1 Accessing internal networks (additional routes | IP and port forwarding | 1:1 NAT)

Document ID: 108406_en_00
Document designation: AH EN MGUARD NETWORK SEGMENT 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 the use of the mGuard device as a router that connects two networks (internal and external network). The internal network is to be accessed from the external network.

The following procedures are described:

– Option 1: additional internal routes
– Option 2: IP and port forwarding
– Option 3: Network Address Translation (1:1 NAT)

1.1 Introduction

In the "Router" network mode (*Router mode*), an mGuard device can be used to connect two networks. The firewall and VPN security functions are also available (depending on license).

With certain models, a demilitarized zone (DMZ) can be connected via the additional DMZ interface as an option.

1.1.1 Example

The production network (= *internal network*) and the company network (= *external network*) are connected via an mGuard router.

The web interface of a machine controller (PLC) in the production network is to be accessed from the company network. The controller should also respond to a ping request sent to it.

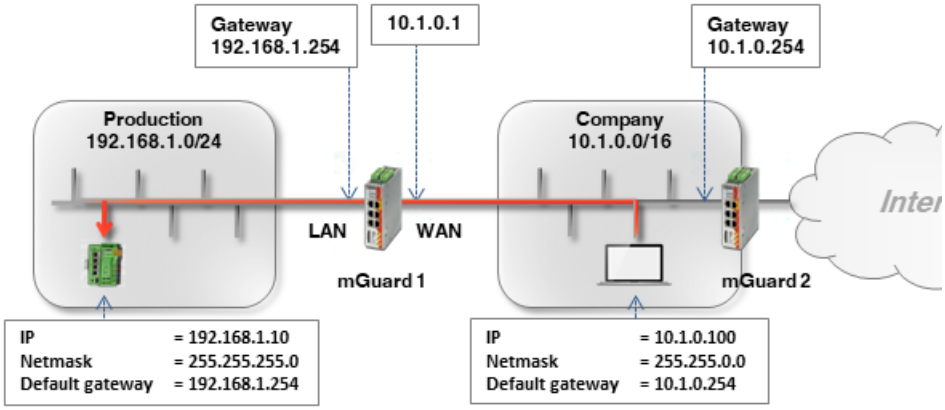


Figure 1-1 Client and mGuard router network settings

The two networks can be connected in various ways:

– Option 1: additional internal routes
– Option 2: IP and port forwarding
– Option 3: Network Address Translation (1:1 NAT)

1.1.2 Procedure

1. Configure the WAN and LAN interface of the router (*mGuard 1*)
2. Configure firewall rules
3. Configure network settings in accordance with option 1, 2, or 3

1.2 mGuard router network settings

To enable network traffic between the two networks, the external interface (= WAN port) and the internal interface (= LAN port) of the *mGuard 1* router must be configured in all options and assigned at least one IP address.

Ensure that the clients in the production and company network are configured in accordance with their network.

The internal IP address of *mGuard 1* must be configured as the default gateway (192.168.1.254) for clients in the production network (PLCs).

The internal IP address of *mGuard 2* must be configured as the default gateway (10.1.0.254) for clients in the company network.

To install *mGuard 1* as the router between the company network (WAN) 10.1.0.0/16 and the production network (LAN) 192.168.1.0.0/24, proceed as follows:

1. Log in to the *mGuard 1* web interface (192.168.1.254).
2. Go to **Network >> Interfaces**.
3. *General* tab: select the **network mode** *Router* and the **router mode** *Static*.
4. *Internal* tab: select 192.168.1.254 as the internal IP address (netmask 255.255.255.0).
5. *External* tab: select 10.1.0.1 as the external IP address (netmask 255.255.0.0).

