Firewalls

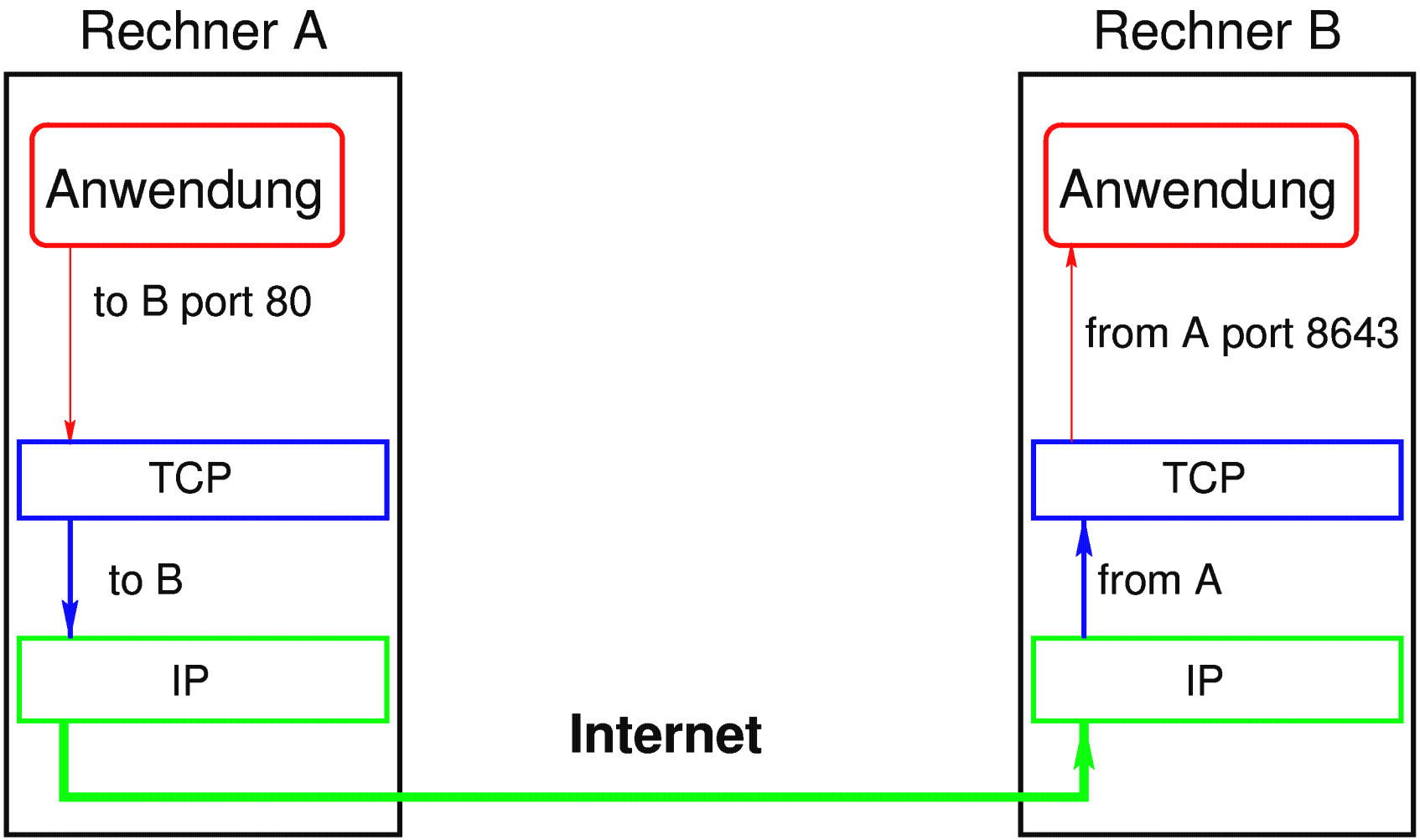
Einsatz, Möglichkeiten, Angriffe

Arno Wagner

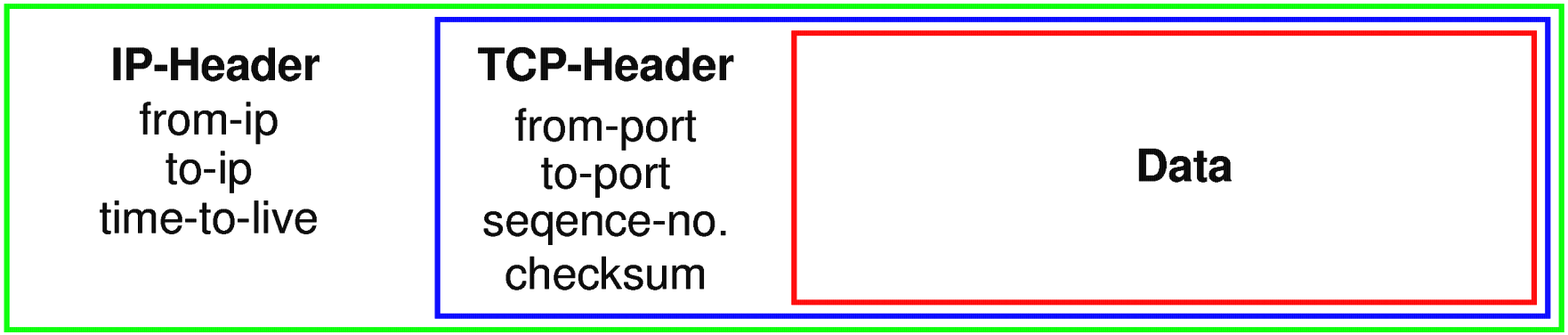
Inhalt des Vortrages:

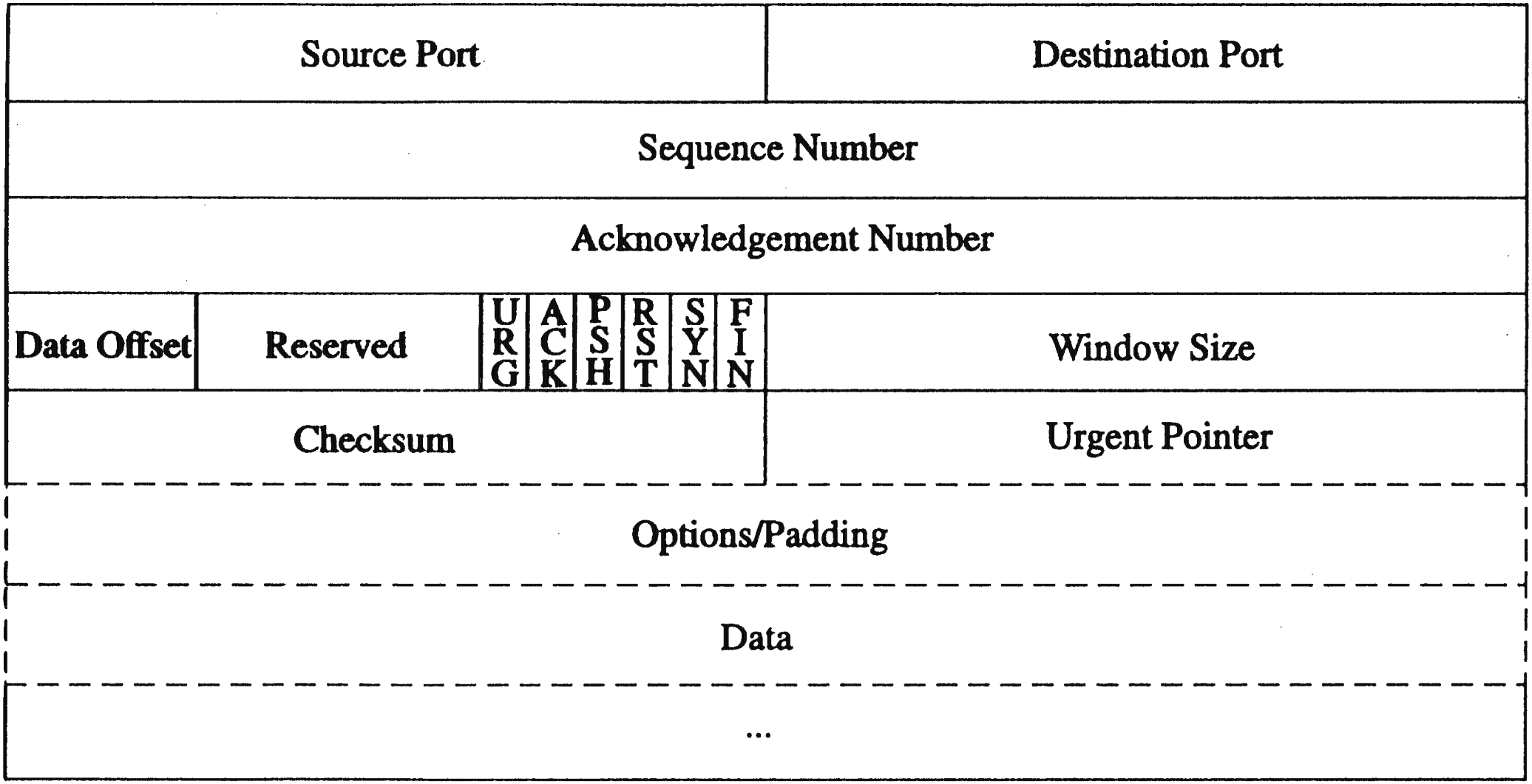
- Kurzeinführung TCP/IP
- „Definition“ des Begriffs **Firewall**
- Einsatz von Filtern und Proxies
- Möglichkeiten von Filtern und Proxies
- Probleme von Filtern
- Denial-of-service-Angriffe und Abwehrmöglichkeiten

