



WALL IE / WALL IE PLUS / WALL IE Compact Industrial NAT Gateway und Firewall Handbuch

Ausgabe 11b | 05.05.2023

Bestellnummern:

WALL IE	700-860-WAL01 ab Firmware V 1.10.200
WALL IE PLUS	700-862-WAL01 ab Firmware V 1.00.000
WALL IE Compact	700-863-WAL01 ab Firmware V 1.00.000



Link zur neuesten Version
des Handbuchs

Hinweise

Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung dieses Handbuchs, oder Teilen daraus, vorbehalten. Kein Teil des Handbuchs darf ohne schriftliche Genehmigung der Helmholz GmbH & Co. KG in irgendeiner Form (Fotokopie, Mikrofilm oder andere Verfahren), auch nicht für Zwecke der Unterrichtsgestaltung, oder unter Verwendung elektronischer Systeme reproduziert, verarbeitet, vervielfältigt oder verbreitet werden.

Die jeweils aktuelle Version des Handbuchs finden Sie im Internet unter www.helmholz.de.

Wir freuen uns über Verbesserungsvorschläge und Anregungen.

Open Source

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 bereitgestellt.

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

Copyright © 2023 by

Helmholz GmbH & Co. KG

Hannberger Weg 2 | 91091 Großenseebach

Änderungen in diesem Dokument:

Stand	Datum	Änderung
1	12.5.17	Erste Version / Firmware V1.04
2	16.1.19	Umbau auf Anwendungsfälle NAT und Bridge; Ergänzungen Firmware V1.06 (DHCP-Server/-Client, Portranges) und Korrekturen
3	8.7.19	FW V1.08.100: SNAT
4	27.9.19	Tippfehler in Kap. 1.2 QR-Codes korrigiert und Hyperlinks hinzugefügt
5	16.1.20	Firmware V1.08.200: Screenshots aktualisiert Produktmaße korrigiert
6	7.4.20	Hinweis auf Recycling/WEEE eingefügt Auflösung der Bilder verbessert Firmware V1.08.400: IP-Ranges für NAT-Regeln
7	13.1.21	Neu: DNS-Server (Kap. 11.2) Neu: ICMP in Filterregeln (Kap. 6.5, 7.4) Neu: FTP-Helper (Kap. 7.7)
8	18.2.22	Aktualisierung Security Empfehlungen Firmware V1.10.100: FTP-Helper funktioniert jetzt auch im NAT-Modus
9	14.7.22	Diverse Textkorrekturen
10	26.8.22	Ergänzung WALL IE PLUS
11	27.4.23	Ergänzung WALL IE Compact Ergänzung „NTP on LAN“ und DHCP „static leases“
11b	5.5.23	Textkorrekturen

STEP, TIA und Simatic sind eingetragene Warenzeichen der Siemens AG.

Inhalt

1	Allgemeines	6
1.1	Zielgruppe des Handbuchs	6
1.2	Sicherheitshinweise	6
1.3	Hinweiszeichen und Signalwörter	7
1.4	Bestimmungsgemäße Verwendung	8
1.5	Missbrauch	8
1.6	Montage / Demontage	9
1.6.1	Zugangsbeschränkung	9
1.6.2	Montage und Mindestabstände	9
1.6.3	Elektrische Installation	9
1.6.4	Schutz vor elektrostatischen Entladungen	9
1.6.5	Überstrom-Schutz	9
1.6.6	EMV-Schutz	10
1.6.7	Betrieb	10
1.6.8	Recycling / WEEE	10
1.7	Haftung	11
1.7.1	Haftungsausschluss	11
1.7.2	Gewährleistung	11
1.8	Open Source	11
2	Security Empfehlungen	12
3	Übersicht	14
3.1	Aufbau des WALL IE (700-860-WAL01)	15
3.2	WALL IE PLUS (700-862-WAL01)	15
3.3	WALL IE Compact (700-863-WAL01)	15
3.4	Anschließen des WALL IE	16
3.5	LEDs Statusinformationen	17
3.5.1	WALL IE (700-860-WAL01)	17
3.5.2	WALL IE PLUS (700-862-WAL01)	17
3.5.3	WALL IE Compact (700-863-WAL01)	17
4	Erster Zugriff auf das Webinterface	18
4.1	Erstanmeldung	19
4.2	Hauptansicht	20
4.2.1	Menü Übersicht	21

4.2.2	Responsive Design	21
4.3	Portzuordnung WAN/LAN	22
5	Wahl der Betriebsart.....	23
5.1	Der NAT Betriebsmodus.....	23
5.2	Der Bridge-Betriebsmodus	24
6	Anwendungsfall NAT	25
6.1	Anpassen der IP-Adressen im NAT-Betriebsmodus	25
6.2	DHCP-Client am WAN-Interface aktivieren	26
6.3	Einrichtung von „Basic NAT“ Regeln	27
6.4	Paketfilter „WAN to LAN“	29
6.5	ICMP Traffic "WAN to LAN"	31
6.6	Paketfilter „LAN to WAN“	32
6.7	ICMP Traffic "LAN to WAN"	32
6.8	FTP-Helper für aktives FTP	33
6.9	SNAT	34
6.10	NAPT	35
6.11	Portforwarding	36
7	Anwendungsfall Bridge	38
7.1	Bridge Modus aktivieren	38
7.2	Anpassen der IP-Adressen im Bridge Betriebsmodus	38
7.3	Paketfilter „WAN to LAN“	39
7.4	ICMP Traffic "WAN to LAN"	41
7.5	Paketfilter „LAN to WAN“	42
7.6	ICMP Traffic "LAN to WAN"	42
8	MAC-Adressen Filterung	43
9	Statische Routen	44
10	Anwendung mit Simatic Step 7 / TIA Portal.....	45
10.1	Anwendung mit Step 7.....	46
10.2	Anwendung im TIA-Portal.....	47
11	Weitere Funktionen	49
11.1	DHCP Server for LAN	49
11.2	DNS-Server für LAN	50
11.3	Hostname (WAN).....	51
11.4	Syslog Server	52

11.4.1	Syslog Local	52
11.4.2	Syslog Remote	52
11.5	Passwort ändern (Password) / Userverwaltung	53
11.6	Zertifikat hinterlegen (HTTPS)	55
11.7	Web Interface Zugriff im WAN-Netzwerk erlauben (Web Interface Access)	55
11.8	Zeiteinstellungen (Time).....	56
11.9	Export / Import der Konfiguration.....	57
12	Firmwareupdate	58
13	Rückstellen auf Werkseinstellung	59
13.1	Rückstellen auf Werkseinstellung über Webseite	59
13.2	Rückstellen auf Werkseinstellung über Taster.....	59
14	FAQ.....	60
15	Technische Daten	61
15.1	WALL IE (700-860-WAL01).....	61
15.2	WALL IE PLUS (700-862-WAL01)	62
15.3	WALL IE Compact (700-863-WAL01).....	63
15.4	Maßzeichnung WALL IE (700-860-WAL01).....	64
15.5	Maßzeichnung WALL IE PLUS (700-862-WAL01)	64
15.6	Maßzeichnung WALL IE Compact (700-863-WAL01)	65

1 Allgemeines

Diese Betriebsanleitung gilt ausschließlich für Geräte, Baugruppen, Software und Leistungen der Helmholz GmbH & Co. KG.

1.1 Zielgruppe des Handbuchs

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



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

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

1.2 Sicherheitshinweise

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

1.3 Hinweiszeichen und Signalwörter



GEFAHR

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



WARNUNG

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



VORSICHT

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



ACHTUNG

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



HINWEIS

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

1.4 Bestimmungsgemäße Verwendung

Die Produkte der WALL IE „Industrial Bridge und Firewall“ Baureihe (im Folgenden "das Gerät" oder „die Geräte“ genannt) verbindet zwei Ethernet Netzwerke.

Die Geräte werden mit einer werkseitigen Hard- und Software-Konfiguration ausgeliefert. Die Hard- und Software-Konfiguration auf die Anwendungsbedingungen muss durch den Anwender erfolgen. Änderungen der Hard- oder Software-Konfiguration, die über die dokumentierten Möglichkeiten hinausgehen, sind unzulässig und bewirken den Haftungsausschluss der Helmholz GmbH & Co. KG.



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

Die WALL IE Industrial Bridge und Firewall ist nicht für eine direkte Verbindung mit dem Internet verwendbar. Verwenden Sie für eine Internetverbindung immer einen dedizierten Router mit einer ausreichend dimensionierten Internet-Firewall. Beachten Sie bei der Projektierung, Verwendung und Wartung die Empfehlungen zur Security (s. Kap. 2).

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

Die in den technischen Daten angegebenen Umgebungsbedingungen müssen eingehalten werden.

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

1.5 Missbrauch



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

1.6 Montage / Demontage

1.6.1 Zugangsbeschränkung

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

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

1.6.2 Montage und Mindestabstände

Die Geräte können auf eine DIN-Hutschiene montiert und in beliebiger Lage eingebaut werden. Es wird empfohlen, bei der Montage Mindestabstände einzuhalten. Durch die Einhaltung der Mindestabstände

- ist das Montieren bzw. Demontieren der Module möglich, ohne andere Anlagenteile demontieren zu müssen.
- ist genügend Raum vorhanden, um alle vorhandenen Anschlüsse und Kontaktierungsmöglichkeiten mit handelsüblichem Zubehör zu verbinden.
- ist Platz für evtl. nötige Kabelführungen vorhanden.



ACHTUNG

Die Montage ist gemäß VDE 0100/IEC 364 und nach geltenden nationalen Normen durchzuführen. Das Gerät besitzt den Schutzgrad IP20. Wird ein höherer Schutzgrad benötigt, muss der Einbau in ein Gehäuse oder einen Schaltschrank erfolgen.

1.6.3 Elektrische Installation

Die regional gültigen Sicherheitsbestimmungen sind zu beachten.

1.6.4 Schutz vor elektrostatischen Entladungen

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

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

1.6.5 Überstrom-Schutz

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

1.6.6 EMV-Schutz

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

1.6.7 Betrieb

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

Nachrüstungen, Veränderungen oder Umbauten am Gerät sind grundsätzlich verboten.

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



ACHTUNG

Bei der Abschaltung des WALL IE werden Netzwerkverbindungen unterbrochen! Stellen Sie vor Beginn jeglicher Arbeiten am Gerät sicher, dass bei Unterbrechung der Netzwerkverbindungen keine unzulässigen Störungen an angeschlossenen Anlagen auftreten.

1.6.8 Recycling / WEEE

Das Unternehmen Helmholz GmbH & Co. KG ist als Hersteller mit der Marke HELMHOLZ und der Geräteart „Kleine Geräte der Informations- und Telekommunikationstechnik für die ausschließliche Nutzung in anderen als privaten Haushalten“ sowie den folgenden Registrierungsdaten registriert:

Firma Helmholz GmbH & Co. KG,
Ort der Niederlassung/Sitz 91091 Großenseebach,
Anschrift Hannberger Weg 2,
Name des Vertretungsberechtigten Carsten Bokholt,
Registrierungsnummer DE 44315750.



Die in diesem Dokument beschriebenen Elektrogeräte sind dem Recycling zuzuführen. Sie dürfen gemäß Richtlinie 2012/19/EU über Elektro- und Elektronik-Altgeräte (WEEE) nicht über kommunale Entsorgungsbetriebe entsorgt werden.

1.7 Haftung

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

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

1.7.1 Haftungsausschluss

Die Helmholz GmbH & Co. KG haftet nicht bei Schäden, wenn diese durch nicht bestimmungs- oder sachgemäße Benutzung oder Anwendung der Produkte verursacht wurden.

Die Helmholz GmbH & Co. KG übernimmt keine Haftung für eventuell in der Bedienungsanleitung enthaltene Druckfehler oder sonstige Ungenauigkeiten, es sei denn, es sind gravierende Fehler, die Helmholz GmbH & Co. KG nachweislich bereits bekannt sind.

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

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

1.7.2 Gewährleistung

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

Die Gewährleistung erlischt bei:

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

Es gelten die bei Vertragsabschluss unter "Allgemeine Geschäftsbedingungen der Firma Helmholz GmbH & Co. KG" getroffenen Vereinbarungen.

1.8 Open Source

Unsere Produkte enthalten unter anderem Open Source Software. Diese Software unterliegt den jeweils einschlägigen Lizenzbedingungen. Die entsprechenden Lizenzbedingungen einschließlich einer Kopie des vollständigen Lizenztextes sind auf der Produkt-Webseite herunterladbar. Sie werden auch in unserem Downloadbereich der jeweiligen Produkte unter www.helmholz.de bereitgestellt.

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

2 Security Empfehlungen

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

Allgemein:

- Stellen Sie in regelmäßigen Abständen sicher, dass alle relevanten Komponenten diese Empfehlungen und ggf. weitere interne Sicherheits-Richtlinien erfüllen.
- Bewerten Sie Ihre Anlage ganzheitlich im Hinblick auf die Sicherheit. Nutzen Sie ein Zellschutzkonzept („Defense-in-Depth“) mit entsprechenden Produkten, wie z.B. dem WALL IE.
- Informieren Sie sich regelmäßig über Security Bedrohungen für alle ihre Komponenten

Physischer Zugang:

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

Sicherheit der Software:

- Halten Sie die Firmware alle Kommunikationskomponenten immer aktuell.
- Informieren Sie sich regelmäßig über Firmware Updates für das Produkt. Informationen hierzu finden Sie im Kapitel 12.
- Aktivieren Sie nur Protokolle und Funktionen, die Sie wirklich benötigen.
- Verwenden Sie nach Möglichkeit stets diejenigen Varianten von Protokollen, die mehr Sicherheit bieten.

Passwörter:

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

Helmholz ist Mitglied beim [CERT@VDE](mailto:cert@vde.de). Wir kommunizieren – neben unserem technischen Newsletter - unsere Security relevanten Updates, Patches und Handlungshinweise (Advisories) an Sie als Anwender der Helmholz Produkte. Informieren Sie sich und nutzen Sie die Dienste und die Datenbank des [CERT@VDE](mailto:cert@vde.de) um Ihre Anlagen sicher zu machen und sicher zu halten.

Das Helmholz „**Product Security Incident Response Team**“ (PSIRT) unterstützt Sie proaktiv, um Ihre Maschinen im Rahmen der industriellen Kommunikation bestmöglich zu schützen. Wann immer neue Gefährdungspotentiale auftreten oder uns gemeldet werden, bewerten und bearbeiten wir diese umgehend und versorgen Sie schnellstmöglich mit Handlungsempfehlungen, Patches und Updates, um das Risiko auf ein Minimum zu reduzieren.

