destination port range VNC (5900) VNC (5900)

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log □ Log packets that are handled by this rule

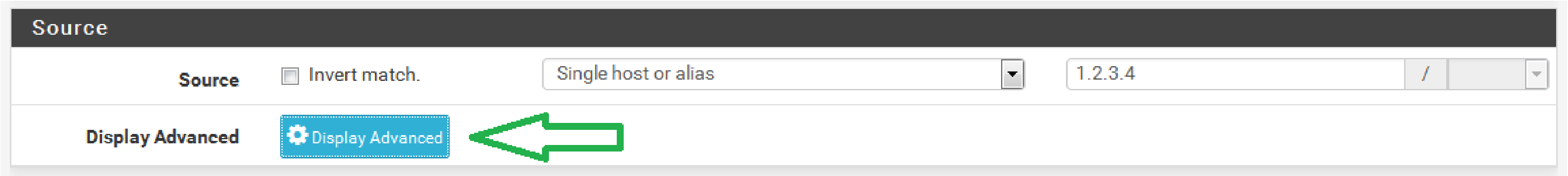
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

A description may be entered here for administrative reference.

Advanced Options

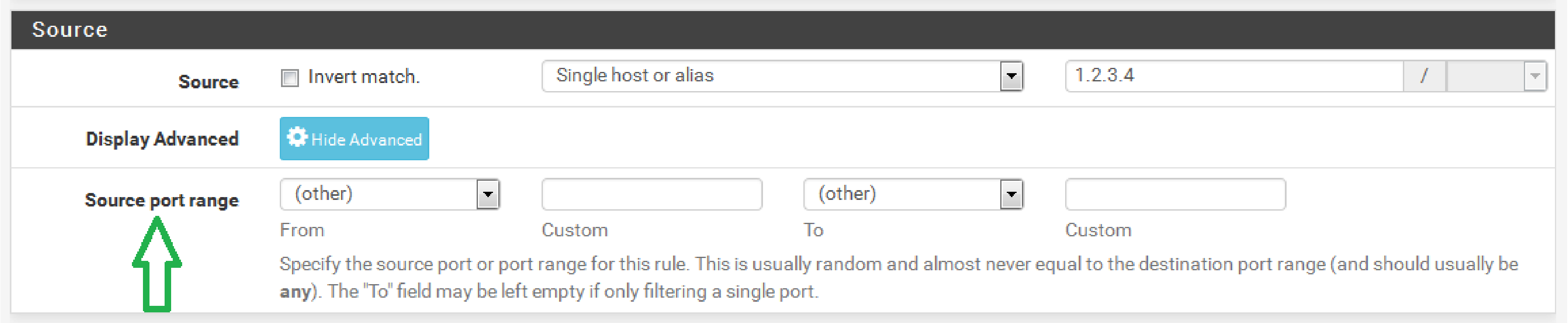
Eine neue Regel hinzufügen – Optionaler Source-Port



Source

Source □ Invert match. Single host or alias 1.2.3.4 /

Display Advanced Display Advanced



Source

Source □ Invert match. Single host or alias 1.2.3.4 /

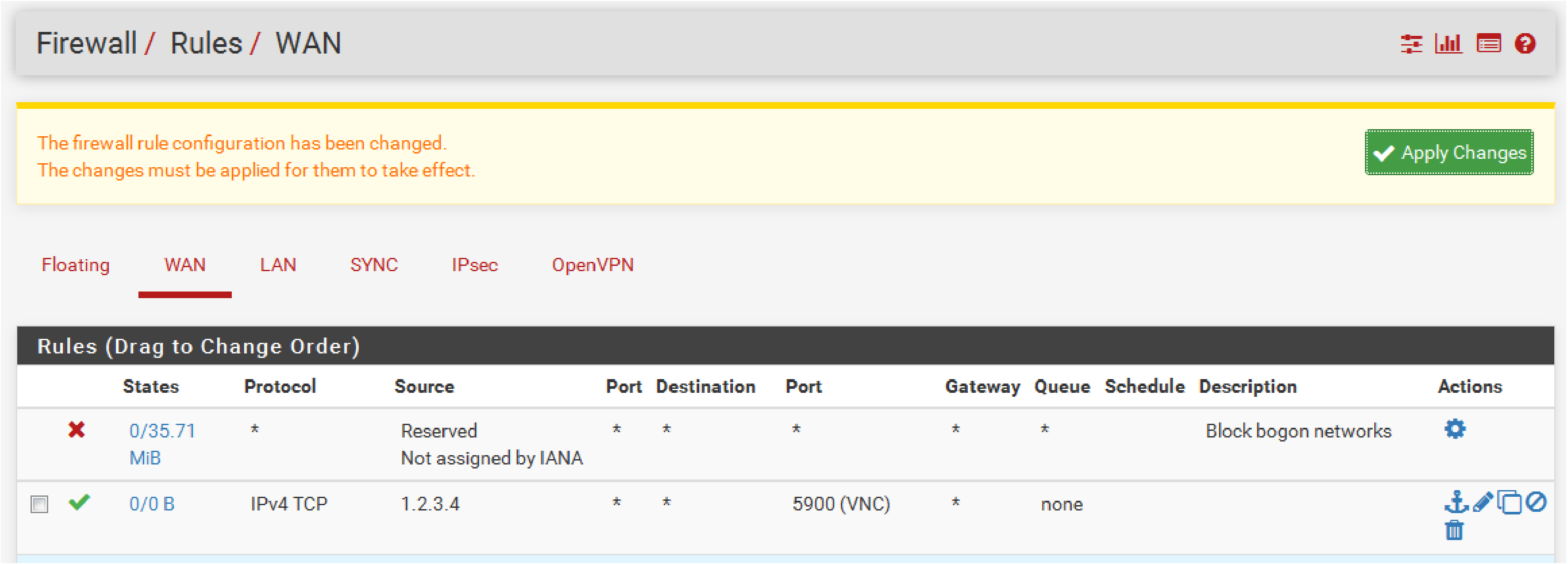
Display Advanced Hide Advanced

Source port range (other) From | Custom | (other) To | Custom

Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be **any**). The "To" field may be left empty if only filtering a single port.

