



Leibniz-Rechenzentrum  
der Bayerischen Akademie der Wissenschaften



pfSense – Virtuelle Firewalls am  
Leibniz-Rechenzentrum

- 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

Aus Perspektive der IT-Sicherheit werden **verschiedene Arten von Rechnernetzen** unterschieden, **die durch Interfaces** an der Firewall technisch umgesetzt werden

### Inside

→ zu schützende Netze

### Outside

→ Externes Netz, MWN, Internet

Eine Firewall ist eine technische Maßnahme, die den Zugriff in bzw. aus einem Rechnernetz reglementiert und einschränkt. Damit eine Firewall diesen Zugriff abhängig von Quelle, dem angesprochenen Zielsystem oder des dort angesprochenen Dienstes (Port) filtern kann, muss der Datenverkehr zwischen den Netzen die Firewall passieren.

Die Funktionalität vieler Firewall-Produkte geht über die Filterung auf Vermittlungs- und Transportschicht hinaus.

Sogenannte Unified Threat Management (UTM) Systeme analysieren die Kommunikation zusätzlich auf höheren

Schichten. In diesem Fall spricht man von einem Intrusion Detection/Prevention System oder einem Web-Proxy,

wenn zusätzlich die abgerufenen Inhalte gefiltert werden (Content Filter).

- 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

Eine Firewall ist eine technische, präventive Sicherheitsmaßnahme und ein wichtiger Bestandteil eines Sicherheitskonzeptes. Sie ist jedoch kein vollständiger Ersatz dafür.

Da die Absicherung der Kommunikation auf der Vermittlungs- und Transportschicht stattfindet, kann eine Firewall dort keinen Schutz vor unberechtigter Datenmanipulation, vor Datenverlust, unerwünschter Offenlegung

vertraulicher Informationen oder die Beeinträchtigung der Verfügbarkeit von Systemen und dort betriebener

Dienste bieten. Möglicherweise vorhandene Zusatzfunktionen (z.B. IDS, Proxies, ...) bieten diese Funktionalität.

Firewalls werden an Netzgrenzen und -übergängen eingesetzt, um die Kommunikation zwischen einem als vertrauenswürdig eingestuftem internen (inside) Netz und nicht vertrauenswürdigen Netzen (outside), z.B. das

Internet, zu reglementieren. Angriffe, die **innerhalb** des vertrauenswürdigen Netzes durchgeführt werden und die Firewall deshalb nicht passieren, können damit nicht verhindert werden.



## 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

Im Rahmen des Dienstangebots „Virtuelle Firewall“ bietet das LRZ für Institute und Organisationen im Münchner Wissenschaftsnetz (MWN) eine virtuelle Firewall auf LRZ-Hardware (VMWare ESXi) an. Die Kunden-Firewall besteht aus zwei virtuellen Maschinen, die als Active-Standby-Paar redundant konfiguriert sind und damit ein hohes Maß an Ausfallsicherheit bieten.

Bereits die Konfiguration im Auslieferungszustand bietet eine grundlegende Absicherung der zu schützenden Systeme in den Inside-Netzen und ist außerdem speziell auf den Einsatz im MWN zugeschnitten. Eine täglich automatisch durchgeführte Sicherung (Backup) der kompletten Firewall-Konfiguration gewährleistet eine schnelle Rückkehr zu einem funktionierenden System innerhalb weniger Minuten, etwa bei einer nicht revidierbaren Fehlkonfiguration oder einem fehlgeschlagenen System-Update.



## Dienst des LRZ: Virtuelle Firewalls

---

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

Die Erreichbarkeit des Firewall-Systems selbst und der dort betriebenen Dienste, z.B. des Web-Interfaces, sowie die aktuelle CPU-, Speicher- und Festplattenauslastung werden überwacht. So wird übermäßiger Ressourcenverbrauch frühzeitig erkannt und daraus resultierende Instabilitäten oder Systemausfälle werden bereits im Vorfeld vermeiden.

Das zentrale Management ermöglicht ein einfaches Ausrollen sowie flächendeckende Software-Updates oder Konfigurationsänderungen.

Im Auslieferungszustand bietet die virtuelle Firewall **3** Netz-Interfaces:

- Inside (LAN)
- Outside (WAN)
- SYNC (privates Netz für High-Availability)

Bei erhöhten Durchsatzanforderungen können optional dedizierte Interfaces bereitgestellt werden. Dies ist jedoch mit zusätzlichen Kosten verbunden. Durch Tagging stellt die pfSense verschiedene VLAN-Interfaces zur Verfügung.

### 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](https://doc.pfsense.org/index.php/Main_Page)

Forum <https://forum.pfsense.org/index.php>

Um seinen Kunden eine aktuelle und den Anforderungen entsprechende Firewall-Lösung anbieten zu können,

hat das Firewall-Team des LRZ eine umfangreiche Evaluation sowohl kommerzieller als auch Open-Source-Produkte

durchgeführt. In einem Katalog wurden mehr als 80 Anforderungen definiert, denen sich knapp 30 Firewall-Lösungen

stellen mussten.

Die drei besten Produkte wurden einem erweiterten Live-Test im MWN unterzogen.

Gewinner dieser Produktauswahl war die auf FreeBSD-basierende Open-Source-Firewall-Distribution **pfSense**

(<https://www.pfsense.org>), die 2004 als Abspaltung des m0n0wall hervorgegangen ist. Eine Übersicht des kompletten

pfSense-Funktionsumfangs findet sich unter

<https://www.pfsense.org/about-pfsense/features.html>



## 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**

Die Firewall kann über ihre IP-Adresse oder ihren DNS-Namen erreicht werden.

