Helmholz
COMPATIBLE WITH YOU

Quick Start Guide
WALL IE / WALL IE PLUS / WALL IE Compact, Industrial NAT Gateway/Firewall

Version 17 de

Bestellnummer:

WALL IE	700-860-WAL01	ab Firmware V 1.10.100
WALL IE PLUS	700-862-WAL01	ab Firmware V 1.00.000
WALL IE Compact	700-863-WAL01	ab Firmware V 1.00.000

Helmholz GmbH & Co. KG | Hannberger Weg 2 | 91091 Großenseebach | Germany
Phone +49 9135 7380-0 | Fax +49 9135 7380-110 | info@helmholz.de | www.helmholz.de

27.04.2023

Inhalt

1 Sicherheitshinweise

Zielgruppe

Diese Beschreibung wendet sich ausschließlich an ausgebildetes, qualifiziertes 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. Das Fachpersonal hat sicherzustellen, dass die Anwendung bzw. der Einsatz der beschriebenen Produkte alle Sicherheitsanforderungen, einschließlich sämtlicher anwendbarer Gesetze, Vorschriften, Bestimmungen und Normen erfüllt.

Bestimmungsgemäße Verwendung

Die Geräte besitzen den Schutzgrad IP 20 (open type) und müssen 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. 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 immer bestimmungsgemäß ein, so dass es z.B. auch niemals als alleiniges Mittel zur Abwendung gefährlicher Zustände an Maschinen und Anlagen verwendet werden kann.

Betrieb

Der einwandfreie und sichere Betrieb der Geräte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Betreiben Sie die Geräte nur im einwandfreien Zustand. Die zulässigen Einsatzbedingungen und Leistungsgrenzen (siehe Technische Daten im Handbuch des Produktes) müssen eingehalten werden. Nachrüstungen, Veränderungen oder Umbauten am Gerät sind grundsätzlich verboten.

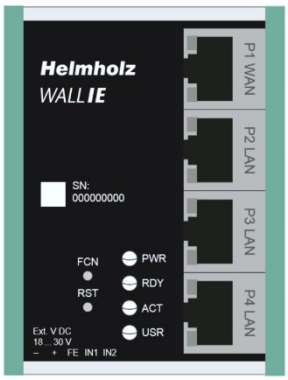
Security

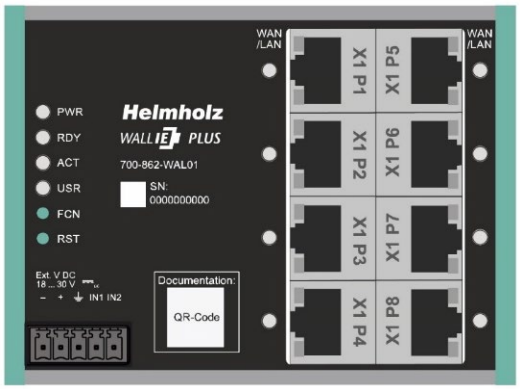
Die Geräte sind Netzwerkinfrastruktur Komponenten und damit ein wichtige Elemente in der Security Betrachtung einer Anlage. Beachten Sie bei der Verwendung der Geräte deshalb die einschlägigen Empfehlungen, um nicht autorisierte Zugriffe auf Anlagen und Systeme zu unterbinden. Weitere Informationen dazu finden Sie im Handbuch der Geräte.

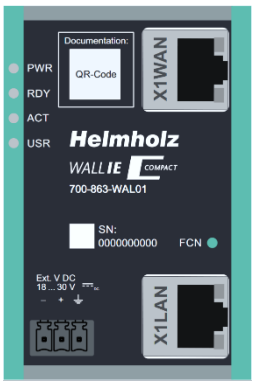
2 Einleitung

Die Produkte der WALL IE „Industrial NAT Gateway und Firewall“ Baureihe integrieren Maschinennetze auf einfache Weise in das übergeordnete Firmen- oder Produktionsnetz mittels Netzwerksegmentierung, Paket- und MAC-Adressen Filterung.

Die Produktreihe besteht aus drei Varianten: **WALL IE (700-860-WAL01)**, **WALL IE PLUS (700-862-WAL01)** und **WALL IE Compact (700-863-WAL01)**. Soweit nicht anders angemerkt, beschreibt dieses Dokument Funktionen, die alle Geräte gleichermaßen unterstützen.







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 darunterliegende Automatisierungsnetzwerk.

Im **Bridge-Betriebsmodus** agiert der WALL IE als Netzwerkbrücke in einem IPv4-Subnetz. 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.

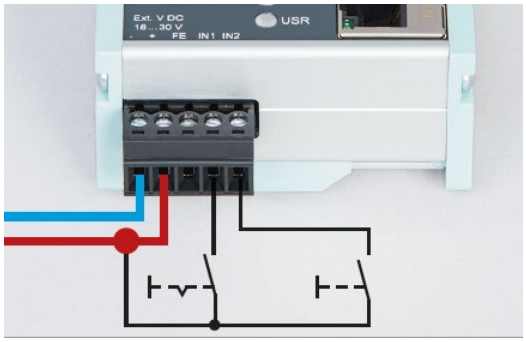
Dieses Dokument erläutert die Erstinbetriebnahme des WALL IE, WALL IE PLUS oder WALL IE Compact an den Anwendungsbeispielen „NAT“ und „Bridge“. Es werden nur die wichtigsten Einstellungen erläutert.

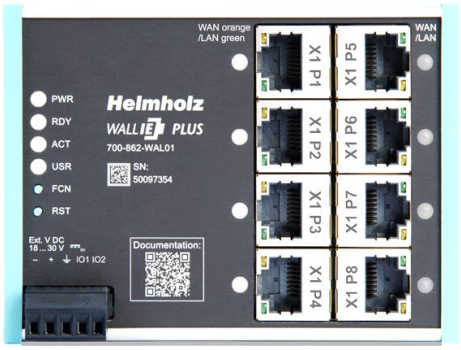
HINWEIS

Eine detaillierte Beschreibung aller Funktionen sowie wichtige Sicherheitshinweise entnehmen Sie bitte dem Handbuch des WALL IE. Dieses finden Sie unter www.helmholz.de oder scannen Sie direkt den QR-Code.

3 Anschließen des WALL IE

Der WALL IE muss, am Weitbereichseingang 18—30 V DC über den mitgelieferten Anschlussstecker, mit DC 24 V versorgt werden. Die WALL IE Produkte sind ausschließlich für den Betrieb mit Sicherheits-kleinspannung (SELV/PELV) ausgelegt.





Die RJ45 Buchse „P1 WAN“ des WALL IE (700-860-WAL01) dient zum Anschluss des externen Netzwerks. Die RJ45 Buchsen „P2 LAN—P4 LAN“ sind geswitcht und dienen zum Anschluss des internen Netzwerks.

Die RJ45 Buchsen „X1 P1“ bis „X1 P8“ des WALL IE PLUS (700-862-WAL01) können beliebig dem Netzwerk WAN oder LAN zugeordnet werden. In der Werkseinstellung ist der Port P1 für WAN und die Ports P2-P8 für LAN eingestellt. Die LEDs neben dem Port zeigen die Zuordnung an, orange für WAN und grün für LAN. Die Einstellung der Zuordnung der Ports für WAN und LAN ist im Webinterface möglich. Nähere Informationen hierzu finden Sie im Handbuch.

Der WALL IE Compact (700-863-WAL01) hat oben eine Buchse „X1 WAN“ für das externe Netzwerk und unten eine Buchse „X1 LAN“ für das interne Netzwerk.

Die Eingänge IN1 und IN2 beim WALL IE und WALL IE PLUS haben in der aktuellen Firmwareversion noch keine Funktion, werden in einer späteren Firmwareversion zum externen Schalten von Firewall Regeln zur Verfügung stehen. Der WALL IE Compact besitzt keine Eingänge.

