Kombinationen von VPN- und Firewall-Systemen

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

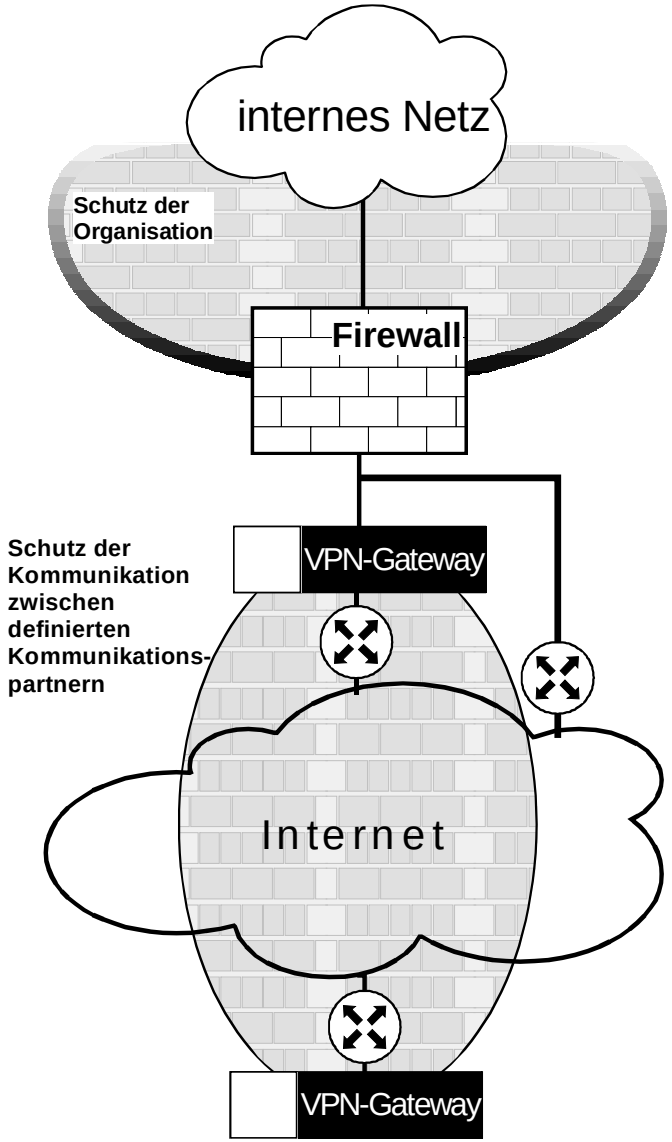
- **Grundsätzliche Unterschiede von VPN- und Firewall-Systemen**
- **Kombinationen von VPN- und Firewall-Systemen**
  - VPN-Systeme vor einem Firewall-System
  - VPN-System vor einem Firewall-System, dahinter ein weiteres VPN-System
  - VPN-System hinter einem Firewall-System
  - VPN- und Firewall-System zusammen realisiert
  - VPN- und Firewall-System parallel
- **Zusammenfassung**

Inhalt

- **Grundsätzliche Unterschiede von VPN- und Firewall-Systemen**
- **Kombinationen von VPN- und Firewall-Systemen**
  - VPN-Systeme vor einem Firewall-System
  - VPN-System vor einem Firewall-System, dahinter ein weiteres VPN-System
  - VPN-System hinter einem Firewall-System
  - VPN- und Firewall-System zusammen realisiert
  - VPN- und Firewall-System parallel
- **Zusammenfassung**

