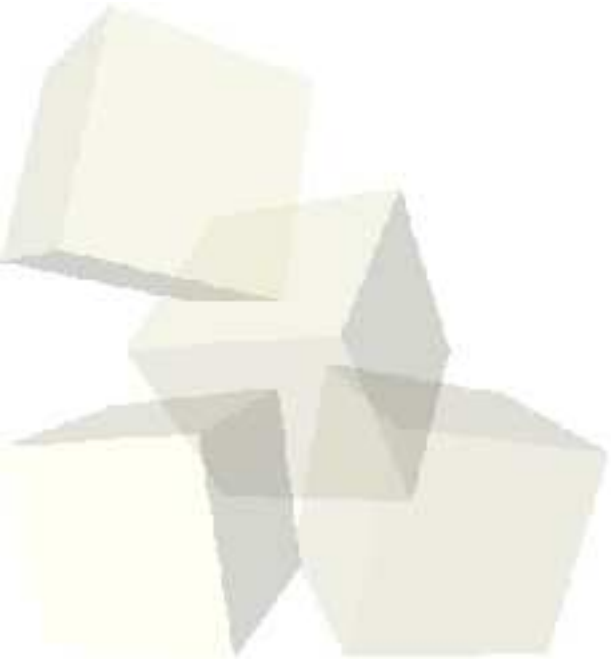
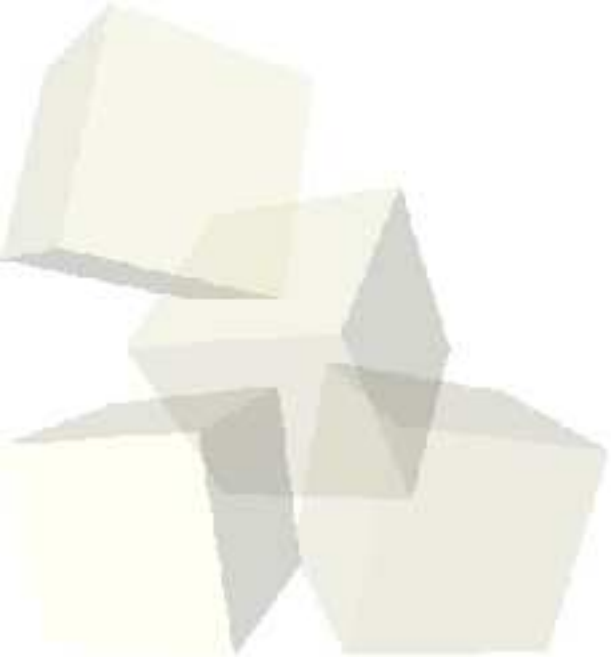
Konzepte zum Aufbau von Firewalls

Christian Schromm
(christian@schromm-net.de)



Übersicht

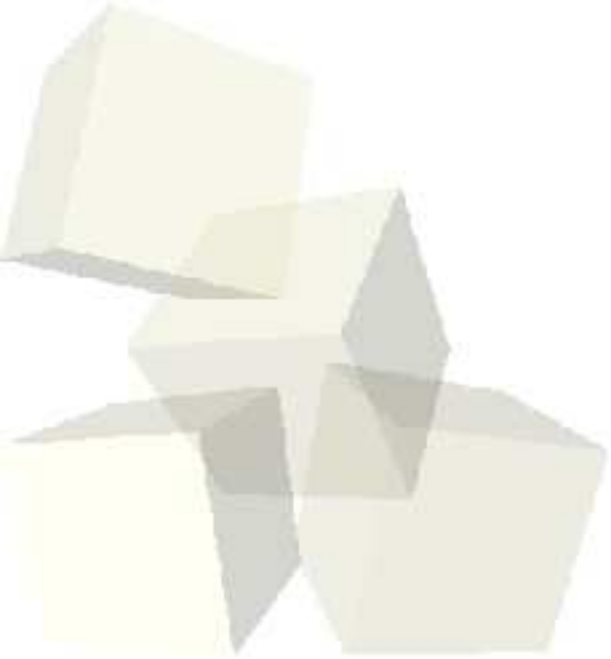
- Motivation zum Betreiben von Firewalls
- Mögliche Angriffsarten auf Rechner(-netze)
- Firewallkomponenten und Architekturen
- Wirkungsbereich von Firewalls
- Beurteilung



Motivation zum Betreiben von Firewalls

- Firewall als „Türsteher“
- Zentral verwaltetes Sicherheitsinstrument

- Schutz vor Datenverlust
- Schutz vor Missbrauch von Ressourcen
- Schutz vor Schädigung des Rufs



Mögliche Angriffsarten auf Rechner(-netze)

- Motivation zum Betreiben von Firewalls
- Mögliche Angriffsarten auf Rechner(-netze)
  - (Distributed) Denial of Service: DoS/DDoS
  - Malicious Software
  - Ausnutzung von Fehlern (Exploits)
  - Manipulieren/Abhören von IP-Paketen
- Firewallkomponenten und Architekturen
- Wirkungsbereich von Firewalls
- Beurteilung

(Distributed) Denial of Service: DoS/DDoS

- Ziel: Lahmlegen eines Dienstes oder Computers
- Methoden:
  Ziel mit Anfragen überfluten oder Fehler im OS oder Dienst ausnützen