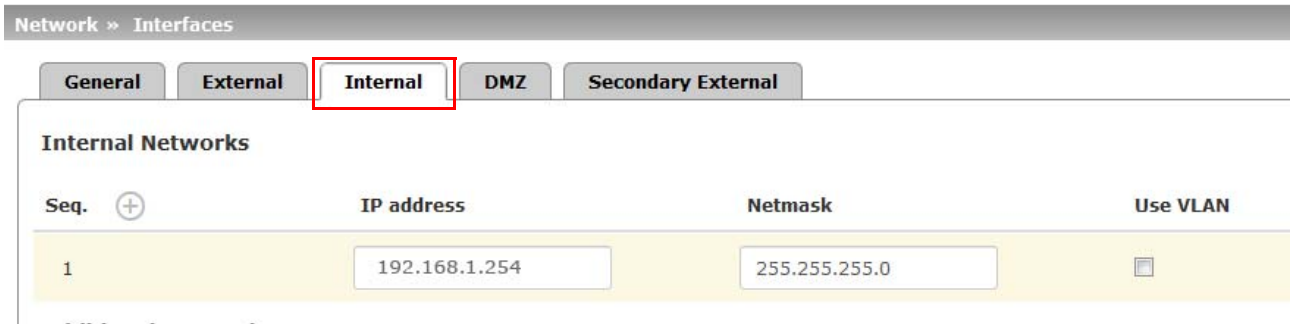


Figure 1-2 Internal interface

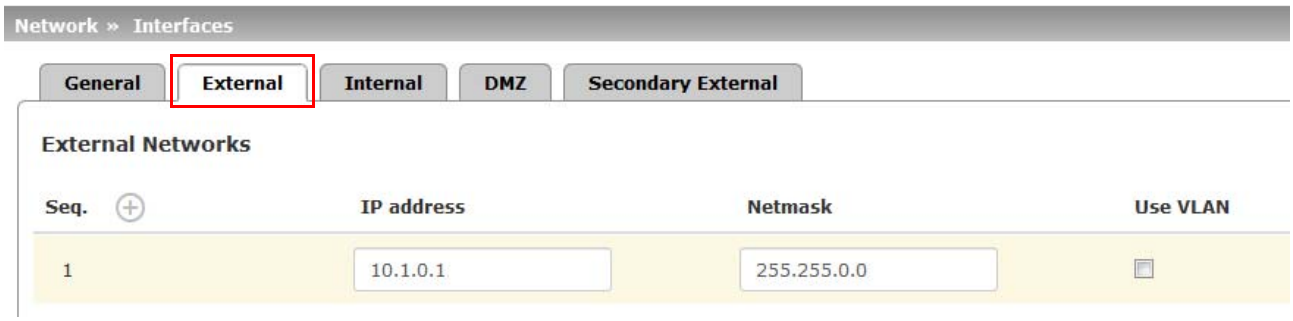


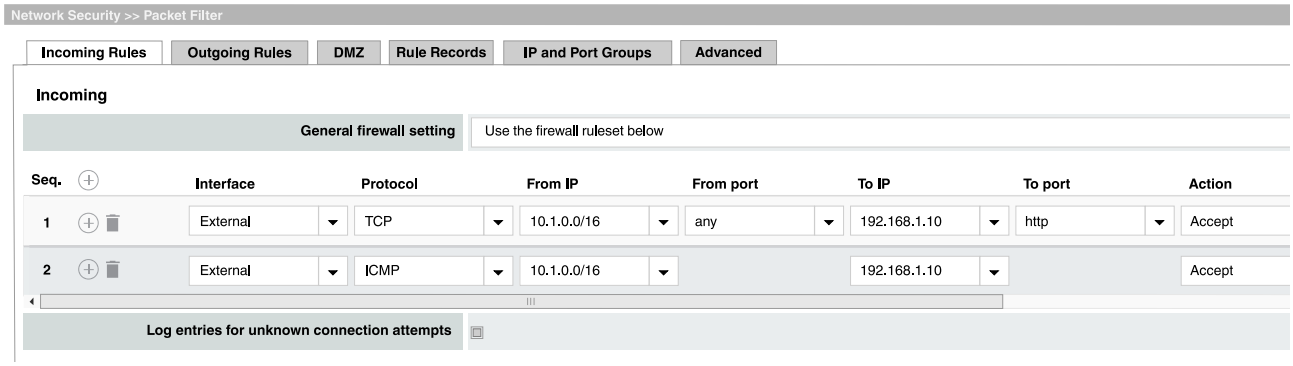
Figure 1-3 External interface

1.3 Configuring firewall rules

mGuard 1 is to be configured to allow the HTTP access to the web interface of the PLC (192.168.1.10) from the company network (= external network: 10.1.0.0/16). In addition, it should also be possible to "*ping*" the controller (ICMP request).

