ETHERLINE® ACCESS NF04T - Industrial NAT Gateway und Firewall

Handbuch

Ausgabe 1.02 | 15.12.21 | ab Firmware V 1.10.000

U.I. Lapp GmbH | Schulze-Delitzsch-Straße 25 | 70565 Stuttgart
Phone: +49 (0)711-7838-01 | Fax: +49 (0)711-7838-2640 | info@lappkabel.de | www.lappkabel.de

Hinweise

Die jeweils aktuellste Version des Handbuchs finden Sie im Internet unter
www.lappkabel.com/activenetworkcomponents.
Wir freuen uns über Verbesserungsvorschläge und Anregungen.

Unsere Produkte enthalten unter anderem Open Source Software. Diese Software unterliegt den jeweils einschlägigen Lizenzbedingungen. Die entsprechenden Lizenzbedingungen einschließlich einer Kopie des vollständigen Lizenztextes lassen wir Ihnen mit dem Produkt zukommen. Sie werden auch in unserem Downloadbereich der jeweiligen Produkte unter www.lappkabel.com/activenetworkcomponents bereitgestellt.

Weiter bieten wir Ihnen an, den vollständigen, korrespondierenden Quelltext der jeweiligen Open Source Software gegen einen Unkostenbeitrag von Euro 10,00 als DVD auf Ihre Anfrage hin Ihnen und jedem Dritten zu übersenden. Dieses Angebot gilt für den Zeitraum von drei Jahren, gerechnet ab der Lieferung des Produktes.

Schulze-Delitzsch-Straße 25 | 70565 Stuttgart

Änderungen in diesem Dokument:

Stand	Datum	Änderung
1	31.03.2020	Erste Version / Firmware V1.08.200
1.01	30.10.2020	6.3 Ergänzung Subnetzmasken-Suffix / Firmware V1.08.400
1.02	15.12.2021	Neu: DNS-Server (Kap. 11.2)/ Neu: ICMP in Filterregeln (Kap. 6.5, 7.4)/ Neu: FTP-Helper (Kap. 7.7) / Firmware V 1.10.000

Inhalt

1 Allgemeines

Diese Betriebsanleitung gilt ausschließlich für Geräte, Baugruppen, Software und Leistungen der U. I. Lapp GmbH.

1.1 Zielgruppe des Handbuchs

Diese Beschreibung wendet sich ausschließlich an ausgebildetes Fachpersonal der Steuerungs- und Automatisierungstechnik, das mit den geltenden nationalen Normen vertraut ist. Zur Installation, Inbetriebnahme und zum Betrieb der Komponenten ist die Beachtung der Hinweise und Erklärungen dieser Betriebsanleitung unbedingt notwendig.

WARNUNG

Projektierungs-, Ausführungs- und Bedienungsfehler können den ordnungsgemäßen Betrieb der NAT / Firewall beeinträchtigen und Personen-, Sach- oder Umweltschäden zur Folge haben. Es darf nur ausreichend qualifiziertes Fachpersonal die Geräte bedienen!

Das Fachpersonal hat sicherzustellen, dass die Anwendung bzw. der Einsatz der beschriebenen Produkte alle Sicherheitsanforderungen, einschließlich sämtlicher anwendbarer Gesetze, Vorschriften, Bestimmungen und Normen erfüllt.

1.2 Sicherheitshinweise

Die Sicherheitshinweise müssen beachtet werden, um Personen und Lebewesen, materielle Güter und die Umwelt vor Schäden zu bewahren. Die Sicherheitshinweise zeigen mögliche Gefahren auf und geben Hinweise, wie Gefahrensituationen vermieden werden können.

1.3 Hinweiszeichen und Signalwörter

GEFAHR

Wenn der Gefahrenhinweis nicht beachtet wird, besteht die unmittelbare Gefahr für Gesundheit und Leben von Personen durch elektrische Spannung.

WARNUNG

Wenn der Gefahrenhinweis nicht beachtet wird, besteht die wahrscheinliche Gefahr für Gesundheit und Leben von Personen.

VORSICHT

Wenn der Gefahrenhinweis nicht beachtet wird, können Personen verletzt oder geschädigt werden.

ACHTUNG

Macht auf Fehlerquellen aufmerksam, die Geräte oder Umwelt schädigen können.

HINWEIS

Gibt einen Hinweis zum besseren Verständnis oder zur Vermeidung von Fehlern.

1.4 Bestimmungsgemäße Verwendung

Die ETHERLINE® ACCESS NF04T Industrial Bridge und Firewall (im Folgenden "das Gerät" genannt) verbindet zwei Ethernet Netzwerke.

Die gesamten Komponenten werden mit einer werkseitigen Hard- und Software-Konfiguration ausgeliefert. Die Hard- und Software-Konfiguration auf die Anwendungsbedingungen muss durch den Anwender erfolgen. Änderungen der Hard- oder Software-Konfiguration, die über die dokumentierten Möglichkeiten hinausgehen, sind unzulässig und bewirken den Haftungsausschluss der U. I. Lapp GmbH.

Das Gerät darf nicht als alleiniges Mittel zur Abwendung gefährlicher Zustände an Maschinen und Anlagen eingesetzt werden.

Der einwandfreie und sichere Betrieb des Gerätes setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus.

Die in den technischen Daten angegebenen Umgebungsbedingungen müssen eingehalten werden.

Das Gerät besitzt den Schutzgrad IP 20 und muss zum Schutz vor Umwelteinflüssen in einem elektrischen Betriebsraum oder einem Schaltkasten/Schaltschrank montiert werden. Um unbefugtes Bedienen zu verhindern, müssen die Türen der Schaltkästen/Schaltschränke während des Betriebes geschlossen und ggf. gesichert sein.

1.5 Missbrauch

WARNUNG

Die Folgen einer nicht bestimmungsgemäßen Verwendung können Personenschäden des Benutzers oder Dritter sowie Sachschäden an der Steuerung, am Produkt oder Umweltschäden sein. Setzen Sie das Gerät nur bestimmungsgemäß ein!

1.6 Montage

1.6.1 Zugangsbeschränkung

Die Baugruppen sind offene Betriebsmittel und dürfen nur in elektrischen Betriebsräumen, Schränken oder Gehäusen installiert werden.

Der Zugang zu den elektrischen Betriebsräumen, Schränken oder Gehäusen darf nur über Werkzeug oder Schlüssel möglich sein und nur unterwiesenem oder zugelassenem Personal gestattet werden.

1.6.2 Elektrische Installation

Die regional gültigen Sicherheitsbestimmungen beachten.

1.6.3 Schutz vor elektrostatischen Entladungen

Um Schäden durch elektrostatische Entladungen zu verhindern, sind bei Montage- und Servicearbeiten folgende Sicherheitsmaßnahmen zu befolgen:

- Bauteile und Baugruppen nie direkt auf Kunststoff-Gegenstände (z.B. Styropor, PE-Folie) legen und auch deren Nähe meiden.
- Vor Beginn der Arbeit das geerdete Gehäuse anfassen, um sich zu entladen.
- Nur mit entladenem Werkzeug arbeiten.
- Bauteile und Baugruppen nicht an Kontakten berühren.

1.6.4 Überstrom-Schutz

Ein Überstromschutz ist nicht erforderlich, da das Gerät keinen Laststrom führt. Die Stromversorgung der Elektronik des Gerätes ist extern mit einer Sicherung maximal 1 A (träge) abzusichern.

1.6.5 EMV-Schutz

Um die elektromagnetische Verträglichkeit (EMV) in Ihren Schaltschränken und in elektrisch rauer Umgebung sicherzustellen, sind bei der Konstruktion und dem Aufbau die bekannten Regeln des EMV-gerechten Aufbaus zu beachten.

1.6.6 Betrieb

Betreiben Sie das Gerät nur im einwandfreien Zustand. Die zulässigen Einsatzbedingungen und Leistungsgrenzen müssen eingehalten werden.

Nachrüstungen, Veränderungen oder Umbauten am Gerät sind grundsätzlich verboten.

Das Gerät ist ein Betriebsmittel zum Einsatz in industriellen Anlagen. Während des Betriebs müssen alle Abdeckungen am Gerät und der Installation geschlossen sein, um den Berührungsschutz zu gewährleisten.

1.6.7 Haftung

Der Inhalt dieser Bedienungsanleitung unterliegt technischen Änderungen, die durch die ständige Weiterentwicklung der Produkte der U. I. Lapp GmbH entstehen. Für den Fall, dass diese Bedienungsanleitung technische Fehler oder Schreibfehler enthält, behalten wir uns das Recht vor, Änderungen jederzeit und ohne Ankündigung durchzuführen.

Aus den Angaben, Abbildungen und Beschreibungen in dieser Dokumentation können keine Ansprüche auf Änderung bereits gelieferter Produkte gemacht werden. Über die in der Bedienungsanleitung enthaltenen Anweisungen hinaus sind in jedem Fall die gültigen nationalen und internationalen Normen und Vorschriften zu beachten.

1.6.8 Haftungsausschluss

Die U. I. Lapp GmbH haftet nicht bei Schäden, wenn diese durch nicht bestimmungs- oder sachgemäße Benutzung oder Anwendung der Produkte verursacht wurden.

Die U. I. Lapp GmbH übernimmt keine Haftung für eventuell in der Bedienungsanleitung enthaltene Druckfehler oder sonstige Ungenauigkeiten, es sei denn, es sind gravierende Fehler, die U. I. Lapp GmbH nachweislich bereits bekannt sind.

Über die in der Bedienungsanleitung enthaltenen Anweisungen hinaus sind in jedem Fall die gültigen nationalen und internationalen Normen und Vorschriften zu beachten.

Die U. I. Lapp GmbH haftet nicht bei Schäden, die durch Software, die auf Geräten des Anwenders aktiv ist und über die Fernwartungsverbindung weitere Geräte oder Prozesse beeinträchtigt, schädigt oder infiziert und unerwünschten Datentransfer auslöst oder ermöglicht.

1.6.9 Gewährleistung

Melden Sie Mängel sofort nach Feststellung des Fehlers beim Hersteller an.

Die Gewährleistung erlischt bei:

- Missachtung dieser Betriebsanleitung
- Nicht bestimmungsgemäßer Verwendung des Geräts
- Unsachgemäßem Arbeiten an und mit dem Gerät
- Bedienungsfehlern
- Eigenmächtigen Veränderungen am Gerät

Es gelten die bei Vertragsabschluss unter „Allgemeine Geschäftsbedingungen der Firma U. I. Lapp GmbH“ getroffenen Vereinbarungen.

2 Security Empfehlungen

ETHERLINE® ACCESS NF04T ist eine Netzwerkinfrastruktur Komponente und damit ein wichtiges Element in der Security Betrachtung einer Anlage oder eines Netzwerkes. Beachten Sie bei der Verwendung des ETHERLINE® ACCESS NF04T deshalb folgende Empfehlungen, um nicht autorisierte Zugriffe auf Anlagen und Systeme zu unterbinden.

Allgemein:

- Stellen Sie in regelmäßigen Abständen sicher, dass alle relevanten Komponenten diese Empfehlungen und ggf. weitere interne Sicherheits-Richtlinien erfüllen.
- Bewerten Sie Ihre Anlage ganzheitlich im Hinblick auf Sicherheit. Nutzen Sie ein Zellenschutzkonzept mit entsprechenden Produkten, wie z.B. dem ETHERLINE® ACCESS NF04T.

Umfangreiche Informationen erhalten Sie z.B. im "ICS-Security-Kompendium" vom Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf

Physischer Zugang:

- Beschränken Sie den physischen Zugang zu sicherheitsrelevanten Komponenten auf qualifiziertes Personal.

Sicherheit der Software:

- Halten Sie die Firmware alle Kommunikationskomponenten immer aktuell.
- Informieren Sie sich regelmäßig über Firmware Updates für das Produkt. Informationen hierzu finden Sie unter: www.lappkabel.com/activenetworkcomponents
- Aktivieren Sie nur Protokolle und Funktionen, die Sie wirklich benötigen

Passwörter:

- Definieren Sie Regeln für die Nutzung der Geräte und die Vergabe von Passwörtern.
- Aktualisieren Sie regelmäßig Passwörter und Schlüssel
- Ändern Sie Standard-Passwörter für
- Verwenden Sie ausschließlich Passwörter mit hoher Passwortstärke. Vermeiden Sie schwache Passwörter wie z. B. "passwort1", "123456789" oder dergleichen.
- Stellen Sie sicher, dass alle Passwörter geschützt und unzugänglich für unbefugtes Personal sind.
- Verwenden Sie ein Passwort nicht für verschiedene Benutzer und Systeme.

3 Übersicht

ETHERLINE® ACCESS NF04T, die Industrial NAT Gateway und Firewall, integriert Maschinennetze auf einfache Weise in das übergeordnete Produktionsnetz mittels Netzwerksegmentierung, Paket- und MAC-Adressen Filterung.

Der **NAT-Betriebsmodus** dient zur Weiterleitung des Datenverkehrs zwischen verschiedenen IPv4-Netzwerken. Er ermöglicht die Adressübersetzung mittels NAT und nutzt Paketfilter für die Zugriffsbeschränkung auf das dahinterliegende Automatisierungsnetzwerk.

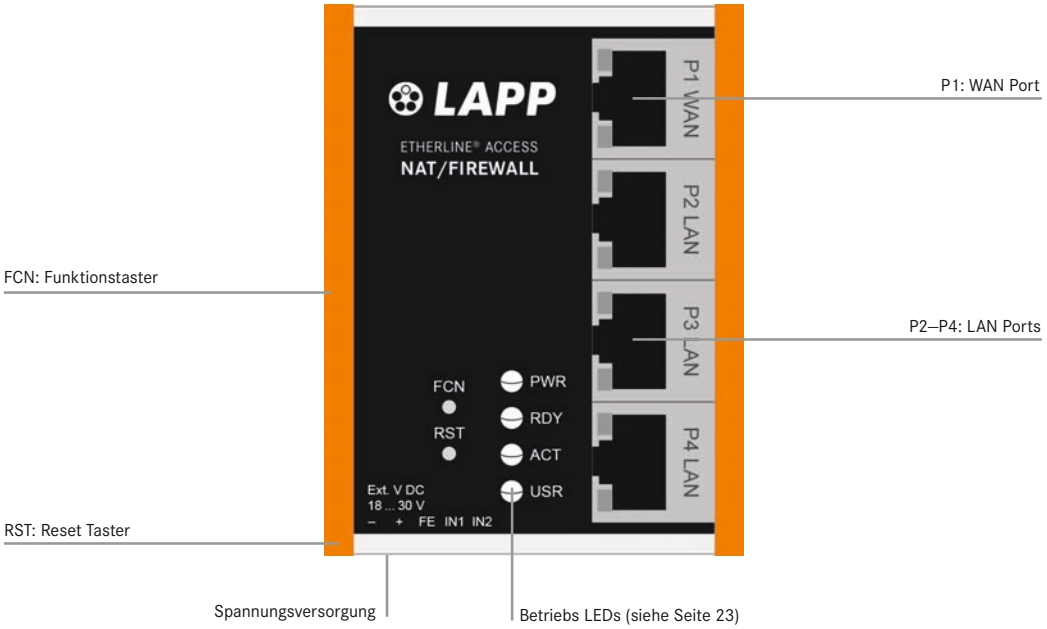
Im **Bridge-Betriebsmodus** agiert ETHERLINE® ACCESS NF04T Netzwerkbrücke in einem IPv4-Subnetzt. Im Gegensatz zu normalen Switches, ist in dieser Betriebsart die Paketfilterung möglich. Dadurch kann die Einschränkung des Zugriffs zu einzelnen Bereichen ihres Netzwerkes erreicht werden, ohne dass hierfür unterschiedliche Netzwerke verwendet werden müssen.

Die Features des ETHERLINE® ACCESS NF04T:

- NAT (Basic NAT, SNAT, NAPT und Portforwarding) zur Netzwerksegmentierung
- Bridge-Funktionalität für Absicherung von Netzwerbereichen mit identische IPv4-Adressbereiche
- Zugriffsbeschränkung durch Paketfilter: IPV4-Adressen, Protokoll (TCP/UDP), Ports
- MAC-Adressen Filterung mit Black und Whitelisting
- DHCP-Server (LAN), DHCP-Client (WAN)
- Schnelle und einfache Konfiguration durch responsive Webinterface
- Statische Routen zu anderen Netzwerken
- Melden von Ereignissen an einen Syslog Server
- Export/Import der Konfiguration
- Industrietaugliche Bauform zur Hutschienenmontage

3.1 Aufbau

Der ETHERLINE® ACCESS NF04T hat einen 100Mbit WAN-Port (P1) und drei 100 Mbit LAN-Ports (P2-P4, geswitcht).

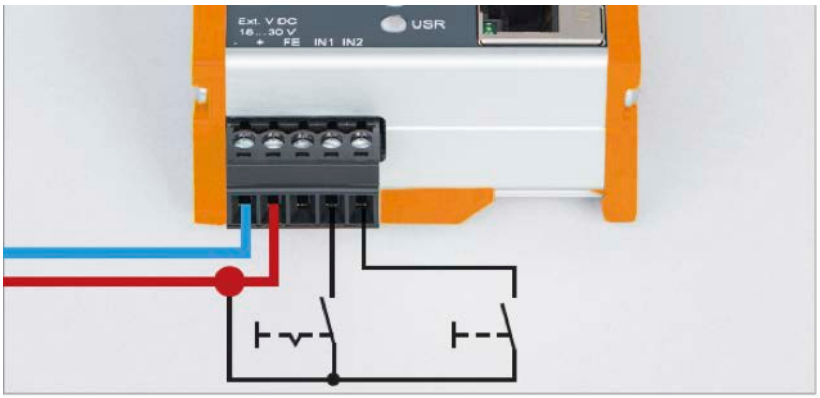


Über den Funktionstaster (FCN) kann ein Rückstellen auf Werkseinstellungen durchgeführt werden (siehe Kap. 12). Der Reset Taster (RST) führt einen Neustart des ETHERLINE® ACCESS NF04T aus.

3.2 Anschluss der Spannungsversorgung

Der ETHERLINE® ACCESS NF04T muss, am Weitbereichseingang 18–30 V DC über den mitgelieferten Anschlussstecker, mit DC 24 V versorgt werden. Der Anschluss (FE) ist für die Funktionserde. Verbinden Sie diese ordnungsgemäß mit dem Bezugspotential.

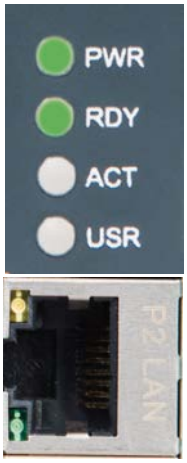
Die RJ45 Buchse „P1 WAN“ dient zum Anschluss des externen Netzwerks. Die RJ45 Buchsen „P2 LAN–P4 LAN“ sind geswitcht und dienen zum Anschluss des internen Netzwerks.



Die Eingänge IN1 und IN2 haben in der aktuellen Firmwareversion noch keine Funktion, werden in einer späteren Firmwareversion zum externen Schalten von Firewall Regeln zur Verfügung stehen.