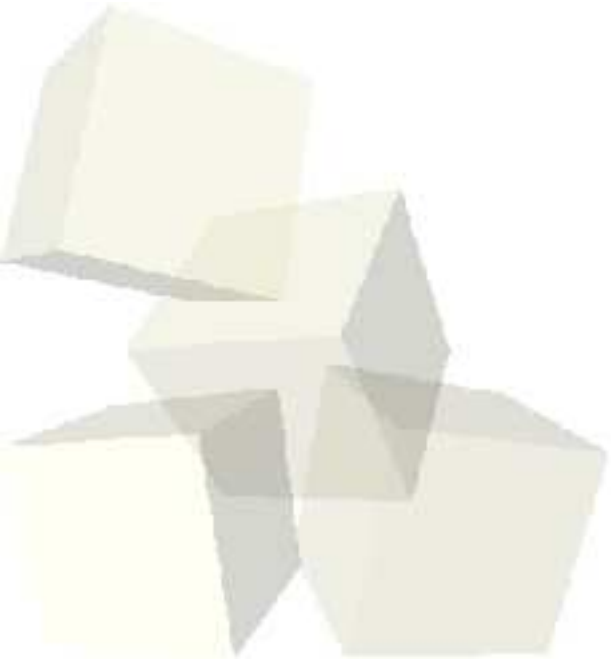
- Wird immer bemerkt → häufig nur letztes Mittel
- Einfach durchzuführen („*Werkzeug von Script Kiddies*“)
- Angriff von mehreren Rechner gleichzeitig → DDoS

Malicious Software

- Sich selbst reproduzierende und weiterverbreitende Software
- Installieren Backdoors oder Passwortschnüffler
- Verbreitung über
  - Mail
  - CIFS
  - IRC
  - Aktive Dokumentinhalte (Makros)
- Bekannt als Viren, Trojaner, Würmer etc.

Ausnutzung von Fehlern (Exploits)

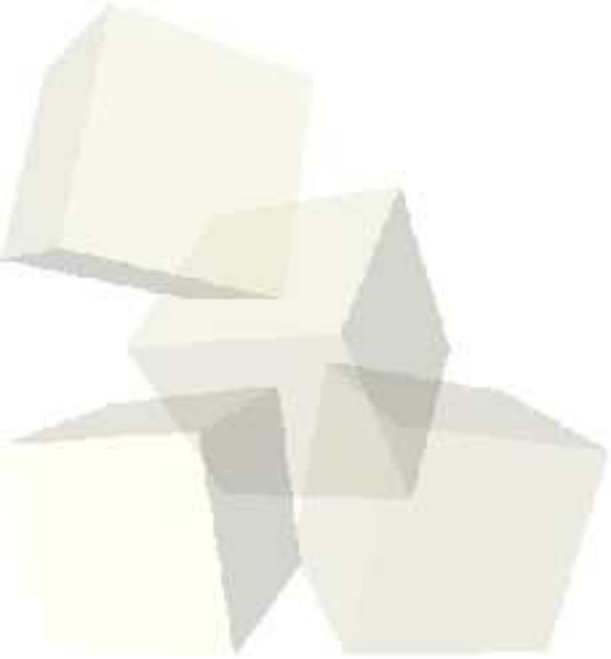
- Großzügig vergebene
  - Zugriffsrechte von Dateien/Verzeichnissen/Programmen
  - SUID/SGID – Bits
  - Zugriff auf /etc/passwd bzw. /etc/shadow ermöglichen den Einsatz von Passwort-Knackern



Ausnutzung von Fehlern (Exploits)

- Großzügig vergebene
  - Zugriffsrechte von Dateien/Verzeichnissen/Programmen
  - SUID/SGID – Bits
  - Zugriff auf /etc/passwd bzw. /etc/shadow ermöglichen den Einsatz von Passwort-Knackern

- Buffer Overflow-Angriffe (auch übers Netzwerk) öffnen häufig eine root-shell



Ausnutzung von Fehlern (Exploits)

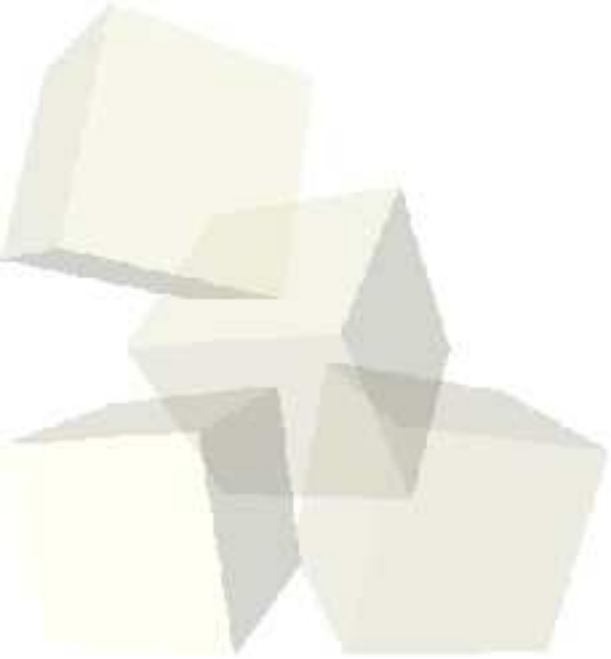
- Großzügig vergebene
  - Zugriffsrechte von Dateien/Verzeichnissen/Programmen
  - SUID/SGID – Bits
  - Zugriff auf /etc/passwd bzw. /etc/shadow ermöglichen den Einsatz von Passwort-Knackern

