1 Using the user firewall to enable access to an external network

Document ID: 108401_en_00

Document designation: AH EN MGUARD USERFIREWALL 1

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

Contents of this document

This document describes how to allow a firewall user access from the internal network to an external network assisted by user firewall rules.

A user firewall is not available on devices of the RS2000 series and the mGuard Blade controller.

1.1 Introduction

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.

1.1.1 Example

In this example, access from the production network (internal) to the company network (external) is enabled by NAT (IP masquerading) (see also “Option 1: masking / IP masquerading” on page 5).

At the same time, however, **all access instances** from the production network to the company network are prohibited via a general firewall rule (outgoing rule).

Assisted by the user firewall, the firewall users *pwerner* and *hpotter* now have individual access to web servers and can therefore access the web server in the company network.

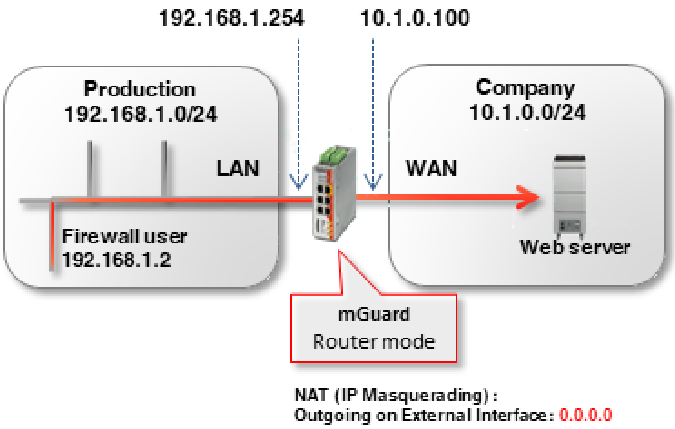


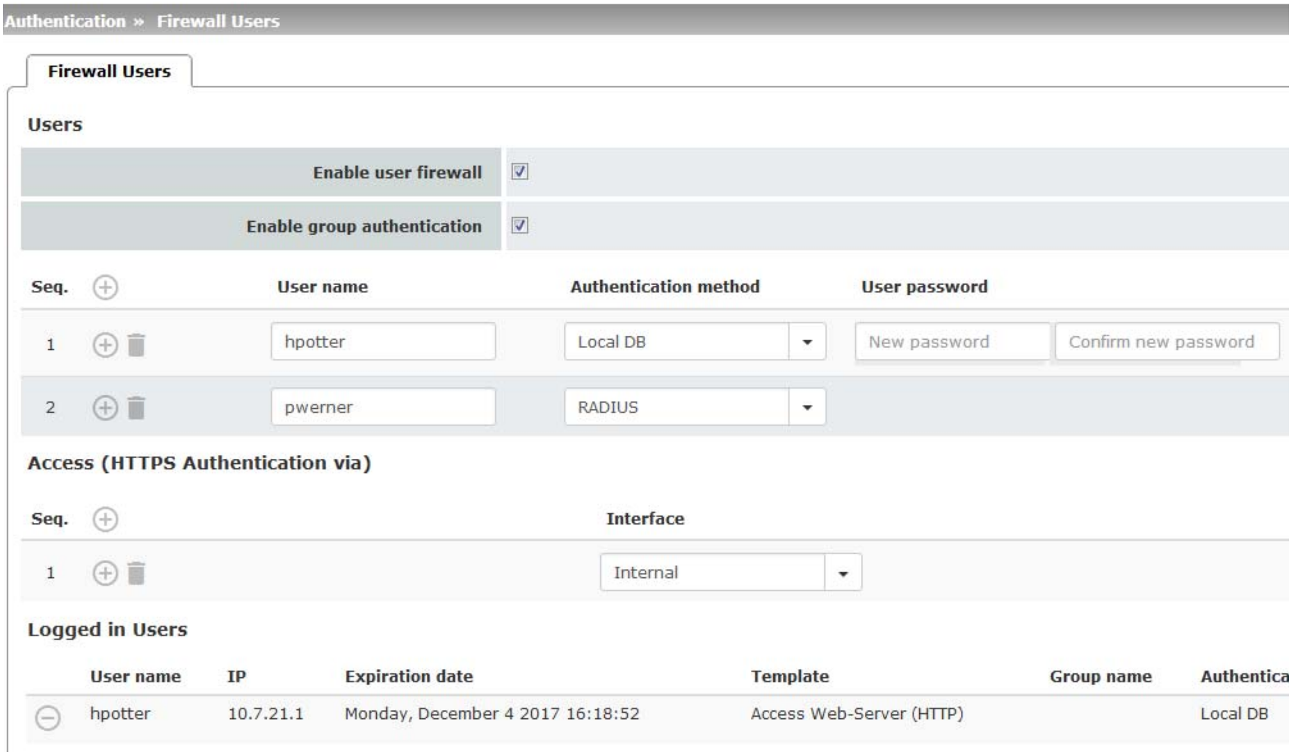
Figure 1-1 Firewall users with access rights to HTTP(S) web servers

