ads-tec GmbH

IRF2000

Application Note
Lösung von IP-Adresskonflikten bei zwei identischen Netzwerken

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 Sie einen IP-Adresskonflikt zwischen zwei Netzwerken lösen können.
In der Praxis kann dies z.B. eine Anlage sein welche serienmäßig immer mit dem Netzwerk 192.168.0.0/24 konfiguriert wird. Nun soll diese Anlage (unverändert) bei einem Kunden installiert werden welcher unglücklicherweie das selbe Netzwerk (192.168.0.0/24) verwendet um die Anlagen in seinem Produktionsnetzwerk zu betreiben.

Im folgenden ist eine beispielhafte Netzwerkkonfiguration abgebildet welches ein solches Setup darstellt.

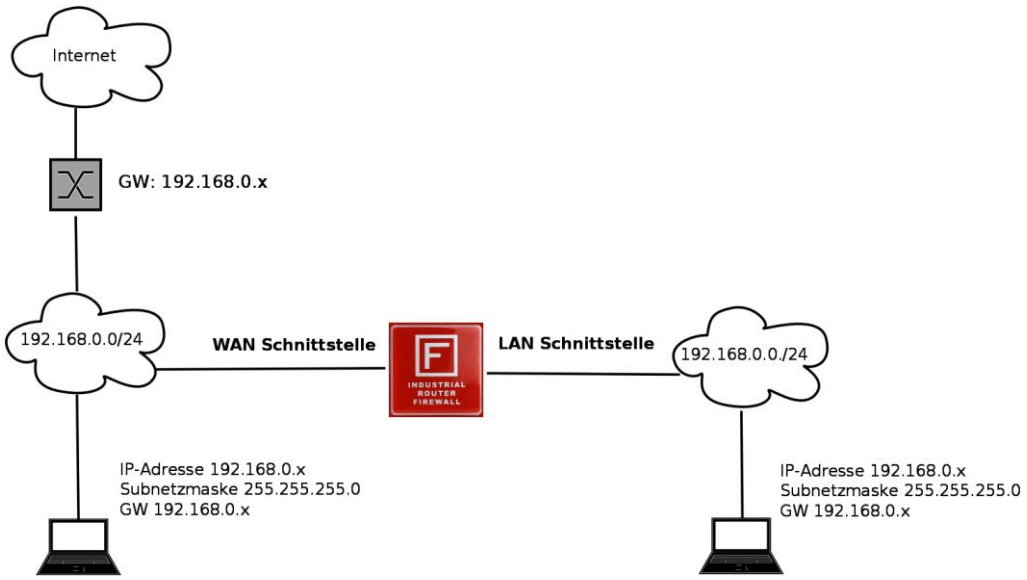

Abbildung 1: beispielhafte Netzwerkkonfiguration

Dieses Dokument erläutert nun die nötigen Schritte um die Anlage unverändert betreiben zu können und im Ergebnis ensteht ein Netzwerk welche folgenden Bedingungen erfüllt:

- Die IP-Adressen aller Anlagenkomponenten bleiben gleich
- Es ist dennoch eine direkte bidirektionale Kommunikation zwischen allen Teilnehmern beider Netze möglich.
- Eine VPN-Fernwartung über die IRF2000, egal ober mit Hilfe von IPsec, OpenVPN oder Big-LinX erfolgt auf die echten Ziel IP-Adressen des Anlagennetzwerks (192.168.0.0/24)
- Das Produktionsnetzwerk wird in einen virtuellen IP-Adressbereich verschoben, aus Sicht der Anlage und aus Sicht der Fernwartung.
- Das Anlagennetzwerk wird in einen virtuellen IP-Adressbereich verschoben, aber nur aus Sicht des Produktionsnetzwerk.

2 Private und öffentliche IP-Adressen

2.1 Auswahl der IP-Adressen

In diesem Beispiel ist das Netzwerk 192.168.0.0/24 doppelt vorhanden. Nun werden zwei virtuelle oder private Netzwerke benötigt die das jeweils andere eindeutig abbilden. Wir wählen hier:

- 172.16.0.0/24 um das Anlagennetzwerk aus Sicht des Produktionsnetzwerks abzubilden
- 172.17.1.1/24 um das Produktionsnetzwerk aus Sicht des Anlagennetzwerks, der Fernwartung und der IRF2000 abzubilden.

