1 Using network address translation (1:1 NAT)

Document ID: 108407_en_00
Document designation: AH EN MGUARD NAT

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 basic use of 1:1 NAT. A description of how to access two internal networks from an external network as well as how to access an external network from an internal network is provided.

1.1 Introduction

Using NAT (*Network Address Translation*), the address information in data packets is replaced with other address information or overwritten in order to be able to connect different networks together.

mGuard devices support the NAT procedures: *IP masquerading* and *1:1 NAT*. Use of NAT in VPN connections is also possible (see Section 1).

IP masquerading

With *IP masquerading* enabled, the mGuard device masks the IP address of senders, e.g. from the production network (= *internal network*) with its own external IP address.

1:1 NAT

1:1 NAT maps the IP addresses of a *Real network* to IP addresses of a *Virtual network*. Devices in the *Real network* can therefore be accessed directly via their assigned (*mapped*) IP addresses from the *Virtual network*.

Depending on the netmask specified in the 1:1 NAT configuration, the entire *Real network* or corresponding subnets can be mapped to the *Virtual network*.

1.2 Important information on the use of NAT

1:1 NAT is not supported in the *Stealth* network mode.

The IP addresses specified under "*Virtual network*" must be free. They must not be assigned to other devices, because an IP address conflict would otherwise occur in the *"Virtual network"*. This is even the case if a device corresponding to an IP address in the specified "*Virtual network*" does not exist at all in the "*Real network*".

With 1:1 NAT, the *network part* of an IP address is rewritten (*mapped*) and the *host part* usually remains unchanged. The network part of the IP address is prescribed by the specified netmask.

The same netmask that is used by the *Virtual network* must not be used at the same time to map the *Real network* to the virtual location. In this case, the mGuard would respond to all ARP requests from the *Virtual network*, therefore rendering it unusable.

The specified netmask must be smaller than that used by the *Virtual network*.

If access is to be limited, corresponding firewall rules must be created.

1.3 Example 1: Mapping IP addresses (1:1 NAT)

1.3.1 Individual devices in the production network are to be accessed from the company network

Individual devices in two production networks (with the same network settings) are to be accessible from the company network via 1:1 NAT.

To do this, the *real* IP address of a client in the production network is rewritten (*mapped)* as a *virtual* IP address in the company network. The assigned client in the production network can be accessed directly via this *virtual* IP address.

(If access is to be limited, corresponding firewall rules must be created.)

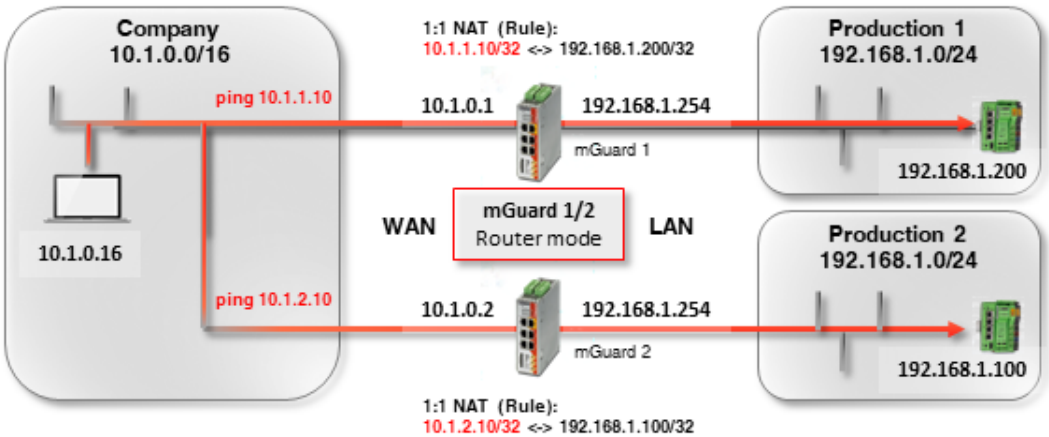

Figure 1-1 1:1 NAT rule: accessing individual IP addresses in the production network from the company network

The ARP *daemon* on the mGuard device will respond to ARP requests sent to the assigned IP addresses in the *Virtual network*. No IP changes may therefore be made in the *Virtual network*.

Table 1-1 Example rules for 1:1 NAT with the netmask 32 (IP address mapping)

Real network	Virtual network	Netmask	Assigned IP addresses
192.168.1.200	10.1.1.10	**32**	192.168.1.200 <-> 10.1.1.10

1.3.2 mGuard device settings

To allow access to devices in the production network from the company network using 1:1 NAT, proceed as follows:

1. Log into the *mGuard 1* web interface.
2. Go to **Network >> NAT**.
3. Configure the 1:1 NAT rules in accordance with Figure 1-2.