Eine neue Regel hinzufügen

Neue Regel wird an oberster Stelle angefügt



Firewall / Rules / WAN

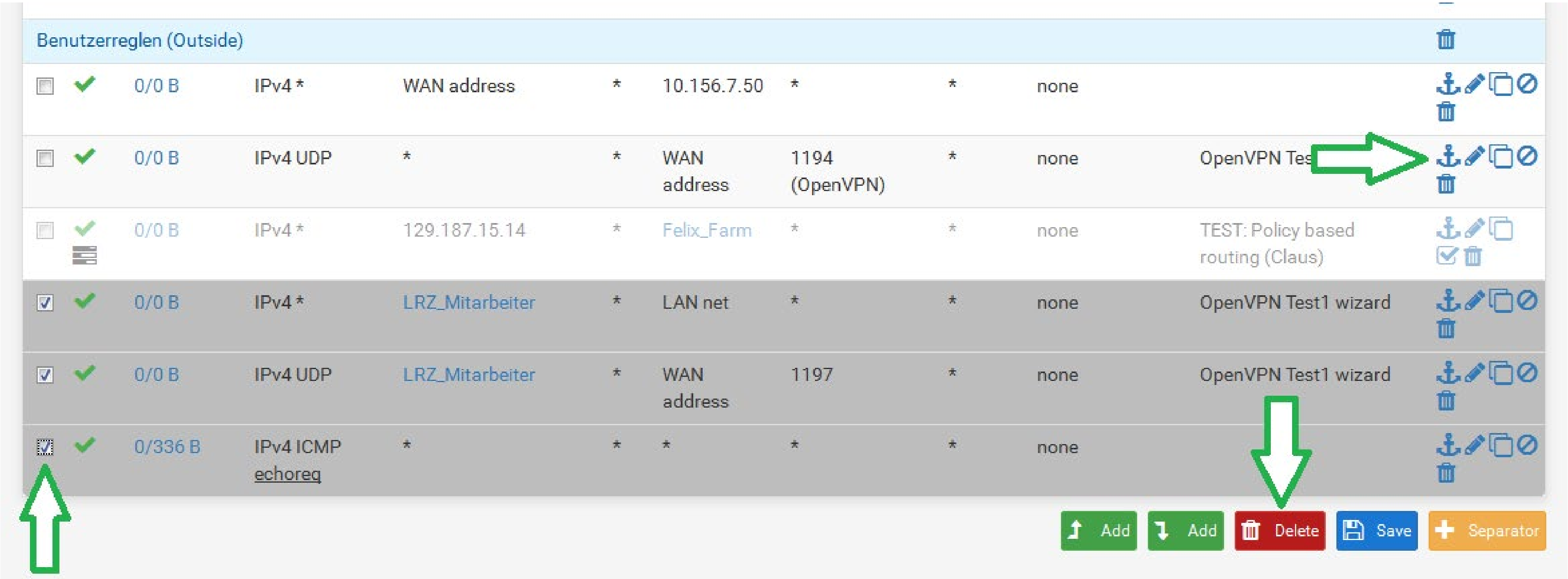
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/35.71 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
□	✓	0/0 B	IPv4 TCP	1.2.3.4	*	*	5900 (VNC)	*	none			

Am unteren Ende der Liste ist eine weitere Schaltfläche zum Hinzufügen einer Regel am **unteren** Ende der Liste!

Auswahl und Bearbeitung mehrerer Einträge

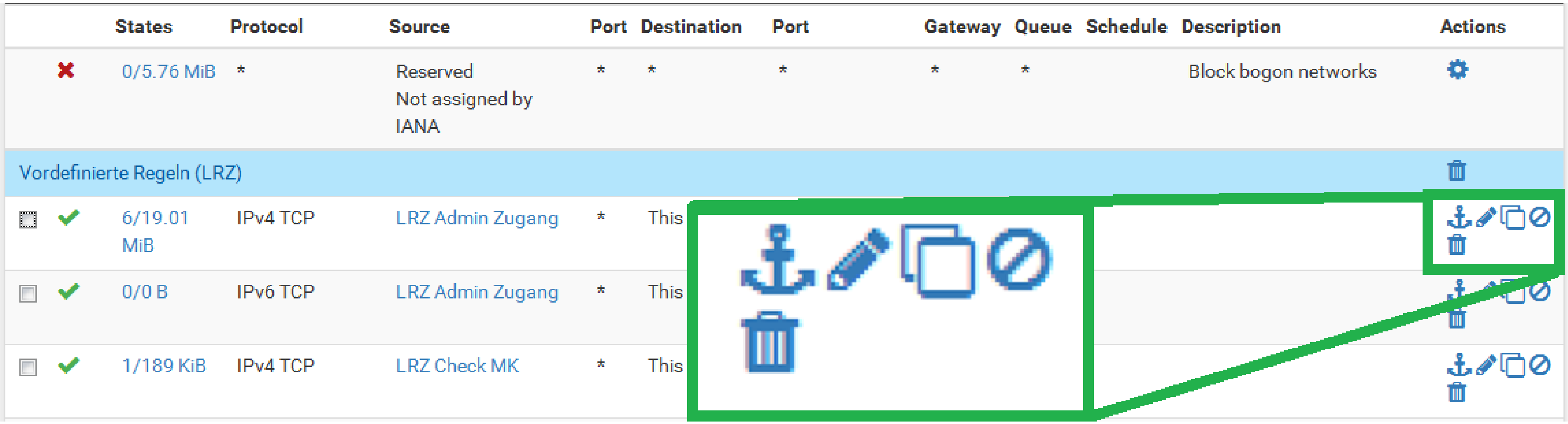


Benutzerreglen (Outside)

□	✓	0/0 B	IPv4 *	WAN address	*	10.156.7.50	*	*	none	
□	✓	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none	OpenVPN Tes
□	✓	0/0 B	IPv4 *	129.187.15.14	*	Felix_Farm	*	*	none	TEST: Policy based routing (Claus)
☑	✓	0/0 B	IPv4 *	LRZ_Mitarbeiter	*	LAN net	*	*	none	OpenVPN Test1 wizard
☑	✓	0/0 B	IPv4 UDP	LRZ_Mitarbeiter	*	WAN address	1197	*	none	OpenVPN Test1 wizard
☑	✓	0/336 B	IPv4 ICMP echoreq	*	*	*	*	*	none	

1. Kontrollkästchen zur Mehrfachauswahl von Einträgen
2. Löschen ausgewählter Einträge (Löschen-Schaltfläche)
3. Verschieben ausgewählter Einträge vor Benutzerregel 2 (Anker-Symbol)

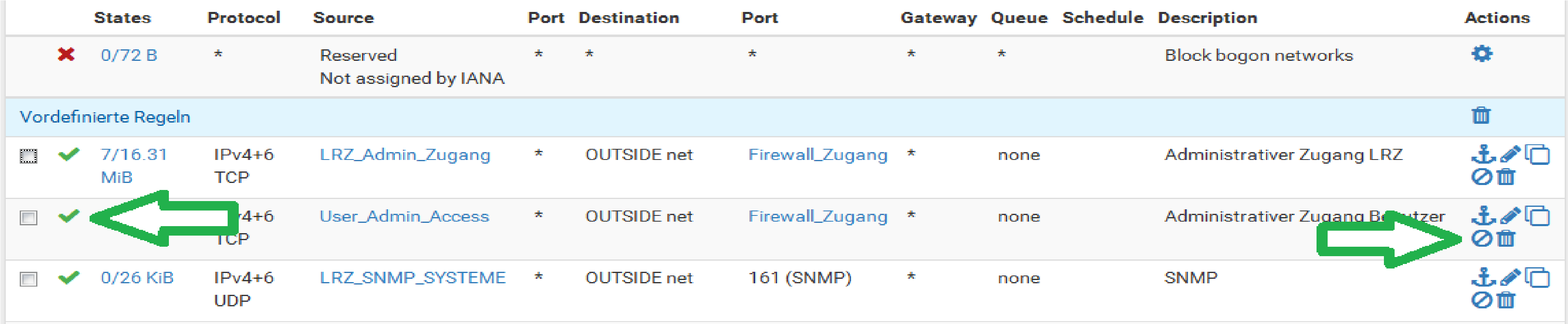
Auswahl und Bearbeitung mehrerer Einträge



