1 Interne Netzwerke erreichen (Zusätzliche Routen | IP-/Port-Weiterleitung | 1:1-NAT)

Dokument-ID: 108406_de_00

Dokument-Bezeichnung: AH DE MGUARD NETWORK SEGMENT 1

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Dokument wird die Verwendung des mGuard-Geräts als Router beschrieben, der zwei Netzwerke (internes und externes Netzwerk) miteinander verbindet. Das interne Netzwerk soll aus dem externen erreicht werden.

Beschrieben werden die folgenden Verfahren:

– Option 1: Zusätzliche interne Routen
– Option 2: IP- und Port-Weiterleitung
– Option 3: Network Address Translation (1:1-NAT)

1.1 Einleitung

Im Netzwerkmodus „Router“ (*Router-Modus*) kann ein mGuard-Gerät dazu eingesetzt werden, zwei Netzwerke miteinander zu verbinden. Die Sicherheitsfunktionen Firewall und VPN (lizenzabhängig) stehen dabei ebenfalls zur Verfügung.

Bei einigen Modellen kann optional eine Demilitarisierte Zone (DMZ) über das zusätzliche DMZ-Interface angebunden werden.

1.1.1 Beispiel

Das Produktionsnetzwerk (= *Internes Netzwerk*) und das Unternehmensnetzwerk (= *Externes Netzwerk*) sind über einen mGuard-Router miteinander verbunden.

Aus dem Unternehmensnetzwerk soll auf das Web-Interface einer Maschinensteuerung (SPS) im Produktionsnetzwerk zugegriffen werden. Eine Ping-Anfrage an die Steuerung soll ebenfalls von dieser beantwortet werden.

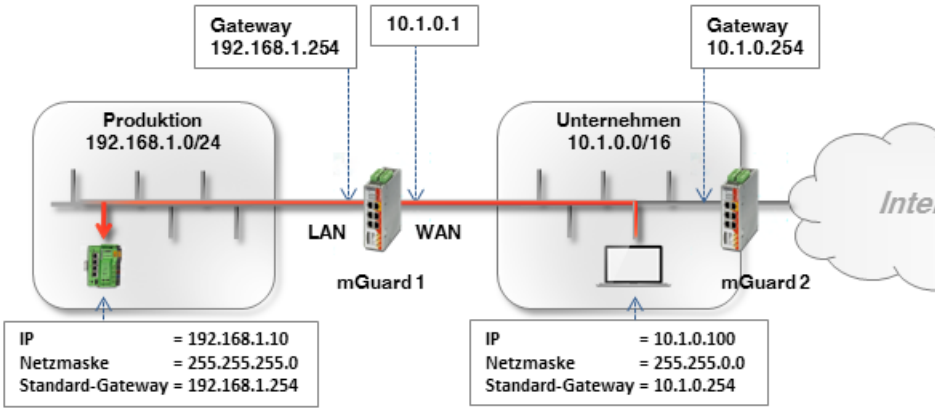


Bild 1-1 Netzwerkeinstellungen der Clients und mGuard-Router

Das Ziel, die beiden Netzwerke miteinander zu verbinden, kann auf unterschiedlichen Wegen erreicht werden:

– Option 1: Zusätzliche interne Routen
– Option 2: IP- und Port-Weiterleitung
– Option 3: Network Address Translation (1:1-NAT)

1.1.2 Vorgehen

1. WAN- und LAN-Interface des Routers (*mGuard 1*) konfigurieren
2. Firewall-Regeln konfigurieren
3. Netzwerkeinstellungen gemäß Option 1, 2 oder 3 konfigurieren

1.2 Netzwerkeinstellungen des mGuard-Routers

Um den Netzwerkverkehr zwischen den beiden Netzwerken zu ermöglichen, müssen in allen Optionen das externe (= WAN-Port) und das internes Interface (= LAN-Port) des Routers *mGuard 1* konfiguriert und mit mindestens einer IP-Adresse versehen werden.

