Grundlegende Begriffe

Um Doppelungen zu vermeiden, soll an dieser Stelle auf zwei wesentliche Wikipedia-Artikel hingewiesen werden, welche die grundlegenden Begriffe erläutern:

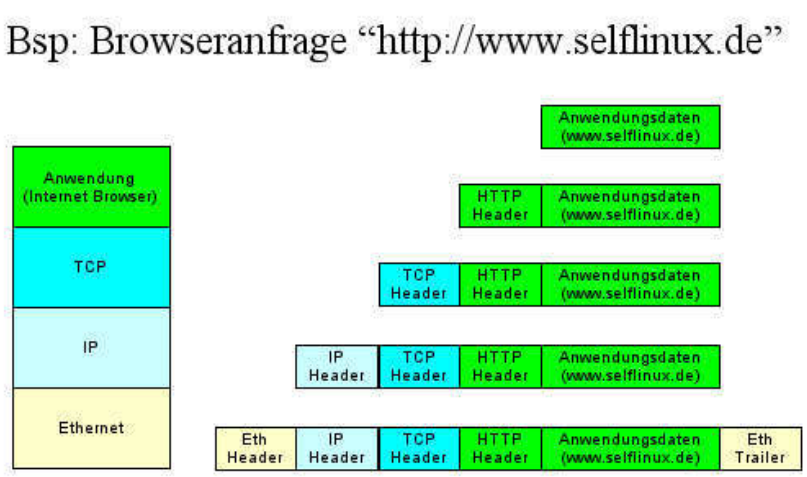
- wikipedia:de:OSI-Referenzmodell
- wikipedia:de:TCP/IP (TCP/IP-Schichtenmodell, Adressierung, Protokolle TCP/UDP/ICMP/IP/ARP, Ports)

Grundlegendes zu Paketfiltern

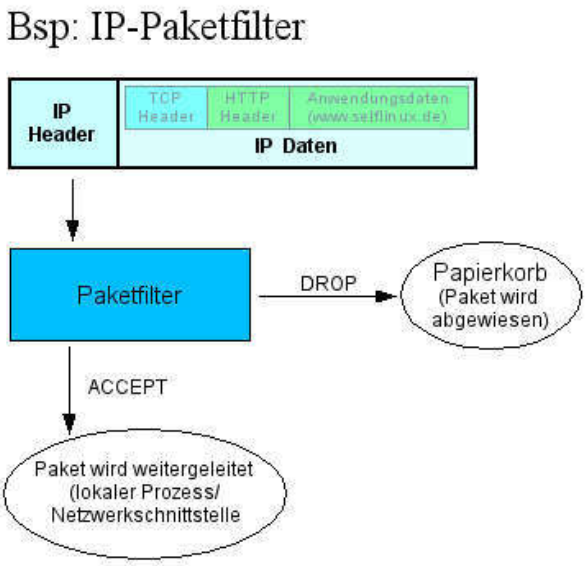
Die Aufgaben und der Zweck eines Paketfilters wurden bereits im Kapitel Überblick zur Sicherheit von Linux-Systemen gründlich vorgestellt. Ebenso wurde eindringlich davor gewarnt, einen Paketfilter als einzige Maßnahme zur Sicherung des heimischen Computers bzw. des kleinen Firmennetzwerks einzusetzen.

Was ist nun ein Paketfilter und wie arbeitet dieser?

Bei paketorientierten Netzwerkprotokollen (z. B. ip, tcp, udp) werden die Daten in Pakete verpackt und ein Header (Paketkopf) vorangestellt.



Paketfilter werten den Paketkopf (Header) aus und entscheiden anhand dessen über das weitere Schicksal des ganzen Paketes. Entweder wird das Paket verworfen (Drop), das bedeutet, es wird einfach gelöscht, oder es wird akzeptiert (ACCEPT), das heißt es passiert den Filter, oder es wird etwas Komplizierteres gemacht, auf das ich später eingehen werde.



Bei Linux ist ein Paketfilter im Kernel integriert (einkompiliert oder als eingebundenes Modul). Mit Hilfe eines Programms (z. B. ipchains für Kernel 2.2 oder iptables für Kernel 2.4/2.6) kann man mit dem Filter kommunizieren. Dies beinhaltet unter anderem das Aufstellen von Regeln, mit denen man definieren kann, welche Pakete den Filter unter welcher Voraussetzung passieren dürfen.

Was leistet ein Paketfilter?

Kontrolle und Sicherheit

Ein Paketfilter kann anhand des Pakettyps, anhand des Herkunftsortes und anhand weiterer Eigenschaften des Paketes bestimmte Kommunikationsarten erlauben oder verbieten. Die Entscheidung basiert nicht auf dem Inhalt des Paketes.

Ein Beispiel: Die meisten Internetbenutzer wollen keine eigenen Dienste vom heimischen PC aus anbieten. Es sollte also niemandem aus dem Internet heraus erlaubt sein, eine Verbindung zu dem privaten PC aufzubauen.

Zweites Beispiel: Ein mittelständiges Unternehmen unterhält eine eigene kleine Entwicklungsabteilung, deren Erkenntnisse einer gewissen Geheimhaltungsstufe unterliegen:

Die Dokumente sollen nicht in die Hände der Konkurrenz fallen. Das schwierige an der Sache ist, dass die Mitarbeiter für ihre Arbeit einen WWW-Zugang benötigen. Ein Paketfilter hat die Aufgabe, den Datenaustausch von geheimen Dokumenten zu erschweren. Wie – dies wird später erläutert.

Paketfilter können auch sehr differenziert entscheiden, wer etwas darf und wer nicht.

Beobachtung des Netzverkehres

Paketfilter können auch den Datenverkehr überwachen und bei Unregelmäßigkeiten eine Meldung erzeugen.

Ein Beispiel: Nachts drei Uhr wird eine Internetverbindung aufgebaut. Da um diese Zeit keiner in der Firma sein dürfte, liegt die Vermutung nahe, es könnte ein Virus oder ein Trojanisches Pferd ungewollte Dinge verrichten.

Paketumleitung und Paketmanipulation

Paketfilter können den Datenverkehr auf einen Proxy umleiten, der auf Applikationsebene Entscheidungen fällt. Damit lassen sich beispielsweise transparente Virenscanner oder Kindersicherungen einrichten, und zwar ohne dass die Netzwerkteilnehmer (also z.B. Schüler) etwas davon merken.

Ein weiteres Einsatzgebiet stellt NAT bzw. IP-Masquerading dar. Damit lassen sich beispielsweise viele Rechner über eine einzige ISDN- oder DSL-Verbindung mit dem Internet verbinden.