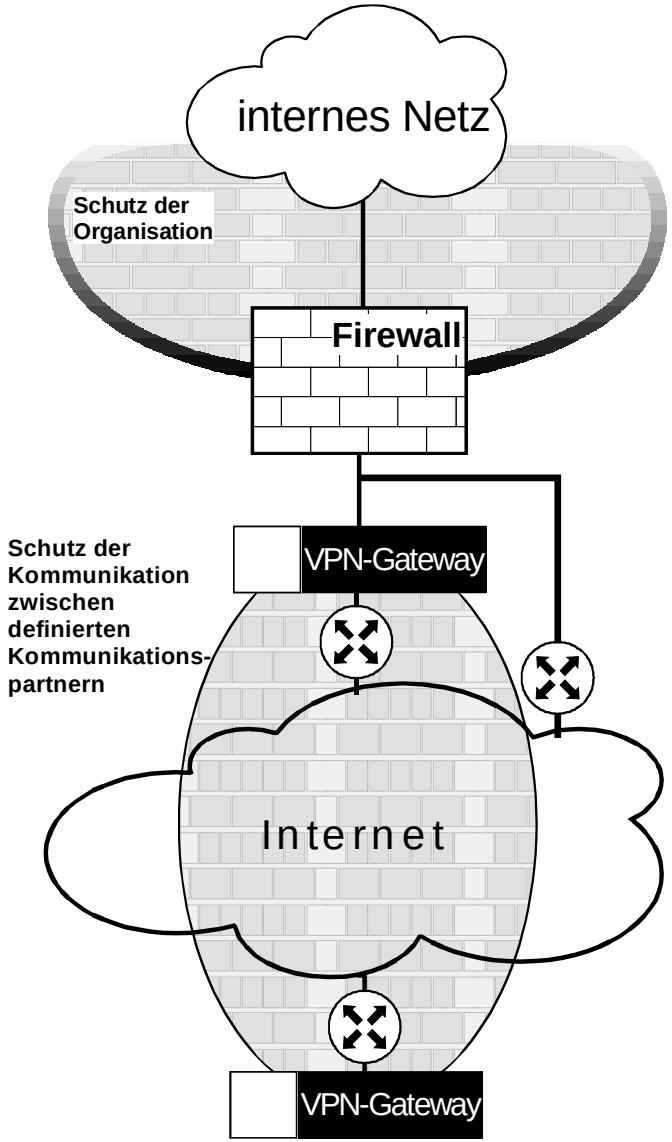
Grundsätzliche Unterschiede von VPN- und Firewall-Systemen (1/3)

- **Geltungsbereich**
  - **Firewall-Systeme**
    schützen eine Organisationseinheit
  - **VPN-Systeme**
    schützen die Kommunikation mehrerer Einheiten (Kommunikationspartner) untereinander



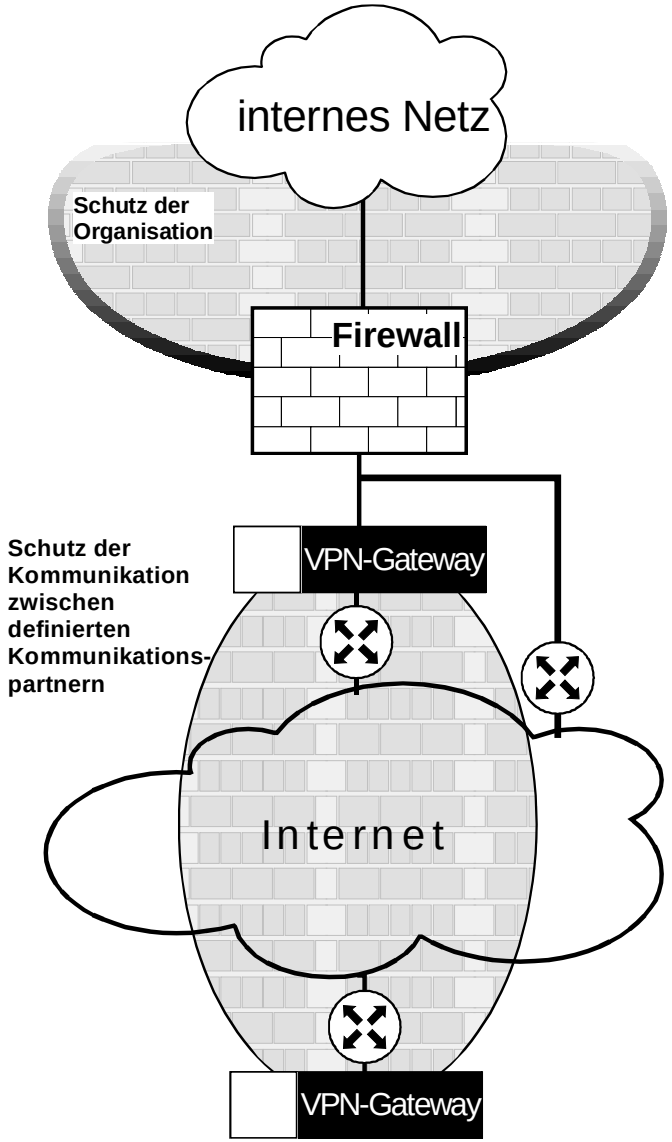
Grundsätzliche Unterschiede von VPN- und Firewall-Systemen (2/3)

