

## MULTI-LEVEL FIREWALLS

By Thomas Neumann

Packet filters have long proved inadequate as firewalls. Take, for example “active content”: to manage this securely, the German Federal Office for Information Security (BSI) recommends a triple-level firewall construction.

The Dortmund issuing house, Dr. Peters, manages the assets of over 34,500 investors, representing a total of 1.75 billion Euro for an investment volume of approximately 3.6 billion Euro. The funds are almost exclusively invested in ships. Today, the Westphalian investment company maintains Germany’s largest fleet, with 32 tankers and 33 large merchant vessels sailing the seas on its behalf. Apart from the deposits invested, the fund management company’s greatest capital is the trust of its customers. “Our investors must have total assurance that their savings have been invested responsibly and will be managed in a professional manner. We work with a huge amount of highly sensitive information that must be protected from manipulation, loss and unauthorized access. For this reason IT security is a top priority in our business”,

said Jürgen Salomon, Managing Director of Dr. Peters.

### POTENTIAL RISK THROUGH ACTIVE CONTENT

Regular IT security checks are a matter of course at the Dr. Peters Group. Following a risk analysis carried out at the beginning of 2004 by Dr. Bülow & Masiak GmbH, a company specializing in internet and network solutions, they concluded that they would need to extend their firewall solution. The reason: the risk posed by active content (i.e. websites containing programs that are implemented locally) could not be ruled out with the existing security measures. Even though the exchange of data between the company’s network (LAN) and the internet is tightly restricted at Dr. Peters – only e-mail traffic, WWW links for



Photo: GeNUA

**With the GeNUGate firewall, the application level gateway and the packet filter are housed in the same box, even though they run on separate computers.**

employees, and an FTP connection to the external web server are allowed – the existing firewall solution could still not guarantee that active content would be reliably recognized. Security for transfer of data from LAN to the internet depended, in fact, on just one packet filter. This kind of firewall is blind to active content. Packet filters are, from a technical point of view, network routers with advanced rule sets. Incoming data packets can only be checked with the information in the IP header. This means sender and receiver addresses are checked, as well as the type of protocol used and the port number being accessed. The firewall administrator defines in the filter rules which IP packets are to be admitted. In this way, packet filters merely allow the formal control of data traffic, but cannot “see” into the data stream to recognize active content.

### APPLICATION LEVEL GATEWAY CHECKS DATA CONTENT

“With ever higher demands for IT security, packet filters have reached their

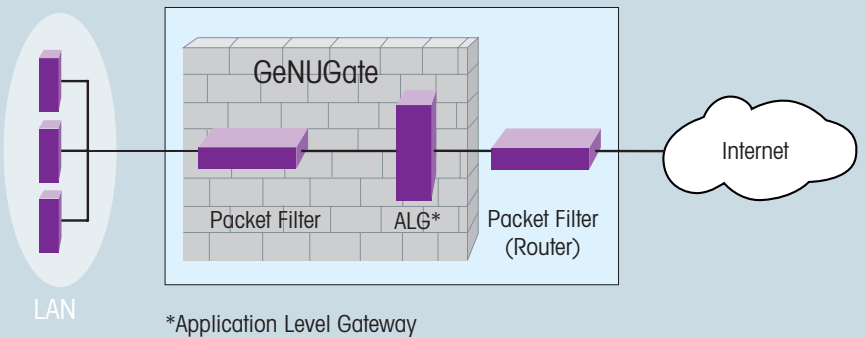


Photo: Dr. Peters Group

**Dortmund issuing house Dr. Peters invests its investors’ funds almost exclusively in ships.**

limits. As a supplementary measure you need to add a high-grade firewall of the application level gateway type, which rigorously screens data from the Internet”, explains Gerhard Bülow, Managing Director of Dr. Bülow & Masiak GmbH. An application level gateway checks the content of a data stream. Incoming data packets are initially blocked, i.e. the application level gateway never allows a continuous connection between LAN and the internet. The individual IP packets are then reassembled like a puzzle, because the only way to check the contents is by the use of complete data sets. The system next analyzes the contents. The active content (Java, JavaScript, VB Script and ActiveX) are identified and filtered according to the individual configuration. In this way, pop-up windows may, for example, be accepted, while at the same time further downloading of data has been prohibited. Data can also be filtered according to MIME types, extensions and URLs, and cookies can be removed. In this way harmful data such as active content and viruses, as well as spam, are already blocked at the firewall. Only after the content has been thoroughly checked as described does the application level gateway transfer the data to the LAN via a new connection.

## The German Federal Office for Information Security (BSI) recommends using P-A-P firewall solutions



For the LAN-Internet interface, the BSI recommends placing an application level gateway at the center of a configuration where it is combined with two packet filters.

Source: GeNUA

The German Federal Office for Information Security (BSI) also advises against depending entirely on a single firewall at the critical LAN-Internet interface. Instead, two packet filters should be combined with an application level gateway in a configuration that places the high-grade firewall at the center (PAP configuration). This means that the application level gateway is protected from direct attacks on both sides, and

even if one firewall system breaks down, a high level of security is still guaranteed.

## TWO FIREWALL SYSTEMS IN ONE BOX

At the Dr. Peters group, the PAP configuration endorsed by the BSI was implemented by linking the existing packet filter to a firewall manufactured by GeNUA in Kirchheim near Munich. The GeNUGate firewall allows the application level gateway and the packet filter to be placed together in a single box, even though they run on separate computers. “The control mechanisms of both firewalls integrated in the box are perfectly tuned to each other, complementing one another on different levels to create an effective protective shield”, explains Gerhard Bülow. The whole system is administrated through a standardized interface on the browser, while the connection is encrypted using SSL.

With these measures, the Dortmund issuing house now has a firewall system which “thanks to the security levels installed in it, guarantees the extremely high security measures required for their EDP system”, says Professor Rolf Lauser, an expert on business information technology/data privacy and security at Munich Technical University, following his appraisal of this system. ■

## BASICS OF THE TECHNOLOGY

### Dealing centrally with active content

Active content travels piggyback on e-mail or www data, and can perform any actions on the host computer, for example building an animated website or deleting files on the hard disk. The number of applications with active content in circulation, whether harmless or dangerous, is constantly increasing. This content can be “switched off” in browsers and e-mail programs with just a few mouse clicks. However, this suppression method on each individual client is as arbitrary as it is insecure. On one hand, a lot of harmless content actually desired by the organization may be blocked, as there is no filtering process. On the other hand, Microsoft’s zone model provides inadequate protection, and can be bypassed with tricks. For example, all applications the client has already installed are considered secure, without distinction. However, if a hacker knew a particular client’s filing system, harmful applications could be sent to this client via e-mail, and then activated in the supposedly secure zone. What’s more, individual settings on all clients are not sufficient to ensure the security-focussed treatment of active content in a business environment. This can only be done through the central network administration. This integrated control concept should be put in place at the point where data from the internet are admitted – in other words, at the firewall.