1 mGuard firewall properties and possible applications

Document ID: 108405_en_00
Document designation: AH EN MGUARD FIREWALL

Make sure you always use the latest documentation.
This is available to download at phoenixcontact.net/products.

Contents of this document

This document describes the fundamental functions of the mGuard firewall, as well as possible applications.

1.1 Stateful packet inspection firewall

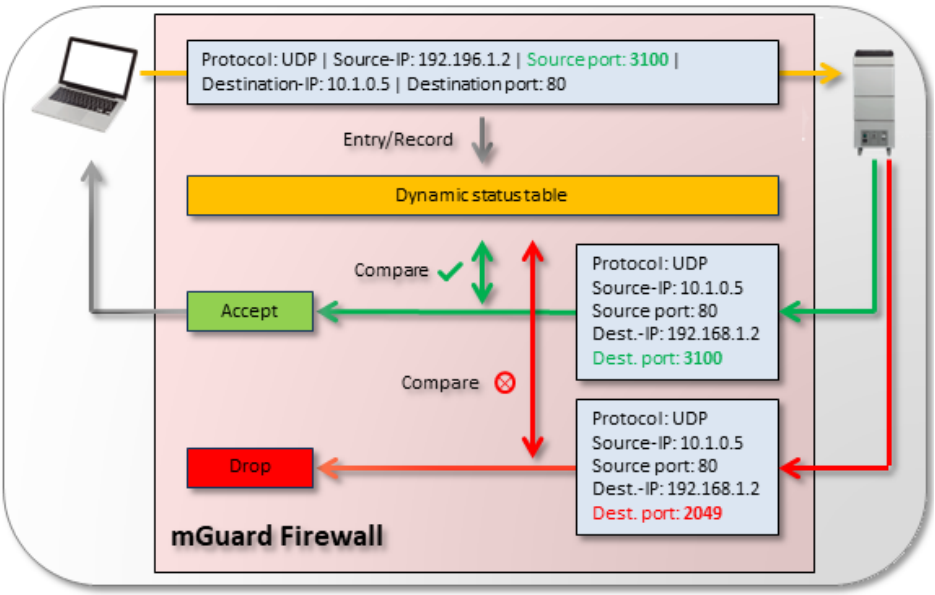

Figure 1-1 If incoming or outgoing packets pass the mGuard firewall (orange arrow), their properties (e.g. protocol, source IP/port, destination IP/port) are stored in a dynamic status table. The properties of the expected response packet are also stored in order that this also passes through the firewall. Response packets are then compared with the values in the status table. If the packets correspond to the dynamically entered values of the status table, they are accepted (green arrow). If they do not match, they are rejected (red arrow).

The mGuard firewall functions as a dynamic packet filter (*Stateful Packet Inspection Firewall*) that analyzes incoming and outgoing network packets in accordance with configured rules.

Dynamic packet filtering allows response packets to pass through the incoming firewall automatically if they can be clearly assigned to the request that previously passed through the outgoing firewall.

It is therefore not necessary in principle to configure incoming rules to accept responses to outgoing requests. An incoming rule could in fact be configured so that all incoming packets are rejected. Incoming responses to requests would still be accepted.

1.2 Static firewall

Static firewall rules are used to control access to the basis of networks (IP addresses, protocols, and ports).

These rules are static and always enabled for the selected interfaces once they have been created. This means that certain devices/networks can communicate with one another.

(**Example**: see Section 1.3, “Configuring firewall rules”)

1.3 Dynamically enabled firewall (via firewall rule records)

Firewall rules that are summarized in firewall rule records can be enabled and disabled dynamically. Enabling and disabling can be carried out

– via web interface,
– via text message (SMS),
– via switch/button,
– by establishing a VPN connection.

As with static firewall rules, access to the basis of networks (IP addresses, protocols, and ports) is controlled. The rules, however, are only enabled when necessary.

(**Example "firewall rule record"**: see Section 1, “Using firewall rule records”)

1.4 User firewall

The user firewall enables user-specific firewall rules that only apply for defined firewall users or user groups to be defined. User firewall rules have priority over firewall rules configured elsewhere (e.g. *Incoming/Outgoing Rules*) and override these where applicable.

Access to the destination is not allowed on the basis of statically configured firewall rules, but dynamically after the firewall user logs on using the user firewall rules assigned to the firewall user.

A user firewall rule comes into effect when a firewall user assigned to the rule logs on via the web interface of the mGuard device. Authentication is performed via the internal database or a RADIUS server.

(**Example**: see Section 1, “Using the user firewall to enable access to an external network”)