



Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften



pfSense – Virtuelle Firewalls am
Leibniz-Rechenzentrum

Vorraussetzungen:

- Es wird davon ausgegangen, dass die generelle Bedienung der pfSense bekannt ist
- Umgang mit der Linux-Kommandozeile / Putty wird ebenfalls benötigt

Themen dieses Kurses:

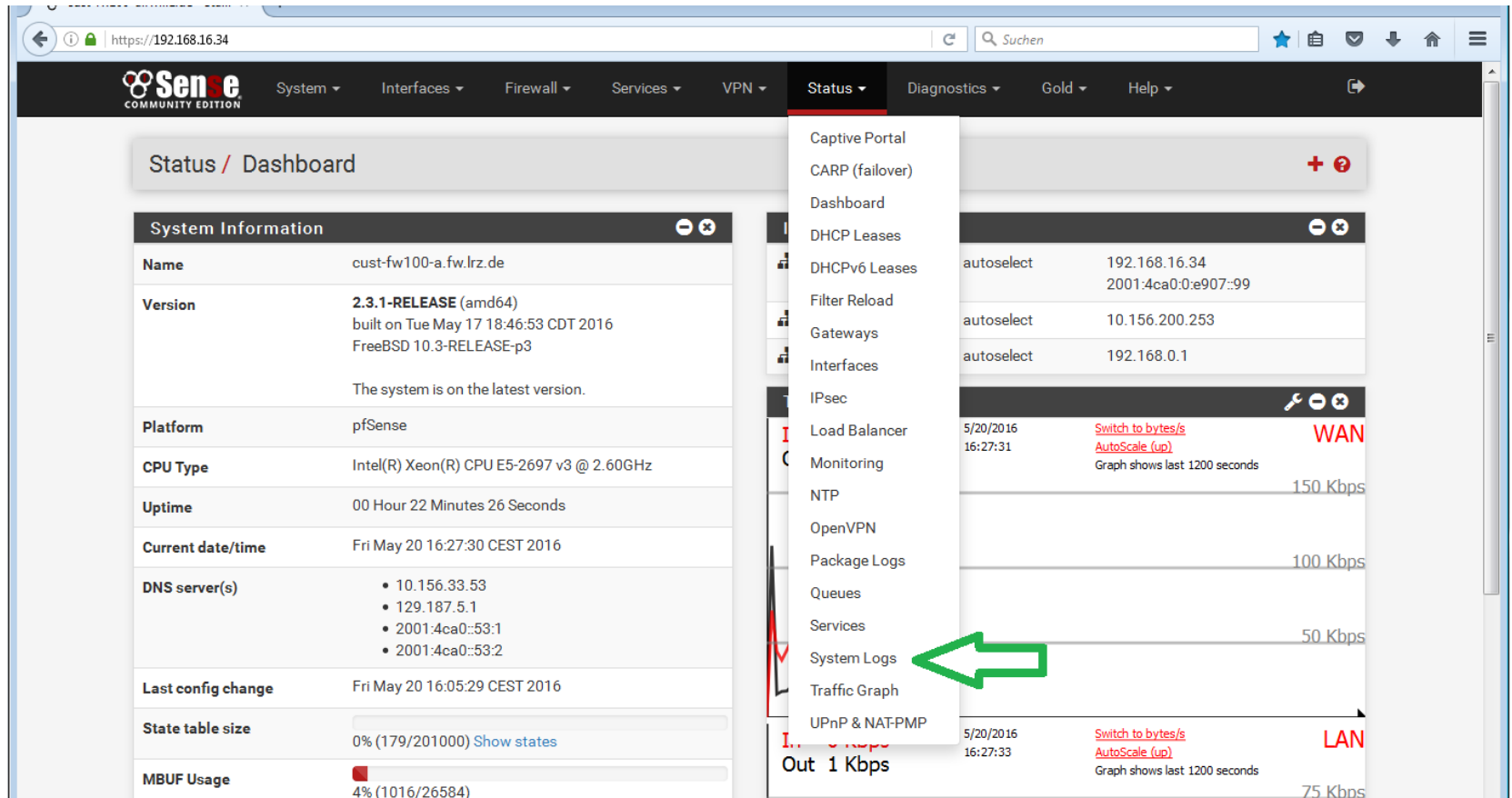
- Port-Forwarding NAT
- Logging und Log-Auswertung
 - Einrichten eines Syslog-Servers
- Installation von Zusatzpaketen
- OpenVPN-Konfiguration (mit Hands-On)

Port-Forwarding (NAT)

- NAT (Network address translation)
 - Portforwarding (1 Dienst auf einer öffentlichen Adresse wird auf eine private Adresse weitergeleitet)
 - Häufig: Um z.B. ein Angebot des Lehrstuhls erreichbar zu machen
 - Einrichtung erfolgt nach Anleitung

Achtung: Auf realen Firewalls wird im Regelfall immer eine CARP-IP verwendet, wg. Failover.

