Helmholz®
COMPATIBLE WITH YOU

Quick Start Guide WALL IE

Version
13 de
ab FW 1.08

www.helmholz.de

Inhalt

Hinweis:

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 10,00 Euro 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.

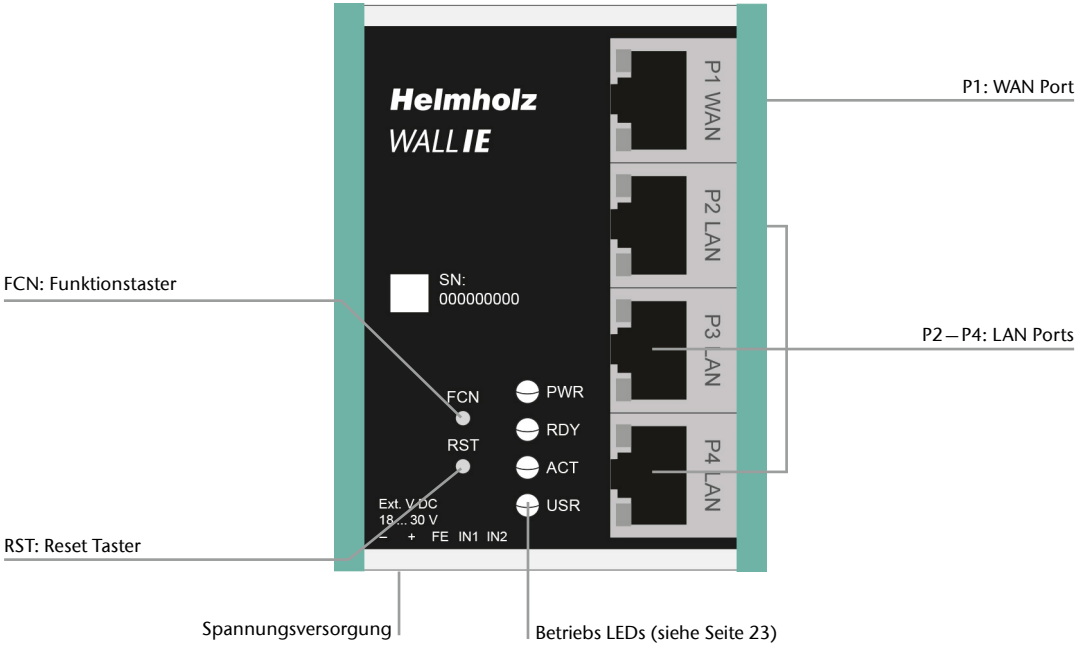
1. Einleitung

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

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.

SCAN QR CODE TO GET MANUAL

WALL IE
Industrial NAT Gateway / Firewall
Dokumentation



2. Anschließen

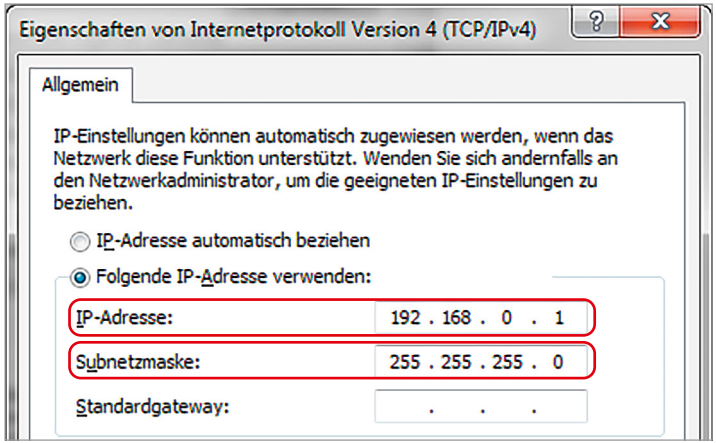
Der WALL IE muss, am Weitbereichseingang 18 – 30 V DC über den mitgelieferten Anschlussstecker, mit DC 24 V versorgt werden. Der Anschluss (FE) ist für die Funktionserde. Verbinden Sie diese ordnungsgemäß mit dem Bezugspotential.

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.

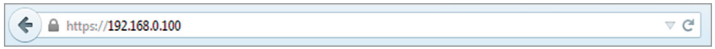
3. Erster Zugriff auf das Webinterface

Der WALL IE ist ab Werk LAN-seitig mit der IP-Adresse 192.168.0.100 und der Subnetzmaske 255.255.255.0 eingestellt. 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 WALL IE eingestellt werden.



Verbinden Sie nun ein Patchkabel mit dem LAN-Anschluss Ihres PCs und einem der LAN-Ports P2 – P4 des WALL IE. Das Webinterface erreicht man im Auslieferungszustand durch Aufruf von https://192.168.0.100 in der Browserleiste.



Hinweis: *Das Webinterface ist aus Sicherheitsgründen ausschließlich über eine gesicherte HTTPS-Verbindung zu erreichen. Um die Webseite zu erreichen, muss einmalig eine Ausnahme im Browser bestätigt werden.*

Im Menü „Device/HTTPS“ kann bei Bedarf ein eigenes Zertifikat für die Verbindungssicherung hinterlegt werden.

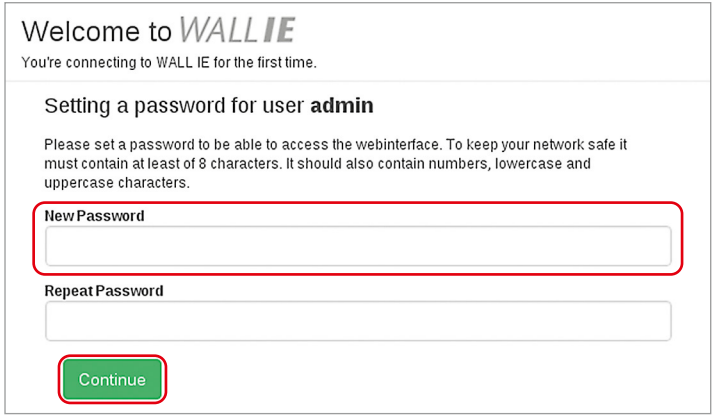
Bei der Erstanmeldung werden Sie aufgefordert ein Passwort für den User „admin“ festzulegen.

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 Haupt-User ist immer „admin“.

Neben dem Haupt-User 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.