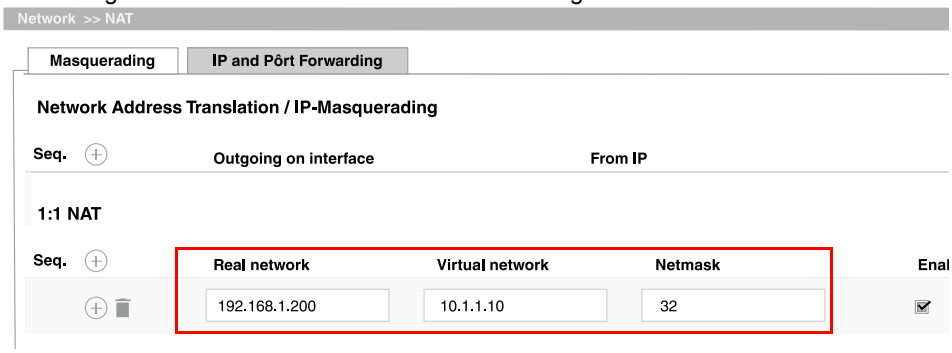

Figure 1-2 *mGuard 1*: Accessing production 1 (IP addresses)

1. Log in to the *mGuard 2* web interface.
2. Go to **Network >> NAT**.
3. Configure the 1:1 NAT rules in accordance with Figure 1-4.

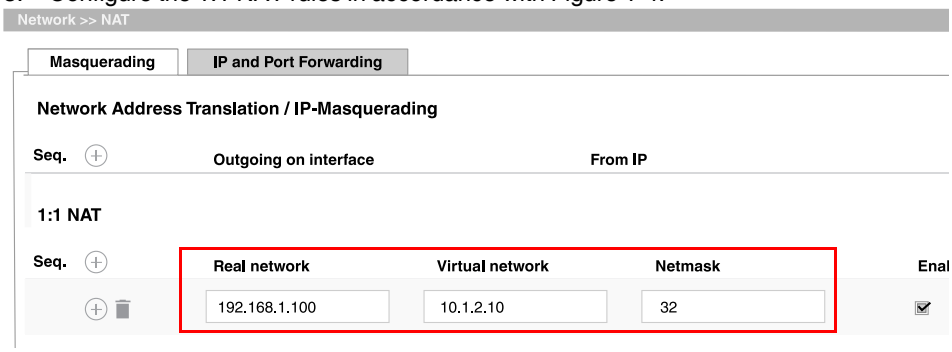

Figure 1-3 *mGuard 2*: Accessing production 2 (IP addresses)

Result

Network packets sent from the company network to the *virtual* IP address 10.1.1.10 are forwarded to the *real* IP address 192.168.1.200 in the production network 1.

Network packets from the company network to the *virtual* IP address 10.1.2.10 are forwarded to the *real* IP address 192.168.1.100 in the production network 1 via mGuard 2.

1.4 Example 2: Mapping networks (1:1 NAT)

1.4.1 The entire production network is to be accessed from the company network

Two production networks with the same network settings are the be accessed from the company network via 1:1 NAT.

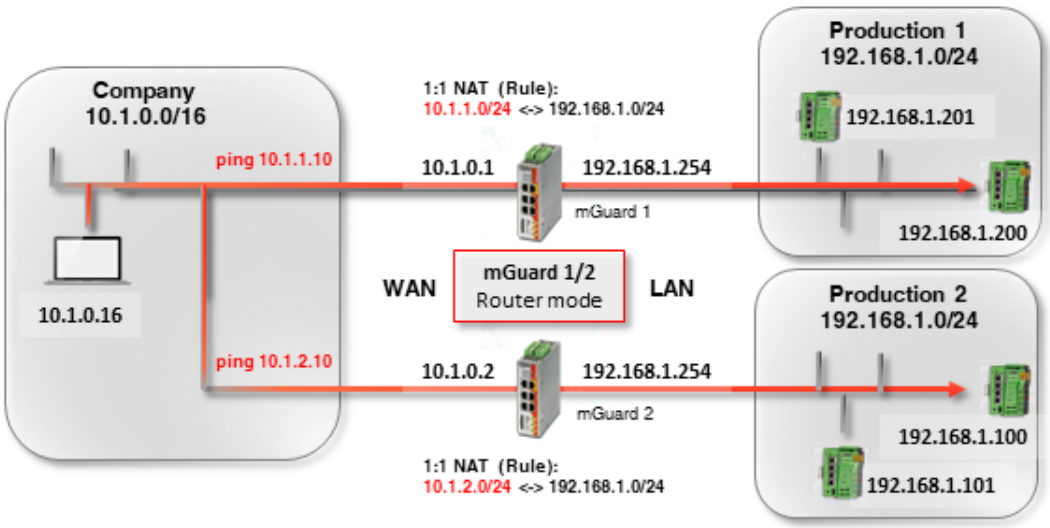

Figure 1-4 1:1 NAT rule: Accessing the entire production network from the company network

The two mGuard devices have external IP addresses that belong to the external company network (10.1.0.1 and 10.1.0.2).

