1 NAT in VPN-Verbindungen verwenden

Dokument-ID: 108411_de_00
Dokument-Bezeichnung: AH DE MGUARD IPSEC VPN 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 werden Konfigurationen von IPsec-VPN-Verbindungen unter Verwendung von 1:1-NAT und IP-Maskierung (IP-Masquerading) beschrieben.

1.1 Einleitung

Eine VPN-Verbindung kann in der Regel nur zwischen unterschiedlichen Netzwerken (z. B. Netz A: 192.168.**1**.0/24 <-> Netz B: 192.168.**2**.0/24).

Werden an zwei Standorten die gleichen internen Netze (z. B. 192.168.**1**.0/24) verwendet, können folgende Probleme auftreten:

1. Wenn die Standorte über einen VPN-Tunnel verbunden sind, würde dies zu Routing-Problemen führen. Es wäre nicht klar, für welches Netz Pakete, die an IP-Adressen des auf beiden Seiten gleichen internen Netzwerks gesendet werden, bestimmt sind.

   Das Problem lässt sich durch die Verwendung von **1:1-NAT** umgehen (siehe Kapitel 1.2).
2. Wenn sich mehrere Standorte mit teilweise gleichen internen Netzen über einen VPN-Tunnel mit einem zentralen Standort verbinden, würde dies ebenfalls zu Routing-Problemen führen. Das Problem lässt sich durch die Verwendung von **1:1-NAT** oder zum Teil mittels **IP-Maskierung** umgehen (siehe Kapitel 1.3 und 1.5).

1.1.1 1:1-NAT

1:1-NAT bedeutet, dass der **Netzwerk-Teil** einer IP-Adresse einem anderen Netzwerk zugeordnet wird und der **Host-Teil** unverändert bleibt (z. B. **192.168.1.102**/24 <-> **192.168.2.102**/24). Der Netzwerkteil wird durch die Subnetzmaske definiert.

Dabei wird ein *Reales Netzwerk* (z. B. das interne Netzwerk) einem *Virtuellen Netzwerk* zugeordnet, um vorhandene Netzwerküberschneidung zu umgehen. Der Aufbau von VPN-Tunneln erfolgt dann nicht mehr über die *Realen* sondern über *Virtuelle Netzwerke*.

1.1.2 IP-Maskierung

IP-Maskierung (*IP-Masquerading*) ist eine besondere Form des NAT. Sie muss z. B. auf Gateways aktiviert werden, die private Netzwerke mit dem Internet verbinden, um auf das Internet zugreifen zu können.

Beim Zugriff auf eine Webseite von einem internen Netzwerk ersetzt das Gateway (NAT-Router) die private IP-Adresse des Absenders (z. B. 192.168.1.100) durch seine eigene öffentliche IP-Adresse (z. B. 77.245.32.78). Damit weiß der Ziel-Webserver, an welche öffentliche Adresse er die Antwort zurückschicken muss.

Die Antwort des Webservers an den NAT-Router (77.245.32.78) wird dann von diesem durch die IP-Adresse des ursprünglichen Absenders ersetzt (192.168.1.100) und an den Client im internen Netzwerk weitergeleitet.

IP-Maskierung wird nur in eine Richtung angewendet, z. B. aus dem internen in ein externes Netzwerk bzw. das Internet. Ein Client im internen Netzwerk (z. B. 192.168.1.100) könnte dann auf Ziele im externen Netzwerk bzw. auf Webseiten im Internet zugreifen, aber er wäre nicht über seine private IP-Adresse aus dem externen Netzwerk oder dem Internet erreichbar.

IP-Maskierung in VPN-Verbindungen

IP-Maskierung in VPN-Verbindungen bietet die gleiche Funktionalität, jedoch innerhalb einer VPN-Verbindung.

Wenn Datenpakete durch den VPN-Tunnel an ein Remote-Netzwerk gesendet werden, ersetzt das mGuard-Gerät die IP-Adresse des Absenders durch eine bestimmte, einzelne IP-Adresse und kehrt die Maskierung beim Empfang der Antwort aus dem Remote-Netzwerk um.

Der große Vorteil ist, dass das gesamte reale (lokale) Netzwerk von einer einzigen IP-Adresse *maskiert* wird.

Wenn mehrere VPN-Verbindungen an einem zentralen VPN-Gateway enden, reduziert diese Funktion den benötigten Adressraum für die VPN-Verbindungen und macht die VPN-Konfiguration übersichtlicher.

1.2 Standorte mit gleichen internen Netzen miteinander verbinden (1:1-NAT)

1.2.1 Beispiel

Zwei Standorte mit dem gleichen internen Netzwerk (192.168.1.0/24) sollen über einen VPN-Tunnel miteinander verbunden werden. Dazu muss auf beiden mGuard-Geräten **Lokales NAT für IPsec-Tunnelverbindungen (1:1-NAT)** verwendet werden.

