Firewalls

Thomas Dornseifer
Informationssicherheit im E-Learning

Inhalt

1. Firewall-Grundlagen
   - Begriff „Firewall“
   - Ziele und Möglichkeiten
2. Elemente von Firewalls
   - Packet Filter
   - Stateful Packet Filter
   - Application Level Gateways und Proxies
3. Architektur von Firewall-Systemen
4. Firewalls im E-Learning

Der Begriff „Firewall“

- Definition:

  Hardware oder Software, welche jeglichen Netzwerkverkehr zwischen zwei Netzwerken gemäß eines Regelwerks filtert.
- „Brandschutzmauer“
- Sicherheitskonzept mit mindestens einer technischen Komponente
- zwei Grundbestandteile:
  - Paketfilter
  - Application Level Gateways
- OSI-Schichtenmodell

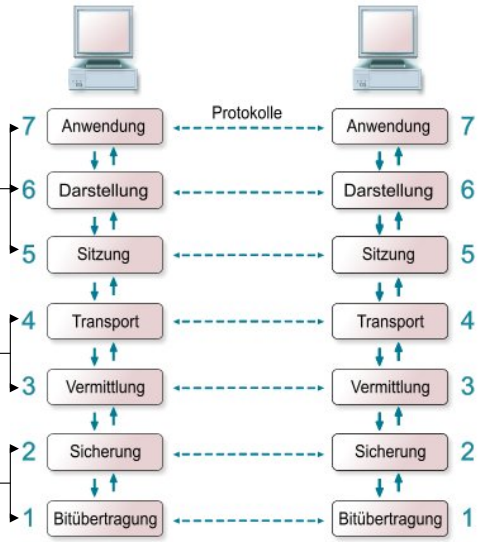
Der Begriff „Firewall“

- OSI-Schichtenmodell
  - *„Open Systems Interconnection Reference Model“*
  - Nachrichtenübermittlung in offenen Kommunikationssystemen

Anwendungsorientiert
Application Level Gateways

Übertragungsorientiert
Packet Filter

Physikalisch



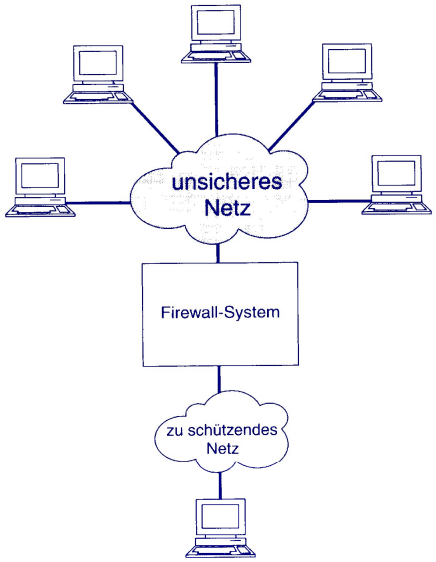
[1]

Ziele und Möglichkeiten von Firewall-Systemen

UNIVERSITÄT SIEGEN

– Firewall zwischen „sicheren“ und „unsicheren“ Netzen

„Common Point of Trust“ = „Single Point of Failure“



[2]

Ziele und Möglichkeiten von Firewall-Systemen

UNIVERSITÄT SIEGEN

Common Point of Trust
- zentrale Sicherheitspolitik
- konzentrierte Sicherheitsmechanismen
- einfache Protokollierbarkeit
- Authentifikation der Benutzer

⟺

Single Point of Failure
- ein Angriffspunkt, keine Redundanz
- Konfiguration der Firewall bedingt Sicherheitsniveau des gesamten Netzes

Lösung: Kombination zentraler und dezentraler Firewall-Elemente zu Firewall-Systemen

