
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

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

Inside	**Outside**
→ zu schützende Netze	→ 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).

Was ist eine Firewall **nicht**?

- Ein <u>vollständiger</u> 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 eingestuften internen (inside) Netz und nicht vertrauenswürdige 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 Deployment 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.

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

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.

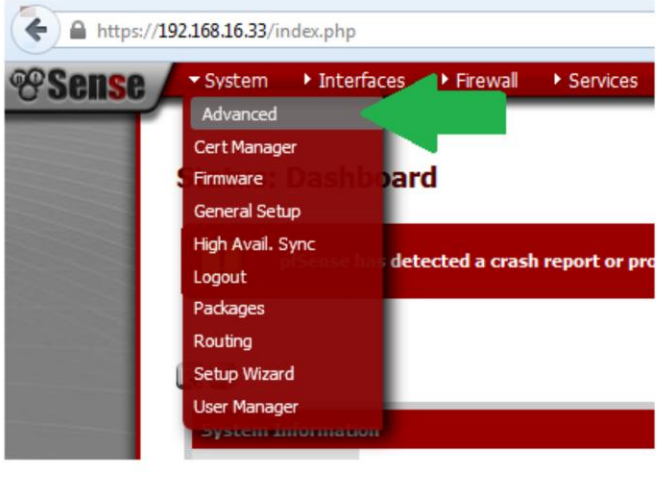
Die Authentifizierung erfolgt mit einer LRZ-SIM-Kennung, so dass das Anlegen und die Pflege lokaler Nutzerkonten entfällt. Das gilt sowohl für die Firewall-Administrator- als auch für die VPN-Zugänge.

Die gruppen-basierte Benutzerverwaltung beruht aus 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.

Konfigurieren des Zugangs

Die Konfiguration des Zugangs erfolgt über den oberen Reiter der Weboberfläche unter

System → Advanced



Hier lassen sich folgende Einstellungen vornehmen:

a) Web-Oberfläche:
   - Zugriff per HTTP oder HTTPS (Verwendung spezieller Ports)
   - Zertifikatsauswahl
   - Anti-Lockout

b) SSH-Zugang:
   - Aktivieren bzw. Deaktivieren des SSH-Zugangs
   - Ändern des Ports
   - Abschalten Passwort-basierter Authentifizierung → Key-basierter Zugriff

Das Dashboard

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

System Information	
Name	pf13.test.lrz.de
Version	**2.2.4-RELEASE** (amd64) built on Sat Jul 25 19:57:37 CDT 2015 FreeBSD 10.1-RELEASE-p15 You are on the latest version.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.20GHz Current: 275 MHz, Max: 2200 MHz 2 CPUs: 2 package(s) x 1 core(s)
Uptime	5 Days 02 Hours 17 Minutes 21 Seconds
Current date/time	Wed Aug 12 17:40:35 CEST 2015
DNS server(s)	127.0.0.1 10.156.33.53 129.187.5.1
Last config change	Fri Aug 7 15:09:16 CEST 2015

Interfaces		
WAN	↑	autoselect
		192.168.16.33
LAN	↑	autoselect
		141.84.42.254 **2001:4ca0:4106::1**

Nach erfolgreicher Anmeldung wird das pfSense-Dashboard angezeigt, das allgemeine Informationen über den aktuellen Status von Hard- und Software bietet.

Das Dashboard

Statistiken und Traffic Graphen (Live) der Netzinterfaces

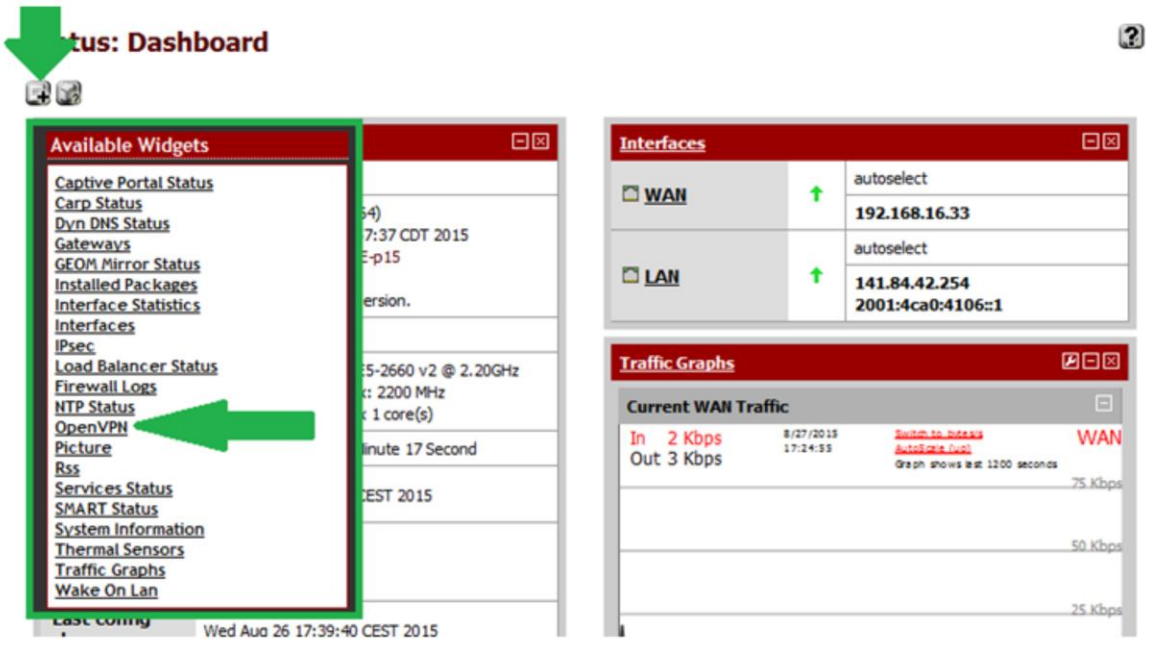
Interface Statistics

	WAN	LAN
Packets In	443650	0
Packets Out	444434	5
Bytes In	34.07 MB	0 bytes
Bytes Out	36.79 MB	448 bytes
Errors In	0	0
Errors Out	0	0
Collisions	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.

