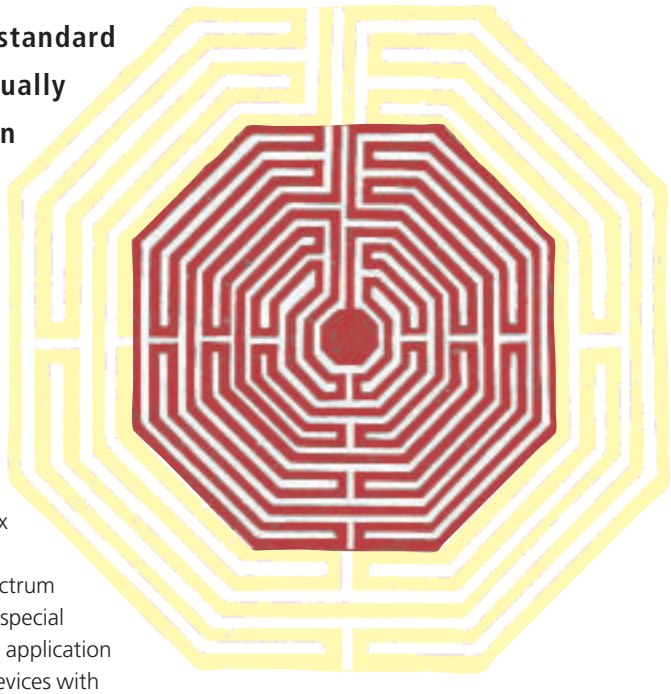
Market Survey of Firewalls

LABYRINTH

JAN SCHUBERT

Firewalls have now developed into a standard utility for network protection. Equally comprehensive is the number of systems on the market. We present a survey...



The market presents a truly bewildering selection of different firewalls. But often, especially with Linux firewalls, the only differences are in the details, such as a different administration interface, behind which a standard kernel does all the actual work. In our market survey, we show a selection of different Linux systems, together with a few well-known commercial firewalls. The spectrum runs from pure software solutions to special appliances and from packet filters via application level gateways up to multifunction devices with their own FTP and Web server.

We have deliberately left out the prices. These depend, not only on various licence models, but also on additional hardware, personal expenditure and suchlike. Although the project costs can easily reach a six-figure amount, the price of the firewall ought to play a fairly unimportant role. What's more important are the respective requirements, serviceability and above all, the available know-how.

All details are based on information supplied by the manufacturer. In the case of software solutions, which require platforms other than Linux on Intel CPUs, this is also stated.

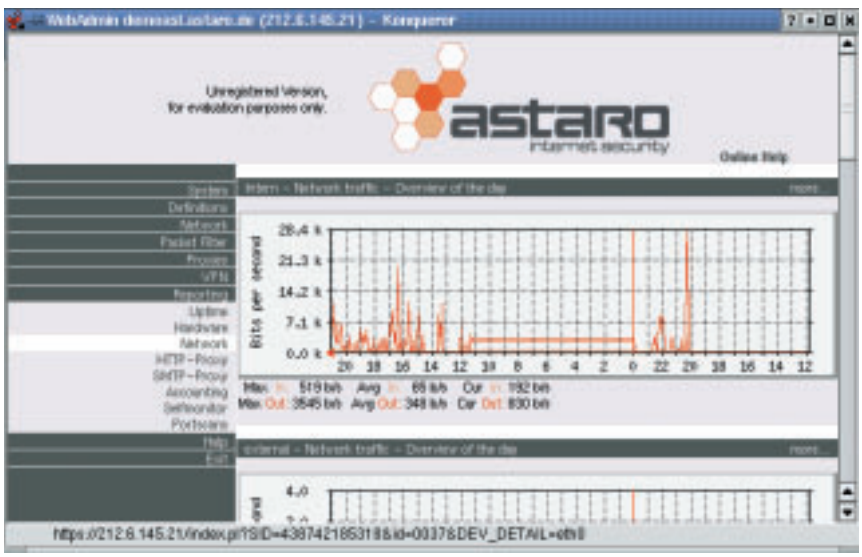


Figure 1: The Astaro interface also provides, apart from configuration of the firewall, exhaustive reporting. The picture shows throughput in the internal network.

Astaro Security Linux: Special Linux distribution with firewall functionality

Astaro Security Linux is a specially protected Linux distribution. On the hardened operating system, there are packet filters with stateful inspection, application level gateways, content filters (banner, virus scan), VPN and a Web-based administration front-end (see Figure 1). The front-end in the test version unfortunately offers only limited options.

