



Secure your Networks with the Opensource Firewall pfSense



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?

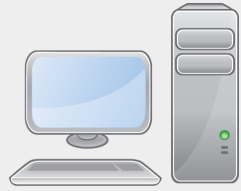
**My provider gave
me a firewall.**

Firewall Market (roughly)

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

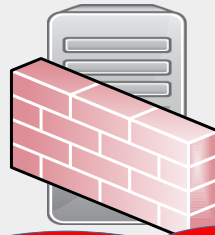
Devices for Home Use

- 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

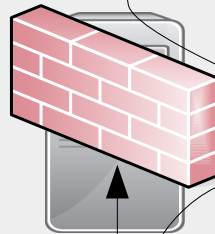


LAN

**local branch
your parents**



Internet



LAN



DMZ
IOT
VOIP



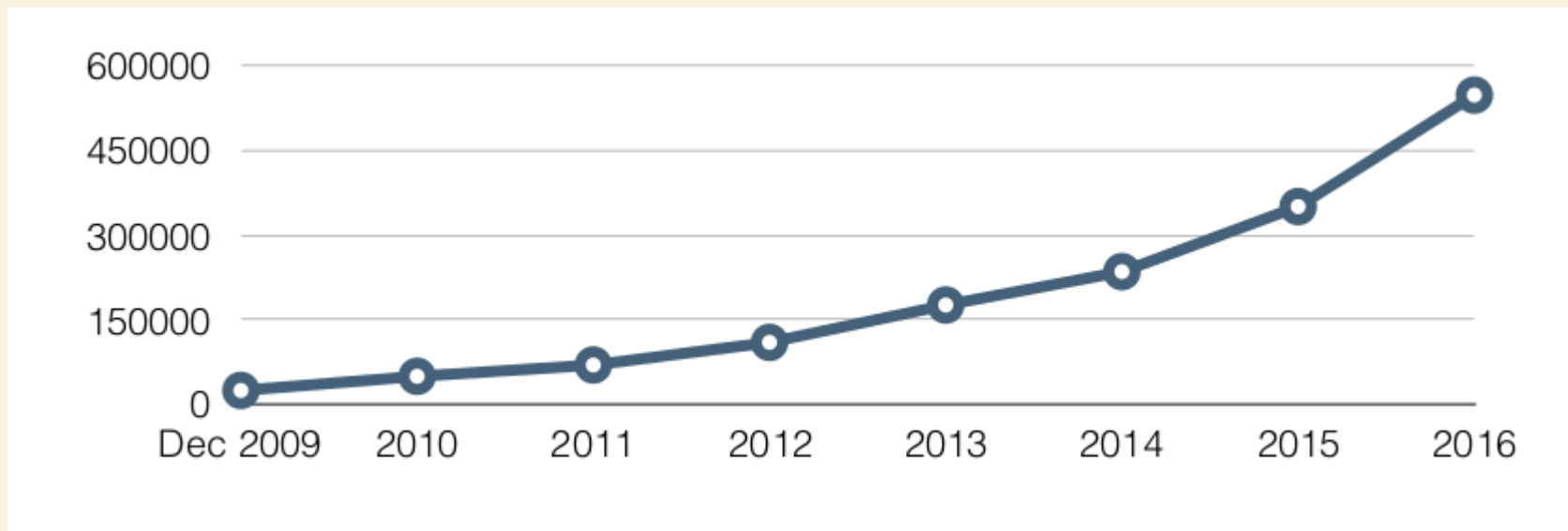
So what exactly is pfSense?