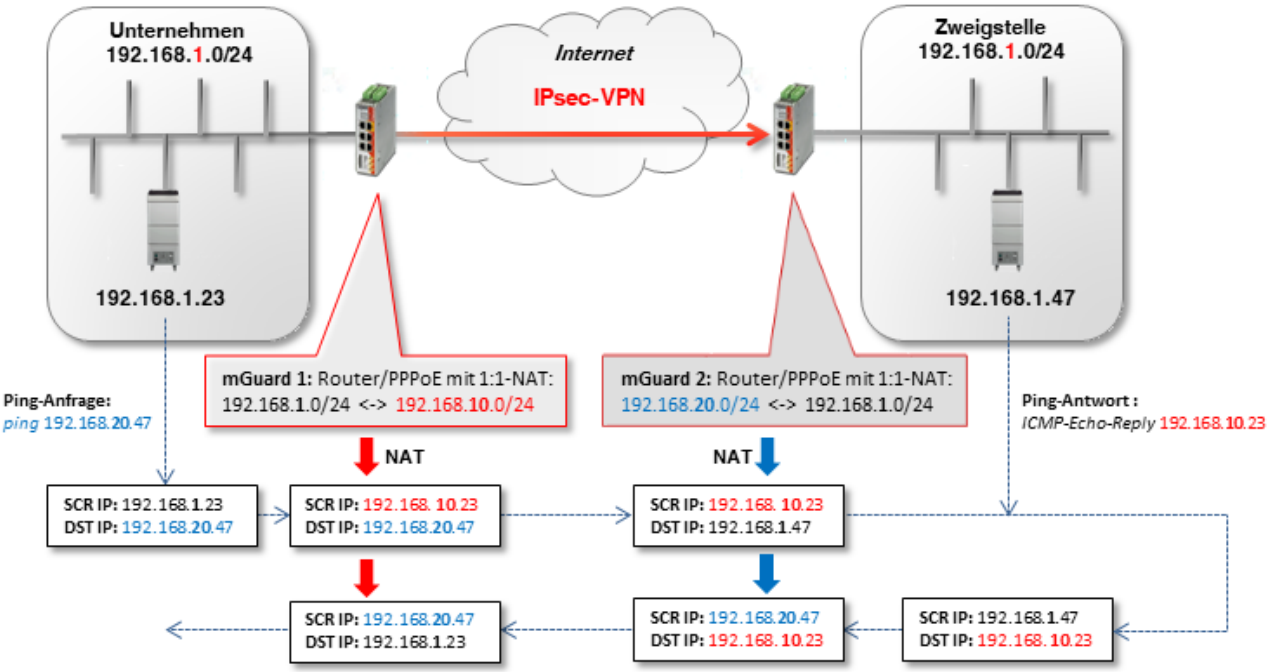


Bild 1-1 Gleiche interne Netze: Ping-Anfrage durch einen VPN-Tunnel unter Verwendung von lokalem 1:1-NAT

- **mGuard 1** macht 1:1-NAT: 192.168.**1**.0/24 <-> 192.168.**10**.0/24.
  Der Netzwerkteil wird umgeschrieben und der Hostteil beibehalten. Damit sind die Clients im Unternehmensnetzwerk durch den VPN-Tunnel im *Virtuellen Netzwerk* 192.168.**10**.0/24 erreichbar.
- **mGuard 2** macht ebenfalls 1:1-NAT: 192.168.**1**.0/24 <-> 192.168.**20**.0/24.
  Die Clients im Zweigstellennetzwerk sind durch den VPN-Tunnel im *Virtuellen Netzwerk* 192.168.**20**.0/24 erreichbar.

1.2.2 VPN-Verbindung konfigurieren

Der VPN-Tunnel muss zwischen *Virtuellen Netzwerken* aufgebaut werden. Dazu wird auf beiden Geräten ein lokales 1:1-NAT durchgeführt.

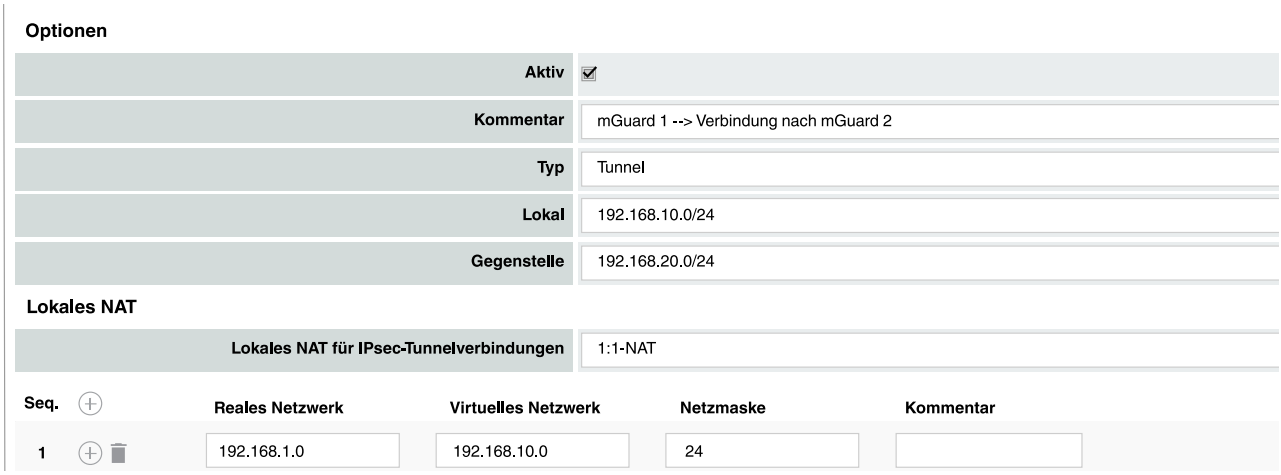


Bild 1-2 **mGuard 1**: IPsec VPN >> Allgemein (Tunneleinstellungen mit 1:1-NAT)

Um die VPN-Verbindung der mGuard-Geräte zu konfigurieren, gehen Sie wie folgt vor:

1. Gehen Sie zu **IPsec VPN >> Verbindungen**.
2. Klicken Sie auf das Icon ⊕, um eine neue VPN-Verbindung hinzuzufügen.
3. Geben Sie der Verbindung einen eindeutigen Namen und klicken Sie auf das Icon ✎.
4. Klicken Sie unter **Transport- und Tunneleinstellungen** auf das Icon ✎.
5. Konfigurieren Sie die VPN-Verbindung gemäß Tabelle 1-1 und Bild 1-2.

Tabelle 1-1 VPN-Verbindung konfigurieren

Sektion	Parameter	Unternehmen / mGuard 1	Zweigstelle / mGuard 2
IPsec VPN >> Verbindungen >> (Edit) >> Allgemein			
Optionen	**Ein beschreibender Name für die Verbindung**	VPN nach Zweigstelle	VPN von Unternehmen
	Adresse des VPN-Gateways der Gegenstelle	77.245.32.78	%any
	Interface, das bei der Einstellung %any für das Gateway benutzt wird	-----	Extern
	Verbindungsinitiierung	Initiiere	Warte
Transport- und Tunneleinstellungen >> (Edit) >> Allgemein			
Transport- und Tunneleinstellungen	**Typ**	Tunnel	Tunnel
	Lokal	192.168.**10**.0/24	192.168.**20**.0/24
	Gegenstelle	192.168.**20**.0/24	192.168.**10**.0/24
Lokales NAT	**Lokales NAT für IPsec-Tunnelverbindungen**	1:1-NAT	1:1-NAT
	Reales Netzwerk	192.168.**1**.0	192.168.**1**.0
	Virtuelles Netzwerk	192.168.**10**.0	192.168.**20**.0
	Netzmaske	24	24

Ergebnis

– Pakete an das Unternehmensnetzwerk im internen Netz von *mGuard 1* müssen an das *Virtuelle Netzwerk* 192.168.**10**.0/24 gesendet werden.
– Pakete an das Zweigstellennetzwerk im internen Netz von *mGuard 2* müssen an das *Virtuelle Netzwerk* 192.168.**20**.0/24 gesendet werden.

