

Firewall mit pfSense

PC-Treff-BB
Roland Egeler

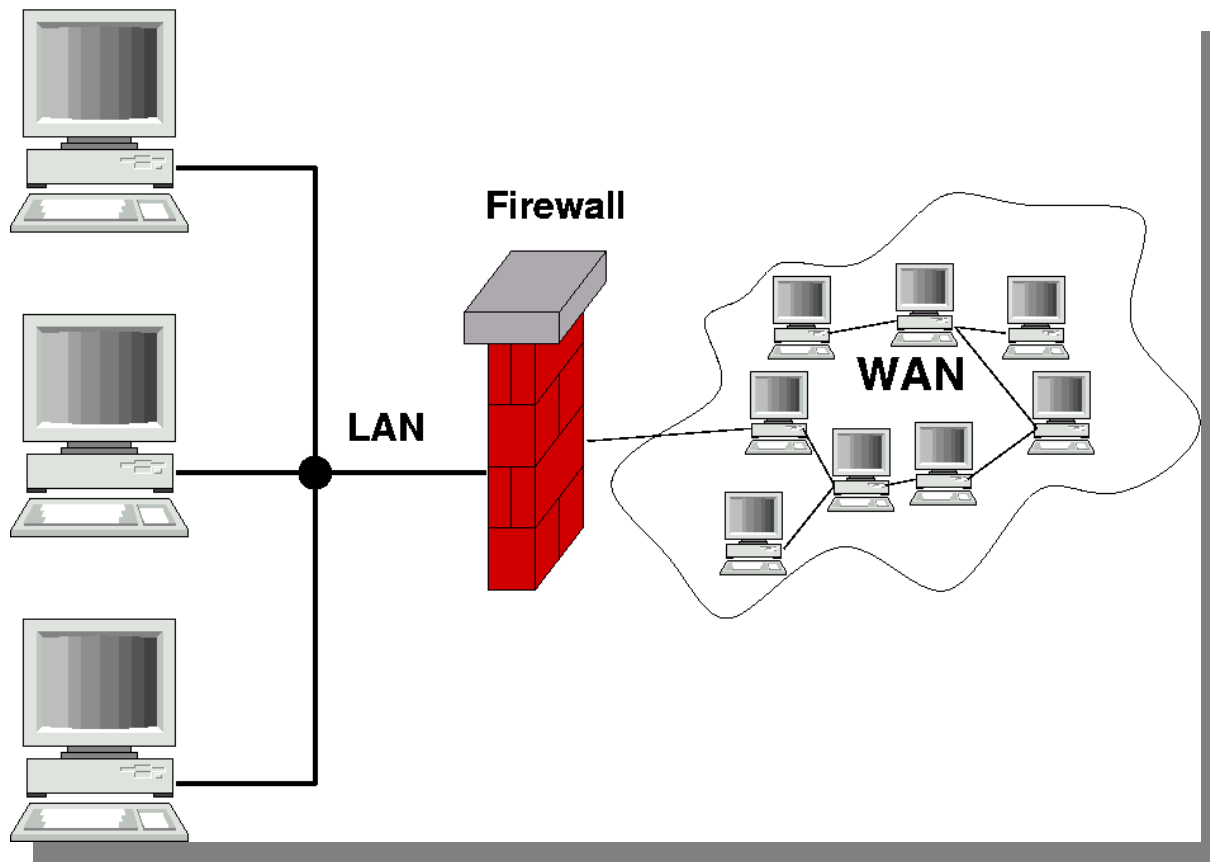
Firewall

Was ist eine Firewall?

- System zum Absichern von Netzwerkverkehr
- Datenpakete werden anhand von Regeln durchgelassen oder nicht (Paketfilter)
- Firewall kann Softwarelösung sein
- Als Teil des Betriebssystems bei Linux, OS X, Windows (Personal Firewall)
- Hardwarelösung besteht aus einem dedizierten Rechner mit mehreren Netzwerkschnittstellen
- Selbstbau möglich

Firewall

Veranschaulichung^[1]



Firewall

Warum mehrere Netzwerkschnittstellen?

