Firewallsysteme, ein Einführung

Thomas J. Wilke

Vortrag zum Administrator-Workshop an der TU Berlin

Berlin, den 10.04.2002

Gliederung

- Motivation zum Einsatz von Firewallsystemen
- Funktionsverfahren von Firewallsystemen
- Firewallsystemkonfigurationen
- Resümee

Motivation zum Einsatz von Firewall-systemen: Zielsetzungen

Absicherung der Kommunikationsvorgängen zwischen Intranet & Internet

- Durchsetzung einer Sicherheitspolitik
- Kontrolle auf Netzwerkebene
- Kontrolle auf Benutzerebene
- Kontrolle auf Datenebene
- Kontrolle auf der Anwendungsebene
- Rechteverwaltung
- Entkoppelung von Diensten
- Erkennung und Behandlung von illegitimen Vorgängen
- Verbergen der internen Netzstruktur
- Wahrung der Vertraulichkeit von Nachrichten

Motivation zum Einsatz von Firewall-systemen: Unzulänglichkeiten

Offene Standards

- Netzwerkprotokolle
- Dienstvielfalt
- Systemvielfalt

Funktionskomplexität

- Hohe Funktionskonzentration auf Server- und Clientsystemen
- Funktionsintegration

Fehlfunktion

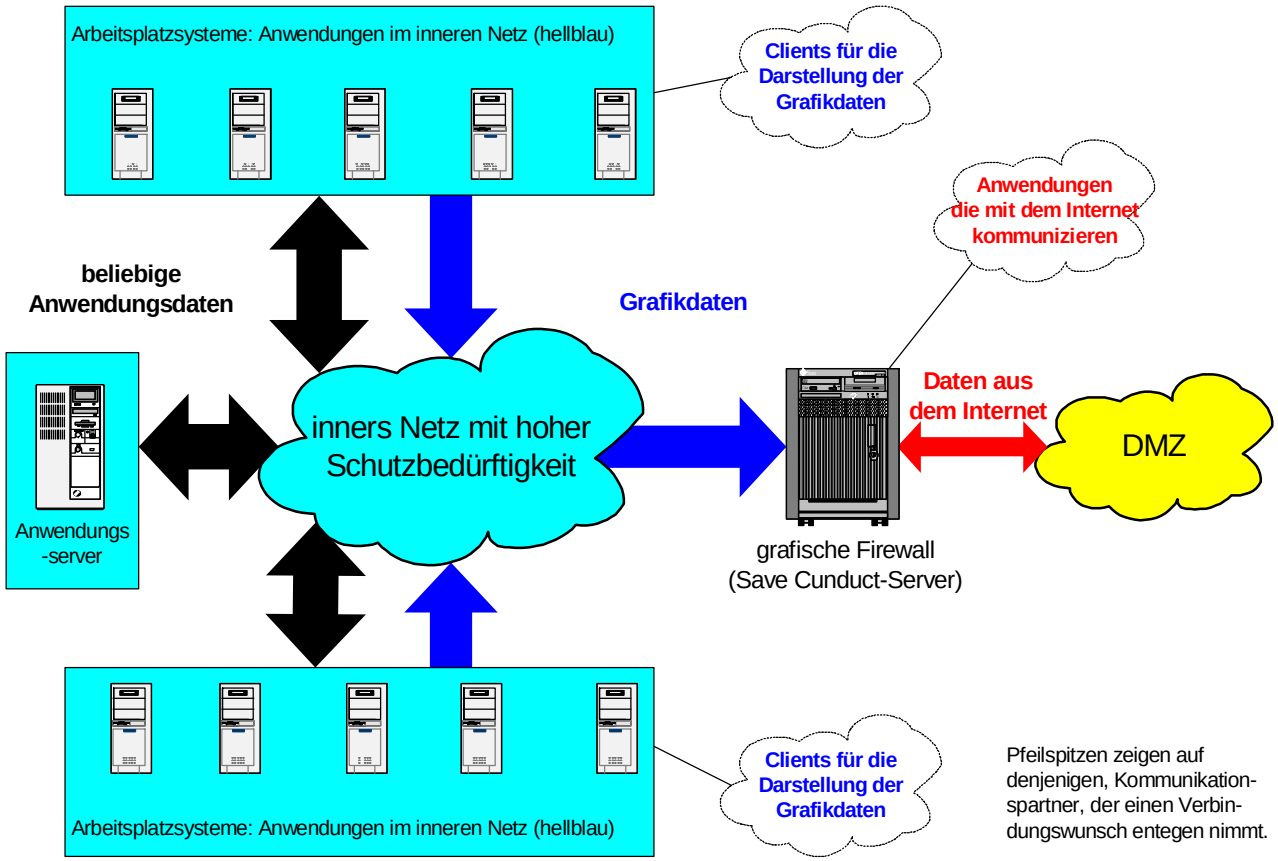
- Falsche Bedienung
- Fehlerhafte Herstellung
- Unzureichendes Wirkprinzip oder Konstruktion