System Logs



The screenshot shows the pfSense Status Dashboard. The 'Status' menu is open, and a green arrow points to the 'System Logs' option. The dashboard includes sections for System Information, DHCP Leases, and traffic graphs for WAN and LAN interfaces.

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)

DHCP Leases

Interface	IP Address	MAC Address
autoselect	192.168.16.34	2001:4ca0:0:e907::99
autoselect	10.156.200.253	
autoselect	192.168.0.1	

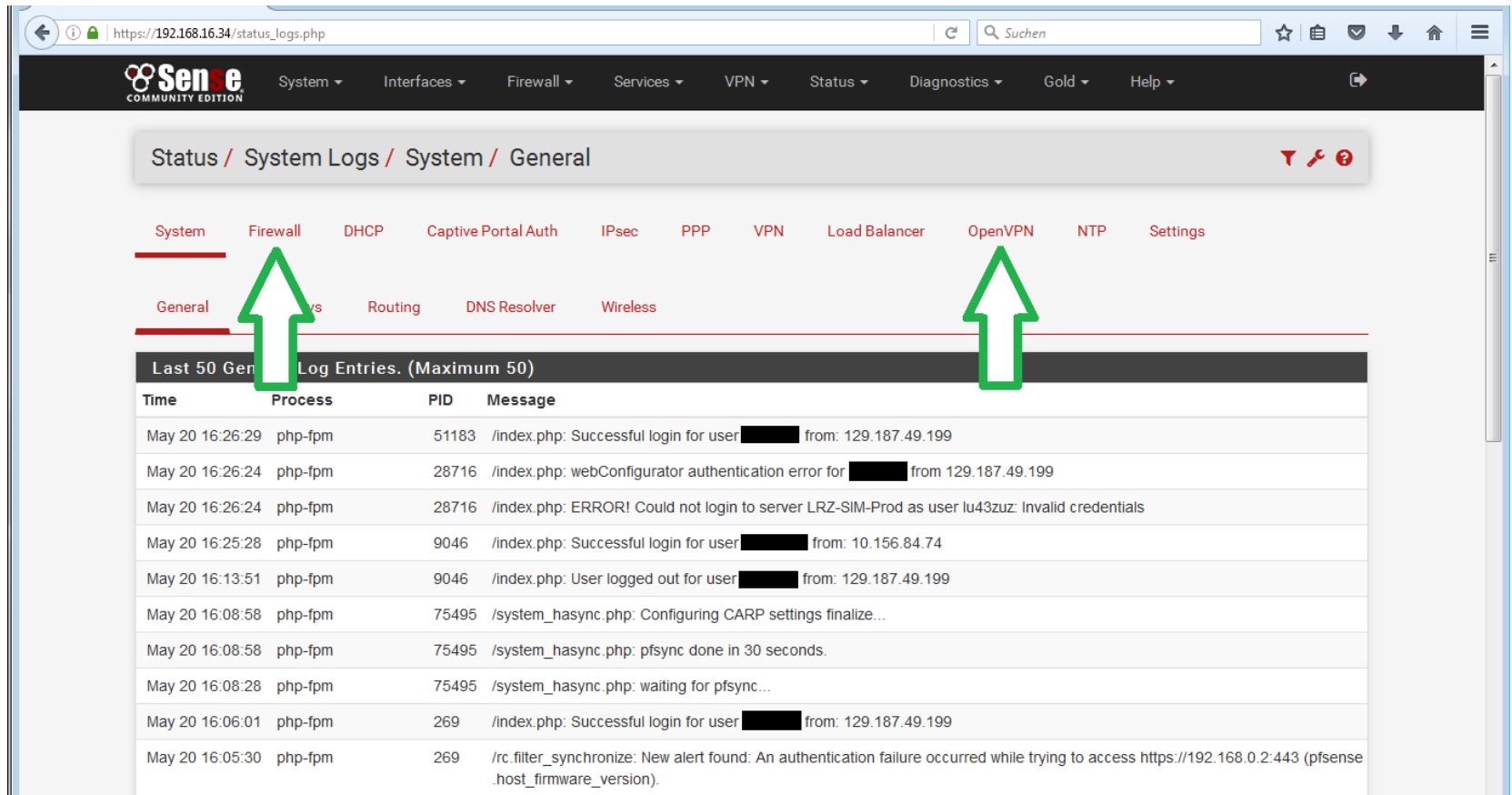
Traffic Graphs

WAN

5/20/2016 16:27:31 [Switch to bytes/s](#) [AutoScale \(up\)](#)
Graph shows last 1200 seconds
150 Kbps

LAN

5/20/2016 16:27:33 [Switch to bytes/s](#) [AutoScale \(up\)](#)
Graph shows last 1200 seconds
75 Kbps



https://192.168.16.34/status_logs.php

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

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).

Einrichten des Rsyslog-Daemons

- `#apt-get install rsyslog`
- `#nano /etc/rsyslog.conf`
- Zeilen 16 und 17 auskommentieren
- `#service rsyslog restart`