Stellen Sie sicher, dass die Clients im Produktions- und Unternehmensnetzwerk ihrem Netzwerk entsprechend konfiguriert sind.

Die Clients im Produktionsnetzwerk (SPS) müssen als Standard-Gateway die interne IP-Adresse des *mGuard 1* konfiguriert haben (192.168.1.254).

Die Clients im Unternehmensnetzwerk müssen als Standard-Gateway die interne IP-Adresse des *mGuard 2* konfiguriert haben (10.1.0.254).

Um *mGuard 1* als Router zwischen dem Unternehmensnetzwerk (WAN)10.1.0.0/16 und dem Produktionsnetzwerk (LAN) 192.168.1.0.0/24 einzusetzen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an (192.168.1.254).
2. Gehen Sie zu **Netzwerk >> Interfaces**.
3. Registerkarte *Allgemein*: Wählen Sie den **Netzwerk-Modus** *Router* und den **Router-Modus** *Statisch*.
4. Registerkarte *Intern*: Wählen Sie als Interne IP-Adresse 192.168.1.254 (Netzmaske 255.255.255.0).
5. Registerkarte *Extern*: Wählen Sie als Externe IP-Adresse 10.1.0.1 (Netzmaske 255.255.0.0).

Bild 1-2 Internes Interface

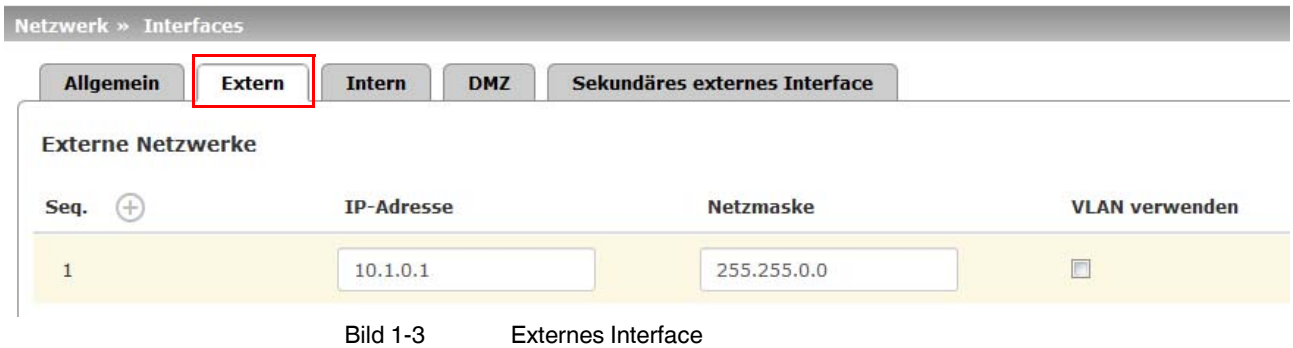


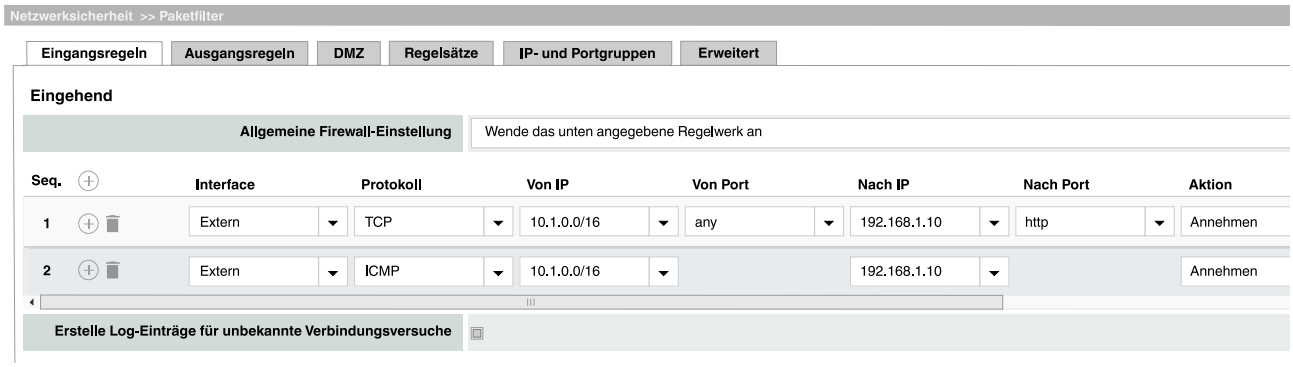
