1 Externe Netzwerke erreichen (IP-Masquerading | 1:1-NAT)

Dokument-ID: 108408_de_01

Dokument-Bezeichnung: AH DE MGUARD NETWORK SEGMENT 2

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 externe Netzwerk soll aus dem internen erreicht werden.

Beschrieben werden die folgenden Verfahren:

– Option 1: NAT– Maskierung (IP-Masquerading)
– Option 2: NAT – 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 Produktionsnetzwerk soll auf einen Server im Unternehmensnetzwerk zugegriffen werden.

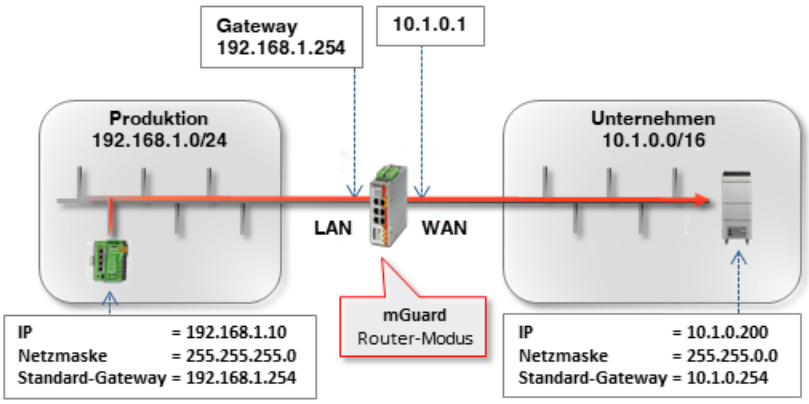


Bild 1-1 Netzwerkeinstellungen der Clients und mGuard-Router

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

– Option 1: **Maskierung / IP-Masquerading**
– Option 2: **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 oder 2 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) 192.168.1.0/24 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.
5. Registerkarte *Extern*: Wählen Sie als Externe IP-Adresse 10.1.0.1.