1.1.2 Procedure

To allow the firewall users *pwerner* and *hpotter* access to a web server via port 80 (http) and 443 (https), the following work steps are necessary:

1. Create firewall users
2. Create user firewall template with firewall rules
3. Enable user firewall
4. Log in as firewall user

1.2 Creating firewall users



Authentication » Firewall Users

Firewall Users

Users

Enable user firewall	☑
Enable group authentication	☑

Seq.		User name	Authentication method	User password	
1		hpotter	Local DB	New password	Confirm new password
2		pwerner	RADIUS		

Access (HTTPS Authentication via)

Seq.		Interface
1		Internal

Logged in Users

	User name	IP	Expiration date	Template	Group name	Authentica
⊖	hpotter	10.7.21.1	Monday, December 4 2017 16:18:52	Access Web-Server (HTTP)		Local DB

Figure 1-2 Create firewall users

Firewall users are created under **Authentication >> Firewall Users**. Whether the users are authenticated via a RADIUS server or via a user password configured locally on the mGuard device is also specified here.

> The general configuration for use of a RADIUS server via the mGuard device is set in the menu **Authentication >> RADIUS**.

A firewall user can be assigned to one or more user firewall templates (see “"Template Users" tab” on page 5).

To create a firewall user, proceed as follows (see also mGuard firmware user manual):

1. Log in to the web interface of the mGuard device.
2. Go to **Authentication >> Firewall Users**.
3. Create the desired firewall users.
4. Specify the authentication procedure for each user (password or RADIUS server).
5. Specify via which interfaces the firewall users may use to log in at the mGuard device.

1.3 Creating a user firewall template

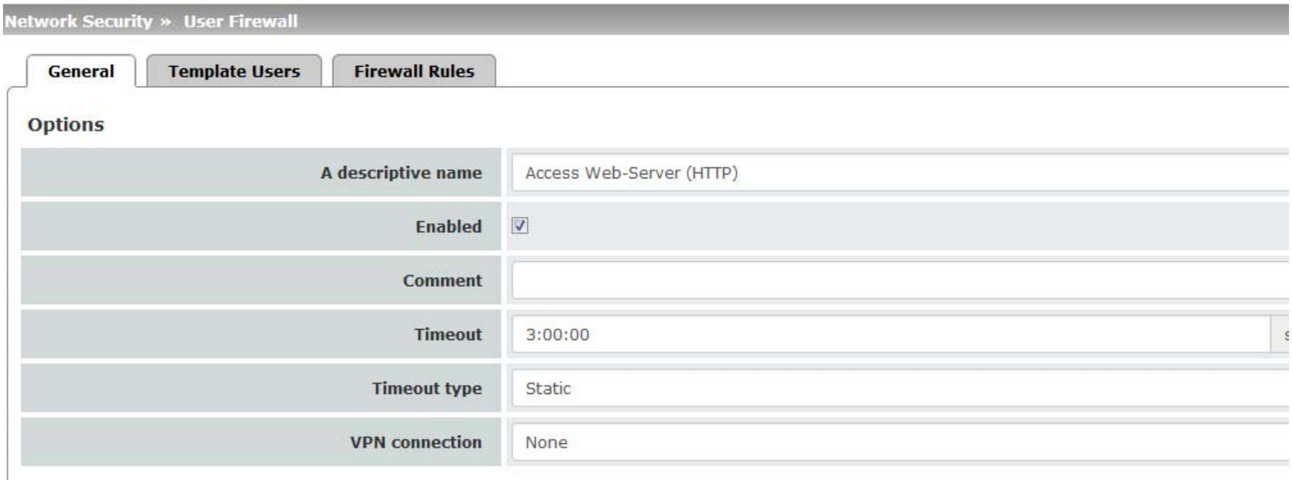
In a user firewall template, firewall rules are created and existing firewall users are assigned.