Diese Netze müssen lediglich die Bedingung erfüllen eindeutig zu sein. Um Verwechslungen von vorne herein auszuschließen wurde der 172er Bereich anstatt des 192er Bereiches verwendet. Aber natürlich wäre jeder freie /24 Bereich geeignet.

2.2 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 192.168.0.0/24 als privates Netzwerk angenommen und eine Abbildung auf 172.16.0.112/24 wird konfiguriert. Dann hat das Gerät im privaten Bereich die IP Adresse 192.168.0.112 und im öffentlichen „virtuellen“ Bereich die IP Adresse 172.16.0.112.
Der Präfix der öffentlichen IP-Adresse des Gerätes lautet 172.16.0 (die ersten 24 Bit sind fix, d.h. 3 Tupel a 8Bit). Das Suffix wird aus den restlichen Bits der Geräte-Adresse gebildet, also „112“. Demnach wird das Gerät auf die öffentliche IP-Adresse „172.16.0.112“ abgebildet.

Gleiches gilt für alle anderen Teilnehmer im Netzwerk, egal ob tatsächlich vorhanden oder nicht.

3 Konfiguration

3.1 IP-Konfiguration

Unter Konfiguration – IP-Konfiguration werden die IP-Adressen für das Anlagen (LAN) und Produktionsnetzwerk (WAN) eingetragen. Hierbei ist darauf zu achten das die “virtuelle“ IP-Adresse auf der Schnittstelle eingetragen werden muss bei der später 1:1 NAT aktiv geschalten ist . (siehe Abbildung 1).

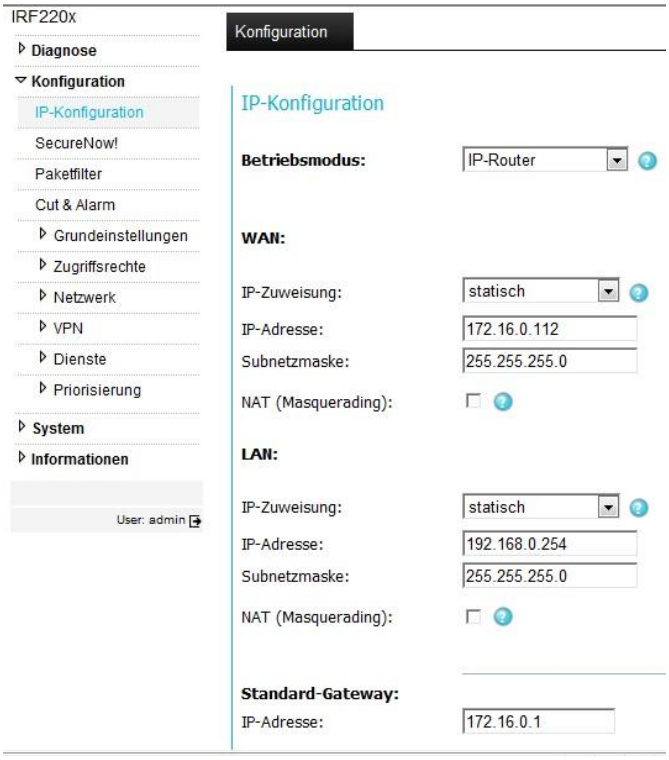

Abbildung 1: IP-Konfiguration (virtuelle IP-Adresse auf WAN)

3.2 1:1 NAT – Netzwerkabbildung in die erste Richtung

Unter „Konfiguration → Netzwerk → 1:1 NAT“ wird dann die private IP-Adresse festgelegt.

