

# A firewall sees red...

In recent issues, we examined in detail the issue of computer security at home [in the company of expert Christian Sudec]. You learnt why some of the data on your system is so coveted by criminal elements and were confronted with several real-life attack scenarios. In times of economic crisis in particular, all this only makes for additional losses – losses in business, too. As virtual attacks can wreak a disproportionate amount of extra havoc in a company, it is here where the protection should be at its best. This article explains that things are different in practice. But we also present an appliance that represents a viable alternative in the market.



Smart: the GPA series of firewalls from gateProtect.

In order to better assess the pros and cons of this hardware, we'll have to beat about the bush a little. Because, whereas private users merely have to install a few software tools such as virus scanners, firewalls and web filters, these precautions are simply no longer enough in a company. So the administrator of even a small company with fewer than, say, 10 employees must already think in much larger terms. This is due to various components not normally found in a private user's home configuration. It makes no odds whether we're talking about a web server for the company's Internet site or an additional file server with data synchronisation to a branch office; the fact is that these services, as well as their interplay within the LAN and the network structure itself, all require monitoring. Otherwise, protection of corporate data cannot be guaranteed. Ultimately, not only could genuinely relevant data fall into the wrong hands, the damage caused would indirectly affect the employees too (unfortunately, mainly through salary cuts or penalties) and thus negatively impact more lives than it would in the case of the private user.

In order for me to highlight more clearly the hurdles to be overcome when securing a company's IT systems, allow me to stay with the example of our small company with its 10 employees (the industry sector is immaterial). This type of company is very prevalent in Austria. Long-term experience suggests that the company will operate according to the following principle when it comes to procuring and maintaining its IT infrastructure. The boss is prepared to spend only what is absolutely necessary on maintaining the IT infrastructure. The company workstations always lag behind the state of the art; as a rule, to the tune of 3-6

years because one depreciation interval is normally skipped. And licences are only ever purchased if the software in question would stop working without activation, or regular updates are needed for financial/productive applications. The latter would be the case e.g. with financial accounting applications and machine control systems.

Generally, the IT specialist is only called in when the going gets tough, i.e. when something goes wrong. Like the car dealer's reminder for the annual service, the letter recommending a comprehensive IT review is often just tossed aside or sails straight into the paper bin. And of course IT projects must be implemented as quickly as possible, either because the competition „already has it“ (e.g. website, centrally synchronised calendar, etc.) or because ever more people/customers/authorities are demanding it (e.g. e-mail address, price list download, etc.). So either the cheapest provider will be commissioned for the job or the in-house IT manager will be told to get the whole thing sorted out as cheaply as possible. And this is where we come to a parting of the ways. It all depends on how competent the person responsible for implementing the project is. The boss will be given either an Open Source-based solution for free or a pirate copy of a „user-friendlier“ commercial software package. No matter which path is taken, both will converge again when – happy with the (hopefully) by now successful deal – the boss affirms: „That should see us right for the next few years/decades!“

Anyway, enough of our typical little firm, the likes of which are to be found not only in small Alpine countries. At this point, we could cite any number of additional studies and propose hypotheses, but let's concentrate on the facts of the case as described above. First of all, the workstations comprise different types of hardware – due in part to the different procurement periods and in part to various emergency repair jobs carried out in the past. Thus the individual PCs not only have different drivers, but they are also capable of different levels of performance. This leads to a situation whereby a program that runs quite happily on computer A will not always do the same on computer B. And we're not just talking about corporate software here, but also security suites.

Due to the lack of an on-site administrator, virtually all the company's employees have full administrative rights to their PCs – nothing is more bothersome (and expensive) than calling in the IT manager for every minor change (e.g. modifying the Windows energy scheme so that a monitor displaying a product demo program does not go into sleep mode automatically). As a result, the secretary will quickly install a school program on her PC for the boss's son so that he can print out his drawings on the company printer, while the warehouse manager has numerous games installed on his hard disk, etc.

