Brandmauer

Ein PC, zwei Netzwerkkarten und ein ISO-Image: Mehr braucht es nicht, um eine Firewall zu bauen, die es mit der käuflichen Konkurrenz durchaus aufnehmen kann. Linux Professionell testet sechs freie Firewalls.

ACHIM WAGENKNECHT

Warum eine Firewall kaufen, wenn noch ein alter PC übrig ist? Jeder Rechner ab dem 486er lässt sich mit Hilfe zweier Netzwerkkarten und einer quelloffenen Firewall-Distribution in eine sichere und komfortable Brandmauer verwandeln. Linux Professionell hat sechs Distributionen auf Herz und Nieren geprüft.

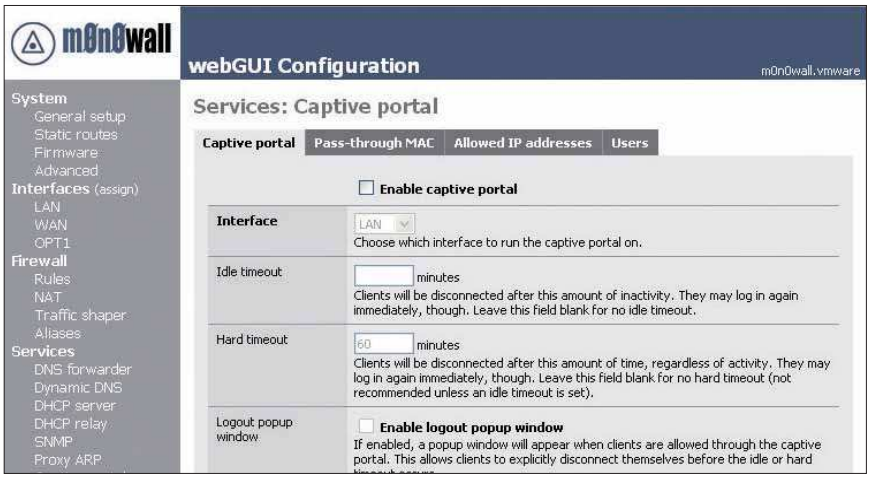
Unterschiedliche Ausstattung

Zwei der bekanntesten Open-Source-Firewalls sind IPCop und Fli4l. Während IPCop von Anfang an als Firewall konzipiert war, sollte Fli4l zunächst nur ISDN-Verbindungen routen. Später kamen dann DSL-Verbindungen und Firewall-Funktionen dazu. IPCop hat sich vom kommerziellen Produkt Smoothwall abgespalten. Smoothwall steht zwar auch unter der freien Lizenz GPL, aber nur in einer abgespeckten Express-Version. Den vollen Funktionsumfang bekommt der Anwender bei Smoothwall nur für Geld.

Das Firewall-Projekt der Firma Endian stammt von IPCop ab. Laut Hersteller ist es zu großen Teilen neu entwickelt worden, die Ähnlichkeiten sind nicht zu übersehen. Die Endian-Firewall bietet zusätzlich Virenschutz mit Clam AV und einen Webcontent-Filter. Eigene Entwicklungen sind Devil Linux von Heiko Zuerker und Coyote Firewall von Vortech. Letztere ist nur für den Privatbereich und in der Ausbildung freigegeben. Der Schweizer Manuel Kasper baut seine Monowall auf FreeBSD auf, das als sicherer gilt als Linux. Monowall ist die einzige Distribution, die nicht nur auf Standard-PCs läuft, sondern auch auf leisen und stromsparenden Embedded-Modellen, unter anderem von Soekris und PC Engines. Zudem bietet Monowall einen echten WLAN-Access-Point, während IPCop diese Technik nur ansatzweise unterstützt.

Bequeme Installation von CD

Die meisten Distributionen sind als bootfähige ISO-Images erhältlich. Das Image wird auf CD gebrannt und der PC damit gestartet. Mit Konsolen-Menüs lässt sich die Firewall dann installieren und konfigurieren. IPCop kann zusätzlich auch per Bootdiskette und Netzwerk installiert werden. Meist ist die Firewall in einer halben Stunde betriebsbereit. Ganz so einfach machen es Fli4l und Monowall ihren Benutzern nicht. Beide Systeme kommen ohne Bootmedium und müssen per Image-Kopie installiert werden. Um Monowall zu installieren, muss die Festplatte oder Speicherkarte der Firewall an einen Gast-PC angeschlossen werden. Dann wird das Image auf das Medium übertragen und das Speichermedium wird in die Firewall eingebaut. Die lässt sich dann starten und per Web konfigurieren. Fli4l ist modular aufgebaut. Es gibt kein fertiges Image, dieses wird bei der Installation neu erzeugt. Dafür muss für jedes Modul eine eigene Konfigurationsdatei bearbeitet werden.



