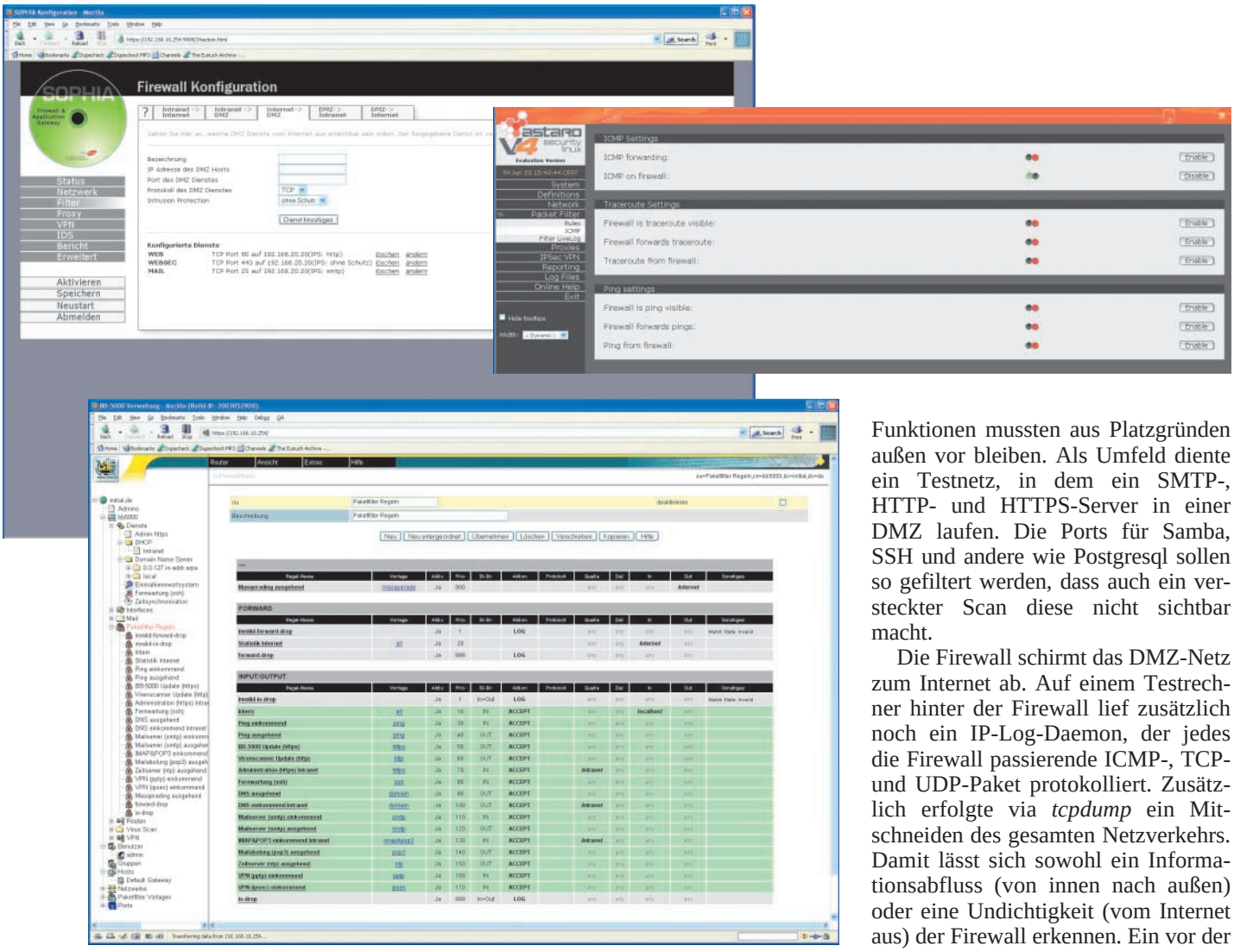


Schlüsselfertige Sicherheitslösungen für Linux

Wunschtraum

Lukas Grunwald

Bequemlichkeit und/oder mangelndes eigenes Know-how lassen Anwender auch bei sicherheitsrelevanten Geräten wie Firewalls mit VPN-Gateway zu „Turn-Key"-Lösungen greifen. Das Drehen des Schlüssels liefert aber nicht immer das erwartete Ergebnis.