On the other hand, because they are unlicensed versions, the „official“ company applications aren't eligible for updates. With each passing day, they tear more and more holes in the system, gaps which are then exploited with the aid of manipulated documents. And because everyone has logged on with an administrator account, there are no further obstacles in the way of a „hostile take-over“ – apart, that is, from a local scanner (and that's not updated regularly anyway).

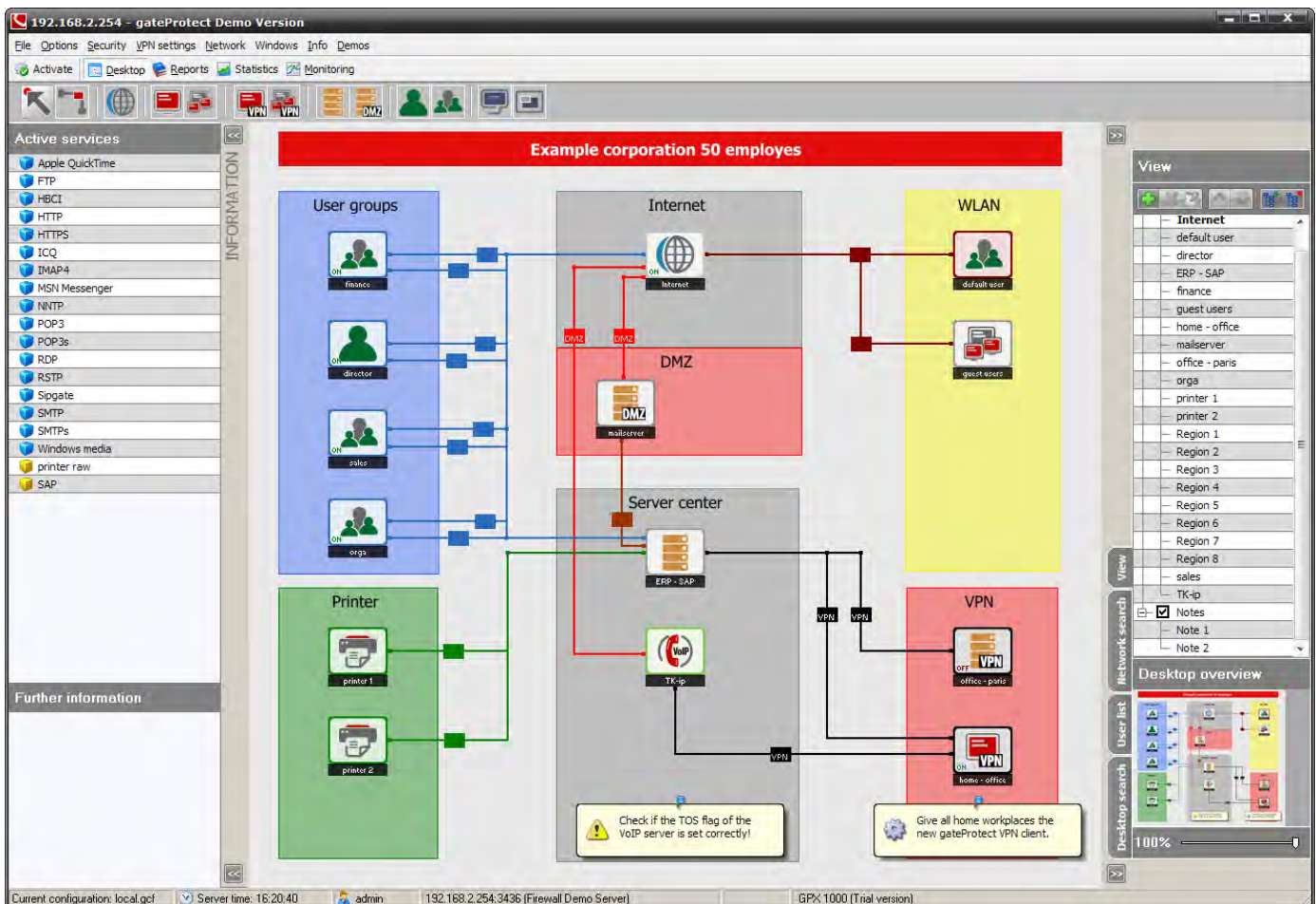
The same applies to the system devices used in the above projects. Because they operate round the clock, they are not allowed to be touched by anyone. That they are running Linux is no guarantee for their security, and thus they are the target of many a hostile attack. And the intruder's advantage? It can remain undetected for weeks!