- `#tail -f /var/log/syslog`

```
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
```

Pfsense: System>System Logs> Settings

Remote Logging Options

Enable Remote Logging ☒ Send log messages to remote syslog server

Source Address ▼

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol ▼

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers

Remote Syslog Contents ☒ Everything
☐ System Events
☐ Firewall Events
☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
☐ Captive Portal Events
☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
☐ Gateway Monitor Events
☐ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
☐ Server Load Balancer Events (relayd)
☐ Network Time Protocol Events (NTP Daemon, NTP Client)
☐ Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

Auswertung der Syslog-Dateien

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

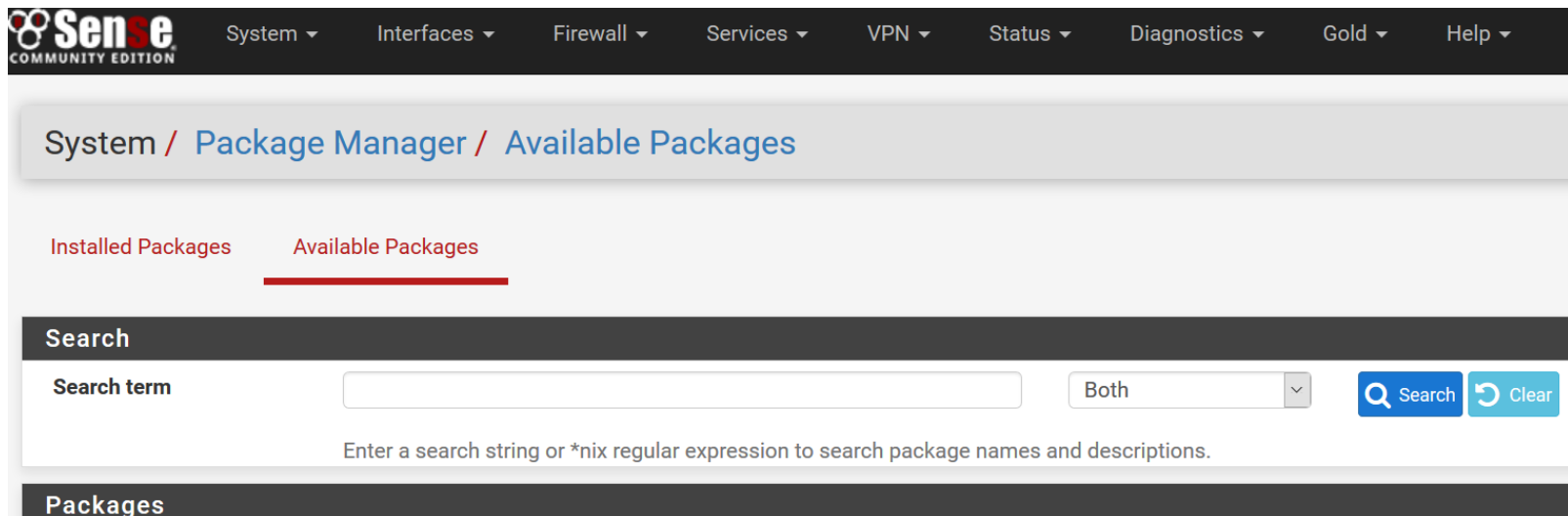
Das LRZ hat gute Erfahrungen mit auf ELK basierendem Logstash gemacht. Damit können die Daten auch anschaulich grafisch dargestellt werden.

