Firewalls

Kryptographie und IT-Sicherheit

Kevin Fehrenbach
Patrick Oberbichler
Bernhard Schnee

Inhalt

- Allgemeine Grundlagen
- Filtertechniken
- Firewall Regelwerk
- Firewallarten

Allgemein Grundlage

- Definition
- „Eine Firewall ist eine Software die dazu dient, den Netzzugriff zu beschränken, basierend auf Absender - und Zieladresse und genutzten Diensten. Die Firewall überwacht den durch sie durchlaufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob gewisse Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht die Firewall unerlaubte Netzwerkzugriffe zu unterbinden.“

Allgemeine Grundlagen

Um auf Dateien und andere Ressourcen zugreifen zu können werden Netzwerkdienste verwendet. Diese werden bei jedem Systemstart unabhängig vom Benutzer ausgeführt. Beim Rückweg können Sicherheitslücken (z. B. im Webbrowser) ausgenutzt werden um ein System anzugreifen.

Allgemeine Grundlagen

Es wird unterschieden zwischen

- Personal (Desktop) Firewall:
  - ist eine Software die den Datenverkehr zum und vom PC filtert

- Netzwerk (Hardware) Firewall:
  - kontrolliert den Datenverkehr zwischen einem lokalen (z. B. LAN) und einen externen (z. B. Internet) Netzwerk

Filtertechniken

- Paketfilter
- Stateful Inspection
- Proxyfilter
- Contentfilter

Filtertechniken

- Paketfilter
  - Die Pakete werden nach bestimmten Regeln untersucht und entweder durchgelassen (ALLOW oder PASS), weitergeleitet (FORWARD oder PERMIT) oder verworfen (DENY oder DROP).
- Stateful Inspection
  - Das Paket wird nach Zustand analysiert, wenn gewisse Kriterien nicht sind, wird es verworfen (z. B. Bei einer DoS – Attacke).

Proxyfilter

- Stellt stellvertretend Verbindung her
  - Kann beliebig beeinflussen
- Auf Protokolle spezialisiert
  - Daten zusammenhängend analysieren

Contentfilter

- Form des Proxyfilters
- Nutzdaten auswerten
  - Spezielle Daten filtern
  - z.B. ActiveX/Javascript
  - Download von Schadsoftware blockieren
  - Sperren von Webseiten

Regelwerk

- Verbotener/Erlaubter Verkehr
- Mandatory Access Control
  - Whitelists
- Regeln werden der Reihe nach überprüft
  - Erste zutreffende Regel angewendet
  - Reihenfolge wichtig
  - Hierarchie

Regelwerk

- Komponenten
  - Absender-IP
  - Ziel-IP
  - Netzwerkprotokoll
  - Port-Nummer (TCP/UDP)
  - Aktion
    - erlauben, verwerfen, ablehnen
  - Loggen

