Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Firewall-Technologien: Basics, Einsatzgebiete und Probleme

M. Heim | HS Alb-Sig | B. Eng TI3

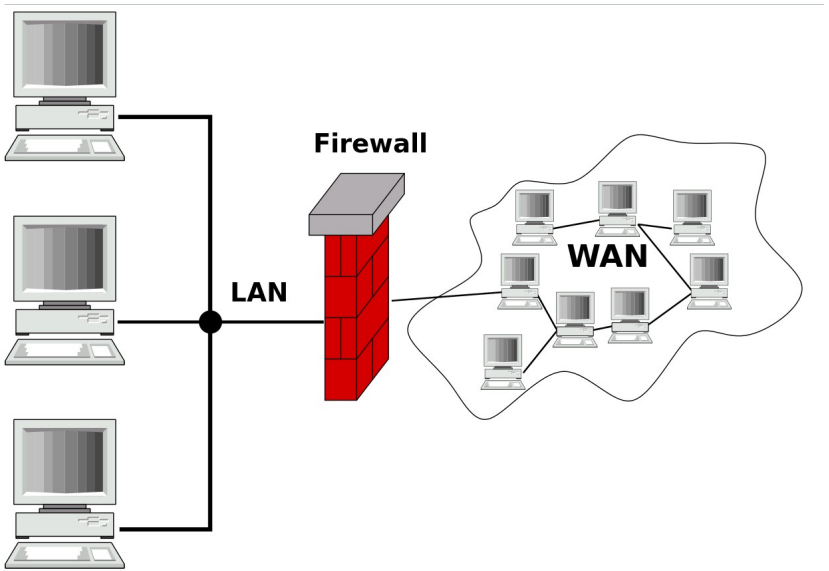
Gliederung

- Was ist eine Firewall?
- Wie konfiguriert man Firewalls?

- Was sind Firewall-Technologien?
- Firewall-Technologien:
  - Statische Paketfilterung
  - Dynamische Paketfilterung (Stateful Inspection)
  - Dedicated Proxyfilter
  - Circuit Level Proxyfilter

Was ist eine Firewall?

- **Sicherungssystem in einem Computernetzwerk**



Grafik 1.1: Firewall

Was ist eine Firewall?

- **Ein Netzwerk Sicherungskonzept besteht jedoch aus mehr Komponenten[2]:**
  - **Honeypot**
  - **IDS/IPS – Intrusion Detection/Prevention System**
  - **meist mehreren Firewalls….**

Was ist eine Firewall?

- **Software-Firewall**

```
pi@raspberrypi:~ $ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
pi@raspberrypi:~ $
```

Grafik 1.2 – Software Firewall

- **Hardware-Firewall**

Grafik 1.3: Hardware Firewall Juniper SSG5

Wie konfiguriert man eine Firewall?

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- **ACL's – Access Control Lists**

Outbound Rules

Name	Local Address	Remote Address	Local Port	Protocol	Action	Remote Port	Group
Windows Peer to Peer Collaboration Foun...	Any	Local subnet	Any	UDP	Allow	1900	Windows Peer to Peer Collab
Windows Peer to Peer Collaboration Foun...	Any	Any	Any	TCP	Allow	Any	Windows Peer to Peer Collab
Windows Peer to Peer Collaboration Foun...	Any	Local subnet	Any	UDP	Allow	3702	Windows Peer to Peer Collab
Windows Search	Any	Any	Any	Any	Allow	Any	Windows Search
Windows Security	Any	Any	Any	Any	Allow	Any	Windows Security
Windows Shell Experience	Any	Any	Any	Any	Allow	Any	Windows Shell Experience
Windows Shell Experience	Any	Any	Any	Any	Allow	Any	Windows Shell Experience
Wireless Display (TCP-Out)	Any	Any	Any	TCP	Allow	Any	Wireless Display

Grafik 1.4 - ACL

Firewall-Technologien

- Methoden zur Erkennung von unzulässigen Datenströmen durch ein Firewall-System
- Systeme können Protokollgebunden sein → Firewall besteht aus mehreren Instanzen
- Verschiedene Technologien arbeiten auf verschiedenen Schichten im OSI Modell

