



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Firewall-Systeme

Konzepte - Möglichkeiten und Grenzen - Realisierung

Prof. Dr. (TU NN)

Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet-sicherheit.


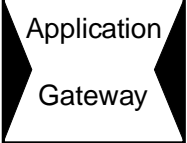
- **Firewall-Konzepte**
- **Das richtige Firewall-Konzept für jeden Einsatzfall**
- **Möglichkeiten und Grenzen**
- **Realisierungskonzepte**
- **Zusammenfassung**

■ Firewall-Konzepte

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

Firewall-Elemente und -Konzepte

■ Firewall-Elemente

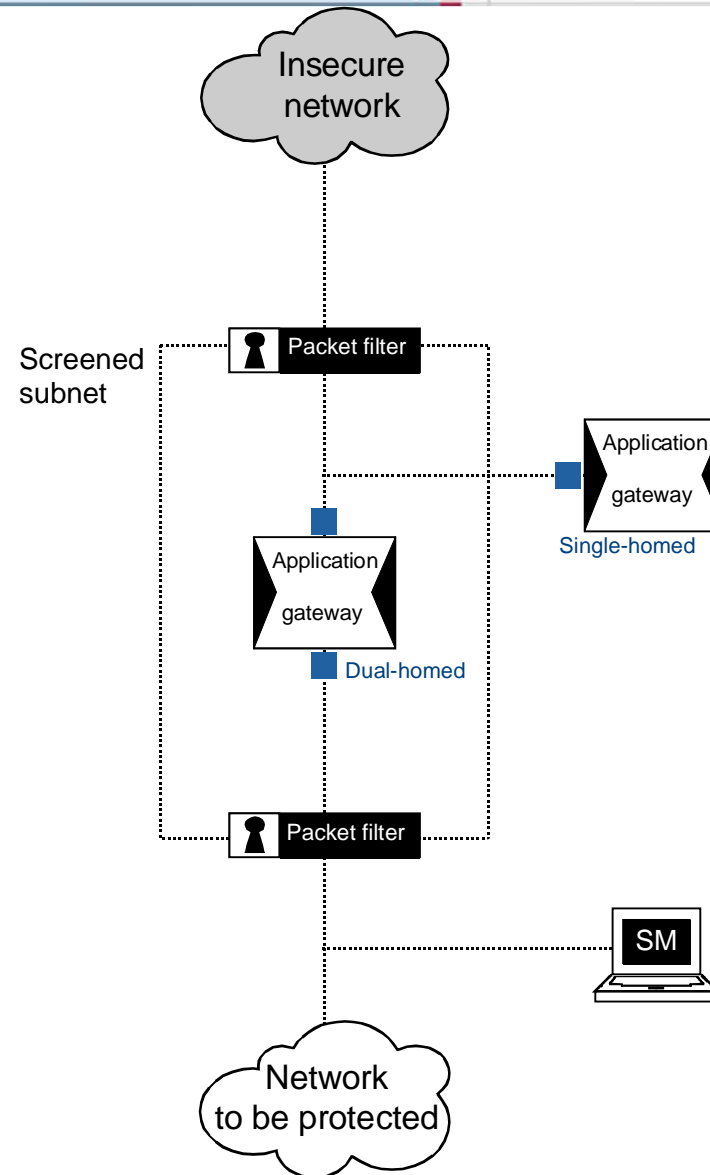
- Packet Filter  Packet Filter
- Zustandsorientierter Packet Filter (stateful inspection)
- Application Gateway 
- Adaptive Proxy

■ 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
- Screened Subnet mit Packet Filter und single-homed Application Gateway
- Screened Subnet mit Packet Filter und dual-homed Application Gateway



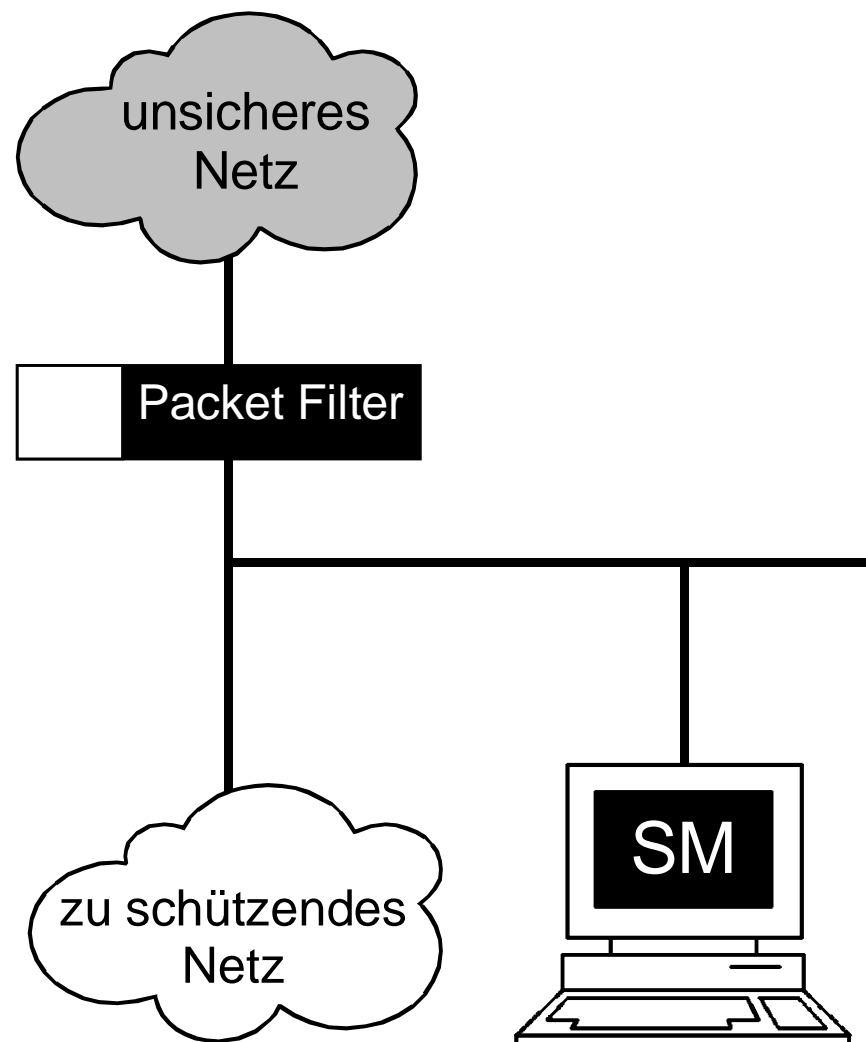
Ausschließlicher Einsatz eines Packet Filters

Bewertung

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

Einsatzgebiet

- Intranet



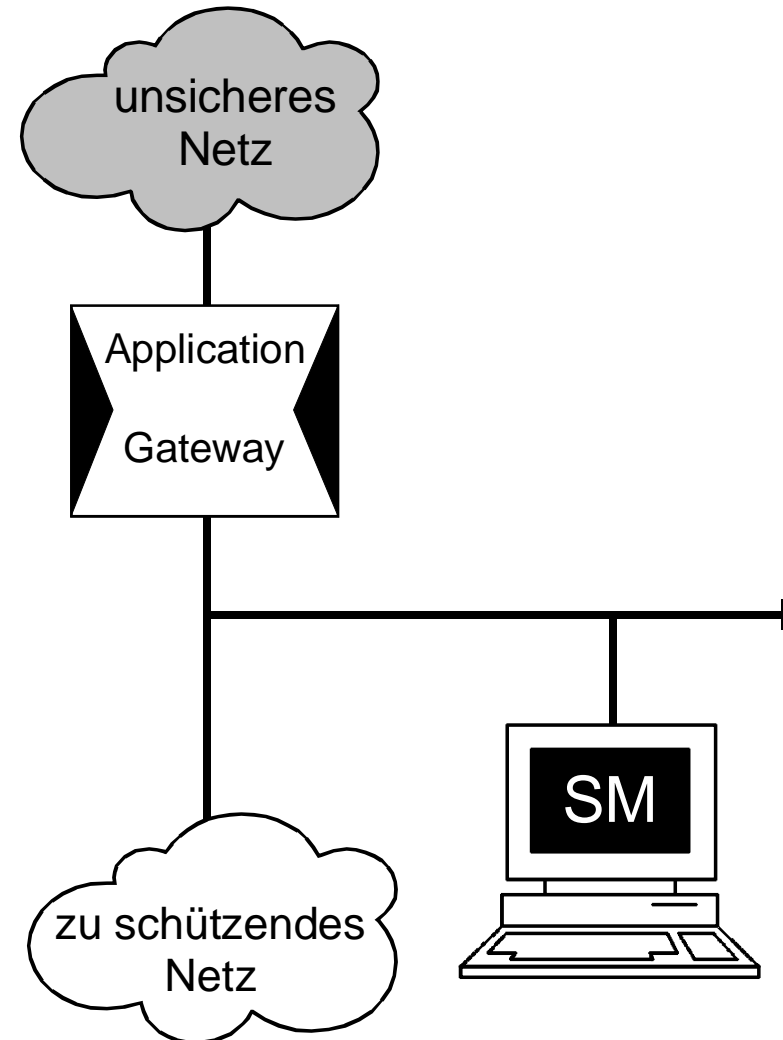
Ausschließlicher Einsatz eines Application Gateway

Bewertung

- Hochwertige Sicherheitsdienste
- Verbindungsdaten können ausführlich protokolliert werden