Auch Sie können helfen: **Melden Sie Auffälligkeiten** zum Produkt an unser „Product Security Incident Response“ Team unter psirt@helmholz.de oder support@helmholz.de.

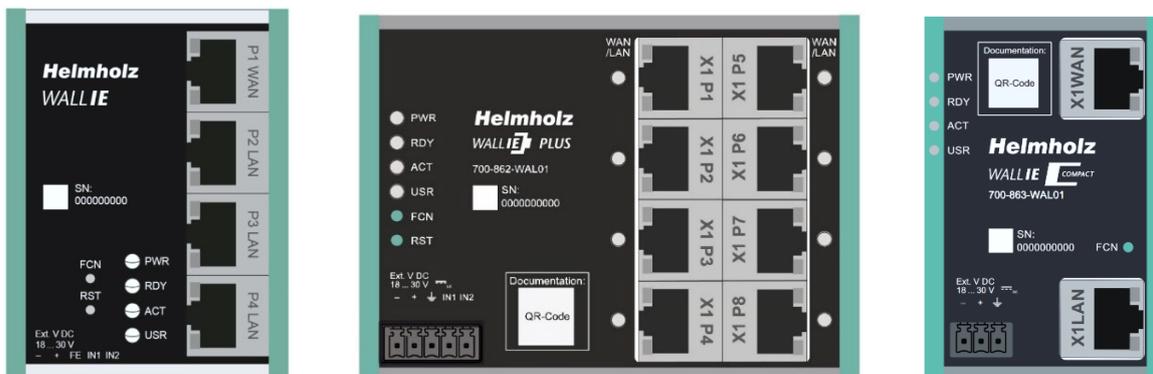
Weitere Informationen zum Thema Security erhalten Sie z.B. hier:

- [CERT@VDE](mailto:cert@vde.de)
- [Sichere-industrie.de](https://www.sichere-industrie.de)
- [Bundesamt für Sicherheit in der Informationstechnik \(BSI\)](https://www.bsi.bund.de)
- [Allianz für Cyber-Sicherheit](https://www.allianz-cyber.de)

3 Übersicht

Die Produkte der WALL IE „Industrial NAT Gateway und Firewall“ Baureihe integrieren Maschinen-netze auf einfache Weise in das übergeordnete Firmen- oder Produktionsnetz mittels Netzwerk-segmentierung, 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 Handbuch 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 dahinterliegende Automatisierungsnetzwerk.

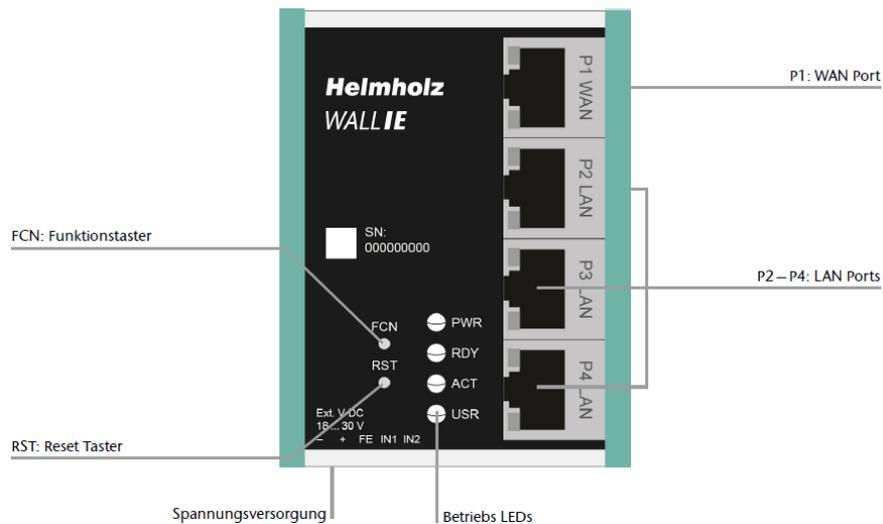
Im **Bridge-Betriebsmodus** agiert der WALL IE als Netzwerkbrücke in einem IPv4-Subnetz. Im Gegensatz zu normalen Switches ist in dieser Betriebsart die Paketfilterung möglich. Dadurch kann die Einschränkung des Zugriffs zu einzelnen Bereichen ihres Netzwerkes erreicht werden, ohne dass hierfür unterschiedliche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

Allgemeine Features:

- NAT (Basic NAT, SNAT, NAT, und Portforwarding) zur Netzwerksegmentierung
- Bridge-Funktionalität für Absicherung von Netzwerkbereichen mit im gleich Subnetz
- Zugriffsbeschränkung durch Paketfilter: IPV4-Adressen, Protokoll (TCP/UDP), Ports
- MAC-Adressen Filterung mit Black und Whitelisting
- DHCP-Server (LAN), DHCP-Client (WAN)
- Schnelle und einfache Konfiguration durch responsive Webinterface
- Statische Routen zu anderen Netzwerken
- Melden von Ereignissen an einen Syslog Server
- Export/Import der Konfiguration
- Industrietaugliche Bauform zur Hutschiene montage
- 4x RJ45 Interfaces 100 Mbit, 1x WAN + 3 x LAN (*WALL IE, 700-860-WAL01*)
- 8x RJ45 Interfaces 100/1000Mbit, WAN/LAN frei einstellbar (*WALL IE PLUS, 700-862-WAL01*)
- 2x RJ45 Interfaces 100/1000Mbit, 1x WAN + 1x LAN (*WALL IE Compact, 700-863-WAL01*)

3.1 Aufbau des WALL IE (700-860-WAL01)

Der WALL IE hat einen 100Mbit WAN-Port (P1) und drei 100 Mbit LAN-Ports (P2-P4, geschw.)

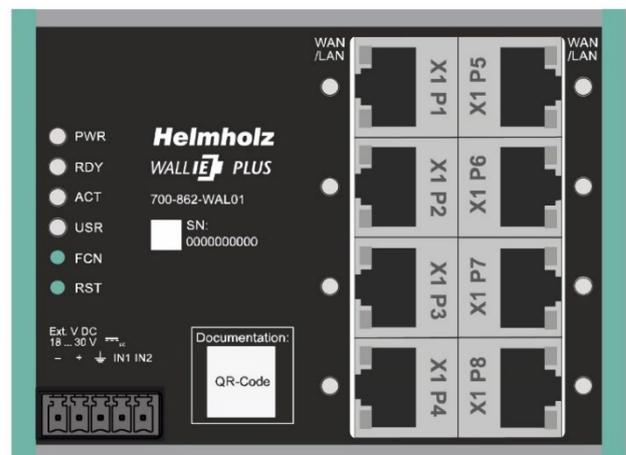


Über den Funktionstaster (FCN) kann ein Zurückstellen auf Werkseinstellungen durchgeführt werden (siehe Kap. 12). Der Reset Taster (RST) führt einen Neustart des WALL IE aus.

3.2 WALL IE PLUS (700-862-WAL01)

Der WALL IE PLUS hat 8 geschaltete Ports mit 100/1000Mbit (X1 P1- X1 P8). Die Ports können in der Konfiguration des WALL IE PLUS für WAN oder LAN beliebig zugeordnet werden (siehe Kap. 4.3). Eine LED an jedem Port zeigt die Zuordnung an. Bei Auslieferung ist Port P1 für das WAN-Netzwerk eingestellt und die Ports P2 bis P8 für das LAN-Netzwerk.

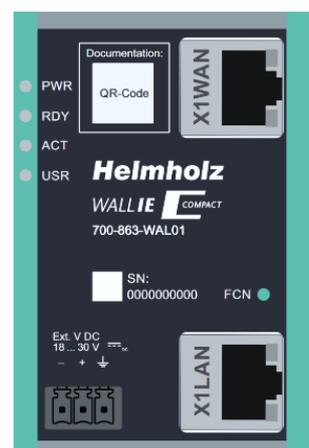
Über den Funktionstaster (FCN) kann ein Zurückstellen auf Werkseinstellungen durchgeführt werden (siehe Kap. 12). Der Reset Taster (RST) führt einen Neustart des WALL IE PLUS aus.



3.3 WALL IE Compact (700-863-WAL01)

Der WALL IE Compact hat die kleinste Bauform der WALL IE Baureihe und stellt 2 Ports mit 100/1000Mbit zur Verfügung (X1 WAN - X1 LAN).

Über den Funktionstaster (FCN) kann ein Zurückstellen auf Werks-einstellungen durchgeführt werden (siehe Kap. 12).



3.4 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 Sicherheitskleinspannung (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 geschwicht 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. Im Kapitel 4.3 ist erläutert, wie die Ports für LAN oder WAN konfiguriert werden können.

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.

3.5 LEDs Statusinformationen

3.5.1 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



3.5.2 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



3.5.3 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

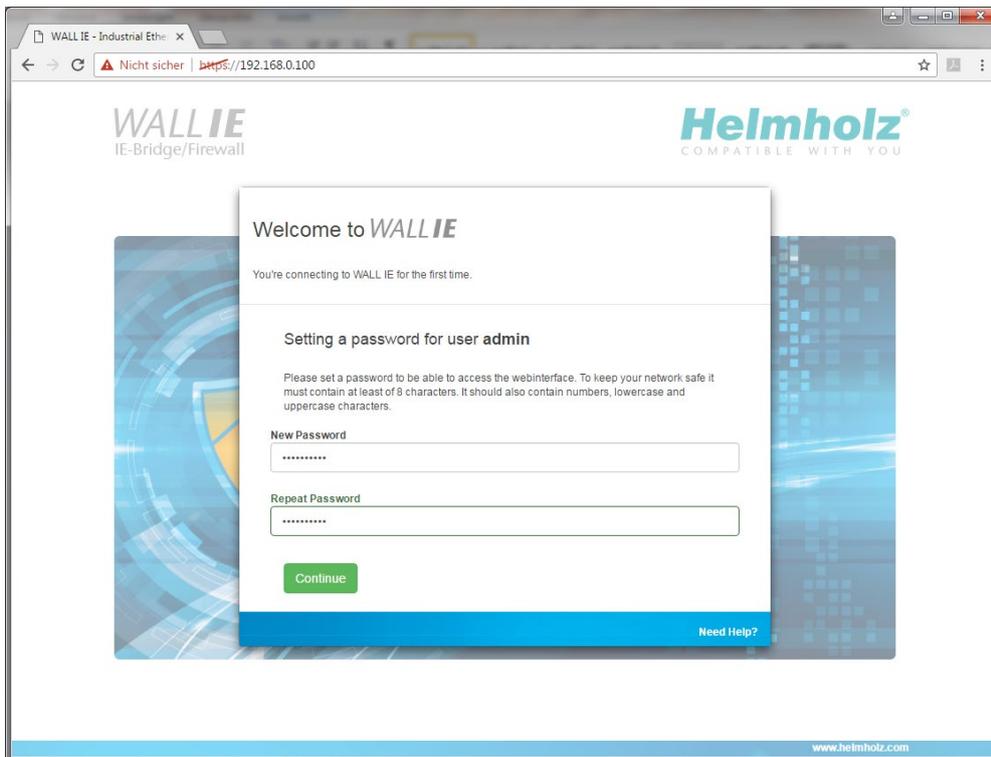
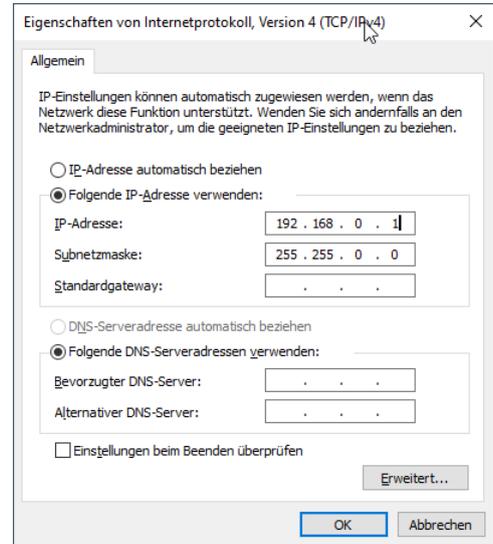


4 Erster Zugriff auf das Webinterface

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 Auslieferungszustand der Zugriff über die Ports P2 - P8 möglich oder über alle Ports deren LED grün leuchtet. Beim WALL IE Compact (700-863-WAL01) kann der LAN-Port verwendet 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 LAN-Port 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.

4.1 Erstanmeldung

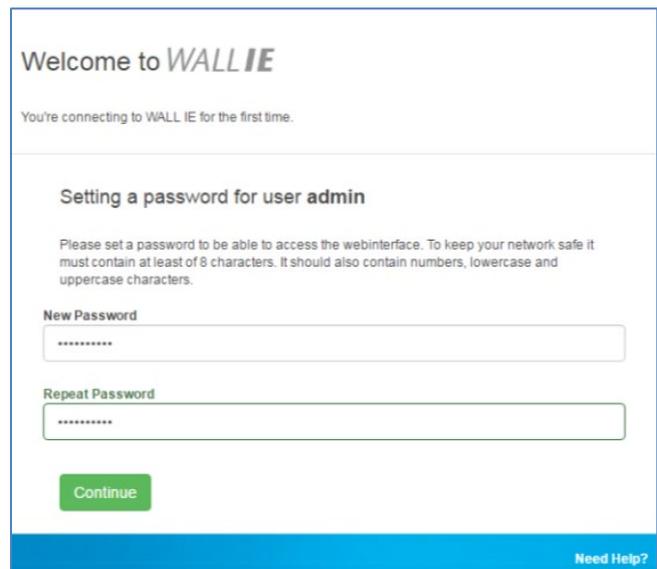
Bei der Erstanmeldung werden sie aufgefordert ein Passwort festzulegen.

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

Der Haupt-User ist immer „admin“.

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

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



The screenshot shows the 'Welcome to WALL IE' page. Below the header, it states 'You're connecting to WALL IE for the first time.' The main section is titled 'Setting a password for user admin'. A message explains that the password must be at least 8 characters long and include numbers, lowercase, and uppercase characters. There are two input fields: 'New Password' and 'Repeat Password', both containing asterisks. A green 'Continue' button is located below the fields. At the bottom right, there is a 'Need Help?' link.



