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

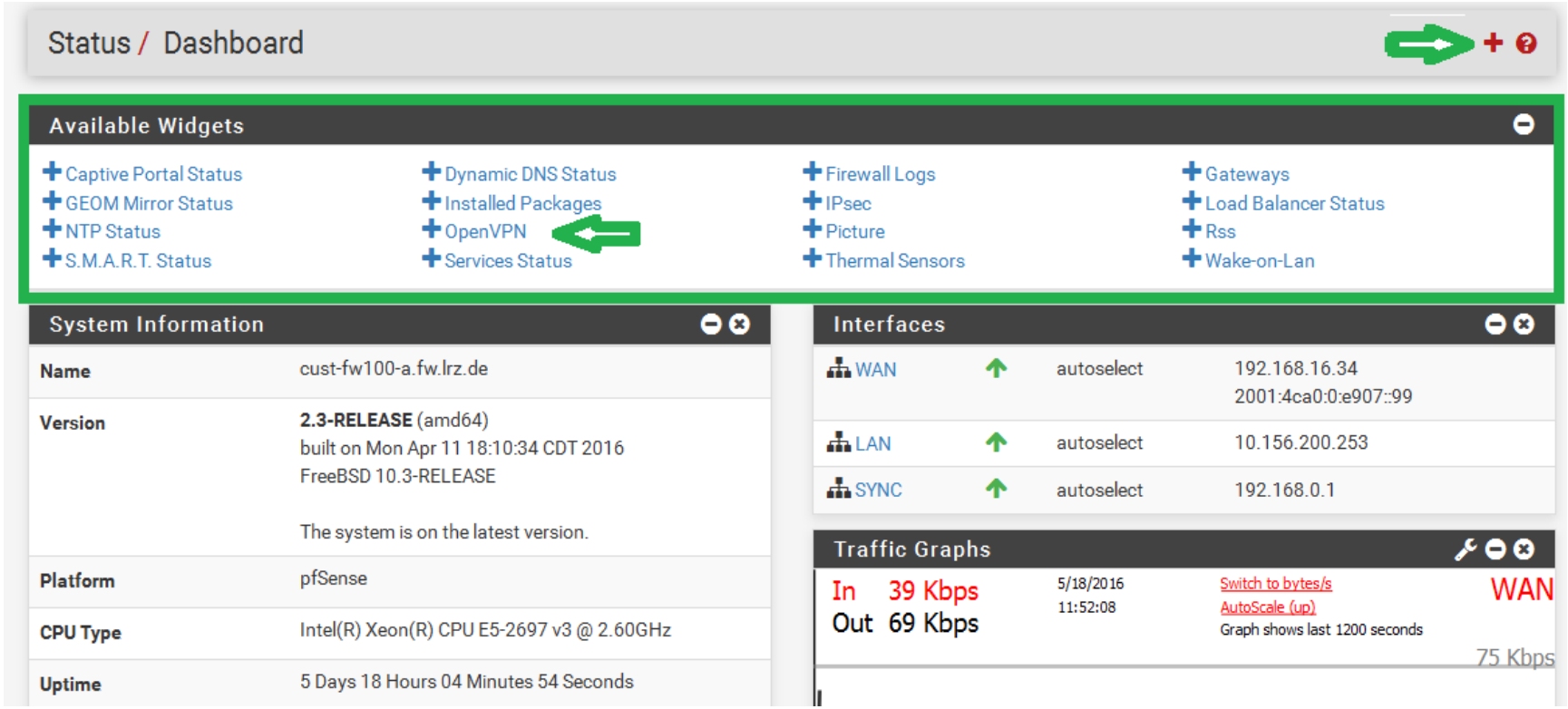
Statistiken und Traffic Graphen (Live) der Netzinterfaces

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

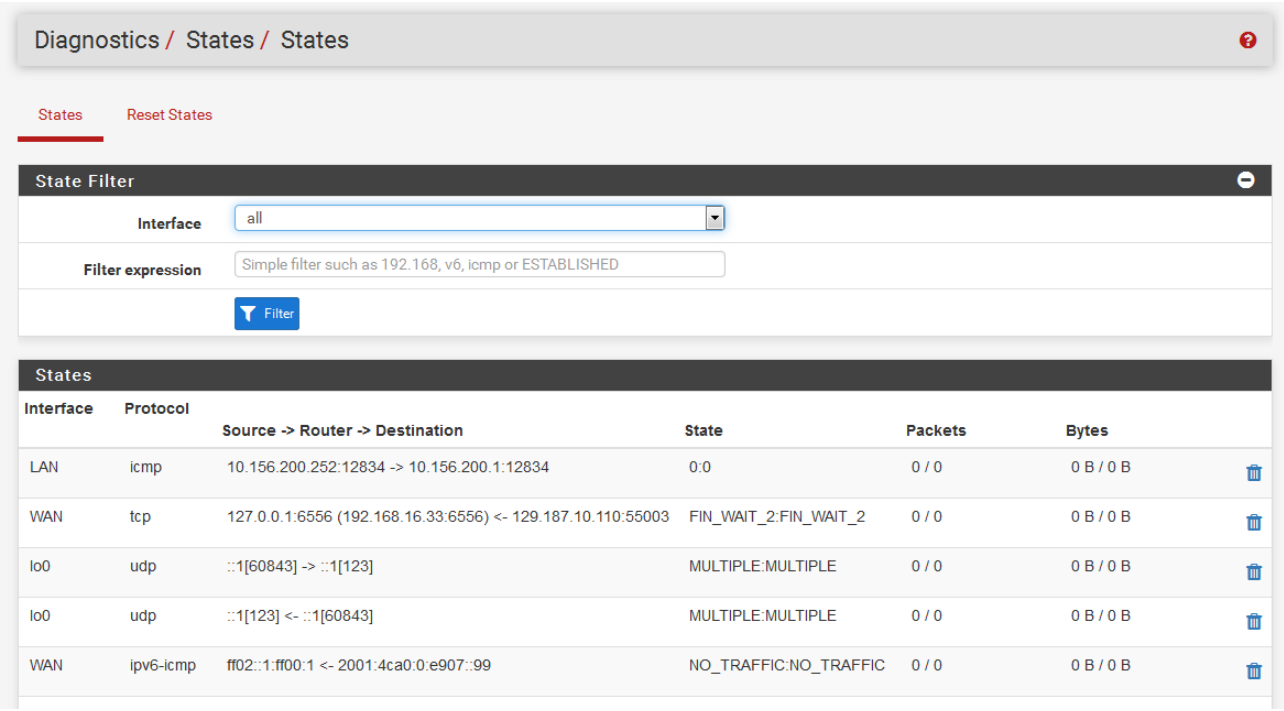
Weitere Widgets können dem Dashboard hinzugefügt werden (z.B. Informationen zum **OpenVPN**)