- **Ziele**
  - **Firewall-Systeme** schützen vor unerlaubtem Zugriff auf Rechnersysteme und deren Dienste und Daten.
    Hacker, Cracker, Spione und sonstige Angreifer werden aktiv abgehalten und erlaubte Kommunikationsverbindungen werden auf das für die Aufgabenstellung notwendige Maß reduziert.
  - **VPN-Systeme** schützen vor unerlaubten Zugriff auf die Daten während der Übertragung zwischen definierten Kommunikationspartnern.



Grundsätzliche Unterschiede von VPN- und Firewall-Systemen (3/3)

- **Unabhängigkeit**
  - Ein besonderer Aspekt bei **Firewall-Systemen** ist, dass sie lokal verwaltet werden können, das heißt, bezogen auf die Kommunikationsmöglichkeiten und die Protokollierung kann die eigene lokale Sicherheitspolitik unabhängig von anderen realisiert werden.
  - Bei **VPN-Systemen** muss die Sicherheitspolitik in Übereinstimmung mit den Kommunikationspartnern realisiert werden, damit eine einheitliche Sicherheit gewährleistet werden kann.



Inhalt

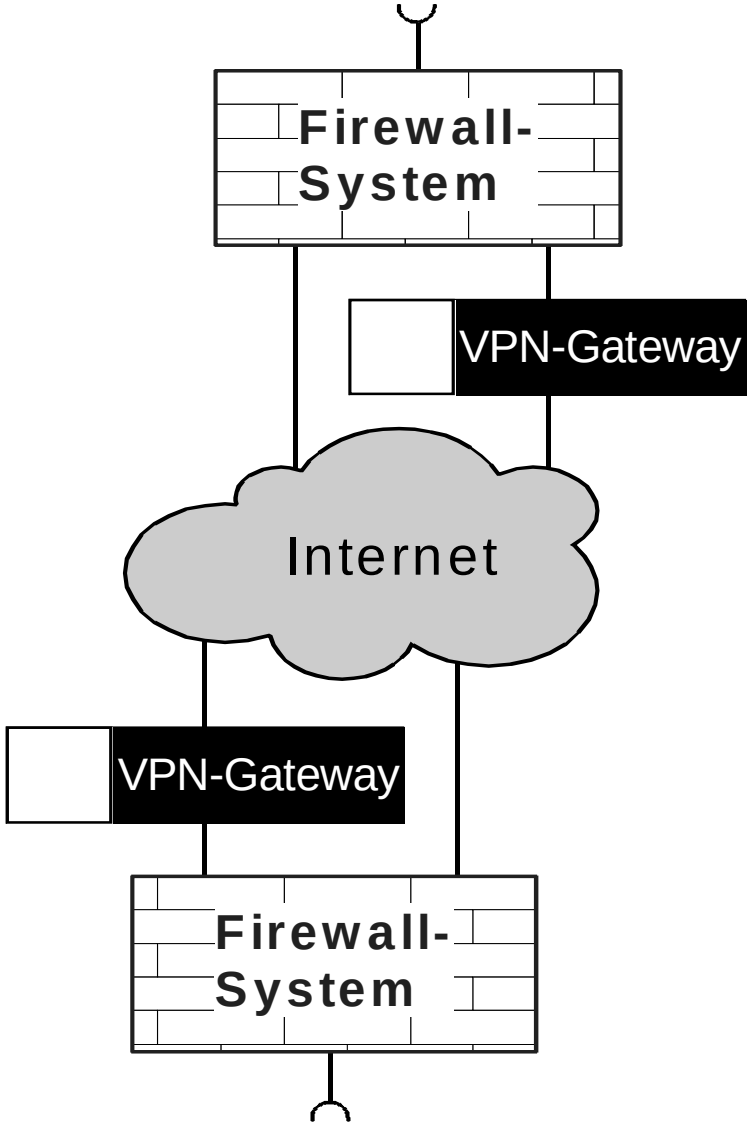
- Grundsätzliche Unterschiede von VPN- und Firewall-Systemen
- **Kombinationen von VPN- und Firewall-Systemen**
  - VPN-Systeme vor einem Firewall-System
  - VPN-System vor einem Firewall-System, dahinter ein weiteres VPN-System
  - VPN-System hinter einem Firewall-System
  - VPN- und Firewall-System zusammen realisiert
  - VPN- und Firewall-System parallel
- Zusammenfassung