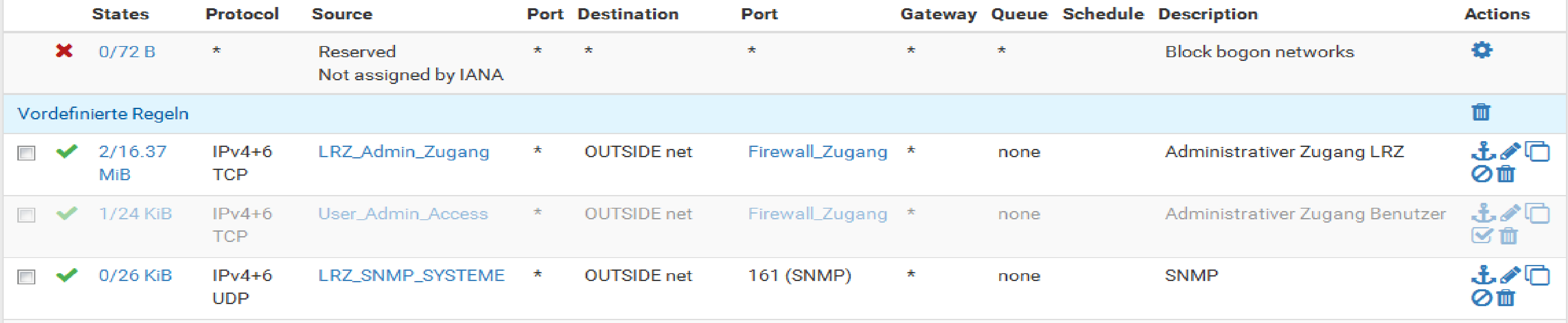
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/5.76 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
Vordefinierte Regeln (LRZ)												🗑
□	✓	6/19.01 MiB	IPv4 TCP	LRZ Admin Zugang	*	This						⚓ ✎ ⧉ ⊘ 🗑
□	✓	0/0 B	IPv6 TCP	LRZ Admin Zugang	*	This						⚓ ✎ ⧉ ⊘ 🗑
□	✓	1/189 KiB	IPv4 TCP	LRZ Check MK	*	This						⚓ ✎ ⧉ ⊘ 🗑

- **Anker**: Ausgewählte Einträge vor diese Zeile einfügen (vgl. Vorgängerfolie)
- **Stift**: Editieren einer Regel
- **Doppelblatt:** Erstellen einer neuen Regel auf Basis der ausgewählten Regel
- **Durchgestrichener Kreis:** Deaktivieren einer Regel
- **Papierkorb:** Löschen einer Regel

Aktivierung und Deaktivierung einzelner Regeln



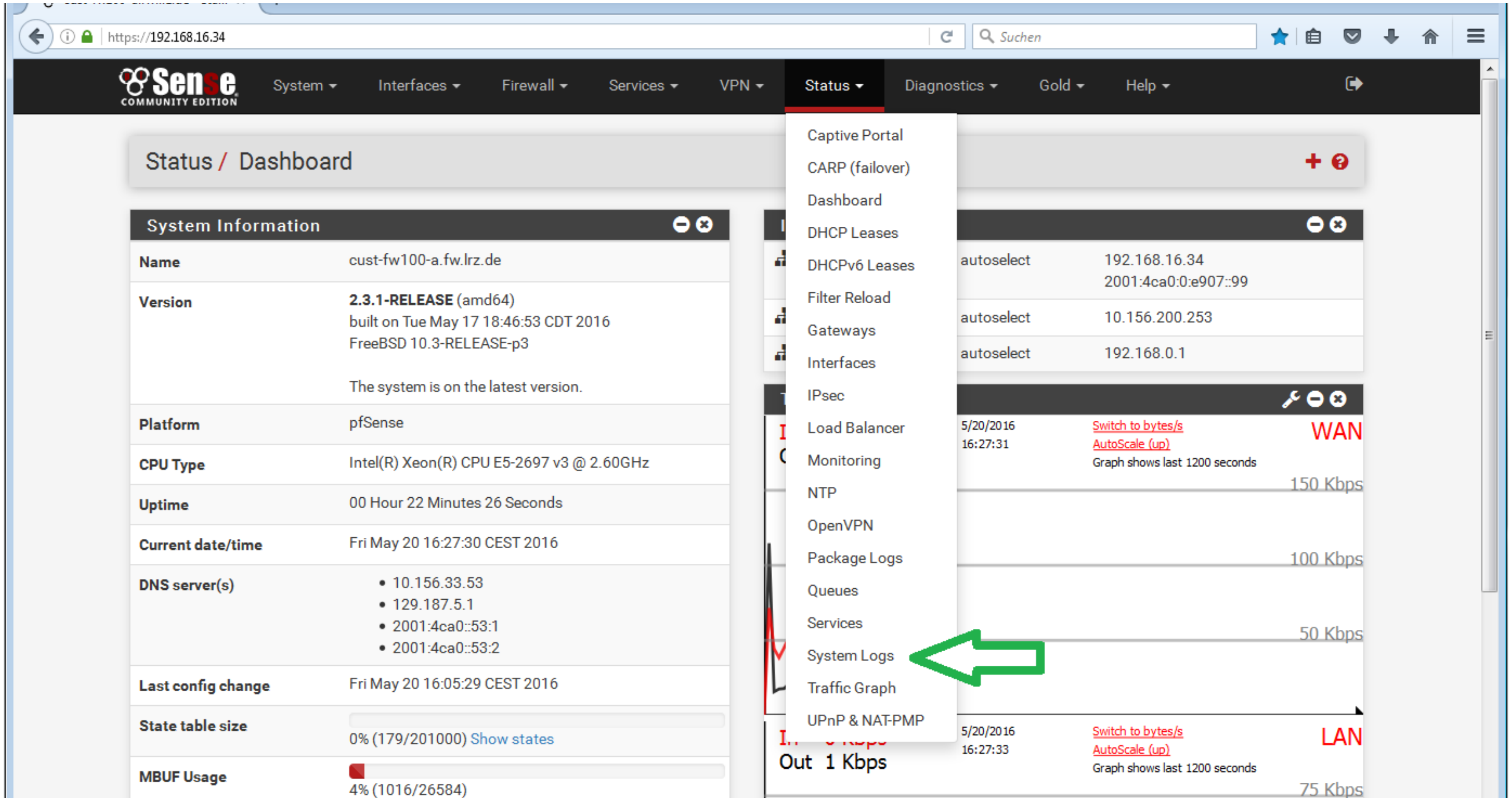
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/72 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
Vordefinierte Regeln												🗑
□	✓	7/16.31 MiB	IPv4+6 TCP	LRZ_Admin_Zugang	*	OUTSIDE net	Firewall_Zugang	*	none		Administrativer Zugang LRZ	⚓ ✎ ⧉ ⊘ 🗑
□	✓		IPv4+6 TCP	User_Admin_Access	*	OUTSIDE net	Firewall_Zugang	*	none		Administrativer Zugang Benutzer	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0/26 KiB	IPv4+6 UDP	LRZ_SNMP_SYSTEME	*	OUTSIDE net	161 (SNMP)	*	none		SNMP	⚓ ✎ ⧉ ⊘ 🗑



		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/72 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
Vordefinierte Regeln												🗑
□	✓	2/16.37 MiB	IPv4+6 TCP	LRZ_Admin_Zugang	*	OUTSIDE net	Firewall_Zugang	*	none		Administrativer Zugang LRZ	⚓ ✎ ⧉ ⊘ 🗑
□	✓	1/24 KiB	IPv4+6 TCP	User_Admin_Access	*	OUTSIDE net	Firewall_Zugang	*	none		Administrativer Zugang Benutzer	⚓ ✎ ⧉ ☑ 🗑
□	✓	0/26 KiB	IPv4+6 UDP	LRZ_SNMP_SYSTEME	*	OUTSIDE net	161 (SNMP)	*	none		SNMP	⚓ ✎ ⧉ ⊘ 🗑

- Aktivierung von Regeln funktioniert analog.

