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?

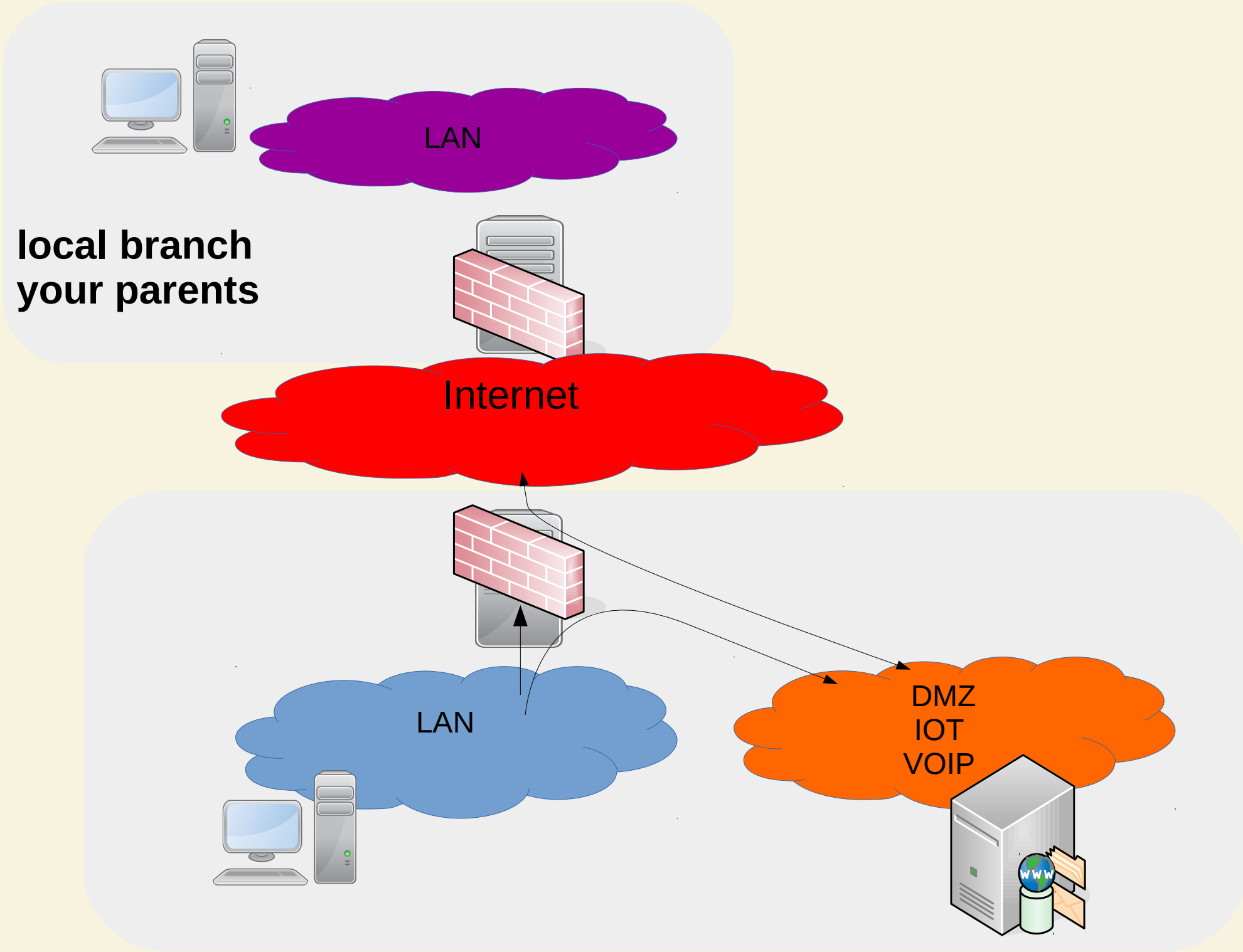
My provider gave me a firewall.

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
WWW

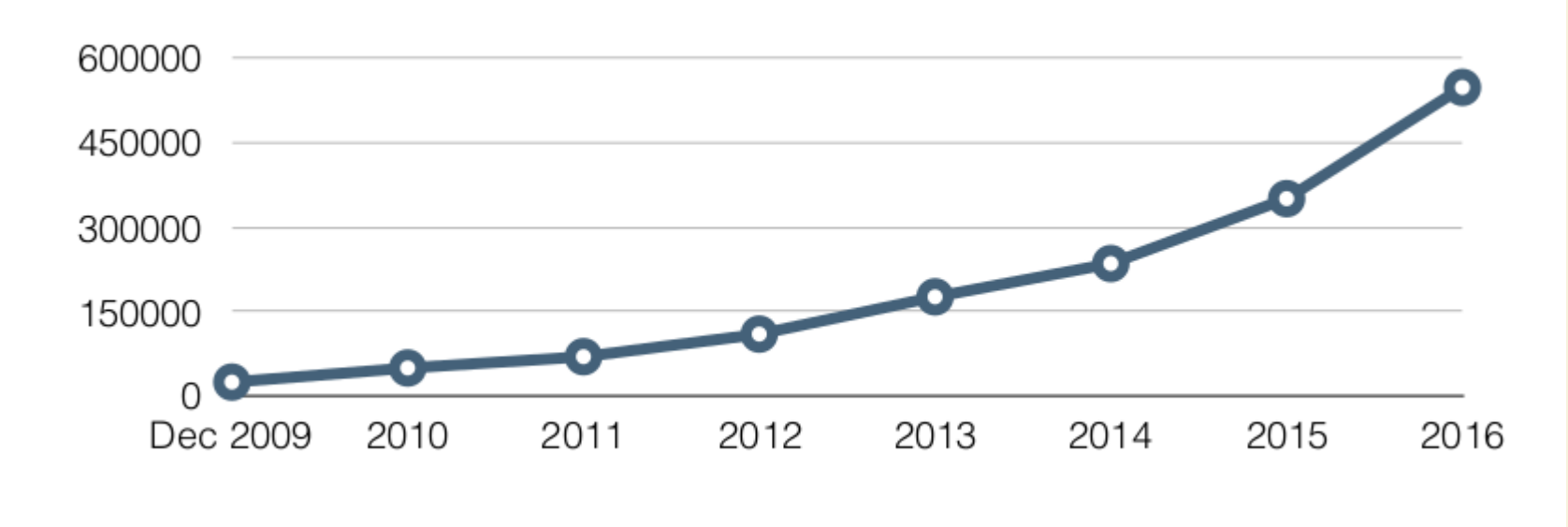
So what exactly is pfSense?