Kombinationen von VPN- und Firewall-Systemen

- Es gibt verschiedene Möglichkeiten, VPN- und Firewall-Systeme miteinander zu kombinieren.
- Hier werden die Vor- und Nachteile der unterschiedlichen Kombinationen diskutiert.
- Bei der Beschreibung der verschiedenen Anordnungen wird die Sichtweise »von außen«, d.h. aus dem Internet, zugrunde gelegt.

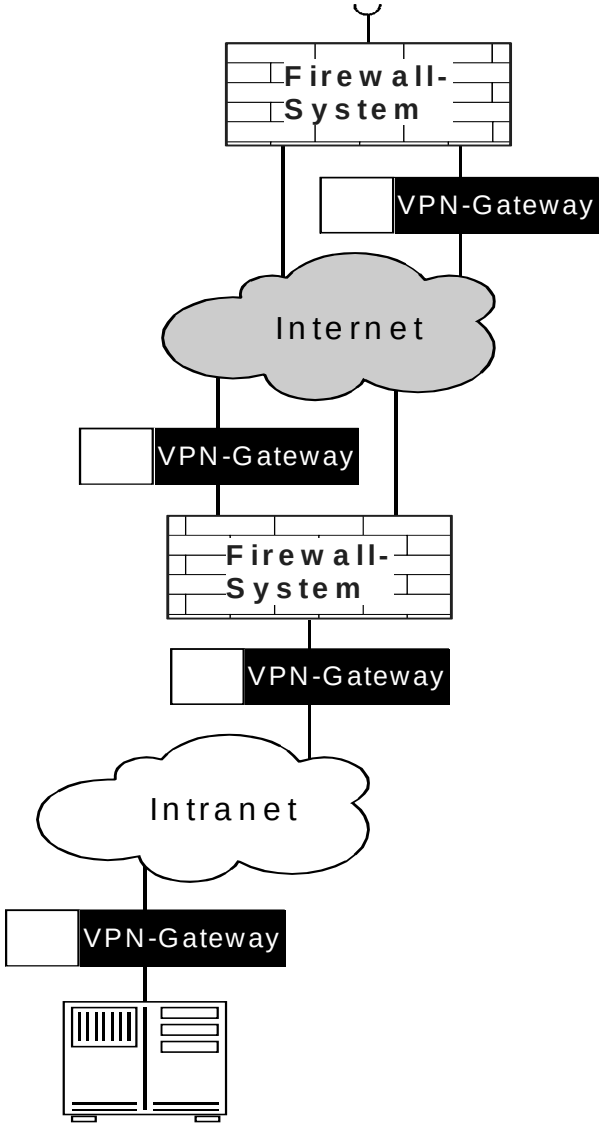
VPN-Systeme vor einem Firewall-System

- **Vorteile**
  - Der gesamte Datenstrom kann vom Firewall-System analysiert und kontrolliert werden, da er im Klartext vorliegt.
  - Die Verwaltung von Firewall- und VPN-System kann getrennt durchgeführt werden.
- **Nachteile**
  - Die Daten liegen im Firewall-System im Klartext vor.
    Dies ist ein Problem, wenn die Verwaltung des Firewall-Systems in der Verantwortung einer Organisation steht, die die Daten nicht lesen soll oder darf.
    Dieser Fall tritt jedoch in der Praxis selten auf.
  - Da Application Gateways nicht jedes Protokoll (z.B. NetBIOS) unterstützen und dies auch nicht sollen, können evtl. nicht alle Kommunikationsverbindungen durch das Firewall-System geführt werden.