Wer sich nicht die Mühe machen möchte eine Firewall selbst zu installieren, die Trägerplattform in Form des Betriebssystems zu härten, um sich dann eventuell mit IP-Tables sein Regelwerk zusammenzustricken, der kann zur Turn-Key-Lösung greifen. Wobei es nicht einfach so ist: Schlüssel umdrehen und schon ist das Company-LAN oder die DMZ sicher.

iX holte mit der BB5000 von Ecos, Sophias Appliance One sowie der Astaro Firewall by Pyramid XL einige Linux-basierte Komplettlösungen ins Labor – Erstere war zum Testzeitpunkt noch nicht ganz fertig. Dieser Test beschränkt sich im Wesentlichen auf die Sicherheitsaspekte, weiter gehende Funktionen mussten aus Platzgründen außen vor bleiben. Als Umfeld diente ein Testnetz, in dem ein SMTP-, HTTP- und HTTPS-Server in einer DMZ laufen. Die Ports für Samba, SSH und andere wie Postgresql sollen so gefiltert werden, dass auch ein versteckter Scan diese nicht sichtbar macht.

Die Firewall schirmt das DMZ-Netz zum Internet ab. Auf einem Testrechner hinter der Firewall lief zusätzlich noch ein IP-Log-Daemon, der jedes die Firewall passierende ICMP-, TCP- und UDP-Paket protokolliert. Zusätzlich erfolgte via *tcpdump* ein Mitschneiden des gesamten Netzverkehrs. Damit lässt sich sowohl ein Informationsabfluss (von innen nach außen) oder eine Undichtigkeit (vom Internet aus) der Firewall erkennen. Ein vor der Firewall installiertes Audit-System probierte in Form eines Penetration-Testes, die Firewall zu überwinden.

Zwei Schwerpunkte der Begutachtung waren die Stabilität der Implementierung sowie die Sicherheit gegen DoS- und dDoS-Angriffe. Darüber hinaus überprüfte der Tester, ob sich Attacken wie Smurf oder ARP von einem Angreifer dazu nutzen lassen, den sonst für ihn dunklen DMZ-Raum hinter einer Firewall auszuleuchten.

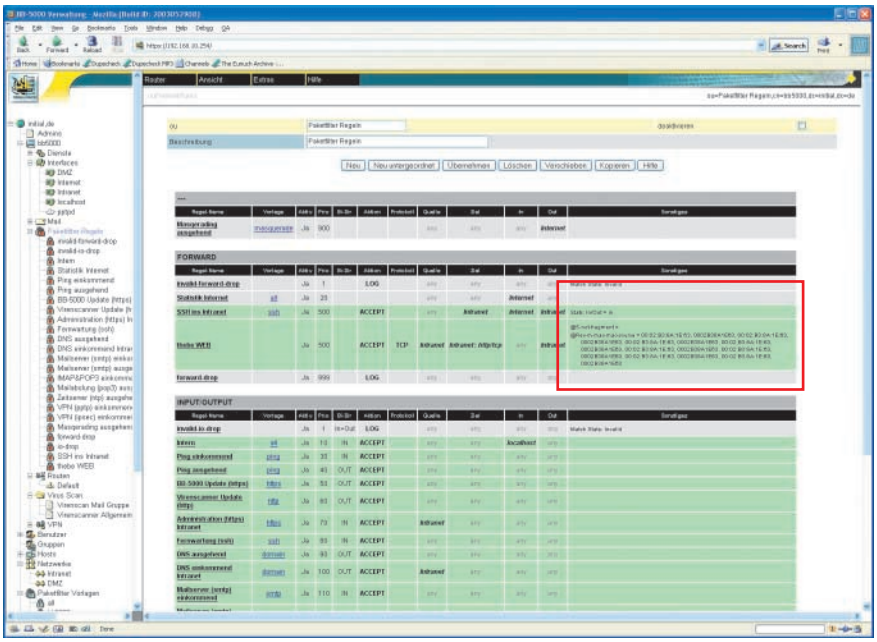
Zum Test der Statefull Inspection dienten via *nmap* generierte spezielle Fin-, XMAS- und RST-Scans, die die Firewall blocken sollte. Via *hping2* erfolgten verschiedene Attacken auf die offenen Ports, unter anderem ein Syn-Flood-Angriff. Des Weiteren fand eine Überprüfung statt, ob sich via Proxy-Arp und ARP-Ping das Intranet und die DMZ hinter der Firewall ausleuchten lassen, um eventuell Rückschlüsse auf laufende Systeme zu erhalten.