State table

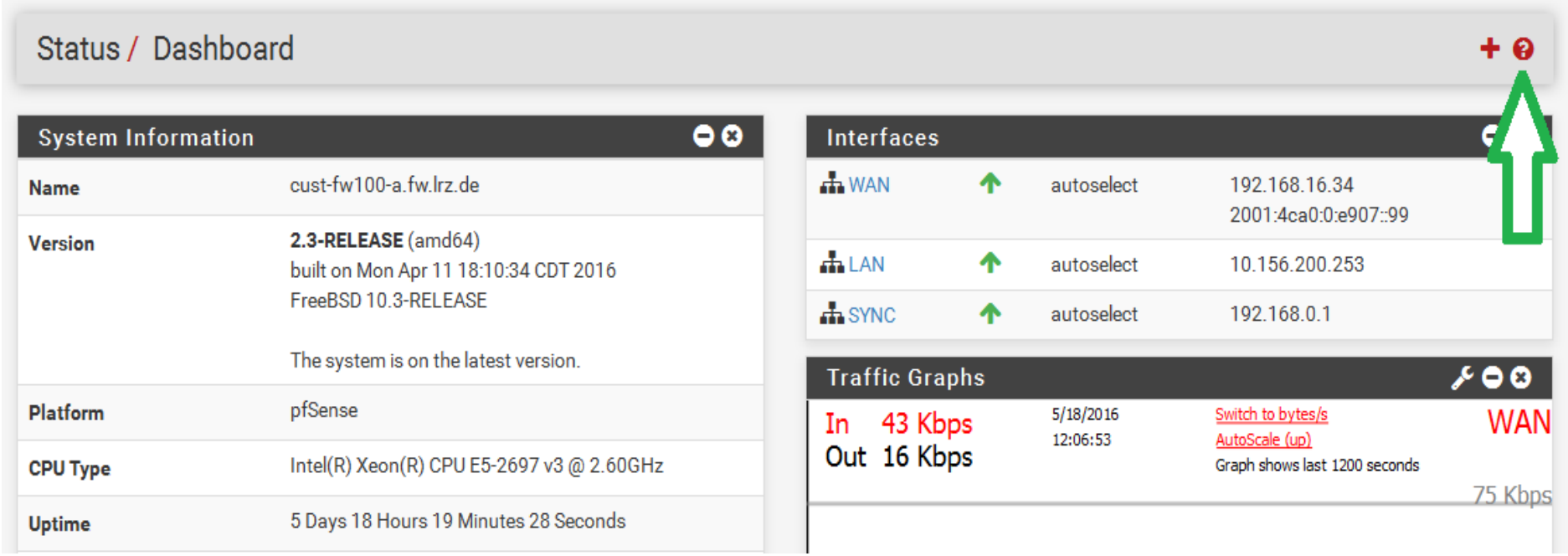
Status aktiver Verbindungen

Diagnostics → States



Hilfe auf der pfSense

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



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

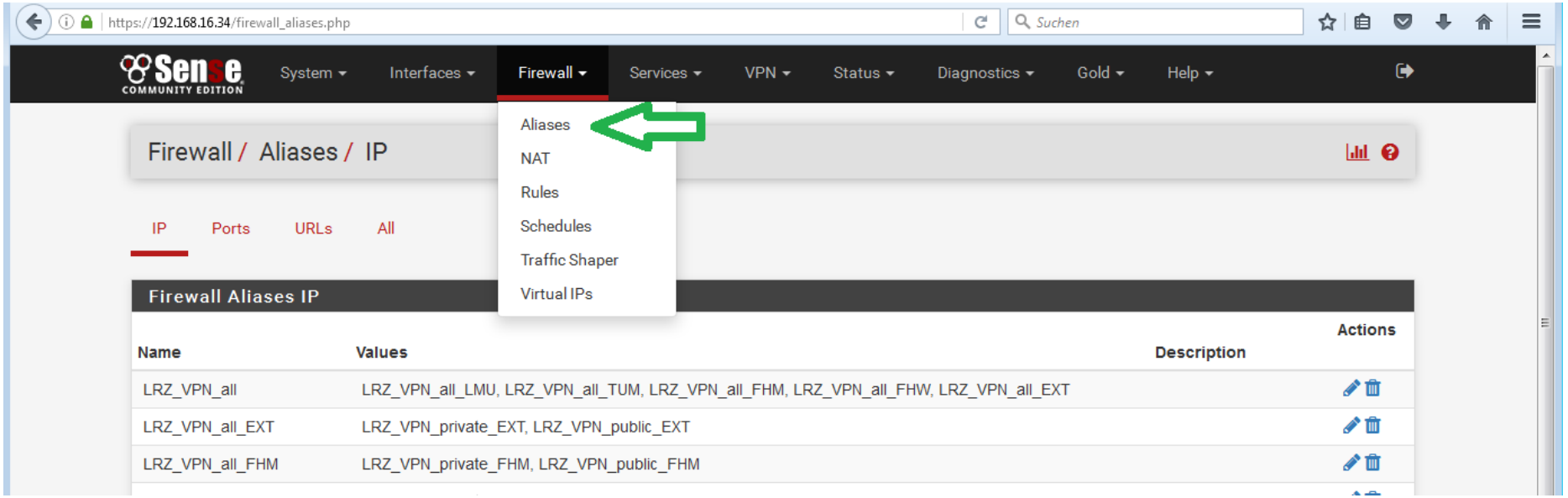
Stateful packet inspection:

- 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

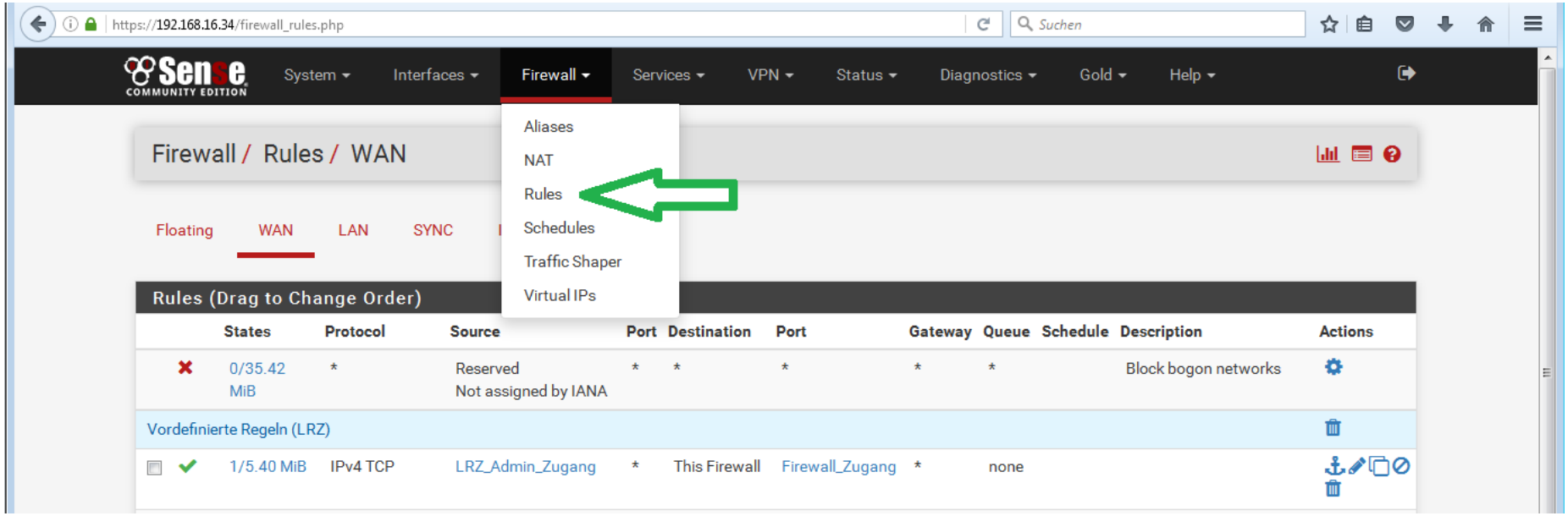
Firewall → Aliases



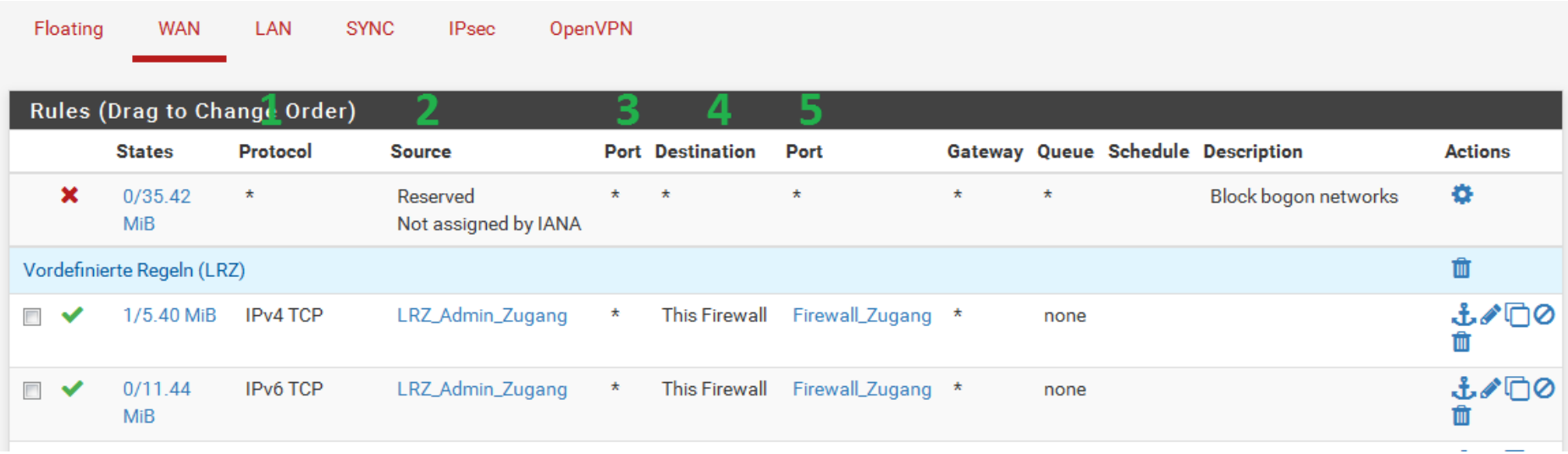
Regeln auf der pfSense

Die Regeln können aufgerufen werden unter

Firewall → Rules



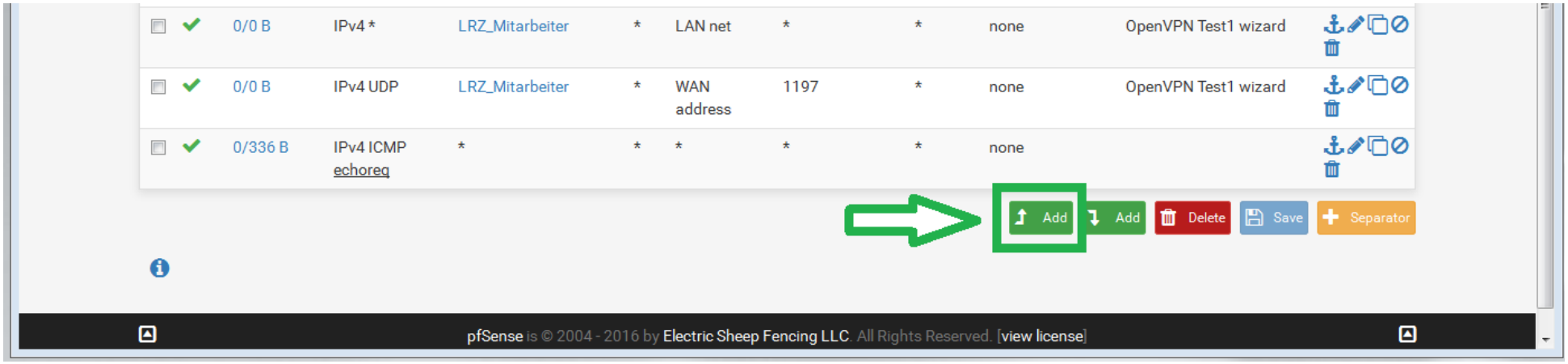
Regeln auf der pfSense



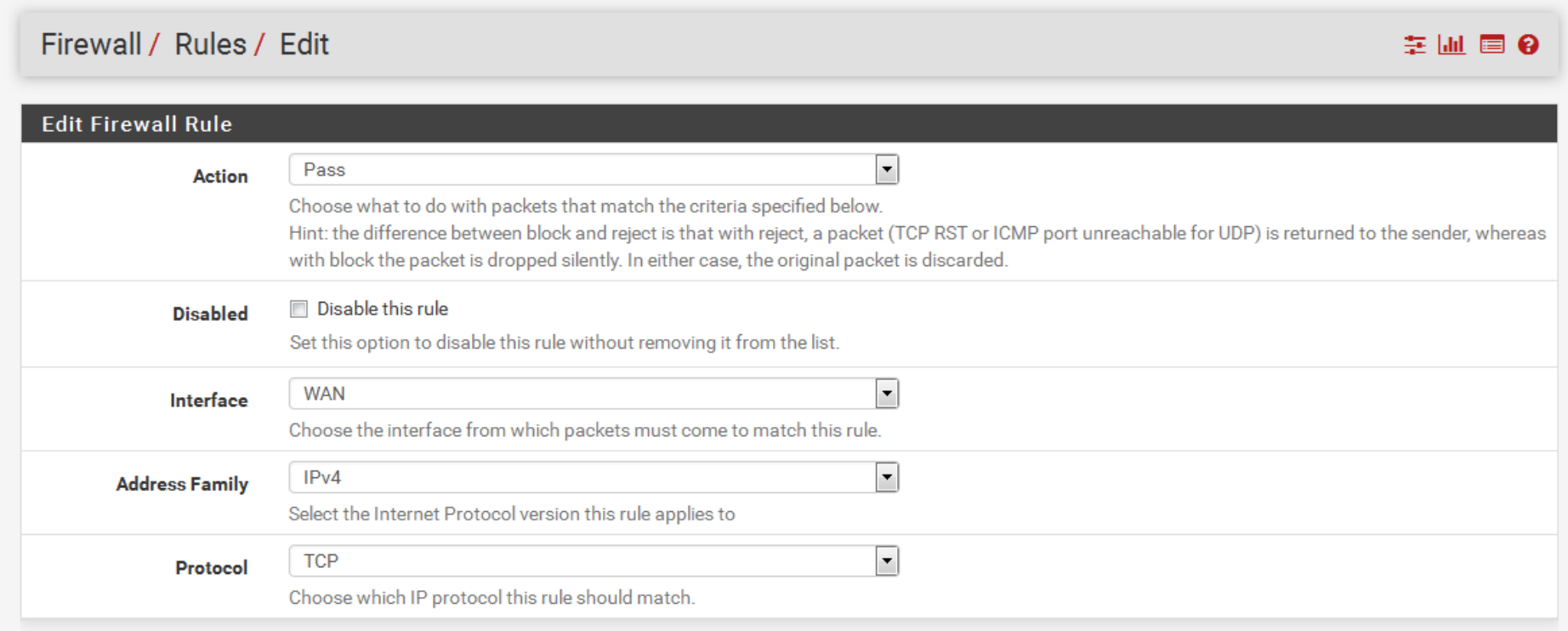
1. Relevantes Protokoll
2. Quell-IP-Adresse
3. Quell-Port
4. Ziel-IP-Adresse
5. Ziel-Port