Die Konfiguration erfolgt über eine Web-Oberfläche.

Falls nötig kann aber auch per SSH auf die Firewall zugegriffen werden.

Die Authentifizierung erfolgt mit einer LRZ-SIM-Kennung, so dass das Anlegen und die Pflege lokaler Nutzerkonten entfällt. Das gilt sowohl für die Firewall-Administrator- als auch für die VPN-Zugänge.

Die gruppenbasierte Benutzerverwaltung beruht auf dem im MWN eingesetzten Master-User-Konzept.

Die Master-User können sowohl die Firewall-Administrator- als auch die VPN-Berechtigungen in speziellen

Gruppen im LRZ-Identity-Management-Portal verwalten.



## Das Dashboard

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

System Information		Interfaces	
Name	cust-fw100-a-fw.lrz.de	WAN	↑ autoselect 192.168.16.34 2001:4ca0:0:e907:99
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.	LAN	↑ autoselect 10.156.200.253
Platform	pfSense	SYNC	↑ autoselect 192.168.0.1
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)	<ul style="list-style-type: none"><li>• 10.156.33.53</li><li>• 129.187.5.1</li><li>• 2001:4ca0:0:53:1</li><li>• 2001:4ca0:0:53:2</li></ul>		
Last config change	Fri May 13 11:50:37 CEST 2016		

10.06.2016

Leibniz-Rechenzentrum

9

Spezielle Dashboard-Widgets zeigen den aktuellen Durchsatz und eventuelle Fehler der angeschlossenen

Netz-Interfaces, je nach Geschmack aufbereitet in Live-Traffic-Graphen oder in interface-spezifischen Statistiken.

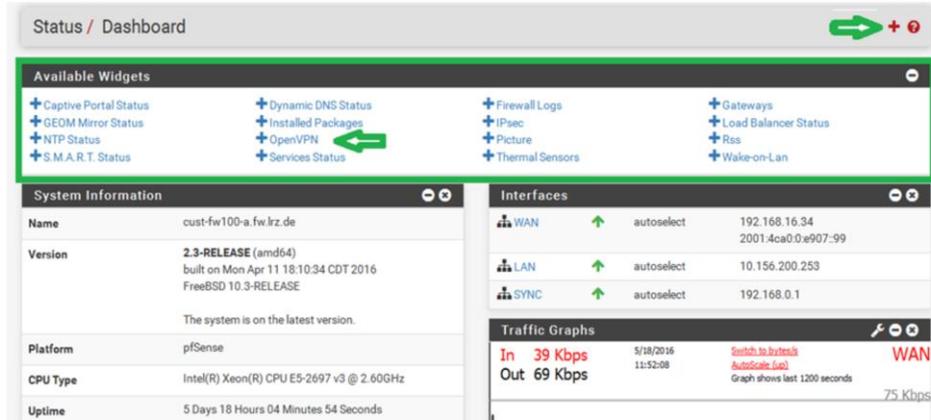
## Statistiken und Traffic Graphen (Live) der Netzinterfaces

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

Spezielle Dashboard-Widgets zeigen den aktuellen Durchsatz und eventuelle Fehler der angeschlossenen

Netz-Interfaces, je nach Geschmack aufbereitet in Live-Traffic-Graphen oder in interface-spezifischen Statistiken.

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



The screenshot shows the pfSense dashboard interface. At the top, there is a breadcrumb 'Status / Dashboard' and a green arrow icon with a plus sign. Below this is a section titled 'Available Widgets' which is highlighted with a green border. This section contains a grid of widget options, each with a plus sign icon. A green arrow points to the 'OpenVPN' widget. Other visible widgets include Captive Portal Status, GEOM Mirror Status, NTP Status, S.M.A.R.T. Status, Dynamic DNS Status, Installed Packages, Services Status, Firewall Logs, IPsec, Picture, Thermal Sensors, Gateways, Load Balancer Status, Rrs, and Wake-on-Lan.

Below the available widgets are two main sections: 'System Information' and 'Interfaces'.

**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	5/18/2016 11:52:08	Switch to bytes!	WAN
Out	69 Kbps		AutoScale (up)	
				Graph shows last 1200 seconds
				75 Kbps

Das Dashboard lässt sich durch Hinzufügen weiterer Widgets individuell anpassen. Auch die Anordnung dieser

Widgets ist per Drag-and-Drop beliebig konfigurierbar.

## Status aktiver Verbindungen

*Diagnostics* → *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	FRI_WAIT_2 FRI_WAIT_2	0/0	0 B / 0 B
lo0	udp	:160843] -> :1123]	MULTIPLE MULTIPLE	0/0	0 B / 0 B
lo0	udp	:1123] <- :160843]	MULTIPLE MULTIPLE	0/0	0 B / 0 B
WAN	ipv6-icmp	802:1:800:1 <- 2001:4c:a0:0:e907:99	NO_TRAFFIC NO_TRAFFIC	0/0	0 B / 0 B

Der Status aktuell aktiver Verbindungen kann über den Menüpunkt Diagnostics – States oder über das Dashboard (System Information – State table size – Show States) angezeigt werden.