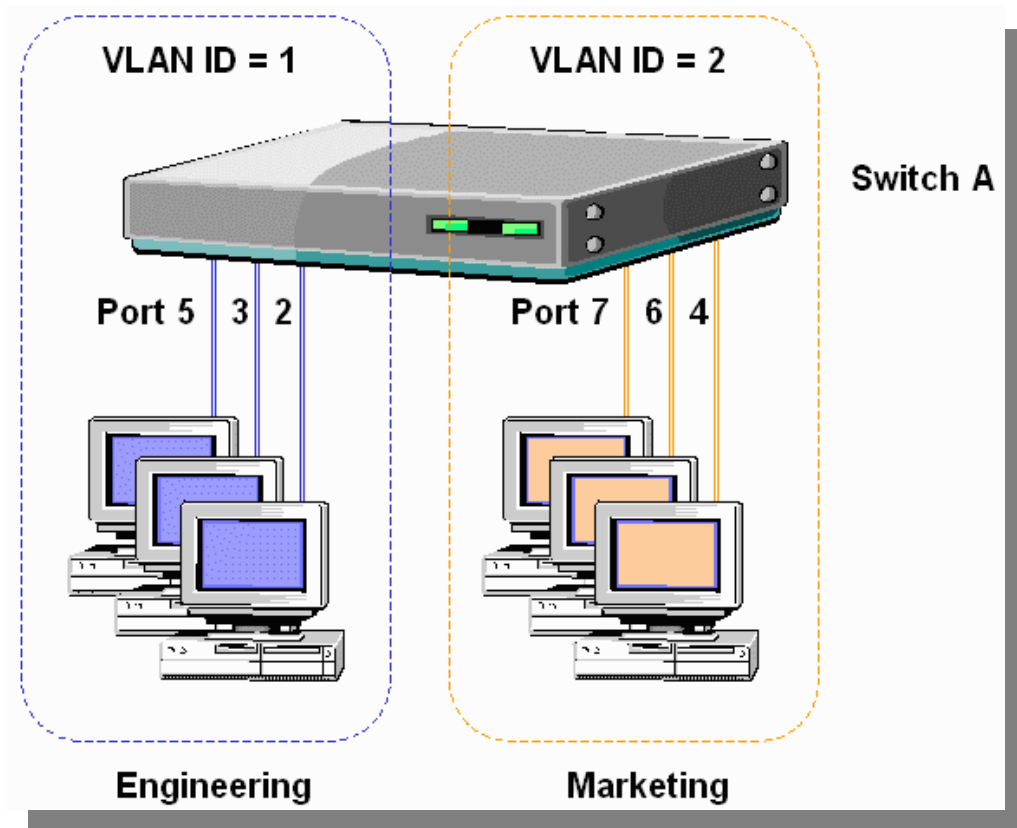
- Zur echten Trennung von Teilnetzen
- Man könnte mehrere logische Teilnetze in einem physikalischen Netz laufen lassen
- Trennung nur anhand von IP-Adressen
- Wer es schafft, alle Pakete zu lesen, kann den Verkehr der anderen Teilnetze mitlesen
- Leicht zu überlisten, da Methoden bekannt
- Switche durch MAC-Flooding in Hub-Modus versetzen

Firewall

Warum mehrere Netzwerkschnittstellen?

- Spezialfall „VLAN“ kann Firewallaufgaben übernehmen
- Logik steckt z.B. im Switch
- Mehrkosten und Administrationsaufwand
- Trennung der logischen Netze durch „Tagging“
- Markierte Pakete dürfen nur in bestimmte Netze
- Eventuelle Probleme durch verlängerte Pakete
- Nicht jede Hardware unterstützt Tags
- Man muss fremder Hard- und Software vertrauen

Veranschaulichung VLAN^[2]



Firewall

Warum mehrere Netzwerkschnittstellen?

