



9. April bis 12. April 2019 am Karlsruher Institut für Technologie

GUUG-Frühjahrsfachgespräch 2019

Sichere Netzwerke mit pfSense



hagen.bauer@rusticus-consulting.de



rusticus consulting

IT | BODENSTÄNDIG & INNOVATIV



Fahrplan

- About me
- Warum etwas neues? Mein Provider gibt mir doch eine Firewall.
- Was genau ist pfSense?
- Der Start ist sehr einfach
- Komplexere Szenarien sind einfach zu realisieren
- Zusammenfassung



About Me

- Beruflich:
 - Technischer Vertriebsberater für Unternehmenssoftware
 - Selbstständig: Berater für Informationssicherheit
- weder Sysadmin noch Netzwerktechniker
- Power User mit “learning by doing”
- pfSense im Homeoffice seit 2009
 - 10 PCs, 4 Server, 8 mobile Geräte,
 - Homeautomation, Freifunk, Sonos, Asterisk
 - 2 Tor Nodes
 - 6 VLANs
 - Dual WAN



Warum etwas Neues?

**Mein Provider gibt mir
doch eine Firewall.**



rusticus consulting

IT | BODENSTÄNDIG & INNOVATIV

Firewall Markt (grobe Aufteilung)

- Unternehmenslösungen
 - \$\$\$\$
- Geräte für Zuhause
 - Preiswert
 - Einfacher aber wachsender Funktionsumfang
 - Unsichere Updatepolitik vieler Hersteller bei Sicherheitslücken



Geräte für Zuhause

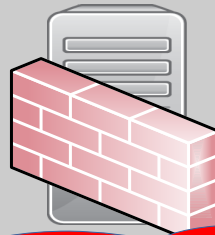
- Fehlender Funktionsumfang für kleine /mittlere Betriebe und Familieneinsatz
 - Protokollierung
 - Site 2 Site Verbindung / VPN
 - Bandbreitenbeschränkung
 - Netzwerksegmentierung
 - Multi WAN
 - Outgoing Block



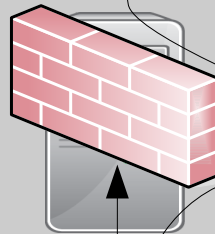


LAN

**Zweigstelle
Eltern**



Internet



LAN

DMZ
IOT
VOIP



rustica

IT | BODENSTÄNDIG & INNOVATIV

Was genau ist pfSense?