HINWEIS

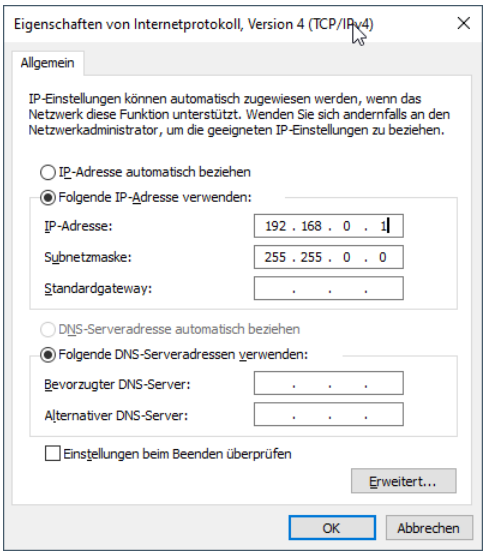
Das Gehäuse des WALL IE ist nicht geerdet. Bitte verbinden Sie den Funktionserdungs-Anschluss (FE) des WALL IE ordnungsgemäß mit dem Bezugspotential.

HINWEIS

Das Gerät darf nur mit Spannungsversorgungen betrieben werden, die die Vorgaben der EN 62368-1 für Stromquellen begrenzter Leistung erfüllen. Andernfalls ist das Gerät in einem Gehäuse zu betreiben, das den Anforderungen einer Brandschutzumhüllung nach EN 62368-1 genügt.

4 Erster Zugriff auf das Webinterface

Der WALL IE 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 beim WALL IE (700-860-WAL01) über die LAN-Anschlüsse P2 - P4 möglich. Beim WALL IE PLUS (700-862-WAL01) ist im Auslieferzustand der Zugriff über die Ports P2 - P8 möglich oder über alle Ports deren LED grün leuchtet. Beim WALL IE Compact kann das Webinterface über „X1 LAN“ erreicht werden.



Zuerst muss die IP-Adresse ihrer Netzwerkkarte entsprechend dem IP-Subnetz des WALL IE eingestellt werden. Stellen Sie in den Netzwerkeinstellungen des Netzwerkadapters die Subnetzmaske und die IP-Adresse des PCs passend zur Default IP-Adresse des WALL IE ein, z.B. 196.168.0.1 mit Subnetzmaske 255.255.0.0.

Verbinden sie nun ein Patchkabel mit dem LAN-Anschluss ihres PCs und einem der LAN-Ports des WALL IE.

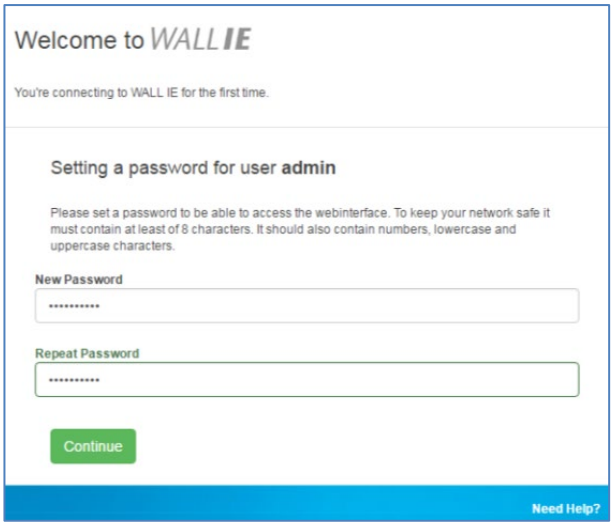
Das Webinterface kann im Auslieferungszustand durch Aufruf von "**https://192.168.0.100**" in der Browserleiste erreicht werden.

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.

Bei der Erstanmeldung werden sie aufgefordert ein Passwort für den User „admin“ 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 WALL IE weitergeleitet.



Der Hauptbenutzer ist immer „admin“.

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

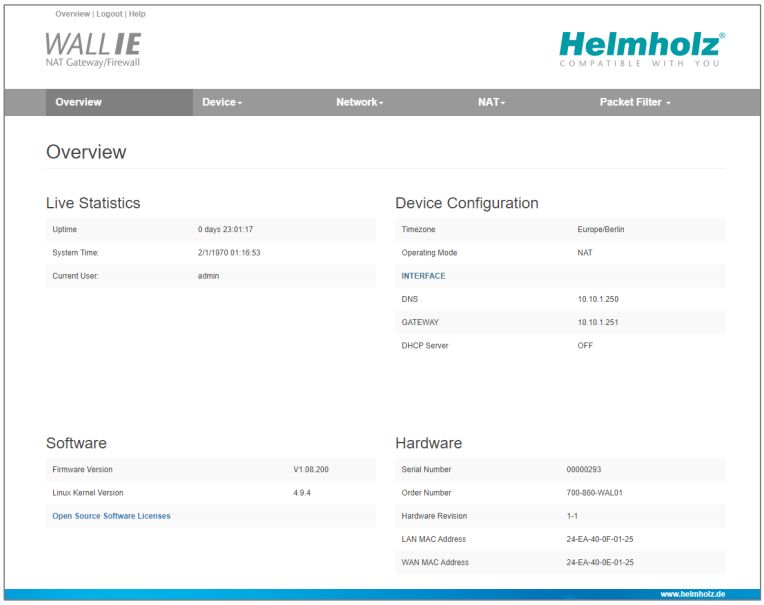
Die Benutzer können im Menü „Device/Password“ aktiviert und zugehörige Passworte eingestellt werden.

HINWEIS

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

5 Hauptansicht

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



HINWEIS

Bitte prüfen Sie auf der Webseite des WALL IE, ob es eine neuere Firmwareversion gibt. Das Firmwareupdate ist auf Seite 19 beschrieben.

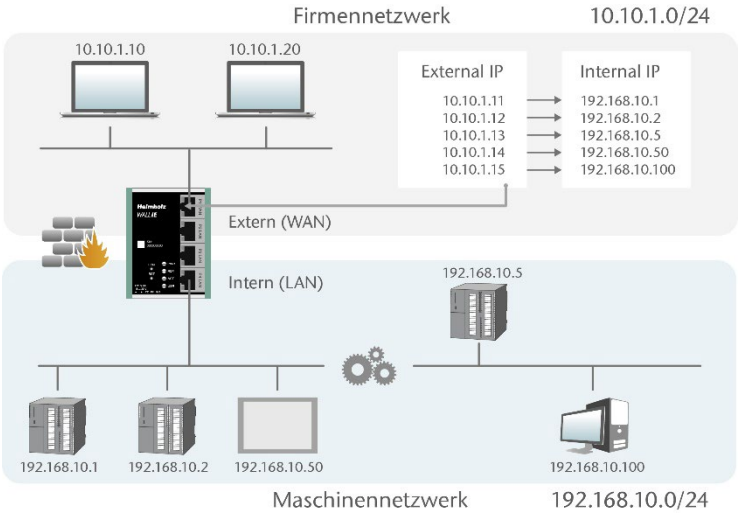
6 Wahl der Betriebsart

Abhängig vom Anwendungsfall für den WALL IE muss zu Beginn die Betriebsart festgelegt werden. WALL IE unterstützt zwei grundsätzliche Betriebsarten: NAT und Bridge.

6.1 Der NAT Betriebsmodus

Wenn eine Automatisierungszelle mit voreingestellten IP-Adressen in ein Firmennetzwerk 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 WALL IE die Möglichkeit, die IP-Adressen der Maschine zu belassen aber die Kommunikation zum Maschinennetzwerk mit eigenen IP-Adressen aus dem Firmennetzwerk zu ermöglichen.