Das Dashboard

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

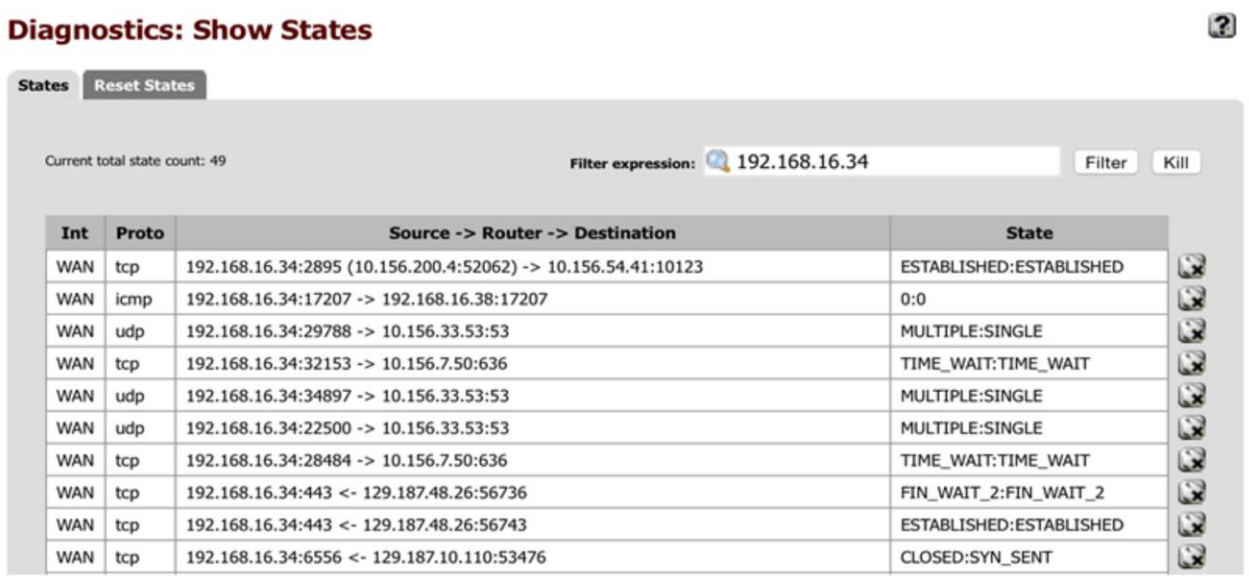


Das Dashboard lässt sich durch Hinzufügen weiterer Widgets individuell anpassen. Auch die Anordnung dieser Widgets ist per Drag-and-Drop beliebig konfigurierbar.

State table

Status aktiver Verbindungen

Diagnostics → States



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, Verbindungs-status, und Kommunikationsrichtung einer Verbindung.

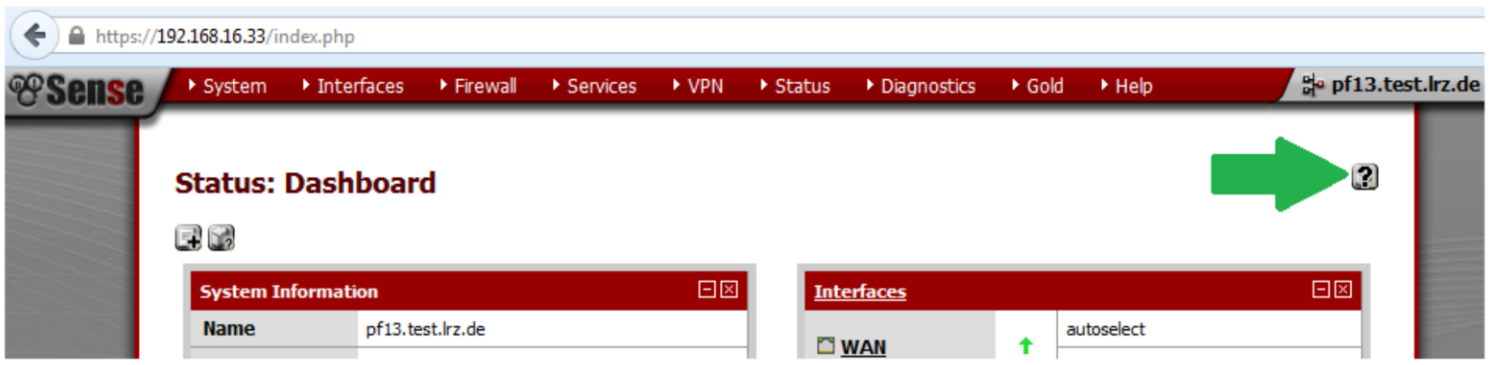
Für jede Verbindung über die Firewall werden zwei States festgehalten:

- 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 angzeigten „x“-Button beenden. Mit dem Tabs Reset States werden alle Verbindungen resetted.

Hilfe auf der pfSense

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



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

Für weitere Informationen bietet pfSense jedoch auch eine ausführliche Dokumentation unter

https://doc.pfsense.org/index.php/Main_Page

Regeln des Paketfilters – Ausgangslage

- Standardregelung:

Inside

any	any	deny

Outside

any	any	deny

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

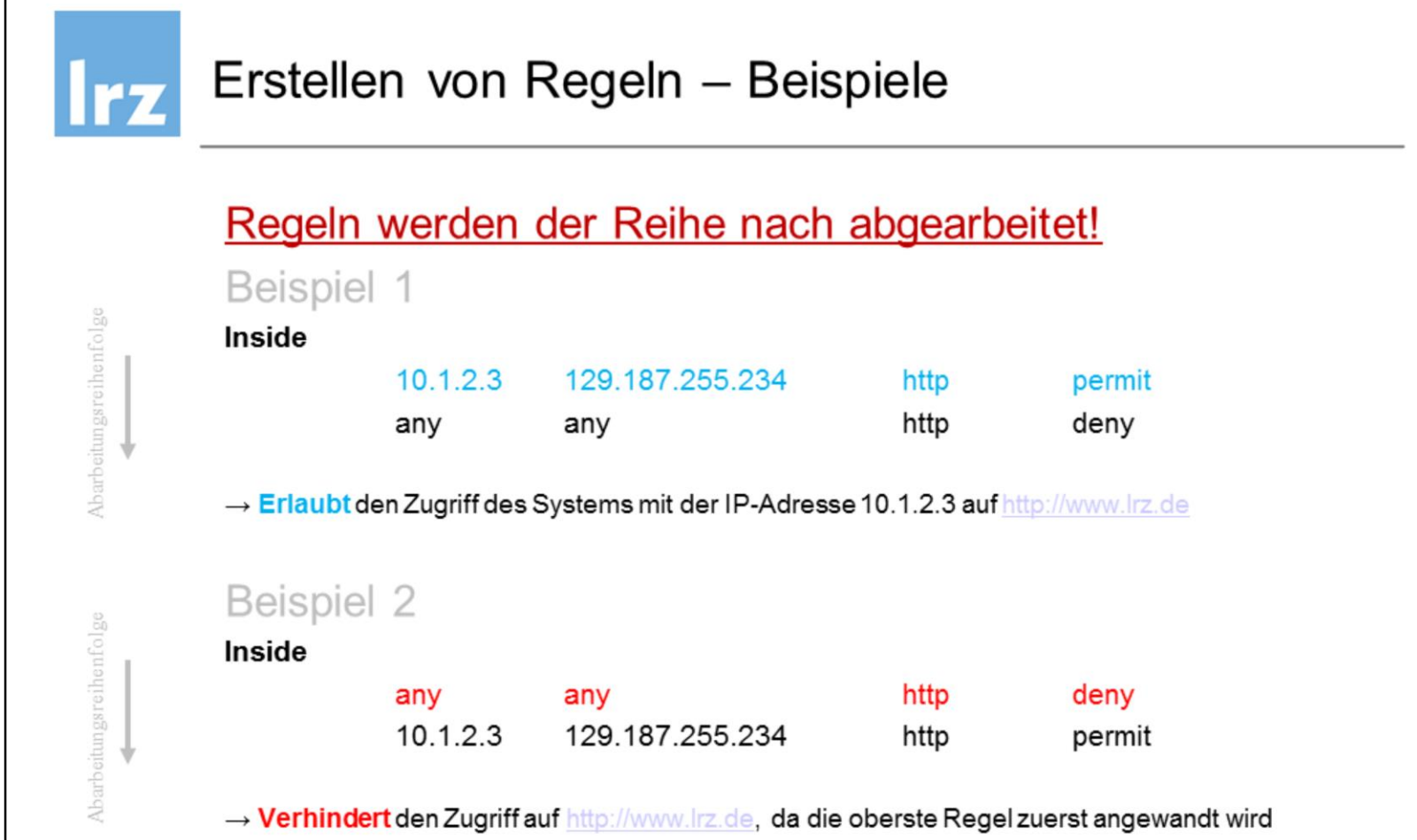
- Der gesamte Verkehr wird geblockt!

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.



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.

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.

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

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.

Aliase

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

Firewall → Aliases

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 iin 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

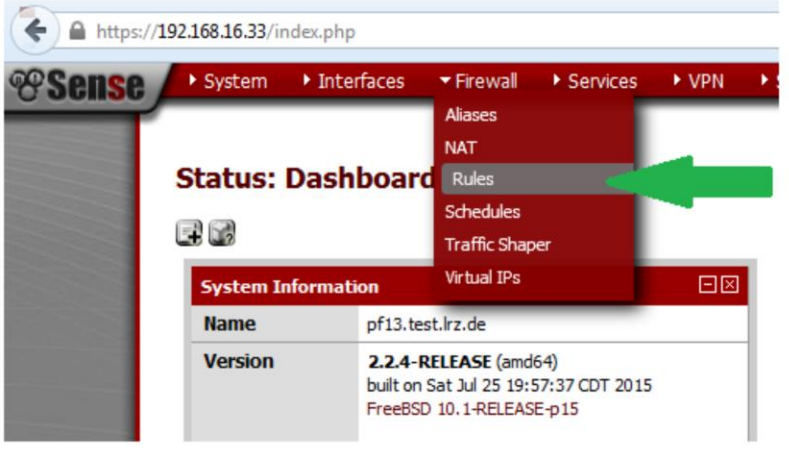
Hier geben die Bezeichner „Home router“ und „Office network“ den Beschreibungstext für das CIDR-Objekt an.

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.

Regeln auf der pfSense

Die Regeln können aufgerufen werden unter

Firewall → Rules



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

Regeln auf der pfSense

Floating | WAN | LAN

	ID	Proto (1)	Source (2)	Port (3)	Destination (4)	Port (5)	Gateway	Queue	Schedule	Description
		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
		IPv4 TCP	129.187.15.0/24	*	192.168.16.0/24	443 (HTTPS)	*	none		
		IPv4 TCP	HTTPS_Management_Clients	*	192.168.16.0/24	443 (HTTPS)	*	none		HTTPs Zugang
		IPv4	129.187.15.0/24	*	192.168.16.0/24	22 (SSH)	*	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-Type (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.

