

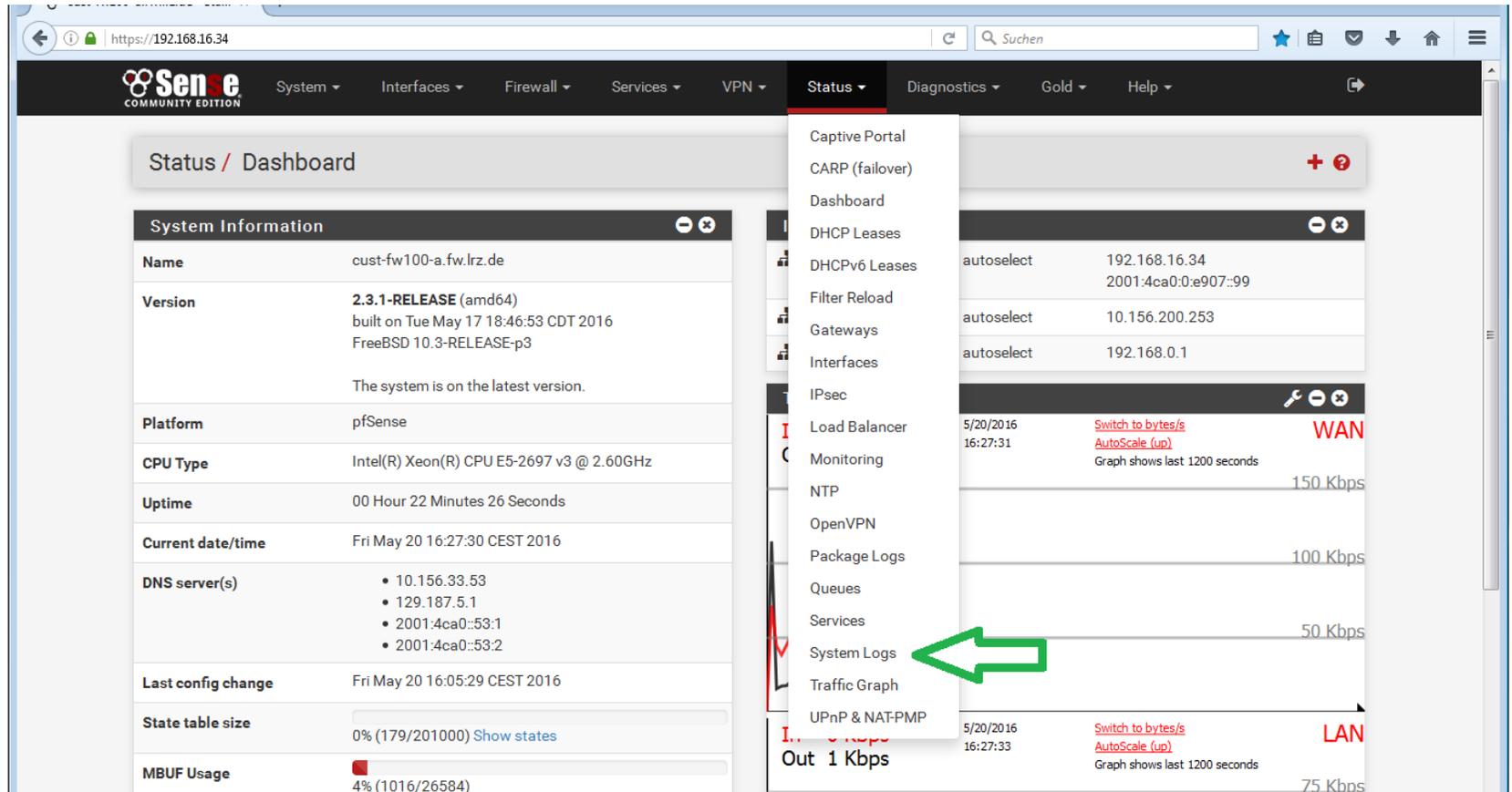


Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften



pfSense – Virtuelle Firewalls am
Leibniz-Rechenzentrum

- Es wird davon ausgegangen, dass die generelle Bedienung der pfsense bekannt ist
- Logging und Log-Auswertung
 - Einrichten eines Syslog-Servers
- Installation von Zusatzpaketen
- OpenVPN-Konfiguration (mit Hands-On)



The screenshot shows the pfSense Status Dashboard. The 'Status' menu is open, and 'System Logs' is highlighted with a green arrow. The dashboard includes a 'System Information' panel and several monitoring graphs.