- Buffer Overflow-Angriffe (auch übers Netzwerk) öffnen häufig eine root-shell

- Bleiben i.d.R. unbemerkt
- Sind sehr lukrativ

Manipulieren/ Abhören von IP-Paketen

- Abhören des IP-Verkehrs
  - Mitlesen von Klartextpasswörtern



Manipulieren/ Abhören von IP-Paketen

- Abhören des IP-Verkehrs
  - Mitlesen von Klartextpasswörtern
- Port-Scanning (stealth-scans)
  - Auskundschaften des Ziels
  - Überprüfen von offenen Ports
  - Ermitteln (häufig) das OS
  - Verbindungslose scans (stealth) werden häufig nicht erkannt

Manipulieren/ Abhören von IP-Paketen

- Abhören des IP-Verkehrs
  - Mitlesen von Klartextpasswörtern
- Port-Scanning (stealth-scans)
  - Auskundschaften des Ziels
  - Überprüfen von offenen Ports
  - Ermitteln (häufig) das OS
  - Verbindungslose scans (stealth) werden häufig nicht erkannt
- IP-Spoofing: Einsatz von gefälschten IP-Paketen
  - Ziel- oder Absenderadresse
  - Ziel- oder Absenderport
  - Fragmentierte Pakete

Firewallkomponenten und Architekturen

- Motivation zum Betreiben von Firewalls
- Mögliche Angriffsarten auf Rechner(-netze)
- Firewallkomponenten und Architekturen
  - Paketfilter (Screening Router: stateful/stateless)
  - Proxies (Application Layer Gateways)
  - Netzanbindung ohne Bereitstellung von Diensten
  - Grenznetz (DMZ) für externe Dienste
  - Bastion Host
- Wirkungsbereich von Firewalls
- Beurteilung

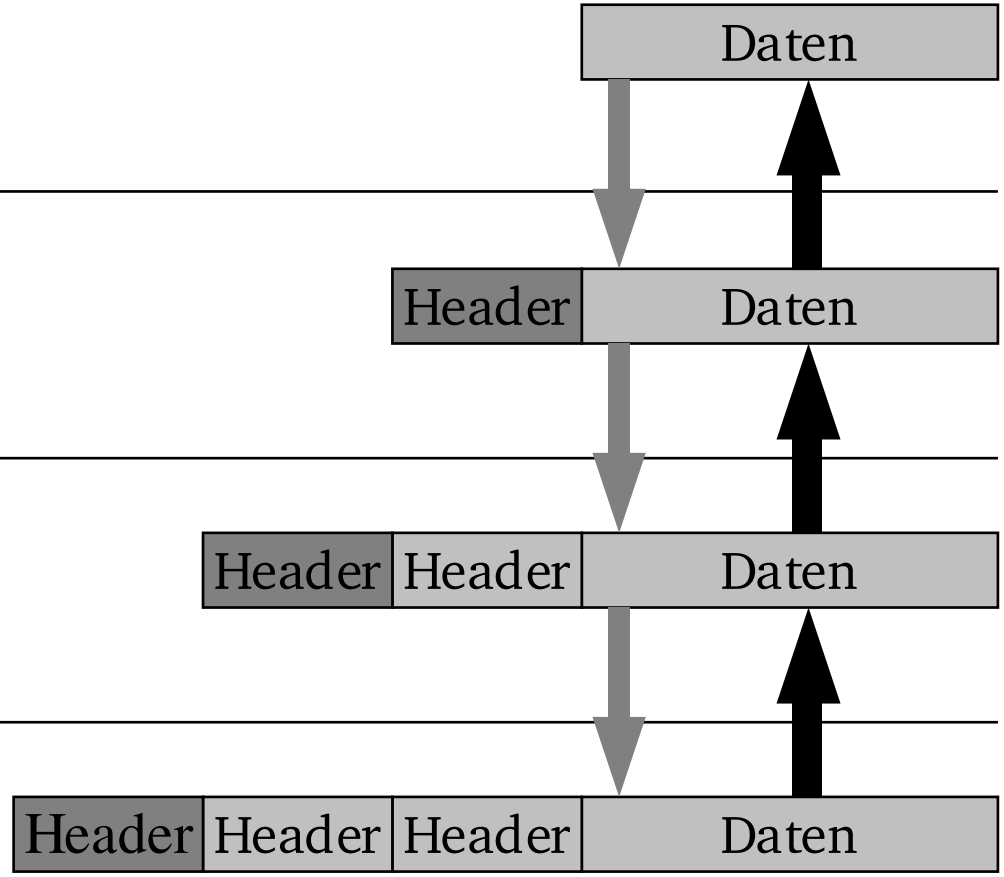
Schichtenmodell

Anwendungsschicht
(SMTP, DNS, IMAP, FTP etc.)

Transportschicht
(TCP, UDP, ICMP)

Internet-Schicht
(IP)

Netzzugangsschicht
(Ethernet, FDDI, TokenRing etc.)