3.3 LEDs Statusinformationen

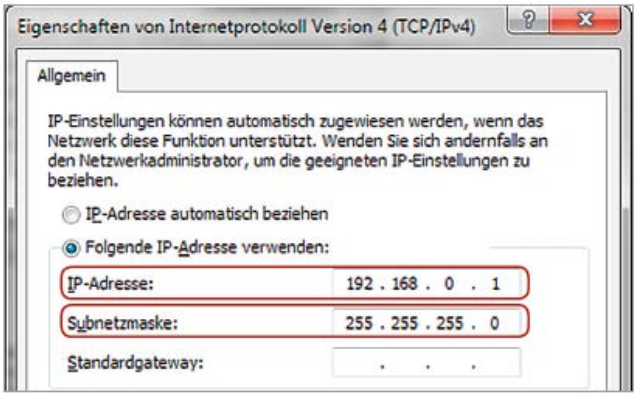
PWR	**Aus**	**Keine Spannungsversorgung oder Gerät defekt**
	Ein	**Gerät ist korrekt mit Spannung versorgt**
RDY	**Ein**	**Gerät ist betriebsbereit**
ACT	**Blinkt oder An**	**Erlaubter Datenverkehr zwischen WAN und LAN**
USR	**Blinkt**	**Rücksetzen auf Werkseinstellung aktiviert**
RJ45 LEDs	**Grün (Link)**	**Verbunden**
	Orange (Act)	**Datenübertragung am Port**



4 Erster Zugriff auf das Webinterface

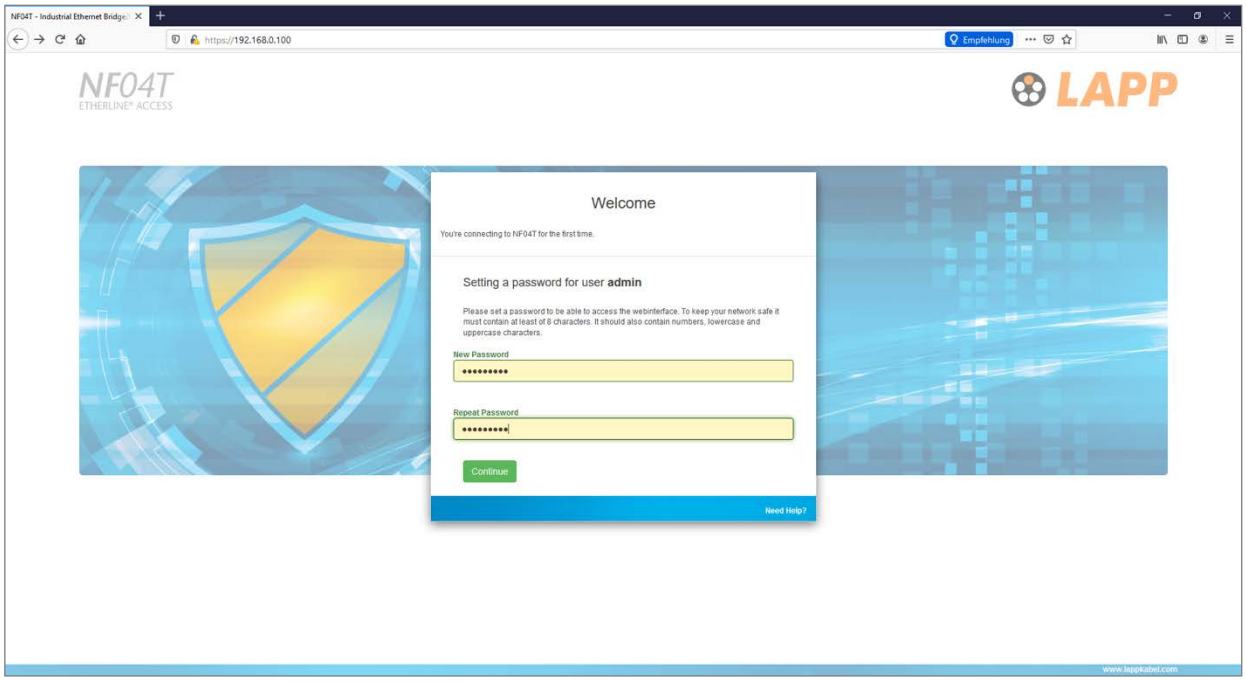
Der ETHERLINE® ACCESS NF04T wird ab Werk LAN-seitig mit der IP-Adresse 192.168.0.100 und der Subnetzmaske 255.255.255.0 ausgeliefert. Der Zugriff auf das Webinterface ist nur über die LAN-Anschlüsse P2–P4 möglich.

Zuerst muss die IP-Adresse ihrer Netzwerkkarte entsprechend dem IP-Subnetz des ETHERLINE® ACCESS NF04T eingestellt werden:
Start → Systemsteuerung →
Netzwerk- und Freigabeeinstellungen →
Adaptereinstellungen →
LAN-Verbindungseigenschaften →
Internet Protokoll Version 4



Verbinden sie nun ein Patchkabel mit dem LAN-Anschluss ihres PCs und einem der LAN-Ports P2 bis P4 des ETHERLINE® ACCESS NF04T.

Das Webinterface kann im Auslieferungszustand durch Aufruf von "**https://192.168.0.100**" in der Browserleiste erreicht werden.



HINWEIS

Das Webinterface ist aus Sicherheitsgründen ausschließlich über eine gesicherte HTTPS-Verbindung zu erreichen. Um die Webseite zu erreichen, muss einmalig eine Ausnahmeregel im Browser bestätigt werden. Im Menü „Device/HTTPS“ kann bei Bedarf ein eigenes Zertifikat für die Verbindungssicherung hinterlegt werden.

4.1 Erstanmeldung

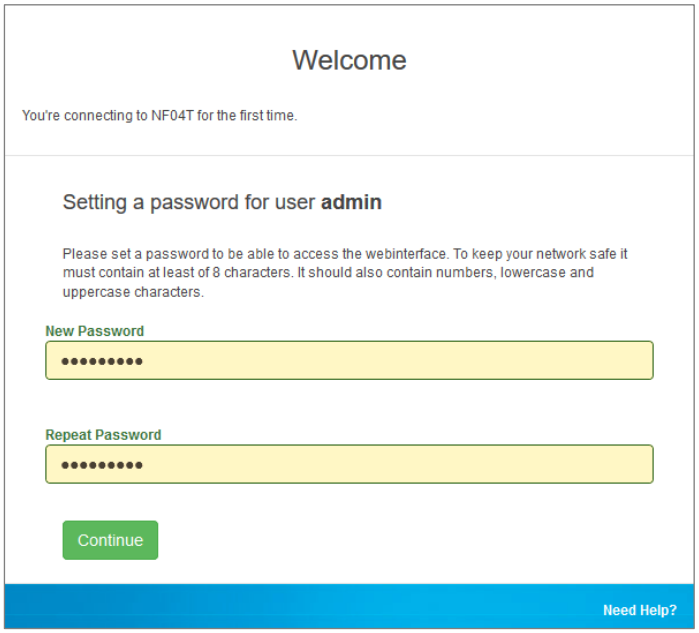
Bei der Erstanmeldung werden sie aufgefordert ein Passwort festzulegen.

Das Passwort muss mindestens 8 Zeichen enthalten und darf maximal 128 Zeichen lang sein, es kann Sonderzeichen und Ziffern enthalten. Mit dem Button „Continue“ wird das Passwort im Gerät gespeichert und Sie werden auf die „Overview“ Seite des ETHERLINE® ACCESS NF04T weitergeleitet.

Der Haupt-User ist immer „admin“.

Neben dem Haupt-User „admin“ können noch die User „it-user“ und „machine-user“ mit eingeschränkten Rechten verwendet werden.

Die User können im Menü „Device/Password“ aktiviert und zugehörige Passworte eingestellt werden.

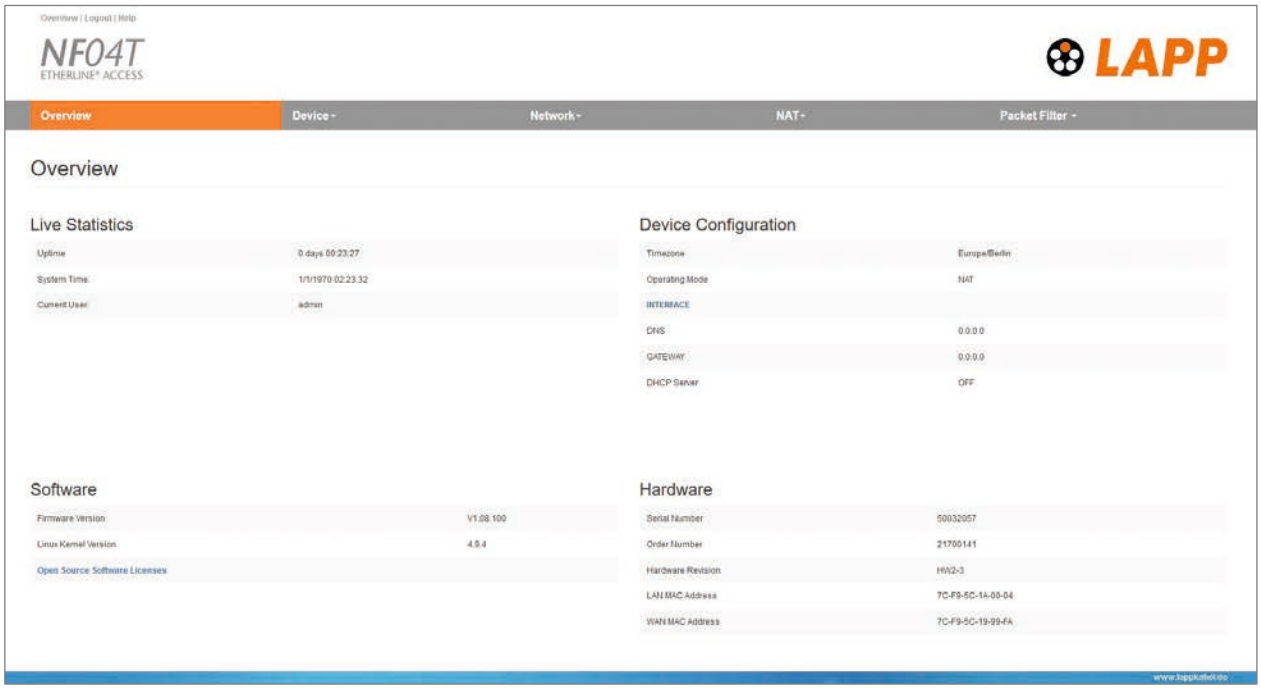


ACHTUNG

Bitte prägen Sie sich das Passwort gut ein! Aus Sicherheitsgründen gibt es keine Möglichkeit das Passwort zurückzusetzen, ohne das Gerät auf Werkseinstellungen zu setzen.

4.2 Hauptansicht

Nach dem Login öffnet sich immer die „Overview“ Webseite des ETHERLINE® ACCESS NF04T. Die Hauptansicht "Overview" enthält eine Übersicht der wichtigsten Einstellungen und Informationen des ETHERLINE® ACCESS NF04T.
In der obersten Zeile befindet sich das Menü mit den Funktionen zur Konfiguration.

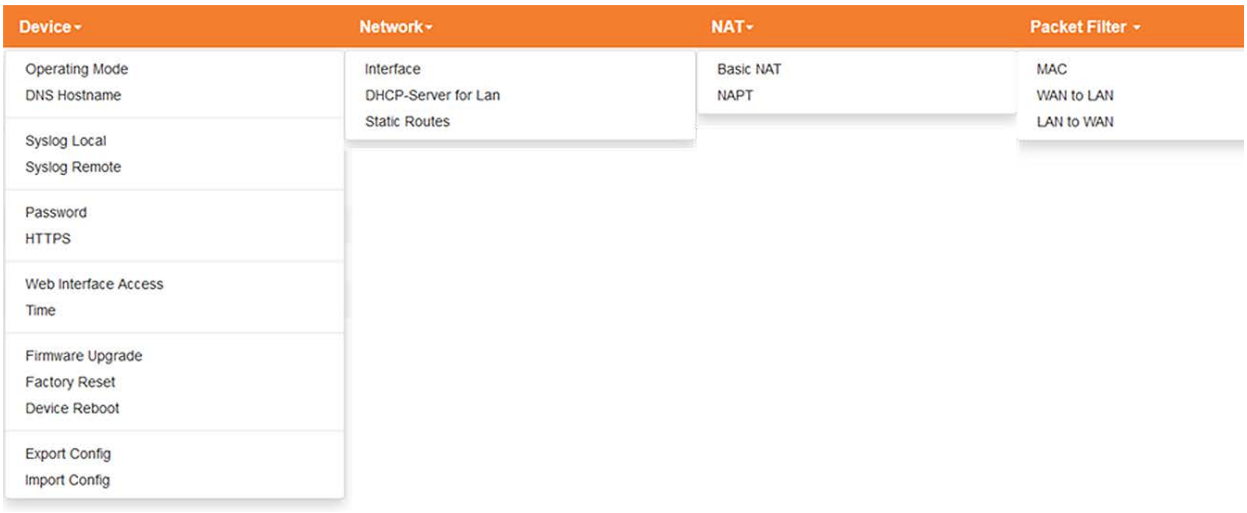


HINWEIS

Bitte prüfen Sie auf der Webseite des ETHERLINE® ACCESS NF04T, ob es eine neuere Firmwareversion gibt. Das Firmwareupdate ist im Kapitel 12 beschrieben.

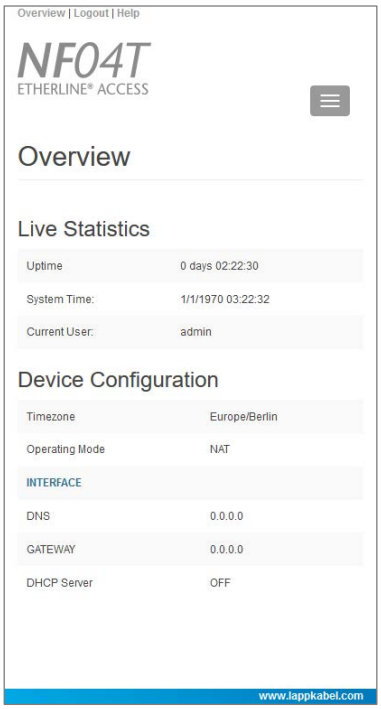
Link zur Landingpage:
www.lappkabel.com/activenetworkcomponents

4.2.1 Menü Übersicht



4.2.2 Responsive Design

Das Webinterface ist auch geeignet für die Verwendung auf Tablets und Smartphones ("Responsive Design").



HINWEIS

Bitte beachten Sie, dass der Webzugriff auf den ETHERLINE® ACCESS NF04T aus Sicherheitsgründen mit einer Inaktivitätsüberwachung versehen ist. Wenn die Webseite für einige Minuten nicht verwendet wird, findet ein automatisches "Ausloggen" statt.

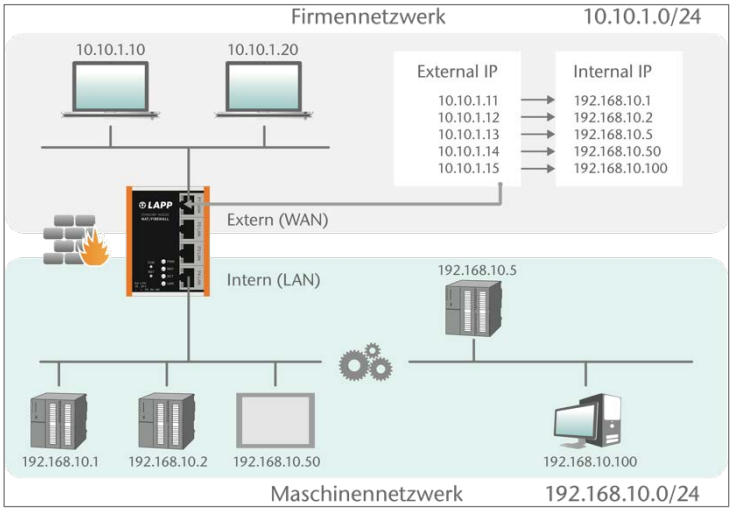
5 Wahl der Betriebsart

Abhängig von Anwendungsfall für den ETHERLINE® ACCESS NF04T muss zu Beginn die Betriebsart festgelegt werden. ETHERLINE® ACCESS NF04T unterstützt zwei grundsätzliche Betriebsarten: NAT und Bridge

5.1 Der NAT Betriebsmodus

Wenn eine Automatisierungszelle mit voreingestellten IP-Adressen in ein Produktionsnetzwerk mit anderen IP-Adressen eingebunden werden soll, dann müssen normalerweise die IP-Adressen der Maschine alle neu eingestellt werden.

Unter Verwendung von Network Address Translation (NAT) bietet ETHERLINE® ACCESS NF04T die Möglichkeit, die IP Adressen der Maschine zu belassen aber die Kommunikation zum Maschinennetzwerk mit eigenen IP-Adressen aus dem Produktions-netzwerk zu ermöglichen.



Im NAT-Betriebsmodus leitet ETHERLINE® ACCESS NF04T den Datenverkehr zwischen verschiedenen IPv4-Netzwerken weiter (Layer 3) und setzt die IP-Adressen mithilfe von NAT um.

Zusätzlich können Paketfilter und MAC-Adressen Filter zur Einschränkung des erlaubten Datenverkehrs verwendet werden.

Broadcasts-Traffic wird generell am ETHERLINE® ACCESS NF04T gefiltert, somit wird das Zeitverhalten des Maschinen-netzwerks nicht durch das Produktionsnetzwerk beeinträchtig.

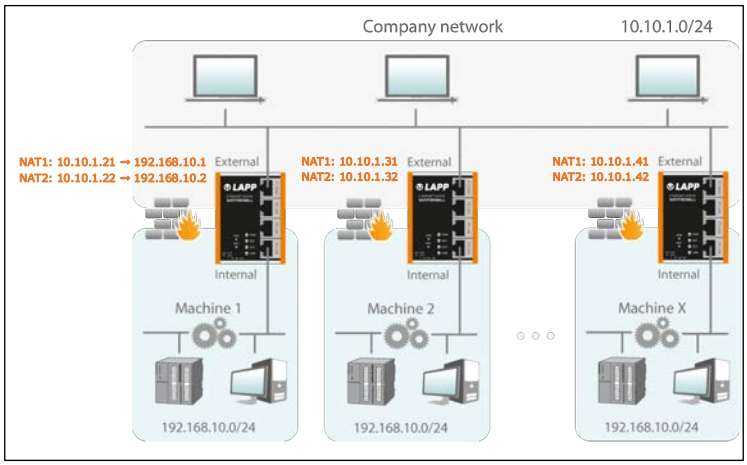
Basic NAT, auch “1:1 NAT” oder “Static NAT” genannt, ist die Übersetzung von einzelnen IP-Adressen oder von ganzen IP-Adressbereichen.

Mithilfe von Portweiterleitungen („**Portforwarding**“) kann alternativ konfiguriert werden, dass Pakete an einen bestimmten TCP/UDP-Port des ETHERLINE® ACCESS NF04T an einen bestimmten Teilnehmer im Maschinennetzwerk (LAN) weitergeleitet werden.

Der NAT Betriebsmodus erlaubt es somit auch, mehrere Automatisierungszellen, die einen gleichen IP-Adress-bereich verwenden, in dasselbe Produktionsnetzwerk zu integrieren.

Jeder Automatisierungszelle können hierbei unterschiedliche freie IP-Adresse aus dem Produktionsnetzwerk zugewiesen werden.

Wenn „NAT“ Ihr geplanter Anwendungsfall ist, dann lesen Sie bitte im Kapitel 6 weiter.

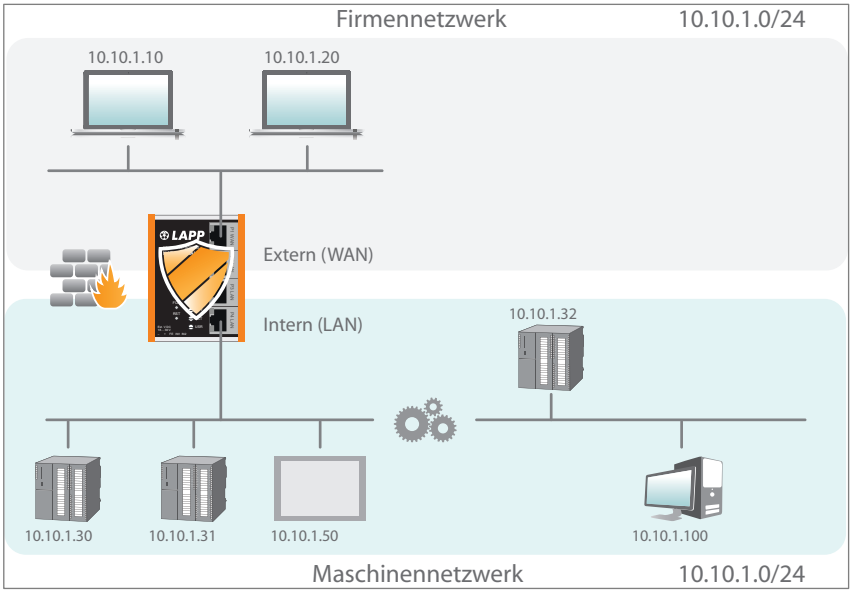


5.2 Der Bridge-Betriebsmodus

Im Bridge Betriebsmodus verhält sich ETHERLINE® ACCESS NF04T wie ein Layer 2 Switch zwischen dem Maschinennetzwerk (Automatisierungszelle) und dem Produktionsnetzwerk. Die IP-Adressen im Produktionsnetzwerk sind hierbei im gleichen IP-Adressraum (Subnetz) wie die Adressen im Maschinennetzwerk.

Durch Paketfilter und MAC-Adressen Filter kann der Zugriff zwischen den beiden Netzwerkbereichen eingeschränkt bzw. abgesichert werden.

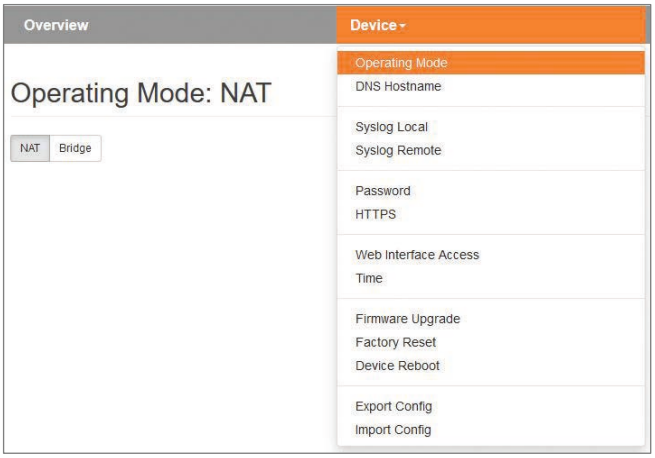
Dies erlaubt die Abtrennung eines Teils des Produktionsnetzwerkes ohne die Verwendung von unterschiedlichen Netzwerk-Adressen.



Wenn „Bridge“ Ihr gewünschter Anwendungsfall ist, dann lesen Sie bitte im Kapitel 7 weiter.

6 Anwendungsfall NAT

Zur Aktivierung des NAT Betriebsmodus wählen Sie im Menü „Device“ den Menüpunkt „Operating Mode“ und stellen diesen auf „NAT“.