Bild 1-3 Externes Interface

1.3 Firewall-Regeln konfigurieren

mGuard 1 soll so konfiguriert werden, dass er den HTTP-Zugriff auf das Webinterface der SPS (192.168.1.10) aus dem Unternehmensnetzwerk (= Externes Netzwerk: 10.1.0.0/16) ermöglicht. Abgesehen davon soll es auch möglich sein, die Steuerung zu "*pingen*" (ICMP-Anfrage).

Gehen Sie wie folgt vor:

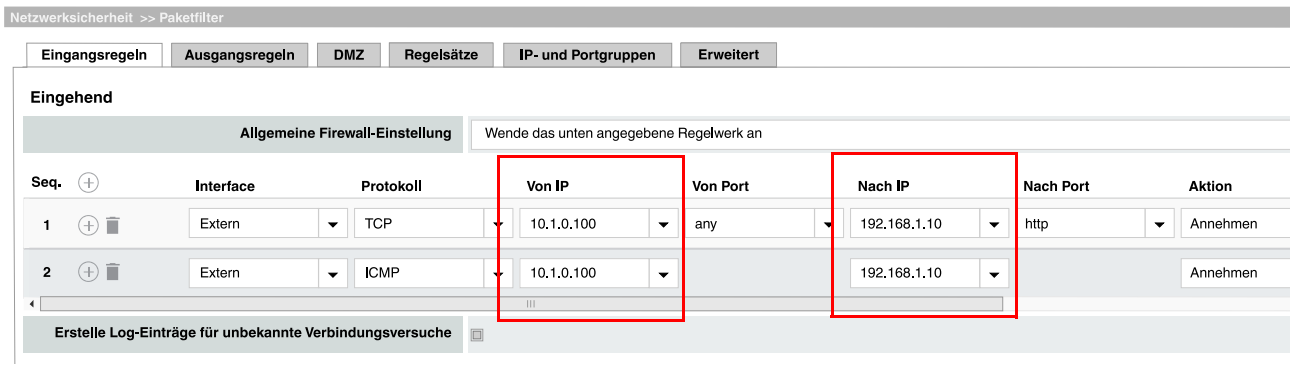
1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an (192.168.1.254).
2. Gehen Sie zu **Netzwerksicherheit >> Paketfilter >> Eingangsregeln**.
3. Wählen Sie bei **Allgemeine Firewall-Einstellung** „*Wende das unten angegebene Regelwerk an*“.
4. Legen Sie zwei Firewall-Regeln wie folgt an:



Ergebnis

Die Firewall-Regeln erlauben eingehende TCP-Pakete an den HTTP-Port sowie eingehende ICMP-Pakete aus dem Unternehmensnetzwerk an die IP-Adresse der SPS. Alle anderen Pakete werden von der Firewall verworfen.

Die Felder **Von IP** und **Nach IP** können auch dazu verwendet werden, die Erlaubnis auf einzelne Clients zu beschränken (z. B. von **10.1.0.100** auf **192.168.1.10**).