> If a user firewall template or a firewall rule in a template is added, changed, deleted or disabled, all logged-in firewall users are affected immediately.
>
> Existing connections are interrupted. An exception to this is when firewall rules are changed, and the function "Abort existing connections upon firewall reconfiguration" is disabled in the menu **Network security** >> **Packet Filter** >> **Advanced**. In this case, a network connection that exists due to a previously permitted rule is not interrupted.
>
> If a firewall rule record (template) is **disabled** and then **enabled**, the affected logged-in user must first log out then log back in for the firewall rules in the template to be enabled again.

To create a user firewall template, proceed as follows:

1. Log in to the web interface of the mGuard device.
2. Go to **Network security** >> **User firewall**.
3. Create a new template and click on the *Edit Row* icon ✎.

1.3.1 "General" tab



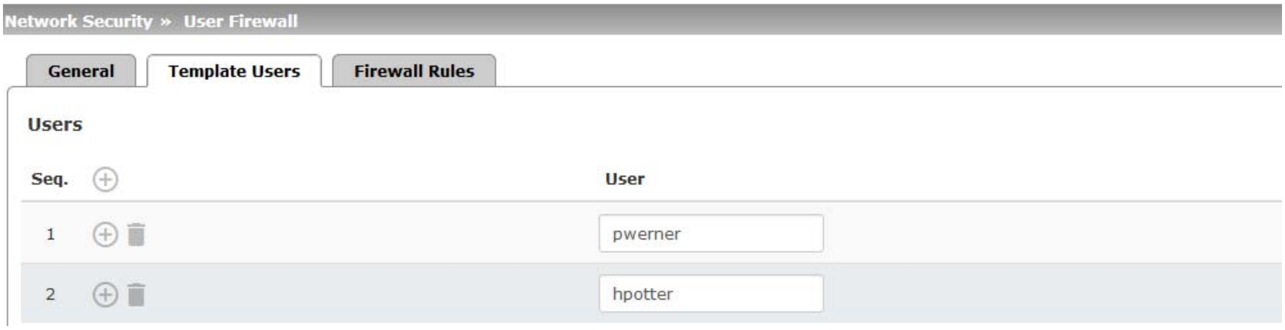
A descriptive name	Access Web-Server (HTTP)
Enabled	☑
Comment	
Timeout	3:00:00
Timeout type	Static
VPN connection	None

Figure 1-3 Creating a user firewall template: *General* tab

Proceed as follows (see also mGuard firmware user manual):

- Assign a descriptive name to the user firewall template.
- Specify how long a user firewall is to be valid once a firewall user has logged in (note Timeout type).
- If the rules of the user firewall template are only to be valid for a particular VPN connection, specify this.

1.3.2 "Template Users" tab



Users

Seq.	User
1	pwerner
2	hpotter

Figure 1-4 Creating a user firewall template: *Template Users* tab

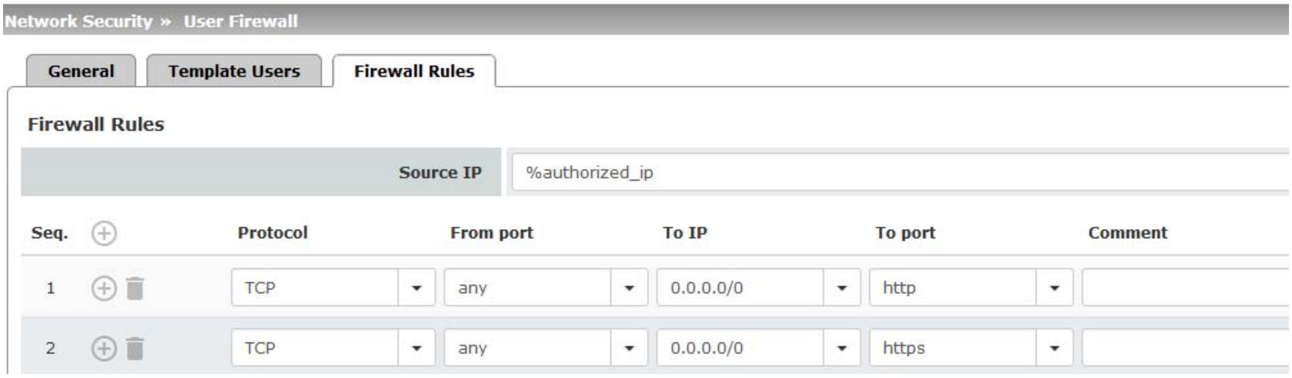
Proceed as follows (see also mGuard firmware user manual):