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
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)	<ul style="list-style-type: none">10.156.33.53129.187.5.12001:4ca0::53:12001:4ca0::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)

System Logs

5/20/2016 16:27:31	Switch to bytes/s AutoScale (up)	WAN
Graph shows last 1200 seconds		
150 Kbps		
100 Kbps		
50 Kbps		
Out 1 Kbps		
5/20/2016 16:27:33	Switch to bytes/s AutoScale (up)	LAN
Graph shows last 1200 seconds		
75 Kbps		

https://192.168.16.34/status_logs.php

Sense COMMUNITY EDITION

System / System Logs / System / General

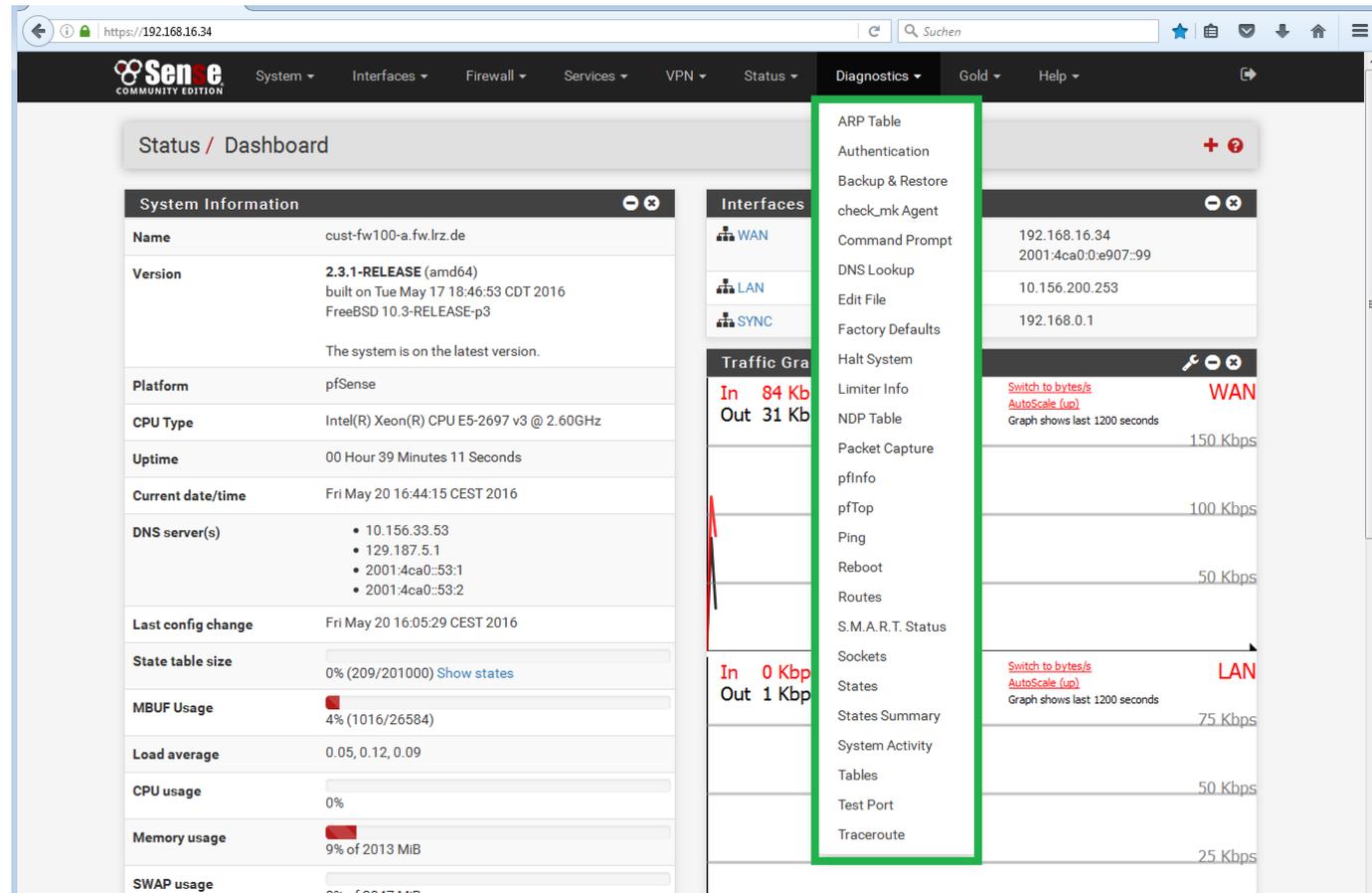
System Firewall DHCP Captive Portal Auth IPsec PPP VPN Load Balancer **OpenVPN** NTP Settings

