Firewalls

Grundlagen und Konzepte

Mirko Dziadzka

dziadzka@gmx.net

http://www.dziadzka.de/mirko

Inhalt

- Definition, Sinn und Zweck
- Architekturen
- Realisierung mit OpenSource
- Missverständnisse
- Diskussion

Definition

Aus der d.c.s.f FAQ:

Unter einer Firewall versteht man ein organisatorisches und technisches Konzept zur Trennung von Netzbereichen, dessen korrekte Umsetzung und dauerhafte Pflege.

Architekturen / Komponenten

- Paketfilter
- Proxy
- DMZ
- NAT
- IDS

Paketfilter

- Filtert den Datenstrom auf IP Ebene
- oftmals schon in Routern implementiert
- in der Regel stateless, kann aber auch statefull sein.

Proxy Server

- Filtert Datenstrom auf Applikation Level
- Kann Wissen über die Applikation zum filtern mit einbringen

- Circuit-Level Gateways filtern auf TCP Ebene

Demilitarisierte Zone (DMZ)

- Netzwerkbereich der zwischen dem externen Netzwerk und dem zu schützenden Netzwerk liegt
- Über Paketfilter von den anderen Netzwerken getrennt
- Standort von Proxy Servern, eventuell auch von Applikation-Server (HTTP)

Network Address Translation (NAT)

- unter Linux auch als IP Masquerading bekannt
- bildet transparent Netzwerkadressen auf einen anderen Bereich ab
- Wird nur benutzt, wenn eine direkte IP Verbindung notwendig ist

Intrusion Detection System (IDS)

- System zur (möglichst) automatischen Erkennung von ungewöhnlichen bzw. unerwünschtem Verhalten von Applikation bzw. Netzwerkverkehrs
- In der Regel in der DMZ und im Intranet eingesetzt

Beispielarchitektur (1)

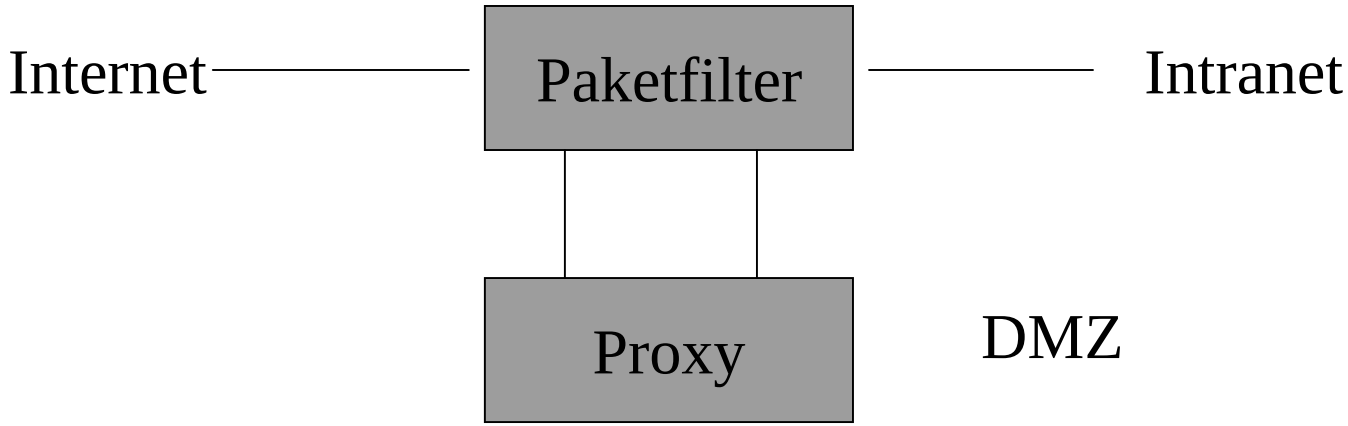
- Einfacher Paketfilter
- nur für den Heimgebrauch
- meistens mit NAT kombiniert

Beispielarchitektur (2)

- Paketfilter mit Proxy Server
- nur für den Heimgebrauch
- Proxy für DNS, HTTP, FTP, SMTP, POP üblich
- Ein Fehler in einem Proxy öffnet das gesammte interne Netzwerk