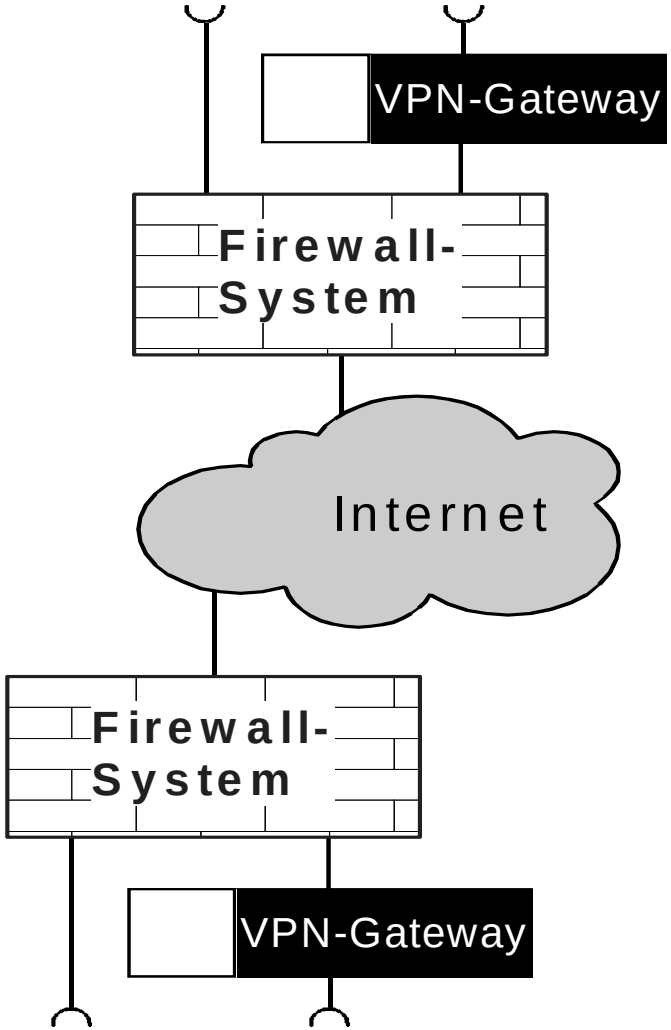
VPN-System vor einem Firewall-System, dahinter ein weiteres VPN-System

- **Vorteile**
  - Es bestehen die gleichen Vorteile wie bei VPN-System von einem Firewall-System beschriebenen Anordnung
  - Die Sicherheitsumgebung ist modular aufgebaut und es können granuläre Regeln verwendet werden.
  - Bei dieser Anordnung kann eine höhere Tiefe der End-to-End-Verschlüsselung erzielt werden.
  - Verschlüsselte Kommunikation kann nur mit Server-Systemen durchgeführt werden, die in den Verbindungsregeln der VPN-Gateways eingetragen sind
- **Nachteile**
  - Es bestehen die gleichen Nachteile wie bei VPN-System vor einem Firewall-System beschriebenen Anordnung.
  - Aufgrund der zusätzlichen Geräte sind die Kosten für Anschaffung und Betrieb hoch.



