KAPITEL 12

Firewall

Linux-Computer sind wie jede andere technische Vorrichtung möglichem Missbrauch ausgesetzt. Während der Missbrauch durch einen Angreifer mit direktem Zugriff auf die Hardware nicht zu vermeiden ist, können missbräuchliche Zugriffe auf die Software weitestgehend vermieden werden. Zugriffe auf die Hardware können nur durch die Verhinderung eines direkten Zugangs, wie das Einschließen in Schränke und ausgewiesene EDV-Räume mit Zutrittsbeschränkung und abschließbare Gehäuse vermieden werden. Die Entsprechung der physikalischen Einschränkung des Zugriffs durch eine Wand (eines Gehäuses oder Gebäudes) entspricht die Firewall (Brandschutzmauer) auf Softwareseite. Eine Firewall schirmt einen *Linux*-Computer gegen Angriffe aus dem Netz ab. *Linux*-Computer ohne Netzzugriff benötigen keine Firewall.

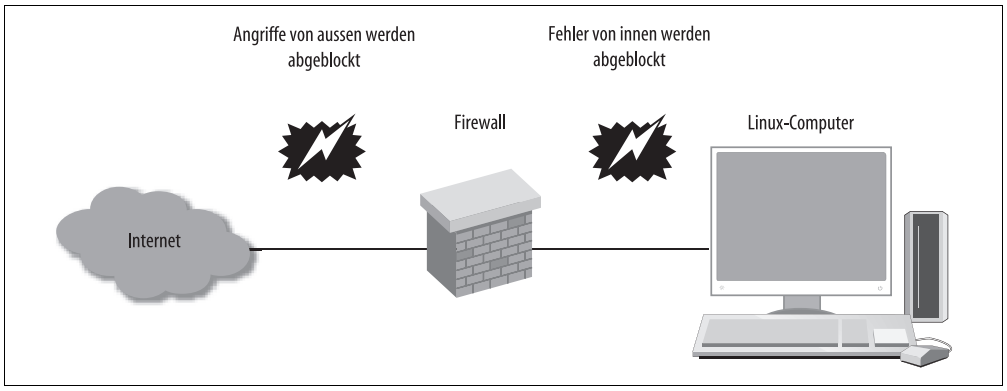

Abbildung 12-1: Prinzip einer Firewall

Schutz für Ihren Computer

Linux-Computer sind von sich aus relativ sicher, da das Entwurfsprinzip von Computern der *Unix*-Familie war und ist, nur das Unverzichtbare einzuschalten und zu erlauben.

Risikoananlyse

Angriffe auf *Linux*-Computer kennt aus zwei Formen heraus

- Vandalismus und
- Ressourcenmissbrauch.

Vandalismus richtet sich gegen alles, was dem Angreifer zugänglich ist. Die Motivation des Angreifers ist oft Spieltrieb, Neugier oder Schadenfreude im weitesten Sinne, leider auch zunehmend Erpressung. Hinter Ressourcenmissbrauch stehen meist wirtschaftliche Interessen oder eine Ideologie. Beim Ressourcenmissbrauch werden gezielt eine oder einige wenige Funktionen eines Computers genutzt

Vandalismus

Vandalismus richtet sich gegen die Funktionsfähigkeit eines *Linux*-Computers. Dies kann durch Beschädigen der Software oder durch Behinderung des Netzzugangs erfolgen.

Zur Beschädigung der Software auf dem *Linux*-Computer muss der Angreifer entweder ausführbaren Code auf den *Linux*-Computer einschleusen (*Malicous Code*) oder sich einen direkten Zugang auf den Linux-Computer verschaffen (*Hacken*). Das Einschleusen von Code erfolgt häufig unter Ausnutzung häufiger, charakteristischer Programmierfehler von Serverprogrammen wie den Web- oder den FTP-Servern. Einen unberechtigten Zugang kann sich ein Angreifer auch verschaffen, indem er Passwörter errät beziehungsweise stiehlt oder Programmierfehler in einem der Programme für den Fernzugriff wie `telnetd` oder `sshd` ausnutzt. Stehlen wird ihm besonders durch Programme wie `telnet` oder `ftp` leicht gemacht, da hier die Passwörter unverschlüsselt über das Netz übermittelt werden und ein schlichtes Mithören (Sniffing) auf dem Netz alles verrät.