TCP/IP Kommunikation

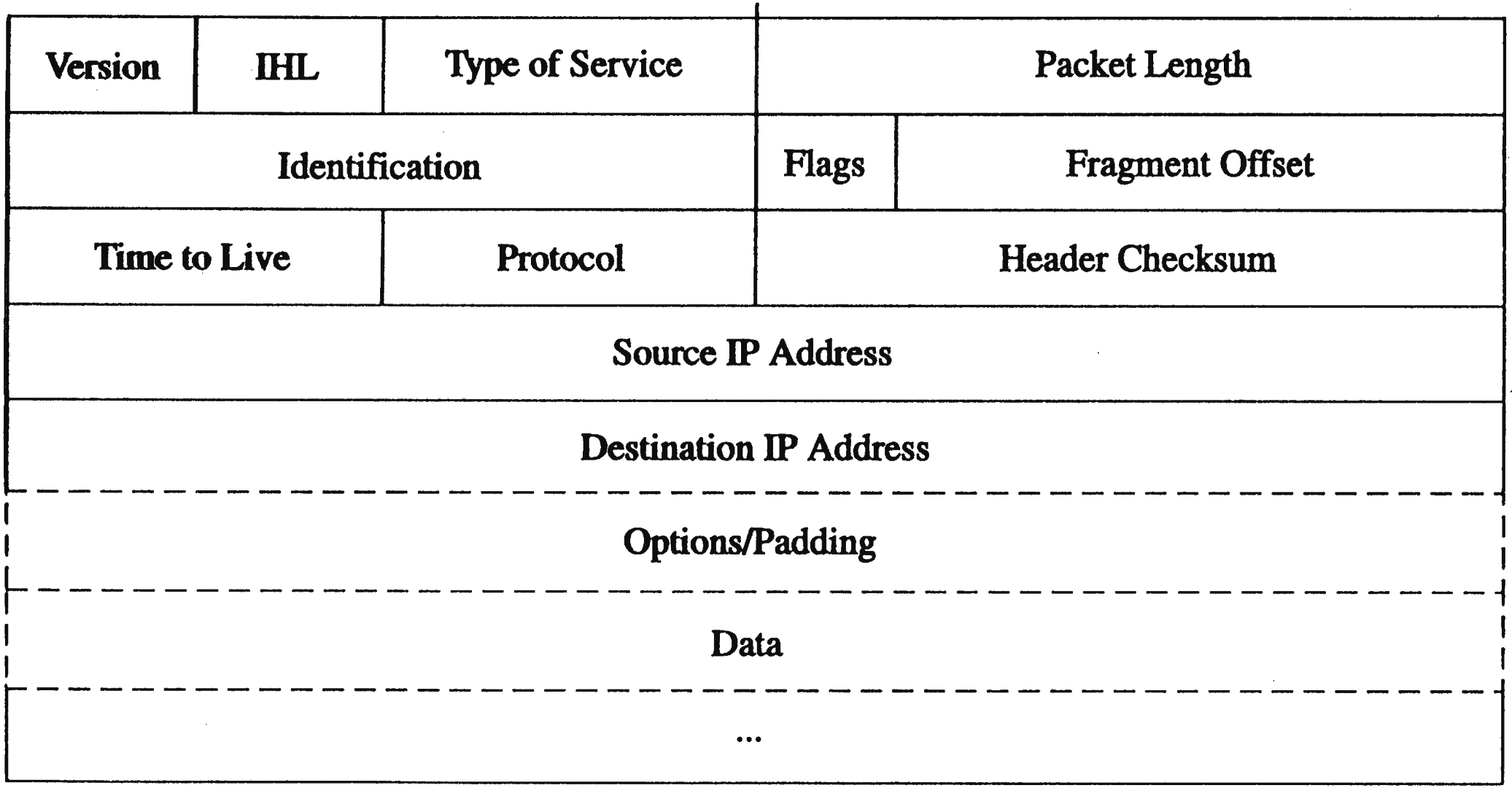


TCP/IP Packetformat





TCP-Segment-Format



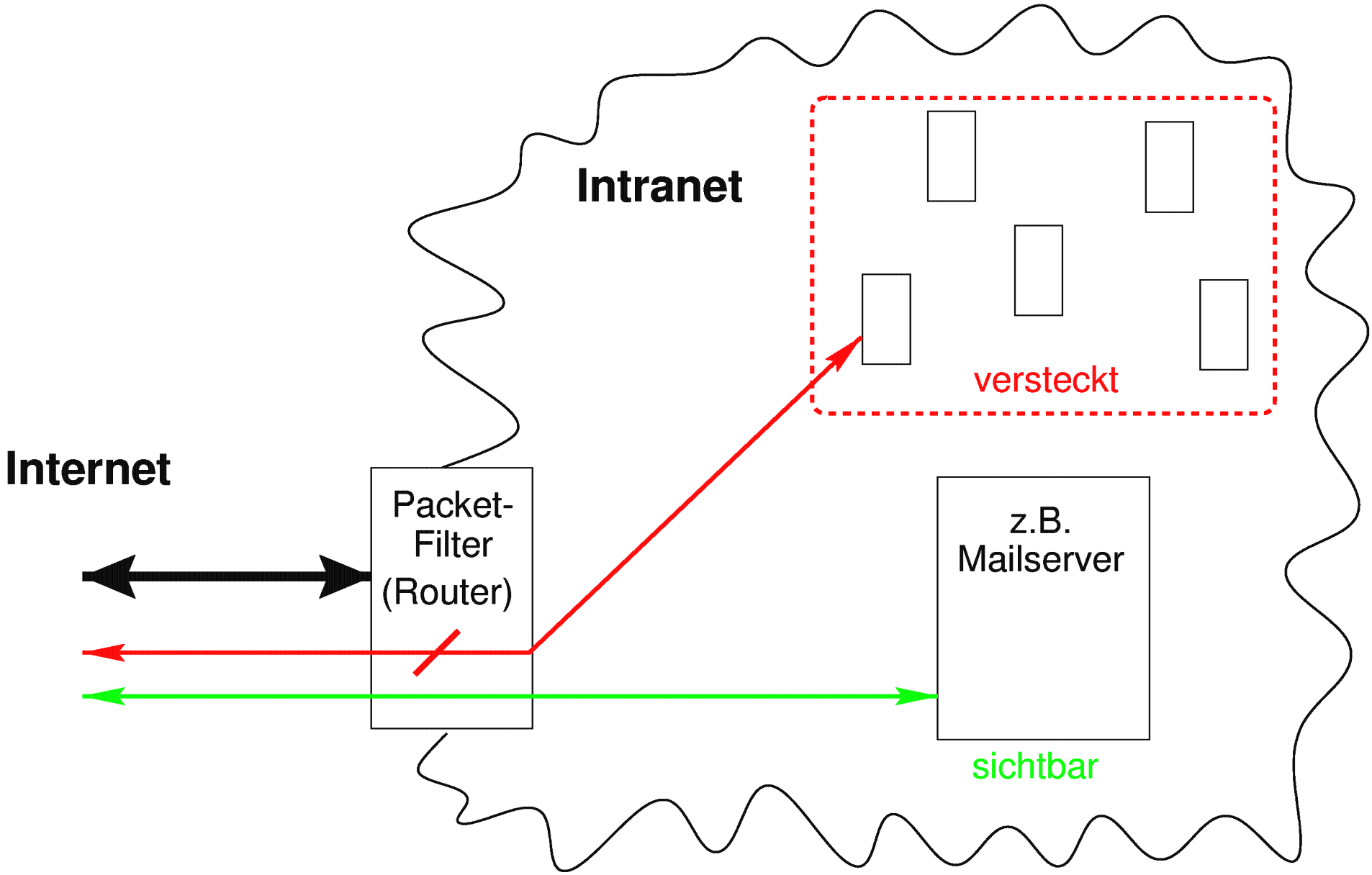
IP-Datagramm

Definition des Begriffs **Firewall**:

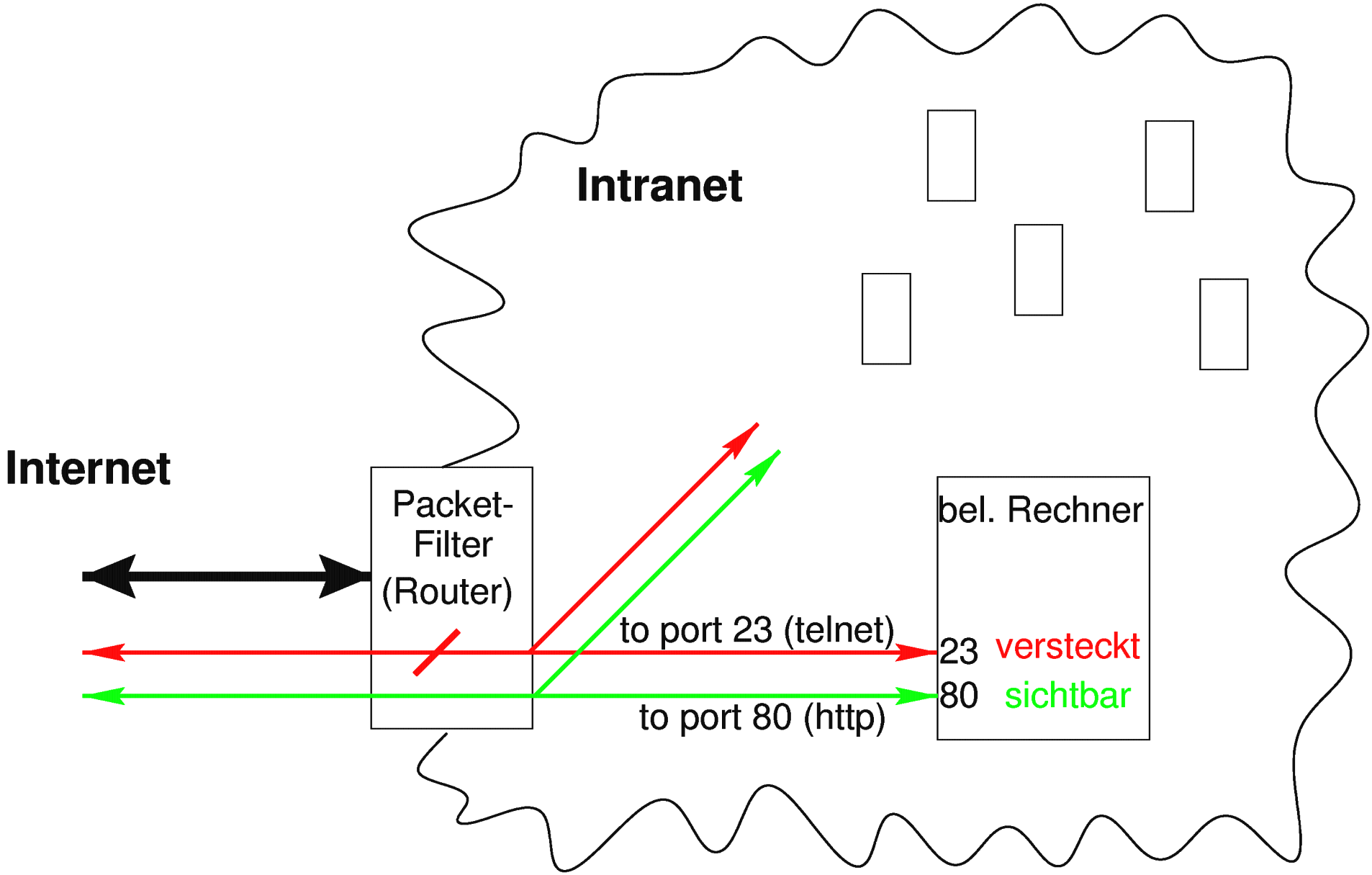
Ein *Firewall-System*

- besteht aus einem oder mehreren Rechnern
- hat Kontakt zum Intranet und zum Internet
- hat einen Administrator
- erschwert/verhindert bestimmte Klassen von Angriffen
- erschwert/verhindert die Benutzung bestimmter Dienste

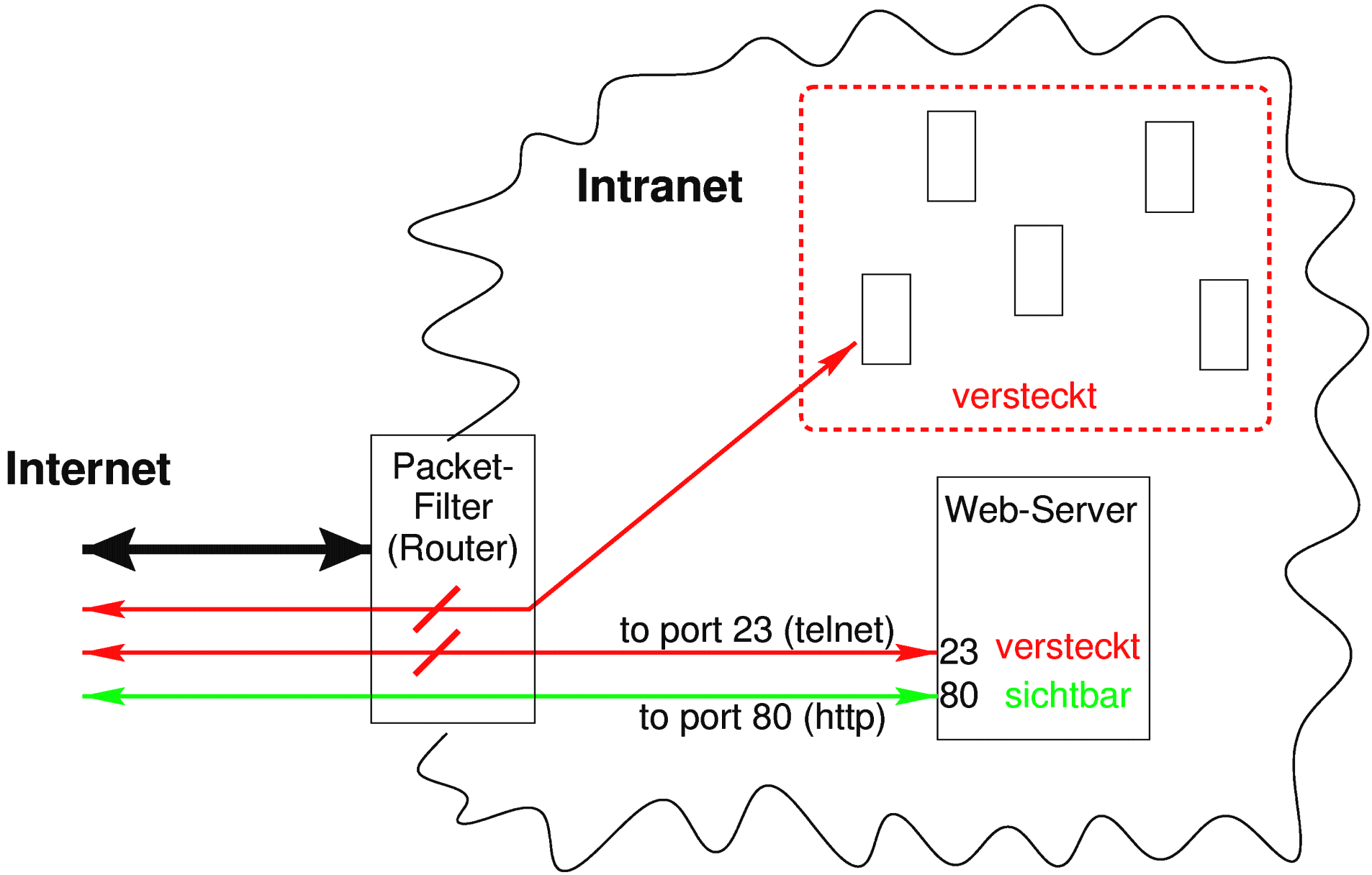
Verstecken innerer Rechner



Verstecken innerer Ports (Dienste)

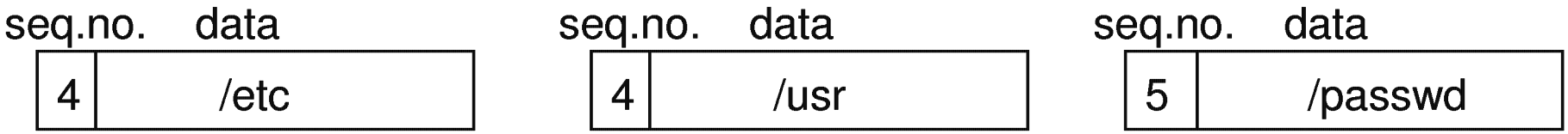


Rechner und Ports verstecken



Warum Filter nicht den Datenstrom sehen

Beispiel: Doppelte Daten



Alternative im Datenstrom:

Bei erste Daten: /etc/passwd
Bei letzte Daten: /usr/passwd

Filter kann nicht entscheiden, was die Anwendung sieht, bzw.
Filter sieht nur eine der beiden Alternativen!

Andere Möglichkeiten Filter zu umgehen

- Packetlebensdauern
- ungültige Packete
- Bufferüberlauf beim Zielsystem
- Grenzen des Zielsystems, z.B. zu grosse/zu kleine Packete
- ...

