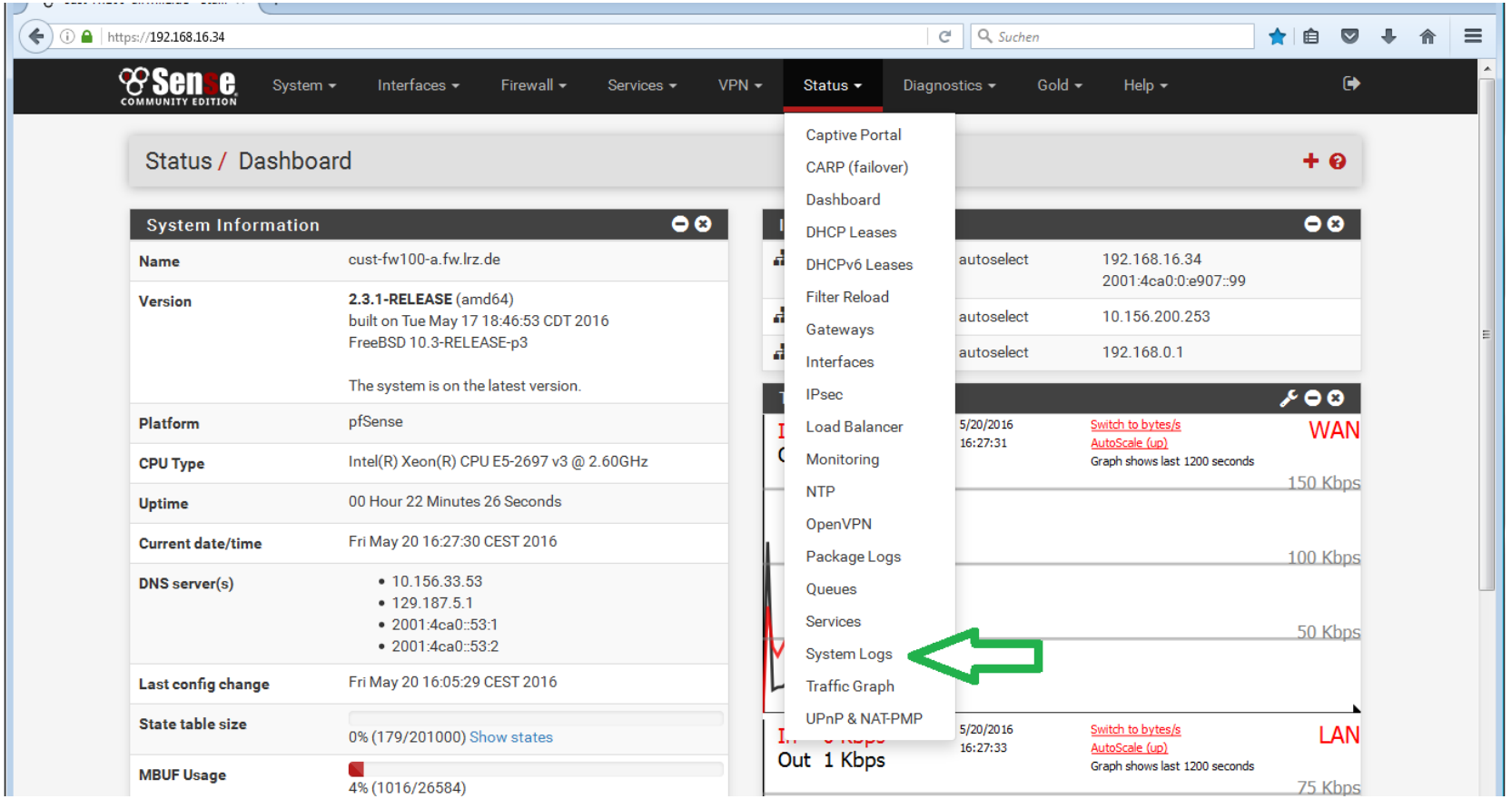
pfSense – Virtuelle Firewalls am Leibniz-Rechenzentrum

