Firewall

TBZ Technikerschule Zürich

IT-Services Technologien,
Vorträge zu Entwicklungstrends

1. Juli 2002

Kuno Pfund, Gregor Battilana

Mein Heim-PC ist meine Burg

Bekannte Firewalls für Windows und Mac-OS

Produkt	Kosten	Stärke	Info
Zone Alarm	kostenlos	Bewährtes Produkt	www.zonealarm.com
Tiny Personal Firewall	kostenlos	Einfache Bedienung	www.fwnetwork.com
Web Washer	kostenlos	Entfernt Werbung	www.webwasher.de
Norton Internet Security Suite 2001	Fr. 120.-	Zusatzfunktionen (Kinderschutz, Antivirus), automatische Aktualisierung	www.symantec.ch
Sphinx Firewall 2.0	79 Mark	Integrierte Kindersicherung mit Bildanalyse	www.pcfirewall.de
BlackIce Defender	40 US-$	Erkennt Hackerangriffe und versucht diese zurückzuverfolgen	www.networkice.com
Norton Internet Security für Macintosh	Fr. 179.-	Für Apple Macintosh	www.symantec.ch

NZZ Online

Frontseite

AKTUELL
Kommentar
International
Wirtschaft
Börsen · Märkte
Schweiz
Zürich · Region
Sport
Feuilleton
Vermischtes
Wetter

HINTERGRUND
Dossiers
Netzstoff
Forschung · Technik
Tourismus
Medien · Informatik
Literatur · Kunst
Zeitfragen
Buchrezensionen
English Window

NZZ · FINFOX
Ihr Finanzplaner

MEDIEN · INFORMATIK

Tabelle: Bekannte Firewalls für Windows und Mac-OS

Mein Heim-PC ist meine Burg

Firewall-Software für Privatanwender

Der Internetanschluss liefert nicht nur vielfältige Informationen, sondern auch Gefahren und Risiken. Gegen neugierige Marketingmanager oder gar böswillige Hacker schützt eine PC-Firewall, die sich als Wächter zwischen Internet und PC stellt.

Das Internet bietet jedermann die Freiheit, Musik zu hören, Nachrichten abzurufen, elektronische Briefe