The system is offered for download free of charge as an ISO-CD image, but firms must acquire a licence later. Costs are in line with the number of computers to be protected. Astaro complete solutions are offered on Cobalt Raq3i. Also of interest is the paid Up2Date service, with which for example patches and the latest virus patterns can be loaded automatically.

LinkX offers a similar product, with the Securepoint firewall server (*http://www. securepoint.de*).

Licence: Basic GPL, partly proprietary. Free of charge for private users.
http://www.astaro.de/ products

Biodata BIGfire: Stand-alone firewall appliance

Biodata, with BIGfire, offers a firewall as black box. The 19-inch plug-in offers packet filters with stateful inspection, NAT and VPN. Software and hardware are both in-house developments by the manufacturer, who has specialised for many years in security. In combination with BIGapplication it is possible to expand to application level gateways and to integrate products from third party suppliers (such as Cobion Webfilter).

Licence: Commercial
http://www.biodata.com/de/products/bigfire/biodata_bigfire.cphtml

Checkpoint Firewall 1: Proven software solution with a high market share

With the Firewall 1, which has been established for many years, the Israeli manufacturer Checkpoint has achieved very high market penetration. Checkpoint was a leader in the development and implementation of new technologies, especially in the case of stateful inspection and the company's own INSPECT technology. In this process, all the necessary information is extracted between physical layer and network layer (OSI layers 2 and 3) and compared with the security policy. If the data does not contradict this is it passed on to the IP-layer (OSI layer 3) of the operating system. Potential errors in the TCP/IP stack of the operating system therefore have no effect on the firewall rules.

In the latest version 4.1 Checkpoint offers, in addition to the packet filter, a range of integrated application level gateways, support for NAT and VPN. Components from third part suppliers can be integrated through the company's own standard OPSEC (Open Platform for Security). With the exception of a few control commands, a special interface has to be used for configuration (Figure 2).

The connection between GUI and firewall is produced by a management server; this allows several firewalls to be administered centrally and consistently. Like many other commercial products, Firewall 1 is also certified by the ICSA (*http://www.icsalabs.com/html/communities/firewalls/certification/vendors*).

Nokia offers an Intel-based appliance with the IP range with Firewall 1 (*http://www.nokia.com/securitysolutions/network/firewall.html*). The combination of established firewall software and special network and routing functionality should meet the high standards of security and speed.

Licence: Commercial

Platforms: HP-UX, AIX, Linux, Solaris, Windows
http://www.checkpoint.com/products/firewall-1

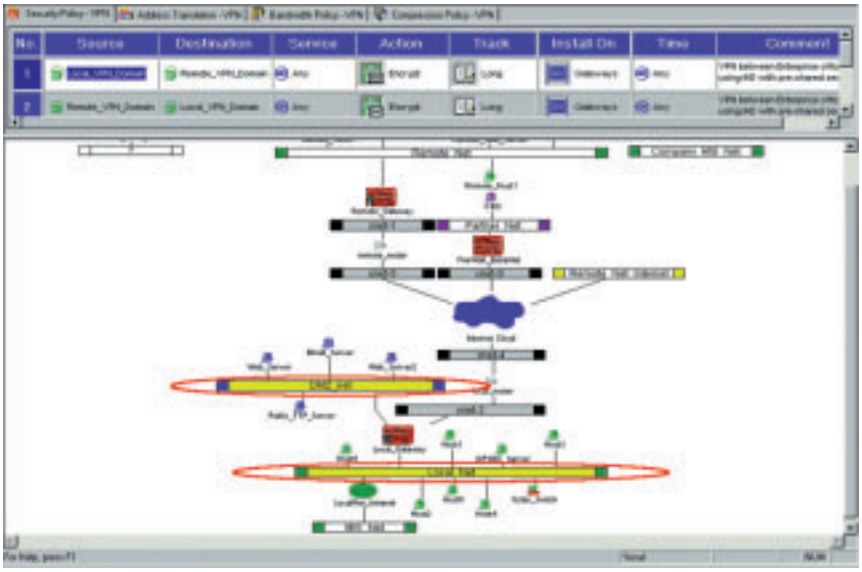


Figure 2: With Checkpoint's Visual Policy Editor, even complex firewall policies can be created simply and easily.

Cisco PIX 500: High-performance complete solution with high market penetration

The PIX firewall series builds on the many years of know-how of Cisco in the domain of network management and routing. The extremely high data throughput stands out as a particular characteristic. There is support for stateful packet filtering, NAT and VPN. In the latest version 5.3 remote access via secure shell is possible. Also, the PIX uses its IDS (Intrusion Detection System) to recognise some well-known methods of attack and blocks them.