Due to the diversity of the service providers who are continuously adding or extending components, there is no standard documentation for the network. Normally, DHCP is used so that new devices can obtain an

IP address quickly and easily. But the same applies the moment an employee connects his private laptop to the LAN. Then, at the latest, any measure of control in respect of who is doing what in the network, i.e. which PCs and which addresses should be there and which should not, is lost. An attempt at consolidating this kind of structure (and introducing security measures) is a never-ending task which is unsurprisingly generally avoided like the plague.

It is virtually impossible, therefore, to deploy security suites and other stand-alone products in identical fashion on all the company workstations. Firstly, there is the problem with performance and updates, as mentioned above. Secondly, these tools only ever monitor a local PC and exist only for one type of operating system. This is where „appliances“ attempt to step into the breach. Appliance is the name given to a relatively inconspicuous item of hardware. These are usually rack-mount chassis affairs which sometimes house a logical array of PC components, but sometimes also special chipsets. The same applies to the operating system: either standard software or a special OS is used. Regardless of the combination, it will be explicitly adapted to its future task. Attention is also paid to the aspect of simplicity. This applies both to initial installation and to subsequent operation. The aim is that even staff without extensive IT know-how should have no problem in setting up the appliance and interpreting its output correctly. This allows several birds to be killed with one stone: 1. There's no possibility of user error during installation because the product is supplied out-of-the-box; 2. The system is lean, stable and

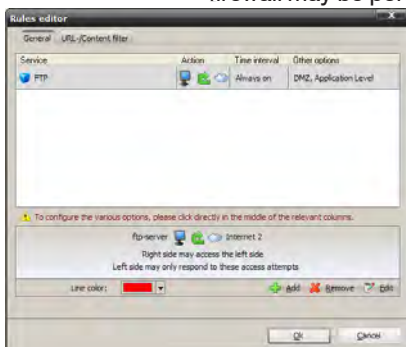
*Administrator interface with mail and web servers, each with their own DMZ.*



secure because it offers only those services that are absolutely essential and does not, therefore, represent an easy target; 3. The user-friendly GUI cuts down on complex error messages, using simple icons instead (e.g. the traffic light system to denote the overall state of the system); 4. The high degree of interoperability means that appliances can be integrated quickly in any environment; 5. The manufacturer guarantees the initial points mentioned above in the form of a service level agreement (SLA) which includes routine maintenance (updates; minimum response time in the case of faults/problems, etc.).

So we finally arrive at gateProtect, a German security product that we will sound out below. As the name suggests, it is a firewall appliance, i.e. a beefed-up router which is capable of connecting several networks together while scrutinising the data traffic carefully at the same time. By way of comparison, while a desktop firewall may be perfectly sufficient for a home PC user,

DMZ connection properties can be defined precisely.

