Firewall-Systeme

Konzepte - Möglichkeiten und Grenzen - Realisierung

Prof. Dr. Norbert Pohlmann

Fachbereich Informatik

Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

- Firewall-Konzepte
- Das richtige Firewall-Konzept für jeden Einsatzfall
- Möglichkeiten und Grenzen
- Realisierungskonzepte
- Zusammenfassung

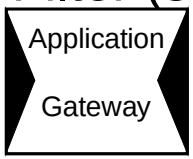
Inhalt

- **Firewall-Konzepte**
  - Das richtige Firewall-Konzept für jeden Einsatzfall
  - Möglichkeiten und Grenzen
  - Realisierungskonzepte
  - Zusammenfassung

Firewall-Elemente und -Konzepte

- **Firewall-Elemente**
  - Packet Filter

  - Zustandsorientierter Packet Filter (stateful inspection)
  - Application Gateway

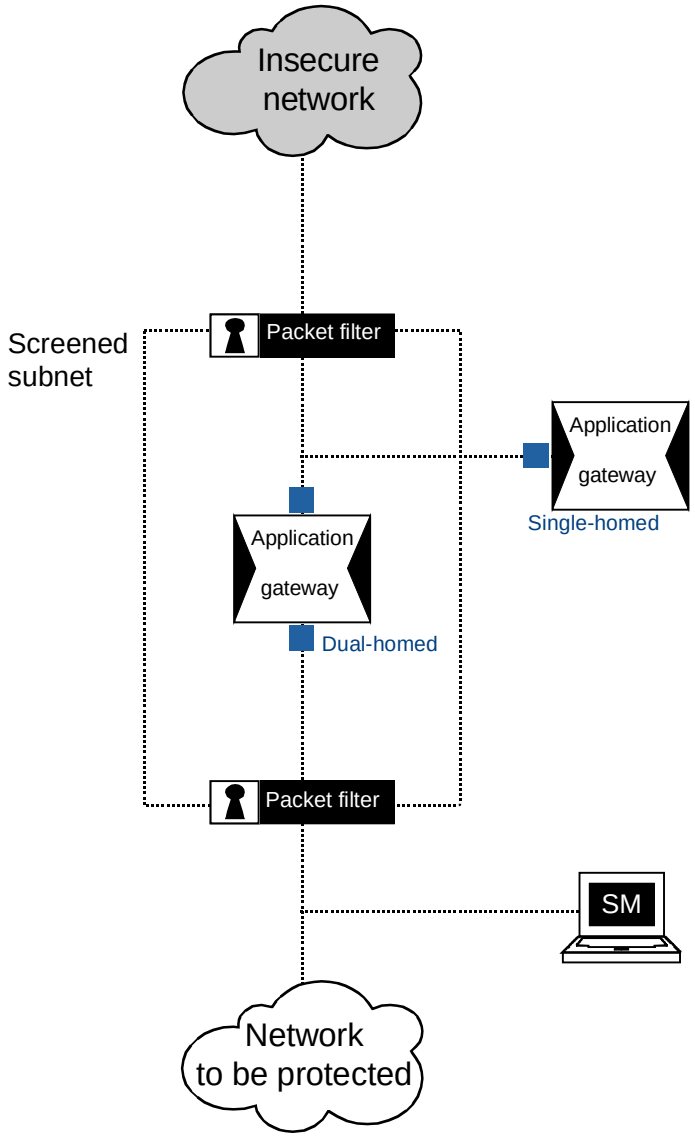


  - Adaptive Proxy

- **Firewall-Konzepte**
  - ausschließlicher Einsatz von Firewall-Elementen
  - Kombination von Firewall-Elementen
    - **z.B. High-level Security Firewall-System**

Firewall Konzepte

- Packet Filter
- Single-homed Application Gateway
- Dual-homed Application Gateway
- Packet Filter und single-homed Application Gateway
- Stateful Inspection
- Adaptive Proxy
- Packet Filter und dual-homed Application Gateway
- Screend Subnet mit Packet Filter und single-homed Application Gateway
- Screend Subnet mit Packet Filter und dual-homed Application Gateway



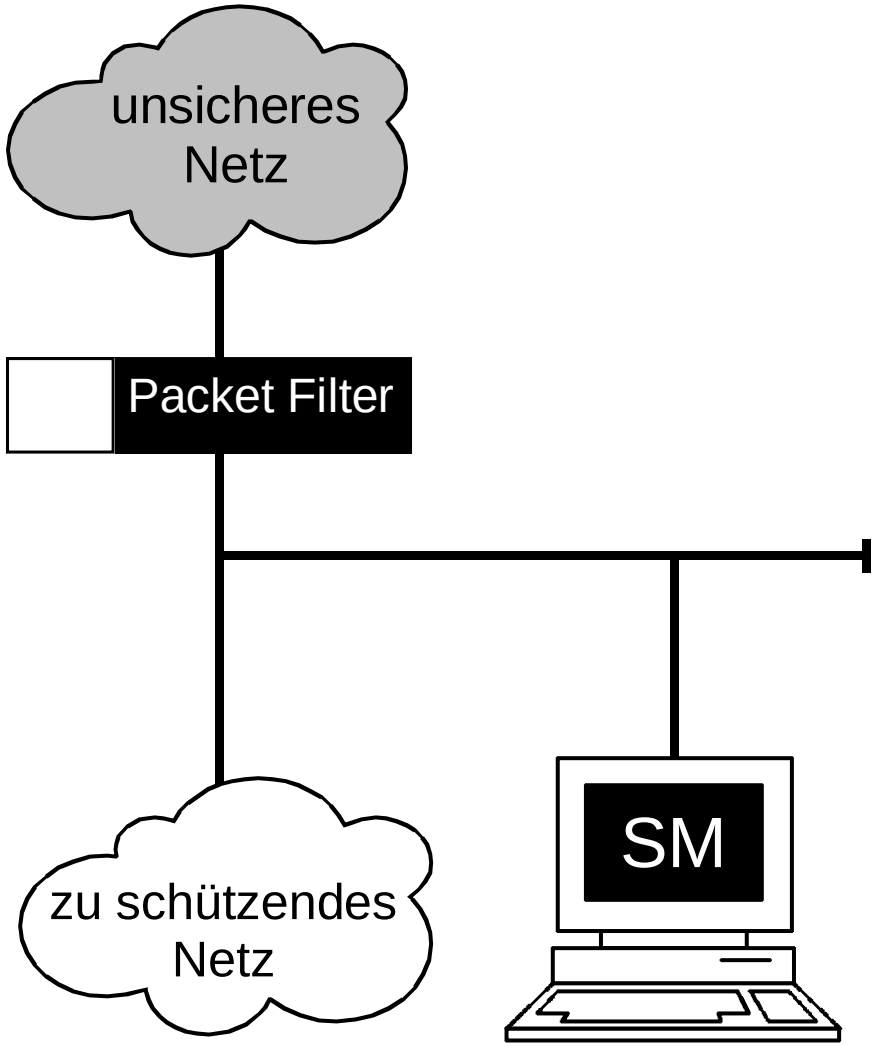
Ausschließlicher Einsatz eines Packet Filters

Bewertung

- Sicherheitsdienste nicht für hohe Anforderungen geeignet
- Kann auch andere Protokollfamilien unterstützen (IPX, OSI, SNA, ...)

Einsatzgebiet

- Intranet



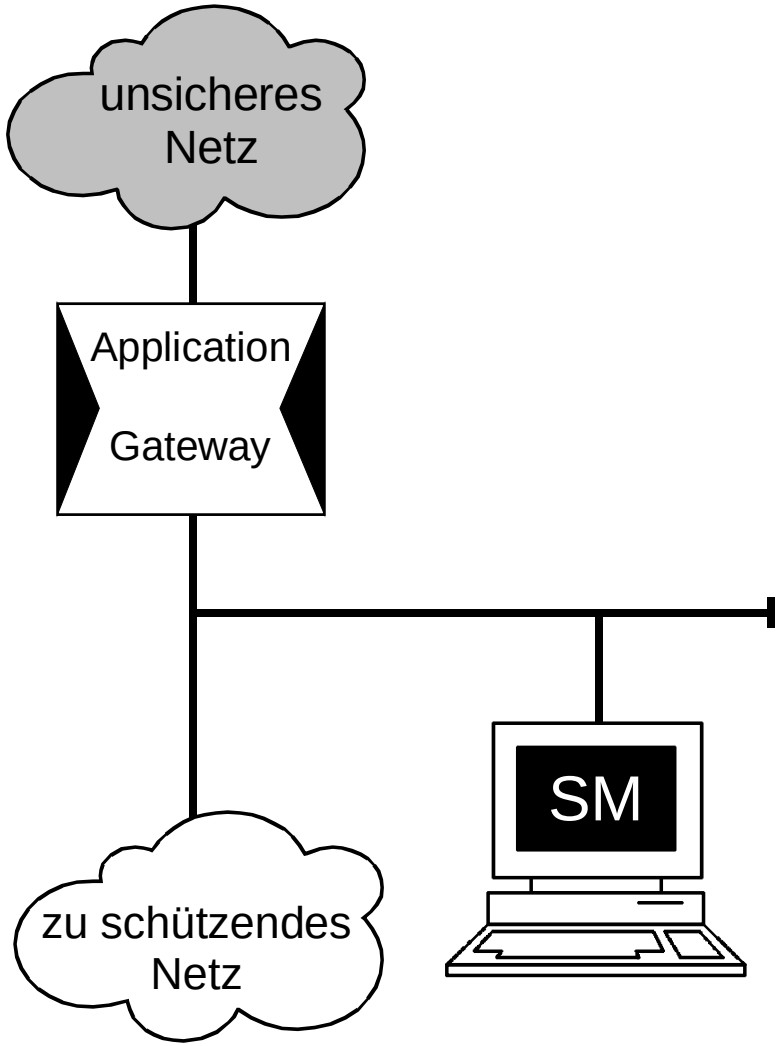
Ausschließlicher Einsatz eines Application Gateway

Bewertung

- Hochwertige Sicherheitsdienste
- Verbindungsdaten können ausführlich protokolliert werden

