PROG. CNTLR.
E482663

RA10C - Kompakte Industrie-Firewall

Schnelleinstieg zur Inbetriebnahme **DE** (V 1.2.9 08. 08. 2023)

NFH100 - ab **HW02**

LP1174C

Inhalt

Dieses Dokument ist gültig für die
Kompakte Industrie-Firewall RA10C0000000S0D0 und RA10C000000000DA,
in dieser Anleitung auch als NFH100 bezeichnet; in Hardware-Ausführung ab HW 02.

Diese Kurzanleitung bietet Ihnen eine schnelle Übersicht zu ausgewählten Bedienvorgängen und Funktionen der kompakten Industrie-Firewall (NFH100). Sie kann jedoch das ausführliche Handbuch mit den wichtigen Erläuterungen und Warnhinweisen nicht ersetzen.

Lesen Sie die folgenden Hinweise aufmerksam durch und bewahren Sie dieses Dokument sorgfältig auf.
Neueste Informationen, Aktualisierungen sowie das komplette Gerätehandbuch finden Sie auf unseren Internetseiten unter www.redlion.net.

1 Sicherheitshinweise

- Montage, Installation und Inbetriebnahme des Gerätes darf nur durch qualifiziertes Fachpersonal ausgeführt werden. Die jeweiligen nationalen Sicherheits- und Unfallverhütungsvorschriften sind einzuhalten.
- Das Gerät ist nach dem Stand der Technik und den anerkannten sicherheitstechnischen Regeln gebaut (siehe Konformitätserklärung).
- Das Gerät ist ausschließlich für den Betrieb im Schaltschrank und mit Sicherheitskleinspannung (SELV) nach IEC 60950/EN 60950/VDE 0805 ausgelegt.
- Das Gerät darf nur an Geräte angeschlossen werden, die die Bedingungen der EN 60950 erfüllen.
- Das Gerät ist nur für die Anwendung innerhalb von Gebäuden und nicht im Freien vorgesehen.
- Öffnen Sie niemals das Gehäuse des Gerätes. Durch unbefugtes Öffnen und unsachgemäße Reparatur können Gefahren für Benutzer des Gerätes entstehen. Der Hersteller übernimmt für eigenmächtige Veränderungen keinerlei Gewährleistung.

Die Garantie erlischt mit dem Öffnen des Gerätes!

ACHTUNG: Elektrostatische Entladung!
Beachten Sie die notwendigen Vorsichtsmaßnahmen bei der Handhabung elektrostatisch gefährdeter Bauelemente (EN 61340-5-1 und IEC 61340-5-1)!

2 Wartung

Bei den kompakten Industrie-Firewalls handelt es sich um wartungsfreie Einheiten. Sollte eine Industrie-Firewall Beschädigungen oder Funktionsstörungen aufweisen, so ist das Gerät unverzüglich außer Betrieb zu setzen und gegen unbeabsichtigten Betrieb zu sichern.

NOTE

Unabhängig von der wartungsfreien Hardware besteht Handlungsbedarf in Sachen IT-Sicherheit.

- Halten Sie die Software / Firmware auf dem neuesten Stand.
- Informieren Sie sich regelmäßig über Sicherheitsupdates des Produkts..

Informationen hierzu finden Sie unter www.redlion.net

3 Verwendung von Open-Source-Software

3.1 Allgemeines

Unsere Produkte beinhalten unter anderem auch sogenannte Open-Source-Software, die von Dritten hergestellt und für die freie Verwendung durch jedermann veröffentlicht wurde. Die Open-Source-Software steht unter besonderen Open-Source-Softwarelizenzen und dem Urheberrecht Dritter. Jeder Kunde kann die Open-Source-Software nach den Lizenzbestimmungen der jeweiligen Hersteller grundsätzlich frei verwenden.

Die Rechte des Kunden, die Open-Source-Software über den Zweck unserer Produkte hinaus zu verwenden, werden im Detail von dem jeweils betroffenen Open-Source-Softwarelizenzen geregelt. Der Kunde kann die Open-Source-Software, so wie in der jeweiligen gültigen Lizenz vorgesehen, über die Zweckbestimmung, die die Open-Source-Software in unseren Produkten erfährt, hinaus frei verwenden. Für den Fall, dass zwischen unseren Lizenzbestimmungen für eines unserer Produkte und der jeweiligen Open-Source-Softwarelizenz ein Widerspruch besteht, geht die jeweils einschlägige Open-Source-Softwarelizenz unseren Lizenzbedingungen vor, soweit die jeweilige Open-Source-Software hiervon betroffen ist

Die Nutzung der verwendeten Open-Source-Software ist unentgeltlich möglich. Wir erheben für die Benutzung der Open-Source-Software, die in unseren Produkten enthalten sind, keine Nutzungsgebühren oder vergleichbare Gebühren. Die Benutzung der Open-Source-Software durch den Kunden in unseren Produkten ist nicht Bestandteil des Gewinns, den wir mit der vertraglichen Vergütung erzielen.

Aus der erhältlichen Liste ergeben sich alle Open-Source-Softwareprogramme, die in unseren Produkten enthalten sind. Die wichtigsten Open-Source-Softwarelizenzen sind im Abschnitt Lizenzen am Ende dieser Publikation aufgeführt.