Die Behinderung des Netzzugangs kann durch *Denial-of-Service*-Attacken erfolgen. Dabei werden – an sich legitime – Anforderungen an den *Linux*-Computer mit so hoher Häufigkeit abgesetzt, dass für die eigentlichen Aufgaben keine Kapazität mehr zur Verfügung steht.

Ressourcenmissbrauch

Auch ein *Linux*-Computer kann für illegale Taten benutzt werden. Zum Schutz vor Verfolgung wird versucht, die Ressourcen von Computern anderer Besitzer für die illegalen Zwecke zu missbrauchen. Das können das Auslösen von Denial-of-Service-Attacken gegen Dritte sowie das Speichern von illegalen Inhalten wie Pornografie oder raubkopierter Software und Filme und das Versenden von Spam-Mails sein. Spam-Mail ist das Versenden von E-Mails werblichen Inhalts, die vom Empfänger unerwünscht sind. Spam hat sich als eine der größten Gefahren für die Funktionsfähigkeit des Internets herausgestellt. Ein von Unberechtigten in Besitz genommener Computer kann wegen der ihm zugestandenen Rechte zur Ausforschung der Netze, zu denen er direkt Zugang hat, verwendet werden.

Abwehrmaßnahmen

Die erste, einfachste und sicherste Maßnahme besteht im Abschalten aller der Dienste auf einem *Linux*-Computer, die augenblicklich nicht benötigt werden. Wenn sie nie benötigt werden, sollte auch ein Deinstallieren in Betracht gezogen werden.

Wenn ein Dienst nicht in vollem Leistungsumfang benötigt wird, kann die Menge der Leistungen im Allgemeinen über seine Konfigurationsdatei angepasst werden. Oft steht neben dem installierten Dienst auch noch ein anderer mit deutlich geringem Leistungsumfang zur Verfügung, der den Ansprüchen genügt. Dies gilt insbesondere für Web- und FTP-Server.

Compiler- und Skriptsprachen sind auf ihre Unverzichtbarkeit zu prüfen. Sie können zur Erzeugung von Schad-Programmen (Malicous Code) verwendet werden und sollten – wenn nicht benötigt – vom *Linux*-Computer entfernt werden.

Programmierfehler in den Serverdiensten und im Kernel werden von besonderen Institutionen (*CERT = Computer Emergency Response Team*) überwacht. Ihre Bulletins enthalten die Fehlerbeschreibung und die Abhilfe. Der Betreiber eines direkt mit dem Internet verbundenen *Linux*-Computers muss diese Bulletins regelmäßig lesen und die Anweisungen befolgen.

Wenn das Anbieten von Diensten durch einen *Linux*-Computer im Internet unverzichtbar ist, müssen über eine sorgfältige Installation und Administration der Dienste hinaus die Dienste gegen Missbrauch mit einer Firewall geschützt werden.

Eigenschaften einer Firewall

Eine Firewall verbindet mindestens zwei Netze miteinander. Im Fall eines mit dem Internet verbundenen *Linux*-Computers wird das innere, virtuelle Netz mit dem Internet über die Linux-Firewall kontrolliert verbunden.

Die Firewall kontrolliert den Datenaustausch zwischen den verschiedenen Netzen, an die sie angeschlossen ist. Der Verkehr innerhalb eines Netzes kann von ihr beobachtet werden, ein Unterbinden problematischen Datenverkehrs innerhalb eines Netzes kann sie jedoch nicht vornehmen.

Datenverkehr in lokalen Netzen und im Internet findet paketvermittelt statt. Daten und Aufforderungen zum Datensenden werden in relativ kleinen Paketen untergebracht, die eine Absender und Empfängeradresse führen. Zur Kennzeichnung des Verwendungszwecks werden auch noch Dienste-Kennungen[1] (Port Numbers) vergeben, die teilweise festgelegt sind (Siehe */etc/services* – übrigens unter den Windows-Versionen gibt es eine entsprechende Datei, sie liegt bei neueren NT-Versionen unter \windows\system32\drivers\etc\services). Neben diesen Grundinformationen enthält jedes Paket auch noch diverse Zähler und Zustellanweisungen.

