



# Secure your Networks with the Opensource Firewall pfSense



[hagen.bauer@rusticus-consulting.de](mailto:hagen.bauer@rusticus-consulting.de)



# Agenda

- About me
- Why something new? My provider gave me a firewall.
- What exactly is pfSense?
- It's an easy start
- More complex scenarios are easy to implement
- Summary

# About Me

- First job: technical sales for enterprise collaboration software
- neither sysadmin nor network engineer
- Power User with “learning by doing”
- pfSense in my home office since 2009
  - 10 PCs, 4 Server, 8 mobile devices,
  - Home automation, Freifunk, Sonos, Asterisk
  - 2 Tor Nodes
  - 4 VLANs
  - Dual WAN
- netgate authorized partner



**Why something new?**

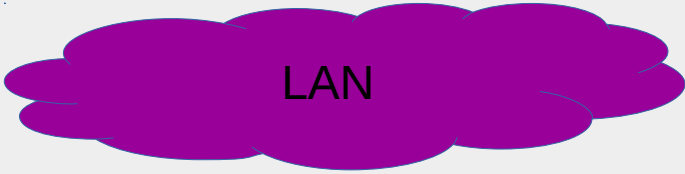
**My provider gave  
me a firewall.**

# Firewall Market (roughly)

- Enterprise solutions
  - \$\$\$\$
- Home use devices
  - Cheap
  - Simple but growing set of functions
  - Bad track record in regards of security updates

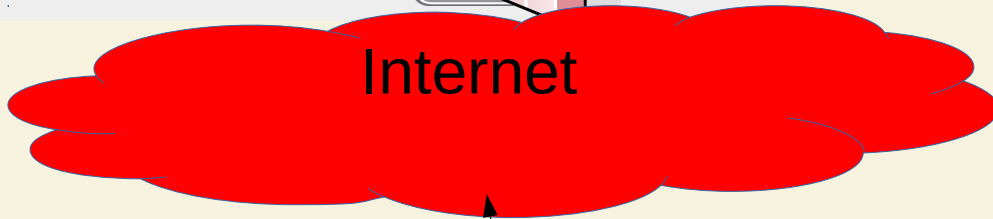
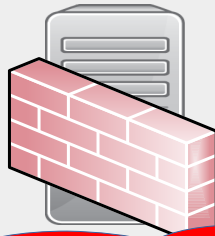
# Devices for Home Use

- Missing functions for small / medium enterprises and family use.
  - Logging
  - Site to site connections / VPN
  - Bandwidth limiting
  - Network segmentation
  - Multi WAN
  - Outgoing block of traffic

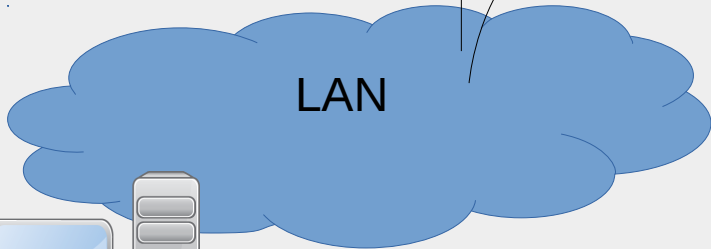
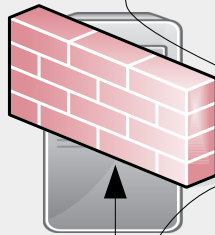