Inhalte

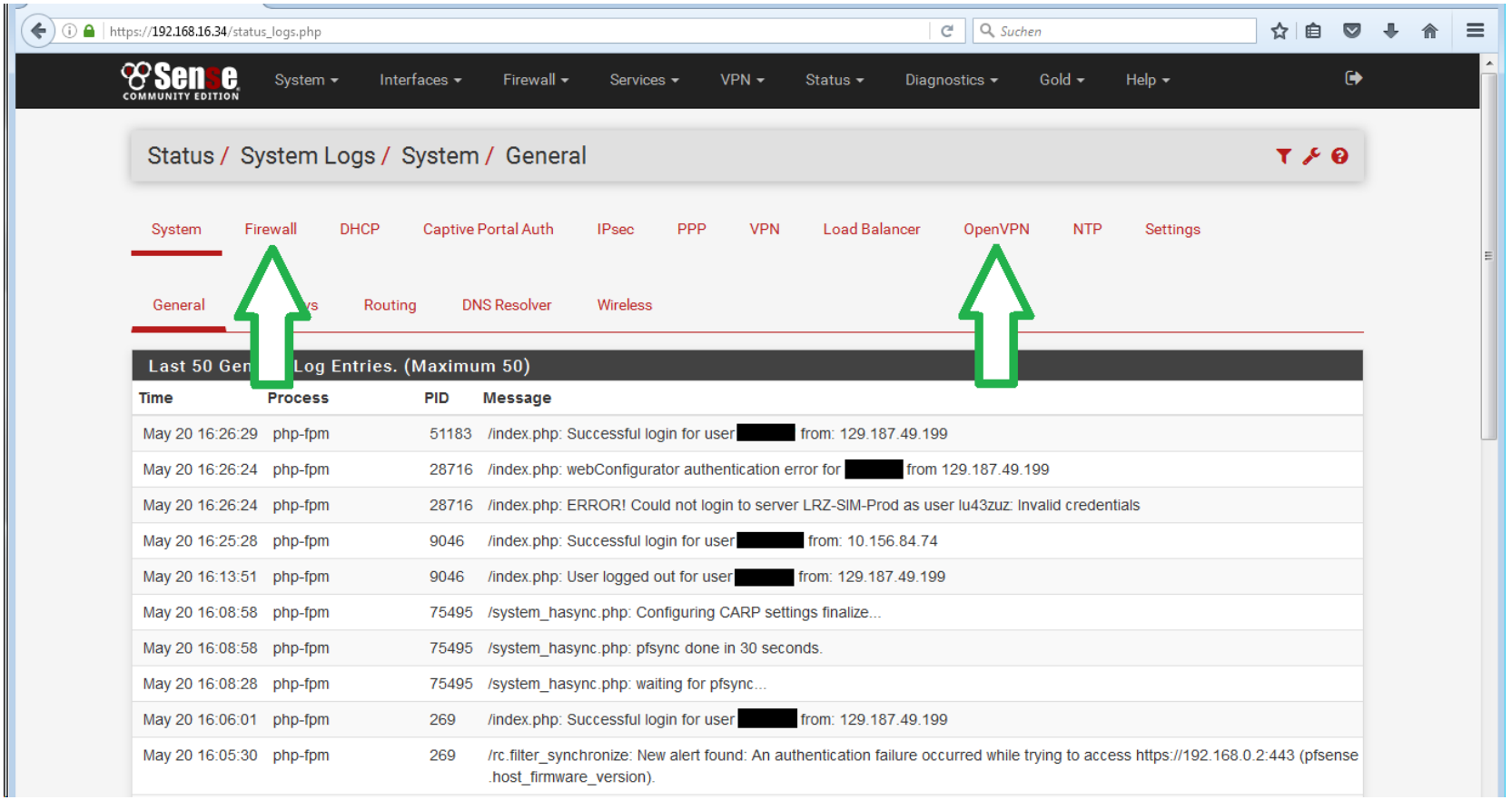
- Es wird davon ausgegangen, dass die generelle Bedienung der pfsense bekannt ist

- Logging und Log-Auswertung
  - Einrichten eines Syslog-Servers
- Installation von Zusatzpaketen
- OpenVPN-Konfiguration (mit Hands-On)