1.3 Standorte mit gleichen internen Netzen mit Zentrale verbinden (1:1-NAT)

1.3.1 Beispiel

Zwei Standorte, die das gleiche interne Netzwerk verwenden (192.168.1.0/24), sollen gleichzeitig über jeweils einen VPN-Tunnel mit der Unternehmens-Zentrale verbunden werden. Dazu muss auf beiden mGuard-Geräten **Lokales NAT für IPsec-Tunnelverbindungen (1:1-NAT)** verwendet werden.

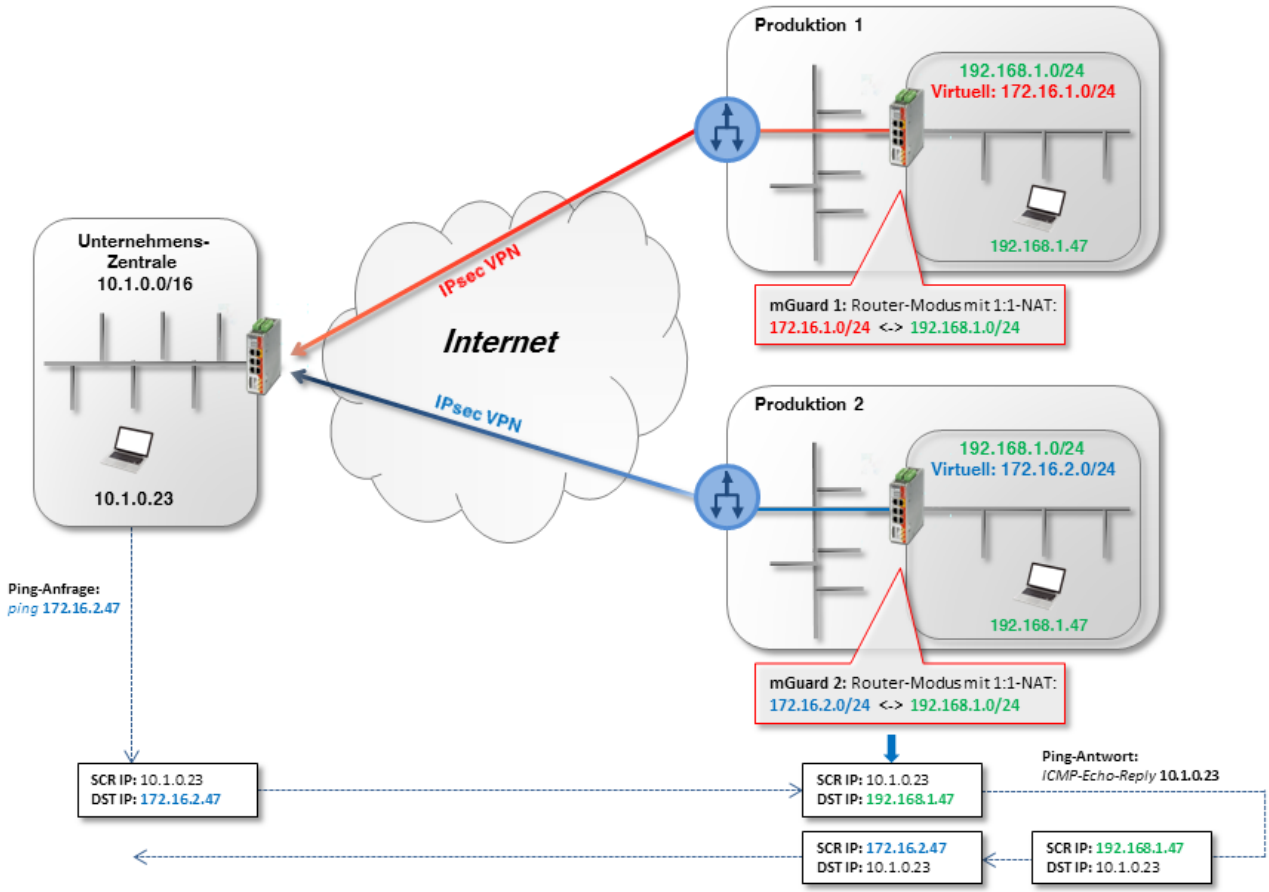


Bild 1-3 (Beispiel *mGuard 2*) Gleiche interne Netze: Ping-Anfrage (nach Produktion 2) aus der Unternehmens-Zentrale durch den VPN-Tunnel unter Verwendung von lokalem 1:1-NAT

- **mGuard 1** macht 1:1-NAT: 192.168.1.0/24 <-> 172.16.**1**.0/24).
  Die Clients in seinem internen Netzwerk (**Produktion 1**) sind durch den VPN-Tunnel im *Virtuellen Netzwerk* 172.16.**1**.0/24 erreichbar.
- **mGuard 2** macht 1:1-NAT (192.168.1.0/24 <-> 172.16.**2**.0/24).
  Die Clients in seinem internen Netzwerk (**Produktion 2**) sind durch den VPN-Tunnel im *Virtuellen Netzwerk* 172.16.**2**.0/24 erreichbar.

VPN-Verbindung konfigurieren

Auf dem mGuard-Gerät der Zentrale müssen zwei VPN-Verbindungen konfiguriert und jeweils ein lokales 1:1-NAT durchgeführt werden. In den Tunneleinstellungen muss dort als Gegenstelle jeweils das *Virtuelle Netzwerk* von mGuard **1** bzw. **2** angegeben werden (172.16.**1**.0/24 bzw. 172.16.**2**.0/24).

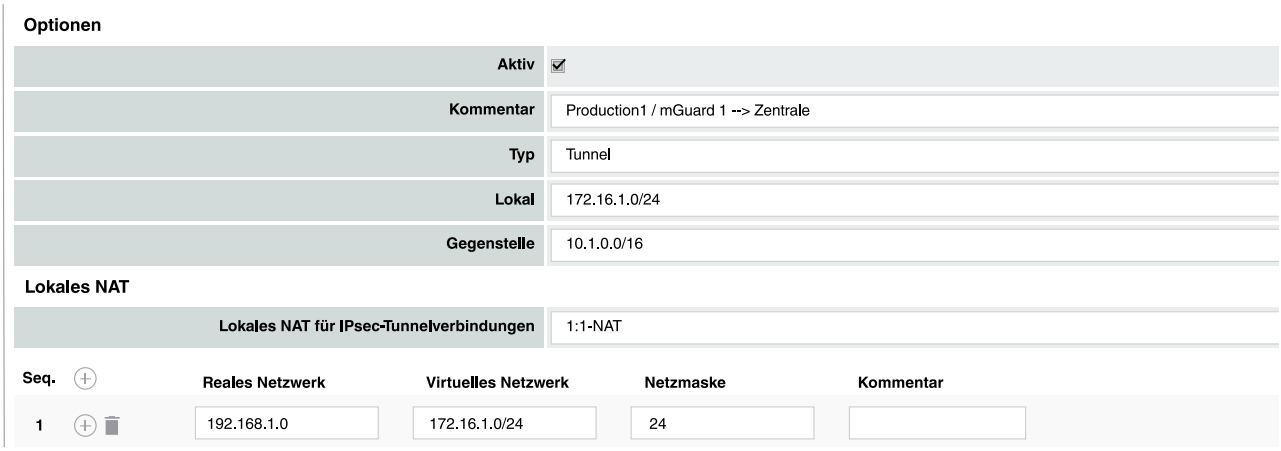


Bild 1-4 **mGuard 1**: IPsec VPN >> Allgemein (Tunneleinstellungen mit 1:1-NAT)

Um die VPN-Verbindung der mGuard-Geräte zu konfigurieren, gehen Sie wie folgt vor:

1. Gehen Sie zu **IPsec VPN >> Verbindungen**.
2. Klicken Sie auf das Icon ⊕, um eine neue VPN-Verbindung hinzuzufügen.
3. Geben Sie der Verbindung einen eindeutigen Namen und klicken Sie auf das Icon ✎.
4. Klicken Sie unter **Transport- und Tunneleinstellungen** auf das Icon ✎.
5. Konfigurieren Sie die VPN-Verbindung gemäß Tabelle 1-2 und Bild 1-3.

Tabelle 1-2 VPN-Verbindung konfigurieren

Sektion	Parameter	Produktion mGuard 1	Produktion mGuard 2	Zentrale
IPsec VPN >> Verbindungen >> (Edit) >> Allgemein				
Optionen	**Ein beschreibender Name für die Verbindung**	VPN nach Zentrale	VPN nach Zentrale	Nach Produktion (**1** bzw. **2**)
	Adresse des VPN-Gateways der Gegenstelle	77.245.32.78	77.245.32.78	%any
	Interface, das bei der Einstellung %any für das Gateway benutzt wird	-----	-----	Extern
	Verbindungsinitiierung	Initiiere	Initiiere	Warte
Transport- und Tunneleinstellungen >> (Edit) >> Allgemein				
Transport- und Tunneleinstellungen	**Typ**	Tunnel	Tunnel	Tunnel
	Lokal	172.16.**1**.0/24	172.16.**2**.0/24	10.1.0.0/16
	Gegenstelle	10.1.0.0/16	10.1.0.0/16	172.16.**1**.0/24 bzw. 172.16.**2**.0/24
Lokales NAT (Nur mGuard 1 bzw. 2)	**Lokales NAT für IPsec-Tunnelverbindungen**	1:1-NAT	1:1-NAT	
	Reales Netzwerk	192.168.**1**.0	192.168.**1**.0	
	Virtuelles Netzwerk	172.16.**1**.0/24	172.16.**2**.0/24	
	Netzmaske	24	24	

Ergebnis

Pakete an das Netzwerk **Produktion 1** (im internen Netz von *mGuard 1*) bzw. **Produktion 2** (im internen Netz von *mGuard 2*) müssen an das *Virtuelle Netzwerk* 172.10.**1**.0/24 bzw. 172.16.**2**.0/24 gesendet werden.

1.4 Standorte mit gleichen internen Netzen mit Zentrale verbinden (Maskierung)

Die Zentrale soll über ein zentrales VPN-Gateway über VPN-Tunnel mit mehreren externen Standorten (Produktion) verbunden werden. Die externen Standorte verwenden teilweise die gleichen internen Netze oder das gleiche interne Netz wie die Zentrale.

1.4.1 Beispiel 1: Übertragung in eine Richtung (IP-Maskierung)

Wenn die Datenübertragung in nur eine Richtung – von den Maschinensteuerungen zur Zentrale – erfolgen soll, kann IP-Maskierung verwendet werden.

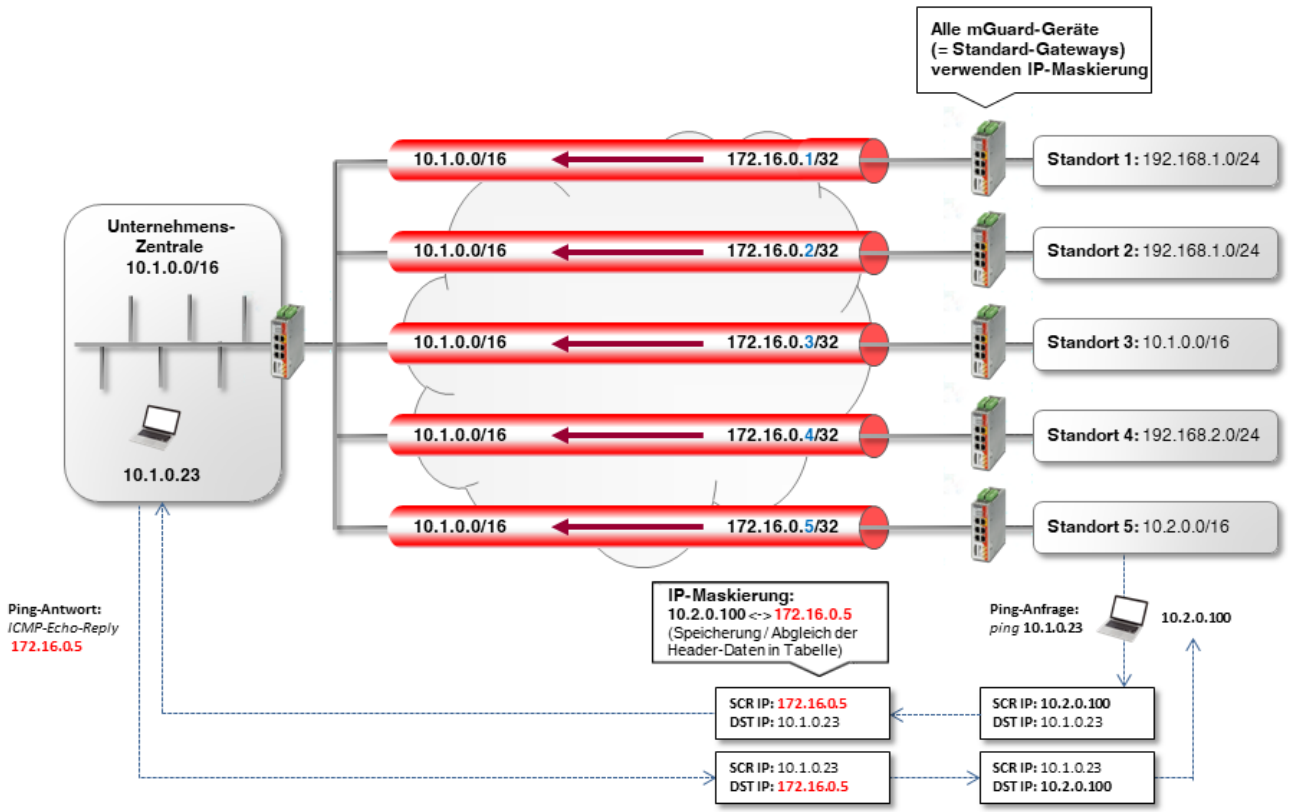


Bild 1-5 **Übertragung in nur eine Richtung (IP-Maskierung)**: Clients (z. B. SPS) in den externen Netzwerken können Daten über VPN an die Zentrale schicken. Die Zentrale kann jedoch **nicht** auf die Clients zugreifen. Das jeweilige mGuard-Gerät ist das Standard-Gateway der internen Clients.

VPN-Verbindung konfigurieren

Um VPN-Verbindungen von allen Standorten zur Zentrale aufzubauen, muss an jedem Standort IP-Maskierung verwendet werden. Dabei kann die für das Maskieren verwendete IP-Adresse einfach bei jedem Standort erhöht werden.

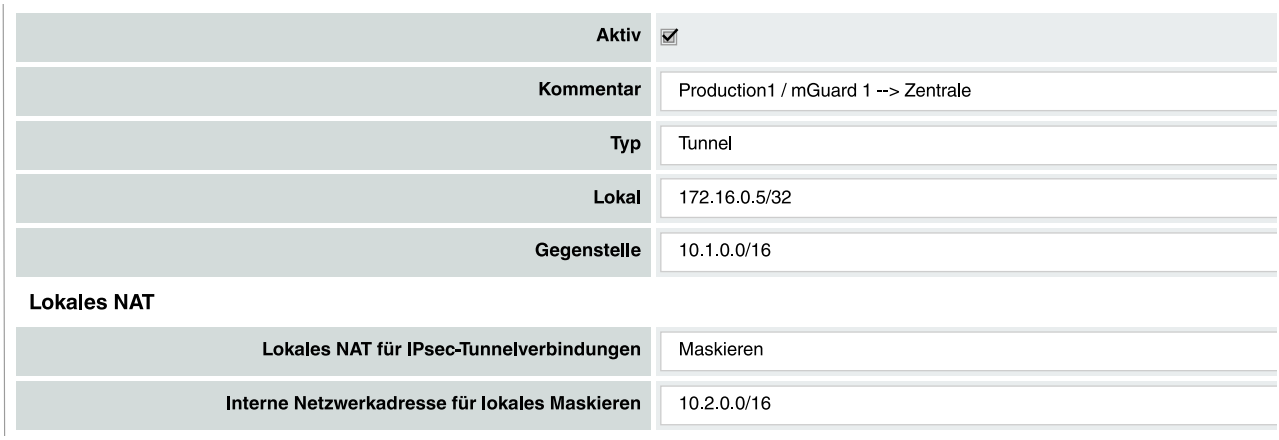


Bild 1-6 Konfigurationsbeispiel *Standort 5* (Tunneleinstellungen mit IP-Maskierung)

Tabelle 1-3 VPN-Verbindung konfigurieren

Sektion	Parameter	Zentrale	Standort 5
IPsec VPN >> Verbindungen >> (Edit) >> Allgemein			
Optionen	**Ein beschreibender Name für die Verbindung**	VPN von Standort 5	VPN nach Zentrale
	Adresse des VPN-Gateways der Gegenstelle	%any	77.245.32.78
	Interface, das bei der Einstellung %any für das Gateway benutzt wird	Extern	-----
	Verbindungsinitiierung	Warte	Initiiere
Transport- und Tunneleinstellungen >> (Edit) >> Allgemein			
Transport- und Tunneleinstellungen	**Typ**	Tunnel	Tunnel
	Lokal	10.1.0.0/16	172.16.0.5/32
	Gegenstelle	172.16.0.5/32	10.1.0.0/16
Lokales NAT	**Lokales NAT für IPsec-Tunnelverbindungen**	Kein NAT	Maskieren
	Interne Netzwerkadresse für lokales Maskieren	-----	10.2.0.0/16

Ergebnis

Die Clients im Netzwerk der Zentrale sind unter ihren realen IP-Adressen zu erreichen.

Vorteile

Die VPN-Konfigurationen ist unkompliziert und leicht nachvollziehbar. Der Adressraum für die Gegenstellen ist reduziert.

Nachteile

Die VPN-Verbindungen können nur in eine Richtung genutzt werden. Im obigen Beispiel können nur die Standorte auf die Zentrale zugreifen.

1.4.2 Beispiel 2: Übertragung in beide Richtungen (1:1-NAT)

Wenn die Datenübertragung in beide Richtungen erfolgen soll, muss lokales 1:1-NAT verwendet werden (siehe auch Kapitel 1.3).

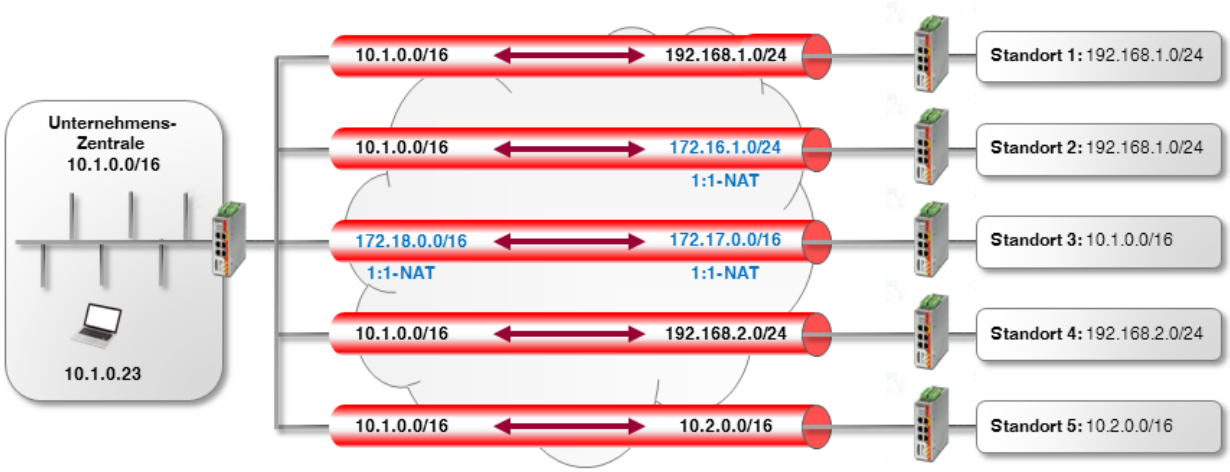


Bild 1-7 **Übertragung in beide Richtungen (Lokales 1:1-NAT)**: Die Clients (z. B. SPS) in den externen Netzwerken können durch den VPN-Tunnel auf das Netzwerk der Zentrale zugreifen und umgekehrt.

1. **Standort 1**: Beide Standorte haben unterschiedliche interne Netzwerke, so dass der VPN-Tunnel zwischen den Netzwerken 10.1.0.0/16 und 192.168.1.0/24 aufgebaut werden kann.
2. **Standort 2**: Das interne Netzwerk von *Standort 2* (192.168.1.0/24) wird bereits für die VPN-Verbindung zu *Standort 1* verwendet.

   Um auf das interne Netzwerk von Standort 2 über VPN zugreifen zu können, muss auf dem dortigen VPN-Gateway 1:1-NAT verwendet werden. Der VPN-Tunnel wird zwischen dem realen Netzwerk 10.1.0.0/16 und dem virtuellen Netzwerk 172.16.1.0/24 aufgebaut (siehe auch Kapitel 1.3).
3. **Standort 3**: Beide Standorte haben das gleiche interne Netzwerk 10.1.0.0/16.

   Um eine VPN-Verbindung zwischen den beiden Netzwerken herzustellen muss auf beiden VPN-Gateways 1:1-NAT verwendet werden. Der VPN-Tunnel wird zwischen den virtuellen Netzwerken 172.18.0.0/16 und 172.17.0.0/16 aufgebaut (siehe auch Kapitel 1.2).
4. **Standort 4 und 5**: Beide Standorte verfügen über interne Netzwerke, die von keiner anderen VPN-Verbindung genutzt werden. Es muss daher weder 1:1-NAT noch IP-Maskierung verwendet werden, um auf das jeweils andere Netzwerk zugreifen zu können.

ACHTUNG: Verwenden Sie keine virtuellen Netzwerke, die bereits für andere VPN-Verbindungen genutzt werden.

VPN-Verbindung konfigurieren

Die Konfiguration der Verbindungen erfolgt analog Kapitel 1.3.

Vorteile

Die VPN-Verbindungen können in beide Richtungen genutzt werden. Die Standorte sind von der Zentrale aus über die VPN-Verbindungen erreichbar und umgekehrt.

Nachteile

Jede VPN-Verbindung muss einzeln konfiguriert werden, abhängig davon, welche interne Netzwerkkonfiguration die beteiligten Gegenstellen verwenden.

Bei einer steigenden Anzahl von Remote-Standorten wird die Konfiguration zunehmend unübersichtlich, was leicht zu Fehlkonfigurationen führen kann.

1.5 1:1-NAT für das Remote-Netzwerk verwenden

Das Unternehmensnetzwerk ist mit einer Zweigstelle über eine VPN-Verbindung verbunden. Die Clients (Zielsysteme) im Zweigstellennetzwerk können über den VPN-Tunnel erreicht werden.

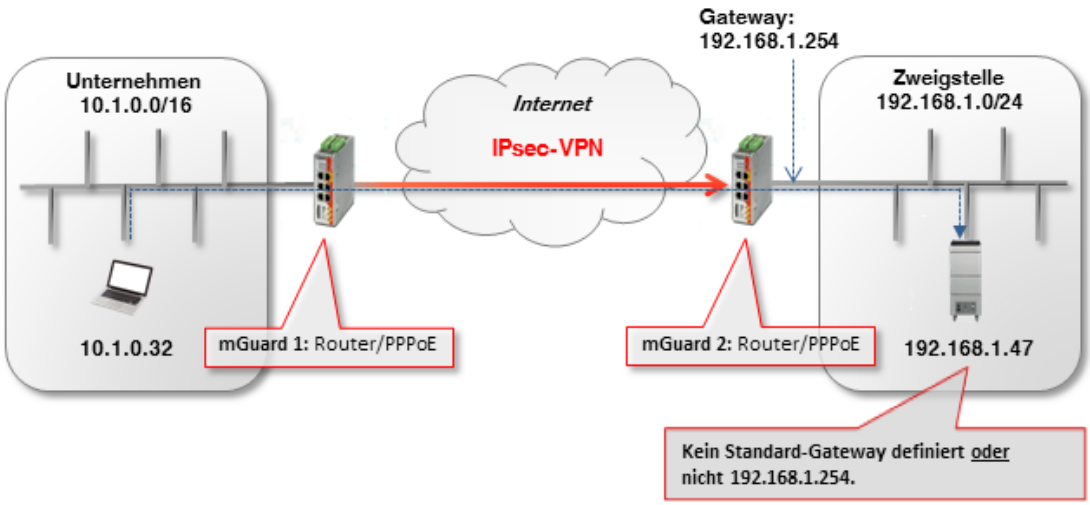
Auf einem Zielsystem (z. B. eine Maschinensteuerung, die in der Regel nur intern erreicht werden muss) ist allerdings kein Standard-Gateway definiert oder das definierte Standard-Gateway ist nicht das mGuard-Gerät, das als VPN-Gateway den VPN-Tunnel zur Verfügung stellt.

Damit kann das Zielsystem nicht auf VPN-Zugriffe aus dem Unternehmensnetzwerk antworten. Wenn sich die IP-Einstellung des Zielsystems nicht ändern lässt, kann die Funktion **Remote-NAT für IPsec-Tunnelverbindungen** genutzt werden, um das Problem zu umgehen.

1.5.1 Beispiel

Das Unternehmensnetz (10.1.0.0/16) ist dem Zielsystem (192.168.1.47/24) nicht bekannt. Wenn das Ziel (z. B. Maschinensteuerung) ein Paket über den VPN-Tunnel aus dem Unternehmensnetz empfängt,

– antwortet es entweder gar nicht (wenn kein Standard-Gateway definiert ist) oder
– es sendet die Antwort an sein Standard-Gateway (und nicht an den VPN-Gateway *mGuard 2*).

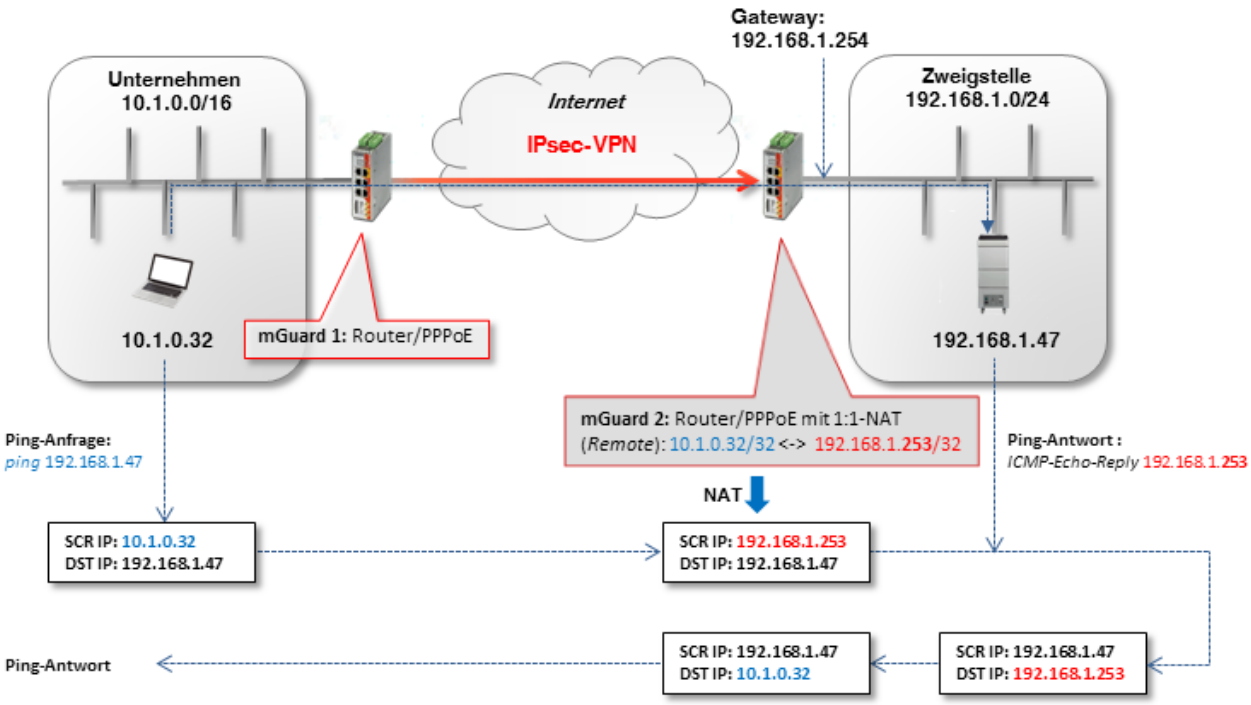


Lösung

In den VPN-Tunneleinstellungen von *mGuard 2* (VPN-Gateway der Zweigstelle) wird die Funktion **Remote-NAT für IPsec-Tunnelverbindungen** (*1:1-NAT*) verwendet.

1.5.2 VPN-Verbindung konfigurieren

Um eine Antwort des Zielsystem (z. B. Maschinensteuerung mit der IP 192.168.1.47) an den „unbekannten“ Absender zu ermöglichen, muss Remote-1:1-NAT verwendet werden.



Optionen

Aktiv	☑
Kommentar	Von Unternehmen nach Zweigstelle
Typ	Tunnel
Lokal	192.168.1.0/24
Gegenstelle	10.1.0.32/32
Lokales NAT	
Lokales NAT für IPsec-Tunnelverbindungen	Kein NAT
Remote-NAT	
Remote-NAT für IPsec-Tunnelverbindungen	1:1-NAT
Netzwerkadresse für 1:1-NAT im Remote-Netz	192.168.1.253

Bild 1-8 **mGuard 2**: IPsec VPN >> Allgemein (Tunneleinstellungen mit 1:1-NAT)

Um die VPN-Verbindung der mGuard-Geräte zu konfigurieren, gehen Sie wie folgt vor:

1. Gehen Sie zu **IPsec VPN >> Verbindungen**.
2. Klicken Sie auf das Icon ⊕, um eine neue VPN-Verbindung hinzuzufügen.
3. Geben Sie der Verbindung einen eindeutigen Namen und klicken Sie auf das Icon ✎.
4. Klicken Sie unter **Transport- und Tunneleinstellungen** auf das Icon ✎.
5. Konfigurieren Sie die VPN-Verbindung gemäß Tabelle 1-4 und Bild 1-8.