Soweit Programme, die in unseren Produkten enthalten sind, unter der GNU General Public License (GPL), GNU Lesser General Public License (LGPL), der Berkeley Software Distribution (BSD), des Massachusetts Institute of Technology (MIT) oder einer anderen Open-Source-Softwarelizenz stehen, die vorschreibt, dass der Quellcode zur Verfügung zu stellen ist, und sollte diese Software nicht bereits mit unserem Produkt auf einem Datenträger oder im Quellcode mitgeliefert worden sein, so übersenden wir diesen jederzeit auf Nachfrage. Unser Angebot, den Quellcode auf Nachfrage zu versenden, endet automatisch mit Ablauf von 3 Jahren nach Lieferung des jeweiligen Produkts an den Kunden.

Anfragen sind insoweit möglichst unter Angabe der Seriennummer des jeweiligen Produktes an folgende Adresse zu senden:

Red Lion Controls, Inc.
35 Willow Springs Circle
York, PA 17406

Tel: Innerhalb der USA: +1 (877) 432-9908
Außerhalb der USA: +1 (717) 767-6511
Website: www.redlion.net
Support: support.redlion.net

3.2 Besondere Haftungsbestimmungen

Wir übernehmen keine Gewährleistung und Haftung, wenn die Open-Source-Softwareprogramme, die in unseren Produkten enthalten sind, vom Kunden in einer Art und Weise verwendet werden, die nicht mehr dem Zweck des Vertrages, der dem Erwerb eines unserer Produkte zu Grunde liegt, entspricht. Dies betrifft insbesondere jede Verwendung der Open-Source-Softwareprogramme außerhalb unserer Produkte. Für die Verwendung der Open-Source-Software jenseits des Vertragszwecks gelten die Gewährleistungs- und Haftungsbestimmungen, die die jeweils gültige Open-Source-Softwarelizenz für die entsprechende Open-Source-Software, wie nachstehend aufgeführt, vorsieht. Wir haften insbesondere auch nicht, wenn die Open-Source-Software in unseren Produkten oder die gesamte Softwarekonfiguration in unseren Produkten geändert wird. Die mit dem Vertrag, der dem Erwerb unserer Produkte zugrunde liegt, gegebene Gewährleistung gilt nur für die unveränderte Open-Source-Software und die unveränderte Softwarekonfiguration in unseren Produkten.

3.3 Verwendete Open-Source-Software

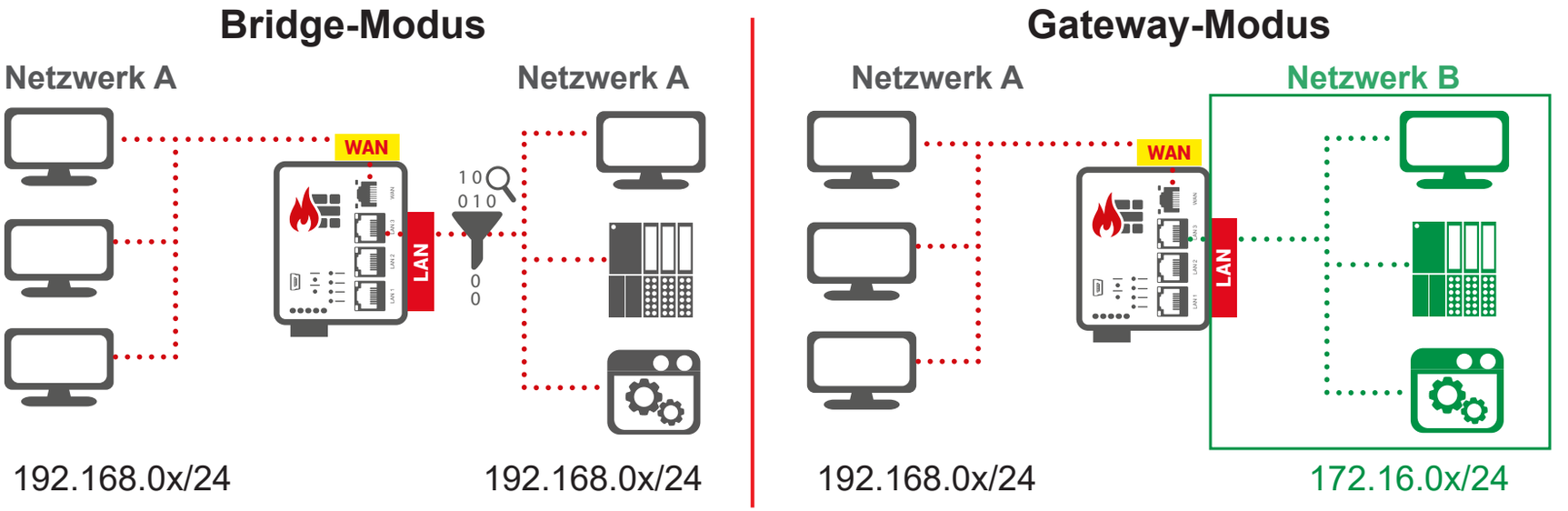
Eine Liste der in unseren Produkten verwendeten Open-Source-Software finden Sie unter

https://mbconnectline.com/de/downloadportal/

https://bit.ly/3DzJi3P

4 Kurzbeschreibung

RA10C ist eine „selbstlernende“ einfach zu konfigurierende Industrie-Firewall, die sowohl im Bridge- wie auch im Gateway-Modus betrieben werden kann.