Such

Weit

Kamp

Wohr

1000

Alle w
sein

Fürs

Im Br
Wettb

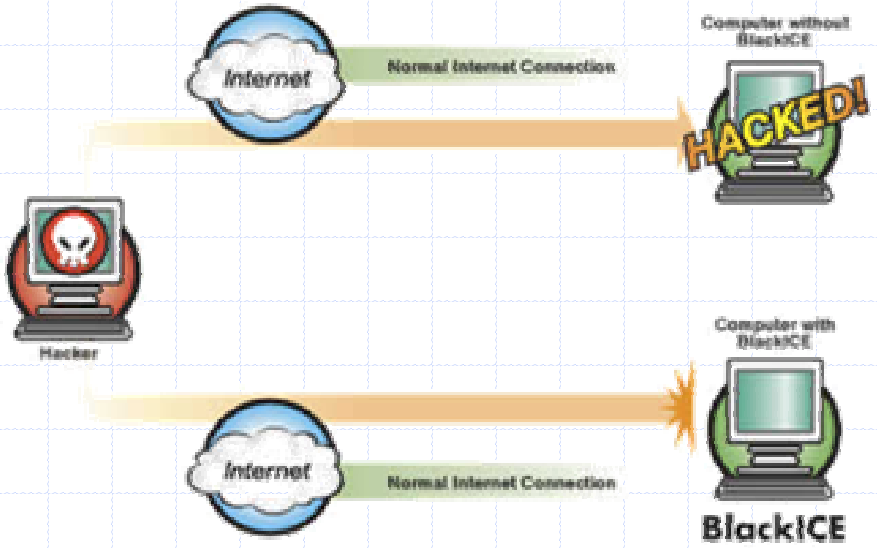
Schel

Mehr

Link: http://www.nzz.ch/2001/10/26/em/page-article7QOHQ.html

BlackICE™ PC Protection

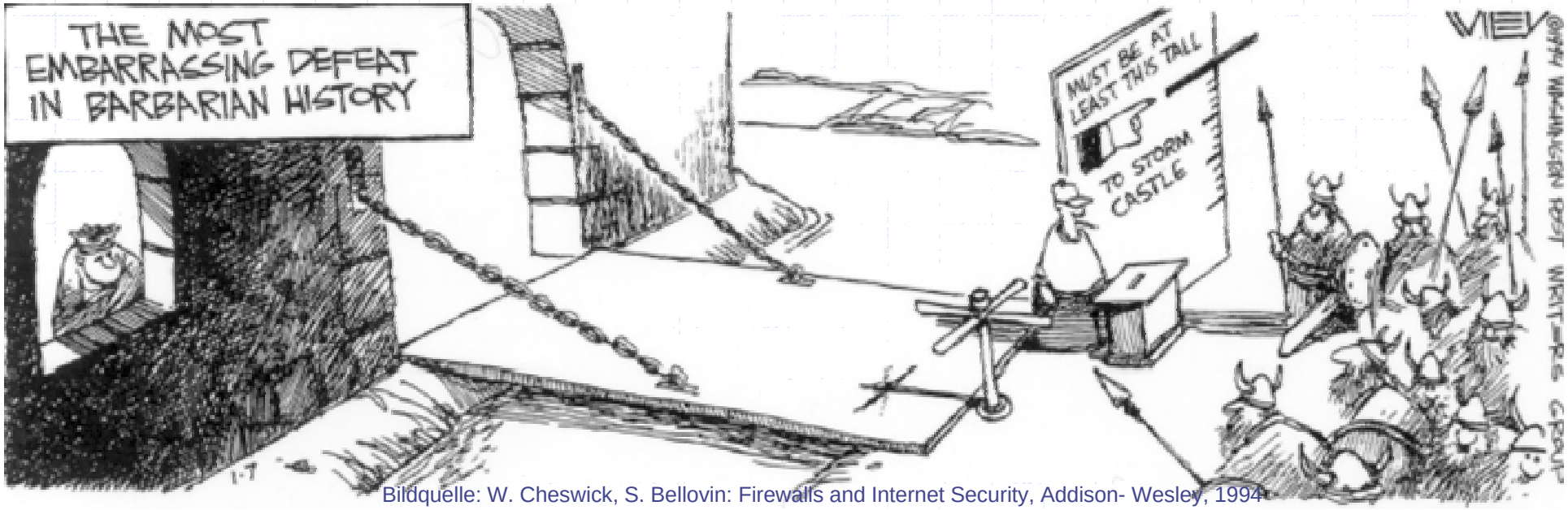
- The product contains two independent modules:
  - Firewall
  - Intrusion detection system (IDS).
- The software's technology is based upon basic packet filtering and packet analysis technology.
- The product does not contain proxy features.
- The software does not replace an anti-virus program.



Link: http://www.iss.net/products_services/hsoffice_protection/blkice_protect_pc.php

Firewall – Worum geht es?

- Netzwerkkomponente, bestehend aus einem oder mehreren Elementen
- Bildet einziger Übergang zwischen einem zu schützenden und einem unsicheren Netzbereich
- Kontrolle von Zugang und Diensten an einem Punkt nach definierten Regeln durchsetzen



Bildquelle: W. Cheswick, S. Bellovin: Firewalls and Internet Security, Addison- Wesley, 1994

Ziele

- Sich der Schwächen von IT-Infrastrukturen (insb. Netzwerken) und sich daraus ergebenen Gefahren bewusst werden.
- Grob den Aufbau und Funktionen einer Firewall kennen.
- Die Bedeutung und Elemente einer Sicherheitspolitik kennen.
- Die wichtigsten Technologien und Architekturen kennen und deren Einsatz in einem konkreten Kontext beurteilen können.