ACHTUNG

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

4.2 Hauptansicht

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

Overview | Logout | Help

WALL IE
NAT Gateway/Firewall

Helmholz
COMPATIBLE WITH YOU

Overview Device Network NAT Packet Filter

Overview

Live Statistics

Uptime	0 days 23:01:17
System Time:	2/1/1970 01:16:53
Current User:	admin

Device Configuration

Timezone	Europe/Berlin
Operating Mode	NAT
INTERFACE	
DNS	10.10.1.250
GATEWAY	10.10.1.251
DHCP Server	OFF

Software

Firmware Version	V1.08.200
Linux Kernel Version	4.9.4
Open Source Software Licenses	

Hardware

Serial Number	00000293
Order Number	700-860-WAL01
Hardware Revision	1-1
LAN MAC Address	24-EA-40-0F-01-25
WAN MAC Address	24-EA-40-0E-01-25

www.helmholz.de



HINWEIS

Bitte prüfen Sie auf der Webseite des WALL IE, ob es eine neuere Firmwareversion gibt. Das Firmwareupdate ist im Kapitel 12 beschrieben.

Link zur Firmware:

<https://www.helmholz.de/goto/700-860-WAL01>

<https://www.helmholz.de/goto/700-862-WAL01>

<https://www.helmholz.de/goto/700-863-WAL01>

4.2.1 Menü Übersicht

Device ▾	Network ▾	NAT ▾	Packet Filter ▾
<ul style="list-style-type: none"> Operating Mode Hostname 	<ul style="list-style-type: none"> Interface DHCP-Server for Lan Static Routes 	<ul style="list-style-type: none"> Basic NAT NAPT 	<ul style="list-style-type: none"> MAC WAN to LAN LAN to WAN
<ul style="list-style-type: none"> Syslog Local Syslog Remote 			
<ul style="list-style-type: none"> Password HTTPS 			
<ul style="list-style-type: none"> Web Interface Access Time 			
<ul style="list-style-type: none"> Firmware Upgrade Factory Reset Device Reboot 			
<ul style="list-style-type: none"> Export Config Import Config 			

4.2.2 Responsive Design

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



HINWEIS

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

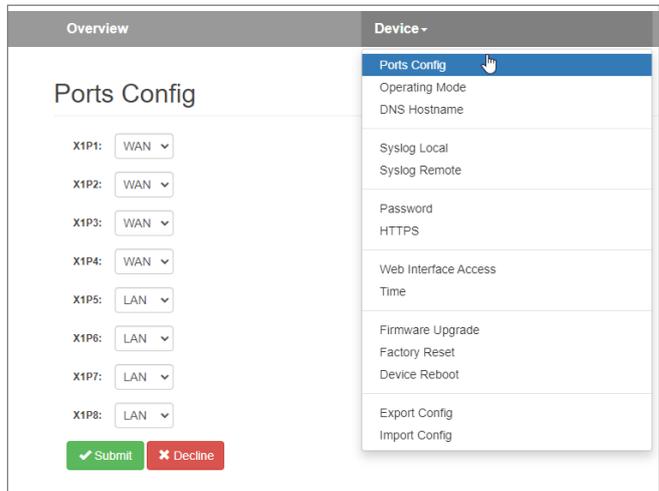
4.3 Portzuordnung WAN/LAN

Die Zuordnung der Ports für WAN (Firmennetzwerk) und LAN (Maschinennetzwerk) sind beim WALL IE (700-860-WAL01) fest vorgegeben. Der oberste Port „P1 WAN“ verbindet den WALL IE mit dem Firmennetzwerk, die 3 weiteren Ports („P2-P4 LAN“) verbinden den WALL IE mit dem Maschinennetzwerk. Die Ports P2 bis P4 sind geschaltet.

Der WALL IE PLUS (700-862-WAL01) hat 8 Ports („X1 P1 – X1 P8“), die frei für WAN oder LAN eingestellt werden können.

Die Konfiguration der Ports kann im Menü „Device/ Ports Config“ eingestellt werden.

Alle Ports für LAN und alle Ports für WAN sind untereinander geschaltet.



The screenshot shows the configuration interface for the WALL IE. On the right, a 'Device' menu is open, highlighting 'Ports Config'. The main area displays the 'Ports Config' page with eight ports (X1P1 to X1P8) and their assigned network types (WAN or LAN). At the bottom, there are 'Submit' and 'Decline' buttons.

Port	Assignment
X1P1	WAN
X1P2	WAN
X1P3	WAN
X1P4	WAN
X1P5	LAN
X1P6	LAN
X1P7	LAN
X1P8	LAN



ACHTUNG

Es muss mindestens ein Port des WALL IE PLUS für LAN und mindestens ein Port für WAN eingestellt sein.

5 Wahl der Betriebsart

Die folgenden Erläuterungen gelten gleichermaßen für WALL IE (700-860-WAL01) als auch für WALL IE PLUS (700-862-WAL01). Für die bessere Lesbarkeit wird im Folgenden nur von „WALL IE“ gesprochen.

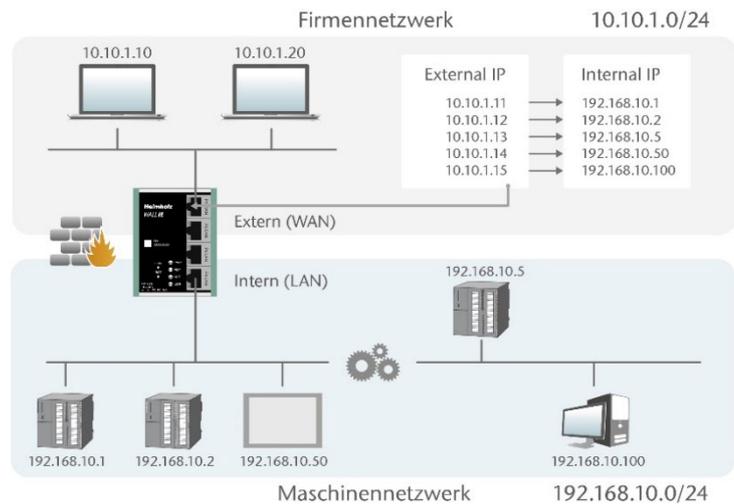
Abhängig von Anwendungsfall für den WALL IE muss zu Beginn die Betriebsart festgelegt werden. WALL IE unterstützt zwei grundsätzliche Betriebsarten: NAT und Bridge

5.1 Der NAT Betriebsmodus

Wenn eine Automatisierungszelle mit voreingestellten IP-Adressen in ein Firmennetzwerk mit einem anderen Subnet 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 Datenverkehrs parametrisiert werden.

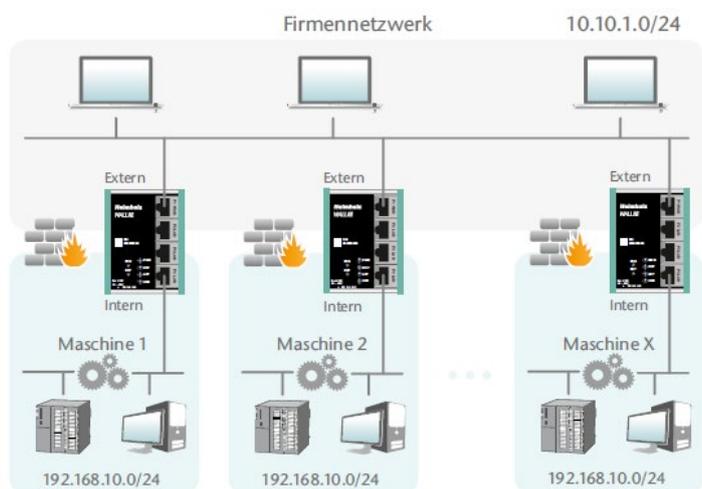
Broadcasts-Traffic wird generell am WALL IE gefiltert, somit wird das Zeitverhalten des Maschinennetzwerks nicht durch das Firmennetzwerk beeinträchtigt.

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.



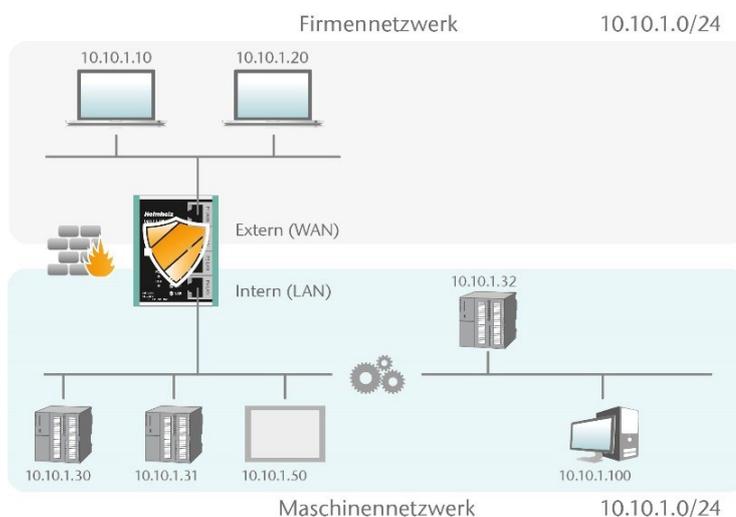
Wenn „NAT“ Ihr geplanter Anwendungsfall ist, dann lesen Sie bitte im Kapitel 6 weiter.

5.2 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.

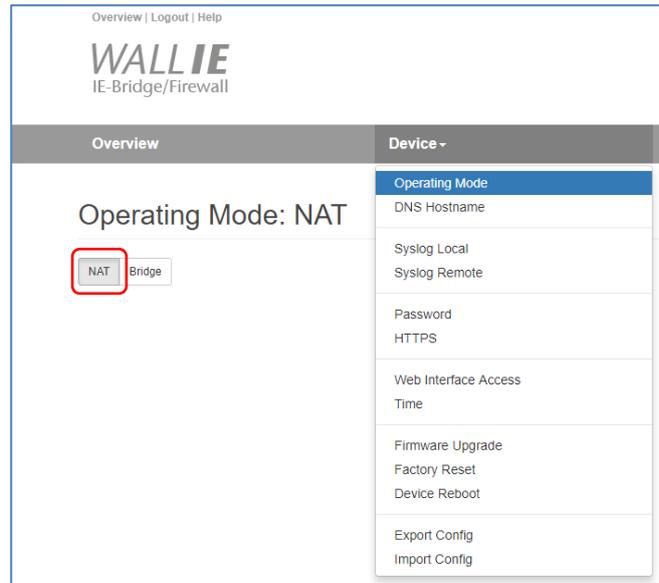
Dies erlaubt die Abtrennung eines Teils des Firmennetzwerkes ohne die Verwendung von unterschiedlichen Netzwerk-Adressen.



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

6 Anwendungsfall NAT

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



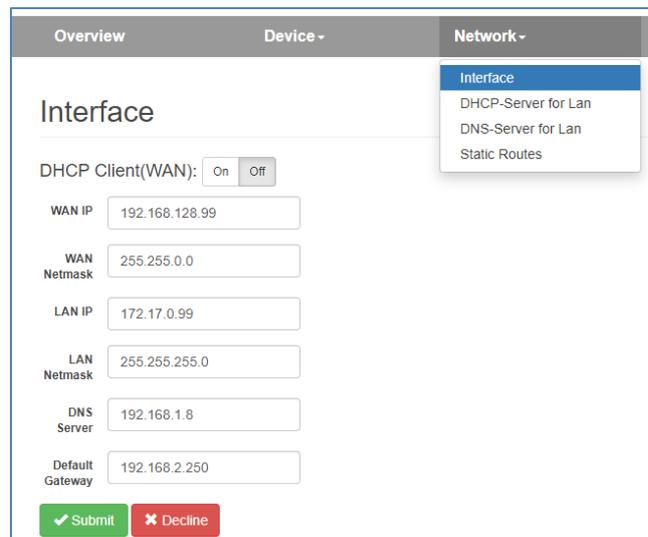
6.1 Anpassen der IP-Adressen im NAT-Betriebsmodus

Klicken Sie auf das Menü „Network“ und wählen das Untermenü „Interface“ aus. Hier können die IP-Adressen des 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 festgelegt 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.

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.



Für den SNTP-Dienst ist die Angabe eines DNS-Servers notwendig (siehe Kap. 11.8).



ACHTUNG

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



HINWEIS

Der WALL IE hat immer nur eine aktive Konfiguration. Änderungen an der Konfiguration werden immer sofort aktiv. Ein Neustart des WALL IE ist bei Änderung der Konfiguration nicht notwendig.

6.2 DHCP-Client am WAN-Interface aktivieren

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

The screenshot shows the 'Interface' configuration page for the DHCP Client. A green banner at the top indicates 'DHCP Client enabled for WAN interface'. Below this, the 'DHCP Client(WAN):' is set to 'On'. The 'LAN IP' is 172.17.0.99 and the 'LAN Netmask' is 255.255.255.0. There are 'Submit' and 'Decline' buttons at the bottom.

Die Verwendung des DHCP-Clients setzt voraus, dass im WAN-Netzwerk ein DHCP-Server aktiv ist. Die vom DHCP-Client bezogenen IP-Einstellungen sind auf der Overview-Seite durch Klick auf "INTERFACE" sichtbar.

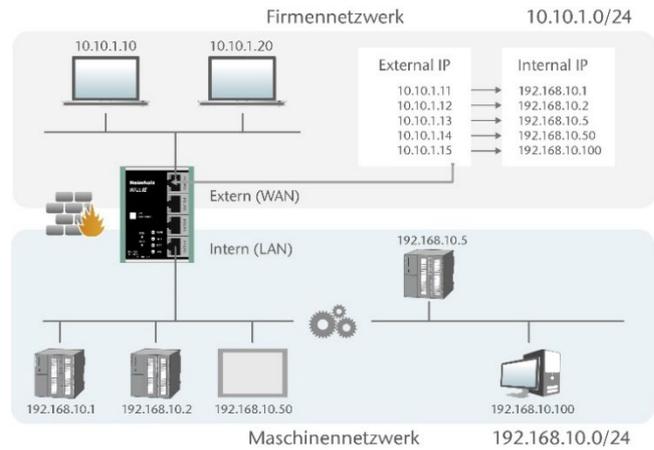
The screenshot shows the 'Overview' page of the WALL IE interface. On the left, there are 'Live Statistics' for Uptime (5 days 19:16:18), System Time (12/11/1970 23:33:43), and Current User (admin). On the right, there is a 'Device Configuration' table. A tooltip is open over the 'INTERFACE' row, showing the following settings:

Interface	IP	Netmask
LAN	172.17.0.99	255.255.255.0
WAN	192.168.20.123	255.255.0.0

6.3 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.



