Proxies, Firewalls und drumherum

Was Firewalls sind, was sie leisten und was sie nicht leisten

13.01.2015 – Jan-Dirk Kranz

Seminar: Internet Protokolle, Alexander Sczyrba u. Jan Krüger

Chain

- Was ist eine Firewall?
  - Sicherheitsstrategie moderner Firewalls
- Firewall Klassen
  - Paketfilter (Definition, Filterregeln, Vor- und Nachteile)
  - Proxies bzw. Proxy-Firewall (Definition, Vor- und Nachteile)
  - Applikationsfilter (Definition, Vor- und Nachteile)
- Firewall-Architekturen
  - Dual-Homed Firewall
  - Screened-Host
  - Screened-Subnet
- Fazit und Ausblick

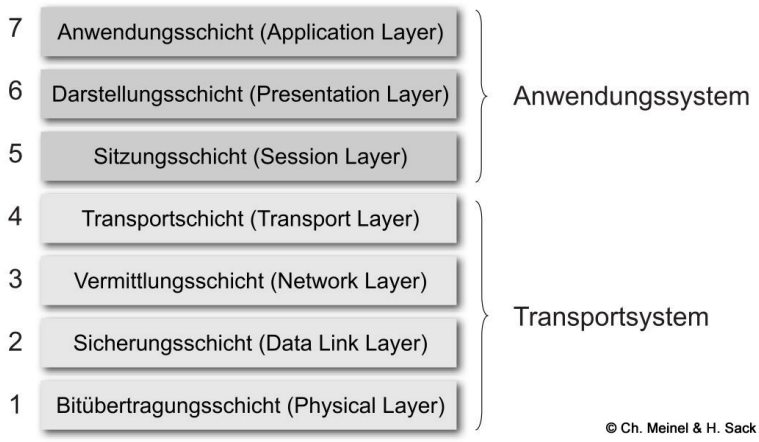
Was ist eine Firewall?

- RFC 2828: "A Firewall is an Internetwork Gateway that restricts data Communication traffic to and from one of the connected Networks (the one Said to be inside the Firewall) and thus protects that Networks System Ressources against Threats from the other Network (the one Said to be outside the Firewall)"
- Sicherheitskonzept in vernetzten Systemen: First Line of Defense
- Abschottung unterschiedlicher Netze gegeneinander
- Aber kontrollierte und gezielte Übergänge möglich: **NUR** über Firewall
- Firewall = Security Gateway

Sicherheitsstrategie moderner Firewalls

- Def.: Kontrollstrategie durch einzelne Regeln
- Eine Firewall leitet nur diejenigen Pakete weiter, die der jeweiligen Sicherheitsstrategie entsprechen
- Sicherheit ist keine Eigenschaft, sondern Anforderungsabhängig
- Betreiben einer Firewall nicht trivial

Firewall Klassen (1)



Firewall Klassen (2)

- Paketfilter
- Proxies (Proxy Firewall)
- Applikationsfilter (Application Level Gateway)

Paketfilter (1)

- OSI Schicht 3 und 4 (Netzwerk und Transportschicht)
- Filterung anhand von Rules und Informationen aus dem IP-Header (bedingt Payload)
- Plausibilitätsprüfungen
- Filterregel: Eintrag in einer Liste von Regeln (Rules in Chains)
- **Pakete gezielt manipulieren:** Adressänderung (NAT), Portänderung (PAT)
- Beispiele: iptables/netfilter (linux), Routing und Remote Access Dienst (Windows), ipfilter (Unix-Derivate; FreeBSD)

Paketfilter (2)

Stateless

- Entscheidung anhand aktuellen Pakets

Stateful

- Speicherung von Paketinformationen
- Filterung anhand dieser Informationen
- Dynamische Filter, stateful Inspection, Content based Access Control

Paketfilter (3)

Vorteile

- Preiswert zu realisieren
- IP-Spoofing und Routing-Attacken abwehrbar
- Absicherung eines kompletten Subnetzes mit zentraler Firewall
- Effizienz: direkt in den Paketvermittlungsweg eingebunden

Nachteile

- Filterentscheidungen basieren auf IP-Header (manipulierbar)
- Grobgranulare Kontrolle
- Niedriges Abstraktionsniveau
- Stateless: Callback Problem
- Stateful: Performanceeinbußen (DoS)

Leitlinien für Filterregeln (1)