- Eine Firewall als ein Element von Sicherheitsmassnahmen verstehen und die konzeptionellen Grenzen kennen.

Ablauf der Doppellektion

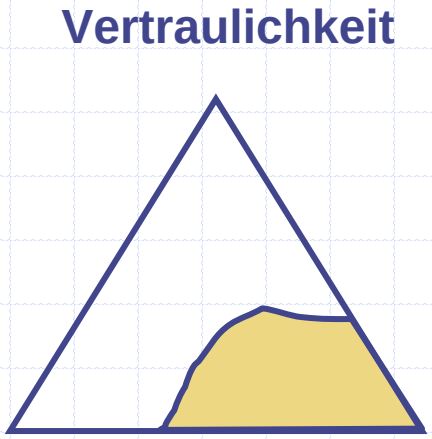
Inhalt	**Lehrform**	**Dauer**
Konzept der Firewall: Ziele, Prinzip und Funktionen, Aufbau und funktionale Komponenten, Sicherheitspolitik	Lehrervortrag	25‘
Fallstudie Spital KliniX, 1. Teil	Partnerübung Besprechung	20‘
Pause		
Technologien und Architekturen: Paketfilter, Application Gateway, Anwendung, Typische Topologien, Arten der Implementierung	Lehrervortrag	15‘
Fallstudie Spital KliniX, 2. Teil:	Gruppenübung Besprechung	30‘

Sicherheitsanforderungen

- Vertraulichkeit
- Integrität
- Authentizität
- Verfügbarkeit
- Zugriffskontrolle
- Verbindlichkeit
- Anonymität

Internet – TCP/IP

Designziele



Potentielle Schwachstellen

Anwendung
Transport
Netzwerk
Netzzugang

- **Anwendungs-protokolle**
- **Netzverwaltung / Bootstrap**
- **Transport-protokolle**
- **Routing-System**
- **Internetprotokoll**

Quelle: Plattner et. al., ETH Zürich, Vorlesung „IT-Security“, 2001

Sicherheitsmechanismen und Systeme

- Verschlüsselungssysteme (DES, RSA, etc.)
- Message Authentication und Digitale Signatur
- Key Management, Authentication: PKI, Kerberos, etc.
- IP-Security: IPSec, VPN
- Web Security: SSL / TLS
- Email: PGP, S/MIME
- Payment: SET
- Intrusion Detection
- Schutz vor Malware (Viren, Würmer, etc.)
- Firewalls
- etc.