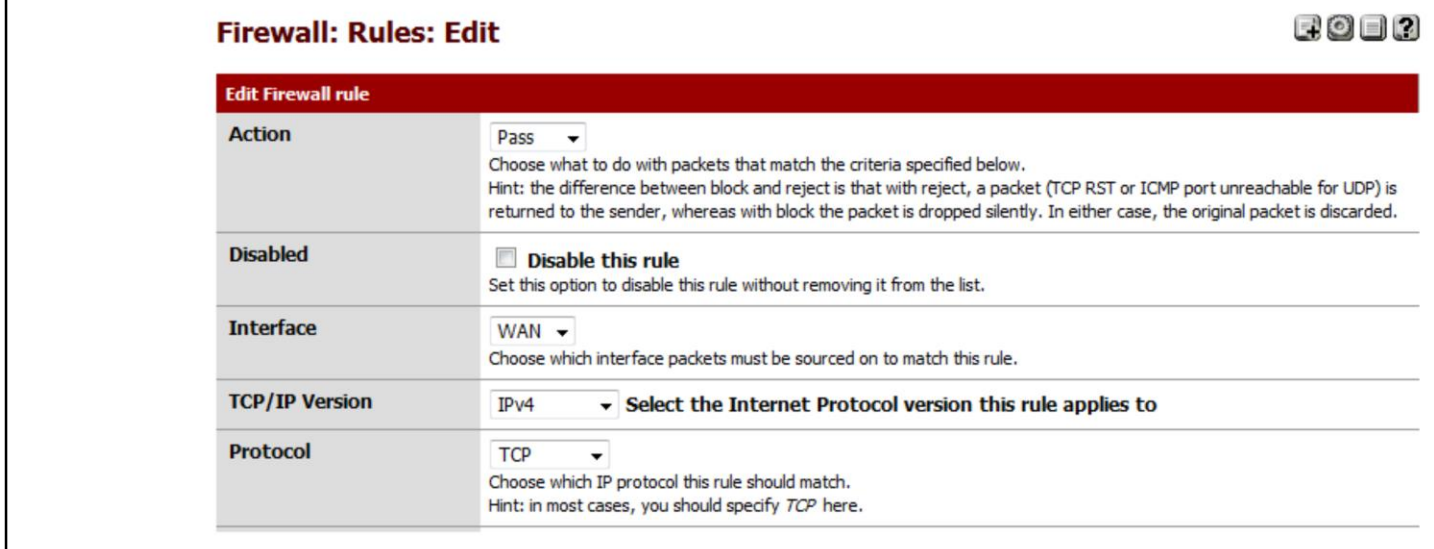
Funktionen zum Regel-Management, z.B. Hinzufügen neuer Regeln, Änderung der Regelreihenfolge oder das Löschen einer selektierten Regel finden sich über die Buttons rechts neben der Tabelle bzw. Regel.

Eine neue Regel hinzufügen

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	
		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
		IPv4 TCP	129.187.15.0/24	*	192.168.16.0/24	443 (HTTPS)	*	none		
		IPv4 TCP	HTTPS_Management_Clients	*	192.168.16.0/24	443 (HTTPS)	*	none		HTTPs Zugang

Das Hinzufügen einer neuen Regel zum Regelwerk erfolgt über den mit „+“ gekennzeichneten Button.
Dies startet den Regel-Editor.

Eine neue Regel hinzufügen – Schritt 1



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.

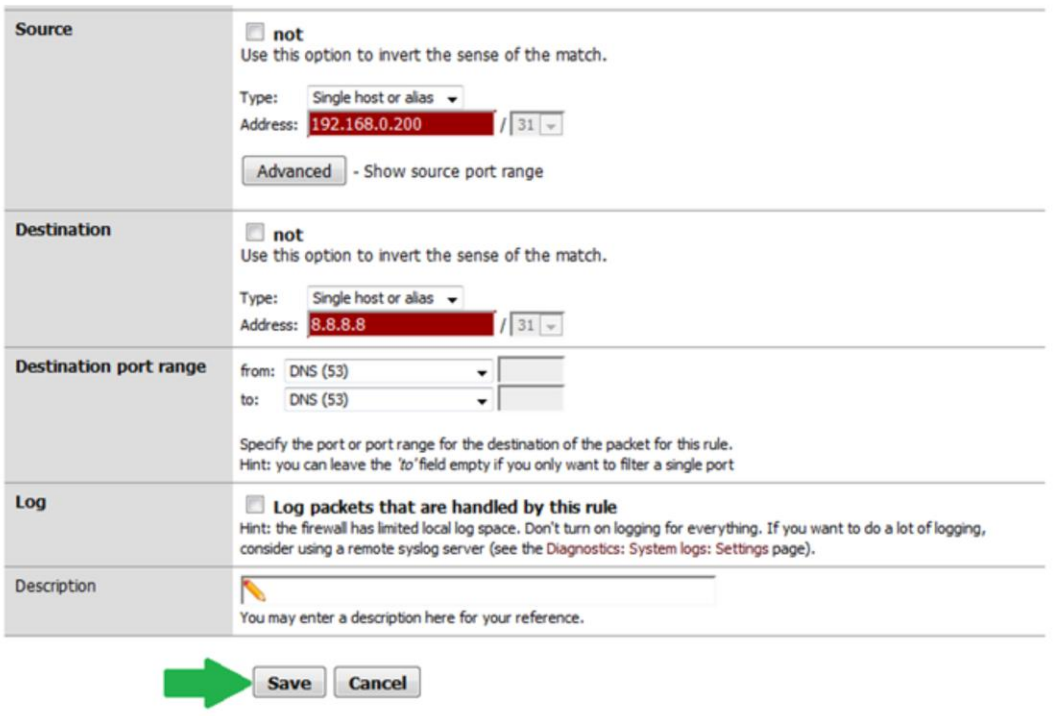
Disabled: Regeln lassen sich explizit disablen, d.h. temporär deaktivieren ohne sie z.B. löschen zu müssen

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

TCP/IP-Version: 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,...)

Eine neue Regel hinzufügen – Schritt 2



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

Durch Aktivieren der Checkbox „not“ lässt sich die Regel sehr einfach invertieren.

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

Durch Aktivieren der Checkbox „not“ 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. zu Debugging-Zwecke, aktiviert werden.