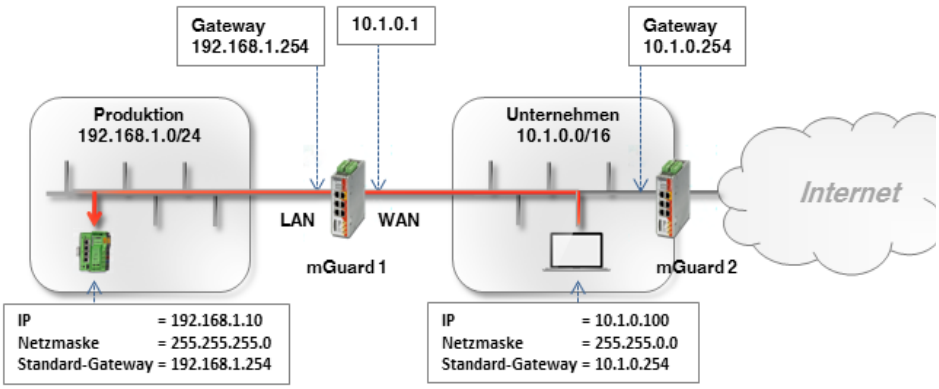
1.4 Netzwerkeinstellungen gemäß Option 1, 2 und 3

1.4.1 Option 1: Zusätzliche interne Routen auf dem Gateway

Der Büro-Computer (10.1.0.100) und die SPS (192.168.1.10) befinden sich nicht im gleichen Netzwerk. Der Büro-Computer sendet Pakete, die an die SPS gerichtet sind, grundsätzlich an sein Standard-Gateway (*mGuard 2*: 10.1.0.254).

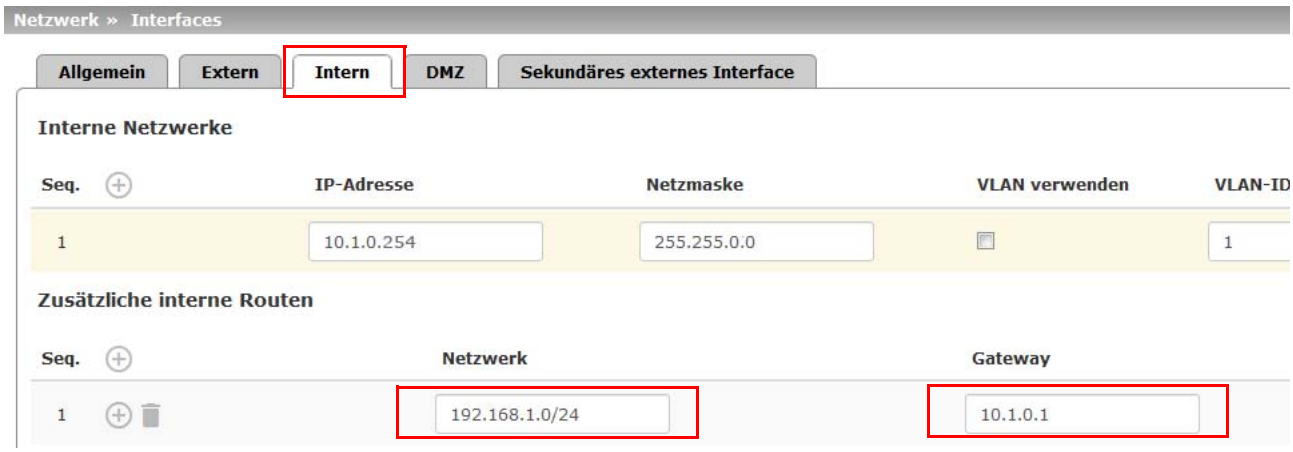
Dieses Gateway muss nun wissen, wohin es die Pakete weiterleiten soll. Das erfolgt über das Hinzufügen von zusätzlichen internen Routen:

Auf dem Standard-Gateway (10.1.0.254) des Büro-Computers muss eine zusätzliche Route konfiguriert werden, die *mGuard 1* (10.1.0.1) als Gateway und das Produktionsnetzwerk (192.168.1.0/24) als Zielnetzwerk angibt. *mGuard 1* fungiert als Router, der die beiden Netzwerke miteinander verbindet.