Paketfilter (Screening Router)

- Arbeiten auf Internet- und Transportschicht
- Überprüfen anhand der Headerinformationen die Gültigkeit eines Paketes
- Überprüfung möglich nach
  - Ziel-/Herkunfts-IP
  - Ziel-/Herkunftsport
  - Flags (SYN, ACK, FIN etc.)
- Werten nur den Inhalt der Header aus, nicht aber den der Datensegmente
- Logging der Pakete
- Können eigenes Netzwerk verstecken (NAT)

Stateful vs. Stateless Packetfilter

Stateful

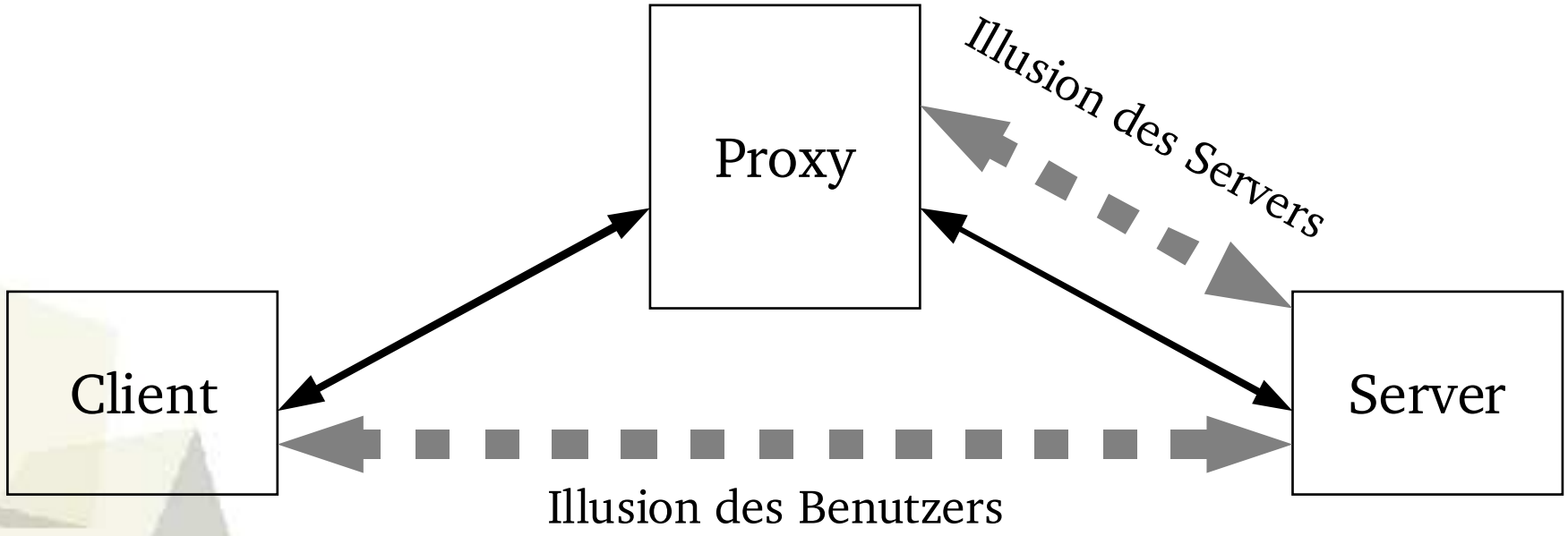
- Erkennt zu bestehender Verbindung gehörende Pakete
- Speicherung von Verbindungsdaten notwendig (Angriffspunkt für DoS-Attacken!)

Stateless

- Filtern nur Pakete zum Vebindungsaufbau, Folgepakete nicht mehr
- Reassemblierung fragmentierter Pakete vor dem Filtern ist notwendig, um versteckte Angriffe abzuwehren

Proxies (Application Layer Gateways)

- Arbeiten auf Anwendungsschicht
- Bieten Stellvertreterfunktion für Verbindungen zu anderen Netzen (z.B. Internet)

