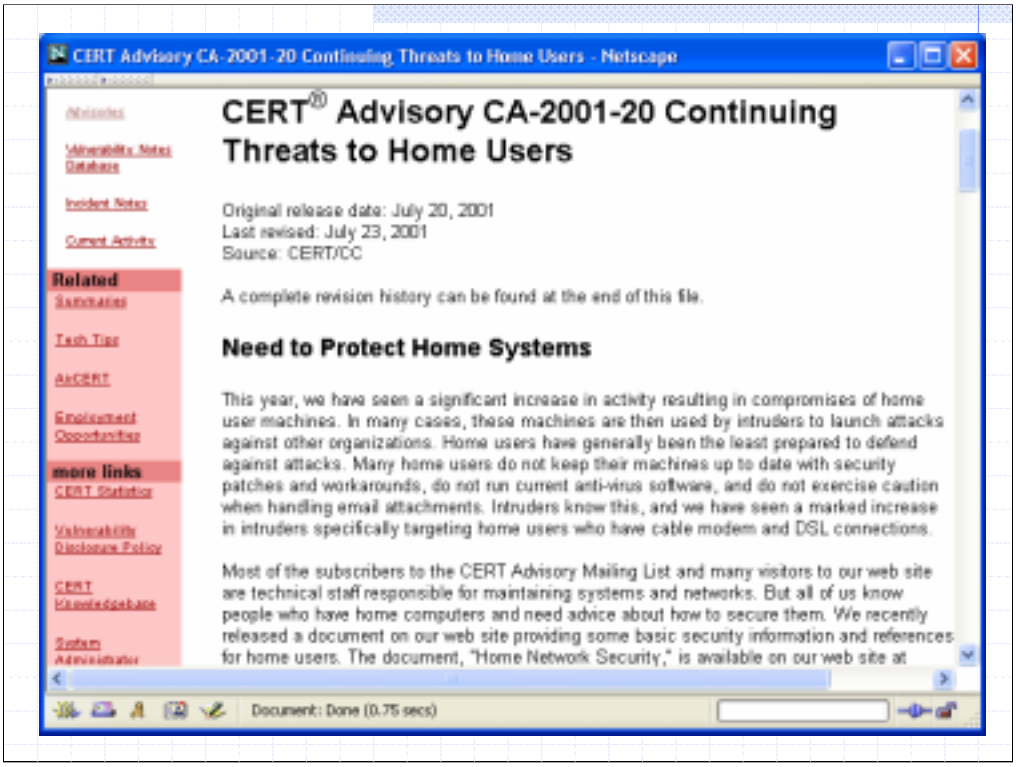
Firewall, Teil 2

TBZ Technikerschule Zürich

IT Services Technologien,
Vorträge zu Entwicklungstrends

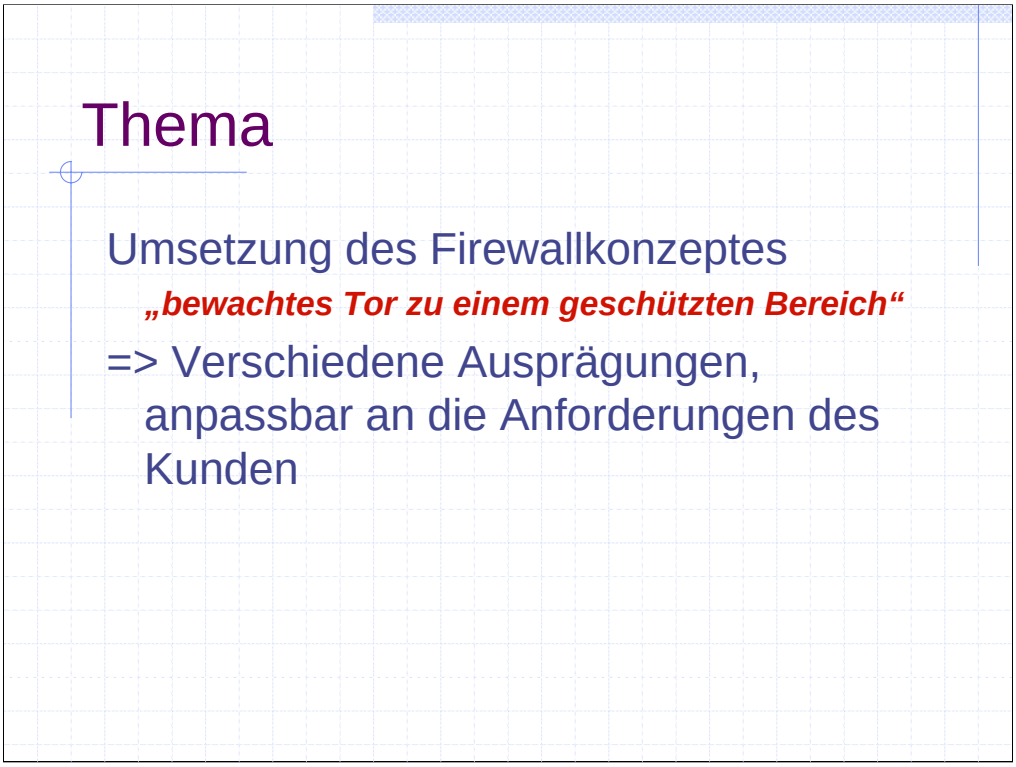
1. Juli 2002

Kuno Pfund, Gregor Battilana



Warnung vom CERT (früher: Computer Emergency Response Team = Organisation, die Informationen über Angriffe gegen Computer sammelt und Tipps zur Abwehr gibt.):

Heimcomputer sind gute Ausgangspunkte für Hackerangriffe, da die Heim-PC‘s häufig nicht geschützt sind. => Frage an die Zuhörer: Wer hat zu Hause einen Internet-Zugang => Wer hat irgendeine Form von Firewall installiert?



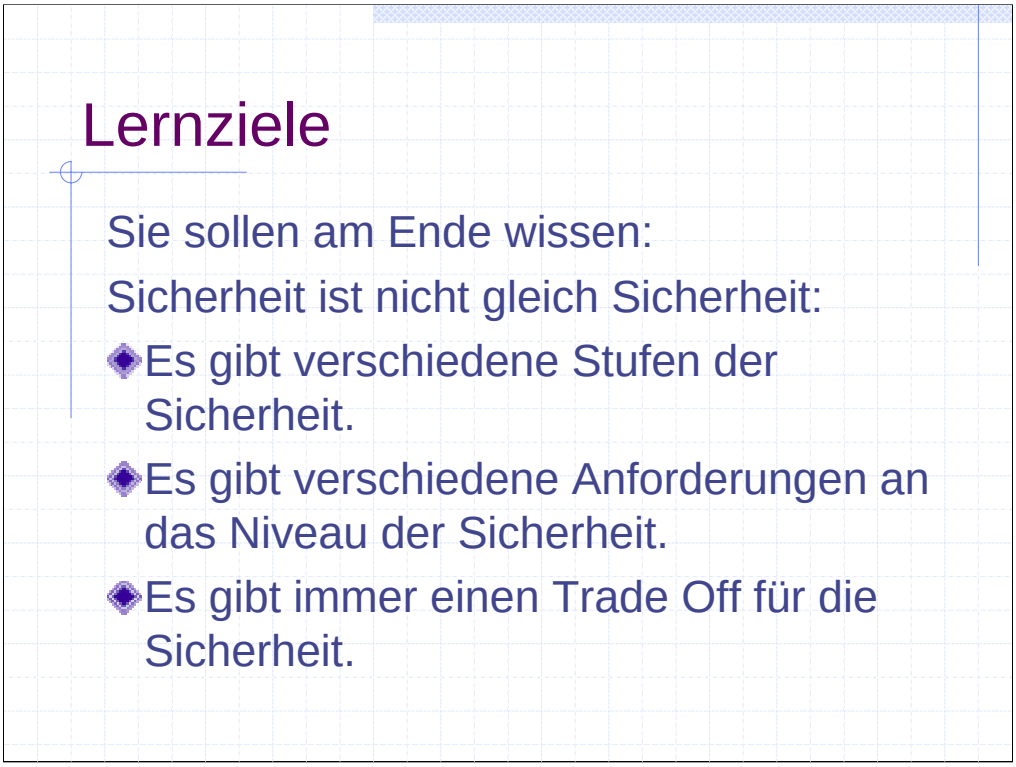
Advance Organizer: Thema

Zur Erinnerung: Es geht um zwei Aspekte:

•Geschützter Bereich: Man ist sich bewusst, dass das Internet nicht sicher ist, d.h. man trennt seinen eigenen Bereich davon ab: Trennung

•Bewachtes Tor: Der Übergang zwischen der geschützten und der ungeschützten Zone wird kontrolliert, so dass nur bestimmte Pakete passieren können.

Ich will im Folgenden zeigen: Es gibt verschiedene Wege, diese beiden Eigenschaften zu erreichen. Fast jedes Netzwerk hat andere Anforderunge.

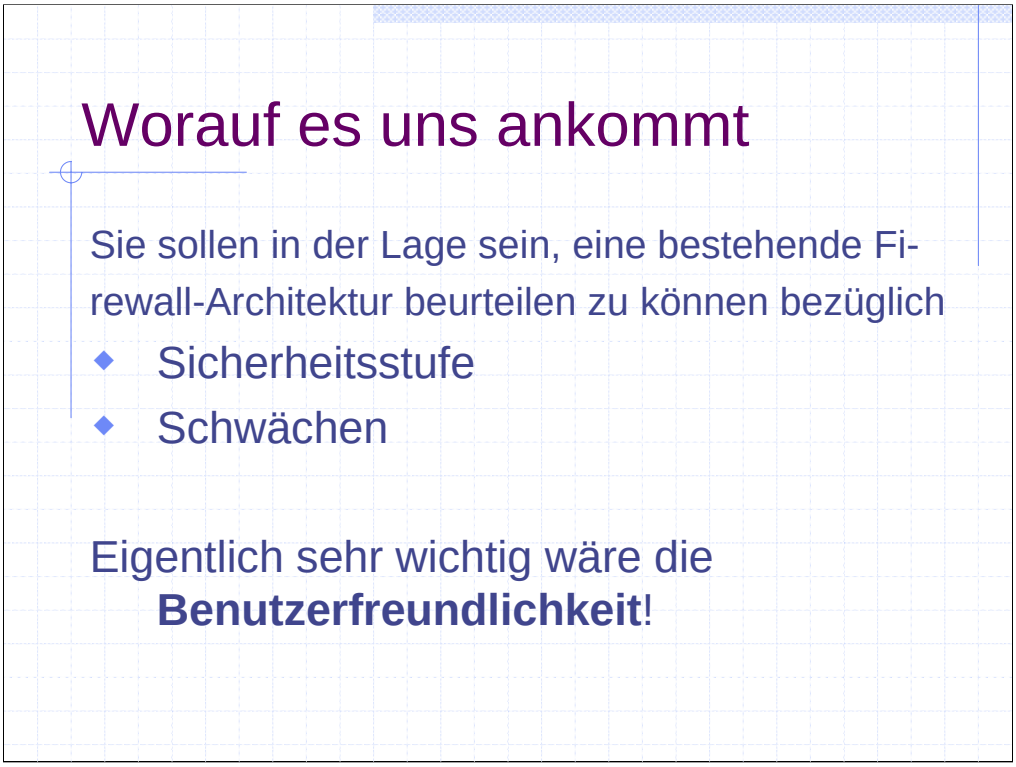


Advance Organizer: Lernziele

•Absolute Sicherheit gibt es nicht.

•Das ist nicht schlimm, denn kaum jemand braucht absolute Sicherheit.

•Sicherheit ist nie umsonst: Im Fall der Firewall kann der Trade Off bestehen aus: Verlust an Netzwerk-Performance, Einschränkung der Dienste, die für Benutzer zugänglich sind, finanzieller Aufwand, personeller Aufwand zur Wartung, was letzten Endes wieder finanziellen Aufwand bedeutet.



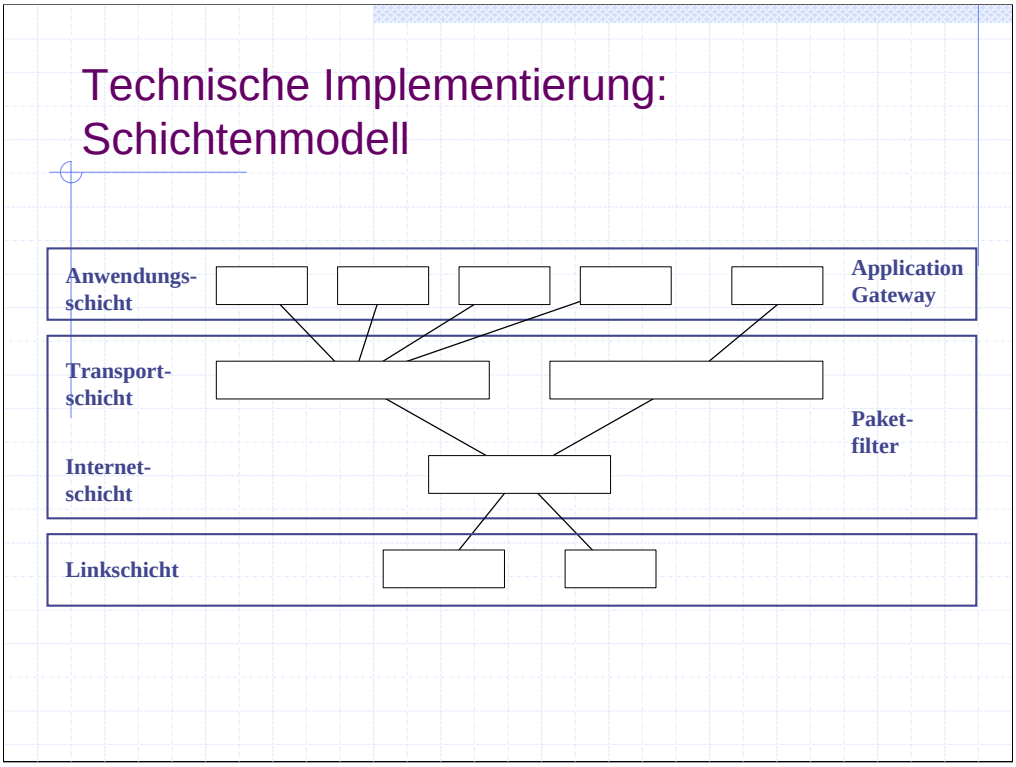
Advance Organizer: Worauf es uns ankommt

Nebst den genannten zwei Punkten gibt es einen Aspekt, der gerne vergessen geht, nämlich die Leute, die schlussendlich mit dem System arbeiten müssen. Wir werden diese hier aus Zeitgründen nicht betrachten.

Ablauf von Teil 2

Inhalt	Form	Dauer [min]
Technische Implementierung Typische Topologien Arten der Umsetzung	Theorievortrag	45
Fallstudie, Teil 2: Beurteilung einer bestehenden Firewall-Lösung an Hand einer konkreten Situation	Gruppenübung	25
Plenumsdiskussion zum Teil 2 der Fallstudie	Besprechung	20

Alle Zeiten sind Schätzungen.



Die Graphik zeigt ein vereinfachtes OSI-Modell:

•OSI-Schichten 1 und 2 wurden zur Linkschicht zusammengefasst.

•Die Schichten 5, 6 und 7 werden hier als Anwendungsschicht bezeichnet.

„Historisch bedingt“ finden wir die Einordnung von Application Gateway und Paketfilter im Schichtenmodell: „Paketfilter“ meint grundsätzlich eine Filterung auf Ebene von Transport- und Internetschicht, während mit „Application Gateway“ eine Filterung im Bereich der Anwendungsschicht gemeint ist.

Technische Implementierung: Paketfilter

Filterung auf Grund von 6 Eigenschaften:

- Pakete gehen **ein** oder **aus**.
- **IP-Adressen** von **Sender** und **Empfänger** sind aus der Internetschicht bekannt.
- **Portnummern** von **Sender** und **Empfänger** sind aus der Transportschicht bekannt.

Verfeinerungen:

- Dynamischer Filter => **temporäre** Regeln für Pakete, die als Antwort erwartet werden
- Zustandsabhängiger Filter => Regeln berücksichtigen den Zustand einer Verbindung einer **höheren** Schicht

Regeln für den Pförtner: was genau soll er tun

Am einfachsten wäre:

•Nix darf weder rein noch raus => gute Lösung aus Sicht der Sicherheit

•Alles darf rein oder raus => gute Lösung aus Sicht der Produktivität (Kerngeschäft)

Beispiele:

•Verwirf alle eingehenden Pakete die aus Internet-Domains stammen, die mit 123.456. anfangen.
=> Lastwagenbeispiel: keine Lastwagen mit ZH Nummernschildern einlassen

•Leite alle eingehenden Pakete auf den Ports von 12001 bis 12099 auf den jeweils entsprechenden Port auf der Maschine 234.456.678.891 weiter.
=> Lastwagenbeispiel: Alle eingehenden Lastwagen, die zum Lager wollen, sollen an die Spedition umgeleitet werden.

•Blockiere alle ausgehenden Verbindungen an die Adresse 345.567.789.912.
=> Lastwagenbeispiel: Lass keinen Lastwagen vom Gelände fahren, der als Ziel die Firma XY angibt. (Denn diese Firma wird nicht mehr beliefert!)

Dynamische Filter:

Auf eine ausgehende Anfrage sollte demnächst eine Antwort eingehen. Damit diese passieren kann, wird eine Filterregel dafür eingesetzt. Diese wird nach einer gewissen Zeit wieder gelöscht.

=> Lastwagenbeispiel: Wir lassen den Pizza-Kurier nur dann rein (und idealerweise hinterher wieder raus), wenn wir vor kurzem etwas bestellt haben.

Zustandsabhängige Filter:

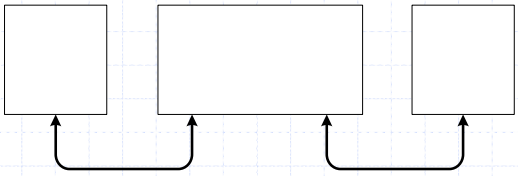
Es wird versucht, auf den Zustand einer Verbindung zu schliessen und dementsprechend zu filtern.

Bsp.: Telnet-Verbindung: Solange der Benutzername nicht übermittelt wurde, ist wohl ein Verbindungsaufbau im Gange.

=> Lastwagenbeispiel: Wenn ich sehe, dass Maschinenteil XY auf dem Lastwagen drauf ist, wird wohl Produkt FGH gebaut, d.h. es sind noch mehr Lastwagen von dieser Firma zu erwarten, die ich auch reinlasse.

Bei beiden Verfeinerungen geht es also darum, temporär wirksame Filterregeln aufzustellen, die nach einer gewissen Zeit entfernt werden.

Technische Implementierung: Application Gateway



Zwei verschiedene Arten von Proxy-Prozessen:

- Application Level Proxy
- Circuit Level Proxy

„Proxy“ = engl. „bevollmächtigt“:

•Aus Sicht des Users ist der Proxy der Server.

•Aus Sicht des Information Server ist der Proxy der Client.

Application Level Proxy:

•Ein Prozess pro Protokoll

•Alle Datenpakete werden „ausgepackt“ und der Inhalt überprüft, danach wieder „eingepackt“. => saubere physische und logische Trennung

•Bsp.: HTTP-Proxy => Filtern nach URLs (geht nicht mit Paketfilter), Java Applets, ...

Circuit Level Proxy:

•Generischer Proxy Prozess, der für alle Protokolle eingesetzt werden kann

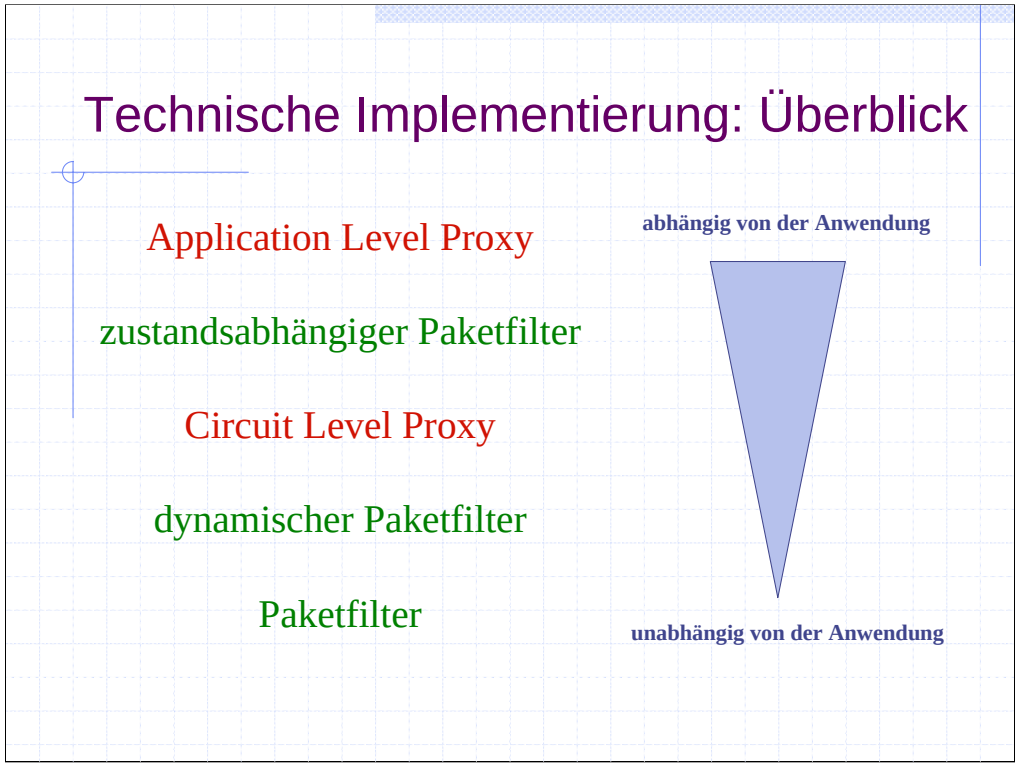
•Braucht entweder die protokollspezifischen Infos vom Client (=> dieser muss modifiziert werden, damit er das kann), oder

•Er leitet die Verbindung einfach weiter, ohne überhaupt zu filtern

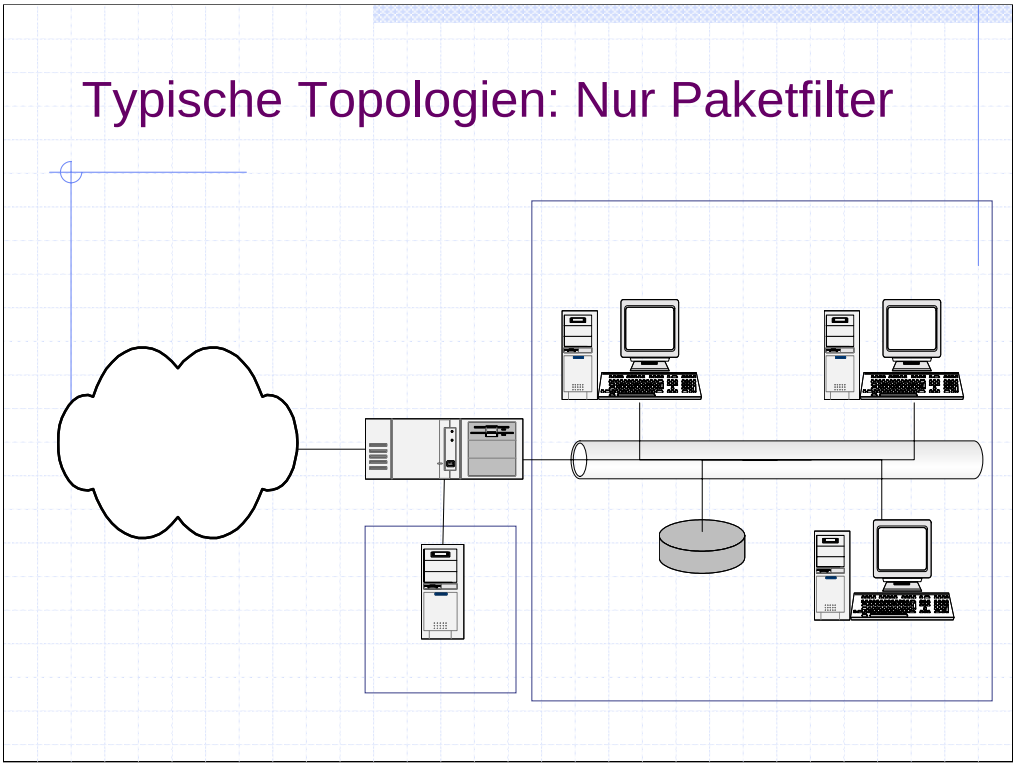
Technische Implementierung: Vergleich

	Schwächen	Stärken
Paketfilter	Filterregeln sind nur grobkörnig einstellbar. Bei vielen Regeln geht leicht die Übersicht verloren.	Rel. einfache Konfiguration (neues Protokoll => neue Regeln) Effiziente Verarbeitung
Application Gateway	Jeder Prozess muss einzeln konfiguriert werden. Verarbeitung eher ineffizient	Feinkörnige Filterung ist möglich. Inhaltliche Überprüfung ist möglich. Logische Trennung der Verbindung

Eigentlich ist es nicht erstaunlich: Die Schwächen des einen Ansatzes sind die Stärken des anderen und umgekehrt.



In rot sind die beiden vorgestellten Varianten von Application Gateways, in grün die gezeigten Varianten von Paketfiltern. Geordnet nach dem Grad der Abhängigkeit von Informationen aus der Anwendungsschicht erkennt man, dass die Trennung der beiden Ansätze keineswegs so klar ist, wie ursprünglich einmal im Schichtenmodell definiert.



Einfachste (und billigste) Variante - ein einziger Paketfilter:

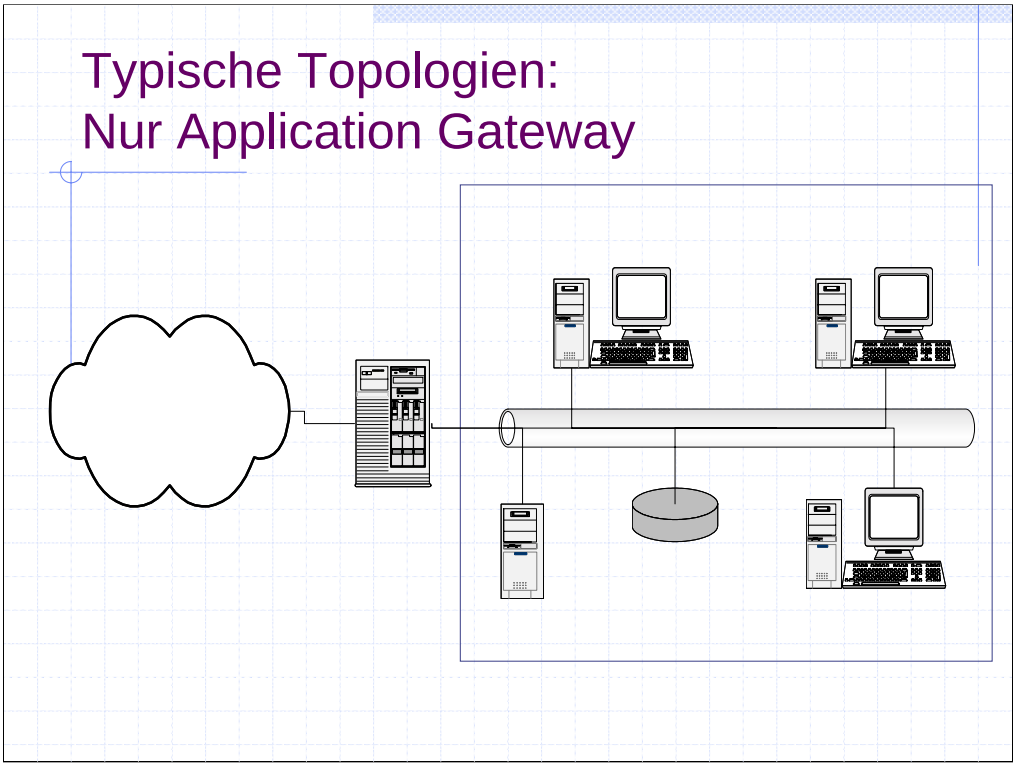
•Aus dem Intranet heraus macht es keinen Sinn, nach IP Adressen zu filtern (kann leicht gefälscht werden)

•Eine einzige Komponente trennt die beiden Netze => Konfiguration ist kritisch!

•Erlaubte Dienste müssen beim End User abgesichert sein!

Die gezeichnete Variante enthält eine sog. „demilitarisierte Zone“, die hier gelb eingezeichnet ist. Die Idee dahinter ist, dass dort Dienste angeboten werden, die sowohl von innen als auch von aussen zugänglich sind ohne eine direkte Verbindung der zu trennenden Netze. Der Paketfilter kann hier Anfragen vom Internet an den Web Server weiterleiten, ohne dass das Intranet (hier blau) angesprochen werden muss. Das bedingt, dass der Paketfilter unterscheiden kann, von welchem Netzwerk-Interface er welche Anfrage erhalten hat. Zum jetzigen Zeitpunkt (Juli 2002) können das viele Produkte nicht!

Internet

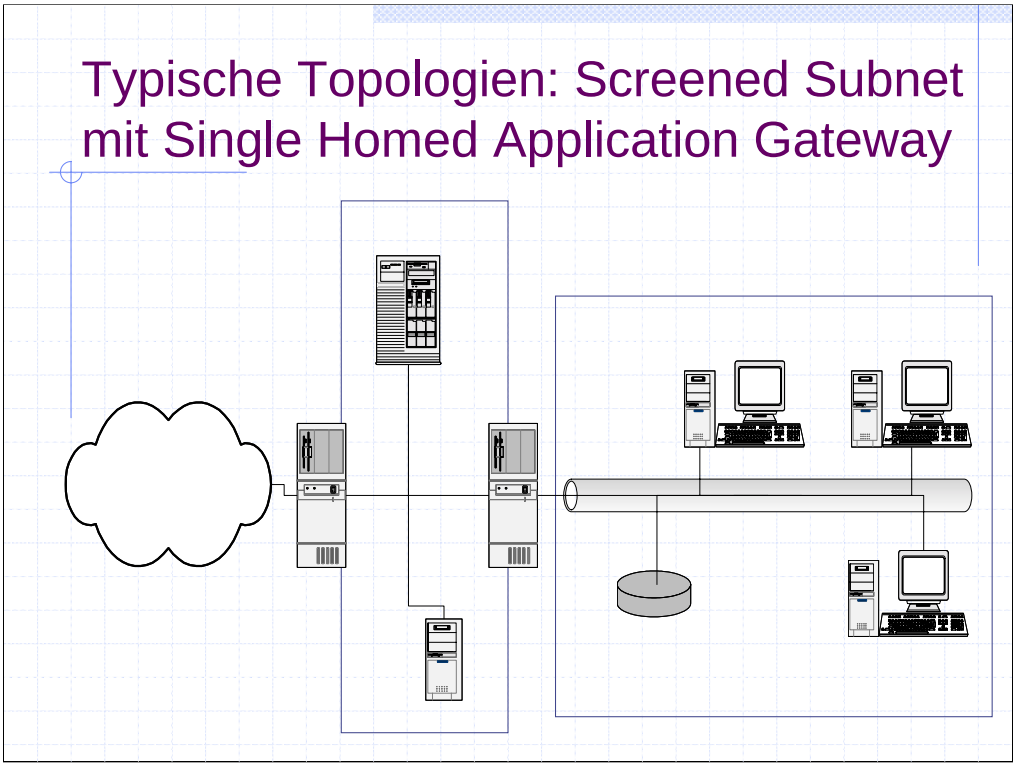


•Unterschied gegenüber vorheriger Lösung: Stärkerer Schutz, weil halt Application Gateways mehr schützen als nur Paketfilter

•Mit 2 oder noch mehr Interfaces wird nicht nur eine logische, sondern auch eine physikalische Trennung möglich.

Die hier gezeigte Lösung besitzt nur 2 Netzwerk-Interfaces und daher keine entmilitarisierte Zone. In diesem Beispiel wurde der Web Server im Intranet angehängt. Ein Zugriff auf den Web Server aus dem Internet führt als zu einer direkten Verbindung ins Intranet!

Internet



•Mehrere Schutzinstanzen => mehrere Hürden.

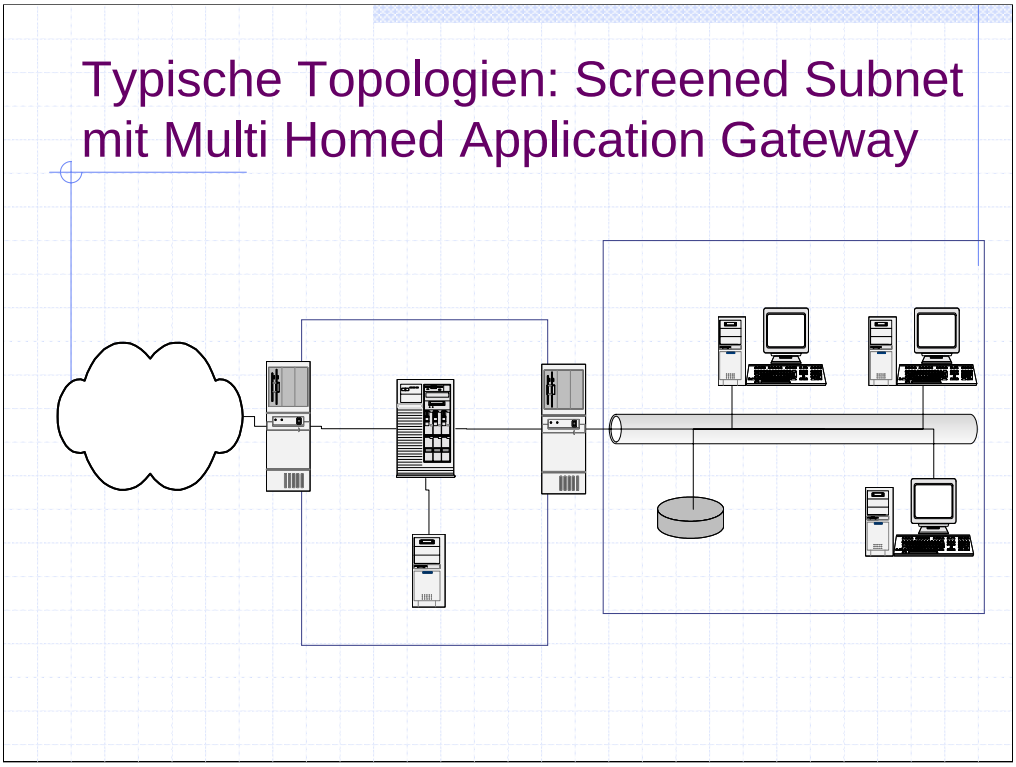
•Abstufung der Sicherheit in verschiedene Stärken ist möglich.

•Leicht skalierbar: ein zweiter Application Gateway lässt sich hier problemlos einfügen.

•Schwachstelle Information Server (hier Web Server): dieser kann gehackt und dann missbraucht werden für Angriffe gegen innen => Darum braucht es den 2. Paketfilter!

Wiederum in gelb gibt es hier eine demilitarisierte Zone, die in dieser Konfiguration als Screened Subnet bezeichnet wird. Der Application Gateway besitzt in diesem Fall nur ein einziges Netzwerk-Interface („single homed“), so dass die beiden Paketfilter erzwingen müssen, dass ein- und ausgehende Datenpakete über den Application Gateway laufen.

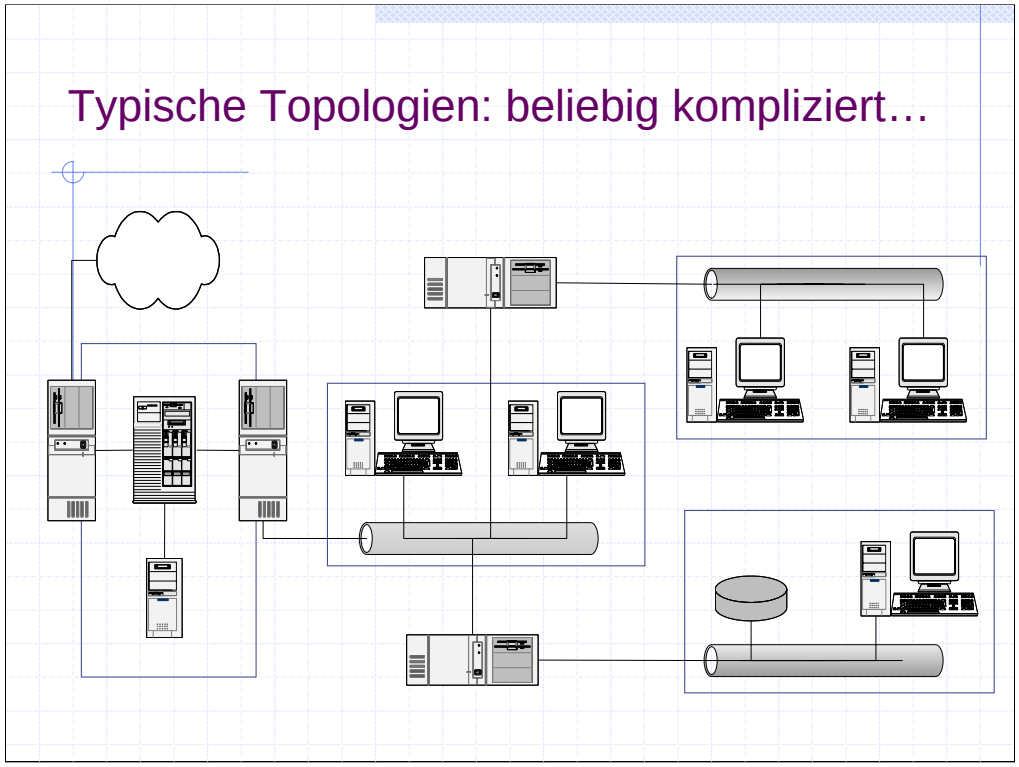
Internet



•Symmetrische Lösung => gut für ungewisse Zustände innerhalb des Intranets, Bsp. Provider, Universität

•Wenig Flexibilität: im Idealfall ist jedes Kästchen ein Produkt eines anderen Herstellers (damit nicht alle die gleichen Sicherheitslücken haben), d.h. ich habe drei verschiedene Produkte, die ich warten muss

Internet



•Verschiedene Zonen, anpassbar an die Bedürfnisse der einzelnen Teile des Intranets. Bsp.: Grüne Zone (Buchhaltung) soll keinen Zugang haben zu den Daten der roten Zone (Forschung und Entwicklung).

•Im Beispiel 5 Maschinen, im Idealfall alles unterschiedliche Produkte => enormer Wartungsaufwand!

Die gezeichnete Konfiguration ist nur ein Beispiel. Es wäre genauso denkbar, die rote Zone direkt am zweiten Paketfilter von links anzuhängen, oder die blaue Zone zwischen die rote, oder … je nach den Bedürfnissen.

Internet

Application Gateway

Paketfilter

Separate Einrichtung, d.h. ein Knotenpunkt, wo alle Verbindungen drüber laufen sollen:

•Hardware Produkte (immer mit Konfigurationssoftware, oft ein Web-Interface)

•Software Produkte

•Kombinationen aus Hard- und Software

Die meisten Produkte halten sich nicht an die vorher gezeigte Aufteilung in Paketfilter und Application Gateway, sondern bieten eine Kombination aus beidem, zum Teil mit weitern Funktionen wie NAT (Network Address Translation) IDS (Intrusion Detection System) oder auch Virenscannern.

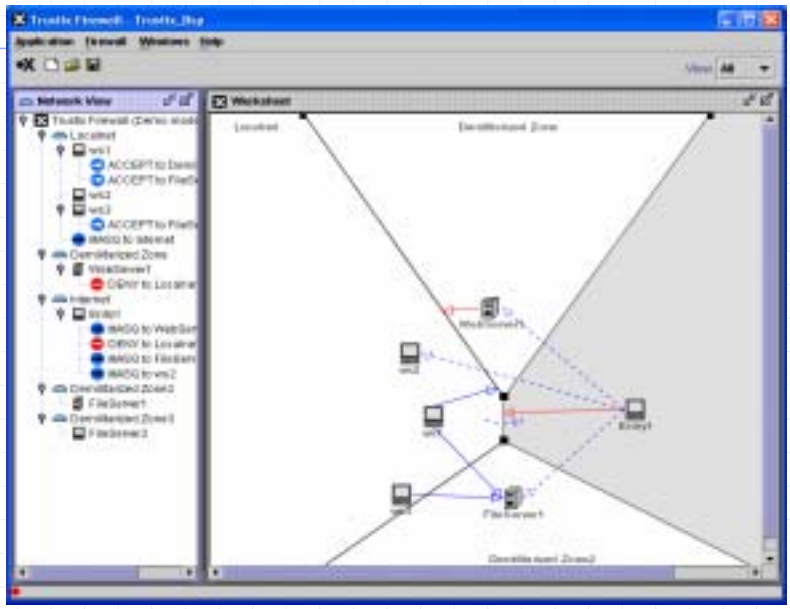
Darüber hinaus gibt es Hardware, die noch weitere Funktionen beherrscht, hHier z.B. links oben ein Gerät von Cisco, welches Routing- und Firewall-Funktionen übernimmt.

Produkt, welches gleich auf dem Rechner des Anwenders selbst installiert wird:

•Personal Firewall

Diese wurden in letzter Zeit populär, weil sie es dem einzelnen Benutzer erlauben, sich gegen Attacken aus dem Internet zu schützen. Gerade für den Heim-Anwender ist dies nützlich, den oft wird er durch seinen Provider nicht geschützt, oder nur gegen Aufpreis.