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.*

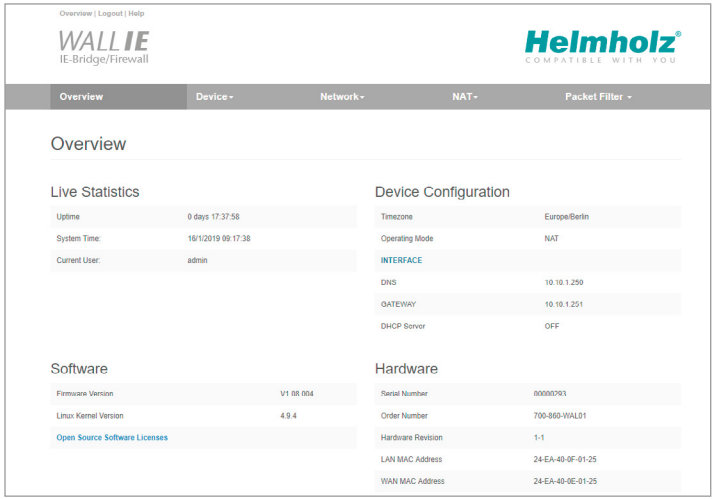


4. Übersicht

Nach dem Login öffnet sich immer die „Overview“ Webseite des WALL IE.

Diese enthält im oberen Bereich eine Menüleiste und darunter eine Übersicht über den Status, die Systeminformationen und die Grundeinstellungen des WALL IE.

Hinweis: *Bitte prüfen Sie auf der Webseite des WALL IE unter www.helmholz.de ob es eine neuere Firmwareversion gibt. Das Firmwareupdate ist auf Seite 22 beschrieben.*



5. 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.

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 WALL IE die Möglichkeit, die IP Adressen der Maschine zu belassen aber die Kommunikation zum Maschinennetzwerk mit eigenen IP-Adressen aus dem Produktionsnetzwerk 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 verwendet werden.

Broadcasts-Traffic wird generell am WALL IE gefiltert, somit wird das Zeitverhalten des Maschinennetzwerks nicht durch das Produktionsnetzwerk beeinträchtig.

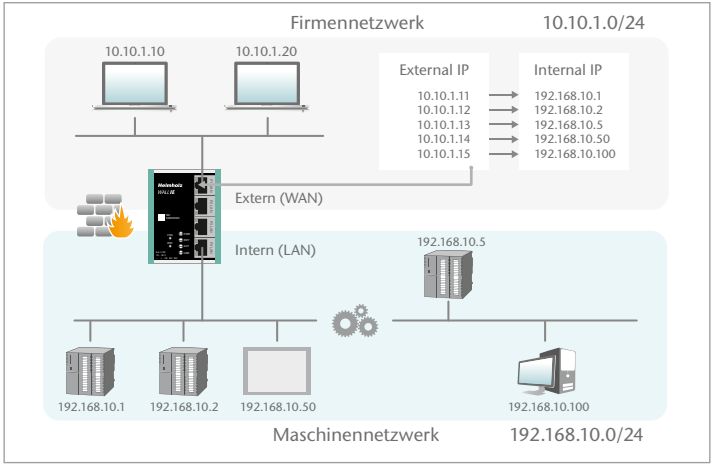
Basic NAT, auch “1:1 NAT” oder “Static NAT” genannt, ist die Übersetzung von einzelnen IP-Adressen oder von ganzen IP-Adressbereichen.

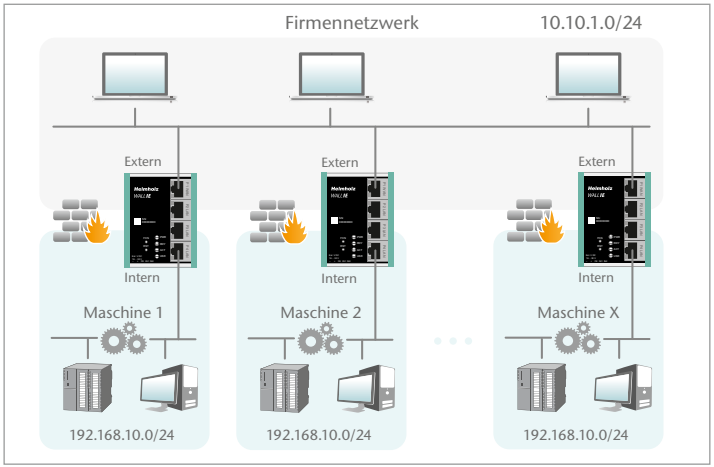
Mithilfe von Portweiterleitungen (**„Portforwarding“**) kann alternativ konfiguriert werden, dass Pakete an einen bestimmten TCP/UDP-Port des WALL IE an einen bestimmten Teilnehmer im Maschinennetzwerk (LAN) weitergeleitet werden.

Der NAT Betriebsmodus erlaubt es somit auch, mehrere Automatisierungszellen die einen gleichen IP-Adressbereich verwenden, in ein 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 auf Seite 7 weiter.





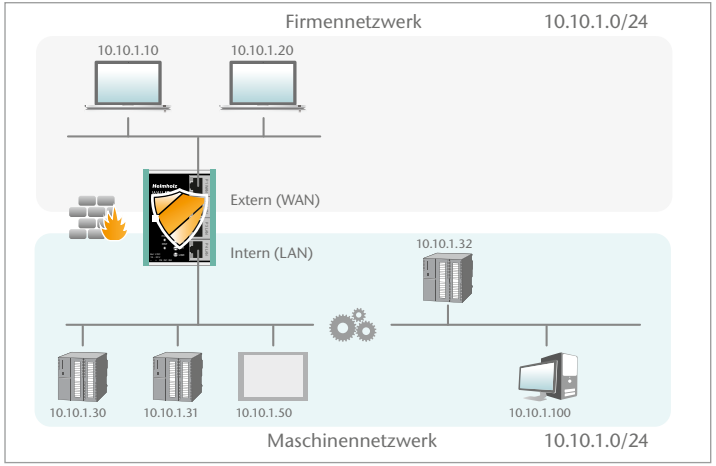
5.2. Der Bridge-Betriebsmodus

Im **Bridge Betriebsmodus** verhält sich WALL IE wie ein Layer 2 Switch zwischen dem Maschinennetzwerk (Automatisierungszelle) und dem Produktionsnetzwerk. Die IP-Adressen im Produktionsnetzwerk sind hierbei im gleichen IP-Adressraum (Subnetzmaske) wie die Adressen im Maschinennetzwerk.