Die Konfiguration erfolgt über die USB-Schnittstelle mittels Software **mbNETFIX Manager** (nicht im Lieferumfang enthalten).

Die Software kann unter **www.redlion.net** kostenlos heruntergeladen werden.

5 Leistungsmerkmale

- Schutz der Maschinen im Netzwerk vor Angriffen aus dem Internet
- einfache Netzwerksegmentierung durch Routing und NAT
- bequemes Erstellen von Filtertabellen dank Lernmodus
- Integration in bestehende Netzwerke
- Bridge- oder Gatewaymodus
- IP-, Port- und Protokollfilter zur Überwachung und Einschränkung des Datenverkehrs
- Konfiguration per sicherer Software
- weniger Angriffsvektoren durch Verzicht auf ein Webinterface
- vielfältige NAT-Funktionalitäten, z. B. 1:1 NAT, SimpleNAT und Portforwarding

6 Lieferumfang

Überprüfen Sie den Packungsinhalt auf Vollständigkeit:

1 x Firewall RA10C

1 x Steckbrücke

1 x Kabel USB A - USB-mini B

1 x Kurzanleitung

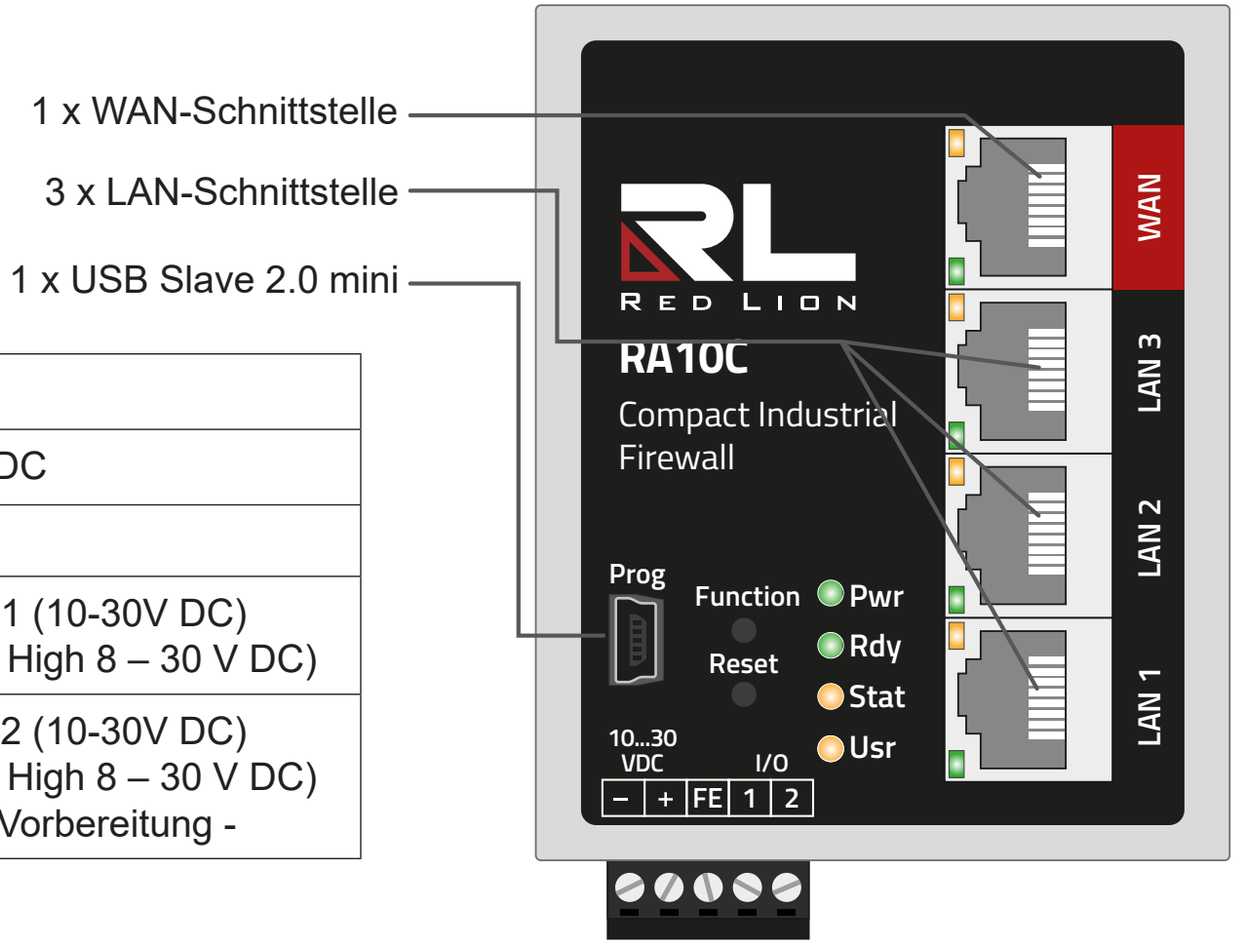
Sollte eines dieser Teile fehlen oder beschädigt sein, wenden Sie sich bitte an folgende Adresse:

Red Lion Controls, Inc.
35 Willow Springs Circle
York, PA 17406

Tel: Innerhalb der USA: +1 (877) 432-9908
Außerhalb der USA: +1 (717) 767-6511
Website: www.redlion.net
Support: support.redlion.net

Bewahren Sie den Originalkarton sowie das Original-Verpackungsmaterial für den Fall auf, dass Sie das Gerät zu einem späteren Zeitpunkt zur Reparatur einsenden müssen.