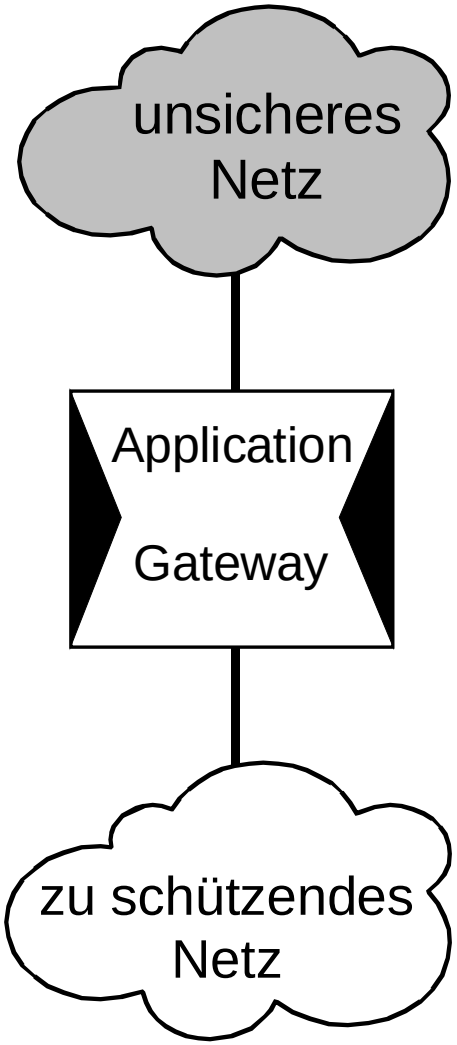
Einsatzgebiet

- Gleichwertige Organisationen mit hohem Schutzbedarf



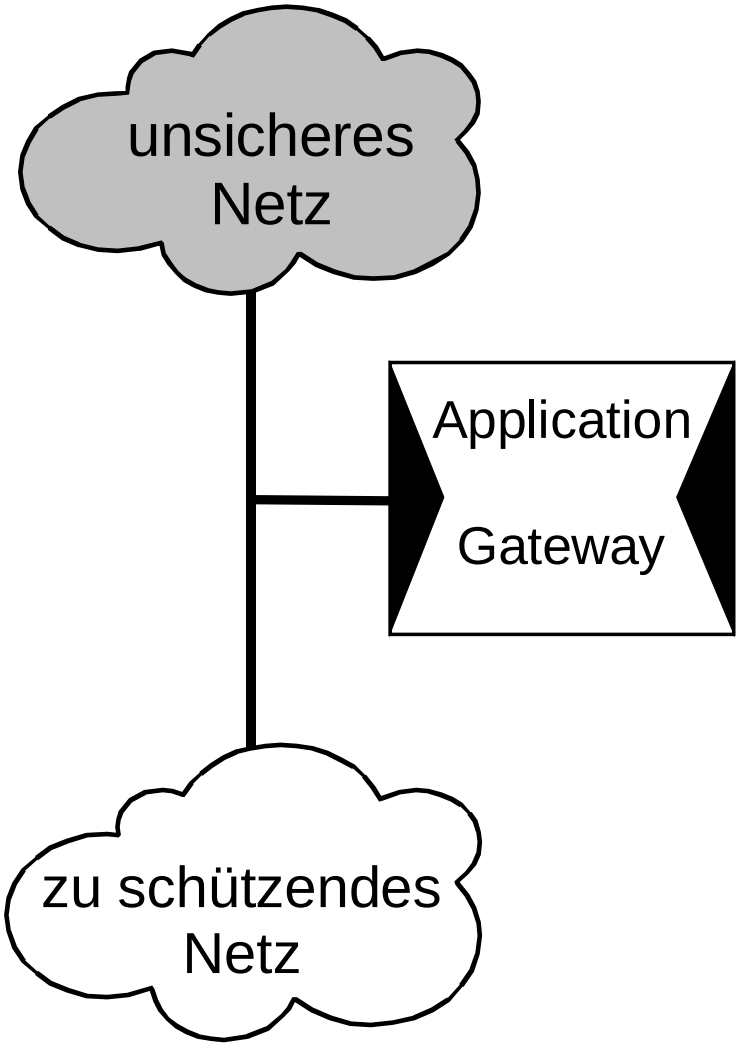
Dual-homed Application Gateway

- Arbeitet mit zwei Netzschnittstellen
- **Volle Kontrolle** über die Pakete
- es gibt „keinen“ Weg vorbei



Single-homed Application Gateway

- Arbeitet mit einer Netzschnittstelle
- Die selbe Schnittstelle für eingehende und ausgehende Pakete
- Es wird **nicht garantiert**, dass alle Pakete analysiert und kontrolliert werden



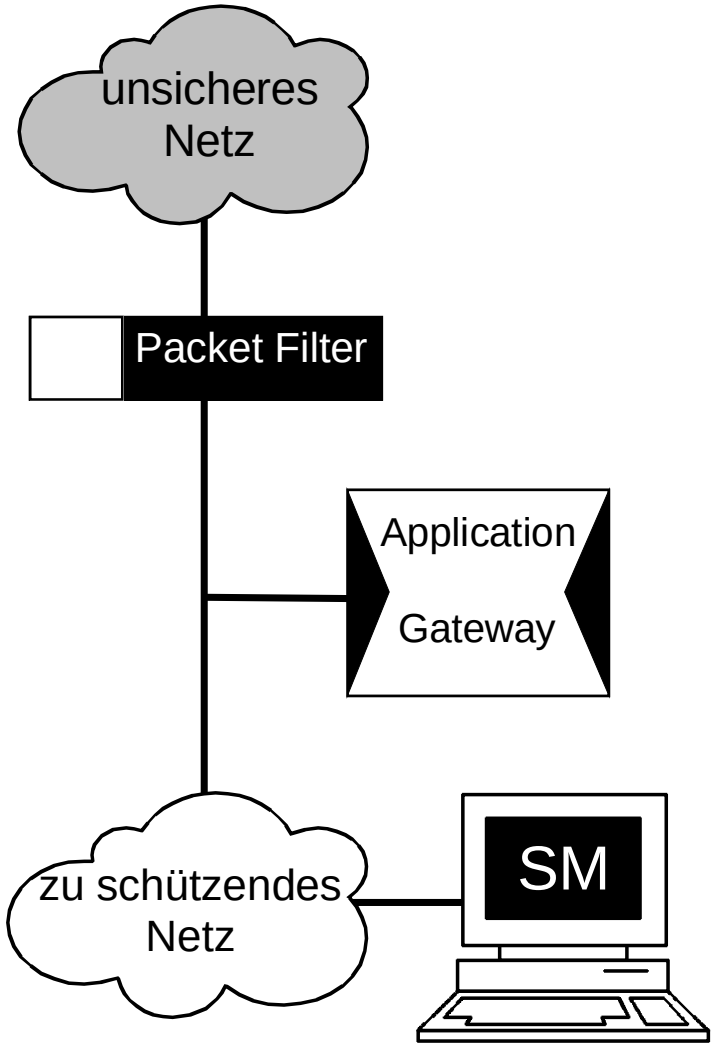
Packet Filter und single-homed Application Gateway (1/2)

Bewertung

- Flexibel für Dienste, für die es keinen Proxy gibt
- Die Sicherheit hängt in erster Linie vom Packet Filter ab
- **Application Gateway befindet sich im zu schützenden Netz (+++)**

Einsatzgebiet

- Besonders schutzwürdige Organisationen im Intranet



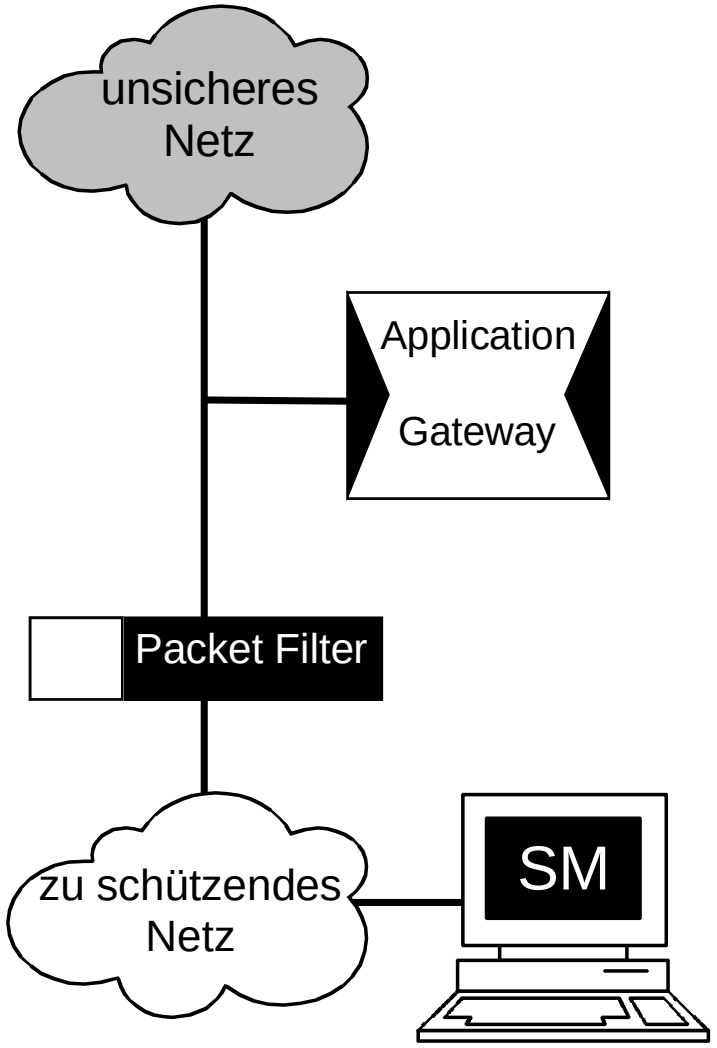
Packet Filter und single-homed Application Gateway (2/2)

Bewertung

- Flexibel für Dienste, für die es keinen Proxy gibt
- Die Sicherheit hängt in erster Linie vom Packet Filter ab
- **Application Gateway befindet sich im unsicheren Netz (---)**

Einsatzgebiet

- Besonders schutzwürdige Organisationen im Intranet



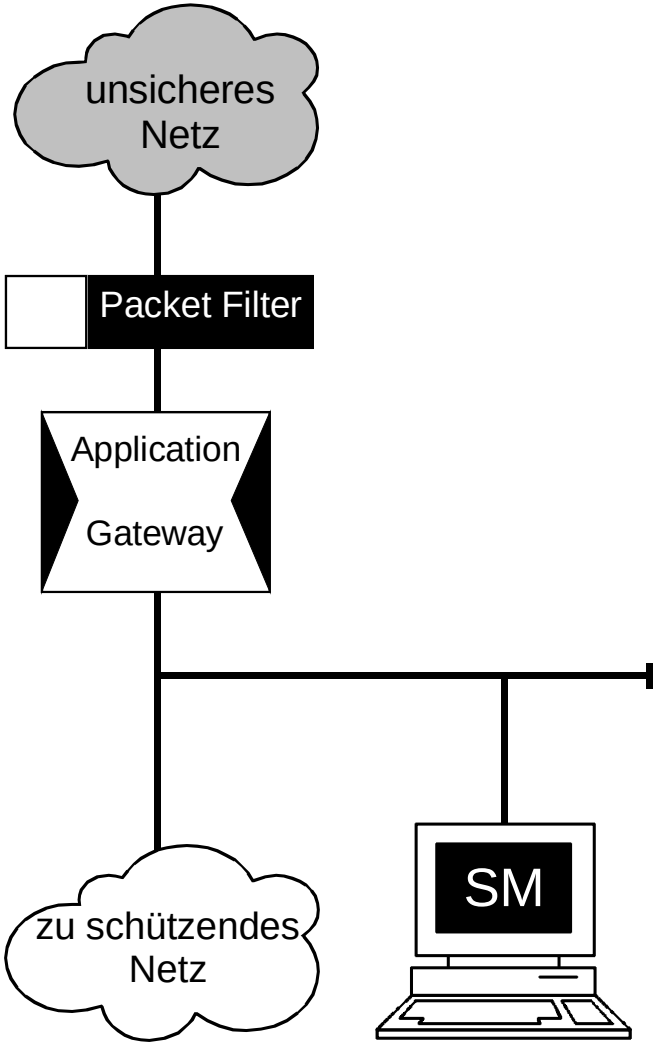
Packet Filter und dual-homed Application Gateway (1/2)