Monowall enthält ein Captive-Portal, mit dem die Firewall zusätzlich als Wireless-Access-Point für drahtlose Verbindungen genutzt werden kann

Das können alle

Der klassische Paketfilter, NAT und Routing gehören zum Standard. Alle Kandidaten beherrschen außerdem DSL und lassen sich per Standleitung mit fester IP oder DHCP ins Netz einbinden. Alle erlauben neben dem inneren und dem äußeren Netz noch ein drittes Segment, das sich als demilitarisierte Zone (DMZ) nutzen lässt. Mit Endian und IPCop lässt sich noch ein viertes Segment definieren. Das ist zwar als Wireless-Segment gedacht, erlaubt aber nur den Anschluss eines externen Access-Points an eine zusätzliche Netzwerkkarte. Die Firewall selbst kann nicht für den drahtlosen Zugang genutzt werden. Aus Fli4l lässt sich ein AP basteln, eine fertige Lösung bietet nur Monowall.

Wer trotz wechselnder IPs unter einer festen DNS-Adresse erreichbar sein will, kann jede Firewall an einen Service für dynamisches DNS anbinden. Alle Systeme schreiben Log-Dateien über Firewall-Zugriffe und weitere Dienste wie IDS. Bis auf Devil Linux und Fli4l können die Logs auch an einen Remote-Logging-Server weitergereicht werden.

Positives Ergebnis: Alle Firewalls werden im Testlabor mit Nessus 3 auf über 10 000 bekannte Schwachstellen überprüft. Da alle Systeme dieser Überprüfung standhalten, haben die Tester das Ergebnis nur am Rande in die Wertung einfließen lassen. Zum Vergleich: In einem ungepatchten Windows XP findet Nessus 14 Sicherheitslücken und lässt den Windows-Rechner abstürzen.

IPCop

IPCop hat sich in den vergangenen fünf Jahren zur beliebtesten Open-Source-Firewall gemausert

Die Firewall lässt sich per Boot-CD und Konsolenmenü installieren. Die Internetverbindung setzt auf Standleitung, Modem, ISD oder DSL auf. IPCop verwaltet bis zu vier Netzwerkkarten: eine interne, eine externe für DSL, eine für eine demilitarisierte Zone und die vierte als Wireless-Zone. Den Wireless-Zugang stellt IPCop aber nur über einen externen Access-Point her. Schon die Installationsmenüs lassen sich auf Deutsch umschalten, und auch die Web-Oberfläche steht auf Deutsch zur Verfügung. Sicherheitslücken werden vom IPCop-Team schnell behoben. Steht ein Patch zur Verfügung, so weist die Firewall automatisch darauf hin. Das größte Manko von IPCop ist der fehlende Regel-Editor. Wer die Firewall-Regeln ändern will, muss den Regelsatz von Hand aus der Distribution extrahieren, ändern und wieder einfügen. Als Schutz gegen Ping-Flood-Angriffe lässt sich die Ping-Funktion nach außen hin abschalten. Verschlüsselte VPN-Verbindungen lassen sich mit Zertifikaten und vorher ausgetauschten Schlüsseln herstellen. Wer Server-Dienste hinter der Firewall betreiben will, hat die Möglichkeit, einzelne Ports auf einen Rechner im LAN weiterzuleiten. Um IPCop zu erweitern, kann der Anwender auf Add-ons zugreifen.

Fazit

IPCop ist schnell, sicher und lässt sich einfach installieren und warten. Optionale Pakete integrieren Zusatzfunktionen.

Endian

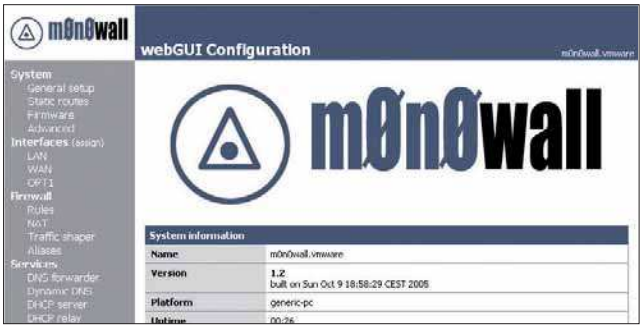
Die Firewall aus Italien ergänzt IPCop um Virenschutz, Spamfilter und professionellen Support