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

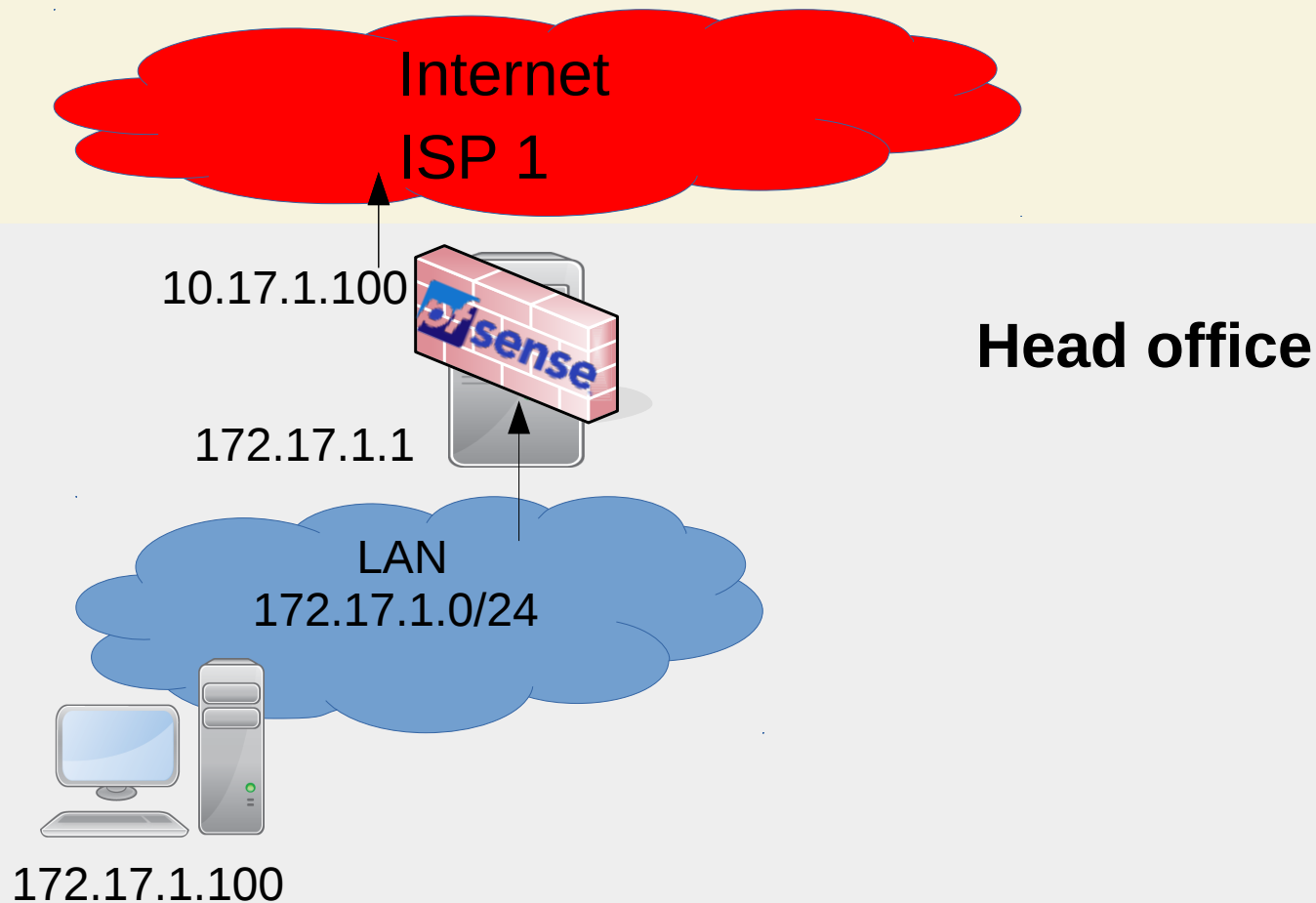
- DHCP Server
- DHCP Relay
- DNS Resolver
- Dynamic DNS
- Load Balancer
- Multi WAN
- Wake on LAN
- VLAN
- Intrusion Detection
- PKI
- HA
- Captive Portal
- Freeradius3
- Squid
- ...
- ...

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

Applications zentral-pfsense.pfsense... 16:13 hbauer

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

zentral-pfsense.pfsen... x +

https://172.17.1.1 Search

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)	<ul style="list-style-type: none">127.0.0.110.17.1.998.8.8.8
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