Arten der Umsetzung (2)



Beispiel einer graphischen Oberfläche zur Konfiguration einer Software-Lösung (Trustix Firewall):

Die einzelnen Teilnetze werden in Zonen eingeteilt, die Regeln zur Filterung können durch Pfeile zwischen Rechnern oder Teilnetzen intuitiv dargestellt werden.

Arten der Umsetzung (3)

16 ACCEPT	15 udp	------	123.123.121.123	eth0	123.123.123.125	137:139 -> *
17 ACCEPT	15 udp	------	123.123.121.123	eth0	123.123.123.125	445 -> *
18 DENY	tcp	------	123.123.122.123	eth0	20.0.0.0/16	* -> *
19 ACCEPT	tcp	------	123.123.123.123	eth2	20.1.0.0/16	* -> *
20 ACCEPT	tcp	------	123.123.123.123	eth3	123.123.121.123	* -> 53
21 ACCEPT	tcp	------	123.123.123.123	eth3	123.123.121.123	1024:65535 -> 1352
22 ACCEPT	tcp	------	123.123.123.123	eth3	123.123.121.123	* -> 137:139
33 ACCEPT	35 udp	------	123.123.123.125	eth3	123.123.121.123	* -> 137:139
34 ACCEPT	35 udp	------	123.123.123.125	eth3	123.123.121.123	* -> 445
35 ACCEPT	udp	------	123.123.123.125	eth3	123.123.121.123	* -> *
36 DENY	tcp	------	123.123.125.123	eth0	20.0.0.0/16	* -> *
37 MASQ	tcp	------	123.123.125.123	eth3	123.123.121.123	* -> 53
38 MASQ	tcp	------	123.123.125.123	eth3	123.123.121.123	1024:65535 -> 1352
39 MASQ	tcp	------	123.123.125.123	eth3	123.123.121.123	* -> 137:139
40 MASQ	tcp	------	123.123.125.123	eth3	123.123.121.123	* -> 445
41 MASQ	44 udp	------	123.123.125.123	eth3	123.123.121.123	* -> 53
47 MASQ	tcp	------	123.123.125.123	eth2	123.123.122.123	1024:65535 -> 21
48 MASQ	tcp	------	123.123.125.123	eth2	123.123.122.123	1024:65535 -> 23
…	…	…		…		…

Fortsetzung (Trustix Firewall):

Falls die graphische Konfiguration nicht ausreicht, um gewisse Regeln darzustellen, kann der erfahrene Benutzer auch direkt an den Filterregeln Hand anlegen.

Fallstudie, Teil 2

Aufgaben

1. Vergleichen Sie die vorliegende Topologie der bestehenden Firewalllösung im KliniX-Netzwerk mit dem Anforderungsprofil. Erfüllt das Netzwerk die Anforderungen des Profils? Beurteilen Sie insbesondere die Kriterien
   - Stärke des Schutzes
   - Untergliederung in unterschiedliche Schutzzonen
   - Angreifbarkeit der Firewall selbst.

   Welche Änderungen würden Sie allenfalls vorschlagen?
2. Wo liegen die Schwächen der – allenfalls durch Ihre Änderungen ergänzten – Firewalllösung? Mit welchen Arten von Bedrohung kann diese Firewall nicht umgehen?

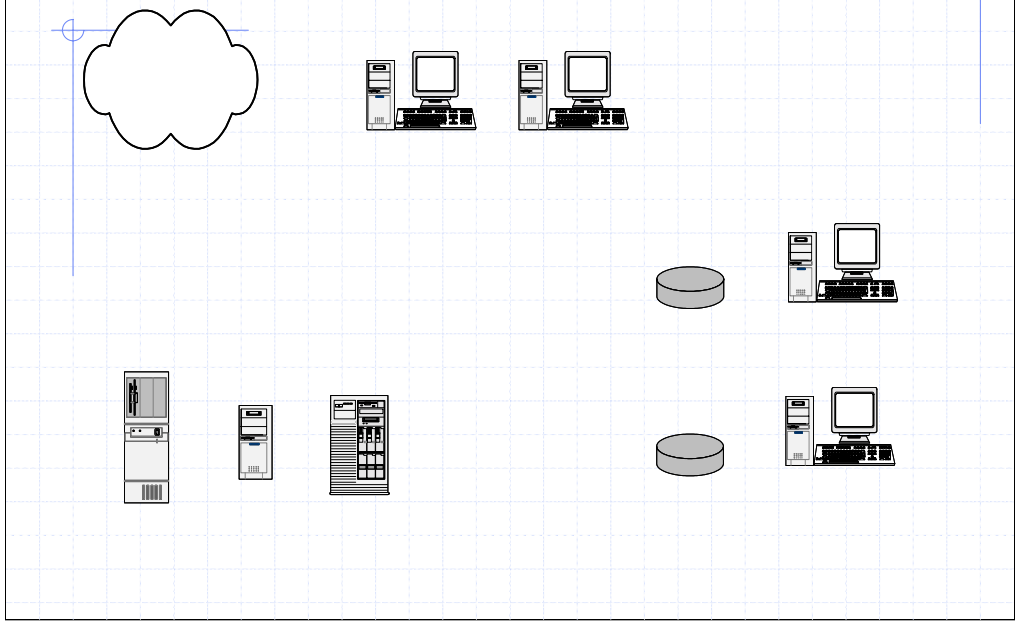
Gruppenarbeit: Je nach Anordnung im Klassenzimmer bilden 3 bis maximal 4 Personen jeweils eine Gruppe zur Bearbeitung der Fallstudie.

Bekannt geben:

•Dauer der Bearbeitungszeit (25 Minuten)

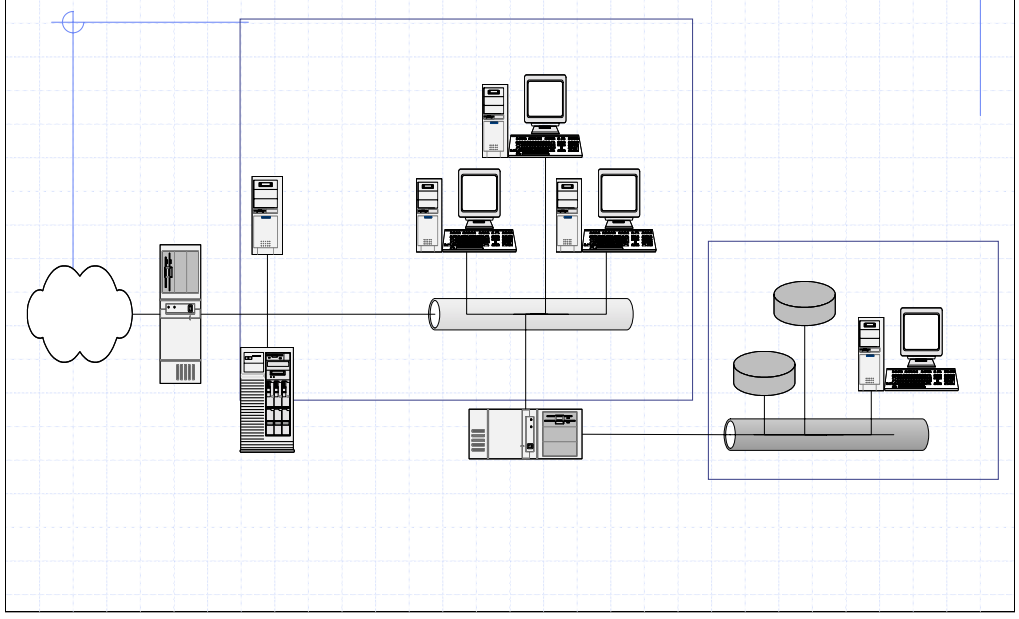
•Danach erfolgt eine Besprechung / Diskussion im Plenum (10 – 20 Minuten).

Fallstudie, Teil 2: Lösungsblatt



Internet

Fallstudie, Teil 2: Variante 1

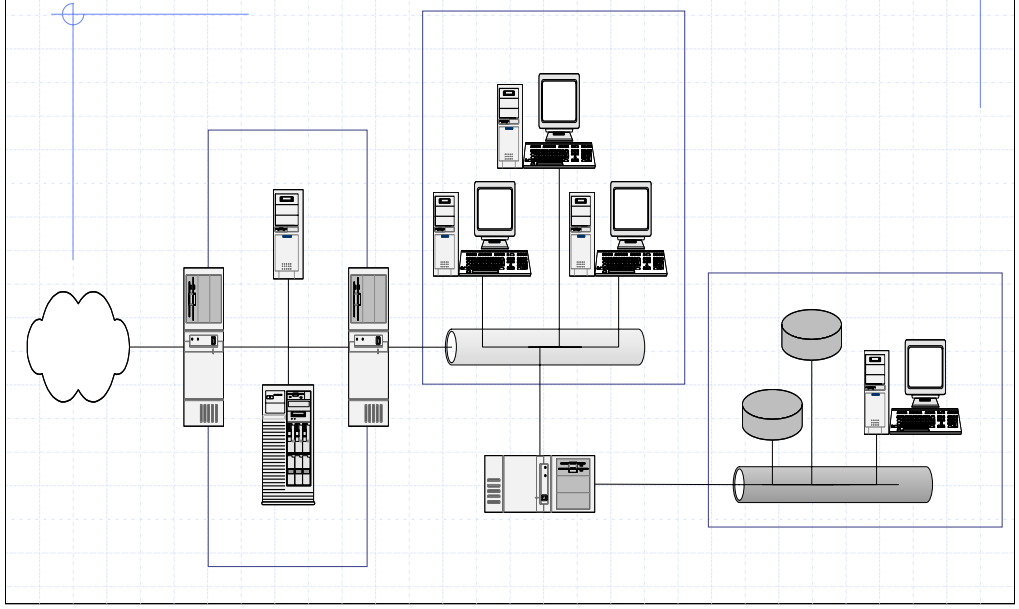


Ir

Paketfilter

Internet

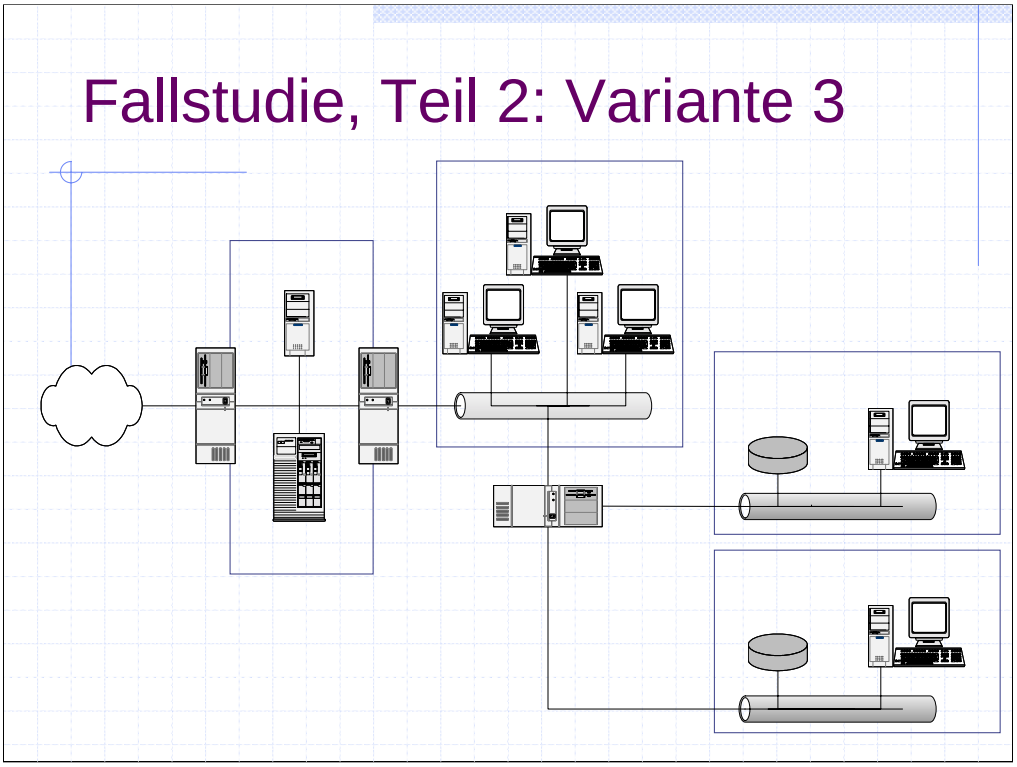
Fallstudie, Teil 2: Variante 2



Paketfilte

Internet

Fallstudie, Teil 2: Variante 3



Paketfil

Internet

Informationsquellen (Auswahl)

Bücher:

- N. Pohlmann, Firewallsysteme, 3. Aufl., Bonn, MITP-Verlag, 2000, ISBN 3-8266-4075-6
- W. Stallings, Network Security Essentials, Prentice-Hall, 2000
- M. Raepple, Sicherheitskonzepte für das Internet, Heidelberg, dpunkt-Verl. 2001
- W. Barth, Das Firewall Buch, Nürnberg, SuSE-Press, 2001, (speziell zu Linux),
- B. Chapman, E. Zwicky, Building Internet Firewalls, O'Reilly & Associates, 1995
- W. Cheswick, S. Bellovin, Firewalls and Internet Security, Addison- Wesley, 1994
- B. Plattner, ETH Zürich, Skript zu IT-Security, Wintersemester 2001
- K. Fuhrberg, D.Hager, S. Wolf, Internet-Sicherheit, Carl Hanser Verlag, 2001

Links:

- http://www.bsi.de/ — Deutsches Bundesamt für Sicherheit in der Informationstechnik
- http://www.cert.org/other_sources/ — Guter Einstieg zu diversen weiterführenden Quellen
- http://www.it-secure-x.de/ — Allerhand Wissenswertes zum Thema IT-Security in deutscher Sprache

Hersteller:

- http://www.symantec.com/
- http://www.cisco.com/go/pix
- http://www.sophiafirewall.com/

Zusammenfassung:

- Verschiedene Stufen der Sicherheit werden erreicht durch
  - verschiedene Mechanismen:
    Paket Filter, Application Gateways
  - verschiedenartige Kaskadierung der Sicherheitsmechanismen
- Es gibt immer einen Trade-Off für die Sicherheit.