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
 - Lokale Änderungen werde in der Regel bei einem pfsense-Update überschrieben

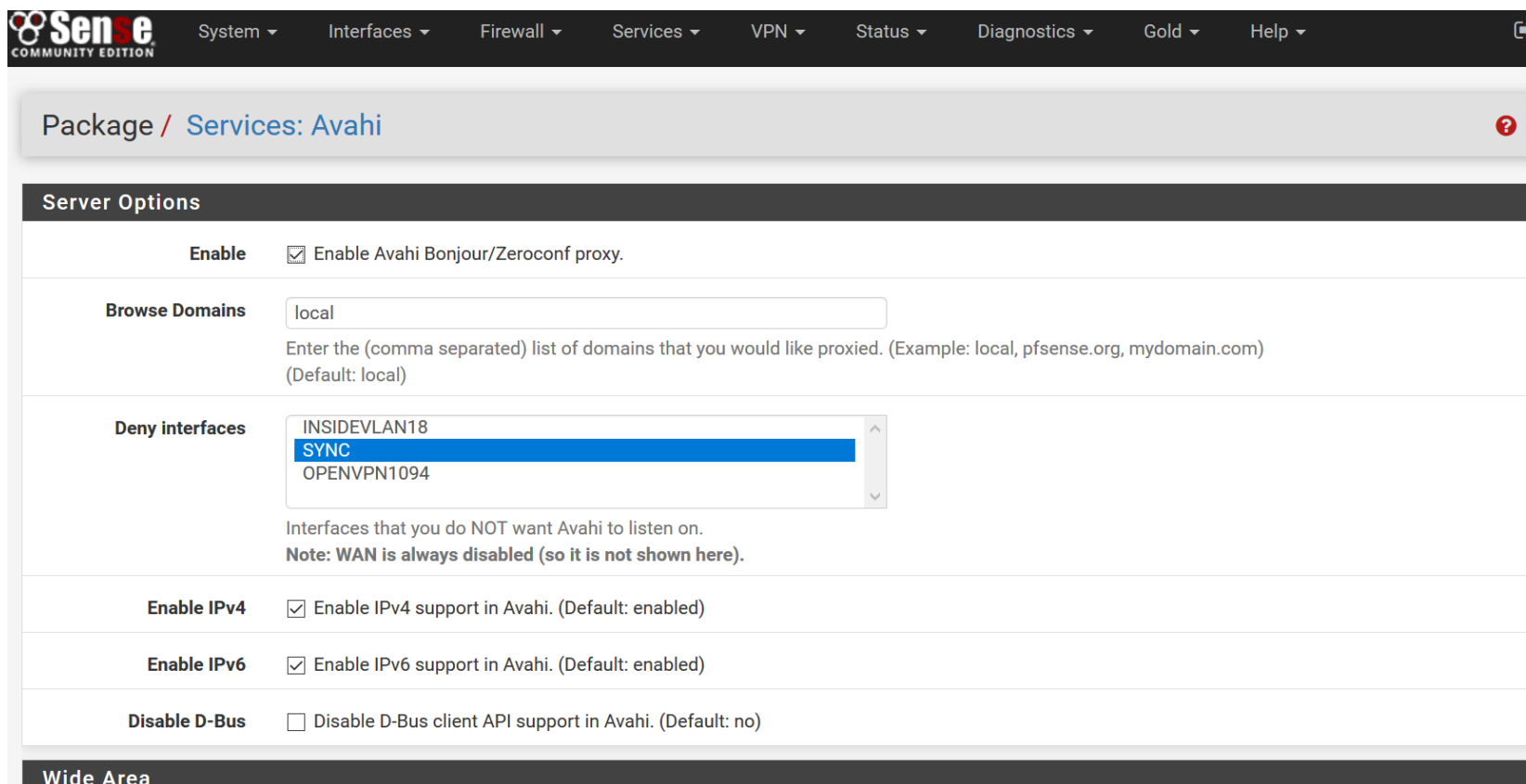
Beispiel: Avahi-Paket

- Erlaubt mDNS



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

Konfiguration von Avahi

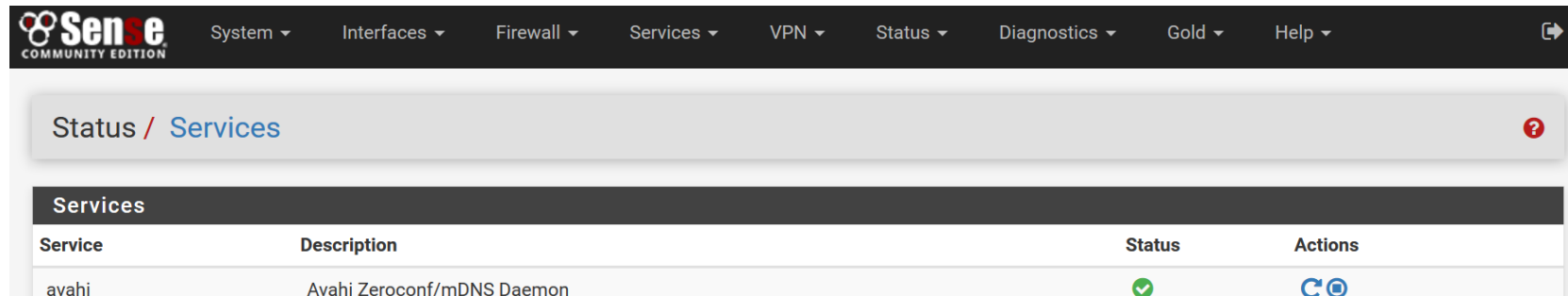


The screenshot shows the pfSense Sense Community Edition web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "Package / Services: Avahi". Below this, the "Server Options" section contains several configuration fields:

- Enable:** A checkbox labeled "Enable Avahi Bonjour/Zeroconf proxy." which is checked.
- Browse Domains:** A text input field containing "local". Below it, a note says: "Enter the (comma separated) list of domains that you would like proxied. (Example: local, pfsense.org, mydomain.com) (Default: local)".
- Deny interfaces:** A dropdown menu showing "INSIDEVLAN18", "SYNC" (highlighted in blue), and "OPENVPN1094". Below it, a note says: "Interfaces that you do NOT want Avahi to listen on. Note: WAN is always disabled (so it is not shown here)."
- Enable IPv4:** A checkbox labeled "Enable IPv4 support in Avahi. (Default: enabled)" which is checked.
- Enable IPv6:** A checkbox labeled "Enable IPv6 support in Avahi. (Default: enabled)" which is checked.
- Disable D-Bus:** A checkbox labeled "Disable D-Bus client API support in Avahi. (Default: no)" which is unchecked.

At the bottom of the configuration area, there is a section titled "Wide Area".