pfSense Overview

- Based on FreeBSD
  - Popular OS plaform 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 then 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

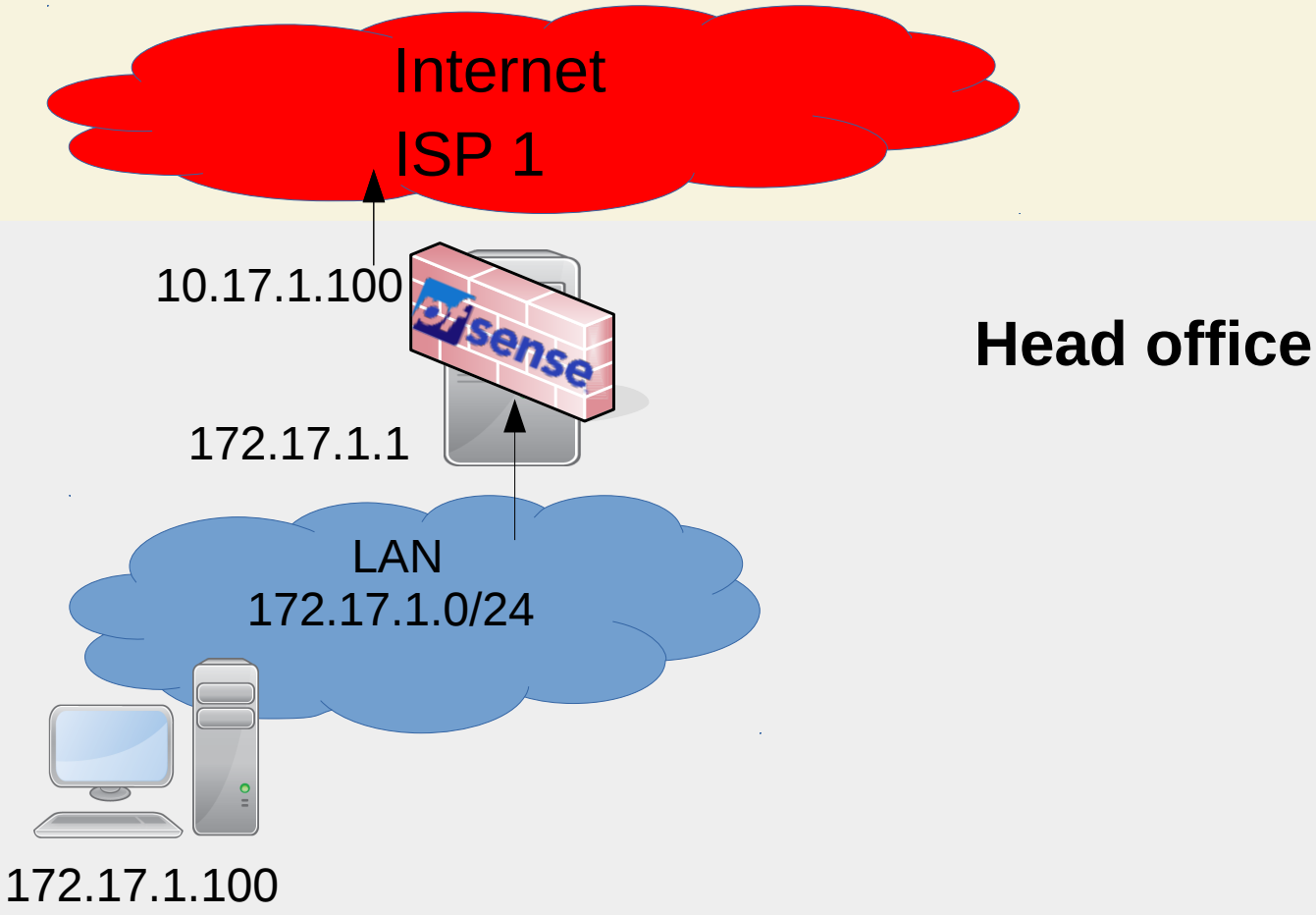
- DHCP Server
- DHCP Relay
- DNS Resolver
- Dynamic DNS
- Load Balancer
- Multi WAN
- Wake on LAN
- VLAN
- Intrusion Detection
- PKI
- HA
- Captive Portal
- Freeradius3
- Squid
- …
- …