Motivation zum Einsatz von Firewall-systemen: abzuwehrende Gefährdungen

- Funktionsbeeinträchtigung der Netzwerkfunktion des Intranetzes
- Illegitime Nutzung von Diensten
- Illegitime Funktionsausführung auf Netzknoten
- Funktionseinschränkung von Netzknoten
- Illegitimer Zugriff auf Daten
- Kombination aus den vorbenannten Gefährdungen

Funktionsverfahren von Firewall-systemen: Trennung von Datenströmen

Strikte Trennung der Datenströme: „datentechnische galvanische Trennung“.



Funktionsverfahren von Firewall-systemen: Filterung von Datenströmen

Daten aus dem Internet können ins Internet gelangen und umgekehrt.

- Datenfilterung auf Netzwerkebene:
  statisch , dynamisch
- Datenfilterung auf Anwendungsebene:
  dienstorientierte, transparent, socks, circuit-level, socks,
- Zustandsorientierte Paketfilter:
  Kombination aus Datenfilterung auf Anwendungs- und Netzwerkebene

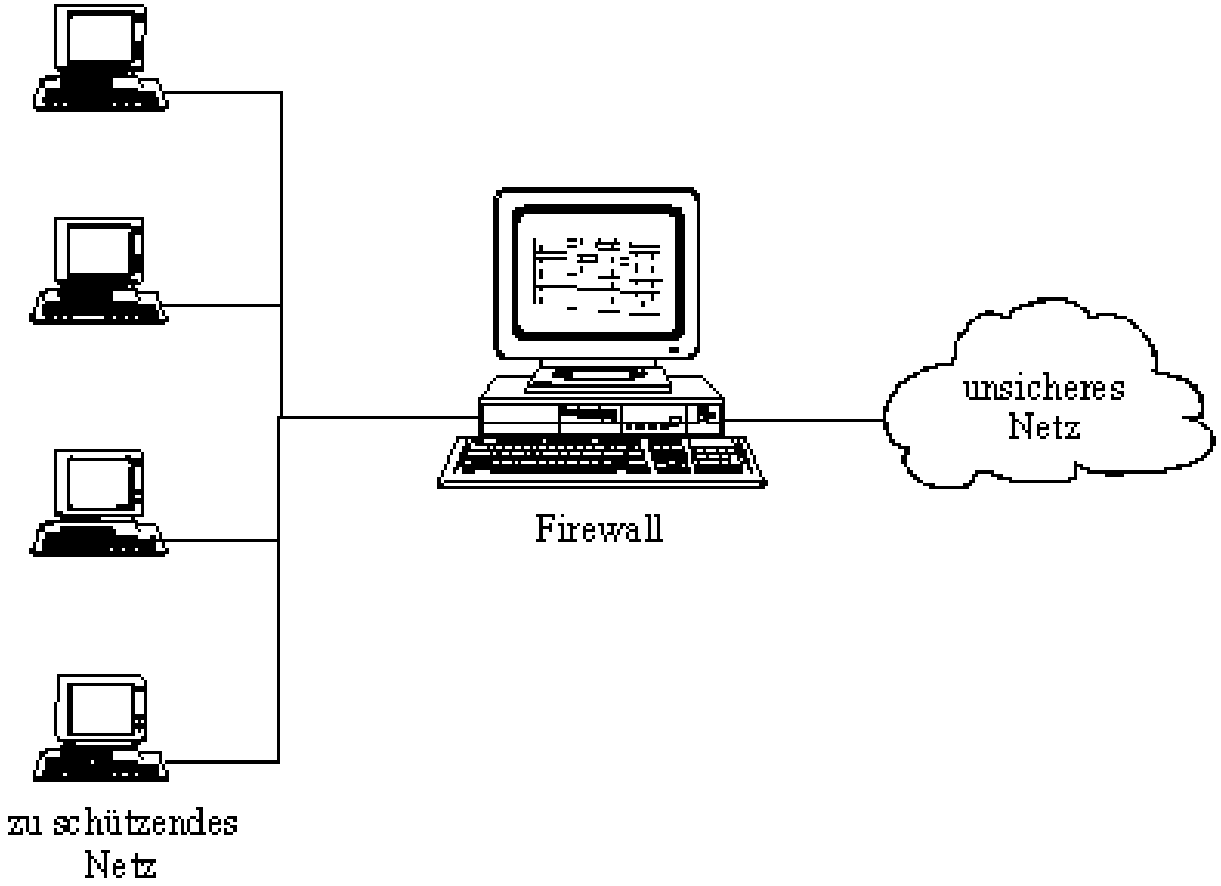
Funktionsverfahren von Firewall-systemen: Schleusenverfahren