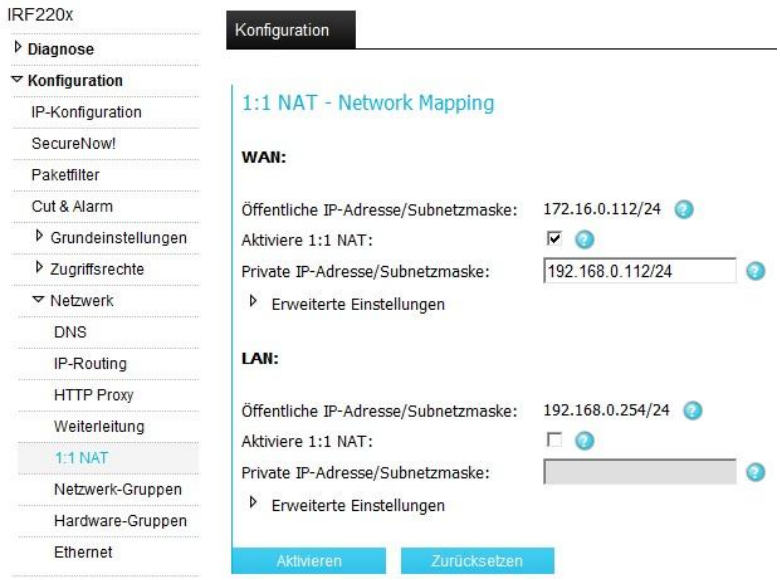

Abbildung 2: aktivieren von 1:1 NAT und Definition des privaten IP-Adressbereiche

Wir haben nun das Produktionsnetzwerk in einen virtuellen Bereich verschoben (172.16.0.0/24). Theoretisch könnten nun alle Teilnehmer im Anlagennetzwerk einen Teilnhemer im Produktionsnetzwerk über diesen Bereich adressieren.
Die jedoch würden als Quelle der Anfrage keine eindeutige IP Adresse sehen sondern eine Adresse aus dem Bereich 192.168.0.0/24, dies wäre ein Fehler.
Es muß daher jetzt noch die Abbildung in die zweite Richtung konfiguriert werden.

3.3 1:1 NAT – Netzwerkabbildung in die zweite Richtung

Hierzu muss unter 1:1 NAT bei den erweiterten Einstellungen „Double Side Network“ aktiviert und definiert werden.

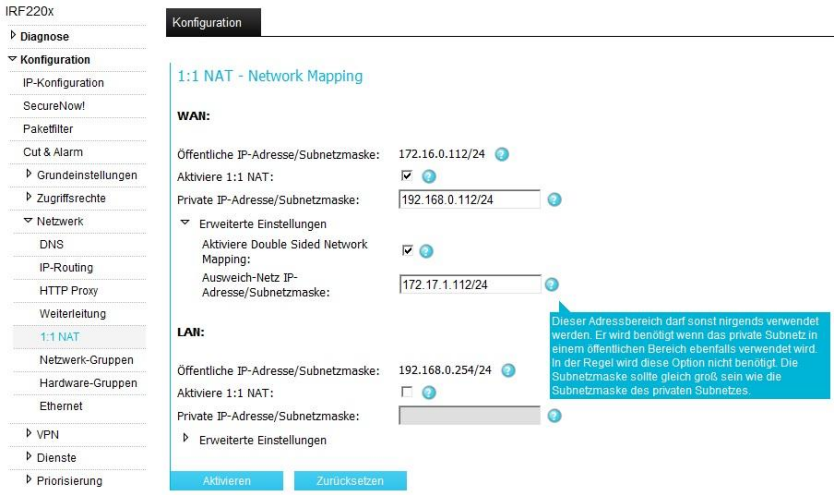

Abbildung 3: 1:1 NAT und aktiviertes Double Side Network Mapping um den Adresskonflikt von Anlagen und Produktionsnetzwerk zu umgehen.

4 IP-Adressen und Netzwerktopologie im finalen Zustand

4.1 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 ist die bekannte Netzwerktopologie gegeben wie in Abbildung 1 gezeigt. WAN ist mit 1:1-NAT / network mapping konfiguriert und WAN und LAN nutzen identische private Netze (192.168.0.0/24).
Die Firewall selbst ist erreichbar im 192.168.0.0/24 Netz. An WAN und LAN ist jeweils ein Gerät mit der IP-Adresse 192.168.0.x vorhanden. Will man nun über die Firewall hinweg mit einem dieser Geräte kommunizieren, so muss die öffentliche IP-Adresse des jeweiligen Gerätes verwendet werden.

Die nachstehenden Bilder zeigen die jeweilige Sichtweise.
Blau stellt hierbei das jeweilige öffentliche Netz dar und braun das private.