Bewertung

- Packet Filter und dual-homed Application Gateway kontrollieren die Kommunikation
- Unterschiedliche Einbindungskonzepte (+++)
- Packet Filter schützt Application Gateway
- **Application Gateway befindet sich im zu schützenden Netz (+++)**

Einsatzgebiet

- Internet-Ankopplung mit einem hohen Schutzbedarf



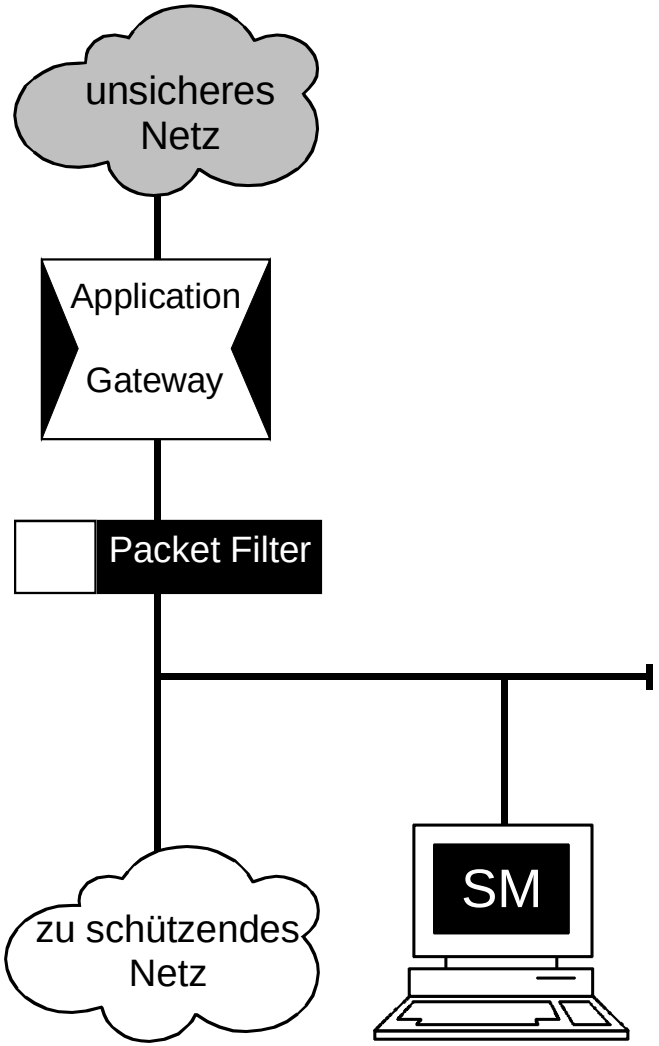
Packet Filter und dual-homed Application Gateway (2/2)

Bewertung

- Packet Filter und dual-homed Application Gateway kontrollieren die Kommunikation
- Unterschiedliche Einbindungskonzepte (+++)
- Packet Filter schützt Application Gateway
- **Application Gateway befindet sich im unsicheren Netz (---)**

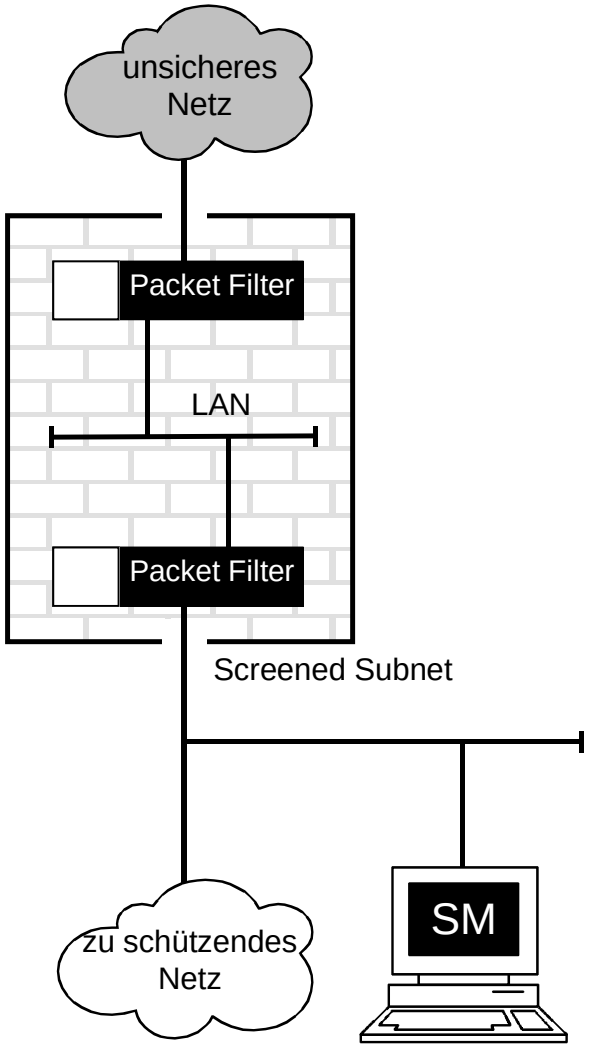
Einsatzgebiet

- Ganz besonders schutzwürdige Organisationen im Intranet



Screened Subnet

- Grenznetz oder auch DMZ (De-Militarised Zone)
- Rechnersysteme werden im Screened Subnet positioniert
- Werden von beiden Seiten geschützt
- Filterregeln können einfacher definiert werden



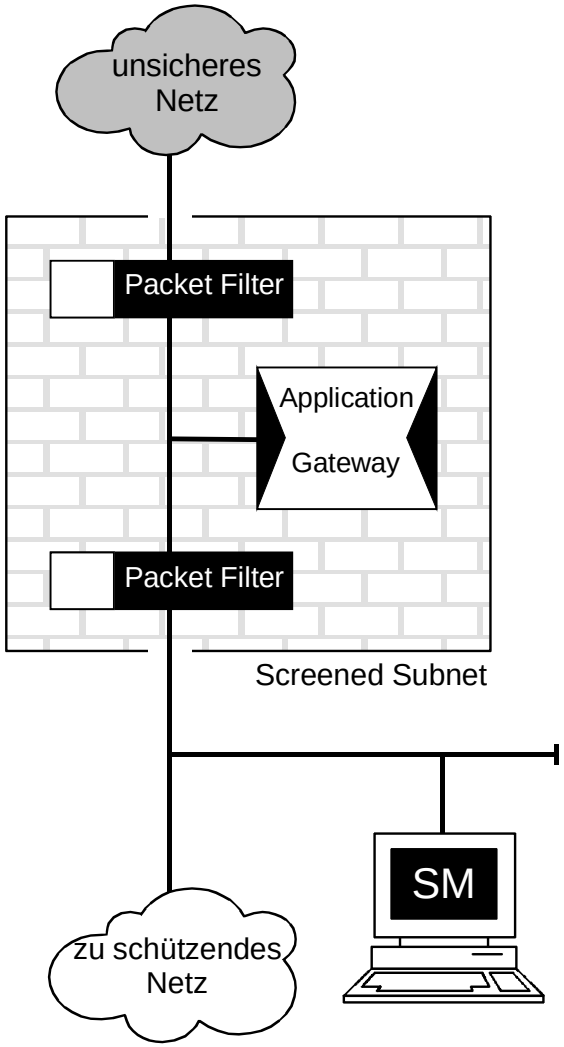
Zwei Packet Filter als Screened Subnet und ein single-homed Application Gateway

Bewertung

- Flexibel für Dienste, für die es keinen Proxy gibt
- Die Sicherheit hängt in erster Linie vom Packet Filter ab
- Application Gateway wird von beiden Seiten geschützt