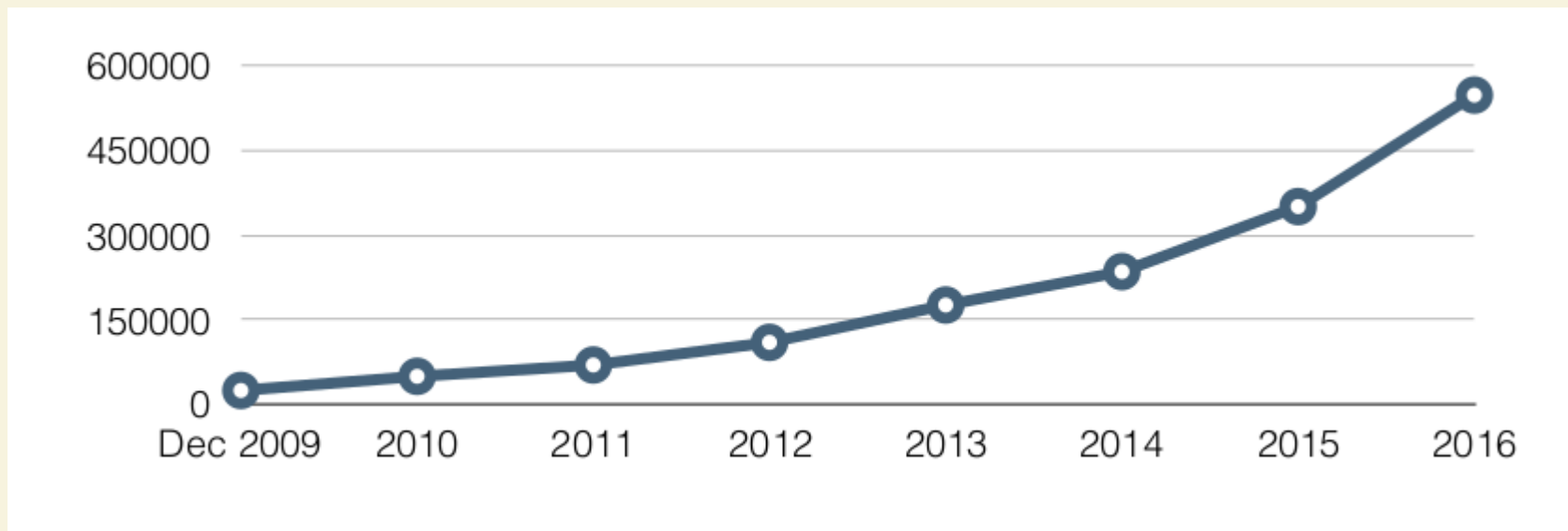
Überblick pfSense

- Basiert auf FreeBSD
 - Beliebte OS Plattform für Netzwerk- und Sicherheitsprodukte
 - Juniper Junos, NetApp, NetASQ, Cisco IronPort, Citrix, Netflix, etc...
- Verwaltung über Weboberfläche
- Verbindet die Basiskomponenten von FreeBSD in eine einfach zu verwendende Oberfläche
- Mehr Funktionen als die meisten kommerziellen Produkte



Projektgeschichte

- Start in 2004 als Fork von m0n0wall



1.2 - 02/2008 (FreeBSD 6.2)
2.0 - 09/2011 (FreeBSD 8.1)
2.1 - 09/2013 (FreeBSD 8.3)
2.2 - 01/2015 (FreeBSD 10.1)
2.3 - 04/2016 (FreeBSD 10.3)
2.4 - 10/2017 (FreeBSD 11.1)



Umfangreiche Funktionen

- DHCP Server
- DHCP Relay
- DNS Resolver
- Dynamic DNS
- Load Balancer
- Multi WAN
- Wake on LAN
- VLAN
- Intrusion Detection
- PKI
- Hochverfügbarkeit
- Captive Portal
- Freeradius3
- Squid
- ...
- ...