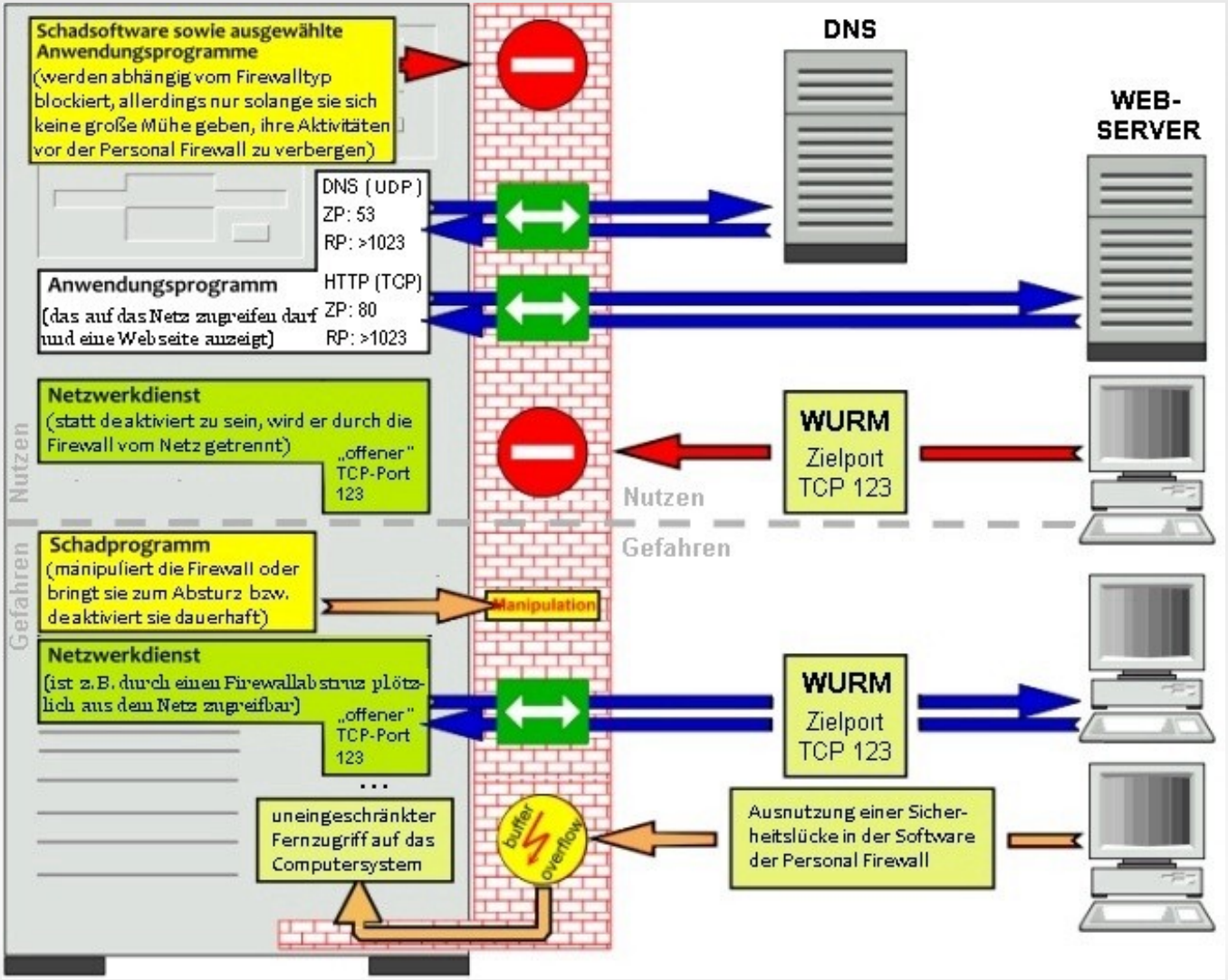
Regelwerk

- Stealth-Regel
  - Selbstschutz
- ICMP Regel
  - Austausch von Fehler und Informationsmeldungen
  - Komplett blockieren/erlauben zu viele Probleme

Firewallarten

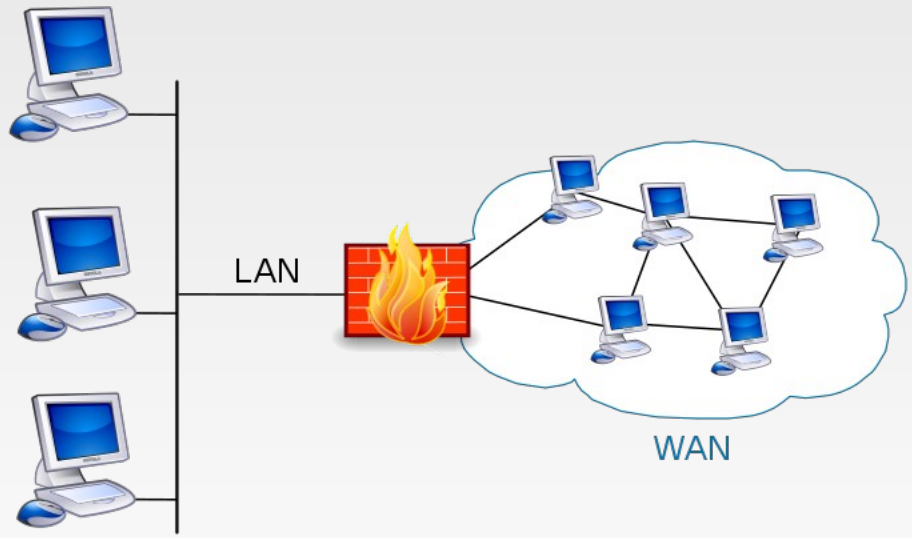
- Personal Firewall
  - Lokal installiert
  - Überwacht Netzverkehr und Ports
  - Bsp.: Kaspersky, Symatec

