

1 Using firewall rule records



Document ID: 108402_en_00
Document designation: AH EN MGUARD FIREWALL RULESETS 1
© PHOENIX CONTACT 2018-10-16



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

Contents of this document

The use of firewall rule records is described in this document. This simplifies and accelerates the creation of firewall rules.

1.1	Introduction.....	1
1.2	Example 1 ("Server" rule record)	3
1.3	Example 2 ("Service" rule record)	4

1.1 Introduction

Individual firewall rules can be summarized in rule records. These rule records can then be selected in firewall rules as actions and therefore put into use.

1.1.1 Example

External access to three particular servers in the internal network via the network services *ftp*, *telnet* and *https* is to be allowed. Access to all other services and network addresses from the external network (WAN) is to be prohibited.

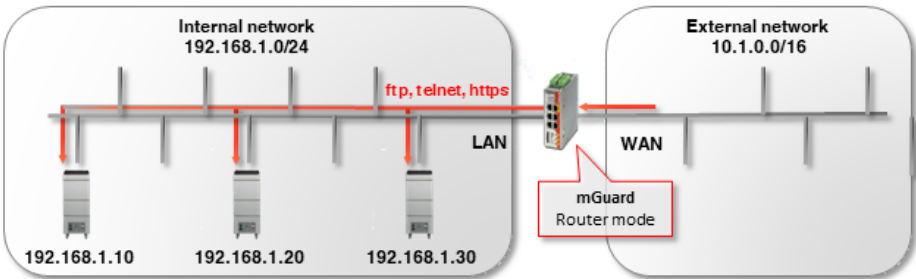


Figure 1-1 Allow access to special services on certain servers

Problem

Without rule records, nine firewall rules must be created in a firewall table: three server IP addresses for each of the three services.

Solution

With the help of rule records, certain sub-rules, i.e. the server IP addresses or the network services, can be summarized in rule records. These can then be selected as actions in firewall tables.

In this example, three incoming rules in the firewall table are sufficient to only allow access to the three servers and the three network services. Here, **either** a "Server" rule record or a "Service" rule record must be created (see "Example 1 ("Server" rule record)" and "Example 2 ("Service" rule record)").



Please note: if a connection associated with a firewall rule record has been established and this connection is continuously generating data traffic, deactivation of the firewall rule record may not interrupt this connection as would normally be expected (see [mGuard firewall user manual](#)).


1.1.2 Procedure

To allow access to defined servers and network services, the following work steps are necessary:

1. Create firewall rule record.
2. Create firewall rule records in firewall tables and refer to the rule record.

1.2 Example 1 ("Server" rule record)

To create the rule record, proceed as follows:

1. Log in to the web interface of the mGuard device.
2. Go to **Network Security >> Packet Filter >> Rule Records**.
3. Create a new rule record with the name *Server* and click on the icon  *Edit Row*.
4. Configure the rule record in accordance with Figure 1-2.

Network Security >> Packet Filter >> Server

Rule Record

General

A descriptive name	Server
Initial mode	Active
Controlling service input or VPN connection	None
Token for text message trigger	
Deactivation timeout	0:00:00 seconds (hh:mm:ss)

Firewall Rules

Seq.	Protocol	From IP	From port	To IP	To port	Action	Comment
1	TCP	0.0.0.0/0	any	192.168.1.10/32	Service	Annehmen	
2	TCP	0.0.0.0/0	any	192.168.1.20/32	Service	Annehmen	
3	TCP	0.0.0.0/0	any	192.168.1.30/32	Service	Annehmen	

Figure 1-2 The permitted destination IP addresses (destination server) are summarized in the *Server* rule record.

To use the rule record in a firewall rule, proceed as follows:

1. Log in to the web interface of the mGuard device.
2. Go to **Network Security >> Packet Filter >> Incoming Rules**.
3. Select **Use the firewall ruleset below**.
4. Create three firewall rules in accordance with Figure 1-3.

Network Security >> Packet Filter

Incoming Rules | Outgoing Rules | DMZ | Rule Records | IP/Port Groups | Advanced

Incoming

General firewall setting Use the firewall ruleset below

Seq.	Interface	Protocol	From IP	From port	To IP	To port	Action
1	External	TCP	0.0.0.0/0	any	0.0.0.0/0	ftp	Server
2	External	TCP	0.0.0.0/0	any	0.0.0.0/0	telnet	Server
3	External	TCP	0.0.0.0/0	any	0.0.0.0/0	https	Server

Figure 1-3 The **firewall table** refers to the *Server* rule record as an action when accessing the specified network services.

The firewall rules define access to specific network services (*To port*) and refer to the *Server* rule record. Access to the destinations are defined in this rule record.

1.3 Example 2 ("Service" rule record)

Instead of the server IP addresses, you can also summarize the network services in a rule record and use these in the firewall rules. The settings are as follows (see Figure 1-4 and Figure 1-5).

Network Security >> Packet Filter >> Service

Rule Record

General

A descriptive name: Service

Initial mode: Active

Controlling service input or VPN connection: None

Token for text message trigger:

Deactivation timeout: 0:00:00 seconds (hh:mm:ss)

Firewall Rules

Seq.	Protocol	From IP	From port	To IP	To port	Action	Comment
1	TCP	0.0.0.0/0	any	192.168.1.10/32	ftp	Accept	
2	TCP	0.0.0.0/0	any	192.168.1.20/32	telnet	Accept	
3	TCP	0.0.0.0/0	any	192.168.1.30/32	https	Accept	

Figure 1-4 The permitted network services are summarized in the **Service rule record**.

Network Security >> Packet Filter

Incoming Rules | Outgoing Rules | DMZ | Rule Records | IP/Port Groups | Advanced

Incoming

General firewall setting: Use the firewall ruleset below

Seq.	Interface	Protocol	From IP	From port	To IP	To port	Action
1	External	TCP	0.0.0.0/0	any	192.168.1.10/32	any	Service
2	External	TCP	0.0.0.0/0	any	192.168.1.20/32	any	Service
3	External	TCP	0.0.0.0/0	any	192.168.1.30/32	any	Service

Figure 1-5 The **firewall table** refers to the **Service rule record** as an action when accessing the destination IP addresses (destination server).

The firewall rules define access to specific destination IP addresses (*To IP*) and refer to the *Service rule record*. Access to the permitted network services are defined in this rule record.