Neues Verfahren, das keinen direkten Datenverkehr zwischen den Netzen zuläst.

Im Unterschied zu Firewalls trennt das Lock-Keeper-System das Netzwerk physisch vom Internet ab; erst wenn diese Schleuse offen steht, können Datenpakete wieder passieren. Je nach Zustand der "Tore" findet der Informationsaustausch zunächst nur mit einem Intranet-Rechner statt. Während des Aufenthalts in der Schleuse können die Daten je nach Sicherheitserfordernissen der Firma überprüft werden

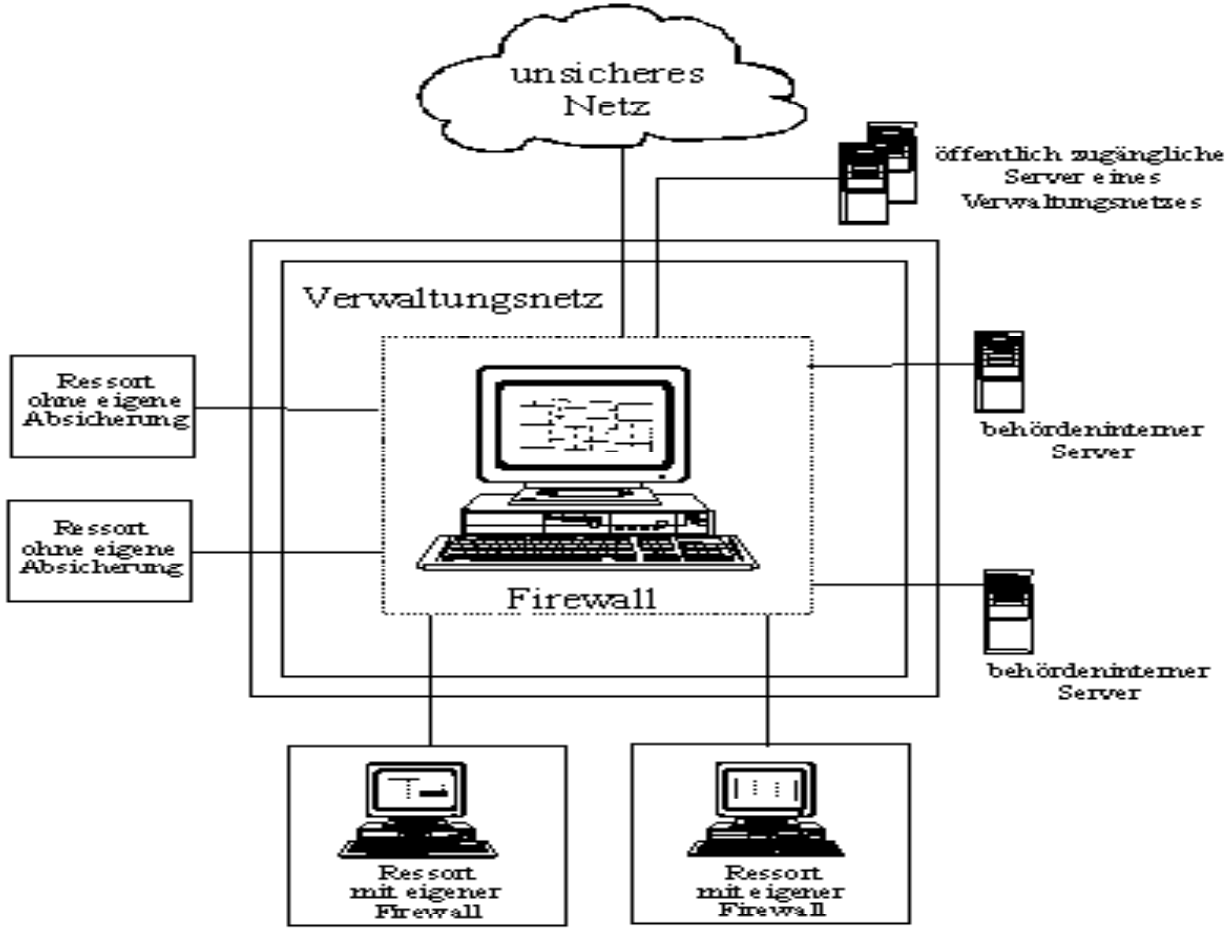
Firewallsystemkonfigurationen:

zentrale Firewall



Firewallsystemkonfigurationen:

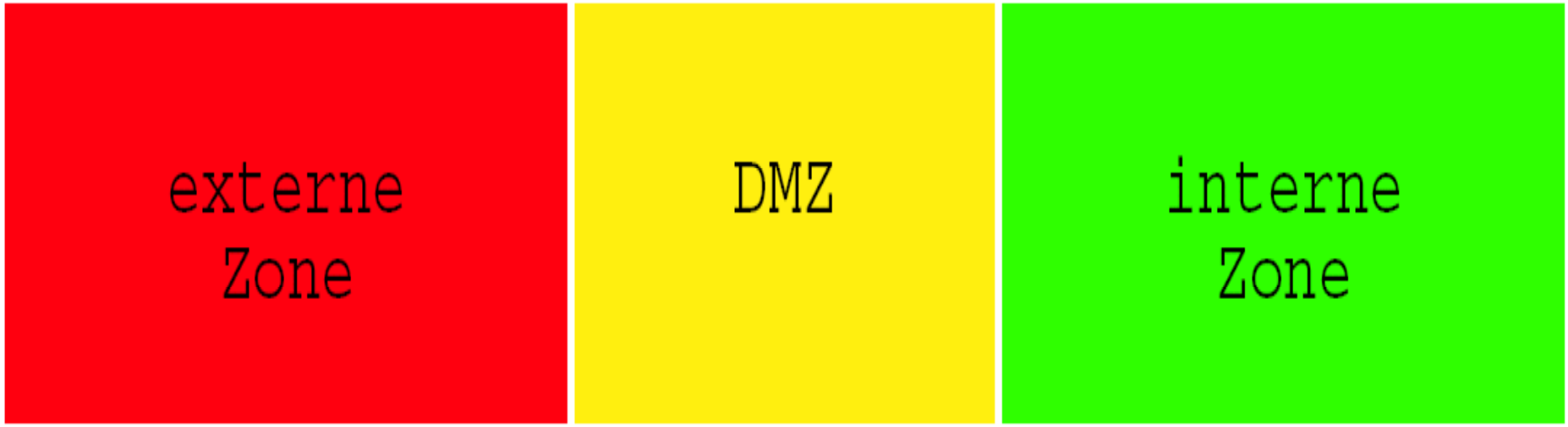
gestaffelte Firewall



Firewallsystemkonfigurationen:

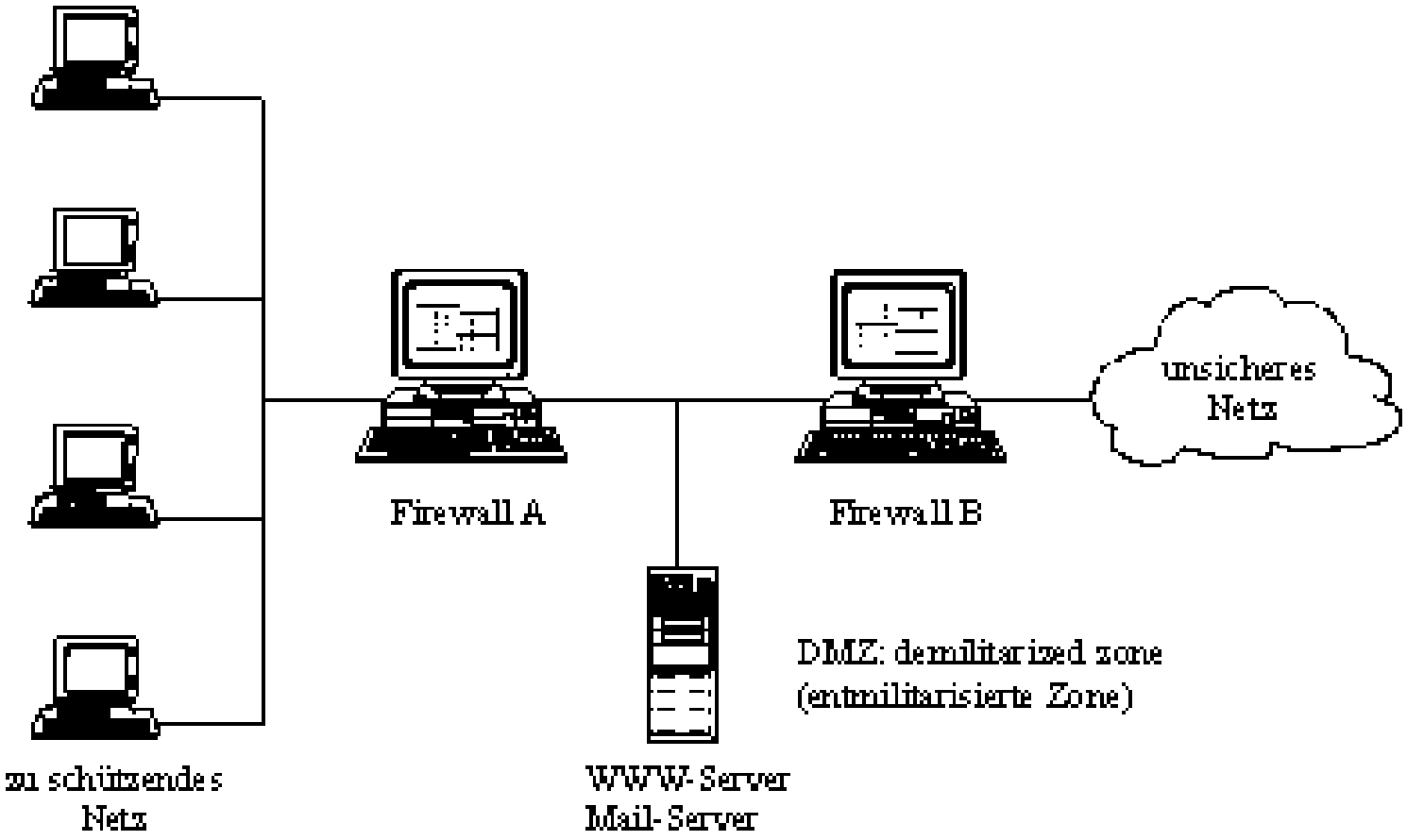
Zonen und sicherheitstechnische Taxonomie

Allgemein unterscheidet man die externe Zone, die DMZ und die interne Zone.