Description: (optionale) Beschreibung der Regel

Eine neue Regel hinzufügen

Neue Regel wird an oberster Stelle angefügt

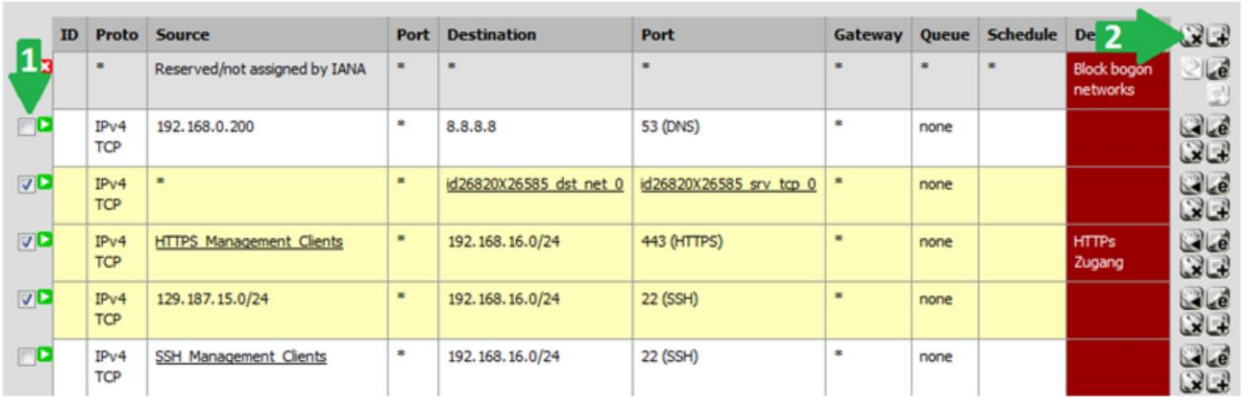
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
		IPv4 TCP	192.168.0.200	*	8.8.8.8	53 (DNS)	*	none		
		IPv4 TCP	129.187.15.0/24	*	192.168.16.0/24	443 (HTTPS)	*	none		
		IPv4 TCP	HTTPS_Management_Clients	*	192.168.16.0/24	443 (HTTPS)	*	none		HTTPs Zugang
		IPv4 TCP	129.187.15.0/24	*	192.168.16.0/24	22 (SSH)	*	none		

Am unteren Ende der Liste ist ein Button zum Hinzufügen einer Regel am **unteren** Ende der Liste!

Neue Regeln lassen sich an verschiedenen Stellen im Regelwerk hinzufügen, abhängig davon welchen mit „+“ gekennzeichneten Button man anklickt.

Regeln lassen sich auch „auf Basis“ einer bereits bestehenden Regel erstellen. Dazu wählt man den mit „+“ gekennzeichneten Button rechts neben der zu kopierenden Regel.

Auswahl und Bearbeitung mehrerer Einträge



1. Checkboxen zur Mehrfachauswahl von Einträgen

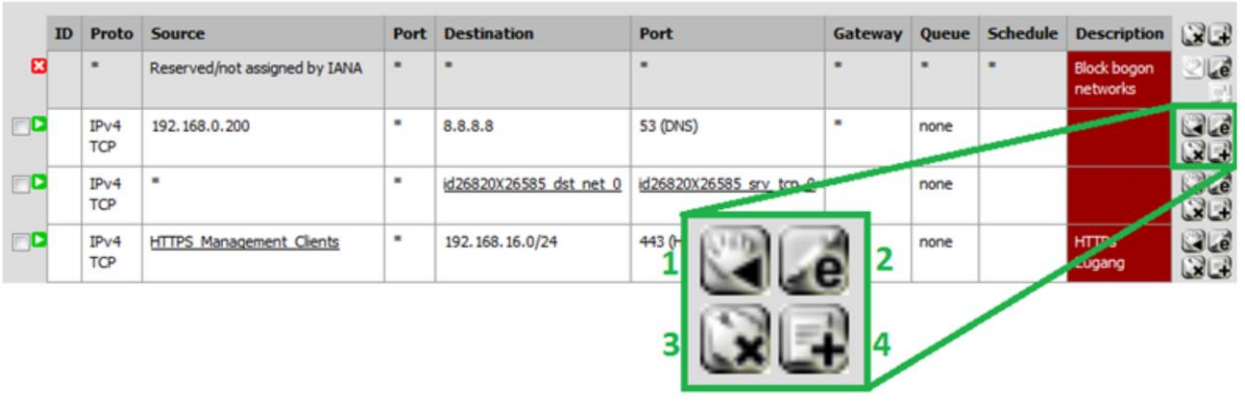
2. Löschen ausgewählter Einträge

Für die Bearbeitung des Regelwerks stehen verschiedene Funktionen zu Verfügung:

- Checkboxen für Mehrfachauswahl, z.B. um mehrere Regeln im Regelwerk zu verschieben oder auf einmal zu löschen.

- Hinzufügen einer neuen Regel am „oberen“ Ende des bestehenden Regelwerks

Auswahl und Bearbeitung mehrerer Einträge



1. Ausgewählte Einträge vor diese Zeile einfügen (vgl. Vorgängerfolie)
   → Änderung der Bearbeitungsreihenfolge
2. Editieren einer Regel
3. Löschen einer Regel
4. Erstellen einer neuen Regel auf Basis der ausgewählten Regel

Für die Bearbeitung des Regelwerks stehen verschiedene Funktionen zu Verfügung:

- Hinzufügen einer neuen Regel („+“ Button)