6.1 Anpassen der IP-Adressen im NAT-Betriebsmodus

Klicken Sie auf das Menü „Network“ und wählen das Untermenü „Interface“ aus. Hier können die IP-Adressen des ETHERLINE® ACCESS NF04T im WAN und im LAN („WAN IP“/“LAN IP“) sowie die zugehörigen Subnetzmasken („WAN netmask“/LAN netmask“) festgelegt werden.

Ein DNS-Server und ein Default-Gateway können ebenfalls angegeben werden. Das ist notwendig, wenn Geräte aus dem LAN über den ETHERLINE® ACCESS NF04T das Internet erreichen sollen. Werden diese nicht angegeben ("0.0.0.0"), dann wird verhindert, dass Geräte im LAN mit dem Internet kommunizieren.

Optional können die WAN-IP-Einstellungen, der DNS-Server und das Standard Gateway auch per DHCP bezogen werden.

Die Eingabe wird mit dem Button „Submit“ gespeichert und die IP-Einstellungen werden dann sofort aktiviert. Mit "Decline" wird die aktuelle Eingabe ohne Übernahme verworfen.

Ein DNS-Server kann bei Bedarf ebenfalls angegeben werden. Für den SNTP-Dienst ist die Angabe eines DNS-Servers notwendig (siehe Kap. 11.8).

ACHTUNG

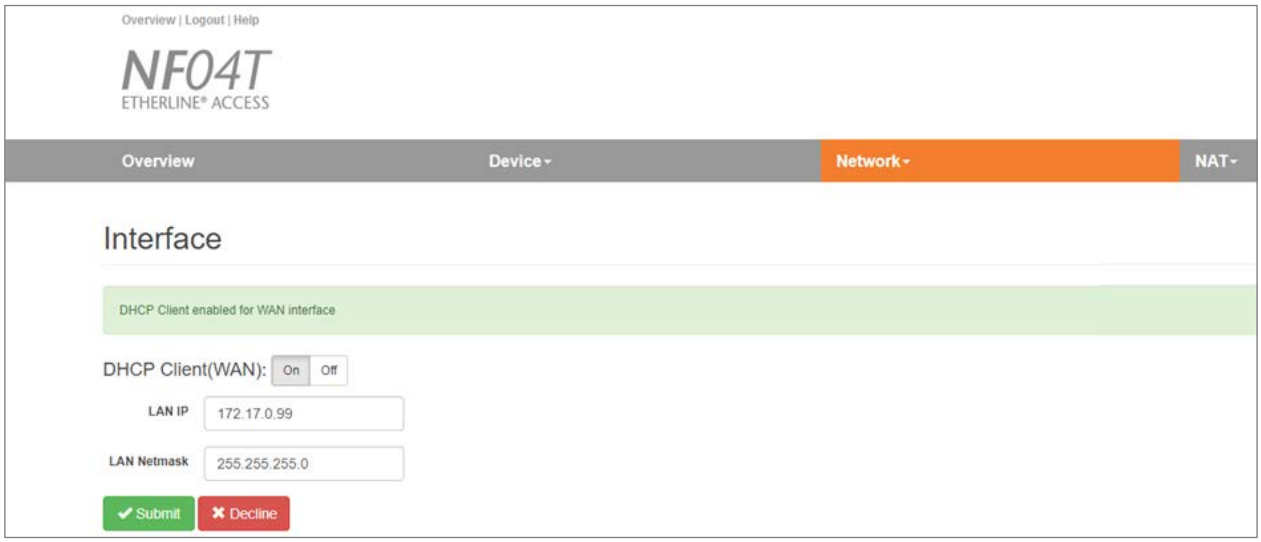
Wenn Sie die LAN IP-Adresse verändern, müssen Sie ggf. am Browser die Webseite des ETHERLINE® ACCESS NF04T unter der neuen IP-Adresse erneut öffnen und sich wieder einloggen.

HINWEIS

Der ETHERLINE® ACCESS NF04T hat immer nur eine aktive Konfiguration. Änderungen an der Konfiguration werden immer sofort aktiv. Ein Neustart des ETHERLINE® ACCESS NF04T ist bei Änderung der Konfiguration nicht notwendig.

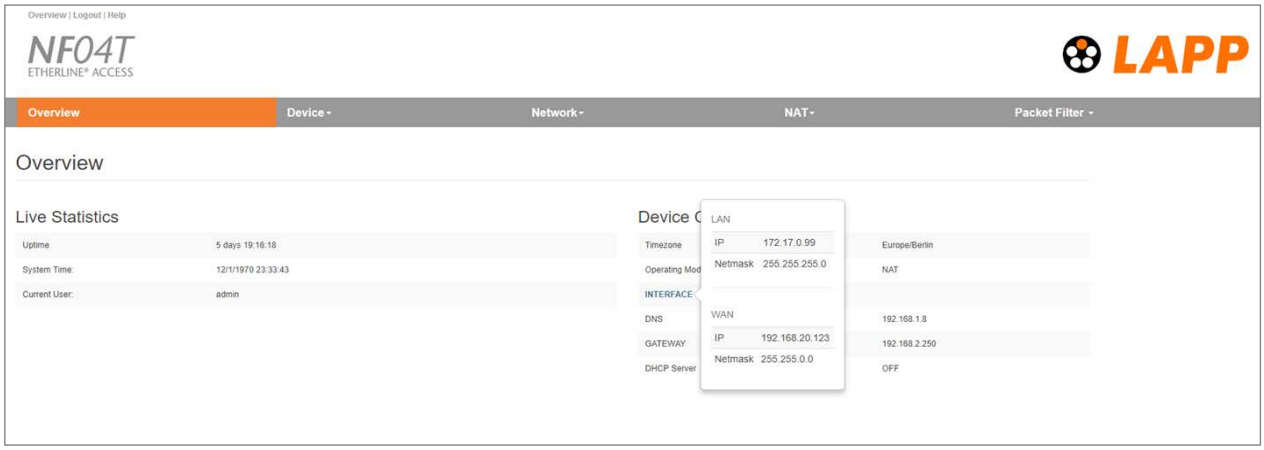
6.2 DHCP-Client am WAN-Interface aktivieren

Alternativ zur Angabe der IP-Adresse kann auch für das WAN-Interface auch ein DHCP-Client aktiviert werden.



Die Verwendung des DHCP-Clients setzt voraus, dass im WAN-Netzwerk ein DHCP-Server aktiv ist.

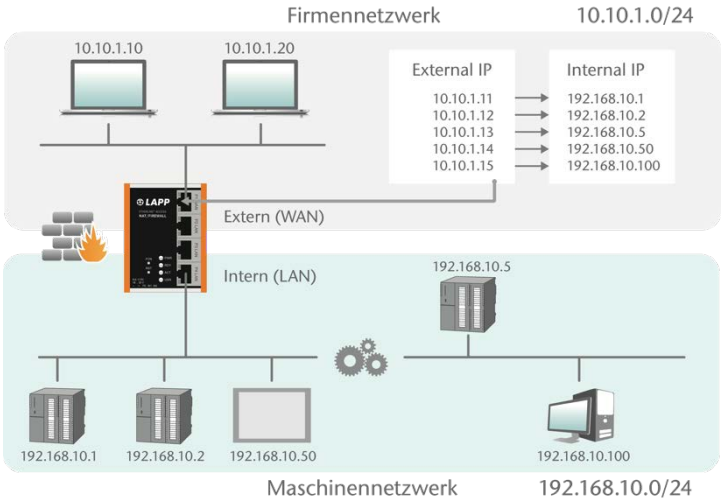
Die vom DHCP-Client bezogenen IP-Einstellungen sind auf der Overview-Seite durch Klick auf "INTERFACE" sichtbar.

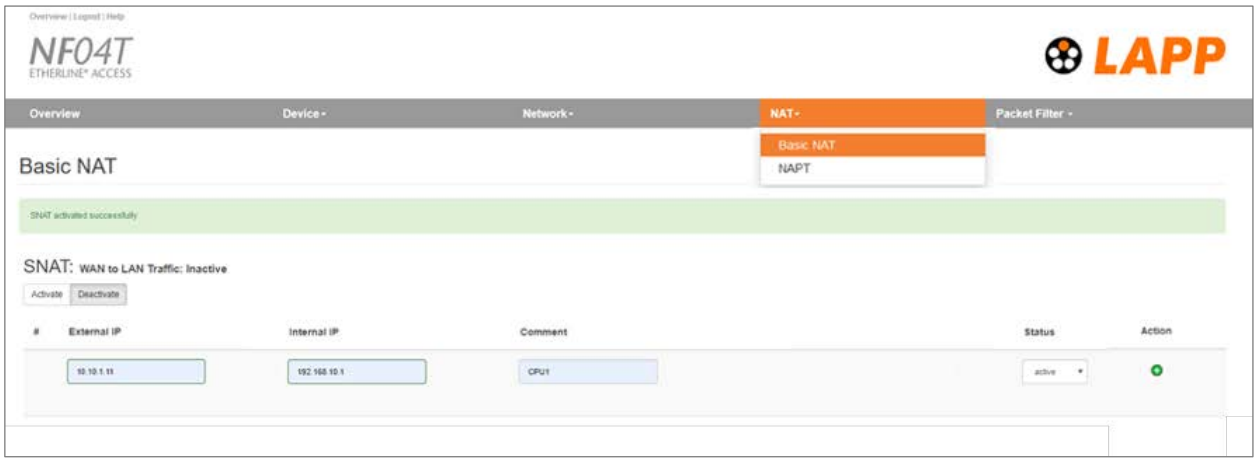


6.3 Einrichtung von „Basic NAT“ Regeln

Um Basic-NAT-Funktionalitäten nutzen zu können, muss die Betriebsart des ETHERLINE® ACCESS NF04T auf "NAT" eingestellt sein.

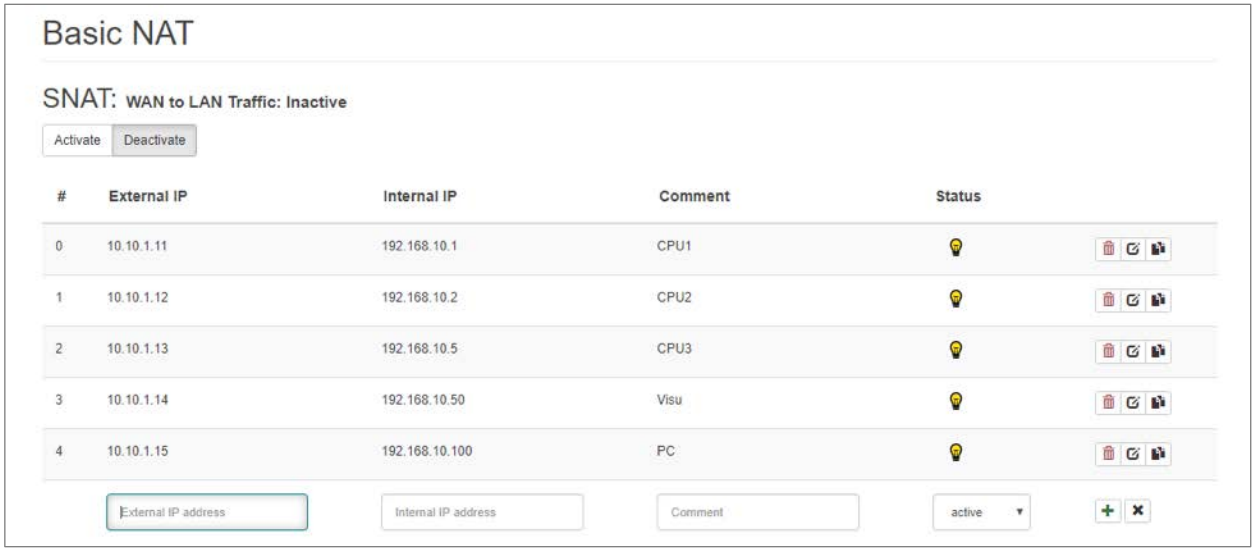
Wählen Sie dann das Menü „NAT“ und das Untermenü „Basic NAT“ aus. Tragen Sie die erste Regel ein und speichern Sie diese mit dem Button .





Die „External IP“ ist die IP-Adresse unter der der Netzwerkteilnehmer der Maschine im Firmennetzwerk (WAN) sichtbar wird. Die „Internal IP“ ist die IP-Adresse des Teilnehmers im Maschinennetzwerk (LAN). Als Kommentar kann ein beliebiger Text eingegeben werden.

Jeder Eintrag wird mit der Nachricht „Rule added successfully“ bestätigt.



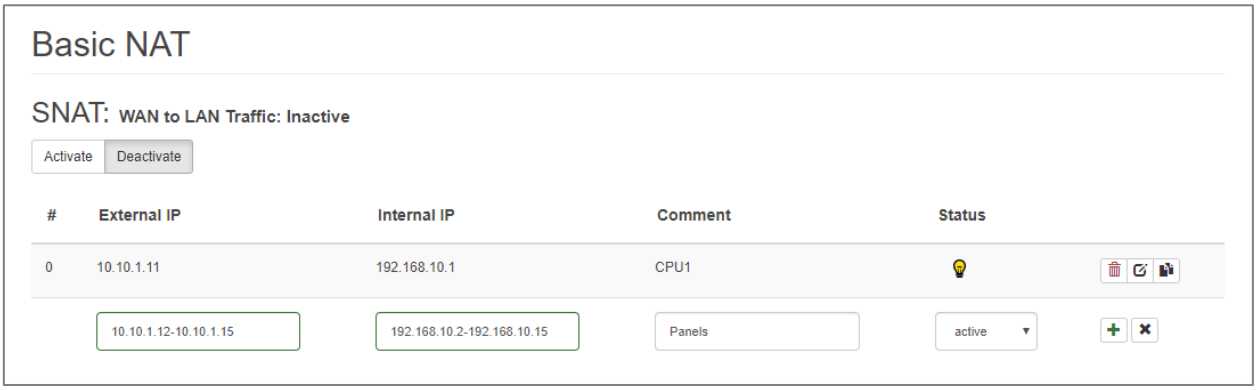
Status: = Regel ist aktiv; Ein Klick auf das Lampensymbol ändert den Regelstatus in Inaktiv

= Regel ist inaktiv: Ein Klick auf das Lampensymbol ändert den Regelstatus in Aktiv

Mögliche Aktionen:

löschen einer Regel bearbeiten einer Regel kopieren einer Regel

Es können auch Bereiche von IP-Adressen in einer NAT-Regel definiert werden, wenn die Geräte hintereinander liegende IP-Adressen haben.



Die Verwendung eines Subnetzmasken-Suffixes zur Beschreibung eines ganzen IP-Bereiches ist an dieser Stelle ebenfalls möglich: „10.10.2.1/24“ definiert eine NAT-Regel für alle IP-Adressen von 10.10.2.0 bis 10.10.2.255.

ACHTUNG

Bei einer "Basic NAT" Regel sind aus Sicherheitsgründen zuerst alle Ports für den „WAN-to-LAN“ Datenverkehr bei dieser Regel gesperrt!

Um Zugriffe zu erlauben, müssen Paketfilter-Regeln erstellt oder die "Default Action" bei den Paket-Filtern auf „Accept“ gestellt werden. Siehe folgendes Kapitel.

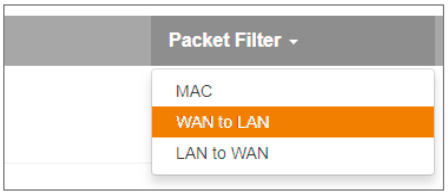
Der Datenverkehr „LAN to WAN“ ist per default immer freigegeben, kann aber ebenfalls durch Paket-Filter oder die Default Action eingeschränkt werden.

HINWEIS

Es können maximal 128 Basic NAT Einträge definiert werden.

6.4 Paketfilter „WAN to LAN“

Mit den Paketfiltern lässt sich der Zugriff zwischen dem Produktionsnetzwerk (WAN) und dem Maschinennetzwerk (LAN) einschränken.



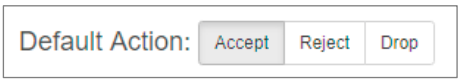
Es kann beispielsweise konfiguriert werden, dass nur bestimmte Teilnehmer aus dem Produktionsnetzwerk mit definierten Teilnehmern aus der Automatisierungszelle Daten austauschen dürfen.

Folgende Filterkriterien auf Layer 3 und 4 stehen zur Verfügung: IPv4-Adressen, Protokoll (TCP/UDP) und Ports.

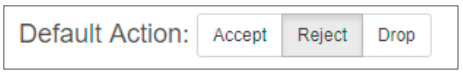
Die Paketfilter stehen auch in der Richtung „LAN to WAN“ zur Verfügung, siehe Kapitel 0.

Im Menü „Packet Filter“ wählen Sie den Menüpunkt „WAN to LAN“.

Über die Option „Default Option“ können Sie einstellen, ob generell alle Telegramme erlaubt sind („Accept“) und nur spezielle Pakete gefiltert werden („Blacklisting“), oder ob generell alle Telegramme verboten sind („Reject“ / „Drop“) und nur die Telegramme nach den Filterregeln durchgelassen werden sollen („Whitelisting“).

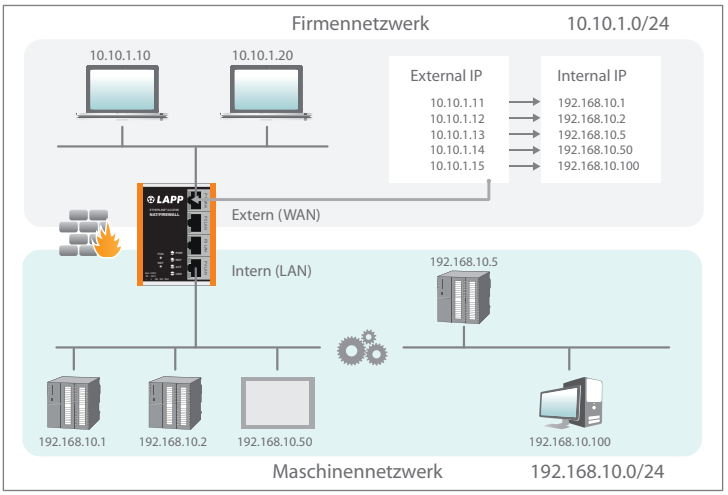


Wollen Sie erstmal nicht filtern, so stellen Sie die Default Action auf „Accept“.



Um den Zugriff auf das Maschinennetzwerk auf bestimmte Teilnehmer im WAN zu beschränken, stellen Sie die Default Action auf „Reject“ oder „Drop“. „Reject“ sendet bei nicht erlaubten Telegrammen aus dem WAN eine Fehlermeldung zurück, „Drop“ verwirft das Telegramm ohne Fehlermeldung.

Beispiel: Es soll einem PC im Produktionsnetzwerk (WAN), mit der 10.10.1.11 (z.B. eine Visualisierung), der Zugriff auf die CPU im LAN mit der IP 192.168.10.1 über den Port 102 mit dem TCP-Protokoll erlaubt werden.



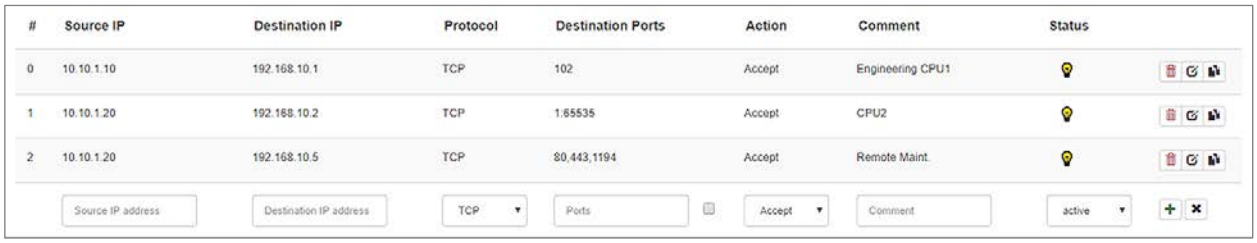
Tragen Sie nun folgende Regel ein und speichern Sie mit dem + Button.

Source IP gibt die IP-Adresse des aktiven Gerätes im Produktionsnetzwerk (WAN) an. **Destination IP** das angesprochene Gerät im Maschinennetzwerk (LAN).

Mit **Protocol** „TCP“, „UPD“ oder „ICMP“ kann die Filterregel auf einen Protokolltyp festgelegt werden.

Destination Ports gibt die Ports an, auf denen die Filterregel wirkt.

Soll sich eine Filterregel auf mehrere oder gar alle Ports beziehen so kann dies im Feld „Destination Ports“ einfach festgelegt werden. Eine Liste von Ports wird durch Kommata getrennt angegeben: „80,443,1194“. Ein Portbereich kann mit einem Doppelpunkt angegeben werden: „4000:5000“ oder für alle Ports „1:65535“. Es sind auch Kombinationen daraus möglich: „80,443,4000:5000“.



Es ist auch möglich, den Zugriff von mehreren Teilnehmer untereinander zu konfigurieren. Ein IP-Bereich kann mit einem Bindestrich definiert werden: “10.10.1.10-10.10.1.20“. Eine Liste von IP-Adressen wird mit Kommata angegeben: “10.10.1.10,10.10.1.15,10.10.1.20”. Ein IP-Subnetz kann mit der CIDR-Notation angegeben werden: "10.10.1.10/24".