Die Liste aktiver Verbindungen enthält Informationen zu Protokoll, IP-Adressen, Verbindungsstatus, und Kommunikationsrichtung einer Verbindung.

Für jede Verbindung über die Firewall werden zwei States festgehalten:

- einer beim Eintreffen an der Firewall
- einer beim Verlassen der Firewall

Zur Verfügung stehende Filteroperationen helfen, die jeweils gesuchten Verbindungen schnell zu finden. Wird eine IP-Adresse in CIDR-Notation als Filter eingegeben, erscheint ein „Kill“ Button, mit dessen Hilfe sich alle angezeigten (gefilterten) Verbindungen beenden lassen. Einzelne Verbindungen lassen sich mit dem hinter jeder Zeile angezeigten „x“-Button beenden. Im Tab „Reset States“ könne alle Verbindungen zurückgesetzt werden.



## Hilfe auf der pfSense

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

The screenshot shows the pfSense Status / Dashboard page. It features three main sections: System Information, Interfaces, and Traffic Graphs. A green arrow points to a help icon (a question mark) in the top right corner of the dashboard area.

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 5/18/2016 12:06:53 [Switch to bytes/s](#) [AutoScale \(up\)](#) WAN  
Out 16 Kbps  
Graph shows last 1200 seconds 75 Kbps

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

10.06.2016

Leibniz-Rechenzentrum

13

Auf jeder Konfigurationsseite steht eine Hilfe-Funktion zur Verfügung. Diese beschreibt in Kurzform die Einstellmöglichkeiten der jeweiligen Konfigurations- oder Übersichtsseite. Diese verlinkt auf die Dokumentationsseiten von pfSense

Für weitere Informationen bietet pfSense jedoch auch eine ausführliche Dokumentation unter

[https://doc.pfsense.org/index.php/Main\\_Page](https://doc.pfsense.org/index.php/Main_Page)

- 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!**

Zugriffe in bzw. aus einem Netz über die Firewall lassen sich mithilfe von Regeln (Rules) einschränken.

Bei der Erstellung dieser Regeln sollte man generell an Folgendes denken:

- Wie sieht mein Netz generell aus?
- Wie viele Rechner/Drucker befinden sich in dem Netz?
- Wie werden die IP-Adressen dort vergeben? (DHCP/statisch)
- Welche Rechner sind Server und bieten Dienste an?
- Welche Dienste werden nach außerhalb angeboten? (z.B. Webserver, FTP, etc.)
- Welche Dienste, bereitgestellt auf Systemen in anderen Netzen werden verwendet?
- Bieten weitere Geräte Dienste im Netz an? (z.B. Zeiterfassung, Netzwerkdrucker, etc.)

Man unterscheidet beim Aufbau von Firewall-Regelwerken zwischen

- Blacklist (alles, was nicht explizit verboten ist, ist erlaubt)
- Whitelist (alles, was nicht explizit erlaubt ist, ist verboten)

Die pfSense-Plattform verwendet einen Whitelist-Ansatz und blockt jegliche Kommunikation, die nicht explizit per

Regeln erlaubt ist, was im Rahmen des LRZ-Dienstes virtuelle Firewall als sichere Grundkonfiguration gilt.

Vom Whitelist-Ansatz zum Blacklist-Ansatz kommt man, wenn man als letzte Regel ein any/any/allow definiert

Regeln werden der Reihe nach abgearbeitet!

## Beispiel 1

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

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

Regeln, welche die Kommunikation über die Firewall reglementieren, werden in einem Regelwerk zusammengefasst. Jede Regel besitzt eine Nummer, die ihrer Position in diesem Regelwerk entspricht, sowie Bedingungen für die Anwendbarkeit dieser Regel.

Erreicht ein im Rahmen einer Kommunikation zwischen zwei Teilnehmern (Quelle, Ziel) versendetes Paket

ein FW-Netzinterface, wird dort überprüft ob eine Regel diese Kommunikation explizit erlaubt. Das Regelwerk wird dabei, beginnend bei der ersten Regel, d.h. von oben nach unten, abgearbeitet. Die erste Regel, deren Bedingungen erfüllt sind, „matched“ und wird angewendet.

In Beispiel 1 gibt es eine Regel, welche den Zugriff auf den Webserver des LRZ des Systems mit der Quell-IP-Adresse 10.1.2.3, Ziel-IP-Adresse 129.187.255.234, Protokoll HTTP explizit erlaubt. Die nachfolgende Default-Blockregel kommt für dieses System nicht zur Anwendung.

Wie komme ich nun auf die IP-Adresse 129.187.255.234? (Diagnostics /DNS-Lookup)

In Beispiel 2 steht die Regel, welche den Zugriff auf den Webserver des LRZ des Systems mit der Quell-IP-Adresse 10.1.2.3 explizit erlaubt erst nach der Default-Block-Regel, d.h. der Zugriff wird verhindert.

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

Bei einer „stateful“ Firewall muss nicht, im Gegensatz zu einem reinen Paketfilter, eine Regel für die ein- und eine für die ausgehende Kommunikation definiert werden.