Die Installation der Endian-Firewall ist mit IPCop nahezu identisch. Zusätzlich sind das Open-Source-Antivirenprogramm Clam AV und der freie Spamfilter SpamAssassin vollständig integriert. Zu den ausgereiften Sicherheitsfunktionen zählen beispielsweise Paketfilter, IDS, VPN, Virenschutz, Spamfilter und Webcontent-Filter. Somit ist Endian die erste Open-Source-Firewall, die in der UTM-Liga (Unified Threat Management) mitspielt. Im Gegensatz zu IPCop filtert Endian auch ausgehende Verbindungen, statt nur Verbindungsversuche von außen. Das ist sehr hilfreich, falls einmal ein Trojaner ins Netz gelangt. Die Firewall-Regeln für den ausgehenden Traffic lassen sich mit einem praktischen Regel-Editor komfortabel ändern. Für VPN-Verbindungen stehen OpenVPN und IPsec zur Verfügung. Leider ist die automatische Update-Funktion von IPCop bei der Weiterentwicklung von Endian auf der Strecke geblieben, Patches müssen manuell eingespielt werden. Die sollte das Endian-Entwicklerteam so bald wie möglich wieder integrieren. Und die Funktionsfülle fordert ihren Tribut auch bei der Geschwindigkeit: Keine andere Firewall in diesem Test bremst den Datenverkehr so wie Endian.

Fazit

Die Endian-Firewall bietet die umfangreichsten Sicherheitsfunktionen im Testfeld und bietet so guten Rundum-Schutz.

Monowall



Das Schweizer Projekt Monowall beruht auf FreeBSD und ist mit nur 5,3 MByte der kleinste Download im Test

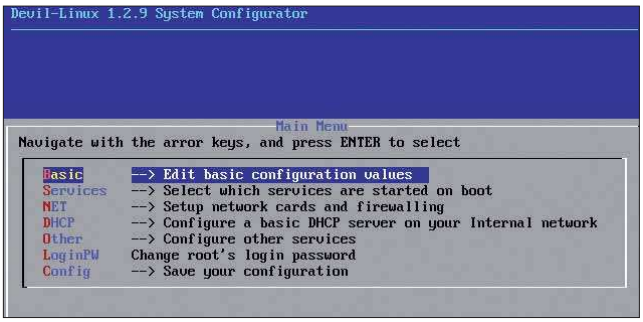
Um Monowall zu installieren, müssen Sie die Festplatte des Ziel-PCs in einen Installationsrechner einbauen, das Monowall-Image darauf kopieren und die Platte dann wieder in den PC einbauen. Der Grund dafür liegt in der Zielplattform von Monowall: Die Firewall ist nämlich für Embedded-PCs konzipiert, die weder CD-ROM-Laufwerk noch Festplatte haben. Auf einem solchen Gerät installieren Sie Monowall, indem Sie das Image auf eine CF-Speicherkarte schreiben und diese in den Embedded-PC einstecken.

Monowall bietet zwar auch ein rudimentäres Konsolen-Menü, lässt sich aber viel komfortabler per Web-Interface bedienen. Das Gerät meldet automatisch, wenn ein Update vorliegt, und lässt sich per Web aktualisieren. Allerdings sind keine Patches vorgesehen, sondern das Betriebssystem wird vollständig ersetzt. Die Firewall-Regeln werden in einem Regel-Editor definiert. Hier lässt sich auch der Schutz vor ICMP-Attacken einrichten. Das Highlight ist aber der Wireless-Access-Point. Um drahtlosen Netzzugang zu ermöglichen, ist ein Captive-Portal in die Firewall integriert. Die Benutzer können lokal auf der Firewall angelegt werden. Alternativ bindet der Administrator einen Radius-Server zur Authentifizierung ein.

Fazit

Monowall lässt sich als einziger Kandidat im Testfeld als Wireless-Access-Point und auf Embedded-PCs nutzen.

Devil Linux



Devil Linux kommt zwar ohne Web-Oberfläche, dafür aber mit gehärtetem Programmcode und haufenweise Zusatzfunktionen

Diese Lösung fällt aus dem Rahmen, weil Devil Linux als modular aufgebauter Rund-um-Server konzipiert ist. Es lässt sich aber gut als Firewall einsetzen, indem der Admin alle nicht benötigten Diente abschaltet. Wer noch sicherer gehen will, kann das System mit der eingebauten Build-Funktion auch als reine Firewall neu kompilieren.

Devil Linux sichert seinen Kernel mit GR-Security gegen Pufferüberlauf. Die Firewall startet von CD und braucht nicht installiert zu werden. Die Konfigurationsdateien speichert das System auf einer Diskette oder einem USB-Stick. Devil Linux wird komplett über Konsolenmenüs konfiguriert, was im Test problemlos gelingt. Einen Regel-Editor bringt die Firewall nicht mit, stattdessen arbeitet sie nahtlos mit dem Firewall-Builder zusammen *(www.fwbuilder.org)*. Trotz der vielen Zusatzfunktionen liegt Devil Linux im Feature-Test nicht vorne. Das liegt daran, dass viele Funktionen auf einer Firewall nichts zu suchen haben. In der Wertung mitgezählt wurden nur der Virenschutz mit Clam AV, der Spamfilter SpamAssassin, das IDS Snort und das Heartbeat-Modul. Letzteres dient dazu, eine hochverfügbare Sicherheitslösung aufzubauen, in der bei Ausfall eines Servers ein anderer einspringt.

Fazit

Wer auf ein Webfrontend verzichten kann und statt dessen viele Zusatzfunktionen braucht, sollte zu Devil-Linux greifen.

Fli4l

Fli4l ist eine modular aufgebaute Firewall, die anfangs gar keine sein wollte. Die Distribution passt auf eine Diskette

Ursprünglich war Fli4l nur als ISDN-Router gedacht. Nach und nach kamen immer mehr Funktionen hinzu, so dass das Programm inzwischen eine vollwertige Firewall darstellt. Als einzige Distribution im Test verlangt Fli4l bei der Installation, dass der Benutzer Textdateien bearbeitet. Fli4l ist modular aufgebaut: Um die einzelnen Pakete zu konfigurieren, müssen die Tester für jedes Paket eine Textdatei im Ordner *config* bearbeiten. Bei einigen Paketen verstecken sich weitere Einstellungen noch an anderer Stelle. In der Vergangenheit existierte ein Windows-Programm, das die Installation mit einem Assistenten erledigte. Das sollten die Entwickler schleunigst wieder auferstehen lassen. Denn das modulare Konzept von Fli4l ist genial. Der Administrator kann damit eine Firewall erzeugen, die auf eine Diskette passt. Fli4l stellt Internetverbindungen per ISDN, Standleitung oder DSL her. Es bezieht auf Wunsch eine feste IP-Adresse von einem dynamischen DNS-Dienst. Sehr einfach lässt sich per Modul eine demilitarisierte Zone aufbauen. Das Proxy-Modul Privoxy stellt Web-Inhalte schneller zur Verfügung und filtert sie. Ganz Mutige bauen aus Fli4l sogar einen Wireless-Access-Point.

Fazit

Fli4l ist eine richtig gute Firewall mit vielen praktischen Zusatzfunktionen. Die komplizierte Installation ist sehr störend.

Coyote

Vortech bringt seine kostenlose Firewall für Diskette und für Festplatte heraus. Linux Professionell testet die Festplatten-Version

Im Test lässt sich die Firewall problemlos installieren und konfigurieren. Die Internetverbindung wird über Standleitung oder DSL hergestellt. Coyote kann auch als unsichtbare Bridging-Firewall konfiguriert sein. Coyote bietet ein Konsolen-Menü, das Fernzugriff per SSH aus der Ferne erlaubt. Bequemer ist es aber, die Firewall mit dem übersichtlichen Web-Interface zu steuern. Hier sichern die Tester die Konfiguration auf der lokalen Festplatte und stellen sie bei Bedarf wieder her. Auch ein komplettes Update kann per Web eingespielt werden.

Coyote Linux reicht seine Firewall-Logs bei Bedarf an einen Remote-Logging-Server weiter. Es versorgt auf Wunsch die internen PCs per DHCP mit Adressen und bezieht eine feste Adresse von einem dynamischen DNS-Service. Die Firewall kann per SNMP von einem Netzwerk-Überwachungs-Server abgefragt werden und, falls benötigt, Ports automatisch für UPnP-Dienste öffnen. Firewall-Regeln lassen sich in einem Regel-Editor per Web setzen. Dabei wird der ausgehende Traffic ebenso gefiltert wie der eingehende. Ein Schutz gegen Ping-Flood-Angriffe lässt sich ebenfalls im Regel-Editor einrichten. Mit Port-Forwarding ermöglicht Coyote zudem Server-Dienste auf Clients.

Fazit

Coyote ist die schnellste Firewall im Test, bietet aber zu wenig Ausstattung, um im Vergleich vollauf zu überzeugen.

Die Ergebnisse im Überblick

Alle Firewalls werden auf der gleichen PC-Plattform installiert, müssen eine Internetverbindung herstellen und einen Nessus-Scan über sich ergehen lassen.

Sicherheit

Punkte gibt es neben den Werten aus dem Nessus-Test auch für Sicherheitsfunktionen wie IDS, Virenschutz und Spamfilter.