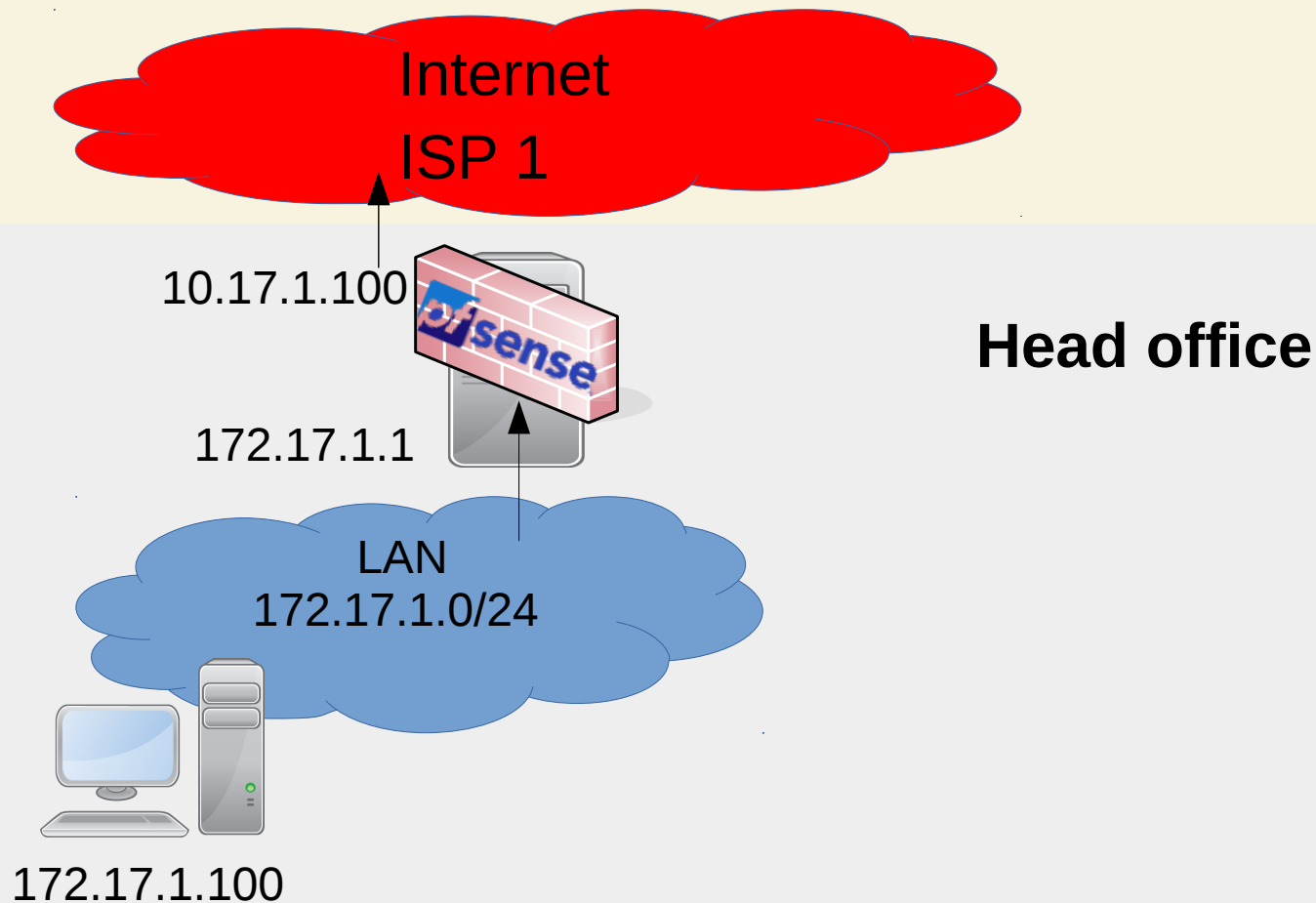
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale, you can [register](#) your community support subscription for access to [pfSense Gold](#).