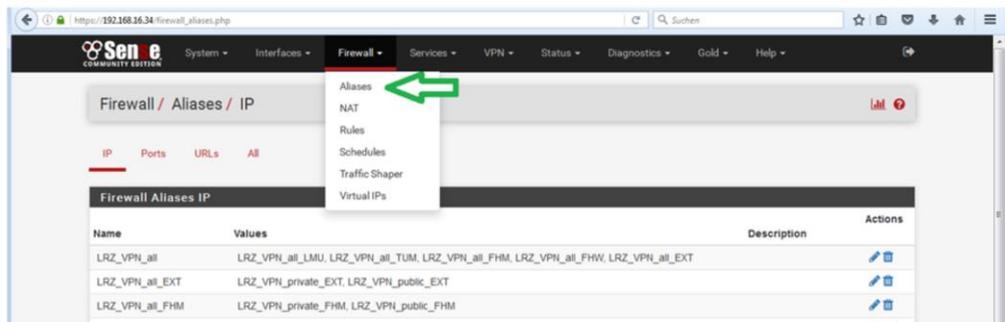
Antworten auf eine Anfrage aus dem vertrauenswürdigen Inside-Netz sind erlaubt, d.h. werden nicht geblockt.

Hierzu protokolliert die Firewall in dynamischen Zustandstabellen (State table) die ausgehenden Anfragen.

Direkte Anfragen aus dem Outside-Netz, z.B. dem Internet, ohne vorherige Anfrage, d.h. es existiert kein entsprechender Eintrag in der Zustandstabelle, werden automatisch geblockt.

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

### Firewall → Aliases



10.06.2016

Leibniz-Rechenzentrum

17

Aliase dienen einerseits als Platzhalter für meist nur über ihre IP-Adressen definierten Hosts, Netze oder Ports und können andererseits auch zur Gruppierung dieser Elemente eingesetzt und später, z.B. in der Konfiguration von Regeln verwendet werden.

Hier einige Beispiele, auf welche Arten sich Aliase in der pfSense definieren lassen:

- Eingabe von Test-Alias1 → 192.168.23.12, 192.168.23.16
- Eingabe von Test-Alias2 → 192.168.23.12 – 192.168.23.16  
(Ranges, werden automatisch expandiert)
- Eingabe von Test-Alias3 → testsystem.mwn.de, d.h. mittels Hostname
- Eingabe von Test-Alias4 → Netzen (CIDR-Notation) → 10.10.0.0/16, 2001:4ca0:bbbb::/64
- Eingabe von Test-Alias5 → Test-Alias1, Test-Alias2

IPv4- und IPv6-Aliase lassen sich kombinieren, so dass z.B. ein Host, der sowohl über IPv4 als auch IPv6 angebunden ist, über einen Alias definiert werden kann.

Löschen eines Alias, der in einer anderen Alias-Definition verwendet wird, ist nicht möglich.

Aliase lassen sich auch über eine außerhalb der Firewall gepflegte Liste von IP-Adressen, Subnetzen importieren (Bulk import). Z.B.

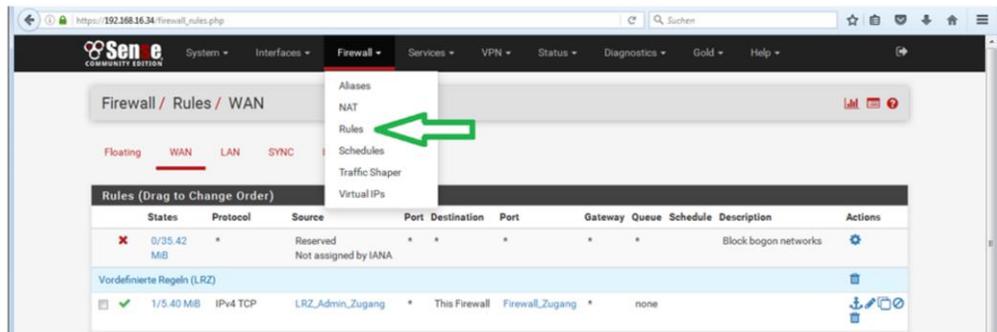
```
192.168.1.254 Home router
10.20.0.0/16 Office network
```

Hier geben die Bezeichner „Home router“ und „Office network“ den Beschreibungstext für das CIDR-Objekt an.

Änderungen an den Alias-Definitionen werden erst nach einem „Apply Changes“ aktiv, d.h. auch, dass sich Aliase erst nach ihre Definition und Aktivierung in anderen Alias-Definitionen verwenden lassen.

Die Regeln können aufgerufen werden unter

*Firewall* → *Rules*



Die Erstellung von Regelwerken auf der pfSense findet sich im Menü *Firewall* – *Rules*.

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 Übersicht über das aktuelle Regelwerk liefern mehrere Tabellen. Für jedes Netz-Interface sowie für jeden

aktiven VPN-Typ (z.B. IPSec, OpenVPN) existiert eine eigene Tabelle. Darüber hinaus gibt es so genannte

Floating Rules, mithilfe derer sich innerhalb einer einzigen Regel Einschränkungen sowohl für komplexere

Kommunikationsbeziehungen als auch für mehr als eine Kommunikationsrichtung oder beispielsweise die Kommunikation mehrerer interner Netzinterfaces untereinander festlegen lassen.

Funktionen zum Regel-Management, z.B. Hinzufügen neuer Regeln, Änderung der Regelreihenfolge oder das

Löschen einer selektierten Regel finden sich über die Schaltsymbole rechts neben der Tabelle bzw. Regel.

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



Das Hinzufügen einer neuen Regel zum Regelwerk erfolgt über einen der beiden [Add]-Schaltflächen, die die neue Regel entweder am Anfang oder Ende der Regelliste platzieren. Das Betätigen einer [Add]-Schaltflächen startet den Regel-Editor.