General **System** Routing DNS Resolver Wireless

Last 50 General 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



The screenshot shows the pfSense web interface. The top navigation bar includes: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "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 39 Minutes 11 Seconds
Current date/time	Fri May 20 16:44:15 CEST 2016
DNS server(s)	<ul style="list-style-type: none"> • 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
- LAN
- SYNC

Traffic Graphs

- WAN: In 84 Kb, Out 31 Kb
- LAN: In 0 Kbp, Out 1 Kbp

Diagnostics Menu (highlighted in green):

- ARP Table
- Authentication
- Backup & Restore
- check_mk Agent
- Command Prompt
- DNS Lookup
- Edit File
- Factory Defaults
- Halt System
- Limiter Info
- NDP Table
- Packet Capture
- pfinfo
- pfTop
- Ping
- Reboot
- Routes
- S.M.A.R.T. Status
- Sockets
- States
- States Summary
- System Activity
- Tables
- Test Port
- Traceroute

Einrichten des Rsyslog-Daemons

- apt-get install rsyslog
- Vi /etc/rsyslog.conf
- Entsprechende Zeilen hinzufügen
 - Je nach Konfiguration die Dateien in eine eigene Datei umleiten.

```
udp,76,172.16.189.101,85.254.217.235,123,123,56
Sep 28 17:36:19 pfsense filterlog: 80,16777216,,1463497428,em1,match,pass,in,4,0xc0,,64,31170,0,DF,
7,udp,76,172.16.189.101,176.9.1.211,123,123,56
Sep 28 17:36:26 pfsense filterlog: 80,16777216,,1463497428,em1,match,pass,in,4,0xc0,,64,15747,0,DF,
7,udp,76,172.16.189.101,149.210.142.45,123,123,56
Sep 28 17:37:19 pfsense filterlog: 80,16777216,,1463497428,em1,match,pass,in,4,0xc0,,64,64580,0,DF,
7,udp,76,172.16.189.101,217.91.44.17,123,123,56
Sep 28 17:37:22 pfsense filterlog: 80,16777216,,1463497428,em1,match,pass,in,4,0xc0,,64,16638,0,DF,
7,udp,76,172.16.189.101,85.254.217.235,123,123,56
Sep 28 17:37:27 pfsense filterlog: 80,16777216,,1463497428,em1,match,pass,in,4,0xc0,,64,47791,0,DF,
7,udp,76,172.16.189.101,176.9.1.211,123,123,56
Sep 28 17:37:32 pfsense filterlog: 80,16777216,,1463497428,em1,match,pass,in,4,0xc0,,64,23288,0,DF,
7,udp,76,172.16.189.101,149.210.142.45,123,123,56
```