Overview Device Network NAT Packet Filter

Basic NAT

SNAT: WAN to LAN Traffic: Inactive

Activate Deactivate

#	External IP	Internal IP	Comment	Status
	10.10.1.11	192.168.10.1	CPU1	active

"Externe IP" ist eine freie IP-Adresse aus dem WAN-IP-Adressbereich. Diese darf noch keinem anderen Ethernet-Teilnehmer (im WAN) zugewiesen worden sein! "Interne IP" ist die Adresse, die dem physikalischen Gerät (dem Zielgerät) zugewiesen ist. WALL IE ordnet die IP-Adresse entsprechend der NAT-Regel zu und leitet die Pakete vom WAN zum LAN und umgekehrt.

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

Basic NAT

SNAT: WAN to LAN Traffic: Inactive

Activate Deactivate

#	External IP	Internal IP	Comment	Status
0	10.10.1.11	192.168.10.1	CPU1	
1	10.10.1.12	192.168.10.2	CPU2	
2	10.10.1.13	192.168.10.5	CPU3	
3	10.10.1.14	192.168.10.50	Visu	
4	10.10.1.15	192.168.10.100	PC	

External IP address Internal IP address Comment active

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

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

Mögliche Aktionen:  löschen einer Regel  bearbeiten einer Regel  kopieren einer Regel

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

Basic NAT

SNAT: WAN to LAN Traffic: Inactive

Activate Deactivate

#	External IP	Internal IP	Comment	Status
0	10.10.1.11	192.168.10.1	CPU1	

10.10.1.12-10.10.1.15 192.168.10.2-192.168.10.15 Panels active ▼ + ×

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



ACHTUNG

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

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

Packet Filter: WAN to LAN

Default Action: Accept Reject Drop

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



HINWEIS

Es können maximal 128 Basic NAT Einträge definiert werden.

6.4 Paketfilter „WAN to LAN“

Mit den Paketfiltern lässt sich der Zugriff zwischen dem 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.

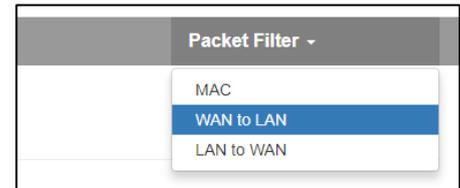
Folgende Filterkriterien auf Layer 3 und 4 stehen zur Verfügung: IPv4-Adressen, Protokoll (TCP/UDP/ICMP) und Ports.

Die Paketfilter stehen auch in der Richtung „LAN to WAN“ zur Verfügung, siehe Kapitel 6.6.

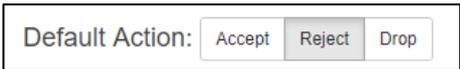
Im Menü „Packet Filter“ wählen Sie den Menüpunkt „WAN to LAN“.

Über die Option „Default Action“ 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“).

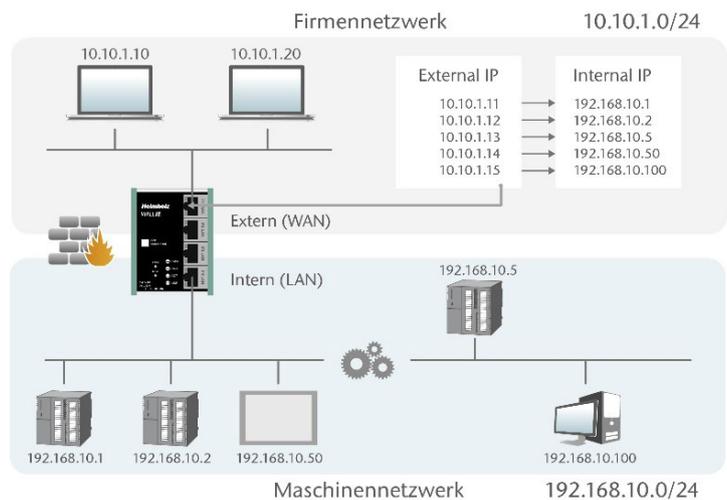
Wollen Sie erstmal nicht filtern, so stellen Sie die Default Action auf „Accept“.



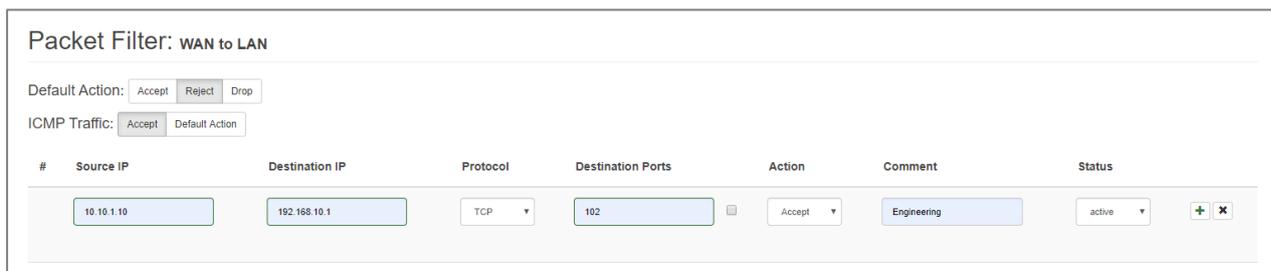
Um den Zugriff auf das Maschinennetzwerk auf bestimmte Teilnehmer im WAN zu beschränken, stellen Sie die Default Action auf „Reject“ oder „Drop“. „Reject“ sendet bei nicht erlaubten Telegrammen aus dem WAN eine Fehlermeldung zurück, „Drop“ verwirft das Telegramm ohne Fehlermeldung.



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 TCP Port 102 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“, „UDP“ 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	192.168.10.1	TCP	102	Accept	Engineering CPU1	
1	10.10.1.20	192.168.10.2	TCP	1:65535	Accept	CPU2	
2	10.10.1.20	192.168.10.5	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	10.10.1.1-10.10.1.9	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	All LAN access	

Für den Fall, dass die Source IP Adresse vorher überhaupt nicht bekannt ist, z.B. wenn WALL IE seine WAN-IP per DHCP bezieht, dann kann auch der gesamte WAN IP-Bereich freigegeben werden. Hierfür muss man „0.0.0.0-255.255.255.255“ bei **Source IP** eintragen.

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).

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

Mögliche Aktionen: löschen einer Regel bearbeiten einer Regel kopieren einer Regel.



HINWEIS

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

6.5 ICMP Traffic "WAN to LAN"

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

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

Default Action:
ICMP Traffic:

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

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

Packet Filter: WAN to LAN

Default Action:
ICMP Traffic:

#	Source IP	Destination IP	Protocol	Destination Ports	Action	Comment	Status
	<input type="text" value="10.10.1.20"/>	<input type="text" value="192.168.10.2"/>	<input type="text" value="ICMP"/>	<input type="text" value="Ports"/>	<input type="text" value="Accept"/>	<input type="text" value="CPU2 Ping"/>	<input type="text" value="active"/>

6.6 Paketfilter "LAN to WAN"

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

The screenshot shows the configuration page for a Packet Filter named "LAN to WAN". At the top, there are tabs for "Overview", "Device", "Network", "NAT", and "Packet Filter". The "Packet Filter" tab is active, and a dropdown menu is open, showing options: "MAC", "WAN to LAN", and "LAN to WAN" (which is selected). Below the tabs, the filter name "Packet Filter: LAN to WAN" is displayed. There are two sections for default actions: "Default Action:" with buttons for "Accept", "Reject", and "Drop"; and "ICMP Traffic:" with buttons for "Accept" and "Default Action". Below these is a table with columns: "#", "Source IP", "Destination IP", "Protocol", "Destination Ports", "Action", "Comment", and "Status". The table has a single row with input fields for "Source IP address", "Destination IP address", a "TCP" protocol dropdown, "Ports" input, an "Accept" action dropdown, a "Comment" input, and an "active" status dropdown. There are also "+" and "-" icons for adding or removing rules.

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.



HINWEIS

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

6.7 ICMP Traffic "LAN to WAN"

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

The screenshot shows the configuration options for ICMP Traffic. It has two sections: "Default Action:" with buttons for "Accept", "Reject", and "Drop"; and "ICMP Traffic:" with buttons for "Accept" and "Default Action".

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

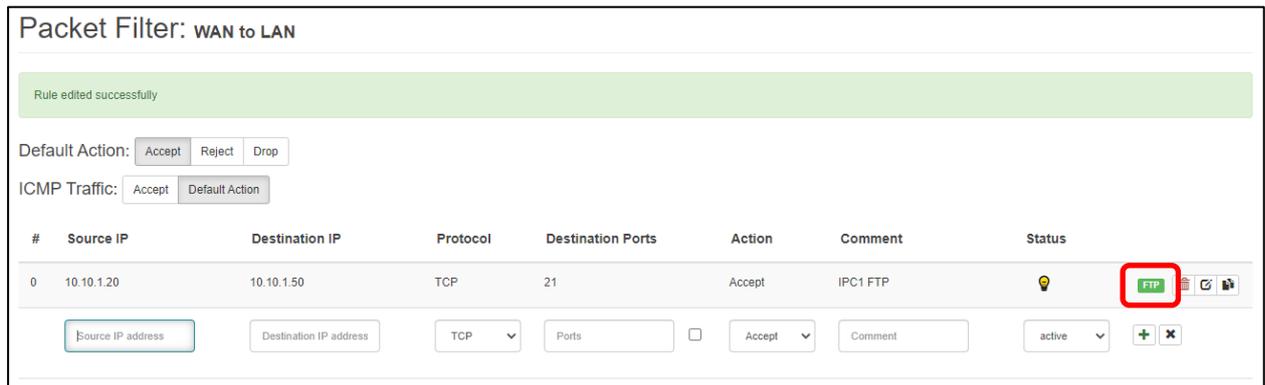
Alternativ zum generellen Freigeben von ICMP können auch einzelne Filterregeln festgelegt werden, in dem bei der Filterregel als Protokoll „ICMP“ ausgewählt wird.

6.8 FTP-Helfer für aktives FTP

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

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

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



Packet Filter: WAN to LAN

Rule edited successfully

Default Action:

ICMP Traffic:

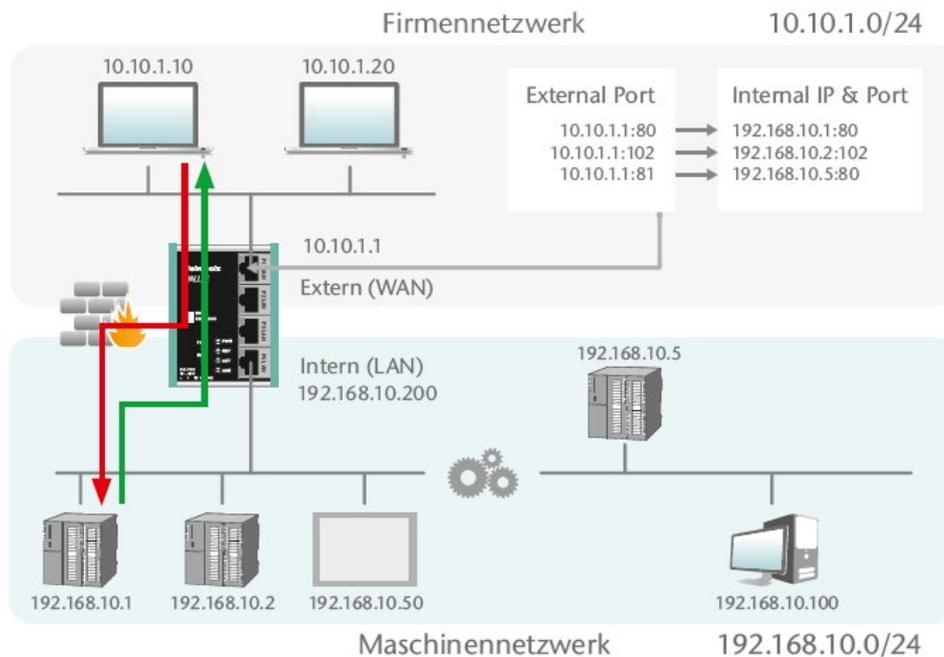
#	Source IP	Destination IP	Protocol	Destination Ports	Action	Comment	Status
0	10.10.1.20	10.10.1.50	TCP	21	Accept	IPC1 FTP	

Source IP address: Destination IP address: Protocol: Ports: Action: Comment: Status:

6.9 SNAT

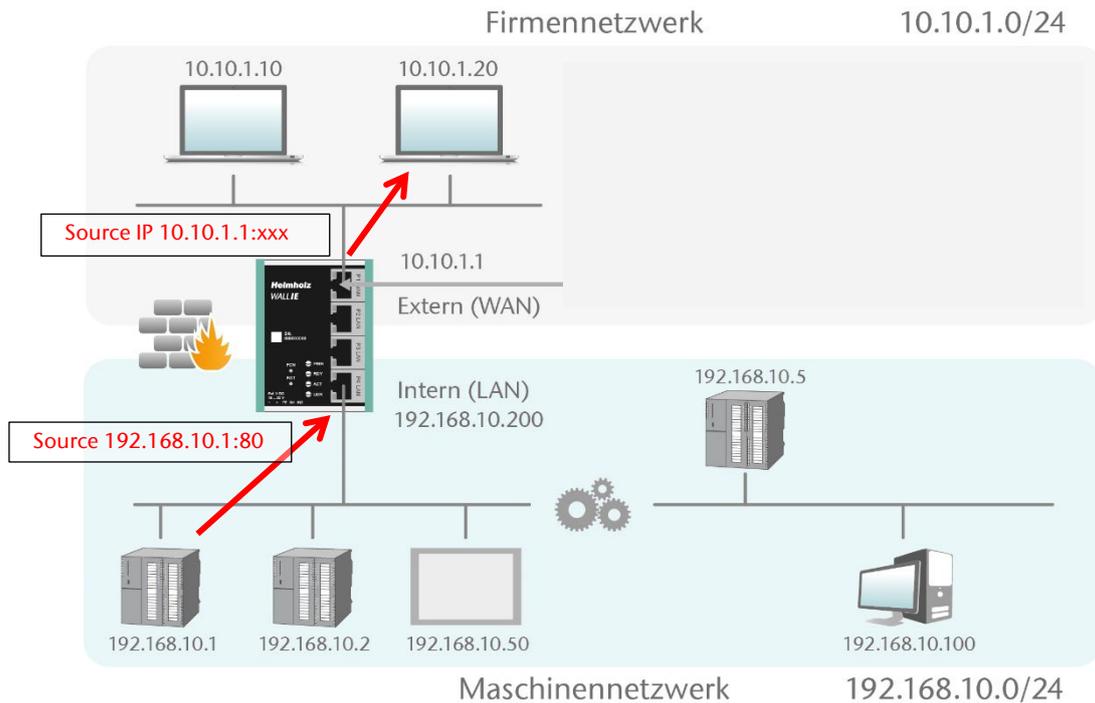
Mit der Funktion „SNAT (Source NAT)“ wird der eingehende Datenverkehr von der WAN Seite transparent an das LAN-Netzwerk weitergegeben. Bei allen Paketen, die auf LAN-Seite von WALL IE weitergeleitet werden, wird die Quell-IP-Adresse durch die LAN-IP-Adresse von WALL IE ersetzt.