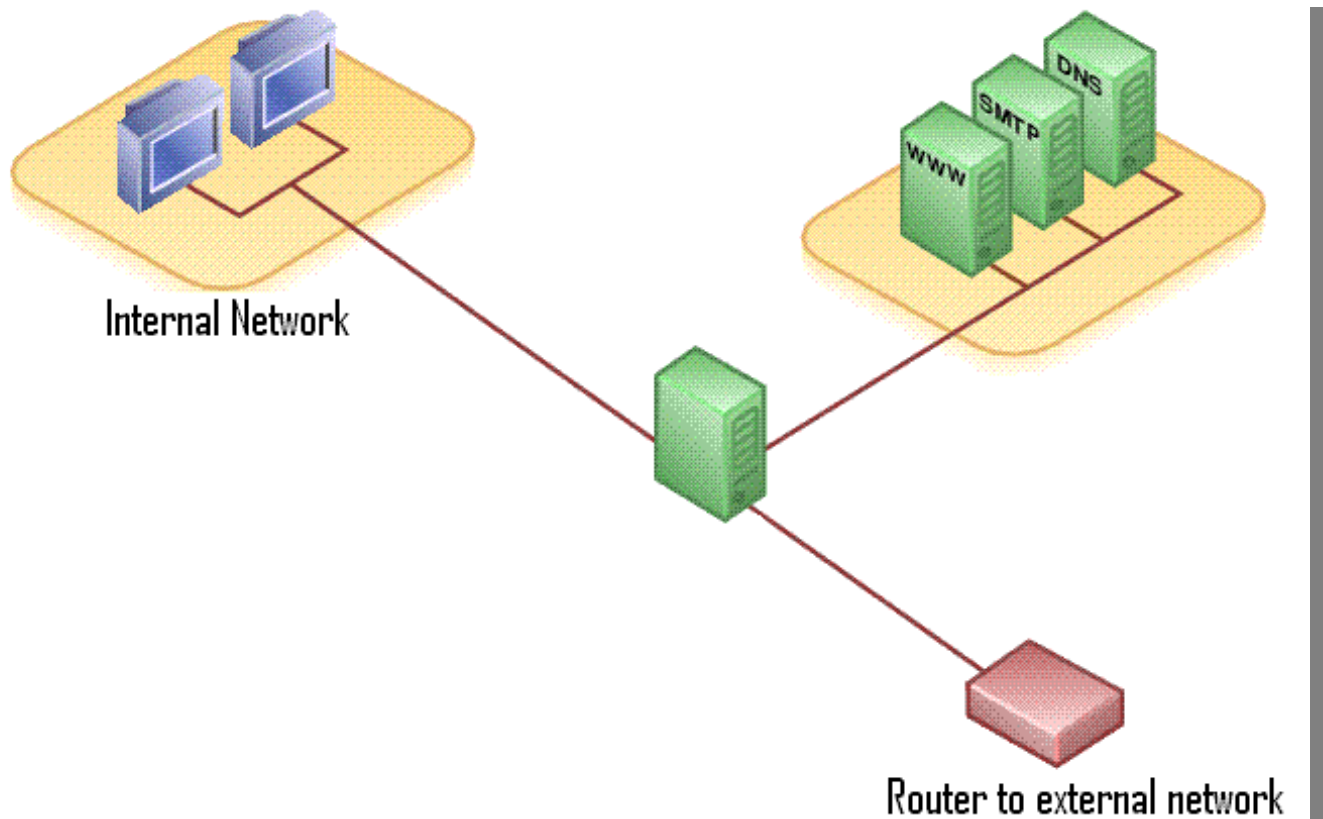
- Zur echten Trennung von Teilnetzen
- Es gibt mindestens ein „Außen“ und ein „Innen“
- Auch „Extranet“ und „Intranet“ genannt
- Das Extranet ist meist das Internet
- Weitere Teilnetze sind möglich
- Jedes Teilnetz benötigt eine eigene Netzwerkschnittstelle
- Es können unterschiedliche Netzwerktypen benutzt werden (DSL, Ethernet, WLAN, ...)