Grafik 1.5 - OSI-Modell

Firewall-Technologien: Statische Paketfilter

- Paketfilter-Firewall
  - **Statische Paketfilterung**
  - Dynamische Paketfilterung (Stateful Inspection)
- Proxy-Firewall
  - Dedicated Proxyfilter
  - Circuit Level Proxyfilter

Firewall-Technologien: Statische Paketfilter

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- Primitivste Art der Erkennung von unzulässigen Paketen
- Erkennung via Adressen im IP & TCP Header[3]
- Unabhängig von den verwendeten Diensten/Protokollen ab Schicht 5

Firewall-Technologien: Statische Paketfilter

- Vorteile:
  - Einfach, schnell...
- Nachteile:
  - Ip Spoofing (bei falscher Konfiguration) [4]
- Implementierungen:
  - Ipchains, ipfw
- Anwendungsbereiche:
  - Nicht sicherheitskritisch
- Problem:
  - Immer Regel von A-B und B-A

Firewall-Technologien: Stateful Inspection

- *Paketfilter-Firewall*
  - Statische Paketfilterung
  - **Dynamische Paketfilterung (Stateful Inspection)**
- Proxy-Firewall
  - Dedicated Proxyfilter
  - Circuit Level Proxyfilter

Firewall-Technologien: Stateful Inspection

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- Weiterentwicklung des Paketfilters
- Bei ausgehender Anfrage wird flüchtige “Established” bzw “Related” Regel erzeugt[5].
- Diese erlaubt dann bis zum Verbindungsabbau oder auch bis zu einem gewissen Timeout einkommenden Verkehr vom Kommunikationspartner

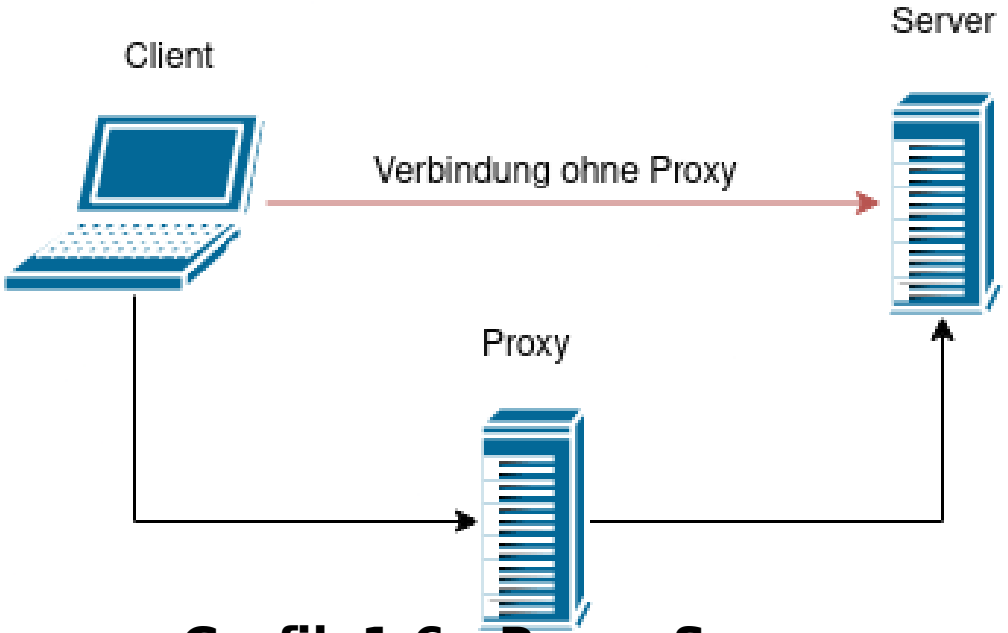
Firewall-Technologien: Stateful Inspection

- Vorteile:
  - Lößt Problem!, Protokoll-unabhängig
- Nachteile:
  - Kein Schutz auf OSI Ebene 7, VoIP
- Implementierungen:
  - Windows Defender Firewall[2], Iptables, Fritzbox
- Anwendungsbereiche:
  - Personal Firewalls, Router Firewalls und Hardware Firewalls (CISCO PIX)[3]

Firewall-Technologien: Proxy-Firewall

- Basiert auf Prinzip eines regulären Proxy-Servers
- Ist jedoch um zusätzliche Filtermodule erweitert
- 2 Techniken:
  - Dedicated Proxy Firewall
  - Circuit Level Proxy Firewall