Bild 1-2 Internes Interface

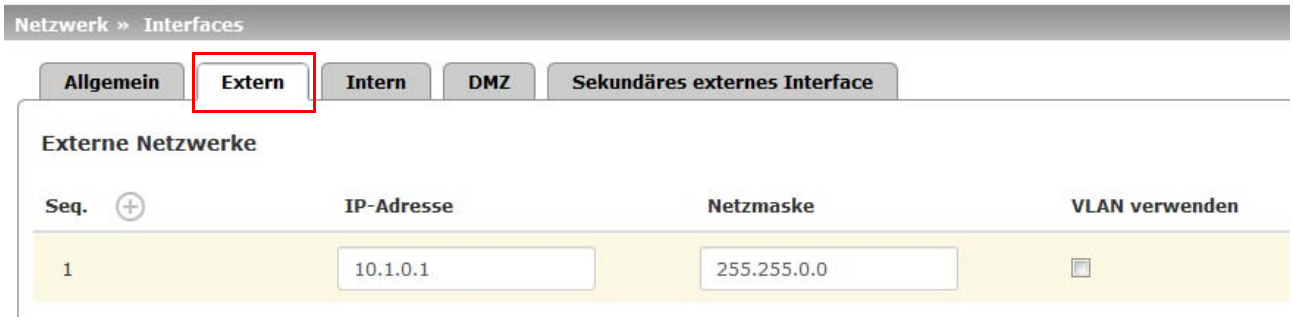


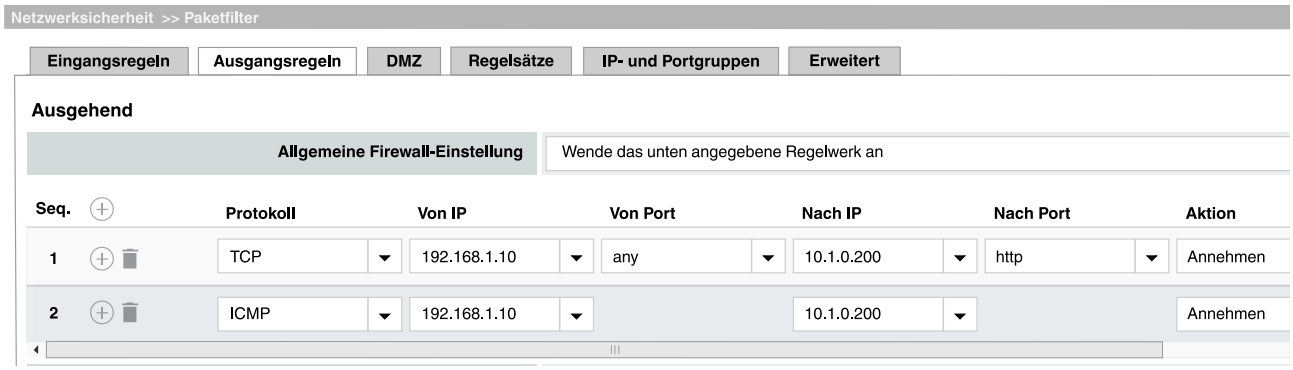
Bild 1-3 Externes Interface

1.3 Firewall-Regeln konfigurieren

mGuard 1 soll so konfiguriert werden, dass er ausschließlich den Zugriff eines bestimmten Clients aus dem Produktionsnetzwerk (192.168.1.10) auf den Webserver (10.1.0.200) im Unternehmensnetzwerk erlaubt. Abgesehen davon soll es auch möglich sein, den Webserver 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 >> Ausgangsregeln**.
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 ausgehende TCP-Pakete an den HTTP-Port sowie ausgehende ICMP-Pakete. Alle anderen Pakete werden von der Firewall verworfen. Die Felder **Von IP** und **Nach IP** geben an, von welcher IP-Adresse (Client) auf welche IP-Adresse (Server) zugegriffen werden kann.

1.4 Netzwerkeinstellungen gemäß Option 1 und 2

1.4.1 Option 1: Maskierung / IP-Masquerading

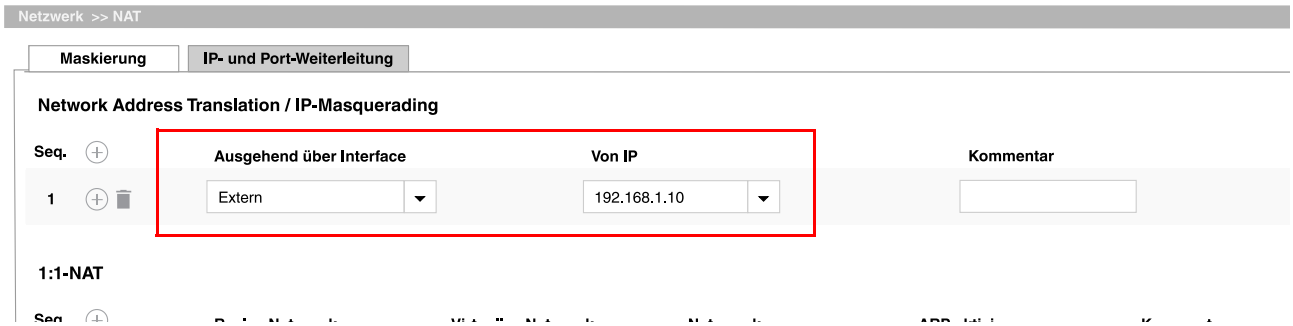
Das mGuard-Gerät maskiert die IP-Adressen von Absendern aus dem Produktionsnetzwerk (= *Internes Netzwerk*) mit seiner eigenen externen IP-Adresse.

Das heißt, der mGuard ersetzt in den Datenpaketen die IP-Adresse des Absenders (192.168.1.10) durch seine externe IP-Adresse (10.1.0.1).

Wenn die Pakete beim Ziel-Server (10.1.0.200) ankommen, befindet sich die IP-Adresse des Absenders (mGuard: 10.1.0.1) im selben Netzwerk und der Server sendet die Antwort direkt an den mGuard zurück. Der mGuard macht die NAT-Änderungen rückgängig und leitet die Antwort an den ursprünglichen Absender (192.168.1.10) weiter.

Um den Server im Unternehmensnetzwerk für den Client aus dem Produktionsnetzwerk erreichbar zu machen, gehen Sie wie folgt vor:

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



4. **Optional**: Sie können im Feld *Von IP* auch alle IPs angeben (0.0.0.0/0), wenn Sie allen Clients aus dem Produktionsnetzwerk IP-Masquerading ermöglichen wollen. Die Zugriffsbeschränkung müsste dann über die Firewall-Einstellungen geregelt werden.

Ergebnis

Pakete, die vom Client (192.168.1.10) im Produktionsnetzwerk an die IP-Adresse des Servers im Unternehmensnetzwerk (10.1.0.200) gesendet werden, werden vom mGuard-Router auf seine externe IP-Adresse umgeschrieben und weitergeleitet.