Eine neue Regel hinzufügen

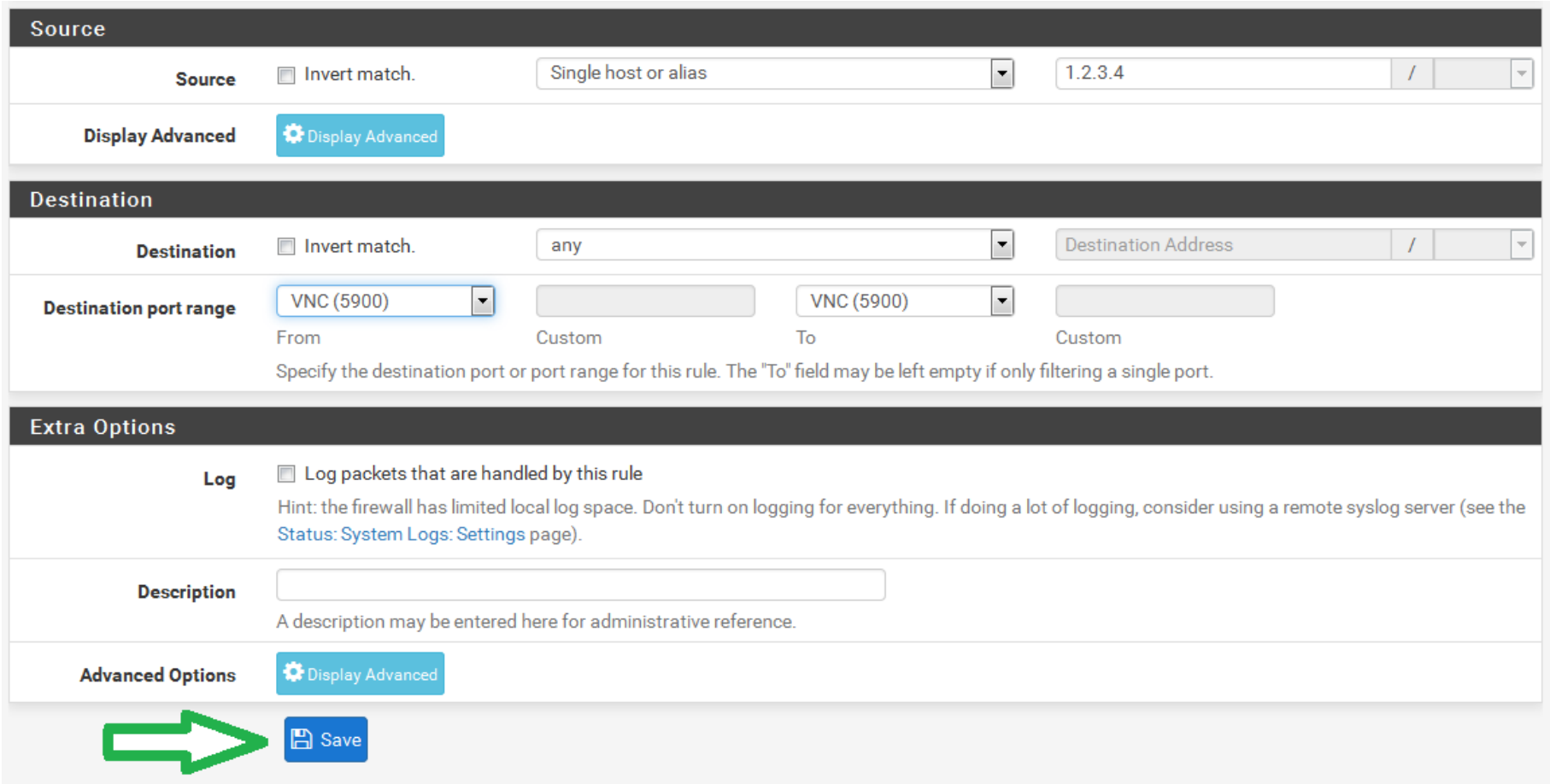
Am unteren Ende der Liste befindet sich ein Button zum Hinzufügen einer Regel an den ersten Listenplatz.



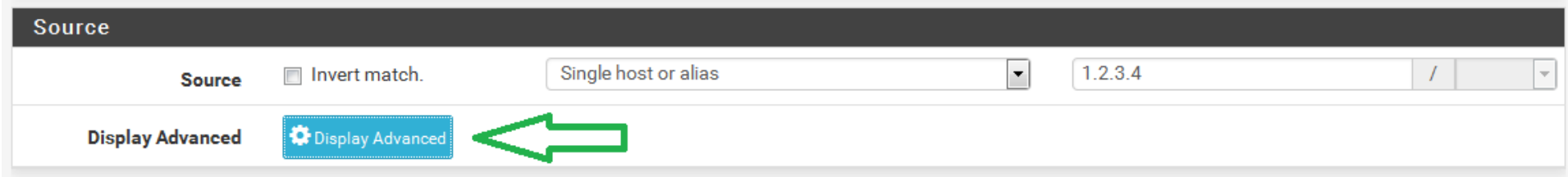
Eine neue Regel hinzufügen – Schritt 1

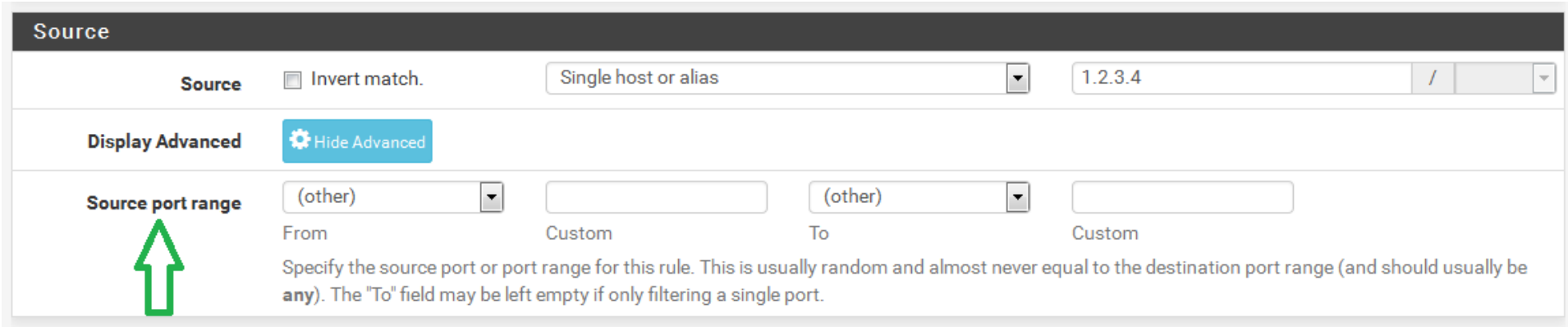


Eine neue Regel hinzufügen – Schritt 2



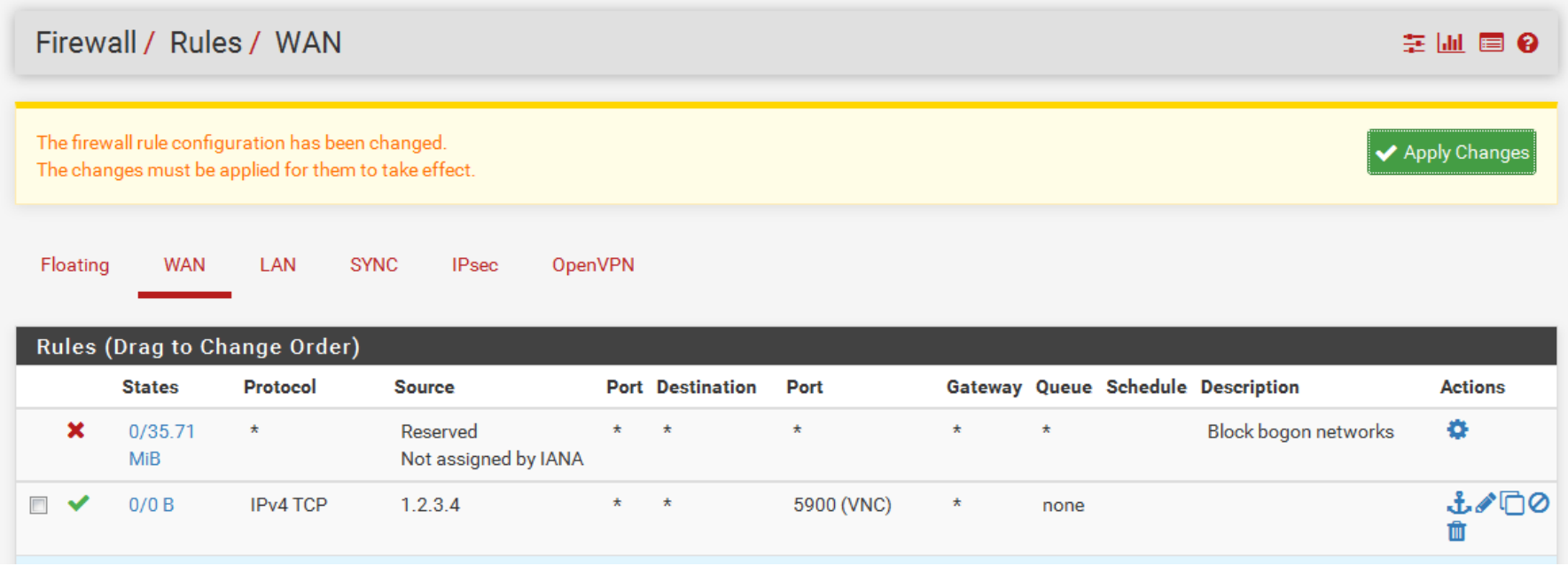
Eine neue Regel hinzufügen – Optionaler Source-Port





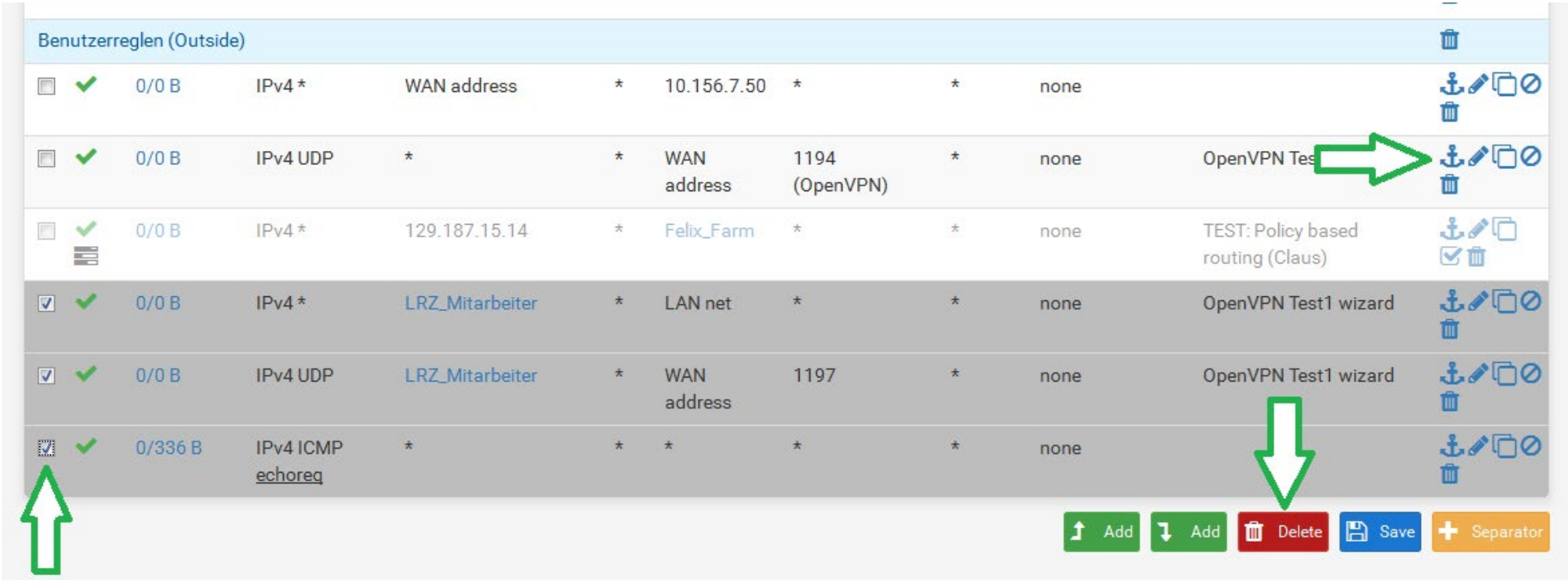
Eine neue Regel hinzufügen

Neue Regel wird an oberster Stelle angefügt



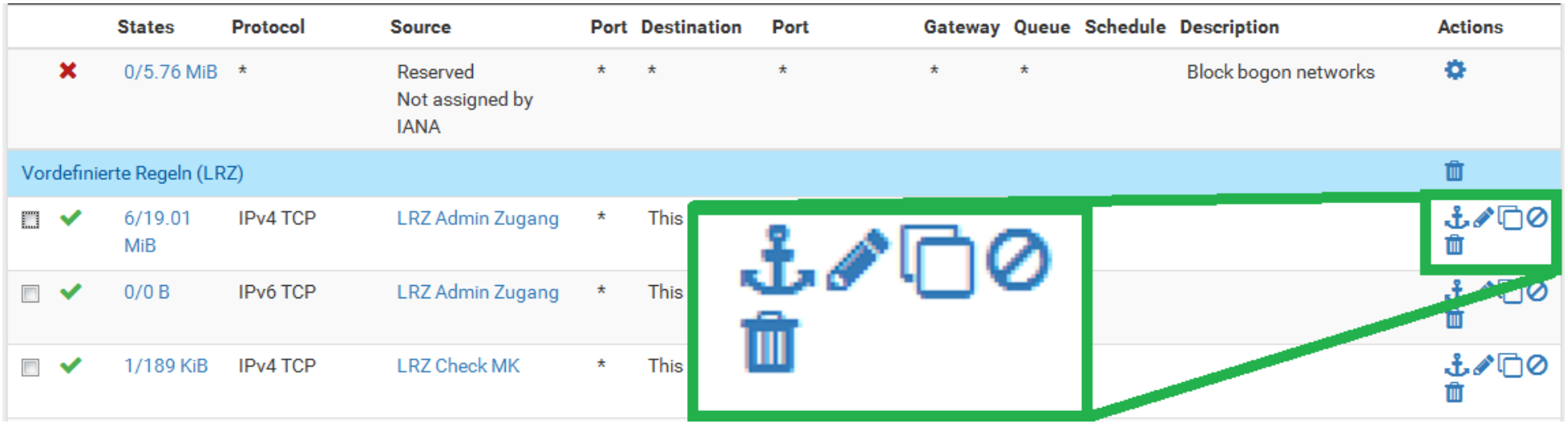
Am unteren Ende der Liste ist eine weitere Schaltfläche zum Hinzufügen einer Regel am **unteren** Ende der Liste!

Auswahl und Bearbeitung mehrerer Einträge



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



- **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

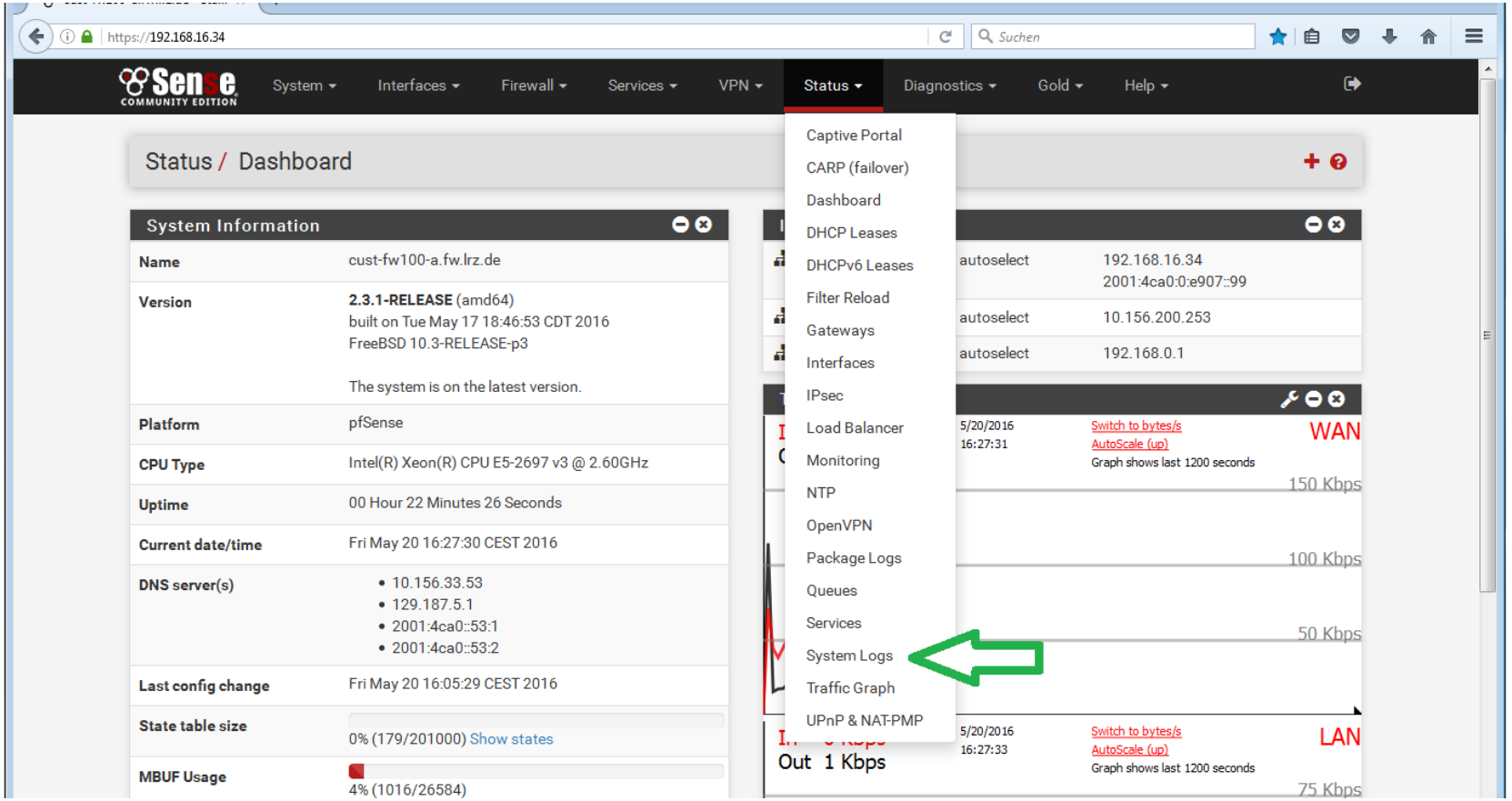
Aktivierung und Deaktivierung einzelner Regeln

	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	⚓ ✎ ⧉ ⊘ 🗑
☐ ✔		v4+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	⚓ ✎ ⧉ ⊘ 🗑

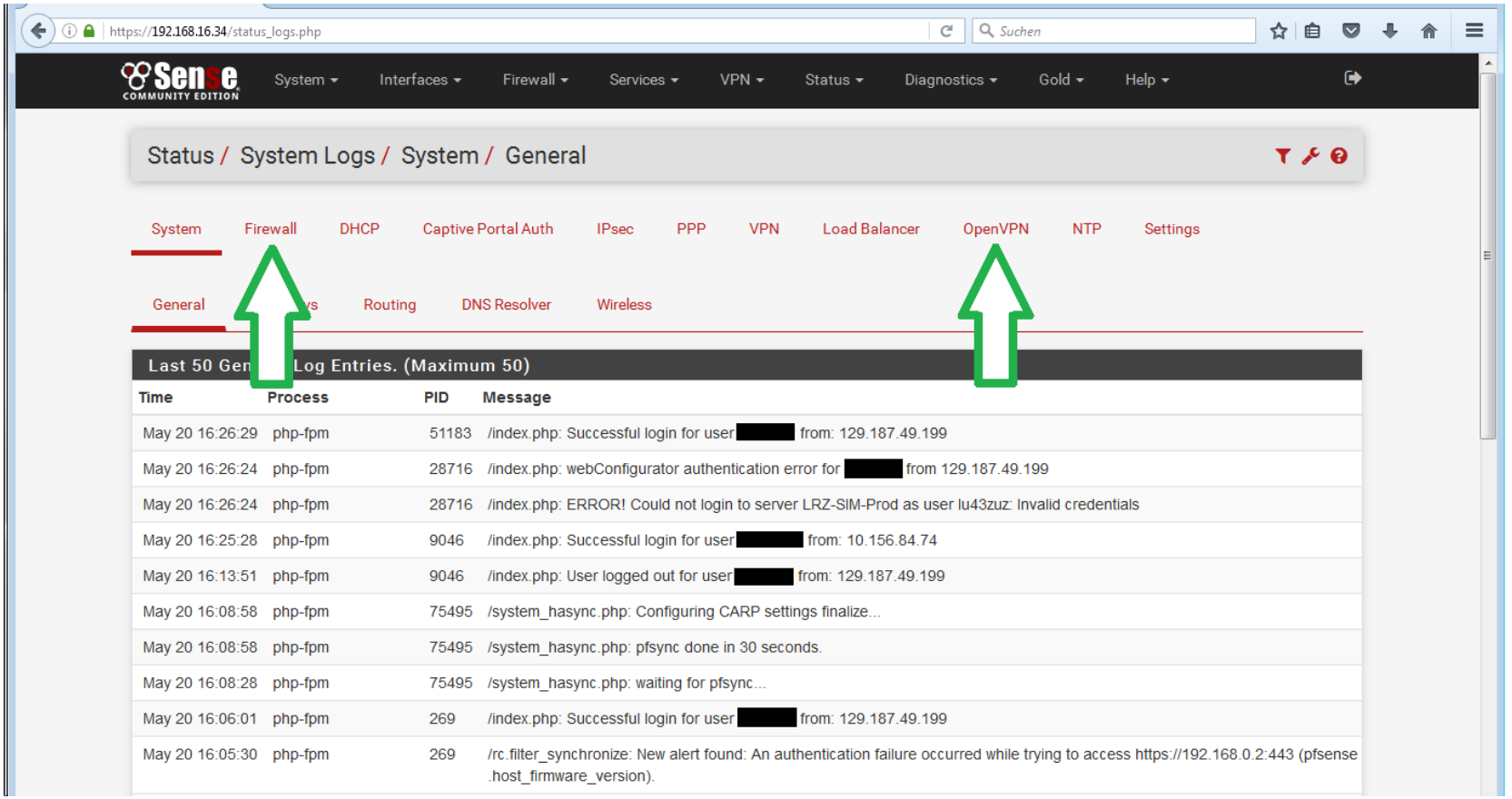
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✖	0/72 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
Vordefinierte Regeln											🗑
☐ ✔	2/16.37 MiB	IPv4+6 TCP	LRZ_Admin_Zugang	*	OUTSIDE net	Firewall_Zugang	*	none		Administrativer Zugang 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.