Wenn das Standard-Gateway im Unternehmensnetzwerk ein mGuard-Gerät (hier *mGuard 2*) ist, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des Standard-Gateways (*mGuard 2*) im Unternehmensnetzwerk an (LAN-Interface unter 10.1.0.254).
2. Gehen Sie zu **Netzwerk >> Interfaces >> Intern**.
3. Legen Sie eine **Zusätzliche Interne Route** zum Produktionsnetzwerk an (Netzwerk: 192.168.1.0/24 über Gateway 10.1.0.1):



4. Clients im Unternehmensnetzwerk (z. B. der Büro-Computer) senden Pakete, die an das Netzwerk 192.168.1.0/24 gerichtet sind, über das Standard-Gateway (*mGuard 2*) an *mGuard 1*

Ergebnis

Clients aus dem Unternehmensnetzwerk können nun die SPS im Produktionsnetzwerk über ihre reale IP-Adresse erreichen:

– Webbrowser: http://192.168.1.10
– Ping: 192.168.1.10

Vorteile

– Die SPS kann direkt über ihre reale IP-Adresse erreicht werden.
– Die Netzwerkkonfiguration des Büro-Computers und anderer Clients im Unternehmensnetzwerk muss nicht geändert werden.

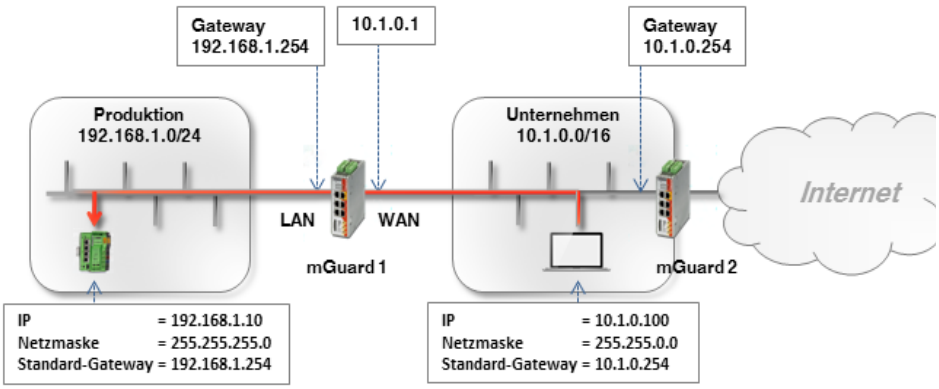
Nachteile

– Auf dem Gateway müssen zusätzliche Routen konfiguriert werden.

1.4.2 Option 2: IP- und Port-Weiterleitung

Bei der IP- und Port-Weiterleitung wird die IP-Adresse und Port-Nummer im Header eingehender Datenpakete so umgeschrieben, dass Datenpakete an die externe IP-Adresse von *mGuard 1* an eine beliebige IP-Adresse und/oder Port-Nummer im internen Netzwerk weitergeleitet werden.

Die SPS (192.168.1.10) befindet sich nicht in dem Netzwerk, in dem sich der anfragende Büro-Computer befindet (10.1.0.100).



Netzwerkpakete an *mGuard 1* aus dem Unternehmensnetzwerk (WAN), die an seine externe IP-Adresse gerichtet sind, werden so umgeschrieben, dass sie an die IP-Adresse der SPS im Produktionsnetzwerk (LAN) weitergeleitet werden. Neben der IP-Adresse kann der Port, an den das Paket adressiert ist, ebenfalls in einen beliebigen Port umgeschrieben werden.

IP- und Port-Weiterleitung kann nur für die Netzwerkprotokolle TCP, UDP und GRE angewendet werden. ICMP wird nicht unterstützt. Ein *Ping* auf die SPS ist daher mit dieser Option nicht möglich.