- Möglichst früh
- Sequenzielle Regelabarbeitung: Erlaubnisprinzip (!)
  - Alles was nicht ausdrücklich erlaubt ist, ist verboten: Am Schluss eine Verbotsregel
- Pakete von Außen mit interner Adresse abweisen (und umgekehrt)
- ICMP und UDP Filtern (beliebte Angriffsziele)
- Drei Listen: INPUT, OUTPUT, Forward
- Benutzerdefinierte Ketten möglich

Proxies (1)

- Proxy-Firewall, Verbindungs-Gateway, Circuit-Level-Gateway
- Transportschicht
- Stellvertreterkonzept: Statt direkt auf externes Netz, wird zunächst auf einen Gateway-Rechner zugegriffen
- Werden auf "Bastionsrechner" betrieben
- Umfassendere Möglichkeiten als bei Paketfiltern

Proxies (2)

Vorteile

- Keine direkte TCP-Verbindung zwischen Client und Server (Adressumsetzung)
- Auch Kontrolle bestehender Verbindungen
- Authentifikations- und Protokollierfähigkeiten
- Generische Proxies universell einsetzbar

Nachteile

- Transportschicht, daher keine spezifische Unterscheidung von Anwendungen
- Anpassungen an der Clientsoftware

Applikationsfilter (1)

- Application-Level Gateway
- Anwendungsschicht
- Dedizierter statt generischer Proxy (Telnet, FTP, SMTP, HTTP)
- Anwendungsbezogene Filterung statt "Alles oder Nichts"
- Nur Dienste filterbar, für die Proxy verfügbar, ansonsten wird blockiert

Applikationsfilter (2)

Vorteile

- Differenzierte Authentifikationen/Überprüfungen
- Nutzungsprofile, Angrifferkennung anhand von Mustern (stateful)
- Softwaremodule für IDS
- Protokollierung von Zugriffen (zB Abrechnung)
- Caching möglich
- Betrieb eingeschränkter Dienste möglich

Nachteile

- Für jenen Proxy-Dienst eigener Prozess -> Performance -> DoS
- Contentfilterung leicht aushebelbar (Komprimierung)
- Unflexibel (Pro Dienst ein Proxy)

Firewall Klassen

Paketfilter

- OSI 3/4
- Rules in Chains
- Direkt im Paketvermittlungsweg
- Iptables/netfilter

Proxies

- OSI 4
- Stellvertreterkonzept
- Umfassendere Möglichkeiten (bestehende Verbindungen)
- Protokollierung
- Generische Proxies

Application-Filter

- OSI 7
- Dedizierte Proxies
- Erkennung von Mustern
- Betrieb eingeschränkter Dienste

=> In der Regel werden verschiedene Firewall-Klassen in Firewall-Architekturen verbunden

Firewall Architekturen

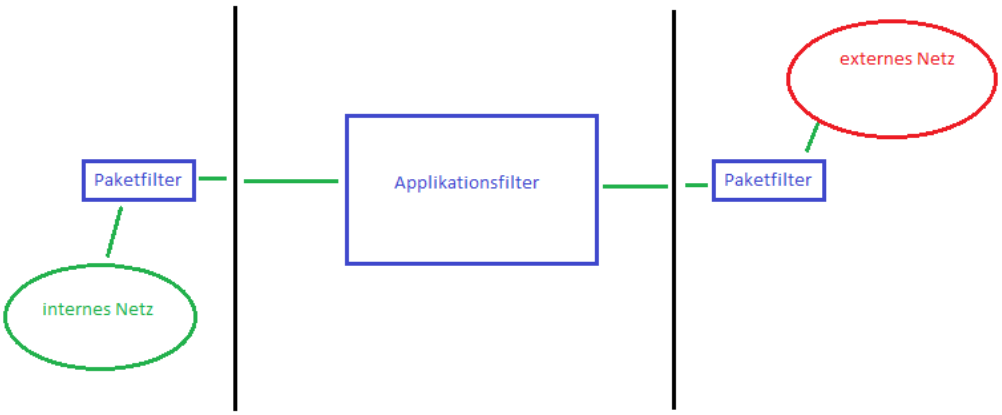
- Firewalls sind sicherheitskritisch, daher so wenig andere Software wie möglich (Angriffsvektoren)

- Dual-Homed Firewall
- Screened-Host
- Screened-Subnet

Dual-Homed Firewall

- 2 Netzwerkschnittstellen (2 Teilnetze)
- Keine IP-Routing oder IP-Forwarding Dienste (Isolierung für Paketanalyse)
- Single Point of Failure (kaum noch verwendet)