Definition

Eine Firewall besteht aus einer Gruppe von Netzwerkkomponenten (Hard- und Software) an der Schnittstelle zweier Netze.

Sie gewährleistet die Einhaltung von Sicherheits-richtlinien zwischen einem zu schützenden und einem unsicheren Netz (z.B. dem Internet).

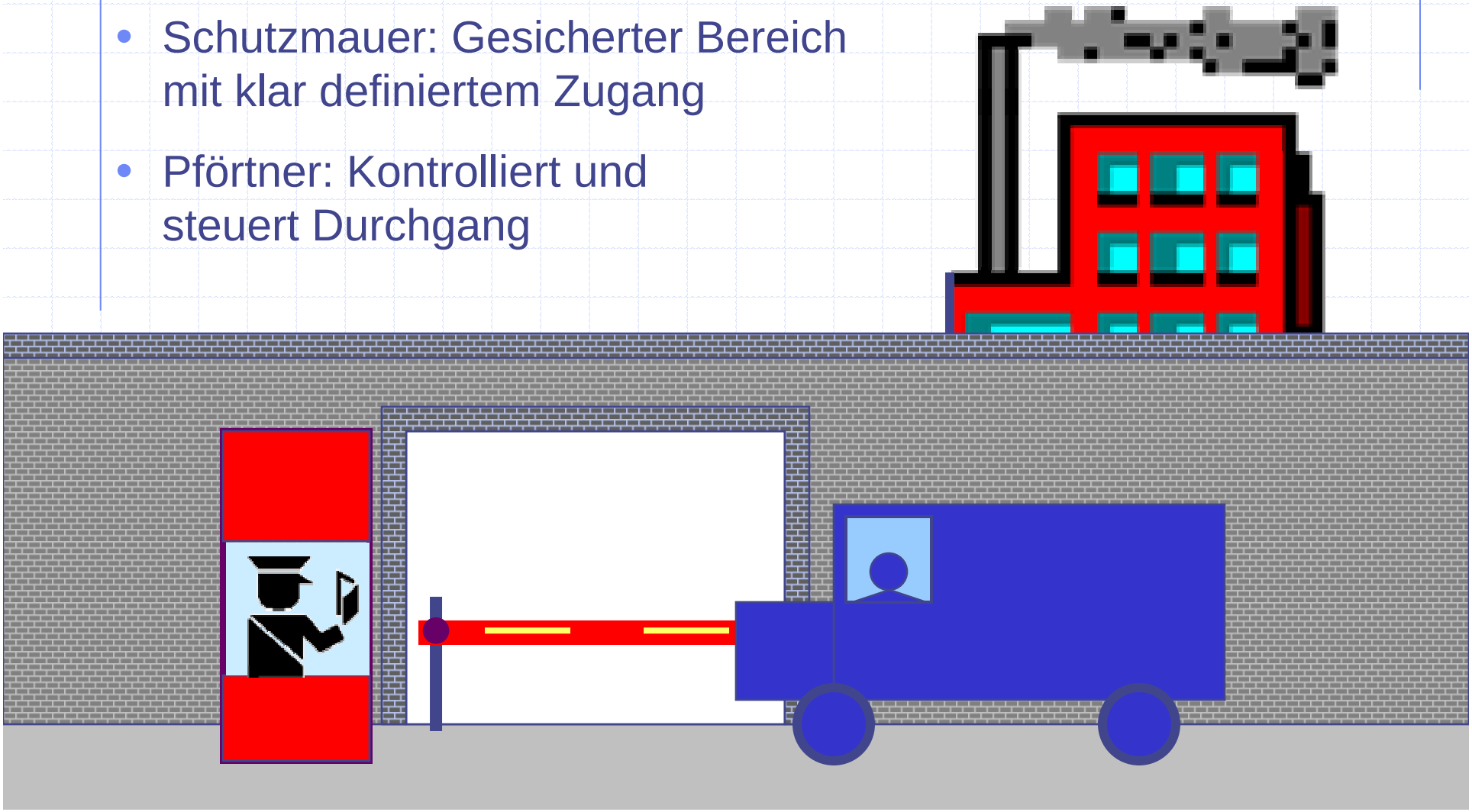
An dieser "Brandschutzmauer" entscheidet sich, auf welche Dienste innerhalb des privaten Netzes zugegriffen werden kann und welche Dienste des nicht sicheren Netzes aus dem privaten Netz heraus nutzbar sind.