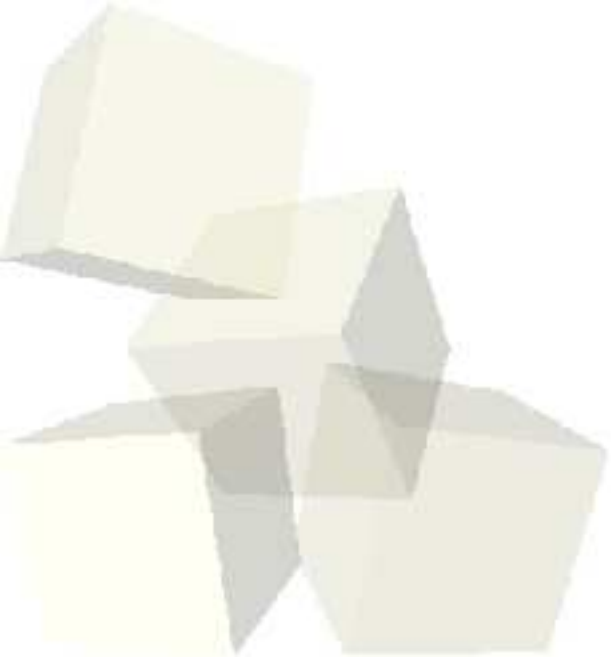


Scheinbare Verbindung

Tatsächliche Verbindung

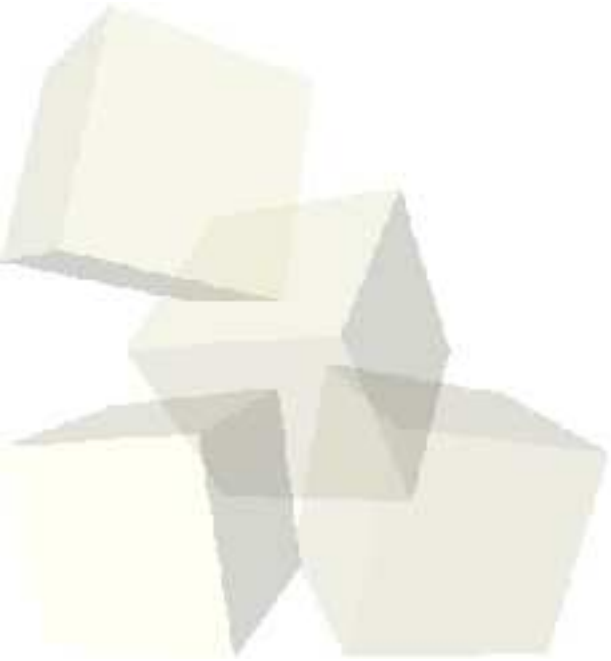
Vorteile von Proxies

- Untersuchung der Paketinhalte nach bösartigem Code (DDoS, Java/Javascript, Viren, Spam-Mail ...)
- Bessere Protokollierungsmöglichkeiten
- Filterung auch per User möglich
- Keine direkte Client-Server Verbindung
- Client-IP bleibt verborgen



Nachteile von Proxies

- Eigener Proxy für jeden Dienst erforderlich
- Häufig sind spezielle Konfigurationen an den Clients vorzunehmen
- Für manche Dienste gibt es keinen Proxy
- Unsichere Dienste (telnet, ftp ...) werden durch einen Proxy auch nicht sicherer



Generischer Proxy

- Ist nicht für bestimmten Dienst beschränkt einsetzbar

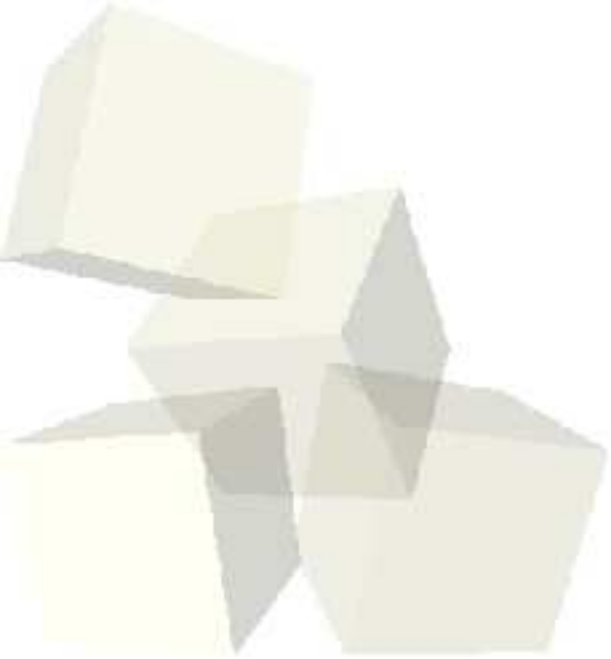
Nachteile gegenüber dedizierten Proxies:

- Kann kein Content Filtering
- Keine Benutzerauthentifizierung

Vorteile gegenüber fehlenden Proxies:

- Keine direkte Client-Server Verbindung
- Client-IP bleibt verborgen

- Immer abhängig von den jeweiligen Anforderungen
- Optimale Ausschöpfung aller Filtermöglichkeiten
- Minimaler Administrationsaufwand
- Minimale Störung der Benutzer



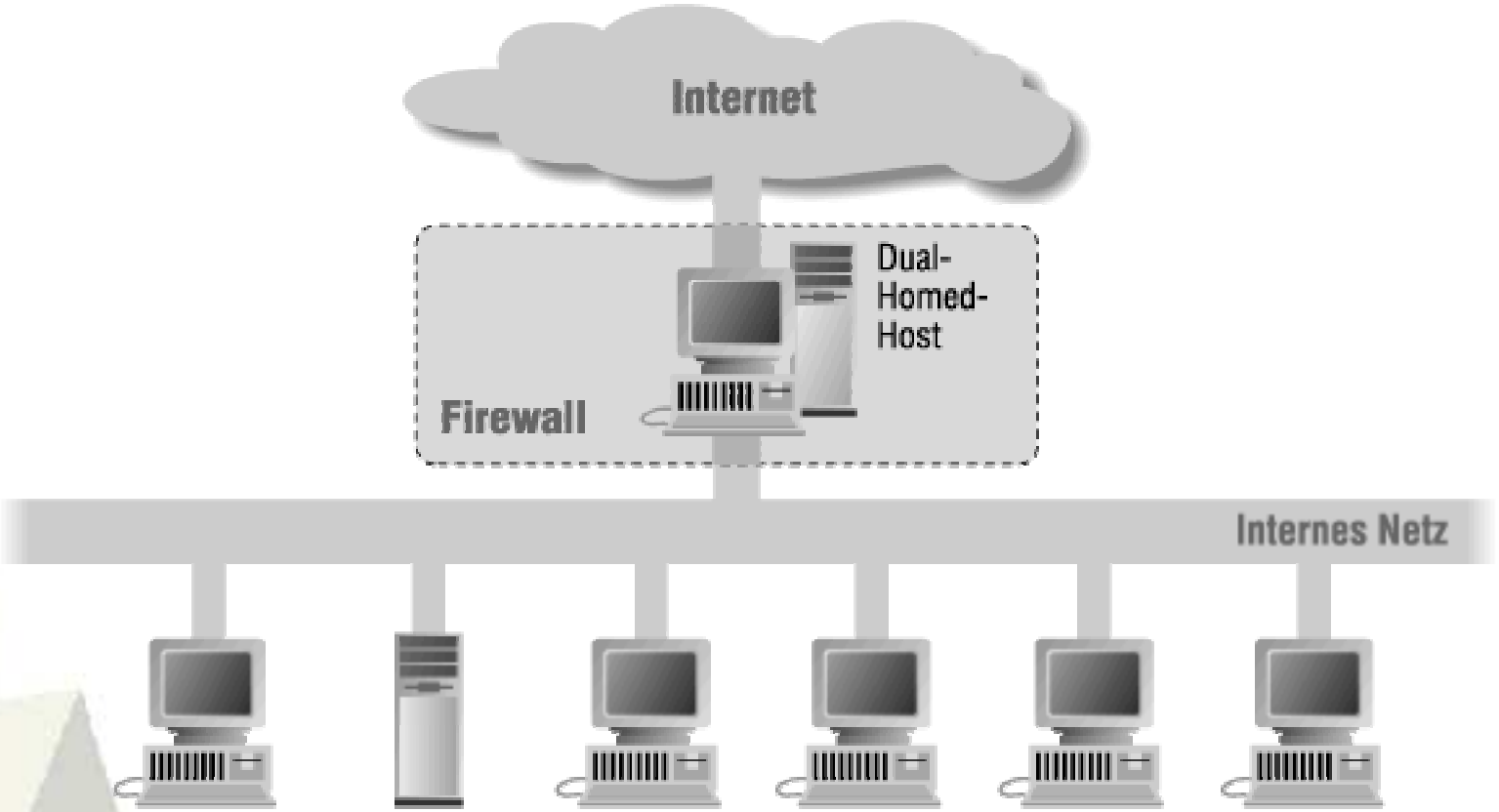
Netzanbindung ohne Bereitstellung von Diensten