System Logs

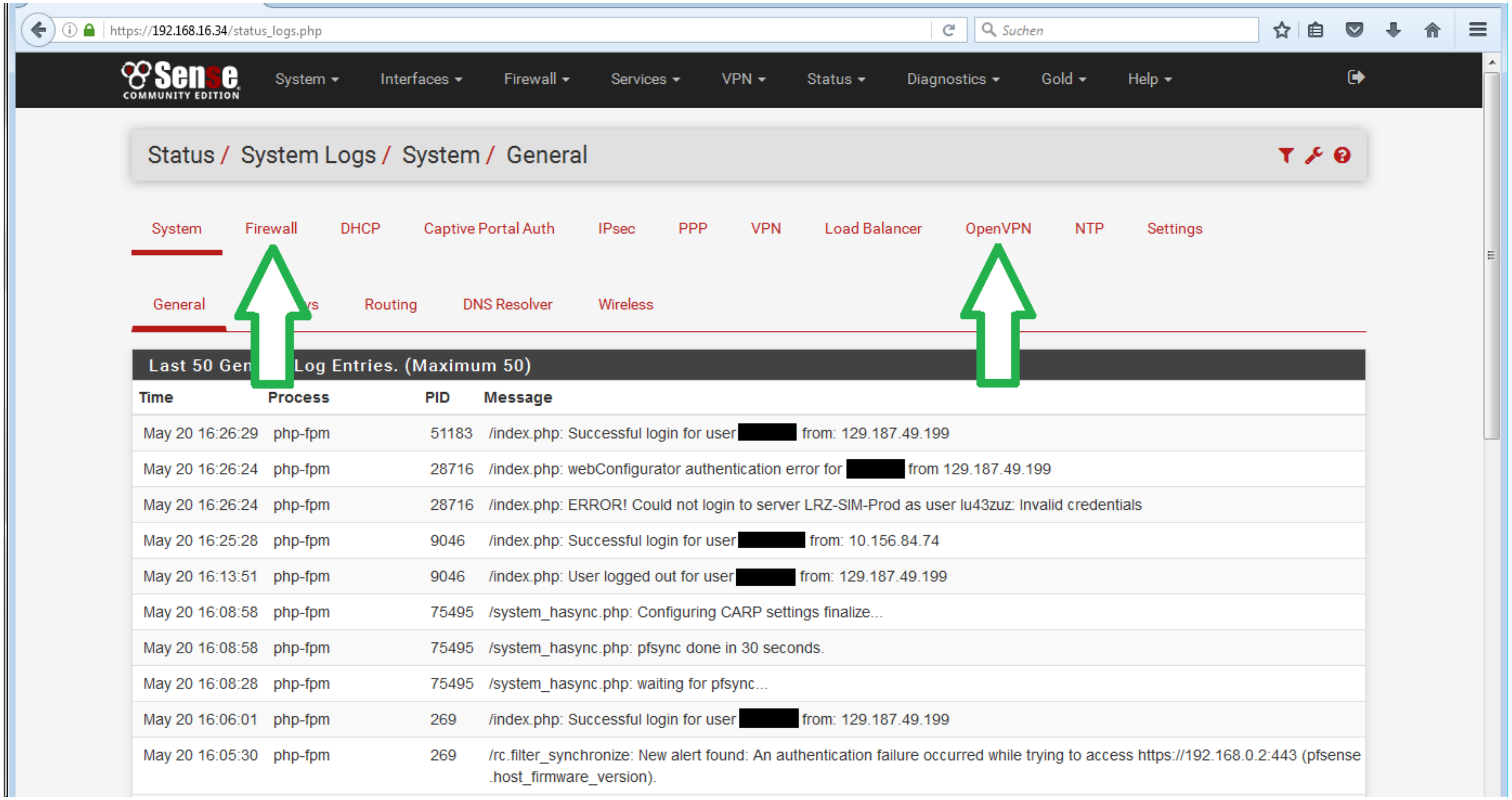


System Information

Name	cust-fw100-a.fw.lrz.de
Version	**2.3.1-RELEASE** (amd64) built on Tue May 17 18:46:53 CDT 2016 FreeBSD 10.3-RELEASE-p3 The system is on the latest version.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz
Uptime	00 Hour 22 Minutes 26 Seconds
Current date/time	Fri May 20 16:27:30 CEST 2016
DNS server(s)	• 10.156.33.53 • 129.187.5.1 • 2001:4ca0::53:1 • 2001:4ca0::53:2
Last config change	Fri May 20 16:05:29 CEST 2016
State table size	0% (179/201000) Show states
MBUF Usage	4% (1016/26584)

autoselect	192.168.16.34 2001:4ca0:0:e907::99
autoselect	10.156.200.253
autoselect	192.168.0.1