Statusinformationen: Status > Services



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 eine Internetrecherche 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 Eingriff mittels SSH notwendig.
 - SSH funktioniert (bislang leider) nicht mit LDAP-Anbindung; daher benötigt man unter Users einen eigenen Benutzer

- Installieren sie das Avahi-Paket, überprüfen Sie, ob dies gestartet wurde, welche Einträge Sie im Log finden und deinstallieren es anschließend.
- Installieren Sie dann den OpenVPN-Client Exporter indem sie in den Available Packages nach OpenVPN suchen.

- Ist auf der pfsense integriert (eigenständiges Projekt siehe:

<https://openvpn.net/>



- Wird regelmäßig von unabhängigen Quellen untersucht z.B: <https://srlabs.de/blog/openvpn-audit>
Kritische Updates fließen zeitnah in pfsense-Releases ein.
- Vom LRZ als VPN-Lösung unterstützt und supportet.

Unterschied OpenVPN zu LRZ-VPN

LRZ-VPN

- LRZ-VPN: eduVPN(mit automatischem Software-Update)
- Generelle Unterscheidung nur zwischen den verschiedenen Einrichtungen: TUM / LMU / HM etc.

Eigenes VPN (OpenVPN)

- Lehrstuhlnetze hinter der Firewall können erreicht werden
- Feingranulare Benutzerrechtevergabe (über eigenen Server/ TUM-Online/ AD / Inst-VPN möglich) durch den Lehrstuhl/das Institut / Masteruser möglich

- 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, wenn ein Bridge-Adapter verwendet wird, ist dies nicht möglich.
- Bridging ist auch möglich, Konfiguration ist aufwendiger und externe Clienten befinden sich im lokalen LAN(!)