7 Anzeige-, Bedienelemente und Anschlüsse



–	Anschluss 0V DC
+	Anschluss 10-30V DC
FE	Funktionserde
I1*	Digitaler Eingang E1 (10-30V DC) (Low 0 – 3,2 V DC, High 8 – 30 V DC)
I2	Digitaler Eingang E2 (10-30V DC) (Low 0 – 3,2 V DC, High 8 – 30 V DC) - Funktion in Vorbereitung -

* Eingang 1 kann bei der Erstinbetriebnahme dazu verwendet werden, die Betriebsart Bridge mit ausgeschaltetem Paketfilter zu aktivieren.
Der Eingang wird nur ausgewertet, bis die ***Firewall*** einmalig konfiguriert wurde, danach wird der Zustand von Eingang 1 ignoriert.

Bezeichnung	Status	Beschreibung
Prog (Programming)	–	USB-Schnittstelle Mini-B zum Verbinden mit dem Konfigurations-PC
Function	–	Taster - Funktion in Vorbereitung.
Reset	–	Taster - Durchführen eines Geräte-Neustarts (Kaltstart).

Bezeichnung	Status	Beschreibung
Pwr (Power)	LED aus	Die Stromversorgung für das Gerät ist ausgeschaltet bzw. das Gerät ist nicht an die Stromversorgung/Netzteil angeschlossen.
	LED ein	Die Stromversorgung ist an der Klemmleiste des Gerätes angeschlossen und eingeschaltet.
Rdy (Ready)	LED blinkt	Sobald das System überprüft wurde und startet, blinkt die LED für die Dauer des Bootvorgangs.
	LED ein	Das Gerät ist betriebsbereit.
Stat (Status)	LED ein	Der Paketfilter ist in beide Richtungen (WAN > LAN, LAN > WAN) aktiv.
	LED aus	Der Paketfilter ist in beide Richtungen (WAN > LAN, LAN > WAN) INAKTIV.
	LED blinkt	Der Paketfilter ist in mindestens einer Richtungen (WAN > LAN, LAN > WAN) INAKTIV.
Usr (User)	LED ein	Das Gerät ist nicht konfiguriert.
	LED aus	Das Gerät wurde durch die Software mbNETFIX Manager konfiguriert.
WAN	-	WAN-Anschluss (Rechnernetzwerk, DSL-Router etc.)
WAN-LED	orange LED blinkt	Netzwerkdatenverkehr aktiv
	grüne LED ein	Übertragungsrate = 100 MBit/s
	grüne LED aus	Übertragungsrate = 10 MBit/s
LAN 1 – 3	-	LAN-Anschluss (Maschinennetz)
LAN LED 1 – 3	orange LED blinkt	Netzwerkdatenverkehr aktiv
	grüne LED ein	Übertragungsrate = 100 MBit/s
	grüne LED aus	Übertragungsrate = 10 MBit/s

8 Erstinbetriebnahme

Vor der Verbindung des Gerätes mit einem Netzwerk oder mit einem PC muss das Gerät ordnungsgemäß an die Versorgungsspannung angeschlossen werden, da sonst weitere Geräte beschädigt oder zerstört werden können.

Die kompakte Industrie-Firewall kann in zwei Modi betrieben werden (siehe hierzu Kap.4). Vor der Erstinbebtriebnahme und nach jedem Werkseinstellungs-Reset, ist die ***Firewall*** grundsätzlich in der Betriebsart Bridge, mit aktivem Paketfilter in beide Richtungen, eingestellt (Security By Default). Der Paketfilter kann durch Beschaltung von Eingang 1 (High 8 – 30 VDC) INAKTIV geschaltet werden.
Wählen Sie die Voreinstellung per Eingang 1, wenn einer dieser Punkte zutrifft:

Sie möchten die ***Firewall*** als Bridge betreiben
und die Konfiguration zu einem späteren Zeitpunkt vornehmen
und die Installation jetzt schon durchführen
und Sie wollen das vorhandene Netzwerk nicht beeinflussen

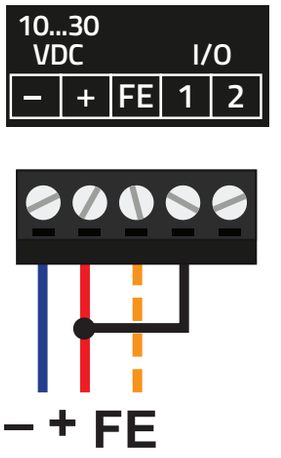
ODER

Sie möchten die Lernfunktion der ***Firewall*** aktivieren, um später bei der Konfiguration den gelernten Netzwerkverkehr auslesen zu können.

a. Bridge Mode:
Nach dem Bootvorgang ist der Paketfilter INAKTIV.