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

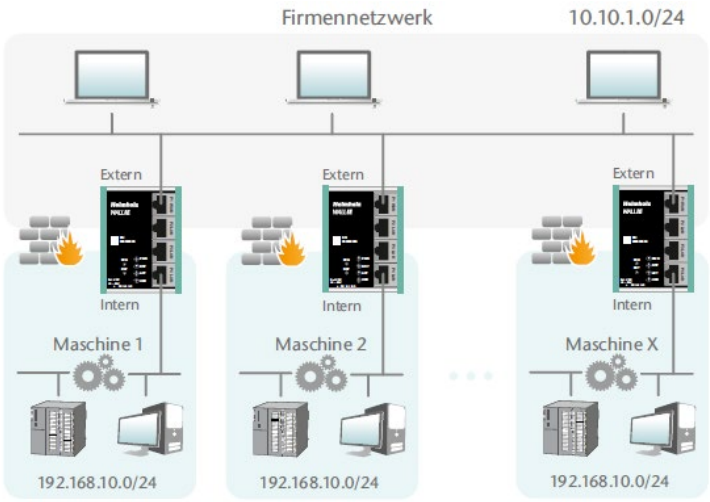
Zusätzlich können Paketfilter und MAC-Adressen Filter zur Einschränkung des erlaubten Datenverkehrs parametriert werden.

Broadcasts-Traffic wird generell am WALL IE gefiltert, somit wird das Zeitverhalten des Maschinennetzwerks nicht durch das Firmennetzwerk 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 WALL IE zu einem bestimmten Teilnehmer im Maschinennetzwerk (LAN) weitergeleitet werden.

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



Jeder Automatisierungszelle können hierbei unterschiedliche freie IP-Adressen aus dem Firmennetzwerk zugewiesen werden.

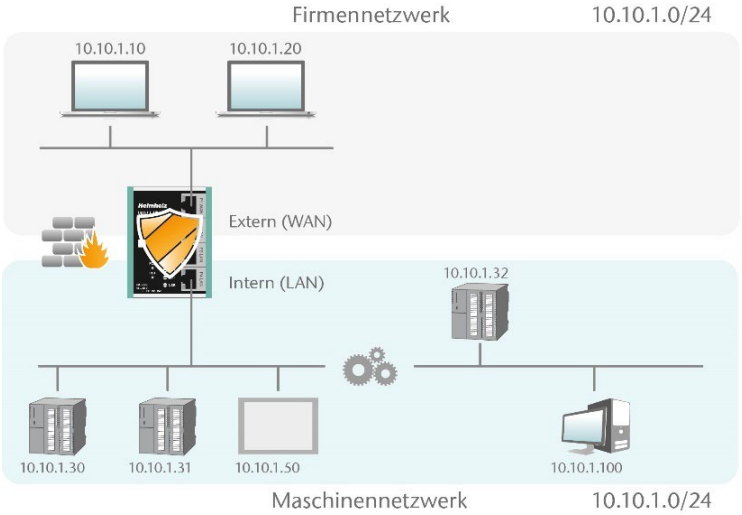
Wenn „NAT“ Ihr geplanter Anwendungsfall ist, dann lesen Sie bitte auf Seite 9 weiter.

6.2 Der Bridge-Betriebsmodus

Im Bridge Betriebsmodus verhält sich WALL IE wie ein Layer 2 Switch zwischen dem Maschinennetzwerk (Automatisierungszelle) und dem Firmennetzwerk. Die IP-Adressen im Firmennetzwerk 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.

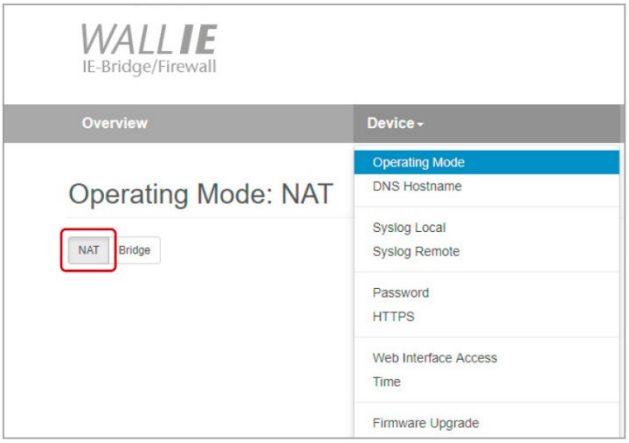
Dies erlaubt die Abtrennung eines Teils des Firmennetzwerkes ohne die Verwendung von unterschiedlichen Netzwerk-Adressen.



Wenn „Bridge“ Ihr gewünschter Anwendungsfall ist, dann lesen Sie bitte auf Seite 16 weiter.

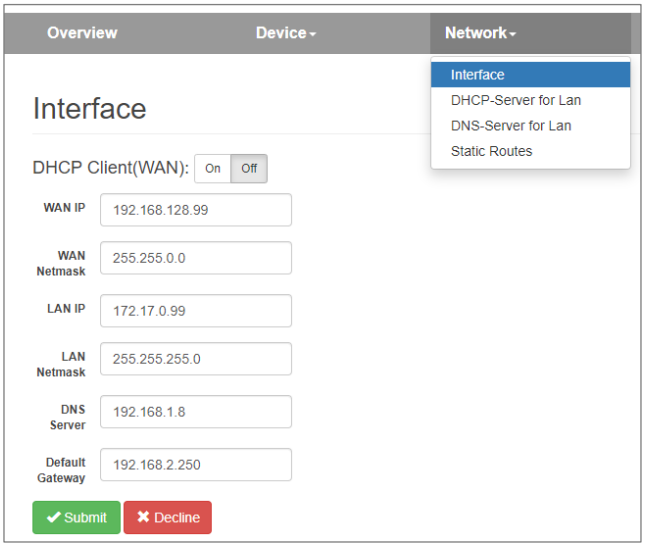
7 Anwendungsfall „NAT“

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



7.1 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 WALL IE 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 WALL IE das Internet erreichen sollen. Werden diese nicht angegeben ("0.0.0.0"), dann wird verhindert, dass Geräte im LAN mit dem Internet kommunizieren. Für den SNTP-Dienst ist die Angabe eines DNS-Servers notwendig.

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.