Proceed as follows:

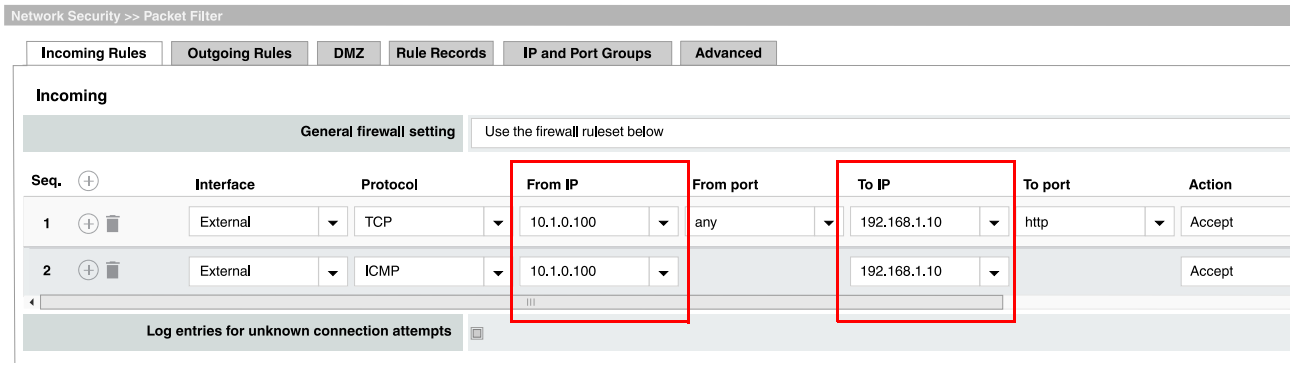
1. Log in to the *mGuard 1* web interface (192.168.1.254).
2. Go to **Network Security >> Packet Filter >> Incoming Rules**.
3. Select "*Use the firewall ruleset below*" under **General firewall setting**.
4. Create two firewall rules as follows:



Result

The firewall rules allow incoming TCP packets to the HTTP port and incoming ICMP packets from the company network to the IP address of the PCL. All other packets are rejected by the firewall.

As an option, the **From IP** and **To IP** fields can also be used to limit access to certain clients (e.g. from **10.1.0.100** to **192.168.1.10**).



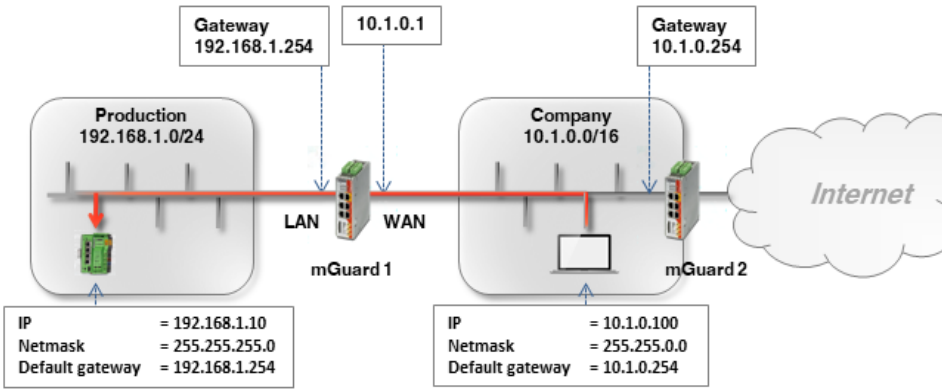
1.4 Network settings in accordance with option 1, 2, and 3

1.4.1 Option 1: additional internal routes on the gateway

The PLC (192.168.1.10) and the office computer (10.1.0.100) are not in the same network. The office computer sends packets intended for the PLC to its default gateway (*mGuard 2*: 10.1.0.254).