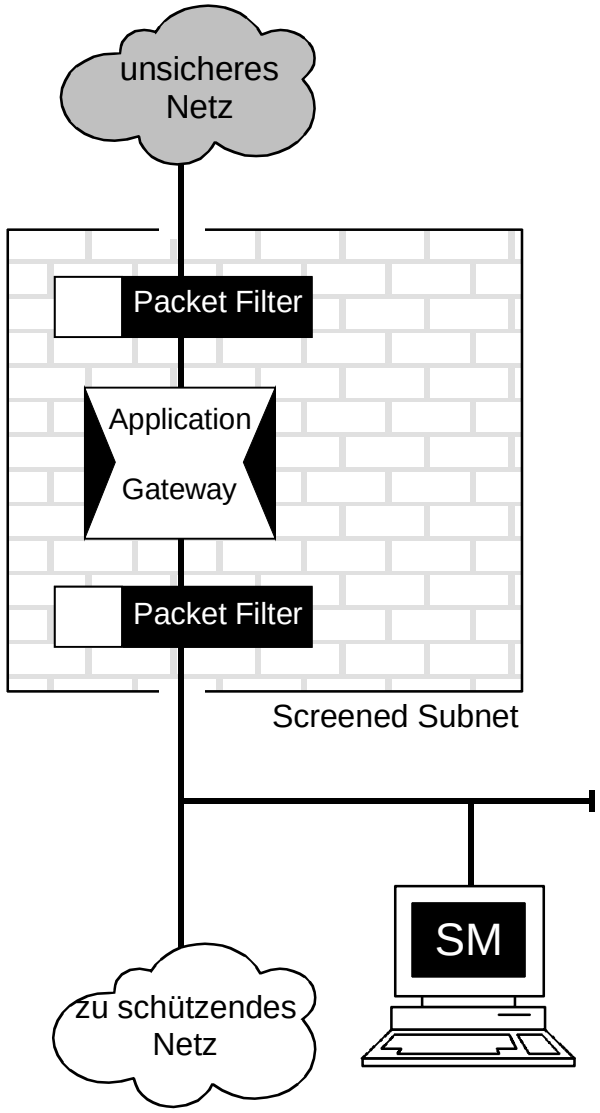
Einsatzgebiet

- Besonders schutzwürdige Organisationen im Intranet



High-level Security Firewall-System

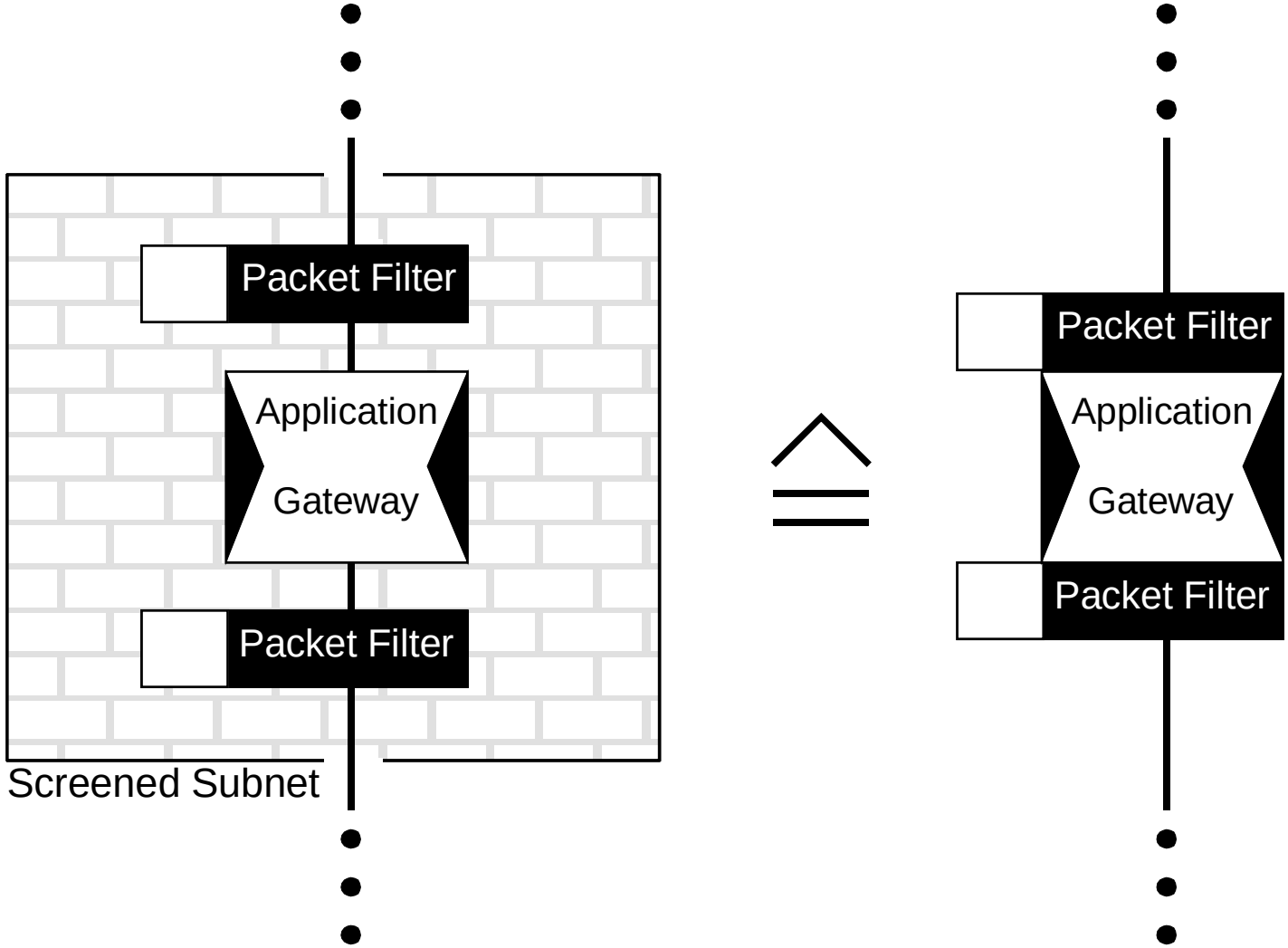
- Einfache Regeln
- Gegenseitiger Schutz
- Geschachtelte Sicherheit
- Verschiedene Betriebssysteme
- Unterschiedliche Einbindungs- und Analysemöglichkeiten
- Separates Security Management



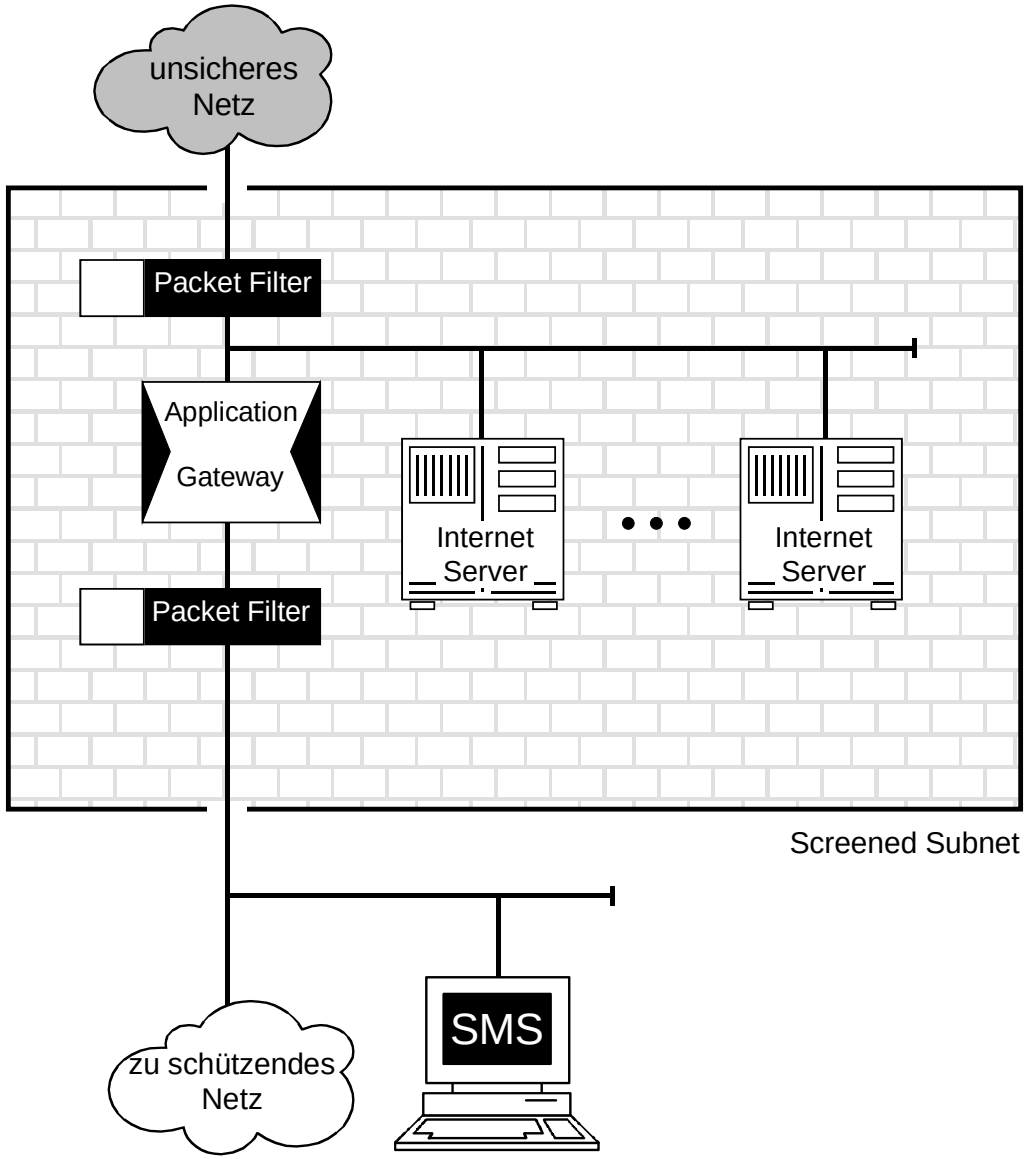
Einsatzgebiet

- Das Internet Firewall-System

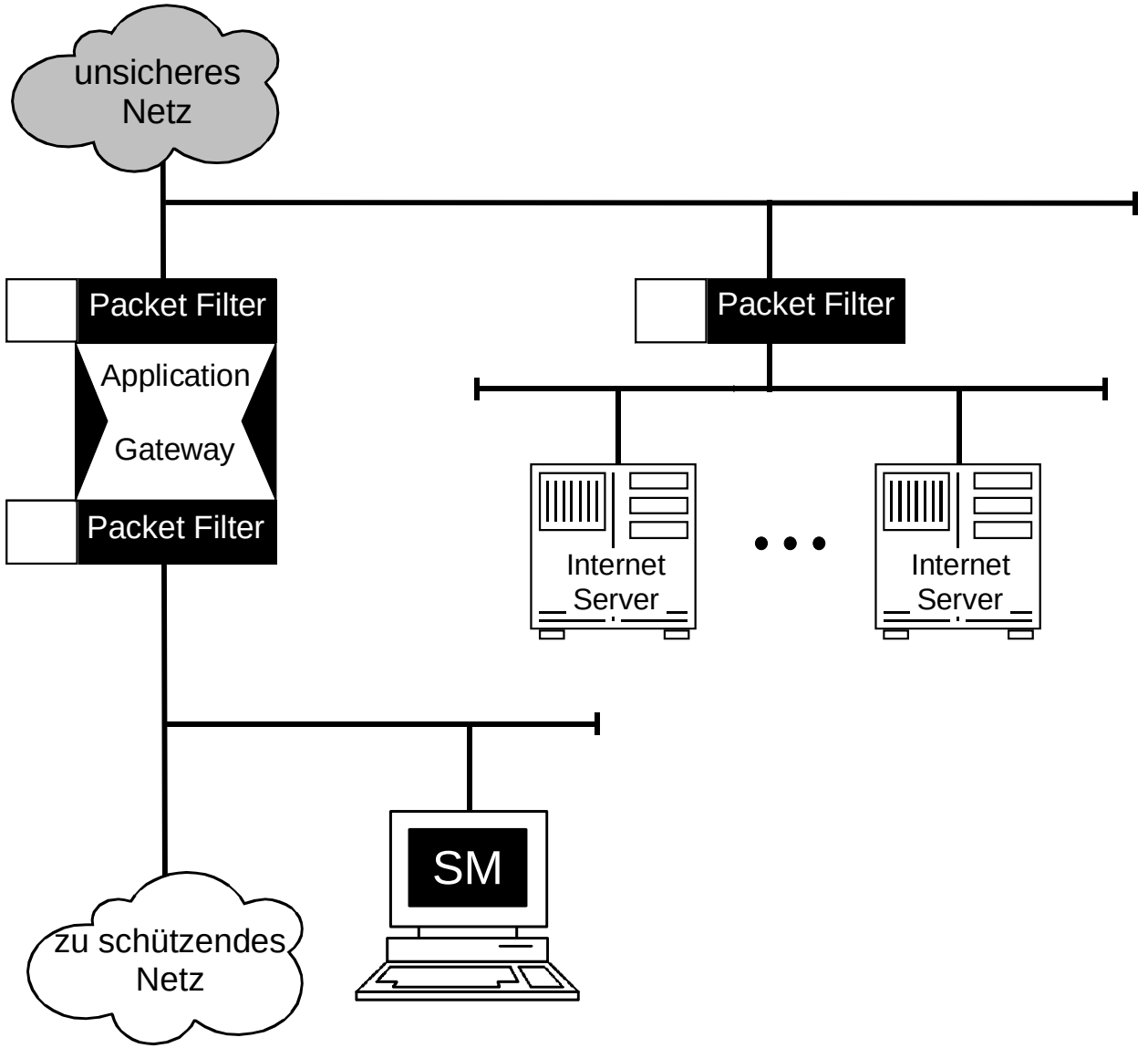
Symbol eines High-level Security Firewall-Systems