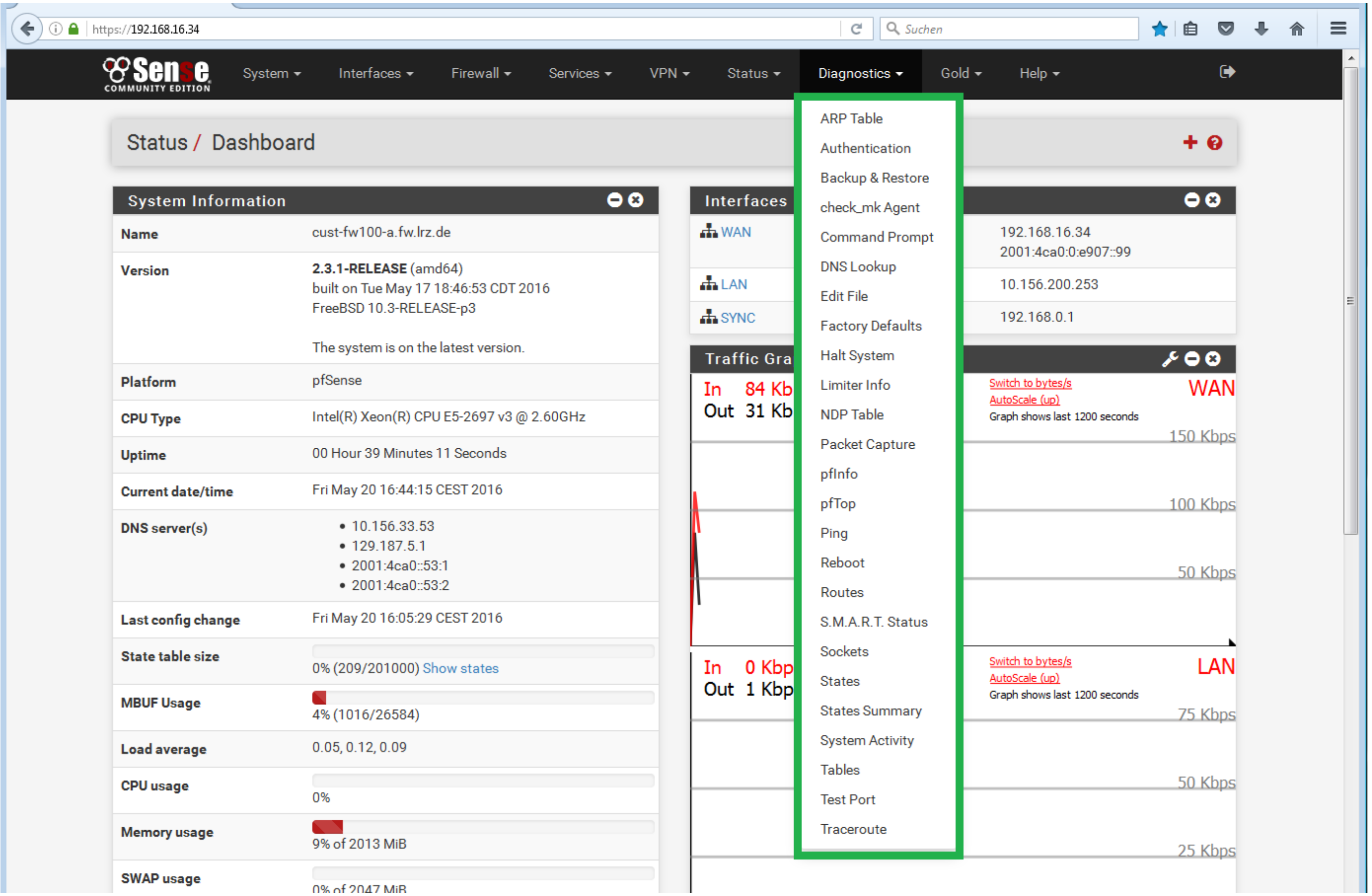
System Logs



Last 50 Gen Log Entries. (Maximum 50)

Time	Process	PID	Message
May 20 16:26:29	php-fpm	51183	/index.php: Successful login for user [redacted] from: 129.187.49.199
May 20 16:26:24	php-fpm	28716	/index.php: webConfigurator authentication error for [redacted] from 129.187.49.199
May 20 16:26:24	php-fpm	28716	/index.php: ERROR! Could not login to server LRZ-SIM-Prod as user lu43zuz: Invalid credentials
May 20 16:25:28	php-fpm	9046	/index.php: Successful login for user [redacted] from: 10.156.84.74
May 20 16:13:51	php-fpm	9046	/index.php: User logged out for user [redacted] from: 129.187.49.199
May 20 16:08:58	php-fpm	75495	/system_hasync.php: Configuring CARP settings finalize...
May 20 16:08:58	php-fpm	75495	/system_hasync.php: pfsync done in 30 seconds.
May 20 16:08:28	php-fpm	75495	/system_hasync.php: waiting for pfsync...
May 20 16:06:01	php-fpm	269	/index.php: Successful login for user [redacted] from: 129.187.49.199
May 20 16:05:30	php-fpm	269	/rc.filter_synchronize: New alert found: An authentication failure occurred while trying to access https://192.168.0.2:443 (pfsense.host_firmware_version).

Diagnosetools auf der pfSense



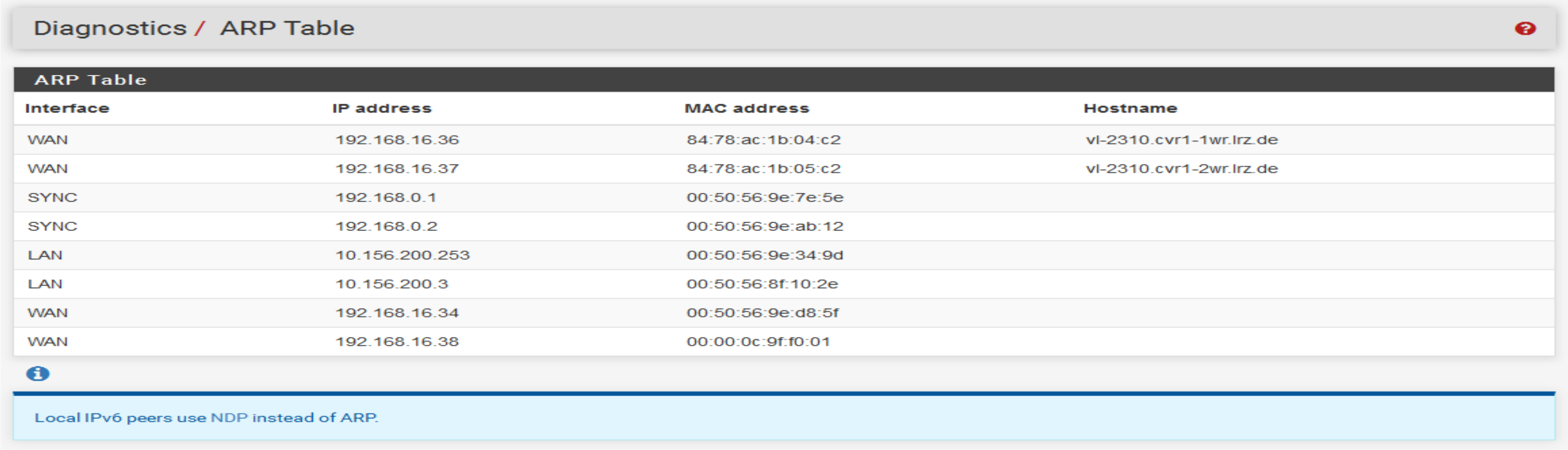
System Information

Name	cust-fw100-a.fw.lrz.de
Version	**2.3.1-RELEASE** (amd64) built on Tue May 17 18:46:53 CDT 2016 FreeBSD 10.3-RELEASE-p3 The system is on the latest version.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz
Uptime	00 Hour 39 Minutes 11 Seconds
Current date/time	Fri May 20 16:44:15 CEST 2016
DNS server(s)	• 10.156.33.53 • 129.187.5.1 • 2001:4ca0::53:1 • 2001:4ca0::53:2
Last config change	Fri May 20 16:05:29 CEST 2016
State table size	0% (209/201000) Show states
MBUF Usage	4% (1016/26584)
Load average	0.05, 0.12, 0.09
CPU usage	0%
Memory usage	9% of 2013 MiB
SWAP usage	0% of 2047 MiB