LAN

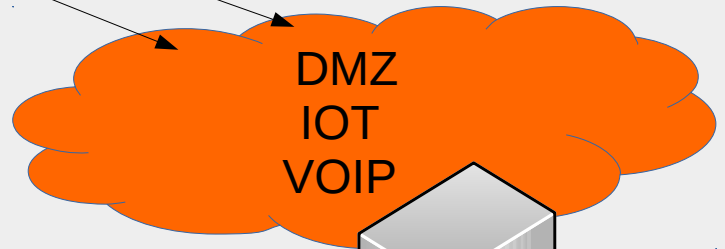
**local branch  
your parents**



Internet



LAN



DMZ  
IOT  
VOIP



**So what exactly is pfSense?**

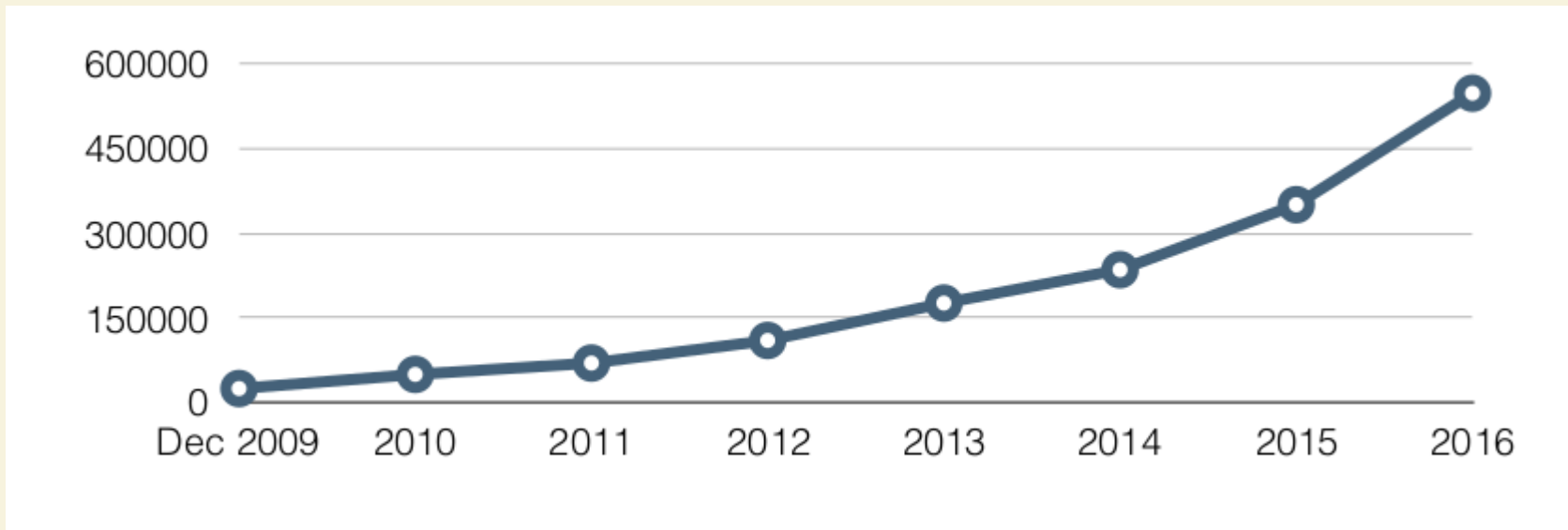


# pfSense Overview

- Based on FreeBSD
  - Popular OS platform for network- and security products
  - Juniper Junos, NetApp, NetASQ, Cisco IronPort, Citrix, Netflix, etc...
- Administration via web interface
- Connects the base components of FreeBSD in one easy to use web user interface
- More functions than most commercial products

# Project History

- Started in 2004 as fork from 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)