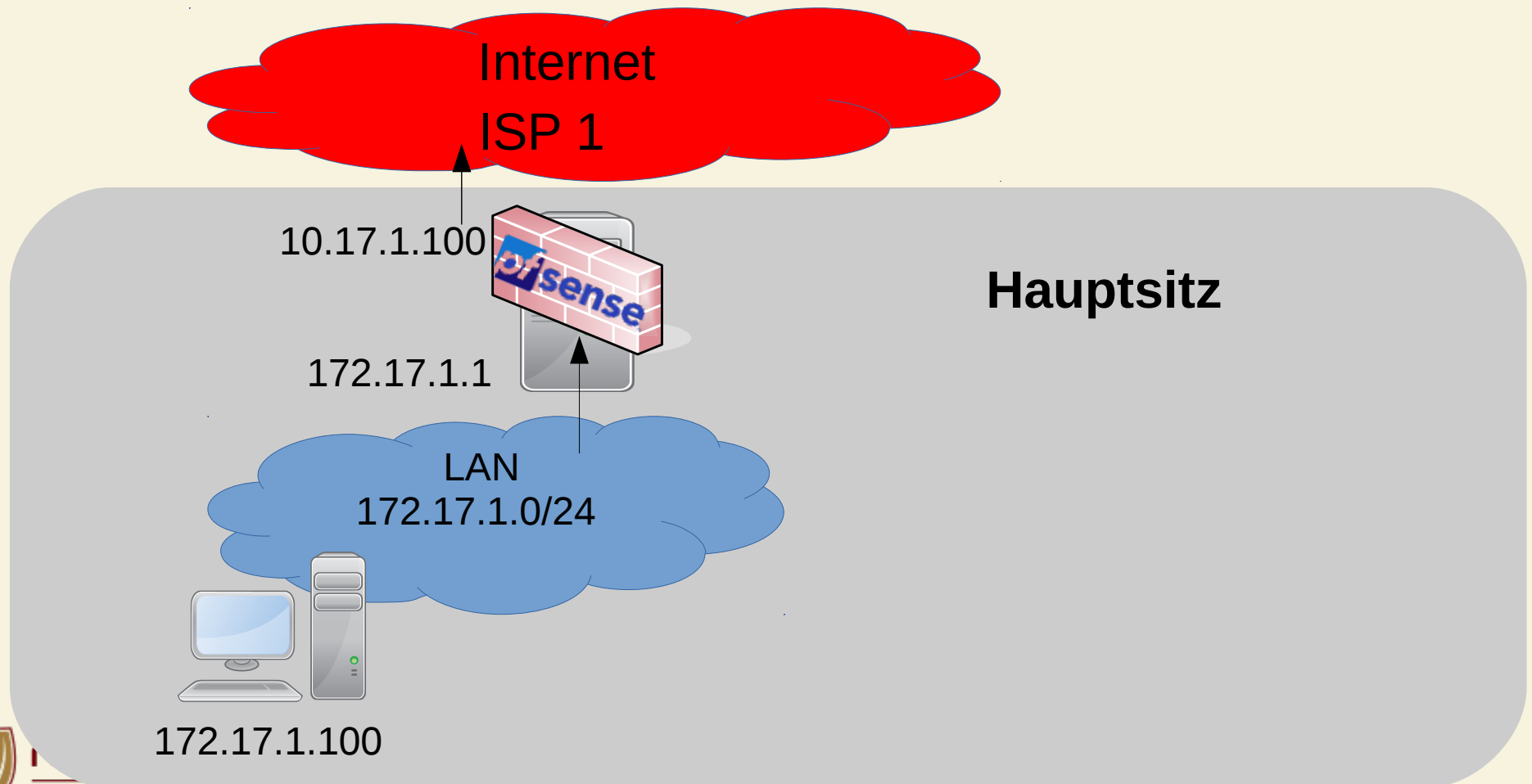
Läuft auf

- Eigener Hardware
 - Min CPU - 500 Mhz RAM - 512 MB
- Appliances von Netgate
 - Vorkonfiguriert und optimiert
 - Mit und ohne Support
- In der Cloud
 - Microsoft Azure / Amazon Cloud
- Ausstattung abhängig von Durchsatz und installierten Funktionen



Der Start ist sehr einfach

Szenario 1: Basisinstallation



Demonstration Basisinstallation

Applications zentral-pfsense.pfsense...

zentral-pfsense.pfsense-lab.lcl - Status: Dashboard - Mozilla Firefox

zentral-pfsense.pfsen... x +

https://172.17.1.1

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Status / Dashboard

System Information

Name	zentral-pfsense.pfsense-lab.lcl
System	VirtualBox Virtual Machine Netgate Device ID: 630ca8825ac1e2e083d4
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.4.1-RELEASE (amd64) built on Sun Oct 22 17:26:33 CDT 2017 FreeBSD 11.1-RELEASE-p2 The system is on the latest version. Version information updated at Fri Oct 27 15:49:58 UTC 2017
CPU Type	Intel(R) Core(TM) i7-5650U CPU @ 2.20GHz AES-NI CPU Crypto: Yes (inactive)
Uptime	00 Hour 23 Minutes 56 Seconds
Current date/time	Fri Oct 27 14:13:13 UTC 2017
DNS server(s)	127.0.0.1 10.17.1.99 8.8.8.8
Last config change	Fri Oct 27 14:05:46 UTC 2017