Interfaces

WAN	192.168.16.34 2001:4ca0:0:e907::99
LAN	10.156.200.253
SYNC	192.168.0.1

Diagnosetools auf der pfSense

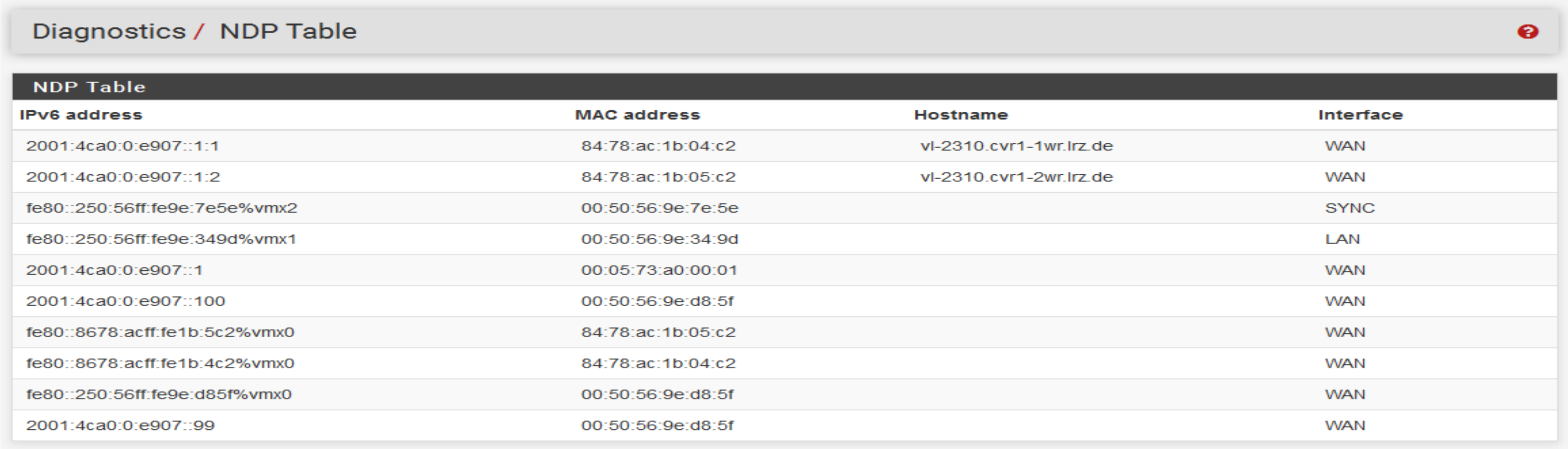


Diagnostics / ARP Table

ARP Table

Interface	IP address	MAC address	Hostname
WAN	192.168.16.36	84:78:ac:1b:04:c2	vl-2310.cvr1-1wr.lrz.de
WAN	192.168.16.37	84:78:ac:1b:05:c2	vl-2310.cvr1-2wr.lrz.de
SYNC	192.168.0.1	00:50:56:9e:7e:5e	
SYNC	192.168.0.2	00:50:56:9e:ab:12	
LAN	10.156.200.253	00:50:56:9e:34:9d	
LAN	10.156.200.3	00:50:56:8f:10:2e	
WAN	192.168.16.34	00:50:56:9e:d8:5f	
WAN	192.168.16.38	00:00:0c:9f:f0:01	

Local IPv6 peers use NDP instead of ARP.

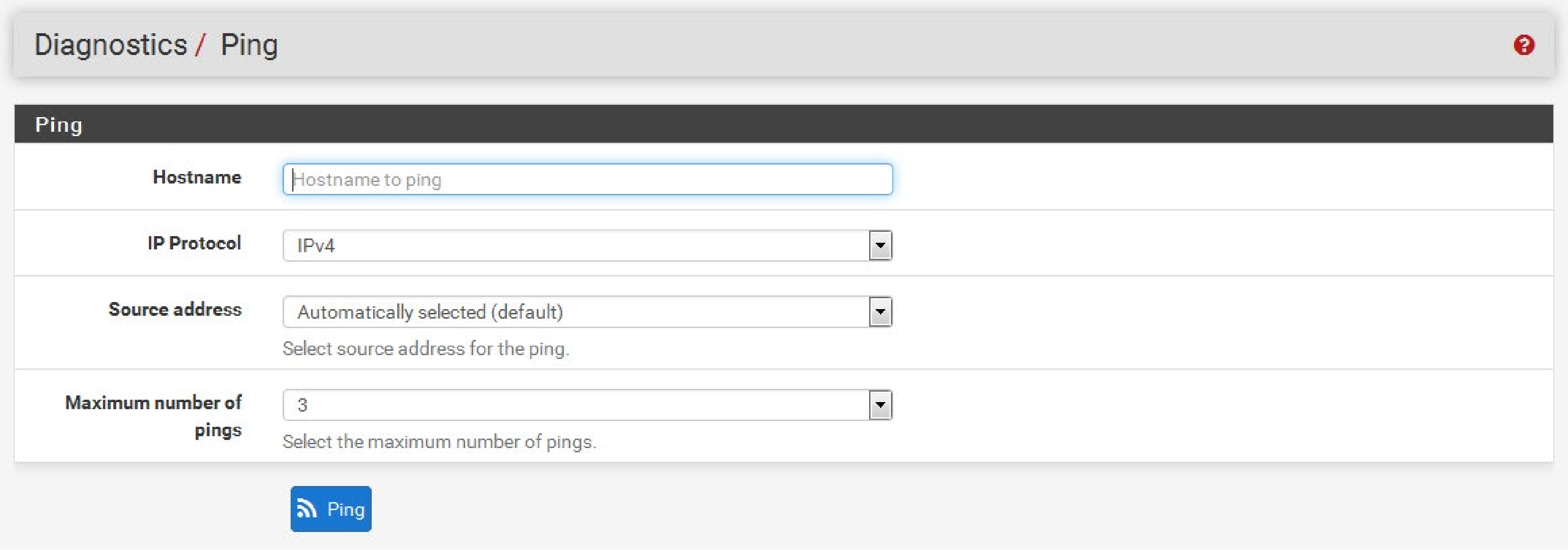


Diagnostics / NDP Table

NDP Table

IPv6 address	MAC address	Hostname	Interface
2001:4ca0:0:e907::1:1	84:78:ac:1b:04:c2	vl-2310.cvr1-1wr.lrz.de	WAN
2001:4ca0:0:e907::1:2	84:78:ac:1b:05:c2	vl-2310.cvr1-2wr.lrz.de	WAN
fe80::250:56ff:fe9e:7e5e%vmx2	00:50:56:9e:7e:5e		SYNC
fe80::250:56ff:fe9e:349d%vmx1	00:50:56:9e:34:9d		LAN
2001:4ca0:0:e907::1	00:05:73:a0:00:01		WAN
2001:4ca0:0:e907::100	00:50:56:9e:d8:5f		WAN
fe80::8678:acff:fe1b:5c2%vmx0	84:78:ac:1b:05:c2		WAN
fe80::8678:acff:fe1b:4c2%vmx0	84:78:ac:1b:04:c2		WAN
fe80::250:56ff:fe9e:d85f%vmx0	00:50:56:9e:d8:5f		WAN
2001:4ca0:0:e907::99	00:50:56:9e:d8:5f		WAN

Diagnosetools auf der pfSense

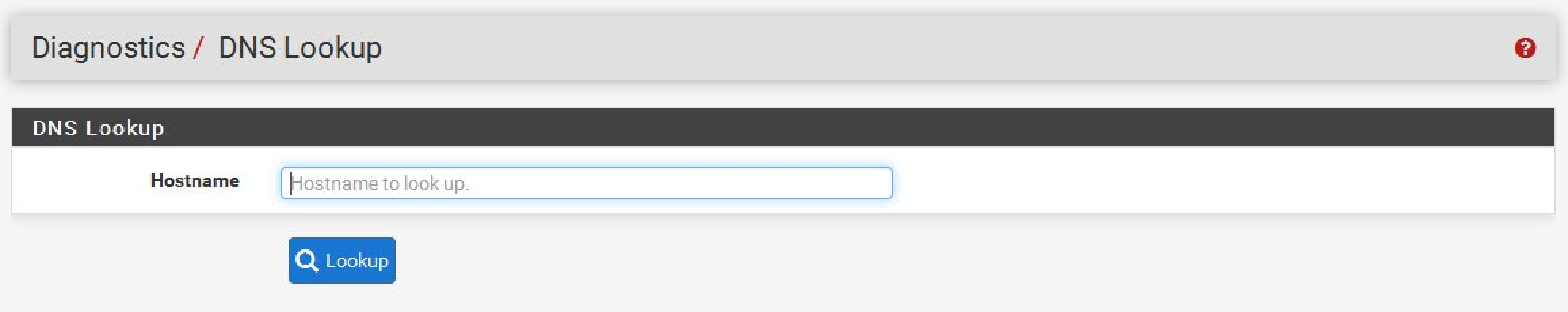


Diagnostics / Ping

Ping

Hostname	Hostname to ping
IP Protocol	IPv4
Source address	Automatically selected (default) Select source address for the ping.
Maximum number of pings	3 Select the maximum number of pings.