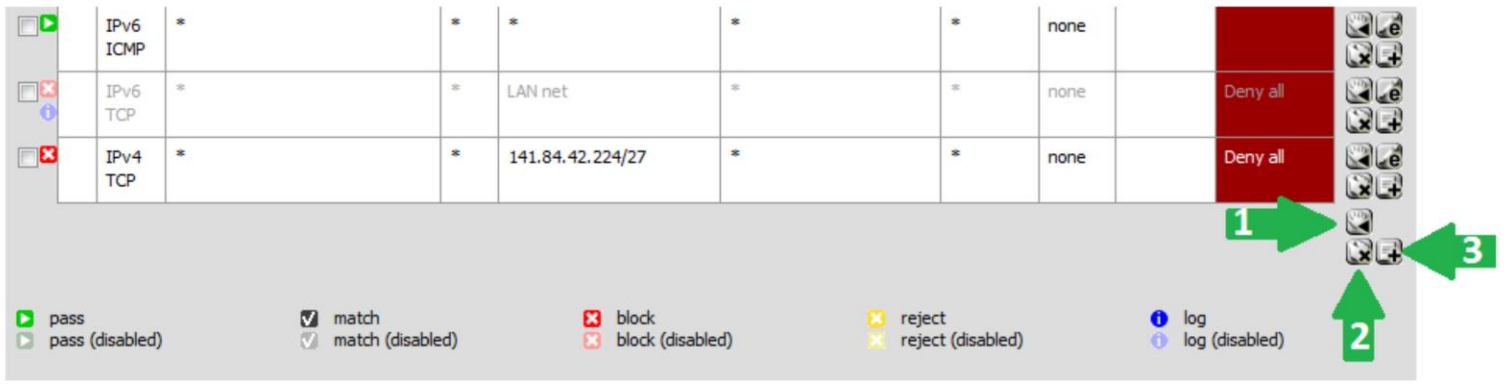
- Bearbeiten einer Regel mithilfe des Regel-Editors („e“ Button)

- Löschen einer Regel („x“ Button)

- Erstellen einer neuen Regel auf Basis der ausgewählten Regel („Klonen“) und öffnen des Regeleditors

Auswahl und Bearbeitung mehrerer Einträge

Unteres Ende der Liste:



1. Ausgewählte Regel am unteren Ende einfügen
2. Ausgewählte Regeln löschen
3. Neue Regel erstellen und am unteren Ende einfügen

Für die Bearbeitung des Regelwerks stehen verschiedene Funktionen zu Verfügung:

- Hinzufügen einer neuen Regel am „unteren“ Ende des bestehenden Regelwerks

- Ausgewählte Regel ans untere Ende des Regelwerks verschieben

- Ausgewählte Regeln löschen

Aktivierung und Deaktivierung einzelner Regeln

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
		TCP	192.168.0.200	*	8.8.8.8	53 (DNS)	*	none		
		IPv4 TCP	*	*	id26820X26585_dst_net_0	id26820X26585_srv_tcp_0	*	none		

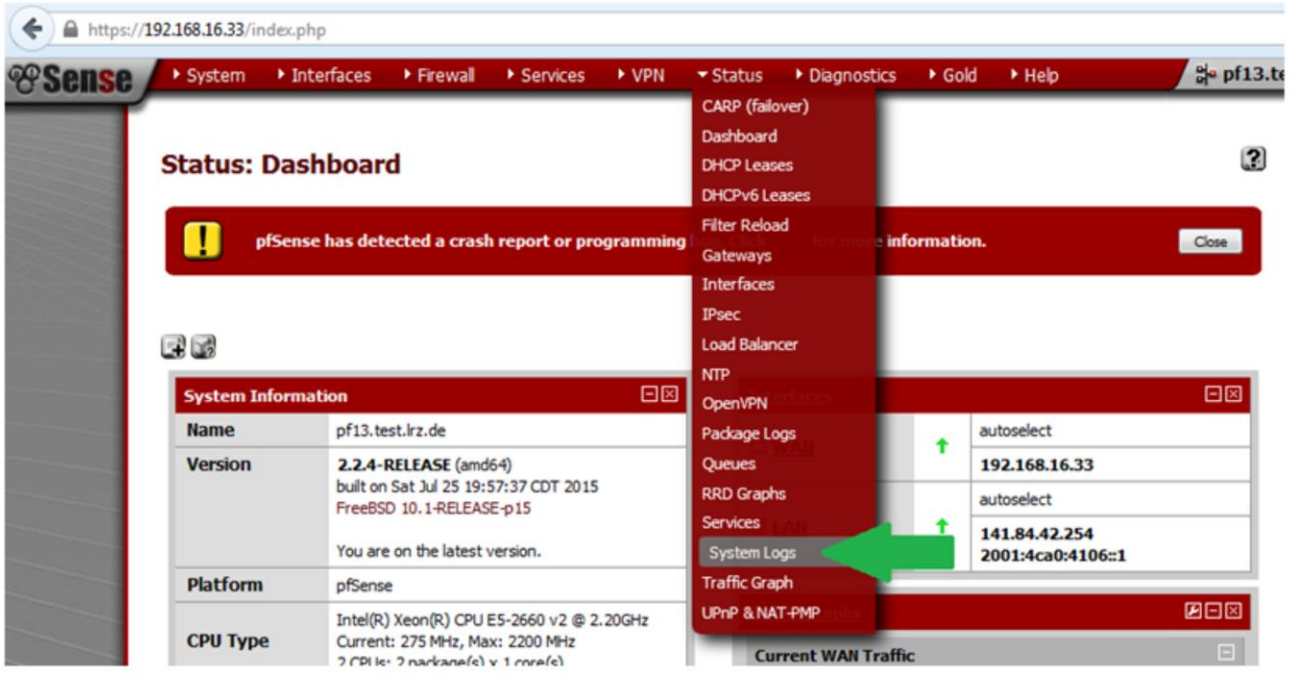
linke Maus

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
		IPv4 TCP	192.168.0.200	*	8.8.8.8	53 (DNS)	*	none		
		IPv4 TCP	*	*	id26820X26585_dst_net_0	id26820X26585_srv_tcp_0	*	none		