Firewall-Technologien: Proxy-Firewall



Grafik 1.6 - Proxy-Server

Firewall-Technologien: Proxy-Firewall

- Paketfilter-Firewall
  - Statische Paketfilterung
  - Dynamische Paketfilterung (Stateful Inspection)
- Proxy-Firewall
  - **Dedicated Proxyfilter**
  - Circuit Level Proxyfilter

Firewall-Technologien: Proxy-Firewall - Dedicated

- Ist Protokoll-Abhängig[8]
- Analysiert Daten zusammenhängend
- OSI Schicht 7[8]
- Firewall kann mehrere Module für mehrere Protokolle enthalten

Firewall-Technologien: Proxy-Firewall - Dedicated

- Vorteile:
  - Hat Zugriff auf alles, Client lässt sich nicht direkt angreifen, realisiert daher sogar noch eine weitere Form von Schutz[8]
- Nachteile:
  - Rechenintensiv, Speicherintensiv, Protokollabhängig[8]
- Implementierungen:
  - Fortinet FortiProxy, Watchguard Firebox
- Anwendungsbereiche:
  - Höchste Sicherheitsanforderung, Unternehmensnetze

Firewall-Technologien: Proxy-Firewall – Circuit Level

- Paketfilter-Firewall
  - Statische Paketfilterung
  - Dynamische Paketfilterung (Stateful Inspection)
- Proxy-Firewall
  - Dedicated Proxyfilter
  - **Circuit Level Proxyfilter**

Firewall-Technologien: Proxy Firewall – Circuit level

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- Ist Protokoll-Unabhängig
- Im Gegensatz zur Dedicated Proxy Firewall: Setzt Paketfilter um
- OSI Schicht 3 und 4 bzw. zum Teil auch Schicht 5, d.h. Authentifizierung (können Sitzungen validieren)

Quellen

- Firewall-Technologien:
  - https://www.geeksforgeeks.org/firewall-methodologies/

Paketfilter:
  - https://de.wikipedia.org/wiki/Paketfilter
  - https://de.wikipedia.org/wiki/Stateful_Packet_Inspection
- Proxy:
  - https://www.cs.ait.ac.th/~on/O/oreilly/tcpip/firewall/ch07_03.htm
  - https://www.nm.ifi.lmu.de/teaching/Praktika/2004ss/secp/Unterlagen/main_secp_student_Termin_3.pdf

Zitierte Quellen

[1] - https://de.wikipedia.org/wiki/Firewall - Abgerufen am 13.06.2021

[2] - https://de.wikipedia.org/wiki/Intrusion_Detection_System - Aufgerufen am 13.06.2021

[3] - https://einstein.informatik.uni-oldenburg.de/rechnernetze/router1.htm - Aufgerufen am 13.06.2021

[4] - https://users.informatik.uni-halle.de/~beckmann/Firewall/ - Aufgerufen am 13.06.2021

[5] - https://de.wikipedia.org/wiki/Stateful_Packet_Inspection - Aufgerufen am 13.06.2021

[6] - https://en.wikipedia.org/wiki/Cisco_PIX - Abgerufen am 13.06.2021

[7] - https://www.itmz.uni-rostock.de/anwendungen/software/windows/sicherheit/grundlagen/windows-firewall-stateful-inspection-firewall/ - Aufgerufen am 11.06.2021

[8] - https://www.ip-insider.de/was-ist-eine-proxy-firewall-a-621987/ - Abgerufen am 13.06.2021

Zitierte Quellen

[8] - **https://www.ip-insider.de/was-ist-eine-proxy-firewall-a-621987/** - Abgerufen am 13.06.2021

Foto Quellen

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Grafik 1.1 - Harald Mühlböck - https://de.wikipedia.org/wiki/Datei:Gateway_firewall.svg

Grafik 1.2 – Maximilian Heim

Grafik 1.3 – Chris Dag - https://www.flickr.com/photos/chrisdag/5212583486

Grafik 1.4 – Maximilian Heim

Grafik 1.5 – Maximilian Heim

Grafik 1.6 – Maximilian Heim

Grafik 1.7 – Datenblatt Watchguard Firebox t40 - https://www.watchguard.com/wgrd-resource-center/docs/firebox-t40 - aufgerufen am 13.06.2021

Vielen Dank fürs Zuhören!
Fragen?