Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Firewall-Systeme

Firewall-Elemente

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.

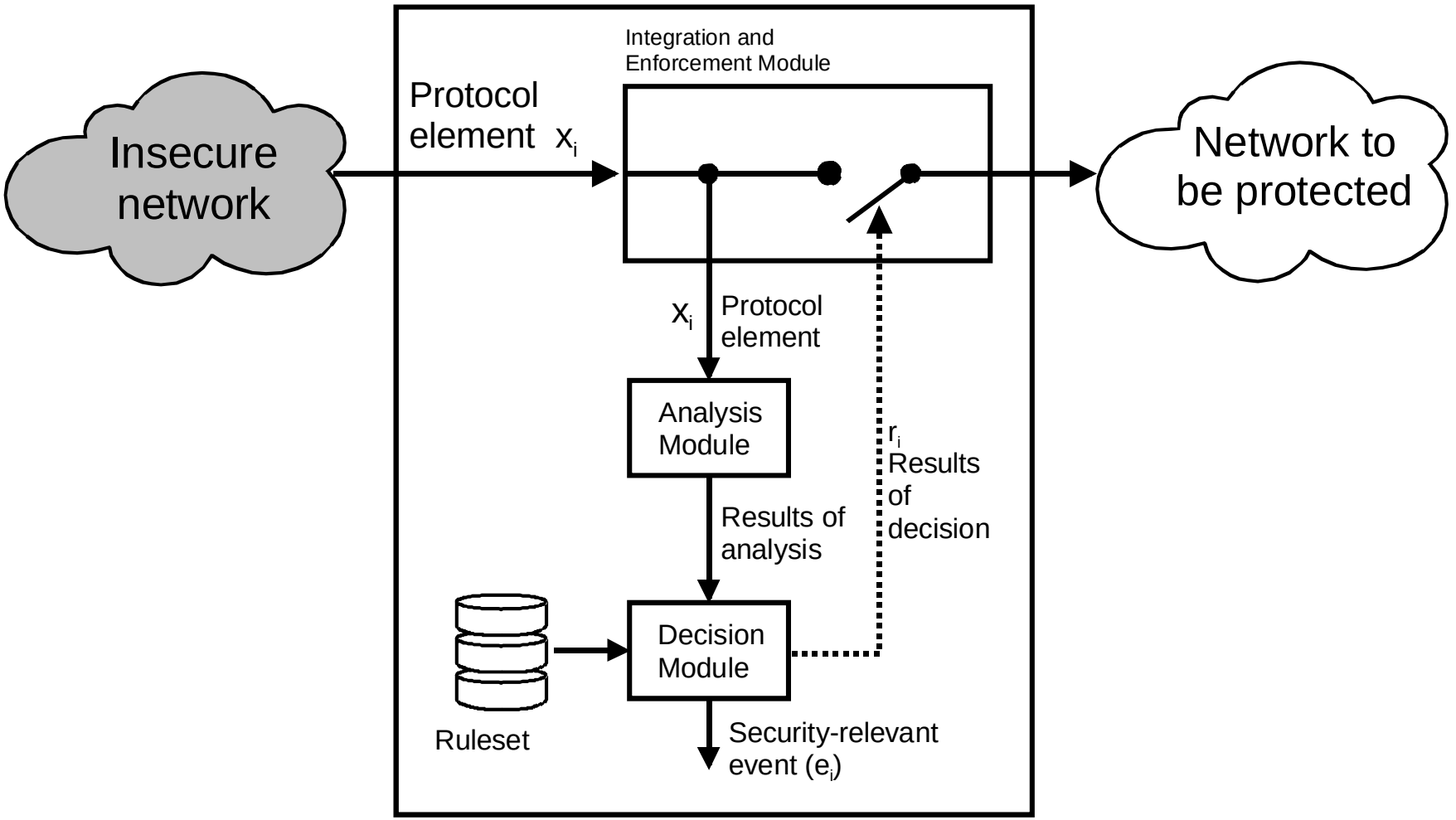
Inhalt

- Definition eines Firewall-Elements
- Packet Filter
- zustandsorientierter Packet Filter
- Application Gateway
- Adaptive Proxy
- Firewall-Elemente im Verhältnis zu Schnelligkeit und Sicherheit

Inhalt

- **Definition eines Firewall-Elements**
- Packet Filter
- zustandsorientierter Packet Filter
- Application Gateway
- Adaptive Proxy
- Firewall-Elemente im Verhältnis zu Schnelligkeit und Sicherheit

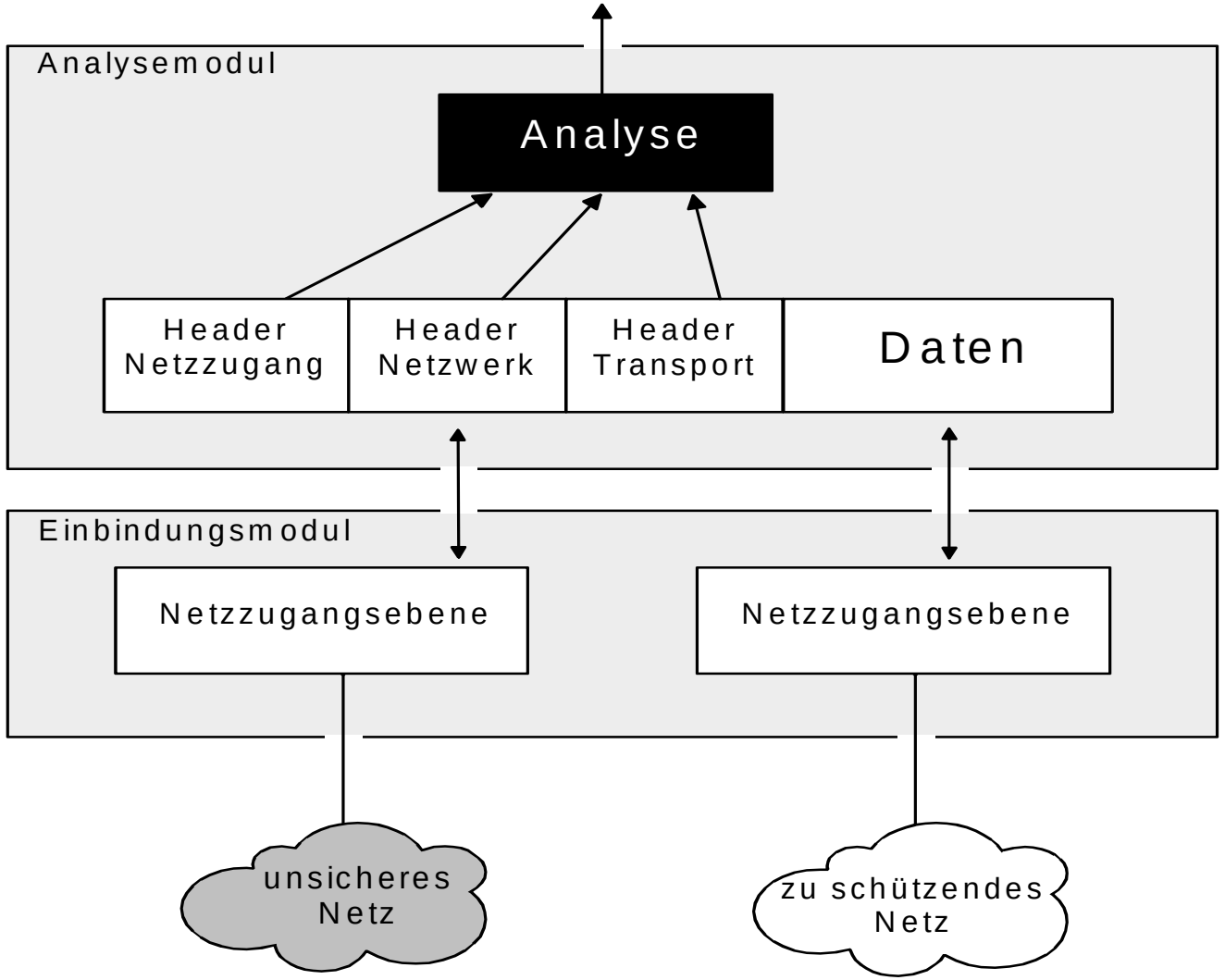
Definition eines Firewall-Elements



Inhalt

- Definition eines Firewall-Elements
- **Packet Filter**
- zustandsorientierter Packet Filter
- Application Gateway
- Adaptive Proxy
- Firewall-Elemente im Verhältnis zu Schnelligkeit und Sicherheit

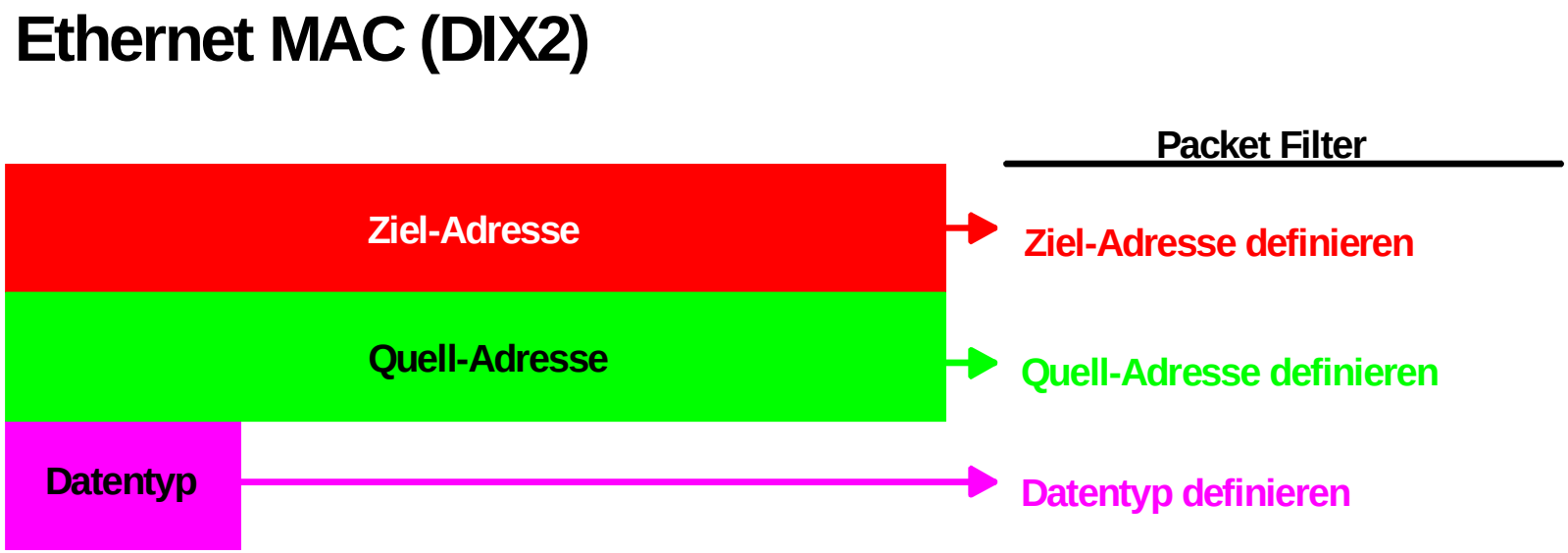
Allgemeine Arbeitsweise
→ Packet Filter



Analogie zum Pförtner
→ Paket Filter

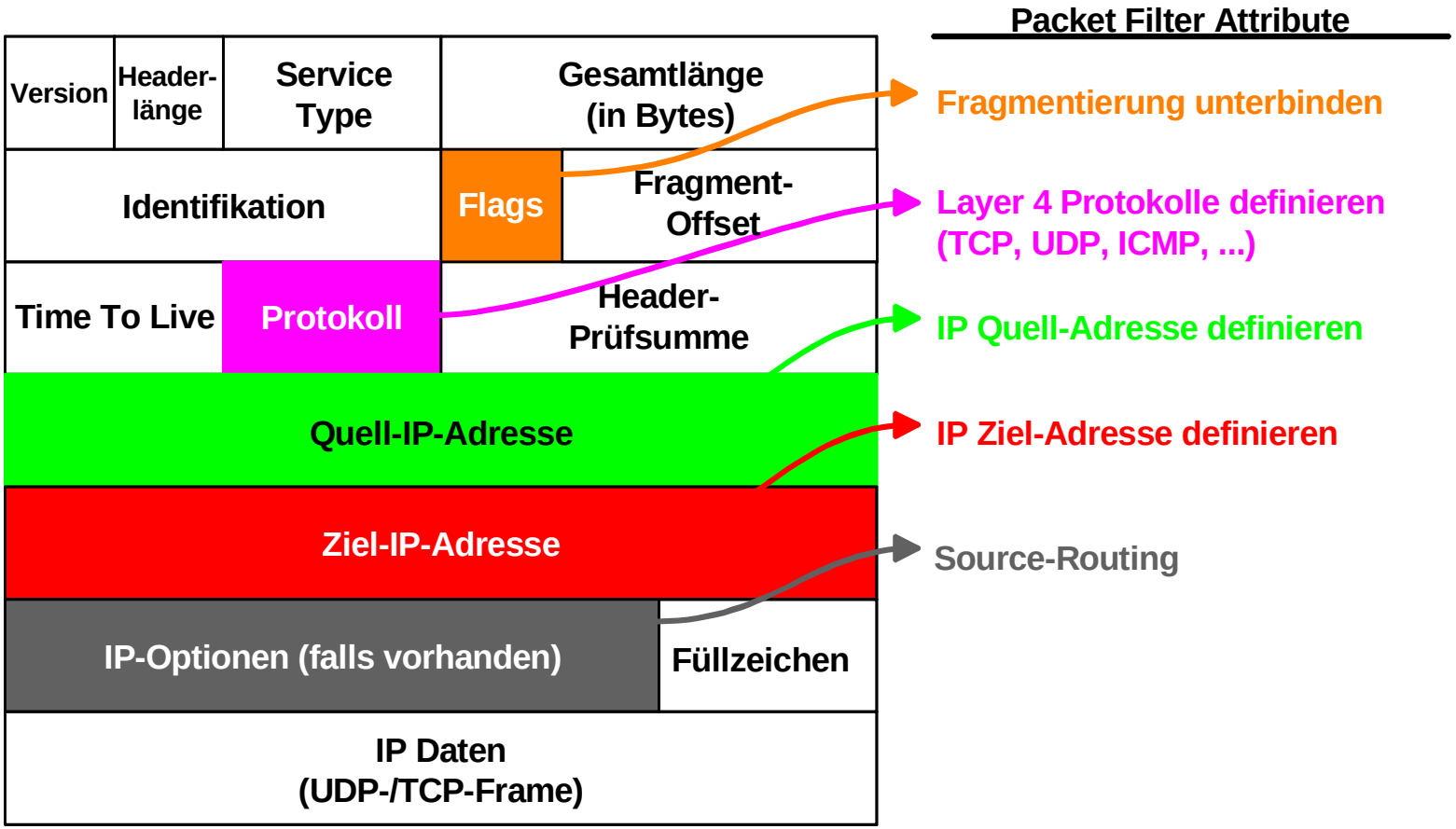
- Wenn der LKW eines Lieferanten am Werktor mit einer Lieferung vorfährt, schaut der “Packet-Filter-Pförtner” auf das Logo an der Seite des LKWs, um zu überprüfen, ob es ihm bekannt ist, und läßt den LKW gegebenenfalls unmittelbar durch das Tor, ohne den Lieferschein zu kontrollieren.

Analysemöglichkeit
→ Ethernet: MAC Frames (z.B. DIX 2)



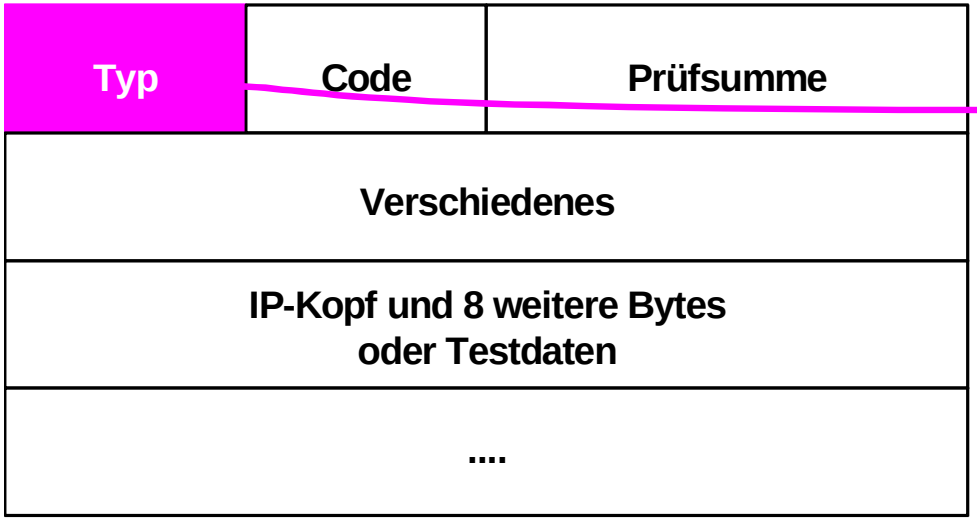
Analysemöglichkeit → IP-Frame

IP-Frame



Analysemöglichkeit
→ ICMP-Frame

ICMP

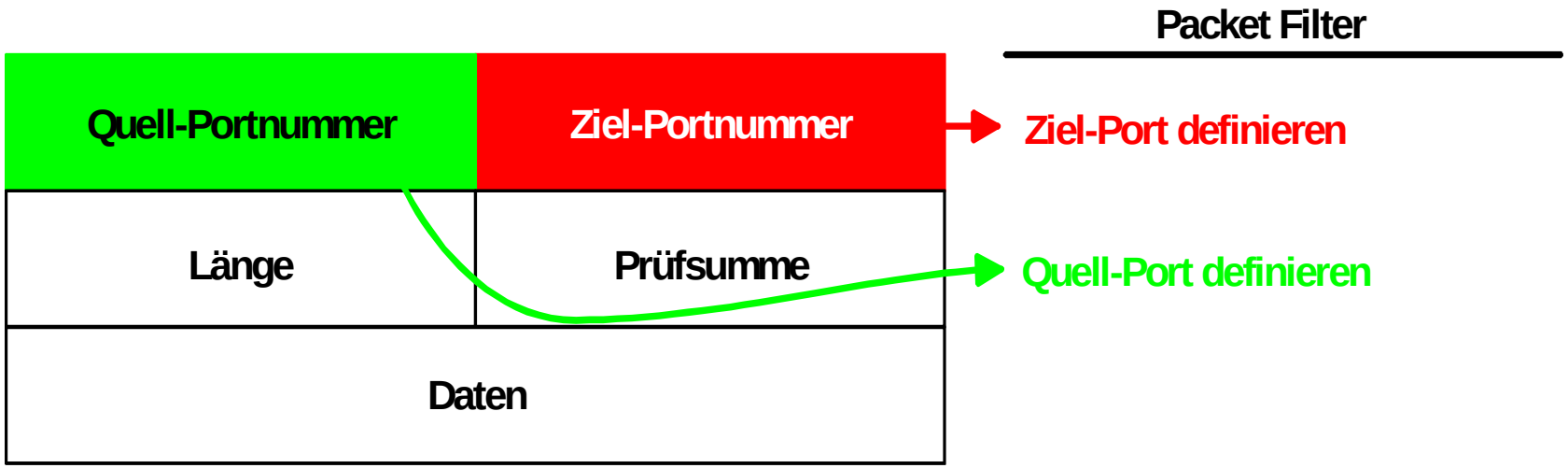


Packet Filter

Kommando
- Echo Request
- Echo Reply
- Redirect (anderen Weg nehmen)

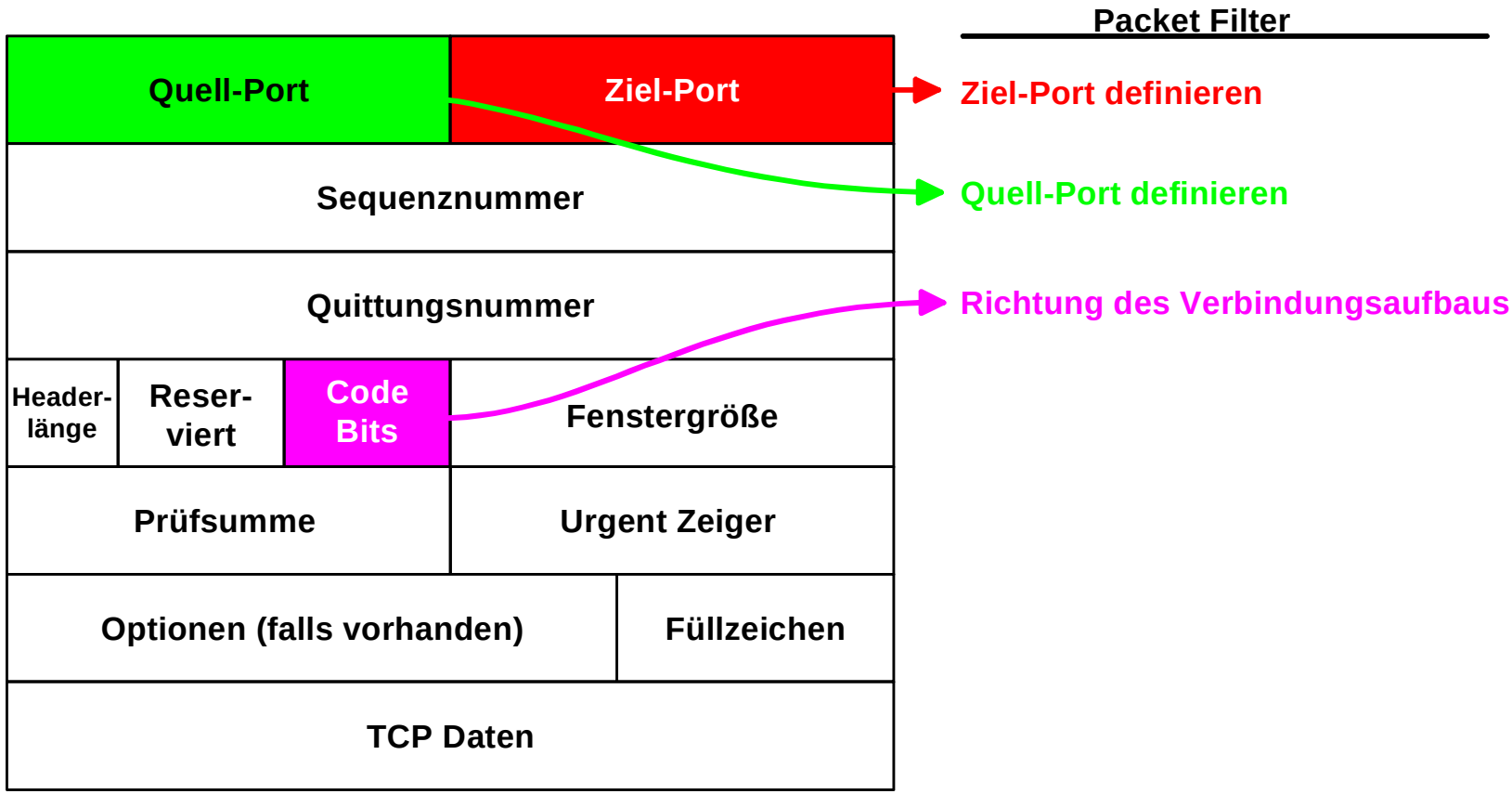
Analysemöglichkeit
→ UDP-Frame

UDP-Frame

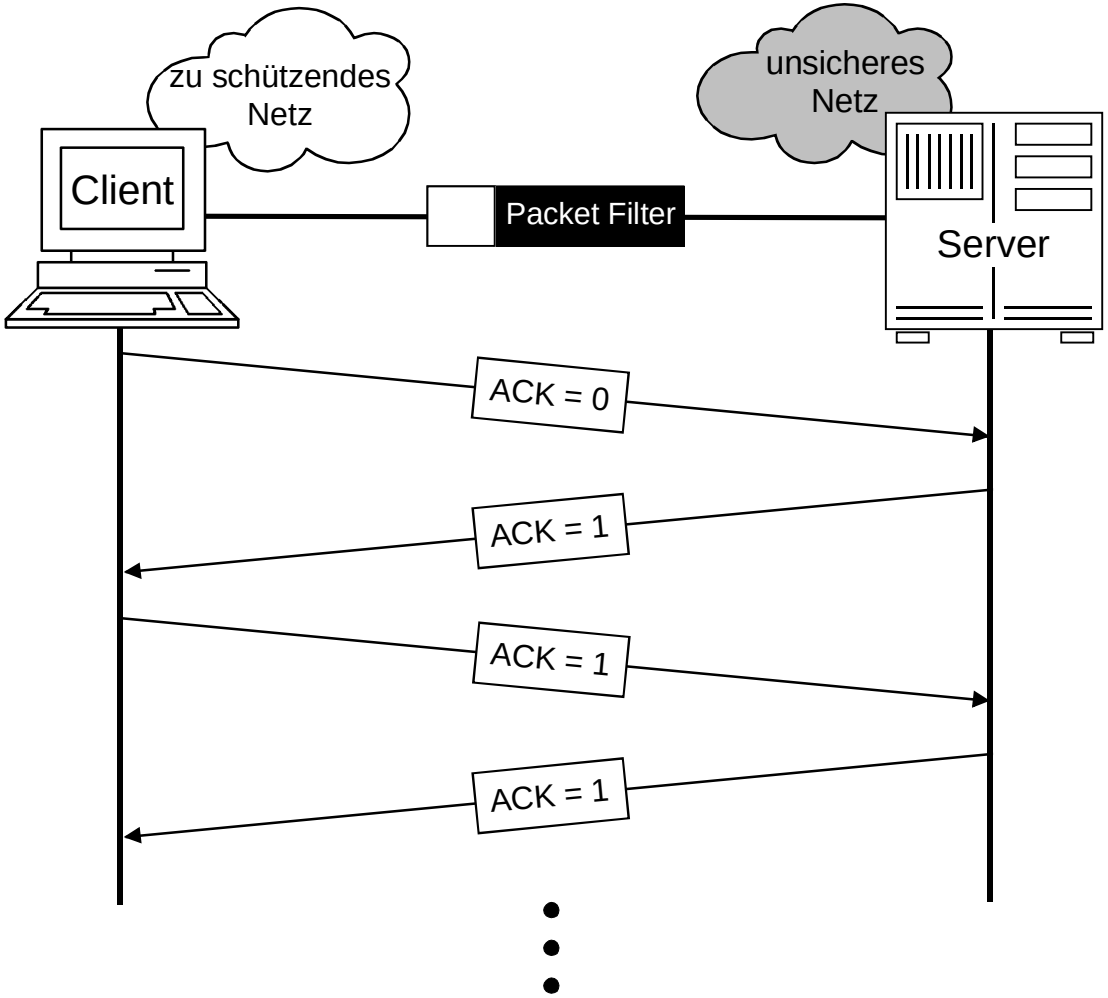


Analysemöglichkeit → TCP-Frame

TCP-Frame



Überprüfung des Verbindungsaufbaus



- Bei TCP wird beim Verbindungsaufbau das ACK=0 gesetzt, dadurch kann ein Packet Filter den Verbindungsaufbau kontrollieren

TCP - Transmission Control Protocol
→ Beispiel - Verbindungsaufbau

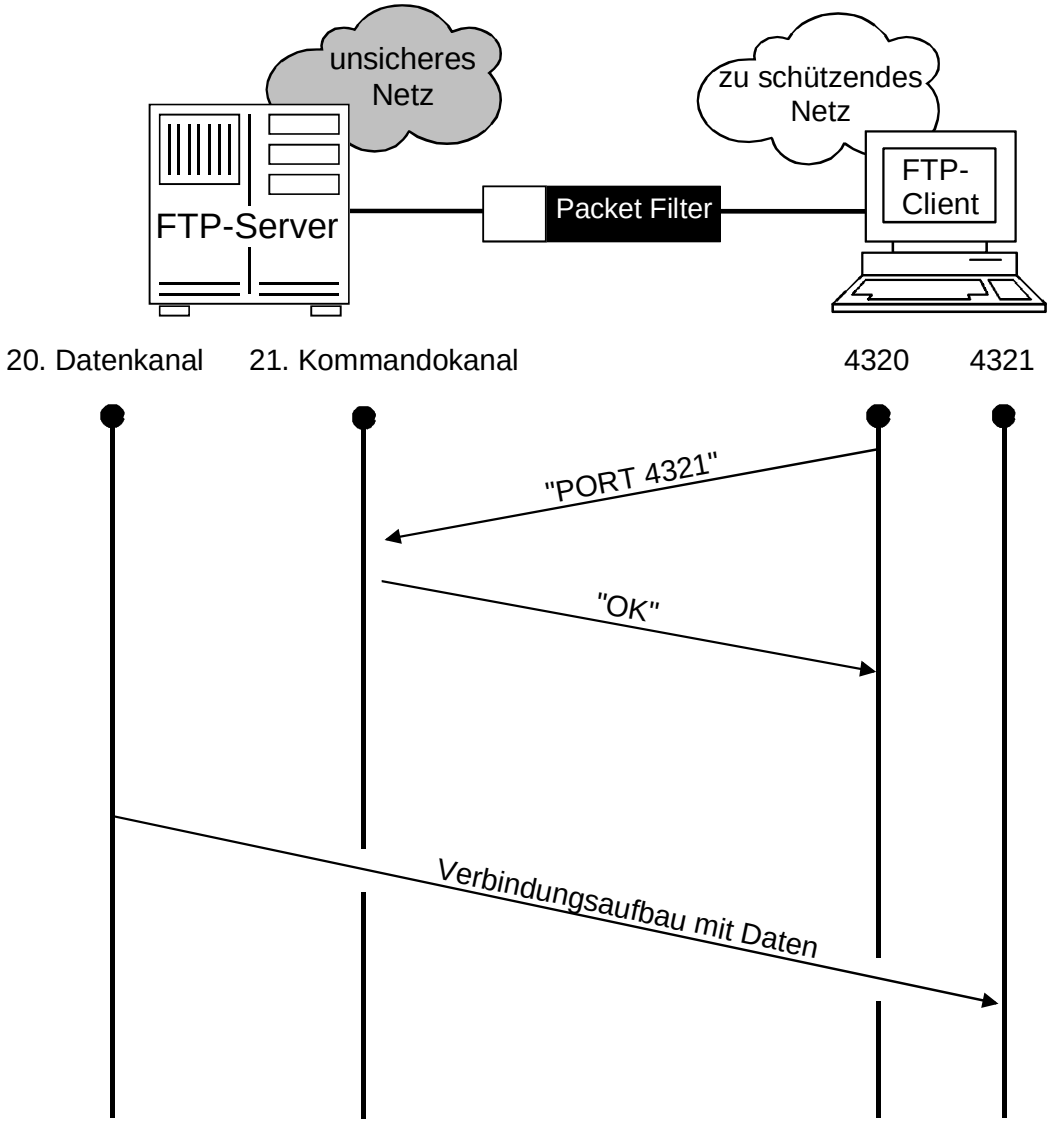
Nr. 134 Transmission Control Protocol, Src Port: 3606 (3606), Dst Port: http (80), Seq: 61094067, Ack: 0, Len: 0
- Source port: 3606 (3606)
- Destination port: http (80)
- Sequence number: 61094067
- **Header length: 28 bytes**
- **Flags: 0x0002 (SYN)**
  - 0... .... = Congestion Window Reduced (CWR): Not set
  - .0.. .... = ECN-Echo: Not set
  - ..0. .... = Urgent: Not set
  - ...0 .... = Acknowledgment: Not set
  - .... 0... = Push: Not set
  - .... .0.. = Reset: Not set
  - .... ..1. = Syn: Set
  - ....0 = Fin: Not set
- Window size: 64240
- Checksum: 0x38e9 (correct)
- Options: (8 bytes)
  - **Maximum segment size: 1460 bytes**
  - NOP
  - NOP
  - SACK permitted

Nr. 148 Transmission Control Protocol, Src Port: http (80), Dst Port: 3606 (3606), Seq: 3740935862, Ack: 61094068, Len: 0
- Source port: http (80)
- Destination port: 3606 (3606)
- Sequence number: 3740935862
- Acknowledgement number: 61094068
- **Header length: 28 bytes**
- **Flags: 0x0012 (SYN, ACK)**
  - 0... .... = Congestion Window Reduced (CWR): Not set
  - .0.. .... = ECN-Echo: Not set
  - ..0. .... = Urgent: Not set
  - ...1 .... = Acknowledgment: Set
  - .... 0... = Push: Not set
  - .... .0.. = Reset: Not set
  - .... ..1. = Syn: Set
  - ....0 = Fin: Not set
- Window size: 15466
- Checksum: 0xf1e3 (correct)
- Options: (8 bytes)
  - **Maximum segment size: 1406 bytes**
  - NOP
  - NOP
  - SACK permitted

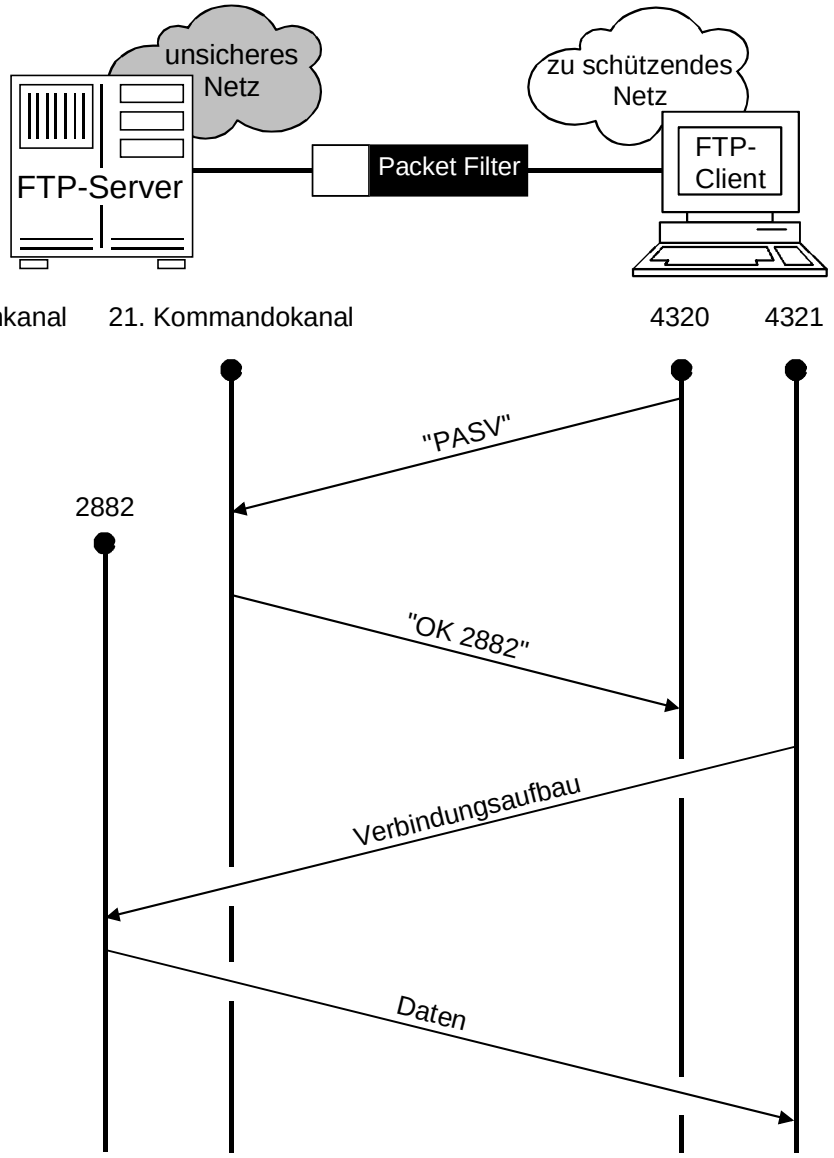
Nr. 149 Transmission Control Protocol, Src Port: 3606 (3606), Dst Port: http (80), Seq: 61094068, Ack: 3740935863, Len: 0
- Source port: 3606 (3606)
- Destination port: http (80)
- Sequence number: 61094068
- Acknowledgement number: 3740935863
- Header length: 20 bytes
- **Flags: 0x0010 (ACK)**
  - 0... .... = Congestion Window Reduced (CWR): Not set
  - .0.. .... = ECN-Echo: Not set
  - ..0. .... = Urgent: Not set
  - ...1 .... = Acknowledgment: Set
  - .... 0... = Push: Not set
  - .... .0.. = Reset: Not set
  - .... ..0. = Syn: Not set
  - ....0 = Fin: Not set
- Window size: 64676
- Checksum: 0x5e37 (correct)

Dienste: FTP (Beispiel - Verbindungsaufbau) → Datentransfer bei FTP: ACTIVE MODE

- **Problem:**
  es muss für TCP-Verbindungen ein Verbindungsaufbau aus dem unsicheren Netz ermöglicht werden
- Dies ist **sicherheitskritisch!**

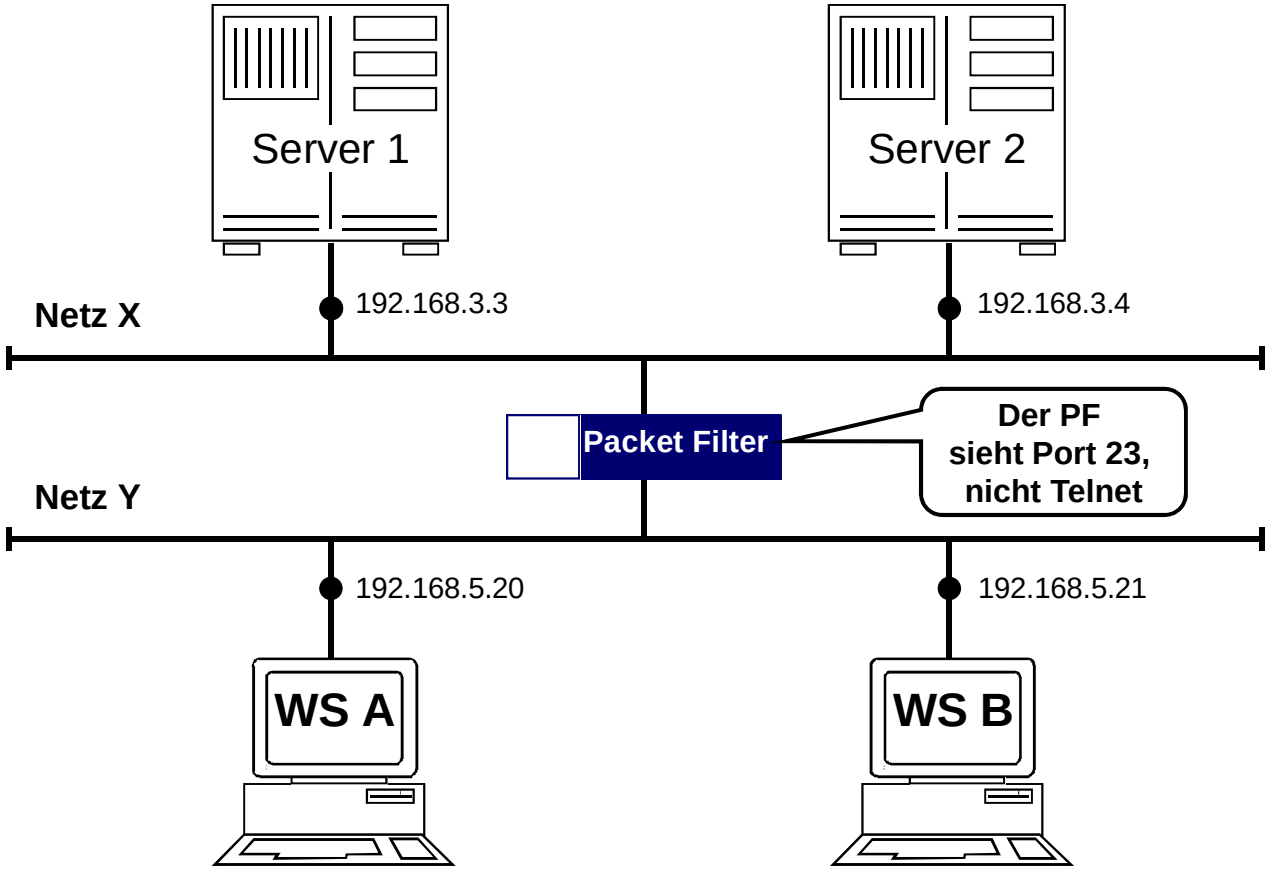


Dienste: FTP (Beispiel - Verbindungsaufbau) → Datentransfer bei FTP: PASSIVE MODE



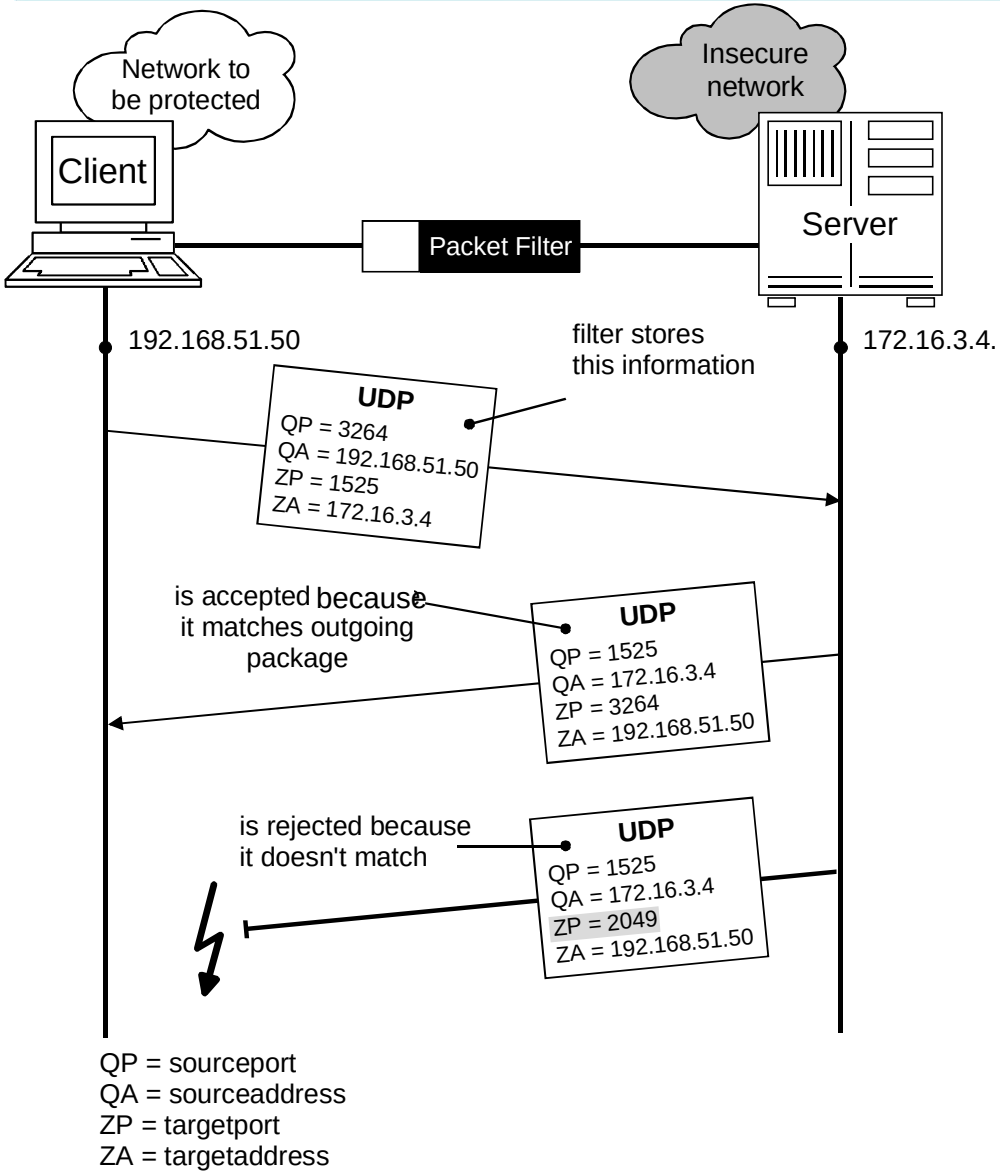
- **Der „Passive Mode“ ist zu bevorzugen**, da hier die Verbindung aus dem sicheren Netz definiert und aufgebaut wird!

Beispiel für den Einsatz eines Packet Filter → Telnet-Session über Port 23



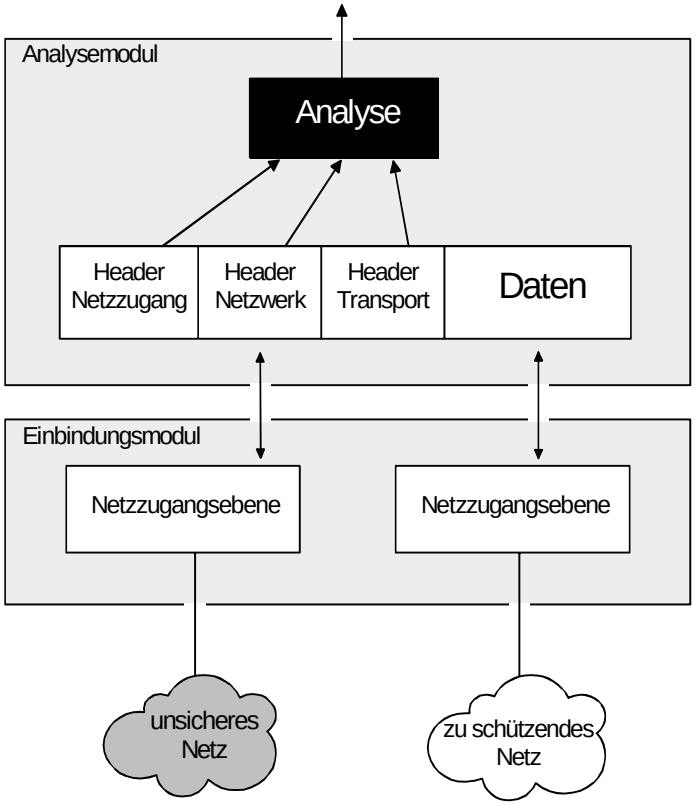
- Der **Packet-Filter ist nicht in der Lage festzustellen**, ob wirklich eine **Telnet-Session** oder eine andere Anwendung über den Post 23 gefahren wird!

Dynamischer Packet Filter
→ Beispiel: UDP



- Dynamische Packet Filter besitzen im Fall der Verwendung des UDP-Protokolls ferner die Eigenschaft, sich für nach “außen” geschickte UDP-Pakete die IP-Adressen und Ports der Quelle und des Ziels zu merken, und nur die entsprechenden passenden“Antworten” der virtuellen Verbindung zu erlauben.

Bewertung:
→ Packet Filter



Möglichkeiten

- transparent, unsichtbar
- einfach erweiterungsfähig für neue Protokolle und Dienste
- für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA, ...)
- hohe Performance

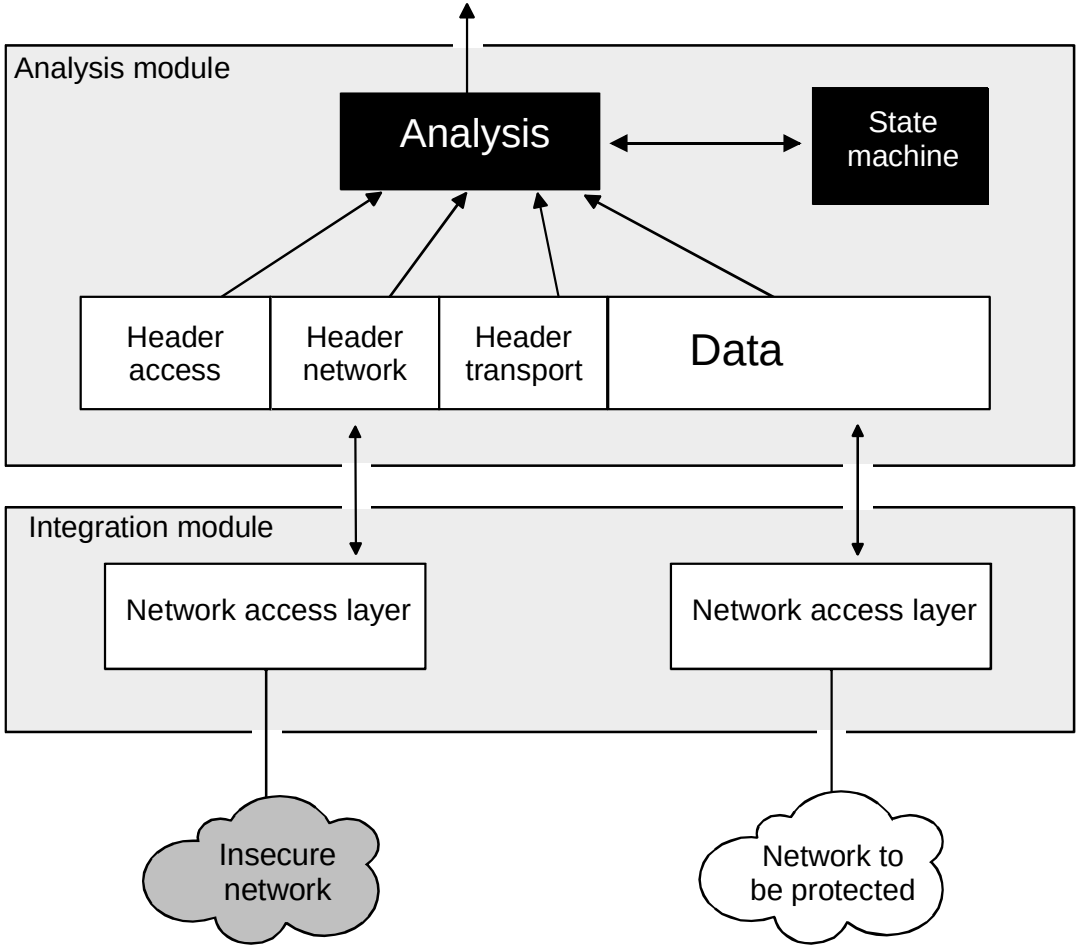
Grenzen

- keine Analyse oberhalb der Transportebene
- keine Separierung der Netzwerke
- die Struktur des Netzes wird nicht verborgen
- es werden nur die Ports überprüft, nicht die Anwendungen

Inhalt

- Definition eines Firewall-Elements
- Packet Filter
- **zustandsorientierter Packet Filter**
- Application Gateway
- Adaptive Proxy
- Firewall-Elemente im Verhältnis zu Schnelligkeit und Sicherheit

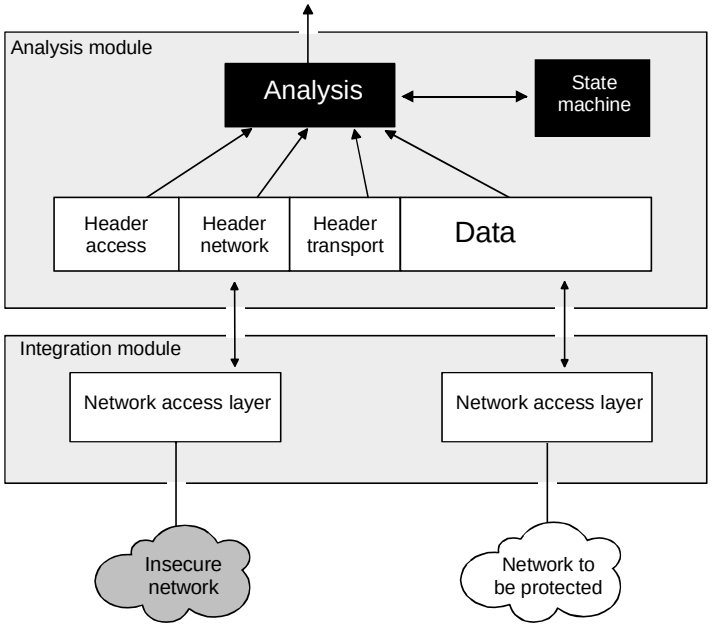
Allgemeine Arbeitsweise
→ zustandsorientierten Packet Filters



Analogie zum Pförtner
→ zustandsorientierten Paket Filter

- Wenn die Lieferung ankommt, dann schaut der Pförtner nicht nur auf die Adressen, sondern auch auf den Lieferschein, um zu überprüfen, ob in dem Paket etwas Verbotenes steckt.
- Das ist eine gute Überprüfung, jedoch nicht so sicher wie das tatsächliche Öffnen des Pakets und die Überprüfung des Inhaltes.
- Wenn das Paket akzeptabel aussieht, dann öffnet der Pförtner das Tor und gestattet dem Fahrer des LKWs die Zufahrt auf das Werksgelände.

Bewertung:
→ zustandsorientierter Packet Filter



Möglichkeiten

- transparent, unsichtbar
- einfach erweiterungsfähig für neue Protokolle und Dienste
- für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA, ...)

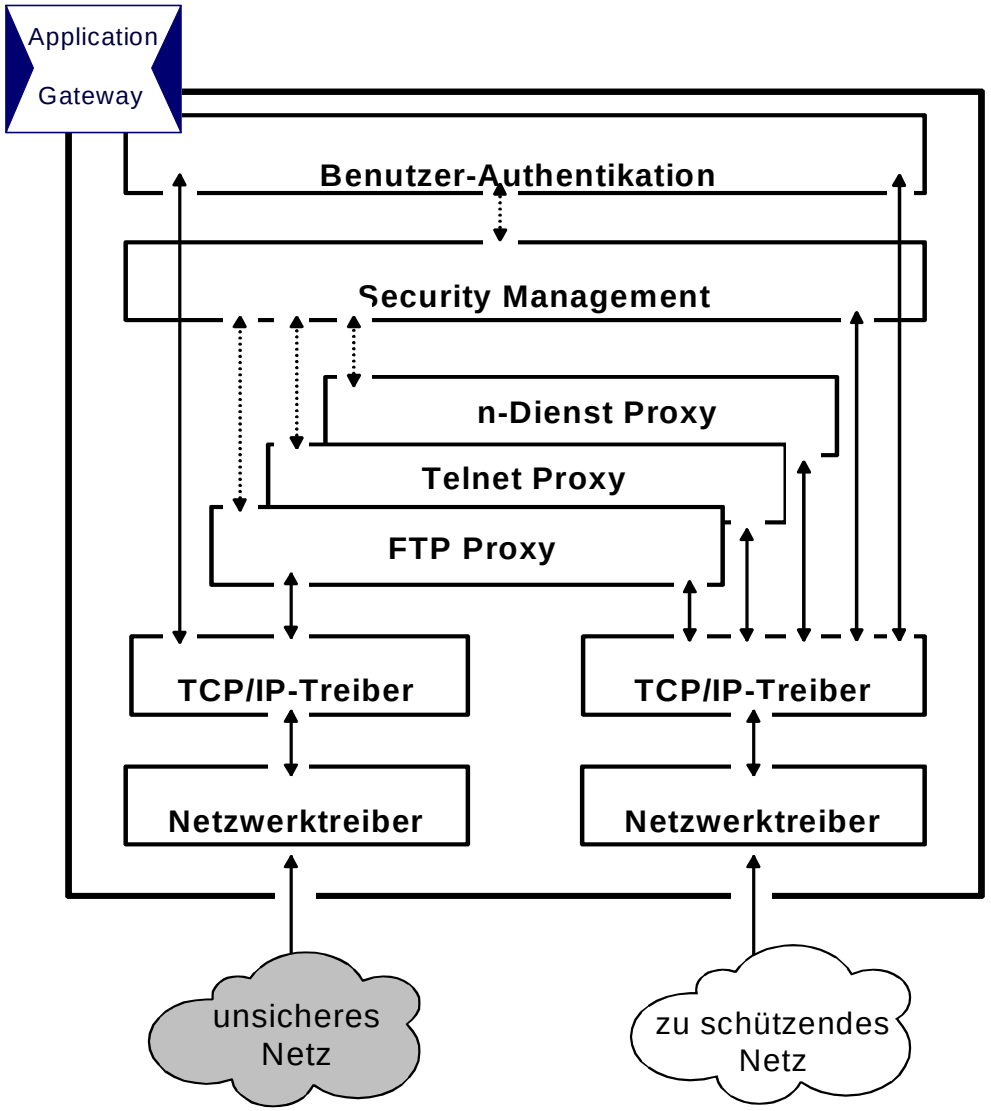
Grenzen

- **sehr komplexe Lösung**
  hohe Fehleranfälligkeit
- keine Separierung der Netzwerke
- die Struktur des Netzes wird nicht verborgen

Inhalt

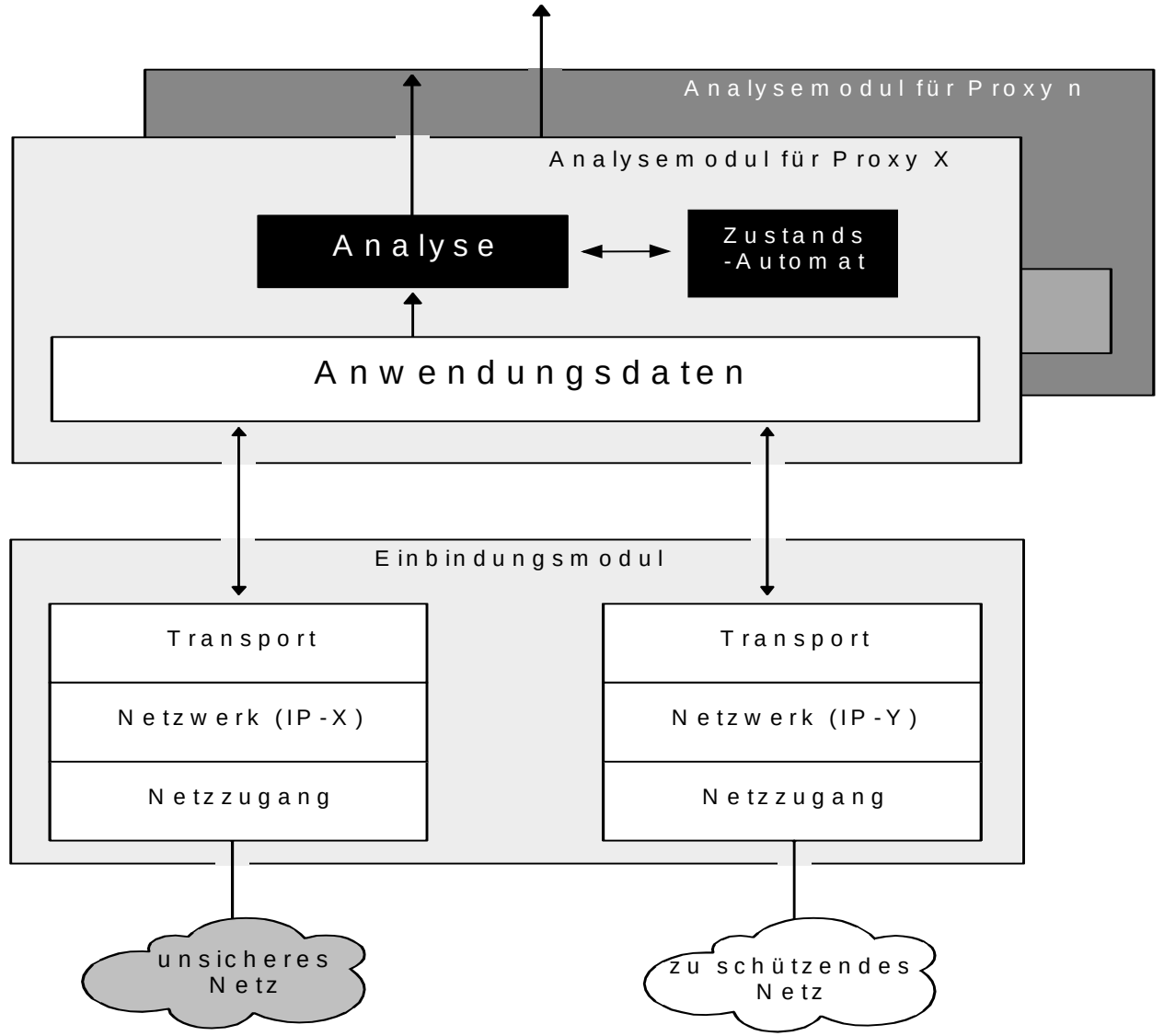
- Definition eines Firewall-Elements
- Packet Filter
- zustandsorientierter Packet Filter
- **Application Gateway**
- Adaptive Proxy
- Firewall-Elemente im Verhältnis zu Schnelligkeit und Sicherheit

Application Gateway



Application Gateway

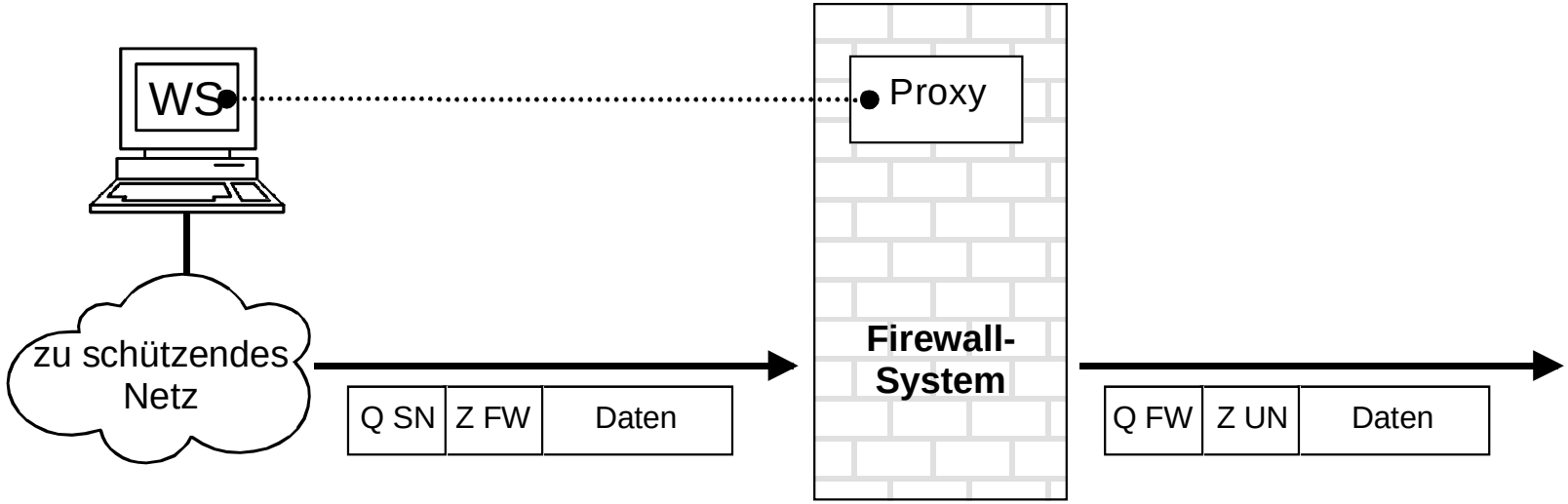
Analysemodule für Proxies
→ Application Gateway



Analogie zum Pförtner
→ Application Gateway

- Der “Application-Gateway-Pförtner” schaut nicht nur die Adressen der eingehenden Lieferungen an, er öffnet auch jedes Paket, prüft den kompletten Inhalt und checkt die Arbeitspapiere des Absenders gegen eine klar festgelegte Reihe von Beurteilungskriterien.
- Nach der erfolgten detaillierten Sicherheitsüberprüfung unterzeichnet der Pförtner den Lieferschein und schickt den LKW wieder auf seinen Weg.
- Stattdessen bestellt er einen vertrauenswürdigen Fahrer der eigenen Firma, der nun die Pakete zum eigentlichen Empfänger bringt.
- Die Sicherheitskontrolle ist an dieser Stelle wesentlich zuverlässiger und der Fahrer der Fremdfirma erhält keinen weiteren Einblick in das Firmengelände.
- Die Überprüfungen nehmen zwar mehr Zeit in Anspruch, dafür können jedoch auch mehr sicherheitsgefährdende Aktivitäten ausgeschlossen werden.

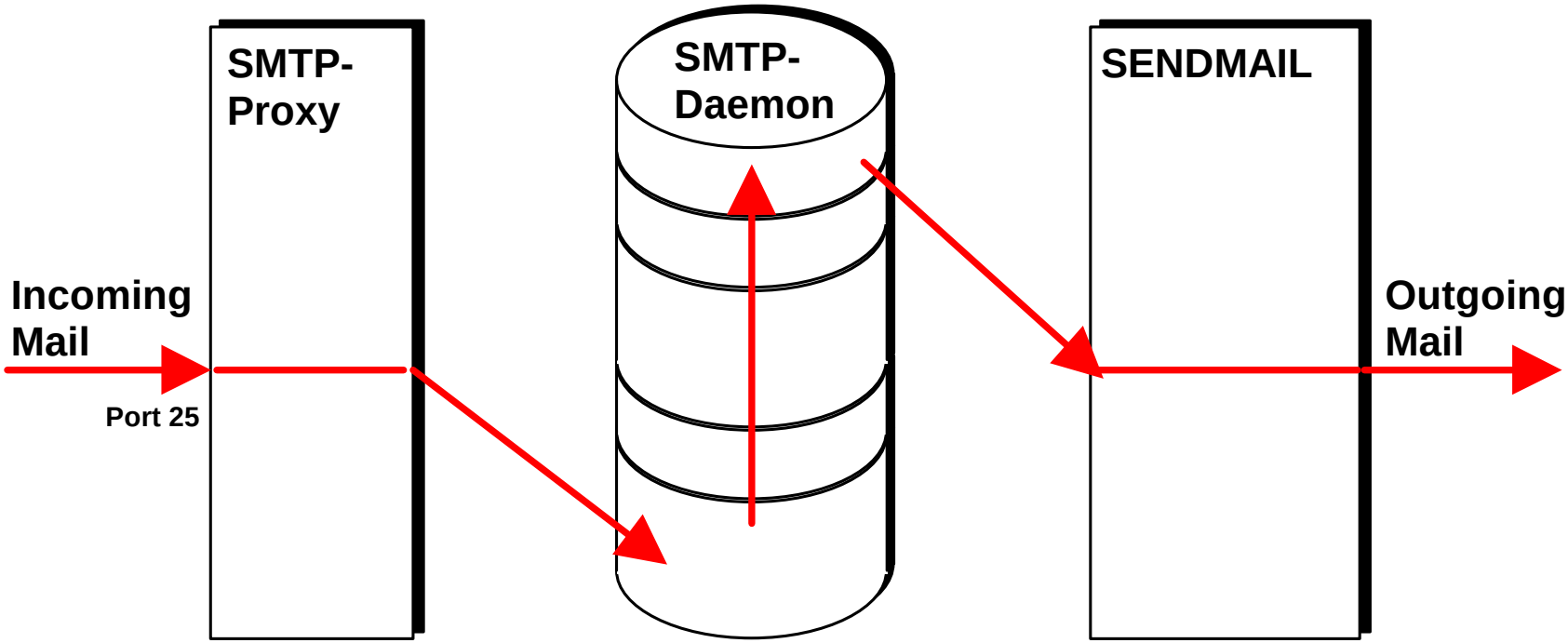
Firewall-System und Network Address Translation



Q SN: Quelladresse zu schützendes Netz
Z UN: Zieladresse unsicheres Netz
Q FW: Quelladresse Firewall-System
Z FW: Zieladresse Firewall-System

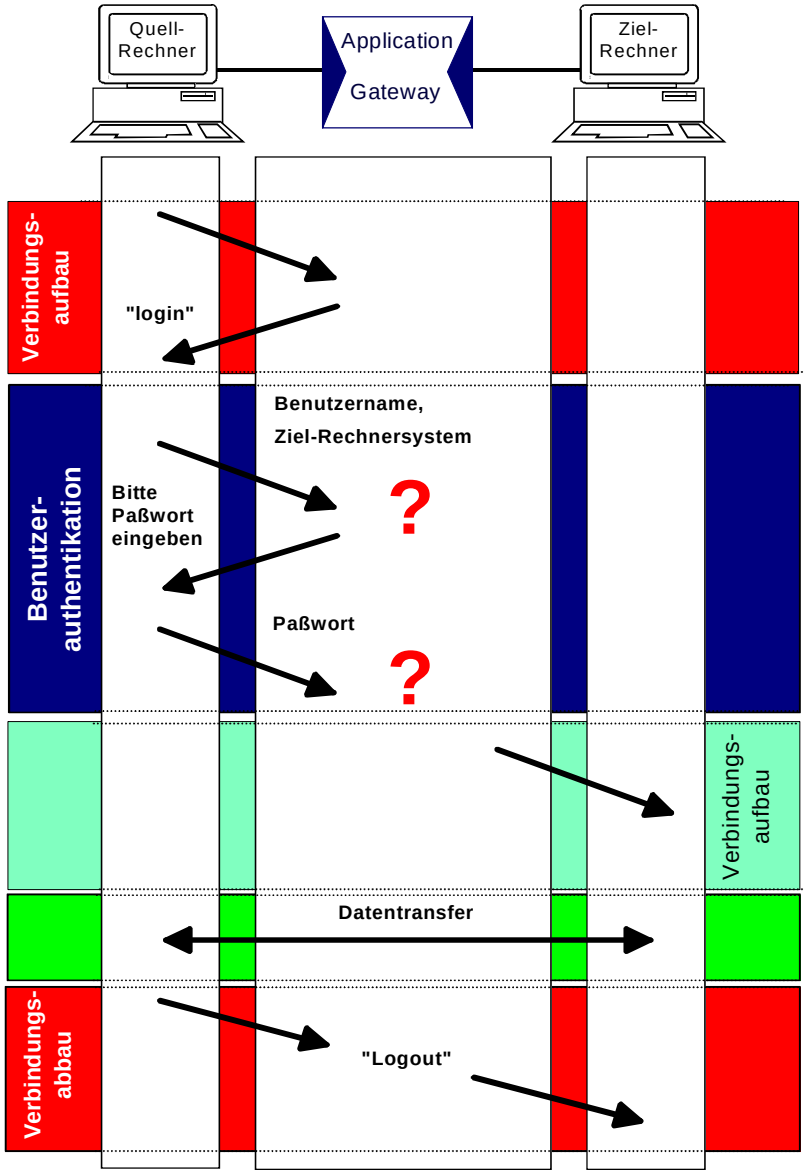
- Als Kommunikationspartner im zu schützenden Netz ist meist eine IP-Adresse aus dem reservierten IP-Adressbereich angegeben (Ziel-Adresse)
- Als Kommunikationspartner im unsicheren Netz ist meist eine offizielle Internet IP-Adresse angegeben (Quell-Adresse)
- Dadurch ist nicht erkennbar, welches Rechnersystem sich hinter der Kommunikation über das Firewall-System im zu schützenden Netz verbirgt.

SMTP Proxy
→ Analogie zum Sammelbriefkasten



- Eingehende Mail wird vom SMTP-Proxy entgegen genommen und abgelegt
- Der SMTP-Daemon überprüft zyklisch, ob Mail eingetroffen ist und startet ggf. sendmail bzw. alternativen MTA

Verbindungsaufbau
→ Application Gateway



Verbindungsaufbau
→ Application Gateway

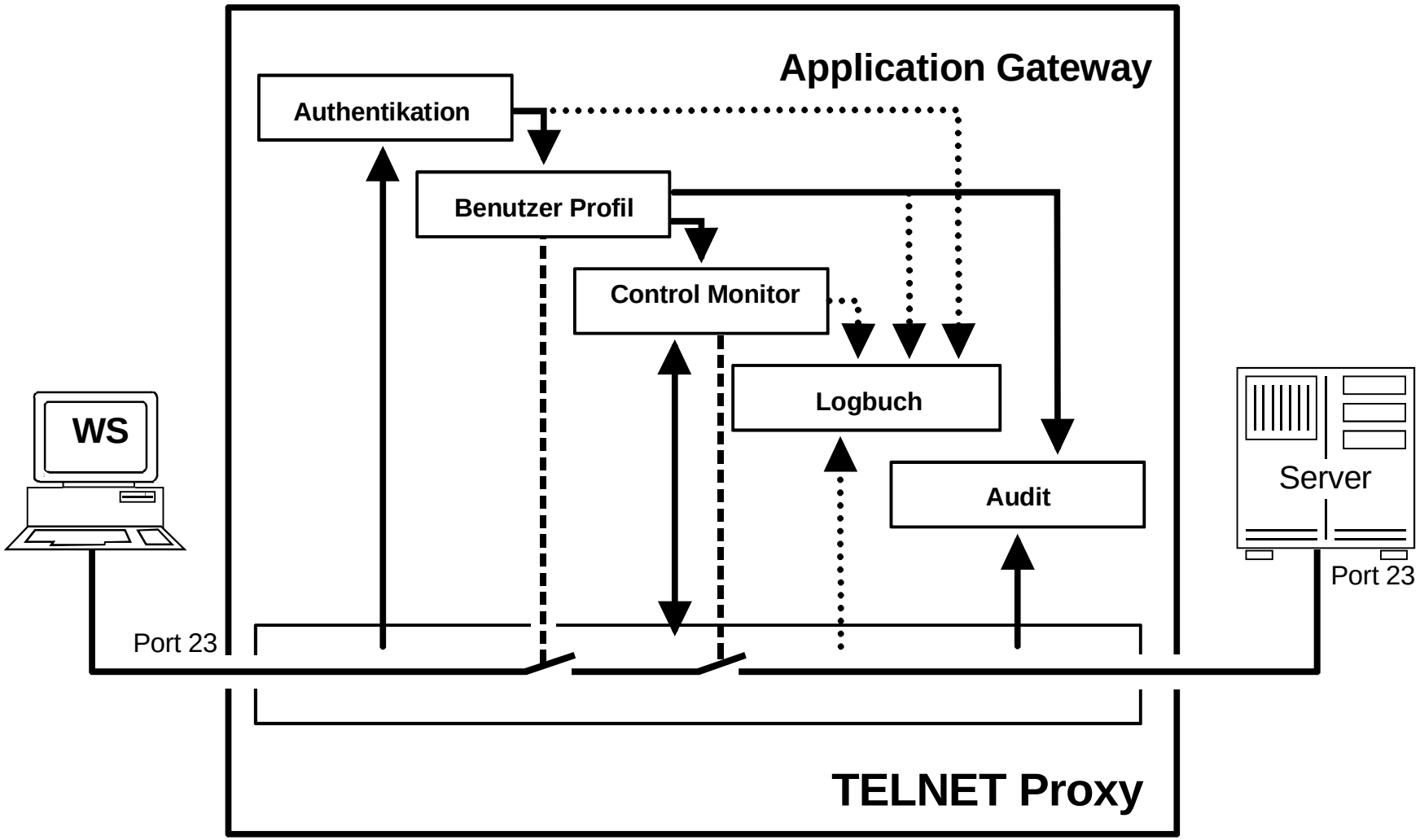
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.200.3	192.168.200.1	TCP	1040 > http [SYN] Seq=73524268 Ack=0 Win=8192 Len=0
2	0.000006	192.168.200.1	192.168.200.3	TCP	http > 1040 [SYN, ACK] Seq=512687201 Ack=73524269 Win=32120 Len=0
3	0.007049	192.168.200.3	192.168.200.1	TCP	1040 > http [ACK] Seq=73524269 Ack=512687202 Win=8760 Len=0
4	**0.063287**	**192.168.200.3**	**192.168.200.1**	**HTTP**	**GET http://www.compumatica.de/ HTTP/1.0**
5	0.067133	192.168.200.1	192.168.200.3	TCP	http > 1040 [ACK] Seq=512687202 Ack=73524588 Win=31801 Len=0
6	**0.278093**	**192.168.200.1**	**192.168.200.3**	**HTTP**	**HTTP/1.0 403 Forbidden**
7	0.278099	192.168.200.1	192.168.200.3	TCP	http > 1040 [FIN, ACK] Seq=512687731 Ack=73524588 Win=32120 Len=0
8	0.278102	192.168.200.3	192.168.200.1	TCP	1040 > http [ACK] Seq=73524588 Ack=512687732 Win=8231 Len=0
9	0.756554	192.168.200.3	192.168.200.1	TCP	1040 > http [FIN, ACK] Seq=73524588 Ack=512687732 Win=8231 Len=0
10	0.756560	192.168.200.1	192.168.200.3	TCP	http > 1040 [ACK] Seq=512687732 Ack=73524589 Win=32120 Len=0

Frame 6 (583 bytes on wire, 583 bytes captured)
Internet Protocol, Src Addr: 192.168.200.1 (192.168.200.1), Dst Addr: 192.168.200.3 (192.168.200.3)
Transmission Control Protocol,SrcPort:http(80)DstPort:1040(1040)Seq:512687202Ack:73524588 Len:529
Hypertext Transfer Protocol

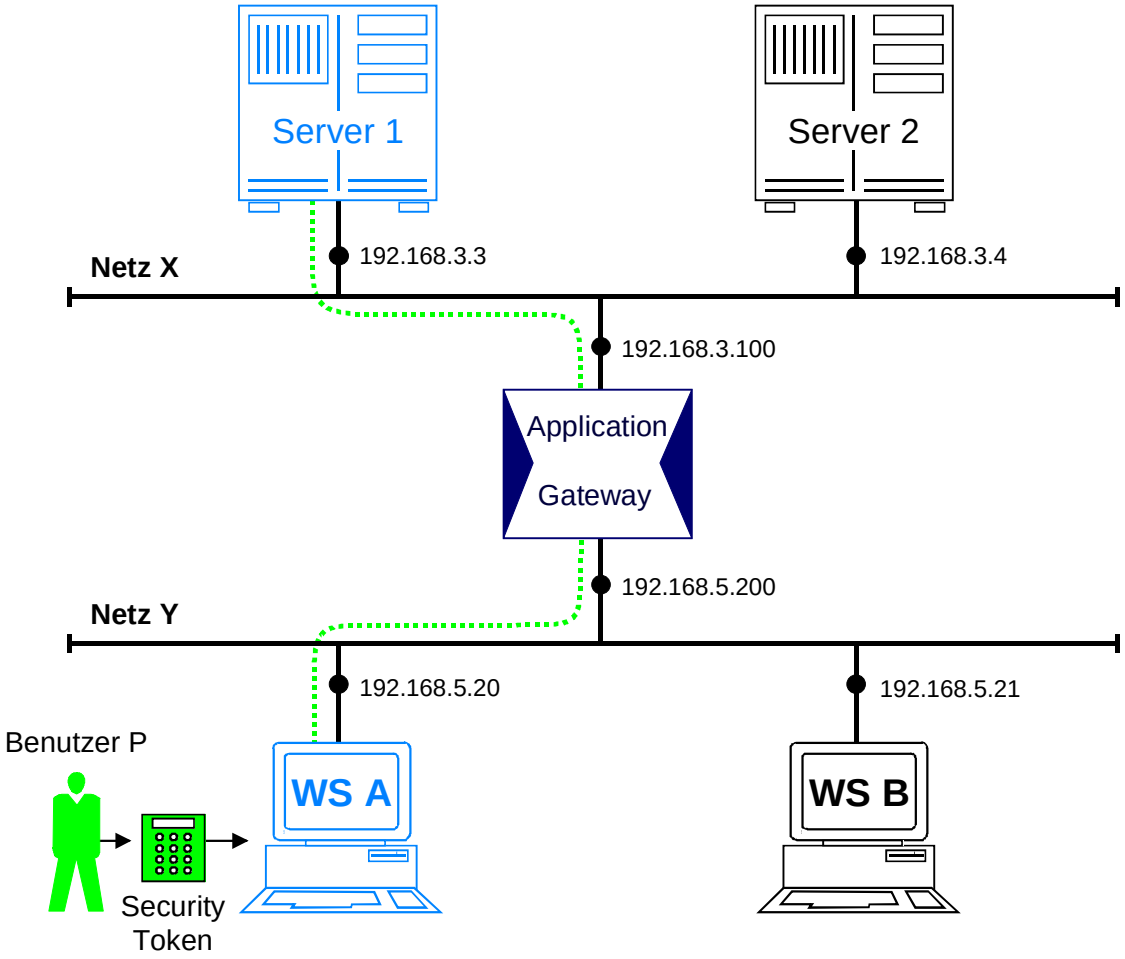
HTTP/1.0 403 Forbidden\r\n
Server: HTTP-Proxy\r\n
Date: Fri, 17 Oct 2003 10:57:03 GMT\r\n
MIME-Version: 1.0\r\n
Content-Type: text/html\r\n
Content-Encoding: 8bit\r\n
Content-Length: 357\r\n
Data (357 bytes)

```
0000  3c 48 54 4d 4c 3e 0a 20 20 3c 48 45 41 44 3e 3c   <HTML>.  <HEAD><
0010  54 49 54 4c 45 3e 41 63 63 65 73 73 20 44 65 6e   TITLE>Access Den
0020  69 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41   ied</TITLE></HEA
0030  44 3e 0a 20 20 3c 42 4f 44 59 20 42 47 43 4f 4c   D>.  <BODY BGCOL
0040  4f 52 3d 22 23 62 30 62 30 62 30 22 20 54 45 58   OR="#b0b0b0" TEX
0050  54 3d 22 23 46 46 30 30 30 30 22 3e 0a 20 20 3c   T="#FF0000">.  <
0060  63 65 6e 74 65 72 3e 0a 20 20 20 20 3c 68 31 3e   center>.    <h1>
0070  3c 69 3e 4b 72 79 70 74 6f 57 61 6c 6c 3c 2f 69   <i>KryptoWall</i
0080  3e 20 41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e   > Authentication
0090  3c 70 3e 3c 2f 68 31 3e 0a 20 20 20 20 3c 68 33   <p></h1>.    <h3
00a0  3e 20 49 50 20 3c 69 3e 31 39 32 2e 31 36 38 2e   > IP <i>192.168.
00b0  32 30 30 2e 33 3c 2f 69 3e 20 41 63 63 6f 75 6e   200.3</i> Accoun
00c0  74 20 3c 69 3e 75 6e 6b 6e 6f 77 6e 3c 2f 69 3e   t <i>unknown</i>
00d0  3c 70 3e 3c 2f 68 33 3e 0a 20 20 20 20 3c 68 72   <p></h3>.    <hr
00e0  3e 0a 20 20 20 20 4e f6 20 64 61 73 20 77 61 72   >.    N. das war
00f0  b4 73 20 21 0a 20 20 3c 2f 63 65 6e 74 65 72 3e   .s !.  </center>
0100  0a 0a 3c 50 3e 3c 48 52 3e 3c 41 44 44 52 45 53   ..<P><HR><ADDRES
0110  53 3e 3c 41 20 48 52 45 46 3d 22 68 74 74 70 3a   S><A HREF="http:
0120  2f 2f 77 77 77 2e 75 74 69 6d 61 63 6f 2e 64 65   //www.utimaco.de
0130  22 3e 55 74 69 6d 61 63 6f 20 53 61 66 65 77 61   ">Utimaco Safewa
0140  72 65 20 41 47 20 3c 2f 41 3e 3c 2f 41 44 44 52   re AG </A></ADDR
0150  45 53 53 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48   ESS>.</BODY>.</H
0160  54 4d 4c 3e 0a                                     TML>.
```

Telnet Proxy

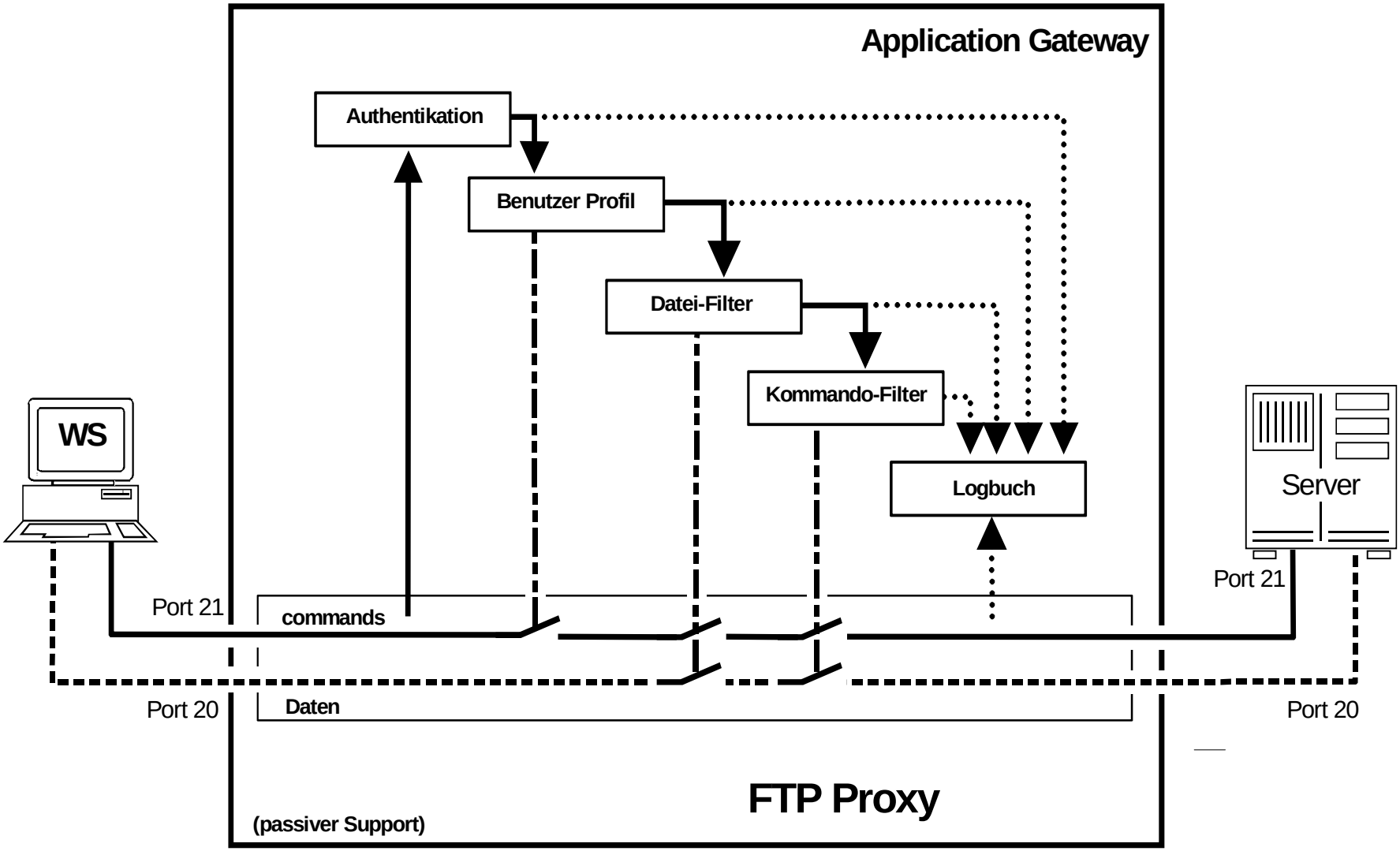


Application Gateway mit Telnet Proxy
→ Telnet-Session über Port 23



- Der Application Gateway gibt nach einer erfolgreichen Authentikation die Telnet-Session frei (evtl. Protokollierung)

FTP Proxy



Protokollmitschnitt - FTP

→ Löschen einer Datei und Abfrage des aktuellen DIR

No.	Time	Source	Destination	Protocol	Info
131	51.887371	192.168.2.101	194.94.127.28	FTP	Request: NOOP
132	51.967210	194.94.127.28	192.168.2.101	FTP	Response: 200 NOOP command successful.
133	52.147505	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243773 Ack=635576369 Win=64646 Len=0
135	64.340826	192.168.2.101	194.94.127.28	FTP	Request: DELE SNMP_MRTG_22_05_03.pdf
136	64.433651	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635576369 Ack=1054243802 Win=15466 Len=0
137	64.442653	194.94.127.28	192.168.2.101	FTP	Response: 250 DELE command successful.
138	64.443136	192.168.2.101	194.94.127.28	FTP	Request: CWD /home/pohlmann/files/Netzwerkmanagement
139	64.524986	194.94.127.28	192.168.2.101	FTP	Response: 250 CWD command successful.
141	64.606888	194.94.127.28	192.168.2.101	FTP	Response: 257 "/home/pohlmann/files/Netzwerkmanagement" is current d
142	64.615883	192.168.2.101	194.94.127.28	FTP	Request: TYPE A
143	64.694610	194.94.127.28	192.168.2.101	FTP	Response: 200 Type set to A.
144	64.705696	192.168.2.101	194.94.127.28	FTP	Request: PASV
145	64.785212	194.94.127.28	192.168.2.101	FTP	Response: 227 Entering Passive Mode (194,94,127,28,7,92).
146	64.789566	192.168.2.101	194.94.127.28	TCP	3489 > 1884 [SYN] Seq=1070679364 Ack=0 Win=64240 Len=0
147	64.789820	192.168.2.101	194.94.127.28	FTP	Request: LIST -a
148	64.866012	194.94.127.28	192.168.2.101	TCP	1884 > 3489 [SYN, ACK] Seq=707013412 Ack=1070679365 Win=15466 Len=0
149	64.866093	192.168.2.101	194.94.127.28	TCP	3489 > 1884 [ACK] Seq=1070679365 Ack=707013413 Win=64676 Len=0
150	64.883151	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635576566 Ack=1054243875 Win=15466 Len=0
151	64.950192	194.94.127.28	192.168.2.101	FTP	Response: 150 Opening ASCII mode data connection for file list
152	64.953386	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 56 bytes
153	64.962424	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 733 bytes
154	64.962496	192.168.2.101	194.94.127.28	TCP	3489 > 1884 [ACK] Seq=1070679365 Ack=707014202 Win=63887 Len=0
155	64.964597	194.94.127.28	192.168.2.101	FTP	Response: 226 Transfer complete.
156	64.964622	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243875 Ack=635576644 Win=64371 Len=0
157	65.051509	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 758 bytes
158	65.051615	192.168.2.101	194.94.127.28	TCP	3489 > 1884 [ACK] Seq=1070679365 Ack=707014961 Win=64676 Len=0
159	65.057978	192.168.2.101	194.94.127.28	TCP	3489 > 1884 [FIN, ACK] Seq=1070679365 Ack=707014961 Win=64676 Len=0
160	65.146712	194.94.127.28	192.168.2.101	TCP	1884 > 3489 [ACK] Seq=707014961 Ack=1070679366 Win=15466 Len=0

Löschen der Datei „SNMP_MRTG_22_05_03.pdf“

Protokollmitschnitt - FTP
→ Übertragung einer Datei vom Client zum Server

```
No. Time        Source          Destination     Protocol Info
 161 76.627677   192.168.2.101   194.94.127.28   FTP      Request: TYPE I
 162 76.705590   194.94.127.28   192.168.2.101   FTP      Response: 200 Type set to I.
 163 76.724403   192.168.2.101   194.94.127.28   FTP      Request: PASV
 164 76.804915   194.94.127.28   192.168.2.101   FTP      Response: 227 Entering Passive Mode (194,94,127,28,7,93).

 165 76.850636   192.168.2.101   194.94.127.28   TCP      3490 > 1885 [SYN] Seq=1073714353 Ack=0 Win=64240 Len=0
 166 76.929386   194.94.127.28   192.168.2.101   TCP      1885 > 3490 [SYN, ACK] Seq=708235639 Ack=1073714354 Win=15466 Len=0
 167 76.929474   192.168.2.101   194.94.127.28   TCP      3490 > 1885 [ACK] Seq=1073714354 Ack=708235640 Win=64676 Len=0

 168 76.929857   192.168.2.101   194.94.127.28   FTP      Request: STOR SNMP_MRTG_22_05_03.pdf
 169 77.022998   194.94.127.28   192.168.2.101   FTP      Response: 150 Opening BINARY mode data connection for SNMP_MRTG_22_0

 170 77.023963   192.168.2.101   194.94.127.28   FTP-DATA FTP Data: 1406 bytes
 171 77.024001   192.168.2.101   194.94.127.28   FTP-DATA FTP Data: 54 bytes
 172 77.167857   194.94.127.28   192.168.2.101   TCP      1885 > 3490 [ACK] Seq=708235640 Ack=1073715760 Win=15466 Len=0
 173 77.167928   192.168.2.101   194.94.127.28   FTP-DATA FTP Data: 1406 bytes
 174 77.167950   192.168.2.101   194.94.127.28   FTP-DATA FTP Data: 1406 bytes
 175 77.174142   194.94.127.28   192.168.2.101   TCP      1885 > 3490 [ACK] Seq=708235640 Ack=1073715814 Win=15466 Len=0
 176 77.174199   192.168.2.101   194.94.127.28   FTP-DATA FTP Data: 1406 bytes
 177 77.174216   192.168.2.101   194.94.127.28   FTP-DATA FTP Data: 1406 bytes
 178 77.183488   192.168.2.101   194.94.127.28   TCP      3483 > ftp [ACK] Seq=1054243918 Ack=635576781 Win=64234 Len=0
 179 77.382012   194.94.127.28   192.168.2.101   TCP      1885 > 3490 [ACK] Seq=708235640 Ack=1073718626 Win=15466 Len=0
 180 77.382114   192.168.2.101   194.94.127.28   FTP-DATA FTP Data: 1406 bytes
 181 77.382135   192.168.2.101   194.94.127.28   FTP-DATA FTP Data: 1406 bytes

...

 286 81.879903   194.94.127.28   192.168.2.101   TCP      1885 > 3490 [FIN, ACK] Seq=708235640 Ack=1073770017 Win=15466 Len=0
 287 81.879939   192.168.2.101   194.94.127.28   TCP      3490 > 1885 [ACK] Seq=1073770017 Ack=708235641 Win=64676 Len=0

 288 81.881715   194.94.127.28   192.168.2.101   FTP      Response: 226 Transfer complete.
```

Aktivierung des „Image“-Modes

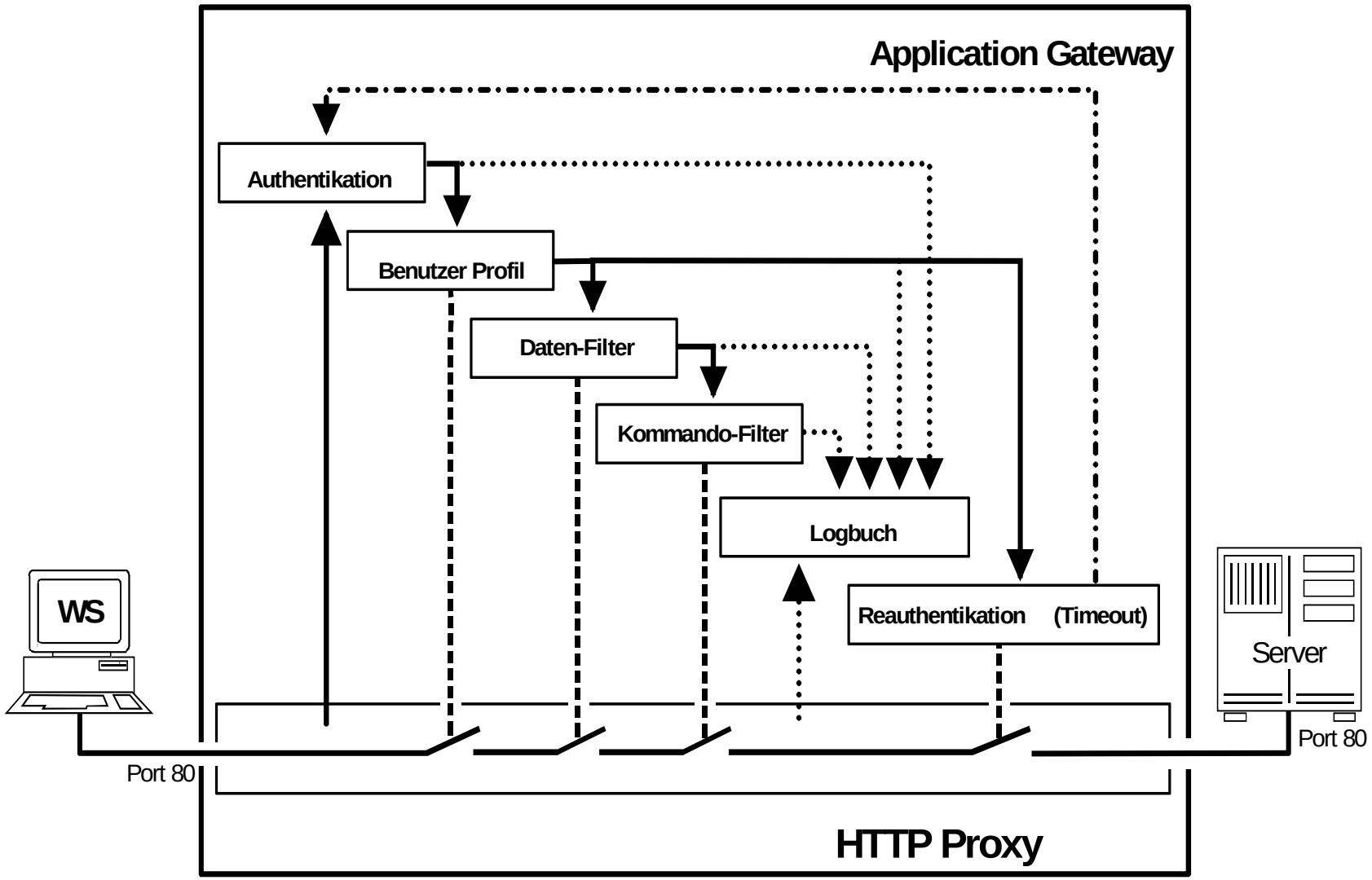
Passive Mode

Aufbau eines Datenkanals (Port 1885)

Datenübertragung - STOR „SNMP_MRTG_22_05_03.pdf“

Abbau des Datenkanals (Port 1885) durch den Client

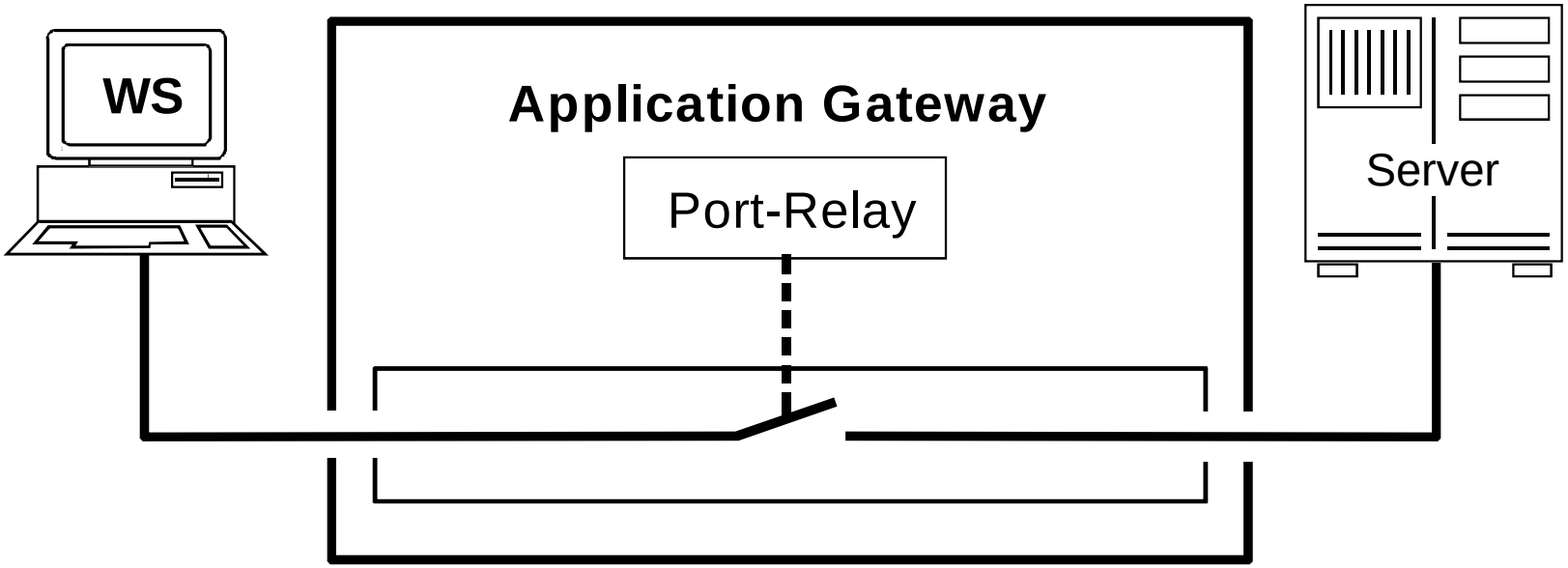
HTTP Proxy



Hypertext Transfer Protocol (HTTP 1.0)
→ Protokollmittschnitt - Beispiel 1 (3/4)

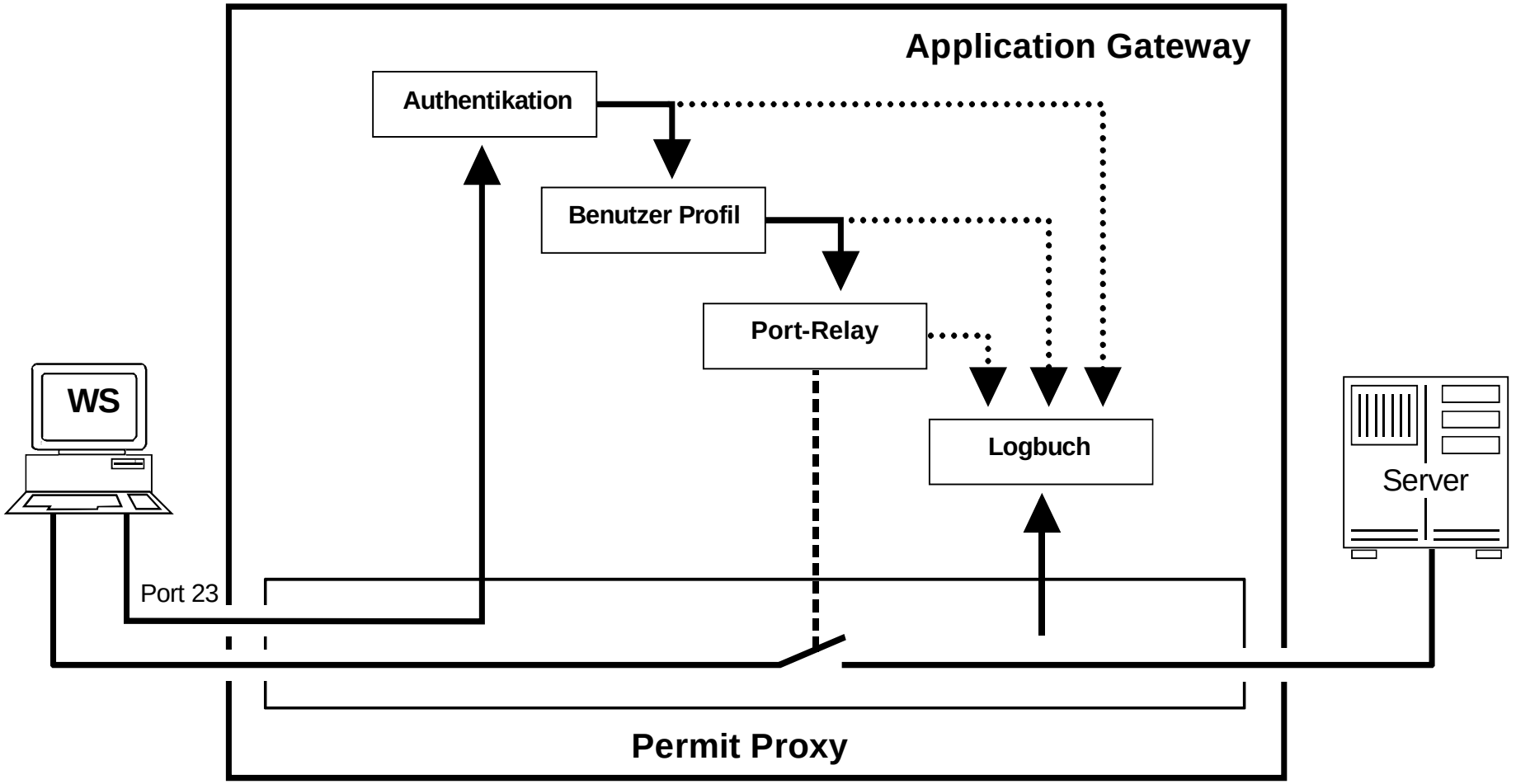
```
No. Time       Source          Destination     Protocol Info
  1 0.000000   192.168.2.101   192.168.2.1     DNS      Standard query A www.joes-hardware.com
  2 0.234871   192.168.2.1     192.168.2.101   DNS      Standard query response CNAME joes-hardware.com A 161.58.228.45
  3 0.442260   192.168.2.101   161.58.228.45   TCP      3163 > http [SYN] Seq=343924507 Ack=0 Win=64240 Len=0
  4 0.591326   161.58.228.45   192.168.2.101   TCP      http > 3163 [SYN, ACK] Seq=1145840618 Ack=343924508 Win=16872 Len=0
  5 0.591416   192.168.2.101   161.58.228.45   TCP      3163 > http [ACK] Seq=343924508 Ack=1145840619 Win=64676 Len=0
  6 0.592711   192.168.2.101   161.58.228.45   HTTP     GET /tools.html HTTP/1.0
  7 0.770411   161.58.228.45   192.168.2.101   HTTP     HTTP/1.1 304 Not Modified
  8 0.873553   192.168.2.101   161.58.228.45   TCP      3163 > http [ACK] Seq=343924859 Ack=1145840835 Win=64460 Len=0

. . .

. . .

 82 19.679595  192.168.2.101   161.58.228.45   TCP      3163 > http [FIN, ACK] Seq=343924859 Ack=1145840835 Win=64460 Len=0
 94 19.866455  161.58.228.45   192.168.2.101   TCP      http > 3163 [ACK] Seq=1145840835 Ack=343924860 Win=16872 Len=0
 95 19.867356  161.58.228.45   192.168.2.101   TCP      http > 3163 [FIN, ACK] Seq=1145840835 Ack=343924860 Win=16872 Len=0
 96 19.867389  192.168.2.101   161.58.228.45   TCP      3163 > http [ACK] Seq=343924860 Ack=1145840836 Win=64460 Len=0

No. Time       Source          Destination     Protocol Info
  6 0.592711   192.168.2.101   161.58.228.45   HTTP     GET /tools.html HTTP/1.0
GET /tools.html HTTP/1.0
If-Modified-Since: Fri, 12 Jul 2002 07:50:17 GMT; length=433
Connection: Keep-Alive
User-Agent: Mozilla/4.78 [de] (Windows NT 5.0; U)
Host: www.joes-hardware.com
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Encoding: gzip
Accept-Language: de
Accept-Charset: iso-8859-1,*,utf-8


No. Time       Source          Destination     Protocol Info
  7 0.770411   161.58.228.45   192.168.2.101   HTTP     HTTP/1.1 304 Not Modified
HTTP/1.1 304 Not Modified
Date: Mon, 11 Aug 2003 16:56:21 GMT
Server: Apache/1.3.27 OpenSSL/0.9.6i (Unix) FrontPage/5.0.2.2510
Connection: Keep-Alive
Keep-Alive: timeout=5, max=20
ETag: "5fa0f6-1b1-3d2e8a39"
```

TCP/UDP Port Relay
→ Circuit Level Proxy



- Circuit Level Proxies sind eine Art generische Proxies, die für eine Mehrzahl von Diensten mit verschiedenen Protokollen verwendet werden können
- Wird verwendet für Dienste, für die kein Application Level Proxy zur Verfügung steht
- **Stellen ein Sicherheitsproblem dar!**

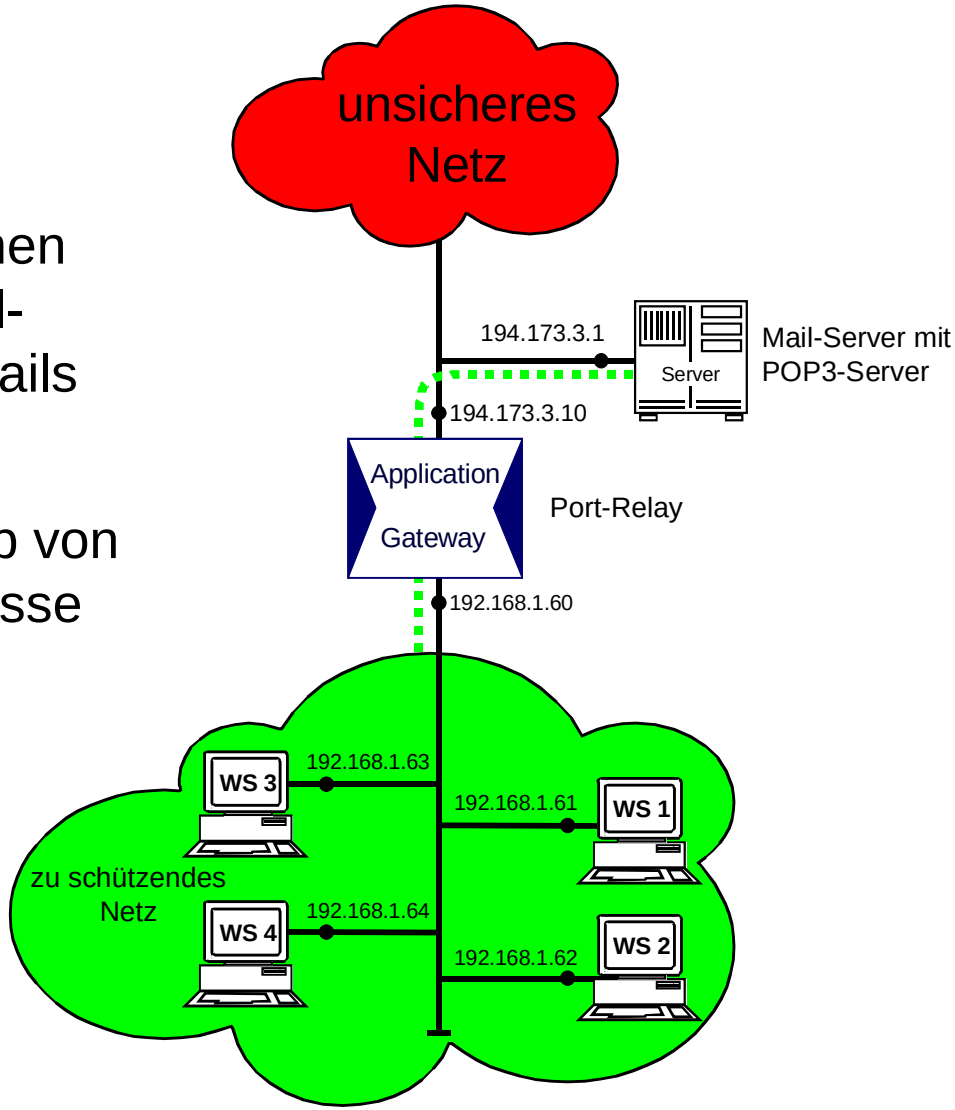
TCP Port Relay mit Authentikation



- Bietet eine höhere Sicherheit!

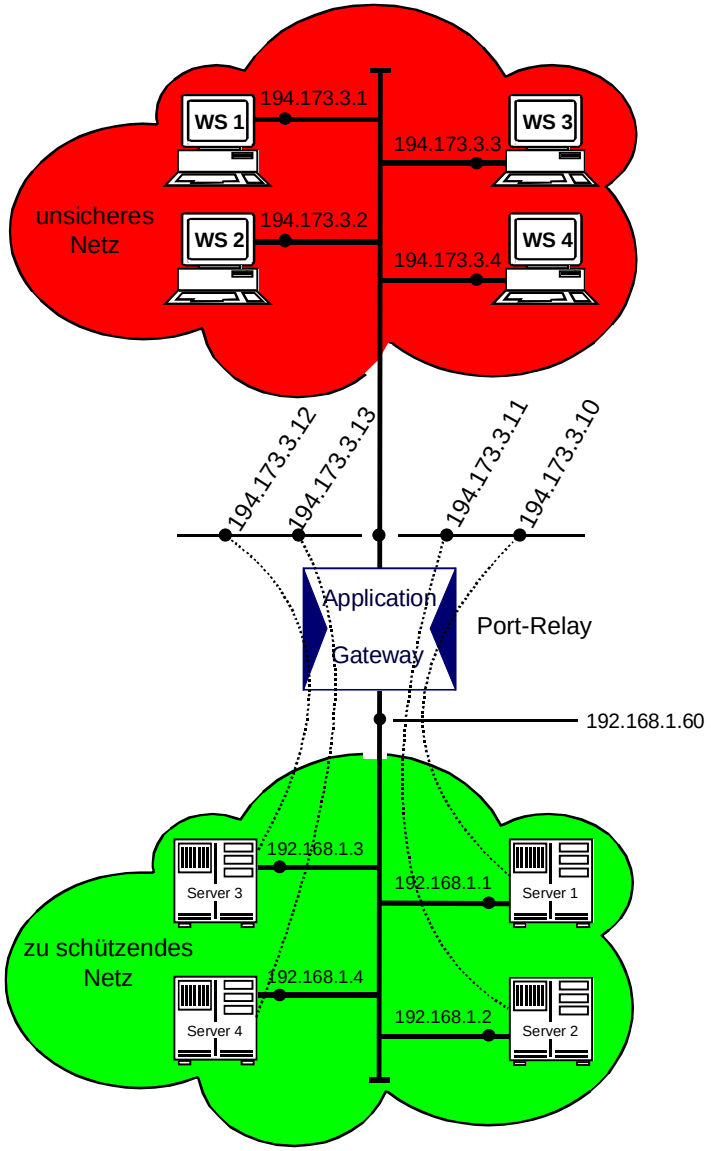
Beispiel eines n:1 Port-Relays

- Clients können z.B. über einen definierten Port auf den Mail-Server zugreifen, um ihre Mails zu holen.
- Das Port-Relay überprüft, ob von einer zugelassenen IP-Adresse zugegriffen wird!

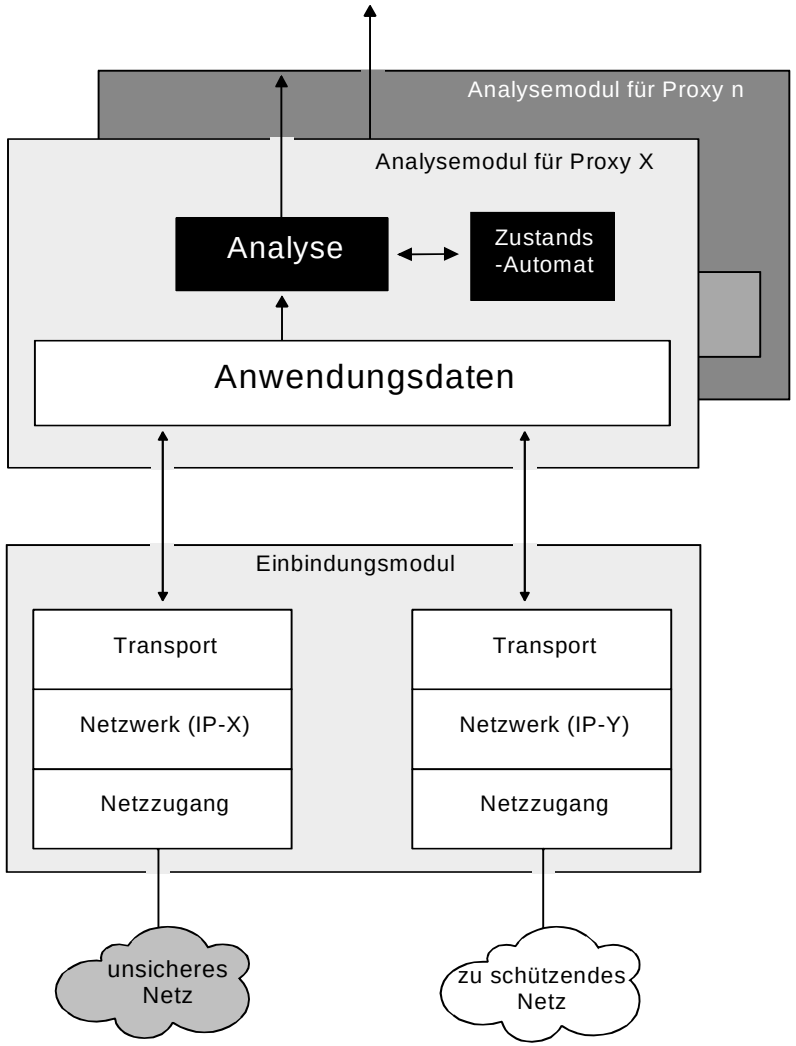


Beispiel eines n:m Port-Relays

- Das Application Gateway kann über mehrere IP-Adressen aus dem unsicheren Netz angesprochen werden
- Dabei bleiben die IP-Adressen aus dem zu schützenden Netz verborgen



Bewertung:
→ Application Gateway



Möglichkeiten

- Service-orientierte Kontrolle aller Pakete durch den Proxy
- spezielle Sicherheitsfunktionen für jeden Proxy
- **modulares, klares und überprüfbares Konzept**
- Verbergen der internen Netzstruktur

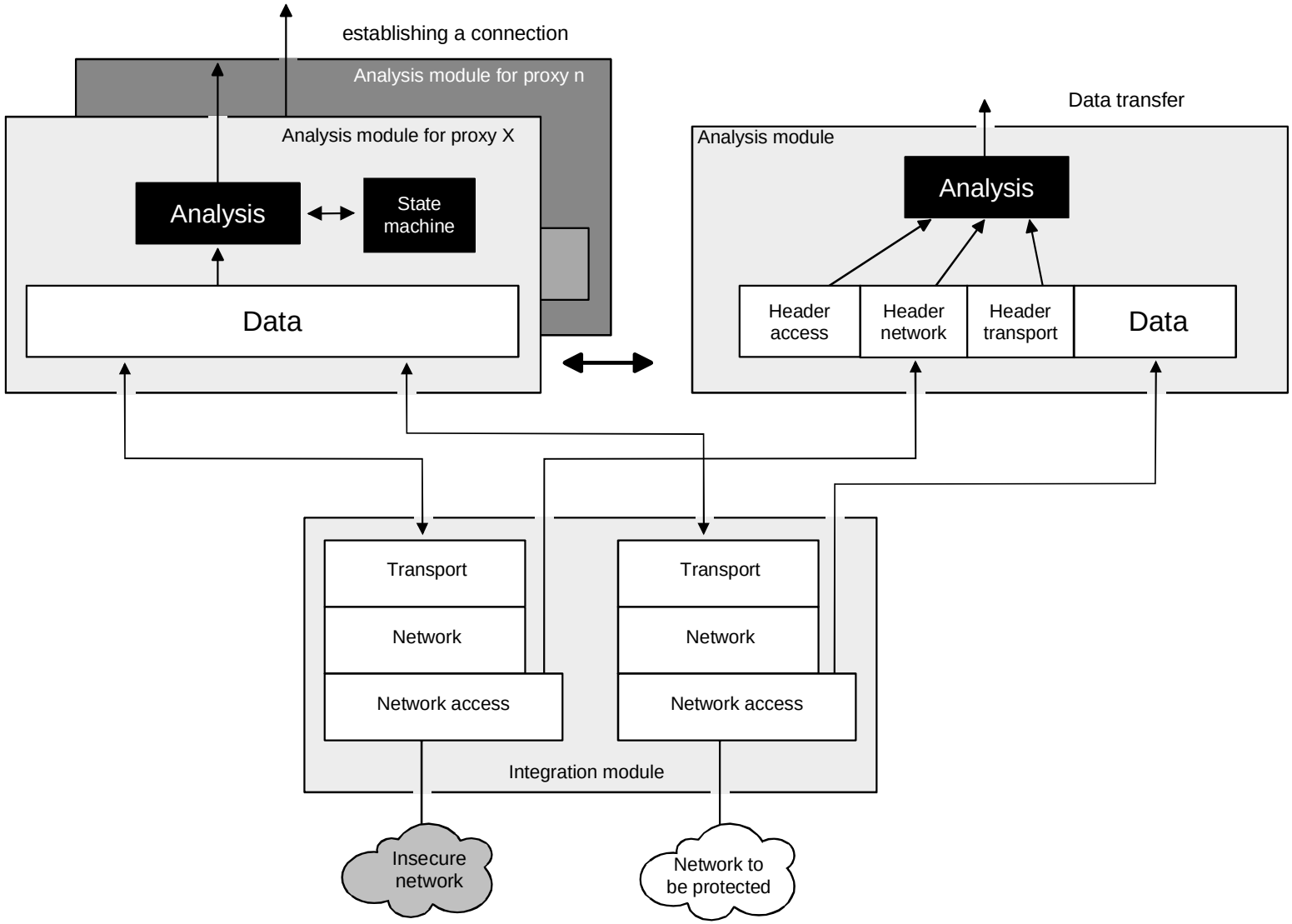
Grenzen

- geringe Flexibilität
- die Kosten sind in der Regel höher
- nicht transparent

Inhalt

- Definition eines Firewall-Elements
- Packet Filter
- zustandsorientierter Packet Filter
- Application Gateway
- **Adaptive Proxy**
- Firewall-Elemente im Verhältnis zu Schnelligkeit und Sicherheit

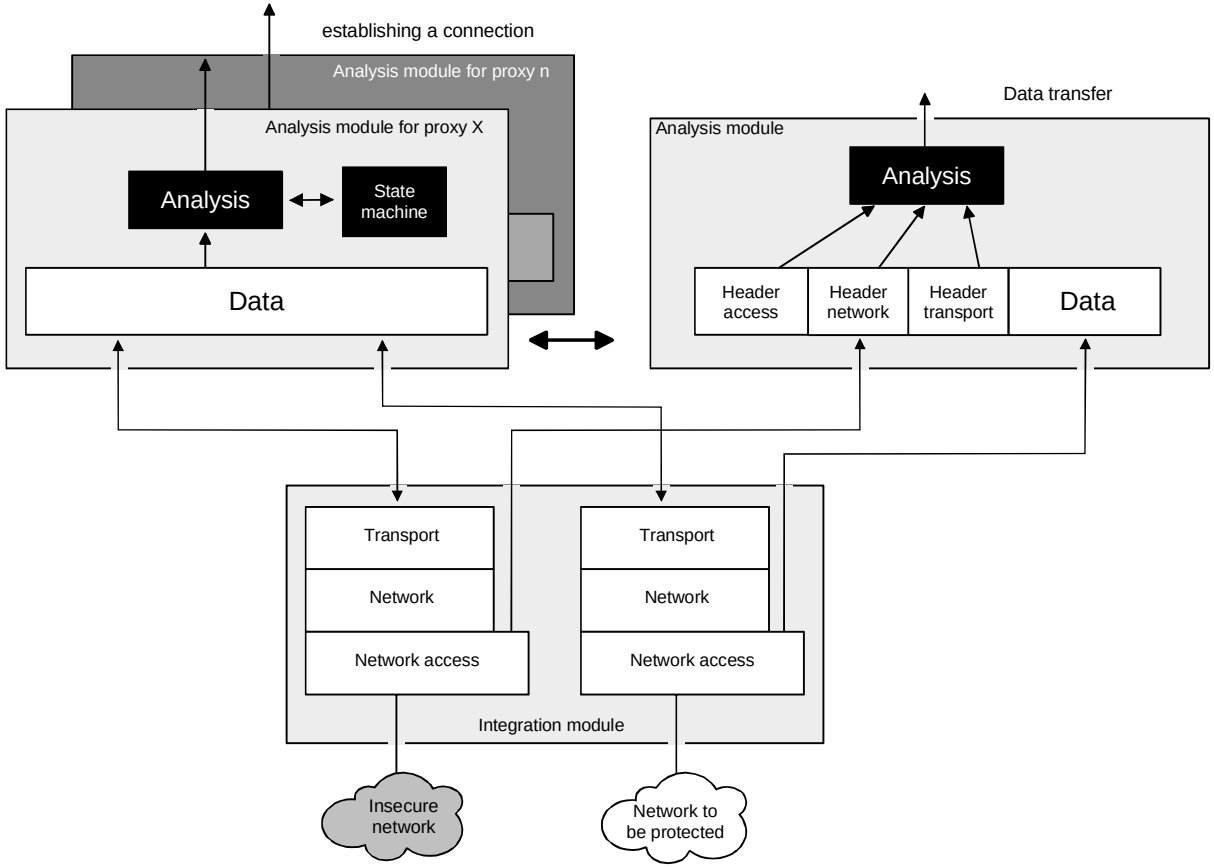
Allgemeine Arbeitsweise
→ „Adaptive Proxies“



Analogie zum Pförtner
→ Adaptive Proxies

- Der Adaptive Proxy arbeitet in der ersten Phase (Verbindungsaufbauphase) wie der Application Proxy: Er schaut sich nicht nur die Adresse der eingehenden Pakete an, er öffnet auch das Paket und überprüft den gesamten Inhalt.
- Wenn der Adapive Proxy den Lieferanten seit langem kennt, dann sendet er den LKW des Lieferanten durch das Tor, damit dieser die Lieferung direkt zustellt.
- Kennt er den Lieferanten jedoch nicht, dann schickt er den LKW-Fahrer nach Ausladung der Lieferung weg und bestellt den firmeneigenen Fahrer, der im eigenen LKW das Paket zum Empfänger bringt.

Bewertung:
→ Adaptive Proxy



Möglichkeiten

- bietet die Flexibilität eines Packet Filters und eines Application Gateways

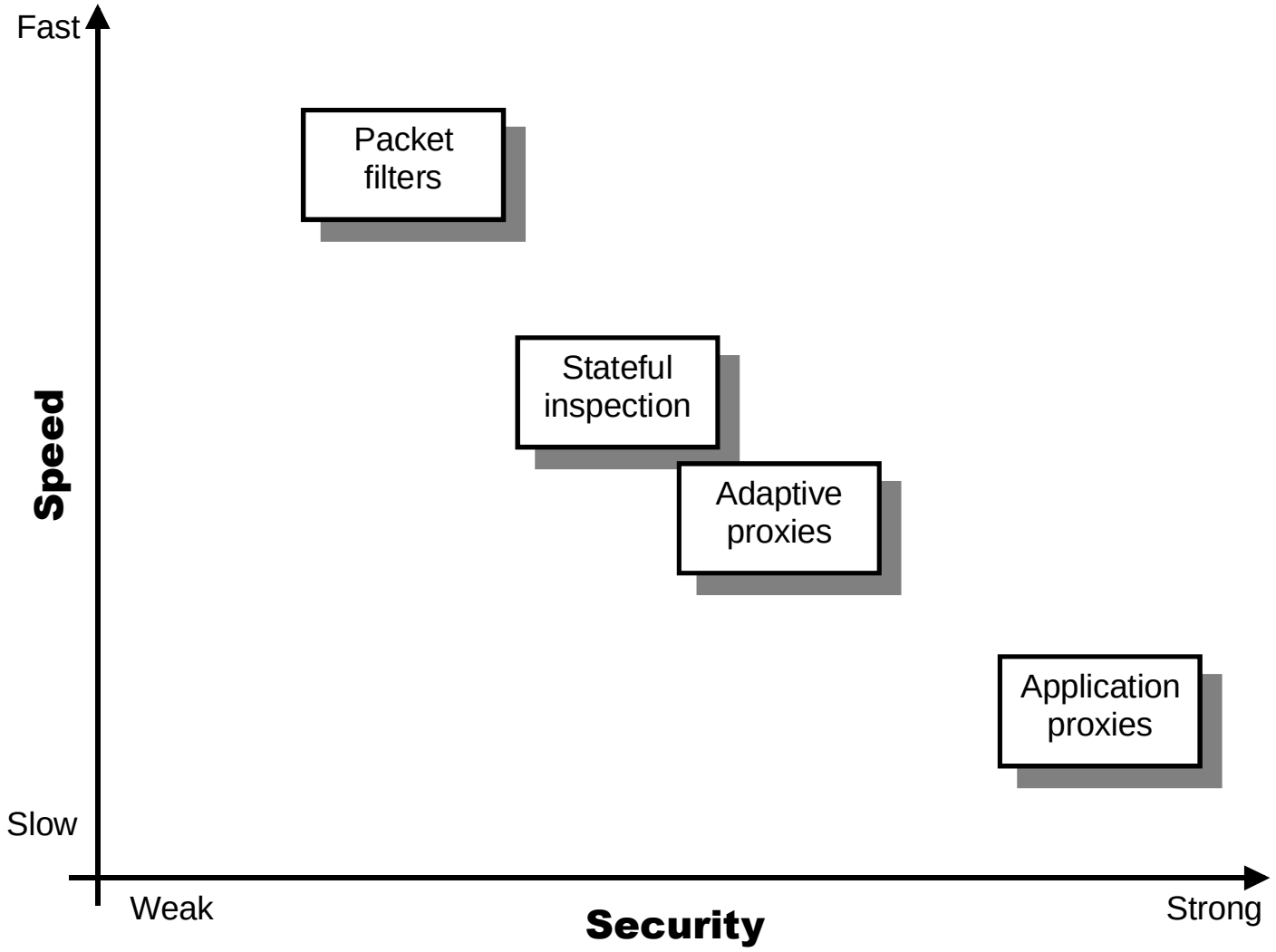
Grenzen

- die Sicherheit hängt von der schwächsten Komponente ab (Packet Filter)

Inhalt

- Definition eines Firewall-Elements
- Packet Filter
- zustandsorientierter Packet Filter
- Application Gateway
- Adaptive Proxy
- **Firewall-Elemente im Verhältnis zu Schnelligkeit und Sicherheit**

Firewall-Elemente im Verhältnis zu Schnelligkeit und Sicherheit



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Firewall-Systeme

Firewall-Elemente

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.