Runs On

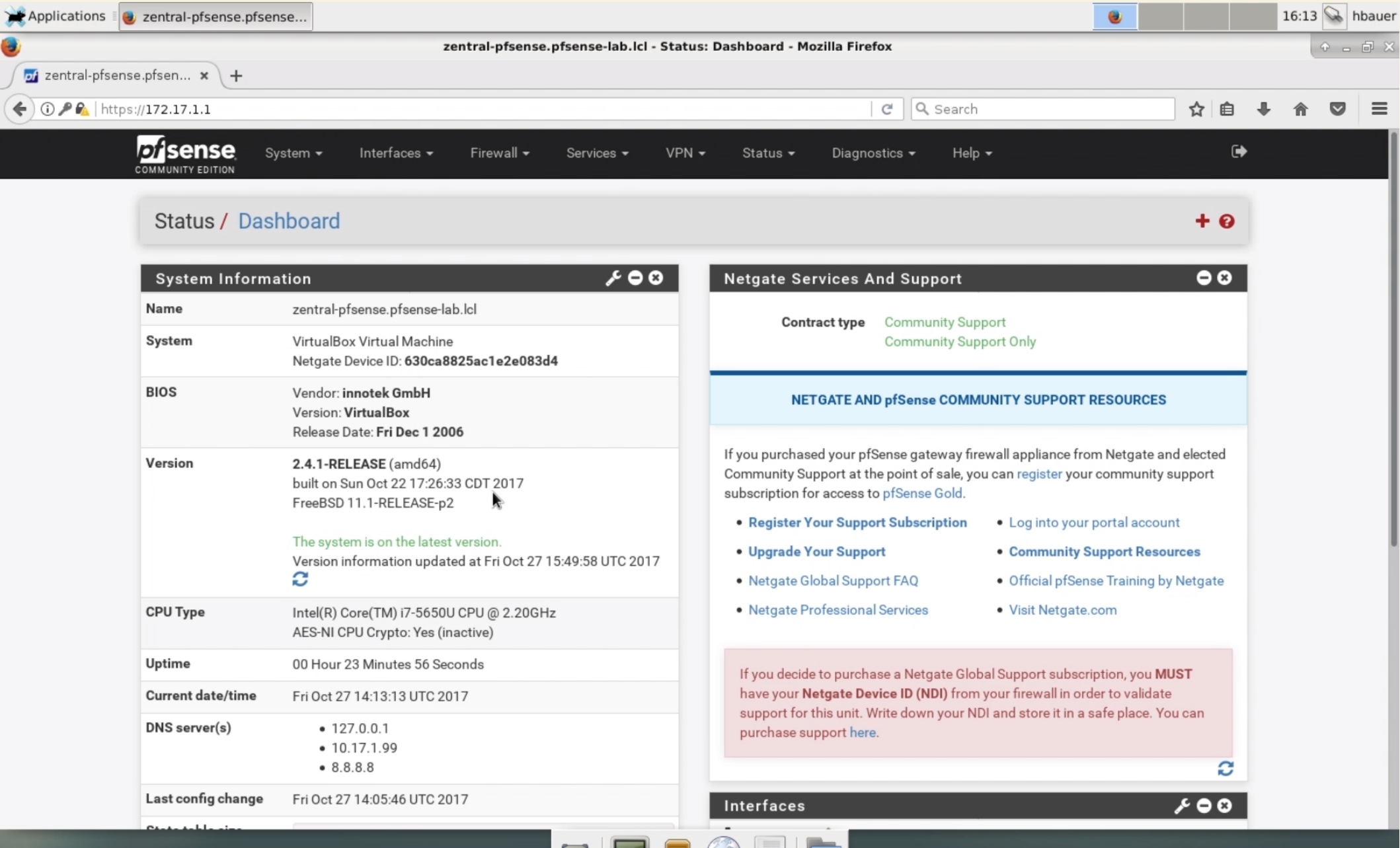
- Your own hardware
  - Min CPU - 500 Mhz RAM - 512 MB
- Appliances from Netgate
  - Preconfigured and optimized
  - With or without support
- In the cloud
  - Microsoft Azure / Amazon Cloud
- Hardware requirements depend on throughput and installed packages