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

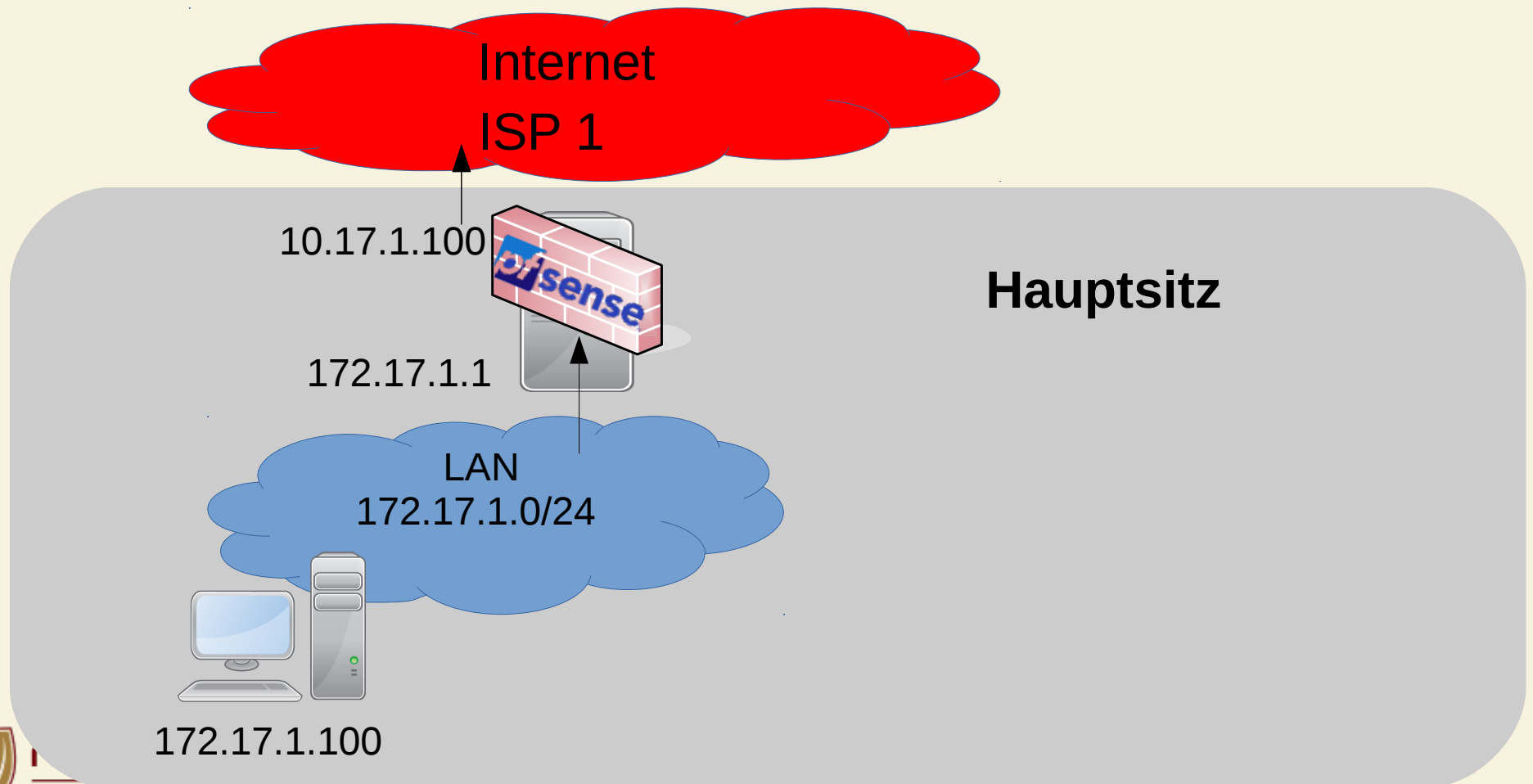
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale, you can [register](#) your community support subscription for access to pfSense Gold.