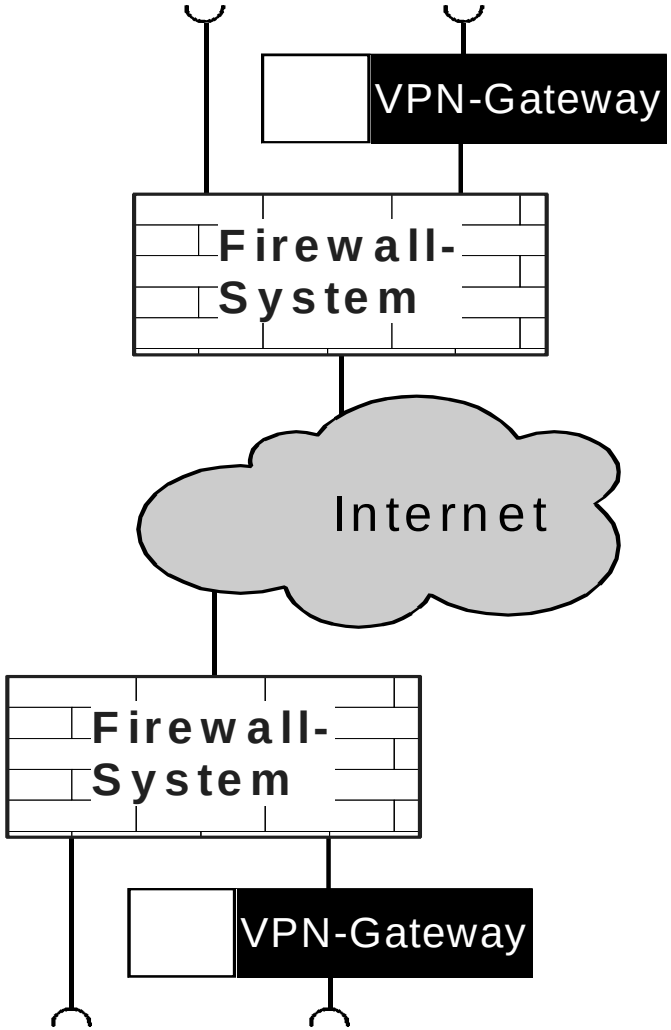
VPN-System hinter einem Firewall-System (1/2)

- **Vorteile**
  - Hierbei wird eine höhere Tiefe der End-to-End-Verschlüsselung erreicht.
  - Die VPN-Gateways können auch außerhalb des Intranet positioniert werden, z.B. vor dem Ziel-System
  - Das VPN-System ist optimal vor Angriffen und Manipulationsversuchen aus dem Internet geschützt.
    Über das Firewall-System können nur die verschlüsselten Dienste (ESP, AH, IKE) auf den VPN-Gateway zugreifen.



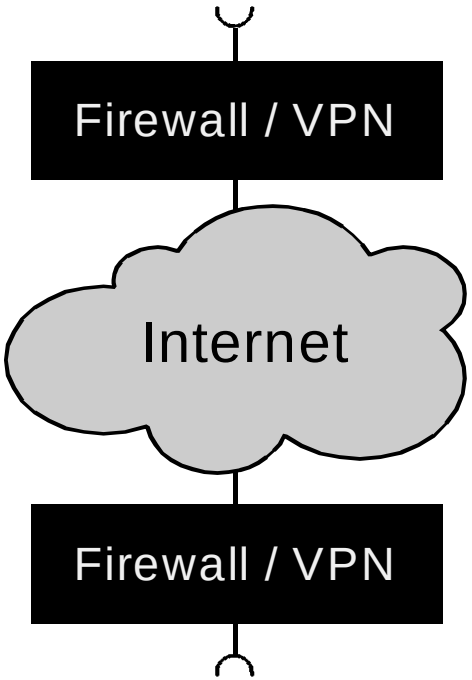
VPN-System hinter einem Firewall-System (2/2)

- **Nachteile**
  - Das Firewall-System ist nicht in der Lage, den verschlüsselten Datenstrom zu analysieren und zu kontrollieren, da die Daten auf der IP-Ebene (IPSec-Tunnel) verschlüsselt sind.
    Dies ist dann ein Problem, wenn über die verschlüsselte Kommunikation ein Angriff durchgeführt wird.
  - Da ein Firewall-System typischerweise eine Adressumwandlung (Network Address Translation, NAT) durchführt, können viele VPN-Gateways nicht verwendet werden, da IPSec die NAT-Funktionalität nicht unterstützt.
    Stattdessen gibt es verschiedene proprietäre NAT-Lösungen (L2TP, NAT traversal u.ä.).