Fragen

- Pfsense: tcp-Syslog
- <https://securityonion.net/>

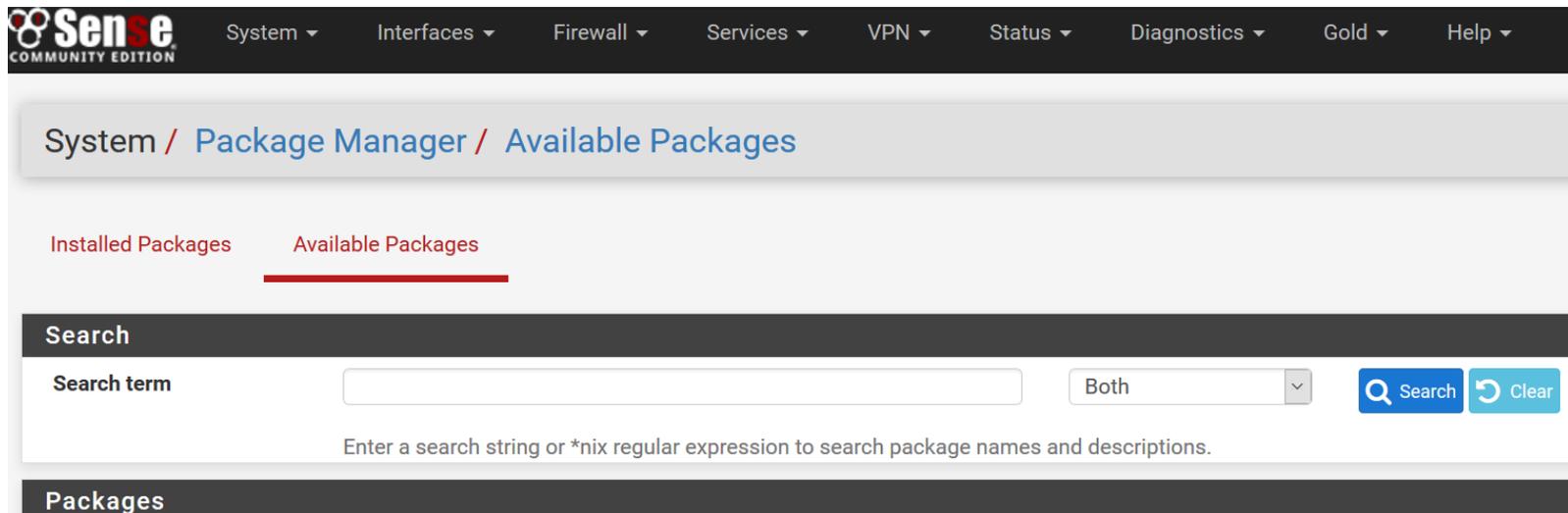
- Für die Auswertung der syslog-Daten kann man die folgenden Tools verwenden:
 - Graylog (<https://www.graylog.org/>)
 - Logcheck
 - Logwatch
 - Logstash

Das LRZ empfiehlt auf ELK basierendes Logstah. Damit können die Daten anschaulich grafisch dargestellt werden.

- Pakete können mittels [System > Packet Manager] installiert werden. Das LRZ bietet zur Zeit keinen weitergehenden Support für Pakete an. Voll supported wird: Open-VM-Tools, sudo, openvpn-client-export
- Vorteil der Pakete:
 - Updateprozess ist vereinfacht; Pakete werden beim Update wieder eingespielt
 - Im Regelfall einfach via Oberfläche zu bedienen
 - Einfache Updates zwischen verschiedenen Paketen