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.

Mithilfe des Regel-Editors werden die Einstellungen einer bestimmten Regel vorgenommen.

**Action:**

Regeln können den Zugriff explizit erlauben (Pass) bzw. blocken (block, reject). Im Gegensatz zu einem einfachen „block“ wird beim „reject“ dem Sender ein TCP RST oder ICMP port unreachable für UDP als Antwort gesendet.

**Disabled:** Regeln lassen sich explizit deaktivieren, auch temporär, ohne sie z.B. löschen zu müssen.

**Interface:** Auswahl für welches Netz-Interface die Regel gelten soll

**Address Family:** Regeln können sowohl für IPv4, IPv6 oder IPv4+IPv6 konfiguriert werden.

**Protocol:** Auswahl des IP-Protokolls, für das die Regel gelten soll (z.B. TCP, UDP, ICMP, any,...)

The screenshot shows a web-based configuration interface for adding a new firewall rule. It is divided into several sections:

- Source:** Includes a "Source" dropdown menu set to "Single host or alias" with the value "1.2.3.4". There is an "Invert match" checkbox and a "Display Advanced" button.
- Destination:** Includes a "Destination" dropdown menu set to "any" with a "Destination Address" field. Below it, the "Destination port range" is set to "VNC (5900)" for both "From" and "To" ports. There are "Invert match" and "Display Advanced" options.
- Extra Options:** Features a "Log" checkbox with the label "Log packets that are handled by this rule" and a descriptive hint. There is also a "Description" text input field.
- Advanced Options:** Includes a "Display Advanced" button.

A green arrow points to the "Save" button at the bottom of the form.

**Source:** Angabe der Quelle der Kommunikation (z.B. Single Host, Network, Alias, ...)

Durch Aktivieren der Checkbox „Invert match“ lässt sich die Regel sehr einfach invertieren.

**Destination:** Angabe des Ziels der Kommunikation (z.B. Single Host, Network, Alias, ...)

Durch Aktivieren der Checkbox „Invert match“ lässt sich auch hier die Regel sehr einfach invertieren.

**Destination Port Range:** Port- bzw. Port-Range auf dem Zielsystem, für die die Regel gelten soll.

**Log:** Anhaken dieser Checkbox aktiviert das Logging für diese Regel. Aufgrund des begrenzten Speicherplatzes für Log-Einträge auf der Firewall, sollte das Logging nur sehr selektiv, z.B. für Debugging-Zwecke, aktiviert werden.

**Description:** (optionale) Beschreibung der Regel, (besser ist das)



Source

Source  Invert match. Single host or alias 1.2.3.4 /

Display Advanced

A green arrow points to the 'Display Advanced' button.



Source

Source  Invert match. Single host or alias 1.2.3.4 /

Display Advanced

Source port range (other) From Custom 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.

A green arrow points to the 'Source port range' label.

**Display Advanced:** Aufklappen der Eingabemaske für den Quellport.

**Source Port Range:** Port- bzw. Port-Range auf dem Quellsystem, für das die Regel gelten soll.

## 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. Apply Changes

Floating **WAN** LAN SYNC IPsec OpenVPN

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!

Regeln lassen sich auch „auf Basis“ einer bereits bestehenden Regel erstellen. Dazu wählt man das Copy-Symbol mit den zwei symbolischen Blättern rechts neben der zu kopierenden Regel.

Die Reihenfolge der Regeln kann durch einfaches Drag-and-Drop (Ziehen und Ablegen) einer Regel verändert werden.

Benutzerregeln (Outside)										
<input type="checkbox"/>	✓	0/0 B	IPv4 *	WAN address	*	10.156.7.50	*	*	none	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none	OpenVPN Test
<input type="checkbox"/>	✓	0/0 B	IPv4 *	129.187.15.14	*	Felix_Farm	*	*	none	TEST: Policy based routing (Claus)
<input checked="" type="checkbox"/>	✓	0/0 B	IPv4 *	LRZ_Mitarbeiter	*	LAN net	*	*	none	OpenVPN Test1 wizard
<input checked="" type="checkbox"/>	✓	0/0 B	IPv4 UDP	LRZ_Mitarbeiter	*	WAN address	1197	*	none	OpenVPN Test1 wizard
<input checked="" type="checkbox"/>	✓	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)

Für die Bearbeitung des Regelwerks stehen verschiedene Funktionen zu Verfügung:

- Kontrollkästchen (Checkboxes) für Mehrfachauswahl, z.B. um mehrere Regeln im Regelwerk zu verschieben oder auf einmal zu löschen.
- Verschiedene Aktionssymbole zum Bearbeiten einer bestimmten Regel.

