ads-tec GmbH

IRF2000, IF1000

Application Note
Network Mapping mit 1:1 NAT

Inhaltsverzeichnis

Das Original dieser Betriebsanleitung wurde in deutscher Sprache verfasst. Jede nicht deutschsprachige Ausgabe dieser Betriebsanleitung ist eine Übersetzung der deutschen Betriebsanleitung.

1 Einführung

Dieses Dokument zeigt, wie sich die weitreichenden NAT-Funktionen der ads-tec Industrial Firewall in der Praxis einsetzen lassen.
NAT (Network Address Translation) bezeichnet den Vorgang, eine IP-Adresse eines IP-Paketes durch eine andere Adresse zu ersetzen. Dabei gibt es verschiedene Möglichkeiten:

- „NAT / 1:N-NAT / Masquerading“: Eine IP-Adresse eines bestimmten Bereichs wird, unter bestimmten Bedingungen, durch eine einzige IP-Adresse ersetzt. Eine solche Bedingung ist z.B. wenn ein Paket über ein Interface versendet wird, auf dem Masquerading aktiviert ist.
- Weiterleitungen und „Port-Weiterleitung / PAT (Port Address Translation)“: Hier wird eine Ziel-Adresse ersetzt wobei gleichzeitig die Portnummer des Transport-Protokolls (UDP oder TCP) umgeschrieben wird. Dies wird meistens benutzt um den Verbindungsaufbau zu Hosts zu ermöglichen, die wegen eines NAT-Routers mit Masquerading sonst nicht erreichbar sind. Bei den ads-tec Routern ist es zusätzlich möglich IP Aliase zu starten und Protokoll unabhängig alle Daten an interne Hosts durchzureichen.
- „1:1 NAT / symmetrisches NAT“: hierbei wird ein ganzer Adressbereich für die Ersetzung genutzt, wodurch die Eindeutigkeit des Absenders oder Ziels gewährleistet ist. Verbindungsaufbau ist somit von beiden Seiten des NAT aus möglich.

1.1 NAT (Masquerading)

Die Konfiguration findet unter „Konfiguration → IP Konfiguration“ statt. Abhängig von einer bestimmten Netzwerk-Schnittstelle werden alle Pakete, die über dieses Interface versendet werden, umgeschrieben. Als Absender-IP-Adresse bekommt jedes Paket die IP-Adresse der Firewall auf diesem Interface.

1.2 Weiterleitung

Einstellungen werden unter „Konfiguration → Netzwerk → Weiterleitung“ vorgenommen und sind nicht Thema diesers Aplication Notes.

1.3 1:1 NAT – Network Mapping

Normalerweise ist es nicht möglich einen Router so zu konfigurieren, dass gleiche IP-Adressbereiche (z.B. 192.168.0.0/24) auf verschiedenen Netzwerkschnittstellen verwendet werden. In der Regel wird hierzu ein Switch verwendet, dann ist aber kein Routing möglich.
Insbesondere kann es vorkommen, dass Geräte miteinander kommunizieren sollen, die die gleiche IP-Adresse haben. Hier sollte normalerweise bei den Geräten eine entsprechende Konfiguration stattfinden, so dass alle Geräte eindeutige IP-Adressen haben. Manchmal ist dies aber nur mit größeren Umständen möglich, oder dieser Adress-Konflikt ist nur mit zusätzlichen NAT-Routern aufzulösen.
Um dieses Problem zu umgehen beherrscht die ads-tec Industrial Firewall eine exklusive NAT Technik - Network Mapping - die den Einsatz zusätzllicher NAT-Router erspart. Mit herkömmlichen Methoden müsste man jedes solcher gleichen Subnetze mit einem eigenen NAT-Router maskieren.
Dies kommt insbesondere bei der IF1000 zum Tragen, da dieses Gerät mit vier internen Ports auch vier identische Netze beherscht.
Die IRF2000 kann mit Ihren zwei Ports maximal zwei gleiche Netze abhandeln wenn der Uplink über UMTS realisiert ist, anonsten muss für jedes Segment ein einzelnes Gerät verwendet werden.

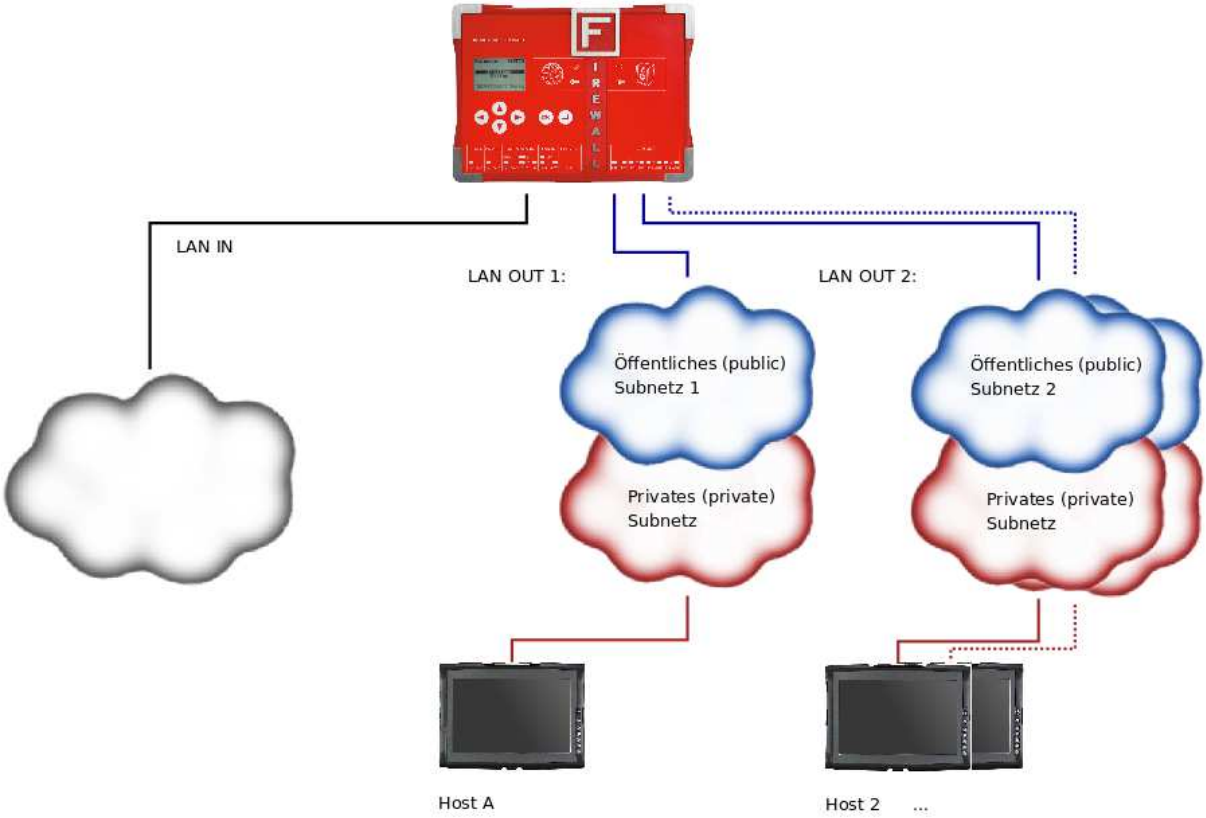


Abbildung 1: 1:1 NAT mit (identischen) privaten Subnetzen an der IF1000. Das Setup an der IRF2000 ist identisch jedoch kann hier nur jeweils ein Privates Subnetz angeschlossen werden.