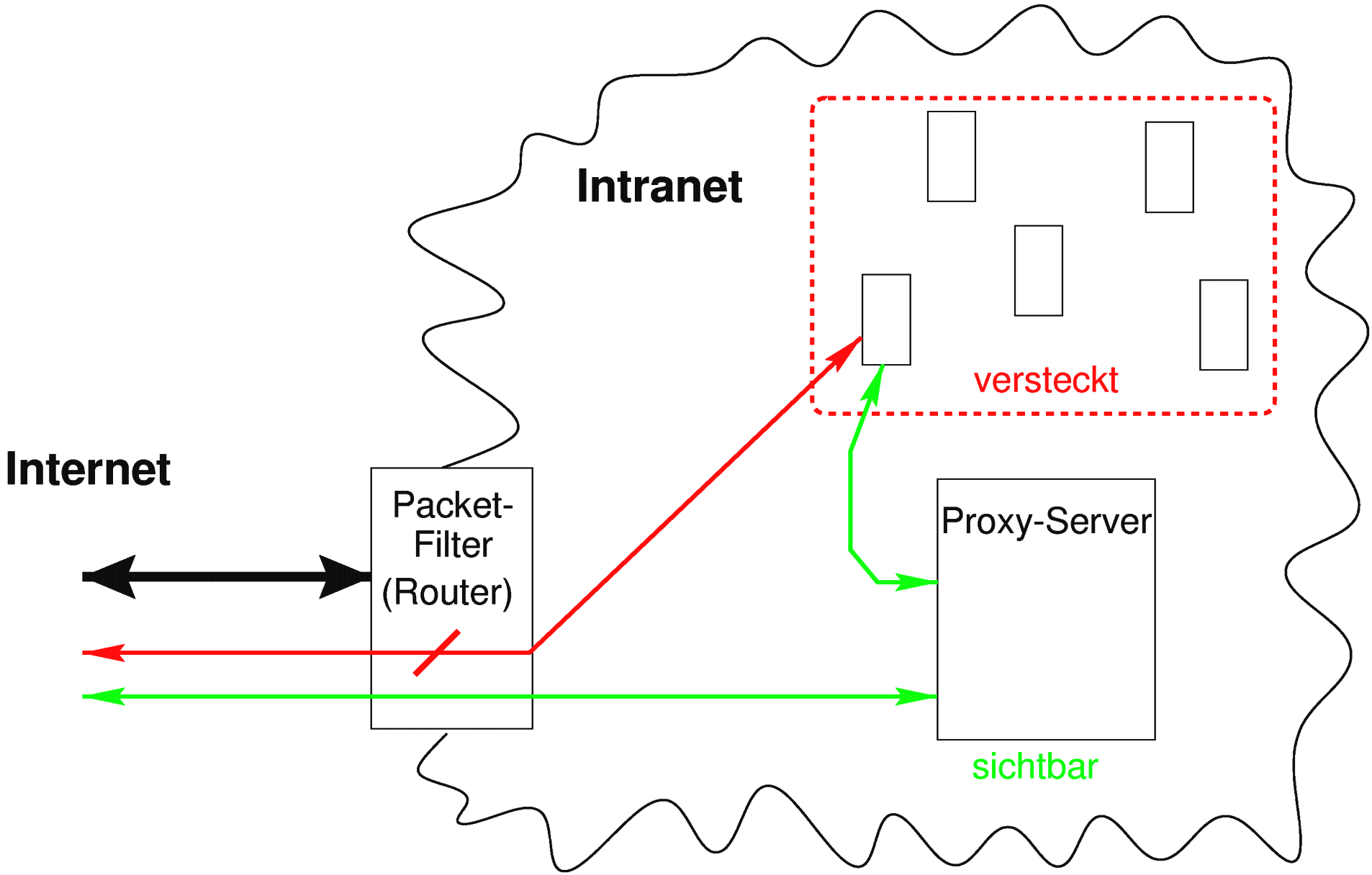
Ein Angriff auf Filter: Remote OS Detection

- Automatisiertes Erkennen der Betriebssysteme von Rechnern hinter der Firewall
- Benutzt TCP/IP fingerprinting
- Tools: z.B. nmap (Phrack Magazine 54)
- Wichtige Vorstufe für gezielte Angriffe

Abwehr:

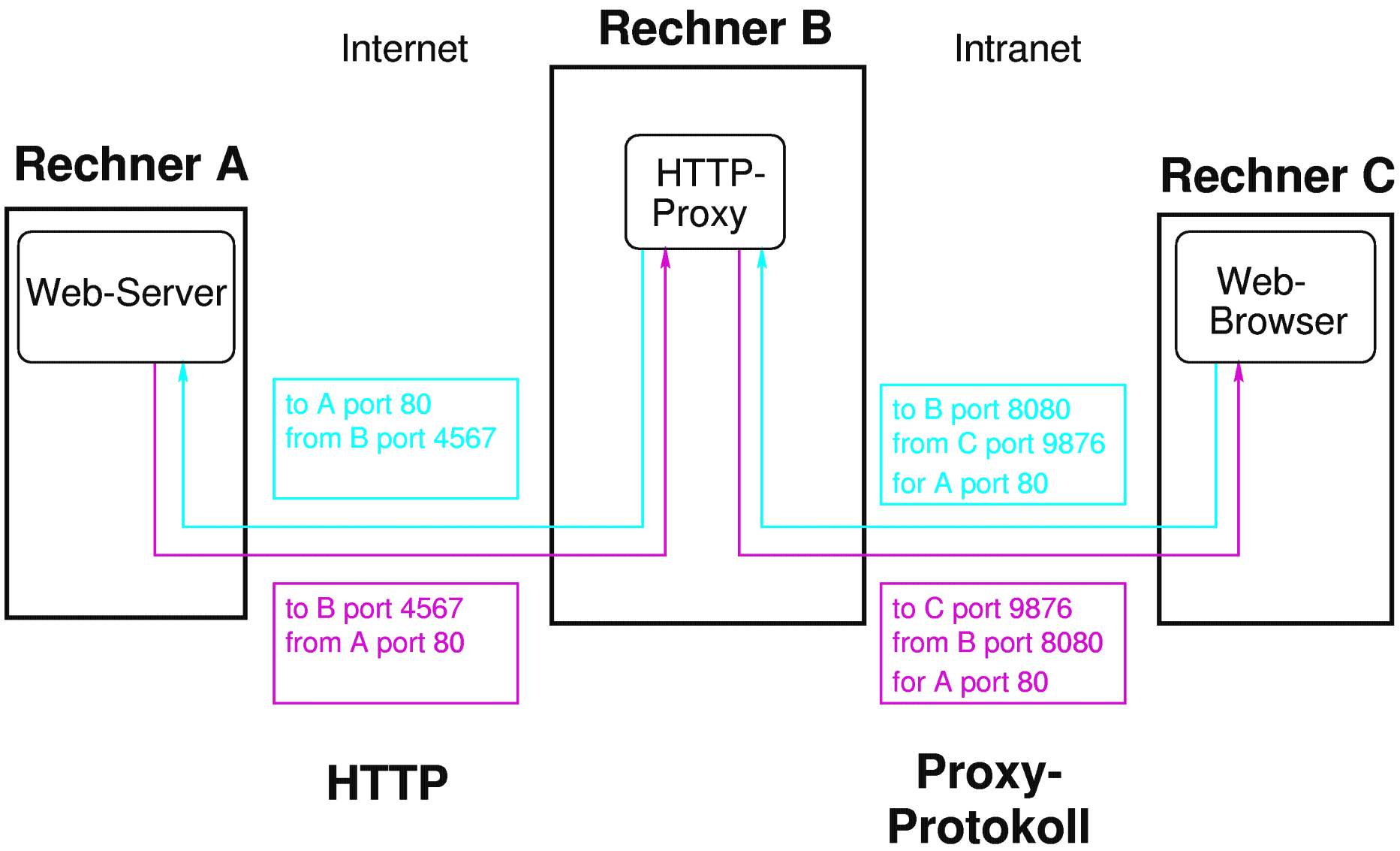
- Filter: Nur totale Blockade hilft
- Spezifischer Proxy: Sichere bis eingeschränkte Abwehr
- Generischer Proxy: Eingeschränkte Abwehr.