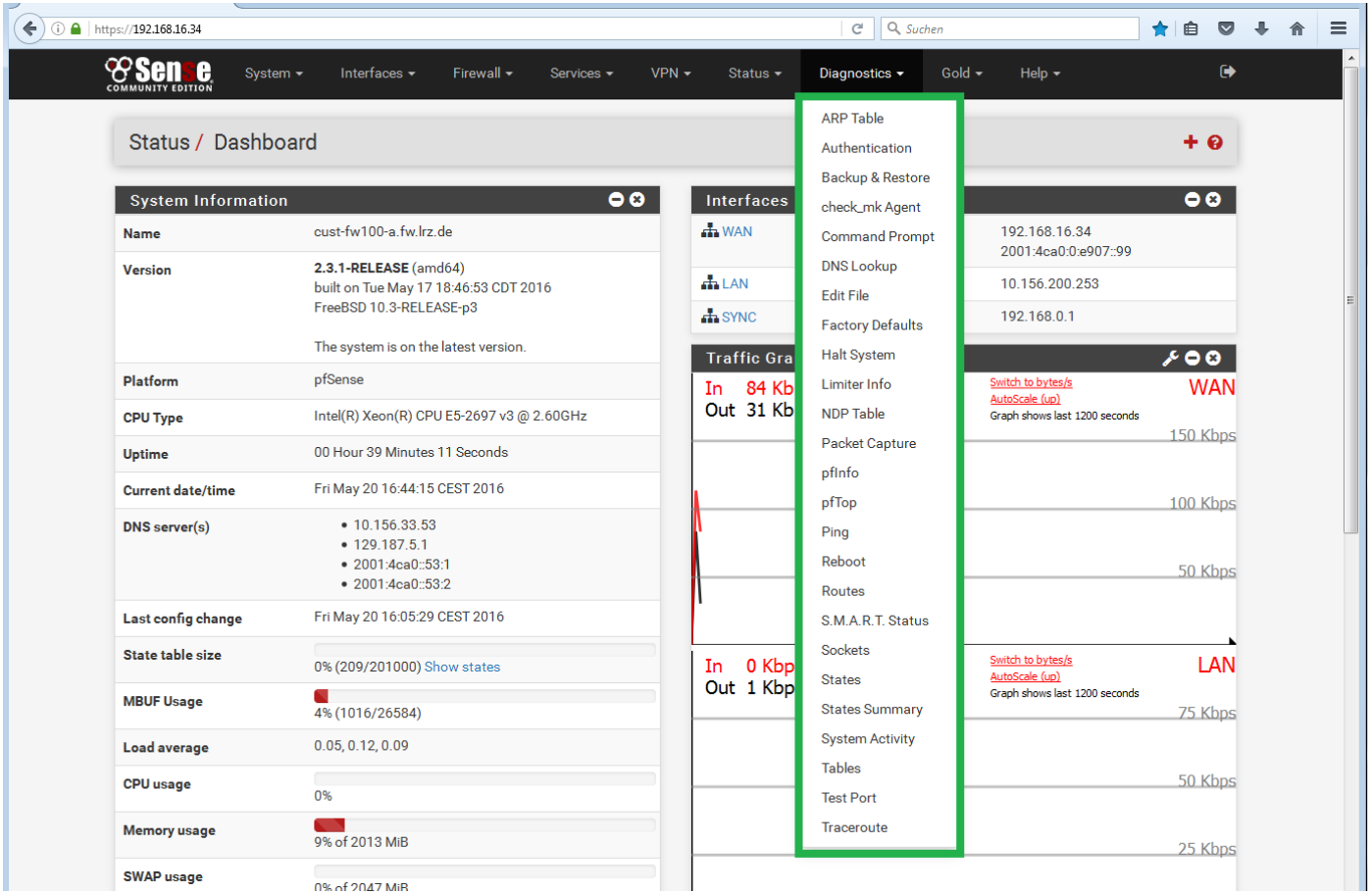
System Logs


https://192.168.16.34
Suchen
pfSense 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
Sense 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