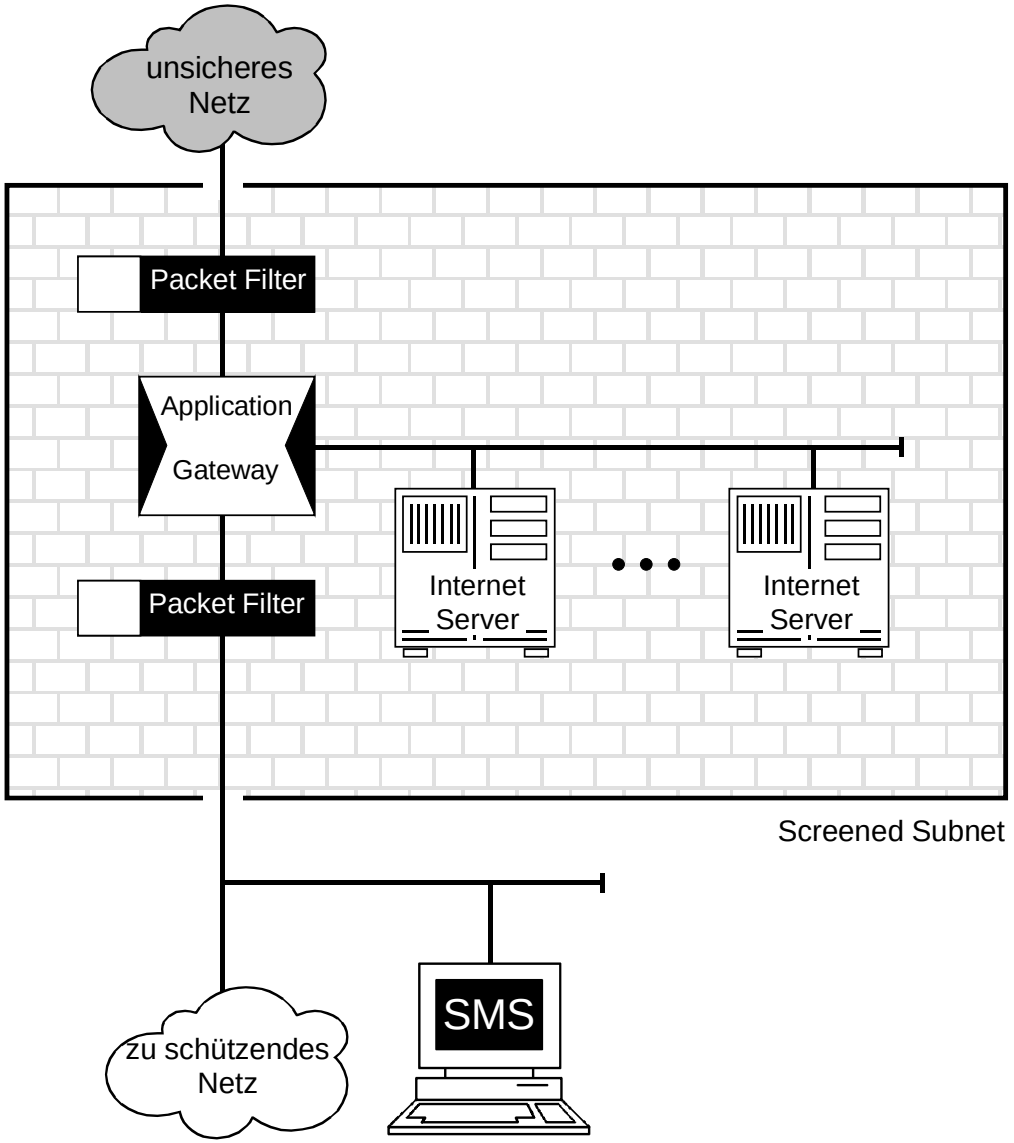
Internet Server



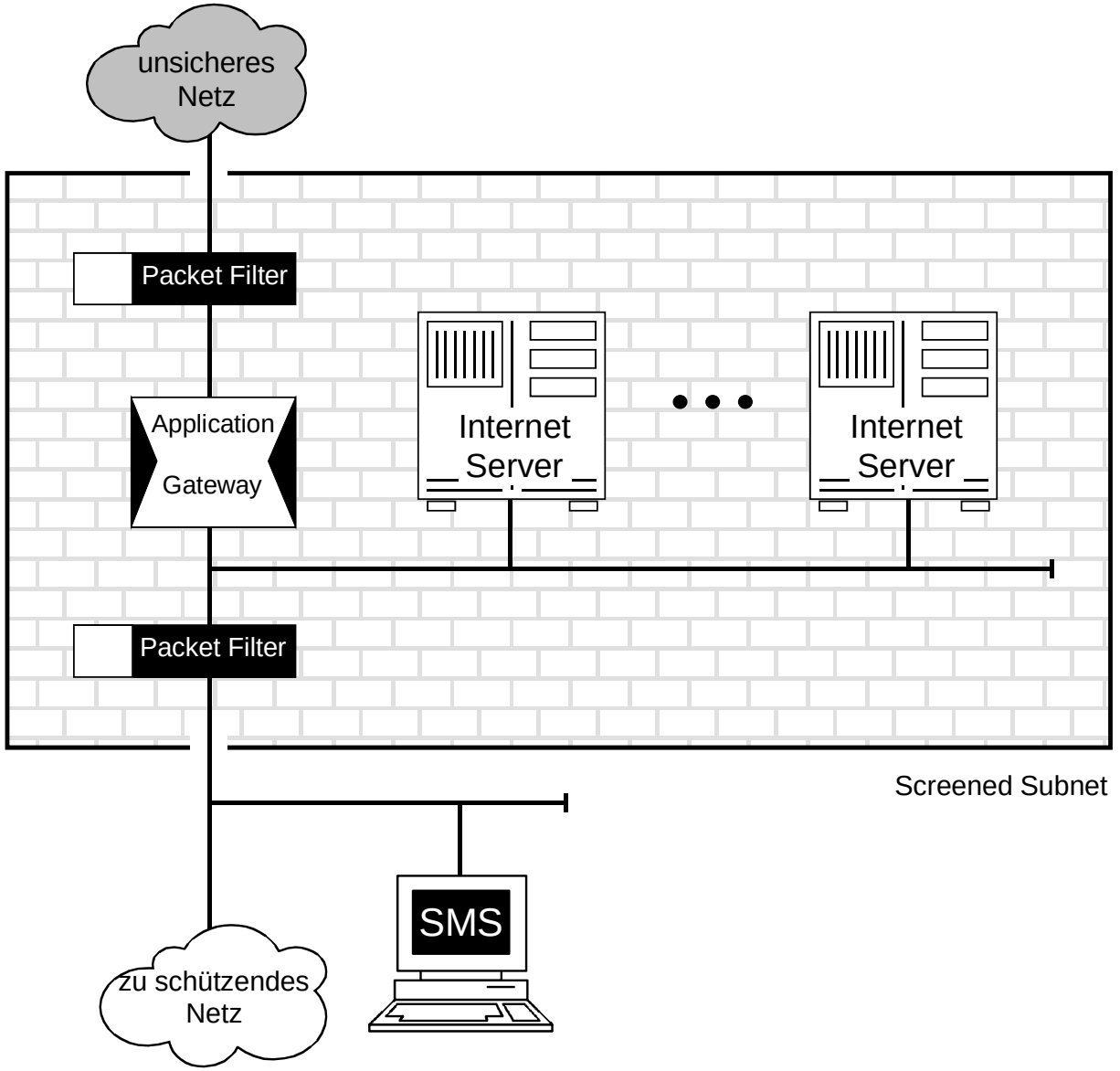
Eigener Packet Filter für die Internet-Server



Dritter Netzanschluß am Application Gateway

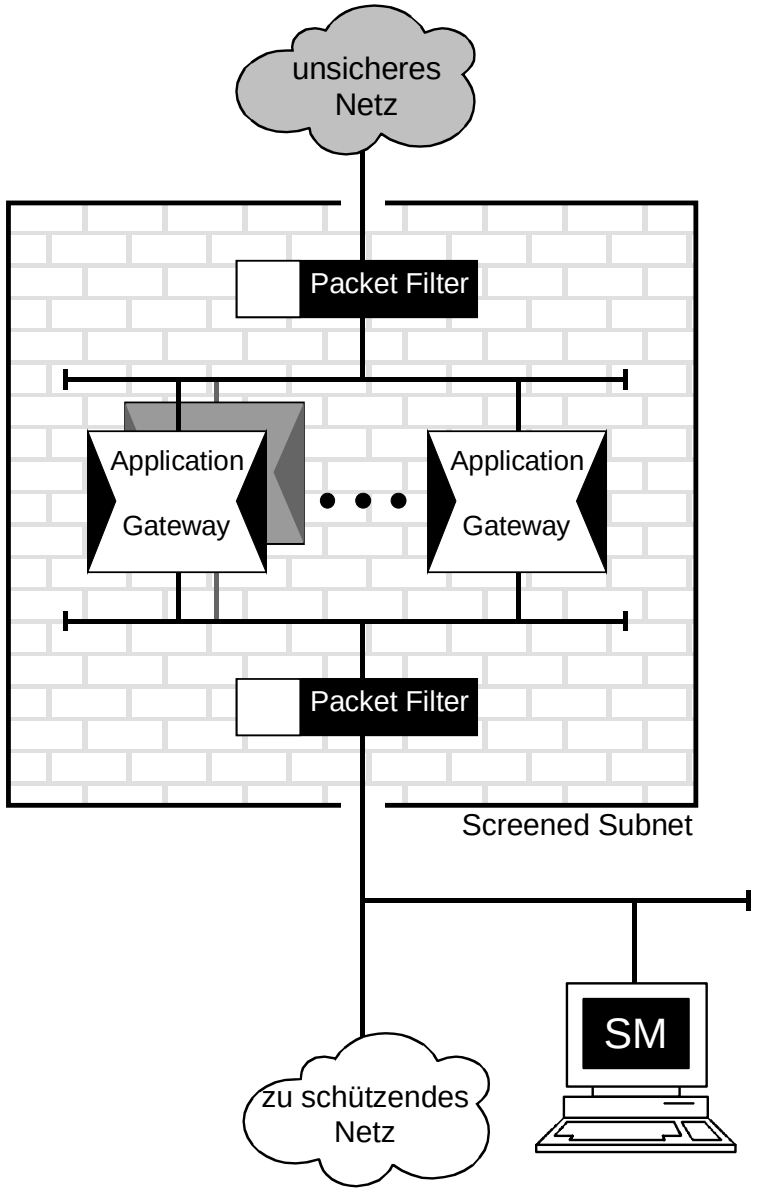


Intranet Server



Mehrere Application Gateways parallel

- Trennung bestimmter Dienste
- Leistung steigern
- Redundanz schaffen



Inhalt

- Firewall-Konzepte
- **Das richtige Firewall-Konzept für jeden Einsatzfall**
- Möglichkeiten und Grenzen
- Realisierungskonzepte
- Zusammenfassung

