April 2005

ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Firewall auf Boot-CD

Im Test: Gibraltar 2.1

Sonderdruck für Esys Informationssysteme

Im Test: Gibraltar 2.1

Firewall auf Boot-CD

Für viele kleine und mittelständische Unternehmen ist die Anschaffung einer professionellen Firewallappliance zu teuer. Doch oft gibt es noch ein paar ältere Rechner im Kämmerlein, die sich ziemlich leicht zu einer Firewall umbauen lassen. Die Firma Esys Informationssysteme aus Österreich bietet mit ihrem Produkt Gibraltar eine passende Lösung hierfür an. Eine Debian-Linux-basierte Boot-CD verwandelt laut Hersteller jeden Rechner in eine voll funktionsfähige Firewall mit vielen zusätzlichen Features. Wir haben uns das Produkt näher angesehen.

Die Linux-Firewall Gibraltar läuft direkt von einer Boot-CD

Als Systemvoraussetzung verlangt Gibraltar lediglich einen Pentium-PC mit mindestens 300 MHz, 32 MByte RAM, CD- und Diskettenlaufwerk und zwei Netzwerkkarten (10/100/1000 MBit/s). In unserem Test kam ein Pentium-II-Rechner mit 366 MHz Taktfrequenz zum Einsatz. Wir bestückten den Rechner mit zwei unterschiedlichen Netzwerkkarten – eine für das Intranet und eine für die Verbindung zum Internet. Außerdem installierten wir in dem Rechner eine Festplatte, um die Proxy-Cache-Funktion von Gibraltar testen zu können.

Installation und Konfiguration

Nachdem wir das von der Website des Herstellers heruntergeladene ISO-Image auf eine CD gebrannt hatten, starteten wir unsere Testmaschine von der CD. Während das System bootet, sucht es nach einer Konfigurationsdatei auf Diskette oder einem USB-Stick. Ist diese nicht vorhanden, startet das Programm mit Standardeinstellungen. Nach dem Start meldet sich der Anwender entweder als Benutzer "root" ohne Passwort lokal an der Konsole an oder er öffnet die "Gibadmin" genannte webbasierte Administrationsoberfläche auf einem Rechner in seinem LAN. Die erste Netzwerkkarte in unserem Testrechner erhielt die IP-Adresse 10.0.0.1, die zweite Karte die 10.0.1.1. Leider gibt es keine einfache Möglichkeit herauszufinden, welcher Karte welche IP-Adresse zugewiesen wurde. Um auf die Firewall zugreifen zu können, muss der Administrator also ein wenig herumprobieren. Im nächsten Schritt definierten wir eine Festplatte für die Dateien für den Proxycache. Das Programm formatierte im Anschluss die Festplatte und verlangte einen Neustart.

Unter dem Menüpunkt "Network" konnten wir dann unsere Netzwerkkarten einstellen. Unsere externe Netzwerkkarte sollte ihre IP-Adresse vom Internet Provider erhalten. Gibraltar unterstützt wahlweise ein Modem, ADSL PPP, ADSL via ATM oder ADSL PPP via Ethernet, um sich bei einem Provider einzuwählen. Wir wählten für unseren Test eine direkte IP-Verbindung zu einem Kabelmodem. Die interne Karte erhielt eine IP-Adresse aus dem 192.168.0.0-Netz um zu testen, wie sich das System beim Wechsel eines Subnets verhält. Das Programm warnt den Anwender, dass er dabei ist, die Verbindung zum Webinterface zu verlieren, falls er mit den Änderungen fortfährt. Nach einem Klick zur Bestätigung mussten wir die IP-Adresse unseres Administrationsrechners anpassen und uns am Gibadmin-Interface neu anmelden. Der Wechsel funktionierte reibungslos.