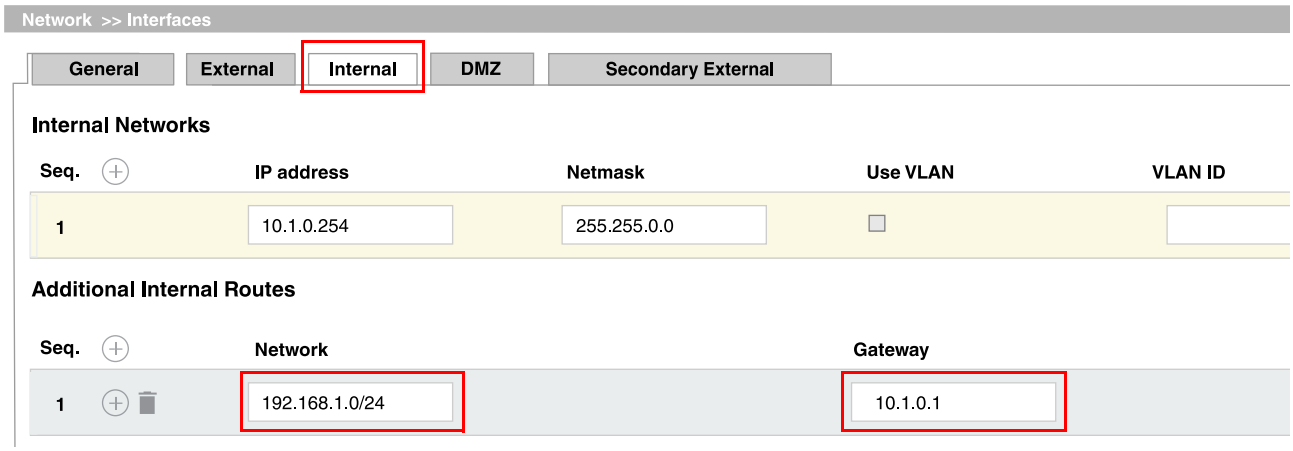
This gateway now needs to know where it should forward the packet to. This is specified by adding additional internal routes:

An additional route must be configured on the default gateway (*mGuard 2*: 10.1.0.254) of the office computer. This route specifies *mGuard 1* (10.1.0.1) as gateway and the production network (192.168.1.0.0/24) as destination network. *mGuard 1* acts as the router that connects the two networks.



If the default gateway in the company network is an mGuard device (in this case *mGuard 2*), proceed as follows:

1. Log into the default gateway web interface (*mGuard 2*) in the company network (LAN interface at 10.1.0.254).
2. Go to **Network >> Interfaces >> Internal**.
3. Create an **additional internal route** to the production network (network: 192.168.1.0/24 via gateway 10.1.0.1):



4. Clients in the company network send packets intended for the network 192.168.1.0/24 via their standard gateway (*mGuard 2*) to *mGuard 1*.

Result

Clients in the company network can now reach the PLC in the production network via its real IP address:

– Web browser: http://192.168.1.10
– Ping: 192.168.1.10

Advantages

– The PLC can be reached directly via its real IP address.
– There is no need to change the network configuration of the office computer and other clients in the company network.

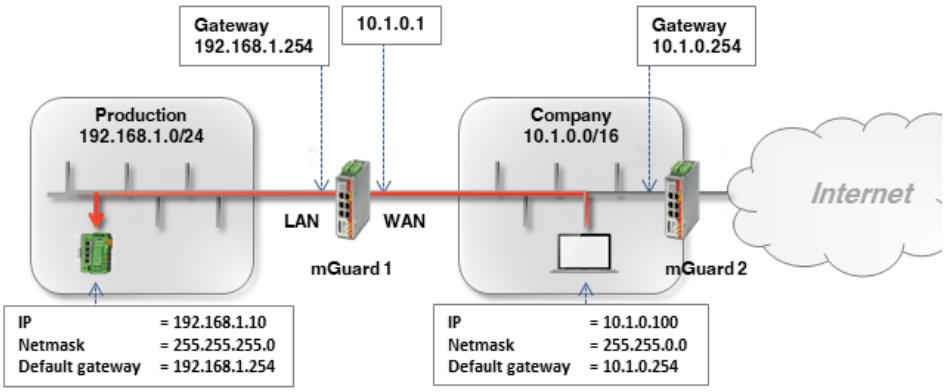
Disadvantages

– Additional routes have to be configured on the gateway.