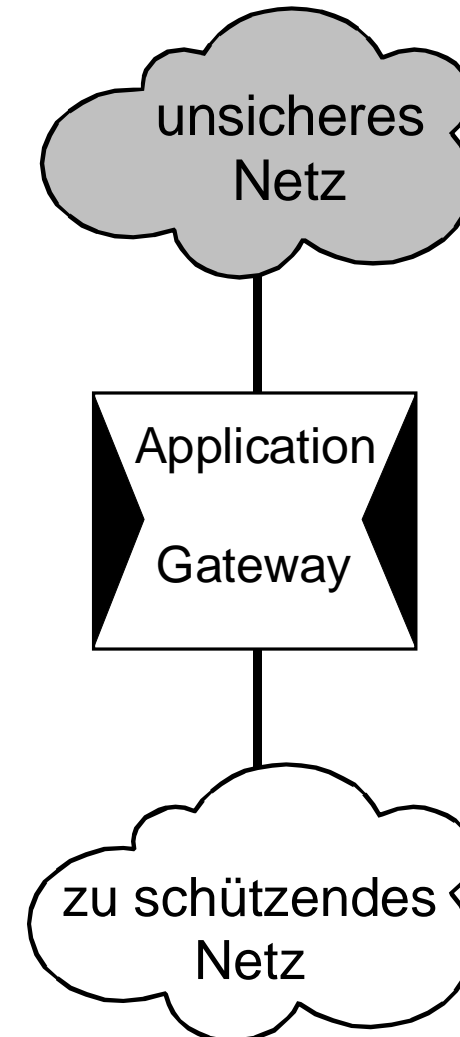
Einsatzgebiet

- Gleichwertige Organisationen mit hohem Schutzbedarf



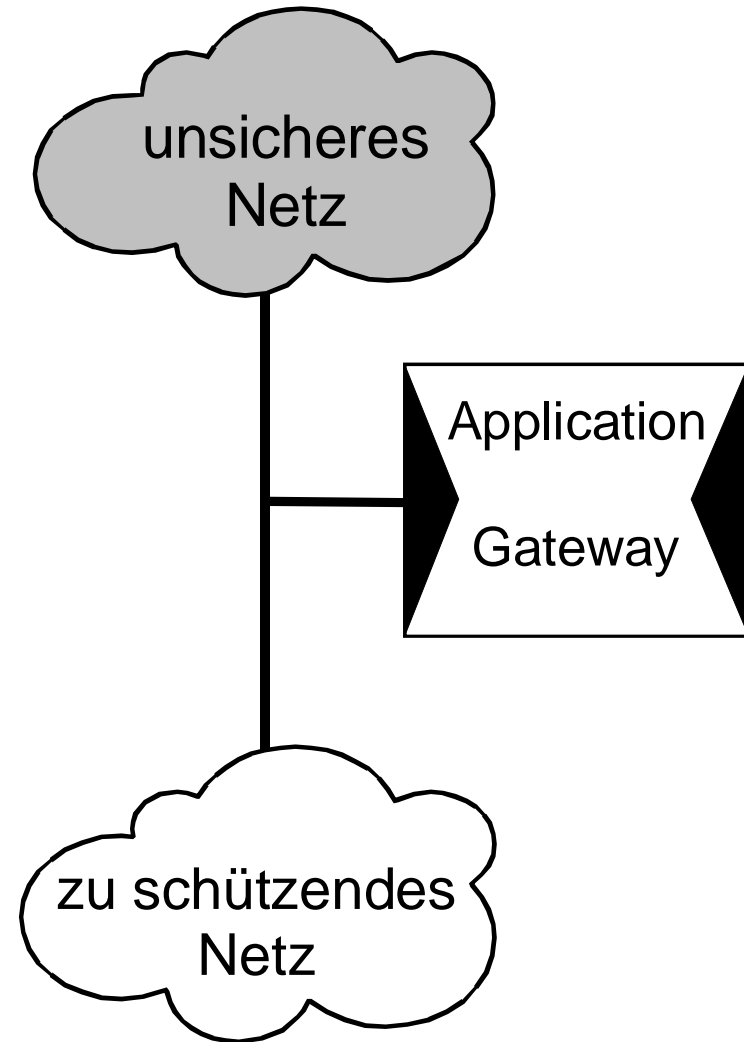
Dual-homed Application Gateway

- 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



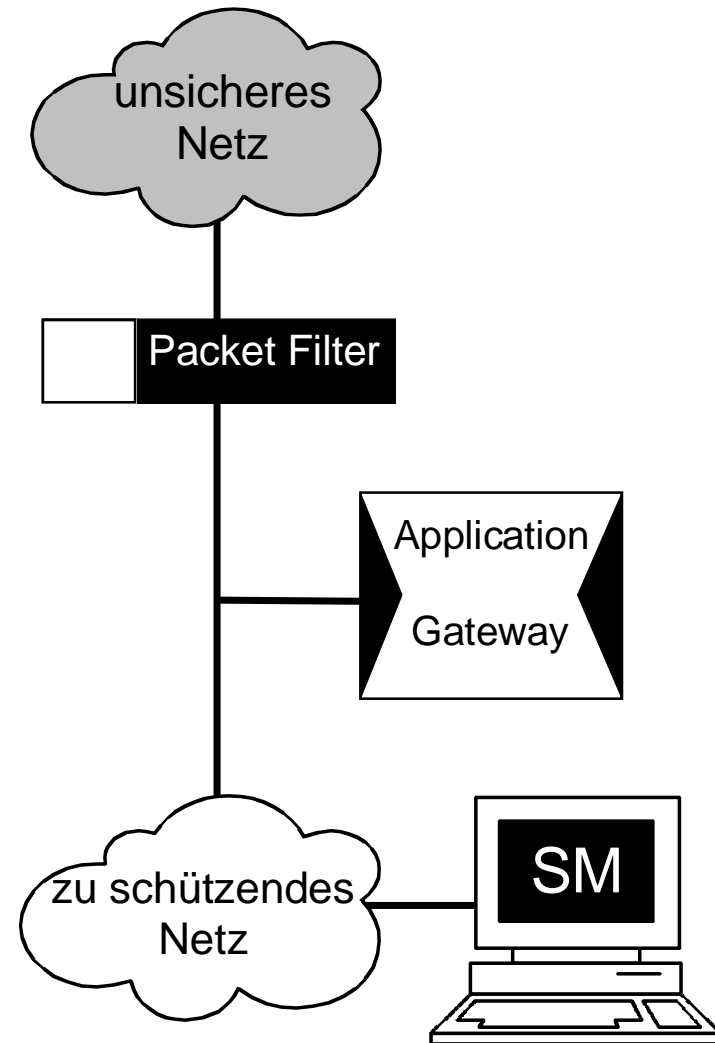
Packet Filter und single-homed Application Gateway (1/2)

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



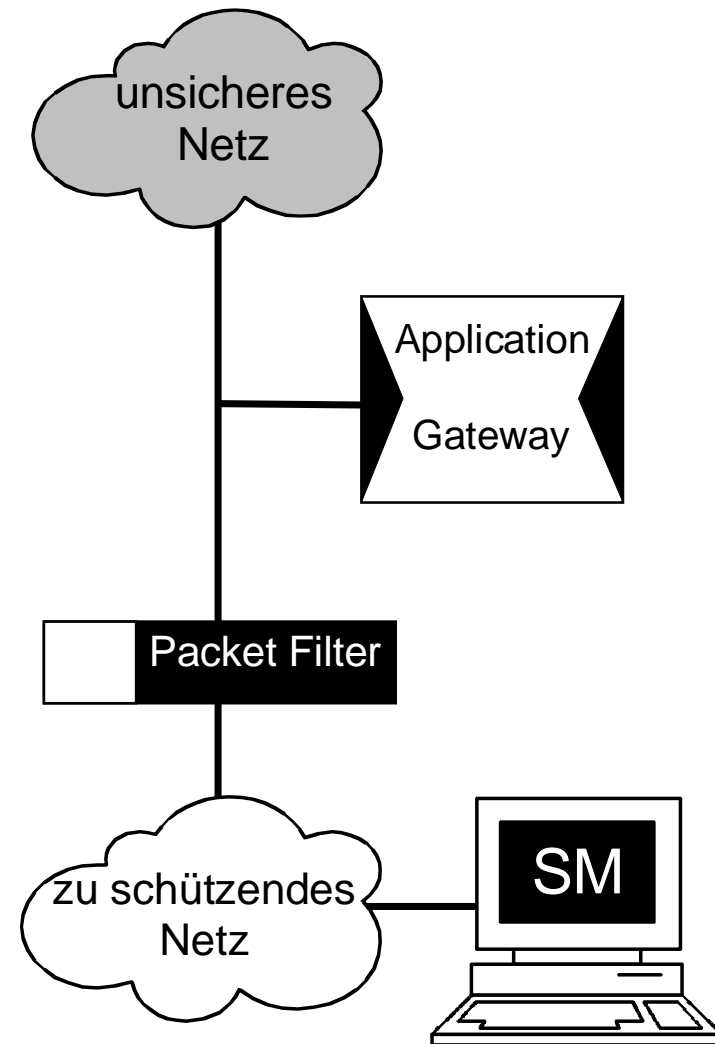
Packet Filter und single-homed Application Gateway (2/2)