It’s an easy start

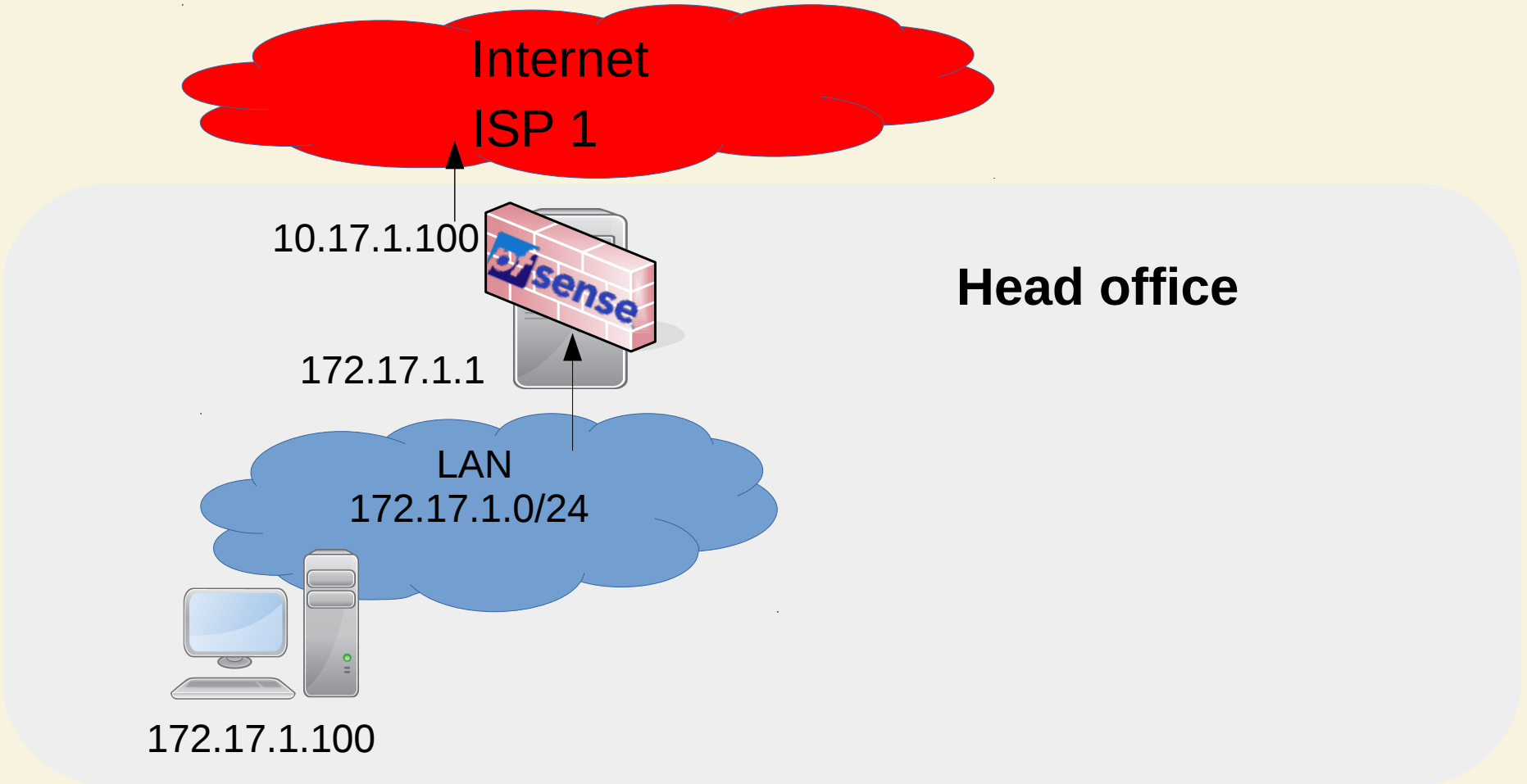
Scenario 1: Base Installation



Demonstration Base Installation



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

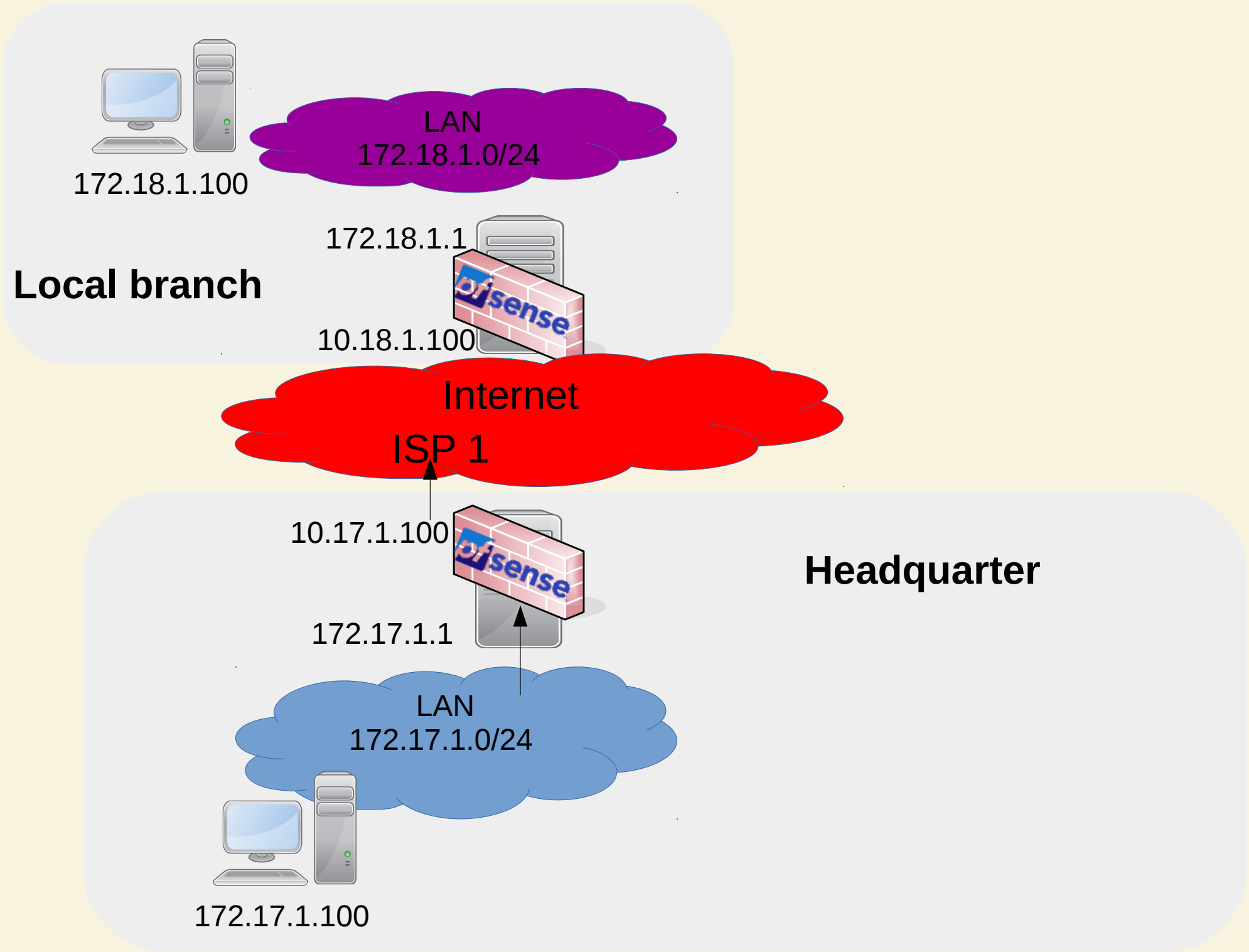
More complex scenarios are easy to implement

Advanced Features

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

Virtual Private Network

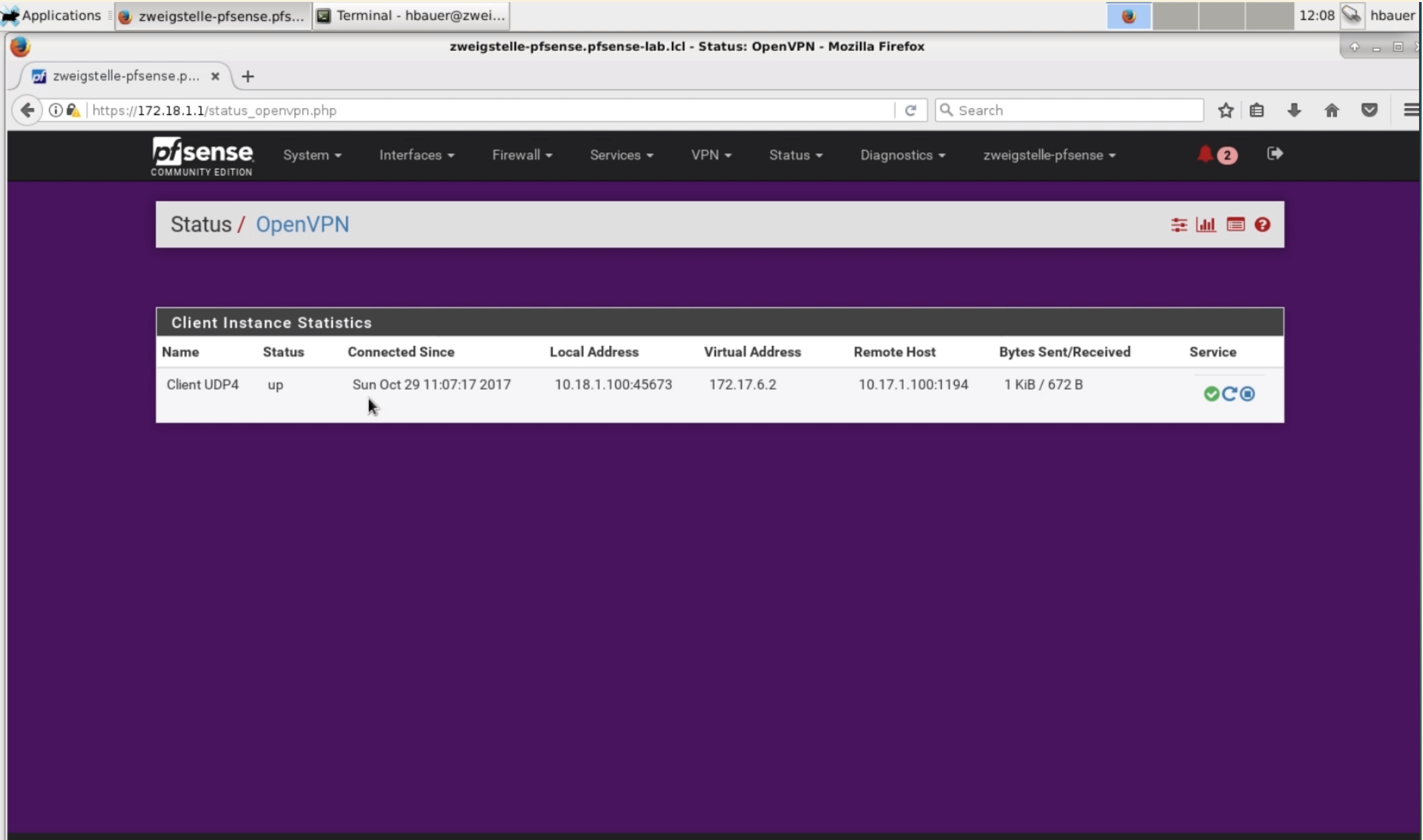
- Connection to remote offices or mobile clients
- IPSec
  - Standard clients on OS X, iOS, Android
  - Interoperable
- OpenVPN
  - Clients behind NAT
  - Very easy client configuration