Neben der reinen handwerklichen Implementierung und der Konfiguration des Linux-Kernels sowie seiner Härtung und der Anpassung des User-

Timekeeping und Protokollieren

Damit man nach einem Angriff über die Registry im Internet den zugehörigen Provider herausfinden und den Angreifer verfolgen kann, muss genau feststehen, wann der Angriff erfolgt ist. Dazu ist ein Timekeeping von besonderer Bedeutung. Die Firewall sollte möglichst in Universalzeit (UTC) laufen. So kann ein einfacherer Abgleich erfolgen, beispielsweise mit den Einwahlprotokollen der Accessrouter des Netzes, aus dem der Angriff kam. Anderenfalls muss man bei einer CERT-Meldung (Computer Emergency Response Team) unbedingt auch die Zeitzone der Firewall melden.

Unter dem Protokollieren oder Systemlogging ist zu verstehen, dass das System sicherheitsrelevante Informationen sammelt. Nun kann es aber passieren, dass ein Angreifer es schafft, in das Firewall-System einzubrechen. Daher ist sicherzustellen, dass sich diese Ereignisse an ein anderes besonders geschütztes System weiterleiten lassen. Dabei muss man verhindern, dass ein Angreifer von der Firewall aus diese Ereignisse verfälschen oder unterbrechen kann.



Bei der Kombination aus IP- und Ethernet-basierten Regeln reagiert das System zum Teil mit eigenartigen Effekten (Abb. 1).

Landes kommt es auf die Nachvollziehbarkeit von Angriffen an, dazu sind zwei Punkte von besonderer Bedeutung: Timekeeping und Protokollieren (siehe gleichnamiger Kasten). Beide Mechanismen sollten manipulationssicher ausgelegt sein.

Ein letzter Blick galt den implementierten Alarmierungsmethoden, die beispielsweise bei einem Portscan oder einem DoS-Angriff den Administrator benachrichtigen sollen

Ecos BB-5000

Ecos hatte die Desktop-Version seiner BB-5000 Appliance Box geschickt, wird die fertige Version aber auch in 19-Zoll-Technik mit 2 oder 4 HE anbieten. Nach dem Starten passierte nichts, auch die serielle Schnittstelle blieb tot. Erst als wie bei einem Desktop-PC Monitor und Keyboard angeschlossen waren, meldete sich ein GRUB, der das Linux-System bootete. Nach dem Anmelden mit dem Benutzer „Setup“ steht eine Konfigurationsoberfläche zur Verfügung, unter der sich die IP-Adresse des Intranet-Interface einstellen lässt. Danach kann man sich in die Box via SSL-Webbrowser einloggen.

Für die Änderung des Admin-Passwortes vertraut die Software der BB-5000 nur auf eine Eingabe, somit wirkt sich hier ein Tippfehler fatal aus, eine doppelte Eingabe des Admin-Passwortes gehört normalerweise zum Standard und ist laut Hersteller in der aktuellen Version bereits implementiert.

Bei der grafischen Konfiguration stellte der HTTP-Server nach der Eingabe des zweiten externen Internet-Interface seinen Dienst ein. Das unter der Oberfläche laufende Skript hatte dem Netzdevice für das Intranet wieder die Default-IP-Adresse zugewiesen.

Ein funktionaler Mangel des GUI: man kann zwar die IP-Adresse für das Internet-Interface eintragen, aber die Postfix-Konfiguration übernimmt diesen Wert nicht. Ecos verspricht hier baldige Abhilfe.

Sämtliche Konfigurationsdaten befinden sich in einem LDAP-Directory. Beim Einstellen der Default-Route gerät die Suche nach den geeigneten Plätzen im LDAP-Baum mangels Dokumentation und grafischer Repräsentation zur Sisyphusarbeit. Eine Hilfe hierzu fehlt leider.