Dual-Homed Firewall

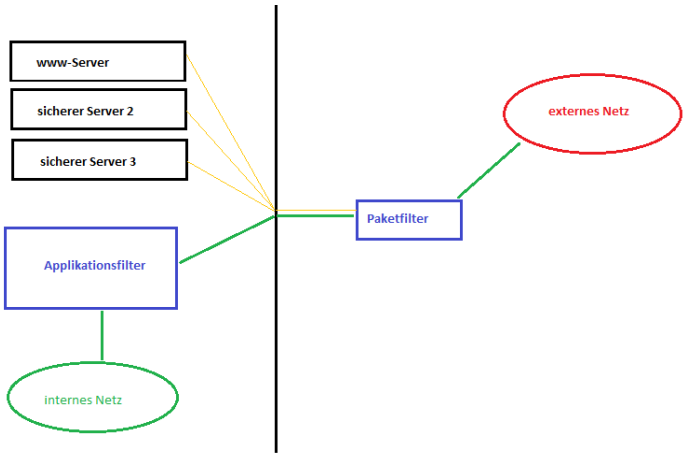


Quelle: Eigene Darstellung

Screened-Host

- "Überwachte Rechner"
- 1 Netzwerkschnittstelle (nur privates Netz)
- Paketfilter vor dem Bastionsrechner (Applikation-Filter)
- Bastionsrechner und Paketfilter im gleichen Netzsegment
- Wichtig: Router ist sicherheitskritisch, er muss jeglichen Datenverkehr vom externen ins interne Netz durch den Filter zum Bastionsrechner routen
- Große Flexibilität (Paketfilter kann Pakete am Bastionsrechner vorbei schleusen)

Screened-Host

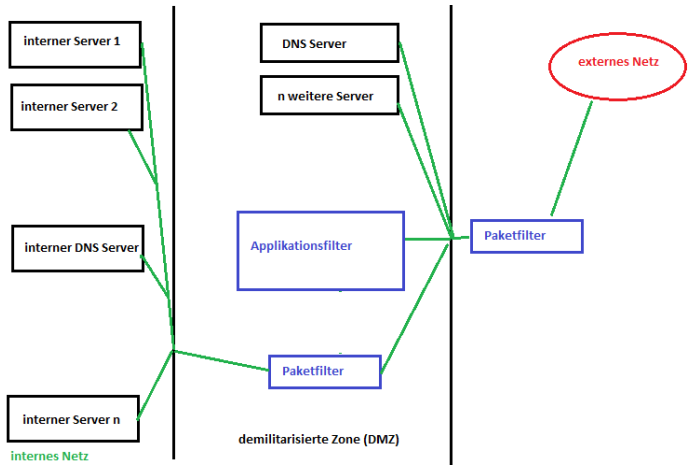


Quelle: Eigene Darstellung

Screened-Subnet

- "Überwachte Teilnetze"
- Screened-Host um 1 Netzsegment erweitert -> komplette Isolation
- Bastionsrechner nur mit dem externen Netz verbunden
- Zur Erreichung der isolierten Netzsegmente: Router vor und nach dem Bastionsrechner. Dadurch entsteht nach außen und Innen isoliertes Netz (demilitarisierte Zone = DMZ)

Screened-Subnet



Quelle: Eigene Darstellung

Fazit / Ausblick

- Gut konfiguriert: Sicherheitsgewinn
- Sicherheit ist Anforderungsabhängig (Kombination versch. Filtertechnologien)
- Zentralisierung und Bündelung von Sicherheitsdiensten
- Paketfilter -> generische Sicherheitsdienste (Transportebene) -> Applikationsfilter
- Risiken
  - Einrichtung und Wartung nicht trivial: Netzstrukturen, OS, Bedrohungen
  - Kenntnis interner Netzstruktur um Umgehen der Firewall zu verhindern
  - Psychologie: Firewall? Mir kann ja nichts passieren!
  - Tunneling
  - Mobile Geräte

Vielen Dank für die Aufmerksamkeit!

- Bei Unklarheiten oder Thesen nicht zögern, sondern fragen :-)

Quellen

(1) Eckert, Claudia, IT-Sicherheit: Konzepte – Verfahren – Protokolle. München 2012, Oldenbourg Wissenschaftsverlag GmbH

(2) Lessing, Andreas G, Linux Firewalls: Ein praktischer Einstieg. Köln 2006, O'Reilly Verlag GmbH und Co KG

(3) Ietf.org

(4) w3.org

(5) Nießen, Benedikt: Der eigene Server mit FreeBSD 9. Heidelberg 2012, dpunkt.verlag GmbH