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)										🗑️
<input type="checkbox"/>	✓ 6/19.01 MiB	IPv4 TCP	LRZ Admin Zugang	*	This					📌 ✎ 📄 ⚪ 🗑️
<input type="checkbox"/>	✓ 0/0 B	IPv6 TCP	LRZ Admin Zugang	*	This					📌 ✎ 📄 ⚪ 🗑️
<input type="checkbox"/>	✓ 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

Für die Bearbeitung des Regelwerks stehen verschiedene Funktionen zu Verfügung:

- Bearbeiten einer Regel mithilfe des Regel-Editors (Stift-Symbol)
- Erstellen einer neuen Regel auf Basis der ausgewählten Regel („Klonen“) und öffnen des Regeleditors (Doppelblatt-Symbol)
- Deaktivieren einer Regel (Durchgestrichener-Kreis-Symbol)
- Löschen einer Regel (Papierkorb-Symbol)

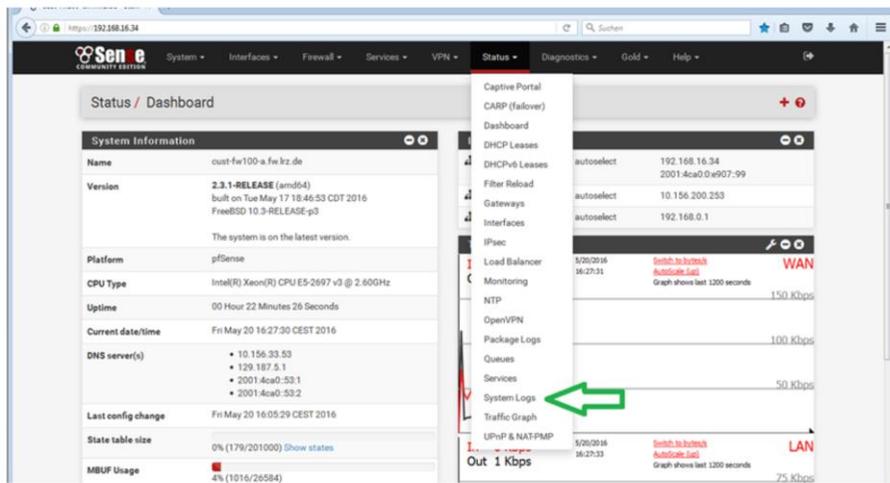
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✘ 0/72 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	⚙️
Vordefinierte Regeln										
<input checked="" type="checkbox"/>	7/16.31 MIB	IPv4+6 TCP	LRZ_Admin_Zugang	*	OUTSIDE net	Firewall_Zugang	*	none	Administrativer Zugang LRZ	📌 🗑️
<input checked="" type="checkbox"/>	4+6 TCP	User_Admin_Access	*	OUTSIDE net	Firewall_Zugang	*	none	Administrativer Zugang Benutzer	📌 🗑️	
<input checked="" type="checkbox"/>	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										
<input checked="" type="checkbox"/>	2/16.37 MIB	IPv4+6 TCP	LRZ_Admin_Zugang	*	OUTSIDE net	Firewall_Zugang	*	none	Administrativer Zugang LRZ	📌 🗑️
<input checked="" type="checkbox"/>	1/24 KIB	IPv4+6 TCP	User_Admin_Access	*	OUTSIDE net	Firewall_Zugang	*	none	Administrativer Zugang Benutzer	📌 🗑️
<input checked="" type="checkbox"/>	0/26 KIB	IPv4+6 UDP	LRZ_SNMP_SYSTEME	*	OUTSIDE net	161 (SNMP)	*	none	SNMP	📌 🗑️

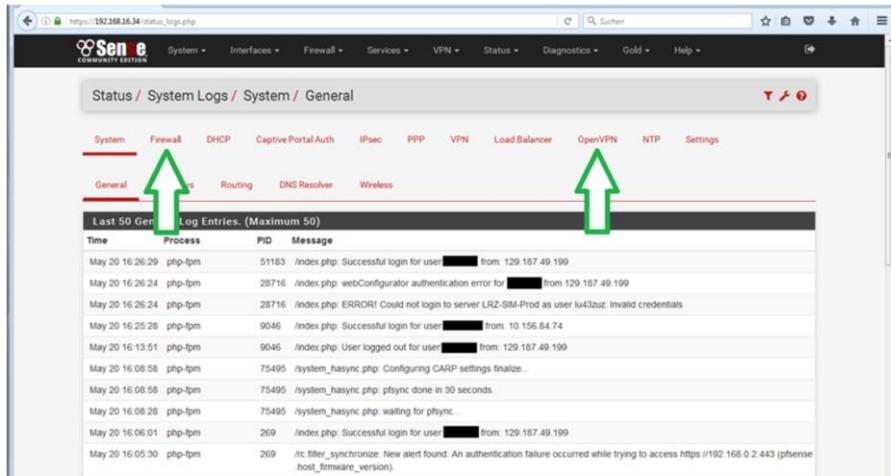
- Aktivierung von Regeln funktioniert analog.

Einzelne Regeln lassen sich auch in der tabellarischen Übersicht auf zwei Arten aktivieren bzw. deaktivieren:

1. Klicken auf Grünes Häkchen, links.
2. Klicken auf Durchgestrichener-Kreis-Symbol, rechts.



Statusmeldungen zum aktuellen System- bzw. Dienstzustand lassen sich in der Web-Oberfläche über das Menü *Status – System Logs* einsehen.