Die BB-5000 erlaubt ein Update des kompletten Systems über das Internet. Via Weboberfläche ist einsehbar, welche Aktionen erfolgen; der Update-Server benutzt ebenfalls SSL. Leider sind die Zertifikate nicht gegen Manipulation gesichert da keine Trust-Kette aufgebaut wird. Im Testlabor gelang es, den Update-Strom durch DNS-Spoofing umzuleiten. Laut Ecos soll es aber nicht möglich sein, dem BB-5000 Daten eines falschen Update-Servers unterzuschieben.

Filterregeln lassen sich über das GUI ebenfalls in einem LDAP-Container speichern, was eine Replikation erlaubt. Dafür erschlagen die Konfigurationsmöglichkeiten den Anwender im erweiterten Modus mit allen Optionen

iX-TRACT

- Schlüsselfertige Linux-Sicherheits-Appliances versprechen Schutz ohne tief gehendes Netz-Know-how.
- Turn-Key-Lösungen sind entgegen der Behauptungen des Marketing nicht schlüsselfertig.
- Trotz aller Bemühungen der Anbieter erreichen die via GUI konfigurierten Systeme bei weitem nicht den Sicherheitsstand einer handoptimierten Linux-Lösung.
- In Sachen Hardwaredokumentation haben alle getesteten Systeme deutliche Defizite.

von IP-Tables. Zwar bietet die Firewall als Einzige im Test neben IP-Regeln auch Regeln auf Ethernet-Level an, aber auf das Setzen eines MAC-Filters sollte man verzichten. Dieser kann, wie in Abbildung 1 zu sehen, die Konfiguration der Firewall verwirren.

Trotz dieser Option erkannte die BB-5000 eine Änderung der MAC-Adresse des Routers nicht. Das legt den Verdacht nahe, dass das GUI hier zwar alle Optionen von IP-Tables abbildet, diese aber nicht vollständig integriert respektive implementiert sind.

Teilweise ist das Löschen von Regeln sehr zeitaufwendig. Dafür liegen oft benutzte Regelkombinationen schon als fertige Templates vor.

Etwas Besonderes ist der Support für One-Time-PAD-Passworte. Hier kann man mit einem an einen Tamagotchi erinnernden kleinen Zusatzgerät Einmalpassworte generieren.

Beim Test kam eine Syn-Flood-Attacke ohne Schwierigkeiten und ohne Alarmierung zum Zielsystem durch. Hier wäre eine Default-Einstellung wünschenswert, die zumindest einen sinnvollen Maximalwert für Syn-Pakete setzt – im Idealfall konfigurierbar über das GUI.

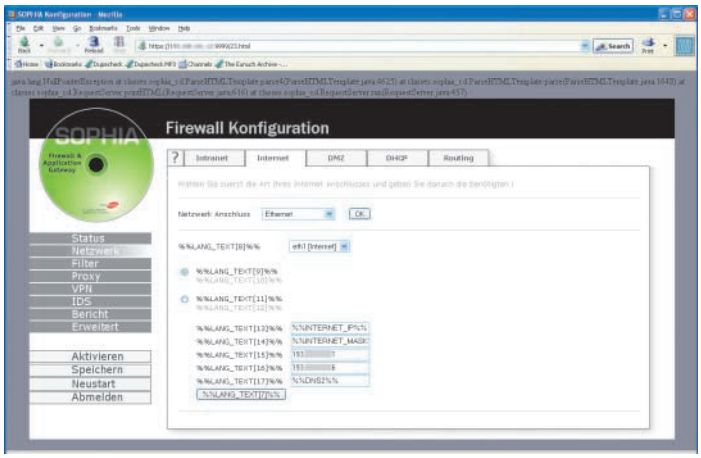
Ebenso reagiert der Stack auf einen ICMP-Broadcast-Ping. Dies sollte bei jedem Linux-System im Normalbetrieb abgeschaltet sein, da sonst eine Smurf-Attacke Erfolg haben könnte. Die TCP-Stack-Parameter lassen sich aber nicht via Weboberfläche einstellen.

Es fehlen für die Alarmierung alle wesentlichen Funktionen. So lässt sich zwar ein proprietärer Remote-Log-Server einrichten aber es existiert keine Möglichkeit, bei bestimmten Ereignissen eine Funktion zu starten – beispielsweise dem Administrator eine E-Mail zu schicken.