Action legt fest, ob diese Regel die Kommunikation erlaubt („Accept“), mit Fehler ablehnt („Reject“) oder einfach verwirft („Drop“). Im Zusammenspielt mit der „Default Action“ sollte hier immer die passende Methode gewählt werden. Ist die Default Action z.B. „Reject“ oder „Drop“ so sollten die Filter Regeln alle auf „Accept“ gestellt werden (Whitelisting). Ist die Default Action „Accept“ so kann in den Filter Regeln mit „Reject“ oder „Drop“ für bestimmte Geräte eine Sperre definiert werden (Blacklisting).

Status: = Regel ist aktiv; Ein Klick auf das Lampensymbol ändert den Regelstatus in Inaktiv

= Regel ist inaktiv: Ein Klick auf das Lampensymbol ändert den Regelstatus in Aktiv

Mögliche Aktionen:

löschen einer Regel bearbeiten einer Regel kopieren einer Regel

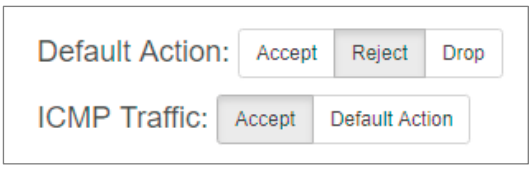
HINWEIS

Es können maximal 128 Paketfilter Regeln pro Richtung ("WAN to LAN" und "LAN to WAN") definiert werden.

6.5 ICMP Traffic "WAN to LAN"

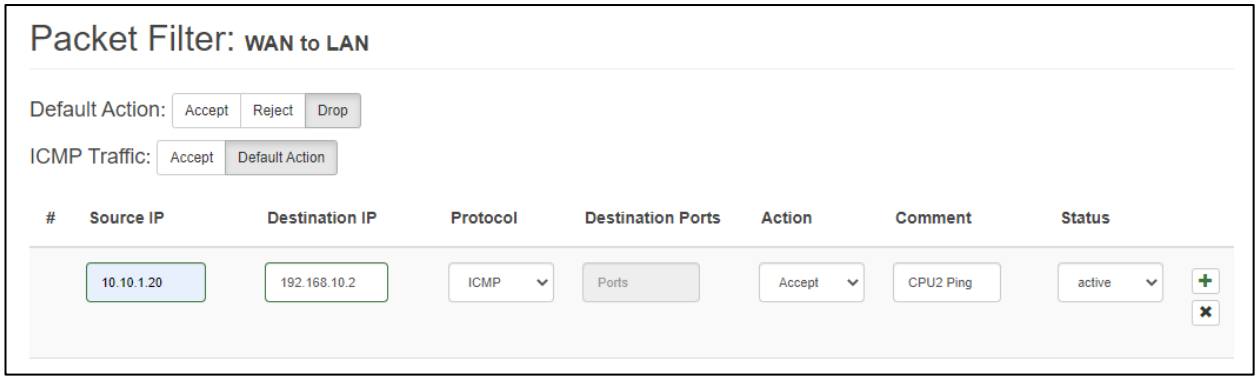
Das Internet Control Message Protocol (ICMP) dient dem Austausch von Informations- und Fehlermeldungen über das Internet-Protokoll IPv4. Typische ICMP-Telegramme sind z.B. "ping" oder "traceroute".

Mit der Option „ICMP-Traffic“ können Sie ICMP-Pakete generell annehmen („Accept“) oder abhängig von den Packet Filtern regeln („Default Action“).



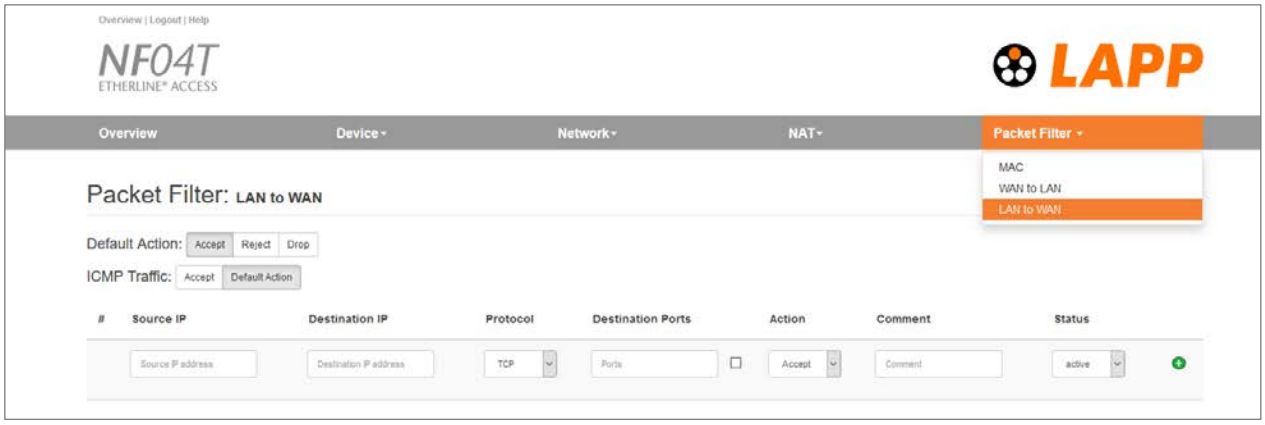
Ist z.B. die Paketfilter „Default Action“ auf „Reject“ oder „Drop“ eingestellt und ICMP Traffic auf „Default Action“, dann werden keinerlei ICMP-Telegramme durchgelassen.

Alternativ zum generellen Freigeben von ICMP können auch einzelne Filterregeln festgelegt werden, in dem bei der Filterregel als Protokoll „ICMP“ ausgewählt wird.



6.6 Paketfilter “LAN to WAN”

Im Grundzustand ist der Datenverkehr für Geräte vom Maschinennetzwerk (LAN) zum Produktionsnetzwerk (WAN) ohne Beschränkung freigegeben („Default Action“: „Accept“).



Im Paket Filter “LAN to WAN” kann die Kommunikation von Geräten im LAN mit Geräten im Produktionsnetzwerk (WAN) oder ins Internet ganz unterbunden oder für bestimmte Geräte gesperrt oder erlaubt werden.

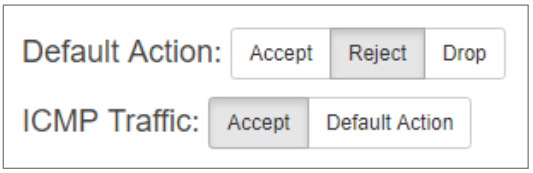
Die Eingabe der Filterregeln entspricht den Paketfiltern „WAN to LAN“ nur dass die Source IP jetzt die LAN-IP ist und die Destination IP ein Gerät im WAN adressiert.

HINWEIS

Es können maximal 128 Paketfilter Regeln pro Richtung ("WAN to LAN" und "LAN to WAN") definiert werden.

6.7 ICMP Traffic "LAN to WAN"

Mit der Option „ICMP Traffic“ können Sie das Durchleiten von ICMP Telegrammen vom LAN zum WAN- Netzwerk generell erlauben („Accept“) oder abhängig von den Packet Filtern verbieten („Default Action“).



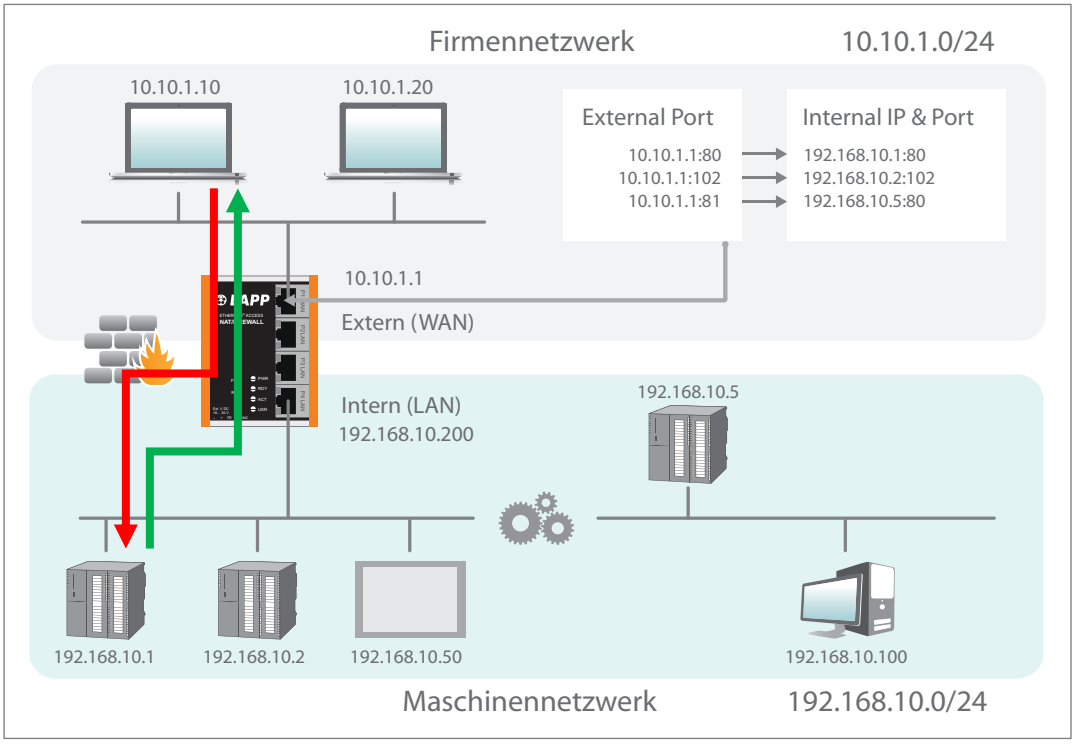
Ist z.B. die Paketfilter „Default Action“ auf „Reject“ oder „Drop“ eingestellt und ICMP Traffic auf „Default Action“, dann werden keinerlei ICMP-Telegramme durchgelassen.

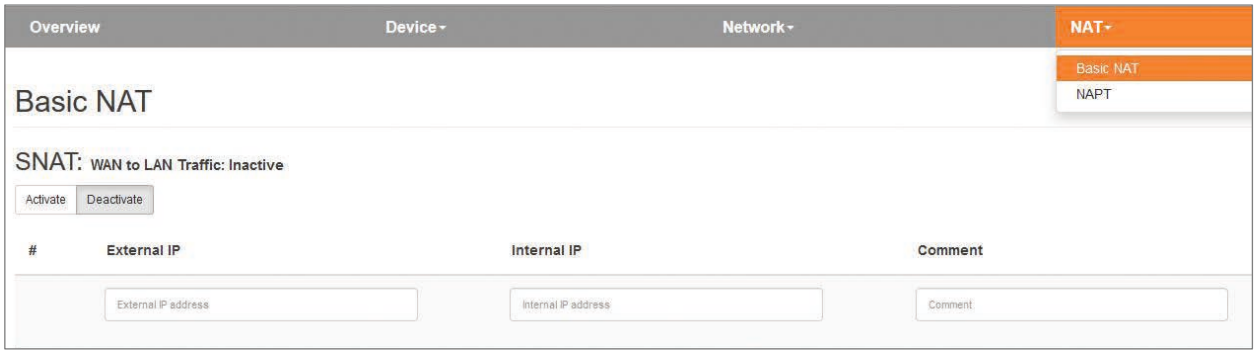
Alternativ zum generellen Freigeben von ICMP können auch einzelne Filterregeln festgelegt werden, in dem bei der Filterregel als Protokoll „ICMP“ ausgewählt wird.

6.8 SNAT

Mit der Funktion „SNAT (Source NAT)“ wird der eingehende Datenverkehr von der WAN Seite transparent an das LAN-Netzwerk weitergegeben. Bei allen Paketen, die auf LAN-Seite von ETHERLINE® ACCESS NF04T weitergeleitet werden, wird die Quell-IP-Adresse durch die LAN-IP-Adresse von ETHERLINE® ACCESS NF04T ersetzt..

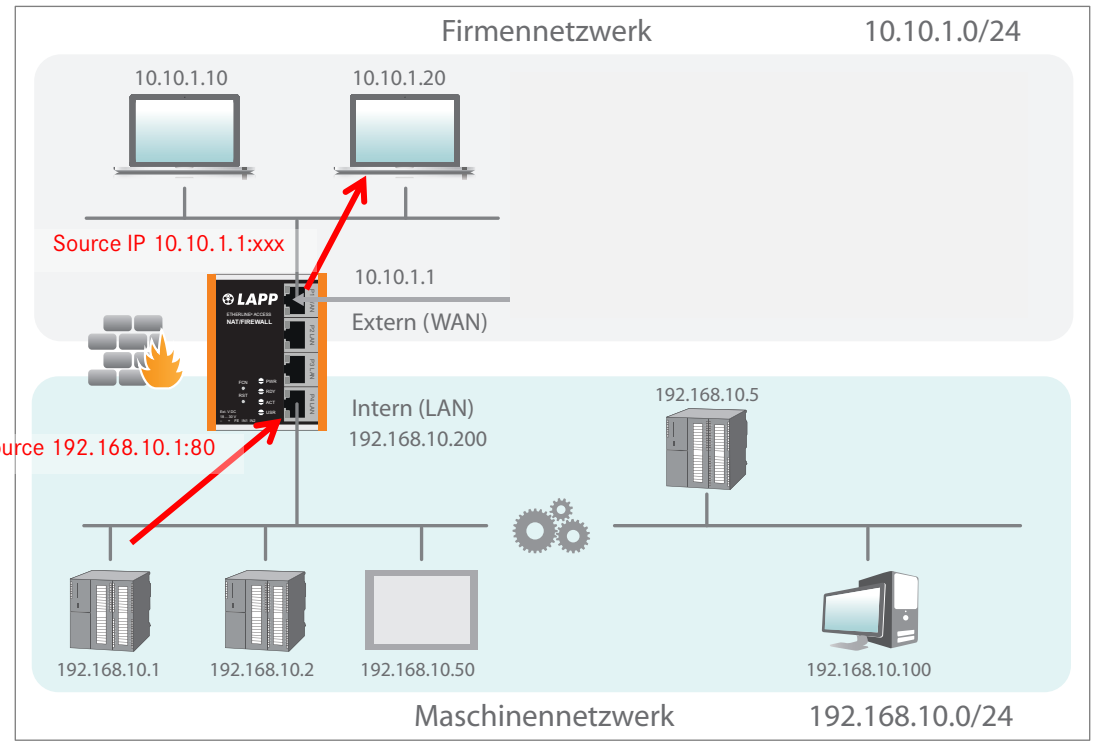
Somit benötigt keiner der LAN-Teilnehmer als „Gateway“ die ETHERLINE® ACCESS NF04T LAN-IP-Adresse. Dies ist ein erheblicher Vorteil bei der Integration in bestehende Netzwerkstrukturen, da die Parameter der LAN-Geräte nicht mehr geändert werden müssen.





6.9 NAPT

„NAPT for LAN to WAN traffic“ ersetzt die Absender-Adressen von Anfragen aus dem LAN durch die ETHERLINE® ACCESS NF04T WAN IP Adresse.



Die Option „**NAPT: Active**“ ermöglicht somit eine Kommunikation von Geräten aus dem LAN mit Geräten im WAN. ETHERLINE® ACCESS NF04T verwaltet dabei als Gateway die Umsetzung auf die IP-Adressen des WAN-Netzwerks und kümmert sich auch um die Zuordnung der Antwort.

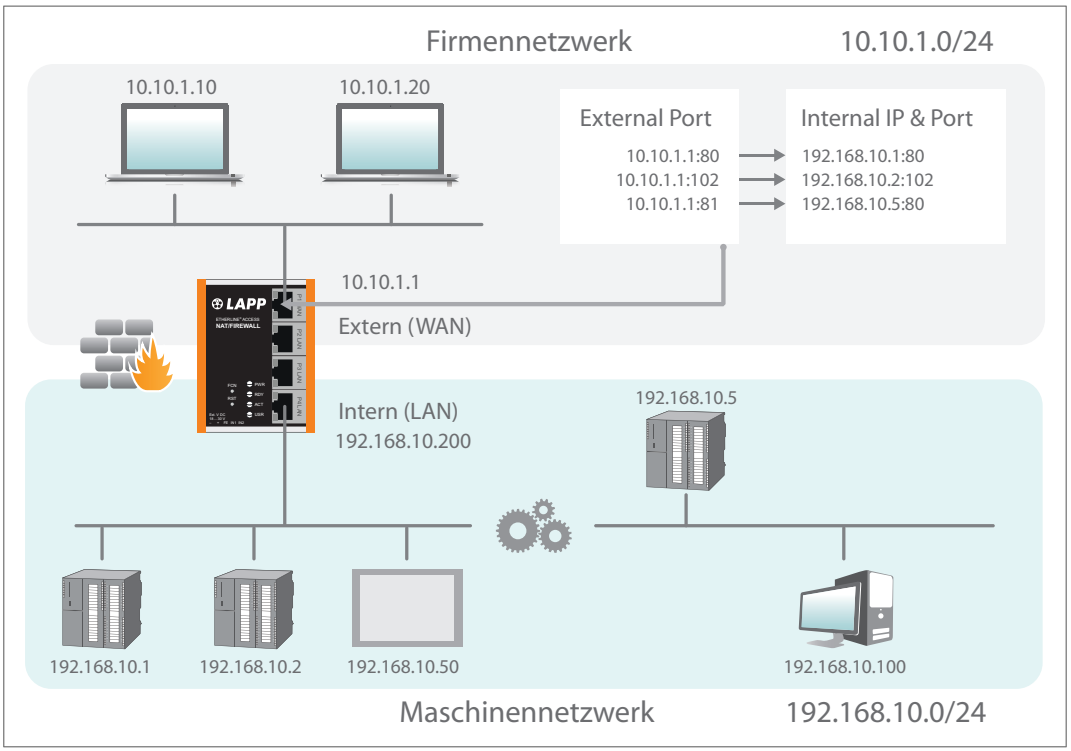
ACHTUNG

Damit bei aktiviertem NAPT die Kommunikation vom LAN nach WAN funktioniert, muss die ETHERLINE® ACCESS NF04T LAN IP Adresse in allen Geräten am LAN als Gateway eingetragen werden!

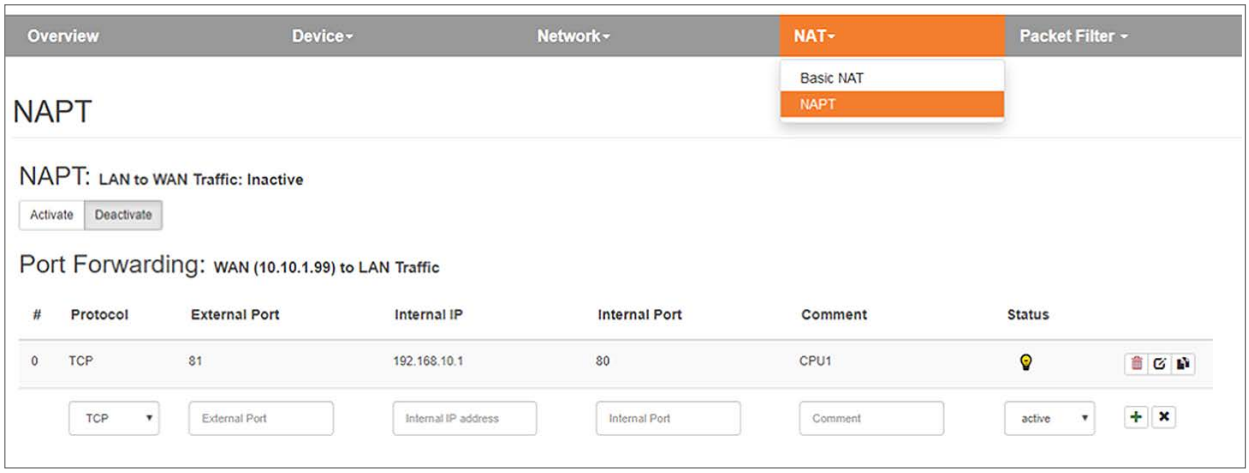
Ist die Option **NAPT** abgeschaltet („Deactivate“), so werden die Anfrage-Pakete aus dem LAN mit ihrer original Absender-IP und Absender-Port an das WAN weitergeleitet.

6.10 Portforwarding

Mithilfe von Portweiterleitungen („Portforwarding for WAN to LAN traffic“) kann konfiguriert werden, dass Pakete an einen bestimmten TCP/UDP-Port des ETHERLINE® ACCESS NF04T (WAN) an einen Teilnehmer im LAN weitergeleitet werden (z.B. 10.10.1.1:81 zu 192.168.10.5:80).



Im folgenden Beispiel kann die Webseite (Port 80) der CPU mit der IP 192.168.10.5 über WAN durch den Zugriff auf die ETHERLINE® ACCESS NF04T eigene IP-Adresse 10.10.1.1 mit Port 81 erreicht werden.



Protocol: "TCP" oder "UDP"

External Port: Der Port unter dem die Telegramme im WAN unter der Adresse des ETHERLINE® ACCESS NF04T empfangen werden.

Internal IP: Die im Maschinennetz (LAN) anzusprechende IP-Adresse.

Internal Port: Der im Maschinennetz (LAN) anzusprechende Port des Gerätes.

Comment: Frei definierbarer Kommentar.

