

## User-friendliness improves security

# Easy-to-use firewalls

What would Formula 1 drivers be without their electronic cockpit? Good drivers relying on luck to keep their racing cars under control. Modern firewalls are so complex that their administrability is threatening to become a risk to security. But new operational concepts can combat this danger.

In these times of shrinking investment budgets, ergonomics has become a cost issue. However, one might pose the question of whether this argument has a place in the world of firewalls. These security solutions are becoming increasingly complex but their administrators are generally IT professionals to whom the command lines and code represent a world that they have come to know and love. But is that always the best choice?

In this era of e-business, the differences between the levels of security dependent on company and network size are disappearing. There are in principle two different responses to this: increasing the number of IT administrators significantly or simplifying administration.

Anyone choosing the latter option will have to focus on human beings, and their ideas and expectations when considering the design of administration consoles for firewalls.

## The five laws of ergonomics

A measure of how ergonomic a firewall cockpit is are the principles governing the design of software dialogue, as formulated in ISO 9241, part 10.

### A screen dialogue must be „suitable for the task.“

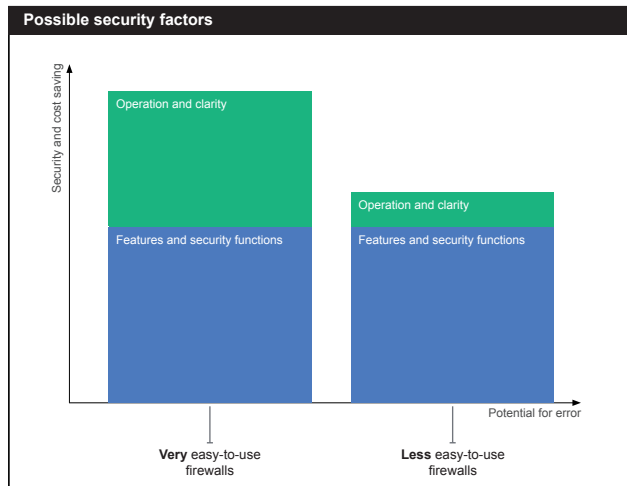
This rule means, amongst other things, that unnecessary steps must be avoided or carried out automatically by the system. Furthermore, only that information should be displayed which is directly related to the task in question. Traditional firewall user interfaces show the various features and possibly also the relationships between the various settings. However, this is of little use if an administrator needs to create a new user who works in Sales and therefore is subject to the same security rules as his department colleagues. A „suitable“ user interface therefore shows the new user and the user group to which the user is to be assigned. The new user’s symbol is integrated in the group with drag and drop and automatically acquires its security settings. Should some of the rules vary for this user, for example if he/she is the new Head of Sales, one click on his symbol should be sufficient to display all the functions relevant to him/her in the different firewall applications and their current configuration in a consolidated display.

It would then have to be possible to make changes to the settings with multiple-choice menus.

### A successful dialogue can describe itself.

An interface meeting the criterion of „self-descriptiveness“ should give a quantity of information content when the symbol is selected that allows its meaning to be identified as easily and, at the same time, as unambiguously as possible. The symbol for a workstation computer should therefore be as similar as possible to its real counterpart. On the other hand, a real user can also be represented by their full name, with no need for a graphical symbol. Self-descriptive also means that the meaning of a symbol does not change, no matter which context it is used in. Context-dependent differences in the meaning accordingly require new symbolisation to remain unambiguous.

The user must have control of the dialogue. Returning to the example above, the security settings for a Head of Sales can be so different from those of the non-managerial staff that it would mean additional, unnecessary work to assign the manager all the department’s security settings.



Easy-to-use firewalls improve security considerably.

Source: gateProtect

In this case, the administration console must offer the option of entering the required configurations directly on the user's level.

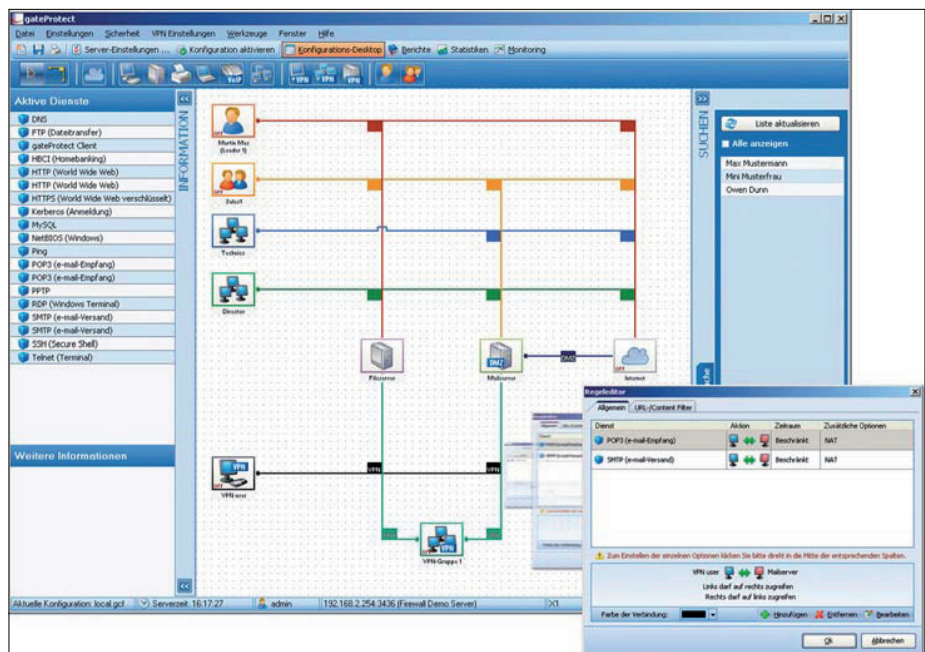
### Conformity with expectations is very important

It is unacceptable for a user if information within one and the same application environment is presented in different ways or if the dialogue looks different or uses different words from one application to another. For example, for a user, URL and content filtering are two sides of the same coin when settings are displayed at group or user level. Obviously, there are two different firewall applications operating in the background, but display of the menus and configuration options must be consolidated. What is more, the nomenclature of both applications must be the same. For example, if sexual content and Internet addresses that lead to pages of this nature need to be blocked, the categories of URLs and the content must have the same designations. This is not a trivial requirement, because OEM products from different manufacturers are often used in this area. URL and content filtering is, incidentally, an excellent example for the interaction of all the criteria listed so far. Unambiguous and generally understandable nomenclature presents the option of allowing configuration by users other than the IT administrator. There might well be websites with a domain name containing the letter sequence „sex“, and which are blocked, although they are important for the Sales department. But who knows more about this website than the Sales department? If the settings for URL and content filtering can be made in a single dialogue pane by a non-technical staff member for all the users in the group „Sales“, then the user guidance is suitable for the task, self-descriptive and controllable, because it is adjusted to the users' level of knowledge.

### A vital component of a firewall user concept is support for learning.

The requirement for „support for learning“ says that the degree of technical knowledge in the administration of the system should be as low as possible. For example, branch offices of retail chains or banks, geographically scattered production and sales locations of large companies, and also smaller compa-

arrow points to the right, which is where the Internet symbol is placed. One click must be enough to bring up a more detailed description to explain the symbols. Instead of the technical term „stateful inspection“, the non-technician only needs a self-explanatory description, such as „left can access right, right may only respond“. What is more, these formulations reduce the risk of incorrect input.



Designing a user interface demands a great deal of insight

Source: gateProtect

nies such as law chambers or tax advisers who have a special responsibility regarding personal data have similarly high security requirements to the head offices of large conglomerates, but do not have the same level of technical expertise. It is therefore advisable to describe security functions without technical terminology, wherever possible. For example, a user skilled in using the Internet knows that the ability to access his computer in his network from the Internet represents a threat. In a graphical interface this relationship can be shown with an arrow symbol. On the left of the arrow is the computer, the

### Conclusion:

The ergonomic design of firewall cockpits creates direct access to the various administrative tasks and avoids sources of errors through multi-application views and options for control. This makes it possible to delegate administration to different user groups, saving time and money and also increasing the level of security - it is the cockpit that elevates good drivers to Formula One class.