- Screening Router
  - DDoS
  - Verstecken des Netzwerks (Portscans)
  - Abwehr von gespooften Paketen

- Proxy
  - Maskiert internes Netz
  - Macht Content-Filtering

- Können bei Softwarelösung auf gleichem Rechner laufen
- Bei Harwarerouter muss dieser zwischen dem Internet und dem Proxy stehen (spoofing!)

Netzanbindung ohne Bereitstellung von Diensten



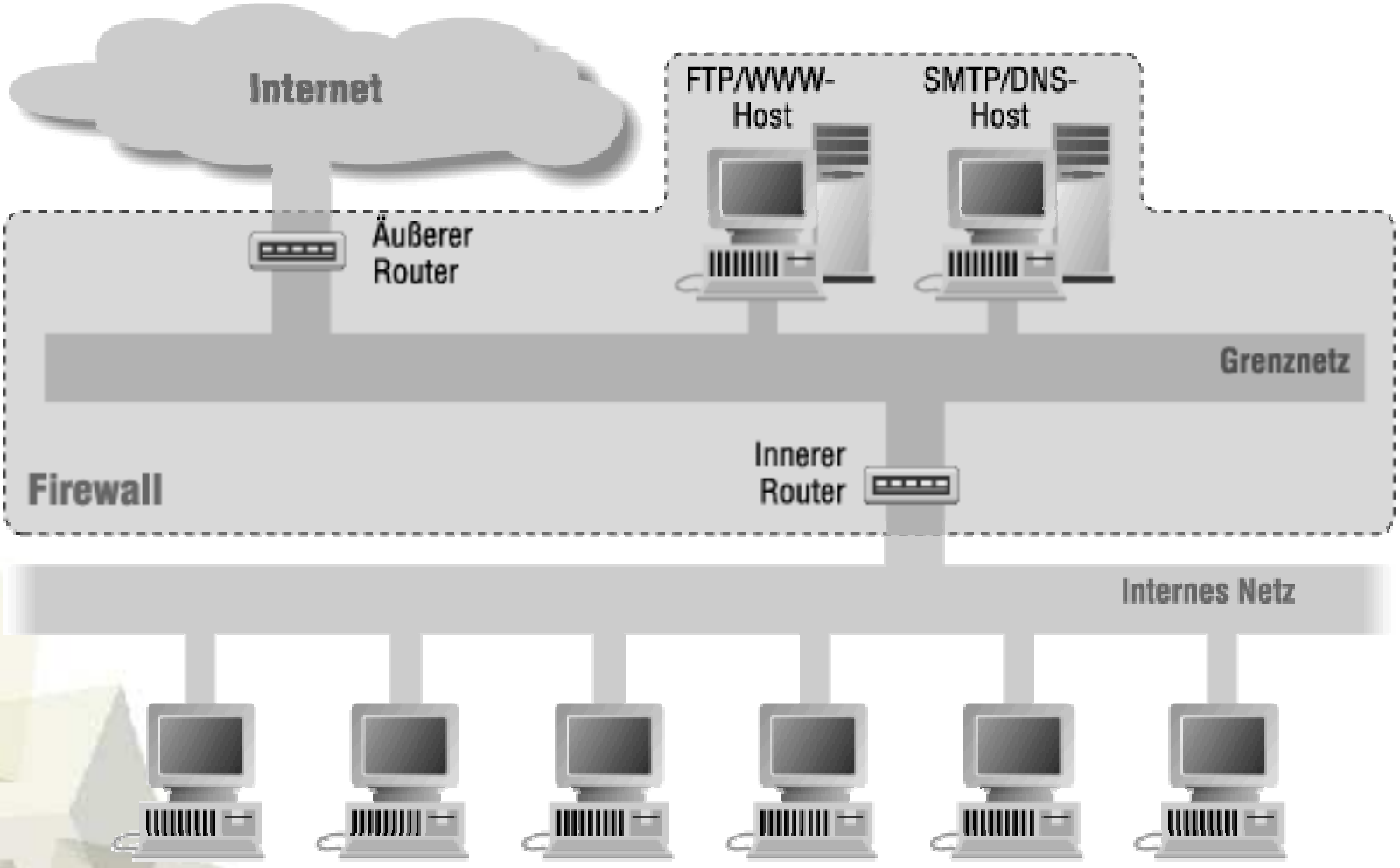
Quelle: Einrichten von Internet Firewalls, Chapman & Zwicky,O'Reilly