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



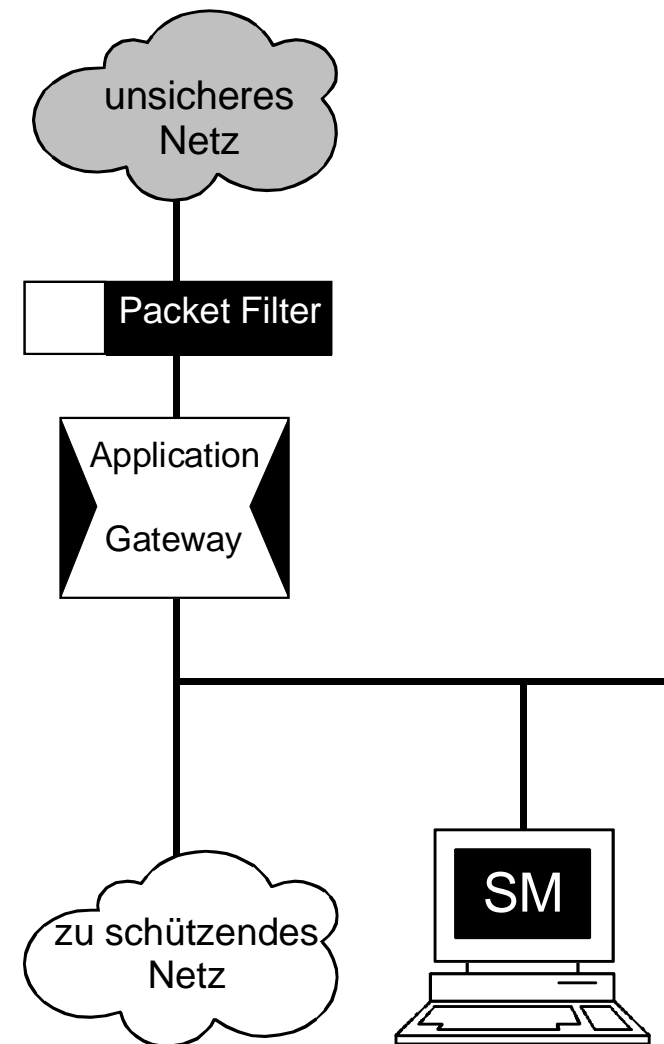
Packet Filter und dual-homed Application Gateway (1/2)

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



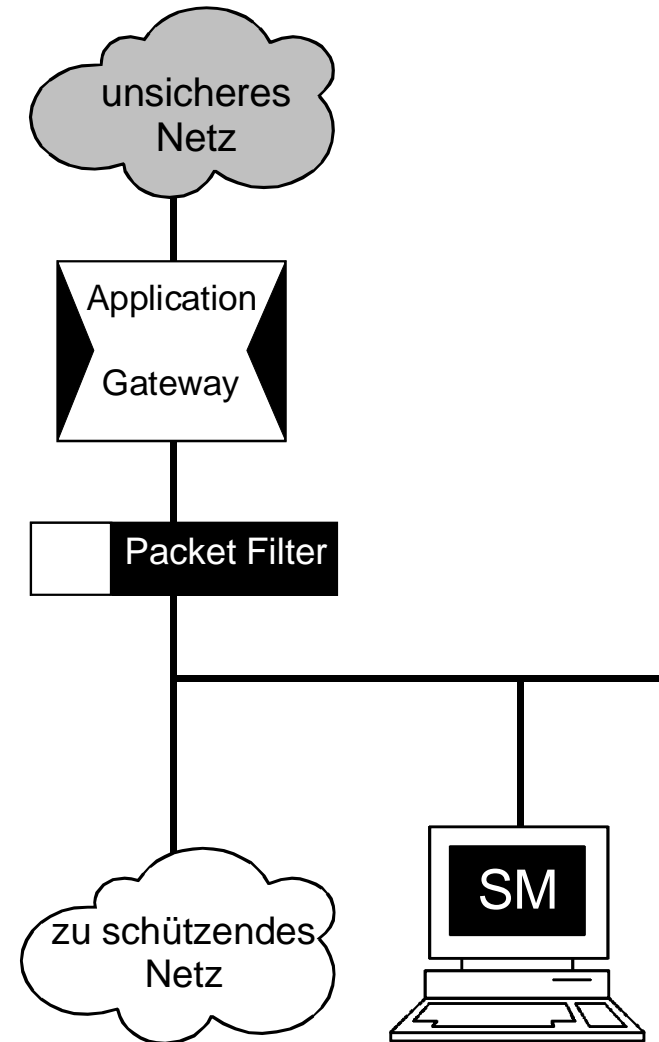
Packet Filter und dual-homed Application Gateway (2/2)

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 (---)**

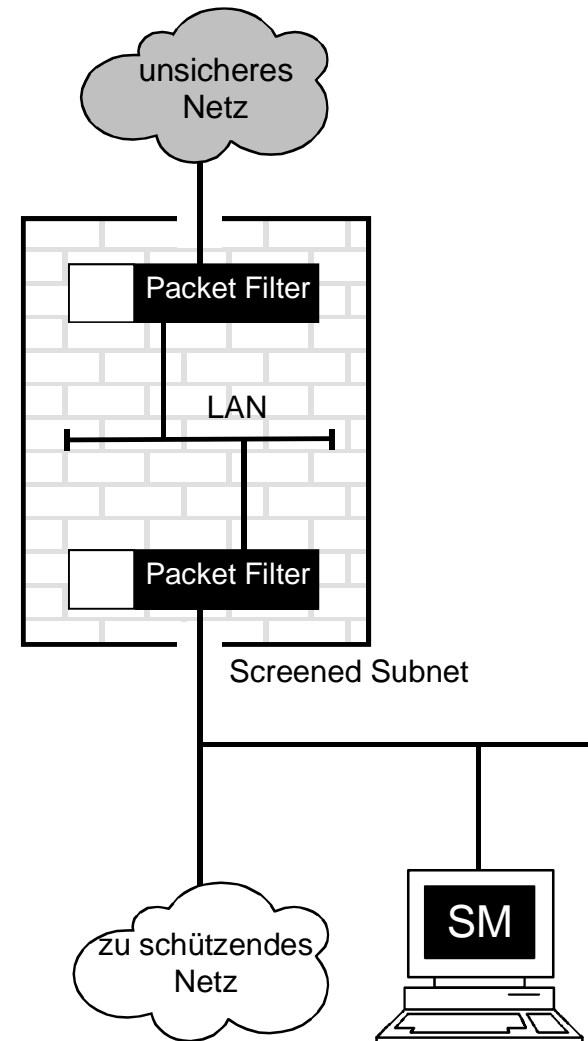
Einsatzgebiet

- 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



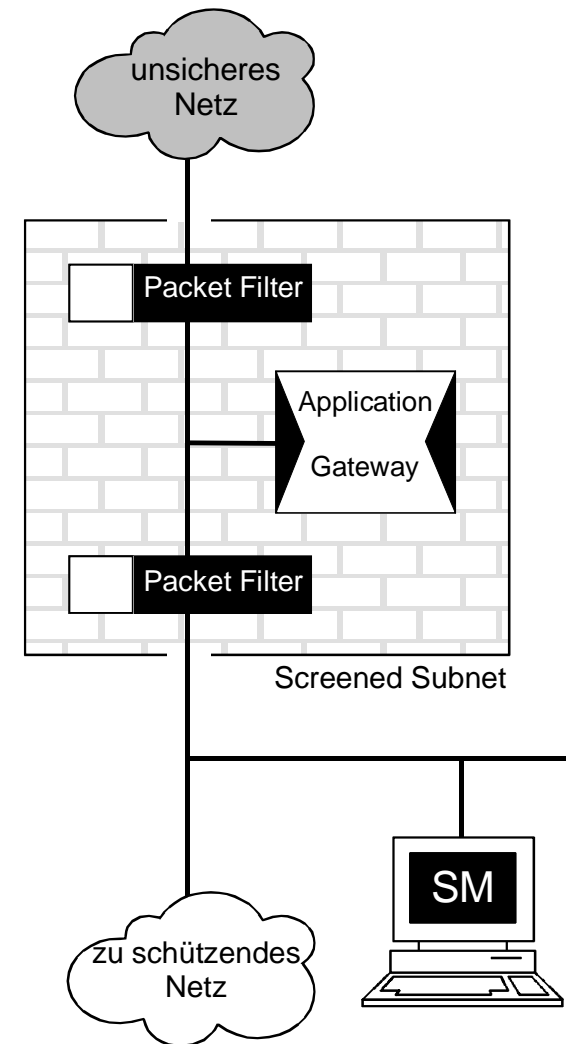
Zwei Packet Filter als Screened Subnet und ein single-homed Application Gateway