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/

Auswertung der Syslog-Dateien

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

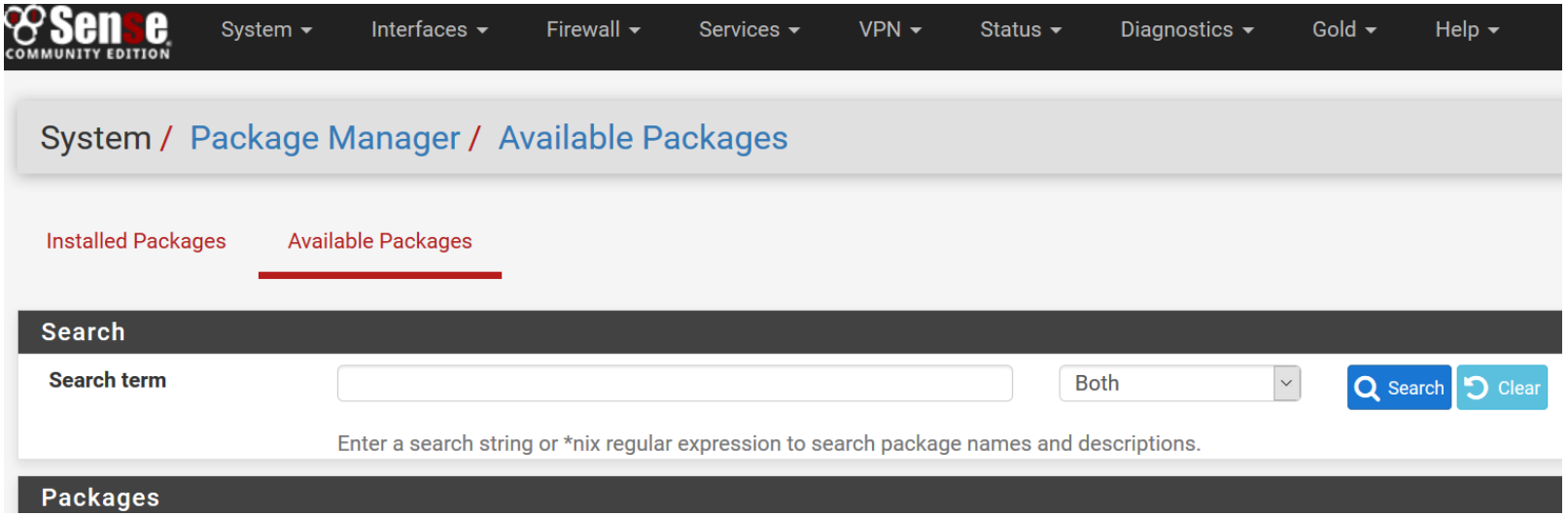
  Das LRZ empfiehlt auf ELK basierendes Logstah. Damit können die Daten anschaulich grafisch dargestellt werden.