Firewallarten



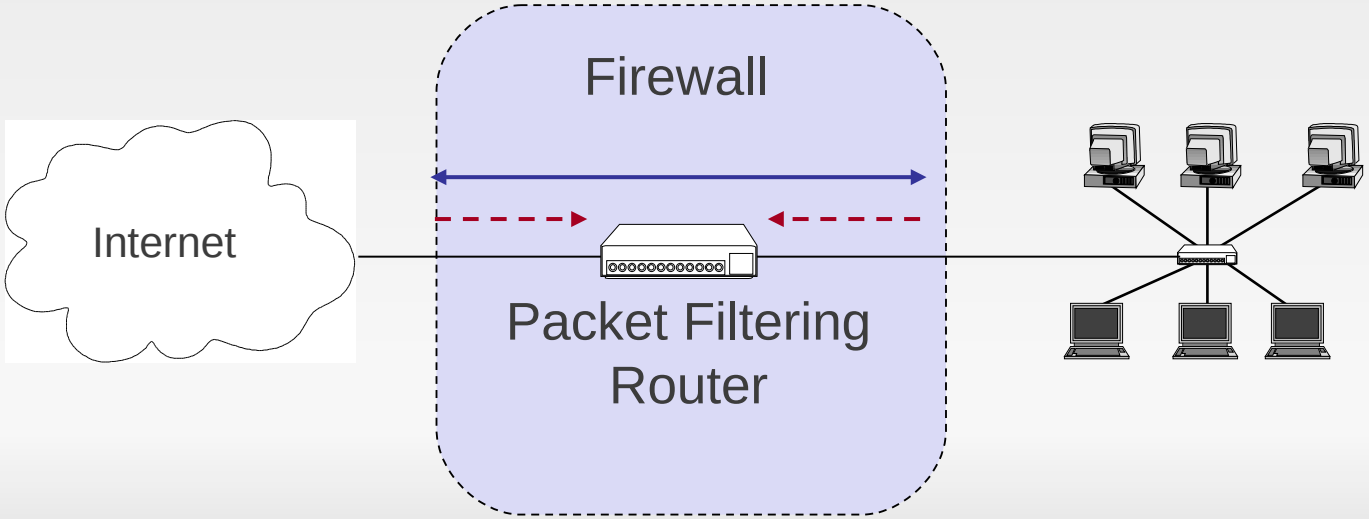
Firewallarten

- Hardware Firewall/Externe Firewall
  - „Hardware“ Firewall = Software, installiert auf separater Hardware



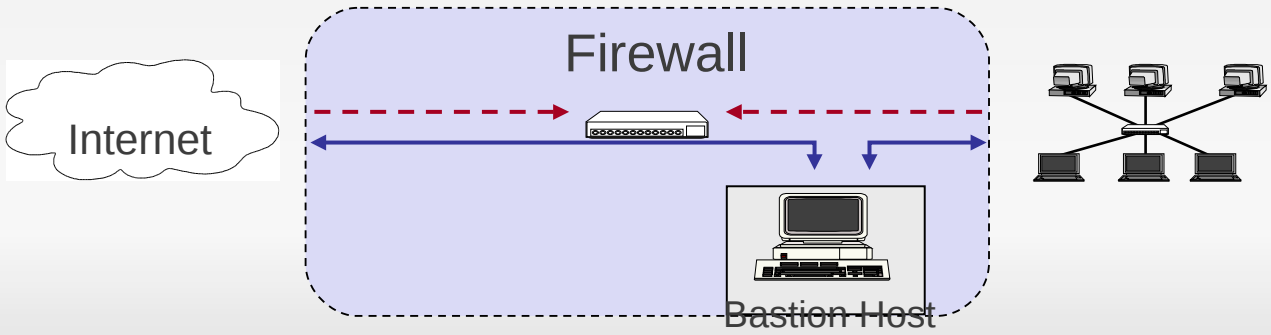
Firewallarten

- Einfacher Paketfilter
- Realisiert durch:
  - Eine Standard Workstation (z.B. Linux-Pc) mit zwei Netzwerkinterfaces und Filter Software
  - Spezielles Routergerät mit Filterfähigkeit