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



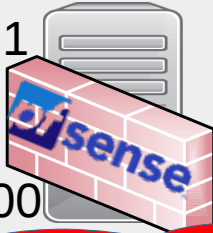
172.18.1.100

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

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	✓ ↻



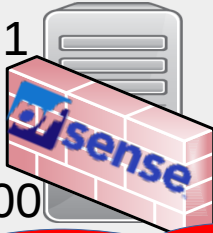
172.18.1.100

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

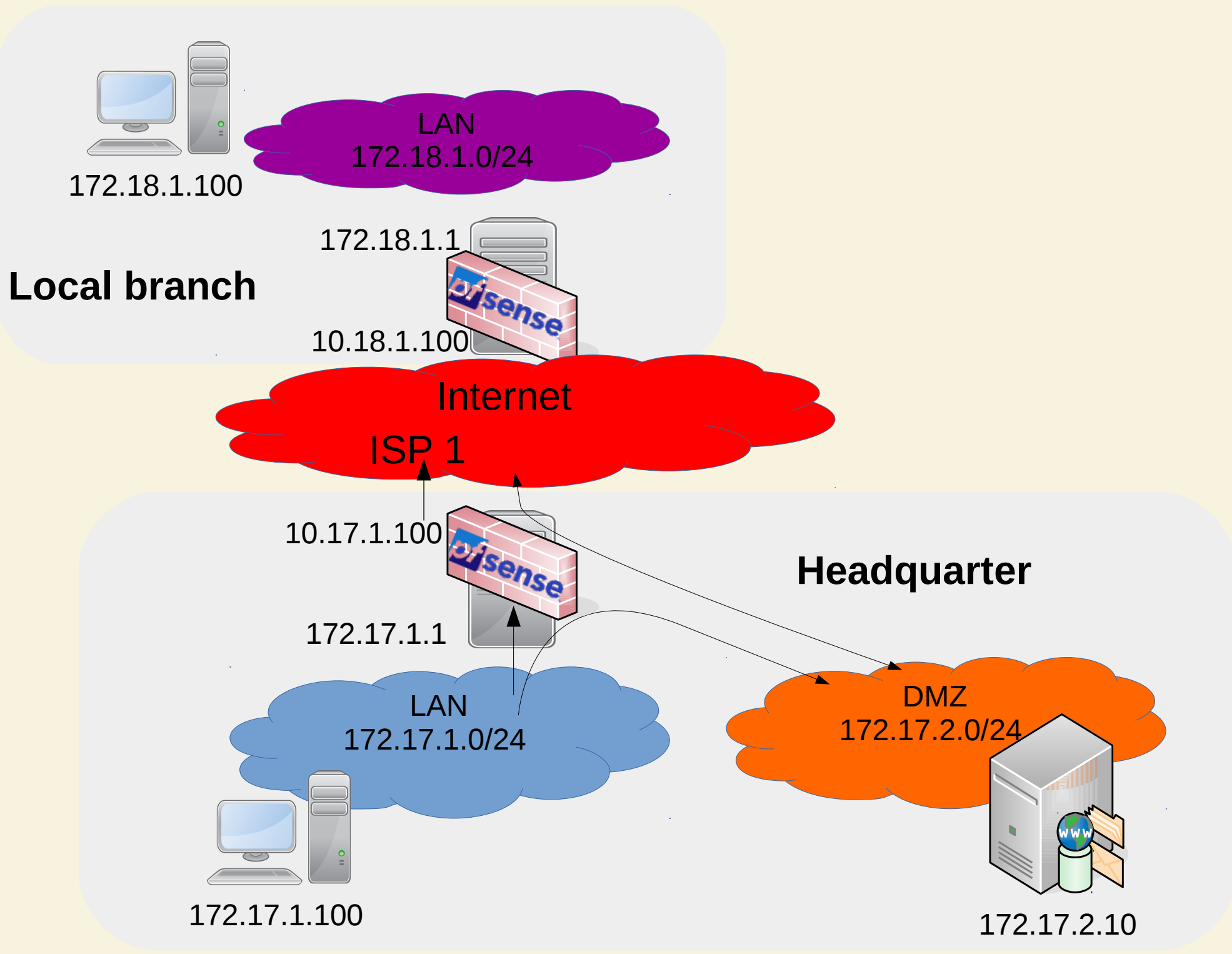


172.17.1.100

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

pfsense

Internet
ISP 1

10.17.1.100

172.17.1.1

pfsense

LAN
172.17.1.0/24

172.17.1.100

Headquarter

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 a web browser window displaying the pfSense status dashboard. The browser's address bar shows the URL `https://172.17.1.1`. The dashboard is divided into two main panels. The left panel, titled "System Information", contains a table with details about the system, including its name, system type, BIOS information, version, CPU type, uptime, current date/time, DNS servers, last configuration change, state table size, MBUF usage, and load average. The right panel, titled "Netgate Services And Support", displays the contract type as "Community Support" and provides links to various support resources. Below this, a red box contains a warning about the importance of the Netgate Device ID (NDI) for support. At the bottom right, there is a table titled "Interfaces" showing the configuration for WAN, LAN, and DMZ interfaces.

