UTM a simple configuration

The patented eGUI interface from gateProtect makes it easy to set up a UTM appliance

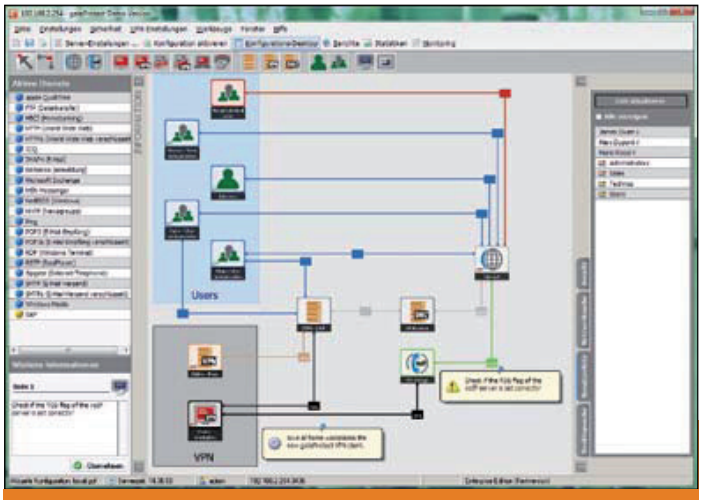
The simple firewall is increasingly being replaced by Unified Threat Management (UTM) This is intended to avert not only direct attacks by hackers, but also all sorts of possible unwanted network activity. A whole series of manufacturers offer for this purpose turnkey configured UTM appliances which are usually based on a Linux distribution specifically designed for the purpose.

Complex functionality, simple operation

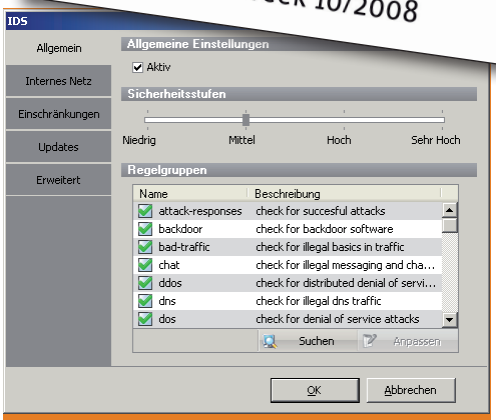
Even traditional firewalls offer an abundance of configuration options that only specialists can cope with. An employee responsible for IT in an SME is therefore soon up against his or her limits and, afraid of making mistakes, prefers to do without some of the available options. As a result the firewall configuration is not ideal, the network does not fulfil its potential and some of the security problems that a firewall is actually supposed to eliminate remain in evidence. If the firewall has additional UTM functions, the issue becomes even more complex. The German supplier gateProtect has come to this realisation. „A firewall system can only offer as much security as the user can operate it with.“ gateProtect has therefore developed a GUI desktop for its UTM firewall appliances that allows process-oriented configuration and administration in a clearly depicted environment. This is a Windows application – it is not intended for operation through a web browser.

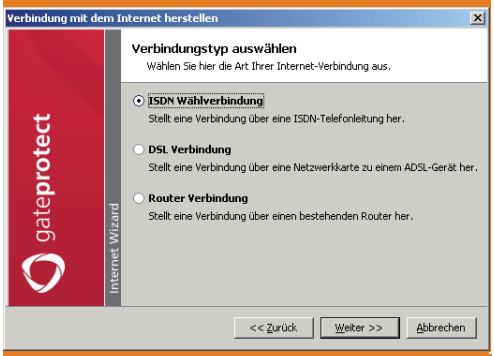
Configuration by Drag&Drop

The graphical representation of all the objects in the network is at the centre of the interface: clients, servers, internal users and user groups and those connected by VPN, objects in the DMZ and so on are shown as icons with their connections. New objects are created with drag and drop. The appropriate symbol is dragged from the toolbar to the desktop and a dialog window appears automatically to allow the object's properties to be entered. Existing objects can be grouped together, also with drag and drop. Connections are equally easy to create, by choosing a connection tool and then clicking the objects to be connected one after the other. Clicking on a node in the connection line displays a rule editor, an uncomplicated tool with which to define the access rules for different network services. Obviously, the GUI client is not a substitute for a lack of network knowledge – with gateProtect, the administrator needs to have a good understanding of the way a firewall works and how the various UTM functions are used. However, correct configuration of the security system is not made more difficult by clumsy operation on a confusing interface, with important settings hidden in several nested dialogs or in the form of cryptically labelled operating elements – all of which happen with many other suppliers.



Clear representation of the whole network structure makes it much easier to configure a firewall.





gateProtect uses the SNORT open source project (above) as an intrusion detection system. The installation wizard adjusts to the type of Internet connection (below).