And other established manufacturers in the field of communications are also offering complete solutions, such as 3COM with Superstack III and Zyxel with ZyxWALL 10.

Licence: Commercial
http://www.cisco.com/ go/pix

GeNUA GeNUGate: Several firewalls in one

The GeNUGate actually consists of two or more firewalls. This is intended to reduce the high expense involved in the integration and servicing of multi-level firewall scenarios. The solution includes, in the basic expansion stage, a packet filter and an application level gateway (see Figure 3).

At this expansion stage GeNUGate separates four networks which are independent of each other. As the result of the modular structure, in the form of processor boards in an ordinary commercial 19-inch casing, redundant, hot standby and more powerful expansions are possible.

A Web-based administration front-end makes it easy to configure these complex solutions, in which, for example, a separate nameserver is operating in each sub-network.

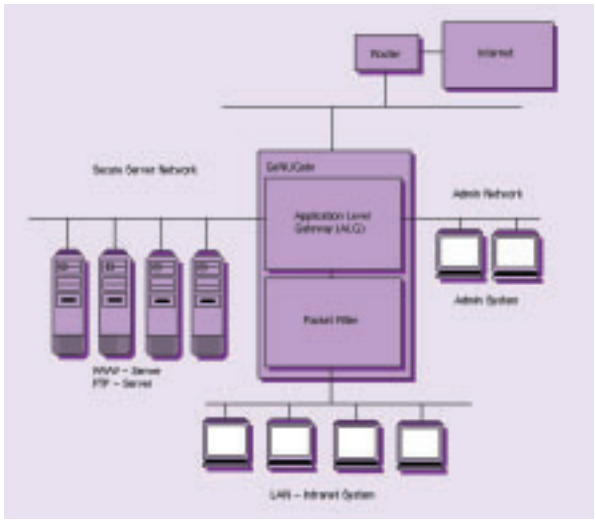


Figure 3: Schematic structure of the GeNUGate basic expansion level. External network, secure-server network and admin network are linked by means of an application level gateway. The internal network is also protected by a packet filter.

The basic software is the commercial BSD version BSD/OS 4.01 (4.2 planned). This operating system is a secure basis, especially as the result of the special access permissions at file level, which go beyond the normal options of UNIX. The open architecture allows for manual configuration and individual software and hardware expansions. The product is currently certified by the German Federal Office for IT Security to the international standard ITSEC E3 High.

Licence: Commercial
http://www.genua.de/produkte/ggfamilie

Linux Netfilter/Iptables: Professional packet filter in the Linux kernel 2.4

As successor to the tried and tested Ipchains (in kernel 2.2), Iptables offers, in addition to simplified configuration, additional options. Instead of the previous three, data packets now need only run through a single control chain when being passed on.

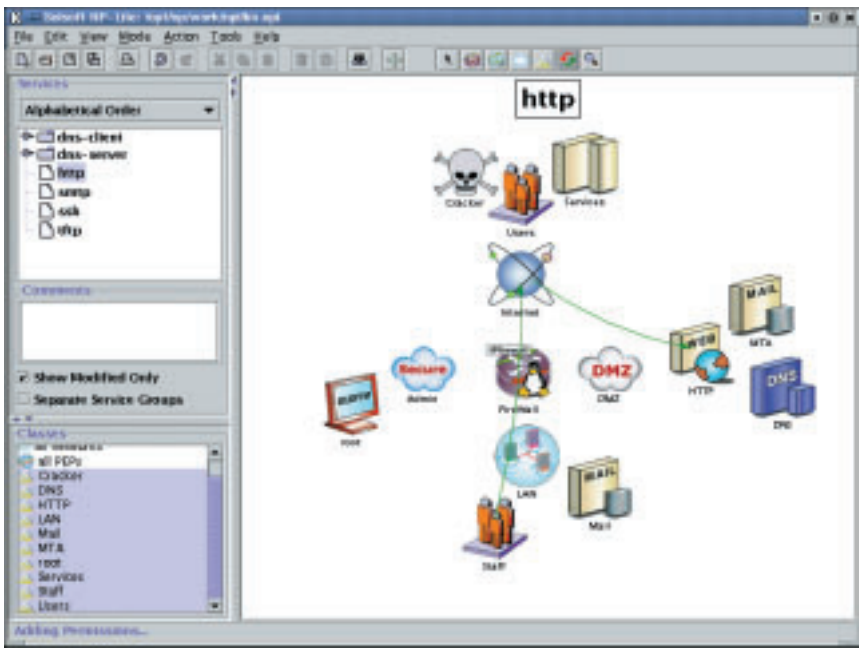


Figure 4: Solsoft NP Lite, programmed in Java, can configure Linux firewalls, with not only the rules, but the entire network topology being clearly displayed with various objects.