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.



6.10 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.

Overview	Device -	Network -	NAT -
NAPT			Basic NAT
NAPT: LAN to WAN Traffic: Inactive			NAPT
<input type="button" value="Activate"/> <input type="button" value="Deactivate"/>			



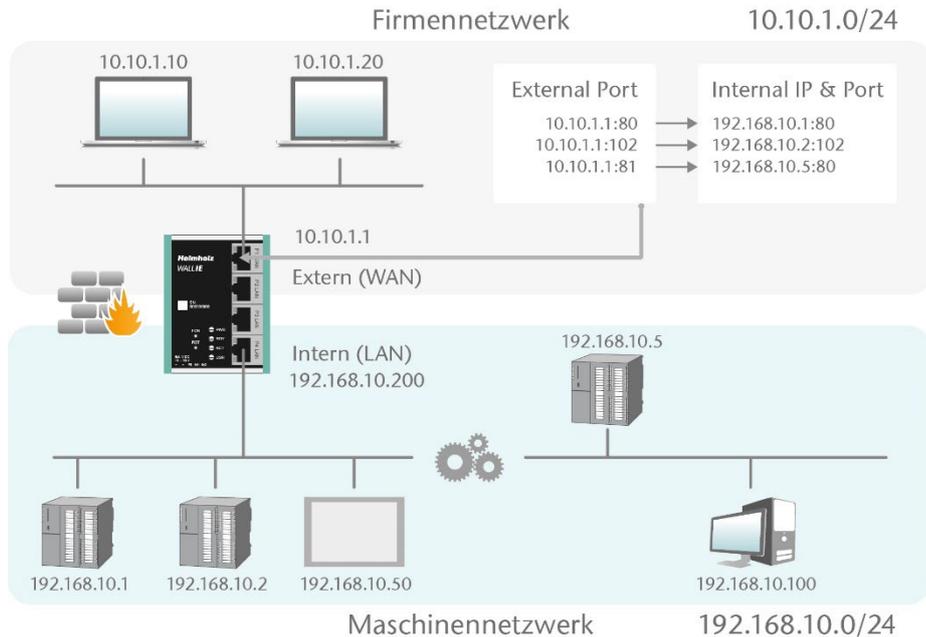
ACHTUNG

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.

6.11 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 192.168.10.1 über WAN durch den Zugriff auf die WALL IE eigene IP-Adresse 10.10.1.1 mit Port 81 erreicht werden.

The screenshot shows the NAT configuration page in the WALL IE web interface. The 'NAPT' tab is selected under the 'NAT-' menu. The status is 'NAPT: LAN to WAN Traffic: Inactive'. Below this, there are 'Activate' and 'Deactivate' buttons. The 'Port Forwarding: WAN (10.10.1.99) to LAN Traffic' section contains a table with one rule:

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

Below the table, there are input fields for 'Protocol' (set to TCP), 'External Port', 'Internal IP address', 'Internal Port', 'Comment', and 'Status' (set to active). There are also '+' and 'x' icons for adding and deleting rules.

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.

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

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

Mögliche Aktionen: löschen einer Regel, bearbeiten einer Regel, kopieren einer Regel.



HINWEIS

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



ACHTUNG

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



HINWEIS

Es ist nicht möglich die reservierten Ports 443 und 80 zu verwenden, wenn WALL IE die eigene Webseiten auf dem WAN aktiviert hat (Web Interface Access = "WAN and LAN", siehe Kapitel 11.6).



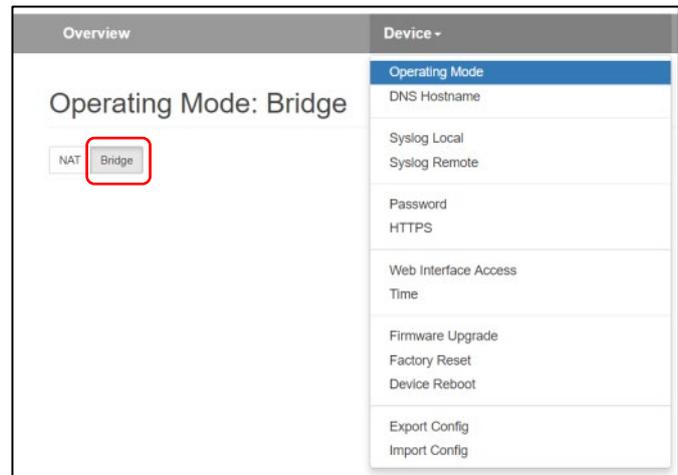
ACHTUNG

Es können maximal 128 Portforwarding Einträge erstellt werden.

7 Anwendungsfall Bridge

7.1 Bridge Modus aktivieren

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

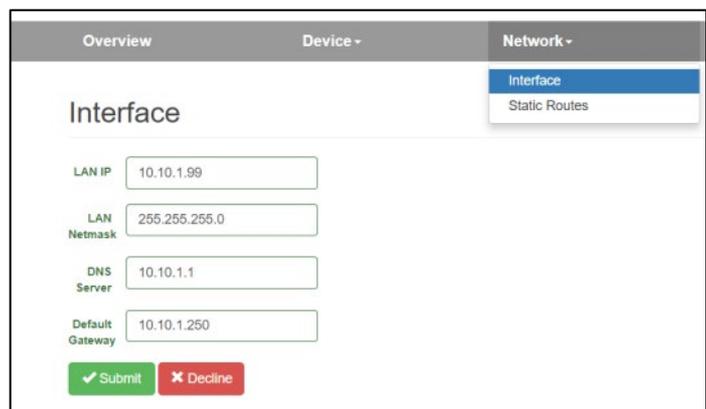


7.2 Anpassen der IP-Adressen im Bridge Betriebsmodus

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

Ein DNS-Server und ein Default-Gateway können ebenfalls festgelegt werden.

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



ACHTUNG

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

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



HINWEIS

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



ACHTUNG

Im Bridgemode 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.

Packet Filter: WAN to LAN

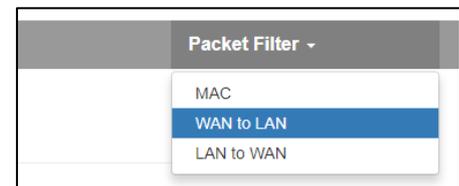
Default Action:

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

7.3 Paketfilter „WAN to LAN“

Mit den Paketfiltern lässt sich der Zugriff zwischen dem 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.

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

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

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

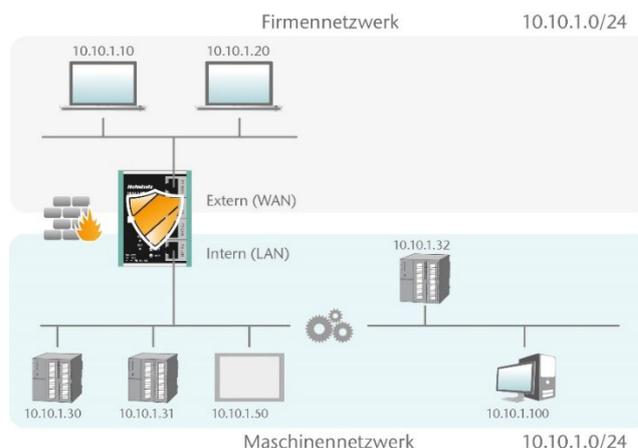
Wollen Sie erstmal nicht filtern, so stellen Sie die Default Action auf „Accept“.

Default Action:

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.

Default Action:

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 TCP-Port 102.



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

Packet Filter: WAN to LAN

Default Action:

ICMP Traffic:

#	Source IP	Destination IP	Protocol	Destination Ports	Action	Comment	Status
	<input type="text" value="10.10.1.10"/>	<input type="text" value="10.10.1.30"/>	TCP	<input type="text" value="102"/>	Accept	CPU1	active

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	10.10.1.121	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).



HINWEIS

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

7.4 ICMP Traffic "WAN to LAN"

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

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

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

Default Action: Accept Reject Drop
ICMP Traffic: Accept Default Action

Packet Filter: WAN to LAN

Default Action: Accept Reject Drop
ICMP Traffic: Accept Default Action

#	Source IP	Destination IP	Protocol	Destination Ports	Action	Comment	Status
	<input type="text" value="10.10.1.20"/>	<input type="text" value="10.10.1.50"/>	<input type="text" value="ICMP"/>	<input type="text" value="Ports"/>	<input type="text" value="Accept"/>	<input type="text" value="CPU2 Ping"/>	<input type="text" value="active"/>

7.5 Paketfilter „LAN to WAN“

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

The screenshot shows the configuration page for a Packet Filter named 'LAN to WAN'. At the top, there are navigation tabs: Overview, Device, Network, and Packet Filter. The Packet Filter tab is active, and a dropdown menu is open, showing options: MAC, WAN to LAN, and LAN to WAN (which is selected). Below the tabs, the title 'Packet Filter: LAN to WAN' is displayed. Underneath, there are two sections: 'Default Action:' with buttons for 'Accept', 'Reject', and 'Drop'; and 'ICMP Traffic:' with buttons for 'Accept' and 'Default Action'. Below these is a table with columns: #, Source IP, Destination IP, Protocol, Destination Ports, Action, Comment, and Status. The table has a single row with input fields for 'Source IP address', 'Destination IP address', a dropdown for 'TCP', a text field for 'Ports', a radio button, a dropdown for 'Accept', a text field for 'Comment', and a dropdown for 'active'. There are also '+' and '-' icons at the end of the row.

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.

7.6 ICMP Traffic "LAN to WAN"

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

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

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

This is a close-up of the configuration options for the Packet Filter. It shows the 'Default Action:' section with three buttons: 'Accept', 'Reject', and 'Drop'. The 'Reject' button is highlighted. Below it is the 'ICMP Traffic:' section with two buttons: 'Accept' and 'Default Action'. The 'Default Action' button is highlighted.

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“).

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

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

#	MAC	Interface	Comment	Status	
	<input type="text" value="24:EA:40:12:34:56"/>	<input type="text" value="ANY"/>	<input type="text" value="my Laptop"/>	<input type="text" value="active"/>	<input type="button" value="+"/> <input type="button" value="x"/>

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.

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

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



HINWEIS

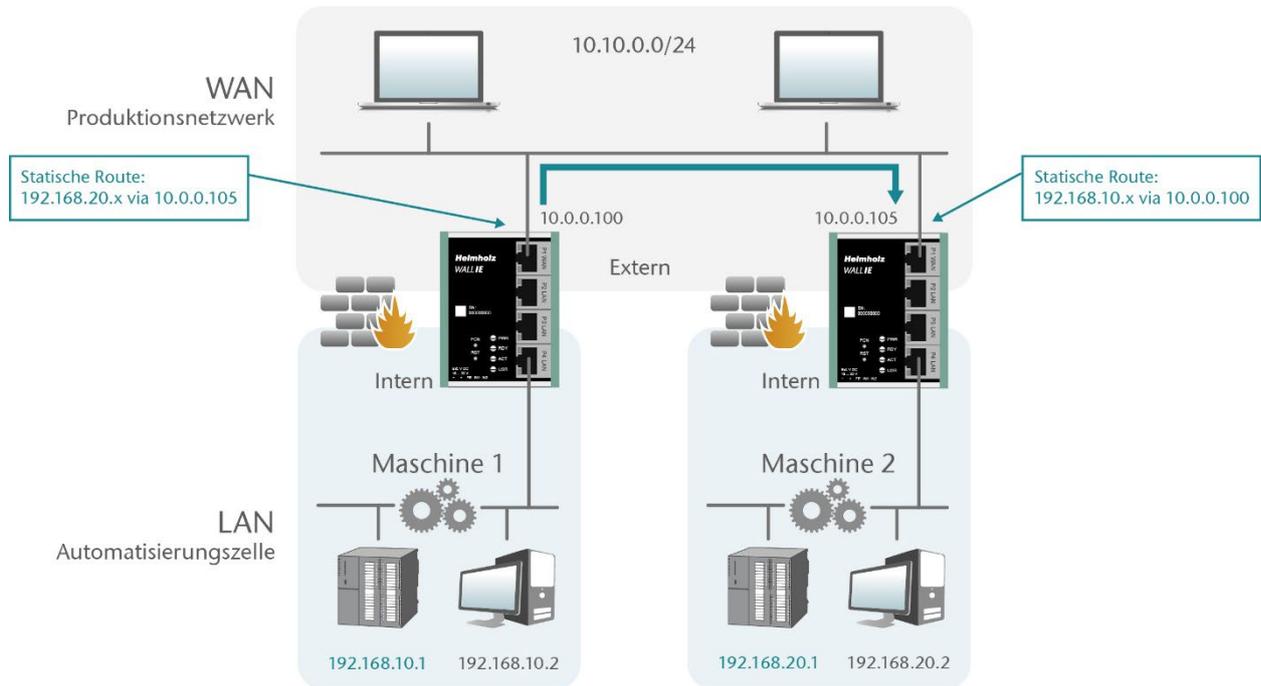
Im NAT-Mode wird die MAC-Filterung nur durchgeführt, wenn im IP-Header des Paketes die MAC-Adresse mit angegeben ist. Layer 2 Frames werden im NAT-Mode nicht weitergeleitet.

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

Es können maximal 128 MAC-Filterregeln definiert werden.