Status: = Regel ist aktiv; Ein Klick auf das Lampensymbol ändert den Regelstatus in Inaktiv

= Regel ist inaktiv: Ein Klick auf das Lampensymbol ändert den Regelstatus in Aktiv

Mögliche Aktionen:

löschen einer Regel bearbeiten einer Regel kopieren einer Regel

HINWEIS

„Portforwarding“ und „Basic NAT“ können gleichzeitig im NAT Betriebsmodus verwendet werden.

ACHTUNG

Wenn bei den Paketfiltern „WAN to LAN“ die Default Action auf „Reject“ oder „Drop“ gestellt ist, so müssen für jeden Portforwarding-Eintrag auch entsprechende Filterregeln für den Zugriff erstellt werden.

HINWEIS

Es ist nicht möglich die reservierten Ports 443 und 80 zu verwenden, wenn ETHERLINE® ACCESS NF04T die eigene Webseiten auf dem WAN aktiviert hat (Web Interface Access = "WAN and LAN", siehe Kapitel 11.7).

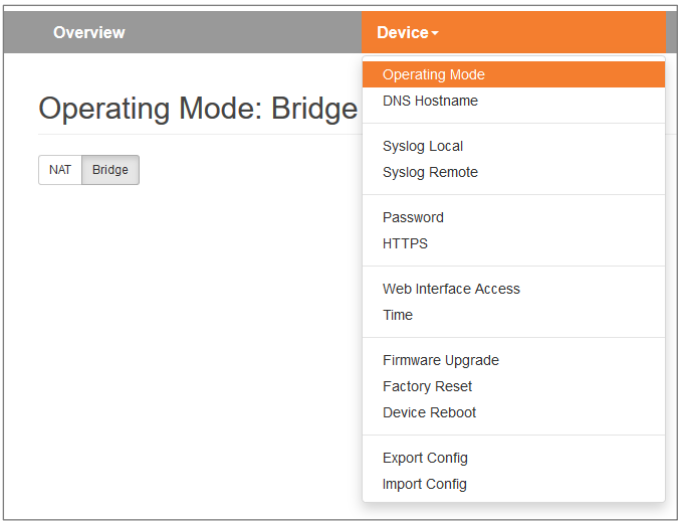
ACHTUNG

Es können maximal 128 Portforwarding Einträge erstellt werden.

7 Anwendungsfall Bridge

7.1 Bridge Modus aktivieren

Zur Aktivierung des Bridge-Betriebsmodus wählen Sie im Menü „Device“ den Menüpunkt „Operating Mode“ und stellen diesen auf „Bridge“.

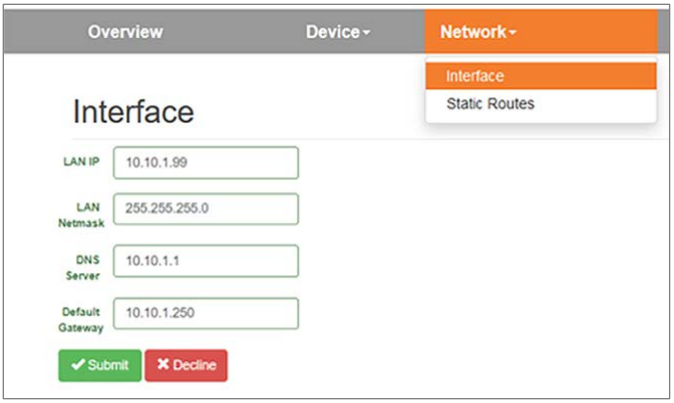


7.2 Anpassen der IP-Adressen im Bridge Betriebsmodus

Klicken Sie auf das Menü „Network“ und wählen das Untermenü „Interface“ aus. Hier können die IP-Adressen des ETHERLINE® ACCESS NF04T („LAN IP“) sowie die zugehörigen Subnetzmaske („LAN netmask“) festgelegt werden.

Ein DNS-Server und ein Default-Gateway können ebenfalls angegeben werden. Das ist notwendig, wenn Geräte aus dem LAN über den ETHERLINE® ACCESS NF04T das Internet erreichen sollen. Werden diese nicht angegeben, dann wird verhindert, dass Geräte im LAN mit dem Internet kommunizieren.

Die Eingabe wird mit dem Button „Submit“ gespeichert und die IP-Einstellungen werden damit sofort aktiv. Mit "Decline" wird die aktuelle Eingabe ohne Übernahme verworfen.



ACHTUNG

Wenn Sie die LAN IP-Adresse verändern, müssen Sie ggf. am Browser die Webseite des ETHERLINE® ACCESS NF04T unter der neuen IP-Adresse erneut öffnen und sich wieder einloggen.

Ein DHCP-Client oder ein DHCP-Server stehen im Bridge-Betriebsmodus nicht zur Verfügung.

HINWEIS

Im Bridge Betriebsmodus sind die festgelegten Interface Einstellungen gleichermaßen auch am WAN-Port des ETHERLINE® ACCESS NF04T gültig.

ACHTUNG

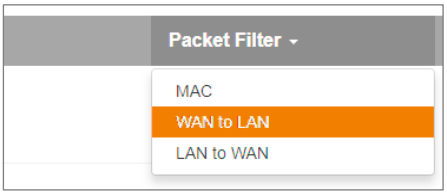
Im Bridgemodus sind aus Sicherheitsgründen zuerst alle Ports für den „WAN-to-LAN“ Datenverkehr gesperrt!

Um Zugriffe zu erlauben, müssen Paketfilter-Regeln erstellt oder die "Default Action" bei den Paket-Filtern auf „Accept“ gestellt werden. Siehe folgendes Kapitel.

Der Datenverkehr „LAN to WAN“ ist per default immer freigegeben, kann aber ebenfalls durch Paket-Filter oder die Default Action eingeschränkt werden.

7.3 Paketfilter „WAN to LAN“

Mit den Paketfiltern lässt sich der Zugriff zwischen dem Firmen-/ Produktionsnetzwerk (WAN) und dem Maschinennetzwerk (LAN) einschränken.



Es kann beispielsweise konfiguriert werden, dass nur bestimmte Teilnehmer aus dem Produktionsnetzwerk mit definierten Teilnehmern aus der Automatisierungszelle Daten austauschen dürfen.

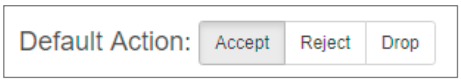
Folgende Filterkriterien auf Layer 3 und 4 stehen zur Verfügung: IPv4-Adressen, Protokoll (TCP/UDP/ICMP) und Ports.

Hinweis: Die Paketfilter stehen auch in der Richtung „LAN to WAN“ zur Verfügung, siehe 7.5.

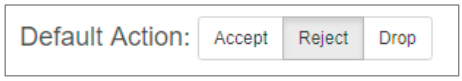
Im Menü „Packet Filter“ wählen Sie den Menüpunkt „WAN to LAN“.

Über die Option „Default Option“ können Sie einstellen, ob generell alle Telegramme erlaubt sind („Accept“) und nur spezielle Pakete gefiltert werden („Blacklisting“), oder ob generell alle Telegramme verboten sind („Reject“ / „Drop“) und nur die Telegramme nach den Filterregeln durchgelassen werden sollen („Whitelisting“).

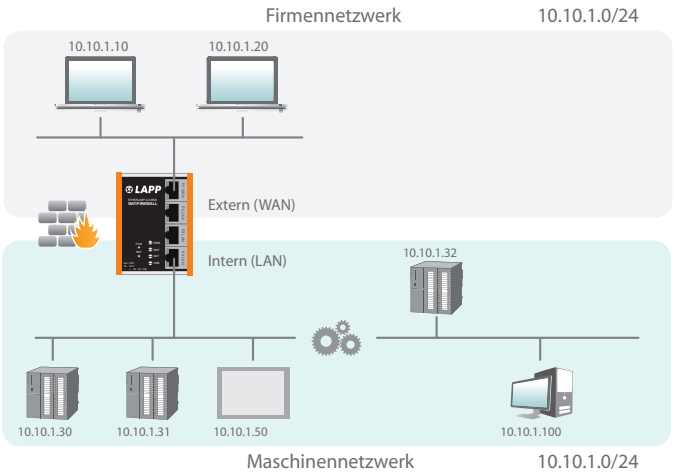
Wollen Sie erstmal nicht filtern, so stellen Sie die Default Action auf „Accept“.



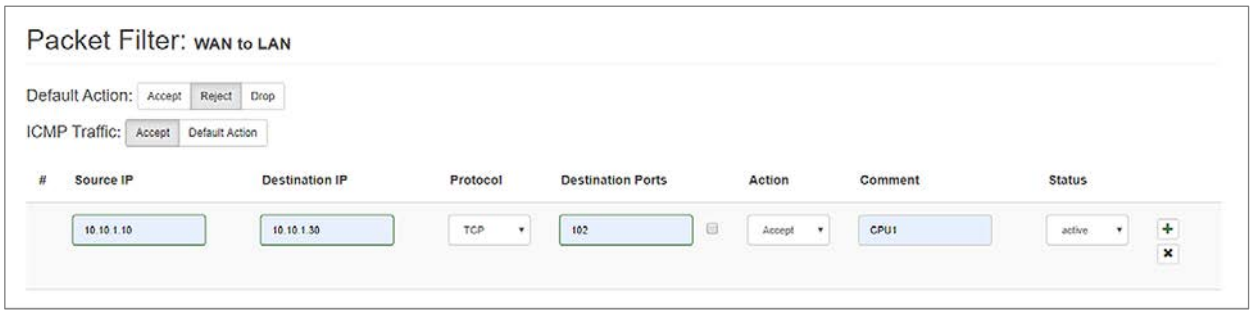
Um den Zugriff auf das Maschinennetzwerk auf bestimmte Teilnehmer im WAN zu beschränken, stellen Sie die Default Action auf „Reject“ oder „Drop“. „Reject“ sendet bei nicht erlaubten Telegrammen aus dem WAN eine Fehlermeldung zurück, „Drop“ verwirft das Telegramm ohne Fehlermeldung.



Beispiel: Es soll einem PC im Firmennetzwerk (WAN), mit der 10.10.1.11 (z.B. eine Visualisierung), der Zugriff auf die CPU im LAN mit der IP 10.10.1.30 über den Port 102 mit dem TCP-Protokoll erlaubt werden



Tragen Sie nun folgende Regel ein und speichern Sie mit dem + Button.



Source IP gibt die IP-Adresse des aktiven Gerätes im Produktionsnetzwerk (WAN) an.

Destination IP das angesprochene Gerät im Maschinennetzwerk (LAN).

Mit **Protocol** „TCP“, „UPD“ oder „ICMP“ kann die Filterregel auf einen Protokolltyp festgelegt werden.

Destination Ports gibt die Ports an, auf denen die Filterregel wirkt.

Soll sich eine Filterregel auf mehrere oder gar alle Ports beziehen so kann dies im Feld „Destination Ports“ einfach festgelegt werden. Eine Liste von Ports wird durch Kommata getrennt angegeben: „80,443,1194“. Ein Portbereich kann mit einem Doppelpunkt angegeben werden: „4000:5000“ oder für alle Ports „1:65535“. Es sind auch Kombinationen daraus möglich: „80,443,4000:5000“.

#	Source IP	Destination IP	Protocol	Destination Ports	Action	Comment	Status
0	10.10.1.10	10.10.1.30	TCP	102	Accept	CPU1	
1	10.10.1.20	10.10.1.30	TCP	1:65535	Accept	Engineering	
2	10.10.1.20	10.10.1.31	TCP	80,443,1194	Accept	Remote Maint.	

Es ist auch möglich, den Zugriff mehrerer Teilnehmer untereinander zu konfigurieren. Ein IP-Bereich kann durch einen Bindestrich definiert werden: „10.10.1.10-10.10.1.20“. Eine Liste von IP-Adressen wird mit Kommata angegeben: „10.10.1.10,10.10.1.15,10.10.1.20“. Ein IP-Subnetz kann mit der CIDR-Notation angegeben werden: „10.10.1.10/24“.

3	10.10.1.10-10.10.1.20	10.10.1.50	TCP	1:65535	Accept	Visu	
4	10.10.1.21	10.10.1.30-10.10.1.50	TCP	80,443	Accept	Webpages	

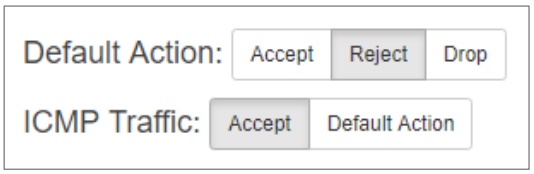
Action legt fest, ob diese Regel die Kommunikation erlaubt („Accept“), mit Fehler ablehnt („Reject“) oder einfach verwirft („Drop“). Im Zusammenspielt mit der „Default Action“ sollte hier immer die passende Methode gewählt werden. Ist die Default Action z.B. „Reject“ oder „Drop“ so sollten die Filter Regeln alle auf „Accept“ gestellt werden (Whitelisting). Ist die Default Action „Accept“ so kann in den Filter Regeln mit „Reject“ oder „Drop“ für bestimmte Geräte eine Sperre definiert werden (Blacklisting).

HINWEIS

Es können maximal 128 Paketfilter Regeln pro Richtung ("WAN to LAN" und "LAN to WAN") definiert werden.

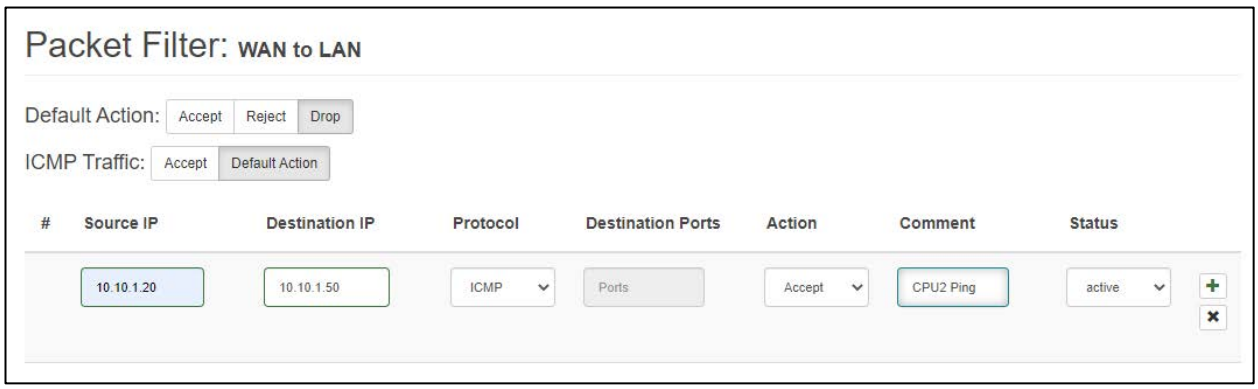
7.4 ICMP Traffic "WAN to LAN"

Mit der Option „ICMP-Traffic“ können Sie ICMP-Pakete generell annehmen („Accept“) oder abhängig von den Packet Filtern regeln („Default Action“).



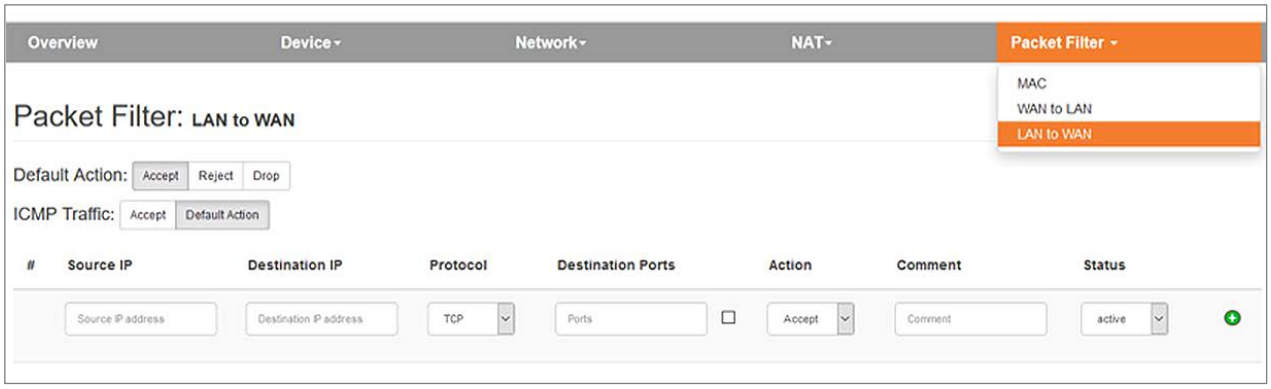
Ist z.B. die Paketfilter „Default Action“ auf „Reject“ oder „Drop“ eingestellt und ICMP Traffic auf „Default Action“, dann werden keinerlei ICMP-Telegramme durchgelassen.

Alternativ zum generellen Freigeben von ICMP können auch einzelne Filterregeln festgelegt werden, in dem bei der Filterregel als Protokoll „ICMP“ ausgewählt wird.



7.5 Paketfilter „LAN to WAN”

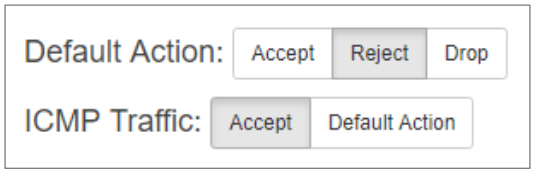
Im Grundzustand ist der Datenverkehr für Geräte vom Maschinennetzwerk (LAN) zum Produktionsnetzwerk (WAN) ohne Beschränkung freigegeben („Default Action“: „Accept“).



Im Packet Filter “LAN to WAN” kann die Kommunikation von Geräten im LAN mit Geräten im Produktionsnetzwerk (WAN) ganz unterbunden oder für bestimmte Geräte gesperrt oder erlaubt werden.

7.6 ICMP Traffic "LAN to WAN"

Mit der Option „ICMP-Traffic“ können Sie ICMP-Pakete generell annehmen („Accept“) oder abhängig von den Packet Filtern regeln („Default Action“).



Ist z.B. die Paketfilter „Default Action“ auf „Reject“ oder „Drop“ eingestellt und ICMP Traffic auf „Default Action“, dann werden keinerlei ICMP-Telegramme durchgelassen.

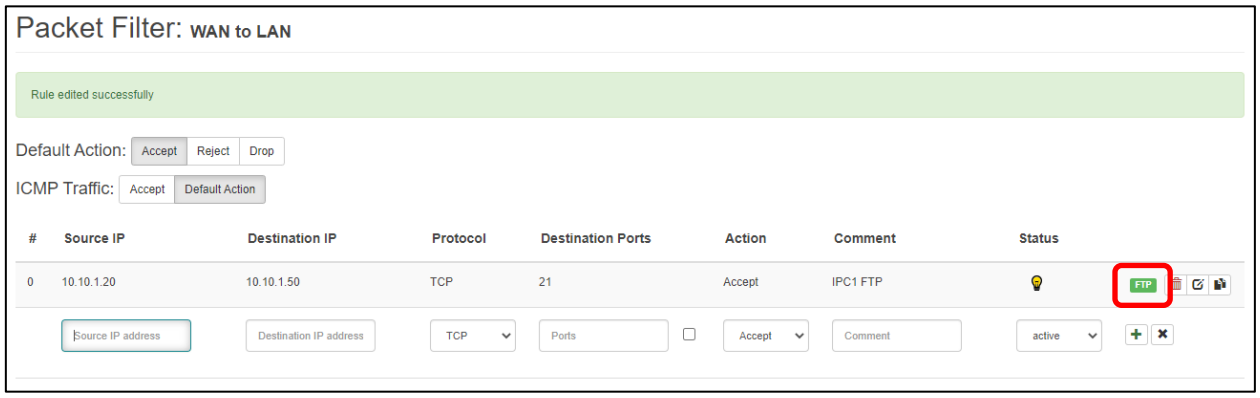
Alternativ zum generellen Freigeben von ICMP können auch einzelne Filterregeln festgelegt werden, in dem bei der Filterregel als Protokoll „ICMP“ ausgewählt wird.

7.7 FTP-Helper für aktives FTP

Eine besondere Anwendung im Zusammenhang mit Filterregeln auf Portebene ist das aktive FTP Protokoll. Im Gegensatz zum passiven FTP Protokoll, bei dem der Port 20 fest für den Datenaustausch festgelegt ist, wird beim Aktiven FTP der verwendete Port für den Datenaustausch nach dem Verbindungsaufbau über Port 21 zufällig festgelegt. Da man bei der Einrichtung des ETHERLINE® ACCESS NF04T den Port nicht kennen kann, kann man auch keine feste Port Regel einstellen. Um für diesen Anwendungsfall nicht immer alle Ports öffnen zu müssen unterstütz ETHERLINE® ACCESS NF04T die Funktion „FTP-Helper“.

Der FTP-Helper liest beim FTP-Verbindungsaufbau das FTP -Protokoll mit und gibt nach Verbindungsaufbau nur den dort ausgehandelten Port für die Zeit der FTP-Verbindung frei.

Erstellen Sie eine „WAN to LAN“ Regel für den FTP-Verbindungsaufbau und aktivieren Sie dann die „FTP-Helper“ Option an der Regel für aktives FTP.



HINWEIS

Der FTP-Helper funktioniert in der aktuellen Firmware nur im Bridge-Mode und für Filter in Richtung „WAN to LAN“. Fragen Sie den Support, wenn Sie den FTP-Helper auch in anderen Applikationen verwenden wollen.