Der Server im Unternehmensnetzwerk kann von dem Client unter seiner realen IP-Adresse erreicht werden:

– Webbrowser: http://10.1.0.200
– Ping: 10.1.0.200

Vorteile

– Im Produktionsnetzwerk müssen keine Änderungen vorgenommen werden.
– Jeder Client im Produktionsnetzwerk kann alle Ziele im Unternehmensnetzwerk unter ihren realen IP-Adressen erreichen.
– Der Zugriff auf die Ziele im Unternehmensnetzwerk kann über Protokolle und Ports gemäß festgelegter Firewall-Regeln (Ausgangsregeln) erfolgen.

1.4.2 Option 2: 1:1-NAT

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

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 **Virtuelle Netzwerk** abgebildet werden.

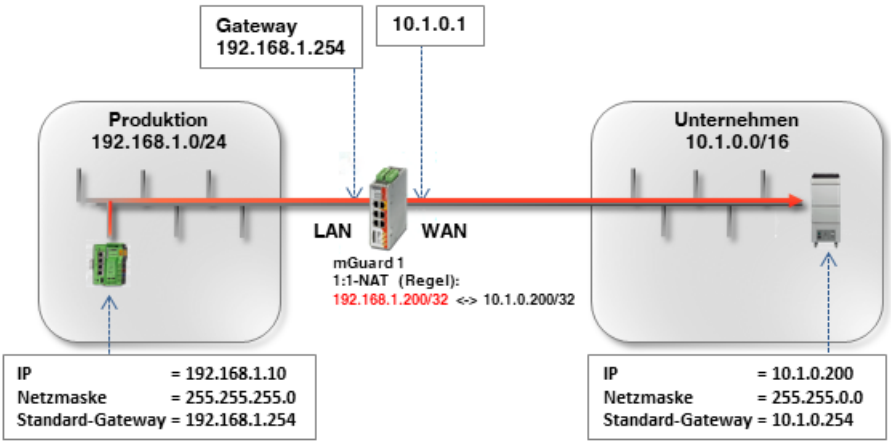
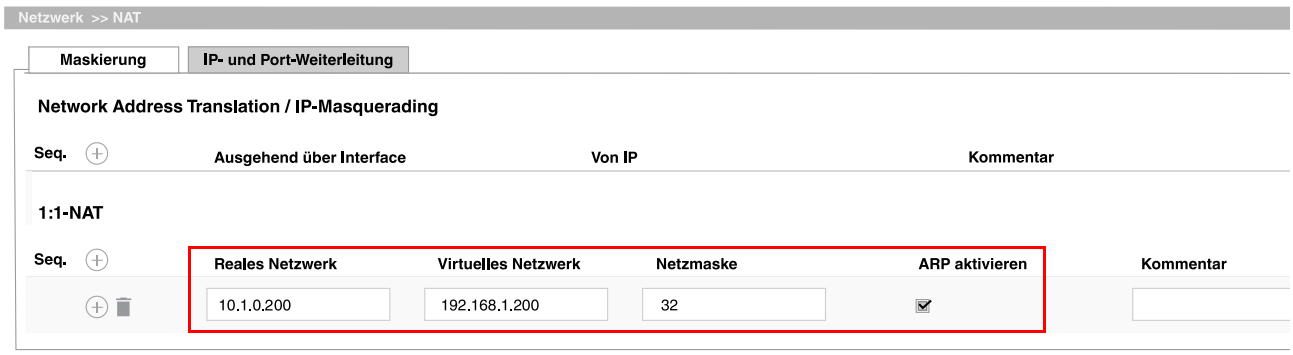


Tabelle 1-1 Beispiel-Regeln für 1:1-NAT mit unterschiedlichen Netzmasken und resultierende Zuordnungen

Reales Netzwerk	Virtuelles Netzwerk	Netzmaske	Zugeordnete IP-Adressen
10.1.0.200	192.168.1.200	**32**	10.1.0.200 <-> 192.168.1.200

Um den Server im Unternehmensnetzwerk für den Client aus dem Produktionsnetzwerk erreichbar zu machen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des mGuards 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 Produktionsnetzwerk an die IP-Adresse 192.168.1.200 gesendet werden, werden nun an IP-Adresse 10.1.0.200 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

Der Server im Unternehmensnetzwerk kann über die folgende IP-Adresse erreicht werden:

– Webbrowser: http://192.168.1.200
– Ping: 192.168.1.200

Vorteile

– Im Unternehmensnetzwerk müssen keine Änderungen vorgenommen werden.
– Jeder Client im Unternehmensnetzwerk ist über eine *virtuelle* IP-Adresse des Produktionsnetzwerks erreichbar.
– Der Zugriff auf die Ziele im Unternehmensnetzwerk kann über Protokolle und Ports gemäß den festgelegten Regeln der eingehenden Firewall erfolgen.

Nachteile

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