Weitere Teilnetze

- Häufig benutztes Teilnetz ist die DMZ
- „Demilitarisierte Zone“
- In der DMZ befinden sich nur Rechner, die aus dem Extranet erreichbar sein müssen
- Diese sind auch aus dem Intranet erreichbar (Konfiguration, Administration, Backup)
- Sollte einer dieser Rechner aus dem Internet übernommen werden, sind die Rechner in den übrigen Teilnetzen geschützt

Firewall

Veranschaulichung DMZ^[3]



pfSense

„A **p**acket **f**ilter that makes **Sense**“

- Entwickelt von Rubicon Communications, LLC (Netgate)
- Open Source: Apache 2.0 Lizenz
- Basiert auf FreeBSD (ein UNIX-Derivat)
- Läuft auf ARM- und PC-Hardware
- Vorgänger war „m0n0wall“
- Benutzt Paketfilter „pf“ (aus OpenBSD)
- Web-Interface
- SSH-Zugang

pfSense

„A packet Filter that makes Sense“

- Erweiterbar durch „Pakete“
- Wird laufend weiterentwickelt
- Sicherheitslücken werden zeitnah korrigiert (Heartbleed)
- Administration übersichtlich und einleuchtend
- Läuft von CF- oder SD-Karten, USB-Sticks oder eMMC
- Konfiguration kann leicht auf andere Hardware migriert werden
- Sehr stabil

pfSense

Fähigkeiten (teils durch Pakete nachrüstbar)

- Firewall
- NAT (Network Address Translation)
- Proxy (Netzwerkcache)
- Routing (Weiterleitung zwischen Teilnetzen)
- Load Balancing (Lastverteilung)
- Captive Portal (Allgemeine Startseite für Netze)
- VPN (Virtual Private Network)
- IDS (Intrusion Detection System)
- ...

OPNsense

„OPeN source makes sense“

- Fork von pfSense
- Versuch der Modernisierung (besser strukturierter Code)
- Offenerer Ansatz (Einbindung der Community)
- Flexiblere Lizenzierung
- Noch nicht näher angesehen
- Nicht Gegenstand dieses Vortrags

Installation

Installation von pfSense

- Installation ohne Grafik (Kommandozeile)
- Vergleichbar mit debian (z.B. c't-VDR)
- Automatische Installation überschreibt Zielmedium
- Dann werden die „Rollen“ abgefragt
- Welche Schnittstelle ist „WAN“, „LAN“, „OPT“?
- Nach Installation ist DHCP und HTTP aktiv
- Über Web-Schnittstelle kann dann konfiguriert werden
- Wizard fragt neues Admin-Passwort ab

Konfiguration von pfSense

Anmeldemaske



SIGN IN

admin

Password

SIGN IN

Konfiguration von pfSense

Dashboard

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Dashboard

System Information

Name pfsense.egeler.home

System pfSense
Netgate Device ID: 0f1d1[REDACTED]520

BIOS Vendor: Intel Corp.
Version: TYBYT10H.86A.00[REDACTED]255
Release Date: Wed Dec 24 2014

Version 2.4.3-RELEASE (amd64)
built on Mon Mar 26 18:02:04 CDT 2018
FreeBSD 11.1-RELEASE-p7

The system is on the latest version.
Version information updated at Thu Apr 12 14:43:13 CEST 2018

CPU Type Intel(R) Atom(TM) CPU E3815 @ 1.46GHz
AES-NI CPU Crypto: Yes (active)

Hardware crypto AES-CBC,AES-XTS,AES-GCM,AES-ICM

Kernel PTI Enabled

Uptime 3 Days 01 Hour 57 Minutes 02 Seconds

Current date/time Thu Apr 12 14:44:03 CEST 2018

DNS server(s)

- 127.0.0.1
- 192.168.248.248
- 192.168.2.1
- 192.168.1.1

Last config change Wed Apr 11 20:15:00 CEST 2018

State table size 0% (123/189000) Show states

MBUF Usage 1% (760/118130)

Temperature 47.0°C

Interfaces

WAN	↑	100baseTX <full-duplex>	192.168.1.2
LAN	↑	1000baseT <full-duplex>	192.168.248.248
KINTRANET	↑	1000baseT <full-duplex>	192.168.2.1

