

Plug-in network security: gateProtect appliance on test

(http://www.zdnet.de/sicherheit_in_der_praxis_netzwerksicherheit_als_plug_in_gateprotect_appliance_im_test_story-39001543-39198451-1.htm)

Wednesday, 5. November 2008

Plug-in network security: gateProtect appliance on test

UTM security appliances promise total security for company networks Using gateProtect as an example, ZDNet shows what the appliances deliver and when they need to be supplemented with additional security measures.

Von Christoph H. Hochstätter, ZDNet

Reading the marketing brochures from many suppliers of UTM[1] appliances, one gains the impression that IT security is really quite simple: place one appliance between the intranet and the Internet, and between the clients and the servers in the network and you are protected from every threat. Unified Threat Management (UTM) averts every danger - viruses and spam remain outside. Confidential data, on the other hand, can no longer leave the company. Security company Sophos even presents decision-makers overwhelmed with glossy brochures with this message in the form of a detective novel.

ZDNet tested the UTM appliance GPX 800 from gateProtect. The GPX 800 is one of a total of six hardware appliances offered by gateProtect, whose range also includes three software appliances as VMware images.



All the appliances run under Linux, with the two smallest implemented in Fritzbox form factor. They are suitable for 10 - 25 users. The four larger hardware appliances are available in 2U rack format.

The GPX 800 tested by ZDNet is configured for networks with up to 500 users. The firewall is said to achieve throughput of up to 3 Gbit/sec. VPNs are possible up to 250 Mbit/sec. The device has a dual-core 1.86 GHz Intel Xeon 3040 CPU[11] and a 2Mbyte level 2 cache plus 4Gbytes of main memory. Although the 65 nanometre CPU with 65 watt TDP is not ideal from the „green IT“ point of view, appliances that are always based on the latest hardware technology are hard to come by. On the other hand, what you get is a combination of hardware and software that has been subjected to intensive stability testing.

The GPX 800 has eight Intel Gigabit Ethernet controllers with hardware TCP/IP offloading. This allows you to construct eight virtual networks with „dumb“ Ethernet switches, without any layer 2 or layer 3 functionality such as 802.1X.

The firewall function of the appliance can only be used to restrict data traffic between different networks, i.e. computers connected to different ports of the appliance. It makes sense, for example, to connect all the workstation computers to one port and all the company servers to another. Then you can define on layer 3 level which workstation computers can communicate with which servers and how they should do this. If you want to prevent workstation computers from communicating with each other, as a minimum layer-2 switches must be installed in the company to ensure that each computer can only exchange data with the appliance's MAC address.

The appliance is normally operated with a Windows client application. Though possible, logging on at shell level is not necessary as a rule. gateProtect recommends that only administrators or partners with platinum certification from gateProtect work at shell level.

Working with the administration client

After first logging onto the administration client, one normally sets up the Internet connection. This can be done in three ways: By PPPoE, referred to by gateProtect as a DSL connection, with standard IP routing or via ISDN.



Missing here is the option to assign an IP address by DHCP. All the German cable Internet suppliers use this variant, as do many telecommunications companies which offer glass fibre as far as the customer. In this case, an additional router is a must.

Managing the Internet access points is convenient. Several modes of access can be configured. One access point can be defined as back-up access. For example, ISDN can be used in the short term if the DSL connection fails.

Plug-in network security: gateProtect appliance on test

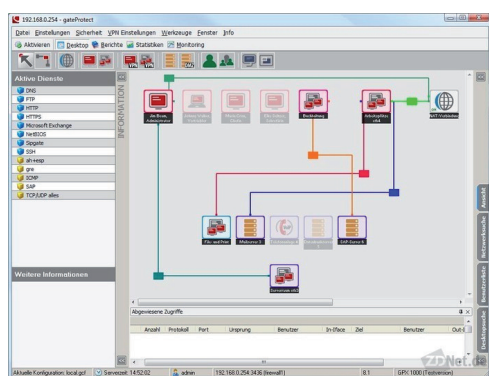
(http://www.zdnet.de/sicherheit_in_der_praxis_netzwerksicherheit_als_plug_in_gateprotect_appliance_im_test_story-39001543-39198451-1.htm)

Back-up connection via UMTS is only possible with an external router. Many companies prefer UMTS access as back-up, as it achieves better speeds compared with ISDN. Other suppliers, such as Lancom, offer devices with an integrated UMTS module.

A function for dynamic DNS is also integrated. Even if the main connection has a permanent IP address, another IP address is supplied at the latest when a back-up connection is used. Dynamic DNS makes it possible to set up permitted connections from outside, for example VPN or e-mail.