Neben den allgemeinen, das gesamte System betreffenden Ereignissen existieren zusätzlich, dienst-spezifische Protokollübersichten, z.B. für

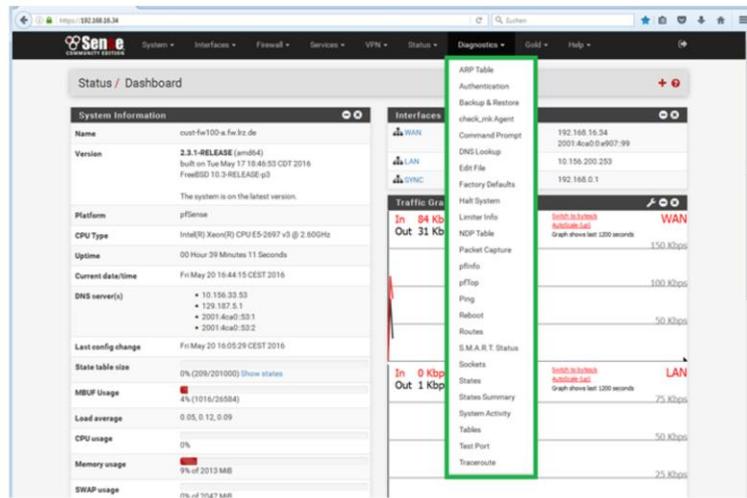
- Firewall: Ereignisse, die aufgrund einer Regel-Aktivität (z.B. Block, Pass) erzeugt wurden (vorausgesetzt das Logging wurde für diese Regel aktiviert)
- VPN-Zugang
- Dienst-spezifische Log-Dateien (DHCP, Load Balancer, NTP, ...)

Über den Tab *Settings* lassen sich allgemeine Einstellungen für das Logging, z.B. Anzahl der Log-Einträge in der Web-Oberfläche, generelles Deaktivieren des Loggings oder das Zurücksetzen der Log-Dateien vornehmen.

Desweiteren kann hier ein „Remote Logging“ beispielsweise an einen bereits vorhandenen, zentralen Syslog-Server konfiguriert werden:

- 1) Bis zu maximal drei remote Syslog-Server lassen sich mit Ihrer IP-Adresse bzw. IP:Port konfigurieren
- 2) Auswahl welche Ereignisse dorthin übertragen werden sollen

Die Weiterleitung an einen zentralen Syslog-Server erfolgt mittels UDP Datagramme auf Port 514.



Neben dem Protokollieren von System-Ereignissen in verschiedenen Logdateien, bietet pfSense auch diverse, bekannte Diagnosewerkzeuge, die sehr einfach über die Web-Oberfläche bedienbar sind

Die verschiedenen Werkzeuge finden sich im Menü *Diagnostics*.

Diagnostics / ARP Table

Interface	IP address	MAC address	Hostname
WAN	192.168.16.36	84:78:ac:1b:04:c2	vi-2310.cvr1-1wr.lrz.de
WAN	192.168.16.37	84:78:ac:1b:05:c2	vi-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:80:01	

Local IPv6 peers use NDP instead of ARP

Diagnostics / NDP Table

IPv6 address	MAC address	Hostname	Interface
2001:4ca0:0:e907:1:1	84:78:ac:1b:04:c2	vi-2310.cvr1-1wr.lrz.de	WAN
2001:4ca0:0:e907:1:2	84:78:ac:1b:05:c2	vi-2310.cvr1-2wr.lrz.de	WAN
fe80::250:56ff:fe9e:7e5e%vms2	00:50:56:9e:7e:5e		SYNC
fe80::250:56ff:fe9e:349d%vms1	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%vms0	84:78:ac:1b:05:c2		WAN
fe80::8678:acff:fe1b:4c2%vms0	84:78:ac:1b:04:c2		WAN
fe80::250:56ff:fe9e:d85f%vms0	00:50:56:9e:d8:5f		WAN
2001:4ca0:0:e907:99	00:50:56:9e:d8:5f		WAN

ARP Address Resolution Protocol

Dient zum Identifizieren von IPv4-Systeme anhand Ihrer MAC-Adresse

NDP Neighbor Discovery Protocol

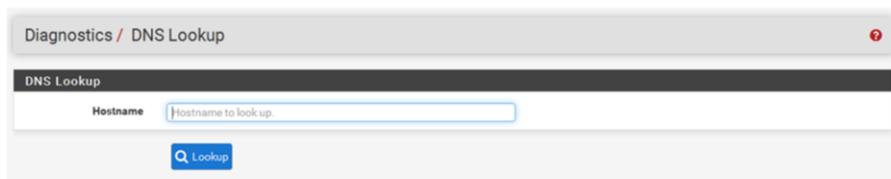
Zeigt die IPv6 Geräte mit ihrer zugehörigen MAC-Adresse an, in etwa analog zu ARP

The screenshot shows the 'Diagnostics / Ping' configuration page in pfSense. The page has a title bar 'Diagnostics / Ping' with a red error icon on the right. Below the title bar is a dark header 'Ping'. The main content area contains four configuration fields: 'Hostname' with a text input field containing 'Hostname to ping'; 'IP Protocol' with a dropdown menu set to 'IPv4'; 'Source address' with a dropdown menu set to 'Automatically selected (default)' and a subtext 'Select source address for the ping.'; and 'Maximum number of pings' with a dropdown menu set to '3' and a subtext 'Select the maximum number of pings.'. At the bottom of the form is a blue button with a ping icon and the text 'Ping'.

Mithilfe des Ping-Tools lässt sich die generelle Erreichbarkeit eines Systems mithilfe von ICMP Echo Requests überprüfen.

Die Konfiguration des Test erfolgt durch Angabe der IP-Adresse (IPv4 oder IPv6) oder DNS-Namens und der Anzahl der zu sendenden Pakete (Count).

Mithilfe des Source-Address-Feldes können auch spezielle Tests, z.B. LAN-to-LAN VPN-Konnektivität geprüft werden.



Ein weiteres Tool ist *DNS Lookup*.