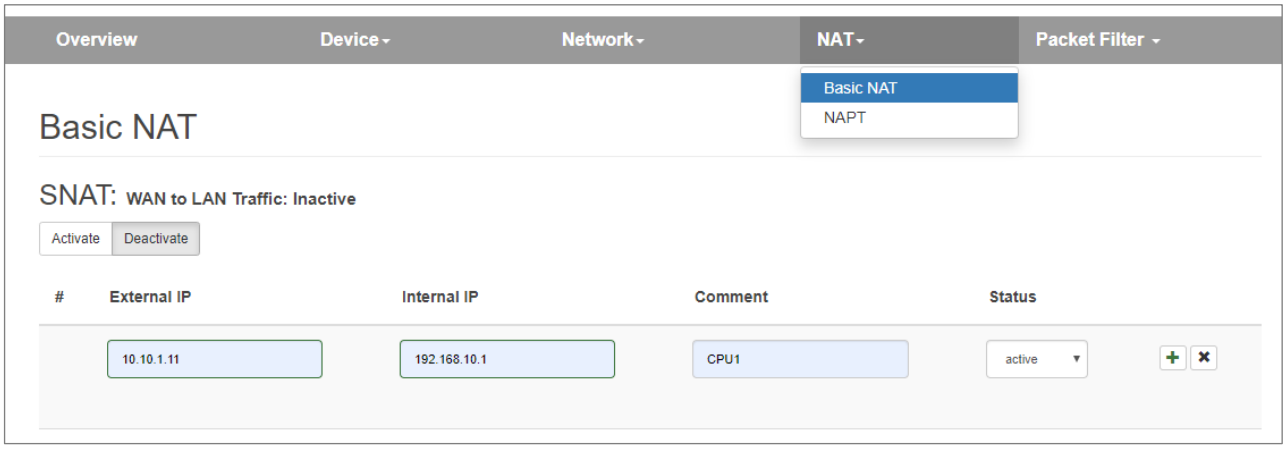
HINWEIS

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

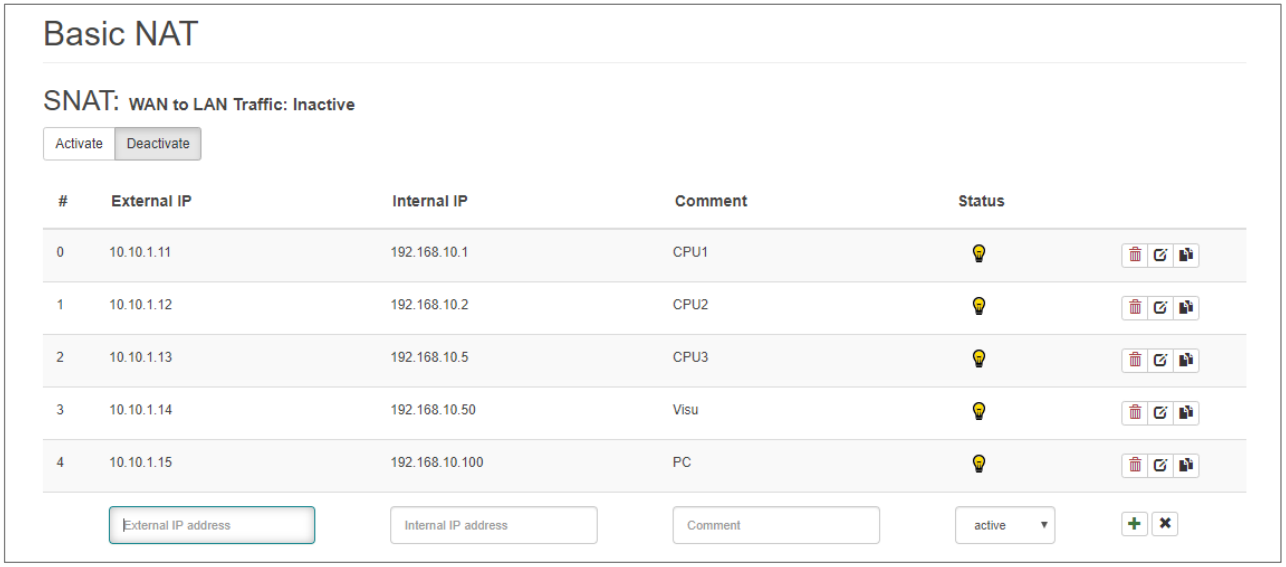
7.2 Einrichtung von „Basic NAT“ Regeln

Um Basic-NAT-Funktionalitäten nutzen zu können, muss die Betriebsart des WALL IE 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 eine freie IP-Adresse aus dem WAN IP-Adressbereich. Diese darf noch keinem anderen Ethernet Teilnehmer (im WAN) zugewiesen worden sein! Die „Internal IP“ ist die vorhandene IP-Adresse des Netzwerkteilnehmers in der Maschine (LAN). Als Kommentar kann ein beliebiger Text eingegeben werden. Mit dieser ‚zusätzlichen WAN-Schnittstelle‘ wird im WALL IE dann die Adress-umsetzung („natting“) zur eingetragenen LAN-IP (dem Zielgerät) realisiert.



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

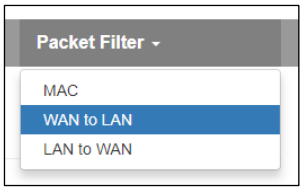
HINWEIS

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.

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

7.3 Paketfilter „WAN to LAN“

Mit den Paketfiltern lässt sich der Zugriff zwischen dem Firmennetzwerk (WAN) und dem Maschinennetzwerk (LAN) einschränken. Es kann beispielsweise konfiguriert werden, dass nur bestimmte Teilnehmer aus dem Firmennetzwerk mit definierten Teilnehmern aus der Automatisierungszelle Daten austauschen dürfen.

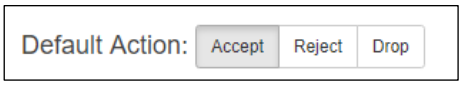


Folgende Filterkriterien auf Layer 3 und 4 stehen zur Verfügung: IPv4-Adressen, Protokoll (TCP/UDP/ICMP) und Ports.

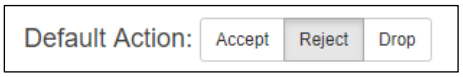
Im Menü „Packet Filter“ wählen Sie den Menüpunkt „WAN to LAN“.

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“).

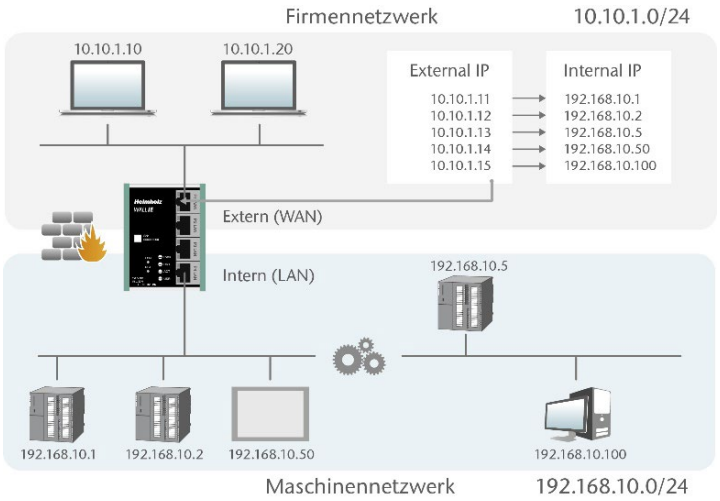
Wollen Sie erstmal nicht filtern, so stellen Sie die Default Action auf „Accept“.



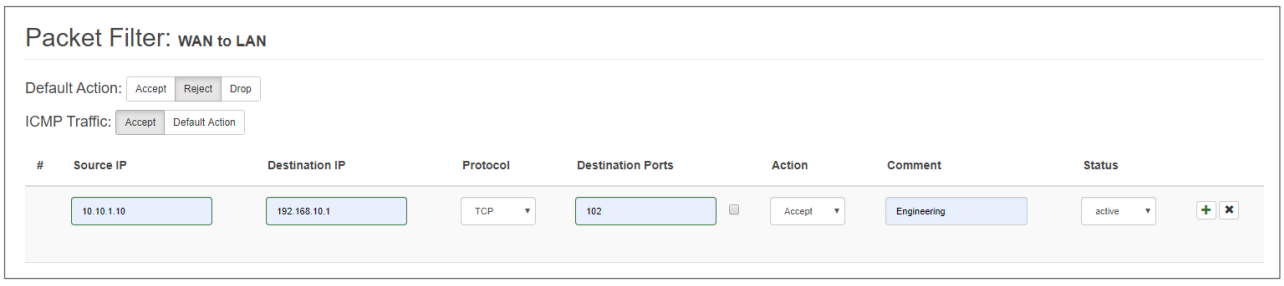
Um den Zugriff auf das Maschinennetzwerk auf bestimmte Teilnehmer im WAN zu beschränken, stellen Sie die Default Action auf „Reject“ oder „Drop“. „Reject“ sendet bei nicht erlaubten Telegrammen aus dem WAN eine Fehlermeldung zurück, „Drop“ verwirft das Telegramm ohne Fehlermeldung.



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 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.



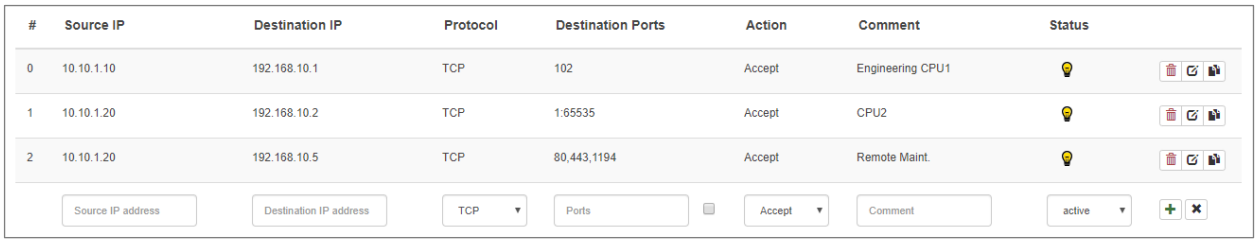
Source IP gibt die IP-Adresse des aktiven Gerätes im Firmennetzwerk (WAN) an.