- Specify the name of the firewall users for which the rules of this user firewall template are to apply.

The specified users must have been defined and created under **Authentication >> Firewall Users >> Users** (see “Creating firewall users” on page 3).

NOTE: A check is not made as to whether the specified user names actually exist. Ensure that the names are entered correctly.

1.3.3 "Firewall Rules" tab



Firewall Rules

Source IP: %authorized_ip

Seq.	Protocol	From port	To IP	To port	Comment
1	TCP	any	0.0.0.0/0	http	
2	TCP	any	0.0.0.0/0	https	

Figure 1-5 Creating a user firewall template: *Firewall Rules* tab

The mGuard device automatically recognizes the interface used to log in and applies the user firewall templates accordingly as *Incoming Rules* (logon from the external network) or *Outgoing Rules* (logon from the internal network).

If the template is configured with dynamic timeout, approved UDPs and other network packets (excluding ICMP) reset the dynamic timeout to the initial value at this point.

To configure the firewall rules of the template, proceed as follows (see also mGuard firmware user manual):

- Specify a source IP address from where the connection is to be permitted.

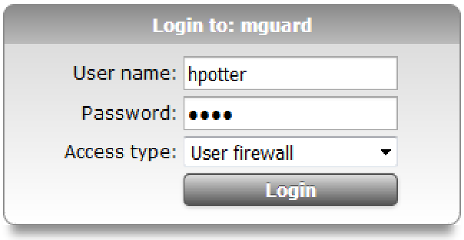
If %authorized_ip is specified, the firewall rules are used on data packets that are sent from the same source IP address via which the user logged in. Data packets from other IP addresses are dropped .

If an IP address is specified, the firewall rules are applied to data packets that are sent from this source IP address. Data packets from other IP addresses are dropped. This option should be used, for example, if an administrator logs into the device to enable the user firewall for a technician who is working on another computer.

- Create firewall rules to enable the assigned firewall users access in accordance with the rules created.

  In this example, access to any web server via the network services *http* and *https*.

1.4 Logging in as a firewall user

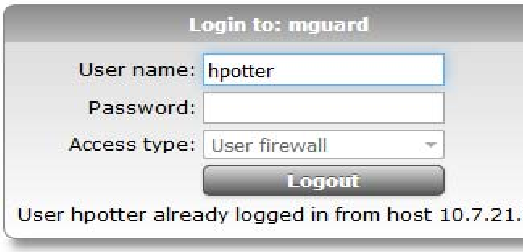


Login to: mguard

User name: hpotter

Password: ●●●●

Access type: User firewall



Login to: mguard

User name: hpotter

Password:

Access type: User firewall

User hpotter already logged in from host 10.7.21.

A firewall user must log into the mGuard device web interface via HTTPS using the web browser in order to enable the firewall rules. This can be from either the internal network or the external network (or via VPN, DMZ, and dial-up). To log in via the external network on the device, HTTPS remote access must be enabled on the mGuard device (Menu **Management >> Web Settings >> Access**).

The mGuard device automatically recognizes the interface used to log in and applies the user firewall templates accordingly as *Incoming Rules* (logon from the external network) or *Outgoing Rules* (logon from the internal network).

To log in as a firewall user, proceed as follows:

1. Open the login window in the mGuard device web interface.
2. Select the access type "User firewall".
3. Enter the user name and password for the firewall user.
4. If the login is successful, this is displayed in the login window.

Result

All connections to an HTTP(S) web server via the selected protocol are enabled when a firewall user logs in until the timeout period elapses.