- Register Your Support Subscription
- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional Services
- Log into your portal account
- Community Support Resources
- Official pfSense Training by Netgate
- Visit Netgate.com

If you decide to purchase a Netgate Global Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase support [here](#).

Interfaces

Szenario 1: Basisinstallation



Firewall Regeln

- Regeln gelten immer für Inbound
- Erste Regel gewinnt, der Rest wird ignoriert
- Stateful filtering
- Aliases vereinfachen Verwaltung und reduzieren die Fehlermöglichkeiten
 - IP Adressen
 - Netzwerke
 - Hostnamen
 - Ports



**Komplexere Szenarien sind
einfach zu realisieren**

Erweiterte Funktionen

- VPNs
- DMZ/ Netzwerke segmentieren
- Bandbreiten beschränken
- Protokolle der Konfigurationsänderungen



Virtuelle Private Netzwerke

- Anbindung von Standorten und mobilen Clients
- IPSec
 - Standard Clients auf OS X, iOS, Android
 - Interoperable
- OpenVPN
 - Clients hinter NAT
 - Einfache Client Konfiguration





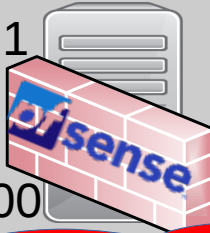
172.18.1.100

Zweigstelle

LAN
172.18.1.0/24

172.18.1.1

10.18.1.100



Internet
ISP 1

10.17.1.100

172.17.1.1

LAN
172.17.1.0/24



172.17.1.100

Hauptsitz



RUS

IT | BODENSTÄNDIG & INNOVATIV

Szenario: 2 Standorte verbinden

- Server
 - Definition VPN Server
 - Öffnen Firewall für OpenVPN
 - Definition Netzwerkverkehr für VPN Tunnel
- Client
 - Definition VPN Client
- Verbindungstest



Demo: 2 Standorte verbinden

Applications | zweigstelle-pfsense.pfs... | Terminal - hbauer@zwei... | 12:08 | hbauer

zweigstelle-pfsense.pfsense-lab.lcl - Status: OpenVPN - Mozilla Firefox

zweigstelle-pfsense.p... x +

https://172.18.1.1/status_openvpn.php

pfsense COMMUNITY EDITION | System ▾ | Interfaces ▾ | Firewall ▾ | Services ▾ | VPN ▾ | Status ▾ | Diagnostics ▾ | zweigstelle-pfsense ▾ | 2

Status / OpenVPN

Client Instance Statistics

Name	Status	Connected Since	Local Address	Virtual Address	Remote Host	Bytes Sent/Received	Service
Client UDP4	up	Sun Oct 29 11:07:17 2017	10.18.1.100:45673	172.17.6.2	10.17.1.100:1194	1 KiB / 672 B	✓ ↻



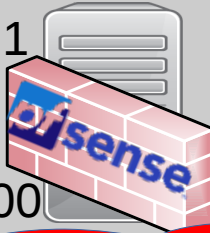
172.18.1.100

Zweigstelle

LAN
172.18.1.0/24

172.18.1.1

10.18.1.100



Internet
ISP 1

10.17.1.100

172.17.1.1

LAN
172.17.1.0/24



172.17.1.100

Hauptsitz



RUS

IT | BODENSTÄNDIG & INNOVATIV

Netzwerksegmentierung

- Ist grundlegender Bestandteil der Sicherheitsinfrastruktur
- Physikalisch oder Virtuel (VLAN)
- Privat : IOT, VOIP, Multifunktionsfaxgeräte
- Business: DMZ, Alte OS in Produktionsanlagen