- Aktivierung von Regeln ist analog möglich

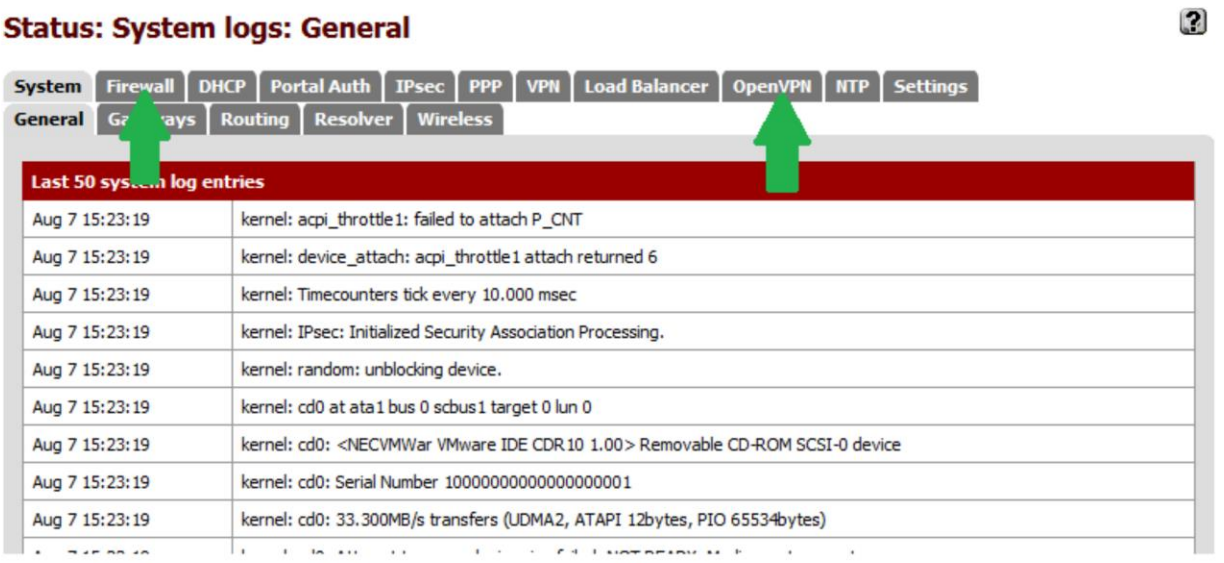
Einzelne Regeln lassen sich auch in der tabellarischen Übersicht aktiveren bzw. deaktivieren.

System Logs



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

System Logs



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.

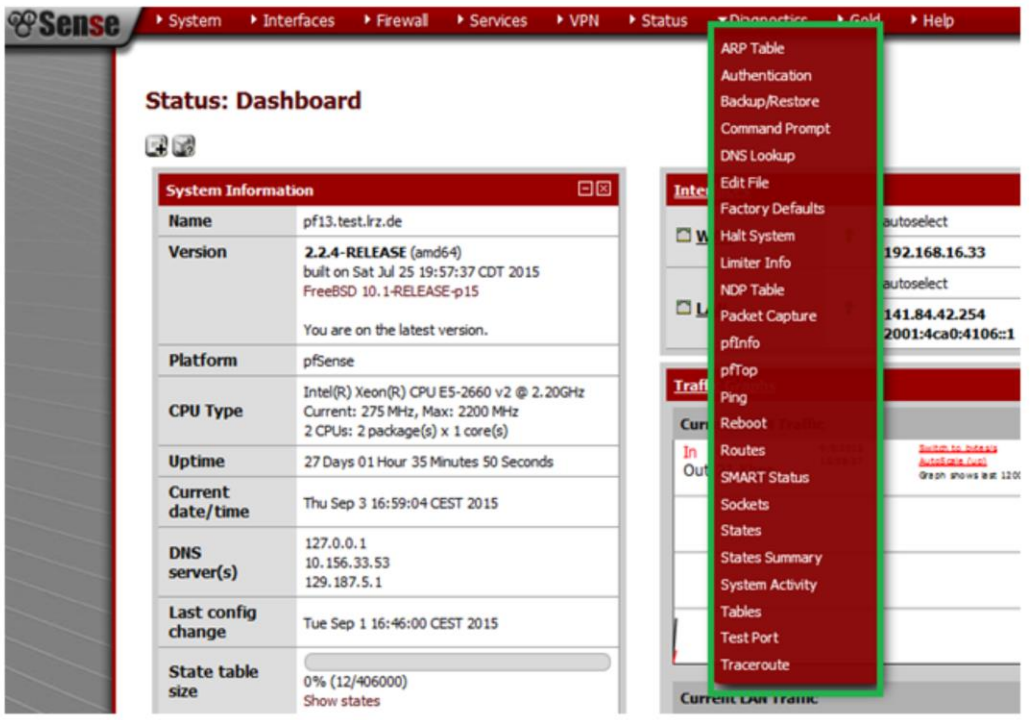
Desweitern kann hier ein „Remote Logging“ beispielsweise an einen bereits vorhandenen, zentralen Syslog-Server konfiguriert werden:

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.

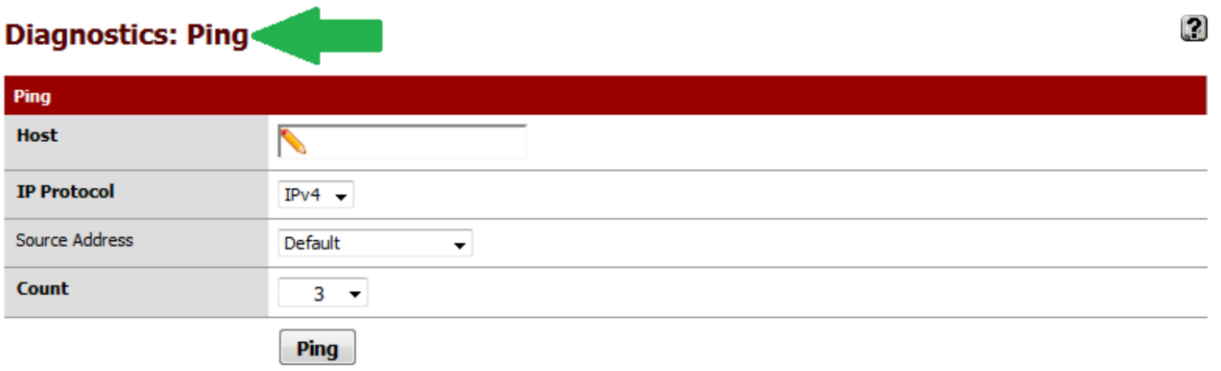
Diagnosetools auf der pfSense



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*.