Installation von Zusatzpaketen

- 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

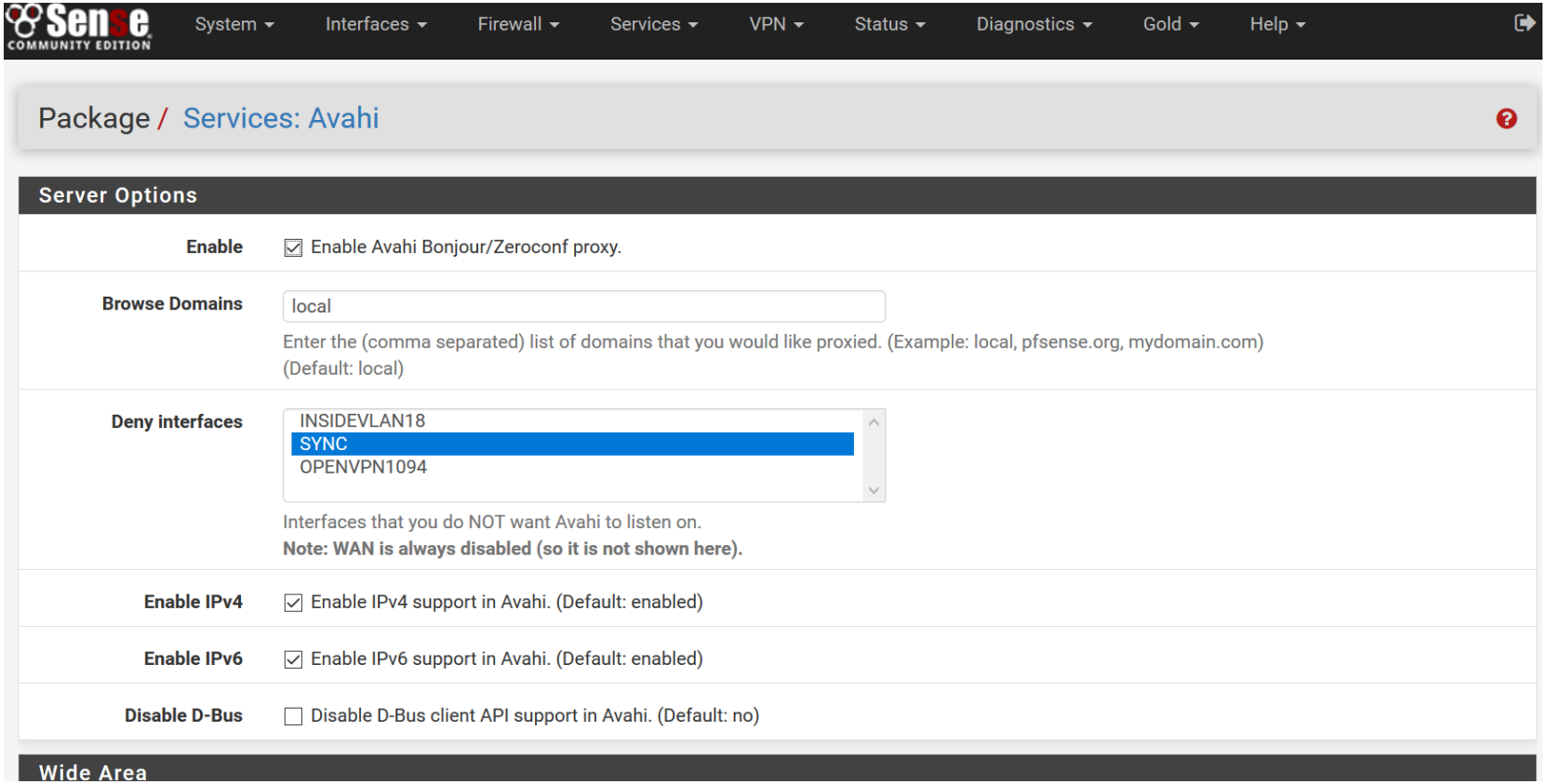
- Erlaubt mDNS



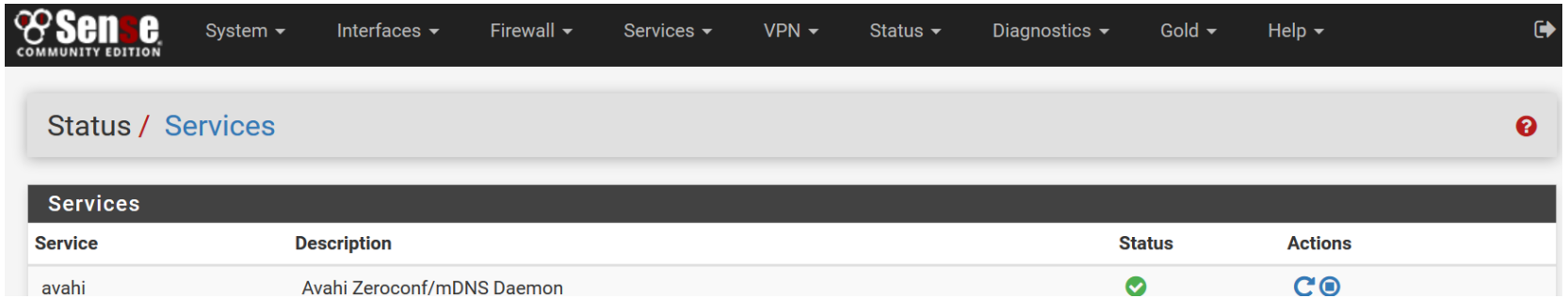
Dort das Avahi-Paket auswählen und installieren.