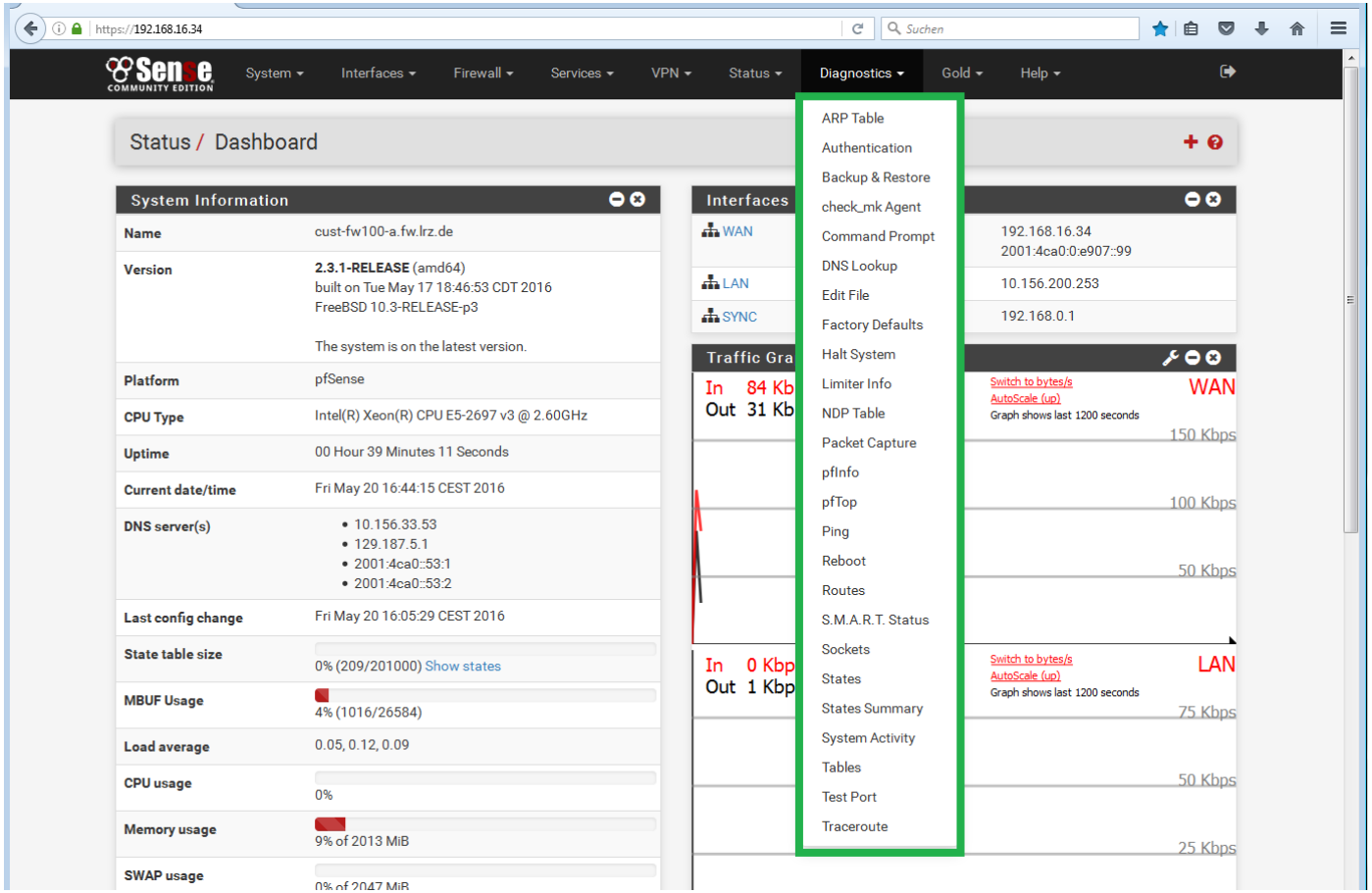
System Logs


https://192.168.16.34
Suchen
Sense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Captive Portal
CARP (failover)
Dashboard
DHCP Leases
DHCPv6 Leases
Filter Reload
Gateways
Interfaces
IPsec
Load Balancer
Monitoring
NTP
OpenVPN
Package Logs
Queues
Services
System Logs
Traffic Graph
UPnP & NAT-PMP
Status / Dashboard
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
5/20/2016
16:27:31
Switch to bytes/s
AutoScale (up)
Graph shows last 1200 seconds
WAN
150 Kbps
100 Kbps
50 Kbps
5/20/2016
16:27:33
Switch to bytes/s
AutoScale (up)
Graph shows last 1200 seconds
LAN
Out 1 Kbps
75 Kbps

System Logs


https://192.168.16.34/status_logs.php
Suchen
pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Status / System Logs / System / General
System
Firewall
DHCP
Captive Portal Auth
IPsec
PPP
VPN
Load Balancer
OpenVPN
NTP
Settings
General
Routing
DNS Resolver
Wireless
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



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	

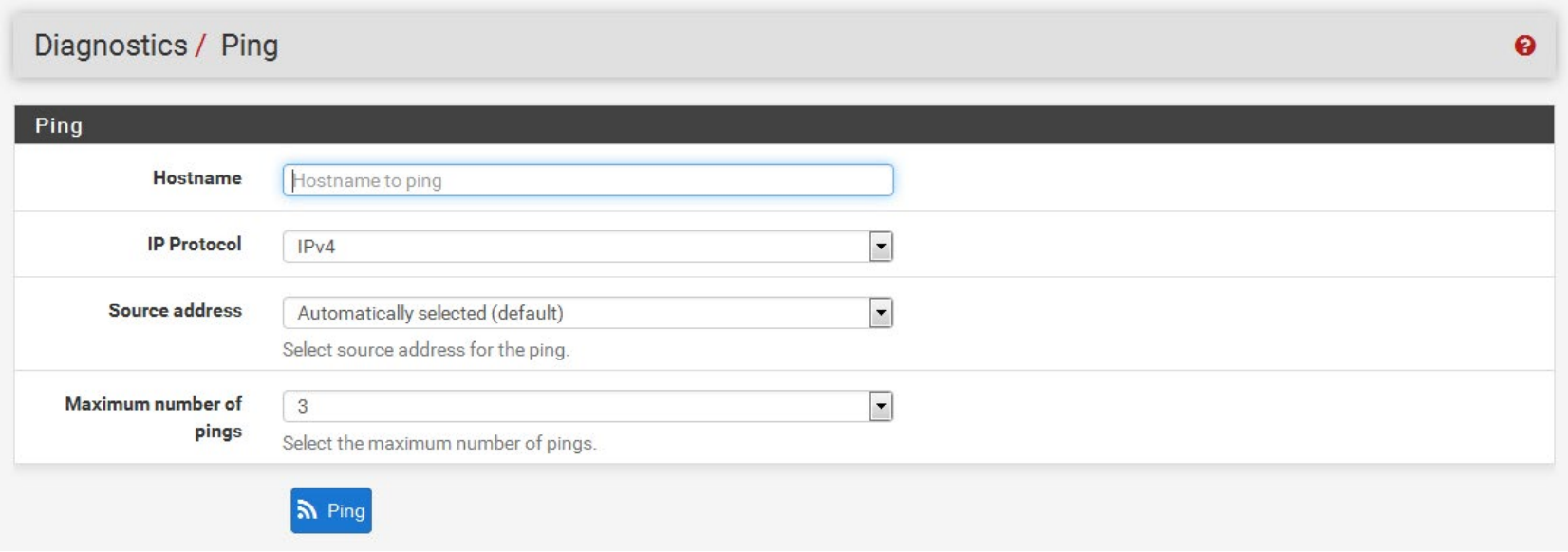
Local IPv6 peers use NDP instead of ARP.