Ziele und Möglichkeiten von Firewall-Systemen

UNIVERSITÄT SIEGEN

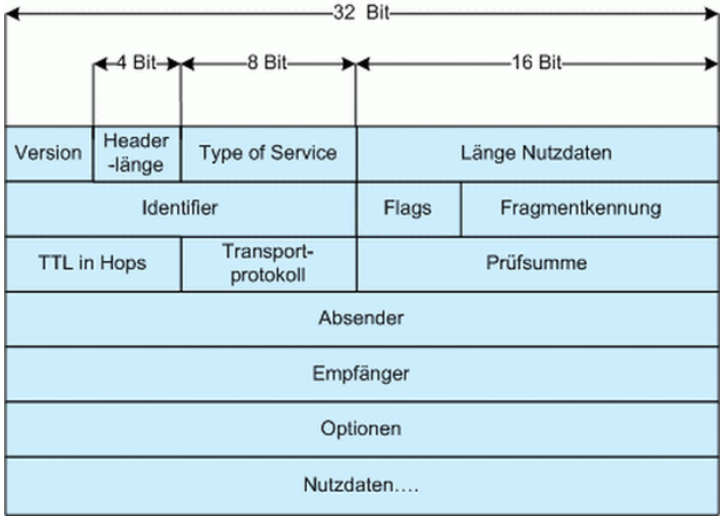
– Mögliche Zielsetzungen von Firewall-Systemen:
  - Zugangskontrolle
  - Rechteverwaltung
  - Kontrolle auf Anwendungsebene
  - Entkopplung von Diensten
  - Beweissicherung und Protokollauswertung
  - Alarmierung
  - Verbergen der internen Netzwerkstruktur
  - Vertraulichkeit der Nachrichten
  - Accounting

Packet Filter

UNIVERSITÄT SIEGEN

– Erweiterung von Netzwerk-Routern
– Router:
  - Verbinden Subnetze miteinander
  - Interfaces, Routing-Tabellen
  - Physikalische Entkopplung
  - Adressierung von IP-Paketen
  - OSI-Layer 3(/4), *Paketschicht*
    (Flusskontrolle, Aktualisierung von Routing-Tabellen)
– „Selektive Router“
– Analyse der Datenpakete

Packet Filter



Struktur eines IP-Paketes (IPv4) [3]

Packet Filter

- Wichtige Kenngrössen zur Analyse:
  - Protokoll auf Layer 4 (z.B. TCP oder UDP)
    - TCP: Datenströme; verbindungsorientiert, zuverlässig
    - UDP: Datenpakete; verbindungslos, unzuverlässig, geringer Overhead
  - Quell- und Ziel-IP-Adresse
  - Typ der ICMP-Nachricht (Internet Control Message Protocol)
  - Flags
- keine Analyse der Nutzdaten
- Filterregeln auf Basis der Kenngrößen

Packet Filter

Das Regelwerk

– Positives Regelwerk:
  - zunächst jegliche Kommunikation nicht erlaubt; explizite Festlegung der erlaubten Kommunikation
  - kurze Regelliste zugelassenen Netzwerkverkehrs
  - höchstmögliche Sicherheit
– Negatives Regelwerk:
  - zunächst alles erlaubt; Festlegung der verbotenen Kommunikation
  - geringe Sicherheit
  - kompliziertes Regelwerk

Packet Filter

Kenngrössen des Regelwerks

– Quell- und Ziel- IP-Adressen als einzige Kenngröße ungeeignet

Problem:
- *IP-Spoofing*
- *Denial-of-Service*
- *Source-Routing*

Lösung:
- *Sorgfältige Auswahl erlaubter externer IP-Adressen*
- *Source-Routing generell nicht erlauben*

IP-Spoofing:	Versenden von IP-Paketen mit gefälschter IP-Adresse
Denial-of-Service:	Arbeitsunfähigkeit bestimmter Dienste durch Überbelastung
Source-Routing:	Return-Paket „besucht“ auf Rückweg zusätzliche IP-Adressen

Packet Filter

Kenngrössen des Regelwerks

– ICMP-Nachrichten

Problem:
- *„Redirect“ - Befehl*
- *Denial-of-Service durch Umleitung der Daten*
- *Veränderung der Routing-Tabellen*

Lösung:
- *Rechteverwaltung von ICMP-Kommandos*
- *ICMP-Befehle werden von Firewall überprüft*

ICMP-Redirect: Eintragung eines „Umweges“ in die Routing-Tabelle.
Firewall sendet Ausgangspakete über manuell eintragbaren Weg.

