

Straightforward configuration, strong performance

Dr. Götz Gütlich

The xUTM appliance V8 from gateProtect is a product for safeguarding medium-sized corporate networks. This producer has focused particularly on offering a solution that is easy to configure and manage, making it easy for administrators to work with the product. IAIT took a practical look at whether the appliance meets this requirement.

The gateProtect appliance is available in various virtual variants and hardware versions from solutions with a 500 MHz CPU up to devices with Dual Xeon processors. According to the producers, the range is aimed mainly at medium-sized companies with up to 500 users. Our test scenario (the GPA 400 appliance) works with a dual processor system and also has a total of six network interfaces, which can be used for LAN or WAN connections, to set up a DMZ (demilitarized zone) or also to realise a separate WLAN segment. As a rule, administrators put the solution into operation by placing it at its final working location in the network



(in the test, we used the solution as an Internet router, that is between the WAN connection and our LAN switch), installing the configuration client on a Windows workstation and then setting up the appliance with its assistance so that it takes on the functions it is intended for.

When the configuration software contacts the solution for the first time, it automatically starts a wizard with the intention of carrying out the initial configuration. It offers two options: quick start and standard.

As the producer recommends configuration with the quick start wizard, we decided on this one for our test. The first step: the wizard asks about the services that are to be approved and offers various options. These include the HTTP, HTTPS and DNS web services, FTP for file transfers and the mail services POP3, SMTP and IMAP4.

The administrators also have the option of using the wizard to enable the services NetBIOS, Kerberos, LD-AP, DNS and RDP. This choice is followed by configuration of the Internet access. Here, the UTM solution offers ISDN, PPPoE, PPTPoE and router connections.

In the test, we used the product on a DSL connection (in PPPoE mode) as an Internet router, so we had to enter the network connection to be used

IAITested

★★★★★

Excellent ! Test 11 / 2008

Conclusion:
The UTM appliance from gateProtect was impressive across the board and scored well with all its functions.

Benefits

- + Excellent clarity
- + Very straightforward operation
- + VPN wizard and client
- + Quality hardware
- + Price/performance

Disadvantage

- No web interface as yet

**gateProtect GPA 400
xUTM solution**

Client-Installation

The client runs under the current Windows versions and requires a CPU, minimum 1 GHz, and 512 Mbyte RAM; it can be operated in virtual machines without any problems. As is usual with Windows, set up is carried out using a wizard, which offers users German, English, French and Italian and which is quite straightforward for anyone to use. After the setup routine has run, the software can be called up and automatically searches for the firewall in the network. If it can't find it, the next step gives the administrators the opportunity to enter the IP address of the appliance (which the producer delivers with the appliance on a print-out) and create the connection in this way.

and our access data. After a few more questions about the network connection and system settings (time out, administration password, time zone and so on), initial configuration is complete and the appliance starts operation as a security solution. If the IT staff choose the standard configuration instead of the quick start option, they have to carry out all the administration functions from the start with the configuration tool.

Administration

The configuration that the quick start wizard leaves behind is fairly general and permits all the systems in the LAN (or on the non-WAN interfaces) outgoing use of the services enabled in the first configuration step by the IT staff. For the next step, it makes sense to adapt this configuration to the requirements of the company in question with the administration tool.

but presents its rules in a graphical form.

In concrete terms, this means that the individual computers, users, groups of computers and groups of users are displayed in the form of icons on the desktop of the configuration tool. The IT employee can draw lines between these icons and, for example, the graphic representing the Internet connection to assign the authority to use certain services. This creates rules such as „User A may surf the Internet and transfer files by FTP“ or „Access via SSL can only be undertaken from computer B“. Clicking on the line in question then opens a window in which the administrators can modify the access privileges at any time.