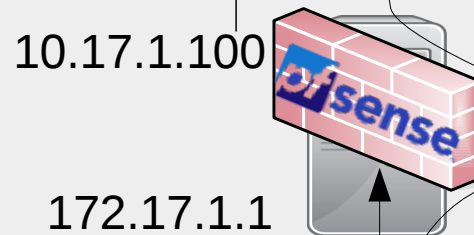
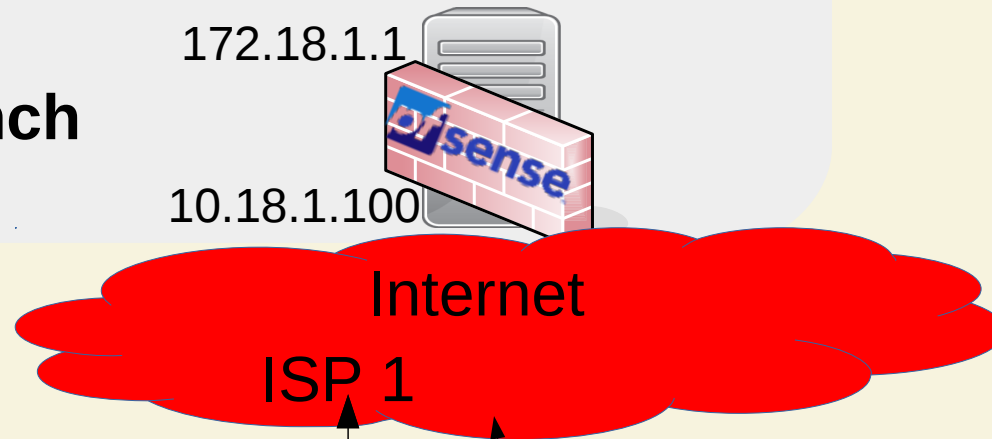
System Information	
Name	zentral-pfsense.pfsense-lab.lcl
System	VirtualBox Virtual Machine Netgate Device ID: 0a09bc4a02797edae681
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.4.1-RELEASE (amd64) built on Sun Oct 22 17:26:33 CDT 2017 FreeBSD 11.1-RELEASE-p2 The 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">127.0.0.110.17.1.998.8.8.8
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			
<p>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.</p> <ul style="list-style-type: none">Register Your Support SubscriptionLog into your portal accountUpgrade Your SupportCommunity Support ResourcesNetgate Global Support FAQOfficial pfSense Training by NetgateNetgate Professional ServicesVisit Netgate.com			
<p>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.</p>			

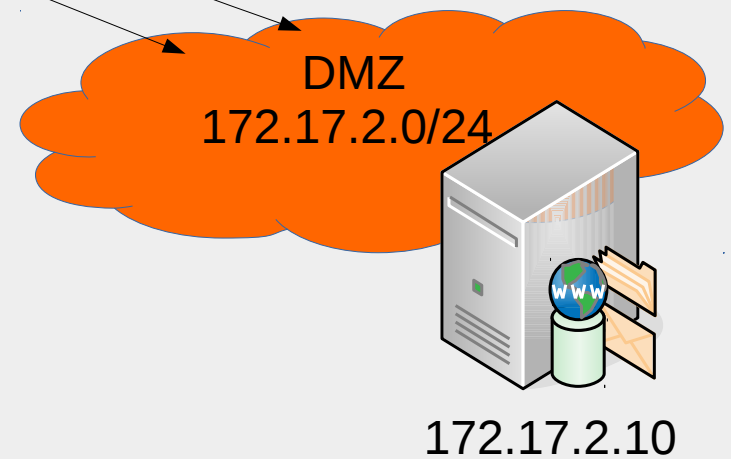
Interfaces			
WAN	↑	1000baseT <full-duplex>	10.17.1.100
LAN	↑	1000baseT <full-duplex>	172.17.1.1
DMZ	↑	1000baseT <full-duplex>	172.17.1.1



Local branch



Headquarter



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 displays the PfSense web interface in a Mozilla Firefox browser. The browser's address bar shows the URL `https://172.17.1.1:3000/firewall_rules.php?if=lan`. The PfSense interface has a top navigation bar with the following items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and zentral-pfsense. The main content area is titled "Firewall / Rules / LAN" and includes tabs for Floating, WAN, LAN (selected), DMZ, and OpenVPN. Below these tabs is a table titled "Rules (Drag to Change Order)".

	States	Protocol	Source	Port	Destination	
<input checked="" type="checkbox"/>	0 / 229.84 MiB	*	*	*	LAN Address	3
<input type="checkbox"/> <input checked="" type="checkbox"/> ⚙	4 / 441.13 MiB	IPv4 *	LAN net	*	*	*
<input type="checkbox"/> <input checked="" type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*

Below the table is an information icon (i). Overlaid on the right side of the interface is a terminal window titled "Terminal - hbauer@zentrale-client-1: ~". The terminal shows the execution of the `./speedtest.py` script, which performs speed tests using speedtest.net. The output of the first test shows a download speed of 78.17 Mbit/s and an upload speed of 5.87 Mbit/s. The second test shows a download speed of 2.75 Mbit/s and an upload speed of 1.05 Mbit/s.

```
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

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>
```

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