Packet Filter

Kenngrössen des Regelwerks

– Flags (Fragmentierung von IP-Paketen)

Problem:
- *starke Fragmentierung (niedrige Maximum Transmission Unit)*
- *Denial-of-Service*
- *keine Kontrolle der Fragmente*
- *Tarnung von Paketen als Fragmente*

Lösung:
Konfiguration interner Netzwerkcomputer:
Ablehnung aller Fragmente bei Abwesenheit des ersten Fragmentes

Maximum Transmission Unit : (MTU) — maximale Paketgrösse für die Übertragung in einem Netzwerk

Packet Filter

Statisches Regelwerk

- „statuslose“ (stateless) Paketfilterung
- „Kein Gedächtnis“
- Beispiel:
  - HTTP-Anforderung an öffentlichen Server aus internem Netz
  - Paket enthält IP-Adresse und Portnummer (>1023) für Antwortpaket
  - Firewall kann Antwortpaket nicht zuordnen
- Lösung: alle Ports größer als 1023 stets geöffnet halten

⇨ „Stateful“ Packet Filter

Packet Filter

- Vorteile von Paketfiltern
  - einfache Konfigurierbarkeit, übersichtliches Regelwerk
  - geringe Kosten durch integrierte Paketfilter
  - hoher Datendurchsatz
  - einfaches Sperren oder Freischalten von Diensten über Ports
  - einfache Festlegung von Nutzungseinschränkungen (zeitlicher Rahmen)
  - Logbuchaufzeichnungen
  - Möglichkeit der Strukturierung des internen Netzwerkes (Subnetze)

Packet Filter

– Nachteile von Paketfiltern
  - keine Kontrolle von Dateiinhalten
  - zu wenige Kenngrößen für Regelwerk
  - Identifikation nur über IP-Adressen
  - Logbuch zeichnet nur IP-Adressen und Dienste auf
  - viele stets geöffnete Ports (Angriffsfläche) bei „stateless“ Paketfilterung
  - niedriges Sicherheitsniveau

Stateful Packet Filter

– Weiterentwicklung der einfachen (statuslosen) Paketfilter
– zu jeder aktuellen Verbindung wird Status verwaltet
– Eingehende Pakete können vorherigen Verbindungen zugeordnet werden
– Intern: Info-Tabelle mit Ports, welche Antwortpakete erwarten
– Bei Verbindungsende (oder nach einer bestimmten Zeitspanne) werden Ports wieder geschlossen
– *Dynamische* Paketfilterung (Regeln werden abhängig von aktuellen Verbindungen generiert und gelöscht)

Stateful Packet Filter

UNIVERSITÄT SIEGEN

- Vorteile:
  - Vorteile einfacher Paketfilter (einfache Bedienung, hoher Datendurchsatz)
  - Zugewinn an Sicherheit im Vergleich zu einfachen Paketfiltern
  - geringerer Konfigurationsaufwand (weniger Regeln)
- Nachteil:
  - Nachteile einfacher Paketfilter bei verringerter Angriffsfläche
  - reduzierte Kontrollierbarkeit des Verhaltens (kein statisches Regelwerk)

Application Level Gateways / Proxies

UNIVERSITÄT SIEGEN

- Arbeit auf Anwendungsschicht des OSI-Modells (Layer 7)
- Häufig realisiert durch Rechnersystem zwischen sicherem und unsicherem Netzwerk
- von unsicherem Netzwerk aus als einziges Rechnersystem erreichbar
- „Bastion Host“
- mögliche Benutzerauthentifikation