Tabelle 1-4 VPN-Verbindung konfigurieren

Sektion	Parameter	Unternehmen / mGuard 1	Zweigstelle / mGuard 2
IPsec VPN >> Verbindungen >> (Edit) >> Allgemein			
Optionen	**Ein beschreibender Name für die Verbindung**	VPN nach Zweigstelle	VPN von Unternehmen
	Adresse des VPN-Gateways der Gegenstelle	77.245.32.78	%any
	Interface, das bei der Einstellung %any für das Gateway benutzt wird	-----	Extern
	Verbindungsinitiierung	Initiiere	Warte
Transport- und Tunneleinstellungen >> (Edit) >> Allgemein			
Transport- und Tunneleinstellungen	**Typ**	Tunnel	Tunnel
	Lokal	**10.1.0.32/32**	192.168.1.0/24
	Gegenstelle	192.168.1.0/24	**10.1.0.32/32**
Remote NAT	**Remote-NAT für IPsec-Tunnelverbindungen**	Kein NAT	1:1-NAT
	Netzwerkadresse für 1:1-NAT im Remote-Netz	-----	192.168.1.**253**

Das Remote-Netzwerk oder die Remote-IP-Adresse wird auf eine **freie (virtuelle) IP-Adresse** im internen Netzwerk der Zweigestelle umgeschrieben (*gemapped*): **10.1.0.32/32 <-> 192.168.1.253**.

Eine Netzmaske muss für das Remote-Netz (192.168.1.253) nicht angegeben werden. Diese wird automatisch vom angegebenen Netz der Gegenstelle übernommen.

Das virtuelle Netzwerk/die virtuelle IP-Adresse darf von keinem Netzwerk-Client im internen Netzwerk der Zweigstelle verwendet werden.

Entsprechend der im Beispiel verwendeten Konfiguration hat nur der Client 10.1.0.32 im Unternehmensnetzwerk Zugriff auf das Ziel in der Zweigstelle.

Seien Sie vorsichtig, wenn Sie die Subnetzmaske für das Remote-Netzwerk auswählen und das Netzwerk angeben, dem das Remote-Netzwerk zugeordnet werden soll (siehe „Problem bei 1:1-NAT für Remote-Netzwerke“).

Der ARP-Proxy von *Guard 2* liefert die ARP-Auflösung für das virtuelle Netzwerk/ IP-Adresse. Das Zielsystem sendet seine Antworten an *mGuard 2*:

– Pakete aus dem Unternehmensnetzwerk (10.1.0.0/16) werden über das VPN-Gateway (*mGuard 1*) an die reale IP-Adresse des Ziel-Clients in der Zweigstelle (**192.168.1.47)** gesendet.
– *mGuard 2* erhält die Anfrage, führt ein 1:1-NAT für das Remote-Netzwerk/IP-Adresse durch (**10.1.0.32/32** <-> **192.168.1.253**) und leitet die Anfrage an den Ziel-Client (**192.168.1.47**) weiter.
– Der Ziel-Client empfängt die Anfrage und sendet seine Antwortpakte an die virtuelle Absender-IP-Adresse (**192.168.1.253**).
– *mGuard 2* erhält die Antwort, macht das 1:1-NAT rückgängig (**192.168.1.253** <-> **10.1.0.32/32**) und leitet die Antwort an *mGuard 1* bzw. den Absender im Unternehmensnetzwerk (**10.1.0.32**) weiter.

Problem bei 1:1-NAT für Remote-Netzwerke

Die Subnetzmaske */24* für das Remote-Netzwerk (z. B. 10.1.0.0/24) und eine Remote-1:1-NAT-Adresse (z. B. 192.168.1.0) würde nicht funktionieren, da in diesem Fall der ARP-Proxy von *mGuard 2* auf alle ARP-Anfragen des internen Netzwerks der Zweigstelle antworten würde (192.168.1.0 – 192.168.1.255).

Eine Erhöhung der Subnetzmaske des Remote-Netzwerks würde auch die Anzahl der Clients im Unternehmensnetzwerk erhöhen, von denen aus auf den Client in der Zweigstelle zugegriffen werden kann. Es würde aber auch die erforderliche Anzahl unbenutzter IP-Adressen in der Zweigstelle für die Zuordnung der Quell-IP-Adresse erhöhen.

Die folgende Tabelle zeigt, den Zusammenhang zwischen

– der Remote-Subnetzmaske,
– den Clients, die auf das Zielsystem zugreifen können,
– der Anzahl der benötigten unbenutzten IP-Adressen im internen Netzwerk.

	Beispiel 1	**Beispiel 2**	**Beispiel 3**	**Beispiel 4**
Angegebenes Remote-Netzwerk	10.1.0.0**/26**	10.1.0.64**/26**	10.1.0.128**/28**	10.1.0.32**/32**
Remote-IP-Adressen, die auf das Zielsystem zugreifen können	10.1.0.0 – 10.1.0.63	10.1.0.64 – 10.1.0.127	10.1.0.128 – 10.1.0.143	10.1.0.32
Internes Netzwerk	192.168.1.0**/24**			
Netzwerkadresse für Remote 1:1-NAT	192.168.1.128**/26**	192.168.1.192**/26**	192.168.1.240**/28**	192.168.1.253**/32**
Hosts, denen der mGuard auf ARP-Anfragen antworten würde **(Dürfen nicht im internen Netzwerk verwendet werden!)**	192.168.1.128 – 192.168.1.191 **64 Hosts**	192.168.1.192 – 192.168.1.255 **64 Hosts**	192.168.1.240 – 192.168.1.255 **16 Hosts**	192.168.1.253 **1 Host**

Zusätzlicher NAT-Router

Wenn von mehreren Clients im Unternehmensnetzwerk auf die Zielsysteme in der Zweigstelle zugegriffen werden soll, kann ein NAT-Router verwendet werden, bevor die Pakete in den VPN-Tunnel übergeben werden.

Damit muss als Remote-Netzwerk die IP-Adresse des NAT-Routers mit der Subnetzmaske */32* angegeben werden. Nur eine unbenutzte IP-Adresse würde benötigt.

IP-Maskierung

Wenn die VPN-Verbindung nur in eine Richtung genutzt werden muss, z. B. vom Unternehmensnetzwerk zur Zweigstelle (Fernwartung), kann statt eines weiteren NAT-Routers auf *mGuard 1* auch IP-Maskierung (*IP-Masquerading*) im VPN-Tunnel verwendet werden (siehe auch Kapitel 1.4).

Auf diese Weise hätten die ankommenden Datenpakete bei *mGuard 2* immer die gleiche Quell-IP-Adresse (/32).