Firewall Logs

Act	Time	IF	Source	Destination
✗	Apr 12 14:43	KINTRANET	192.168.2.4	255.255.255.255:7437
✗	Apr 12 14:43	KINTRANET	192.168.2.5	255.255.255.255:7437
✗	Apr 12 14:43	KINTRANET	192.168.2.4	255.255.255.255:7437
✗	Apr 12 14:43	KINTRANET	192.168.2.5	255.255.255.255:7437
✗	Apr 12 14:43	KINTRANET	192.168.2.5	239.255.255.250:1900

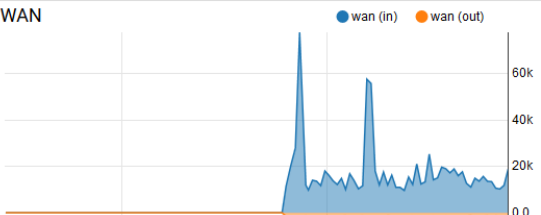
OpenVPN

Peer to Peer Server Instance Statistics

Name/Time	Remote/Virtual IP
Versuch ischs wert UDP4:1194	
Mon Apr 9 12:50:47 2018	192.168.249.1

Traffic Graphs

WAN



Konfiguration von pfSense

Schnittstellen

pfSense
COMMUNITY EDITION

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges

LAGGs

Interface	Network port
WAN	re0 (c0:00:00:00:00:02:07)
LAN	ue0 (00:00:00:00:00:00:68) Delete
KINTRANET	ue1 (00:00:00:00:00:00:2a) Delete

Available network ports: ovpns1 (Versuch ischs wert) + Add

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

Konfiguration von pfSense

Regeln im LAN

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / LAN ⌵ ⌆ ⌂ ?

Floating WAN LAN KINTRANET OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	3 / 1.11 GiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	⚙️
✗	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙️
📄 ✓	0 / 21.84 MiB	IPv4 *	192.168.248.2	*	*	*	*	none		karotte	📌 ✎ 📄 🗑️
📄 ✓	0 / 0 B	IPv4 *	192.168.248.3	*	*	*	*	none		ion	📌 ✎ 📄 🗑️
📄 ✓	0 / 0 B	IPv4 *	192.168.248.4	*	*	*	*	none		video	📌 ✎ 📄 🗑️
📄 ✓	0 / 0 B	IPv4 *	192.168.248.5	*	*	*	*	none		athlan64	📌 ✎ 📄 🗑️
📄 ✓	0 / 0 B	IPv4 *	192.168.248.6	*	*	*	*	none		nuc3815	📌 ✎ 📄 🗑️













Konfiguration von pfSense

Regeln im Kintranet

<input type="checkbox"/>		0/0 B	IPv4 *	*	*	LAN net	*	*	none		Kinder aus dem LAN!			
<input type="checkbox"/>		0/0 B	IPv4 TCP	KINTRANET net	*	KINTRANET address	443 (HTTPS)	*	none		Kinder aus der Firewall!			
<input type="checkbox"/>		0/0 B	IPv4 TCP	192.168.2.24	*	youtube	*	*	none		Annika Galaxy S5			
<input type="checkbox"/>		0/0 B	IPv4 TCP	192.168.2.22	*	youtube	*	*	none		Annika Lenovo Notebook per Funk			
<input type="checkbox"/>		0/0 B	IPv4 TCP	192.168.2.27	*	youtube	*	*	none		Annika Lenovo Notebook per Kabel			
<input type="checkbox"/>		0/0 B	IPv4 TCP	192.168.2.23	*	youtube	*	*	none		Kinderrechner per Funk			
<input type="checkbox"/>		0/0 B	IPv4 TCP	*	*	youtube	*	*	none	<input checked="" type="checkbox"/>				
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.25	*	*	*	*	none		Sempre USB-Boppel ohne Zeitbeschränkung			
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.33	*	*	*	*	none	<input checked="" type="checkbox"/>	Dominik Laptop per Kabel ohne Zeitbeschränkung			
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.24	*	*	*	*	none	<input checked="" type="checkbox"/>	Annika Galaxy S5 ohne Zeitbeschränkung			
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.24	*	*	*	*	none		Annika_Schulzeit	Annika Galaxy S5 zur Schulzeit		
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.24	*	*	*	*	none	Annika_Bonus	Annika Galaxy S5 Bonuszeit			
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.24	*	*	*	*	none		Annika_Extrazeit	Annika Galaxy S5 Extrazeit		
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.24	*	*	*	*	none	Annika_Ferien	Annika Galaxy S5 in den Ferien			
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.23	*	*	*	*	none	<input checked="" type="checkbox"/>	Kinderrechner WLAN 5GHz ohne Zeitbeschränkung			
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.23	*	*	*	*	none		Kinderrechner_Schulzeit	Kinderrechner WLAN 5GHz zur Schulzeit		
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.23	*	*	*	*	none	Kinderrechner_Bonus	Kinderrechner WLAN 5GHz Bonuszeit			
<input type="checkbox"/>		0/0 B	IPv4 *	192.168.2.23	*	*	*	*	none		KinderRechner_Extrazeit	Kinderrechner WLAN 5GHz Extrazeit		