Destination IP gibt das angesprochene Gerät im Maschinennetzwerk (LAN) an.

Mit **Protocol** „TCP“, „UPD“ oder „ICMP“ kann die Filterregel für 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“.

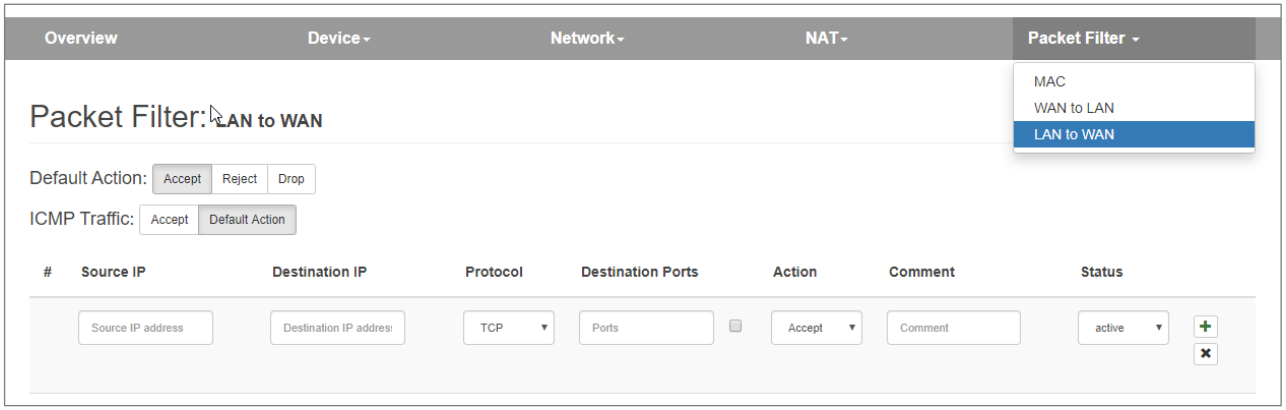


Es ist auch möglich, den Zugriff mehrerer Teilnehmer untereinander zu konfigurieren. Ein IP-Bereich kann mit einem Bindestrich definiert werden: “10.10.1.10-10.10.1.20“. Eine Liste von IP-Adressen wird mit Kommata angegeben: “10.10.1.10,10.10.1.15,10.10.1.20”. Ein IP-Subnetz kann mit der CIDR-Notation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

7.4 Paketfilter “LAN to WAN”

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



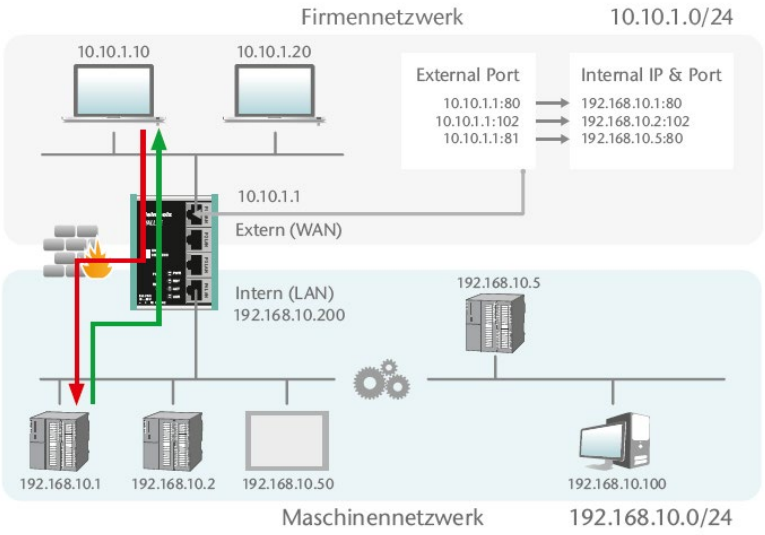
Im Paket Filter “LAN to WAN” kann die Kommunikation von Geräten im LAN mit Geräten im Firmennetzwerk (WAN) oder ins Internet ganz unterbunden oder für bestimmte Geräte gesperrt oder erlaubt werden.

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.

7.5 SNAT

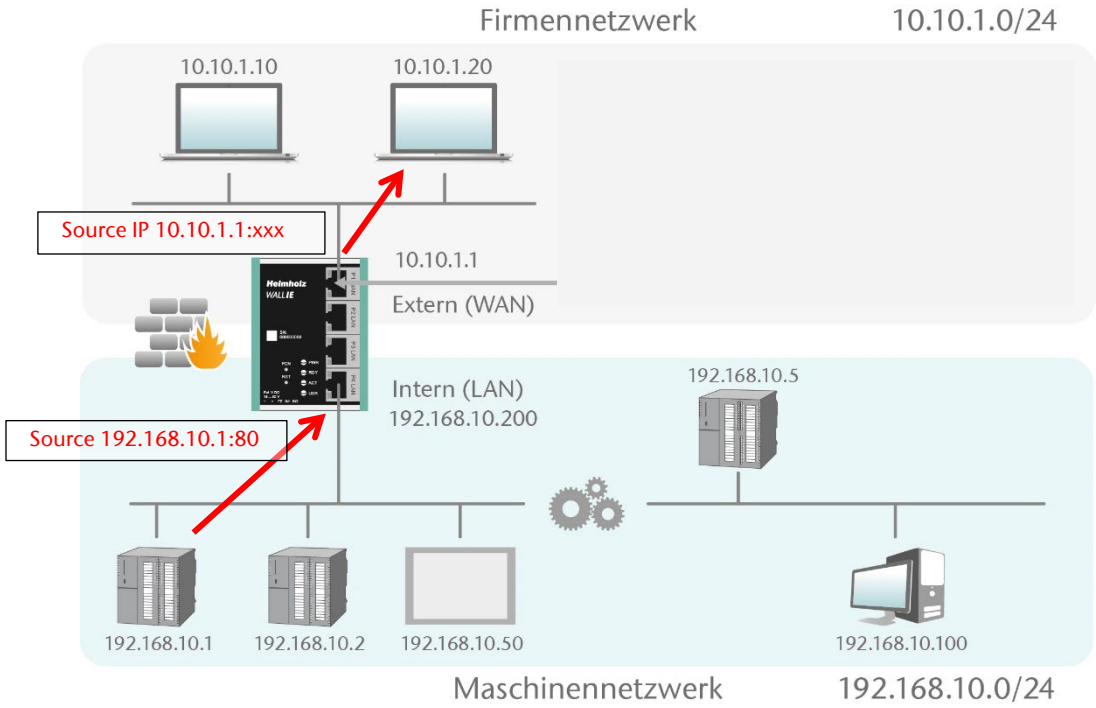
Mit der Funktion „SNAT (Source NAT)“ wird der eingehende Datenverkehr von der WAN Seite transparent an das LAN-Netzwerk weitergegeben. Bei allen Paketen, die auf LAN-Seite von WALL IE weitergeleitet werden, wird die Quell-IP-Adresse durch die LAN-IP-Adresse von WALL IE ersetzt.

Somit benötigt keiner der LAN-Teilnehmer als „Gateway“ die WALL IE 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.

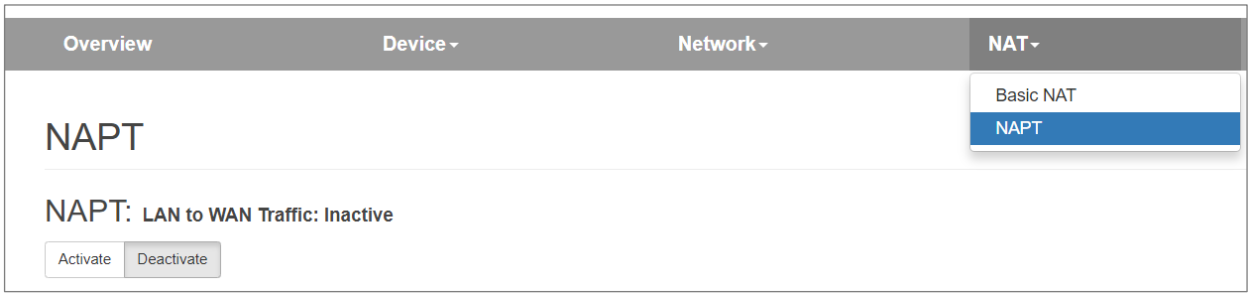


7.6 NAPT

„NAPT for LAN to WAN traffic“ ersetzt die Absender-Adressen von Anfragen aus dem LAN durch die WALL IE WAN IP-Adresse.



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



HINWEIS

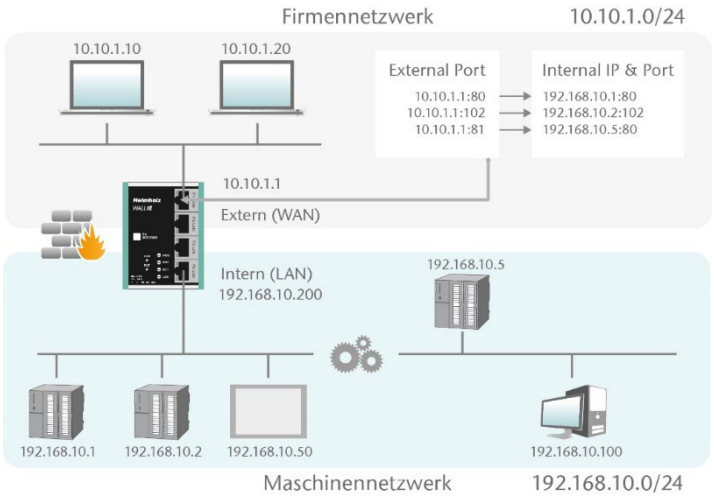
Damit bei aktiviertem NAPT die Kommunikation von LAN nach WAN funktioniert, muss die WALL IE LAN IP Adresse in allen Geräten am LAN als Gateway eingetragen werden!

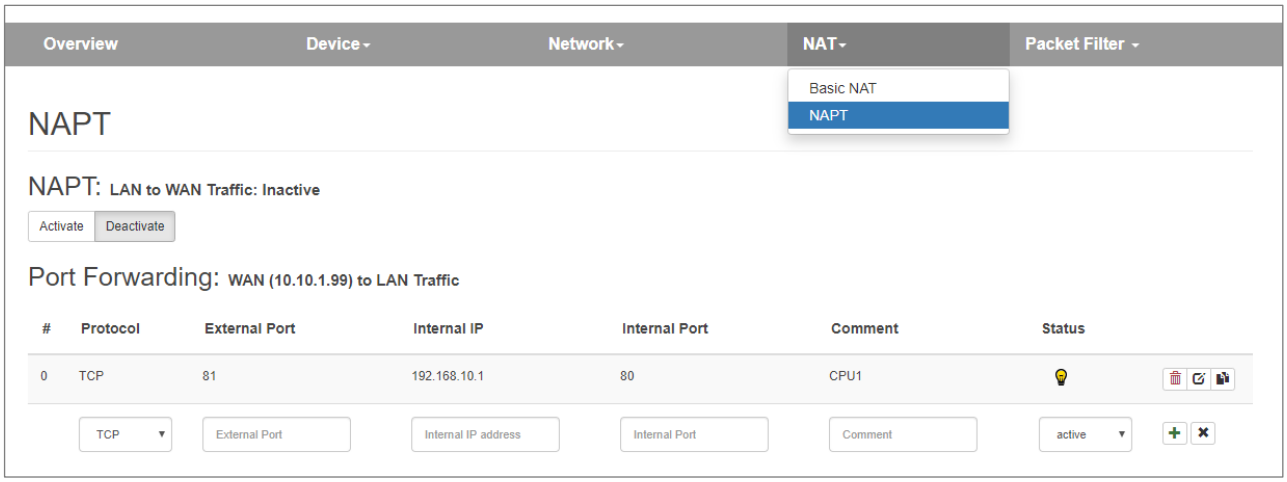
Ist die Option **NAPT** abgeschaltet („Deactivate“), so werden die Anfrage-Pakete aus dem LAN mit ihrer original Absender-IP und Absender-Port an das WAN weitergeleitet.

7.7 Portforwarding

Mithilfe von Portweiterleitungen („Portforwarding for WAN to LAN traffic“) kann konfiguriert werden, dass Pakete an einen bestimmten TCP/UDP-Port des WALL IE (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 WALL IE eigene IP-Adresse 10.10.1.1 mit Port 81 erreicht werden.





Protocol: "TCP" oder "UDP"

External Port: Portnummer, über die auf das Gerät auf der LAN-Seite zugegriffen wird. Auf der LAN-Seite wird auf das Gerät über die interne IP-Adresse und die interne Portnummer zugegriffen.

Internal IP: IP-Adresse des mit dem LAN verbundenen Geräts.

Internal Port: Port, der für den Zugriff auf das mit dem LAN verbundene Gerät verwendet wird.

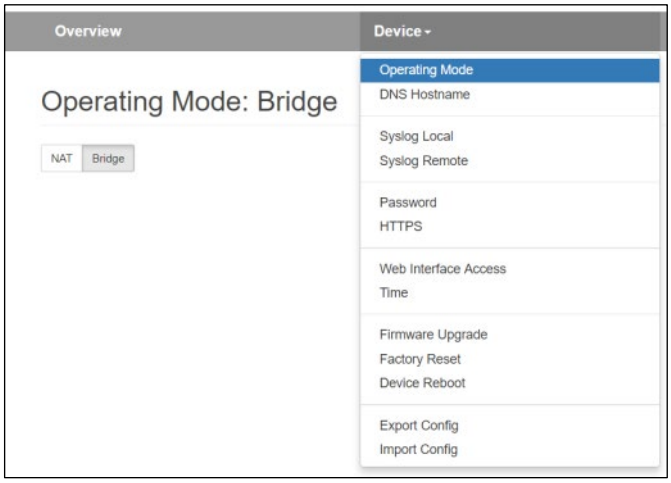
Comment: Frei definierbarer Kommentar.

HINWEIS

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

8 Anwendungsfall „Bridge“

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

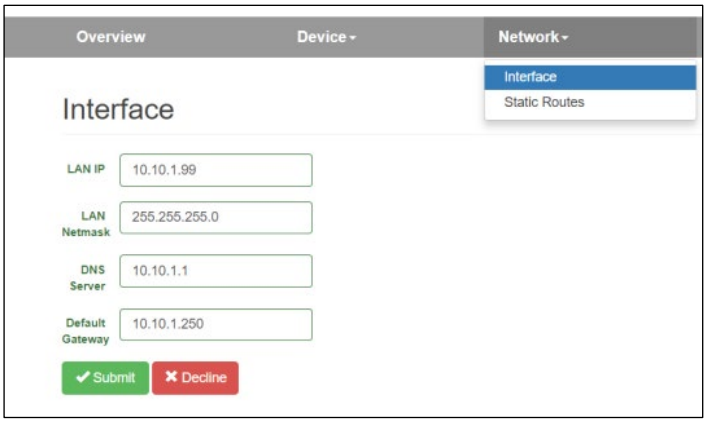


8.1 Anpassen der IP-Adressen im Bridge Betriebsmodus

Klicken Sie auf das Menü „Network“ und wählen das Untermenü „Interface“ aus. Hier können die IP-Adressen des WALL IE („LAN IP“) sowie die zugehörige Subnetzmaske („LAN netmask“) festgelegt werden.

Im Bridge Betriebsmodus sind die hier festgelegten Interface Einstellungen gleichermaßen auch am WAN-Port des WALL IE gültig.

Ein DNS-Server und ein Default-Gateway können ebenfalls angegeben werden. Das ist notwendig, wenn Geräte aus dem LAN über den WALL IE 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.