9 Statische Routen

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



Overview	Device	Network	NAT	Packet Filter
Static Routes				
#	Network	Netmask	Next Hop	Comment
	192.168.20.0	255.255.255.0	10.0.0.105	Machine 2 over WALL IE 2
				active



ACHTUNG

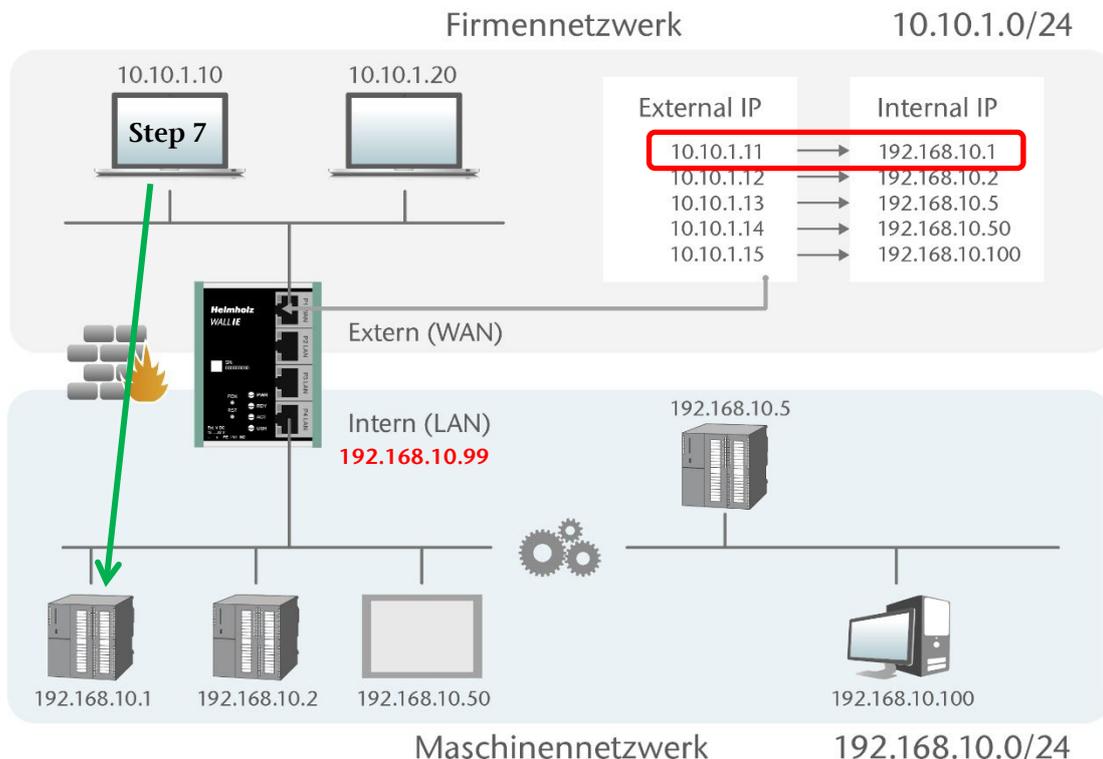
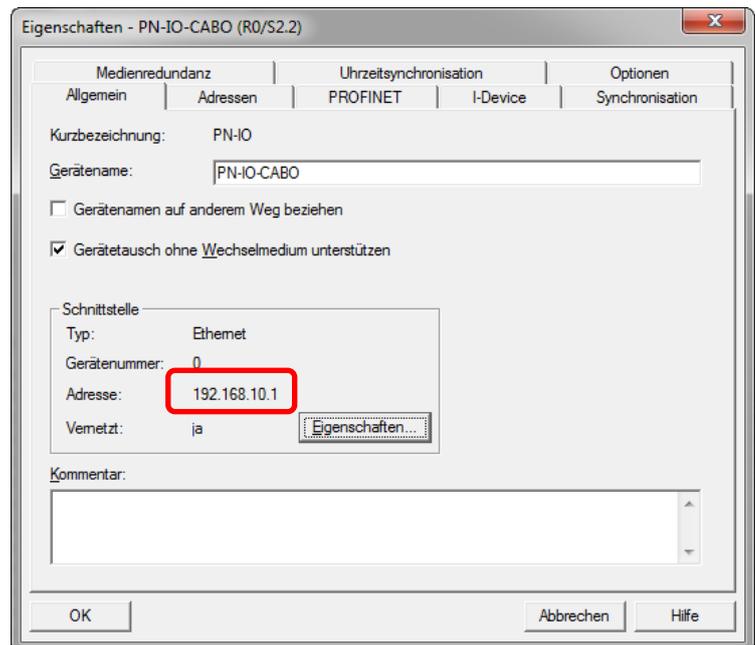
Um den Rückweg der Antwort zu ermöglichen, muss im entfernten Gateway (Maschine 2) auch eine Route zur IP-Adresse des WALL IE an der Maschine 1 eingerichtet werden!

10 Anwendung mit Simatic Step 7 / TIA Portal

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

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

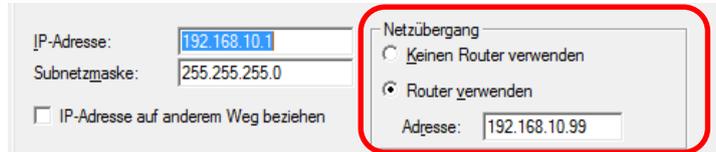
Die im Folgenden beschriebenen Lösungen können in angepasster Form auch für andere Anwendungen funktionieren.



10.1 Anwendung mit Step 7

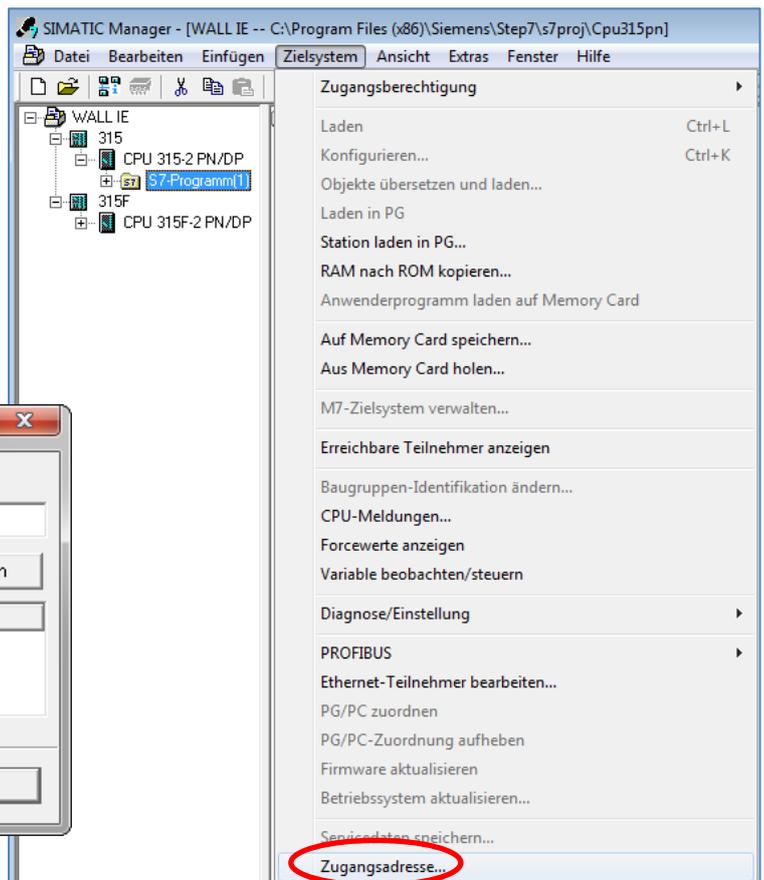
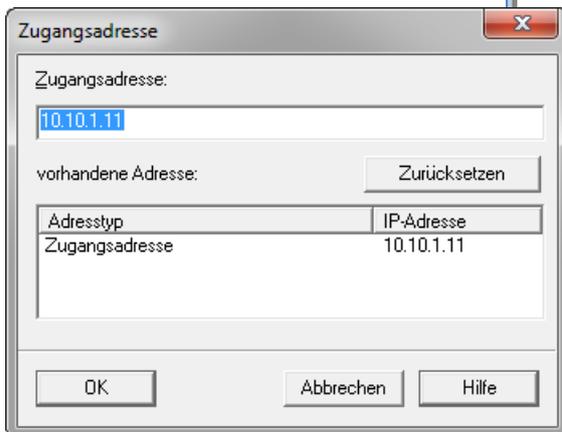
Step 7 bietet eine Möglichkeit auf eine CPU zuzugreifen und dabei aber eine andere als die im Projekt eingestellte IP-Adresse zu verwenden.

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



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

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



ACHTUNG

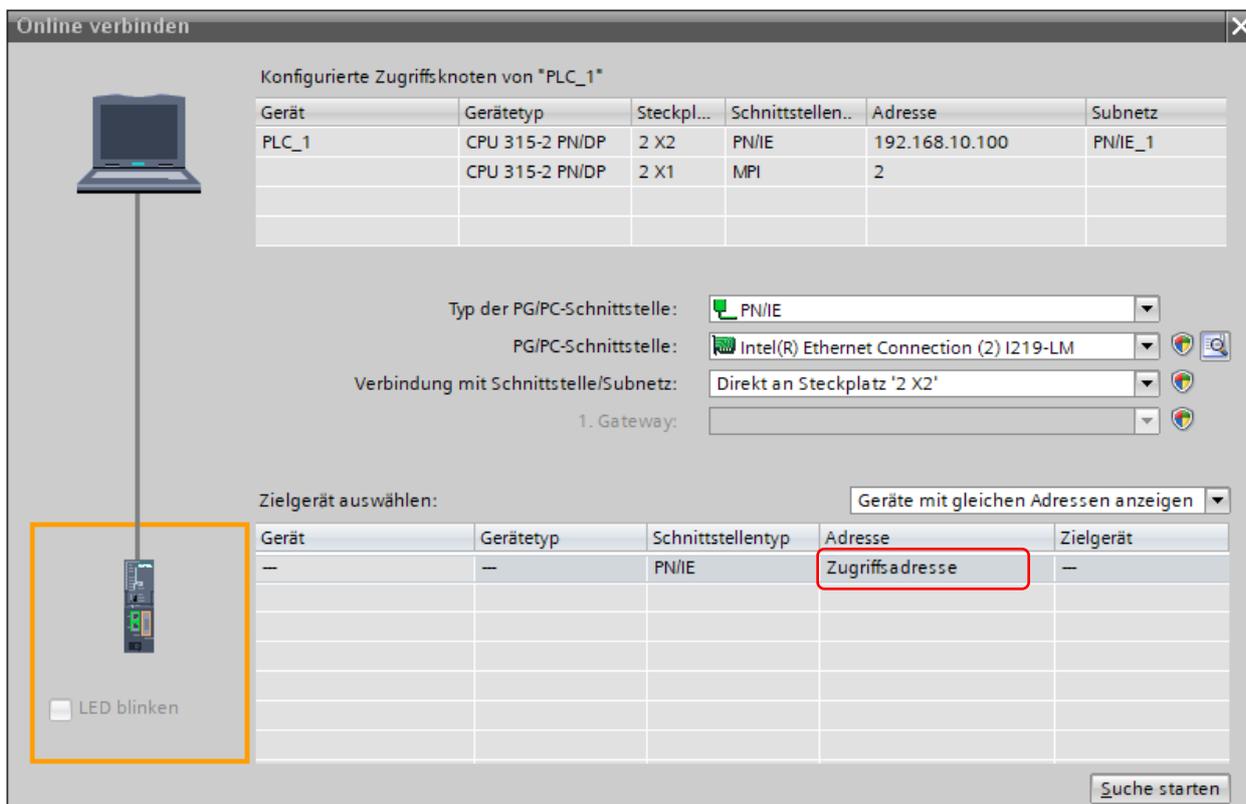
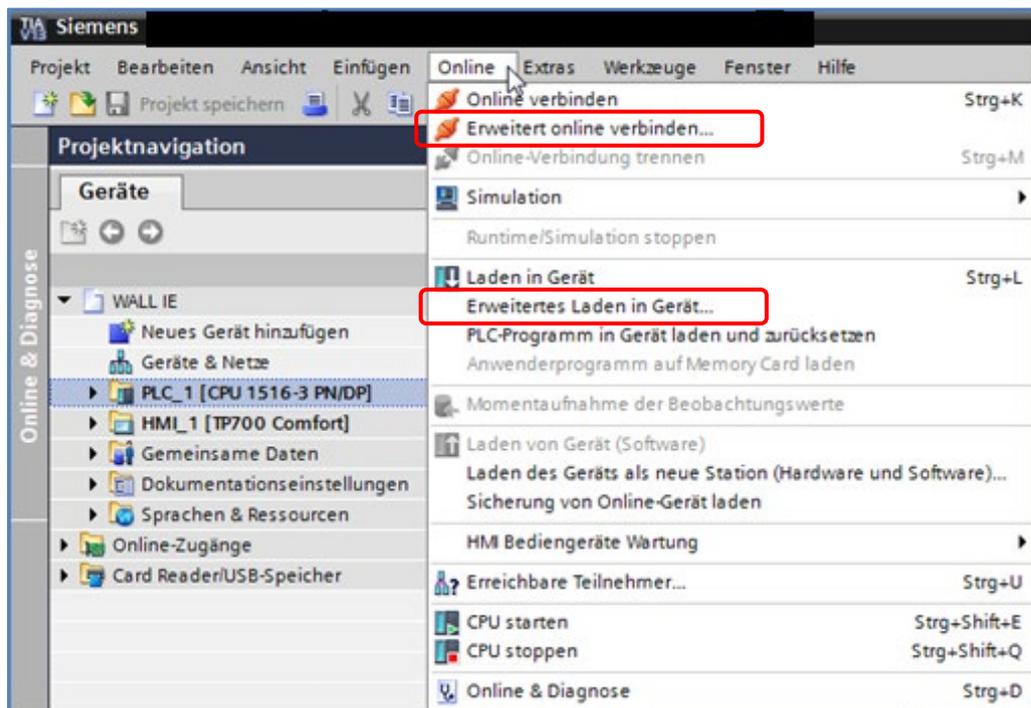
Diese Lösung ist nur im Betriebsmodus Basic NAT sinnvoll verwendbar. Bei NATP mit Portforwarding kann nur eine CPU erreicht werden, da der Simatic Manager immer mit dem nicht verstellbaren Port 102 auf die CPU zugreift.

Die Suche über die Siemens Funktion „erreichbare Teilnehmer“ funktioniert nicht durch die WALL IE Firewall hindurch.

PROFINET RT Telegramme werden nicht durch WALL IE durchgeroutet!