D. h.: die Übergänge WAN > LAN und LAN > WAN sind offen.
Alle anstehenden Verbindungsversuche/ Verbindungen werden detektiert.

Dieser Modus ist nur solange aktiv, bis das Gerät das erste Mal konfiguriert worden ist.



1. Schließen Sie den Potentialausgleich an Funktionserde **FE** an.
2. Verbinden Sie die Klemmen **I1** und **+** (I1 = high). Verwenden Sie hierfür die mitgelieferte Steckbrücke.
3. Schließen Sie das Gerät an die Versorgungsspannung (**DC 10 – 30 V**) an.

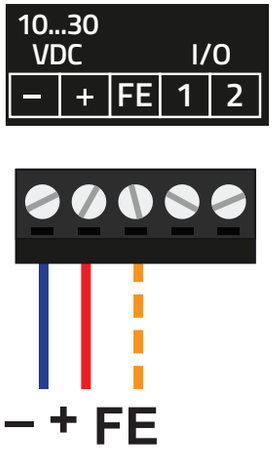
Achten Sie auf die richtige Polung!

HINWEIS

Der Eingang 1 wird nur ausgewertet, bis die kompakte Industrie-Firewall erstmalig konfiguriert wurde, danach wird der Zustand von Eingang 1 ignoriert.

b. **Bridge Mode mit aktivem Paketfilter** (Security by default)**:**
Nach dem Bootvorgang ist sowohl der Paketfilter als auch der Lernmodus aktiv.

D. h.: die Übergänge WAN > LAN und LAN > WAN sind blockiert. Alle anstehenden Verbindungsversuche werden detektiert.



1. Schließen Sie den Potentialausgleich an Funktionserde **FE** an.

2. Schließen Sie das Gerät an die Versorgungsspannung (**DC 10 – 30 V**) an.

Achten Sie auf die richtige Polung!

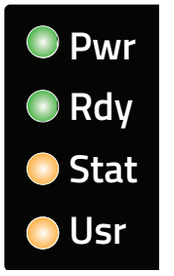
Nach dem Einschalten der Versorgungsspannung leuchtet die LED Pwr.

Sobald das System überprüft worden ist und startet, blinkt die LED Rdy für die Dauer des Bootvorgangs (ca. 90 Sek.).

Wenn die ***Firewall*** betriebsbereit, leuchten die LED Pwr + Rdy.

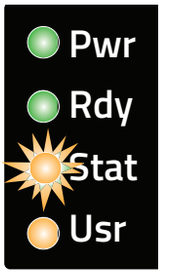
Leuchtcode im Bridge-Modus - Paketfilter aktiv -

LED Stat leuchtet => Firewall aktiv
LED Usr leuchtet => Gerät wurde noch nicht konfiguriert.

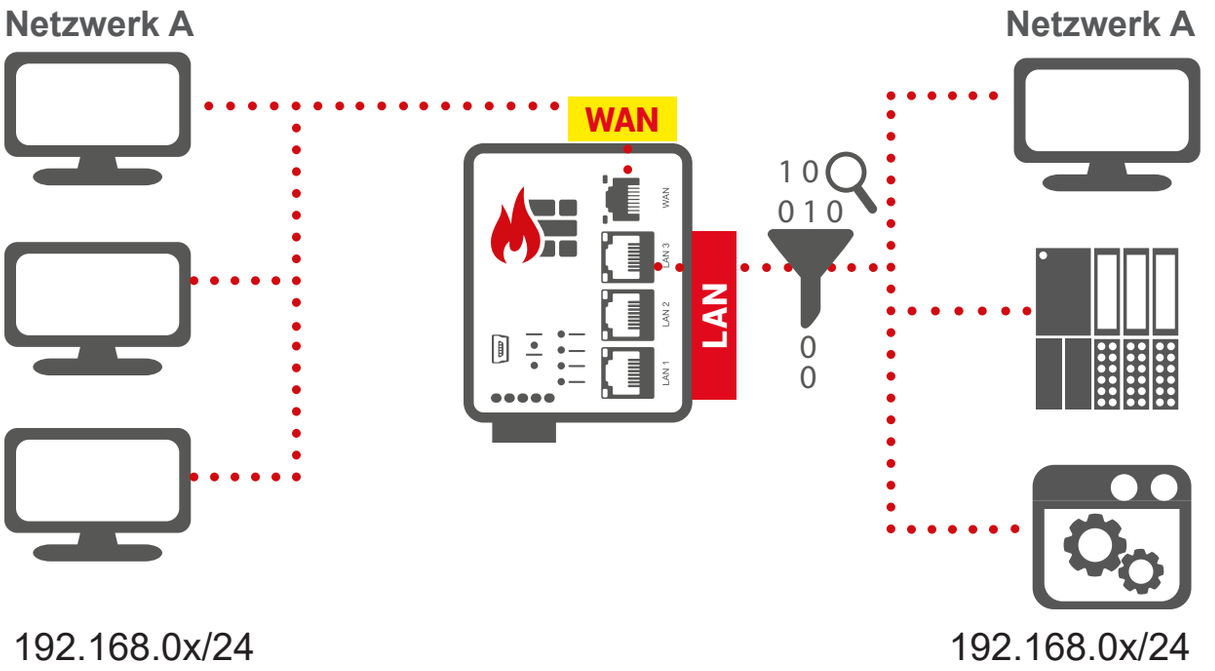


Leuchtcode im Bridge-Modus, Paketfilter INAKTIV

LED Stat blinkt => Paketfilter inaktiv
LED Usr leuchtet => Gerät wurde noch nicht konfiguriert.