Funktion von Firewall-Systemen

- Servicekontrolle
  - Netzwerkebene
  - Anwedungsebene
- Benutzerkontrolle
- Entkopplung von Diensten
- Verbergen des internen Netzes
- Protokollierung
- Alarmierung
- Zusatzfunktionen:
  - NAT
  - IPSec / VPN
  - Schutz vor Malware, etc.

Analogie zur Firewall

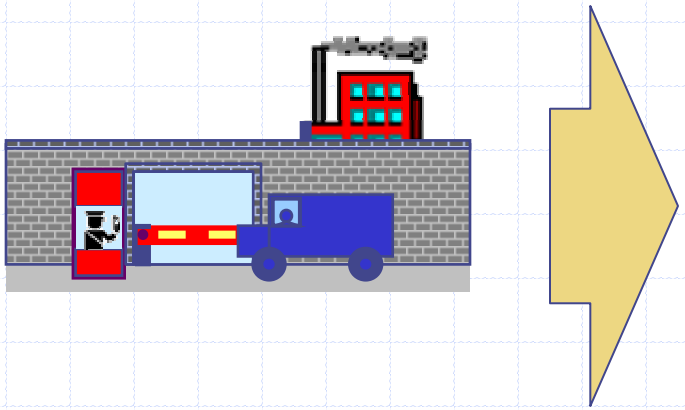
- Schutzmauer: Gesicherter Bereich mit klar definiertem Zugang
- Pförtner: Kontrolliert und steuert Durchgang



Analogie zur Firewall

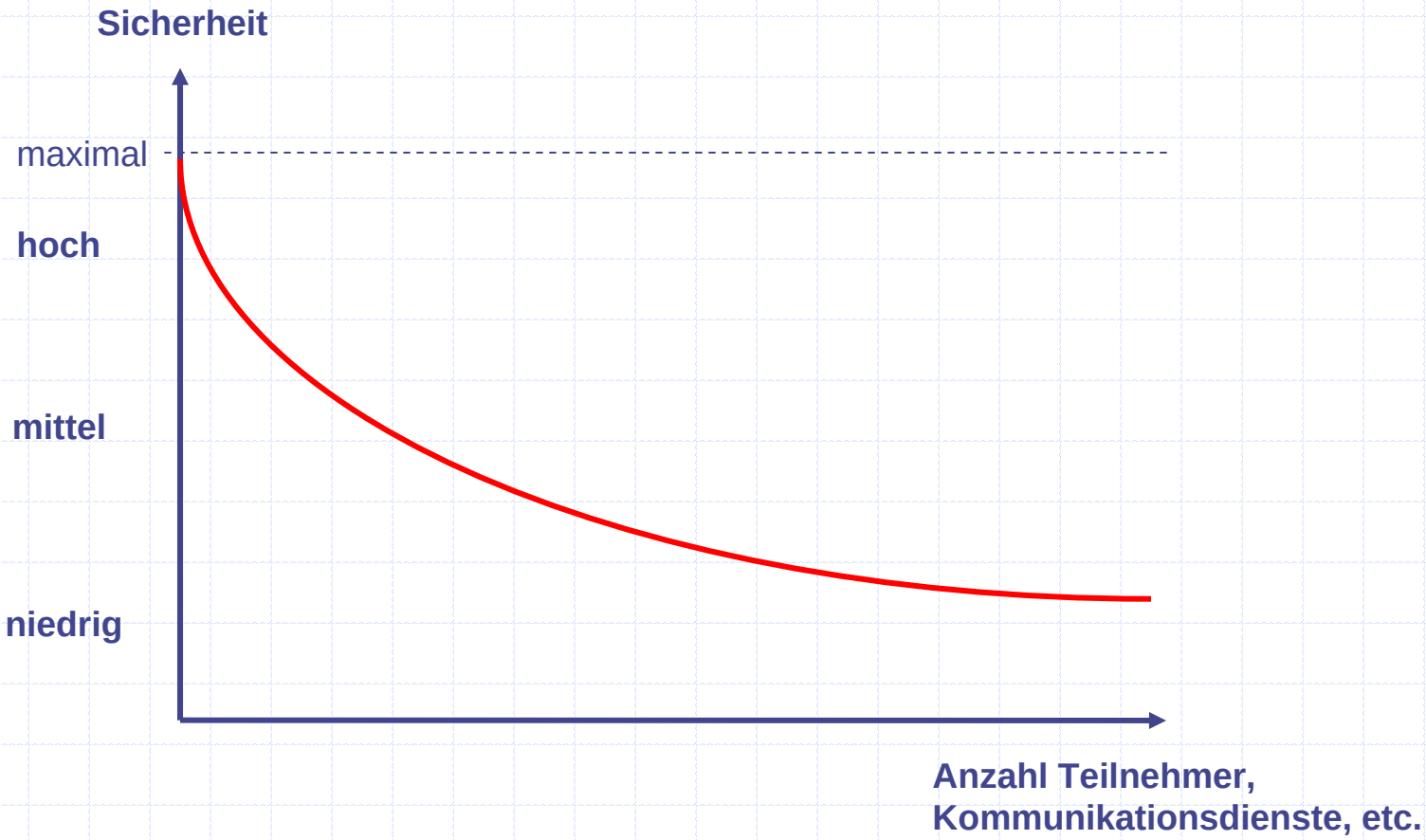
	Gebäude	Firewall
Schutzmauer	• Gebäudeteile trennen, Übergang zu definiertem Bereich abschotten	• Netzabschnitte bilden, zu schützendes Netz abschotten • Einziger, sicherer Übergang
Pförtner	• Zugang prüfen und Personen prüfen (identifizieren und authentifizieren) • Besucher registrieren, Verbindung herstellen • Transportmittel und Gegenstände prüfen • Ereignisse protokollieren	• Wer hat Zugriff • Über welche Protokolle und welche Dienste • Mit welchen Rechner-systemen darf kommuniziert werden • Sicherheitsrelevante Vorfälle in das Logfile schreiben