Client ⟺ Bastion Host

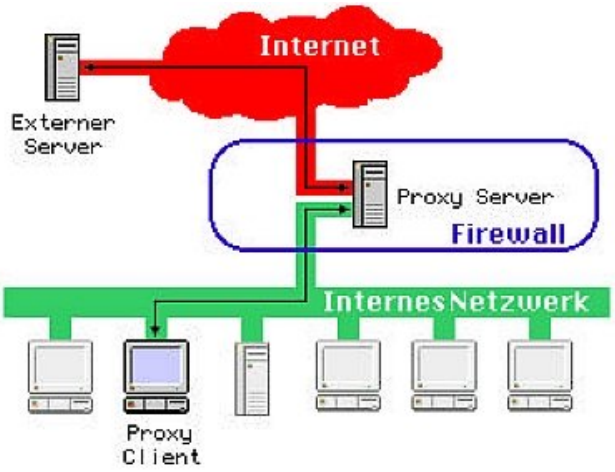
- nach Authentifizierung übernimmt Gateway Kommunikation

Bastion Host ⟺ Zielrechner (unsicher)

Application Level Gateways / Proxies

UNIVERSITÄT SIEGEN

- „Stellvertreter“ zwischen externem Zielrechner und internem Benutzer
- Transparenter Proxy
  - schwer zu umgehen
  - Proxy-Einstellungen können nur am Gateway vorgenommen werden
- physikalische und logische Entkopplung zwischen Kommunikationspartnern
- „Dual-homed“ Proxy



[4]

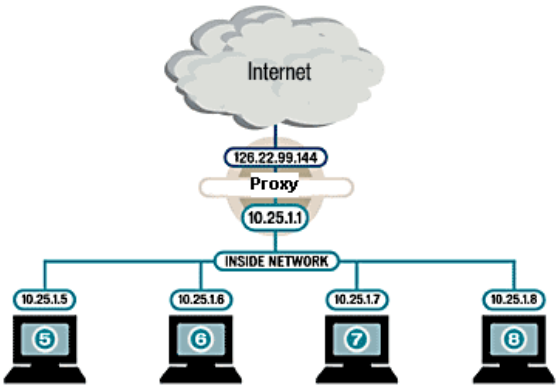
Application Level Gateways / Proxies

UNIVERSITÄT SIEGEN

- zugelassene Pakete werden durch Anwendungsproxy neu erzeugt (für beide Seiten des Datenflusses)
- Kopf- und Anwendungsdaten werden überprüft
- ein Proxy pro Dienst/Protokoll nötig (teilweise kombinierte Lösungen verfügbar)
- nur Software für benötigte Dienste auf Gateway
- Konfigurations- und Instandhaltungssoftware wird ausgelagert
- Network Address Translation (NAT)

Application Level Gateways / Proxies

– Network Address Translation (NAT):
  - NAT-Funktionalität durch andere Mechanismen erreicht als bei Netzwerk-Routern
  - Gateway besitzt zwei IP-Adressen, da „dual-homed“
  - Übersetzung der IP-Adressen in beide Richtungen
  - Nach Außen verbirgt sich das interne Netzwerk hinter einer einzigen IP-Adresse
  - *IP-Masquerading* (Maskierung)



[5]

Application Level Gateways / Proxies

– Vorteile:
  - Anwendungsorientierung (statt Transportorientierung)
  - effektive Filterung (Analyse der Nutzdaten und Neuerstellung der Pakete)
  - Möglichkeit der Manipulation der Pakete (z.B. Entfernung von unerwünschten Inhalten)
  - genaue Protokollierung (Dateinamen, URLs)
  - mögliche Benutzerauthentifikation
  - Reduktion der Netzbelastung durch Zwischenspeichern („Caching“)
  - bei Ausfall: Trennung angeschlossener Netze
  - hoher Schutzwert

