1 Network Address Translation (1:1-NAT) verwenden

Dokument-ID: 108407_de_00
Dokument-Bezeichnung: AH DE MGUARD NAT

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 grundsätzliche Verwendung von 1:1-NAT beschrieben. Der Zugriff aus einem externen Netzwerk auf zwei interne Netzwerke sowie der Zugriff aus einem internen auf ein externes Netzwerk werden beschrieben.

1.1 Einleitung

Mithilfe von NAT (*Network Address Translation*) werden die Adressinformationen in Datenpaketen durch andere ersetzt bzw. umgeschrieben, um verschiedene Netze miteinander zu verbinden.

mGuard-Geräte unterstützen die NAT-Verfahren *IP-Maskierung* und *1:1-NAT*. Die Verwendung von NAT in VPN-Verbindungen ist ebenfalls möglich (siehe Kapitel 1).

IP-Maskierung

Beim Aktivieren von IP-Maskierung (*IP-Masquerading*) maskiert das mGuard-Gerät die IP-Adressen von Absendern, z. B. aus dem Produktionsnetzwerk (= *Internes Netzwerk*), mit seiner eigenen externen IP-Adresse.

1:1-NAT

1:1-NAT bildet IP-Adressen eines *Realen Netzwerks* auf IP-Adressen eines *Virtuellen Netzwerks* ab. Geräte im *Realen Netzwerk* können somit direkt über die ihnen zugeordneten (*mapped*) IP-Adressen aus dem *Virtuellen Netzwerk* erreicht werden.

Abhängig von der angegebenen Netzmaske in der 1:1-NAT-Konfiguration können das gesamte *Reale Netzwerk* oder Subnetze davon auf das *Virtuelle Netzwerk* abgebildet werden.

1.2 Wichtige Hinweise zur Verwendung von NAT

1:1-NAT wird im Netzwerkmodus *Stealth* nicht unterstützt.

Die unter *„Virtuelles Netzwerk“* angegebenen IP-Adressen müssen frei sein. Sie dürfen nicht für andere Geräte vergeben sein, weil sonst im „*Virtuellen Netzwerk*“ ein IP-Adressenkonflikt entsteht. Dies gilt selbst dann, wenn zu einer IP-Adresse aus dem angegebenen „*Virtuellen Netzwerk*“ gar kein Gerät im „*Realen Netzwerk*" existiert.

Beim 1:1-NAT wird der *Netzwerk-Teil* einer IP-Adresse umgeschrieben (*mapped*) und der *Host-Teil* in der Regel unverändert beibehalten. Der Netzwerkteil der IP-Adresse wird durch die angegebene Netzmaske vorgegeben.

Die gleiche Netzmaske, die vom *Virtuellen Netzwerk* verwendet wird, darf nicht gleichzeitig zur Abbildung des *Realen Netzwerks* auf den virtuellen Standort verwendet werden. In diesem Fall würde der mGuard auf alle ARP-Anfragen des *Virtuellen Netzwerks* antworten und es damit unbenutzbar machen.

Die angegebene Netzmaske muss kleiner sein als diejenige, die vom *Virtuellen Netzwerk* verwendet wird.

Soll der Zugriff beschränkt werden, müssen entsprechende Firewall-Regeln erstellt werden.

1.3 Beispiel 1: Mapping von IP-Adressen (1:1-NAT)

1.3.1 Aus dem Unternehmensnetzwerk soll auf einzelne Geräte im Produktionsnetzwerk zugegriffen werden

Einzelne Geräte in zwei Produktionsnetzwerken (mit der gleichen Netzwerkeinstellung) sollen aus dem Unternehmensnetzwerk über 1:1-NAT erreichbar sein.

Die *reale* IP-Adresse eines Clients im Produktionsnetzwerk wird dazu auf eine *virtuelle* IP-Adresse im Unternehmensnetzwerk umgeschrieben (*gemappt*). Über diese *virtuelle* IP-Adresse kann direkt auf den zugeordneten Client im Produktionsnetzwerk zugegriffen werden.

(Soll der Zugriff beschränkt werden, müssen entsprechende Firewall-Regeln erstellt werden.)