8 MAC-Adressen Filterung

Mit der Funktion „MAC Filtering“ kann die Kommunikation über den ETHERLINE® ACCESS NF04T auf Geräte mit bestimmten MAC-Adressen beschränkt werden („Whitelisting“) oder Geräten mit bestimmten MAC-Adressen der Zugriff verweigert werden („Blacklisting“).

MAC Filterung kann sowohl im NAT als auch im Bridge Betriebsmodus verwendet werden.

Die Filterung kann auf der WAN, auf der LAN oder auf beiden Seiten für jede MAC-Adresse aktiviert werden.

MAC-Adressen müssen immer im Format "AA:BB:CC:DD:EE:FF" eingegeben werden, wobei Zahlen in Hexadezimal anzugeben sind.

ACHTUNG

MAC-Filterung hat die höchste Priorität von allen Filtern im ETHERLINE® ACCESS NF04T.

Sobald die erste MAC-Adresse im MAC-Filtermodus "Whitelist" eingetragen wurde, werden nur noch Telegramme von dieser MAC-Adresse durchgelassen, unabhängig von allen anderen Paketfilter-Regeln.

Wird MAC-Filterung im Modus "Whitelist" verwenden so müssen die MAC-Adressen **aller** erlaubten Geräte angegeben werden.

Wird MAC-Filterung im Modus "Whitelist" verwenden so müssen die MAC-Adressen **aller** erlaubten Geräte angegeben werden.

Ist keine MAC-Filterregel eingetragen, so wird das „MAC Filtering“ deaktiviert, unabhängig von der „Default MAC Policy“.

HINWEIS

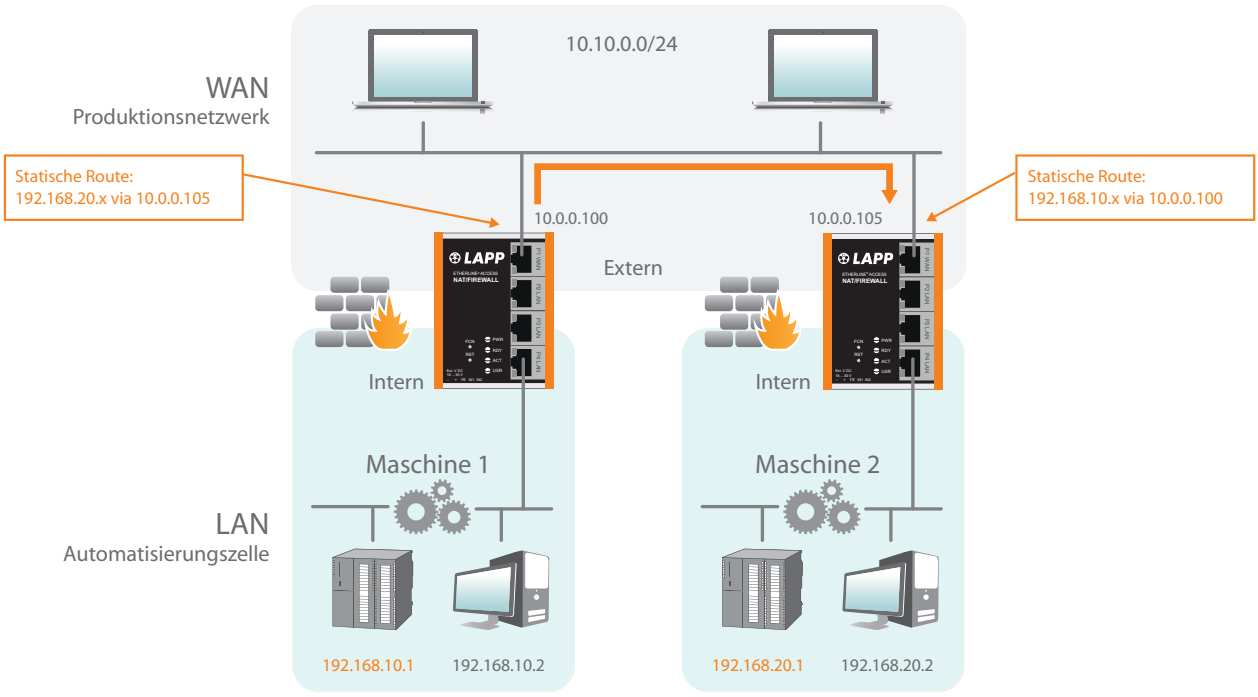
Im NAT-Mode wird die MAC-Filterung nur durchgeführt, wenn im IP-Header des Paketes die MAC-Adresse mit angegeben ist. Layer 2 Frames werden im NAT-Mode nicht weitergeleitet.

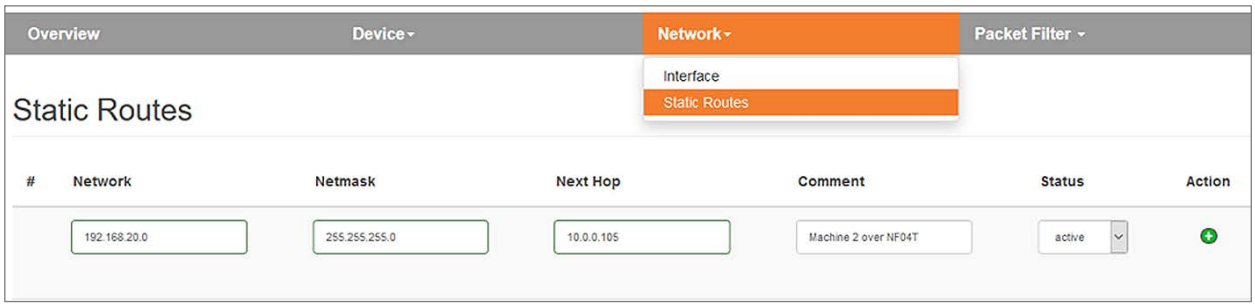
Im Bridge Mode findet die MAC-Filterung auf Layer 2 statt.

Es können maximal 128 MAC-Filterregeln definiert werden.

9 Statische Routen

Für die Kommunikation mit anderen Automatisierungszellen kommen statische Routen zum Einsatz. Hierfür muss das Netzwerk sowie die Adresse des dafür zuständigen Routers oder ETHERLINE® ACCESS NF04Ts („Next Hop“ oder „Gateway“) konfiguriert werden.





ACHTUNG

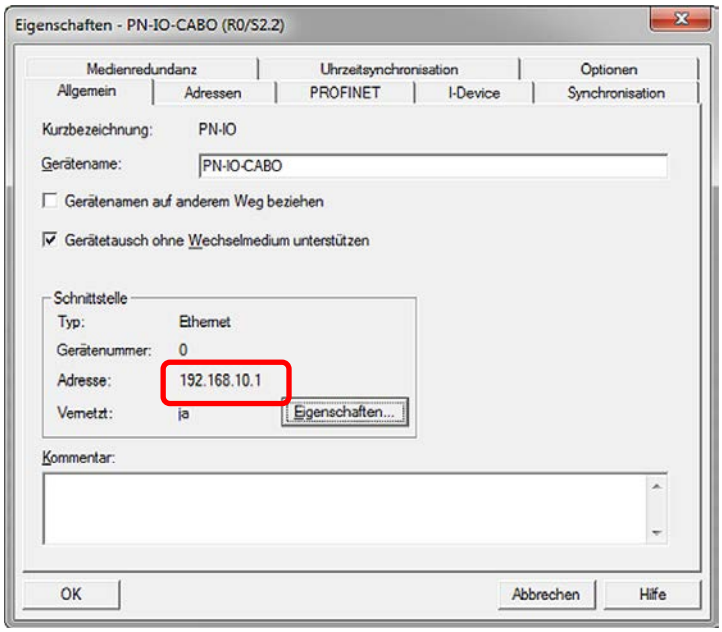
Um den Rückweg der Antwort zu ermöglichen, muss im entfernten Gateway (Maschine 2) auch eine Route zur IP-Adresse des ETHERLINE® ACCESS NF04T an der Maschine 1 eingerichtet werden!

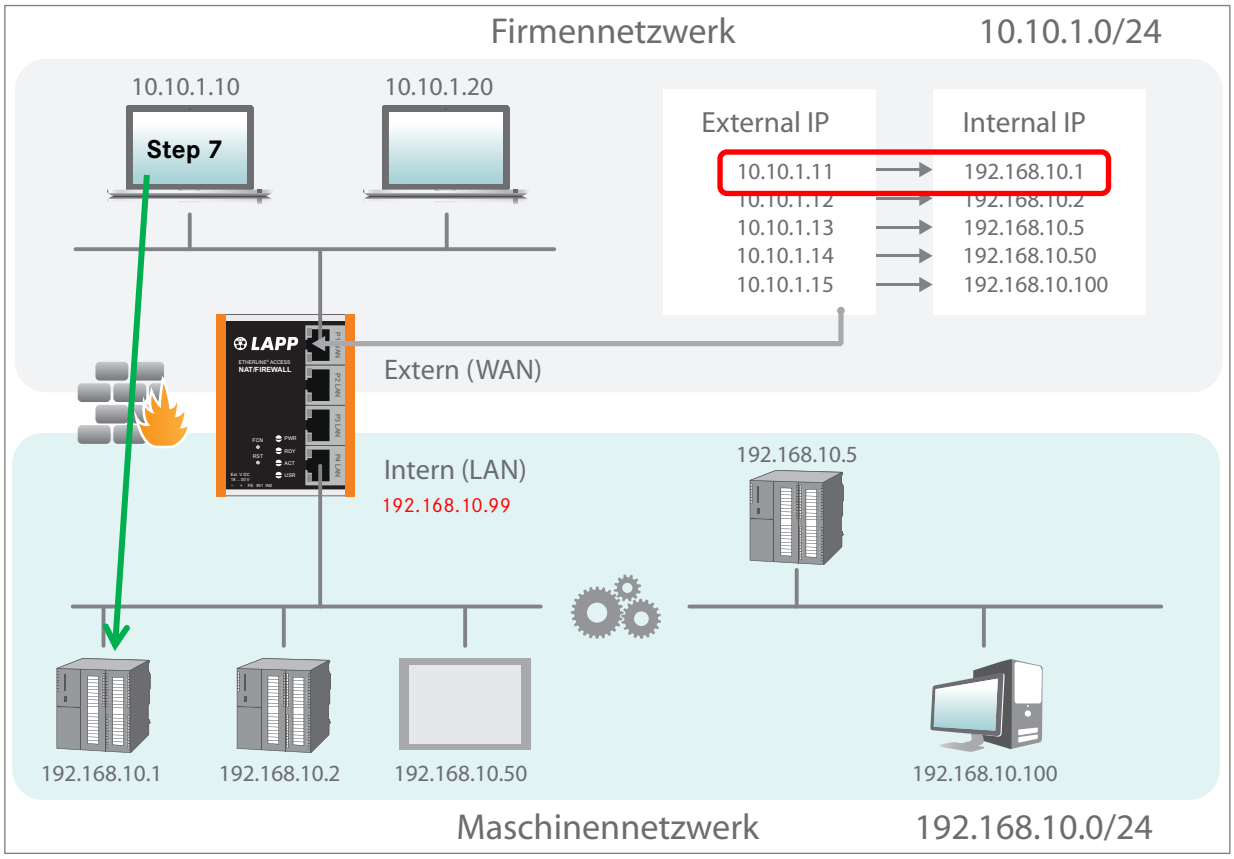
10 Anwendung mit Simatic Step 7 / TIA Portal

Problemstellung: Soll mit einer Engineering-Station im WAN Simatic CPUs im LAN hinter einem ETHERLINE® ACCESS NF04T angesprochen oder projektiert werden, zeigt sich das Problem, dass Step 7 oder TIA-Portal, beim Zugriff auf die CPU, die IP-Adresse aus dem Projekt nutzt.

Beim Zugriff über einen ETHERLINE® ACCESS NF04T, der im Betriebsmodus Basic NAT konfiguriert ist, muss eine andere IP-Adresse zum Zugriff auf die CPU im Step 7 oder TIA-Portal verwendet werden.

Die im Folgenden beschriebenen Lösungen können in angepasster Form auch für andere Anwendungen funktionieren.

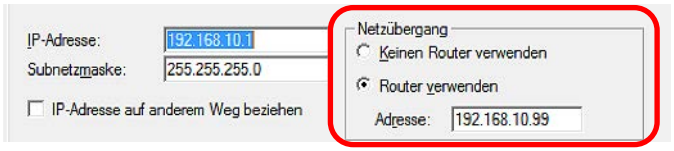




10.1 Anwendung mit Step 7

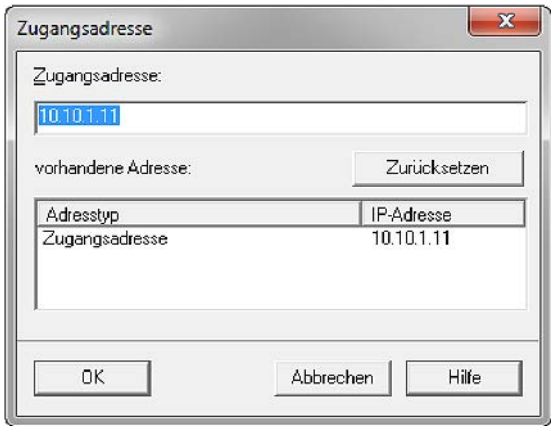
Step 7 bietet eine Möglichkeit auf eine CPU zuzugreifen und dabei aber eine andere als die im Projekt eingestellte IP-Adresse zu verwenden.

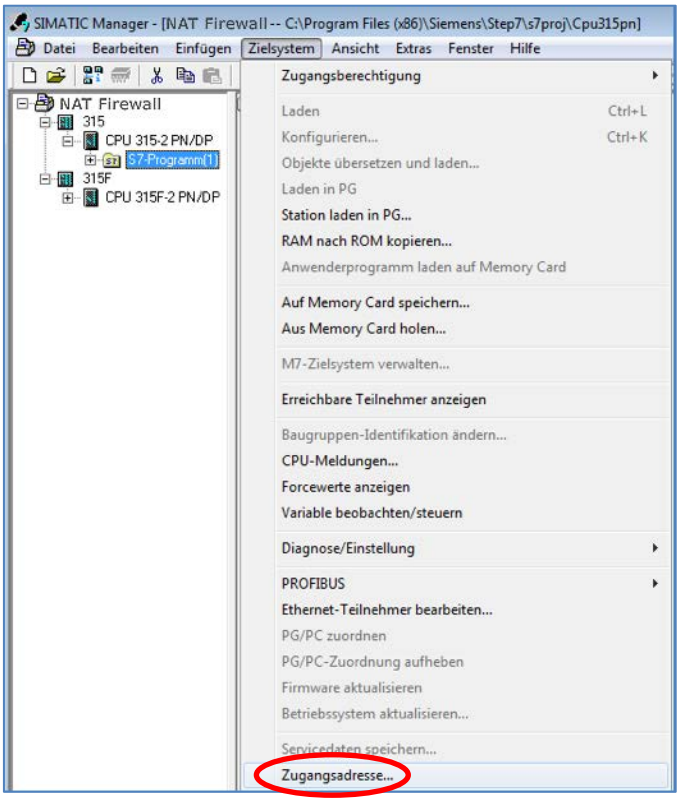
Damit aber auch die Antworten von der CPU wieder über den ETHERLINE® ACCESS NF04T an die Engineering-Station im WAN zurückgeleitet werden kann, muss entweder im ETHERLINE® ACCESS NF04T unter „Basic NAT“ die SNAT Funktion aktiviert werden oder im Projekt bei der CPU der ETHERLINE® ACCESS NF04T als Netzübergang (Router) eingetragen werden.



Um eine CPU über eine alternative IP-Adresse erreichen zu können, kann diese im Menü "Zielsystem" im Dialog "Zugangsadresse" eingegeben werden.

Diese Adresse bleibt solange aktiv bis sie im selben Dialog durch "Zurücksetzen" gelöscht wird.





ACHTUNG

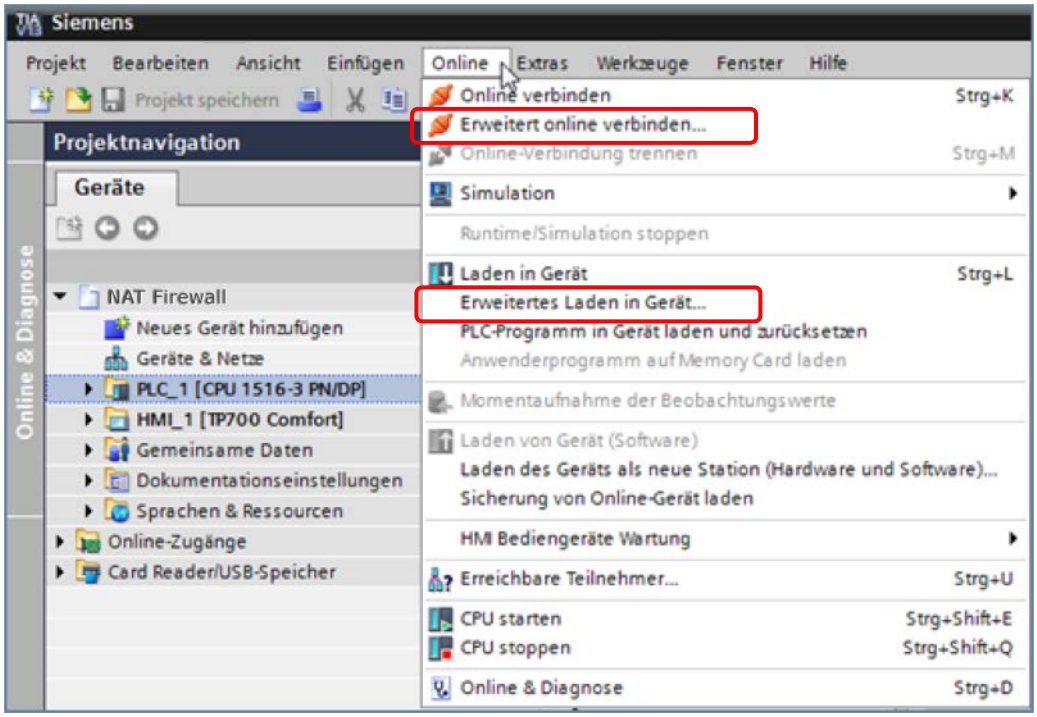
Diese Lösung ist nur im Betriebsmodus Basic NAT sinnvoll verwendbar. Bei NAPT mit Portforwarding kann nur eine CPU erreicht werden, da der Simatic Manager immer mit dem nicht verstellbaren Port 102 auf die CPU zugreift.

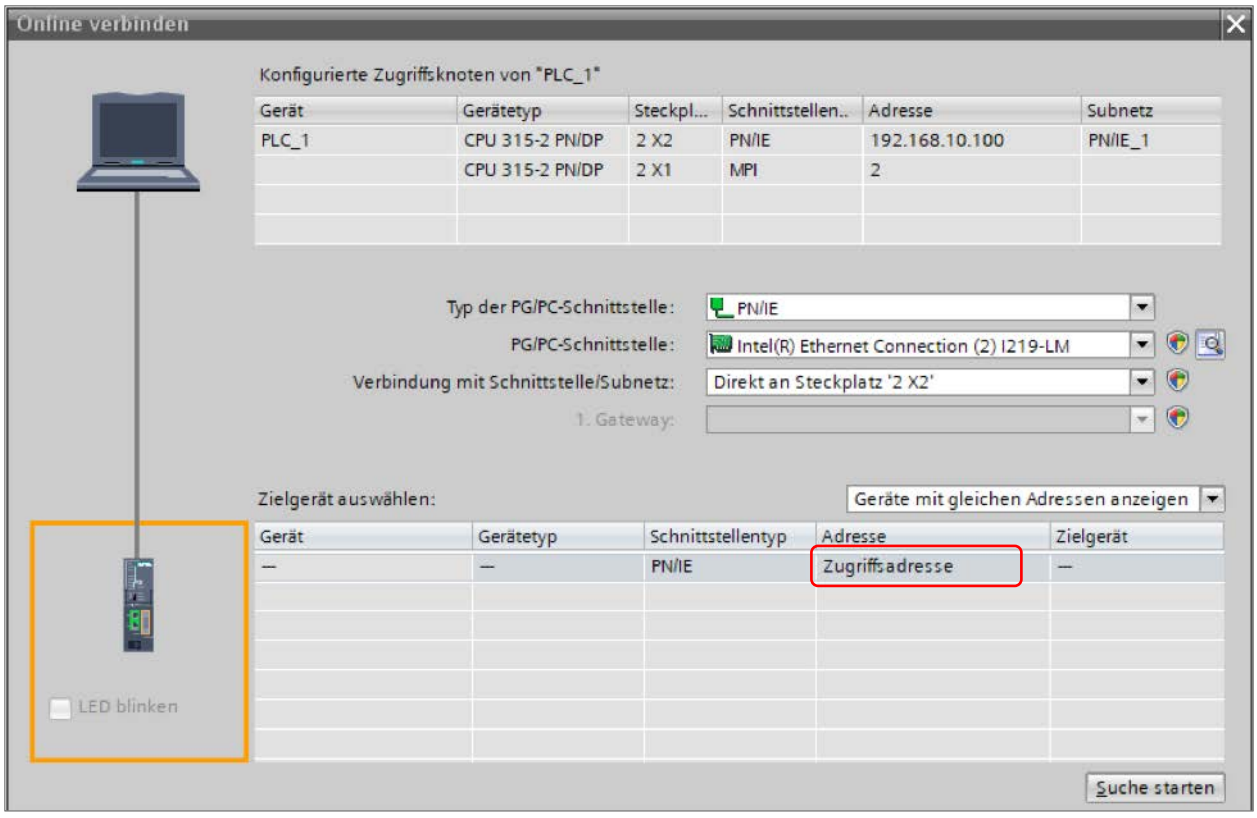
Die Suche über die Siemens Funktion „erreichbare Teilnehmer“ funktioniert nicht durch die ETHERLINE® ACCESS NF04T Firewall hindurch.