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

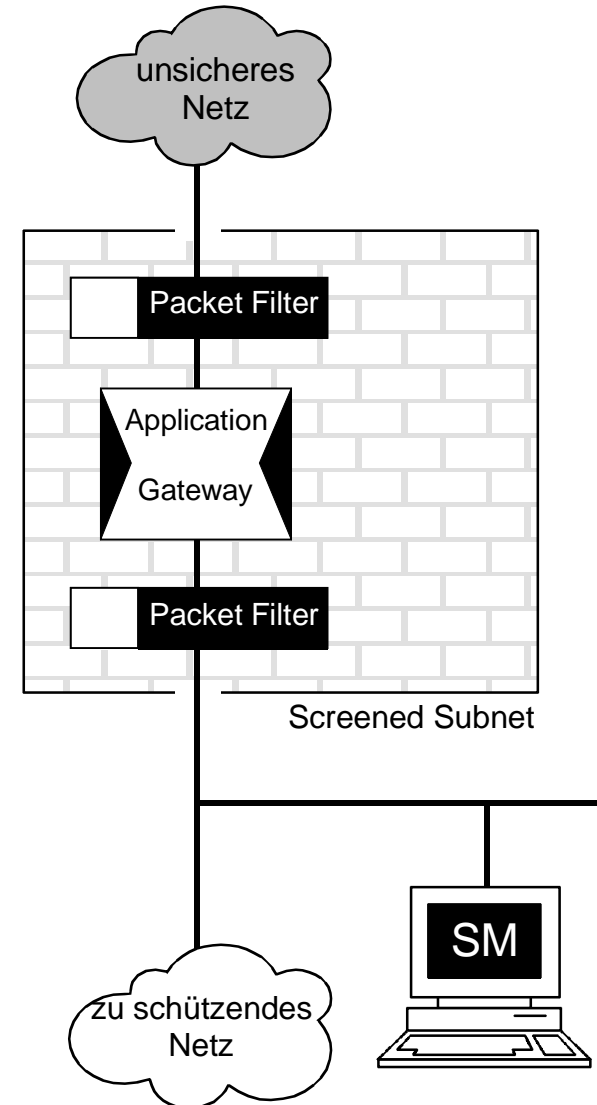


High-level Security Firewall-System

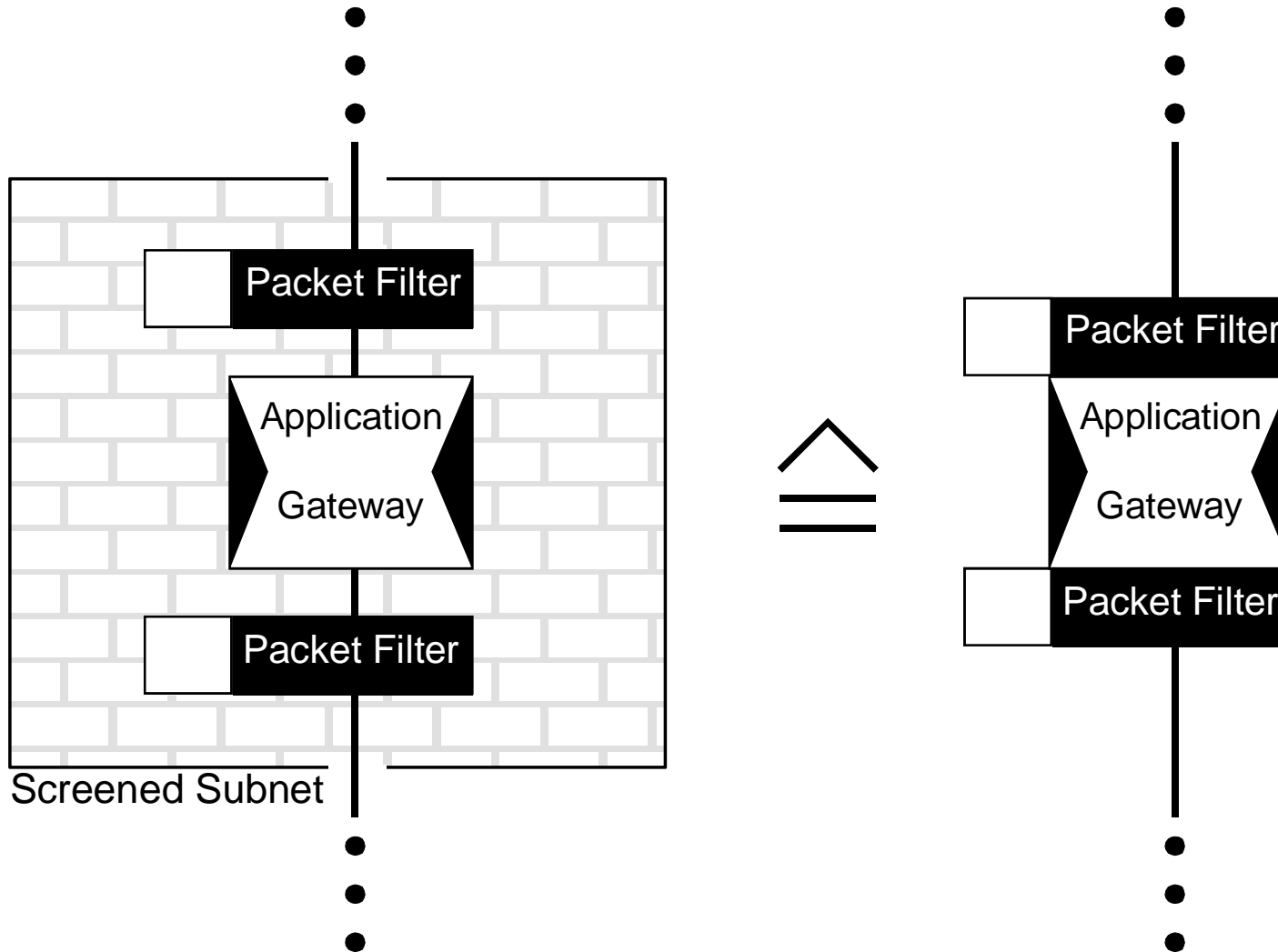
- Einfache Regeln
- Gegenseitiger Schutz
- Geschachtelte Sicherheit
- Verschiedene Betriebssysteme
- Unterschiedliche Einbindungs- und Analysemöglichkeiten
- Separates Security Management

