Firewalls

Definition

Alle Schutzmaßnahmen, die den Datenverkehr zwischen zwei Netzen kontrollieren.

Aufgaben

- Kontrolle des Zugriffs von internen Netzen auf Ressourcen im Internet (Webseiten, Dienste, …)
- Verhinderung unberechtigter Zugriffe aus dem externen Netz auf das interne Netz
- Protokollierung der nicht berechtigten Zugriffsversuche, der Netzzugriffe und Dienste

Zwei grundlegende Funktionsprinzipien

- Blacklist, es ist alles erlaubt, was nicht verboten ist
- Whitelist, es ist alles verboten, was nicht erlaubt ist

Aufbau einer Firewall

- Firewall
  - Paketfilter
    - statisch
    - dynamisch
  - Application Gateway

Paketfilter

- arbeitet auf dem Network- und Transport-Layer (3+4)
- analysiert die Header von TCP/UDP und IP und wendet Filterregeln (sogenannte Access Control Lists) an
- entscheidet anhand der IP-Adressen und Port-Adressen, welches Paket die Firewall passieren darf
- statisch: hier werden dauerhaft feste Portnummern und IP-Adressen im Filter interpretiert
- dynamisch: ein ausgehendes Paket wird analysiert und die benötigten Ports werden kurzfristig für das Antwortpaket von externen Netzen freigegeben → stateful inspection

Application Gateway

- stellt auf der Anwendungsschicht eine Verbindung in andere Netze her
- filtert Inhalt der Datenpakete und trifft Weiterleitungsentscheidungen anhand von Begriffen (Content Filter) oder URLs
- arbeitet häufig als Proxy-Server (Proxy = Stellvertreter)
  - der Datenaustausch mit dem Internet wird vom Proxy-Server als Stellvertreter durchgeführt
  - die Verbindung des Clients mit dem Internet besteht nur virtuell
  - Web-Seiten werden gecached
  - Für jede Anwendung muss ein entsprechender Proxy-Dienst zur Verfügung gestellt werden
- Beispiele: ISA-Server, Squid