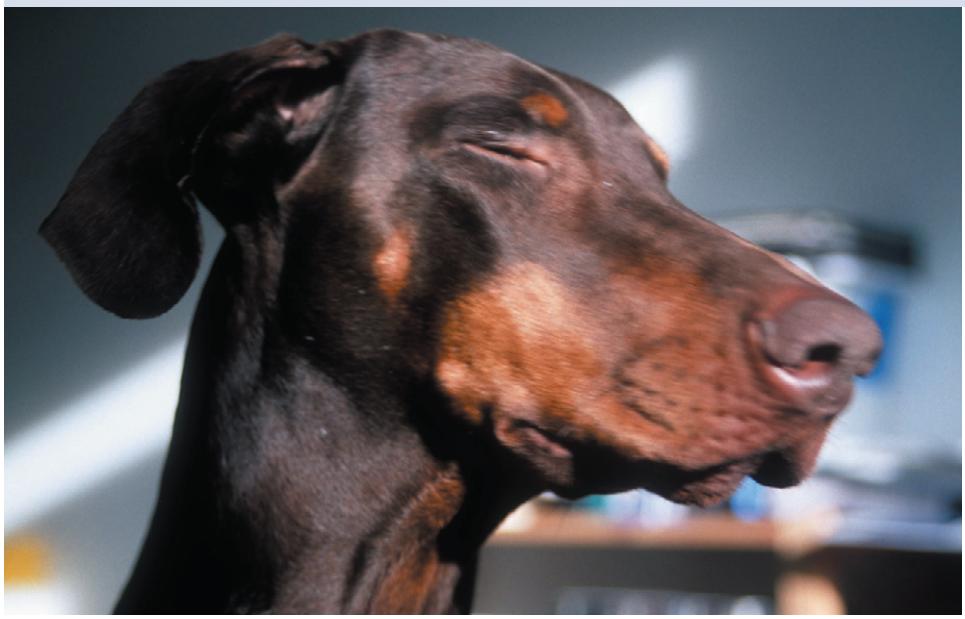
Firewall-Konfiguration mit Guarddog

Eitler Wachhund

Mit wenigen Klicks eine Linux-Firewall einrichten, das verspricht die KDE-Applikation Guarddog. Auch wenig erfahrene Anwender sichern so ihren Rechner oder ein ganzes Netzwerk gegen Angriffe ab. Holger Junge



Für die Konfiguration der Linux-eigenen Firewallfunktionen sind die Tools IPChains (Linux 2.2) und IPTables (Linux 2.4) zuständig. Vor allem Linux-Ein- und Umsteiger haben mit der Bedienung der oft kryptischen Kommandozeilenprogramme so ihre Probleme. Die grafische Oberfläche Guarddog [1] will hier Abhilfe schaffen. Sie läuft mit KDE 2 und 3 und steht unter der GPL.

Die stabile Version ist 2.2.0, sie findet sich auf der Homepage [2] zum Download. Neben den Sourcen gibt es dort auch schon fertige Binärpakete für Mandrake, Red Hat und Debian. Wer die neuesten Features ausprobieren will, der lädt Version 2.3.2 von [2] herunter. Mehr zu dieser Entwicklungsversion im Kasten „Für Mutige“.

Guarddog ist in erster Linie für Heimsysteme und kleine private Netzwerke nützlich. Hersteller wie Red Hat, Mandrake und Suse bieten zwar einfach zu bedienende, grafische Firewall-Tools standardmäßig an. Oftmals verfügen sie aber nicht über die nötigen feingranularen Einstellungsmöglichkeiten. Für Poweruser, die detailliertere Einstellungen vornehmen wollen, ist der Einsatz von Guarddog bei diesen Distributionen ebenfalls sinnvoll.

Gefährliche Sicherheit

Unerfahrene Benutzer sollten bei der Konfiguration ihrer Firewall jedoch Vorsicht walten lassen. Denn die einfache Bedienung per Maus verleitet dazu, mehr Ports zuzulassen als nötig. Umgekehrt ist es auch möglich, einen Rechner so sehr abzusichern, dass Dienste nicht mehr funktionieren.

Außerdem ist Guarddog eine KDE-Applikation, die auf einem klassischen Server-Computer nichts zu suchen hat. Daher sollten alle Anwender, die einen dedizierten Firewallrechner einsetzen, die Konfiguration auf einem Desktop-Computer erstellen und das resultierende Skript auf den Server kopieren.

Da Guarddog auf IPChains respektive IP-Tables setzt, muss der Anwender darauf achten, dass alle nötigen Kernelmodule auf dem Rechner vorhanden sind. Das ist bei den meisten Distributionen der Fall. Ansonsten ist es nötig, den Kernel mit den entsprechenden Optionen neu zu kompilieren.