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

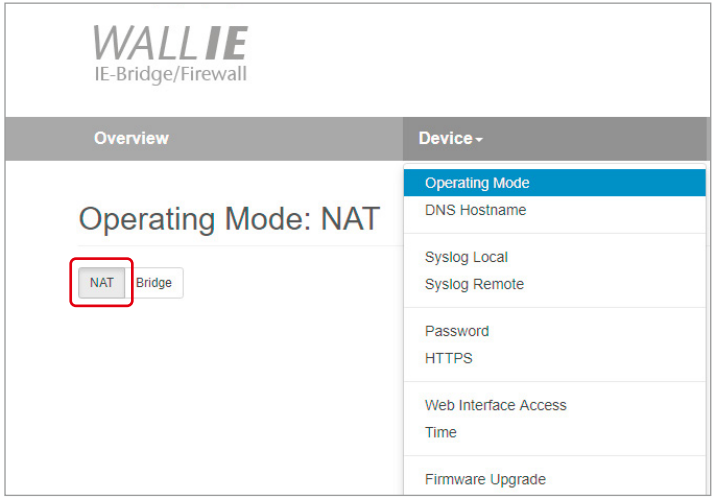
Dies erlaubt die Abtrennung eines Teils des Produktionsnetzwerkes ohne die Verwendung von unterschiedlichen Netzwerk-Adressen.

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

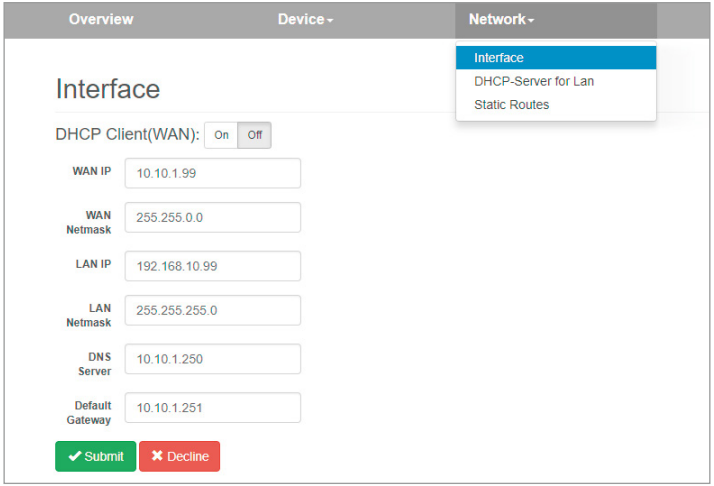
Klicken Sie auf das Menü „Network“ und wählen das Untermenü „Interface“ aus. Hier können die IP-Adressen des WALL IE im WAN und im LAN („WAN IP“/“LAN IP“) sowie die zugehörigen Subnetzmasken („WAN netmask“/LAN netmask“) festgelegt werden.

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, 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.

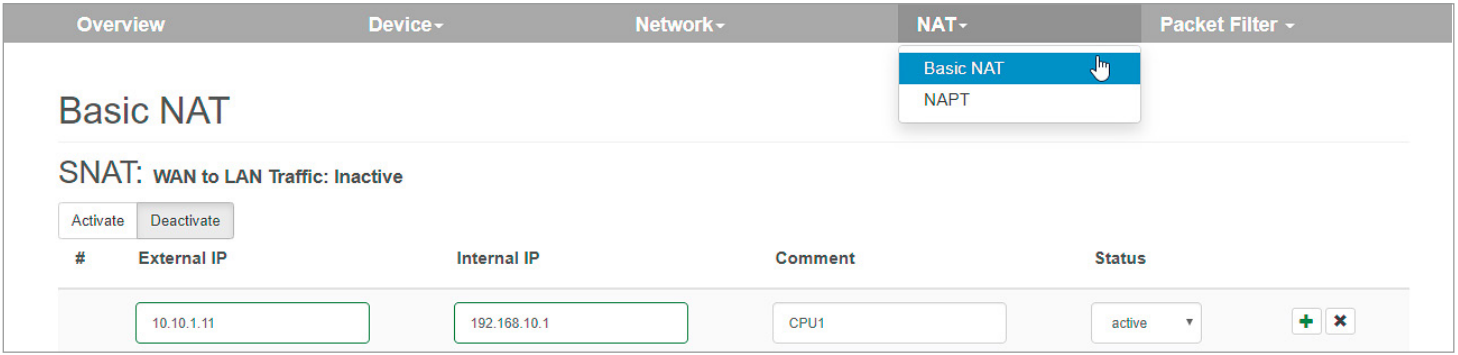
Hinweis: *Wenn Sie die LAN IP-Adresse verändern, müssen Sie ggf. am Browser die Webseite des WALL IE unter der neuen IP-Adresse erneut öffnen und sich wieder einloggen.*



6.2. Einrichtung von „Basic NAT“ Regeln

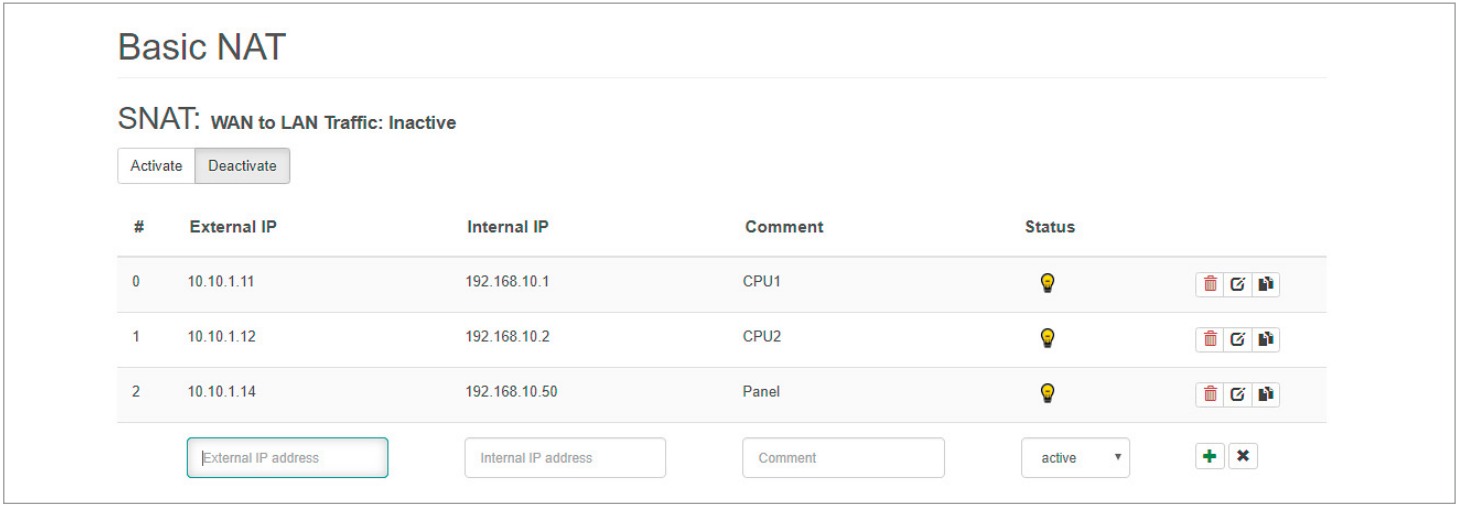
Zum Eintragen von „Basic NAT“ Regeln muss WALL IE im Betriebsmodus „NAT“ sein.

