Paketfilterung

D-Link Deutschland GmbH / Marcus Schmitt

13. Dezember 2006

Inhaltsverzeichnis

1 Aufgabe dieses Dokuments

Dieses Dokument soll die Aufgabe und Funktionsweise von Paketfilterung beschreiben. Hierbei geht es nicht um Details der Abwicklung bestimmter Protokolle. Es soll hiermit ein Überblick über Paketfilterung vermittelt werden um diese Art der Filter somit besser verstehen zu können. Dieses Dokument lässt die Nutzung von NAT komplett ausser acht, da dies den Rahmen dieses Dokuments sprengen würde.

2 Paketfilterung allgemein

2.1 Was ist ein Paket ?

Wenn Sie über den Browser eine Webseite aufrufen, erhalten Sie vom Webserver eine Antwort. Meistens in Form des Inhalts der Website. Beispielsweise erhalten Sie beim Aufruf von "www.google.de" das Suchfenster um nach einem bestimmten Begriff suchen zu können. Sowohl beim Senden der Anfrage, als auch beim Erhalten der Antwort werden Daten übertragen. Da die Antwort von "www.google.de" Bild und Text enthält, kann dies nicht in einem einzigen Paket alleine übertragen werden und wird in einige kleiner Stücke aufgeteilt. Alle Filterregeln, die Sie in der Firewall oder im Internet-Gateway eingeben, werden auf jedes einzelne dieser Paket angewendet.

2.2 Warum Filtern ?

Die Filterung von Paketen ist wichtig um beispielsweise Personen im Internet keinen Zugriff auf den Heimcomputer oder den Firmencomputer zu gewähren. Wenn Pakete vom Internet auf die Firewall bzw. das Internetgateway treffen, so wird jedes dieser Pakete geprüft, ob eine Weiterleitung erlaubt ist oder nicht.

2.3 Grundlegende Firewalleinstellung ohne Filterregel

Wenn keine Filterregeln definiert sind, werden in den meisten Firewalls und Internet-Gateways alle Pakete verworfen. Dies soll im konkreten Fall folgendes bedeuten: Eine Person im Internet versucht auf die Windowsfreigaben Ihres PC zu gelangen, die Anfrage "Zeig mir deine Freigaben" gelangt vom PC der Person im Internet auf das Internet-Gateway bzw. die Firewall. Dort vergleicht der Paketfilter, ob eine Anfrage an den PC erlaubt ist. Sollte keine Regel für die Freigabe definiert sein, so wird diese Anfrage abgelehnt und der Anfrager aus dem Internet erhält die von Ihm gewünschte Antwort nicht.

3 Inhalt eines Pakets

Datenpakete bestehen aus verschiedenen Teilen. Grob unterteilt besteht es aus einem Teil mit Informationen über die Quelle und dem Ziel (dem sogenannten Header) und dem eigentlichen Datenteil (also beispielsweise dem Teil der Webseite (dem sogennanten Body)). Bei der Paketfilterung ist der Body nicht von Bedeutung. Wichtig sind die Informationen im Header. Der Header enthält unter anderem folgende Informationen:

Quell-IP	IP-Adresse des Senders
Ziel-IP	IP-Adresse des Empfängers
Ziel-Port und Protokoll	Information des genutzten Diensts

Der Header enthält noch mehr Informationen als die eben erwähnten. Hier soll auf diese Informationen nicht eingegangen werden. Sollten Sie hierzu genauere Informationen wünschen, so finden Sie Literaturempfehlungen oder Weblinks unter Kapitel 6 auf Seite 3.

4 Ziel-Ports und Protokolle

Im Normalfall werden die von Computer angebotenen Dienste an speziellen Informationen im Header des Datenpakets erkannt. Diese Informationen sind im Regelfall das Protokoll und der Ziel-Port. Dies bedeutet, dass wenn beispielsweise ein Webbrowser eine Information vom Webserver abrufen möchte, der Webserver über eine spezielle Information (eben über das Protokoll und den Ziel-Port) angesprochen wird. Würde man einem Browser einen anderen Zielport oder ein anderes Protokoll angeben und wollte von dort die Webinhalt abholen, so wäre dies nicht möglich, da der Webserver nur auf den offiziellen Port reagiert.

4.1 Ports in Verbindung mit den gängigsten Internetprotokollen

Obwohl bei den meisten Firewalls und Internet-Gateways die Dienste mit den Protokollen und Port verknüpft sind und bereits durch eine interne Tabelle für den Benutzer in Zusammenhang gebracht wurde, soll die nächste Tabelle zur Vervollständigung dienen.

Dienst	Beschreibung	Protokoll	Port
http	Aufruf von Websites	TCP	80
pop3	Abholen von E-Mails	TCP	110
smtp	Senden von E-Mails	TCP	25
ftp	Filetransfer	TCP	20 + 21
dns	Auflösung Domainnamen zu IP-Adresse	meist UDP	53

5 Paketfilterung im Speziellen

Sollten Sie selbst keinen Webserver, Mailserver oder FTP Server anbieten, so müssen keine Port vom Internet in das interne Netz (auf den PC) freigegeben werden. Bei der Datenübertragung in die entgegengesetzte Richtung steht Ihnen frei, ob Sie von Ihrem PC (Ihrem internen Netzwerk) verschiedene Ports in Verbindung mit Protokollen sperren oder nicht. Er gäbe beispielsweise die Möglichkeit für einen speziellen PC nur HTTP und DNS freizugeben, somit wäre im Normalfall keine Kommunikation mit dem E-Mail Server möglich.

Aber Achtung: Einige Programme, wie z.B Filesharing, Skype usw. versuchen auch eine Verbindung über beispielsweise Port 80 aufzubauen. Einen 100%igen Schutz bei ausgehenden Verbindungen bietet ein Paketfilter also nicht.

6 Literaturtipps

6.1 Bücher

Das Firewall Buch	SuSE Press	ISBN 3-934678-40-8
Einrichten von Internet Firewalls	O'Reilly	ISBN 3-89721-169-6

6.2 Weblinks

http://www.itseccity.de/content/fachbeitraege/grundlagen/020720_fac_gru_kknetworks.html

7 Glossar

Internet-Gateway	Hiermit sind Geräte gemeint, welche eine Internetverbindung fr mehrere PCs zur Verfgung stellen
Dienst	Anbieten eine Leistung, welche von mehreren PCs genutzt werden können z.B. Mail, Webserver etc.