2 Konfiguration

Unter „Konfiguration → Netzwerk → 1:1 NAT“ können identische Subnetze für verschiedene Routing-Schnittstellen festgelegt werden (siehe Abbildung 1).

Hinweis zur IRF2000
Die Screenshoots und Schnittstellen Namen in diesem Application Note sind in erster Linie ür die IF1000. Der Application Note läßt ich jedoch auch für die IRF2000 verwenden wenn man die Schnittsellennamen LAN-in duch WAN und LAN-out-1 durch LAN ersetzt. Und natürlich hat die IRF2000 meist nur ein internes Netzwerk.

2.1 Zuordnung privater zu öffentlichen Adressen

Die jeweilig öffentliche IP-Adresse ergibt sich (1:1) aus der privaten IP-Adresse eines Gerätes indem ein Präfix aus der Subnetz-Bezeichnung (Länge entsprechend der Subnet-Maske) mit dem Suffix aus der Geräte-Adresse verknüpft wird.

Beispiel:

Es wird das Netzwerk 192.168.10.0/24 als privates Netzwerk angenommen und eine Abbildung auf 192.168.110.0/24 und 192.168.120.0/24 wird konfiguriert. Dann hat das Gerät im privaten Bereich die IP Adresse 192.168.10.10 und m öffentlichen virtuellen Bereich die IP Adresse 192.168.110.10.
Der Prefix der öffentlichen IP-Adresse des Gerätes lautet 192.168.10 (die ersten 24 Bit sind fix, d.h. 3 Tupel a 8Bit). Das Suffix wird aus den restlichen Bits der Geräte-Adresse gebildet, also „10“. Demnach wird das Gerät auf die öffentliche IP-Adresse „192.168.120.10“ abgebildet.

Kompliziertes wird es wenn ungerade Netzwerkmasken verwendet werden und sich der Bereich intern verschiebt, auch dies wird unterstützt.

komplexes Beispiel:

Angenommen das interne Gerät habe die IP-Adresse 172.16.100.40, jedoch ist die Größe des Subnetz diesmal „/28“. Das bedeutet es enthält die IP-Adressen 172.16.100.32 – 172.16.100.47 da die ersten 28 Bits (172.16.100.32) fest sind und nur die letzten 4 Bits variabel. Das Gerät hat in diesem Subnetz die neunte IP-Adresse und dies wird eins zu eins in den öffentlichen Bereich abgebildet. Das bedeutet insbesondere, auch dort hat das Gerät die neunte IP-Adresse (Achtung: die Null wird mitgezählt).
Das öffentliche Subnetz sei diesmal definiert als 10.20.30.0/28. Verknüpft man dies mit den letzten 4 Bits der privaten IP-Adresse des Gerätes, so erhält man die öffentliche IP-Adresse des Gerätes: „10.20.30.8“.

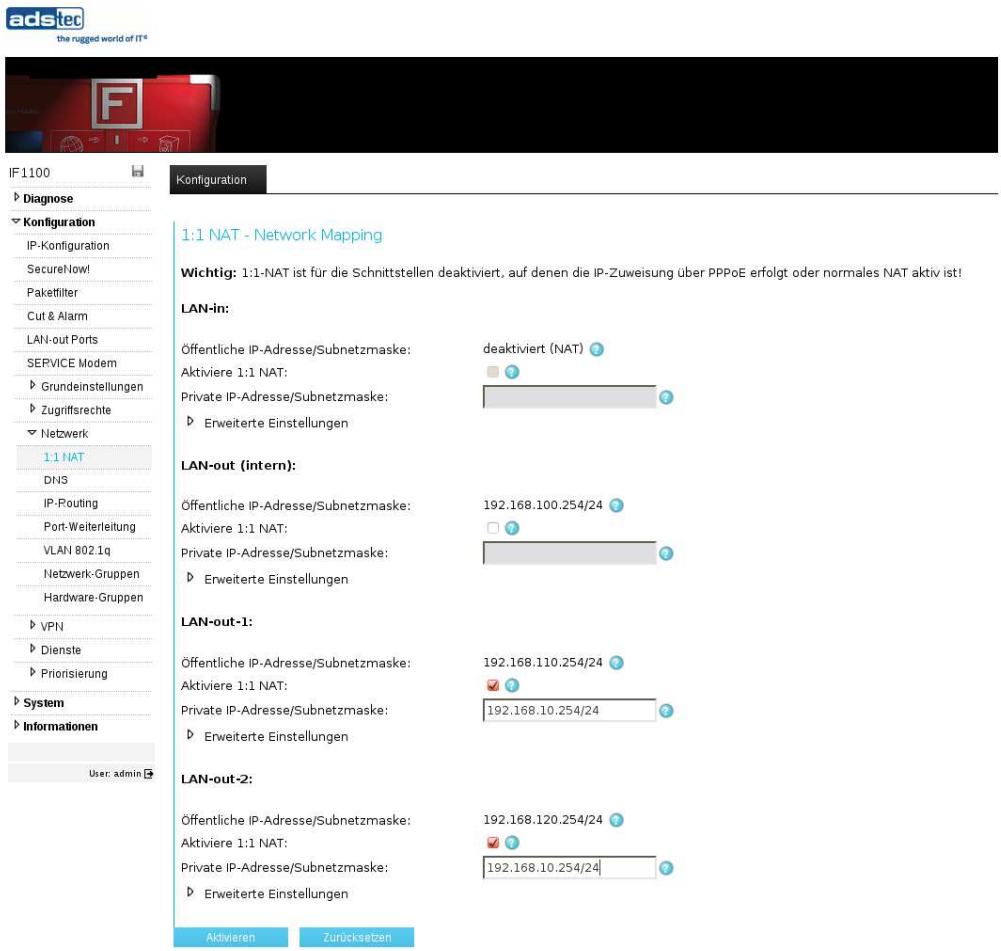


Abbildung 2: Webinterface 1:1 NAT Einstellungen

Wichtiger Hinweis:

Auf der Konfigurations-Seite für 1:1 NAT wird mit der Einstellung „privates Subnetz“ gleichzeitig die IP-Adresse der Firewall im privaten Bereich festgelegt (siehe dazu Abbildung 2). Die Industrial Firewall hat in diesem Fall zwei IP-Adressen: eine private IP-Adresse für Geräte die an dem jeweiligen 1:1 NAT Interface angeschlossen sind und eine öffentliche IP-Adresse für die übrige Welt. Hier sollte darauf geachtet werden dass die eins-zu-eins-Zuordnung zwischen privater und öffentlicher IP-Adresse gewahrt bleibt, da sie vom Benutzer festgelegt wird. Hat beispielsweise die Firewall als öffentliche IP-Adresse die „192.168.0.99/24“ (also die 100. Adresse im Subnetz), so ist darauf zu achten dass für „privates Subnetz“ auch die 100. Adresse des privaten Subnetz verwendet wird (z.B. „192.168.1.99/24). Sollte dies aus beliebigem Grund nicht möglich sein, z.B. bekommt die Firewall als private Adresse die „192.168.1.100“, so muss für ein evtl. vorhandenes Gerät im privaten Netz mit der Adresse „192.168.1.99“ mit Problemen gerechnet werden. D.h. diese Adresse sollte dann dort nicht verwendet werden.

2.2 Kommunikation über 1:1 NAT / Network Mapping

Bei der Kommunikation über 1:1 NAT-Grenzen hinweg ist hauptsächlich darauf zu achten dass Geräte hinter dem 1:1 NAT, d.h. Im privaten Subnetz, immer mit ihrer öffentlichen IP-Adresse angesprochen werden. Des Weiteren dürfen die Adressen der privaten Subnetze nicht an anderer Stelle auf der Industrial Firewall referenziert werden, z.B. bei Routing-Einträgen oder Filter-Regeln. Auch hier sind die öffentlichen IP-Adressen zu verwenden.

Beispiel:

Es sei eine Netzwerktopologie gegeben wie in Abbildung 3 gezeigt. LAN-out-1 und LAN-out-2 sind mit 1:1-NAT / network mapping konfiguriert und nutzen identische private Netze (192.168.10.254/24).
Die Firewall selbst ist erreichbar im 192.168.10.0/24 Netz über LAN-out-1 oder LAN-out-2 unter der IP-Adresse 192.168.10.254.
An LAN-out-1 und LAN-out-2 ist jeweils ein Gerät mit der IP-Adresse 192.168.10.1 vorhanden. Will man nun über die Firewall hinweg mit einem dieser Geräte kommunizieren, so muss die öffentliche IP-Adresse des jeweiligen Gerätes verwendet werden. Dies ist bei Host A die 192.168.110.1 und bei Host B die 192.168.120.1 .
Dies gilt auch für die Kommunikation der beiden Hosts untereinander: Will z.B. Host A eine Verbindung zu Host B aufbauen, so muss Host A die Ziel-Adresse 192.168.120.1 verwenden. Umgekehrt „kennt“ Host B Host A nur unter der Bezeichnung „192.168.110.1“.