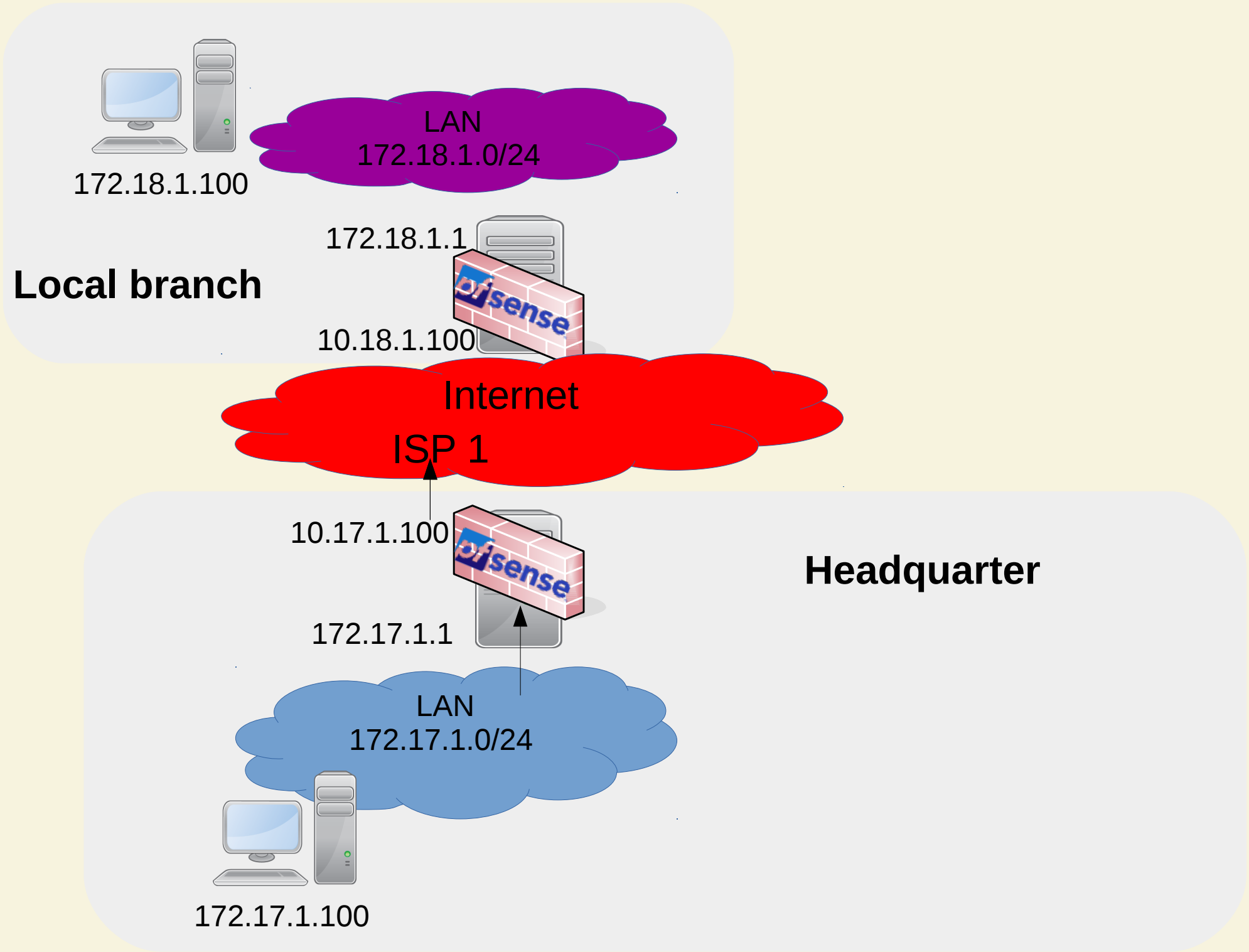

LAN
172.18.1.0/24
172.18.1.100
172.18.1.1
Local branch
10.18.1.100
Internet
ISP 1
10.17.1.100
Headquarter
172.17.1.1
LAN
172.17.1.0/24
172.17.1.100