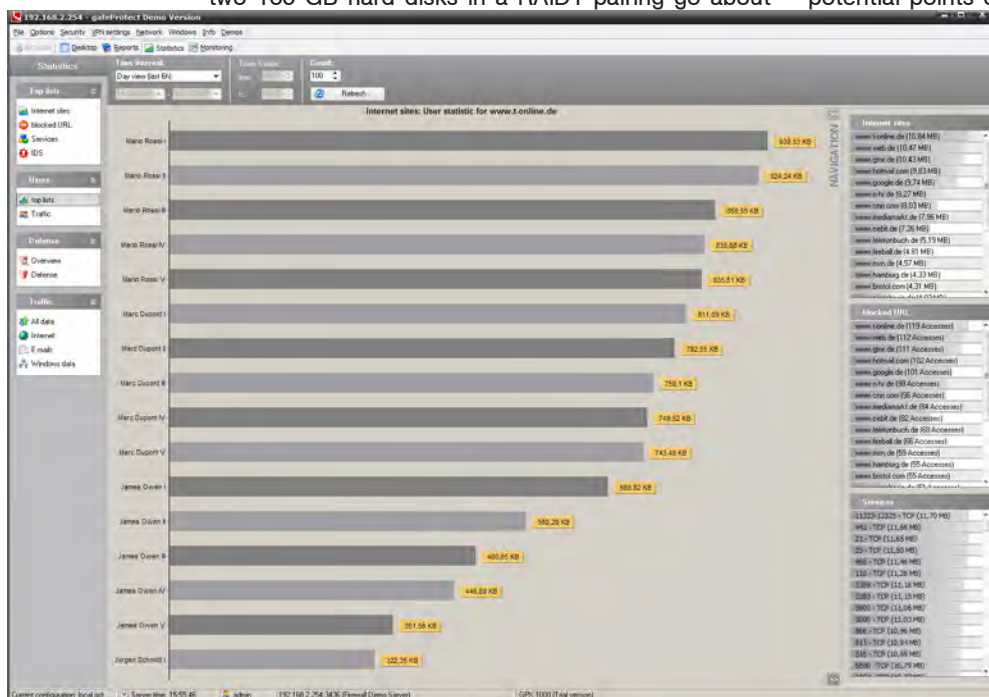


a company has additional devices to secure. So, although the above-mentioned web server needs to feed data into the Internet, it should not be part of the LAN. This is because if the server were ever compromised, the intruder would immediately have access to all the workstations which would be part and parcel of the same network. It therefore makes sense to house proprietary Internet servers

in „demilitarised zones“ (DMZs), as they restrict data connections into both the Internet and the LAN.

For this very reason, our test device is equipped with five LAN connectors located in different private sub-networks. But one thing at a time. The gateProtect appliance comes in a 19“ rack-mount chassis in classic Ferrari red. Within the chassis, standard components such as a Pentium Dual Core E2180 processor on an Intel DG965WH motherboard with 1 GB of RAM, and two 160 GB hard disks in a RAID1 pairing go about

Administrator screen with user statistics



their work.

On the rear of the unit are all the usual connectors for keyboard, mouse, screen, etc. To set up the appliance, just connect these three hardware items and switch the appliance on. The Linux operating system now boots. Actually it is a Debian derivative based on the soon-to-appear Version 4.1., so it's quite up to date. By the way, as this is open source code, the appliance's software component can be downloaded free of charge.

If everything has gone according to plan, the IP addresses of the five Ethernet connectors will be displayed and the firewall will announce that it is ready for operation in the last line displayed. From now on, all further installation steps are carried out by the gateProtect Administration Client (for Windows) which is really the heart and soul of the appliance and needs to be licensed. By double-clicking on the Administration Client, you can choose between two types of configuration, depending on your level of know-how. With the „Quick start“ option, you will be asked to specify the approved services and the type of Internet access. You can now choose between ISDN dial-in (if the appliance has a modem), ADSL (PPP or PPTP), or direct connection with a router. Whatever you select, you should have the corresponding access data to hand, as you will be asked to provide this in the dialogue boxes which follow. However, this procedure offers only minimal protection (a fact pointed out by the manufacturer) and only works if the IP addresses of the local LAN correlate with those of the appliance. If you intend to integrate the appliance into existing networks, you will have to use the „Default“ option. After specifying a password (make sure you remember it!) and your time zone, the administration desktop appears from which you can make all further configuration inputs manually.

By keeping the firewall lean and transferring graphical configuration in its entirety to the client, the manufacturer has taken a different path. This helps minimise potential points of attack and the appliance's appetite for resources, while enabling all the Windows options (mouse support, high resolution, drag-and-drop, etc.) to be exploited, thus making remote maintenance as pleasant as possible. Put simply, the administrator can design the entire network structure himself on a graphical user interface (similar to Visio)! The menu bar provides ready-made icons for servers, user groups, VPNs and several other entities. You simply choose the one you want and drag it onto the desktop. There is, for example, an icon for the Internet (= web access). A brief glance under Properties reveals the connection data. In order to place our trusty web server in a DMZ, we simply drag the corresponding icon (DMZ ser-