Typische Proxy-Konfiguration



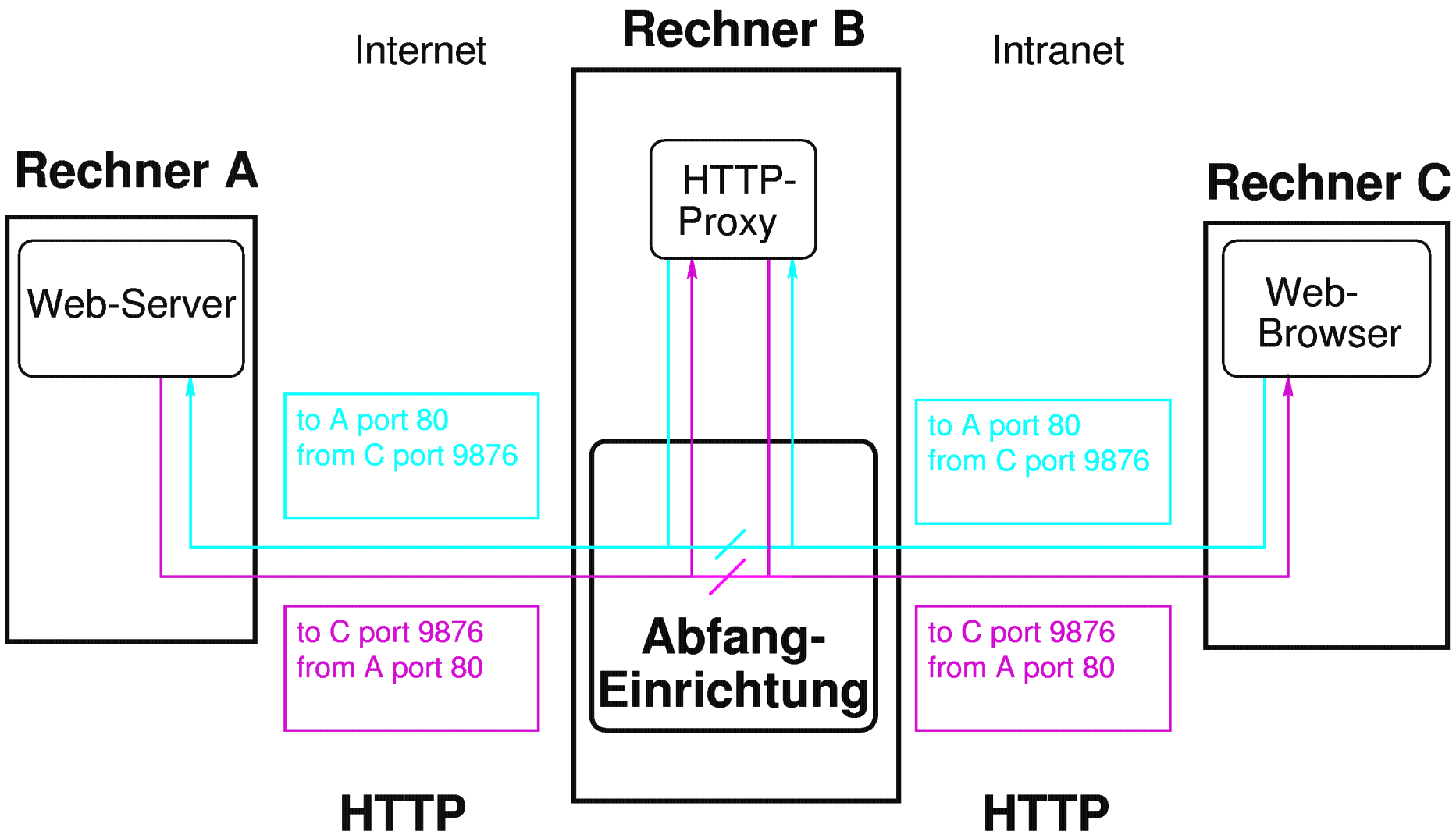
Funktion eines Proxies

Beispiel: HTTP-Proxy



Transparenter Proxy

Beispiel: HTTP-Proxy



Kontrollmöglichkeiten von Filtern und Proxies:

Filter:

- Quelle, Ziel, Port (Dienst)
- Packetinhalt
- Nicht: Datenstrom

Proxy:

- Quelle, Ziel, Dienst
- Datenstrom
- Applikationsfunktionen

Loggingmöglichkeiten von Filtern und Proxies:

Filter:

- Quelle, Ziel, Port (Dienst)

Proxy:

- Quelle, Ziel, Dienst
- Verbindungsdaten
- Applikationsfunktionen

Fazit: Filter gegen Proxy

Filter:

- nur Verkehrsregelung, keine inhaltliche Kontrolle
- schnell, einfach zu warten
- zugreifbare Endsysteme müssen eigenen Schutz aufweisen
- Loggingmöglichkeiten stark eingeschränkt

Proxy:

- ermöglicht komplette Kontrolle der Verbindungsinhalte
- langsam, hoher Wartungsaufwand
- erlaubt Schutz von zugreifbaren Endsystemen
- erlaubt erweitertes Logging

Denial-of-Service Attacken

- basieren auf Überlastung oder Fehlern im Zielsystem
- machen einen Dienst/ein Netzwerk unbenutzbar
- reine Sabotageattacken
- oft einfach zu realisieren
- schwer abzuwehren

Ping-flooding:

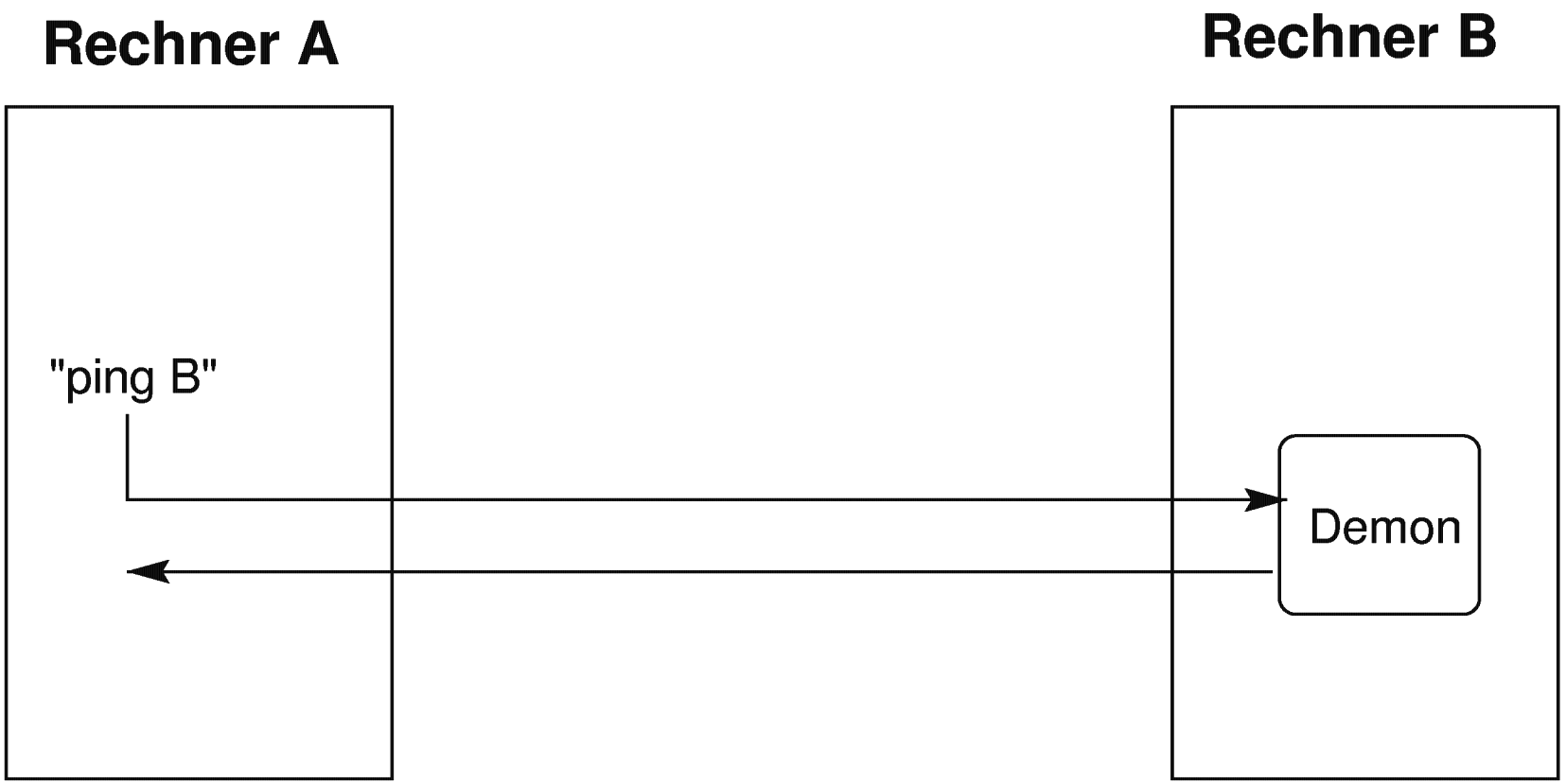
Schickt große Anzahl von Ping-Anfragen an das Zielsystem

- Bindet Resourcen im Zielrechner (bis zum Zusammenbruch)
- Verursacht Netzlast

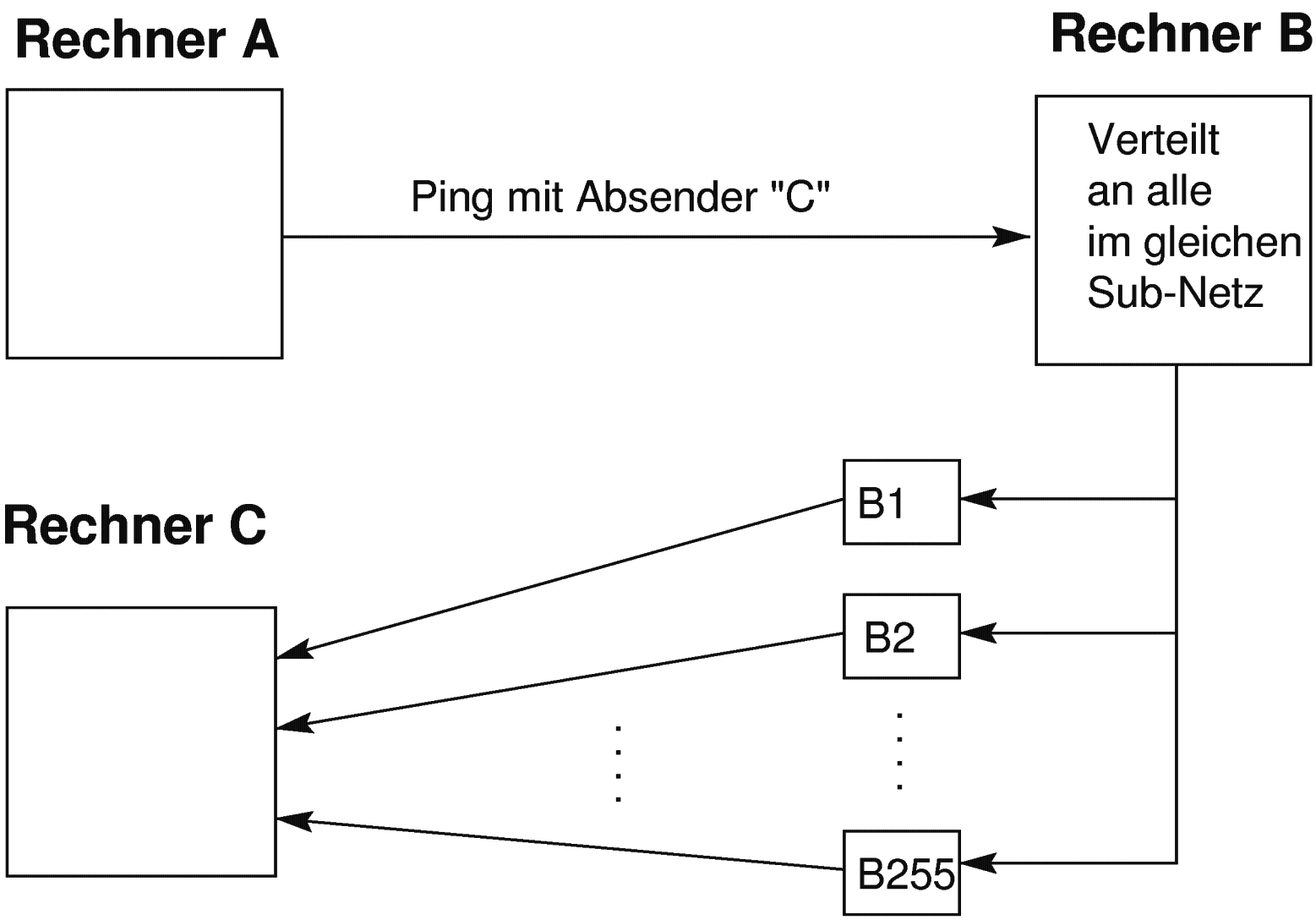
Verbesserte Variante: „Smurf-Attacke“:
Verschlimmerung um Faktor bis zu 255!