Einsatzgebiet

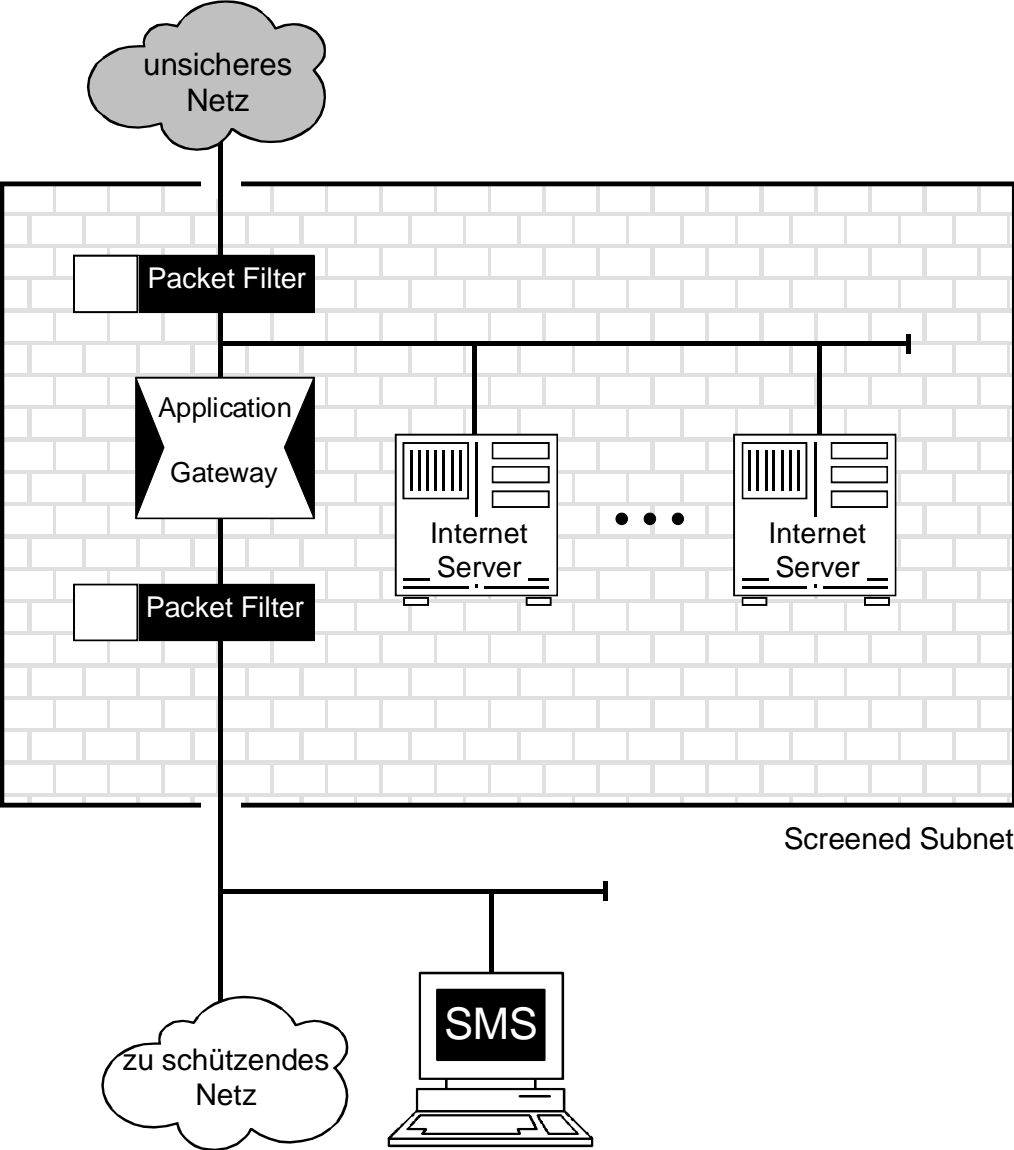
- Das Internet Firewall-System



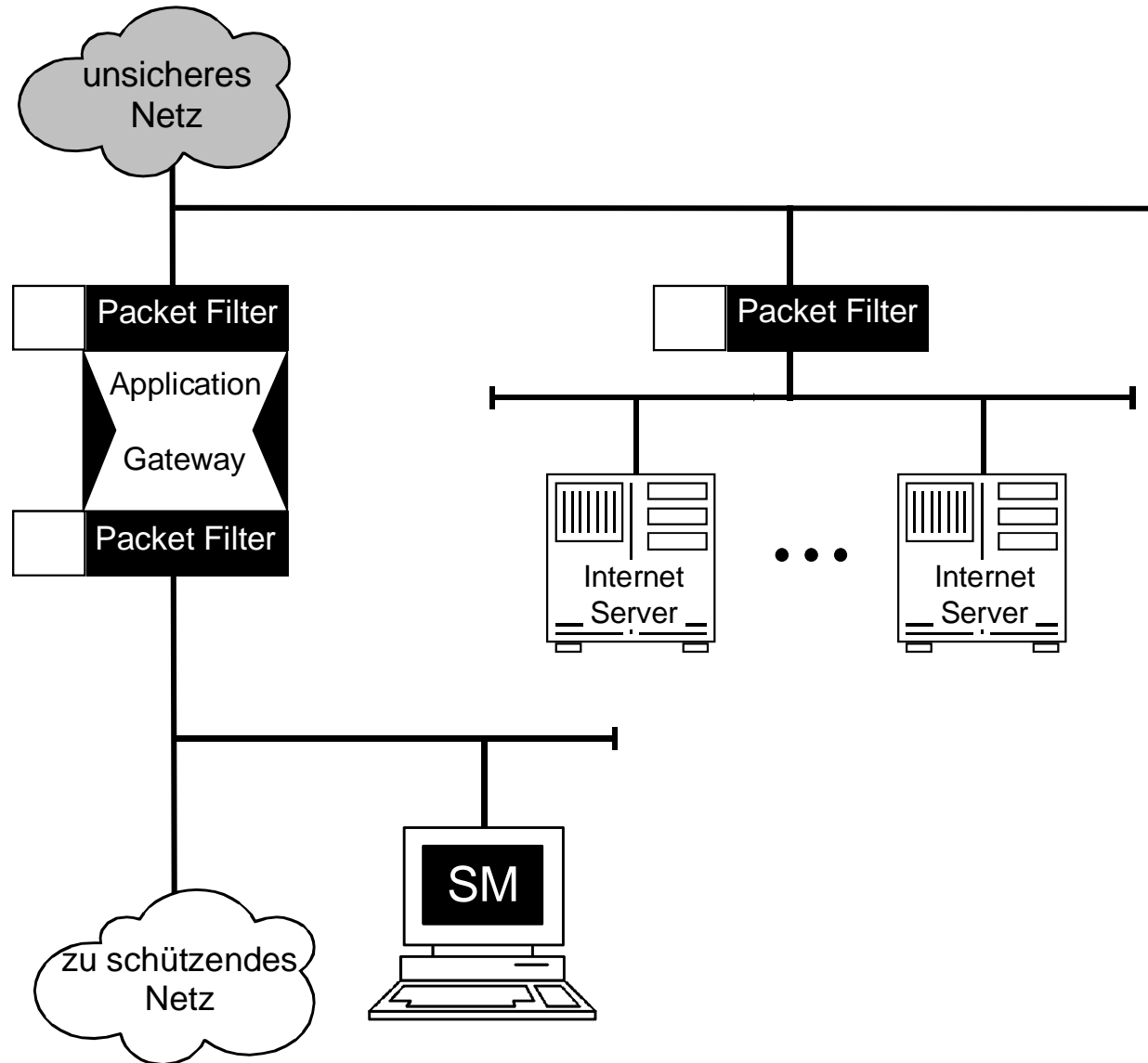
Symbol eines High-level Security Firewall-Systems



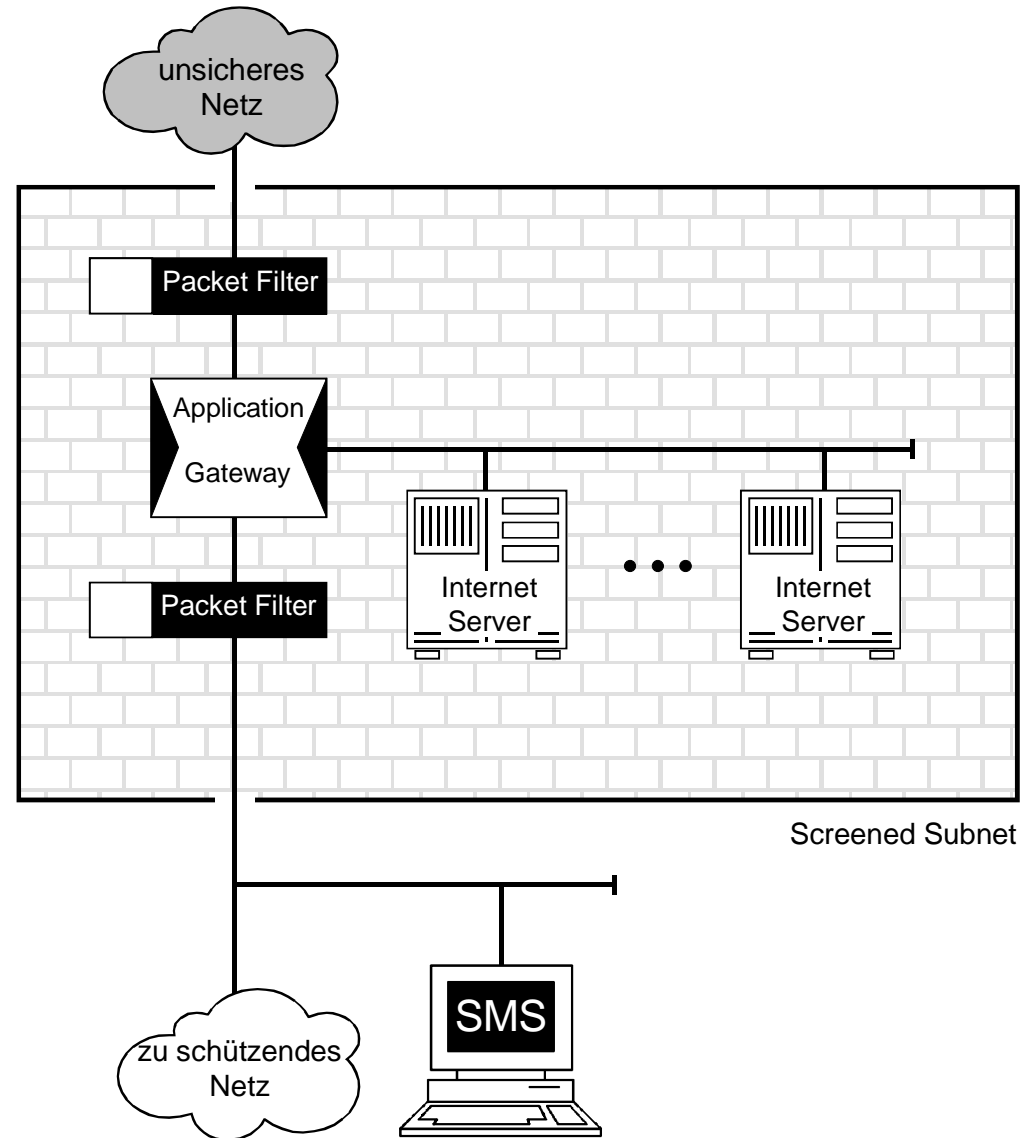
Internet Server



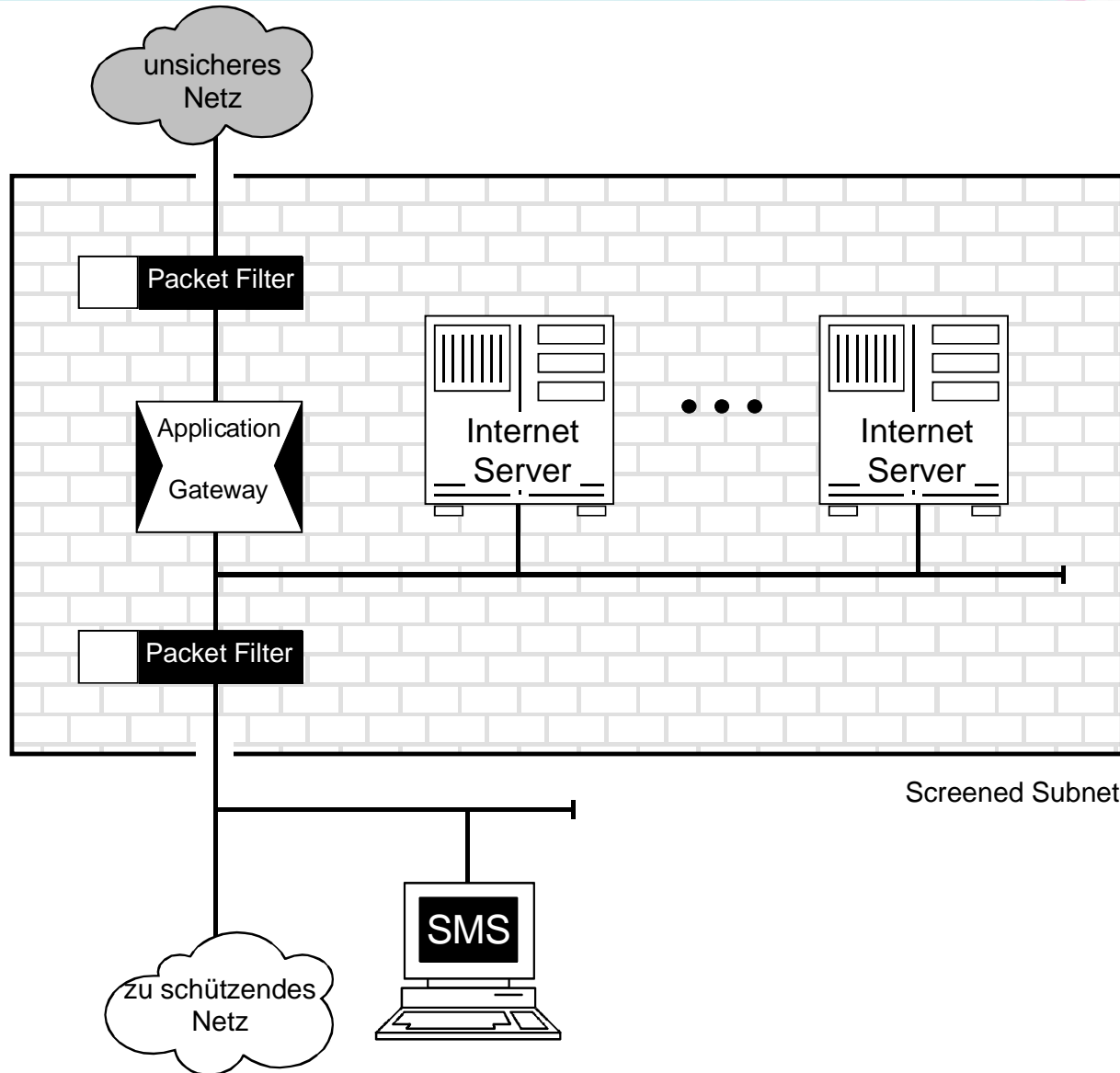
Eigener Packet Filter für die Internet-Server