Grenznetz (DMZ) für externe Dienste

- Nach außen angebotene Dienste werden in ein Zwischennetz zwischen Intra- und Internet gestellt (DeMilitarisierte Zone)
- DMZ gilt als prinzipiell unsicher
- Absicherung zum Internet durch Paketfilter und Proxy

- Absicherung des Intranet durch mindestens einen Proxy, besser zusätzlich durch einen weiteren Paketfilter
  - Zweiter Paketfilter hat im günstigsten Fall andere Eigenschaften als der erste (stateful/stateless)
- Innerer Router/Proxy betrachtet DMZ als unsicher; strengere Filterregeln notwendig

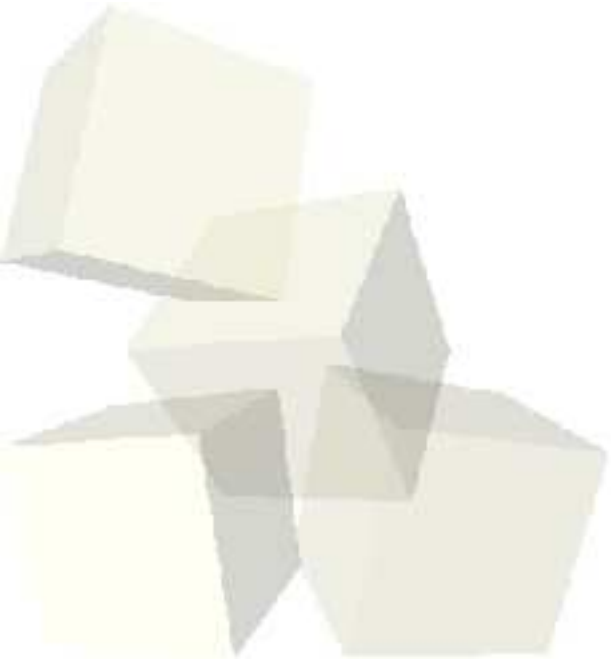
Grenznetz (DMZ) für externe Dienste



Quelle: Einrichten von Internet Firewalls, Chapman & Zwicky,O'Reilly

Bastion Host

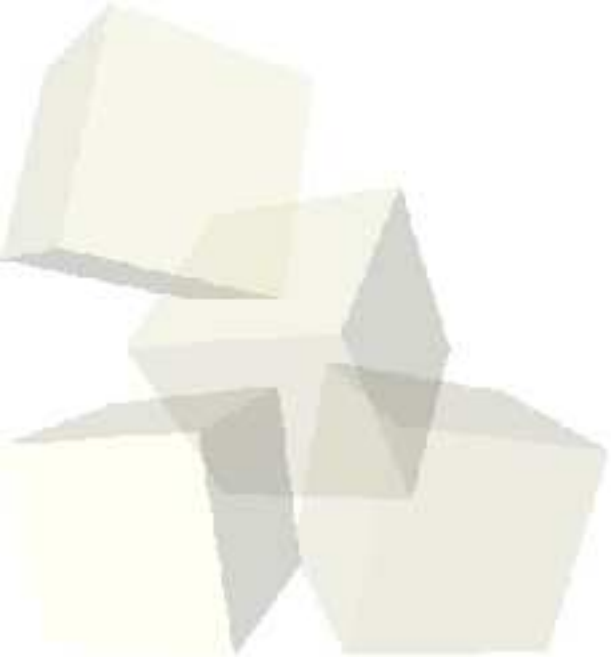
- Besonders abgesicherter Rechner
  - Keine unnötige Software
  - Keine User Accounts
  - Keine SUID/SGID-Bits



Bastion Host

- Besonders abgesicherter Rechner
  - Keine unnötige Software
  - Keine User Accounts
  - Keine SUID/SGID-Bits
- Einsatzgebiete
  - Proxies in der DMZ bei Verwendung von HW-Routern
  - ARGUS-Hosts
  - Log-Host

- Motivation zum Betreiben von Firewalls
- Mögliche Angriffsarten auf Rechner(-netze)
- Firewallkomponenten und Architekturen
- Wirkungsbereich von Firewalls
- Beurteilung

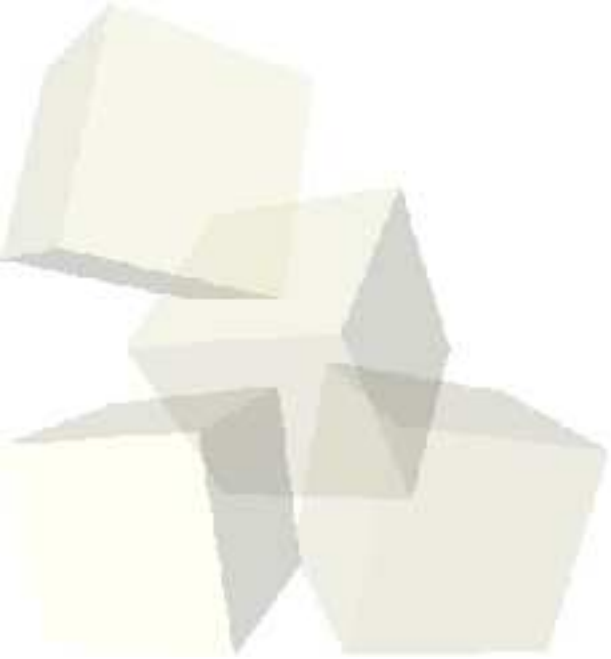


Was kann ein Firewallsystem?

