1 Accessing external networks (IP masquerading | 1:1 NAT)

Document ID: 108408_en_01
Document designation: AH EN MGUARD NETWORK SEGMENT 2
© PHOENIX CONTACT 2019-03-04

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 external network is to be reached from the internal network.

The following procedures are described:

– Option 1: NAT masking (IP masquerading)
– Option 2: 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.

A server in the company network is to be accessed from the production network.

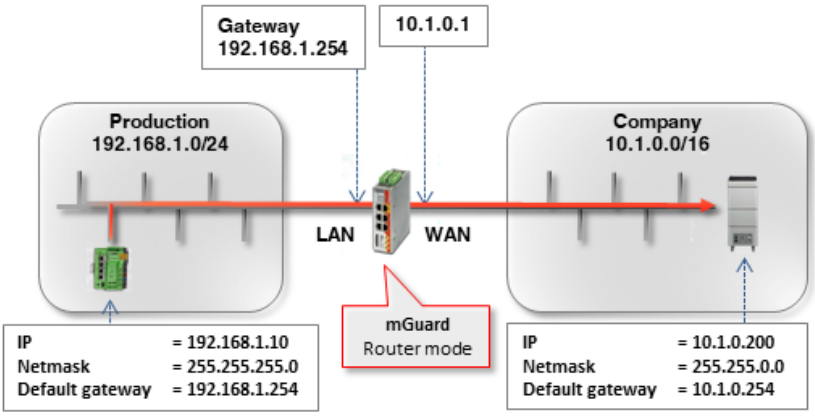


Figure 1-1 Client and mGuard router network settings

The two networks can be connected in various ways:

– Option 1: **Masking / IP masquerading**
– Option 2: **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 or 2

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 production network (LAN) 192.168.1.0/24, 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.
5. *External* tab: select 10.1.0.1 as the external IP address.