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 Fertigungsnetzwerk (WAN) sichtbar wird. Die „Internal IP“ ist die IP-Adresse des Netzwerkteilnehmers in der Maschine (LAN). Als Kommentar kann ein beliebiger Text eingegeben werden.

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

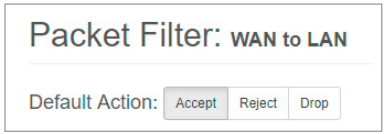


Status	
	Regel aktiv (ein Klick auf die Lampe ändert den Status).
	Regel inaktiv (ein Klick auf die Lampe ändert den Status).

Action			
	Regel hinzufügen		Regel bearbeiten
	Regel löschen		Regel kopieren

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.



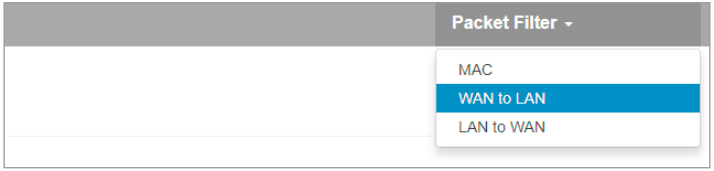
6.3. Paketfilter „WAN to LAN“

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 Produktions-netzwerk mit definierten Teilnehmern aus der Automatisierungs-zelle Daten austauschen dürfen.

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

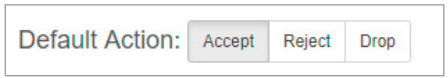
Hinweis: *Die Paketfilter stehen auch in der Richtung „LAN to WAN“ zur Verfügung, siehe Seite 13.*



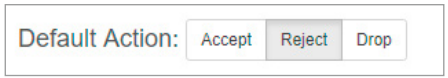
Im Menü „Packet Filter“ wählen Sie den Menüpunkt „WAN to LAN“.

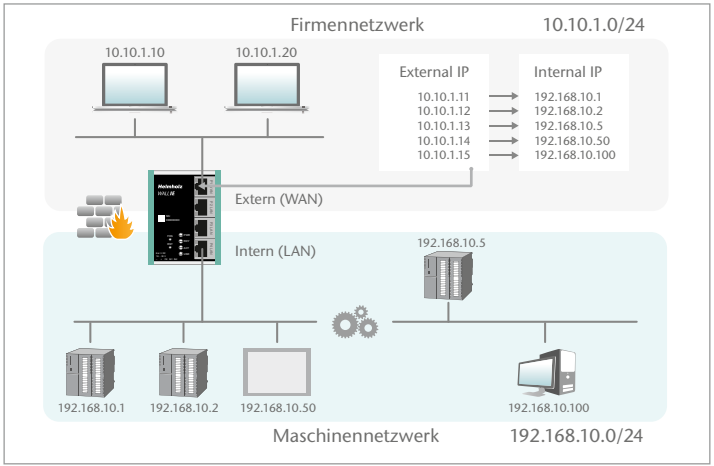
Über die Option „Default Option“ können Sie einstellen, ob generell alle Tele-gramme erlaubt sind („Accept“) und nur spezielle Pakete gefiltert werden („Blackli-sting“), oder ob generell alle Telegramme verboten sind („Reject“/„Drop“) und nur die Telegramme nach den Filterregeln durchgelassen werden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

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



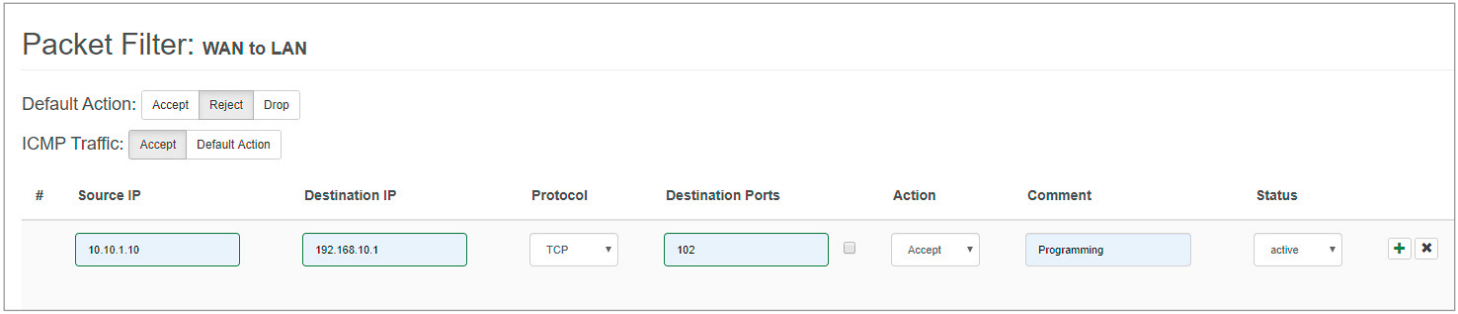
Um den Zugriff auf das Maschinennetzwerk auf bestimmte Teilnehmer im WAN zu beschränken, stellen Sie die Default Action auf „Reject“ oder „Drop“. „Reject“ sendet bei nicht erlaubten Telegrammen aus dem WAN eine Fehlermeldung zurück, „Drop“ verwirft das Telegramm ohne Fehlermeldung.





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“ oder „UPD“ 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“.

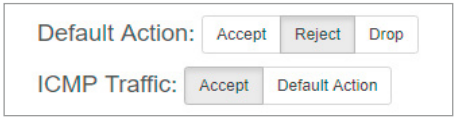
#	Source IP	Destination IP	Protocol	Destination Ports	Action	Comment	Status
0	10.10.1.10	192.168.10.1	TCP	102	Accept	Programming	
1	10.10.1.20	192.168.10.1	TCP	1:65535	Accept	Engineering	
2	10.10.1.10	192.168.1.2	TCP	80,443,1194	Accept	Remote Maint.	

Es ist auch möglich den Zugriff von mehreren Teilnehmern zueinander zu regeln. 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“.