1.4.2 Option 2: IP and port forwarding

With IP and port forwarding, the IP address and port number is in the header of the incoming data packets is rewritten so that the data packets sent to the external IP address of *mGuard 1* are forwarded to a chosen IP address and/or port number in the internal network.

The PLC (192.168.1.10) is not in the same network as the requesting office computer (10.1.0.100).



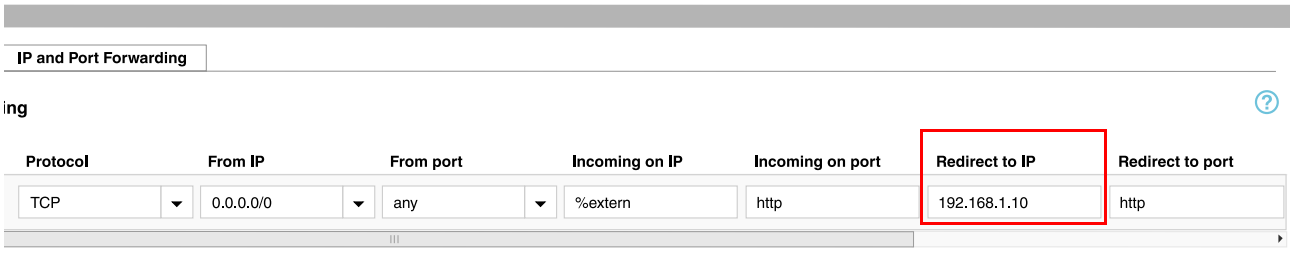
Network packets sent from the company network (WAN) to *mGuard 1* that are intended for its external IP address are rewritten so that they are forwarded to the IP address of the PLC in the production network (LAN). Along with the IP address, the port to which the packet is addressed can also be rewritten with a chosen port.

IP and port forwarding can only be used for the network protocols TCP, UDP and GRE. ICMP is not supported. A *ping* to the PLC is therefore not possible with this option.

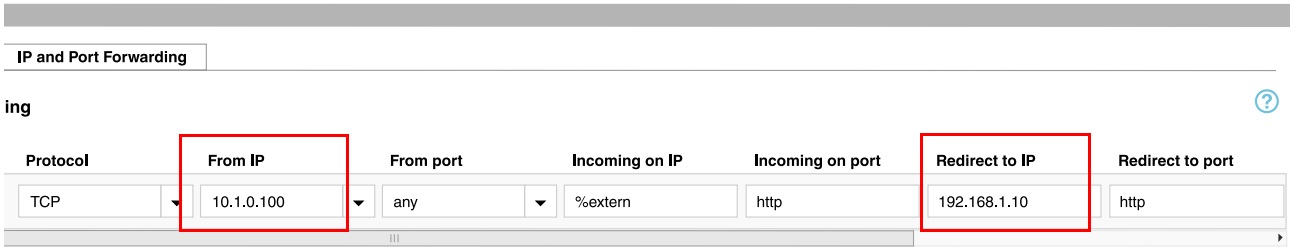
NOTE: If a rule for IP and port forwarding applies to a packet, it is immediately forwarded to the specified destination. Any existing firewall rules that have been configured via **Network Security >> Packet Filter** are not taken into consideration.

Proceed as follows:

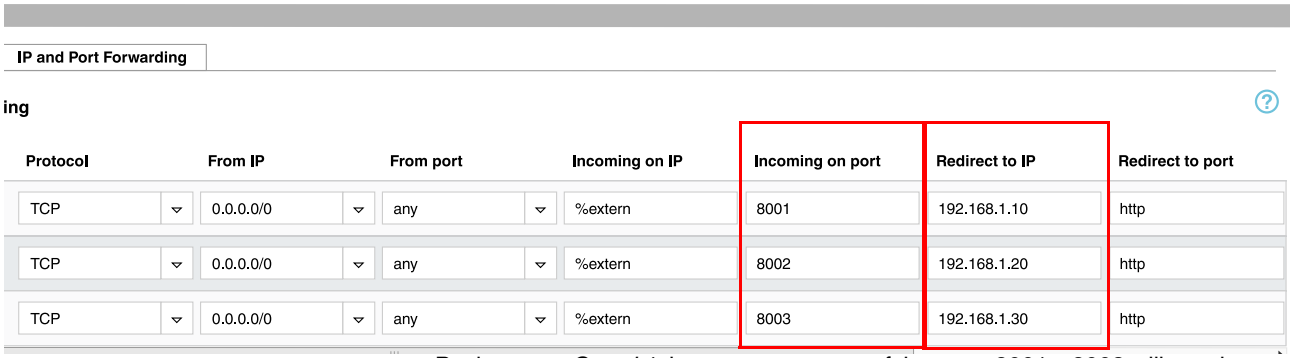
1. Log in to the *mGuard 1* web interface (LAN interface at 192.168.1.254).
2. Go to **Network >> NAT >> IP and Port Forwarding**.
3. Create a rule with the following configuration:



4. **Optional**:
   – With the *From IP* and *From port* fields, the rule can be restricted to certain sender addresses (e.g. a particular computer in the company network: 10.1.0.100) or networks, as well as to certain ports.



– The external IP address of the mGuard can also be specified in the field *Incoming on IP*.
  If the variable **%extern** is used when several static IP addresses are used for the WAN interface, this entry only applies to the first IP address on the list.
  The variable **%extern** is to be used if the mGuard IP address can be changed dynamically so that a particular external IP address cannot be specified.
– In our example, only requests to port 80 (*http*) are forwarded to the destination address and the destination port.
– In order to be able to reach several clients in the destination network using IP and port forwarding, the following configuration can be used:



Packets at *mGuard 1* that are sent to one of the ports 8001 – 8003 will now be forwarded to port 80 (*http*) of the corresponding IP addresses (e.g. 192.168.1.10).

Result

All or (optional) only certain clients in the company network can reach the PLC in the production network via the following IP address:

– Web browser: http://10.1.0.1 (= mGuard device)
– *Ping*: Not possible.

Advantages

– Easy to configure for a small number of destinations.

Disadvantages

– Only port-based protocols (UPD/TCP) can be forwarded (*ping* not possible).
– The destination client (PLC) is accessed via the external IP address of the mGuard device and not via its real IP address.

– If several clients (machine controllers) in the production network are to be reached via the same port, a type of mapping table must be maintained in order to know which port is to be used to access a particular client (e.g. http://10.1.0.1:8001 for 192.168.1.10 or http://10.1.0.1:8002 for 192.168.1.20). This can easily lead to confusion.

For further information, also refer to mGuard firmware user manual.

1.4.3 Option 3: 1:1 NAT

With 1:1 NAT, a **real network** (e.g. the internal production network) is mapped to a **virtual network** via the mGuard. (In our example, the virtual network is part of the external company network.)

The mGuard thus assigns IP addresses of the real network to specific IP addresses of the virtual network. If packets are sent to these virtual IP addresses, mGuard forwards these to the real IP addresses.

Depending on the application, the real and virtual networks can be LAN, WAN or DMZ networks.

Depending on the subnet mask specified in the 1:1 NAT configuration, the subnets of the **real network** can also be mapped in the **virtual network**.