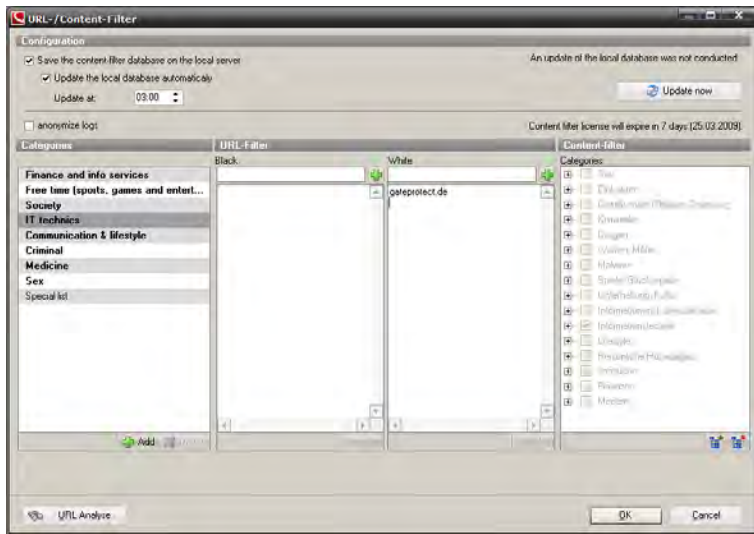
ver) alongside it and enter the IP address of the server in the dialogue box which appears. All you need to do now is specify the LAN connector to which it is linked,

colleagues. As well as content blocking, time locks can be set in similar fashion (this time, however, for the workstations), enabling e.g. private surfing after office hours (see also Proxies below).

The entire system can be configured in the same manner as described above: drag the required icon onto the desktop, fill in the dialogue box, and connect the entity to any other objects using connecting lines. You can now review your work and then press F9 to have the rules translated into machine-readable format and transferred to the appliance, whereupon it becomes active immediately.

Let us now take a look at the remaining features that can be configured conveniently via the client. Besides the usual directional filters, virtually all the gateProtect types offer a full IDS (Intrusion Detection System) to scan data traffic for certain attack patterns. In addition, application-level filters and proxies which monitor outgoing data for compliance with company policies are available for the most important Internet services (HTTP(S), FTP, SMTP, POP3 & VoIP). To this end, you can access appropriate databases containing classified URLs, or create your own URL lists. The proxies can, of course, be operated transparently as well (i.e. without the user noticing).

The next feature is of interest to larger installations in particular. Firewall users can be authenticated against existing databases (Active Directory, openLDAP, etc.) to save you having to configure additional user accounts and even, perhaps, to pave the way towards a single-sign-on regime at a later date. Single sign-on is



URL filter settings are made here.

grant the Internet object access to it (i.e. only previously defined web services), and you're done! A line immediately appears denoting a connection between the Internet and the web server. By double clicking on this line, you get a graphical display of the points between which data traffic is permitted. All other packages remain blocked and out of the way, as befits a good firewall. In another tab, you can set filters so that only work-related content passes via the web server and employees are prevented from storing games for

## Die neue 500 Mbit Firewall FortiGate 110C

500 Mbit Firewall / 100 Mbit IPSec VPN / max. 400.000 Sessions  
1.500 VPN Tunnel / 4.000 Policies  
10 konfigurierbare Ports\*  
\* 2x 10/100/1000 Mbit, 8x 10/100 Mbit



Der neue Fortinet ASIC sorgt für höchste Performance

**ab EUR 2.245,- / 3.235,-\*\***

\*\*inkl. 12m AV-, IPS-, WEB-Filter und SPAM-Filter- Updates - exkl. MwSt.!