9 Einsatz der kompakten Industrie-Firewall im Bridge-Modus



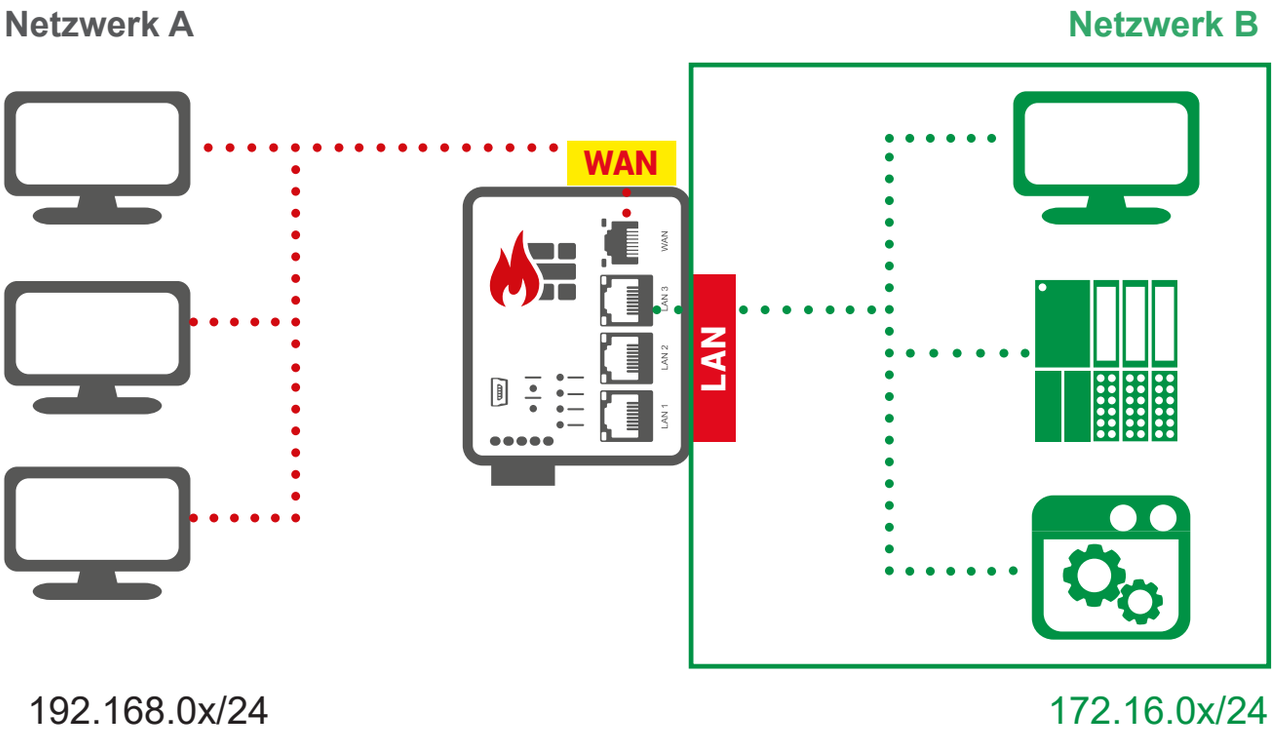
Wenn Sie die ***Firewall*** im Bridge-Modus einsetzen und unkonfiguriert in Ihre Netzwerkumgebung einbauen, starten Sie das Gerät im Bridge Mode mit Paketfilter INAKTIV (Eingang 1 = HIGH).

Nach dem Bootvorgang ist der Paketfilter inaktiv und der Lernmodus aktiv.
D. h.: die Übergänge WAN > LAN und LAN > WAN sind offen.
Alle anstehenden Verbindungsversuche/Verbindungen werden detektiert.

Der Eingang 1 wird nur ausgewertet, bis der mbNETFIX einmalig konfiguriert wurde, danach wird der Zustand von Eingang 1 ignoriert.

Verwenden Sie den Bridge-Modus, wenn sich Ihr Netzwerk auf der LAN- und WAN-Seite der ***Firewall*** im selben Netzwerksegment befindet (siehe Grafik oben mit den Beispiel-IP-Adressen).

10 Einsatz der kompakten Industrie-Firewall im Gateway-Modus



Wenn Sie die ***Firewall*** im Gateway-Modus einsetzen, starten Sie das Gerät im Bridge-Modus mit aktivem Paketfilter.

Nach dem Bootvorgang ist sowohl der Paketfilter als auch der Lernmodus aktiv.
D. h.: die Übergänge WAN > LAN und LAN > WAN sind blockiert.
Alle anstehenden Verbindungsversuche werden detektiert.