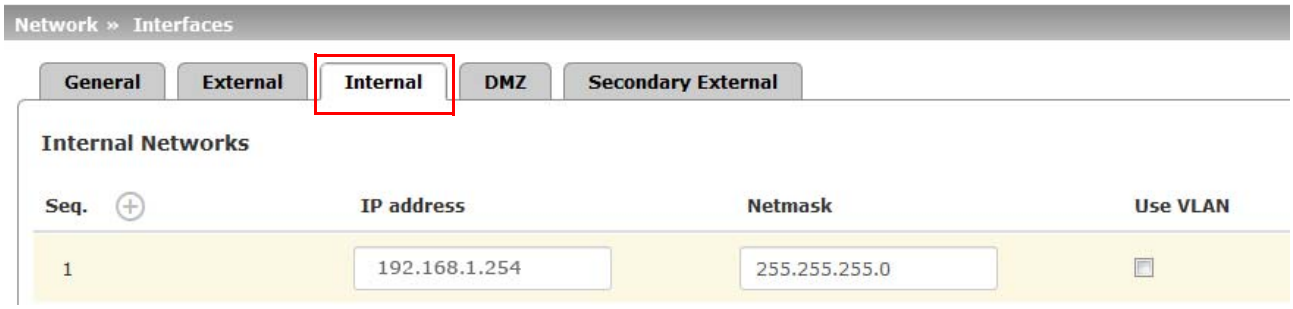


Figure 1-2 Internal interface

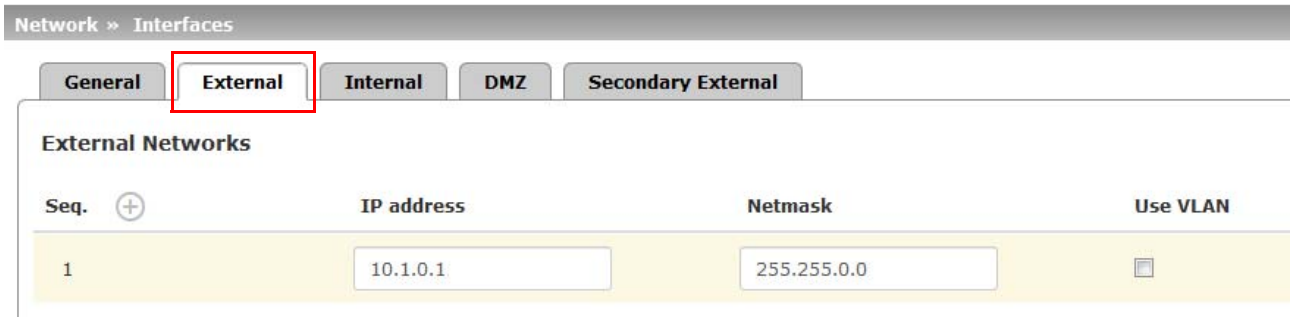


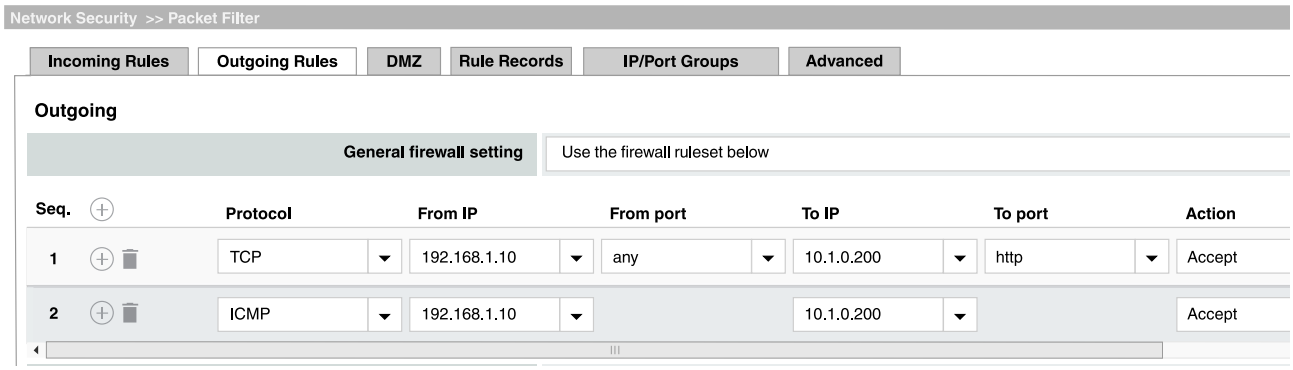
Figure 1-3 External interface

1.3 Configure firewall rules

mGuard 1 is to be configured so as only to allow a particular client from the production network (192.168.1.10) to access the web server (10.1.0.200) in the company network. Apart from that, it should also be possible to "*ping*" the web server (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 >> Outgoing Rules**.
3. Select "*Use the firewall ruleset below*"under **General firewall setting.**
4. Create two firewall rules as follows:



Result

The firewall rules allow outgoing TCP packets to the HTTP port and outgoing ICMP packets. All other packets are rejected by the firewall. The fields **From IP** and **To IP** specify which IP address (server) can be accessed from which IP address (client).

1.4 Network settings in accordance with option 1 and 2

1.4.1 Option 1: masking / IP masquerading

The mGuard device masks the IP addresses of senders from the production network (= *internal network*) with its own external IP address.

This means that the mGuard replaces the IP address of the sender (192.168.1.10) in the data packets with its external IP address (10.1.0.1).

When the packets arrive at the destination server (10.1.0.200), the IP address of the sender (mGuard: 10.1.0.1) is in the same network, and the server sends the response back to the mGuard directly. The mGuard reverses the NAT changes and forwards the response to the original sender (192.168.1.10).

To make the server in the company network accessible to the client in the production network, proceed as follows:

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

4. **Optional**: You can also specify all IPs (0.0.0.0/0) in the *From IP* field if you want to enable IP masquerading for all clients in the production network. The access limitation must then be regulated via the firewall settings.

Result

The mGuard router replaces the IP address of packets sent from the client (192.168.1.10) in the production network to the IP address of the server in the company network (10.1.0.210) with its own external IP address and forwards them.