Application Level Gateways / Proxies

– Nachteile:
  - aufwändiger Betrieb durch Vielzahl an Proxy-Servern
  - existiert kein Proxy-Server für eine Anwendung: generischer Proxy
  - generische Proxies arbeiten nur auf den ersten vier OSI-Schichten (Schutzwert von Paketfiltern)
  - Um Applikationen kompatibel zu machen sind häufig Modifikationen an Applikationen oder Diensten nötig
  - niedrigerer Datendurchsatz im Vergleich zu Paketfiltern

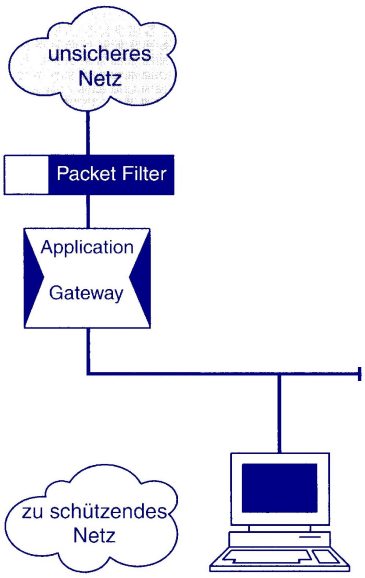
Architektur von Firewall-Systemen

– ausschließlicher Einsatz eines Firewall-Elementes nicht sinnvoll
– In der Praxis finden sich verschiedene Kombinationen von Paketfiltern (stateful) und Application Level Gateways bzw. Proxies
– Packet Filter + dual-homed Application Level Gateway
– „Screened Subnet“ (auch Demilitarisierte Zone, DMZ)
– „High-level-Security-Firewall-System“
– keine optimale Firewall-Architektur möglich
– Faktoren:
  - erreichbares Schutzniveau
  - Wartungsaufwand
  - Kosten
  - Komplexität der Regeln

Architektur von Firewall-Systemen

UNIVERSITÄT SIEGEN

– Packet Filter + dual-homed Application Gateway:
  - Application Level Gateway Teil des internen Netzes
  - Paketfilter Teil des unsicheren Netzes

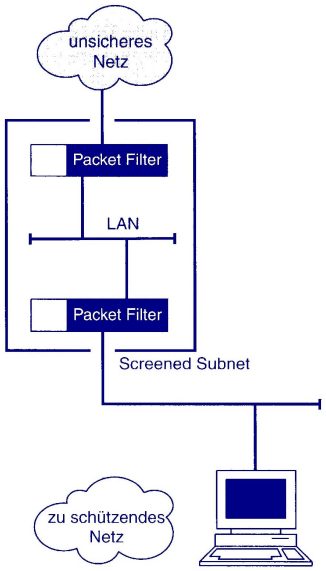


[2]

Architektur von Firewall-Systemen

UNIVERSITÄT SIEGEN

– Screened Subnet:
  - zwei Barrieren
  - beidseitiger Schutz von Rechnersystemen im Screened Subnet
  - einfache Aufstellung von Filterregeln, da zwei Sichten (zum unsicheren und zum zu schützenden Netz)

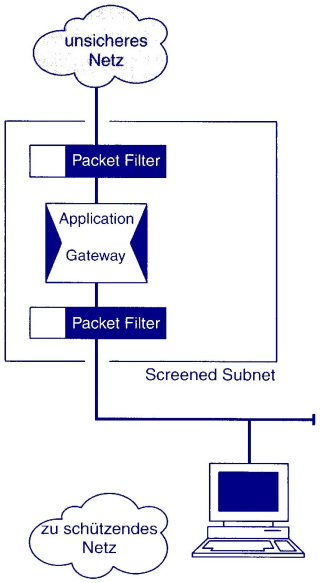


[2]

Architektur von Firewall-Systemen

UNIVERSITÄT SIEGEN

- High-level-Security-Firewall-System:
  - Application Gateway wird vor Angriffen von beiden Seiten geschützt
  - besonders hohe Gesamtsicherheit



[2]