172.18.1.100

LAN
172.18.1.0/24

Zweigstelle

172.18.1.1

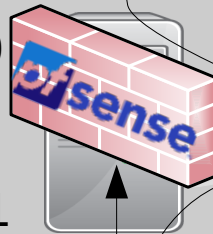
10.18.1.100



Internet

ISP 1

10.17.1.100



172.17.1.1

LAN
172.17.1.0/24



172.17.1.100

Hauptsitz

DMZ
172.17.2.0/24



172.17.2.10



rustica

IT | BODENSTÄNDIG & INNOVATIV

Szenario 3: DMZ

- Definition Netzwerk / DHCP
- Test Ping
 - Zentrale LAN → DMZ => OK
 - DMZ → Intranet => Fehler
 - DMZ → Internet => Fehler
 - Niederlassung → DMZ Server => NA
- Portfreigabe auf Webserver in DMZ
- Test Webserver
 - Niederlassung → DMZ Server => OK



Demo: DMZ

zentral-pfsense.pfsense... Terminal - hbauer@zent... 17:26 hbauer

zentral-pfsense.pfsense-lab.lcl - Status: Dashboard - Mozilla Firefox

zentral-pfsense.pfsen... x +

https://172.17.1.1

System Information

Name	zentral-pfsense.pfsense-lab.lcl
System	VirtualBox Virtual Machine Netgate Device ID: 0a09bc4a02797edae681
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.4.1-RELEASE (amd64) built on Sun Oct 22 17:26:33 CDT 2017 FreeBSD 11.1-RELEASE-p2 The system is on the latest version. Version information updated at Mon Oct 30 15:52:10 UTC 2017
CPU Type	Intel(R) Core(TM) i7-5650U CPU @ 2.20GHz AES-NI CPU Crypto: Yes (inactive)
Uptime	00 Hour 34 Minutes 57 Seconds
Current date/time	Mon Oct 30 16:26:25 UTC 2017
DNS server(s)	127.0.0.1 10.17.1.99 8.8.8.8
Last config change	Mon Oct 30 16:26:14 UTC 2017
State table size	0% (33/97000) Show states
MBUF Usage	2% (1266/61006)
Load average	1.12, 0.78, 0.62

Netgate Services And Support

Contract type **Community Support**
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

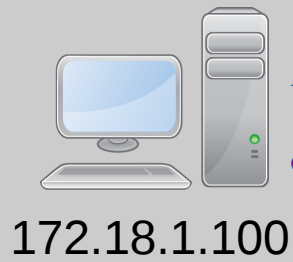
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale, you can [register](#) your community support subscription for access to [pfSense Gold](#).

- Register Your Support Subscription
- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional Services
- Log into your portal account
- Community Support Resources
- Official pfSense Training by Netgate
- Visit Netgate.com

If you decide to purchase a Netgate Global Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase support [here](#).

Interfaces

WAN	↑	1000baseT <full-duplex>	10.17.1.100
LAN	↑	1000baseT <full-duplex>	172.17.1.1
DMZ	↑	1000baseT <full-duplex>	172.17.1.1