Diagnosetools auf der pfSense

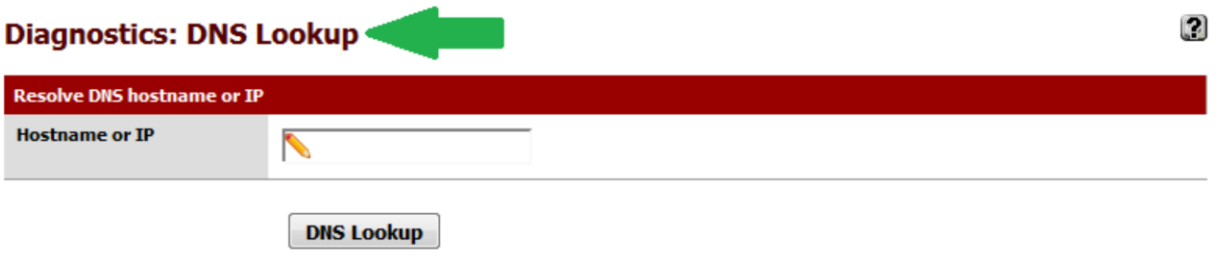


Mithilfe des Ping-Tools lässt sich die generelle Erreichbarkeit eines Systems mithilfe von ICMP Echo Requests überprüfen.

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

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

Diagnosetools auf der pfSense

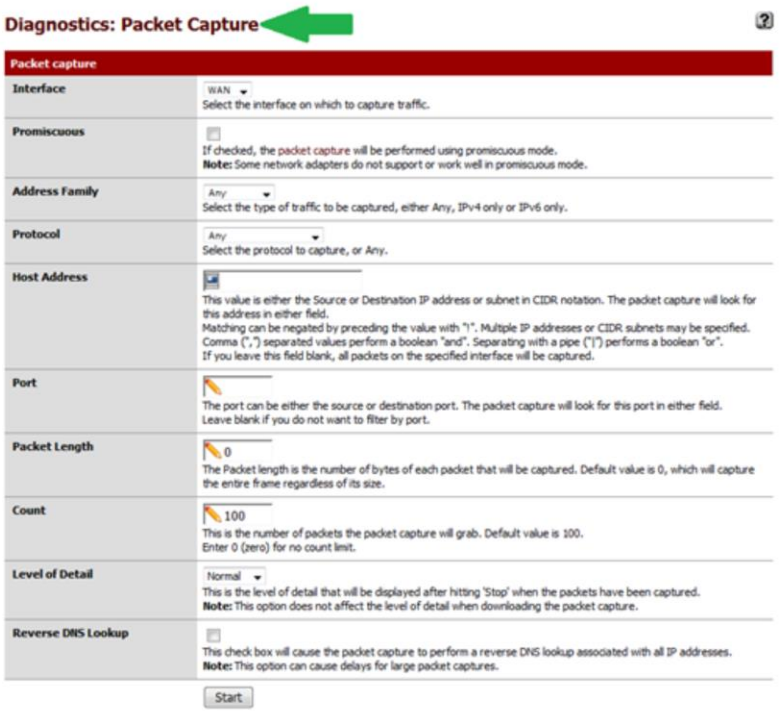


Ein weiteres Tool ist *DNS Lookup*.

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.

Diagnosetools auf der pfSense



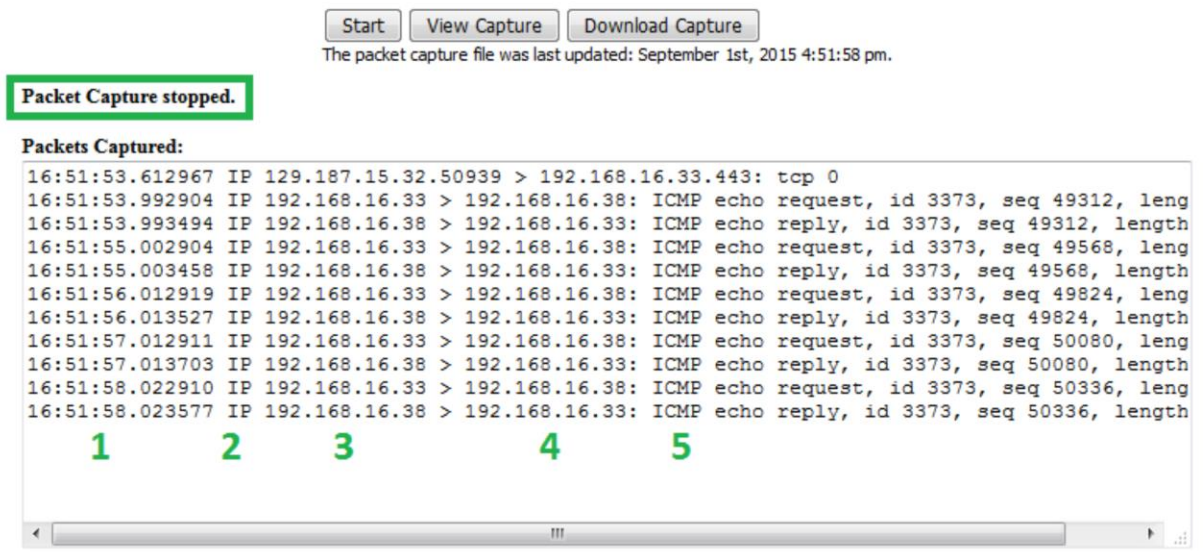
Speziell für erweiterte Diagnose-Zwecke bietet die pfSense auch eine Packet Capture Werkzeug.

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 downloaden.

Diagnosetools auf der pfSense



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

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

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
- PPTP Server

pfSense – genereller Funktionsumfang

Reporting und Monitoring

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

pfSense – genereller Funktionsumfang

Dynamic DNS

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

pfSense – genereller Funktionsumfang

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