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 'OpenVPN Remote Access Server Setup' wizard in the Sense Community Edition interface. The breadcrumb trail is 'Wizard / OpenVPN Remote Access Server Setup /'. The wizard title is 'OpenVPN Remote Access Server Setup'. The instructions state: '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.' The section 'Select an Authentication Backend Type' contains a 'Type of Server' dropdown menu with 'Local User Access' selected. A note below the dropdown reads: 'NOTE: If unsure, leave this set to "Local User Access."' At the bottom is a blue button labeled '» Next'.

Wizard / OpenVPN Remote Access Server Setup /

OpenVPN Remote Access Server Setup

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

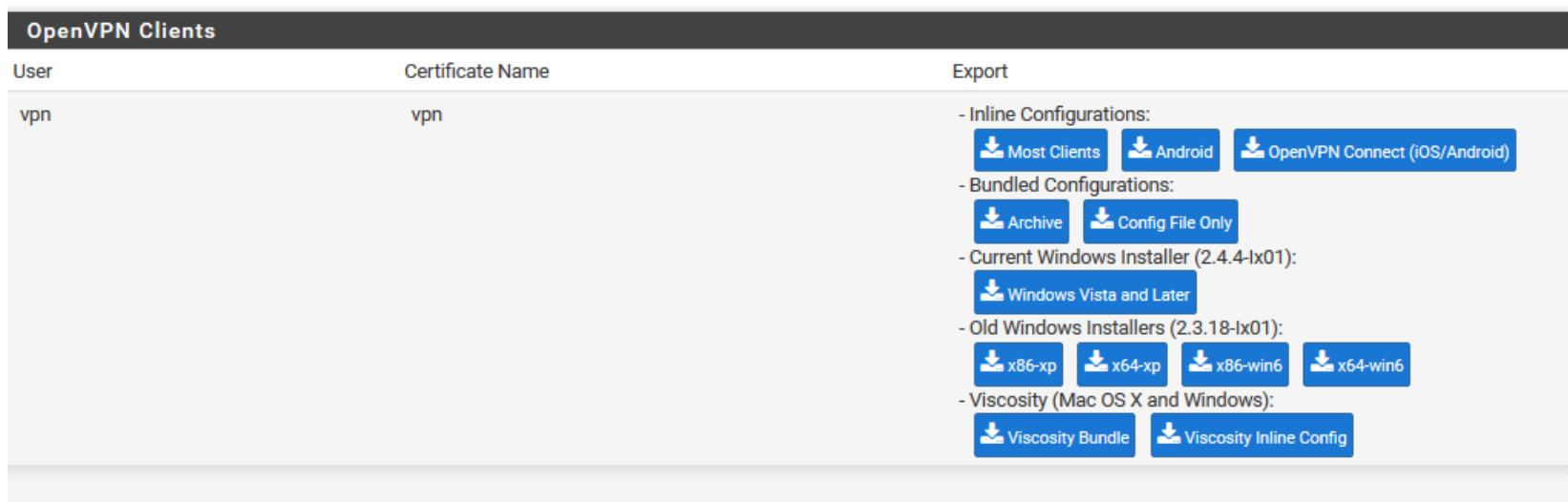
Type of Server: Local User Access

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

» Next

Authentification-Server ist hier erforderlich

Export der Konfiguration für debian-client



The screenshot shows the 'OpenVPN Clients' web interface. It has a table with columns 'User' and 'Certificate Name'. The first row shows 'vpn' for both. To the right of the table is an 'Export' section with several download buttons organized into categories:

- Inline Configurations:
 - Most Clients
 - Android
 - OpenVPN Connect (iOS/Android)
- Bundled Configurations:
 - Archive
 - Config File Only
- Current Windows Installer (2.4.4-lx01):
 - Windows Vista and Later
- Old Windows Installers (2.3.18-lx01):
 - x86-xp
 - x64-xp
 - x86-win6
 - x64-win6
- Viscosity (Mac OS X and Windows):
 - Viscosity Bundle
 - Viscosity Inline Config

Most-Clients wählen, Datei in Notepad speichern und auf dem Debian-System mittels copy & paste in vi i, importieren.

```
#apt-get update
```

```
#apt-get install openvpn
```

```
#openvpn konfiurations-datei
```

- Folgen Sie dem Handout für die Einrichtung des VPN-Servers



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>