Dritter Netzanschluss am Application Gateway

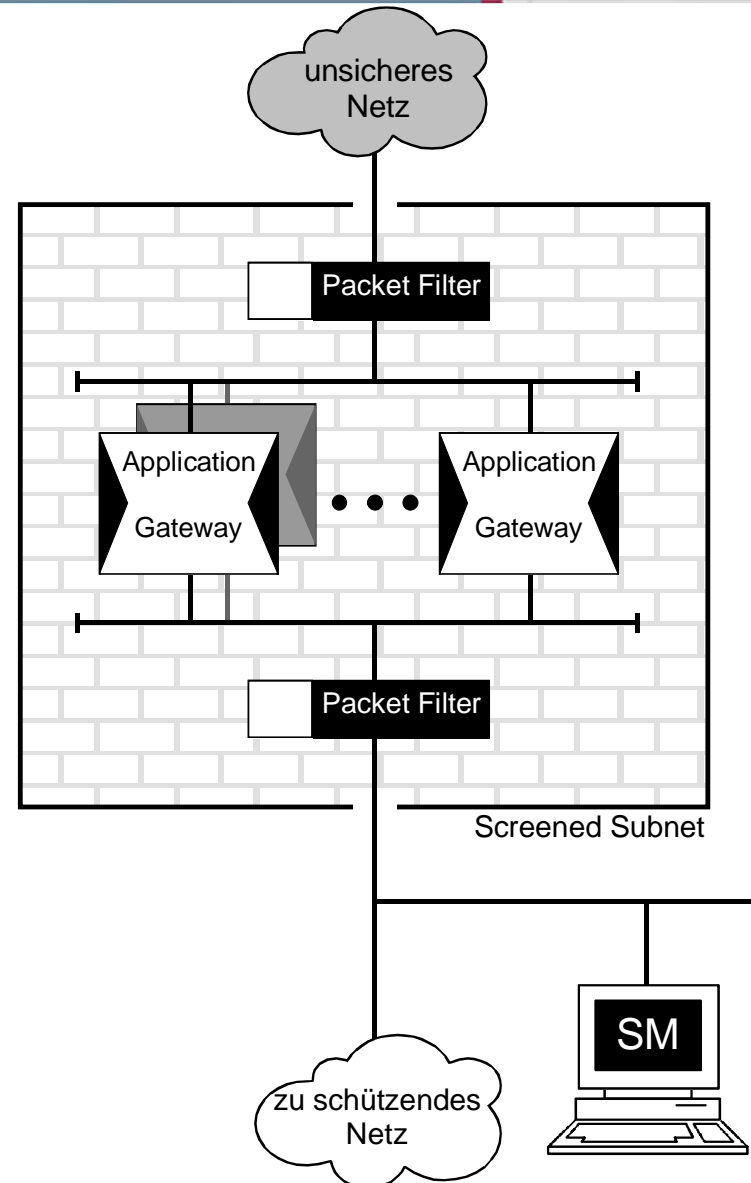


Intranet Server



Mehrere Application Gateways parallel

- Trennung bestimmter Dienste
- Leistung steigern
- Redundanz schaffen



- 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	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

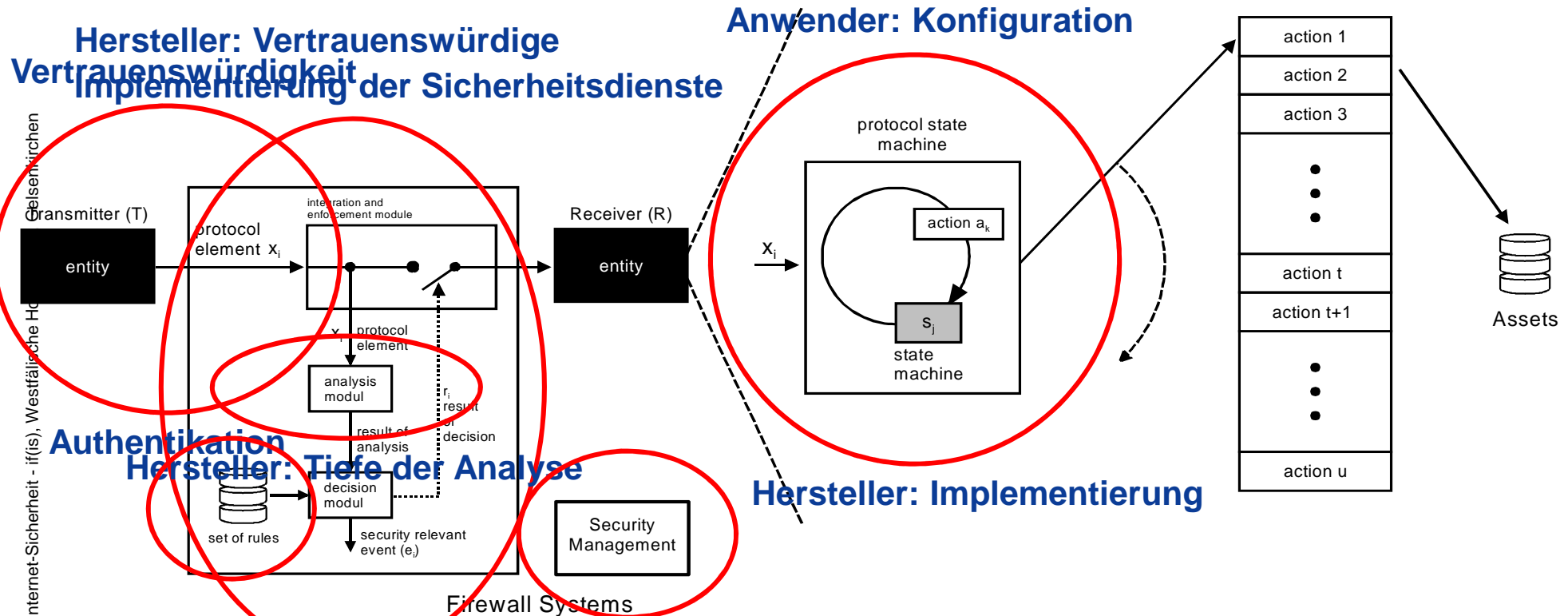
Das richtige Firewall-Konzept

→ Entscheidungsmatrix

Schutzbedarf	Risiken	Einsatzfall	Firewall-Konzept
niedrig	<ul style="list-style-type: none"> geringfügiger Verstoß gegen Gesetze beschränkte negative Außenwirkung finanzieller Schaden < 25.000 € 	innerhalb der Organisation:	Packet Filter
		außerhalb der Organisation:	Dual homed Applikation Gateway
hoch	<ul style="list-style-type: none"> erheblicher Verstoß gegen Gesetze breite negative Außenwirkung finanzieller Schaden < 5 Millionen € 	innerhalb der Organisation:	Packet Filter + Single-homed Applikation Gateway <i>oder</i> Stateful Inspection <i>oder</i> Adaptiv Proxy
		außerhalb der Organisation:	Packet Filter + dual homed Applikation Gateway
Sehr hoch	<ul style="list-style-type: none"> fundamentaler Verstoß gegen Gesetze existenzgefährdend negative Außenwirkung finanzieller Schaden > 5 Millionen € 	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

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

Das Kommunikationsmodell mit integriertem Firewall-System



$$a_k = \text{action-select} \left(\begin{array}{l} \text{protocol-state-machine}(x_i, s_j), \\ \text{authenticity}(x_i, t_i), \\ \text{result-of-decision}(\text{analysis}(x_i), \text{security-management}(\text{rules})), \\ \text{functionality-of-the-firewall-system}() \end{array} \right)$$

Konzeptionelle Möglichkeiten (1/2)

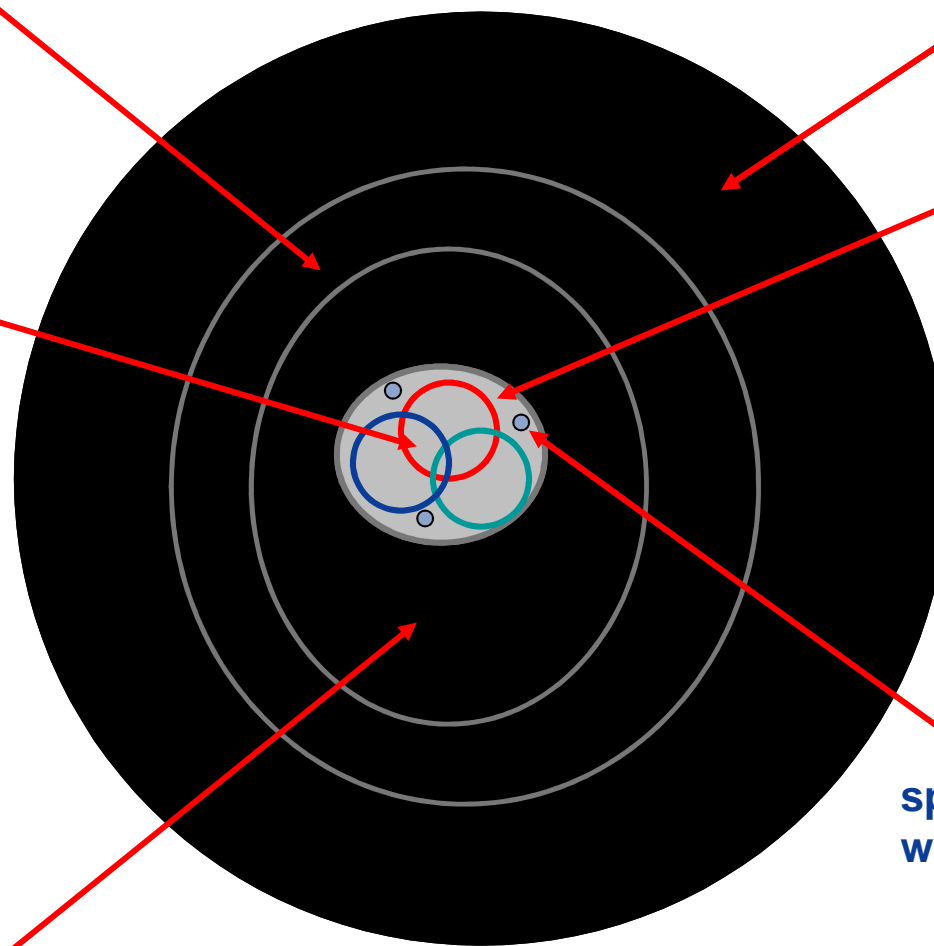
→ Reduzierung des Schadensrisikos

Einschränkung der erlaubten Protokolle

Protokolle, die nicht erlaubt sind

Kommunikations-
Profile

zeitliche
Einschränkung



spezielle Anwendungen,
wie z.B. SMTP

Einschränkung der erlaubten Rechnersysteme

Konzeptionelle Möglichkeiten (2/2)