PROFINET RT Telegramme werden nicht durch ETHERLINE® ACCESS NF04T durchgeroutet!

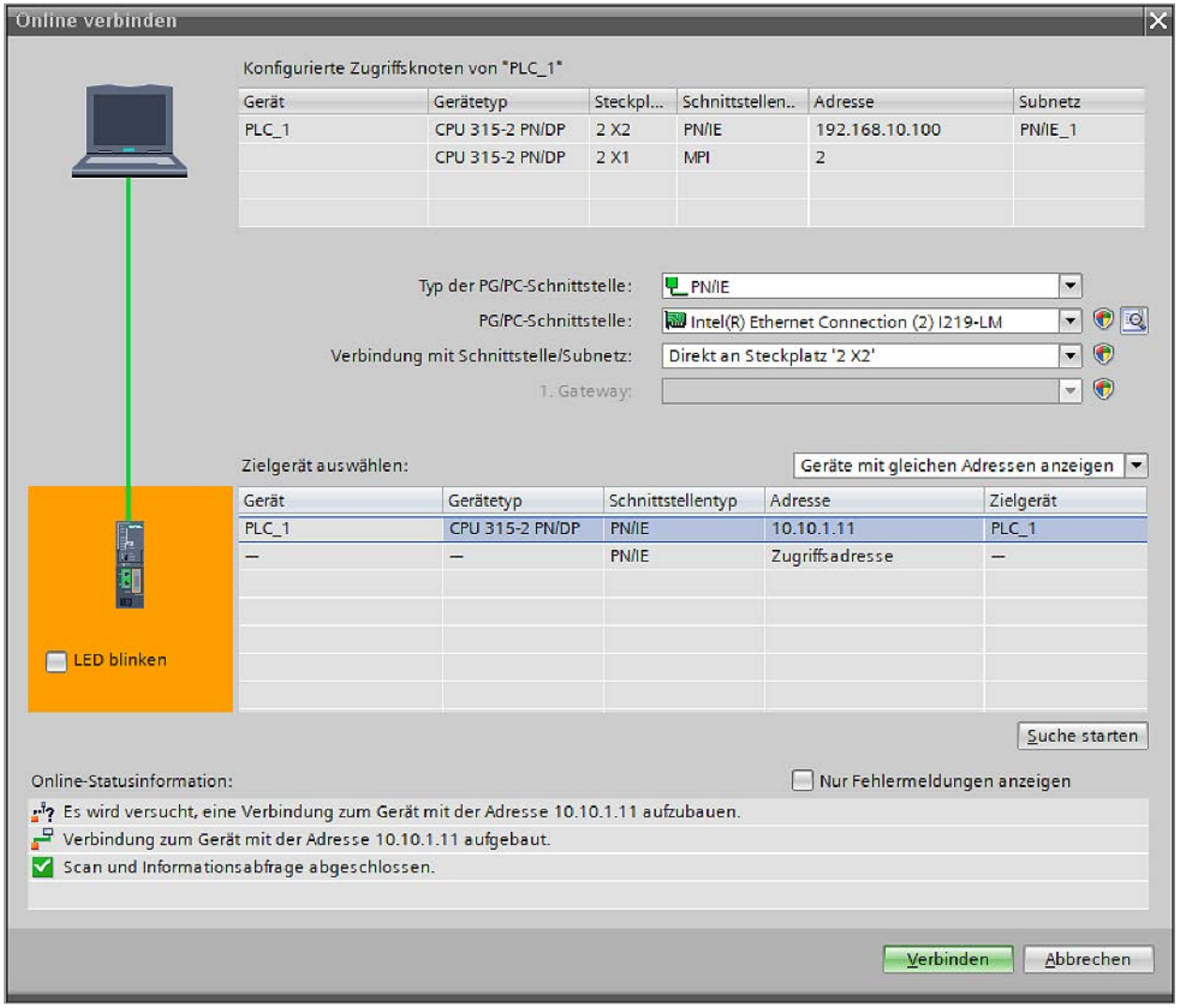
10.2 Anwendung im TIA-Portal

Hier benutzen sie im Menü unter „Online“ die Funktion „Erweitertes Laden in Gerät“ oder bei Bedarf „Erweitert online verbinden“.





Auf „Zugriffsadresse“ klicken und die WAN IP-Adresse eingeben, die für den Teilnehmer (CPU) im ETHERLINE® ACCESS NF04T unter Basic NAT festgelegt wurde. Bestätigen sie die Eingabe mit einem Klick auf das Fenster. Es wird nun versucht eine Verbindung zu der eingetragenen IP-Adresse aufzubauen.



ACHTUNG

Diese Lösung ist nur im Betriebsmodus Basic NAT sinnvoll verwendbar. Bei NAPT mit Portforwarding kann nur eine CPU erreicht werden, da der Simatic Manager/das TIA-Portal immer mit dem nicht verstellbaren Port 102 auf die CPU zugreift.

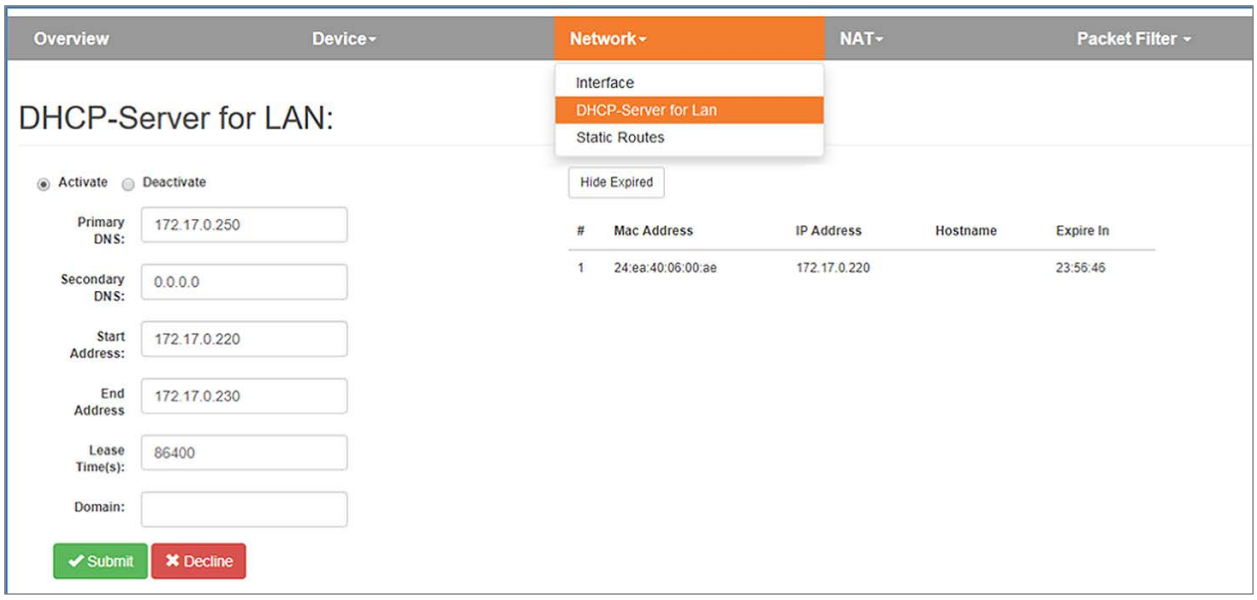
Die Suche über die Siemens Funktion „erreichbare Teilnehmer“ funktioniert nicht durch die ETHERLINE® ACCESS NF04T Firewall hindurch.

PROFINET RT Telegramme werden nicht durch ETHERLINE® ACCESS NF04T durchgeroutet!

11 Weitere Funktionen

11.1 DHCP Server for LAN

Für das LAN-Netzwerk des ETHERLINE® ACCESS NF04T kann ein DHCP-Server aktiviert werden, um im LAN eine dynamische IP-Adressvergabe zu ermöglichen.



Primary/Secondary DNS: Gibt die IP-Adresse eines DNS-Servers an, der für einen DHCP-Client verfügbar ist.

Start Address: Erste vom DHCP-Server verwendbare IP-Adresse im LAN-Netzwerk.

End Address: Letzte vom DHCP-Server verwendbare IP-Adresse im LAN-Netzwerk.

Lease Time (s): Die Zeitspanne, in der ein Netzwerkgerät eine IP-Adresse im Netzwerk verwenden kann. Wenn die Lease-Zeit abläuft, muss das Gerät die Lease erneuern, sonst wird die IP-Adresse vom DHCP-Server zurückgefordert und kann anderen Geräten angeboten werden. Die Standard Lease Time ist 86400 Sekunden (1 Tag). Die Lease Time kann von 60 Sekunden bis zu 31.536.000 Sekunden (365 Tage) eingestellt werden.

Domain: Domänenname, der den DHCP-Clients zugewiesen wird. Ein Domänenname ist eine Identifizierungszeichenfolge, die einen Bereich der administrativen Autonomie, Autorität oder Kontrolle innerhalb des Netzwerks definiert. Um den Domain-Namen zu verwenden, muss mindestens ein DNS-Server zugewiesen werden.

Auf der rechten Seite der Webseite befindet sich eine Tabelle der durch den DHCP-Server zugewiesenen IP-Adressen mit den zugehörigen Geräte MAC-Adressen.

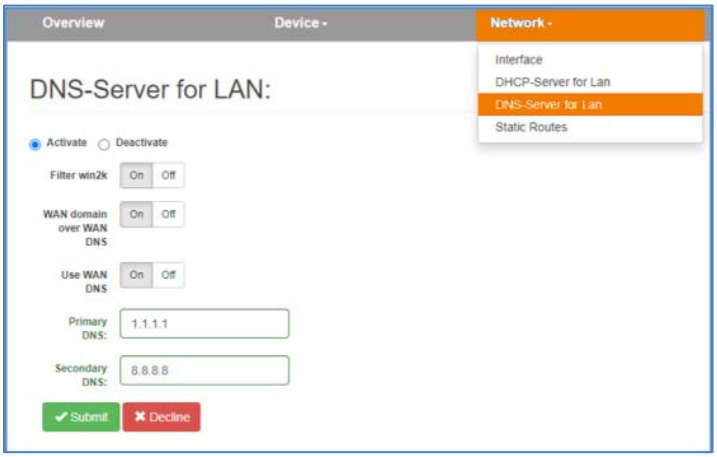
Mit "**Hide Expired**" kann die Liste der vergebenen IP-Adressen um die Einträge gekürzt werden, die nicht mehr aktiv sind.

11.2 DNS-Server für LAN

Für das LAN-Netzwerk des ETHERLINE® ACCESS NF04T kann ein DNS-Server aktiviert werden.

Der DNS-Server im ETHERLINE® ACCESS NF04T beantwortet DNS-Anfragen direkt auf dem LAN. Dazu benötigt ETHERLINE® ACCESS NF04T Zugriff auf DNS-Server auf der WAN-Schnittstelle.

Wird der DNS-Server im ETHERLINE® ACCESS NF04T verwendet, müssen die Geräte im LAN nicht durch den ETHERLINE® ACCESS NF04T hindurch auf DNS-Server zugreifen und es müssen dafür dann keine eignen Filterregeln angelegt werden.



Auf der Konfigurationsseite „**DNS-Server for Lan**“ können die vom ETHERLINE® ACCESS NF04T verwendeten DNS-Server (Primary, Secondary) angegeben werden.

Mit der Option „**Use WAN DNS**“, kann zusätzlich ein im WAN vorhandene DNS-Server verwendet werden. Dieser wird dann zuerst abgefragt.

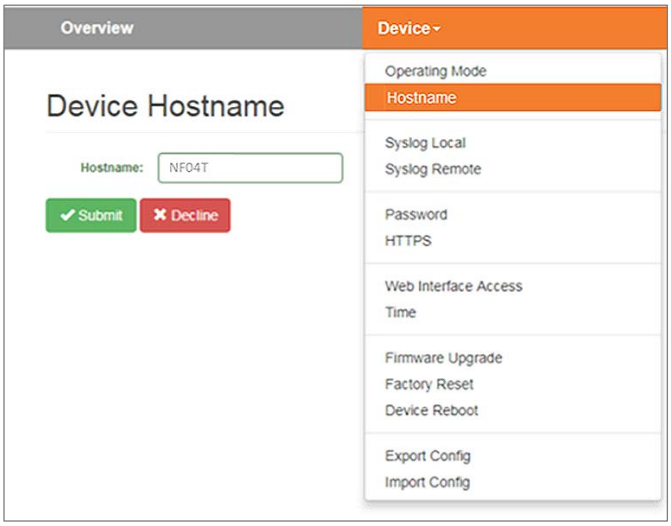
„**WAN domain over WAN DNS**“: Jede DNS-Abfrage wird normalerweise an alle DNS-Server aus der Liste (primär, sekundär, usw.) gesendet, unabhängig von der Domäne. Falls es eine Anfrage innerhalb der Domäne gibt, für die WAN-DNS zuständig ist, wird das Senden der Anfrage an WAN-DNS erzwungen.

„**Filter win2k**“ filtert periodische DNS-Anfragen, die vom öffentlichen DNS keine sinnvollen Antworten erhalten. Diese Anfragen können Probleme verursachen, indem sie Dial-on-Demand-Verbindungen auslösen.

11.3 Hostname (WAN)

Der DNS Hostname des ETHERLINE® ACCESS NF04T kann für die WAN-Schnittstelle festgelegt werden.

Der eingegebene Gerätehostname wird an den DHCP / DNS-Server übertragen, wenn die DHCP-Lease zugewiesen ist und der verwendete DHCP-Server die "DHCP Option 12" unterstützt. Immer wenn ein neuer Gerätename mit dieser Funktion festgelegt wird, wird die DHCP-Lease freigegeben und eine neue angefordert.



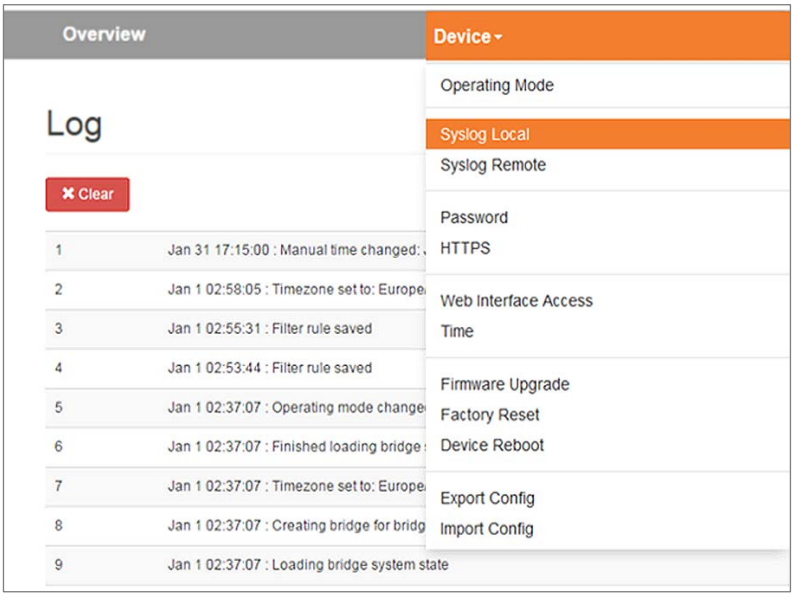
11.4 Syslog Server

Der im ETHERLINE® ACCESS NF04T verbaute Syslog Server protokolliert alle Benutzer- und Systemereignisse mit Uhrzeit und Datum. Benutzerereignisse sind Veränderungen der Konfiguration oder User Logins. Die Systemereignisse kommen aus dem Betriebssystem oder der laufenden Applikation. Damit der Syslog Server die Zeit korrekt anzeigt, muss diese im Menü "Time" eingestellt sein (siehe Kap. 11.8).

11.4.1 Syslog Local

Die lokale Syslog Anzeige listet die aufgezeichneten Ereignisse auf.

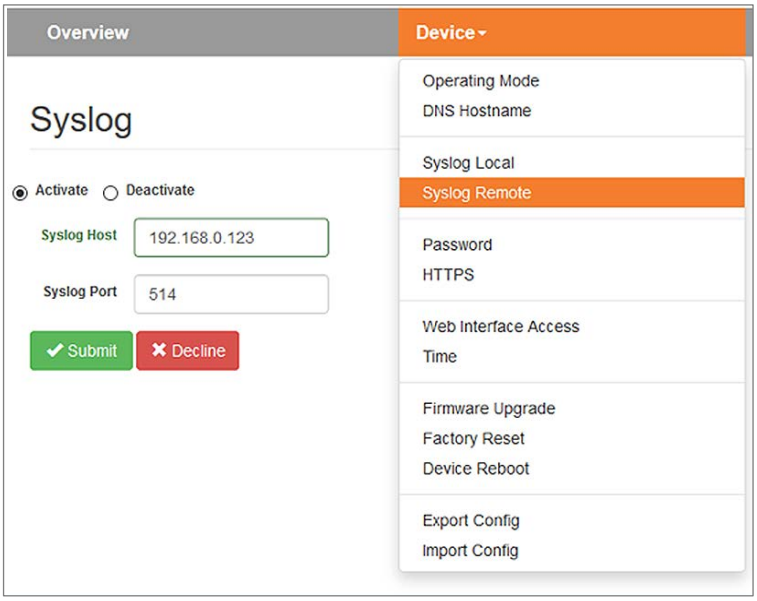
Mit "Clear" kann der Syslog-Speicher gelöscht werden.



11.4.2 Syslog Remote

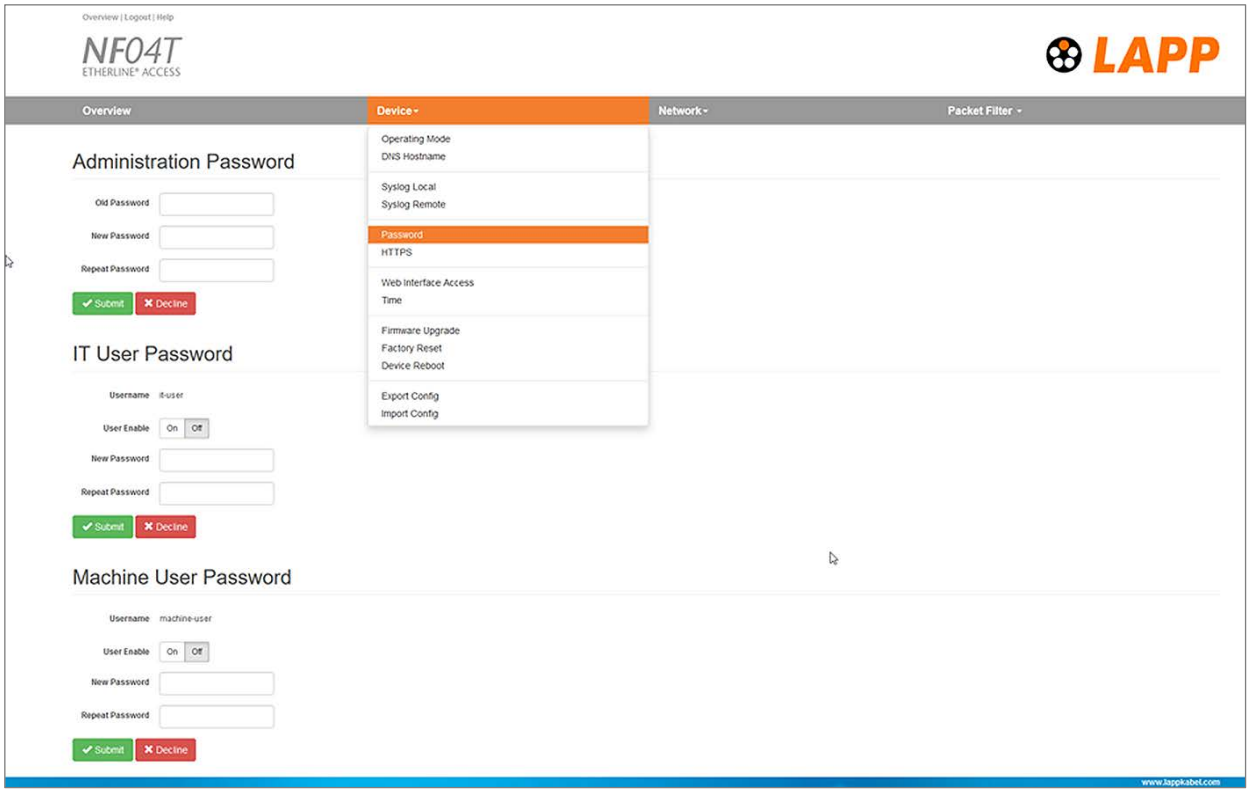
Die Syslog Nachrichten können vom ETHERLINE® ACCESS NF04T auch an einen PC über das Netzwerk gesendet werden, auf dem ein Programm zur Syslog Aufzeichnung läuft.