However, dynamic DNS can only be realised via providers such as DynDNS.org with RFC 2845. DDNS with RFC 2136 with BIND or the Microsoft DNS Server is not supported, which large companies in particular will miss. One of the ZDNet test scenarios represents a small company. All the employees are permitted to access two file servers and the mail server.

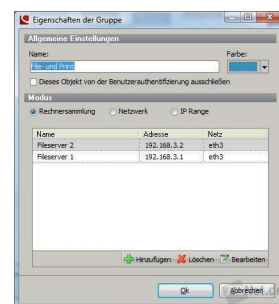
They are also allowed to use normal Internet services. The employees in Accounts are also allowed access to the SAP server. The administrator needs to have access to all the servers, particularly to the database server and the telephone system, which everyone else can only use indirectly. The administrator also has unrestricted Internet access.



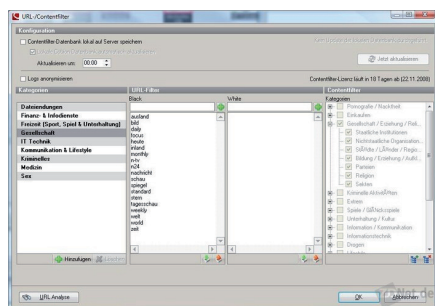
This scenario is illustrated here. The network of all the workstation computers is attached to the eth4 network card of the appliance. All the servers are connected to eth3. The connections show which servers and services can be accessed by the clients.

Even such a small demo scenario can become somewhat confusing in the administration client. It therefore makes sense to group computers with the same privileges together, as far as possible.

The illustration shows that the two company file servers have been placed in the „File and Print“ group. Similarly, the computers used by the Accounts staff are assigned to the „Accounts“ group.



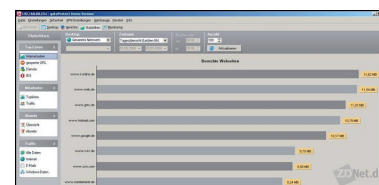
Finding a balance of freedom and security in Internet access



Which services individual users can access on the Internet can be defined precisely. For the FTP, HTTP and HTTPS services, it is also possible to force proxy usage. This can be done in the traditional way, so that users have to configure the UTM appliance as a proxy in their browser or it can be done transparently as a „hidden proxy“.

If a proxy is used, then URL and content filtering are possible and access to certain websites can be blocked for the users. It is also possible to block access on the basis of content, whereby the firewall blocks websites which contain certain key words (see illustration).

The logging and statistics functions are very extensive. Depending on the configuration, all the websites visited can be analysed by user. The works council should be consulted on the extent to which functions like these are activated.



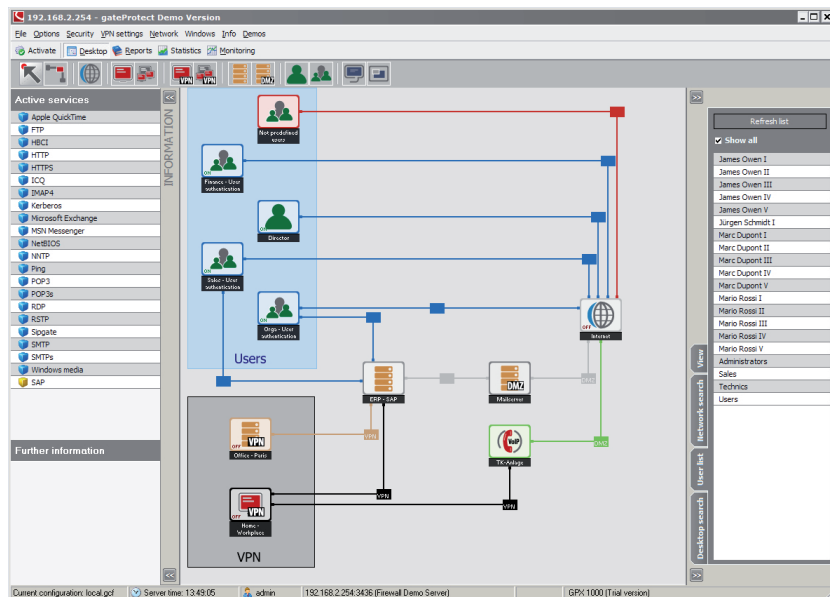
Using the proxy function with HTTPS is not without its dangers. Like all SSL/TLS encryption, HTTPS is an end-to-end encryption function. The appliance has to act as „the man in the middle“. This means that, on the one hand, all the HTTPS connections are decrypted on the firewall. On the other, the user can no longer verify the HTTPS server certificate. It is not possible to determine whether there is another man in the middle in the Internet surreptitiously inserting a forged certificate.

In order to implement a scenario like the one above, all the client computers must have permanent IP addresses, or all the computers with special privileges such as those of the administrator or the Accounts department must be connected to their own port on the firewall. If it is not easy to arrange this, because cabling presents a problem, for example, it is possible to use user authentication. This means that the access privileges are not assigned to computers but to users. However, this requires that the authentication client is installed on every computer. Alternatively there is a web client, which means that the browser window cannot be closed.

Plug-in network security: gateProtect appliance on test

(http://www.zdnet.de/sicherheit_in_der_praxis_netzsicherheit_als_plug_in_gateprotect_appliance_im_test_story-39001543-39198451-1.htm)

With user authentication, each user needs to log on again before accessing network resources. This screen shows an example of a topology with user-based authentication.



Handling restrictions on incoming connections

Incoming connections from the Internet are blocked by default. This also applies to the ICMP protocol, which is used for ping, amongst other things. Incoming connections, for a mail server, for example, must be permitted individually. A DMZ object is defined for this purpose. For a mail server, TCP port 25 is forwarded from the Internet to the mail server.

In principle, all incoming and outgoing packets are scanned for viruses. gateProtect uses the engine and the self-updating databank from Kaspersky for this. As with any appliance, this is not a substitute for virus protection on client and server machines. If end-to-end encryption is used, the appliance is unable to perform a scan.

E-mail is also searched for spam. In technical terms, the appliance uses an SMTP proxy for this, which automatically intercepts the data traffic on TCP port 25. The spam database is also automatically updated and is based on data from the large e-mail providers. If they receive a large number of e-mails with the same wording, they suspect spam. This method is very reliable, but also slightly prone to false positives, as opt-in newsletters are sometimes identified as spam. White lists help to reduce this problem.

As well as configuration at port level, the appliance has the ability to recognise the HTTP, FTP, POP3, SMTP and DNS protocols at layer 7 level. This allows users to connect, for example, with web servers that do not run on the standard port 80. Similarly, one sees whether malware is trying to use the standard port 80 for protocols other than HTTP. Malicious programs such as botnets, which receive their commands through HPPT tunnels, are not identified in this way, however.

As attackers from outside often use layer 7 protocols they have developed themselves, protocol identification should only be used to permit users the connection if a protocol is identified clearly. Unfamiliar protocols on non-standard ports should always be forbidden on principle if you want to play it safe.

Issues such as SSH port 22 are difficult to decide. As the firewall does not identify the SSH handshake reliably, malware that has been smuggled in can use it to send „home“ any data it has spied out. On the other hand, if the port is blocked users cannot use an SSH. This also applies automatically to file transfer with SCP or SFTP.

Sophisticated functions include the VPN connection between locations equipped with UTM appliances from gateProtect. VPN dial-in is also possible for mobile employees using the VPN client supplied.

Plug-in network security: gateProtect appliance on test

(http://www.zdnet.de/sicherheit_in_der_praxis_netzwerksicherheit_als_plug_in_gateprotect_appliance_im_test_story-39001543-39198451-1.htm)

gateProtect supports the IPSec and VPNs protocols with SSL/TLS. PPTP is also possible, mainly to enable Windows clients access without additional software.

It is also possible to set up VPNs between locations which are not linked through gateProtect appliances. gateProtect support includes expertise in the VPNs from suppliers Cisco and Funkwerk. With other suppliers it might be necessary to invest a little time in the configuration.

Conclusion

The UTM appliances from gateProtect offer a very good and very reliable solution for what can be achieved with a firewall. This applies similarly to the arrangements for access to company servers at layer 3 level and for making Internet traffic safe.

The graphical administration software is very sophisticated and offers many options. Although possible, access to the appliance with SSH is not necessary in order to integrate other security systems that are available for Linux, for example.

However, inexperienced administrators will not get very far, despite the graphical client. Without wide experience of the TCP/IP protocol and the knowledge of which ports are responsible for which services, it will not be possible to give users access to the services they need, nor to protect the company network from threats.

One must also be aware that a firewall does not provide protection from every danger. It does not protect against intentional or unintentional data theft. The same applies to all end-to-end encrypted connections. Neither virus nor spam protection are effective here. The transparent HTTPS proxy is an exception; however, this has other security-related disadvantages, such as the fact that users cannot verify the authenticity of server certificates.

The VPN functionality should be highlighted in addition to that of the firewall. Both site-to-site and site-to-end VPNs for dial-in by mobile users can be set up conveniently and securely with the gateProtect appliances.