→ Common Point of Trust-Konzept

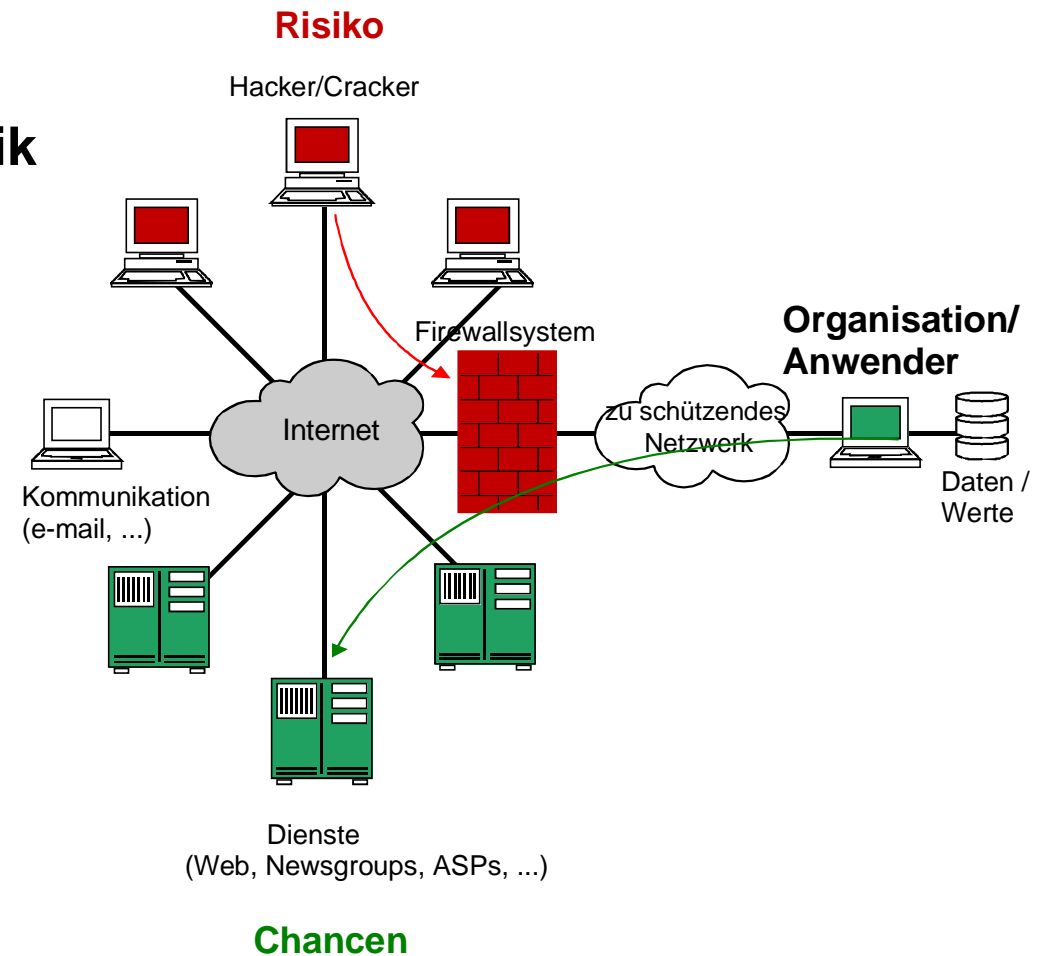
- **Kosten**

- **Umsetzung der Sicherheitspolitik**

- **Sicherheitsinfrastruktur**

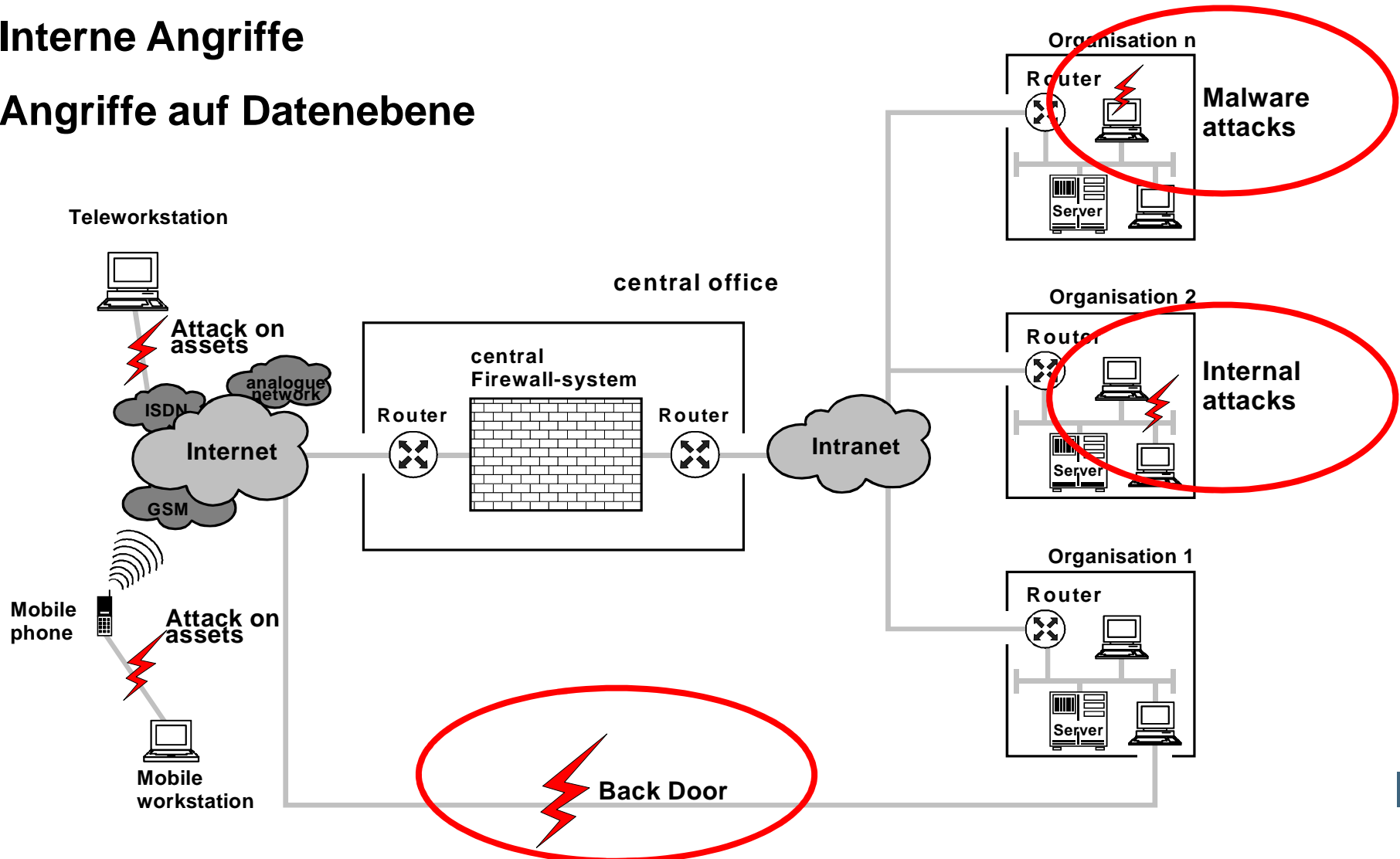
- **Sicherheit durch Abschottung**

- **Überprüfbarkeit**



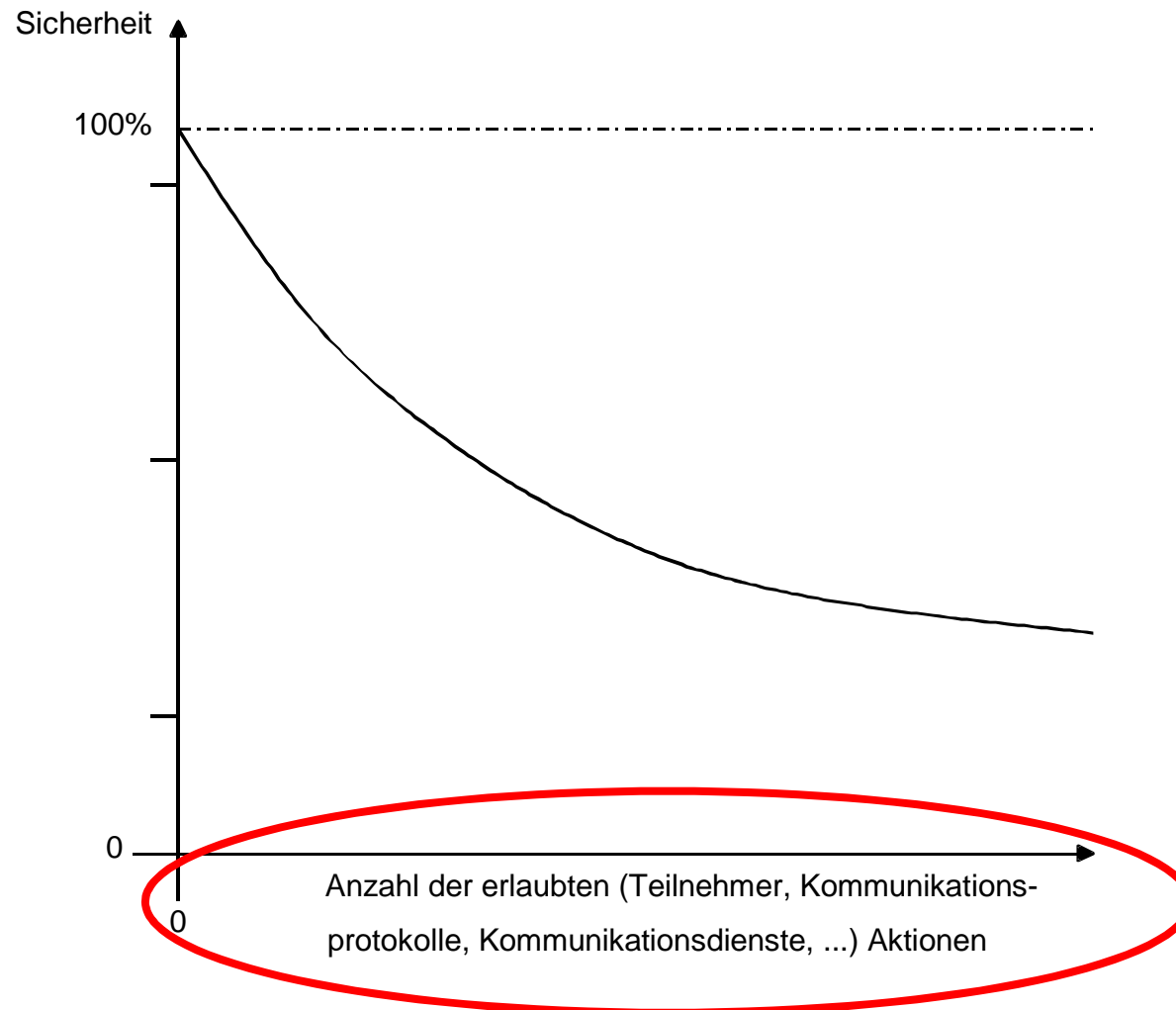
Konzeptionelle Grenzen eines zentralen Firewall-Systems (1/2)

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



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

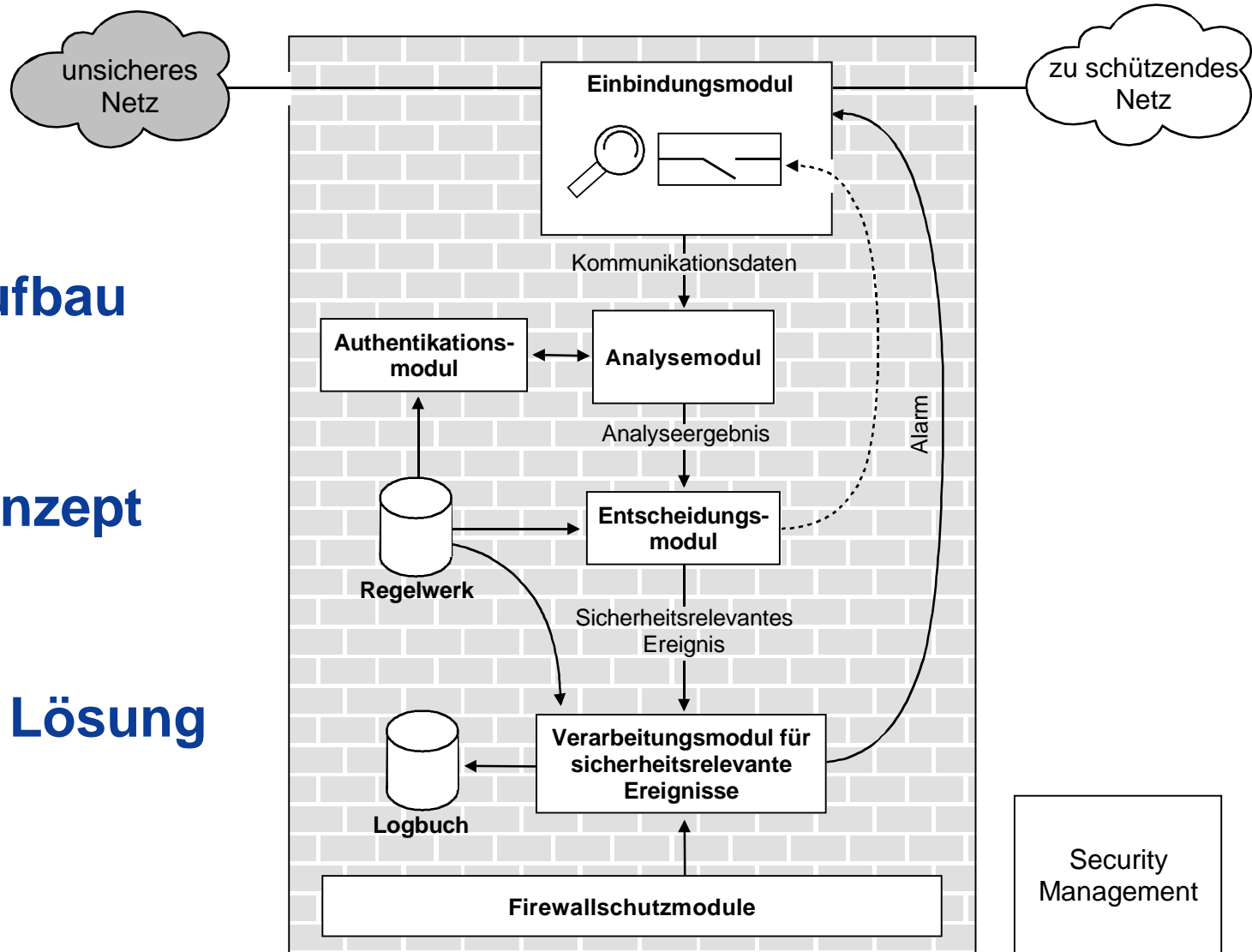
- Security versus connectivity <-> Risiko versus Chance



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

Realisierungskonzepte

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



Systemaufbau

→ Firewallschutzmechanismen

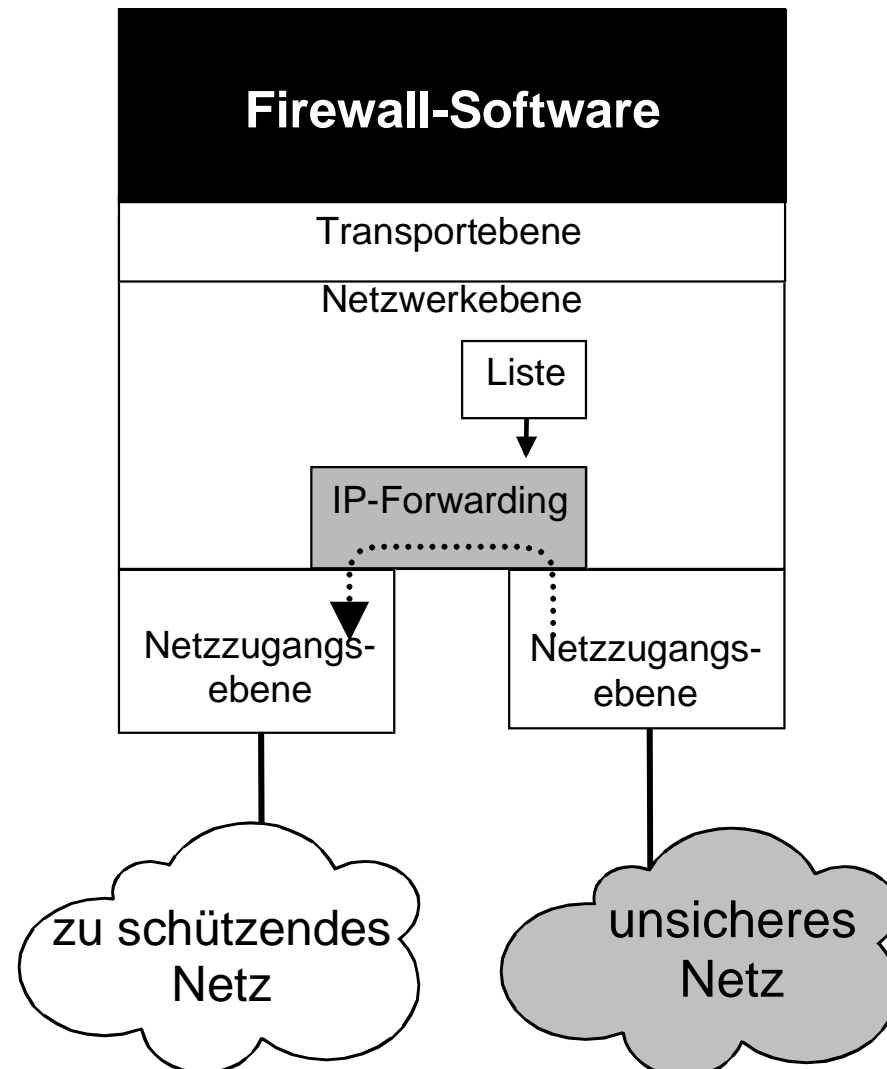
- Ein aktives Firewall-Element muss nicht nur Sicherheitsdienste erbringen, sondern auch selbst gegen Angriffe resistent sein.
 - **Sicheres Betriebssystem**
 - **Integritätstest**
(regelmäßige/spontane Checksummenüberprüfung)
 - Gewährleistung der Softwareintegrität
(Betriebssystem, Firewall-Software)
 - 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 Sicherheitsmechanismen

- 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

- 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!



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Firewall-Systeme

Konzepte - Möglichkeiten und Grenzen - Realisierung

**Vielen Dank für Ihre Aufmerksamkeit
Fragen ?**

Prof. Dr. (TU NN)

Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet-sicherheit.