Beispiel: Avahi-Paket

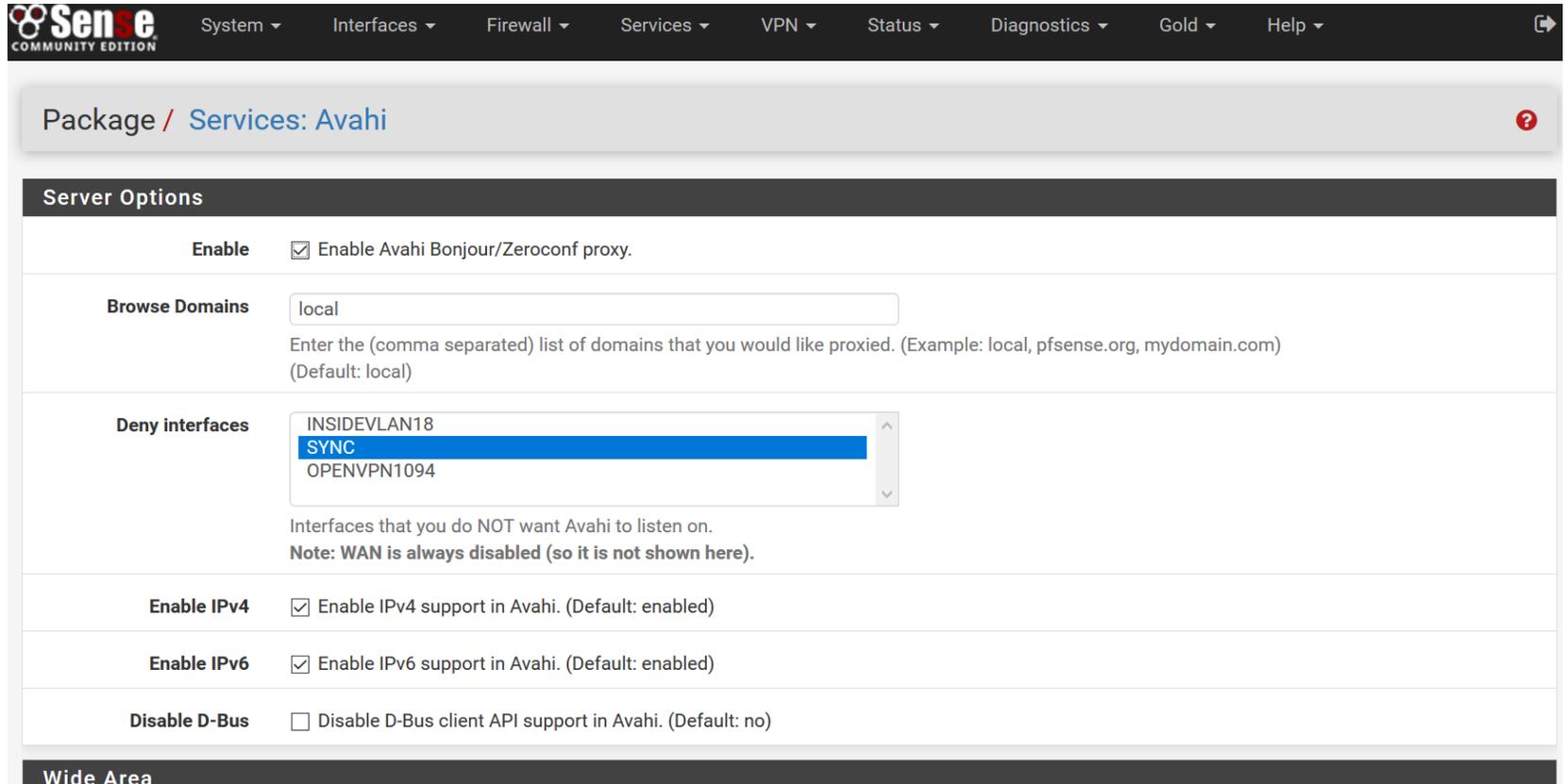
- Erlaubt mDNS



The screenshot shows the Sense Community Edition web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "System / Package Manager / Available Packages". Below this, there are two tabs: "Installed Packages" and "Available Packages", with the latter being selected. A search bar is present with a "Search term" input field, a dropdown menu set to "Both", and "Search" and "Clear" buttons. Below the search bar, there is a prompt: "Enter a search string or *nix regular expression to search package names and descriptions." The bottom of the screenshot shows the "Packages" section header.

Dort das Avahi-Paket auswählen und installieren.
Nach der Installation ist die Konfiguration unter
Services > Avahi möglich

Konfiguration von Avahi



Package / Services: Avahi

Server Options

Enable Enable Avahi Bonjour/Zeroconf proxy.

Browse Domains
 Enter the (comma separated) list of domains that you would like proxied. (Example: local, pfsense.org, mydomain.com)
 (Default: local)

Deny interfaces
 Interfaces that you do NOT want Avahi to listen on.
Note: WAN is always disabled (so it is not shown here).

