15. Firewalls unter UNIX

15. Firewall

Gliederung

- **Grundlagen**
- Linux – iptables
- OpenBSD, FreeBSD – PF Toolkit
- BSD, Solaris - IPF Toolkit
- Löcher in Firewalls – Virtuelle private Netzwerke

15. Firewall - Grundlagen

Allgemeines(1)

Was ist ein Firewall?

Anordnung von Hard- und Software, die als alleinige Verbindung zwischen einem zu schützenden Netz (Intranet) und einem unsicheren Netz (Internet) dient.

Aufgabe eines Firewalls ist es (aus Nutzersicht):

- Unbefugte daran zu hindern Informationen aus dem zu schützenden Netz abzurufen.
- Unbefugte daran zu hindern Aktionen auszulösen und Programme auf Rechnern des zu schützenden Netzes zu starten.
- Unbefugte daran zu hindern Ressourcen des zu schützenden Netzes in irgend einer Art und Weise zu nutzen.

15. Firewall - Grundlagen

Allgemeines(2)

Aufgaben von Firewalls (intern)

- Zugangskontrolle auf der Basis von IP-Adressen
- Zugangskontrolle auf der Basis von Applikationen (proxy)
- Überprüfen der Datenströme (Viren)
- Verbergen der Struktur des zu schützenden Netzes
- Zugangskontrolle auf der Basis von Nutzern
- Verwaltung von Zugriffsrechten
- Logging und Beweissicherung
- Alarmierung bei ungewöhnlichem Netzverkehr

15. Firewall - Grundlagen

Allgemeines(3)

Sicherheitsregeln für einen Firewall (Security Policy)

- Welcher Rechner und welcher Nutzer des zu sichernden Netzes darf welchen Rechner und welchen Dienst des unsicheren Netzes benutzen?
- Welche Dienste im zu sichernden Netz müssen wie geschützt werden (lesen, schreiben)?
- Welcher Funktionsumfang der Dienste wird eingeschränkt.
- Welche Datenströme sollen gefiltert werden (Viren)
- Welche Ereignisse und Informationen sollen wo und wie protokolliert werden? (Datenschutz!?)
- Wer erhält Information über Ereignisse und wer wertet wann die Protokolle aus (Datenschutz!?)

15. Firewall - Grundlagen

Allgemeines(4)

Organisatorische Fragen

- Welche Risiken bestehen bei ordnungsgemäßen Betrieb des Firewall trotzdem? Welche prinzipiellen Löcher gibt es?
- Welcher Schaden kann in dem zu schützenden Netz auftreten, falls der Firewall versagen sollte (Einbruch durch den Firewall)? Entstehende Kosten? Ausfallzeiten?
- Wann und wie wird der Einbruch/Angriff entdeckt?
- Was ist bei einem entdeckten Einbruch/Angriff zu tun?
- Welche Protokolle und andere Informationen müssen für die Beweissicherung wo gespeichert werden?

15. Firewall - Grundlagen

Allgemeines(5)

Arten von Firewalls

- Paket Filter
- Circuit Level Filter
- Applikation Level Filter (Proxy)
- Dynamic Paket Filter (Stateful Paket Filter)
- Stealth Firewalls (IP-less Firewalls)
- Personal Firewalls
- Hybride Filterarchitekturen
- verteilte Firewalls

15. Firewall - Grundlagen

Allgemeines(6)

Paket Filter

- Der Filter benutzt Protokollinformationen aus den Schichten 2 und 3 zum Filtern von Paketen (Absenderadressen, Empfängeradressen, Protokolltypen, Portnummern)
- Filterung erfolgt auf Paketebene
- Durchsatz: hoch
- Sicherheit: mäßig
- Beispiele: Standardrouter (Access- und Deny-Listen), Linux-Firewall mit iptables, Solaris mit ipf

15. Firewall - Grundlagen

Allgemeines(8)

Circuit Level Filter

- Relais für TCP-Verbindungen!!!
- keine Überprüfung der Protokolle der Applikationsschicht
- Übersetzung aller TCP/IP-Pakete vor Weiterleitung
- Wird benutzt für TCP-Applikationen, für die kein Applikation-Level Filter vorhanden ist.
- Durchsatz: niedrig
- Sicherheit: hoch
- Beispiel: SOCKS

15. Firewall - Grundlagen

Allgemeines(7)

Applikation-Level Filter (Proxy)

- Filter, die die in der Anwendungsschicht vorhandenen Protokollinformationen nutzt (z.B. http).
- Der Filter stellt sich gegenüber dem Clienten als Server dar und gegenüber dem Server als Client dar.
- Für jedes zu filternde Protokoll ist ein separater Filterprozess notwendig.
- Bietet häufig weitere Zusatzfunktionen wie Caching oder Adressumsetzung zur Verschleierung der internen Netzstruktur an
- Durchsatz: niedrig
- Sicherheit: hoch
- Beispiele: Squid

15. Firewall - Grundlagen

Allgemeines(9)

Dynamic Paket Filter (Stateful Paket Filter)

- Filter, die zusätzlich zu den Informationen, die ein Paket Filter benutzt, auch noch Informationen über den Zustand einer Verbindung nutzten.
- komplexere Regeln möglich
- kombinierbar mit Adressumsetzung zur Verdeckung der internen Netzwerkstruktur
- Durchsatz: hoch
- Sicherheit: mittel, voll transparent
- Beispiele: PIX (Cisco), Linux Firewall mit iptables, Solaris ipf

15. Firewall - Grundlagen

Allgemeines(10)

Stealth(IP-less Filter)

- benutzt mehrere Interfaces und arbeitet als Bridge (Layer-2-Switch). Besitzt keine IP-Adresse.
- Schwer zu lokalisieren und anzugreifen.
- Überprüft sowohl auf Paketebene als auch auf Applikationsebene. Erzeugt keine typischen Filteraktionen z.B. keine Verringerung des TTL. Mit Ping nicht lokalisierbar.
- Kompliziert zu konfigurieren und zu warten. Kommerzielles Produkt.
- Durchsatz: mittel
- Sicherheit: hoch
- Beispiele: SunScreen, Linux iptables

15. Firewall - Grundlagen

Allgemeines(11)

Personal Firewalls

- schützt nur einen Rechner, kein Netzwerk
- verschiedene Filtertechniken einsetzbar
- Durchsatz: mittel
- Sicherheit: mittel, niedrig
- Beispiel: Solaris ipf, Linux iptables

Hybride Filterarchitekturen

- Kombination von Firewalls verschiedener Architekturen (Pakaetfilter, Applikation-Filter,...)

15. Firewall - Grundlagen

Allgemeines(12)

Verteilte Firewalls

- Einsatz von verschiedenen oder gleichartigen Firewalls auf verschiedenen Rechnern. Die Pakete müssen mehrere Firewalls durchlaufen um an das Ziel zu gelangen.
- Durchsatz: gering
- Sicherheit: sehr hoch
- Es können verschiedene Firewallprodukte zum Einsatz kommen.

15. Firewall - Grundlagen

Paketfilter (1)

Anforderungen:

- Filterung muss getrennt für jedes Interfaces möglich sein. Eingehende und ausgehende Interfaces müssen unterschiedlich behandelt werden können.
- Filterung von ICMP-Paketen muss meldungsspezifisch gefiltert werden können.
- Filterung muss getrennt nach Quell- und Zieladresse erfolgen können (netzwerk- und hostspezifisch).
- Filterung muss getrennt nach Quell- und Zielport erfolgen (applikationsspezifisch).
- Reihenfolge der Filterregeln muss vom Filter berücksichtigt werden, um bei der Konfiguration Optimierungen festlegen zu können.
- Bei TCP Unterscheidung von Verbindungsaufbau und Verbindungsbenutzung unterscheiden
- Source Routing muss unterbunden werden.
- Internes und externes Logging muss möglich sein.

15. Firewall - Grundlagen

Paketfilter(2)

Eigenschaften von Paketfilter

- kostengünstig realisierbar
- leicht verwaltbar (auch für neue Dienste)
- komplexe Filterregeln aufstellbar, dadurch leicht falsch konfigurierbar
- die erlaubten Dienste auf den Zielrechnern im Intranet müssen selbst sicher sein (100%ig).
- bedingt durch den erreichbaren geringen Schutz nur begrenzt einsetzbar.
- sinnvoll einsetzbar für besonders zu schützende Netze innerhalb eines Intranetzes

15. Firewall - Grundlagen

Paketfilter(3)

Beispiele für Filterregeln für eingehenden Verkehr

- verwerfen aller Pakete mit Source Routing (spoofing)
- verwerfen aller Pakete mit direktem Broadcast (smurf)
- verwerfen aller Pakete mit Sourceadressen aus dem Intranet oder anderen privaten Netzen
- erlauben aller Pakete für bereits erlaubte Verbindungen
- verbieten aller TCP-Verbindungen außer zu bewusst erlaubten Ports, z.B. http, smtp,...
- verbieten aller UDP-Pakete außer zu bewusst erlaubten Ports, z.B. dns
- verwerfen aller ICMP-Pakete außer für die Typen 0,3,11
- Fragmentierung erlauben

15. Firewall - Grundlagen

Paketfilter(4)

Beispiele für Filterregeln für ausgehenden Verkehr

- Verwerfen aller Pakete bei denen die Quelladresse nicht aus dem Bereich des Intranetzes kommt
- Verwerfen aller Pakete, die nicht an gewünschte Zielports gehen. Gewünschte Zielports sind z.B. smtp, www, ftp, ...
- Verwerfen aller UDP-Pakete, außer an den DNS-Port eines Hosts im Internet
- Verwerfen aller ICMP-Pakete außer vom Type 3, 8, 11

15. Firewall - Grundlagen

Applikation Firewall(1)

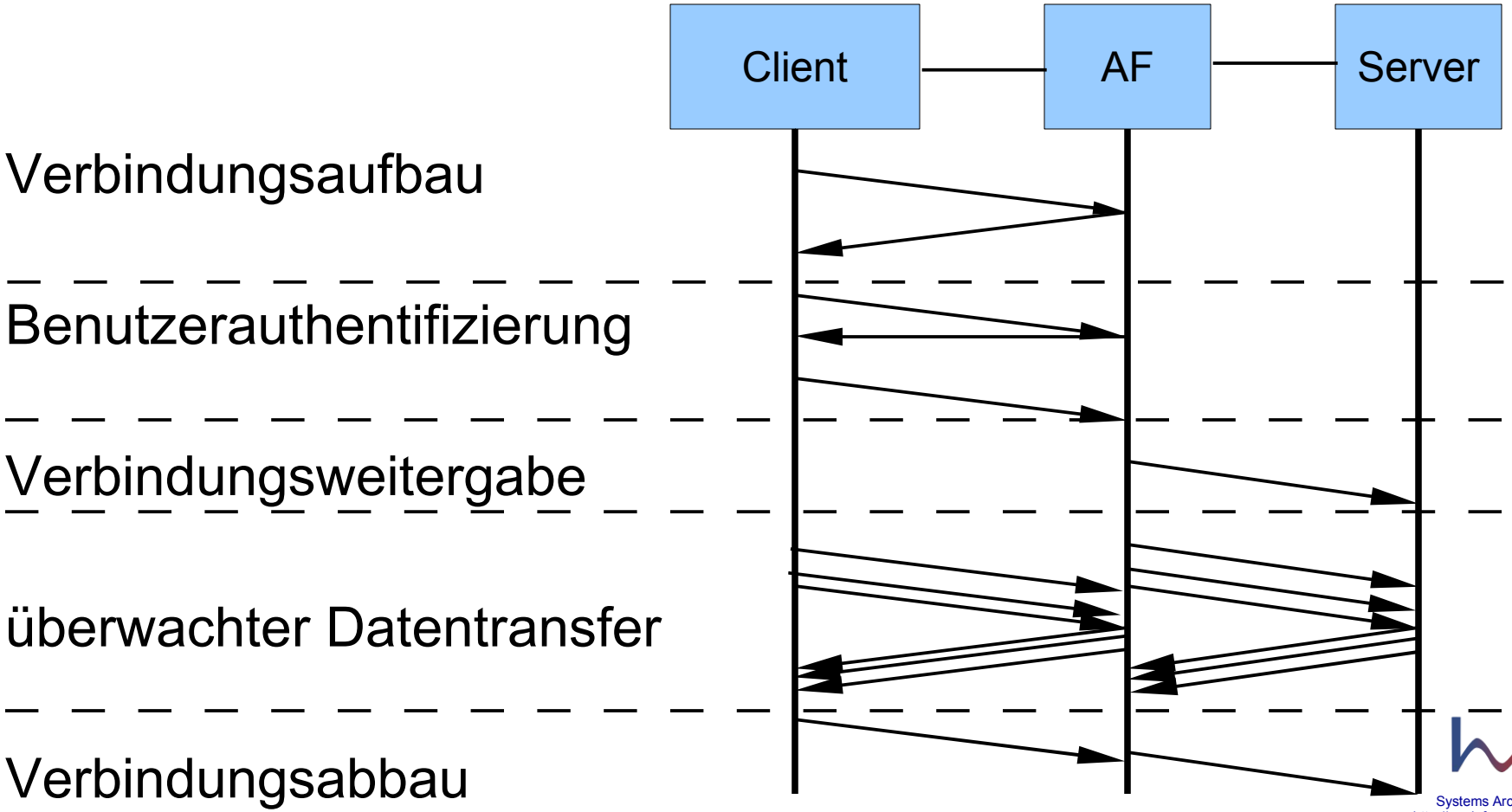
Anforderungen

- Filterregeln müssen benutzerspezifisch formulierbar sein.
- Filterregeln müssen für Benutzergruppen formulierbar sein.
- Anwendungsspezifische Einschränkungen müssen möglich sein. z.B.
  - gewisse ftp- und smtp-Kommandos müssen verbietbar sein.
  - gewisse ftp-Kommandos müssen an Benutzerrechte gebunden sein (Zugriffsrechte zu Dateien)
  - bestimmte http-Methoden müssen einschränkbar sein
- Filterung der Datenpakete muß mögliche sein (Viren und Würmer)
- Prinzipiell verboten: RPC, X11, NFS, NIS, TFTP, R-Utilities
- Logs sollten an externe Hosts gesendet werden können.
- Starke Authentisierung für Benutzer muss möglich sein.
- Verschlüsselung muss möglich sein.

15. Firewall - Grundlagen

Applikation Firewall(2)

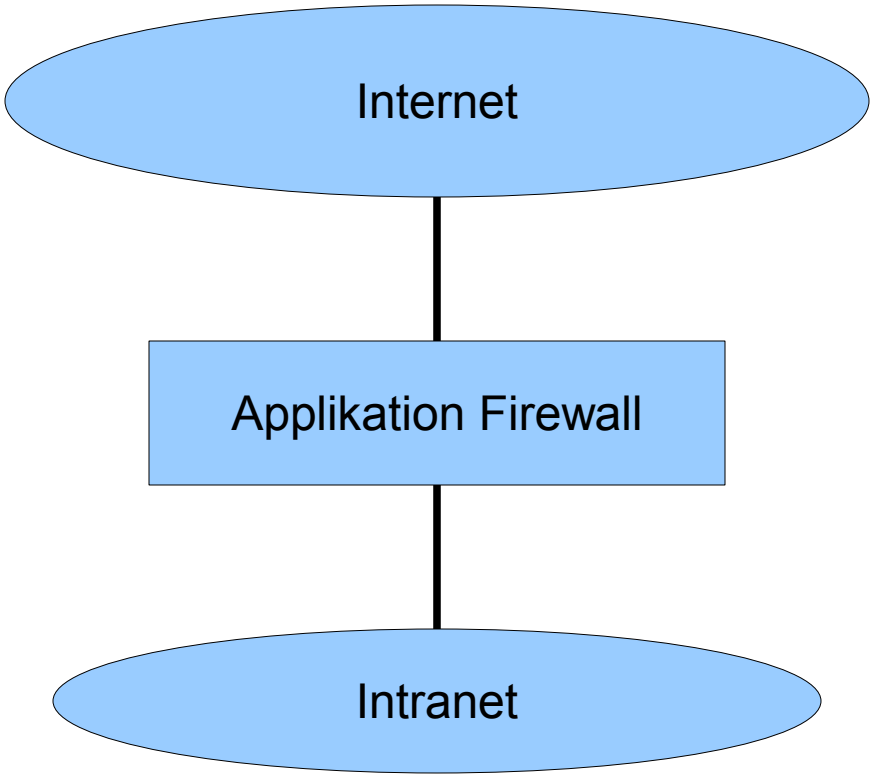
Prinzipielle Funktion



15. Firewall - Grundlagen

Applikation Firewall(3)

dual-homed Applikation Firewall(1)



15. Firewall - Grundlagen

Applikation Firewall(4)

dual-homed Applikation Firewall(2)

- verdeckt die Strukturen des Intranetzes
- jedes Paket durchläuft den Proxy (IP-Forwarding muss auf dem Firewall ausgeschaltet sein)
- starke Sicherheitsfunktionen machbar
- applikationsspezifische Fehler lassen sich auf dem Proxy behandeln
- kryptografische Funktionen lassen sich gut einbinden
- Login-Funktionen lassen sich gut einbinden
- erfordert einen höheren Aufwand (Kosten) als Paketfilter
- keine Transparenz auf der Netzwerkebene und Transportebene
- ein neuer Dienst erfordert einen neuen Proxy-Server

15. Firewall - Grundlagen

Kombinationen von Firewalls(1)

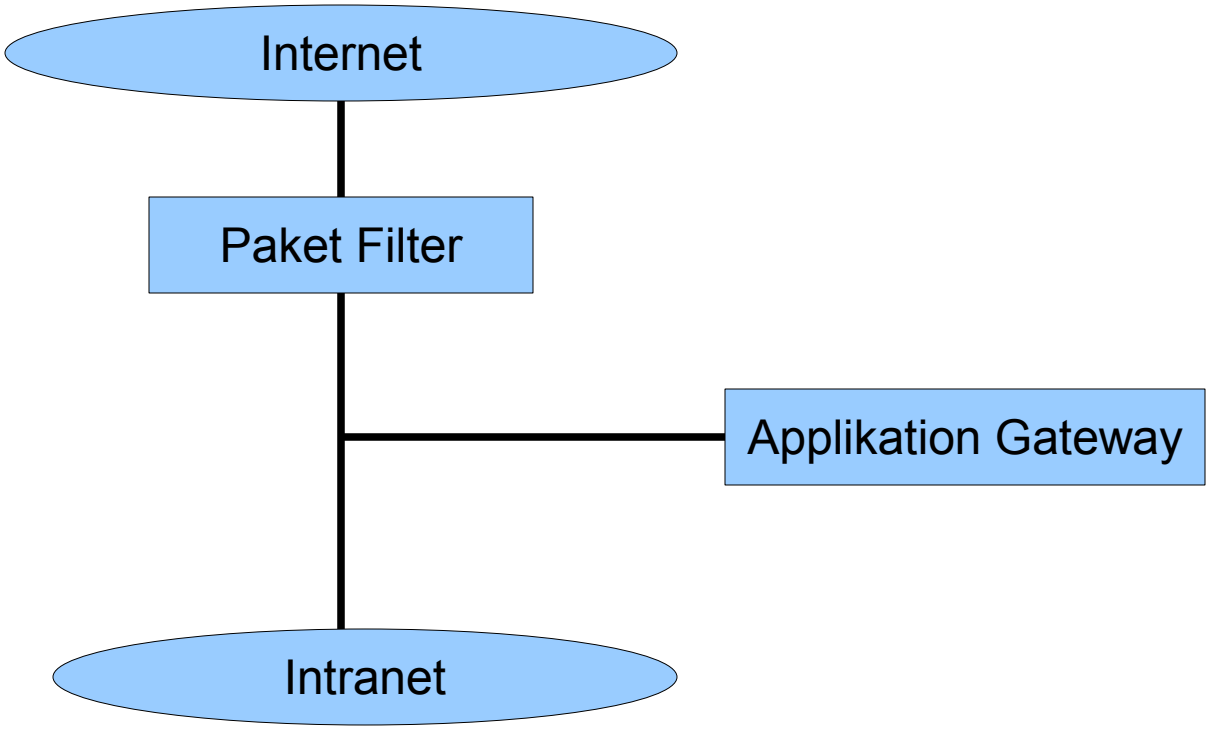
Vorteile

- Durch Kombination von verschiedenen Paket Filtern und Applikations Filtern lässt sich eine höhere Sicherheit erreichen
  - der Angreifer muss mehrere Firewalls durchbrechen, dies kostet Zeit und ist eventuell erkennbar, so dass eine gezielte Abwehr leichter möglich ist
  - der Verteidiger kann verschieden Firewall-Produkte von verschiedenen Herstellern einsetzen und dadurch eventuelle Sicherheitslöcher einzelner Produkte verschleiern.
  - der Verteidiger errichtet verschiedene Bereiche mit unterschiedlichem Schutzniveau (DMZ – Demilitarisierte Zone: Bereich für MAIL- und WWW-Server)
- Kombination von Firewall und Virtuell Private Network Security Gateway ist möglich
  - Über VPN kann das Intranet auf externe Clienten erweitert werden.
- Kosten für Anschaffung und **Betrieb** sind sehr hoch.

15. Firewall - Grundlagen

Kombinationen von Firewalls(2)

Paket Filter und single-homed Applikation Gateway (1)



15. Firewall - Grundlagen

Kombinationen von Firewalls(3)

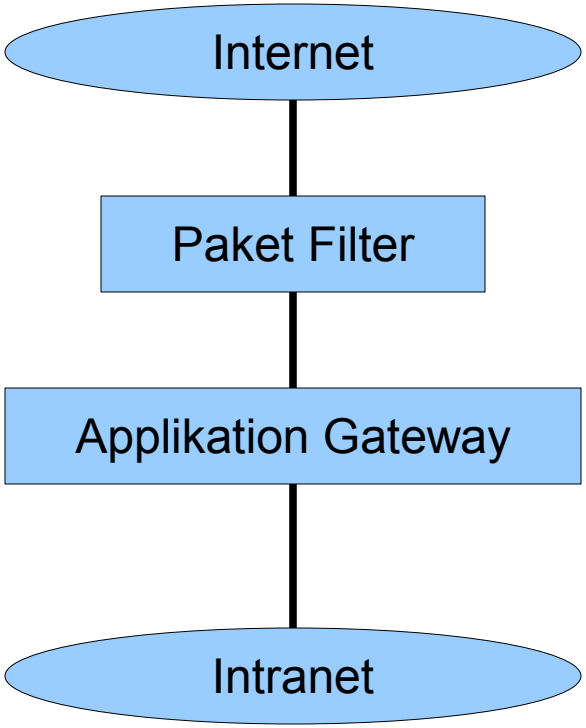
Paket Filter und single-homed Applikation Gateway(2)

- Applikation Gateway ist Teil des zu schützenden Netzes
- Sicherheit hängt wesentlich von der Qualität des Paket Filters ab.
- Paket Filter kann die Sichtbarkeit auf das Intranet einschränken. Im eingeschränktesten Fall ist nur das Applikation Gateway aus dem Internet sichtbar.
- Der Paket Filter erlaubt auch den Schutz von Diensten ohne Applikation Gateway (Proxy nicht vorhanden).
- Das Intranet ist nur durch den Paket Filter geschützt. Das Sicherheitsniveau ist niedrig.
- Das Applikation Gateway ist umgehbar!!!

15. Firewall - Grundlagen

Kombinationen von Firewalls(4)

Paket Filter und dual-homed Applikation Gateway



Es gibt keinen Weg, das Applikation Gateway zu umgehen!!!

15. Firewall - Grundlagen

Kombinationen von Firewalls(5)

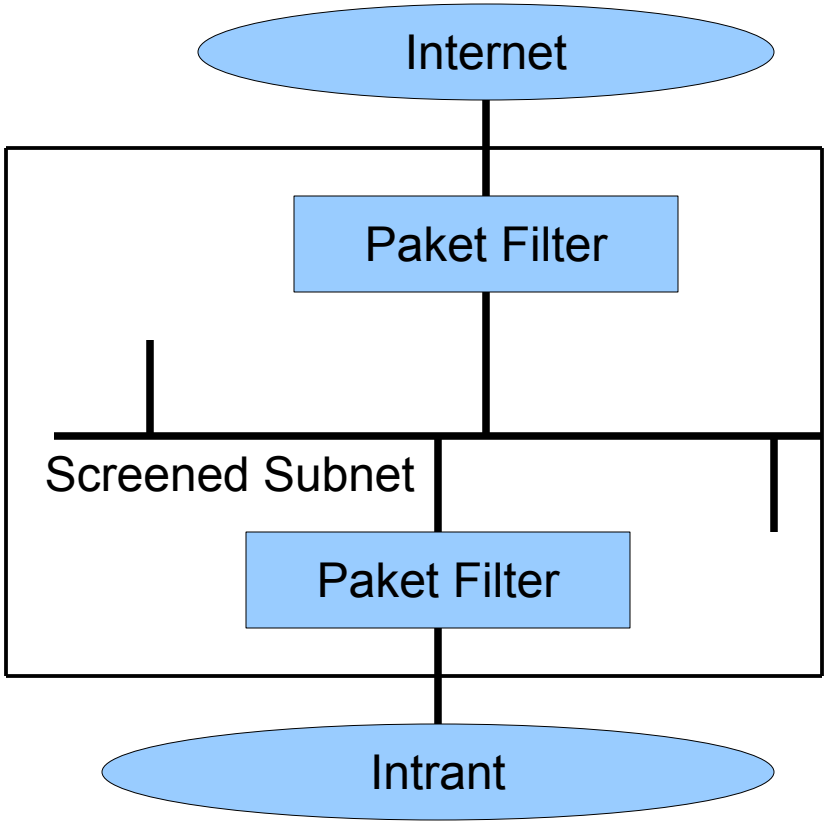
Screened Subnet(1)

- Unter einem Screend Subnetz versteht man ein isoliertes Teilnetz, das zwischen zwei Firewalls liegt. Eine Firewall grenzt das Screened Subnetz vom Internet ab und die andere Firewall grenzt das Screened Subnetz vom Intranet ab
- Das Screened Subnetz wird auch als DMZ – Demilitarisierte Zone bezeichnet
- Die Benutzung von zwei Firewalls vereinfacht die Konfiguration der Firewalls erheblich. Es können einfachere Filterregeln formuliert werden.
- Das Intranet ist besser geschützt.

15. Firewall - Grundlagen

Kombinationen von Firewalls(6)

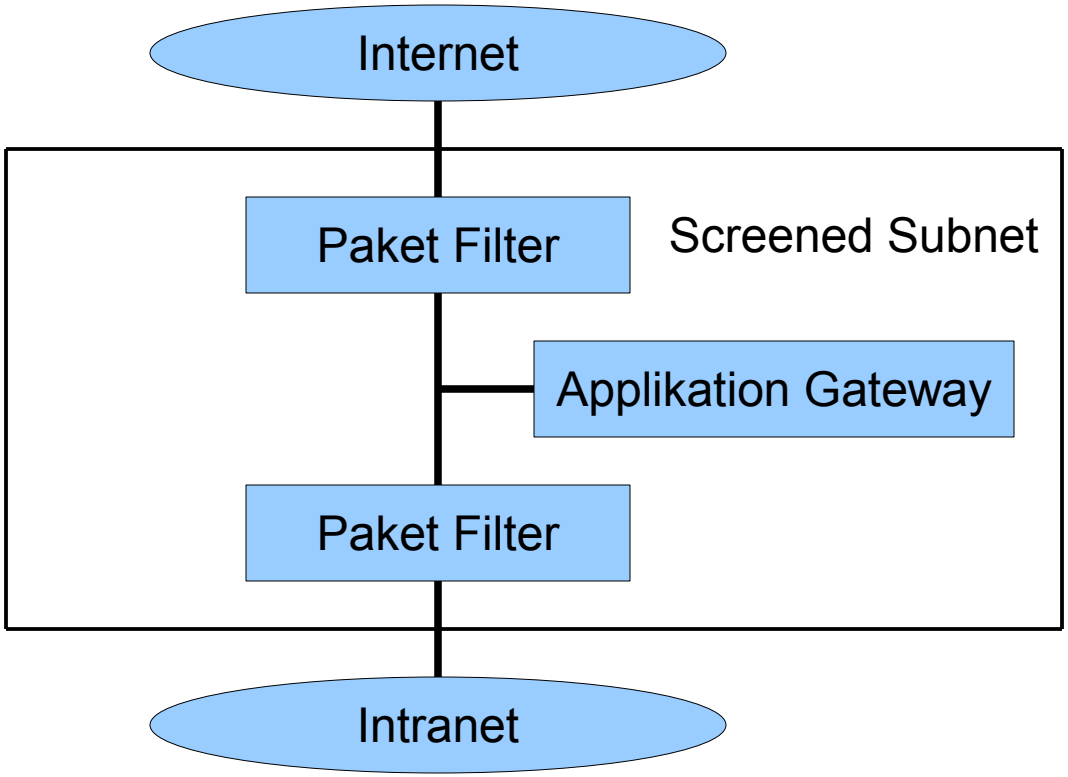
Screened Subnet(2)



15. Firewall - Grundlagen

Kombinationen von Firewalls(5)

Screened Subnet und single-homed Applikation Gateway(1)

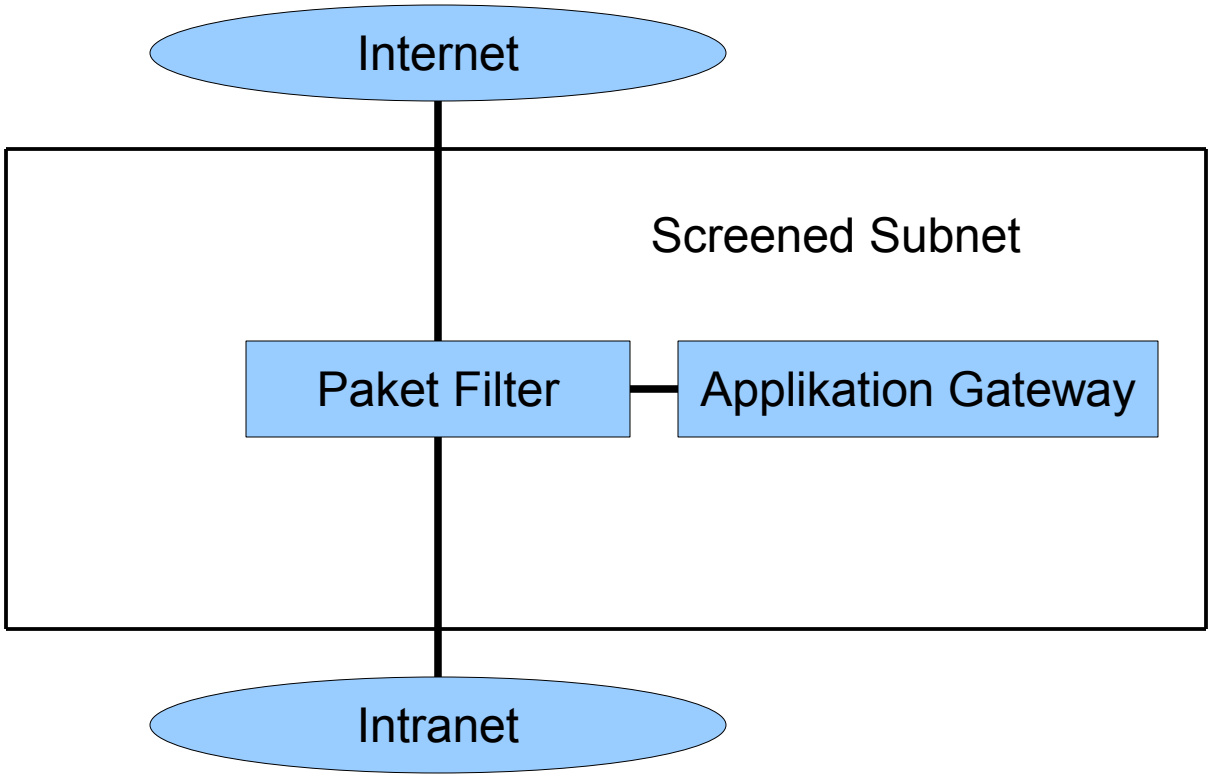


15. Firewall - Grundlagen

Kombinationen von Firewalls(5)

Screened Subnet und single-homed Applikation Gateway(2)

Mit nur einem Paket Filter – arme Leute Variante.



15. Firewall - Grundlagen

Kombinationen von Firewalls(6)

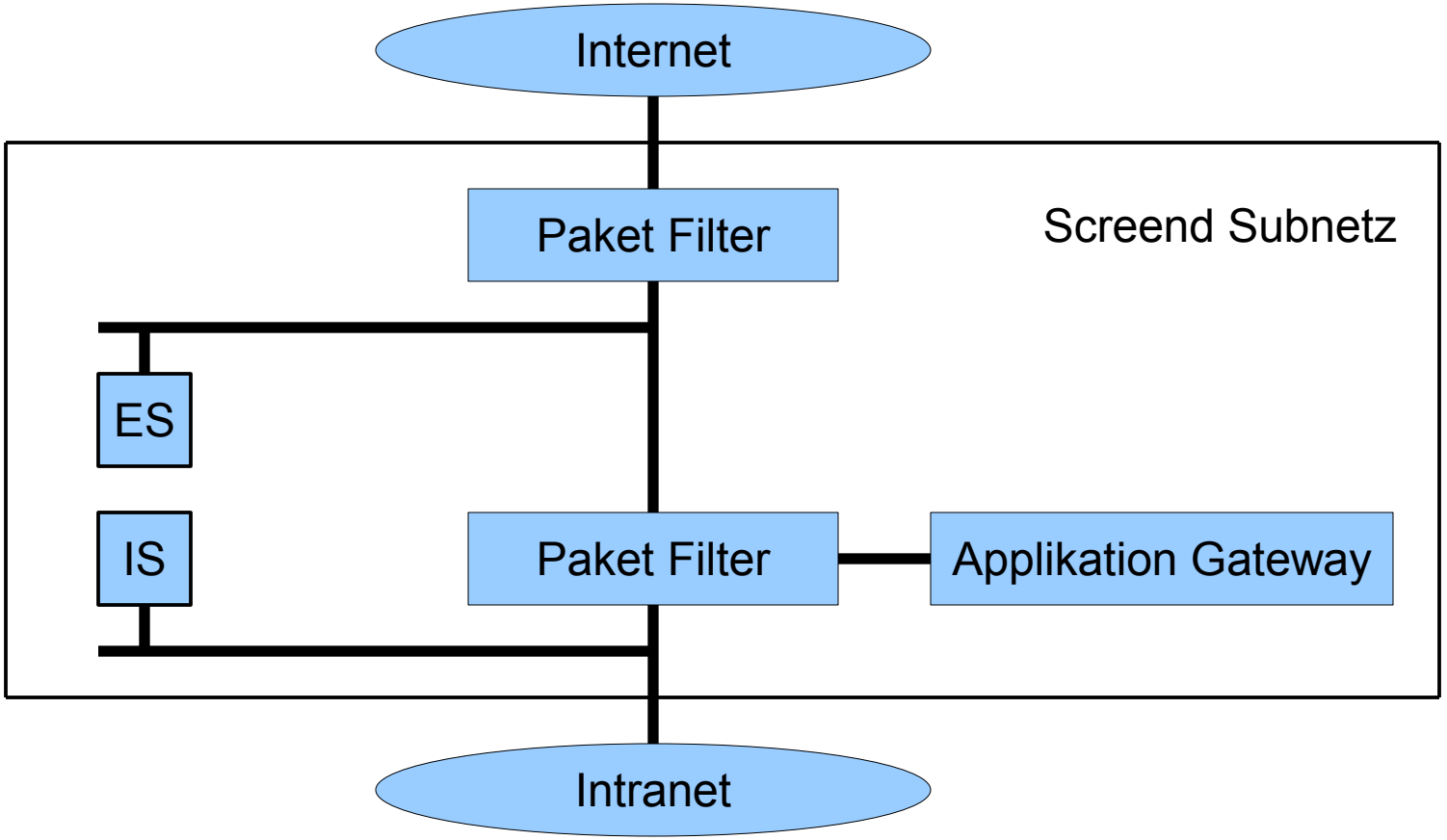
Screened Subnet und single-homed Applikation Gateway(3)

- Das Intranet ist im allgemeinen nicht sehr gut geschützt. Die Benutzung des Applikation Gateways ist nicht obligatorisch.
- Die Firewallregeln sollten allerdings so gestaltet sein, dass die Benutzung des Applikation Gateways obligatorisch ist.
- In der Variante mit nur einem Paket Filter wird diese Form auch als „collapsed DMZ“ bezeichnet
- Wenn das Applikation Gateway der einzige Host ist, der aus dem Internet angesprochen werden kann, wird der zugehörige Rechner auch als „Bastion Host“ bezeichnet.

15. Firewall - Grundlagen

Kombinationen von Firewalls(7)

Screened Subnet und single-homed Applikation Gateway(4)



15. Firewall - Grundlagen

Kombinationen von Firewalls(8)

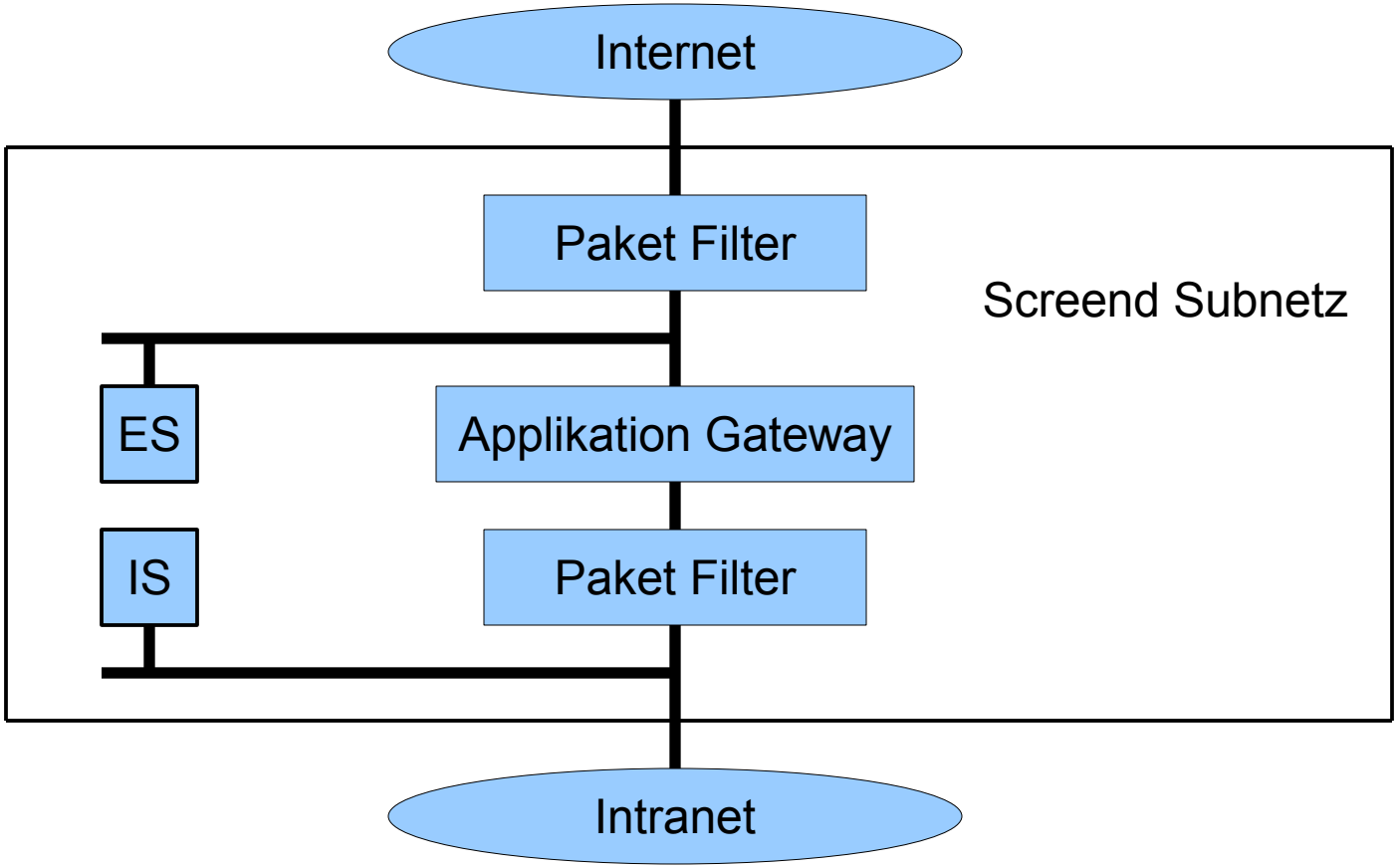
Screened Subnet und single-homed Applikation Gateway(5)

- Hohes Maß an Sicherheit
- hiermit kann das Intranet ohne größeres Risiko an das Internet angeschlossen werden!!!
- Server im Screened Subnet
  - ES – Externe Server: Mailserver, WWW-Server, Name-Server
  - IS – Interne Server: Mailserver, WWW-Server, Name-Server, File-Server

15. Firewall - Grundlagen

Kombinationen von Firewalls(9)

Screened Subnet und dual-homed Applikation Gateway(1)



15. Firewall - Grundlagen

Kombinationen von Firewalls(10)

Screened Subnet und dual-homed Applikation Gateway(2)

- Sehr hohes Maß an Sicherheit
- sehr gut geeignet für die Anbindung eines Intranetzes an das Internet.
- Geringes Einbruchsrisiko.
- Gut geeignet um im Screened Subnet Intrusion Detection Systeme zu installieren – zur Vorwarnung
- Passieren des Applikation Gateways ist zwangsweise notwendig.
- Interne und externe Server im Screened Subnet durch Applikation Gateway zwangsweise getrennt.

15. Firewall - Grundlagen

Kombinationen von Firewalls(11)

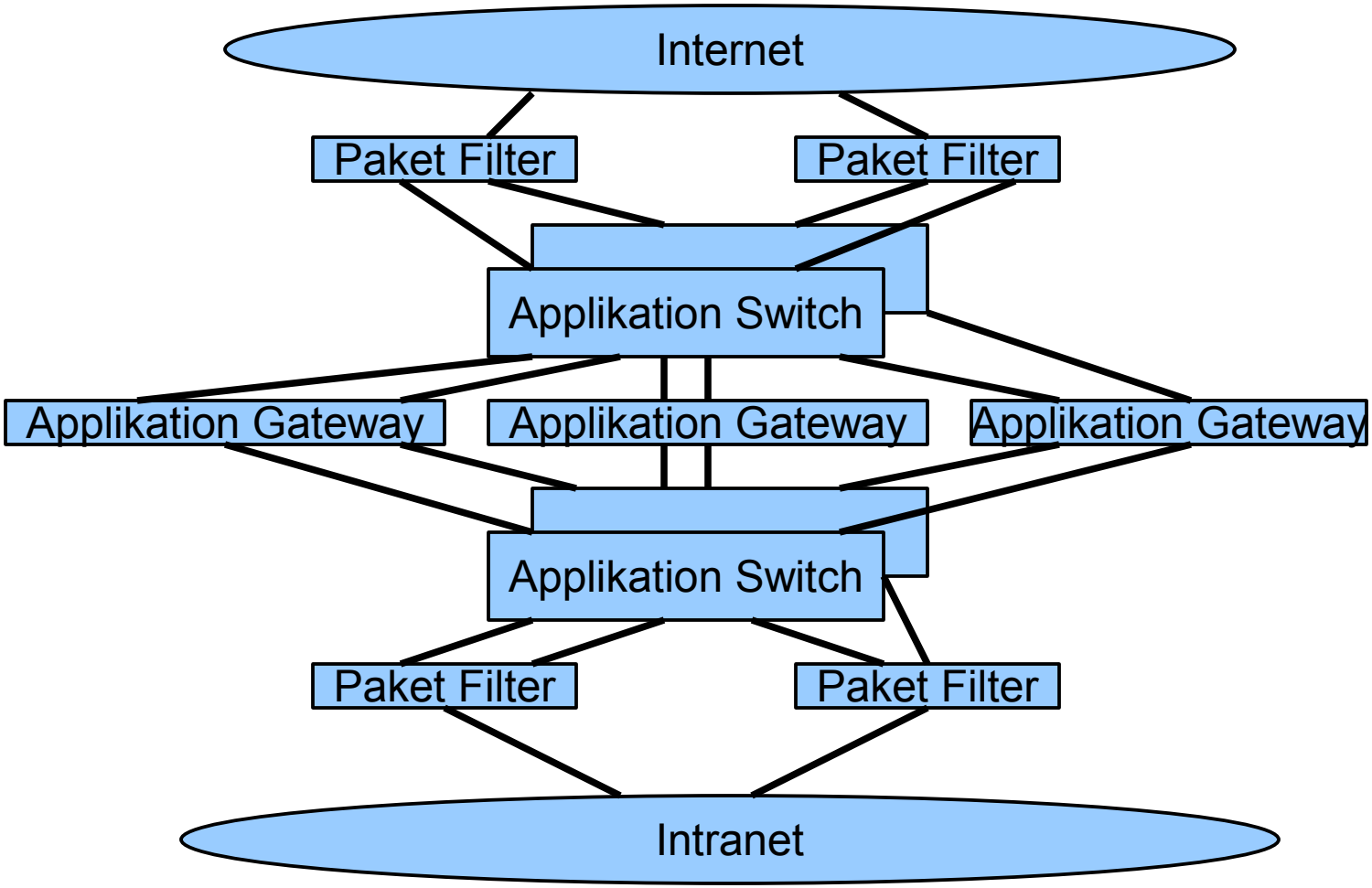
Redundante Firewall-Lösungen – Ziele

- Kein Single Point of Failure – der Ausfall einer Komponente führt nicht zur Trennung des Intranet vom Internet
- Wenn kein Fehler auftritt sollen die redundanten Teile für ein Load Balancing benutzt werden.
- Applikationsswitche sollen für eine Verteilung bezüglich der Applikation Gateways sorgen.
- Soll als komplexes Gebilde schwerer angreifbar sein – deshalb ohne eigene IP-Adresse.

15. Firewall - Grundlagen

Kombinationen von Firewalls(12)

Redundante Firewall Lösung – für Reiche



15. Firewall - Grundlagen

Firewall und NAT

- NAT ermöglicht es die Adressen des Intranet gegenüber dem Internet zu verbergen. Damit ist im Intranet die Nutzung privater Adressen möglich. Die Struktur des Intranet ist nach Außen nicht sichtbar. Dadurch können große Komplikationen auftreten, da alle nach Außen sichtbaren Dienste und Dienstanforderungen von nur einem Rechner kommen.
- Adressen und Portnummern können in höheren Schichten mitgeführt werden!?
  - z.B. bei Mobility Anwendungen, wenn die Adresse anderen Teilnehmern mitgeteilt werden soll
  - Bei der dynamischen Benutzung von Ports
  - Bei Verschlüsselungen
- Für kleinere Netze und den Heimanwender trotzdem ideal!!!

15. Firewall - Grundlagen

Firewall und IDS(1)

Firewall und IDS (Intrusion Detection System) ergänzen sich. Sie erfüllen unterschiedliche Aufgaben:

- Ein Firewall soll unerwünschten Verkehr blockieren. Er ist primär dazu da Angriffe aus dem Internet abzuwehren.
- Ein IDS soll den auftretenden Verkehr analysieren und ungewöhnlichen Netzwerkverkehr erkennen und melden, dabei kann es folgende Leistungen erbringen
  - Angriffe aus dem Internet und dem Intranet erkennen
  - Fehlbenutzungen und Fehlkonfigurationen erkennen
  - bekannte und unbekannte Angriffsmuster erkennen
  - kann an mehreren Stellen das Netz überwachen
  - Verhalten von Benutzern überwachen
  - Den Durchbruch durch den Firewall erkennen
  - Hilfestellung bei der Analyse eines Angriffes geben

15. Firewall - Grundlagen

Firewall und IDS(2)

Klassifikation von IDS

- Klassische Lösung
  - Arbeitet nach vorgegebenen Regeln, Mustern und Signaturen. Überprüft ob die Protokolle dem Standard entsprechen.
  - Meldet Standardverletzungen
  - Meldet nur bekannte Angriffe
- Anomaly Detection
  - Entdeckt Vorgänge und Zustände, die außerhalb der Norm liegen
  - Schwer zu konfigurieren und zu tunen
  - kann unbekannt Angriffe erkennen
  - Probleme

    Unterscheidung von wirklichen Anomalien und regulärem Netzwerk-verkehr? Wie scharf kann man die Regeln formulieren? Wie kann man die große Menge von Meldungen verarbeiten?

15. Firewall - Grundlagen

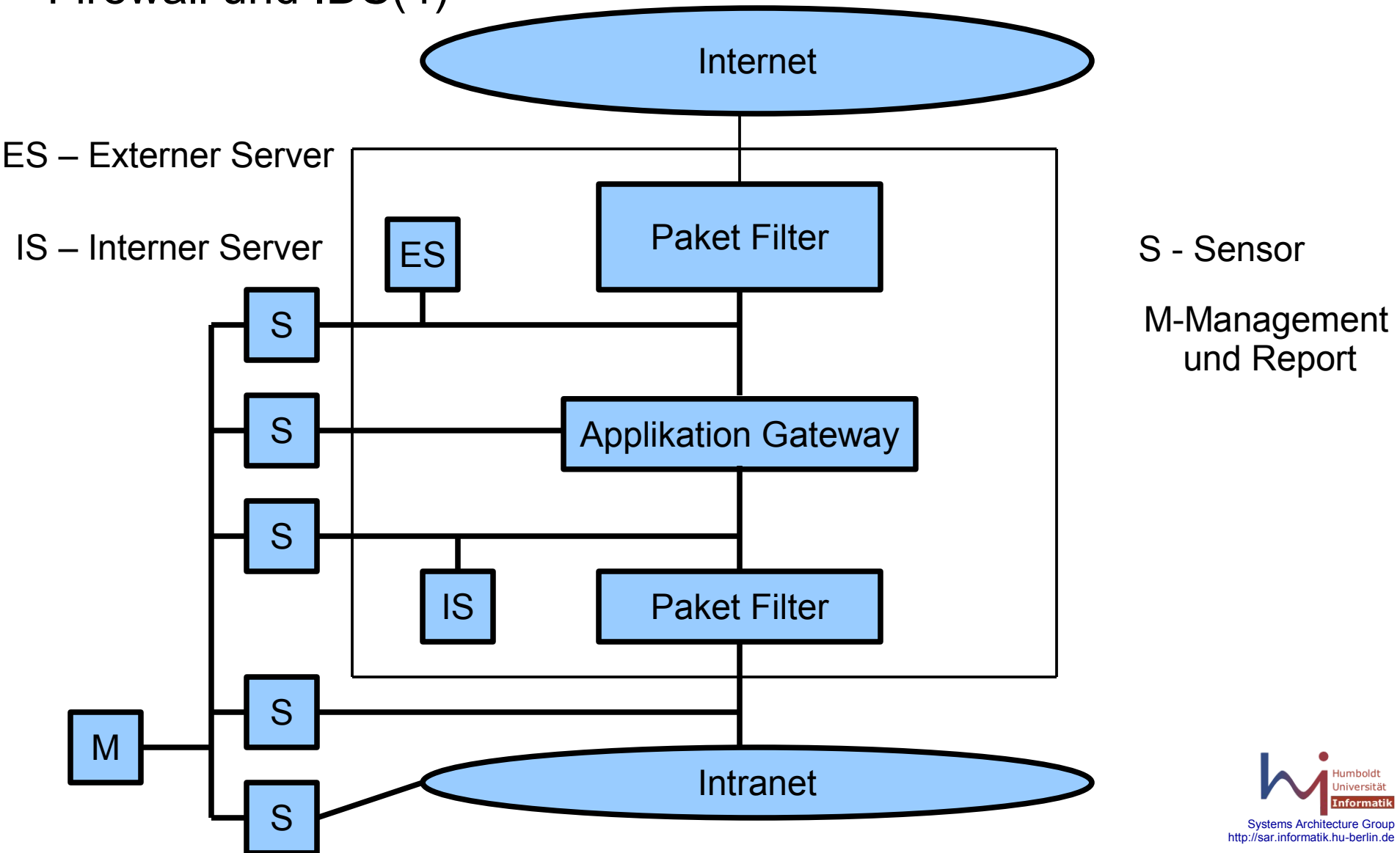
Firewall und IDS(3)

Typen von IDS

- Network-Based-IDS
  - Spezielle Sensoren überwachen kritische Netzwerksegmente z.B. die DMZ
  - Sensoren müssen problemlos den gesamten Netzwerkverkehr mitschneiden können und gegebenenfalls speichern können.
  - Stealth Sensoren sind möglich. Schwer erkennbar und angreifbar.
  - Beispiele: Snort, Dragon, BlackICE
- Host-Based IDS
  - Software, die einen einzelnen Host überwacht (extern, intern)
  - Alle Komponenten einschließlich Log-Files können hinzu gezählt werden.
  - Bei erfolgreichen Angriffen kann das IDS eventuell nicht mehr arbeiten.
  - Beispiele: Network Flight Recorder

15. Firewall - Grundlagen

Firewall und IDS(4)



15. Firewall - Grundlagen

Security Management bei Firewalls – Tätigkeit des Personals

- Einhaltung der Security Policy muss ständig überprüft und durchgesetzt werden, Verstöße müssen geahndet werden
- Das Management der Firewalls muss außerhalb der Firewalls im zu sichernden Netz (Intranet) erfolgen, eventuell aus einem zusätzlich geschütztem Netz heraus (Managementnetz)
- Folgende Rollen müssen mit unterschiedlichen Rechten versehen seien: Administrator, Operator, Editor, Observer
- Alle Ereignisse müssen protokolliert werden:
  - Verletzung der Policy
  - Erkennung von Angriffsversuchen
  - Alarmierung bei sicherheitsrelevanten Ereignissen
  - Sicherung von Beweisen
- Regelmäßige manuelle und automatische Auswertung der LOG-Dateien – Datenschutz beachten!!!!!

15. Firewall - Grundlagen

Grenzen von Firewalls(1)

- Firewalls sind **hinderlich**
- Firewalls sind **umständlich**
- Firewalls sind **aufwendig** im Betrieb
  - hohe Betriebskosten (Personal)
  - schwer zu konfigurieren
- Firewalls haben **nur eine gewisse Standzeit** – bis die Hacker die Sicherheitslöcher entdeckt haben
- Firewalls können die korrekte und verantwortliche Administration der dahinterliegenden Systeme **nicht** ersetzen
- Firewalls schützen nicht vor Feuer und Wasser
- Firewalls schützen nicht vor inneren Feinden
- Firewalls werden überflüssig, wenn alle Dienste sicher sind!!!

15. Firewall - Grundlagen

Grenzen von Firewalls(2)

Schutz vor DOS- (Denial of Service) und DDOS (Distributed Denial of Service)- Angriffen

- DOS und DDOS Angriffe sind schwer zu erkennen und schwer abzuwehren, da sie sich von normalem Verkehr nur durch die Häufigkeit des Auftretens von Anfragen unterscheiden.
- Die Abwehr von DOS und DDOS Angriffen ist nur durch die Zusammenarbeit von Anbietern und Nutzern von Servicen gemeinsam zu realisieren
    - ISP müssen ungültige Absenderadressen verhindern (spoofing)
    - Betreiber von Server müssen ihre Server überwachen, um nicht selber zum Angreifer zu werden: Spoofing verhindern, Broadcast verhindern, Speicher- und Netzwerkauslastung überwachen. Eventuell IDS benutzen.
    - Als Inhalteanbieter aktive Elemente vermeiden
    - Nutzer sollten vermeiden, als Agenten benutzt zu werden(Viren)!!!!!

15. Firewall - Grundlagen

Grenzen von Firewalls(3)

Möglichkeiten eines Angriffs auf einen WWW-Server

- Bufferowerflow ausnutzen
- Falsch gesetzte oder nicht gesetzte Parameter ausnutzen
- Zugangskontrolle aushebeln
- Passworte abgreifen
- Session Management aushebeln – sich in eine bestehende TCP-Verbindung einklinken
- Command Injection bei SQL
- WWW-Server mit Fehlern überhäufen
- Fehler in der Kryptographie ausnutzen
- Fehler in der Absicherung der Remote-Administration ausnutzen
- Fehlkonfiguration des WWW-Servers ausnutzen

15. Firewall - Grundlagen

Betrieb eines Firewalls – Mit der Auswahl eines Produktes ist es nicht getan.

Der Firewall verursacht erhebliche Betriebskosten

- Logs müssen regelmäßig ausgewertet werden
- Angriffsversuche müssen erkannt und abgewehrt werden
- Erfolgreiche Angriffe müssen erkannt und analysiert werden, um zukünftige Angriffe unterbinden zu können.
- Die Software auf den Firewallsystemen muss ständig aktualisiert werden
- Änderungen, neue Dienste müssen eingepflegt werden

Das Personal muss präsent sein und sich ständig weiterbilden.

Die Wirksamkeit des Firewalls muss in regelmäßigen Abständen überprüft werden - eventuell von externem Personal.