10.2 Anwendung im TIA-Portal

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



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

Online verbinden

Konfigurierte Zugriffsknoten von "PLC_1"

Gerät	Gerätetyp	Steckpl...	Schnittstellen..	Adresse	Subnetz
PLC_1	CPU 315-2 PN/DP	2 X2	PN/IE	192.168.10.100	PN/IE_1
	CPU 315-2 PN/DP	2 X1	MPI	2	

Typ der PG/PC-Schnittstelle:

PG/PC-Schnittstelle:

Verbindung mit Schnittstelle/Subnetz:

1. Gateway:

Zielgerät auswählen:

Gerät	Gerätetyp	Schnittstellentyp	Adresse	Zielgerät
PLC_1	CPU 315-2 PN/DP	PN/IE	10.10.1.11	PLC_1
--	--	PN/IE	Zugriffsadresse	--

LED blinken

Online-Statusinformation: Nur Fehlermeldungen anzeigen

- Es wird versucht, eine Verbindung zum Gerät mit der Adresse 10.10.1.11 aufzubauen.
- Verbindung zum Gerät mit der Adresse 10.10.1.11 aufgebaut.
- Scan und Informationsabfrage abgeschlossen.



ACHTUNG

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

Die Suche über die Siemens Funktion „erreichbare Teilnehmer“ funktioniert nicht durch die WALL IE Firewall hindurch.

PROFINET RT Telegramme werden nicht durch WALL IE durchgeroutet!

11 Weitere Funktionen

11.1 DHCP Server for LAN

Für das LAN-Netzwerk des WALL IE kann ein DHCP-Server aktiviert werden, um im LAN eine dynamische IP-Adressvergabe zu ermöglichen.

#	Mac Address	IP Address	Hostname	Expire In
1	24:ea:40:06:00:ae	172.17.0.220		23:56:46

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

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

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

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

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

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

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

Für eine feste Zuweisungen einer IP-Adresse über DHCP unterstützt WALL IE auch „Static Leases“:

#	MAC	IP	Comment	Status
0	11:22:33:44:55:66	172.17.0.222	PC1	active

11.2 DNS-Server für LAN

Für das LAN-Netzwerk des WALL IE kann ein DNS-Server aktiviert werden.

Der DNS-Server im WALL IE beantwortet DNS-Anfragen direkt auf dem LAN. Dazu benötigt WALL IE Zugriff auf DNS-Server auf der WAN-Schnittstelle.

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

The screenshot shows the 'DNS-Server for LAN' configuration page. The page has a header with 'Overview', 'Device -', and 'Network -'. The 'Network -' menu is open, showing 'Interface', 'DHCP-Server for Lan', 'DNS-Server for Lan' (selected), and 'Static Routes'. The main content area is titled 'DNS-Server for LAN:' and contains the following options:

- Activate Deactivate
- Filter win2k: On Off
- WAN domain over WAN DNS: On Off
- Use WAN DNS: On Off
- Primary DNS:
- Secondary DNS:

At the bottom, there are two buttons: a green 'Submit' button and a red 'Decline' button.

Auf der Konfigurationsseite „DNS-Server for Lan“ können die vom WALL IE verwendeten DNS-Server (Primary, Secondary) angegeben werden.

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

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

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

11.3 Hostname (WAN)

Der DNS Hostname des WALL IE kann für die WAN-Schnittstelle festgelegt werden.

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

The screenshot displays the 'Device Hostname' configuration page in the WALL IE web interface. The page is divided into two main sections: 'Overview' and 'Device -'. The 'Device -' section is active and contains a list of device settings. The 'Device Hostname' setting is expanded, showing a text input field with the value 'wallie-abc' and two buttons: a green 'Submit' button and a red 'Decline' button. The 'Device -' section also includes other settings such as Operating Mode, Syslog Local, Syslog Remote, Password, HTTPS, Web Interface Access, Time, Firmware Upgrade, Factory Reset, Device Reboot, Export Config, and Import Config.

11.4 Syslog Server

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

11.4.1 Syslog Local

Die lokale Syslog Anzeige listet die aufgezeichneten Ereignisse auf.

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

The screenshot shows the 'Log' configuration page. On the left, there is a 'Log' section with a red 'Clear' button and a table of log entries. On the right, there is a 'Device' menu with various options. The 'Syslog Local' option is highlighted in blue.

Overview	Device -																		
<h3>Log</h3> <p><input type="button" value="✖ Clear"/></p> <table border="1"><tr><td>1</td><td>Jan 31 17:15:00 : Manual time changed: ...</td></tr><tr><td>2</td><td>Jan 1 02:58:05 : Timezone set to: Europe/...</td></tr><tr><td>3</td><td>Jan 1 02:55:31 : Filter rule saved</td></tr><tr><td>4</td><td>Jan 1 02:53:44 : Filter rule saved</td></tr><tr><td>5</td><td>Jan 1 02:37:07 : Operating mode change...</td></tr><tr><td>6</td><td>Jan 1 02:37:07 : Finished loading bridge s...</td></tr><tr><td>7</td><td>Jan 1 02:37:07 : Timezone set to: Europe/...</td></tr><tr><td>8</td><td>Jan 1 02:37:07 : Creating bridge for bridg...</td></tr><tr><td>9</td><td>Jan 1 02:37:07 : Loading bridge system state</td></tr></table>	1	Jan 31 17:15:00 : Manual time changed: ...	2	Jan 1 02:58:05 : Timezone set to: Europe/...	3	Jan 1 02:55:31 : Filter rule saved	4	Jan 1 02:53:44 : Filter rule saved	5	Jan 1 02:37:07 : Operating mode change...	6	Jan 1 02:37:07 : Finished loading bridge s...	7	Jan 1 02:37:07 : Timezone set to: Europe/...	8	Jan 1 02:37:07 : Creating bridge for bridg...	9	Jan 1 02:37:07 : Loading bridge system state	<p>Operating Mode</p> <p>Syslog Local</p> <p>Syslog Remote</p> <p>Password</p> <p>HTTPS</p> <p>Web Interface Access</p> <p>Time</p> <p>Firmware Upgrade</p> <p>Factory Reset</p> <p>Device Reboot</p> <p>Export Config</p> <p>Import Config</p>
	1	Jan 31 17:15:00 : Manual time changed: ...																	
	2	Jan 1 02:58:05 : Timezone set to: Europe/...																	
	3	Jan 1 02:55:31 : Filter rule saved																	
	4	Jan 1 02:53:44 : Filter rule saved																	
	5	Jan 1 02:37:07 : Operating mode change...																	
	6	Jan 1 02:37:07 : Finished loading bridge s...																	
	7	Jan 1 02:37:07 : Timezone set to: Europe/...																	
	8	Jan 1 02:37:07 : Creating bridge for bridg...																	
9	Jan 1 02:37:07 : Loading bridge system state																		

11.4.2 Syslog Remote

Die Syslog Nachrichten können vom WALL IE auch an einen PC über das Netzwerk gesendet werden, auf dem ein Programm zur Syslog Aufzeichnung läuft.

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

The screenshot shows the 'Syslog' configuration page. On the left, there is a 'Syslog' section with 'Activate' and 'Deactivate' radio buttons, input fields for 'Syslog Host' (192.168.0.123) and 'Syslog Port' (514), and 'Submit' and 'Decline' buttons. On the right, there is a 'Device' menu with various options. The 'Syslog Remote' option is highlighted in blue.

Overview	Device -
<h3>Syslog</h3> <p><input checked="" type="radio"/> Activate <input type="radio"/> Deactivate</p> <p>Syslog Host: <input type="text" value="192.168.0.123"/></p> <p>Syslog Port: <input type="text" value="514"/></p> <p><input type="button" value="✔ Submit"/> <input type="button" value="✖ Decline"/></p>	<p>Operating Mode</p> <p>Syslog Local</p> <p>Syslog Remote</p> <p>Password</p> <p>HTTPS</p> <p>Web Interface Access</p> <p>Time</p> <p>Firmware Upgrade</p> <p>Factory Reset</p> <p>Device Reboot</p> <p>Export Config</p> <p>Import Config</p>

11.5 Passwort ändern (Password) / Userverwaltung

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

The screenshot displays the WALL IE web interface. At the top, there are navigation links for 'Overview | Logout | Help' and the 'Helmholz' logo. The main content area is divided into tabs: 'Overview', 'Device', 'Network', 'NAT', and 'Packet Filter'. The 'Device' tab is active, showing a dropdown menu with options: 'Operating Mode', 'DNS Hostname', 'Syslog Local', 'Syslog Remote', 'Password' (highlighted), 'HTTPS', 'Web Interface Access', 'Time', 'Firmware Upgrade', 'Factory Reset', 'Device Reboot', 'Export Config', and 'Import Config'. Below the menu, there are two password management sections: 'Administration Password' and 'IT User Password'. Each section has input fields for 'Old Password', 'New Password', and 'Repeat Password', along with 'Submit' and 'Decline' buttons. The 'IT User Password' section shows a 'Username' of 'it-user' and a 'User Enable' toggle set to 'Off'. Below this is the 'Machine User Password' section, which shows a 'Username' of 'machine-user' and a 'User Enable' toggle set to 'Off'. The interface is clean and professional, with a blue and white color scheme.

Neben dem User "admin", welcher uneingeschränkte Zugriffsrechte hat, unterstützt WALL IE noch zwei weitere User mit eingeschränkten Zugriffsrechten: "it-user" und "machine-user"

Zugriffsrechte des "it-user":

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

Zugriffsrechte "machine-user":

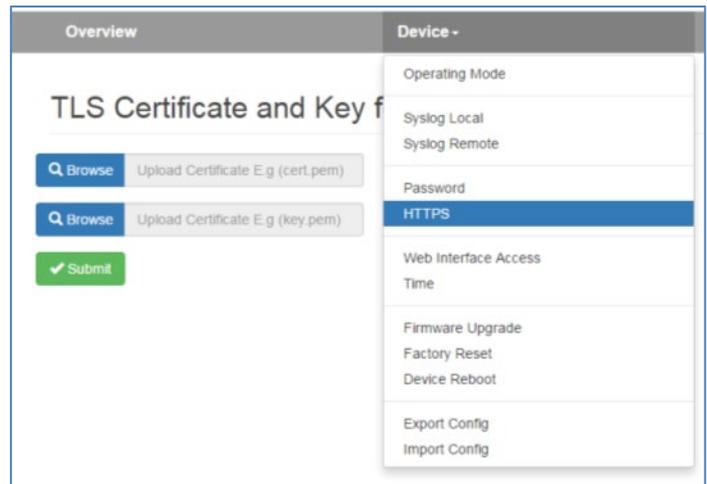
- Zugriff auf den WALL IE ausschließlich über das LAN-Interface
- Änderung der Einstellungen des DHCP-servers
- Ändern der Basic NAT/NAPT Regeln und Einstellungen

- Ändern aller Paketfilter Regeln
- Ändern der MAC-Filter Regeln
- Ändern der Static Routing Regeln
- Passwort des "machine-user" ändern
- Gerät neu starten
- WALL IE Konfiguration exportieren
- Alle anderen Einstellungen sind "ReadOnly"

11.6 Zertifikat hinterlegen (HTTPS)

Für die Webseite des WALL IE kann ein firmeneigenes Zertifikat hinterlegt werden.

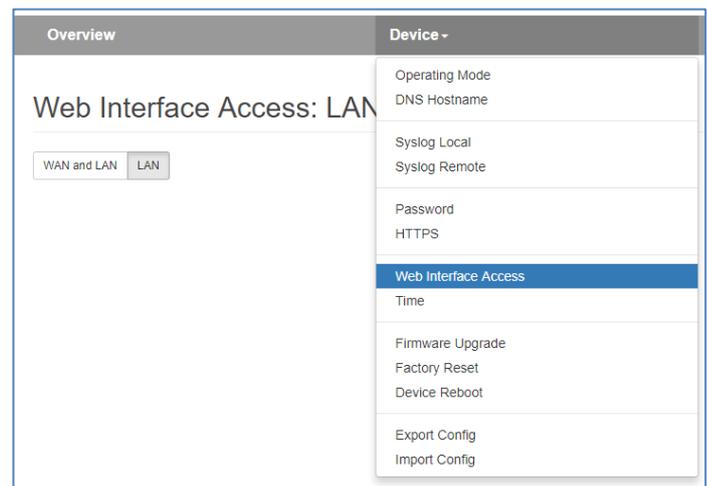
Damit kann sichergestellt werden, dass der Aufruf der WALL IE Konfigurationswebseite neben der HTTPS-Verschlüsselung auch vertrauenswürdig ist.



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

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

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

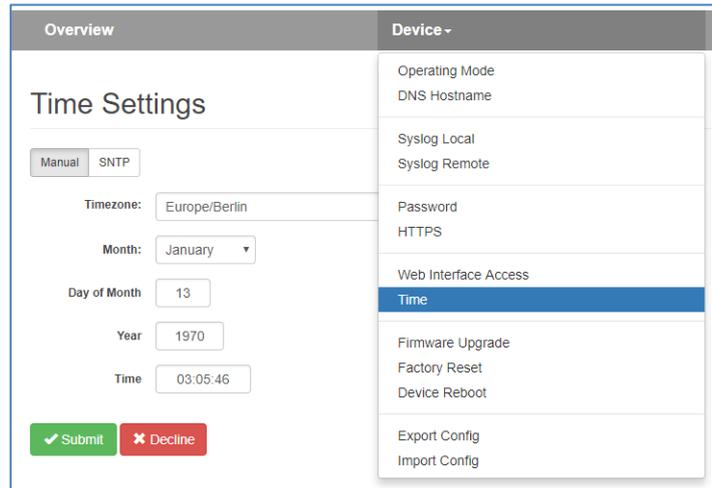


11.8 Zeiteinstellungen (Time)

Im Menü "Time" kann die Uhrzeit des WALL IE eingestellt werden.

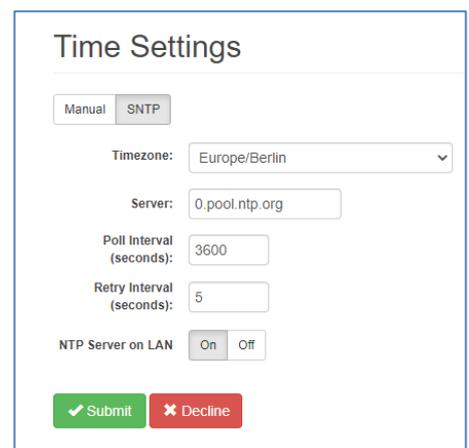
Die Uhrzeit wird hauptsächlich für die Syslog-Aufzeichnungen benötigt.

