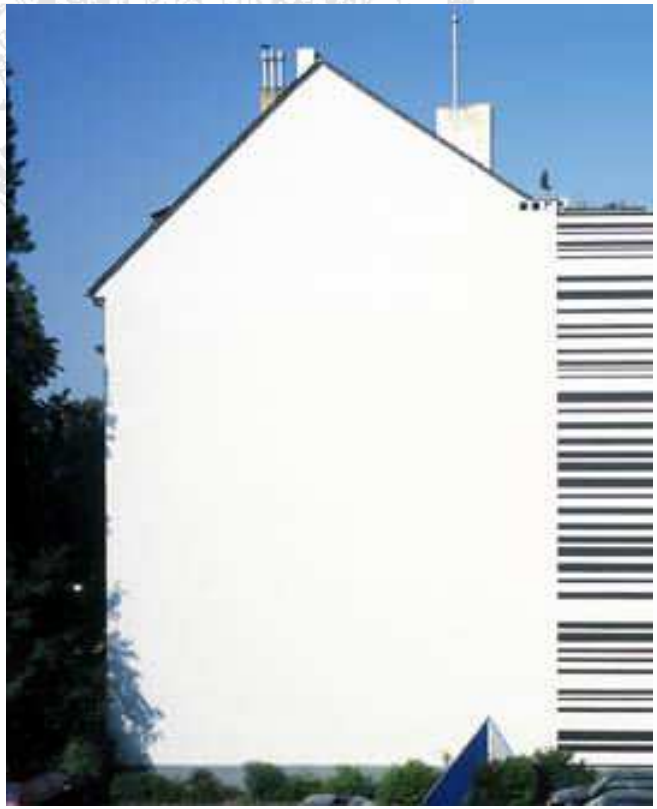
Uni-Firewall

Absicherung des Überganges vom Hochschulnetz
zum Internet am Wingate

(Helmut Celina)

Was ist eine Firewall?



oder

Was ist eine Firewall?

- Eine Firewall muss ein „Tor“ besitzen
- Schutz vor Angriffen erfolgt, indem nur kontrollierte Verbindungen zugelassen werden
- nur so zuverlässig wie die Kontrolle der Verbindungen
- kein Schutz vor Angriffen von innen
- kein Schutz vor zulässigen Verbindungen
- kein Schutz vor Verbindungen an der Firewall vorbei
- Kontrollen für beide Richtungen möglich

Welche Arten von Firewalls gibt es?

- Paketfilter (Access Control List – ACL)
- Reflexive ACLs
- Transparent Proxy
- Application Level FW
- Stateful Inspection FW
- Air Gap / Split Reverse Proxy
- Personal FW (Host-Based FW)

Paketfilter (ACLs)

- Unterscheidung von IP-Paketen anhand von Quell- und Ziel-IP-Adresse sowie Dienste-Ports
  - OSI-Layer 3 und 4
  - Bsp.: WWW-Zugriff 80.145.89.151 → 132.187.3.5:80
- bei verbindungslosen Protokollen (z.B. udp) Antwortpakete nicht zuzuordnen
- bei tcp Verbindungskontrolle über Flags
- Schwierigkeiten bei Diensten mit dynamisch ausgehandelten Ports und Diensten mit Verbindungsaufbau von außen (z.B. active ftp oder X11)

Reflexive ACLs

- Erweiterung von ACL-Paketfilter
- erlaubter Verbindungsaufbau von innen erzeugt Regel für Antwortpakete
- theoretisch Lösung für udp etc.
- bislang nicht zuverlässig implementiert (Probleme mit Timeouts etc.)

Transparent Proxy

- Client adressiert eigentliche Zieladresse
- Anfrage wird aber vom Proxy (Stellvertreter) entgegengenommen und weitergereicht
- Server adressiert Proxy, der die Antwort weiterreicht
- z.B.: NAT
- „dedicated proxy“: spezielles Softwarepaket für ein bestimmtes Protokoll; damit kann der Paketinhalt ausgewertet werden

Application Level Firewall

- setzt Pakete zusammen und untersucht Inhalt auf Applikationsebene (OSI Layer 7): z.B. Virenscanner, http-Filter, ftp-Verbindungsüberwachung usw.
- erstellt dynamische Regeln
- verwendet „dedicated proxies“
- hohe Hardwareanforderung
- hoher Konfigurations-/Administrations-Aufwand

Stateful Inspection Firewall

- Kombination aus Paketfilter und Application Level FW
- speichert Statusinformationen für Verbindungen (Quelle, Ziel, Sequenznummern, belegte Ports, Offsets usw.) und fungiert dann als Paketfilter
- kann Ports dynamisch freigeben wenn protokollspezifische Module vorhanden sind

Sonstige

- Air Gap / Split Reverse Proxy
- Personal FW (Host-Based FW)
  - kann Features beinhalten, die nicht im eigentlichen Sinn zu einer FW gehören
  - z.B. IDS/IPS, Prozesszugriffskontrolle, Sandbox, Personalprotektoren (nicht zu empfehlen)

Was für eine Firewall ist zur Zeit am Wingate im Einsatz?

- Paketfilter auf Ebenen 3 und 4
- überwiegend Blacklist
- Whitelist für Server-Blöcke in manchen Subnetzen

Was für eine Firewall ist für das Wingate geplant?

- Router-Einschubkarte
- Stateful Inspection mit Protocol Inspection Engines
- kombinierte Black- und Whitelist

Wichtig:

- eine zentrale Firewall ist nur ein Bestandteil eines Sicherheitskonzeptes
- eine zentrale Firewall ersetzt nicht
  - regelmäßige System-Updates
  - aktuelle Antiviren-Software
  - „gute“ Passworte
  - Sperren ungewollter Dienste auf dem eigenen PC (Personal FW)
  - sichere Netzprotokolle
  - Vorsicht
  - …