Systems of **production location 1** are to be accessed from the company network via the *Virtual* network **10.1.1.0/24** and systems of **production location 2** are to be accessed via the *Virtual* network **10.1.2.0/24** using 1:1 NAT.

Real clients in the company network may not use an IP address from the *virtual* networks.

Table 1-2 Examples of rules for 1:1 NAT with different netmasks and resulting assignments

Real network	Virtual network	Netmask	Assigned IP addresses
192.168.1.0	10.1.0.0	**24**	192.168.1.0 <-> 10.1.0.0 192.168.1.1 <-> 10.1.0.1 … 192.168.1.254 <-> 10.1.0.254 192.168.1.255 <-> 10.1.0.255

The respective ARP daemon on the two mGuard routers ensure that clients in the external network know where to send packets addressed to the networks 10.1.1.0/24 and 10.1.2.0/24.

1.4.2 mGuard device settings

To make the production network accessible from the company network using 1:1 NAT, proceed as follows:

1. Log into the *mGuard 1* web interface.
2. Go to **Network >> NAT**.
3. Configure the 1:1 NAT rules in accordance with Figure 1-5.

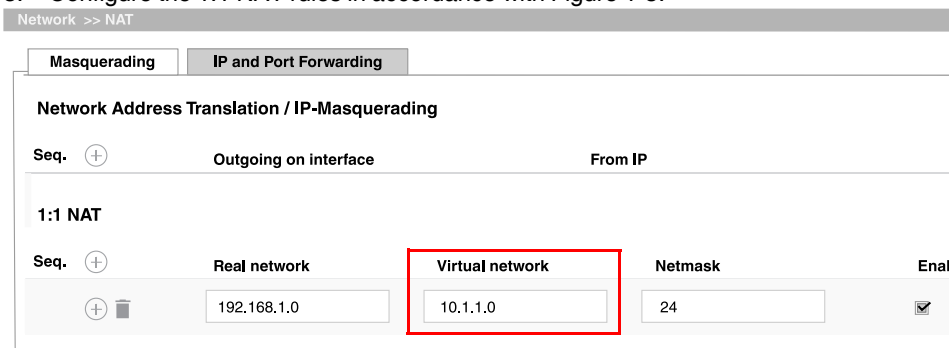

Figure 1-5 *mGuard 1*: Accessing production 1 (networks)

1. Log in to the *mGuard 2* web interface.
2. Go to **Network >> NAT**.
3. Configure the 1:1 NAT rules in accordance with Figure 1-6.

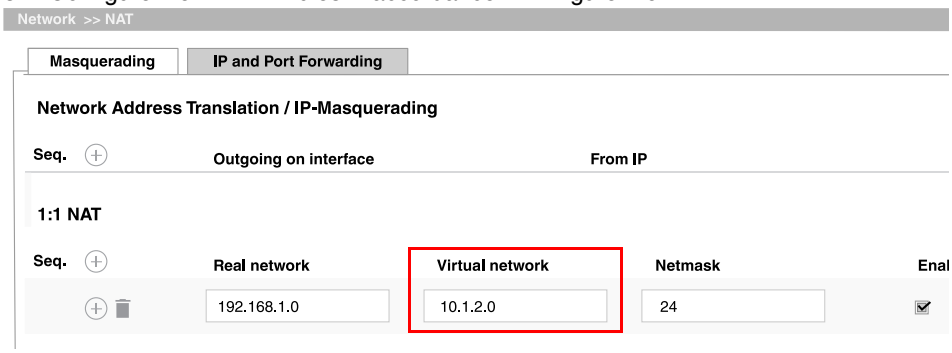

Figure 1-6 *mGuard 2*: Accessing production 2 (networks)

Result

The client 192.168.1.200 in production location 1 can be accessed from the external network via the IP address 10.1.1.200. Client 192.168.1.201 can be accessed via 10.1.1.201.

The client 192.168.1.10 in production location 2 can be accessed via the IP address 10.1.2.10 from the external network; the client 192.168.1.11 can be accessed via the IP address 10.1.2.11, etc.

Clients in production location 2 can in principle also be accessed from production location 1 via their *virtual* IP addresses (10.1.2.0/24), and vice versa.