Verwenden Sie den Gateway-Modus, wenn sich Ihr Netzwerk an der LAN- und WAN-Seite der ***Firewall*** in unterschiedlichen Netzwerksegmenten befindet (siehe Grafik oben mit den IP-Beispiel-Adressen).

11 Konfiguration der kompakten Industrie-Firewall

Die Konfiguration der Firewall erfolgt über die USB-Schnittstelle mittels der Konfigurations-Software „**mbNETFIX Manager“** (nicht im Lieferumfang enthalten).

Der „**mbNETFIX Manager**“ bietet neben einer komfortablen grafischen Benutzeroberfläche (GUI) und einer Public-Key-Authentifizierung alle Funktionen die ein Automatisierer aus seiner SPS-Programmierumgebung kennt (z.B. exportieren, importieren, duplizieren, Onlinevergleich, Onlinefunktionen, etc).

Laden Sie die Konfigurations-Software „**mbNETFIX Manager**“ **kostenlos** unter dieser Adresse herunter: **www.redlion.net**

Nach der Installation können Sie den mbNETFIX für den jeweiligen Einsatzzweck assistentengestützt konfigurieren.

12 Werkseinstellungen bei Lieferung

Default-Einstellungen der ***Firewall***:

IP-Adresse (USB-Port):	169.254.0.1
Subnetzmaske:	255.255.0.0
Benutzer 1:	admin
Benutzer 2:	factoryreset
Passwort:	*Das Gerätepasswort befindet sich auf der Geräte-Rückseite und gilt sowohl für* Benutzer 1 *wie auch für* Benutzer 2*.*

13 Werkseinstellungen Laden (Factory Reset)

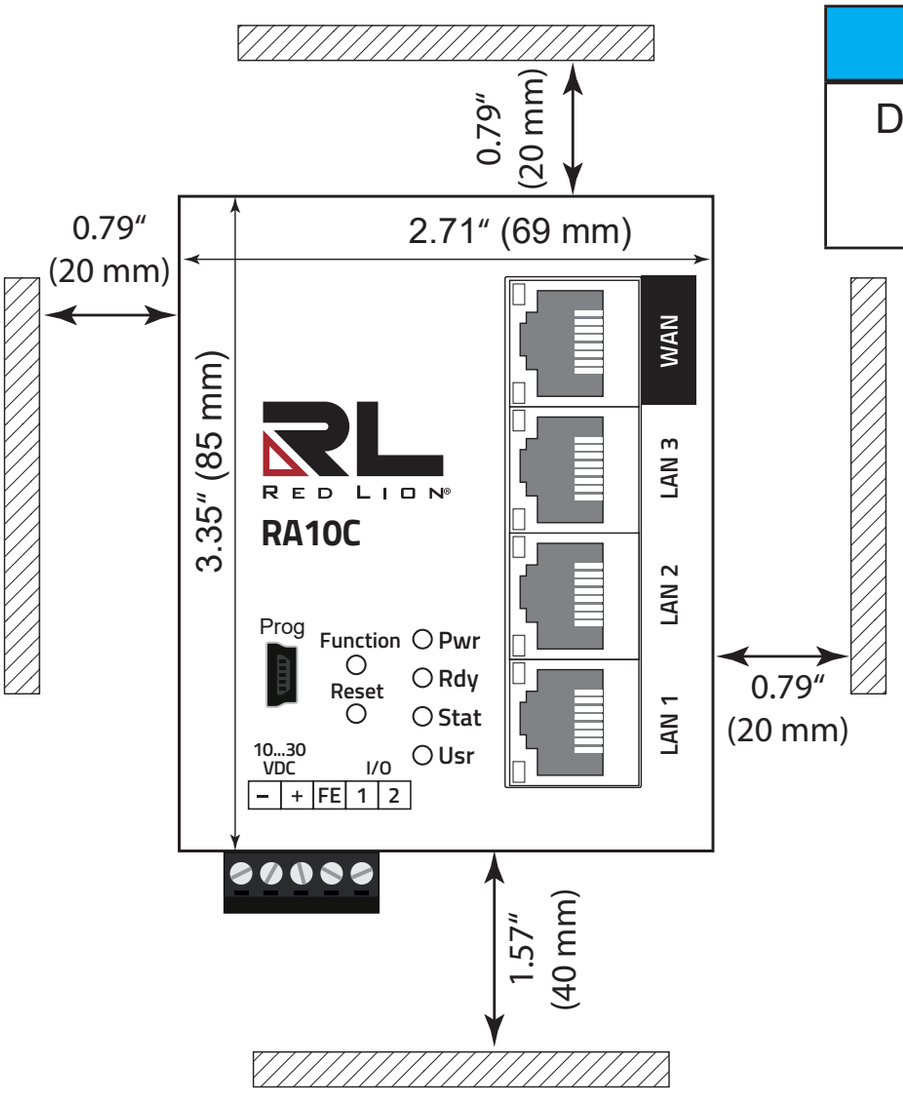
- Öffnen Sie im mbNETFIX Manager ein Projekt mit dem **Benutzer** „**factoryreset**“.
- Verbinden Sie sich mit der ***Firewall*** („**Online gehen**“).
- Wählen Sie im Menü „**Gerät**“ den Menüpunkt „**Werkseinstellungen zurücksetzen**“.
- Schließen Sie das Projekt und melden Sie sich wieder mit dem **Benutzer** „**admin**“ an.