3	10.10.1.1-10.10.1.9	192.168.10.1	TCP	1:65535	Accept	Many		
4	10.10.1.200	192.168.10.1-192.168.10.200	TCP	1:65535	Accept	Master machine		

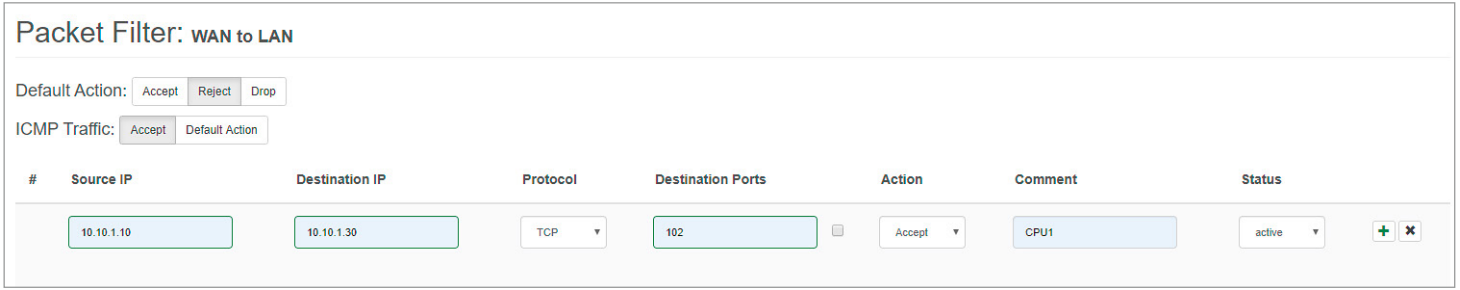
Action legt fest ob diese Regel die Kommunikation erlaubt („Accept“), mit Fehler ablehnt („Reject“) oder einfach verwirft („Drop“). Im Zusammenspielt mit der „Default Action“ sollte hier immer die passende Methode gewählt werden. Ist die Default Action z.B. „Reject“ oder „Drop“ so sollten die Filter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

Mit der Option „ICMP Traffic“ können Sie das Durchleiten von ICMP-Paketen – z.B. ein „Ping“ – generell erlauben („Accept“) oder abhängig von den Packet Filtern ggf. 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



6.4. 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.

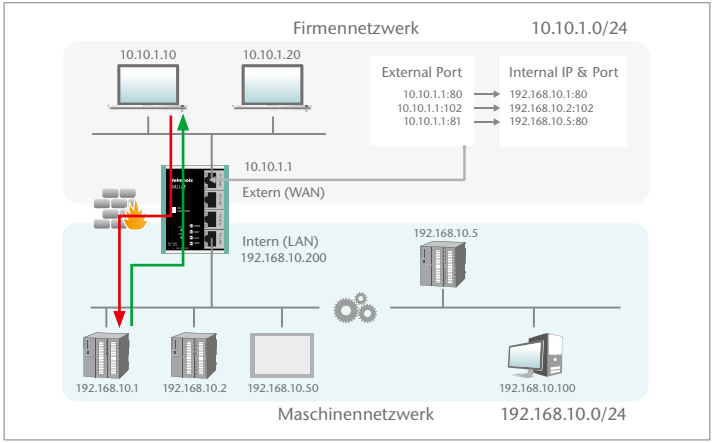
Die Eingabe der Filterregeln entspricht den Paketfilterregeln „WAN to LAN“ nur dass die Source IP jetzt die LAN-IP ist und die Destination IP ein Gerät im WAN adressiert.

Hinweis: *Im NAT Betriebsmodus steht zusätzlich noch die MAC Adressen Filterung zur Verfügung,* *siehe Seite 21.*

6.5. SNAT

Mit der Funktion „SNAT (Source NAT)“ wird der eingehende Datenverkehr von der WAN Seite transparent an das LAN-Netzwerk weitergegeben. Alle zum LAN ausgehenden Datenpakete erhalten als Absenderadresse die IP-Adresse des WALL IE.

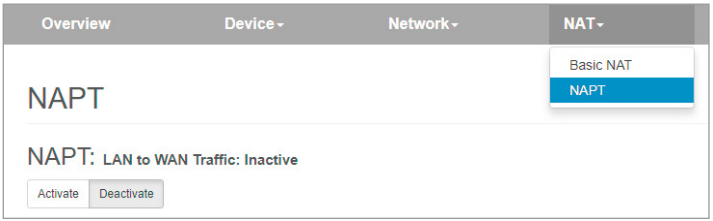
Somit benötigt keiner der LAN-Teilnehmer als „Gateway“ die WALL IE LAN-IP-Adresse. Dies ist ein erheblicher Vorteil bei der Integration in bestehende Netzwerkstrukturen, da die Parameter der LAN-Geräte nicht mehr geändert werden müssen.

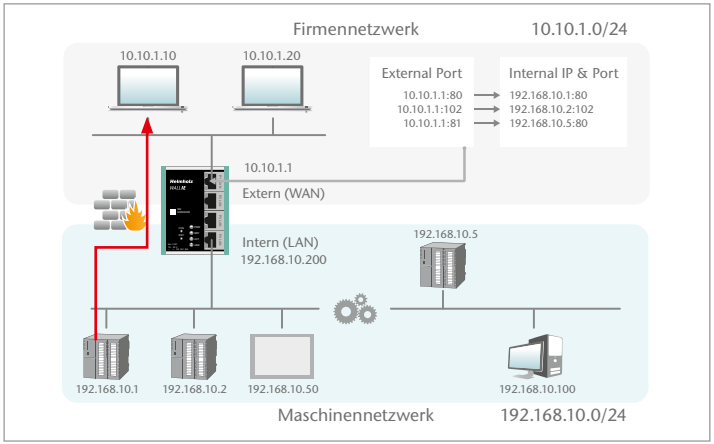


6.6. NAPT

„NAPT for LAN to WAN traffic“ ersetzt die Absender-Adressen von Anfragen aus der Automatisierungszelle (LAN) durch die Adresse des WALL IE („Source NAT“) im WAN.

Ist die Option abgeschaltet, so werden die Anfrage-Pakete mit ihrer original Absender-IP an das WAN weitergeleitet.