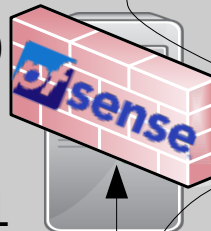
LAN
172.18.1.0/24

Zweigstelle



Internet
ISP 1

10.17.1.100



172.17.1.1

LAN
172.17.1.0/24



Hauptsitz

DMZ
172.17.2.0/24

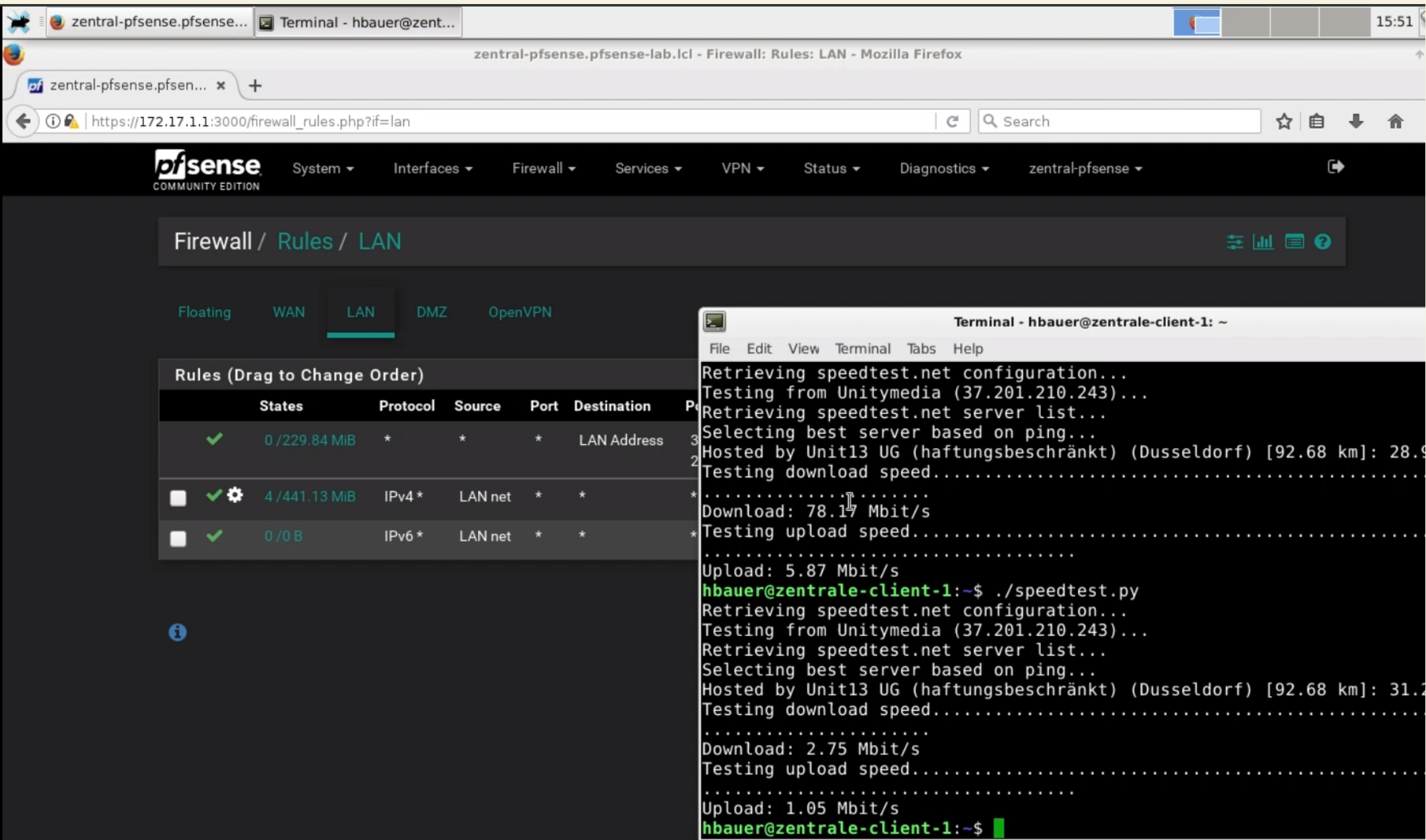


Scenario 4: Traffic Shaping

- “Managed unfairness of bandwidth” statt FIFO
- Queues definieren die Prioritäten
- Rules verteilen die Queues
- Zwei Methoden
 - Limiter: harte Grenzen einfach zuweisen
 - Traffic Shaper (ALTQ)



Demo 4: Traffic Shaping



zentral-pfsense.pfsense... Terminal - hbauer@zent...