1 *http://www.iana.org/assignments/port-numbers*

Ein lokales Netz mit mehreren Teilnehmern sollte eine Firewall erhalten, vorzugsweise durch die Verwendung eines *Linux*-Computers. Neben der vereinfachten Verwaltung aller Computer im Netz empfiehlt sich bei diesem Ansatz, Dienste zentral zusammenzufassen, wie die Mail-Zustellung. Ein eigener Mail-Server mit integriertem Virenscan befreit Arbeitsplatzrechner von der viel Rechenzeit verbrauchenden lokalen Virensuche. Proxyserver für die verschiedenen benötigten Dienste aus dem Internet erlauben eine noch viel weiter gehende Sicherheit und Leistungsverbesserung. Die Firewall ist die zentrale Verteilstelle für die unterschiedlichen Dienste auf die spezialisierten Computer.

Eine Firewall verhindert den direkten und den vollständigen Zugriff aus dem Internet auf einen hinter ihr im geschützten Netz liegenden Computer. Sie prüft Zugriffe aus dem Internet auf Zulässigkeit und Berechtigung. Sie verhindert, dass Computer im von der Firewall geschützten Netz unerwünschte Zugriffe auf das Internet vornehmen. So kann hinter einer Firewall ein willentlich oder unwissentlich falsch bedienter Computer nur geringeren Schaden anrichten und ein von einem Angreifer in Besitz genommener Computer nicht den vollen Absichten des Angreifers Genüge tun.

Häufig ist eine Firewall zugleich ein Router. Sie verbindet so unterschiedliche Netze und kann damit netzübergreifende Aktionen erlauben oder verbieten. Ein Router nimmt dann oft auch noch eine Adress-Umsetzung (*NAT = Network Address Translation*) vor. Er versteckt damit die im lokalen Netz liegenden Computer vor dem Internet. Im lokalen Netz liegende Computer geben ihre Anforderung an einen Computer im Internet an die Firewall-Router-Kombination weiter und diese macht sie sich gewissermaßen zu eigen und sendet sie als ihre eigene Anforderung in das Internet. Der Computer im Internet antwortet der Firewall-Computer-Kombination direkt und sieht den lokalen Rechner nicht. Die Firewall-Router-Kombination leitet die Antwort aus dem Internet dann so weiter, als sei sie direkt an den lokalen Computer gerichtet. Wenn mit NAT gearbeitet wird, ersetzt die Firewall-Router-Kombination die Adresse des lokalen Senders durch die eigene, und leitet die eintreffenden Reaktionen an den lokalen Empfänger weiter, wobei sie wieder die Adresse umsetzt, diesmal wird anstelle der eigenen Adresse die des lokalen Empfängers einsetzt.

Für höherer Sicherheitsanforderungen werden zwei Firewalls hintereinander geschaltet. Die innere Firewall blockiert alle unzulässigen Zugriffe aus dem inneren, lokalen Netz. Im Zwischennetz, der so genannten *Demilitarisierten Zone* (*DMZ*) liegen Proxy-Server, die Anforderungen der Computer im lokalen Netz umsetzen und filtern. Die äußere Firewall verwirft alle unzulässigen Zugriffe aus dem globalen Internet. Zugriffe aus der DMZ werden von beiden Firewalls streng kontrolliert.

Eine sehr ökonomische Lösung ist eine gewissermaßen anderthalbstufige Firewall mit mindestens drei Interfaces für das innere Netz, die DMZ und das äußere, globale Netz. Bei störungsfreiem Funktionieren ist sie in ihrer Funktion nicht von einer echten zweistufigen Firewall zu unterscheiden. Sie ist jedoch gegenüber Angriffen gegen sie selber wesentlich weniger widerstandsfähig, da bei einer zweistufigen Firewall die zum Erreichen des inneren Netzes notwendigen Angriffe zweimal erfolgen müssen. Wenn die beiden Firewalls einer zweistufigen Lösung zudem noch unterschiedliche Betriebssysteme,

Software und Passwörter besitzen, ist die Zeit für eine erfolgreich Attacke verdoppelt. Der Angriff auf die erste Firewall führt zudem häufig zu Leistungseinschränkungen, die bemerkt werden können und zu sofortigen Gegenmaßnahmen Gelegenheit geben.

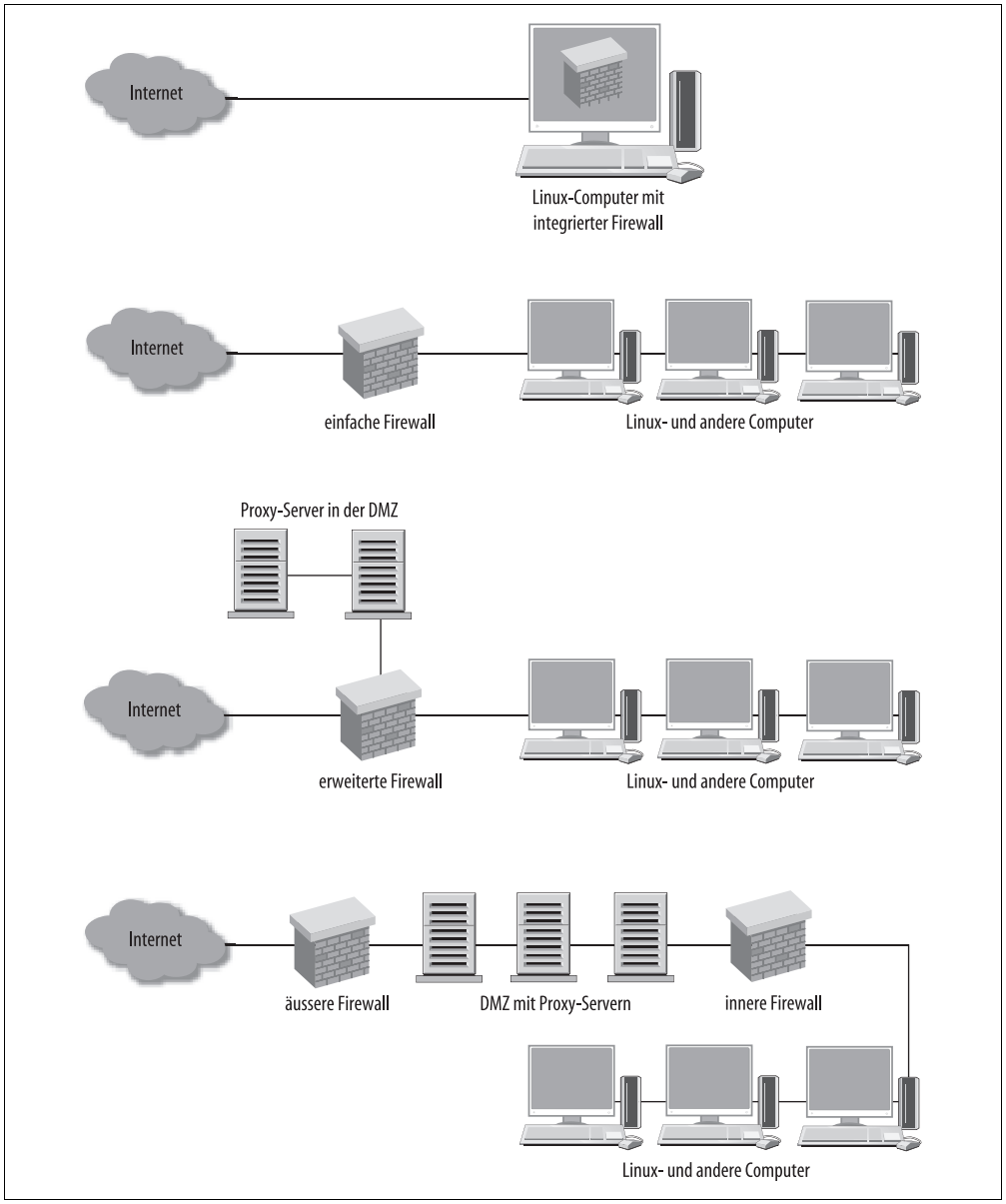

Abbildung 12-2: Einfache, erweiterte und zweistufige Firewall

Adress-Analyse

Die Firewall prüft für jede Schnittstelle, ob eine Datenanforderung oder Datensendung aus der zulässigen Klasse von Adressen stammt. Anforderungen anderer Adressen werden nicht zugelassen. Ein beliebter Trick zur Ausspähung von lokalen Netzen ist die Verwendung von Anforderungen mit Source-Route-Einträgen. So sollen Computer im Netz veranlasst werden, sich mehr oder minder direkt mit bestimmten Computern im Netz zu verbinden. Die Firewall fängt das ab.

Port-Analyse

Jeder Dienst hat eine Port-Nummer (Dienstadresse). Eine Firewall kann so konfiguriert werden, dass sie nur bestimmte Dienste und damit Portnummern zulässt. Sie kann auch angewiesen werden, bestimmte Dienste nur auf ausgewählte Adressen und Dienstanforderungen nur von berechtigten Adressen zuzulassen. Insbesondere kann so die Verwendung eines Proxy-Servers obligatorisch gemacht werden. Über einen Proxy-Server kann eine gezielte Auswahl von Internetinhalten vorgenommen werden, beispielsweise die Beschränkung auf jugendfreie Inhalte.

