G DATA Security Client Firewall - Regelsaetze

G DATA Security Client Firewall - Rule sets

In the Rule sets module you can create and edit rule sets (groups of firewall rules that can be applied to networks).

- **New**: Create a new rule set. In the following dialog, enter a **Rule set name** and decide if the rule set should be pre-populated with rules from the default rule sets for untrusted, trusted or blocked networks.
- **Delete**: Delete the selected rule set. The default rule sets cannot be deleted.
- **Edit**: Edit the selected rule set using the **Rule Wizard**.

The Rule sets module contains default rule sets for the following network types:

- **Direct Internet connection**: This covers rules that involve direct Internet access.
- **Untrusted networks**: This generally covers open networks with Internet access.
- **Trusted networks**: Home and company networks are generally trusted.
- **Blocked networks**: This rule set can be used if access to a specific network should be blocked.

G DATA Security Client Firewall - Rule Wizard

The Rule Wizard allows you to define new rules for the selected rule set or to modify existing rules. The Rule Wizard is especially suitable for users unfamiliar with firewall technology. For a granular control over individual rules, use the **Advanced Rule Set Editor**.

The Rule wizard offers various rules. All of them can be used to quickly allow or deny a specific type of traffic. For most rules, a specific **Direction** can be defined, which governs whether the program is tobe blocked for inbound connections, outbound connections or both.

- **Share or block applications**: Select a specific application on the hard disk to explicitly permit or deny it access to the network governed by the rule set.
- **Share or block network services**: Blocking one or more ports is a quick way of eliminating vulnerabilities that could be used for attacks by hackers. The wizard provides the option ofblocking ports completely or for a particular application only.
- **File/printer sharing**: Allow or block file and printer sharing.
- **Share or block domain services**: Allow or block network domain services.
- **Shared use of the Internet connection**: Allow or block Internet connection sharing (ICS).
- **Share or block VPN services**: Allow or block Virtual Private Network (VPN) services.
- **Advanced Rule Set Editor (expert mode)**: Open the **Advanced Rule Set Editor**.

G DATA Security Client Firewall - Advanced Rule Set Editor

The Advanced Rule Set Editor allows for the creation of highly specific rules. It can be used to create all of the rules that are also available through the Rule Wizard, but also supports custom settings.

The Advanced Rule Set Editor window resembles the **Rule sets** pane of G DATA Administrator's Firewall module. It can be used to create, edit, delete, and rank rules within the rule set. In addition to the options available in G DATA Administrator, the Advanced Rule Set Editor offers the followingoptions:

- **Action if no rule applies**: Specify what happens when no existing rule applies to a filtered communication type: Allow, Deny or Ask user.
- **Adaptive mode**: The adaptive mode supports applications that use feedback channel technology (e.g. FTP and numerous online games). These applications connect to a remote computer and negotiate a feedback channel with it, which the remote computer then uses to reverse connect to the application. If the adaptive mode is enabled, the firewall detects this feedback channel and permits it without querying it separately.
- **Reset**: Delete all rule set modifications as well as all auto-learned rules.

By double-clicking a rule or clicking the **Edit** button, individual rules can be edited. The individual rule editor corresponds to the **Edit rule** window in G DATA Administrator.