Die Filterkommandos für die Firewall erstellt der Admin bei Guarddog protokollorientiert. Er muss also nicht selbst die Ports bestimmen, was Konfigurationsfehler reduziert. Guarddog erlaubt auch die Einteilung in verschiedene Maschinengruppen, Zonen genannt. So lässt sich zum Beispiel eine demilitarisierte Zone (DMZ) aufbauen.

Der Administrator muss Guarddog mit Root-Rechten starten, damit das Programm die Firewall-Regeln direkt anwenden kann. Nach dem Start zeigt sich Guarddog, wie in Abbildung 1 zu sehen ist. Die Logik der Oberfläche ist leider nicht sehr intuitiv. Guarddog gruppiert seine Optionen unter vier Reiter: Unter dem Feld »Netzwerkzone« richtet der Anwender die erwähnten Zonen ein, in denen entsprechende Maschinengruppen enthalten sind.

Für Mutige

Die aktuelle Entwicklungsversion von Guarddog ist 2.3.2. An den Einsatz dieser Version in produktiven Umgebungen ist allerdings nur mit Vorsicht zu denken. Mutige kommen in den Genuss einiger neuer Features: Für benutzerdefinierte Protokolle unterstützt 2.3.2 auch Portbereiche.

Außerdem haben die Entwickler die Version für Linux 2.6 angepasst und eine Reihe neuer Protokolle in die Liste integriert wie RSync, Distcc, GKRellm, Bittorrent, PGP Key Server, Jabber über SSL und Microsofts Media-Server-Protokoll.

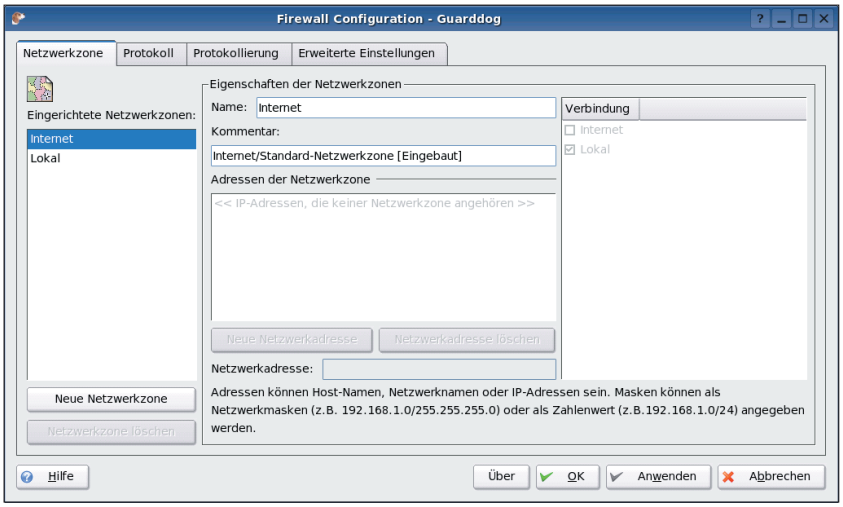


Abbildung 1: Die Guarddog-Oberfläche nach dem ersten Start. Zwei Netzwerkzonen sind bereits eingerichtet, »Internet« und »Lokal«. Auch komplizierte Setups lassen sich in Guarddog nachbilden.

Im Teil »Eigenschaften der Netzwerkzonen« lassen sich dann die IP-Adressen oder -Bereiche jeder Zone festlegen. Die vorkonfigurierten Zonen »Internet« und »Lokal« können nicht gelöscht werden. In Ersterer befinden sich automatisch alle IP-Adressen, die in keiner anderen Zone enthalten sind. »Lokal« enthält alle Adressen der lokalen Netzwerkkarten. Für ein Standalone-System reichen diese beiden Zonen bereits aus.

Protokollbäume

Unter dem Reiter »Protokoll« (Abbildung 2) schalten die Admins einzelne Protokolle frei oder sperren sie. In der Baumstruktur auf der rechten Seite sind die Protokolle nach Kategorien sortiert. Der erste Dienst, den es in der Regel freizuschalten gilt, ist DNS in der Kategorie »Netzwerk«. Ein Klick auf die Checkbox versieht sie mit einem Häkchen, das anzeigt, dass der Dienst auf dem Rechner zugelassen ist. (Die vorgenommenen Einstellungen sind aber erst nach dem Drücken des »Anwenden«-Buttons wirksam.) Ein zweiter Klick auf die Checkbox verwandelt das Häkchen in ein Kreuz. Dann lehnt die Firewall jeden Verbindungsaufbau explizit ab.