Das richtige Firewall-Konzept

→ Definition des Einsatzfalles

Kriterien	Einsatzfall: das unsichere Netz ist innerhalb der eigenen Organisation	Einsatzfall: das unsichere Netz ist außerhalb der eigenen Organisation
Vertrauenswürdigkeit des Netzes	**sehr hoch** - liegt in der eigenen Verantwortung - wird regelmäßig überprüft	von speziellen, **schwer bemessbaren** Faktoren abhängig - liegt nicht in der eigenen Verantwortung - es muß mit allen Risiken gerechnet werden
Vertrauenswürdigkeit des Kommunikationspartners	**sehr hoch** - die Kommunikationsteilnehmer gehören zur gleichen Organisation und arbeiten unter der gleichen Sicherheitspolitik	es wird hier angenommen, dass diese **sehr gering** ist
Angriffspotential	**sehr gering** - die Kommunikationsteilnehmer gehören zur gleichen Organisation und arbeiten unter der gleichen Sicherheitspolitik	**sehr hoch** - die Teilnehmer des Netzes haben einen sehr unterschiedlichen Schutzbedarf (Hacker neben professionellen Anwendungen) - z.B. Internet

Das richtige Firewall-Konzept

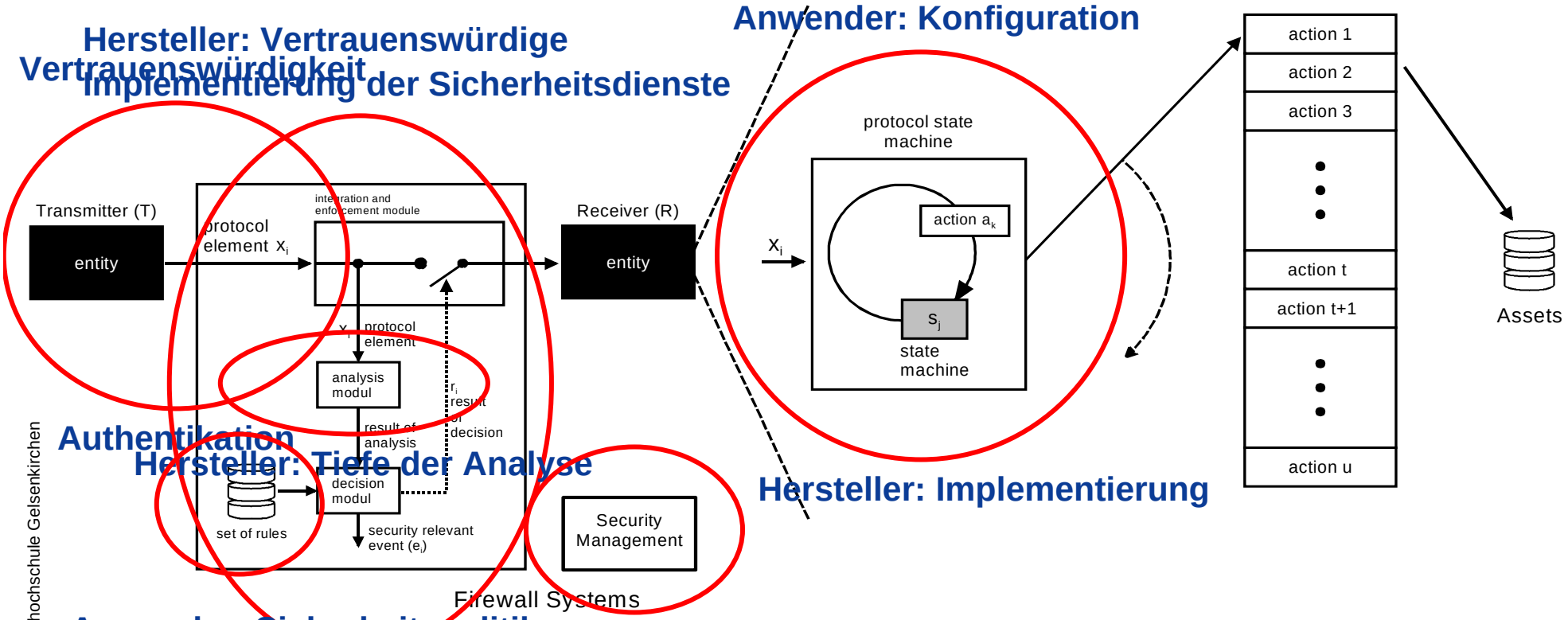
→ Entscheidungsmatrix

Schutz-bedarf	Risiken	Einsatzfall	Firewall-Konzept
niedrig	• geringfügiger Verstoß gegen Gesetze • beschränkte negative Außenwirkung • finanzieller Schaden < 25.000 DM	innerhalb der Organisation:	Packet Filter
		außerhalb der Organisation:	Dual homed Applikation Gateway
hoch	• erheblicher Verstoß gegen Gesetze • breite negative Außenwirkung • finanzieller Schaden < 5 Millionen DM	innerhalb der Organisation:	Packet Filter + Single-homed Applikation Gateway *oder* Stateful Inspection *oder* Adaptiv Proxy
		außerhalb der Organisation:	Packet Filter + dual homed Applikation Gateway
Sehr hoch	• fundamentaler Verstoß gegen Gesetze • existenzgefährdend negative Außenwirkung • finanzieller Schaden > 5 Millionen DM	innerhalb der Organisation:	Screened Subnet mit Packet Filter + Single-homed Applikation Gateway
		außerhalb der Organisation:	Screened Subnet mit Packet Filter + dual homed Applikation Gateway ⇨ High-Level Firewall-System

Inhalt

- Firewall-Konzepte
- Das richtige Firewall-Konzept für jeden Einsatzfall
- **Möglichkeiten und Grenzen**
- Realisierungskonzepte
- Zusammenfassung

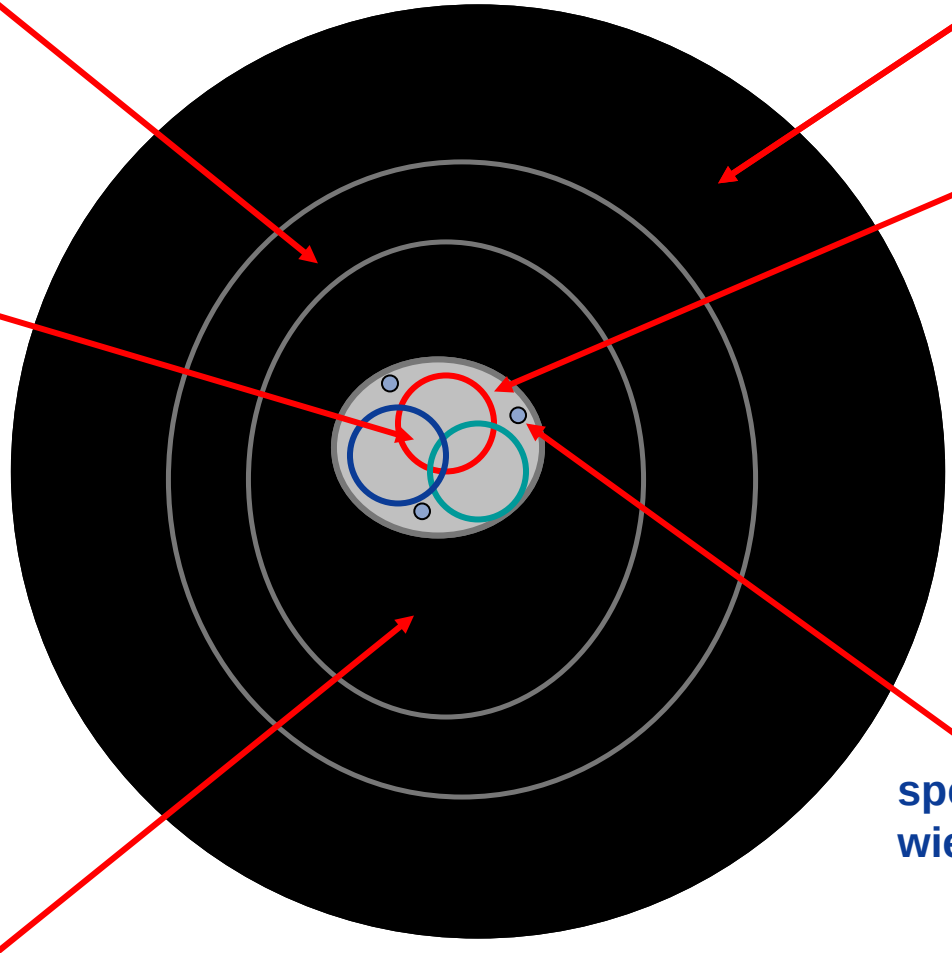
Das Kommunikationsmodell mit integriertem Firewall-System