Analogie zur Firewall



- Sicherheitspolitik notwendig
- Je weniger Besucher / Zugänge desto sicherer
- Effizient dank Zentralisierung
- Interne Angreifer! Kein Bewegungsmelder, keine Überwachungskamera (IDS)
- Der gesamte Datenverkehr muss über diese Station laufen
- Die Firewall selber muss resistent gegen Eindringlinge sein

Security vs. Connectivity

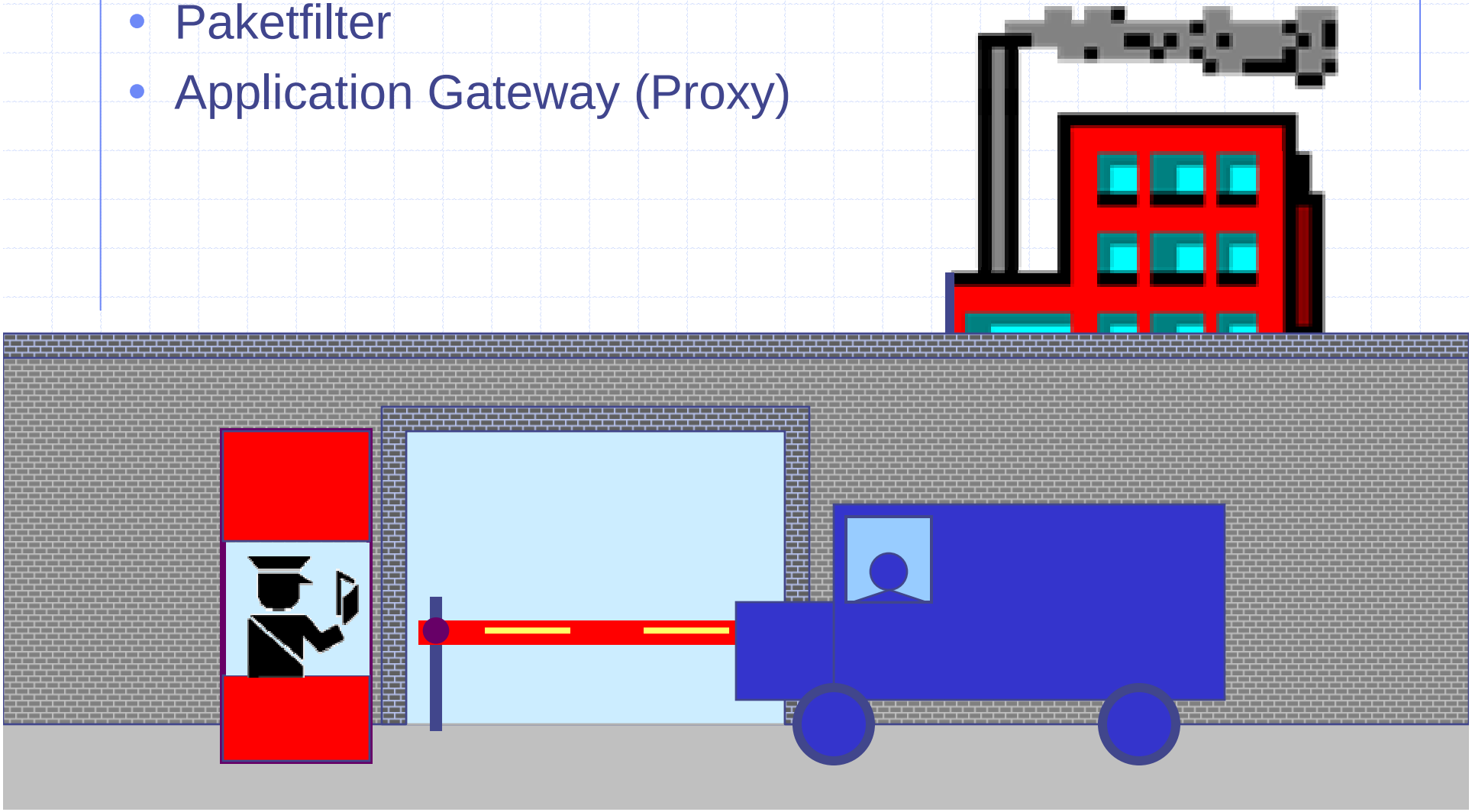


Typen von Firewalls

- In der Praxis habe sich folgende Firewall-Typen herauskristalisiert:
  - Paket Filter
  - Application Gateway (Proxy)
- Unterschiede:
  - Art der Einbindung
  - Funktion

Analogien zu Firewall-Typen

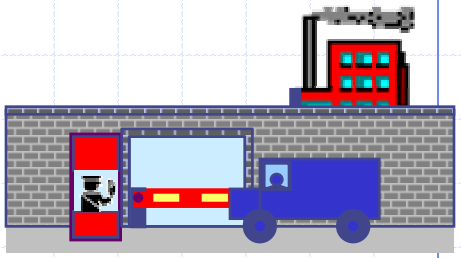
- Paketfilter
- Application Gateway (Proxy)



Analogien zu Firewall-Typen

	Paketfilter	Application Gateway (Proxy)
Firewall	• Analyse und Kontrolle bis auf Transportebene: • Netzzugang: Header, z.B. Quelle, Ziel, Protokol-Typ • Netzwerk: IP- / ICMP-Header • Transport: TCP/UDP-Header • Zeit	• Analyse und Kontrolle bis auf Applikationsebene • Stellvertreter (Proxy) entkoppelt Netz logisch und physikalisch: Es erfolgt keine direkte Verbindung zum Zielsystem. • Proxy Software notwendig
Gebäude	• Der Pförtner prüft, ob das Logo auf dem LKW bekannt ist und lässt den Lastwagen passieren.	• Der Pförtner prüft Papiere und Inhalt. Er nimmt die Pakete entgegen und bestellt einen Fahrer der eigenen Firma, der die Pakete zum eigentlichen Empfänger bringt.