# Comprehensive Feature Set

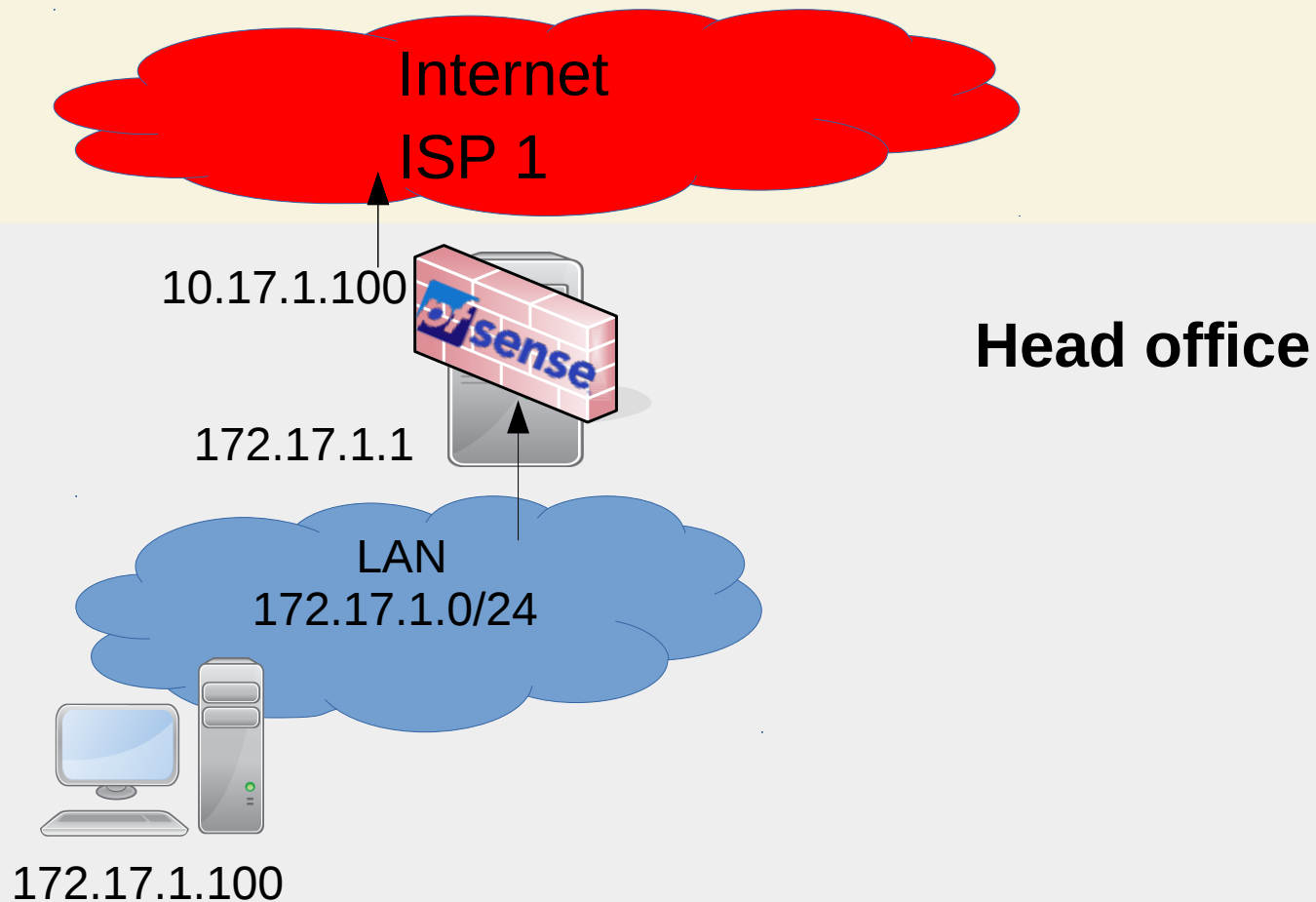
- DHCP Server
- DHCP Relay
- DNS Resolver
- Dynamic DNS
- Load Balancer
- Multi WAN
- Wake on LAN
- VLAN
- Intrusion Detection
- PKI
- HA
- Captive Portal
- Freeradius3
- Squid
- ...
- ...

# Runs On

- Your own hardware
  - Min CPU - 500 Mhz RAM - 512 MB
- Appliances from Netgate
  - Preconfigured and optimized
  - With or without support
- In the cloud
  - Microsoft Azure / Amazon Cloud
- Hardware requirements depend on throughput and installed packages

**It's an easy start**

# Scenario 1: Base Installation



# Demonstration Base Installation

The screenshot shows the pfSense Status Dashboard in a Mozilla Firefox browser window. The browser's address bar shows the URL `https://172.17.1.1`. The dashboard is titled "Status / Dashboard" and features a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two panels: "System Information" and "Netgate Services And Support".