Firewalls in E-Learning-Systemen

UNIVERSITÄT SIEGEN

- verschiedene Klassen von E-Learning-Systemen (z.B. virtuelle Klassenzimmer, Simulationssysteme etc.)
- Realisierung von E-Learning-Konzepten erfordert sowohl mehrere Rollen (z.B. Lehrende, interne/externe Tutoren, Lernende) als auch mehrere Netzwerksegmente
- mögliche Netzwerksegmente:
  - Fachdatenbank zur Informationsgewinnung Lernender / Mitarbeiter
  - Seminarraum für Präsenzveranstaltungen
  - Webserver mit Tutorials für Lernende
  - Interner Server mit vertraulichen Daten (Unternehmensdatenbank)
  - …
- Netzwerk muss gemäß möglicher Benutzerrollen strukturiert werden

Firewalls in E-Learning-Systemen

UNIVERSITÄT SIEGEN

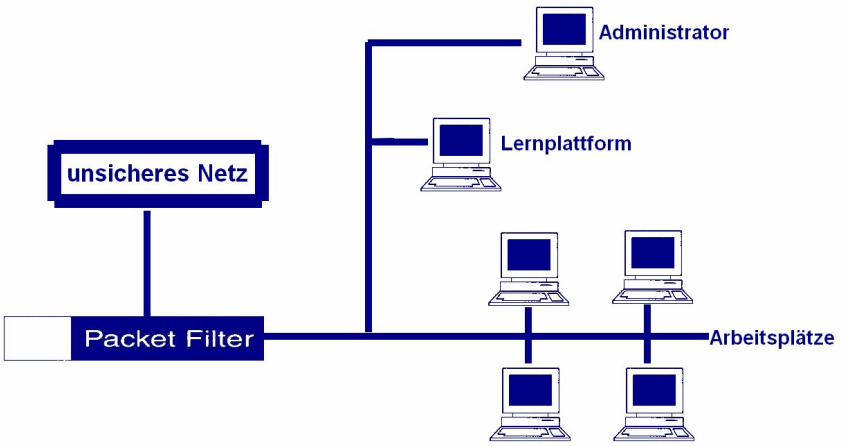
- Beispiel:
  - Seminarraum mit Präsenzveranstaltungen stellt zahlreiche Arbeitsplätze mit Zugriff auf eine Lernplattform (Kursunterlagen) zur Verfügung und ist gleichzeitig mit einem Arbeitsplatz des Lehrenden physikalisch gekoppelt.
- aktive Auseinandersetzung mit Lehrinhalten erwünscht: unbeschränkte HTTP-Nutzung
- gleichzeitig soll das interne Netzwerk kostengünstig vor Angriffen von außen geschützt werden
- es sollen Eckdaten der Internetnutzung wie Zeiten und Transfervolumina aufgezeichnet werden

Firewalls in E-Learning-Systemen

UNIVERSITÄT SIEGEN

Paketfilter zwischen internem und externem Netzwerk kann ausreichen:

⇨
- Inhalte der Kommunikation irrelevant
- vollständige Blockade einzelner Dienste bzw. Ports



[6]

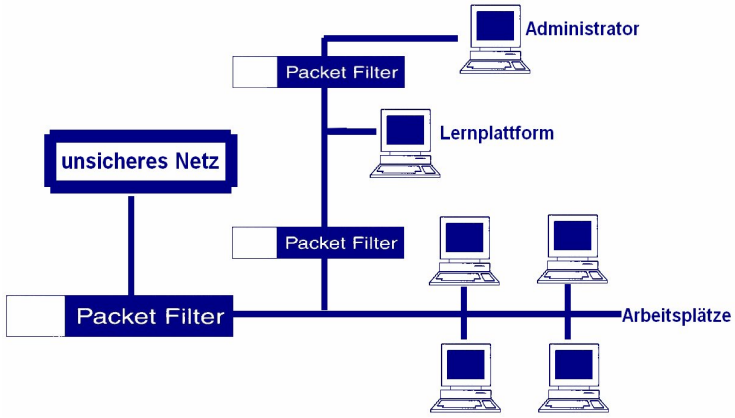
Firewalls in E-Learning-Systemen

UNIVERSITÄT SIEGEN

– ein Paketfilter zwischen internem Netz und dem Internet:
  - kein Schutz zwischen internen Netzwerksegmenten
  - Arbeitsplatz des Lehrenden + Webserver mit Lehrmaterialien gefährdet