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

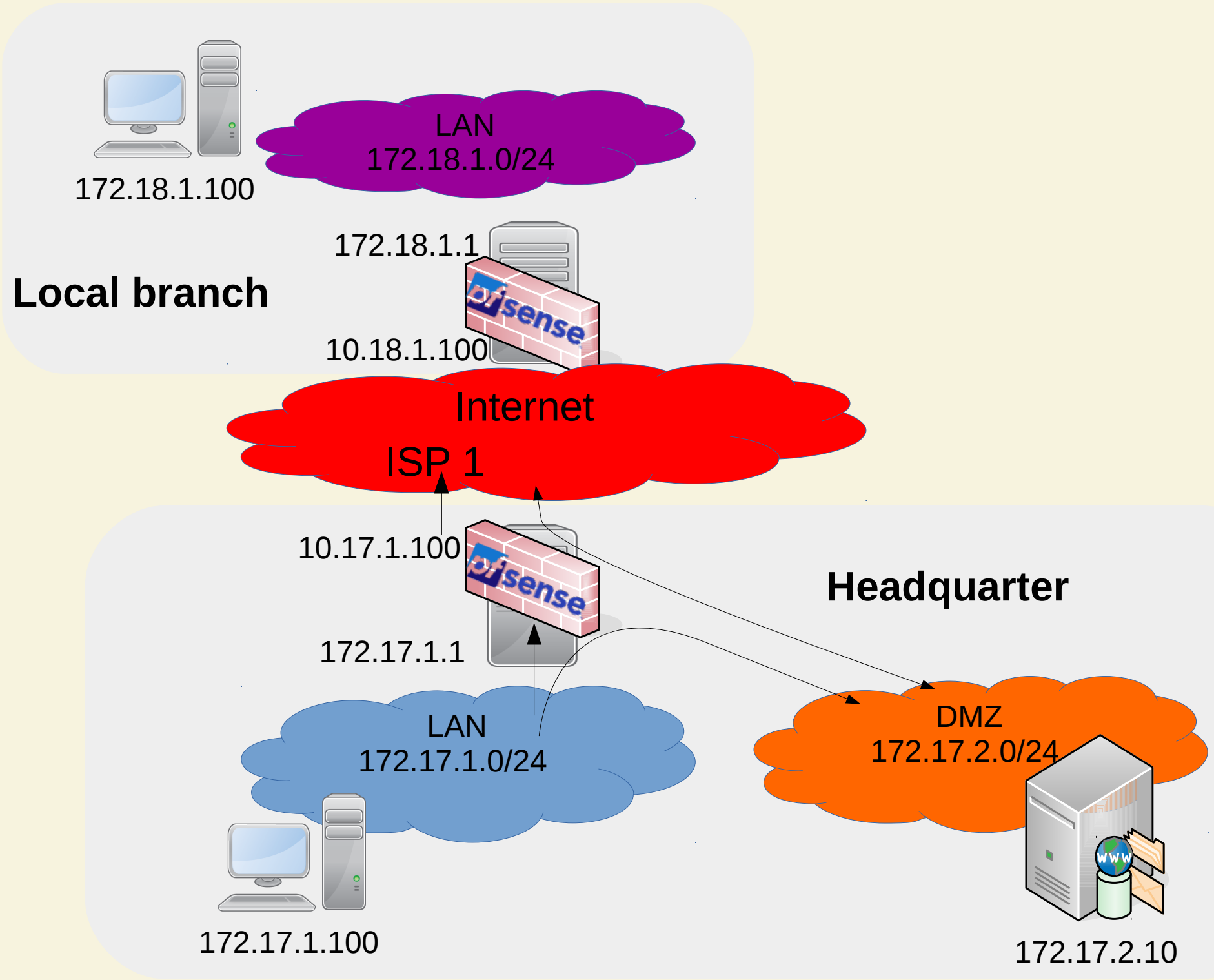
Demo: Connect 2 Offices




LAN
172.18.1.0/24
172.18.1.100
172.18.1.1
Local branch
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

Network Segmentation

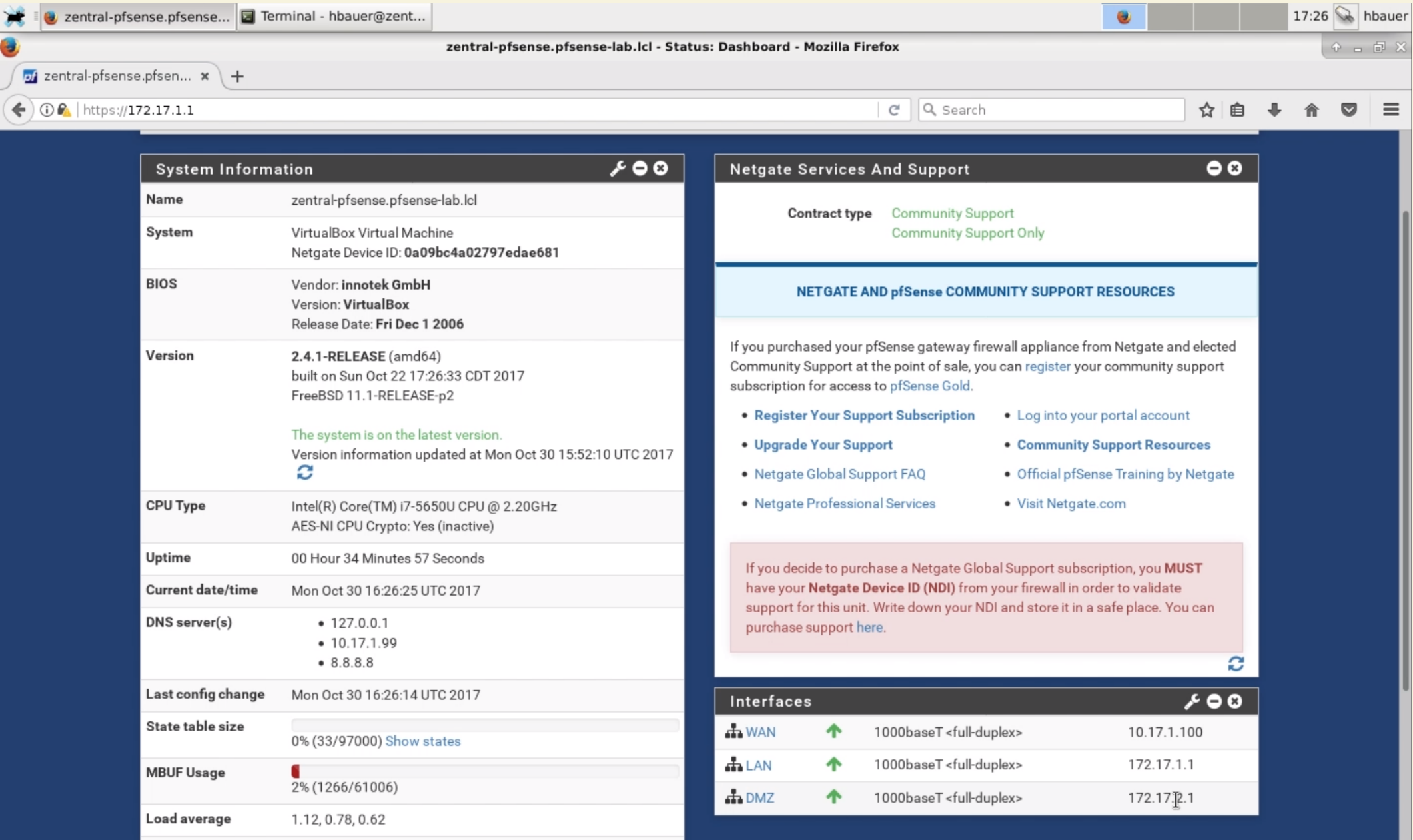
- Base component of network security
- Physical or virtual (VLAN)
- Privat use: IOT, VOIP, „YourChildsLAN”
- Business use: DMZ, old OS in manufacturing facilities