Ist eine Checkbox leer, ignoriert die Firewall alle Anfragen an die entsprechenden Ports. Weitere Protokolle, die fast jeder Anwender braucht, sind HTTP, HTTPS und FTP (Kategorie »Dateiübertragung«) sowie SMTP und POP3 (Kategorie »Email«).

Beim Reiter »Protokollierung« stellt der Admin detailliert ein, welche Aktionen

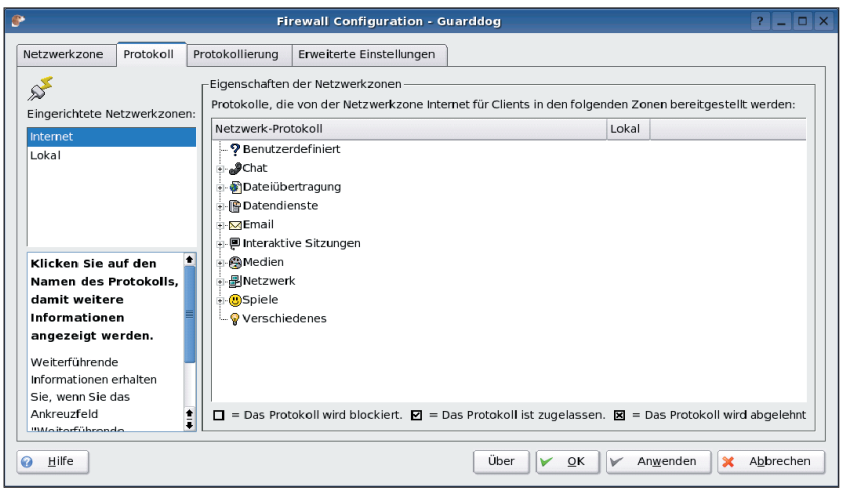


Abbildung 2: Unter dem »Protokoll«-Reiter stellt der Administrator ein, welche Protokolle die Firewall zulassen und sperren soll. Um Portnummern muss er sich dabei nicht kümmern.

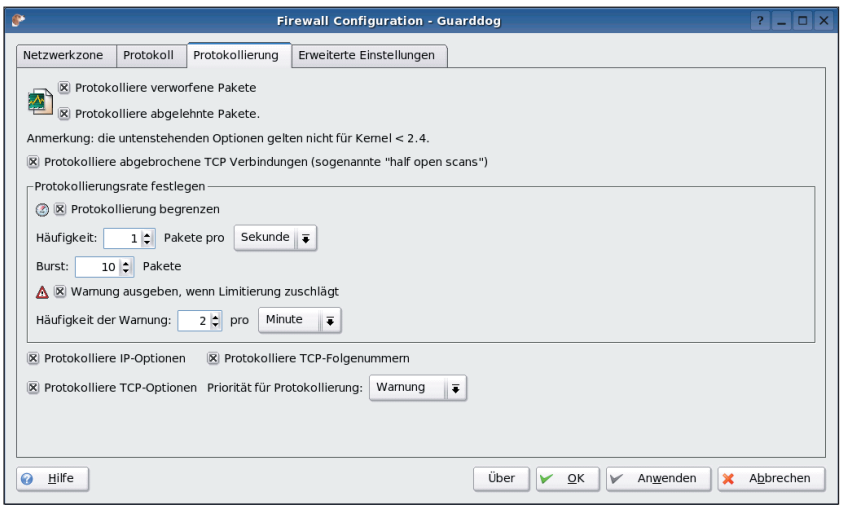


Abbildung 3: In diesem Fenster legt der Admin fest, wie genau die Firewall alle Vorgänge auf dem System protokollieren soll. Dabei schützt Guarddog auch vor bestimmten Denial-of-Service-Angriffen.

Guarddog im Syslog speichern soll. So lassen sich auch Portscans sehr schnell erfassen. Mit der Protokollierungsrate bestimmt der Guarddog-Anwender, wie oft die Firewall Einträge im Syslog vornimmt. Eine Limitierung ist sinnvoll, um Denial-of-Service-Angriffe zu vermeiden. Das Syslog könnte nämlich bei einem Sturm von IP-Paketen rasant wachsen und die Festplatte füllen. Wer alle Details zu den ankommenden IP- und TCP-Paketen erfahren will, stellt im unteren Teil des Fensters ein, alle Optionen der Pakete sowie die TCP-Sequenznummern zu protokollieren.