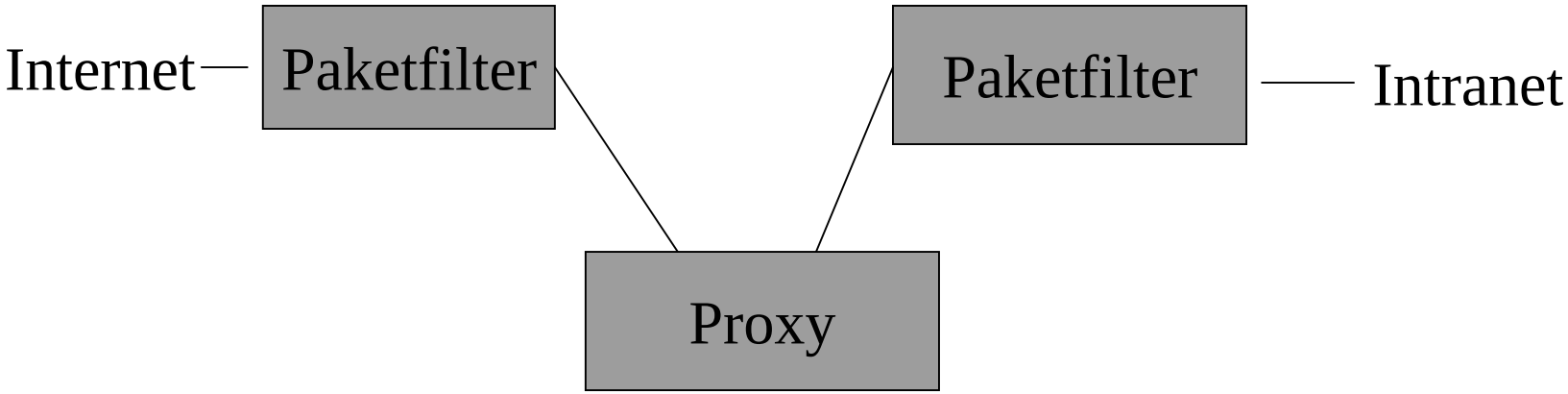
Beispielarchitektur (3)

- ein Paketfilter mit DMZ
- besserer Schutz der Rechner in der DMZ
- Wenn der Paketfilter angreifbar ist, ist das interne Netz offen



Beispielarchitektur (4)

- klassische DMZ mit zwei unabhängigen Paketfiltern
- für Real-World Szenarien geeignet
- auch mehrstufig ausbaubar



Realisierung mit OpenSource

- Warum OpenSource
- Proxy
- Paketfilter
- NAT
- IDS
- VPN

Warum OpenSource

- Closed Source ist zwar bunter, aber auch nicht besser, siehe FW-1
- Mehr Peer Reviews bei sicherheitskritischen Produkten
- Sauberer Code
- Gegenbeispiel gibt es immer

Proxy

- FWTK (smap, http-gw, ftp-gw, telnet-gw, …)
- SMTP Proxy mit smap/sendmail oder qmail + Virenscanner
- DNS Proxy mit dnscache
- HTTP Proxy mit Apache
- Applikatorische Proxyserver

Paketfilter

- Linux 2.2: IP Chains
  - primär stateless, Module für ftp, … vorhanden
- Linux 2.4: IP Tables
  - primär stateless, erlaubt aber einfache Erweiterung um statefull Komponenten
    - Connection Tracking, ...
- OpenBSD: IPF

NAT

- Warum?
- Probleme?
- Unter Linux im ipchains bzw. IP Tables integriert

VPN

- Wozu
  - Verbindung von privaten Netzen übers Internet
  - Remote Access Service
- IPSec
  - Industriestandard
  - LinuxImplementation Free/Swan
- Cipe

Intrusion Detection (1)

- Hostbasiert
  - Auswertung von Logfiles
  - Erkennen von Portscans (portsentry)
  - Erkennen von Änderungen am System (tripwire)
  - Erkennen von ungewöhnlichem Applikationsverhalten
    - LIDS (Kernel)
    - Softwarewrapper (Userspace: Projekt: Wrapper für Netscape)

Intrusion Detection (2)

- Netzwerkbasiert
  - Erkennen von ungewöhnlichen Datenpaketen im Netzwerk
    - Verbotenen Source bzw. Destination
    - “Defekte” Pakete
  - Traffikanalyse im Netzwerk

Missverständnisse

- VPN muss in DMZ enden
- Statefull vs. Stateless Paketfilterung
- REJECT vs. DENY
- Sinn und Unsinn von “Desktop Firewalls”
- Firewall A ist besser als Firewall B, weil sie einfacher zu konfigurieren ist
  - A fool with a tool is still a fool
- Ohne Admin keine Firewall

Missverständnisse (2)

- ständige Logfileanalyse ist notwendig
- Was passiert, wenn das tolle Tool XYZ nicht funktioniert.
  - Beim User
  - Beim Chef
- Das technische Konzept Firewall ist unsicher, ein internen User kann immer Daten nach aussen “tunneln”

Fragen / Diskussion