**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)	<ul style="list-style-type: none"><li>127.0.0.1</li><li>10.17.1.99</li><li>8.8.8.8</li></ul>
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**

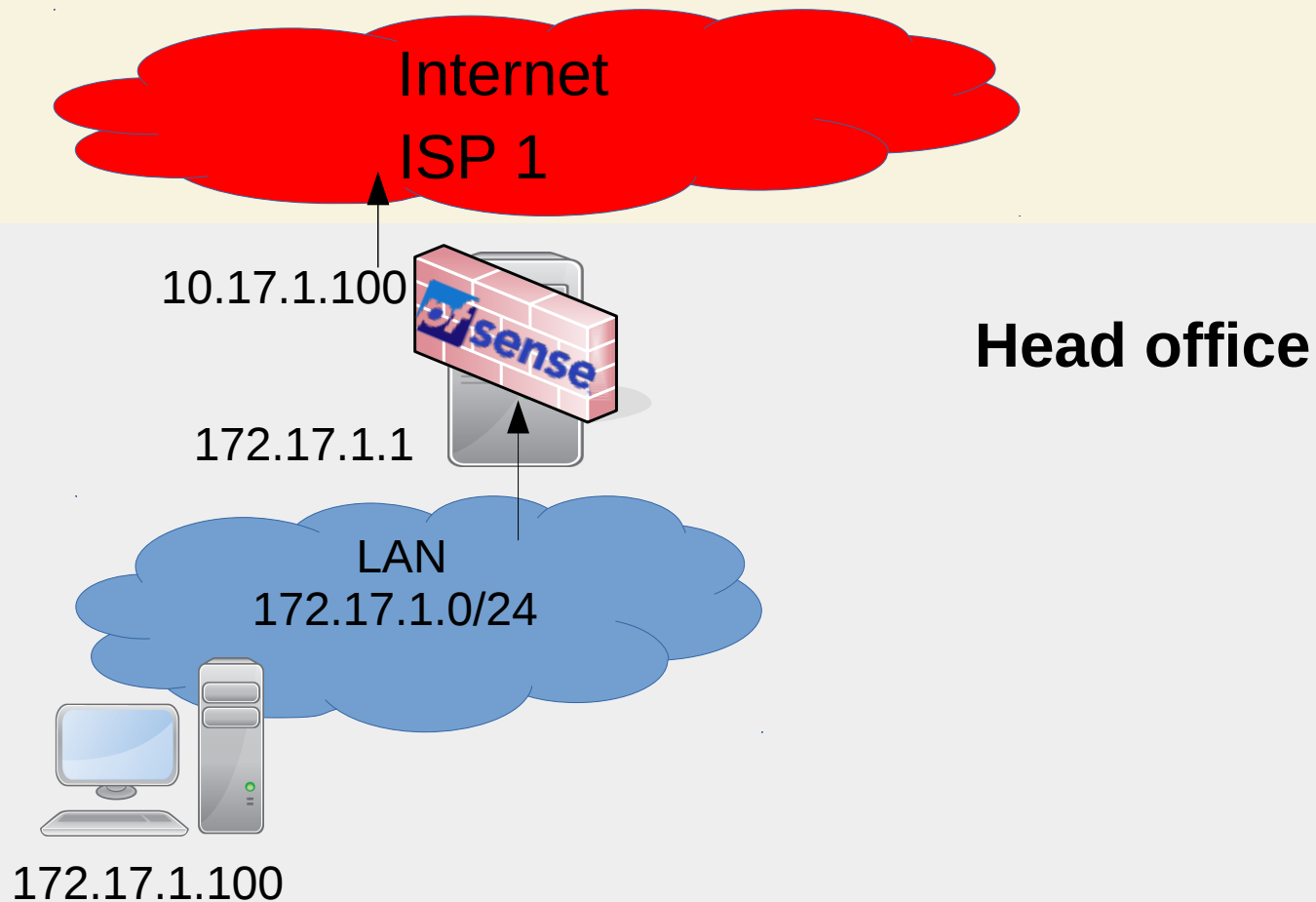
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale, you can register your community support subscription for access to pfSense Gold.