zentral-pfsense.pfsense-lab.lcl - Firewall: Rules: LAN - Mozilla Firefox

zentral-pfsense.pfsen... x +

https://172.17.1.1:3000/firewall_rules.php?if=lan

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ zentral-pfsense ▾

Firewall / Rules / LAN

Floating WAN LAN DMZ OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	
✓	0 / 229.84 MiB	*	*	*	LAN Address	3
☐ ✓ ⚙	4 / 441.13 MiB	IPv4 *	LAN net	*	*	*
☐ ✓	0 / 0 B	IPv6 *	LAN net	*	*	*

Terminal - hbauer@zentrale-client-1: ~

```
File Edit View Terminal Tabs Help
Retrieving speedtest.net configuration...
Testing from Unitymedia (37.201.210.243)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by Unit13 UG (haftungsbeschränkt) (Dusseldorf) [92.68 km]: 28.9
Testing download speed.....
Download: 78.17 Mbit/s
Testing upload speed.....
Upload: 5.87 Mbit/s
hbauer@zentrale-client-1:~$ ./speedtest.py
Retrieving speedtest.net configuration...
Testing from Unitymedia (37.201.210.243)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by Unit13 UG (haftungsbeschränkt) (Dusseldorf) [92.68 km]: 31.2
Testing download speed.....
Download: 2.75 Mbit/s
Testing upload speed.....
Upload: 1.05 Mbit/s
hbauer@zentrale-client-1:~$
```

Configuration History

- Automatisches Backup jeder Änderung
- Zurückspringen auf letzte Version möglich
- Einzelne Änderungen können nachvollzogen werden
 - Wer, wann und was



Demo: Configuration Historie

5. pfsense-logging.mp4

zentral-pfsense.pfsense... Terminal - hbauer@zent...

zentral-pfsense.pfsense-lab.lcl - Diagnostics: Backup & Restore: Config History - Mozilla Firefox

zentral-pfsense.pfsen... * +

https://172.17.1.1:3000/diag_confbak.php?diff=Diff&newtime=1509389787&oldtime=1509389397

```
<rule>
@@ -260,6 +283,24 @@
    <username>admin@172.17.1.11</username>
  </created>
</rule>
+ <rule>
+   <source>
+     <any></any>
+   </source>
+   <interface>wan</interface>
+   <protocol>tcp</protocol>
+   <destination>
+     <address>172.17.2.10</address>
+     <port>80</port>
+   </destination>
+   <descr><![CDATA[NAT DMZ WebServer]]></descr>
+   <associated-rule-id>nat_59f775db485343.83614067</associated-rule-id>
+   <tracker>1509389787</tracker>
+   <created>
+     <time>1509389787</time>
+     <username>NAT Port Forward</username>
+   </created>
+ </rule>
+ <separator>
+   <wan></wan>
+   <openvpn></openvpn>
@@ -449,8 +490,8 @@
</unbound>
<dyndnses></dyndnses>
<revision>
-   <time>1509389397</time>
-   <description><![CDATA[admin@172.17.1.11: /firewall_nat.php made unknown change]]></description>
+   <time>1509389787</time>
+   <description><![CDATA[admin@172.17.1.11: Firewall: NAT: Port Forward - saved/edited a port forward rule.]]></description>
+   <username>admin@172.17.1.11</username>
</revision>
<cert>
```

Zusammenfassung

- Standard Geräte der Provider bieten keine ausreichende Funktionalität mehr
- pfSense zeichnet sich aus durch
 - Geringe / keine Anfangsinvestitionen
 - Funktionen einer Enterprise Firewall
 - Enterprise Support wenn gewünscht
 - Keine laufenden Lizenzkosten einzelner Funktionen
- Idealer Start für
 - kleinere und mittlere Unternehmensgrößen
 - gehobenen Heimarbeitsplatz
 - Haushalte





9. April bis 12. April 2019 am Karlsruher Institut für Technologie

GUUG-Frühjahrsfachgespräch 2019

Sichere Netzwerke mit pfSense



hagen.bauer@rusticus-consulting.de



rusticus consulting

IT | BODENSTÄNDIG & INNOVATIV