Keeping an overview

In order to ensure that even complex networks are clearly understandable, the gateProtect desktop offers various convenient features. For example, when an object is selected, its connections and all the objects it is connected to are highlighted and all the others are hidden. The left-hand section of the

Infoweek.ch • Infoweek.ch • Infoweek.ch • Infoweek.ch • Infoweek.ch • Infoweek.ch • Infoweek.ch

InfoWeek.ch
DAS IT-MAGAZIN FÜR DIE SCHWEIZ

TESTED:

GATEPROTECT xUTM FIREWALL APPLIANCE 8.0

VERY GOOD

InfoWeek 10/2008

window shows a list of all the network services. If an object is selected on the desktop, the active services are highlighted. A click on a service in the list, on the other hand, highlights all the objects for which the service is activated.

The right-hand window section optionally presents a list of all the defined users and groups or various search functions for any objects and individual computers.
It also contains the „View" option: the gateProtect desktop allows the network objects to be arranged on several levels which can be displayed or hidden as required. Below this is a small picture of the whole desktop and a zoom control to make the displayed section larger or smaller.

Gateprotect xUTM Firewall Appliance 8.0

Conclusion
Configuring and operating a UTM system with the patented operating interface from gateProtect is not a completely trivial issue. However the supplier's intention to install more professional Unified Threat Management, in SMEs in particular, is certainly easier to achieve with the graphical administration client, given its drag and drop facility and easy to understand dialogues, than with the cryptic interfaces that many a UTM supplier expects their customers to deal with.
Like many comparable products, the firewall itself is based on an adapted Linux distribution, supplemented by various other open-source components such as SNORT and L-7 and commercial technology such as Kaspersky's virus protection and the Commtouch spam filter. With a total of six models for 10 – 2500 users and a throughput of 90 Mbits to 4.5 Gbits per second, the gateProtect appliances have the whole SME sector covered. The entry-level price of a little under 500 euros makes UTM attractive even for very small environments with a few users.

Features
- Firewall with VPN, QoS and application level filtering
- Intrusion detection
- Spam filter, virus scanner
- Graphical configuration interface

Pluses
+ Easy to operate
+ Clarity even in large environments
+ New bridge mode simplifies installation

Minuses
- Configuration client only for Windows
- Configuration client

Producer/supplier
gateProtect, www.gateprotect.de

Price
from €495
(Model GPO 75 for max. 10 users)

Score

Functionality	★★★★★☆
Operation	★★★★★☆
Price/performance	★★★☆☆☆
Overall	★★★★★☆

Comprehensive functions

In functional terms, the gateProtect software complies with the current standard for Linux-based UTM firewall systems. According to the producer, the system is based on an adapted Debian distribution. In addition to the basic firewall functions – blocking ports and handling VPN connections – the gateProtect xUTM firewall server offers the following main features:

➢ Web access control with URL and content filtering based on Cobion technology.

➢ Quality of Service and Traffic Shaping.

➢ Application level filtering independent of the ports used (protocols HTTP, FTP, POP3, SMTP and DNS) using the Open Source solution L7 filter.

➢ Intrusion Detection, based on the Open Source system SNORT.

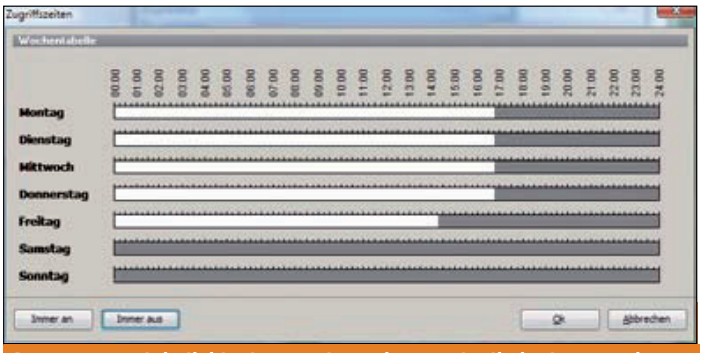
➢ A spam filter based on Commtouch anti-spam technology. The appliance comes with a 30-day test licence; companies wishing to use the spam filter permanently must buy an additional licence.

➢ A virus scanner with Kaspersky technology – again, a separate licence is needed after a 30 day test phase.

New features in Version 8

At CeBIT this year, gateProtect presented its firewall software in a new version. A special new feature in Version 8.0 is bridge mode. This makes it easier to integrate the appliance in an existing network, without having to adapt the existing IP addresses and access privileges. The gateProtect firewall now also supports sub-division of the physical network into any number of VLANs. As well as the already available IPSec mode, the gateProtect firewall now also supports universally usable SSL-protected VPN connections.

The gateProtect software can in theory be installed on its own server, but typically it is used on a fully configured appliance. The manufacturer offers the devices, which are supplied in fire engine red housing, in three product lines for environments of different sizes: The Office series serves small companies with 5 – 25 users. The smallest model, GPO 75, offers firewall throughput of 90 Mbit/sec, handles up to 2500 e-mails per day and costs just under 500 euros. Devices in the A-series and the X-series are suitable for environments with 100 – 2500 users. gateProtect gives the prices for the larger models on application.



Access to each individual network service can be limited to certain periods.The installation wizard adjusts to the type of Internet connection (below).

infoweek.ch • infoweek.ch • infoweek.ch • infoweek.ch • infoweek.ch • infoweek.ch • infoweek.ch