- 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: Base Installation





# Firewall Rules

- Rules are inbound (to the pfSense box)
- First rule wins, the rest will be ignored
- Stateful filtering
- Aliases simplify the administration and reduce possibilities of errors
  - IP addresses
  - Networks
  - Hostnames
  - Ports

**More complex scenarios  
are easy to implement**

# Advanced Features

- VPN
- DMZ and network segmentation
- Bandwidth limitation
- Logs of configuration changes

# Virtual Private Network

- Connection to remote offices or mobile clients
- IPSec
  - Standard clients on OS X, iOS, Android
  - Interoperable
- OpenVPN
  - Clients behind NAT
  - Very easy client configuration



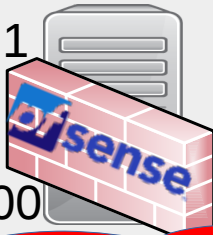
172.18.1.100

**Local branch**

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

**Headquarter**

# Szenario: Connect 2 Offices



- Server
  - Definition of the VPN server
  - Open firewall for OpenVPN
  - Define network traffic for VPN tunnel
- Client
  - Definition VPN client
- Connection test

# Demo: Connect 2 Offices

pfSense COMMUNITY EDITION

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

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	 



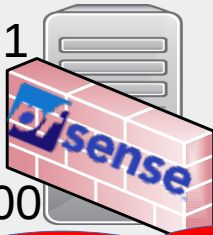
172.18.1.100

**Local branch**

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



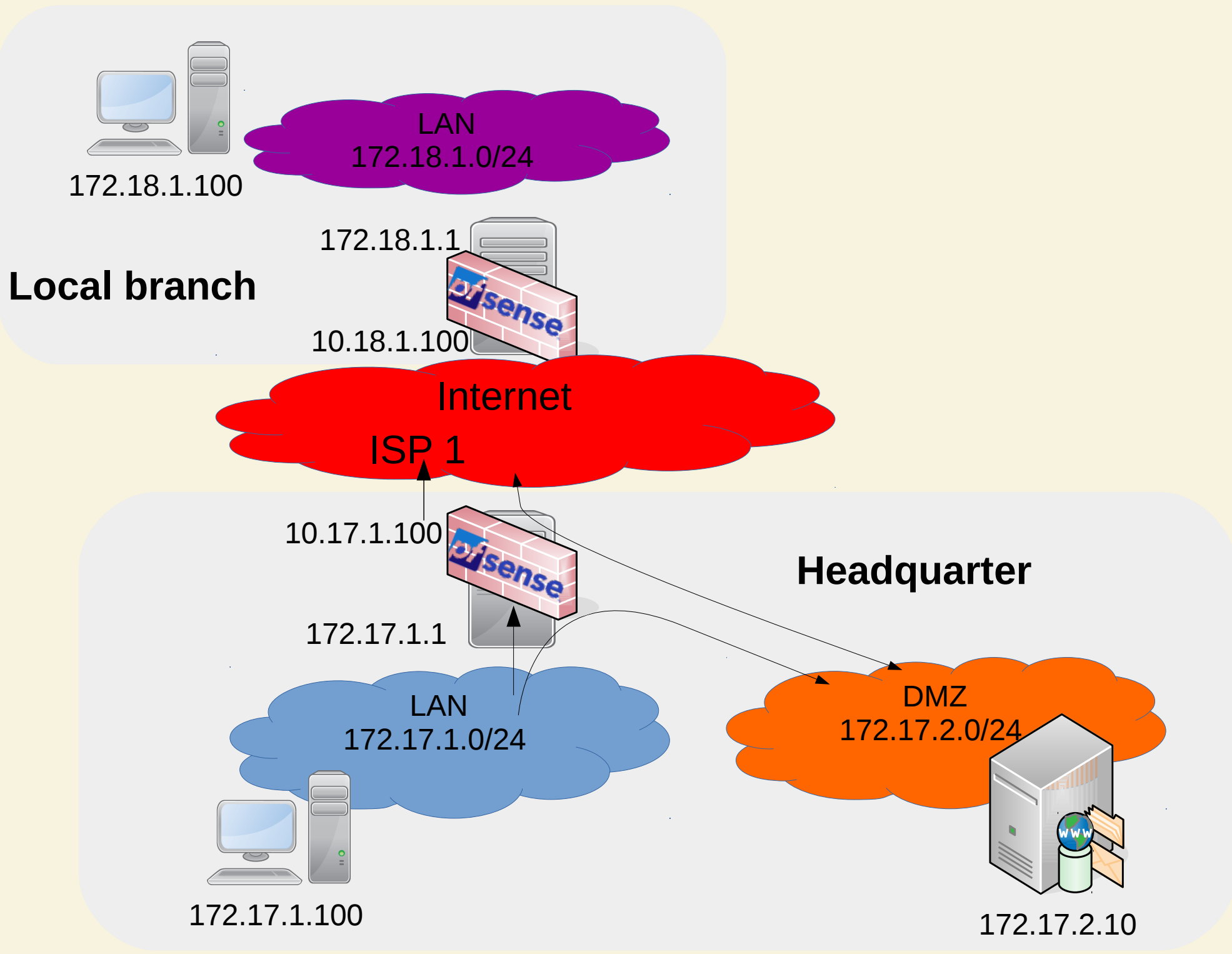
172.17.1.100

**Headquarter**



# Network Segmentation

- Base component of network security
- Physical or virtual (VLAN)
- Privat use: IOT, VOIP, „YourChildsLAN”
- Business use: DMZ, old OS in manufacturing facilities



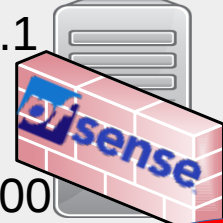
172.18.1.100

LAN  
172.18.1.0/24

Local branch

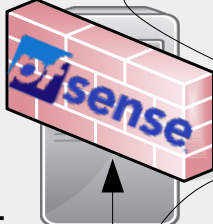
172.18.1.1

10.18.1.100



Internet  
ISP 1

10.17.1.100



Headquarter

172.17.1.1

LAN  
172.17.1.0/24



172.17.1.100

DMZ  
172.17.2.0/24



172.17.2.10

# Szenario 3: DMZ

- Definition Network / DHCP
- Test Ping
  - HQ LAN → DMZ => OK
  - DMZ → HQ Intranet => Error
  - DMZ → Internet => Error
  - Branch → DMZ Server => NA
- Port forward to webserver in DMZ
- Test Webserver
  - Branch → DMZ Server => OK

# Demo: DMZ

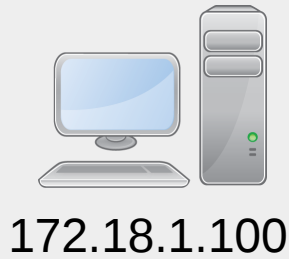
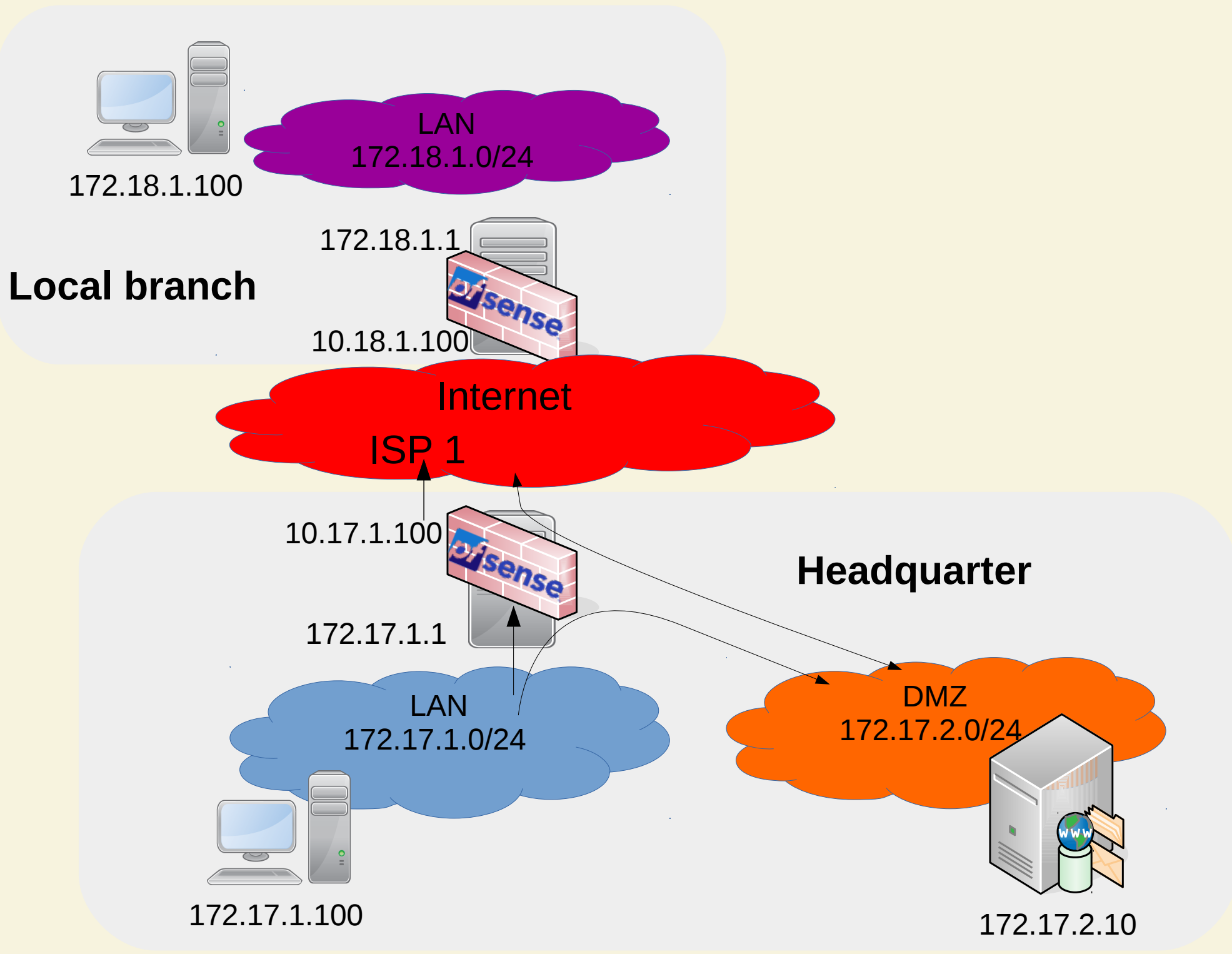
The screenshot shows the pfSense Status Dashboard in a Mozilla Firefox browser window. The browser's address bar displays the URL `https://172.17.1.1`. The dashboard is divided into several panels:

- System Information:** A table providing details about the system, including name, system type, BIOS, version, CPU type, uptime, current date/time, DNS servers, last config change, state table size, MBUF usage, and load average.
- Netgate Services And Support:** A section detailing the contract type (Community Support) and providing resources for support, such as registration, login, and training.
- Interfaces:** A table listing the network interfaces (WAN, LAN, DMZ) and their configurations, including speed and duplex settings.