Paket-Analyse

Innerhalb eines bestimmten Dienstes (Portnumber) sind manche Informationen völlig unbedenklich, andere können problematisch sein. Die Firewall kann angewiesen werden, die unproblematischen Paket durchzulassen und die problematischen zu sperren.

Stateful Firewall

Das gezielte Versenden von unangeforderten Paketen, die ihrerseits eine Quittierung des Empfangs oder sonstige Antwort anfordern, ist eine verbreitete Methode zur Ausspähung von Netzen hinter einfachen Firewalls und Routern. Eine leistungsfähige Firewall vergleicht ein- und ausgehenden Verkehr und blockiert eingehende Pakete, für die keine Anforderung vorlag.

Realisieren einer Firewall

Jeder *Linux*-Computer, der über mindestens zwei Netzwerkanschlüsse verfügt, kann Firewallfunktionen übernehmen. Dabei können die Netzwerkanschlüsse beispielsweise

- zwei gleichartige LAN-Anschlüsse (Local Area Network) sein, aber auch gemischt, wie
- LAN – WLAN (Wireless Local Area Network),
- LAN – ISDN (Integrated Services Digital Network),
- LAN – Modem,
- LAN – DSL (Digital Subscriber Line) oder eine sonstige Kombination.

Daneben muss ein Kernel installiert sein, der

```
[*] Network packet filtering (replaces ipchains)  --->
```

und in dem Untermenü

```
IP: Netfilter Configuration  --->
```

die Optionen – möglichst als Modul – aktiviert sind. Dies ist bei den von den Distributoren bereitgestellten Standardkerneln der Fall. Ebenso gilt dies für die Standardkonfiguration der unmodifizierten Standardkernel[2]

Bedarfsanalyse

Die Planung und Einrichtung einer Firewall kann sehr anspruchsvoll sein und viel Arbeitszeit verschlingen. Für den Durchschnittsanwender sind jedoch die Konfigurationsskripten der Distributoren aber ausreichend. So empfiehlt sich im Einzelnen

Tabelle 12-1: verschiedene Firewall-Lösungen

Situation	Maßnahmen
Einzelner Linux-Computer ohne Internetanbindung	Keine Firewall notwendig
Einzelner Linux-Computer mit Internetanbindung für Privatnutzung	Integrierte Firewall (gemäß Distributorvorgaben) mit Portfilterung
Einzelner Linux-Computer mit Internetanbindung für berufliche Nutzung als Arbeitsplatzrechner	Integrierte Firewall (gemäß Distributorvorgaben) mit Port- und Adressfilterung
Einzelner Linux-Computer mit Internetanbindung für berufliche Nutzung als Server	Integrierte Firewall (gemäß Distributorvorgaben) mit Port- und Adressfilterung, bei kritischer Bedeutung Paketanalyse
Linux-Computer wie oben aber über einen externen Router und LAN an das Internet angebunden	Maßnahmen jeweils entsprechend wie oben
Linux-Computer wie oben, aber über eine externe Firewall und LAN ans Internet angebunden	Port- und Adressfilterung
Linux-Computer als Gateway für ein LAN im privaten Bereich	Firewall (gemäß Distributorvorgaben) mit Port- und Adressfilterung, Paketanalyse
Linux-Computer als Gateway für ein LAN im beruflichen Bereich für allgemeine, unkritische Bürokommunikation	Firewall individuell angepasst mit Port- und Adressfilterung, Paketanalyse, Statusüberwachung
Linux-Computer als Gateway für ein LAN im beruflichen Bereich für Produktion[a]	Zweistufige Firewall individuell angepasst mit Port- und Adressfilterung, Paketanalyse, Statusüberwachung, obligatorische Proxys für alle Dienste, direkte Internetnutzung unterbunden

a Gemeint ist hier nicht nur Warenproduktion, sondern auch das Erbringen von Dienstleistungen.