Die Angabe einer IP-Adresse liefert den zugehörigen Hostname bzw. die Angabe eines Hostnames die zugehörige IP-Adresse.

Nach Ausführung des Lookups kann auf Knopfdruck ein zugehöriger Alias für den jeweiligen Host erstellt werden, um ihn zukünftig beispielsweise in den Regeln zu verwenden.

The screenshot shows the 'Diagnostics / Packet Capture' configuration page in pfSense. The page is titled 'Packet Capture Options' and contains several sections for configuring the capture process:

- Interface:** A dropdown menu set to 'WAN'. Below it is the instruction: 'Select the interface on which to capture traffic.'
- Promiscuous:** A checkbox labeled 'Enable promiscuous mode' is checked. Below it is the text: '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:** A dropdown menu set to 'Any'. Below it is the instruction: 'Select the type of traffic to be captured.'
- Protocol:** A dropdown menu set to 'Any'. Below it is the instruction: 'Select the protocol to capture, or "Any".'
- Host Address:** An empty text input field. Below it is the text: '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:** An empty text input field. Below it is the text: '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:** A text input field containing '0'. Below it is the text: '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:** A text input field containing '100'. Below it is the text: '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:** A dropdown menu set to 'Normal'. Below it is the text: '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:** A checkbox labeled 'Do reverse DNS lookup' is checked. Below it is the text: 'The packet capture will perform a reverse DNS lookup associated with all IP addresses. This option can cause delays for large packet captures.'

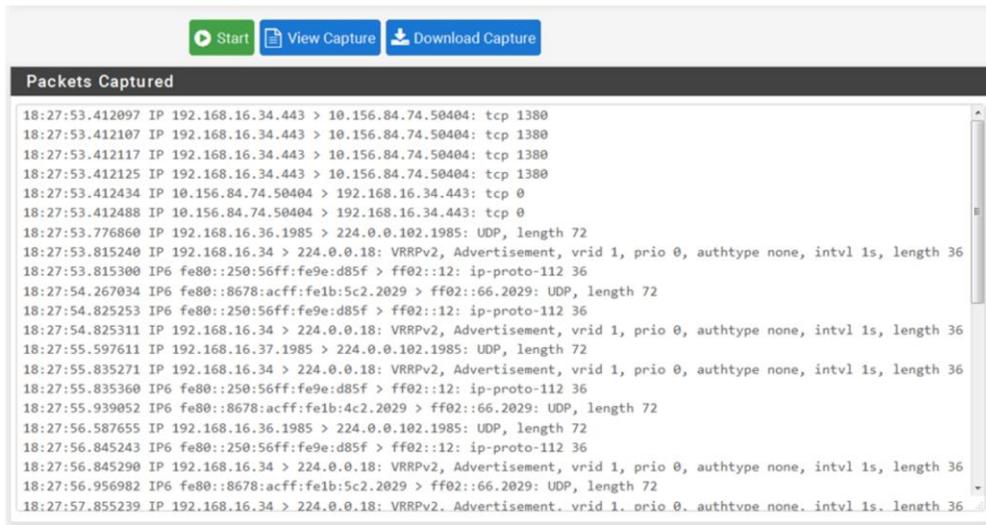
At the bottom of the form, there is a green 'Start' button.

Speziell für erweiterte Diagnose-Zwecke bietet die pfSense auch ein Packet Capture Werkzeug.

Damit lässt sich unter Angabe, an welchem Netz-Interface die Aufzeichnung durchgeführt werden soll, zusätzliches Aktivieren des promiscuous Modes und der Konfiguration von Filtern (Protocol, Host, Port) die Kommunikation auf Paket-Ebene im Detail aufzeichnen.

Daneben gibt es noch Einstellungen für die Länge des aufgezeichneten Pakets, des Loglevels (höherer Detailgrad in der Web-GUI-Anzeige des Captures) bzw. eine automatische Namensauflösung.

Die aufgezeichneten Daten lassen sich direkt in der Web-Oberfläche auswerten (View) bzw. auch für Auswertungen mit tcpdump oder Wireshark im PCAP-Format herunterladen.



Start View Capture Download Capture

Packets Captured

```
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
```

Ein Beispiel für die Ausgabe eines Packet captures. Die Daten werden in folgenden Spalten übersichtlich dargestellt:

1. Zeitpunkt der Aktivität
2. Protokoll
3. Quell-IP
4. Ziel-IP
5. Paketinhalt



## Kontakt

---

Allgemeiner Kontakt und Support:

**LRZ Servicedesk / IT-Sicherheit / Firewalls**

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

Bei Fragen rund um den Dienst „Virtuelle Firewall“ des LRZ wenden Sie sich bitte an unseren Servicedesk.

Unter

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

können Sie Störungen bzw. Service Requests direkt für den Dienst „virtuelle Firewall“ melden und erreichen  
damit auf sehr einfache Weise das richtige Bearbeiter-Team.



# Anhang Features pfSense

### 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...*

### State Table

- Hält Informationen über offene Netzwerkverbindungen
  - Größe der Tabelle anpassbar
  - Regelbasiert
- Begrenzung der Anzahl an Verbindungen,  
Verbindungen pro Sekunde,...

*und weitere...*

## Network Address Translation (NAT)

### High Availability

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



### Server Load Balancing

### Virtual Private Network (VPN)

- IPsec
- OpenVPN
- L2TP

### Reporting und Monitoring

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

### Dynamic DNS Client

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



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