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)	<ul style="list-style-type: none"><li>127.0.0.1</li><li>10.17.1.99</li><li>8.8.8.8</li></ul>
Last config change	Mon Oct 30 16:26:14 UTC 2017
State table size	0% (33/97000) <a href="#">Show states</a>
MBUF Usage	2% (1266/61006)
Load average	1.12, 0.78, 0.62

Netgate Services And Support	
Contract type	Community Support Community Support Only
<b>NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES</b>	
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.	
<ul style="list-style-type: none"><li><a href="#">Register Your Support Subscription</a></li><li><a href="#">Upgrade Your Support</a></li><li><a href="#">Netgate Global Support FAQ</a></li><li><a href="#">Netgate Professional Services</a></li></ul>	<ul style="list-style-type: none"><li><a href="#">Log into your portal account</a></li><li><a href="#">Community Support Resources</a></li><li><a href="#">Official pfSense Training by Netgate</a></li><li><a href="#">Visit Netgate.com</a></li></ul>
If you decide to purchase a Netgate Global Support subscription, you <b>MUST</b> have your <b>Netgate Device ID (NDI)</b> 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 <a href="#">here</a> .	

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

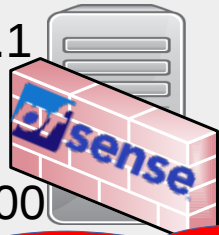


LAN  
 $172.18.1.0/24$

**Local branch**

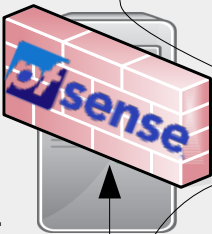
$172.18.1.1$

$10.18.1.100$



Internet  
ISP 1

$10.17.1.100$



**Headquarter**

$172.17.1.1$

LAN  
 $172.17.1.0/24$



$172.17.1.100$

DMZ  
 $172.17.2.0/24$



$172.17.2.10$

# Scenario 4: Traffic Shaping

- “Managed unfairness of bandwidth” instead of FIFO
- Queues define priorities
- Rules manage the queues
- Two methods
  - Limiter: hard boundary
  - Traffic Shaper (ALTQ)

# Demo 4: Traffic Shaping

The screenshot shows a web browser window displaying the PfSense Firewall Rules configuration for the LAN interface. The browser address bar shows the URL `https://172.17.1.1:3000/firewall_rules.php?if=lan`. The PfSense interface shows the 'Firewall / Rules / LAN' page with tabs for Floating, WAN, LAN, DMZ, and OpenVPN. The LAN tab is selected, and the 'Rules (Drag to Change Order)' table is visible. The table has columns for States, Protocol, Source, Port, Destination, and Priority. There are three rules listed:

States	Protocol	Source	Port	Destination	Priority
0 / 229.84 MIB	*	*	*	LAN Address	3
4 / 441.13 MIB	IPv4 *	LAN net	*	*	2
0 / 0 B	IPv6 *	LAN net	*	*	2

Below the table, there is an information icon. To the right, a terminal window titled 'Terminal - hbauer@zentrale-client-1: ~' is open, showing the output of the `./speedtest.py` command. The terminal output shows the speedtest.net configuration, server selection, and download/upload speeds for two consecutive tests.

```
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

- Necessary to be GDPR compliant
- Automatic backup of every change
- “Go back to last version” (save your a\*\*)
- Who did what at what time?



# Demo: Configuration History

The screenshot shows a web browser window displaying the configuration history for a NAT rule in pfSense. The browser's address bar shows the URL: `https://172.17.1.1:3000/diag_confbak.php?diff=Diff&newtime=1509389787&oldtime=1509389397`. The page title is "zentral-pfsense.pfsense-lab.lcl - Diagnostics: Backup & Restore: Config History - Mozilla Firefox".

The configuration history is displayed as a list of XML snippets, with each snippet representing a configuration change. The snippets are color-coded: green for additions, red for deletions, and grey for unchanged parts. The current configuration is highlighted in green.

```
<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>
```

# Summary

- Standard device supplied by your provider do not match your growing need.
- pfSense stands out due to
  - Low / no pre-investments
  - Enterprise level feature set
  - Enterprise support if needed
  - No running license fees of individual capabilities (ports / user)
- Ideal start for
  - Small and medium companies
  - High end home office
  - Domestic home



# Secure your Networks with the Opensource Firewall pfSense



[hagen.bauer@rusticus-consulting.de](mailto:hagen.bauer@rusticus-consulting.de)