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



The screenshot shows the 'Time Settings' page in the WALL IE configuration interface. The 'Manual' tab is selected, and the time is set to 03:05:46 on January 13, 1970, in the Europe/Berlin timezone. A 'Device' menu is visible on the right side of the page, with 'Time' highlighted.

Mit der Option „NTP-Server on LAN“ kann WALL IE die aktuelle Zeit im LAN-Netzwerk über NTP den dort angeschlossenen Geräten zur Verfügung gestellt werden.



The screenshot shows the 'Time Settings' page in the WALL IE configuration interface with the 'SNTP' tab selected. The NTP server is set to 0.pool.ntp.org, and the 'NTP Server on LAN' option is turned on.



ACHTUNG

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



ACHTUNG

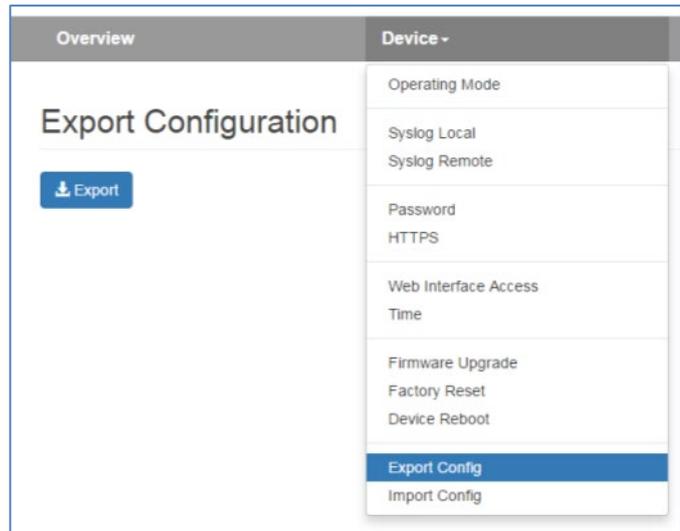
Für "SNTP" müssen in den Interfaceeinstellungen des WALL IE das Default-Gateway und der DNS-Server konfiguriert sein, damit der SNTP-Dienst den NTP-Server im Internet erreichen kann

11.9 Export / Import der Konfiguration

Die Konfiguration des WALL IE kann in eine lesbare Konfigurationsdatei exportiert und auch wieder importiert werden.

Damit ist es möglich sowohl ein Backup einer WALL IE Konfiguration zu sichern als auch eine bestehende Konfiguration für einen neuen WALL IE mit ähnlicher Anwendung zu kopieren.

Die Konfigurationsdateien hat die Dateiendung ".CFG".



Beispiel einer WALL IE Konfigurationsdatei:

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

12 Firmwareupdate

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

Link zur Firmware:

<https://www.helmholz.de/goto/700-860-WAL01> (WALL IE)

<https://www.helmholz.de/goto/700-862-WAL01> (WALL IE PLUS)

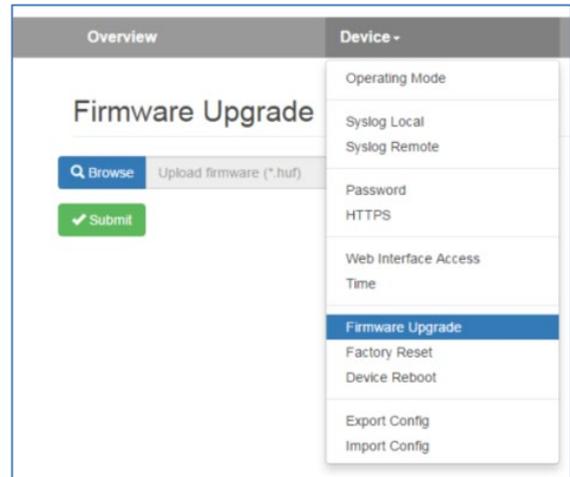
<https://www.helmholz.de/goto/700-863-WAL01> (WALL IE Compact)

Die Firmwaredatei kann an der Dateiendung "HUF" (Helmholz Update File) erkannt werden und ist verschlüsselt, um diese vor einer Manipulation 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 abschließend 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.

13 Rückstellen auf Werkseinstellung

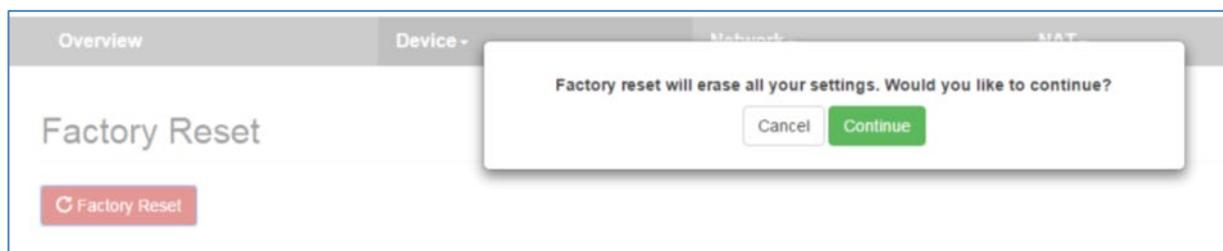
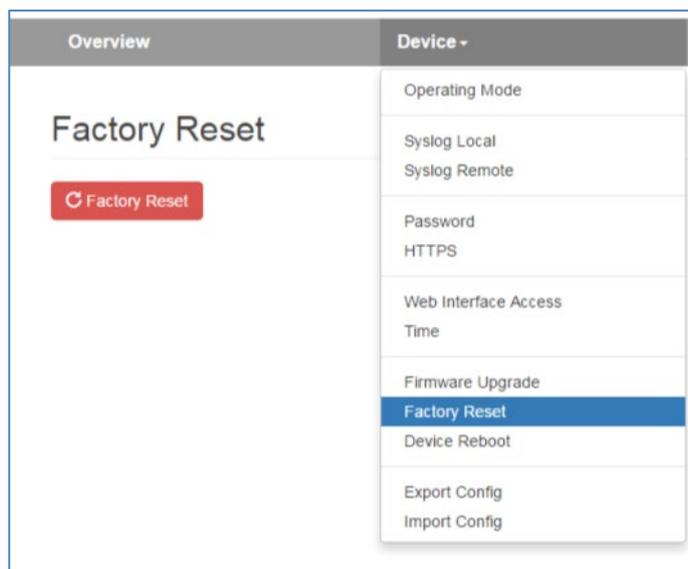
Das Rückstellen des WALL IE auf Werkseinstellung kann sowohl über die Webseite ausgelöst werden als auch ohne Zugriff auf das Gerät durch den „FCN“-Taster.

Es werden beim Rücksetzen des WALL IE die Konfiguration unwiederbringlich gelöscht und die IP-Einstellungen auf den Auslieferungszustand gesetzt. Die Firmware bleibt dabei auf dem aktuellen Stand.

13.1 Rückstellen auf Werkseinstellung über Webseite

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

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

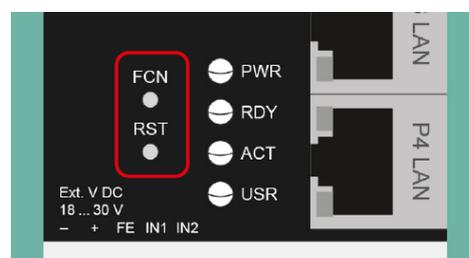


13.2 Rückstellen auf Werkseinstellung über Taster

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

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.



14 FAQ

Werden Broadcasts oder Multicasts durch den WALL IE durchgelassen?

Im NAT-Modus können Broadcast- und Multicast-Nachrichten zwischen Schnittstellen (WAN zu LAN oder LAN zu WAN) nicht weitergeleitet werden. Im Bridge-Modus ist es möglich, die Weiterleitung von ARP- und DCP-Nachrichten zu aktivieren.

Die Blockung von Broadcasts reduziert die Bus-Last in den beiden Netzwerken und erhöht die Echtzeitfähigkeit des Maschinennetzwerks.

Kann ich über den WALL IE PROFINET RT Telegramme senden?

Nein, PROFINET RT-Frames werden zwischen LAN- und WAN-Schnittstelle nicht weitergeleitet.

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

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

Kann der WALL IE mehrere Konfigurationen speichern?

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

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

In der "Overview" Webseite des WALL IE wird die aktive Firmware des WALL IE angezeigt.

Die aktuelle Firmware kann auf der Webseite www.helmholz.de heruntergeladen werden.

Das Einspielen der Firmware ist im Kapitel 12 beschrieben.



Software	
Firmware Version	V1.08.004
Linux Kernel Version	4.9.4
Open Source Software Licenses	

15 Technische Daten

15.1 WALL IE (700-860-WAL01)

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)
Pollution degree	2
Altitude	up to 2000m
Temperature cable rating	87 °C
RoHS	Ja
REACH	Ja

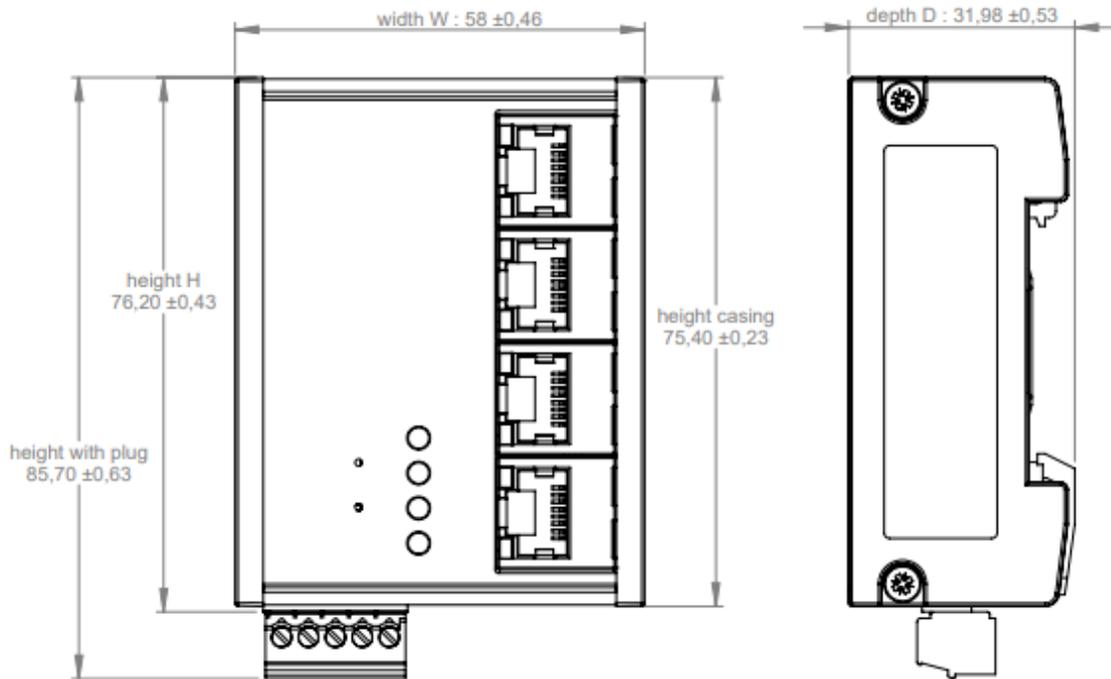
15.2 WALL IE PLUS (700-862-WAL01)

Artikelnummer	700-862-WAL01
Name	WALL IE PLUS, Industrial NAT Gateway/Firewall
Abmessungen (T x B x H)	34,5 x 101,5 x 76,5 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, NATPT)
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

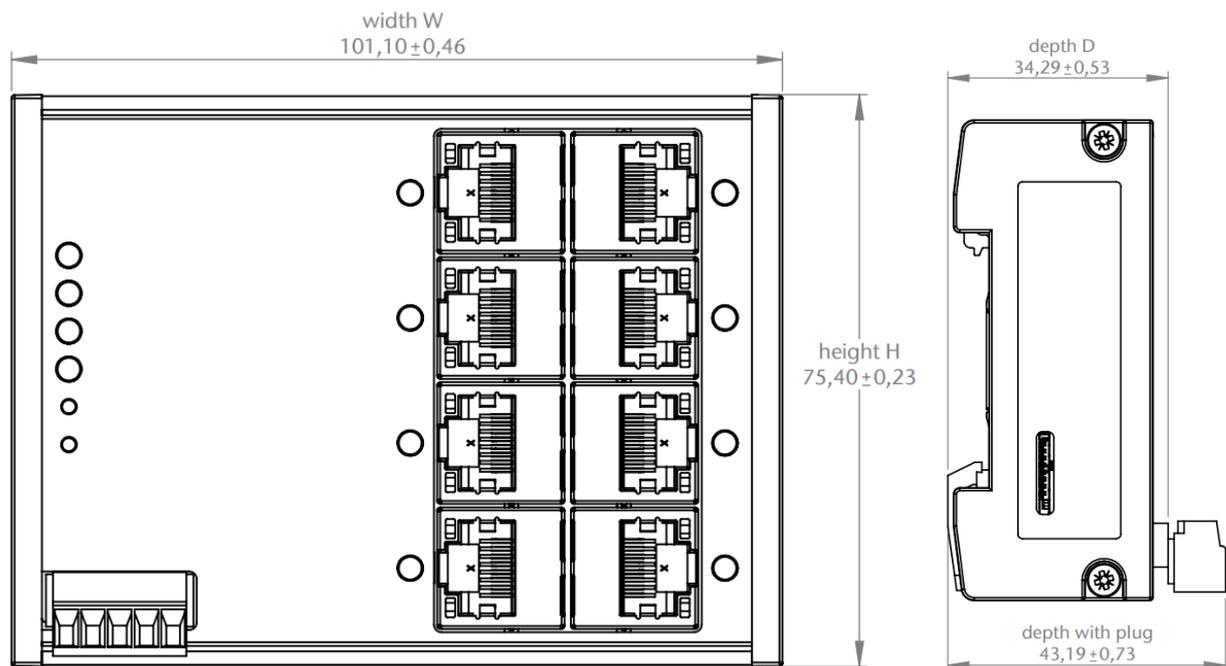
15.3 WALL IE Compact (700-863-WAL01)

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

15.4 Maßzeichnung WALL IE (700-860-WAL01)



15.5 Maßzeichnung WALL IE PLUS (700-862-WAL01)



15.6 Maßzeichnung WALL IE Compact (700-863-WAL01)