Anwender: Sicherheitspolitik

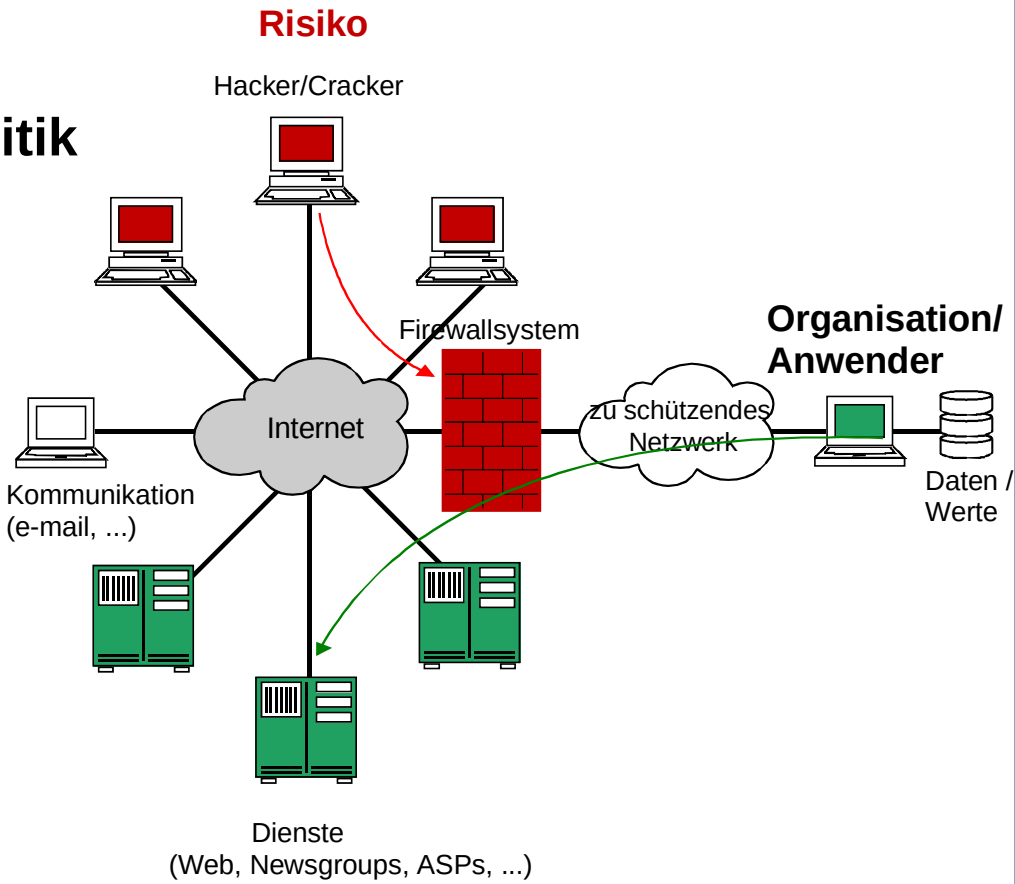
$$a_k = \textit{action-select}(\ \textit{protocol-state-machine}(x_i, s_j),\ \textit{authenticity}(x_i, t_l),\ \textit{result-of-decision}(\ \textit{analysis}(x_i),\ \textit{security-management}(\textbf{rules})\ ),\ \textit{functionality-of-the-firewall-system}()\ )$$

Konzeptionelle Möglichkeiten (1/2)
→ Reduzierung des Schadensrisikos



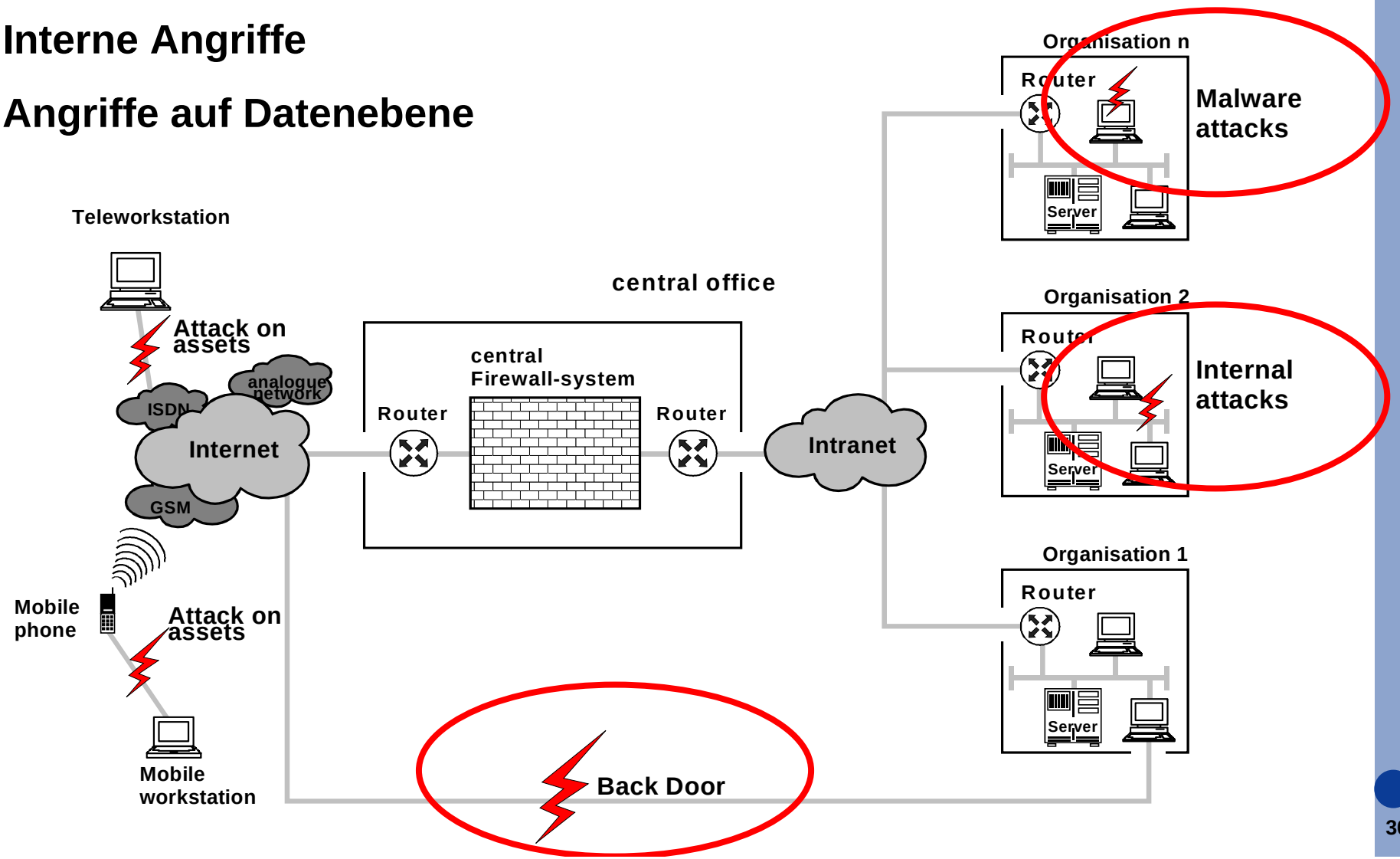
Konzeptionelle Möglichkeiten (2/2)
→ Common Point of Trust-Konzept

- **Kosten**
- **Umsetzung der Sicherheitspolitik**
- **Sicherheitsinfrastruktur**
- **Sicherheit durch Abschottung**
- **Überprüfbarkeit**



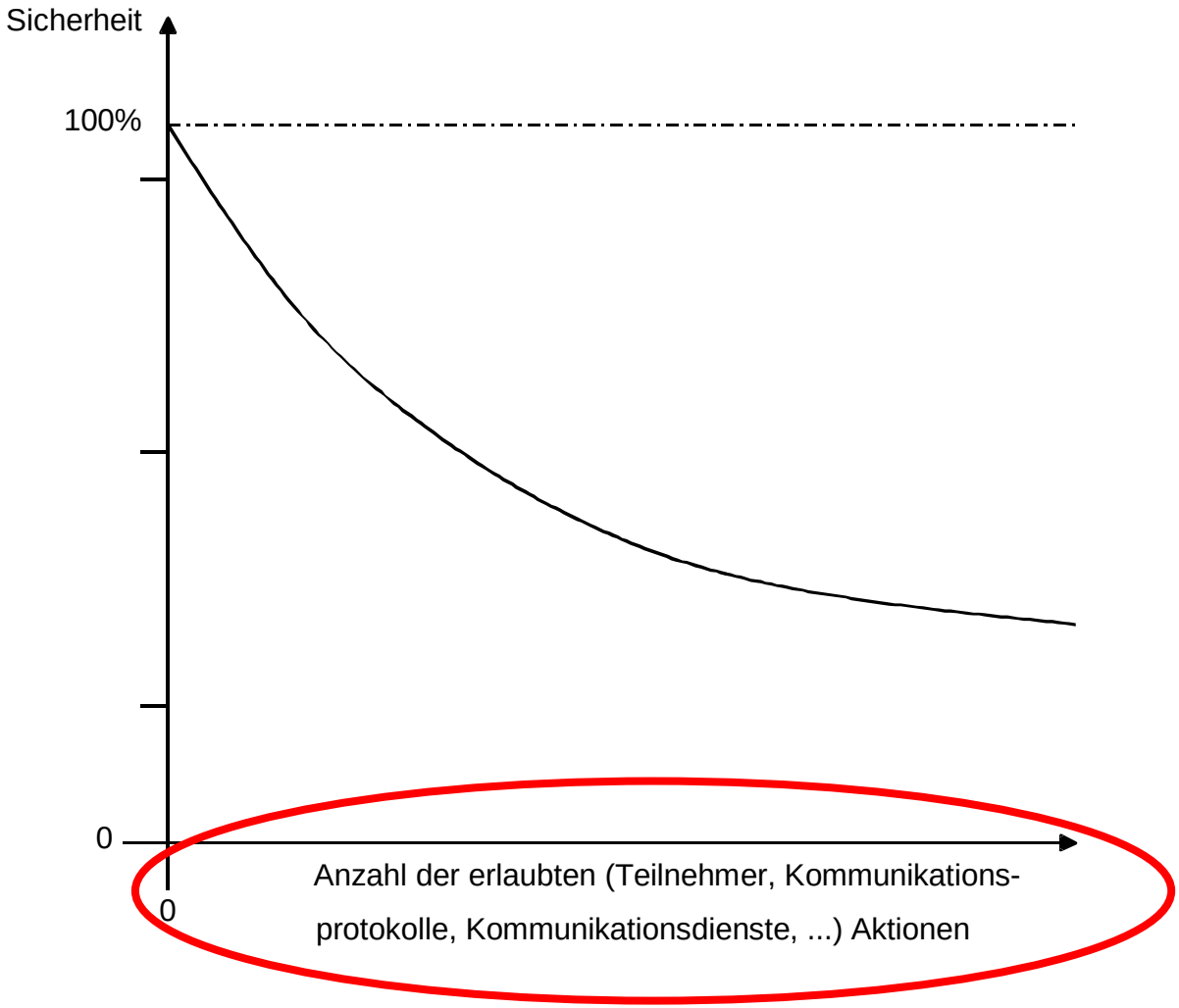
Konzeptionelle Grenzen eines zentralen Firewall-Systems (1/2)