HINWEIS

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

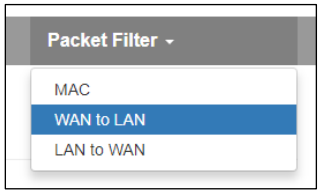
Im Bridgemodus sind aus Sicherheitsgründen zuerst alle Ports für den „WAN-to-LAN“ Datenverkehr gesperrt! Um Zugriffe zu erlauben, müssen Paketfilter-Regeln erstellt, oder die "Default Action" bei den Paket-Filtern auf „Accept“ gestellt werden.

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

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

8.2 Paketfilter „WAN to LAN“

Mit den Paketfiltern lässt sich der Zugriff zwischen dem Firmennetzwerk (WAN) und dem Maschinennetzwerk (LAN) einschränken. Es kann beispielsweise konfiguriert werden, dass nur bestimmte Teilnehmer aus dem Firmennetzwerk mit definierten Teilnehmern aus der Automatisierungszelle Daten austauschen dürfen.

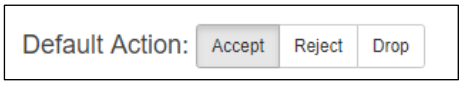


Folgende Filterkriterien auf Layer 3 und 4 stehen zur Verfügung: IPv4-Adressen, Protokoll (TCP/UDP/ICMP) und Ports.

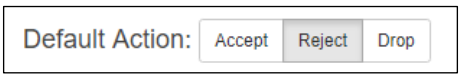
Im Menü „Packet Filter“ wählen Sie den Menüpunkt „WAN to LAN“.

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“).

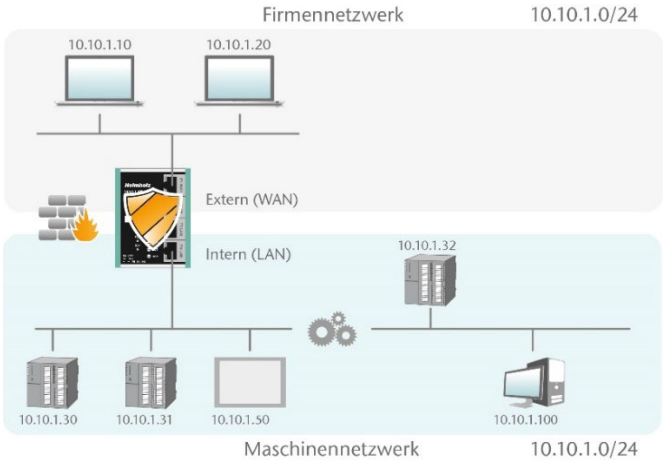
Wollen Sie erstmal nicht filtern, so stellen Sie die Default Action auf „Accept“.



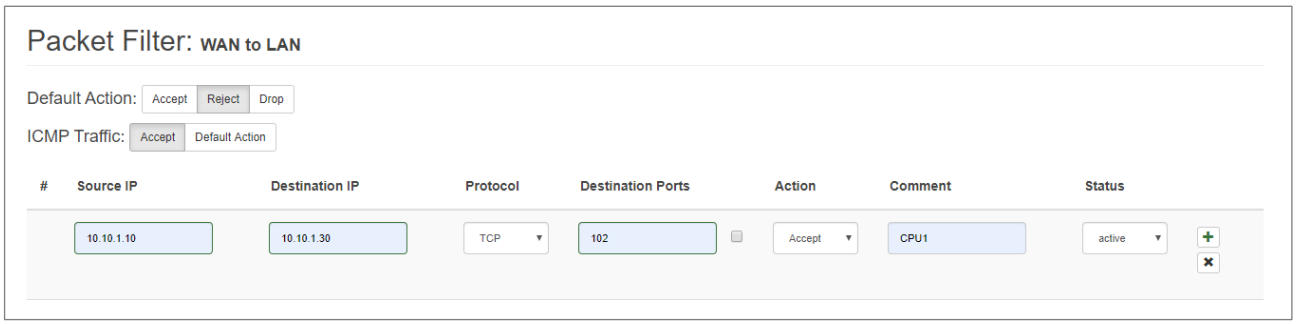
Um den Zugriff auf das Maschinennetzwerk auf bestimmte Teilnehmer im WAN zu beschränken, stellen Sie die Default Action auf „Reject“ oder „Drop“. „Reject“ sendet bei nicht erlaubten Telegrammen aus dem WAN eine Fehlermeldung zurück, „Drop“ verwirft das Telegramm ohne Fehlermeldung.



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 Firmennetzwerk (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.	

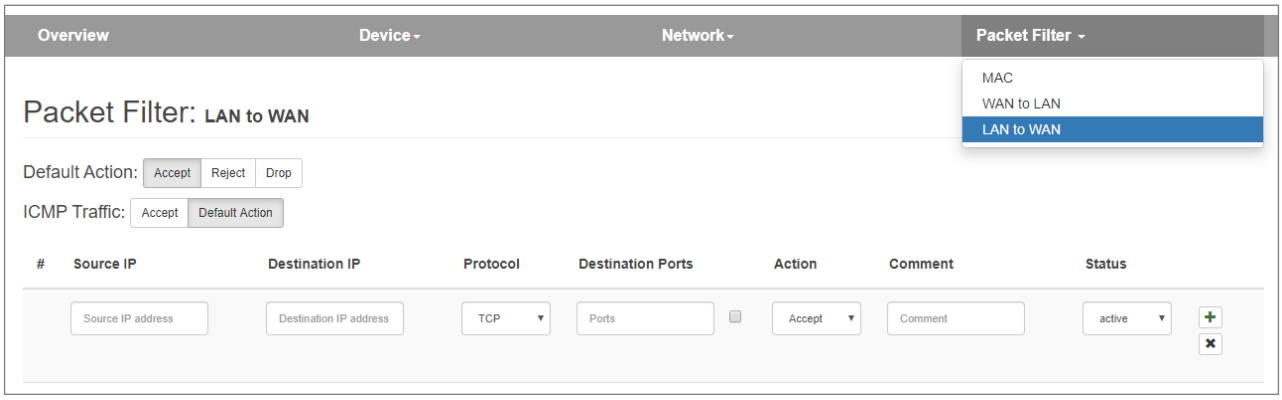
Es ist auch möglich, den Zugriff mehrerer Teilnehmer untereinander zu konfigurieren. Ein IP-Bereich kann mit einem Bindestrich definiert werden: “10.10.1.10-10.10.1.20“. Eine Liste von IP-Adressen wird mit Kommata angegeben: “10.10.1.10,10.10.1.15,10.10.1.20”. Ein IP-Subnetz kann mit der CIDR-Notation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

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 Zusammenspiel 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).

8.3 Paketfilter „LAN to WAN”

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



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

9 Firmwareupdate

Die Firmware des WALL IE kann über die Webseite sehr einfach aktualisiert werden. Bitte laden Sie vorab die Firmware-Update-Datei herunter.

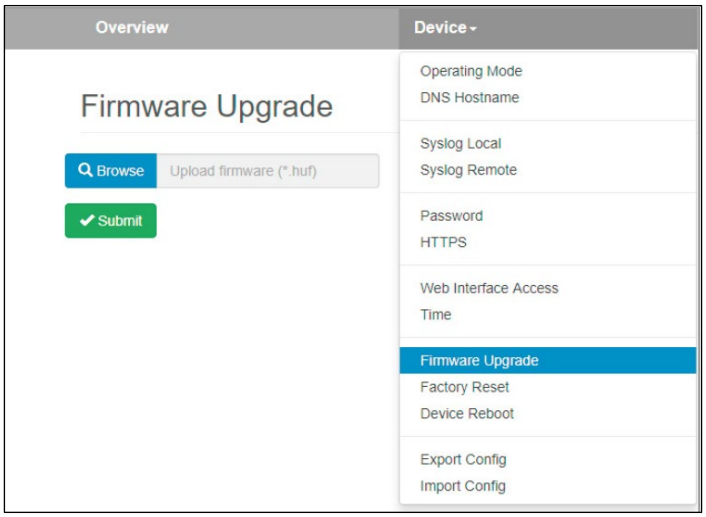
Link zur Firmware:
http://www.helmholz.de/goto/700-860-WAL01
http://www.helmholz.de/goto/700-862-WAL01
http://www.helmholz.de/goto/700-863-WAL01

Die Firmwaredatei hat die Dateiendung „HUF“ (Helmholz Update File) und ist verschlüsselt, um diese vor Manipulationen zu schützen.