Diagnosetools auf der pfSense

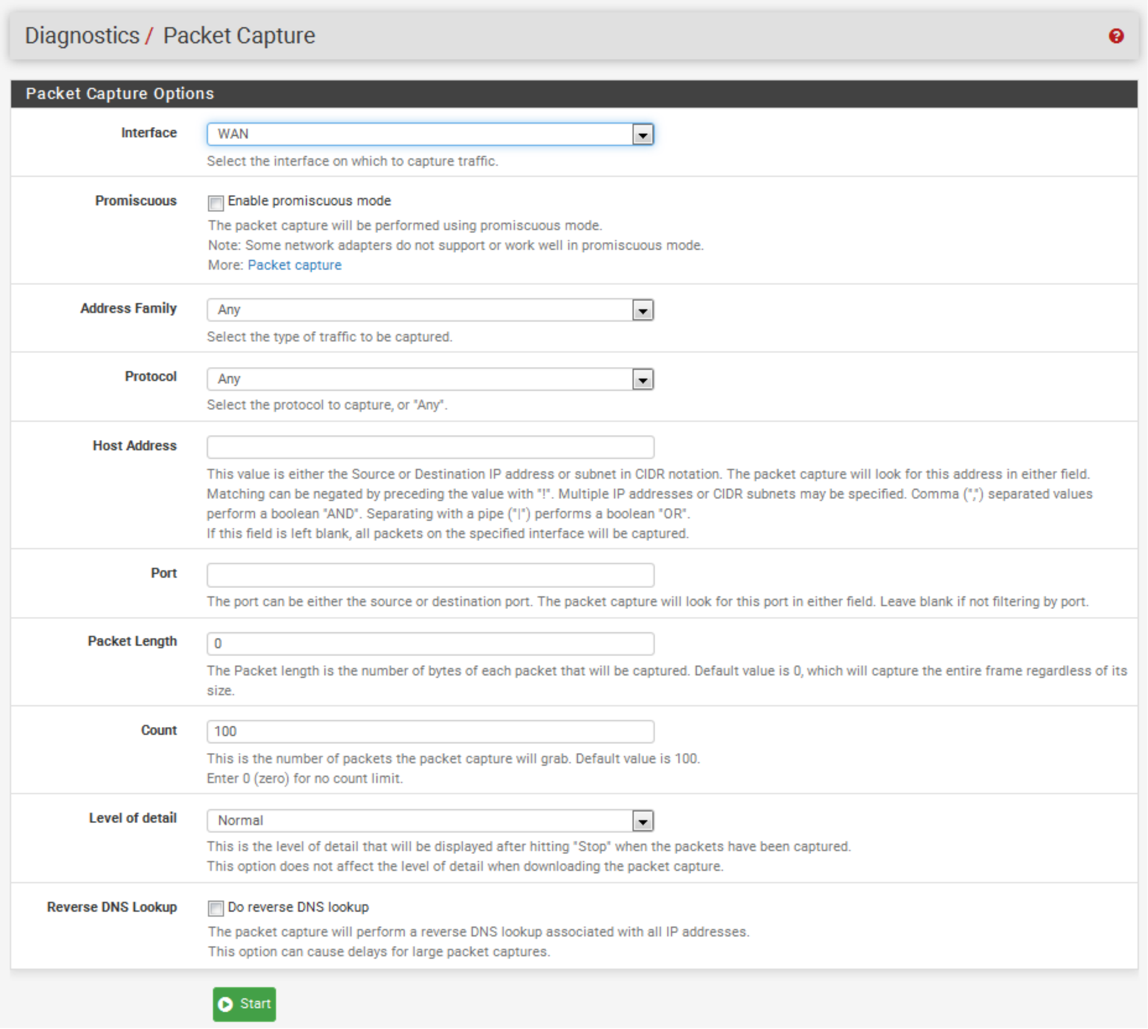


Diagnostics / DNS Lookup

DNS Lookup

Hostname: Hostname to look up.

Diagnosetools auf der pfSense



Diagnostics / Packet Capture

Packet Capture Options

Interface: WAN
Select the interface on which to capture traffic.

Promiscuous: □ Enable promiscuous mode
The packet capture will be performed using promiscuous mode.
Note: Some network adapters do not support or work well in promiscuous mode.
More: Packet capture

Address Family: Any
Select the type of traffic to be captured.

Protocol: Any
Select the protocol to capture, or "Any".

Host Address:
This value is either the Source or Destination IP address or subnet in CIDR notation. The packet capture will look for this address in either field.
Matching can be negated by preceding the value with "!". Multiple IP addresses or CIDR subnets may be specified. Comma (",") separated values perform a boolean "AND". Separating with a pipe ("|") performs a boolean "OR".
If this field is left blank, all packets on the specified interface will be captured.

Port:
The port can be either the source or destination port. The packet capture will look for this port in either field. Leave blank if not filtering by port.