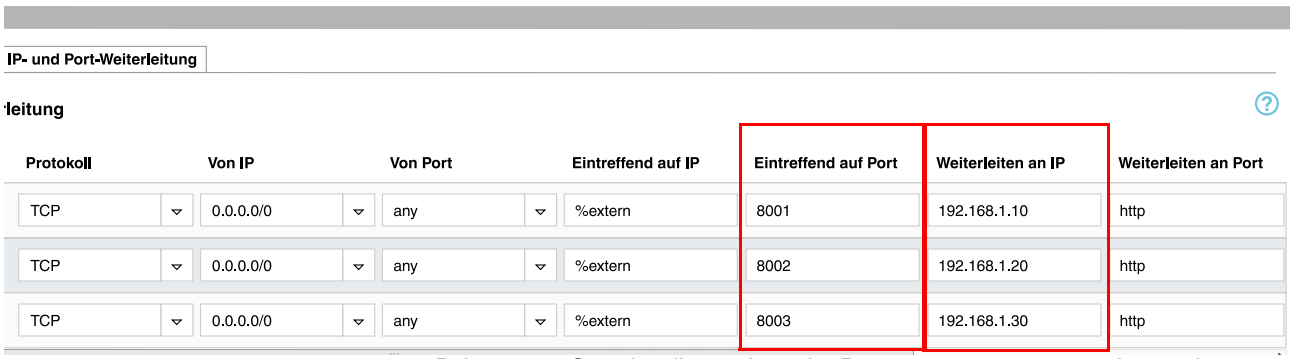
ACHTUNG: Trifft eine Regel zur IP- und Portweiterleitung auf ein Paket zu, wird dieses sofort an das angegebene Ziel weitergeleitet. Eventuell vorhandene Firewall-Regeln, die unter **Netzwerksicherheit >> Paketfilter** konfiguriert wurden, werden nicht mehr berücksichtigt.

Gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des *mGuard 1* an (LAN-Interface unter 192.168.1.254).
2. Gehen Sie zu **Netzwerk >> NAT >> IP- und Port-Weiterleitung**.
3. Legen Sie eine Regel mit folgender Konfiguration an:

4. **Optional**:
   – Mit den Angaben *Von IP* und *Von Port* kann die Regel auf bestimmte Absenderadressen (z. B. ein bestimmter Rechner im Unternehmensnetzwerk: 10.1.0.100) oder Netzwerke sowie bestimmte Ports beschränkt werden.

   – Im Feld *Eintreffend auf IP* könnte auch die externe IP-Adresse des mGuards angegeben werden.
     Wird die Variable **%extern** bei der Verwendung von mehreren statischen IP-Adressen für die WAN-Schnittstelle verwendet, bezieht sich die Angabe nur auf die erste IP-Adresse der Liste.
     Die Variable **%extern** muss verwendet werden, wenn ein dynamischer Wechsel der externen IP-Adresse des mGuards erfolgen kann, so dass eine bestimmte externe IP-Adresse nicht angegeben werden kann.
   – In unserem Beispiel werden nur Anfragen an Port 80 (*http*) an die Zieladresse und den Zielport weitergeleitet.
   – Um mithilfe von IP- und Port-Weiterleitung mehrere Clients im Zielnetzwerk zu erreichen, könnte die folgende Konfiguration verwendet werden:



   Pakete an *mGuard 1*, die an einen der Ports. 8001 – 8003 gesendet werden, werden nun an Port 80 (*http*) der jeweils entsprechenden IP-Adressen (z. B. 192.168.1.10) weitergeleitet.

Ergebnis

Alle oder (optional) nur bestimmte Clients aus dem Unternehmensnetzwerk können die SPS im Produktionsnetzwerk über die folgende IP-Adresse erreichen:

– Webbrowser: http://10.1.0.1 (= mGuard-Gerät)
– *Ping*: nicht möglich!

Vorteile

– Einfach zu konfigurieren für eine kleine Anzahl von Zielen.