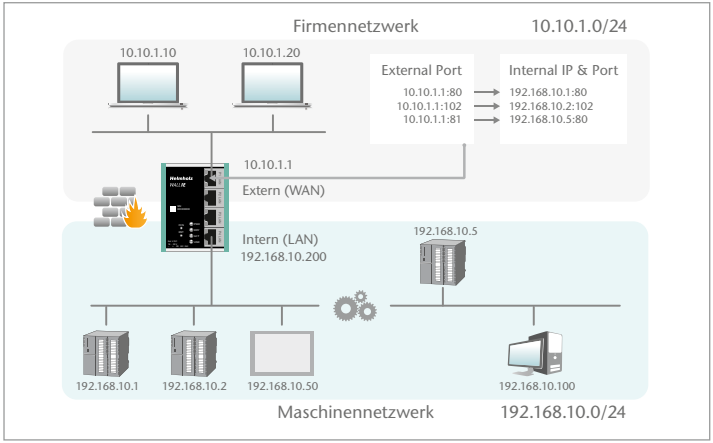




6.7. Portforwarding

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 in der Automatisierungszelle (LAN) weitergeleitet werden (z.B. 10.10.1.1:81 zu 192.168.10.5:80).

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.*



Port Forwarding: WAN (10.10.1.99) to LAN Traffic

#	Protocol	External Port	Internal IP	Internal Port	Comment	Status	
0	TCP	81	192.168.10.1	80	CPU1		
	TCP	External Port	Internal IP address	Internal Port	Comment	active	

Protocol	TCP/UDP
External Port	Der Port unter dem die Telegramme im WAN unter der Adresse des WALL IE empfangen werden.
Internal IP	Die im Maschinennetz (LAN) anzusprechende IP-Adresse.
Internal Port	Der im Maschinennetz (LAN) anzusprechende Port des Gerätes.

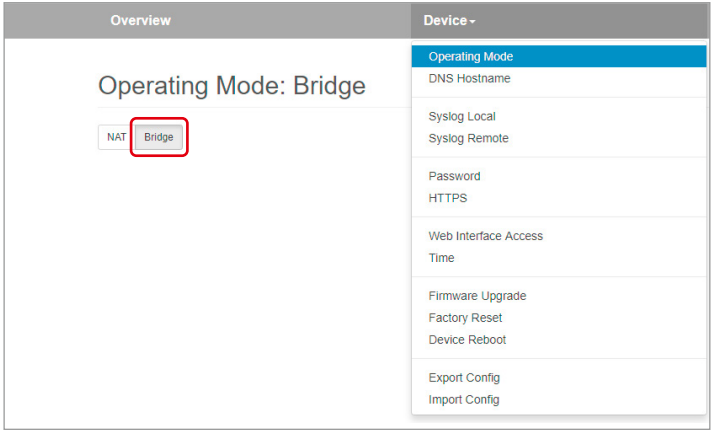
Comment	Frei definierbarer Kommentar
Status	Regel ist aktiv (Ein Klick auf das Lampensymbol ändert den Regelstatus in Inaktiv) Regel ist inaktiv (Ein Klick auf das Lampensymbol ändert den Regelstatus in Aktiv)
Action	Regel löschen Regel hinzufügen

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

Im NAT Betriebsmodus steht zusätzlich noch die MAC Adressen Filterung zur Verfügung, siehe Seite 21.

7. Bridge Mode

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



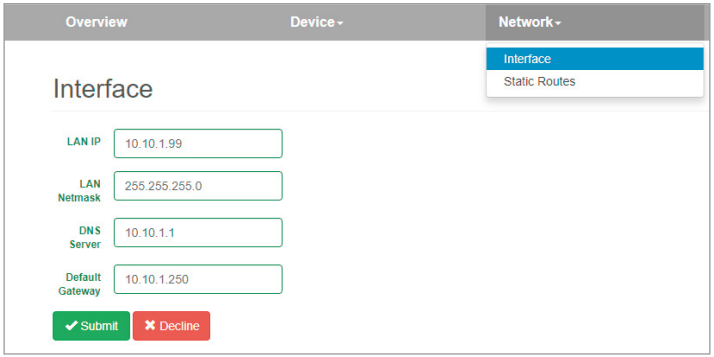
7. Anpassen der IP-Adressen im Bridge Betriebsmodus

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

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

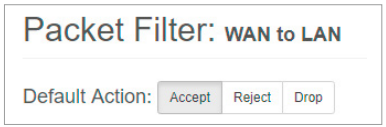
Ein DNS-Server und ein Default-Gateway können ebenfalls angegeben werden. Das ist notwendig, wenn Geräte aus dem LAN über den WALL IE das Internet erreichen sollen. Werden diese nicht ange-geben, dann wird verhindert, dass Geräte im LAN mit dem Internet kommunizieren.

Die Eingabe wird mit dem Button „Submit“ gespeichert.



Achtung *: Im Bridge Betriebsmodus 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.



7.2. 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.

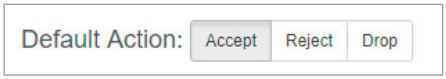
Folgende Filterkriterien auf Layer 3 und 4 stehen zur Verfügung: IPv4-Adressen, Protokoll (TCP/UDP) und Ports.

Hinweis: *Die Paketfilter stehen auch in der Richtung „LAN to WAN“ zur Verfügung, siehe Seite 20.*

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

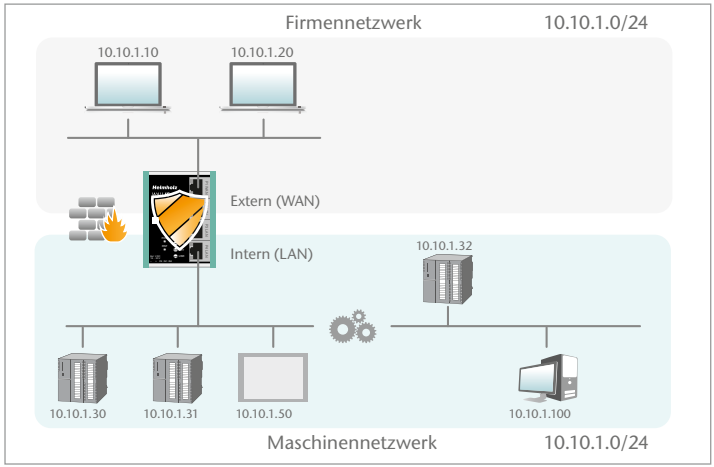
Über die Option „Default Option“ können Sie einstellen, ob generell alle Telegramme erlaubt sind („Accept“) und nur spezielle Pakete gefiltert werden („Blacklisting“), oder ob generell alle Telegramme verboten sind („Reject“/„Drop“) und nur die Telegramme nach den Filterregeln durchgelassen werden sollen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