- Verkleinerung der potentiellen Angriffsfläche eines Netzwerks durch
  - Sperrung nicht benötigter Ports
  - Vergabe spezifischer Zugriffsrechte von externen Netzwerken
  - Maskierung des Intranet
- Filterung des Inhalts von Paketen
- Protokollierung des Netzwerkverkehrs zur Früherkennung bzw. Zurückverfolgung von Angriffen
- Schutz vor Überlastung des eigenen Netzwerks bei DoS-Attacke auf Netzwerkbasis

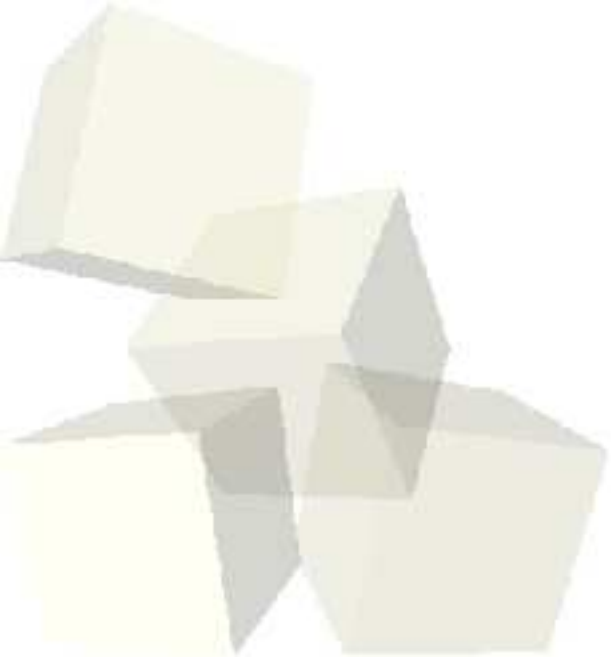
Was kann ein Firewallsystem nicht?

- Filtern unbekannter Schädlinge (Viren ...)
- Angriffe aus dem eigenen Netz abwehren (möglicherweise von Mitarbeiter durchgeführt)
- Verhalten von Benutzern zu 100% kontrollieren
- Abwehr neuartiger Angriffe
- Sicherung von Einwahlzugängen (brauchen eigene Schutzmechanismen)

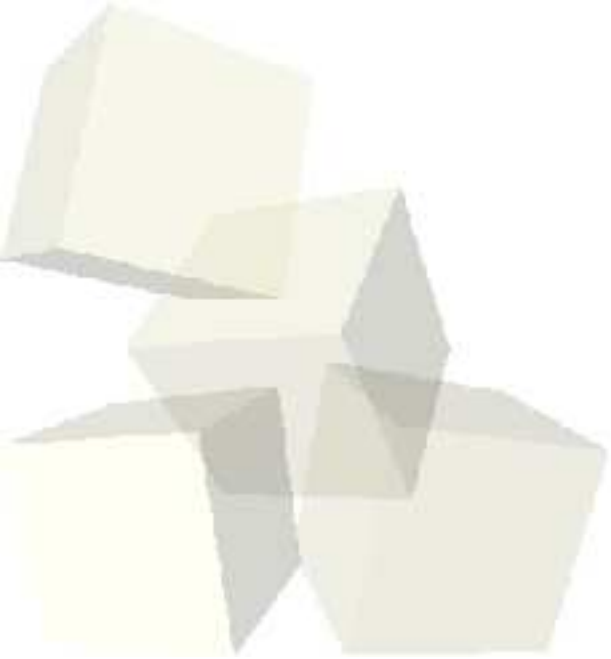


Übersicht

- Motivation zum Betreiben von Firewalls
- Mögliche Angriffsarten auf Rechner(-netze)
- Firewallkomponenten und Architekturen
- Wirkungsbereich von Firewalls
- Beurteilung



- Kein Netzwerk kann zu 100% sicher gemacht werden!
- Firewalls erhöhen den Schutz und sind nötig
- Firewalls sind nur ein Teil einer Sicherheitspolitik, welche ferner enthalten sollte:
  - Sensibilisierung der Benutzer
  - Host-Security
  - Regelmäßiges Einspielen von Patches
  - Backups



Beurteilung

- Kein Netzwerk kann zu 100% sicher gemacht werden!
- Firewalls erhöhen den Schutz und sind nötig
- Firewalls sind nur ein Teil einer Sicherheitspolitik, welche ferner enthalten sollte:
  - Sensibilisierung der Benutzer
  - Host-Security
  - Regelmäßiges Einspielen von Patches
  - Backups

Das Ziel ist, einem potentiellen Angreifer möglichst viele Hindernisse in den Weg zu stellen.
Ein Angriff kann immer erfolgreich sein. Ob dem so ist, ist eine Kosten/Nutzen-Frage.