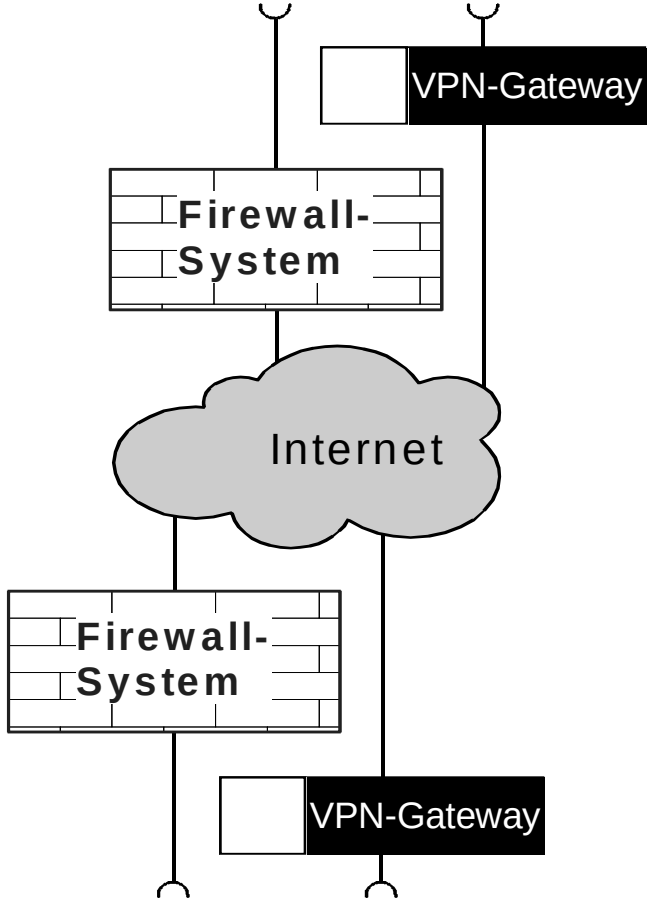
VPN- und Firewall-System zusammen realisiert

- **Vorteile**
  - Typischerweise sind die Kosten geringer
  - Aufgrund der einheitlichen Verwaltung der Firewall- und VPN-Lösung können transparentere Regeln verwendet werden.
- **Nachteile**
  - Falls eine organisationsübergreifende Verschlüsselung notwendig ist, muß eine VPN-Kommunikation auch mit anderen Lösungen realisiert werden.
  - Da der Geltungsbereich und die Ziele von VPN- und Firewall-Systemen unterschiedlich sind, können Konflikte auftreten.



VPN- und Firewall-System parallel

- **Vorteile**
  - VPN- und Firewall-System sind völlig unabhängig voneinander.
- **Nachteile**
  - Die verschlüsselte Kommunikation wird in dieser Kombination nicht analysiert und kontrolliert, da in diesen Kommunikationsweg kein Firewall-System eingebunden ist.
  - Die Sicherheit gegen Angriffe aus dem Internet hängt von der Sicherheit des VPN-Gateways ab.



Inhalt

- **Grundsätzliche Unterschiede von VPN- und Firewall-Systemen**
- **Kombinationen von VPN- und Firewall-Systemen**
  - VPN-Systeme vor einem Firewall-System
  - VPN-System vor einem Firewall-System, dahinter ein weiteres VPN-System
  - VPN-System hinter einem Firewall-System
  - VPN- und Firewall-System zusammen realisiert
  - VPN- und Firewall-System parallel
- **Zusammenfassung**

Zusammenfassung
→ VPN- und Firewall-Systemen

- VPN- und Firewall-Systeme haben unterschiedliche Ziele und Geltungsbereiche.
- Die Kombination von VPN- und Firewall-Systeme ist sinnvoll und notwendig.
- Wie VPN- und Firewall-Systeme miteinander kombiniert werden sollen, hängt von den Randbedinungen ab und muss individuell entschieden werden.

Kombinationen von VPN- und Firewall-Systemen

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen