Die Firewall-Software IPCop

Der Polizist fürs Internet

Zum Schutz des Firmennetzwerks durch Firewalls lassen sich sowohl fertige Hardware-Boxen als auch Software-Tools einsetzen. Heute stellen wir Ihnen die Firewall-Software IPCop vor, die unter Kennern einen guten Ruf genießt. Der Slogan der frei verfügbaren Software lautet: „The bad packets stop here" – hier werden die schlechten Datenpakete abgefangen.

IPCop ist eine Linux-basierte Software-Appliance, d.h. die Software wird auf Ihrer Hardware installiert, ohne dass Sie Einfluss nehmen können. Die Technik der Firewall basiert auf dem bewährten IPtables unter Linux.

Die gesamte Administration erfolgt über eine webbasierte Oberfläche im Browser.

Die Firewall wird über CD installiert

Die klassische Installation erfolgt von einer CD-ROM. Laden Sie dazu das ISO-Image aus dem Internet herunter und brennen Sie es auf eine CD-ROM. Von dieser CD wird dann gebootet.

Es darf kein anderes System laufen

Es ist nicht möglich, das System zusätzlich zu einem anderen Betriebssystem zu installieren.

Achtung, die Installation löscht die Festplatte

Die Festplatte des Rechners wird komplett gelöscht. Installieren Sie daher die Firewall nur auf ausgemusterter Hardware!

Kann der Rechner nicht von einer CD-ROM booten, ist auch ein Floppy-Boot möglich. Außerdem können Sie das System von USB-Sticks (formatiert als Harddisk oder Superfloppy) und einer USB-ZIP-Disk booten.

Notfalls kann auch über den PXE-Netzwerk-Bootmechanismus von einem Server gebootet werden.

Unbedingt neue Passwörter für Root und Admin festlegen

Während der Installation werden einige Grundinformationen wie Sprache, Tastaturlayout, Zeitzone und Details der Netzwerkkonfiguration abgefragt.

Wichtig sind auch die Passwörter für den Benutzer root (für die Kommandozeile des Systems), den Benutzer admin (für die Webadministration) und den Backup-User (zur Datensicherung). Danach startet das System neu und ist bereit zur Konfiguration.

Verbindungen laufen stets über SSL

Die erste Verbindung erfolgt per Webbrowser auf

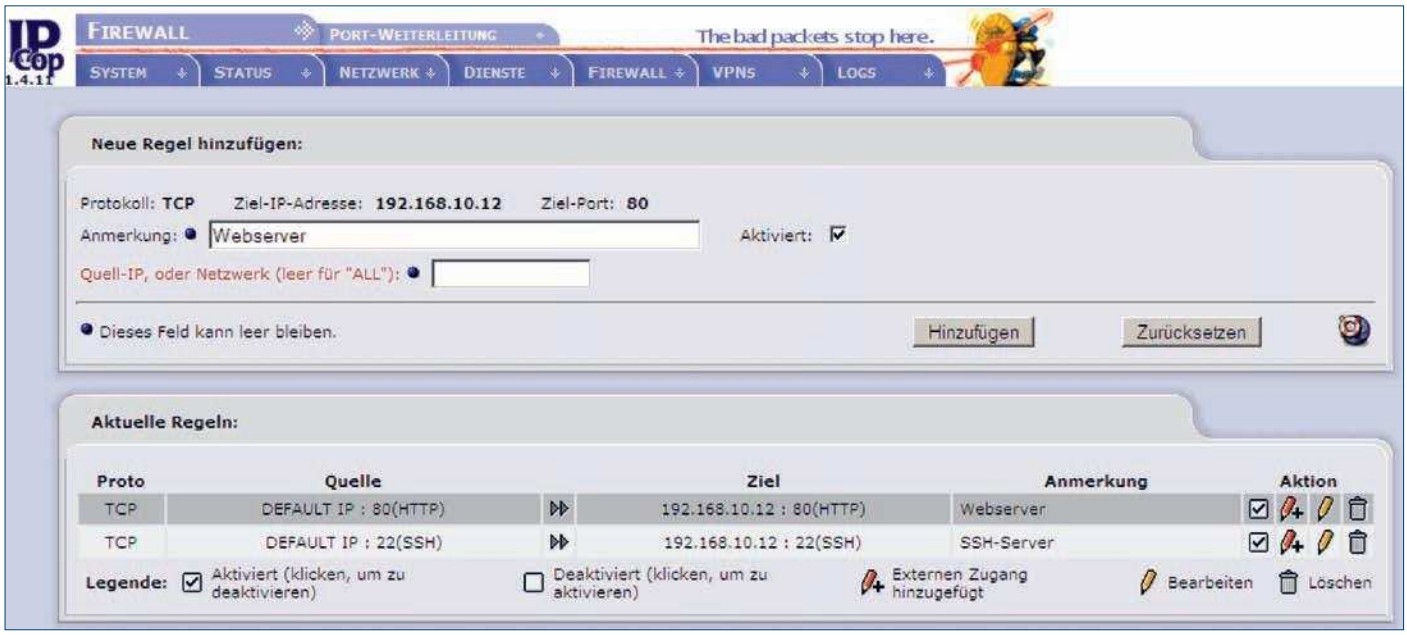
http://rechnername: 81 oder
https://rechnername: 445

Beides sind keine Standard-Ports und müssen deshalb angegeben werden. Die erste Adressvariante ist aber nur eine Umleitung auf die zweite Variante. Damit wird immer eine verschlüsselte SSL-Verbindung genutzt.

Bunte Netzwerkinterfaces – die Bedeutung der Farben

Im Administrationskonzept von IPCop haben die maximal vier Netzwerkinterfaces je eine eigene Farbe:

- **Rot:** das externe, d.h. zum Internet orientierte Interface. Dieses



Die Weboberfläche (hier die Konfiguration der Port-Weiterleitungen) zur Administration des IPCop

Von\Nach	Firewall	Rot	Orange	Blau	Grün
Rot	verboten	–	verboten	verboten	verboten
Orange	verboten	erlaubt	–	verboten	verboten
Blau	verboten	verboten	verboten	–	verboten
Grün	erlaubt	erlaubt	erlaubt	erlaubt	–

Die Voreinstellungen für den Datenfluss zwischen den Interfaces

Interface kann eine echte Netzwerkverbindung, ein DSL-Modem, eine ISDN-Karte oder ein analoges Modem sein. Auf der Webseite von IPCop gibt es eine detaillierte Hardware-Kompatibilitätsliste.

- **Grün:** das interne, sichere Interface. Per Default ist die Administration nur darüber möglich.
- **Blau:** das blaue Interface ist für ein Funk-LAN vorgesehen. Es kann aber auch für andere Zwecke verwendet werden.
- **Orange:** das orange Interface ist für die neutrale Zone oder die DMZ (Demilitarisierte Zone) vorgesehen. Hier werden typischerweise Server (z.B. der Mailserver) aufgestellt.

Der minimale Ausbau der Firewall besteht aus dem roten und dem grünen Interface.

Alles, was nicht erlaubt ist, verbieten!

Die Voreinstellungen für den Datenfluss zwischen den Interfaces zeigt die Tabelle auf dieser Seite.

Für eine seriöse Firewall-Konfiguration sollten Sie auch vom grünen Interface zum roten Interface (ausgehend) alle Ports, die nicht benötigt werden, sperren. Die Grundregel lautet: Alles, was nicht erlaubt ist, ist verboten.

Der smtp-Port (25) darf nur für die Kommunikation mit dem Firmen-Mailserver offen sein, damit Viren und Würmer auf Arbeitsplatzrechnern keine Mails verschicken können. Eine solche Konfiguration ist nicht über die Weboberfläche möglich. Hierzu müssen manuell Iptables-Regeln erstellt oder eine Erweiterung benutzt werden.

Datenvolumen sparen, Einbruchsversuche rasch und sicher erkennen

Der IPCop beinhaltet einen DHCP-Server, der Rechner im Unternehmen mit der Netzwerkkonfiguration versorgt. Ein DNS-Proxy vermittelt die DNS-Anfragen zu einem externen Name-Server.

Der Web-Proxy Squid kann durch eine automatische Zwischenspeicherung von häufig heruntergeladenen Dateien Datenvolumen sparen. Auch die Einbruchserkennung Snort ist an Bord.

Viele Möglichkeiten für Cracks

Wer einen verschlüsselten Zugang (also ein VPN – Virtual Private Network) von außen benötigt, kann sich an die Konfiguration von IPsec machen.

Ein erfahrener Administrator kann auch einen Secure-Shell-(SSH-)Zugang aktivieren und damit spezielle Administrationsaufgaben erledigen, die über das Webinterface nicht möglich sind. Für eine normale Administration ist SSH aber nicht erforderlich.

Zahlreiche Ergänzungen möglich

Eine Standardinstallation von IPCop lässt sich durch eine Vielzahl von Erweiterungen ausbauen. Neben dem Einbinden des Virenscanners ClamAV lassen sich auch verschiedene URL- oder Inhaltsfilter ergänzen.

Mit COPfilter gibt es einen Mail-Proxy zur Spam- und Virenabwehr bei ein- und ausgehenden E-Mails. BOT erlaubt es, den Datenverkehr von grün nach rot detaillierter zu kontrollieren.

Viele Hardware-Lösungen – ganz nach Geschmack

Das IPCop-Forum stellt mit Fotos viele Hardwarelösungen für IP-Cop vor. Mini-PCs (z.B. Mini-ITX) sind je nach Bandbreite des Internetanschlusses hervorragend geeignet. Wer keine bewegten Teile mag, kann IPCop auch auf einer Speicherkarte (z.B. CompactFlash) installieren. Eine Anleitung dazu finden Sie auf der IPCop-Webseite.

Fazit: einfach und verlässlich

Mit IPCop lässt sich mit einfachen Mitteln auf ausgemusterter Hardware eine Firewall-Lösung schaffen. Die Firewall bietet deutlich mehr Funktionalität als ein gängiger DSL-Router. Die Softwarekomponenten sind alle erprobt und verlässlich. Installation und Management sind verhältnismäßig einfach, erfordern aber grundlegende Netzwerkkenntnisse.

Prof. Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der FH München.

Infos zu IPCop im Web

Details zum Umgang mit IPCop finden Sie in der englischen Dokumentation, die teilweise ins Deutsche übersetzt ist. Alle wichtigen Anleitungen gibt es auch als PDF-Dateien. Deutschsprachige Hilfe finden Sie im IPCop-Forum.

http://www.ipcop.org/

http://www.ipcop-forum.de/