Nachteile

– Nur Port-basierte Protokolle (UDP/TCP) können weitergeleitet werden (kein *Ping*).

- Der Zugriff auf den Ziel-Client (SPS) erfolgt über die externe IP des mGuard-Geräts und nicht über seine reale IP-Adresse
- Wenn mehrere Clients (Maschinensteuerungen) im Produktionsnetzwerk auf dem gleichen Port erreicht werden sollen, muss eine Art Mapping-Tabelle gepflegt werden, um zu wissen, welcher Port für den Zugriff auf einen bestimmten Client verwendet werden muss (z. B. http://10.1.0.1:8001 für 192.168.1.10 oder http://10.1.0.1:8002 für 192.168.1.20). Dies kann leicht zur Verwirrung führen.

Für mehr Informationen siehe auch mGuard-Firmwarehandbuch.

1.4.3 Option 3: 1:1-NAT

Bei 1:1-NAT wird ein **Reales Netzwerk** (z. B. das internen Produktionsnetzwerk) durch den mGuard in einem **Virtuellen Netzwerk** abgebildet. (Das virtuelle Netzwerk ist in unserem Beispiel ein Teil des externen Unternehmensnetzwerks.)

Der mGuard ordnet also IP-Adressen des Realen Netzwerks bestimmten IP-Adressen des Virtuellen Netzwerks zu. Werden Pakete an diese virtuellen IP-Adressen gesendet, leitet der mGuard diese an die realen IP-Adressen weiter.

Bei den realen und virtuellen Netzwerken kann es sich je nach Anwendungsfall um LAN-, WAN- oder DMZ-Netzwerke handeln.

Abhängig von der angegebenen Subnetzmaske in der 1:1 NAT-Konfiguration können auch Subnetze des **Realen Netzwerks** im **Virtuellen Netzwerk** abgebildet werden.

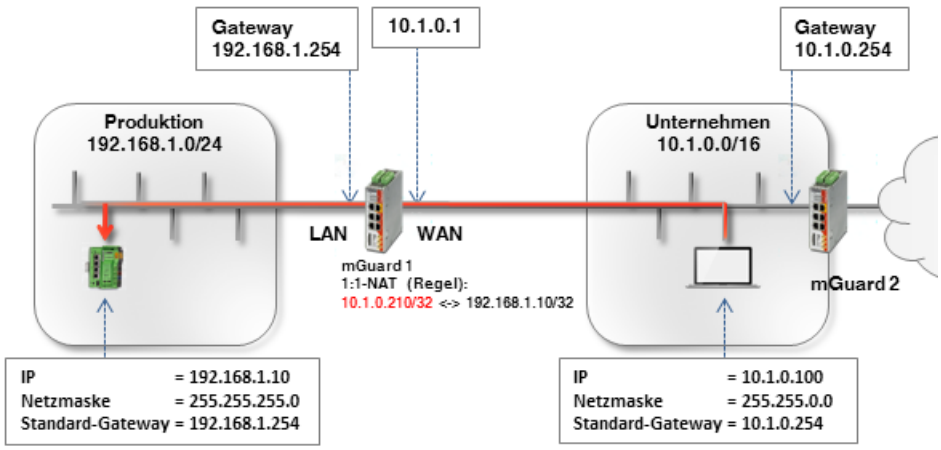
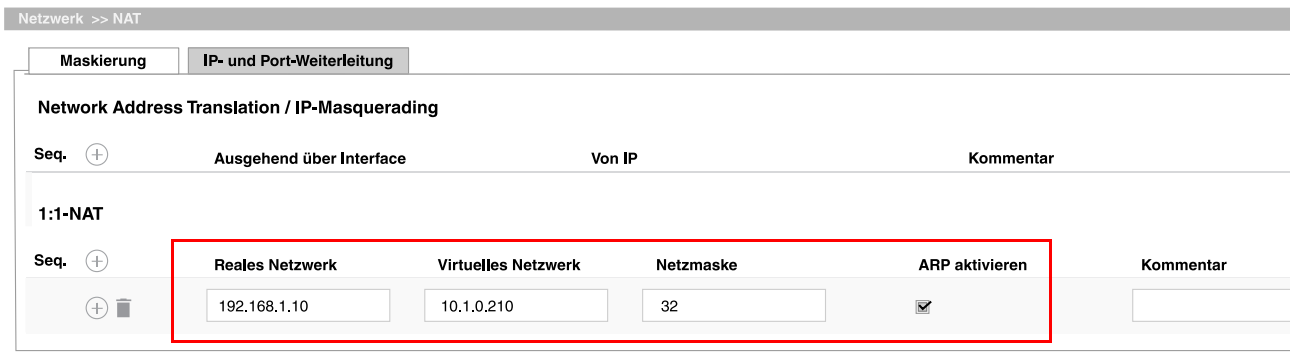