Unter dem Punkt „Systeminfos“ listet das Webfenster verschiedene Unix-Kommandoausgaben wie die von *ifconfig*, *who*, *netstat* oder *iptables*. Eine grafische Aufbereitung findet nicht statt.

Bei der näheren Betrachtung fällt die Abstammung des Systems von Suse 7.3 auf: Zwar haben die Entwickler bei Ecos fast alle laufenden Systemdienste in */usr/local* neu übersetzt, dennoch beinhaltet User-Land unnötige Anwendungen, was für ein Sicherheitssystem untragbar ist. Der Hersteller ist sich dessen bewusst und arbeitet mit Hochdruck an einer Verbesserung.

Alle Daten liegen in einem LDAP-Verzeichnisbaum, die Konfiguration und Administrationsoberfläche ist in EmbPerl 2.0b9 geschrieben.



Mit sauberer Programmierung würden sich solche Java-Nullpointer-Exceptions verhindern lassen (Abb. 2).

Als Boot-Loader setzt die BB-5000 GRUB ein, wobei sie dessen MD5-Passwortfunktion nicht nutzt, um ein einfaches *init=/bin/sh* am Boot-Prompt zu verhindern, was ohne weitere Passwortabfrage eine Shell mit Root-Rechten auf die Konsole zaubern würde.

Trotz des durchdachten Konzepts hakt das System noch an einigen Ecken, von der fehlenden Syn-Flood-Protection bis hin zum aufgeblasenen User-Land – zum Teil sicher durch den frühen Status bedingt. Auch sollte Ecos den Kernel lieber ohne Modul-Support betreiben, denn das macht es Angreifern mit einem Root-Kit leichter als nötig, die Kontrolle über das System zu übernehmen.

IPSec realisiert die BB-5000 über FreeSWAN. Dies beinhaltet die üblichen Hakeleien mit FreeSWAN, da dessen Entwickler den im Standard festgelegten DES-Support wegen potenzieller Sicherheitsmängel boykottieren.

Alles in allem bietet die Pre-Release der BB-5000 derzeit noch zu viel Desktop und zu wenig Turn-Key-Lösung, trotz LDAP und Einmalpassworten.

Sophia Appliance One

Im Lieferumfang der Sophia Appliance befindet sich neben der Hardware und drei farbigen Ethernet-Kabeln eine bootfähige CD-ROM mit dem System, auf der auch die Dokumentation der Software liegt. Ein Handbuch für die Bedienung der Hardware liegt nicht bei, dieses muss man sich erst als PDF vom Hersteller besorgen. Startet man die Appliance-Box das erste Mal via Power-On, liefert sie keine weiteren Meldungen. Ohne PDF-Download hängt man an dieser Stelle fest.

Das BIOS hat den Bootvorgang zu schnell beendet, sodass das System vor dem Einlegen der gelieferten CD-ROM angehalten hat. Erst nach einem erneuten Kaltstart bootet das System von der CD und fragt nach den Basisparametern, die sich auch auf einer 3.5“-Diskette speichern lassen. Ein Flash-Baustein oder ein PCMCIA-Flash-Slot wie bei Cisco-Routern würden der Appliance-Box deutlich besser stehen. Die IP-Adresse ist schnell abgelegt, und das System zeigt auf dem Display des Bedienfelds ein generiertes Passwort an.

Mit 150 MByte Dateisystemumfang ist das Sophia-Gerät das genügsamste im Test. Bei der Installation gibt weder das Webinterface noch die Dokumentation den Benutzernamen für die weitere Konfiguration an. Erst nach einigem Probieren stellte sich heraus, dass hier als Kennung *ROOT* zu benutzen ist.

Beim Testen der Konfigurationsschnittstelle kann man leicht eine Java-Null-Pointer-Exception (siehe Abbildung 2) auslösen, so etwas darf bei einer Firewall nicht passieren. Auch macht die Weboberfläche einen sehr schwerfälligen Eindruck.

Unter den Menüpunkten „Bericht“ und „Erweiterte Einstellungen“ lassen sich zwar ein Syslog-Server und ein NTP-Server eintragen, aber eine kryptographische Sicherung fehlt ebenso wie ein Secure-Syslog-Mechanismus. Letzterer könnte die verlustanfälligen UDP-Syslog-Pakete sichern und dem Administrator wenigstens mitteilen, dass Pakete abhanden kommen.

Bei der ersten Softwareversion (2.0g) ließen sich bei Benutzung eines DHCP-

Servers für die Netzparameter die allgemeinen Konfigurationsdaten nicht mehr auf Diskette speichern. Diesen Fehler hat Sophia inzwischen behoben.

Darüber hinaus bereiten Konfigurationen mit nur einem Nameserver-Eintrag Schwierigkeiten, das System läuft nach einem Reboot nicht mehr hoch. Laut deutschem Support sollte man in diesem Fall den Nameserver doppelt eintragen. Zwar lässt sich die Konfiguration via Webbrowser speichern, aber nicht wieder auf die Maschine laden.

Beim Netzwerk-Transceiver hätte Sophia lieber ein paar Euro mehr ausgeben und keine Realtek-Billigchips verbauen sollen. Diese bereiteten im Zusammenspiel mit den Switches im Testlabor erhebliche Schwierigkeiten. Bei kurzen Kabeln (1 m) kam kein Link zu Stande, und bei einem 100-MBit-Half-Duplex-Hub meinte die Sophia-Box immer einen 10-MBit-Link zu haben.

Bei der Installation der Filterregeln fällt auf, dass die Regelsätze sehr begrenzt sind. Zwar lässt sich so ein einfaches Setup reibungslos realisieren, bei einem komplexeren stößt man schnell an die Grenzen des Machbaren.

Die VPN-Lösung legt ihre Konfigurationsdaten zum Teil verschlüsselt auf der Diskette ab. Dies führt allerdings dazu, dass es für einen Umzug der Firewall nicht ausreicht, die Konfigurationsdiskette und die CD mitzunehmen. Die kryptographisch gesicherte VPN-Konfiguration auf der Diskette lässt sich erst nach Eingabe eines Passwortes auf anderer Hardware in Betrieb nehmen.

In der Default-Einstellung waren DoS- und dDoS-Attacken möglich. Erst nach einem Anruf beim Support mit anschließendem Update war das System durch Setzen eines Syn-Rate-Limit gegen DoS-Angriffe gefeit.

Benachrichtigung können via Syslog-NG auf einen Syslog-Server oder als PDF-Report via E-Mail an den Administrator erfolgen. Hier ist die Sophia Firewall beispielsweise weiter als die letztes Jahr getestete Firewall-On-CD von Suse.

Als Beigabe enthält das Gerät von Sophia das Intrusion Detection System (IDS) Inline-Snort. Dieses schluckt nur Pakete mit verdächtigen Pattern, entsorgt sie lokal und alarmiert den Administrator per E-Mail. Dadurch stellt Inline-Snort im Gegensatz zu anderen IDS, die auf eine Attacke hin den Port schließen, sicher, dass ein Angreifer nicht durch Ausnutzen des IDS eine DoS-Attacke realisieren und den Dienst auf der Firewall schließen kann.

Astaro Firewall by Pyramid XL

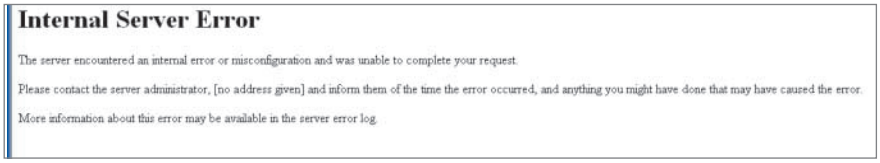
Schon von der Hardwareausstattung her spielt der 2-HE-19“-Server von Pyramid in einer anderen Liga. Wie in Abbildung 4 zu sehen, verfügt das Gerät über fünf dreifach-Ethernet-Karten, was reichlich Optionen für mehrere DMZ und Intranets eröffnet. Dazu kommt ein SCSI-RAID-Controller von ICP-Vortex; die als RAID-1 konfigurierten Harddisks sind hot-swappable und das Netzteil ist redundant ausgelegt. Das Gerät bietet seitens der Hardware eine höhere Verfügbarkeit als die anderen Kandidaten – bei einer Firewall durchaus wünschenswert.

Das gesamte entpackte Dateisystem belegt lediglich knapp 250 MByte auf der Festplatte. Nachdem der Port für das eth0-Interface gefunden war, musste der Tester auch beim Pyramid-System zunächst Monitor und Tastatur anschließen, um in der Shell für das primäre Interface die IP-Adresse einzutragen; die auf der Front des Gehäuses am Display befindlichen Tasten funktionierten leider nicht. Auf dem ersten Bildschirm lassen sich die Systempasswörter vergeben, wobei das System auch den Bootloader LILO absichert.

Beim Booten zeigt sich, dass die von Astaro stammende Software nicht optimal an die Pyramid-Firmware angepasst ist. So versucht der Kernel den PCMCIA-Support zu laden, was bei dieser Hardware sinnlos ist. Wie bei der BB-5000 läuft der Kernel unnötigerweise mit Modul-Support. Letztlich fehlen die Userspace-Programme für den ICP-Vortex-RAID-Kontroller des Geräts.

Hinsichtlich Performance und Bedienung gibts am Webinterface nichts zu rütteln, es lässt sich intuitiv bedienen und bietet einen mächtigen Funktionsumfang. Unter Connection-Tracking lassen sich alle aktiven Verbindungen anzeigen, die Oberfläche ist die schnellste im Test und hinterlässt einen sauberen und aufgeräumten Eindruck. Allerdings tendiert auch die Astaro-Software dazu, mit der Back-Funktion des Browsers manchmal einen Internal Server Error zu produzieren (siehe Abbildung 3).

Nachdem die Rechner und Netze definiert sind, kann man sich ans Regelwerk machen. Ein „simple“-Setup mit der Freischaltung einzelner Dienste gestaltet sich sehr einfach. Darüber hinaus bietet Astaro ebenfalls Socks, HTTP-, IDENT- und SMTP-Proxy. In den HTTP-Proxy hat Astaro einen Content-Checker von Cobion eingebaut, der nach Kategorien, die der Dienstleister bestimmt, gewisse URLs und Webseiten blockiert. Allerdings realisiert Cobion mehr die amerikanische Sicht, so findet sich beispielsweise die National Rifle Organisation (NRA) bei „Non-Governmental Organizations“ und nicht unter dem Begriff „Waffen“. Weiter fiel auf, dass das Gerät nicht alle verfügbaren Sicherheitsfunktionen benutzt. So fehlte in der Default-Konfiguration bei SSH der Host-Key für das SSH2-Protokoll.



Allzu unbedarfes Hantieren mit der Back-Funktion des Browsers kann schon mal unerwünschte Ergebnisse liefern (Abb. 3).

15 Ethernet-Schnittstellen bieten größtmögliche Flexibilität für die Organisation der Netzumgebung (Abb. 4).

DATEN UND PREISE

Ecos BB-5000

Hersteller	Ecos Electronic Communication Services GmbH, Mainz www.bb-5000.info
Hardware	Pentium IV 2,4 GHz, 245 MByte RAM, 40 GByte Festplatte, 3 × Ethernet
Preis	3300 Euro (Testkonfiguration), Einstiegspreis 1490 Euro

Sophia Firewall

Hersteller	GCT Gesellschaft für Computer & Netzwerktechnik mbh, Mühltal www.sophiafirewall.de
Hardware	Via C3 667 MHz, 128 MByte RAM, 20 GByte Festplatte, 3 × Ethernet
Preis	2753 Euro (Testkonfiguration), Einstiegspreis 2283 Euro (5 User)

Astaro Firewall by Pyramid XL

Hersteller	Pyramid Computer Systeme GmbH, Freiburg www.pyramid.de
Hardware	Pentium III 1,3 GHz, 512 MByte RAM, ICP-SCSI-Controller mit 2 × 36 GByte Festplatte, 15 × Ethernet
Preis	7980 Euro (Testkonfiguration), Einstiegspreis 1590 Euro

Auch fand sich im Wurzelverzeichnis des Dateisystems folgende Meldung:

```
iptables v1.2.7a: can't initialize iptables table `nat':
Table does not exist (do you need to insmod?)
Perhaps iptables or your kernel needs to be
upgraded.
```

Nach einer Aktualisierung des Systems über den Astaro Update Service – von der Shell via *aus* abgesichert mit GPG-signierten Archiven – wurden die Tests wiederholt.