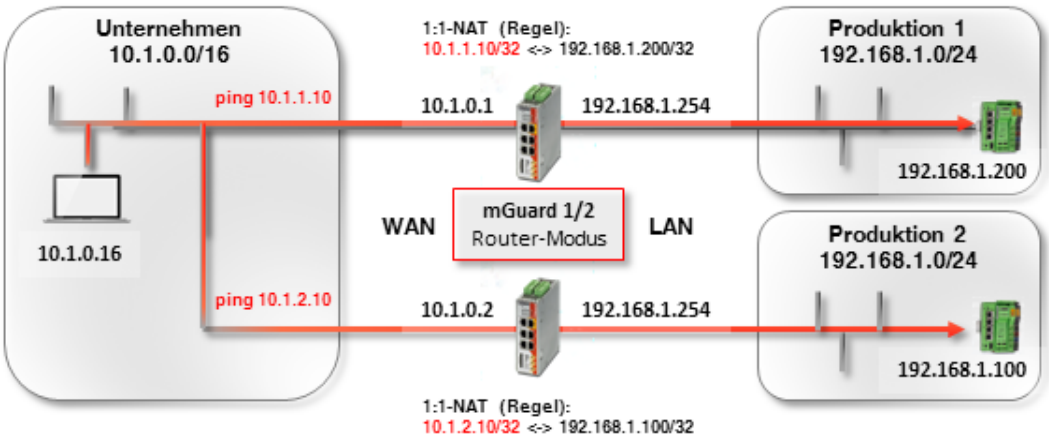

Bild 1-1 1:1-NAT-Regel: Aus dem Unternehmensnetzwerk auf einzelne IP-Adressen im Produktionsnetzwerk zugreifen

Der ARP-*Daemon* auf dem mGuard-Gerät wird auf ARP-Anfragen, die an die zugeordneten IP-Adressen des *Virtuellen Netzwerks* gerichtet sind, antworten. Daher müssen keine IP-Änderungen im *Virtuellen Netzwerk* vorgenommen werden.

Tabelle 1-1 Beispiel-Regeln für 1:1-NAT mit der Netzmasken 32 (Mapping von IP-Adressen)

Reales Netzwerk	Virtuelles Netzwerk	Netzmaske	Zugeordnete IP-Adressen
192.168.1.200	10.1.1.10	**32**	192.168.1.200 <-> 10.1.1.10

1.3.2 Einstellung auf dem mGuard-Gerät

Um Geräte in Produktionsnetzwerken aus dem Unternehmensnetzwerk mithilfe von 1:1-NAT erreichbar zu machen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an.
2. Gehen Sie zu **Netzwerk >> NAT**.
3. Konfigurieren Sie die 1:1-NAT-Regeln gemäß Bild 1-2.

Bild 1-2 *mGuard 1*: Produktion 1 erreichen (IP-Adressen)

1. Melden Sie sich auf der Weboberfläche von *mGuard 2* an.
2. Gehen Sie zu **Netzwerk >> NAT**.
3. Konfigurieren Sie die 1:1-NAT-Regeln gemäß Bild 1-4.

Bild 1-3 *mGuard 2*: Produktion 2 erreichen (IP-Adressen)

Ergebnis

Netzwerkpakte aus dem Unternehmensnetzwerk an die *virtuelle* IP-Adresse 10.1.1.10 werden über *mGuard 1* an die *reale* IP-Adresse 192.168.1.200 im Produktionsnetzwerk 1 geleitet.

Netzwerkpakte aus dem Unternehmensnetzwerk an die *virtuelle* IP-Adresse 10.1.2.10 werden über *mGuard 2* an die *reale* IP-Adresse 192.168.1.100 im Produktionsnetzwerk 2 geleitet.

1.4 Beispiel 2: Mapping von Netzwerken (1:1-NAT)

1.4.1 Aus dem Unternehmensnetzwerk soll auf das gesamte Produktionsnetzwerk zugegriffen werden

Zwei Produktionsnetzwerke mit der gleichen Netzwerkeinstellung sollen aus dem Unternehmensnetzwerk über 1:1-NAT erreicht werden.