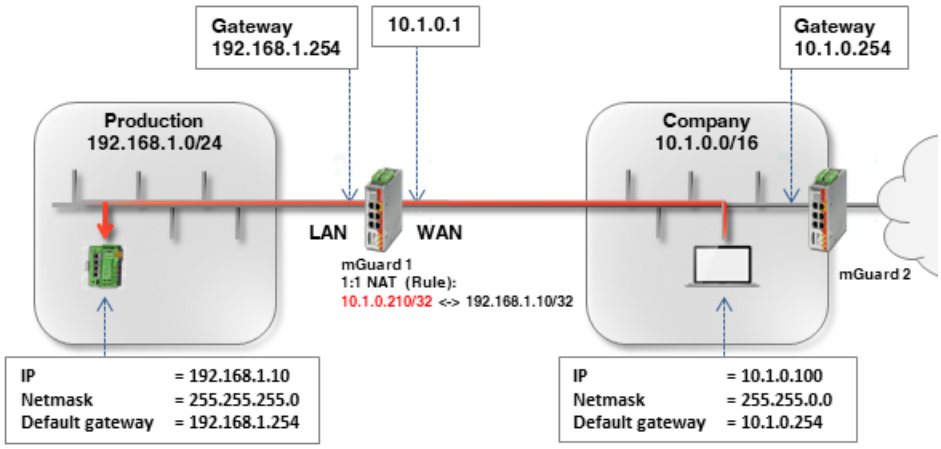
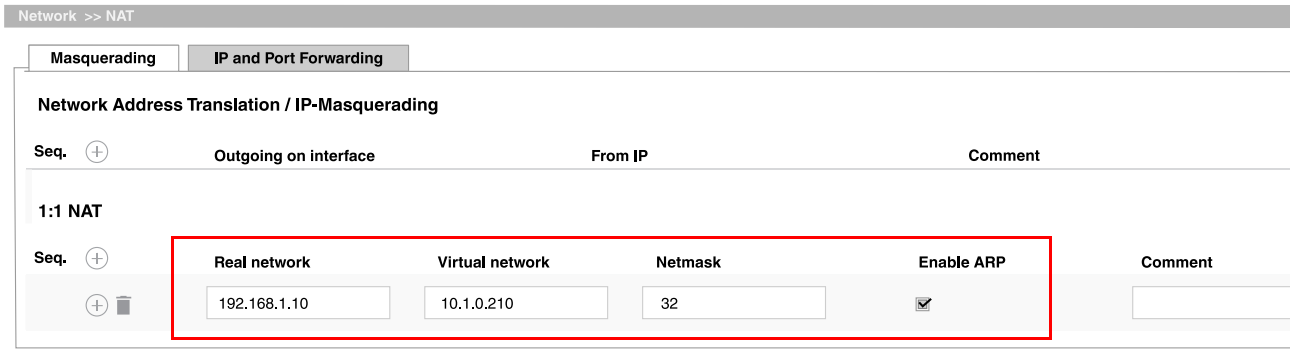


Table 1-1 Examples of rules for 1:1 NAT with different netmasks and the resulting assignments

Real network	Virtual network	Netmask	Assigned IP addresses
192.168.1.10	10.1.0.210	**32**	192.168.1.10 <-> 10.1.0.210

To make the PLC accessible to all clients in the company network, proceed as follows:

1. Log in to the *mGuard 1* web interface (LAN interface at 192.168.1.254).
2. Go to **Network >> NAT >> Masquerading**.
3. In the section 1:1 NAT, create a rule with the following configuration:



4. Packets that are sent to the IP address 10.1.0.210 in the company network are now forwarded to the IP address 192.168.1.10.

NOTE: The IP addresses specified in *Virtual network* must be free. They may not be assigned to other devices or used in any way, because otherwise an IP-address conflict would occur in the *Virtual network*. This even applies when no device exists in the *Real network* for one or more IP addresses from the specified *Virtual network*.

The PLC can now be accessed from the company network via the following IP address:

– Web browser: http://10.1.0.210
– Ping: 10.1.0.210

Advantages

– No changes in the production network are necessary.
– Each client in the production network can be accessed via a *virtual* IP address of the company network.
– The PLC can be accessed via protocols and ports in accordance with the rules specified for the incoming firewall.
– The integration of further network segments (e.g. different production units) into the company network is also possible using an mGuard device in each of the segments to be integrated. Some or all of these networks can use the same internal network settings (e.g. 192.168.1.0.0/24).

  Broadly speaking: if, for example, the (virtual) external network has a subnet mask of 16 and the systems in this network only use IP addresses in the range 10.1.0.1 – 10.1.0.254, the networks 10.1.1.0/24, 10.1.2.0/24, 10.1.3.0/24 can be used to map the (real) internal networks to IP addresses of the (virtual) external network.

Disadvantages

A sufficient number of unused virtual network IP addresses is necessary to be able to perform the mapping.