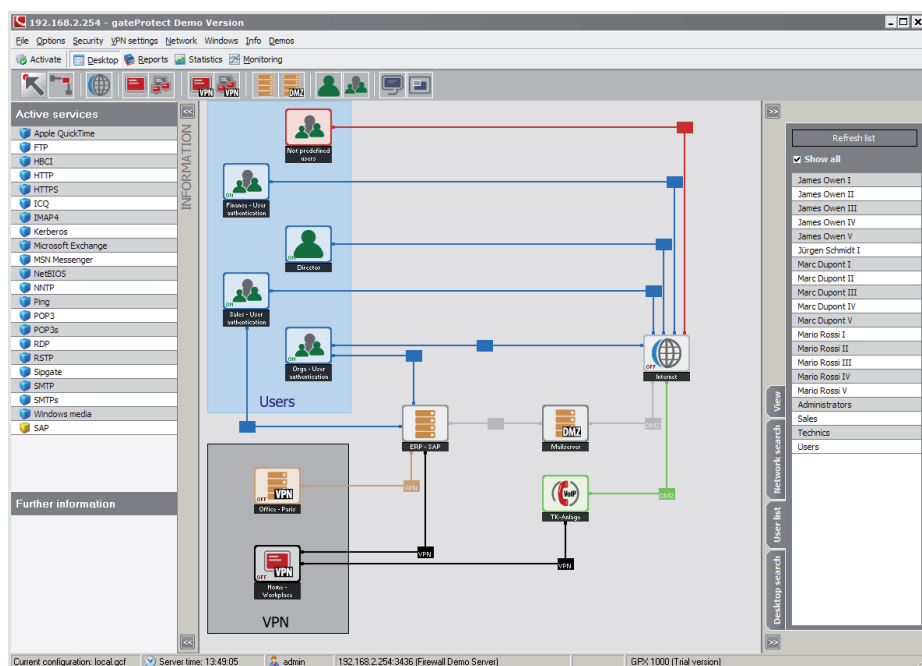
As mentioned above, after the initial configuration the administration tool contains just one icon symbolising the Internet connection, five icons which represent the LAN sys-

more precisely and define systems that were permitted to surf the Internet, set up computers which could only access external servers via SSH and create entries which were only able to get firmware updates from the Internet. First of all, we had to introduce the computers and the users in the network to the firewall.

There are two ways to do this: First of all there is a manual procedure: we dragged a computer, a user or a group icon from the icon bar to the desktop and then entered details such as IP address, user name or network address. Secondly, the appliance makes available functions for searching for computers in the network and for importing user data from an active directory server. It then presents the systems and accounts it has found in a list of known objects on the right-hand side of the work space. From there, we were able after the search or import process to drag and drop the relevant components with all the information (IP address, user name etc) onto the desktop and provide them with connection privileges.

There were no problems with importing the active directory data in the test and the search function found all the active components in the network. The function described here therefore saves the administrators, particularly in larger networks, a lot of time and also makes error-prone manual data entry almost superfluous.

Once the objects were available on the desktop, we started to define the individual connection rules. We selected the connection tool in the icon bar of the configuration tool, clicked on source and target and then had the option of enabling or blocking the connection of certain services, service groups and directions. The supplier had already defined important services such as HTTP, HTTPS, FTP, SMTP, POP and also Elster, but



The gateProtect administration tool with the straightforward configuration desktop

As already mentioned in the introduction, the gateProtect administration tool is a special feature. Unlike products from most other suppliers, the solution does not work with lists containing the services to be permitted and those to be blocked with their source and target addresses,

terms connected to the five internal interfaces as computer groups and five connecting lines between the computer groups and the Internet in which the previously defined services were enabled.

We now wanted to set up the rules

server settings: the host name, domain, routing, the NTP configuration, the time zone and so on. There is also external configuration access to the firewall and a function to switch off ping responses.

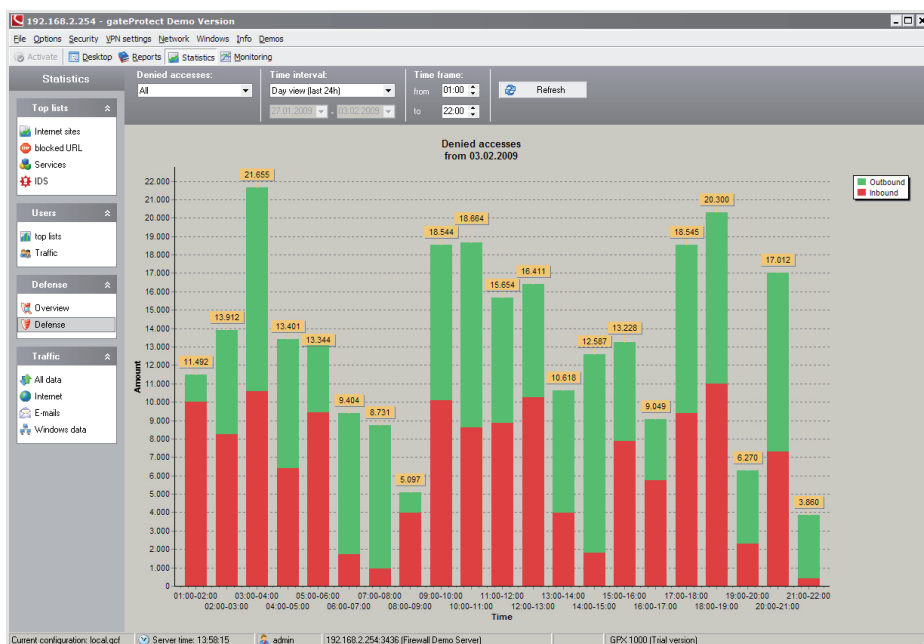
The network configuration facility is not only used to configure the network cards, but also the VLAN interfaces, bridges and SSL-VPN access. Incidentally, the Internet connection not only controls access via routers, DSL and ISDN, but also supports set up and updating of DynDNS accounts, so that the users of DSL access with dynamic IP addresses can reach their services from outside. This is particularly important for VPN functions, which will be covered later in this article.

The proxy settings are also interesting, as this is where the administrators establish whether the system should function as a proxy and, if so, how. In total, the solution offers three different proxies for HTTP, HTTPS and VoIP (SIP). The HTTP proxy can be used both as a transparent and a non-transparent proxy via port 10080 and can be combined with authentication functions (e.g. user authentication, radius authentication, etc.) in non-transparent mode. A traffic-shaping function, which allows QoS threshold values to be set for the individual services of each network component, is included in the software plus a high-availability feature which will allow the IT staff to configure their Internet access so that it continues to work after an appliance has failed.

There are also details about the DHCP servers running on the interfaces, the languages that can be used (German, English, French and Italian) and messages. These might be e-mail alerts, syslog reports or SNMP traps and are available for all the relevant subject areas. The test did not present any problems with configuring and using messages.

User administration creates different user accounts, contain access authorization to the various functions of the configuration tool as required.

tion of users' privacy, IT staff have the option of adding an anonymity function for the content filter logs. The content filter function is licensed



The statistics function provides information about the action taken by the UTM appliance.

For example, this makes it possible to permit individual users to work with the user administration tool, the reporting settings and the proxy settings, whilst others may change rules with the configuration desktop. This means that every company has the opportunity to delegate administration of the security appliance to several different staff members (thus practising division of labour) without having to allow individual users more privileges than necessary.

User authentication is used to configure user log-in. As mentioned above, it not only supports a local user database on the appliance, but also access to active directory data. If requested, a single-sign-on system can also be implemented with Kerberos. The content filter is configured through the security menu. It is based on technology from Cobion and allows blocking of certain categories such as „medicine“, „sex“ or „society“ and also allows the use of blacklists and whitelists, e.g. to block content such as „mp3“ or „wma“. If corporate policy demands protec-

tion separately and the administrators activate its operation at connection level. In the test, the feature functioned as expected. The anti spam and the mail filter functions are also interesting. The system uses blacklists and whitelists for the mail filter, whilst the anti-spam function (which is from Commtouch and also requires a separate licence) offers the additional option of putting a spam identifier in the subject line of e-mails which appear to the system to be „suspicious“, „known“ or „confirmed“. This label can be used later on the clients to move the e-mails to a spam folder automatically if required.

A real UTM appliance must have an optional anti-virus function. gateProtect uses the anti-virus system from Kaspersky. The configuration dialogue shows information not only about the most recent update but also allows the employees responsible to activate the scanner for the HTTP, FTP, SMTP and POP protocols and to define how the anti-virus function should deal with certain files, such as archive files.

The test revealed no problems in handling the antivirus engine. The system also handled zip bombs such as „42.zip“. One helpful feature deserves a mention here: the appliance can be instructed to scan HTTPS traffic.

Finally, the solution also comes with an Intrusion Detection System (IDS) based on Snort. The administrators have the option of defining the level of security required, to activate rule groups such as „DDoS“ and „Backdoor“, to specify which computers belong to the internal network, to update the identification signatures and to limit the capacity of the IDS to free up system performance for other things. For example, it makes sense in this respect to register attacks on certain ports for defined addresses only or also to switch off port scan monitoring.

VPN configuration

The product supports PPTP, IPsec and SSL VPNs (virtual private networks). In the test, we used the gateProtect VPN client in order to set up a connection to our test laboratory from an external Notebook under Windows XP SP2. We followed the supplier's recommendations and used the wizard in the appliance's administration tool to set up the connection.

The wizard asks for the normal parameters for an IPsec connection such as certificates, encryption algorithms and similar, then sets up the connection on the server and, finally, enables the IT staff member to download a configuration file containing the connection data for the client. On the client side, it is sufficient to install the VPN software and to click on the configuration file specified to open the tunnel. The procedure is foolproof, at least as far as homogeneous gateProtect environments are concerned, and will certainly not throw any administrators into confusion.

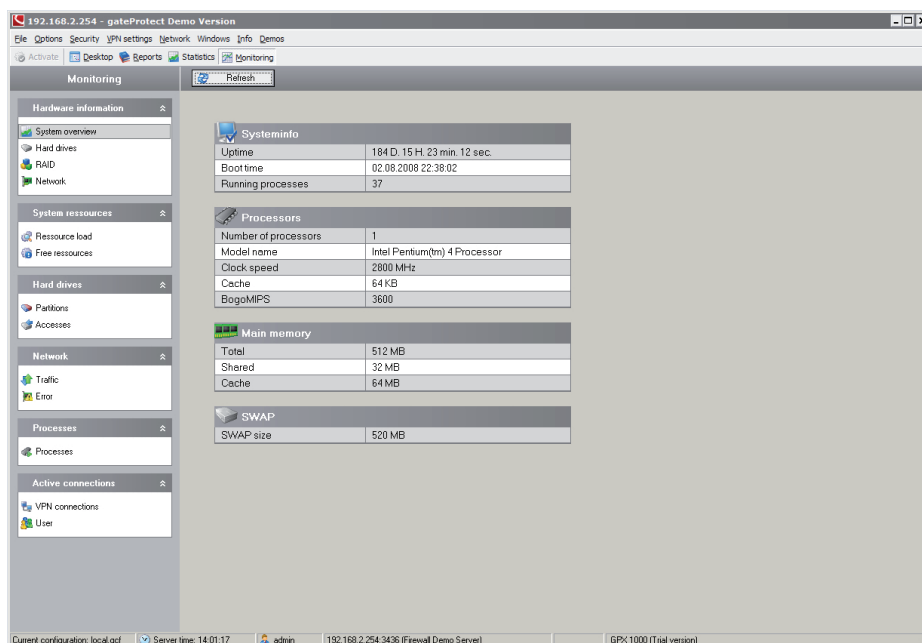
As the supplier supports VPN connections with preshared keys, but recommends working with certificate-based VPNs, we set up a connection with certificates as part of the test. This did not create any problems; indeed it was noticeable that the producer had realised an ideal certificate management system (also for SSL-VPNs).

The system shows the user exactly which certificates are needed, offers support in creating them and also helps to manage the CAs and to create requests. With these functions, even an inexperienced user would succeed in creating a functioning certificate-based VPN within a very short time.

menu line is an icon bar that allows administrators to switch between several different windows.

In addition to the configuration desktop discussed above, the tool offers windows on which users can configure the computer and their connections and also pages with reports, statistics and a system overview.

Let us return briefly to the configuration desktop. This not only distinguishes between systems and groups, but also makes it possible for IT staff to use different icons for desktops, servers and notebooks. This makes the graphic representation clearer. The entries for the underlying configuration parameters (IP address etc)



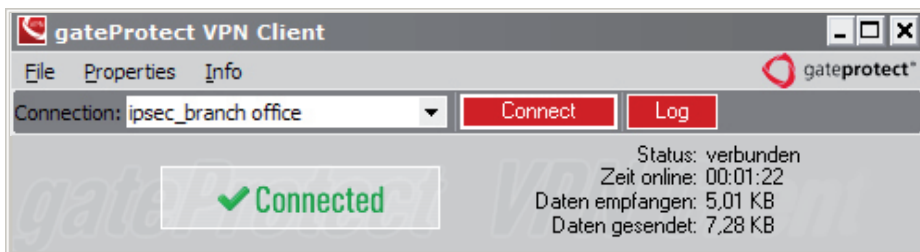
The monitoring section informs the administrators about the system status and the active connections.

In summary, it can be said that gateProtect has provided a very good solution for VPN configuration. Again, the configuration tool not only makes routine jobs easier for specialists, but also supports administrators with less in-depth knowledge of security issues.

Other functions

Diagnosis tools such as Ping and Traceroute complete the set of administration tools supplied. Below the

are identical. The administrators also create VPN systems, VPN groups, VIP components, printers and DMZ hosts similar to the computers. For the VPN systems, the appliance asks for the VPN connection to be used, whilst for the DMZ hosts a wizard is launched that requests the name, the interface involved, the IP address and the type (mail server, web server, FTP server). Alternatively, users can also define the services to be enabled themselves.



The VPN client performed impeccably in the test.

As far as the connections themselves are concerned, it is possible to group several services and limit the period over which the rules apply. This means, for example, that it is possible to ensure that certain users have more access privileges during breaks and after the working day has ended than they have during working hours.

Apart from that, the administrators also define as part of the rule configuration whether the system records access for statistical purposes, uses the proxy for the connection or uses an application level gateway. Port forwarding configuration is also done at this point.

A brief explanation of the remaining functions: The reports include an overall report, a list with current events (timeouts and so on) and an IDS report. The statistics can be output for specific systems, users and time periods and include Internet pages visited, blocked URLs, ser-

vices (i.e. protocols used), the IDS, the amount of traffic, employees, e-mail traffic and data transferred from Windows.

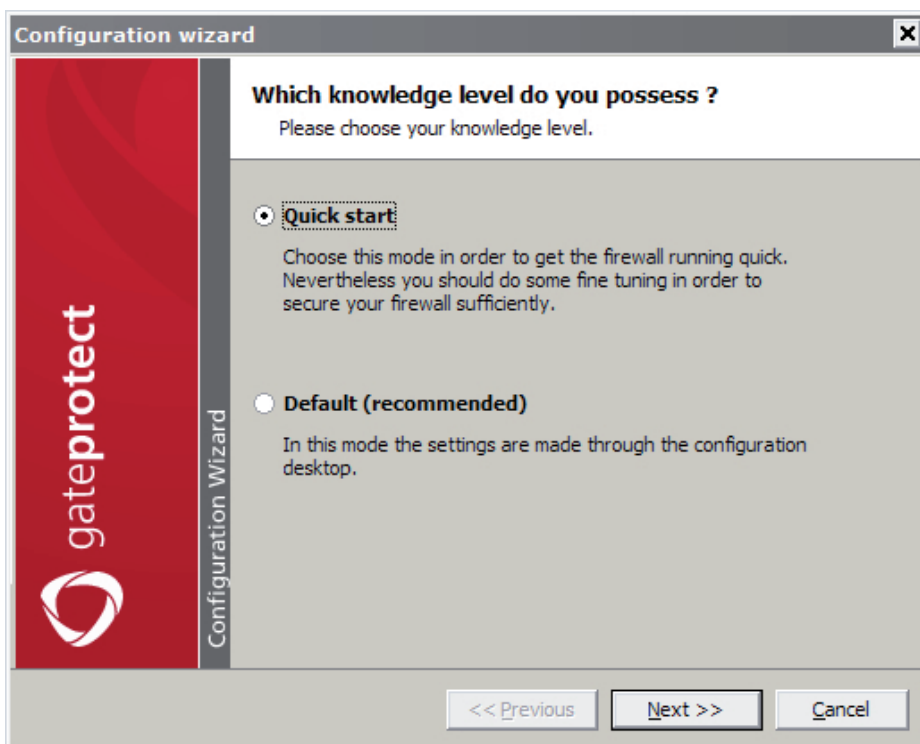
Incidentally, it is also possible to pass data such as URLs directly from the statistical overviews to the content filter. Finally, monitoring offers users hardware information such as space on the hard disk, CPU data, up time and similar. There are also overviews of system resources, partitions, network traffic, processes and active VPN and user connections.

Conclusion

The xUTM appliance V8 made an extremely good impression in the test. Thanks to its many wizards, the solution was quick to put into operation and the ease with which it can be configured fully lives up to the supplier's promises. The approach

of symbolising the systems and users as icons and setting up access rules for each connection is simple, easy to understand and provides a very clear interface for operation, both for security specialists and for administrators without special training in the security environment.

The solution stood up well to testing in all other respects. We subjected the appliance to various attacks from DoS tools, security test suites and malware programs. These did not result in instability or delays. Nor did the product reveal any more than was necessary in response to port scans. All the viruses used in the test were found and the content filter behaved as requested. The gateProtect product was most impressive across the board and scored well in every functional area. It deserves to be considered not only by security experts but also administrators looking for an easy-to-use firewall.



Wizards such as this one help in routine work with the product

Dr. Götz Güttich

runs the Institute for the Analysis of IT components (IAIT) in Korschenbroich / Germany.

Go to www.iait.eu to read his test blog.

IAITested