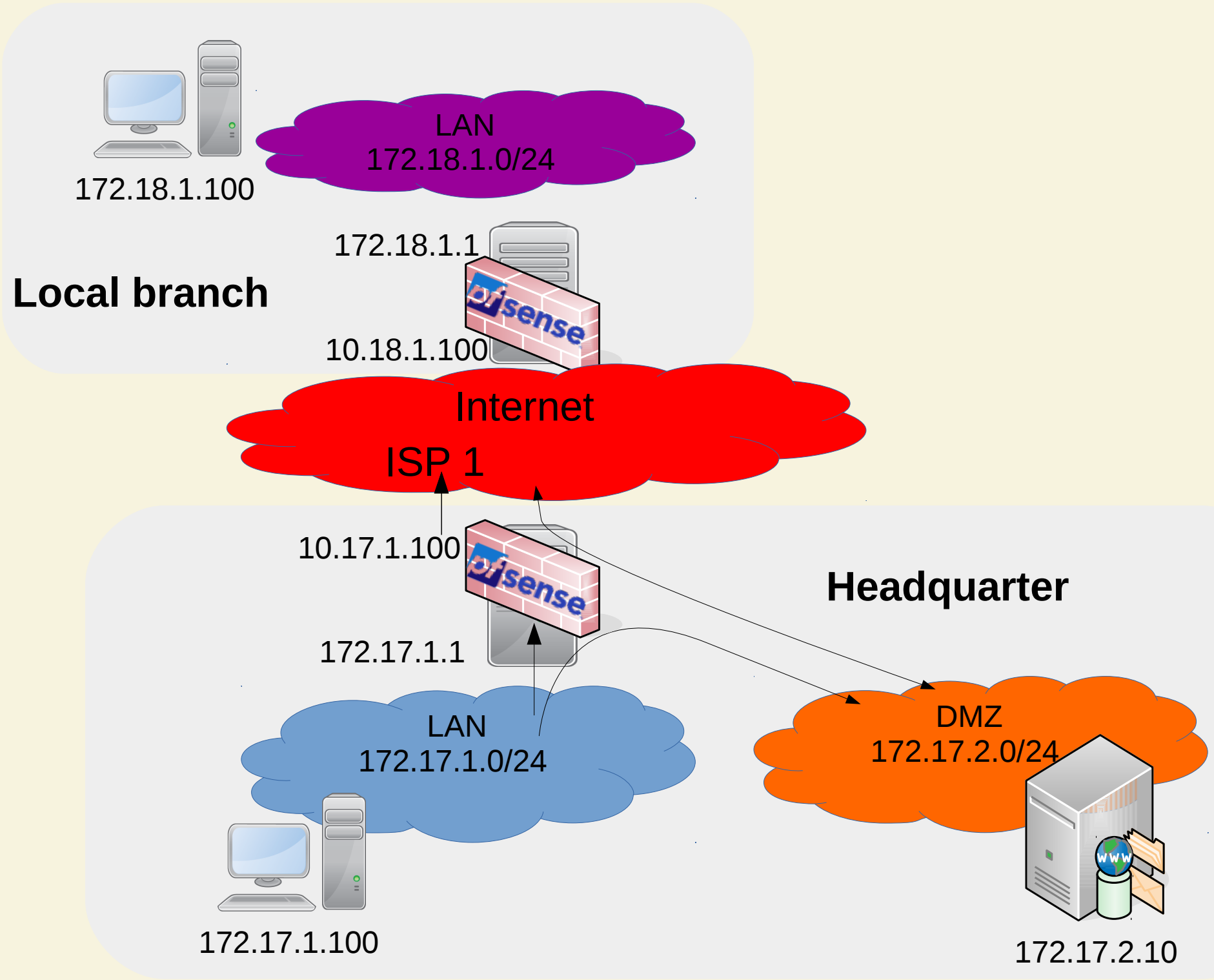

LAN
172.18.1.0/24
172.18.1.100
172.18.1.1
Local branch
10.18.1.100
Internet
ISP 1
10.17.1.100
Headquarter
172.17.1.1
LAN
172.17.1.0/24
DMZ
172.17.2.0/24
172.17.1.100
172.17.2.10