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

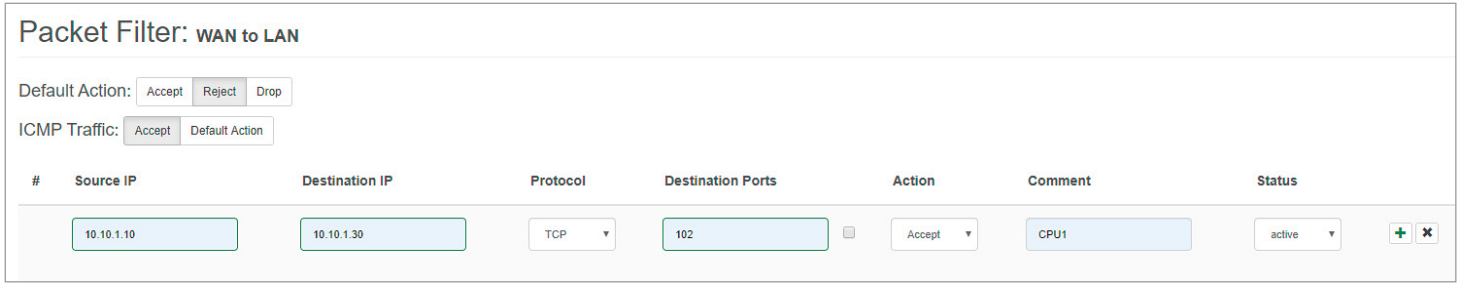


Um den Zugriff auf das Maschinennetzwerk auf bestimmte Teilnehmer im WAN zu beschränken, stellen Sie die Default Action auf „Reject“ oder „Drop“. „Reject“ sendet bei nicht erlaubten Telegrammen aus dem WAN eine Fehlermeldung zurück, „Drop“ verwirft das Telegramm ohne Fehlermeldung.

Beispiel: Es soll einem PC im Produktionsnetzwerk (WAN), mit der 10.10.1.10 (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“ oder „UPD“ 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“.

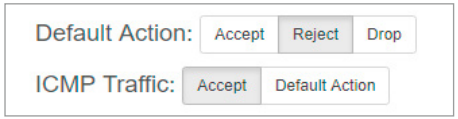
#	Source IP	Destination IP	Protocol	Destination Ports	Action	Comment	Status
0	10.10.1.10	10.10.1.30	TCP	102	Accept	CPU1	
1	10.10.1.20	10.10.1.30	TCP	1:65535	Accept	Engineering	
2	10.10.1.20	10.10.1.31	TCP	80,443,1194	Accept	Remote Maint.	

Es ist auch möglich den Zugriff von mehreren Teilnehmern zueinander zu regeln. 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“.

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	Webaccess	

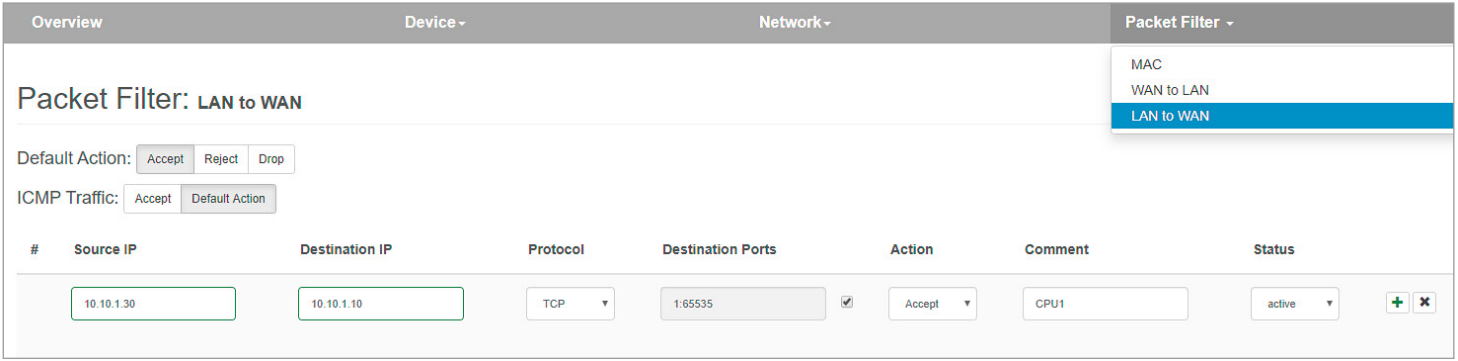
Action legt fest, ob die Regel die Kommunikation erlaubt („Accept“), mit Fehler ablehnt („Reject“) oder einfach verwirft („Drop“). Im Zusammenspiel mit der „Default Action“ sollte hier immer die passende Methode gewählt werden. Ist die Default Action z.B. „Reject“ oder „Drop“ so sollten die Filter Regeln 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).

Mit der Option „ICMP Traffic“ können Sie das Durchleiten von ICMP-Paketen – z.B. ein „Ping“ – generell erlauben („Accept“) oder abhängig von den Packet Filtern ggf. 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.



7.3. Paketfilter „LAN to WAN”

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



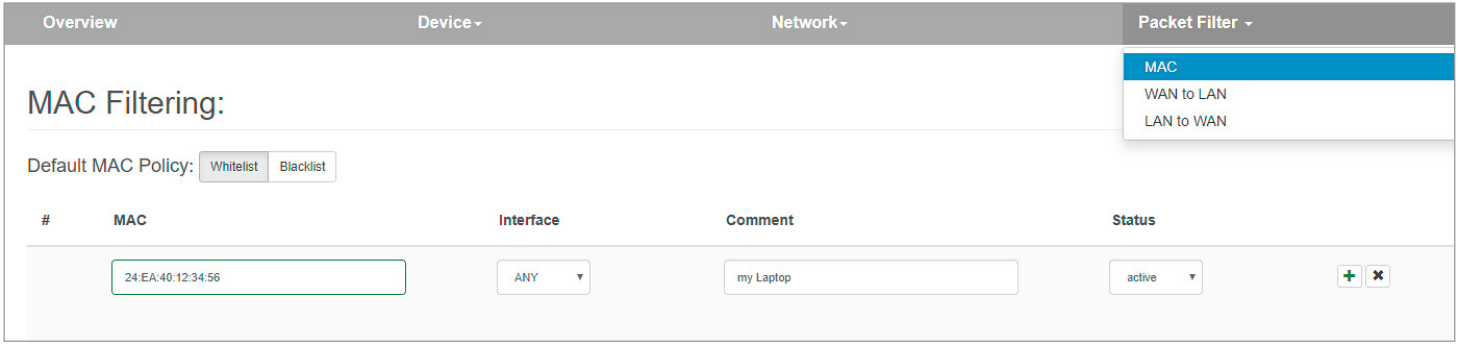
Im Packet Filter “LAN to WAN” kann die Kommunikation von Geräten im LAN mit Geräten im Produktionsnetzwerk (WAN) ganz unterbunden oder für bestimmte Geräte gesperrt oder erlaubt werden.