Tabelle 1-1 Beispiel-Regeln für 1:1-NAT mit unterschiedlichen Netzmasken und resultierende Zuordnungen

Reales Netzwerk	Virtuelles Netzwerk	Netzmaske	Zugeordnete IP-Adressen
192.168.1.10	10.1.0.210	**32**	192.168.1.10 <-> 10.1.0.210

Um die SPS für alle Clients im Unternehmensnetzwerk erreichbar zu machen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des *mGuard 1* an (LAN-Interface unter 192.168.1.254).
2. Gehen Sie zu **Netzwerk >> NAT >> Maskierung**.
3. Legen Sie in der Sektion 1:1-NAT eine Regel mit folgender Konfiguration an:



4. Pakete, die im Unternehmensnetzwerk an die IP-Adresse 10.1.0.210 gesendet werden, werden nun an IP-Adresse 192.168.1.10 weitergeleitet.

ACHTUNG: Die unter *Virtuelles Netzwerk* angegebenen IP-Adressen müssen frei sein. Sie dürfen nicht für andere Geräte vergeben oder gar in Benutzung sein, weil sonst im virtuellen Netzwerk ein IP-Adressenkonflikt entsteht. Dies gilt selbst dann, wenn zu einer oder mehreren IP-Adressen aus dem angegebenen *Virtuellen Netzwerk* gar kein Gerät im *Realen Netzwerk* existiert.

Ergebnis

Die SPS kann aus dem Unternehmensnetzwerk über die folgende IP-Adresse erreicht werden:

– Webbrowser: http://10.1.0.210
– Ping: 10.1.0.210

Vorteile

– Im Produktionsnetzwerk müssen keine Änderungen vorgenommen werden.
– Jeder Client im Produktionsnetzwerk ist über eine *virtuelle* IP-Adresse des Unternehmensnetzwerks erreichbar.
– Der Zugriff auf die SPS kann über Protokolle und Ports gemäß den festgelegten Regeln der eingehenden Firewall erfolgen.
– Die Anbindung weiterer Netzwerk-Segmente (z. B. verschiedene Produktionseinheiten) an das Unternehmensnetzwerk, ist über jeweils eigene mGuard-Geräte möglich. Diese Netzwerke könnten teilweise oder alle die gleichen internen Netzwerkeinstellungen verwenden (z. B. 192.168.1.0.0/24).

  Allgemein formuliert: Wenn z. B. das (virtuelle) externe Netzwerk eine Subnetzmaske von 16 hat und die Systeme in diesem Netzwerk nur IP-Adressen aus dem Bereich 10.1.0.1 – 10.1.0.254 verwenden, können die Netzwerke 10.1.1.0/24, 10.1.2.0/24, 10.1.3.0/24 zur Abbildung der (realen) internen Netzwerke auf IP-Adressen des (virtuellen) externen Netzwerks verwendet werden.

Nachteile

Eine ausreichende Anzahl unbenutzter IP-Adressen aus dem virtuellen Netzwerk ist erforderlich, um das Mapping durchzuführen.