The server in the company network can be reached by the client via its real IP address:

– Web browser: http://10.1.0.200
– Ping: 10.1.0.200

Advantages

– No changes in the production network are necessary.
– Each client in the production network can reach all destinations in the company network via their real IP addresses.
– The destinations in the company network can be accessed via protocols and ports in accordance with the specified firewall rules (outgoing rules).

1.4.2 Option 2: 1:1 NAT

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

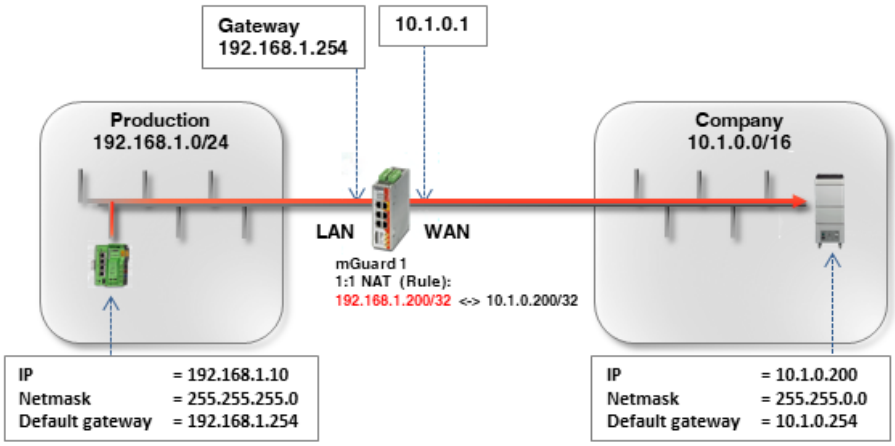
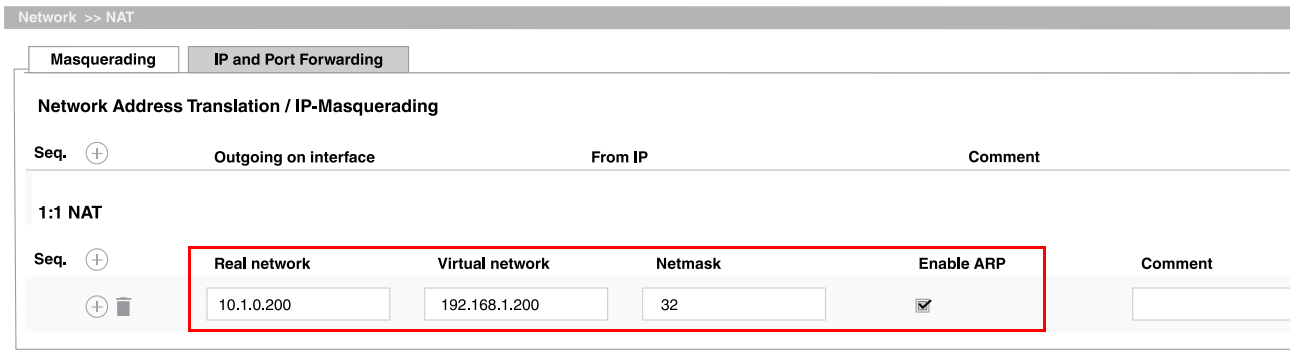


Table 1-1 Examples of rules for 1:1 NAT with different netmasks and the resulting assignments

Real network	Virtual network	Netmask	Assigned IP addresses
10.1.0.200	192.168.1.200	**32**	10.1.0.100 <-> 192.168.1.200

To make the server in the company network accessible to the client in the production network, proceed as follows:

1. Log in to the mGuard 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 192.168.1.200 in the production network are now forwarded to the IP address 10.1.0.200.

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 server in the company network can now be accessed via the following IP address:

– Web browser: http://192.168.1.200
– Ping: 192.168.1.200

Advantages

– No changes are necessary in the company network.
– Each client in the company network can be accessed via a *virtual* address of the production network.
– The destinations in the company network can be accessed via protocols and ports in accordance with the rules specified in the incoming firewall.

Disadvantages

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