Additional features now include support for stateful inspection, filtering of MAC addresses and very comprehensive NAT functions. Application level gateways and VPNs can be realised with additional solutions, for example with the TIS firewall toolkit (see below), or the IPSec implementation FreeS/WAN.

Configuration is done solely on the command line. But by using addon products, GUI-supported configuration is also possible. Examples of GUIs are Solsoft NP Lite (see below) or Firewall Builder. Older rules, which were created for Ipchains (Kernel 2.2) or for Ipfwadm (Kernel 2.0), can continue to be used — Iptables offers its own compatibility layer for this purpose.

Ipfilter from Darren Reed is suitable for various BSD versions and also a few commercial UNIX systems (*http://www.ipfilter.org*).

Licence: GPL
http://netfilter.samba.org

Network Associates Gauntlet: Comprehensive application level gateway

Although packet filters and NAT are supported in the latest Version 6.0, NAI recommends use as a pure application level gateway. If necessary an additional packet filter can be integrated, before or after the Gauntlet firewall. Gauntlet contains proxies for a great many current applications protocols, including database links and print services, and there is even a UDP proxy.

The basis for development was the TIS firewall toolkit. Unlike older versions, unfortunately, it is now no longer possible to peek into the source code.

Licence: commercial
Platforms: Solaris 8, HP-UX 11.0
http://www.pgp.com/products/gauntlet

Smooth Wall: Linux distribution with firewall functionality

Designed as a complete distribution, Smooth Wall is based on a special kernel 2.2.18 with IPSec support. Smooth Wall is designed as a more secure router, with Web-based configuration of packet filters, proxy, DHCP and PPP (via ISDN and DSL). As a special highlight, a Java SSH client is included. This can be downloaded free as an ISO-CD image.

Licence: GPL
http://www.smoothwall.org

Solsoft NP: Management platform for several firewalls

Solsoft NP (Net Partitioner) serves to manage various firewalls. The graphical tool supports, in addition to the various Linux filters, Checkpoint Firewall 1, Cisco

PIX and the configuration of access control lists for diverse routers and switches. NP can transfer the actual configuration to the firewalls. The aim is for a configuration which is as error-free and intuitive as possible.

The free version, NP Lite 4.1 for Linux (see Figure 4) is interesting, and this supports a graphical configuration of Iptables.

Licence: commercial, free version for Linux

Platforms: Linux, AIX, HP-UX, Solaris, Windows

http://www.solsoft.com/products/net_partitioner.html

Symantec Raptor: Comprehensive software solution

After the take-verification by Symantec, there was silence on this product, which was tried and proven in the past. In the latest Version 6.5 there are now some fairly obviously characteristics being represented as special features (NAT, application level gateway and VPN). Stateful inspection is apparently not possible.

Licence: Commercial

Platforms: Tru64, Solaris, HP-UX, Windows NT

http://enterprisesecurity.symantec.com/products/products.cfm?Product-ID=47

Telco Tech LAN Internet Support Station: Linux-based access router with firewall function

In addition to the management of domains, e-mail and Web server, this flexible solution also offers packet filters, VPN and IDS. Based on Linux 2.2, only a standard interface is provided to manage all services. Initial configuration of the 19-inch device (see Figure 5) is performed by floppy disk, after which a Web front-end is available.

Similar products include Linogate Defendo (*http://www.defendo.de*) and the Firebox-II series from Watchguard (*http://www.watchguard.com/products/firebox.asp*), but the latter with kernel 2.0.

Licence: Commercial

http://www.liss.de/

TIS Firewall Toolkit: Building set for application level gateways

Although the last version came out over three years ago, FWTK is still an interesting building set for constructing application level gateways. All proxies are configured in the file *netperm-table*. Users can use the *authsrv* to authenticate themselves at the firewall, before they are allowed to use a proxy.

Figure 5: The LAN Internet Support Station is, as a network appliance, a ready-expanded piece of hardware. The connections for the networks are located, together with a few status indicators, on the front plate.

There is support for a range of standard protocols, and additional ones can be transferred via universal gateways (*plug-gw*). Additionally, there is also a port scanner and other utilities. The accessible source code contributes to the installation of an individual application level gateway which is as secure as possible.

Licence: Free, also available in source code. Not for commercial use.

http://www.tis.com/research/software/index. html ■