Hinweis: *Im Bridge Betriebsmodus steht zusätzlich noch die MAC Adressen Filterung zur Verfügung,* *siehe Seite 21.*

8. MAC-Adressen Filterung

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

Die Filterung kann auf der WAN, auf der LAN oder auf beiden Seiten („ANY“) für jede MAC-Adresse getrennt 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 WALL IE. 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.

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

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

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.*

9. Firmwareupdate

Die Firmware des WALL IE kann über die Webseite sehr einfach aktualisiert werden.

Bitte laden Sie die Firmware-Update-Datei unter **www.helmholz.de** herunter oder scannen Sie den QR-Code.

SCAN QR CODE TO GET FIRMWARE

WALL IE Industrial NAT Gateway / Firewall

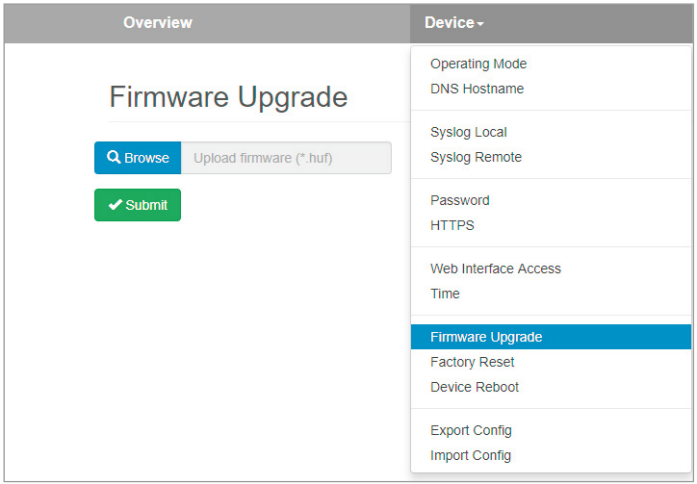
Firmware

Die Firmwaredatei hat die Dateiendung „HUF“ (Helmholz Update File) 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 WALL IE übertragen - das kann je nach Netzverbindung - bis zu 1 Minute dauern.

Im WALL IE wird die Firmwaredatei entschlüsselt und überprüft. Ist der Inhalt korrekt wird die Firmware in den Programmspeicher gebrannt und ein Neustart des WALL IE 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 aber zu Konfigurationsfehlern 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 WALL IE Webseite zu aktualisieren.*

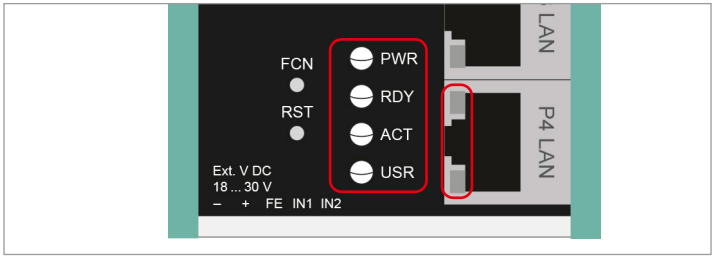
10. Rückstellen auf Werkseinstellungen

Um WALLIE in den Auslieferungszustand zurückzustellen, muss der „FCN“-Taster betätigt werden, während das Gerät neu gestartet wird. Ein Neustart kann durch Power OFF/ON, durch betätigen des „RST“-Tasters oder durch die Funktion „Device reboot“ auf der Webseite ausgeführt werden.

Das erfolgreiche Zurücksetzen der Parameter und Einstellungen wird beim Bootvorgang durch Aufleuchten der „USR“-LED quittiert.

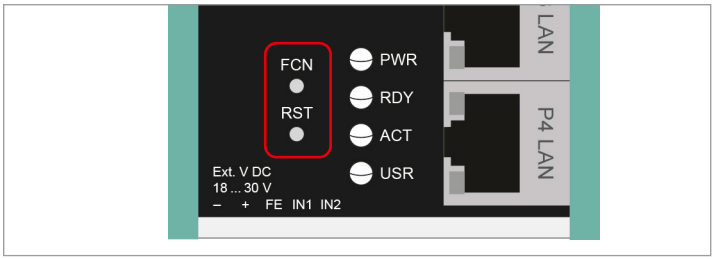
11. LED-Statusinformationen

PWR	Aus Ein	Keine Spannungsversorgung oder Gerät defekt. Gerät ist korrekt mit Spannung versorgt.
RDY	Ein	Gerät ist betriebsbereit.
ACT	Blinkt oder ein	Erlaubter Datenverkehr zwischen WAN und LAN.
USR	Ein	Werkseinstellung Reset aktiv.
RJ45-LEDs	Grün (Link) Orange (Act)	Verbunden. Datenübertragung am Port.



12. Tasterfunktionen

FCN	Mit dem „FCN“-Taster kann der WALLIE auf Werkseinstellungen zurückgesetzt werden. Der „FCN“-Taster muss dafür während der Hochlaufphase des WALLIE gedrückt gehalten werden. Das erfolgreiche Zurücksetzen der Parameter und Einstellungen wird beim Bootvorgang durch Aufleuchten der „USR“-LED quittiert. Der „FCN“-Button kann dann losgelassen werden.
RST	Der „RST“-Button löst einen sofortigen Neustart des WALLIE aus, bei dem alle gespeicherten Einstellungen erhalten bleiben.



13. Technische Daten

WALLIE, Industrial Ethernet Bridge und Firewall (700-860-WAL01)

Abmessungen (TxBxH)	32,5 x 58,5 x 76,5 mm
Gewicht	ca. 130 g
Anzahl der Eingänge	2 | DC 24 V, nach DIN EN 61131-2 Type 2
WAN-Schnittstelle	1 x
- Typ	10-Base-T/100-Base-T
- Anschluss	RJ45 Buchse
- Übertragungsrate	10/100 Mbit/s
LAN-Schnittstelle	3 x
- 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- und 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	
- 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/UL 61010-2-201
- Voltage supply	DC 24 V (18 ... 30 V DC, SELV and limited energy circuit)
- Pollution degree	2
- Altitude	Up to 2000 m
- Temperature cable rating	87 °C

Hinweis:

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 Kunden sind uns wichtig. Wir freuen uns über Verbesserungsvorschläge und Anregungen.