Konfiguration von pfSense

Zeitpläne

	KinderRechner_Extrazeit	April 10 / 15:45-16:15 / April 11 / 14:15-14:45 /	 
	Kinderrechner_Bonus	Mon - Sun / 12:30-18:00 /	 
	Kinderrechner_Ferien	Mon - Sun / 10:00-12:59 / Mon - Sun / 13:30-18:00 /	 
	Kinderrechner_Lern_Ferien	Mon - Sun / 10:00-10:30 /	 
	Kinderrechner_Schulzeit	Sat - Sun / 10:00-12:30 / Sat - Sun / 13:00-18:00 /	 

Konfiguration von pfSense

Aliases

pfSense
COMMUNITY EDITION

Firewall / Aliases / IP

IP Ports URLs All

Firewall Aliases IP

Name	Values	Description	Actions
[REDACTED]			
youtube	youtube.com,youtu.be, video.google.com		

Add Import

Konfiguration von pfSense

Zeitpläne editieren

The screenshot shows the pfSense web interface for editing a schedule. The page title is "Firewall / Schedules / Edit". The "Schedule Information" section includes:

- Schedule Name:** Dominik_Schutzzeit (Note: This schedule is in use so the name may not be modified)
- Description:** (Empty field)
- Month:** April_18
- Date:** A calendar for April 2018. The selected date is the 1st (Sunday).
- Time:** 0:00 to 23:59. (Note: Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.)
- Time range description:** (Empty field)

At the bottom, there is a "Configured Ranges" table with the following entries:

Day(s)	Start time	Stop time	Description	Action
Wed	14:30	20:00		Delete
Sat - Sun	8:00	17:59		Delete
Mon - Tues, Thur, Sun	18:00	19:59		Delete
Fri - Sat	18:00	19:59		Delete
Mon - Fri	6:00	15:59		Delete








A "Save" button is located at the bottom left of the configuration area.

Konfiguration von pfSense

DHCP Static Mapping

Deny unknown clients Only the clients defined below will get DHCP leases from this server.



DHCP Static Mappings for this Interface

Static ARP	MAC address	IP address	Hostname	Description	
	00:00:00:00:00:00:2c:64	192.168.248.1	pfsense-eltranet	Die Firewall	 
	00:0b:00:00:00:00:00:ed	192.168.248.2	karotte	Der Datenserver	 
	90:e6:00:00:00:00:53:e1	192.168.248.3	ion	Ach, ist der süß...	 
	00:20:00:00:00:00:a1:23	192.168.248.4	video	Der eine Videorekorder	 
	00:11:00:00:00:00:eb:04	192.168.248.5	athlan64	Der andere Videorekorder	 
	c0:3f:00:00:00:00:92:07	192.168.248.6	nuc3815	Intel NUC 3815 per Kabel	 
	00:16:00:00:00:00:72:e1	192.168.248.7		Win8.1VM	 
	10:c3:00:00:00:00:dc:5a	192.168.248.8	mumm	Der bessere Datenserver	 

Konfiguration von pfSense

VPN

The screenshot shows the pfSense web interface for the OpenVPN Servers configuration. The breadcrumb trail is "VPN / OpenVPN / Servers". The "Servers" tab is selected. Below the navigation tabs, there is a table titled "OpenVPN Servers" with the following data:

Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	192.168.249.0/30	Crypto: AES-128-CBC/SHA1	Versuch ischs wert (tun)	 

A green "+ Add" button is located at the bottom right of the table.