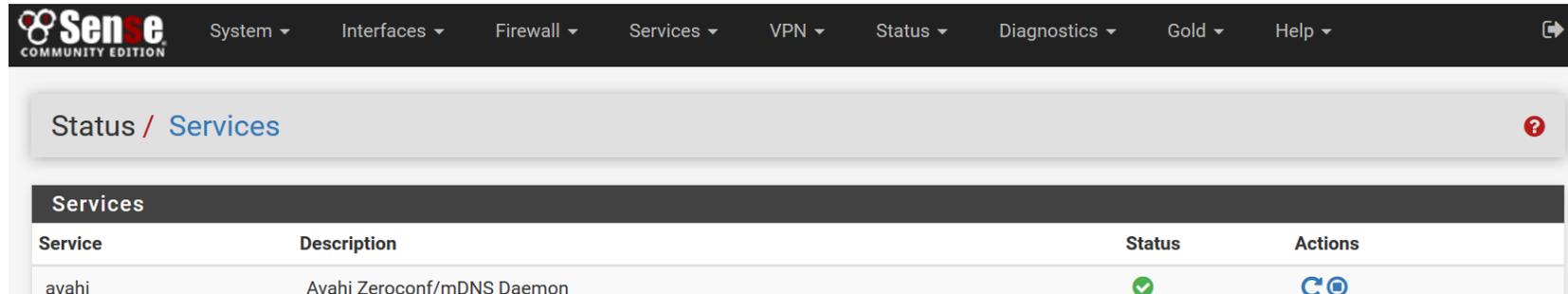
Enable IPv4 Enable IPv4 support in Avahi. (Default: enabled)

Enable IPv6 Enable IPv6 support in Avahi. (Default: enabled)

Disable D-Bus Disable D-Bus client API support in Avahi. (Default: no)

Wide Area

Statusinformationen: Status > Services



The screenshot shows the Sense Community Edition web interface. The top navigation bar includes: Sense COMMUNITY EDITION, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The breadcrumb trail is Status / Services. Below the breadcrumb is a table titled "Services".

Service	Description	Status	Actions
avahi	Avahi Zeroconf/mDNS Daemon	✓	↻

Wenn es sich um einen Dienst handelt, kann der Status des Dienstes unter Status > Services abgefragt werden

- Wenn ein Dienst nicht startet, findet man dies in der Regel unter System Status heraus; genauere Informationen befinden sich aber in der Regel in System > System Logs > System > General, oder aber auf dem Syslog –Server ;-)
- Leider sind die Informationen zum Teil nicht sehr aussagekräftig. Hier hilft in der Regel google oder das pfsense-Forum weiter

- Erfolgt wie die Installation, jedoch den Mülleimer anklicken
- Achtung: manche Pakete hinterlassen Reste auf dem System (z.B. Datendateien/Logdateien, die u.U. nicht deinstalliert werden.
 - Hier ist manchmal eine manuelle Intervention mittels SSH notwendig.

- Ist auf der pfsense integriert (eigenständiges Projekt siehe:

<https://openvpn.net/>



- Wird regelmäßig von unabhängigen Quellen untersucht: <https://ostif.org/the-openvpn-2-4-0-audit-by-ostif-and-quarkslab-results/>
- Kritische Updates fließen zeitnah in pfsense-Releases ein.
- Vom LRZ als VPN-Lösung unterstützt und supportet.

