Da ich zu Hause auch des öfteren mal Virenverseuchte Rechner reparieren muss, habe ich mich für eine Abtrennung zum Produktivnetz entschieden. Erste Ideen gab mir der folgende heise-Artikel: Router-Kaskaden. Eine super Idee, günstige Hardware (Router) zur Trennung zu nutzen. Nachteil: SMB-Freigaben im DMZ-Netz sind schwierig zu konfigurieren und der Zugang von Netzt zu Netz ist fast nicht möglich. Deshalb habe ich mir eine Firewall angeschaft:

Hardware

- Igel 5200LX 5/3
- D-Link DFE-580TX 100MBit Quad-Port Netzwerkkarte
- 1GB RAM
- 8GB Compact Flash

Stromverbrauch: 27-33Watt

Software

Erster Gedanke war M0n0Wall. Leider hat die BSD-Version die Netzwerkkarten nicht richtig erkannt

Zweiter Gedanke: pfSense. Dieser Fork von M0n0wall hat eine neuere BSD-Version und unterstützt die Netzwerkkkarte.

Installation ging reibungslos von Statten. Boot von USB-Stick, Installation, Fertig.

Probleme

VDSL-Modem einrichtung

Da ich VDSL-habe, habe ich mich auf die suche nach einem VDSL-Modem (nicht Router) gemacht. Vorteile: Die Firewall selbst macht das NAT und die Einwahl ins Netz. Das Modem ist quasi nur für die Umsetzung von VDSL auf LAN zuständig

Als Modem habe ich mir das Zyxel P-870H-53A gekauft.

Nach langer Recherche und mehreren Tagen bin ich auf die Rezensionen von Amazon und auf diesen Link gestoßen. Mit Hilfe des Heise-Artikels habe ich die Einwahl versucht.

Leider hat es nicht funktioniert. Fehler: 1und1 benutzt zwar das VLAN 7 für die Übertragung, dieses VLAN endet aber am Modem. Die Firewall muss also nicht für VLAN7 konfiguriert werden. Außerdem muss der Benutzername (bei 1und1) ein „H“ vorangestellt werden (Quelle: http://forum.pfsense.org/index.php?topic=51582.0). Dann klappts auch mit dem Zugang.

VDSL-Modem Geschwindigkeit

Die offiziell letzte Firmware auf der Website hat ein Problem mit der Downloadgeschwindigkeit.

Nach Rücksprache mit dem Support wurde mir diese Firmware empfohlen

VoIP-Telefon

VoIP einzurichten ist eigetlich nicht sonderlich schwer, nur ein paar Ports öffnen und fertig. Weit gefehlt.

Zunächst sollte man die Fritzbox selbst umkonfigurieren, da sie ja nicht mehr selbst die Einwahl übernimmt. Hilfe gibt es hier

Dann muss man die folgendnen Ports in der Firewall öffnen:

- UDP-Port 5060
- UDP-Port 7078 bis 7097
- ~~UDP-Port 53 (DNS-Anfragen und Antworten)~~ [nicht unbedingt notwendig und nicht empfohlen (Open DNS Resolver)]

Normalerweise sollte es jetzt funktionieren.

Aus Sicherheitstechnischen Gründen ändert pfsense den Source-Port aller ausgehenden Pakete. Dies ist aber Gift für VoIP und IPSec. Um dies zu ändern, muss man sich diesen pfsense-Artikel zu gemüte führen und Outbound-Regeln definieren.

Traffic Shaper

- http://www.hammerweb.com/blog/2011/09/traffic-shaper-in-pfsense-2-0/

Firewall reloaded

Neue Aufgaben brauchen neue Hardware. Die 100MBit Netzwerkkarten wurden auf dauer doch zu langsam. Deshalb wurde ein neues System gekauft

Spezifikation

- Mainboard: Jetway NF96FL-525-LF
- CPU: Intel Atom D525
- Nnetzwerk: 4x GigaBit Ethernet (1x Realtek, 3x Intel)
- RAM: 2GB Kingston ValueRAM DDR2-800
- Festplatte: 80GB SATA 2,5 Zoll
- M350 mini-ITX Gehäuse

Stromverbrauch: 20-25 Watt

Netzwerkdurchsatz: 30 - 50MB/s 😬

openVPN

1. ein Server, mehrere Netze: https://doc.pfsense.org/index.php/OpenVPN_multi_purpose_single_server
2. RoutingProblem: http://www.administrator.de/wissen/pfsense-und-openvpn-ein-hartn%C3%A4ckiges-routing-problem-im-remote-netz-erfolgreich-gel%C3%B6st-wie-immer-254195.html
3. Routed Lans: https://community.openvpn.net/openvpn/wiki/RoutedLans

From:
https://wiki.da-checka.de/ - **PSwiki**

Permanent link:
https://wiki.da-checka.de/doku.php/wiki/basteleien/firewall?rev=1415711000

Last update: **2014/11/11 14:03**