Konfiguration von pfSense

VPN konfigurieren

The screenshot shows the pfSense web interface for configuring an OpenVPN server. The breadcrumb trail is "VPN / OpenVPN / Servers / Edit". The page has tabs for "Servers", "Clients", "Client Specific Overrides", and "Wizards".

General Information

- Disabled:** Disable this server. Set this option to disable this server without removing it from the list.
- Server mode:** Peer to Peer (Shared Key)
- Protocol:** UDP on IPv4 only
- Device mode:** tun - Layer 3 Tunnel Mode. "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)
- Interface:** WAN. The interface or Virtual IP address where OpenVPN will receive client connections.
- Local port:** 1194. The port used by OpenVPN to receive client connections.
- Description:** Versuch ischs wert. A description may be entered here for administrative reference (not parsed).

Cryptographic Settings

Shared Key:

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
78ec5a56858cf75f7c07644aa5ca95d1
```

Motivation für eigene Firewall

Erhöhung der Netzwerksicherheit

- Weiteres Hindernis für Hacker
- Man hat zwei unterschiedliche Systeme
- Hat ein System eine Lücke, ist noch das andere da
- Wahrscheinlichkeit für gleichzeitige Lücken in beiden Systemen sehr niedrig
- Anbieter benutzt „Zwangsrouter“
- Kontrolle über eigenes Netz
- Spaß am Selbstbau

Standardsituation bei Internetanschluss

Fast überall in Deutschland:

- Internetanschlusssanbieter teilt IP-Adresse zu
- Am Teilnehmeranschluß Standard-“Kiste“ des Anbieters
- Modem oder Router
- Reines Modem setzt dahinterliegende Rechner direkt dem Internet aus
- Router bildet implizite Firewall durch NAT (Network Address Translation)
- Man hat die Kiste nicht unter eigener Kontrolle

Modem

Ungeschützter Anschluss

- Gerät direkt aus dem Internet erreichbar
- Allen Hackversuchen ausgesetzt
- Vermutlich nach spätestens zehn Minuten gehackt
- Bis vor einigen Jahren bei DSL durchaus möglich
- Bis vor Kurzem auch bei TV-Kabelanschlüssen
- Hoffentlich bei Glasfaser dazugelernt
- Nicht zu empfehlen

Router

Verteilt Internetanschluss auf mehrere Geräte

- Enthält üblicherweise Ethernetswitch
- Falls zu wenige Ports expliziten Switch benutzen
- Enthält meistens WLAN Access Point
- NAT (Network Address Translation) ermöglicht Anschluss mehrerer Geräte
- Dadurch schon recht guter Schutz, da kein direkter Zugriff aus dem Internet möglich
- Firewallmöglichkeiten sind begrenzt

Zweite Firewall

- Kein Vertrauen in „Box“ des Anbieters
- Mehrere Teilnetze sind möglich
- Trennung der Teilnetze
 - Internet
 - Intranet
 - DMZ
 - WLAN
 - Eltern
 - Kinder
 - ...

Kommerzielle Lösung

Welche Software als Firewall?

- Astaro
- Cisco
- Juniper
- Checkpoint
- Barracuda

Wird meist zusammen mit eigener Hardware verkauft.
Teuer, keine Eigenkontrolle. Durchaus mit Fehlern.

Welche Software als Firewall?

- IPFire (Basiert auf Linux und netfilter)
- Endian Firewall (Debian)
- Smoothwall (Gehärtetes Linux mit Firewall)
- IPCop (Linux From Scratch)
- M0n0wall (Entwicklung 2015 eingestellt)
- PfSense / OPNSense (FreeBSD)
- OpenWRT / LEDE (Alternative Firmware)
- Fli4l (Floppyrouter; veraltet)

Historie

Mein allererstes Netz

- Ein Analogmodem mit 9600 Bit/s
- Zuerst Direktanschluss an „Mailbox“ („Maus-Netz“)
- Einwahl nach Bedarf (häufig besetzt)
- Ortstarif
- Keine Firewall nötig wegen „Punkt zu Punkt“-Verbindung
- Extrem beschränkte Möglichkeiten

Historie

Mein allererstes „Internet“

- ISDN-Steckkarte für den PC (64 KBit/s)
- Karte steckte im Server
- Netz ein/aus via HTTP und CGI-Skript
- Viele Einwahlpunkte ins Internet waren kostenpflichtig
- Anschluss an Softwarezentrum BB (Ortstarif)
- Dessen Firewall wurde mitbenutzt
- Kein Bedarf für eigene Firewall
- SWZ war „Man in the Middle“

Historie

Mein erstes eigenes Internet

- DSL-Provider war Strato
- 2 MBit/s Volumentarif; 2 GByte/Monat
- Router war Marke „Siemens Gigaset“
- Bekannt von Funktelefonen
- Kein Vertrauen in Hersteller
- Floppyrouter (fli4l)
- Hardware: Intel 486-66 (Heruntergetaktet auf 33 MHz)
- Zwei 10-MBit Ethernetkarten

Mein erstes schnelles Internet

- Neuer Vertrag mit 16MBit/s (Flatrate)
- Ethernetkarten waren der Flaschenhals
- ISA-Bus zu langsam
- Neue Hardware: Intel Pentium 200MHZ / 192 MB RAM
- Drei 100MBit PCI-Karten
- Floppyrouter veraltet
- Neue Lösung: pfSense
- Bekannt von PI-Data

Optimierungsmaßnahmen

- „Blechkasten“ brauchte zu viel Strom
- Hinweis in c't auf „6 Watt PC“
- Intel NUC 2820 Barebone
- Ein SO-DiMM-Steckplatz mit 2GByte bestückt
- „Festplatte“ war 4 GByte USB-Stick
- Nur ein Ethernetport
- Aber ein USB3-Port und zwei USB2-Ports
- Zwei USB zu GBit Ethernet Adapter von „Icy Box“

Migration

Geeignere Hardware

- NUC 2820 als Medienabspieler freispielen
- Besser geeigneter NUC 3815
- 4GB interner Flash-Speicher für pfSense
- Lüfterlos
- Mini-PCI-Slot für WLAN-Hardware
- Ebenfalls ein Ethernet- und drei USB-Anschlüsse
- Vorher Backup in XML-Datei
- Unnötig, da nach Umstecken von USB-Stick und Kabeln alles lief wie vorher

Migration

Nach Migration

- NUC 2820 fährt jetzt Kodi im Wohnzimmer
- Damalige Variante von freeBSD hat internen Flash nicht erkannt → lief weiter vom USB-Stick
- Seit Version 11 wird er erkannt
- Backup auf XML-Datei
- Neuinstallation über selbst erzeugten USB-Stick
- Grundkonfiguration über Kommandozeile
- Nach Umstecken aller Kabel Backup rückgespielt

Weitere Möglichkeiten

- Ein USB-Port freigespielt
- Möglichkeit für weiteres internes Netz „DMZ“
- Vom Internet sichtbarer Server
- DynDNS
- Spielwiese für ownCloud und vieles mehr

Quellen

- 1. Firewall:
https://upload.wikimedia.org/wikipedia/commons/5/52/Gateway_firewall.png
- 2. VLAN:
<https://upload.wikimedia.org/wikipedia/commons/b/be/Vlan-fig1.gif>
- 3. DMZ:
https://upload.wikimedia.org/wikipedia/commons/5/52/DMZ_network_diagram_1_firewall.png



Vielen Dank!

PC-Treff-BB

Firewall mit pfSense.odp, Folie 42 von 42

© 14.04.2018 Roland Egeler