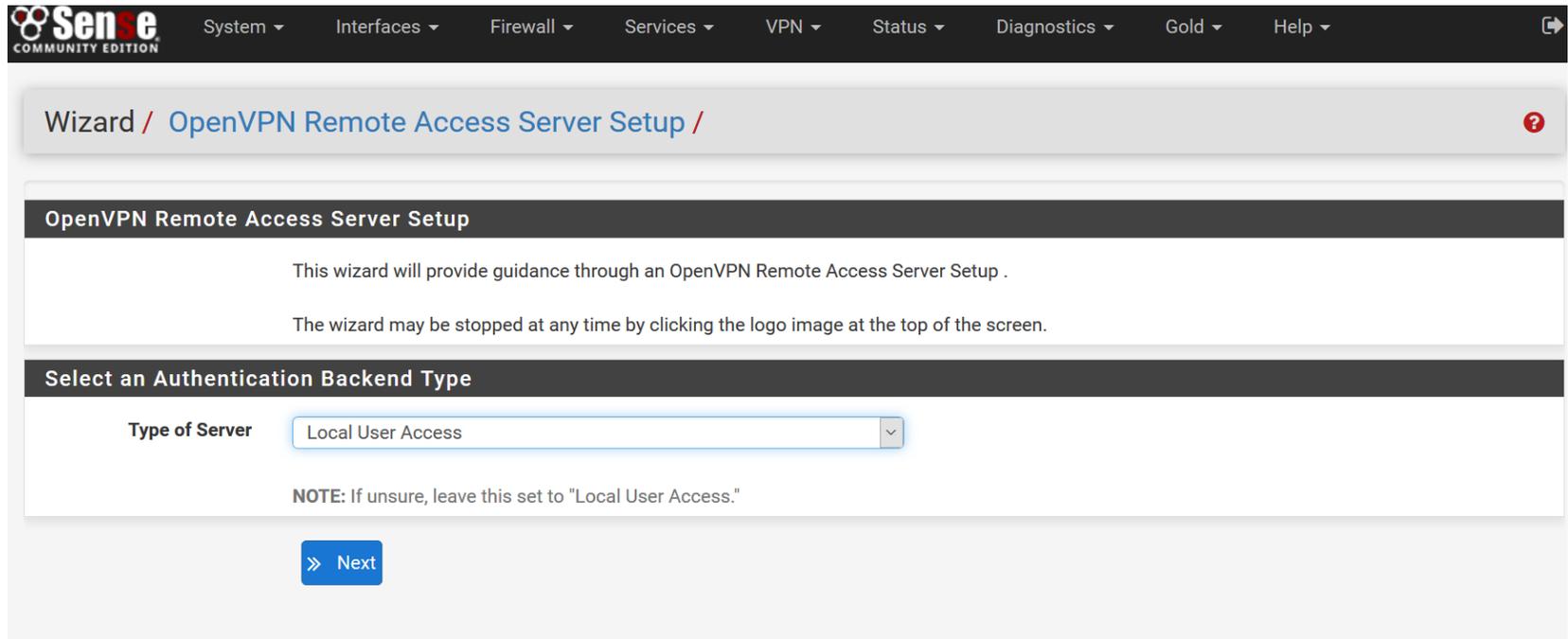
- Es gibt verschiedene Konzepte ein VPN zu realisieren, der vom LRZ empfohlene Weg ist: eine eigenes geroutetes Netz zu nehmen (hierbei gibt es zwei Varianten: ein komplett nicht geroutetes Netz (z.B. 10.0.1.0/24) oder ein vom LRZ vergebenes privates Netz (z.B. 10.152.xx.xx)).
- Vorteil eines gerouteten Netzes ist, dass Verkehr zu sämtlichen innenliegenden Netzen mittels Regeln reglementiert werden kann, wen ein Bridge-Adapter verwendet wird, ist dies nicht möglich.
- Bridging ist möglich, wird aber nicht empfohlen

Was braucht man für VPN ?

- Eine öffentliche IP (sofern das VPN weltweit erreichbar sein soll), in unserem Hands-on nur eine lokale; per Service-Request an den Service-Desk
- Eine Authentifizierungs-Quelle: LDAP, Active-Directory, Local, Radius-Server oder andere
- CA für Zertifikate
- Einen OpenVPN-Server (mit eigenem Zertifikat)
- Client-Konfiguration und Client OpenVPN

- Auch möglich: VPN mit Zertifikaten für jeden Benutzer (dazu wäre aber ein Radius-Server anzuraten); Verteilung der Zertifikate skaliert momentan nicht so gut

Einrichten von VPN mittels des OpenVPN Wizards



The screenshot shows the web interface of Sense Community Edition. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The breadcrumb trail indicates the current page is 'Wizard / OpenVPN Remote Access Server Setup'. The main content area is titled 'OpenVPN Remote Access Server Setup' and contains the following text:

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

Type of Server:

NOTE: If unsure, leave this set to "Local User Access."

[» Next](#)

Authentication-Server ist hier erforderlich



Jede Menge weiterer Einstellung



Kontakt

Allgemeiner Kontakt und Support:

LRZ Servicedesk / IT-Sicherheit / Firewalls

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



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>