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

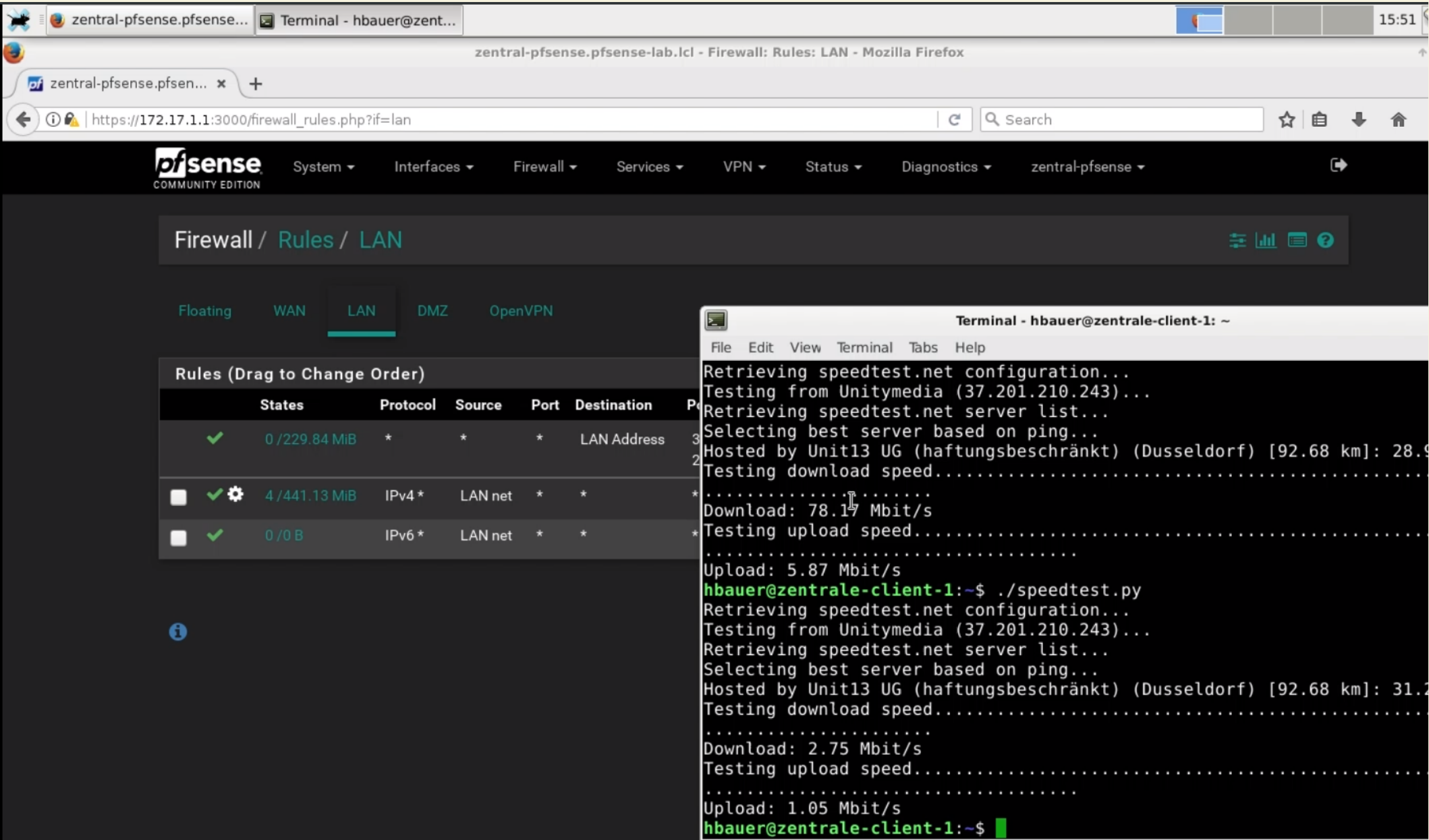

zentral-pfsense.pfsense...
Terminal - hbauer@zent...
17:26
hbauer
zentral-pfsense.pfsense-lab.lcl - Status: Dashboard - Mozilla Firefox
zentral-pfsen...
https://172.17.1.1
Search
System Information
Name
zentral-pfsense.pfsense-lab.lcl
System
VirtualBox Virtual Machine
Netgate Device ID: 0a09bc4a02797edae681
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>
172.17.2.1


LAN
172.18.1.0/24
172.18.1.100
172.18.1.1
Local branch
10.18.1.100
Internet
ISP 1
10.17.1.100
Headquarter
172.17.1.1
LAN
172.17.1.0/24
DMZ
172.17.2.0/24
172.17.1.100
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)

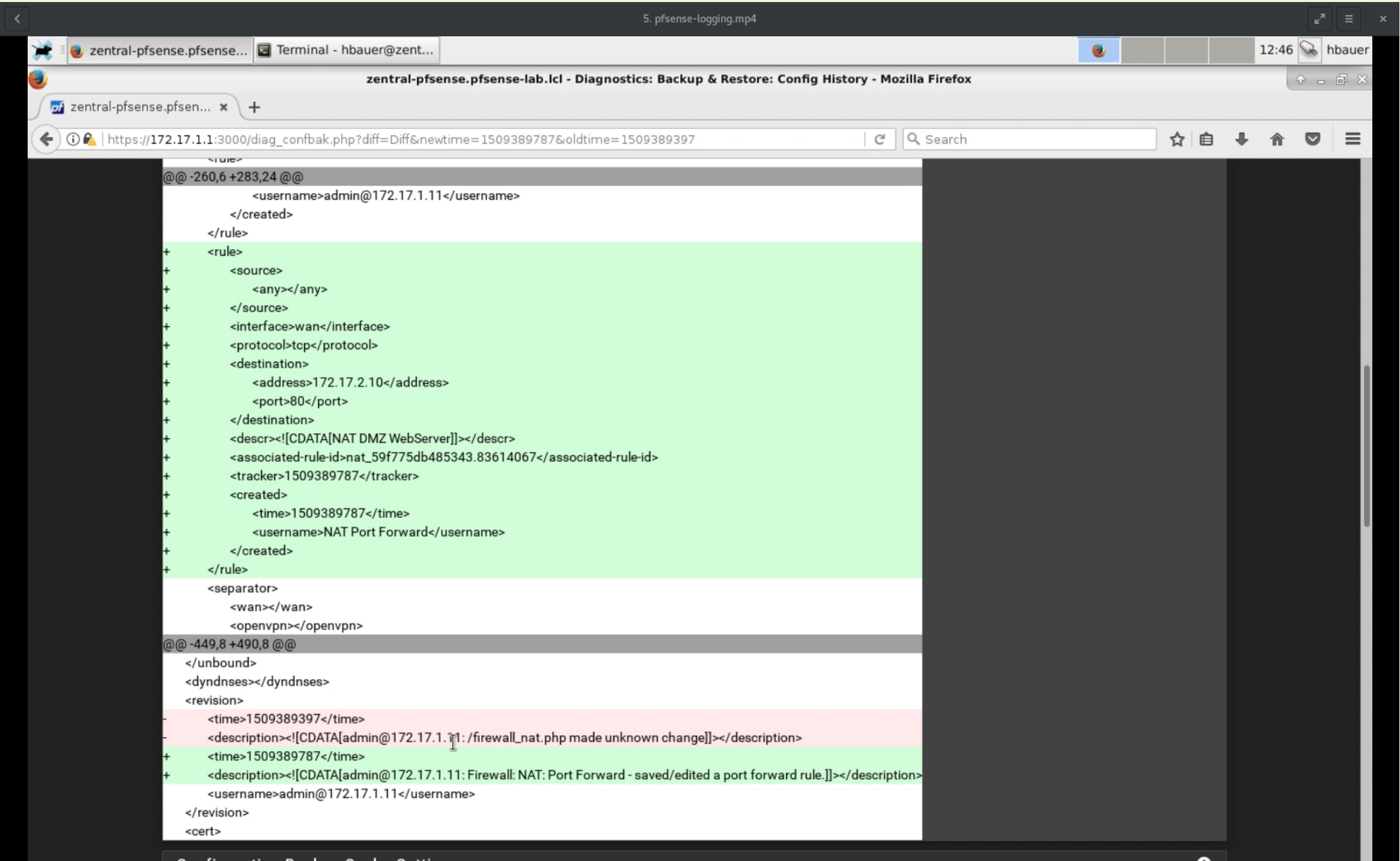
Demo 4: Traffic Shaping



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



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