Firewallregeln

Gibraltar kommt mit ein paar sehr vernünftigen Standardfirewallregeln daher: Alle Zugriffe vom externen Interface sind gesperrt, werden protokolliert und sind gleichzeitig mit Floodprotection ausgestattet. Die Ausnahmen sind Port 22 für einen externen Zugang zum SSH-Server und Port 443 für das Webinterface. Falls der Administrator den Port für den Fernzugriff auf das Webinterface in den Systemeinstellungen ändert, passt dies das System auch automatisch in den Firewallregeln an. Dies zeigt die besondere Benutzerfreundlichkeit der Software. Für zusätzliche Firewallregeln bietet die Software einen grafischen Editor, mit dem es ziemlich einfach ist, auch komplizierte Regeln anzulegen. Zur weiteren Vereinfachung ist es außerdem möglich, eine Liste von Portaliasen anzulegen. Hier konnten wir für unseren Test einer Gruppe von Ports – also beispielsweise allen Ports, die ein bestimmtes Programm verwendet – einen bestimmten Namen zuweisen. Die gleichen Funktionen wie für die Verwaltung von Ports stehen auch für Rechnernamen (Hosts) bereit. So verwaltet Gibraltar eine Liste von Hostaliasen und Hostgruppen. Die Konfiguration von NAT (Network Address Translation) erfolgt ebenfalls über einen grafischen Editor.

Weitere Funktionen

Als weiteres Feature haben die Programmierer dem System einen Dynamic-DNS-Client spendiert. Diese Funktion ist für kleinere Firmen oder Privatanwender nütz-

lich, deren externe IP-Adresse sich in regelmäßigen Abständen ändert. Der DynDNS-Client funktionierte im Test ohne Probleme und erlaubte den externen Zugriff auf Gibadmin über einen Hostnamen.

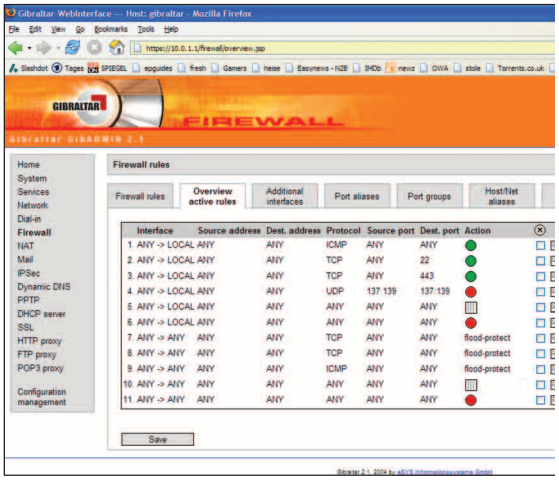
Als weiteren Punkt in unserem Test sahen wir uns die Administration des integrierten Squid-Proxys an. Der Proxyserver läuft auf einem frei wählbaren Port als transparenter Proxy. Die Anwender im LAN müssen also keinerlei spezielle Einstellungen an ihren Webbrowsern vornehmen, was dem Administrator viel Kopfweh ersparen kann. Der Proxy speichert seine Daten wahlweise im RAM der Firewallmaschine oder auf einer vorher definierten Festplatte. Wir konnten unsere fertig konfigurierte Festplatte auswählen und die Größe des verwendeten Speicherplatzes einstellen.

In den Optionen lässt sich auswählen, ob der Proxyserver eine Passwortabfrage und Contentfiltering mit dem beigefügten Clam-Antiviruspaket aktiviert. Dieses Modul untersucht den gesamten Webverkehr, der die Firewall passiert, nach Viren. Infizierte Webseiten filtert das System automatisch. Ein Test mit dem EICAR-Testvirus bestätigte die grundsätzliche Funktion des Scanners. Als Alternative zu Clam bietet der Hersteller auch eine Lizenz für die Aktivierung des kostenpflichtigen Kaspersky-Virenscanners an. Allerdings konnten wir weder im Handbuch noch auf der Website eine detaillierte Beschreibung der Vorteile des Kaspersky-Scanners im Vergleich zu Clam-Antivirus finden. Sehr erfreulich ist die Tatsache, dass das Programm bei einer Änderung des Ports für den Proxyserver auch automatisch die Redirectregel in den NAT-Optionen der Firewall anpasst.