Legen Sie die Firmwaredatei auf Ihren PC ab und wählen im Menü „Device“ unter „Firmware Upgrade“ den Speicherort mit „Browse“ aus.

Danach wird die Firmwaredatei auf den WALL IE übertragen - das kann je nach Netzverbindung - bis zu einer Minute dauern.

Im WALL IE wird die Firmwaredatei entschlüsselt und überprüft. Ist der Inhalt korrekt wird die Firmware remanent in den Programmspeicher übertragen und anschließend wird ein automatischer Neustart durchgeführt.



ACHTUNG

Während dem Updatevorgang ist der Betrieb des WALL IE unterbrochen. Schalten Sie das Gerät während dem Updatevorgang nicht aus.

HINWEIS

Die Konfiguration des WALL IE wird bei einem Update auf eine höhere Version, soweit es technisch möglich ist, beibehalten.
Ein „Downgrade“ auf eine ältere Firmwareversion kann zu Konfigurationsfehlern führen. Es wird empfohlen vor einem Downgrade ein Werksrücksetzen durchzuführen.

HINWEIS

Nach einem Firmwareupdate ist es ggf. notwendig den Browser Cache einmal zu löschen, um veraltete JavaScript Elemente der WALL IE Webseite zu aktualisieren.

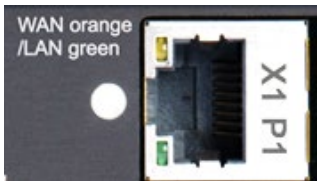
10 LED-Status Informationen

10.1.1 WALL IE (700-860-WAL01)

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

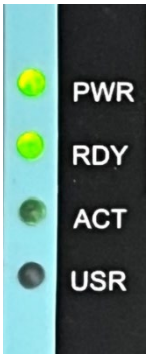
10.1.2 WALL IE PLUS (700-862-WAL01)

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
LEDs neben RJ45 Ports	Orange	Port ist dem WAN-Netzwerk zugeordnet
	Grün	Port ist dem LAN-Netzwerk zugeordnet
RJ45 LEDs	Grün (Link) blinkt	Verbunden mit 100 Mbit/s
	Grün (Link) an	Verbunden mit 1000 Mbit/s
	Orange (Act)	Datenübertragung am Port



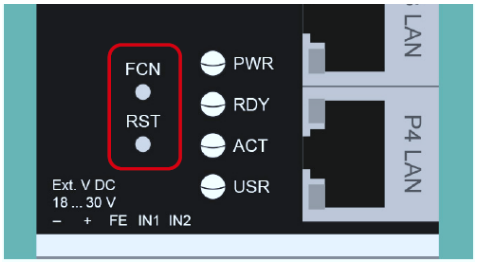
10.1.3 WALL IE Compact (700-863-WAL01)

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) blinkt	Verbunden mit 100 Mbit/s
	Grün (Link) an	Verbunden mit 1000 Mbit/s
	Orange (Act)	Datenübertragung am Port



11 Funktion der Taster

Mit dem „**FCN**“-Taster kann der WALL IE auf **Werkseinstellungen zurückgesetzt** werden. Der „**FCN**“-Taster muss dafür während der Hochlaufphase des WALL IE gedrückt gehalten werden. Das erfolgreiche Zurücksetzen der Parameter und Einstellungen wird beim Bootvorgang durch Aufleuchten der „USR“-LED quittiert. Der „**FCN**“-Taster kann dann losgelassen werden.



Der "**RST**"-Taster löst einen sofortigen Neustart des WALL IE aus, bei dem alle gespeicherten Einstellungen erhalten bleiben. Der WALL IE Compact hat keinen Reset-Taster.

12 Technische Daten

Artikelnummer	**700-860-WAL01**
Name	WALL IE, Industrial NAT Gateway/Firewall
Abmessungen (T x B x H)	32,5 x 58,5 x 76,5 mm
Gewicht	ca. 130 g
WAN-Schnittstelle	
Anzahl	1
Typ	10Base-T/100Base-Tx
Anschluss	RJ45 Buchse
Übertragungsrate	10/100 Mbit/s
LAN-Schnittstelle	
Anzahl	3, geswitcht
Typ	10Base-T/100Base-Tx
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
Verlustleistung	Max. 2,4 W
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 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
RoHS	Ja
REACH	Ja

Artikelnummer	**700-862-WAL01**
Name	WALL IE PLUS, Industrial NAT Gateway/Firewall
Abmessungen (T x B x H)	34,5 x 101,5 x 75,5 mm
Gewicht	ca. 230 g
WAN/LAN-Schnittstelle	
Anzahl	8, geswitcht
Typ	100Base-Tx/1000Base-T
Anschluss	RJ45 Buchse
Übertragungsrate	100/1000 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 Port-Zuordnung, 16 LEDs Ethernet-Status
Spannungsversorgung	DC 24 V, 18–30 V DC
Stromaufnahme	max. 275 mA bei DC 24 V
Verlustleistung	Max. 6,7 W
Umgebungsbedingungen	
Einbaulage	beliebig
Umgebungstemperatur	0 °C ... +60°C
Transport- und Lagertemperatur	-40 °C ... +85°C
Relative Luftfeuchte	95 % r. H. ohne Betauung
Verschmutzungsgrad	2
Schutzart	IP20
Zertifizierungen	CE
RoHS	Ja
REACH	Ja

Artikelnummer	**700-863-WAL01**
Name	WALL IE Compact, Industrial NAT Gateway/Firewall
Abmessungen (T x B x H)	35 x 48,5 x 76 mm
Gewicht	ca. 105 g
WAN/LAN-Schnittstelle	
Anzahl	2
Typ	100Base-Tx/1000Base-T
Anschluss	RJ45 Buchse
Übertragungsrate	100/1000 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, 4 LEDs Ethernet-Status
Spannungsversorgung	DC 24 V, 18–30 V DC
Stromaufnahme	max. 140 mA bei DC 24 V
Verlustleistung	Max. 3,3 W
Umgebungsbedingungen	
Einbaulage	beliebig
Umgebungstemperatur	0 °C ... +60°C
Transport- und Lagertemperatur	-40 °C ... +85°C
Relative Luftfeuchte	95 % r. H. ohne Betauung
Verschmutzungsgrad	2
Schutzart	IP20
Zertifizierungen	CE
RoHS	Ja
REACH	Ja

Der Inhalt dieses Quick Start Guides ist von uns auf die Übereinstimmung mit der beschriebenen Hard- und Software überprüft worden. Da dennoch Abweichungen nicht ausgeschlossen sind, können wir für die vollständige Übereinstimmung keine Gewährleistung übernehmen. Die Angaben in diesem Quick Start Guide werden jedoch regelmäßig aktualisiert.

Bitte beachten Sie beim Einsatz der erworbenen Produkte jeweils die aktuellste Version des Quick Start Guides, welche im Internet unter www.helmholz.de einsehbar ist und auch heruntergeladen werden kann.

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.helmholz.de bereit gestellt. 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.

Unsere Kunden sind uns wichtig, wir freuen uns über Verbesserungsvorschläge und Anregungen. Sollten Sie Fragen zur Verwendung des Produktes haben, wenden Sie sich bitte telefonisch an den Helmholz Support oder schreiben Sie eine E-Mail an support@helmholz.de.

Alle in diesem Dokument gezeigten Markenzeichen oder genannten Marken sind Eigentum der jeweiligen Inhaber bzw. Hersteller. Die Darstellung und Nennung dienen ausschließlich der Erläuterung der Verwendung- und Einstellmöglichkeiten der hier dokumentierten Produkte.