Unter dem Reiter »Erweiterte Einstellungen« passen erfahrene Admins die Firewall-Details nach ihren Wünschen an. Ist einmal etwas schief gelaufen, setzt ein Klick auf »Werkseinstellung wiederherstellen« Guarddog zurück. Die Einstellung in »Lokaler Bereich für dynamische Ports« ist in den meisten Fällen völlig ausreichend. Sie legt fest, welchen Portbereich Linux für ausgehende Verbindungen nutzen soll.

Im- und Export

Sind nicht alle benötigten Protokolle beim Reiter »Protokoll« voreingestellt, definiert der Admin mit »Neues Protokoll« einfach das passende. Dazu gibt er ihm einen Namen, legt fest, ob es TCP oder UDP spricht, und gibt an, welche Portnummer es benutzt.

Sehr nützlich ist die Möglichkeit, mit Guarddog erstellte Firewallskripte zu im- und exportieren. Guarddog speichert alle Einstellungen nämlich in einem einfachen Shellskript unter »/etc/rc.firewall«. Da auf einem Server in der Regel kein KDE laufen sollte, exportiert der Admin dieses über den »Exportieren«-Button, kopiert es auf den Server und führt es dort aus.

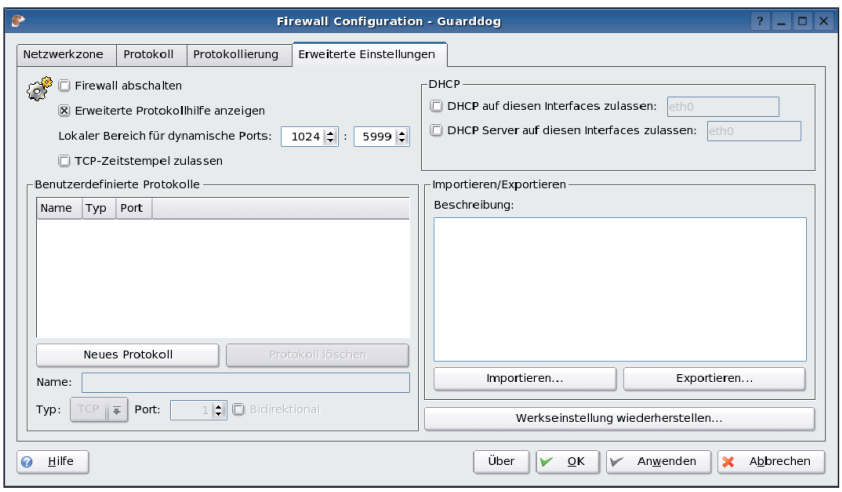


Abbildung 4: Guarddog erlaubt auch die detaillierte Konfiguration der Firewall. So lassen sich zum Beispiel neue IP-Protokolle definieren oder Skripte im- und exportieren.

Tor zur Welt

Der verbreitetste Anwendungsfall einer Linux-Firewall liegt in der Absicherung eines LAN. Der Linux-Rechner dient dabei als Gateway und besitzt zwei Netzwerk-Interfaces: eins ins Internet und ein weiteres ins LAN. Guarddog meistert auch diese Situation. Jedoch ist dazu ein System mit Kernelversion ab 2.4 nötig. Außerdem muss der Administrator vorher IP-Masquerading einrichten, das Guarddog nicht beherrscht. Dazu dienen Tools wie Guidedog von [4].

Der erste Schritt ist, eine neue Zone für das lokale Netz einzurichten. Dazu klickt der Anwender auf »Neue Netzwerkzone« im Reiter »Netzwerkzone« und nennt sie zum Beispiel »LAN«. Mit einem Klick auf »Neue Netzwerkadresse« stellt er die IP-Adressen ein, etwa »192.168.1.0/24«. Indem er unter »Verbindung« auf »Internet« und »Lokal« klickt, sorgt er zudem dafür, dass das LAN mit dem Internet und dem lokalen Rechner verbunden ist.

Unter dem Reiter »Protokoll« ist dann die Zone »Internet« auszuwählen. Danach versieht der Administrator alle nötigen Protokolle in der Spalte »LAN« mit einem Häkchen. Ein Klick auf »Anwenden« speichert die Einstellungen und startet die Firewall. *(mwe)* ■

Infos

[1] Guarddog: [http://www.simonzone.com/software/guarddog/]
[2] Download: [http://www.simonzone.com/software/guarddog/#download]
[3] Online-Manual: [http://www.simonzone.com/software/guarddog/#manual]
[4] Guidedog: [http://www.simonzone.com/software/guidedog/]

Der Autor

Holger Junge betreut bei der Lifemedien GmbH Linux-Server für das Domain-Hosting, administriert Web- und MySQL-Datenbankserver sowie Oracle-Datenbanken.