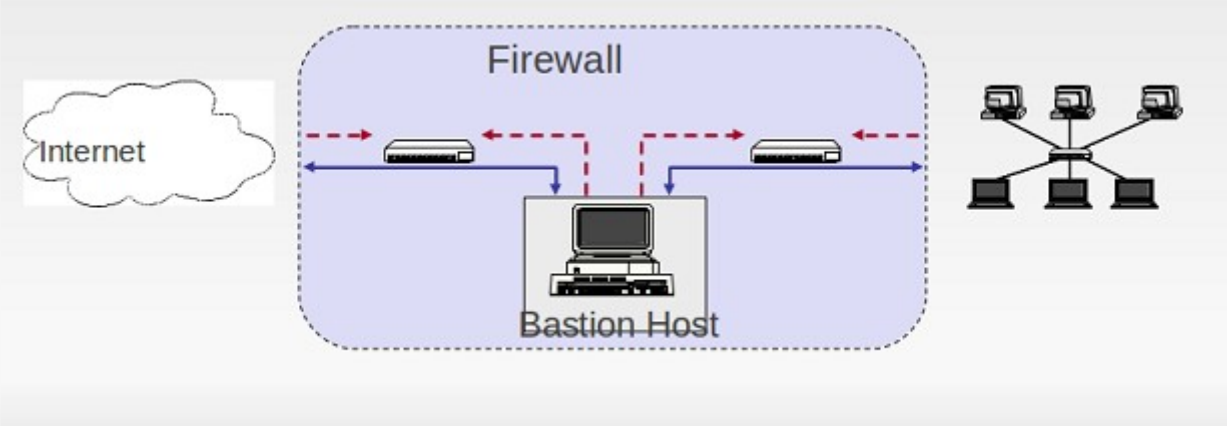
Firewallarten

- Screened Host
- Paketfilter erlaubt nur Verkehr zwischen:
  - Internet und dem Bastion Host
  - Geschütztes Netzwerk und Bastion Host
- Screen Host bietet sich als Proxy an
  - Selbst die Fähigkeit Angriffe abzuwehren



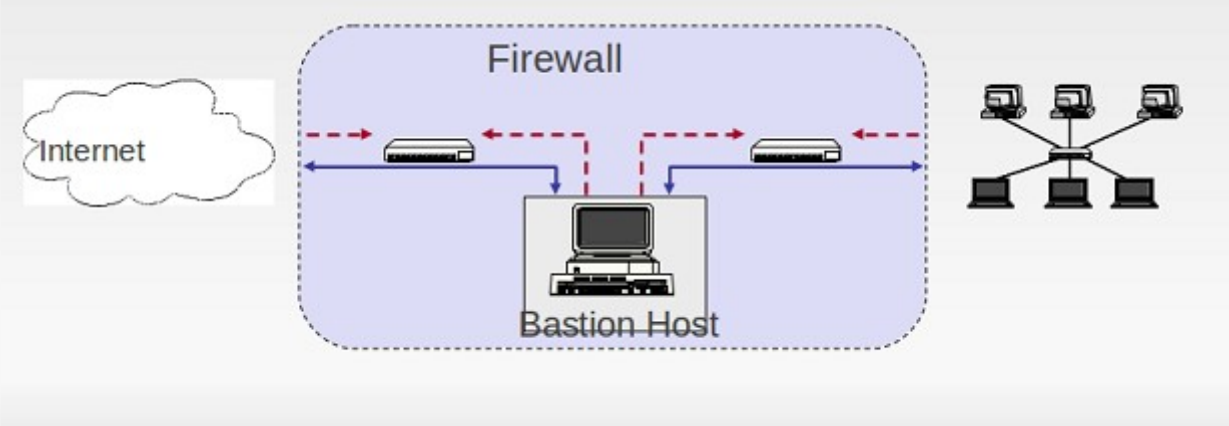
Firewallarten

- Perimeter Network zwischen Paketfiltern
  - Screened Subnet
- Innerer Paketfilter schützt inneres Netzwerk, falls Perimeter Network in Schwierigkeiten kommt



Firewallarten

- Gehackter Bastion Host kann so das Netzwerk nicht ausspionieren
- Perimternetzwerke sind besonders geeignet für die Bereitstellung öffentlicher Dienste



Kosten

- Software
  - Kostenlos
  - 40-60€ pro Jahr
- Hardware
  - Router ab 20€
  - Cisco Asa5510 ~1600€

iptables

- Konfiguration Tabelle der Linux Firewall
- Besteht aus Chains und Rules
  - Chains bestehen aus mehreren Rules

- Regel in Tabelle input erstellen:

  sudo iptables -I INPUT 1 -p icmp -s 141.201.226.211 -j DROP

iptables

- Regel wieder löschen:

  sudo iptables --flush

Quellen

- http://archive.cone.informatik.uni-freiburg.de/teaching/vorlesung/systeme-II-s10/folien/systeme-II-11.pdf
- http://de.wikipedia.org/wiki/Firewall
- Strobel, Stefan: Firewalls und IT-Sicherheit (ISBN-13: 978-3898641524)