Analogie zur Firewall-Typen



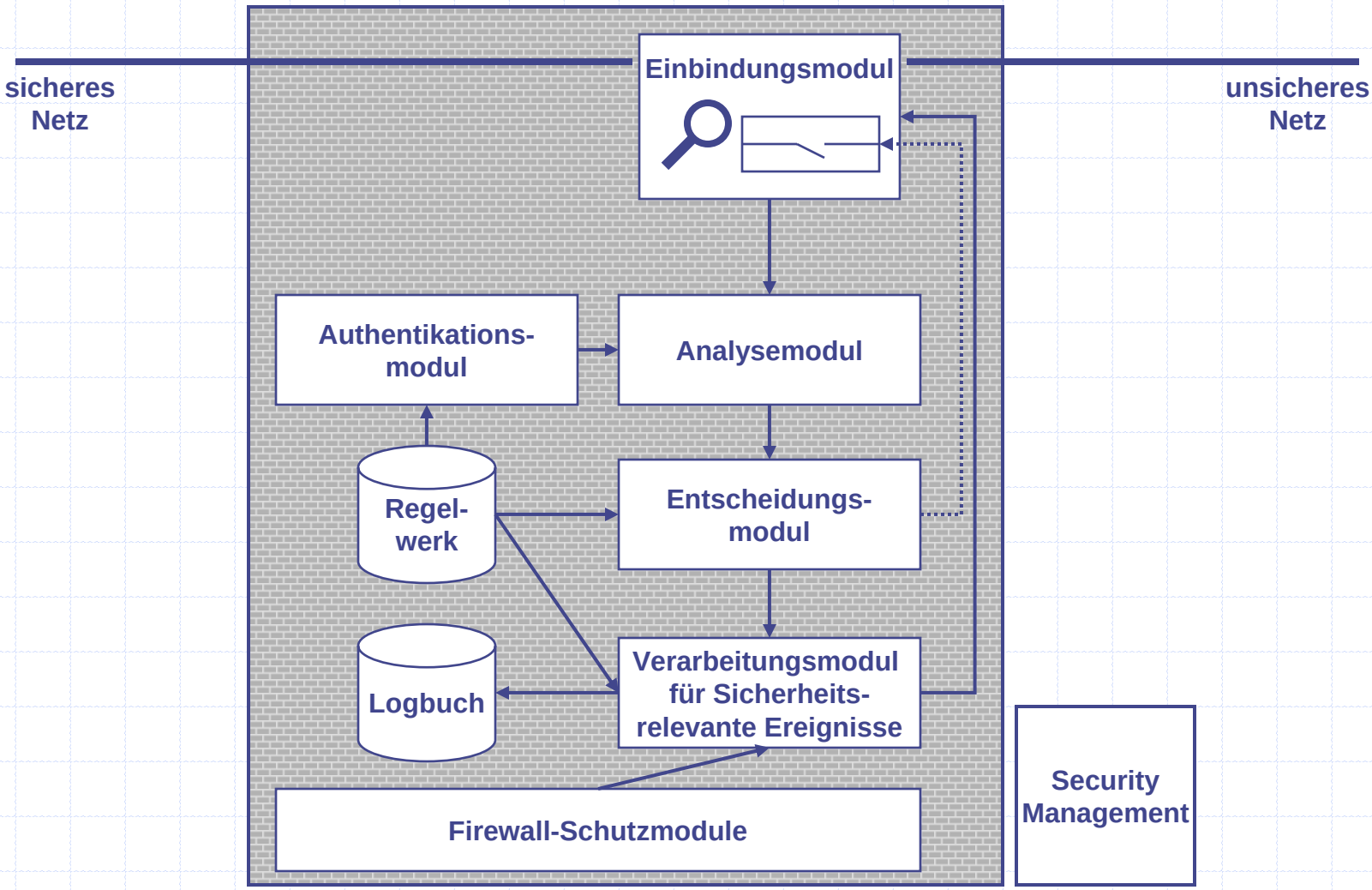
Paketfilter

- Gute Performance
- Einfach erweiterungsfähig
- Transparent
- Verbergen i.A. zu schützendes Netz nicht
- Daten oberhalb der Transportebene werden i.d.R. nicht analysiert

Application Gateway (Proxy)

- Sicherheitsfunktionen auf Anwendungsebene
- Stellvertreter (Proxy) benötigt
- Entkopplung der Dienste
- Verbergen internes Netz
- Bessere Protokollierungs-möglichkeiten
- Geringe Flexibilität
- Kosten i.d.R. höher

Komponenten einer Firewall (1)



Quelle: N. Pohlmann, Firewallsysteme, 3. Aufl., Bonn, MITP-Verlag, 2000

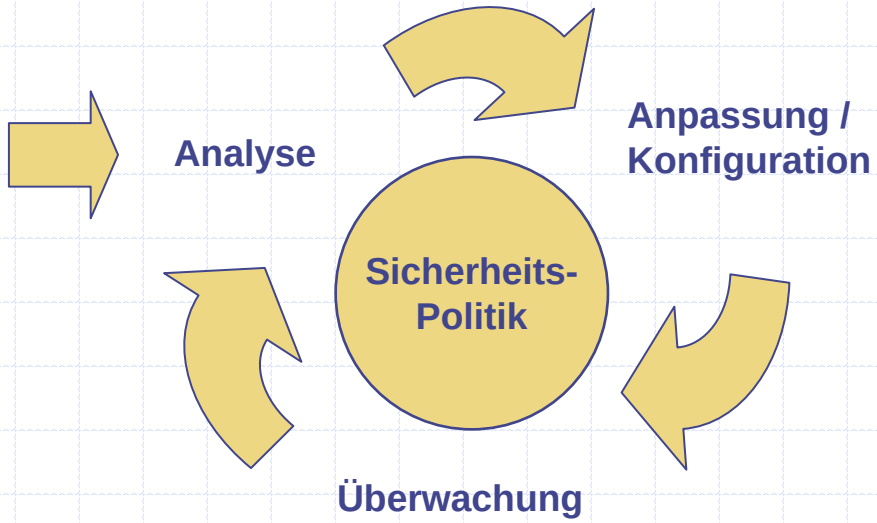
Komponenten einer Firewall (2)

- **Einbindungsmodul**: Realisiert Verbindung der Netze.
- **Analysemodul**: Analyse der Kommunikationsdaten. Paket Filter und Application Gateway analysieren auf unterschiedlichen Ebenen.
- **Entscheidungsmodul**: Auswertung der Analyseergebnisse. Vergleich mit den im Regelwerk festgelegten Definitionen der Sicherheitspolitik. Steuerung des Einbindungsmoduls.
- **Verarbeitungsmodul für sicherheitsrelevante Ereignisse**: Eintrag in das Logbuch und/oder Alarm, in Abhängig des Regelwerks.
- **Authentikationsmodul**: Identifikation und Authentisierung der Instanzen (Prozesse, Benutzer, etc.). Verschiedene Verfahren möglich.
- **Regelwerk**: Technische Umsetzung der Sicherheitspolitik und wird mit Hilfe eines Security Management erstellt.
- **Logbuch**: Enthält alle Protokolleinträge der sicherheitsrelevanten Ereignisse, die gemäss Regelwerk im Betrieb aufgezeichnet werden sollen.
- **Security Management**: Benötigt, um die Regeln für die Firewall festzulegen und die Protokolldaten aus den Logbuch zu analysieren.
- **Firewallschutzmodul**: Firewall-Element muss neben den Sicherheitsdiensten selber gegen Angriffe resistent sein.