Nach der Installation ist die Konfiguration unter Services > Avahi möglich

Konfiguration von Avahi



Statusinformationen: Status > Services



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

Troubleshooting

- Wenn ein Dienst nicht startet, findet man dies in der Regel unter System Status herraus; 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

Package deinstallieren

- 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.

OpenVPN

- 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.

VPN-Konzepte

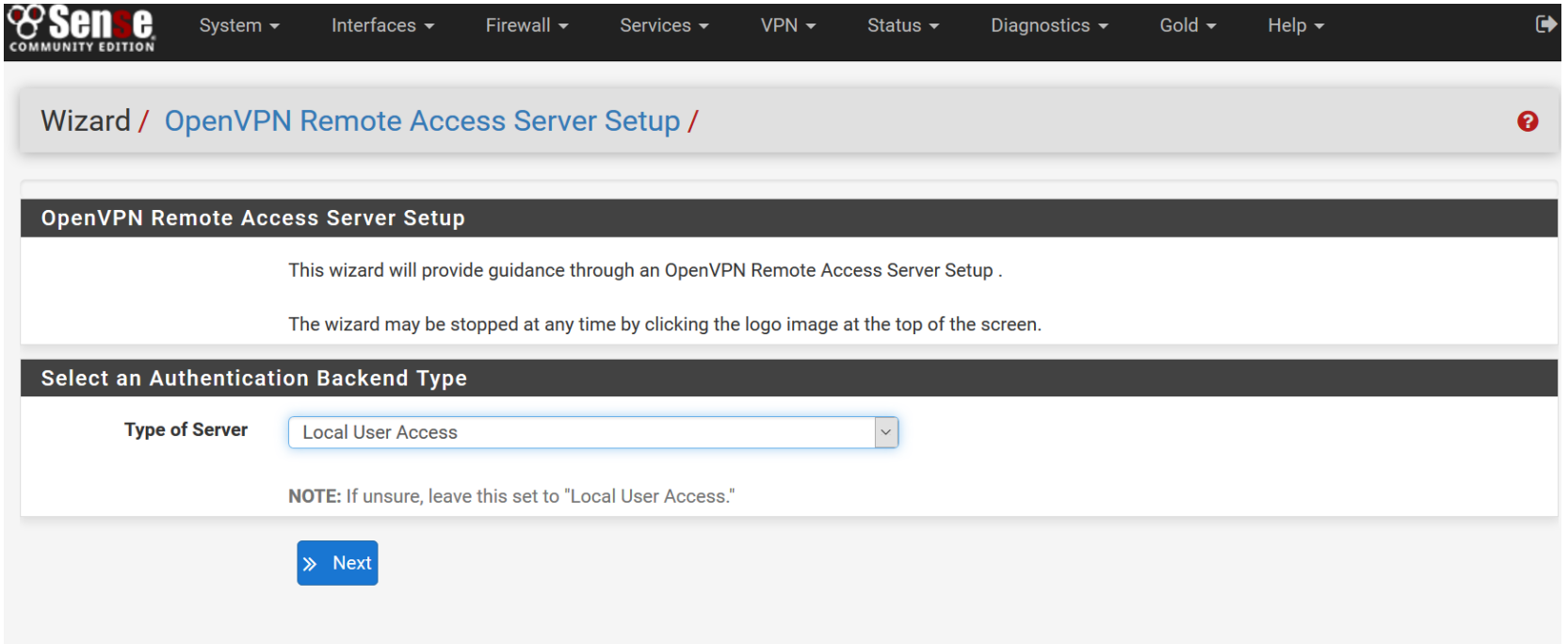
- Es gibt verschiedene Konzepte ein VPN zu realisieren, der vom LRZ empfohlene Weg ist: eine eigenes geroutetes Netz zu nehmen (hierbei gibt es zwei Varianten: ein komplett nicht geroutetes Netz (z.B. 10.0.1.0/24) oder ein vom LRZ vergebenes privates Netz (z.B. 10.152.xx.xx).
- Vorteil eines gerouteten 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 userem 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



Authentification-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

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