Bedienung

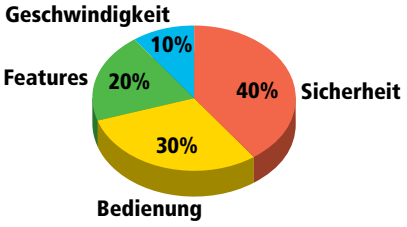
Ein Regel-Editor und eine menügesteuerte Installation bringen Pluspunkte ebenso wie eine Web-Oberfläche – möglichst auf Deutsch – sowie eine gute Update-Funktion.

Features

Firewalling, NAT und Routing beherrschen alle Kandidaten. Pluspunkte gibt es für WLAN-Zugang oder Fail-over-Funktion. Firewall-fremde Dienste werden nicht gewertet.

Geschwindigkeit

Um die Geschwindigkeit der Filter zu testen, werden 300 Dateien im Umfang von insgesamt 3 MByte mit dem Linux-Befehl *time wget -rp* von einem HTTP-Server im lokalen Netzwerk heruntergeladen.



Überblick

	IPCop	Endian Firewall	Monowall	Devil Linux	Fli4l	Coyote
Produkt	IPCop	Endian Firewall	Monowall	Devil Linux	Fli4l	Coyote
Hersteller	IPCop Team	Endian	Manuel Kasper	Heiko Zuerker	Fli4l Team	Vortech
Internet	ipcop.org	www.efw.it	m0n0.ch/wall	devil-linux.org	fli4l.de	www.vortech.net
Version	1.4.10	1.1rc7	1.21	1.2.8	3.0	3.00.37
Gesamtwertung (%)	79	76	71	69	65	64
Sicherheit (%)	75	91	74	87	72	70
Bedienung (%)	93	69	61	52	38	66
Features (%)	67	63	74	57	84	40
Geschwindigkeit (%)	81	64	78	77	84	84
Ausstattung						
Hardware-Plattform	PC	PC	PC, Embedded PC	PC	PC	PC
Wird installiert auf	Festplatte	Festplatte	Festplatte, CF-Karte, CD, Floppy	Festplatte, CD, Diskette, USB	Diskette, Festplatte	Festplatte
Betriebssystem	Linux	Linux	FreeBSD	Linux	Linux	Linux
SSH	ja	ja	nein	ja	ja	ja
Bridging	nein	nein	ja	nein	ja	ja
DNS/Dynamic DNS	ja/ja	nein/ja	ja/ja	ja/ja	nein/ja	nein/ja
Port-Forwarding	ja	ja	nein	nein	ja	ja
VPN	ja	ja	ja	ja	ja	nein
Verbindungen						
Standleitung/Modem	ja/ja	ja/nein	ja/nein	ja/nein	ja/nein	ja/nein
ISDN/DSL	ja/ja	ja/ja	nein/ja	nein/ja	ja/ja	nein/ja
Wireless-Access-Point	nein	nein	ja	nein	ja	nein
Sicherheit						
Logging/Remote Logging	ja/ja	ja/ja	ja/ja	ja/nein	ja/nein	ja/ja
ICMP-Flood-Schutz	ja, Ping deaktivieren	nein	ja	nein	nein	ja
IDS	ja, Snort	ja, Snort	nein	ja, Snort	nein	nein
Virenschutz/Spamfilter	nein/nein	ja, Clam/ja, RBL	nein/nein	ja, Clam/ ja, SpamAssassin	nein/nein	nein/nein
Webcontent-Filter	nein	ja, PICS	nein	nein	ja, Privoxy	nein
Fail-over	nein	nein	nein	ja	nein	nein
Bedienung						
Installation	Boot-CD oder Start-diskette plus Netzwerk	Boot-CD	Image manuell kopieren	Boot-CD	manuell	Boot-CD
Regel-Editor	nein	ja	ja	nein	nein	ja
Web-Oberfläche	ja	ja	ja	nein	ja	ja
Sprachen	Deutsch, 26 weitere	Deutsch, Englisch, Ital.	Englisch	Englisch	Deutsch, Englisch	Englisch
Update-Funktion	ja	nein	ja	nein	ja	ja
Geschwindigkeit						
Wget 3 MByte, 300 Dateien (s)	25,4	29,5	27,7	25,9	25,7	26,4
Wget-Verzögerung (%)	9	27	19	12	11	14
Ping (ms)	0,633	0,740	0,536	0,646	0,550	0,550
Ping-Verzögerung (ms)	0,31	0,41	0,21	0,32	0,22	0,22
Reboot (s)	54	102	56	74	36	29