2 *http://www.kernel.org*

Umsetzung der Adress-Filterung

Zu einer ordentlichen Adressfilterung gehört, dass alle Computer in einem lokalen Netz (LAN) eine feste Adresse besitzen. Nur so sind Verursacher von Störungen zu identifizieren. Daher muss bei Benutzung von `bootp` oder DHCP für alle dauerhaft im Netz befindlichen Computer ein Eintrag in die Konfigurationsdatei vorgenommen werden. Die Störungen, die von gelegentlich im Netz befindlichen Computern verursacht werden, können dann diesen Computern eindeutig zugeordnet werden.

Die von Internet-Providern vergebenen dynamischen Adressen gelten nur für die Interfaces zum externen Netz oder für einzeln am Internet hängende *Linux*-Computer.

Eine einzelne vom Internet-Provider vergebene IP-Adresse kann zur Anbindung eines einzelnen *Linux*-Computers mit Firewallfunktionalität an das Internet verwendet werden. Diese Adresse kann sowohl dynamisch als auch fest sein. Der *Linux*-Computer kann den Zugang anderen Computern zur Verfügung stellen. Die Verwendung von Adress-Umsetzung ist dabei zwingend. Die IP-Adressen für das private Netz müssen auf jeden Fall aus dem für private Netze reservierten Bereich[3] stammen.

Netzadressen	Verwendung
0.0.0.0	Internes Netz für Verwaltungszwecke
10.0.0.0	A-Class-Netzwerk für private Netze
127.0.0.0	Internes Netz für Verwaltungszwecke
169.254.0.0	Internes Netz für Verwaltungszwecke
172.16.0.0 – 172.31.255.255	B-Class-Netze für private Netze
192.168.0.0 – 192.168.255.255	C-Class-Netze für private Netze
224.0.0.0 – 255.255.255.255	Spezielle Verwendung für Broadcast, IP-V6-Einbettung und Weiteres

Bei Vergabe mehrerer IP-Adressen durch den Internet-Provider können Computer hinter der Firewall gezielt von außen über die IP-Adresse angesprochen werden. Typische Anwendungen sind Verschlüsselungs-, Web- und Datenbankserver. Diese Computer müssen in die DMZ einer zweistufigen Firewall verlegt werden.

Umsetzung des Port-Filterns

Jeder tcp/ip-basierte Dienst wird durch eine oder mehrere charakteristische Portnummern[4] beschrieben. Während einige Dienste wie WWW grundsätzlich nur eine feste Nummer (WWW Port 80) verwenden, verwenden andere Dienste wie FTP einige feste Nummern (FTP Port 20 und 21) und zusätzlich dynamisch vergebene Port-Nummern aus einem für dynamische Vergaben reservierten Bereich. Dieser Bereich waren ursprünglich die Portnummern über 1024. Die Zahl der zugewiesenen Ports ist auf über 7000

3 *http://www.isi.edu/rfc/rfc3964.txt*

4 *http://ww.iana.org/assignments/port-numbers*

erweitert worden. Da bei Diensten wie WWW andere Portnummern explizit zugewiesen werden können und manche Anbieter dies auch tun, führt eine Einschränkung in den zulässigen Portnummern durch eine Firewall möglicherweise zu einer Beschränkung der erreichbaren WWW-Server. Hier muss ein individueller Kompromiss zwischen Sicherheit und Anwenderinteressen gefunden werden.

Grundregel der Firewallkonfiguration ist es, nur die unbedingt benötigten Ports freizugeben. Für Programme wie ftp können spezielle Übertragungsformen (Passive FTP) verwendet werden, die den Zugriff auf dynamische Ports vermeiden.

Bei einer mehrstufigen Firewall werden die freigegebenen Ports auf entsprechende Proxy-Server umgeleitet und auf andere Ports umgesetzt, so dass kein Paket aus dem inneren Netz es verlassen kann. Pakete aus dem äußeren Netz können das innere nicht erreichen.

Wegen der hohen Zahl der zugewiesenen Ports und ihrer Verteilung über einen weiten Bereich muss die Verwendung von Ports für die Port-Umsetzung genau geprüft werden.

Umsetzung der Paket-Filterung

Unter den Nachrichten, insbesondere den Netzverwaltungsnachrichten, die Computer über das Netz austauschen, sind einige Typen sehr nützlich und völlig unschädlich. Andere haben neben ihrem hohem Nutzen ein beträchtliches Schadpotential, da sie beispielsweise zur Ausspähung eines von einer Firewall geschützten Netzes dienen können.

Eine Firewall kann angewiesen werden, kritische Pakete zu sperren, zu protokollieren und zu verwerfen.