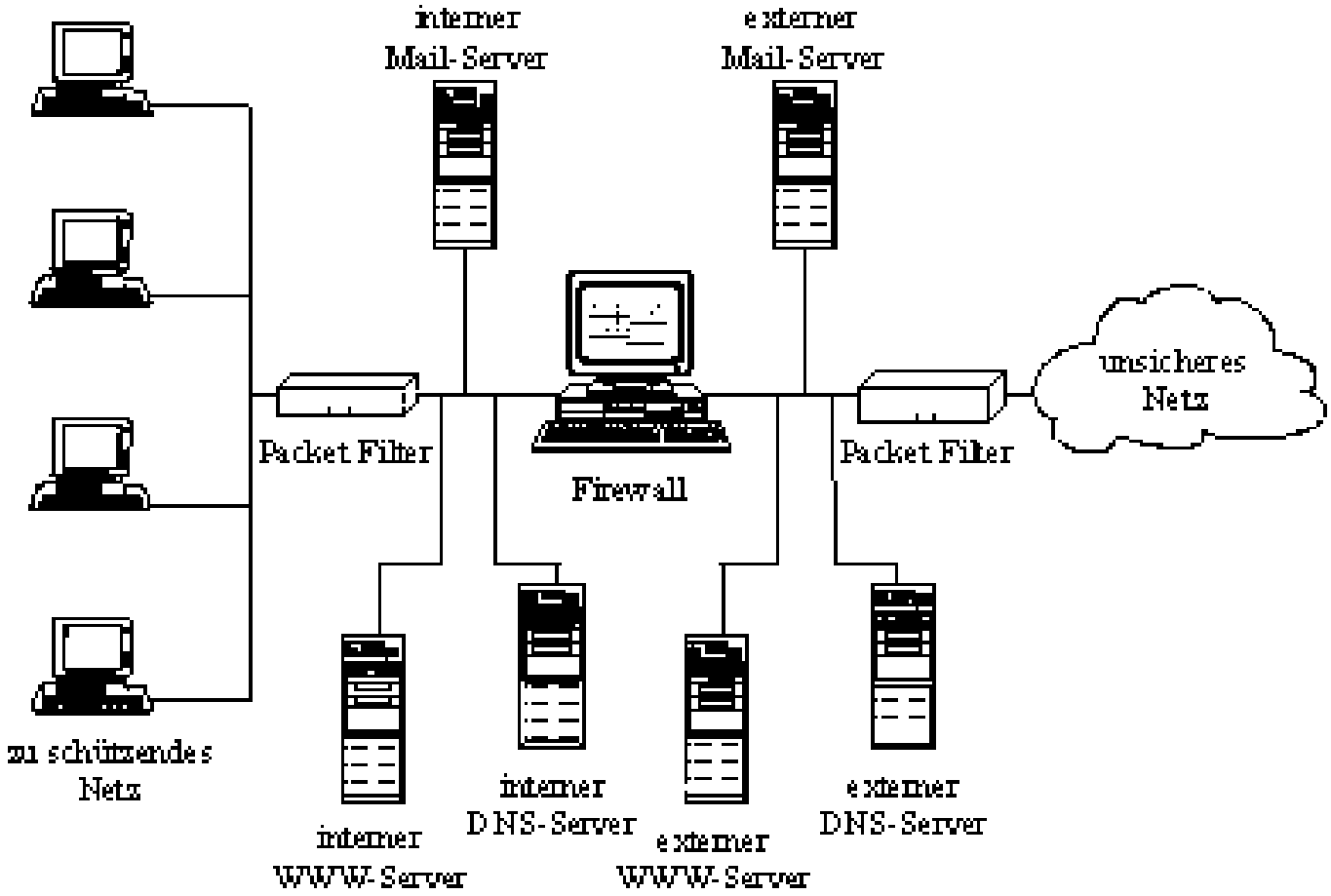
Firewallsystemkonfigurationen:

kaskadierte Firewall



Firewallsystemkonfigurationen:

screened Gateway



Resümee

- Firewallsysteme sind dafür konstruiert Intranetze vor Einflüssen aus offenen Netzen zu schützen.
- Die Aufrechterhaltung der Qualität des Schutzes einer Firewall hängt wesentlich von deren regelmäßigen Wartung und Überwachung ab.
- Firewallsysteme können keinen absoluten Schutz bieten:
  - Schutzniveau ist nur für bekannte Angriffsverfahren bei entsprechender Wartung hoch.
  - Firewallsysteme können Implementierungs- oder Archtekturelle aufweisen.

Weiter Informationen

Ansprechpartner / Vortrag

Ansprechpartner: Thomas J. Wilke

tub@tjw.li

Vortrag: http://ws.tjw.li/tjw/activities/teaching/lectures/FWS_Einf.pdf