Abwehr: Lastüberwachung und dynamische Anpassung des Routing

Funktion von "Ping"

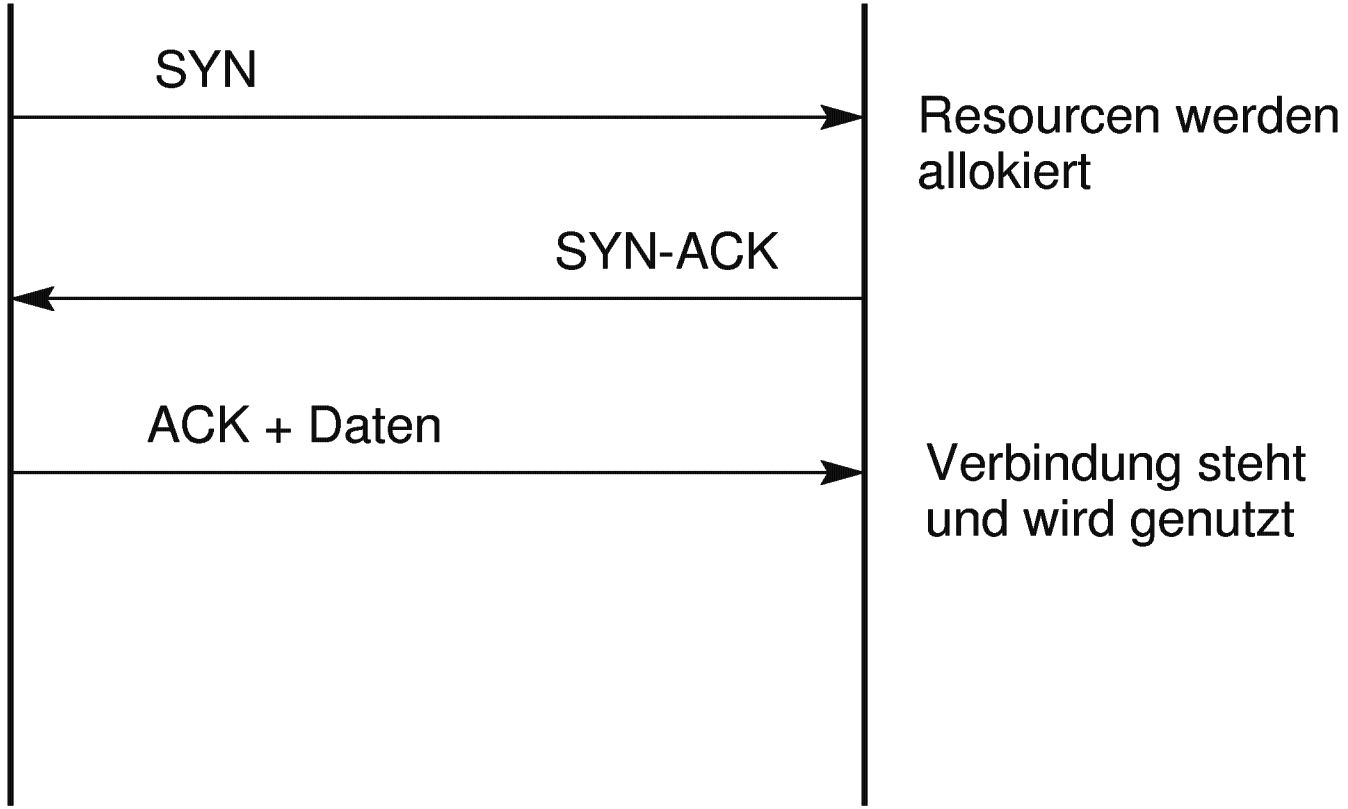


"Smurf"-Attacke

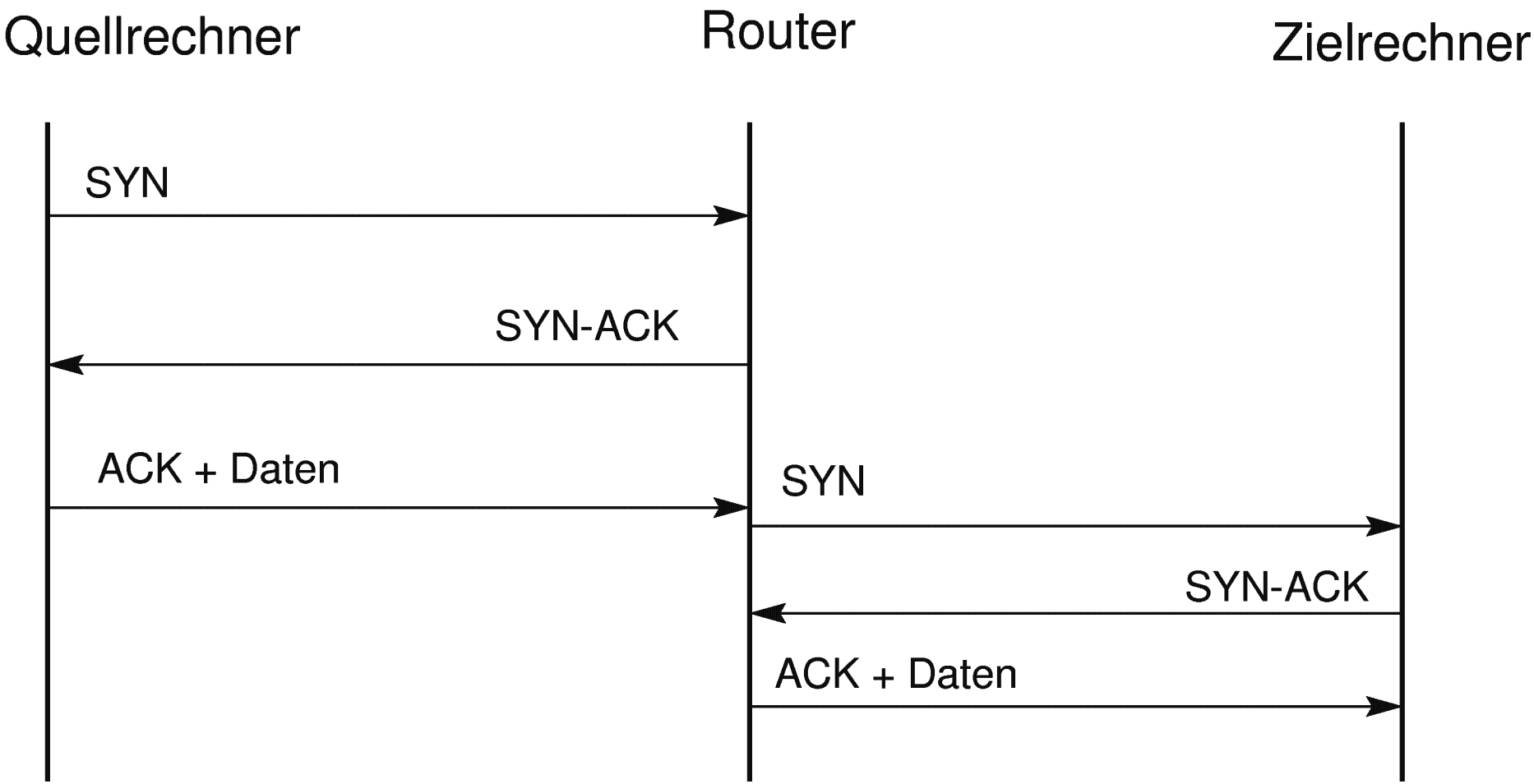


SYN-Flooding

TCP-Verbindungsaufbau



SYN-Flooding: Abwehr



Fazit

Firewalls sind kein „Allheilmittel“!

- Mit Filtern müssen die erreichbaren Rechner/Anwendungen immer noch sicher sein.
- Proxies erlauben ein ausgereiftes Sicherheitskonzept. Bei gravierenden Sicherheitsproblemen in Anwendungen ist hoher Aufwand notwendig.
- Die Firewallrechner müssen besonders sicher sein.
- Ohne kompetente Administration ist niedrigste/keine Sicherheit gegeben.
- Firewallsysteme müssen maßgeschneidert werden.