⇒ Strukturierung des gesamten Netzwerks durch mehrere Paketfilter:

Zugriff der Lernenden auf vertrauliche Daten von internen Rechnern erschwert



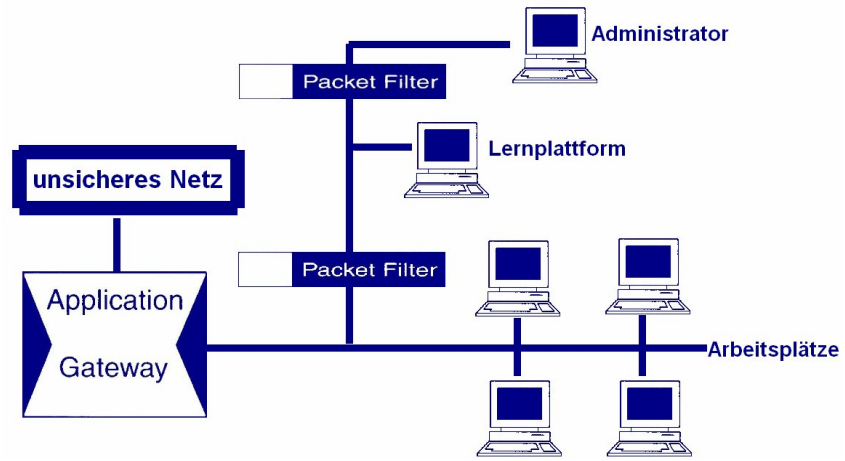
[6]

Firewalls in E-Learning-Systemen

UNIVERSITÄT SIEGEN

Sollen bestimmte Inhalte unterbunden werden und die Nutzer Sicherheitsverstößen zugeordnet werden können:

⇒ Einsatz von Application Level Gateways



[6]

Firewalls in E-Learning-Systemen

UNIVERSITÄT SIEGEN

- zwischen internem Netz und Internet: High-level-Security-Firewall
- verschiedene Benutzerrollen (mit unterschiedlichen Sicherheitsbedürfnissen) im internen Netz: Screened Subnets im internen Netz
- bei erforderlicher Protokollierung des Zugriffs von Außen (z.B. auf Datenbanken und Lernplattformen): Dual-homed Application Gateways
- Fazit:

  Zweiteilung des für ein E-Learning-System genutzten Netzes in sicheres und unsicheres Netz und Zwischenschaltung eines Firewall-Systems nicht ausreichend. Meist viele Subnetze nötig (Rollenvielfalt, örtliche Aufteilung), was den Einsatz mehrerer verschiedener Firewall-Lösungen erfordert.

  Nur dadurch kann unterschiedlicher Handlungsspielraum bei unterschiedlichem Schutzwert einzelner Systeme umgesetzt werden.

Quellenverzeichnis

UNIVERSITÄT SIEGEN

[1] http://www.selflinux.org/selflinux/bilder/osi_osi.png (22.01.2007)

[2] Pohlmann, Norbert, Firewall-Systeme. 5.Auflage, Bonn 2003

[3] http://www.lebensland.de/tech_net.html (09.02.2007)

[4] http://www.auto.tuwien.ac.at/%7Erlieger/Firewalls/Firewall.Fig3.gif (22.01.2007)

[5] http://www.computerworld.com/computerworld/records/images/story/08_Router.gif (22.01.2007)

[6] Teile der Grafik aus: Pohlmann, Norbert, Firewall-Systeme. 5.Auflage, Bonn 2003