- Hintertüren (Back Door)
- Interne Angriffe
- Angriffe auf Datenebene



Konzeptionelle Grenzen eines zentralen Firewall-Systems (2/2)

- **Security versus connectivity <-> Risiko versus Chance**

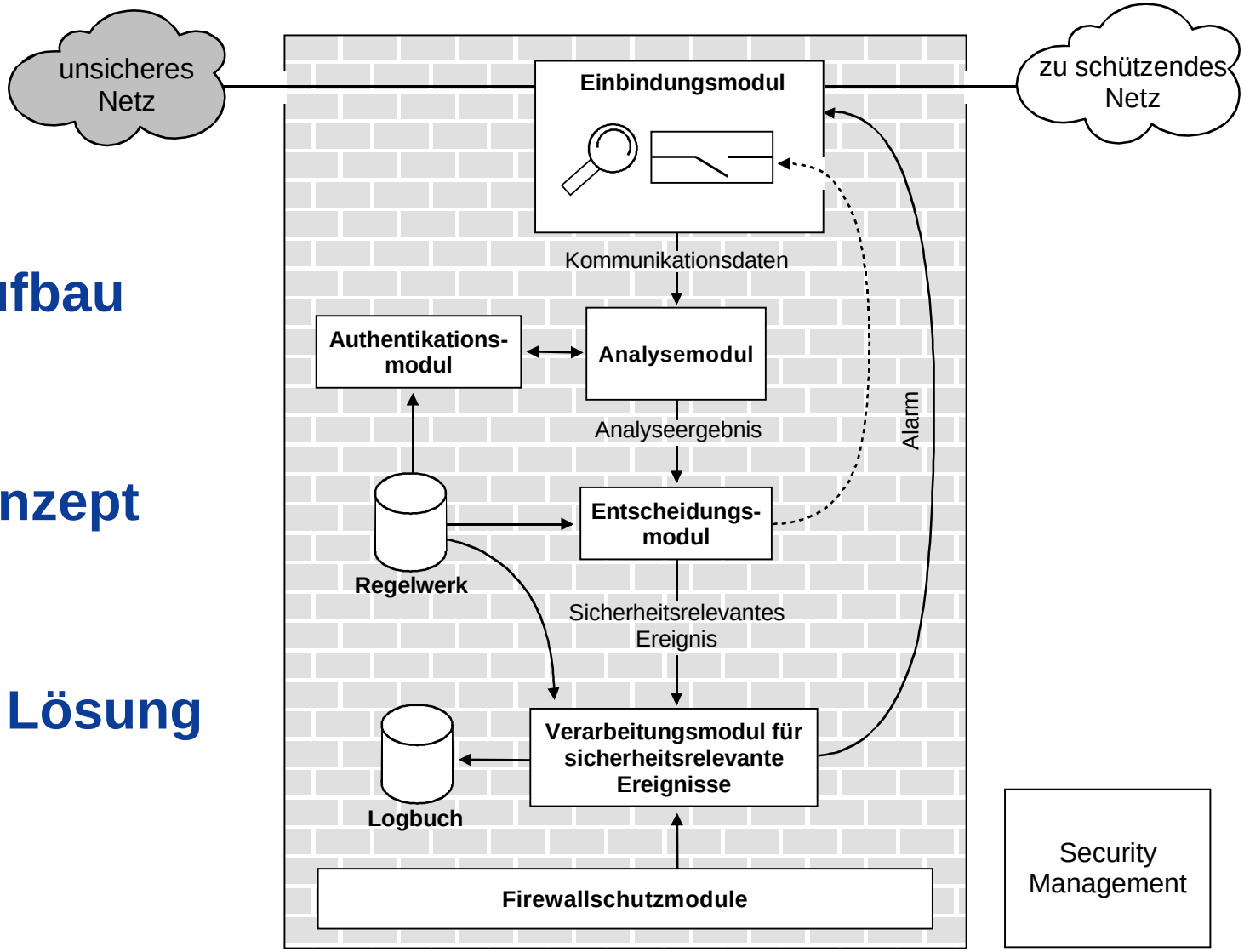


Inhalt

- Firewall-Konzepte
- Das richtige Firewall-Konzept für jeden Einsatzfall
- Möglichkeiten und Grenzen
- **Realisierungskonzepte**
- Zusammenfassung

Realisierungskonzepte

- **Systemaufbau**
- **Designkonzept**
- **Turn-Key Lösung**



Systemaufbau
→ Firewallschutzmechanismen

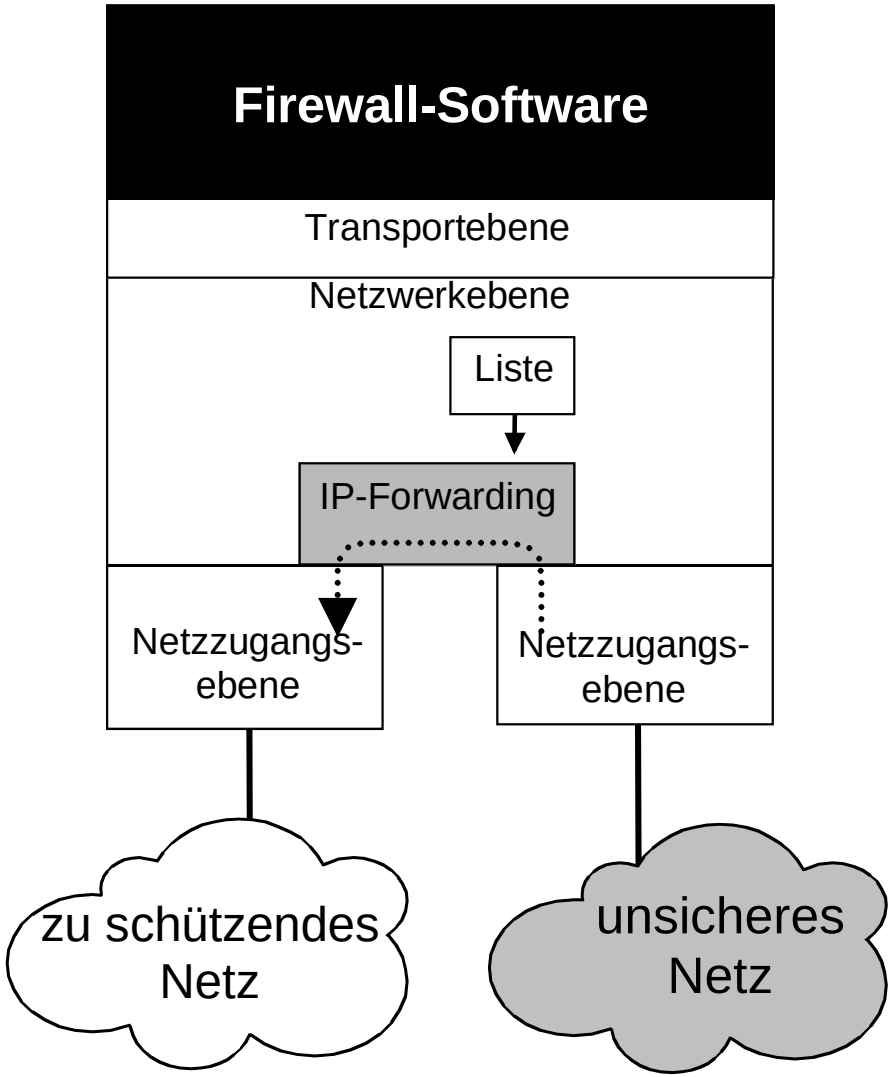
- Ein aktives Firewall-Element muss nicht nur Sicherheitsdienste erbringen, sondern auch selbst gegen Angriffe resistent sein.
  - **Sicheres Betriebssystem**
  - **Integritätstest**
    (regelmäßige/spontane Checksummenüberprüfung)
    - Gewährleistung der Softwareintegrität
      (Betriebssystem, Firewall-Software)
    - Gewährleistung der Informationen
      (Regelwerk, Logbuch)
  - **Authentikationsmechanismus**
    (nur berechtigte können Regelwerk u. Logbücher beeinflussen)
  - **Betriebssicherungsmechanismen**
    - Überprüfung des Überlaufes von Logbüchern und Speichermedien
    - Überprüfung der Automatenzustände

Designkonzept (1/2)

- **Minimale Software**
  - fehlerfreie Software
  - klar strukturiert und nachvollziehbarer Aufbau
  - keine Routerfunktionalitäten, keine weiteren Anwendungen
- **Getrenntes Security Management**
  z.B. auf einem separaten Rechnersystem
- **Einfache, zuverlässige und berechtigte Bedienung**
  des Security Managements

Designkonzept (2/2)

- **Sichere Einbindung** in das Kommunikationssystem (Netzwerksoftware, Betriebssystem, ...)
  - Sicherstellung, dass die Firewall-Funktionalität nicht über das Betriebssystem umgangen werden kann (z.B. IP-Forwarding - Kernel-Funktionalität)



Turn-Key Lösung

- **Fertiglösung**
  - Stellt ein vollständiges Sicherheitskonzept zur Verfügung, nicht nur Module
- **Verantwortungsbereich**
  - Die Verantwortung für Hardware, Betriebssystem, Firewall-Software liegt in einer Hand
- **Besseres Zusammenwirken der Sicherheitsmechansimen**
  - Immer die gleichen Firewall-Elemente arbeiten zusammen und sind in ihrer Konfiguration optimal eingestellt und passen zusammen
- **Sicherheitsaspekte**
  - Weniger Fehler, da die Lösung aus einer Hand kommt

Inhalt

- Firewall-Konzepte
- Das richtige Firewall-Konzept für jeden Einsatzfall
- Möglichkeiten und Grenzen
- Realisierungskonzepte
- **Zusammenfassung**

Firewall-Konzept
→ Zusammenfassung

- Durch eine geschickte Kombination einzelner aktiver Firewall-Elemente lässt sich ein höheres Maß an Sicherheit erzielen als bei der Nutzung nur eines aktiven Firewall-Elementes.
- Es gibt sehr unterschiedliche Entscheidungskriterien, welches Firewall-Konzept wann für die Kopplung unterschiedlicher Netze eingesetzt werden soll.
- Aus den konzeptionellen Grenzen eines zentralen Firewall-Systems folgt, dass bei einer praktischen Realisierung von Firewall-Systemen weitere ergänzende Sicherheitsmechanismen hinzugefügt werden müssen, damit die Verwundbarkeit minimiert wird.
- Die Sicherheit von Firewall-Systemen hängt auch von den Realisierungskonzepten ab!

Firewall-Systeme

Konzepte - Möglichkeiten und Grenzen - Realisierung

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen