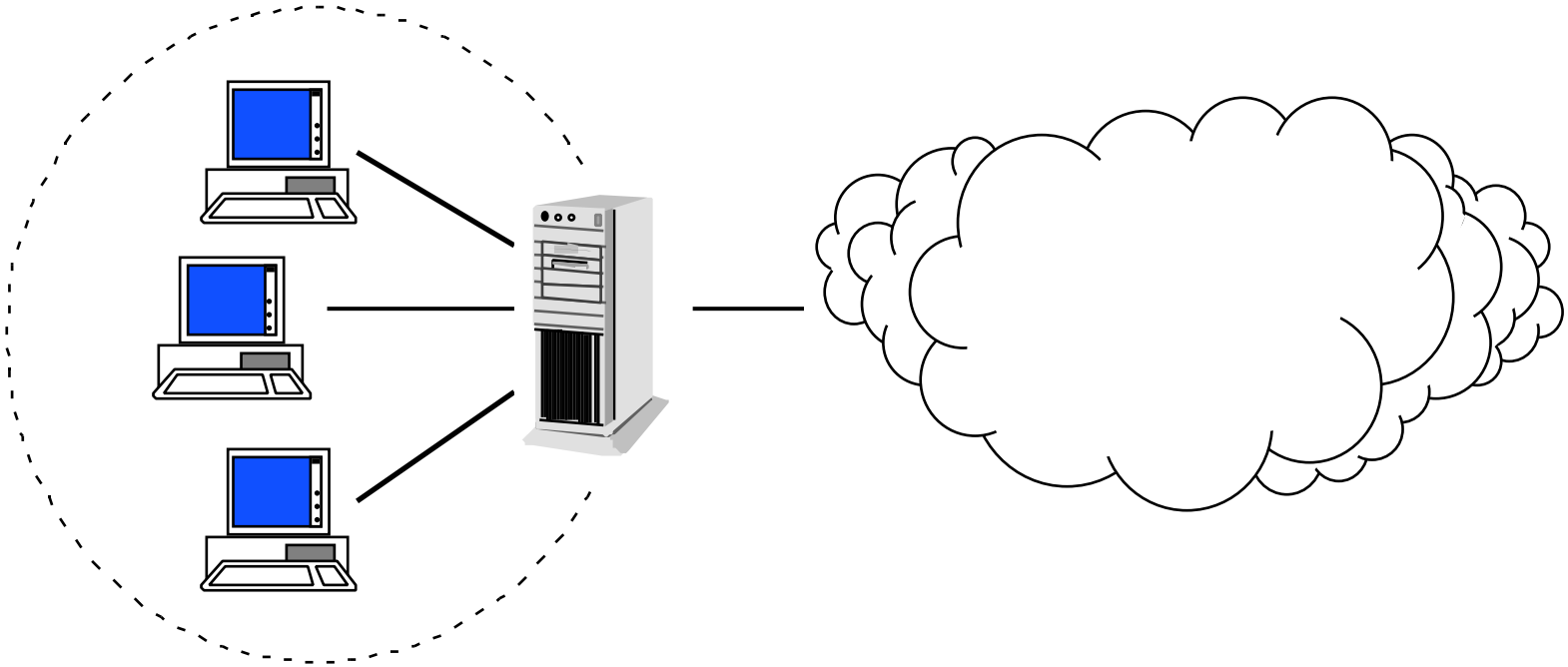
Der SINUS-Firewall

Harald Weidner
weidner@ifi.unizh.ch

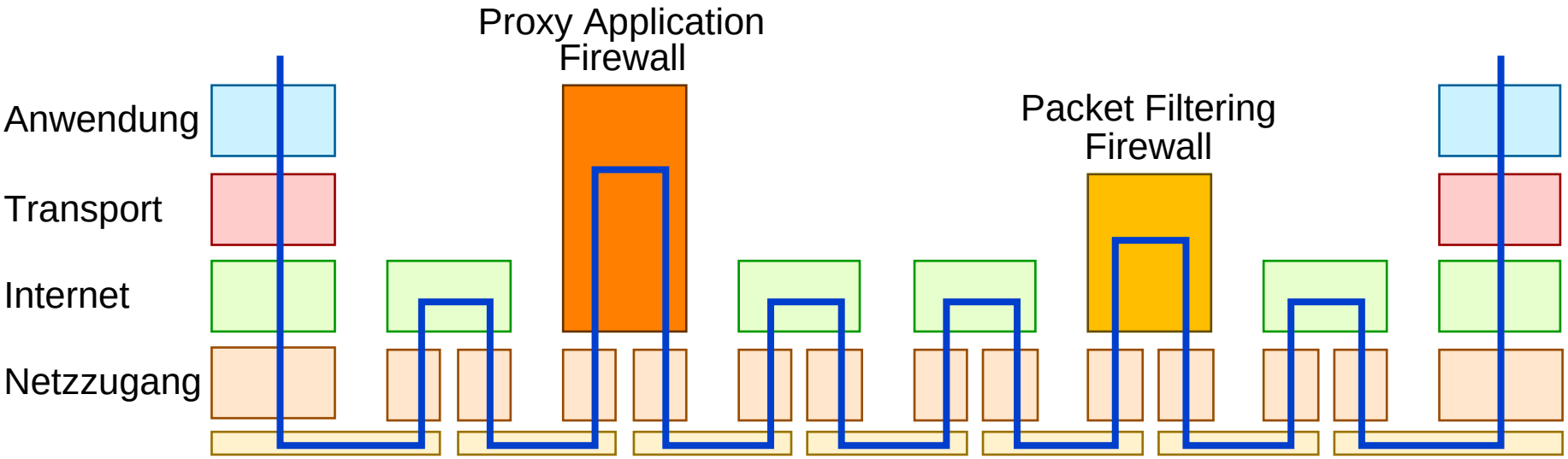
Firewalls (1)



Firewalls (2)

- Hilfsmittel zur kontrollierten Verbindung von Netzen unterschiedlicher Vertrauenswürdigkeit
- Weiterleiten oder Blockieren von Daten anhand definierter Regeln
- Protokollierung, Alarmierung
- Filterung auf Netzwerk- oder Anwendungsebene

Firewall-Typen (1)



Firewall-Typen (2)

Paketfilter

- Filterung anhand der Steuerinformationen von Vermittlungs- und Transportschicht
- Keine Filterung des Paketinhaltes
- Keine Anpassung der Dienste nötig

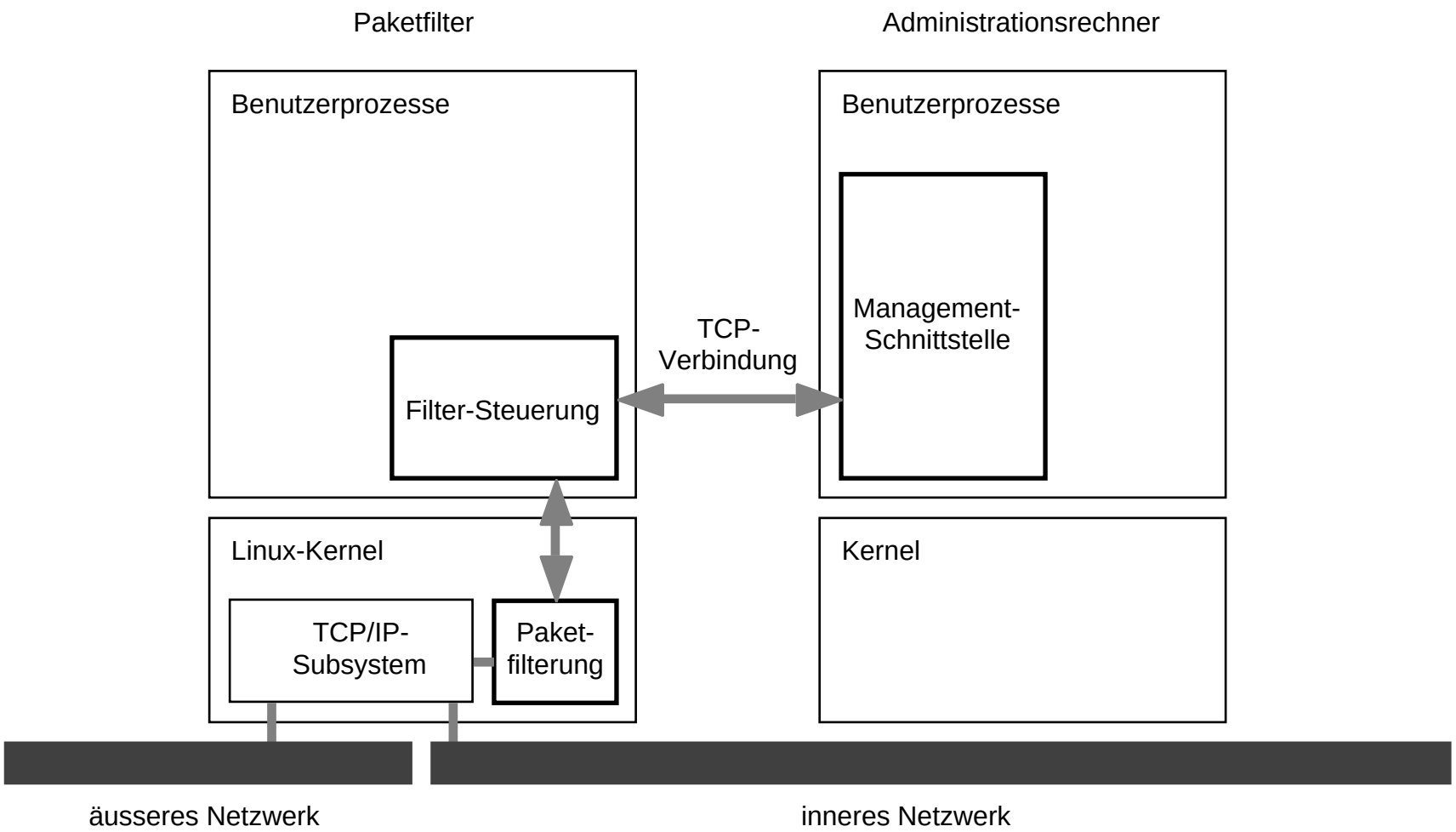
Application Gateways

- Filterung der Datenströme
- Nicht für alle Dienste verfügbar

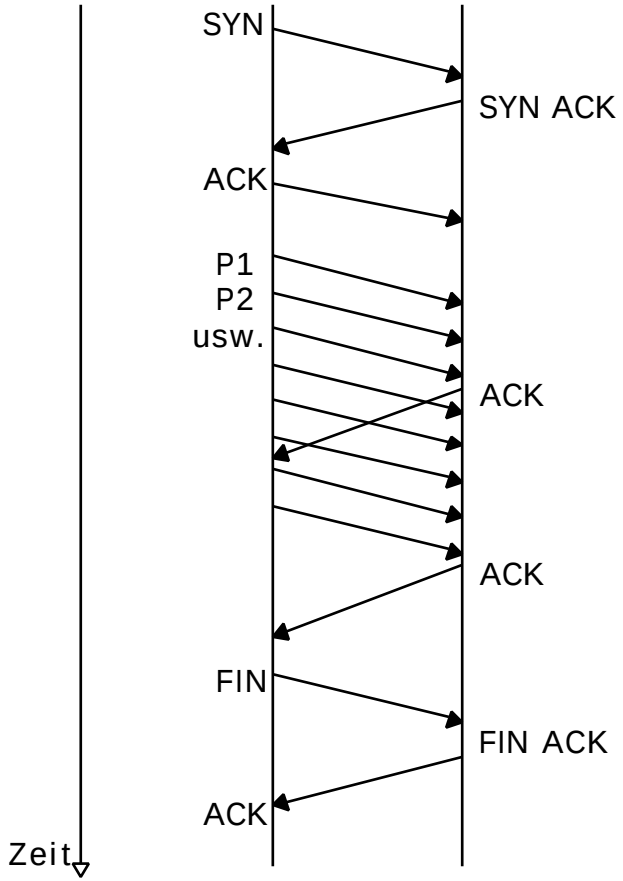
Der SINUS-Firewall

- Paketfilter unter Linux
- zustandsorientierte Filterung
- menschenlesbare Konfiguration
- dynamische Regeln
- graphisches Konfigurationstool
- GNU General Public License

Architektur



Zustandsorientierte Filterung



zustandslos:

- Filterung für jede Richtung des Paketaustausches
- Unterscheidung der Verbindungsaufbau-richtung schwierig

zustandsorientiert:

- eine Regel der Art accept tcp from ... to ...

Konfigurationsdatei

```
setup
  internalnets 130.60.106.0 mask 255.255.255.0;
rules
  accept tcp from 130.60.106.3 port 1024..65535
     to 130.60.48.10 port 25 notification_level 1;
  reject tcp from outside to port 79
     notification_level 2;
  block udp notification_level 0;
notification
  level 1:
    ;
  level 2:
    message “we have been fingered”;
    spy;
end.
```

Dynamische Regeln

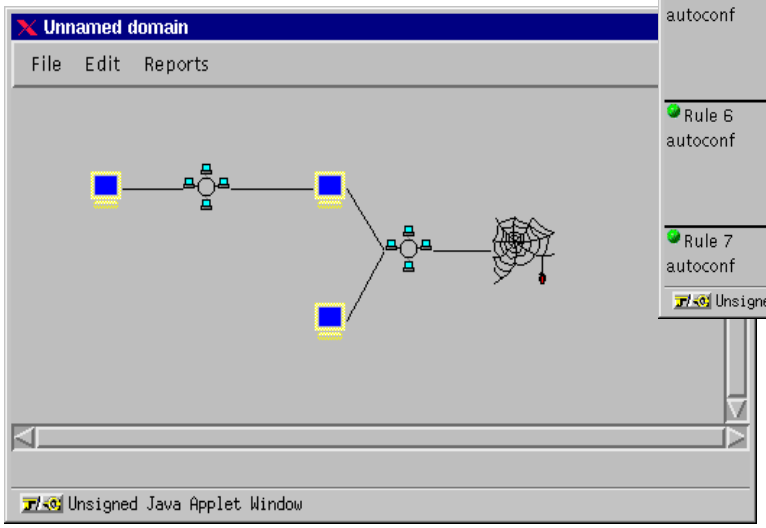
```
# Zugriff auf WWW von aussen erlaubt
accept tcp from outside to 130.60.106.4 port 80
  notification_level 8;


# mehr als 100 Zugriffe in 2 Minuten
# -> 10 Minuten Sperre
level 8:
  let access:sourcehost = access:sourcehost + 1
  timeout 120;
  if access:sourcehost > 100 then
    message “Blocking access for 10 minutes.”;
    block all from sourcehost notification_level 0
    timeout 600;
  endif;
```

Weitere Funktionen

- Sonderbehandlung für FTP
  - active mode / passive mode
- Erkennung von IP Spoofing
- Gegenspionage
  - finger, ident, rusers
- Verschlüsselung/Authentifikation über ENskip
- FW-to-FW-Kommunikation

Graphisches Konfigurationstool



Domain

File Edit Help

Rule	Action	Protocol	From	To	Notification	Valid for
Rule 1 autoconf priority	accept	TCP no FTP data conn.	CONFCLIENTS 130.60.48.132/255.255.25 130.60.106.1/255.255.255	FW-CONFPORT 130.60.106.1/255.255.255 130.60.48.132/255.255.25 Port 7227	None	All
	Description: Allow configuration connections from configuration clients.					
Rule 2 autoconf	accept	all protocols	LOCALHOST 127.0.0.1/255.255.255.25	LOCALHOST 127.0.0.1/255.255.255.25	None	All
	Description: Accept connections from localhost to localhost.					
Rule 3 autoconf	accept	all protocols	OWNADDR Own addresses	OWNADDR Own addresses	None	All
	Description: Accept connections from local addresses to local addresses.					
Rule 4 autoconf	accept	TCP no FTP data conn.	FW-UNPRIV 130.60.106.1/255.255.255 130.60.48.132/255.255.25 Ports 1024..65535	SMTP-PORT Port 25	None	All
	Description: e-Mail from firewalls					
Rule 5 autoconf	accept	TCP no FTP data conn.	FW-UNPRIV 130.60.106.1/255.255.255 130.60.48.132/255.255.25 Ports 1024..65535	FINGER-PORT Port 79	None	All
	Description: finger from firewalls					
Rule 6 autoconf	reject with tcp reset	TCP		FW-IDENTPORT 130.60.106.1/255.255.255 130.60.48.132/255.255.25 Port 113	None	All
	Description: reject ident to firewalls					
Rule 7 autoconf	accept	TCP	FW-UNPRIV 130.60.106.1/255.255.255	IDENT-PORT Port 113	None	All

Unsigned Java Applet Window

Grenzen, Bugs, TODO

- kein IP-Masquerading
- kein Transparent Proxying
- Linux-2.0.36, JDK-1.1, Swing-1.0 oder älter
- Spoofing-Erkennung nur für 2 Interfaces
- Java-Tool sehr langsam
- Installation nicht ganz einfach

Installation

- Voraussetzungen
  - Linux-2.0.36, libc5 oder libc6 (glibc2)
  - optional JDK-1.1.6, Swing-1.0, ENskip-0.67
- Kernel-Konfiguration
  - Set version information on all symbols for modules
  - Network Firewalling, IP Forwarding, IP Firewalling
  - IP always defragment, Optimize as router not host

Ressourcen

- WWW-Seite
  - http://www.ifi.unizh.ch/ikm/SINUS/firewall/
- Mailingliste
  - firewall@ifi.unizh.ch
  - echo subscribe firewall | \
    Mail majordomo@ifi.unizh.ch
  - geschlossene Liste, d.h. Schreibrecht nur für Mitglieder