Sowohl der fehlende SSH-V2-Key als auch die ominöse NAT-Fehlermeldung waren repariert und das Display funktioniert jetzt wie erwartet. Die initiale IP-Adresse ließ sich nun auch ohne angeschlossenen Monitor und Keyboard eingeben.

Hakeleien könnten durch die Compiler-Version entstehen. Astaro Security Linux (ASL) verwendet die sonst nur von Red Hat in den Distributionen der 7.x-Serie eingesetzte, inoffizielle GCC-Version 2.96. Hier könnten sich Fehler einschleusen, die nicht auf Anhieb entdeckt werden, da die GCC-Entwickler – wie auch Programmierer der meisten Userland-Tools – für diese Version keinen Support leisten. Laut Astaro will man mit der nächsten Release hier auf den GCC 3.x wechseln.

Neben der Firewall-Funktion mit Applikation- und Socket-Level-Proxy bietet die ASL weitere Funktionen wie einen Content-Filter im Squid-Proxy. Darüber hinaus bietet ASL Funktionen wie SMTP-Relay mit Virusschutz, die im Rahmen dieses Artikels außen vor bleiben.

Im Bereich Reporting, Kontrolle und Beobachtung liefert ASL eine vorbildliche Implementierung, Meldungen oder Ereignisse kann man verschicken oder lokal herunterladen. Events lassen sich ebenfalls via E-Mail an den Administrator eskalieren.

Beim Test mit HPING2 auf Syn-Flood fiel das fehlende Rate-Limit negativ auf: die DoS-Attacke gelang direkt in die DMZ und legte den dortigen Test-Webserver lahm. ProxyArp und andere sicherheitsrelevante Funktionen lassen sich hingegen via GUI konfigurieren.

Beim IPSec-Stack fällt auf, dass ASL neben 3DES und AES auch DES unterstützt. Damit verfügt die Pyramid-Maschine als einziger Vertreter in diesem Test über eine standardkonforme IPSec-Implementierung, die auch Verbindung beispielsweise zu bestimmten Cisco-Routern aufbauen kann, die eben nur DES beherrschen.

Geplant für die Version 5 von Astaro sind Inline-Snort und Stack-Protection.

Fazit

Benötigt man eine kompatible und vollständige IPSec-Implementierung, bleibt Pyramids Lösung mit der Astaro Firewall als einziger Kandidat übrig. Geht es dagegen nur um die Absicherung des Firmenwebservers mit ein paar Diensten in der DMZ oder reicht IPSec mit 3DES aus, bietet die Sophia Firewall-Appliance eine gute Alternative, da das Setup einfach und nicht überladen ist. Besonders das Rate Limit der Sophia bei DoS-Angriffen und das Inline Snort verschaffen diesem Produkt gegebenenfalls Interessenten. Lediglich die Hardware müsste Sophia nachbessern und das Webinterface beschleunigen. Alle Firewall-Appliances versprechen ein einfaches Webinterface, wobei jede hier und da noch etwas hakt. Die Lösung von Ecos zeigt zwar gute Ansätze, hier sollte man aber zunächst die endgültige Release abwarten, bevor man sie produktiv einsetzt. „Auspacken, Einschalten, Sicher“ ist niemals möglich, zu einer Absicherung gehören planvolles Vorgehen, klare Konzepte und mächtige Tools. (avr)

LUKAS GRUNWALD

arbeitet als Consultant bei der DN Systems GmbH in Hildesheim und ist in diverse freie Softwareprojekte involviert.

iX-WERTUNG

Ecos BB-5000

- ⊕ alle IP-Tables-Regeln lassen sich abbilden
- ⊕ One-Time-Passwort-Support
- ⊕ LDAP-Integration
- ⊖ unnötig großer Softwareumfang
- ⊖ anfällig für Syn-Flood-, Smurf- und andere Angriffe

Sophia Firewall

- ⊕ InlineSnort
- ⊕ gute Alarmierung
- ⊕ nicht DoS-anfällig durch Rate Limit
- ⊖ Instabilitäten beim Webinterface
- ⊖ qualitativ schlechte Netzadapter

Astaro Firewall by Pyramid XL

- ⊕ sehr gute Hardwareausstattung
- ⊕ viele Application-Level Proxys/ Mehrwertdienste
- ⊕ gute Administrationsoberfläche
- ⊕ volle IPSec Implementierung
- ⊖ anfällig für DoS-Attacke