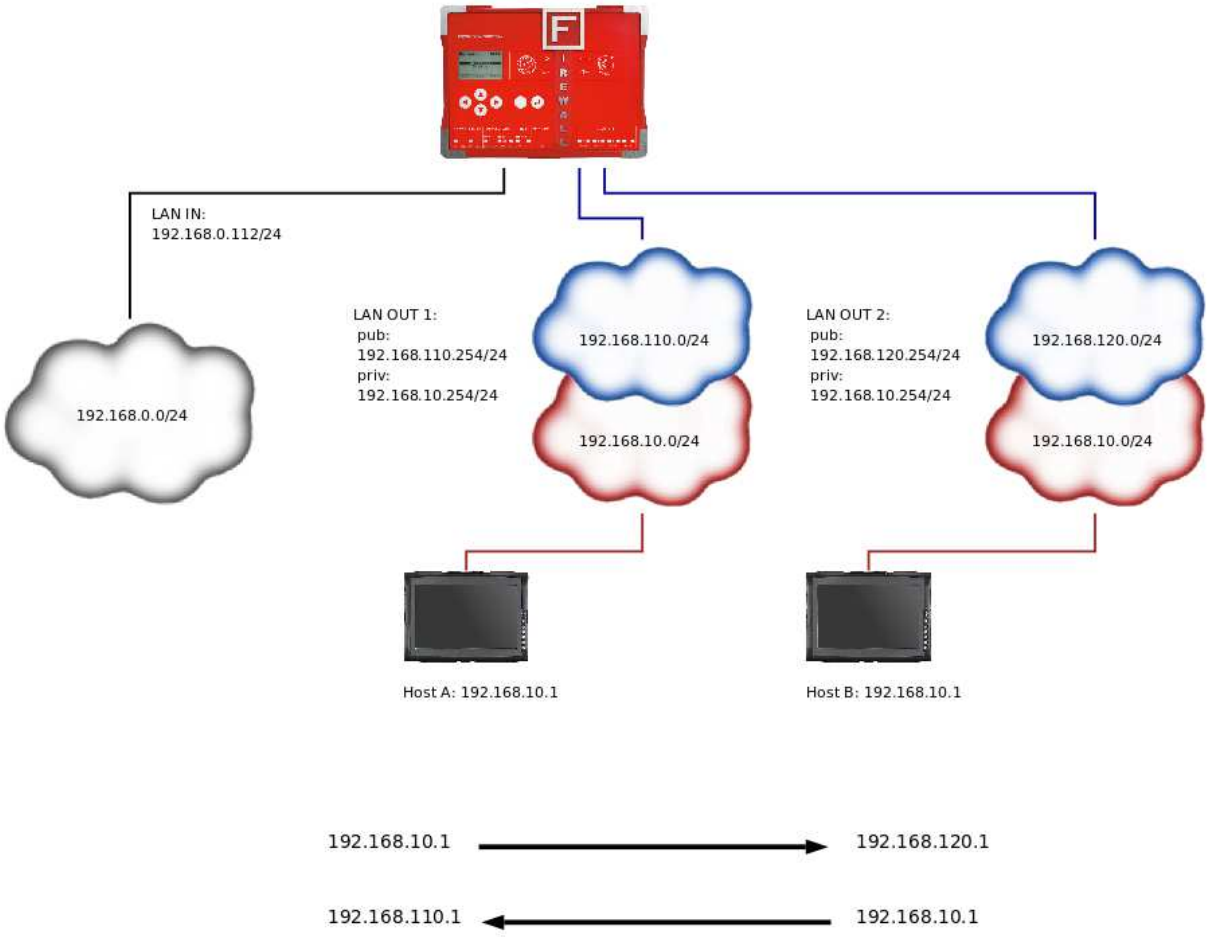


Abbildung 3: Network Mapping Netzwerktopologie, einfach

2.3 1:1 NAT – erweiterte Einstellungen

Unter Umständen wird der IP-Adressbereich, der als privates Subnetz beim 1:1 NAT verwendet wird, ebenfalls von Hosts auf anderen, öffentlichen Schnittstellen genutzt. Wenn z.B. eine Situation gegeben ist wie in Abbildung 4, dann wird der Adressbereich „192.168.10.0/24“ von Host C genutzt, der sich auf der LAN-in Seite der Firewall befindet. In einem einfacheren Fall würde es ausreichen für LAN-in ebenfalls eine 1:1 NAT Konfiguration vorzunehmen, jedoch scheitert das in unserem Beispiel an zwei Gegebenheiten:

1. auf LAN-in ist NAT (Masquerading) aktiv, und somit ist dort kein zusätzliches 1:1 NAT möglich
2. das verbundene Subnetz an LAN-in ist die „192.168.0.0/24“. Die Pakete von Host C mit dem Adressbereich „192.168.10.0/24“ werden durch einen zusätzlichen Router zur Firewall geleitet. 1:1 NAT lässt sich aber immer nur für das direkt angrenzende Subnetz definieren da die Firewall auf der jeweiligen Schnittstelle ebenfalls eine IP-Adresse aus diesem Subnetz erhält.

Damit der entstandene Adresskonflikt trotzdem gelöst werden kann, gibt es die „Erweiterte Einstellungen“ mit „Double Sided Network Mapping“. Hier wird ein weiterer Netzbereich festgelegt, der in bestimmten Situationen anstelle der IP-Adresse von Host C genutzt wird (und allen anderen Hosts mit Adressen aus diesem Bereich), d.h. Ein zusätzliches, spezielles 1:1 NAT wird aktiviert, das unabhängig von der Schnittstelle des Absenders angewendet wird.

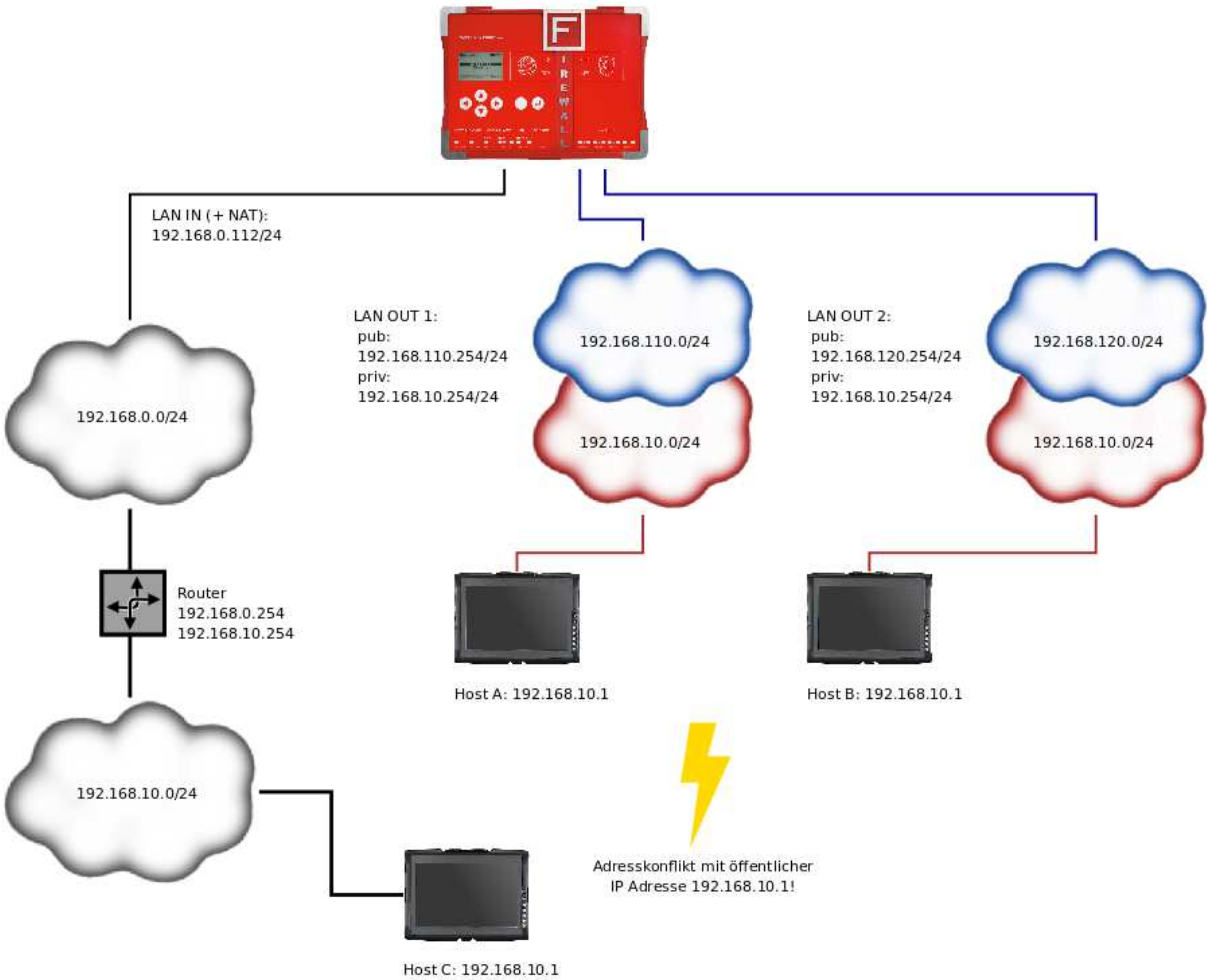


Abbildung 4: Network Mapping Netzwerktopologie, komplex

Beispiel:

Es gelten die Einstellungen wie in den vorangegangenen Beispielen und zusätzlich die Einstellungen und Annahmen in Abbildung 5 und Abbildung 4.
Zusätzlich sind zwei Ausweich-Adressbereiche für das Double Sided Network Mapping konfiguriert: 192.168.210.0/24 für das private Subnetz von LAN-out Port 1 und 192.168.220.0/24 für das private Subnetz von LAN-out Port 2
Es gibt nun also insgesamt drei Hosts mit der gleichen IP-Adresse „192.168.10.1“: Host A, Host B und Host C. Im Gegensatz zu Hosts A und B ist die IP-Adresse von Host C öffentlich. Dadurch kann es vorkommen dass Pakete von Host C mit dieser öffentlichen IP die Firewall passieren (wie zuvor erläutert). Mit den Einstellungen in Abbildung 5 läuft eine Kommunikation zwischen Host A und Host C wie folgt entweder mit Port Weiterleitungen oder über Routing:

1. **TCP Port 80 über LAN-in NAT + Port-Weiterleitung:**

   - es existiert ein Weiterleitungs-Eintrag auf der Firewall, so dass TCP-Pakete an die IP-Adresse „192.168.0.112“ und Port „2000“ weitergeleitet werden an Host A, also „192.168.110.1“ und Port 80.
   - auf LAN-in ist NAT (Masquerading) aktiviert
   - Host C erreicht Host A über die IP 192.168.0.112 und Port 2000. Bei Host A erscheint Host C unter der maskierten Quell-Adresse 192.168.210.1
   - Host A erreicht Host C über die IP 192.168.210.1

2. **Über LAN-in mit Routing:**

   - Auf Host C gibt es eine Route der Form „default via 192.168.10.254“ (IP des Routers zwischen den grauen Wolken in Abbildung 4) oder spezieller.
   - Auf dem Router gibt es eine Route der Form „default via 192.168.0.112“ oder spezieller
   - Auf der Industrial Firewall gibt es eine Route der Form „default via 192.168.0.254“ oder spezieller.
   - Auf Host A existiert eine Route der Form „default via 192.168.10.254“ (dies wurde in den bisherigen Beispielen immer stillschweigend vorausgesetzt)
   - Host C erreicht Host A über die IP 192.168.110.1
   - Host A erreicht Host C über die IP 192.168.210.1
   - Host B erreicht Host C über die IP 192.168.220.1
   - Die Firewall selbst, oder Hosts an evtl. definierten anderen Schnittstellen (LAN-out int. , LAN-out Port 3, etc.), erreichen Host C über die IP 192.168.10.1

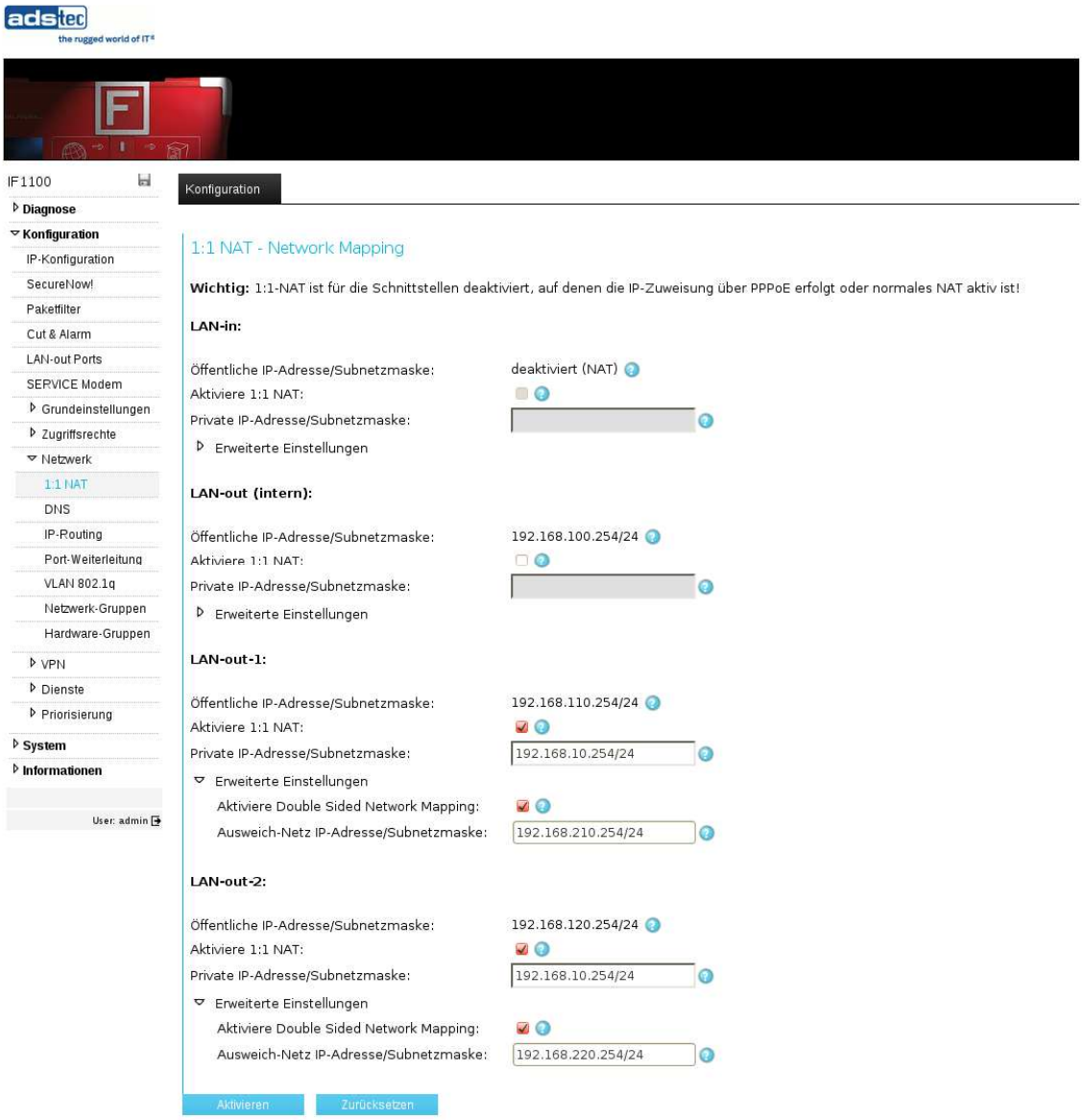
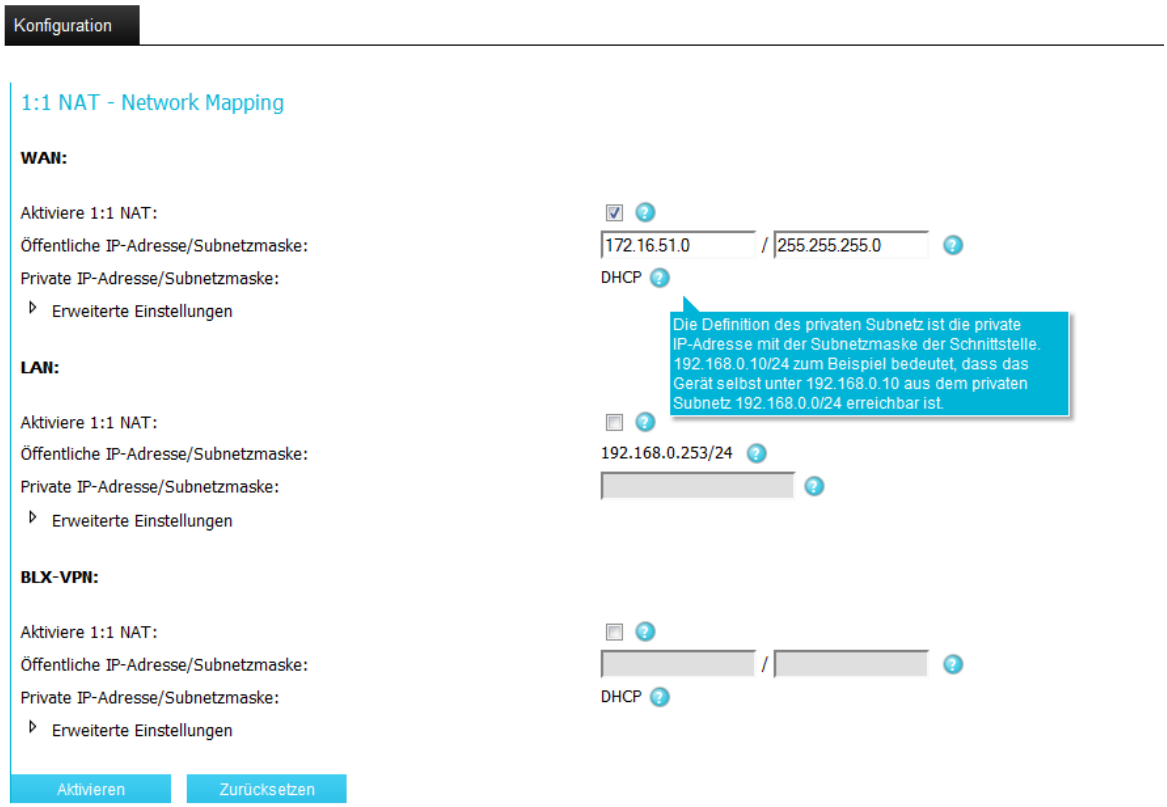


Abbildung 5: Webinterface 1:1 NAT, erweiterte Einstellungen

2.4 1:1 NAT auf Schnittstellen mit DHCP IP-Adresszuweisung

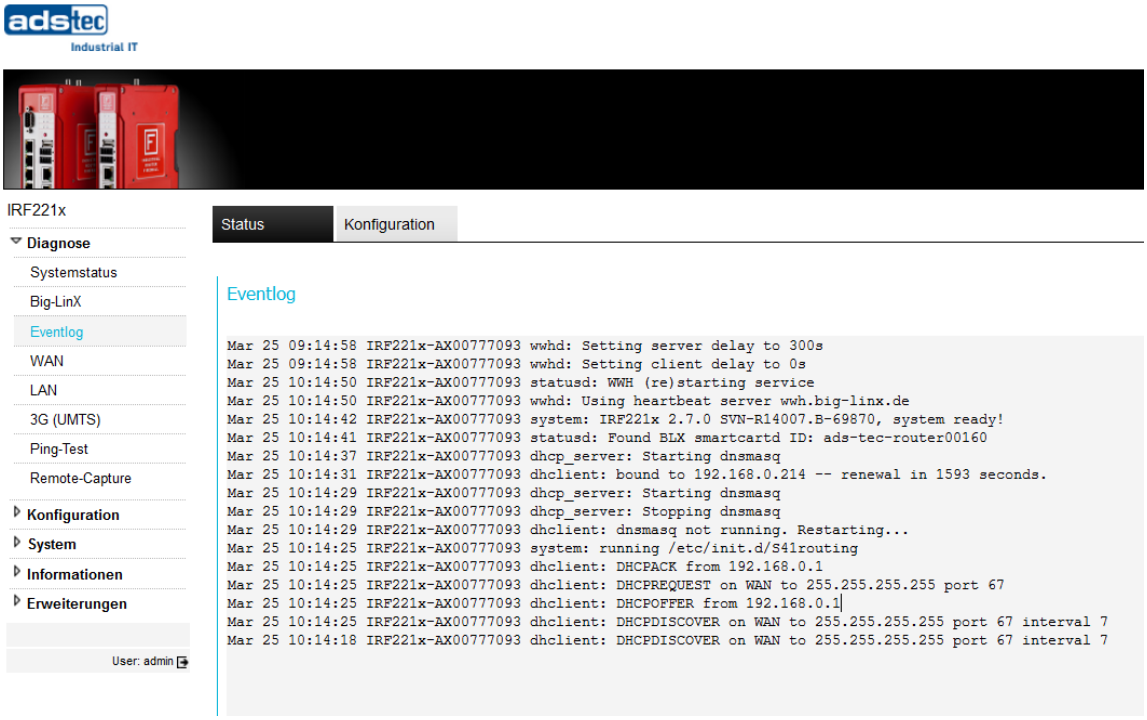
Geräte der IRF2000 Serie mit Firmware ab Version 2.7.0 unterstützen 1:1 NAT auch auf Schnittstellen mit dynamischen IP-Adressen.

Erhält das Gerät z.B. auf der WAN-Schnittstelle per DHCP die IP-Adressen im Bereich 192.168.0.200-220 und hat auf der LAN Schnittstelle die IP-Adresse 192.168.0.253, so liegt zunächst ein Konflikt vor.
Für diesen Fall könnte man also die WAN-Schnittstelle vom Netzwerk 192.168.0.0/24 in das freie Netzwerk 172.16.51.0/24 verschieben. Wobei der dynamische Offset im Netzwerk (1-20) beibehalten wird.



Das Gerät selbst wird dann z.B. auf der Startseite die IP-Adresse 172.16.51.214 anzeigen obwohl der DHCP Server eigentlich die IP 192.168.0.214 ausgestellt hat.

Der Eventlog wird dagegen die tatsächlichen IP-Adresse 192.168.0.214 anzeigen:



2.5 1:1 NAT auf OpenVPN und Big-LinX Schnittstellen

Geräte der IRF2000 Serie mit Firmware ab Version 2.7.0 unterstützen 1:1 NAT auch auf Schnittstellen welche auf OpenVPN basieren.

Im Folgenden ist eine Beispielkonfiguration dargestellt welche einen IP-Adresskonflikt und seine Auflösung zwischen dem Big-LinX VPN Netzwerk (hier 10.1.0.0/16) und dem Anlagennetzwerk (ebenfalls 10.1.0.0/16) darstellt.

Angenommen das Gerät erhält auf der Big-LinX VPN Schnittstelle per OpenVPN die IP-Adresse 10.1.1.66 /16 und hat auf der LAN Schnittstelle die IP-Adresse 10.1.1.20/16, so liegt zunächst ein Konflikt vor.
Im Folgenden wird nun der Big-LinX VPN IP Adressbereich aus Sicht der Anlage in das Netzwerk 172.16.0.0/26 verschoben.
Ebenfalls werden durch das „Doubled Sided Network Mapping“ die IP-Adressen des Anlagenetzwerks aus Sicht der Fernwartung in das Netzwerk 172.20.0.0/16 verschoben.

Für die Kommunikation zwischen Anlage und Kundennetzwerk ändert sich nichts.

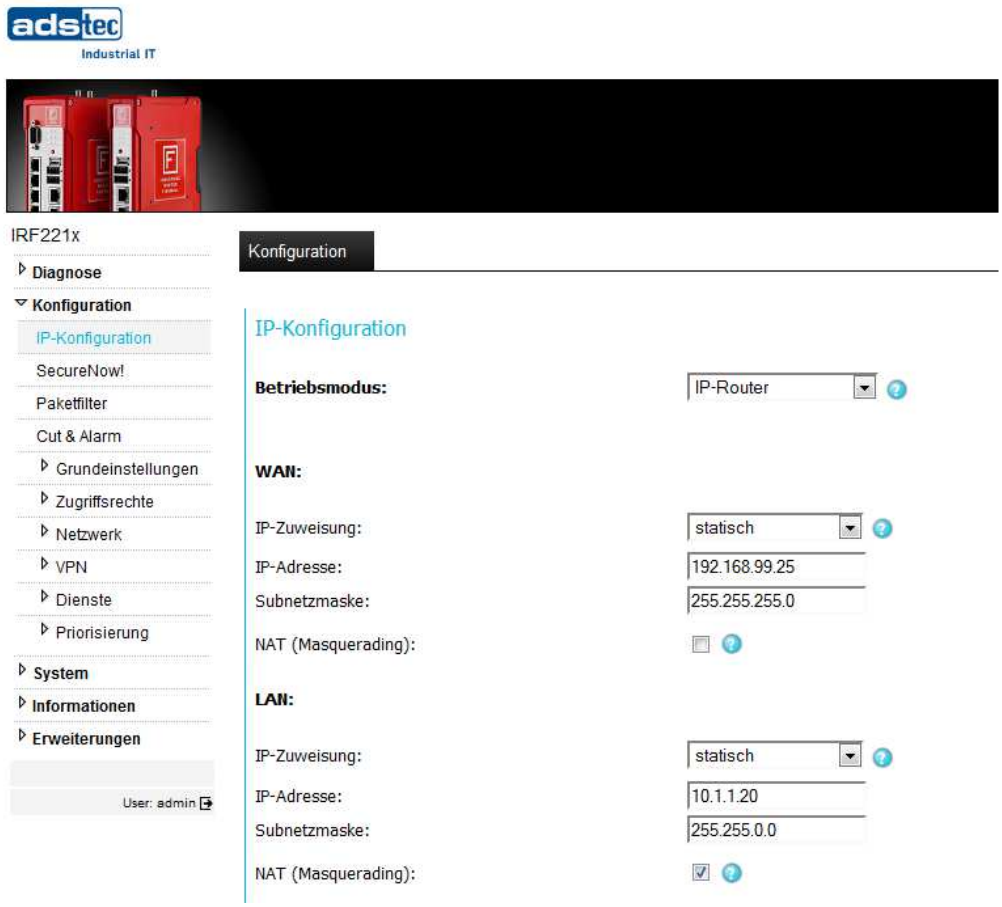


Abbildung 6: Beispiel IP-Konfiguration mit IP-Konflikt von Big-LinX und LAN

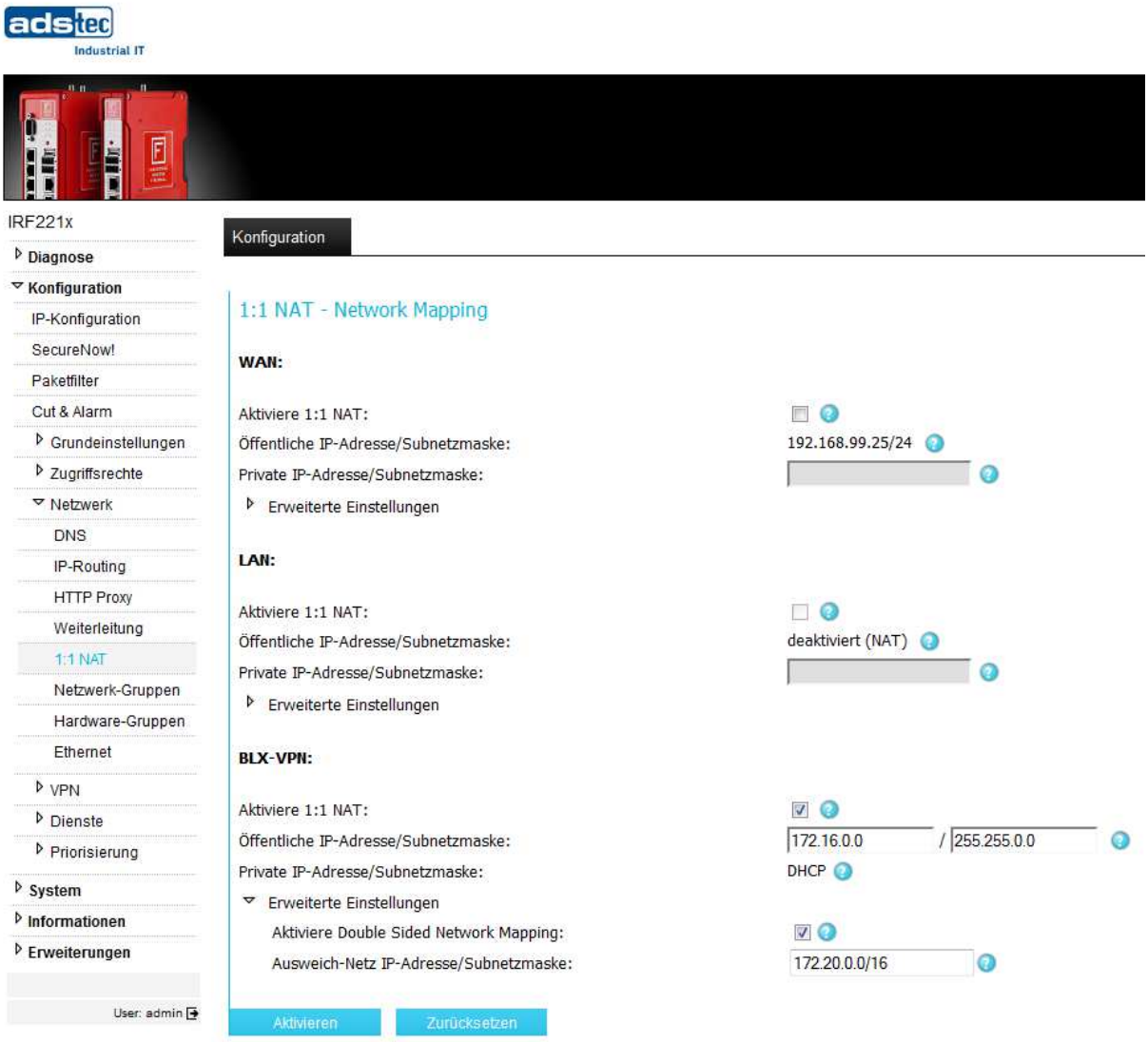


Abbildung 7: 1:1 NAT Konfiguration um den Konflikt abzufangen

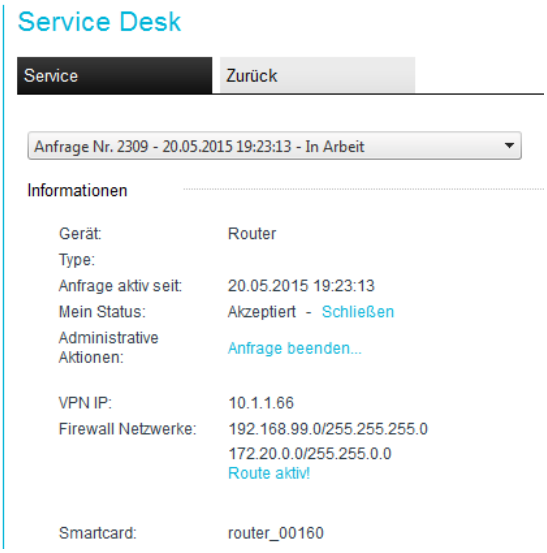


Abbildung 8: resultierende Detailansicht in Big-LinX

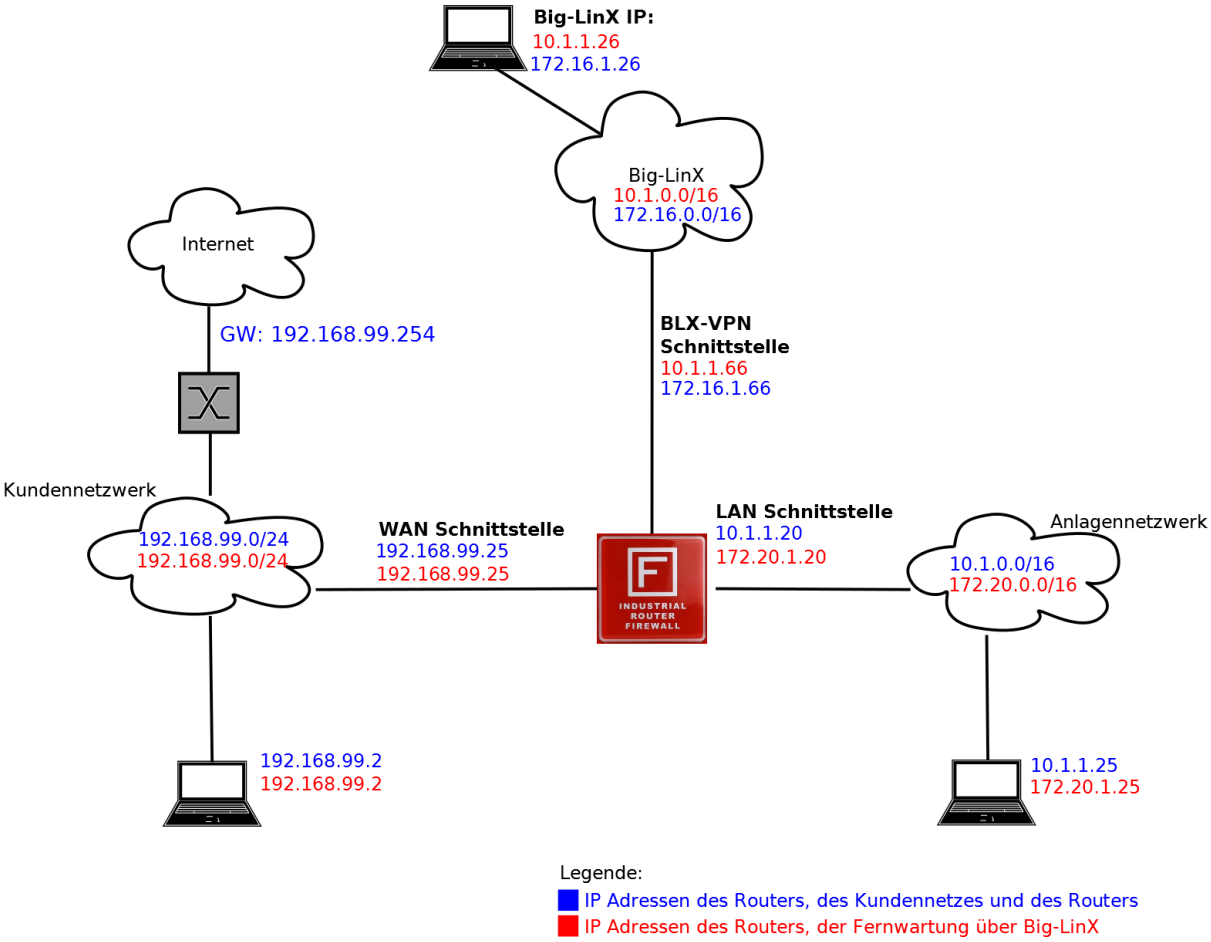


Abbildung 9: Sichtweise der IP-Adresse aus Fernwarter Perspektive und Anlagennetzwerk