1 Frequently occurring errors when creating firewall rules

Document ID: 108403_en_00
Document designation: AH EN MGUARD FIREWALL MISCONFIG

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

Contents of this document

This document describes common errors when creating firewall rules (e.g. incorrect sequence, incorrect source port).

1.1 Introduction

The mGuard firewall functions as a dynamic packet filter that analyzes incoming and outgoing network packets in accordance with configured rules (see also Section 1, “mGuard firewall properties and possible applications”).

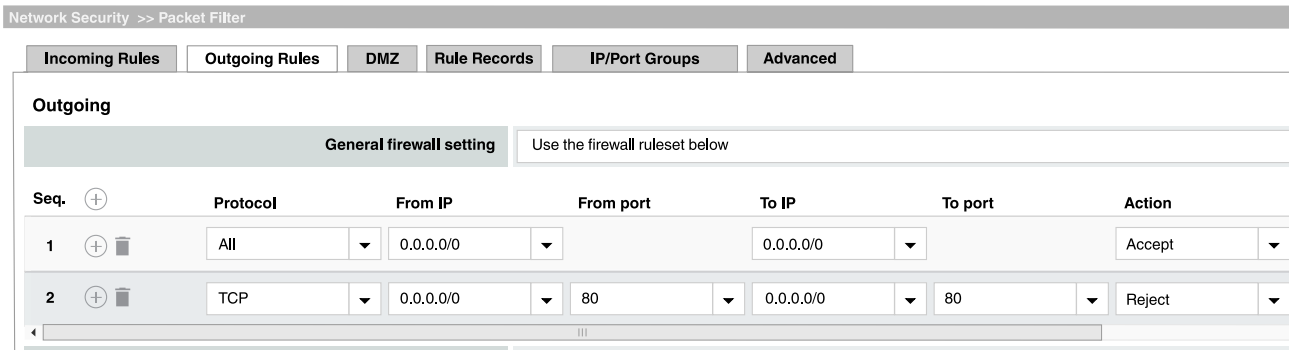
Common errors: when creating firewall rules in a table, their sequence is decisive. The firewall rules created in the table are checked consecutively from top to bottom. If a rule applies, the specified action (*accept, drop*, or *reject*) is performed and the subsequent rules are subsequently **disregarded**.

1.1.1 Example

Access to HTTP web servers from the internal network are to be prevented with the aid of configured firewall rules (mGuard menu: **Network Security >> Packet Filter >> Outgoing Rules**).

Specified ports (*From port* and *To port*) are only taken into consideration if the protocol is set to TCP or UDP.

1.2 Incorrect configuration



Error 1: incorrect sequence

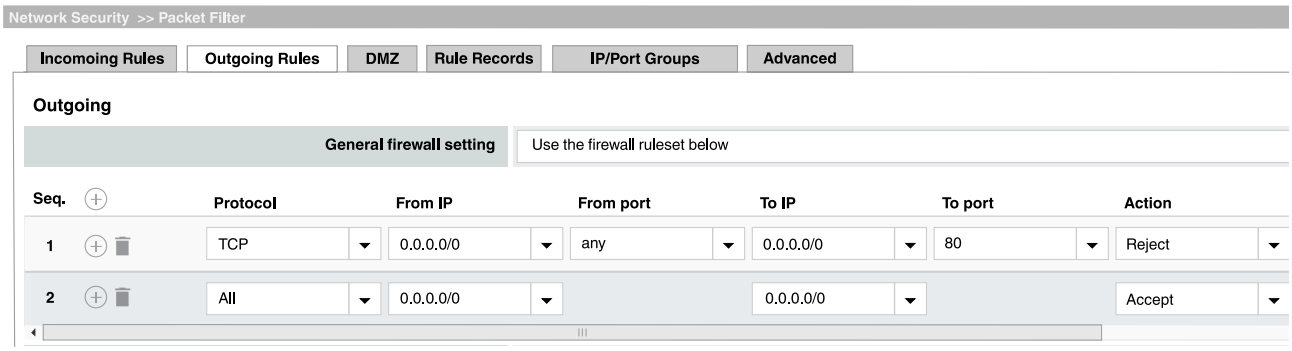
Because the first rule in line 1 already applies for all packets, the following rules are disregarded. An outgoing TCP connection to port 80 will therefore not be rejected.

Error 2: incorrect source port

HTTP requests from web browsers use a varying source port greater than or equal to 1024. The request is sent to port 80. The rule specified in line 2 will not apply because of the entered source port (*From port* = 80), i.e. less than 1024.

1.3 Correct configuration

In the correct configuration, the sequence of the firewall rules must be changed such that the rule that rejects access to a web server is checked first.



"*any*" can be specified, for example, as the source port (*From port*) in order to check requests from a standard web browser. Specifying the destination port (*To port* = *80*) rejects access to a web server.

If the first rule **applies**, the second rule is disregarded. If the first rule **does not apply**, the second rule allows the outgoing data traffic to pass.