Diagnostics / NDP Table

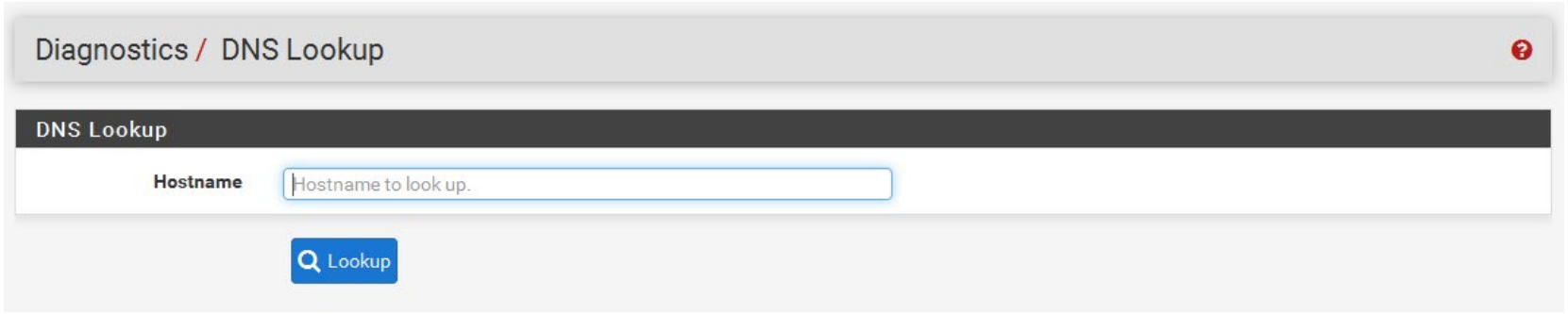
NDP Table

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

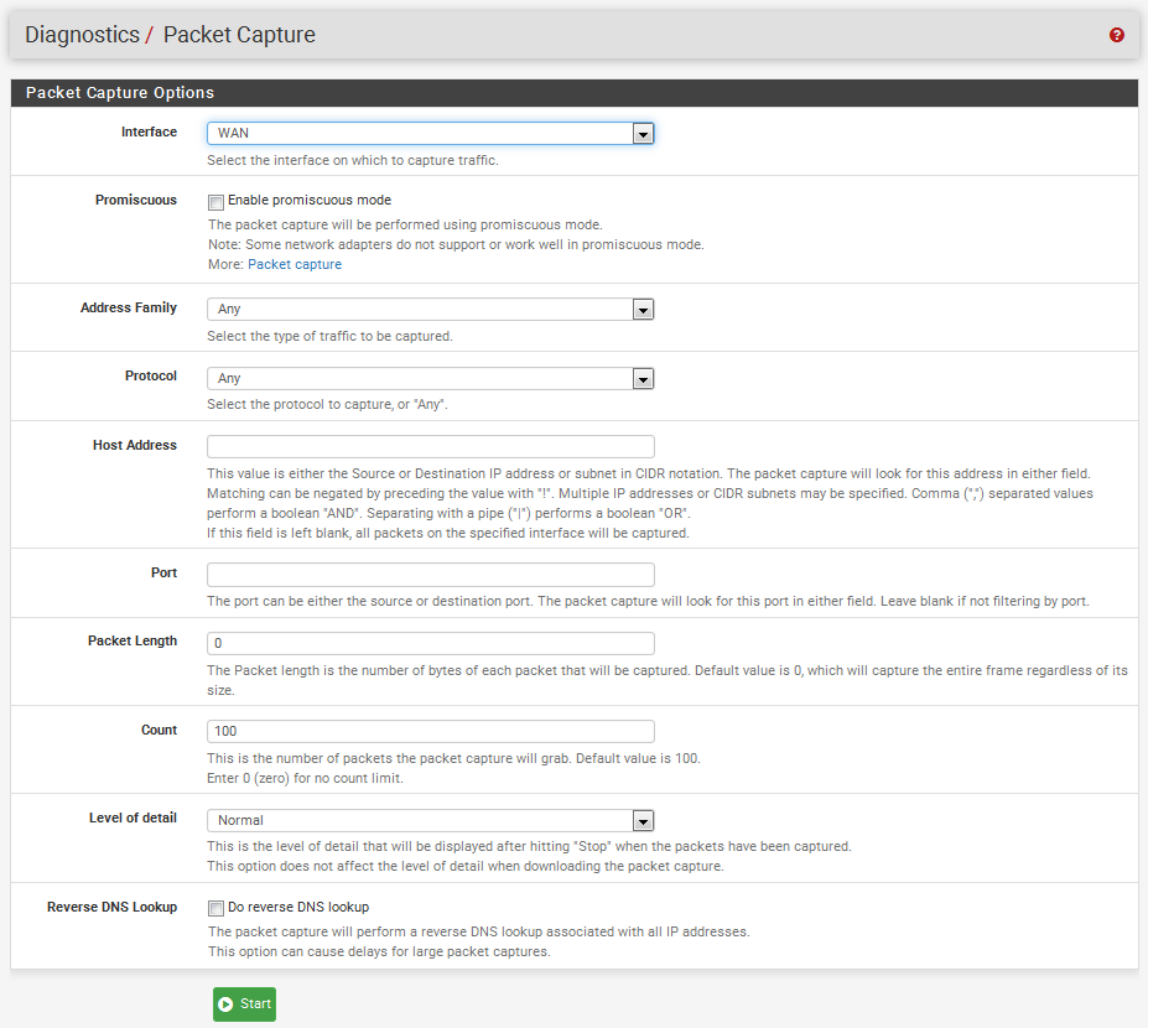
Diagnosetools auf der pfSense



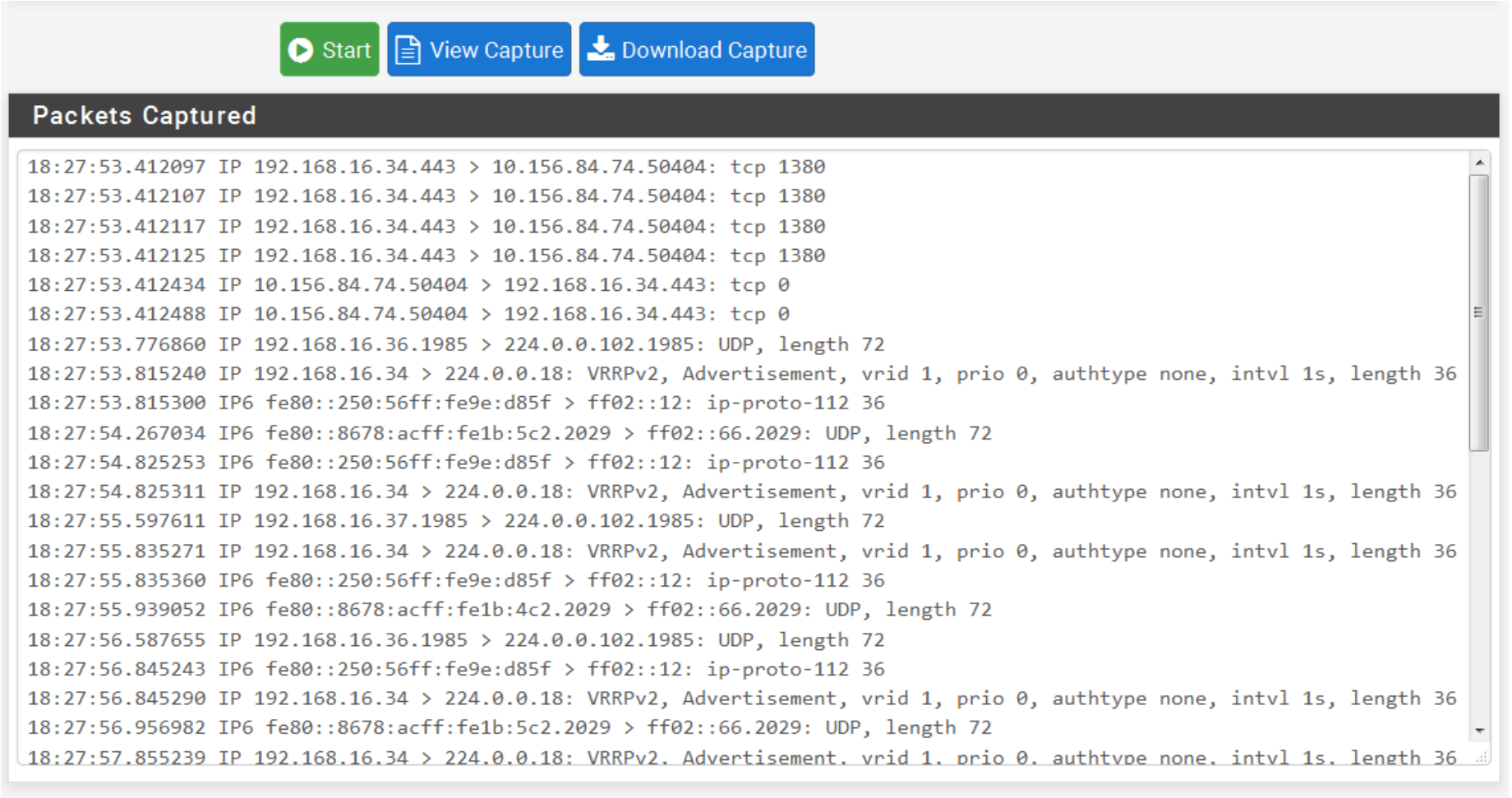
Diagnosetools auf der pfSense



Diagnosetools auf der pfSense



Diagnosetools auf der pfSense



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