Wie bereits erwähnt, speichert Gibraltar alle Einstellungen wahlweise auf Diskette oder einem USB-Stick und lädt diese automatisch bei einem Neustart. Zusätzlich kann der Administrator sich die Konfiguration per E-Mail zusenden oder auf der Proxyfestplatte ablegen. Als sehr nützlich empfanden wir die Option zur automatischen Speicherung, während das System heruntergefahren wird. Dies ist für einen vergesslichen Administrator ein guter Rettungsring. Nach einem Neustart war unsere Firewall-Proxy-DHCP-Maschine voll einsatzfähig.

Wir testeten die grundlegende Konfiguration der Firewall zunächst mit einem Nmap-Scan. Dabei fanden sich in den Logdateien von Gibraltar ein paar Fehlermeldungen, die beim automatischen Verschicken der Statusmeldungen auftraten. Da der SMTP-Server unseres Providers aus Sicherheitsgründen keine E-Mails von Gibraltar akzeptierte, mussten wir uns an der Konsole der Firewall als "root" anmelden und den Relay-Host-Eintrag der Konfigurationsdatei des Portfix-SMTP-Servers anpassen. Vielleicht könnte der Hersteller dies in einer neuen Version in das Webinterface integrieren. Nach einem Neustart des Postfix-Servers erhielten wir wie gewünscht jede Stunde eine E-Mail mit allen Syslog-Einträgen und Warnungen des mitgelieferten "Port Scan Attack Detectors".

Neben den getesteten Bestandteilen der Gibraltar-Firewall enthält diese zusätzliche Netzwerkdienste wie IPSec- und SSL-Tunnel, FTP- und POP3-Proxies. Der Postfix-SMTP-Server ist als komplette Installation mit Benutzerverwaltung vorhanden und ist mit Spamschutz und dem Clam-Virenscanner konfigurierbar. Gibadmin enthält zudem eine komplette Onlinehilfe in deutscher und englischer Sprache. Erfreulicherweise sind in diesem Handbuch alle Funktionen der Firewall anhand sechs verschiedener Szenarien erläutert. Jedes der Beispiele enthält eine Schritt-für-Schritt-Anleitung der zu konfigurierenden Optionen. Im Anschluss daran findet der Leser Erläuterungen zu jeder Konfigurationsoption der Firewall, die in manchen Fällen etwas ausführlicher sein könnte. Zusätzlich zum Handbuch bietet der Hersteller Support per E-Mail, eine Mailingliste und ein Forum auf seiner Homepage an.



Die Standardregeln von Gibraltar sind gut vorkonfiguriert

Fazit

Gibraltar ist eine durchdachte Firewalllösung, die wir weiterempfehlen können. Die enthaltenen Dienste erweitern das System zu einem kompletten Internetgateway, das mit vielen Internetappliances mithalten kann. Die Boot-CD-Lösung und das durchdachte Konfigurationshandling erlauben bei einem Serverausfall eine schnelle Migration auf andere Hardware. Einzige Nachteile sind der schleppende Support per E-Mail und ein an manchen Stellen knappes Handbuch. Die Mailingliste und das Forum im Internet bieten jedoch viele Tipps und Hilfe bei eventuellen Problemen.

Fabian Warkalla/gh

Produkt
Linux-basierte Firewall auf einer Boot-CD

Vorteile
- Viele Funktionen
- Leichte Installation und Konfiguration
- Günstiger Preis

Nachteile
- Support des Herstellers ausbaufähig
- Handbuch teils etwas knapp

Hersteller
Esys Informationssysteme
www.gibraltar.at

Preise
10 User, 1 VPN-Tunnel: 350 Euro
100 User, 50 VPN-Tunnel: 1.790 Euro

Gibraltar