Die Firewall wird nun auf seine ursprünglichen Werkseinstellungen zurückgesetzt und muss neu konfiguriert werden.

14 Geräte-Montage

Einbaulage/Mindestabstände

Das Gerät ist für die Montage auf Hutschienen
(gemäß DIN EN 50 022) konzipiert und für den Schaltschrankeinbau vorgesehen.
Die Installation und Montage muss nach VDE 0100 / IEC 364 erfolgen.
Der Router darf nur, wie beschrieben, in senkrechter Einbaulage montiert werden.



NOTICE

Die Nichteinhaltung der Mindestabstände kann das Gerät bei hohen Umgebungstemperaturen zerstören!

15 Technische Daten

Auszug aus dem technischen Datenblatt.
Die vollständigen technischen Daten finden Sie in unserem Support-Portal unter **www.redlion.net**

Leistungsdaten	
Spannung V (DC)	10 - 30 VDC (SELV and Limited Energy circuit)
Stromaufnahme	max. 250 mA @ 24 V
Temperatur (Betrieb)	-40 – +75 °C
Abmessungen	69 mm x 33.5 mm x 92.5 mm (B x T x H)
Gehäuse (Material)	Metall
Montage	Hutschienen-Montage

Schnittstellen	**Anzahl**	**Beschreibung**
USB-Schnittstellen	1 x	USB Slave 2.0 mini
Digitale Eingänge	2 x	10 – 30 V DC (Low 0 – 3,2 V DC, High 8 – 30 V DC)
LAN-Schnittstellen	3 x	10/100MBit/s Voll- und Halbduplexbetrieb, automatische Erkennung Patch-Kabel / Cross-Over-Kabel (autodetection)
WAN-Schnittstellen	1 x	10/100MBit/s Voll- und Halbduplexbetrieb, automatische Erkennung Patch-Kabel / Cross-Over-Kabel (autodetection)

16 Technischer Support

Technischen Support (FAQ, Fehlerbehebung, neueste Informationen usw.)
finden Sie auf unserer Website www.redlion.net.

Geben Sie bei Support-Anfragen immer die Seriennummer Ihres Routers an.
Support: support.redlion.net
Tel: Innerhalb der USA: +1 (877) 432-9908
Außerhalb der USA: +1 (717) 767-6511

17 Hinweise zur Cybersicherheit

Beachten Sie folgende Sicherheitsempfehlungen, 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. Siehe z.B. „ICS-Security-Kompendium“ vom BSI (Bundesamt für Sicherheit in der Informationstechnik) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html; gekürzte URL: **http://bit.ly/1rP9znm**

Physischer Zugang

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

Sicherheit der Software

- Halten Sie die Soft-/Firmware aktuell.
  -> Informieren Sie sich regelmäßig über Sicherheitsupdates des Produkts.
  -> Informieren Sie sich regelmäßig über Produkt-Updates.

Informationen hierzu finden Sie unter: **www.redlion.net.**

Passwörter

- Definieren Sie Regeln für die Nutzung der Geräte und die Vergabe von Passwörtern.
- Ändern Sie regelmäßig die Passwörter, um die Sicherheit zu erhöhen.
- 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 dasselbe Passwort nicht für verschiedene Benutzer und Systeme.

18 Entsorgung von Altgeräten

HINWEIS
Bevor Sie ein Altgerät entsorgen, stellen Sie sicher, dass alle Gerätedaten oder/und personenbezogenen Daten sowie die Gerätekonfiguration komplett gelöscht worden sind. 1. Entfernen/löschen Sie **alle** Speichermedien die mit dem Gerät verbunden sind. 2. Trennen Sie das Gerät von allen Netzwerken (LAN und WAN) und führen Sie **direkt am Gerät das "Zurücksetzen auf Werkseinstellung"** aus. 3. Achten Sie darauf, dass durch die Entnahme eines Gerätes aus dem Netzwerk kein Sicherheitsrisiko entsteht!

Im Interesse des Umweltschutzes müssen Altgeräte am Ende ihrer Lebensdauer vom Endnutzer einer vom unsortierten Siedlungsabfall getrennten Erfassung zugeführt werden.

Altbatterien und Altakkumulatoren, die nicht von Altgerät umschlossen sind, sowie Lampen, die zerstörungsfrei aus dem Altgerät entnommen werden können, sind vor der Abgabe an eine Erfassungsstelle vom Altgerät zerstörungsfrei zu trennen.

Das Löschen personenbezogener Daten auf den zu entsorgenden Altgeräten liegt in der Eigenverantwortung des Endnutzers.

Werfen Sie Altgeräte nicht in den Hausmüll! 

Nur für EU-Länder:

Entsorgen Sie das Gerät gemäß der Elektro- und Elektronik Altgeräte EG-Richtlinie 2012/19/EU - WEEE (Waste Electrical and Electronic Equipment).

RED LION®
www.redlion.net

PROG. CNTLR.
E482663