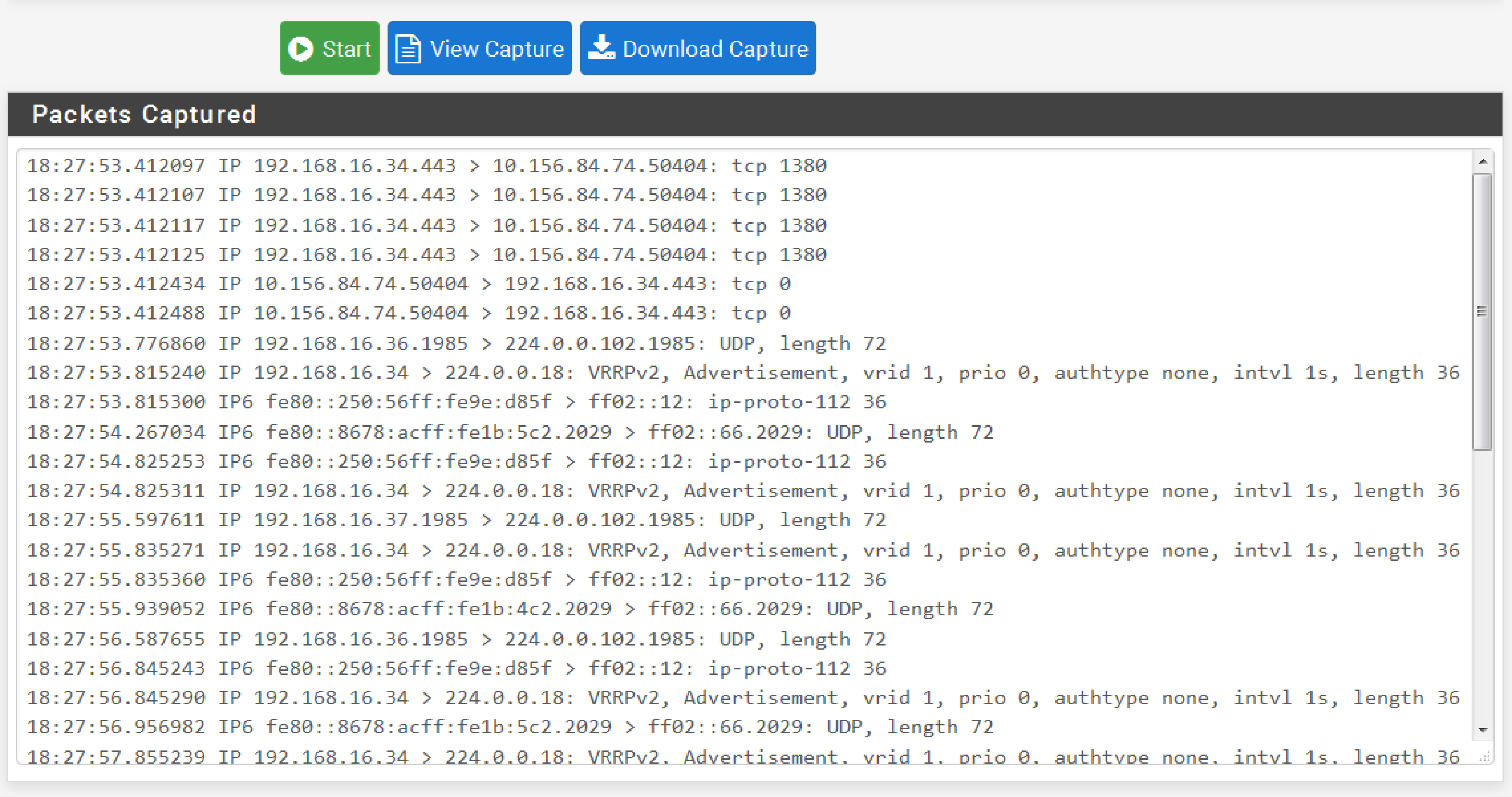
Packet Length: 0
The Packet length is the number of bytes of each packet that will be captured. Default value is 0, which will capture the entire frame regardless of its size.

Count: 100
This is the number of packets the packet capture will grab. Default value is 100.
Enter 0 (zero) for no count limit.

Level of detail: Normal
This is the level of detail that will be displayed after hitting "Stop" when the packets have been captured.
This option does not affect the level of detail when downloading the packet capture.

Reverse DNS Lookup: □ Do reverse DNS lookup
The packet capture will perform a reverse DNS lookup associated with all IP addresses.
This option can cause delays for large packet captures.

Diagnosetools auf der pfSense



```
18:27:53.412097 IP 192.168.16.34.443 > 10.156.84.74.50404: tcp 1380
18:27:53.412107 IP 192.168.16.34.443 > 10.156.84.74.50404: tcp 1380
18:27:53.412117 IP 192.168.16.34.443 > 10.156.84.74.50404: tcp 1380
18:27:53.412125 IP 192.168.16.34.443 > 10.156.84.74.50404: tcp 1380
18:27:53.412434 IP 10.156.84.74.50404 > 192.168.16.34.443: tcp 0
18:27:53.412488 IP 10.156.84.74.50404 > 192.168.16.34.443: tcp 0
18:27:53.776860 IP 192.168.16.36.1985 > 224.0.0.102.1985: UDP, length 72
18:27:53.815240 IP 192.168.16.34 > 224.0.0.18: VRRPv2, Advertisement, vrid 1, prio 0, authtype none, intvl 1s, length 36
18:27:53.815300 IP6 fe80::250:56ff:fe9e:d85f > ff02::12: ip-proto-112 36
18:27:54.267034 IP6 fe80::8678:acff:fe1b:5c2.2029 > ff02::66.2029: UDP, length 72
18:27:54.825253 IP6 fe80::250:56ff:fe9e:d85f > ff02::12: ip-proto-112 36
18:27:54.825311 IP 192.168.16.34 > 224.0.0.18: VRRPv2, Advertisement, vrid 1, prio 0, authtype none, intvl 1s, length 36
18:27:55.597611 IP 192.168.16.37.1985 > 224.0.0.102.1985: UDP, length 72
18:27:55.835271 IP 192.168.16.34 > 224.0.0.18: VRRPv2, Advertisement, vrid 1, prio 0, authtype none, intvl 1s, length 36
18:27:55.835360 IP6 fe80::250:56ff:fe9e:d85f > ff02::12: ip-proto-112 36
18:27:55.939052 IP6 fe80::8678:acff:fe1b:4c2.2029 > ff02::66.2029: UDP, length 72
18:27:56.587655 IP 192.168.16.36.1985 > 224.0.0.102.1985: UDP, length 72
18:27:56.845243 IP6 fe80::250:56ff:fe9e:d85f > ff02::12: ip-proto-112 36
18:27:56.845290 IP 192.168.16.34 > 224.0.0.18: VRRPv2, Advertisement, vrid 1, prio 0, authtype none, intvl 1s, length 36
18:27:56.956982 IP6 fe80::8678:acff:fe1b:5c2.2029 > ff02::66.2029: UDP, length 72
18:27:57.855239 IP 192.168.16.34 > 224.0.0.18: VRRPv2, Advertisement, vrid 1, prio 0, authtype none, intvl 1s, length 36
```

Kontakt

Allgemeiner Kontakt und Support:

LRZ Servicedesk / IT-Sicherheit / Firewalls

https://servicedesk.lrz.de/ql/create/40

Anhang
Features pfSense

pfSense – genereller Funktionsumfang

Firewall

- Filtern auf Basis von Quell- und Ziel-IP sowie –Port
- Regelbasiert
- Optionales Logging der Regelanwendung
- Gruppierung und Benennung von IPs, Netzwerken und Ports
- Layer 2 Firewall

und weitere…

pfSense – genereller Funktionsumfang

State Table

- Hält Informationen über offene Netzwerkverbindungen
- Größe der Tabelle anpassbar
- Regelbasiert

→ Begrenzung der Anzahl an Verbindungen, Verbindungen pro Sekunde,…

und weitere…

pfSense – genereller Funktionsumfang

Network Address Translation (NAT)

High Availability

- CARP
- pfsynch
- Synchronisation der Konfiguration
- Konfiguration mehrerer Firewalls als „Failover“ Gruppe

pfSense – genereller Funktionsumfang

Server Load Balancing

Virtual Private Network (VPN)

- IPsec
- OpenVPN
- L2TP

pfSense – genereller Funktionsumfang

Reporting und Monitoring

- Visualisierungen
  - CPU Nutzung
  - Durchsatz (gesamt und pro Interface)
  - Pakete pro Sekunde
  - …
- Echtzeitinformationen

pfSense – genereller Funktionsumfang

Dynamic DNS Client

- DNS-O-MAT
- DynDNS
- DHS
- DyNS
- easyDNS
- freeDNS
- …

pfSense – genereller Funktionsumfang

Der gesamte Funktionsumfang unter
https://www.pfsense.org/about-pfsense/features.html