Firewall: Mehr als ein Produkt ...

Damit effektiv Schutz geboten wird, muss eine Firewall:

- Auf einer Sicherheitspolitik aufsetzen,
- korrekt installiert und konfiguriert,
- korrekt administriert werden.



Quelle, mit umfassender Information: Bundesamt für Sicherheit in der Informationstechnik (BS): www.bsi.de

- Netzwerkzugriff auf Server mit internen Datenbeständen.
- Portscan möglich, ohne Alarm: Port 1433 verriet den Hackern, dass das WEF einen Microsoft-Server mit dem Betriebssystem Windows 2000 betrieb.
- Passwort: Die Administratoren hatten das Standard-Passwort des MS SQL-Server (Benutzernamen "sa" mit leeren Passwort) nicht geändert.

Erstellung der Sicherheitspolitik

- (Risiken und Schutzbedarf klären, Vorgaben beachten)
- Anforderungen festlegen:
  - Sicherheitsanforderungen
  - Kommunikationsanforderungen
- Massnahmen festlegen:
  - Organisation
  - Personal
  - Infrastruktur

Sicherheitsanforderungen

Möglich Punkte:

- Zu schützende Ressourcen: Daten, Rechnersysteme, Kommunikationseinrichtungen, etc.
- Zugangskontrolle auf der Benutzerebene (Authentisierung), Anwendungsebene, Netzwerkebene
- Verbergen der internen Netzstruktur
- Vertraulichkeit von Nachrichten
- Schutz gegen Angriffe auf Verfügbarkeit, z.B. für Informationsserver
- Schutz vor Angriffen durch das Bekanntwerden von neuen sicherheitsrelevanten Softwareschwachstellen
- Anforderungen an das Firewall-System selber
- Behandlung von sicherheitsrelevanten Ereignissen

Kommunikationsanforderungen

Möglich Punkte:

- Diensten und Anwendungen
  - Unterscheidung von internen und externen Benutzer, ev. unterteilt nach Kommunikationsprofilen
  - Richtung der Dienste und Anwendungen
  - ggf. Anforderungen wie Authentisierungsverfahren, Verschlüsselung, Protokollierung, Zeitfenster
- Information, welche (nicht) nach aussen gelangen darf
- Filterregeln für die unteren Schichten (IP, ICMP, ARP, TCP und UDP) und für die Anwendungsschicht (SMTP, DNS, HTTP, etc.)
- Default Policy
- Verfügbarkeit
- Datendurchsatz

Massnahmen: Organisation

Möglich Punkte:

- Festlegung der Verantwortlichkeiten für Firewall-System (Sicherheitspolitik, Koordination, Umsetzung, Testen, Administration, etc.)
- Zugriffsrechte zum Security Management
- Kontrolle der Protokolldaten (wer, welche, wie oft, etc.)
- Reaktion auf Verletzungen der Sicherheitspolitik definieren
- Informationsbeschaffung zu Sicherheitslücken (u.a. des Firewall-Systems), Installation der Updates
- Betreuung der Benutzer
- Regelung für Wartungs- und Reparaturarbeiten

Massnahmen: Personal

Möglich Punkte:

- Security Management
  - Profil des Security Administrators
  - Auswahl des Security Administrators und Externer
  - Vertreterregelung
  - Verfahren beim Ausscheiden eines Security Administrators
- Benutzer
  - Regelungen und Anweisungen
  - Schulung der Benutzer
  - Verfahren beim Ausscheiden eines Benutzers

Massnahmen: Infrastruktur

Möglich Punkte:

- Sicherheitskritischen Zonen
- Sicherheitsmassnahmen und ihren Orte
- Firewall-Architektur
- Anforderung an von aussen erreichbare Systeme
- Netzzugänge (ISP, Modempool, etc.)
- Leitungsführung und physische Zugangssicherung

Fallbeispiel „SpitiX“ - Teil 1

- Ausgabe Aufgabenblätter zu Teil 1
- Bearbeitung in Zweiergruppen
- Gemeinsame Diskussion der Ergebnisse 5 Minuten vor der Pause

Firewall-Sicherheitspolitik

- Voraussetzung für den sicheren Betrieb eines Firewall-Systems.
- Definiert Sicherheitsziele, die durch den Einsatz eines Firewall-Systems erfüllt werden sollen.
- Orientiert sich am Schutzbedarf des zu schützenden Systems.
- Muss bestehende allgemeine oder übergeordnete Sicherheitspolitik berücksichtigen.
- Verantwortlich: Leiter IT, IT-Sicherheitsmangement