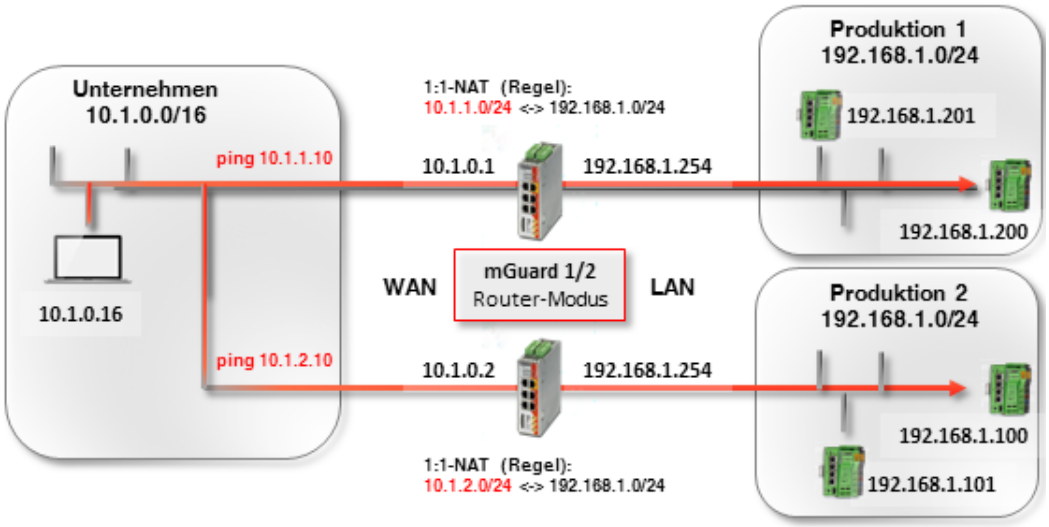

Bild 1-4 1:1-NAT-Regel: Aus dem Unternehmensnetzwerk auf das gesamte Produktionsnetzwerk zugreifen

Die beiden mGuard-Geräte verfügen über externe IP-Adressen, die zum externen Unternehmensnetzwerk gehören (10.1.0.1 und 10.1.0.2).

Aus dem Unternehmensnetzwerk soll mittels 1:1-NAT über das *virtuelle* Netzwerk **10.1.1.0/24** auf die Systeme des **Produktionsstandortes 1** und über das *virtuelle* Netzwerk **10.1.2.0/24** auf die Systeme des **Produktionsstandortes 2** zugegriffen werden.

Kein *realer* Client im Unternehmensnetzwerk darf eine IP-Adresse aus den *virtuellen* Netzwerken verwendet.

Tabelle 1-2 Beispiel-Regeln für 1:1-NAT mit unterschiedlichen Netzmasken und resultierende Zuordnungen

Reales Netzwerk	Virtuelles Netzwerk	Netzmaske	Zugeordnete IP-Adressen
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

Der jeweilige ARP-Daemon auf den beiden mGuard-Routern stellt sicher, dass Clients im externen Netzwerk wissen, wohin sie Pakete senden sollen, die an die Netzwerke 10.1.1.0/24 und 10.1.2.0/24 adressiert sind.

1.4.2 Einstellung auf dem mGuard-Gerät

Um die Produktionsnetzwerke aus dem Unternehmensnetzwerk mithilfe von 1:1-NAT erreichbar zu machen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an.
2. Gehen Sie zu **Netzwerk >> NAT**.
3. Konfigurieren Sie die 1:1-NAT-Regeln gemäß Bild 1-5.

Bild 1-5 *mGuard 1*: Produktion 1 erreichen (Netzwerke)

1. Melden Sie sich auf der Weboberfläche von *mGuard 2* an.
2. Gehen Sie zu **Netzwerk >> NAT**.
3. Konfigurieren Sie die 1:1-NAT-Regeln gemäß Bild 1-6.

Bild 1-6 *mGuard 2*: Produktion 2 erreichen (Netzwerke)

Ergebnis

Auf den Client 192.168.1.200 der Produktionsstandortes 1 kann aus dem externen Netzwerk über die IP-Adresse 10.1.1.200 zugegriffen werden. Der Client 192.168.1.201 ist über die IP-Adresse 10.1.1.201 erreichbar.

Auf den Client 192.168.1.10 der Produktionsstandortes 2 kann aus dem externen Netzwerk über die IP-Adresse 10.1.2.10 auf den Client 192.168.1.11 mit der IP-Adresse 10.1.2.11 usw. zugegriffen werden.

Clients des Produktionsstandorts 2 können prinzipiell auch von Produktionsstandort 1 aus über ihre *virtuellen* IP-Adressen (10.1.2.0/24) erreicht werden und umgekehrt.