

Firewalls

Von Christian Borchardt, Sebastian Kleinschmager und
Timmy Metzler

Firewalls allgemein

- Trennung und Kontrolle zwischen Netzen
 - Firewall Regeln
 - Schutz von Angriffen von außen
 - Schutz vor unerwünschtem Inhalt
-
- Kein Schutz vor Viren
 - Single Point of Failure
 - Komplexe Administration

Die Firewall Prinzipien

- Alles was nicht explizit erlaubt ist, ist verboten.
- Alles was nicht explizit verboten ist, ist erlaubt.

Packet Filter

- Headerinformationen
- Source- & Destination IP
- Source- & Destination Port
- TCP / UDP

Packet Filter

- Kontrolle auf Layer 3 => Geschwindigkeit
 - Kostengünstig
 - In Hardware integriert (Router)
-
- Direkte Verbindung (End-to-end)
 - Ports sind offen oder geschlossen
 - Leicht zu umgehen: IP-Spoofing, Buffer overruns, ICMP tunneling

Stateful Inspection

- Headerinformationen
- Dynamic state table
- Verbindungsstatus

Stateful Inspection

- Sicherer als Packet Filter
 - Gründlichere Kontrolle des IP-Header
 - Protokolle (Fehlverhalten)
-
- Komplexe Regeln
 - Anfällig für Fehler
 - Schwer zu testen

Application Gateway / Proxy

- Client Server Modell wird gebrochen
- End-to-end Verbindung mit jedem Teilnehmer
- OSI-Layer 7
- Präzise Content Analyse
- User Authentifizierung
- Ausführliche Logfiles
- Schlechtere Performance