Die IP-Adresse des Host und der Port können hier angegeben werden.



11.5 Passwort ändern (Password) / Userverwaltung

Im Menü "Password" kann das Passwort das Administrators "admin" geändert werden sowie die weiteren User aktiviert und Passworte festgelegt oder geändert werden.



Neben dem User "admin", welcher uneingeschränkte Zugriffsrechte hat, unterstützt ETHERLINE® ACCESS NF04T noch zwei weitere User mit eingeschränkten Zugriffsrechten: "it-user" und "machine-user"

Zugriffsrechte des "it-user":

- Zugriff auf den ETHERLINE® ACCESS NF04T ausschließlich über das WAN-Interface
- Hostname ändern
- Update TLS Zertifikat
- Einstellung Remote Syslog server
- DHCP-Client für WAN ändern
- Gerät neu starten
- ETHERLINE® ACCESS NF04T Konfiguration exportieren
- Passwort des "it-user" ändern
- Datum und Uhrzeit Einstellungen bearbeiten
- Alle anderen Einstellungen sind "ReadOnly"

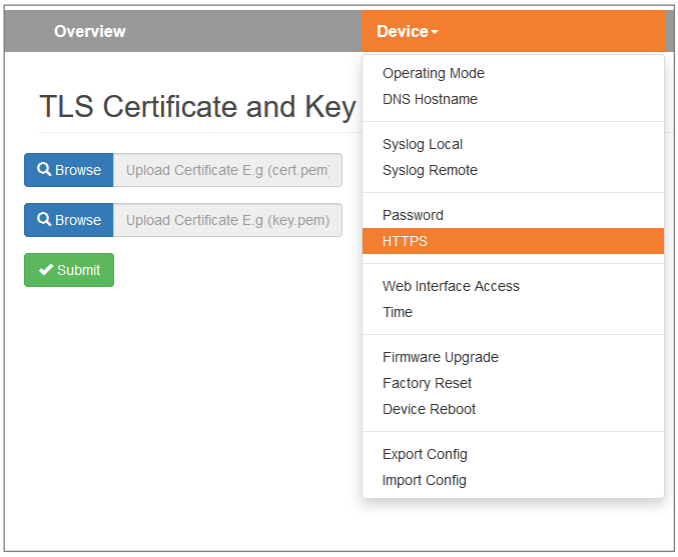
Zugriffsrechte "machine-user":

- Zugriff auf den ETHERLINE® ACCESS NF04T ausschließlich über das LAN-Interface
- Änderung der Einstellungen des DHCP-servers
- Ändern der Basic NAT/NAPT Regeln und Einstellungen
- Ändern aller Paketfilter Regeln
- Ändern der MAC-Filter Regeln
- Ändern der Static Routing Regeln
- Passwort des "machine-user" ändern
- Gerät neu starten
- ETHERLINE® ACCESS NF04T Konfiguration exportieren
- Alle anderen Einstellungen sind "ReadOnly"

11.6 Zertifikat hinterlegen (HTTPS)

Für die Webseite des ETHERLINE® ACCESS NF04T kann ein firmeneigenes Zertifikat hinterlegt werden.

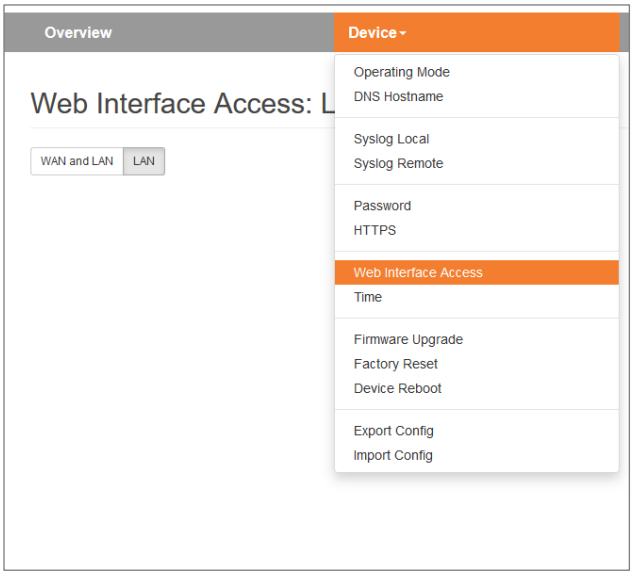
Damit kann sichergestellt werden, dass der Aufruf der ETHERLINE® ACCESS NF04T Konfigurationswebseite neben der HTTPS-Verschlüsselung auch vertrauenswürdig ist.



11.7 Web Interface Zugriff im WAN-Netzwerk erlauben (Web Interface Access)

Das Webinterface ist aus Sicherheitsgründen standardmäßig nur über das LAN-Netzwerk erreichbar.

Soll das Webinterface auch im WAN-Netzwerk erreichbar sein, kann das im Menü "Web Interface Access" eingestellt werden → "WAN and LAN".

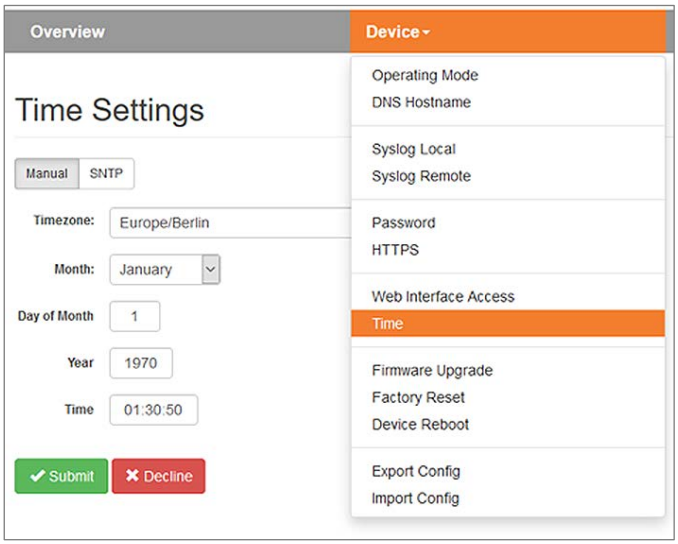


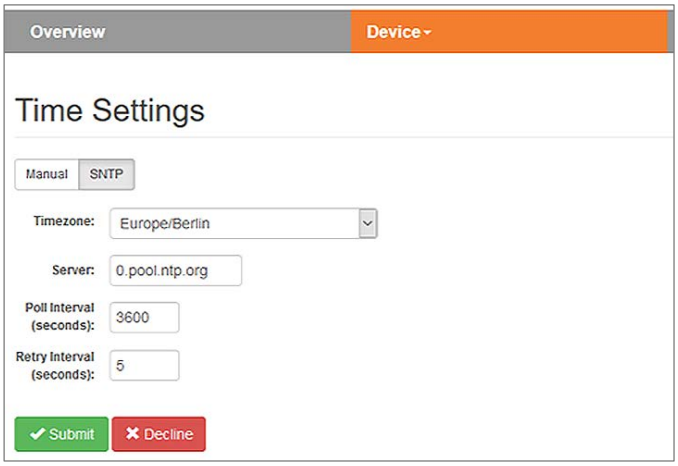
11.8 Zeiteinstellungen (Time)

Im Menü "Time" kann die Uhrzeit des ETHERLINE® ACCESS NF04T eingestellt werden.

Die Uhrzeit wird hauptsächlich für die Syslog-Aufzeichnungen benötigt.

Die Uhrzeit kann entweder manuell eingestellt werden oder von einem SNTP Server ("Simple Network Time Protocol") automatisch geholt werden.





ACHTUNG

Die manuell eingestellte Uhrzeit wird bei Spannungsausfall nicht gespeichert. Für eine immer verfügbare Zeit sollte "SNTP" verwendet werden.

ACHTUNG

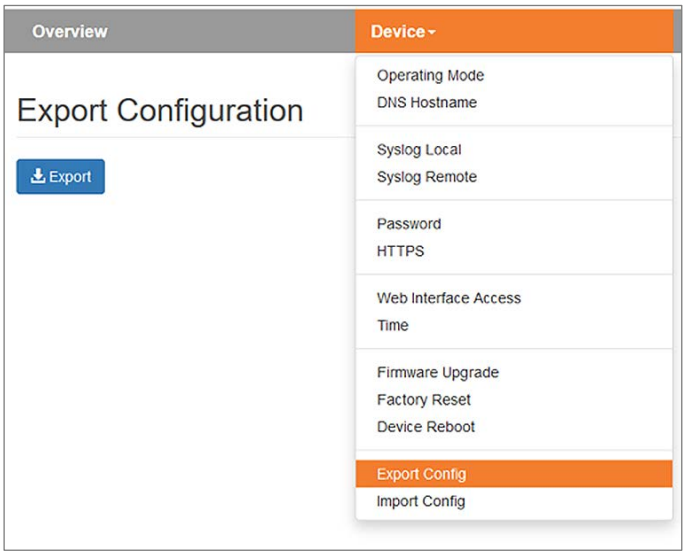
Für "SNTP" müssen in den Interfaceeinstellungen des ETHERLINE® ACCESS NF04T das Default-Gateway und der DNS-Server konfiguriert sein, damit der SNTP Dienst den NTP-Server im Internet erreichen kann

11.9 Export / Import der Konfiguration

Die Konfiguration des ETHERLINE® ACCESS NF04T kann in eine lesbare Konfigurationsdatei exportiert und auch wieder importiert werden.

Damit ist es möglich sowohl ein Backup einer ETHERLINE® ACCESS NF04T Konfiguration zu sichern als auch eine bestehende Konfiguration für einen neuen ETHERLINE® ACCESS NF04T mit ähnlicher Anwendung zu kopieren.

Die Konfigurationsdateien hat die Dateiendung "CFG".



Beispiel einer ETHERLINE® ACCESS NF04T Konfigurationsdatei:

```
general :
{
        router-mode = true;
        web-wan-access = false;
        intip = "192.168.0.100";
        intip-netmask = "255.255.255.0";
        extip = "10.10.1.99";
        extip-netmask = "255.255.255.0";
        dnsip = "0.0.0.0";
        gatewayip = "0.0.0.0";
        rsyslog :
        {
                active = false;
                host = "0.0.0.0";
                port = 514;
        };
        time :
        {
                sntp = false;
                zone = "Europe/Berlin";
                sntp-host = "0.pool.ntp.org";
                poll-interval = 3600;
                retry-interval = 5;
        ;
};
...
```

12 Firmwareupdate

Die aktuellste Firmware des ETHERLINE® ACCESS NF04T kann über die Webseite aktualisiert werden.

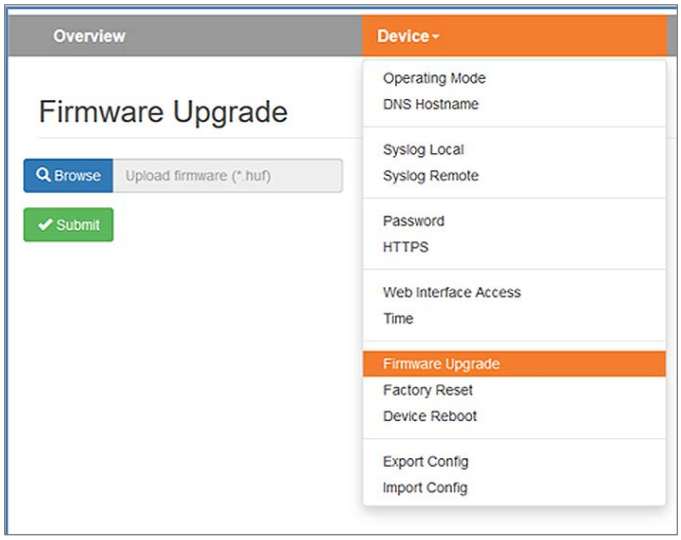
Link zur aktuellsten Firmware:
www.lappkabel.com/activenetworkcomponents

Die Firmwaredatei kann an der Dateiendung "HUF" erkannt werden
und ist verschlüsselt, um diese vor einer Veränderung zu schützen.

Legen Sie die Firmwaredatei auf Ihrem PC ab und wählen den Speicherort mit "Browse" aus.

Danach wird die Firmwaredatei auf den ETHERLINE® ACCESS NF04T übertragen - das kann je nach Netzverbindung - bis zu 1 Minute dauern.

Im ETHERLINE® ACCESS NF04T wird die Firmwaredatei entschlüsselt und überprüft. Ist der Inhalt korrekt wird die Firmware in den Programmspeicher gebrannt und ein Neustart des ETHERLINE® ACCESS NF04T durchgeführt.



ACHTUNG

Während dem Updatevorgang ist der Betrieb des ETHERLINE® ACCESS NF04T unterbrochen. Schalten Sie das Gerät während dem Updatevorgang nicht aus!

HINWEIS

Die Konfiguration des ETHERLINE® ACCESS NF04T wird bei einem Update auf eine höhere Version soweit es technisch möglich ist beibehalten. Ein "Downgrade" auf eine ältere Firmwareversion kann aber zu Konfigurations-fehlern führen. Es wird empfohlen nach einem Downgrade ein Werksrücksetzen durchzuführen.

HINWEIS

Nach einem Firmwareupdate ist es ggf. notwendig den Browser Cache einmal zu löschen, um veraltete JavaScript Elemente der ETHERLINE® ACCESS NF04T Webseite zu aktualisieren.

13 Rückstellen auf Werkseinstellung

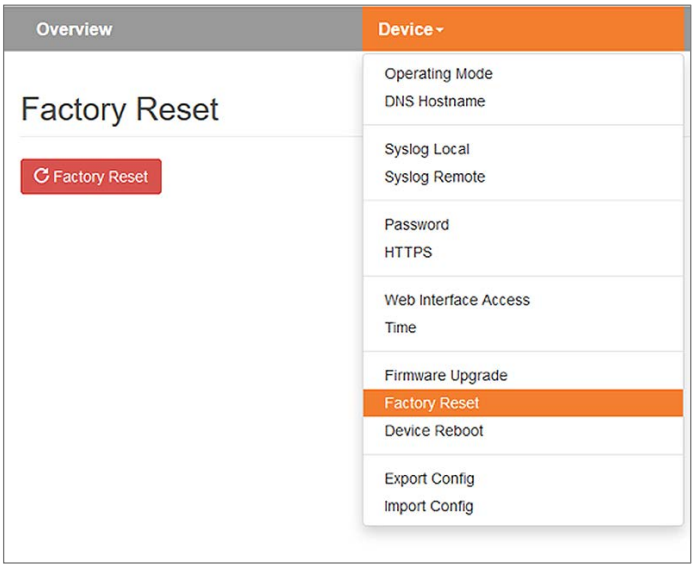
Das Rückstellen des ETHERLINE® ACCESS NF04T auf Werkseinstellung kann sowohl über die Webseite ausgelöst werden als auch ohne Zugriff auf das Gerät durch den „FCN“-Taster.

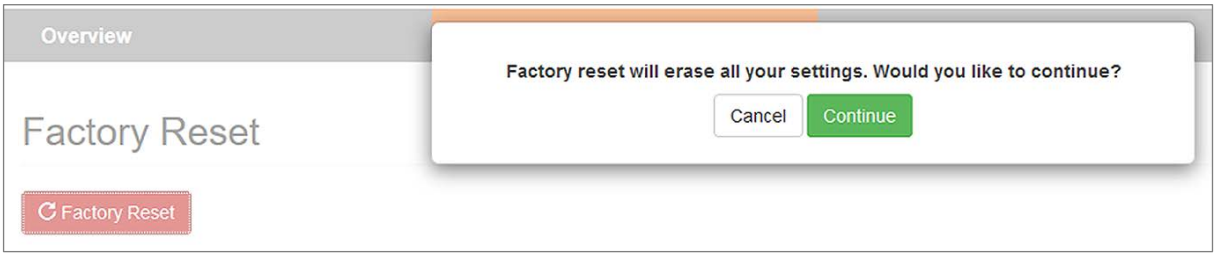
Es werden beim Rücksetzen des ETHERLINE® ACCESS NF04T die Konfiguration unwiederbringlich gelöscht und die IP-Einstellungen auf den Auslieferzustand gesetzt. Die Firmware bleibt dabei auf dem aktuellen Stand.

13.1 Rückstellen auf Werkseinstellung über Webseite

Wählen Sie im Menü „Device“ den Menüpunkt „Factory Reset“.

Drücken Sie den Button „Factory Reset“ und bestätigen die Sicherheitsabfrage.





13.2 Rückstellen auf Werkseinstellung über Taster

Um ETHERLINE® ACCESS NF04T in den Auslieferungszustand zurückzustellen, muss der „FCN“-Taster gedrückt gehalten sein, während das Gerät neu gestartet wird. Das erfolgreiche Zurücksetzen der Parameter und Einstellungen wird durch das aufleuchten der „USR“-LED angezeigt. Der „FCN“-Taster kann dann losgelassen werden.

Einen Neustart des ETHERLINE® ACCESS NF04T können Sie mit dem Taster „RST“ auslösen oder die Spannung aus- und wieder einschalten.

14 FAQ

Werden Broadcasts oder Multicasts durch den ETHERLINE® ACCESS NF04T durchgelassen?

ETHERLINE® ACCESS NF04T ist ein TCP/IP NAT oder Bridge Gerät. Es arbeitet auf Layer 3 und 4. Broadcasts und Multicasts werden am ETHERLINE® ACCESS NF04T in beide Richtungen (LAN→WAN und WAN→LAN) geblockt. Die Blockung von Broadcasts reduziert damit auch die Bus-Last in den beiden Netzwerken und erhöht die Echtzeitfähigkeit des Maschinennetzwerks.

Kann ich über den ETHERLINE® ACCESS NF04T PROFINET RT Telegramme senden?

Nein, PROFINET RT Telegramme werden vom ETHERLINE® ACCESS NF04T geblockt.

Was muss ich beachten, wenn ich über den ETHERLINE® ACCESS NF04T mit dem Simatic Manager oder dem TIA Portal (WAN) mit einer CPU im LAN arbeiten will?

Im Betriebsmodus NAT muss in der CPU die LAN-Adresse des ETHERLINE® ACCESS NF04T als Router eingetragen werden, damit die Antworten der CPU den Weg zurück zum PC im WAN finden. Weitere Informationen zu diesem Anwendungsfall finden Sie im Kapitel 10.

Kann der ETHERLINE® ACCESS NF04T mehrere Konfigurationen speichern?

Nein, ETHERLINE® ACCESS NF04T hat immer nur eine aktuelle Konfiguration. Es ist aber möglich einzelne Paketfilter Regeln oder NAT Einträge über das Lampensymbol zu deaktivieren oder aktivieren. Des Weiteren ist es möglich eine ETHERLINE® ACCESS NF04T Konfiguration zu exportieren, zu bearbeiten und wieder zu importieren.

Wo kann ich erkennen ob ich die neueste Firmware habe und wo finde ich die neueste Firmware?

In der "Overview" Webseite des ETHERLINE® ACCESS NF04T wird die aktive Firmware des ETHERLINE® ACCESS NF04T angezeigt.

Die aktuellste Firmware kann auf der Webseite www.lappkabel.com/activenetworkcomponents heruntergeladen werden.

Das Einspielen der Firmware ist im Kapitel 12 beschrieben.

15 Technische Daten

Artikelnummer	21700141
Name	ETHERLINE® ACCESS NF04T
Lieferumfang	ETHERLINE® ACCESS NF04T, Quick Start Guide
Abmessungen (T x B x H)	35 x 59 x 76 mm
Gewicht	ca. 130 g
WAN-Schnittstelle	
Anzahl	1
Typ	10-Base-T/100-Base-T
Anschluss	RJ45 Buchse
Übertragungsrate	10/100 Mbit/s
LAN-Schnittstelle	
Anzahl	3, geswitcht
Typ	10-Base-T/100-Base-T
Anschluss	RJ45 Buchse
Übertragungsrate	10/100 Mbit/s
Betriebsmodi	Bridge, NAT (Basic NAT, NAPT)
Paketfilter	IPV4-Adressen, Protokoll (TCP/UDP), Ports („WAN to LAN“ und „LAN to WAN“ getrennt) MAC-Adressen (Black- & Whitelisting)
Statusanzeige	4 LEDs Funktions-Status, 8 LEDs Ethernet-Status
Spannungsversorgung	DC 24 V, 18–30 V DC
Stromaufnahme	max. 250 mA bei DC 24 V
Umgebungsbedingungen	
Einbaulage	beliebig
Umgebungstemperatur	-40 °C ... +75°C
Transport- und Lagertemperatur	-40 °C ... +85°C
Relative Luftfeuchte	95 % r. H. ohne Betauung
Verschmutzungsgrad	2
Schutzart	IP20
Zertifizierungen	CE, UL
UL	
UL	UL 61010-1/UL61010-2-201
Voltage supply	DC 24 V (18 ... 30 VDC, SELV and limited energy circuit)
Pullution degree	2
Altitude	up to 2000m
Temperature cable rating	87°C
CE	
RoHS	Ja
REACH	Ja

15.1 Maßzeichnung