<http://corex.at/Produktinfos/FGT110C.pdf>

- ✓ Traffic-Shaping
- ✓ Anti-SPAM
- ✓ Web-Filter
- ✓ Anti-Virus / Anti-Spyware
- ✓ IDS / IPS
- ✓ Firewall
- ✓ IPSec / SSL VPN

**COREX**  
EDV-Dienstleistungen GmbH

<http://www.fortinet.com>  
<http://www.corex.at>  
<mailto:fortinet@corex.at>

**FORTINET**

where the user logs on only once and the appliance takes care of all further authentication routines. So if certain users are generally permitted to use the web server, they will be logged on automatically whenever they want to transfer new content to the website. Gone are the days of having to remember countless different passwords!

Mail and spam filters are naturally included in the package, as is a facility for providing teleworkers with access to the company LAN via VPN. A Kaspersky licence can be purchased separately to check inter-host data traffic for viruses so as to prevent infections at data transfer level. Everything else is just the same: configure using drag-and-drop or by adjusting the extended properties of an existing connection.

Network professionals will be delighted at the functions supporting high availability and traffic shaping with QoS (Quality of Service). The latter allows pre-defined bandwidths to be assigned to certain services and users for data traffic. For example, this can help prevent dropouts from occurring during Internet telephony when Bill from R&D has decided to download a mega-update for his statistics tool again.

And while we're on the subject of statistics, let's take a look at the menu item of the same name in our client. Here, the company boss will find a complete list of all the websites surfed, sorted by time of day. The administrator, on the other hand, can see at a glance which viruses have been on the march, and is also provided with a percentage breakdown of bandwidth usage by service. „Reports“ lists other important events arising from current operations, while the „Monitoring“ section provides detailed information on technical appliance aspects (disk and processor utilisation, NIC traffic, etc.).

## SUMMARY

When I was asked to review this hardware, I admit that my initial thought was: „OK, yet another firewall appliance trying to hide its open-source architecture behind an attractive GUI.“ Normally, X-Windows or a web interface is used – with results that don't exactly bowl me over. I've even found graphical front-ends like fwbuilder irritating to the extent that I have stuck with shell scripting in the past. So I was more than a little sceptical when I came to assess the usability of the gateProtect high-end firewall. I couldn't have been more wrong. The idea of outsourcing the whole configuration process to Windows and using all its design registers is just what I've always been looking for. User A needs a VPN connection? A few clicks and it's done! I take my hat off to the manufacturers because they've succeeded in combining two universes in an ideal way, providing administrators with a powerful tool with which to monitor a LAN structure effectively. Provided, of course, that he or she has prior knowledge of TCP/IP and of user and rights management. By contrast, the average PC user who has the job of IT administrator foisted upon him by his boss will be somewhat perplexed by the whole thing, despite the German user interface. So all that remains to be said is that red is the only suitable colour for gateProtect because it really is the Ferrari of the firewall appliances!



gateProtect High End  
Firewall GPA-250

**Manufacturer:**

gateProtect AG Germany

<http://www.gateprotect.com>

Ein Blick ins „Rat & Tat-Forum“ auf [www.wcm.at](http://www.wcm.at) lohnt immer!

Angeführte Preise inkl. MwSt. ab Lager Perchtoldsdorf. Stand eine Woche vor Erscheinen des Inseerts, gültig solange der Vorrat reicht.  
© 2008 E.Weinzettl

## Speed Up Your Net!



*Ihr Netzwerk liegt darnieder? Die Verkabelung leidet an Altersschwäche, der Server ist schon lange überfordert? Wir können helfen. Wir liefern nicht nur Workstations für Office, CAD und Bildbearbeitung sowie leistungsfähige Server, sondern auch stabile und hochperformante Netzwerkkomponenten. Wenn Sie Performance im Netz benötigen, können Sie auch komplette, strukturierte Verkabelung sowie kompetenten Netzwerksupport von uns ordern. Derzeit sind unsere Netzwerktechniker im Einsatz. Morgen vielleicht auch bei Ihnen. Kontaktieren Sie uns unter 01 244 0058 und verlangen Sie Herrn Weinzettl.*

A-2380 Perchtoldsdorf, Wienergasse 32, Tel. 01/244 0058, Fax 01/244 0070  
email [office@i-design.at](mailto:office@i-design.at), <http://i-design.at>, Öffnungszeiten: Montag-Freitag 10-18:30 Uhr

**i-design**